1 Projet de thèse

Aujourd'hui, les villes intelligentes disposent des réseaux sans fil hétérogènes dans le but de simplifier, d'améliorer et de sécuriser notre vie quotidienne. Par exemple, les réseaux sans fil ad hoc pour véhicules (IEEE 802.11p) et les réseaux LTE (LTE-V) sont proposés pour améliorer la sécurité routière. L'Internet industriel des objets (IIoT) est également une alternative pour les applications de sécurité et de divertissement. Les réseaux de capteurs sans fil, tels que IEEE 802.15.4, LoRa et NB-IoT, sont des réseaux qui collectent et communiquent des données pour construire une vue globale de l'environnement de la ville. Toutes ces données collectées peuvent être utilisées pour prédire les comportements humains et améliorer la sécurité de leurs déplacements grâce à des algorithmes d'apprentissage. Ainsi, la fiabilité et la qualité de service de la transmission des données restent un des problèmes de recherche avec des contraintes différentes à chaque couche de communication.

La dynamique et l'hétérogénéité des appareils et de leur utilisation rendent la conception de réseaux robustes et évolutifs très complexe. Cependant, les réseaux restreints (IIoT ou véhicules) sont vulnérables à plusieurs types d'attaques. Par exemple, l'attaquant ou le brouilleur peut générer un bruit, interférant avec les fréquences radio utilisées par les dispositifs IoT. Il peut en résulter un plus grand nombre de communications provenant d'appareils IoT pouvant épuiser leurs batteries. Par conséquent, le déni de service pourrait facilement être causé. Même si la sécurité est assurée, le réseau doit fournir une bonne qualité de service à d'autres applications (par exemple, les retards de transmission). Les protocoles de qualité de service (QoS) peuvent permettre aux réseaux d'identifier et de hiérarchiser la transmission des données en fonction de la criticité des données. Dans la littérature, plusieurs protocoles ont été proposés concernant la sécurité et la QoS [1]. Le protocole MQTT (Message Queuing Telemetry Transport) a été défini avec trois niveaux de QoS. Il supporte la fiabilité des messages en définissant leurs priorités mais sans diminuer les délais sur l'ensemble des appareils du réseau. La stratégie de défense contre les attaques de brouillage pourrait être basée sur l'évasion spectrale, le contrôle de la puissance de sortie ou le codage des communications en fonction des ressources des dispositifs [2][3].

2 Objectifs et contributions attendues

Un démonstrateur d'un système de contrôle des feux de circulation urbaine basé sur (IoT-UTLC) a été prototypé à ECE Paris.

- Le premier objectif de la thèse serait d'intégrer des aspects innovants à notre IoT-UTLC. Le candidat étudiera de nouvelles architectures, de nouveaux protocoles et proposera plusieurs cas d'utilisation tenant compte du délai et de la sécurité de la transmission des données.
- Le deuxième objectif sera l'étude des vulnérabilités de sécurité et des attaques possibles dans les réseaux IoT pour les villes intelligentes. Cette étude portera sur deux niveaux d'attaques : les attaques physiques et les attaques de la couche application.
- Le troisième objectif consistera à évaluer et à étudier l'immunité des réseaux du monde réel. Le candidat proposera des solutions pour les vulnérabilités identifiées et démontrera leur efficacité.

3 Tâches

- État de l'art du sujet proposé (Sécurité et QoS)
- Conception des solutions aux problèmes décrits
- Mise en œuvre, tests et évaluations

References

[1] A. A. Simiscuka and G. Muntean, " A Relay and Mobility Scheme for QoS Improvement in IoT Communications," in *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, 00002, May 2018, pp. 1–6.

[2] W. Xu, K. Ma, W. Trappe, and Y. Zhang, " Jamming Sensor Networks: Attack and Defense Strategies," *IEEE Network*, vol. 20, no. 3, pp. 41–47, May 2006, 00559.

[3] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, " A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2018, 00000.