الجمهورية الجزائرية الديمقراطية الشعبية

Republique Algerienne Democratique et Populaire

وزارة التعليم العالي والبحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة الشهيد الشيخ العربي التبسي- تبسة

Université Echahid Cheikh Larbi Tébessi– Tébessa

Faculté des Sciences et de la Technologie

Département d'Électronique et de Télécommunications

MEMOIRE

Présenté pour l'obtention du **diplôme** de **Master Académique**

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

Par:

Yassine GHOUL

THEME

Étude et Conception d'un Système de Brouillage Wi-Fi/Bluetooth

Présenté et évalué, le: 11/06/2025, par le jury composé de:

		Grade	Qualité
Dr.	Abdallah.MERAOUMIA	Professeur	Président
Dr.	Hassene. NEZZARI	MCA	Rapporteur
Dr.	Karim.FERROUDJI	MCA	Examinateur

Promotion: 2024/2025

Dédicaces



Yassine

Je dédie ce modeste travail aux personnes chères à mon cœur,

À chère mère,
À celle dont l'amour, la patience et les prières silencieuses m'accompagnent chaque jour.
Merci pour ta tendresse infinie, ton soutien inébranlable et tes sacrifices silencieux.

À la mémoire de mon père,
dont l'absence physique n'a jamais effacé la présence dans mon cœur.

À ma femme,
pour ton amour inconditionnel, ton soutien sans faille et ta patience infinie.

À mes enfants, ***IKRAM, MOHAMED,AMINE,AOUS***
vous êtes ma plus belle source de motivation, mon inspiration de chaque jour.

À mon frère, ma sœur, et à leurs familles,
merci pour votre présence, vos encouragements et l'affection que vous m'avez toujours témoignée.

À toute ma grande famille.

Tous mes amis.

Remerciements

Tout d'abord, je remercie Dieu Tout-Puissant de m'avoir accordé la santé, la volonté, la force, le courage et la patience pour surmonter les moments difficiles et atteindre mes objectifs. Sans cela, ce projet n'aurait pas pu voir le jour.

Je tiens à adresser mes sincères remerciements à tous ceux qui ont contribué directement ou indirectement à la réalisation de ce projet, en particulier :

Mon Encadreur M. Nezzari Hassane pour tous les conseils et outils qu'il a fournis pour faire de ce projet un succès.

A l'enseignant M. Bouabida Seddik qui a continué à superviser la thèse après que l'encadreur soit allé au Hajj

Tous les enseignants du Master 2 Réseaux et Télécommunications

Tous mes collègues de la promotion Master 2, Réseaux et Télécommunications 2024/2025, en particulier Gaidi Ahmed et Hamdi Safi El-Din

Nous adressons également nos sincères remerciements aux membres du jury pour l'intérêt qu'ils ont porté à nos recherches en acceptant d'étudier nos travaux et de les enrichir de leurs suggestions.

Table des Matières

Dédicace…….. **i**

Remerciement…… **ii**

Table des matières…….. **iii**

Liste des figures…….. **vi**

Liste des tableaux……... **viii**

Liste des abréviations…… **ix**

Résumé…… **xii**

Introduction Générale……..…….…….. 01

Chapitre I :LES TECHNOLOGIES SANS FILS

Introduction……...03
I.1 Les Catégories des Réseaux Sans Fils……..…..…..…03
I.1.1 Classification Selon Leur Couverture ..……..…….....…....03
I.1.1.1 WPAN……..……...……...…..…… 03
I.1.1.2 WLAN……..……...…….…… 04
I.1.1.3WMAN……..……...…..…… 04
I.1.1.4 WWAN……..……...……...…… 04
I.1.2 Selon Leur Application au Quotidien……..……...……...…..…04
I.1.2.1 Communication à Courte Portée……...……...…..……04
I.1.2.2 Communication Cellulaire ...……...…..……04
I.1.2.3 Communication Satellite……...…..……...…..……05
I.1.2.4 Autres Technologies sans Fil……...……...……..……05
I.2 Le Wifi (Wireless Fidelity) ……...……...……...…..…… 06
I.2.1 Définition……..…… 06
I.2.2 Les Normes du Wifi……...…..……06
I.2.3 Notion de Canal……...…..….. 07
I.2.4 Fonctionnement du Wifi……...…..……08
I.2.5 Les Modes de Fonctionnement du Wifi……..…08
I.2.5.1 Le Mode Infrastructure……..……...…..…… 08
I.2.5.2 Le Mode "Ad-Hoc"…….....…..…...09
I.2.6 Les Protocoles de Sécurité Wifi et Leurs Fonctionnements……..…..10
I.2.6.1 Le WPA/WPA2 Personal (PSK) ……...……...…..….. 10
I.2.6.2 Le WPA/WPA2 Entreprise……...……...…..…....10
I.2.6.3 Le WPA3……...…..…… ……....10
I.2.6.4 Le 802.1X……...…..……...……..11
I.3 Le Bluetooth ……...…..……12
I.3.1 Définition……...…..…… ……12
I.3.2 La Topologie du Réseau (Architecture) ……..….12
I.3.3 Notion canal……...…..…… ……....14
I.3.4 Les Sauts en Fréquence de Bluetooth……..……....…..14

I.3.5 Les Caractéristiques de la Modulation…….....15
I.3.6 Puissance d'Emission……..……..…..…….... 16
I.3.7 Mécanisme de Transmission par Paquets……..…16
I.3.8 Liens Entre Maître est Esclaves……..…..…..... 18
I.3.9 Mise en Place d'une Association (Liaison) ……20
I.3.10 L'architecture Bluetooth……..…..…… ……...21
I.3.10.1 Spécification de la couche L2CAP……....….22
I.3.10.2 Les couches logicielles……..…..…… …….22

Chapitre II : Techniques de Brouillage dans les Réseaux sans Fils

Introduction……..…..…… ……....23
II.1 Techniques de Brouillage……...……...…..…… ……..23
II.1.1 Types de Brouilleurs……..... 23
II.1.1.1 Brouilleur Proactif……..…..…… ……..…24
II.1.1.2 Brouilleur Réactif……...…..…… ……...25
II.1.1.3 Brouilleurs à Fonction Spécifique……..……...26
II.1.1.4 Brouilleurs Hybrides Intelligents……...……..27
II.2 Placement des Brouilleurs……...…..……29
II.2.1 Attaques par Brouillage Optimales……....….29
II.2.2 Brouillage en Situation d'Incertitude Totale……..…….29
II.2.3 Attaques par Brouillage à Portée Limitée……...30
II.2.4 DSS pour La Localisation des Brouilleurs VHF/UHF……....31
II.2.5 Brouilleur de Taille Nanométrique……...……...31
II.3 Conclusion……..…..…… ……....32

Chapitre III : Système de Brouillage sans Fil Utilisant ESP32 et NRF24L01

Introduction ……..…..…… ……34
III.1 Objectifs du Projet……..…..…… ……..34
III.2ComposantsPrincipaux……..…..…… ……...34
III.3 Description de la Carte ESP32-WROOM-32E……34
III.3.1 Avantages dans ce projet……..…..…… ……..36
III.3.2 Utilisation dans le Projet ……..…..…… …….36
III.3.3 Brochage ESP32 WROOM32E……..…..…...37
III.4Description sur le NRF24……..…..…… ……...37
III.4.1 Caractéristiques du NRF24L01 (avec ou sans antenne)……..……38
III.4.1.1 Fréquence de Transmission (2,4 GHz et plus)……..……...…...38
III.4.1.2 Vitesse de Transmission des Données, par Radio…….……....39
III.4.1.3 Brochage (NRF24L01+ pinout)……..……..…..……..39
III.4.1.4 Alimentation Electrique du Module NRF24L01……..……..……40
III.5 Le Logiciel et le Langage Arduino……..…..……..41
III.5.1 Présentation du Logiciel IDE Arduino……..……...…..…41
III.5.1.1 L'Interface……..…..…… ……42
III.5.1.2 Les Boutons……..…..…… ……...43
III.5.1.3 Présentation du Langage Arduino……..…..…… .44
III.5.2 Programmation de la Carte ESP32 WROOM32 E……..……44

III.5.3 La Librairie Utilisée, pour Piloter le NRF24L01……..……46
III.6 Les Travaux Réalisés……...…..…… ……46
III.6.1 Utilisations un Seul Module nRF24l01…….....46
III.6.1.1 Le Code Utilisé pour Un nRF24L01…….....47
III.6.1.2 Résultats attendus avec un seul module NRF24L01……..47
III.6.2 Ajout d'un deuxième module NRF24L01……..48
III.6.2.1 Objectif ……...…..……49
III.6.2.2 Le Code Utilisé pour Deux NRF24L01……..50
III.6.2.3 Résultats Attendus Avec Deux modules NRF24L01…….50
III.6.2.4 Conclusion……...…..……...……..51
III.6.3 Ajout d'un troisième module NRF24L01……...51
III.6.3.1Objectif ……...…..……..51
III.6.3.2 Le Code Utilisé pour Trois NRF24L01……...…52
III.6.3.3 Résultats Attendus Avec Trois modules NRF24L01……..53
III.6.3.4 Conclusion……...……...…..……..53
III.6.4 Analyse Finale des Tests……...…..…….53
III.6.5 Description du Prototype Final – Brouilleur 2.4 GHz……...…53
III.6.5.1 Composants non Intégrés et Perspectives d'Amélioration……..54
III.6.5.2 Évolution Attendue du Système Avec ces Ajouts……..55
III.7 Le Projet de Point de vue Commercial……... …56
III.7.1 Applications pratiques……...…..……. 56
III.7.2 Avantages du dispositif proposé ……...…..…….56
III.7.3 Estimation des Coûts de Réalisation……...…..56
III.7.4 Perspectives Commerciales……...…..…… …..57
III.8 Conclusion ……...…..……..…….57
Conclusion Générale……..……...……58
Bibliographie……..…..59
Annexe I……..…..61
Annexe II…… …62
Annexe III……... …64
Annexe IV……..……...….. …66

Liste des Figures :

Figure I-1 : La Bande 2,4 GHz……07
Figure I-2 : La Bande 5 GHz ……..08
Figure I-3 : Le Mode Infrastructure ……09
Figure I-4 : Le Mode Ad-Hoc ……09
Figure I.5 : Un Piconet ……13
Figure I-6 : Un Scatternet formé de 3 piconets ……...13
Figure I-7 : Canal Bluetoth ……14
Figure I-8 : Division de la Bande en Plusieurs Canaux ……..14
Figure I-9 : Deux piconets A et B (proche l'un de l'autre) utilisant FHSS ……15
Figure I-10 : Principe de la Transmission FHSS ……16
Figure I-11: Echange de Données entre Maître et Esclave (paquet court 1 time-slot) ……...17
Figure I-12 : Communication avec des Paquets plus longs ……17
Figure I-13 : Un Maître établi une liaison SCO + 2 liaisons ACL ……19
Figure I-14 : Mécanisme de Retransmission de Paquet ……..19
Figure I-15 : Les Différents états d'un équipement Bluetooth ……...20
Figure I-16 : Architecture en couches (Bluetooth) ……21
Figure II-1 : Types de Brouilleurs dans les Réseaux sans Fil ……24
Figure III-1:ESP32 WROOM32 E ……35
Figure III-2: Brochage ESP32 WROOM32 E ……37
Figure III-3 : Brochage du NRF24L01 ……..39
Figure III-4 : Brochage du NRF24L01+PA+LNA ……40
Figure III-5 : Condensateur d'Alimentation ……..41
Figure III-6 : Interface logiciel Arduino ……42
Figure III-7 : Menu Fichier ……43
Figure III-8 : Les Boutons ……..43
Figure III-9 : Préférences ……...44
Figure III-10 : Choix de la Carte ESP32 ……45
Figure III-11 : Installation Bibliothèque ESP32 ……45
Figure III-12 : Installation Bibliothèque RF24 ……..46
Figure III-13 : Schéma Electrique ESP32+Un NRF24L01……47
Figure III-14 : Plaque d'Essai ESP32+Un NRF24L01 ……..47
Figure III-15 : Schéma Electrique ESP32+Deux NRF24L01 ……49
Figure III-16 : Plaque d'Essai ESP32+Deux NRF24L01 ……..50
Figure III-17 : Schéma Electrique ESP32+Trois NRF24L01 ……52
Figure III-18 : Plaque d'Essai ESP32+Trois NRF24L01 ……...52
Figure III-19 : Le Prototype Final ……..55

Liste des Tableaux :

Tableau I-1 : Différents standards 802.11 ……..06
Tableau II-1 : Classification des brouilleurs ……..30
Tableau II-2 *:* Placement des Brouilleurs ……...32
Tableau III-1 : Les Versions du nRF24L01……38
Tableau III-2 : Fréquence de Transmission ……...38
Tableau III-3 : Brochage du NRF24L01 ……40
Tableau III-4 : Estimation des Coûts ……56

Liste des Abréviations

3G: 3ième Génération
4G: 4ième Génération
5G: 5ième Génération
ACL: Asynchronous Connection-oriented logical transport
ACK: Acknowledgement (accusé de réception)
AP: Access Point
CAC: Channel Access Code
CSMA: Carrier Sense Multiple Access
DAC: Device Access Code
DCF: Distributed Coordination Function
DFS: Dynamic Frequency Selection
DHSS: Dynamic Hub Station Selection
DIFS: DCF Inter frame Space
DSS: Decision Support System
EAP: Extensible Authentication Protocol
EAP-TLS: EAP - Transport Layer Security
FEC: Forward Error Correction
FHSS: Frequency Hopping Spread Spectrum
GFSK: Gaussian Frequency Shift Keying
GPRS: General Packet Radio Service
GSM: Global System for Mobile Communications
HDP: Health Device Profile
HDLC: High-Level Data Link Control
Hi-fi: High Fidelity
HIDP: Human Interface Device Profile
HSP: Headset Profile
HSPI: Hardware Serial Peripheral Interface
IAC: Inquiry Access Code
IDE: Integrated Development Environment
IEEE: Institute of Electrical and Electronics Engineers
IoT: Internet of Things (Internet des objets)
ISM: Industrial, Scientific and Medical
L2CAP: Logical Link Control & Adaptation Protocol
LNA: Low Noise Amplifier
LLC: Logical Link Control
MAC: Media Access Control
MIMO: Multiple-Input Multiple-Output
NFC: Near Field Communication
NodeMCU: Micro Controller Unit
NRF: Nordic Semiconductor RF
OBEX: Object Exchange
OPNET: Optimized Network Engineering Tools
OSI: Open Systems Interconnection
PA: Power Amplifier
PCB: Printed Circuit Board
PC: Personal Computer
PEAP: Protected EAP
PHY: Physique
PSK: Pre-Shared Key

PDR: Packet Deliverability Rate
PTK: Pairwise Transient Key
RADIUS: Remote Authentication Dial-In User Service
RF: Radio Frequency
RFID: Radio-Frequency Identification
RFCOMM: Radio Frequency Communication
RTS: Request To Send
SAE: Simultaneous Authentication of Equals
SCO: Synchronous Connection Oriented
SDP: Service Discovery Protocol
SMA: Sub Miniature version A
SMS: Short Message Service
SPI: Serial Peripheral Interface
SSID: Service Set Identifier
TCS: Telephony Control Protocol Specification
UHF: Ultra High Frequency
UMTS: Universal Mobile Telecommunications Service
VHF: Very High Frequency
VSPI: Virtual Serial Peripheral Interface
Wi-Fi: Wireless Fidelity
WiMAX: Worldwide Interoperability for Microwave Access
WLAN: Wireless Local Area Network
WMAN: Wireless Metropolitan Area Network
WPAN: Wireless Personal Area Network
WPA: Wi-Fi Protected Access
WWAN: Wireless Wide Area Network

ملـــخـــص:

يتناول هذا المشروع تصميم وتنفيذ نظام تشويش لاسلكي يستهدف شبكات Wi-Fi و Bluetooth العاملة في نطاق 2.4 غيغاهرتز. تم تطوير نموذج أولي باستخدام لوحة ESP32 WROOM-32E ووحدات NRF24L01 مبرمجة لإرسال إشارات تشويش عبر واجهات SPI متعددة. اعتمد النهج على دراسة نظرية ونمذجة عددية، تلتها تجارب ميدانية لتقييم فعالية التشويش. يُعد هذا النظام حلاً بسيطًا ومنخفض التكلفة مخصصًا لمكافحة الغش داخل قاعات الامتحانات.

الكلمات المفتاحية : Wi-Fi ، Bluetooth، تشويش، ESP32، NRF24L01، 2.4 غيغاهرتز، الأمن، الامتحانات.

Résumé :

Ce mémoire porte sur la conception et la mise en œuvre d'un système de brouillage sans fil ciblant les communications Wi-Fi et Bluetooth dans la bande des 2,4 GHz. Un prototype a été développé à l'aide d'une carte ESP32 WROOM-32E et de modules NRF24L01, configurés pour émettre des signaux perturbateurs via plusieurs interfaces SPI. L'approche adoptée repose sur une étude théorique, une modélisation numérique, puis des tests expérimentaux pour valider l'efficacité du brouillage. Le système, simple et économique, est destiné à prévenir la fraude dans les environnements d'examen.

Mots-clés : Wi-Fi, Bluetooth, brouillage, ESP32, NRF24L01, 2.4 GHz, sécurité, examens.

Abstract:

This thesis focuses on the design and implementation of a wireless jamming system targeting Wi-Fi and Bluetooth communications within the 2.4 GHz band. A prototype was developed using an ESP32 WROOM-32E board and NRF24L01 modules configured to transmit interference signals via multiple SPI interfaces. The approach combined theoretical study, numerical modeling, and experimental validation to assess jamming effectiveness. This simple and low-cost solution is intended to help prevent cheating in exam environments.

Keywords: Wi-Fi, Bluetooth, jamming, ESP32, NRF24L01, 2.4 GHz, security, exams.

Introduction Générale

La technologie radiofréquence (RF) constitue aujourd'hui l'un des fondements essentiels de notre société connectée, permettant des applications aussi diverses que les télécommunications mobiles, les systèmes de navigation, les dispositifs médicaux et les solutions industrielles [1-3]. Fonctionnant sur une gamme de fréquences s'étendant de 3 kHz à 300 GHz, cette technologie offre une transmission sans fil performante pour la voix, les données et divers signaux, avec une efficacité et une rapidité toujours accrues.

Son omniprésence dans les réseaux modernes (4G, 5G, Wifi, RFID, radars) témoigne de sa polyvalence et de son importance stratégique. Les avantages qu'elle présente – couverture étendue, compatibilité avec les appareils mobiles et capacité à supporter des débits élevés – en font un pilier incontournable de la révolution numérique.

Cependant, cette technologie n'est pas sans défis. Les questions de sécurité des données, les interférences électromagnétiques et les préoccupations sanitaires font l'objet de recherches intensives et de débats réglementaires [3-5]. Parmi les solutions développées pour répondre à ces enjeux, le brouillage RF émerge comme une approche à double aspect : outil de protection potentiel, mais aussi menace pour les communications légitimes lorsqu'il est mal employé.

Dans ce contexte, notre projet s'intéresse plus particulièrement à l'application ciblée du brouillage RF pour la lutte préventive contre la fraude académique aux examens [6-8]. Face à l'utilisation croissante de dispositifs sans fil (smartphones, oreillettes Bluetooth) à des fins de triche, nous proposons la conception d'un brouilleur intelligent WiFi/Bluetooth. Ce système innovant se distingue par sa capacité à neutraliser sélectivement les communications dans une zone strictement délimitée (salle d'examen ou amphithéâtre), tout en préservant les connexions adjacentes.

Notre approche combine une gestion fine des fréquences avec une modulation de puissance adaptative, offrant ainsi une solution à la fois efficace contre la fraude et respectueuse des réglementations en vigueur. L'objectif ultime est de fournir un outil fiable, éthique et conforme aux normes, contribuant à préserver l'intégrité académique sans compromettre les libertés numériques environnantes.

Ce travail s'articule autour de trois chapitres complémentaires :

Le premier chapitre est dédié aux fondements théoriques, où on a présenté les types de réseaux sans-fil, avec un focus particulier sur les technologies WiFi et Bluetooth, leur architecture et leurs caractéristiques.

Le deuxième chapitre est consacré aux techniques de brouillage, où une analyse approfondie était réalisée sur les différents types de brouilleurs, ainsi de leurs mécanismes d'action et des stratégies de déploiement optimal.

Le dernier chapitre représente le développement pratique du prototype, incluant la sélection des composants, la programmation, les tests de performance et les améliorations successives. Des exemples concrets illustreront le fonctionnement final du système.

Cette progression méthodologique permettra d'aborder successivement les aspects théoriques, techniques et pratiques du projet, pour aboutir à une solution opérationnelle et efficace contre la fraude aux examens.

Chapitre I :

LES TECHNOLOGIES

SANS FILS

Introduction

Depuis la fin du XIXe siècle, l'humanité a connu une révolution technologique majeure grâce à la découverte des ondes radio, ou ondes RF (radiofréquences). Tout commence avec les travaux pionniers de scientifiques tels que James **Clerk Maxwell**, qui a théorisé l'existence des ondes électromagnétiques, puis Heinrich Hertz, qui en a démontré l'existence expérimentale. Ces découvertes fondamentales ont ouvert la voie à l'utilisation des ondes radio pour la transmission d'informations sans fil [9].

Au début du XXe siècle, **Guglielmo Marconi** réussit à transmettre un signal radio à longue distance, marquant ainsi la naissance de la télécommunication sans fil. Au fil des décennies, les progrès en électronique et en traitement du signal ont permis d'améliorer la qualité, la portée et la sécurité des communications sans fil [10].

Avec l'essor de l'informatique et de l'électronique grand public à la fin du XXe siècle, de nouvelles technologies sont apparues, exploitant les bandes de fréquences RF pour permettre la connectivité entre les appareils. C'est dans ce contexte que sont nés les réseaux sans fil modernes, tels que **le GSM** (Global System for Mobile Communications) pour la téléphonie mobile, **le Wi-Fi** pour l'accès à Internet sans fil, et **le Bluetooth** pour les communications à courte portée entre dispositifs électroniques.

Ces technologies ont profondément transformé notre quotidien, en rendant possibles des échanges d'informations rapides, fiables et omniprésents, sans avoir recours à des connexions filaires. Aujourd'hui, les systèmes sans fil sont au cœur de la communication moderne et continuent d'évoluer avec l'avènement de la 5G, de l'Internet des objets (IoT) et des réseaux intelligents.

1. Les Catégories des Réseaux sans-Fils

Dans le panorama technologique actuel, les technologies sans fil jouent un rôle prépondérant en transformant la manière dont nous interagissons. Cette section se penchera sur les principales catégories de technologies sans fil [11].

1.1 Classification Selon leur Couverture

1.1.1 WPAN

WPAN, acronyme de "Wireless Personal Area Network", se distingue par sa capacité à permettre des communications sans fil entre des dispositifs spécifiques. En d'autres termes, il offre une couverture purement personnelle, s'étendant sur environ 10 mètres.

1.1.2 WLAN

Par rapport au WPAN précédent, la technologie WLAN (Wireless Local Area Network) possède une portée plus étendue et permet principalement la connexion de dispositifs portables tels que des tablettes.

Application au quotidien : réseau Wifi domestique, réseau local au bureau permettant le partage d'imprimantes et de fichiers.

1.1.3 WMAN

Les réseaux WMAN (Wireless Metropolitan Area Network), également appelés "réseaux métropolitains sans fil", sont conçus pour les zones urbaines ou rurales. Ils offrent une interopérabilité avec une couverture et une bande passante remarquables.

1.1.4 WWAN

Les réseaux WWAN (Wireless Wide Area Network), également connus sous le nom de "réseaux étendus sans fil", se distinguent par leur portée la plus vaste parmi tous les types de réseaux sans fil. Les téléphones mobiles sont couramment connectés à des réseaux WWAN, qui peuvent inclure des technologies telles que GSM, GPRS et UMTS.

1.2 Selon Leur Application au Quotidien

1.2.1 Communication à Courte Portée

Les technologies à courte portée ont révolutionné la manière dont nos appareils communiquent entre eux dans un monde de plus en plus connecté, comme le [12]:

• **Wifi** : Le Wifi est une technologie de communication sans fil qui permet aux dispositifs de se connecter à un réseau local et à Internet. Il est utilisé dans les foyers, les entreprises et les lieux publics pour fournir une connectivité haut débit.

• **Bluetooth** : Bluetooth permet la communication sans fil entre des dispositifs à courte distance. Il est fréquemment utilisé pour connecter des écouteurs, des claviers, des souris et d'autres périphériques à des smartphones, des ordinateurs et des tablettes.

• **NFC** (Near Field Communication) : Le NFC permet la communication entre des dispositifs lorsque ceux-ci sont très proches les uns des autres justes à quelques centimètres. Il est utilisé pour des paiements mobiles, le partage de fichiers et l'appariement rapide de dispositifs.

1.2.2 Communication Cellulaire

• **GSM** : C'est un système de communication cellulaire numérique qui a jeté les bases de la révolution des télécommunications mobiles. Il a introduit la possibilité de passer des appels vocaux et d'envoyer des messages texte (SMS) sur des réseaux cellulaires.

• **3G** : La 3G a marqué une étape importante dans les communications mobiles, offrant des vitesses de données plus élevées pour la navigation Web, les appels vidéo et d'autres services.

• **4G** : Le passage à la 4G a apporté des améliorations significatives en termes de vitesse, de latence et de capacité. Elle a permis le streaming vidéo haute définition, les jeux en ligne et d'autres applications.

• **5G** : La 5G représente une avancée majeure, offrant des vitesses ultra-rapides, une latence réduite et une capacité accrue. Elle permettra le développement d'applications telles que la réalité virtuelle, la télémédecine et l'Internet des objets à grande échelle.

1.2.3 Communication Satellite

Les satellites de communication sont positionnés en orbite pour transporter les signaux entre les émetteurs et les récepteurs à travers de longues distances. Ils sont essentiels pour la communication dans les zones éloignées permettant la communication mondiale.

1.2.4 Autres Technologies sans Fil

En plus des technologies de communication sans fil déjà établies, d'autres solutions ont été créées pour répondre à des besoins spécifiques en matière de connectivité. Parmi celles-ci, nous trouvons :

• **Le RFID** (Radio-Frequency Identification) : il permet l'identification et le suivi d'objets àl'aide d'étiquettes radiofréquences. Il est utilisé dans la gestion des stocks, le suivi des actifs et d'autres applications.

• **Le WiMAX** (World wideInter-operability for Microwave Access) : WiMAX offre une connectivité haute débit à longue portée, en concurrence avec d'autres technologies sans fil. Il peut être utilisé pour fournir un accès Internet à des zones rurales.

• **Les Réseaux Mesh** : utilisent plusieurs nœuds interconnectés pour données sur de longues distances. Ils sont utilisés dans les environnements relier les où une couverture étendue et une redondance sont nécessaires, comme les villes intelligentes et les grands espaces [13].

Nous allons explorer plus en détail les caractéristiques et les fonctionnalités spécifiques des technologies sans fil, en mettant l'accent sur les aspects liés au Wifi et Bluetooth.

2 Le Wifi (Wireless Fidelity)

2.1 Définition:

D'après le dictionnaire Larousse, le Wifi est un « Réseau local hertzien (sans fil) à haut débit destiné aux liaisons d'équipements informatiques dans un cadre domestique ou professionnel ».

2.2 Les Normes du Wifi

Depuis l'introduction du premier standard Wi-Fi en 1986, les normes de la famille 802.11 n'ont cessé d'évoluer afin d'intégrer les avancées technologiques. Ces évolutions ont permis une amélioration constante des performances, notamment en termes de débit.

Le tableau ci-dessous présente les principales caractéristiques des différents standards 802.11.

Normes	Date du standard	Fréquence	Largeur bande	Débit max par flux Mb:s	Nombre de flux MIMO*	Portée moyenne (m)	
		GHz	MHz			Int.	Ext.
802.11a	1999	5	20	54	1	35	120
802.11b	1999	2,4	22	11	1	38	140
802.11g	2003	2,4	20	54	1	38	140
802.11n	2009	2,4 / 5	20	72	4	70 (2,4)	250
			40	150		35 (5)	250
802.11ac	2013	5	20	96	8	35	
			40	200		35	
			80	433		35	
			160	866		35	

Tableau I-1 : Différents Standards 802.11.

MIMO (Multiple-Input Multiple-Output) est une technique de multiplexage qui utilise plusieurs antennes afin d'optimiser le rapport signal/bruit et/ou d'augmenter le débit. Chaque antenne transmet un flux de données distinct. Par exemple, le standard 802.11ac peut gérer jusqu'à 8 flux de 866 Mb/s chacun, permettant ainsi d'atteindre un débit théorique maximal d'environ 7 Gb/s.

Cependant, les débits indiqués dans le tableau sont des valeurs théoriques. En pratique, ces débits ne sont jamais atteints. Des facteurs comme les délais liés à la transmission sans fil et la taille des en-têtes entraînent une réduction significative du débit réel, qui correspond en général à environ la moitié du débit théorique.

Enfin, pour exploiter pleinement les capacités du standard le plus récent, à savoir le **802.11ac**, il est indispensable de mettre en œuvre l'ensemble des fonctionnalités prévues par la norme, y

compris celles qui sont optionnelles, afin d'atteindre les performances maximales annoncées [14].

2.3 Notion de Canal

Lorsqu'on parle des fréquences 2,4 GHz et 5 GHz, il s'agit en réalité de deux bandes de fréquences réparties en plusieurs canaux de 20 MHz. Selon le standard utilisé, ces canaux peuvent être regroupés afin d'augmenter la bande passante, ce qui entraîne une occupation plus large du spectre radioélectrique. Cette extension peut toutefois engendrer des interférences.

Ainsi, dans le cadre du déploiement d'une architecture sans fil, le choix judicieux des canaux est essentiel pour limiter les risques d'interférences. Cela nécessite une analyse préalable de l'environnement radio existant.

La bande 2,4 GHz comporte 13 canaux dont 3 ne se superposent pas et donc ne s'interfèrent pas.

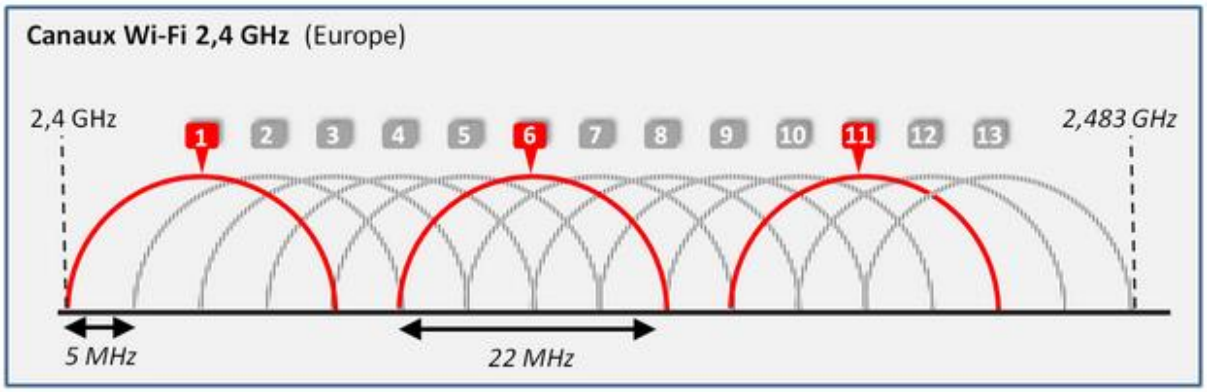


Figure I-1 : La Bande 2,4 GHz

La bande 5 GHz comporte 19 canaux indépendants. En fonction du standard 802.11 utilisé il est possible de regrouper 2 à 8 canaux adjacents pour augmenter la bande passante.

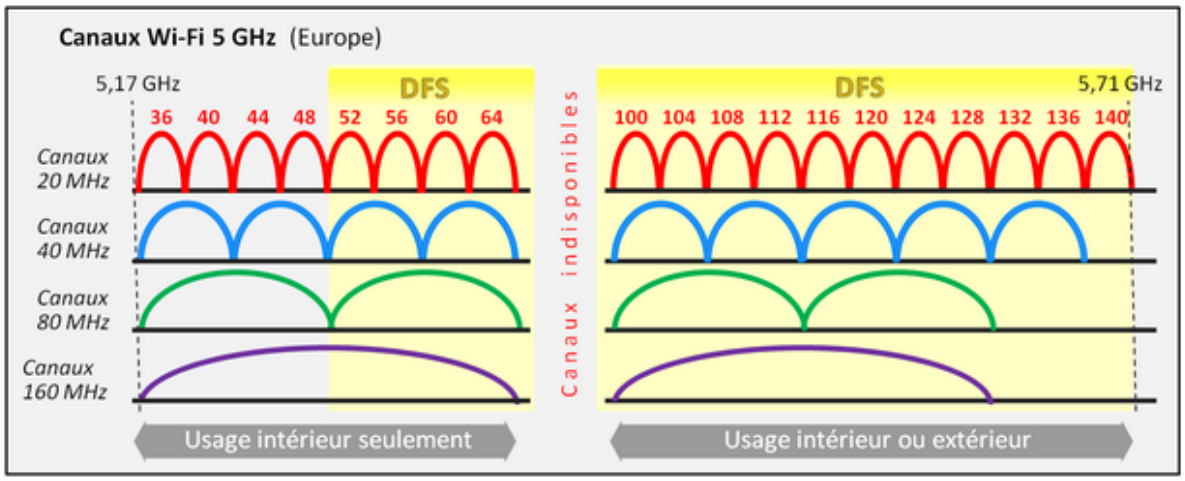


Figure I-2 : La Bande 5 GHz

Ce mécanisme est appelé DFS (Dynamic Frequency Selection) il est obligatoirement implanté sur les équipements WiFi travaillant sur les canaux concernés (fond jaune). Cette contrainte est à prendre en compte car en cas d'activation du DFS la perte temporaire de communication qui s'ensuit peut se révéler néfaste dans le cadre d'une application automatisée.

2.4 Fonctionnement du Wifi

La norme 802.11 forme les bases au niveau des couches inférieures du modèle OSI pour établir une communication sans fil en utilisant des ondes électromagnétiques. Cette norme englobe principalement deux couches clés :

• La couche physique parfois appelée "couche PHY", offre trois méthodes distinctes de codage de l'information : DHSS, FHSS et Infrarouge.

• La couche liaison de données se subdivise en deux sous-couches distinctes :

- Le contrôle de la liaison logique ou LLC en anglais, qui gère les aspects logiques de la connexion entre les appareils.

- Le contrôle d'accès au support ou la couche MAC, qui est responsable de la gestion de l'accès au support de communication partagé entre les différents appareils [15].

2.5 Les Modes de Fonctionnement du Wifi

2.5.1 Le Mode Infrastructure

Le mode Infrastructure facilite la liaison entre les ordinateurs munis de cartes Wifi en les reliant par le biais d'un ou de plusieurs points d'accès ou connu sous son abréviation AP en anglais.

• Les AP agissent de manière semblable à des hubs comme des répéteurs ou des commutateurs dans les réseaux Ethernet.

• La création d'un tel réseau nécessite l'installation périodique d'AP à intervalles réguliers dans la zone à couvrir.

• Les AP doivent être configurés avec un même nom de réseau (SSID, ou Service Set IDentifier) pour permettre la communication.

• L'avantage de ce mode réside dans le fait qu'il impose le passage par l'AP, ce qui permet de vérifier les accès au réseau [15].

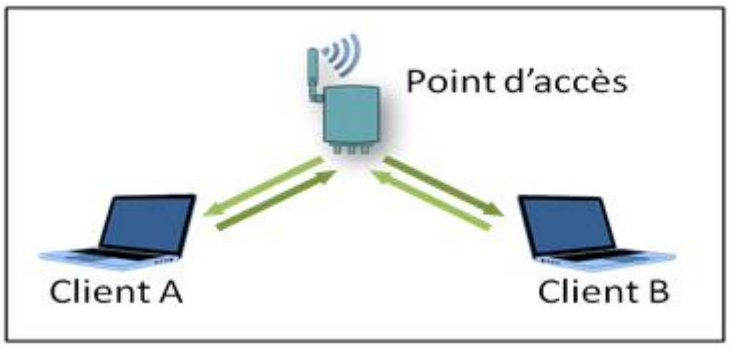


Figure I-3 : Le mode Infrastructure

2.5.2 Le Mode "Ad-Hoc"

Le mode "Ad-Hoc" offre la possibilité de connecter directement des appareils équipés de Wifi sans recourir à des points d'accès intermédiaires.

• La configuration de ce type de réseau implique simplement la mise en place des appareils en mode ad hoc, le choix d'un canal ou la fréquence et d'un nom de réseau(SSID) commun à tous les participants, et si nécessaire, l'utilisation d'une clé de chiffrement.

• L'avantage de ce mode réside dans sa capacité à fonctionner sans nécessiter d'équipements externes tels que des points d'accès [15].



Figure I-4 : Le Mode Ad-Hoc

2.6 Les Protocoles de Sécurité Wifi et Leurs Fonctionnements

Les protocoles de sécurité Wifi sont conçus pour protéger les réseaux sans fil contre les menaces et les accès non autorisés. Voici comment fonctionnent généralement les principaux protocoles de sécurité Wifi :

2.6.1 Le WPA/WPA2 Personal (PSK)

Dans les réseaux Wi-Fi configurés avec une clé pré-partagée (PSK), un ensemble d'étapes est suivi pour permettre l'authentification. Voici ces étapes :

• Lors de la configuration, un mot de passe pré-partagé (Pre-Shared Key, PSK) est défini sur le point d'accès et sur les appareils clients.

• Lorsqu'un appareil souhaite se connecter au réseau Wifi, il envoie le PSK au point d'accès pour l'authentification.

• Le point d'accès vérifie le PSK et génère ensuite une clé de chiffrement temporaire (Pairwise Transient Key, PTK) à utiliser pour chiffrer les données entre cet appareil et le point d'accès.

• Les données sont chiffrées avec le PTK et transmises entre le point d'accès et l'appareil.

2.6.2 Le WPA/WPA2 Entreprise

Des mesures supplémentaires de sécurité sont mises en place pour garantir l'intégrité des communications.

• Un serveur d'authentification RADIUS (Remote Authentication Dial-In User Service) est mis en place. Ce serveur gère les informations d'authentification et les clés de chiffrement individuelles pour chaque appareil client.

• Lorsqu'un appareil tente de se connecter, il envoie ses informations d'identification (par exemple, un nom d'utilisateur et un mot de passe) au serveur RADIUS via le point d'accès.

• Le serveur RADIUS vérifie les informations d'identification et génère une clé de chiffrement temporaire (Pairwise Transient Key, PTK) spécifique à cet appareil.

• Les données sont chiffrées avec le PTK et échangées entre le point d'accès et l'appareil.

2.6.3 Le WPA3

Le WPA3 utilise "Simultaneous Authentication of Equals" (SAE), un protocole basé sur des échanges cryptographiques Diffie-Hellman, pour renforcer la sécurité de l'authentification.

Voici le protocole de fonctionnement du WPA3 :

• Lorsqu'un appareil tente de se connecter, il échange des messages avec le point d'accès pour prouver qu'ils partagent un secret commun (mot de passe).

• Le protocole SAE empêche les attaques par force brute en rendant difficile la tentative de deviner le mot de passe.

2.6.4 Le 802.1X

Le 802.1X est utilisé en conjonction avec des protocoles d'authentification EAP ou "Extensible Authentication Protocol", tels que EAP-TLS (Transport Layer Security) ou PEAP (Protected EAP). Voici comment il fonctionne :

• Lorsqu'un appareil tente de se connecter, il envoie ses informations d'identification au point d'accès.

• Le point d'accès transmet ces informations au serveur RADIUS.

• Le serveur RADIUS vérifie les informations d'identification et génère une clé de chiffrement spécifique à cet appareil.

• Une fois l'authentification réussie, les données sont chiffrées avec la clé de chiffrement et échangées entre le point d'accès et l'appareil [16].

3 Le Bluetooth

3.1 Définition

Le Bluetooth est une technologie sans fil permettant la communication sur de courtes distances. Il a été constitué au départ par Ericsson, IBM, Intel, Nokia et Toshiba. La première norme de communication été approuvée en 2002 sous le numéro IEEE 802.15.1. La bande de fréquence choisie pour cette communication est la bande ISM des 2.4 GHz. Elle permet un débit de 1 Mbits/s (v1), (3 Mbits/s v2.1EDR), (24 Mb/s v3 HS), (v4 LE).

Le réseau doit pouvoir travailler en parallèle (même fréquence, même lieu ou espace) d'un réseau IEEE 802.11 (WiFi). Il peut y avoir des interférences mutuelles.

Les applications du Bluetooth ne sont limitées que par l'imagination :

- Liaisons sans fil entre PC, clavier, joystick, imprimante
- Mise à jour des assistants personnels
- Transfert de fichiers d'un appareil photo numérique ou d'un caméscope vers un PC
- Accès à internet à travers un téléphone portable
- Liaison « main libre » entre un téléphone portable et autoradio ou une oreillette
- Contrôle à distance de l'autoradio, de la chaîne Hi-fi, du chauffage, d'un distributeur de boisson … via un téléphone
- Messages d'avertissement en cas de panne d'un appareil domestique
- Ajout d'intelligence dans les appareils domestiques

3.2 La Topologie du Réseau (Architecture)

Le Bluetooth est un réseau de type « Ad-Hoc » c'est-à-dire sans station de base. Il est auto-configurable : deux machines se retrouvant proche l'une de l'autre peuvent se reconnaître puis échanger des données.

L'ensemble des appareils reliés définit un petit espace de communication appelé « Piconet » (pico réseau en français).

Un réseau Piconet est formé de 8 appareils au maximum (adresse codée sur 3bits).

L'appareil qui initie l'échange joue le rôle de maître, tandis que le ou les autres (**7** maximum Actifs) sont dits esclaves (255 en mode Parcked ou inactif) [17].

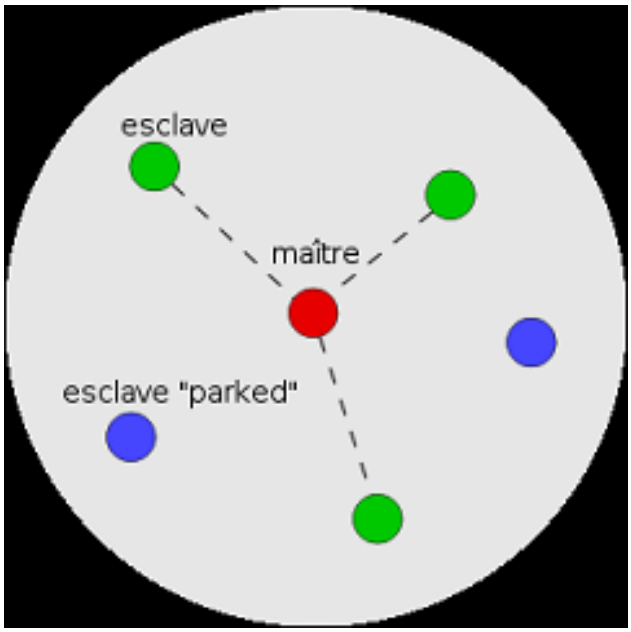


Figure I.5 : Un piconet

C'est le maître qui impose son horloge aux esclaves (synchronisation) et défini les fréquences de travail (saut de fréquence).

Les appareils qui ne sont pas actifs sont en mode « Standby » ou « Parck ».

Pour avoir plus d'équipements interconnectés, les piconets peuvent être connectés afin de former un réseau de diffusion ou scatternet (10 piconets au maximum) [17].

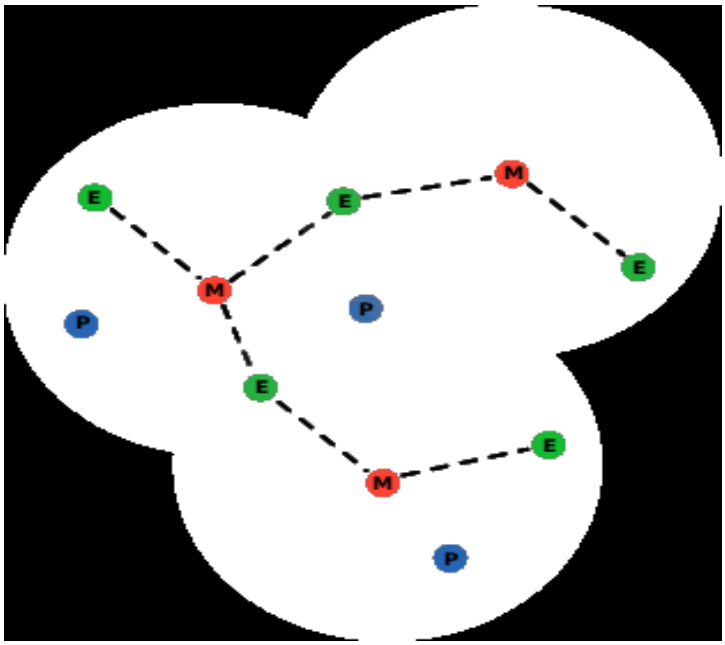


Figure I-6 : Un Scatternet formé de 3 piconets

3.3 Notion de Canal

Le Bluetooth utilise donc la bande allant de 2.4 GHz à 2.4835 GHz, elle est divisée en**79** canaux de **1 MHz** chacun.

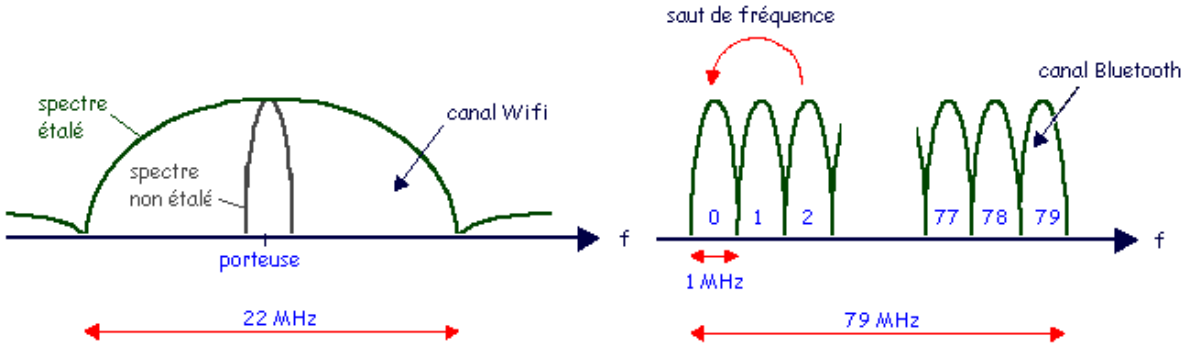


Figure I-7 : Canal Bluetooth

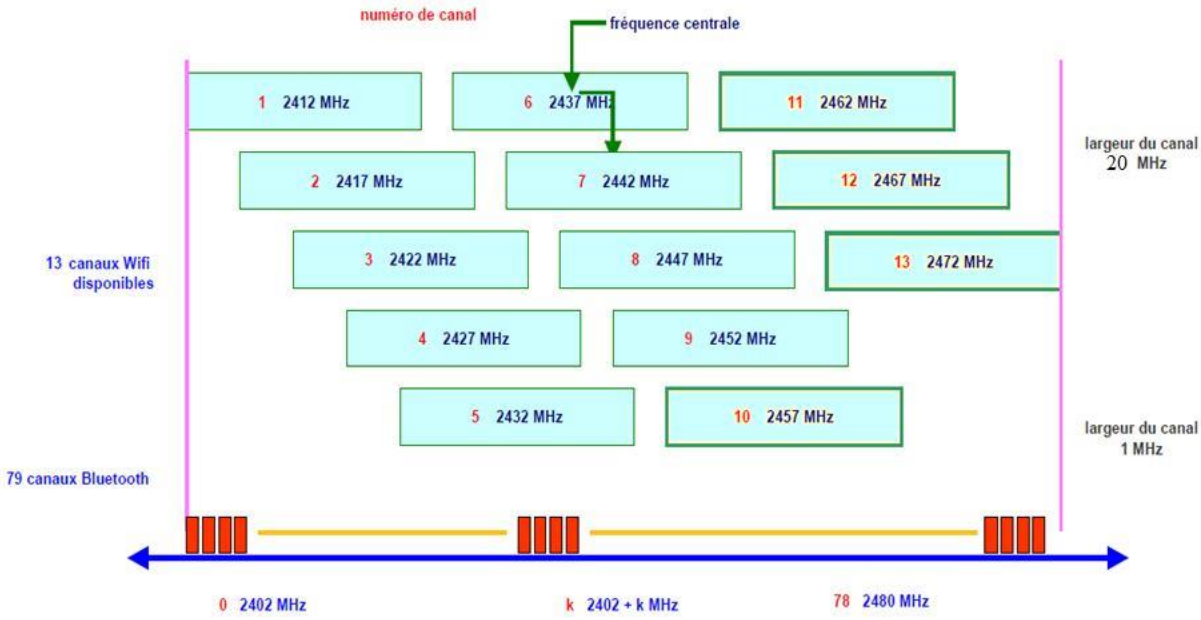


Figure I-8 : Division de la bande en plusieurs canaux

3.4 Les Sauts en Fréquence de Bluetooth

Le Bluetooth utilise une transmission par saut de fréquence entre les différents canaux de la bande de fréquence : FHSS (Frequency Hopping Spread Spectrum).Le principe du FHSS est la commutation rapide entre plusieurs canaux de fréquence, utilisant un ordre pseudo aléatoire connu tant à l'émetteur qu'au récepteur pour la synchronisation. Ainsi, les équipements radio participant à une transmission utilisant FHSS doivent utiliser la même séquence de saut de fréquence pour pouvoir communiquer [17].

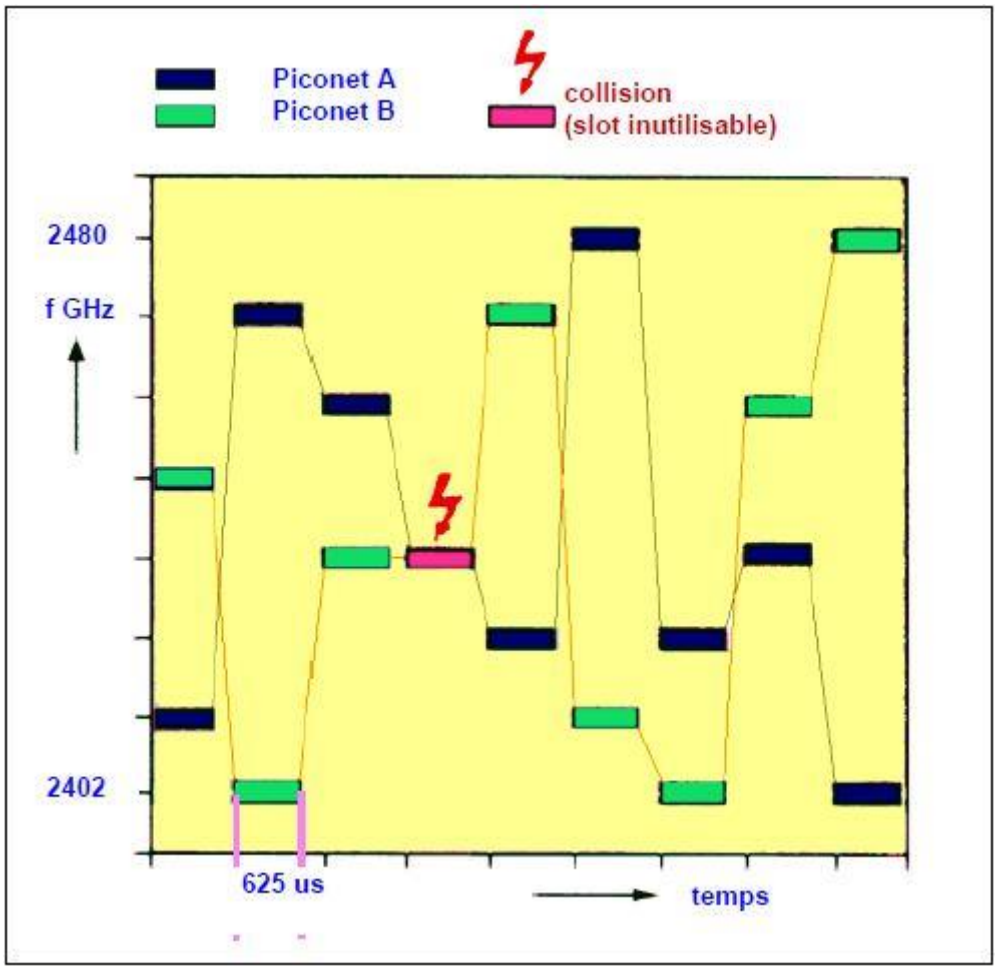


Figure I-9: Deux piconets A et B (proche l'un de l'autre) utilisant FHSS

Les sauts en fréquence dans le standard Bluetooth sont définis comme suit :

- L'information est transmise sur une fréquence pendant un Time-Slot de 625 µs, puis l'émetteur bascule sur une autre fréquence de manière pseudo-aléatoire définie par le maître du piconet (à partir de l'adresse et de l'horloge).
- Les sauts de fréquence (1/625µs = 1600 sauts/s) ont une amplitude de saut de 6MHz au minimum.
- S'il y a plusieurs piconets, chacun d'eux suit une séquence différente (définie parle maître de chaque piconet) pour minimiser les interférences entre piconets.
- S'il y a collisions elles sont gérées par retransmission du paquet.

3.5 Les Caractéristiques de la Modulation

La porteuse est modulée en fréquence par le signal binaire filtré par un filtre passe-bas gaussien, ce qui donne une modulation GFSK (Gaussian Frequency Shift Keying).L'excursion en fréquence de la porteuse est de 150 kHz environ, et un spectre de 1 MHz.

Le spectre réel doit tenir dans un certain gabarit que doit respecter l'émission (220KHz (-3dB) ,1 MHz (-20 dB)) [17].

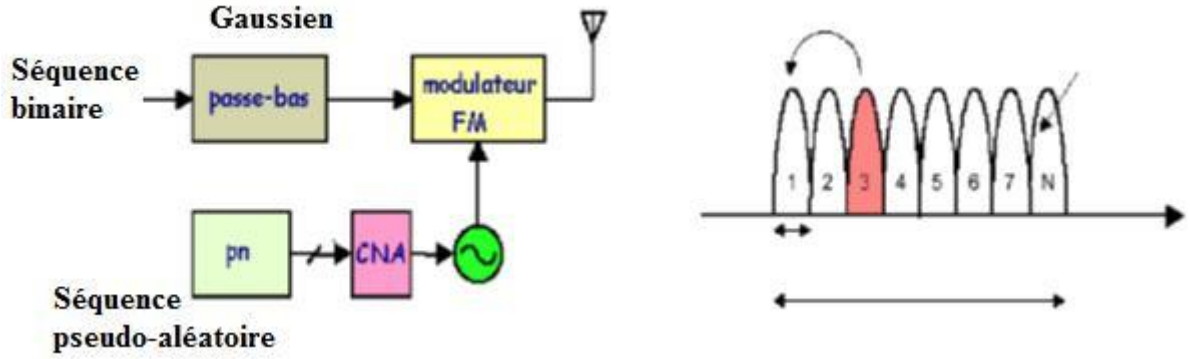


Figure I-10 : Principe de la transmission FHSS

3.6 Puissance d'Emission

- **Classe 1 :** puissance max émise de 100 mW avec un minimum de 4 mW. Dans cette catégorie, le contrôle de puissance est obligatoire variant de 4 à 20 dBm. Ce mode offre la plus grande portée de 100 m.

- **Classe 2 :** puissance max émise de 2.4 mW avec un minimum de 0.25 mW. Ce mode offre une portée de 10 m à 20 m.

- **Classe 3 :** puissance nominale de 1 mW. Sans avantage une autonomie de la batterie très élevée.

3.7 Mécanisme de Transmission par Paquets

Pour la transmission, les données sont formatées en paquets et associées à des informations d'adresse et de description du paquet :

- Code d'accès (72 bits) : chaque paquet débute par un code de canal CAC (Chanel Access Code), un code DAC (Device Access Code) utilisé pour le paging, un code IAC (Inquiry Access Code) pour la recherche dans un piconet.

- En-tête (54 bits) : il contient l'adresse de l'esclave (codée sur 3 bits), le type de paquet et des bits de contrôle.

- Données binaires : la taille de cette partie est variable et peut aller jusqu'à 240 bits. Le maître émet dans les time-slots pairs et l'esclave dans les time-slots impair. Les time-slots sont numérotés de k = 0 à k = $k_{max} = 2^{27} - 1$.

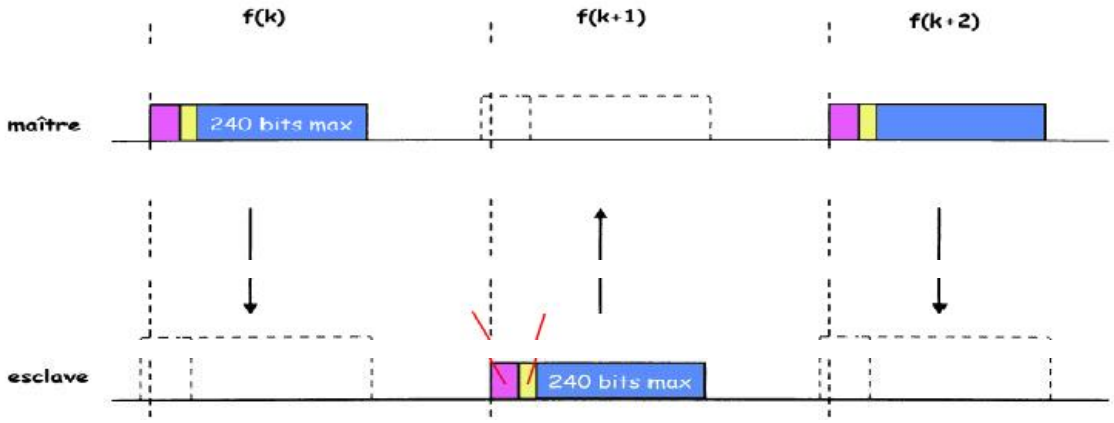


Figure I-11: Echange de données entre Maître et Esclave (paquet court 1 time-slot)

Dans ce mode le débit maximal d'une station vers une autre est de :

$$D = \frac{240}{2 * 625.10^{-6}} = 192\ kbits/s$$

Pour avoir un débit plus élevé Bluetooth peut utiliser des paquets moyens (3 time-slot, 1480bits) ou longs (5 time-slots, 2745 bits).

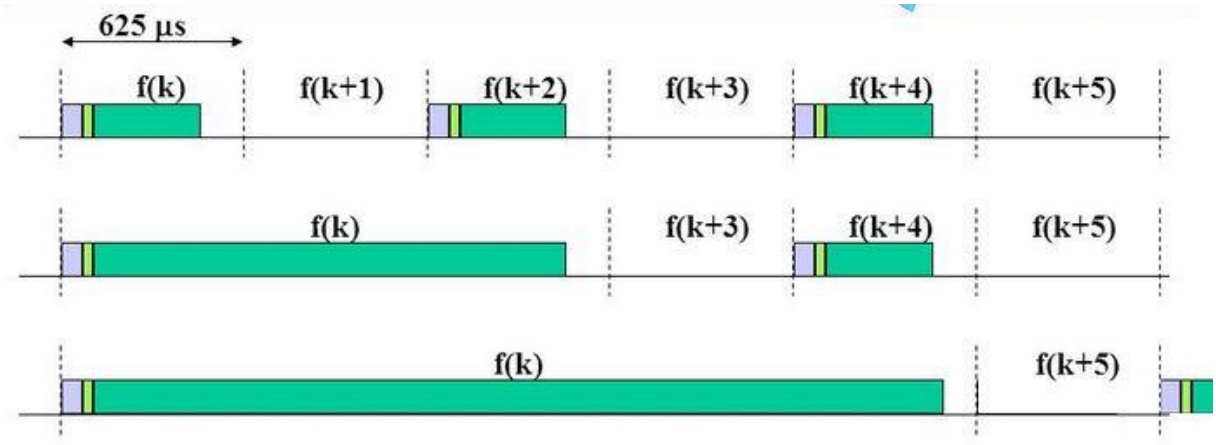


Figure I-12 : Communication avec des paquets plus longs

Dans les deux derniers cas le saut de fréquence se fait après transmission complet du paquet. En fonction de la taille des paquets utilisés, le débit varie :

- Paquet long dans un sens, court dans l'autre : (D1 = 732 kbits/s, D2 = 64 Kbits/s).
- Paquet moyen dans un sens, court dans l'autre : (D1 = 592 kbits/s, D2 = 96 Kbits/s).
- Paquet long dans les deux sens : (D1 = D2 = 439.2 kbits/s).

Les données peuvent être protégées par FEC 2/3 ou FEC 1/3 (Forword Error Correction).

L'en-tête de chaque paquet est toujours protégé par une correction d'erreur en aval (FEC) [17].

3.8 Liens Entre Maître est Esclaves

Il y a deux types de liens qui peuvent être établis entre un maître et un esclave :

- Lien synchrone avec connexion (SCO)
  - Allocation d'une bande passante fixe sur une connexion point à point entre le maître et un esclave. Le maître maintien le lien en utilisant des slots réservés à intervalles réguliers.
  - Le maître peut gérer jusqu'à 3 liens synchrones simultanés et un esclave peut en accepter jusqu'à 2.
  - Pas de retransmission de paquets (des paquets de voix).
- Lien asynchrone sans connexion (ACL)
  - Liaison multipoint entre maître et les esclaves du Piconet. Dans les slots non réservés aux liaisons asynchrones, le maître peut échanger des paquets avec tout autre esclave sur la base d'un slot par esclave, même avec un esclave impliqué dans une liaison synchrone.
- Existence que d'une liaison asynchrone
- Un mécanisme de retransmission de paquets est appliqué

Dans l'exemple suivant une illustration des liaisons SCO et ACL.

Le maître échange des données avec deux esclaves du Piconet :

- Avec l'esclave 1 un lien synchrone SCO pour une communication vocale lien ACL pour les données.
- Avec l'esclave 2 un asynchrone ACL pour les données [7].

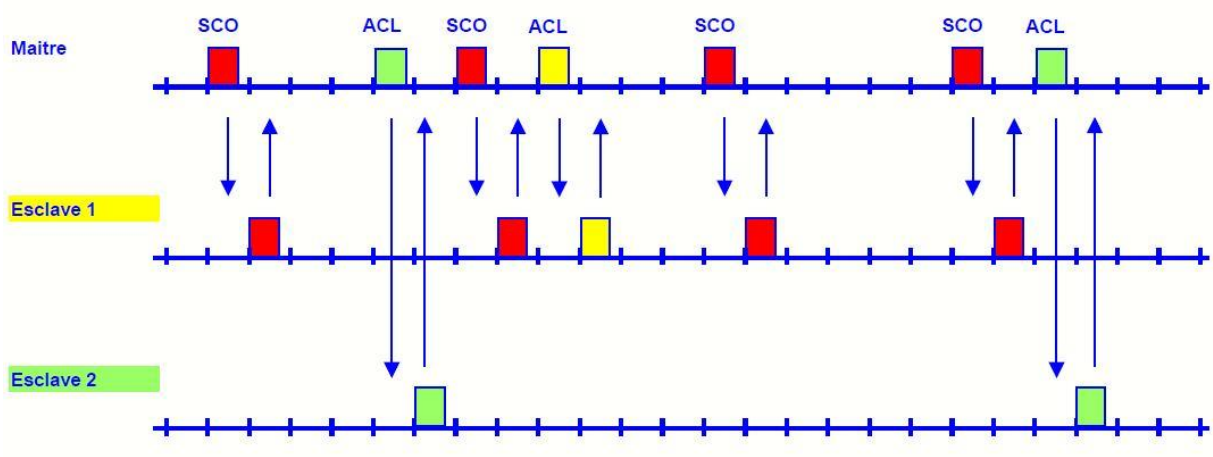


Figure I-13 : Un maître établi une liaison SCO + 2 liaisons ACL

Illustration de la retransmission automatique

La transmission du paquet B vers l'esclave 1 a été perturbée, l'acquittement n'a pas eu lieu(NAK) et le paquet est renvoyé dans le time-slot suivant : c'est la retransmission automatique.

La transmission du paquet Z envoyé par l'esclave 2 vers le maître a été perturbée. Le maître en avertit l'esclave dès qu'il est disponible pour recevoir une nouvelle transmission du même paquet [17].

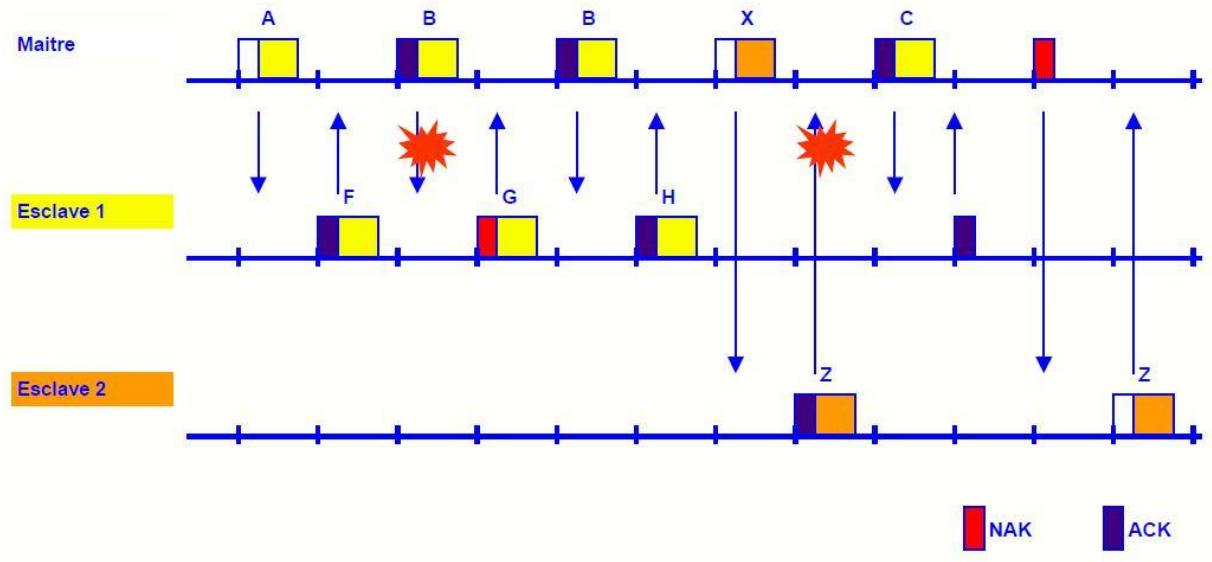


Figure I-14 : Mécanisme de retransmission de paquet

3.9 Mise en Place d'une Association (Liaison)

Un équipement Bluetooth est au départ en mode « standby » et cherche la présence d'activité à proximité toutes les 1.28 s en écoutant successivement les porteuses d'éveil (32/79).

S'il veut s'associer il envoi une requête « Inquiry » si les adresses sont inconnues ou« Page » si elles sont connues. Les équipements à proximité lui répondent. Il devient alors le maître du Piconet, et son adresse définit la suite des sauts en fréquence suivie dans le Piconet.

Les esclave se synchronisent sur le maître et communiquent leurs adresses.

Si le maître veut échanger des données, il passe en mode d'appel et définit avec l'esclave le type et les caractéristiques de la liaison qu'il veut mettre en place. Au bout de 0.6s il passe dans l'état « Connected ».Il peut transmettre des données « Transmit Data ». Après l'échange il retourne dans l'un des états suivants:

- Il passe en mode de maintien « Hold »
- Il passe en mode renifleur « Sniff »
- Ou il passe en mode parcage « pack » [17].

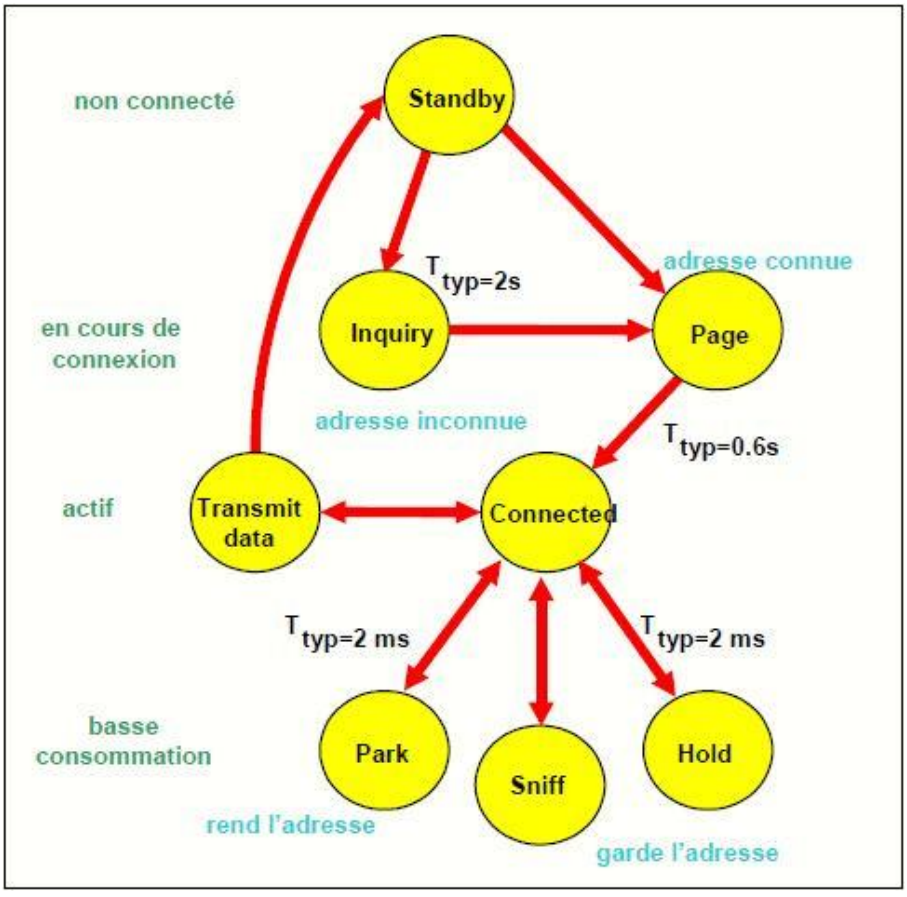


Figure I-15 : Les différentes états d'un équipement Bluetooth

3.10 L'Architecture Bluetooth

L'architecture Bluetooth permet l'interconnexion de tout type de terminal qui possède l'interface radio Bluetooth. Elle est composée de deux grands types de couches comme illustré ci-dessous:

- Les couches matérielles,
- Les couches logicielles.
- Les couches basses correspondent à la partie transmission sur l'interface radio.
- Les adresses sont gérées au niveau de la bande de base sur une longueur de 48 bits(IEEE).

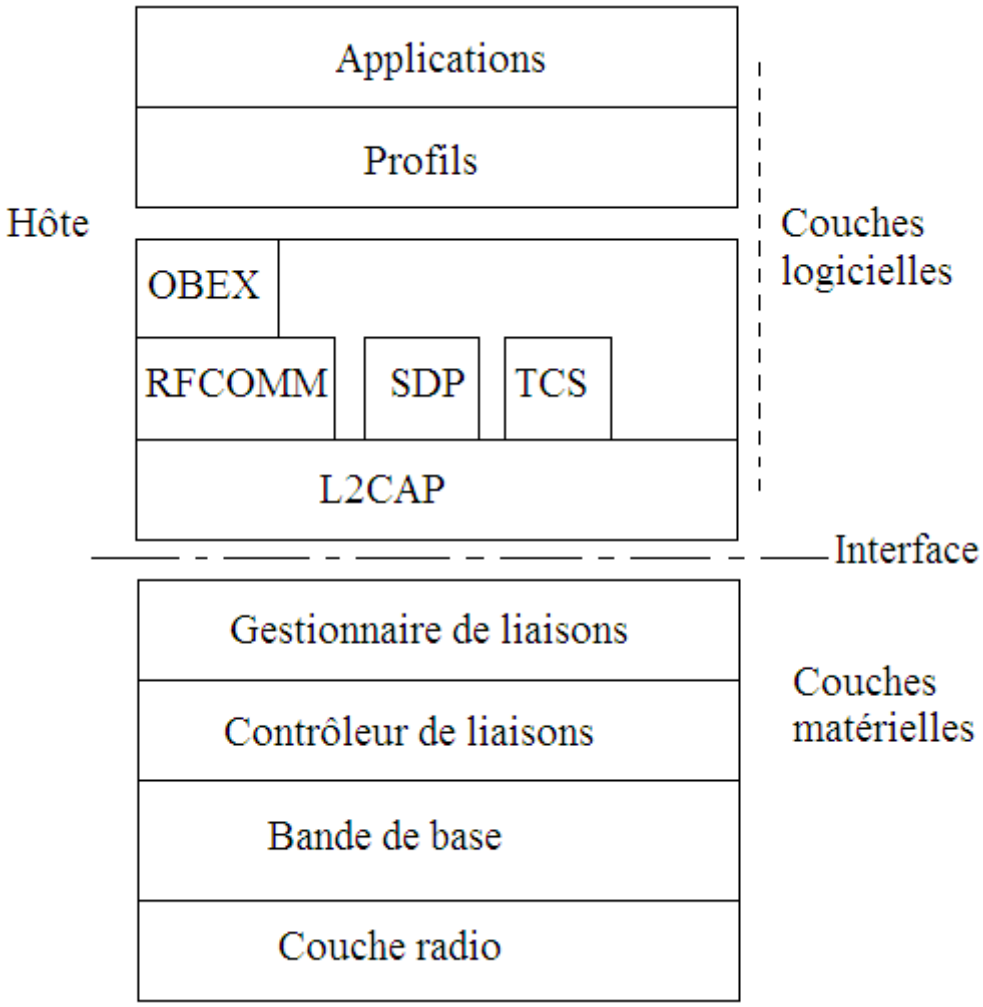


Figure I-16 : Architecture en Couches (Bluetooth)

- Le contrôleur de liaison a pour objectif de gérer la configuration de la liaison,
- Le gestionnaire de liaison vise la sécurité en gérant l'authentification et le chiffrement.

3.10.1 Spécification de la Couche L2CAP

La couche L2CAP (**L**ogical **L**ink **C**ontrol &**A**daptation **P**rotocol) contrôle la liaison entre les entités d'un réseau au support partagé et assure un certain nombre de services en s'appuyant sur la couche inférieure pour le contrôle de flux et d'erreurs.

Cette couche permet donc de multiplexer les flots qui proviennent des différents protocoles de niveau supérieur.

Le protocole emploie des liaisons asynchrones et il ne supporte pas les liaisons synchrones. Il fournit deux types de service au protocole de la couche supérieure :

- Service sans connexion : service de type datagramme fiable
- Service avec connexion : service équivalent à celui offert par HDLC. Une connexion logique est établie entre deux utilisateurs qui s'échangent des données avec un contrôle de flux et un contrôle d'erreurs assurés.

3.10.2 Les Couches Logicielles :

Les protocoles situés au-dessus correspondent :

- Des services de transport sur l'interface série RS-232 (RFCOMM),
- La découverte de service avec SDP (**S**ervice **D**iscovery **P**rotocol),
- Telephony control protocol (TCS),
- Le protocole d'échange d'objet OBEX (**Ob**ject **EX**change).

Au-dessus de cette couche, des profils d'équipements on été choisis pour permettre de mettre en place une relation simple entre terminaux de même nature (une vingtaine de profils ont été définis). Le profil Bluetooth définit les commandes et les fonctionnalités que des appareils peuvent échanger grâce à la technologie Bluetooth. Headset Profile (HSP) : Casque audio, Human Interface Device Profile (HIDP) : Souris ou clavier, Health Device Profile (HDP) : Thermomètre [18].

Chapitre II : Techniques de Brouillage dans les Réseaux sans Fils

Introduction

Avec la généralisation des technologies sans fil telles que le Wi-Fi et le Bluetooth, les réseaux sans fil sont devenus une composante essentielle dans de nombreuses applications, tant domestiques qu'industrielles. Toutefois, cette omniprésence s'accompagne de défis croissants en matière de sécurité, notamment les menaces liées au **brouillage (jamming)**, qui consistent à perturber intentionnellement les communications radio en générant des signaux parasites sur les mêmes bandes de fréquence.

Le brouillage représente l'une des attaques les plus redoutables contre les réseaux sans fil, car il peut désactiver complètement une communication sans nécessiter le contournement des protocoles de sécurité [19].

Ce type d'attaque est à la fois simple à mettre en œuvre et potentiellement dévastateur, ce qui en fait un véritable danger, notamment dans les environnements sensibles tels que les systèmes industriels, les infrastructures critiques ou les applications militaires.

Dans ce chapitre, nous présentons de manière systématique les différentes techniques de brouillage ciblant les réseaux sans fil, en commençant par les formes les plus simples jusqu'aux attaques les plus sophistiquées et adaptatives. Nous analysons également les mécanismes d'action de ces attaques, leur classification, ainsi que les stratégies de positionnement utilisées pour maximiser leur efficacité tout en minimisant leur consommation énergétique. Enfin, nous illustrons notre étude par des exemples concrets et des références issues de la littérature scientifique récente.

1 Techniques de Brouillage

Le brouillage utilise des interférences radio intentionnelles pour nuire aux communications sans fil en occupant le support de communication, obligeant ainsi un émetteur à ralentir lorsqu'il détecte une occupation du support sans fil ou un signal corrompu reçu par les récepteurs. Le brouillage cible principalement les attaques au niveau de la couche physique, mais des attaques inter-couches sont également possibles. Dans cette section, nous détaillons les différents types de brouilleurs et leur positionnement pour maximiser la zone de brouillage.

1.1 Types de Brouilleurs

Les brouilleurs sont des nœuds sans fil malveillants installés par un attaquant pour provoquer des interférences intentionnelles dans un réseau sans fil. Selon la stratégie

d'attaque, un brouilleur peut avoir des capacités identiques ou différentes de celles des nœuds légitimes du réseau attaqué. L'effet de brouillage d'un brouilleur dépend de la puissance de son émetteur radio, de son emplacement et de son influence sur le réseau ou le nœud ciblé. Un brouilleur peut brouiller un réseau de différentes manières pour optimiser son efficacité. Un brouilleur peut être élémentaire ou avancé, selon ses fonctionnalités. Les brouilleurs élémentaires sont divisés en deux sous-groupes : proactifs et réactifs. Les brouilleurs avancés sont également classés en deux sous-types : spécifiques à une fonction et hybrides intelligents. La classification détaillée des différents brouilleurs est présentée à la figure 1.

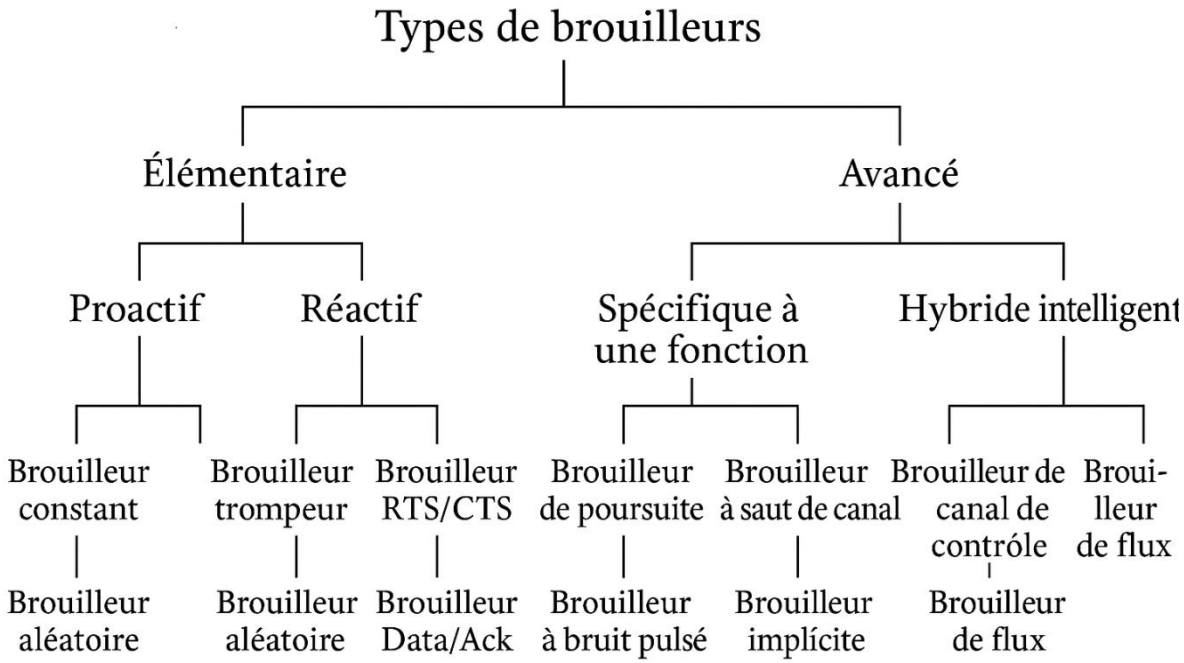


Figure II-1 : Types de Brouilleurs dans les Réseaux sans Fil

1.1.1 Brouilleur Proactif

Un brouilleur proactif transmet des signaux de brouillage (interférents), qu'il y ait ou non communication de données sur un réseau. Il envoie des paquets ou des bits aléatoires sur le canal sur lequel il fonctionne, mettant tous les autres nœuds de ce canal en mode inactif. Cependant, il ne change pas de canal et ne fonctionne que sur un seul canal jusqu'à épuisement de son énergie. Il existe trois principaux types de brouilleurs proactifs : constants, trompeurs et aléatoires. Désormais, chaque utilisation de brouilleurs proactifs peut avoir trois conséquences :

Un brouilleur constant émet des bits aléatoires en continu sans respecter le protocole CSMA.

Selon le mécanisme CSMA, un nœud légitime doit détecter l'état du support sans fil avant de transmettre. Si le support est continuellement inactif pendant une durée DIFS (DCF Inter frame Space), il est alors seulement entendu transmettre une trame. Si le canal est occupé pendant l'intervalle DIFS, la station doit différer sa transmission. Un brouilleur constant empêche les nœuds légitimes de communiquer entre eux en provoquant une occupation constante du support sans fil. Ce type d'attaque est énergivore et facile à détecter, mais très facile à lancer et peut endommager les communications réseau au point que personne ne puisse communiquer.

Un brouilleur trompeur transmet en continu des paquets réguliers au lieu d'émettre des bits aléatoires (comme dans un brouilleur constant). Il trompe les autres nœuds en leur faisant croire qu'une transmission légitime est en cours, les forçant ainsi à rester en état de réception jusqu'à ce que le brouilleur soit désactivé ou mette fin à son fonctionnement. Comparé à un brouilleur permanent, il est plus difficile à détecter car il transmet des paquets légitimes au lieu de bits aléatoires. Tout comme le brouilleur permanent, le brouilleur permanent est également peu économe en énergie en raison de sa transmission continue, mais sa mise en œuvre est très simple. Le brouilleur aléatoire transmet par intermittence des bits aléatoires ou des paquets réguliers aux réseaux. Contrairement aux deux brouilleurs précédents, il vise à économiser l'énergie. Il alterne en permanence entre deux états : la phase de veille et la phase de brouillage. Il reste en veille pendant un certain temps, puis devient actif pour le brouillage avant de revenir à son état de veille. Les périodes de veille et de brouillage sont soit fixes, soit aléatoires. Il existe un compromis entre l'efficacité du brouillage et les économies d'énergie, car il ne peut pas brouiller pendant sa période de veille. Les ratios entre temps de veille et temps de brouillage peuvent être manipulés pour ajuster ce compromis entre efficacité et efficience [20].

1.1.2 Brouilleur Réactif

Un brouilleur réactif ne commence à brouiller que lorsqu'il détecte une activité réseau sur un canal spécifique. Par conséquent, il vise à compromettre la réception d'un message. Il peut perturber les paquets, petits comme grands. Comme il doit surveiller le réseau en permanence, le brouilleur réactif est moins économe en énergie qu'un brouilleur aléatoire. Cependant, il est beaucoup plus difficile de détecter un brouilleur réactif qu'un brouilleur proactif, car le taux

de délivrabilité des paquets (PDR) ne peut être déterminé avec précision en pratique. Deux méthodes différentes permettent de mettre en œuvre un brouilleur réactif.

Le brouilleur réactif RTS/CTS brouille le réseau lorsqu'il détecte la transmission d'un message de demande d'envoi (RTS) par un émetteur. Il commence à brouiller le canal dès l'envoi du RTS. Ainsi, le récepteur ne renvoie pas de réponse CTS (Clear-to-Send), car le paquet RTS envoyé par l'émetteur est déformé. L'émetteur n'envoie alors pas de données, pensant que le récepteur est occupé par une autre transmission en cours. Le brouilleur peut également attendre la réception du RTS et brouiller le réseau lorsque le CTS est envoyé par le récepteur. Dans ce cas, l'émetteur n'envoie pas de données et le récepteur attend toujours le paquet de données.

Le brouilleur réactif de données/ACK brouille le réseau en corrompant les transmissions de données ou de paquets d'accusé de réception (ACK). Il ne réagit pas tant qu'une transmission de données n'a pas commencé du côté de l'émetteur. Ce type de brouilleur peut corrompre les paquets de données ou attendre que les paquets atteignent le récepteur avant de corrompre les paquets ACK. La corruption des paquets de données et des messages ACK entraîne des retransmissions du côté de l'émetteur. Dans le premier cas, les paquets de données ne sont pas reçus correctement par le récepteur et doivent être retransmis. Dans le second cas, l'émetteur ne reçoit pas les ACK et soupçonne un problème côté récepteur, par exemple un dépassement de tampon. Il retransmet donc les paquets de données [20].

1.1.3 Brouilleurs à Fonction Spécifique

Le brouillage à fonction spécifique est implémenté grâce à une fonction prédéfinie. En plus d'être proactifs ou réactifs, ils peuvent fonctionner sur un seul canal pour économiser l'énergie ou brouiller plusieurs canaux et maximiser le débit de brouillage, quelle que soit la consommation d'énergie. Même lorsque le brouilleur brouille un seul canal à la fois, il n'est pas dépendant de ce canal et peut changer de canal en fonction de ses fonctionnalités spécifiques. Le brouilleur de suivi saute sur tous les canaux disponibles très fréquemment (des milliers de fois par seconde) et brouille chaque canal pendant une courte période. Si un émetteur détecte le brouillage et change de canal, le brouilleur de suivi balaie toute la bande et recherche une nouvelle fréquence à brouiller. Il peut également suivre une séquence de sauts de fréquence pseudo-aléatoire. Ce type de brouilleur économise de l'énergie en limitant son attaque à un seul canal avant de passer à un autre. Grâce à sa vitesse de saut de fréquence élevée, le brouilleur de suivi est particulièrement efficace contre certains techniques

antibrouillages, comme l'étalement de spectre par sauts de fréquence (FHSS), qui utilise une vitesse de saut lente. Le brouilleur à saut de canal passe pro-activement d'un canal à l'autre.

Ce type de brouilleur a un accès direct aux canaux en surpassant l'algorithme CSMA fourni par la couche MAC. De plus, il peut brouiller plusieurs canaux simultanément. Pendant ses phases de découverte et de coloration des vertex, le brouilleur est silencieux et invisible pour ses voisins.

Il commence ensuite à attaquer différents canaux à différents moments, selon une séquence pseudo-aléatoire prédéterminée. Le brouilleur à bruit pulsé peut changer de canal et brouiller sur différentes bandes passantes à des moments différents. Comme le brouilleur aléatoire, le brouilleur à bruit pulsé permet également d'économiser de l'énergie en s'éteignant et en s'allumant selon le calendrier programmé. Contrairement au brouilleur aléatoire proactif élémentaire qui n'attaque qu'un seul canal, le brouilleur à bruit pulsé peut attaquer plusieurs canaux. De plus, il peut être implémenté pour brouiller plusieurs canaux simultanément [21].

1.1.4 Brouilleurs Hybrides Intelligents

On les appelle intelligents en raison de leur faible consommation d'énergie et de leur efficacité de brouillage. L'objectif principal de ces brouilleurs est d'amplifier leur effet de brouillage sur le réseau qu'ils souhaitent brouiller. De plus, ils sont économes en énergie. Ils placent suffisamment d'énergie au bon endroit pour bloquer la bande passante de communication de l'ensemble du réseau ou d'une partie importante du réseau, dans les très grands réseaux. Chacun de ces types de brouilleurs peut être mis en œuvre de manière proactive ou réactive, donc hybride. Les brouilleurs de canal de contrôle fonctionnent dans les réseaux multicanaux en ciblant le canal de contrôle, ou le canal utilisé pour coordonner l'activité du réseau.

Un brouilleur aléatoire ciblant le canal de contrôle peut entraîner une dégradation importante des performances du réseau, tandis qu'un brouilleur continu ciblant le canal de contrôle peut bloquer l'accès au réseau. Ces attaques sont généralement réalisées en compromettant un nœud du réseau. De plus, les emplacements futurs des canaux de contrôle peuvent être obtenus à partir des nœuds compromis.

Les attaques par brouillage implicite sont celles qui, en plus de désactiver la fonctionnalité de la cible visée, provoquent également un déni de service sur d'autres nœuds du réseau. Cette attaque exploite l'algorithme d'adaptation de débit utilisé dans les réseaux sans fil, où le point

d'accès (AP) s'adapte au nœud faible en réduisant son débit. De ce fait, le point d'accès passe plus de temps à communiquer avec ce nœud faible qu'avec les autres nœuds. Par conséquent, lorsque l'attaquant implicite brouille un nœud communiquant avec le point d'accès, l'effet d'adaptation de débit augmente la concentration du point d'accès sur le nœud bloqué, ce qui nuit aux autres clients.

Les attaques par brouillage de flux impliquent plusieurs brouilleurs répartis sur le réseau qui brouillent les paquets afin de réduire le flux de trafic. **Tague et al. (2008)** ont mis en œuvre ces attaques en utilisant les informations de la couche réseau. Ce type d'attaque par brouillage est adapté aux attaquants disposant de ressources limitées. En cas de contrôle centralisé, la puissance minimale nécessaire pour brouiller un paquet est calculée et le brouilleur agit en conséquence. Dans un modèle de brouilleur non centralisé, chaque brouilleur partage des informations avec ses voisins afin de maximiser son efficacité. Nous résumons les caractéristiques de toutes les techniques de brouillage mentionnées ci-dessus dans le tableau 1. Pour chaque type de brouilleur, nous déterminons s'il est proactif ou réactif, économe en énergie ou non, et sa capacité à brouiller un ou plusieurs canaux. Cependant, certaines stratégies de brouillage combinent deux ou plusieurs de ces techniques. Par exemple**, Wilhelm et al**. (2011) mettent en œuvre un brouillage réactif monotonal pour générer une stratégie de brouillage optimale en combinant les différentes formes disponibles. **Bayraktaroglu et al. (2008)** utilisent les différentes variantes de brouilleurs pour analyser les performances de la meilleure stratégie de brouillage dans leurs réseaux IEEE 802.11. Ils expérimentent des brouilleurs périodiques sans mémoire basés sur des processus de Poisson, des brouilleurs sensibles au canal et des brouilleurs omniscients, concluant que les brouilleurs sensibles au canal sont les plus efficaces parmi les quatre types. De même, **Wood et al. (2007)** utilisent les variantes et la combinaison de brouilleurs réactifs/aléatoires et multicanaux/à bruit pulsé pour concevoir des attaques telles que le brouillage par interruption, le brouillage par balayage et le brouillage par impulsion. Lors du brouillage par interruption, le brouilleur reste en veille et ne commence à brouiller que lorsqu'il est signalé par le matériel lors de la détection d'activités radio. Le brouillage par balayage permet à l'attaquant de balayer chaque canal en premier et de commencer le brouillage si des activités sont détectées. Le brouillage par impulsions est un brouillage continu ou intermittent sur un seul canal, où l'attaquant transmet à l'aveugle par courtes rafales [22-24].

2. Placement des Brouilleurs

Outre les qualités mentionnées ci-dessus, le placement du brouilleur joue un rôle important pour un brouillage efficace. Les brouilleurs peuvent être placés de manière aléatoire ou selon une technique de brouillage qui localise la meilleure position pour atteindre l'objectif de brouillage avec le plus grand nombre de nœuds possible. Dans cette section, nous examinerons ce problème d'optimisation en examinant différents placements de brouilleurs.

2.1 Attaques par Brouillage Optimales

Li et al. (2007) montrent que la probabilité de brouillage peut être élevée si l'attaquant connaît la stratégie du réseau ainsi que sa puissance de transmission. De plus, le brouilleur doit connaître les probabilités d'accès aux canaux du réseau et le nombre de voisins du nœud de surveillance (nœud de détection). Tous les autres nœuds du réseau effectuent simplement la communication simplex IEEE 802.11 habituelle. Le nœud de surveillance utilise le test de rapport de probabilité séquentiel pour tester séquentiellement deux hypothèses concernant la probabilité de fausse alarme et la probabilité de détection manquée[25].

Les brouilleurs et les émetteurs/récepteurs sont répartis dans une zone donnée selon une loi de Poisson. Les valeurs attendues d'une transmission réussie sont calculées en termes de probabilités. Si une zone particulière est brouillée, le nœud de surveillance est censé envoyer la notification de brouillage hors de cette zone (via une transmission multi-sauts) ; ce dernier est également affecté par le brouillage présent dans la zone. À l'aide d'une loi de probabilité et d'une preuve mathématique, les auteurs ont démontré que la stratégie optimale pour l'attaquant est généralement modérée et à long terme [25].

2.2 Brouillage en Situation d'Incertitude Totale

Commander et al. (2008) utilisent une approche dynamique pour calculer l'emplacement des dispositifs de brouillage en intégrant les limites de la zone à brouiller. Ils supposent qu'une zone carrée entoure le réseau où les brouilleurs sont placés aux intersections d'une grille uniforme. Ils formulent le problème comme suit :

Si les brouilleurs doivent brouiller de manière optimale tous les nœuds du réseau, où doivent-ils être placés ? Des sous-problèmes sont créés et résolus afin d'obtenir un résultat optimal [26].

Classification des brouilleurs

Brouilleur	Proactif	Réactif	Économe en énergie	Canal unique	Canaux multiples
Constant	✓	✓	✓	✓	
Trompeur	✓	✓		✓	
Aléatoire	✓		✓		✓
Brouilleur RTS/CTS		✓	✓	✓	
Suivi		✓	✓	✓	✓
Saut de canal	✓		✓	✓	
Bruit pulsé	✓		✓	✓	✓
Canal de contrôle		✓	✓	✓	
Implieite	✓	✓	✓	✓	
Brouillage de flux	✓	✓	✓	✓	

Tableau I-1 : Classification des brouilleurs

Ils supposent que l'attaquant a une connaissance limitée du réseau, c'est-à-dire qu'il ne connaît que la zone délimitée, et que les brouilleurs sont équipés d'antennes omnidirectionnelles. Ils considèrent que la puissance de brouillage diminue inversement au carré de la distance par rapport à un appareil. De plus, le nombre minimal d'appareils de brouillage permettant de brouiller l'ensemble du réseau est calculé dans ce schéma, sachant qu'en tout point, il y a brouillage lorsque la puissance totale reçue en un point donné est supérieure au seuil de puissance requis pour brouiller la communication sans fil [26].

2.3 Attaques par Brouillage à Portée Limitée

Les brouilleurs dont la portée de transmission est deux fois inférieure à celle des nœuds légitimes peuvent brouiller le réseau, car la portée d'interférence des appareils sans fil est deux fois supérieure à la portée de transmission. Contrairement aux schémas ci-dessus, cette attaque par brouillage ne nécessite pas de connaissances globales. De plus, en raison de leur portée de transmission limitée, ces brouilleurs sont difficiles à détecter. Ils sont placés à des emplacements stratégiques, généralement à proximité des nœuds les plus fréquentés (entrée/sortie). Les auteurs ont présenté des résultats expérimentaux avec des brouilleurs à portée normale, à portée limitée et à double portée (portée de transmission). Les brouilleurs à

portée normale ont la même portée de transmission que les nœuds légitimes ; leur portée d'interférence est donc deux fois supérieure à celle des nœuds légitimes. De même, les brouilleurs à portée limitée ont une portée de transmission deux fois inférieure, ce qui signifie que leur portée d'interférence est égale à celle des nœuds légitimes. Des expériences menées sur ces brouilleurs dans un simulateur OPNET montrent que la détection de ces brouilleurs à portée limitée est difficile, car leur puissance d'émission est deux fois inférieure à celle des nœuds légitimes. Ils ont conclu que les brouilleurs à portée limitée sont difficiles à détecter car ils réduisent les paramètres les plus couramment utilisés pour la détection, tels que le rapport signal/bruit et le rapport signal/réponse [27].

2.4 DSS Pour la Localisation des Brouilleurs VHF/UHF

Gencer et al. (2008) ont défini un système de brouillage devant être placé à l'emplacement optimal pour détruire complètement la capacité de communication du système cible. Ces types de systèmes sont généralement utilisés dans les applications militaires. Un plus grand nombre de points candidats ou de points sélectionnés pour le déploiement du système de brouillage est pris en compte par rapport aux points cibles et au nombre de systèmes de brouillage disponibles. Ils supposent qu'il existe une ligne de visée directe entre le brouilleur et les systèmes cibles, que les cibles se trouvent à portée de l'antenne et que la puissance du signal du système de brouillage est supérieure à celle du système cible. L'objectif principal de ce système d'aide à la décision est de trouver ou d'identifier l'emplacement des systèmes de brouillage radio afin de brouiller la zone la plus large possible. C'est pourquoi ils utilisent le modèle de couverture maximale et le résolvent à l'aide du package LINGO-8.

LINGO est un package intégré qui inclut un langage puissant pour exprimer les modèles d'optimisation. En fonction du nombre de points cibles, de points candidats et de systèmes de brouillage disponibles, les emplacements de déploiement des brouilleurs sont déterminés [28].

2.5 Brouilleur de Taille Nanométrique

Panyim et al. (2009) préconisent l'utilisation d'un grand nombre de brouilleurs minuscules et de faible puissance, difficiles à détecter car invisibles à l'œil nu en raison de leur petite taille. Ces brouilleurs sont mis en œuvre sous forme de réseau. La puissance de brouillage totale étant constante, ils permettent une transition de phase du débit de brouillage. Des brouilleurs réactifs sont déployés sur l'ensemble du réseau. Les résultats expérimentaux de cet article montrent que ces brouilleurs offrent des performances supérieures à celles des

brouilleurs traditionnels. Le nombre de brouilleurs peut être augmenté, réduisant ainsi leur puissance de brouillage et maintenant constante la puissance totale consommée par les brouilleurs. Ils ont utilisé le comportement d'échelle de la théorie de la percolation. Ils ont démontré la difficulté de détection de leurs brouilleurs en raison de leur faible puissance, de leur petite taille et de leur grande efficacité dans la formation de leur réseau [29].

Tableau 2 Placement des brouilleurs

Stratégie de placement	Connaissance du réseau	Puissance d'émission	Niveau de détection
Attaques de brouillage optimales	Oui	Contrôlable	Difficile
Brouillage sous incertitude totale	Limitée	Calculée	Modéré
Attaques de brouillage à portée limitée	Non	Plusieurs	Difficile
Systèmes DSS pour localiser un brouilleur	Oui	Élevée	Facile
VHF/UHF	Non	Plusieurs	Très difficile

Tableau II-2: Placement des brouilleurs

En résumé, ces cinq stratégies de placement de brouilleurs sont analysées dans le tableau 2. Nous examinons si la connaissance du réseau est nécessaire, la puissance d'émission des brouilleurs, leur nombre et la difficulté de détection.

3. Conclusion

Dans ce chapitre, nous avons exploré de manière approfondie les différentes techniques de brouillage utilisées pour perturber les communications dans les réseaux sans fil. Nous avons classé les types de brouilleurs en quatre grandes catégories — proactifs, réactifs, à fonction spécifique et hybrides intelligents — chacune présentant des caractéristiques, des objectifs et des niveaux de complexité distincts. Cette classification met en lumière la diversité des méthodes d'attaque possibles, allant des stratégies simples mais énergivores à des approches plus subtiles, économes et adaptatives.

Nous avons également examiné les mécanismes de fonctionnement de ces techniques, leurs capacités à cibler un ou plusieurs canaux, ainsi que les compromis entre efficacité de l'attaque et consommation énergétique. L'analyse des stratégies de placement des brouilleurs a souligné l'importance de la position dans la réussite d'une attaque, avec une distinction claire entre les scénarios de placement optimal basé sur des connaissances préalables du réseau et ceux fondés sur une incertitude totale.

L'ensemble de ces éléments montre que le brouillage reste une menace redoutable pour la sécurité des communications sans fil. La compréhension fine de ces techniques est indispensable non seulement pour concevoir des systèmes de communication plus robustes, mais aussi pour anticiper les attaques et mettre en œuvre des contre-mesures efficaces.

Chapitre III : Système de Brouillage sans Fil Utilisant ESP32 et NRF24L01

Introduction

Ce projet vise à concevoir et réaliser un système de brouillage sans fil simple et efficace, en utilisant un microcontrôleur **ESP32** et trois modules **NRF24L01**. Le système cible les réseaux Wi-Fi et Bluetooth fonctionnant dans la bande de fréquence 2,4 GHz, en émettant des ondes porteuses continues et en changeant les canaux de manière aléatoire ou séquentielle.
Le choix de l'**ESP32** repose sur ses capacités de traitement avancées, son support de deux interfaces **SPI** indépendantes (**HSPI** et **VSPI**), ainsi que sa flexibilité dans la gestion des ressources logicielles et matérielles. Les interfaces sans fil natives (Wi-Fi et Bluetooth) de l'ESP32 sont désactivées afin de libérer les ressources et de concentrer toute la puissance sur les modules NRF pour le brouillage.

1. Objectifs du Projet :

- Comprendre le fonctionnement des réseaux **Wi-Fi et Bluetooth** dans la bande des 2,4 GHz.
- Générer des **signaux de brouillage efficaces** couvrant le maximum de canaux sans fil.
- Analyser les **performances et l'impact du brouillage** sur les communications à proximité.
- Concevoir un **système multi-modules** en utilisant l'ESP32 pour gérer plusieurs NRF24L01 simultanément.
- Maîtriser la communication **SPI** et la répartition des tâches entre les interfaces **HSPI et VSPI**.

2. Composants Principaux :

- ✓ Microcontrôleur **ESP32 WROOM-32E**
- ✓ **3 modules NRF24L01** (avec antennes haute puissance pour une meilleure portée)
- ✓ Fils de connexion, plaque d'essai ou circuit imprimé (PCB) personnalisé
- ✓ Alimentation externe stable (3,3V régulée avec condensateurs recommandés)
- ✓ Outils d'analyse sans fil (comme **Wi-Fi Analyzer** sur Smartphone ou PC)

3. Description de la Carte ESP32-WROOM-32E

La **carte ESP32-WROOM-32E** est un module Wi-Fi et Bluetooth puissant basé sur le microcontrôleur **ESP32**, développé par **Espressif Systems**. Ce module est une évolution du populaire ESP32-WROOM-32, offrant une meilleure stabilité et une certification plus large. Il constitue le cœur du système utilisé dans ce projet de **brouillage de signaux sans fil (Wi-Fi/Bluetooth)**.

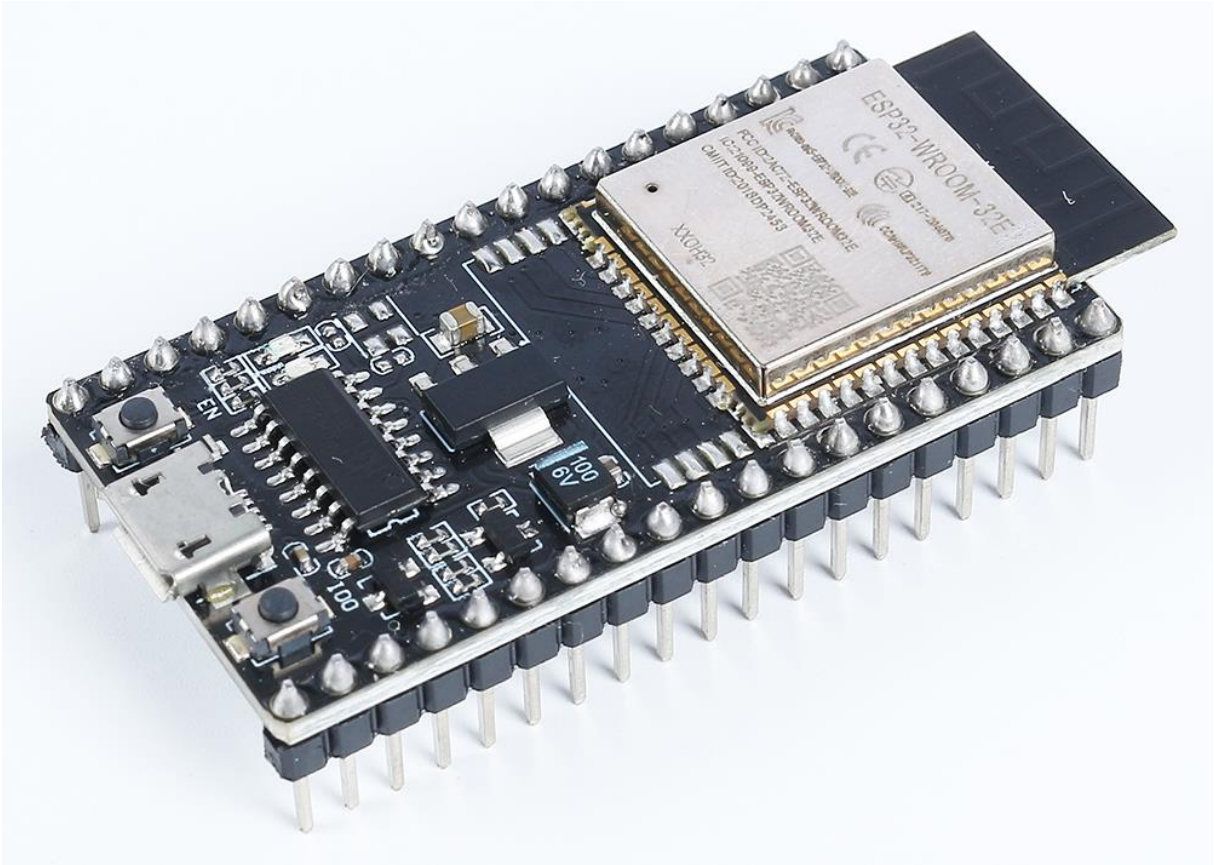


Figure III-1 :ESP32 WROOM32 E

a. Caractéristiques techniques principales :

- **Processeur :** Dual-coreXtensa® 32-bit LX6, jusqu'à 240 MHz
- **Mémoire :**
  - **Mémoire Flash intégrée :** 4 Mo (ou plus selon version)
  - **SRAM :** 520 Ko
- **Connectivité sans fil :**
  - **Wi-Fi 802.11 b/g/n** (2.4 GHz)
  - **Bluetooth v4.2 BR/EDR et BLE (Bluetooth Low Energy)**
- **Interfaces périphériques :**
  - Jusqu'à **34 GPIO**
  - **SPI, I2C, UART, I2S, PWM, ADC, DAC**
- **Tension d'alimentation :** 3.0V – 3.6V
- **Consommation faible**, avec plusieurs modes de veille
- **Boîtier :** module compact avec blindage métallique, certifié CE/FCC/IC

3.1 Avantages dans ce Projet :

- **Capacité multitâche** grâce aux deux cœurs, permettant de gérer plusieurs modules NRF24L01 simultanément via différentes interfaces SPI (HSPI, VSPI)
- **Compatibilité Arduino IDE**, facilitant le développement du code embarqué
- **Intégration facile avec des modules de communication RF**, comme le NRF24L01, pour générer des signaux constants de brouillage
- **Support Bluetooth désactivable**, ce qui est exploité ici pour maximiser l'usage des ressources matérielles pour le brouillage
- **Bonne gestion des interfaces SPI**, essentielle pour gérer plusieurs modules simultanément avec stabilité

3.2 Utilisation dans le Projet :

Dans ce projet, l'ESP32-WROOM-32E est utilisé pour :

- Contrôler trois modules NRF24L01 configurés pour émettre des porteuses continues (const carrier mode) sur différentes fréquences,
- Exploiter deux bus SPI (HSPI et VSPI) avec des lignes CE/CS séparées pour chaque module,
- Désactiver les interfaces Wi-Fi/Bluetooth internes afin de concentrer toute la puissance du microcontrôleur sur l'émission de signaux de brouillage,
- Scanner aléatoirement ou balayer systématiquement les canaux Wi-Fi/Bluetooth pour maximiser l'efficacité du brouillage.

3.3 Brochage ESP32WROOM32E

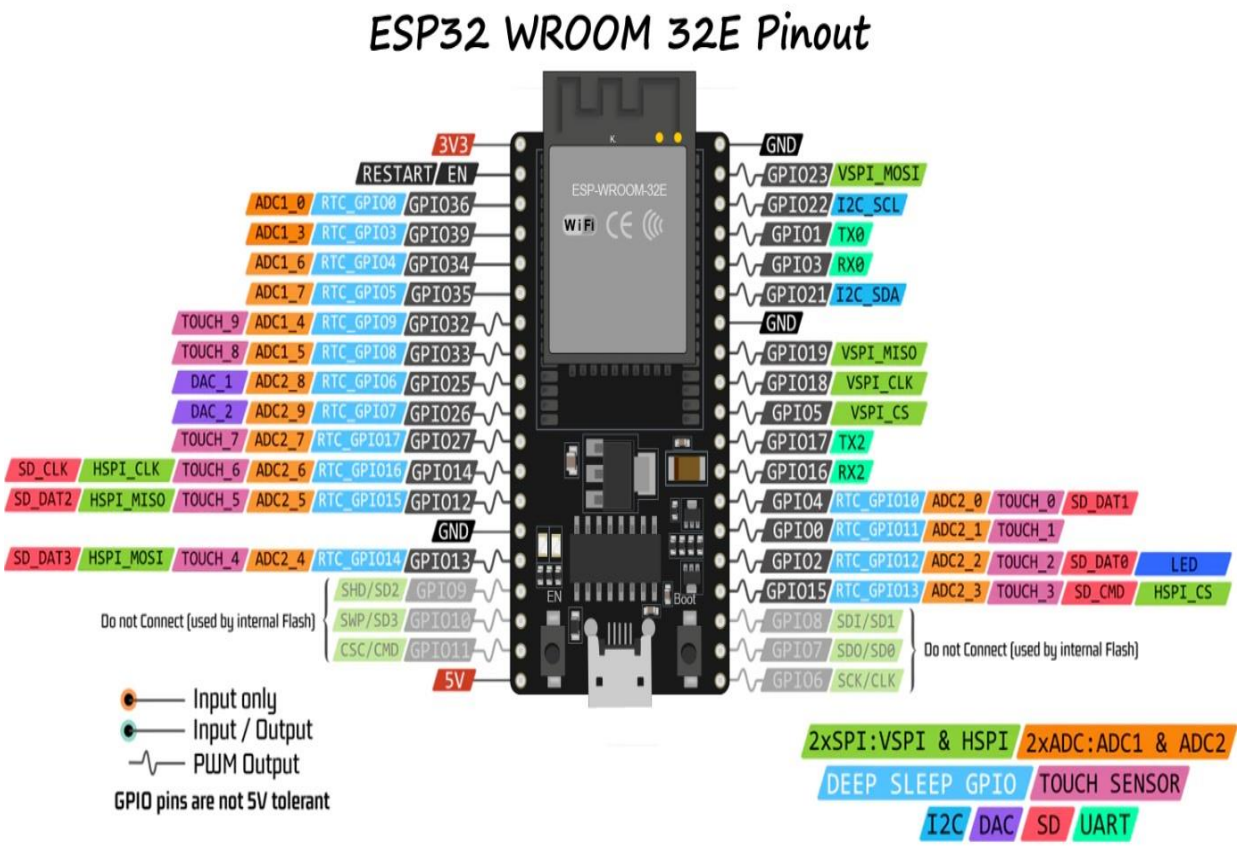


Figure III-2 : Brochage ESP32 WROOM32 E

4.Description sur le NRF24

La puce **nRF24** est un circuit intégré de chez **Nordic Semiconductor**. En fait, il s'agit ni plus ni moins que d'un module d'émission / réception radio, opérant sur la bande des 2,4 GHz (comme le WiFi, ou le Bluetooth). Mais ce qui fait toute sa beauté, c'est qu'il se pilote le plus simplement du monde. En effet, un simple petit Arduino permet d'en prendre le contrôle, via le port SPI.

Sachez que le nRF24 est décliné en 2 versions courantes, actuellement :

- **Le nRF24L01+,** avec son antenne intégrée au PCB (reconnaissable avec ses pistes de cuivre en zigzag).
- **Le nRF24L01+ PA LNA, avec son antenne externe** (raccordable avec un connecteur à visser, type SMA).

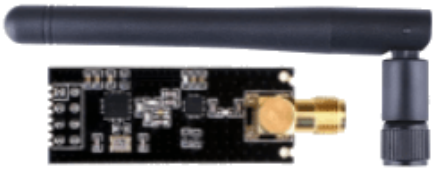
APERÇU	MODELE	PORTEE en MILIEU « CLOS »	PORTEE en « PLEIN AIR »
	NRF24L01+	~ 25 m	~ 50 m
	NRF24L01+ PA LNA	~ 50 m	~ 400 m

Tableau III-1 : Les Versions du nRF24L01

4.1 Caractéristiques du NRF24L01 (avec ou sans antenne)

4.1.1 Fréquence de Transmission (2,4 GHz et plus):

Le NRF24L01 est prévu pour fonctionner dans la plage de 2,4 GHz à 2,525 GHz, par « pas » de 1 MHz. Chaque pas de 1 MHz est ce qu'on appelle ici un canal. Du coup, on dispose ici de 126 canaux, permettant de communiquer sur la fréquence de notre choix, entre 2,4 à 2,525 MHz.

№ Canal	FREQUENCE DE TRANSMISSION
Canal 0	2,400 GHz
Canal 1	2,401 GHz
Canal 2	2,402 GHz
……	……..
Canal 124	2,524 GHz
Canal 125	2,525 GHz

Tableau III-1 : Fréquence de Transmission

4.1.2 Vitesse de Transmission des Données, par Radio

Le nRF24 permet la transmission de données à vitesse plus ou moins rapide, selon ses besoins, et la portée que l'on souhaite atteindre. Par défaut, nous avons le choix entre trois valeurs possibles :

- Vitesse de 250 kbps (vitesse la plus lente, qui « porte » le plus loin)
- Vitesse de 1 Mbps
- Vitesse de 2 Mbps (vitesse la plus rapide, qui « porte » le moins loin)

4.1.3 Brochage (NRF24L01+ pinout)

Qu'il s'agisse du « nRF24L01+ » ou du « nRF24L+01 PA LNA », ils sont tous deux équipés d'un connecteur à 8 broches. Celui-ci comprend deux choses : l'alimentation du module en lui-même, et les broches de communication, pour dialoguer avec lui.

Voici comment cela se présente pour le NRF24L01+ (version avec antenne intégrée au PCB) :

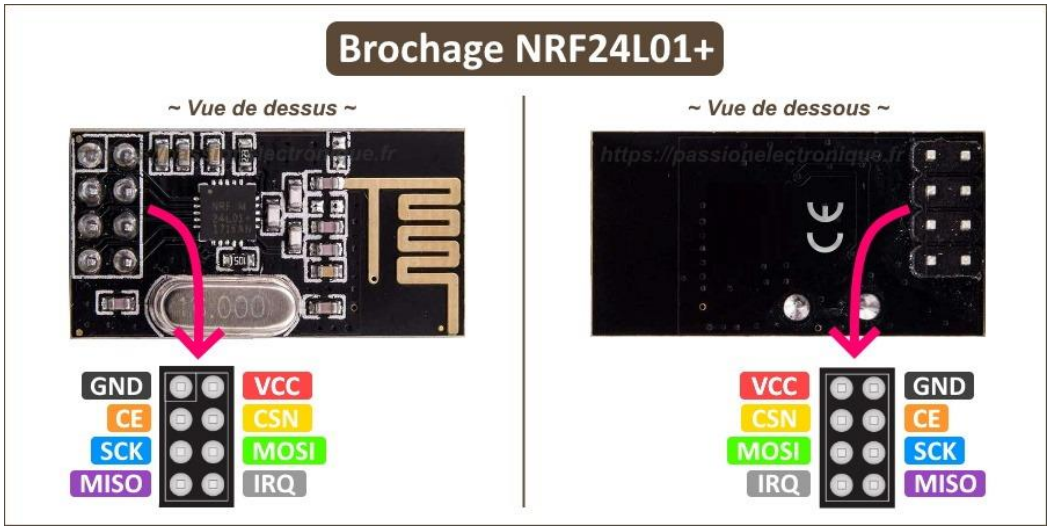


Figure III-3 : Brochage du NRF24L01

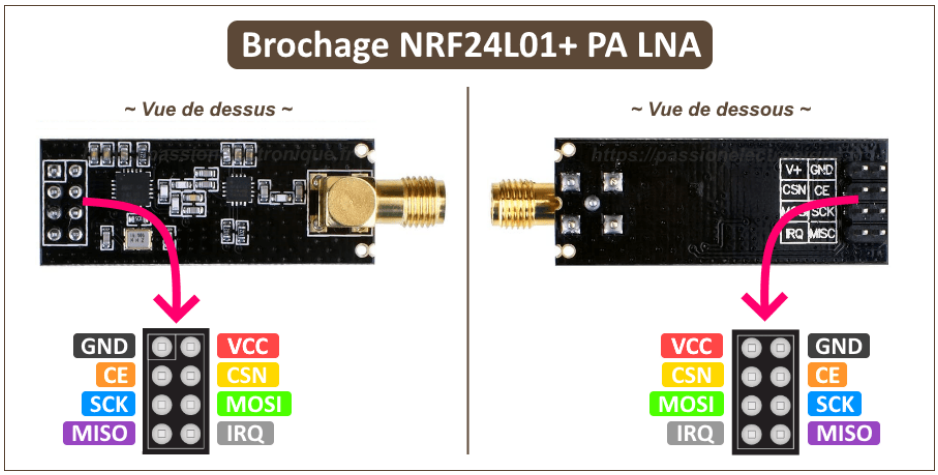


Figure III-4 : Brochage du NRF24L01+PA+LNA

Broche	Signification	Rôle
VCC	-	Alimentation du module (1,9 et 3,6 V)
GND	-	Alimentation du module (0 V)
SCK	Serial ClocK	Horloge communication SPI
MISO	Master In Slave Out	Voie de communication nRF24 ->arduino
MOSI	Master Out Slave In	Voie de communication arduino -> nRF24
CE	Chip Enable	Active le mode RX ou TX (émission / réception)
CSN	Chip Select Not	Active le module nRF24, lorsque mis à la masse (port SPI)
IRQ	InterruptReQuest	Permet d'interagir avec un microcontrôleur, si besoin

Tableau III-2:Brochage du NRF24L01

4.1.4 Alimentation Electrique du Module NRF24L01

Les modules nRF24L01 fonctionnent avec une tension d'alimentation entre 1,9 et 3,6 V, et ils sont souvent alimentés par du 3,3 V. Toutefois, si cette tension provient directement d'un Arduino, il y a un risque que les pics de courant, notamment lors des émissions de données, fassent chuter cette tension. Pour éviter cela, il est recommandé d'ajouter un condensateur de 10 µF aux bornes d'alimentation du module nRF24, afin de lisser la tension.

Si la puce nRF24 est configurée pour émettre à pleine puissance, il est préférable de ne pas utiliser l'alimentation de l'Arduino, car cela pourrait entraîner des problèmes de stabilité. Dans ce cas, il est conseillé d'utiliser des cartes d'alimentation intermédiaires pour garantir une alimentation stable à 3,3V.

En résumé, il faut :

- Ajouter un condensateur électrolytique (10 à 100 µF) pour lisser la tension si la puissance d'émission est faible.

- Utiliser une carte d'alimentation intermédiaire si la puissance d'émission est moyenne ou élevée.

Cela permet de garantir un fonctionnement stable et fiable du module nRF24L01.



Figure III-5 : Condensateur d'Alimentation

5. Le Logiciel et le Langage Arduino

Le langage Arduino se distingue des langages utilisés dans l'industrie de l'informatique embarquée de par sa simplicité. En effet, beaucoup de librairies et de fonctionnalités de base occulte certains aspects de la programmation de logiciel embarquée afin de gagner en simplicité. Cela en fait un langage parfait pour réaliser des prototypes ou des petites applications.

La carte **ESP32 WROOM32 E** peut se programmer de plusieurs façons :

- Avec des scripts Lua, interprétés ou compilés, avec le firmware NodeMCU
- En C++, avec l'IDE Arduino
- En JavaScript, avec le firmware Espruino
- En MicroPython, avec le firmware Micro Python.

5.1 Présentation du Logiciel IDE Arduino

Un IDE (environnement de développement) libre et gratuit est distribué sur le site d'Arduino (compatible Windows, Linux et Mac) à l'adresse http://arduino.cc/en/main/software. D'autres alternatives existent pour développer l'Arduino (extensions pour Code Blocks, Visual Studio, Eclipse, etc.) mais nous n'aborderons dans le chapitre suivant que l'IDE officiel.

L'interface de l'IDE Arduino est plutôt simple (Figure 2.11), il offre une interface minimale et épurée pour développer un programme sur les cartes Arduino. Il est doté d'options de

configuration du logiciel (1) et de boutons pour la programmation des cartes (2).On retrouvent aussi un éditeur de code (3) plus classique qui est utilisé pour accéder aux fonctions avancées de l'IDE. Enfin, une console/débogueur(4) affichant les résultats de la compilation du code source, des opérations sur la carte.

5.1.1 L'Interface

L'interface du logiciel Arduino se présente de la façon suivante :

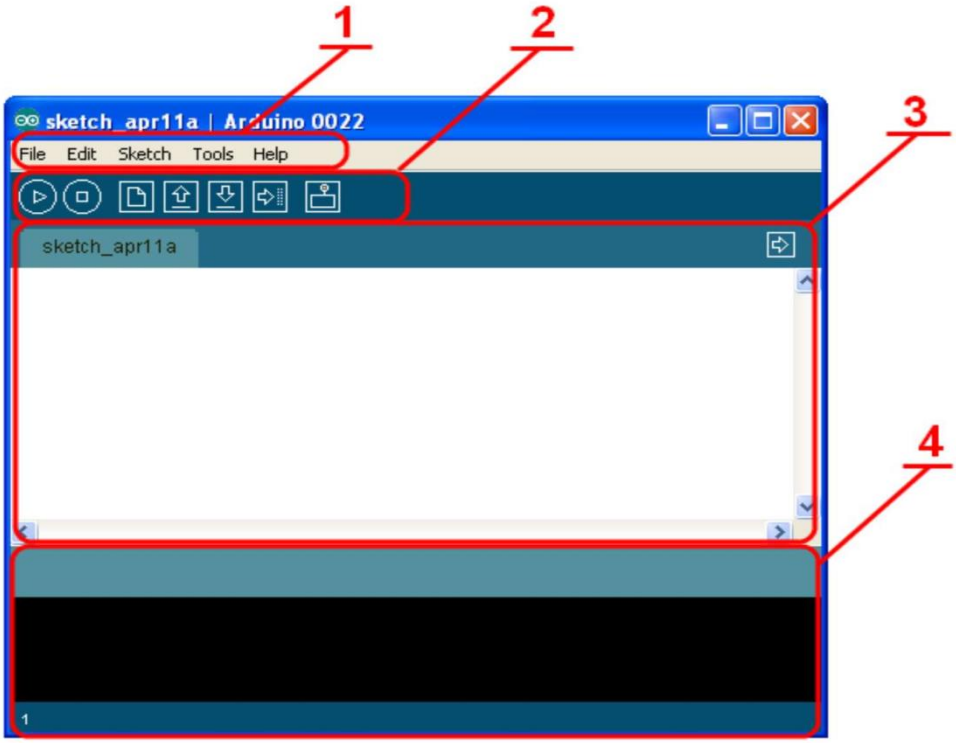


Figure III-6 : Interface logiciel Arduino

Le menu Fichier dispose d'un certain nombre de choses qui vont être très utiles :

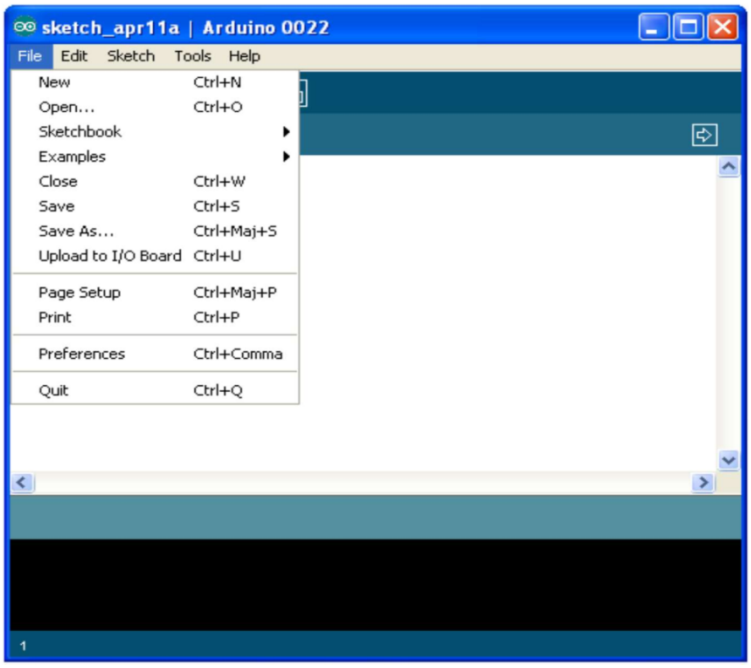


Figure III-7 : Menu Fichier

• New (nouveau) : va permettre de créer un nouveau programme. Quand on appuie sur ce bouton, une nouvelle fenêtre, identique à celle-ci, s'affiche à l'écran.

• Open... (Ouvrir) : avec cette commande, on peut ouvrir un programme existant.

• Save / Save as... (enregistrer / enregistrer sous..) : enregistre le document en cours/demande ou enregistrer le document en cours.

•Exemples: ceci est important, toute une liste se déroule pour afficher les noms d'exemples de programmes existant.

5.1.2 Les Boutons

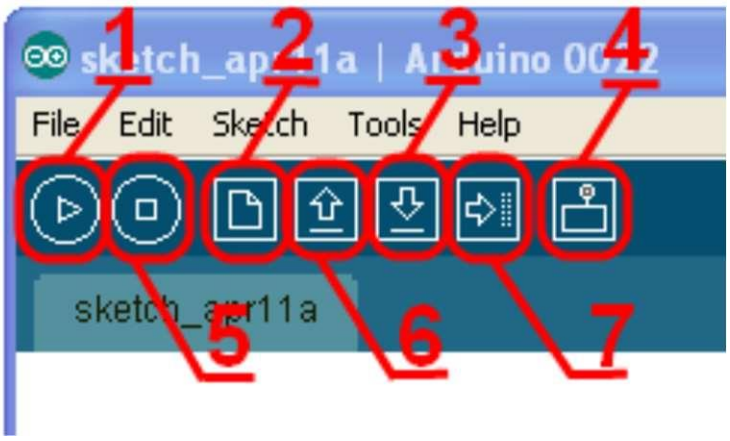


Figure III-8 : Les Boutons

1. Permet de vérifier le programme, il actionne un module qui cherche les erreursdans le programme.
2. Créer un nouveau fichier
3. Sauvegarder le programme en cours
4. Liaison série
5. Stoppe la vérification
6. Charger un programme existant
7. Compiler et envoyer le programme vers la carte.

5.1.3 Présentation du Langage Arduino

Le projet Arduino était destiné à l'origine principalement à la programmation multimédia interactive en vue de spectacle ou d'animations artistiques. C'est une partie de l'explication de la descendance de son interface de programmation de Processing.

Le Processus est une librairie java et un environnement de développement libre. Le logiciel fonctionne sur Macintosh, Windows, Linux, BSD et Android.

5.2.1 Programmation de la Carte ESP32 WROOM32 E

Pour installer la carte ESP8266 dans l'IDE Arduino, suivre les instructions suivantes : Dans l'IDE Arduino, allez dans **Fichier** >**Préférences**

On appui sur Entrez, nous visualisons la fenêtre, puis on sélectionne l'URL : **https://dl.espressif.com/dl/package_esp32_index.json**dans le champ « URL du gestionnaire de cartes supplémentaires », comme indiqué dans la figure ci-dessous. Cliquez ensuite sur le bouton « OK » :

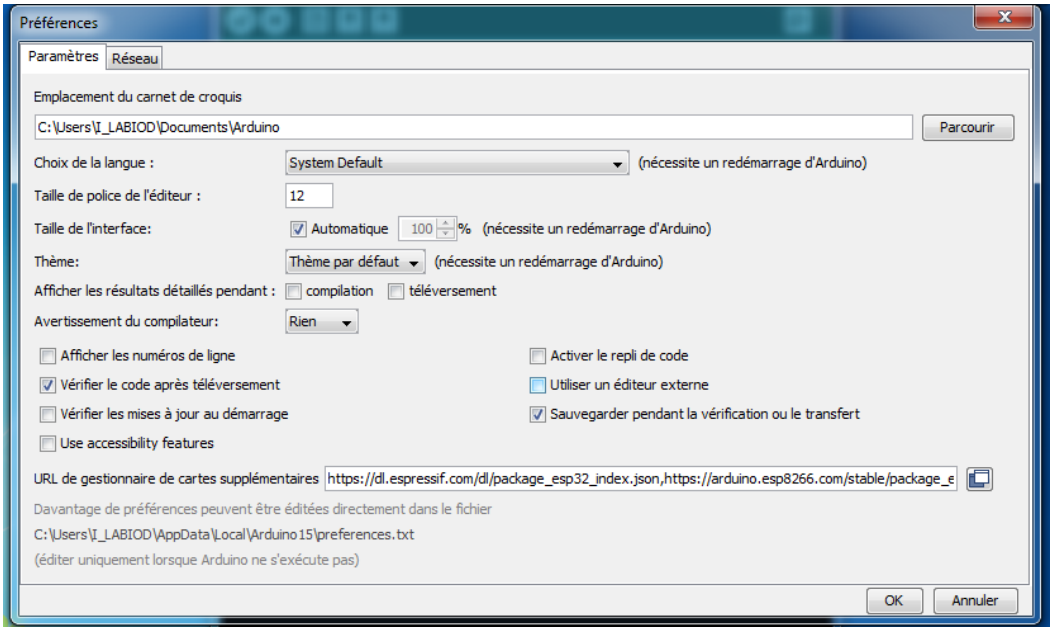


Figure III-9 : Préférences

On ouvre le gestionnaire de cartes, Allez dans **Outils** >**Tableau** >**Gestionnaire de carte** On choisit le module ESP32 Dev Module

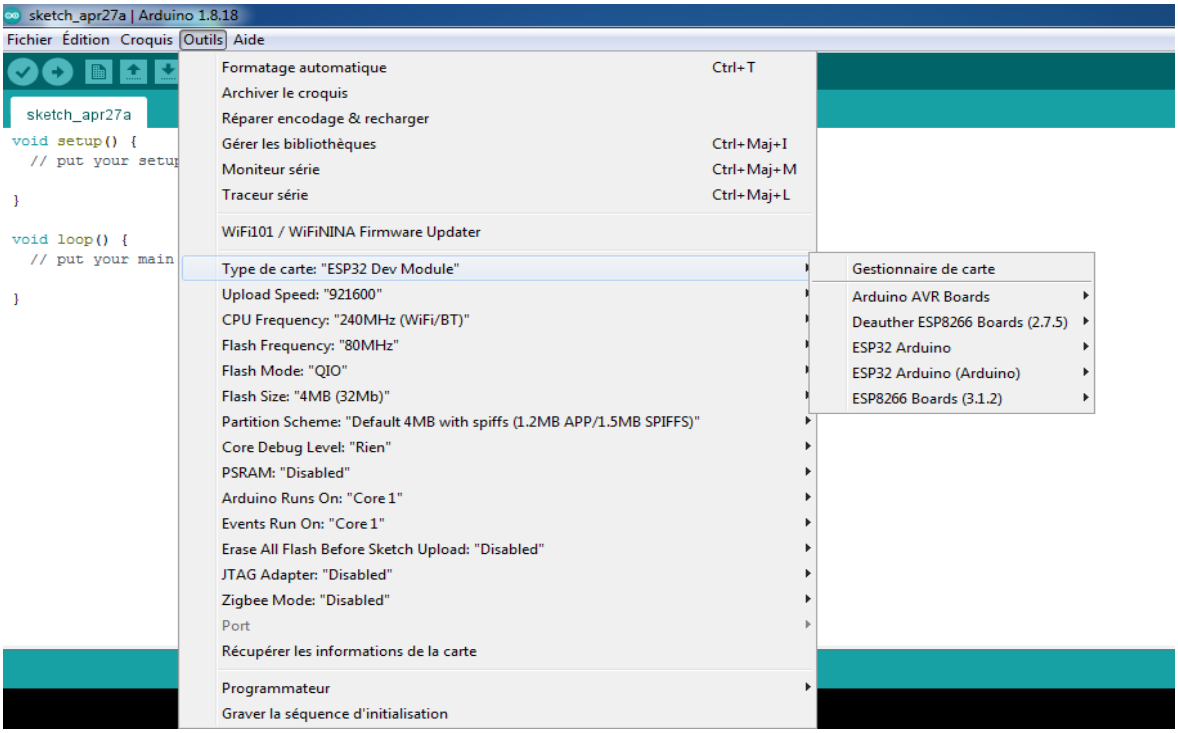


Figure III-10:Choix de la Carte ESP32

Ouvrir le gestionnaire de cartes et rechercher ESP32 et appuyer sur le bouton d'installation pour la " **Communauté ESP32**» tout de suite il sera installé.

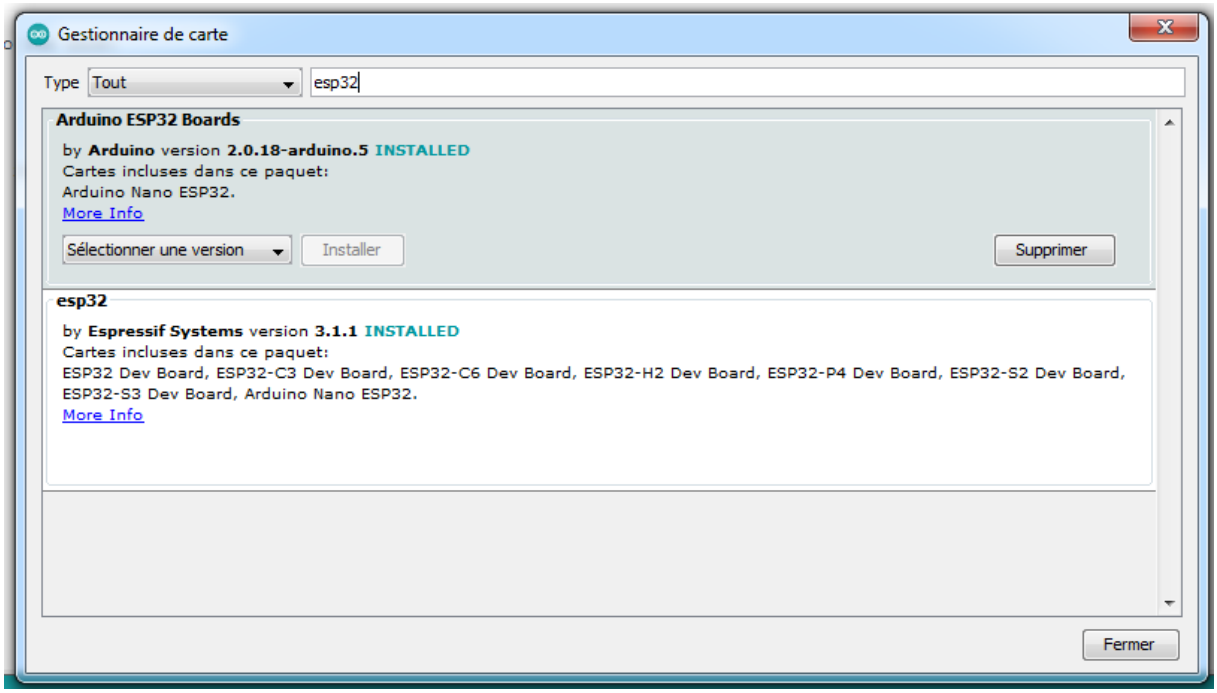


Figure III-11 : Installation Bibliothèque ESP32

5.2.2 La Librairie Utilisée Pour Piloter le NRF24L01

Avant tout, il sera nécessaire d'installer la librairie nRF24, disponible dans le gestionnaire de bibliothèque, de votre IDE Arduino. Pour cela, il vous suffit d'ouvrir cette fenêtre (depuis Arduino IDE -> Menu Outils -> Gérer les bibliothèques), et de taper NRF24 dans la zone de recherche.

Ensuite, il ne vous restera plus qu'à sélectionner le package ayant comme sous-titre « by TMRh20 », et de cliquer sur « Installer » (attention à ne pas vous tromper avec tous les autres noms de package, comme le nRF24 Ethernet, ou le nRF24 Network, qui sont seulement complémentaires, et prévu pour d'autres usages). Voici d'ailleurs ce que vous devriez avoir à l'écran, avec le « bon » package visible au milieu :

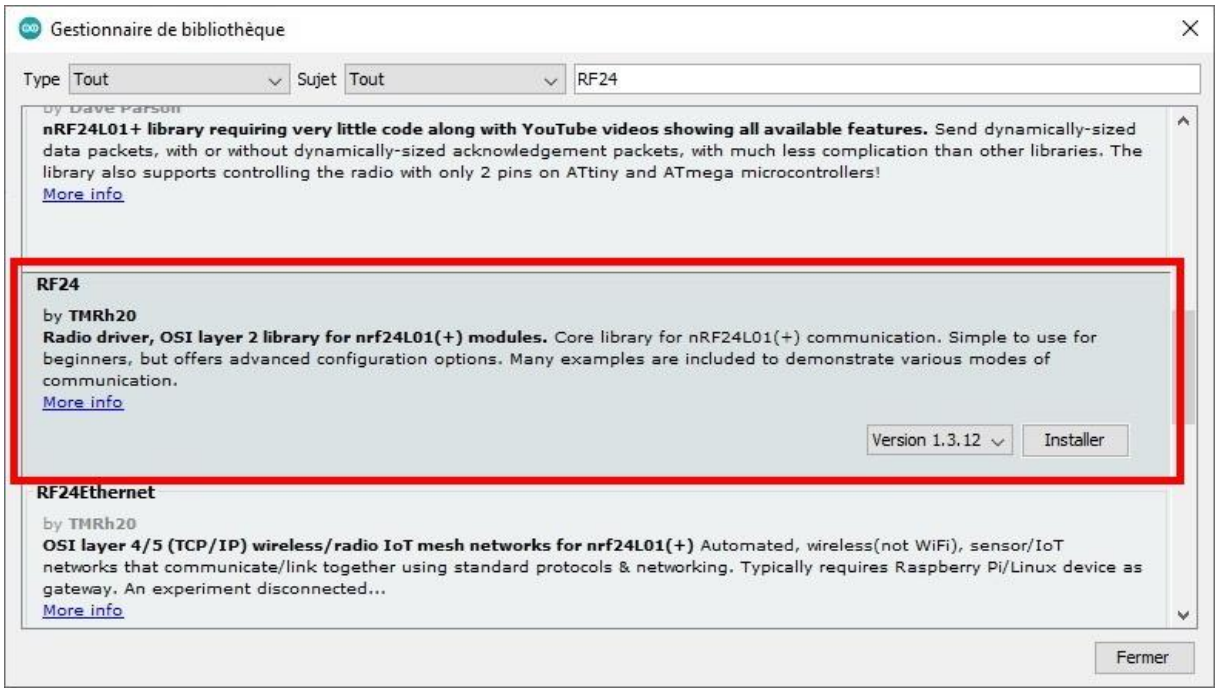


Figure III-12 : Installation Bibliothèque RF24

6. Les Travaux Réalisés

6.1 Utilisations un Seul Module nRF24l01

Au début du projet, j'ai utilisé une carte **ESP32 WROOM-32E** associée à un module sans fil **NRF24L01**. Cette combinaison m'a permis d'exploiter les capacités de communication rapide et flexible de l'ESP32 pour contrôler le module NRF24L01 et générer les signaux nécessaires au brouillage.

L'ESP32 offre également la possibilité d'utiliser l'un de ses deux bus SPI matériels, **HSPI** ou **VSPI**, pour interfacer facilement un seul module NRF24L01, ce qui permet une grande flexibilité dans le choix des broches et des performances optimales.

Ensuite, j'ai développé le code adapté pour configurer et piloter les modules. Après l'implémentation, j'ai procédé à l'analyse des résultats obtenus afin d'évaluer l'efficacité du brouillage réalisé.

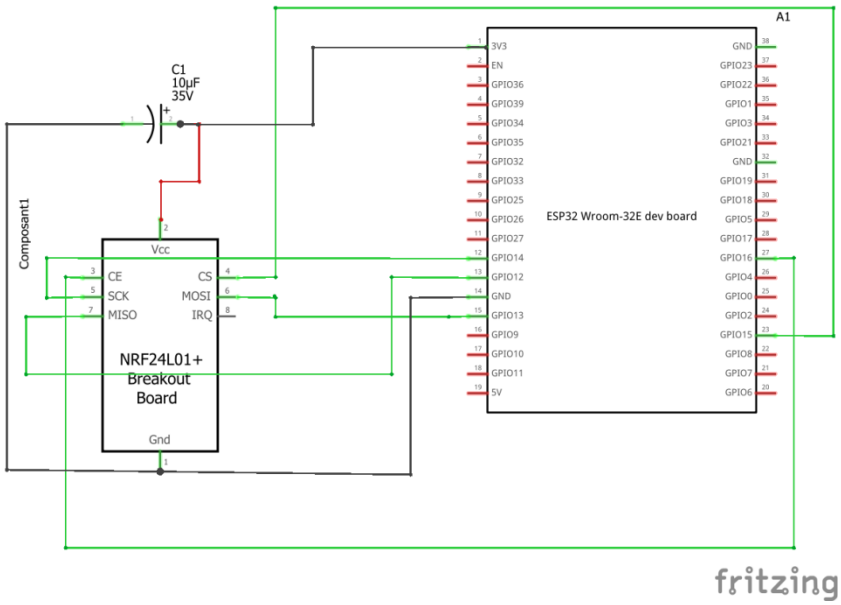


Figure III-13 : Schéma Electrique ESP32+Un NRF24L01

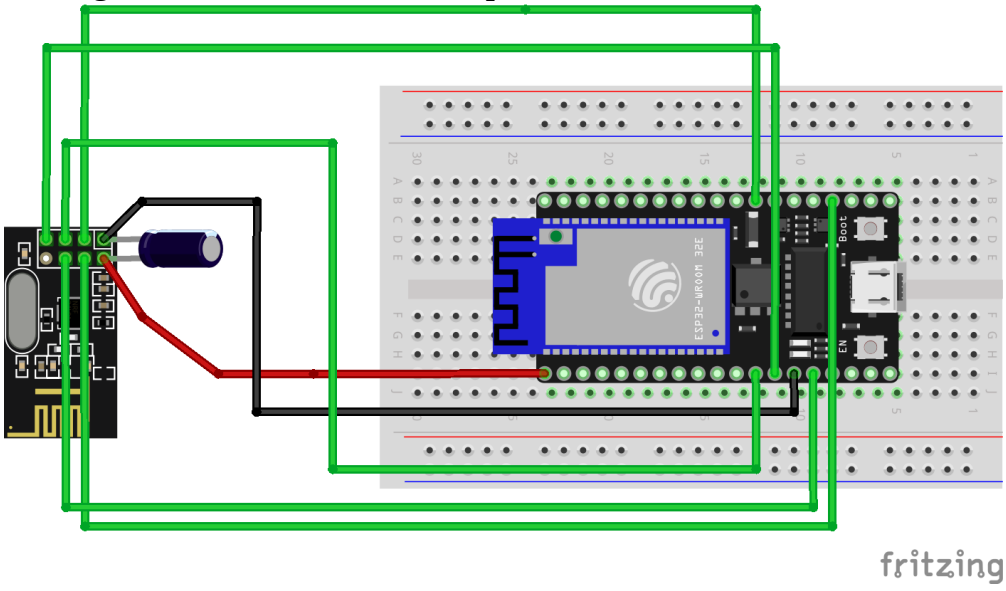


Figure III-14 : Plaque d'Essai ESP32+Un NRF24L01

6.1.1 Le Code Utilisé pour UnNRF24L01 : voir Annexe I

6.1.2 Résultats Attendus Avec un Seul Module NRF24L01 :

a. Sur les Réseaux Wi-Fi (2,4 GHz) :

- On observe que :

- Certains réseaux Wi-Fi deviennent inaccessibles ou leur connexion devient très lente.
- L'appareil peut rester connecté au réseau mais sans accès à Internet ("Connecté - Pas d'Internet").
- Certains points d'accès peuvent redémarrer ou tenter de se reconnecter automatiquement.
- L'effet est particulièrement visible sur les réseaux ouverts ou faiblement sécurisés (WEP/WPA).

Cela s'explique par l'émission continue d'un signal de porteuse forte, provoquant un **brouillage fréquentiel** (brouillage large bande) des canaux Wifi.

b. Sur les Connexions Bluetooth :

- L'effet du brouillage est moins visible que sur le Wi-Fi.
- On remarque :
  - Des coupures intermittentes dans la connexion entre les appareils.
  - Une augmentation de la latence (temps de réponse) lors des communications Bluetooth.
  - Des échecs lors de la tentative d'appairage (connexion initiale).

Cela est dû au fait que le Bluetooth utilise une technique de **saut de fréquence rapide (FHSS)**, changeant de canal 1600 fois par seconde, ce qui le rend plus résistant aux brouillages continus.

c. Analyse Complémentaire :

- Plus le module NRF24L01 est proche du routeur Wi-Fi ou des appareils Bluetooth, plus l'effet de brouillage est fort.
- L'utilisation de plusieurs modules NRF24L01 sur différentes fréquences augmente l'efficacité du brouillage.
- La configuration optimale inclut :
  - Puissance maximale (RF24_PA_MAX)
  - Désactivation du CRC et de l'AutoAck.
- Le type de brouillage utilisé est **proactif**, c'est-à-dire qu'on émet continuellement sans attendre la présence d'une cible.

6.2 Ajout d'un Deuxième Module NRF24L01

Après avoir réalisé les premiers tests avec un seul module NRF24L01, nous avons décidé d'ajouter un **deuxième module** afin d'augmenter l'efficacité du brouillage sur l'ensemble de la bande 2,4 GHz.

6.2.1 Objectif :

- Étendre la couverture de brouillage.
- Balayer plusieurs canaux simultanément.
- Perturber plus efficacement les communications Wi-Fi et Bluetooth.

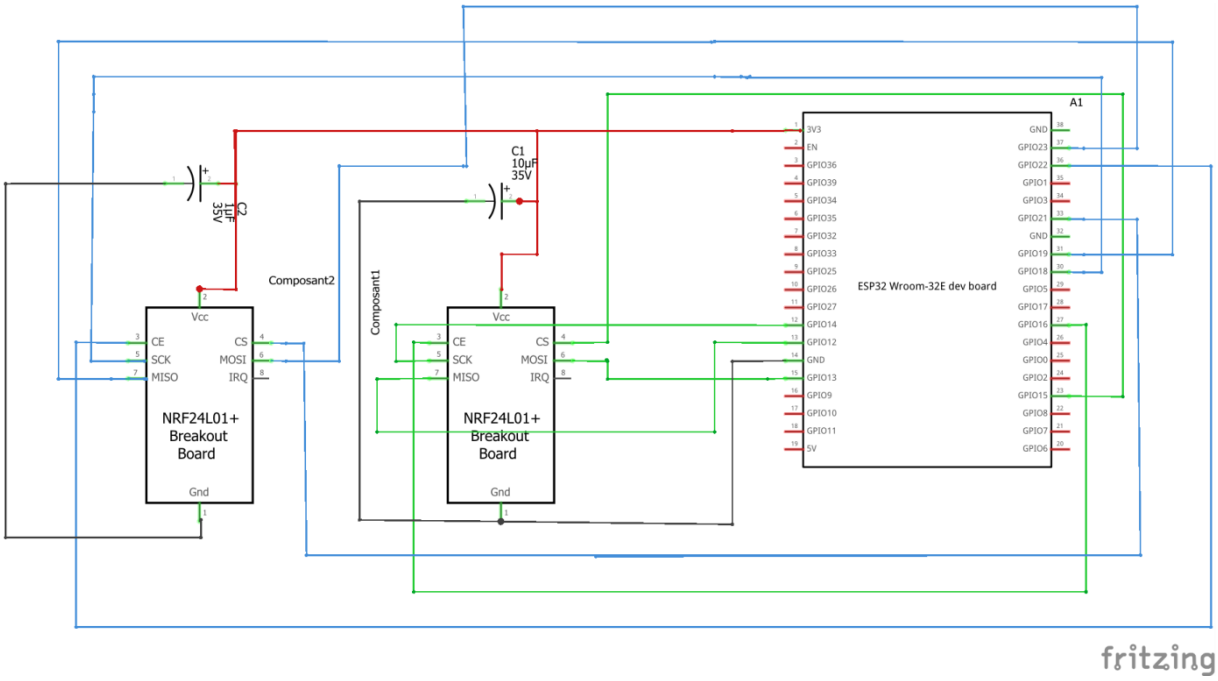


Figure III-15 : Schéma Electrique ESP32+Deux NRF24L01

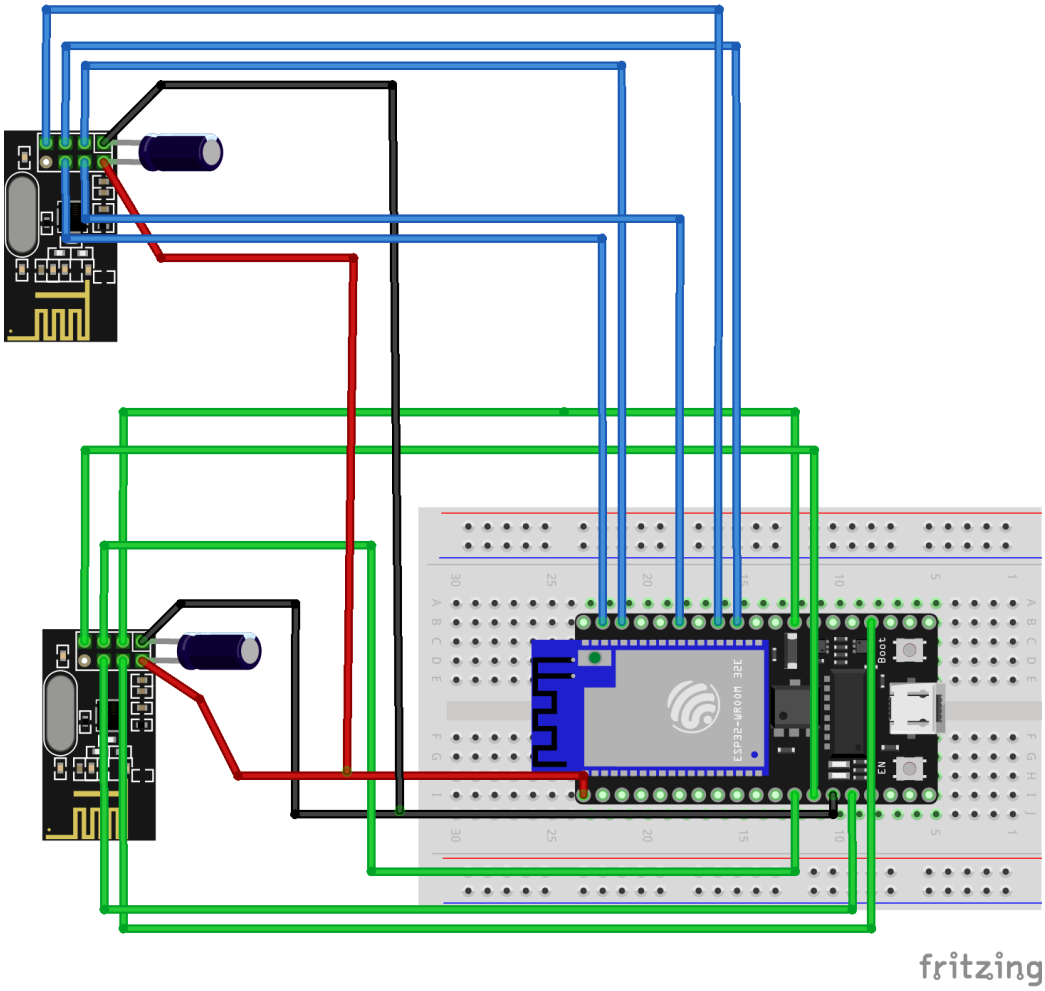


Figure III-16 : Plaque d'Essai ESP32+Deux NRF24L01

6.2.2Le Code Utilisé pour Deux NRF24L01 : voir Annexe II

6.2.3 Résultats Attendus Avec Deux modules NRF24L01:

a. Sur les réseaux Wi-Fi (2,4 GHz) :

Avec deux modules NRF24L01, l'effet du brouillage devient nettement plus sévère. Le réseau devient pratiquement inutilisable, même en se plaçant à proximité immédiate du point d'accès. Les tentatives de connexion échouent dans la majorité des cas, et les périphériques montrent souvent des erreurs de type « Impossible de se connecter au réseau » ou restent bloqués en mode de reconnexion.

Cette augmentation d'efficacité s'explique par la couverture de plusieurs canaux simultanément grâce aux deux modules, réduisant les chances pour le Wi-Fi d'opérer sur un canal "propre". Le brouillage devient ainsi plus dense et plus étendu sur la bande des 2,4 GHz.

b. Sur les Connexions Bluetooth :

Le brouillage devient également beaucoup plus efficace. Les liaisons Bluetooth sont fortement perturbées :

- L'appairage devient difficile, voire impossible dans certains cas.
- Les connexions établies présentent des pertes fréquentes ou sont interrompues brutalement.
- La latence augmente significativement, rendant certaines applications (audio, transfert de fichiers) inutilisables.

Même si le Bluetooth utilise encore le saut de fréquence (FHSS), le fait d'avoir deux émetteurs augmente les chances d'interférer avec les fréquences visitées par le protocole Bluetooth.

c. Analyse Complémentaire :

- L'ajout d'un second module NRF24L01 double les sources de perturbation et améliore l'efficacité sans nécessiter une augmentation de puissance par module.
- Il est possible de configurer chaque module pour couvrir un ensemble de canaux différents (ex : l'un balaye les canaux pairs, l'autre les impairs), ce qui augmente l'efficacité du brouillage proactif.
- Le Wi-Fi, particulièrement sur les réseaux domestiques ou publics non optimisés, est presque totalement paralysé.
- Le Bluetooth devient instable, bien que certaines communications puissent toujours passer si le canal n'est pas couvert à l'instant donné.

6.2.4 Conclusion :

L'ajout d'un deuxième **NRF24L01** a permis d'augmenter significativement l'efficacité du brouillage **proactif**, affectant non seulement la bande Wi-Fi principale (2,4 GHz) mais aussi les canaux utilisés par la majorité des dispositifs Bluetooth.

6.3 Ajout d'un Troisième Module NRF24L01

Après avoir constaté une amélioration notable avec deux modules, nous avons décidé d'ajouter un **troisième module NRF24L01** pour optimiser encore plus le brouillage du spectre 2,4 GHz.

6.3.1Objectif :

- Couvrir un plus grand nombre de canaux simultanément.

- Augmenter la densité du signal de brouillage.
- Rendre le Wi-Fi et le Bluetooth pratiquement inutilisables dans la zone ciblée.

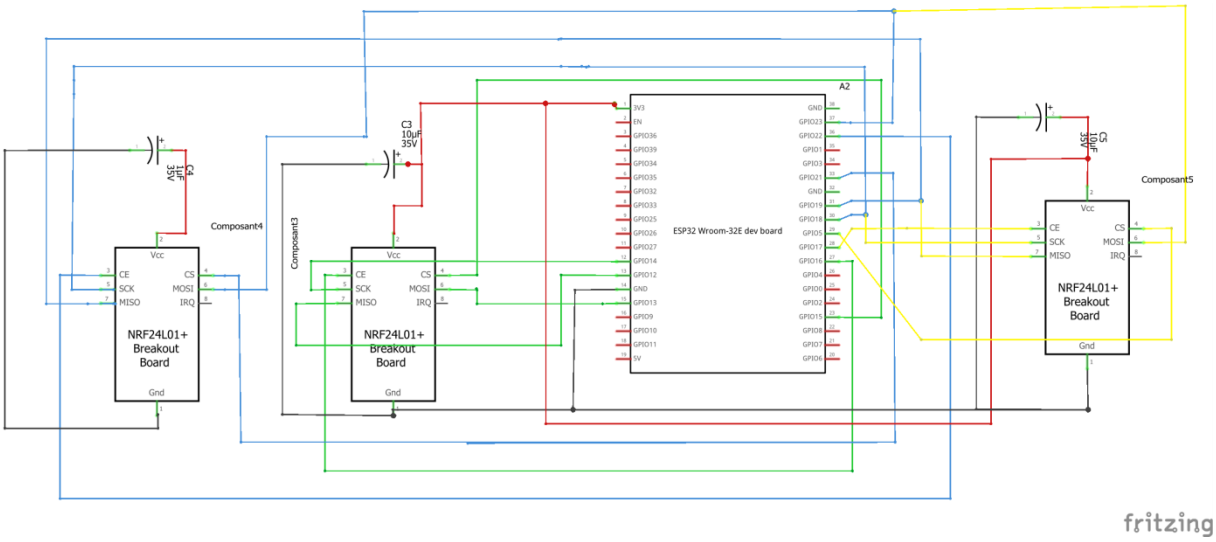


Figure III-17 : Schéma Electrique ESP32+Trois NRF24L01

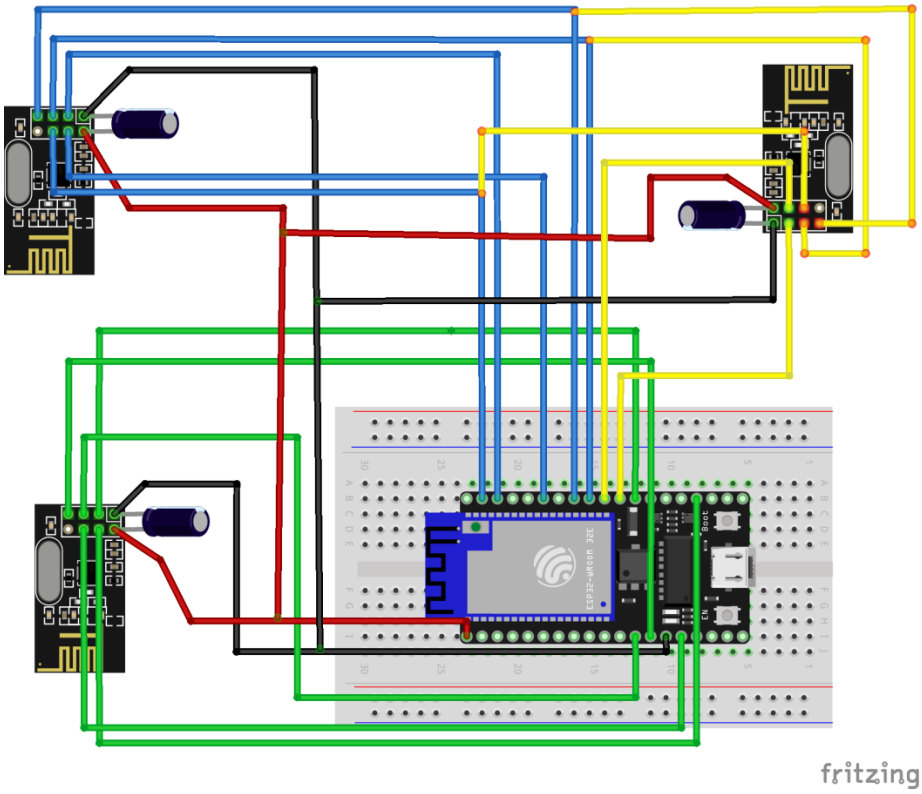


Figure III-18 : Plaque d'Essai ESP32+Trois NRF24L01

6.3.2 Le Code Utilisé pour Trois NRF24L01 : voir Annexe III

6.3.3 Résultats Attendus Avec Trois Modules NRF24L01 :

- **Wi-Fi** : Le réseau devient complètement inutilisable. Les appareils ne détectent même plus les points d'accès dans certains cas.
- **Bluetooth** : Le brouillage est total. Les tentatives d'appairage échouent systématiquement, et aucun transfert de données n'est possible.
- **Spectre 2,4 GHz** : L'occupation du spectre est désormais quasi-constante, empêchant tout type de communication sans fil classique.

6.3.4Conclusion :

L'utilisation de trois modules **NRF24L01**, chacun configuré pour couvrir différentes parties du spectre ou balayer les canaux rapidement, permet d'obtenir un **brouillage proactif** extrêmement efficace sur l'ensemble de la bande 2,4 GHz.

Ce montage s'est révélé très performant pour perturber aussi bien les réseaux **Wi-Fi** que les dispositifs **Bluetooth** dans un périmètre donné.

6.4 Analyse Finale des Tests :

L'augmentation progressive du nombre de modules NRF24L01 a permis d'améliorer de manière significative l'efficacité du brouillage, tant sur les réseaux Wifi que Bluetooth.

Avec un seul module, les effets étaient perceptibles mais limités. L'ajout d'un deuxième puis d'un troisième module a renforcé la couverture des canaux radio et la densité des signaux parasites, rendant le brouillage plus efficace et plus stable.

L'utilisation du **mode proactif** (brouillage continu sans écoute préalable) combinée aux capacités de l'**ESP32 WROOM-32E** (gestion parallèle sur HSPI et VSPI) a joué un rôle déterminant dans l'amélioration globale des performances.

6.5 Description du Prototype Final – Brouilleur 2.4 GHz

Le prototype final réalisé présente une conception fonctionnelle, compacte et orientée vers l'expérimentation. Il intègre les composants suivants:

➢ Alimentation : Deux batteries Li-ion 18650 (3.7 V) connectées en série fournissent une tension totale de 7.4 V, garantissant une autonomie suffisante pour les essais en environnement mobile.

➢ Régulation de tension : Un régulateur LM317T a été utilisé pour abaisser la tension d’alimentation à un niveau adapté aux besoins de l’ESP32 et des modules NRF24L01. Ce choix a été motivé par l’indisponibilité temporaire de régulateurs plus efficaces, tout en assurant une alimentation stable durant les tests.

- Modules d'émission : Trois modules NRF24L01 avec antenne externe sont connectés au microcontrôleur ESP32 WROOM-32E via trois bus SPI indépendants (SPI, HSPI, VSPI). Cette architecture permet une couverture plus large et simultanée du spectre 2,4 GHz, augmentant ainsi l'efficacité du brouillage.
- Interrupteur général ON/OFF : Intégré entre la borne positive des batteries et l'entrée du régulateur LM317T, il permet une gestion simple et sécurisée de l'alimentation du système.
- Conception matérielle : Le montage est effectué sur une plaque perforée de 9 x 15 cm, avec un câblage manuel soigné. L'ensemble reste modulaire, ce qui facilite les ajustements ou réparations durant la phase expérimentale.

Ce prototype répond ainsi aux critères de portabilité, de flexibilité et de performance, indispensables pour les tests en laboratoire comme sur le terrain.

6.5.1Composants non intégrés et Perspectives d'Amélioration

Certaines pièces n'ont pas été intégrées dans cette version du prototype en raison de leur indisponibilité. Leur ajout permettrait cependant d'optimiser considérablement le fonctionnement du système :

- Circuit de charge intelligent (ex. TP4056, BMS 2S) : Il permettrait une recharge sûre et automatique des batteries Li-ion sans démontage, avec protections intégrées contre surcharge, décharge profonde et courts-circuits.
- Régulateur de tension à découpage plus efficace (ex. LM2596 3.3V, AMS1117 3.3V) : Ces régulateurs offriraient un meilleur rendement énergétique et une stabilité accrue, particulièrement utile avec plusieurs modules émetteurs actifs en parallèle.

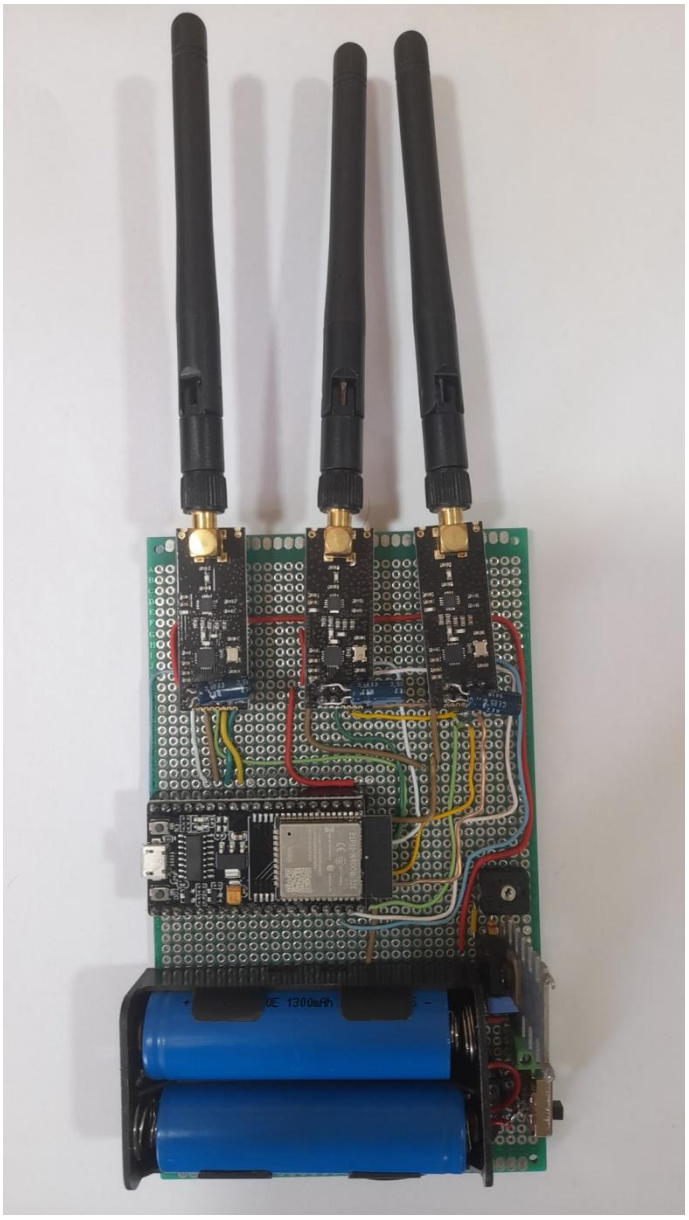


Figure III-19 : Prototype Final

6.5.2 Évolution Attendue du Système Avec ces Ajouts

L'intégration des composants ci-dessus conduirait à une version plus robuste, fiable et adaptée à un usage professionnel :

- ✓ Autonomie améliorée, grâce à une consommation optimisée.
- ✓ Sécurité accrue, en protégeant efficacement les batteries.
- ✓ Utilisation facilitée, avec une recharge directe via USB sans ouvrir le boîtier.
- ✓ Prototype compact et professionnel, prêt pour les démonstrations sur site ou l'intégration dans un système embarqué.

7 Le Projet de Point de vue Commercial

Avec la montée en flèche des moyens de communication sans fil (Wi-Fi, Bluetooth, etc.), les établissements scolaires et universitaires sont de plus en plus confrontés à des cas de triche lors des examens. Des dispositifs discrets comme des écouteurs Bluetooth ou des montres connectées permettent aux étudiants malintentionnés de recevoir de l'aide à distance, compromettant l'intégrité des évaluations.

Notre système de brouillage Wi-Fi/Bluetooth, initialement conçu à des fins expérimentales, possède un fort potentiel commercial en tant que solution de prévention contre la triche électronique. En ciblant spécifiquement les fréquences des technologies utilisées pour la triche (2,4 GHz, typiques du Wi-Fi et Bluetooth), notre appareil empêche efficacement toute communication non autorisée pendant une durée déterminée.

7.1 Applications Pratiques :

- Écoles secondaires : empêcher l'usage de téléphones ou d'écouteurs durant les épreuves.
- Universités : sécuriser les amphithéâtres lors des examens finaux.
- Centres de concours : assurer une équité entre tous les candidats.
- Salles de réunion/conférence : garantir la confidentialité des discussions.

7.2 Avantages du Dispositif Proposé :

- Portable et autonome (grâce à une alimentation sur batterie).
- Sélectif : ne gêne que les bandes spécifiques, sans affecter les réseaux câblés ou autres fréquences.
- Coût réduit, donc accessible aux établissements éducatifs.

7.3 Estimation des Coûts de Réalisation

Composant	Référence	Quantité	Prix unitaire (€)	Prix total (€)
ESP32 Wroom-32E Dev Board	**----**	**1**	**3,00**	**3,00**
Modules NRF24L01+	**-----**	**3**	**1,50**	**4,50**
Condensateurs et résistances	**10µF, 100nF, etc.**		**1,00**	**1,00**
Câblage / Connecteurs			**2,00**	**2,00**
PCB personnalisé (fabrication)	**selon schéma**	**1**	**5,00**	**5,00**
Boîtier imprimé 3D	**ou boîtier ABS**	**1**	**4,00**	**4,00**
Batterie Li-ion + circuit de charge	**3.7V**	**1**	**5,00**	**6,00**
****Total estimé****				**25.50**

Tableau III-4: Estimation des Coûts

Le coût peut varier selon la fabrication en série. Pour une production industrielle (> 100 unités), le prix unitaire pourrait descendre à **10–20 €**.

7.4 Perspectives Commerciales

Le projet peut évoluer vers un **produit commercialisable** sous forme de :

- Dispositif portatif à activer lors des examens.
- Brouilleur à fixer dans des salles d'examen, activable à distance.
- Solution intégrée dans des **valises anti-triche** prêtes à l'emploi.

Une démarche de certification devra cependant être envisagée afin d'assurer la **conformité aux lois nationales** sur l'utilisation des brouilleurs de fréquences, car leur usage est souvent **réglementé ou restreint**.

8. Conclusion

Ce chapitre a détaillé la conception et la réalisation d'un système de brouillage proactif dans la bande des 2,4 GHz (Wi-Fi et Bluetooth), reposant sur un ESP32 WROOM-32E et trois modules NRF24L01. L'exploitation des interfaces SPI (HSPI et VSPI) a permis de faire fonctionner plusieurs modules simultanément, augmentant ainsi l'efficacité du brouillage à chaque étape du développement.

Les tests ont montré que :

- Le Wi-Fi devient inutilisable dès deux modules actifs.
- Le Bluetooth, plus résistant, est fortement perturbé avec trois modules.
- Le mode proactif d'émission continue s'est révélé simple et efficace.

Le prototype final est resté modulaire, économique et évolutif. Des améliorations sont envisageables (alimentation, recharge, régulation) pour un usage plus professionnel. Enfin, le projet présent un fort potentiel commercial, notamment dans la lutte contre la triche électronique dans les établissements scolaires et universitaires.

Conclusion Générale

À travers cette étude structurée en trois chapitres complémentaires, nous avons pu explorer en profondeur l'univers des réseaux sans fil, les menaces auxquelles ils sont exposés, ainsi que les solutions pratiques pour concevoir un système de brouillage ciblé, économique et fonctionnel.

Le premier chapitre a permis de poser les fondations théoriques indispensables, en présentant les principes de fonctionnement des technologies Wi-Fi et Bluetooth, les normes associées, les fréquences utilisées ainsi que les protocoles de sécurité. Cette compréhension fine des couches physiques et logiques était essentielle pour identifier les vulnérabilités exploitables par un brouillage.

Dans le deuxième chapitre, nous avons étudié les différentes techniques de brouillage (proactif, réactif, hybride, etc.) en insistant sur leurs caractéristiques techniques, leur efficacité énergétique, et les méthodes de détection ou d'évitement. Cette analyse a mis en évidence la diversité des stratégies disponibles pour perturber les communications sans fil, et a justifié le choix du brouillage proactif pour notre implémentation.

Enfin, le troisième chapitre a concrétisé la partie pratique du projet en concevant un prototype fonctionnel basé sur un ESP32 WROOM-32E et **trois modules NRF24L01, capables d'émettre des signaux de brouillage sur l'ensemble de la bande 2,4 GHz. Grâce à l'utilisation parallèle des bus HSPI et VSPI, nous avons pu maximiser l'efficacité du brouillage, tout en conservant un design modulaire, portable et à faible coût.

Les résultats expérimentaux ont confirmé l'impact significatif de notre solution sur les réseaux Wi-Fi (rendus inopérants dès deux modules actifs) et sur le Bluetooth (fortement dégradé avec trois modules). De plus, les perspectives commerciales sont prometteuses, notamment dans les environnements académiques où la prévention de la triche électronique devient un enjeu critique.

En somme, ce travail a démontré la faisabilité d'un système de brouillage simple mais redoutablement efficace, alliant connaissances théoriques, conception électronique et développement embarqué. Des pistes d'amélioration (alimentation optimisée, recharge USB, boîtier sécurisé) sont identifiées pour aboutir à un produit final adapté à des usages professionnels et institutionnels.

Bibliographie

[1] K. Chang, "RF and Microwave Wireless Systems", John Wiley & Sons, 2004.

[2] S.S. Oyewobi, K. Djouani, A.M. Kurien, "A review of industrial wireless communications, challenges, and solutions: A cognitive radio approach", Trans Emerging Tel Tech, Vol.31-9, 2020.

[3] D.Krewski, B. W.Glickman, R. W. Y.Habash, B.Habbick, W. G.Lotz, R. Mandeville, "Recent Advances in Research on Radiofrequency Fields and Health: 2001–2003", Journal of Toxicology and Environmental Health, Part B, Vol. 10-4, 2007.

[4] A.-K. Al Tamimi and R. Jain, "Security in wireless data networks," in Handbook of Security and Networks, vol. 1, World Scientific, 2011, pp. 3–38.

[5] Mathur, P., Raman, S. Electromagnetic Interference (EMI): Measurement and Reduction Techniques. J. Electron. Mater. **49**, 2975–2998 (2020).

[6] https://www.vie-publique.fr/files/rapport/pdf/124000295.pdf

[7] https://rm.coe.int/ok-prems-137322-fra-2512-cmrec-2022-18-et-expose-motifs-web-a5-1-/1680a96148.

[8] E. Bajul," *La tricherie scolaire de la generation Z"*, Mémoire de recherche, Master MEEF Économie Gestion Marketing, Université Toulouse Jean Jaurès, Toulouse, France, 2021.

[9] G. Pelosi, "Historical corner column," in *URSI Radio Science Bulletin*, vol. 2020, no. 374, pp. 83-83, Sept. 2020, doi: 10.23919/URSIRSB.2020.9523814.

[10] G.Falciasecca and B. Valotti, "Guglielmo Marconi: The pioneer of wireless communications," *2009 European Microwave Conference (EuMC)*, Rome, Italy, 2009, pp. 544-546, doi: 10.23919/EUMC.2009.5296358.

[11] « Réseaux sans fil : quels sont-ils, quels types et à quoi servent ces réseaux sans fil ? »,https://stepbystepinternet.com/fr/reseaux-sans-fil-quels-sont-ils-quels-types-et-a-quoiservent-ces-reseaux-sans-fil/, août 2023.

[12] « *Technologie de communication sans fil à courte portée vs technologie de communication sans fil à longue portée »*, https://www.mokosmart.com/fr/short-rangewireless-communication-technology-vs-long-range-wireless-communicationtechnology/, Aout 2023.

[13] « *An overview of the classification of wireless network technologies*", https://www.jakelectronics.com/blog/an-overview-of-the-classification-of-wirelessnetwork-technologies, 2023.

[14] « *Réseau sans-fil : La technologie WiFi*», https://www.bestcours.com/pdf/0115- formation-reseau-wifi.pdf, 2023.

[15] *« Réseau Wifi »*, https://www.tala-informatique.fr/wiki/images/f/f7/WiFi-802.11.pdf, *2023.*

[16] « *Quels sont les différents protocoles de sécurité WIFI* », https://www.jilnetwork.com/2023/05/quels-sont-les-protocoles-de-securite.html

[17] J.-P. Muller, « Bluetooth », [En ligne]. Disponible sur : https://jipehem.fr/cours/l-bluetooth.pdf.

[18]Bluetooth SIG, *Bluetooth Core Specification: Part A – Logical Link Control and Adaptation Protocol (L2CAP)*, Version 5.4, 2023. [En ligne]. Disponible sur : https://www.bluetooth.com/wp-content/uploads/Files/Specification/HTML/Core-54/out/en/host/logical-link-control-and-adaptation-protocol-specification.html.

[19] H. Pirayesh and H. Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey," in *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 767-809, Secondquarter 2022

[20] Xu, W., Trappe, W., Zhang, Y., & Wood, T. (2005). *The feasibility of launching and detecting jamming attacks in wireless networks*. ACM MobiHoc. DOI: 10.1145/1062689.1062697.

[21] Li M, Koutsopoulos I, Poovendran R (2007) Optimaljamming attacks and network defense policiesin wireless sensor networks. In: IEEE 26thIEEE International Conference on ComputerCommunications, pp 1307–1315.

[22] Tague P, Slater D, Poovendran R, Noubir G (2008) Linear programming models for jamming attacks on network traffic flows. 6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops pp 207–216.

[23] Bayraktaroglu E, King C, Liu X, Noubir G, Rajaraman R, Thapa B (2008) On the performance of IEEE 802.11 under jamming. In: IEEE the 27th Conference on Computer Communications, pp 1265–1273.

[24] Wood A, Stankovic J, Son S (2003) JAM: a jammed-area mapping service for sensor networks. In: 24th IEEE Real-Time Systems Symposium, pp 286–297.

[25] L. Zhanget al., "RSVP: A New Resource Reservation Protocol," IEEE Communications Magazine, Vol. 40, No. 5, May 2002, pp 116-127.

[26] Commander CW, Pardalos PM, Ryabchenko V, Shylo OV, Uryasev S, Zrazhevsky G (2008) Jamming communication networks under complete uncertainty. Optimization Letters 2(1):53–70.

[27] Huang H, Ahmed N, Pulluru S (2010) Onlimitedrange strategic/random jamming attacks in wireless ad hoc networks. In: IEEE 34th Conference on Local Computer Networks, pp 1–8.

[28] Gencer C, Aydogan EK, Celik C (2008) A decision support system for locating VHF/UHF radio jammer systems on the terrain. Information Systems Frontiers 10(1):111–124.

[29] Panyim K, Hayajneh T, Krishnamurthy P, Tipper D (2009) Jamming dust: A low power distributed jammer network. In: 27th Army Science Conference, pp 922–929.

Annexe I

Le Code Utilisé pour Un nRF24L01

```
#include "RF24.h"
#include <SPI.h>
#include "esp_bt.h"
#include "esp_wifi.h"
// إعداد SPI
SPIClass *hp = nullptr;
// إعداد NRF24L01 واحد
RF24 radio(16, 15, 16000000);   // CE=16, CSN=15 HSPI
unsignedint flag = 0;
intch = 45;  // بدايةالقناة
voidtwo() {
  if (flag == 0) ch += 2;
elsech -= 2;
  if ((ch> 79) && (flag == 0)) flag = 1;
else if ((ch< 2) && (flag == 1)) flag = 0;
radio.setChannel(ch);
}
void one() {
radio.setChannel(random(80));
delayMicroseconds(random(60));
}
voidsetup() {
Serial.begin(115200);
  // تعطيلالبلوتوثوالوايفاي
esp_bt_controller_deinit();
esp_wifi_stop();
esp_wifi_deinit();
esp_wifi_disconnect();
  // تهيئةواجهة SPI
hp = new SPIClass(HSPI);
hp->begin(14, 12, 13, 15);  // SCK=14, MISO=12, MOSI=13, CSN=15
  if (radio.begin(hp)) {
Serial.println("NRF24L01 Démarré✓");
radio.setAutoAck(false);
radio.stopListening();
radio.setRetries(0, 0);
radio.setPALevel(RF24_PA_MAX, true);
radio.setDataRate(RF24_2MBPS);
radio.setCRCLength(RF24_CRC_DISABLED);
radio.printPrettyDetails();
radio.startConstCarrier(RF24_PA_MAX, ch);
  } else {
Serial.println("Erreur: Impossible de démarrer NRF24L01 ✗");
  }
}
voidloop() {
one();  // لمسحالقنواتتدريجيا two()أويمكنكاستخدام
}
```

Annexe II

Le Code Utilisé pour Deux NRF24L01

```
#include "RF24.h"
#include <SPI.h>
#include "esp_bt.h"
#include "esp_wifi.h"
SPIClass *sp = nullptr;
SPIClass *hp = nullptr;
RF24 radio(16, 15, 16000000);   //HSPI CAN SET SPI SPEED TO 16000000 BY DEFAULT ITS
10000000
RF24 radio1(22, 21, 16000000);  //VSPI CAN SET SPI SPEED TO 16000000 BY DEFAULT ITS
10000000
//HSPI=SCK = 14, MISO = 12, MOSI = 13, CS = 15 , CE = 16
//VSPI=SCK = 18, MISO =19, MOSI = 23 ,CS =21 ,CE = 22
unsigned int flag = 0;   //HSPI// Flag variable to keep track of direction
unsigned intflagv = 0;  //VSPI// Flag variable to keep track of direction
intch = 45;    // Variable to store value of ch
int ch1 = 45;   // Variable to store value of ch
void two() {
  if (flagv == 0) {  // If flag is 0, increment ch by 4 and ch1 by 1
    ch1 += 4;
  } else {  // If flag is not 0, decrement ch by 4 and ch1 by 1
    ch1 -= 4;
  }
  if (flag == 0) {  // If flag is 0, increment ch by 4 and ch1 by 1
ch += 2;
  } else {  // If flag is not 0, decrement ch by 4 and ch1 by 1
ch -= 2;
  }
  // Check if ch1 is greater than 79 and flag is 0
  if ((ch1 > 79) && (flagv == 0)) {
flagv = 1;                          // Set flag to 1 to change direction
  } else if ((ch1 < 2) && (flagv == 1)) {  // Check if ch1 is less than 2 and flag is 1
flagv = 0;                          // Set flag to 0 to change direction
  }
  // Check if ch is greater than 79 and flag is 0
  if ((ch> 79) && (flag == 0)) {
    flag = 1;                          // Set flag to 1 to change direction
  } else if ((ch< 2) && (flag == 1)) {  // Check if ch is less than 2 and flag is 1
    flag = 0;                          // Set flag to 0 to change direction
  }
radio.setChannel(ch);
  radio1.setChannel(ch1);
  /*Serial.print("SP:");
Serial.println(ch1);
Serial.print("\tHP:");
Serial.println(ch);*/
}
void one() {
  ////RANDOM CHANNEL
  radio1.setChannel(random(80));
radio.setChannel(random(80));
delayMicroseconds(random(60));//////REMOVE IF SLOW
 /*  YOU CAN DO -----SWEEP CHANNEL
  for (inti = 0; i< 79; i++) {
```

```
radio.setChannel(i);
*/
}
void setup() {
Serial.begin(115200);
esp_bt_controller_deinit();
esp_wifi_stop();
esp_wifi_deinit();
esp_wifi_disconnect();
initHP();
initSP();
}
void initSP() {
sp = new SPIClass(VSPI);
sp->begin();
  if (radio1.begin(sp)) {
Serial.println("SP Started !!!");
    radio1.setAutoAck(false);
    radio1.stopListening();
    radio1.setRetries(0, 0);
    radio1.setPALevel(RF24_PA_MAX, true);
    radio1.setDataRate(RF24_2MBPS);
    radio1.setCRCLength(RF24_CRC_DISABLED);
    radio1.printPrettyDetails();
    radio1.startConstCarrier(RF24_PA_MAX, ch1);
  } else {
Serial.println("SP couldn't start !!!");
  }
}
void initHP() {
hp = new SPIClass(HSPI);
hp->begin();
  if (radio.begin(hp)) {
Serial.println("HP Started !!!");
radio.setAutoAck(false);
radio.stopListening();
radio.setRetries(0, 0);
radio.setPALevel(RF24_PA_MAX, true);
radio.setDataRate(RF24_2MBPS);
radio.setCRCLength(RF24_CRC_DISABLED);
radio.printPrettyDetails();
radio.startConstCarrier(RF24_PA_MAX, ch);
  } else {
Serial.println("HP couldn't start !!!");
  }
}
void loop() {
// switch out one() for whatever
one();
}
```

Annexe III

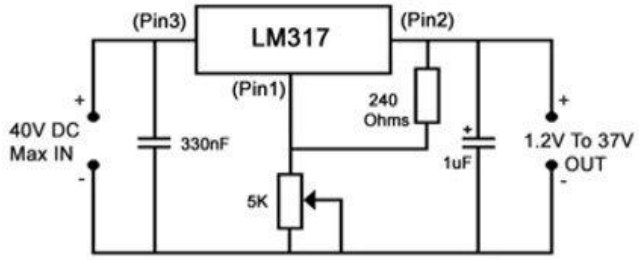
Le Code Utilisé pour Trois NRF24L01

```
#include "RF24.h"
#include <SPI.h>
#include "esp_bt.h"
#include "esp_wifi.h"
SPIClass *sp = nullptr;
SPIClass *hp = nullptr;
RF24 radio(16, 15, 16000000);   // HSPI: CE, CSN
RF24 radio1(22, 21, 16000000);  // VSPI: CE, CSN
RF24 radio2(17, 5, 16000000);   // VSPI: CE, CSN (جديدة)
unsignedint flag = 0;
unsignedintflagv = 0;
intch = 45;
int ch1 = 45;
int ch2 = 45;  // للقناة الثالثة
voidtwo() {
if (flagv == 0) ch1 += 4;
  else ch1 -= 4;
  if (flag == 0) ch += 2;
  else ch -= 2;
ch2 = random(80); // قناة عشوائية للراديو الثالث
if ((ch1 > 79) && (flagv == 0)) flagv = 1;
  else if ((ch1 < 2) && (flagv == 1)) flagv = 0;
  if ((ch> 79) && (flag == 0)) flag = 1;
  else if ((ch< 2) && (flag == 1)) flag = 0;
radio.setChannel(ch);
  radio1.setChannel(ch1);
  radio2.setChannel(ch2);
}
void one() {
radio.setChannel(random(80));
  radio1.setChannel(random(80));
  radio2.setChannel(random(80));
delayMicroseconds(random(60));
}
void setup() {
Serial.begin(115200);
esp_bt_controller_deinit();
esp_wifi_stop();
esp_wifi_deinit();
esp_wifi_disconnect();
initHP();
initSP();
initTHIRD();  // إضافة الراديو الثالث
}
voidinitSP() {
sp = new SPIClass(VSPI);
sp->begin();  // VSPI: 18, 19, 23
  if (radio1.begin(sp)) {
Serial.println("VSPI Started !!!");
```

```
    radio1.setAutoAck(false);
    radio1.stopListening();
    radio1.setRetries(0, 0);
    radio1.setPALevel(RF24_PA_MAX, true);
    radio1.setDataRate(RF24_2MBPS);
    radio1.setCRCLength(RF24_CRC_DISABLED);
    radio1.printPrettyDetails();
    radio1.startConstCarrier(RF24_PA_MAX, ch1);
  } else {
Serial.println("VSPI couldn't start !!!");
  }
}
void initHP() {
hp = new SPIClass(HSPI);
hp->begin();  // HSPI: 14, 12, 13
  if (radio.begin(hp)) {
Serial.println("HSPI Started !!!");
radio.setAutoAck(false);
radio.stopListening();
radio.setRetries(0, 0);
radio.setPALevel(RF24_PA_MAX, true);
radio.setDataRate(RF24_2MBPS);
radio.setCRCLength(RF24_CRC_DISABLED);
radio.printPrettyDetails();
radio.startConstCarrier(RF24_PA_MAX, ch);
  } else {
Serial.println("HSPI couldn't start !!!");
}
}
voidinitTHIRD() {
  // يستخدم نفس VSPI لكن بخط CS و CE مختلفين
  if (radio2.begin(sp)) {
Serial.println("NRF24L01 بدأ الثالث✓");
radio2.setAutoAck(false);
radio2.stopListening();
radio2.setRetries(0, 0);
radio2.setPALevel(RF24_PA_MAX, true);
radio2.setDataRate(RF24_2MBPS);
    radio2.setCRCLength(RF24_CRC_DISABLED);
    radio2.printPrettyDetails();
    radio2.startConstCarrier(RF24_PA_MAX, ch2);
} else {
Serial.println("✗فشل بدء NRF24L01 الثالث");
  }
}
voidloop() {
one();  // أوtwo() لمسح القنوات
}
```

Description and pinout LM317

Application Circuit



Part Number Suffix	Package	Design Load Current
K	TO-3	1.5A
H	**TO-39**	**0.5A**
T	TO-220	1.5A
E	**LCC**	**0.5A**
S	TO-263	1.5A
EMP	SOT-223	1A
MDT	**TO-252**	**0.5A**

TO - 220 Package



ChipDatasheet.com