Governance for the Internet of things?

Laurent Toutain,
IMT Atlantique

Abstract:
The Internet, now the main vector for communicating information, has managed to federate a very large number of parties and joint protocols from various organizations of standardization and equipment-makers. Given that their current comes from batteries, the devices used on the Internet of things have a limited capacity and low energy consumption. Engineers have been forced to rework protocols by taking account of these new requirements while conserving the architecture that has made the Internet a success. A description of trends and interactions for building robust, interoperable services…

The Internet has become the main vector for communicating information, now including the transmission of data, telephony and television. How is it going to transmit communications involving connected devices?[1] This hegemony stems from the fact that the Internet is an open system that enables users to evolve while using a common set of specifications. Provocatively described as an hourglass,[2] this basic architecture is simply a rendering of the model with seven layers that underlies digital communications, each layer implementing a protocol. Assembling these layers results in a global communication service adapted to the information to be transmitted.

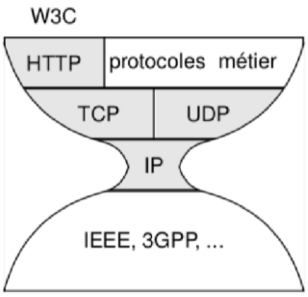
Internet protocols

Strictly speaking, the Internet lies at the center of this model, in between the protocols for transmitting data by type of connection (cable, radio, etc.) and the applications using these protocols. The engineers who designed the Internet insisted that this central protocol, Internet Protocol, have limited interactions with the lower and upper layers in the stack. IP, which adapts to any means of communication, proposes to the layers with applications an abstract representation of these means. Access to the network and the address system are thus made universal.

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references.
[2] DEERING S. (No date) "Watching the waist of the protocol hourglass", IETF 51, London, available at https://www.iab.org/wp-content/IAB-uploads/2010/11/hourglass-london-ietf.pdf

As studies on game theory have shown,[3] any layered, stacked system evolves toward a single central protocol while allowing for a wide variety of elements at the lowest and highest layers in the stack.

Figure 1: The Internet as an hourglass



A simple protocol boosts efficiency. Routers, the devices for routing the data packets containing information across the network, have to do their job as fast as possible so as to transmit a maximum of packets per second. Another advantage, IP does not specialize the network for one service or another; it only routes information toward the right destination. Protocols on the network's periphery (such as TCP) are assigned to verify that the data have been correctly received or, on the contrary for telephone communications, to authorize losses of data.

For the general public, the Internet refers to this whole assemblage of protocols and is often confused with the Web, the application that has popularized using the Internet. The Web formalizes interactions between client and server computers, the server managing "resources" referenced by a URI (Uniform Resource Identifier). The HTTP protocol formalizes the interactions between clients and servers through primitive integrals (*e.g.*, the GET method to obtain information on a server or PUT to write data into a resource managed by a server). By not keeping any state information on the server and by seeing to it that each request to a server is handled independently of the preceding request, systems can be built that cope with heavy traffic loads.

These principles are universal, having been generalized to other operations than Web browsers, for example to exchanges of information between programs. The representation of the data exchanged, which might contain URIs, has to be clearly specified: HTML is widely used for the Web; and XML has been designed for exchanging data. Since XML is too formal at times, programmers use JSON, a lighter format closer to the structures of data in modern programming languages (JavaScript, Python, Go, etc.).

As we see, the Internet has managed to federate a very large number of parties around a substantial set of joint protocols, which handle subsets of the full system. The Institute of Electrical and Electronics Engineers (IEEE) sets standards for the lower layers[4] of two major families of protocols: hardwired protocols (Ethernet) and wireless protocols (Wi-Fi). At the same level, the mobile broadband standard 3GPP[5] defines protocols for cell phones (4G). The Internet Engineering Task Force (IETF)[6] standardizes Internet protocols (IP), which uniformize the representation of the lower protocols and introduces a worldwide logical address system for connected devices. Above IP, protocols such as TCP or UDP check the integrity of transmitted data and of applications such as

[3] AKHSHABI S. & DOVROLIS C. (2011) "The evolution of layered protocol stacks leads to an hourglass-shaped architecture", paper presented at SIGCOMM'11, 15-19 August, Toronto, Canada. Available at https://www.cc.gatech.edu/~dovrolis/Papers/evoarch.pdf.

[4] http://standards.ieee.org/innovate/iot/stds.html

[5] http://www.3gpp.org

[6] http://www.ietf.org

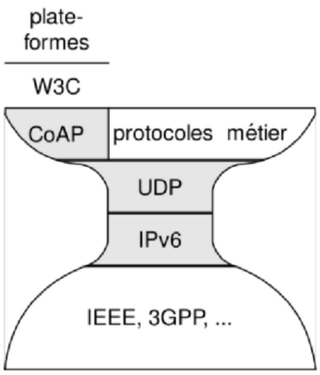
HTTP. The World Wide Web Consortium (W3C)[7] sets the standards for data and for linking them. Each of these standards organizations defines auxiliary protocols for assigning identifiers and enciphering communications.

This layered, stacked model is very flexible. It has laid the grounds for the evolution of the Internet: its penetration rate, increases in bandwidth and the types of applications used. The advent of the Internet of Things (IoT) is not as simple as its name would lead us to believe.

Adapting to the Internet of things

The devices used on the Internet of things have a limited capacity and low energy consumption, given the limited autonomy of a device's charged battery. Emitting and receiving data are the activities that consume the most energy. To maximize the autonomy of connected devices, all protocols have to be reviewed while keeping them in line with existing architectures so as to ensure compatibility.

Figure 2: The Internet of Things as an hourglass



Since most devices use wireless connections, organizations, like the IEEE for local networks or the 3GPP for cellular networks, are proposing changes in standards or new protocols. The Wi-Fi protocol, for instance, since it is continually receptive to the network, cannot meet up to the drastic constraints on energy for IoT devices. IEEE standard 802.15.4 was a first adjustment made to this protocol. By reducing the volume of the transmitted data, setting the transmission rate at 250 kbit/s and modifying Wi-Fi protocols so as to limit the phases of reception and transmission, it launched the first wave of communicating devices. It is also the basis of the ZigBee protocol; and Google uses it for its Thread architecture. An adaptation of this protocol to electricity grids enables Linky, a smart electricity meter installed in French households, to communicate.[8] The Bluetooth Low Energy standard has also moved toward lower consumption. BLE, present on mobile telephones, is intended for communications mainly in the health and fitness markets *via* GPS tracking devices. The European Telecommunications Standards Institute (ETSI) has modified the DECT standard used by wireless telephones into what is called DECT Ultra Low Energy. More recently, Wi-Fi has undergone a similar

7 http://www.w3.org

8 DOC TB (2018) "Compteurs Linky – Fantasmes et réalités: l'autopsie", *Canard PC Hardware*, 28 March on https://www.cpchardware.com/linky-fantasmes-et-realites/3/.

adaptation for the IoT: the HaLow amendment, which can be used in the United States on 900 MHz without a license.

The limited range of transmission, owing to the requirement for low energy consumption, implies two modes of operation: either in a star pattern around a central point (*e.g.*, BLE with mobile phones); or in a grid where the nodes serve as relays for reaching a destination. Building a grid has a cost in terms of energy. Furthermore, each node in the grid will be asked to share its energy in order to transmit other parties' messages.

To simplify the infrastructure, a network in a new category has been devoted to the IoT: the low-power wide-area network (LPWAN). As its name states, this network, while keeping energy consumption low, has a wide range: about 2 km in urban areas and 15 km in the absence of obstacles. On the contrary, traffic is very limited: approximately a hundred messages per day. Sigfox, a pioneer in this technology, has worked out its own transmission protocol and set up its network in several countries. On its heels has come the LoRa Alliance, with a different sales approach. Unlike Sigfox, the specifications are open so as to allow a large number of parties to intervene on the value chain. Two operators are proposing nationwide coverage in France. These two forms of technology operate on a license-exempt bandwidth of 868 MHz. To ensure fair access, regulatory authorities require that an emitter not emit more than 1% of the time. This is no drawback for connected devices, but it is a constraint on stations in the infrastructure, since they have to limit transmissions toward such devices. These networks are mainly intended for collecting information.

A late-comer to the market, 3GPP (with the evolution of 4G protocols and eventually 5G on line) is also proposing an energy-saving mode similar to LPWAN. By using the infrastructure and frequencies of service-providers, the restrictions imposed on unlicensed frequencies no long hold. This facilitates communications toward connected devices; and the network can coordinate instantaneous emissions and authorize new uses (such as communications with vehicles or robots).

During the 2020s, the majority of devices will be connected via LPWAN networks. However the service-provider's income per device will be very low (€1/year).

The protocols that make up this IoT must take up the challenge of curbing the impact on a device's memory. The IPv6 protocol, still not widely used on the Internet, is preferred for its addressing capacity. Thanks to 6LoWPAN, a layer of adaptation that reduces the IPv6 header's size (by a factor of 2 to 10), intermediate nodes can relay traffic from sensors. Compression does not necessitate a context. 6LoWPAN introduces a fragmentation mechanism for transmitting IPv6 packets on connections that limit the size of the data transmitted.

6LoWPAN has been adapted to other environments derived directly from IEEE 802.15.4. The Linky meters use this compression to transmit information between the smart meter and a concentrator located upstream on the grid. Linky only borrows the IPv6 and UDP layers from the Internet. The data transmitted use the formal representations defined by electricians (DLMS/CoSEM).

On LPWAN networks, the volume of data transmitted requires a specific mode of compression: static context header compression. This SCHC takes advantage of characteristics of these networks (absence of routing, a known traffic format) and reduces the impact of protocol headers to a few bits.

To further integrate devices in the Internet, the constraint application protocol (CoAP) replaced HTTP, while borrowing from it the procedures for naming and referencing resources and the primitive integrals used between client and server. In this architecture, since the server has the resource, the focus is on the sensor that can yield a measurement or the trigger that can set off an action. The processing capacity and energy supply are often quite limited. CoAP's major advantage is its full compatibility with HTTP. It is possible to switch from the one to the other via generic procedures not linked to a particular use and to thus install devices in an ecosystem built around the REST principles.

Security, in particular the enciphering of data, has also followed the same paths taken by the traditional Internet. There is an encryption above UDP that, equivalent to HTTPS, encrypts exchanges. CoAP has its own protection procedures, which encrypt exchanges from end to end (even when translated into HTTP) and simplifies implementation.

Platforms

The REST model, as represented by HTTP or CoAP, is not sufficient for managing a fleet of connected devices. It is also necessary to:

- construct in real time a directory of the devices present in the system and of their capacities;
- add controls for authorizing or refusing access to resources;
- formulate a universal abstract representation of data in order to ensure interoperability and the durability of data processing;
- define links between the collected data so as to formulate a representation of a system.

This is the job of platforms.

Each major operator in the cloud has designed its interface for retrieving and processing information from connected devices. The principal standards organizations worldwide are grouped in oneM2M,[9] which seeks to define a common interface and a standardized representation of information for the purpose of offering interoperability and breaking up technological bunkers. This global organization's work centers around the concept of resources, some of which are used to manage the Net, others to contain information from or for connected devices. oneM2M is above the Internet, which is seen only as a means for transmitting data packets from one point to another. It focuses on the fields of health, industry and domotics. Others organizations, such as the Open Connectivity Foundation (OCF)[10] or Lightweight M2M (LwM2M)[11] for managing home devices or machine-to-machine connections respectively, rely on IETF and W3C data representations.

Prospects

Contrary to the Internet, no governance has been formed around a global model of the Internet of Things. Each player is advancing by adapting its technology to the constraints of the devices to be connected. The basic bricks are now available, but their integration will still take time.

Consolidating these solutions, proprietary or standardized, passes through the market. Interoperability is, it is worth noting, a determinant in the adoption of a technique. If it is missing, the market will be deterred; and the applications, preferred that offer a fast return on investment. One challenge is to break up either technological bunkers (formed around applications because a generic solution was lacking at the time) or informational bunkers (by adopting standardized representations of information via ontologies). These bunkers impede the massive processing of data by artificial intelligence.

Interoperability guarantees continuity with what has already been installed. After all, systems will be rolled out over several decades and have to be adapted to changes in information systems.

---

9 http://www.onem2m.org/
10 https://openconnectivity.org/
11 https://www.omaspecworks.org/what-is-oma-specworks/iot/lightweight-m2m-lwm2m/