Article extrait de la REE 2016-5

L'Internet des objets

Deux technologies clés : les réseaux de communication et les protocoles

Deuxième partie

Introduction

JEAN-PIERRE HAUET
MEMBRE ÉMÉRITE DE LA SEE.
RÉDACTEUR EN CHEF DE LA REE

Dans un article précédent, publié dans la REE 2016-4, nous avons exposé le rôle clé que sont appelés à jouer les nouveaux systèmes de communication, et essentiellement de radiocommunication, dans le développement de l'Internet des objets (IoT). Cependant, établir des communications ne suffit pas. Il faut que les réseaux permettent des échanges de données et que ces données soient comprises par les entités qui les reçoivent.

Le but de l'Internet des objets est en effet d'étendre à des « choses », c'est-à-dire à des entités matérielles ou logicielles, les fonctionnalités offertes par l'Internet dans le domaine de la communication afin de leur permettre d'échanger entre elles ou avec des humains toutes sortes d'informations ou de données. Dans le succès de l'Internet, deux facteurs clés ont joué un rôle essentiel : **l'adressage** qui permet de repérer un utilisateur par son adresse IP (Internet Protocol) ou plus couramment par son adresse Web (l'URL ou Uniform Resource Locator) et **l'interopérabilité** qui permet, grâce à un ensemble de protocoles qui se sont progressivement imposés dans le monde Internet, à des usagers quelconques de communiquer et d'échanger des données et des services, où qu'ils soient dans le monde et quelle que soit l'origine des équipements qu'ils utilisent. On doit cette universalité de l'Internet au protocole IP qui est le principal composant de la suite de protocoles qu'utilise l'Internet. C'est lui qui permet d'encapsuler les données à transmettre dans des datagrammes (ou paquets) en y adjoignant les adresses IP des émetteurs et des destinataires, ce qui permet aux routeurs d'aiguiller convenablement lesdits paquets de façon qu'ils puissent parvenir à leurs destinataires.

Le protocole IP, de niveau 3 dans le modèle OSI, est le **facteur commun** à toutes les suites de protocoles Internet. Dans le modèle TCP/IP de l'Internet, qui diffère quelque peu du modèle OSI (figure 1), ces suites :

- reposent sur un niveau inférieur **d'accès au réseau** (correspondant aux couches 1 et 2 du modèle OSI), c'est-à-dire sur des solutions de communication, telles qu'Ethernet, le Wi-Fi ou les réseaux cellulaires, en utilisant un milieu de

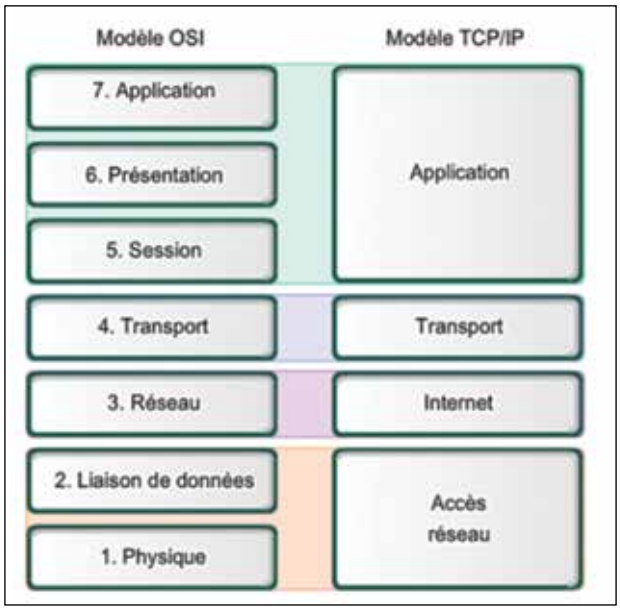

Figure 1 : Le modèle TCP/IP comparé au modèle OSI.

ABSTRACT

This article is a continuation of a first article devoted to new protocols used in the Internet of Things (IoT). It is dedicated to data transmission protocols that might be installed on top of the layers dealing with communications and more specifically radio communications.

In the first part, the role played at the layer 3 by the IP protocol is discussed. Although many solutions today claiming to be compliant with the IoT, do not implement the IP protocol, the future seems open to a general use of IP and in particular of IPv6.

In the second part, are discussed protocols aiming to adapt IPv6 to the lower layers of communication networks and in particular to local networks compliant with IEEE 802.15.4. The 6LoWPAN and TSCH protocols are presented.

In the third part, we discuss high level protocols and particularly application layers. New protocols such as CoAP, MQTT and OPC UA are introduced.

Finally an overview is given on cybersecurity issues and the need to use secure versions of Internet protocols, most of them having been developed at a time when the risks of cyber-attacks were negligible.

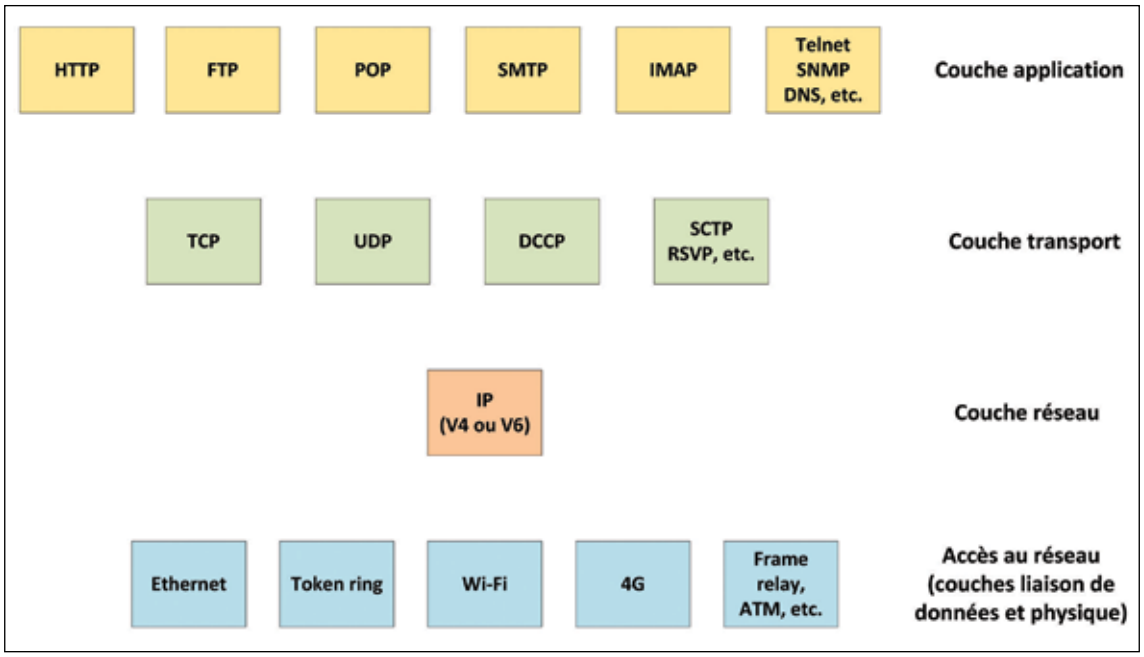

Figure 2 : Aperçu sur le diabolo des protocoles Internet.

transmission qui peut être filaire, radio au satellitaire : c'était l'objet de la première partie de cet article ;

- offrent au-dessus d'IP une interface de niveau supérieur, **la couche application**, qui permet d'accéder au travers du réseau à des services divers dont les plus connus sont le Web, la messagerie, l'échange de fichiers et la voix sur IP.

Dans ce triptyque vient s'insérer la couche transport qui est en fait un complément au protocole IP (on parlait initialement de TCP/IP et l'appellation reste fréquemment usitée) pour assurer des services de communication de bout en bout (origine-destination) que le protocole IP n'assure pas.

Le monde des protocoles Internet apparaît ainsi comme une sorte de diabolo dont les deux hémisphères seraient les couches d'accès réseau d'une part, les couches application d'autre part, cependant que l'axe central serait le protocole IP (figure 2).

Cette description est cependant simplificatrice : il existe dans le monde Internet beaucoup de protocoles aux finalités très techniques qu'il est difficile de positionner dans une échelle à quatre niveaux. Parmi les plus connus, on peut mentionner ARP, DNS, DHCP.

Par ailleurs, l'édifice construit en plus de trois décennies, s'est fissuré sous les attaques que lui ont portées les hackers et les cybercriminels. Des mesures d'adaptation ont dû être proposées, parfois à la hâte, pour rendre plus robustes des protocoles qui n'avaient pas été conçus pour faire face à la menace de cyberattaques. On a vu ainsi apparaître des variantes réputées sûres de protocoles largement répandus mais dont la vulnérabilité a été établie.

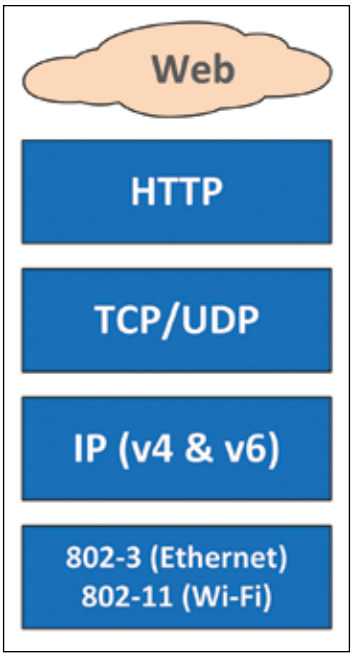

Figure 3 : Pile simplifiée des protocoles du Web.

Vouloir transposer au monde des objets les fonctionnalités de l'Internet pose évidemment la question de l'adéquation de ces protocoles aux spécificités du monde des choses. Pour faire simple, et puisque l'Internet des objets est souvent qualifié de Web 3.0, on doit se poser la question de savoir si la pile classique du Web classique (figure 3) reste adaptée au cas de l'IoT.

On a vu dans la première partie de cet article que la diversité des besoins à satisfaire conduisait à envisager l'utilisation de réseaux de communication beaucoup plus variés que les

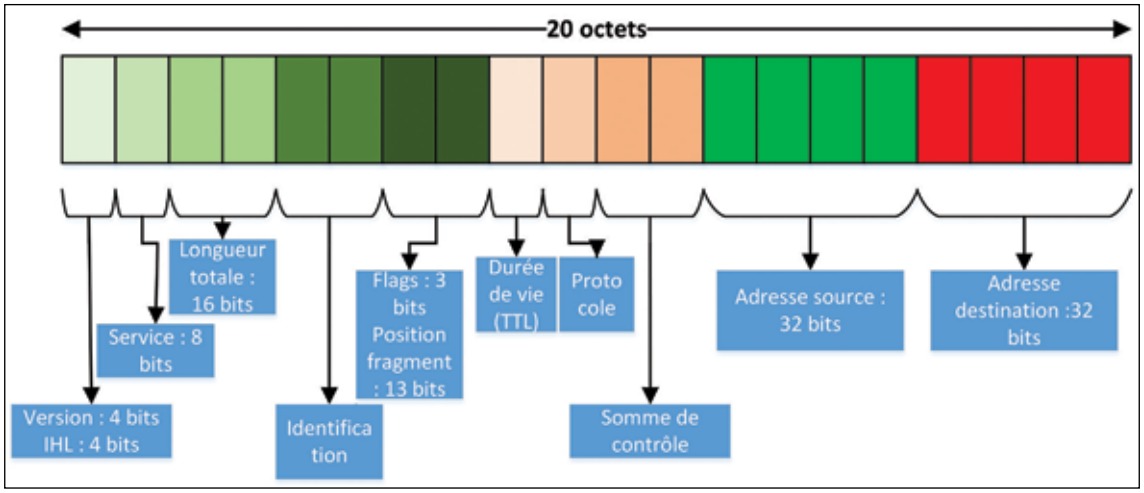

Figure 4 : Schéma minimal d'entête IPv4.

solutions conventionnelles de l'Ethernet et du Wi-Fi. Pour ne citer que les principales, on mentionnera les solutions LR WPAN (Low Rate Wireless Personal Area Network), basées sur les standards IEEE 802.15.4, et les solutions LPWAN (Low-Power Wide-Area Network). L'interfaçage de ces réseaux avec l'Internet pose des problèmes difficiles qui ne sont pas intégralement résolus à ce jour, notamment en ce qui concerne les solutions LPWAN.

Par ailleurs au niveau supérieur, le protocole HTTP et sa version sécurisée HTTPS ont été développés dans les années 1990 sans tenir compte des contraintes de ressources (capacité de traitement, mémoire, débit des communications) propres aux dispositifs constitutifs des systèmes Machine to Machine (M2M) ou IoT[1]. Il faut donc recourir à des protocoles dérivés voire à de nouveaux protocoles spécifiquement développés pour répondre aux besoins de l'IoT.

Avant d'aborder ces problèmes d'interfaçage de la couche IP avec les niveaux inférieurs et supérieurs, il faut se poser la question de l'adéquation du protocole IP aux finalités de l'IoT. Il peut paraître curieux de poser la question de l'utilisation du protocole IP dans l'Internet des objets dont on peut penser que l'essence même est le protocole IP. On constate cependant que l'appellation IoT tend aujourd'hui à être employée pour désigner toute architecture capable de rapatrier vers Internet des informations en provenance d'équipements de terrain sans que le protocole IP soit pour autant utilisé de bout en bout. Les avantages et les inconvénients de l'implémentation "full IP" méritent d'être discutés, de même que les perspectives de la version 6 de l'Internet : l'IPv6 qui, sans avoir été développée pour répondre aux besoins de l'IoT, offre des avantages mais aussi des inconvénients.

Ces questions sont abordées de façon synthétique dans les paragraphes qui suivent, en se plaçant dans une optique d'applications stationnaires ou faiblement mobiles. Les applications de l'IoT à des domaines fortement mobiles (véhicule connecté, transports ferroviaires) posent en effet des problèmes spécifiques (hand over, disponibilité, fiabilité notamment) qui demandent des analyses particulières.

Le protocole IP

IP : jusqu'où ?

L'idée de doter tous les équipements de la capacité de communiquer en mode IP est séduisante. C'est-elle qui est à la base du concept d'IoT et qui est susceptible de permettre, grâce à l'universalité du protocole, l'interopérabilité des équipements connectés et la connectivité au monde de l'Internet.

Cependant la connexion en IP jusqu'au niveau le plus reculé des systèmes pose des problèmes pratiques. Outre la question de l'adressage sur laquelle nous reviendrons à propos de l'IPv6, se pose la question de la lourdeur et de l'efficacité des protocoles IP. Une trame IP comporte au minimum 20 octets d'entête en IPv4 (figure 4) et 40 octets en IPv6, auxquels il faut ajouter les trames UDP (8 octets) ou TCP (≥ 20 octets).

Un tel « arsenal » est sans objet dès lors qu'il s'agit de transmettre des données de format modeste, typiquement de quelques octets, telles que celles émises par la plupart des capteurs. Ceci explique que beaucoup de solutions se réclamant de l'IoT soient en fait des solutions offrant une connectivité Internet « de bordure », c'est-à-dire des solutions dans lesquelles les informations sont rapatriées par des protocoles non IP depuis les capteurs (de façon bidirectionnelle

[1] La distinction entre les appellations M2M et IoT n'est pas toujours évidente. Notre perception est que le M2M se réfère davantage au monde professionnel alors que l'IoT englobe la mise en relation d'objets les plus divers (capteurs et actionneurs, mais aussi "wearables", véhicules connectés, etc.)

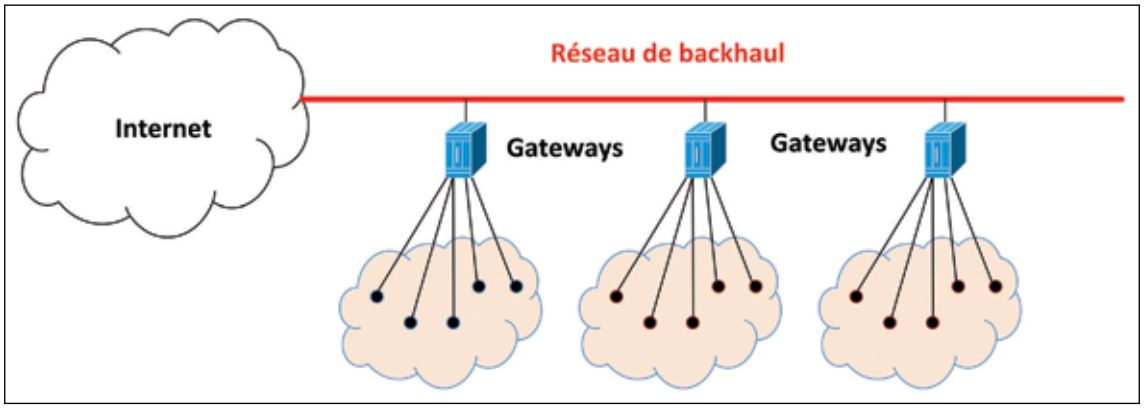

Figure 5 : Architecture de réseaux en grappes autour de gateways.

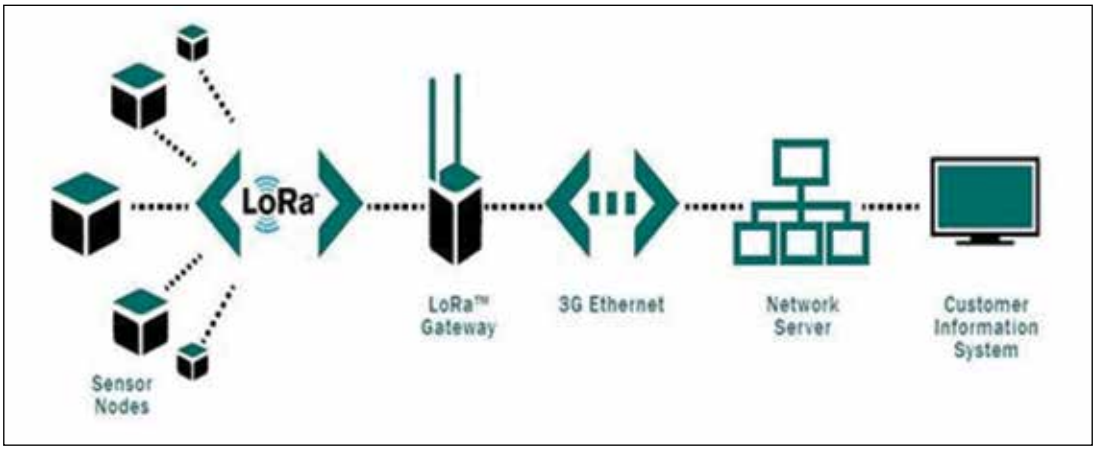

Figure 6 : Architecture LoRA.

ou non) vers un gateway de bordure qui assure la connexion avec le monde Internet et leur transfert ou amenée (leur "backhaul") vers des serveurs accessibles en IP (figure 5).

Une telle architecture « de grappes » correspond aux solutions récemment apparues dans le cadre des LPWAN : LoRa, SIGFOX notamment. Dans le cas de LoRa, les informations sont acheminées par le protocole LoRaWAN vers des gateways qui sont reliés à des réseaux filaires de type Ethernet ou à des réseaux cellulaires 3G ou 4 G. Ces réseaux assurent par des trames IP le transfert des informations vers les serveurs LoRa (figure 6).

Une telle vision, qui correspond à la vision traditionnelle des systèmes de contrôle à longue distance ou Scadas, a le mérite de l'efficacité et de la compatibilité avec des ressources matérielles limitées. Cependant, une partie des avantages attendus de l'Internet des objets disparait :

- les équipements ne sont plus accessibles directement par une adresse IP et donc par les protocoles de l'IoT fonctionnant sur IP spécialement dédiés aux applications distantes (tels que MQTT abordé plus loin) ;
- le réseau de grappe est un réseau propriétaire créant une dépendance, limitant l'interopérabilité et le roaming ;
- ce réseau est un réseau en étoile construit autour du gateway de bordure, ce qui a des avantages sur le plan de la simplicité de configuration et de la dynamique de fonctionnement, mais ne permet pas de bénéficier des avantages des réseaux maillés, en termes de reconfiguration des trajets et donc de disponibilité.

Après la publication de l'édition 13 du 3GPP (mars 2016), il va être intéressant d'observer comment les solutions assurant la course en tête des protocoles LPWAN vont résister aux deux solutions normalisées par le 3GPP sous forme de profils additionnels aux profils 4G LTE (figure 7) :

- e-MTC (ou LTE-M), extension logicielle de la 4G LTE, dédiée au trafic M2M et offrant un débit pouvant aller jusqu'à 1 Mbit/s ;
- NB-IoT, intégrée dans la LTE mais utilisant une interface radio distincte, offrant un débit de quelques dizaines de kbit/s et spécifiquement dédiée aux applications de l'IoT.

Outre leur intégration aux réseaux 4G, préfigurant les fonctionnalités qui seront offertes par la 5G, ces solutions ont l'avantage d'être ouvertes quant au format de données et de pouvoir accueillir des datagrammes IP aussi bien que d'autres formats. La solution NB-IoT, validée en Espagne et

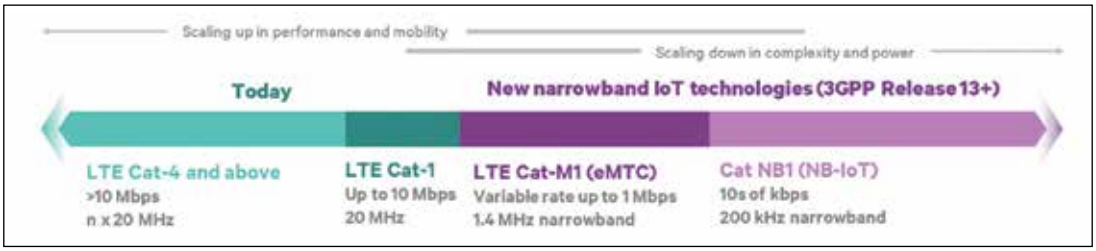

Figure 7 : Nouveaux profils 4G LTE destinés au M2M et à l'IoT.

[8000:0000:0000:0000:0123:4567:89AB:CDEF]

pouvant être noté

[8000::123:4567:89AB:CDEF]

Figure 8 : Format d'adresse IPv6.

en Turquie par Vodaphone, pourrait être lancée commercialement dès 2017.

Sur le plan des LR WPAN, on évoquera plus loin les développements faits, dans le cadre du protocole 6LowPAN, pour réaliser un couplage aussi étroit que possible entre l'Internet et les réseaux locaux IEEE 802.15.4. Moyennant le recours à l'adressage IPv6 évoqué ci-après, 6LowPAN permet de transformer le réseau local 805.15.4 en une sorte de mini-Internet local dont les abonnés peuvent être adressés depuis un client distant au travers d'un proxy.

En conclusion, la question : « Jusqu'où le protocole Internet doit-il descendre ? » n'a pas aujourd'hui de réponse unique. Elle doit être abordée en fonction des exigences à satisfaire et des contraintes à respecter. Nous pensons cependant que l'argument de « ressources limitées » n'aura qu'un temps. On voit en effet apparaître des SoC (System on a Chip) spécialement dédiés à l'IoT, donc à faible consommation mais intégrant processeur, mémoire, interfaces de communication et modules de sécurité. Il nous semble donc, mais ce point peut être sujet à discussion, que les solutions supportant le protocole IP finiront par l'emporter.

Il reste à savoir de quel IP il s'agit et ceci pose la question de l'émergence de l'IPv6 en substitution à l'IPv4.

IPv6 – IPv4

Le protocole IPv6 a été développé dans les années 1990 afin de succéder à l'IPv4 dont les capacités d'adressage apparaissaient insuffisantes pour faire face au développement de l'Internet. Il est devenu un standard officiel de l'IETF en 1998 et a fait l'objet de nombreux perfectionnements depuis.

La caractéristique principale de l'IPv6 est d'utiliser un format d'adresses sur 128 bits au lieu de 32 bits dans l'IPv4 (figure 8). Il est donc possible de créer des milliards de milliards d'adresses (2^{128}) différentes en IPv6 alors que l'IPv4 plafonne à quatre milliards d'adresses environ (2^{32}). Ceci permet de se passer du mécanisme de traduction d'adresse et du protocole NAT (Network Address translation) qui permet de regrouper plusieurs adresses privées autour d'une même adresse IPv4 publique. Ceci élimine un degré de complexité en permettant un adressage direct des abonnés.

Simultanément, l'IPv6 remédie à certains inconvénients de l'IPv4 : il utilise des entêtes de longueur fixe (40 octets) alors que celles de l'IPv4 varient de 20 à 60 octets, ce qui simplifie le routage. La fragmentation éventuelle des datagrammes ne se fait plus au niveau des routeurs mais au niveau des machines émettrices qui reçoivent, éventuellement, un message d'alerte "*Packet too big*".

IPv6 incorpore également dans sa spécification le protocole sécurisé IPsec.

Le protocole bien connu de couche 2 de l'IPv4, l'ARP (Address Resolution Protocol), permettant à un nœud de découvrir et d'identifier les autres nœuds situés sur un même segment, est remplacé par le protocole NDP (Neighbor Discovery Protocol) qui peut être sécurisé par une méthode cryptographique (SEND – Secure Neighbor Discovery Protocol), remédiant ainsi aux vulnérabilités du protocole ARP.

L'IPv6 n'a pas été développé pour répondre aux besoins de l'Internet des objets. Il offre cependant des atouts précieux pour répondre aux exigences de l'IoT :

- un adressage sans limite permettant l'identification unique de chaque objet et l'extensibilité de n'importe quelle architecture ;
- le non recours au protocole ARP qui rompt, dans l'IPv4, la connexion point à point ;

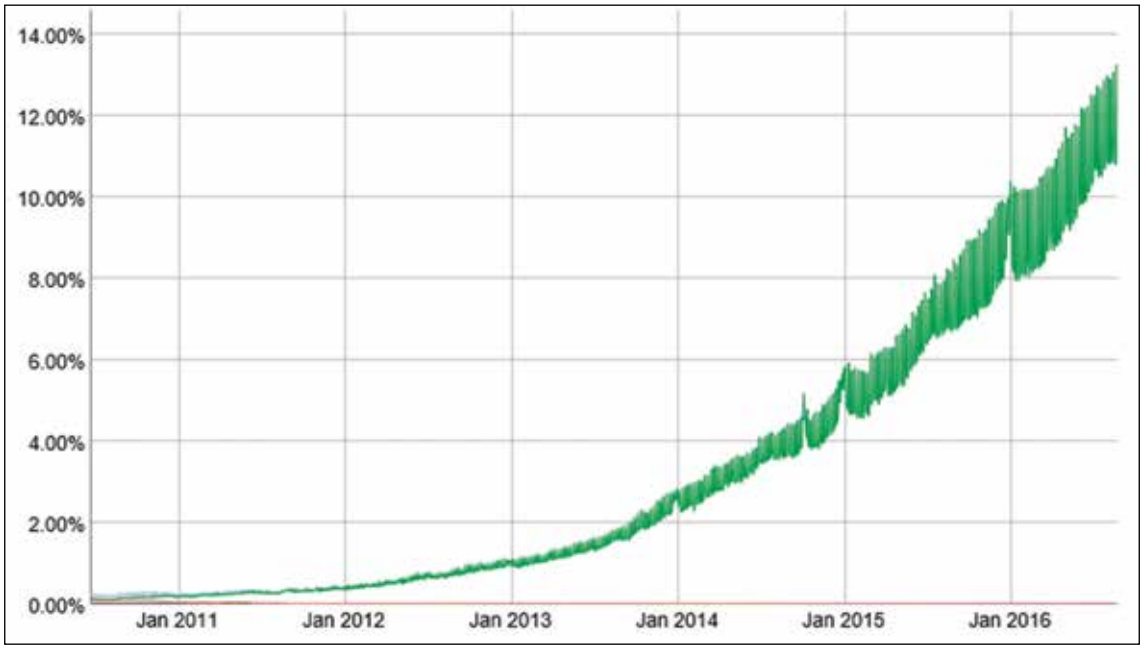

Figure 9 : Pourcentage des connexions aux serveurs de Google s'effectuant en IPv6 – Source : Google.

- un renforcement substantiel de la sécurité ;
- une couche adaptation, 6LowPAN, permettant la connectivité avec les réseaux IEEE 802.15.4 ;
- des couches applications légères (telles que CoAP) compatibles IPv6 ;
- des mécanismes d'autoconfiguration des adresses, basées sur le protocole SLAAC (Stateless Address Autoconfiguration) ou sur le DHCPv6, remplaçant le DHCP de l'IPv4 qui permet d'attribuer dynamiquement à un équipement une adresse IPv6 avec moins de risques cybersécuritaires.

Cependant, certains arguments allant à l'encontre de l'utilisation de l'IPv6 dans l'IoT ont été exposés. Certains constatent que l'IoT fait largement appel à des méthodes d'interrogation périodique ou "polling" dans lesquelles des capteurs sont scrutés de façon périodique par un serveur qui recueillent leurs données en mode "pull". Si la scrutation des devices se fait ainsi en adressage direct, leurs adresses se trouvent directement exposées à des attaques sur le réseau, notamment en déni de service, pouvant prendre une très grande ampleur du fait du grand nombre d'équipements concernés. Les équipements seraient ainsi mieux protégés derrière le NAT qui peut filtrer les trames entrantes en fonction des adresses (par un mécanisme de « port » gardé en mémoire). Mais cette sécurité est très illusoire car elle ne protège pas contre les attaques contenues dans les trames de données ni contre les attaques venues de l'intérieur du réseau en amont du NAT. La vérité est que, s'il y a lieu de protéger un grand réseau en le décomposant en cellules autonomes, comme c'est le cas du réseau des compteurs communicants Linky, il faut le faire en mettant en place au niveau de chaque cellule des mécanismes de sécurité bien plus élaborés que le simple NAT.

Beaucoup pensent donc que le développement de l'IoT est intimement lié à celui de l'IPv6. Cependant, force est de constater que ce développement se fait encore aujourd'hui majoritairement sur l'IPv4. Les équipements de réseaux ou d'extrémité supportant et utilisant l'IPv6 restent une minorité et il est patent que l'IPv6 ne s'est pas développé à la vitesse qui était escomptée, pour au moins deux raisons :

- il constitue une solution de continuité par rapport à l'IPv4 dans la mesure où les adresses IPv4 et IPv6 sont incompatibles entre elles ;
- des solutions palliatives (telles que l'ARP) ont permis de prolonger la durée de vie de l'IPv4.

Il semble cependant que l'on assiste en 2016 à un véritable décollage de l'IPv6. Google publie une statistique qui donne l'évolution de la proportion des requêtes faites sur ses serveurs en IPv6. La courbe de la figure 9 montre une croissance exponentielle des accès réalisés en IPv6 avec une moyenne mondiale de 13,1 % à fin août 2016, mais aussi avec des disparités fortes entre les pays (29,3 % aux Etats-Unis, 24,1 % en Allemagne, 11,5 % en France).

Dans le même temps, la pénurie d'adresse IPv4 commence à se faire sentir et certains fournisseurs d'accès à Internet sont amenés à dédoubler les adresses IP publiques en les différenciant par les numéros de port qu'elles sont autorisées à utiliser, ce qui constitue un pis-aller plus qu'une véritable solution.

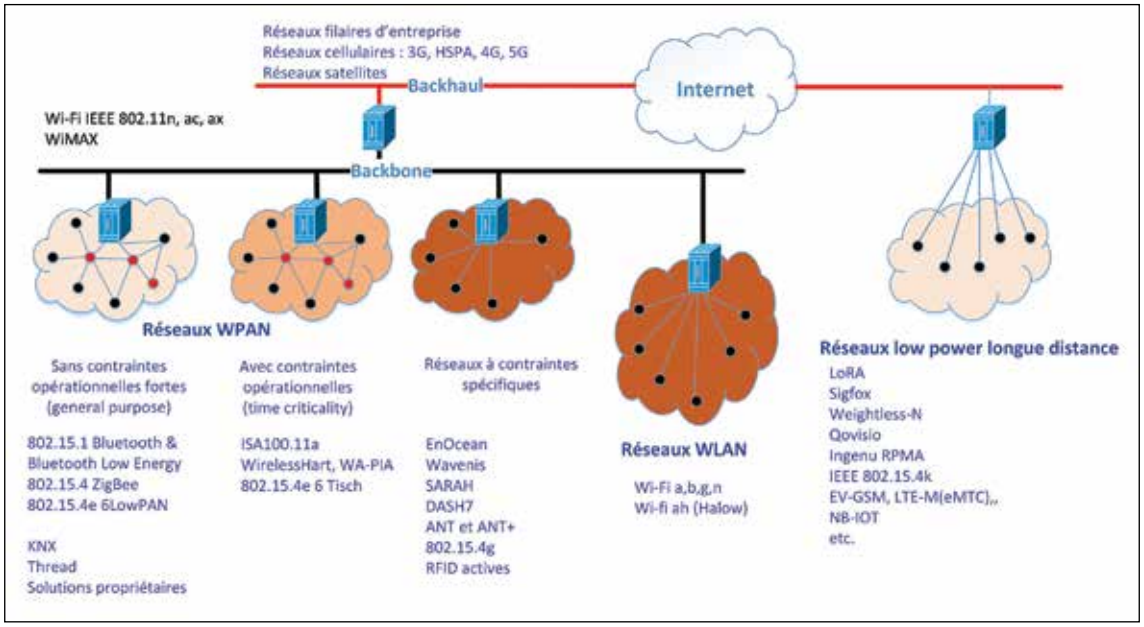

Figure 10 : Positionnement des différentes solutions de réseau sans-fil dans l'architecture générale de l'IoT.

Nous pensons donc que, même si l'IPv4 a encore de belles années devant lui, il n'est plus possible d'ignorer l'IPv6 et donc qu'il y a lieu aujourd'hui de déployer des solutions, et les équipements qui les supportent, fonctionnant à la fois en IPv4 et en IPv6.

L'interfaçage de l'IP avec les couches basses

Le problème posé

Nous avons vu en première partie que l'IoT s'installait sur des couches basses très diversifiées, beaucoup d'entre elles étant des solutions sans fil afin de bénéficier de la souplesse qu'offrent les radiocommunications. Nous rappelons dans la figure 10 les principales solutions actuellement en lice, classées selon la typologie que nous avons proposée.

Ces différentes solutions se différencient en premier lieu par leurs couches basses, couche physique et accès au réseau, qui imposent des structures de trames spécifiques. Si l'espace réservé aux données est d'une longueur suffisante, l'encapsulation de trames IP dans cet espace ne pose pas de problème majeur, à l'instar de ce que permettent le protocole Ethernet, qui supporte des trames de données allant de 64 à 1 518 octets, et le Wi-Fi (IEEE 802.11), conçu comme un Internet sans fil supportant des "payloads" de données allant jusqu'à 2 312 octets. Tel est aussi le cas du Bluetooth Classic qui supporte des trames TCP/IP via une couche d'adaptation, dénommée BNEP (Bluetooth Network Encapsulation Protocol), admettant aussi bien des trames IPv4 qu'IPv6, dans la limite de 1 500 octets.

Le problème est plus complexe avec les protocoles qui ont été développés en prenant en compte les contraintes de l'IoT : très faible consommation d'énergie, compatibilité avec des équipements dotés de faibles ressources et n'ayant à transmettre que des données brèves. Ces protocoles se caractérisent tous par des trames courtes, avec des entêtes courtes mais aussi des espaces réservés aux données fortement réduits. Tel est le cas du protocole Bluetooth Low Energy (Bluetooth V4.0 et suivants), dérivé du protocole Bluetooth afin de desservir les objets connectés mais qui ne permet de transmettre dans chaque trame que des paquets de données de 31 octets maximum, éventuellement doublés.

L'installation sur de telles couches basses de trames IP est plus problématique. Elle est facilitée par le recours à la couche transport UDP (de 8 octets), de préférence à TCP (≥ 20 octets), mais ceci ne suffit pas à résoudre le problème. Celui-ci a été réglé dans le cas du protocole de réseau local IEEE 802.15.4 servant de base à différents réseaux tels que ZigBee et Thread (pour la domotique et le comptage) ainsi qu'à l'ISA100.11a et au WirelessHart (pour les applications industrielles). La solution repose sur le développement d'une couche adaptation, le 6LowPAN (IPv6 Low power Wireless Personal Area Networks), publiée à partir de 2007 par l'IETF (Internet Engineering Task Force). Ses mécanismes sont transposables à d'autres réseaux, tels que le Bluetooth Low Energy et les liaisons CPL. Ses principes en sont résumés ci-après. Le développement de 6LowPAN est illustratif de la volonté discutée précédemment de rendre le protocole Internet applicable aux plus petits dispositifs dans le cadre de l'IoT.

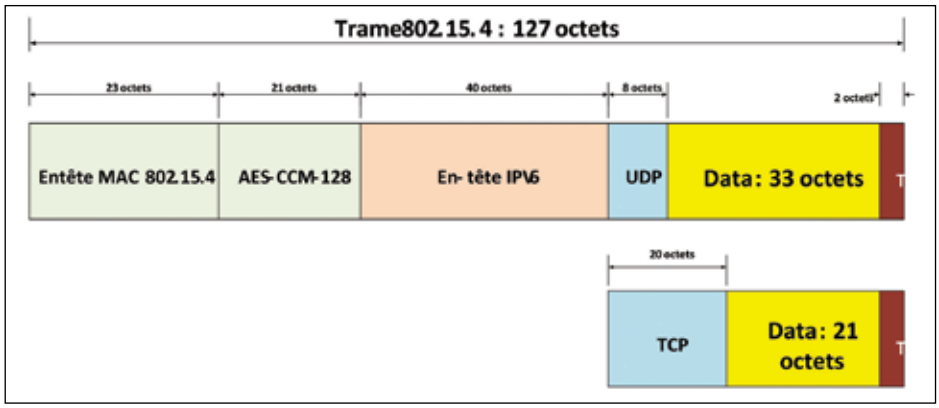

Figure 11 : Le problème de la compression des entêtes IPv6 à l'entrée des réseaux 802.15.4.

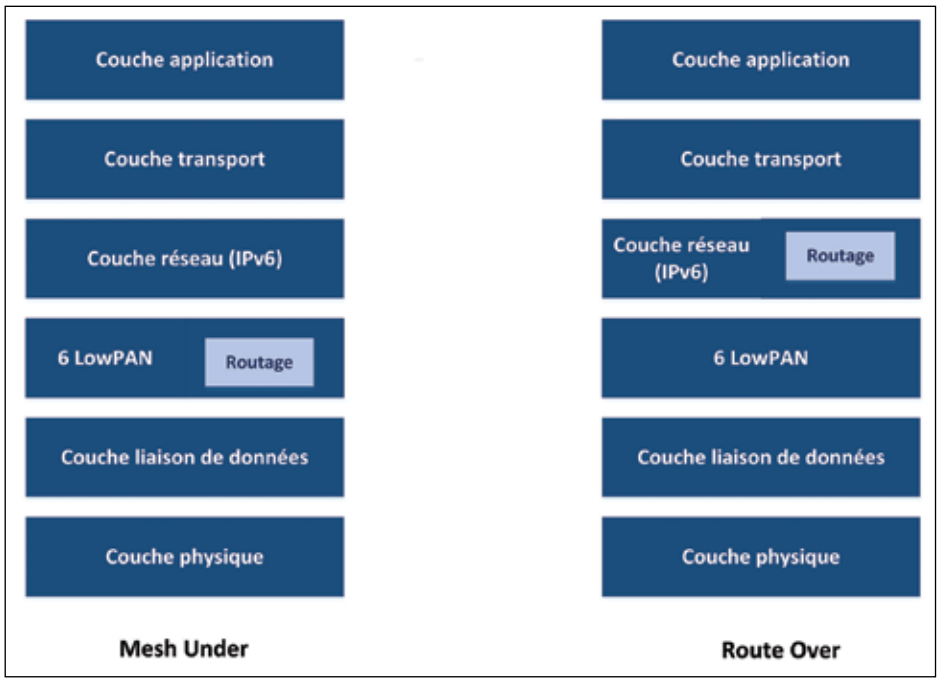

Figure 12 : Pile IPv6 6LowPAN selon le mode de routage.

Le protocole 6LowPAN

6LowPAN (pour IPv6 Low Power Wireless Personal Area Networks) est une couche "adaptation" permettant d'assurer la connectivité entre l'IPv6 et les réseaux IEEE 802.15.4 qui ne supportent pas les trames Internet. De nombreux problèmes sont à régler pour faire coexister les deux mondes en garantissant les performances et la sécurité du réseau local. En particulier le routage doit être assuré à l'intérieur de chaque réseau et entre le réseau local et l'Internet IPv6

Un premier problème est celui de la compression des entêtes, de 40 octets en IPv6 auxquelles s'ajoutent les entêtes TCP ou UDP. Les encapsuler en l'état dans les trames 802.15.4 de 127 octets ramènerait l'espace réservé aux données à 21 ou 33 octets, avec une efficacité du protocole chutant à 16,5 % ou 25 % (figure 11).

6LowPAN ramène les entêtes de l'IPv6 de 40 à 2 ou 7 octets.

Un autre problème est celui de la fragmentation. Les réseaux 802.15.4 sont évidemment incapables d'acheminer les trames IPv6 dont la longueur peut atteindre 1 280 octets. 6Low PAN fixe des règles de fragmentation qui permettent de décomposer la trame IP en datagrammes successifs. Mécanismes de compression et de fragmentation permettent de maintenir l'efficacité du protocole 802.15.4 au-dessus de 50 %.

Mais d'autres problèmes doivent être traités : modalités de routage, auto-configuration (car les mécanismes de "Neighbor Discovery" sont trop lourds pour le 802.15.4), compatibilité avec les applications hautes (en particulier avec CoAP), supervision de réseau.

Le routage donne lieu à un débat intéressant : faut-il router des fragments et ne reconstituer la trame qu'en extrémité

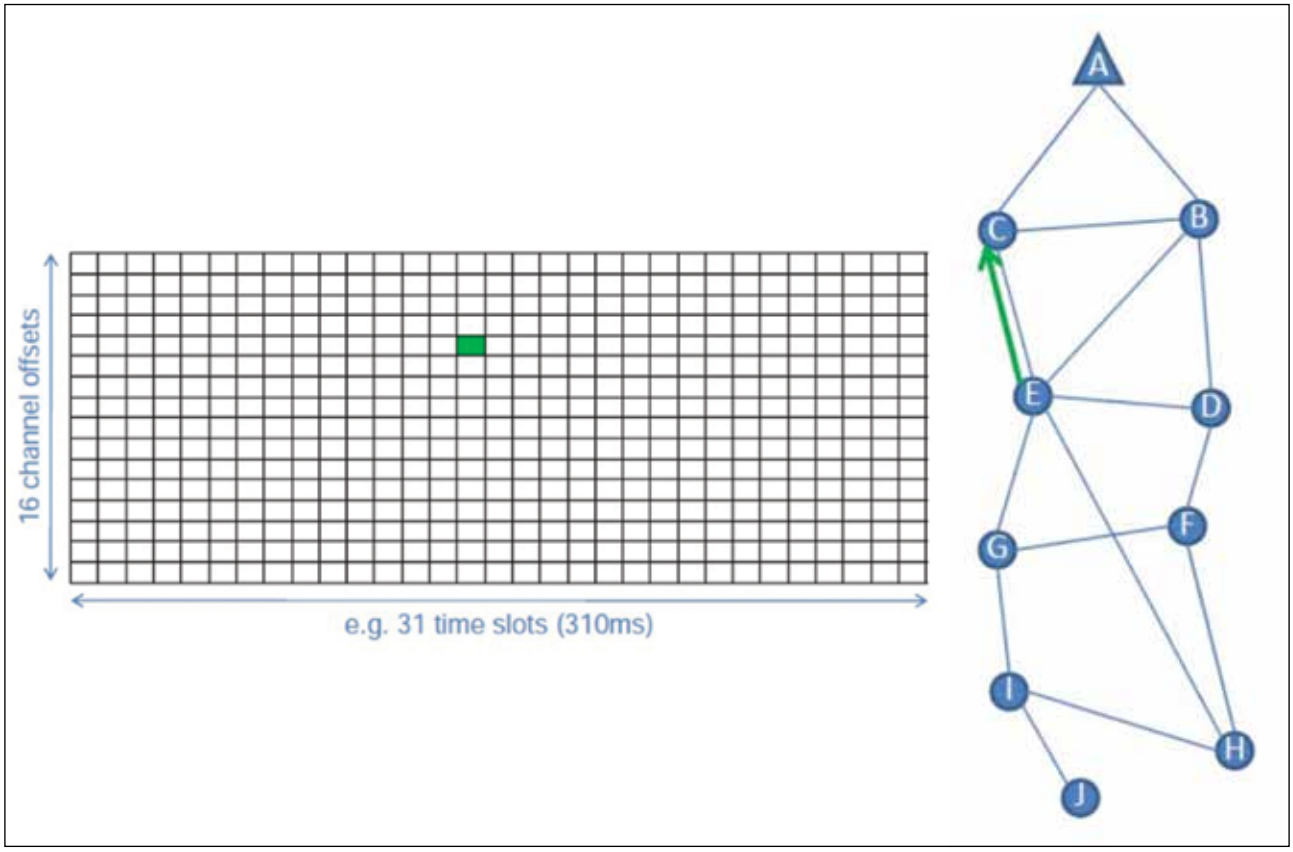

Figure 13 : 802.15.e – Un slot de 10 ms pour chaque élément de communication point à point.

(c'est le "mesh under") ou bien faut-il router des trames reconstituées à chaque nœud (c'est le "route over") ? L'une et l'autre des solutions ont des avantages et des inconvénients et le 6LowPAN permet les deux modes. Selon le mode choisi, on parvient à l'une ou l'autre des piles de la figure 12.

Les exigences industrielles – Le TSCH (Timeslotted Channel Hopping) et la pile IIoT

La plupart des réseaux 802.15.4, tels que ZigBee et le Thread, sont des réseaux fonctionnant en "best effort". Ils implémentent au niveau de la couche liaison de données un mécanisme d'écoute du réseau, le CCA (Clear Channel Assessment) et peuvent utiliser au niveau de la sous-couche MAC d'accès au réseau le mécanisme d'évitement de collision CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance) utilisée par le Wi-Fi (IEEE 802.11).

Ces solutions sont suffisantes pour beaucoup d'applications relevant de l'IoT notamment la collecte d'informations non critiques en provenance de capteurs pour le comptage ou la télésurveillance. Elles sont insuffisantes dans le domaine de l'automation, c'est-à-dire celui de **l'IIoT (Industrial Internet of Things)** lorsqu'on se propose de piloter un procédé industriel présentant des contraintes particulières telles que :

- synchronisation et déterminisme ;
- haute fiabilité et robustesse face aux interférences ;
- faible latence ;
- faible consommation.

Pour répondre à ces besoins, l'ISA (International Society of Automation) a développé à partir de 2005 le protocole ISA 100.11a (normalisé IEC 62734) dont un précurseur est le WirelessHart. L'ISA 100.11a est fondé sur l'allocation déterministe de slots temporels et fréquentiels à chaque élément de trafic, avec saut de fréquence entre chaque slot. Ces principes sont repris depuis 2012 dans le standard 802.15.4 sous forme d'un amendement : le 802.15.4e qui a introduit le TSCH (Time Slotted Channel Hopping). Dans ce mode, des frames de longueur variable, composées de slots de 10 ms positionnés dans un canal donné, assurent les communications. Chaque slot est programmé de façon déterministe dans le temps et dans l'espace des fréquences (figure 13).

Sur la base de ce principe, le trafic est organisé par multiplexage temporel (TDMA : Time Division Multiple Access), sans collision, de façon à satisfaire l'ensemble des besoins (figure 14).

Il reste à standardiser la façon dont le TSCH sera opéré c'est-à-dire comment l'ordonnancement est organisé en statique et/ou en dynamique, pour répondre aux besoins du trafic, compte-tenu de la bande passante disponible. C'est

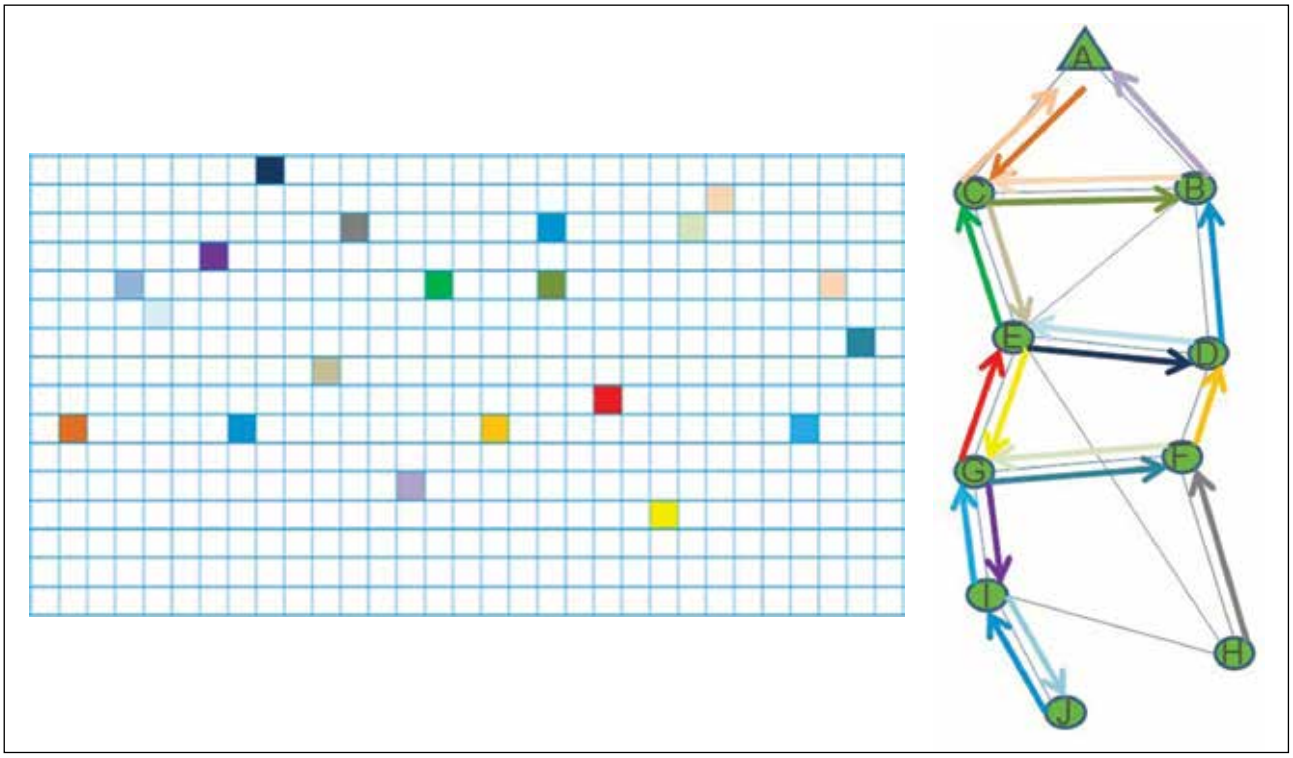

Figure 14 : Multiplexage du trafic et saut de fréquence dans le 802.15.4e TSCH.

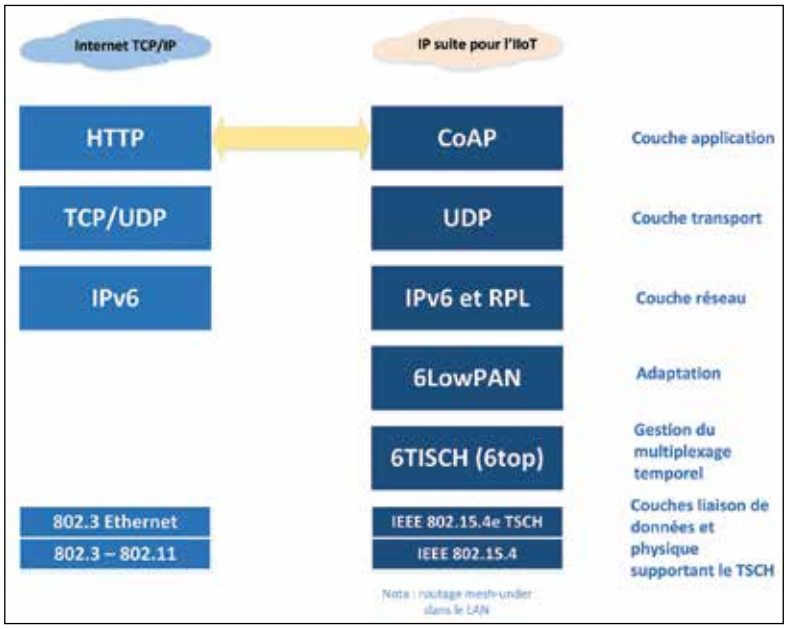

Figure 15 : Suite de protocoles pour l'IIoT comparée à la suite TCP/IP classique.

l'objet du groupe de travail 6TISCH de l'IETF qui, en liaison avec le groupe 6TiSCH Interest Group (IG 6T) de l'IEEE devrait produire les spécifications d'une couche "6TOP" venant se positionner au-dessus du 802.15.4e.

Pour être complet, il faudrait également parler de la définition des protocoles de routage adaptés au cas des réseaux locaux. Le groupe de travail ROLL (Routing Over Low power and Lossy networks) de l'IETF a standardisé le protocole RPL (Routing Protocol for Low power and Lossy Networks) qui est un protocole "route over" permettant de construire de façon économe en ressources, des graphes d'acheminement du trafic vers le routeur de bordure.

Une fois achevée cette construction, les réseaux locaux construits sur IEEE 802.15.4 utilisés dans le domaine industriel, y compris dans celui du comptage avancé ou AMI (Advanced Metering Infrastructure) se comporteront comme

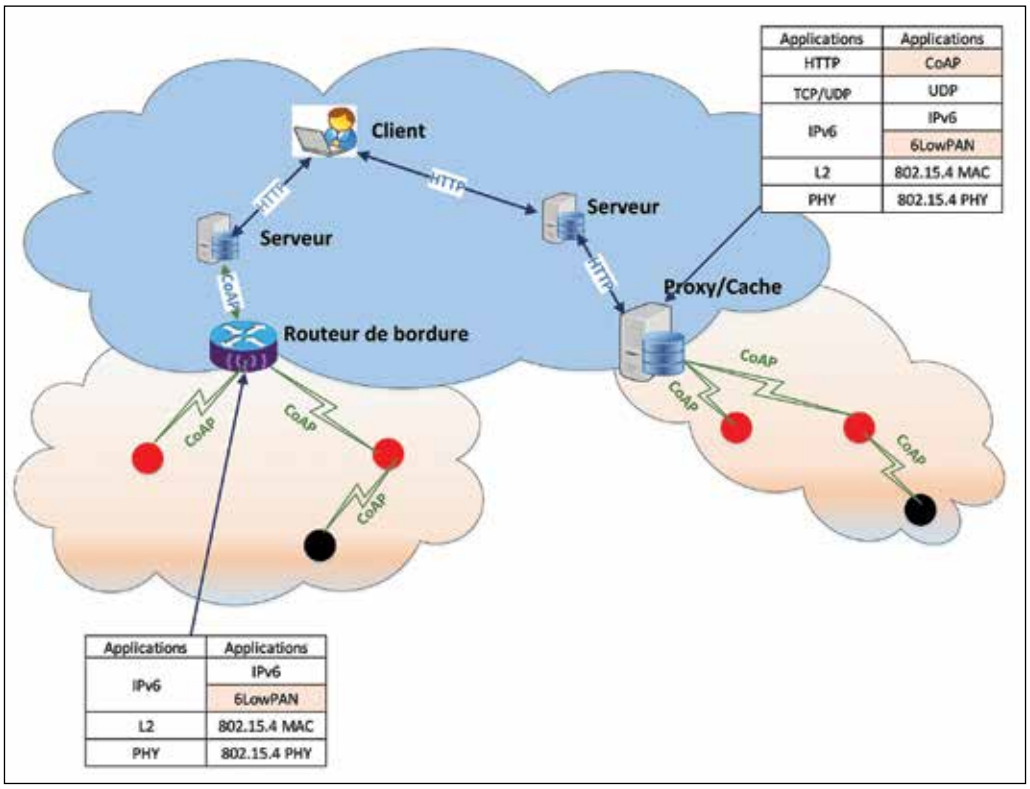

Figure 16 : Architecture REST de l'IoT fondée sur l'association de CoAP à HTTP.

des Internet IPv6 miniatures, avec des performances garanties et avec la possibilité de communiquer avec l'IPv6 selon la pile résumée par la figure 15.

Il reste cependant à s'assurer que le dialogue ne se limite pas à la communication et que les couches application peuvent supporter des services communs. C'est ce que nous allons examiner à présent.

L'interfaçage avec les couches supérieures – Les couches application de l'IoT

Les limites de HTTP

HTTP (Hypertext Transfer Protocol) est le protocole client/serveur à la base du Web. C'est lui qui fixe les règles pour qu'un client puisse solliciter et obtenir des données de la part d'un correspondant désigné comme serveur. Il est aujourd'hui sécurisé par la mise en œuvre des mécanismes TLS (Transport Layer Security) au niveau de la couche transport ce qui a donné naissance à l'HTTPS. Cependant ce protocole est inadapté pour des équipements dotés de faibles ressources car il génère des "frais généraux" importants. Par ailleurs, il est inapproprié pour les communications à dynamique rapide (100 ms et moins).

CoAP (Constrained Application Protocol)

Dans ce contexte, il est apparu nécessaire de développer une version allégée d'HTTP, adaptée aux équipements à faibles ressources. Le CoAP (Constrained Application Protocol) a été mis au point au sein de l'IETF et publié en 2014. C'est un protocole "Canada dry" de HTTP, client/serveur comme lui, mais destiné à fonctionner essentiellement sur UDP (bien que son installation sur TCP soit possible), avec des frais généraux réduits et un bloc de données limité à 1 024 octets. Il utilise les spécifications originelles d'HTTP, notamment l'URI (Uniform Resource Identifier) comme identifiant des ressources et des verbes (méthodes) et des codes de réponse issus d'HTTP.

Le passage d'HTTP en CoAP (et vice versa) se fait de façon simple au niveau d'un proxy situé en bordure du réseau local qui garde en cache toutes les informations locales nécessaires à la traduction. Il est ainsi possible de bâtir, en associant CoAP à HTTP, des architectures satisfaisant aux critères REST (Representational State Transfer) caractéristiques du Web et bien adaptées aux systèmes distribués (figure 16).

CoAP apparaît comme une bonne solution pour des applications IoT dans les domaines de la domotique et du comptage intelligent. Comme HTTP, il peut être considéré comme un protocole généraliste. Dans certains cas, le recours à des protocoles plus spécifiques apparaît justifié.

OPC UA : le protocole d'Industrie 4.0

Dans l'industrie, le recours aux protocoles TCP/IP basés sur Ethernet s'est fortement développé compte tenu des

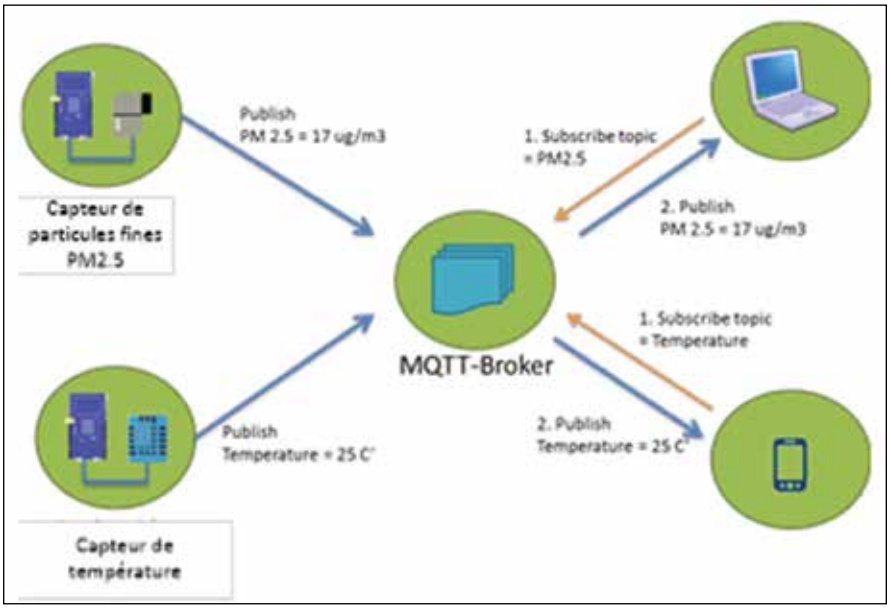

Figure 17 : Schéma de fonctionnement du MQTT.

progrès accomplis en matière de performances. On a vu ainsi apparaître les protocoles plus ou moins propriétaires EtherCAT, Powerlink, Ethernet/IP, Profinet, SERCOS III, etc. Cependant l'industrie utilise peu HTTP bien que les serveurs Web embarqués se soient développés au cours dernières années, pour les applications de maintenance notamment. L'industrie reste attachée aux solutions « métier » prenant en compte ses besoins propres. C'est ainsi que le protocole client/serveur MODBUS/TCP est largement employé, dans le domaine du manufacturier notamment.

Cependant, dans le cadre du concept allemand d'IIoT, Industrie 4.0, le protocole OPC UA (Open Platform Communications Unified Architecture) connait un succès grandissant. Il est le lointain successeur du protocole OPC, aujourd'hui quasiment abandonné du fait de failles de sécurité importantes. C'est un protocole client/serveur de couche application avec architecture orientée objet visant à permettre l'interopérabilité entre vendeurs de composants d'automatisme grâce à une traduction sémantique des protocoles industriels existants.

Il assure les communications entre capteurs, contrôleurs, postes de supervision, etc. à l'intérieur des systèmes d'automatisme, des scadas et des MES (Manufacturing Execution Systems). Il convient aux échanges d'information assez lourds mais reste mal adapté à des échanges brefs entre équipements légers.

MQTT (Message Queuing Telemetry Transport).

Ceci nous amène au protocole MQTT (Message Queuing Telemetry Transport). Ce protocole part de la constatation que le polling d'un nombre de plus en plus grand d'équipements connectés conduit à un gaspillage de bande passante en véhiculant des informations sans intérêt. C'est un protocole de type Pub/Sub (Publish/Subscribe) dans lequel les données émises par les équipements de terrain sont transférées vers un serveur MQTT (un « broker »), qui les trie, les stocke et les publie en les mettant à la disposition de clients intéressés (figure 17). Ces clients peuvent être des systèmes scadas ou n'importe quelle autre entité intéressée par certaines données publiées par le broker. Les clients s'abonnent auprès du broker à un service en sélectionnant les types de données qui les intéressent.

Ce découplage entre producteurs des données et consommateurs permet une gestion beaucoup plus efficace du trafic de données et offre davantage de simplicité pour les extensions éventuelles du système. Les informations sont transmises au broker par exception et, à la différence des protocoles de polling systématique, seules les données ayant évolué sont transmises. L'entête des trames MQTT est très courte (deux octets) et n'induit pas de frais généraux excessifs. Basé sur TCP, il fonctionne en mode connecté et lorsqu'un équipement perd la connexion, les clients concernés reçoivent automatiquement de la part du broker le « testament » de l'équipement perdu.

Plusieurs détails du protocole le rendent particulièrement attractif pour les applications de télémétrie ou de contrôle distant de type scada mais il peut être mis en œuvre dans toute application MtoM. Il confère un avantage particulier aux réseaux locaux qui supportent TCP/IP.

Autres protocoles

D'autres protocoles de couche application apparaissent comme susceptibles de répondre à certains besoins particuliers des applications IoT :

- **DDS (Data Distribution Service (DDS)**, protocole Pub/Sub décentralisé (pas de broker) développé par l'OMG (Object Management Group) pour les communications soumises à de fortes contraintes de performances et de fiabilité (aéronautique, défense, télécommunications) ;
- **XMPP (Extensible Messaging and Presence Protocol, originellement Jabber)** : ce protocole client-serveur de messagerie instantanée destinée à permettre des échanges au format XML, est utilisé par les entreprises et administrations dans le cadre d'échanges de données entre applications, mais aussi dans le cadre du grid computing, des notifications d'alertes ou d'informations, de la supervision système et réseau ou du cloud computing ;
- **AMQP (Advanced Message Queuing Protocol**, protocole Pub/Sub destiné à assurer des transactions entre serveurs fiabilisées (à la différence de MQTT et de DDS), utilisé surtout dans le domaine bancaire, mais pouvant être appliqué dans l'industrie pour des applications critiques.

La cybersécurité

La cybersécurité de l'Internet des objets est une question absolument centrale et l'IoT ne pourra pas se développer si une réponse appropriée ne lui est pas apportée. L'IoT offre une surface d'attaque considérable (par exemple plus de 30 millions d'abonnés pour le réseau de distribution électrique français), des frontières évolutives, mal connues et difficiles à défendre, des équipements très diversifiés sujets à toutes sortes de menaces. L'attaque en déni de service du 25 septembre 2016 menée contre les serveurs d'OVH à partir de 145 607 caméras de surveillance mal protégées, illustre l'ampleur de la menace.

Dans l'IoT, la cybersécurité doit se construire par quatre canaux au minimum :

- appliquer des règles générales de prévention des cyberattaques, comme dans tout système d'information (c'est l'approche "policies and procedures") ;
- identifier et isoler les zones de sécurité selon les normes en vigueur (IEC 62443 notamment) ;
- sécuriser les protocoles ;
- recourir à des composants offrant à l'état natif, en capacité, un niveau de sécurité approprié. On voit ainsi se développer aujourd'hui des modules de sécurité inviolables et indissociables des équipements à protéger, mais qu'il faut mettre en œuvre selon des procédures adaptées.

La question de la cybersécurité ne peut donc se traiter en quelques phrases. Nous ne donnerons ici qu'un aperçu concernant la sécurité des protocoles dont beaucoup sont nés à une époque où les préoccupations de cybersécurité n'étaient pas aussi sensibles. Beaucoup de protocoles bâtis au-dessus de TCP/IP présentent des vulnérabilités notoires (HTTP, SNMP V1&V2, FTP, DNS, POP3, SMTP, etc.). Le recours à IP multiplie en outre les entrées possibles dans les systèmes et élargit considérablement la surface d'attaque.

Il faut donc revoir chaque protocole et, chaque fois que cela est possible, adopter une version sécurisée :

- HTTP → HTTPS
- DNS → DNSec
- CoAP + DTLS
- OPC Classic → OPC UA
- Modbus → Modbus Secure
- EtherNET/IP → EtherNET/IP Secure
- IPsec, SSL/TLS, L2TP et autres protocoles de VPN

Conclusion

La question des protocoles peut paraître aride pour le non initié. Elle est cependant centrale dans la question de l'IoT. L'adoption de protocoles adaptés aux objectifs recherchés est essentielle pour parvenir au résultat visé.

D'une façon générale, c'est le souci de sobriété et d'adaptation à des équipements à ressources limitées qui a guidé l'évolution des protocoles et l'adoption de variantes aux protocoles usuels du monde l'internet. Dans le cas de l'IIoT, des dispositions particulières doivent être mises en œuvre pour remédier aux exigences du monde industriel. Nul doute que le monde de la mobilité, non traité dans cette note, apportera lui aussi des exigences spécifiques.

Les organismes de normalisation travaillent activement sur tous ces sujets, avec parfois une concurrence entre eux. Les plus actifs sont l'IETF, l'IEEE et l'ISA. Les Américains, les Chinois, les Japonais sont très présents dans ces organismes. L'Europe et la France en particulier le sont moins et la tentation de développer des solutions nationales reste forte. Pourtant, la présence dans ces instances est le moyen d'apprécier les tendances technologiques du moment et de faire, le cas échant, prévaloir ses propres points de vue. ■

Jean-Pierre Hauet *est ingénieur au corps des Mines. Il est associate partner de KB Intelligence. Au cours de sa carrière, il a dirigé les Laboratoires de Marcoussis du groupe Alcatel-Alsthom, il a dirigé la branche Produits et Techniques de Cegelec et a été Chief Technology Officer du Groupe ALSTOM. Il est membre émérite de la SEE et rédacteur en chef de la REE.*