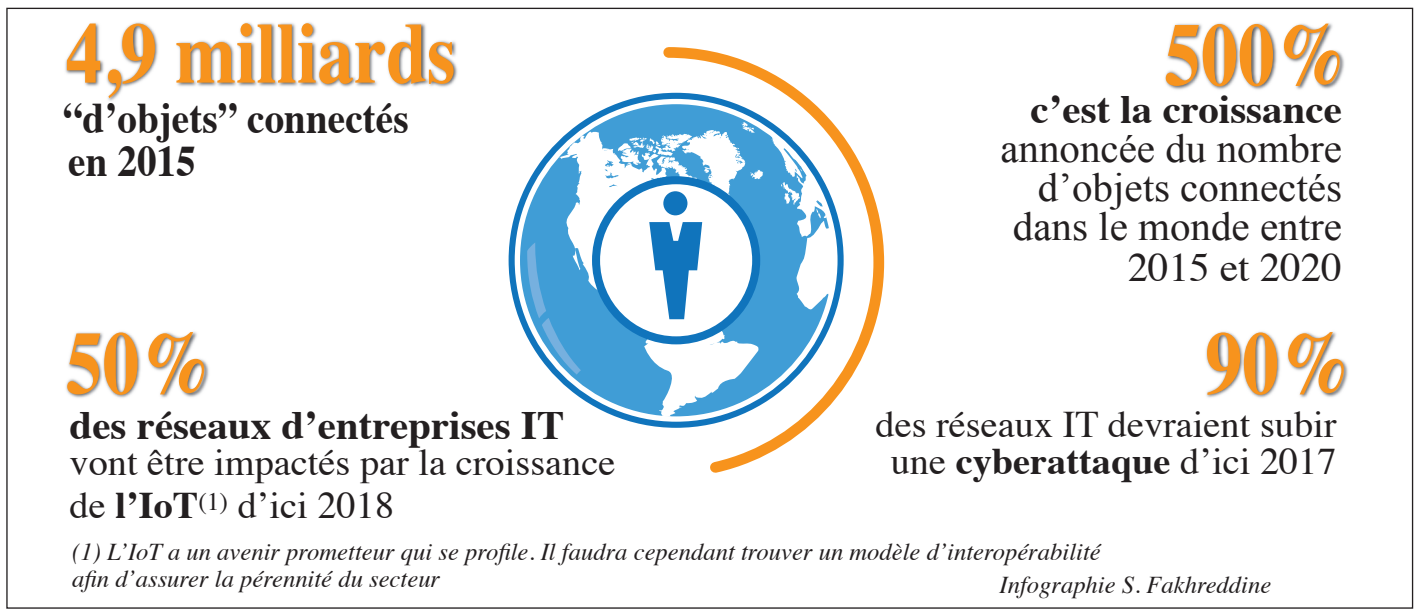
Internet des objets: Encore peu fiable!

■ Le secteur bute contre deux écueils: interopérabilité et sécurité

■ L'industrie avance trop vite pour la recherche fondamentale

■ Les grandes entreprises s'essayent à des protocoles open source



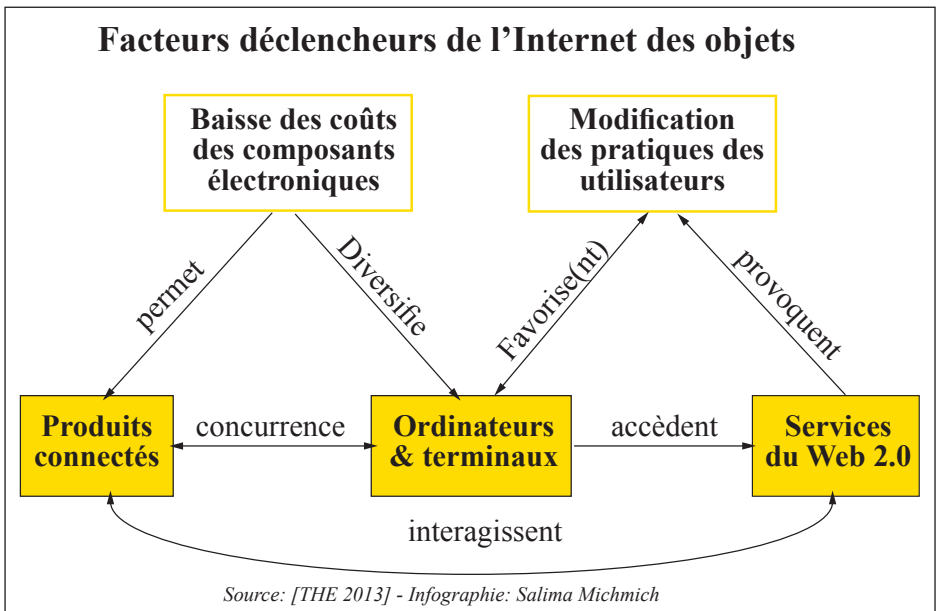
(1) L'IoT a un avenir prometteur qui se profile. Il faudra cependant trouver un modèle d'interopérabilité afin d'assurer la pérennité du secteur

Infographie S. Fakhreddine

UN frigo, une télé, une machine à laver, une montre qu'on gère à distance… C'est loin d'être une sinécure! Ce qu'on appelle l'internet des objets (IoT) souffre de deux écueils majeurs: le manque d'interopérabilité et la sécurité encore perfectible. Aujourd'hui 80% des objets connectés ne fonctionnent pas correctement ainsi que le souligne Imad Saleh, professeur en sciences de l'information et de la communication de l'Université Paris 8 et directeur du laboratoire Paragraphe. «Tout ne va pas bien. Le défi majeur pour l'IoT est technique. Il faut pouvoir gérer l'hétérogénéité des normes technologiques d'objets couplées à des multitudes de besoin d'applications en termes de services de sécurité», explique-t-il. Le développement de l'IoT ne pourra être réellement positif et efficient que si et seulement si ces deux conditions sont garanties. Car aujourd'hui tout reste à faire ou presque, explique le chercheur. Et chacun essaie d'imposer sa norme, ses solutions, son écosystème, et ce à tous les niveaux. Que ce soit dans les réseaux (Sigfox, LoRa, Wifi HaLow, 5G, Bluetooth, ZigBee, 6LowPan, etc.), dans les plateformes cloud (Microsoft Azure, AWS, IBM, Google, Salesforce, etc.), dans les API, les frameworks, les protocoles de communication, les systèmes d'exploitation, le hardware… «Ceci soulève des problèmes de gestion et de sécurité des objets dans un milieu technologique hétérogène. Il est donc important d'instaurer des politiques de sécurité claires qui définissent les responsabilités des opérateurs», poursuit Imad Saleh.

• L'interopérabilité: Quelle harmonie entre les différents acteurs?

Il est compliqué de faire coexister des objets connectés produits par des constructeurs différents. En effet, les opérateurs désirant occuper la meilleure place possible sur le marché en devenir de l'IoT élaborent des protocoles propriétaires, pour des objets intelligents. Les entreprises essayent chacune de leur côté de bâtir leur écosystème, le but étant de se démarquer des concurrents. Le business model de l'IoT a évolué et s'oriente désormais vers des objets adaptables aux consommateurs afin d'offrir une utilisation facile de tous les objets connectés. D'ailleurs le développement de cette technologie tend peu à peu vers une harmonisation des protocoles, en open source, pour que les objets connectés communiquent entre eux, à la fois dans l'environnement technologique propre à chaque constructeur et plus largement avec d'autres constructeurs. Pour l'industrie des objets connectés, intégrer l'écosystème du libre est une nécessité et une assurance de pérennité. Il y a 6 mois le consortium Open Connectivity Foundation (OCF), promoteur du projet open source IoTivity, et l'AllSeen Alliance, qui fournit le cadre IoT open source AllJoyn, une technologie open source de communication développée par Qualcomm, ont annoncé leur fusion. Celle-ci devrait faire avancer l'interopérabilité entre les appareils connectés des deux groupes, libérant ainsi le plein potentiel opérationnel de l'Internet des objets et représentant une étape significative vers un écosystème connecté. «Il n'y aura pas de protocole de communication commun pour IoT, comme on peut l'imaginer pour la sécurité. Mais nous pouvons toutefois espérer une future interopérabilité grâce à l'utilisation d'un protocole open source ou d'un protocole propriétaire qui ferait l'unanimité», explique Mehdi Ammi, chercheur au CNRS. «Pour y arriver, il faut faire passer les intérêts du secteur avant les intérêts commerciaux», renchérit-il. En effet, les marques qui disposent des fonds nécessaires peuvent se permettre de créer leur écosystème à coup de dollars mais cela bride l'innovation et la visibilité que peuvent avoir de plus petits acteurs qui ne disposeraient pas des mêmes moyens.



Source: [THE 2013] - Infographie: Salima Michmich

L'émergence de l'IoT s'explique par deux facteurs majeurs: la banalisation des ressources informatiques et l'adoption des services web par les utilisateurs

• La sécurité des données, principal frein au développement de l'IoT

La sécurité des données collectées et traitées par les objets intelligents est la seconde problématique d'envergure de l'IoT, sur laquelle de nombreux constructeurs et chercheurs planchent activement. Selon une étude HP (Hewlett Packard), les dix premiers objets connectés commercialisés pour le grand public étaient peu, voire non protégés de possibles piratages. A tous les maillons de la chaîne de l'IoT, on constate des défaillances sur la sécurité des données, notamment au sein des protocoles de communication ou de l'interface dans laquelle arrivent les données collectées par ces objets. Tous ces aspects doivent être sécurisés, pour que le marché de l'IoT évolue et qu'entreprises et particuliers l'adoptent. Des petits aux grands acteurs de l'écosystème, cette problématique est fignolée et des solutions sont trouvées. Thales, Safran, Atos, Xerox, Schneider Electric ou encore Capgemini œuvrent pour créer des technologies fiables pour leurs clients, dans leurs propres domaines d'expertise. Des sociétés plus petites, telles que Tiempo par exemple, spécialisée dans les cartes à puces, sont en train de muter vers les objets connectés. L'enjeu est donc, aujourd'hui, global. «La sécurité a toujours posé problème en informatique. Quelles que soient les méthodes utilisées, dès qu'il y a de la technologie et des connexions, il y a un risque. Mais il faut avancer. Tant qu'il n'y aura pas un consortium solide pour la sécurité, le développement de l'IoT risque d'être compliqué», confie Nasredinne Bouhai, maître de conférences à l'Université Paris 8, section hypermedia et chercheur au laboratoire Paragraphe.

Bien que le marché de l'IoT soit en constante mutation et que les business models soient plus ou moins aboutis, les constructeurs et chercheurs doivent continuer à œuvrer en collaboration, pour faire converger ce marché. La sécurité des données ainsi que l'harmonisation des protocoles de communication sont des objectifs réalisables. Mais pour cela, la confiance numérique doit être garantie à chaque maillon de la chaîne de l'IoT.❑

Reda BENOMAR