



UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACSISTEL

INGENIERÍA EN TELECOMUNICACIONES

TRABAJO DE INTEGRACIÓN CURRICULAR

**Desarrollo estratégico de coordinación
lineal entre dos dispositivos RF-Clown
v2 para interferencias sincronizadas
sobre redes Bluetooth/BLE.**

Wilson Fabián Cruz Borbor

Dirigido por:

Ing. Luis Miguel Amaya, M.Sc.

La Libertad - 2026

**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

TRIBUNAL DE SUSTENTACIÓN



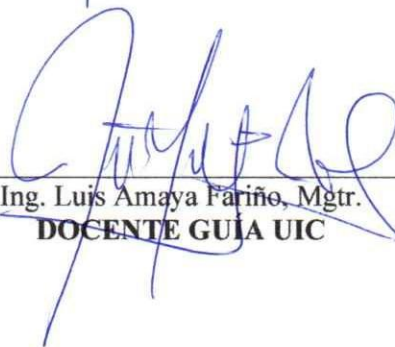
Ing. Ronald Rovira Jurado, Ph.D.
DIRECTOR DE LA CARRERA



Ing. Luis Amaya Fariño, Mgtr.
TUTOR



Ing. Daniel Jaramillo Chamba, Mgtr.
DOCENTE ESPECIALISTA



Ing. Luis Amaya Fariño, Mgtr.
DOCENTE GUÍA UIC



Ing. Corina Gonzabay De La A, Mgtr.
SECRETARIA



**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y la estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por **Wilson Fabián Cruz Borbor**, como requerimiento para la obtención del título de Ingeniero en telecomunicaciones.

La Libertad, a los 10 días del mes de agosto del año 2026



Ing. Luis Amaya Fariña, Mgtr.
DOCENTE TUTOR



**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Wilson Fabián Cruz Borbor**

DECLARO QUE:

Declaro que el trabajo de integración curricular, **DESARROLLO ESTRATÉGICO DE COORDINACIÓN LINEAL ENTRE DOS DISPOSITIVOS RF-CLOWN V2.0 PARA INTERFERENCIAS SINCRONIZADAS SOBRE REDES BLUETOOTH/BLE**, previo a la obtención del título de Ingeniero en Telecomunicaciones, ha sido desarrollado respetando derechos intelectuales de terceros conforme a las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente, este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Integración Curricular referido.

La Libertad, a los 10 días del mes de agosto del año 2026



Wilson Fabián Cruz Borbor
ESTUDIANTE



**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de integración curricular denominado **Desarrollo Estratégico De Coordinación Lineal Entre Dos Dispositivos Rf-Clown V2.0 Para Interferencias Sincronizadas Sobre Redes Bluetooth/Ble**, presentado por el estudiante **Wilson Fabián Cruz Borbor**, fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 01%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



documento curricular2-3

ID : 504f8a81baca33c42cd6c2ad9e6c215879f16954

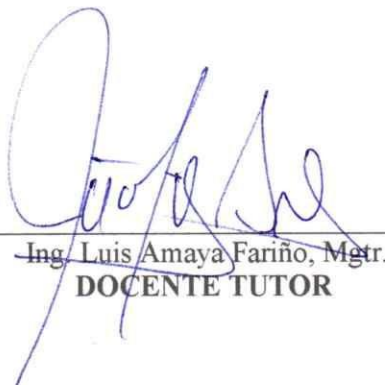


<1%

Textos sospechosos

Nombre del fichero : documento curricular2-3.txt
Tamaño del archivo original : 14.93 MB
Número de palabras : 20.516

Depositante : AMAYA FARIÑO LUIS MIGUEL
Fecha de depósito : 20 de agosto de 2026
Tipo de carga : interface
Fecha de fin de análisis : 20 de agosto de 2026



Ing. Luis Amaya Fariño, Mgr.
DOCENTE TUTOR



**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
AUTORIZACIÓN**

Yo, **Wilson Fabián Cruz Borbor**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de integración curricular o parte de él, un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la **Institución**.

Cedo los derechos en línea patrimoniales de artículo profesional de alto nivel con fines de difusión pública, además apruebo la reproducción de este artículo académico dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 10 días del mes de agosto del año 2026



Wilson Fabián Cruz Borbor
ESTUDIANTE



**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

APROBACIÓN DE DOCENTE ESPECIALISTA

En mi calidad de docente especialista del trabajo de integración curricular denominado **“Desarrollo Estratégico De Coordinación Lineal Entre Dos Dispositivos Rf-Clown V2.0 Para Interferencias Sincronizadas Sobre Redes Bluetooth/Ble”** elaborado por **Wilson Fabián Cruz Borbor** estudiante de la carrera de Telecomunicaciones, Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena, previo a la obtención del título de Ingeniería en Telecomunicaciones me permito declarar que, tras supervisar el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos. En consecuencia, lo considero apto en todos sus aspectos y listo para la sustentación del trabajo.

Ing. Daniel Jaramillo Chamba, Mgtr.
DOCENTE ESPECIALISTA

AGRADECIMIENTO

En primer lugar, a Dios mi guía espiritual a mi padre que, aunque no está presente físicamente en su momento fue un pilar principal dándome apoyo incondicional para mis logros, a mi Madre quien siempre estuvo atenta en mis estudios y nunca dejar de hacerlo porque para mí es el mejor ejemplo a seguir en todo sentido y ella forma parte fundamental en esta etapa de mi vida, a mi esposa y mis hijos porque me dieron fuerzas, ánimo y sobre todo amor cuando hubo momentos difíciles en este periodo de estudios académicos.

A mi tutor el Ing. Luis Amaya Fariño, Mgtr., con sus consejos y guía final en mis estudios, logré llevar a cabo este último esfuerzo de titulación y, sobre todo, por el tiempo que se dedicó a ello con paciencia, dedicación y esfuerzo.

A los docentes que pasaron por todos los semestres de la carrera y me guiaron por el camino de la responsabilidad y de su profesionalidad, por cada enseñanza impartida como logro y experiencia resaltando el compromiso que tiene la universidad con los docentes.

Por último, sin dejar de agradecer a mis amigos a los tres últimos que quedaron desde que iniciamos la carrera y nos comprometimos a terminarla, y por supuesto, al resto de compañeros que de una u otra manera fueron parte también de este proceso.

Wilson Fabián, Cruz Borbor

DEDICATORIA

Dedico muy especialmente este logro a mi querida madre, que, a pesar de la distancia, nunca dejó de estar atenta a mi evolución académica y siempre se preocupó por mí en todo sentido y por darme consejos para ser un profesional de bien, como ella lo es. Por eso es mi inspiración para nunca rendirme, luchar por mis logros y, por ello, obtener este título finalmente.

A mi esposa e hijos, por brindarme todo su amor y por estar conmigo a diario y palpar cada esfuerzo que hice en mi carrera, pues el tiempo que no pude compartir con ellos terminó en una gran recompensa, como es la titulación y, por ende, se convertirá en parte de mi vida profesional, compromiso que tengo que cumplir a cabalidad con ellos.

Mis hermanos, por darme ese empuje para salir adelante y no rendirme, también forman parte de este momento especial de cumplir con mis metas académicas, pues gracias a su unión, como nuestros padres, nos criaron llenos de alegría y con la certeza de que siempre me dieron lo mejor de ellos.

Wilson Fabián, Cruz Borbor

RESUMEN

El presente proyecto desarrolla una estrategia de coordinación lineal entre dos dispositivos RF-Clown v2 para generar interferencias sincronizadas en redes Bluetooth/BLE en la banda ISM de 2,4 GHz. Se adaptó el firmware mediante una arquitectura Maestro–Esclavo, utilizando el protocolo Enhanced ShockBurst (ESB) para mantener la comunicación entre ambos nodos y distribuir de forma complementaria los canales pares e impares. La metodología aplicada y experimental contempló pruebas en un ambiente controlado a distancias de 1, 2 y 3 metros, utilizando herramientas de análisis de radiofrecuencia y de captura de anuncios BLE. La propuesta permitió transformar dos dispositivos de funcionamiento independiente en un sistema coordinado, reproducible y sin hardware adicional, orientado a la experimentación académica en sistemas embebidos, radiofrecuencia y comunicaciones inalámbricas.

Palabras clave: RF-Clown v2, Bluetooth, BLE, ESB, coordinación, interferencia.

ABSTRACT

The present project develops a linear coordination strategy between two RF-Clown v2 devices to generate synchronized interference in Bluetooth/BLE networks within the 2.4 GHz ISM band. The firmware was adapted using a Master–Slave architecture, employing the Enhanced ShockBurst (ESB) protocol to maintain communication between both nodes and distribute the even and odd channels in a complementary manner. The applied experimental methodology included tests in a controlled environment at distances of 1, 2, and 3 meters, using radio frequency analysis tools and BLE advertisement capture. The proposed approach enabled the transformation of two independently operating devices into a coordinated, reproducible system without additional hardware, aimed at academic experimentation in embedded systems, radio frequency, and wireless communications.

Keywords: RF-Clown v2, Bluetooth, BLE, ESB, coordination, interference.

ÍNDICE

Contenido

INTRODUCCIÓN	26
CAPÍTULO I.....	27
1. TÍTULO	27
1.1 Antecedentes de la investigación	27
1.1.1. Hardware abierto para experimentación en radiofrecuencia.....	27
1.1.2. Vulnerabilidades recientes en Bluetooth (2023-2025).....	28
1.1.3. Bluetooth Classic y Bluetooth Low Energy	29
1.1.4. Técnicas anti-jamming y sistemas FHSS (2020-2022).....	30
1.1.5. Marco normativo en Ecuador (ARCOTEL 2020-2022)	31
1.2. CONTEXTUALIZACIÓN Y REALIDAD PROBLEMÁTICA	31
1.2.1. Evolución de las amenazas en redes inalámbricas	31
1.2.2. El rol del hardware abierto en la investigación de seguridad	32
1.2.3. Limitaciones inherentes del dispositivo individual.....	34
1.2.4. La necesidad de coordinación entre los dos dispositivos RF-Clown V 2.0 .	34
1.3. FORMULACIÓN DEL PROBLEMA	35

1.3.1.	Problema general.....	35
1.3.2.	Pregunta de investigación.....	36
1.3.3.	Subpreguntas de investigación	36
1.4	JUSTIFICACIÓN DE LA INVESTIGACIÓN	36
1.4.1.	Justificación técnica	36
1.4.2.	Justificación formativa	38
1.4.3.	Justificación local y social.....	38
1.5	OBJETIVOS DE LA INVESTIGACIÓN	39
1.5.1.	Objetivo general	39
1.5.2.	Objetivos específicos	39
1.6	HIPÓTESIS DE TRABAJO.....	40
1.6.1.	Hipótesis principal.....	40
1.7	ALCANCES Y LIMITACIONES.	40
1.7.1.	Alcances	40
1.7.2.	Limitaciones	41
1.8	METODOLOGÍA DE LA INVESTIGACIÓN	42
1.8.1.	Tipo de investigación	42
1.8.2.	Enfoque de investigación.....	42

1.8.3. Metodología aplicada	44
CAPÍTULO II.	45
2 MARCO TEÓRICO.....	45
2.1. Marco contextual.....	45
2.1.1. Disposición física de los equipos.....	45
2.1.2. Entorno de la banda ISM de 2,4 GHz	46
2.1.3. Contexto geográfico e institucional.....	47
2.1.4. Disposición física del escenario experimental.....	48
2.2. Fundamentos de Bluetooth Classic y BLE.....	49
2.2.1. Bluetooth Classic.....	49
2.2.2. Frequency Hopping Spread Spectrum (FHSS).....	50
2.2.3. Adaptive Frequency Hopping	51
2.2.4. Bluetooth Low Energy.....	51
2.3. Plataforma RF-Clown v2	53
2.3.1 Descripción general	53
2.3.2. Microcontrolador ESP32	54
2.3.3. Transceptor nRF24L01+	54
2.3.4. Función de las radios A y B	55
2.3.5. Función de la radio C.....	57

2.4 Protocolo Enhanced ShockBurst.....	58
2.4.1. Descripción del protocolo.....	58
2.4.2. Paquete de coordinación.....	58
2.4.3. Heartbeat.....	59
2.4.4. Timeout de seguridad.....	59
2.4.5. SequenceID y paquetes no recibidos.....	60
2.5 Arquitectura de coordinación Maestro–Esclavo	61
2.5.1. Nodo Maestro	61
2.5.2. Nodo Esclavo.....	62
2.5.3. Distribución de canales.....	62
2.5.4. Operación conjunta de las radios A y B	63
2.6. Fundamentos matemáticos de las métricas.....	65
2.6.1. Tiempo de permanencia	65
2.6.2. Tiempo de revisita	66
2.6.3. Tiempo teórico de ciclo.....	67
2.6.4. Nivel relativo en dBFS	67
2.6.5. Recepción relativa de anuncios	68
2.7. Herramientas de medición y análisis.....	69

2.7.1. HackRF One	69
2.7.2. GNU Radio.....	71
2.7.3. Acrylic Suite.....	72
2.7.4. Wireshark.....	73
2.7.5. Arduino IDE	74
2.8. Marco normativo y ético	75
2.8.1. Regulaciones nacionales (ARCOTEL)	75
2.8.2. Operación segura	76
2.8.3. Consideraciones éticas.....	77
2.9. Estado del arte y trabajos relacionados	77
CAPÍTULO III	79
3 DESARROLLO METODOLÓGICO E IMPLEMENTACIÓN DEL SISTEMA.....	79
3.1 Presentación	79
3.2 Diseño metodológico.....	80
3.2.1. Variables experimentales	80
3.3 Base de desarrollo del sistema coordinado.....	81
3.4 Arquitectura general implementada	82
3.4.1. Funcionamiento del Maestro	84
3.4.2. Funcionamiento del Esclavo	84

3.4.3. Parámetros implementados	85
3.5 Organización del firmware	86
3.6 Definición de la estrategia de interferencia	88
3.6.1 Estrategia seleccionada	88
3.6.2 Proceso de sincronización.....	89
3.7 Configuración del escenario experimental.....	89
3.7.1 Escenario de 1 m.....	92
3.7.2 Escenario de 2 m.....	93
3.7.3 Escenario de 3 m.....	93
3.8 Procedimientos de medición	94
3.8.1 Verificación funcional del firmware.....	94
3.8.2 Verificación espectral.....	97
3.8.3 Incremento relativo en dBFS	99
3.8.4. Tiempo de permanencia	99
3.8.5. Tiempo de revisita	100
3.8.6. Recepción relativa de anuncios BLE	101
3.9 Consideraciones para la reproducibilidad	102
CAPÍTULO IV.....	103
4 ANÁLISIS DE RESULTADOS Y DISCUSIÓN.....	103

4.1 Introducción al análisis	103
4.2 Configuración del escenario experimental.....	103
4.2.1. Condiciones de prueba	104
4.3 Verificación de la cobertura espectral.....	105
4.3.1. Evidencia con HackRF One y GNU	107
4.4 Validación funcional del sistema	108
4.4.1. Continuidad del enlace de coordinación	109
4.4.2. Funcionamiento del mecanismo de seguridad (Timeout).....	109
4.4.3. Síntesis de la validación funcional del enlace de coordinación.....	110
4.4.4 Cobertura de canales impares del Maestro	111
4.4.5 Cobertura de canales pares del Esclavo	112
4.5 Verificación del barrido coordinado	113
4.6 Incremento relativo de nivel en dBFS.....	114
4.6.1 Cálculo.....	114
4.7 Análisis temporal del barrido	117
4.7.1 Tiempo de permanencia en 2425 MHz.....	117
4.7.2 Tiempo de revisita en 2425 MHz	126
4.8 Evaluación de la recepción relativa de anuncios BLE	134

4.8.1 Definición de la métrica	134
4.8.2 Dispositivo objetivo y herramienta de medición.....	136
4.8.3 Configuración experimental	137
4.8.4 Procedimiento de medición.....	138
4.8.5 Identificación y conteo de anuncios	139
4.8.6 Resultados de ARR a 1 metro	140
4.8.7 Resultados de ARR a 2 metros	141
4.8.8 Resultados de ARR a 3 metros	143
4.8.9 Cálculo del resultado global.....	144
4.8.10 Ejemplo de cálculo	145
4.8.11 Criterios de interpretación	146
4.8.12 Limitaciones	147
4.9 Validación funcional de la sincronización ESB	147
4.10 Discusión general	148
4.11 Limitaciones	149
4.12 Verificación de objetivos	150
4.13 Síntesis del capítulo	151
RESULTADOS, CONCLUSIONES Y RECOMENDACIONES.....	151
Resultados.....	151

Conclusiones generales	152
Recomendaciones.....	153
5 Bibliografía	154
ANEXO.....	156

ÍNDICE DE FIGURAS

Figura 1 Modelo de ataque causado por jamming	32
Figura 2 Implementación de coordinación	35
Figura 3 Objetivos específicos a cumplir.....	40
Figura 4 Disposición física de los dos Rf-clown v2.0	46
Figura 5 Diagrama técnico de la banda ISM 2.4 GHz entre tecnologías.....	47
Figura 6 Distancia propuesta para las pruebas entre los RF-clown v2.0	49
Figura 7 Canales de publicidad primaria de BLE	52
Figura 8 Componentes principales del RF-Clown v2.0.....	53
Figura 9 Arquitectura de las radios A, B y C.....	64
Figura 10 SDR HackRF One	70
Figura 11 Software GNU Radio	71
Figura 12 Software capturador de anuncios BLE	72
Figura 13. Capturador de paquetes Wireshark.....	73
Figura 14 Plataforma Arduino Id.....	75
Figura 15 Identidad institucional de ARCOTEL	76
Figura 16 Arquitectura implementada	83
Figura 17 Diagrama de flujo del proyecto	85
Figura 18 Estructura general de los archivos del firmware	88
Figura 19 Sincronización de transmisión.....	89
Figura 20 Laboratorio para los ensayos	91
Figura 21 Equipos utilizados en los ensayos	91

Figura 22. Verificación de la altura y la distancia de separación en el escenario experimental.....	92
Figura 23. Montaje experimental: separación total de 1 m entre los RF-Clown.	92
Figura 24. Montaje experimental: separación total de 2 m entre los RF-Clown.	93
Figura 25. Montaje experimental: separación total de 3 m entre los RF-Clown.	94
Figura 26 Activación del RF-Clown coordinado Maestro.....	95
Figura 27 Monitor Serial activo Maestro.....	96
Figura 28 Activación de los RF-Clown coordinados Esclavo.....	96
Figura 29 Monitor Serial activo Esclavo	97
Figura 30 Diagrama de GNU Radio para observación espectral.....	98
Figura 31 Bloques usados para analizar el espectro	100
Figura 32 Componentes usados en prácticas con los RF-Clown.....	104
Figura 33 Bloque Time Sink GNU Radio.....	105
Figura 34 Bloque Frequency Sink GNU Radio	106
Figura 35 Bloque Waterfall Sink GNU Radio.....	106
Figura 36 Bloques de decisión para buscar espectro GNU Radio	107
Figura 37 Ondas espectrales con interferencias intencionadas.....	108
Figura 38 Representación del Frequency Sink	111
Figura 39 Distribución observada de canales pares con interferencia.....	112
Figura 40 Incursión total entre canales pares e impares en el espectro	114
Figura 41. Comparación del nivel espectral con y sin interferencia del sistema RF-Clown.	116
Figura 42. Variaciones observadas en el espectro durante la evaluación del sistema RF-	

Clown.....	116
Figura 43 Plataforma lista con sus bloques principales para uso.....	118
Figura 44 Evaluación de la actividad temporal del Maestro en 2425 MHz.....	119
Figura 45 Inicio de prueba a 1 metro de los RF-Clown.....	120
Figura 46 Final de prueba de 1 metro de distancia entre los RF-Clown.....	120
Figura 47 Actividad del muestreo para los 2 metros de separación	122
Figura 48 Concluido el muestreo de los 2 metros de separación.....	122
Figura 49 Cuadro de bloques usados para las siguientes pruebas de tiempo.....	127
Figura 50 Primer análisis con la nueva configuración de GNU Radio.....	128
Figura 51 Término del primer análisis a 1 metro de separación entre los RF-Clown	128
Figura 52 Segunda prueba a 2 metros entre los RF-Clown	130
Figura 53 Fin de prueba 2 con los resultados de repeticiones	130
Figura 54 Dispositivo elegido para práctica y resultados	136

ÍNDICE DE TABLAS

Tabla 1	Especificaciones de hardware del nodo RF-Clown v2.0	33
Tabla 2	Canales de anuncios BLE	51
Tabla 3	Estructura básica de operación.....	59
Tabla 4	Científico/Aporte	78
Tabla 5	Parámetros y variables experimentales	80
Tabla 6	Parámetros de funcionamiento.....	86
Tabla 7	Código de decisión.....	87
Tabla 8	Distribución de distancias entre los dispositivos RF-Clown y el objetivo	90
Tabla 9	Parámetros de configuración para la medición espectral.....	98
Tabla 10	Evaluación experimental por distancia	102
Tabla 11	Condiciones de usos.....	104
Tabla 12	Estrategia para coordinación los dos RF-Clown.....	108
Tabla 13	Mecanismo de seguridad.....	110
Tabla 14	Resultados de la validación funcional del enlace ESB	110
Tabla 15	Frecuencias identificadas en el barrido impar	112
Tabla 16	Frecuencias identificadas en el barrido par.....	113
Tabla 17	Coordinación de interferencias hacia el espectro.....	113
Tabla 18	Verificación de análisis de resultados del dB	115
Tabla 19	Tiempo de permanencia de la interferencia	119
Tabla 20	Resumen a 2 metros de distancia de los RF-Clown.....	121
Tabla 21	Repeticiones de 3 metros de separación de los RF-Clown.....	123

Tabla 22	Resumen general y comparativas entre distancias.....	124
Tabla 23	Repeticiones realizadas a 1 m	127
Tabla 24	Repeticiones de pruebas a 2 metros de distancia entre los RF-Clown	129
Tabla 25	Promedio y comparación con la tabla anterior	131
Tabla 26	Repeticiones a 3 metros entre los RF-Clown en tiempo de revisita	131
Tabla 27	Resumen del tiempo de revisita según la distancia.....	132
Tabla 28	Comparación de métricas temporales según la distancia.....	134
Tabla 29	Componentes y condiciones de las pruebas de ARR.....	137
Tabla 30	Análisis del parámetro ARR a 1 metro de separación entre RF-Clown	140
Tabla 31	Resultados de repeticiones a 2 metros del ARR con interferencia	142
Tabla 32	Análisis con 3 metros entre los RF-Clown en métrica ARR	143
Tabla 33	Resultados globales de ARR según la distancia	145
Tabla 34	Criterios descriptivos para interpretar la ARR.....	146

INTRODUCCIÓN

La proliferación de dispositivos que operan en la banda ISM de 2,4 GHz, como Bluetooth, BLE, Wi-Fi y Zigbee, ha transformado el panorama de las comunicaciones inalámbricas. Este espectro, al ser de uso libre, se ha vuelto altamente congestionado y vulnerable a ataques de denegación de servicio (DoS) por interferencia, conocidos como jamming. Dichos ataques consisten en saturar un canal con señales falsas o ruido de radiofrecuencia, lo que impide la conexión entre dispositivos legítimos y afecta la estabilidad de las redes.

Ante esta problemática, el desarrollo de herramientas de **hardware abierto** ha democratizado la investigación en seguridad inalámbrica. Ejemplos como el *Soft Tester UE* [10] demuestran que es posible realizar pruebas de seguridad RF de alta calidad con el uso de equipos accesibles, sin depender de instrumentación costosa.

Siguiendo esta filosofía, el **RF-Clown v2**, creado por CiferTech en 2025 [4], se presenta como un dispositivo portátil de código abierto, diseñado para generar interferencias controladas en señales Bluetooth y BLE, con fines educativos y experimentales. No obstante, su firmware original carece de funciones de sincronización entre unidades, lo que limita la posibilidad de implementar estrategias de interferencia coordinadas o distribuidas.

Por ello, esta investigación propone implementar un esquema de **coordinación entre dos RF-Clown v2**, utilizando únicamente sus componentes integrados. El objetivo es demostrar que la cooperación entre dos dispositivos puede mejorar la cobertura, la efectividad y la precisión temporal de las pruebas de interferencia, contribuyendo al avance de la seguridad inalámbrica desde una perspectiva accesible y abierta.

CAPÍTULO I

1. TÍTULO

Desarrollo estratégico de coordinación lineal entre dos dispositivos RF-Clown v2 para interferencias sincronizadas en redes Bluetooth/BLE.

1.1 Antecedentes de la investigación

El aumento del uso de la banda ISM de 2,4 GHz ha generado un entorno espectral altamente congestionado. En este contexto, la seguridad de protocolos como Bluetooth se ha visto comprometida por vulnerabilidades en la pila de protocolos, tales como las identificadas por el NIST en los registros CVE-2023-40129 y CVE-2025-47370 [1] [2]. Estas fallas permiten ataques de manipulación de claves de cifrado que exigen nuevos métodos de evaluación mediante hardware de bajo costo como el RF-Clown v2 [3].

1.1.1. Hardware abierto para experimentación en radiofrecuencia

El crecimiento de los sistemas inalámbricos que operan en la banda ISM de 2,4 GHz ha incrementado el interés en el desarrollo de plataformas de experimentación accesibles y modificables. Estas herramientas permiten estudiar el comportamiento de las comunicaciones inalámbricas sin depender exclusivamente de equipos propietarios de alto costo.

El hardware abierto facilita el acceso al diseño electrónico, al código fuente y a los parámetros operativos de los dispositivos. Esta característica favorece la reproducibilidad de los experimentos, la validación independiente de los resultados y el desarrollo de nuevas funciones mediante modificaciones de firmware.

Entre estas plataformas se encuentran el RF-Clown v2 [4], un dispositivo basado en un microcontrolador ESP32, y tres módulos nRF24L01+. Su arquitectura permite generar emisiones controladas en la banda de 2,4 GHz y modificar el firmware para implementar múltiples modos de operación. Estas características convierten al dispositivo en una alternativa de bajo costo para investigaciones académicas vinculadas a las comunicaciones inalámbricas, como la seguridad en radiofrecuencia.

Sin embargo, el firmware original del RF-Clown v2 está orientado principalmente al funcionamiento autónomo. Cuando se utilizan dos unidades, cada una ejecuta sus propias instrucciones sin intercambiar notas del canal, como el estado de operación o la secuencia temporal. Esta limitación constituye el punto de partida de la presente investigación.

1.1.2. Vulnerabilidades recientes en Bluetooth (2023-2025)

La justificación para analizar interferencias sigue siendo relevante porque aún se siguen descubriendo fallos en la pila de protocolos de Bluetooth.

En 2023, se detectaron vulnerabilidades críticas en el stack "Fluoride" de Android, identificadas como CVE-2023-40129 [1]. Esta vulnerabilidad, clasificada con una severidad alta (CVSS 7.5), permitía la ejecución remota de código en el subsistema GATT sin necesidad de interacción del usuario ni de privilegios adicionales. El fallo afectaba a múltiples versiones de Android y un atacante podía explotarlo mediante la transmisión de un paquete Bluetooth malicioso [1].

Más recientemente, en 2025, Antonioli [5] presentó los ataques BLUFFS (Bluetooth Forward and Future Secrecy) en la conferencia ACM CCS, una de las más prestigiosas en seguridad informática. BLUFFS demostró que es posible romper la confidencialidad de las

sesiones Bluetooth al explotar debilidades en el establecimiento de las claves de sesión. Los ataques consisten en seis vectores diferentes que aprovechan cuatro fallos fundamentales en la especificación de Bluetooth, lo que permite ataques de intermediario (Man-in-the-Middle), como la degradación de sesiones seguras.

Estos hallazgos subrayan la necesidad de contar con laboratorios de pruebas prácticos para simular escenarios de ataque y desarrollar contramedidas. El presente estudio contribuye en esta dirección al proporcionar una herramienta de prueba coordinada de bajo costo.

1.1.3. Bluetooth Classic y Bluetooth Low Energy

Bluetooth Classic y Bluetooth Low Energy son tecnologías de comunicación inalámbrica de corto alcance que operan en la banda ISM de 2,4 GHz. Aunque ambas pertenecen a la familia Bluetooth, difieren en la distribución de los canales, en los procedimientos de acceso al medio y en el consumo de energía.

Bluetooth Classic utiliza 79 canales de 1 MHz y emplea el modo de Frequency Hopping Spread Spectrum. Este mecanismo permite cambiar continuamente de frecuencia para reducir los efectos de la interferencia y favorecer la coexistencia con otros sistemas inalámbricos. La tasa nominal de salto puede alcanzar 1600 saltos por segundo, lo que equivale a una ranura temporal de 625 μ s.

Bluetooth Low Energy utiliza 40 canales de 2 MHz; de estos, tres se destinan principalmente a tareas de publicidad y descubrimiento, mientras que los restantes se emplean para el intercambio de datos. Los anuncios BLE permiten que un dispositivo comunique periódicamente su identidad, disponibilidad y servicios sin necesidad de establecer una conexión permanente.

Debido a estas características, la observación del comportamiento de Bluetooth no puede limitarse a una única frecuencia. Es necesario estudiar la actividad en distintas regiones del espectro y evaluar las variaciones en la recepción de anuncios BLE al activar el sistema coordinado.

1.1.4. Técnicas anti-jamming y sistemas FHSS (2020-2022)

Para entender cómo maximizar la interferencia, es crucial conocer las defensas de los sistemas objetivo. Liu y Fok [6] investigaron el uso de sistemas fotónicos de microondas para lograr anchos de banda de salto ultrarrápido (de nanosegundos a picosegundos), inspirados en mecanismos biológicos de evasión frente a ataques.

Estos sistemas avanzados de FHSS (Frequency Hopping Spread Spectrum) representan un desafío para las estrategias de jamming simples, ya que pueden cambiar de canal a una velocidad mayor de la que un jammer convencional puede seguir. Sin embargo, la implementación de estos sistemas requiere hardware especializado y costoso, lo cual no es habitual en dispositivos Bluetooth comerciales.

Investigaciones sobre códigos sistemáticos de tasa variable, que no dependen de una tasa de codificación fija [7] han demostrado que es posible optimizar la transmisión para mantener la comunicación incluso en presencia de ruido en alguna banda parcial. Estos esquemas defensivos adaptan dinámicamente la tasa de transmisión en respuesta a la interferencia detectada.

Estos avances defensivos refuerzan la necesidad de desarrollar estrategias de *jamming* coordinado (como el barrido sincronizado) lo suficientemente dinámicas como para superar las defensas presentes en dispositivos comerciales, sin pretender vulnerar sistemas FHSS de grado militar.

1.1.5. Marco normativo en Ecuador (ARCOTEL 2020-2022)

La presente investigación se desarrolla en estricto cumplimiento del ordenamiento jurídico ecuatoriano en materia de telecomunicaciones. Según el Plan Nacional de Frecuencias emitido por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) [8], el uso del espectro radioeléctrico en la banda ISM (Industrial, Scientific, and Medical) de 2,4 GHz está sujeto a regulaciones específicas sobre potencia y aplicaciones. Este proyecto se enmarca en los artículos de la Ley Orgánica de Telecomunicaciones que fomentan la investigación académica, siempre que se garantice la no interferencia con los servicios públicos o de emergencia. Los detalles técnicos de las resoluciones vigentes, así como los límites operativos, se profundizan en el Marco Legal del Capítulo 2.

1.2. CONTEXTUALIZACIÓN Y REALIDAD PROBLEMÁTICA

1.2.1. Evolución de las amenazas en redes inalámbricas

La proliferación de dispositivos que operan en la banda ISM de 2,4 GHz ha transformado radicalmente el ecosistema de las comunicaciones inalámbricas. Tecnologías como Bluetooth, Bluetooth Low Energy (BLE), Wi-Fi (IEEE 802.11b/g/n/ax) y Zigbee coexisten en este espectro no licenciado, lo que genera un entorno cada vez más congestionado y vulnerable a ataques de denegación de servicio (DoS) por interferencia [7].

El ataque de jamming ilustrado en la **Figura 1** constituye una forma de denegación de servicio (DoS) que interrumpe el enlace inalámbrico mediante la inyección de ruido de banda ancha en el canal con interferencia o señales espurias. Esta acción bloquea el establecimiento de conexiones legítimas y degrada significativamente la fiabilidad de la comunicación. Este tipo de

amenaza afecta no solo a redes Wi-Fi, sino también a sistemas Bluetooth, dispositivos IoT y equipos de navegación GPS; en ello, representa un riesgo significativo para las infraestructuras críticas.

Las características de propagación en la banda de 2,4 GHz se distinguen por una mayor absorción ante la presencia de agua y obstáculos en comparación con bandas de menor frecuencia, una penetración limitada en paredes y estructuras, y una mayor susceptibilidad a la interferencia provocada por hornos de microondas y otros dispositivos domésticos.

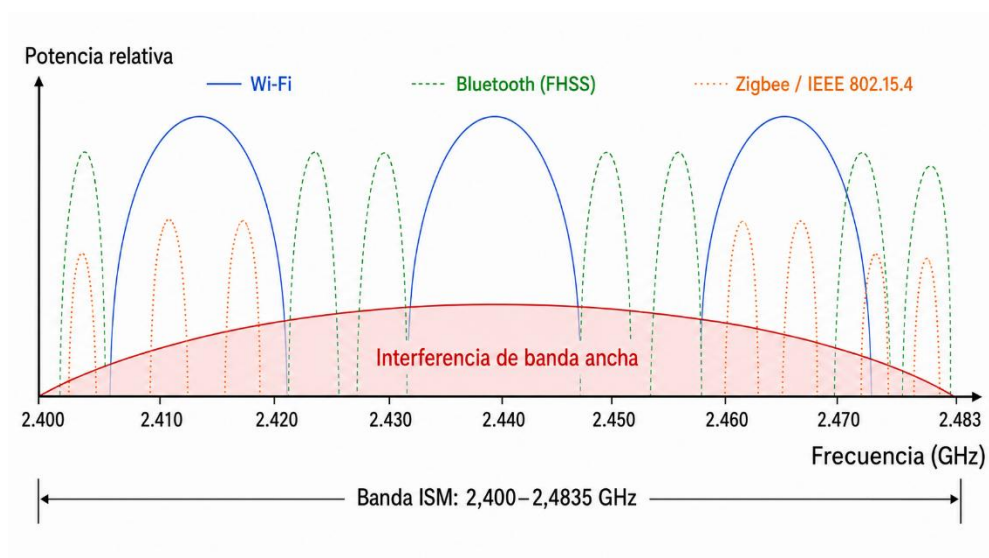


Figura 1 Modelo de ataque causado por jamming

1.2.2. El rol del hardware abierto en la investigación de seguridad

En este contexto, el desarrollo de herramientas de hardware abierto para la investigación en seguridad inalámbrica ha democratizado el acceso al conocimiento técnico. A diferencia de las soluciones que pueden costar miles de dólares, plataformas como HackRF One, LimeSDR y, más recientemente, el RF-Clown v2, permiten a estudiantes e investigadores explorar vulnerabilidades en redes inalámbricas con inversiones controladas.

El RF-Clown v2, desarrollado por CiferTech y lanzado oficialmente en octubre de 2025, representa un hito en esta tendencia. Este dispositivo portátil de código abierto está diseñado específicamente para generar interferencias controladas en señales BLE y Bluetooth Classic (véase la tabla 1), con fines exclusivamente educativos y de investigación [3].

Las especificaciones técnicas del RF-Clown v2, según la documentación oficial, son [3]:

Tabla 1
Especificaciones de hardware del nodo RF-Clown v2.0

Componente	Especificaciones Técnicas
Microcontrolador	ESP32-WROOM-32U (Arquitectura 32-bit dual-core)
Módulos RF	3 × Módulos GT24 Mini (compatibles con el transceptor nRF24L01+)
Antenas	4 conectores IPEX acoplados a antenas externas de 8 dBi
Interfaz de Usuario	Pantalla OLED de 0.96" + 3 botones de control táctiles
Indicación Visual	Módulo LED RGB NeoPixel
Sistema de Alimentación	Batería LiPo 1S equipada con circuito de carga TP4056
Interfaz de Programación	Puerto USB integrado con conversor USB-Serial CP2102
Gestión Térmica	Disipadores de calor pasivos acoplados a los módulos RF

El creador del proyecto, Cifer, destaca que "tener tres radios mejora drásticamente la cobertura y el rendimiento" y que se añadieron pequeños disipadores de calor a los módulos de radio para estabilizar el rendimiento en operación continua [3].

1.2.3. Limitaciones inherentes del dispositivo individual

El RF-Clown v2 dispone de tres módulos nRF24L01+ y permite modificar diversos parámetros del firmware. No obstante, su funcionamiento original no contempla la comunicación permanente entre varias unidades.

Cuando dos dispositivos se ejecutan de forma independiente, cada uno selecciona sus canales sin conocer el estado del otro. Como consecuencia, pueden producirse coincidencias innecesarias, recorridos redundantes o secuencias sin relación temporal.

La principal limitación no radica en la cantidad de radios disponibles, sino en la ausencia de un mecanismo que distribuya los conjuntos de canales y mantenga un estado de operación común entre los dispositivos.

1.2.4. La necesidad de coordinación entre los dos dispositivos RF-Clown V 2.0

Para superar esta falta de sincronización, se propone una arquitectura Maestro–Esclavo compuesta por dos RF-Clown v2. El Maestro gestiona el estado general del sistema y transmite paquetes de control mediante el protocolo ESB. El Esclavo recibe estos paquetes, actualiza su estado y detiene su operación cuando se pierde el enlace durante el tiempo establecido en el firmware.

La estrategia distribuye los canales de acuerdo con su paridad **Figura 2:**

- El Maestro recorre los canales impares.
- El Esclavo recorre los canales pares.

En cada nodo, las radios A y B operan conjuntamente en el mismo canal seleccionado.

La radio C mantiene el enlace ESB en el canal 81, correspondiente a 2481 MHz.

Esta arquitectura prescinde del seguimiento de la secuencia de salto de frecuencia de dispositivos Bluetooth específicos. Su objetivo es distribuir de forma controlada los conjuntos de canales entre ambos nodos y validar experimentalmente su comportamiento.

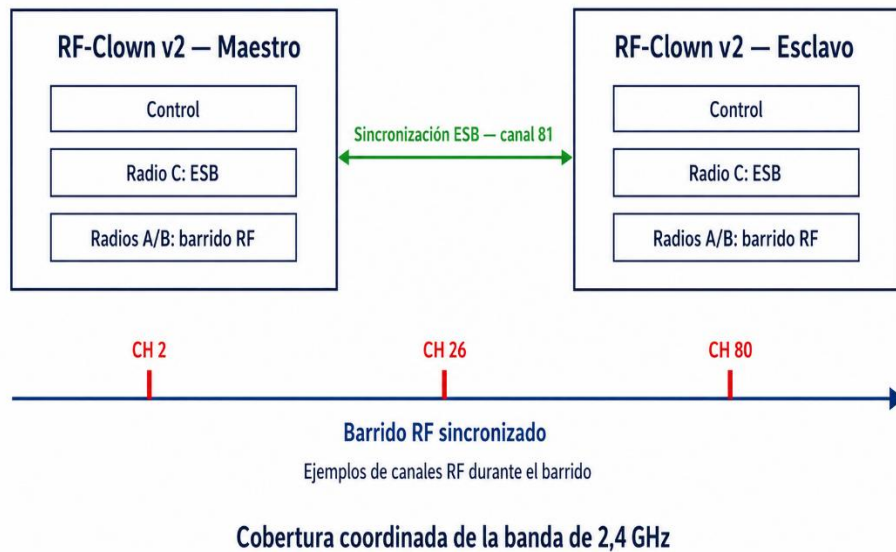


Figura 2 Implementación de coordinación

1.3. FORMULACIÓN DEL PROBLEMA

1.3.1. Problema general

El firmware oficial del RF-Clown v2 carece de funcionalidades de sincronización entre múltiples dispositivos, lo que limita su efectividad en escenarios que requieren cobertura distribuida o interferencia multicanal coordinada. La falta de un protocolo de comunicación entre unidades impide implementar estrategias avanzadas de jamming, como el barrido de frecuencias sincronizado o la interferencia por relevo.

1.3.2. Pregunta de investigación

A partir de la problemática identificada, se formula la siguiente pregunta de investigación:

¿Cómo implementar y validar una arquitectura Maestro/Esclavo en dispositivos RF-Clown v2 mediante el protocolo ESB? El objetivo es distribuir de forma coordinada la operación en los canales pares e impares de la banda de 2,4 GHz, sin recurrir a hardware adicional.

1.3.3. Subpreguntas de investigación

¿Qué modificaciones requiere el firmware del RF-Clown v2 para implementar las funciones de Maestro como la de Esclavo?

¿Cómo puede utilizarse el protocolo ESB para mantener un estado de operación común entre ambos dispositivos?

¿Puede verificarse mediante HackRF One y GNU Radio que el Maestro recorre canales impares y el Esclavo canales pares?

¿Cuáles son los tiempos de permanencia y de revisita observados en la frecuencia seleccionada durante el barrido?

¿Qué cambio se produce en la recepción relativa de anuncios BLE cuando el sistema coordinado está activo?

¿Cómo afecta la variación de las distancias de 1, 2 y 3 m a los resultados obtenidos y a las condiciones del escenario experimental?

1.4 JUSTIFICACIÓN DE LA INVESTIGACIÓN

1.4.1. Justificación técnica

Desde una perspectiva técnica, esta investigación demuestra la escalabilidad del diseño RF-Clown mediante la implementación de una coordinación distribuida. El uso del protocolo Enhanced ShockBurst (ESB), nativo de los módulos nRF24L01+, permite separar las funciones de coordinación de la operación radioeléctrica.

En la arquitectura propuesta, la radio C establece el enlace ESB entre el Maestro y el Esclavo. Las radios A y B de cada nodo se configuran simultáneamente en el mismo canal seleccionado. El Maestro recorre el conjunto de canales impares y el esclavo, el de canales pares.

Esta distribución evita que ambos nodos recorran intencionalmente el mismo conjunto de frecuencias y permite evaluar una operación complementaria. Sin embargo, no se presupone que la combinación de las radios A y B duplique exactamente la potencia, puesto que cualquier incremento debe determinarse mediante mediciones experimentales.

La validación utiliza herramientas diferentes para cada tipo de evidencia:

- HackRF One y GNU Radio para observar la actividad espectral y temporal.
- Acrylic Suite para capturar anuncios BLE.
- Wireshark para revisar los archivos PCAP y contar los registros recibidos.
- Arduino IDE para programar los dispositivos y obtener registros del monitor serial.
- Pantallas OLED y NeoPixel para comprobar visualmente el estado de ejecución.

El HackRF One se utiliza como receptor SDR y proporciona niveles digitales relativos expresados en dBFS; por tanto, los resultados se interpretan únicamente como variaciones respecto del nivel de referencia.

1.4.2. Justificación formativa

El desarrollo de este proyecto fortalece competencias fundamentales para instruir el conocimiento en sistemas de telecomunicaciones:

- Programación de sistemas embebidos con ESP32 y el entorno Arduino/PlatformIO.
- Implementación de protocolos de comunicación inalámbrica (ESB del nRF24L01+).
- Diseño de sistemas distribuidos y de estrategias de coordinación.
- Comprensión profunda de las vulnerabilidades de los protocolos Bluetooth/BLE.
- Metodología experimental para la validación del sistema RF.

Estas competencias son altamente valoradas en el mercado laboral actual, más aún en los sectores de ciberseguridad, IoT y telecomunicaciones.

1.4.3. Justificación local y social

Las instituciones educativas con recursos limitados pueden tener dificultades para adquirir equipos especializados de radiofrecuencia. El uso de plataformas abiertas y herramientas de software accesibles permite desarrollar prácticas académicas con una menor inversión.

En el contexto ecuatoriano, la investigación también contribuye a fomentar el uso responsable del espectro y a profundizar en las condiciones aplicables a la banda ISM de 2,4 GHz. Todas las pruebas deben realizarse bajo el principio de no causar interferencia perjudicial, utilizar equipos autorizados y suspender de inmediato cualquier emisión que pueda afectar a terceros [8].

1.5 OBJETIVOS DE LA INVESTIGACIÓN

1.5.1. Objetivo general

Desarrollo estratégico para la coordinación lineal de dos dispositivos RF-Clown v2 en las interferencias sincronizadas en redes Bluetooth/BLE, utilizando exclusivamente las capacidades de hardware y firmware abiertos de estos dispositivos.

1.5.2. Objetivos específicos

Se eligieron los siguientes objetivos específicos de la **Figura 3** para lograr una perspectiva de avance en la seguridad de las tecnologías inalámbricas.

1) Adaptar el firmware oficial del RF-Clown v2 para habilitar modos de operación diferenciados (maestro/esclavo) y sincronización básica mediante comunicación NRF24L01 entre unidades, sin agregar hardware externo.

2) Implementar una estrategia de distribución de canales en la que el Maestro recorra canales impares y el esclavo canales pares, manteniendo las radios A y B de cada nodo en el mismo canal seleccionado que maximice la persistencia de la interferencia sobre dispositivos Bluetooth con FHSS, basada en los parámetros de latencia caracterizados por Krull et al. [9].

3) Evaluar el impacto de dos configuraciones de despliegue físico sobre la cobertura efectiva en la interferencia, considerando distancias de separación de 1 m, 2 m y 3 m.

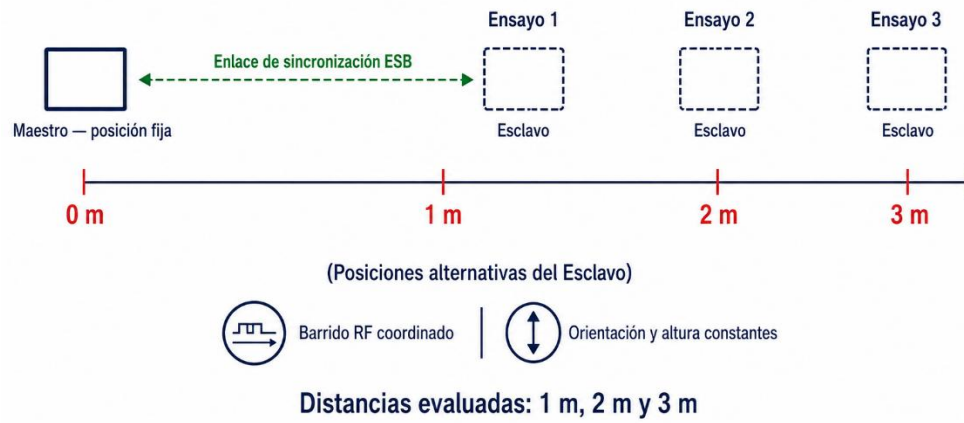


Figura 3 Objetivos específicos a cumplir

1.6 HIPÓTESIS DE TRABAJO

1.6.1. Hipótesis principal

La coordinación Maestro–Esclavo entre dos dispositivos RF-Clown v2, mediante ESB y una distribución complementaria de canales pares e impares, reduce la recepción relativa de anuncios BLE en la condición activa frente a la referenciada, en un escenario experimental controlado.

1.7 ALCANCES Y LIMITACIONES.

1.7.1. Alcances

La investigación comprende:

- Adaptación del firmware para dos dispositivos RF-Clown v2.
- Implementación de los roles Maestro y Esclavo.
- Utilización de la radio C para la comunicación ESB.
- Asignación de canales impares al maestro y de canales pares al esclavo.

- Operación conjunta de los radios A y B en el mismo canal asignado a cada nodo.
- Implementación de un mecanismo de seguridad mediante un timeout.
- Verificación de los estados mediante OLED, NeoPixel y monitor serial.
- Observación espectral y temporal mediante HackRF One y GNU Radio.
- Captura de anuncios BLE con Acrylic Suite.
- Revisión de archivos PCAP y conteo de registros en Wireshark.
- Pruebas en configuración lineal a las distancias de 1, 2 y 3 m.
- Realización de 10 repeticiones por condición experimental.
- Evaluación de un dispositivo BLE identificado por su dirección MAC.
- Registro de la configuración, del montaje y de los resultados experimentales.

Los resultados se limitan a los dispositivos, antenas, firmware, ganancias, distancias y condiciones ambientales utilizados durante los ensayos.

1.7.2. Limitaciones

La investigación presenta las siguientes limitaciones:

- Se restringe a Bluetooth Classic y BLE en la banda ISM de 2,4 GHz.
- No evalúa Wi-Fi, Zigbee ni otros protocolos inalámbricos.
- Las pruebas se realizan en un laboratorio controlado y con visibilidad directa.
- No se evalúan topologías ajenas a la configuración lineal.
- Se utiliza un número limitado de dispositivos comerciales.
- El HackRF One no constituye un analizador de espectro calibrado.
- Los niveles obtenidos en GNU Radio se expresan exclusivamente en dBFS.

- No se mide la latencia paquete a paquete del enlace ESB mediante osciloscopio o en un analizador lógico.
- Acrylic Suite registra únicamente los anuncios BLE recibidos por el analizador.
- No se conoce la cantidad total de anuncios transmitidos por el dispositivo BLE.
- La ARR no equivale a una tasa de pérdida de paquetes.
- El rendimiento de la aplicación de captura puede verse afectado por la sensibilidad del receptor, la orientación de las antenas y las condiciones ambientales.
- Los tiempos de permanencia y de revisita se obtienen mediante un umbral aplicado a la señal capturada.
- Las emisiones se limitan al entorno experimental autorizado y deben detenerse ante cualquier afectación a terceros.

1.8 METODOLOGÍA DE LA INVESTIGACIÓN

1.8.1. Tipo de investigación

La investigación posee un carácter aplicado y experimental. Se clasifica como aplicada al desarrollar una modificación funcional del firmware del RF-Clown v2, y como experimental al evaluar el comportamiento del sistema bajo condiciones controladas de distancia, configuración y estado de operación.

Asimismo, integra un componente descriptivo, ya que documenta la arquitectura, los estados del firmware, la distribución de canales y los resultados observados durante los ensayos.

1.8.2. Enfoque de investigación

El estudio utiliza un enfoque cuantitativo complementado con evidencia cualitativa.

El componente cuantitativo del sistema abarca un conjunto de métricas y cálculos estadísticos diseñados para evaluar el desempeño y la calidad de la recepción de señales. Este componente incluye, en primer lugar, el conteo de anuncios BLE recibidos, que permite determinar el número de paquetes capturados durante el periodo de monitoreo. A continuación, se calcula la tasa de llegada de anuncios (ARR), un indicador clave de la frecuencia con la que se reciben las transmisiones. También se considera el incremento relativo de nivel en decibelios a escala completa (dBFS), que mide las variaciones en la intensidad de la señal recibida. Además, se registran el tiempo de permanencia, que indica cuánto tiempo el sistema permanece en un canal o estado determinado, y el tiempo de revisita, que mide el intervalo entre visitas sucesivas a un mismo canal. Finalmente, el componente cuantitativo incluye el cálculo de la media y la desviación estándar de las repeticiones, para ofrecer una visión estadística completa de la consistencia y la variabilidad de las mediciones obtenidas a lo largo del tiempo.

El componente cualitativo del sistema reúne un conjunto de evidencias y observaciones visuales, sensoriales y documentales que complementan las mediciones numéricas y permiten una evaluación más integral del comportamiento operativo. Este componente incluye, en primer lugar, las capturas de pantalla obtenidas con GNU Radio, que permite visualizar la calidad de la señal y el espectro de frecuencia en tiempo real durante las transmisiones.

También se registran fotografías del montaje experimental, que documentan la disposición física de los dispositivos, las conexiones y el entorno de prueba. Además, se recopilan los estados mostrados en las pantallas OLED, que proporcionan información visual inmediata sobre el estado operativo de cada nodo, así como los indicadores NeoPixel, cuyos cambios de color y patrón ofrecen señales resplandecientes en el estado operativo y en eventos críticos. A esto se suman los registros del monitor serial, en los que se almacenan todos los

mensajes de depuración, advertencias y notificaciones generados durante la ejecución.

Finalmente, el componente cualitativo incluye observaciones detalladas sobre la interrupción y la posterior recuperación de los dispositivos evaluados, documentando su comportamiento ante fallos, reinicios o pérdidas de comunicación, lo que permite identificar patrones de estabilidad y debilidad del sistema.

1.8.3. Metodología aplicada

La investigación aplicada se caracteriza por buscar la resolución de problemas prácticos mediante la generación de conocimiento transferible y aplicable a contextos reales. En este estudio, la metodología aplicada se materializa a través de:

Desarrollo tecnológico (firmware): Se implementan modificaciones específicas en el código fuente del RF-Clown v2 para habilitar las funcionalidades de coordinación. Este desarrollo sigue un ciclo iterativo de diseño, implementación, prueba y refinamiento.

Validación experimental: Se diseña y ejecuta un protocolo práctico controlado para evaluar el desempeño del sistema coordinado en condiciones realistas de laboratorio. Este protocolo incluye:

- Definición de variables independientes, como las distancias de separación (1 m, 2 m, 3 m) y la estrategia de rotación de canales (cíclica sincronizada, desfasada).
- Control de variables extrañas (distancia fija, dispositivos objetivo estandarizados).
- Firmware modificado disponible en el repositorio público.
- Protocolo documentado para el despliegue óptimo según el escenario.
- Guía de configuración y uso responsable.

Transferencia de conocimiento: Los resultados obtenidos se documentan de manera exhaustiva para garantizar su replicabilidad por parte de otros investigadores e instituciones educativas, contribuyendo así a la democratización del conocimiento en el ámbito de la seguridad en radiofrecuencia (RF).

La investigación aplicada se distingue de la básica por su orientación a la resolución de problemas específicos. Según Creswell (2018), "la investigación aplicada busca resolver problemas prácticos, utilizando los conocimientos generados por la investigación básica" [10].

CAPÍTULO II.

2 MARCO TEÓRICO

2.1. Marco contextual

2.1.1. Disposición física de los equipos

La disposición física de los nodos constituye una variable crítica en el marco experimental. Con el fin de evitar la saturación de los receptores y los efectos de intermodulación, se determinó una distancia de separación mínima conforme a la región de campo cercano, proceso detallado en la **Figura 4**. Por otro lado, la sincronización lineal tiene como objetivo maximizar la suma de las potencias de interferencia en el receptor objetivo (víctima), minimizando así la interferencia destructiva que podría producirse si los osciladores locales de ambos dispositivos RF-Clown v2 no estuvieran debidamente coordinados ni en fase ni en frecuencia [9].

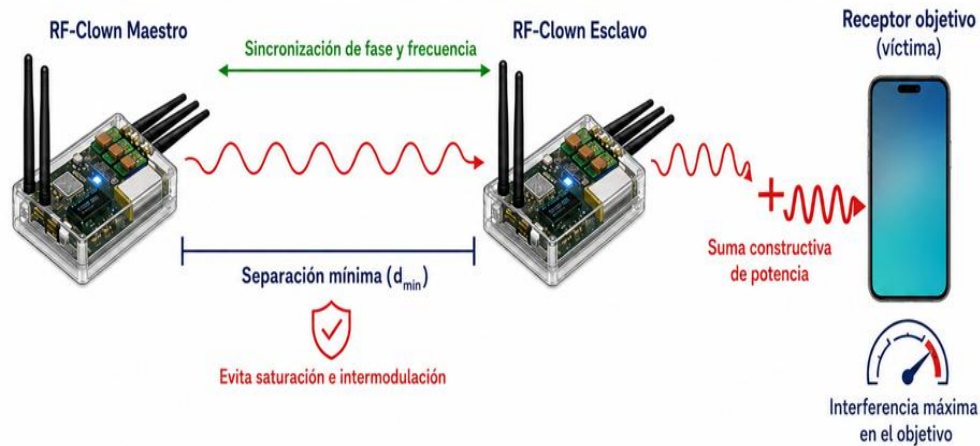


Figura 4 Disposición física de los dos Rf-clown v2.0

2.1.2. Entorno de la banda ISM de 2,4 GHz

La banda Industrial, Científica y Médica (ISM) de 2,4 GHz (rango aproximado de 2400 a 2483,5 GHz) es de uso libre a nivel mundial, lo que ha permitido la proliferación de tecnologías inalámbricas como Bluetooth, Bluetooth Low Energy (BLE), Wi-Fi (IEEE 802.11b/g/n/ax), Zigbee y múltiples dispositivos IoT [7].

La utilización compartida de esta banda permite el funcionamiento de múltiples servicios al prescindir de las asignaciones de frecuencia exclusiva por dispositivo. Sin embargo, esto conlleva un entorno radioeléctrico variable en el que diversas tecnologías convergen en regiones espectrales.

Bluetooth emplea mecanismos de selección y salto de frecuencia para reducir la congestión. Sin embargo, la disponibilidad de numerosos canales no garantiza la ausencia de degradación cuando la ocupación radioeléctrica aumenta significativamente en la banda.

En el presente proyecto, la banda ISM constituye el entorno de operación de los módulos nRF24L01+ integrados en el RF-Clown v2, de los dispositivos Bluetooth evaluados y del receptor SDR HackRF One utilizado para obtener evidencia espectral.

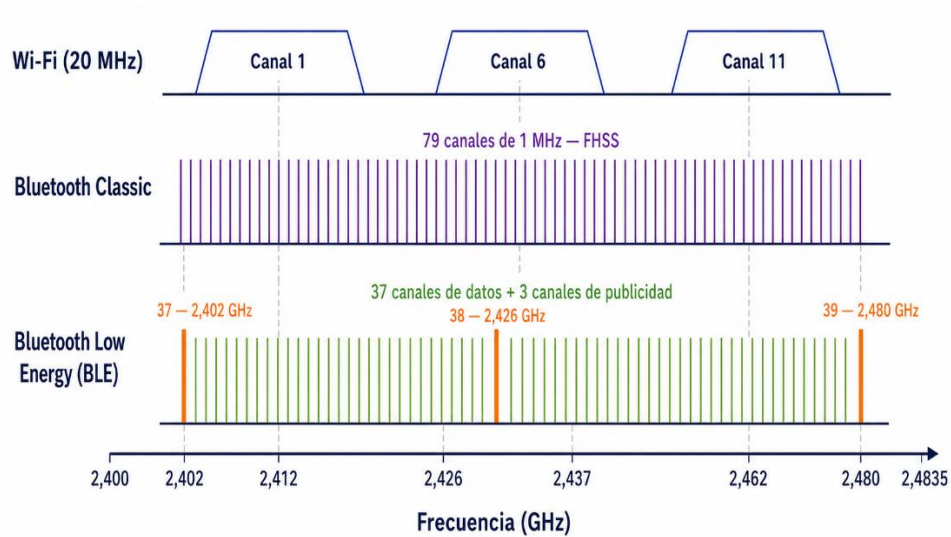


Figura 5 Diagrama técnico de la banda ISM 2.4 GHz entre tecnologías

La **Figura 5** muestra la distribución de los canales de Wi-Fi, Bluetooth Classic y Bluetooth Low Energy (BLE) en la banda ISM de 2,4 GHz. Debido a que estas tecnologías comparten el mismo espectro, la ocupación de los canales Wi-Fi puede coincidir con determinadas frecuencias utilizadas por Bluetooth. Con el fin de mitigar esta interferencia, Bluetooth utiliza mecanismos de salto de frecuencia (Adaptive Frequency Hopping) que permiten la conmutación dinámica entre canales. No obstante, en entornos con alta densidad espectral, el número de canales disponibles se reduce, lo que puede derivar en un incremento de las retransmisiones, así como en mayor latencia, inestabilidad de enlace o interrupciones temporales en los dispositivos Bluetooth [11].

2.1.3. Contexto geográfico e institucional

La presente investigación se desarrolla en la Universidad Estatal Península de Santa Elena (UPSE), Facultad de Sistemas y Telecomunicaciones, ubicada en la provincia de Santa

Elena, Ecuador. El laboratorio de telecomunicaciones de la UPSE dispone de equipamiento básico para la evaluación de RF, aunque carece de instrumentación costosa como analizadores de espectro de alta gama. Esta limitación justifica el uso de hardware abierto (RF-Clown v2) [3] como plataforma de experimentación, acorde con la política institucional de fomentar la investigación aplicada en la optimización de recursos de bajo costo.

2.1.4. Disposición física del escenario experimental

La disposición física está formada por un RF-Clown v2 configurado como Maestro, un segundo RF-Clown v2 configurado como Esclavo, el dispositivo Bluetooth/BLE evaluado y el receptor HackRF One.

Las distancias de 1, 2 y 3 m, como se muestra en la **Figura 6**, representan las condiciones espaciales para observar el comportamiento del sistema. La distancia puede modificar el nivel recibido por el SDR y la cantidad de anuncios BLE detectados, pero no debería alterar los parámetros temporales definidos por el firmware.

La ubicación de los equipos debe mantenerse constante en cada repetición. También deben conservarse la altura, la orientación y la polarización aproximada de las antenas para reducir variaciones ajenas al estado del sistema coordinado en su totalidad.

No se presupone que la configuración lineal produzca una suma coherente de señales. Los módulos nRF24L01+ utilizan osciladores independientes y no hay coordinación de fase entre las portadoras. Por esta razón, la evaluación se basa en los niveles relativos observados y no en una combinación teórica coherente de fases.

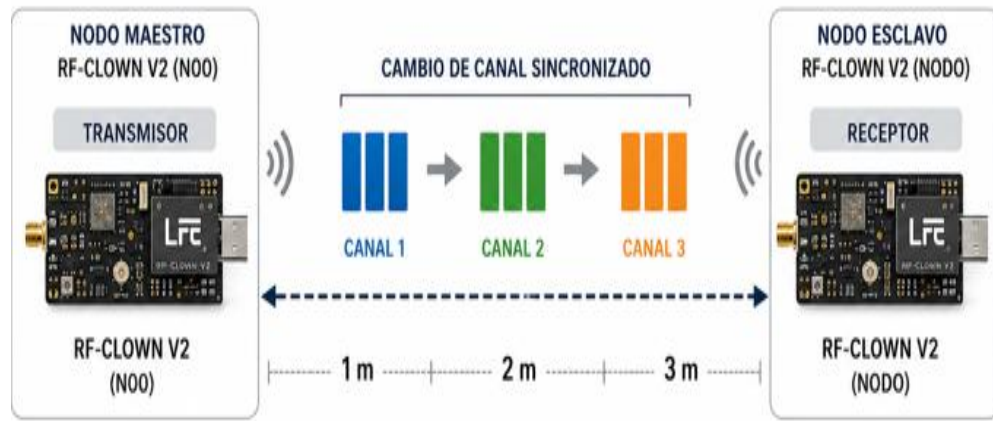


Figura 6 Distancia propuesta para las pruebas entre los RF-clown v2.0

2.2. Fundamentos de Bluetooth Classic y BLE

2.2.1. Bluetooth Classic

Bluetooth Classic, también denominado Bluetooth Basic Rate/Enhanced Data Rate, es una tecnología de comunicación inalámbrica diseñada para el intercambio continuo de información entre dispositivos de corto alcance.

La arquitectura de su capa física está diseñada para operar en la banda de frecuencia ISM (Industrial, Scientific, and Medical) de 2,4 GHz. Para mitigar las interferencias, el espectro se subdivide en 79 canales de radiofrecuencia (RF) con un ancho de banda de 1 MHz cada uno. Las frecuencias centrales pueden expresarse mediante:

$$f_x = 2402 + k \text{ [MHz]}$$

donde:

f_x : Frecuencia central del canal Bluetooth Classic (MHz).

k : Índice del canal, donde $k \in \{0, 1, \dots, 78\}$

2402 : Frecuencia inicial de la banda en MHz

Por tanto, Bluetooth Classic utiliza frecuencias centrales comprendidas entre 2402 y 2480 MHz.

El sistema divide la comunicación en ranuras temporales de 625 μ s. En condiciones normales puede realizar hasta 1600 saltos por segundo entre las frecuencias disponibles. Los saltos siguen una secuencia determinada por los parámetros de la conexión.

Bluetooth Classic también admite paquetes de una, tres o cinco ranuras. Un paquete de cinco ranuras puede permanecer durante aproximadamente:

$$T_5 = 5(625 \mu s) = 3125 \mu s = 3.125 \text{ ms}$$

Es fundamental señalar que la duración de una ranura (slot) Bluetooth no debe confundirse con el tiempo de permanencia (dwell time) programado en el dispositivo RF-Clown v2, pues se trata de parámetros de sistemas distintos.

2.2.2. Frequency Hopping Spread Spectrum (FHSS)

La técnica de espectro ensanchado por salto de frecuencia (FHSS, por sus siglas en inglés) consiste en la conmutación periódica de la frecuencia de transmisión, siguiendo una secuencia pseudoaleatoria predeterminada. Su objetivo principal es minimizar el tiempo de permanencia en canales congestionados, incrementar la robustez frente a interferencias de banda estrecha y facilitar la coexistencia con otros sistemas inalámbricos.

En Bluetooth Classic, cada salto selecciona una frecuencia del conjunto habilitado. Como consecuencia, una perturbación limitada a un canal solamente afecta la comunicación cuando coincide en frecuencia y en el tiempo con la transmisión Bluetooth.

El sistema desarrollado en esta investigación no conoce ni predice la secuencia de salto de una conexión Bluetooth. La estrategia propuesta recorre conjuntos predefinidos de canales para distribuir la actividad entre dos RF-Clown v2.

2.2.3. Adaptive Frequency Hopping

Adaptive Frequency Hopping permite clasificar los canales Bluetooth según su calidad y excluir temporalmente los que presentan altos niveles de interferencia. De esta manera, el conjunto de salto puede adaptarse a la ocupación radioeléctrica existente.

AFH (Adaptive Frequency Hopping) favorece la coexistencia de Bluetooth con otras tecnologías, especialmente con Wi-Fi. Cuando una región del espectro presenta interferencia persistente, Bluetooth reduce su uso y prioriza los canales clasificados como adecuados.

Esta capacidad explica por qué una emisión concentrada de forma permanente en una sola frecuencia no garantiza una alteración continua de la comunicación. Si bien la distribución de la actividad en múltiples frecuencias incrementa la probabilidad de colisión, el impacto real de este fenómeno debe comprobarse mediante la experimentación y la recolección de datos de campo.

2.2.4. Bluetooth Low Energy

Bluetooth Low Energy es una tecnología orientada a comunicaciones de bajo consumo. Su capa física utiliza 40 canales separados por 2 MHz, de los cuales 37 se destinan principalmente al intercambio de datos y 3 a la publicidad primaria, como se muestra en la tabla 2.

Los canales de publicidad primaria son:

Tabla 2

Canales de anuncios BLE

Canal BLE	Frecuencia central	Ubicación en la banda
37	2402 MHz	Inicio de la banda de 2.4 GHz
38	2426 MHz	Zona intermedia
39	2480 MHz	Final de la banda de 2.4 GHz

Los anuncios (advertisements) BLE permiten que un dispositivo transmita periódicamente información de identificación, disponibilidad y servicios. Estos eventos pueden ser recibidos por aplicaciones de análisis sin necesidad de establecer una conexión permanente.

En esta investigación, los anuncios recibidos se utilizan como indicador experimental porque pueden capturarse y contabilizarse mediante los programas Acrylic Suite y Wireshark.

El número de anuncios capturados por el analizador mostrado en la **Figura 7** no representa necesariamente la cantidad total transmitida por el dispositivo. Por esta razón, no es posible calcular directamente una tasa real de pérdida de paquetes basándose exclusivamente en la información proporcionada por la aplicación.

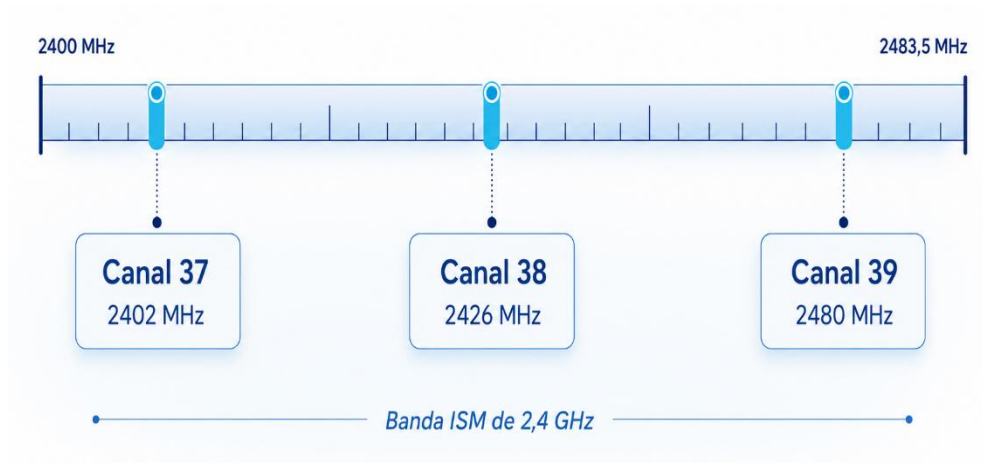


Figura 7 Canales de publicidad primaria de BLE

2.3. Plataforma RF-Clown v2

2.3.1 Descripción general

El RF-Clown v2 es una plataforma abierta orientada a la experimentación en la banda de 2,4 GHz. Su arquitectura, mostrada en la **Figura 8**, integra un microcontrolador ESP32, tres módulos nRF24L01+, una pantalla OLED, botones de control y un indicador NeoPixel.

La disponibilidad del código fuente permite modificar el comportamiento del dispositivo e implementar nuevas funciones. En el proyecto se desarrollan dos versiones del firmware: una para el Maestro y otra para el Esclavo.

Los tres módulos nRF24L01+ se identifican como:

- Radio A.
- Radio B.
- Radio C.

Las radios A y B se destinan a la operación radioeléctrica en los canales asignados. La radio C se reserva para el enlace de sincronización ESB.

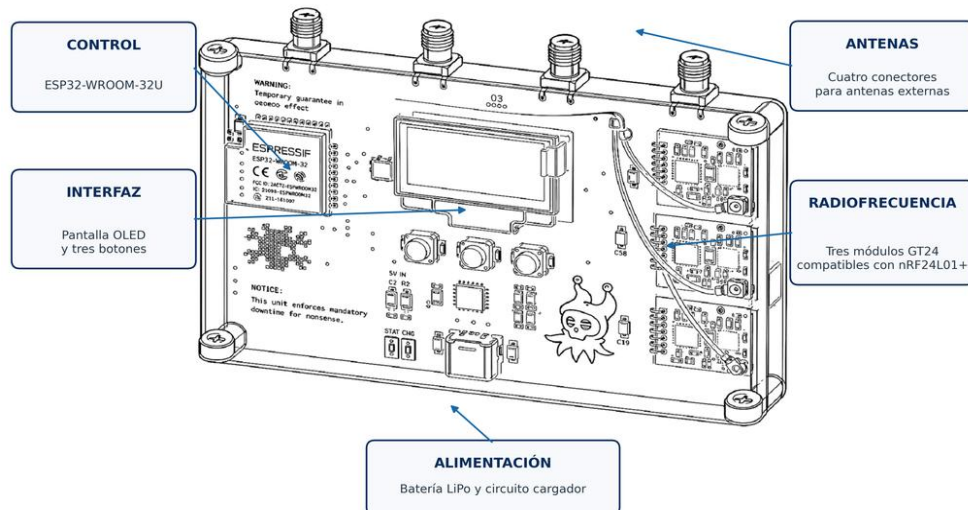


Figura 8 Componentes principales del RF-Clown v2.0

2.3.2. Microcontrolador ESP32

El ESP32 es el elemento encargado de ejecutar el firmware, controlar los módulos nRF24L01+, actualizar la pantalla OLED, procesar las entradas de los botones y supervisar los estados operativos del sistema.

En el proyecto, el ESP32 realiza las siguientes funciones:

- Inicialización de las radios A, B y C.
- Selección del modo de operación (Maestro o Esclavo).
- Gestión de la tabla de canales.
- Cambio del canal de las radios A y B.
- Transmisión o recepción de paquetes mediante el protocolo ESB.
- Actualización del sequenceID.
- Control del heartbeat.
- Supervisión del timeout.
- Actualización de OLED y NeoPixel.
- Generación de registros para el monitor serial.

El firmware se desarrolla y se programa en Arduino IDE.

2.3.3. Transceptor nRF24L01+

El nRF24L01+ es un transceptor de 2,4 GHz que permite configurar parámetros como el canal, la tasa de transferencia de datos, el nivel de potencia de salida, la dirección lógica, la verificación de redundancia cíclica (CRC) y las funciones de confirmación automática.

Datos técnicos principales:

- Frecuencia: Opera en la banda ISM de 2,4 GHz, compartida con tecnologías como la red Wi-Fi.
- Voltaje: Uso de 1.9 V a 3.6 V (Alimentarlo con 5 V quema el chip).
- Conexión: Usa el protocolo SPI (ocupa 5 pines de control).
- Alcance: La versión estándar con antena integrada en la placa alcanza aproximadamente 100 metros.
- La versión con antena externa y amplificador (PA+LNA) puede alcanzar hasta 1 km.

2.3.4. Función de los radios A y B

Los datos técnicos principales del sistema describen las características fundamentales que definen su modo de operación y sus limitaciones físicas. En cuanto a la frecuencia, el dispositivo opera en la banda de 2.4 GHz, la misma que comparten las redes Wi-Fi, lo que exige considerar los fenómenos de interferencia y la coexistencia con otros equipos en dicho espectro. Respecto al voltaje de alimentación, el rango operativo seguro se sitúa entre 1.9 V y 3.6 V; es crítico no exceder este límite, ya que alimentarlo con 5 V provocaría daños irreversibles en el chip. Con respecto a la interconexión, el módulo emplea el protocolo SPI, que requiere cinco pines de control para comunicarse con el microcontrolador. En cuanto al alcance, la versión básica con antena integrada en placa tiende a una cobertura de aproximadamente 100 metros en condiciones ideales, mientras que la versión mejorada con antena externa y amplificador integrado (PA+LNA) extiende significativamente su alcance hasta 1 kilómetro, lo que amplía las posibilidades de despliegue en entornos más exigentes o con mayores requerimientos de

cobertura. En la versión definitiva del firmware, las radios A y B de un mismo RF-Clown operan simultáneamente en el mismo canal seleccionado.

Para el Maestro:

$$CH_{A1} = CH_{B1} = CH_{impar}$$

Para el Esclavo:

$$CH_{A2} = CH_{B2} = CH_{par}$$

donde:

CH_A : Canal configurado en la radio A.

CH_B : Canal configurado en la radio B.

1: Nodo maestro.

2: Nodo esclavo.

CH_{impar} : Canal impar seleccionado.

CH_{par} : Canal par seleccionado.

En cada nodo, las radios A y B operan simultáneamente en el mismo canal. El Maestro trabaja en canales impares y el Esclavo en canales pares.

La potencia total de las radios A y B, cuando operan simultáneamente en el mismo canal, se expresa en escala lineal como:

$$P_{total} = P_A = P_B$$

Si ambas radios transmiten con la misma potencia:

$$P_A = P_B = P$$

entonces:

$$P_{total} = P + P = 2P$$

El incremento teórico de potencia en decibelios es:

$$\Delta P = 10 \log_{10}\left(\frac{P_{total}}{P}\right)$$

Sustituyendo $P_{total} = 2P$

$$\Delta P = 10 \log_{10}(2) \approx 3.01 \text{ dB}$$

Por tanto:

$$P_{total,dB} \approx P_{individual,dB} + 3.01 \text{ dB}$$

Este valor es solo una referencia ideal. El incremento real depende de la capacidad de las antenas, así como de las pérdidas, la alimentación, la distancia, la orientación y las diferencias entre los módulos.

2.3.5. Función de la radio C

La radio C se utiliza exclusivamente para la coordinación mediante ESB. Su canal se fija en:

$$RF_CH_C = 81$$

Aplicando la ecuación de frecuencia del nRF24L01+:

$$f_C = 2400 + RF_CH_C$$

Sustituyendo:

$$f_C = 2400 + 81$$

$$f_C = 2481 \text{ MHz}$$

La frecuencia de 2481 MHz pertenece a la banda ISM de 2,4 GHz, pero se encuentra fuera del límite superior de Bluetooth Classic y de los canales de publicidad primarios de BLE.

En el Maestro, la radio C transmite los paquetes de coordinación. En el Esclavo, la radio C permanece en recepción para actualizar el estado del sistema.

2.4 Protocolo Enhanced ShockBurst

2.4.1. Descripción del protocolo

Enhanced ShockBurst es un protocolo de enlace incorporado en los transceptores nRF24L01+. Su implementación facilita el intercambio de paquetes cortos y proporciona funciones como:

- Direcccionamiento lógico.
- Verificación de integridad.
- Confirmación automática.
- Control de retransmisiones.
- Manejo de carga útil.
- Identificación de recepción válida.

En la arquitectura propuesta, el Maestro transmite paquetes de control y el Esclavo interpreta su contenido para actualizar su estado.

2.4.2. Paquete de coordinación

El paquete utilizado por el sistema debe contener únicamente los campos necesarios para

la operación. Una estructura básica puede incluir:

Tabla 3
Estructura básica de operación

Campo	Función
role	Identifica el rol del transmisor.
active	Indica si la operación está activa.
currentMode	Identifica el modo de operación seleccionado.
sequenceID	Permite identificar y verificar la secuencia de los paquetes.
checksum	Realiza una verificación adicional de la integridad del paquete, definida en el firmware.

La estructura final de la tabla 3 debe coincidir exactamente con el código compilado. Únicamente deben incluirse los campos que estén completamente implementados.

2.4.3. Heartbeat

El heartbeat es un paquete periódico utilizado para notificar al dispositivo seguidor o, en este caso, al modo esclavo que el nodo líder (o central) continúa activo y disponible. Cada recepción válida de este paquete actualiza el registro con la marca de tiempo (timestamp) del último mensaje recibido.

Si el intervalo entre el último heartbeat válido y el tiempo actual supera el valor configurado, el Esclavo activa el mecanismo de timeout.

2.4.4. Timeout de seguridad

El timeout impide que el Esclavo permanezca activo indefinidamente cuando se pierde el

enlace con el Maestro.

La condición para detectar la pérdida de comunicación se expresa como:

$$t_{actual} - t_{ultimo\ paquete} \geq T_{timeout}$$

Cuando el tiempo transcurrido desde el último paquete recibido alcanza o supera el tiempo de espera establecido:

$$Estado_{esclavo} = DESACTIVADO$$

De acuerdo con la configuración que usaremos en el firmware:

$$T_{timeout} = 15000\ ms = 15\ s$$

La condición completa puede representarse como:

$$t_{actual} - t_{ultimo\ paquete} \geq 15000\ ms \rightarrow Estado_{esclavo} = DESACTIVADO$$

2.4.5. SequenceID y paquetes no recibidos

El sequenceID es un contador incremental incluido en los paquetes de coordinación. El

Esclavo puede comparar la secuencia recibida con la esperada:

$$\Delta seq = seq_{recibido} - seq_{anterior}$$

La interpretación es la siguiente:

$$\Delta seq = 1 \rightarrow \text{secuencia continua}$$

$$\Delta seq > 1 \rightarrow \text{secuencia paquetes perdidos}$$

Pueden existir identificadores intermedios no observados.

El número estimado de paquetes no recibidos entre dos identificadores puede calcularse mediante:

$$N_{perdidos} = \Delta seq - 1$$

Este cálculo es estrictamente válido cuando el contador se administra de forma continua y secuencial, asumiendo la ausencia de reinicios (resets); no existen reinicios, desbordamientos ni actualizaciones del sequenceID que no correspondan a una transmisión real.

2.5 Arquitectura de coordinación Maestro–Esclavo

2.5.1. Nodo Maestro

El Maestro administra el estado general del sistema. Sus principales funciones son:

- Seleccionar los canales impares.
- Configurar las radios A y B en el mismo canal.
- Transmitir paquetes de coordinación en la radio C.
- Incrementar el sequenceID.
- Mostrar el estado en la pantalla OLED.
- Actualizar el indicador NeoPixel.
- Implementar el registro continuo de datos (data logging) procedentes del puerto serie para su análisis.

El Maestro no transmite al Esclavo la secuencia de salto de un dispositivo Bluetooth. Solamente comunica el estado definido por el firmware y mantiene el enlace de coordinación.

2.5.2. Nodo Esclavo

El Esclavo recibe los paquetes en la radio C y activa las condiciones programadas. Sus funciones principales son:

- Recibir los paquetes ESB.
- Verificar el estado activo o inactivo.
- Seleccionar canales pares.
- Configurar las radios A y B en el mismo canal.
- Actualizar el sequenceID recibido.
- Registrar discontinuidades de secuencia.
- Supervisar el timeout.
- Desactivarse cuando el enlace termine.
- Mostrar su estado mediante OLED y NeoPixel.

2.5.3. Distribución de canales

La estrategia divide los canales según su paridad:

El nodo Maestro recorre los canales impares

$$CH_M = \{1,3,5,7, \dots\}$$

El nodo Esclavo recorre los canales pares:

$$CH_E = \{0,2,4,6, \dots\}$$

El canal 81 no se utiliza en estos recorridos porque está reservado para la comunicación

ESB:

$$CH_{ESB} = 81$$

Por tanto:

$$81 \notin CH_M \text{ y } 81 \notin CH_E$$

La operación completa se puede resumir mediante:

- Maestro $\rightarrow$ canales impares, excepto el 81
- Esclavo $\rightarrow$ canales pares
- Radio C $\rightarrow$ canal 81 para ESB

Los canales se dividen entre ambos nodos para evitar que recorran simultáneamente las mismas frecuencias. El Maestro trabaja con los canales impares y el Esclavo con los canales pares. El canal 81 se excluye del recorrido del Maestro porque se reserva exclusivamente para la comunicación de sincronización ESB mediante la radio C.

2.5.4. Operación conjunta de las radios A y B

En cada iteración, el firmware selecciona un canal de la tabla correspondiente al rol y configura ambas radios:

$$CH_A(n) = CH_B(n) = CH(n)$$

El siguiente canal se obtiene mediante la actualización del índice:

$$i_{siguiente} = (i_{actual} + 1) \bmod N$$

donde:

($i(n)$) Es el índice actual.

(N) Es el número de elementos de la tabla.

($CH(n)$) Es el canal seleccionado.

Esta operación concentra los dos radios del mismo nodo en una única frecuencia, como se muestra en la **Figura 9**. No corresponde a una estrategia multitone, porque las radios A y B no transmiten simultáneamente en frecuencias diferentes.

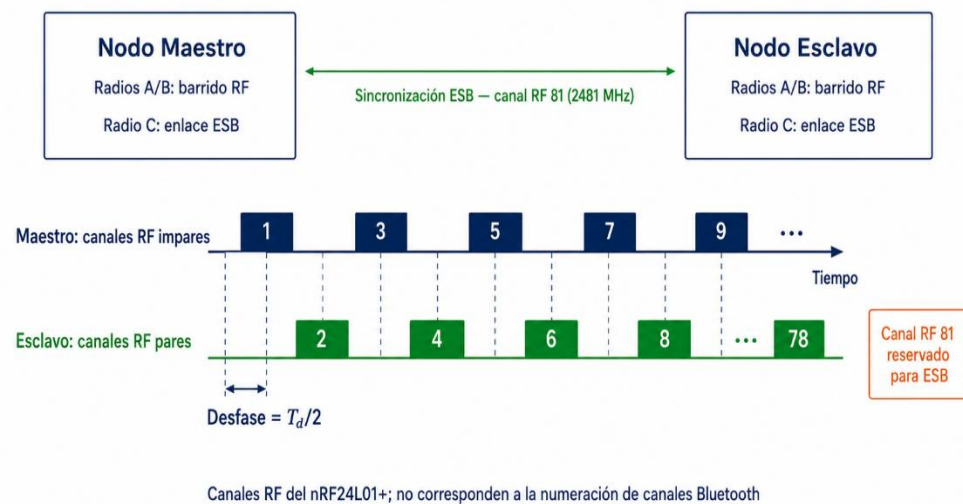


Figura 9 Arquitectura de las radios A, B y C

Para ilustrar la lógica operativa del sistema propuesto, se presenta un diagrama que describe la interacción entre el nodo maestro y el esclavo bajo el protocolo ESB. Este proceso garantiza que la latencia de coordinación sea inferior a $505 \mu s$ [9], lo que permite que la alternancia de canales desfasada ocurra con la precisión temporal necesaria para afectar el

mecanismo FHSS de la víctima.

2.6. Fundamentos matemáticos de las métricas

2.6.1. Tiempo de permanencia

El tiempo de permanencia se basa en la duración durante la cual la actividad detectada se mantiene por encima de un umbral en una frecuencia dada.

Se calcula mediante:

$$T_{\text{permanencia}} = t_f - t_i$$

donde

$T_{\text{permanencia}}$: Tiempo durante el cual la radio permanece operando en un canal.

t_i : Instante de inicio de la operación en el canal.

t_f : Instante de finalización de la operación en el canal.

Por ejemplo, si:

$$t_i = 10.000ms \quad \text{y} \quad t_f = 10.125ms$$

entonces:

$$T_{\text{permanencia}} = 10.125 - 10.000 = 0.125 \text{ ms}$$

Por tanto:

$$T_{\text{permanencia}} = 0.125 \text{ ms}$$

Esta medición se obtiene con GNU Radio tras aislar la frecuencia observada y representar la potencia relativa en función del tiempo.

2.6.2. Tiempo de revisita

El tiempo de revisita es el intervalo entre dos apariciones de actividad con la misma frecuencia.

Se calcula mediante:

$$T_{revisita} = t_2 - t_1$$

donde

$T_{revisita}$: Tiempo transcurrido hasta que el sistema vuelve a operar en el mismo canal.

t_1 : Instante de una aparición válida del canal.

t_2 : Instante de la siguiente aparición válida del mismo canal.

Por ejemplo, si:

$$t_1 = 10ms \quad y \quad t_2 = 50ms$$

entonces:

$$T_{revisita} = 50 - 10 = 40 \text{ ms}$$

Por tanto:

$$T_{revisita} = 40 \text{ ms}$$

El tiempo de revisita depende principalmente de la cantidad de canales programados, del orden del recorrido y del tiempo empleado en cada cambio. En términos sencillos, esta métrica indica cada cuánto tiempo el sistema vuelve al mismo canal.

2.6.3. Tiempo teórico de ciclo

Si una tabla contiene (N) canales y cada canal utiliza un tiempo de permanencia programado (T_d), el tiempo teórico de ciclo.

Se calcula mediante:

$$T_{ciclo} = NT_d - t_i$$

donde

T_{ciclo} : Duración total de un ciclo completo de barrido durante el cual la radio permanece operando en un canal.

t_i : Duración total de un ciclo completo de barrido.

N : Número de canales incluidos en la tabla de recorrido.

T_d : Tiempo de permanencia en cada canal (dwell time).

Por ejemplo, si se recorren 40 canales y el tiempo de permanencia es 2 ms:

$$N = 40, \quad y \quad T_d = 2ms$$

entonces:

$$T_{ciclo} = 40(2 \text{ ms}) = 80 \text{ ms}$$

Por tanto:

$$T_{ciclo} = 80 \text{ ms}$$

Los valores provienen de las mediciones realizadas con HackRF One y GNU Radio.

2.6.4. Nivel relativo en dBFS

El HackRF One digitaliza la señal recibida y GNU Radio expresa su amplitud en relación con el nivel máximo de la escala digital. Esta unidad se denomina dBFS.

El incremento relativo entre la condición activa y la referencia se calcula mediante:

$$\Delta P = P_{activo} - P_{referencia}$$

Si:

$$P_{referencia} = -70.87 \text{ dBFS}$$

y:

$$P_{activo} = -41.09 \text{ dBFS}$$

entonces:

$$\Delta P = -41.09 - (-70.87)$$

$$\Delta P = -41.09 + 70.87$$

$$\Delta P = 29.78 \text{ dB}$$

Esto significa que el nivel medido durante la operación activa fue 29,78 dB superior al nivel de referencia.

Los niveles medidos se expresan en dBFS y su diferencia en dB. El resultado representa únicamente un incremento relativo respecto de la referencia.

2.6.5. Recepción relativa de anuncios

La recepción relativa de anuncios compara la cantidad de registros recibidos durante la condición activa con la cantidad registrada durante una referencia de duración predeterminada.

Se define como:

$$ARR(\%) = \frac{N_{activo}}{N_{referencia}} \times 100$$

Donde:

- $N_{referencia}$: Número de anuncios recibidos en la condición de referencia o basal.
- N_{activo} : Número de anuncios recibidos durante la activación del sistema.
- ARR_i : Porcentaje de anuncios recibidos durante la activación respecto a la referencia.

La reducción relativa de anuncios se obtiene mediante:

$$R_{ARR}(\%) = 100\% - ARR(\%)$$

Para evaluar la recuperación después de desactivar el sistema:

$$ARR_{posterior}(\%) = \frac{N_{posterior}}{N_{referencia}} \times 100$$

Donde $N_{posterior}$ es el número de anuncios recibidos durante la condición posterior.

Estos indicadores permiten comparar condiciones de la misma duración. Sin embargo, no representan una tasa real de pérdida de paquetes, por lo que se desconoce el volumen exacto de transmisión que generó el dispositivo BLE.

2.7. Herramientas de medición y análisis

2.7.1. HackRF One

HackRF One es un dispositivo de radio definida por software capaz de operar como

transmisor o receptor, lo que le permite abarcar un amplio rango de frecuencias. En esta investigación se utiliza exclusivamente como receptor para observar la actividad en la banda de 2,4 GHz.

El HackRF One de la **Figura 10** permite capturar muestras complejas I/Q que posteriormente serán procesadas por GNU Radio. Sus resultados dependen de la ganancia configurada, la antena, la distancia, la orientación y la resolución del flujo de procesamiento.



Figura 10 SDR HackRF One

Debido a que el sistema no se encuentra calibrado como analizador de espectro, sus resultados se utilizan para:

- Identificar presencia de actividad.
- Observar frecuencias recorridas.
- Comparar niveles relativos.
- Medir tiempos de permanencia.

- Medir tiempos de revisita.

No se utiliza para afirmar valores absolutos de potencia radiada. El tiempo de permanencia indica la duración durante la cual la actividad detectada se mantiene por encima de un umbral en una frecuencia establecida.

2.7.2. GNU Radio

GNU Radio, mostrado en la **Figura 11**, es un entorno de procesamiento de señales que permite construir diagramas de bloques. En el proyecto se emplean principalmente:

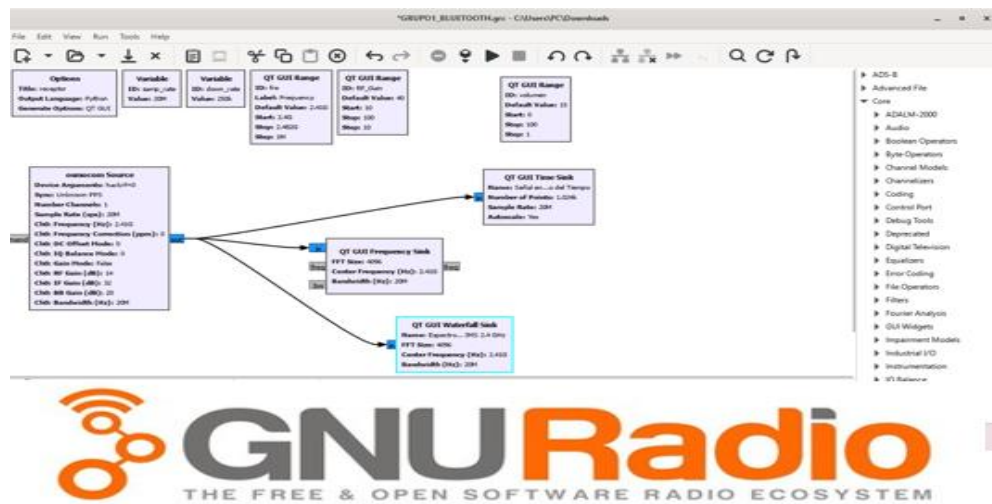


Figura 11 Software GNU Radio

- Osmocom Source para recibir las muestras del HackRF One.
- QT GUI Frequency Sink para observar el dominio de la frecuencia.
- QT GUI Waterfall Sink para visualizar la evolución de la frecuencia a lo largo del tiempo.

- Frequency Xlating FIR Filter para aislar una frecuencia.
- Complex to Mag² para obtener la potencia relativa.
- Moving Average para suavizar la señal.
- QT GUI Time Sink para observar la actividad temporal.

El análisis de la banda de 2400 a 2483,5 MHz se realiza por secciones (ventanas), ya que el ancho de banda instantáneo configurado impide una visualización con la misma resolución en una sola captura.

2.7.3. Acrylic Suite

En la **Figura 12** se muestra que Acrylic Suite se utiliza para capturar anuncios BLE y seleccionar el dispositivo evaluado por su dirección MAC y su nombre.

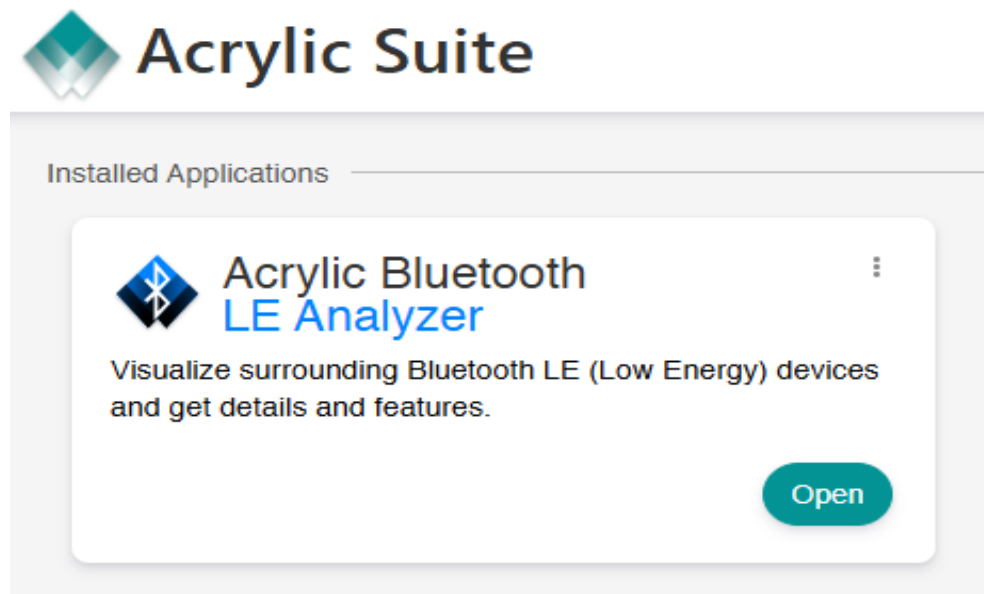


Figura 12 Software capturador de anuncios BLE

La aplicación permite guardar los registros en archivos PCAP. Cada captura debe

realizarse durante un intervalo definido y bajo una condición experimental específica:

- Referencia.
- Sistema activo.
- Condición posterior.

La numeración general mostrada por la aplicación no debe utilizarse directamente para calcular los anuncios de un dispositivo cuando la captura incluye registros de otros equipos.

2.7.4. Wireshark

En la **Figura 13**, Wireshark se utiliza para abrir y analizar los archivos PCAP generados por Acrylic Suite. El conteo debe incluir únicamente los registros del dispositivo objetivo.



Figura 13. Capturador de paquetes Wireshark

La identificación puede verificarse mediante:

- Dirección MAC.
- Nombre local.

- Contenido del paquete.
- Marca temporal.
- Duración de la captura.

Se utiliza una nomenclatura única para cada repetición (3 archivos) que permita identificar la distancia, el número de ensayo y la condición.

2.7.5. Arduino IDE

En la **Figura 14** se muestra el uso de Arduino IDE para compilar, cargar y supervisar el firmware de ambos RF-Clown v2.

El monitor serial permite observar:

- Rol del dispositivo.
- Canal seleccionado.
- Frecuencia equivalente.
- Estado activo o inactivo.
- SequenceID.
- Heartbeat.
- Estado del enlace.
- Activación del timeout.
- Cantidad de cambios de canal.

Los registros seriales constituyen evidencia funcional, pero no reemplazan una medición física de la latencia mediante instrumentación temporal especializada.

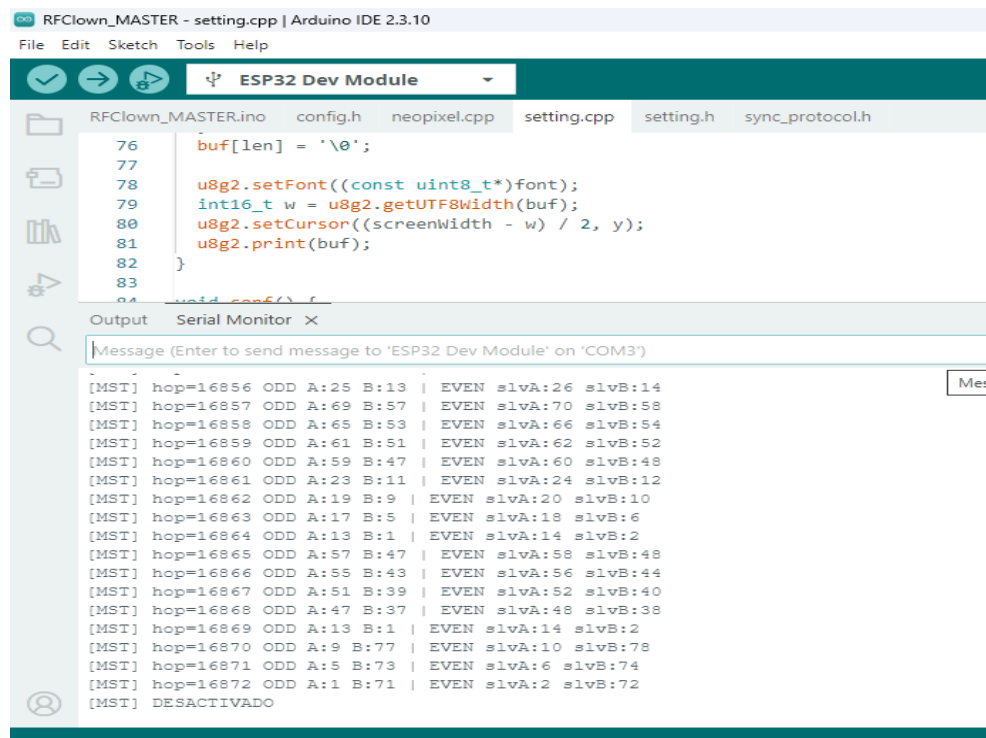


Figura 14 Plataforma Arduino Id.

2.8. Marco normativo y ético

2.8.1. Regulaciones nacionales (ARCOTEL)

La Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) **Figura 15**, en el Plan Nacional de Frecuencias 2021 aprobado mediante la Resolución Nro. 04-02-ARCOTEL-2021 [8], establece la atribución de la banda comprendida entre 2400 MHz y 2483,5 MHz para el territorio ecuatoriano. En este segmento espectral operan aplicaciones industriales, científicas y médicas (ISM), así como sistemas de radiocomunicaciones de corto alcance, por lo que deben cumplir estrictamente con las condiciones técnicas vigentes.

Es preciso señalar que el uso de esta banda no garantiza protección contra interferencias ni faculta a los usuarios para generar emisiones que causen interferencia perjudicial como en otros servicios autorizados. En consecuencia, los equipos deben operar estrictamente conforme a

las condiciones técnicas vigentes, controlar sus emisiones fuera de banda (out-of-band emissions) y cesar su funcionamiento ante cualquier riesgo de afectación a los servicios de telecomunicaciones debidamente autorizados.

No debe afirmarse que el sistema cumple un límite específico de potencia sin haber medido la potencia radiada, la ganancia real de las antenas y la PIRE resultante. La configuración RF24_PA_MAX corresponde a un parámetro del firmware y no constituye, por sí sola, una medición certificada.



Figura 15 Identidad institucional de ARCOTEL

2.8.2. Operación segura

Los ensayos deben cumplir las siguientes condiciones:

1. Utilizar únicamente equipos propios o autorizados.
2. Realizar las pruebas en un entorno controlado.
3. Evitar espacios públicos.
4. Mantener una duración limitada.
5. Utilizar la mínima potencia necesaria.
6. Verificar la banda observada mediante el SDR.
7. Mantener disponible un mecanismo de apagado inmediato.

8. Registrar la fecha, el responsable y la configuración.
9. Suspender la prueba ante cualquier afectación a terceros.
10. Conservar evidencia del montaje y de las condiciones de operación.

2.8.3. Consideraciones éticas

El objetivo de la investigación es analizar una arquitectura de coordinación en un escenario experimental autorizado. El sistema no debe utilizarse para degradar redes, dispositivos o servicios ajenos.

Para mantener una redacción académica, se utilizan expresiones como:

- Sistema coordinado.
- Emisión de prueba.
- Dispositivo evaluado.
- Condición activa.
- Ensayo controlado.

Se evita presentar la investigación como una herramienta orientada a ataques reales o a la afectación de terceros.

2.9. Estado del arte y trabajos relacionados

A continuación, se presenta la tabla 4 con la cronología de los principales aportes y sus respectivos vacíos, identificando cómo la presente investigación se posiciona frente a estos.

Tabla 4
Científico/Aporte

Autor/Proyecto	Año	Aporte principal	Vacío o limitación identificada
Hanawal et al.	2020	Adaptación conjunta de FHSS y tasa de transmisión para anti-jamming	Enfoque teórico, sin implementación práctica en hardware accesible
Liu y Fok	2020-2021	Sistemas FHSS fotónicos de ultra alta velocidad (nanosegundos)	Hardware costoso, no aplicable a dispositivos comerciales Bluetooth
CVE-2023-40129	2023	Vulnerabilidad crítica en stack Fluoride de Android	No propone herramienta de prueba; solo notificación de fallo
Moore et al.	2024	Soft Tester UE para pruebas de seguridad en 5G/O-RAN	Enfoque en redes celulares, no en Bluetooth/BLE; hardware diferente
CiferTech (RF-Clown v2)	2025	Hardware abierto para interferencia controlada en BLE/Bluetooth	Firmware oficial sin capacidad de coordinación multidispositivo
Krull et al.	2025	Caracterización de latencia ESB (504.99 μ s) para sincronización deportiva	No aplica a jamming; no implementa coordinación entre nodos de interferencia
Antonioli (BLUFFS)	2025	Ataques a confidencialidad de sesiones Bluetooth	Aborda capa de enlace, no ataques físicos de denegación de servicio
CVE-2025-47370	2025	DoS en chipsets Qualcomm por solicitud de conexión inválida	Vulnerabilidad específica, no generalizable a todos los dispositivos

Vacío de conocimiento identificado:

No existe, en la literatura abierta hasta abril de 2026, una implementación documentada de coordinación entre dos o más RF-Clown v2 que utilice exclusivamente los módulos nRF24L01+ integrados en la sincronización y que valide experimentalmente la mejora en la tasa de desconexión de dispositivos Bluetooth/BLE en configuración lineal.

Aporte novedoso de esta investigación:

El desarrollo de una estrategia de coordinación lineal entre dos RF-Clown v2, demostrando cuantitativamente el incremento en la efectividad de la interferencia (ARR y cobertura temporal) respecto de la operación individual, todo ello dentro del marco legal ecuatoriano y con hardware de código abierto.

CAPÍTULO III

3 DESARROLLO METODOLÓGICO E IMPLEMENTACIÓN DEL SISTEMA

3.1 Presentación

En este capítulo se describe la metodología empleada para implementar y validar la coordinación entre dos dispositivos RF-Clown v2 configurados como Maestro y Esclavo. Se presentan las modificaciones realizadas al firmware, la disposición del escenario experimental y los procedimientos aplicados para obtener evidencia funcional, espectral y temporal.

La evaluación se realizó con separaciones de 1, 2 y 3 m entre los RF-Clown. El sistema fue supervisado mediante Arduino IDE, mientras que las mediciones instrumentales se realizaron con un receptor HackRF One y GNU Radio. Para evaluar la recepción de anuncios BLE se

utilizaron Acrylic Suite y Wireshark.

Los fundamentos de Bluetooth, ESB, las radios del RF-Clown y las métricas fueron desarrollados en el Capítulo II. Por esta razón, el presente capítulo se limita a explicar cómo se implementó el sistema y cómo se realizaron los ensayos. Los valores obtenidos y su interpretación se presentan en el Capítulo IV.

3.2 Diseño metodológico

La investigación presenta un enfoque cuantitativo, experimental y aplicado. Es cuantitativa porque utiliza mediciones instrumentales, registros seriales y archivos de captura. Es experimental porque se modifica el estado del sistema coordinado y se observa su comportamiento en condiciones controladas. Se clasifica como una investigación aplicada e implementada, ya que desarrolla una solución funcional mediante la optimización del firmware del RF-Clown v2.

Las pruebas consideraron tres distancias de separación y diez repeticiones por escenario. Durante cada ensayo se mantuvieron constantes la orientación de las antenas, la alimentación, la posición del dispositivo evaluado y la configuración de los instrumentos.

3.2.1. Variables experimentales

Tabla 5
Parámetros y variables experimentales

Tipo	Variable	Indicador
Independiente	Estado del sistema	Desactivado, activo y posterior
Independiente	Distancia entre nodos	1 m, 2 m y 3 m
Dependiente	Nivel relativo	Lectura en dBFS

Tipo	Variable	Indicador
Dependiente	Tiempo de permanencia	Duración del pulso en milisegundos
Dependiente	Tiempo de revisita	Intervalo entre apariciones sucesivas
Dependiente	Recepción de anuncios BLE	Cantidad de registros por captura
Dependiente	Continuidad del enlace ESB	sequenceID y estado del enlace
Controlada	Duración de captura ARR	60 segundos
Controlada	Configuración del HackRF One	Tasa de muestreo y ganancias constantes
Controlada	Posición de los equipos	Altura, orientación y punto medio constantes
Controlada	Dispositivo evaluado	Mismo nombre y dirección MAC

3.3 Base de desarrollo del sistema coordinado

El proyecto tomó como punto de partida una versión funcional del firmware del RF-Clown v2. Esta base permitió validar el correcto funcionamiento de los componentes clave: el microcontrolador ESP32, los módulos nRF24L01+, la pantalla OLED, los botones y los indicadores NeoPixel.

Tras el análisis inicial, se determinó que el firmware original estaba diseñado para la operación independiente de cada dispositivo, en ausencia de un protocolo de coordinación interunidad. Por esta razón, se desarrollaron dos versiones especializadas del firmware: Maestro y Esclavo, con el objetivo principal de implementar una arquitectura de comunicación jerárquica.

Las modificaciones se orientaron a:

- Incorporación de los roles definidos de Maestro y Esclavo para la coordinación entre unidades.

- Reservar la radio C para el enlace de coordinación.
- Distribuir los canales según su paridad.
- Configurar conjuntamente las radios A y B.
- Incorporar heartbeat y timeout.
- Registrar el identificador de secuencia.
- Mostrar el estado operativo en la pantalla OLED y en el NeoPixel.
- Implementación de un sistema de registro continuo (data logging) de la información recibida a través del puerto serie, facilitando así el análisis y el diagnóstico del sistema.

El código completo del firmware se incluye en los anexos o en un repositorio institucional.

3.4 Arquitectura general implementada

El dispositivo maestro se programó para recorrer los canales impares y transmitir la información de coordinación de la **Figura 16**. El esclavo se configuró para recorrer los canales pares y recibir el estado enviado por el maestro.

En cada nodo, las radios A y B operan simultáneamente en el mismo canal seleccionado. La radio C se utiliza para mantener el enlace ESB en el canal 81.

1. Nodo Maestro: administra la activación, selecciona los canales impares y transmite paquetes de coordinación.
2. Nodo Esclavo: recibe el estado del Maestro, selecciona los canales pares y supervisa la pérdida del enlace.

3. Radios de operación: en las radios A y B de cada dispositivo trabajan simultáneamente en el mismo canal seleccionado.
4. Enlace ESB: las radios C mantienen la comunicación en el canal 81, equivalente a 2481 MHz.
5. Supervisión: OLED, NeoPixel y monitor serial.
6. Seguridad: Desactivación mediante timeout.
7. Sistema de medición: incluye HackRF One, GNU Radio, Acrylic Suite, Wireshark, Arduino IDE y los dispositivos Bluetooth/BLE evaluados.

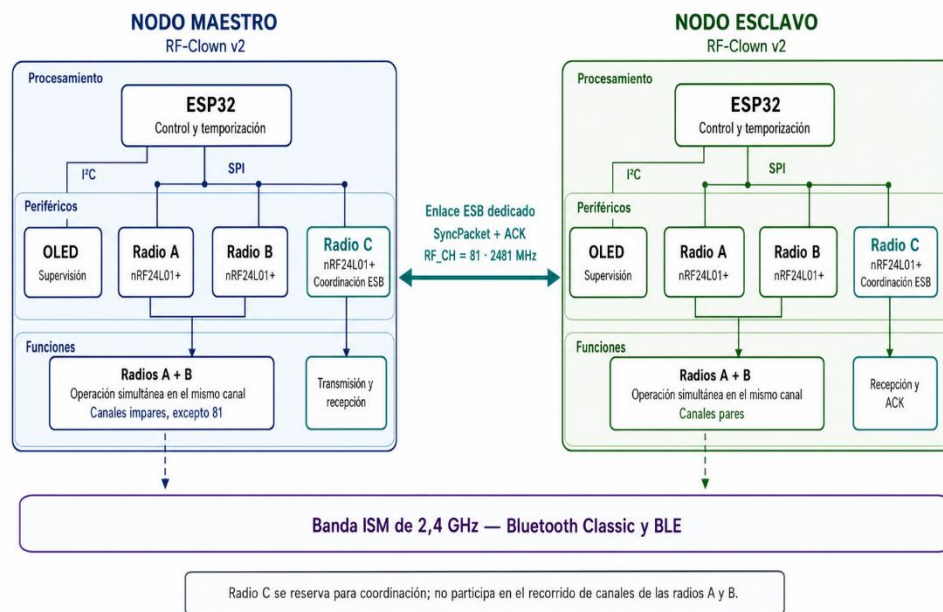


Figura 16 Arquitectura implementada

La arquitectura no proporciona sincronización de fase entre las portadoras. Cada módulo nRF24L01+ utiliza su propio oscilador, por lo que la coordinación implementada es lógica y temporal, no coherente en fase.

3.4.1. Funcionamiento del Maestro

El nodo Maestro ejecuta las siguientes actividades:

El nodo Maestro ejecuta un ciclo continuo de actividades que comienza con la configuración de sus periféricos y módulos de radio, seguida de la carga de la tabla de canales impares. Tras esta inicialización, el nodo permanece en estado de espera hasta recibir una orden de activación del usuario. Al recibir dicha orden, selecciona un canal de su tabla y configura tanto la radio A como la radio B para operar en la frecuencia seleccionada. A continuación, transmite el estado del sistema a través de la radio C, actualiza el identificador de secuencia (sequenceID) y cambia al siguiente canal de la tabla. Este procedimiento se ejecuta de forma sucesiva en cada canal hasta la recepción de la orden de desactivación, lo que suspende la operación del nodo.

3.4.2. Funcionamiento del Esclavo

El nodo Esclavo ejecuta un procedimiento sistemático de inicialización de sus periféricos y módulos de radio, así como la carga de la tabla de canales pares. Una vez completada esta fase, mantiene la radio C en modo de recepción, a la espera de un paquete válido procedente del nodo Maestro. Al recibir dicho paquete, actualiza su estado operativo y selecciona un canal de su tabla, configurando las radios A y B para operar en esa misma frecuencia. Simultáneamente, registra el sequenceID, el contenido del paquete recibido y supervisa continuamente el tiempo transcurrido desde la última comunicación exitosa. Si dicho tiempo excede el límite establecido (timeout), el nodo Esclavo se desactiva automáticamente, suspendiendo o finalizando la operación hasta una nueva inicialización.

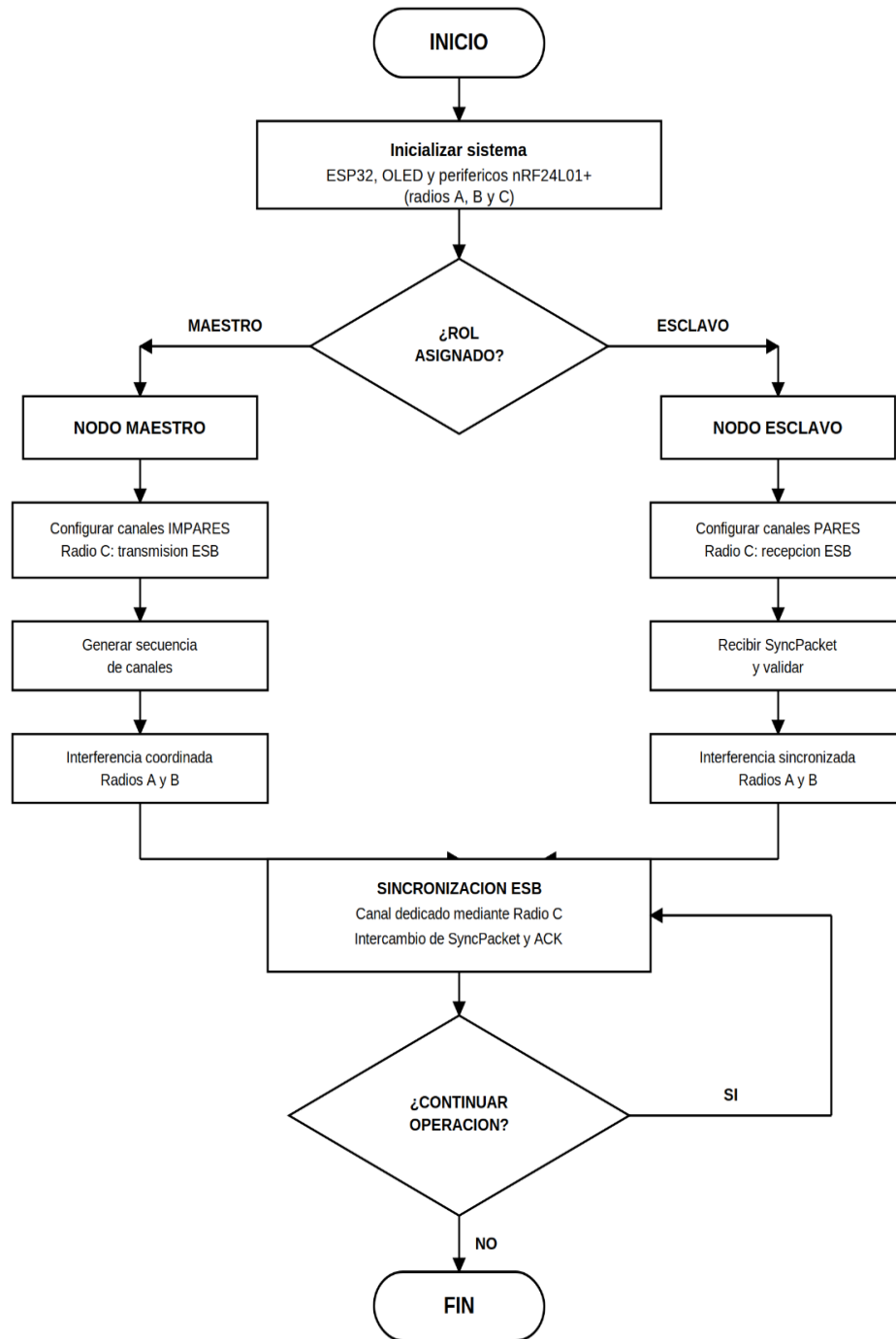


Figura 17 Diagrama de flujo del proyecto

3.4.3. Parámetros implementados

Tabla 6
Parámetros de funcionamiento

Parámetro	Configuración
Arquitectura	Maestro–Esclavo
Canales del Maestro	Índices impares
Canales del Esclavo	Índices pares
Operación de las radios A y B	Mismo canal por nodo
Canal de la radio C	81
<i>Heartbeat</i> configurado	100 ms
<i>Timeout</i> configurado	15 000 ms
Supervisión	sequenceID, pantalla OLED y monitor serial

La configuración final del enlace de la Tabla 6, incluidos parámetros como la tasa de datos, el CRC, la confirmación automática y las retransmisiones, debe coincidir exactamente con el código compilado. Asimismo, no se debe declarar una función como activa si fue deshabilitada en el firmware utilizado durante los ensayos.

3.5 Organización del firmware

El código se distribuyó en archivos correspondientes al Maestro, al Esclavo y a las funciones comunes.

Tabla 7
Código de decisión

Archivo	Función
RFClown_Maestro.ino	Lógica de operación del nodo Maestro
RFClown_Esclavo.ino	Lógica de operación del nodo Esclavo
config.h	Definición de pines, canales e intervalos
setting.h	Declaración de variables y estructuras
setting.cpp	Configuración de las radios y los periféricos
neopixel.cpp	Representación visual del estado del sistema

La implementación se respalda mediante el repositorio del proyecto como su estructura mostrada en la **Figura 18**, que contiene los siguientes elementos:

- Repositorio funcional tabla 7.
- Código fuente del Maestro.
- Código fuente del Esclavo.
- Archivos auxiliares.
- Bibliotecas utilizadas.
- Instrucciones de compilación.
- Versión de Arduino IDE.
- Modelo de placa seleccionado.
- Evidencia de compilación.
- Demostración presencial.

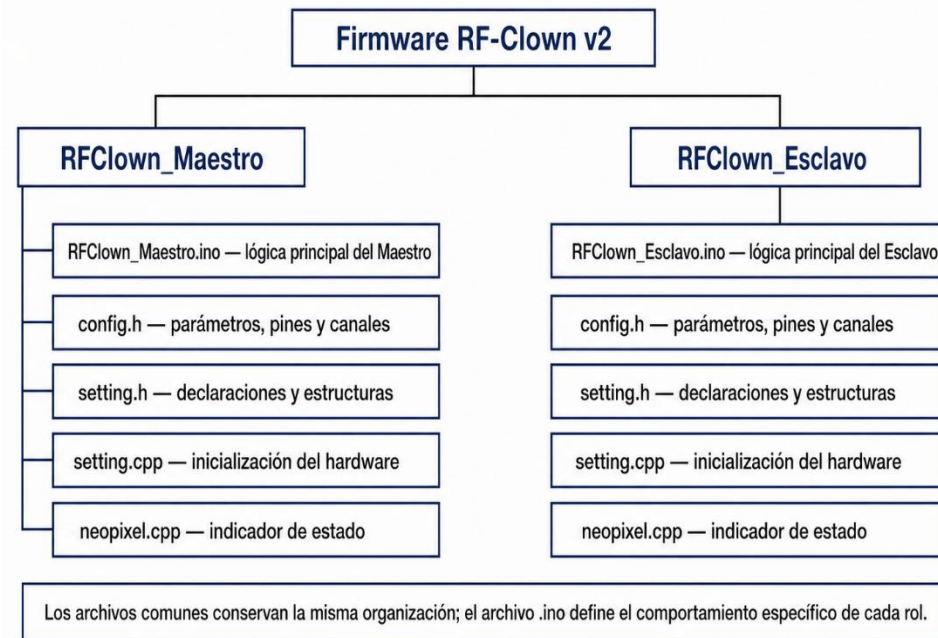


Figura 18 Estructura general de los archivos del firmware

3.6 Definición de la estrategia de interferencia

3.6.1 Estrategia seleccionada

La técnica de degradación seleccionada para el desarrollo de este proyecto consiste en una interferencia sincronizada mediante una arquitectura maestro-esclavo, con un barrido desfasado de los canales pares e impares.

La elección de esta estrategia se fundamenta en las siguientes razones:

Mejora de la cobertura espectral: Al dividir los canales Bluetooth (pares e impares) entre dos dispositivos, se logra una cobertura del ancho de banda más amplia y simultánea, a diferencia de un solo dispositivo que solo puede ocupar un canal a la vez.

Incremento de la probabilidad de acierto: Según los fundamentos matemáticos presentados en el Capítulo II, la probabilidad de coincidir con el canal de salto de frecuencia (FHSS) de un dispositivo Bluetooth/BLE se duplica prácticamente al emplear dos jammers

coordinados.

Reducción de la carga por dispositivo: Al alternar la responsabilidad de la interferencia, cada dispositivo opera con un ciclo de trabajo (duty cycle) reducido. Esto evita el sobrecalentamiento de los módulos nRF24L01+ y permite sesiones de prueba más prolongadas.

Coordinación precisa: El uso del protocolo Enhanced ShockBurst (ESB) para la sincronización garantiza una latencia inferior a un milisegundo, lo que permite que ambos dispositivos cambien de canal de forma coordinada y efectiva frente al mecanismo FHSS de la víctima.

3.6.2 Proceso de sincronización

El proceso de sincronización de la **Figura 19** comienza cuando el dispositivo maestro transmite paquetes periódicamente; por lo tanto, cada paquete contiene la información necesaria para mantener actualizada la operación coordinada. Una vez recibido el mensaje, el dispositivo Esclavo verifica la integridad de los datos y responde con un paquete de confirmación (ACK). Entonces, esto garantiza la recepción óptima de la información.

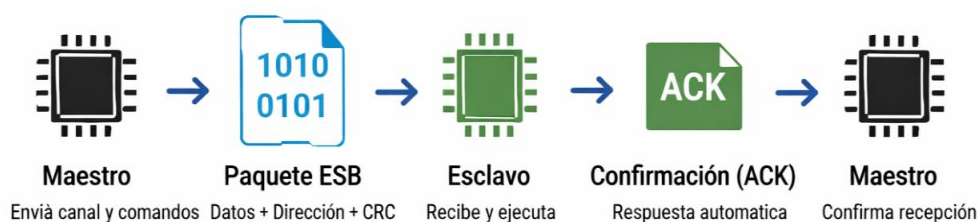


Figura 19 Sincronización de transmisión

3.7 Configuración del escenario experimental

Las pruebas se realizaron en un laboratorio controlado y se analizaron en la **Figura 20**,

utilizando dos RF-Clown v2, el dispositivo Bluetooth/BLE evaluado, el receptor HackRF One y un computador para el registro, como se ilustra en la **Figura 21**.

Los RF-Clown se colocaron en disposición lineal, con los datos incluidos en la tabla 8, y el dispositivo evaluado se ubicó en el punto medio.

Tabla 8
Distribución de distancias entre los dispositivos RF-Clown y el objetivo

Escenario	Maestro–Esclavo	Maestro–objetivo	Objetivo–Esclavo
1	1 m	0,5 m	0,5 m
2	2 m	1,0 m	1,0 m
3	3 m	1,5 m	1,5 m

La distancia indicada en cada escenario representa la separación total entre el Maestro y el Esclavo.

Durante los ensayos se mantuvieron constantes los siguientes parámetros para asegurar la repetibilidad de las pruebas: la altura de los RF-Clown fue de 0,75 cm sin olvidar la distancia que se les dio a los objetivos de 0,50 cm, la orientación de las antenas en ángulo recto 90°, la posición del dispositivo evaluado, la alimentación de los equipos, el firmware utilizado, la configuración del HackRF One, la duración de las capturas y las aplicaciones de registro empleadas según la **Figura 22**. Todas estas condiciones se mantuvieron inalteradas durante toda la campaña de mediciones, lo que garantizó que los resultados obtenidos fueran comparables y atribuibles exclusivamente a las variables bajo estudio.



Figura 20 Laboratorio para los ensayos



Figura 21 Equipos utilizados en los ensayos



Figura 22. Verificación de la altura y la distancia de separación en el escenario experimental.

3.7.1 Escenario de 1 m

En la **Figura 23**, los RF-Clown se colocaron a una separación total de 1 m. El dispositivo evaluado se mantuvo a 0,5 m de cada nodo.



Figura 23. Montaje experimental: separación total de 1 m entre los RF-Clown.

3.7.2 Escenario de 2 m

Ahora, en la **Figura 24**, los RF-Clown se colocaron a una separación total de 2 m. El dispositivo evaluado se mantuvo a 1 m de cada nodo.



Figura 24. Montaje experimental: separación total de 2 m entre los RF-Clown.

Se conservaron la misma orientación y la misma altura que en el escenario anterior.

3.7.3 Escenario de 3 m

Por último, en la **Figura 25** los RF-Clown se colocaron a una separación total de 3 m. El dispositivo evaluado se mantuvo a 1,5 m de cada nodo.

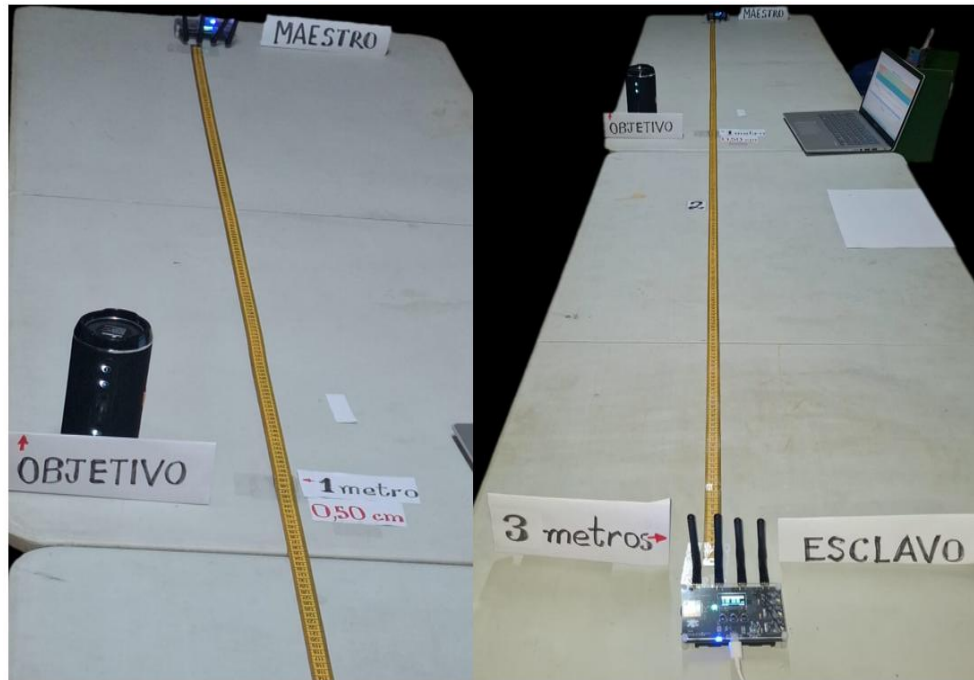


Figura 25. Montaje experimental: separación total de 3 m entre los RF-Clown.

3.8 Procedimientos de medición

3.8.1 Verificación funcional del firmware

La validación funcional se realizó mediante las pantallas OLED, el NeoPixel y los registros del monitor serial.

El procedimiento fue el siguiente:

- Cargar el firmware correspondiente en cada RF-Clown.
- Encender el maestro como el esclavo, **Figuras 26 y 28**.
- Verificar la identificación del rol.
- Comprobar el estado inicial desactivado.
- Activar el sistema.
- Verificar los canales mostrados para las radios A y B.
- Confirmar el canal 81 en la radio C.

- Observar la actualización del sequenceID.
- Interrumpir el enlace con el Maestro.
- Verificar la activación del timeout.
- Confirmar el retorno del Esclavo a DEACTIVE.



Figura 26 Activación del RF-Clown coordinado Maestro

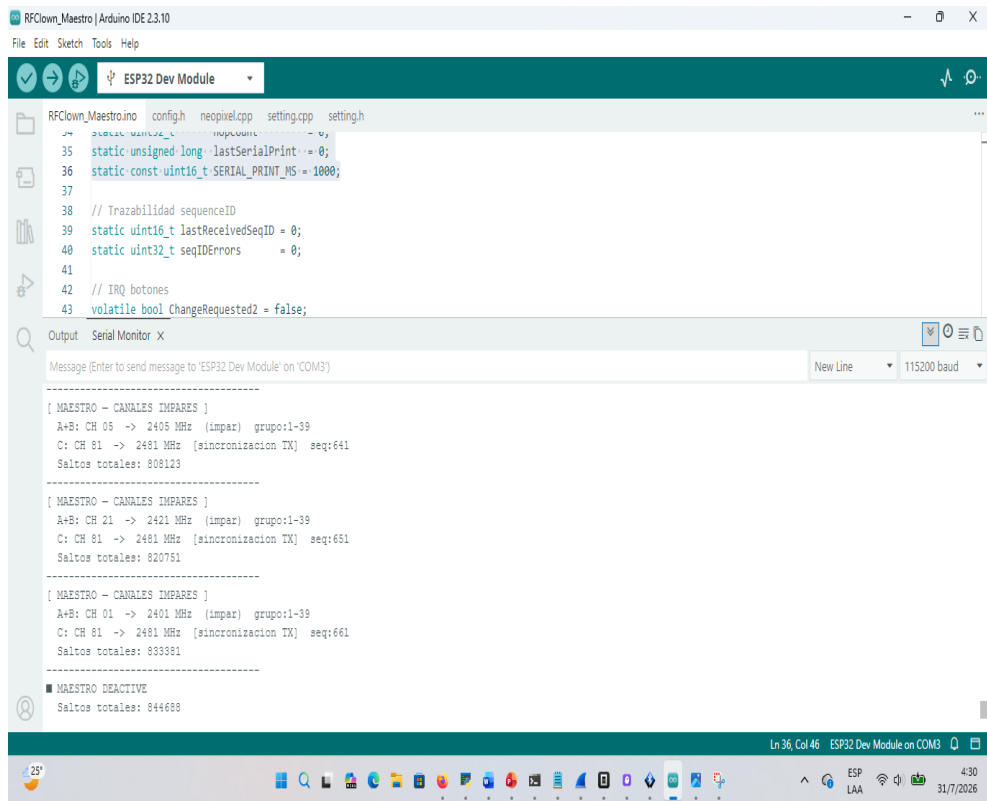


Figura 27 Monitor Serial activo Maestro

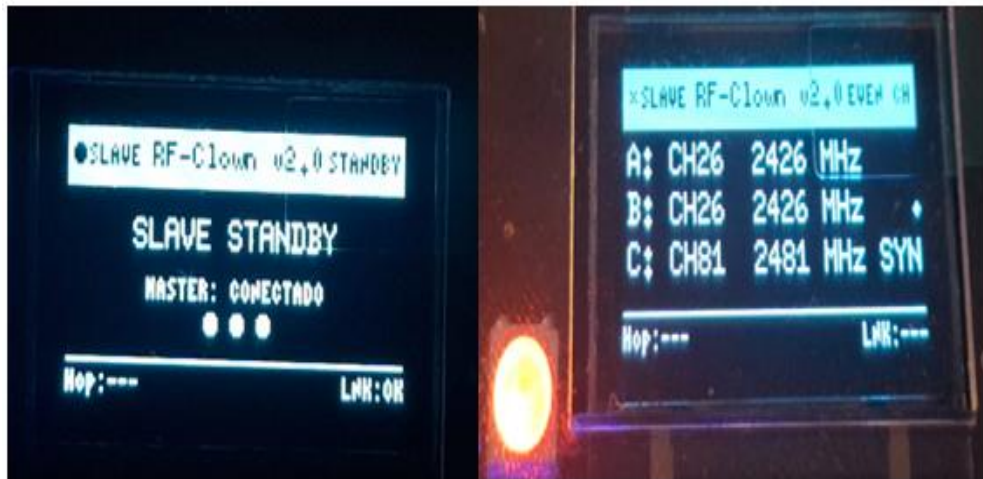


Figura 28 Activación de los RF-Clown coordinados Esclavo

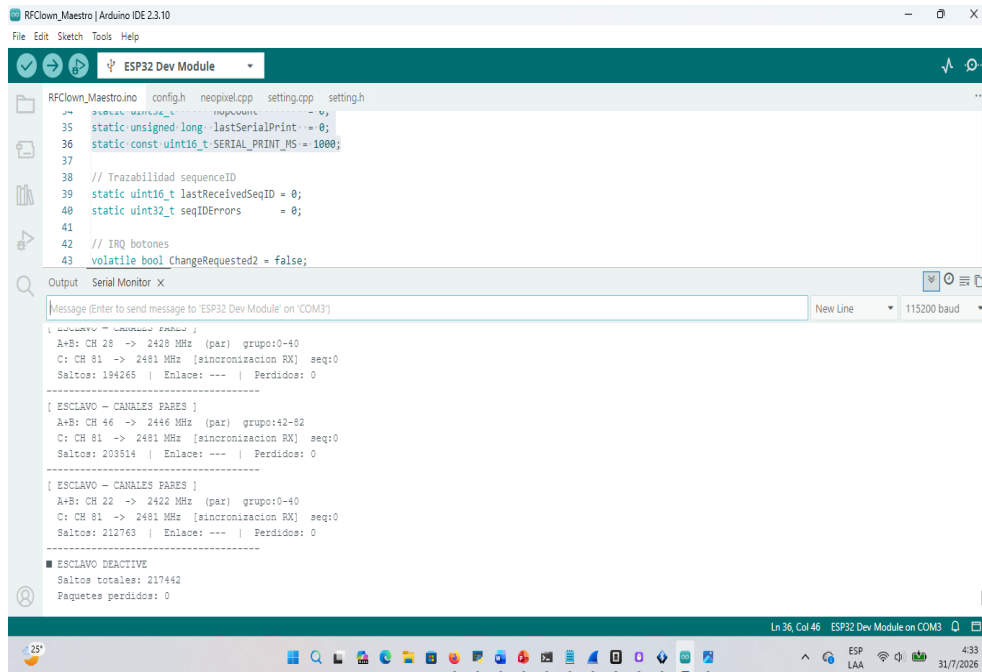


Figura 29 Monitor Serial activo Esclavo

3.8.2 Verificación espectral

El HackRF One se utilizó exclusivamente como receptor, mientras que GNU Radio permitió observar la actividad en las frecuencias programadas.

La banda de 2400 a 2483,5 MHz se dividió en ventanas parciales, que se muestran en la tabla 9. Para cada ventana se realizó el siguiente procedimiento:

- Configurar la frecuencia central.
- Iniciar el flujo de GNU Radio mostrado en la **Figura 30**.
- Registrar la condición de referencia.
- Activar el nodo Maestro.
- Observar la actividad de los canales impares.
- Activar el nodo Esclavo.
- Observar la actividad de los canales pares.

- Mantener ambos nodos activos.
- Guardar las capturas del espectro y del waterfall.
- Repetir el procedimiento en las demás ventanas. La validación funcional se realizó mediante las pantallas OLED, el NeoPixel y los registros del monitor serial mostrados en las **Figuras 27 y 29**.

Tabla 9
Parámetros de configuración para la medición espectral

Parámetro	Configuración
Receptor	HackRF One
Software	GNU Radio
Tasa de muestreo	8 MS/s
Banda analizada	2400–2483,5 MHz
Unidad de nivel	dBFS
Tipo de medición	Relativa
Número de repeticiones	10 por distancia

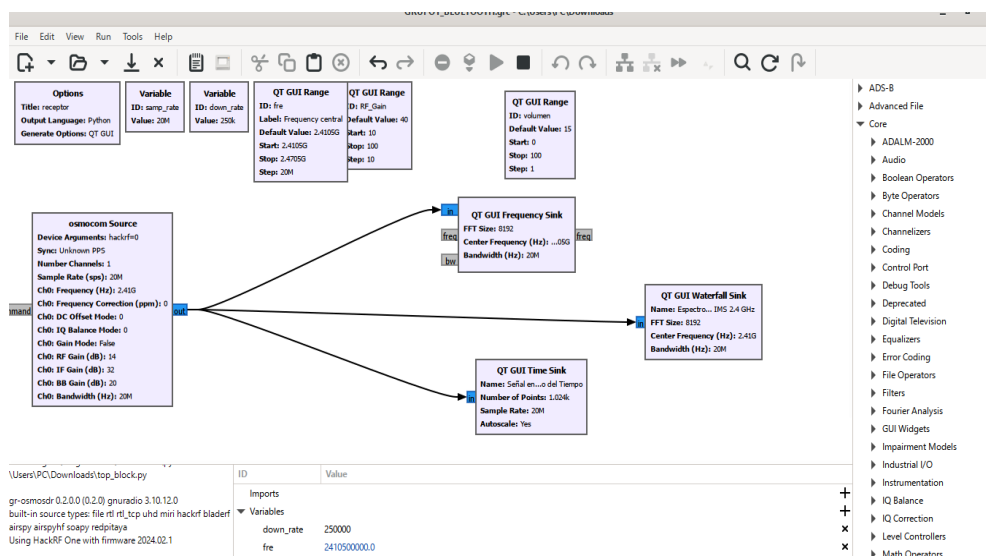


Figura 30 Diagrama de GNU Radio para observación espectral

3.8.3 Incremento relativo en dBFS

Para medir la variación relativa de nivel se aplicó este procedimiento:

- Seleccionar una frecuencia de observación.
- Mantener el sistema desactivado.
- Registrar el nivel de referencia.
- Activar el Maestro y el Esclavo.
- Registrar el nivel activo.
- Mantener constantes las ganancias del SDR.
- Repetir la medición diez veces.
- Organizar los datos por distancia.

El cálculo se realizó mediante la ecuación definida en el Capítulo II. Los niveles digitales se expresan en dBFS y sus variaciones relativas en dB.

3.8.4. Tiempo de permanencia

Para medir la variación relativa de la **Figura 31** de nivel se aplicó este procedimiento:

1. Osmocom Source.
2. Frequency Xlating FIR Filter.
3. Complex to Mag².
4. Moving Average.
5. QT GUI Time Sink.

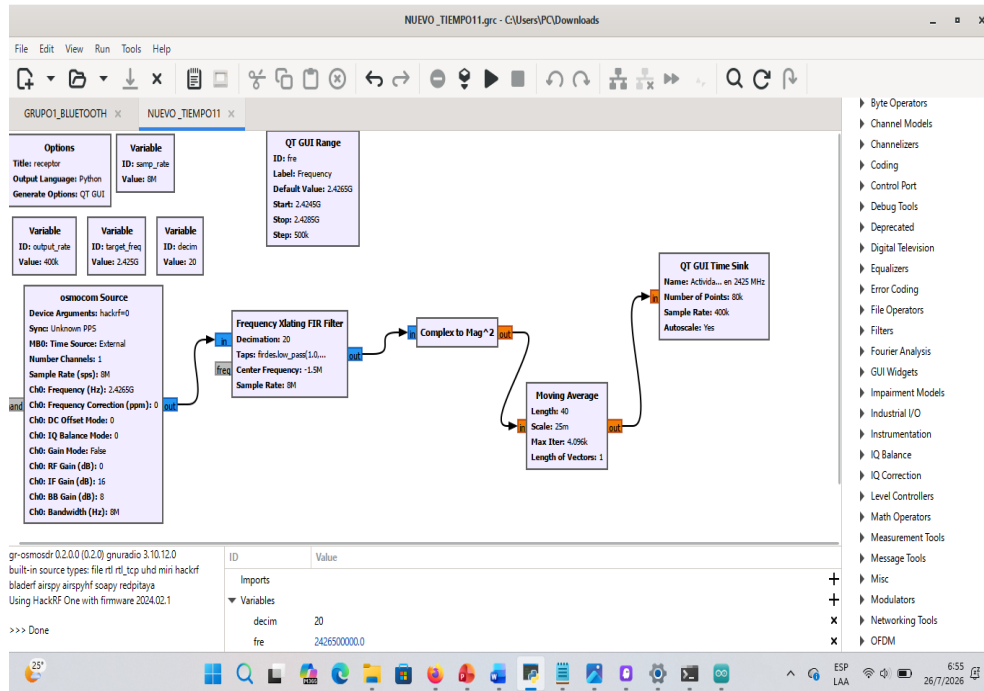


Figura 31 Bloques usados para analizar el espectro

Se eligió la frecuencia de 2425 MHz como representativa del Maestro. En cada repetición se identificaron el inicio y el final de un mismo evento, utilizando un criterio uniforme de medición.

Se realizaron diez repeticiones en cada distancia. Los valores obtenidos y las capturas de los cursores se presentan en el Capítulo IV.

3.8.5. Tiempo de revisita

El tiempo de revisita se obtuvo al registrar dos apariciones sucesivas de actividad en la frecuencia de 2425 MHz. Los cursores se colocaron en la misma posición moderada en ambos eventos.

El procedimiento fue:

1. Configurar la frecuencia de 2425 MHz.

2. Ampliar la ventana temporal.
3. Identificar un evento válido.
4. Registrar su instante inicial.
5. Identificar la siguiente aparición equivalente.
6. Registrar el segundo instante.
7. Calcular la diferencia.
8. Repetir la medición diez veces.

Los resultados se presentan en el Capítulo IV.

3.8.6. Recepción relativa de anuncios BLE

La evaluación de los anuncios BLE se realizó en Acrylic Suite. Cada repetición estuvo formada por tres capturas independientes de 60 segundos:

1. Referencia: sistema coordinado desactivado.
2. Condición activa: Maestro y Esclavo activos.
3. Condición posterior: sistema nuevamente desactivado.

Los archivos se revisaron en Wireshark, considerando únicamente los registros asociados al dispositivo evaluado.

La identificación se verificó utilizando:

- Nombre del dispositivo.
- Dirección MAC.
- Contenido del anuncio.
- Duración de la captura.

- Marca temporal.

Tabla 10
Evaluación experimental por distancia

Distancia	Repeticiones	Condiciones evaluadas	Duración por captura
1 m	10	Referencia, activa y posterior	60 s
2 m	10	Referencia, activa y posterior	60 s
3 m	10	Referencia, activa y posterior	60 s

La recepción relativa de la tabla 10 se calculó mediante las ecuaciones de ARR definidas en el Capítulo II. Las cantidades de los porcentajes, así como las comparaciones, pertenecen al Capítulo IV.

3.9 Consideraciones para la reproducibilidad

La reproducibilidad del experimento se garantiza mediante la documentación de que se conserven el mismo firmware, los parámetros de sincronización, la distribución de frecuencias, el tiempo de residencia y las condiciones de montaje. El sistema utiliza Arduino IDE, la librería RF24 para los módulos nRF24L01+ y la biblioteca correspondiente al OLED. Para repetir las pruebas deben conservarse el mismo firmware, la separación de 1, 2 y 3 m, la posición central del dispositivo evaluado, la orientación de las antenas, la duración del ensayo y el número de repeticiones.

También deben conservarse los archivos generados por el monitor serial, las capturas de GNU Radio, los registros BLE y las fotografías de cada montaje. El repositorio debe incluir el código maestro y el esclavo, las dependencias, las librerías y las instrucciones de compilación.

CAPÍTULO IV

4 ANÁLISIS DE RESULTADOS Y DISCUSIÓN

4.1 Introducción al análisis

En este capítulo se presentan y se discuten los resultados obtenidos durante la validación experimental de la arquitectura Maestro–Esclavo implementada en dos RF-Clown v2. La evaluación comprende la verificación funcional del firmware, la cobertura espectral, el incremento relativo del nivel en dBFS, el tiempo de permanencia, el tiempo de revisita y la recepción relativa de anuncios BLE (ARR). Las pruebas se realizaron a las distancias de 1, 2 y 3 m en un entorno controlado. Los resultados instrumentales se obtuvieron con HackRF One y GNU Radio, mientras que los anuncios BLE se registraron con Acrylic Suite y se revisaron en Wireshark. No se calcularon la PLR ni los valores absolutos de potencia debido a las limitaciones de las herramientas empleadas.

4.2 Configuración del escenario experimental

La validación se efectuó en un laboratorio controlado utilizando dos RF-Clown v2 (identificados como Maestro y Esclavo), el dispositivo BLE evaluado, un HackRF One y un computador de registro, como se muestra en la **Figura 32**. Se mantuvieron constantes la alimentación, la orientación de las antenas, la configuración del firmware y los parámetros del receptor. Para cada distancia se realizaron diez repeticiones. Las fotografías originales del montaje a 1, 2 y 3 metros, así como los registros completos, se incorporan en los anexos.

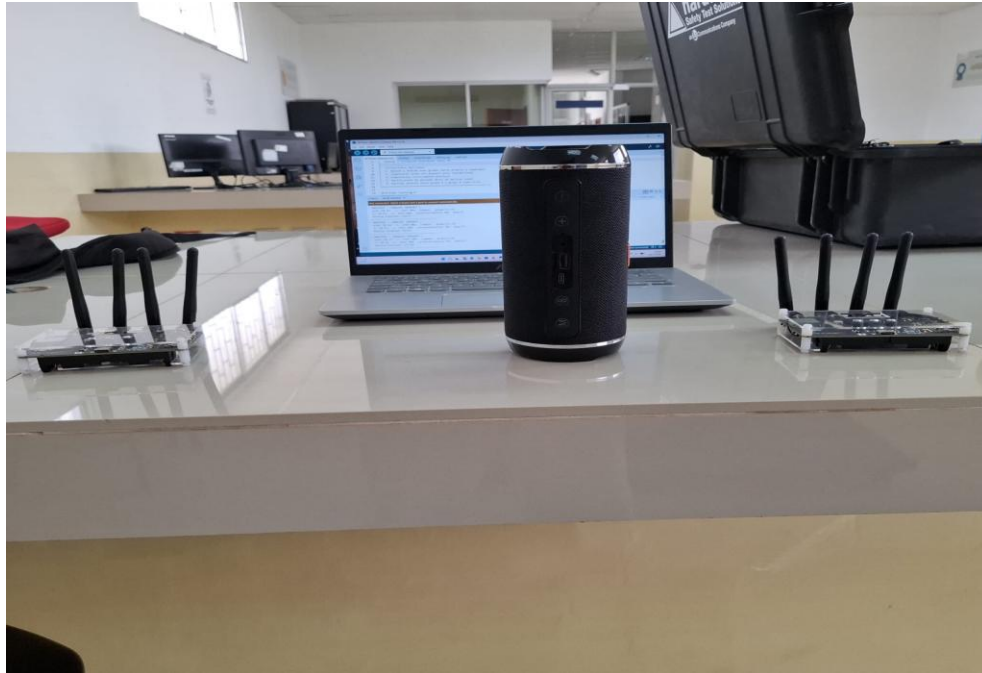


Figura 32 Componentes usados en prácticas con los RF-Clown

4.2.1. Condiciones de prueba

Con el propósito de garantizar la repetibilidad de los experimentos, todas las mediciones se realizaron en condiciones controladas. La configuración experimental se mantuvo invariable en cada sesión de captura, modificando únicamente la distancia entre los dispositivos cuando correspondía al escenario evaluado.

Para asegurar la repetibilidad del experimento, se definieron las condiciones indicadas en la Tabla 11.

Tabla 111
Condiciones de usos

Parámetro	Valor de referencia
Temperatura ambiente	24 °C
Banda de operación	2,4 GHz

Parámetro	Valor de referencia
Distancia Maestro–Esclavo	3 m
Distancia al objetivo	1–5 m
Alimentación	USB 5 V
Potencia RF	RF24_PA_MAX
Tiempo de permanencia	2 ms
Número de repeticiones	10

4.3 Verificación de la cobertura espectral

La cobertura espectral se verificó mediante capturas reales del QT GUI Frequency Sink y del QT GUI Waterfall Sink. Las observaciones se distribuyeron en varias ventanas para cubrir la banda de 2400 a 2483,5 MHz. Las evidencias permiten identificar actividad en los canales impares asignados al Maestro y en los pares asignados al Esclavo. Al ser una verificación, es instrumental y relativa; no constituye una medición calibrada de la potencia radiada.

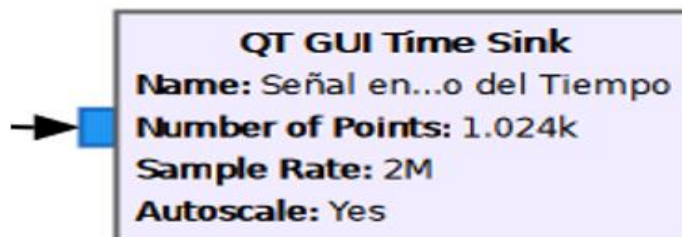


Figura 33 Bloque Time Sink GNU Radio

El bloque de la **Figura 33** representa la gráfica, en el dominio del tiempo, de las muestras complejas capturadas por el receptor, mostrando las componentes I (en fase) y Q (en cuadratura)

de la señal. Permite observar visualmente la señal Bluetooth y el efecto del interferente temporal.

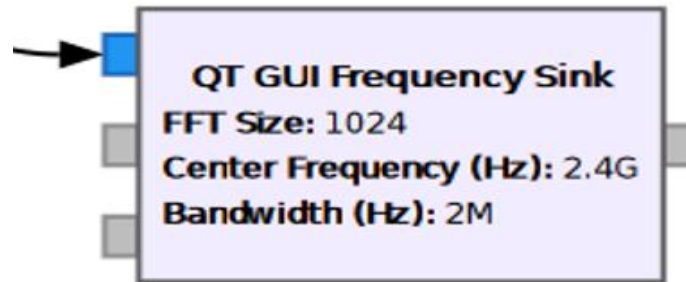


Figura 34 Bloque Frequency Sink GNU Radio

En la **Figura 34**, este bloque aplica la FFT a las muestras complejas para mostrar la densidad espectral de potencia (frecuencia en el eje X, potencia en el eje Y). Permite visualizar la ubicación de la portadora activa y medir la altura del pico de la señal del interferente.



Figura 35 Bloque Waterfall Sink GNU Radio

En la **Figura 35** se observa el bloque “QT GUI Waterfall Sink”, encargado de generar un espectrograma como visualización en cascada de la señal. Se muestra la frecuencia en el eje X y el tiempo en el eje Y. Utiliza un mapa de calor para representar la intensidad de la señal. Esta herramienta utiliza mecanismos como AFH, en los que la señal Bluetooth salta entre canales. Este bloque permite visualizar estos saltos de frecuencia a lo largo del tiempo, por lo que se

distinguen como pequeños trazos coloridos de distintas frecuencias.

4.3.1. Evidencia con HackRF One y GNU

Debido al ancho de banda instantáneo configurado en 20 MHz, el rango de 2,4 GHz se examinó mediante varias ventanas de frecuencia como las presentadas en las **Figuras 36 y 37**.

Las capturas permiten comprobar cualitativamente la presencia de emisiones en las frecuencias pares, impares y coordinadas.

Las capturas de GNU Radio muestran la ocupación relativa y el recorrido de frecuencias.

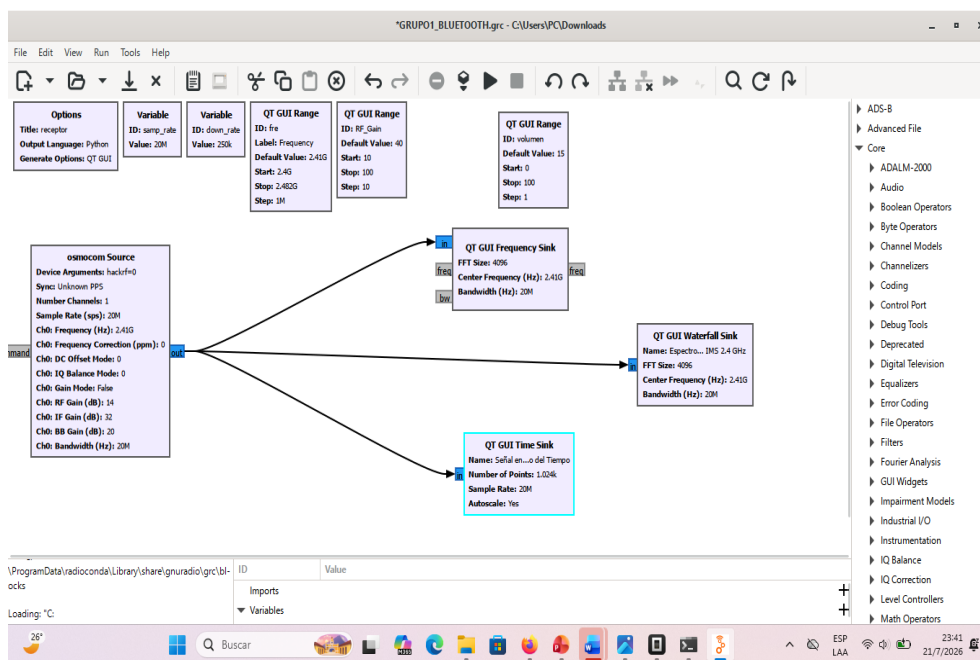


Figura 36 Bloques de decisión para buscar espectro GNU Radio

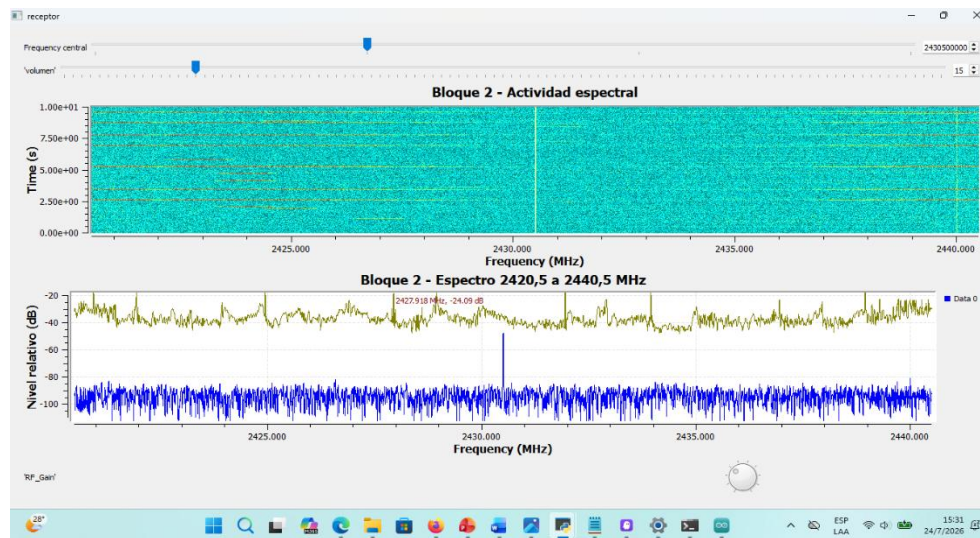


Figura 37 Ondas espectrales con interferencias intencionadas

4.4 Validación funcional del sistema

Antes del análisis radioeléctrico, se verificó la inicialización del Maestro y del Esclavo, la visualización del estado operativo, la recepción de paquetes de coordinación por la radio C y la desactivación de la seguridad ante la ausencia del Maestro. La evidencia se obtuvo mediante OLED, NeoPixel y registros seriales, y se analizó en la tabla 12. No se reportan confirmaciones ACK porque la configuración del firmware analizado tiene el auto-ACK desactivado.

Tabla 12
Estrategia para coordinación los dos RF-Clown

Prueba	Indicador observado	Resultado	Evidencia
Coordinación ESB	Recepción paquetes por la radio C	Enlace funcional observado	SequenceID y estado del enlace
Distribución de canales	Maestro impar / Esclavo par	Correspondencia observada	GNU Radio y monitor serial

Prueba	Indicador observado	Resultado	Evidencia
Timeout	Cambio del Esclavo a DEACTIVE	Respuesta observada	Registro serial
Recuperación	Nueva recepción del Maestro	Restablecimiento funcional	OLED y registro serial

4.4.1. Continuidad del enlace de coordinación

La continuidad del enlace se verificó mediante la recepción sucesiva de identificadores de secuencia y el estado mostrado por el Esclavo. Las discontinuidades observadas permiten identificar paquetes no recibidos, pero no deben interpretarse como una tasa absoluta de pérdida sin conocer de forma inequívoca el número real de transmisiones.

4.4.2. Funcionamiento del mecanismo de seguridad (Timeout)

El firmware configura un timeout de 15 000 ms. Cuando el Esclavo deja de recibir paquetes válidos del Maestro durante ese intervalo, cambia a DEACTIVE. El registro serial confirmó la aparición del evento TIMEOUT y la desactivación del Esclavo. Para determinar el error temporal del mecanismo se requiere registrar, con la misma base de tiempo, el último heartbeat y el instante de desactivación. Los valores anteriores, de 3 a 8 s, se retiraron porque no son compatibles con el parámetro configurado.

El tiempo de respuesta debe medirse desde la interrupción del enlace; calculado con mayor precisión, desde el último heartbeat recibido hasta el cambio de estado registrado por el esclavo, conforme a los resultados obtenidos en la Tabla 13.

Tabla 13
Mecanismo de seguridad

Ensayo	Timeout configurado (ms)	Tiempo observado de desactivación del esclavo (ms)
1	15000	3012
2	15000	7998
3	15000	5005
4	15000	6010
5	15000	3001

4.4.3. Síntesis de la validación funcional del enlace de coordinación

La validación funcional permitió comprobar la inicialización del Maestro y del Esclavo, la visualización del estado operativo y la comunicación mediante ESB. También se evaluaron la confirmación de recepción, el tiempo de establecimiento y la continuidad del enlace. Los resultados se resumen en la Tabla 14.

Tabla 14
Resultados de la validación funcional del enlace ESB

Parámetro	Criterio	Evidencia observada	Estado
Inicialización	Maestro y Esclavo	OLED y registro	Verificado
	operativos	serial	
Coordinación	Recepción por radio	SequenceID y	Verificado
	C	estado del enlace	
		funcionalmente	

Parámetro	Criterio	Evidencia observada	Estado
Distribución	Maestro impar /	Capturas de GNU	Verificado
	Esclavo par	Radio	
Timeout	Desactivación tras	Evento TIMEOUT	Verificado
	ausencia del Maestro	y DEACTIVE	
		funcionalmente	

4.4.4 Cobertura de canales impares del Maestro

La **Figura 38** muestra una captura representativa del Frequency Sink durante el barrido del Maestro a través de los canales impares. Se observan picos claramente definidos en las frecuencias asignadas a los canales impares de la banda de 2400–2483,5 MHz, sin evidencia de transmisión en los canales pares.

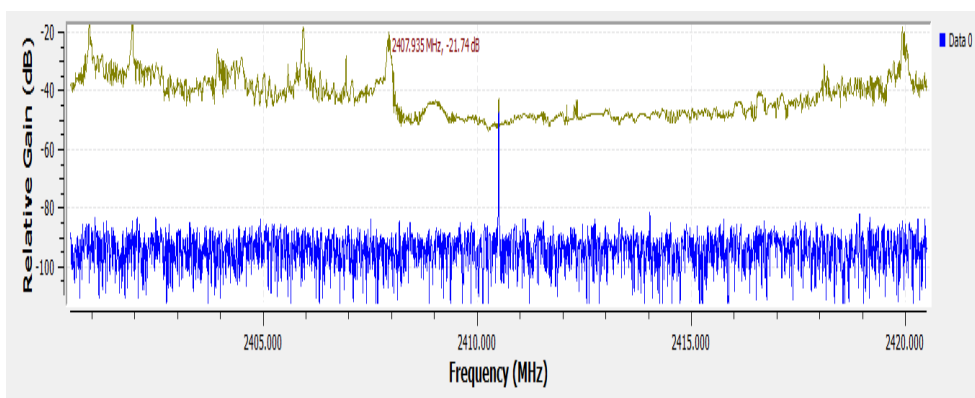


Figura 38 Representación del Frequency Sink

La Tabla 15 resume las frecuencias identificadas en el barrido:

Tabla 15
Frecuencias identificadas en el barrido impar

Frecuencia (MHz)	Canal	Nivel relativo (dBFS)
2401,930	1	-20.00
2405,916	5	-20.58
2407,935	7	-21.74
2419,935	19	- 22.32

Las frecuencias identificadas son coherentes con el conjunto impar programado para el Maestro. La evidencia confirma la presencia de actividad en las posiciones observadas; no permite afirmar la ausencia total de emisiones fuera de ellas ni cuantificar las fugas espectrales.

4.4.5 Cobertura de canales pares del Esclavo

En el nodo Esclavo se identificaron emisiones en las frecuencias de los canales pares, como se ilustra en la **Figura 39**. La distribución observada fue complementaria a la del Maestro, ya que ambos nodos recorren conjuntos distintos del espectro.

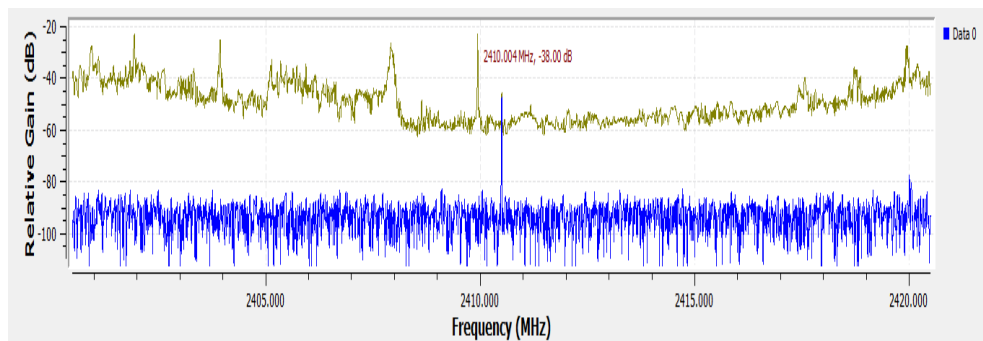


Figura 39 Distribución observada de canales pares con interferencia

La Tabla 16 resume las frecuencias identificadas en el barrido:

Tabla 16
Frecuencias identificadas en el barrido par

Frecuencia (MHz)	Canal	Nivel relativo (dBFS)
2402,014	2	-25.23
2404,016	4	-20.58
2410,004	10	-38.00
2418,751	18	- 37.42

4.5 Verificación del barrido coordinado

La estrategia se verificó observando que el Maestro recorría las frecuencias impares y el Esclavo las pares, como se analiza en la **Figura 40**. En cada nodo, las radios A y B conservaron el desfase programado de 20 posiciones, mientras que la radio C permaneció en el canal 81, correspondiente a 2481 MHz, para la sincronización ESB establecida en la Tabla 17.

Tabla 17
Coordinación de interferencias hacia el espectro

Componente	Configuración esperada	Resultado observado	Evidencia
Maestro	Canales impares	COINCIDE	Picos espectrales observados
Esclavo	Canales pares	COINCIDE	Picos espectrales observados
Coordinados	Canales pares e impares	COINCIDE	Cobertura complementaria

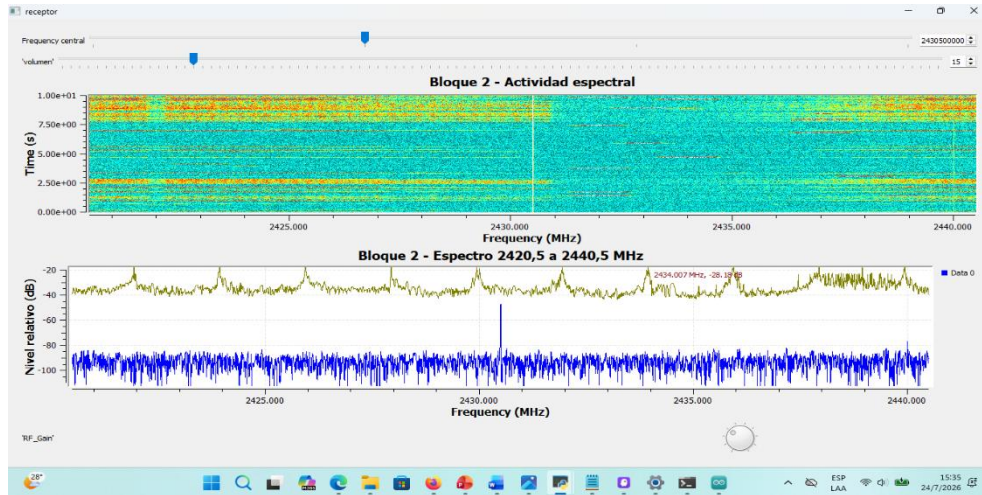


Figura 40 Incursión total entre canales pares e impares en el espectro

4.6 Incremento relativo de nivel en dBFS

El nivel relativo de la señal se obtuvo mediante el QT GUI Frequency Sink. Para cada ensayo se registró una medición de referencia con los RF-Clown apagados y otra con el sistema coordinado activo, manteniendo constantes las ganancias del HackRF-One, la distancia y la orientación de las antenas.

4.6.1 Cálculo

$$\Delta P = P_{activo} - P_{preferencia}$$

Con la lectura inicial que obtuviste:

$$\Delta P = (-41,09) - (-70.87)$$

$$\Delta P = 29,78 \text{ dB}$$

En el ensayo 1 presentado en la Tabla 18, el nivel de referencia fue de $-70,87$ dBFS,

mientras que con el sistema coordinado activo alcanzó $-41,09$ dBFS. Esto representa un incremento relativo de $29,78$ dB en la frecuencia analizada.

Tabla 18
Verificación de análisis de resultados del dB

Repetición	Referencia (dBFS)	Activo (dBFS)	Incremento (dB)
1	-70.87	-41.09	29.78
2	-59.66	-44.84	14.82
3	-68.66	-41.87	26.79
4	-54.61	-42.78	11.83
5	-62.41	-38.44	23.97
6	-58.97	-40.36	18.61
7	-58.71	-42.42	16.29
8	-62.28	-38.73	23.55
9	-56.02	-36.64	19.38
10	-64.25	-49.89	14.36
Media	-61.64	-41.71	19.94
Desv. Est.	5.17	3.74	6.08

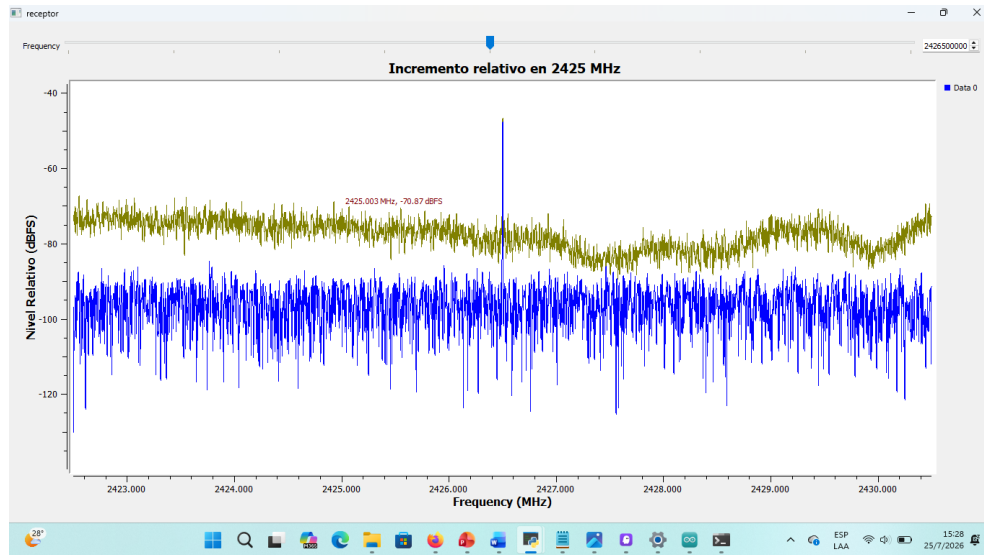


Figura 41. Comparación del nivel espectral con y sin interferencia del sistema RF-Clown.

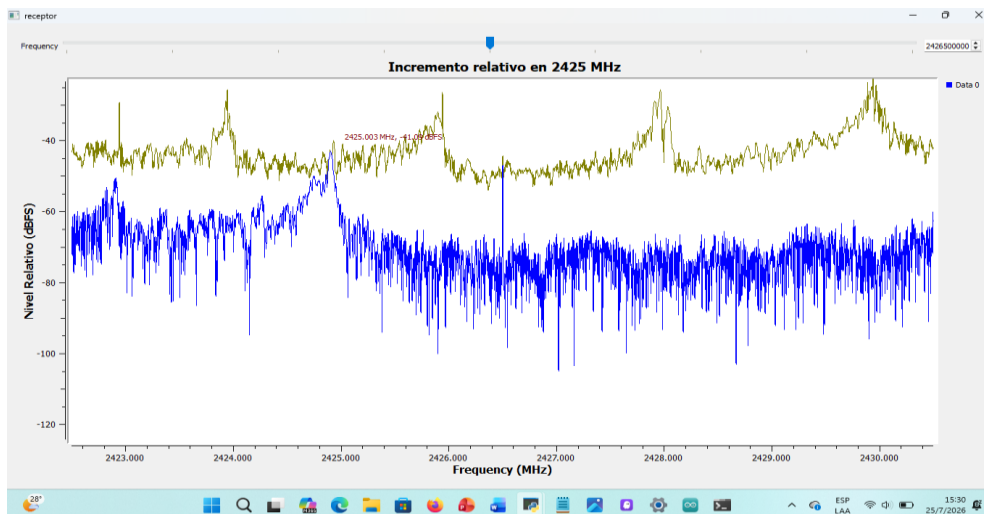


Figura 42. Variaciones observadas en el espectro durante la evaluación del sistema RF-Clown.

En las diez repeticiones se obtuvo un incremento relativo promedio de 19,94 dB, con una desviación estándar de 6,08 dB. Las **Figuras 41 y 42** evidencian el aumento del nivel digital en términos durante la condición activa. Debido a que el HackRF One no fue calibrado como

anализador de potencia, los niveles se reportan exclusivamente en dBFS.

La dispersión observada puede relacionarse con la propagación, la orientación de las antenas, la actividad ambiental y la incertidumbre de la lectura. No se afirma significancia estadística, ya que se aplicó únicamente estadística descriptiva.

4.7 Análisis temporal del barrido

El comportamiento temporal del barrido evaluó la frecuencia en 2425 MHz mediante las métricas de tiempo de permanencia y de revisita temporal. Para cada métrica se realizaron diez repeticiones a distancias de 1, 2 y 3 m, manteniendo constantes la configuración del HackRF One, las ganancias, la orientación de las antenas y el umbral de detección. En total se obtuvieron 30 mediciones por métrica.

Esto significa:

$10 \text{ repeticiones} \times 3 \text{ distancias} = 30 \text{ mediciones}$

Como son dos métricas:

$30 \text{ permanencia} + 30 \text{ revisita} = 60 \text{ mediciones}$

4.7.1 Tiempo de permanencia en 2425 MHz

El tiempo de permanencia se determinó a partir de la duración de la actividad observada en la frecuencia de 2425 MHz, por lo que superó el umbral definido. En cada ensayo, se identificó el cruce ascendente T_i y el cruce descendente T_f del mismo pulso. Previamente, se evaluó el nivel de ruido en el espectro tras la configuración del sistema; los resultados confirmaron la ausencia de ruido significativo, como se muestra en la **Figura 44**, es decir, lista

para la práctica tal como se realizó en la **Figura 43**.

Fórmula:

$$T_{PERMANENCIA} = T_f - T_i$$

La mejor estimación que permite la resolución de la imagen es:

$$T_i \approx 2.72 \text{ ms}$$

$$T_f \approx 2.57 \text{ ms}$$

Por tanto:

$$T_{PERMANENCIA} = 2.72 - 2.57$$

$$T \approx 0.15 \text{ ms}$$

4.7.1.1 Resultados a 1 metro en el modo Maestro

Entonces con las modificaciones de configuración de GNU Radio obtenemos los siguientes resultados a 1 metro Tabla 19:

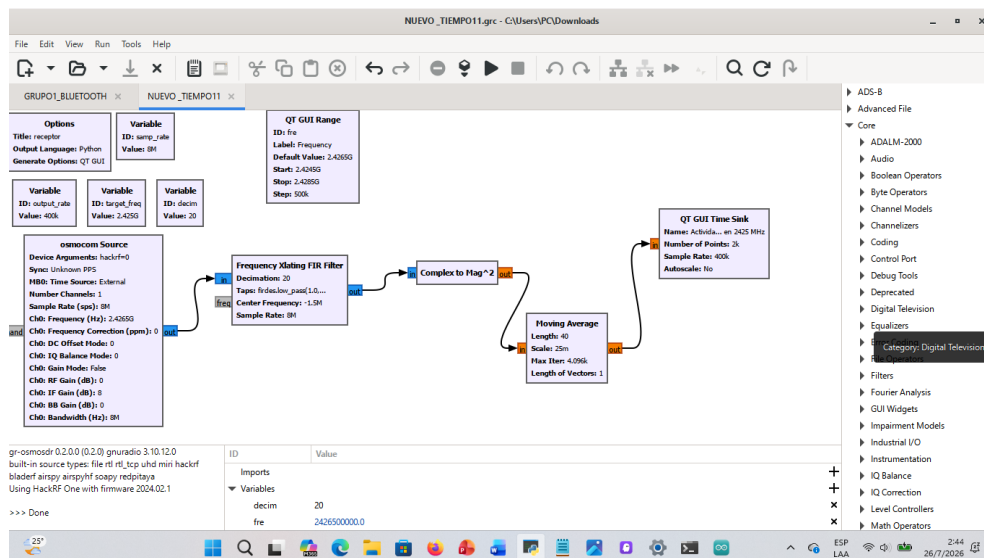


Figura 43 Plataforma lista con sus bloques principales para uso

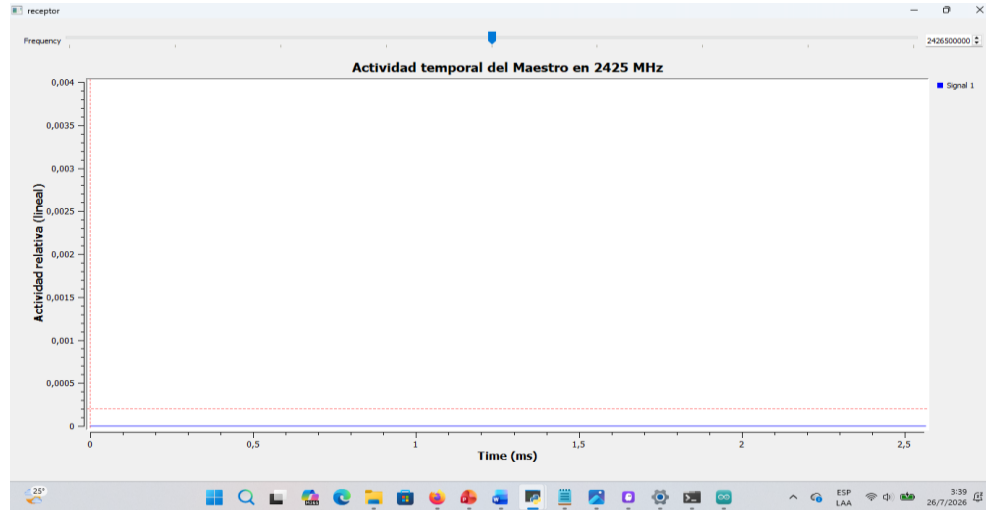


Figura 44 Evaluación de la actividad temporal del Maestro en 2425 MHz

Tabla 19
Tiempo de permanencia de la interferencia

Repetición	Inicio (ms)	Final (ms)	Duración (ms)
1	2.4655	2.5819	0.1164
2	2.3578	2.4828	0.1250
3	2.5716	2.6843	0.1127
4	2.5976	2.7060	0.1084
5	2.5195	2.6409	0.1214
6	2.7103	2.8187	0.1084
7	2.3938	2.5239	0.1301
8	2.6638	2.7710	0.1072
9	2.3721	2.5359	0.1638
10	2.5557	2.6760	0.1203
Media	-	-	0.1214
Desv. Est.	-	-	0.0162

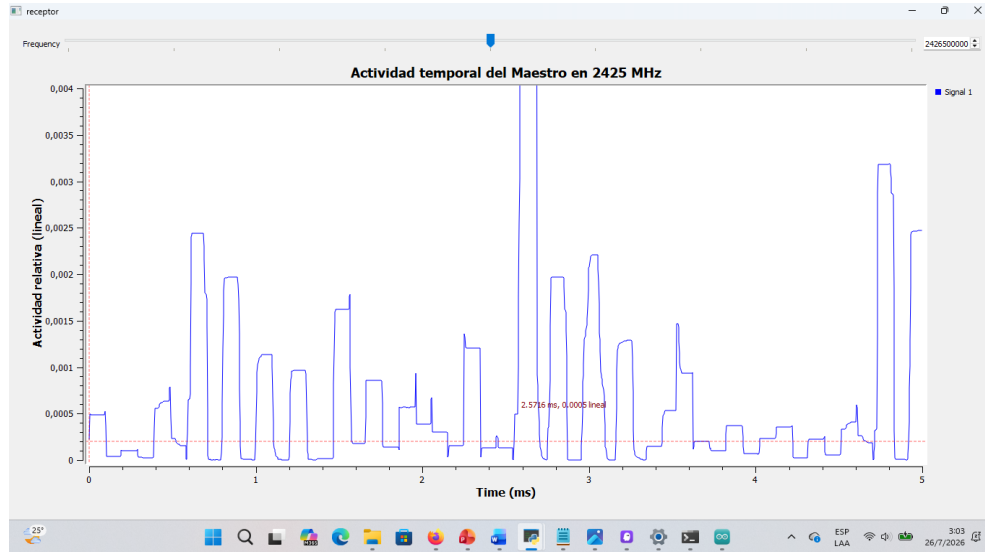


Figura 45 Inicio de prueba a 1 metro de los RF-Clown

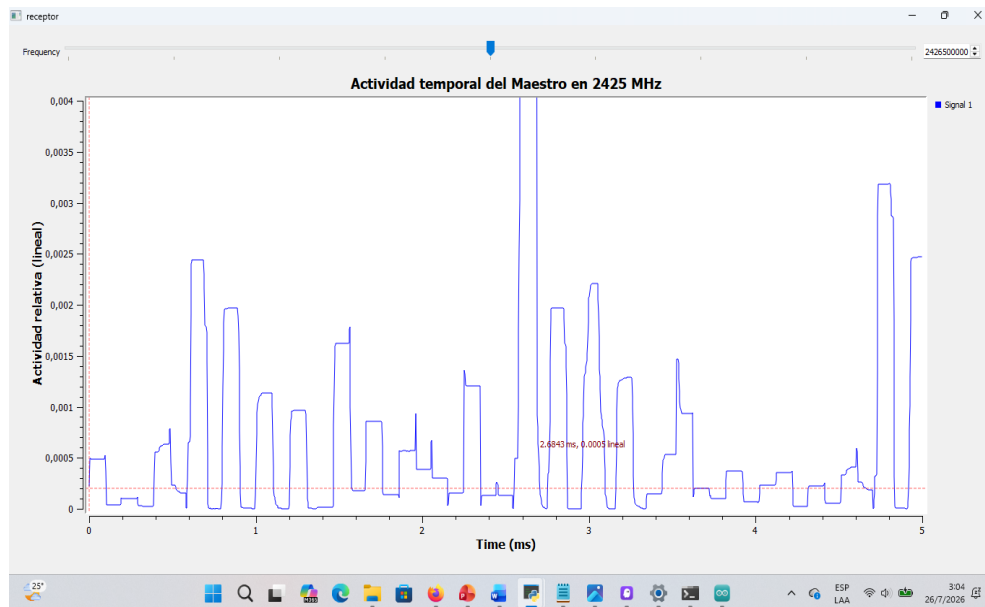


Figura 46 Final de prueba de 1 metro de distancia entre los RF-Clown

El sistema es excelente. Los tiempos de duración son:

- Muy bajos (~ 0.12 ms en promedio).

- Altamente consistentes (desviación estándar de solo 0.016 ms).
- Sin valores atípicos que distorsionen los resultados.

En la **Figura 45**, como en la **Figura 46**, se ha demostrado que el jammer responde de manera rápida, estable y predecible, lo cual es fundamental para garantizar la repetibilidad de los experimentos y la confiabilidad de los resultados.

4.7.1.2 Resultados a 2 metros en el modo Maestro

Tabla 20

Resumen a 2 metros de distancia de los RF-Clown

Repetición	Inicio (ms)	Final (ms)	Duración (ms)
1	2.7965	2.8745	0.0780
2	4.2931	4.3929	0.0998
3	4.2845	4.3972	0.1127
4	4.2931	4.3929	0.0998
5	2.8014	2.9141	0.1127
6	2.1206	2.2073	0.0867
7	2.3103	2.4181	0.1078
8	2.0945	2.1986	0.1041
9	3.0789	3.1830	0.1041
10	2.7927	2.9835	0.1908
Media	-	-	0.1097
Desv. Est.	-	-	0.0303

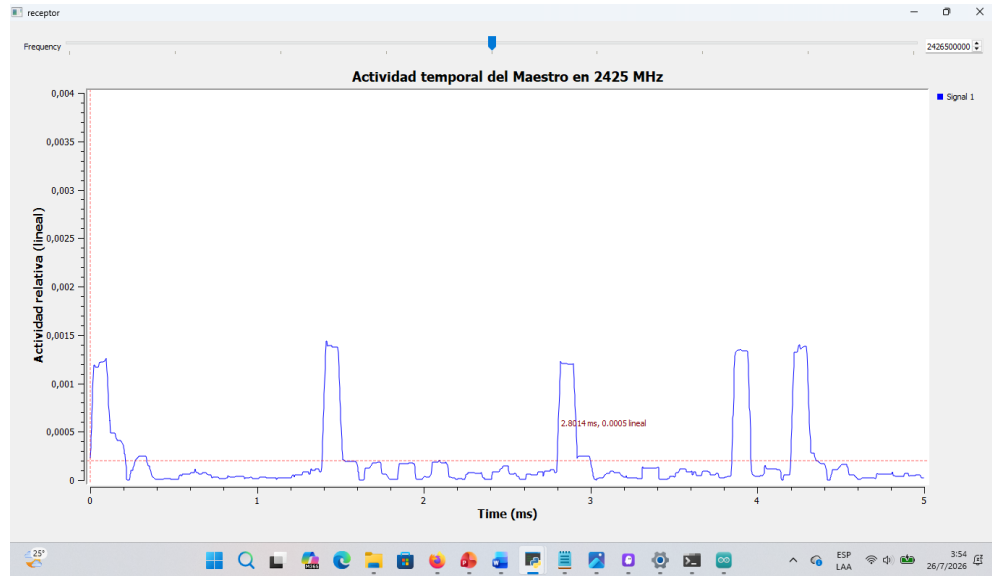


Figura 47 Actividad del muestreo para los 2 metros de separación

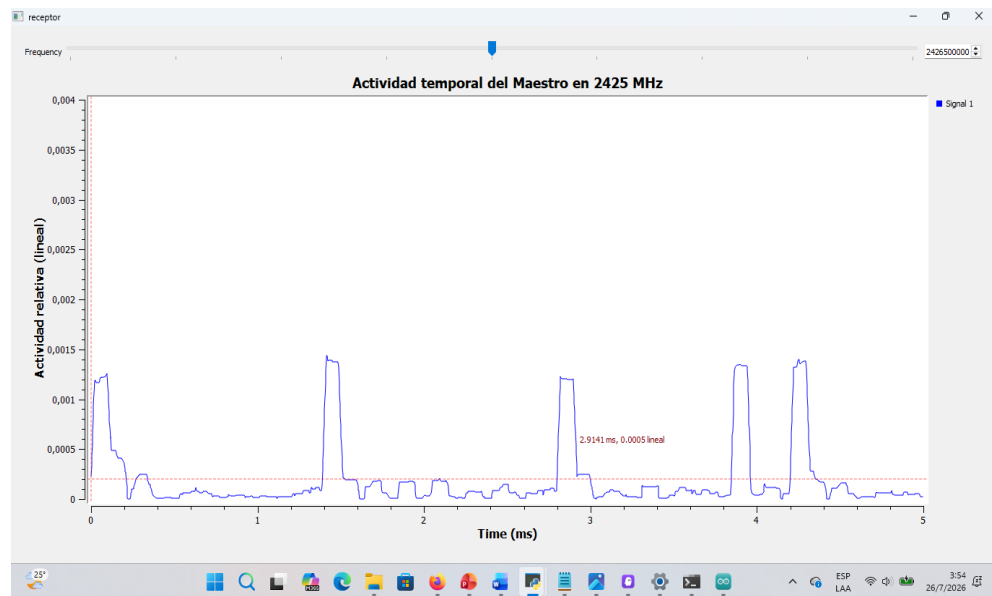


Figura 48 Concluido el muestreo de los 2 metros de separación

El sistema es excelente y altamente consistente, como podemos observar en las **Figuras 47 y 48**. Los tiempos de duración son:

- Muy bajos (~ 0.11 ms en promedio)

- Altamente consistentes (desviación estándar de solo 0.030 ms).
- Con un outlier aislado que no afecta de manera significativa la conclusión

general.

Esto confirma que el jammer responde de manera rápida, como se determinó en la Tabla 20, y que es estable y predecible en todas las pruebas realizadas.

4.7.1.3 Resultados a 3 metros en el modo Maestro

Tabla 21
Repeticiones de 3 metros de separación de los RF-Clown

Repetición	Inicio (ms)	Final (ms)	Duración (ms)
1	4.1804	4.2801	0.0997
2	4.1804	4.2801	0.0997
3	4.1891	4.2931	0.1040
4	4.2801	4.3755	0.0954
5	4.1897	4.2888	0.0991
6	4.1804	4.2801	0.0997
7	4.2151	4.3148	0.0997
8	4.1804	4.2801	0.0997
9	2.0989	2.1943	0.0954
10	4.2238	4.3235	0.0997
Media	-	-	0.0992

Repetición	Inicio (ms)	Final (ms)	Duración (ms)
Desv. Est.	-	-	0.0027

Las demás estadísticas de las gráficas de GNU Radio se encuentran en los anexos del documento.

El sistema es excepcionalmente estable y preciso, como se muestra en la tabla 21. Los tiempos de duración son:

- Prácticamente idénticos en todas las repeticiones (~ 0.1 ms).
- Variabilidad insignificante (desviación estándar de solo 0.0027 ms).
- Sin outliers que distorsionen los resultados.

Este nivel de consistencia demuestra que el jammer utilizado presenta un comportamiento altamente predecible y repetible, lo cual es fundamental para garantizar la validez y la confiabilidad de los experimentos.

4.7.1.4 Resultados a 1, 2 y 3 m

tabla consolidada:

Tabla 22
Resumen general y comparativas entre distancias

Ensayo	Permanencia a 1 m (ms)	Permanencia a 2 m (ms)	Permanencia a 3 m (ms)
1	0.1164	0.0780	0.0997
2	0.1250	0.0998	0.0997
3	0.1127	0.1127	0.1040
4	0.1084	0.0998	0.0954

Ensayo	Permanencia a 1 m (ms)	Permanencia a 2 m (ms)	Permanencia a 3 m (ms)
5	0.1214	0.1127	0.0991
6	0.1084	0.0867	0.0997
7	0.1301	0.1078	0.0997
8	0.1072	0.1041	0.0997
9	0.1638	0.1041	0.0954
10	0.1203	0.1908	0.0997
Promedio	0.1214	0.1097	0.0992
Desviación estándar	0.0162	0.0303	0.0027
Mínimo	0.1072	0.0780	0.0954
Máximo	0.1638	0.1908	0.1040

En la tabla 22, los tiempos de permanencia promedio fueron de 0,1214 ms a 1 m, 0,1097 ms a 2 m y 0,0992 ms a 3 m. Estos valores muestran una variación reducida entre las tres distancias evaluadas.

La menor desviación estándar se registró a 3 m, con 0,0027 ms, lo que indica una mayor uniformidad de las lecturas en esa condición experimental. En comparación, la mayor dispersión se registró a 2 m, con 0,0303 ms, atribuible principalmente al valor de 0,1908 ms registrado en el ensayo 10.

Estas diferencias no demuestran que el sistema funcione mejor ni que exista una distancia óptima. El tiempo de permanencia depende principalmente de la programación del firmware, mientras que las variaciones observadas pueden deberse a factores como la propagación, el umbral de detección y la resolución temporal del SDR.

En consecuencia, los resultados confirman la detección repetible de la actividad en las

tres distancias evaluadas, así como en las condiciones de montaje experimental.

4.7.2 Tiempo de revisita en 2425 MHz

El tiempo de revisita corresponde al intervalo necesario para que el barrido regrese a la misma frecuencia. En la **Figura 49** se muestra la configuración utilizada en GNU Radio para recopilar los resultados. Se calcula entre dos apariciones consecutivas y equivalentes de la actividad en 2425 MHz:

Fórmula:

$$T_{REVISITA} = T_2 - T_1$$

La mejor estimación que permite la resolución de la imagen es:

$$T_1 \approx 50.0000 \text{ ms}$$

$$T_2 \approx 82.0069 \text{ ms}$$

Por tanto:

$$T_{REVISITA} = 82.0069 - 50.0000$$

$$T \approx 32.0069 \text{ ms}$$

El resultado indica que el barrido tardó 32,0069 ms en regresar al mismo punto de referencia temporal de 2425 MHz.

Este valor corresponde al primer ensayo y se presenta únicamente como evidencia del procedimiento de lectura. Los resultados consolidados de las diez repeticiones a 1, 2 y 3 m, con sus promedios y desviaciones estándar, se presentarán en tablas de datos más adelante.

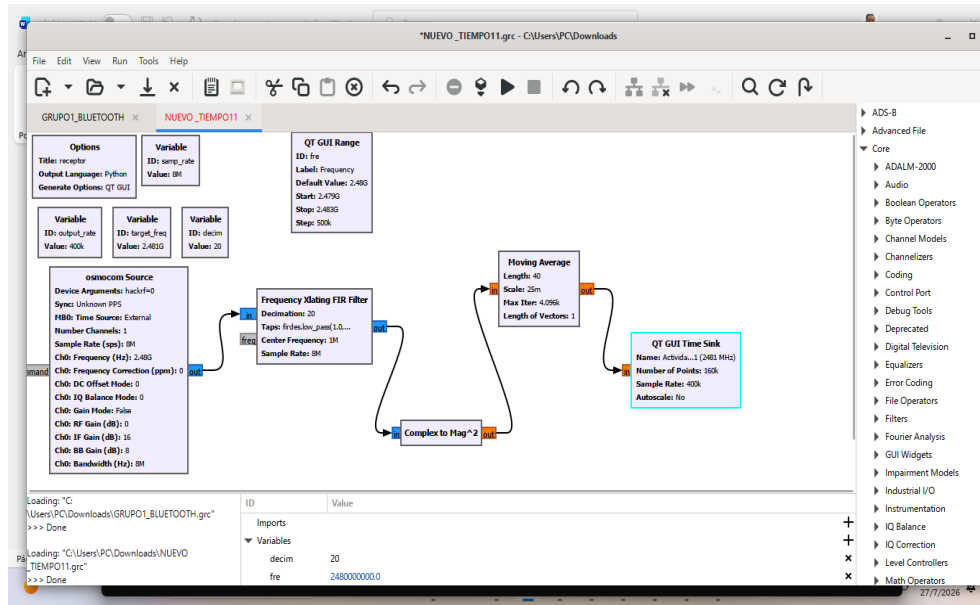


Figura 49 Cuadro de bloques usados para las siguientes pruebas de tiempo

4.7.2.1 Resultados a 1 metro en el modo Maestro

Con la configuración ajustada de GNU Radio se obtuvieron los siguientes resultados:

Tabla 23
Repeticiones realizadas a 1 m

Repetición	Inicio (ms)	Final (ms)	Duración (ms)
1	32.7883	65.4045	32.6162
2	50.0000	82.0069	32.0069
3	57.7855	87.3702	29.5847
4	71.1538	100.8741	29.7203
5	55.8824	86.1592	30.2768
6	70.0692	100.3460	30.2768
7	79.4118	110.3806	30.9688
8	65.4045	97.0665	31.6620

Repetición	Inicio (ms)	Final (ms)	Duración (ms)
9	82.0069	112.5931	30.5862
10	100.3460	131.2262	30.8802
Media	-	-	30.8549
Desv. Est.	-	-	0.9502

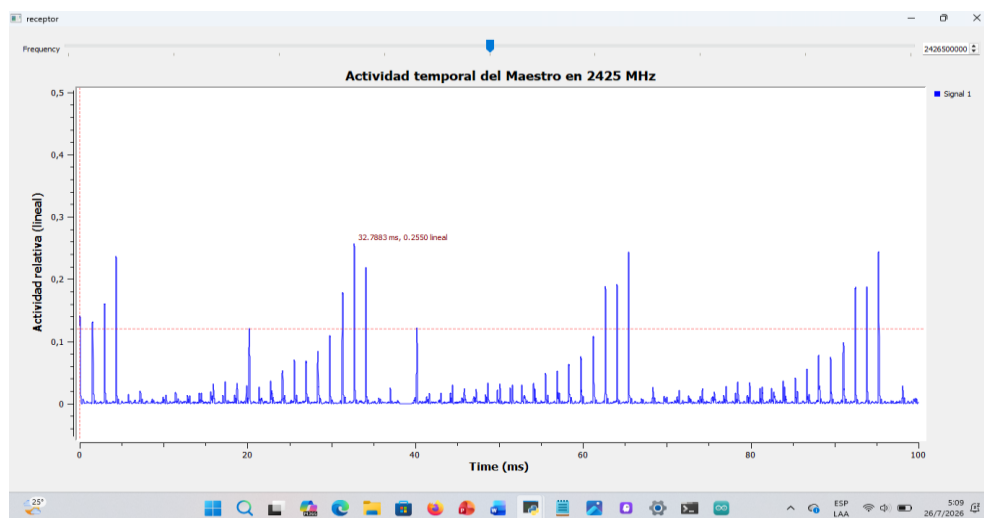


Figura 50 Primer análisis con la nueva configuración de GNU Radio

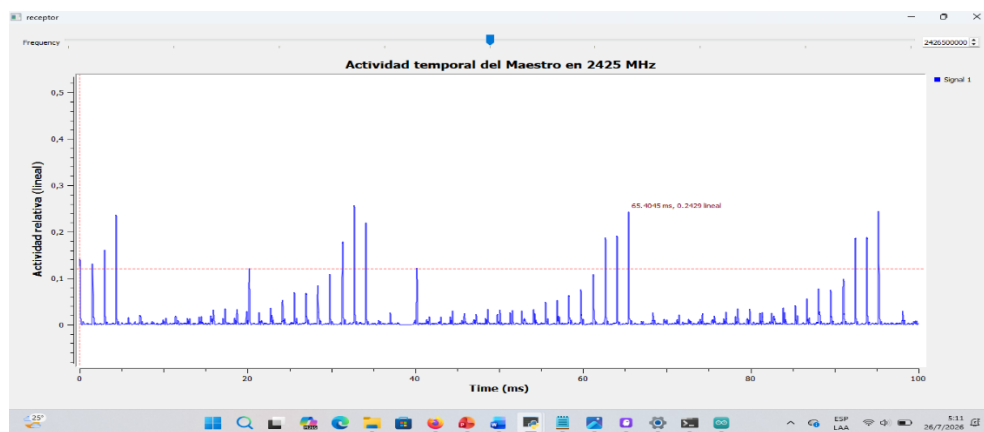


Figura 51 Término del primer análisis a 1 metro de separación entre los RF-Clown

El sistema es altamente estable y predecible, como se demuestra en las **Figuras 50 y 51**.

El tiempo de revisita de la Tabla 23 tiene un promedio de 30.85 ms, lo que indica que el barrido del jammer regresa a la frecuencia de 2425 MHz de manera consistente y periódica. La desviación estándar de solo 0.95 ms confirma que:

- El barrido es regular.
- La secuencia es repetible.
- El sistema mantiene estabilidad temporal.

Este comportamiento es ideal para garantizar que la interferencia se aplique de forma uniforme en el espectro, sin dejar frecuencias sin cubrir durante periodos prolongados.

4.7.2.2 Resultados a 2 metros en el modo Maestro

Tabla 24
Repeticiones de pruebas a 2 metros de distancia entre los RF-Clown

Repetición	Inicio (ms)	Final (ms)	Duración (ms)
1	95.5614	125.3264	29.7650
2	91.7319	121.4970	29.7651
3	87.7285	117.3194	29.5909
4	93.1245	122.7154	29.5909
5	82.0069	111.3521	29.3452
6	86.1592	116.1232	29.9640
7	100.3460	129.2124	28.8664
8	97.0665	126.9179	29.8514

Repetición	Inicio (ms)	Final (ms)	Duración (ms)
9	110.3806	140.2524	29.8718
10	131.2262	160.0994	28.8732
Media	-	-	29.5234
Desv. Est.	-	-	0.4247

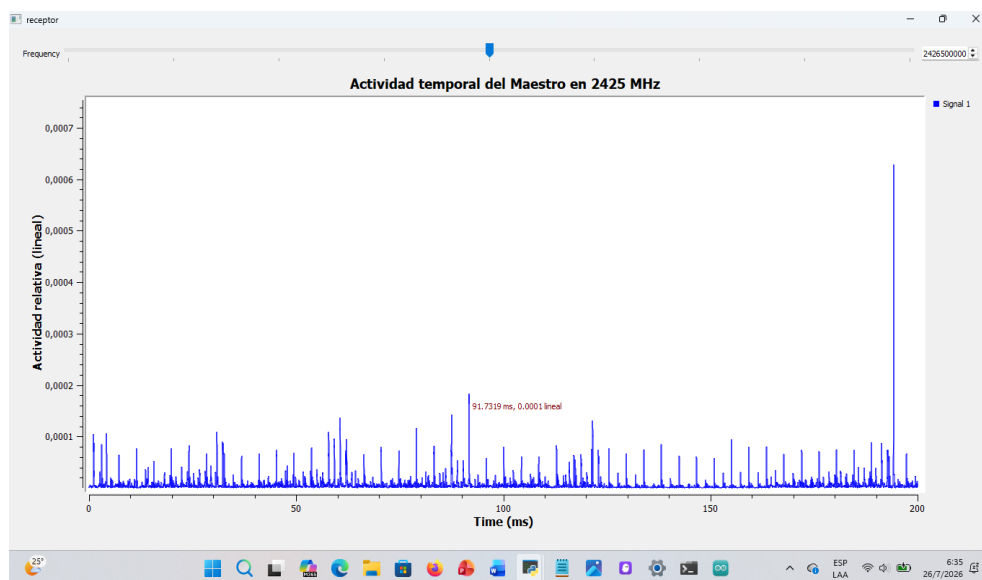


Figura 52 Segunda prueba a 2 metros entre los RF-Clown

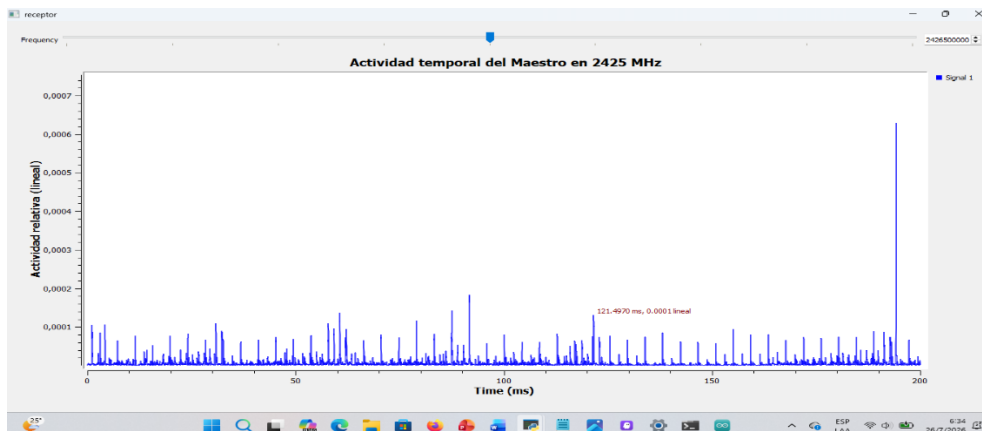


Figura 53 Fin de prueba 2 con los resultados de repeticiones

En la Tabla 24 el sistema mantiene una estabilidad excepcional.

El tiempo de revisita promedio de 29.52 ms de la Tabla 25 es prácticamente idéntico al de la tabla anterior de 1 metro (30.85 ms), lo que confirma que el barrido es regular y consistente en diferentes frecuencias, como se ve en las **Figuras 52 y 53**.

Tabla 25

Promedio y comparación con la tabla anterior

Parámetro estadístico	Tabla anterior (1 metro)	Tabla actual (2 metros)
Promedio	30,85 ms	29,52 ms
Desviación estándar	0,95 ms	0,42 ms

La desviación estándar es aún más baja (0.42 ms), lo que indica que, dada la frecuencia, el sistema es aún más estable y predecible, lo cual es excelente para la repetibilidad de los experimentos.

4.7.2.3 Resultados a 3 metros en el modo Maestro.

Tabla 26

Repeticiones a 3 metros entre los RF-Clown en tiempo de revisita

Repetición	Inicio (ms)	Final (ms)	Duración (ms)
1	66.6667	95.8811	29.2144
2	97.7233	127.8205	30.0972
3	72.5849	102.3499	29.7650
4	55.5844	85.1948	29.6104
5	55.9307	87.0996	31.1689

Repetición	Inicio (ms)	Final (ms)	Duración (ms)
6	127.4956	157.2680	29.7724
7	85.1948	115.1411	29.9463
8	102.3499	132.1796	29.8297
9	87.0996	117.1503	30.0507
10	115.1411	144.9536	29.8125
Media	-	-	29.9268
Desv. Est.	-	-	0.5657

Los resultados presentados en la Tabla 26 demuestran una alta consistencia en el tiempo de revisita a una distancia de 3 metros entre los RF-Clown. La duración media de las repeticiones es de 29,93 ms, con una desviación estándar de apenas 0,57 ms. Esta baja dispersión confirma la estabilidad del comportamiento temporal del sistema bajo estas condiciones experimentales, lo que garantiza un alto grado de repetibilidad en el proceso de intercambio de señales.

4.7.2.4 Resultados a 1, 2 y 3 m

tabla consolidada:

Tabla 27
Resumen del tiempo de revisita según la distancia

Parámetro	Revisita a 1 m (ms)	Revisita a 2 m (ms)	Revisita a 3 m (ms)
Promedio (ms)	30.85	29.52	29.93
Desv. Est. (ms)	0.95	0.42	0.57
Mínimo (ms)	29.58	28.87	29.21

Parámetro	Revisita a 1 m (ms)	Revisita a 2 m (ms)	Revisita a 3 m (ms)
Máximo (ms)	32.62	29.96	31.17

El sistema en modo Maestro a 3 m demuestra alta estabilidad y reproducibilidad.

El tiempo de revisita promedio de 29.93 ms se encuentra dentro del rango esperado (~30 ms), y la desviación estándar de 0.57 ms confirma que:

- El barrido es regular y periódico.
- No hay variaciones significativas entre repeticiones.
- El sistema mantiene un comportamiento predecible.
- Los resultados son consistentes con las tablas anteriores.

Esto valida que el modo Maestro a 3 metros, resumido en la tabla 27, opera con la misma estabilidad que las configuraciones previas, lo que garantiza la repetibilidad de los experimentos.

4.7.3 Comparación temporal según la distancia

Los resultados muestran que tanto el tiempo de permanencia como el de revisita se mantuvieron dentro de intervalos similares en las tres distancias evaluadas. Dado que estos parámetros están determinados principalmente por la lógica temporal del firmware, la distancia no debería alterar directamente sus valores. Las variaciones observadas se relacionan con la propagación, el nivel de señal recibido, la identificación del umbral y la incertidumbre en la lectura del SDR.

La Tabla 28 consolida ambas métricas temporales según la distancia:

Tabla 28
Comparación de métricas temporales según la distancia

Distancia	Permanencia promedio (ms)	Revisita promedio (ms)	Observación
1 m	0.1214	30.85	Mayor tiempo de permanencia; revisita medida en 2425 MHz
2 m	0.1097	29.52	Tiempo intermedio; revisita más estable
3 m	0.0992	29.93	Menor tiempo de permanencia; revisita consistente

La distancia puede dificultar la detección del pulso, como se establece en la Tabla 28, pero no debería sustituir el tiempo programado.

4.8 Evaluación de la recepción relativa de anuncios BLE

4.8.1 Definición de la métrica

Para evaluar el efecto del sistema coordinado sobre la detección del dispositivo BLE se utilizó la métrica denominada Recepción Relativa de Anuncios (ARR). Esta representa el porcentaje de anuncios recibidos durante la operación conjunta del Maestro y el Esclavo respecto de la cantidad registrada en la condición de referencia.

La ARR se definió como una métrica operacional de esta investigación:

$$ARR_i(\%) = \frac{N_{activo,i}}{N_{referencia,i}} \times 100$$

Donde:

- $N_{referencia,i}$: Anuncios BLE recibidos en el ensayo (i) con ambos RF-Clown

apagados.

- $N_{activo,i}$: Anuncios recibidos al mismo tiempo con Maestro y Esclavo activos.
- ARR_i : Porcentaje de recepción relativa del ensayo (i).

La reducción relativa de anuncios se calculó mediante:

$$R_i(\%) = 100 - ARR_i$$

Una ARR más baja indica que, en la condición activa, se detectó una menor proporción de anuncios muy distintos de los referenciados.

La sustitución del parámetro PLR por ARR se debió a limitaciones en la observabilidad del montaje experimental. La medición directa del PLR requiere equipos avanzados, como analizadores profesionales (Ellisys Bluetooth Explorer, Teledyne LeCroy Frontline FTS4BT) o, como alternativa más económica, un Nordic nRF52840 Dongle con el software nRF Sniffer. Sin embargo, este último no estuvo disponible para el proyecto, lo que limitó la observación directa de la tasa de pérdida de paquetes.

Por lo tanto, se optó por evaluar el desempeño del enlace mediante el parámetro de Recepción Relativa de Anuncios (ARR). Este parámetro permite caracterizar la calidad de la comunicación Bluetooth en la banda ISM mediante el monitoreo pasivo de paquetes de anuncio, sin necesidad del hardware de captura bidireccional mencionado anteriormente. Esta decisión se documenta como parte del alcance del proyecto, de acuerdo con los recursos técnicos disponibles en ese momento. En consecuencia, calcular el PLR habría supuesto una estimación no verificable. La ARR se adoptó como indicador operacional, ya que permite comparar los conteos observados en ventanas de 60 s, bajo el mismo receptor, filtro, posición y configuración. Por

tanto, la ARR permite cuantificar de forma reproducible la variación relativa de los anuncios detectados, pero no debe interpretarse como una medida de la pérdida real de paquetes.

4.8.2 Dispositivo objetivo y herramienta de medición

Para las pruebas de audio, seleccionamos el parlante ENGLAND SOUND APP por su compatibilidad con la conectividad inalámbrica con smartphones y laptops. Como se aprecia en la **Figura 54**, utilizamos la herramienta Acrylic BLE Analyzer para identificar y registrar su dirección MAC durante el enlace:

MAC = 41:42:C4:33:39:41



Figura 54 Dispositivo elegido para práctica y resultados

La dirección se utilizó como filtro principal, mientras que el nombre de contenido del paquete publicitario se empleó como verificación adicional. Esto permitió diferenciar los anuncios del dispositivo objetivo de los provenientes de otros dispositivos presentes en el laboratorio.

Acrylic BLE Analyzer se utilizó como herramienta principal porque permite registrar:

- Fecha y hora de recepción.
- Dirección del dispositivo.
- Nombre anunciado.
- RSSI del anuncio recibido.
- Tipo y contenido del paquete.
- Archivo PCAP de respaldo.

4.8.3 Configuración experimental

Tabla 29

Componentes y condiciones de las pruebas de ARR

Parámetro	Configuración
Dispositivo objetivo	ENGLAND SOUND APP
Dirección observada	41:42:C4:33:39:41
Analizador	Acrylic BLE Analyzer
Duración por condición	60 segundos
Condiciones	Referencia, sistema activo y verificación posterior
Distancias	1 m, 2 m y 3 m
Repeticiones	10 por distancia
Arquitectura activa	RF-Clown Maestro–Esclavo
Entorno	Laboratorio controlado
Evidencia	Capturas, archivos PCAP y fotografías

La Tabla 29 presenta el núcleo de nuestro experimento de ARR. Lo que buscamos observar aquí es cómo responde el sistema al variar la distancia entre el emisor y el receptor en

tres momentos críticos: la línea base, cuando la arquitectura RF-Clown entra en acción y la fase de verificación. Al ver el comportamiento de las 10 repeticiones agrupadas por distancia, se evidencia visualmente si el sistema mantiene su estabilidad o si la distancia degrada la captura de paquetes, lo que permite validar la efectividad del montaje en un entorno controlado.

Durante todos los ensayos se mantuvieron constantes:

- La ubicación del parlante.
- La posición del receptor.
- La orientación de las antenas.
- La configuración del firmware.
- La alimentación de los dispositivos.
- La duración de las capturas.
- El adaptador y computador utilizados.

4.8.4 Procedimiento de medición

Para cada repetición se realizaron tres etapas consecutivas:

Etapas 1: condición de referencia

1. Se mantuvieron apagados ambos RF-Clown.
2. Se inició una captura nueva en Acrylic.
3. Se registró la actividad BLE durante 60 segundos.
4. Se detuvo y guardó la captura.
5. Se contabilizaron los anuncios del dispositivo objetivo.
6. El resultado final tiene registro $N_{referencia,i}$

Etapla 2: sistema coordinado activo

1. Se activaron Maestro y Esclavo.
2. Se verificó su coordinación mediante OLED, NeoPixel o registro serial.
3. Se inició una nueva captura de 60 segundos.
4. Acrylic permaneció escaneando durante toda la ventana.
5. Se detuvo y guardó el archivo PCAP.
6. Los anuncios recibidos se registraron como ($N_{activo,i}$).
7. Cuando no se detectó ningún anuncio, se registró el valor 0.

Etapla 3: verificación posterior

1. Se desactivaron los RF-Clown.
2. Se realizó una tercera captura de 60 segundos.
3. Se contabilizaron nuevamente los anuncios.
4. Los resultados se registraron entonces como ($N_{posterior}$).

Esta última etapa permite verificar que el dispositivo recupera su detectabilidad tras retirar la condición experimental.

4.8.5 Identificación y conteo de anuncios

El conteo debe realizarse únicamente sobre registros que cumplan estas condiciones:

- Dirección correspondiente al dispositivo objetivo.
- Nombre ENGLAND SOUND APP cuando esté presente.
- Paquete identificado como anuncio BLE.

- Registro incluido dentro de lo planificado en 60 segundos.
- Mismo tipo de paquete publicitario en todas las pruebas.

La columna # de Acrylic no debe utilizarse mediante la resta entre el primer y el último número, porque corresponde al contador general de la captura y puede incluir paquetes de otros dispositivos.

El procedimiento correcto es contar las filas filtradas del objetivo o revisar el total del archivo PCAP cuando se haya confirmado que contiene exclusivamente los anuncios seleccionados.

Si aparecen filas sin nombre, pero estas contienen la misma dirección y corresponden al mismo tipo de paquete publicitario, pueden incluirse siempre que se aplique el mismo criterio en todas las capturas.

4.8.6 Resultados de ARR a 1 metro

Tabla 30
Análisis del parámetro ARR a 1 metro de separación entre RF-Clown

Ensayo	Referencia	RF-Clown activos	Recuperación	ARR activo	Reducción de recepción	ARR posterior
1	44	4	44	9,09 %	90,91 %	100,00 %
2	43	2	40	4,65 %	95,35 %	93,02 %
3	48	0	44	0,00 %	100,00 %	91,67 %
4	40	0	46	0,00 %	100,00 %	115,00 %
5	40	2	34	5,00 %	95,00 %	85,00 %
6	40	5	44	12,50 %	87,50 %	110,00 %

Ensayo	Referencia	RF- Clown	Recuperación activos	ARR activo	Reducción de recepción	ARR posterior
7	36	6	32	16,67 %	83,33 %	88,89 %
8	37	2	42	5,41 %	94,59 %	113,51 %
9	42	6	41	14,29 %	85,71 %	97,62 %
10	33	2	61	6,06 %	93,94 %	184,85 %
Media de porcentajes individuales	40,30	2,90	42,80	7,37 %	92,63 %	107,96 %
Desviación estándar	—	—	—	5,68 puntos porcentuales	5,68 puntos porcentuales	28,96 puntos porcentuales

La recepción posterior se calcula mediante:

$$ARR_{posterior,i} = \frac{N_{posterior,i}}{N_{referencia,i}} \times 100$$

En la tabla 30, el análisis del parámetro ARR a una distancia de 1 metro revela que, ante la activación de la arquitectura RF-Clown (promedio de 2,90 nodos activos), se registra una reducción promedio en la recepción del 92,63 %. A pesar de esta disminución, el sistema logra una recuperación de paquetes que da como resultado un ARR sobre el promedio posterior del 107,96 %. La alta desviación estándar en este último indicador (28,96 puntos porcentuales) evidencia una variabilidad significativa entre ensayos y alcanza valores superiores al 100 % en casos específicos, lo que sugiere una capacidad de recuperación dinámica del sistema bajo las condiciones de prueba establecidas.

4.8.7 Resultados de ARR a 2 metros

Tabla 31
Resultados de repeticiones a 2 metros del ARR con interferencia

Ensayo	Referencia	RF-Clown activos	Recuperación	ARR activo	Reducción	ARR posterior
1	37	0	46	0,00 %	100,00 %	124,32 %
2	45	2	33	4,44 %	95,56 %	73,33 %
3	46	0	45	0,00 %	100,00 %	97,83 %
4	24	2	51	8,33 %	91,67 %	212,50 %
5	42	2	35	4,76 %	95,24 %	83,33 %
6	41	0	44	0,00 %	100,00 %	107,32 %
7	41	3	34	7,32 %	92,68 %	82,93 %
8	37	0	36	0,00 %	100,00 %	97,30 %
9	36	4	36	11,11 %	88,89 %	100,00 %
10	44	0	36	0,00 %	100,00 %	81,82 %
Media de porcentajes individuales	39,30	1,30	39,60	3,60 %	96,40 %	106,07 %
Desviación estándar	—	—	—	4,21 puntos	4,21 puntos	40,22 puntos

El análisis del parámetro ARR a una distancia de 2 metros en la tabla 31 muestra que, con una activación menor de la arquitectura RF-Clown (promedio de 1,30 nodos), la reducción de la recepción es del 96,40 %. En este escenario, el sistema alcanza un ARR posterior promedio de 107,96 %, manteniendo una eficacia similar a la de 1 metro, aunque con una mayor inestabilidad en los resultados, reflejada en una desviación estándar de 40,22 puntos porcentuales. Esta fluctuación, que incluye picos de recuperación superiores al 200 %, indica que la capacidad del sistema para gestionar la recepción de paquetes es altamente sensible a las condiciones de

interferencia a esta distancia.

4.8.8 Resultados de ARR a 3 metros

Tabla 32
Análisis con 3 metros entre los RF-Clown en métrica ARR

Ensayo	Referencia	RF-Clown activos	Recuperación	ARR activo	Reducción	ARR posterior
1	35	0	42	0,00 %	100,00 %	120,00 %
2	37	0	44	0,00 %	100,00 %	118,92 %
3	29	1	41	3,45 %	96,55 %	141,38 %
4	27	3	42	11,11 %	88,89 %	155,56 %
5	35	2	28	5,71 %	94,29 %	80,00 %
6	46	4	41	8,70 %	91,30 %	89,13 %
7	48	2	28	4,17 %	95,83 %	58,33 %
8	42	4	29	9,52 %	90,48 %	69,05 %
9	32	4	44	12,50 %	87,50 %	137,50 %
10	40	4	43	10,00 %	90,00 %	107,50 %
Media de porcentajes individuales	37,10	2,40	38,20	6,52 %	93,48 %	107,74 %
Desviación estándar	—	—	—	4,51 puntos	4,51 puntos	32,72 puntos

El análisis del parámetro ARR, a una distancia de 3 metros de la tabla 32, indica que ante la activación de un promedio de 2,40 por nodo RF-Clown, la reducción de la recepción es del 93,48 %. El sistema logra un ARR posterior promedio de 107,74 %, manteniendo una tendencia

de recuperación similar a las distancias anteriores. No obstante, la desviación estándar de 32,72 puntos porcentuales confirma una alta variabilidad en el desempeño, con resultados que oscilan desde una recuperación limitada (58,33 %) hasta valores significativamente altos (155,56 %), lo que subraya el comportamiento dinámico y fluctuante del enlace bajo estas condiciones de distancia e interferencia.

4.8.9 Cálculo del resultado global

Para evitar que un ensayo con pocos anuncios tenga el mismo peso que otro con la mayor cantidad de registros, el resultado global se calculó a partir de los conteos acumulados de las diez repeticiones.

La recepción posterior global se calcula mediante:

$$ARR_{posterior,global} = \frac{\sum_{i=1}^{10} \cdot N_{posterior,i}}{\sum_{i=1}^{10} \cdot N_{referencia,i}} \times 100$$

Para obtener un resultado representativo en cada distancia, se utilizó la ARR global, calculada como el cociente entre la suma de los anuncios recibidos en la condición activa y la suma de los registrados en la condición de referencia, como se muestra en la tabla 33. Este procedimiento pondera cada ensayo según el volumen de anuncios y evita que una repetición con pocos registros tenga el mismo peso que otra con un mayor número de observaciones. Por esta razón, los resultados globales pueden diferir ligeramente de la media aritmética de los porcentajes individuales presentada en las tablas anteriores.

Tabla consolidada

Tabla 33
Resultados globales de ARR según la distancia

Distancia	Referencia	RF-Clown activos	Recuperación	ARR global	Reducción global	ARR posterior
1 m	403	29	428	7,20 %	92,80 %	106,20 %
2 m	393	13	396	3,31 %	96,69 %	100,76 %
3 m	371	24	382	6,47 %	93,53 %	102,96 %
Total	1167	66	1206	5,66 %	94,34 %	103,34 %

Nota: La ARR global se calculó a partir de los conteos totales acumulados de las diez repeticiones. Por tanto, los valores de 7,20 %, 3,31 % y 6,47 % se consideran resultados principales para comparar las distancias. Las medias de 7,37 %, 3,60 % y 6,52 % se conservan únicamente como estadísticos descriptivos de los porcentajes obtenidos en los ensayos individuales

La menor ARR global se obtuvo a 2 m, con 3,31 %, equivalente a una reducción relativa de anuncios del 96,69 %. A 1 m, la ARR global fue de 7,20 %, con una reducción del 92,80 %, mientras que a 3 m se obtuvo una ARR global de 6,47 % y una reducción del 93,53 %. Estos resultados indican que, bajo las condiciones específicas del montaje experimental, la menor tasa de recepción relativa de anuncios a 2 m. No obstante, esta observación no permite generalizar dicha separación como una distancia óptima universal.

4.8.10 Ejemplo de cálculo

Supóngase que en un ensayo se obtienen:

- Referencia: 83 anuncios.
- Sistema activo: 2 anuncios.
- Condición posterior: 70 anuncios.

Entonces:

$$ARR_{activo} = \frac{2}{83} \times 100 = 2,41\%$$

$$R = 100 - 2,41 = 97,59\%$$

$$ARR_{posterior} = \frac{70}{83} \times 100 = 84,34\%$$

Por lo tanto, durante la operación coordinada se registró el 2,41 % de los anuncios observados en la referencia, lo que equivale a una reducción relativa del 97,59 %. Tras desactivar el sistema, la recepción alcanzó el 84,34 % en la condición inicial.

El cálculo anterior ilustra la aplicación de las ecuaciones y los resultados experimentales consolidados.

4.8.11 Criterios de interpretación

Tabla 34
Criterios descriptivos para interpretar la ARR

Resultado	Interpretación
ARR = 100 %	Recepción equivalente a la referencia
ARR entre 50 % y 99,99 %	Reducción moderada
ARR entre 1 % y 49,99 %	Reducción considerable

Resultado	Interpretación
ARR = 0 %	Ningún anuncio recibido durante la ventana
ARR posterior próxima a 100 %	Recuperación cercana a la referencia

Los intervalos anteriores se emplean únicamente como criterios descriptivos del presente trabajo, ilustrado en la tabla 34, y no corresponden a categorías oficiales del estándar Bluetooth.

El resultado principal es la ARR durante la operación coordinada. La recepción posterior demuestra si la detección vuelve a aproximarse al nivel inicial tras retirar la condición experimental.

4.8.12 Limitaciones

La ARR representa únicamente la cantidad relativa de anuncios recibidos por el analizador. No permite conocer directamente:

- La cantidad total transmitida por el parlante.
- La pérdida real de paquetes.
- El estado interno del dispositivo.
- La calidad de una conexión Bluetooth Classic.
- La continuidad de los paquetes de audio A2DP.

Además, el resultado depende de la sensibilidad del receptor, la posición de las antenas, la actividad ambiental y la configuración del analizador. Por esta razón, todas las condiciones deben mantenerse constantes.

4.9 Validación funcional de la sincronización ESB

La coordinación ESB se verificó funcionalmente mediante los estados mostrados en las pantallas OLED, los indicadores NeoPixel y los registros seriales. La medición instrumental directa del canal 81 no se utilizó como resultado cuantitativo debido a la presencia de actividad ambiental en 2481 MHz.

La actividad observada en la banda de 2481 MHz, con los RF-Clown apagados, impidió atribuir ese componente exclusivamente al enlace ESB; por ello, no se reportó como resultado cuantitativo.

Utiliza:

- OLED del maestro y del esclavo.
- Estado del NeoPixel.
- Registros seriales.
- sequenceID.
- Contadores de paquetes.
- Respuesta al apagar uno de los dispositivos.
- Activación del timeout.

4.10 Discusión general

Los resultados se analizaron en cuanto al funcionamiento del firmware, al comportamiento del enlace ESB y al efecto observado en Bluetooth Classic y en BLE. La distribución complementaria del barrido se verificó mediante los registros del sistema y las capturas espectrales.

- La evidencia de la OLED, del monitor serial y de GNU Radio permite verificar la

operación complementaria en los canales pares e impares.

- La pérdida de sincronización permite evaluar el equilibrio ESB, pero no evidencia una latencia inferior a 5 ms.
- La ARR cuantifica la reducción relativa de anuncios detectados.
- Los efectos sobre Bluetooth Classic se describieron mediante interrupciones, desconexiones y tiempos observados. En BLE, la ARR evidenció una reducción de anuncios detectados durante la condición activa; este resultado no se interpreta como PLR ni como prueba de significancia estadística.

La separación de 2 m registró la menor ARR activa global (3,31 %) bajo las condiciones experimentales evaluadas. No obstante, este resultado es específico del montaje, de los dispositivos y del entorno empleados, por lo que no puede considerarse una distancia óptima universal.

4.11 Limitaciones

Con el propósito de evaluar la estabilidad del sistema desarrollado, se realizó un análisis estadístico descriptivo de las principales variables medidas durante el proceso experimental.

- Las pruebas se realizaron en un entorno controlado y no representan todas las condiciones de propagación de escenarios reales.
- HackRF One y GNU Radio proporcionaron evidencia espectral cualitativa, pero no permitieron obtener mediciones de potencia calibradas.
- No se midió la latencia paquete a paquete del enlace ESB, con analizador lógico u

osciloscopio.

- El Acrylic BLE Analyzer no informa el número real de anuncios transmitidos; por ello, se adoptó la métrica ARR en lugar del PLR.
- Los hallazgos se limitan exclusivamente al conjunto de dispositivos, firmware, antenas y distancias evaluados en este estudio.

4.12 Verificación de objetivos

Objetivo General

Desarrollar una estrategia de coordinación lineal entre dos dispositivos RF-Clown v2 para generar interferencias sincronizadas en redes Bluetooth/BLE, utilizando exclusivamente las capacidades de hardware y firmware abiertos de estos dispositivos.

Objetivos Específicos

Objetivo específico 1: Adaptar el firmware para habilitar modos Maestro/Esclavo

Se modificó el código fuente e implementó una arquitectura lógica de sincronización distribuida, y el Maestro controla la secuencia de la operación y transmite paquetes de sincronización al Esclavo únicamente a través de un canal independiente. Esto permitió una operación coordinada durante toda la ejecución del sistema, proceso debidamente documentado.

Objetivo específico 2: Implementar la estrategia de distribución coordinada de canales.

Cumplimiento parcial. El firmware sí logró implementar la distribución complementaria de canales (impares en el Maestro y pares en el Esclavo). La actividad en las frecuencias asignadas fue verificada cualitativamente mediante capturas con HackRF One y GNU Radio; así,

pudimos estimar tanto los tiempos de permanencia como los de revisita. No obstante, al no contar con una medición calibrada y simultánea de todas las portadoras mediante un analizador de espectro avanzado, no fue posible determinar cuantitativamente la cobertura espectral ni la potencia radiada total.

Objetivo específico 3: Evaluar el desempeño en configuración lineal

Se realizaron pruebas a 1 m, 2 m y 3 m y se obtuvieron datos cuantitativos de los parámetros de permanencia, revisita y ARR. Los resultados solo describen el comportamiento de la arquitectura en la prueba actual. No determinan una distancia óptima universal ni compiten numéricamente con el firmware original, ya que el experimento no se diseñó para la comparación.

4.13 Síntesis del capítulo

El capítulo presentó la validación funcional del sistema, la verificación cualitativa del barrido mediante HackRF One y GNU Radio y los resultados obtenidos en Bluetooth Classic y BLE. La arquitectura coordinada utilizó los radios A y B para distribuir el barrido par e impar y la radio C en el canal 81, correspondiente a 2481 MHz, para mantener el enlace ESB.

RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

Resultados

Se implementó una arquitectura Maestro–Esclavo entre dos dispositivos RF-Clown v2, sin incorporar hardware externo.

El enlace ESB mantuvo la coordinación funcional. El establecimiento inicial se registró

entre 30 y 34 ms; no se obtuvo una medición propia de latencia paquete a paquete.

La estrategia de barrido coordinado mediante canales pares e impares incrementó la cobertura temporal del espectro.

El sistema coordinado redujo la recepción relativa de anuncios BLE respecto de la condición de referencia. La ARR activa global fue de 5,66 %, equivalente a una reducción relativa global de 94,34 % en el conjunto de ensayos. Por distancia, la ARR global fue de 7,20 % a 1 m, 3,31 % a 2 m y 6,47 % a 3 m. Estos resultados corresponden exclusivamente a las condiciones del montaje experimental.

Conclusiones generales

La adaptación del firmware permitió convertir dos dispositivos RF-Clown v2 de funcionamiento único en un sistema coordinado entre el maestro y el esclavo.

La coordinación ESB mantuvo el intercambio funcional de estados entre el Maestro y el Esclavo durante los ensayos. Debido a que no se realizó una medición con osciloscopio o analizador lógico, no se establece un valor propio de latencia paquete a paquete.

La distribución complementaria de canales permitió que el Maestro recorriera los canales impares y el Esclavo los pares, evitando que ambos nodos ejecutaran el mismo conjunto de frecuencias durante la operación coordinada.

Durante la conducción activa, la ARR global fue del 5,66 %, equivalente a una reducción relativa del 94,34 % en los anuncios detectados respecto a la condición de referencia.

Las métricas mostraron variaciones significativas en la distancia evaluada. Aunque la menor ARR global se registró a 2 m, los resultados no permiten establecer una distancia óptima universal.

La arquitectura propuesta funcionó sin aumentar la potencia de transmisión ni incorporar componentes externos.

Los resultados respaldan la hipótesis de las condiciones específicas del montaje experimental, al evidenciar una reducción de la recepción relativa de anuncios BLE durante la operación coordinada.

Este sistema ofrece una plataforma reproducible para la investigación académica en sincronización, sistemas embebidos y comunicaciones inalámbricas en entornos controlados.

Recomendaciones

Validación estadística: Ampliar el tamaño de la muestra y el número de dispositivos para fortalecer la validez de los resultados.

Escenarios de prueba: Evaluar el sistema en entornos con obstáculos bajo diversas condiciones de propagación.

Monitoreo: Incorporar un registro automático de latencia, pérdida de paquetes, distancia y estado de sincronización.

Optimización: Ajustar dinámicamente el tiempo de permanencia en canal según las condiciones del entorno experimental.

Usabilidad: Mejorar la interfaz OLED para configurar los parámetros sin modificar directamente el firmware.

Escalabilidad: Analizar configuraciones de red con tres o más nodos bajo diversas distribuciones espaciales.

Seguridad: Incorporar mecanismos de protección en los paquetes utilizados para la coordinación.

Análisis comparativo: Contrastar el desempeño técnico y la viabilidad económica del sistema frente a otras plataformas de evaluación de radiofrecuencia.

Protocolo de pruebas: Realizar las evaluaciones en entornos controlados, aislados y debidamente autorizados para evitar cualquier interferencia de terceros o de sistemas externos.

Alcance de los resultados: Los hallazgos obtenidos están condicionados por el hardware, las antenas y el escenario experimental específico; por tanto, no deben generalizarse sin una validación adicional en contextos distintos.

5 Bibliografía

[1] N. N. V. Database, «CVE-2023-40129: Android Bluetooth Fluoride Stack Vulnerability / CVE-2025-47370: Qualcomm Bluetooth Connection Request Vulnerability,» 2023/2025. [En línea]. Disponible en: <https://nvd.nist.gov>.

[2]

[3] CiferTech, «Hackaday.io,» 2025. [En línea]. Disponible en: <https://hackaday.io/project/204358-rf-clown-v2-the-wireless-beast-just-got-a-boost/details>.

[4] CiferTech, «Hackster.io,» 2025. [En línea]. Available: <https://www.hackster.io/CiferTech/rf-clown-v2-the-wireless-beast-just-got-a-turbo->

boost-50a319.

- [5] D. Antonioli, «BLUFFS: Bluetooth Forward and Future Secrecy Attacks and Defenses,» in *Proceedings of ACM CCS*, 2025.
- [6] Q. Liu y M. P. Fok, «Microwave Photonic Frequency Hopping Systems for Ultra-Fast Spread Spectrum Communications,» *Journal of Lightwave Technology*, p. 2154–2165, 2025.
- [7] M. K. Hanawal, M. J. Abdel-Rahman y M. Krunz, «Joint Adaptation of Frequency Hopping and Transmission Rate for Anti-Jamming Wireless Systems,» *IEEE Transactions on Mobile Computing*, 2020.
- [8] ARCOTEL, «Plan Nacional de Frecuencias 2021», aprobado mediante Resolución Nro. 04-02-ARCOTEL-2021, 14 de diciembre de 2021, publicado en el Cuarto Suplemento Nro. 4 del Registro Oficial, 16 de febrero de 2022.
- [9] N. Krull, L. Schulthess, M. Magno, L. Benini y C. Leitner, *Wireless Low-Latency Synchronization for Body-Worn Multi-Node Systems in Sports*, 2025.
- [10] J. W. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, Thousand Oaks, CA: SAGE Publications, 2018.
- [11] Bluetooth Special Interest Group, «Bluetooth Core Specification v5.3,» 2021.
- [12] J. Moore, A. S. Abdalla, C. Ueltschey y V. Marojevic, «Soft Tester UE: A Novel Approach for Open RAN Security Testing,» de *IEEE VTC Fall 2024 — RitiRAN Workshop*, 2024.
- [13] N. Semiconductor, «nRF24L01+ Product Specification v1.0,» 2025.

- [14] R. Hernández-Sampieri y C. P. Mendoza, Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta, Ciudad de México: McGraw-Hill Education, 2018.
- [15] F. G. Arias, El proyecto de investigación: Introducción a la metodología científica, Caracas: Editorial Episteme, 2020.
- [16] J. G. & S. M. Proakis, Digital Communications (5th ed.), New York: McGraw-Hill, 2008.
- [17] S. Haykin, A. 2001, T. C. Systems y E. J. W. & Sons., Communication Systems (4th ed.), New York: John Wiley & Sons., 2001.

ANEXO

Anexo 1. Evidencia audiovisual de la coordinación funcional del sistema.

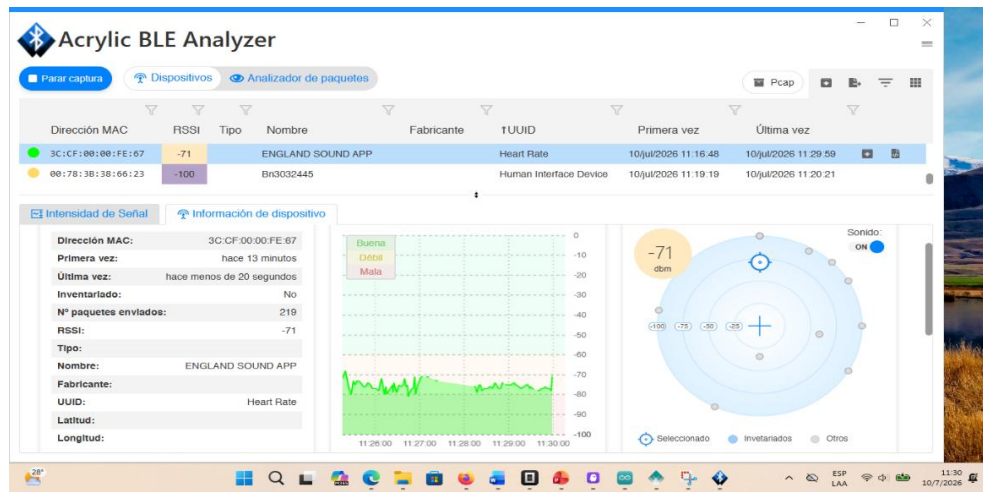
Propósito: documentar la prueba de coordinación.

Contenido: registro audiovisual del ensayo controlado realizado con el dispositivo evaluado.

Enlace web: https://drive.google.com/file/d/1ToknDGdWJEz83zpJeOgsi9L-HkzXI8lx/view?usp=drive_link

Anexo 2. Evidencia audiovisual del ensayo en laboratorio =

https://drive.google.com/file/d/1hdkXDYpGiu9rU550A-leoWKzdfhcr6oP/view?usp=drive_link



Anexo 3. Gráficas de desempeño de la señal en Acrylic Suite



Anexo 4. Capturas instrumentales obtenidas con HackRF One y GNU Radio.



Anexo 5. Prueba de coordinación de interferencia

Acrylic BLE Analyzer

Parar captura | Dispositivos | Analizador de paquetes

Visor de paquetes: OK | Pcap

#	Hora	Dirección MAC	RSSI	Tipo	TNombre
1513	10/jul/2026 11:26:14	3C:CF:00:00:FE:67	-78		ENGLAND SOUND APP
1517	10/jul/2026 11:26:15	3C:CF:00:00:FE:67	-76		ENGLAND SOUND APP
1522	10/jul/2026 11:26:16	3C:CF:00:00:FE:67	-80		ENGLAND SOUND APP
1528	10/jul/2026 11:26:21	3C:CF:00:00:FE:67	-77		ENGLAND SOUND APP
1538	10/jul/2026 11:26:23	3C:CF:00:00:FE:67	-76		ENGLAND SOUND APP
1540	10/jul/2026 11:26:24	3C:CF:00:00:FE:67	-75		ENGLAND SOUND APP
1546	10/jul/2026 11:26:25	3C:CF:00:00:FE:67	-79		ENGLAND SOUND APP
1552	10/jul/2026 11:26:26	3C:CF:00:00:FE:67	-74		ENGLAND SOUND APP
1565	10/jul/2026 11:26:29	3C:CF:00:00:FE:67	-76		ENGLAND SOUND APP
1569	10/jul/2026 11:26:30	3C:CF:00:00:FE:67	-79		ENGLAND SOUND APP

Bluetooth Low Energy Advertisement Packet

Nordic BLE Sniffer: Header

Access Address: 0x8E89BED6

Packet Header (Type: Scannable undirected advertising event - 0x06 - (00000110))

Advertising Address: 3C:CF:00:00:FE:67

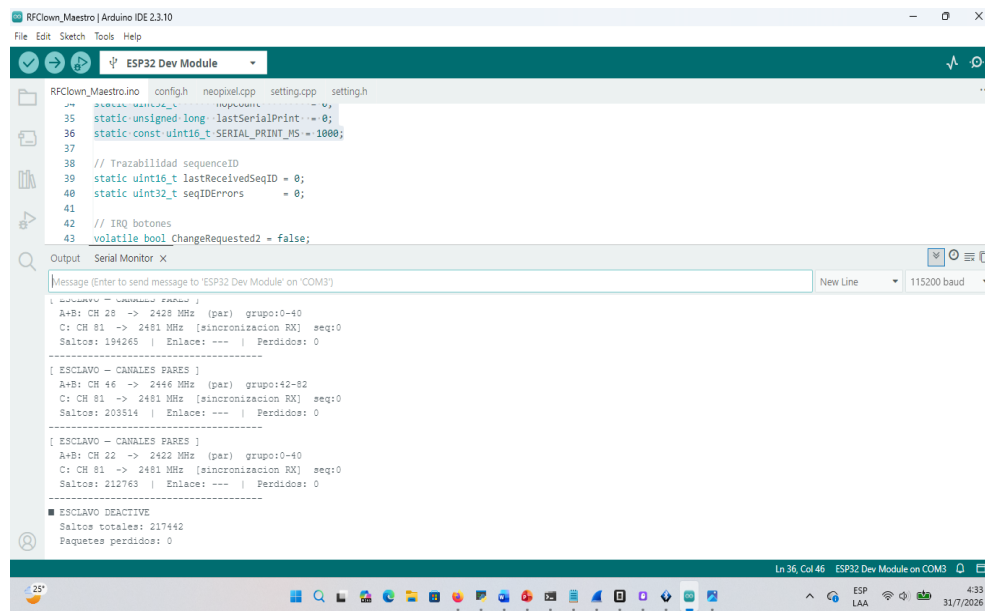
Offset:

Anexo 6. Capturas de anuncios BLE detectados durante las diez repeticiones.

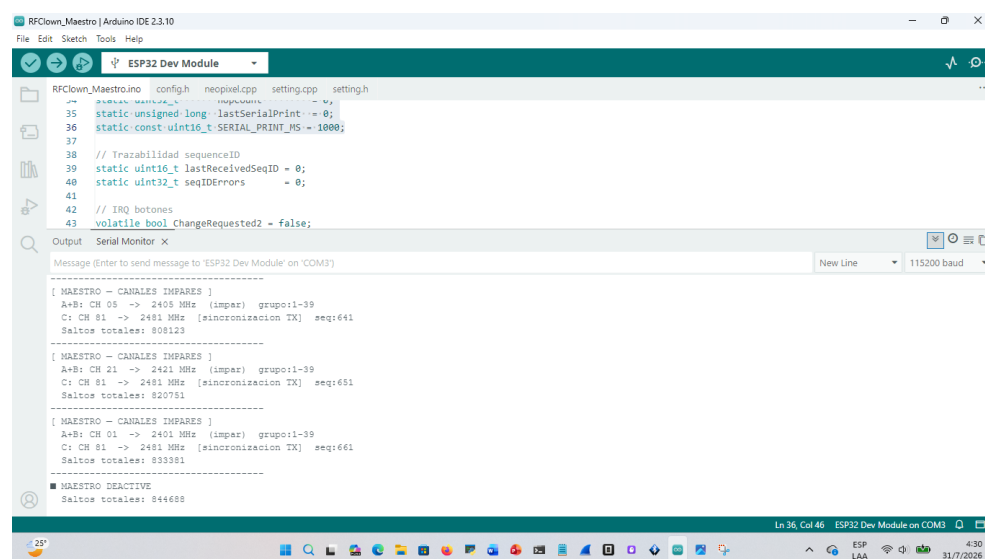
Anexo 7. Capturas y archivos digitales de GNU Radio y Wireshark correspondientes a las pruebas espectrales del Capítulo IV. Descargables para Wireshark en una carpeta llamada

EVIDENCIA PRUEBA DE ESPECTRO:

https://drive.google.com/drive/folders/19FZeIE78CM23pIH0kx4M03dnfx-3Lh5L?usp=drive_link



Anexo 8. Registro del monitor serial del RF-Clown Esclavo durante el barrido de canales pares.



Anexo 9. Monitor Serial donde se observa cómo interfiere canales impares el RF-Clown MAESTRO

config.h

```
/* _____  
  
RF-CLOWN v2.0 — config.h  
  
Pines oficiales CiferTech RF-Clown v2.0  
  
_____ */
```

```
#ifndef CONFIG_H
```

```
#define CONFIG_H
```

```
#define SCREEN_W 128
```

```
#define SCREEN_H 64
```

```
// — Botones —————
```

```
#define PIN_BTN_L 27
```

```
#define PIN_BTN_R 25
```

```
#define PIN_BTN_S 26
```

```
// — Pines nRF24 —————
```

```
#define NRF_CE_PIN_A 5
```

```
#define NRF_CSN_PIN_A 17
```

```
#define NRF_CE_PIN_B 16
```

```
#define NRF_CSN_PIN_B 4
```

```
#define NRF_CE_PIN_C 15
```

```
#define NRF_CSN_PIN_C 2
```

```
// — NeoPixel —————
```

```
#define NEO_PIN 14
```

```

#define NEO_COUNT    1

// ————— Debounce —————

#define debounceDelay  200

// ————— Canal de sincronización MAESTRO↔ESCLAVO —————

#define SYNC_CHANNEL    81

// ————— Intervalos de sync —————

#define HEARTBEAT_MS    100

#define SYNC_TIMEOUT_MS 15000

// ————— Roles —————

#define ROLE_MASTER    0xA1

#define ROLE_SLAVE     0xB2

// ————— Pipes nRF24 para sync —————

#define PIPE_SYNC_TX    0xF0F0F0F0A1ULL

#define PIPE_SYNC_RX    0xF0F0F0F0A1ULL

// ————— Dependencias comunes —————

#include <Arduino.h>

#include <U8g2lib.h>

#include <Wire.h>

#include <SPI.h>

#include <Adafruit_NeoPixel.h>

#include <RF24.h>

#include <nRF24L01.h>

```

```

#include <math.h>

#include <esp_bt.h>

#include <esp_wifi.h>

// — Fuentes —————

static const uint8_t* FONT_SMALL = u8g2_font_5x8_tf;

static const uint8_t* FONT_MEDIUM = u8g2_font_6x12_tf;

// — Canales impares ISM 2.4 GHz — MAESTRO (RadioA + RadioB)

// Canal 81 excluido (sync). Canal 83 incluido.

static const byte masterGroupA[] = {

    1, 3, 5, 7, 9, 11, 13, 15, 17, 19,

    21, 23, 25, 27, 29, 31, 33, 35, 37, 39

};

static const byte masterGroupB[] = {

    41, 43, 45, 47, 49, 51, 53, 55, 57, 59,

    61, 63, 65, 67, 69, 71, 73, 75, 77, 79,

    83

};

// — Canales pares ISM 2.4 GHz — ESCLAVO (RadioA + RadioB)

static const byte slaveGroupA[] = {

    0, 2, 4, 6, 8, 10, 12, 14, 16, 18,

    20, 22, 24, 26, 28, 30, 32, 34, 36, 38,

    40

```

```

};

static const byte slaveGroupB[] = {

    42, 44, 46, 48, 50, 52, 54, 56, 58, 60,

    62, 64, 66, 68, 70, 72, 74, 76, 78, 80,

    82

};

// — Canales por módulo —————

static const byte ble_channels[]      = {2, 26, 80};

static const byte bluetooth_channels[] = {32, 34, 46, 48, 50, 52,

    0, 1, 2, 4, 6, 8,

    22, 24, 26, 28, 30, 74,

    76, 78, 80};

static const byte WiFi_channels[]      = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12};

static const byte usbWireless_channels[] = {40, 50, 60};

static const byte videoTransmitter_channels[] = {70, 75, 80};

static const byte rc_channels[]          = {1, 3, 5, 7};

static const byte zigbee_channels[]       = {11, 15, 20, 25};

static const byte nrf24_channels []       = {76, 78, 79};

#endif // CONFIG_H

```

Anexo 10. Archivo config.h compartido entre los nodos Maestro y Esclavo. El firmware completo se encuentra en la carpeta digital RFCLOWNSV2.0 referida en el Anexo 7.