Réseaux
securité-IIOT

Sujet de Master2 Recherche
2021–2022

Détection d'Anomalies et d'Attaques dans l'Internet des Objets Industriels (IIoT)

Lieu	Équipe Réseaux, ICube (UMR CNRS 7357)
Encadrants	Fabrice Theoleyre (theoleyre@unistra.fr)

Mots-clés

Détection d'anomalie ; Attaques ; Internet des Objets Industriels ; Traitement Statistique ; Prédiction

Contexte

L'Internet des Objets Industriels (IIoT) connait actuellement un engouement académique et industriel important. Il s'agit de déployer des équipements autonomes, capables d'envoyer et recevoir de l'information grâce à une interface radio [1]. L'environnement industriel est complexe, bruité, et présente des caractéristiques temporelles pouvant évoluer. Il est donc nécessaire d'exploiter une suite de protocoles robustes, capables de garantir une haute fiabilité [2].

Sujet

Pour garantir une haute fiabilité, l'infrastructure doit pouvoir gérer des liens radio de qualité fluctuante, tout en ordonnançant de façon adéquate les transmissions dans le réseau. Bien souvent, un ordonnancement centralisé est nécessaire : un contrôleur donne les temps de parole à chaque émetteur. Cette collecte centralisée des informations de gestion du réseau représente une opportunité clé pour détecter des anomalies (ex : mauvaise configuration) ou même des attaques (ex : jamming).

- Les objets du réseau doivent remonter à un contrôleur des métriques mesurant la qualité du réseau. Cependant, plusieurs métriques ont montré déjà leurs limites en termes de précision (e.g., RSSI) [3] et/ou de coût d'estimation (e.g., taux de livraison) [4].
- Nous devons également contrôler finement le volume des données à remonter au contrôleur,. En effet, cette information de contrôle consomme des ressources radio et énergétiques importantes. Eventuellement, un sous-échantillonnage des mesures doit être envisagé [5].
- Le contrôleur doit être capable de prédire de l'évolution du réseau, afin de pouvoir discriminer fautes temporaires (ex : variation de la qualité d'un lien radio) et anomalie demandant des contre-mesures (ex : jamming radio, blocage du forwarding).

L'étudiant se focalisera sur une attaque particulière (par exemple jamming radio qui consiste à brouiller une fréquence particulière), et proposera les algorithmes et protocoles permettant de détecter une telle attaque.

Nous souhaitons donc mettre en place une solution de supervision, et explorer les questionnements suivants :

- Quelles sont les données minimales à transmettre pour surveiller efficacement le réseau et détecter une violation ?
- Peut-on prédire les performances futures (minute / heure / jour) avec les performances passées et instantanées afin de pouvoir identifier des comportement déviants (i.e., attaques) ?
- Est-il possible de corréler certaines données (certaines métriques étant mutuellement dépendantes) ?

Compétences attendues

— maitrise des langages de programmation (C & Python) ;
— maitrise des bases en statistiques ;
— maitrise des bases en algorithmie distribuée ;
— un intérêt pour les réseaux sans-fil et l'Internet des Objets.

Déroulement du stage et résultats attendus

Le stagiaire devra réaliser les tâches suivantes :

1. étude d'une pile réseau pour l'IIoT afin de comprendre le contexte ;
2. instrumentation d'un réseau IIoT reposant sur une architecture de type SDN avec un contrôleur ;
3. collecte des données, génération de scénarios de pannes (redémarrage d'un équipement, changement de qualité d'un lien) ;
4. étude des statistiques obtenues, proposition d'algorithmes de prédiction de qualité ;
5. si le temps le permet, test en réel de l'algorithme dans un réseau déployé.

Références

[1] V. C. Gungor and G. P. Hancke. Industrial wireless sensor networks : Challenges, design principles, and technical approaches. IEEE Transactions on Industrial Electronics, 56(10) :4258–4265, Oct 2009.

[2] Maria Rita Palattella, Nicola Accettura, Xavier Vilajosana, Thomas Watteyne, Luigi Alfredo Grieco, Gennaro Boggia, and Mischa Dohler. Standardized Protocol Stack for the Internet of (Important) Things. IEEE Communications Surveys & Tutorials, 15(3) :1389–1406, 2013.

[3] D. Fanucchi, F. Righetti, C. Vallati, B. Staehle, and G. Anastasi. Improving link quality estimation accuracy in 6tisch networks. In 2019 Sixth International Conference on Internet of Things : Systems, Management and Security (IOTSMS), pages 243–250, 2019.

[4] Rodrigo Teles Hermeto, Antoine Gallais, and Fabrice Theoleyre. Experimental in-depth study of the dynamics of an indoor industrial low power lossy network. Ad Hoc Networks, 93 :101914, 2019.

[5] Dingwen Yuan, Salil S. Kanhere, and Matthias Hollick. Instrumenting wireless sensor networks — a survey on the metrics that matter. Pervasive and Mobile Computing, 37 :45 – 62, 2017.