Rapport de PJI 2016

Théo PLOCKYN et Rémy DEBUE

« *Détection d'intrusions dans un réseau 6LowPAN* »

Encadré par Gilles Grimaud

Table des matières

Introduction : 3
Travail en cours : 4
Introduction 5
Présentation de 6LowPAN 5
6LowPAN une réponse à une problématique (RFC 4919) 5
But de notre sujet 5
Développement du sujet 5
Technologies utilisées 5
Fonctionnement de notre sujet 5
Réponse à quels besoins 5
Exemples d'applications 5
Conclusion 5
Bilan personnel technique 5
Bilan apporté à l'équipe de recherche 5
Utilisations futures 5
1. Développement du Sujet 6
Technologies utilisées : 6
Fonctionnement de notre sujet : 6
Réponses à un besoin : 6

Introduction :

Nous avons choisi de nous intéresser à un sujet de projet individuel 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.

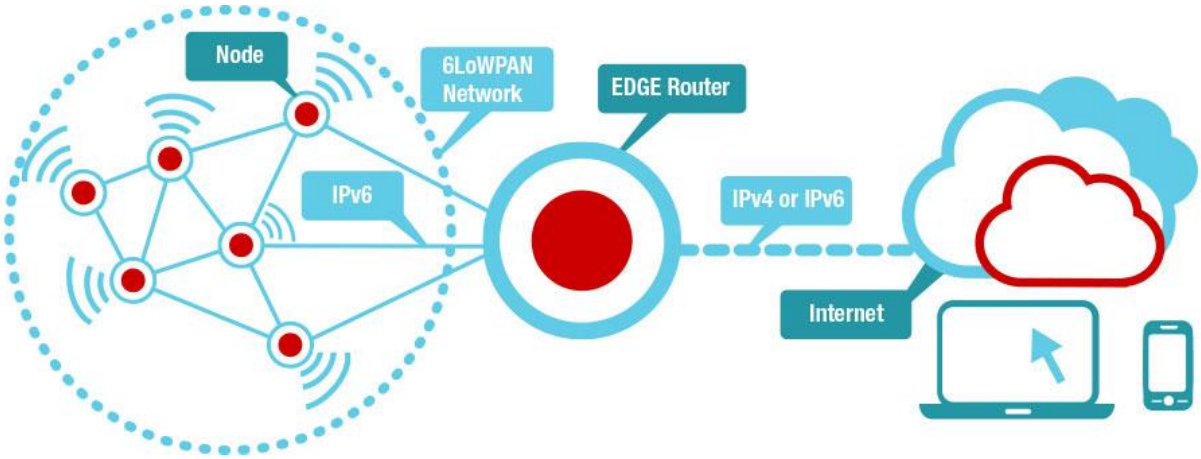

Figure 1 Représentation d'un réseau 6LoWPAN

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.

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.

Pour l'implémentation de ces nœuds, nous nous basons sur Contiki OS, un système d'exploitation embarqué open source, et dans son environnement de développement et de simulation Cooja.

Travail en cours :

Implémentation d'une application sur un nœud collectant les paquets circulant sur le réseau. Pour le moment nous travaillons dans des simulations enregistrant le flux de données dans un fichier spécialisé (en .pcap pour **p**aquets **cap**ture). Par la suite nous pourrons analyser le flux de données collectées à la volée.

Ensuite, une application sur ce nœud produira une table contenant les différentes informations comme la force du réseau, adresses IP, identifiant du réseau provenant des paquets collectés. Cette table sera la base de l'analyse du flux à la volée.

Introduction

Présentation de 6LowPAN

6LowPAN une réponse à une problématique (RFC 4919)

But de notre sujet

Développement du sujet

Technologies utilisées

Fonctionnement de notre sujet

Réponse à quels besoins

Exemples d'applications

Conclusion

Bilan personnel technique

Bilan apporté à l'équipe de recherche

Utilisations futures

1. Développement du Sujet

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.

Fonctionnement de notre sujet :

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. 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.

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.

Réponses à un besoin :

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