Campagne 2020 Contrats Doctoraux Instituts/Initiatives

Proposition de Projet de Recherche Doctoral (PRD)

Appel à projet MSTD - Maîtrise des syst tehno durables 2020

Intitulé du Projet de Recherche Doctoral : Modèles sécurisés et robustes pour une communication économe en énergie dans l'IoT à large échelle

Directeur de Thèse porteur du projet (titulaire d'une HDR) :

NOM : **BOUABDALLAH** Prénom : **Abdelmadjid**
Titre : Professeur des Universités ou
e-mail : madjid.bouabdallah@hds.utc.fr
Adresse professionnelle : 57 avenue de Landshut, Compiègne 60200
(site, adresse, bât., bureau)

Unité de Recherche :
Intitulé : Heudiasyc
Code *(ex. UMR xxxx)* : UMR CNRS 7253

ED71 - Sciences pour l'ingénieur UTC

Ecole Doctorale de rattachement de l'équipe & d'inscription du doctorant :

Doctorants actuellement encadrés par le directeur de thèse (préciser le nombre de doctorants, leur année de 1ere inscription et la quotité d'encadrement) : Kandi Mohamed Ali (3ème année, 50%) ; Aktouche Sadek Rayane (2ème année, 50%) ; Aboubakar Moussa (2ème année, 100%) ; Benhamaid Sana (1ère année, 50%)

Co-encadrant :

NOM : **Jaber** Prénom : **Ghada**
Titre : Maître de Conférences des Université HDR ☐
ou
e-mail : ghada.jaber@utc.fr

Unité de Recherche :
Intitulé : Heudiasyc
Code *(ex. UMR xxxx)* : UMR CNRS 7253

ED71 - Sciences pour l'ingénieur UTC
Ecole Doctorale de rattachement : Ou si ED non Alliance SU :

Doctorants actuellement encadrés par le co-directeur de thèse (préciser le nombre de doctorants, leur année de 1ere inscription et la quotité d'encadrement) :

Cotutelle internationale : ☒ Non ☐ Oui, précisez Pays et Université :

Description du projet de recherche doctoral *(en français ou en anglais)*

3 pages maximum – interligne simple – Ce texte sera diffusé en ligne

Détailler le contexte, l'objectif scientifique, la justification de l'approche scientifique ainsi que l'adéquation à l'initiative/l'Institut.
Le cas échéant, préciser le rôle de chaque encadrant ainsi que les compétences scientifiques apportées. Indiquer les publications/productions des encadrants en lien avec le

projet.
Préciser le profil d'étudiant(e) recherché.
Etudiant ingénieur ou master 2 en informatique

1) Sujet de thèse

L'Internet des objets (IoT) est une technologie prometteuse ayant de nombreux domaines d'applications. L'objectif de l'IoT est d'intégrer les mondes physique et numérique dans un seul écosystème qui constitue une nouvelle ère intelligente d'Internet. Cet objectif est atteint en interconnectant un grand nombre d'objets intelligents et hétérogènes du monde physique à Internet. Cependant, l'IoT souffre de plusieurs problèmes dont certains présentent plusieurs verrous comme la sécurité et l'énergie vu les ressources limitées et hétérogénéité des objets IoT [1-3]. L'un des principaux obstacles de la mise en œuvre de telles applications est la garantie d'une énergie suffisante qui permet de faire fonctionner le réseau de manière autosuffisante en termes d'énergie tout en garantissant un bon niveau de sécurité. Par conséquent, il est impératif de développer des solutions efficaces permettant d'offrir un bon niveau de sécurité tout en optimisant la consommation énergétique, et ainsi améliorer la longévité des objets de l'IoT [4].
Bien qu'il existe de nombreuses méthodes pour assurer une efficacité énergétique [5] comme l'utilisation de protocoles de communication légers (lightweight) [6] ou l'endormissement des nœuds [7], une solution qui prend en considération la sécurité, la scalabilité ainsi que l'hétérogénéité des objets n'a pas été encore proposé [8]. En effet, alors que les performances des réseaux sans fil ont atteint un degré acceptable en communication, il n'est pas encore facile de déterminer un dimensionnement énergétique efficace de l'objet tout en répondant aux exigences de sécurité [9]. Ainsi, il est très important de modéliser et de dimensionner la consommation énergétique des objets IoT lors des étapes de pré-déploiement en particulier lorsque on considère des facteurs critiques, tels que la réduction des coûts, la durée de vie et l'énergie disponible.
Étant donné que les solutions de sécurité (par exemple, le chiffrement des données) augmentent de manière similaire leurs exigences de calcul au fil du temps afin de rester robustes face à des attaquants de plus en plus capables, un écart de consommation d'énergie associé existe. Néanmoins, il est nécessaire de concevoir des solutions de sécurité optimisées en termes d'efficacité énergétique. En effet, les solutions de sécurité peuvent exploiter des informations spécifiques au contexte pour améliorer l'efficacité énergétique. Par exemple, dans le contexte cloud, de nombreux appareils IoT peuvent fournir des opportunités pour gérer les calculs liés à la sécurité de manière économe en énergie [9].
Notre sujet rentre tout à fait dans l'axe « Green Computing » dans le sens où les résultats de cette thèse permettront de réduire la consommation énergétique et contribuer au développement durable.

Pour illustrer les activités qui seront menées dans le cadre de ce sujet de thèse, nous allons considérer comme exemple l'usine du futur ou "industrie 4.0" qui fait appel aux capteurs, automates et actionneurs pour relancer le dynamisme de l'industrie ce qui permet d'optimiser la production, d'avoir une production plus flexible, une traçabilité poussée, et d'assurer la maintenance ou encore l'efficacité énergétique des usines. Le réseau considéré est composé de N objets connectés réalisant un objectif donné et ayant les caractérisitiques suivantes :

- Chaque nœud a une capacité énergétique donnée et limitée ;
- Les nœuds du réseau communiquent dans le temps et consomment de l'énergie.

A noter que la communication radio est une des principales causes de la consommation d'énergie.
- Dans le cas des applications sensibles des algorithmes de sécurité nécessaires à intégrer (cryptographiques, authentifications) constituent une nouvelle source de consommation d'énergie. En effet, les algorithmes de sécurité nécessitent une puissance de calcul importante afin de rester robustes face à des attaques.

Ainsi, l'objectif de cette thèse est de proposer des modèles de communication sécurisés et robustes qui prennent en considération l'économie en énergie pour les objets communicants ayant des ressources limitées. Au cours de la modélisation nous ferons appel à des modèles stochastiques permettant d'obtenir des solutions optimisées spécifiques au domaine d'applications à considérer [10].

Pour répondre aux objectifs de cette thèse, les principaux verrous scientifiques que nous avons identifiés et qui seront traités dans cette thèse sont les suivants :

1. Étude de l'impact des solutions de sécurité sur la consommation énergétique des objets hétérogènes.
2. Développement de nouveaux modèles d'optimisation des communications pour les objets communicants hétérogènes à grande échelle sous contrainte de limitation d'énergie et de nombre de canaux de communication.
3. Développement de nouveaux modèles d'optimisation offrant un bon compromis entre la consommation énergétique et le niveau de sécurité.
4. Extension des résultats obtenus pour intégrer de nouvelles contraintes comme la limitation des capacités de stockage.

Pour lever ces verrous scientifiques, il est nécessaire de proposer des architectures d'économie d'énergie complètement décentralisées qui devront s'appuyer sur la coordination et la collaboration entre les objets hétérogènes pour offrir un niveau de sécurité robuste.

Pour atteindre cet objectif, nous envisageons suivre les directions de rercherche suivantes :
- la modélisation et l'optimisation énergétique des communication, séquences de stockage de messages pour prendre en considération les contraintes de ressources ;
- intégration la technologie récente de la récolte d'énergie (Energy Harvesting) qui fournit une méthode prometteuse fondamentale pour prolonger la durée de vie du réseau [11]. De plus, la capacité de récolter de l'énergie à partir de sources ambiantes ou dédiées permet le chargement sans fil (Wireless Charging) des batteries des objets ayant besoin [12] ;
- la diminution de la complexité des algorithmes de sécurisation des objets hétérogènes.

2) L'état du sujet dans le laboratoire et l'équipe d'accueil

L'équipe SCOP du laboratoire HEUDIASYC (UMR CNRS) a une vingtaine d'années d'expérience en recherche et développement de solutions innovantes pour divers problèmes liés aux communications dans les réseaux et systèmes distribués. En particulier les problèmes d'allocations de ressources dans les systèmes, le routage, les communications dans les réseaux mobiles et leur sécurité. Dans le cadre de divers projets industriels, nationaux, régionaux, et internationaux, l'équipe a développé des protocoles de routage avec Qualité de Service et économie

d'énergie pour les communications point-à-point et multipoints (ou multicast), et des solutions de sécurité (confidentialité et authentification) efficaces et supportant la dynamique des membres et la résistance aux défaillances. L'équipe travaille également sur la sécurité d'un nouveau modèle de communication où la contrainte énergie est très forte et a mené des projets interdisciplinaires comme les réseaux de capteurs pour l'agriculture de précision et pour la rééducation fonctionnelle. L'équipe a obtenu quatre brevets en collaboration avec Motorola Lab, plusieurs publications dans des revues et conférences internationales de bon niveau1, et de nombreuses avancées issues de thèses de doctorat et masters.

3) Le programme et l'échéancier de travail :

1ère année :
Tâche 0 (Oct. 2020- jan. 2021) : Étude de l'état de l'art sur l'IoT et les applications de l'usine de futur.
Tâche 1 (jan. 2021- mars. 2021) : Identification les principaux défis qui doivent être pris en compte dans le développement d'une architecture IoT hétérogène, économe en énergie et sécurisée.
Tâche 2 (04 mars. 2021- 04 mai. 2021) : Étude de différents modèles stochastiques permettant de modéliser la consommation énergétique dans l'internet des objets.
Tâche 3 (mai. 2021- juillet 2021) : Identification et étude des verrous à lever pour le développement de solutions innovantes qui prend en considération la sécurité des service et l'économie d'énergie dans l'usine de futur.

2 ème année : Développement de nouvelles solutions et publication des résultats scientifiques.

3 ème année : Expérimentation sur la plateforme IoT et rédaction de la thèse

4) Publications liées au sujet de thèse :
[1] Lee, I., & Lee, K. "The Internet of Things (IoT): Applications, investments, and challenges for enterprises". Business Horizons, 58(4), 431-440, 2015.
[2] A. Al-Fuqaha, M. Guizani, M, Mohammadi, M. Aledhari, & M. Ayyash, (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys & tutorials, 17(4), 2347-2376, 2015.
[3] G.Jaber, A.Bouabdallah, al.: Distributed Time Slots Assignment Protocol in Dynamic Networks : First Study. 25th IEEE Symposium on Computers and Communications (ISCC) 2020, soumis.
[4] A.Barki, A.Bouabdallah, S.Gharout, J.Traoré: M2M Security: Challenges and Solutions. IEEE Communications Surveys and Tutorials 18(2):1241-1254, 2016.
[5] T. Rault, A.Bouabdallah, and Y. Challal. "Energy efficiency in wireless sensor networks: A top-down survey." Computer Networks 67: 104-122, 2014.
[6] Z. Sheng, C. Zhu, and V. C. M. Leung, "Surfing the Internet-of-Things: Lightweight Access and Control of Wireless Sensor Networks Using Industrial Low Power Protocols," EAI Endorsed Trans. Industrial Networks and Intelligent Systems, vol. 14, no. 1, 2014.
[7] V. Jelicic et al., "Analytic Comparison of Wake-Up Receivers for WSNs and Benefits Over the Wake-On Radio Scheme," Proc. 7th ACM Wksp. Performance Monitoring and Measurement of Heterogeneous Wireless and Wired Networks, 2012, pp. 99–106.
[8] R. Arshad, S. Zahoor, M. A. Shah, A. Wahid and H. Yu, "Green IoT: An Investigation on Energy Saving Practices for 2020 and Beyond," in IEEE Access, vol. 5, pp. 15667-15681, 2017.[9] B. Martinez, Borja, et al. "The power of models: Modeling power

consumption for IoT devices." IEEE Sensors Journal 15.10 (2015): 5777-5789.
[10] C. Tunc, and N. Akar. "Markov fluid queue model of an energy harvesting IoT device with adaptive sensing." Performance Evaluation 111 (2017): 1-16.
[11] S. Sudevalayam and P. Kulkarni, "Energy Harvesting Sensor Nodes: Survey and Implications," IEEE Commun. Surveys and Tutorials, vol. 13, no. 3, 3rd 2011, pp. 443–61.
[12] C. Wang, J. Li, Y. Yang and F. Ye, "Combining Solar Energy Harvesting with Wireless Charging for Hybrid Wireless Sensor Networks," in IEEE Transactions on Mobile Computing, vol. 17, no. 3, pp. 560-576, 1 March 2018.