Entrainement ECSC - Hardware

Tristan Claverie

Agence nationale de la sécurité des systèmes d'information

11 Juillet, 2022

1. Introduction

Sommaire

Introduction aux communications RF

Présentation brève de protocoles communs

- Communications sans-fil
- Bluetooth Low Energy
- Wi-Fi

Non abordés

- NFC
- Ultrason (micro/enceintes intégrés)
- Infrarouge (suivant les modèles)
- Réseaux cellulaires

2. Communications sans-fil

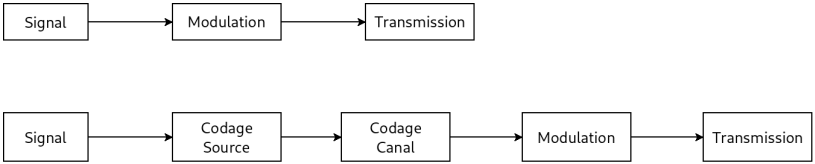
Plusieurs types de communications

- Communications radio
- Communications sonores (*e.g.* ultrason)
- Communications optiques (*e.g.* fibre optique, infrarouge)
- ...

- Beaucoup de concepts communs de traitement du signal / codage de l'information
- Des différences aux niveaux des couches physiques / de l'outillage

Transmission d'information

- Modulation analogique : modulation d'un signal analogique (*e.g.* radio FM)
- Modulation numérique : modulation d'un signal numérique

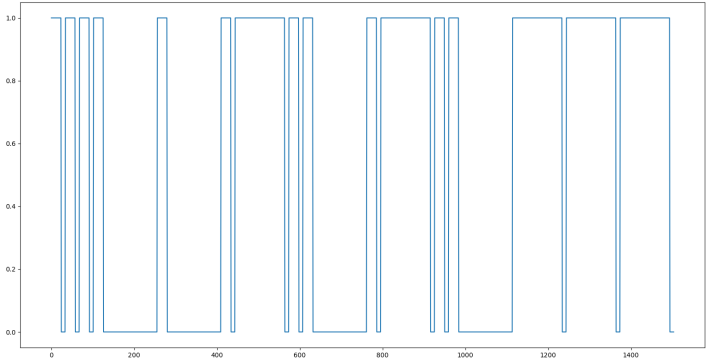


Transmission numérique

- Information à transmettre : texte, image...
- Codage source : ASCII, UTF-8...
- Codage canal : Manchester, NRZ, NRZI...
- Modulation : Amplitude, Fréquence, Phase...

Exemple : Daddy Morse

- Information à transmettre : "HELLO"
- Après codage source : ".... . .-.. .-.. —"
- Après codage canal : "101010 ..."
- Après modulation :



Modulations standards

En CTF :

- Modulation d'amplitude : On-Off keying -> Un symbole est représenté par une amplitude donnée (haut/bas)
- Modulation de fréquence : Frequency Shift Keying -> Un symbole est représenté par une fréquence donnée
- Modulation de phase : Phase Shift Keying -> Un symbol est représenté par une phase donnée

En vrai :

- GFSK (Bluetooth Low Energy)
- GMSK (GSM/GPRS - 2G)
- OFDM (4G, Wi-Fi)

Exemple de challenge

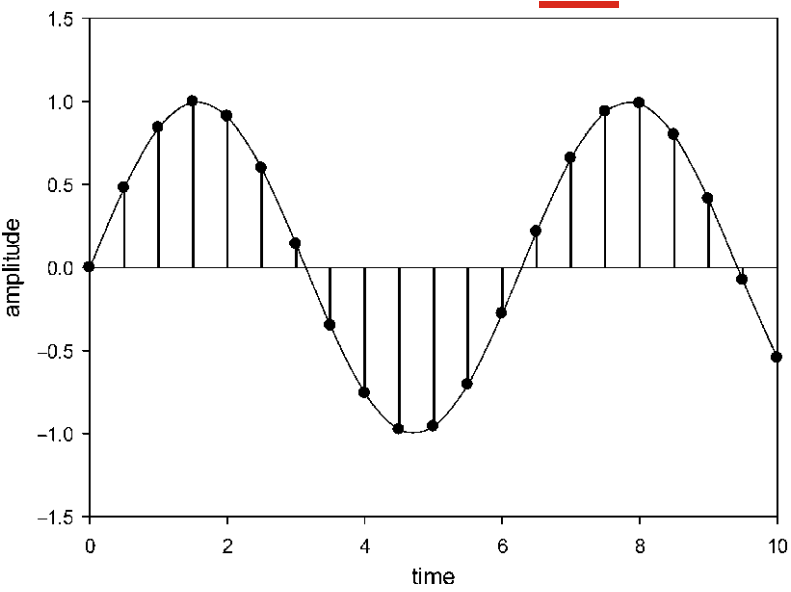
CTF Hardwear.io 2021 :

- 4 LEDs qui clignotent -> trouver le flag
- Certaines LEDs sont allumées en même temps
- => Retrouver l'encodage

Solution :

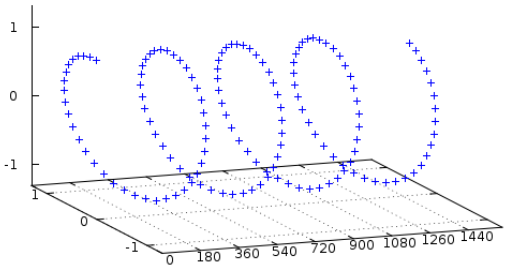
- Chaque LED représente un 0 ou un 1
- A chaque tic, 4 bits sont transmis
- L'encodage est en ASCII, le flag est en clair

Représentation numérique d'un signal radio - signal réel



- Chaque échantillon : amplitude instantanée
- Période : Durée de répétition d'un signal
- Phase : Fragment de la période qui est complété à un instant t
- Fréquence : Nombre de "cycles" par seconde

Représentation numérique d'un signal radio - signal complexe



- Deux échantillons par instant : I et Q ; représentation polaire
- Chaque échantillon : Abscisse et ordonnée
- Amplitude : Longueur du vecteur
- Période : Durée de répétition d'un signal
- Phase : Angle par rapport à x
- Fréquence : Vitesse de rotation sur le cercle
- Fréquence négative : Rotation en sens anti-horaire

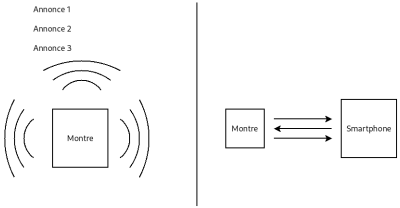
3. Bluetooth Low Energy

Bluetooth Low Energy - Introduction

- Différent du Bluetooth Classique
- Présent dans la norme à partir de la version 4.0
- Utilisé par de nombreux objets connectés (montres, cadenas, appareils médicaux, ...)

Deux modes de fonctionnement

- Annonce (*advertising*) : un équipement envoie des paquets à destination de tout le monde
- Connexion : deux équipements s'échangent des données



Quelques généralités

- Dans la bande des 2.4GHz (comme le Wi-Fi)
- 40 canaux de 2MHz : 3 canaux d'annonces, 37 canaux pour les connexions
- Plusieurs implémentations open source
- Support natif dans les smartphones, ordinateurs
- Connexion à l'équipement : l'équipement qui fait la demande de connexion est le maitre, l'autre est l'esclave de la connexion

Interagir avec un équipement BLE [1]

- L'esclave expose des services, chaque service contient des caractéristiques identifiées par un UUID.

1. **(En gros)**

Interagir avec un équipement BLE [1]

- L'esclave expose des services, chaque service contient des caractéristiques identifiées par un UUID.
- Caractéristique : Un endroit où on peut lire/écrire des données
- Caractéristique (bis) : On peut demander à être notifié des changements de valeurs de caractéristique

1. **(En gros)**

Interagir avec un équipement BLE [1]

- L'esclave expose des services, chaque service contient des caractéristiques identifiées par un UUID.
- Caractéristique : Un endroit où on peut lire/écrire des données
- Caractéristique (bis) : On peut demander à être notifié des changements de valeurs de caractéristique
- Certaines caractéristiques sont standardisées (e.g. Nom de l'équipement)

1. **(En gros)**

Interagir avec un équipement BLE [1]

- L'esclave expose des services, chaque service contient des caractéristiques identifiées par un UUID.
- Caractéristique : Un endroit où on peut lire/écrire des données
- Caractéristique (bis) : On peut demander à être notifié des changements de valeurs de caractéristique
- Certaines caractéristiques sont standardisées (e.g. Nom de l'équipement)
- Toutes les caractéristiques ne permettent pas toutes les opérations, ça dépend de l'implémentation.
- Avec ces trois primitives, on peut implémenter n'importe quoi, pas de règle générale.

1. **(En gros)**

Exemple : Concevoir les interactions BLE d'un équipement

Montre connectée : nom, capteur cardiaque, nombre de pas, mise à jour

- Caractéristique exemple : <role de la caractéristique> (permission)
- Caractéristique 1 : Nom de la montre (R/W)

Exemple : Concevoir les interactions BLE d'un équipement

Montre connectée : nom, capteur cardiaque, nombre de pas, mise à jour

- Caractéristique exemple : <role de la caractéristique> (permission)
- Caractéristique 1 : Nom de la montre (R/W)
- Caractéristique 2 : Capteur cardiaque (N)

Exemple : Concevoir les interactions BLE d'un équipement

Montre connectée : nom, capteur cardiaque, nombre de pas, mise à jour

- Caractéristique exemple : <role de la caractéristique> (permission)
- Caractéristique 1 : Nom de la montre (R/W)
- Caractéristique 2 : Capteur cardiaque (N)
- Caractéristique 3 : Nombre de pas (R)

Exemple : Concevoir les interactions BLE d'un équipement

Montre connectée : nom, capteur cardiaque, nombre de pas, mise à jour

- Caractéristique exemple : <role de la caractéristique> (permission)
- Caractéristique 1 : Nom de la montre (R/W)
- Caractéristique 2 : Capteur cardiaque (N)
- Caractéristique 3 : Nombre de pas (R)
- Caractéristique 4 : Mise à jour (W)

Exemple : Concevoir les interactions BLE d'un équipement

Montre connectée : nom, capteur cardiaque, nombre de pas, mise à jour

- Caractéristique exemple : <role de la caractéristique> (permission)
- Caractéristique 1 : Nom de la montre (R/W)
- Caractéristique 2 : Capteur cardiaque (N)
- Caractéristique 3 : Nombre de pas (R)
- Caractéristique 4 : Mise à jour (W)

Le développeur d'un équipement conçoit les échanges BLE supportés par un équipement (nbs de caractéristique, role, permissions, ...) et les implémente dans des applications mobiles.
=> Pas de vérité générale

Quelques exemples baroques

- Un drone qui expose un FTP over BLE
- Une télécommande connectée qui envoie l'entrée micro sur du BLE
- Un équipement qui réimplémente une session TLS sur du BLE

Outillage

Linux :

- Pile BlueZ et ses outils :
  - bluetoothctl
  - hcitool (déprécié)
  - pyBluez

Android/iOS :

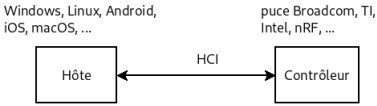
- nRF Connect
- nRF Toolbox
- ...

Demo time

1. nRF Connect
2. Scan Bluetooth
3. Logs HCI Android
4. Wireshark

Logs HCI Android

- Activer mode développeur, puis logs HCI Bluetooth
- Host Controller Interface : communication standardisée entre OS et puce
- Commandes (e.g. scan, connexion), événements, messages échangés en radio
- Peu importe le chiffrement ou non, les logs contiennent les messages en clair



4. Wi-Fi

Wireless Fidelity - Introduction

- Permet de créer un réseau local sans-fil
- Beaucoup de modes de fonctionnement disponibles :
  - Passage par un point d'accès
  - Mode point à point (Wi-Fi Direct)
  - Réseau Mesh (Wi-Fi Mesh)
  - Délégation de l'authentification (Wi-Fi Entreprise)

Quelques généralités

- C'est une couche 1 et 2
- => Certaines attaques couche 2 fonctionnent de la même manière (e.g. ARP poisoning)
- Les échanges entre interlocuteurs se situent sur un seul canal (pas de saut de fréquence)
- Globalement en Europe [a] :
  - 14 canaux sur la bande des 2.4GHz
  - Beaucoup de canaux sur la bande des 5GHz (ça dépend comment on compte)
- $ iw phy

a. **et dans des modes de fonctionnement standard, e.g. box Internet, AP Wi-Fi**

Modes de sécurité

- Echange de clé avec le point d'accès, puis chiffrement
- Plusieurs échanges de clés possibles :
  - WEP
  - WPA/WPA2
  - WPA3
- Plusieurs chiffrements possibles
- Wi-Fi ouverts : toutes les trames passent en clair

Casser un mot de passe Wi-Fi

- WEP : multiples attaques crypto, récupération du mot de passe en observant les paquets
- WPA/WPA2 : brute-force hors ligne à partir d'une capture d'échange de clé
- WPA3 : canal auxiliaire à partir d'un client Wi-Fi compromis, puis attaque par force brute (Dragonblood)

Sniff Wi-Fi

Desactiver les processus qui peuvent utiliser l'interface Wi-Fi (e.g. NetworkManager)

```
ip link set wlan0 down # Eteindre Wi-Fi
iwconfig wlan0 mode monitor # Activer mode Monitor
ip link set wlan0 up # Reactiver interface
wireshark & # Lancer Wireshark, puis lancer capture
iwconfig wlan0 channel <chan> # Changement de canal
```

Demo

- Sniff Wi-Fi (non)
- Analyse point d'accès ouvert
- Déchiffrement de capture
- Probe Requests

Mais aussi

- Slawomir Jasek (BLE, Mifare)
- Damien Cauquil (BLE)
- Internet

Questions

Merci !