

Rapport réunion 27/10

Zoé Lagache

Octobre 2022

1 Présents

Oum-El-Kheir Aktouf, Annabelle Mercier, Zoé Lagache

2 Résumé

La réunion était plus orientée sur la recherche et le choix des outils que j'allais utiliser.

2.1 Outil SMA

Plusieurs outils disponibles (Netlogo, MESA, Jade, SARL, Matkit...). Le choix dépend de si on veut s'orienter plutôt sur de la prévention ou vers de la détection.

Le problème de la prévention dans un réseau de véhicules communicant est que la solution revient souvent à faire de la cryptographie, de la signature électronique et du hashing. Ces solutions n'étant pas le point important de mon projet, nous nous sommes mises d'accord sur le fait que la détection serait sûrement un meilleur choix.

Afin de ne pas tomber dans la création d'un TMS, nous avons aussi convenu que la détection devrait être "légère". J'ai proposé de ne prendre en compte que des "simples" vulnérabilités de routage telles que le "sinkhole" ou le "blackhole". Ainsi, il n'est pas nécessaire de prendre en considération la confiance dans les capteurs ou dans les agents pour la détection. L'intérêt du modèle trouvé est aussi qu'on peut avoir confiance en les agents puisqu'ils ne sont pas en lien direct avec l'extérieur et donc ne seront pas malveillants en soi, ils ne feront que faire apparaître le caractère malveillant d'un capteur ou ensemble de capteurs du monde réel (bien mettre en avant ça dans ma contribution).

2.2 Outil JN

Il n'y a pas vraiment d'outils de simulation de jumeaux numériques étant donné que le concept de jumeaux numérique est assez malléable. Il faudrait trouver un simulateur adapté au cas d'étude que je compte couvrir.

J'ai recherché des datasets ou générateur de datasets de VANETs sans avoir de résultats très concluants. EN outre je me suis rendue compte que si j'utilise un dataset déjà complet, il n'y a alors pas vraiment de Digital Twin. Oum-El-Kheir a fait remarquer que je peux tout de même en utiliser un Dataset pour tester ce que j'aurai pu faire côté SMA. Elle a aussi indiqué qu'elle pourrait avoir une piste pour un dataset venant qu'un workshop qu'elle avait fait.

Les autres possibilités seraient de chercher un simulateur de VANETs ou même un simulateur de trafic routier auquel on ajouterait de la communication. Les besoins identifiés à présent sont la possibilité de sérialiser les données obtenues et la prise en compte des données nécessaires sur les véhicules et RSU pour détecter l'attaque souhaitée (adresse IP ou MAC, adresses des voisins etc...).

2.3 Autre

Nous nous sommes mis d'accord sur la date de la prochaine réunion hebdomadaire : mercredi 2 Novembre à 15h (distanciel).

References