Université Lille Nord de France

Ecole doctorale régionale Sciences Pour l'Ingénieur
Lille Nord-de-France - 072

Titre Thèse	Techniques de Machine Learning pour la géolocalisation de systèmes communicants sans fils non autorisés	
(Co)-Directeur	Eric Simon	E-mail : eric.simon@univ-lille.fr
(Co)-Directeur	Virginie Deniau	E-mail : virginie.deniau@ifsttar.fr
(Co)-Encadrant		E-mail :
Laboratoire	IEMN	Web :
Equipe	TELICE	Web :
Financement prévu	Contrat Doctoral Etablissement	ULille ☒ UPHF ☐ Centrale Lille ☐ Yncrea ☐
	Région – Autre ☐	Contrat de recherche ☐ Préciser :
Financement acquis ? ☐	Contrats de Recherche ☐ Préciser	Autre ☐ Préciser

Résumé du sujet :

Depuis quelques années, de nombreux cas d'introduction de systèmes communicants sans fils dans des zones sensibles, dans un but malveillant, ont été rapportés dans la presse. L'objectif de ces intrusions étant principalement de faire de l'espionnage ou du déni de service. Ainsi l'actualité récente a fait état d'une affaire relative à de la fuite de données au moyen d'un point d'accès WiFi illicite. L'opération utilisait des ordinateurs sur lesquels les cartes WiFi avaient été réactivées de manière malveillante par des intervenants extérieurs en charge de la maintenance. Ce point d'accès WiFi illicite a ensuite permis la récupération des données par un drone survolant la zone de couverture radio du WiFi. Par ailleurs, l'introduction de téléphones portables dans des zones où leur usage est interdit, comme des bâtiments ministériels ou des prisons, pose des problèmes de sécurité important. On peut citer également l'utilisation de brouilleurs électromagnétiques qui viennent mettre en déni de service un certain nombre de fonctions de communication sans fil dans des sites critiques (sites industriels Seveso par exemple) où il y a des éléments de surveillance importants : transmission vidéo, transmission de données de maintenance, etc. Tous ces sujets de sécurité ont un point commun : un terminal communicant qui est entré de manière illicite dans une zone sensible.

L'objectif de la thèse est dans un premier temps de détecter la présence d'une activité électromagnétique "anormale" dans la zone à surveiller, puis dans un second temps de géolocaliser cette source illicite (un point d'accès WiFi, un téléphone portable, un brouilleur, etc), en s'appuyant sur des techniques de machine learning. Nous partirons de cas d'usage bien définis. L'équipe encadrante participe à un projet sur la susceptibilité aux brouilleurs des communications LoRa pour la maintenance des équipements ferroviaires. Ce contexte pourra constituer le premier cas d'usage.
Les techniques de machine learning semblent particulièrement bien adaptées à ces scénarios où la zone à surveiller est parfaitement définie, ce qui autorise la réalisation de campagnes de mesures intensives ou de simulations pour nourrir la phase d'apprentissage des algorithmes.

Plus précisément, les algorithmes de géolocalisation qui seront développés combineront une double approche : triangulation puis machine learning. Il s'agira donc d'abord d'identifier les points chauds en terme de puissance, mais à ce stade sans information en terme de protocole. Ensuite, l'algorithme travaillera sur les fenêtres de temps actives au moment de la reconnaissance des points chauds pour faire de la reconnaissance et de la classification de protocoles.

Mis en forme : Couleur de police : Automatique

L'originalité de l'approche est de travailler uniquement sur le signal physique, alors que la plupart des systèmes de détection d'intrusion sont positionnés sur les couches les plus hautes, les couches applicatives. Ceci permet de se libérer de toute question de confidentialité puisqu'il ne s'agit à aucun moment de lire ou détecter des données.

L'équipe encadrante travaille depuis plusieurs années sur la susceptibilité des protocoles de communication aux attaques par brouillage (jamming en anglais) ou de type protocolaires, ainsi qu'à leur détection et classification (voir références à la fin). Le candidat pourra s'appuyer sur cette expertise pour aborder la question de la géolocalisation d'une source illicite dont on ne connait pas grand-chose par nature.

Références :

J. Villain, V. Deniau, A. Fleury, E.P. Simon, C. Gransard, R. Kousri, "EM Monitoring and classification of IEMI and protocol-based attacks on IEEE 802.11n communication networks", *IEEE Trans. Electromagn. Compat.*, 2019.

J Farah, J Akiki, EP Simon, "Energy-efficient techniques for combating the influence of reactive jamming using Non-Orthogonal Multiple Access and Distributed Antenna Systems", Wireless Telecommunications Symposium - WTS 2019

C. Gransart, V. Deniau, E.P. Simon, A. Fleury, S. Lecoeuche, P. Millot, E. Masson “Cyber Security of the Railway wireless system: detection, decision and Human-in-the-Loop”, Proceedings of 7th Transport Research Arena TRA 2018, April 16-19, Vienna, Austria, 2018

G. Romero, V. Deniau, E.P. Simon, “Mitigation Technique to Reduce the Wi-Fi Susceptibility to Jamming Signals”, 2nd URSI AT-RASC, Gran Canaria, 28 May – 1 June, 2018

V.Deniau, C. Gransart, G. Romero, E. P. Simon, J. Farah, “IEEE 802.11n Communications in the Presence of Frequency-Sweeping Interference Signals”, *IEEE Trans. Electromagn. Compat.*, 2017.