Laboratoire Sécurité des Systèmes Informatique

Rapport de recherche de fin de projet

La vulnérabilité des appareils associés au fréquences radios tous publics.

Réalisé par :

EVEILLARD Thomas, DURAND Samy & MARQUIÉ Médéric

Encadré par :

F. Bryan, M. Arthur, V. Sacha

Travail proposé et réalisé en collaboration avec

Ynov Bordeaux

Année scolaire 2023 / 2024

Table des matières

Introduction.

Notre sujet porte sur la récupération et la réutilisation des informations projetées sur les ondes communes à divers outils utilisés par n'importe qui dans sa vie quotidienne.

Nous avons porté notre attention sur le fonctionnement du déclenchement de l'ouverture des portières de voitures. Typiquement une des utilisations les plus fréquentes dans la vie de tous les jours.

Les ondes radios utilisées par les clés à distance dans ce cadre envoient un signal sur une fréquence précise et très répandue.

Dans ce cadre nous entreprendrons de percevoir la sûreté de ces équipements outillant la vie de n'importe qui. Mais surtout, de savoir si ces méthodes sont à la portée de tout le monde grâce à n'importe quel matériel abordable ou non.

Selon l'INSEE, en 2021, on estime que le parc automobile s'étant à plus de 37,9 millions de véhicules de particuliers. - source

C'est donc un peu plus de la moitié de la population française (en 2021) qui possède un véhicule, en effet nous sommes sur une population de plus de 67,76 millions de français en 2021, encore selon l'INSEE.

"En 2023, 70 649 véhicules ont été volés en France. C'est 11,1 % de plus qu'en 2022 (63 565 vols) et 18,9 % de plus qu'en 2021 (59 440)." - Ouest France.

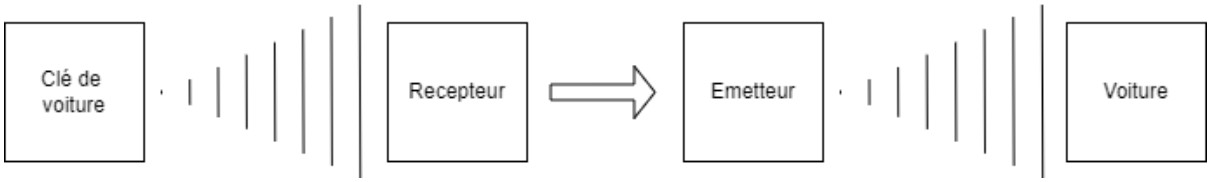
Avec cette augmentation des vols, nous nous sommes donc posé la question suivante : **"Est-ce si facile de voler une voiture ?"**.

Notre regard c'est donc naturellement tourné vers l'exploitation des failles informatiques. De plus en plus de voitures sont régies par l'informatique embarquée et nous savons à quel point il peut être facile d'exploiter une faille en informatique. En effet, le nombre de voitures connectées ne cesse d'augmenter ces dernières années, passant de 3,1 millions en 2017 à 12,8 millions en 2022, sur les routes de France selon

Statista, une multiplication par 4 de la circulation de ces véhicules lourdement informatisés.

Nous nous intéresserons donc à la capture de ce signal et sa reproduction dans un cadre strictement à but éducatif. Grâce à l'utilisation de matériel que nous préciserons plus tard dans notre rapport. Nous allons ainsi capturer, comprendre, puis répliquer le signal reçu afin d'imiter la clé d'une voiture. Permettant ainsi son ouverture ou du moins l'étude du signal reçu.

Voici un schéma logique pour mieux comprendre notre démarche :



I. Un peu de contexte ...

Quelques mots-clés :

- **Rolling-Code - “RC”**
- **Key FOB.**
- **Mégahertz - “Hz”**
- **Emetteur.**
- **Récepteur.**
- **Transcepteur – “Transceiver”**
- **Radiofréquence - “RF”**

A. La sécurisation du signal d'une clé de voiture.

La sécurisation du signal d'ouverture et fermeture d'une voiture est évidemment un élément crucial pour protéger les véhicules contre le piratage et le vol. Les constructeurs automobiles mettent donc en œuvre diverses techniques pour protéger ce signal et garantir la sécurité de la propriété et des propriétaires.

Dans un premier temps, il faut savoir que le signal d'ouverture est généralement encodé à l'aide d'un algorithme. On pourra parler ici du *Rolling-Code*, le plus répandus.

- Le **Rolling-code** :

Il est le plus souvent utilisé dans le verrouillage centralisé pour prévenir le "brute force" par réémission ou émission.

À la différence d'un code fixe, qui n'est pas amené à changer, celui-ci change à chaque fois que vous appuyez sur le bouton de votre clé. L'avantage d'un Rolling-code, ou code tournant, est qu'il amène une sécurité supplémentaire, amenant un changement permanent dans un signal chiffré.

1. Le Rolling-code est une sécurité efficace, il permet de rendre la duplication du signal moins facile et donc sa réplication.

2. Nous avons aussi la mise en place de codes uniques pour différents véhicules bien que de la même marque ou même modèle. Ainsi, on évitera l'ouverture de plusieurs véhicules avec la réémission d'un code capturé.

3. Une authentification mutuelle de la clé et du véhicule est souvent également mise en place évitant une clé similaire d'ouvrir un véhicule semblable.

4. Les technologies anti-relais sur certains systèmes empêchent les pirates d'amplifier le signal de la clé.

5. Le verrouillage passif du véhicule bloquant l'ouverture après un certain d'inactivité même si la clé n'est pas utilisée pour fermer la voiture.

6. Divers autres moyens mis en place par les constructeurs ou des revendeurs permettent aussi de drastiquement baisser les chances de vol de véhicules comme : un coupe-circuit, alarmes, ou un suivi GPS.

B. Les ondes & radios-fréquences.

1. Les utilisations des radiofréquences.

"La fréquence radio est une mesure de la vitesse à laquelle les ondes électromagnétiques oscillent, mesurées en Hertz (Hz)." - source

Les fréquences radios, ou radiofréquences, sont utilisés dans de nombreux domaines pour différentes applications.

Notamment :

- La téléphonie mobile

- La radiodiffusion FM

- La radiodiffusion vers des équipements

- La télédiffusion

- Les téléphones sans fil

- Le réseau Wi-Fi

- Les liaisons sans-fil Bluetooth

Notre vie actuelle est parsemée d'ondes et nous sommes en permanence submergée par celles-ci. Dans certains cas d'étude, cela peut créer des interférences ou "parasites" sur la visualisation de réception des informations. Un problème commun dans les transports aériens demandant par exemple de couper son téléphone en vol.

2. Les Ondes

Nous ne pouvons distinguer les radiofréquences sans les ondes.

Une onde radioélectrique, communément abrégée en onde radio, est une onde électromagnétique dont la fréquence est inférieure à 300 GHz. Si la longueur d'onde dans le vide est supérieure à 1 mètre (fréquences inférieures à 300 MHz) on parle d'ondes « radiofréquences ». Si la longueur d'onde dans le vide est comprise entre 1 millimètre et 1 mètre (fréquences comprises entre 300 MHz et 300 GHz) on parle d'ondes « hyperfréquences ».

Ici, ce sont les ondes situées sur une fréquence précise qui vont nous intéresser.

Les véhicules européens utilisent généralement des émetteurs radio d'une fréquence de 433 MHz ou 434 MHz. Sur les marchés américains ou asiatiques, la fréquence utilisée est de 315 MHz. L'Europe a aussi ouvert la bande 868 MHz.

Les clés de voiture, comme les clés de porte de garage, fonctionnent en 433 MHz. C'est une bande de fréquence qui ne nécessite pas d'autorisation pour émettre moyennant quelques restrictions sur la puissance d'émission ainsi que la durée des signaux plus précisément la fréquence tourne souvent autour de 433,92/94 MHz.

Ici, nous n'étudierons que le cas des voitures européennes dans les fréquences de 433.92 MHz.

C. Les Types de clés.

Pour ouvrir une porte, il faut une clé. Pour qu'un signal soit réceptionné, il faut un émetteur. Nous avons donc inventé les deux en un dans divers types de clés de voitures ci-dessous.

On peut distinguer alors plusieurs types de clés, suivant l'évolution dans le temps :

- **Les clés mécaniques** : ce sont les clés traditionnelles, qui équipent les véhicules depuis leur création, et même encore aujourd'hui pour certains scooters, véhicules sans permis ou autre, souvent distribués en clé de secours dans les véhicules les plus récents.

- **Les clés équipées d'un système d'anti-démarrage :** dans cette catégorie, on distingue une multitude de systèmes différents, développés par chaque fabricant depuis la fin des années 90. Ces clés sont munies de transpondeurs, sans lesquels il n'est pas possible de démarrer le véhicule. Les transpondeurs peuvent être de formes différentes (sous protection en carbone, sous une capsule en verre, ou directement soudé sur une carte électronique). Ils se sont également complexifiés au fil du temps afin de rendre toujours plus difficile le vol de véhicules.

- **Les smart keys ou clés keyless go : c**es clés sont encore plus complexes que les précédentes, car elles possèdent une double technologie :

  - Une fonction "main-libres". Ceci signifie que le démarrage s'effectue par un simple bouton "Start & Stop", en gardant la clé dans la poche ou le sac.

  - Le système d'entrée et de départ passifs *HELLA* est une évolution de la radiocommande avec déclenchement actif des fonctions de confort au moyen de boutons. Il suffit d'avoir la clé sur soi, par exemple dans la poche de son pantalon. Si le propriétaire de la voiture s'en approche à une distance d'environ deux mètres, un émetteur d'identification (une clé radio complétée du spectre de fonctions passives) autorise l'ouverture du véhicule par la poignée de porte. Un contrôle préalable vérifie que l'émetteur détient effectivement une autorisation d'accès. Le système de verrouillage fonctionne également de manière passive, via une surface de détection sur la poignée de la porte (module électronique de la poignée de la porte). L'émetteur communique de manière bidirectionnelle par radio avec l'unité de commande du système de confort et permet de nombreuses autres fonctions. Par exemple, différents paramètres peuvent être enregistrés dans chaque clé individuelle attribuée à une personne, comme la position du volant, la hauteur du siège ou la position du siège. La fonction de mémoire peut également être étendue à d'autres paramètres individuels du véhicule. Le démarrage du moteur s'effectue par un bouton de démarrage, l'émetteur d'identification devant être situé à l'intérieur du véhicule. Bien entendu, la

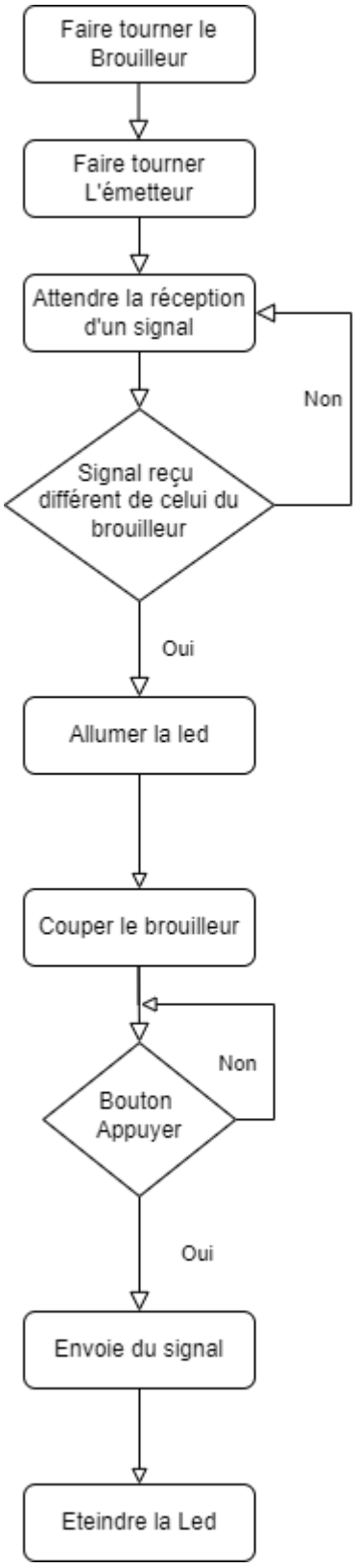
radiocommande (émetteur ID) est également équipée de boutons correspondants pour la commande active du verrouillage des portes ou du hayon ou, selon le constructeur du véhicule, même pour le démarrage du moteur.

- **Les clés infrarouges ou à déblocage d'anti-démarrage par la centralisation :** très peu de véhicules en sont équipés. Le système infrarouge est utilisé chez Renault et Mercedes principalement, notamment au début des années 2000. Le système de déblocage d'anti-démarrage par la centralisation concerne principalement les véhicules Smart jusqu'à 2006.

- **Pour le système d'entrée sans clé**, il résout plein de problèmes grâce à différents avantages : il existe plusieurs types de méthodes d'authentification. Dans le cas d'une communication bidirectionnelle, il existe la preuve à connaissance nulle et le défi-réponse. Dans le défi-réponse, tout d'abord, l'émetteur envoie une demande d'authentification. Après réception, le récepteur renvoie une séquence de nombres aléatoires. Cela s'appelle un défi. L'émetteur reçoit le défi et le combine avec le mot de passe et le défi. Cela s'appelle une réponse. L'émetteur envoie la réponse. De la même manière, le récepteur répond. Il reçoit le défi de l'émetteur et le vérifie. Là "Zero-knowledge proof" ou "Preuve à divulgation nulle de connaissance" est une méthode de vérification du reste du quotient. Le récepteur envoie le diviseur à l'émetteur. L'émetteur divise par le mot de passe diviseur reçu. L'émetteur calcule le reste et l'envoie au récepteur. De la même manière, le récepteur calcule le reste. Il reçoit le reste de l'émetteur et vérifie. L'émetteur et le récepteur répètent ces étapes plusieurs fois. - source

II … Pour une mise en place …

Afin de mieux comprendre notre démarche, nous avons créé ce schéma fonctionnel :



A. Arduino ou Raspberry ?

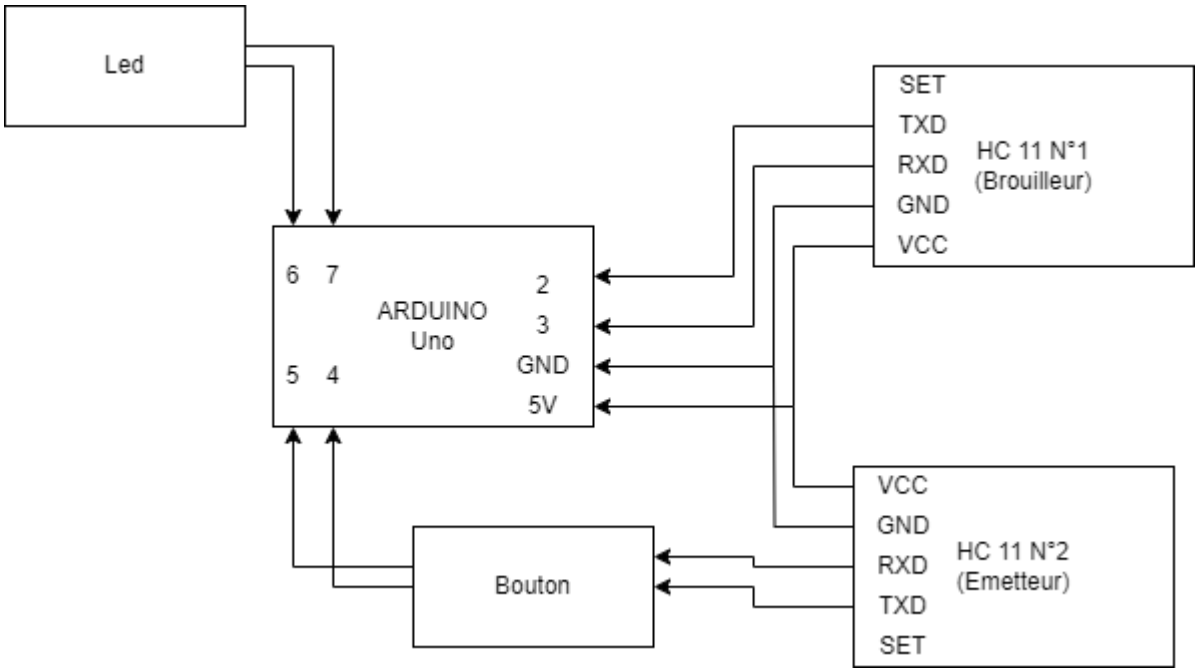
Nous utilisons une Arduino puisque les ressources à disposition tendent plus vers celle-ci. Bien que notre matériel et notre code s'adaptent aux deux. Il n'y a pas de mauvais choix pour ici.

Notre code Arduino :

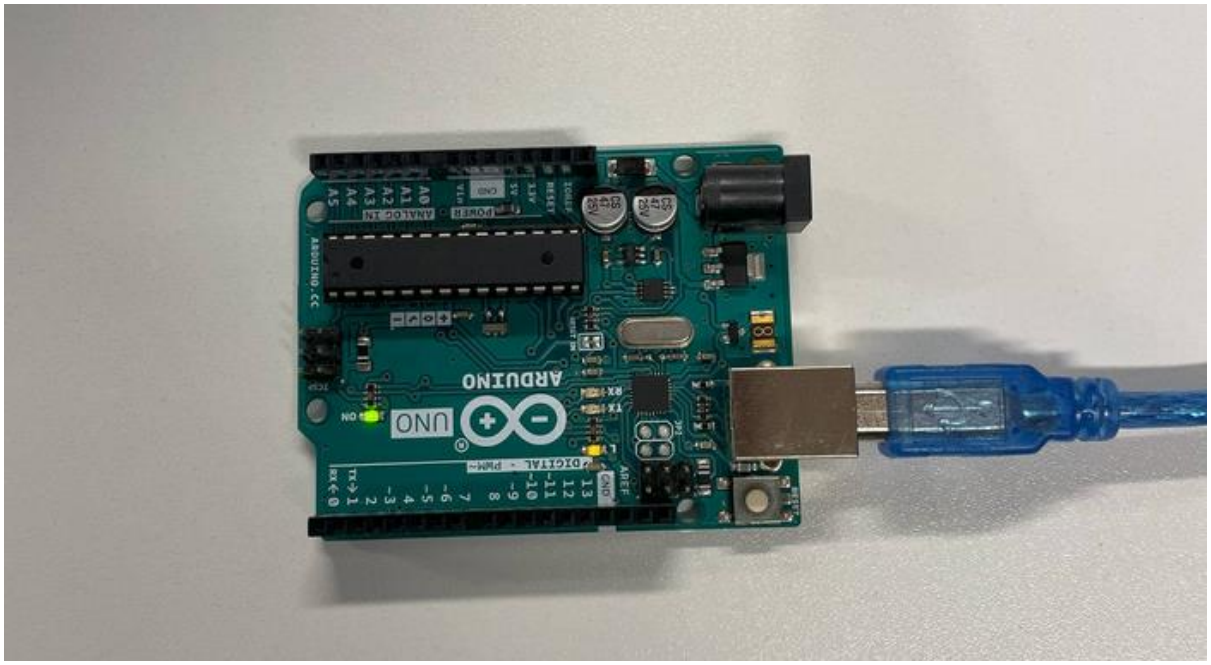
```
#include <SoftwareSerial.h>

SoftwareSerial mySerial(2, 3); // TX, RX

const int buttonPin = 2;
const int ledPin = 13;

int buttonState = 0;

void setup() {
  Serial.begin(9600);
  mySerial.begin(9600);
  pinMode(ledPin, OUTPUT);
  pinMode(buttonPin, INPUT);
}

void loop() {
  buttonState = digitalRead(buttonPin);
  if (mySerial.available() & mySerial.read() ==
"################################") {
    brouilleur(0)
  }
  else if (mySerial.available() & mySerial.read() !=
"################################") {
    brouilleur(1)
    digitalWrite(ledPin, HIGH);
    if (buttonState == HIGH) {
      digitalWrite(ledPin, LOW);
      mySerial.println(mySerial.read())
    }
  }
}


void brouilleur(on int) {
  if (in == 0) {
  mySerial.println("################################");
  }
}
```

B. Matériel employé.

Voici un premier schéma de montage :



Nous nous sommes portés vers l'utilisation de deux cartes Arduino UNO comme celle ci-dessous :

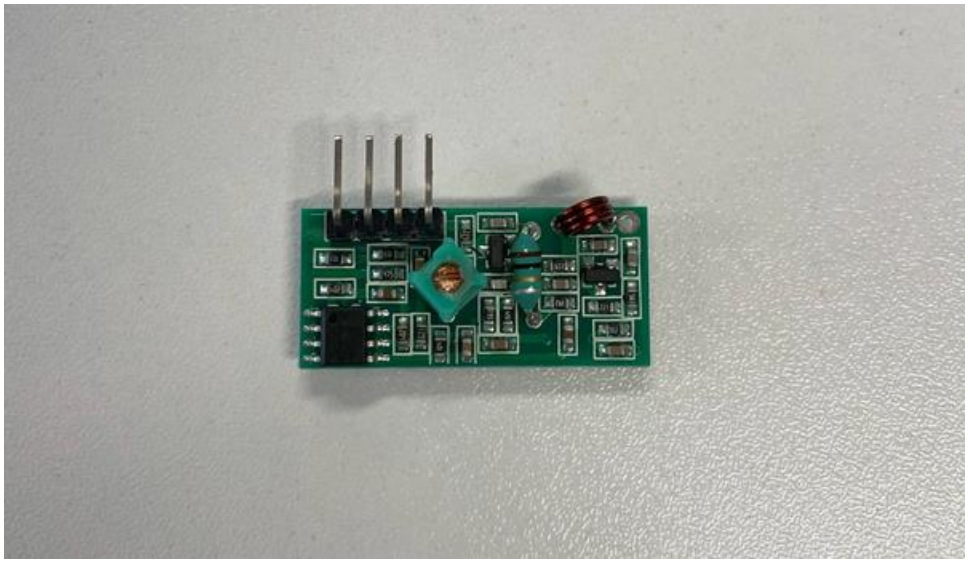


Nous avons également utilisé dans un premier temps un récepteur :

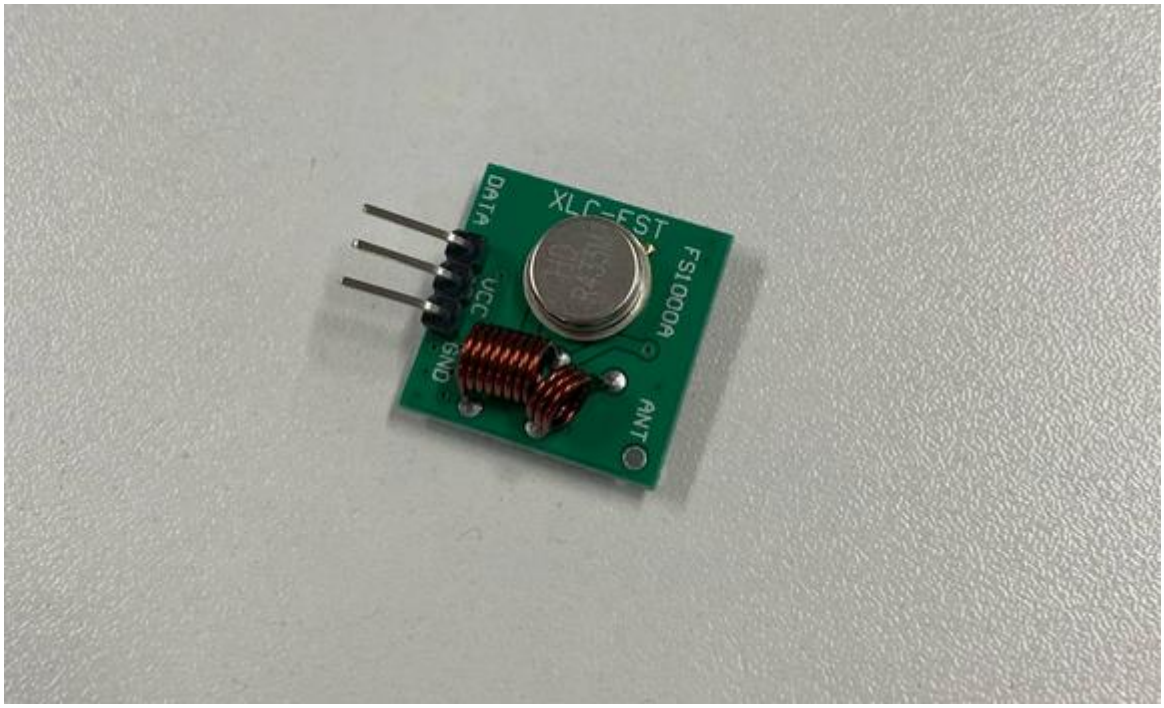
Un ***émetteur-récepteur*** est un équipement électronique combinant un récepteur et un émetteur qui partagent des circuits communs. Les anglophones disent « transceiver », contraction de « TRANSmitter » (« émetteur ») et de « reCEIVER » (« récepteur »). Ce mot est parfois francisé en « transcepteur ». Il est utilisé dans plusieurs contextes.

Nous avons utilisé cette référence :

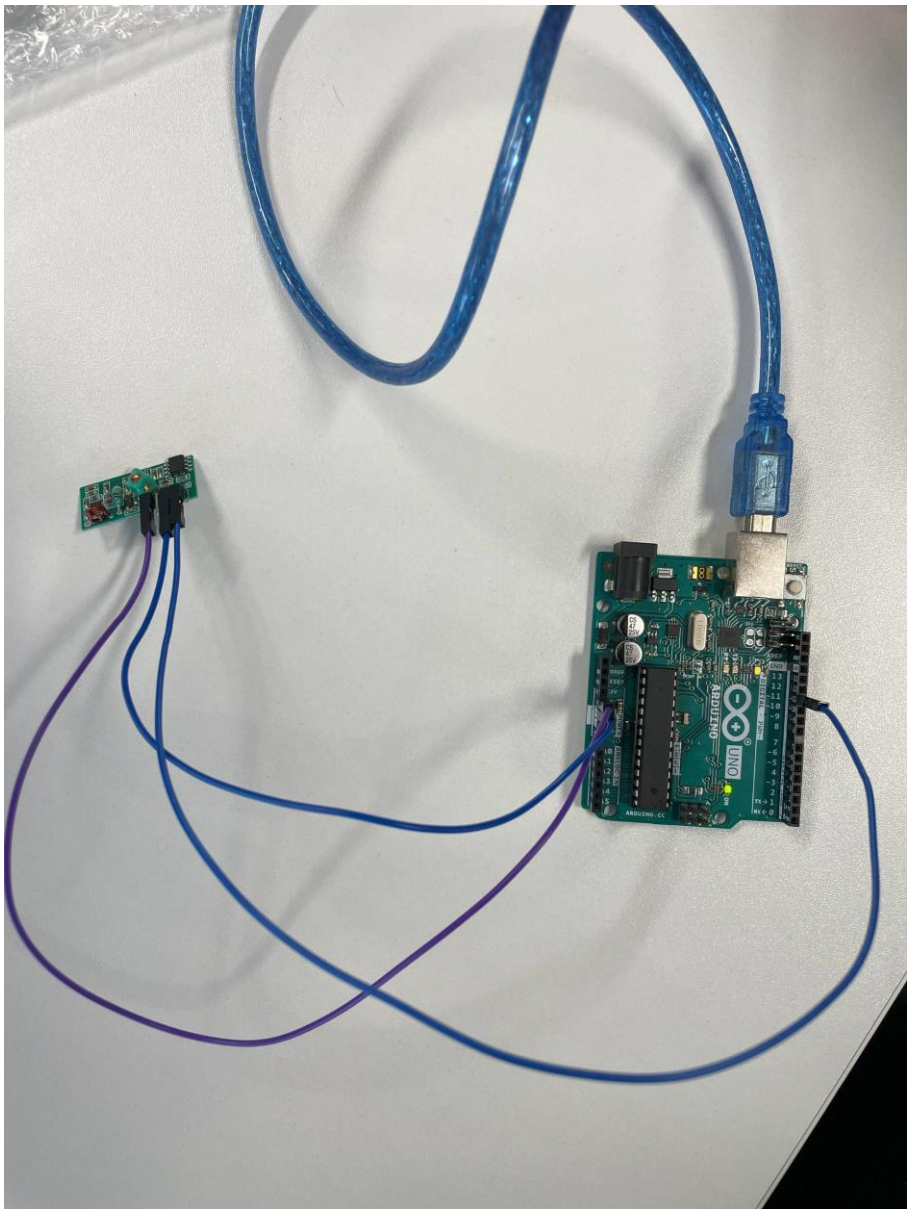
- émetteur-récepteur 433 MHz Kit Émetteur Récepteur 433MHz DC5V Module RF Haute Fréquence PCB.



Également un émetteur :



Voici un exemple de notre premier montage :



Cependant après plusieurs séances sans avoir de résultats, nous avons déterminé que nous avions un problème de matériel.

Nous avons donc fait des tests avec un oscilloscope et un multimètre sur notre émetteur et notre récepteur, pour finir nous nous sommes rendu compte que notre récepteur présentait de gros problèmes :

Il ne recevait pas notre signal que l'on envoyait à partir de notre émetteur, mais il recevait beaucoup, beaucoup, de parasites donc : il était s**urchargé.**

Le problème ne venait donc pas du code en lui-même, mais bien du **composant.**

Du côté de notre émetteur, nous avons essayé de faire un petit projet de tour radio pour vérifier en même temps si lui, il n'avait pas de problèmes.

Enfin, depuis notre souci de composants, nous avons décidé d'en acheter de nouveaux différents de ceux précédemment utilisés.

Nous avons acquis des composants "HC-12" :

- Un type de module de communication sans fil qui est utilisé pour la transmission de données à distance. Il est basé sur la technologie de modulation de fréquence (FM) et utilise la bande de fréquence de 433 MHz pour la communication.

C. Logiciels utilisés

Arduino pour la configuration du code téléversé dans notre carte.

Python pour l'étude du code reçu.

Éventuellement d'autres pistes de logiciels à utiliser :

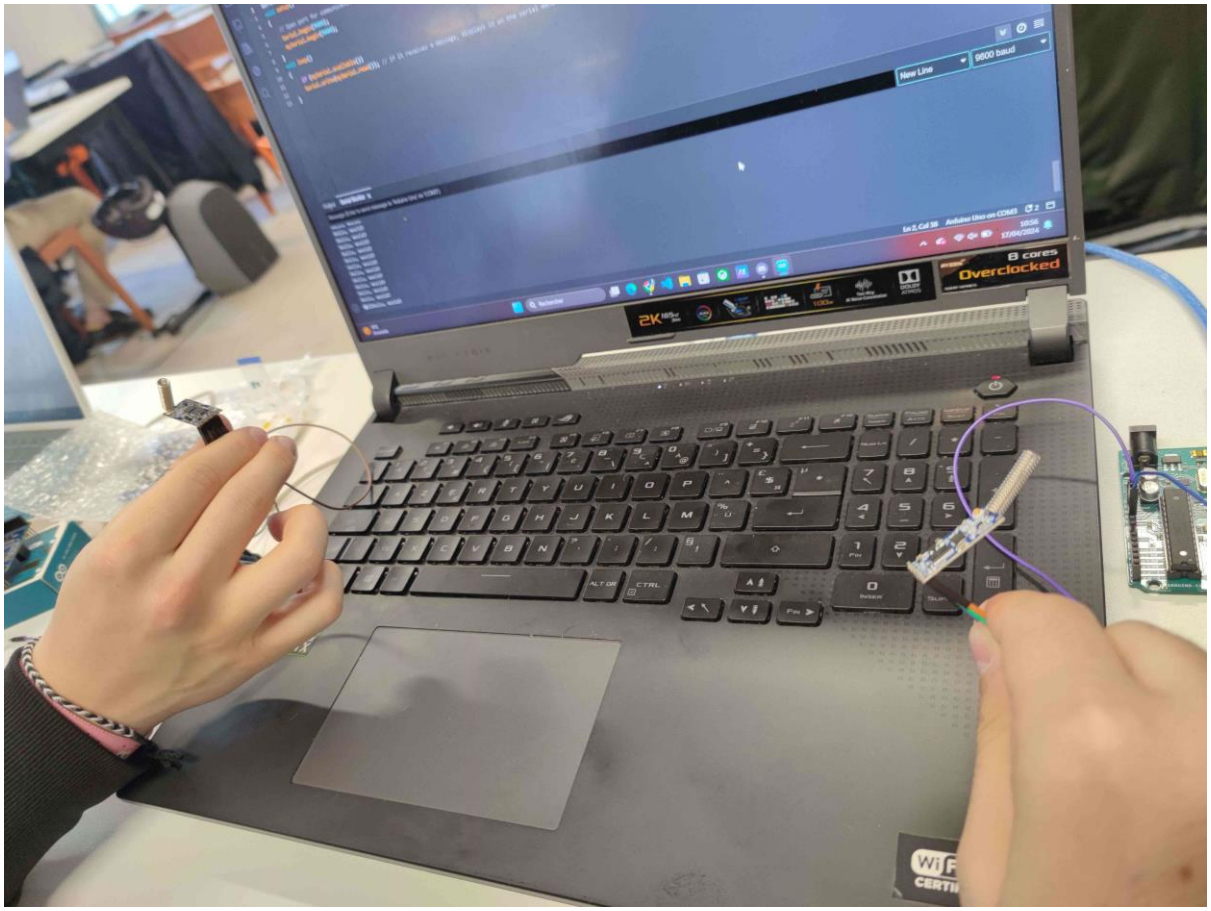
- Gqrx, SDRangel, GNU Radio, HackRF One - Analyse d'ondes.

III ... Des expériences ...

A. Notre montage.

Avec notre nouveau matériel, nous avons réessayés de faire communiquer un HC12 qui va jouer le rôle de récepteur et un HC12 qui va jouer le rôle d'émetteur.

Voici notre montage :



Ici, nous pouvons voir l'émetteur et le récepteur avec leurs antennes respectives.

Nous avons réussi à recevoir ce que l'émetteur envoyait avec notre récepteur : mission réussie.

Maintenant, il faut encore que nous arrivions avec notre récepteur à recevoir d'autres choses comme des signaux radio (Clés de voitures, etc. ...).

IV ... Et des problèmes ...

Nous avons eu quelques soucis lors de la majeure partie de notre projet fil rouge. En effet, ce n'est que tardivement que nous avons compris que notre récepteur recevait énormément de parasites. Empêchant donc tout tests et compréhension de la non-réussite de ceux-ci.

Après l'étude des composants nous avons décidé de changer de matériel et réitéré nos expérimentations.

Les fréquences désirées ne sont malheureusement pas captées par notre montage. Aussi, notre manque de connaissances en électronique et I.O.T ne nous permet pas de résoudre cet imprévu.

Nous avons donc dû apprendre à souder, les différents principes de l'électronique et de l'I.O.T. sur le terrain en expérimentant lors de notre projet, nous avons néanmoins réussi à faire transiter divers messages entre les montages, donc capter et émettre.

V ... Pour s'améliorer ...

Nous avons plusieurs axes d'amélioration envisageable :

- En faire un boîtier compact et ergonomique, avec autonomie énergétique.

- Améliorer notre montage et le matériel utilisé.

- S'adapter au RFID et d'autres modes de communication.

- L'utilisation d'un brouilleur d'onde (interdit en France).

- S'inspirer du Flipper-0 afin d'améliorer l'expérience utilisateur et ses fonctions.

VI ... Et apprendre.

Pour conclure, nous pouvons dire que ce projet nous a permis d'acquérir des compétences en électronique, mais aussi en radiofréquences, soudure, etc. ...

Nous avons beaucoup investigué dans le fonctionnement des verrous d'une voiture, mais aussi des commandes permettant le verrouillage/déverrouillage de celles-ci. Les divers fonctionnements d'algorithmes, les manières d'envoyer les signaux et de les reconnaître. Nous avons eu par la même occasion l'opportunité de travailler sur le challenge RF-Fixed Code de rootme, avec un peu d'aide.

Certes, le projet n'a pas pu aboutir, mais nous avons appréciés apprendre des compétences sortant de notre cadre éducatif.

En conclusion, casser une vitre peut être plus rapide.

Références.

- https://www.instagram.com/reel/C5l_ZNrIHV8/?utm_source=ig_web_copy_link
- Okuda, Kuniyoshi & Shirai, Hideaki. (2014). A Novel Keyless Entry System Using Visible Light Communication. International Journal of Ad hoc, Sensor & Ubiquitous Computing. 5. 10.5121/ijasuc.2014.5501. (Figure 4 - https://www.researchgate.net/figure/the-transmitter_fig5_280929044)
- https://botland.store/content/119-arduino-hc12-Bluetooth
- https://dyrk.org/2019/03/31/radio-frequence-controler-les-garages-les-portails-et-tout-ce-qui-fonctionne-en-433mhz/
- http://anothermaker.xyz/iot/domotique-arduino-nano-raspberry-pi-partie1-rf433mhz-4995
- https://devotics.fr/jouer-avec-du-433mhz-sur-home-assistant/
- https://www.raspberryme.com/telecommande-un-raspberry-pi-avec-emetteur-radio-433mhz/
- https://blog.idleman.fr/raspberry-pi-08-jouer-avec-les-ondes-radio/
- https://www.instructables.com/Decoding-and-sending-433MHz-RF-codes-with-Arduino-/
- https://github.com/lucaercoli/rolling-code-grabber
- https://web.stanford.edu/class/ee26n/Assignments/Assignment5.html