Hes·so

Ingénierie et Architecture

SECV2ICOMM

Haute école d'ingénierie et d'architecture Fribourg HEIA-FR, Bd de Pérolles 80, 1700 Fribourg;

michael.maeder@hefr.ch

RÉSUMÉ DU PROJET

La numérisation progresse à pas de géant dans de nombreux domaines; dans la mobilité des transports, elle accroît la sécurité et permet une utilisation plus efficace des ressources. Ainsi, les véhicules intelligents combinés à des infrastructures intelligentes vont façonner le paysage mondial de la mobilité.

Grâce à divers capteurs et à la communication avec des infrastructures intelligentes (des caméras, des feux de signalisation ou des panneaux, par exemple), ces véhicules intelligents sont en mesure d'agir de manière proactive et donc d'éviter, par exemple, des situations dangereuses

Assurer une communication fiable et sécurisée entre les véhicules intelligents et l'infrastructure intelligente (V2I) est un facteur clé. L'objectif principal de ce projet est donc de créer un concept pour la validation de la communication V2I selon les standards actuels et de confirmer ce concept sur un banc d'essai comprenant une infrastructure de communication V2I [1] (5G et ITS-G5) et un véhicule intelligent disponible à la HEIA-FR.

Perception - Véhicule intelligent

MÉTHODOLOGIE

Le projet s'échelonne en plusieurs étapes :

- **Recherches sur les communications V2I**

Différents protocoles sont définis et analysés en vue de l'utilisation des communications V2I. Il est nécessaire de les connaître pour pouvoir définir clairement le cadre du projet.

- **Concept et mise en place d'un laboratoire**

Pour pouvoir tester les différents systèmes au sein de la HEIA-FR, un laboratoire est conçu et mis en place dans les locaux du centre de compétences ROSAS.

- **Spécification et réalisation d'outils de cyberattaques**

Des outils électroniques et logiciels sont développés pour mettre en pratique les attaques possibles découvertes durant les recherches sur les communications V2I.

- **Audit de sécurité à ROSAS**

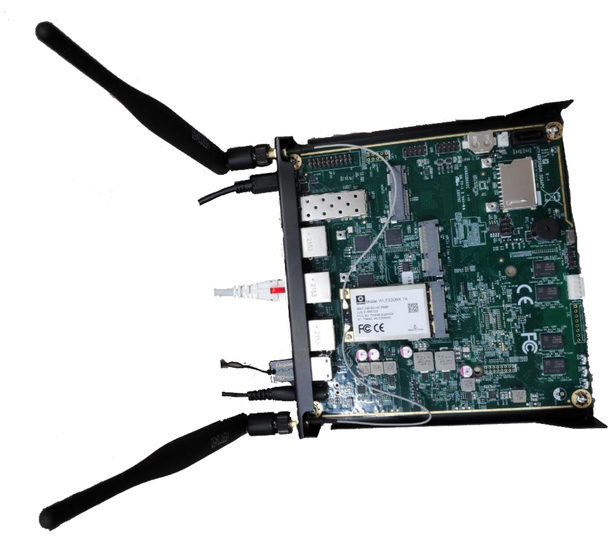
Les véhicules intelligents de ROSAS équipés d'outils de communication V2I sont attaqués afin d'étudier les différents scénarios. Un audit de sécurité est réalisé sur cette base.

RÉSULTATS

Un laboratoire est mis en place pour pouvoir tester et valider la sécurité de différents systèmes de communication entre véhicules intelligents et infrastructures intelligentes. Il est composé d'un feu de signalisation envoyant des messages à un véhicule qui traite les informations automatiquement.

Un dispositif de *hacking* est placé à proximité des antennes des différents systèmes du laboratoire. Il tente de bloquer, d'envoyer de fausses informations ou d'usurper l'identité des différents systèmes intelligents, afin de causer des dysfonctionnements et des dommages potentiels dans l'infrastructure.

Une infrastructure à clé publique est aussi mise en place pour garantir l'intégrité et signer les différents messages envoyés par les infrastructures.



Dispositif permettant la réalisation de cyberattaques sur les véhicules intelligents

CONCLUSIONS

- La sécurité des communications entre véhicules et infrastructures nécessite que les constructeurs de systèmes de communication implémentent correctement tous les aspects liés à la sécurité.
- Ces communications restent dans tous les cas sensibles aux attaques réalisables sur les communications radio, tels que le *Jamming.*
- Un laboratoire est mis en place à ROSAS et des outils sont en développement pour tester la sécurité des différents systèmes.
- Des outils de test permettent de découvrir des failles de sécurité dans les différents systèmes de communication V2I.

RÉFÉRENCES

1 Technologie V2X (https://cutt.ly/GBkoCKt)

2 Security issues and challenges in V2X: A Survey (https://cutt.ly/tBko0ml)

3 C-Roads Report on European Security Mechanism (https://cutt.ly/bBkpyRU)

Haute école d'ingénierie et d'architecture Fribourg
Hochschule für Technik und Architektur Freiburg