UNIVERSIDAD CATÓLICA DE SANTA MARÍA
FACULTAD DE CIENCIAS E INGENIERÍAS FÍSICAS Y FORMALES
PROGRAMA PROFESIONAL DE INGENIERIA DE SISTEMAS

TÍTULO:

ESQUEMA FLEXIBLE DE MÚLTIPLES CRITERIOS PARA DETECTAR ATAQUES DE EMULACIÓN DE USUARIO PRIMARIO EN REDES AD HOC DE RADIO COGNITIVO

TESIS
Presentada por los Bachilleres:

FUENTES MAMANI, LUIS ALBERTO
HUARACHI SOTO, JULIO CESAR

Para optar el Título Profesional de:
INGENIERO DE SISTEMAS

AREQUIPA - PERÚ

2014

Dedicamos este trabajo a nuestros padres y hermanos, que supieron implantar en nosotros los valores fundamentales de la vida e inculcarnos siempre ese deseo de superación, además de demostrarnos su constante apoyo.

En teoría, no hay diferencia entre práctica y teoría. En la práctica, si la hay.

Albert Einstein y Jan L. A. van de Snepscheut

RESUMEN

El uso ineficiente del espectro de radiofrecuencias y la alta proliferación de dispositivos móviles motivaron el desenvolvimiento de la tecnología de radio cognitivo. Esta permite un mejor aprovechamiento del espectro de radiofrecuencias y motivo el surgimiento de las redes ad hoc de radio cognitivo (CRAHNs, del ingles, Cognitive Radio Ad Hoc Networks). En estas redes dos tipos de usuarios comparten el espectro: el usuario primario y los usuarios secundarios. El usuario primario posee licencia para usar las bandas de frecuencia y tienen prioridad para el acceso; por otro lado, los usuarios secundarios no poseen licencias, pero utilizan las bandas de frecuencias cuando están ociosas o desocupadas. A pesar de las ventajas de la tecnología de radio cognitivo, el aprovechamiento de las frecuencias ociosas puede ser altamente comprometido por ataques de emulación de usuario primario (EUP). Un ataque EUP es generado por un usuario secundario, malicioso o egoísta, que emula el comportamiento y las características de los usuarios primarios legítimos a fin de ganar prioridad en el uso del espectro de radiofrecuencias. Los esquemas propuestos en la literatura para el análisis, detección y mitigación de los ataques EUPs siguen arquitecturas de redes centralizadas o distribuidas, además de exhibir abordajes cooperativos y no-cooperativos. Por tal motivo, esos esquemas realizan un análisis considerando un único criterio que puede ser la potencia de recepción o distancia para evaluar la presencia de ataques en la red, resultando en altas tasas de falsos positivos. Con el fin de proveer un análisis más sofisticado y eficiente, este trabajo propone FLEXEUP, un esquema FLEXible de múltiplos criterios para detectar ataques de Emulación de Usuario Primario en CRAHNs. Este esquema sigue un abordaje descentralizado y cooperativo en el que cada usuario secundario realiza dos fases para determinar la probabilidad de la presencia de ataques EUPs. La primera fase consiste en el sensoreamiento y el análisis de los valores de los múltiplos criterios; la segunda fase consiste en la compartición de información entre vecinos, seguida de un análisis de las informaciones compartidas atreves del teorema de Bayes. El esquema FLEXEUP fue implementado y evaluado en el simulador de red, Network Simulator (NS), versión 2.31. Los resultados muestran que el esquema presenta una superioridad de hasta 25 % cuando es comparado con un esquema mono-criterio no-cooperativo en su primera fase, ya cuando es aplicado las dos fases en conjunto este presenta una eficacia de hasta 77 % en la determinación de la probabilidad de la presencia de ataques EUP.

Palabras-clave: radio cognitivo, emulación de usuario primario, redes ad hoc, análisis de múltiplos criterios.

ABSTRACT

The inefficient use of the radio spectrum and the high proliferation of mobile devices have motivated the development of Cognitive Radio technology. The CR technology enables a better use of the spectrum and has promoted the development of Cognitive Radio Ad Hoc Networks (CRAHNs). These networks handle two types of users sharing the spectrum: primary user and secondary user. A Primary User has license to use the frequency bands and has a higher priority to access them, whereas a Secondary User has no license, but use licensed bands when they are idle. However, the use of idle frequencies can be highly compromised by Primary User Emulation Attack (PUEA). This attack is generated by a malicious or selfish secondary user, that emulates the behavior and the characteristics of a legitimate PU to take priority in the use of radio spectrum access. Existing proposals in the literature for analyzing, detecting or mitigating PUEA in cognitive radio networks focus on centralized or decentralized architecture, following cooperative or non-cooperative approaches. All of them apply a single criterion to evaluate the presence of attacks on the network. In order to provide a more sophisticated and efficient approach, this work proposes a FLEXible multi-criteria scheme to detect Primary User Emulation attacks in CRAHNs, called FLEXEUP. In FLEXEUP, each secondary user conducts two phases to determine the probability of the presence of PUEA. Initially, the secondary user carries a single phase sensing and analyzing the values of multiple criteria. Then, in the second phase, each secondary user exchanges information with its neighbors and analyzes it based on the Bayes'theorem in order to determine the probability of PUEA occurrence on the network. FLEXEUP has been implemented in the Network Simulator, version 2.31, and evaluated. Results show that the FLEXEUP scheme in its individual non-cooperative phase increases up to 25 % of the efficiency on detecting the PUEA presence when compared with a mono-criterion non-cooperative scheme. Further, the FLEXEUP scheme applying both phases has improved in approximately 77 % a mono-criterion cooperative scheme.

Keywords: cognitive radio, primary user emulation attack, ad hoc networks, multiple criteria analysis.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

CAPÍTULO 1

INTRODUCCIÓN

1.1. Título

"Esquema Flexible de Múltiples Criterios para Detectar Ataques de Emulación de Usuario Primario en Redes Ad Hoc de Radio Cognitivo"

1.2. Preambulo

Tradicionalmente, El espectro de radiofrecuencias ha sido distribuido por agencias reguladoras, como MTC (Ministerio de Transportes y Comunicaciones) en el Perú y la FCC (Federal Communications Commission) en los Estados Unidos de forma estática [2, 3]. Una parte significativa de las frecuencias es atribuida atreves de licencias a empresas privadas de telecomunicaciones e instituciones gubernamentales, resultado en la escases del espectro y limitando la escalabilidad necesaria para soportar nuevos servicios y aplicaciones [3]. Análisis recientes demuestran que esta forma de distribución subutuliza el espectro, permitiendo la existencia de frecuencias ociosas en determinados momentos (también llamadas de "espacios en blanco" o "white spaces"), como mostrado en [4, 5]. Tal comportamiento ha motivado el desenvolvimiento y uso de mecanismos oportunistas y cognitivos a fin de aprovechar mejor La capacidad Del espectro de radiofrecuencias [6, 7].

La tecnología de radio cognitiva (RC) es un nuevo paradigma en las comunicaciones inalámbricas que permite una mejor utilización del espectro de radiofrecuencias [8]. La RC permite implantar en un dispositivo computacional un sistema de comunicación flexible capaz de reconfigurar y adaptar sus parámetros de transmisión y recepción [9]. Esta adaptación se lleva a cabo proporcionando las funcionalidades de RC, tales como la gestión, el sensoriamento, la decisión, la compartición y la movilidad [1, 10, 11]. Estos beneficios han motivado el uso de la tecnología RC para la comunicación entre dispositivos informáticos formando las redes de radio cognitivo [12].

Las redes de radio cognitivo se componen de dispositivos (nodos) que utilizan la tecnología de RC y son capaces de monitorear e identificar las frecuencias ociosas en el espectro [13]. Con base en las mediciones y los conocimientos adquiridos a través de la historia de los acontecimientos pasados, cada nodo puede elegir y acceder a los espacios en blanco del espectro de forma inteligente [14]. Una red de radio cognitivo puede organizarse siguiendo una arquitectura centralizada o arquitectura descentralizada. Una arquitectura centralizada se compone de una estación base central que gestiona los nodos de la red y su uso del espectro. En la arquitectura descentralizada, cada nodo es responsable de

su propia gestión en la red y por las decisiones de cómo usar los espacios en blanco del espectro. Por lo tanto, una arquitectura descentralizada constituye una bf red ad hoc de radio cognitivo (CRAHN, del inglés, Cognitive Radio Ad Hoc Networks) [1, 15].

Dos tipos de usuarios comparten el espectro de radiofrecuencias en el contexto de las redes de radio cognitivo, siendo denominados usuarios primarios (UP) y los usuarios secundarios o cognitivas (US) [16]. Los usuarios primarios poseen licencias de uso de las bandas y el acceso prioritario a ellas, mientras que los usuarios secundarios no tienen licencias, pero pueden utilizar las bandas cuando están ociosoas. Sin embargo, por determinación de los organismos reguladores, los usuarios secundarios no deben interferir en la comunicación de los usuarios primarios [17, 18]. Por lo tanto, los nodos en una CRAHN deben vigilar constantemente el medio a fin de detectar la presencia de un usuario primarios en el canal utilizado. En los casos en que se detecta un usuario primario, el usuario secundario debe mudar rápidamente a otro canal [19], lo que resulta en una interrupción temporal de las conexiones entre los nodos de una CRAHN hasta que se selecciona un nuevo canal para continuar la comunicación.

Además de realizar un mejor uso de las frecuencias ociosas del espectro, las CRAHNs benefician directamente a los usuarios finales. Estas redes hacen un mejor uso del espectro y pueden proporcionar una mejor calidad de servicio (QoS, del inglés, Quality of Service), tiempos de respuesta, la cobertura, el acceso al medio y otros [20]. Una ventaja de la CRAHN en relación a una red tradicional es la baja latencia que genera en su transmisión [21].

1.3. Problema

1.3.1. Identificación del problema

Las CRAHNs son vulnerables a diversos tipos de ataques debido a las características de la comunicación inalámbrica y la forma de organización de este tipo de red [22]. Estos ataques pueden ser clasificados de acuerdo a las capas de la pila de protocolo [23]. Ejemplos de ello son los ataques de negación de servicio (DoS, del inglés it Denial of Service) que puede actuar en las capas física y de enlace generando una interrupción en la comunicación de los nodos de la red, un ejemplo de estos son los ataques jamming, los ataques EUP (Emulación de Usuario Primario), ataques OFA (Objective Function Attack), CCDA (Common Control Data Attacks) y otros. Por otro lado, están los ataques de manipulación de datos que afectan a la capa de enlace, como los ataques Spoofing/Sybil, inyección de paquetes, false feedback y otros [24]. Ataques como Jellyfish y Lion, operan en la capa de transporte, degradando las conexiones TCP dentro de una CRAHN [25].

1.3.2. Descripción del problema

El ataque Emulación de Usuario Primario (EUP) es una de las más peculiares en las CRAHNs [25, 26, 27]. Estos ataques pueden ser generados por usuarios malintencionados - malicioso y egoísta - con el fin de maximizar su uso del espectro [28]. En el ataque EUP, un usuario secundario malintencionado manipula su radio para imitar el comportamiento de un usuario primario legítimo. Por ejemplo, un usuario malintencionado puede cambiar la potencia de transmisión, el modo de modulación, ancho de banda, tasa de transmisión, entre otros. Este ataque causa una degradación en las oportunidades de acceso al espectro de usuarios secundarios legítimos [17, 29].

1.3.3. Justificación

Desarrollar soluciones para la detección o la mitigación de los usuarios secundarios generando ataques de emulación de usuarios primarios es de gran importancia en las CRAHNs. Estos ataques son difíciles de detectar debido a que los usuarios secundarios maliciosos pueden modificar su interfaz de radio para imitar las características de un usuario principal y causar un error en la identificación por los usuarios secundarios legítimos [28]. En la literatura proponen soluciones de contramedidas frente a los ataques EUP siguiendo enfoques no-cooperativos o cooperativos en arquitecturas centralizadas o descentralizadas. Inicialmente, esos trabajos se centran en los enfoques centralizados no-cooperativos generando una alta latencia y un punto de falla en la estación base [17, 28, 29, 30, 31]. Por lo tanto, modelos de cooperación centralizada surgieron para reducir la latencia de la decisión, pero no la existencia del punto único de falla [32, 33, 34].

Por otro lado, se han propuesto los sistemas no-cooperativos y descentralizados en paralelo. Estos tienen un mayor rendimiento puede contrarrestar las dificultades de soluciones que siguen un enfoque centralizado. En los enfoques no-cooperativos descentralizados [22, 35], cada nodo realiza individualmente una detección del ataque EUP, que puede generar una alta tasa de falsos positivos y falsos negativos. Para combatir estos problemas, los abordajes cooperativos en arquitecturas descentralizadas fueron propuestas [26]. Sin embargo, las soluciones de la literatura que tienen en en cuenta los enfoques cooperativos y no-cooperativos, proporcionan un análisis de un solo criterio, y estos pueden conducir a una identificación errónea de ataque [17, 28, 29, 31], estos errores ocurren debido a que este criterio es el único dato para determinar la aparición de un ataque EUP en la red. Por esta razón, es necesario proporcionar una solución que tenga en cuenta las ventajas de cada propuesta en la literatura junto a un análisis de múltiples criterios para determinar la presencia del ataque EUP en redes ad hoc de radio cognitivo.

1.4. Objetivos

1.5. Objetivo General

Este trabajo tiene como objetivo identificar la presencia de ataques EUPs en los canales de frecuencia. Para lograr este objetivo se propone un esquema FLEXible de múltiples criterios para detectar ataques de Emulación de Usuario Primario en redes ad hoc de radio cognitivo, llamado FLEXEUP. El esquema sigue un enfoque cooperativo con una arquitectura descentralizada.

1.6. Objetivos específicos

- Reducir las altas tasas de falsos positivos y falsos negativos resultantes de los esquemas actualmente existentes en la literatura.
- Evaluación de las vulnerabilidades de una red ad hoc de radio cognitivo ante los ataques de emulación de usuario primario. Estos análisis permiten la comprensión de las necesidades de seguridad en tales redes.
- La propuesta y la especificación del esquema FLEXEUP, un esquema FLEXible de múltiples criterios para detectar ataques de Emulación de Usuario Primario en redes ad hoc de radio cognitivo. Este esquema permite determinar la probabilidad de suceso del ataque EUP.
- La comparación del esquema FLEXEUP frente a un esquema mono-criterio, representando los esquemas actualmente abordados en la literatura. Esta revisión mostró que el esquema FLEXEUP presenta resultados relevantes.
- El desarrollo del esquema FLEXEUP nos dará como resultado la implementación del esquema en el simulador NS-2, a su vez estos módulos desarrollados podrán ser proporcionados a la comunidad investigadora para su evaluación y posterior crecimiento.

1.7. Hipótesis

Dado que en la literatura se abordan soluciones teniendo en cuenta los enfoques cooperativos y no-cooperativos, proporcionando un análisis de un solo criterio, y estos pueden conducir a una identificación errónea de ataque. Se parte de la hipótesis de utilizar un análisis de múltiples criterios conjuntamente con un análisis de probabilidad condicional para desarrollar un esquema que permita determinar la presencia de ataques EUP en la

red ad hoc de radio cognitivo. Este esquema tendrá que ser desarrollado en una arquitectura distribuida que permita la autonomía de los nodos de la red. Con la hipótesis planteada, se pretende aumentar y mejorar la probabilidad de detección del ataque EUP y disminuir las tasas de falsos positivos y negativos.

1.8. Variables

1.8.1. Independientes

- Múltiples criterios.
- Sensoriamento del espectro.

1.8.2. Dependientes

- Análisis de múltiples criterios.
- Análisis PCA.
- Análisis de probabilidad condicional.

1.8.3. Indicadores

- Probabilidad de presencia del ataque EUP en la red.
- Tasa de detección.
- Falsos positivos.
- Falsos negativos.

1.9. Alcances y limitaciones

La implementación del módulo CRAHN [36] en el simulador de la red NS-2 con el desarrollo del esquema FLEXEUP. Este proporcionara una herramienta para la determinación de la presencia de ataques de EUP. Esta extensión está integrada con otros módulos del simulador y podrá estar disponible para la comunidad científica.

1.10. Área, línea, tipo, y nivel científico

- Área: Ciencias exactas.
- Línea: Seguridad en redes inalámbricas.

- Tipo: Analítica y descriptiva.
- Nivel: Simulación.

CAPÍTULO 2

MARCO TEORICO

2.1. La tecnologia de radio cognitivo

El espectro de radiofrecuencias es un recurso natural y un medio de transmisión/recepción de las comunicaciones inalámbricas. Estas frecuencias son utilizadas por los usuarios autorizados a través de licencias [37]. Sin embargo, el crecimiento y el uso extendido de las tecnologías inalámbricas hacen del espectro un recurso escaso debido a la asignación de frecuencias. A pesar de esta escasez, los estudios muestran una alta subutilización de frecuencias licenciadas. Esta sub-utilización del espectro se caracteriza por el uso del espectro inactivo durante ciertos períodos de tiempo. Estos tiempos muertos pueden ser mejor utilizados por los usuarios secundarios (US) (usuarios sin licencia) [38, 39], como se muestra en la Figura 2.1

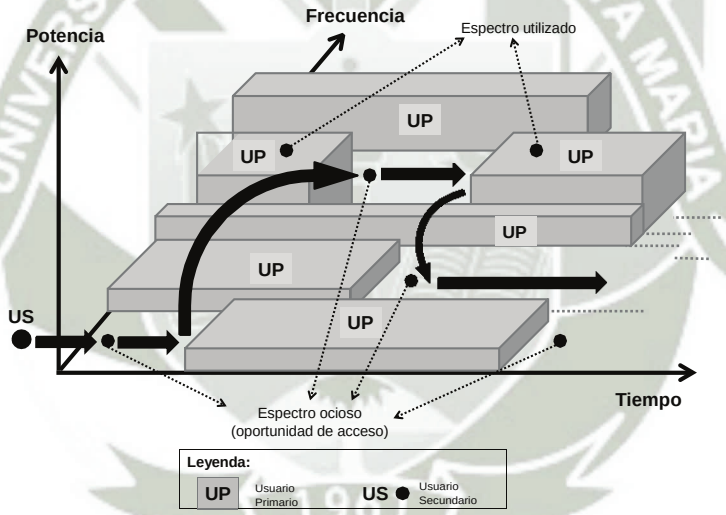


Figura 2.1: Oportunidad de acceso al espectro [1]

La tecnología de radio cognitivo (RC) verifica el espectro para reconocer la variación del medio de forma inteligente y reconfigurar sus parámetros para la reutilización de espacios vacíos dejados por los usuarios primarios [13, 14]. Para el procedimiento de verificación del espectro se considera las funcionalidades básicas del RC , tales como la gestión, el sensoriamento, la decisión, la compartición y la movilidad del espectro [1, 9, 10, 11]. A continuación, cada una de estas funciones se describe, y la Figura 2.2 ilustra estas características del RC.

- Sensoriamento

  El sensoriamento del espectro permite el monitoreamento de las bandas licenciadas

disponibles. Esto realiza la detección del inicio y final de las actividades licenciadas, además de identificar los espacios vacios del espectro. El sensoriamento captura la información que sirve como entrada para la función de decisión. Algunas de las técnicas de detección se presentan en [40, 41, 42].

- Decisión

  Para llevar a cabo la comunicación, el radio cognitivo utiliza un canal que puede cambiar de acuerdo con las condiciones de la red. Para ello, la decisión de ocupar un canal se produce a través de la función de gestión con base en la información de sensoriamento del espectro. La función de decisión es el preámbulo de la función de compartición. Algunos de los algoritmos para la toma de decisión espectral se presentan en [43, 44, 45, 46].

- Compartición

  Debido a la existencia de múltiples radios cognitivos que desean acceder al espectro al mismo tiempo, los radios cognitivos deben coordinar de manera que no entren en conflicto entre sí o con los usuarios con licencia. Esta función permite a la radio garantizar la asignación de espectro entre los usuarios primarios y secundarios según el tipo de técnica de acceso al espectro, siendo estas técnicas superpuesta (overlay) o sobrepuesta (underlay). Algunas de estas técnicas de compartición del espectro se presentan en [47, 48].

- Movilidad

  Todos los radios cognitivas son catalogados como visitantes en el espectro. Por lo tanto, la movilidad del espectro es el proceso de desocupación de un canal que está siendo utilizado por un visitante y llevar el visitante a otro canal. Este cambio se debe a las condiciones del canal o el comienzo de la actividad de un usuario primario en su banda licenciada. El RC debe garantizar a los terminales de radio operar en las mejores bandas de frecuencia. Los trabajos en [49, 50] muestran algoritmos para realizar la movilidad en el espectro.

- Gestion

  La gestión del espectro es la función que supervisa y controla las otras funciones. Este determina cuando una de las características mencionadas anteriormente entra en acción. Además, tiene que garantizar y satisfacer la comunicación entre los usuarios, con lo mejor en términos de calidad de servicio (QoS). Los trabajos en [1, 51, 52, 53] presentan una revisión de los algoritmos empleados para gestionar el espectro.

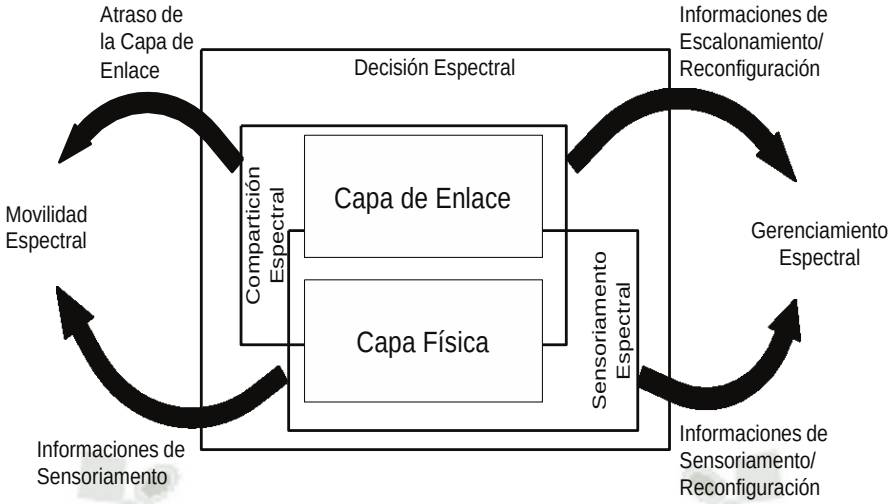


Figura 2.2: Funcionalidades de la tecnologia de radio cognitivo [Elaborado por los autores]

2.1.1. Redes de radio cognitivo

Las redes de radio cognitivo tienen por objeto eliminar las limitaciones de acceso dinámico al espectro de las redes tradicionales, lo que permite optimizar el uso del espectro y por lo tanto su rendimiento [54, 55]. Para ello, los nodos de una red mediante la tecnología de radio cognitivo adaptan sus configuraciones de radio a los cambios permanentes en el medio de transmisión y tienen un uso más amplio del espectro [39]. Sin embargo, la red de radio cognitivo captura las condiciones del espectro para luego planificar, decidir y actuar en el espectro, teniendo en cuenta los usuarios (primarios y secundarios), compartiendo el medio [38].

La arquitectura de una red de radio cognitivo tiene dos tipos de usuarios que comparten el espectro. Un usuario autorizado para el uso prioritario de las bandas con licencia, llamado usuario primario (UP) y el usuario secundario (US), que no tiene prioridad en el uso de bandas de frecuencias, pero puede usarlas cuando estas están ociosas. Un transmisor secundario (US) empieza a sensoriar el espectro y luego decide que canal licenciado utilizara para realizar su transmisión. Para esto, el US transmisor comunica al US receptor el canal que será utilizado por el envío de un paquete de control por un canal de control común. Después el US receptor responde con otro paquete de control, confirmando la recepción y la configuración de canal, esta respuesta se hace por el canal establecido para la transmisión. A continuación, el US transmisor accede al canal y puede compartir este canal con otros usuarios, dependiendo del tipo de técnica de acceso al medio. Los USs al detectar la presencia de un UP en el mismo canal de transmisión debe evitar la interferencia y cambiar a otro canal en el espectro, por lo tanto se hace uso de otras funcionalidades de un RC [12]. Con esto, las redes de radio cognitivo proporcionan un rendimiento óptimo a los USs en términos de gestión de recursos, calidad de servicio (QoS), seguridad, control

de acceso al medio [39].

Sin embargo, el proceso de comunicación entre los USs dependerá directamente del tipo de arquitectura de red de radio cognitivo. En estas arquitecturas encontraron dos tipos: centralizada, y descentralizada o distribuida [1, 16, 25, 15]. A continuación se describen estos dos tipos de arquitecturas.

- Arquitectura centralizada

  En la arquitectura centralizada, una estación base o centro de fusión maneja la información recopilada por USs. Estos USs se organizan en la red y están monitoreando el medio con el fin de recopilar información. Esta información se devuelve a la estación base con el fin de determinar las acciones a realizar mediante la aplicación de la tecnología RC.

- Arquitectura distribuida

  En la arquitectura distribuida, los USs no necesitan una estación base. Cada uno es independiente del otro y gestiona su propia tecnología de RC. Este tipo de arquitectura representa una red ad hoc de radio cognitivo (CRAHNs, del inglés, Cognitive Radio Ad Hoc Network). Las CRAHNs presentan varios desafíos, ya que cada US será responsable de su propia gestión del espectro. Estos desafíos incluyen: el costo de la recolección de información genera una latencia en la capa de enlace, el consumo de energía por la característica de presentar una forma ad hoc, la tasa de mensajes de actualización para mantener un correcto estado de la red. Por otra parte, este modelo de arquitectura utiliza un canal de control común para mantener la comunicación de mensajes de control. Este canal de control abre otro reto, ya que tiene que ser elegido correctamente para evitar la sobrecarga del canal y generar latencias en la comunicación [51].

  Sin embargo, a pesar de los desafíos de las CRAHNs, estas también tienen ventajas en términos de cooperación. Por la falta de apoyo centralizado, la CRAHN debe confiar en observación local de cada US, para determinar sus acciones. Para superar este conocimiento limitado de la topología de la red, todas las decisiones del espectro son basadas en las operaciones cooperativas. Los USs determinan sus acciones con base en la información intercambiada sobre las observaciones de sus vecinos. Además, este modelo de arquitectura ofrece una menor complejidad en su aplicación, ya que sólo requiere información USs y no de una unidad centralizada. El tiempo de decisión para la acción es inferior a una arquitectura centralizada [53]. Tenga en cuenta que este trabajo aborda su propuesta en virtud de este tipo de arquitectura.

La Figura 2.3 ilustra las dos arquitecturas existentes para lãs redes de radio cognitivo. Observamos una arquitectura centralizada que contiene la estación base y los usuarios se-

cundarios. Por otra parte, se presenta una arquitectura descentralizada, que es compuesta sólo de usuarios secundarios autónomos.

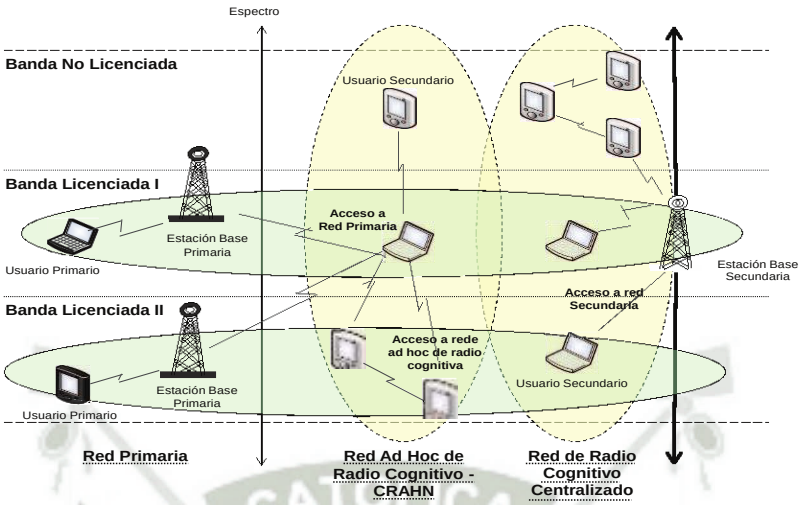


Figura 2.3: Arquiteturas de las redes de radio cognitivo [1]

2.2. Vulnerabilidades de seguridad

A pesar de las ventajas de las redes ad hoc de radio cognitivo, estas son vulnerables a diversos tipos de ataques, ya que el espectro de radiofrecuencias licenciado utilizado por los usuarios secundarios puede ser fácilmente comprometido por uno o más atacantes. Los ataques pueden resultar en la inyección de datos falsos en el momento de intercambio de información de detección, de la emulación de un usuario primario, utilizando el espectro de forma egoísta o maliciosa. En el contexto de las redes ad hoc de radio cognitivo, llevamos a cabo nuestra propia clasificación de los diferentes ataques que se producen en la red, siguiendo las definiciones y clasificaciones de los autores: Clancy y Goergen, Zhang y Li, Leon et al. y Araujo et al. y teniendo en cuenta las capas de la pila de protocolo [24, 25, 56, 57].

- Capa de transporte
  Los ataques de esta capa ocurren cuando un sistema criptográfico ha sido comprometido. Estos ataques pueden afectar directamente el protocolo de control de transmisión (TCP, del inglés, Transmission Control Protocol), lo que resulta en una degradación del TCP y forzar un cambio de canal por el US legítimo.

- Capa de red
  Estos ataques afectan al cifrado que se utiliza en la transmisión. Como en una red ad hoc de radio cognitivo los nodos son móviles y un desafío clave es el consumo de energía, los nodos no tienen los recursos suficientes para utilizar un mecanismo

de cifrado poderoso y son vulnerables a los ataques. El principal objetivo de estos ataques es el de obtener la clave criptográfica de la transmisión.

- Capa de enlace

  Los ataques en esta capa pueden generar una decisión errónea del estado actual del espectro de radiofrecuencias. Esto sucede cuando los USs de la red intercambian información de sensoriamento, pero esta información intercambiada puede verse comprometida por los ataques a la capa de enlace, pudiéndose inyectar datos falsos, modificar datos o eliminarlos. La información recogida a través del intercambio entre múltiples nodos puede dar lugar a una decisión equivocada acerca de la banda de frecuencia que los USs quieren usar, y puede causar interferencias en la comunicación de otros USs o en el peor de los casos genere una colisión con un UP legítimo.

- Capa física

  En esta capa se destaca los ataques de negación de servicio (DoS, del inglés, Denial of Service). Algunos de estos ataques están dirigidos a tratar de emular algunas de las características de un usuario legítimo. Otros ataques pueden generar una alta interferencia, debido al hecho de que los atacantes podrían ocupar los canales como USs simples, dificultando la comunicación entre el USs legítimos.

La Tabla 2.1 presenta algunos de los ataques a las redes ad hoc de radio cognitivo. Se clasifican de acuerdo a las capas de la pila de protocolos como se describió anteriormente. Dentro de esta clasificación, nos hemos centrado en la vulnerabilidad de la capa física, que representan un gran desafío, ya que un atacante puede comprometer la capa física y, posteriormente, se refleja en las capas superiores alcanzando así una decisión equivocada sobre el estado actual del espectro.

Cuadro 2.1: Ataques en redes ad hoc de radio cognitivo

Capa	Tipo de ataque
Física	Jamming EUP OFA CCDA
Enlace/Rede	Spoofing/Sybil Packet injection Selective forwarding False feedback Worm/Sink/Grey/Black - hole Flooding Power consumption
Transporte	Jellyfish Lion

2.2.1. Ataque de emulación de usuario primario

El ataque de la emulación de usuario primario (EUP) fue introducido por primera vez por Chen y Park [28] y afecta directamente a la capa física. Este ataque es realizado por los usuarios secundarios mal intencionados que manipulan sus radios para tener comportamientos y características similares a la transmisión de los usuarios primarios [17, 29]. Esto es debido a que los radios cognitivos permiten la reconfiguración de las interfaces de radio. Un atacante equipado con tecnología RC puede modificar su interfaz y emular las características de la señal de un usuario primario. Esta modificación permite a los usuarios secundarios legítimos identificar incorrectamente un usuario secundario como un usuario primario, lo que resulta en un ataque EUP [38]. Las investigaciones muestran que un ataque EUP puede afectar seriamente el rendimiento del espectro y reducir significativamente la disponibilidad de los canales legítimos a los usuarios secundarios, pasando una negación de servicio [24, 25].

Un ataque EUP puede ser generado por dos tipos de usuarios secundarios mal intencionados: (i) usuario malicioso, que tiene como objetivo poner en peligro el funcionamiento de la red y (ii) usuario egoísta, que se beneficia de los privilegios que este tiene para establecer una comunicación exclusiva con otro usuario [28]. Estas dos acciones maliciosas reducen significativamente los recursos de acceso a los medios de comunicación disponibles para los usuarios secundarios legítimos. Además, se comprometen las características cognitivas de estos usuarios [29, 39].

La Figura 2.4 ilustra el espectro licenciado por los usuarios primarios que es utilizado por un usuario secundario legítimo. Los USs llevan a cabo el sensoriamento del espectro y accesa a las frecuencias ociosas del espectro. Cuando un usuario primario se activa en su banda con licencia, el US cambia a otro espacio ocioso dentro del espectro de frecuencias. Los ataques EUP (representados por los cráneos de la Figura 2.4) son realizados en diferentes bandas de frecuencia, ocupando el espectro espacios en blanco y tornando el espectro ocupado. El US legitimo detecta estas actividades de los atacantes como actividades legítimas de UPs, perdiendo oportunidades de acceso al espectro.

2.3. Técnicas de sensoriamento del espectro

Existen varias técnicas utilizadas para el sensoriamento del espectro en las redes de radio cognitivo con el objetivo de detectar la presencia de usuarios primarios legítimos en el espectro. En general, estas técnicas tienen como referencia las características de transmisión de la señal primaria. Estas características pueden ser la potencia de transmisión, potencia de recepción, el tipo de onda de señal, la modulación, la amplitud, la ubicación del transmisor, entre otras características. Técnicas de detección se clasifican como: no-cooperativas y cooperativas [40].

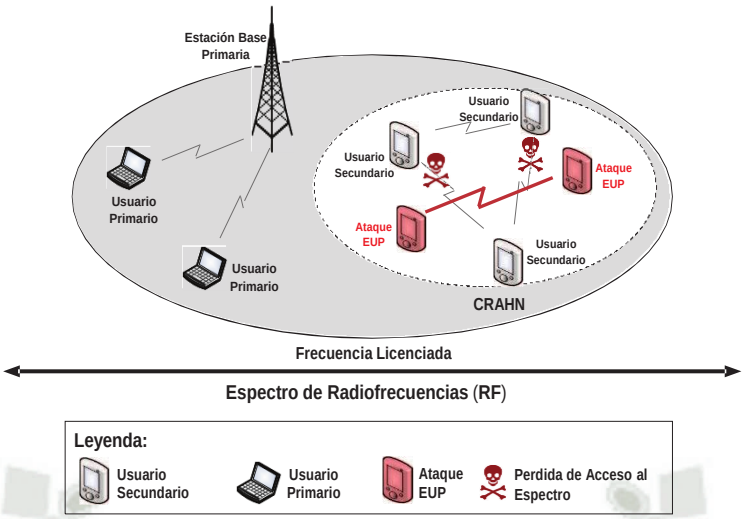


Figura 2.4: Presencia del ataque EUP en la red de radio cognitivo [Elaborado por los autores]

Sin embargo, en las técnicas de sensoriamento no-cooperativas un usuario secundario no consigue identificar una transmisión primaria debido al desvanecimiento de canal o de obstáculos en la transmisión [38]. En consecuencia, para llevar a cabo una detección de obstáculos presentes, las técnicas de sensoriamento han evolucionado con la necesidad de determinar la presencia de un UP a partir de la información de sensoriamento de otros usuarios secundarios cooperativos. La Figura 2.5 presenta la clasificación de las técnicas de sensoriamento del espectro. A seguir, estas técnicas se clasifican y se describen conforme son presentadas en la literatura [38, 40].

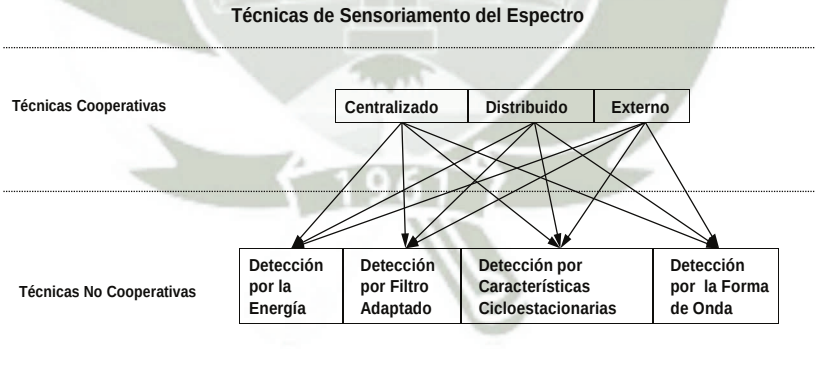


Figura 2.5: Técnicas de sensoriamento del espectro en las redes de radio cognitivo [Elaborado por los autores]

2.3.1. Técnicas de sensoriamento del espectro no-cooperativas

En un enfoque no-cooperativo, los usuarios secundarios son dispuestos en la red, cada uno de los cuales es capaz de realizar su sensoriamento del espectro con el fin de detectar

la presencia de un UP. Este sensoriamento se realiza en la banda de frecuencia adecuada para el acceso al espectro. Estas técnicas de detección, identifican las características de transmisión de la señal primaria para decidir sobre el tipo de usuario presente en la red. A continuación, se presentan las principales técnicas de sensoriamento no-cooperativas:

- Detección basada en la energia

  La detección por la energía es la técnica más común por su bajo costo computacional y su fácil implementación en comparación con otras técnicas [41, 58, 59, 60, 61]. Además de estas ventajas, esta técnica es más general, ya que no necesita un conocimiento previo de la señal del UP [62]. La señal se detecta después de dos hipótesis definidas en la Ecuación 2.1 y se compara con los límites establecidos, como se ve en la Ecuación 2.2 [63].

  En la Ecuación 2.1, observamos H_0 e H_1 denominadas hipótesis de detección de señal del UP. Siendo, H_0 la hipótesis de ausencia de señal del UP, y H_1 la hipótesis que representa la presencia de señal del UP. En las hipótesis, se observa que s(n) es la señal a ser detectada, w(n) es la adición de ruido Gaussiano, y n es el índice de la muestra. Si s(n) = 0, no ocurrirá una transmisión del usuario primario. Estas dos hipótesis (H_0 e H_1) se comparan con un límite denotado por μ y λ para obtener el resultado de la detección denotado por D y representado en la Ecuación 2.2.

$$\begin{aligned} H_0 &: y(n) = w(n), \\ H_1 &: y(n) = s(n) + w(n) \end{aligned} \tag{2.1}$$

$$D = \begin{cases} 1 & \mu > \lambda \\ -1 & \mu < \lambda \end{cases} \tag{2.2}$$

- Detección por filtro adaptado

  Es conocido como una gran técnica de detección de usuarios primarios cuando se conoce la señal transmitida [64]. La principal ventaja de este método es el tiempo que se utiliza para obtener una probabilidad de falsos positivos o probabilidad de pérdida de la detección cuando se compara con otras técnicas [65]. El filtro adaptado puede extraer información de la señal primaria, tales como el tipo de modulación, la forma del pulso y la forma del paquete para optimizar la probabilidad de detección. Sin embargo, esta técnica requiere el conocimiento previo de la señal de un usuario primario, y su desempeño se ve comprometido si el conocimiento no es exacto. Además, debido a las necesidades de los receptores de radio cognitivo para todos los tipos de señales, la complejidad de la aplicación de la unidad de detección es muy grande. Otra desventaja del filtro adaptado es el alto consumo de energía por os algoritmos utilizados [40].

- Detección por características ciclo-estacionarias

  Se trata de una técnica para detectar transmisiones primarias, tomando ventaja de las características ciclo-estacionarias de las señales recibidas [9, 40, 66]. La técnica incorpora los ciclos de frecuencia de las señales de onda modulada, onda sinusoidal, ciclos prefijados que posibilita la detección de la señal principal por el análisis de la función de correlación espectral de la señal transmitida. Los algoritmos basados en la detección ciclo-estacionaria pueden diferenciar mejor el ruido de las señales de los usuarios primarios, siendo mejor que la detección por energía [66]. Sin embargo, la detección ciclo-estacionaria requiere una mayor complejidad computacional y un tiempo de observación más prolongado. Por otra parte, la técnica ciclo-estacionaria se utiliza para distinguir entre diferentes tipos de transmisores y los usuarios primarios [67]. El ciclo de densidad espectral (CDS) en función de la señal recibida puede ser calculado por la Ecuación 2.3.

  $$S(f,\alpha) = \sum_{\tau=-\infty}^{\infty} R_y^{\alpha}(\tau) e^{-j2\pi f\tau}, l \tag{2.3}$$

  siendo,

  $$R_y^{\alpha}(\tau) = E[y(n+\tau)y*(n-\tau)e^{-j2\pi\alpha n}] \tag{2.4}$$

  una función de correlación cíclica (CAF) denotada por f y alpha es la frecuencia cíclica. La función CSD proporciona valores máximos cuando la frecuencia cíclica es igual a las frecuencias fundamentales de la señal transmitida. La frecuencia cíclica puede ser conocido, o puede ser extraido y utilizada como características para la identificación de las señales transmitidas [68, 69].

- Detección por la forma de onda

  Los patrones de ondas son comúnmente conocidos y utilizados en los sistemas inalámbricos para ayudar en la sincronización u otros fines. Estos estándares incluyen preámbulos, midámbulo, datos de control regularmente transmitidos, secuencias, etc. Un preámbulo es una secuencia conocida de transmisión antes de cada intervalo de tiempo, y midámbulo se transmite en el medio de un intervalo de tiempo. Con la presencia de un patrón conocido, la detección puede llevarse a cabo mediante la correlación de la señal recibida en comparación con una copia de la señal conocida [63]. Este sistema supera el sistema de detección por la energía [70]. Por otra parte, el rendimiento de la detección por la forma de onda aumenta en la medida en que el patrón conocido sea mayor.

  Utilizando el mismo tipo de detección por la energía $y(n) = s(n) + w(n)$, la métrica de detección por la forma de onda puede ser obtenida por la Ecuación 2.5.

$$M = Re[\sum_{n=1}^{N} y(n)s^*(n)] \tag{2.5}$$

Donde $*$ representa La operación de junción. En la ausencia del usuario primario, la métrica puede ser evaluada con la Ecuación 2.6.

$$M = Re[\sum_{n=1}^{N} w(n)s^*(n)] \tag{2.6}$$

Similarmente, en la presencia de señal del usuario primario, la métrica de sensoriamento es representada por la Ecuación 2.7

$$M = \sum_{n=1}^{N} |s(n)|^2 + Re[\sum_{n=1}^{N} w(n)s^*(n)] \tag{2.7}$$

La decisión sobre la presencia de usuario principal puede llevarse a cabo mediante la comparación del resultado de la métrica M con un límite λ. Esta detección basada en la forma de onda es eficaz, pero la desventaja es la necesidad de un conocimiento previo de los preámbulos y midámbulos de onda con el fin de realizar la detección. Además, esta técnica resulta menos eficiente en relación a la técnica de detección por la energía al requerir el conocimiento previo de las características de la señal transmitida [40].

2.3.2. Técnicas cooperativas de sensoriamento del espectro

Las técnicas cooperativas, son propuestas en la literatura como la solución a los problemas que surgen en el espectro debido al ruido, decoloración u obstáculos en el canal de transmisión. Un enfoque cooperativo recoge e incorpora información de sensoriamento de varios usuarios secundarios con el fin de mejorar el rendimiento de detección del espectro [60, 71, 72]. Este enfoque reduce considerablemente las probabilidades de perdida de detección de un UP y falsos positivos. Por otra parte, la detección de cooperación pueden reducir el tiempo de detección [73].

Las técnicas de sensoriamento cooperativas incluyen el desarrollo de algoritmos eficientes de mayor complejidad computacional [73, 74]. En las soluciones de sensoriamento cooperativo, un canal de control se puede utilizar en diferentes tipos de bandas de frecuencia. Dependiendo de los requisitos del sistema, un canal de control puede ser implementado. El canal de control se puede utilizar para compartir los resultados del sensoriamento del espectro entre los usuarios secundarios. Varios soluciones de canales de control se proponen en la literatura de radio cognitivo [75, 76]. Un acceso multiples por división de

tiempo (TDMA) basada en un protocolo para el intercambio de datos de sensoriamento se propone en [77].

Por otro lado, el sensoriamento cooperativo es ventajoso para la cooperación entre los nodos de la red. Además, este sensoriamento puede ser mejor utilizado teniendo en cuenta la cantidad de nodos cooperadores, es decir, cuanto mayor es el número de nodos cooperadores mejor los resultados de sensoriamento [16]. Además, el sensoriamento cooperativo depende exclusivamente del tipo de arquitectura de la red radio cognitivo. A continuación se describen las formas de sensoriamento cooperativo en la red de radio cognitivo [16, 40].

- Sensoriamento cooperativo centralizado
  En el sensoriamento centralizado, una unidad central recoge la información de detección de usuarios cognitivos, identifica el espectro disponible y envía esta información a otros usuarios cognitivos. Esta unidad se conoce como centro de fusión o estación base. El resultado obtenido en el centro de fusión se calcula a partir de observaciones independientes de cada nodo. Estas observaciones se transmiten al centro de fusión en forma binaria para reducir el ancho de banda. Además, sólo algunos de los usuarios cognitivos con información fiable son considerados por el centro de fusión.

- Sensoriamento cooperativo distribuido
  El sensoriamento distribuido no necesita un centro de fusión para recoger la información. Esta información de detección se comparte entre los nodos de la red, por lo que cada nodo hace que sus propias decisiones con respecto a la parte del espectro que se puede utilizar. Esta detección es más ventajosa que la detección centralizada en el sentido de que no requiere un soporte de infraestructura de la red y tienen un costo reducido. Al igual que en la detección centralizada, las decisiones individuales se transmiten en forma binaria para reducir el ancho de banda.

- Sensoriamento cooperativo externo
  En el sensoriamento externo, los agentes realizan la detección de la actividad primaria en el canal licenciado, y transmiten la información del canal monitorizado a los nodos de la red o estación base, esto depende del tipo de arquitectura de la red. Estos agentes están representados por sensores. Las principales ventajas de los sensores son la superación a los problemas de sombreado. Además, los sensores disminuyen el tiempo de detección del espectro por estar fuera de la red.

2.4. Técnicas de análisis de múltiples criterios y análisis condicional

En esta sección, se presentan las técnicas empleadas para el análisis de la presencia del ataque EUP. En primer lugar, se explica una técnica de análisis de múltiples criterios

utilizados para determinar la probabilidad preliminar de la presencia del ataque EUP. Por otra parte, la técnica para determinar los pesos de importancia para cada uno de los criterios utilizados en este estudio es descrita. Por último, se presenta la técnica de probabilidad condicional utiliza para determinar la probabilidad final de la presencia del ataque a la red.

2.4.1. Análisis de múltiples criterios

Una técnica para el análisis de múltiples criterios puede seguir una formalización de la decisión de sentido común a los problemas complejos que son informales [78]. El análisis de múltiples criterios (MCDM y MCDA, del inglés, Multiple-criteria decision-making o Multiple-criteria decision analysis) se utiliza como un término general que abarca los métodos que explícitamente consideran varios criterios para ayudar a los individuos o grupos en la evaluación integral de alternativas de decisión con diferentes objetivos y efectos contradictorios sobre sus valores, ayudando así a la toma de decisiones. El análisis de múltiples criterios utiliza varios métodos para encontrar la mejor alternativa [79].

El desarrollo de MCDA está estrechamente relacionado con el avance de la tecnología informática. Por un lado, el rápido desarrollo de la tecnología informática en los últimos años ha hecho posible la realización de un análisis sistemático de los problemas complejos MCDA. Por otro lado, el uso generalizado de los ordenadores y la tecnología informática ha generado una enorme cantidad de información, que hace que el MCDA cada vez más importante y útil para el apoyo a la decisiones [80].

El objetivo de los métodos de decisión MCDA es tomar la mejor decisión entre varias alternativas para solucionar un problema, teniendo en cuenta un conjunto de criterios de evaluación. En particular, este documento emplea el método NWAUF (Normalized Weighted Additive Utility Function) [81], fundamentado en los estudios que muestran su bajo coste computacional en comparación con otros métodos, tales como AHP (Analytic Hierarchy Process) [82] o ELECTRE [83], y sus respectivas variantes [81, 84].

- Normalized Weighted Additive Utility Function

  El proceso de análisis de multiples criterios implica la elección entre alternativas. Estas alternativas se pueden clasificar en función de diversos criterios, utilizando un MCDA. En general, la metodología MCDA implica cuatro pasos [81]:

  1. Identificar y evaluar los valores de los criterios.
  2. Identificar el conjunto de alternativas.
  3. Escoger y aplicar um método de clasificación alternativa.
  4. Escoger la mejor alternativa.

Para ejecutar las etapas del MCDA aplicando el método NWAUF en las CRAHNs, los siguientes pasos son realizados [81, 85, 86]:

1. NWAUF define los valores mínimos y máximos para cada criterio c recolectados utilizando uma técnica de sensoriamento del espectro. Estos valores componen, respectivamente, los conjuntos denotados por $\mathbf{MIN}$ y $\mathbf{MAX}$. Cada criterio c contiene un número de muestras. Siendo que $\mathbf{MIN}_z = c_{z,min}$ y $\mathbf{MAX}_z = c_{z,max}$, donde $z = 1, 2, 3, ...c$, por otro lado, min y max representan el valor mínimo y máximo de los conjuntos de muestras para cada criterio c.

2. Cada criterio c es normalizado en $c' = \frac{c_z - \mathbf{MIN}_z}{\mathbf{MAX}_z - \mathbf{MIN}_z}$. Note que los valores obtenidos estan en el intervalo de 0 y 1.

3. Los pesos de importancia para cada criterio normalizado c' son adicionados y evaluados. Donde, la cantidad de pesos de importancia es igual a la cantidad de criterios. Además, cada peso w es representado en un intervalo [0,1] y la suma de los pesos necesariamente debe ser igual a 1. Esto es $\sum_{i=1}^{k} w_z = 1$, donde $w_z > 0 \; \forall \; z$.

4. Por fin, una función de utilidad se calcula y se denota por U. El cálculo se consigue mediante la siguiente Ecuación 2.8, donde se utiliza la suma de los pesos de importancia en relación con los criterios normalizados. Esta utilidad determina una probabilidad, teniendo en cuenta los pesos de importancia sobre los valores recolectados previamente.

$$U = \sum_{z=1}^{c} w_z c'_z, \; \forall \; z = 1, 2, ..., c \tag{2.8}$$

Sin embargo, NWAUF en el paso número 3 considera pesos de importancia a cada criterio. Este es un punto importante porque estos pesos determinan el grado de importancia de un criterio en la decisión conjuntamente con los demás. Para obtener estos pesos es utilizada la técnica de análisis de componente principal (PCA, del inglés, Principal-component analysis), que se describe a continuación.

- Análisis de componente principal

PCA es una técnica estadística que se utiliza para clasificar los criterios por la suma de pesos de importancia. La técnica identifica patrones en los conjuntos de criterios, y expresa esos criterios de forma que resalten sus similitudes y diferencias. Cuando estos patrones se encuentran en los criterios, la técnica permite comprimir los criterios, reduciendo el número de dimensiones de los criterios sin pérdida de información [87]. De esta dimensionalidad reducida, la técnica encuentra las causas de la

variabilidad de los conjuntos de criterios, que se llaman componentes principales, y se presentan en un orden de importancia decreciente [88, 89]. PCA fue elegido frente a otras técnicas por la característica de la correlación entre los criterios analizados, esto puede indicar que hay alguna información redundante [90]. Para aplicar PCA en un conjunto de criterios se realizan los siguientes pasos [87]:

1. PCA analiza un conjunto de criterios S, cada criterio considera un número de muestras. Donde, el objetivo es reducir los criterios para obtener un conjunto de observaciones y pueda ser descrita con apenas, L variables, L < S.

2. Calculo de la media para los conjuntos de los criterios $S = \{c_1, c_2, c_3, ..., c_z\}$, denotado por la Ecuación 2.9, y el cálculo de la desviación estándar por la Ecuación 2.10.

$$u[m] = \frac{1}{N}\sum_{n=1}^{N} c[m,n] \tag{2.9}$$

(2.10)

$$c_m^2 = \frac{1}{N-1}\sum_{n=1}^{N}(c[m,n] - u[m])^2$$

3. Seguidamente, es calculada la correlación y la preparación de la matriz de correlación de los criterios con la Ecuación 2.11, con ayuda de las medias y la desviación estándar encontradas en el paso anterior.

$$R_{c_m} = \frac{\frac{1}{N-1}\sum_{n=1}^{N}(c[m_m,n] - u[m])^2}{c_m} \tag{2.11}$$

4. Estadisticamente, sobre el conjunto de criterios $S = \{c_1, c_2, c_3, ..., c_z\}$, el análisis del componente principal produce un nuevo conjunto de factores $Y = \{y_1, y_2, y_3, ..., y_z\}$, entonces el conjunto de componentes principales Y es una combinación linear del conjunto S, denotada por la Ecuación 2.12, donde a_z es llamada carga del criterio c_z en el factor y_z.

$$y_z = \sum_{z=1}^{n} a_z c_z \tag{2.12}$$

5. Cada elemento del conjunto Y denota el grado de importancia de los componentes principales.

2.4.2. Teorema de Bayes

Bayes introduce el concepto de probabilidad condicional de estadística elemental. Tomamos nota de que la probabilidad condicional de un evento es una probabilidad obtenida con la información adicional de otro evento ya ha ocurrido. Utilizamos P(A|B) para inferir la probabilidad condicional del evento A, ya que el evento B ha ocurrido. La Ecuación 2.13 determina P(A|B) [91]. En este contexto, al ser Bayes un método de fusión de datos de la inferencia probabilística y no un método de estimación, clasificación, agregación, entre otros. Utilizamos Bayes para inferir una probabilidad final de un evento que se ve afectado por otro evento [92].

$$P(A|B) = \frac{P(B|A)}{P(B)} \tag{2.13}$$

El factor clave para entender la esencia del teorema de Bayes es reconocer que se trata de eventos secuenciales, en los que la información adicional se utiliza para recalcular la probabilidad del evento inicial [91]. En este contexto, se utilizan los términos de la probabilidad previa y posterior. La probabilidad previa es el valor de probabilidad inicial obtenida en las informaciones adicionales P (a_i). La parte posterior de probabilidad es el valor de probabilidad de que se calcula con el uso de la información P(A_i|B) [93, 94]. Así que, después de haber considerado la información adicional y los tipos de probabilidades, la probabilidad del evento A dado el evento B, que subsecuentemente sucedió, es determina por la Ecuación 2.14.

$$P(A_i|B) = \frac{P(A_i).P(B|A_i)}{\sum_{k=1}^{n} P(A_k).P(B|A_k)} \tag{2.14}$$

Un análisis realizado por el teorema de Bayes proporciona una forma de tratar la información conceptualmente diferente de todos los otros métodos estadísticos. Bayes proporciona un método en el que se utilizan las observaciones para actualizar las estimaciones de los parámetros desconocidos de un modelo estadístico [95]. Bayes determina la probabilidad de un evento considerando los valores de las probabilidades de las informaciones adicionales. Este teorema relaciona el evento que va a pasar con su condicional, es decir, un valor de la información adicional.

2.5. Resumen

Este capítulo introduce los conceptos relacionados al funcionamiento de la tecnología de radio cognitivo, destacando su uso en redes ad hoc de radio cognitivo. Además, se describen las vulnerabilidades de estas redes, y se clasifican estas vulnerabilidades en conformidad con las capas de la pila de protocolo. En este trabajo, nos centramos en las vulnerabilidades causadas en la capa física, enfatizando en el ataque EUP. También

presentamos las técnicas de sensoriamento del espectro que están destinados a recolectar información de canales de frecuencia para su posterior análisis. Por otra parte, describimos la técnica de análisis de múltiples criterios conjuntamente con una técnica de análisis de pesos de importancia para cada criterio. Por último, se presenta el teorema de Bayes como método de fusión de información y análisis de la probabilidad condicional.

CAPÍTULO 3

ANÁLISIS DE TRABAJOS RELACIONADOS

3.1. Detección y mitigación de ataques de emulación de usuario primario

En esta sección, se describen los esquemas para la detección y mitigación de ataques de emulación de usuario principal (EUP) en las redes de radio cognitivo. Algunos de estos esquemas aplican técnicas descritas anteriormente y otras presentan nuevos algoritmos. La Tabla 3.1 ilustra una visión general de los esquemas o modelos de detección y mitigación encontrados en la literatura y son clasificados según el enfoque: cooperativa o no cooperativa.

Cuadro 3.1: Esquemas de detección e mitigación de ataques EUP

Esquema / Abordaje	Detección	Mitigación
No cooperativo	Chen e Park 2006 [28], Chen et al. 2007 [29], Jin et al. 2009 [17], Zhao et al. [96], Li e Han 2010 [30], Chen et al. 2011 [31]	Anand et al. 2008 [22], Jin et al. 2009 [35]
Cooperativo	Jin et al. [97], Huang et al. [98], Min et al. 2011 [34], Chen et al 2011 [33], Leon et al. [27]	Jin et al. 2010 [32], Jin et al. 2010 [26]

Se clasifico las soluciones existentes en la literatura como esquemas para detectar o mitigar los ataques EUP. Los primeros trabajos tienen como objetivo el detectar ataques en el espectro y localizar los nodos maliciosos en la red. Los segundos realizan una doble tarea: primero detectan un ataque, para después identificar a los atacantes y realizar alguna acción en la red con el fin de no utilizar esta parte del espectro que está siendo atacado. Todos estos sistemas emplean en su desarrollo de técnicas de detección para recolectar datos para su análisis. En la Tabla 3.1, se presenta enfoques no cooperativos y cooperativos. Un enfoque no cooperativo puede ser desarrollado en cualquiera de los tipos de arquitecturas presentados en el capítulo 2, cada nodo de la red lleva a cabo su propia detección y análisis de espectro con el fin de tomar una decisión sobre la presencia del ataque EUP en la red. Sin embargo, esta decisión no se verá influenciada por las decisiones de otros nodos de la red. En un enfoque de cooperativo, la decisión sobre el espectro está influenciada por otros nodos cooperativos. Estos intercambios de informa-

ción y llegan a un consenso en común sobre la presencia de ataques EUP en la red. Un enfoque cooperativo de la misma forma que un enfoque no cooperativa también puede ser implementado en cualquier tipo de arquitecturas presentadas en el capítulo 2. A continuación se presentan los esquemas y soluciones en la literatura, siguiendo la perspectiva de enfoque no cooperativo y cooperativo.

3.1.1. Esquemas con abordaje no cooperativo

Chen y Park [28] usan dos técnicas para la verificación del transmisor con el fin de distinguir señales primarias de señales secundarias maliciosas. Una primera técnica se llama la prueba de la relación de distancia (DTR, del inglés, Distance Ratio Test). Esta técnica utiliza un par de verificadores que son nodos dedicados a la detección. La ubicación de estos nodos es conocida por los nodos del esquema. El nivel de potencia recibida se mide para comprobar posteriormente la ubicación del transmisor. La segunda técnica llamada prueba de diferencia de distancia (DDT, del inglés, Distance Difference Test) comprueba la diferencia de las distancias entre el transmisor primario y los verificadores. Esta diferencia se obtiene por el desplazamiento de fase de la señal de los verificadores. Sin embargo, para la verificación de la señal recibida, estas técnicas utilizan una técnica basada en la detección por la energía con el fin de recolectar datos. Estos datos se analizaron mediante las técnicas propuestas en el esquema.

Chen et al. [29] propusieron un esquema de verificación del transmisor llamado LocDef (del inglés, Localization-based Defense). Este esquema utiliza las características de la señal y la ubicación del transmisor para comprobar las señales de transmisión de los UP. El esquema utiliza una red de sensores inalámbricos para recopilar información de las señales recibidas. Este plan tiene tres etapas: verificación de características de la señal, medición de potencia recibida y la ubicación de la señal del transmisor. Inicialmente, un proceso de detección se lleva a cabo, en donde se detecta la señal en la banda con licencia. Si la señal de exploración de UP es negativo, se concluye como un signo de US. Sin embargo, si la verificación es positiva, se procede a calcular la ubicación del transmisor y la compara con la ubicación conocida de los transmisores primarios. Si la ubicación no coincide con los transmisores primarios se concluye como un ataque EUP. Por otra parte, si la ubicación es igual a los transmisores primarios, una comparación del nivel de energía se lleva a cabo con el fin de obtener el resultado final en la presencia de ataque EUP.

Jin et al. [17] presentan un modelo analítico para la detección de ataques EUP. Se propone un análisis de aproximación de Fenton y WSPRT (del inglés, Wald's Sequential Probability Ratio Test). Inicialmente, es la aproximación de Fenton para detectar la probabilidad del éxito del ataque EUP. Ellos usan la desigualdad de Markov para proporcionar un límite inferior en la probabilidad de éxito del ataque EUP. Una función de densidad de probabilidad (PDF) de la señal recibida de los usuarios maliciosos se obtiene a partir de

la aproximación de Fenton. Este PDF es utilizado por WSPRT para lograr la detección de ataques EUP.

Zhao et al. [96] presentan un plan de seguridad contra los ataques EUP. Este sistema se basa en la verificación de fingerprint para identificar un ataque EUP. Un fingerprint se define como una característica de la señal que se transmite espectro. En este esquema se utiliza un fingerprint que se determina por el ruido de la señal. Esta potencia de ruido se extrae de la señal recibida para identificar al transmisor mal intencionado en el espectro.

Li y Han [30] propusieron un esquema llamado Dogfight para la detección de ataques EUP. Este utiliza un usuario secundario legítimo para controlar el espectro en intervalos de tiempo. Con ello, este sistema realiza una detección proactiva del ataque. Un atacante y un defensor compiten por el acceso al espectro, y se correlaciona esa competición como un juego de combate aéreo. El esquema se modela utilizando el principio de la teoría del juego entre el atacante y el defensor. Un equilibrio de Nash se determina entre los dos, que proporciona una estrategia de operación para los usuarios secundarios honestos.

Chen et al. [31] presentan un método para la detección de ataques EUP en escenarios con usuarios primarios móviles con una potencia de transmisión baja. Estos dispositivos móviles se representan mediante micrófonos que añaden mayores dificultades en la detección de ataques, ya que los métodos existentes no son aplicables porque presentan escenarios con usuarios primarios fijos y una potencia de transmisión más alta. En este esquema todos los USs legítimos están equipados con sensores acústicos. Las correlaciones entre el nivel de energía y la información acústica recibida por el sensor se explora para verificar la autenticidad de los micrófonos inalámbricos como usuarios primarios.

Además de los enfoques que tratan la detección de ataques EUP, también son los que tienen como objetivo mitigar los efectos de estos ataques. Primeramente los trabajos de mitigación en escenarios no cooperativos son presentados. Anand et al. [22] proponen un modelo analítico basado en la aproximación de Fenton y la desigualdad de Markov. Ellos obtienen las expresiones matemáticas de Fenton y Markov para establecer los límites inferiores de la probabilidad de éxito de un ataque EUP. Para ello, la potencia de la señal recibida de un usuarios secundario es modelada y utilizan Fenton para determinar la media y la varianza de esta potencia recibida. A continuación, se utilizó la media y la varianza para establecer los límites más bajos utilizando el desigualdad de Markov. Con estos límites los autores establecen la medida en que uno puede identificar un ataque EUP en la red.

En Jin et al. [35] la técnica NPCHT (del inglés, Neyman-Pearson Composite Hypothesis Test) y la técnica WSPRT (del inglés, Wald's Sequential Probability Ratio Test) se proponen para mitigar los ataques EUP. Ambas técnicas mitigan el ataque en el desvanecimiento de los entornos inalámbricos, sin asumir funciones adicionales para los nodos secundarios o la presencia de nodos de sensores. En el esquema, una aproximación de Fenton se utiliza para modelar la potencia recibida por el usuario secundario. El NPCHT

logra una baja probabilidad de pérdida de la señal de usuario principal y reduce al mínimo la probabilidad de éxito del ataque EUP. Sin embargo, la aplicación de la WSPRT es posible mitigar el ataque EUP.

3.1.2. Esquemas con abordaje cooperativo

Jin et al.[97] presentan un análisis para estudiar el impacto de los ataques EUP contra los usuarios secundarios legítimos en términos de pérdida de acceso al espectro. En este análisis, se utiliza la cadena de Markov 3D-CTMC (del inglés, Three Dimensional Continuous Time Markov Chain) para modelar la ocupación del canal con la presencia de los atacantes y los usuarios primario legítimos. Este análisis se evaluó en escenarios con arquitecturas centralizadas y distribuidas con criterios de cooperación, en el que los usuarios secundarios compartiendo la información con el fin de decidir sobre el espectro. Los resultados muestran que los ataques afectan un 40 % de las oportunidades de acceso a los canales por parte de los usuario secundarios legítimos.

Huang et al. [98] exponen las técnicas TDOA (del inglés, Difference Of Arrival) y FDOA (del inglés, Frequency Difference Of Arrival), que se utiliza para localizar el transmisor. Esta ubicación se utiliza para diferenciar una emisión primaria legítima de un atacante. Se logra la combinación de las dos técnicas. En un primer paso, la técnica TDOA se aplica para la detección de transmisores maliciosos a través de la potencia señal recibida. En la segunda etapa, la técnica FDOA es aplicada con los datos calculados por el TDOA para una mejor identificación del atacante.

Min et al. [34] presentan un framework de cooperación para la detección de ataques EUP llamado IRIS (del inglés, cooperatIve sensing via iteRatIve State estimation). Este utiliza la potencia de transmisión del usuario principal y su exponente de pérdida de propagación para la estimación de la detección. Este sistema emplea sensores distribuidos en la red para recoger información de detección. Posteriormente, la información se procesa en una estación base para una decisión final (cooperación centralizada).

Chen et al. [33] proponen un esquema de detección del ataque EUP que presenta un modelo de cooperación para maximizar la probabilidad de detección del usuario principal. Cada usuario secundario recibe señales desde el atacante y del usuario principal, y envía la información de detección a un centro de fusión (estación base). La señal recibida se combina con pesos apropiados para maximizar la probabilidad de detección mediante la restricción de la probabilidad de falsa alarma.

En Leon et al. [27] un esquema centralizado utilizando un enfoque de cooperación es propuesto. Este esquema presenta una técnica para determinar la ubicación del atacante en la red, con el conocimiento previo de la ubicación de la estación base primaria. La técnica utilizada es la TDOA (del inglés, Time Difference Of Arrival). Esto verifica la ubicación del usuario malintencionado por la diferencia de tiempo en la señal recibida en

cada receptor (usuarios secundarios). La técnica proporciona un enfoque cooperativo por el hecho de que necesita un tiempo de recepción de la señal en otros receptores. Por otra parte, este esquema de administración se lleva a cabo en una estación base centralizada.

Nguyen et al. [99] presentan un esquema llamado DECLOAK. Este esquema es pasivo, en el que un dispositivo está en el entorno de escucha para reunir los datos. Estos datos recolectados son fingerprints de los dispositivos, que no pueden ser fácilmente imitados. Después de esta colección, el esquema DECLOAK aplica el modelo de mezcla infinita de Gauss (IGMM, del inglés, Infinite Gaussian mixture model) para la fusión de los fingerprints clasificados por el método de Gibbs para determinar la presencia del ataque EUP en una red con una arquitectura distribuida y enfoque cooperativo.

Además de las soluciones de detección de ataques, existen aquellas que mitigan los ataques EUP en escenarios cooperativos. Jin et al. [32] presentan un protocolo para la mitigación. Este sigue una arquitectura centralizada y divide el procedimiento de dos pasos. En el primer paso, los nodos secundarios legítimos supervisan el espectro, recibiendo la potencia de transmisión de la señal del UP, US y usuario malintencionado. Estas tres señales se modelan para determinar la presencia del ataque por la técnica de detección por la energía. Cada usuario secundario informa de su decisión de detección a una estación base. En esta estación, el segundo paso tiene lugar en la toma de una decisión final teniendo en cuenta la información de detección de otros USs. Este protocolo trata de reducir la probabilidad de éxito del ataque EUP.

Jin et al. [26] proponen un protocolo llamado NEAT (del inglés, NEighbor AssisTed Spectrum Decision). NEAT se presenta con una arquitectura distribuida para mitigar ataques EUP. Este protocolo es una mejora de su propuesta anterior en [32]. En la primera etapa del esquema, las señales del UP, US y usuario malicioso se modelan en términos de recepción de energía y se aplica un mecanismo de mitigación preliminar. En la segunda etapa se muestra el proceso de detección y mitigación de cooperativo. La información recopilada se comparte entre los nodos de la red. Para un nodo para determinar la presencia de un ataque, este solicita información de detección a sus nodos vecinos, es decir, los nodos que se encuentran a un salto de distancia. Con la información de detección, toma la decisión final del éxito del ataque EUP.

3.2. Análisis de los trabajos relacionados

Como se mencionó anteriormente, los trabajos en la literatura presentan esquemas para detectar o mitigar los ataques EUP en las redes de radio cognitiva. Estos esquemas se clasifican siguiendo abordajes no cooperativos y cooperativos. A continuación, realizamos un análisis de las principales ventajas y desventajas de estos esquemas.

- Ventajas

  Se observa que los esquemas propuestos han evolucionado en la literatura sobre el tipo de abordaje utilizado para cada esquema. En este contexto, vale la pena señalar que esquemas con una arquitectura distribuida tienen un mejor desempeño en la detección y mitigación de ataques EUP en relación a otro tipo de esquemas. Por otra parte, el uso de enfoques de cooperación para identificar estos ataques representan un ahorro de tiempo y reducción de falsos positivos y negativos, así como la disminución de la pérdida de detección del usuario primario legítimo, como son expuestas en los siguientes trabajos: [26, 27, 32, 33, 34, 97, 98, 99].

  Sin embargo, no se puede excluir a los trabajos que tienen arquitecturas centralizadas o distribuidas con enfoques no cooperativos. Pues estos, además de considerar un enfoque no cooperativo, presentan técnicas y métodos para la obtención de las características o criterios del canal de radio. Estos criterios pueden ser utilizados para llevar a cabo un análisis para determinar la presencia del atacante en la red. Por ejemplo, Chen y Park [28] y Chen et al. [29] proponen técnicas que identifican la ubicación del transmisor por la potencia de la señal recibida en el dispositivo receptor. Por otra parte, Huang et al. [98] y Leon et al. [27] proporcionan a la aplicación de técnicas similares para determinar la ubicación del atacante en enfoques de cooperación.

  Sin embargo, trabajos como el de Zhao et al. [96] y Nguyen et al. [99] introducen el término fingerprints . Estas fingerprints denotan las características del canal en el espectro de radiofrecuencias. Estos planes ofrecen técnicas para la recoleccion de los valores de estas características o criterios del canal. Por otro lado, se puede inferir que uno de los criterios más importantes ampliamente estudiados y utilizados entre todos los trabajos reportados en la literatura es la potencia de la señal recibida por un dispositivo. A continuación, otros criterios considerados en estos trabajos son la ubicación, distancia, tipos de modulación, ruido, entre otros.

- Desventajas

  Sistemas centralizados o distribuidos con enfoques no cooperativas tienen una alta tasa de falsos positivos y negativos. Estos inconvenientes están tratando de ser suplidos por la aparición de esquemas cooperativos distribuidos. Sin embargo, a pesar de las ventajas de los esquemas vistos en la literatura, se descubre que en su ámbito de trabajo, un análisis de criterios múltiples, es casi inexistente.

  Los trabajos presentados en este capítulo se basan en el análisis casi exclusivamente de un solo criterio o característica. Un ejemplo es el trabajo de Jin et al. [26], que propone un esquema cooperativo distribuida con referencia al análisis de un solo criterio, la intensidad de la señal recibida. Nguyen et al. [99] proponen el único

esquema que lleva a cabo un análisis de múltiples criterios basados en características cicloestacionárias. El trabajo de Nguyen et al. puede representar un gran avance en la detección y mitigación de ataques EUP, pero también tiene desventajas importantes. Al tener en cuenta las características cicloestacionárias, se requiere que el esquema tenga un conocimiento previo de las características del canal, con el fin de establecer una autocorrelación de las características obtenidas con las conocidas previamente. Por otra parte, al ser características cicloestacionárias este esquema debe utilizar necesariamente una técnica de detección cicloestacionária lo que significa un mayor coste computacional y robustez en la implementación.

3.3. Resumen

Este capítulo presento los esquemas y las soluciones propuestas en la literatura para la detección y mitigación de ataques EUP. En este contexto, fue realizada una breve contextualización esquema de detección y mitigación, además de los enfoques no cooperativos y cooperativos. En seguida, fue relatado un análisis de las ventajas y desventajas de los esquemas encontrados en la literatura.

CAPÍTULO 4

ESQUEMA FLEXEUP

4.1. Vision general del esquema FLEXEUP

El esquema FLEXible de múltiples criterios para detectar ataques de Emulación de Usuario Primario en redes ad hoc de radio cognitivo, tiene como objetivo determinar La probabilidad de La presencia de ataques de emulación de usuario primario (EUP). El esquema FLEXEUP esta formado por dos fases principales: la individual y la de cooperación que se ejecutan en cada nodo de la red. La Figura 4.1 ilustra las fases del esquema FLEXEUP.

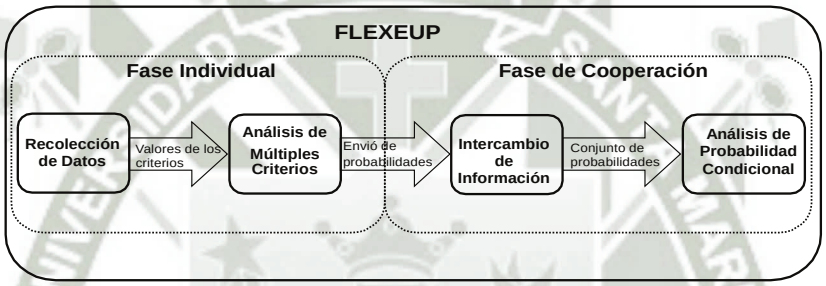


Figura 4.1: Esquema FLEXEUP [Elaborado por los autores]

La fase individual es responsable de calcular de forma probabilística las hipótesis preliminares para cada usuario de la red secundaria (US). Se compone de las operaciones, recolección de datos y análisis de multiples criterios. La operación de recolección de datos realiza un sensoriamento del espectro con el fin de obtener los valores de los criterios utilizados por el esquema. El sensoriamento del espectro emplea la técnica de detección por la energía para recolectar los datos en diferentes canales de frecuencia. A continuación, la operación de análisis de múltiples criterios emplea el método NWAUF y determina la probabilidad preliminar de la presencia del ataque EUP a partir de los valores recolectados para cada criterio establecido.

Después de que cada US obtiene su hipótesis preliminar, la fase de la cooperación determina la probabilidad final de la presencia del ataque EUP. En esta fase, cada nodo envía la probabilidad preliminar calculado por él a sus nodos vecinos. Siendo definido un nodo vecino, como los nodos que están en el mismo canal de frecuencia y un salto de distancia del nodo interesado en el análisis. A su vez, cada nodo vecino también comparte su respectiva probabilidad preliminar. Después de este intercambio de información, cada nodo emplea un análisis de fusión de datos usando el teorema de Bayes para calcular su probabilidad final de la presencia de un ataque EUP.

4.1.1. Modelo del sistema

En este apartado se describe el modelo de red y el modelo de ataque considerado en este trabajo. Usamos la notación definida en la Tabla 4.1 para explicar los modelos y ataques de red.

Cuadro 4.1: Notación del esquema FLEXEUP

Notación	Definición
N_{UP}	Conjunto de usuarios primarios
N_S	Conjunto de usuarios secundarios
N_{SL}	Conjunto de usuarios secundarios legítimos
N_{SB}	Conjunto de usuarios secundarios malintencionados
i-ésimo	índice que representa un usuario secundario arbitrario
j-ésimo	índice que representa un usuario secundario vecino arbitrario
n_i	Usuario secundario
n_j	Usuario secundario vecino de n_i
$P_{n_i}(A)$	Probabilidad preliminar calculada por el nodo n_i
$P_{n_j}(B)$	Probabilidad preliminar calculada por el vecino n_j
$P_{n_i}(A\|B)$	Probabilidad final calculada por el nodo n_i
$P_{n_j}(B\|A)$	Probabilidad final calculada por el vecino n_j
S	Conjunto de criterios
W	Conjunto de pesos de importancia para los criterios
MIN e MAX	Conjunto de valores mínimos y máximos
M	Conjunto de canales de frecuencias
m	Canal de frecuencia

Modelo de Red - La red ad hoc de radio cognitivo está formado por un conjunto de usuarios secundarios estáticos (nodos sin movimiento) representado por N_S. Cada elemento de N_S está representado por n_i, siendo $N_S = N_{SL} \cup N_{SB}$, donde N_{SL} es el subconjunto de USs legítimo y N_{SB} es el subconjunto de USs malintencionados (maliciosos y egoístas). Cada US arbitrario n_i tiene un mecanismo de sensoriamento del espectro. Los nodos de la red se comunican mediante un canal de frecuencia, denotados por m y comprende por lo tanto un conjunto de canales M. Cada n_i que desee transmitir, realiza el proceso de detección con el fin de comprobar que canales del espectro están libres y luego determinar que canal se utilizará. La elección del canal se produce en tres formas: aleatoria, secuencial, y teniendo en cuenta la oportunidad de alta transmisión en el canal como se define en el modelo de red CRAHN.

Después de la detección, cada uno n_i calcula una probabilidad de la presencia del ataque EUP, denotado por $P_{n_i}(A)$. Posteriormente, cada n_i calcula la probabilidad final de la presencia del ataque EUP, denotado por $P_{n_i}(A|B)$, teniendo en cuenta las probabilidades preliminares vecinas $P_{n_j}(B)$, donde n_j representa un nodo vecino del nodo n_i. Por otro lado, se supone que la red ad hoc de radio cognitivo opera en paralelo con una red primaria formada por el conjunto de usuarios primarios, denotado por N_{UP}. Cada usuario primario $UP \in N_{UP}$ realiza sus transmisiones en su respectiva banda licenciada. Estas comunicaciones primarias comienzan en el transmisor principal y terminan el receptor primario.

Modelo del ataque - Los nodos que pertenecen al grupo de usuarios malintencionados $N_{SB} \in N_S$, llamado atacantes, que emulan las características de un usuario primario al adaptar y modificar sus parámetros de radio de su dispositivo. Por ejemplo, el cambio de la potencia de transmisión, el tipo de modulación, ancho de banda, velocidad de transmisión, etc). Esta emulación permite a los usuarios malintencionados aprovechar los espacios vacíos del espectro y deja a los usuarios secundarios legítimos $N_{SL} \in N_S$ sin oportunidades de acceso. Los atacantes actúan teniendo en cuenta las características de los usuarios primarios en términos de prioridad en el acceso a los canales del espectro. Asumimos que el atacante, así como un usuario secundario legítimo está equipado con un mecanismo de sensoriamento del espectro que permite detectar la presencia de un usuario primario. Este equipo permite al atacante acceder a un canal para ser atacado. Por lo tanto, el atacante emulara las características de un usuario primario legítimo en ese canal con el fin de aprovechar el uso prioritario del espectro, y haciendo que un US legitimo detecte esta presencia como un UP como legitimo y dejando sin oportunidad de acceso al espectro.

La Figura 4.2 ilustra el funcionamiento de una red ad hoc de radio cognitivo (CRAHN, del inglés, Cognitive Radio Ad Hoc Network) bajo la acción de los atacantes. En esta red, observamos distintos nodos legítimos, representados por círculos blancos, y nodos malintencionados representados por círculos grises. Cada nodo tiene una lista de canales disponibles. Cada nodo malintencionado tiene las mismas características que un US legítimo. Por otro lado, un usuario malintencionado (por ejemplo, n_{10}) puede comprometer la comunicación entre dos nodos legítimos (por ejemplo, n_7 y n_9) por tener el mismo canal de frecuencia para transmitir (por ejemplo, canal 4).

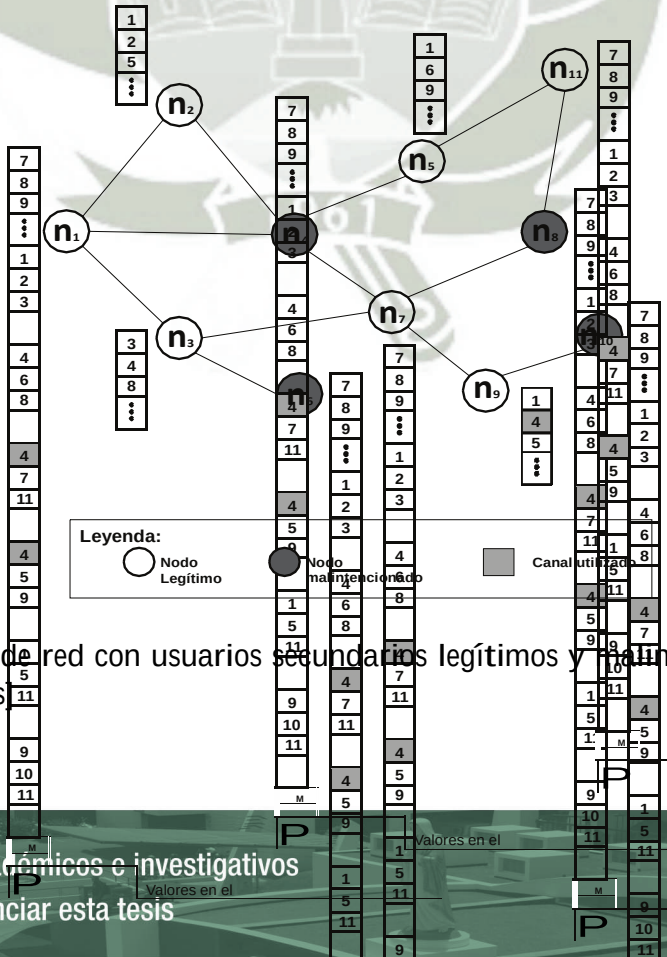


Figura 4.2: Modelo de red con usuarios secundarios legítimos y malintencionados [Elaborado por los autores].

4.2. Fase individual

La fase individual determina de forma probabilística la hipótesis preliminar de la presencia de ataques de EUP en la red y consta de dos operaciones: la recolección de datos y análisis de múltiples criterios. En la primera operación, el FLEXEUP realiza un sensoriamento del espectro, monitoreando cada uno de los M canales que conforman la red primaria. En este sensoriamento, los valores son obtenidos utilizando la técnica de detección por la energía, que se describe en el Capítulo 2, debido a su fácil implementación y no requerir un conocimiento previo de la señal, como se muestra en [41, 100] . Estos valores representan los datos para cada criterio establecido por FLEXEUP. Estos criterios definen las características de la señal en una transmisión en canales de frecuencia. La Figura 4.3 ilustra el sensoriamento del espectro para recolectar datos en la fase individual esquema FLEXEUP. Observe que el nodo n_{11} vigila el canal M_3 del espectro radioeléctrico, así mismo, los nodos n_9 y n_{10} monitorean el canal M_1 donde se puede establecer una comunicación entre estos dos usuarios secundarios. Luego, cada nodo secundario n_i obtiene los valores para cada uno de los criterios. Después de la recolección, estos datos se agrupan en un conjunto de muestras de S por cada c criterio.

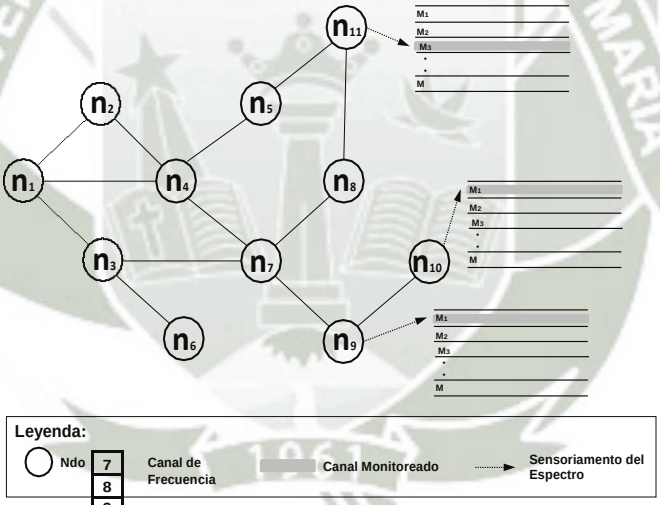


Figura 4.3: Recolección de datos en la fase individual del esquema FLEXEUP [Elaborado por los autores]

A continuación, los conjuntos W, MIN y MAX se definen para calcular la probabilidad de la presencia del ataque EUP, denotado por $P_{n_i}(A)$. Los conjuntos MIN y MAX son compuestos por los valores mínimos y máximos para cada uno de los criterios. El conjunto W está determinada por los pesos de importancia de cada criterio. El cálculo preliminar de la probabilidad se realiza por el método de análisis de múltiples criterios NWAUF (del inglés, emphNormalized Weighted Additive Utility Function) [81]. Los estudios demuestran el bajo coste computacional de este método en comparación a otros métodos de análisis de múltiples criterios, como AHP (Analytic Hierarchy Process) [82]

o ELECTRE [83], y sus respectivas variantes [81, 84]. Los pasos generales del método NWAUF se presentan en el Algoritmo 1. Los conjuntos S, W, MIN y MAX son utilizados por el algoritmo NWAUF. Este método utiliza los conjuntos MIN y MAX para normalizar los valores de S y generar el conjunto normalizado correspondiente, $\overline{S} = \{\overline{s} \mid 0 \leq \overline{s} \leq 1\}$ (lineas 5–6). Por último, el método utiliza el conjunto de pesos $W = \{w_1, w_2, \ldots, w_c \mid \sum_{z=1}^{c} w_z = 1\}$, donde cada peso de importancia es asignado a un criterio en $\overline{S}$ para el cálculo de $P_{n_i}(A)$ (linea 7). Los valores de W son valores estáticos, basados en la relevancia de estudio de cada criterio para determinar la probabilidad de la presencia del ataque EUP. Estos métodos pueden ser definidos por alguna de las técnicas presentadas en Raj [87].

Algoritmo 1 Análisis NWAUF

```
1: procedimiento NWAUFAnalysis(S, W, MIN, MAX)
2:     P_{n_i}(A) ← 0;
3:     S̄ ← ∅;
4:     para todo z = 1 → |c| hacer
5:         s̄_z ← (S_z − MIN_z) / (MAX_z − MIN_z);
6:         S̄ ← S̄ ∪ {s̄};
7:         P_{n_i}(A) ← P_{n_i}(A) + W_z · s̄_z;
8:     fin para
9: fin procedimiento
```

Cada nodo aplica el método NWAUF para calcular la probabilidad de la presencia del ataque EUP mediante la agregación de datos de múltiples criterios. Este resultado es utilizado para calcular la probabilidad final de la presencia del ataque EUP en la fase de cooperación del esquema FLEXEUP. La Figura 4.4 destaca cada paso del análisis que realiza el método NWAUF para los múltiples criterios.

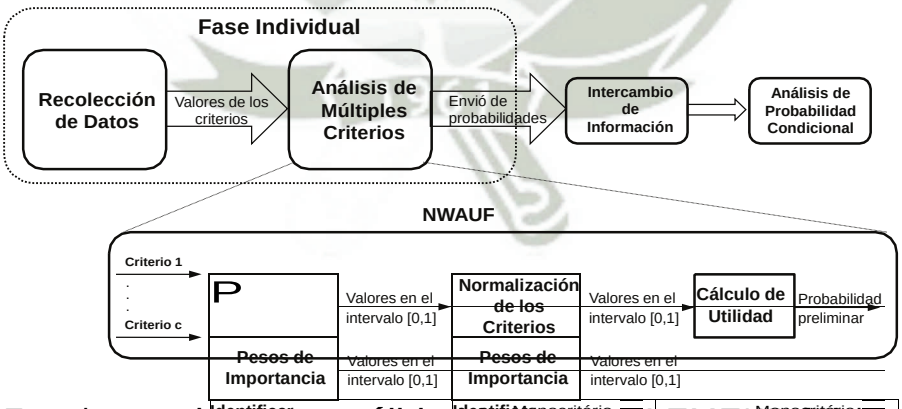


Figura 4.4: Fase de sensoriamento y análisis del esquema FLEXEUP [Elaborado por los autores]

4.3. Fase de cooperación

En la fase de cooperación, el **i**-enésimo US no sólo realiza el intercambio de $P_{n_i}(A)$, también recibe probabilidades preliminares de los nodos vecinos. El primer cambio de probabilidades se realiza mediante el establecimiento de un canal de comunicación común entre n_i y cada uno de sus vecinos n_j. La probabilidad preliminar se envía a los vecinos dentro de un paquete de control. De la misma manera, los vecinos responden con otro paquete de control que contiene sus probabilidades de detección preliminares. La Figura 4.5 ilustra el intercambio de paquetes entre el nodo n_i y sus vecinos correspondientes $n_j, j = 1, \ldots, k$. Observamos que un nodo (por ejemplo, n_1) envía su probabilidad preliminar en un paquete de control a sus vecinos (por ejemplo, n_2, n_3, n_4), y estos responden con otro paquete de control conteniendo sus respectivas probabilidades preliminares.

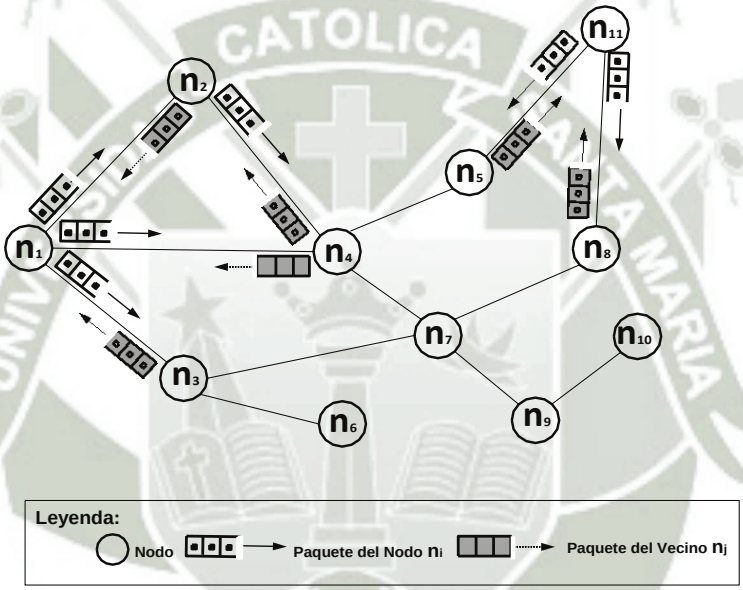


Figura 4.5: Intercambio de probabilidades preliminares [Elaborado por los autores]

Después de recibir $k \leq |N_{SL}| - |\{n_i\}|$ probabilidades preliminares de la vecindad, el nodo $n_i \in N_{SL}$ calcula su probabilidad final $P_{n_i}(A|B)$ referente a la presencia de un ataque EUP en la red por medio del teorema de Bayes (Ecuación 4.1). Este teorema permite calcular la probabilidad condicional $P_{n_i}(A|B)$ de acontecer un dado evento A, mediante la ocurrencia de un evento B. Para esto, el teorema considera uma probabilidad preliminar $P_{n_i}(A)$ de acontecer un evento A sin la influencia del evento B. Además de eso, el también considera la probabilidad preliminar $P_{n_j}(B)$ de acontecer el evento B como la probabilidad inversa de $P_{n_i}(A|B)$, esto es, $P_{n_j}(B|A)$.

Siguiendo el teorema, un nodo n_i calcula la probabilidad final de la presencia de ataque a partir de las probabilidades preliminares $P_{n_i}(A)$, $P_{n_j}(B)$ y $P_{n_j}(B|A)$. En particular, el evento A denota el acontecimiento de un ataque EUP en la perspectiva del nodo n_i. La probabilidad $P_{n_i}(A)$ del evento A acontecer el inicialmente estimada

por n_i a partir del método NWAUF, como es explicado en la fase individual del esquema FLEXEUP. Del mismo modo, cada vecino del nodo n_i calcula su respectiva probabilidad preliminar sobre un ataque EUP en la red. Desde la perspectiva del nodo n_i, el evento B denota la detección de la presencia de un ataque EUP por cada vecino $n_j, j = 1, \ldots, k$, en que k es el total de vecinos del nodo n_i. Cada vecino n_j calcula su propia probabilidad preliminar sobre un ataque EUP en la red. Desde la perspectiva de un nodo n_i, tal probabilidad es denotada por $P_{n_j}(B)$. El teorema de Bayes requiere que cada probabilidad del tipo $P_{n_j}(B|A)$ sea inicialmente estimada a fin de calcular $P_{n_i}(A|B)$. En particular, para nuestro esquema este valor fue estimado considerando rigorosas simulaciones. Con todo ello, este valor es regulado por la influencia de las probabilidades calculadas a partir de las mediciones que cada nodo realiza. La Figura 4.6 destaca los pasos para que cada US determine la probabilidad de la presencia del ataque EUP a través de la probabilidad condicional definida por el teorema de Bayes.

$$P_{n_i}(A|B) = \frac{P_{n_i}(A).P_{n_1}(B|A)}{[\sum_{j=1}^{k} P_{n_j}(B).P_{n_j}(B|A)]} \tag{4.1}$$

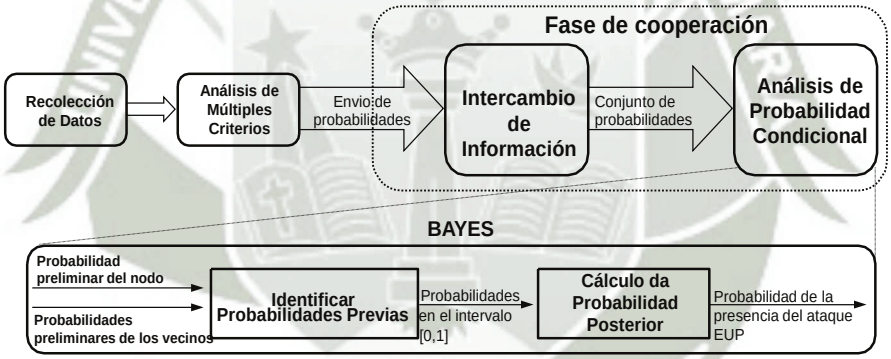


Figura 4.6: Fase de cooperación del esquema FLEXEUP [Elaborado por los autores]

4.4. Resumen

En este capítulo presento el esquema esquema FLEXible de múltiples criterios para detectar ataques de Emulación de Usuario Primario en redes ad hoc de radio cognitivo, denominado FLEXEUP. En un principio, una visión general del esquema FLEXEUP es presentada, seguida de los modelos de red y de ataque. Las dos fases del esquema de FLEXEUP se describen. En la fase individual se destaca la utilización del método NWAUF para el análisis de múltiples criterios y la obtención de la probabilidad preliminar de la presencia del ataque EUP. En la fase de cooperativa se describe como es obtenida la probabilidad final de la presencia de ataque EUP aplicando el teorema de Bayes.

CAPÍTULO 5

ANÁLISIS Y RESULTADOS

5.1. Escenarios de simulación

El simulador de red NS, versión 2.31 se utilizó para evaluar el rendimiento y la eficiencia de FLEXEUP. El esquema ha sido implementado e integrado al código del módulo CRAHN, desarrollado por investigadores de la Universidad de Northeastern, EUA [36]. El esquema FLEXEUP se evaluó teniendo en cuenta la interferencia de los nodos malintencionados en la red, y que actúan como los ataques de emulación de usuario primario (EUP). Estos ataques imitan las características del usuario primario (PU) en los canales de transmisión, emulando así a un usuario primario legítimo. Como se ha mencionado, un ataque EUP reduce la posibilidad de acceso al espectro a los usuarios secundarios legítimos.

Los escenarios de red simulados se componen de $|N_S| = 50$ o $= |N_S| = 100$ nodos estáticos, siendo que la cantidad de $|N_{SL}|$ (USs legítimos) y $|N_{SB}|$ (USs malintencionados) varían para reflejar diferentes tasas de atacantes en la red. Los usuarios secundarios de la CRAHN pueden comunicarse utilizando $|M| = 11$ canales en el rango de frecuencias de radio de 2,412 a 2,462 GHz. A pesar de este rango de frecuencias considerarse libre, el módulo CRAHN emplea este rango de frecuencias y obliga a los usuarios primarios a compartir estas bandas de frecuencias con los usuarios secundarios. Por ser un modelo, este aspecto no pone en peligro la generalidad de los resultados obtenidos en este trabajo.

En particular, se asume el modelo de propagación Free Space para la señal primaria detectada por un nodo n_i, si $UP \in N_{UP}$, y un modelo de propagación Two Ray Ground de la señal detectada por un nodo n_i a partir de un US malintencionado o un US legítimo [22, 26]. El conjunto de usuarios secundarios N_S están dispuestos en una superficie de 1000m x 1000m siguiendo una variación del modelo Random Waypoint, donde se fuerza la ausencia de movimiento de los nodos. El protocolo de enrutamiento utilizado es el Ad hoc On demand Distance Vector Routing (AODV), el rango de los nodos es de 250 m como se especifica en el estándar IEEE 802.11.

Cada nodo $n_i \in N_S$ es implementado de las dos fases del esquema FLEXEUP. La fase individual realiza una recolección de datos para los c criterios. En particular, fueron definidos dos casos de simulación: caso 1 y caso 2, que emplean diferentes cantidades y tipos de criterios. En el caso 1, se consideran tres criterios, siendo estos: la potencia de recepción, la potencia de transmisión y la distancia. En el caso 2, tenemos en cuenta cuatro criterios, siendo estos: potencia de recepción, SNR (del inglés, Signal to noise ratio), ruido y tasa de transmisión. El esquema FLEXEUP usa

múltiples criterios que han sido ampliamente estudiados y evaluados en la literatura para la detección y mitigación de ataques EUP. Estos criterios se agregan utilizando una técnica de fusión de datos para determinar la presencia de ataques de EUP.

Además de la recolección de datos, el esquema FLEXEUP realiza principalmente un análisis de múltiples criterios. En este análisis, el régimen utiliza el método NWAUF con base en el conjunto de muestras S para cada uno de los c criterios. Inicialmente, se utilizan los conjuntos mínimos MIN y máximos MAX para normalizar los valores del conjunto S. Estos conjuntos mínimos y máximos están constituidos por los valores mínimos y máximos para cada criterio obtenido de las muestras. Luego, NWAUF utiliza un conjunto W de pesos de importancia a cada criterio. Estos pesos se obtienen mediante la aplicación de la técnica de análisis de componentes principales (PCA, del inglés Principal Component Analysis).

- Análisis de pesos de importancia

  PCA considera un conjunto de muestras para cada criterio como entrada en la definición de los pesos de importancia. Este conjunto de muestras se obtiene a partir de simulaciones y mediciones en escenarios reales. Las muestras obtenidas en simulaciones fueron utilizadas en el caso 1. Estas muestras se obtuvieron de simulaciones realizadas en NS-2. Las muestras de escenarios reales se basaron en los datos disponibles en CRAWDAD (Community Resource for Archiving Wireless Data At Dartmouth) [101], extraídos de dos escenarios de experimentación diferentes en redes en malla inalámbrica (802.11g y 802.11a). A pesar de que estas experimentaciones se encuentran en entornos de redes de malla inalámbrica, el comportamiento de los datos no se diferencian de los datos correspondientes en una red ad hoc de radio cognitivo, ya que el comportamiento de los criterios utilizados es independiente del tipo de red inalámbrica. El escenario que se aplica a 802.11g utiliza 10 nodos con una potencia de transmisión de 15 dBm y una velocidad de transmisión de 11 Mbps. Los datos fueron recolectados en situaciones en que se establecieron 54 enlaces en 3 canales ortogonales entre nodos. El escenario que aplica la tecnología 802.11a se compone de 13 nodos con una potencia de transmisión de 15 dBm y una velocidad de transmisión de 6 Mbps en 78 enlaces diferentes con 13 canales ortogonales. Las especificaciones de estos escenarios y de la recolección de datos se detallan en Subramanian et al. [102] y son consideradas para analizar y definir los pesos de importancia en el caso 2.

  Inicialmente, las muestras se normalizaron para representar el conjunto de los factores principales y posteriormente obtener una matriz de correlación de los criterios para establecer los pesos de importancia. Tenga en cuenta que la descripción de la técnica de PCA se expone en el capítulo 2. Después del análisis de PCA utilizando la herramienta R [103] para calcular los pesos con base en las muestras, fueron ob-

tenidos los siguientes valores para los pesos de importancia de cada criterio. En el caso 1, se establecieron los pesos de 45 %, 29 % y 26 % para los criterios de potencia de recepción, potencia de transmisión y distancia, respectivamente. En el caso 2, se establecieron los porcentajes de pesos de 45 %, 25 %, 18 % y 12 % para los criterios de potencia de recepción, relación señal-ruido, ruido y velocidad de transmisión, respectivamente. Un resumen de los valores de pesos de importancia obtenidos para cada criterio se muestran en la Tabla 5.1. Para mostrar la importancia de un análisis idóneo de los pesos, los primeros resultados que se presentan en la sección 5.3 sobre la evaluación del esquema FLEXEUP no se aplica un análisis de los pesos de importancia. Los otros resultados se lograron mediante la aplicación de la técnica PCA para definir los pesos de importancia.

Cuadro 5.1: Porcentajes de pesos de importancia

Casos de estudio / Criterios	Caso 1 (%)	Caso 2 (%)
Potencia de recepción	45	45
Potencia de transmisión	29	
Distancia	26	
SNR (relación señal-ruido)		25
Ruido		18
Tasa de Transmisión		12
Total	100	100

La fase de cooperación del esquema FLEXEUP comienza con un intercambio de probabilidades preliminares entre el US y sus vecinos. Después de este intercambio, el esquema lleva a cabo una fusión de las probabilidades preliminares utilizando el teorema de Bayes para determinar la probabilidad final de la presencia de ataques de EUP. Para calcular la probabilidad final, $P_{n_i}(A|B)$, para un nodo dado n_i, el teorema de Bayes necesita la probabilidad final de un vecino n_j, denotado por $P_{n_j}(B|A)$. Como en una primera iteración esta probabilidad es desconocida, esta debe ser estimada o adivinada. Por lo tanto, la probabilidad estimada para $P_{n_j}(B|A)$, en la primera iteración, es definida como 0,5, lo que representa una probabilidad inicial neutral. Este valor se establece a través de las rigurosas simulaciones del esquema FLEXEUP, en las simulaciones se observo que un valor inicial para Bayes igual o cerca de 1,0 denota una alta tasa de falsos positivos, ocurrió lo contrario, cuando el valor inicial fue cerca o equivalente a 0,0, una alta tasa de falsos negativos se generó. En particular, cabe señalar que un valor neutral para el teorema de Bayes inicial óptima es de 0,5.

En las simulaciones, se consideran los siguientes porcentajes de nodos malintencionados: 10 %, 30 % y 50 % del total de USs en la red. Estos nodos actúan de forma malintencionada durante períodos aleatorios en la simulación. Además, es importante mencionar

que los nodos malintencionados tienen mecanismos cognitivos para detectar la presencia de un usuario primario a fin de no provocar colisiones o interferencias en las transmisiones primarias. Los resultados que se presentan son la media de 35 simulaciones para cada porcentaje de atacantes en diferentes escenarios, teniendo en cuenta ambos casos del esquema FLEXEUP. Además, los resultados se muestran con un intervalo de confianza del 90 %. La Tabla 5.2 resume los principales parámetros y los valores utilizados en las simulaciones.

Cuadro 5.2: Principales parametros de simulación

Parâmetros	Valor
Cantidad de nodos - usuarios secundarios (USs)	50, 100
Cantidad de usuarios primarios (UPs)	2
Porcentaje de nodos malintencionados (EUPs)	10, 30, 50 (%)
Tiempo de vida de la red	500 segundos
Área de movimentación	1000x1000 metros
Rayo de transmisión de los USs	250 metros
Rayo de transmisión de los UPs	1000 metros
Rayo de transmisión de los EUPs	250 hasta 1000 metros
Potencia de transmisión USs	24,5 dBm (0.2818 w)
Potencia de transmisión UPs	94 dBm (2511886,43 w)
Potencia de transmisión EUPs	24,5 até 94 dBm
Protocolo de ruteamiento	AODV

5.2. Métricas

Fueron empleados cuatro métricas para evaluar el esquema FLEXEUP. La primera métrica aborda la probabilidad de éxito del atacante en CRAHN. Las otras tres métricas consolidan los resultados obtenidos con la primera, además de inferir la eficacia del esquema FLEXEUP frente a la detección de ataques EUP. A continuación, se define cada uno de las métricas utilizadas.

1. La primera métrica mide el éxito del ataque en la CRAHN y es denominada de probabilidad de la presencia del ataque EUP (Pr). Ella cuantifica las probabilidades finales de los nodos que detectan un posible ataque a la red. La métrica Pr se define de acuerdo a la Ecuación 5.1 en que $P_{n_i}(A|B)$ representa la probabilidad de éxito de un ataque determinada por un nodo n_i y R la cantidad total detecciones de los atacantes realizada por el esquema FLEXEUP.

$$Pr = \frac{\sum_{i=1}^{|Ns|} P_{n_i}(A|B)}{|R|} \tag{5.1}$$

2. La segunda métrica muestra una variación de la primera y es llamada tasa de detección (T_k). Esta representa el impacto de las probabilidades vecinas en la probabilidad

individual de un nodo n_i. Para este propósito, se vio obligado a forzar la variación del valor k, que representa la cantidad de vecinos cooperadores, en 3, 6 y 10 con el fin de realizar el cálculo final de la probabilidad de la presencia de ataques de EUP. T_K se calcula según la Ecuación 5.2, donde $P_{n_j}(B), \mathbf{j} = 1, 2, 3, .., k$ representa la probabilidad preliminar compartida por **j**-ésimo vecino de n_i y k es la cantidad total de vecinos cooperadores.

$$T_k = \frac{\sum_{j=1}^{k} P_{n_j}(B)}{|k|} \tag{5.2}$$

3. La tercera métrica cuantifica la tasa de falsos positivos en la probabilidad de éxito del ataque. La tasa de falsos positivos (Tx_{fp}) determina la relación de la cantidad de veces que se ha identificado un ataque siendo este negativo. Esta métrica se calcula por la Ecuación 5.3, donde B significa el número total de detecciones en el esquema, en la forma de $B = (d, v)$, donde d representa la probabilidad de detección llevada a cabo por el esquema FLEXEUP y v es la condición real del nodo $n_i \in N_S$, donde $v = 1$ representa un nodo malintencionado y $v = 0$ un nodo legítimo.

$$Tx_{fp} = \frac{\sum Dp_i}{|B|} \forall i \in B \quad donde \quad Dp_i = \begin{cases} 1 \; se \; d_i = 1 \\ 0 \; se \; d_i \neq 0 \end{cases} \tag{5.3}$$

4. La cuarta métrica mide la tasa de falsos negativos (Tx_{fn}) que cuantifica las veces que los nodos no detectan la presencia de ataques EUP cuando estos realmente ocurren. Tx_{fn} se calcula según la Ecuación 5.4, donde B representa el número total de detecciones del esquema, en la forma de $B = (d, v)$, donde d representa la probabilidad de detección del esquema FLEXEUP y v es la condición real del nodo $n_i \in N_S$, donde $v = 1$ representa un nodo malintencionado y $v = 0$ representa un nodo legítimo.

$$Tx_{fp} = \frac{\sum Dn_i}{|B|} \forall i \in B \quad donde \quad Dn_i = \begin{cases} 0 \; se \; d_i = 1 \\ 1 \; se \; d_i \neq 0 \end{cases} \tag{5.4}$$

5.3. Resultados del desempeño del esquema FLEXEUP

En esta sección, se presenta una evaluación del esquema FLEXEUP en las CRAHNs bajo ataque EUP. Las métricas se aplican a cada escenario simulado, y los resultados obtenidos por el esquema FLEXEUP se comparan con los resultados de un esquema de monocritério. Tenga en cuenta que el esquema de monocritério utiliza apenas el criterio de la potencia de recepción de la señal, que es un criterio ampliamente estudiado y evaluado para detectar o mitigar los ataques EUP en los esquemas y análisis presentados en la

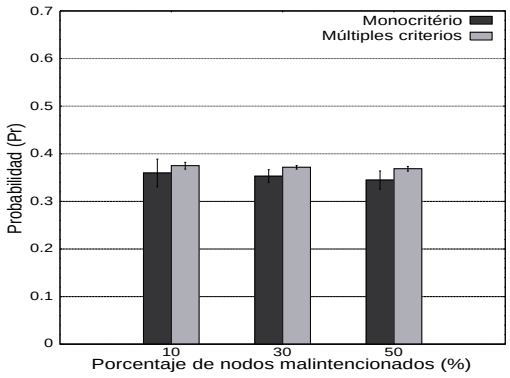
literatura. El esquema monocritério muestra dos fases, en la fase individual, se calcula la probabilidad de la presencia del ataque con base en la potencia de recepción. En la fase cooperativa, los nodos intercambian información para detectar el ataque EUP. Luego, cada nodo lleva a cabo un cálculo de la probabilidad final del éxito del ataque sobre la base de la información intercambiada. El esquema monocritério sigue los conceptos y las especificaciones de los esquemas presentados en la literatura y que fueron descritos en el Capítulo 3.

En las Figuras 5.1(a), 5.1(b) y 5.1(c), se muestran los resultados del esquema FLEXEUP en la detección de ataques. Para la obtención de estos resultados no se realizo ningún análisis con el fin de definir los pesos de importancia para los criterios. La figura 5.1(a), muestra los resultados del esquema FLEXEUP frente al esquema monocritério en su fase individual. En la figura 5.1(b), muestra el esquema FLEXEUP teniendo en cuenta sus dos fases. En la figura 5.1(c), se presenta la tasa de detección por vecinos cooperadores. En todos estos resultados nos dimos cuenta de una pequeña variación en la probabilidad de la presencia de la EUP ataque, esto puede ser debido a la ausencia de análisis de los pesos de importancia.

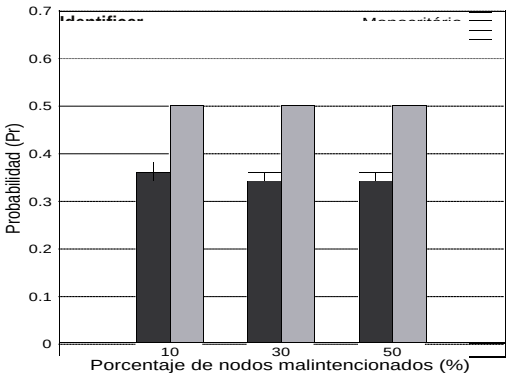
A continuación, se muestran los resultados de una evaluación de los pesos de importancia determinados por la técnica de PCA. Hacemos hincapié que para en el caso 1, los datos utilizados para evaluar los pesos de importancia se derivan a partir de simulaciones, y en el caso 2 los datos de los ensayos experimentales. Las Figuras 5.2(a) y 5.2(b) presentan los resultados con respecto a la métrica de la probabilidad de la presencia del ataque EUP (P_r), considerando sólo la primera fase del esquema FLEXEUP en presencia de nodos malintencionados. Las figuras muestran los resultados de los esquemas monocritério y múltiples criterios, siendo los resultados obtenidos por el esquema de múltiples criterios etiquetados como casos 1 y 2, como se definió anteriormente.

En la Figura 5.2(a), los resultados muestran una probabilidad preliminar de la presencia del ataque EUP en el análisis de múltiples criterios superior en todos los escenarios con respecto a la probabilidad preliminar obtenida por el análisis monocritério. El caso 1 tiene una ganancia de 16 %, 19 % y 18 % en relación al esquema monocritério en las tres variaciones de porcentajes de atacantes en la CRAHN, siendo la red constituida por un total de 50 nodos. Por otro lado, el caso 2 del esquema FLEXEUP muestra una ganancia de 19 %, 22 % y 25 % en comparación con el esquema de monocritério. Las variaciones de la probabilidad entre los dos casos del esquema FLEXEUP representa una ganancia en el caso 2del 3 % en comparación con el caso 1, esto determina que la elección de los criterios junto a la cantidad de criterios puede representar una ganancia significativa en la fase individual sin llevar a cabo la fase de cooperación.

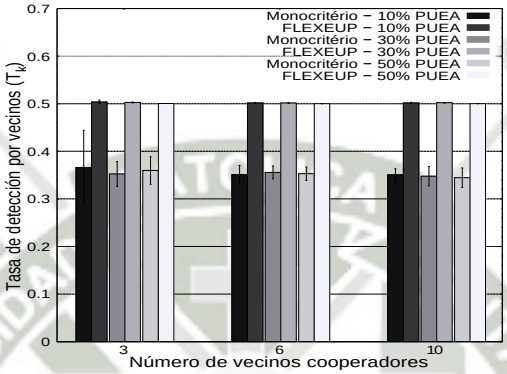
La Figura 5.2(b), presenta los resultados en un ambiente con 100 nodos dispuestos en la CRAHN. El caso 1 tuvo una ganancia de hasta un 20 % en las diferentes variaciones de atacantes en la red y en relación con el esquema monocritério. El caso 2 del FLEXEUP



(a) Fase individual



(b) FLEXEUP vs Monocritério

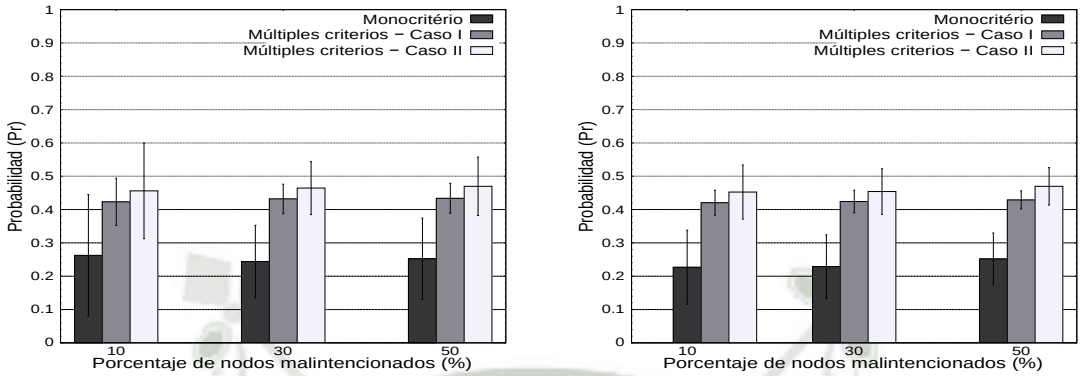


(c) Análisis de la cooperación

Figura 5.1: Esquema FLEXEUP sin análisis de pesos de importancia

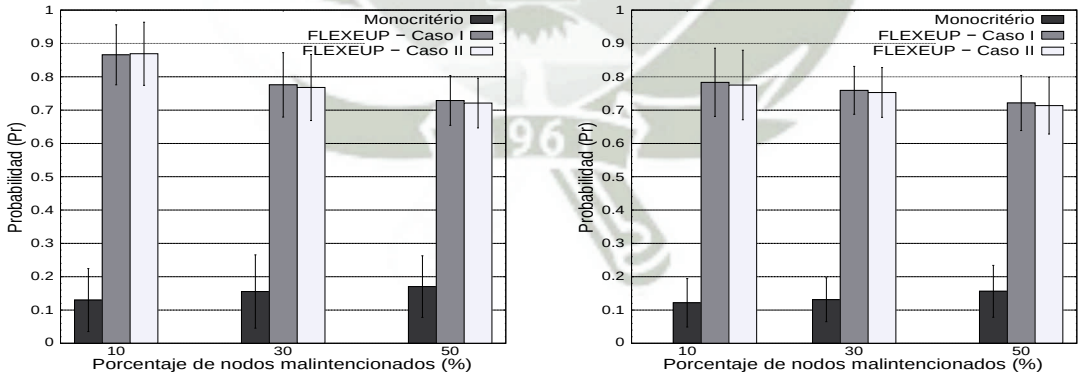
obtiene una ganancia de hasta un 23 % en comparación con el esquema monocritério. La variación entre los dos casos del esquema FLEXEUP es de hasta un 4 %. Estos resultados reflejan la estabilidad en la determinación del ataque en la fase individual y definen que el análisis de múltiples criterios determina una alta probabilidad de la presencia de ataque primario independientemente de la importancia de la cantidad de nodos en la red.

En la Figura 5.3(a), compara los resultados del esquemas FLEXEUP en sus dos casos de estudio frente al esquema monocritério cooperativo en un escenario con 50 nodos de la red. El caso 1 del esquema FLEXEUP tiene una ganancia de hasta un 77 % en comparación con el esquema de monocritério. El caso 2 obtiene una ganancia de hasta un 73 % en comparación con el esquema monocritério. Se observó que el esquema monocritério cooperativo presenta una reducción en la probabilidad de detección en contra del esquema monocritério individuala. Esto se debe a la unión de la información en un nodo representan el promedio de todas las probabilidades, y se basan sólo en un análisis de un único criterio para determinar la presencia del ataque EUP. Por otra parte, los dos casos del esquema FLEXEUP muestran una variación del 1 %, entre ellos, con esto demostramos que un análisis de múltiples criterios junto con un abordaje cooperativo con un análisis de fusión de la información usando el teorema de Bayes proporciona una alta probabilidad (Pr) de la presencia del ataque a EUP en las CRAHNs.



(a) Escenario con 50 nodos (b) Escenario con 100 nodos

Figura 5.2: Pr preliminar de los análisis de múltiples criterios y monocritério

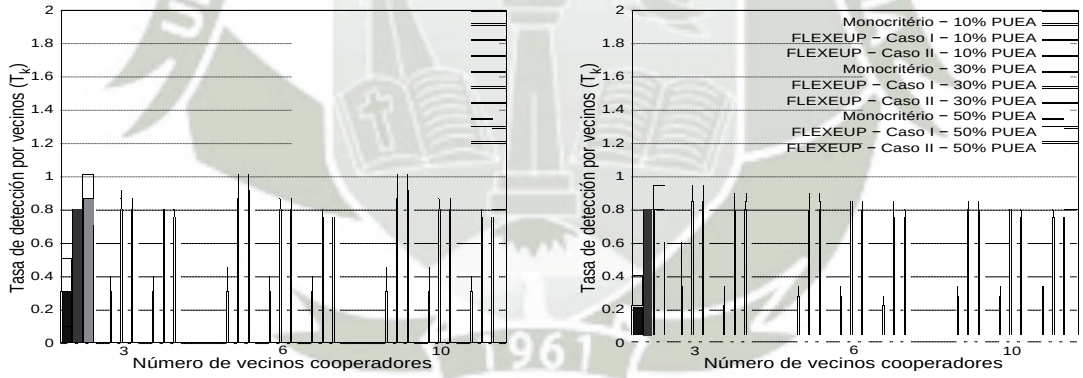


(a) Escenario con 50 nodos (b) Escenario con 100 nodos

Figura 5.3: Pr del esquema FLEXEUP vs esquema monocritério

La Figura 5.3(b) representa los resultados obtenidos con los dos casos del esquema FLEXEUP y el esquema monocritério cooperativo en un escenario con 100 nodos. Se observa que los resultados muestran el mismo comportamiento con respecto a los resultados que se muestran en la Figura 5.3(a). En el escenario con 100 nodos, el caso 1 del esquema FLEXEUP tiene una ganancia de hasta un 66 % al comparar con el esquema monocritério. El caso 2 resulta en un aumento del 65 % en comparación con el esquema monocritério, la variación entre los dos casos del esquema FLEXEUP es 1 %. Estos resultados demuestran que un análisis en múltiples criterios en un enfoque cooperativo proporciona una alta probabilidad de detectar la presencia de ataque EUP (Pr).

La Figura 5.4(a) presenta la tasa de detección por vecinos T_k obtenida por el esquema FLEXEUP y por esquema monocritério. En la evaluación de la cooperación tienen como referencia el número de nodos cooperadores comparado con el porcentaje de atacantes en la CRAHN. El esquema monocritério muestra una variación de aproximadamente un 4 % de probabilidad entre los escenarios con 3, 6 y 10 nodos cooperadores. Los dos casos del esquema FLEXEUP muestran una variación del 10 % y 15 % entre los escenarios con diferentes cantidades de nodos cooperadores. En la Figura 5.4(b) se muestra una variación de T_k en el esquema monocritério, lo que corresponde a un 9 % en escenarios con diferentes cantidades de nodos cooperadores. Por otro lado, las variaciones del esquema FLEXEUP representan un 11 % y 12 %, respectivamente.

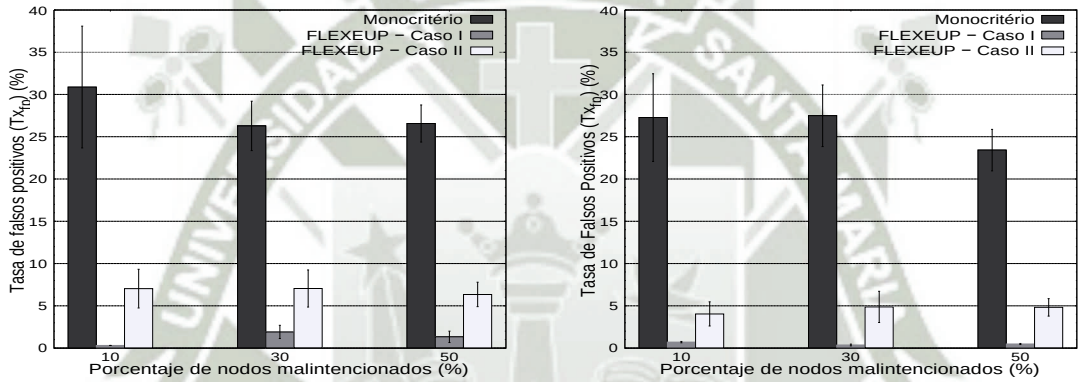


(a) Escenario con 50 nodos (b) Escenario con 100 nodos

Figura 5.4: T_k tasa de detección por cantidad de vecinos cooperadores

En las Figuras 5.4(a) y 5.4(b) se resalta que la probabilidad Pr muestra un aumento en ambos casos del esquema FLEXEUP en relación con el esquema monocritério. Esto refuerza la eficiencia del esquema FLEXEUP, donde podemos afirmar que un enfoque de cooperación con un análisis bayesiano ayuda a lograr un mejor rendimiento en términos de detección del ataque EUP. Por otra parte, se observa que la probabilidad Pr del esquema FLEXEUP tiene una pequeña variación debido al acceso aleatorio del ataque EUP, es decir, un usuario secundario no necesariamente monitora el canal que está siendo atacado, esto debido a la elección del canal por parte del usuario secundario.

El esquema FLEXEUP tiene una tasa baja de falsos positivos, como se muestra en las Figuras 5.5(a) y 5.5(b). En el escenario con 50 nodos y diferentes porcentajes de ataques EUP, que se muestra en la Figura 5.5(a), la tasa de falsos positivos en ambos casos del esquema FLEXEUP no es más que un 7 %, mientras que el esquema monocritério tiene una alta tasa de falsos positivos que alcanza el 30 %. En los resultados presentados en la Figura 5.5(b) con 100 nodos en la red, la Tx_{fp} de los dos casos del esquema FLEXEUP es sólo de 4 % al comparar con el esquema monocritério que llega a un 27 %. En los casos del esquema FLEXEUP el bajo porcentaje de falsos positivos se produce cuando el nodo detecta que un canal está siendo atacado, y en realidad esto no sucede. En entornos de simulación esto se produce cuando un usuario secundario monitorea un canal que está siendo utilizado por otro usuario secundario legítimo y están cerca el uno al otro. De este modo, el usuario secundario monitoriza el canal y realiza las mediciones de los valores en el canal y después el análisis concluye que se trata de un usuario primario.



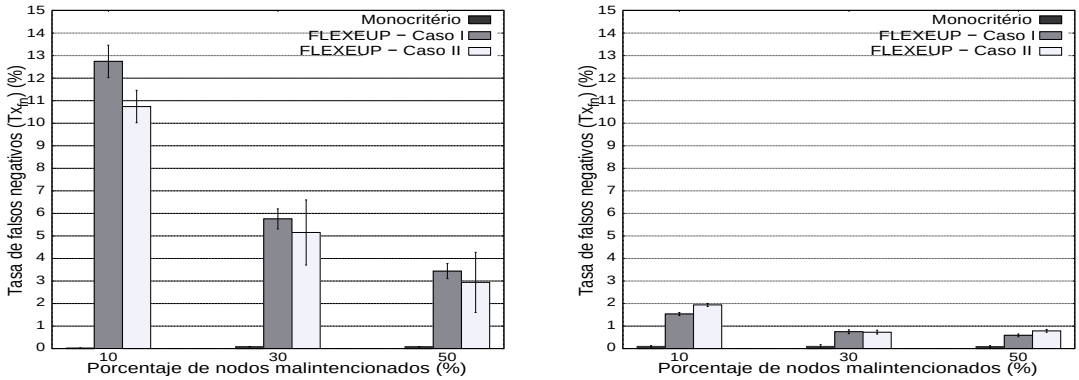
(a) Escenario con 50 nodos (b) Escenario con 100 nodos

Figura 5.5: Tx_{fp} en la detección de ataques EUPs

Por otro lado, la Tx_{fp} en el esquema monocritério presenta un alto porcentaje en los escenarios. Esto sucede por el mismo problema que es visto en el esquema FLEXEUP, y otro factor que puede afectar es la ausencia de un análisis de múltiples criterios, ya que su solución se basa en un único criterio. Por otra parte, la cooperación no muestra una mejora significativa en términos de reducción de esta tasa de falsos positivos.

El esquema FLEXEUP presenta una tasa de falsos negativos del 12 %, y esta disminuye a una tasa del 3 % en los diferentes casos, como se muestra en la Figura 5.6(a). La Tx_{fn} de 12 % puede suceder debido a los atacantes ocupan canales al azar, con algunos usuarios secundarios pueden presentar un retardo en el sensoriamento del canal en un momento dado y al momento siguiente el ataque puede migrar a otro canal porque un usuario primario inicio actividad en ese canal. Por lo tanto, los nodos que monitorean el canal detectan un usuario primario legítimo con las mismas características de un atacante.

También se puede generar un falso negativo debido al hecho de encontrar un usuario secundario monitoreando un canal de frecuencia que está siendo usado por un nodo ma-



(a) Escenario con 50 nodos

(b) Escenario con 100 nodos

Figura 5.6: Tx_{fn} en la detección de ataques EUPs

lintencionado, estando este atacante a una distancia considerable del nodo que monitorea el canal. Por tal motivo, algunos de los valores de los criterios analizados arrojan valores pequeños que pueden ser fácilmente tomados como valores de criterios de un usuario secundario legítimo cuando en realidad no lo es. En la Figura 5.6(b) la Tx_{fn} es menor al 4% y se reduce al 1% en los dos casos del esquema FLEXEUP. Por otro lado, el esquema monocritério siempre tiene una Tx_{fn} menor que el 1%. Sin embargo, podemos decir que el esquema FLEXEUP también tiene un mejor rendimiento en redes con una mayor cantidad de nodos.

5.4. Resumen

En este capítulo se presenta en análisis y resultados del esquema FLEXEUP. Se emplearon dos escenarios con diferentes cantidades de nodos y diferente porcentaje de atacantes. También se utilizaron dos casos de estudio del esquema FLEXEUP con diferentes cantidades y tipos de criterios. Además, se presentó una revisión de los pesos de importancia utilizando la técnica de PCA. Inicialmente, se presentan los resultados del esquema FLEXEUP sin evaluar pesos de importancia, a continuación, mostrar los resultados con esta evaluación. En los escenarios en que fue empleado el esquema FLEXEUP se muestra una eficiencia en la determinación de la presencia del ataque EUP, en comparación a un esquema monocritério que representa a los esquemas o análisis tratados en la literatura. Sin embargo, el funcionamiento del esquema FLEXEUP depende de la evaluación de los pesos de importancia para un correcto análisis de múltiples criterios en combinación con un enfoque de cooperación para lograr una alta probabilidad de presencia del ataque EUP en la CRAHN.

CONCLUSIONES

Las redes ad hoc redes de radio cognitivo (CRAHN, del inglés, Cognitive radio ad hoc networks) estan compuestas de dispositivos (nodos) que utilizan la tecnología de radio cognitivo. Esta tecnología es capaz de controlar y determinar las frecuencias de inactividad en el espectro. Basado en las mediciones y los conocimientos adquiridos a través de la historia de los acontecimientos pasados, cada nodo de manera inteligente puede elegir y reutilizar partes subutilizadas del espectro. Hay dos tipos de usuarios que comparten el espectro de radio, estos son llamados usuarios primarios y los usuarios secundarios. Siendo que los usuarios primarios tienen licencias de uso de las bandas y de mayor prioridad para acceder a ellas, mientras que los usuarios secundarios no tienen licencias, pero pueden utilizar las bandas cuando están ociosas.

Las CRAHNs son vulnerables a los ataques de emulación de usuario primario (EUP). Estos ataques son realizados por usuarios secundarios malintencionados. Estos usuarios imitan las características de los usuarios primarios legítimos con el fin de beneficiarse de la utilización del espectro. Además, estos ataques comprometen el uso de las bandas de frecuencia licenciadas, degradando el acceso al espectro a los usuarios secundarios legítimos.

En ese contexto, fue propuesto un esquema FLEXible de múltiples criterios para detectar ataques de Emulación de Usuario Primario en redes ad hoc de radio cognitivo, llamado FLEXEUP. El esquema FLEXEUP tiene como objetivo determinar La probabilidad de la presencia del ataque EUP, para esto el esquema considera los criterios comúnmente utilizados en una transmisión inalámbrica junto con un abordaje cooperativo. El esquema FLEXEUP presenta dos fases para determinar dicha probabilidad, estas son la fase individual y la fase cooperativa.

La fase individual del esquema FLEXEUP permite llevar a cabo la recolección de datos utilizando una técnica de detección de la energía en la función de sensoriamento. Posteriormente, los valores obtenidos se agrupan siguiendo los criterios de selección establecidos por el esquema FLEXEUP y son llevados a un análisis individual de múltiples criterios. Este análisis preliminar determina una probabilidad de éxito del ataque EUP calculada individualmente por cada nodo de red. La fase de la cooperación comienza con un intercambio de probabilidades preliminares entre nodos de la red. Enseguida, cada nodo realizará una fusión de la información, aplicando el teorema de Bayes y considerando las probabilidades preliminares intercambiadas. Esta fusión de las probabilidades determina la probabilidad final de la presencia del ataque EUP en la red ad hoc de radio cognitivo.

5.5. Conclusiones finales

El esquema FLEXEUP fue implementado y adicionado a los módulos de una CRAHN y se evaluó de la presencia de nodos malintencionados en la forma de ataques de emulación de usuario primario. Inicialmente, mostramos los resultados sin una definición de pesos de importancia. A continuación, se muestran los resultados de un análisis de pesos importancia definidos por la técnica PCA. Los resultados de la fase individual sin el análisis de pesos de importancia alcanzaron sólo una ganancia de 2.36 % en comparación con un esquema monocritério definido en la literatura. A continuación, los resultados en la fase cooperativa del esquema FLEXEUP con la definición de pesos de importancia mostraron una superioridad de hasta un 19 % en el primer caso, y hasta un 25 % en el segundo caso de estudio contra un esquema monocritério.

Los resultados alcanzados en la primera fase de los dos esquemas concluyen que un esquema para la detección de ataques EUP no puede basarse en un único criterio de detección, por el hecho de que estos atacantes pueden modificar sus características de transmisión en el espectro. Esto lleva a un esquema de detección monocritério sólo verifique una de sus características o criterios, dejando de lado los demás criterios que pueden influir en la detección. Además, se puede generar una gran tasa de error de detección y en consecuencia un alta tasa de falsos positivos y falsos negativos. Para contrarrestar este problema los resultados del esquema FLEXEUP en la primera fase muestran que el análisis de múltiples criterios genera una detección óptima de la presencia de ataques EUP, teniendo en cuenta el hecho de que muchos de estos criterios se aplican en una transmisión inalámbrica común y además pudiendo llegar a un consenso entre sí para determinar si existe una presencia malintencionada o no. Tal como puede observarse, los resultados muestran que FLEXEUP con un análisis de múltiples criterios, inicialmente sin una evaluación de los pesos de importancia el esquema FLEXEUP muestra una superioridad al esquema monocritério, y esta superioridad se refuerza con una evaluación correcta de pesos de importancia la cual hace que la detección del ataque EUP sea mucho mejor, y asi eliminar los altos índices de falsos positivos generados por el esquema monocritério. Con esto, abarcamos los objetivos especificos planteados.

Por otra parte, el esquema FLEXEUP también se evaluó considerando las dos fases (individual y cooperativa). En esta revisión, los resultados obtenidos en el esquema FLEXEUP sin evaluar pesos de importancia muestran una ganancia de 15.56 % en comparación con un esquema monocritério. Sin embargo, los resultados con el análisis de pesos de importancia por la técnica de PCA representan una ganancia de hasta 77 % y 65 % en el primero y segundo caso, respectivamente. Los resultados obtenidos mediante la aplicación de las dos fases en el esquema FLEXEUP refuerza los resultados obtenidos en la fase individual. Como se ve, el esquema monocritério sigue un enfoque de cooperación, pero sólo tiene en cuenta un único criterio, que puede conducir a una detección

errónea y generar altas tasas de falsos positivos y negativos. En el esquema FLEXEUP se considera el análisis de múltiples criterios, junto con la correcta evaluación de los pesos de importancia realizadas en la primera fase y agrega un sentido de cooperación entre los nodos de la red que lleva a corregir detecciones erróneas de los nodos y disminuir las tasas de falsos positivos y negativos que se logra en el esquema monocritério.

Por lo tanto, llegamos a la conclusión de que el principal objetivo de este trabajo fue alcanzado, el cual consiste en la identificación de la presencia del ataque EUP en la CRAHN. Este objetivo se consigue mediante la aplicación del análisis de múltiples criterios definidos por el método NWAUF, junto con una evaluación de los pesos de importancia definidos por la técnica PCA, además de representar un enfoque cooperativo juntamente con un análisis de fusión de información. Este esquema utilizo cuatro procedimientos principales y se dividieron en dos fases para su óptimo desempeño en la detección de ataques EUP. Cada uno de estos procedimientos mejora aún más la detección, lo que hace un esquema eficaz y eficiente para la determinación de la presencia de los ataques EUP en las CRAHNs.

5.6. Recomendaciones y trabajos futuros

Como recomendaciones y trabajos futuros se considera lo siguiente:

- Evaluar el comportamiento del esquema FLEXEUP en escenarios con nodos móviles.
- Evaluar el consumo de energía en cada uno de los nodos que conforman la red.
- Con las recomendaciones anteriores se pretenden realizar una utilización de escenarios más realistas.
- Otras consideraciones para el trabajo futuro es el análisis del coste computacional y la sobrecarga de red que puede ocasionar el esquemas FLEXEUP en la red ad hoc de radio cognitivo.

ANEXO A: GLOSARIO DE ABREVIATURAS Y SIGLAS

3D-CTMC	Three Dimensional Continuous Time Markov Chain
MTC	Ministerio de Transportes y Comunicaciones
AODV	Ad hoc On Demand distance Vector routing protocol
CRAHN	Cognitive Radio Ad Hoc Network
DoS	Denial of Service
DDT	Distance Difference Teste
DTR	Distance Ratio Test
EUP	Emulación de Usuario Primario
FCC	Federal Communications Commission
FDOA	Frequency Difference Of Arrival
LocDef	Localization-based Defense
MCDA	Multi-Criteria Decision Analysis
NEAT	NEighbor AssisTed Spectrum Decision)
NS-2	Network Simulator 2
NWAUF	Normalized Weighted Additive Utility Function
PCA	Principal Component Analysis
QoS	Quality of Service
RC	Rádio Cognitivo
TDOA	Time Difference Of Arrival
UP	Usuario Primario
US	Usuario Secundario
WSPRT	Walds Sequential Probability Ratio Test

ANEXO B: NOTACIÓN

N_{UP}	Conjunto de usuarios primarios
N_S	Conjunto de usuarios secundarios
N_{SL}	Conjunto de usuarios secundarios legítimos
N_{SB}	Conjunto de usuarios secundarios malintencionados
n_i	usuario secundario
n_j	usuario secundario vecino de n_i
i-ésimo	Índice que representa un usuario secundario arbitrario
j-ésimo	Índice que representa un usuario secundario vecino arbitrario
$P_{n_i}(A)$	Probabilidad preliminar calculada por el nodo n_i
$P_{n_j}(B)$	Probabilidad preliminar calculada por el vecino n_j
$P_{n_i}(A\|B)$	Probabilidad final calculada por el nodo n_i
$P_{n_j}(B\|A)$	Probabilidad final calculada por el vecino n_j
S	Conjunto de criterios
W	Conjunto de pesos de importancia para los criterios
MIN e MAX	Conjunto de valores mínimos y máximos
Pr	Probabilidad de la presencia de ataque
T_k	Tasa de detección por vecinos cooperadores
Tx_{fp}	Tasa de falsos positivos
Tx_{fn}	Tasa de falsos negativos

BIBLIOGRAFÍA

[1] I. Akyildiz, W. Lee, M. Vuran, and S. Mohanty. A survey on spectrum management in cognitive radio networks. IEEE Communications Magazine, 46(4):40 –48, Abril 2008.

[2] Opsitel. División del espectro en el Perú, último acesso: Junio 2013. http://www.osiptel.gob.pe/WebSiteAjax/.

[3] Federal Communication Commision Report FCC. Spectrum policy task force report, no. 02.2135, Noviembre 2002.

[4] G. Staple and K. Werbach. The end of spectrum scarcity [spectrum allocation and utilization]. IEEE Spectrum, 41(3):48 – 52, Marzo 2004.

[5] D. Cabric, S.Mishra, D. Willkomm, R. Brodersen, and A. Wolisz. A cognitive radio approach for usage of virtual unlicensed spectrum. In IST Mobile Wireless Communications Summit, Junio 2005.

[6] Federal Communication Commision Report FCC. Facilitating opportunities for flexible, efficient, and reliable spectrum use employing cognitive radio technologies, no. 03.108, Noviembre 2003.

[7] M. Sousa, R. Lopes, W. Lopes, and M. Alencar. Redes cognitivas um novo paradigmas para as comunicações sem fio. In Simpósio Brasileiro de Redes de Computadores e Sitemas Distribuídos (SBRC), Mayo 2010.

[8] Y.-C. Liang, A. Hoang, and H.-H. Chen. Cognitive radio on TV bands: A new approach to provide wireless connectivity for rural areas. Wireless Communications, 15(3):16–22, 2008.

[9] D. Cabric, S. Mishra, and R. Brodersen. Implementation issues in spectrum sensing for cognitive radios. In Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, volume 1, pages 772 – 776, Noviembre 2004.

[10] W. Lee and I. Akyldiz. A spectrum decision framework for cognitive radio networks. IEEE Transactions on Mobile Computing, 10(2):161 –174, Febrero 2011.

[11] S. Tang and B. Mark. Modeling an opportunistic spectrum sharing system with a correlated arrival process. In IEEE Wireless Communications and Networking Conference (WCNC), pages 3297–3302, Abril 2008.

[12] H. Arslan. Cognitive Radio, Software Defined Radio, and Adaptive Wireless Systems (Signals and Communication Technology). Springer-Verlag New York, Inc., Secaucus, EUA, 2007.

[13] C. Haro and L. Giupponi. Radio y redes cognitivas. Technical report, AEI eMOV Plataforma Tecnológica Española de Comunicaciones Inalambricas, Marzo 2010.

[14] J. Mitola and G. Maguire. Cognitive radio: making software radios more personal. IEEE Personal Communications, 6(4):13–18, 1999.

[15] K.-C. Chen, Y.-J. Peng, N. Prasad, Y.-C. Liang, and S. Sun. Cognitive radio network architecture: part I – general structure. In International Conference on Ubiquitous Information Management and Communication (ICUIMC), pages 114 –119, New York, EUA, 2008. ACM.

[16] I. Akyildiz, W. Lee, M. Vuran, and S. Mohanty. Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey. Computer networks journal (ELSEVIER), 50:2127– 2159, Septiembre 2006.

[17] Z. Jin, S. Anand, and K. Subbalakshmi. Detecting primary user emulation attacks in dynamic spectrum access networks. In IEEE International Conference on Communications (ICC), pages 2749– 2753, 2009.

[18] W. Webb. On using white space spectrum. IEEE Communications Magazine, 50(8):145 –151, Agosto 2012.

[19] L. Giupponi and A. Perez-Neira. Fuzzy-based spectrum handoff in cognitive radio networks. In Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), pages 1 –6, Mayo 2008.

[20] B. Ishibashi, N. Bouabdallah, and R. Boutaba. QoS performance analysis of cognitive radio-based virtual wireless networks. In IEEE Conference on Computer Communications (INFOCOM), pages 2423 –2431, Abril 2008.

[21] A. Yau, P. Komisarczuk, and P. Teal. C2net: A cross-layer quality of service (QoS) architecture for cognitive wireless ad hoc networks. Australasian Telecommunication Networks and Applications Conference, pages 306–311, 2008.

[22] S. Anand, Z. Jin, and K. Subbalakshmi. An analytical model for primary user emulation attacks in cognitive radio networks. In IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), pages 1–6, Octubre 2008.

[23] O. León, J. Hernández-Serrano, and M. Soriano. A new cross-layer attack to TCP in cognitive radio networks. In IEEE Second International Workshop on Cross Layer Design (IWCLD), Junio 2009.

[24] T. Clancy and N. Goergen. Security in cognitive radio networks: Threats and mitigation. In Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), pages 1 –8, Mayo 2008.

[25] O. León, J. Hernández-Serrano, and M. Soriano. Securing cognitive radio networks. International Journal Communication Systems, 23(5):633–652, 2010.

[26] Z. Jin, S. Anand, and K. Subbalakshmi. NEAT: A neighbor assisted spectrum decisionprotocol for resilience against primary user emulation attacks. Relatório técnico, 2010.

[27] O. León, J. Hernández-Serrano, and M. Soriano. Cooperative detection of primary user emulation attacks in CRNs. Computer Networks, 2012.

[28] R. Chen and J. Park. Ensuring trustworthy spectrum sensing in cognitive radio networks. In IEEE Workshop on Networking Technologies for Software Defined Radio Networks, pages 110 –119, Septiembre 2006.

[29] R. Chen, J. Park, and J. Reed. Defense against primary user emulation attacks in cognitive radio networks. IEEE Journal on Selected Areas in Communications, 26(1):25–37, Enero 2008.

[30] H. Li and Z. Han. Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, part I: Known channel statistics. IEEE Transactions on Wireless Communications, 9(11):3566 –3577, Noviembre 2010.

[31] S. Chen, K. Zeng, and P. Mohapatra. Hearing is believing: Detecting mobile primary user emulation attack in white space. In IEEE Conference on Computer Communications (INFOCOM), pages 36 –40, Abril 2011.

[32] Z. Jin, S. Anand, and K. Subbalakshmi. Robust spectrum decision protocol against primary user emulation attacks in dynamic spectrum access networks. In IEEE Global Telecommunications Conference (GLOBECOM), pages 1–5, 2010.

[33] C. Chen, H. Cheng, and Y.-D. Yao. Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack. IEEE Wireless Communications, 10(7):2135 –2141, Julio 2011.

[34] A. Min, K.-H. Kim, and K. Shin. Robust cooperative sensing via state estimation in cognitive radio networks. In IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), pages 185 –196, Mayo 2011.

[35] Z. Jin, S. Anand, and K. Subbalakshmi. Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis esting. Mobile Computing and Communications Review (SIGMOBILE), 13:74–85, Septiembre 2009.

[36] M. Di Felice, K. Chowdhury, W. Kim, A. Kassler, and L. Bononi. End-to-end protocols for cognitive radio ad hoc networks: An evaluation study. Performance Evaluation, 68(9):859 – 875, 2011.

[37] Federal Communication Commision Report FCC. Frequency spectrum allocation chart in united sated, http://www.ntia.doc.gov/osmhome/allochrt.pdf, Octubre 2003.

[38] C. Chen. Investigation of Primary User Emulation Attack in Cognitive Radio Networks. Tese de doutorado, Faculty of the Stevens Institute of Technology, Hoboken, EUA, 2011.

[39] B. Ealey. Primary user emulation attacks in cognitive radio - an experimental demonstration and analysis. Dissertação de mestrado, The University of Tennessee, Knoxville, EUA, 2011.

[40] T. Yucek and H. Arslan. A survey of spectrum sensing algorithms for cognitive radio applications. IEEE Communications Surveys Tutorials, 11(1):116 –130, Abril 2009.

[41] D. Arianandа, M. Lakshmanan, and H. Nikoo. A survey on spectrum sensing techniques for cognitive radio. In International Workshop on Cognitive Radio and Advanced Spectrum Management (CogART), pages 74 –79, Mayo 2009.

[42] E. Axell, G. Leus, and E. Larsson. Overview of spectrum sensing for cognitive radio. In 2nd International Workshop on Cognitive Information Processing (CIP), pages 322 –327, Junio 2010.

[43] Y. Ge, Y. Sun, S. Lu, and E. Dutkiewicz. Adsd: An automatic distributed spectrum decision method in cognitive radio networks. In First International Conference on Future Information Networks (ICFIN), pages 253 –258, Octubre 2009.

[44] M. Kaplan and F. Buzluca. A dynamic spectrum decision scheme for heterogeneous cognitive radio networks. In 24th International Symposium on Computer and Information Sciences (ISCIS), pages 697 –702, Septiembre 2009.

[45] B. Canberk, I. Akyildiz, and S. Oktug. A qos-aware framework for available spectrum characterization and decision in cognitive radio networks. In IEEE 21st International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), pages 1533 –1538, Septiembre 2010.

[46] W. Lee and I. Akyldiz. A spectrum decision framework for cognitive radio networks. IEEE Transactions on Mobile Computing, 10(2):161 –174, Febrero 2011.

[47] D. Niyato and E. Hossain. Market-equilibrium, competitive, and cooperative pricing for spectrum sharing in cognitive radio networks: Analysis and comparison. IEEE Transactions on Wireless Communications, 7(11):4273 –4283, Noviembre 2008.

[48] R. Dubey and S. Sharma. Distributed shared spectrum techniques for cognitive wireless radio networks. In International Conference on Computational Intelligence and Communication Networks (CICN), pages 259 –264, Noviembre 2010.

[49] R. Zhou, X. Li, V. Chakravarthy, and Z. Wu. Spectrum mobility demonstration of smse based overlay cognitive radio via software defined radio. In New Frontiers in Dynamic Spectrum Access Networks (DySPAN), pages 668 –669, Mayo 2011.

[50] I. Christian, S. Moh, I. Chung, and J. Lee. Spectrum mobility in cognitive radio networks. IEEE Communications Magazine, 50(6):114 –121, Junio 2012.

[51] I. Akyildiz, W. Lee, and K. Chowdhury. Spectrum management in cognitive radio ad hoc networks. IEEE Network, 23(4):6 –12, Julio-Agosto 2009.

[52] L. Wang and C. Wang. Spectrum management techniques with qos provisioning in cognitive radio networks. In IEEE International Symposium on Wireless Pervasive Computing (ISWPC), pages 116 –121, Mayo 2010.

[53] G. Salami, O. Durowoju, A. Attar, O. Holland, R. Tafazolli, and H. Aghvami. A comparison between the centralized and distributed approaches for spectrum management. IEEE Communications Surveys Tutorials, 13(2):274 –290, Abril 2011.

[54] K. Du, M. Swamy, and Q. Ni. A dynamic spectrum access scheme for cognitive radio networks. In Canadian Conference on Electrical and Computer Engineering (CCECE), pages 450 –454, Mayo 2009.

[55] R. Mahapatra and E. Strinati. Interference-aware dynamic spectrum access in cognitive radio network. In IEEE 22nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), pages 396 –400, Septiembre 2011.

[56] X. Zhang and C. Li. The security in cognitive radio networks: a survey. In International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly (IWCMC), pages 309–313, 2009.

[57] A. Araujo, J. Blesa, E. Romero, and D. Villanueva. Security in cognitive wireless sensor networks. challenges and open problems. EURASIP J. Wireless Comm. and Networking, page 48, 2012.

[58] N. Shankar, C. Cordeiro, and K. Challapali. Spectrum agile radios: utilization and sensing architectures. In IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), pages 160 –169, Noviembre 2005.

[59] Y. Yuan, P. Bahl, R. Chandra, P. Chou, J. Ferrell, T. Moscibroda, S. Narlanka, and Y. Wu. Knows: Cognitive radio networks over white spaces. In IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), pages 416 –427, Abril 2007.

[60] P. Pawelczak, G. Janssen, and R. Venkatesha Prasad. Performance measures of dynamic spectrum access networks. In IEEE Global Telecommunications Conference (GLOBECOM), Noviembre 2006.

[61] M. Subhedar and G. Birajdar. Spectrum sensing techniques in cognitive radio networks: A survey. International Journal of NextGeneration Networks, 3(2):37–51, 2011.

[62] D. Cabric, A. Tkachenko, and R. Brodersen. Experimental study of spectrum sensing based on energy detection and network cooperation. In ACM International Workshop on Technology and Policy for Accessing Spectrum (TAPAS), 2006.

[63] H. Tang. Some physical layer issues of wide-band cognitive radio systems. In IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), pages 151 –159, Noviembre 2005.

[64] J. Proakis. Digital Communications. McGraw-Hill Science/Engineering/Math, 4 edition, Agosto 2000.

[65] R. Tandra and A. Sahai. Fundamental limits on detection in low snr under noise uncertainty. In International Conference on Wireless Networks, Communications and Mobile Computing, volume 1, pages 464 – 469, Junio 2005.

[66] N. Khambekar, L. Dong, and V. Chaudhary. Utilizing ofdm guard interval for spectrum sensing. In IEEE Wireless Communications and Networking Conference (WCNC), pages 38 –42, Marzo 2007.

[67] W. Gardner. Exploitation of spectral redundancy in cyclostationary signals. IEEE Signal Processing Magazine, 8(2):14 –36, Abril 1991.

[68] A. Fehske, J. Gaeddert, and J. Reed. A new approach to signal classification using spectral correlation and neural networks. In IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), pages 144 –150, Noviembre 2005.

[69] M. Ghozzi, F. Marx, M. Mischa, and J. Palicot. Cyclostatilonarilty-based test for detection of vacant frequency bands. In Cognitive Radio Oriented Wireless Networks and Communications, pages 1 –5, Junio 2006.

[70] S. Mishra, S. Brink, R. Mahadevappa, and R. Brodersen. Cognitive technology for ultra-wideband/wimax coexistence. In IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), pages 179 –186, Abril 2007.

[71] D. Cabric, A. Tkachenko, and R. Brodersen. Spectrum sensing measurements of pilot, energy, and collaborative detection. In Military Communication Conference (MILCOM), Octubre 2006.

[72] A. Ghasemi and E. Sousa. Asymptotic performance of collaborative spectrum sensing under correlated log-normal shadowing. IEEE Communications Letters, 11(1):34 –36, Enero 2007.

[73] Efficient Signaling of Spectral Resources in Spectrum Pooling Systems, Holanda, Noviembre 2003.

[74] C. Guo, T. Zhang, Z. Zeng, and C. Feng. Investigation on spectrum sharing technology based on cognitive radio. In International Conference on Communications and Networking in China (ChinaCom), pages 1 –5, Octubre 2006.

[75] J. Perez-Romero, O. Salient, R. Agusti, and L. Giupponi. A novel on-demand cognitive pilot channel enabling dynamic spectrum allocation. In IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), pages 46 –54, Abril 2007.

[76] M. Buddhikot, P. Kolodzy, S. Miller, K. Ryan, and J. Evans. Dimsumnet: new directions in wireless networking using coordinated dynamic spectrum. In IEEE International Symposium on World of Wireless Mobile and Multimedia Networks (WoWMoM), pages 78 – 85, Junio 2005.

[77] P. Pawelczak, C. Guo, R. Venkatesha Prasad, and R. Hekmat. Clusterbased spectrum sensing architecture for opportunistic spectrum access networks. Technical report, IEEE Vehicular Technology Conference (VTC), 2006.

[78] R. Keeney. Decision analysis: An overview. Operations Research, 30(5), 1982.

[79] M. Marttunen. Interactive Multi-Criteria Decision Analysis in the Collaborative Management of Watercourses. Tese de doutorado, Aalto University School of Science, Espoo, Finlândia, Mayo 2011.

[80] L. Xu and J.-B. Yan. Introduction to Multi-Criteria Decision Making and the Evidential Reasoning Approach. Tese de doutorado, University of Manchester Institute of Science and Technology, Mayo 2001.

[81] B. Malakooti, I. Thomas, S. Tanguturi, S. Gajurel, and H. Kim. Multiple criteria network routing with simulation results. Industrial Engineering Research Conference (IERC), 2006.

[82] T. Saaty. The analytic hierarchy process. McGraw Hill, 1980.

[83] R. Benayoun, B. Roy, and N. Sussman. Manual de reference du programme electre. Note De Synthese et Formaton, 1966.

[84] X. Wang and E. Triantaphyllou. Ranking irregularities when evaluating alternatives by using some electre methods. Omega, 36(1):45 – 63, Marzo 2008.

[85] S. Gajurel and B. Malakooti. Re-configurable antenna & transmission power for location aware manet routing with multiple objective optimization. Journal of Networks (JNW), 3(3):11–18, 2008.

[86] B. Malakooti and I. Thomas. A distributed composite multiple criteria routing using distance vector. In International Conference on Networking, Sensing and Control (ICNSC), pages 42 –47, 2006.

[87] Raj Jain. The Art of Computer Systems Performance Analysis. John Wiley and Sons, 1th edition, 1991.

[88] I.T. Jolliffe. Principal Component Analysis. Springer Series in Statistics. Springer, 2002.

[89] W. Liang-chen, Z. Xue-feng, and W. Hui. Method of synthetic evaluation based on the principal component analysis and entropy weight. In International Conference on Computer Application and System Modeling (ICCASM), volume 8, pages V8–312 –V8–315, Octubre 2010.

[90] Z. Hui and Y. Honggeng. Application of weighted principal component analysis in comprehensive evaluation for power quality. In IEEE Power Engineering and Automation Conference (PEAM), volume 3, pages 369 –372, Septiembre 2011.

[91] M. Triola. Elementary Statistics. Addison Wesley, 11 edition.

[92] E. Nakamura, A. Loureiro, and A. Frery. Information fusion for wireless sensor networks: Methods, models, and classifications. ACM Comput. Surv., 39(3), Septiembre 2007.

[93] St. Andrews. Bayes. School of Mathematics and Statistics, University of St Andrews, Escócia, 2003.

[94] C. Brown. Bayes'Theorem and the Philosophy of Science. 2005.

[95] E. Medova. Bayesian Analysis and Markov Chain Monte Carlo Simulation. John Wiley Sons, Ltd, 2008.

[96] C. Zhao, W. Wang, L. Huang, and Y. Yao. Anti-pue attack based on the transmitter fingerprint identification in cognitive radio. In 5th International Conference on Wireless Communications, Networking and Mobile Computing (WiCom), pages 1 –5, Septiembre 2009.

[97] Z. Jin, S. Anand, and K. P. Subbalakshmi. Performance analysis of dynamic spectrum access networks under primary user emulation attacks. In IEEE Global Telecommunications Conference (GLOBECOM), pages 1–5, USA, Miami, Florida, Diciembre 2010.

[98] L. Huang, L. Xie, H.n Yu, W. Wang, and Y. Yao. Anti-pue attack based on joint position verification in cognitive radio networks. In International Conference on-Communications and Mobile Computing (CMC), volume 2, pages 169 –173, Abril 2010.

[99] N.T. Nguyen, R. Zheng, and Z. Han. On identifying primary user emulation attacks in cognitive radio systems using nonparametric bayesian classification. Signal Processing, IEEE Transactions on, 60(3):1432 –1445, Marzo 2012.

[100] A. Fragkiadakis, E. Tragos, and I. Askoxylakis. A survey on security threats and detection techniques in cognitive radio networks. IEEE Communications Surveys Tutorials, (99):1 – 18, 2012.

[101] CRAWDAD. Community Resource for Archiving Wireless Data At Dartmouth, último acesso: Agosto 2012. http://crawdad.cs.dartmouth.edu/.

[102] A. Subramanian, J. Cao, Ch. Sung, and S. Das. Understanding channel and interface heterogeneity in multi-channel multi-radio wireless mesh networks. In Proceedings of the 10th International Conference on Passive and Active Network Measurement, pages 89–98, Berlin, Heidelberg, 2009. Springer-Verlag.

[103] The R Project for Statistical Computing, último acesso: Agosto 2012. http://www.r-project.org/.