# Protocoles pour l'Internet des objets

Que signifie la phrase internet des objets (Internet of Things) ? Cela dépend beaucoup de votre position dans la chaîne d'approvisionnement. Beaucoup ont essayé de la définir, et les définitions sont souvent influencées par les besoins et intérêts des différents secteurs économiques. Mais en tant qu'ingénieur matériel ou logiciel, vous comprenez déjà l'élément essentiel : construire des produits qui sont interconnectés. Et les systèmes intégrés vont jouer - et jouent - un rôle crucial dans le développement de l'IoT. Dans cet article, nous allons nous intéresser à internet et ses protocoles existants et nouveaux à l'appui des efforts de l'IoT. Avant de nous pencher sur ces protocoles, nous allons définir ce qu'est un objet parce que les tâches des appareils utilisateurs dicteront la plupart des exigences à utiliser par les protocoles.

# L'IoT industriel par rapport à l'IoT grand-public

Les exigences en matière de logiciels pour les appareils IoT industriels et grand-public peuvent être un peu différentes. Bien qu'ils puissent partager un noyau commun et des services de bas niveau, le middleware requis par leurs applications peut être radicalement différent.

Dans le cas de l'IoT industriel, un nœud de WSN représente une pile de logiciel pour un appareil IoT industriel, par exemple un nœud de capteurs sans fil (WSN). L'appareil de faible puissance, de coût faible, peut fonctionner entièrement sur batterie. Un tel appareil peut généralement utiliser un

processeur 32 bits. Il peut également utiliser un processeur 8 ou 16 bits, mais avec des piles de communications fonctionnant sur un module additionnel. Il utiliserait un protocole de réseau très efficace comme 6LoWPAN pour réduire le temps de transmission et économiser l'énergie. Il pourrait également communiquer sur de courtes distances sans fil via Bluetooth. En tant que nœud de périphérie, nous avons besoin de transférer les données à partir du réseau sans fil vers un réseau IP (Internet local ou public) et en utilisant une faible puissance Wifi ou Ethernet.

De toute évidence, les exigences en matière de logiciels pour cet appareil sont beaucoup plus importantes. Il pourrait avoir besoin d'une machine virtuelle Java. Il pourrait aussi bien utiliser un protocole de marché vertical. Malheureusement, l'IoT grand-public est très fragmenté en termes de protocoles de marché verticaux (de protocole d'application). Beaucoup d'entreprises proposent des solutions propriétaires. Dans le cas du marché domestique du consommateur, par exemple :

- Apple possède le protocole MFI (Made For iDevices)
- Google (Nest) a annoncé Thread
- Samsung, Intel, Dell, Atmel et Broadcom ont uni leurs forces pour lancer le Consortium Open Interconnect (OCI, Open Interconnect Consortium)
- L'Alliance AllSeen (précédemment AllJoyn) a proposé une norme depuis des années. Les premiers membres en sont Haier, LG, Microsoft, Panasonic, Qualcomm, Sharp, Silicon Image, Technicolor et TP-Link.

Il y a d'autres exemples comme la communication par courant porteur de ligne électrique : HomePlug et HomeGrid.

Sur le marché vertical médical, des organisations comme l'Alliance Continua, IHE (Integrating the Healthcare Enterprise) ou IEEE sont également en train d'élaborer et de proposer des normes.

Ces protocoles ne sont pas proposés par Micrium. Un fabricant d'équipement nécessitant que ses produits soient compatibles avec l'un de ces protocoles IoT grand-public doit s'inscrire auprès de ces organisations et ensuite intégrer ces protocoles dans le cadre de l'application de son produit.

Dans l'IoT industriel, il y a moins d'initiatives axées sur le marché. Il existe une initiative majeure appelée Consortium Internet Industriel (IIC, Industrial Internet Consortium) avec AT&T, Cisco, GE, Intel et IBM en tant que membres fondateurs. Mais, en dehors de l'IIC, le développement d'appareils et de systèmes pour l'internet des objets est essentiellement propriétaire. Voilà pourquoi la connaissance d'internet et du protocole internet (IP) est si importante désormais pour les développeurs de systèmes intégrés. Protocole internet (IP, Internet Protocol)

L'utilisation de la technologie IP est fondamentale pour l'IoT. IP permet l'interopérabilité des systèmes. Cette fonction peut ne pas sembler importante aujourd'hui, mais comme l'IoT évolue, l'interopérabilité des systèmes deviendra une fonctionnalité importante générant des revenus. Ethernet/Wifi et 6LoWPAN dépendent tous deux fortement d'IPv4 et d'IPv6.

# Protocoles IP utilisés par l'IoT

Il est certainement possible de construire un système IoT avec les technologies web existantes, même si elles ne sont pas aussi efficaces que les nouveaux protocoles. HTTP(S) et Websockets sont des normes couramment utilisées pour la charge utile, de même que XML ou JavaScript Object Notation (JSON). En utilisant un navigateur web standard (client HTTP), JSON fournit une couche d'abstraction aux développeurs web pour créer une application web comportant un état avec une connexion duplex persistante à un serveur web (serveur HTTP) en maintenant ouvertes deux connexions HTTP.

## HTTP

HTTP est le fondement du modèle client-serveur utilisé pour le web. La méthode la plus sûre pour mettre en œuvre HTTP dans votre appareil IoT est de n'inclure qu'un client, pas un serveur. En d'autres termes, il est plus sûr que l'appareil IoT puisse initier des connexions vers un serveur Web, mais ne soit pas en mesure de recevoir de demandes de connexion. Après tout, nous ne voulons pas permettre aux machines de l'extérieur d'avoir accès au réseau local où les appareils IoT sont installés.

### WebSocket

WebSocket est un protocole qui permet une communication full-duplex sur une seule connexion TCP sur laquelle les messages peuvent être envoyés entre le client et le serveur. Il fait partie de la

spécification HTML5. La norme WebSocket simplifie beaucoup la complexité entourant la communication bi-directionnelle et la gestion des connexions web. L'utilisation de Websockets en conjonction avec HTTP est une bonne solution pour les appareils IoT s'ils peuvent supporter les charges utiles HTTP.

#### XMPP

XMPP (Extensible Messaging and Presence Protocol) est un bon exemple de technologie web existante qui trouve un nouvel emploi dans l'espace IoT.

XMPP prend ses racines dans les informations de messagerie instantanée et de présence, et s'est étendu aux appels vocaux et vidéo, à la collaboration, au middleware léger, à la syndication de contenu, et au routage généralisé de données XML. C'est un concurrent pour la gestion à grande échelle des produits blancs de consommation tels que les lave-linge, les sèche-linge, les réfrigérateurs, et ainsi de suite.

Les atouts de XMPP sont son adressage, sa sécurité et évolutivité. Cela le rend idéal pour les applications IoT grand-public.

HTTP, Websocket et XMPP ne sont que des exemples de technologies sollicitées en tant que services pour l'IoT. D'autres groupes travaillent également avec acharnement pour développer des solutions pour les nouveaux défis auxquels nous confronte l'IoT.

## Protocoles dédiés à l'IoT

De nombreux experts se réfèrent aux appareils IoT en tant que systèmes contraints parce qu'ils pensent que les appareils IoT devraient être aussi bon marché que possible et utiliser les plus petits MCU disponibles, tout en exécutant une pile de communication.

Actuellement, l'adaptation de l'Internet à l'IoT est l'une des principales priorités de la plupart des organismes internationaux de normalisation.

Si votre système n'a as besoin des caractéristiques de TCP, et peut fonctionner avec les capacités plus limitées d'UDP, supprimer totalement le module PCM contribue largement à réduire l'impact total de votre produit sur le code. C'est pourquoi 6LoWPAN (pour le WSN) et CoAP (protocole internet léger) contribuent à l'univers IoT. CoAP

Bien que l'infrastructure du web soit disponible et utilisable par les appareils IoT, elle est trop lourde pour la majorité des applications de l'IoT. En juillet 2013, l'IETF a publié le Protocole d'application contrainte (CoAP, Constrained Application Protocol) pour utilisation avec une faible puissance et des nœuds et réseaux à pertes (limitées) (LLNs). CoAP, comme HTTP, est un protocole REST.

CoAP est sémantiquement aligné sur HTTP, et comporte même une correspondance un-un vis-à-vis de l'émission et réception HTTP. Les périphériques réseau sont limitées par de petits microcontrôleurs avec de petites quantités de mémoire flash et de RAM, tandis que les contraintes sur les réseaux locaux, tels que 6LoWPAN sont dues à des taux d'erreurs de paquets élevés et à un débit faible (de dizaines de kilobits par seconde). CoAP peut être un bon protocole pour les appareils fonctionnant sur batterie ou sur captage d'énergie.

### Caractéristiques de CoAP : CoAP utilise UDP

Dans la mesure où CoAP utilise UDP, quelques-unes des fonctionnalités de TCP sont répliquées directement dans CoAP. Par exemple, CoAP opère une distinction entre les messages confirmables (nécessitant un accusé de réception) et non confirmables.

- Les demandes et les réponses sont échangées de manière asynchrone sur les messages CoAP (contrairement à HTTP, où une connexion TCP existante est utilisée).
- Tous les en-têtes, les méthodes et les codes d'état sont codés binaire, ce qui réduit le surcoût en débit du protocole. Cependant, cela nécessite l'utilisation d'un analyseur de protocole pour résoudre les problèmes de réseau.
- Contrairement à HTTP, la capacité de mettre en cache les réponses CoAP ne dépend pas de la méthode de la demande, mais du code de la réponse.
- CoAP répond pleinement aux besoins d'un protocole extrêmement léger et avec la nature d'une connexion permanente. Il présente une similarité sémantique avec HTTP et constitue un protocole REST (ressources, identificateurs de ressources et manipulation de ces ressources par l'intermédiaire d'interface de programmation d'application uniforme (API)). Si vous provenez de l'univers du web, utiliser CoAP est relativement facile.

#### MQTT

MQ Telemetry Transport (MQTT) est un protocole open source qui a été développé et optimisé pour les appareils limités et à faible bande passante, à latence élevée, ou pour les réseaux non fiables. Il s'agit d'un transport de messages de publication/d'abonnement qui est extrêmement léger et idéal pour le raccordement à des réseaux de petits appareils avec une bande passante minimale. MQTT utilise efficacement la bande passante, accueille toutes les données, et est en permanence informé de l'état de la session, car il utilise le protocole TCP. Il est destiné à minimiser les besoins en ressources de l'appareil tout en essayant d'assurer une fiabilité et un certain degré d'assurance de livraison avec des niveaux de service.

MQTT cible de grands réseaux de petits appareils qui doivent être surveillés ou contrôlés à partir d'un serveur back-end sur Internet. Il n'a pas été conçu pour le transfert d'appareil à appareil. Il n'a pas non plus été conçu pour « diffuser de manière multiple » des données vers de nombreux récepteurs. MQTT est simple, offrant seulement quelques options de contrôle. Les applications utilisant MQTT sont généralement lentes dans le sens que la définition du « temps réel » dans ce cas est généralement mesurée en secondes.

### Comparaison des protocoles IoT potentiels

- Cisco est au cœur de l'Internet ; leur équipement IP est partout. Cisco participe désormais activement à l'évolution de l'IoT. Il voit le potentiel de connecter des objets physiques et d'obtenir des données de notre environnement et de traiter ces données pour améliorer notre niveau de vie.
- Ces protocoles IoT spécifiques à internet ont été développés pour répondre aux exigences des appareils disposant de petites quantités de mémoire, et à celles des réseaux à faible bande

passante et latence élevée.

- HTTP peut être un protocole gourmand pour un appareil IoT. Il comporte de grands messages, car ils sont envoyés dans un format lisible par l'homme. Pour les appareils IoT, la taille de la charge utile est souvent une contrainte. Pour une grande famille d'appareils, rapporter et accepter des commandes peut être fait de manière plus efficace avec un protocole beaucoup plus léger. MQTT a été proposé comme réponse à ces problèmes. MQTT n'est pas une norme de l'IETF, et est dirigé par IBM et la fondation Eclipse.

## Conclusion

- Dans le terme « Internet des objets » il y a internet. Certains peuvent proposer des appareils inventés en tant qu'appareils IoT sans utilisation du protocole internet. Nous devrions nous y attendre. Aujourd'hui, l'IoT est devenu est un terme tellement fort (certains pourraient dire issu du battage médiatique) que chaque fabricant veut profiter de l'énorme couverture médiatique de l'IoT.
- Le protocole Internet (IP) est un transporteur ; il peut encapsuler des protocoles aussi nombreux pour l'IoT qu'il le fait aujourd'hui pour le web. Un grand nombre d'experts de l'industrie réclament une standardisation des protocoles. Mais s'il y a un si grand nombre de protocoles pour le web, pourquoi n'y en aurait-il pas tout autant pour l'IoT ? Vous choisissez les protocoles qui répondent à vos besoins. La seule différence est que les protocoles IoT sont encore assez jeunes, et doivent encore démontrer leur fiabilité. Rappelez-vous que, lorsque l'internet est devenu une réalité, IP version 4 a été ce qui l'a rendu possible. Nous déployons maintenant massivement IP version 6, et l'IoT est l'application phare que les opérateurs de télécommunications ont attendu pour justifier l'investissement nécessaire.
- Le positionnement de chacun des protocoles IoT nécessite un questionnement similaire. A l'exception de HTTP, tous ces protocoles sont positionnés comme des protocoles IoT temps réel de publication-abonnement, avec prise en charge de millions d'appareils. Selon la façon dont vous définissez « temps réel » (en secondes, millisecondes ou microsecondes) et « objets » (nœud de WSN, appareil multimédia, dispositif portable personnel, scanner médical, commande de moteur, etc.), la sélection du protocole pour votre produit est essentielle. Fondamentalement, ces protocoles sont tous très différents.
- Au-delà de la conception du matériel et du logiciel, cependant, il y a la conception des systèmes de données de l'IoT. Nous devons séparer les données de l'application afin que nous puissions en faire de nouvelles choses, des choses que nous n'avons pas encore imaginées. Pour le développeur de système intégré typique, penser spécifiquement aux données générées par le système nécessite un nouvel état d'esprit. Ces données ont de la valeur. Dans la conception des systèmes intégrés, nous comprenons très bien comment concevoir l'architecture de l'objet, du réseau local et même de la passerelle. Le processeur, le capteur, la connectivité sans fil, la passerelle, le réseau IP et la sécurité sont des éléments qui sont tous bien connus du développeur intégré.
- Le nouveau défi pour la communauté intégrée est de profiter de la valeur inhérente à nos données en tirant parti d'un certain type d'informatique cloud. Afin de monétiser les données du système intégré, un certain type d'informatique cloud est absolument nécessaire, que le cloud soit privé, public ou externalisé. Il s'agit d'un nouveau paradigme pour la communauté des systèmes intégrés.
- La technologie matérielle, la technologie du logiciel, l'infrastructure et l'informatique cloud des

systèmes intégrés sont activement testés et déployés, en favorisant l'émergence de l'internet des objets. Pour réussir vraiment, et réaliser les 50 milliards d'appareils qui seront déployés d'ici à 2020, nous avons besoin des mêmes normes ouvertes, du même développement et de la même coopération que ceux qui ont soutenu la création de l'internet des personnes (également connu sous le nom de web). L'Alliance IPSO réalise la promotion des normes IP et les utilise pour construire les architectures de référence que les développeurs de produits recherchent.

- L'IoT pour les systèmes intégrés constitue la nouvelle révolution industrielle. Le potentiel de croissance de l'industrie des systèmes intégrés est énorme. Pour réaliser ce potentiel, l'industrie des systèmes intégrés doit adopter le nouveau paradigme IoT. Nous comprenons maintenant ce qui doit être fait. Nous pouvons ne pas encore avoir de normes bien définies et établies pour chaque élément structurel des futurs systèmes IoT, comme la facilité de configuration ou la mise à niveau sécurisée du firmware à distance. Mais cela ne devrait pas empêcher quiconque de construire un système qui apportera de la valeur aux clients.