Rapport de PJI 2016

Théo PLOCKYN et Rémy DEBUE

« *Systèmes de Détection d'Intrusion pour l'Internet des Objets*»

Encadré par Gilles Grimaud
Sujet n° 104

Table des matières

Introduction :

Dans le cadre de notre cursus en Master Informatique à Lille 1, nous avons eu l'opportunité de réaliser un projet sur l'ensemble du semestre appelé PJI. Chaque étudiant ou binôme pouvait choisir un sujet sur lequel travailler parmi une liste mais également proposer le sien.

Nous avons choisi de nous intéresser à un sujet proche de l'informatique embarquée, qui est un domaine grandissant à l'aube de l'Internet des Objets. Notre sujet se porte sur la détection de paquets falsifiés dans un réseau 6LoWPAN.

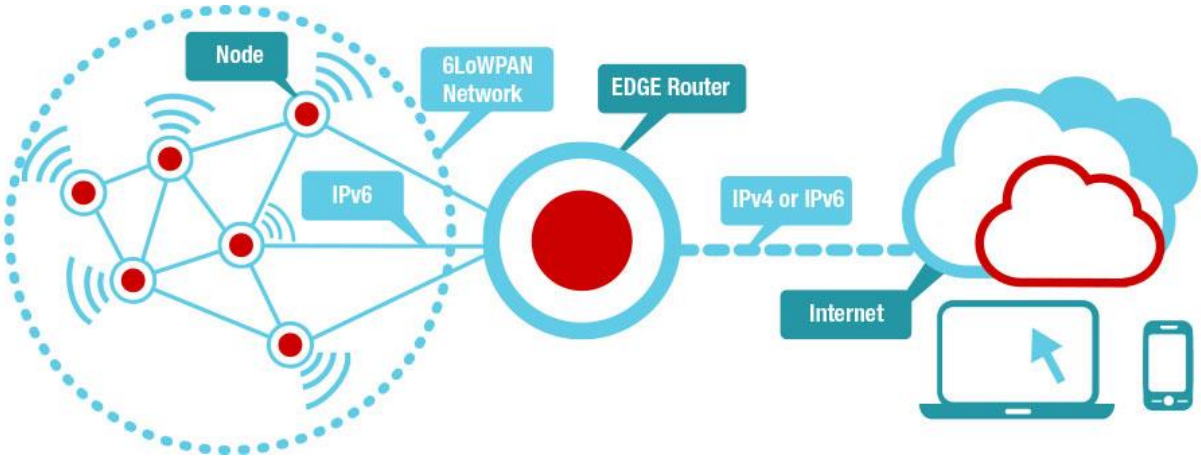

Figure 1 Représentation d'un réseau 6LoWPAN

L'équipe proposant ce sujet est le groupe 2XS « e**X**tra **S**mall e**X**tra **S**afe » composée de notamment « Gilles GRIMAUD » notre encadrant, « Michael HAUSPIE» son associé et bien sûr le reste de l'équipe.

[Peut être bouger cette partie de l'intro et la mettre dans Développement du sujet ? Dans l'intro ne mettre que la présentation de IRCICA, 2XS etc non ?]

1. Contexte du sujet

1.1 Analyse de l'existant

6LoWPAN est l'acronyme de IPv**6 Lo**w Power **W**ireless **P**ersonal **A**rea **N**etwork, autrement dit un réseau sans fil IPV6 dans une zone restreinte. IPv6 ainsi que IPv4 sont majoritairement utilisés pour l'envoi de données. Cependant, leur implémentation dans des systèmes contraints est difficile en raison de la taille des entêtes IP des paquets envoyés.

6LoWPAN permet ainsi, en compressant la taille de l'entête IPv6, de répondre à cette problématique et réussir à intégrer ces systèmes contraints dans un réseau de communication wifi.

De par leurs contraintes, ces réseaux ne sont pas forcément protégés par des systèmes qui peuvent s'avérer coûteux. Cette éventuelle absence peut permettre à des personnes malintentionnées de falsifier des paquets et de s'introduire dans le réseau, typiquement "l'attaque du parking", car l'intrus pourrait accéder au réseau d'une entreprise, d'une usine ou toute autre infrastructure, depuis son ordinateur, dans sa voiture se trouvant dans le parking.

1.2 But de notre projet

Notre sujet est donc de créer un nœud qui écoute et analyse les paquets circulants dans le réseau, à la recherche d'événements suspects et de signaler que le réseau a un problème. Une suite envisageable est de créer un réseau de nœuds vigilants, qui permettrait de positionner la source de cette anomalie.

1.3 Technologies utilisées

Pour mettre en place l'analyse du trafic 6LoWPan et progresser dans notre PJI, nous avons utilisé différents outils :

- Contiki OS (Système d'exploitation Open Source) permettant de gérer l'Internet des Objets (assez léger et flexible)
- Cooja (Simulateur de réseau d'objets sur Contiki OS) qui nous a permis de réaliser les simulations d'exécution.
- Git (Gestionnaire de version d'un logiciel ou programme) qui s'avère être utile pour garder le projet à jour et travailler sur la même version entre les membres du binôme.

1.4 Limites de 6LoWPAN

2. Développement du sujet

2.1 Fonctionnement et déroulement du PJI

- L'initialisation
- Les tests en simulation
- Décomposition des paquets reçus
- Stockage des données
- Interprétation et détection des données anormales

Dans un premier temps, nous avons mis en place une machine virtuelle Linux avec Cooja déjà installé. Le dossier de ce simulateur contient différents exemples de "nœuds" réseaux, nous nous sommes inspirés du code mais aussi d'une partie du projet Github traitant des sniffers. Les nœuds sont sous la forme de fichier en « .c » et une fois compilé on obtient un fichier « .sky » qui pourra être importé dans la simulation.

Une fois que les nœuds sont créés, il suffit de les placer dans la simulation et l'exécuter. Dans la fenêtre d'événement, on peut suivre le bon déroulement du programme et l'échange de messages entre les objets. Diverses options permettent de voir le trafic, la zone de portée des nœuds, leur identifiant ou d'autres informations facilitant la lecture.

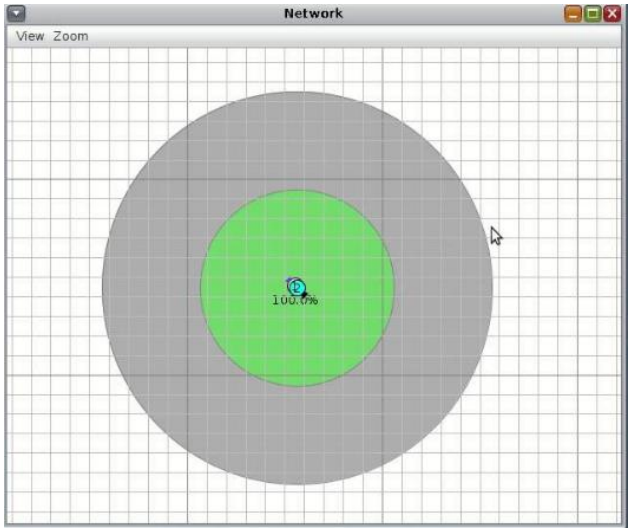

Figure 2 Exemple d'un nœud et de sa portée

L'avantage d'exécuter en simulation est que nous n'avons pas besoin de partager le matériel pour vérifier notre code mais aussi de travailler chacun de son côté quand c'est nécessaire.

Au cours de notre projet, nous étions invités à l'**IRCICA**[1] chaque semaine pour expliquer notre avancement, les problèmes rencontrés et les objectifs suivant à atteindre. De plus, un étudiant de Licence 3 est venu par la suite rejoindre notre projet en développant une autre partie. Nous avons donc également eu des réunions avec ce stagiaire pour lui expliquer le fonctionnement du projet et bien se répartir le travail.

2.2 Réponses à un besoin

- Problèmes de sécurité
- Coût de l'installation de matériels de détection
- Avantages des sondes

La sécurité des systèmes d'information reste un critère d'investissement très élevé dans les entreprises. C'est pourquoi de nombreux moyens sont mis en places (firewall, analyseur de trafic) sont mis en place pour éviter la fuite de données mais aussi le coût de réparation pour revenir à une situation de fonctionnement normal.

Le but de construire ce sniffer 6LoWPAN est donc de répondre notamment aux attaques dites de parking (énoncé dans l'introduction).

L'intérêt d'établir cette sonde sur ce matériel est au niveau de sa portabilité (technologie de l'embarqué). On peut donc installer plusieurs sondes qui vont surveiller une zone précises ou la faire déplacer sans les inconvénients d'une installation plus conséquente. De plus, ce système embarqué est plus faible en consommation énergétique.

Un autre point intéressant de mettre en place un analyseur de données est que la simple lecture des entêtes des paquets suffit à détecter un évènement anormal. Ceci permet d'éviter de lire le contenu des données et donc d'éviter des problèmes légaux sur la sensibilité des données.

[1] IRCICA : **I**nstitut de **R**echerche sur les **C**omposants logiciels et matériels pour l'**I**nformation et la **C**ommunication **A**vancée de Lille

2.3 Exemple d'applications

Bien que notre sujet traite des détections d'intrusion dans un réseau 6LoWPAN, les applications peuvent se diversifiées. En effet on peut changer le support comme des RFID ou Bluetooth, tout en surveillant le trafic avec les sondes.

3. Les limites de l'application

3.2 Le défi de notre projet

Durant notre projet de Master 1, nous avons rencontrés des difficultés nous empêchant d'avancer rapidement. Les premières réunions étaient difficiles à organiser à cause de l'emploi du temps de notre binôme mais aussi de notre encadrant.

Conclusion

Bilan personnel technique

Bilan apporté à l'équipe de recherche

Utilisations futures