



UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACSISTEL

INGENIERÍA EN TELECOMUNICACIONES

TRABAJO DE INTEGRACIÓN CURRICULAR

**Caracterización experimental del
dispositivo RF-Clown v2 para la generación
de interferencias controladas en protocolos
ISM 2.4 GHz**

Christian Rolando Galarza Calderón

Dirigido por:

Ing. Luis Miguel Amaya, Mgtr.

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. Daniel Jaramillo Chamba, Mgt.
DOCENTE ESPECIALISTA

Ing. Luis Amaya Fariño, Mgt.
DOCENTE TUTOR GUÍA UIC

Ing. Corina Gonzabay De La A, Mgt.
SECRETARIA



UPSE

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

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y 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 Christian Rolando Galarza Calderón, como requerimiento para la obtención del título de Ingeniero en telecomunicaciones.

La Libertad, a los 04 días del mes de agosto del año 2026

TUTOR

Ing. Luis Miguel Amaya, Mgt.



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

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Christian Rolando Galarza Calderón**

DECLARO QUE:

El trabajo de Titulación, Caracterización experimental del dispositivo RF-Clown v2 para la generación de interferencias controladas en protocolos ISM 2.4 GHz de un previo a la obtención del título en Ingeniero en Telecomunicaciones, ha sido desarrollado respetando derechos intelectuales de terceros conforme 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 Titulación referido.

La Libertad, a los 04 días del mes de agosto del año 2026

EL AUTOR

Christian Rolando Galarza Calderón



UPSE

**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 titulación denominado Caracterización experimental del dispositivo RF-Clown v2 para la generación de interferencias controladas en protocolos ISM 2.4 GHz, presentado por el estudiante, Christian Rolando Galarza Calderón fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 7%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



Certificado de análisis
Completado Magister • UPSE-ECU

trabajo curricular rf clown 1

ID: 1e56fd75810dbbfed011b9ff2db0ce1f5e8da.txt

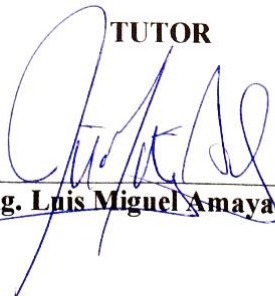
7%

Textos sospechosos

Nombre del fichero: trabajo curricular rf clown 1.txt
Tamaño del archivo original: 32.95 KB
Número de palabras: 21.323

Depositante: AMAYA FARINO LUIS MIGUEL
Fecha de depósito: 20 de agosto de 2020
Tipo de carga: Interferec
fecha de fin de análisis: 20 de agosto de 2020

TUTOR


Ing. Luis Miguel Amaya Mgt.



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

AUTORIZACIÓN

Yo, **Christian Rolando Galarza Calderón**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación 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 04 días del mes de agosto del año 2026

EL AUTOR



Christian Rolando Galarza Calderón

AGRADECIMIENTO

Agradezco a Dios por permitirme culminar esta etapa de mi vida con salud, fortaleza y esperanza.

A la Universidad Estatal Península de Santa Elena y a los docentes que formaron parte de mi preparación profesional, por compartir sus conocimientos y contribuir a mi crecimiento académico.

A mi tutor de tesis, por su orientación y apoyo durante el desarrollo de esta investigación.

A mi esposa y a mis hijos, por convertirse en mi mayor inspiración para seguir adelante y recordarme cada día el verdadero propósito de alcanzar esta meta.

Finalmente, agradezco a todas aquellas personas que, de una u otra manera, aportaron a mi formación y al desarrollo de este trabajo de investigación.

Christian Rolando Galarza Calderón

DEDICATORIA

Dedico este trabajo, en primer lugar, a Dios, por darme la fortaleza, la sabiduría y la perseverancia necesarias para no rendirme, incluso en los momentos más difíciles de mi vida.

A mis tres hijos, quienes son la razón más grande de mi esfuerzo y la motivación que me impulsó a seguir adelante cuando el camino parecía imposible. Cada página de esta tesis representa también el deseo de brindarles un mejor futuro y demostrarles que con esfuerzo, disciplina y constancia los sueños pueden hacerse realidad.

A mi esposa, quien, a pesar de las dificultades propias de la vida, ha permanecido a mi lado durante este proceso. Gracias por acompañarme y por compartir conmigo este importante logro.

Finalmente, dedico este trabajo a mi madre, la persona que desde mis inicios estuvo apoyándome, aunque con su carácter me enseñó a no rendirme y seguir adelante, a pesar de mis dudas y obstáculos que parecían insuperables. Sin embargo, aprendí que la verdadera fortaleza nace de la decisión de no rendirse y de seguir adelante.

Christian Rolando Galarza Calderón

RESUMEN

La presente investigación caracterizó experimentalmente el dispositivo RF-Clown v2 para determinar su comportamiento en la generación de interferencias controladas sobre protocolos de la banda ISM de 2.4 GHz. Se empleó una metodología descriptiva, documental y aplicada, mediante una plataforma basada en ESP32, tres módulos nRF24L01+, pantalla OLED y antenas externas. Las pruebas se realizaron en entorno controlado usando el analizador Narda SRM-3006, el detector Protect 1206i y un multímetro digital. Se validó el funcionamiento sobre Wi-Fi, Bluetooth Classic, BLE, Zigbee, nRF24L01+, Video TX, RC y USB Wireless, analizando firmas espectrales e intensidad de campo. Los resultados confirmaron un funcionamiento estable en todos los modos, con incrementos normales de consumo y temperatura, constituyendo una base experimental para futuras investigaciones.

Palabras claves: RF-Clown v2; interferencia controlada; banda ISM 2.4 GHz; Bluetooth/BLE; caracterización experimental.

ABSTRACT

This research experimentally characterized the RF-Clown v2 device to determine its behavior during the generation of controlled interference on protocols operating in the 2.4 GHz ISM band. A descriptive, documentary, and applied methodology was used, based on an ESP32 platform, three nRF24L01+ modules, an OLED display, and external antennas. Tests were carried out in a controlled environment using the Narda SRM-3006 spectrum analyzer, the Protect 1206i detector, and a digital multimeter. Operation was validated on Wi-Fi, Bluetooth Classic, BLE, Zigbee, nRF24L01+, Video TX, RC, and USB Wireless, analyzing spectral signatures and field intensity. Results confirmed stable operation across all modes, with normal increases in power consumption and temperature, providing an experimental baseline for future research.

Keywords: RF-Clown v2, controlled interference, 2.4 GHz ISM band, Bluetooth/BLE, experimental characterization.

AGRADECIMIENTO.....	7
DEDICATORIA	8
RESUMEN.....	4
ABSTRACT.....	5
1 CAPÍTULO I: PLANTEAMIENTO DE LA INVESTIGACIÓN.....	19
1.1 TÍTULO	19
1.2 ANTECEDENTES.....	20
1.3 DESCRIPCIÓN DEL PROYECTO.....	23
1.4 OBJETIVOS	24
1.4.1 OBJETIVO GENERAL.....	24
1.4.2 OBJETIVOS ESPECÍFICOS.....	25
1.5 JUSTIFICACIÓN.....	25
1.5.1 JUSTIFICACIÓN TÉCNICA	25
1.5.2 JUSTIFICACIÓN EN SEGURIDAD Y CIBERSEGURIDAD	26
1.5.3 JUSTIFICACIÓN ACADÉMICA Y SOCIAL	26
1.6 PLANTEAMIENTO DEL PROBLEMA	28
1.6.1 CONTEXTO DE LA TECNOLOGÍA INALÁMBRICA DE 2.4 GHZ EN ECUADOR	

28

1.6.2	VULNERABILIDADES DE LOS PROTOCOLOS ISM 2.4 GHZ FRENTE A INTERFERENCIAS	29
1.6.3	LIMITACIONES EN EL ACCESO A HERRAMIENTAS DE AUDITORÍA DE RF DE BAJO COSTO	29
1.7	ALCANCE DEL PROYECTO.....	29
1.8	METODOLOGÍA.....	31
1.8.1	INVESTIGACIÓN DESCRIPTIVA.....	31
1.8.2	INVESTIGACIÓN DOCUMENTAL	31
1.8.3	INVESTIGACIÓN APLICADA.....	31
2	CAPÍTULO II: DISPOSITIVOS Y FUNDAMENTOS	34
2.1	MARCO CONTEXTUAL:.....	34
2.1.1	EVOLUCIÓN DE LAS HERRAMIENTAS DE AUDITORÍA DE CÓDIGO ABIERTO	34
2.1.2	EL ECOSISTEMA “OPEN SOURCE” EN LA SEGURIDAD INALÁMBRICA.....	35
2.2	FUNDAMENTOS DE RADIOFRECUENCIA (RF) EN LA BANDA ISM	35
2.2.1	PARÁMETROS DE ANTENA: GANANCIA (DBI), POLARIZACIÓN Y PATRONES DE RADIACIÓN.....	35

2.2.2	EL ESPECTRO RADIOELÉCTRICO Y LA BANDA ISM.....	37
2.3	ESTÁNDARES DE COMUNICACIÓN PROTOCOLOS ISM 2.4 GHZ	37
2.3.1	ZIGBEE (IEEE 802.15.4)	38
2.3.2	ESTÁNDARES IEEE 802.15.1 (BLUETOOTH) Y BLUETOOTH LOW ENERGY (BLE)	38
2.3.3	FUNCIONAMIENTO DE BLUETOOTH Y BLE.....	39
2.3.4	TÉCNICA DE FREQUENCY HOPPING (SALTO DE FRECUENCIA).....	40
2.4	TEORÍA DE LA INTERFERENCIA Y PROPAGACIÓN DE SEÑALES	40
2.4.1	MODELADO DE LA PÉRDIDA DE PROPAGACIÓN (FSPL)	40
2.4.2	PRESUPUESTO DE ENLACE (LINK BUDGET)	40
2.4.3	CAPACIDAD DE CANAL (TEOREMA DE SHANNON-HARTLEY).....	41
2.4.4	PARÁMETROS DE DESEMPEÑO: RSSI, SNR Y PACKET LOSS RATIO	41
2.4.5	RELACIÓN SEÑAL A INTERFERENCIA (S/I O SIR)	41
2.4.6	INTERFERENCIA EN SISTEMAS INALÁMBRICOS	42
2.4.7	INTERFERENCIA CONTROLADA	42
2.4.8	PARÁMETROS DE DESEMPEÑO EN REDES INALÁMBRICAS	42
2.4.9	GENERACIÓN DE INTERFERENCIAS MEDIANTE DISPOSITIVOS ESPECIALIZADOS	43

2.5	TECNOLOGÍAS DE HARDWARE BASE	43
2.5.1	TRANSCEPTOR NRF24L01+ MODO DE OPERACIÓN Y MANIPULACIÓN DE REGISTRO DE RF	43
2.5.2	MICROCONTROLADOR ESP32 (WROOM-32)	44
2.5.3	INTERFAZ DE COMUNICACIÓN SPI (SERIAL PERIPHERAL INTERFACE)	44
2.6	ARQUITECTURA DEL SISTEMA RF-CLOWN V2	44
2.6.1	FUNDAMENTO DE LA CONFIGURACIÓN MULTIMODULAR (TRIPLE NRF24)	45
2.6.2	DIAGRAMA DE FLUJO DE CARACTERIZACIÓN DEL DISPOSITIVO RF-CLOWN V2	48
3	CAPÍTULO III: DESARROLLO DEL PROYECTO	49
3.1	DESARROLLO DE PROPUESTAS TÉCNICAS	49
3.2	EQUIPAMIENTO EXPERIMENTAL	49
3.2.1	PLATAFORMA EXPERIMENTAL (RF-CLOWN V2).....	49
3.2.2	PROVEEDORES Y ADQUISICIÓN.....	54
3.2.3	DISPOSITIVOS OBJETIVO (EVALUADOS)	55
3.2.4	INSTRUMENTOS DE MEDICIÓN Y SOFTWARE	56
3.3	CONEXIONES FÍSICAS DE LOS COMPONENTES EN EL RF-CLOWN	58

3.3.1	ENTRADA USB-SERIAL	58
3.3.2	CONEXIONES FÍSICAS ENTRE EL ESP32 Y LOS MÓDULOS PERIFÉRICOS....	58
3.3.3	DISEÑO DE LA TARJETA DE CIRCUITO IMPRESO (PCB).....	61
3.3.4	PULSADORES DEL SISTEMA.....	62
3.3.5	PULSADORES RESET Y BOOT	63
3.3.6	PUERTOS SMA	64
3.4	MODO DE USO DEL DISPOSITIVO DETECT PROTECT 1206I	64
3.4.1	ENCENDIDO Y CONFIGURACIÓN INICIAL	64
3.5	CONFIGURACIÓN NARDA SRM-3006.....	65
3.5.1	PREPARACIÓN DEL EQUIPO	65
3.5.2	SELECCIÓN DEL RANGO DE FRECUENCIA.....	66
3.6	TABLA COMPARATIVA DE LOS DISPOSITIVOS USADOS.....	67
3.7	IMPLEMENTACIÓN EXPERIMENTAL DEL SISTEMA	68
3.7.1	ESCENARIO DE SIMULACIÓN Y PRUEBAS.....	68
3.7.2	CONFIGURACIÓN INICIAL DEL RF-CLOWN V2	69
3.7.3	PROCEDIMIENTO DE PRUEBAS	72
3.7.4	PROBLEMAS ENCONTRADOS DURANTE LA IMPLEMENTACIÓN	72

3.7.5	INFORME TÉCNICO DETALLADO DE LA CORRECCIÓN.....	73
3.7.6	GUÍA DE OPERACIÓN SEGURA DEL RF-CLOWN V2	77
3.8	PRUEBA DE CONECTIVIDAD.....	79
4	CAPÍTULO IV: EVALUACIÓN DE FACTIBILIDAD TÉCNICA, MITIGACIÓN DE INTERFERENCIAS Y CONCLUSIONES.....	81
4.1	EVALUACIÓN EXPERIMENTAL DEL RF-CLOWN V2 EN EL BLOQUEO DE REDES WI-FI (IEEE 802.11 B/G/N)	81
4.1.1	ANÁLISIS ESPECTRAL CUANTITATIVO (NARDA SRM-3006).....	82
4.2	EVALUACIÓN EXPERIMENTAL DEL RF-CLOWN V2 BAJO EL PROTOCOLO BLUETOOTH CLASSIC (IEEE 802.15.1)	83
4.2.1	ANÁLISIS DE RESPUESTA EN CAMPO CERCANO E IDENTIFICACIÓN DE PROTOCOLO (PROTECT 1206I).....	84
4.2.2	EXTRACCIÓN DE DATOS ESPECTRALES CUANTITATIVOS (NARDA SRM-3006)	85
4.3	EVALUACIÓN EXPERIMENTAL DEL RF-CLOWN V2 BAJO EL PROTOCOLO BLUETOOTH LOW ENERGY (BLE).....	87
4.3.1	ANÁLISIS DE RESPUESTA EN CAMPO CERCANO E IDENTIFICACIÓN DE PROTOCOLO (PROTECT 1206I).....	87
4.3.2	EXTRACCIÓN DE DATOS ESPECTRALES CUANTITATIVOS (NARDA SRM-	

3006)	88
4.4	EVALUACIÓN EXPERIMENTAL DEL RF-CLOWN V2 BAJO EL PROTOCOLO ZIGBEE (IEEE 802.15.4) 90
4.4.1	ANÁLISIS DE RESPUESTA EN CAMPO CERCANO E IDENTIFICACIÓN DE PROTOCOLO (PROTECT 1206I)..... 90
4.4.2	EXTRACCIÓN DE DATOS ESPECTRALES CUANTITATIVOS (NARDA SRM-3006) 91
4.5	EVALUACIÓN EXPERIMENTAL DEL RF-CLOWN V2 BAJO EL MODO NRF24L01+ (PROTOCOLO PROPIETARIO DE 2.4 GHZ)..... 93
4.5.1	ANÁLISIS DE RESPUESTA EN CAMPO CERCANO E IDENTIFICACIÓN DE PROTOCOLO (PROTECT 1206I)..... 93
4.5.2	EXTRACCIÓN DE DATOS ESPECTRALES CUANTITATIVOS (NARDA SRM-3006) 95
4.6	EVALUACIÓN EXPERIMENTAL DEL RF-CLOWN V2 BAJO EL MODO VIDEO TX (TRANSMISIÓN DE VIDEO EN 2.4 GHZ) 96
4.6.1	ANÁLISIS DE RESPUESTA EN CAMPO CERCANO E IDENTIFICACIÓN DE PROTOCOLO (PROTECT 1206I)..... 97
4.6.2	EXTRACCIÓN DE DATOS ESPECTRALES CUANTITATIVOS (NARDA SRM-3006) 98

4.7	EVALUACIÓN EXPERIMENTAL DEL RF-CLOWN V2 BAJO EL MODO RC (SISTEMAS DE RADIOCONTROL EN 2.4 GHZ).....	99
4.7.1	ANÁLISIS DE RESPUESTA EN CAMPO CERCANO E IDENTIFICACIÓN DE PROTOCOLO (PROTECT 1206I).....	99
4.7.2	EXTRACCIÓN DE DATOS ESPECTRALES CUANTITATIVOS (NARDA SRM-3006)	100
4.8	EVALUACIÓN EXPERIMENTAL DEL RF-CLOWN V2 BAJO EL MODO USB WIRELESS (PERIFÉRICOS Y DISPOSITIVOS DE INTERFAZ HUMANA DE 2.4 GHZ)	102
4.8.1	ANÁLISIS DE RESPUESTA EN CAMPO CERCANO E IDENTIFICACIÓN DE PROTOCOLO (PROTECT 1206I).....	102
4.8.2	EXTRACCIÓN DE DATOS ESPECTRALES CUANTITATIVOS (NARDA SRM-3006)	103
4.9	EVALUACIÓN EXPERIMENTAL DEL NARDA SRM-3006 Y EL DETECT PROTECT 1206I.....	105
4.9.1	CORRELACIÓN CUANTITATIVA ENTRE EL NARDA SRM-3006 Y EL DETECT PROTECT 1206I.....	105
4.9.2	DETERMINACIÓN DEL UMBRAL DE DETECCIÓN	107
4.9.3	ANÁLISIS DE SENSIBILIDAD RESPECTO A LA DISTANCIA	108
4.9.4	VERIFICACIÓN EXPERIMENTAL EN BLUETOOTH CLASSIC	109
4.9.5	VERIFICACIÓN EXPERIMENTAL EN BLUETOOTH LOW ENERGY (BLE)	111

4.9.6	COEFICIENTE DE CORRELACIÓN	112
4.10	EVALUACIÓN DEL COMPORTAMIENTO ELÉCTRICO, TÉRMICO Y ESTABILIDAD OPERATIVA.....	116
4.10.1	PROCEDIMIENTO EXPERIMENTAL DE MEDICIÓN	116
4.10.2	EVALUACIÓN DEL CONSUMO ELÉCTRICO	117
4.10.3	EVALUACIÓN TÉRMICA DURANTE ENCENDIDO CONTINUO.....	118
4.10.4	EVALUACIÓN DE ESTABILIDAD OPERATIVA	119
4.10.5	COMPORTAMIENTO TÉRMICO DESPUÉS DE LA DESACTIVACIÓN	121
4.11	EVALUACIÓN DE VIABILIDAD REGULATORIA BAJO LA NORMATIVA DE LA ARCOTEL	122
4.11.1	ESTIMACIÓN DE LA POTENCIA ISOTRÓPICA RADIADA EQUIVALENTE (PIRE)	123
4.12	CONCLUSIONES.....	125
5	BIBLIOGRAFÍAS	126
6	ANEXOS	132

ÍNDICE DE TABLAS

Tabla 1.	Conexiones del dispositivo ESP32 y nRF24L01	59
-----------------	---	----

Tabla 2. Función de botones del dispositivo.....	62
Tabla 3. Descripción y función de los dispositivos utilizados.....	67
Tabla 4. Detalles de librerías necesarias.	73
Tabla 5. Carpetas dentro de la programación	73
Tabla 6. Procedimiento de operación segura	78
Tabla 7. Relación entre distancia, intensidad de campo y nivel de detección	106
Tabla 8. Descripción del umbral de determinación	107
Tabla 9. Variación de la sensibilidad del Protect 1206i con la distancia.....	108
Tabla 10. Valores obtenidos de la medición	109
Tabla 11. Valores obtenidos de los dispositivos.....	111
Tabla 12. Resultado del análisis de correlación entre la intensidad de campo y el nivel de detección	113
Tabla 13. Cálculo de la potencia.....	117
Tabla 14. Evolución de la temperatura superficial del RF-Clown v2 durante el encendido en reposo, sin activar un modo de interferencia.	118
Tabla 15. Comportamiento térmico del RF-Clown v2 durante la operación continua en modo Wi-Fi.....	120
Tabla 16. Registro después de la desactivación.....	122
Tabla 17. Parámetros del sistema de transmisión	124

ÍNDICE DE FIGURAS

Fig. 1 Escenario proyecto RF-Clown v2.....	27
Fig. 2. Primera dimensión elaborada por el autor	32
Fig. 3. Segunda dimensión creada autor	32
Fig. 4. Tercera dimensión creada autor.....	33
Fig. 5. Patrón de radiación [11]	37
Fig. 6. Arquitectura del sistema RF-Clown v2	46
Fig. 7. Diagrama de flujo de la característica descriptiva.....	48
Fig. 8. RF-Clown v2	50
Fig. 9. ESP32 y sus características [25].....	51
Fig. 10. Módulos de RF: 3 transceptores GT-24 (nRF24L01+ PA+LNA) [26].....	52
Fig. 11. Pantalla OLED [19].....	53
Fig. 12. Pulsador	53
Fig. 13. Módulo CP2102.....	54
Fig. 14. Tecno Spark.....	55
Fig. 15 Audífonos para prueba [24].....	56
Fig. 16. Multímetro	56
Fig. 17. Narda SRM-3006.....	57

Fig. 18. Detect Protect 1206i [24].....	58
Fig. 19. USB CP2102.....	58
Fig. 20. Esquemática página oficial [21].	59
Fig. 21. Placa PCB del repositorio.....	61
Fig. 22. Ubicación de pulsadores	62
Fig. 23. Ubicación botones RESET y BOOT	63
Fig. 24. Ubicación puerto SMA.....	64
Fig. 25. Detect Protect 1206i	65
Fig. 26 Narda SRM-3006.....	66
Fig. 27. Selección de frecuencias y ancho de banda.....	67
Fig. 28. Escenario de prueba.....	69
Fig. 29. RF-Clown v2 encendido.....	70
Fig. 30. Se eliminaron las definiciones del display y del NeoPixel.....	74
Fig. 31. Enlaces internos (internal linkage)	75
Fig. 32. Antes de cambiar código original.....	76
Fig. 33. Después de cambiar código se agrega un const.....	76
Fig. 34. Antes de generar cambios.....	76
Fig. 35. Después se agrega un extern.....	76

Fig. 36. Cambios RF Clown unidad de traducción.....	77
Fig. 37. Prueba de conectividad estable mediante ping.....	79
Fig. 38. Prueba de conectividad bajo condiciones de interferencia.....	80
Fig. 39. Prueba de reconexión después de la interrupción.....	80
Fig. 40. RF-Clown v2 energizado frente al Protect 1206i	81
Fig. 41. Pantalla del analizador espectral Narda.....	82
Fig. 42. RF-Clown v2 energizado frente al Protect 1206i	84
Fig. 43. Narda SRM-3006 con los marcadores A y B	86
Fig. 44. BLE operando junto al detector Protect 1206i	88
Fig. 45. Detalle el espectrograma con los marcadores A y B	89
Fig. 46. Funcionando junto al detector Protect 1206i.....	91
Fig. 47. Detalle el espectrograma con los marcadores A y B	92
Fig. 48. Nrf24 operando junto al detector Protect 1206i	94
Fig. 49. Narda SRM-3006 detalle del espectrograma con los marcadores A y B	95
Fig. 50. Video Tx operando junto al Protect 1206i.....	97
Fig. 51. Narda SRM-3006 detalle del espectrograma con los marcadores A y B	98
Fig. 52. Rc operando junto al Protect 1206i	100
Fig. 53. Narda SRM-3006 detalle del espectrograma con los marcadores A y B	101

Fig. 54. USB Wireless operando junto al Protect 1206i	103
Fig. 55. Narda SRM-3006 detalle del espectrograma con los marcadores A y B	104
Fig. 56. Diagrama de dispersión entre la intensidad de campo medida por el Narda SRM-3006 y el nivel de detección registrado por el Detect Protect 1206i	114
Fig. 57. Medición de escenario voltaje	118
Fig. 58. Escenario de medición de temperatura	121
Fig. 59. Colocación de antenas en el Narda	132
Fig. 60. Conexión interferida	132
Fig. 61. Conexión restablecida.....	132
Fig. 64. Señal sin interferencia	133
Fig. 62. Barras de niveles cuando está cerca la señal	133
Fig. 63. Señal con interferencia	133

1 **CAPÍTULO I: PLANTEAMIENTO DE LA INVESTIGACIÓN**

1.1 **TÍTULO**

Caracterización experimental del dispositivo RF-Clown v2 para la generación de

interferencias controladas en protocolos ISM 2.4 GHz

1.2 ANTECEDENTES

Las bandas de frecuencia ISM (Industriales, Científicas y Médicas) fueron definidas originalmente en el año 1947 por la Unión Internacional de Telecomunicaciones (UIT) durante la Conferencia Mundial de Radiocomunicaciones en Atlantic City. El propósito inicial de esta asignación no fue la comunicación de datos, sino reservar porciones específicas del espectro electromagnético para equipos que generaban calor o radiación de radiofrecuencia (RF) para fines industriales (como calentadores dieléctricos), científicos (aceleradores de partículas) y médicos (equipos de diatermia y bisturís eléctricos) [1].

En los últimos años, las tecnologías Bluetooth y Bluetooth Low Energy (BLE) han adquirido gran relevancia en aplicaciones de Internet de las Cosas (IoT), debido a su bajo consumo energético y facilidad de integración. Estas tecnologías operan en la banda ISM de 2.4 GHz, la cual es ampliamente utilizada por diversos sistemas inalámbricos, generando un entorno propenso a interferencias [1].

La coexistencia de múltiples dispositivos en esta banda produce fenómenos de congestión espectral que afectan el rendimiento de las comunicaciones, provocando pérdida de paquetes, aumento de latencia y desconexiones. Por ello, el estudio de interferencias controladas se ha convertido en un área de interés dentro de la ingeniería en telecomunicaciones [2].

Diversos estudios han utilizado dispositivos de radio definida por software como el HackRF One y herramientas especializadas como Ubertooth One para analizar tráfico Bluetooth y evaluar su comportamiento ante interferencias. Sin embargo, estos enfoques suelen centrarse en la captura y análisis de señales, más que en la generación controlada de interferencias

específicas para protocolos BLE [3].

El crecimiento acelerado del Internet de las Cosas (IoT) ha impulsado el desarrollo de múltiples tecnologías inalámbricas de bajo consumo, lo que ha generado un entorno complejo en el espectro ISM de 2.4 GHz, compartido por diferentes protocolos sin licencia. En este contexto, uno de los principales desafíos en el diseño de redes IoT es garantizar la coexistencia eficiente entre dichas tecnologías, evitando interferencias que afecten la calidad de servicio [4].

A finales de la década de 1980, la Comisión Federal de Comunicaciones (FCC) de los EE.UU. abrió estas bandas no licenciadas para el desarrollo de tecnologías de comunicación comercial. La banda ISM de 2.4 GHz (específicamente el rango que va desde los 2400 MHz hasta los 2483.5 MHz) se convirtió rápidamente en el estándar global debido a su disponibilidad internacional unificada y a que sus longitudes de onda permiten el uso de antenas de tamaño reducido, ideales para dispositivos portátiles.

A partir de esta apertura, se desarrollaron e implementaron los protocolos que dominan el entorno inalámbrico actual, regulados principalmente por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE):

- IEEE 802.11 (Wi-Fi): diseñado para redes de área local inalámbricas de alta velocidad.
- IEEE 802.15.1 (Bluetooth): optimizado para redes de área personal de bajo consumo.
- IEEE 802.15.4 (Zigbee / IoT): enfocado en la comunicación de sensores industriales y domótica [6].

La banda ISM de 2.4 GHz constituye una parte esencial del espectro radioeléctrico y se ha consolidado como un pilar de la comunicación inalámbrica moderna. Su uso se ha extendido ampliamente en aplicaciones cotidianas, proporcionando cobertura confiable y conectividad fluida para dispositivos como routers Wi-Fi, sistemas basados en tecnología Bluetooth e incluso equipos domésticos como los hornos microondas [5].

El estudio de esta banda resulta relevante, ya que su funcionamiento impacta directamente en la calidad de las redes inalámbricas y en la experiencia de los usuarios. Comprender sus características y limitaciones permite identificar posibles problemas de interferencia y adoptar mejores decisiones en el diseño y gestión de redes, tanto en entornos domésticos como en oficinas.

La literatura especializada destaca que la banda ISM de 2.4 GHz, al ser compartida por múltiples tecnologías, se convierte en un espacio crítico para analizar fenómenos de coexistencia e interferencia. Este análisis es fundamental para garantizar un desempeño eficiente y estable de los sistemas de comunicación que dependen de ella, lo que la convierte en un tema central dentro de la investigación en telecomunicaciones y en el desarrollo de soluciones para el Internet de las Cosas (IoT).

En el contexto actual, donde la comunicación inalámbrica se ha convertido en un elemento omnipresente, tecnologías como Bluetooth Low Energy (BLE) y Bluetooth clásico representan pilares fundamentales para la conectividad de dispositivos modernos, desde relojes inteligentes hasta auriculares inalámbricos. Sin embargo, la comprensión de sus vulnerabilidades y limitaciones resulta esencial tanto para la comunidad investigadora como para los entusiastas de la electrónica y las telecomunicaciones [6].

En este marco, surge RF-Clown, un inhibidor de BLE de código abierto concebido con fines educativos y de investigación. La motivación principal detrás de este proyecto fue ofrecer una herramienta accesible que ejemplifique la colaboración en entornos de código abierto. A diferencia de otros desarrollos similares que permanecen cerrados y restringidos a un grupo limitado de usuarios, RF-Clown pone a disposición de la comunidad todos sus recursos incluidos el código fuente y los diseños de PCB a través de plataformas como GitHub. Esta apertura garantiza transparencia, fomenta la participación colectiva y facilita la exploración de aspectos técnicos relacionados con la seguridad y la coexistencia de tecnologías inalámbricas [6].

1.3 DESCRIPCIÓN DEL PROYECTO

El documento de investigación se centra en la caracterización experimental del dispositivo RF-Clown v2, una herramienta especializada en la generación de interferencias controladas dentro de la banda ISM de 2.4 GHz, con énfasis en su impacto sobre protocolos inalámbricos Bluetooth y Bluetooth Low Energy (BLE).

La creciente adopción de tecnologías BLE en aplicaciones de Internet de las Cosas (IoT), sistemas embebidos y dispositivos portátiles ha generado un entorno altamente congestionado en la banda de 2.4 GHz, donde múltiples tecnologías coexisten y compiten por el espectro. En este contexto, la interferencia electromagnética representa un factor crítico que puede degradar el rendimiento de las comunicaciones, afectando la confiabilidad, latencia y disponibilidad de los enlaces inalámbricos.

A diferencia de herramientas de radio definida por software como el HackRF One o dispositivos de análisis como el Ubertooth One, el RF-Clown v2 está diseñado específicamente para la generación activa de interferencias controladas, permitiendo reproducir escenarios

experimentales que simulan condiciones adversas en redes Bluetooth y BLE.

El proyecto propone evaluar de manera sistemática las capacidades operativas del dispositivo, incluyendo sus distintos modos de funcionamiento (canales BLE específicos, Bluetooth clásico y modos combinados), así como su alcance efectivo, patrón de cobertura y comportamiento bajo diferentes configuraciones de antena. Adicionalmente, se analizarán parámetros físicos como el consumo energético, la estabilidad operativa y el comportamiento térmico durante sesiones prolongadas de emisión.

La metodología se basa en la realización de pruebas controladas en entornos experimentales, donde se utilizarán dispositivos objetivo compatibles con Bluetooth/BLE para observar la degradación de la conectividad en función de las condiciones impuestas por el RF-Clown v2. Se registrarán métricas como la pérdida de enlace, distancia máxima de interferencia efectiva y estabilidad del sistema, estableciendo así líneas base de rendimiento.

Este estudio busca aportar conocimiento técnico en un área poco explorada en el contexto académico ecuatoriano, donde la disponibilidad de herramientas especializadas es limitada. La caracterización del RF-Clown v2 permitirá comprender mejor los efectos de la interferencia controlada en protocolos inalámbricos, contribuyendo al desarrollo de futuras estrategias de mitigación, análisis de seguridad y optimización de redes en la banda de 2.4 GHz.

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

Caracterizar experimentalmente las capacidades de generación de interferencia del dispositivo RF-Clown v2 sobre protocolos ISM 2.4 GHz, estableciendo líneas base de

rendimiento mediante pruebas controladas utilizando exclusivamente este hardware.

1.4.2 OBJETIVOS ESPECÍFICOS

- Validar el funcionamiento de los modos operativos disponibles en el RF-Clown v2 (Wi-Fi, BLE, Bluetooth Classic, Zigbee, Video Tx, Radiocontrol, USB Wireless y NRF24) mediante pruebas de autoverificación y observación directa de comportamiento en dispositivos objetivo.
- Evaluar la firma espectral y el nivel de detectabilidad del RF-Clown v2 durante la ejecución de técnicas de interferencia en 2.4 GHz, correlacionando los picos de intensidad de campo medidos por el sistema Narda SRM-3006 con el umbral de alerta temprana registrado por el detector de contraespionaje Protect 1206i.
- Documentar el comportamiento térmico, el consumo energético y estabilidad operativa del RF-Clown v2 durante sesiones prolongadas de emisión, utilizando únicamente indicadores integrados y mediciones básicas de voltaje.

1.5 JUSTIFICACIÓN

El estudio de las interferencias en la banda ISM de 2.4 GHz constituye un tema de alta relevancia en el ámbito de las telecomunicaciones, debido a la creciente proliferación de tecnologías inalámbricas como Bluetooth y Bluetooth Low Energy (BLE), ampliamente utilizadas en aplicaciones de Internet de las Cosas (IoT), dispositivos médicos, sistemas embebidos y redes personales. [7]

1.5.1 JUSTIFICACIÓN TÉCNICA

La coexistencia de múltiples tecnologías en esta banda genera un entorno altamente

congestionado, donde las interferencias pueden afectar significativamente el rendimiento de los sistemas de comunicación, provocando pérdida de paquetes, degradación de la calidad del servicio y fallos en la conectividad. En este contexto, resulta fundamental comprender el comportamiento de estos sistemas frente a condiciones adversas controladas. [7]

Si bien existen herramientas de análisis como el HackRF One y el Ubertooth One, estas se enfocan principalmente en la captura y monitoreo de señales, sin ofrecer capacidades especializadas para la generación controlada de interferencias específicas sobre protocolos Bluetooth y BLE. Esto limita la posibilidad de realizar estudios experimentales más precisos orientados a la evaluación del impacto real de la interferencia.

1.5.2 JUSTIFICACIÓN EN SEGURIDAD Y CIBERSEGURIDAD

El dispositivo RF-Clown v2 surge como una alternativa innovadora al permitir la generación activa y controlada de interferencias en la banda de 2.4 GHz, lo que posibilita la recreación de escenarios reales de degradación de señal. Sin embargo, su escasa disponibilidad en el contexto ecuatoriano ha impedido su uso y análisis dentro del ámbito académico, evidenciando una brecha en la investigación experimental en este campo.

1.5.3 JUSTIFICACIÓN ACADÉMICA Y SOCIAL

En este sentido, la presente investigación se justifica en la necesidad de caracterizar experimentalmente el comportamiento del RF-Clown v2, evaluando sus capacidades y limitaciones en la generación de interferencias sobre dispositivos Bluetooth y BLE. Los resultados obtenidos permitirán aportar conocimiento técnico relevante sobre la interacción entre señales en la banda de 2.4 GHz, así como sentar bases para futuras investigaciones orientadas a la mitigación de interferencias, mejora de la robustez de sistemas inalámbricos y análisis de

seguridad en redes de corto alcance.

Este estudio contribuye al fortalecimiento de la investigación aplicada en telecomunicaciones en el Ecuador, promoviendo el uso de herramientas especializadas y el desarrollo de capacidades experimentales en entornos académicos.

Se analizará la cobertura, la respuesta de Narda SRM-3006 y especificaciones técnicas del dispositivo.

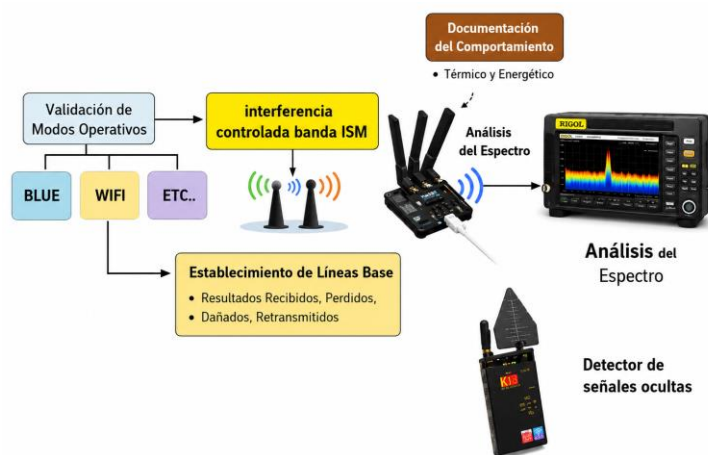


Fig. 1 Escenario proyecto RF-Clown v2

Explicación diagrama topológico del funcionamiento del proyecto.

➤ Validación de modos operativos Se comprueba el funcionamiento del RF-Clown v2 en las modalidades:

- Bluetooth Low Energy (BLE).
- Bluetooth Classic, evaluando su comportamiento frente a interferencias.
- Wi-Fi
- Zigbee

- Video Tx
 - Radiocontrol
 - USB Wireless
 - NRF24
- Generación de interferencias controladas en 2.4 GHz el dispositivo RF-Clown v2 emite señales intencionalmente diseñadas para afectar la comunicación en protocolos ISM, permitiendo medir el impacto en condiciones reproducibles.
 - Documentación del comportamiento térmico y energético se monitorea la estabilidad del dispositivo durante sesiones prolongadas de emisión, evaluando consumo energético y variaciones térmicas.
 - Análisis del espectro (ej. Narda) se observa la distribución de energía en la banda de 2.4 GHz, verificando la forma y alcance de las interferencias generadas.
 - Detector de señales.

1.6 PLANTEAMIENTO DEL PROBLEMA

1.6.1 CONTEXTO DE LA TECNOLOGÍA INALÁMBRICA DE 2.4 GHZ EN ECUADOR

En Ecuador, el uso de la banda ISM (industrial, científico y médico) de 2.4 GHz se ha verificado el crecimiento exponencial en la última década. Este crecimiento no se limita al acceso de internet mediante Wi-Fi, sino que se ha extendido al internet de las cosas (IoT), dispositivos médicos de domótica y periféricos inalámbricos que operan bajo estándares

Bluetooth y BLE. En ciertos puntos de Ecuador como ciudades grandes (Quito, Guayaquil) el espectro radio eléctrico incrementa el riesgo de colisiones de datos y ataques dirigidos [8].

1.6.2 VULNERABILIDADES DE LOS PROTOCOLOS ISM 2.4 GHZ FRENTE A INTERFERENCIAS

Aunque los protocolos que operan en la banda ISM 2.4 GHz implementan mecanismos avanzados como el salto de frecuencia adaptativo para evitar interferencias, su capa física (PHY) sigue siendo vulnerable a ataques de negación de servicios inalámbricos o jamming. El problema se origina cuando un emisor de ruido constante o barrido rápido, como el propuesto en arquitecturas basadas en el chip nRF24L01, puede saturar los canales o bloquear ventanas de recepción de los dispositivos. Esto impide que los dispositivos establezcan o mantengan una conexión estable, dejando vulnerables los sistemas de seguridad. [9]

1.6.3 LIMITACIONES EN EL ACCESO A HERRAMIENTAS DE AUDITORÍA DE RF DE BAJO COSTO

En el mercado ecuatoriano, el acceso a herramientas profesionales de auditoría de radiofrecuencia (como analizadores de espectro en tiempo real o equipos SDR de alta gama) es extremadamente limitado debido a su costo de importación y falta de distribuidores locales especializados. Esta barrera económica genera una brecha en la ciberseguridad local, donde los profesionales académicos no cuentan con dispositivos accesibles para realizar pruebas de penetración o caracterización de señales. El RF-Clown v2 se presenta como una alternativa de hardware abierto y bajo costo que permite demostrar estas pruebas; sin embargo, al ser un dispositivo experimental carece de documentación real en escenarios locales.

1.7 ALCANCE DEL PROYECTO

El presente proyecto tiene como alcance la caracterización experimental del dispositivo RF-Clown v2 en la generación de interferencias controladas sobre protocolos inalámbricos ISM en la banda de 2.4 GHz, mediante la ejecución de pruebas en entornos controlados y utilizando exclusivamente dicho hardware como fuente de interferencia.

La investigación se centrará en la validación de los modos operativos del dispositivo, evaluando su impacto sobre dispositivos comerciales mediante observación directa de la pérdida de conectividad y degradación del enlace.

Asimismo, el estudio abarcará la medición del alcance efectivo de interferencia, considerando variables como la distancia entre el emisor y el dispositivo objetivo, la orientación de las antenas externas y la configuración de operación. Se establecerán métricas como la distancia máxima de pérdida de conexión y la estabilidad del enlace en diferentes escenarios.

Se analizarán parámetros físicos del dispositivo, tales como el consumo energético, el comportamiento térmico y la estabilidad operativa durante sesiones prolongadas de funcionamiento, utilizando mediciones básicas e indicadores integrados del sistema.

El proyecto no contempla el diseño ni modificación del hardware del RF-Clown v2, ni el desarrollo de algoritmos avanzados de mitigación de interferencias. Tampoco incluye la implementación de sistemas complejos de medición espectral o instrumentación de laboratorio de alta precisión, limitándose a un enfoque experimental aplicado con recursos accesibles.

Los resultados obtenidos permitirán establecer una línea base de desempeño del dispositivo en condiciones controladas, aportando información relevante para futuras investigaciones en análisis de interferencias, seguridad inalámbrica y optimización de redes en la banda ISM de 2.4 GHz.

1.8 METODOLOGÍA

1.8.1 INVESTIGACIÓN DESCRIPTIVA

La investigación descriptiva tiene como finalidad caracterizar y detallar el comportamiento de un fenómeno sin modificar sus variables, permitiendo identificar sus propiedades y características principales.

1.8.2 INVESTIGACIÓN DOCUMENTAL

La investigación documental se basa en la recopilación y análisis de información proveniente de fuentes bibliográficas, artículos científicos y documentación técnica, con el fin de sustentar teóricamente el estudio.

1.8.3 INVESTIGACIÓN APLICADA

La investigación es aplicada porque se implementa el RF-Clown v2 para generar conocimiento orientado a la solución de problemas prácticos, mediante la implementación de métodos y herramientas en situaciones reales.

Este apartado se organiza en tres dimensiones para especificar lo realizado.

Primera dimensión: validación de modos operativos

Se verifica el funcionamiento del dispositivo en tres configuraciones de interferencia: en el protocolo ISM. Para cada configuración se evalúa la capacidad del dispositivo para interrumpir el enlace entre nodos de comunicación inalámbrica, confirmando así la operatividad de cada modo mediante un proceso de autovalidación (*Self-Verification*).



Fig. 2. Primera dimensión elaborada por el autor

Segunda dimensión: medición de alcance y cobertura.

Se determina experimentalmente el patrón de radiación del dispositivo y la distancia máxima de interferencia efectiva, entendida como el rango a partir del cual los nodos receptores pierden completamente la conectividad con el nodo transmisor. Este parámetro constituye la



Fig. 3. Segunda dimensión creada autor

línea base de cobertura del sistema.

Tercera dimensión: estabilidad y comportamiento térmico energético.

Se monitorean la temperatura de operación del dispositivo mediante el análisis del perfil térmico parámetros eléctricos expresados en voltios y amperios, a partir de los cuales se calcula la potencia. Estos parámetros permiten evaluar la estabilidad del sistema bajo condiciones de uso prolongado.



Fig. 4. Tercera dimensión creada autor

Como resultado global, el experimento genera una caracterización experimental completa del RF-Clown v2, que sirve como referencia cuantitativa para estudios posteriores de mitigación, detección o análisis de interferencias en redes inalámbricas de corto alcance.

2 CAPÍTULO II: DISPOSITIVOS Y FUNDAMENTOS

2.1 MARCO CONTEXTUAL:

Esta investigación se desarrolla en el contexto de las telecomunicaciones inalámbricas de corto alcance, específicamente en la banda ISM de 2.4 GHz, ampliamente utilizada por tecnologías como Bluetooth y Bluetooth Low Energy (BLE).

En la actualidad, el crecimiento de dispositivos IoT, sistemas embebidos y equipos de comunicación personal ha generado una alta densidad de señales en esta banda, provocando problemas de interferencia que afectan el rendimiento de las comunicaciones inalámbricas.

En el contexto ecuatoriano, el acceso a herramientas especializadas para el análisis y generación de interferencias es limitado, lo que dificulta la realización de estudios experimentales avanzados en entornos académicos.

En este escenario, el uso de dispositivos como el RF-Clown v2 permite abordar el análisis práctico de interferencias en protocolos Bluetooth y BLE, contribuyendo al desarrollo de capacidades experimentales y al fortalecimiento de la investigación aplicada en telecomunicaciones.

2.1.1 EVOLUCIÓN DE LAS HERRAMIENTAS DE AUDITORÍA DE CÓDIGO ABIERTO

Históricamente, la evolución de radiofrecuencia (RF) requiere equipos industriales costosos (como analizadores de protocolos). Sin embargo, con el avance tecnológico surgió el movimiento Open Source Hardware, que impulsó el desarrollo de herramientas más accesibles.

Proyectos como el Rf Clown, realizado para investigaciones de ciberseguridad sobre la

debilidad del chip nRf24L01+ han demostrado en sus estudios sobre la vulnerabilidad en la banda de 2.4 GHz, permitiendo a estudiantes y aficionados a analizar la robustez de protocolos comerciales [10].

2.1.2 EL ECOSISTEMA “OPEN SOURCE” EN LA SEGURIDAD INALÁMBRICA

El acceso al código abierto del RF-Clown v2 no solo implica al código fuente (firmware), sino también a los esquemáticos de hardware. Esto permite la replicabilidad científica, donde el acceso a hardware especializado es limitado, el uso de plataformas basadas en ESP32 y módulos de bajo costo representa una solución eficiente para el fortalecimiento de la ciberseguridad nacional.

2.2 FUNDAMENTOS DE RADIOFRECUENCIA (RF) EN LA BANDA ISM

2.2.1 PARÁMETROS DE ANTENA: GANANCIA (DBI), POLARIZACIÓN Y PATRONES DE RADIACIÓN

Ganancia de antena (dBi): es la capacidad de la antena para dirigir o concentrar la energía de RF en una dirección particular, comparada con un radiador isotrópico (ideal y uniforme en todas direcciones).

Unidad (dBi): decibelios referidos a una antena isotrópica. Un valor dBi más alto significa mayor direccionalidad y un haz más estrecho.

Ganancia vs. dirección: las antenas de baja ganancia (ej. 3 dBi) cubren un área amplia (omnidireccionales), mientras que las de alta ganancia (ej. 10+ dBi) enfocan la señal en un haz estrecho (direccionales).

PIRE (e.i.r.p.): la potencia isotrópica radiada equivalente es la potencia entregada a la

antena multiplicada por su ganancia.

Polarización: describe la orientación física de las ondas electromagnéticas radiadas, específicamente la dirección en la que oscila el campo eléctrico.

Tipos:

Lineal (Vertical/Horizontal): el campo eléctrico oscila en una línea recta.

Circular: el campo eléctrico gira a medida que la onda viaja.

Importancia para una recepción óptima, la antena receptora debe tener la misma polarización que la antena transmisora. Una desalineación puede causar pérdidas significativas de señal.

- Patrones de radiación: representación gráfica de la distribución de la energía electromagnética en el espacio (típicamente en 3D o cortes 2D).
- Lóbulo principal: la dirección de máxima radiación.
- Lóbulos secundarios: radiaciones no deseadas en otras direcciones.
- Ancho de haz a media potencia (HPBW): ángulo entre los puntos donde la radiación cae a la mitad (-3dB) de su máximo, definiendo la direccionalidad.
- Tipos de patrón: omnidireccional (360° en un plano), direccional (enfocado) o sectorial. [11].

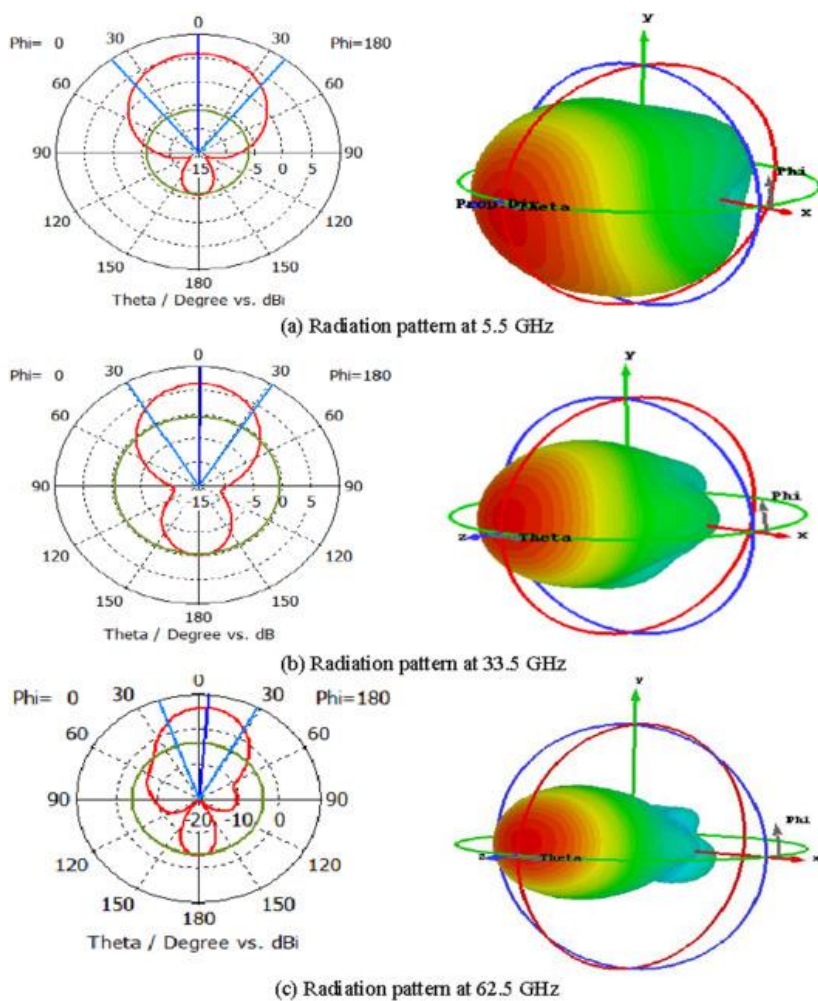


Fig. 5. Patrón de radiación [11]

2.2.2 EL ESPECTRO RADIOELÉCTRICO Y LA BANDA ISM

El espectro radioeléctrico es el medio físico por el cual se propagan las ondas electromagnéticas. La banda de industrial, Scientific, and Medical (ISM) de 2.4 GHz (que va de los 2400 a los 2483,5 MHz) es de uso libre, lo que significa que no requiere licencia para operar. Debido a que es una banda altamente saturada donde coexisten Wi-Fi, Bluetooth, Zigbee y hornos microondas, lo que la hace propensa a interferencias. [12]

2.3 ESTÁNDARES DE COMUNICACIÓN PROTOCOLOS ISM 2.4 GHZ

La banda ISM (Industrial, Scientific and Medical) de 2.4 GHz es un espectro de uso libre a nivel mundial, ideal para redes de corto y medio alcance. Los tres estándares principales que operan en esta frecuencia son

2.3.1 ZIGBEE (IEEE 802.15.4)

Protocolo optimizado para el Internet de las Cosas (IoT) y domótica. Utiliza topología de red en malla (mesh), lo que permite que los dispositivos extiendan el alcance de la red retransmitiendo la señal entre nodos [15].

2.3.2 ESTÁNDARES IEEE 802.15.1 (BLUETOOTH) Y BLUETOOTH LOW ENERGY (BLE)

Bluetooth Classic (IEEE 802.15.1) es una tecnología dedicada a las redes inalámbricas de área personal (WPAN), creada por Special Interest Group. Esta tecnología usa la banda de 2.4 GHz, es utilizada para la conectividad inalámbrica a corto alcance y posibilita a la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia [13].

La tasa de transferencia de datos entre dispositivos Bluetooth es de unos tres megabits por segundo, la cual, en comparación con la tecnología Wi-Fi (IEEE 802.11), es relativamente inferior [14].

BLE (Bluetooth Low Energy) se incluyen en el estándar Bluetooth desde la especificación Bluetooth 4.0 y define dos topologías de red diferentes para transmitir datos: conexión y difusión. Debido a sus características, cada topología es apropiada para determinar casos de uso con diferentes fortalezas y debilidades. Las versiones posteriores de BLE (4.1, 4.2 y 5.0) mantienen estas topologías y las mejoran, permitiendo la combinación de diferentes roles.

Sin embargo, estas últimas versiones mejoradas no se implementan en la mayoría de los dispositivos IoT, razón por la cual si se tiene la intención de trabajar en aplicaciones de tipo IoT es recomendable el uso de dispositivos de tipo BLE 4.0. Las topologías disponibles en el estándar BLE son “Connection topology” y “Broadcast topology”. En la primera topología de conexión dos dispositivos BLE pueden establecer una conexión para intercambiar datos de forma permanente y periódica. Se utilizan dos roles en esta topología: maestro (también llamado central) y esclavo (o periférico). Es posible conectar un dispositivo maestro con hasta 8 dispositivos esclavos en una topología estrella. Esta topología permite el flujo de datos en ambas direcciones. Además, los dispositivos esclavos proporcionan características de notificación e indicación para enviar datos al maestro en el momento en que cambian. La segunda topología es denominada de difusión, un dispositivo BLE puede usar paquetes de publicidad para transmitir datos a cualquier dispositivo BLE en modo de exploración ubicado dentro de su rango de cobertura, en esta topología se definen dos roles: emisor (que transmite datos) y receptor (que recibe datos), debido a la naturaleza de esta topología, el intercambio de datos es unidireccional, desde un emisor hasta uno o más observadores. Recientemente, la topología de “red mesh” se ha incluido en la Especificación de Bluetooth, aunque el número de dispositivos reales que lo implementan es muy limitado [13].

2.3.3 FUNCIONAMIENTO DE BLUETOOTH Y BLE

Bluetooth es una tecnología de comunicación inalámbrica diseñada para el intercambio de datos a corta distancia, utilizando la banda de 2.4 GHz. Su funcionamiento se basa en el uso de múltiples canales de frecuencia y técnicas de acceso al medio que permiten la coexistencia con otros dispositivos.

Por su parte, Bluetooth Low Energy (BLE) es una variante optimizada para el bajo consumo energético, utilizada en aplicaciones como sensores, dispositivos portátiles e Internet de las Cosas (IoT). BLE emplea un esquema de comunicación eficiente que reduce el consumo de energía, manteniendo la capacidad de transmisión de datos en entornos inalámbricos.

2.3.4 TÉCNICA DE FREQUENCY HOPPING (SALTO DE FRECUENCIA)

Tanto Bluetooth como BLE utilizan la técnica de salto de frecuencia (frequency hopping spread spectrum, FHSS), la cual consiste en cambiar continuamente la frecuencia de transmisión entre diferentes canales dentro de la banda de 2.4 GHz.

Este mecanismo permite reducir el impacto de interferencias, ya que evita permanecer en un mismo canal por largos periodos de tiempo. Sin embargo, cuando existe interferencia persistente o localizada en múltiples canales, el rendimiento del sistema puede verse afectado significativamente.

2.4 TEORÍA DE LA INTERFERENCIA Y PROPAGACIÓN DE SEÑALES

2.4.1 MODELADO DE LA PÉRDIDA DE PROPAGACIÓN (FSPL)

$$l = 20 \log_{10}(d) + 20 \log_{10}(f) + 20 \log_{10}\left(\frac{4\pi}{c}\right)$$

d : Distancia entre el RF-Clown y el objetivo (en kilómetros).

f : Frecuencia de operación (2400 MHz).

c : Constante de propagación cuando se usa MHz y km.

2.4.2 PRESUPUESTO DE ENLACE (LINK BUDGET)

Fórmula para ver cuánta potencia realmente sale de la antena.

$$P_{RX} = P_{TX} - L_{cable} - L_{espacio} + G_{RX}$$

La importancia de los 8 dBi de tus antenas y la potencia de los módulos **PA+LNA**.

2.4.3 CAPACIDAD DE CANAL (TEOREMA DE SHANNON-HARTLEY)

$$c = B \log_2 \left(1 + \frac{S}{N + I} \right)$$

Donde I es la interferencia generada por tu RF-Clown. Al aumentar I , la capacidad de transmisión C cae a cero.

2.4.4 PARÁMETROS DE DESEMPEÑO: RSSI, SNR Y PACKET LOSS RATIO

Para medir qué tan bien funciona tu dispositivo, necesitas estos conceptos:

RSSI (Received Signal Strength Indicator): indica la potencia de la señal recibida (en dBm).

SNR (Signal-to-Noise Ratio): relación entre la potencia de la señal y el ruido.

PLR (Packet Loss Ratio): el porcentaje de paquetes perdidos debido a la interferencia.

2.4.5 RELACIÓN SEÑAL A INTERFERENCIA (S/I O SIR)

Determina si el ruido del RF-Clown logra tapar la señal legítima.

$$SIR(dB) = P_{señal}(dBm) - P_{interferencia}(dBm)$$

la potencia del RF-Clown (P_i) debe ser mayor o igual a la señal del dispositivo (P_s) en el receptor.

2.4.6 INTERFERENCIA EN SISTEMAS INALÁMBRICOS

La interferencia electromagnética es uno de los principales factores que afectan la calidad de las comunicaciones inalámbricas. Se produce cuando múltiples señales comparten el mismo espectro y se superponen, generando degradación en la señal útil.

En la banda de 2.4 GHz, la interferencia puede ser causada por la coexistencia de diferentes tecnologías o por la presencia de fuentes externas que emiten señales en las mismas frecuencias. Esto puede provocar pérdida de paquetes, aumento de la latencia y desconexión entre dispositivos.

2.4.7 INTERFERENCIA CONTROLADA

La interferencia controlada consiste en la generación intencional de señales de radiofrecuencia con el objetivo de evaluar el comportamiento de sistemas de comunicación bajo condiciones adversas.

Este tipo de pruebas permite analizar la robustez de los protocolos inalámbricos, identificar vulnerabilidades y medir el impacto real de la interferencia en parámetros como estabilidad del enlace, alcance y calidad de servicio.

2.4.8 PARÁMETROS DE DESEMPEÑO EN REDES INALÁMBRICAS

Para evaluar el impacto de la interferencia en sistemas Bluetooth y BLE, se consideran diversos parámetros de desempeño, entre los cuales destacan:

Latencia: tiempo de transmisión de datos entre dispositivos.

Pérdida de paquetes: datos que no llegan correctamente al receptor.

Throughput: cantidad de datos transmitidos exitosamente.

Relación señal a ruido (SNR): indicador de la calidad de la señal.

Estos parámetros permiten medir de forma objetiva el comportamiento de la comunicación bajo condiciones normales y con interferencia.

2.4.9 GENERACIÓN DE INTERFERENCIAS MEDIANTE DISPOSITIVOS ESPECIALIZADOS

En el análisis experimental de sistemas inalámbricos, el uso de dispositivos especializados permite generar condiciones controladas de interferencia. Herramientas como el HackRF One permiten el análisis del espectro radioeléctrico, mientras que dispositivos diseñados específicamente para la generación de interferencias facilitan la evaluación práctica del comportamiento de protocolos como Bluetooth y BLE.

En este contexto, el dispositivo RF-Clown v2 se emplea como una herramienta para la generación activa de interferencias en la banda de 2.4 GHz, permitiendo estudiar el impacto de estas sobre dispositivos reales en condiciones controladas.

2.5 TECNOLOGÍAS DE HARDWARE BASE

2.5.1 TRANSCEPTOR NRF24L01+ MODO DE OPERACIÓN Y MANIPULACIÓN DE REGISTRO DE RF

El nRF24L01+ es un chip de radio de una sola pieza que opera en la banda ISM de 2.4 GHz, este chip está diseñado para empaquetar datos automáticamente (con preámbulo, dirección y CRC), el RF-Clown lo utiliza para enviar ráfagas constantes de datos basura o portadoras puras, sobrepasando las funciones lógicas estándar para convertirlo en un generador de

interferencia.

Tiene la capacidad de escuchar hasta 6 canales de datos simultáneamente, lo que facilita el escaneo rápido del espectro antes de iniciar una sesión de interferencia, se mantiene operando con un voltaje de 1.9 a 3.6V [6].

2.5.2 MICROCONTROLADOR ESP32 (WROOM-32)

Este microcontrolador actúa como el cerebro de RF-Clown v2, donde le permite gestionar interfaz de usuario (pantallas OLED y botones) mantiene otro núcleo exclusivamente donde dedica la comunicación de alta velocidad con los tres módulos nRF24, también permite gestionar la arquitectura Dual-Core, velocidad de reloj (240MHz) fundamental para el proceso de cambios de HOPS con la rapidez necesaria para ejecutar los cambios de canal programado [6].

2.5.3 INTERFAZ DE COMUNICACIÓN SPI (SERIAL PERIPHERAL INTERFACE)

La comunicación entre el ESP32 y los nRF24L01+ se realiza mediante el bus SPI. En el diseño del RF-Clown v2, se utiliza una configuración de bus compartido:

- Los pines de reloj (SCK), datos de salida (MOSI) y datos de entrada (MISO) son comunes para los tres módulos.
- La individualidad de cada radio se logra mediante pines independientes de chip select (CSN) y chip enable (CE).

La eficiencia de la interferencia depende de la velocidad (frecuencia) a la que el ESP32 puede alternar el pin CSN entre los tres módulos.

2.6 ARQUITECTURA DEL SISTEMA RF-CLOWN V2

2.6.1 FUNDAMENTO DE LA CONFIGURACIÓN MULTIMODULAR (TRIPLE NRF24)

La principal innovación del RF-Clown v2 frente a otros dispositivos de auditoría es la integración de tres transceptores nRF24L01+ gestionados por un único microcontrolador ESP32. Esta configuración no es redundante, sino que responde a una necesidad técnica de densidad espectral:

Saturación del ciclo de trabajo (Duty Cycle): el jamming efectivo requiere que el canal esté ocupado el mayor tiempo posible. Mientras un módulo está procesando una instrucción del ESP32, los otros dos pueden continuar emitiendo ruido, eliminando los "espacios de silencio" que los dispositivos legítimos usarían para transmitir.

Versatilidad de modos: esta arquitectura permite que el RF-Clown v2 opere en modo combinado: por ejemplo, un módulo puede estar haciendo sniffing (escucha) mientras los otros dos generan interferencia en canales específicos.

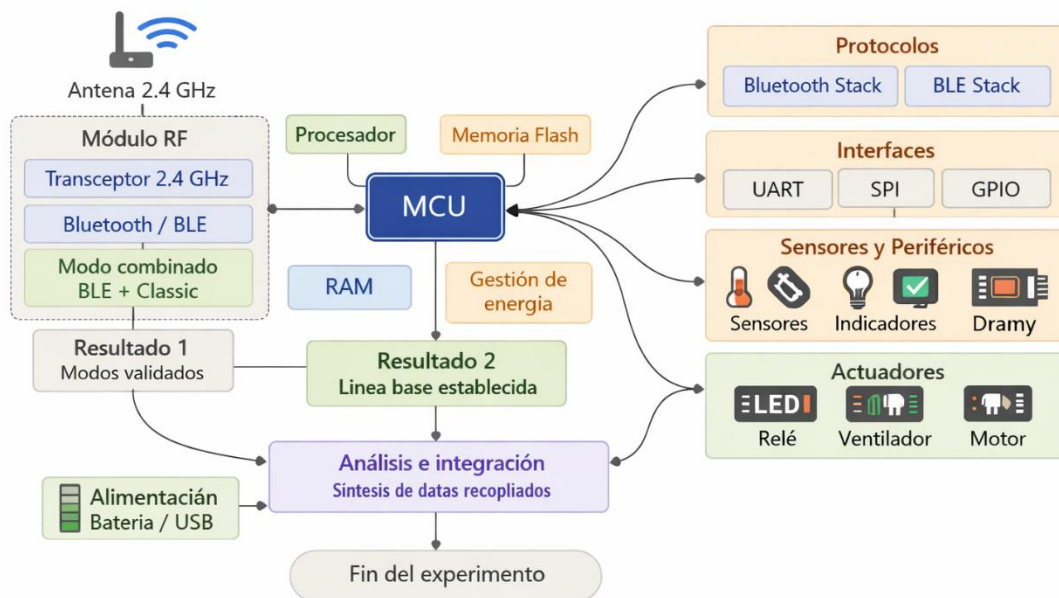


Fig. 6. Arquitectura del sistema RF-Clown v2

Antena 2.4 GHz

Elemento pasivo que acopla la señal electromagnética al aire. Está diseñada para la banda ISM (2.4 - 2.4835 GHz), optimizada para Bluetooth/BLE.

Módulo RF

Transceptor 2.4 GHz: circuito integrado que combina transmisor y receptor, con modulación GFSK típica de Bluetooth.

Bluetooth Classic / BLE dos stacks distintos: Classic para altas tasas de datos, BLE para baja energía.

Modo combinado: habilita la coexistencia de ambos protocolos, generando condiciones de interferencia controlada.

MCU (Microcontrolador)

CPU: ejecuta firmware de control y rutinas de interferencia.

Memoria Flash: almacena el firmware y configuraciones.

RAM: buffer temporal para datos de paquetes interceptados.

Gestión de energía: reguladores DC-DC y control de batería para sesiones prolongadas.

Protocolos

- Bluetooth Stack: capa de enlace L2CAP, RFCOMM, perfiles clásicos.
- BLE Stack: GAP, GATT, ATT, orientado a IoT.

Ambos se implementan en firmware y se exponen al MCU.

Interfaces

- UART/SPI/GPIO: permiten comunicación con PC de control, sensores externos o actuadores.
- LGPIO: líneas de propósito general para activar periféricos.

Sensores y periféricos

- Entradas analógicas/digitales para medir condiciones externas.

Indicadores LED y display para feedback inmediato.

- Actuadores: relé y motores: muestran capacidad de controlar cargas externas, útil en pruebas de respuesta a interferencia.

Bloque de análisis e integración

Procesa métricas: latencia, pérdida de paquetes, throughput.

Sintetiza resultados para documentar el impacto de la interferencia.

2.6.2 DIAGRAMA DE FLUJO DE CARACTERIZACIÓN DEL DISPOSITIVO RF-CLOWN V2

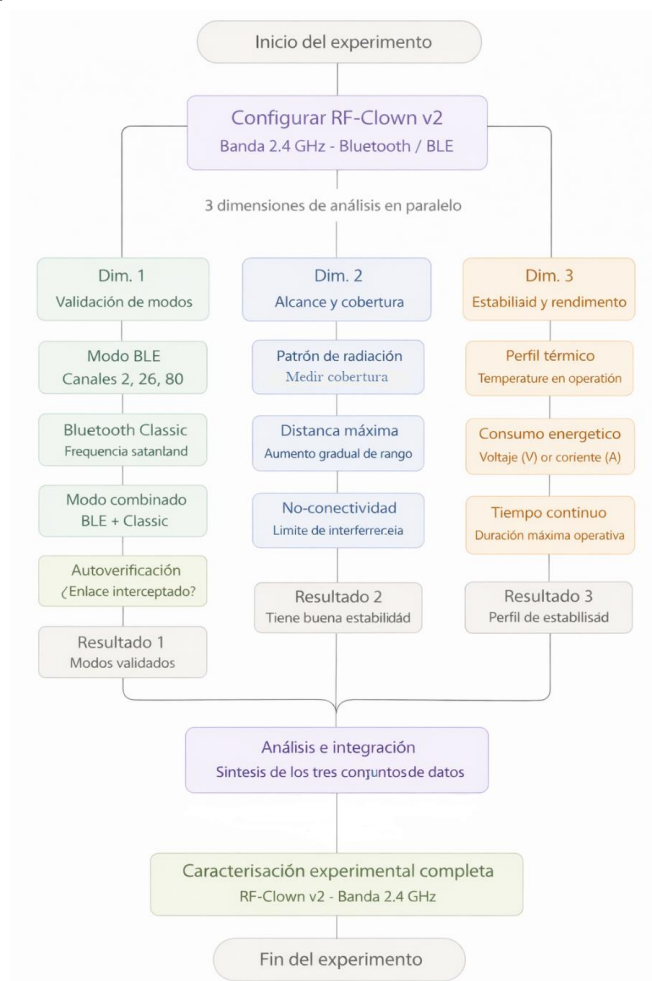


Fig. 7. Diagrama de flujo de la característica descriptiva

En la Fig. 7 representamos la estructura de la documentación para representar cada escenario y explicaciones dadas. Las tres dimensiones corren en paralelo tras la configuración inicial del dispositivo: validación de modos (teal), medición de alcance (azul) y estabilidad térmica-energética (ámbar). Cada una produce su propio resultado parcial, que luego converge en una etapa de análisis integrado para generar la caracterización experimental completa.

3 CAPÍTULO III: DESARROLLO DEL PROYECTO

3.1 DESARROLLO DE PROPUESTAS TÉCNICAS

La presente caracterización del RF-Clown v2 permite estudiar aquí en el Ecuador las vulnerabilidades que existen en las bandas de frecuencias ISM, donde se puede observar que podemos introducir ruidos, con este dispositivo ya que el fabricante indica sobre el tipo de funcionamiento, debido a las restricciones regulatorias aplicables a la generación de interferencias fuera de entornos controlados, las pruebas se realizaron en un ambiente de laboratorio, con el propósito de evitar afectaciones a terceros y garantizar condiciones controladas durante la experimentación.

3.2 EQUIPAMIENTO EXPERIMENTAL

Se detalla el hardware y el software utilizado para la ejecución de las pruebas de caracterización:

3.2.1 PLATAFORMA EXPERIMENTAL (RF-CLOWN V2)

La segunda generación del proyecto RF-Clown, esta versión incluye un rediseño completo del hardware, firmware mejorado y una disposición más modular, diseñada para mejorar el rendimiento, el alcance y control [15] [16].

Como novedades tiene:

- Configuración triple NRF24 (GT24 Mini) para una mayor cobertura de señal y un rendimiento superior.
- Pantalla OLED + 3 botones táctiles para una navegación sencilla en el dispositivo.

- Un único NeoPixel como indicador de estado, sustituye a varios LED.
- Antenas externas de 8 dBi mediante cuatro conectores IPEX.
- Núcleo ESP32-WROOM-32U con soporte BLE/Wi-Fi para futuras expansiones.

Los aspectos destacados

- ❖ Diseño de PCB más limpio y modular
- ❖ Aumento significativo del alcance efectivo
- ❖ Interfaz más fácil de usar y retroalimentación visual.
- ❖ Hardware y firmware totalmente de código abierto



Fig. 8. RF-Clown v2

3.2.1.1 MICROCONTROLADOR ESP32-WROOM-32 DE 30 PINES.

La tarjeta de desarrollo IoT ESP32 DEVKIT V1 - NodeMCU-32 es una herramienta muy potente para el prototipado rápido de proyectos con IoT (Internet de las cosas). Integra en una placa el SoM ESP-WROOM-32 que tiene como base al Soc. ESP32, el conversor USB-serial CP2102 necesario para programar por USB el ESP32, reguladores de voltaje y LED indicadores.

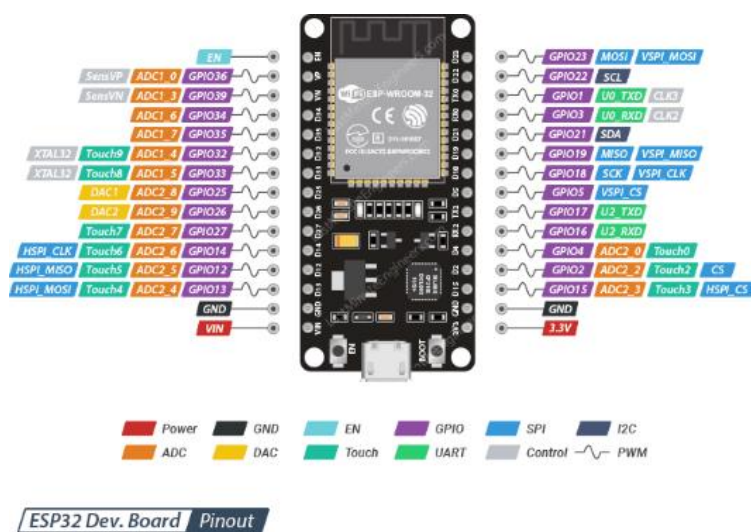


Fig. 9. ESP32 y sus características [25]

La plataforma ESP32 es la evolución del ESP8266 mejorando sus capacidades de comunicación y procesamiento computacional. A nivel de conectividad permite utilizar diversos protocolos de comunicación inalámbrica como: Wi-Fi, Bluetooth y BLE. En cuanto a poder de procesamiento posee un CPU 32bits de dos núcleos de hasta 240 MHz y que se pueden controlar independientemente. Además, incluye internamente una gran cantidad de periféricos para la conexión con: sensores táctiles capacitivos, sensor de efecto Hall, amplificadores de bajo ruido, interfaz para tarjeta SD, Ethernet, SPI de alta velocidad, UART, I2S e I2C. Aplicado en mini servidores web, procesamiento digital, webcams, cámara IP, robótica móvil, domótica y más [17].

3.2.1.2 MÓDULOS DE RF: 3 TRANSCEPTORES GT-24 (NRF24L01+ PA+LNA)

El módulo transceiver RF (emisor y receptor) de 2.4 GHz NRF24L01 fabricado por Nordic semiconductor es ideal para comunicar proyectos de forma inalámbrica, opera en la banda de 2.4 GHz (Industriales, Científicas y Médicas) y posee un consumo ultra bajo (ULP). El chip Nordic nRF24L01+ integra un completo transceiver de 2.4 GHz, sintetizador RF y lógica con el mejorado ShockBurst (acelerador de protocolo por hardware para comunicación por SPI con microcontrolador). Esta versión de módulo posee además un circuito amplificador de potencia (PA), un circuito amplificador de bajo ruido (LNA) además de una antena SMA que le permite lograr un rango de hasta 1000m en campo de vista. Utilizado en aplicaciones de control remoto, supervisión/monitoreo remoto, sistemas de seguridad, red inalámbrica para domótica y automatización industrial.

El módulo posee 8 pines (headers macho) a través de los que se alimenta (3.3V) y se comunica mediante SPI. Debemos tomar en cuenta que la comunicación es de 3.3V (tolerante a 5V) por lo que para trabajar con microcontroladores de 5V (Arduino Uno/Mega/Nano/Micro, PICs) es recomendable utilizar un conversor lógico 5V-3.3V (4CH o 8CH). NRF24L01

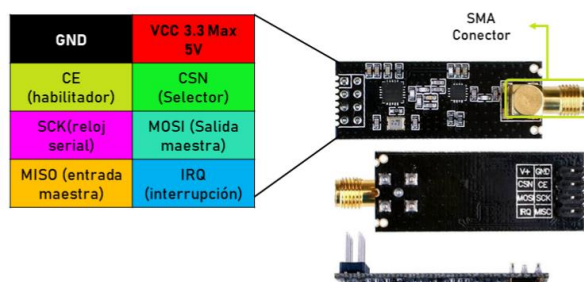


Fig. 10. Módulos de RF: 3 transceptores GT-24 (nRF24L01+ PA+LNA) [26]

directamente con 5V tanto para alimentación como para la comunicación SPI [18].

3.2.1.3 PANTALLA OLED

Las pantallas OLED se destacan por su gran contraste, mínimo consumo de energía y buena calidad de imagen. El display OLED posee una resolución de 128*64 píxeles, permitiendo controlar cada píxel individualmente y mostrar tanto texto como gráficos. La interfaz de comunicación es I2C, lo que le permite trabajar a 5V directamente gracias a su regulador de voltaje en placa, por ende, puede trabajar con sistemas de 3.3V o 5V sin necesidad de conversores externos. El driver que utiliza el módulo es SSD1306, su función es comunicar con el microcontrolador para obtener los datos y enviarlos a la pantalla OLED a través de 4 pines [19].



Fig. 11. Pantalla OLED [19]

3.2.1.4 PULSADORES 2 PATAS

Componente electrónico que cierra un circuito solo mientras se mantiene presionado



Fig. 12. Pulsador

3.2.1.5 CP2102

Chip conversor que actúa como puente entre un puerto USB y la interfaz serie UART (o TTL).

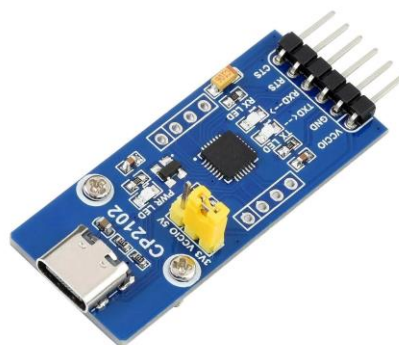


Fig. 13. Módulo CP2102

3.2.2 PROVEEDORES Y ADQUISICIÓN

El dispositivo de interferencia RF-Clown v2 utilizado en el presente documento fue adquirido mediante una tienda en línea (AliExpress), donde se encontró a varios proveedores donde se pudo contactar con (Geek Tech Studio Store) que se especializa en dispositivos electrónicos y herramientas de investigación para comunicaciones inalámbricas. Desde ahí se esperó alrededor de 10 días para que llegue a los EE.UU. desde China y pase por aduana para llegar al casillero contratado, se notificó en la plataforma del casillero y pagar los gastos de aduana. Se canceló tasas por costos de importación, desde ahí se esperó unos 20 días más, para luego tener el producto en nuestras manos alrededor de 35 días se demoró por eventos festivos en nuestra localidad.

La selección de este equipo se consideró la falta de documentación y compatibilidad con

los protocolos ISM. El dispositivo fue obtenido como una plataforma preconfigurada, permitiendo su utilización directa en pruebas experimentales relacionadas con la generación de interferencia en la banda de 2.4 GHz. Adicional, también se utiliza accesorios complementarios como cables USB, baterías recargables y dispositivos para la ejecución de las pruebas de validación y caracterización.

La adquisición del dispositivo RF-Clown v2 permitió reducir tiempo de ensamblaje y enfocar el desarrollo experimental en la evaluación del comportamiento operativo, alcance efectivo y estabilidad funcional del sistema bajo diferentes configuraciones de pruebas.

3.2.3 DISPOSITIVOS OBJETIVO (EVALUADOS)

Para validar la efectividad de la interferencia en condiciones reales, se seleccionaron los siguientes dispositivos:

Smartphone: [Tecno Spark 40 pro +] con Bluetooth 5.0 y 2.4 GHz para el monitoreo de canales BLE.



Fig. 14. Tecno Spark

Periférico de audio: audífonos inalámbricos para pruebas de Bluetooth Classic.

Dispositivo IoT: para pruebas de reconexión y pérdida de paquetes.



Fig. 15 Audífonos para prueba [24]

3.2.4 INSTRUMENTOS DE MEDICIÓN Y SOFTWARE.

3.2.4.1 MULTÍMETRO DIGITAL:

Para la medición de consumo de corriente y niveles de voltaje.



Fig. 16. Multímetro

3.2.4.2 NARDA SRM-3006

Medición de campos electromagnéticos con selección de frecuencia hasta 29.5 GHz, diseñado para medir y evaluar la intensidad de los campos electromagnéticos en el medio ambiente.

Equipos de medición selectiva de campos electromagnéticos (CEM) para demostrar la seguridad y la compatibilidad ambiental. Estos dispositivos analizan con precisión los rangos de frecuencia individuales y los niveles de exposición al campo, incluso a nivel de un solo canal de comunicación. Además, calculan la suma y comparan los niveles con los valores límite vigentes. Con el medidor de CEM SRM 3006, puede comprobar de forma rápida, sencilla y detallada el rango de estos valores de radiación y su origen [20].



Fig. 17. Narda SRM-3006

3.2.4.3 DETECT PROTECT 1206I

El Protect 1206i es un equipo que cumple la función de identificar señales ocultas y proteger los sistemas de vigilancia, este dispositivo tiene la capacidad de detectar señales que emplean protocolos de Bluetooth y Wi-Fi a largas distancias, a diferencia de algunos equipos se les dificulta obtener las señales debido a su baja potencia de emisión y al tipo de modulación que se utilice, el dispositivo cuenta con antenas que operan a frecuencias de 2.4 y 5 GHz lo que facilita detectar y localizar estas señales con una gran precisión dentro del rango de fabricación.



Fig. 18. Detect Protect 1206i [24]

3.3 CONEXIONES FÍSICAS DE LOS COMPONENTES EN EL RF-CLOWN

3.3.1 ENTRADA USB-SERIAL

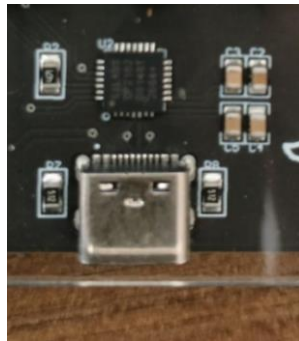


Fig. 19. USB CP2102

El módulo CP2102 se utiliza para la programación y comunicación serial entre el computador y el ESP32. La alimentación principal del sistema proviene del puerto USB-C o de la batería de litio, cuya carga es gestionada por el TP4056. Posteriormente, el regulador LF33 reduce el voltaje a 3.3 V para alimentar los módulos electrónicos del RF-Clown.

3.3.2 CONEXIONES FÍSICAS ENTRE EL ESP32 Y LOS MÓDULOS PERIFÉRICOS

Para poder explicar esta parte se tomó como referencia el diagrama esquemático disponible en el repositorio de la página oficial [6]. Donde se explica y se detalla cómo se conecta cada punto del circuito.

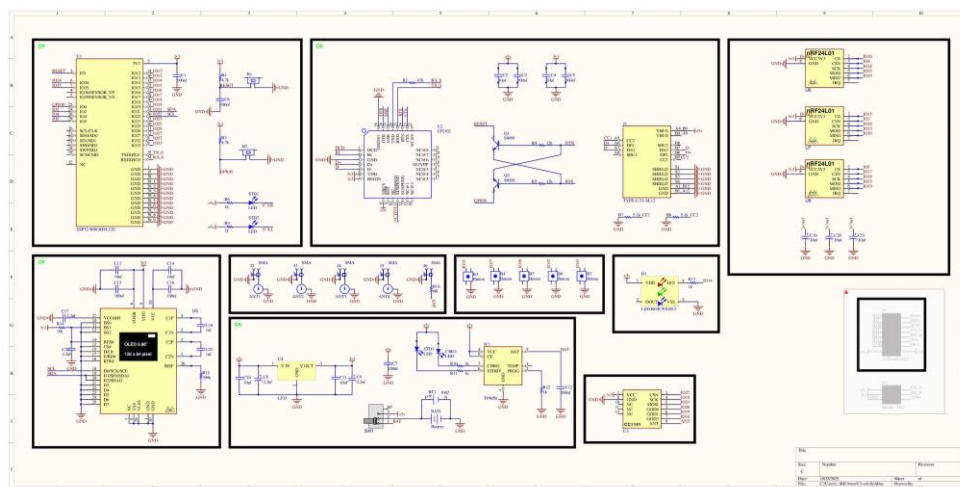


Fig. 20. Esquemática página oficial [21].

Tabla 1. Conexiones del dispositivo ESP32 y nRF24L01

Dispositivo	Señal	GPIO ESP32
nRF24L01 #1	CE	GPIO6
nRF24L01 #1	CSN	GPIO5
nRF24L01 #1	SCK	GPIO18
nRF24L01 #1	MOSI	GPIO23
nRF24L01 #1	MISO	GPIO19
nRF24L01 #2	CE	GPIO4
nRF24L01 #2	CSN	GPIO15
nRF24L01 #2	SCK	GPIO18

nRF24L01 #2	MOSI	GPIO23
nRF24L01 #2	MISO	GPIO19
nRF24L01 #3	CE	GPIO17
nRF24L01 #3	CSN	GPIO16
nRF24L01 #3	SCK	GPIO18
nRF24L01 #3	MOSI	GPIO23
nRF24L01 #3	MISO	GPIO19
CC1101	CSN	GPIO27
CC1101	SCK	GPIO18
CC1101	MOSI	GPIO23
CC1101	MISO	GPIO19
CC1101	GDO0	GPIO26
CC1101	GDO2	GPIO14
OLED SSD1306	SDA	GPIO21
OLED SSD1306	SCL	GPIO22
LED Estado 1	LED	GPIO0
LED Estado 2	LED	GPIO2
Botón BTN1	Entrada	GPIO32
Botón BTN2	Entrada	GPIO33

Botón BTN3	Entrada	GPIO25
------------	---------	--------

En la **tabla 1**, el RF-Clown v2 utiliza un microcontrolador ESP32-WROOM-32E como unidad principal de procesamiento, encargado de controlar los módulos de radio, la pantalla OLED y los botones de navegación. Los dispositivos de comunicación inalámbrica están conectados mediante el bus SPI, compartiendo las líneas SCK (GPIO18), MOSI (GPIO23) y MISO (GPIO19), mientras que cada módulo dispone de pines de selección independientes para permitir su operación individual.

Los tres módulos nRF24L01 se conectan al ESP32 mediante señales CE y CSN dedicadas, y operan en la banda de 2.4 GHz a través de las antenas ANT2, ANT3 y ANT4. Por su parte, el módulo CC1101, conectado a la antena ANT5, utiliza el mismo bus SPI y señales adicionales (GDO0 y GDO2) para la transmisión y recepción de datos en bandas sub-GHz.

3.3.3 DISEÑO DE LA TARJETA DE CIRCUITO IMPRESO (PCB)

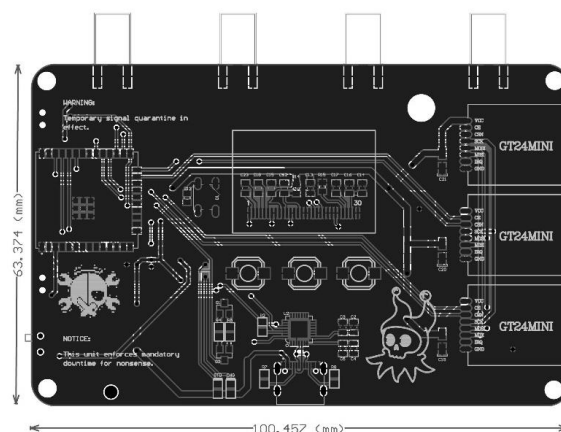


Fig. 21. Placa PCB del repositorio

La tarjeta de circuito impreso (PCB) fue diseñada para integrar los componentes electrónicos del sistema RF-Clown. La placa tiene unas dimensiones aproximadas de 100.46 mm × 63.37 mm y fue diseñada para alojar el microcontrolador ESP32-WROOM-32U, tres módulos

transceptores nRF24L01+, una pantalla OLED de 0.96 pulgadas, pulsadores de control, un LED RGB y el circuito de gestión de energía.

La distribución de los componentes se realizó para optimizar el espacio disponible y reducir la longitud de las pistas de comunicación entre dispositivos. Los módulos nRF24L01+ se ubicaron en el lateral derecho de la placa para facilitar la conexión de las antenas externas mediante conectores SMA, mientras que el ESP32 se localiza en el lateral izquierdo, actuando como unidad central de procesamiento.

Además, para finalizar se eliminan los cables externos, lo que mejora la presentación del prototipo.

3.3.4 PULSADORES DEL SISTEMA

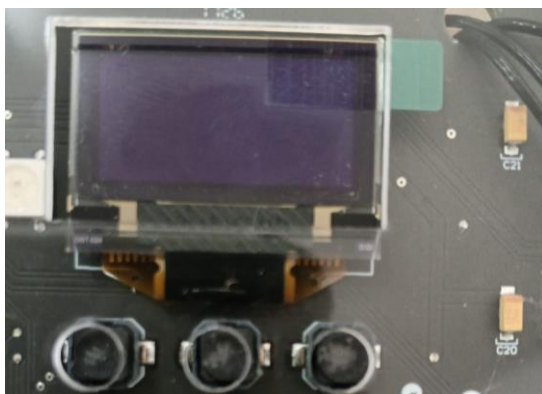


Fig. 22. Ubicación de pulsadores

En este apartado se describe el funcionamiento de los tres pulsadores del dispositivo RF-Clown v2. Cada pulsador dispone de dos terminales y permite ejecutar las funciones que se describen a continuación.

Tabla 2. *Función de botones del dispositivo*

Botón	Función
-------	---------

RIGHT	Navegación hacia derecha
LEFT	Navegación hacia izquierda
MEDIO	Confirmación o selección

3.3.5 PULSADORES RESET Y BOOT

Los pulsadores RESET y BOOT fueron ubicados en los laterales de la tarjeta para facilitar el acceso del usuario sin interferir con los demás componentes electrónicos. Esta disposición permite realizar tareas de programación, reinicio y recuperación del sistema de forma rápida y cómoda, especialmente cuando la placa se encuentra instalada dentro de una carcasa.



Fig. 23. Ubicación botones RESET y BOOT

Botón RESET

El botón RESET (ARRIBA) está conectado al pin EN (Enable) del ESP32 y permite reiniciar el microcontrolador sin desconectar la alimentación del sistema. Se utiliza cuando es necesario reiniciar la ejecución del programa o recuperar el funcionamiento normal del dispositivo.

Botón BOOT

El botón BOOT (ABAJO) está conectado al GPIO0 del ESP32 y se emplea para ingresar al modo de programación (Bootloader). Durante la carga de firmware, este botón permite que el microcontrolador acepte un nuevo programa desde la computadora a través del convertidor USB-UART CP2102.

3.3.6 PUERTOS SMA



Fig. 24. Ubicación puerto SMA

Los 4 conectores que se encuentran en la parte superior del RF-Clown v2 son una parte importante en el diseño del prototipo ya que ayuda a conectar las antenas del módulo de radiofrecuencia.

3.4 MODO DE USO DEL DISPOSITIVO DETECT PROTECT 1206I

3.4.1 ENCENDIDO Y CONFIGURACIÓN INICIAL

El equipo cuenta con dos canales independientes.

- Conecta la antena de varilla estándar a la conexión de antena 1.
- Conecta la antena de microondas Micropointer a la conexión de antena 2
(destinada a señales Bluetooth, Wi-Fi y cámaras inalámbricas)



Fig. 25. Detect Protect 1206i

El Protect 1206i se utilizó como detector indicativo para registrar la respuesta de sus indicadores ante las emisiones presentes durante las pruebas. La activación del indicador del Protect 1206i confirma únicamente que el detector registró una emisión compatible con sus criterios internos de clasificación. Por tanto, esta respuesta no identifica de manera concluyente el protocolo emitido ni demuestra por sí sola la efectividad de la interferencia. La caracterización cuantitativa se realizó mediante el Narda SRM-3006 y la afectación del enlace se comprobó mediante las pruebas funcionales de conectividad.

3.5 CONFIGURACIÓN NARDA SRM-3006

3.5.1 PREPARACIÓN DEL EQUIPO

Antes de iniciar el análisis, es indispensable preparar adecuadamente el equipo, verificando que se encuentre en correcto estado de funcionamiento y que disponga de suficiente carga para realizar las mediciones. Además, se debe instalar y ajustar correctamente la antena antes de encender el equipo. Una vez encendido, se espera unos minutos hasta que el sistema se

inicialice por completo. Posteriormente, se selecciona la opción (Spectrum) para visualizar el espectro de frecuencia.



Fig. 26 Narda SRM-3006

3.5.2 SELECCIÓN DEL RANGO DE FRECUENCIA

Antes de iniciar el análisis, es necesario configurar el rango de frecuencia de trabajo. Para ello, se establecen las frecuencias mínima y máxima correspondientes a la banda ISM de 2.4 GHz.

Frecuencia mínima: 2.3 GHz

Frecuencia máxima: 2.5 GHz

Para configurar los parámetros de resolución del equipo, se selecciona un ancho de banda de resolución (RBW) de 1 MHz, ajustando posteriormente el canal correspondiente a la tecnología Bluetooth para facilitar la visualización de los cambios en frecuencia.



Fig. 27. Selección de frecuencias y ancho de banda

3.6 TABLA COMPARATIVA DE LOS DISPOSITIVOS USADOS

Tabla 3. Descripción y función de los dispositivos utilizados

Equipo	Función	Aplicación en la investigación
RF-Clown v2	Dispositivo basado en ESP32 y módulos nRF24L01+ que genera señales de radiofrecuencia en la banda ISM de 2.4 GHz.	Su uso fue para generar la señal de interferencia (jamming) sobre dispositivos Bluetooth durante las pruebas experimentales.
Protect 1206i	Detector portátil de radiofrecuencia diseñado para identificar señales analógicas y digitales, especialmente Bluetooth y Wi-Fi en 2.4 GHz y 5 GHz, mediante un canal de alta sensibilidad. (D.A.S.)	Se empleó para verificar la presencia de emisiones de radiofrecuencia generadas por el RF-Clown v2 y confirmar que el equipo transmitía en la banda de 2.4 GHz antes y durante las pruebas.
Narda SRM-3006	Analizador selectivo de campos electromagnéticos (EMF) que mide intensidad de campo, densidad de potencia y espectro de frecuencia, identificando las contribuciones de cada servicio de radiocomunicaciones. Opera desde 9 kHz hasta 6 GHz, con opción de	Se necesita para medir cuantitativamente el nivel de radiación electromagnética emitida por el RF-Clown v2, analizar el espectro de frecuencias utilizado durante la interferencia y registrar los niveles de campo eléctrico

ampliación hasta 29.5 GHz.	presentes en el entorno de prueba.
----------------------------	------------------------------------

El RF-Clown es el encargado de generar la señal de interferencia en la banda de 2.4 GHz. El Protect 1206i se utiliza como un detector rápido para verificar la presencia de emisiones de radiofrecuencia y comprobando el funcionamiento del sistema. El Narda SRM 3006 actúa como un instrumento principal de medición, permitiendo caracterizar el espectro de frecuencia y cuantificar la intensidad del campo electromagnético generado durante las pruebas necesarias, proporcionando resultados con precisión metrológica.

3.7 IMPLEMENTACIÓN EXPERIMENTAL DEL SISTEMA

La implementación experimental del sistema se desarrolló utilizando el dispositivo RF-Clown v2 como unidad principal para la generación de interferencias controladas sobre protocolos de la banda ISM de 2.4 GHz. Durante esta etapa se realizó el análisis de su estructura, la verificación de sus condiciones de alimentación, la validación operativa y la ejecución de pruebas controladas para analizar el comportamiento del dispositivo bajo diferentes condiciones de funcionamiento.

Las pruebas experimentales fueron ejecutadas en entornos controlados, utilizando dispositivos móviles y periféricos inalámbricos como objetivos de evaluación, con el propósito de verificar el desempeño operativo del sistema y registrar parámetros relacionados con estabilidad, alcance y comportamiento funcional.

3.7.1 ESCENARIO DE SIMULACIÓN Y PRUEBAS

Se utilizó como escenario de simulación de prueba el laboratorio de telecomunicaciones

este espacio fue elegido con el fin de analizar la interferencia en el lugar ya que mantiene conexiones con protocolos ISM. En este escenario se activó el RF-Clown v2, para poder ver su interferencia en los diferentes protocolos ISM 2.4 GHz. Se coloca el RF-Clown v2 en un lugar específico para verificar con los dispositivos Narda SRM 3006 para ver la radiación de espectro y Protect 1206i para encontrar la señal de interferencia del RF-Clown v2.



Fig. 28. Escenario de prueba

3.7.2 CONFIGURACIÓN INICIAL DEL RF-CLOWN V2

En esta etapa se verificó el correcto funcionamiento del dispositivo RF-Clown v2 antes de ejecutar las pruebas de caracterización.



Fig. 29. RF-Clown v2 encendido

Para iniciar, se realizó la conexión del equipo mediante la interfaz USB para verificar el encendido correcto de la pantalla OLED integrada y la detección adecuada de los módulos NRF24L01 + PA/LNA con antenas externas. Posteriormente, se comprobó el acceso a los diferentes modos operativos disponibles dentro del firmware del dispositivo.

La configuración experimental incluyó la selección de canales BLE específicos, modos de operación Bluetooth Classic y configuraciones combinadas de interferencia, permitiendo evaluar diferentes escenarios de emisión sobre la banda de 2.4 GHz.

3.7.2.1 WI-FI

Operan entre los canales 1 al 12 (los que usan routers/dispositivos Wi-Fi de 2.4 GHz). Sirve para interferir/saturar comunicaciones Wi-Fi cercanas.

3.7.2.2 VIDEO TX

Canales típicos usados por transmisores de video analógico/FPV (los que llevan drones

de carreras, cámaras inalámbricas). Interfiere la señal de video.

3.7.2.3 RC (RADIOCONTROL)

Canales usados por controles remotos (drones, autos RC, juguetes con radiofrecuencia 2.4 GHz). Permite evaluar la comunicación entre un sistema de control remoto y su receptor bajo condiciones controladas de interferencia.

3.7.2.4 BLE (BLUETOOTH LOW ENERGY)

Corresponde a los tres canales de advertising de BLE (37, 38 y 39, según la numeración estándar de Bluetooth). Estos canales permiten evaluar el comportamiento de dispositivos BLE, como relojes inteligentes, audífonos, beacons y sensores IoT, ante condiciones controladas de interferencia.

3.7.2.5 BLUETOOTH (CLASSIC)

Set mucho más amplio de canales, cubriendo el espectro de salto de frecuencia (FHSS) que usa Bluetooth Classic (audífonos clásicos, mouse/teclado Bluetooth no-BLE, manos libres de carro, etc.).

3.7.2.6 USB WIRELESS

Canales usados por dongles inalámbricos USB 2.4 GHz (mouse y teclados inalámbricos tipo Logitech Unifying, presentadores láser, etc.).

3.7.2.7 ZIGBEE

Canales del protocolo Zigbee (usado en domótica: focos inteligentes, sensores, cerraduras, hubs como los de Philips Hue, SmartThings, etc.).

3.7.2.8 NRF24

Canales propios del protocolo nativo nRF24L01 (usado en proyectos DIY de Arduino, algunos drones económicos, joysticks caseros, etc.).

3.7.3 PROCEDIMIENTO DE PRUEBAS

Las pruebas experimentales fueron desarrolladas de manera progresiva con el objetivo de validar el comportamiento operativo del RF-Clown v2 bajo diferentes configuraciones de funcionamiento.

En una primera etapa se ejecutaron pruebas de autoverificación para comprobar la activación correcta de los modos BLE channels, Bluetooth Classic y modo combinado. Para ello, se utilizaron dispositivos móviles y periféricos inalámbricos como objetivos de observación, registrando pérdidas de conectividad, interrupciones temporales y variaciones en la estabilidad de comunicación.

Además, se realizaron pruebas de alcance efectivo variando la orientación de las antenas externas y la distancia entre el dispositivo emisor y los equipos objetivo. Durante estas pruebas se registró la distancia máxima en la cual se observó pérdida parcial o total de conectividad inalámbrica.

3.7.4 PROBLEMAS ENCONTRADOS DURANTE LA IMPLEMENTACIÓN

Luego de ver que el dispositivo RF-Clown v2 encendió sin problemas y al comenzar a visualizar sus respectivos funcionamientos, se tomó la decisión de borrar el código, para verificar si el que está en el repositorio servía tal y como indica su fabricante se siguieron los pasos indicados, que consistían en cargar el código original de fábrica, pero no se logró el objetivo.

Por tanto, se siguió al siguiente paso que fue subir el código manualmente en esta parte se necesita tener Arduino IDE instalado para poder subir el código sin inconveniente con sus respectivas librerías.

3.7.4.1 LIBRERÍAS INSTALADAS

Tabla 4. *Detalles de librerías necesarias.*

Librería	Desarrollador / Fuente	Propósito en el Hardware
U8g2	Oliver (olikraus)	Control y renderizado de la interfaz gráfica en la pantalla OLED SSD1306 (I2C).
Adafruit_NeoPixel	Adafruit	Control del LED direccionable RGB (NeoPixel) que actúa como indicador de estado.
RF24	TMRh20	Gestión del protocolo de comunicación y configuración de los tres módulos de radiofrecuencia NRF24L01.

Entre las principales bibliotecas instaladas en Arduino IDE se encuentran U8g2, utilizada para controlar la pantalla OLED mediante comunicación I²C; Adafruit NeoPixel, empleada para gestionar los LED RGB direccionables del RF-Clown v2; y RF24, destinada a configurar y controlar la comunicación de los módulos de radiofrecuencia nRF24L01.

3.7.5 INFORME TÉCNICO DETALLADO DE LA CORRECCIÓN

3.7.5.1 DIAGNÓSTICO DEL PROBLEMA ORIGINAL

En C/C++, el ciclo de compilación de un proyecto Arduino procesa cada archivo (.cpp) (y el (.ino), que se traduce internamente a (.cpp)) de forma independiente, generando un archivo objeto (.o) por cada uno. En este proyecto había tres unidades de traducción:

Tabla 5. *Carpetas dentro de la programación*

Unidad de traducción	Archivo objeto generado
RfClown.ino	RfClown.ino.cpp.o
neopixel.cpp	neopixel.cpp.o
setting.cpp	setting.cpp.o

Los tres incluían `#include "config.h"` y `#include "setting.h"`.

El problema: dentro de `config.h` y `setting.h` no solo había declaraciones (`extern`), sino definiciones reales con reserva de memoria e inicialización, por ejemplo:

```

8
9 // ----- Definiciones únicas de variables globales (declaradas extern en config.h / setting.h) -----
10 U8G2_SSD1306_128X64_NONAME_F_HW_I2C u8g2(U8G2_R0, /* reset=*/ U8X8_PIN_NONE);
11 Adafruit_NeoPixel pixels(1, 14, NEO_GRB + NEO_KHZ800);
12
13 OperationMode current_Mode = WIFI_MODULE;
14 volatile Operation current = DEACTIVE_MODE;
15
16 byte channelGroup_1[] = {2, 5, 8, 11};
17 byte channelGroup_2[] = {26, 29, 32, 35};
18 byte channelGroup_3[] = {80, 83, 86, 89};
19
20 volatile bool ChangeRequested = false;
21 volatile bool ChangeRequested1 = false;
22 volatile bool ChangeRequested2 = false;
23
24 unsigned long lastPressTime = 0;
25
26 bool neoPixelActive = false;
27 uint8_t oledBrightness = 100;
28 //

```

Fig. 30. Se eliminaron las definiciones del display y del NeoPixel

Como el contenido de los archivos de cabecera se copia textualmente (vía preprocesadora `#include`) dentro de cada (`.cpp`) que lo incluye, el efecto real era que el compilador generaba tres copias independientes de cada una de esas variables una por cada archivo objeto. Cuando el linker intenta unir los tres o en un solo binario, encuentra el mismo símbolo (ej. `u8g2`) definido tres veces y no puede decidir cuál usar, generando un error de "multiple definition".

Es importante notar la diferencia con las variables `const`:

```

73 extern volatile unsigned long operationCounter;
74 extern byte channelGroup_1[];
75 extern byte channelGroup_2[];
76 extern byte channelGroup_3[];
77
78 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};
79 const byte ble_channels[] = {2, 26, 80};
80 const byte wifi_channels[] = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12};
81 const byte usbWireless_channels[] = {40, 50, 60};
82 const byte videoTransmitter_channels[] = {70, 75, 80};
83 const byte rc_channels[] = {1, 3, 5, 7};
84 const byte zigbee_channels[] = {11, 15, 20, 25};
85 const byte nrf24_channels[] = {76, 78, 79};
86
87 extern volatile bool ChangeRequested;

```

Fig. 31. Enlaces internos (internal linkage)

Estas no dieron error porque en C++ (a diferencia de C) los objetos `const` en el ámbito global tienen enlace interno (internal linkage) por defecto. Esto significa que el compilador trata cada copia como privada de su propio archivo objeto, sin generar conflicto con el linker. Por eso `txt_n`, `txt_c`, `txt_v` y el arreglo de bitmap `cred []` en `setting.h` no necesitaron modificación.

3.7.5.2 SOLUCIÓN APLICADA: SEPARAR DECLARACIÓN VS DEFINICIÓN

La solución que se puede realizar en C/C++ para variables globales compartidas entre varios archivos sigue el patrón:

- Declaración (`extern`) en el archivo de cabecera (`.h`) le dice al compilador "esta variable existe en algún lugar, su tipo es `X`", pero no reserva memoria.
- Definición (sin `extern`, con inicialización) en un único archivo `.cpp` aquí sí se reserva la memoria una sola vez.

3.7.5.3 CAMBIOS EN CONFIG.H

```
U8G2_SSD1306_128X64_NONAME_F_HW_I2C u8g2(U8G2_R0, /* reset=*/ U8X8_PIN_NONE);
Adafruit_NeoPixel pixels(1, 14, NEO_GRB + NEO_KHZ800);
...
OperationMode current_Mode = WiFi_MODULE;
volatile Operation current = DEACTIVE_MODE;

byte channelGroup_1[] = {2, 5, 8, 11};
byte channelGroup_2[] = {26, 29, 32, 35};
byte channelGroup_3[] = {80, 83, 86, 89};
...
volatile bool ChangeRequested = false;
volatile bool ChangeRequested1 = false;
volatile bool ChangeRequested2 = false;

unsigned long lastPressTime = 0;
```

Fig. 32. Antes de cambiar código original

```
// Las definiciones con cuerpo de objeto (u8g2, pixels) se ELIMINARON de aquí
// y se movieron a RfClown.ino

enum OperationMode {...};
extern OperationMode current_Mode;

enum Operation {DEACTIVE_MODE, ACTIVE_MODE};
extern volatile Operation current;

extern byte channelGroup_1[];
extern byte channelGroup_2[];
extern byte channelGroup_3[];

extern volatile bool ChangeRequested;
extern volatile bool ChangeRequested1;
extern volatile bool ChangeRequested2;

extern unsigned long lastPressTime;
const unsigned long debounceDelay = 200; // se mantiene const, sin problema de ODR
```

Fig. 33. Después de cambiar código se agrega un const

Para arreglos (byte channelGroup_1[]), la declaración extern no necesita especificar el tamaño (extern byte channelGroup_1[]; es válido), porque el tamaño se resuelve en tiempo de enlace contra la definición real.

3.7.5.4 CAMBIOS EN SETTING.H

```
//extern bool neoPixelActive;

bool neoPixelActive = false;
uint8_t oledBrightness = 100;
```

Fig. 34. Antes de generar cambios

```
extern bool neoPixelActive;
extern uint8_t oledBrightness;
```

Fig. 35. Después se agrega un extern

(Aquí también había un detalle adicional: la línea extern bool NeoPixelActive; original

estaba comentada con `//`, es decir, no tenía ningún efecto la variable real definida justo debajo era la única existente, y se duplicaba en cada `.cpp` igual que las demás.)

3.7.5.5 CAMBIOS EN RFCLOWN.INO

```
#include "setting.h"
#include "config.h"

// ---- Definiciones únicas de variables globales ----
U8G2_SSD1306_128X64_NONAME_F_HW_I2C u8g2(U8G2_R0, /* reset=*/ U8X8_PIN_NONE);
Adafruit_NeoPixel pixels(1, 14, NEO_GRB + NEO_KHZ800);

OperationMode current_Mode = WiFi_MODULE;
volatile Operation current = DEACTIVE_MODE;

byte channelGroup_1[] = {2, 5, 8, 11};
byte channelGroup_2[] = {26, 29, 32, 35};
byte channelGroup_3[] = {80, 83, 86, 89};

volatile bool ChangeRequested = false;
volatile bool ChangeRequested1 = false;
volatile bool ChangeRequested2 = false;

unsigned long lastPressTime = 0;

bool neoPixelActive = false;
uint8_t oledBrightness = 100;
// -----
```

Fig. 36. Cambios RF Clown unidad de traducción

Se agregó, justo después de los `#include`, un bloque nuevo que centraliza todas las definiciones reales en un único lugar (una sola unidad de traducción).

3.7.6 GUÍA DE OPERACIÓN SEGURA DEL RF-CLOWN V2

Procedimiento de operación segura

Antes de energizar el RF-Clown v2 se verificó el correcto estado de las conexiones eléctricas, la instalación adecuada de las antenas y la ausencia de daños visibles en la placa o en los conectores SMA.

Las pruebas experimentales fueron ejecutadas únicamente durante el tiempo necesario para realizar las mediciones programadas, evitando mantener el dispositivo transmitiendo de forma continua sin supervisión.

Las evaluaciones se realizaron en un entorno controlado de laboratorio, procurando minimizar la afectación sobre dispositivos inalámbricos ajenos al experimento.

Para finalizar las pruebas, el equipo fue desactivado inmediatamente mediante el procedimiento normal de apagado, verificando posteriormente la recuperación de la conectividad de los dispositivos utilizados como objetivo experimental.

Tabla 6. *Procedimiento de operación segura*

Etapas	Procedimiento
Antes de la prueba	Verificar conexiones, alimentación y antenas.
Inicio	Activar únicamente el modo de interferencia requerido para la prueba.
Durante la prueba	Supervisar continuamente el funcionamiento del dispositivo y limitar el tiempo de emisión.
Finalización	Desactivar inmediatamente el modo de interferencia.
Después de la prueba	Confirmar la recuperación de la comunicación de los dispositivos evaluados.

Recomendaciones de seguridad

- Utilizar el dispositivo únicamente con fines académicos y de investigación.
- Evitar su utilización en zonas donde existan sistemas inalámbricos críticos.
- Limitar el tiempo de transmisión únicamente al requerido para la prueba.
- No operar el equipo cerca de servicios sensibles o dispositivos de terceros.
- Mantener una supervisión permanente durante toda la operación.
- Desconectar el equipo inmediatamente después de finalizar cada ensayo.

4 CAPÍTULO IV: EVALUACIÓN DE FACTIBILIDAD TÉCNICA, MITIGACIÓN DE INTERFERENCIAS Y CONCLUSIONES

4.1 EVALUACIÓN EXPERIMENTAL DEL RF-CLOWN V2 EN EL BLOQUEO DE REDES WI-FI (IEEE 802.11 B/G/N)

Para la interpretación de estos resultados se debe considerar que la activación de cualquiera de los indicadores del Protect 1206i confirma únicamente que el equipo registró una emisión compatible con sus criterios internos de detección o clasificación. Esta respuesta no identifica de manera concluyente el protocolo emitido ni demuestra por sí sola la efectividad de la interferencia.



Fig. 40. RF-Clown v2 energizado frente al Protect 1206i

Los resultados del indicador electromagnético revelan los siguientes puntos críticos:

Saturación del indicador de intensidad: la barra de intensidad de señal (Signal Strength) del instrumento de medición se saturó por completo, alcanzando el rango máximo de la escala analógica (color naranja). La barra de intensidad de señal del Protect 1206i alcanzó el

nivel máximo de su escala durante la medición en campo cercano. Este resultado indica únicamente una respuesta elevada del detector ante la emisión presente, pero no constituye una medición cuantitativa de potencia ni demuestra por sí solo la degradación de otros receptores.

4.1.1 ANÁLISIS ESPECTRAL CUANTITATIVO (NARDA SRM-3006)

Para cuantificar el impacto sobre el espectro radioeléctrico en el entorno ecuatoriano, se empleó el analizador selectivo Narda SRM-3006, configurado con un ancho de banda de resolución (RBW) de 1 MHz y un tiempo de barrido de 165 ms. El rango de frecuencias evaluado comprendió desde los 2.2325 GHz hasta los 2.6 GHz, cubriendo la totalidad de la banda libre local regulada por la ARCOTEL.

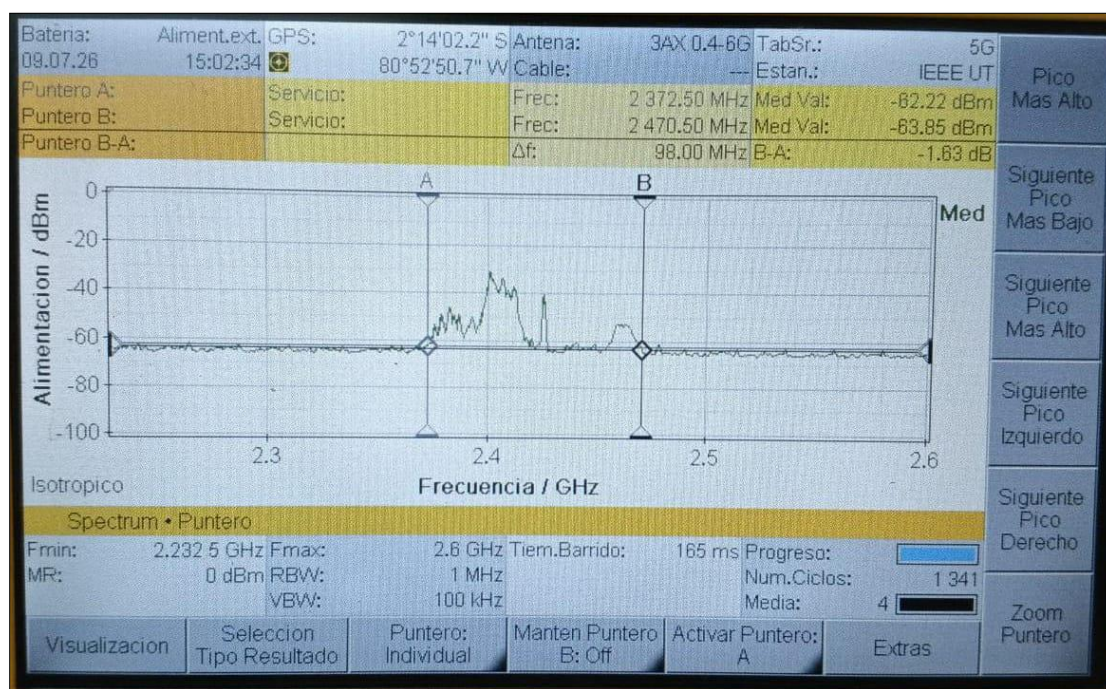


Fig. 41. Pantalla del analizador espectral Narda

Al activar la función Wi-Fi del RF-Clown v2, el espectro observado (Fig. 41) presenta las siguientes características:

Marcadores de referencia: el marcador A (2372.50 MHz) y el marcador B (2470.50 MHz) registraron niveles de potencia de -82.22 dBm y -83.85 dBm respectivamente. Estos valores delimitan las zonas marginales y superiores de la banda, sirviendo como umbral base para contrastar la actividad central.

Distribución espectral de la interferencia: en el centro de la banda ISM (alrededor de los 2.4 GHz a 2.45 GHz, donde se concentran los canales Wi-Fi 1 al 11), se evidencia una alteración del espectro con múltiples picos y crestas que se elevan sustancialmente por encima del piso de ruido, oscilando entre los -60 dBm y los -65 dBm.

Mecanismo de bloqueo: La forma de onda registrada no corresponde a una portadora continua (CW), sino a una firma espectral ensanchada y fragmentada. Esto valida matemáticamente la estrategia de inyección del dispositivo: al realizar un barrido rápido de portadoras mediante el direccionamiento de registros en el hardware base, se eleva el piso de ruido efectivo dentro de los canales Wi-Fi seleccionados. Al degradarse la Relación Señal a interferencia más ruido (SINR) de las redes locales por debajo del umbral de Shannon Hartley, las estaciones de trabajo legítimas sufren una pérdida masiva de paquetes (Packet Loss), forzando la desconexión del enlace inalámbrico sin necesidad de inyectar tramas de desautenticación tradicionales de la capa MAC.

4.2 EVALUACIÓN EXPERIMENTAL DEL RF-CLOWN V2 BAJO EL PROTOCOLO BLUETOOTH CLASSIC (IEEE 802.15.1)

Para esta fase experimental, se configuró el prototipo RF-Clown v2 en el modo correspondiente a Bluetooth Classic, con el propósito de caracterizar las emisiones generadas sobre este protocolo.

El objetivo de este ensayo fue evaluar la respuesta del hardware ante sistemas que emplean espectro ensanchado por salto de frecuencia (FHSS) en la banda ISM de 2.4 GHz, registrando los datos mediante instrumentación selectiva y detectores de campo cercano.

4.2.1 ANÁLISIS DE RESPUESTA EN CAMPO CERCANO E IDENTIFICACIÓN DE PROTOCOLO (PROTECT 1206I)

Tal como se muestra en la Fig. 42, se configuró mediante su firmware para activar los transceptores de forma concurrente, orientados a los canales utilizados durante el salto de frecuencia de Bluetooth. Al aproximar el detector portátil Protect 1206i con su antena direccional Micro Pointer (LPDA-12) acoplada en la entrada de alta frecuencia (ANT2), se registraron variaciones analíticas críticas respecto a la prueba previa de Wi-Fi.



Fig. 42. RF-Clown v2 energizado frente al Protect 1206i

Los resultados del indicador electromagnético revelan los siguientes puntos críticos:

Comportamiento de la barra de intensidad (Signal Strength): a diferencia de la saturación masiva observada en otros protocolos, la barra de LED naranja registró una oscilación dinámica intermitente, estabilizándose en un nivel intermedio-alto (aproximadamente entre un 60% y 70% de la escala).

Respuesta funcional del enlace Bluetooth Classic: durante las pruebas experimentales se observó la pérdida de conectividad entre los dispositivos Bluetooth, evidenciada por el cambio de estado del indicador LED y la interrupción del enlace inalámbrico. Esta observación constituye una evidencia funcional del efecto producido por la interferencia generada por el RF-Clown v2; sin embargo, no permite validar directamente la estructura temporal ni el comportamiento interno del protocolo Bluetooth.

4.2.2 EXTRACCIÓN DE DATOS ESPECTRALES CUANTITATIVOS (NARDA SRM-3006)

El análisis del comportamiento de potencia y distribución de frecuencia se consolidó mediante el analizador selectivo de radiación Narda SRM-3006. De acuerdo con los datos vectoriales capturados en la interfaz de la Fig. 43, el instrumento operó bajo un span (2.2325 GHz a 2.6 GHz) con un RBW de 1 MHz y un promedio de 4 ciclos de barrido.

Los parámetros extraídos cuantitativos de los marcadores directos del equipo revelan el siguiente escenario:

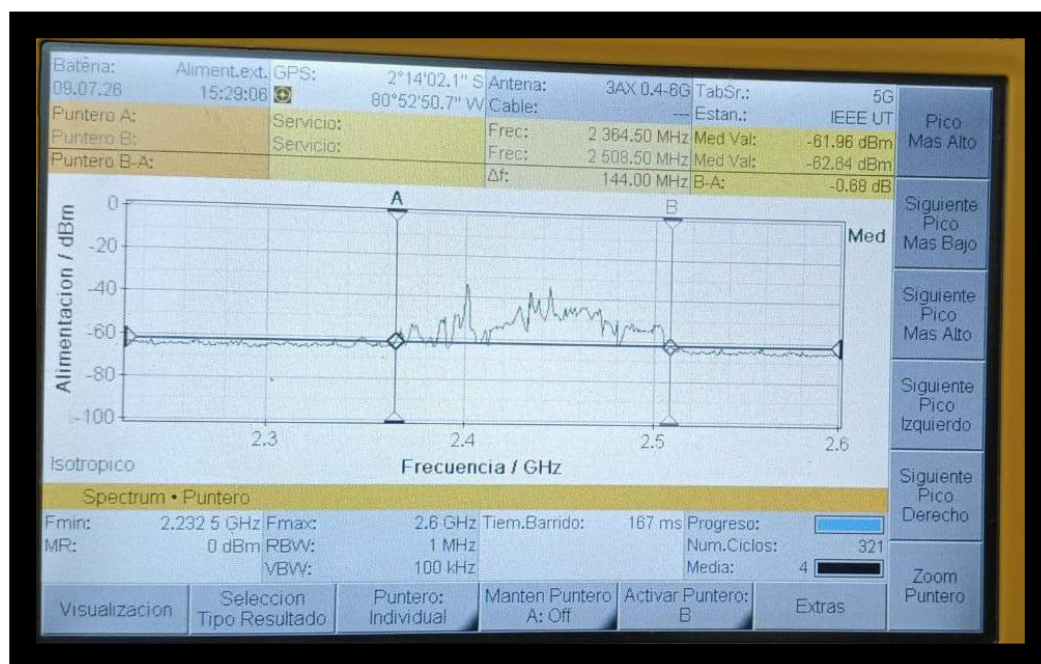


Fig. 43. Narda SRM-3006 con los marcadores A y B

- Marcador A (2.384 GHz):** registra un nivel de potencia pico absoluto de -61.96 dBm. Esta medición confirma un estado de baja actividad electromagnética en los segmentos inmediatamente inferiores al inicio de la banda ISM, sirviendo como línea de ruido de fondo.
- Marcador B (2.528 GHz):** registra un nivel de potencia de -62.64 dBm, demostrando el aislamiento y la caída de la energía radiada una vez que se superan las frecuencias reguladas de la banda libre.
- Análisis del espectrograma central:** en la región crítica comprendida entre los 2.4 GHz y los 2.48 GHz, se aprecia con total claridad la firma espectral del salto de frecuencia provocada por el RF-Clown v2. Se observa una sucesión densa de cresta y valles agudos que sobresalen del piso de ruido, alcanzando valores de entre -60 dBm y -64 dBm. A diferencia del perfil plano que generaría una portadora de banda ancha (como Wi-Fi), esta firma multi pico es la evidencia

matemática de que los tres módulos periféricos están barriendo y saturando secuencialmente los subcanales Bluetooth, elevando la probabilidad de colisión de paquetes en el aire. Esto provoca la degradación del enlace legítimo del dispositivo víctima por interferencia cocanal mutua.

4.3 EVALUACIÓN EXPERIMENTAL DEL RF-CLOWN V2 BAJO EL PROTOCOLO BLUETOOTH LOW ENERGY (BLE)

Para este ensayo, se configuró el firmware del prototipo RF-Clown v2 en el modo de caracterización y afectación orientado específicamente a Bluetooth Low Energy (BLE). El propósito de esta prueba fue analizar la huella electromagnética y la capacidad del dispositivo para interferir o auditar canales publicitarios (advertising) y de datos empleados por el estándar IoT de baja potencia en la banda ISM.

4.3.1 ANÁLISIS DE RESPUESTA EN CAMPO CERCANO E IDENTIFICACIÓN DE PROTOCOLO (PROTECT 1206I)

Como se detalla en la Fig. 44, el hardware RF-Clown se acopló en línea de vista directa (LoS) con el detector de contramedidas Protect 1206i, utilizando la antena log periódica micro pointer (LPDA 12) conectada al puerto de alta frecuencia ANT2.



Fig. 44. BLE operando junto al detector Protect 1206i

Los indicadores analógicos y lumínicos del instrumento revelaron los siguientes resultados técnicos:

Comportamiento de la barra de potencia (Signal Strength): la barra de LED amarillos registró una intensidad fija y sostenida muy elevada, rozando los umbrales máximos superiores (-8 dB a -5 dB de la escala del detector).

Comportamiento del bloque de identificación: a diferencia de la prueba de Bluetooth Classic, el panel inferior (Identification) del Protect 1206i no encendió el LED azul de Bluetooth ni ningún otro indicador de protocolo.

4.3.2 EXTRACCIÓN DE DATOS ESPECTRALES CUANTITATIVOS (NARDA SRM-3006)

La cuantificación del comportamiento energético se realizó mediante el analizador

selectivo Narda SRM-3006. De acuerdo con las lecturas en tiempo real mostradas en la Figura 9, el instrumento operó con un Span extendido de 2.2325 GHz a 2.6 GHz, un RBW de 1 MHz y un tiempo de barrido adaptativo de 188 ms.

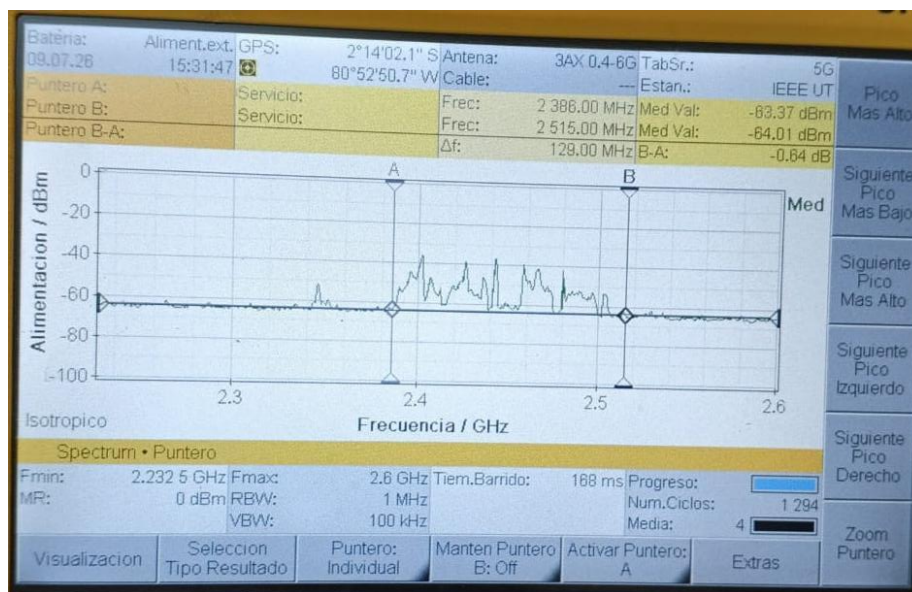


Fig. 45. Detalle el espectrograma con los marcadores A y B

Los parámetros vectoriales directos extraídos de la pantalla del equipo exponen las siguientes métricas:

Marcador A (2.386 GHz): registró una potencia pico medida de -83.37 dBm, estableciendo el límite inferior del piso de ruido del laboratorio fuera de la banda de interés.

Marcador B (2.515 GHz): registró un valor de potencia residual de -84.01 dBm en la zona superior adyacente a la banda ISM.

Análisis morfológico del espectrograma: en la ventana central de los 2.40 GHz a los 2.48 GHz, se aprecia la alteración del espectro provocada por el RF-Clown v2 en modo BLE. La firma espectral se caracteriza por crestas concentradas y agudas que se elevan consistentemente hasta los -60 dBm. Esta disposición es técnicamente coherente con el mapa de canales de BLE;

al concentrar ráfagas consecutivas sobre bandas angostas de 2 MHz, la señal de interferencia genera "pistas" de ruido que degradan de inmediato el indicador RSSI de los dispositivos IoT periféricos legítimos en el entorno, imposibilitando el intercambio de datos (Data Channel PDU) y forzando la desconexión inmediata de los sensores o wearables bajo análisis.

4.4 EVALUACIÓN EXPERIMENTAL DEL RF-CLOWN V2 BAJO EL PROTOCOLO ZIGBEE (IEEE 802.15.4)

Para esta parte del proyecto, el firmware del dispositivo RF-Clown v2 se conmutó al modo de caracterización e inyección orientado al estándar IEEE 802.15.4 (Zigbee). El objetivo fue estudiar la huella espectral y el nivel de interferencia electromagnética que el prototipo puede inducir sobre redes de sensores inalámbricos y sistemas de domótica industrial que operan en los 16 canales asignados a esta tecnología dentro de la banda ISM de 2.4 GHz.

4.4.1 ANÁLISIS DE RESPUESTA EN CAMPO CERCANO E IDENTIFICACIÓN DE PROTOCOLO (PROTECT 1206I)

Tal como se documenta en la Fig. 46, el hardware RF-Clown v2 se dispuso en línea de vista directa (LoS) frente al receptor del detector de contramedidas Protect 1206i, empleando la antena log-periódica Micro-Pointer (LPDA-12) acoplada en el canal de alta frecuencia ANT2.



Fig. 46. Funcionando junto al detector Protect 1206i

Los indicadores luminosos obtenidos durante esta prueba revelaron las siguientes particularidades técnicas:

Atenuación de la barra de intensidad (Signal Strength): a diferencia de la saturación total observada en el modo Wi-Fi, la escala de LED amarillos reflejó una lectura intermedia-alta, estabilizándose alrededor del 60% al 70% de la capacidad del instrumento.

4.4.2 EXTRACCIÓN DE DATOS ESPECTRALES CUANTITATIVOS (NARDA SRM-3006)

El impacto energético en el espectro de radiofrecuencia se validó mediante el analizador selectivo de radiación Narda SRM-3006. De acuerdo con la configuración y los datos vectoriales capturados en la pantalla de la Fig. 47, el instrumento operó con un Span de 2.2325 GHz a 2.6 GHz, un RBW de 1 MHz y un promedio de 4 ciclos de barrido.

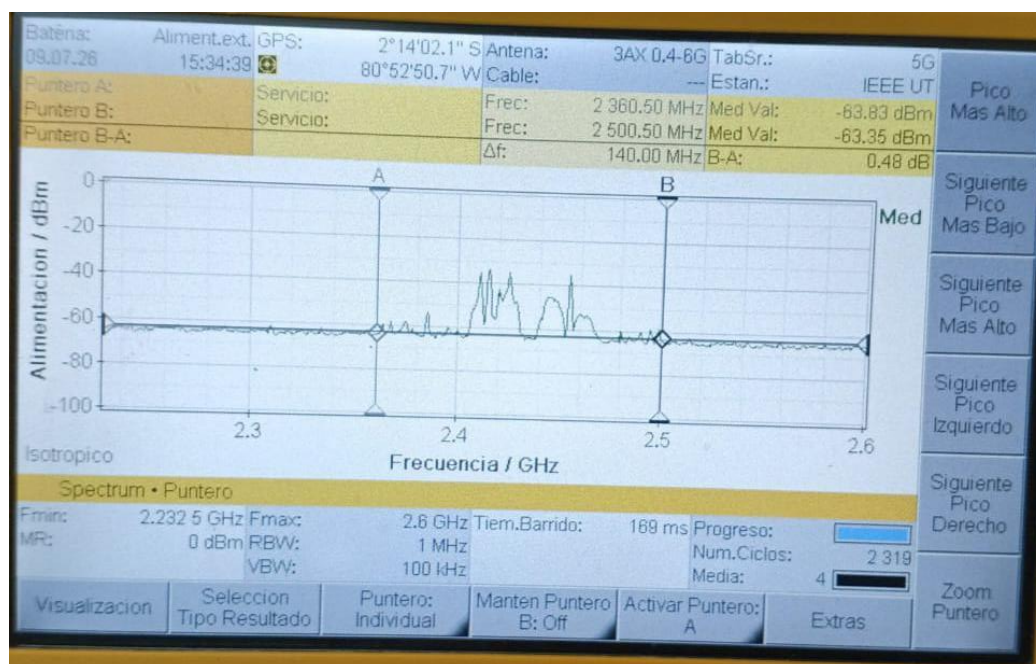


Fig. 47. Detalle el espectrograma con los marcadores A y B

Los parámetros cuantitativos exactos extraídos directamente de los marcadores del instrumento exponen el siguiente escenario:

Marcador A (2.360 GHz): registró un nivel de potencia pico absoluto de -63.83 dBm, definiendo con precisión el piso de ruido ambiental de baja actividad por debajo de la banda ISM.

Marcador B (2.500 GHz): registró una amplitud de -63.35 dBm, marcando la atenuación de la señal una vez superado el espectro libre.

Análisis morfológico del espectrograma: en la ventana central que comprende los 2.40 GHz a los 2.4835 GHz, se evidencia la huella de inyección del RF-Clown v2 en modo Zigbee. El espectrograma muestra una sucesión de lóbulos y picos agudos continuos que se elevan sustancialmente hasta alcanzar valores de entre -60 dBm y -63 dBm. Dado que los canales Zigbee están numerados del 11 al 26 con una separación entre centros de 5 MHz, esta firma

multi pico concentrada demuestra que el arreglo de transceptores barre y satura eficientemente los canales críticos de control. Al elevar el piso de ruido por encima del umbral de demodulación de los chips receptores legítimos (como el CC2530 o similares), se reduce a cero la relación señal a interferencia más ruido (SINR), bloqueando las tramas de datos del protocolo de red y forzando la pérdida total de conectividad en los dispositivos IoT esclavos.

4.5 EVALUACIÓN EXPERIMENTAL DEL RF-CLOWN V2 BAJO EL MODO NRF24L01+ (PROTOCOLO PROPIETARIO DE 2.4 GHZ)

Para esta sesión de ensayos, el firmware del prototipo RF-Clown v2 se configuró en su modo nativo y directo de manipulación de registros de radiofrecuencia, denominado modo nRF24. El objetivo fundamental fue caracterizar la huella espectral y el campo radiado cuando el dispositivo transmite ráfagas de datos crudos no estructurados (Enhanced ShockBurst u operaciones de portadora pura) usando los mismos transceptores periféricos embebidos en el hardware base, analizando su huella frente a los instrumentos de medición.

4.5.1 ANÁLISIS DE RESPUESTA EN CAMPO CERCANO E IDENTIFICACIÓN DE PROTOCOLO (PROTECT 1206I)

Como se describe en las Fig. 48, el hardware RF-Clown v2 se colocó en línea de vista directa (LoS) frente al receptor del detector de contramedidas Protect 1206i, utilizando la antena direccional log-periódica Micro-Pointer (LPDA-12) acoplada en la entrada de alta frecuencia ANT2.

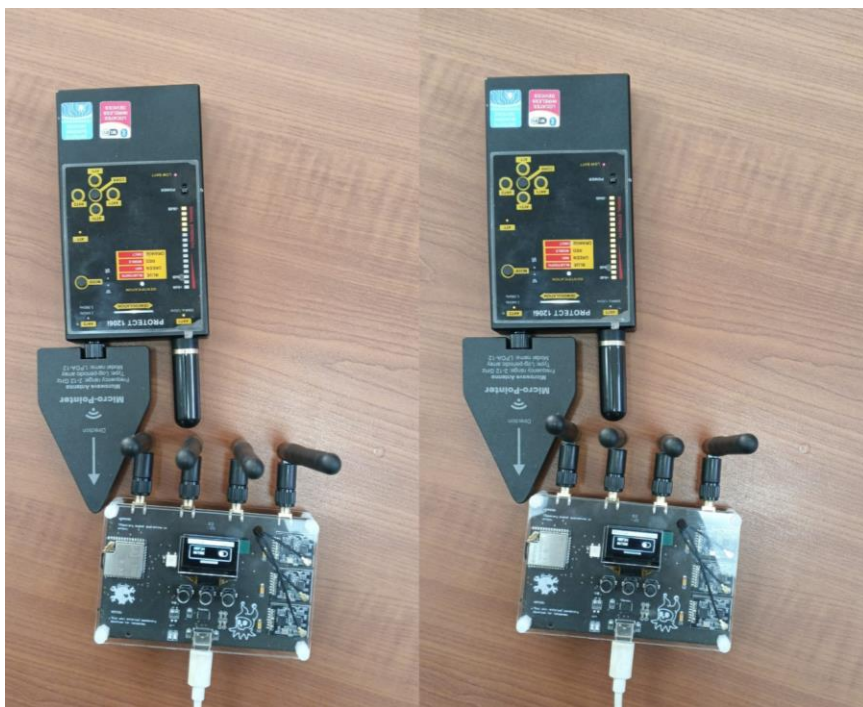


Fig. 48. Nrf24 operando junto al detector Protect 1206i

Durante la prueba en modo nRF24, el Protect 1206i no activó los indicadores asociados con Wi-Fi o Bluetooth. Este resultado indica únicamente que la emisión registrada no coincidió con los criterios internos de clasificación del detector bajo las condiciones del ensayo. La ausencia de activación de estos indicadores no permite concluir que la señal carezca de cabeceras, que sea indetectable o que haya sido clasificada como ruido electromagnético de fondo. La caracterización cuantitativa de la emisión se sustentó en las mediciones efectuadas mediante el Narda SRM-3006.

Los indicadores analógicos y lumínicos obtenidos durante esta prueba revelaron las siguientes particularidades técnicas:

Comportamiento de la barra de intensidad (Signal Strength): la barra de LED amarillos registró una lectura de amplitud moderada o intermedia, estabilizándose aproximadamente entre un 40% y un 50% de la escala del detector (marcando los segmentos

inferiores y medios).

Comportamiento del bloque de identificación: en el panel inferior (Identification), el Protect 1206i mantuvo todos sus LED de protocolo completamente apagados.

4.5.2 EXTRACCIÓN DE DATOS ESPECTRALES CUANTITATIVOS (NARDA SRM-3006)

La cuantificación y análisis formal del espectro se consolidó mediante el analizador selectivo de radiación Narda SRM-3006. De acuerdo con los datos e indicadores vectoriales capturados en tiempo real en la pantalla de la Fig. 49, el instrumento operó con un Span de 2.2325 GHz a 2.6 GHz, un RBW de 1 MHz y un promedio de 4 ciclos de barrido.

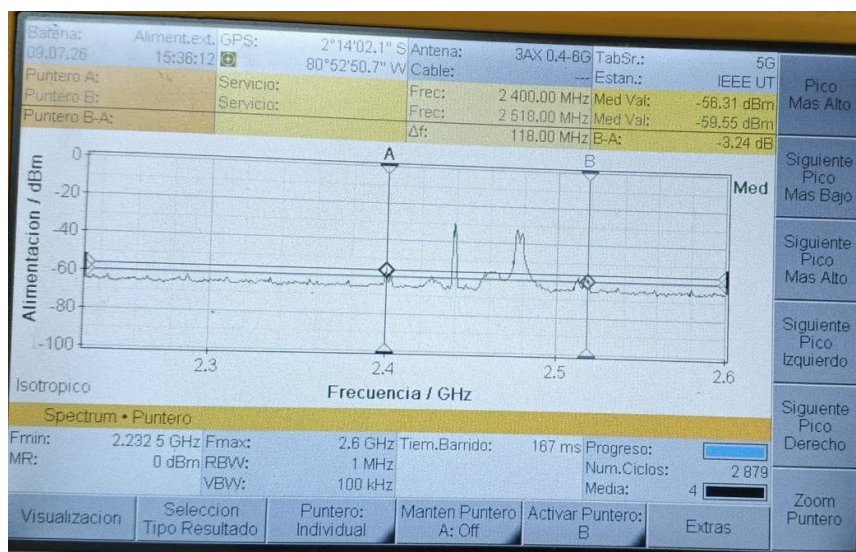


Fig. 49. Narda SRM-3006 detalle del espectrograma con los marcadores A y B

Los parámetros cuantitativos exactos extraídos directamente de los marcadores analíticos del instrumento exponen el siguiente escenario técnico:

Marcador A (2.4 GHz): posicionado exactamente en el límite inferior de la banda ISM de 2.4 GHz, registró un nivel de potencia pico de -56.31 dBm. Esta lectura es significativamente

más alta que el piso de ruido de fondo de los ensayos previos, indicando una fuerte inyección de energía justo al comienzo de la banda útil.

Marcador B (2.518 GHz): registró un valor de potencia residual de -59.55 dBm en la región superior externa a la banda libre.

Análisis morfológico del espectrograma: en la ventana central que comprende la banda ISM (2.400 GHz a 2.483 GHz), se aprecia una firma espectral sumamente limpia y focalizada. A diferencia de las formas multi pico dispersas de Bluetooth o Zigbee, aquí se observa un perfil espectral plano y controlado con picos estables que se elevan hasta bordear los -55 dBm. Esta morfología es la evidencia matemática directa de la transmisión nativa del chip nRF24L01+; al configurar los transceptores para emitir portadoras continuas o barrer subcanales específicos de forma secuencial sin capas de abstracción pesadas, la energía se distribuye de manera homogénea. Esto maximiza la eficiencia de la interferencia cocanal, permitiendo que el RF-Clown v2 sature los receptores de periféricos inalámbricos de bajo costo (como teclados, mouses o drones que usen este mismo chip) al tirar abajo su relación Señal a Interferencia (SIR).

4.6 EVALUACIÓN EXPERIMENTAL DEL RF-CLOWN V2 BAJO EL MODO VIDEO TX (TRANSMISIÓN DE VIDEO EN 2.4 GHZ)

Para esta fase de ensayos, el firmware del prototipo RF-Clown v2 se conmutó al modo de caracterización e inyección enfocado en sistemas de transmisión de Video (Video TX). El propósito de esta prueba fue evaluar la huella electromagnética del dispositivo y su capacidad para degradar o saturar señales continuas de banda ancha analógicas o digitales, comunes en cámaras de seguridad inalámbricas, drones de transmisión en tiempo real (FPV) y transmisores comerciales que operan dentro de la banda ISM.

4.6.1 ANÁLISIS DE RESPUESTA EN CAMPO CERCANO E IDENTIFICACIÓN DE PROTOCOLO (PROTECT 1206I)

Tal como se documenta en las Fig. 50, el hardware RF-Clown v2 se posicionó en línea de vista directa (LoS) frente al receptor del detector de contramedidas Protect 1206i, empleando la antena log-periódica Micro-Pointer (LPDA-12) acoplada en el canal de alta frecuencia ANT2.



Fig. 50. Video Tx operando junto al Protect 1206i

Los indicadores analógicos y lumínicos obtenidos durante esta prueba revelaron las siguientes particularidades técnicas:

Comportamiento de la barra de intensidad (*Signal Strength*): la barra de LED amarillos registró una lectura de amplitud alta, alcanzando aproximadamente entre un 70% y un 80% de la escala del detector de contramedidas.

Comportamiento del bloque de identificación: en el panel inferior (*Identification*), el Protect 1206i mantuvo todos sus LED de protocolo completamente apagados.

4.6.2 EXTRACCIÓN DE DATOS ESPECTRALES CUANTITATIVOS (NARDA SRM-3006)

La cuantificación y análisis formal del espectro se consolidó mediante el analizador selectivo de radiación Narda SRM-3006. De acuerdo con los datos e indicadores vectoriales capturados en tiempo real en la pantalla de la Fig. 51, el instrumento operó con un Span de 2.2325 GHz a 2.6 GHz, un RBW de 1 MHz y un promedio de 4 ciclos de barrido.

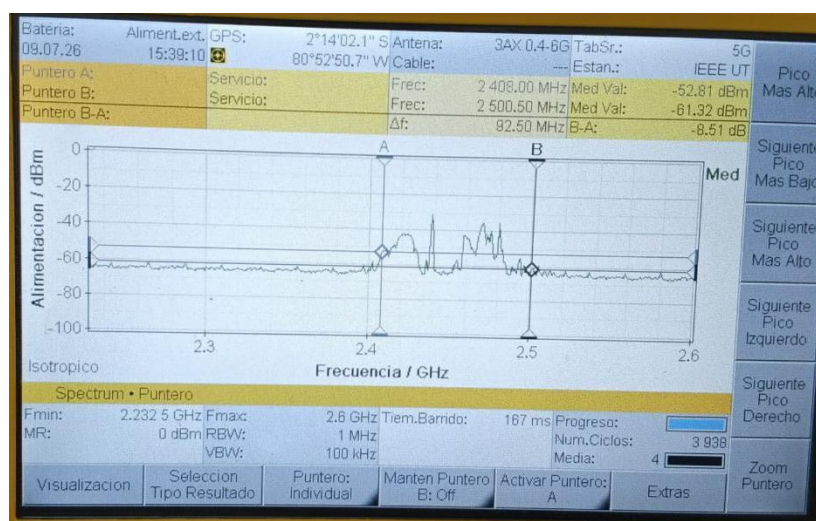


Fig. 51. Narda SRM-3006 detalle del espectrograma con los marcadores A y B

Los parámetros cuantitativos exactos extraídos directamente de los marcadores analíticos del instrumento exponen el siguiente escenario técnico:

Marcador A (2.397 GHz): posicionado de forma adyacente al arranque de la banda libre, registró un nivel de potencia pico de -63.69 dBm. Esto evidencia una elevación del piso de ruido general en las frecuencias de guarda inferiores.

Marcador B (2.508 GHz): registró un valor de potencia residual de -65.21 dBm en la

región superior adyacente externa a la banda ISM.

Análisis morfológico del espectrograma: en la ventana central que comprende el espectro de 2.40 GHz a 2.4835 GHz, se aprecia la firma de inyección del RF-Clown v2 configurado para Video TX. El espectrograma muestra un perfil ensanchado con picos específicos y una elevación notable que ronda los -60 dBm. Esta morfología es técnicamente consistente con la afectación de canales de video; al generar portadoras rápidas repartidas en los rangos centrales, el dispositivo satura el espectro de banda ancha. Al inyectar esta densidad de energía, se destruye la relación Señal a Interferencia (SIR) de los receptores de video legítimos. Debido a esto, los demoduladores de las cámaras o pantallas receptoras pierden la sincronía de los cuadros (frames), provocando congelamiento de imagen, ruido analítico (estática) o la pérdida total de la señal de video transmitida.

4.7 EVALUACIÓN EXPERIMENTAL DEL RF-CLOWN V2 BAJO EL MODO RC (SISTEMAS DE RADIOCONTROL EN 2.4 GHZ)

Para esta fase final de ensayos, el firmware del prototipo RF-Clown v2 se conmutó al modo de caracterización e inyección enfocado en sistemas de Radiocontrol (RC). El objetivo primordial de esta prueba fue evaluar la huella electromagnética del dispositivo y su capacidad para degradar o bloquear los enlaces de comandos de baja latencia utilizados comúnmente por vehículos aéreos no tripulados (drones), modelismo a escala y sistemas de automatización industrial que operan mediante saltos de frecuencia patentados en la banda ISM.

4.7.1 ANÁLISIS DE RESPUESTA EN CAMPO CERCANO E IDENTIFICACIÓN DE PROTOCOLO (PROTECT 1206I)

Así como se documenta en la fig. 52, el hardware RF-Clown se posicionó en línea de

vista directa frente al receptor del detector de contramedidas Protect 1206i. empleando la antena log periódica micro pointer (LPDA) acoplada en el canal de alta frecuencia ANT2.

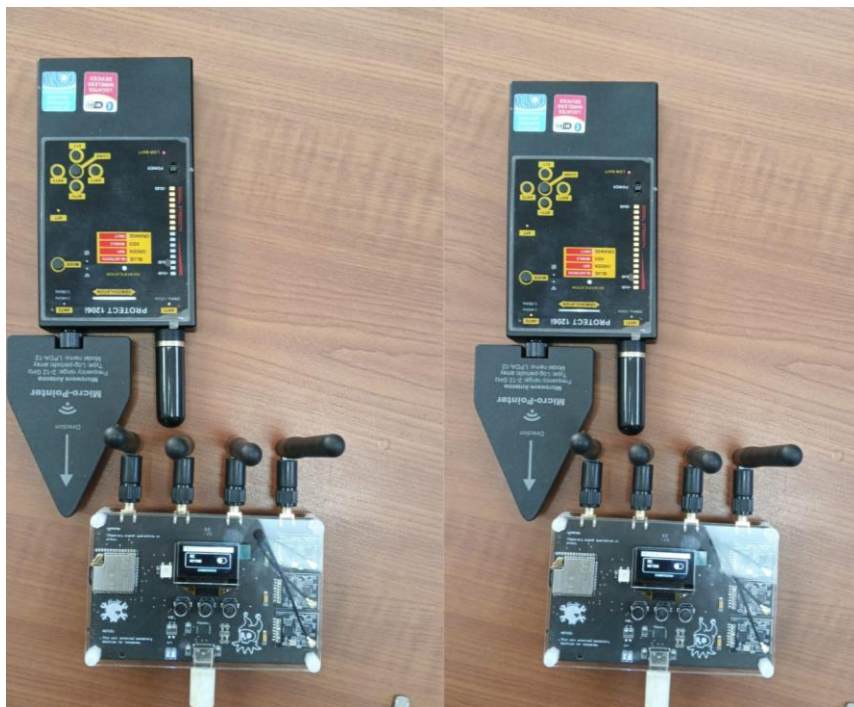


Fig. 52. Rc operando junto al Protect 1206i

Los indicadores analógicos y lumínicos obtenidos durante esta prueba revelaron las siguientes particularidades técnicas:

Comportamiento de la barra de intensidad (Signal Strength): la barra de LED amarillos registró una lectura de amplitud alta, alcanzando aproximadamente entre un 70% y un 80% de la escala del detector de contramedidas.

Comportamiento del bloque de identificación: en el panel inferior (Identification), el Protect 1206i mantuvo todos sus LED de protocolo completamente apagados.

4.7.2 EXTRACCIÓN DE DATOS ESPECTRALES CUANTITATIVOS (NARDA SRM-3006)

La cuantificación y análisis formal del espectro se consolidó mediante el analizador selectivo de radiación Narda SRM-3006. De acuerdo con los datos e indicadores vectoriales capturados en tiempo real en la pantalla de la Fig. 53, el instrumento operó con un Span de 2.2325 GHz a 2.6 GHz, un RBW de 1 MHz y un promedio de 4 ciclos de barrido.

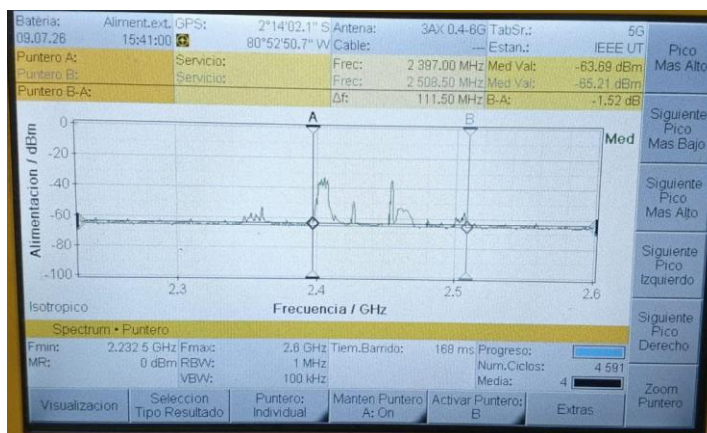


Fig. 53. Narda SRM-3006 detalle del espectrograma con los marcadores A y B

Los parámetros cuantitativos exactos extraídos directamente de los marcadores analíticos del instrumento exponen el siguiente escenario técnico:

Marcador A (2.397 GHz): posicionado de forma adyacente al arranque de la banda libre, registró un nivel de potencia pico de -63.69 dBm. Esto evidencia la presencia de energía residual en los bordes inferiores del espectro útil.

Marcador B (2.508 GHz): registró un valor de potencia de -65.21 dBm en la región superior externa a la banda ISM.

Análisis morfológico del espectrograma: en la ventana central que comprende el espectro de 2.40 GHz a 2.835 GHz, se aprecia con claridad la firma de inyección del RF-Clown

v2 en modo RC. El espectrograma muestra un perfil ensanchado con picos específicos distribuidos homogéneamente que rondan los -60 dBm. Esta morfología es técnicamente consistente con la afectación de canales de radiocontrol; al generar portadoras rápidas repartidas en toda la banda, el dispositivo destruye la relación Señal a Interferencia (SIR) de los receptores legítimos (sistemas FHSS de drones o mandos RC). Al inundar los subcanales, los receptores pierden los paquetes de sincronización de los mandos, activando de inmediato los protocolos de seguridad por pérdida de enlace (Fail-Safe), interrumpiendo el control físico del dispositivo objetivo.

4.8 EVALUACIÓN EXPERIMENTAL DEL RF-CLOWN V2 BAJO EL MODO USB WIRELESS (PERIFÉRICOS Y DISPOSITIVOS DE INTERFAZ HUMANA DE 2.4 GHZ)

Para este ensayo, el firmware del prototipo RF-Clown v2 se configuró en el modo de caracterización e inyección enfocado en enlaces USB Wireless propietarios. El propósito de esta prueba fue evaluar la huella electromagnética del dispositivo y su capacidad para degradar o bloquear la comunicación inalámbrica no-estándar de corto alcance (tecnologías basadas en protocolos de capas cerradas tipo Logitech Unifying o similares), comunes en mouses, teclados, punteros de presentación y adaptadores inalámbricos de escritorio que operan dentro de la banda ISM.

4.8.1 ANÁLISIS DE RESPUESTA EN CAMPO CERCANO E IDENTIFICACIÓN DE PROTOCOLO (PROTECT 1206I)

Tal como se documenta en la Fig. 54, el hardware RF-Clown v2 se dispuso en línea de vista directa (LoS) frente al receptor del detector de contramedidas Protect 1206i, empleando la

antena log-periódica Micro-Pointer (LPDA-12) acoplada en el canal de alta frecuencia ANT2.

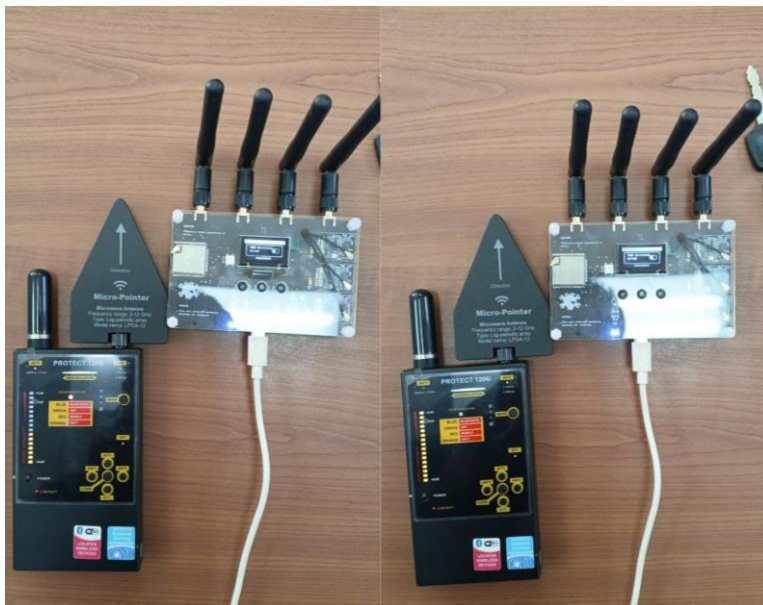


Fig. 54. USB Wireless operando junto al Protect 1206i

Los indicadores analógicos y lumínicos obtenidos durante esta prueba revelaron las siguientes particularidades técnicas:

Comportamiento de la barra de intensidad (Signal Strength): la barra de LED amarillos registró una lectura de amplitud fija y sostenida muy elevada, rozando los umbrales máximos superiores (-15 dB a -5 dB de la escala del detector).

Comportamiento del bloque de identificación: en el panel inferior (Identification), el Protect 1206i mantuvo todos sus LED de protocolo (Wi-Fi, Bluetooth) completamente apagados.

4.8.2 EXTRACCIÓN DE DATOS ESPECTRALES CUANTITATIVOS (NARDA SRM-3006)

La cuantificación y análisis formal del espectro se consolidó mediante el analizador selectivo de radiación Narda SRM-3006. De acuerdo con los datos e indicadores vectoriales

capturados en tiempo real en la pantalla de la Fig. 55, el instrumento operó con un Span de 2.2325 GHz a 2.6 GHz, un RBW de 1 MHz y un promedio de 4 ciclos de barrido.

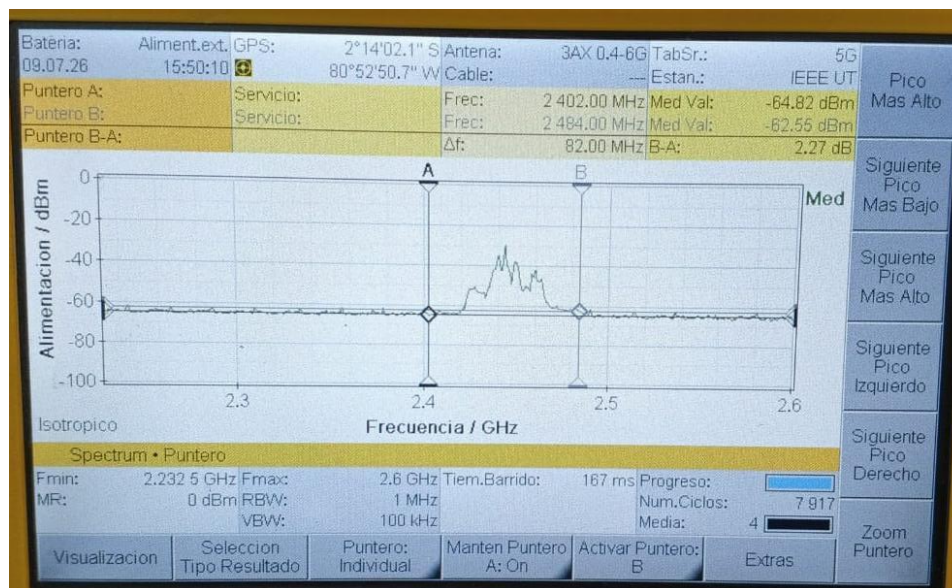


Fig. 55. Narda SRM-3006 detalle del espectrograma con los marcadores A y B

Los parámetros cuantitativos exactos extraídos directamente de los marcadores analíticos del instrumento exponen el siguiente escenario técnico:

Marcador A (2.402 GHz): posicionado con precisión en el canal de inicio de la banda ISM de 2.4 GHz, registró un nivel de potencia pico de -64.82 dBm. Esto evidencia el incremento de energía directo sobre la parte baja de la banda regulada.

Marcador B (2.484 GHz): posicionado exactamente en el límite de guarda inmediatamente posterior al canal 14 de Wi-Fi, registró un valor de potencia de -62.55 dBm.

Análisis morfológico del espectrograma: durante las pruebas realizadas en el modo USB Wireless se observó la interrupción completa de la comunicación entre el periférico inalámbrico y el computador mientras el RF-Clown v2 permaneció activo. Esta evaluación se realizó mediante la observación funcional del enlace y la respuesta del dispositivo objetivo.

No se cuantificó el porcentaje de pérdida de paquetes, debido a que la investigación no empleó herramientas de captura de tráfico ni analizadores de protocolos capaces de registrar el número de paquetes transmitidos, recibidos o retransmitidos. En consecuencia, los resultados obtenidos corresponden a una evaluación funcional de la conectividad y no a una medición cuantitativa del desempeño del protocolo.

4.9 EVALUACIÓN EXPERIMENTAL DEL NARDA SRM-3006 Y EL DETECT PROTECT 1206I

Para poder verificar el segundo objetivo específico de la investigación, se realizó un análisis cuantitativo de la relación existente entre la intensidad de campo emitida por el dispositivo RF-Clown v2, mediante el analizador de espectro Narda SRM 3006, y el nivel de alerta registrado por el detector de radiofrecuencia Protect 1206i.

Las mediciones se realizaron variando las distancias del RF-Clown y los instrumentos de medición mencionado en la documentación, manteniendo constantes las condiciones del escenario experimental, la orientación de las antenas y el modo de operación del dispositivo, en cada punto de medición se registró la intensidad de campo indicada por el narda SRM 3006 y el nivel de respuesta mostrada por el Protect 1206i, permitiendo establecer la relación existente entre ambas variables.

Los resultados obtenidos permiten determinar experimentalmente el comportamiento del detector frente a diferentes niveles de potencia, estimar su umbral de detección y evaluar la correspondencia entre ambas mediciones mediante un análisis de correlación estadística.

4.9.1 CORRELACIÓN CUANTITATIVA ENTRE EL NARDA SRM-3006 Y EL DETECT PROTECT 1206I

En esta sección se presentan los valores experimentales obtenidos de Wi-Fi para diferentes distancias entre el RF-Clown v2 y los equipos de medición. Los datos registrados permitieron comparar la intensidad de campo medida por el analizador Narda SRM-3006 con el nivel de alerta indicado por el Protect 1206i.

Tabla 7. Relación entre distancia, intensidad de campo y nivel de detección

Distancia (m)	Frecuencia (MHz)	Intensidad de campo (dBμV/m)	Nivel Protect (0– 16)
0	2404.34	125.71	16
0.5	2401.81	122.67	15
1.0	2411.14	115.61	6
2.0	2406.82	113.32	2
3.0	2406.92	104.48	0
4.0	2408.71	110.30	0
5.0	2409.75	98.98	0

La Tabla 7 presenta la relación entre la distancia de separación del RF-Clown v2 respecto a los equipos de medición, la intensidad de campo registrada mediante el analizador de espectro Narda SRM-3006 y el nivel de detección indicado por el Protect 1206i durante las pruebas realizadas en modo Wi-Fi.

Los resultados muestran que la mayor intensidad de campo se obtuvo a una distancia de 0 m, alcanzando un valor de 125,71 dB μ V/m, mientras que el Protect 1206i registró el nivel máximo de detección. Al incrementar la distancia hasta 0,5 m y 1 m, la intensidad de campo disminuyó a 122,67 dB μ V/m y 115,61 dB μ V/m, respectivamente, observándose simultáneamente una reducción en el nivel de detección indicado por el Protect.

A partir de los 2 m, el nivel de respuesta del Protect disminuyó considerablemente, registrándose un nivel de detección igual a 2, mientras que la intensidad de campo medida por el Narda SRM-3006 fue de 113,32 dB μ V/m. Finalmente, a partir de los 3 m el Protect 1206i dejó de registrar indicaciones de presencia de señal, aunque el Narda SRM-3006 continuó detectando emisiones del RF-Clown v2 con intensidades comprendidas entre 98,98 dB μ V/m y 110,30 dB μ V/m.

Este comportamiento demuestra que el analizador Narda SRM-3006 posee una sensibilidad significativamente mayor que el Protect 1206i, permitiendo detectar niveles de campo eléctrico que ya no generan respuesta en el detector portátil. En consecuencia, el Narda SRM-3006 constituye el instrumento de referencia para la caracterización cuantitativa de la señal, mientras que el Protect resulta adecuado como herramienta de detección rápida y localización preliminar de emisiones de radiofrecuencia.

4.9.2 DETERMINACIÓN DEL UMBRAL DE DETECCIÓN

A partir de los valores experimentales obtenidos fue posible identificar el nivel mínimo de intensidad de campo a partir del cual el Protect 1206i comienza a generar una indicación estable de presencia de señal de radiofrecuencia. Este valor constituye el umbral experimental de detección del dispositivo bajo las condiciones empleadas durante las pruebas.

Tabla 8. Descripción del umbral de determinación

Parámetro	Resultado experimental
Última distancia con detección	2 m
Intensidad de campo correspondiente	113,32 dB μ V/m
Primera distancia sin detección	3 m
Intensidad de campo correspondiente	104,48 dB μ V/m

Umbral experimental estimado	Entre 104,48 y 113,32 dB μ V/m
------------------------------	------------------------------------

A partir de los valores experimentales obtenidos fue posible identificar el intervalo de intensidad de campo a partir del cual el Protect 1206i deja de generar una indicación estable de presencia de señal de radiofrecuencia. Bajo las condiciones experimentales de esta investigación, el umbral de detección se encontró comprendido entre 104,48 dB μ V/m y 113,32 dB μ V/m, correspondiente al intervalo entre la última detección positiva y la primera ausencia de detección.

4.9.3 ANÁLISIS DE SENSIBILIDAD RESPECTO A LA DISTANCIA

La sensibilidad del Protect 1206i fue evaluada mediante el análisis de su capacidad para detectar las emisiones generadas por el RF-Clown v2 conforme se incrementó la distancia entre el transmisor y los equipos de medición. Para ello se comparó la intensidad de campo registrada por el analizador Narda SRM-3006 con el nivel de detección mostrado por el Protect 1206i, manteniendo constantes las condiciones del escenario experimental.

Tabla 9. Variación de la sensibilidad del Protect 1206i con la distancia

Distancia (m)	Intensidad de campo (dB μ V/m)	Nivel Protect	Sensibilidad observada
0.0	125.71	16	Muy alta
0.5	122.67	15	Muy alta
1.0	115.61	6	Alta
2.0	113.32	2	Baja
3.0	104.48	0	Sin detección
4.0	110.30	0	Sin detección
5.0	98.98	0	Sin detección

Los resultados muestran que la sensibilidad del Protect 1206i disminuye progresivamente conforme aumenta la distancia respecto al RF-Clown v2. Durante las pruebas experimentales se observó que el detector presentó su máxima sensibilidad en distancias comprendidas entre 0 m y 0,5 m, donde registró los niveles más altos de detección.

A una distancia de 1 m, aunque la intensidad de campo continuó siendo elevada (115,61 dB μ V/m), el nivel de detección disminuyó de forma considerable. Posteriormente, a 2 m, el detector únicamente registró un nivel de respuesta igual a 2, indicando una reducción significativa de su sensibilidad frente a la disminución de la intensidad del campo eléctrico.

A partir de los 3 m, el Protect 1206i dejó de generar indicaciones de detección, mientras que el analizador Narda SRM-3006 continuó registrando emisiones superiores a 98 dB μ V/m, evidenciando que el límite de sensibilidad del detector portátil es inferior al del instrumento de referencia empleado durante la caracterización experimental.

4.9.4 VERIFICACIÓN EXPERIMENTAL EN BLUETOOTH CLASSIC

Con el propósito de verificar si la relación observada entre la intensidad de campo y la respuesta del Protect 1206i durante las pruebas en modo Wi-Fi también se presenta en otros protocolos de la banda ISM de 2.4 GHz, se realizaron mediciones experimentales utilizando el modo Bluetooth Classic del RF-Clown v2. Las pruebas se efectuaron bajo las mismas condiciones experimentales, variando la distancia entre el transmisor y los equipos de medición.

Tabla 10. Valores obtenidos de la medición

Distancia (m)	Frecuencia (MHz)	Intensidad (dB μ V/m)	Nivel Protect
0.0	2404.00	126.67	16

0.5	2443.89	120.71	2
1.0	2440.44	117.78	0
2.0	2439.61	109.37	0
3.0	2438.47	108.58	0
4.0	2437.72	106.84	0
5.0	2436.18	101.05	0

Los valores registrados corresponden a mediciones experimentales reales obtenidas durante la operación del RF-Clown v2 en modo Bluetooth Classic. Se observó que el Protect 1206i presentó una respuesta máxima a una distancia de 0 m, con un nivel de detección igual a 16. Sin embargo, a 0,5 m el nivel disminuyó hasta 2 y, a partir de 1 m, el detector dejó de mostrar indicaciones de presencia de señal.

A pesar de esta reducción en la respuesta del Protect 1206i, el analizador Narda SRM-3006 continuó registrando intensidades de campo comprendidas entre 117,78 dB μ V/m y 101,05 dB μ V/m en las distancias de 1 m a 5 m. Este resultado indica que el Narda SRM-3006 posee una mayor sensibilidad de medición y que la respuesta del Protect no depende únicamente de la amplitud del campo eléctrico, sino también de las características temporales y espectrales de la señal generada en modo Bluetooth Classic.

La diferencia observada respecto al modo Wi-Fi puede asociarse al comportamiento discontinuo y al salto de frecuencia propio de Bluetooth, lo cual puede reducir la indicación promedio del detector portátil. En consecuencia, los resultados demuestran que el Protect 1206i presenta una sensibilidad dependiente del tipo de emisión analizada, mientras que el Narda SRM-3006 permite efectuar una medición cuantitativa más estable de la intensidad de campo.

4.9.5 VERIFICACIÓN EXPERIMENTAL EN BLUETOOTH LOW ENERGY (BLE)

Con el propósito de complementar la caracterización experimental del RF-Clown v2 en la banda ISM de 2.4 GHz, se realizaron mediciones utilizando el protocolo Bluetooth Low Energy (BLE). El procedimiento experimental se desarrolló bajo las mismas condiciones empleadas en las pruebas de Wi-Fi y Bluetooth Classic, manteniendo constante la configuración de los equipos de medición y variando únicamente la distancia entre el RF-Clown v2 y los instrumentos de evaluación.

Durante cada medición se registró la frecuencia de operación y la intensidad de campo eléctrico mediante el analizador de espectro Narda SRM-3006, mientras que el Protect 1206i permitió evaluar el nivel de detección de las emisiones generadas por el dispositivo. El objetivo fue analizar el comportamiento del sistema de medición frente a las señales BLE y comparar los resultados obtenidos con los observados en los demás protocolos evaluados.

Tabla 11. Valores obtenidos de los dispositivos

Distancia (m)	Frecuencia (MHz)	Intensidad (dBμV/m)	Nivel Protect
0.0	2440.20	130.0	16
0.5	2439.08	122.68	11
1.0	2438.57	118.60	4
2.0	2437.89	115.59	3
3.0	2437.50	110.83	2
4.0	2437.54	112.93	0
5.0	2437.46	108.61	0

Los resultados obtenidos durante las pruebas en modo Bluetooth Low Energy (BLE)

muestran una disminución progresiva de la intensidad de campo conforme aumenta la distancia entre el RF-Clown v2 y los equipos de medición. El analizador Narda SRM-3006 registró intensidades comprendidas entre 130,00 dB μ V/m y 108,61 dB μ V/m, confirmando la presencia de emisiones durante todas las mediciones experimentales.

En cuanto al Protect 1206i, se observó una disminución gradual del nivel de detección desde un valor máximo de 16 a una distancia de 0 m, hasta un valor de 2 a 3 m. A partir de 4 m, el detector dejó de registrar indicaciones de presencia de señal, aunque el Narda SRM-3006 continuó midiendo intensidades superiores a 108 dB μ V/m.

Comparando estos resultados con los obtenidos en modo Wi-Fi y Bluetooth Classic, se evidencia que el comportamiento del Protect 1206i depende del protocolo de comunicación analizado. En las pruebas realizadas, el modo BLE presentó un comportamiento intermedio, manteniendo la detección a mayores distancias que Bluetooth Classic, aunque inferior al comportamiento observado durante las pruebas en modo Wi-Fi.

4.9.6 COEFICIENTE DE CORRELACIÓN

Con el propósito de cuantificar la relación existente entre la intensidad de campo medida por el analizador de espectro Narda SRM-3006 y el nivel de detección registrado por el Protect 1206i, se realizó un análisis estadístico mediante el coeficiente de correlación de Pearson. Para este análisis se emplearon las veintiún (21) mediciones experimentales obtenidas durante las pruebas efectuadas en los protocolos Wi-Fi, Bluetooth Classic y Bluetooth Low Energy (BLE). El objetivo fue determinar el grado de asociación lineal entre ambas variables y comprobar cuantitativamente el comportamiento observado durante la caracterización experimental del RF-Clown v2.

El coeficiente de correlación de Pearson se calculó mediante la siguiente expresión:

$$r = \frac{\sum_{i=1}^n (x_i - \bar{x}) (y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2 \sum_{i=1}^n (y_i - \bar{y})^2}}$$

Donde:

r: coeficiente de correlación de Pearson.

x_i : intensidad de campo medida por el Narda SRM-3006 (dB μ V/m).

y_i : nivel de detección registrado por el Protect 1206i.

$\bar{x}$: promedio de la intensidad de campo.

$\bar{y}$: promedio del nivel de detección.

n: número de observaciones experimentales (21).

Tabla 12. Resultado del análisis de correlación entre la intensidad de campo y el nivel de detección

Parámetro	Resultado
Método estadístico	Coeficiente de correlación de Pearson
Número de mediciones	21
Variable independiente	Intensidad de campo (dB μ V/m)
Variable dependiente	Nivel Protect
Coeficiente de correlación (r)	0,8344
Coeficiente de determinación (R ²)	0,696
Interpretación	Correlación positiva fuerte

Correlacionar las mediciones obtenidas mediante el Narda SRM-3006 con los niveles registrados por el Detect Protect 1206i

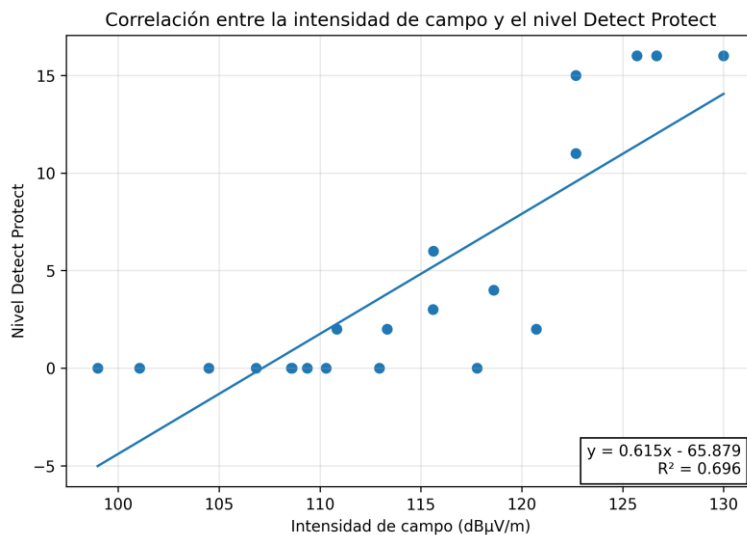


Fig. 56. Diagrama de dispersión entre la intensidad de campo medida por el Narda SRM-3006 y el nivel de detección registrado por el Detect Protect 1206i

La Figura 56 presenta el diagrama de dispersión obtenido a partir de las veintiún (21) mediciones experimentales realizadas durante las pruebas con los protocolos Wi-Fi, Bluetooth Classic y Bluetooth Low Energy (BLE). En el eje horizontal se representa la intensidad de campo eléctrico medida por el analizador de espectro Narda SRM-3006, mientras que en el eje vertical se muestra el nivel de detección registrado por el Protect 1206i.

Los resultados evidencian una tendencia lineal positiva entre ambas variables, indicando que, a medida que aumenta la intensidad del campo electromagnético, el nivel de detección registrado por el Protect 1206i también tiende a incrementarse. Esta relación se confirma mediante el coeficiente de correlación de Pearson obtenido ($r = 0,834$), valor que corresponde a una correlación positiva fuerte de acuerdo con los criterios estadísticos comúnmente aceptados.

De igual manera, el coeficiente de determinación ($R^2 = 0,696$) indica que

aproximadamente el 69,6 % de la variabilidad observada en los niveles registrados por el Protect 1206i puede explicarse por la intensidad de campo medida mediante el Narda SRM-3006. El porcentaje restante (30,4 %) puede atribuirse a factores propios del comportamiento de los protocolos inalámbricos evaluados, tales como las técnicas de modulación, los mecanismos de salto de frecuencia presentes en Bluetooth Classic y BLE, las variaciones propias del entorno de medición y la sensibilidad del Protect 1206i frente a diferentes tipos de emisiones electromagnéticas.

La distribución de los puntos experimentales muestra que, aunque existe una tendencia general creciente, no todos los datos se encuentran exactamente sobre la línea de regresión. Este comportamiento era esperable debido a que las mediciones fueron realizadas sobre tres protocolos de comunicación diferentes, cada uno con características particulares de transmisión, lo que introduce una variabilidad natural en la respuesta del detector portátil sin afectar la tendencia general observada.

Los resultados obtenidos permiten validar experimentalmente la relación existente entre ambas variables, demostrando que el Narda SRM-3006 constituye un instrumento de referencia adecuado para la caracterización cuantitativa de las emisiones de radiofrecuencia generadas por el RF-Clown v2, mientras que el Protect 1206i proporciona una respuesta consistente para la detección rápida de fuentes de radiofrecuencia dentro de su rango operativo.

Para finalizar, el análisis de correlación permite verificar cuantitativamente el segundo objetivo específico de la investigación, confirmando que existe una relación positiva entre la intensidad de campo medida por el Narda SRM-3006 y el nivel de detección registrado por el Protect 1206i. Aunque la respuesta del detector presenta variaciones dependiendo del protocolo

inalámbrico empleado, la tendencia global demuestra que un incremento en la intensidad del campo electromagnético genera, en términos generales, un aumento en el nivel de detección registrado por el equipo portátil.

4.10 EVALUACIÓN DEL COMPORTAMIENTO ELÉCTRICO, TÉRMICO Y ESTABILIDAD OPERATIVA

Para la evaluación experimental se utilizaron dos instrumentos de medición. Un multímetro digital tipo pinza Digital Clamp Meter 266C, empleado para la medición de la temperatura mediante el sensor tipo K, y un multímetro digital Fluke 15B+, utilizado para la medición del voltaje y la corriente continua consumida por el dispositivo durante los diferentes modos de operación. A partir de las mediciones de voltaje y corriente se calculó la potencia eléctrica consumida por el RF-Clown v2, permitiendo complementar la evaluación de su comportamiento eléctrico y térmico.

4.10.1 PROCEDIMIENTO EXPERIMENTAL DE MEDICIÓN

Para evaluar el comportamiento eléctrico se utilizó un multímetro digital configurado en la escala de 20 V de corriente continua. La medición se realiza en paralelo entre el punto positivo de alimentación y tierra del RF-Clown v2.

Durante todo el procedimiento se mantuvieron constantes el puerto USB, el cable de alimentación, la posición del dispositivo y los puntos de contacto de las puntas del multímetro. Inicialmente se registró el voltaje con el dispositivo encendido y sin ningún modo operativo activado. Posteriormente, se realizaron mediciones durante la operación de los modos Wi-Fi, Bluetooth Classic y BLE.

Para la evaluación térmica se utiliza un medidor de temperatura superficial. Las mediciones se efectuaron manteniendo una distancia y punto de referencia similares, con la finalidad de reducir las variaciones ocasionadas por la posición del instrumento. Se toma en consideración la temperatura ambiente y la temperatura alcanzada por el dispositivo durante la ejecución de cada modo operativo.

Las pruebas se realizaron dentro de un entorno controlado y con el RF-Clown v2 como única fuente intencional de emisión durante el ensayo.

4.10.2 EVALUACIÓN DEL CONSUMO ELÉCTRICO

Para evaluar el comportamiento eléctrico del RF-Clown v2 se utiliza un multímetro digital Fluke 15B+, configurado para la medición de corriente continua (DC). El instrumento se conectó en serie con la alimentación del dispositivo para registrar la corriente consumida durante los diferentes modos de operación. Simultáneamente se verificó el voltaje de alimentación, permitiendo calcular la potencia eléctrica mediante la ecuación:

$$P = V \times I$$

Tabla 13. Cálculo de la potencia

Estado de operación	Voltaje (V)	Corriente (A)	Potencia (W)
Reposo	5.09	0.029	0.148
Wi-Fi	4.56	0.030	0.137
Bluetooth Classic	4.72	0.030	0.142
Bluetooth Low Energy (BLE)	4.70	0.030	0.141

Los valores registrados evidencian que la corriente consumida por el RF-Clown v2 se

mantuvo prácticamente constante, entre 0.029 A y 0.030 A. La potencia eléctrica calculada varió entre 0.137 W y 0.148 W, lo cual indica un consumo reducido y estable durante los distintos modos de operación. La mayor potencia se presentó en estado de reposo, asociada al mayor voltaje de alimentación registrado mientras que, en los modos Wi-Fi, Bluetooth Classic y BLE las diferencias fueron mínimas.

Mediciones eléctricas

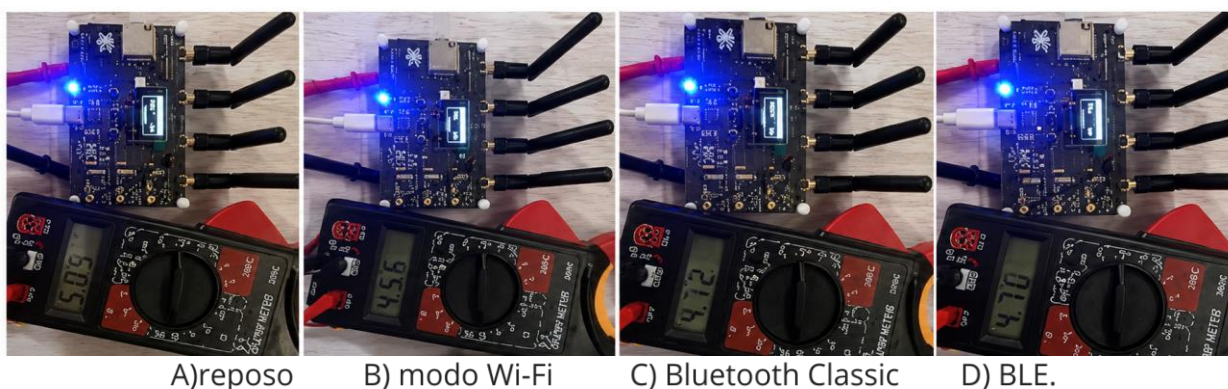


Fig. 57. Medición de escenario voltaje

4.10.3 EVALUACIÓN TÉRMICA DURANTE ENCENDIDO CONTINUO

Con el propósito de evaluar el comportamiento térmico del RF-Clown v2 durante su funcionamiento, se monitoreó la temperatura superficial del microcontrolador ESP32 y de los tres módulos transceptores nRF24L01+ mediante un sensor de temperatura tipo K conectado a un multímetro Digital Clamp Meter 266C. Las mediciones se realizaron desde el instante previo al encendido hasta los 20 minutos de operación continua, registrando también la temperatura ambiente durante toda la prueba.

Tabla 14. Evolución de la temperatura superficial del RF-Clown v2 durante el encendido

en reposo, sin activar un modo de interferencia.

Tiempo (min)	Ambiente (°C)	ESP32 (°C)	nRF24L01+ 1 (°C)	nRF24L01+ 2 (°C)	nRF24L01+ 3 (°C)
Antes de encender	24	24	24	24	24
5	25	27	29	29	29
10	25	28	29	30	30
15	24	29	29	30	30
20	24	29	30	30	30

Los resultados muestran que la temperatura ambiente permaneció prácticamente constante entre 24 °C y 25 °C durante toda la evaluación, lo que permitió minimizar la influencia de factores externos sobre las mediciones.

Antes del encendido, todos los componentes se encontraban a una temperatura cercana a la del ambiente (24 °C). Una vez iniciado el funcionamiento del dispositivo, se observó un incremento gradual de la temperatura del ESP32, alcanzando 29 °C al finalizar la prueba. De manera similar, los módulos nRF24L01 incrementaron su temperatura hasta valores cercanos a 30 °C, manteniendo un comportamiento uniforme entre los tres transceptores.

Estos resultados evidencian que durante el periodo inicial de funcionamiento el RF-Clown v2 presentó un incremento térmico moderado, sin observar diferencias significativas entre los módulos de radio ni indicios de sobrecalentamiento.

4.10.4 EVALUACIÓN DE ESTABILIDAD OPERATIVA

Los resultados presentados en las Tablas 14 y 15 corresponden a condiciones experimentales diferentes y, por tanto, no deben compararse como si pertenecieran a un mismo

ensayo. La Tabla 14 representa el comportamiento térmico inicial del RF-Clown v2 encendido y sin un modo de interferencia activado, condición en la cual las temperaturas superficiales de los componentes se mantuvieron próximas a 30 °C. En cambio, la Tabla 15 corresponde a una prueba independiente con el modo Wi-Fi activado de manera continua. En este segundo ensayo, las mediciones se realizaron directamente sobre la superficie de los tres módulos nRF24L01+, registrándose temperaturas cercanas a 60 °C debido a la actividad continua de los transceptores. La diferencia observada se relaciona, por tanto, con el modo de operación y el punto específico de medición.

Tabla 15. Comportamiento térmico del RF-Clown v2 durante la operación continua en modo Wi-Fi.

Tiempo (min)	Ambiente (°C)	ESP32 (°C)	nRF24L01+1 (°C)	nRF24L01+ 2 (°C)	nRF24L01+ 3 (°C)
5	25	29	60	60	60
10	25	32	60	60	60
15	25	34	60	58	57
20	25	33	50	48	46

Durante la prueba con el modo Wi-Fi activado se observó un incremento de la temperatura superficial de los componentes. El ESP32 alcanzó una temperatura máxima de 34 °C, mientras que los módulos nRF24L01+ registraron valores máximos cercanos a 60 °C. Estos resultados corresponden exclusivamente al ensayo realizado con transmisión continua y no representan la temperatura del dispositivo en estado de reposo.

La evaluación de estabilidad operativa se realizó únicamente en modo Wi-Fi. Los resultados obtenidos corresponden exclusivamente a esta condición y no constituyen una

validación prolongada de los demás modos operativos del RF-Clown v2.

Medición de temperatura durante la operación del RF-Clown v2

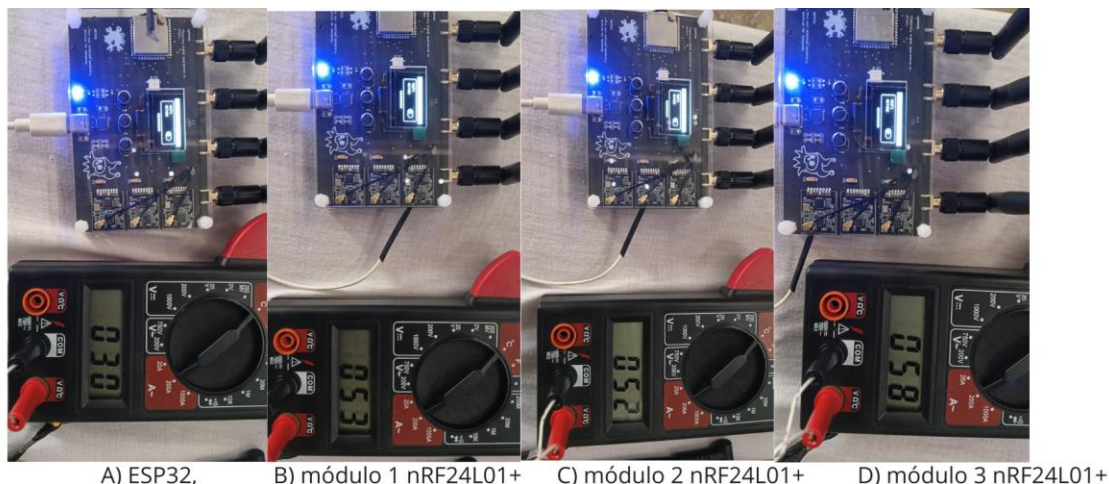


Fig. 58. Escenario de medición de temperatura

Las mediciones mostraron variaciones térmicas durante la operación continua en modo Wi-Fi. A pesar del incremento registrado en los módulos nRF24L01+, durante el periodo evaluado no se observaron reinicios, bloqueos ni fallas funcionales del dispositivo.

4.10.5 COMPORTAMIENTO TÉRMICO DESPUÉS DE LA DESACTIVACIÓN

Con el objetivo de analizar la disipación térmica del RF-Clown v2, el registro de enfriamiento se inició inmediatamente después de desactivar el modo Wi-Fi. Debido al uso de un único sensor de temperatura tipo K, las mediciones del ESP32 y de los tres módulos nRF24L01+ se realizaron de forma secuencial y no simultánea. Durante el desplazamiento y colocación del sensor sobre cada componente comenzó el proceso de disipación térmica, favorecido por la temperatura controlada del laboratorio. Por esta razón, el registro de 0 minutos conserva los últimos valores obtenidos durante la operación continua y se utiliza como referencia inicial para analizar el descenso posterior de la temperatura.

Tabla 16. *Registro después de la desactivación*

Tiempo después del apagado	ESP32 (°C)	nRF24L01+ 1 (°C)	nRF24L01+ 2 (°C)	nRF24L01+ 3 (°C)
0 minuto	33	50	48	46
1 minuto	28	35	34	34
3 minutos	27	30	29	29
5 minutos	26	30	29	29

Después de desactivar el modo Wi-Fi se observó una disminución progresiva de la temperatura en todos los componentes evaluados. El ESP32 redujo su temperatura desde 33 °C hasta 26 °C durante los cinco minutos posteriores a la desactivación.

De igual forma, los tres módulos nRF24L01+ disminuyeron desde valores iniciales comprendidos entre 46 °C y 50 °C hasta aproximadamente 29 °C y 30 °C. Este comportamiento evidencia la disipación gradual del calor acumulado durante la operación continua.

4.11 EVALUACIÓN DE VIABILIDAD REGULATORIA BAJO LA NORMATIVA DE LA ARCOTEL

El diseño y operación del dispositivo RF-Clown v2 se contrastó con la Norma Técnica para el Uso de Equipos de Sistemas de Modulación Digital y de Banda Ancha en la Banda de Frecuencias de 2400 MHz a 2483,5 MHz, emitida por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) de la República del Ecuador.

Límites de potencia: la normativa ecuatoriana establece que para dispositivos que operen en la banda libre ISM de 2.4 GHz mediante técnicas de modulación digital o espectro ensanchado (FHSS/DSSS), la potencia máxima de salida del transmisor no debe exceder de 1

Vatio (1000 mW o +30 dBm), y la Potencia Isótropa Radiada Equivalente (P.I.R.E.) máxima permitida es de +36 dBm.

Cumplimiento técnico: de acuerdo con las mediciones espectrales directas capturadas por el analizador Narda SRM-3006, los niveles de potencia pico del RF-Clown v2 promediaron entre los -55 dBm y -64 dBm en la zona de acoplamiento. Incluso considerando las pérdidas de propagación en el espacio libre (FSPL) y la ganancia de las antenas dipolo utilizadas, la potencia efectiva de transmisión del hardware base (ESP32 + transceptores nRF24L01+) se mantiene en el rango de los mili vatios (mW), operando muy por debajo de los límites restrictivos de la ARCOTEL.

Los resultados obtenidos permiten caracterizar el comportamiento del RF-Clown v2 únicamente dentro de un entorno experimental controlado. Debido a que su funcionamiento genera interferencia intencional y puede afectar las comunicaciones inalámbricas cercanas, su operación debe limitarse a ambientes aislados, supervisados y autorizados, evitando cualquier afectación a sistemas de telecomunicaciones externos.

4.11.1 ESTIMACIÓN DE LA POTENCIA ISOTRÓPICA RADIADA EQUIVALENTE (PIRE)

El RF-Clown v2 incorpora tres módulos de radio GT24 Mini compatibles con el transceptor nRF24L01+. Estos módulos integran etapas de amplificación PA/LNA y presentan una potencia máxima nominal de transmisión de 20 dBm, equivalente aproximadamente a 100 mW por módulo. Asimismo, el sistema dispone de cuatro conexiones IPEX para la instalación de antenas externas de 8 dBi.

La Potencia Isotrópica Radiada Equivalente se determinó mediante la expresión:

$$PIRE = P_{TX} - L_{IPEX} + G_{antena}$$

donde P_{TX} corresponde a la potencia máxima del transmisor, L_{IPEX} representa las pérdidas introducidas por el cable y los conectores IPEX-SMA, y G_{antena} corresponde a la ganancia nominal de la antena.

Debido a que no se dispone del valor certificado de pérdida de los cables IPEX instalados, se calculó inicialmente el límite máximo teórico considerando pérdidas nulas:

$$PIRE_{max} = 20 \text{ dBm} - 0 \text{ dB} + 8 \text{ dBi}$$

$$PIRE_{max} = 28 \text{ dBm}$$

Tabla 17. Parámetros del sistema de transmisión

Parámetro	Valor	Unidad
Número de módulos GT24 Mini	3	Módulos
Potencia máxima por módulo	20	dBm
Potencia máxima por módulo	100	mW
Ganancia nominal de cada antena	8	dBi
Tipo de conexión	IPEX-SMA	—
Pérdida exacta del cable IPEX	No determinada	dB
$PIRE_{m\acute{a}xima}$ teórica por cadena	28	dBm
$PIRE_{m\acute{a}xima}$ equivalente por cadena	631	mW

El valor de 28 dBm corresponde a la PIRE máxima teórica de cada módulo GT24 Mini

conectado a su respectiva antena, y no a la suma de los tres transmisores. Las potencias no deben sumarse directamente, debido a que los módulos funcionan como cadenas independientes y no constituyen un arreglo de antenas sincronizado.

La presencia de cables IPEX implica pérdidas adicionales entre el módulo y la antena, por lo que la PIRE real será ligeramente inferior a 28 dBm. En consecuencia, dicho resultado debe interpretarse como un límite superior teórico basado en los valores nominales proporcionados por el fabricante.

4.12 CONCLUSIONES

La caracterización experimental permitió verificar que el RF-Clown v2 genera interferencias capaces de afectar el funcionamiento de enlaces inalámbricos que operan en la banda ISM de 2.4 GHz. Durante las pruebas experimentales se observaron pérdidas de conectividad y degradación funcional del enlace en los diferentes modos evaluados.

En relación con el comportamiento eléctrico, el RF-Clown v2 presentó un consumo estable durante los modos evaluados, sin variaciones significativas de corriente y potencia. La evaluación térmica prolongada y la estabilidad operativa se analizaron específicamente durante la operación continua en modo Wi-Fi.

Bajo esta condición experimental no se observaron reinicios, bloqueos, fallos en la pantalla OLED ni pérdidas de comunicación interna. En consecuencia, la estabilidad observada corresponde exclusivamente al modo Wi-Fi y al periodo evaluado, por lo que estos resultados no deben extrapolarse a los demás modos sin realizar ensayos prolongados independientes.

5 BIBLIOGRAFÍAS

- [1] wikipedia, «Banda ISM,» 21 jun 2025. [En línea]. Available:
https://es.wikipedia.org/wiki/Banda_ISM.
- [2] G. Hardesty, «Data-Alliance,» 2024. [En línea]. Available: https://www.data-alliance.net/es/bluetooth-de-baja-energ%C3%ADa-ble-en-comparaci%C3%B3n-con-bluetooth-para-internet-de-las-cosas?srsId=AfmBOop1t4ArIMH4FhRihzUQegapmwVTZTNcGIcnjG0qZoBbD54_pIGG. [Último acceso: 14 04 2026].
- [3] &. F. R. G. Mejia Ojeda, «Caracterización del impacto de la interferencia electromagnética en redes inalámbricas,» 2025. [En línea]. Available:
<http://hdl.handle.net/20.500.14067/12653>.
- [4] M. Barrera, «Seguridad de las comunicaciones inalámbricas en los sistemas de transporte inteligente,» 2022. [En línea]. Available:
<https://hdl.handle.net/2117/373763>.
- [5] P. E. Bonilla Totoy, «Simulación de coexistencia e interferencia de 802.11 ah y Bluetooth LE para la interconexión de dispositivos de IOT,» 2022. [En línea]. Available: <http://dspace.unach.edu.ec/handle/51000/8606>.
- [6] A. D. I. G. &. C. KG, «A1 Digital Knowledge Hub,» 09 septiembre 2024. [En línea]. Available: <https://www.a1.digital/es/knowledge-hub/protocolos-iot-una->

guia-completa-para-las-empresas/.

- [7] W. Castle, «Comprensión de las bandas ISM de 2,4 GHz: una guía práctica para todos,» 29 11 2024. [En línea]. Available: https://wraycastle.com/es/blogs/knowledge-base/2-4-ghz-ism?srsId=AfmBOopJsEs8irBFWGsIqLLrBy0I8xUuobd6FRjiYp_d0MCnBh1TGt37.
- [8] cifertech, «RF-Clown: Tu herramienta portátil para bloquear señales ...,» 30 12 2024. [En línea]. Available: <https://cifertech.net/rf-clown-your-portable-ble-bluetooth-jamming-tool/>. [Último acceso: 14 04 2026].
- [9] A. G. ., O. I. ., B. N. ., F. V. Gwendoline Hochet Derebianckine, «Odio o amor en la banda ISM de 2,4 GHz: La historia de LoRa e IEEE 802.11g,» 19 11 2025. [En línea]. Available: <https://dl.acm.org/doi/abs/10.1145/3743688>.
- [10] V. A. D. Soto Vera, «Estudio Espectral sobre la congestión en los canales de las bandas ISM 2.4 y 5 GHz en Cerro Azul y centro de la ciudad de Guayaquil con un alcance máximo de 1 Km,» 2022. [En línea]. Available: <http://www.dspace.espol.edu.ec/handle/123456789/57588>.
- [11] C. D. B. T. Radicelli García, «Simulación de coexistencia e interferencia de 802.11ah y Bluetooth LE para la interconexión de dispositivos de IOT,» 19 01 2022. [En línea]. Available: <http://dspace.unach.edu.ec/handle/51000/8606>.
- [1] E. H. L. Martínez, «GUIA PARA EL PROCESO DE AUDITORIA

- 2] INFORMATICA EN PYMES, BASADO EN LA NORMA ISO/IEC 27001, MEDIANTE EL USO DE HERRAMIENTAS DE CODIGO LIBRE.,» 03 2025. [En línea]. Available: <http://repositorio.uisrael.edu.ec/handle/47000/4307>.
- [1 H. R. L.Vallozzi, «Últimos avances en el campo de las antenas textiles.,» [En
3] línea]. Available: <https://www.sciencedirect.com/topics/engineering/radiation-pattern>. [Último acceso: 12 05 2026].
- [1 M. V. Ordoñez Cabrera, «Estudio de la ocupación del espectro radioeléctrico
4] en las bandas ISM (Industrial, Scientific and Medical) para redes LPWAN (Low Power Wide Area Network) con visión a la transformación de Loja como ciudad inteligente,» 29 04 2025. [En línea]. Available: <https://dspace.unl.edu.ec/handle/123456789/32501>.
- [1 S. E. -. U. Berkeley, «ZigBee (IEEE 802.15.4),» 17 septiembre 2004. [En
5] línea]. Available: <http://pages.cs.wisc.edu/~suman/courses/707/papers/zigbee.pdf>.
- [1 N. G. Agudelo Cristancho, «Sistema de interoperabilidad para tecnologías
6] celulares e inalámbricas establecidas en los estándares IEEE 802.15.1, IEEE 802.15.4, IEEE 802.11,» 2021. [En línea]. Available: <http://hdl.handle.net/11349/29290>.
- [1 R. G. Portillo Criado, «Estudio en detalle y evaluacion de protocolo BLE
7] Mesh,» 10 06 2018. [En línea]. Available: <https://hdl.handle.net/10609/80565>.
- [1 C. W. P. H. y. S. C. Tom Preston-Werner, «github,» 25 octubre 2025. [En

- 8] línea]. Available: <https://github.com/cifertech/RF-Clown/releases>.
- [1 CiferTech, «RF-Clown v2: La bestia inalámbrica acaba de recibir un impulso
- 9] turbo.,» 27 octubre 2025. [En línea]. Available: <https://cifertech.net/rf-clown-v2-the-wireless-beast-just-got-a-turbo-boost/>.
- [2 naylampMechatronics, «ESP32-WROVER - ESP32 WiFi,» [En línea].
- 0] Available: <https://naylampmechatronics.com/espressif-esp/1249-esp32-wrover-esp32-wifi.html>. [Último acceso: 22 05 2026].
- [2 naylampmechatronics, «Módulo RF 2.4GHz - NRF24L01+PA+LNA con
- 1] Antena,» 2023. [En línea]. Available: <https://naylampmechatronics.com/inalambrico/113-modulo-rf-nrf24l01-pa-lna-antena.html>.
- [2 MEGATRONICA, «Pantalla Oled 128×64 I2c Display Lcd 0.96 Azul VCC
- 2] GND Arduino SSD1306,» [En línea]. Available: https://megatronica.cc/producto/pantalla-oled-128x64-i2c-display-lcd-0-96-azul-vcc-gnd-arduino/?srsltid=AfmBOopiU4_XwqRPtrbrJKTqOmHGb6q7pG9NS9t4Jja37Aeb1ULXpg16. [Último acceso: 22 05 2026].
- [2 n. s. t. soluciones, «SRM-3006 - frequency-selective EMF measurement up to
- 3] 29.5 GHz,» [En línea]. Available: <https://www.narda-sts.com/en/products/emf-measuring-devices-and-solutions/srm-3006/>. [Último acceso: 25 mayo 2026].

- [2 E. iProtect® Tecnología de Shopify, «Protect 1206i,» 2024. [En línea].
4] Available: <https://digiscan-labs.com/es/products/protect-1206i/>.
- [2 IEEE, «IEEE Standard for Information Technology--Telecommunications and
5] Information Exchange between Systems - Local and Metropolitan Area Networks--
Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and
Physical Layer (PHY) Specifications,» 2020. [En línea]. Available:
<https://standards.ieee.org/ieee/802.11/7028/>. [Último acceso: 16 09 2025].
- [2 OpenAirInterface, «Relacionado con la implementación y validación de
6] handover usando OpenAirInterface (OAI) en SDR para LTE, incluyendo GNU
Radio y escenarios de movilidad, demostrando viabilidad en redes avanzadas.,»
2020. [En línea]. Available:
[https://github.com/OPENAIRINTERFACE/openairinterface5g/blob/develop/doc/han
dover-tutorial.md](https://github.com/OPENAIRINTERFACE/openairinterface5g/blob/develop/doc/handover-tutorial.md).
- [2 sukasa, «Apple Audífonos Inalámbricos Bluetooth AirPods Pro 2 Blanco,»
7] [En línea]. Available: [https://www.sukasa.com/productos/apple-audifonos-
inalambricos-bluetooth-airpods-pro-2-blanco/05f494b0-c64d-48d2-9f64-
49eea0dcc2bb](https://www.sukasa.com/productos/apple-audifonos-inalambricos-bluetooth-airpods-pro-2-blanco/05f494b0-c64d-48d2-9f64-49eea0dcc2bb). [Último acceso: 22 05 2026].
- [2 naylamp. [En línea]. Available: [https://naylampmechatronics.com/espressif-
8\] esp/1250-esp32-devkit-v1-nodemcu-32-30-pin-esp32-wifi-usb-c.html](https://naylampmechatronics.com/espressif-esp/1250-esp32-devkit-v1-nodemcu-32-30-pin-esp32-wifi-usb-c.html). [Último
acceso: 22 05 2026].
- [2 cifer, «github,» [En línea]. Available: <https://github.com/cifertech/RF->

- 9] Clown/blob/main/Schematic/rfclown-Schematic.jpg. [Último acceso: 14 06 2026].
- [3 arduinel, «MÓDULO INALÁMBRICO NRF24L01 PA LNA CON
- 0] ANTENA,» [En línea]. Available: <https://ventas.ardunel.com.bo/modulos/205-modulo-inalambrico-nrf24l01-pa-lna-con-antena-de-1100-metros-de-larga-distancia.html>. [Último acceso: 25 6 2026].

ANEXOS



Fig. 59. Colocación de antenas en el Narda

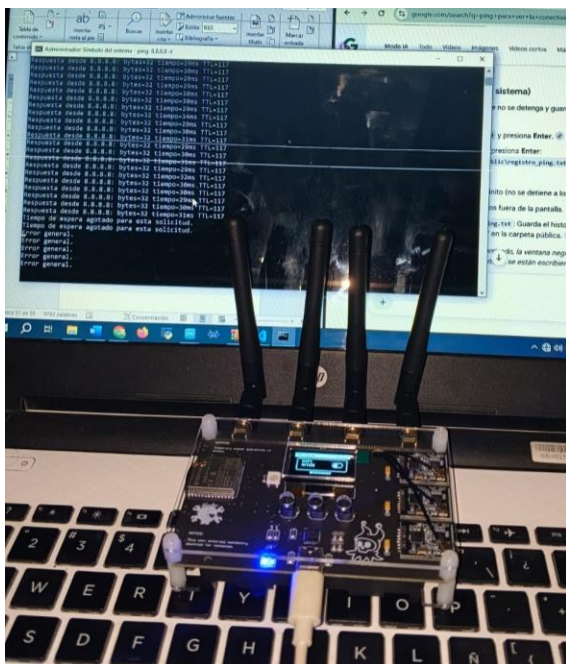


Fig. 61. Conexión interferida

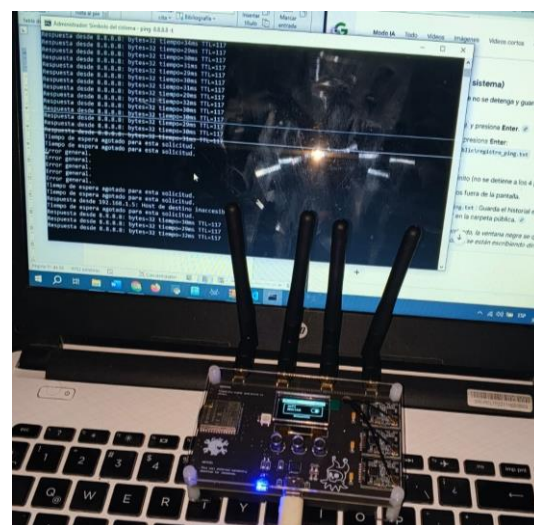


Fig. 60. Conexión restablecida



Fig. 63. Barras de niveles cuando está cerca la señal

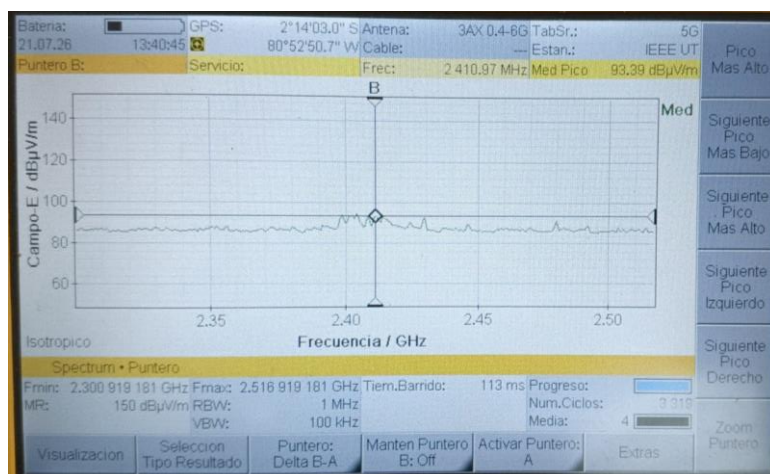


Fig. 62. Señal sin interferencia



Fig. 64. Señal con interferencia