Université de technologie de Compiègne - Proposition de thèse

1re partie : Fiche scientifique	
Intitulé de la thèse	Protocoles de communication sécurisés et adaptatifs pour les objets communicants hétérogènes
Type de financement	allocation Ministère
Laboratoire d'accueil	unité de recherche : HEUDIASYC équipe de recherche : RO (Réseaux et Optimisation) site web : https://www.hds.utc.fr/heudiasyc/recherche/equipe-ro/
Directeur(s) de thèse	Hicham Lakhlef (Dr), Abdelmadjid Bouabdallah (Pr, HDR)
Domaines de compétence	Informatique, électronique Sciences pour l'ingénieur
Description du sujet de thèse	Le développement des solutions d'objets communicants présente des enjeux majeurs. Ce sujet est considéré comme une des priorités des programmes de recherche européen et fait partie des axes stratégiques de la recherche nationale. L'Internet des objets (IdO) est un réseau composé d'une variété de nœuds, comme les dispositifs portables connectés (capteurs, MEMS, robots, montres intelligentes, téléphones intelligents, PDAs, etc.), les voitures connectées, etc. L'IdO a un large domaine d'applications dans notre vie quotidienne notamment dans les services de transport, les services de santé, la surveillance et la sécurité. Vu ce large domaine d'applications, l'IdO va bientôt occuper une place comparable à celle de l'électricité dans le quotidien des citoyens, et jouera un rôle fondamental dans le développement socio-économique. Les objets communicants une fois déployés sont sujet à différentes attaques, externes ou internes au réseau, qui peuvent mettre en péril leur bon fonctionnement. Afin de mettre en œuvre des architectures d'IdO robustes, il est nécessaire de déployer un mécanisme de gestion de clés cryptographiques qui seront distribuées sur les objets (génération, échange, stockage, et renouvellement de clés). Comme l'IdO peut être composé d'un très grand nombre d'objets (jusqu'au milliard de nœuds), les protocoles à développer doivent supporter le passage à l'échelle. Cette gestion de clés devient encore plus difficile et présente de nouveaux challenges lorsque les objets déployés sont hétérogènes (des nœuds ayant différentes caractéristiques et des ressources limitées). Le problème de gestion de clé a été largement étudié dans les réseaux de capteurs mais peu de travaux sont spécifiques à l'IdO. Les travaux de recherche existants portant sur la gestion de clés dans l'IdO sont limités aux nœuds homogènes (ayant les mêmes caractéristiques en termes de capacité de stockage et puissance de calcul). De plus, ces travaux ne prennent pas en considération le cas où la communication fait intervenir une source et plusieurs destinations (communication de groupes). Comme de nombreuses applications nécessitent de faire communiquer des objets ayant des caractéristiques différentes, des défis importants restent encore à relever. En effet, si les objets ont des capacités de stockage différentes (comme dans le domaine de la santé par exemple), certains nœuds risquent de ne pas pouvoir stocker toutes les clés et/ou de ne pas pouvoir faire les calculs de chiffrement nécessaires. En conséquence, les services de sécurité (confidentialité, authentification, intégrité, non-répudiation, vie privée) seront mis en défaut. **Dès lors, comment peut-on développer des solutions de gestion de clés permettant de réaliser les objectifs suivants :** *a) Atteindre un haut niveau de sécurité et d'efficacité en termes d'énergie et de communication (complexité en nombre de message), tout en prenant en compte la capacité de stockage et de calcul plus faible sur certains nœuds.* *b) Fonctionner de manière efficace dans un environnement à grande échelle où le*

	nombre de canaux de communication est limité. Il faut alors sécuriser l'envoi de messages dans le canal pour éviter les collisions et les conflits. De plus, des canaux pouvant être défectueux, il faut pouvoir s'appuyer sur un nombre de canaux limité. *c) Gérer la synchronisation sécurisée des objets ayant des horloges différentes : la grande variabilité du retard des communications entre objets hétérogènes, ajoutée aux limitations des ressources des nœuds (calcul, mémoire, énergie), élève la complexité du problème pour l'IdO.* *d) Prendre en compte l'autonomie et la mobilité des systèmes ubiquitaires tout en considérant la récupération et l'économie de l'énergie ainsi que l'évolutivité et son impact énergétique.* Pour réaliser ces objectifs, il est nécessaire de proposer des architectures de sécurité complètement décentralisées, qui s'appuient sur la coordination et la collaboration entre les objets hétérogènes pour offrir un service de gestion de clés robuste. Plusieurs pistes peuvent être explorées comme : - l'intégration de nouveaux composants additionnels (proxys de calcul et stockage par exemple), - la modélisation et l'optimisation des canaux de communication et des séquences de stockage de clés pour prendre en considération les contraintes de ressources, - l'intégration de modèles de confiance pour renforcer les services de sécurité contre les attaques internes. Le sujet de cette thèse porte ainsi sur la conception de protocoles de gestion de clés dans l'IdO hétérogène en prenant en compte les communications multi-niveau et la mobilité des systèmes ubiquitaires tout en considérant l'économie de l'énergie.
Mots clés	Sécurité, Internet des objets, mobilité, communication
Profil et compétences du candidat	
Date de début de la thèse	09/2017
Lieu de travail de thèse	Université de Technologie de Compiègne

2e partie : Fiche de poste	
Durée	36 mois
Possibilité missions complémentaires	
Laboratoire d'accueil	UMR CNRS 7253 HEUDIASYC
Moyens matériels	
Moyens humains	• Chercheurs CNRS : 9 • Enseignants-Chercheurs : 45 • ITA CNRS : 16 • IATOS : 10 • Doctorants : 52 • ATER : 5 • Post-doctorants et ingénieurs CDD : 14 Visiteurs et Stagiaires : 24
Moyens financiers	
Modalités de travail	
Projet de recherche lié à cette thèse	Financement ministériel
Collaboration(s) nationale(s)	
Collaboration(s) internationale(s	
Thèse en cotutelle internationale	non
Coordonnées de la personne à contacter	Hicham Lakhlef, +33 3 44 23 79 15, hlakhlef@utc.fr

Contacter d'abord le directeur de thèse avant de renseigner
un dossier de candidature en ligne sur https://webapplis.utc.fr/admissions/doctorants/accueil.jsf