Identifier des noeuds IoT en espionnant leur signal radio

Tulippe Hecq Arnaud
Département d'Informatique

L'avènement de l'Internet of Things (IoT) a lancé une nouvelle ère d'appareils connectés, ouvrant de nouvelles possibilités de partage de l'information, d'automatisation et de protection. L'expansion de l'IoT soulève une nouvelle problématique de sécurité. Entre autres, l'identification des noeuds au sein des réseaux est essentielle. Il a été découvert que des noeuds fabriqués avec les mêmes microprocesseurs et modèles d'émetteurs-récepteurs radio peuvent présenter de subtiles particularités dans les caractéristiques de leurs signaux. Cette variabilité intrinsèque de la transmission des signaux radio peut être exploitée pour distinguer les noeuds d'un réseau. En écoutant leurs signaux radio et en analysant leurs signatures distinctes, il devient possible de les identifier, et ainsi prouver leur légitimité.

L'objectif du travail est d'identifier des noeuds de l'Internet of Things utilisant la technologie LoRa, en se basant uniquement sur les caractéristiques spécifiques de leur signal radio, différenciées par une dispersion sensible de la performance des composants électroniques intégrés dans chaque émetteur. LoRa est une technologie de communication sans fil qui permet de transmettre des données sur de longues distances avec une faible consommation d'énergie. LoRa fonctionne avec un protocole de type Low Power Wide Area Network appelé LoRaWAN. Ce travail est structuré en trois parties.

Le premier chapitre développe les aspects du traitement du signal nécessaires à la compréhension des expérimentations menées durant le mémoire. Le concept de signal radio, le principe de modulation, la gestion du bruit et la Transformée de Fourier sont détaillés dans ce chapitre. Cette partie comprend également une description de la couche physique de la technologie LoRa, ainsi qu'une présentation de son protocole LPWAN LoRaWAN.

Le deuxième chapitre se concentre sur les expérimentations effectuées. D'abord tout le matériel est introduit. Les différentes radio logicielles (SDR) DVB-T, R820T2 et HackRF sont détaillées avec leurs schémas blocs respectifs. Les modules d'émission LoRa de type RN2483, Arduino et Pycom LoPy sont présentés avec leurs caractéristiques respectives. Ensuite, les logiciels d'analyse tels que Universal Radio Hacker (URH) ou GQRX sont introduits avec leur fonctionnement. Le chapitre se termine avec l'analyse des signaux LoRa générés par les différents modules d'émission via ces logiciels et via Python.

Le troisième et dernier chapitre présente la méthode utilisée pour l'identification des noeuds. Les diagrammes de constellations différenciées (DCTF) permettent de mettre en évidence l'unique propriété physique appelée **signature** pour chaque noeud. L'article de Yu Jiang, Linning Peng, Aiqun Hu, Sheng Wang, Yi Huang et Lu Zhang intitulé *Lora Devices Identification Based on Differential Constellation Trace Figure* affirme que la position géographique de la signature permet l'identification des noeuds. Cette méthode est appliquée sur le matériel sélectionné par l'analyse du deuxième chapitre.

Les résultats du mémoire ne s'alignent pas avec l'article *Lora Devices Identification Based on Differential Constellation Trace Figure*. Cependant, une approche alternative s'est révélée durant les expérimentations. Cette piste se concentre toujours sur la signature comme propriété discriminante pour des noeuds LoRa, mais en s'intéressant à sa forme géométrique spécifique au sein de la DCTF plutôt qu'à sa position géographique.