Titre du projet: **Securing Vehicle-to-Vehicle (V2V) dynamic energy trading**
Laboratoire, institution : **LIGM / ESIEE-Paris, Université Gustave Eiffel**
Équipe : **LRT**
Partenaire international : **LRSI / UQO, Canada**
Nom et adresse e-mail du tuteur: **Khaled HAMOUID / Email: khaled.hamouid@esiee.fr**
Filière visée (Cybersécurité)

Présentation générale du sujet :

Recently, Electric Vehicles (EVs) industry has become crucial for future transportation systems as it contributes in fuel consumption saving and pollution reduction. However, EVs may have shorter cruising range compared to gasoline vehicles, which necessitates the visit of charging stations very frequently. To cope with the limited EVs driving range, many wireless power transfer technologies have emerged to allow EV charging while driving [1]. This innovation is referred to as EV wireless dynamic charging. In addition to its multiple advantages, such as autonomous charging and reducing range anxiety, dynamic charging can contribute to promoting energy trading as future transportation services. Many dynamic charging strategies are considered like G2V, V2G and V2V, which means that EVs are equipped with bidirectional charger and could, not only buy/receive needed energy from grid/vehicles but also sell/transfer energy back to grid/vehicles. Because it operates in an untrusted environment, the dynamic energy trading process faces various security challenges [2,3] with regard to privacy, mutual authentication and physical security. Furthermore, conventional authentication approaches do not support the mobility of EVs and privacy requirements.

Objectif du projet

The goal of this project is to study the authentication problem raised in V2V energy trading. This includes also a study of authentication approaches that meet the unique features of V2V dynamic charging like EVs mobility, constrained resources and frequent charging. Based on this study we aim in this project to develop a mutual authentication protocol, among the EVs that will exchange energy while driving using dynamic charging technology. This protocol should meet security and efficiency requirements of V2V dynamic charging. In other words, the authentication must be fast, low cost, continuous and with privacy preserving. The security of the protocol should be analyzed formally using AVISPA.

Bibliographie

[1] Golder, Anindita, et al. "Recent Advancements in Vehicle to Vehicle Charging." 2023 IEEE 14th International Conference on Power Electronics and Drive Systems (PEDS). IEEE, 2023.
[2] Babu, Ponnuru Raveendra, et al. "A survey on security challenges and protocols of electric vehicle dynamic charging system." Security and Privacy 5.3 (2022).
[3] Roberts, Braden, et al. "An authentication framework for electric vehicle-to-electric vehicle charging applications." 2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS). IEEE, 2017.