
**UNIVERSIDAD CENTRAL "MARTA ABREU" DE LAS VILLAS**

**FACULTAD DE INGENIERIA ELÉCTRICA**

**DEPARTAMENTO DE ELECTRÓNICA Y TELECOMUNICACIONES**

# Evaluación de los algoritmos de *rendezvous* ciego para redes radio cognitivas ante interferencias

**Tesis presentada en opción al Título Académico de Máster en Telemática**

**Maestría en Telemática**

Autor: Ing. Yaime Fernández Jiménez

Tutor: Dr. C. Erik Ortiz Guerra

**Santa Clara, Cuba, 2016**

# PENSAMIENTO

*“La luz está en ti; desde esa luz se alumbra el camino”*

*Enrique Agilda*

# RESUMEN

La radio cognitiva es una tecnología cuyo objetivo fundamental es lograr una utilización eficiente y racional de los recursos de radio. El proceso de *rendezvous*, permite a los usuarios cognitivos encontrar un canal disponible y establecer un enlace de comunicación. Debido a la naturaleza inalámbrica de estas redes, al igual que los usuarios cognitivos un usuario con intenciones maliciosas o no puede acceder directamente al medio e interferir en el proceso de *rendezvous*. Las interferencias pueden disminuir el rendimiento de las comunicaciones o interrumpirlas. La implementación de algoritmos de *rendezvous* que minimicen el tiempo de *rendezvous* y mitiguen las interferencias, es un desafío en este contexto.

En esta investigación se evalúa el desempeño de los algoritmos de *rendezvous* ciego: Aleatorio, *Jump-Stay* (JS) y *Short Sequence Based* (SSB) ante interferencias de un usuario aleatorio. Además se evalúa el desempeño del algoritmo SSB ante interferencias de un usuario malicioso adaptable. Para ello se caracteriza la tecnología radio cognitiva, los algoritmos de *rendezvous* ciego y las diferentes estrategias de ataque de usuarios maliciosos. Las evaluaciones se realizaron en términos de tiempo de *rendezvous* esperado, tiempo de *rendezvous* máximo y porciento de incidencias del usuario interferente con uno y con ambos usuarios cognitivos. Los resultados obtenidos muestran que ante interferencias de un usuario aleatorio el algoritmo JS es robusto, mientras el algoritmo SSB es el de peor desempeño. Ante interferencias de un usuario malicioso adaptable, el desempeño del algoritmo SSB es próximo a su desempeño ante interferencias de un usuario aleatorio, pero menor.

**Palabras Clave:** radio cognitiva, *rendezvous* ciego, interferencias.

# LISTA DE ACRÓNIMOS

| | |
|---|---|
| ACK | *Acknowledgement* |
| AMRCC | *Adaptative Multiple Rendezvous Control Channel* |
| ASYNC-ETCH | *Asynchronous-Efficient Channel Hopping* |
| CCC | *Common Control Channel* |
| CH | *Channel Hopping* |
| CR | *Cognitive radio* |
| CRN | *Cognitive Radio Network* |
| CRSEQ | *Channel Rendezvous Sequence* |
| CSMA/CA | *Carrier Sense Multiple Access /Collision Avoidance* |
| DRSEQ | *Deterministic Rendezvous Sequence* |
| DSA | *Dynamic Spectrum Access* |
| EJS | *Deterministic Rendezvous Sequence* |
| ETTR | *Expected Time to Rendezvous* |
| FCC | *Federal Communications Commission* |
| FRCH | *Fast Rendezvous Channel Hopping* |
| GOS | *Generated Orthogonal Sequences* |
| IEEE | *Institute of Electrical and Electronics Engineers* |
| ISM | *Industrial, Scientific and Medical* |
| JS | *Jump-Stay* |
| MAC | *Medium Access Control* |
| MC | *Modular Clock* |

| | |
|---|---|
| MCTTR | *Maximum Conditional Time to Rendezvous* |
| MMC | *Modified Modular Clock* |
| MTTR | *Maximum Time to Rendezvous* |
| PUE | *Primary User Emulation* |
| QoS | *Quality of Service* |
| SSB | *Short Sequence Based* |
| SSCH | *Slotted Seeded Channel Hopping* |
| TDMA | *Time Division Multiple Access* |
| TTR | *Time to Rendezvous* |
| UP | Usuario (s) primario (s) |
| US | Usuario (s) secundario (s) |

# ÍNDICE

# INTRODUCCIÓN

El desarrollo de nuevos dispositivos inalámbricos y la necesidad de brindar nuevos servicios de radio durante los últimos años ha provocado el agotamiento de las bandas de frecuencia de interés práctico para las radio comunicaciones [1]. La asignación del espectro es realizada por agencias reguladoras que destinan diferentes bandas de frecuencia para tecnologías o servicios específicos, por ejemplo: la difusión de radio y televisión. Esta asignación es realizada de manera fija y sólo se exceptúan un pequeño conjunto de bandas de frecuencias como la banda Industrial, Científica y Médica (ISM: *Industrial, Scientific and Medical*) [2].

Estudios recientes demuestran que el uso del espectro no es homogéneo ni eficiente [3]. Mientras ciertas bandas se encuentran congestionadas o sometidas a un uso intensivo, otras regiones del espectro se hallan infrautilizadas. La necesidad del uso óptimo del espectro electromagnético sugiere la incursión en nuevas políticas flexibles y dinámicas de asignación de recursos radioeléctricos [4]-[2].

Propuesta originalmente por *Joseph Mitola* en [5], como una tecnología capaz de integrar la radio definida por software con técnicas de inteligencia computacional, tales como el razonamiento basado en modelos y el aprendizaje automático; la radio cognitiva (CR, *Cognitive Radio*) representa en la actualidad un paradigma de las comunicaciones inalámbricas en el cual el objetivo fundamental es el uso eficiente y racional de los recursos de radio. En radio cognitiva cada usuario cognitivo o usuario secundario (US), tiene uno o más radios capaces de explorar el espectro y detectar porciones que no han sido utilizadas por usuarios licenciados de estos canales o usuarios primarios (UP) [6]. Con esta habilidad los usuarios secundarios pueden hacer un uso oportuno del espectro sin interferir con los usuarios primarios [7].

Varios usuarios secundarios pueden establecer un enlace de comunicación, cuando se encuentran en un canal disponible e intercambian información de señalización. El proceso en el cual dos o más usuarios secundarios se encuentran en un mismo canal disponible, es llamado *rendezvous* [8].

Las estrategias empleadas para lograr el *rendezvous* son el uso de un canal común de control (CCC, *Common Control Channel*) y el uso de secuencias de salto de canal (CH, *Channel Hopping*) [9]. En la primera estrategia los usuarios secundarios escogen el mismo canal para intercambiar información de señalización. Aunque es la variante más simple, presenta como inconveniente la congestión ocasionada cuando el número de usuarios secundarios se incrementa frente a la posibilidad de que un CCC sea ocupado por un usuario primario [9]. En la estrategia de salto de canal cada usuario cognitivo emplea secuencias de salto para garantizar el *rendezvous* en uno de los canales disponibles, esta estrategia es conocida también como *rendezvous* ciego o *blind rendezvous* [7].

El uso de técnicas de salto de canal, ha llevado a la creación de diferentes algoritmos de *rendezvous*, algoritmos aleatorios, sincrónicos y asincrónicos, que minimizan el tiempo de *rendezvous* (TTR, *Time to Rendezvous*). Sin embargo no se ha analizado la robustez de dichos algoritmos ante interferencias.

Las interferencias ocasionadas por usuarios maliciosos o no, pueden disminuir el rendimiento de las comunicaciones o interrumpirlas. Los usuarios maliciosos, son usuarios que utilizan dispositivos de radio frecuencias ilegales, para bloquear o interferir la radio comunicaciones de los usuarios secundarios [10]. Mientras que un usuario no malicioso, es un usuario que con su presencia limita por ejemplo, el número de canales disponibles para que dos usuarios secundarios se comuniquen.

Teniendo en cuenta lo anterior surge como **problema científico** de esta investigación:

¿Cómo afectan las interferencias el desempeño de los algoritmos de *rendezvous* ciego, en redes radio cognitivas?

La investigación tiene como **objeto de estudio** los algoritmos de *rendezvous* ciego en redes radio cognitivas y su **campo de acción** lo constituye la evaluación de los algoritmos de *rendezvous* ciego en la herramienta de simulación Matlab.

En correspondencia con el problema científico, el **objetivo general** de esta investigación es: evaluar los algoritmos de *rendezvous* ciego en redes radio cognitivas ante interferencias. Para dar cumplimiento al objetivo general fueron trazados los siguientes **objetivos específicos**:

1. Caracterizar la tecnología radio cognitiva y los algoritmos de *rendezvous* ciego.

2. Caracterizar las estrategias de ataque de usuarios maliciosos en redes radio cognitivas.
3. Identificar los parámetros que determinan la influencia de interferencias en los algoritmos de *rendezvous* ciego para redes radio cognitivas.
4. Comparar el desempeño de los algoritmos de *rendezvous* ciego ante interferencias, mediante los parámetros definidos, a través de los resultados obtenidos en las simulaciones.

En el desarrollo de la investigación se da respuesta a las siguientes **preguntas científicas**:

- ¿Qué investigaciones se han realizado en la actualidad sobre la tecnología radio cognitiva?
- ¿Qué investigaciones se han realizado sobre los algoritmos de *rendezvous* ciego para redes radio cognitivas?
- ¿Cuáles son las estrategias de ataque de usuarios maliciosos en redes radio cognitivas?
- ¿Qué parámetros se utilizan en la evaluación de los algoritmos de *rendezvous* ciego ante interferencias?
- ¿Qué resultados se obtendrán al evaluar el funcionamiento de los algoritmos de *rendezvous* ciego ante interferencias?

En correspondencia con el objetivo del presente trabajo, fue necesario aplicar los siguientes métodos de investigación científica:

De nivel Teórico:

- Histórico-lógico: Se utilizó para caracterizar la evolución histórica del tema, su génesis y desarrollo.

- Análisis y Síntesis: Permitió penetrar en la esencia del fenómeno objeto de estudio a partir de su descomposición, pudiéndose establecer nexos, comparar resultados, determinar puntos comunes y divergentes, de los algoritmos de *rendezvous* ciego para las redes radio cognitivas. Lográndose establecer los componentes de la investigación, su fundamentación, la evaluación de los algoritmos y el análisis de los resultados.

- Inductivo-Deductivo: Su aplicación permitió dar respuesta a las interrogantes planteadas, a partir de los resultados obtenidos en las simulaciones, arribando a las conclusiones de la investigación.

- Sistémico-Estructural: La modelación permitió evaluar el comportamiento de los algoritmos de *rendezvous* ciego, al implementarlos en la herramienta de simulación Matlab.

De nivel Empírico:

- La recolección de información: se aplica en el estudio de documentos, para obtener la información necesaria referente al objeto de investigación.

La novedad científica de este trabajo se concreta en la evaluación de los algoritmos de *rendezvous* ciego: Aleatorio, *Jump-Stay* y *Short Sequence Based* ante interferencias de un usuario aleatorio y del algoritmo *Short Sequence Based* ante interferencias de un usuario malicioso adaptable. Los parámetros utilizados expresan el desempeño de los algoritmos en términos de tiempo de *rendezvous* e incidencias con el usuario interferente, ante diferente disponibilidad de canales en la red radio cognitiva. A lo anterior se le adiciona que la herramienta de simulación utilizada en este trabajo posee gran prestigio y reconocimiento internacional por su versatilidad y prestaciones.

El impacto que se espera de este trabajo es que sirva como punto de partida para la creación en el futuro de algoritmos de *rendezvou*s ciego robustos ante interferencias, y que los resultados obtenidos puedan formar parte de nuevos proyectos investigativos; de ahí que los resultados alcanzados serán de una aplicación práctica y teórica, estando al alcance de todos los que trabajen en este tema.

El informe se estructura en introducción, capitulario, conclusiones, recomendaciones, referencias bibliográficas y anexos. En el Capítulo 1 se establecen los fundamentos teóricos necesarios para abordar la problemática de investigación. En este capítulo se exponen los resultados del estudio realizado sobre la tecnología radio cognitiva, el proceso de *rendezvous*, los algoritmos de *rendezvous* y las interferencias en redes radio cognitivas. En el Capítulo 2, se define el modelo del sistema. Se describen los algoritmos de *rendezvous*: Aleatorio, *Jump-Stay* y *Short Sequence Based*, seleccionados para las simulaciones y se justifica dicha selección.

Además se identifican los parámetros utilizados para evaluar los algoritmos escogidos. En el Capítulo 3 se compara el desempeño de los algoritmos seleccionados ante interferencias de un usuario aleatorio, en términos de tiempos de *rendezvous* esperado, tiempos de *rendezvous* máximo, porciento de incidencias de un usuario interferente con uno y con ambos usuarios secundarios en un mismo canal. Además se compara el desempeño del algoritmo *Short Sequence Based* ante interferencias de un usuario malicioso adaptable con respecto a la presencia de un usuario interferente aleatorio.

En las conclusiones se realiza un análisis crítico de los resultados obtenidos y las limitaciones fundamentales de los algoritmos de *rendezvous* ciego evaluados. Las recomendaciones están encaminadas a enriquecer futuras investigaciones sobre el tema. Los anexos recogen el material de apoyo necesario para ayudar a la comprensión de esta investigación.

# CAPÍTULO 1. *RENDEZVOUS* EN REDES RADIO COGNITIVAS

En el presente capítulo se establecen los fundamentos teóricos necesarios para abordar la problemática de investigación. En el epígrafe 1.1 se exponen las características generales de la tecnología radio cognitiva. En el epígrafe 1.2 se resumen los elementos esenciales del proceso de *rendezvous*. En el epígrafe 1.3 se clasifican los algoritmos de *rendezvous*, atendiendo al tipo de sistema en el que operan, la utilización o no de un canal común de control y la secuencia de salto de canal que utilizan los usuarios cognitivos. En el epígrafe 1.4 se analiza las interferencias en redes radio cognitivas, mediante las estrategias de ataques de usuarios maliciosos y los ataques comunes en redes radio cognitivas. En el epígrafe 1.5 se abordan las conclusiones del capítulo.

## 1.1 Tecnología Radio Cognitiva

La idea de la radio cognitiva fue presentada oficialmente en 1999 por *Joseph Mitola* en su artículo "*Cognitive Radio: Making Software Radios More Personal*" [5]. Posteriormente, la idea fue extendida por el propio autor en su disertación doctoral [11], donde fue presentada la siguiente definición de radio cognitiva:

> "*El término radio cognitiva identifica el punto en el cual los dispositivos de comunicación inalámbrica y las redes relacionadas son, desde el punto de vista computacional, lo suficientemente inteligentes como para: a) detectar las necesidades de comunicación del usuario como una función del contexto, y b) proveer los recursos de radio y servicios inalámbricos más adecuados a estas necesidades*"

A partir de estos trabajos iniciales diferentes organismos consideraron la necesidad de introducir reformas, no sólo para mejorar la utilización del espectro, sino también para intentar proveer nuevo espectro disponible para nuevas aplicaciones. En diciembre de 2003, la Comisión Federal de Comunicaciones (FCC, *Federal Communications Commission*) abogó por el replanteamiento

de las actuales arquitecturas de redes inalámbricas, proponiendo la radio cognitiva. Según la FCC [12]:

> *"Un dispositivo radio cognitivo es un sistema de radiofrecuencia capaz de variar sus parámetros de transmisión basándose en su interacción con el entorno en el que opera."*

La FCC reconocía la capacidad de la radio cognitiva para cambiar de manera radical los métodos tradicionales de explotación del espectro, permitiendo una utilización más eficiente del mismo. Se analizaron además posibles escenarios de aplicación práctica de la radio cognitiva, incluyendo las redes de comunicaciones de los servicios de emergencia, las redes de malla inalámbrica, las redes eléctricas inteligentes y las comunicaciones militares.

Por su parte el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, *Institute of Electrical and Electronics Engineers*) define la radio cognitiva como [13]:

> *"Un transmisor/receptor de radio frecuencia que se diseña para descubrir inteligentemente si un segmento en particular del espectro radioeléctrico está actualmente en uso, y para saltar dentro (o fuera si es necesario) de la banda del espectro sin usar temporalmente, sin interferir con las transmisiones de otros usuarios licenciados."*

De acuerdo con las definiciones anteriores, la radio cognitiva posee dos capacidades fundamentales que la distinguen de los sistemas de comunicaciones inalámbricos convencionales: la capacidad cognitiva y la capacidad de auto-reconfiguración. La capacidad cognitiva denomina el sistema de dominios referidos a: el estado de uso del espectro; la información de localización; el estado interno; las regulaciones establecidas y las necesidades del usuario. Conocimientos que pueden ser adquiridos mediante la captura y procesamiento de información del entorno radioeléctrico y del estado interno del sistema a través de múltiples sensores [1]-[14].

La capacidad de auto-reconfiguración permite que los parámetros de operación sean ajustados dinámica y autónomamente en función de las condiciones del entorno radioeléctrico, con el objetivo de optimizar el desempeño del sistema [15]. Es decir la capacidad de auto-reconfiguración no sólo ajusta en tiempo real los parámetros de operación, sino que también

provee la base para características como: adaptación de la interfaz de radio para soportar nuevos estándares, incorporación de nuevas aplicaciones y servicios emergentes, actualizaciones en el software y explotación de servicios heterogéneos ofrecidos por diversas redes.

El uso del término sistema implica que la capacidad cognitiva; y la capacidad de auto-reconfiguración pueden estar distribuidas a través de múltiples capas de protocolos y dispositivos en una red radio cognitiva [16]. Ambas capacidades permiten la reutilización del espectro, con ganancias significativas en términos de capacidad de la red y reducción de costos [2]. Realizar mejoras en las redes radio cognitivas (CRN, *Cognitive Radio Network*), implicarían cambios de software y no de hardware. Sin embargo el diseño del software para los diversos sistemas o estándares es una desventaja, debido a la complejidad de estos.

### 1.1.1 Ciclo cognitivo

La operación de un sistema radio cognitivo puede describirse a través de un modelo denominado ciclo cognitivo [5]-[17]. El ciclo cognitivo representa una máquina de estado de las diferentes etapas del proceso cognitivo. La idea del ciclo cognitivo inicialmente propuesta en [5] fue modificada por diversos autores para adaptarla al concepto de radio cognitiva como tecnología de acceso dinámico al espectro (DSA, *Dynamic Spectrum Access*). Sin embargo este modelo no representa un paradigma al cual deba ajustarse de forma estricta un sistema radio cognitivo en la práctica. El ciclo cognitivo, como se muestra en la Figura 1.1, para el acceso dinámico al espectro se divide en las etapas siguientes [18]:

- Detección del espectro
- Análisis del espectro
- Decisión del espectro

Mediante la detección del espectro y su análisis se puede conocer de la existencia de agujeros espectrales. Los agujeros espectrales se definen como aquellas porciones del espectro que no están siendo ocupadas por usuarios con licencia para su uso o que tienen e implican un bajo nivel de interferencia [1]-[19]. Luego del reconocimiento de los agujeros espectrales mediante la detección, los usuarios cognitivos escogen la mejor banda de frecuencia y saltan entre múltiples bandas de acuerdo a las características variantes del canal, en aras de satisfacer algún

o algunos requerimientos de calidad de servicio (QoS, *Quality of Service*) [2]. La toma de decisiones está basada en el aprendizaje previo, así como en el modelado y ejecución de procesos de optimización necesarios para reconfigurar el sistema radio cognitivo con el objetivo de elevar su desempeño.

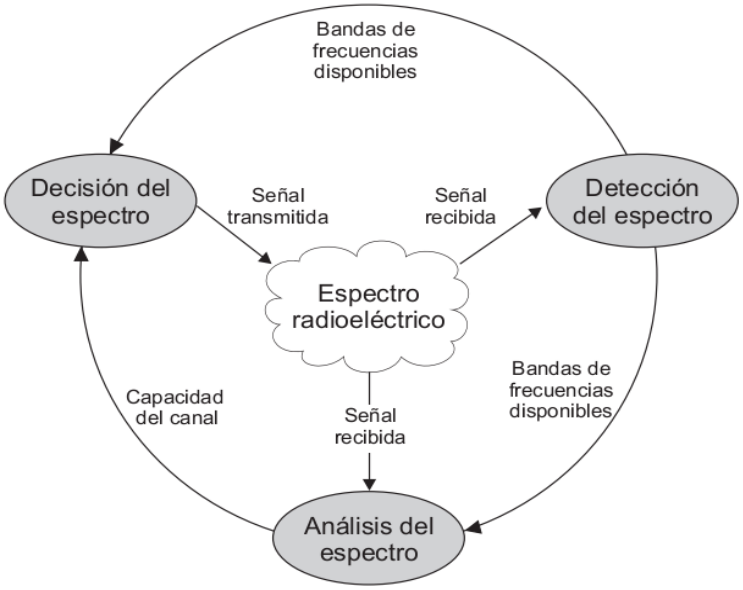



Figura 1.1: Ciclo Cognitivo [17].

La utilización por parte de la radio cognitiva de los agujeros espectrales, se muestra en la Figura 1.2. Los usuarios primarios (UP) son los que cuentan con una licencia para el uso autorizado de determinadas bandas de frecuencias, mientras que los usuarios secundarios (US) son los que intentan acceder a los denominados agujeros espectrales que puedan existir en estas bandas de frecuencias. Idealmente, las comunicaciones en una red primaria no deberían verse afectadas cuando los usuarios secundarios acceden de forma dinámica y oportuna al espectro.

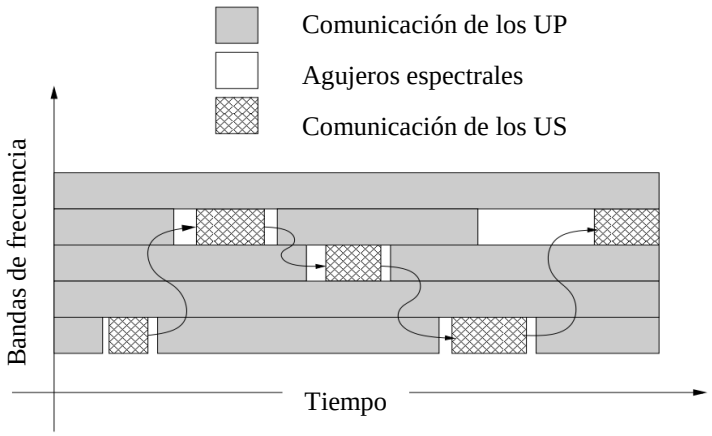



Figura 1.2: Utilización del espectro en redes radio cognitivas [6].

## 1.2 Proceso de *rendezvous*

Es imprescindible para que la comunicación se efectúe que los radios de los usuarios secundarios estén sintonizados en un mismo canal. El proceso en el que los radios de dos o más usuarios se encuentran y establecen un vínculo de comunicación en un mismo canal reconocido como disponible, es llamado *rendezvous* [20].

Para lograr el *rendezvous* los usuarios cognitivos deben: seleccionar un canal comúnmente disponible para ellos e informar mutuamente de que van a utilizar este canal para la comunicación [8]. Durante la selección de un canal disponible un usuario secundario puede encontrar uno o más canales disponibles, y los diferentes usuarios cognitivos pueden encontrar diferente disponibilidad de canal, debido a la posición en que se encuentran con respecto a los usuarios primarios. Atendiendo a la heterogeneidad del espectro observado, son identificados dos modelos de red diferentes, si los usuarios secundarios comparten el mismo conjunto de canales disponibles se denomina modelo simétrico, de lo contrario se denomina modelo asimétrico [20].

Ambos modelos son importantes en la práctica, el modelo simétrico es representativo de redes radio cognitivas donde los usuarios secundarios se encuentran en un área relativamente pequeña y el modelo asimétrico representa a grandes áreas de cobertura [20]. En el modelo asimétrico el proceso de *rendezvous* suele ser más complejo.

Para completar el *rendezvous* los usuarios secundarios deben intercambiar información de control. La duración necesaria del intercambio de los mensajes de control es $\tau$ [21] y se muestra

en la Figura 1.3. Durante este tiempo, τ, los usuarios secundarios reservan un intervalo para la detección y así descubren los canales que no están siendo utilizados por los usuarios primarios. Basado en los resultados de la detección los usuarios secundarios acceden a dichos canales de manera oportunista sin interferir con los usuarios primarios. Al final, el receptor envía un reconocimiento (ACK, *Acknowledgement*) al transmisor si la transmisión de paquetes en el canal tiene éxito [21]. Sin embargo, cada ranura de tiempo tiene una duración total de 2τ, para compensar la falta sincronismo entre los usuarios secundarios. Según IEEE 802.22, estándar para el uso de la radio cognitiva, $\tau = 10ms$ [22] y por lo tanto, cada ranura de tiempo tiene una duración de 20 ms.

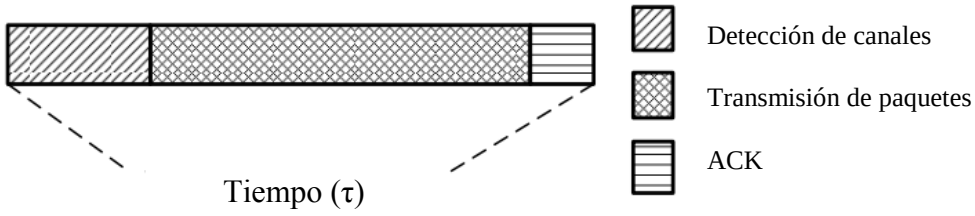



Figura 1.3: Tiempo para el intercambio de los mensajes de control [22].

Después de seleccionado un canal disponible, e intercambiada la información de señalización, los usuarios secundarios pueden enviar datos entre sí. En la práctica, el *rendezvous* con éxito, implica otros procesos, como *beaconing* en un canal previamente programado, la aplicación de un mecanismo de *handshaking* (protocolo de enlace) específico, etc. [7]. Esta investigación se centra en los algoritmos empleados para lograr *rendezvous*.

## 1.3 Clasificación de los algoritmos de r*endezvous*

Los autores en [23] clasifican los algoritmos de *rendezvous* en base a tres criterios diferentes: 1) el tipo de sistema en el que operan, centralizado o descentralizado; 2) la utilización o no de un canal común de control y 3) en dependencia de la secuencia de salto de canal que utilizan, como se muestra en la Figura 1.4.

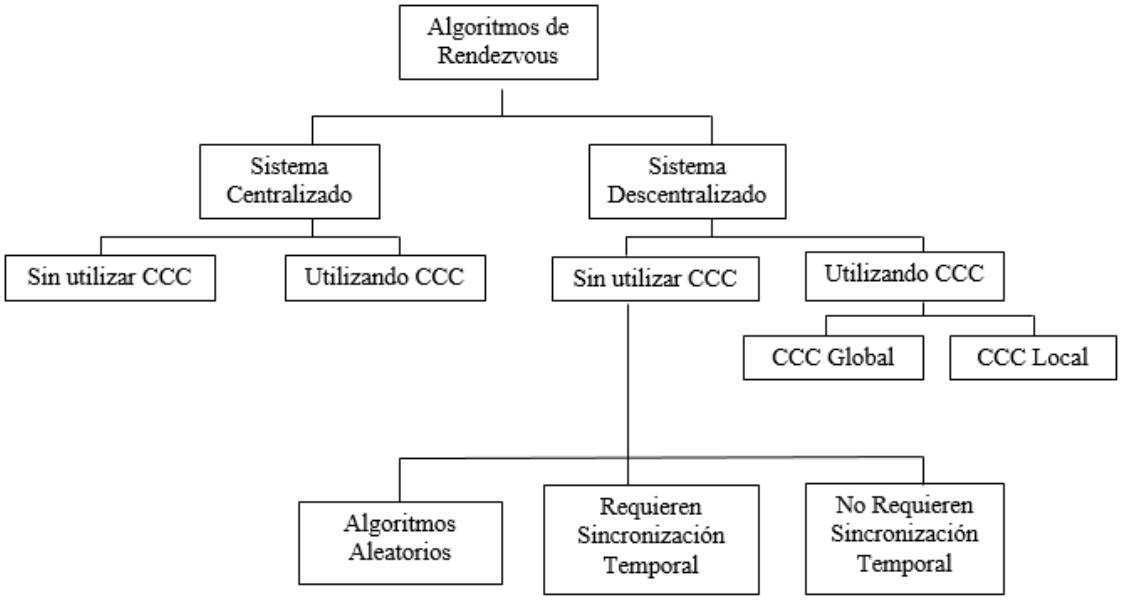



Figura 1. 4: Clasificación de los algoritmos de *rendezvous* [23].

Una arquitectura de red centralizada, como se muestra en la Figura 1.5b), se divide en células, y cada célula se gestiona a través de una estación base secundaria o un servidor que controla y distribuye los canales de *rendezvous*, es decir los usuarios secundarios se comunican con sus estaciones bases y pueden realizar operaciones periódicamente para la gestión del espectro [24]. Las estaciones bases secundarias pueden ser interconectadas a través de una red troncal inalámbrica o cableada. Los sistemas centralizados son relativamente simples de implementar independientemente de si utilizan un CCC (*Common Control Channel*) o no.

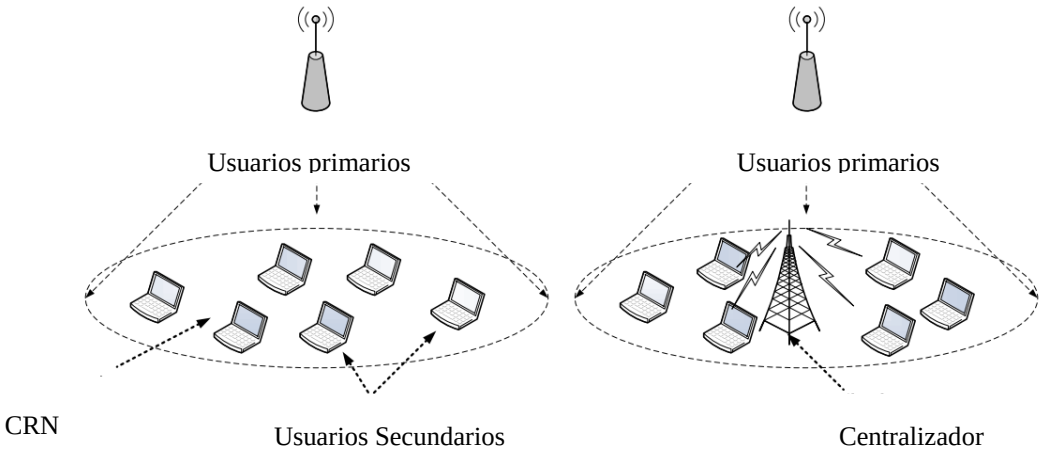



Figura 1.5: Arquitecturas de redes radio cognitivas: a) descentralizada y b) centralizada [24].

Un CCC consiste en un canal siempre disponible entre los usuarios secundarios por el cual se intercambia información de señalización en operaciones como: la detección distribuida, la notificación de detección de usuarios primarios, la selección dinámica de canales y conmutación de canales [25]. La implementación de un CCC introduce varios retos, entre los que destacan la necesidad de ubicarlo en una banda de frecuencias fija, visible a todos los usuarios secundarios, y libre de actividades de los usuarios primarios. El CCC que se desea se puede asignar en bandas sin licencia o en las bandas licenciadas específicas para la aplicación [26]. Además, el CCC requiere en algunos casos, la implementación de otro algoritmo que coordine el acceso de los usuarios secundarios a éste; por ejemplo, los autores en [27] utilizan acceso múltiple por detección de portadora con evasión de colisiones (CSMA/CA, *Carrier Sense Multiple Access /Collision Avoidance*).

Aunque la utilización de un CCC facilitaría el proceso de *rendezvous* tiene varios inconvenientes, por ejemplo, el uso de un CCC en una banda que no requiera licencia sólo agravaría la congestión en dicha banda. Mientras la utilización y mantenimiento del CCC en una banda que requiera licencia no es viable, debido a que la disponibilidad de canales de cada usuario varía dinámicamente con el tiempo y con la posición geográfica. Además un CCC es vulnerable a los ataques de usuarios maliciosos y es un fácil punto de falla para el sistema [28].

La idea básica de los algoritmos para sistemas centralizados sin la utilización de un CCC, consiste en la búsqueda por parte del servidor y de los usuarios secundarios de canales a frecuencias altas. Después de la detección, cuando un usuario secundario encuentra un canal disponible, espera en este canal para reunirse con el servidor y si lo logra, la comunicación se establece [29]. Aunque los sistemas centralizados que utilizan un CCC o no, son relativamente simples de implementar, son débiles en escalabilidad y robustez.

En los sistemas descentralizados, como se muestra en la Figura 1.5a) los usuarios secundarios se comunican de modo *ad-hoc*, no necesitan un controlador. Los usuarios secundarios, que están dentro del radio de cobertura pueden intercambiar información de forma directa, mientras que los usuarios secundarios que no están dentro del radio de cobertura pueden intercambiar información a través de múltiples saltos. Estos sistemas pueden utilizar un CCC o no, mientras que los sistemas que lo utilizan pueden hacerlo de manera local o global. La utilización de un CCC global en un sistema descentralizado es similar a los sistemas centralizados. Debido a lo

difícil que resulta establecer un canal común a todos los usuarios, dadas las variaciones dinámicas de la disponibilidad de canales, los autores en [30] proponen agrupar los usuarios secundarios, de modo que para cada uno de los grupos exista un CCC local por el que puedan establecer la comunicación con cada uno de los miembros de su grupo. La creación de los grupos implica un gran costo computacional y de tiempo.

Ante las limitaciones de seguridad, baja escalabilidad y congestión que implica el uso de un CCC en los sistemas de comunicación radio cognitivos, son ampliamente utilizados los sistemas descentralizados sin utilizar un CCC o como se le conoce también, *rendezvous* ciego (*Blind rendezvous*). Estos sistemas utilizan técnicas de salto de canal (CH, *Channel Hopping*), en las que cada usuario secundario sigue una secuencia de salto de canal predefinida hasta lograr *rendezvous* con uno o más usuarios secundarios. Al utilizar secuencias de salto de canal, las transmisiones son más confiables porque el establecimiento de los recursos de negociación no depende del estado de un solo canal común. Existen tres variantes de algoritmos de *rendezvous* ciego: los algoritmos aleatorios, los algoritmos sincrónicos y los algoritmos asíncronos.

### 1.3.1 Algoritmos de *rendezvous* ciego

En los algoritmos de *rendezvous* aleatorios [31] cada usuario secundario decide su propia secuencia de salto en base a sus canales disponibles, al azar. Debido a su simplicidad, los algoritmos aleatorios son aplicables a los modelos de red simétrico y asimétrico. Sin embargo no pueden garantizar el *rendezvous* de los usuarios secundarios en un tiempo finito y por tanto existe la posibilidad de que los usuarios cognitivos nunca coincidan en un mismo canal. Un ejemplo de algoritmo aleatorio es *Adaptative Multiple Rendezvous Control Channel* (AMRCC) [32], en el cual los canales con baja interferencia a los usuarios primarios tienen mayor oportunidad para ser seleccionados en la secuencia de salto de canal.

El sincronismo en redes radio cognitivas evita resultados erróneos durante la detección del espectro y permite el uso del acceso múltiple por división en el tiempo (TDMA, *Time Division Multiple Access*), técnica considerada eficiente dentro del conjunto de técnicas de control de acceso al medio (MAC, *Medium Access Control*). Además, en disímiles aplicaciones de las redes radio cognitivas, los usuarios secundarios están obligados a mantener la sincronización del tiempo, por ejemplo, como solución al problema del terminal oculto [33]. En el algoritmo

sincrónico *Slotted Seeded Channel Hopping* (SSCH) [33], cada usuario secundario selecciona múltiples pares de canales y la secuencia de salto de canal es determinada basada en estos pares. Aunque SSCH se diseña para un aumento de la capacidad de redes IEEE 802.11, solo garantiza el *rendezvous* bajo el modelo simétrico.

En la práctica el proceso de sincronización es complejo, debido a la heterogeneidad de las redes. La banda de televisión es un ejemplo de banda de frecuencias donde lograr la sincronización de los usuarios secundarios es difícil [23]. Por ello, en la literatura se han propuesto una serie de algoritmos asíncronos de CH, ejemplo de ello son *Generated Orthogonal Sequences* (GOS) [34] y *Asynchronous-Efficient Channel Hopping* (ASYNC-ETCH) [35]. En GOS, los radios utilizan secuencias ortogonales predeterminadas para determinar el orden en que los canales serán visitados. Mientras que el objetivo de ASYNC-ETCH no sólo es disminuir el tiempo de *rendezvous* (TTR) sino también equilibrar la carga y la relación de utilización de los canales. Ambos algoritmos solo funcionan en el modelo simétrico.

Otros algoritmos de *rendezvous* asíncronos son *Modular Clock* (MC) [36], *Modified Modular Clock* (MMC) [36], *Channel Rendezvous Sequence* (CRSEQ) [37] y *Deterministic Rendezvous Sequence* (DRSEQ) [38].

En los algoritmos MC y MMC cada usuario escoge un número primo y aleatoriamente selecciona un número menor que ese número primo. El número primo seleccionado es el menor número primo, mayor que el número de canales disponibles en la red. Basado en estos dos parámetros, el usuario secundario genera su secuencia de salto de canal. Los algoritmos MC y MMC son aplicables a los modelos simétrico y asimétrico; y no pueden ser directamente aplicados al *rendezvous* de múltiples usuarios [36].

El algoritmo CRSEQ es aplicable al modelo asimétrico y DRSEQ al modelo simétrico, sin embargo ambos pueden extenderse para lograr el *rendezvous* de múltiples usuarios. El algoritmo DRSEQ supera el desempeño de los algoritmos GOS, MC y MMC en cuanto a tiempo de *rendezvous*, en un escenario simétrico.

En escenarios donde no ocurren cambios en la actividad de los usuarios primarios o estos cambios ocurren lentamente como por ejemplo en las bandas asignadas a la televisión, el conocimiento previo de la actividad en cada canal contribuye significativamente a minimizar el tiempo de *rendezvous*. De esta forma aun cuando las secuencias de salto sean generadas

considerando todos los canales de la red, cada usuario secundario solo visita los canales disponibles. Los algoritmos asíncronos que se describen a continuación utilizan operaciones de remplazo. En las operaciones de remplazo, se sustituye en las secuencias de salto los canales no disponibles por canales previamente identificados como disponibles.

En [7] es propuesto el algoritmo *Jump-Stay* (JS). La idea básica de este algoritmo es la de generar secuencias de CH en rondas y cada ronda se compone de un patrón de salto y un patrón de espera. El patrón de salto y el patrón de espera son segmentos específicos de la secuencia de salto de canal. Intuitivamente, los usuarios de forma continua "saltan" sobre los canales disponibles durante el patrón de salto mientras "permanecen" en un canal específico durante el patrón de espera. El usuario secundario realiza el patrón de salto y el patrón de espera en cada ronda. En [7] se demuestra que el algoritmo JS garantiza el *rendezvous* bajo cualquier combinación de salto y espera entre usuarios secundarios. La variante mejorada del algoritmo JS denominada *Enhanced Jump Stay* (EJS) es propuesta en [39]. La estrategia de *rendezvous* EJS obtiene mejor desempeño en términos de tiempo de *rendezvous* que el algoritmo JS en el modelo asimétrico.

En [40] se introduce el algoritmo *Fast Rendezvous Channel Hopping* (FRCH), este algoritmo considera una estrategia común para que cada usuario secundario genere las secuencias de salto. En [8] se propone el algoritmo *Short Sequence Based* (SSB) en el cual también se emplea una estrategia común para generar las secuencias de salto, tanto el algoritmo FRCH como el SSB funcionan en ambos modelos (simétrico y asimétrico) pero el SSB supera el desempeño del FRCH en términos de TTR en el modelo asimétrico.

## 1.4 Interferencias en redes radio cognitivas

Durante el desarrollo de la secuencia de salto de canal que han escogido dos usuarios secundarios determinados para comunicarse, un usuario con intenciones maliciosas o no puede interferir con ellos. Un usuario no malicioso, que tiene como objetivo comunicarse con otro u otros usuarios cognitivos interfiere en el *rendezvous* de los usuarios secundarios en cuestión, al limitar por ejemplo el número de canales disponibles para establecer la comunicación, porque durante el proceso de detección del espectro los usuarios secundarios encuentran ese canal como ocupado.

Los usuarios maliciosos, son usuarios que utilizan dispositivos de radio frecuencias ilegales, para interrumpir o interferir la radio comunicaciones de los usuarios secundarios [10]. Estos dispositivos no diferencian entre comunicaciones deseadas o no deseadas, por ejemplo podrían impedir a un dispositivo celular hacer o recibir cualquier tipo de llamada, mensajes de texto, y correos electrónicos; incluyendo llamadas de emergencia. Por tal motivo la FCC prohíbe el uso de estos dispositivos en radio comunicaciones y toma acciones legales contra sus violadores por las consecuencias que implica su empleo [41].

El objetivo de las interferencias ocasionadas por usuarios maliciosos es disminuir el rendimiento de las comunicaciones o interrumpirlas. Para ello, los usuarios maliciosos pueden realizar varias acciones. Entre ellas interferir el canal de comunicación de los usuarios primarios o inutilizarlo. Prever las bandas del espectro libre que los usuarios secundarios pueden utilizar y denegar el servicio o reducir las posibilidades del buen funcionamiento de la comunicación. Acceder a datos privados sin autorización, modificar los datos intercambiados entre varias entidades a su propia ventaja, e introducir datos erróneos dentro de la información [42]-[43].

Entre las acciones comunes en que inciden usuarios maliciosos, se encuentra la suplantación de identidad de uno de los usuarios secundarios y los ataques de emulación de usuario primario (PUE, *Primary User Emulation*) [44]-[45]. Aunque estas acciones no son contra el proceso de *rendezvous*, sí impiden que la comunicación de usuarios secundarios se realice y por tanto el proceso de *rendezvous* no ocurre. Garantizando el empleo de algoritmos de *rendezvous* robustos ante interferencias se pueden evitar o minimizar los efectos de estas acciones.

En la suplantación de identidad el usuario malicioso puede ocupar el rol del trasmisor o del receptor. El proceso en el que el usuario malicioso ocupa el rol del transmisor e interfiere en la comunicación se conoce como *noise-spoofing*. Mientras que el proceso en el que el usuario malicioso ocupa el rol del receptor y evita la recepción correcta del mensaje se conoce como *noise-jamming* [46].

En la Figura 1.6 se muestran los procesos *noise-jamming y noise-spoofing*. Por su parte el *jamming*, es cuando el atacante interfiere en la recepción correcta del mensaje. Enviando a los receptores una señal de potencia alta, para evitar por interferencia la recepción correcta del mensaje. *Spoofing* se refiere a cuando el usuario malicioso (I) simula un canal disponible para

el usuario cognitivo que desea transmitir, como ocupado, saturando el canal de radio con una señal, es decir emula la presencia de un usuario primario.

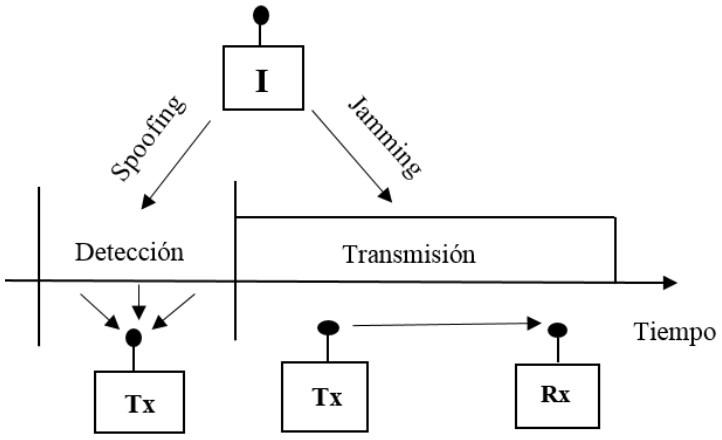



Figura 1.6: Actividad del usuario malicioso durante la transmisión y recepción [6].

En los ataques de emulación de usuario primario, si el usuario malicioso conoce la forma de onda del usuario primario, crea una forma de onda similar a esta, para activar un falso positivo durante la detección del espectro. De esta forma los usuarios secundarios creerán que un usuario primario está activo y desalojarán el canal. Los ataques de emulación de usuario primario pueden clasificarse en dos grupos [45]-[47]:

- *Greedy*: Mediante la transmisión de señales de usuarios primarios falsos el usuario malicioso desea obligar a los demás usuarios secundarios a abandonar una banda específica (*spectrum hole*) con el fin de adquirir su uso exclusivo.

- Malicioso: Mediante la transmisión de señales de usuarios primarios falsos el usuario malicioso desea provocar una denegación de servicio. Por otra parte, también podrían provocar ataques de denegación de servicio en las redes de usuarios primarios creando interferencias perjudiciales.

Para realizar estas acciones los usuarios maliciosos pueden utilizar diferentes estrategias [21]:

- Constante: El usuario malicioso constante selecciona el mismo conjunto de canales para explorar en cada ranura de tiempo y emite una señal de radio continuamente en los canales detectados como libres. Aunque esta conducta podría ser eficaz en una red de comunicación tradicional, resulta ser ineficaz en redes radio cognitivas, que son

intrínsecamente robustas a este tipo de ataque. Los dispositivos radio cognitivos cambian dinámicamente su configuración, es decir, ellos siempre están buscando el espectro libre disponible, ellos auto-reconfiguran repetidamente sus parámetros de comunicación (frecuencia, banda, protocolo). Por consiguiente, una estrategia fija de ataque podría tener éxito por solo un período corto de tiempo.

- Aleatorio: El usuario malicioso aleatorio selecciona aleatoriamente un conjunto de canales para explorar en cada ranura de tiempo y emite una señal de radio continuamente en los canales disponibles, sin tomar en cuenta detecciones previas.

- Reactivo: El usuario malicioso reactivo sólo inicia sus ataques cuando detecta actividad en el canal. Este tipo de usuario malicioso puede aprender el modelo de funcionamiento de los usuarios primarios y predecir el acceso de los usuarios secundarios a los canales, incluso conoce si su ataque tiene éxito. El usuario malicioso reactivo constituye una amenaza importante. La razón es que, mientras destruye los paquetes, minimiza el riesgo de ser detectado [6].

- Adaptable: es un usuario cognitivo que detecta y bloquea determinado canal basado en detecciones anteriores o en observaciones realizadas a la red, por ejemplo, la estrategia de salto de canal que siguen los usuarios secundarios [42]. Determina los canales ocupados por los usuarios primarios y emite señales de bloqueo sobre los canales más probables como disponibles.

- Engañoso (*Deceptive*): El usuario malicioso engañoso constantemente inyecta paquetes al canal. Así los usuarios secundarios creen que el atacante es un usuario primario en estado de transmisión.

## 1.5 Conclusiones del capítulo

La radio cognitiva es una tecnología cuyo objetivo fundamental es lograr una utilización eficiente y racional de los recursos de radio. Para ello los dispositivos radio cognitivos deben ser capaces de explorar y adquirir información de su entorno (capacidad cognitiva), tomar decisiones para ajustar sus parámetros de operación en función de optimizar el desempeño del

sistema (capacidad de auto-reconfiguración), aprender de los resultados de las decisiones tomadas y adaptarse a los cambios del medio radioeléctrico.

Para que los usuarios cognitivos o usuarios secundarios se comuniquen es necesario el proceso de *rendezvous* que incluye la selección de un canal libre y el intercambio de información de señalización. Las estrategias para lograr el *rendezvous* son el uso de un canal común de control y el uso de secuencias de salto de canal. Las soluciones que implican la existencia de un canal común de control son vulnerables a ataques, difíciles de establecer y mantener. El uso de técnicas de salto de canal o algoritmos de *rendezvous* ciego son más confiables. Estos algoritmos pueden ser aleatorios, sincrónicos y asincrónicos, estos últimos muy utilizados, dadas las características heterogéneas de las redes radio cognitivas. Los algoritmos de *rendezvous* ciego tienen como objetivos lograr un menor tiempo de *rendezvous*, ser aplicable a los modelos de red simétrico y asimétrico y extender su uso al *rendezvous* de múltiples usuarios. En esta investigación también se toma en cuenta la robustez de dichos algoritmos ante interferencias.

La interferencias de usuarios maliciosos o no, afecta el *rendezvous* en redes radio cognitivas. El objetivo de los usuarios maliciosos es interferir o evitar la comunicación de los usuarios cognitivos, mientras que los usuarios no maliciosos por encontrarse en el escenario de comunicación también reducen las posibilidades de *rendezvous*, al limitar por ejemplo, el número de canales disponibles. Los usuarios maliciosos pueden equiparse con tecnología cognitiva o no y adoptar diferentes estrategias de ataque.

# CAPÍTULO 2. ALGORITMOS DE *RENDEZVOUS* CIEGO

En este capítulo, se considera una red radio cognitiva formada por dos usuarios secundarios que intentan el *rendezvous* ante interferencias. En el epígrafe 2.1 se describe el sistema propuesto. En el epígrafe 2.2 se seleccionan los algoritmos de *rendezvous*: Aleatorio, *Jump-Stay* y *Short Sequence Based*, como las secuencias de salto de canal utilizadas por los usuarios secundarios. En el epígrafe 2.3 se identifican los parámetros utilizados para medir el desempeño de los algoritmos anteriores, ante interferencias. En el epígrafe 2.4 se presentan las conclusiones del capítulo.

## 2.1 Modelo del sistema

Se considera una red radio cognitiva que consiste en, $s = 3$ usuarios secundarios que coexisten con uno o más usuarios primarios en la misma área geográfica. Los usuarios primarios son los propietarios de una parte del espectro con licencia, que se puede dividir en $M > 1$, canales que no se superponen $C = \{ c_1, c_2, \dots, c_M \}$, en donde $c_i$ denota el canal $i$. Se considera que estos canales son indexados de manera única como $1,2, \dots, M$ y los índices son conocidos por todos los usuarios de la red. Cada usuario en la red está equipado con un radio cognitivo que puede acceder a los canales en reposo en $C$ oportunidades.

Para designar el conjunto de canales disponibles de los usuarios $i$ ($i = 1,2, \dots \dots, s$) se utiliza $C_i \subseteq C$, donde se dice que un canal está disponible para un usuario secundario, si el usuario puede comunicarse en el canal sin causar interferencia a los usuarios primarios. El conjunto de canales disponibles de los usuarios secundarios $C_i$ es determinado por detección de espectro, por el usuario $i$ antes de que el proceso de *rendezvous* comience. Una forma de identificar de manera eficiente los canales disponibles en el espectro se muestra en [48].

Se considera para las simulaciones el siguiente modelo:

Modelo Ideal: se considera un escenario de comunicación con tres usuarios secundarios, un usuario secundario 1 quiere entregar un mensaje a un usuario secundario 2. Mientras que, existe la presencia de un tercer usuario, que interfiere en el proceso de *rendezvous* de los usuarios 1 y

2, al coincidir con ambos en un mismo canal, o de forma independiente. Los usuarios secundarios 1 y 2 siguen la misma secuencia de salto de canal y cada uno de ellos emplea una versión desplazada de dicha secuencia, es decir no están sincronizados. Por lo que se considera $2\tau$ como la duración de una ranura de tiempo garantizando que el solapado de cualquier par de ranuras de tiempo sea suficiente para completar el proceso de *rendezvous* [22]-[49].

Los usuarios de la red tienen la misma disponibilidad de canales si sus ubicaciones geográficas están cerca. Es decir, para cualquier $1 \leq i, j \leq s$ tenemos $C_i = C_j$, para simplicidad, se supone $C_i = C_j = C$. Además los usuarios primarios permanecen por largos períodos de tiempo en inactividad, por lo tanto el número de canales disponibles para el *rendezvous* es igual a la cantidad de canales de la red. En este modelo se asume que los receptores primarios se encuentran lo suficientemente alejados de los transmisores secundarios, de modo que la protección de las comunicaciones primarias puede garantizarse limitando la potencia de transmisión máxima de los usuarios secundarios.

El modelo del sistema que se analiza en la presente investigación se ilustra en la Figura 2.1, la línea continua indica el enlace entre los usuarios secundarios 1 y 2, y las líneas discontinuas la interferencia ocasionada por el tercer usuario.

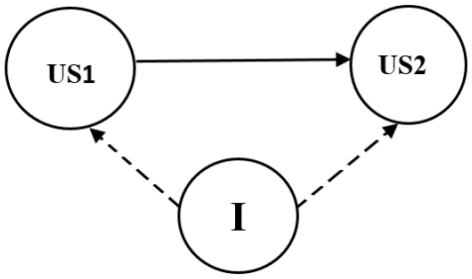



Figura 2.1: Modelo del sistema para una red radio cognitiva de 2 US ante interferencias.

### 2.1.1 Modelo del usuario interferente

Se considera un usuario interferente con dos secuencias de salto de canal diferentes. En un primer experimento se asume que en la red radio cognitiva interfiere en el *rendezvous* de los usuarios secundarios un usuario con una secuencia de salto de canal aleatoria, sin considerar la intención del usuario: maliciosa o no. Debido a que una estrategia de ataque aleatoria, no toma en cuenta detecciones previas, ni ninguna otra información de la red, por lo que afectaría de

igual forma que si se tratase de un usuario no malicioso con una secuencia de salto de canal aleatoria.

En el segundo experimento los usuarios secundarios utilizan el algoritmo de *rendezvous Short Sequence Based* y el usuario interferente es un usuario malicioso con una estrategia de ataque adaptable. Este usuario conoce la secuencia de salto de canal que siguen los usuarios secundarios 1 y 2 y en función de ello genera su propia secuencia de salto de canal. Además se asume que este usuario no interfiere en las bandas licenciadas de los usuarios primarios porque: 1) se penaliza si su identidad es conocida por la red de usuarios primarios [50] y 2) en algunos escenarios, no puede estar cerca de los usuarios primarios, por ejemplo, en una red de usuarios primarios formada por torres de televisión [51]. Por consiguiente, el usuario interferente durante el proceso de detección estima la actividad de los usuarios primarios y bloquea solo los canales libres.

En ambos experimentos el usuario interferente es capaz de detectar e interferir un canal, en cada ranura de tiempo. Conoce el conjunto de protocolos de acceso al espectro, e impide que el espectro sea utilizado eficazmente por los usuarios secundarios.

## 2.2 Algoritmos de *rendezvous* ciego seleccionados

La evaluación de los algoritmos de *rendezvous* es realizada comúnmente en función de lograr el menor tiempo de *rendezvous* [52]. En esta investigación se combina ese criterio con el de lograr el menor número de encuentros entre los usuarios secundarios y el usuario que interfiere, por las consecuencias que ello implica, descritas en el epígrafe 1.4.

Aunque no existe ningún algoritmo que garantice el *rendezvous* ante interferencias, una alternativa para disminuirlas, es la de hacer saltos aleatorios a través de múltiples canales [18]. Mediante el algoritmo Aleatorio, el transmisor y el receptor seleccionan al azar un canal en cada ranura de tiempo, de los $M$ canales disponibles en la red. Para el usuario interferente es complejo estimar cuando el transmisor y el receptor aleatorio logran el *rendezvous*. En redes radio cognitivas esta estrategia puede ser un esquema de *rendezvous* eficiente, efectivo y seguro. En esta investigación, los algoritmos seleccionados para evaluar ante interferencias en redes radio cognitivas, hacen diferentes usos de la aleatoriedad al generar su secuencia de salto de canal.

Los algoritmos de *rendezvous* seleccionados son: Aleatorio [24], *Jump-Stay* (JS) [7] y *Short Sequence Based* (SSB) [8]. El algoritmo Aleatorio sigue una secuencia de salto de canal puramente aleatoria; mientras que el *Jump-Stay* sigue una secuencia de salto de canal periódica, generada a partir de parámetros aleatorios y por último el algoritmo determinista *Short Sequence Based*, basado en el uso de secuencias cortas y periódicas. Además, estos algoritmos no requieran la sincronización de los usuarios secundarios. Son aplicables en los modelos de red simétricos y asimétricos; y su uso puede ser extendido al *rendezvous* de múltiples usuarios.

### 2.2.1 Algoritmo Aleatorio

En el algoritmo Aleatorio el usuario secundario, en cada ranura de tiempo, selecciona cualquiera de los $M$ canales disponibles al azar, con probabilidad $1/M$ e intenta el *rendezvous* en dicho canal. Si se considera $E$ como el evento de que en una misma ranura de tiempo ambos usuarios secundarios seleccionen el mismo canal, $H$ como el evento de intercambio de información de control exitoso y asumiendo que los dos eventos son independientes, se tiene que la probabilidad de *rendezvous* es:

$$p\,(R) = p(H) * p(E)$$

El seudocódigo mostrado en la Figura 2.2 describe la implementación del algoritmo Aleatorio.

**Algoritmo Aleatorio**

1: **Entrada**: $M$
2: **while** (no *rendezvous*)
3: $S\,(t) = randi\,[1, M]$
4: Intentar *rendezvous* en $S\,(t)$
5: **end**
6: **Salida** $S\,(t)$

Figura 2.2: Seudocódigo del algoritmo Aleatorio [24].

### 2.2.2 Algoritmo *Jump-Stay*

En el algoritmo de *rendezvous Jump-Stay* (JS) [7] la secuencia de CH se genera en rondas, y cada ronda consta de un patrón de salto (*jump*) y un patrón de estancia (*stay*). El usuario secundario realiza primero el patrón de salto y después el patrón de estancia en cada ronda. Para que el usuario secundario genere los dos patrones en una ronda, es necesario seleccionar tres parámetros: $P$ , $r$ y $q$.

El parámetro $P$ es el menor número primo, mayor que el número de canales disponibles en la red $(M)$, $r$ es la longitud del paso; y $q$, el índice de arranque [7]. En cada una de las rondas, el patrón de salto dura $2P$ y el patrón de estancia posterior $P$ ranuras de tiempo, para una duración total de $3P$ ranuras de tiempo, como se muestra en la Figura 2.3.

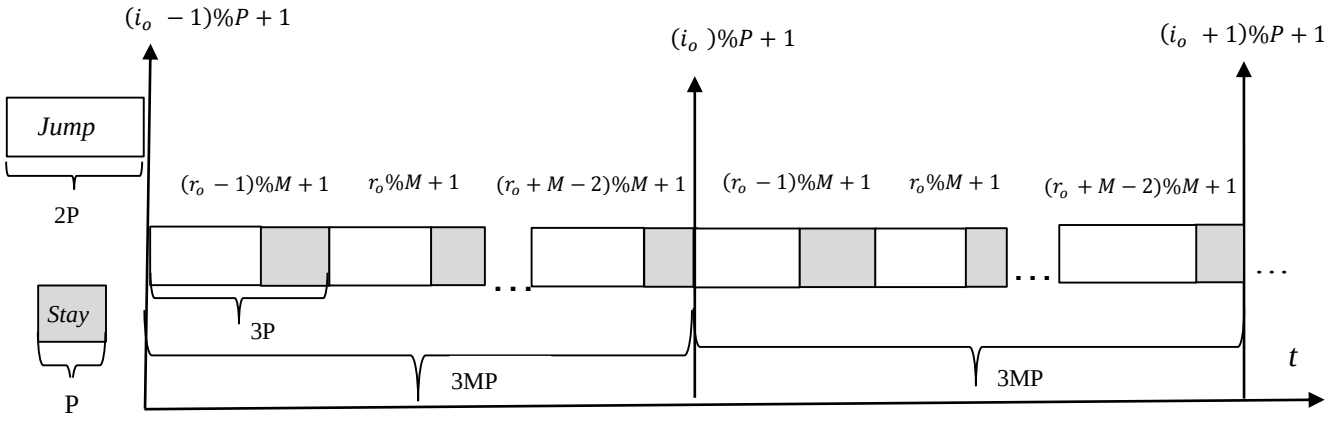



Figura 2.3: Secuencia de salto de canal del algoritmo *Jump-Stay* [7].

En el patrón de salto, el usuario comienza a saltar con índice $q$ y longitud del paso $r$. En el patrón de estancia posterior, el usuario secundario permanece en el canal $r$ que es la longitud del paso de esa ronda, durante $P$ ranuras de tiempo. El parámetro $P$, es el mismo en todas las rondas, mientras que $r$ y q deben ser ajustados correctamente de acuerdo a las siguientes reglas con el fin de garantizar el *rendezvous* de los usuarios secundarios:

- La longitud del paso, $r$ es un número entero entre $[1, M]$.
- En cada ronda de $3P$ ranuras de tiempo, $r$ mantiene su valor. En la siguiente ronda, $r$ cambia al siguiente número entre $[1, M]$.

- El índice de arranque, $q$ toma valores enteros entre $[1, P]$.
- El índice de arranque, $q$ cambia al siguiente número entre $[1, P]$ cada $M$ rondas de $3MP$ ranuras de tiempo.

La implementación de este algoritmo se basa en la función *JSHopping*, que se muestra en la Figura 2.4 y es la que se encarga de decidir el próximo salto en el intervalo de tiempo $t$ [7]. En la línea 1, la variable $t$ es un contador de intervalos de tiempo a partir de 0. En la línea 6, hay una operación de reasignación, si el índice de canal generado $j$ excede a $M$, (esto es posible ya que $P$ es mayor que $M$).

**Función JSHopping**

1: **Entradas**: $M, P, r, q, t$
2: $t = mod\ (3P)$;
3: **if** $(t < 2P)$
    $j = \ ((q + tr - 1)\ mod\ P)\ + 1$;
4: **else** $j = r$;
5: **end**
6: **if** $(j > M)$
    $j \ = \ ((j — 1)\ mod\ M)\ + 1$;
7: **end**
8: **Salida** $c = c_j$

Figura 2.4: Seudocódigo de la función *JSHopping*.

El seudocódigo del algoritmo *Jump-Stay* para dos usuarios se presenta en la Figura 2.5. El valor inicial de la longitud del paso $(r_o)$ y del índice de arranque $(q_o)$ se establece mediante el empleo de la función *rand*. El algoritmo JS puede proporcionar el *rendezvous* en una de las tres posibles combinaciones de patrones: *jump-stay* (*stay-jump* es equivalente a *jump-stay*), *jump-jump* y *stay-stay*. La combinación *jump-stay* significa que el *rendezvous* se logra en el solapamiento entre el patrón de salto de un usuario secundario con el patrón de estancia del otro usuario secundario (el patrón *jump-jump* y el *stay-stay* se definen de forma similar) [7].

**Algoritmo JS_2**

1: **Entrada**: $M$

2: $P = \ menor\ número\ primo\ mayor\ que\ M$

3: $r_o$=$rand[1, M]$;

$q_o = rand[1, P]$;

$t = 0$;

4: **while** (no *rendezvous*)

5: $n = \ [t/3P]$;

$r = ((r_o + n - 1)\ mod\ M + 1)$;

6: $m = \ [t/3PM]$;

$i = \ ((q_o + m - 1)\ mod\ P + 1)$;

7: $S\ (t)\ = \ JSHopping\ (M, P, r, q, t)$

8: $t = t + 1$;

9: Intentar *rendezvous* en el canal $S\ (t)$

10: **end**

2.5: Seudocódigo del algoritmo *Jump-Stay*.

### 2.2.3 Algoritmo *Short Sequence Based*

El algoritmo *Short Sequence Based* (SSB) [8], propone una secuencia de salto de canal determinista. Para generar la secuencia los $M$ canales disponibles de la red, cuyas etiquetas son conocidas por todos los usuarios secundarios, se ubican en un segmento discreto. Los US inician sus secuencias de salto de canal en un extremo del segmento y avanzan progresivamente al otro extremo, una vez alcanzado el final del segmento, ellos retornan por el camino opuesto.

En algunos casos, cuando los US saltan a puntos discretos (canales) del segmento, ellos trasponen sus posiciones sin lograr el *rendezvous*. Para evitar que puedan transponerse sin *rendezvous* al arribar al extremo inicial del segmento cada US espera una ranura de tiempo, logrando así que en la próxima ronda coincidan. En el segmento continuo dos US pueden alcanzar el *rendezvous*, antes de que el segundo usuario en iniciar la secuencia alcance el extremo del segmento.

La representación gráfica de la secuencia de salto de canal se muestra en la Figura 2.6. La línea sólida representa la secuencia de salto de canal de SSB, descrita matemáticamente en [8]. La línea discontinua representa el patrón de un usuario diferente, este inicia $d_o$ranuras de tiempo antes. Estas curvas se intersectan en varios puntos, sin embargo según lo planteado en [8], solo los puntos correspondientes a un valor entero en el eje de las ordenadas son válidos.

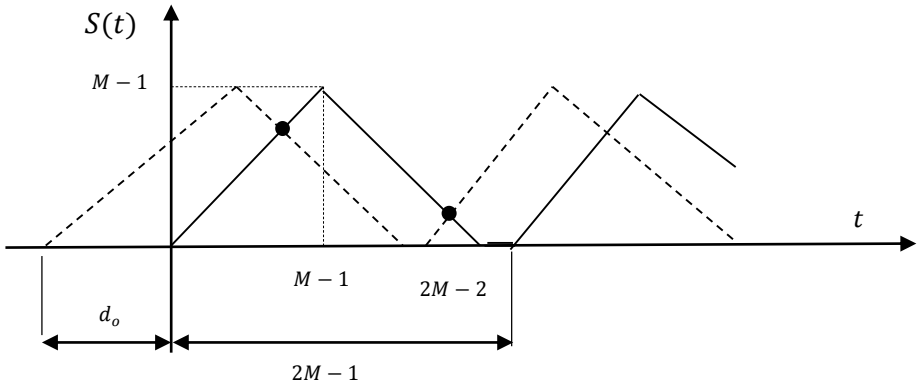



Figura 2.6: Período de la secuencia para el algoritmo de *rendezvous* SSB [8].

El seudocódigo de este algoritmo se muestra en la Figura 2.7. Donde $k \in \mathbb{N}$ es el número de períodos que ha realizado el US. El período de la secuencia es $2M-1$ y es más corto que el de otras secuencias de salto de canal, como *Jump-Stay*.

**Algoritmo SSB**

1: **Entradas**: $t, k, M$
2: **if** $k\,(2M-1) \leq t \leq k\,(2M-1) + M$
3: $\quad S(t) = (t + k)\ mod\ M$
4: **else**
5: $\quad S(t) = M - 2 - (t + k)\ mod\ M$
6: **end**
7: **Salida** $S(t)$

Figura 2.7: Seudocódigo del algoritmo SSB.

## 2.3 Parámetros de evaluación

Cuando se utilizan estrategias de salto de canal (CH, *Channel Hopping*) para lograr el *rendezvous*, el tiempo es dividido en ranuras de duración fija [53]. El tiempo de *rendezvous*

(TTR, *Time to Rendezvous*) es definido como el número de ranuras de tiempo necesarias para encontrar un canal común, después que todos los usuarios secundarios han comenzado su secuencia de salto de canal [7]. El TTR de un algoritmo de CH generalmente no es constante debido al tiempo de arranque aleatorio de las secuencias de CH. El TTR esperado (ETTR, *Expected TTR*) y el TTR máximo (MTTR, *Maximum TTR*), son métricas comúnmente empleadas para evaluar el desempeño de los algoritmos de *rendezvous*.

Estas métricas expresan el número de ranuras de tiempo que los nodos cognitivos necesitan saltar como máximo (MTTR) o como promedio (ETTR) antes de que puedan encontrarse en un canal común que se encuentre disponible [37]. Varios autores adoptan el término de tiempo de *rendezvous* máximo condicional (MCTTR, *maximum conditional TTR*) para referirse al MTTR del modelo asimétrico [40]. Es decir el MTTR cuando no todos los canales están disponibles para los usuarios cognitivos. Si el valor de MCTTR es finito, los usuarios cognitivos logran el *rendezvous* aun cuando solo exista un canal comúnmente disponible, en tal caso se dice que las secuencias de saltos garantizan el *rendezvous*.

En varios algoritmos de *rendezvous* los valores teóricos de ETTR y MTTR especificados por los autores difieren de los valores prácticos. En [54] se muestra la correspondencia entre los valores teóricos y simulados de dichas métricas para determinados algoritmos de *rendezvous*.

En la Tabla 2.1, se muestran los valores teóricos de ETTR y MTTR que brindan los autores de los algoritmos de *rendezvous* mencionados en el subepígrafe 1.3.1, para los modelos simétrico y asimétrico, considerando el *rendezvous* de dos usuarios.

Tabla 2.1 ETTR y MTTR

| Algoritmos | ETTR | | MTTR | |
|---|---|---|---|---|
| | Modelo Simétrico | Modelo Asimétrico | Modelo Simétrico | Modelo Asimétrico |
| MC | $2P^2/(P-1)$ | desconocida | $2P$ | desconocida |
| MMC | desconocida | desconocida | desconocida | desconocida |
| GOS | $\frac{(M^4+2M^2+6M-3)}{(3M^2+3M)}$ | X | $M(M+1)$ | X |
| ASYNC-ETCH | $(2M^2+M)/(M-1)$ | X | desconocida | X |
| SSCH | desconocida | X | desconocida | X |

| | | | | |
|---|---|---|---|---|
| AMRCC | desconocida | desconocida | desconocida | desconocida |
| CRSEQ | desconocida | desconocida | $\geq (P-1)(3P-1)$ | $P(3P-1)$ |
| DRSEQ | desconocida | X | $2M+1$ | X |
| JS | $< 5P/3 + 3$ | $2MP(P-G)+(M$ $+5-P-(2G$ | $3P$ | $3MP(P-G)+3P$ |
| EJS | $3P/2+3$ | desconocida | $4P$ | $4P(P+1-G)$ |
| SSB | $2(M-1)^2/(2M-1)$ | desconocida | $2M-2$ | $(M-1)(2M-1)$ |
| FRCH | desconocida | desconocida | $2M+1$ | $M(2M+1)^*$ |

La "X" denota que el algoritmo no puede ser aplicado en ese modelo de red y "desconocida" que el algoritmo es aplicable pero su desempeño no se conoce, no lo brinda el autor. El número de canales disponibles se representa por $M$, $P$ es el menor número primo mayor o igual a $M$ y $G$ es el número de canales disponibles comunes entre todos los usuarios secundarios de la red radio cognitiva. * El algoritmo solo garantiza el *rendezvous* para determinados valores de $M$.

A partir de la Tabla 2.1 se puede establecer una comparación entre los diferentes algoritmos de *rendezvous*. Por ejemplo, en términos de ETTR el desempeño del algoritmo MC es superior al algoritmo GOS, pero no garantiza el *rendezvous*. El algoritmo EJS con respecto al JS obtiene menores valores de MTTR en el modelo asimétrico pero incrementa ligeramente el MTTR en el modelo simétrico. El SSB supera el desempeño del FRCH en términos de MTTR en el modelo asimétrico. Nótese que pocos autores realizan el análisis analítico de todas las métricas relacionadas con el TTR. Además, sin la información del modelo de red, los usuarios secundarios no pueden escoger previamente los algoritmos de *rendezvous* apropiados. Se infiere la necesidad de utilizar algoritmos de *rendezvous* adaptables y con un buen desempeño en los modelos simétrico y asimétrico

En la presente investigación se analiza el incremento que experimenta el ETTR y MTTR de los algoritmos de *rendezvous* seleccionados en el epígrafe 2.2 ante interferencias en la red radio cognitiva. Además se determina el porciento de veces que el usuario interferente coincide con el *rendezvous* de los usuarios secundarios y el porciento de veces que coincide con al menos uno de los usuarios secundarios en un mismo canal, con respecto a un número específico de *rendezvous* y al número de canales disponibles en la red para los usuarios secundarios. Los casos en que el usuario interferente coincida con ambos usuarios en un canal común se le denomina

casos de no *rendezvous* por interferencias, mientras que los casos en que coincida con un usuario de manera independiente se le denomina encuentro con interferencias.

## 2.4 Conclusiones del capítulo

En este capítulo fueron seleccionados y descritos tres algoritmos cuyo objetivo común es lograr el *rendezvous* de los usuarios secundarios en una red radio cognitiva. En la selección de los algoritmos se tuvo en cuenta el uso que hacen estos algoritmos de la aleatoriedad, lo que pude ser utilizado ante interferencia. Además dichos algoritmos no requieren la sincronización de los usuarios secundarios, son aplicables en los modelos de red simétricos y asimétricos, y su uso pueda ser extendido al *rendezvous* de múltiples usuarios. Los algoritmos abordados son los siguientes:

- Aleatorio: cada usuario secundario decide su propia secuencia de salto en base a sus canales disponibles, de forma aleatoria, pero no puede garantizar el *rendezvous* de los usuarios secundarios en un tiempo finito.

- *Jump-Stay*: cada usuario secundario consta de un patrón de salto (*jump*) y un patrón de estancia (*stay*), en ese orden, para garantizar el *rendezvous*. Para que el usuario secundario genere los dos patrones en una ronda, es necesario seleccionar tres parámetros: el menor número primo, mayor que el número de canales disponibles en la red ($P$), la longitud del paso ($r$); y el índice de arranque ($q$). En el patrón de salto, el usuario comienza con el índice $q$ y salta en el intervalo de [1, P], con la longitud del paso $r$. En el patrón de estancia posterior, el usuario secundario permanece en el canal $r$ que es la longitud del paso de esa ronda.

- *Short Sequence Based*: cada usuario secundario inicia su secuencia de salto de canal en un extremo del segmento formado por los canales libres de la red y avanza progresivamente al otro extremo, una vez alcanzado el final del segmento, retorna por el camino opuesto. Al arribar al extremo inicial del segmento el usuario secundario espera una ranura de tiempo.

Para comparar los algoritmos ante interferencias se analiza el incremento de las métricas: ETTR y MTTR. Además del porciento de veces que los usuarios secundarios coinciden con

interferencias de manera independiente o simultánea, con respecto a un número específico de *rendezvous* y al número de canales disponibles en la red, en un escenario de comunicación ideal.

# CAPÍTULO 3. EVALUACIÓN DE LOS ALGORITMOS DE *RENDEZVOUS* CIEGO

En este capítulo se presentan los resultados obtenidos en la evaluación de los algoritmos de *rendezvous* ciego: Aleatorio, *Jump-Stay* y *Short Sequence Based*; ante interferencias. La evaluación se realiza en términos de tiempos de *rendezvous* y porcientos de interferencias. En el epígrafe 3.1 se describen los experimentos realizados. En el epígrafe 3.2 se muestra el desempeño de cada uno de los algoritmos seleccionados. Para ello se comparan los resultados de ETTR, MTTR, porcientos de no *rendezvous* por interferencias y porcientos de encuentro con interferencias, en función de la disponibilidad de canales de la red radio cognitiva. En el epígrafe 3.3 se compara el desempeño del algoritmo *Short Sequence Based* cuando existe un usuario malicioso adaptable en la red con respecto a la presencia del usuario interferente aleatorio. En el epígrafe 3.4 se presentan las conclusiones del capítulo.

## 3.1 Descripción de los experimentos realizados

Para las simulaciones que se presentarán a partir del epígrafe 3.2, se asume un escenario de comunicación ideal. Donde todos los canales están disponibles tanto para los dos usuarios secundarios como para el usuario que interfiere. El cambio de estado de cada canal es percibido de la misma forma por cada uno de ellos. El número de canales disponibles varía de 5 a 25 con un incremento de 1. El usuario interferente no tiene en cuenta detecciones del espectro previas, no conoce el canal en que los usuarios secundarios inician su secuencia de salto de canal, ni el intervalo de tiempo en el que comienza el proceso de *rendezvous*.

Las simulaciones realizadas evalúan el desempeño de los algoritmos de *rendezvous* ciego: Aleatorio, *Jump-Stay* y *Short Sequence Based*, y se organizan de la siguiente forma. En el epígrafe 3.2 se estiman los ETTR y MTTR de dos usuarios secundarios y de dos usuarios secundarios ante interferencias de un usuario aleatorio. Los valores de ETTR y MTTR, se calculan como la media aritmética y el valor máximo del tiempo que demoran los dos usuarios cognitivos en encontrarse en un mismo canal disponible, sin la presencia de interferencias. El objetivo de estas simulaciones es comparar para diferente disponibilidad de canales, la variación

que experimentan las métricas ETTR y MTTR ante interferencias, utilizando diferentes algoritmos de *rendezvous* ciego.

En el epígrafe 3.2 se determina además, el porciento de interferencias que ocasiona un usuario aleatorio a los usuarios secundarios que utilizan los algoritmos de *rendezvous*: Aleatorio, *Jump-Stay* y *Short Sequence Based*. Para ello se determinan los casos de no *rendezvous* por la presencia de interferencias y los casos de encuentro con interferencias, como el número de veces que el usuario interferente coincide con ambos o con un usuario secundario respectivamente, en un mismo canal y una vez transcurridos 100 *rendezvous.* El número de *rendezvous* se elige de manera arbitraria para comparar por igual el desempeño de los algoritmos simulados.

En el epígrafe 3.3 se compara el desempeño del algoritmo *Short Sequence Based* cuando existe un usuario malicioso adaptable en la red con respecto a la presencia del usuario interferente aleatorio. Para ello se simula la presencia de un usuario malicioso que perfecciona su estrategia de ataque, en función de la información que tiene de la red. En este escenario el usuario malicioso conoce la secuencia de salto de canal utilizada por los usuarios secundarios para lograr el *rendezvous*. Con esa información el usuario malicioso genera su propia secuencia de salto de canal, basada en la probabilidad con que los canales disponibles son visitados por los usuarios secundarios.

En cada uno de los experimentos anteriores se realizan $10^5$ simulaciones con el software Matlab 10.0. Para lograr un error menor que el 5% del valor determinado en cada una de ellas, como se muestra en el anexo I. El cálculo del error se realiza según lo planteado en [55]:

*Si $\bar{x}$ (media muestral) se usa como estimación de $\mu$ (media real), podemos tener (1-$\alpha$)* 100% de confianza de que el error no excederá una cantidad específica $e$ cuando el tamaño de la muestra es:* $n = (\frac{Z_{\alpha/2}\sigma}{e})^2$

Donde $n$ es el número de simulaciones, $Z_{\alpha/2}$ determina el intervalo de confianza del 95%, $\sigma$ la desviación estándar y $e$ el error deseado.

## 3.2 Desempeño de los algoritmos de *rendezvous* ciego ante interferencias de un usuario aleatorio

En el presente epígrafe se estiman los valores de ETTR, MTTR, los porcientos de no *rendezvous* por la presencia de interferencias y los porcientos de encuentro con interferencias, para dos usuarios secundarios que intentan el *rendezvous*. Para cada una de las situaciones y algoritmos simulados se han utilizado diferentes simbologías, como muestra la leyenda en cada Figura. Mientras los colores de las gráficas rojo, azul y verde representan que los resultados obtenidos corresponden a los algoritmos de *rendezvous* ciego: Aleatorio, *Jump-Stay* y *Short Sequence Based*, respectivamente.

### 3.2.1 Tiempo de *rendezvous* esperado y tiempo de *rendezvous* máximo

La diferencia o incremento entre los valores de ETTR y MTTR de dos usuarios secundarios ante interferencias y los valores obtenidos para dos usuarios secundarios, es también un indicador graficado en esta sección para evaluar los algoritmos de *rendezvous* ciego.

En la Figura 3.1 se muestran los resultados obtenidos para el algoritmo Aleatorio. Los ejes de la gráfica muestran los valores de ETTR, expresados en ranuras de tiempo y el número de canales disponibles en la red para intentar el *rendezvous*. Ante interferencias, los valores de ETTR aumentan y coinciden con la disponibilidad de canales de la red, por lo que disminuye el desempeño del algoritmo. La diferencia entre los ETTR es de una ranura de tiempo y permanece constante ante diferente disponibilidad de canales en la red.

Los valores de MTTR se excluyen de las simulaciones para el algoritmo Aleatorio ya que como muestran los autores en [28], este no garantiza el *rendezvous* de los usuarios secundarios en un tiempo finito.

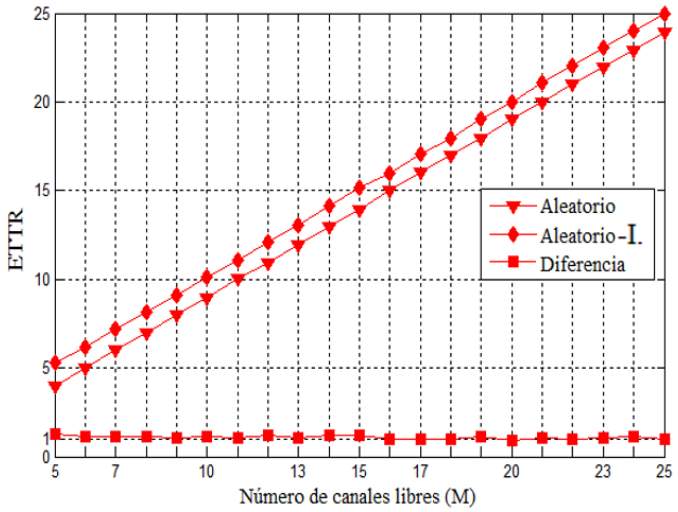
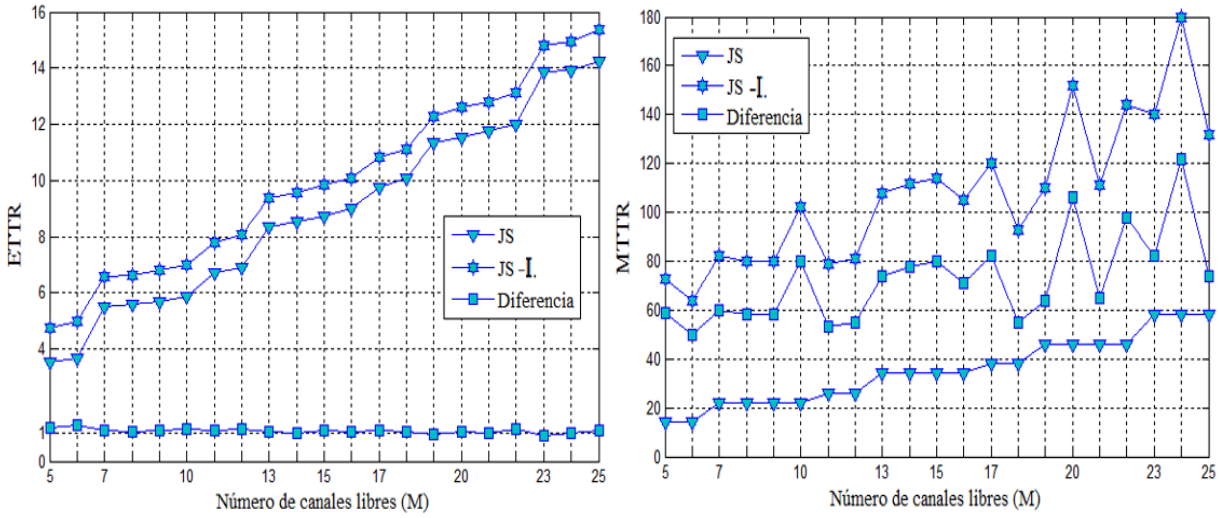


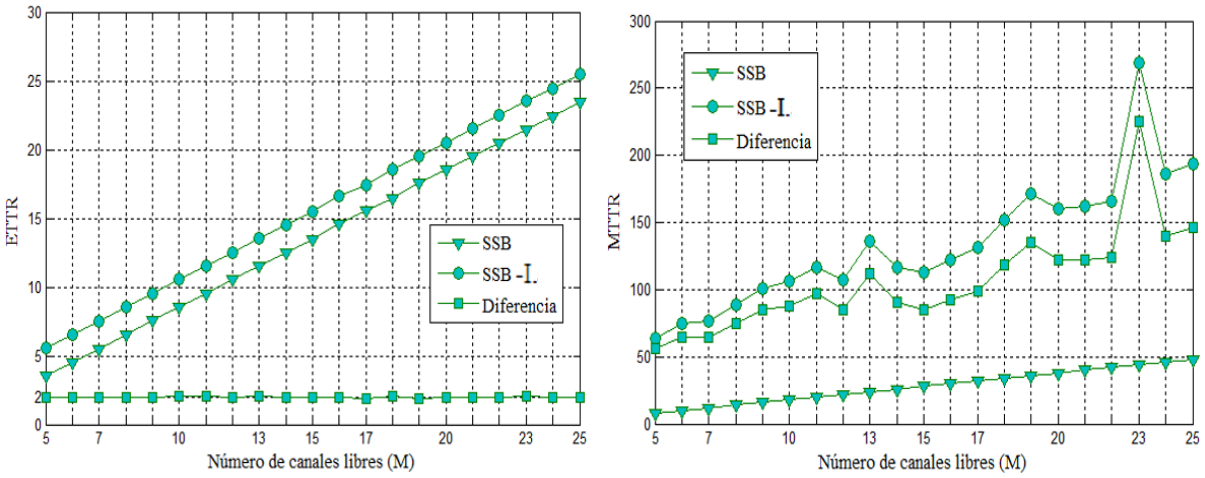

Figura 3.1: Desempeño del algoritmo Aleatorio en términos de ETTR.

Los resultados obtenidos en las simulaciones de los algoritmos de *rendezvous* ciego *Jump-Stay* y *Short Sequence Based* se muestran en las Figuras 3.2 y 3.3 respectivamente. Ante interferencias y el aumento del número de canales disponibles en la red, aumentan los valores de ETTR y MTTR. La diferencia entre los ETTR de ambos algoritmos es constante e igual a una ranura de tiempo para el algoritmo *Jump-Stay* y a dos para el algoritmo *Short Sequence Based*. Mientras la diferencia entre los MTTR de ambos algoritmos varía con la disponibilidad de canales en la red. Para ambos algoritmos el incremento del MTTR es superior al calculado para el *rendezvous* de dos usuarios secundarios sin interferencias.




(a) (b)

Figura 3.2: Desempeño del algoritmo *Jump-Stay*: a) ETTR y b) MTTR.




(a) (b)

Figura 3.3: Desempeño del algoritmo *Short Sequence Based*: a) ETTR y b) MTTR.

En las Figuras 3.4 y 3.5 se muestra el desempeño de los algoritmos Aleatorio, *Jump-Stay* y *Short Sequence Based*, en términos de ETTR y MTTR respectivamente, vistos anteriormente de manera independiente. Los resultados obtenidos para el *rendezvous* de dos usuarios secundarios, en cada uno de los algoritmos simulados, están acotados por los valores teóricos especificados por los autores, que se muestran en la Tabla 2.1. Para el *rendezvous* de dos usuarios secundarios sin interferencias, el algoritmo *Jump-Stay* presenta los menores valores de ETTR y el algoritmo *Short Sequence Based* los menores valores de MTTR. Ante interferencias los valores de ETTR y MTTR para cada uno de los algoritmos aumenta, debido a la presencia de interferencias y el algoritmo *Short Sequence Based* es el de peor desempeño.

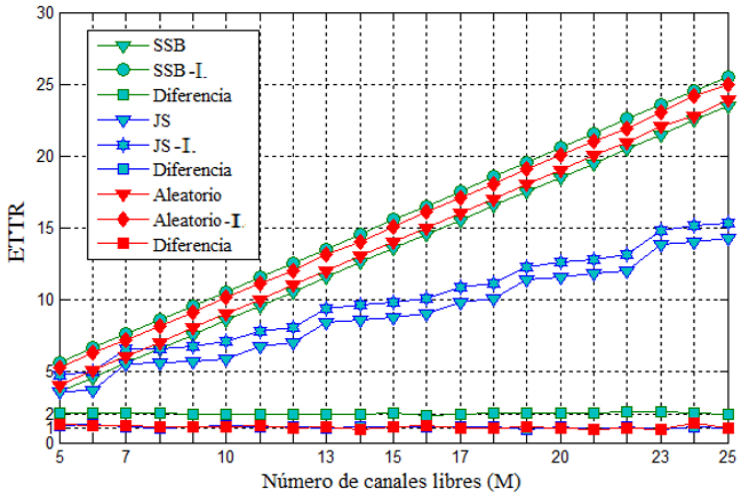
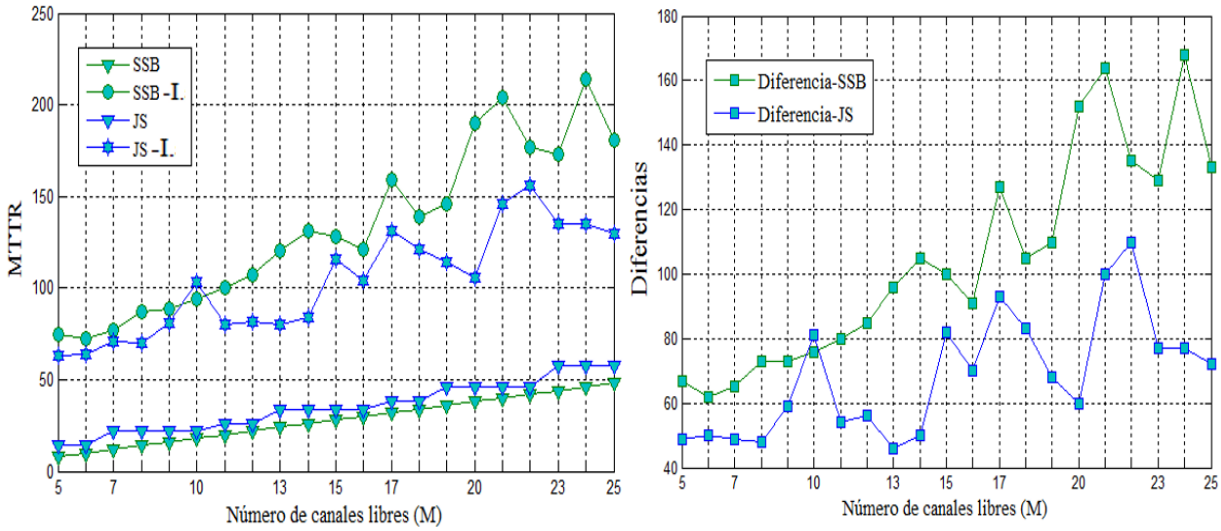



Figura 3.4: Desempeño de los algoritmos seleccionados en términos de ETTR.




(a) (b)

Figura 3.5: Desempeño de los algoritmos seleccionados: a) MTTR y b) Diferencias.

### 3.2.2 Porciento de interferencias

Los parámetros utilizados en esta investigación, para evaluar el desempeño de los algoritmos de *rendezvous* ciego seleccionados se encuentran relacionados entre sí. Los resultados obtenidos en esta sección dependen de los resultados anteriores y coinciden con el desempeño esperado. Para mayores tiempos de *rendezvous* esperados o máximo, mayores son las probabilidades de que coincidan los usuarios secundarios y el usuario interferente.

En las Figuras 3.6 y 3.7 se muestran los porcientos de no *rendezvous* por la presencia de interferencias y los porcientos de encuentro con interferencias para los algoritmos: Aleatorio, *Jump-Stay* y *Short Sequence Based*. En las Figuras 3.6 y 3.7 los ejes de las gráficas muestran el número de veces que un usuario interferente coincide con uno y con ambos usuarios secundarios en un mismo canal, durante 100 *rendezvous*, expresado en porcientos; y el número de canales disponibles en la red.

Observe que el número de casos en que coinciden los tres usuarios cognitivos disminuye con el aumento de la disponibilidad de canales en la red y es independiente de la secuencia de salto de canal utilizada por los usuarios secundarios.

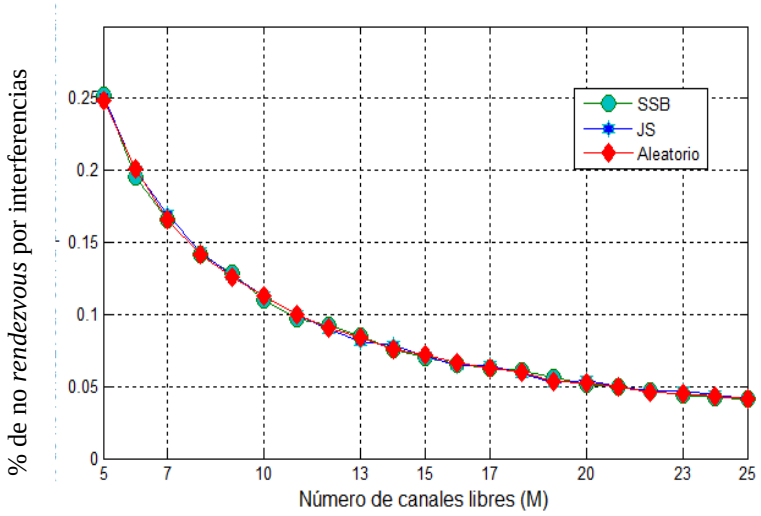



Figura 3.6: Porciento de no *rendezvous* por la presencia de interferencias.

En la Figura 3.7 para el algoritmo Aleatorio el usuario interferente coincide con al menos un usuario secundario 200 veces antes que los usuarios secundarios alcancen 100 *rendezvous*, sin importar el número de canales disponibles en la red. Mientras que el desempeño de los algoritmos *Jump-Stay* y *Short Sequence Based* varía ligeramente con la disponibilidad de canales. En el caso del algoritmo SSB sus resultados prácticamente duplican los obtenidos para el algoritmo Aleatorio. Si se compara los resultados que se muestran en las Figuras 3.6 y 3.7 el usuario interferente coincide con mayor frecuencia con solo un usuario secundario, y ello aumenta en mayor o menor medida en correspondencia con la estrategia de salto que utilice el usuario secundario.

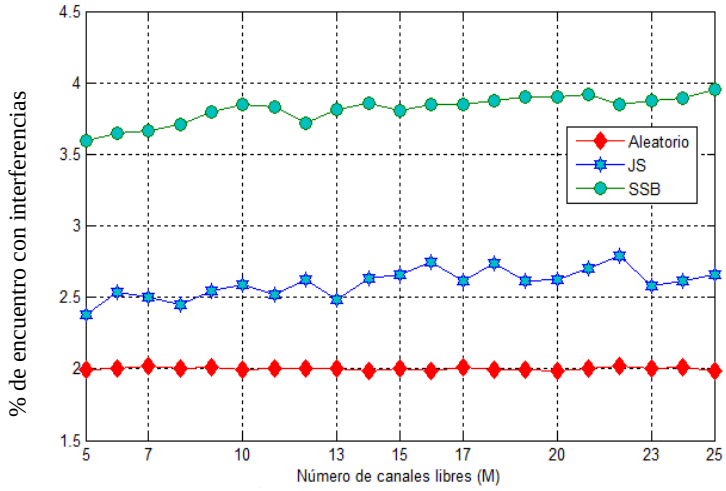



Figura 3.7: Porciento de encuentro con interferencias.

El algoritmo Aleatorio muestra mayor robustez ante interferencias, seguido por los algoritmos *Jump-Stay* y *Short Sequence Based*. Sin embargo el algoritmo Aleatorio no garantiza el *rendezvous* de los usuarios secundarios en un tiempo finito. El desempeño de estos algoritmos ante interferencias se puede explicar a través del uso que hacen de la aleatoriedad al generar sus secuencias de salto de canal. El peor desempeño es el del algoritmo determinista, *Short Sequence Based* y el algoritmo *Jump-Stay* logra un valor intermedio ya que su secuencia de salto de canal se genera a partir de parámetros aleatorios. Además, coinciden los mayores valores de ETTR y MTTR ante inferencias, con el mayor número de encuentro con interferencias para la estrategia de *rendezvous Short Sequence Based*.

## 3.3 Desempeño del algoritmo *Short Sequence Based* ante interferencias de un usuario malicioso adaptable

Las simulaciones realizadas anteriormente no toman en cuenta la intención del usuario interferente: maliciosa o no. Ambas intenciones afectan el *rendezvous* de los usuarios secundarios. Cuando la intención es maliciosa el usuario interferente puede suplantar la identidad de uno de los usuarios secundarios, denegar el servicio a los US, inyectar datos falsos en la red o robar información confidencial de esta. Las consecuencias de un usuario malicioso para la red radio cognitiva podrían ser mayores, no solo se afectaría el proceso de *rendezvous* o el funcionamiento del sistema, sino la seguridad, confidencialidad e integridad de la información. Sin embargo la intención maliciosa del usuario interferente no es suficiente, es necesario conocer la estrategia de ataque del usuario y sus potencialidades.

En el presente epígrafe se compara el desempeño del algoritmo *Short Sequence Based* cuando existe un usuario malicioso adaptable en la red con respecto a la presencia de un usuario interferente aleatorio. Un usuario malicioso adaptable, es un usuario cognitivo que detecta y ajusta sus estrategias de ataque en cada ranura de tiempo, basado en detecciones anteriores o en observaciones realizadas a la red [42]. En el presente epígrafe se asume que el usuario malicioso solo conoce la estrategia de salto de canal que siguen los US para lograr el *rendezvous*.

En función de la probabilidad de ocurrencia o veces que los canales disponibles ($M$) se repiten con respecto a $2M - 1$ que es el período de la secuencia de salto de canal del algoritmo *Short Sequence Based* se genera en la presente investigación una secuencia de salto de canal para el

usuario malicioso adaptable. En la Figura 3.8 se muestra el seudocódigo de la secuencia de salto de canal del usuario malicioso adaptable generada a partir de esta probabilidad.

En el seudocódigo mostrado en la Figura 3.8, se genera la secuencia de ataque a partir de un vector $b$, de 1000 elementos (el número de elementos es escogido de manera arbitraria) y valores aleatorios entre 0 y1. En función del número de canales disponibles, que determina el período de la secuencia de salto de canal de los usuarios secundarios y la probabilidad de ocurrencia de cada canal, se le asignó a cada elemento del vector $b$, un valor comprendido entre 1 y $M$. Por tanto el vector $p$, es un vector de 1000 elementos, con valores enteros entre 1 y $M$, donde la probabilidad de ocurrencia de cada canal depende de la secuencia de salto de canal *Short Sequence Based*.

**Secuencia de CH del usuario malicioso adaptable**

1: **Entrada**: $M$
2: $a = 1e3$;
3: b= $rand\ (1, a)$;
4: $p = ones\ (1, a)$;
5: $t = 1$;
6: $p\ (b <= \ (t/\ (2 * M - 1))) \ = M$;
7: $p\ (b > \ (t/\ (2 * M - 1))\ \&\ b <= \ ((t + 2)/\ (2 * M - 1))) \ = M - 1$;
8: $N = M - 1$;
9: **for** $t = 3{:}\ 2 : (\ 2 * M - 3)$
10: $N = N$;
11: $p\ (b > \ (t/\ (2 * M - 1))\ \&\ b <= \ ((t + 2)/\ (2 * M - 1))) \ = N - 1$;
12: $N = N - 1$;
13: **end**

Figura 3.8: Seudocódigo de la secuencia de CH del usuario malicioso adaptable.

### 3.3.1 Tiempo de *rendezvous* esperado y tiempo de *rendezvous* máximo

En las Figuras 3.9 y 3.10 se representan los valores de ETTR y MTTR, respectivamente, para dos usuarios secundarios sin interferencias y ante interferencias. Además de la diferencia entre estos parámetros. Los resultados señalados en color verde corresponden con los obtenidos ante

interferencias de un usuario aleatorio y los de color violeta con los resultados ante interferencias de un usuario malicioso adaptable.

El desempeño el algoritmo *Short Sequence Based* ante interferencias de un usuario malicioso adaptable, en términos de ETTR es el mismo que ante interferencias de un usuario aleatorio. Ante interferencias de un usuario aleatorio, los valores de MTTR aumentan.

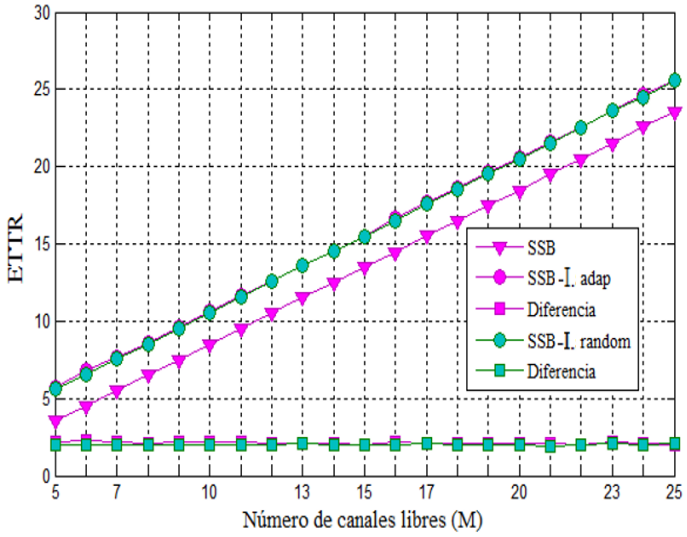
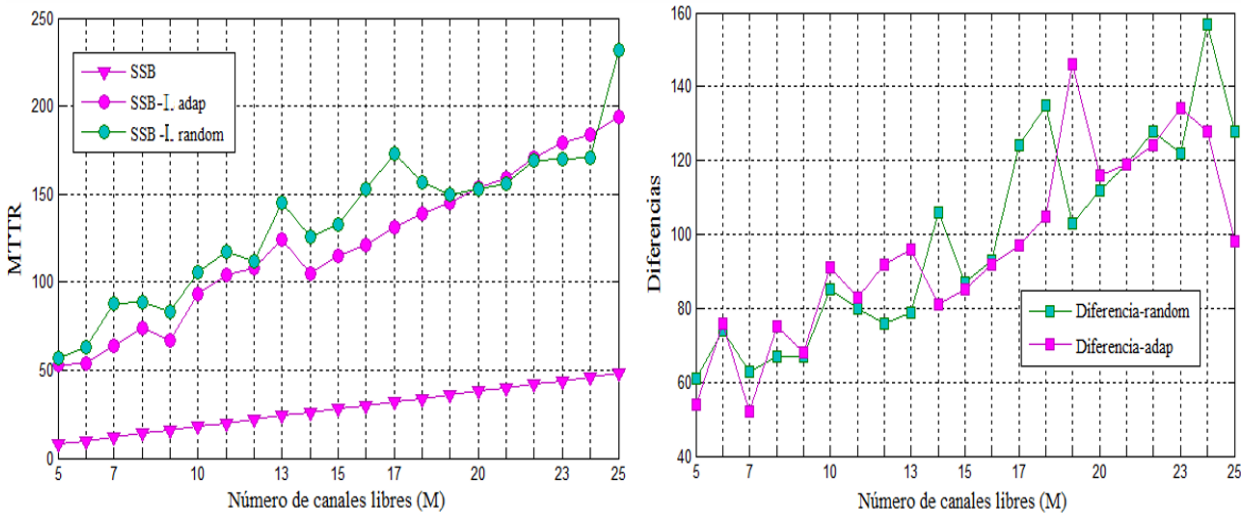



Figura 3.9: ETTR del algoritmo *Short Sequence Based* ante interferencias de un usuario aleatorio y un usuario malicioso adaptable.




(a) (b)

Figura 3.10: Desempeño del algoritmo *Short Sequence Based* ante interferencias de un usuario aleatorio y un usuario malicioso adaptable: a) MTTR y b) Diferencias.

### 3.3.2 Porciento de interferencias

En las Figuras 3.11 y 3.12 se muestran los porcientos de no *rendezvous* por la presencia de interferencias y los porcientos de encuentro con interferencias para el algoritmo *Short Sequence Based*. Los resultados de color verde corresponden con los obtenidos ante interferencias de un usuario aleatorio y los de color violeta con los resultados obtenidos ante interferencias de un usuario malicioso adaptable. Los porciento de no *rendezvous* por la presencia de interferencias y los porcientos de encuentro con interferencias para un usuario malicioso adaptable, se incrementa con respecto a los resultados obtenidos para un usuario interferente aleatorio.

En los resultados que se muestran en la Figura 3.11, el incremento es menor que 0.05%, es decir, en 100 *rendezvous* el usuario adaptable coincide en cinco ocasiones más que el usuario aleatorio con los dos usuarios secundarios en un mismo canal. El aumento ocurre para una disponibilidad de canales entre 5 y 10. Para una disponibilidad de canales entre 11 y 25, el comportamiento del algoritmo *Short Sequence Based*, es idéntico, para ambos usuarios interferentes.

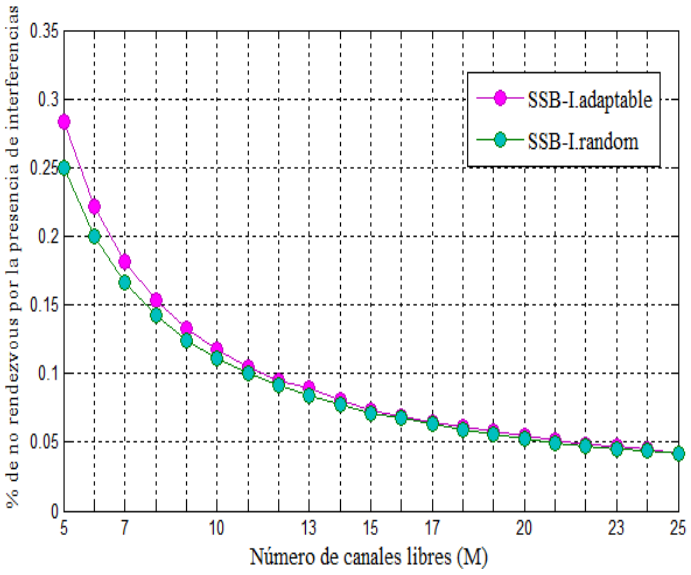



Figura 3.11: Porciento de no *rendezvous* por la presencia de interferencias.

En la Figura 3.12, el incremento de los porcientos de encuentro con interferencias de un usuario adaptable es mayor que para un usuario interferente aleatorio, para una disponibilidad de canales de la red que varía de 5 a 25. La diferencia entre los porcientos de encuentro con interferencias para los usuarios interferentes tiene un máximo de 0.25%, cuando existen 5 canales disponibles y una diferencia mínima, menor de 0.05% para una disponibilidad de 25 canales en la red.

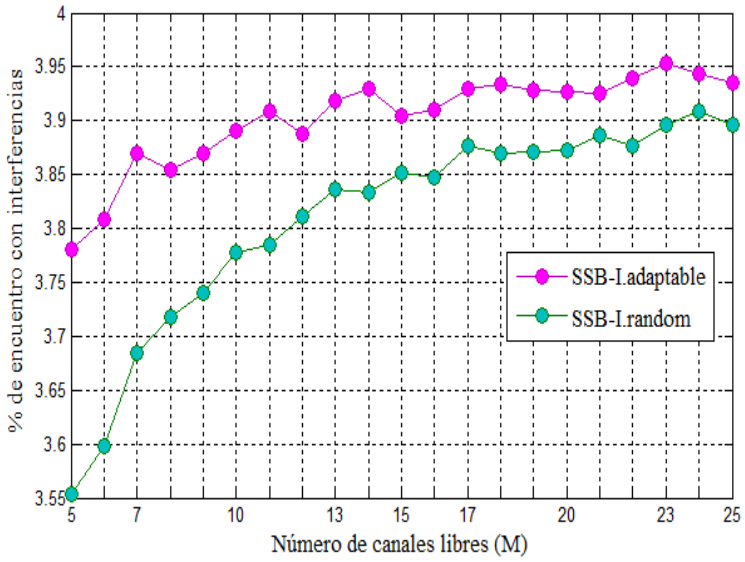



Figura 3.12: Porciento de encuentro con interferencias.

Ante la estrategia de ataque maliciosa adaptable el desempeño del algoritmo *Short Sequence Based* es menor, pero muy próximo a su rendimiento ante interferencias de un usuario aleatorio. Para mejorar o perfeccionar la estrategia de ataque del usuario malicioso adaptable es necesario que el usuario malicioso posea otras informaciones relacionadas con el funcionamiento de la red, por ejemplo, los canales en que comienzan los usuarios secundarios a saltar o el intervalo de tiempo en que inicia el proceso de *rendezvous.*

## 3.4 Conclusiones del capítulo

Para el *rendezvous* de dos usuarios secundarios sin interferencias, el algoritmo *Jump-Stay* presenta los menores valores de ETTR y el algoritmo *Short Sequence Based* los menores valores de MTTR. Ante interferencias el algoritmo *Short Sequence Based* es el de peor desempeño en términos de ETTR, MTTR y porciento de encuentro con interferencias. Lo que comprueba la relación entre los parámetros de evaluación utilizados en las simulaciones. En términos de porciento de interferencias el algoritmo Aleatorio es robusto, pero no garantiza el *rendezvous* de los usuarios secundarios en un tiempo finito.

El porciento de no *rendezvous* por la presencia de interferencias de un usuario aleatorio para dos usuarios secundarios, durante 100 *rendezvous* disminuye con el aumento de la disponibilidad de canales y es independiente de la secuencia de salto de canal utilizada por los usuarios secundarios.

El desempeño del algoritmo de *rendezvous Short Sequence Based* ante interferencias de un usuario aleatorio con respecto a un usuario malicioso adaptable, es similar en términos de ETTR y ligeramente menor en términos de MTTR. El nivel de conocimiento del usuario interferente adaptable, es decir, conocer la secuencia de salto de canal de los US, no es suficiente para superar los resultados obtenidos ante interferencias de un usuario aleatorio. Los canales en que comienzan los usuarios secundarios a saltar o el intervalo de tiempo en que comienza el proceso de *rendezvous* podría ser información útil, para desarrollar una estrategia de ataque adaptable óptima.

# CONCLUSIONES

A partir del cumplimiento de los objetivos planteados se arriba a las siguientes conclusiones:

- La tecnología radio cognitiva es un sistema inteligente de comunicaciones inalámbricas, consciente de su entorno y capaz de ajustar dinámica y autónomamente sus parámetros de operación (potencia de transmisión, frecuencia portadora y tipo de modulación) en tiempo real, de acuerdo al conocimiento obtenido para proporcionar una comunicación altamente confiable y utilizar eficientemente el espectro radioeléctrico. El *rendezvous* es un proceso esencial en redes radio cognitivas, debido a que el establecimiento de los usuarios en un canal disponible común es un requisito imprescindible para el establecimiento de la comunicación.

- Los algoritmos de *rendezvous* ciego basados en técnicas de salto de canal son ampliamente utilizados, porque el establecimiento de los recursos de negociación no depende del estado de un solo canal común. Sin embargo, es recomendable que la lista de secuencia de saltos pueda ser adaptable a la disponibilidad de canales de la red. Estos algoritmos logran el *rendezvous* en redes heterogéneas, y pueden clasificarse en algoritmos aleatorios, sincrónicos y asincrónicos.

- El objetivo de las interferencias ocasionadas por usuarios maliciosos es disminuir el rendimiento de las comunicaciones o interrumpirlas. Los usuarios maliciosos pueden equiparse con tecnología cognitiva o no y adoptar diferentes estrategias de ataque. La robustez de estas estrategias de ataque dependen de la información con que cuente el usuario malicioso, obtenida de detecciones previas. Mientras que los usuarios no maliciosos por encontrarse en el escenario de comunicación también reducen las posibilidades de *rendezvous*, al limitar la disponibilidad de canales de la red.
- Los principales indicadores o parámetros empleados para evaluar el desempeño de los algoritmos seleccionados ante interferencias son el tiempo de *rendezvous* esperado, tiempo de *rendezvous* máximo, porciento de encuentro con interferencias y porciento de no *rendezvous* por interferencias. Los resultados obtenidos muestran una

proporcionalidad directa entre los valores de ETTR, MTTR y el porciento de encuentro con interferencias.

- Los resultados obtenidos en la evaluación de los algoritmos de *rendezvous* ciego seleccionados permiten arribar a las siguientes conclusiones:
  - ✓ Para el *rendezvous* de dos usuarios secundarios sin interferencias, el algoritmo *Jump-Stay* presenta los menores valores de ETTR y el algoritmo *Short Sequence Based* los menores valores de MTTR.
  - ✓ Ante interferencias los algoritmos: Aleatorio, *Jump Stay* y *Short Sequence Based* son susceptibles. En todos los casos la presencia de interferencias en la red aumenta los valores de ETTR y MTTR. Los menores valores de ETTR y MTTR corresponden al algoritmo *Jump-Say*. En términos de porciento de encuentro con interferencias el algoritmo Aleatorio es robusto, pero no garantiza el *rendezvous* de los usuarios en un tiempo finito.
  - ✓ El desempeño del algoritmo de *rendezvous Short Sequence Based* ante interferencias de un usuario aleatorio con respecto a un usuario malicioso adaptable, es similar en términos de ETTR y ligeramente menor en términos de MTTR.

# RECOMENDACIONES

Se considera que las siguientes recomendaciones pueden ser de utilidad para enriquecer el estudio realizado y los resultados obtenidos:

- Evaluar los algoritmos de *rendezvous* ciego seleccionados ante interferencias, en escenarios simétricos y asimétricos.
- Desarrollar la estrategia de ataque del usuario malicioso adaptable basada en otras informaciones de la red, como el canal en que comienzan los usuarios secundarios a saltar y el instante en que comienza el proceso de *rendezvous*.
- Evaluar los algoritmos de *rendezvous* ciego ante interferencias de usuarios maliciosos con otras estrategias de ataque (engañoso, reactivo), en escenarios de red simétricos y asimétricos.

# REFERENCIAS BIBLIOGRÁFICAS


[1] S. Montejo, "Mecanismos de control y asignación de los recursos de transmisión mediante el conocimiento de la ubicación en las Redes Ad Hoc Radio Cognitivas," Tesis doctoral, Dpto. Electrónica y Telecomunicaciones, Universidad Central "Marta Abreu" de Las Villas, Santa Clara, Cuba, 2013.

[2] I. Akyildiz, W. Lee, M. Vuran, and S. Mohanty, "NeXt Generation/Dynamic Spectrum Access/Cognitive Radio Wireless Networks: A survey," *Computer Networks*, vol. 50, no. 13, pp. 2127-2159, Sept. 2006.

[3] G. Y. L. Ying-Chang Liang and K. Cheng Chen, "Cognitive radio: Networking and communications an overview," *IEEE Trans. Veh. Technol*., vol. 60, no. 7, pp. 3386 -3407, 2011.

[4] L. Lu, X. Zhou, U. Onunkwo, and G. Y. Li, "Ten years of research in spectrum sensing and sharing in cognitive radio," *EURASIP Journal on Wireless Communications and Networking*, no. 28, pp. 1-16, 2012.

[5] J. Mitola and G.Q. Jr. Maguire, "Cognitive radio: making software radios more personal," *IEEE Personal Communications,* vol. 6, no. 4, pp. 13–18, Agosto 1999.

[6] R. Di Pietro and G. Oligeri, "Jamming mitigation in cognitive radio networks," *Network IEEE*, vol. 27, no. 3, pp. 10-15, 2013.

[7] H. Liu, Z. Lion, X Chu, and Y. W. Leung, "Jump-Stay Rendezvous Algorithm for Cognitive Radio Networks," *IEEE Transactions on parallel and distributed systems*, vol.23, no 10, pp. 1867-1881, Oct 2012.

[8] V. Alfonso, E. Ortiz, R. Souza, E. Fernandez, and G. Brante, "Short Channel Hopping Sequence Approach to Rendezvous for Cognitive Networks," *IEEE Communications Letters*, vol. 18, no. 2, pp. 289-292, Febrero 2014.

[9] Z. Htike, C. S. Hong, & S. Lee, "The life cycle of the rendezvous problem of cognitive radio ad hoc networks: a Survey," *Journal of Computing Science and Engineering*, vol. 7, no. 2, pp. 81–88, Junio 2013.

[10] S. Dolev, S. Gilbert, R. Guerraoui, and C. Newport, "Secure communication over radio channels," in *Proceedings of the twenty-seventh ACM symposium on Principles of distributed computing*, New York, USA: ACM, pp. 105–114, 2008.

[11] Joseph Mitola III, Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio, PhD Thesis, Royal Institute of Technology (KTH), Sweden, May 2000.

[12] FCC, "Notice of Proposed Rulemaking (NPRM 03 322): Facilitating Opportunities for Flexible, Efficient and Reliable Spectrum agile Radio Technologies" ET Docket no. 03, pp. 108, Dec. 2003.

[13] IEEE USA, "Improving Spectrum Usage through Cognitive Radio Technology," *IEEE USA Position*, Nov. 2003.

[14] S. Filin, et al., "International Standardization of Cognitive Radio Systems," *IEEE Communications Magazine*, vol.49, no. 3, pp. 82-89, 2011.

[15] S. Haykin, "Cognitive Radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol.23, no. 2, pp. 201-220, 2005.

[16] Peh, E. C. Y., et al., "Sensing and power control in cognitive radio with location information," in *IEEE International Conference on Communication Systems*, pp. 255-259, 2012.

[17] L. Bordón, & S. Montejo, "La radio cognitiva y su impacto en el uso eficiente del espectro de radio," *Revista de Ingeniería Electrónica, Automática y Comunicaciones (RIELAC)*, vol. XXXVI, no.1, pp.42-55, Enero–Abril 2015.

[18] B. Wang, & K. Ray Liu, "Advances in Cognitive Radio Networks: A Survey," *IEEE Journal Selected Topics Signal Process*, vol.5, no.1, pp. 5-22, 2011.

[19] P. Kolodzy et al., "Next generation communications: Kickoff meeting," in *Proc. DARPA*, vol. 10, 2001.

[20] I. F. Akyildiz, W. Lee, & K.R. Chowdhury, "CRAHNs: Cognitive radio ad hoc networks," *Ad Hoc Networks*, vol.7, no.5, pp. 810-836, 2009.

[21] Q. Wang, K. Ren & P.Ning, "Anti-jamming Communication in Cognitive Radio Networks with Unknown Channel Statistics," *19th IEEE International Conference on Network Protocols*, 2011.

[22] C.R. Stevenson, G. Chouinard, Z. Lei, W. Hu, S.J. Shellhammer, and W. Caldwell, "IEEE 802.22: The First Cognitive Radio Wireless Regional Area Network Standard," *IEEE Comm. Magazine*, vol. 47, no. 1, pp. 130-138, Jan. 2009.

[23] H. Liu, Z. Lin, X. Chu, & Y.-W. Leung, "Taxonomy and challenges of rendezvous algorithms in cognitive radio networks," In *Proc. of the IEEE ICNC Conf.*, pp 645–649, Enero 2012.

[24] S. Miller K. Ryan M. M. Buddhikot, P. Kolodzy and J. Evans, "DIMSUMnet: New directions in wireless networking using coordinated dynamic spectrum," In *proceedings of IEEE WoWMoM*, pp 78–85, IEEE, June 2005.

[25] L. Ma, X. Han, and C.-C. Shen, "Dynamic Open Spectrum Sharing for Wireless Ad Hoc Networks," *Proc. IEEE Int'l Symp. New Frontiers in Dynamic Spectrum Access Network (DySPAN '05)*, pp. 203-213, Nov. 2005.

[26] K. Bian, & R. Chen, "Control Channel Establishment in Cognitive Radio Networks using Channel Hopping," *IEEE Journal on Selected Areas in Communications*, vol.29, no.4, pp. 689-703, Abril 2011.

[27] Y. Li, "A MAC Protocol Supporting Dynamic Control Channel for Cognitive Radio Ad Hoc Networks," In *International Conference on Electronics, Communications and Control (ICECC)*, pp37-40, Ningbo, China, September 2011.

[28] B.F. Lo, "A Survey of Common Control Channel Design in Cognitive Radio Networks," *Physical Communications*, vol. 4, pp. 26-39, 2011.

[29] Y. Kondareddy, P. Agrawal, and K. Sivalingam, "Cognitive RadioNetwork Setup without a Common Control Channel," *Proc. IEEE Military Comm. Conf.* (*MILCOM '08)*, pp. 1-6, Nov. 2008.

[30] L. Lazos, S. Liu, and M. Krunz, "Spectrum Opportunity-Based Control Channel Assignment in Cognitive Radio Networks," *Proc. IEEE Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON '09),* pp. 1-9, June 2009.

[31] C. N. Theis, R.W. Thomas, & L. A. Dasilva, "Rendezvous for cognitive radios," *EEE Transactions on Mobile Computing*, vol.10, no.2, pp. 216–227, Febrero 2011.

[32] C. Cormio & K. R. Chowdhury, "Common control channel design for cognitive radio wireless ad hoc networks using adaptive frequency hopping," *Ad Hoc Networks*, vol. 8, no. 4, pp. 430-438, 2010.

[33] P. Bahl, R. Chandra, & J. Dunagan, "SSCH: Slotted Seeded Channel Hopping for Capacity Improvement in IEEE 802.11 Ad-Hoc Wireless Networks," *Proc. ACM Mobi Com*, vol.4, pp. 216-230, Sept. 2004.

[34] L. DaSilva & I. Guerreiro, "Sequence-Based Rendezvous for Dynamic Spectrum Access," Proc. *IEEE Int'l Symp. New Frontiers in Dynamic Spectrum Access Network (DySPAN)*, vol. 8, pp. 1-7, Oct. 2008.

[35] Y. SONG, & J. XIE, "A distributed broadcast protocol in multi-hop cognitive radio ad hoc networks without a common control channel," *Proceedings of the IEEE International Conference on Computer Communications*, Orlando, FL, pp. 2273-2281, 2012.

[36] K. Bian & J.Park, "Maximizing Rendezvous Diversity in Rendezvous Protocols for Decentralized Cognitive Radio Networks," *IEEE Trans. Mob. Comput*, vol.12, pp. 1294–1307, 2013.

[37] J. Shin, D. Yang, and C. Kim, "A Channel Rendezvous Scheme for Cognitive Radio Networks," *IEEE Comm. Letters*, vol. 14, no. 10, pp. 954-956, Oct. 2010

[38] D. Yang, J. Shin, & C. Kim, "Deterministic Rendezvous Scheme in Multichannel Access Networks," *Electronics Letters*, vol. 46, no. 20, pp. 1402-1404, 2010.

[39] Z. Lin, H. Liu, X. Chu, &Y.-W. Leung, "Enhanced jump-stay rendezvous algorithm for cognitive radio networks," *IEEE Communications Letters*, vol. 17, no. 9, pp.1742–1745, 2013.

[40] G.-Y. Chang & J.-F. Huang, "A fast rendezvous channel-hopping algorithm for cognitive radio networks," *IEEE Communications Letters*, vol.17, no. 7, pp. 1475–1478, 2013.

[41] *Public Notice*, Federal Communications Commission Enforcement Advisory no. 02, pp.1-2, Marzo 2012.

[42] B. Wang, Y. Wu, K. Ray Liu, & T. Clancy, "Anti-jamming games in multi-channel cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 1, pp. 4–15, Enero 2012.

[43] T. C. Clancy and N. Goergen, "Security in cognitive radio networks: threats and mitigation," in *Proc. International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, Singapore, May 2008.

[44] T. X. Brown and A. Sethi, "Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: A multi-dimensional analysis and assessment," *Mobile Networks and Applications*, vol. 13, no. 5, pp. 516–532, Oct. 2008.

[45] H. Li & Z. Han, "Dogfight in Spectrum: Combating Primary User Emulation Attacks in Cognitive Radio Systems, Part I: Known Channel Statistics", *IEEE Transactions on Wireless Communication*, vol. 9, no. 11, pp. 3566–3577, Noviembre 2010.

[46] Q. Peng, P. Cosman, & L. Milstein, "Spoofing or jamming: Performance analysis of a tactical cognitive radio adversary," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 4, pp. 903 –911, Abril 2011.

[47] --"Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, Part II: Unknown channel statistics," *IEEE Transactions on Wireless Communications*, vol. 10, no. 1, pp. 274–283,2011.

[48] T. Yucek and H. Arslan, "A Survey of Spectrum Sensing Algorithms for Cognitive Radio Applications," *IEEE Comm. Surveys & Tutorials*, vol. 11, no. 1, pp. 116-130, 2009.

[49] K. Bian & J.-M. Park, "Security vulnerabilities in IEEE 802.22," *The Fourth International Wireless Internet Conference (WICON2008)*, Noviembre 2008.

[50] B. Wang, Y. Wu, K. J. R. Liu, and T. C. Clancy, "A stochastic anti-jamming game in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, 2011.

[51] M. S. Kuran and T. Tugcu, "A survey on emerging broadband wireless access technologies," *Computer Networks*, vol. 51, pp. 3013-3046, 2007.

[52] E. Ortiz, V. Alfonso, R. Souza, G. Brante & E.M.G. Fernández, "Simple role-based rendezvous algorithm for cognitive ad hoc radio networks," *Electronics Letters 30th*,vol. 50 no. 3 pp. 182–184, Enero 2014.

[53] H. Liu, Z. Lin, X. Chu, and Y.-W. Leung, "Ring-walk based channel-hopping algorithms with guaranteed rendezvous for cognitive radio networks," in *Proc. IEEE/ACM Int'l Conf. on Green Computing*, pp.755–760.

[54] E. O. Guerra & V. Reguera, "Algoritmos de rendezvous para redes Radio Cognitivas," *Revista de Ingeniería Electrónica, Automática y Comunicaciones (RIELAC)*, vol. XXXVI, no. 3, pp. 35-45, Septiembre–Diciembre 2015.

[55] R. E. Walpole, R. H. Myers and S. Myers, "Problemas de estimación de una y dos muestras," in *Probabilidad y estadística para ingenieros*, Ed: F. Varela, La Habana, Cuba, 2007, pp. 245-248.

# ANEXOS

**Anexo I.** Error cometido en las simulaciones.

El error representado en cada una de las Figuras que se muestran a continuación, está expresado en porciento (%).

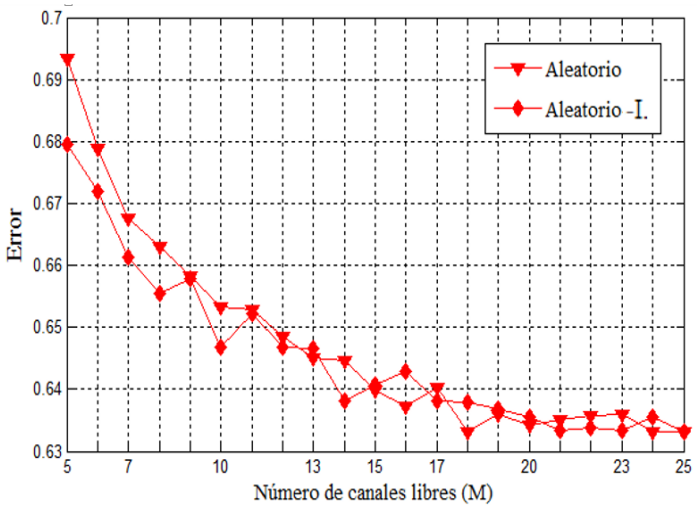
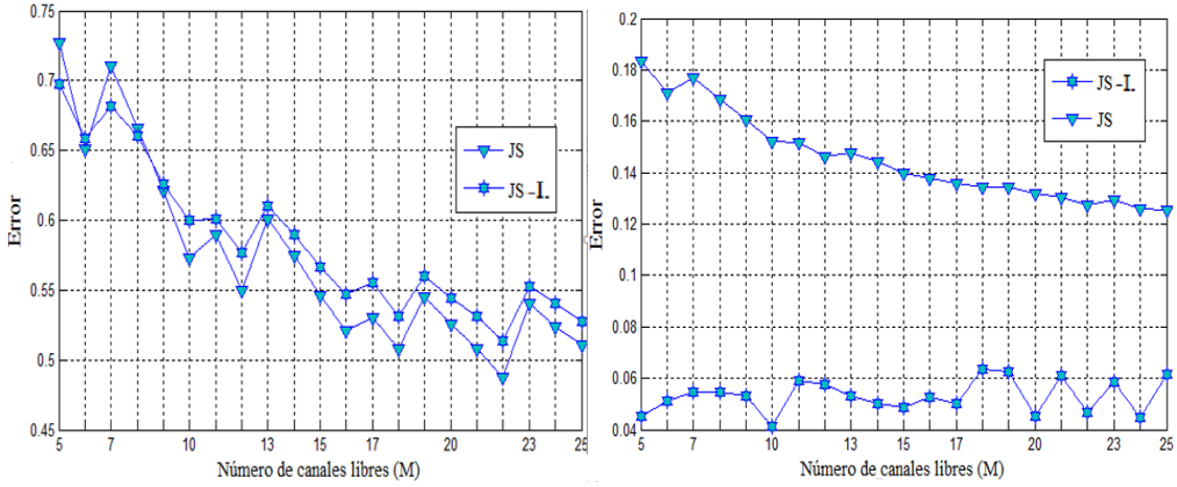
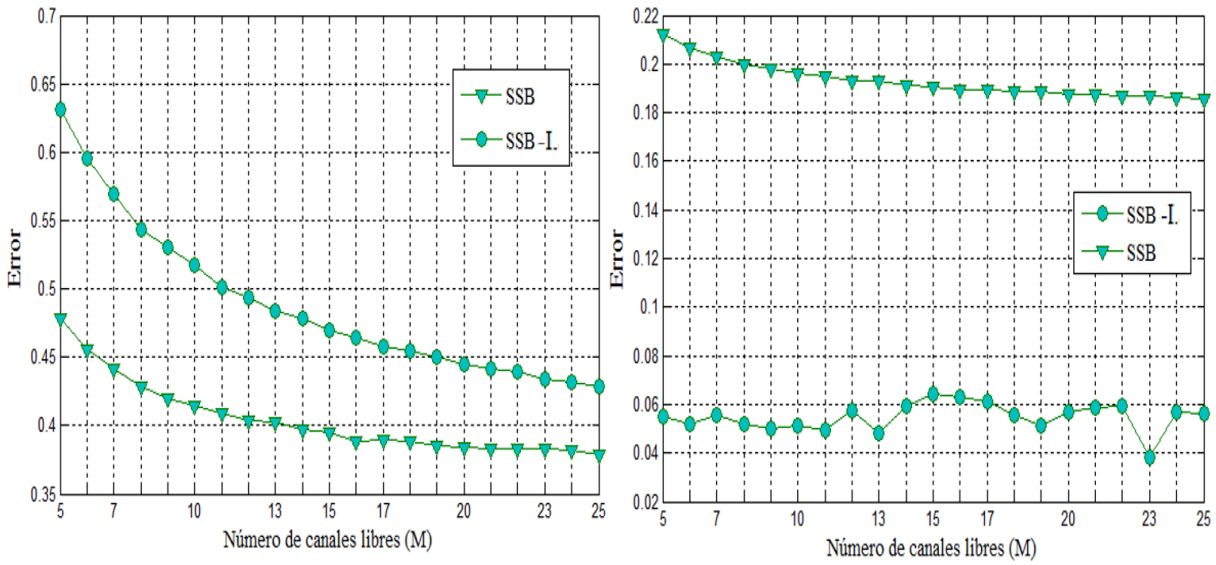



Figura A-I.1: Error cometido en las simulaciones del algoritmo Aleatorio al estimar el ETTR.



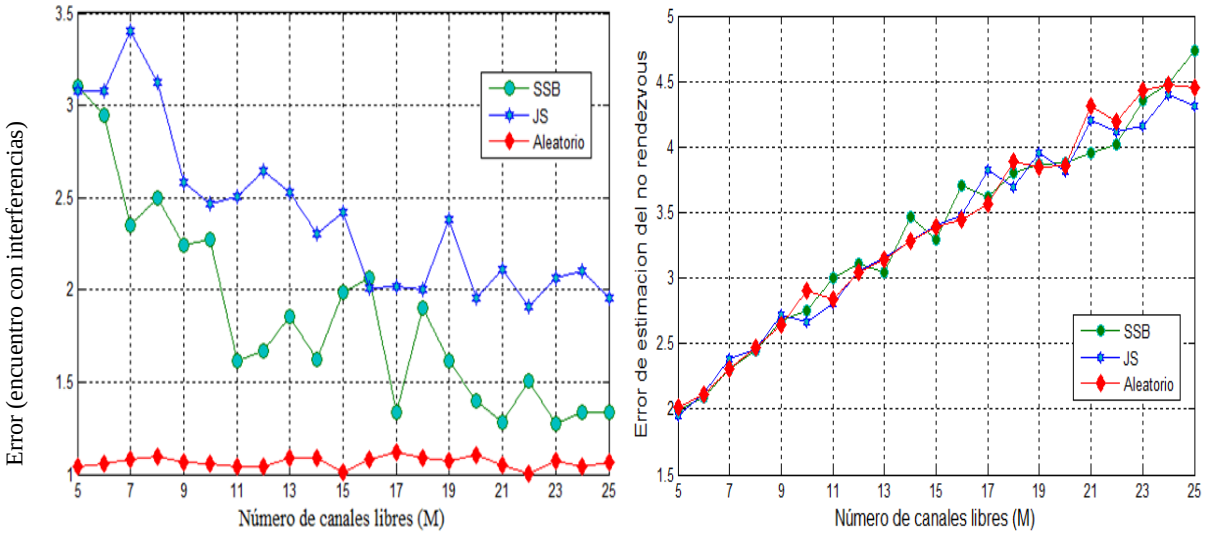

(a) (b)

Figura A-I.2: Error cometido en las simulaciones del algoritmo *Jump-Stay*: a) ETTR y b) MTTR.



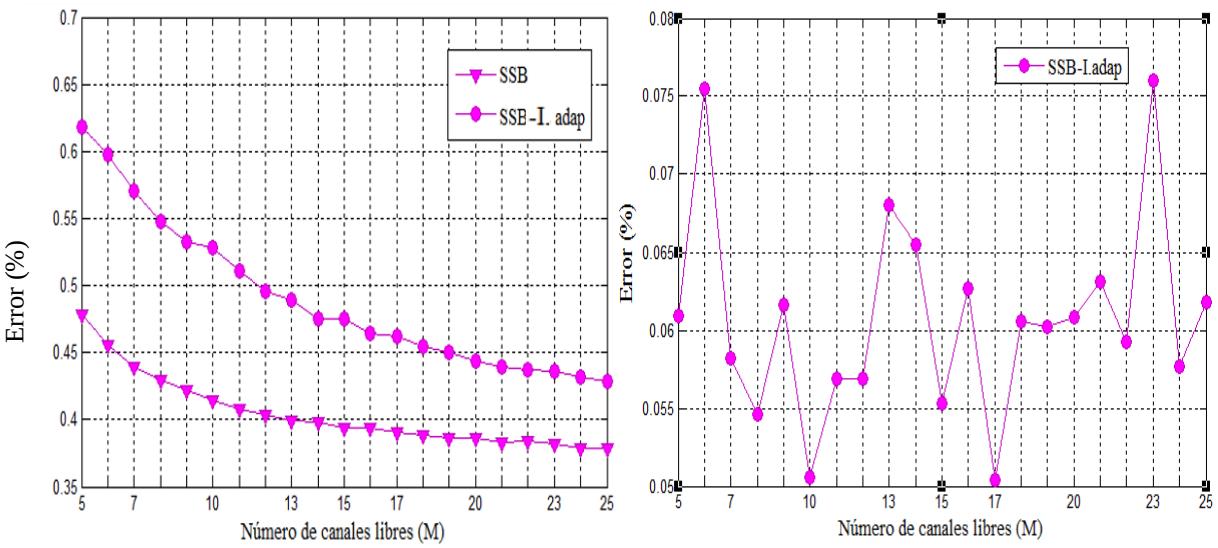

(a) (b)

Figura A-I.3: Error cometido en las simulaciones del algoritmo *Short Sequence Based*: a) ETTR y b) MTTR.



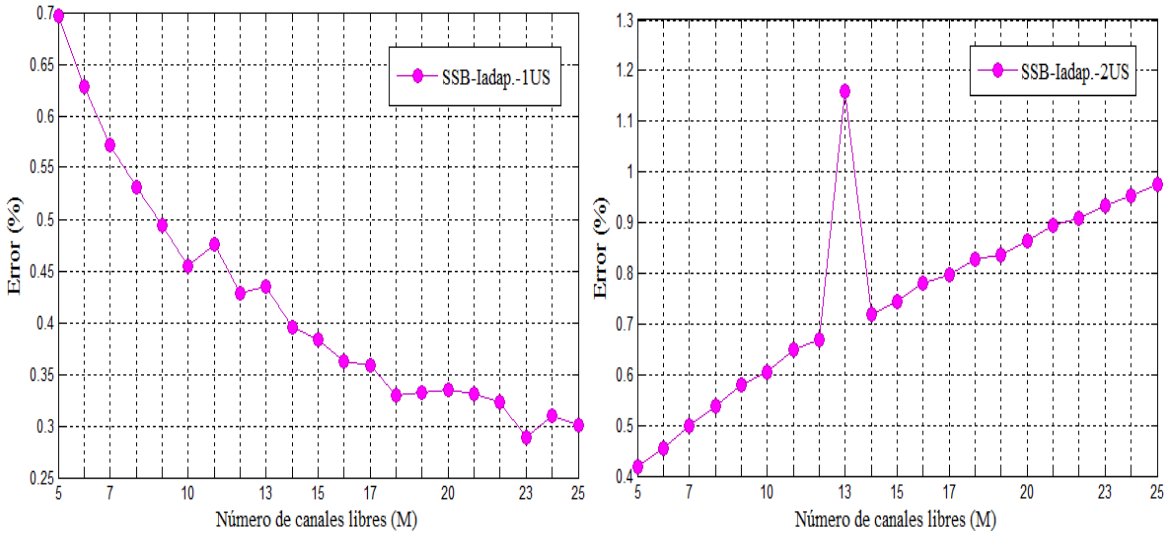

(a) (b)

Figura A-I.4: Error cometido al estimar el número de veces que el usuario interferente aleatorio coincide con los US: a) con un usuario secundario y b) con ambos usuarios secundarios.




(a) (b)

Figura A-I.5: Error cometido en las simulaciones del algoritmo *Short Sequence Based* ante interferencias de un usuario malicioso adaptable: a) ETTR y b) MTTR.




(a) (b)

Figura A-I.6: Error cometido al estimar el número de veces que el usuario maliciosos adaptable coincide con los US: a) con un usuario secundario y b) con ambos usuarios secundarios.