Standards at the Edge of the Cloud

CLOUD COMPUTING ASSUMES COMMUNICATION AMONG PARTICIPATING COMPONENTS. The boundary between the collection of these components and the world of humans and devices has acquired a set of names that encompass different concepts, including fog computing (implying a highly diffuse, distributed cloud), edge computing (implying a clean boundary between connected and non-connected devices), and the Internet of Things (IoT). These concepts all assume a degree of connectedness that requires development of standards.

It's intrinsically difficult to restrain the scope of discussion when tackling topics related to the Internet of Things. The idea that a relatively small number of communication and automation methods can allow simple control over real-world devices is compelling, and the power of this idea naturally leads one to gloss over the many difficulties that come with implementing it. It's good to look at some counter-examples, therefore, from the outset.

Even among humans, communication is not a simple endeavor. Despite many attempts, some political, some altruistic, and most at their core economic, there has never been nor will there ever most likely be a single standard spoken or written language that spans all of humanity and crowds all other languages to non-existence. The closest we have come so far as a species may be HTML, and even this nearly-universal method shows the rapid evolution, fragmentation, and specialization that are characteristic of human endeavors.

In the light of this historical failure, and for other reasons that I'll cover in this column, we should be modest in our expectations for a single unifying paradigm and a single simple set of standards to cover the concepts mentioned above.

The Internet of Everything

A smooth intellectual transition can take place from observing that some real devices can be connected and automated to the assumption that everything can be treated as part of the same collection. It would not be correct, however, to assume that standards for communication protocols, hardware, device management, data formats, security, or any of the other myriad aspects of the "things" in the IoT will all become uniform and simplified on their own.

Even as individuals, people have a natural predisposition to pursue multiple options and to keep their choices flexible and variable. The Internet of Everything, if it comes to exist, will necessarily include many such things chosen to be included in this collection at various times and by different sets of people, all making choices according to their own needs and circumstances.

A large amount of device history and many different physical and communication choices will be aggregated together. Some fog, edge, and IoT aspects will be easier than others to include in the resulting aggregated collection, and some will require special considerations. As covered elsewhere in this special issue, a wide variety of sensors, inputs, and communication mechanisms with an equally wide range of reliability and security considerations will also have to be included.

ALAN SILL

Texas Tech University,
alan.sill@standards-now.org

2325-6095/16/$33.00 © 2016 IEEE

Table 1. A classification of layers and settings for IoT, edge, and fog computing along with examples of relevant standards and protocols.

Layer Type	Example Protocol, Standard, and/or Setting
Infrastructure	6LowPAN, IPv4/IPv6, RPL
Identification	EPC, uCode, IPv6, URIs
Communications / Transport	Wifi, Bluetooth, LPWAN
Discovery	Physical Web, mDNS, DNS-SD
Data and Messaging Protocols	MQTT, CoAP, AMQP, Websocket, Node
Device Management	TR-069, OMA-DM
Semantic	JSON-LD, Web Thing Model
Multi-layer Frameworks	Alljoyn, IoTivity, Weave, Homekit
Security	OTrP, X.509, Blockchain, OAuth, OpenID
Industry Vertical	Connected Home, Industrial, Utility, Telecom

Fog, Edge, and Non-Centralized Computing

These fog, edge, and IoT concepts share the basic characteristic that they are not concentrated in a single location. They are intrinsically distributed, with the characteristic assumption that they can in principle be connected through intermediate mechanisms. Such mechanisms may not be simple single interfaces, but may instead take place through multiple levels or layers, each of which is amenable to one or more standard specifications.

A useful breakdown of these multiple layers has been compiled at the postscapes.com web site. Again, because of history and the variety of communication methods and devices, multiple protocols can be applicable at each layer.

A summary of these topics and typical standards associated with each of them extended from the collection at this site is contained in Table 1. This collection is not at all exhaustive or definitive, but already serves to illustrate the variety of existing specifications and considerations for connecting devices and getting them to operate in IoT settings.

To fit the discussion of these topics in the space available in this column, I won't attempt to cover every topic in Table 1 or to expand each of these abbreviations. Some have been covered in previous columns in this series, and the rest can be found on the web site referenced. Instead, I'll concentrate the rest of this column on standards specific to the edge of the cloud, and especially on those that are receiving recent attention to adapt them to such settings.

Edge-Specific Communication Technologies

Communication technologies have experienced a burst of recent activity driven by the need to improve speeds and reliability across a wide range of transmission methods. Among the standards that have seen rapid evolution are several in the IEEE 802.x family of specifications (www.ieee802.org). Although these are similarly named and differ in designation only in the final numbers and letters, they differ widely in data format and signaling behavior and, for wireless specifications, in frequency spectrum and physical range.

For IoT applications, the standards that have seen the most recent activity include 802.11ad, aimed to replace 802.11ac as the highest-speed short-range WLAN communications; 802.11af, which is being proposed as a long-range wide-area protocol; and

802.11ah (also called "low power WiFi"), which is aimed at long-range but shorter-duration applications such as those for sensors and other sources of intermittent data. A standard designated as "WiFi" is differentiated from other wireless communications in that it always incorporates use of the full TCP/IP protocols.

These various specifications also use different portions of the radio spectrum. For example, 802.11ad is designed for 60 GHz communications using a region of the spectrum that has not been exploited yet due to cost and technology limitations, and that has not yet been agreed for use by international standards bodies.

Another, 802.11ah, uses portions of the spectrum between 54 and 790 MHz that have up to now been used for broadcast television, and therefore must be freed for other uses by individual governments through regulatory processes. It uses the already-crowded 900 MHz band, which is in use also by competing approaches including some non-standardized proprietary WiFi devices.

Similar evolution is taking place in the Bluetooth family of specifications. Low-energy Bluetooth is already built into almost all recent-generation smartphones, for example. Its advantages of low power requirements and inexpensive chip sets are counterbalanced by limited range and complications involving pairing and coordination of key sets among devices.

Emerging approaches to this problem combine Bluetooth access to local devices that serve as bridges to other communication technologies. The Bluetooth standard itself is evolving to include other variants, such as Bluetooth 4.2, which utilizes the Internet Engineering Task Force (IETF) IPv6/6LoWPAN protocol[1] to transmit IPv6 packets and to form corresponding IPv6 link-local addresses with stateless auto-configured addresses on IEEE 802.15.4 networks.

Cellular and mesh network communication approaches are also being applied to machine-to-machine communications, and to overlay networks that can extend and enhance the range and reliability of other networking methods. A wide variety of other communication technologies aimed at reducing the complexity and power requirements for dedicated industrial IoT applications is also being pursued.

A wireless data networking technology based on the earlier Highway Addressable Remote Transducer Protocol (HART) digital instrumentation wired automation standard called WiHART (or WirelessHART) also emerged in 2004. It was adopted as IEC 62591 in 2010, which was replaced in 2016 by an updated version.[2] The radio communications are defined by IEEE 802.15.4, and operate as a mesh protocol in the 2.4 GHz band.

Messaging Standards and Protocols

Beyond the physical transmission layer, selection of a data interchange method is also necessary. The most familiar of these is HTTP and its secure variant (HTTPS), which are specified in a range of IETF documents summarized at the working group website (httpwg.org/specs). Several other application, transport, and link layer protocols are also useful. (see the May/June 2016 "Standards Now" column for an overview of the definitions of these networking layers). [3]

For communications that can be intermittent or don't have to be completely received, the User Datagram Protocol (UDP)[4] is a useful method to carry out Internet communications. It can also be used to carry out IP communications in situations in which handshaking and verification of receipt of the individual message packets aren't necessary. Alternatives to UDP are TCP and the Stream Control Transmission Protocol (SCTP).[5]

Several IETF documents form the basis of the much more complex set of specifications underlying the Transmission Control Protocol (TCP)[6], which continues to receive ongoing attention from the Internet community due to its importance in various settings.

Methods to handle publish/subscribe messaging, such as the Message Queuing Telemetry Transport (MQTT)[7], can have advantages compared to the previously described protocols when used for machine-to-machine communication at high speeds.

The Constrained Application Protocol (CoAP)[8], another manufacturing-relevant specialized transfer standard, provides a "request/response interaction model between application endpoints, supports built-in discovery of services and resources, and includes key concepts of the Web such as URIs and Internet media types. CoAP is designed to easily interface with HTTP for integration with the Web while meeting specialized requirements such as multicast support, very low overhead, and simplicity for constrained environments."

The Advanced Message Queuing Protocol (AMQP)[9] is also a middleware messaging standard set. It can be applied using either publish/subscribe or point-to-point communication patterns. AMQP has a layered architecture and is organized into different parts to reflect that architecture.

The Data Distribution Service (DDS)[10] and related DDS Data Local Reconstruction Layer (DDS-DLRL) specifications handle data interchange tasks related to IoT systems. Unlike the other protocols mentioned here, DDS can handle content-aware network routing, data prioritization by transport priorities, and both unicast and multicast communications within the methods defined by the standard set itself.

The most popular data formats in cloud computing are JavaScript Object Notation (JSON) and XML. JSON shows significant evidence of adoption beyond the context of the JavaScript language, and may outlast it in the long run. For IoT and manufacturing settings, another interesting refinement is the Sensor Network Object Notation (SNON)[11], which is a representation based on JSON that includes some predefined fields that are especially useful in dealing with sensor data.

XML continues to receive attention and to be adapted to different IoT-related settings. The XML-based Extensible Messaging and Presence Protocol (XMPP) is designed for message-oriented middleware communications (see http://xmpp.org/extensions). Beyond its applications to human-oriented communications, XMPP is also used in smart electrical grid applications and a variety of industrial applications. Several extensions directly oriented toward use in IoT settings were published in late 2015.

Security in Edge and Distributed Settings

Because of the huge range in types of input, physical scale, frequency of communication and variety of users, it is nearly impossible to summarize the security considerations for IoT, fog and edge computing within a single set of paradigms. The variable that is hardest to control, it seems to me, will be the degree to which human users wish to change their minds about the security perimeter that applies to a given function.

An owner of a given device might want one set of restrictions to apply on one day to a given setting, but decide to change this to a different set of users or conditions on a different day or even within the same day based on personal whim or variable needs. This characteristic of security—that it is not a static concept but instead can be mutable and subject to complex decision-making characteristics—strikes me as more important than the technical details of specific security protocols, which are well studied. A larger discussion of this topic will have to wait until a future issue.

AS ALWAYS, THIS DISCUSSION ONLY REPRESENTS MY OWN VIEWPOINT. I'd like to hear your opinions and experience in this area. I'm sure other readers of the magazine would also appreciate additional information on this topic. Please respond with your input on this or previous columns. Please include news you think the community should know about in the general areas of cloud standards, compliance, or related topics. I'm happy to review ideas for potential submissions to the magazine or for proposed guest columns. I can be reached for this purpose at alan.sill@standards-now.org.

References

1. IETF Datatracker. "Internet Engineering Task Force (IETF) IPv6/6LoWPAN protocol," https://datatracker.ietf.org/wg/6lowpan/documents.
2. Industrial Electrotechnical Commission, 2016; https://webstore.iec.ch/publication/24433.
3. Sill, Alan, "Standards Underlying Cloud Network,"*IEEE Cloud Computing*, vol. 3, no. 3, 2016, pp. 76–80.
4. "User Datagram Protocol (UDP)," https://tools.ietf.org/html/rfc768
5. "Stream Control Transmission Protocol (SCTP)," https://tools.ietf.org/html/rfc4960
6. "Transmission Control Protocol," https://tools.ietf.org/html/rfc7414
7. OASIS, 2017; "Message Queuing Telemetry Transport (MQTT)," https://www.oasis-open.org/committees/mqtt/
8. "Constrained Application Protocol (CoAP)," https://tools.ietf.org/html/rfc7252

9. "Advanced Message Queuing Protocol (AMQP)," https://www.amqp.org
10. Object Management Group, 2017; "Data Distribution Service (DDS)," www.omg.org/spec/DDS
11. "Sensor Network Object Notation (SNON)," www.snon.org

ALAN SILL *is senior director of the High Performance Computing Center and adjunct professor of physics at Texas Tech University. He also co-directs the US National Science Foundation's multi-university "Cloud and Autonomic Computing" industry/university cooperative research center, and holds a position as visiting professor of distributed computing at the University of Derby. Sill has a PhD in physics from American University. He serves as president for the Open Grid Forum and is an active member of IEEE, the Distributed Management Task Force, and other cloud standards working groups, and serves on national and international computing standards roadmap committees. For further details, visit http://nsfcac.org or contact him at alan.sill@standards-now.org.*

myCS

Read your subscriptions through the myCS publications portal at **http://mycs.computer.org.**

Are Enemy Hackers Slipping through Your Team's Defenses?

Protect Your Organization from Hackers by Thinking Like Them

Take Our E-Learning Courses in the Art of Hacking

You and your staff can take these courses where you are and at your own pace, getting hands-on, real-world training that you can put to work immediately.

www.computer.org/artofhacking

IEEE NOT SO SECURE IEEE computer society