Protocole opportuniste pour la mise à jour distribuée d'un système IoT d'observation de l'environnement reposant sur la science participative

Acronyme du projet: OppNetUpdate
Mots clés: IoT, gestion de version, communications opportunistes, observation de l'environnement
Lieu: Laboratoire IRISA (Vannes)
Équipe d'accueil: CASA (http ://www.irisa.fr/casa)
Directeur de thèse: Yves Mahéo (yves.maheo@univ-ubs.fr)
Co-encadrant: Nicolas Le Sommer (nicolas.le-sommer@univ-ubs.fr) / Lionel Touseau (lionel.touseau@univ-ubs.fr)
Priorité région Bretagne: Adaptation et atténuation du changement climatique

1 Description du projet

1.1 Résumé

Les effets du changement climatique sur les écosystèmes sont de plus en plus marqués. Pour atténuer ces effets, il convient d'adapter nos pratiques à la disponibilité des ressources et aux conditions environnementales. Il convient également de mesurer l'efficacité de ces adaptations afin d'encourager les pratiques aux effets vertueux sur les écosystèmes. Pour cela, il est nécessaire d'observer l'état de l'environnement et des ressources grâce au déploiement de nombreux capteurs.

Le projet ANR Ladybird dans lequel s'inscrit cette thèse, propose d'étudier un système d'observation de l'environnement formé de composants à bas coût communicant sur des réseaux hybrides étendus à faible consommation et bas débit. Ce système s'appuie sur la science participative et devrait améliorer la qualité de l'observation et la capacité de prévention des risques liés au changement climatique. Le système d'observation proposé repose sur des communications LoRa opportunistes et multi-sauts, qui ont vocation à faciliter le déploiement du système en absence d'infrastructure réseau pré-existante, et à tolérer les ruptures de connectivité résultant de la mise en sommeil ou de la mobilité des nœuds.

Cette thèse vise à étudier et définir un protocole sécurisé de mise-à-jour distribuée de ces nœuds. Des solutions de mise-à-jour par les airs existent déjà, mais ces solutions reposent sur des communications point-à-point, et non sur des communications opportunistes, et n'offrent pas de mise-à-jour distribuée. Dans cette thèse, des structures de données distribuées telles que les CRDT pourront être considérées, et être adaptées au système. Les mécanismes de sécurité intégrés à ce protocole de mise-à-jour pourront reposer sur des signatures ou sur des mécanismes de réputation. Les idées proposées s'intégreront dans la plateforme qui sera proposée dans le projet ANR Ladybird.

1.2 Hypothèses, questions posées, identification des points de blocage

Ce travail de thèse vise à proposer un protocole de mise à jour distribuée pour un système d'observation de l'environnement à large échelle reposant sur une science participative. Ce protocole doit ainsi permettre de faire évoluer le système d'observation et de corriger des erreurs ou des failles de sécurité de celui-ci. Les dispositifs qui composent ce système ne sont pas tous connectés directement et de manière permanente aux équipements d'infrastructure. Certains de ces dispositifs peuvent en effet être mobiles, être mis en veille pendant de longues périodes pour des raisons d'économie d'énergie et ne pas être dans la zone de couverture des passerelles d'inter-connexion à Internet. Ils doivent donc s'appuyer sur des dispositifs/objets intermédiaires pour transmettre et recevoir des données. L'absence de connectivité de bout-en-bout, qui résulte de ces mises en veille et de cette mobilité, ne permet pas une administration centralisée d'un tel système. Dans ce contexte où les dispositifs ne sont pas joignables, les opérations d'administration telles que les mises à jour logicielles sont généralement effectuées hors-ligne,

dispositif par dispositif. Lorsque le nombre de dispositifs déployés devient trop important, les procédures de mise à jour devraient pouvoir être effectuées à distance, de manière distribuée.

Cette thèse devra donc répondre aux questions suivantes:

- Quels mécanismes peuvent être mis en œuvre afin d'assurer une mise à jour globale des nœuds d'un système, en tenant compte du fait que les objets impliqués possèdent de faibles capacités de traitement et de stockage ?

- Comment maintenir le système en condition opérationnelle lors d'une mise à jour des modes de communications, alors que des versions hétérogènes co-existent ?

- De manière plus générale, peut-on garantir la convergence de l'état du système (i.e., version des différents nœuds), et comment y parvenir ?

- Quel est l'impact de la dynamique du réseau et des ruptures de connectivité sur la propagation des mises à jour ?

- Enfin, dans quelle mesure un nœud peut-il faire confiance à une mise à jour, et plus généralement comment sécuriser le processus de mise à jour sans connectivité garantie vers une autorité de confiance ?

Cette thèse pourra s'appuyer sur les travaux menés par l'équipe CASA de l'IRISA sur le protocole de communication opportuniste pour LoRa, baptisé LoRaOpp [1].

Les hypothèses de travail concerne l'existence d'un protocole de communication opportuniste. Des travaux préliminaires ont été menés dans ce sens avec la définition du protocole LoRaOpp. Un point de blocage possible concerne la capacité de stockage des dispositifs. En effet, ceux-ci doivent être en mesure de stocker temporairement les éléments à mettre à jour avant leur application. Si les mises à jour sont trop conséquentes, certains objets ne disposant pas d'une capacité de stockage suffisante, pourraient ne pas pouvoir effectuer celles-ci. Il conviendra donc pour lever ce point éventuel de blocage en procédant à des mises à jour incrémentales. En outre les dispositifs ayant des capacités de stockage limitées, il conviendra de répartir les mises à jour sur les dispositifs afin que chaque dispositif ne stocke pas l'intégralité des mises à jour, et déterminer quand une mise à jour peut être supprimée des espaces de stockage des nœuds.

1.3 Collaborations scientifiques (nature/partenariat/pays) et partenariat socio-économique envisagé

Dans le cadre de son plan climat, air, énergie territorial (PCAET), Golfe du Morbihan Vannes Agglomération (GMVA) souhaite mettre en œuvre un observatoire des changements climatiques, observatoire qui se veut complémentaire à l'observatoire de l'environnement en Bretagne[1]. À ce titre, GMVA a initié plusieurs projets, dont un projet de relevé des température d'eau de mer dans le Golfe du Morbihan, qu'elle mène en collaboration avec l'Université de Bretagne Sud et des enseignants-chercheurs de l'équipe CASA de l'IRISA. La solution proposée dans cette thèse pourrait aider à mettre à jour les capteurs déployés pour les besoins de cet observatoire des changements climatiques.

Dans le cadre du projet ANR Ladybird, un partenariat est établi avec les sociétés CGWireless, REQUEA et ANS innovation. La société CGWireless est une société Bretone qui conçoit des dispositifs radio fréquence pour l'IoT. La société REQUEA, qui est localisée à Lyon, déploie des réseaux IoT et propose des solutions cloud d'administration et de supervision de ces réseaux. La société ANS innovation, qui est localisée à Grenoble, est spécialisée quant à elle dans le développement de solutions logicielles pour assurer des communications dans des environnements difficiles.

En outre au niveau national, il est prévu de collaborer avec les équipes de recherche ERODS et Drakkar du LIG (Laboratoire d'Informatique de Grenoble) sur les réseaux pair-à-pair et IoT , ainsi qu'avec l'Institut des Géosciences de l'environnement (IGE) de Grenoble sur l'observation des changements climatiques.

Enfin à l'international, le projet Ladybird prévoit de mener une campagne d'expérimentation autour de la problématique des risques liés à la gestion de l'eau autour de Hô Chi Minh-Ville au Vietnam, en collaboration avec les laboratoires Sub-Institute of Hydro-Meteorology and Climate Change of South Vietnam (SIHYMECC) et Southern Region Hydro-Meteorological Center (SRHMC).

References

[1] Nicolas Le Sommer and Lionel Touseau. Loraopp: A protocol for opportunistic networking and computing in lora networks. In *18th International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob 2022, Thessaloniki, Greece, October 10-12, 2022*, pages 308–313. IEEE, 2022.

[1] `https://bretagne-environnement.fr/`