Lettre mensuelle – Juin 2020 – Disponible sur omc.ceis.eu

Table des matières

ANALYSES (1/2)

NEW IP : UN CHEVAL DE TROIE CHINOIS À L'ITU ?

Fin mars 2020, le *Financial Times* publiait deux articles sur l'ambition chinoise de remplacer le modèle TCP/IP par un énigmatique nouveau protocole appelé « New IP »[1]. Ces articles s'appuyaient sur le rapport du cabinet Oxford Information Labs (Oxil), initialement destiné à l'OTAN, qui met en garde contre ce modèle « qui centraliserait le contrôle du réseau dans les mains des opérateurs télécom, qui appartiennent tous ou sont contrôlés par l'Etat en Chine »[2]. Suite à la présentation de ce projet à l'ITU, certains ont également craint que le système proposé ne dispose même d'un *kill-switch* (« shut-up command » dans le texte) permettant à un point central du réseau de couper les communications vers et depuis un autre point du réseau. Largement repris par les médias spécialisés, les articles semblent insister sur l'urgence du danger et soulignent que des travaux sur ce nouveau protocole sont déjà en cours dans plusieurs pays, à la fois au niveau industriel et universitaire, comme l'a indiqué Sheng Jiang chargé de piloter ces travaux chez Huawei. Et ce d'autant plus que la Russie et l'Arabie Saoudite auraient indiqué leur soutien à la proposition chinoise.

Que faut-il réellement craindre du *New IP* et quels sont les apports mis en avant par ses promoteurs ?

1. La proposition chinoise

Les travaux dont il est question ont été présentés à l'(nternational Telecommunication Union (ITU) en septembre 2019 et en février 2020. Trois documents relatifs à la proposition chinoise sont disponibles : la proposition elle-même[3] était accompagnée d'une lettre de présentation signée de Huawei Technologies, la China Mobile Communications Corporation, la China Unicom et le Ministère chinois de l'Industrie et des Technologies de l'Information (MIIT)[4], et d'un document de présentation[5]. On peut cependant noter que le docteur Richard Li, Chief Scientist chez Huawei, avait déjà proposé la création d'un groupe de travail très similaire à l'ITU en juillet 2018, projet qui comprenait la même rhétorique et mentionnait déjà le terme de *New IP.* Celui-ci avait mené à la création du groupe de travail GF NET-2030 au sein de l'ITU, groupe visant à travailler sur les capacités des réseaux à horizon 2030.

Les experts chinois reprochent à la tendance actuelle consistant à multiplier et à améliorer les protocoles de communication selon les usages d'être source d'inefficience et de risques de sécurité. Ils estiment que l'hétérogénéité des réseaux qui en découle, qui nécessite la mise en place d'interfaces supplémentaires pour lier les réseaux de protocoles différents, engendre des coûts et des pertes de performance non souhaitable. Ils considèrent enfin qu'il est temps de changer d'approche dans l'élaboration des protocoles réseaux en

[1] https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2, https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f
[2] https://www.infosecurity-magazine.com/news/nato-warns-new-authoritarian/
[3] http://prod-upp-image-read.ft.com/e8dd8c46-70e6-11ea-95fe-fcd274e920ca
[4] http://prod-upp-image-read.ft.com/ec34d7aa-70e6-11ea-95fe-fcd274e920ca
[5] http://prod-upp-image-read.ft.com/eff4a82a-70e6-11ea-95fe-fcd274e920ca

définissant un protocole de communication universel qui soit capable de supporter et donc de fédérer tous les types de réseau.

Le document de présentation chinois et la proposition proprement dite évoquent en outre les besoins grandissants en bande passante (liés notamment aux communications holographiques) et en latence (liés par exemple aux véhicules autonomes) que nécessitent le développement de nouveaux usages du numérique encore peu matures afin de justifier ce besoin de gagner en efficience.

Les auteurs de la proposition chinoise proposent, pour dépasser ces limites, de mettre en place le cadre d'un nouveau protocole internet simplement nommé « New IP », qui permettrait de simplifier le transport entre les différents réseaux utilisant ce protocole, notamment en y facilitant l'intégration des réseaux IoT et en réduisant la latence et les coûts de fonctionnement. Il est notamment proposé pour y parvenir de :

- Modifier le format des adresses IP, c'est-à-dire des identifiants numéraires attribués à chaque périphérique utilisant le protocole (ordinateur, tablette, smartphone…), et qui dans le cadre du New IP seraient de longueur variable.
- Définir au sein de ce que l'on appelle les « entêtes » de paquets d'information ou des fichiers transitant sur les réseaux, et qui contiennent les données permettant à l'entité destinatrice d'extraire et traiter les données échangées (telles que les adresses IP de l'expéditeur et du destinataire, le protocole de communication…) des attributs donnant des informations sur l'objet correspondant à une adresse IP donnée. De cette façon, un ordinateur souhaitant communiquer avec une ressource distante dont il ne possède que le nom de domaine (par exemple un site web), ne doit plus nécessairement attendre la réponse du Domain Name pour obtenir l'adresse IP associée.
- Rendre possible la spécification, au sein de ces mêmes entêtes, des actions à effectuer sur les paquets d'information transportés sur les réseaux, comme par exemple son niveau de priorité ou le choix de la route qu'il doit emprunter (ce dernier point étant totalement contraire aux principes de routage qui gouvernent l'Internet depuis sa création et qui reposent sur un routage « opportuniste », c'est-à-dire déterminé par dispositifs de transport).

Ceci étant dit, la proposition chinoise est en réalité très succincte. Très peu détaillée et critiquée par de nombreux observateurs pour son manque de précision et de clareté, elle est encore visiblement à un stade très précoce de conception, et semble avoir plutôt vocation à interpeller et faire réagir les autres membres de l'ITU. Si certains ont d'abord pu craindre que New IP ait été conçu pour devenir un outil de contrôle de réseaux internet mondiaux par la Chine, il semblerait plutôt, au vue du niveau actuel d'avancement du projet, que la proposition chinoise réponde également à un enjeu de visibilité et d'influence au sein d'une instance dans laquelle la Chine a une marge de manœuvre certaine, plutôt qu'à de réels enjeux opérationnels.

2. Le New IP : instrument de contrôle ou outil d'influence ?

Protocole unique fédérant tous les réseaux, on peut intuitivement penser que le New IP entraînerait une centralisation accrue du réseau et, *ipso facto*, l'obsolescence du système actuel du Domaine Name System (DNS), le service qui permet de traduire les adresses IP en noms de domaine internet. Notons cependant qu'une forme de centralisation existe de fait déjà dans l'architecture actuelle de l'Internet, contre-balancée par une certaine flexibilité qui permet à chacun de la contourner : par exemple en définissant des serveurs DNS alternatifs distincts de ceux de son opérateur, ou en encapsulant son trafic dans un tunnel VPN. De même, il

paraît raisonnable d'imaginer que ce nouveau protocole, quand bien même il aurait vocation à être ubiquitaire, serait assez souple pour s'adapter à différents usages. Quant à la crainte de la présence d'un « kill-switch » permettant à une autorité centrale de couper les communications depuis et vers un point du réseau, aucun élément dans la proposition chinsoie ne permet de le confirmer. Il semblerait surtout que cette crainte fasse écho à des arguments régulièrement évoqués mais jamais vérifiés pour agiter le risque représenté par la montée en puissance de la Chine en matière de numérique.

En revanche, le projet New IP, aussi peu abouti qu'il soit, s'inscrit dans une dynamique de guerre d'influence opposant la Chine aux autres grandes puissances numériques, à la fois dans les institutions internationales de normalisation, et en matière de déploiements d'infrastructure réseau dans le monde

L'institution RIPE NNC (Regional Internet Registry for Europe Network Coordination Center)[6] a rapidement fait savoir son opposition aux travaux chinois sur ce nouveau protocole, insistant pour que tous travaux liés à l'évolution du protocole IP et des normes associées soient laissés à l'Internet Engineering Task Force (IETF), historiquement l'organisme en charge du développement des normes relatives aux protocoles Internet, et soient conduits sous sa gouvernance. Rappelons en effet que l'IETF est une organisation ouverte aux individus, là où l'ITU est une émanation des Nations Unies, et composée donc par les États membres de l'ONU. On comprend donc bien que la sphère occidentale – et surtout les États-Unis – puisse bénéficier d'une plus grande influence à l'IETF, originellement créée principalement par des chercheurs américains et où ils ont historiquement toujours joué un rôle clé dans les travaux sur la création des protocoles de l'Internet. On note d'ailleurs que tous les présidents de l'organisation ont été occidentaux, et en majorité américains. A l'inverse, la Chine est plus active à l'ITU où elle peut se reposer sur ses relations bilatérales avec de nombreux pays pour avancer ses pions.

Les ambitions chinoises de contrôle sur les réseaux sont déjà perceptibles dans la stratégie de développement adoptée en 2013 par le gouvernement chinois, appelée *One Belt One Road* (OBOR) et renommée depuis *Belt and Road Initiative* (appelée en France initiative route et ceinture, ou nouvelle route de la soie), qui ne se limite effectivement pas aux seules infrastructures de transport, mais qui comprend également une dimension « télécommunications ». A ce titre, la Chine bénéficie d'une influence considérable dans les nombreux pays où elle participe au développement des infrastructures réseaux, notamment en Afrique, de même qu'elle pourra être soupçonnée d'y projeter ses moyens de surveillance.

Rien ne permet donc d'affirmer en l'état que le "New IP" apporterait à la Chine de réelles capacités supplémentaires de surveillance du trafic ou de contrôle des réseaux ou des dispositifs connectés, rien ne semble permettre de l'affirmer ni même de l'imaginer en l'état. D'autant que le moindre ambiguïté sur les ambitions chinoises risque de rendre encore plus difficile, voire clairement impossible, l'adhésion des autres parties prenantes de l'ITU, rendant inutile et coûteuse le développement d'un nouveau protocole à des fins du surveillance ou de contrôle. Le contexte est effectivement davantage celui d'une guerre d'influence entre parties prenantes constituées de puissances étatiques, de multinationales et dans une moindre mesure de la société civile, dans un contexte gépolitique marqué par la renaissance d'une puissance qui, d'abord industrielle, se veut devenir également technologique.

On peut cependant se poser la question de la pertinence de l'approche radicale défendue à travers le *New IP* qui propose un remplacement drastique et global de tous les protocoles existants, plutôt que leur

[6] RIPE est également en charge de la zone Moyen-Orient et d'une partie de l'Asie Centrale.

développement autonome par briques successives sur le modèle de ce qui a jusqu'à présent a fait le succès d'Internet. Comme le rappelle Hascall Sharp dans son article pour l'Internet Society, *An Analysis of the New IP proposal to the ITU-T*, les différents challenges auxquels les auteurs de la proposition chinoise souhaitent répondre sont en effet déjà traités, au niveau international, par des travaux visant à étendre et améliorer les protocoles actuels. Certains sont toujours en cours, comme par exemple les travaux sur la conception d'un standard pour l'utilisation de transport déterministe compatible TCP/IP , le « Deterministic Networking (DETNET) et Reliable and Availabe Wireless (RAW) » de l'IETF, ainsi que « 802.1 Time Sensitive Networking (TSN) » de l'Institute of Electrical and Electronics Engineers (IEEE), qui sont développés en coordination avec l'ITU-T et le 3GPP[7]. D'autres protocoles existent déjà (BGPSEC, DNSSEC, RPKI, etc.), et la problématique les concernant est bien celle de leur déploiement. Il est ainsi reproché à l'initiative chinoise de faire double emploi avec des travaux existants. D'autre part, le passage à un nouveau protocole faisant fi de tous préexistants engendrerait des coûts dantesques pour un horizon de gain très éloigné. Rappelons qu'un protocole tel que l'IPv6 existe depuis une vingtaine d'année, et qu'il en faudra peut-être probablement autant pour qu'il finisse de remplacer l'IPv4, durée pendant laquelle leur coexistence est source de coûts et de difficultés dans la sécurisation.

[7] 3GPP est une coopération entre organismes de normalisation en télécommunication dont l'ITU, l'ETSI, l'ARIB/TTC, le CCSA, l'ATIS et le TTA.

ANALYSES (2/2)

DISSUASION DANS LE DOMAINE CYBER : QUELLES SOLUTIONS STRATEGIQUE ?

De manière générale, une stratégie de dissuasion consiste « *à inciter un ennemi potentiel à ne pas attaquer une cible en lui faisant croire que les coûts et les conséquences qui résulteront de l'attaque seront supérieurs aux avantages potentiels qu'il pourra en retirer* »[8]. La dissuasion est une stratégie qui a notamment été développée pendant la Guerre froide dans le cadre du développement des capacités nucléaires. Dans ce cadre, la France considère la dissuasion davantage comme une fonction stratégique de découragement qui est « strictement défensive » et que « l'emploi de l'arme nucléaire ne serait concevable que dans des circonstances extrêmes de légitime défense »[9].

Si la conception classique de la dissuasion a été discutée dans le domaine cyber dès les années 1990, elle s'est rapidement révélée inadaptée aux spécificités du cyberespace[10]. En effet, à la différence de l'arme nucléaire qui est considérée comme une arme à n'employer qu'en dernier recours, les armes cyber sont couramment utilisées, notamment sous le seuil de l'agression armée. En outre, les difficultés d'attribution des cyberattaques ou encore les difficultés de connaitre la temporalité et les réels impacts de ces dernières sont autant d'obstacles qui ne permettent pas d'appliquer une dissuasion similaire à celle des moyens nucléaires.

- Le concept stratégique de la dissuasion a donc été adapté au domaine cyber. Deux approchent ont notamment été retenues au niveau académique[11] :

- L'approche par « punition » qui repose sur des mesures offensives sanctionnant le comportement hostile d'un adversaire. Dans le cyberespace, il s'agit notamment de se doter de capacités cyber-offensives permettant par exemple de contre-attaquer ou de lancer une attaque préventive contre des attaquants potentiels ;

- L'approche par « déni » qui consiste à convaincre les cyberattaquants qu'ils n'obtiendront pas les avantages qu'ils recherchent, en adoptant des mesures défensives à tous les niveaux d'une attaque, c'est-à-dire de la prévention jusqu'à la réponse à incident.

Cependant, ces deux approches stratégiques, prises isolément, se révèlent imparfaites pour faire cesser l'augmentation continue des cybermenaces dans leur ensemble (de la lutte contre la cybercriminalité à la cyberguerre). L'approche par « punition » nécessite, en effet, de disposer d'importantes capacités cyber-offensives et se heurte généralement à la difficulté d'attribution des cyberattaques. De son côté, l'approche par « déni » vise plus à décourager les cyberattaquants en sécurisant les systèmes d'information et réseaux critiques nationaux, notamment via une coopération publique-privée renforcée permettant aux États de se doter de composants matériels et logiciels fiables et robustes. Cette approche est donc centrée sur la défense

[8] https://www.airuniversity.af.edu/Portals/10/ASPJ_French/journals_F/Volume-09_Issue-1/iasiello_f.pdf

[9] https://www.defense.gouv.fr/content/download/206186/2286591/Livre-blanc-sur-la-Defense-et-la-Securite-nationale%202013.pdf

[10] https://www.cfr.org/blog/cyber-deterrence-dead-long-live-cyber-deterrence

[11] https://www.airuniversity.af.edu/Portals/10/ASPJ_French/journals_F/Volume-09_Issue-1/iasiello_f.pdf

et la consolidation de la résilience des infrastructures numériques nationales plus que sur une capacité de dissuasion proprement dite.

Aujourd'hui, une approche holistique et « inter-domaines » est préconisée dans les stratégies nationales cyber, notamment aux États-Unis par la Cyberspace Solarium Commission[12]. Cette approche stratégique implique davantage de coordination entre les différents acteurs nationaux publics et privés mais aussi plus d'implication en matière de régulation et de coopération internationale dans le domaine cyber.

Une approche holistique incluant les approches par « déni » et par « punition »

La dissuasion dans le domaine cyber repose aujourd'hui sur des mesures de nature cyber ou non combinant les approches mentionnées précédemment dites par « déni » et par « punition ». La stratégie américaine de dissuasion en « couches » (strategy of layered cyber deterrence) de la Cyberspace Solarium Commission consacre cette approche dans son rapport publié en mars 2020. Cette Commission préconise une nouvelle stratégie cyber qui a pour objectif de réduire la gravité et la fréquence des cyberattaques contre les intérêts américains sur le long terme tout en conservant une capacité de riposte en fonction de l'intensité des cyberattaques. La Commission distingue ainsi trois niveaux (ou « couches ») de mesures :

- Les mesures visant à réguler les comportements dans le cyberespace et limiter la prolifération des cyber-opérations ;
- Les mesures visant à assurer la sécurité des infrastructures vitales et démocratiques du pays ;
- Les mesures s'appuyant sur les capacités militaires.

Dans son rapport, la Commission américaine fait la promotion d'une résilience nationale cyber et affirme la nécessité de renforcer la coopération entre les secteurs public et privé en matière de cybersécurité. La Commission consacre donc une approche de la dissuasion par « déni ». Pour autant, elle réaffirme la stratégie « defend forward » (« arrêter la menace avant qu'elle n'atteigne sa cible ») adoptée par le Département de la défense américaine (DOD) en 2018[13], ce qui consacre également une approche par « punition ». Notons également que la position américaine dite « d'engagement persistant », qui stipule que les États-Unis traquent, ciblent et menacent continuellement ses adversaires dans le cyberespace contribue d'une certaine manière à une dissuasion par « punition »[14].

En Europe, le Royaume-Uni a également consacré dans sa Stratégie nationale de Cybersécurité 2016-2021 une approche holistique de la dissuasion dans le domaine cyber[15]. Tout en précisant que le pays continuera de développer ses capacités cyber-offensives, la stratégie britannique consacre une approche globale en matière de cybersécurité et de résilience pour rendre difficile les cyberattaques sur ses infrastructures critiques.

---

[12] https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view

[13] https://www.lawfareblog.com/cyberspace-solarium-commission-report-and-persistent-engagement ; https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

[14] https://fr.weforum.org/agenda/2019/06/la-dissuasion-dans-le-cyberespace/

[15] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643419/French_translation_-_National_Cyber_Security_Strategy_2016.pdf

Plus implicitement, la Chine a affirmé, dans sa Stratégie nationale de sécurité dans le cyberespace de 2016, qu'elle concentrerait ses efforts sur la protection de ses infrastructures[16]. Néanmoins, tout en se montrant publiquement hostile au développement de la dissuasion dans le cyberespace dans un sens offensif, la Chine a, dans les faits, quand même renforcé ses capacités cyber-offensives pour disposer de mesures de ripostes notamment en réaction à la montée capacitaire des États-Unis[17].

Vers une stratégie systématique du découragement « inter-domaines »

L'adoption d'une approche holistique du découragement s'accompagne d'une conception plus « inter-domaines » combinant des mesures de nature cyber ou non. Autrement dit, les États se réservent le droit de recourir à l'ensemble des instruments nationaux et internationaux pour dissuader les cyberattaquants de conduire des cyberattaques, ce qui peut être par exemple l'utilisation du recours à l'action cinétique. Ce fut par exemple le cas d'Israël contre des cyber-attaquants du Hamas en mai 2019[18]. Les stratégies chinoise[19], américaine[20] et britannique reconnaissent d'ailleurs la possibilité de recourir à des mesures de nature non cyber pour sanctionner les comportements hostiles dans le cyberespace comme le recours au droit international, à la diplomatie ou encore aux mesures militaires classiques.

Les implications aux niveaux national et international

La dissuasion dans le domaine cyber est aujourd'hui un concept stratégique qui se renouvelle et qui laisse place davantage à une stratégie plus globale intégrant des moyens défensifs et offensifs, de nature à la fois cyber et non cyber. Au niveau national, l'approche holistique et « inter-domaines » de la dissuasion dans le domaine cyber impliquera nécessairement de renforcer la coordination nationale sur les enjeux du cyberespace. Plus particulièrement, il s'agira de mieux coordonner l'action des acteurs de la sécurité nationale avec les acteurs de la défense nationale mais aussi avec les acteurs de la justice. Cette coordination nationale est d'ailleurs l'un des enjeux organisationnels de la cyberdéfense française soulevé par la Revue stratégique de cyberdéfense de 2018[21]. L'objectif est de mettre en place quatre chaînes opérationnelles : la chaîne « protection », la chaîne « action militaire », la chaîne « renseignement » et la chaîne « investigation judiciaire ».

Au niveau international, les applications de la nouvelle conception de la dissuasion dans le domaine cyber devraient concerner le renforcement de l'implication des États dans l'application ou l'élaboration de normes internationales relatives au cyberespace ou pour lutter contre la cybercriminalité et la prolifération des cyber-armes. Il devrait en résulter davantage de diplomatie et de coopération internationale, notamment dans les domaines militaire, du renseignement ou judiciaire.

---

[16] https://www.worldscientific.com/doi/pdf/10.1142/S2630531319500021

[17] https://www.worldscientific.com/doi/pdf/10.1142/S2630531319500021

[18] https://siecledigital.fr/2019/05/06/apres-avoir-subi-une-cyberattaque-israel-repond-par-la-force/

[19] https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1366/RAND_RR1366.pdf ; https://www.dems.defense.gouv.fr/sites/default/files/2019-10/dossier_22_chine_2019.pdf

[20] https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF

[21] http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

FOCUS INNOVATION

Acklio : la perspective Internet de l'Internet des objets

Présentation

Acklio est fondée en 2016 à Rennes par Alexandre Pelov et Laurent Toutain, alors tous deux chercheurs à Télécom Bretagne. Travaillant initialement sur un projet appelé Open Energy Data visant à monitorer et partager la consommation d'électricité entre individus, ils ont été confrontés à l'absence d'outils permettant de collecter les données de l'IoT et aux problématiques d'interopérabilités leurs réseaux limités. Partant de ce constat, ils ont développé une technologie facilitant l'interconnexion des réseaux IoT avec les réseaux IP.

La solution

Acklio propose une suite logicielle sous licence aux différents acteurs de l'écosystème IoT : opérateurs, intégrateurs systèmes et fabricants d'objets connectés. Ces acteurs emploient les briques logicielles d'Acklio dans leurs déploiements IoT. Celles-ci intègrent notamment :

- Côté objet connecté, le SDK (Software Development Kit) SCHC Acklio, qui comprend une librairie pouvant etre implémentée sous la forme d'un middleware sur l'objet, sur le module ou sur un *dongle* externe. Il s'agit de la partie client du dispositif.
- Côté serveur, le cœur IP Acklio (Acklio IP Core), qui est la solution logicielle connectée au serveur LPWAN.

La solution Acklio vise à assurer la compatibilité des réseaux LPWAN (LoRaWan, Sigfox, NB-IoT et LTE-M) avec le réseau IP standard. Acklio propose en outre des « kit de démarrage » clé en main à destination des universités et des entreprises en vue de recherche ou de prototypage.

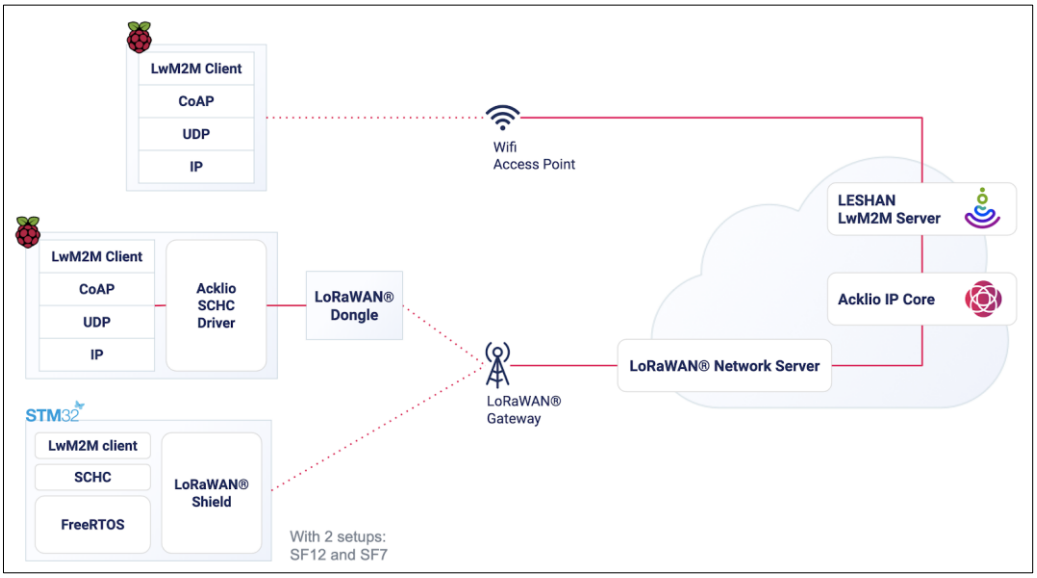

Figure 1 : Schéma d'une architecture démontrant l'intégration du protocole LwM2M au sein d'un réseau mixte IP

L'innovation

Avant le développement du Static Context Header Compression (SCHC), les constructeurs et opérateurs d'objets connectés étaient contraints de choisir une technologie LPWAN puis d'adapter leurs développement et projets autour de ce choix initial, faute d'interopérabilité entre les réseaux. En outre, la nature contrainte des réseaux LPWAN (faible bande passante, messages limités en taille) implique que les fournisseurs de technologie implémentent chacun leurs propres solutions de sécurité spécifique, généralement peu éprouvées et sans réelle sécurité de bout-en-bout.

La technologie SCHC permet de comprimer un message de 70 octets en 3 octets pour communiquer entre l'objet et l'application. Le cœur de réseau IP d'Acklio consiste en une plateforme logicielle qui ajoute les fonctionnalités d'interconnexion et qui sécurise les échanges réseaux de l'objet jusqu'à l'application. Ce dispositif permet de réduire la taille des entêtes protocolaires afin de permettre à des dispositifs sous protocole IP de s'interconnecter avec des dispositifs sous protocole LoRaWan, offrant ainsi l'interopérabilité entre les réseaux dédiés à l'IoT et l'Internet.

Les perspectives

En avril 2020, le SCHC a été reconnu comme standard par L'Internet Engineering Task Force (IETF). Si le SCHC en lui-même devient ouvert à tous, Acklio a pu prendre de l'avance et a déjà développé une solution aboutie. L'entreprise va pouvoir faire usage de sa première levée de fonds de 2 millions d'euros en décembre 2019 pour accélérer la mise sur le marché de ses solutions.

CALENDRIER

07/07, 08/07/ et 09/07 : Cyberdéfense & Stratégie 2020 « Le monde d'après sera-t-il post-digital ? » (Replay)

La crise de la Covid-19 met en relief une double réalité : les usages digitaux ont explosé durant la crise alors que dans le même temps, celle-ci mettait en lumière des dépendances fortes à des contingences matérielles, des flux d'approvisionnement physiques, etc. Dans les régions confinées, le trafic Internet a ainsi bondi de 70%. Alors que certains pronostiquaient un effondrement en cascade des réseaux, Internet a tenu bon : l'utilisation des réseaux sociaux est en hausse de plus de 60%, près de 20 millions de Français se sont mis au télétravail, tandis que de nouvelles formes de rencontre, de loisirs et de sport ont émergé. Des nouveaux usages qui subsisteront, au moins en partie, à l'issue de la crise.

Faut-il y voir l'avènement d'un nouvel âge de maturité numérique où les usages digitaux seront encore plus intégrés à notre quotidien, où la réalité sera mixte et l'expérience utilisateur « *phygitale* » ? Quels enseignements tirer de cette crise ? Quelles sont les technologies clés favorisant cette hybridation du réel et du virtuel, cette fusion des deux mondes ? Quels défis et solutions, notamment en termes de cybersécurité et de souveraineté ?

Accédez aux replays :

ACTUALITÉ

L'ANSSI publie ses premiers « Papiers numériques »

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a lancé le 17 juin 2020 la première édition de ses « *Papiers numériques* ». Nouveau format de son rapport d'activité, cette revue annuelle à vocation nationale et internationale apporte un éclairage sur la cybersécurité française. Elle propose à cet égard une revue de l'actualité de l'année passée, des contenus prospectifs et divers témoignages d'acteurs de l'écosystème de la transformation numérique (évolution de la cybermenace, intelligence artificielle, identité numérique, vote électronique, blockchain, etc.). Les *Papiers numériques* comportent également un dossier en anglais qui permet de promouvoir des initiatives françaises, européennes et internationales.

Accédez à l'édition 2020 des *Papiers numériques* :

La **Direction générale des relations internationales et de la stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

À ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique (OMC)**, qui s'inscrit dans le contrat-cadre n°2018-02. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère des Armées
Direction générale des relations internationales et de la stratégie
60 Boulevard du Général Martial Valin – CS21623 – 75 509 Paris Cedex 15

CEIS
Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com