4. Redes Cognitivas

La convergencia tecnológica de las redes de comunicación hacia arquitecturas IP es un proceso que está cambiando profundamente en el panorama de las telecomunicaciones, afectando a sectores tales como; sociedad e industria, por mencionar algunos. Como consecuencia de estos cambios, surgen nuevos competidores pero también se crean nuevas oportunidades. Los operadores de telecomunicaciones no pueden permanecer impasibles y deben redefinir su papel en la nueva cadena de valor que les garantice no ser marginados, para que de este modo, la rentabilidad de sus negocios se mantenga a flote.

La rápida evolución de las redes inalámbricas que utilizan bandas del espectro no reguladas (sin licencia), es una oportunidad para bajar los costos de acceso de las redes inalámbricas. De este modo, se cree, que en los próximos años los operadores móviles deberán enfrentarse a un nuevo problema derivado de la operación de un entorno diverso y heterogéneo de tecnologías inalámbricas.

Para solucionar este problema se estudian dos posibles topologías que no son excluyentes entre sí:

- Las redes cooperativas, las cuales, trabajan mediante la operación conjunta de las redes de acceso entre varios operadores.
- Las redes cognitivas, que utilizan capacidades de auto configuración para adaptarse dinámicamente a la demanda, ya que estas, consiguen responder a las necesidades de un usuario en especifico, dentro de las políticas definidas por el operador, al tiempo que optimizan los recursos generales de la red.

La principal desventaja de las redes cooperativas radica en la gestión compartida entre las redes y en la interdependencia entre operadores (que a la vez son competidores), por lo que las redes cognitivas se presentan como la gran esperanza para el sector para gestionar redes a un costo aceptable. Las redes cognitivas tienen un proceso cognitivo con el cual pueden determinar cuáles son las condiciones actuales de la red, para así, planificar, decidir y actuar. La red puede aprender de estas adaptaciones, para tomar decisiones futuras, teniendo en cuenta a los objetivos finales. Estas redes, son también conocidas como (CogNet), y se utilizan para desarrollar protocolos de comunicación inalámbrica. El surgimiento de estas redes es gracias a los avances de la microelectrónica, ya que ahora es posible incluir una gran capacidad de procesamiento en dispositivos muy pequeños, donde antes era impensable debido a la falta de espacio y al costo. Esto permite sustituir componentes de hardware por software, permitiendo manipular a los receptores sin incrementar el precio de los dispositivos.

Las redes cognitivas se basan en la información procedente de los nuevos receptores modificados en software para conocer el estado de la red en tiempo real, lo que aumentará su capacidad adaptativa y las dotará de una gran agilidad. Una red de este tipo, podría funcionar por ejemplo como una red de difusión para difundir una alerta a la población, en este caso el teléfono móvil se comportaría como una radio FM, para luego transformarse en una red de grupo cerrado para los servicios de emergencia.

Las redes cognitivas trabajan en el nivel físico de la pila de protocolos, manejando las frecuencias de emisión y los parámetros de modulación.

4.1. Arquitectura de las Redes de Radio Cognitiva

Para poder implementar una red cognitiva, se debe conocer su arquitectura, es decir, los componentes que necesita, ya que estos serán útiles para el desarrollo de protocolos de comunicación, los cuales se describen a continuación.

4.1.1. Componentes de la red

Los componentes de la arquitectura de red de la Radio Cognitiva, se pueden clasificar en dos grupos: la red primaria y la red de CR (Radio Cognitiva) ver Figura 1.
La red primaria (red con licencia) se conoce como una red existente, donde los principales usuarios tienen una licencia para operar en una determinada banda del espectro. Si las redes primarias tienen una infraestructura, las actividades de los usuarios principales son controladas a través de las estaciones base primaria. Debido a su prioridad de acceso al espectro, las operaciones de los usuarios primarios no deben verse afectadas por los usuarios sin licencia. La red de CR, también llamada red dinámica de acceso al espectro, red secundaria, o red sin licencia, como su nombre lo dice, no cuenta con una licencia para operar en una banda deseada. Por lo tanto, se requiere de una funcionalidad adicional de los usuarios de CR para compartir la banda del espectro con licencia. Las redes de CR también pueden ser equipadas con estaciones base de radios Cognitivas, la cual proporciona conexión a los usuarios de CR. Por último, las redes de CR pueden incluir agentes de espectro, los cuales desempeñan un papel en la distribución de los recursos del espectro entre las diferentes redes de CR.

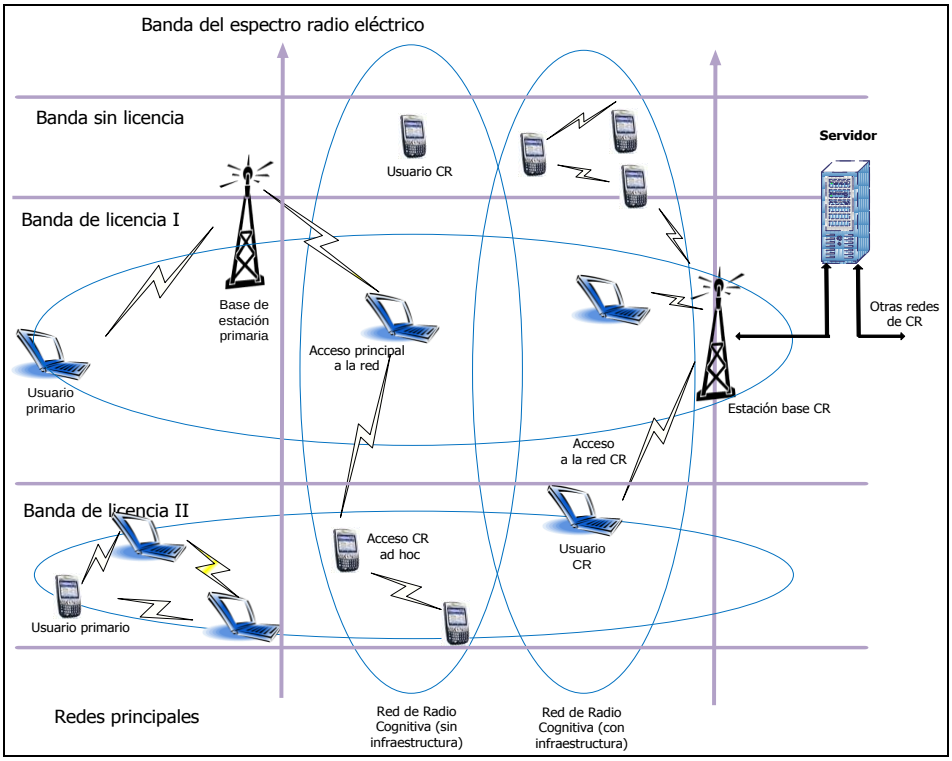

Figura 1. Arquitectura de las redes de radio cognitiva

Heterogeneidad del Espectro

Los usuarios de CR, son capaces de acceder, tanto a las partes del espectro utilizado por los usuarios primarios con licencia y las partes sin licencia del espectro, a través de la tecnología de acceso de banda ancha. En consecuencia, los tipos de operación de las redes de CR pueden ser clasificados como; operación de frecuencia con licencia y sin licencia.

• Operación de la frecuencia con licencia: La banda con licencia se utiliza principalmente por la red primaria. Por lo tanto, las redes de CR se enfocan principalmente en la detección de los principales usuarios.

La capacidad del canal depende de la interferencia en las inmediaciones de los usuarios primarios. Además, si los usuarios primarios aparecen en la banda del espectro ocupado por los usuarios CR, los usuarios de CR deben abandonar esa banda del espectro y moverse a otra banda disponible de inmediato.

• Operación de la frecuencia sin licencia: Cuando hay ausencia de los usuarios principales, los usuarios de CR tienen el mismo derecho de acceder al espectro. Por lo tanto, los métodos de compartición del espectro son sofisticados y necesarios para los usuarios de CR.

Heterogeneidad de la red

Como se muestra en la Figura 1 , los usuarios de CR tienen la oportunidad de realizar tres tipos de acceso diferentes:

• Acceso a la red CR: Los usuarios CR, pueden acceder a su propia estación base CR, en las bandas del espectro, tanto con licencia y sin licencia. Debido a que todas las interacciones que se producen dentro de la red CR, su política de compartición del espectro puede ser independiente de la red primaria.

• Acceso CR tipo ad hoc: Los usuarios CR pueden comunicarse con otros usuarios de CR a través de una conexión ad hoc sobre las bandas del espectro, tanto con licencia y sin licencia.

• Acceso a la red principal: Los usuarios CR también pueden acceder a la estación base primaria, a través de la banda con licencia. A diferencia de otros tipos de acceso, los usuarios CR, requieren una adaptación en el protocolo de acceso al medio, ya que este permite el roaming en las múltiples redes primarias.

De acuerdo con la arquitectura de CR se muestra en la figura. 2, varias funciones son necesarias para apoyar la gestión del espectro en las redes de CR. Una visión general del marco de gestión del espectro y de sus componentes se muestra a continuación.

Administración de la estructura del espectro

Las redes de CR imponen desafíos únicos debido a su coexistencia con las redes primarias, así como, diversos requisitos de QoS. Por lo tanto, se requiere de nuevas funciones para administrar el espectro de las redes de CR. Administrando correctamente el espectro, se pretende:

- Evitar interferencias: Las redes de CR deben evitar las interferencias con las redes primarias.
- Usar el factor de calidad QoS: Para decidir sobre una banda del espectro adecuada, las redes de CR debe apoyarse en el factor de calidad.
- Comunicación ininterrumpida: Las redes de CR deben tener una comunicación ininterrumpida, con la finalidad de avisar a los demás usuarios de CR de la aparición de usuarios primarios.

El proceso de gestión del espectro consta de cuatro pasos principales:

- Detección del espectro: Un usuario CR puede asignar sólo una parte no utilizada del espectro. Por lo tanto, un usuario CR debe supervisar las bandas disponibles del espectro, capturar información, y luego notificar a los demás usuarios de estos espacios disponibles del espectro.
- Decisión sobre el espectro: Basado en la disponibilidad de espectro, los usuarios de CR puede asignar un canal. Esta asignación no sólo depende de la disponibilidad del espectro, ya que también deben de basarse en políticas internas y externas de las redes.
- Compartición del espectro: Debido a que puede haber múltiples usuarios de CR que intentan acceder al espectro, el acceso a la red CR debe coordinarse.
- Movilidad del espectro: Los usuarios de CR son considerados como los visitantes del espectro. Por lo tanto, si la frecuencia es requerida por un usuario primario, la comunicación debe continuar en otra frecuencia disponible del espectro.

La gestión del espectro para las comunicaciones de red de CR se muestra en la Figura 2. Por el gran numero de interacciones que se realizan entre los usuarios de CR se requiere de un diseño entre las capas del modelo TCP, para lograr esto, se emplean las principales funciones de la gestión del espectro.

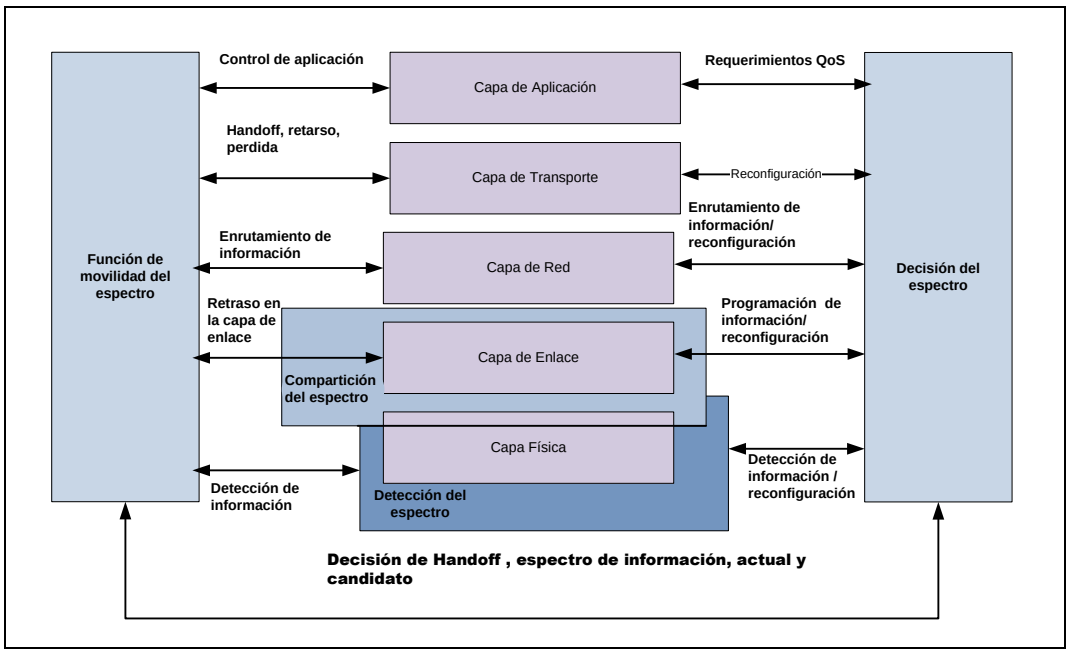

Figura 2. Marco de gestión del espectro para Redes Cognitivas

4.2. Redes Cognitivas Centralizadas

En una arquitectura centralizada, la red secundaria del usuario está orientada a la infraestructura de la red, ya que está se divide en células, y cada célula se gestiona a través de una estación base secundaria.

Estas estaciones base secundarias de control de acceso al medio se muestran en la Figura 3.

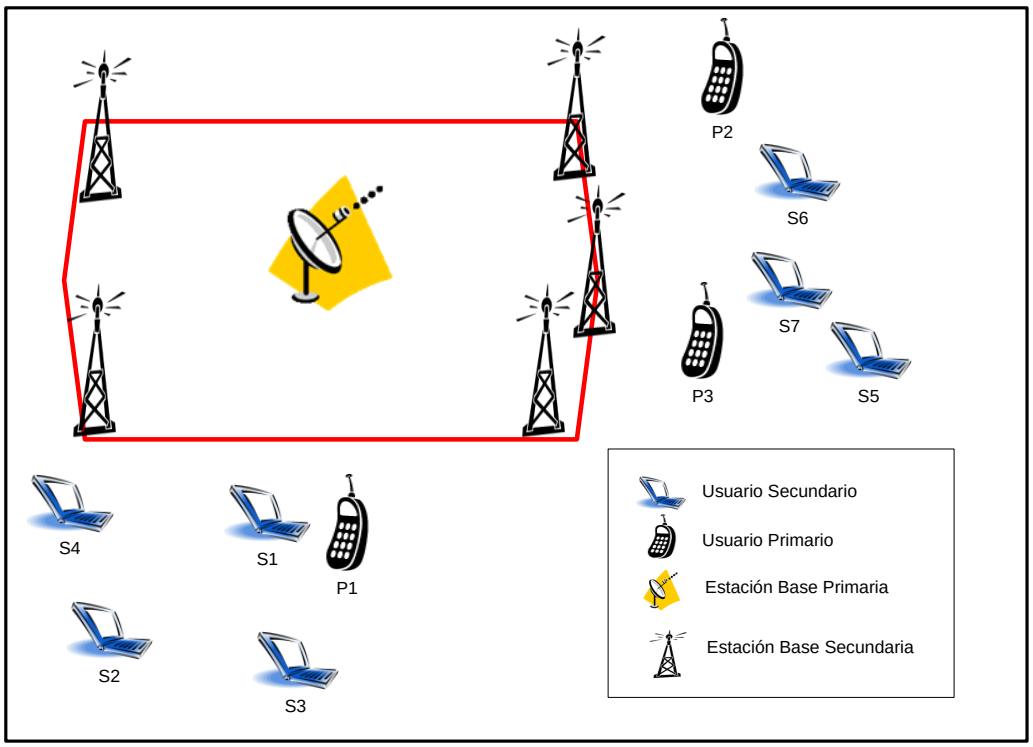

Figura 3. Red Cognitiva Centralizada

Los usuarios secundarios se sincronizan con sus estaciones base, donde pueden llevar a cabo operaciones periódicamente para la detección del espectro. Las estaciones base secundarias pueden ser interconectadas a través de una red troncal alámbrica.

4.3. Redes cognitivas descentralizadas

En una arquitectura descentralizada, los usuarios secundarios no están interconectados por una infraestructura orientada a la red. La Figura 4 representa una red descentralizada, donde los usuarios secundarios pueden comunicarse unos con otros (tipo ad hoc). Se puede observar que dos de los usuarios secundarios, que están dentro de la comunicación serie pueden intercambiar información de forma directa, mientras que los usuarios secundarios que no están dentro de la comunicación serie directa pueden intercambiar información a través de múltiples saltos.

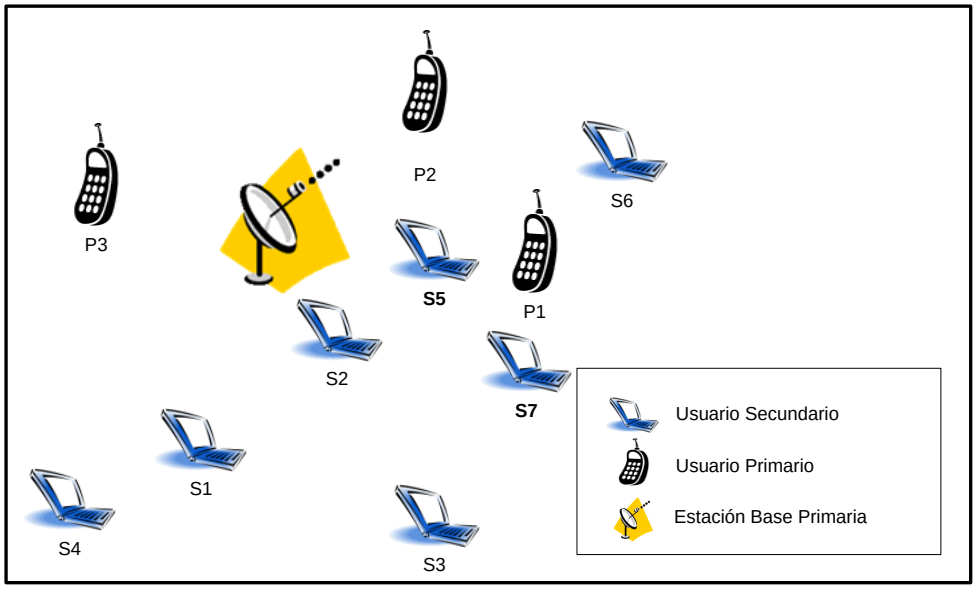

Figura 4. Red Cognitiva Descentralizada

Los usuarios secundarios distribuidos en redes cognitivas, son capaces de tomar decisiones sobre las bandas del espectro, la potencia de transmisión, etc., ya sea de manera local, basándose en observaciones, o en cooperación, para acercarse a un rendimiento óptimo para todos los usuarios secundarios.

Para ilustrar los elementos básicos desde un enfoque de colaboración, considere el siguiente ejemplo ver Figura 4, donde dos de los usuarios secundarios S1 y S2 están operando en una banda con licencia para una estación de base principal. S1 se encuentra en el límite del intervalo de transmisión de la estación base principal, S2 que está más cerca de la estación base principal. S2, por lo tanto, detectará la presencia de los usuarios principales más rápida y fácilmente que S1. Las técnicas de detección cooperativa destacan el hecho de que si los usuarios secundarios comparten la información detectada, se puede mejorar en la detección del usuario en la red cognitiva. Sin embargo, algunas veces, estas técnicas pueden ser empleadas por usuarios malintencionados, provocando problemas de inseguridad en las redes cognitivas.

Una subclase de las redes cognitivas descentralizadas es el espectro de las redes de intercambio, donde coexisten dos redes inalámbricas en una banda sin licencia. Un ejemplo de esta red es la coexistencia de IEEE 802.11 y 802.16. En estas redes, se establece un canal de coordinación del espectro para control del intercambio de información sobre los parámetros de transmisión y recepción. La identificación del usuario principal, el espectro de movilidad y las funciones de gestión no son necesarios en estas clases de redes.

4.4. Tipos de Seguridad en las Redes Cognitivas

A continuación se explica de manera breve los elementos básicos de la seguridad de las comunicaciones. Se describe la forma en que la construcción de bloques se aplican en las redes inalámbricas, como la red LAN inalámbrica IEEE 802.11, así como su importancia en las redes cognitivas.

4.4.1. Disponibilidad

Uno de los requisitos fundamentales para cualquier tipo de red es la disponibilidad. Si la red está abajo y no es utilizable, el propósito de su existencia es nulo. Una cuestión que está estrechamente relacionada con la disponibilidad de la red es la accesibilidad de información de los usuarios en la red. Aunque por lo general se refiere a la disponibilidad de los medios de transmisión inalámbrica. Varias técnicas son usadas para asegurar que el medio de comunicación inalámbrica se encuentra desocupado para su transmisión. Por ejemplo, a veces se emplea un nuevo mecanismo de compensación para evitar interferencias entre varios usuarios en la capa física (MAC) de la subcapa IEEE 802.11 a la capa de enlace.

En el contexto de las redes cognitivas, la disponibilidad se refiere a la capacidad de enseñanza de los usuarios primarios a los usuarios secundarios para acceder al espectro. Para los usuarios primarios la disponibilidad del espectro está garantizada. Para los usuarios secundarios sin licencia, la disponibilidad se refiere a la existencia de espacios desocupados en el espectro, donde el usuario puede transmitir sin causar interferencias perjudiciales a los usuarios primarios.
Algunas de las frecuencias asignadas en el espectro de radiofrecuencias, podrían emplearse, siempre y cuando, los usuarios primarios no estén usando las bandas de frecuencia. Sin embargo, la disponibilidad del espectro para los usuarios secundarios no está garantizada. Para las redes cognitivas centralizadas, la disponibilidad también se refiere a la disponibilidad de estaciones base secundarias.

4.4.2. Integridad

Un aspecto importante cuando se envía información en una red es la integridad, es decir, se debe proteger la información, contra cualquier tipo de modificación, inserción, supresión y repetición.

La integridad es la garantía de que al recibir los datos, estos estarán exactamente igual a los datos enviados. La integridad es muy importante en las redes inalámbricas, ya que, a diferencia de sus homólogos, es más fácil que un intruso acceda a una red inalámbrica. Por esta razón, se agrega una capa de seguridad en la capa de enlace en las redes LAN, con la finalidad de los enlaces inalámbricos sean tan seguros como una red por cable.
El protocolo de seguridad utilizado en esta capa es CCMP (modo contador de encriptación con protocolo CBC-MAC de autenticación).
El protocolo CCMP utiliza la técnica estándar de cifrado avanzado (AES) en el modo de encadenamiento del cifrado de bloque, para producir un mensaje de comprobación de integridad (MIC), que se utiliza para verificar la integridad del mensaje del destinatario. Estas técnicas también pueden ser empleados en redes de radio cognitiva.

4.4.3. Identificación

La identificación es uno de los requisitos básicos de seguridad para cualquier dispositivo de comunicación. Es un método para asociar un usuario o dispositivo con su nombre o identidad. Por ejemplo, en las redes celulares, los dispositivos móviles cuentan con un equipo de identificación de llamada internacional de equipo móvil

(IMEI). Este identificador se utiliza para identificar de forma exclusiva los dispositivos móviles en las redes celulares. Del mismo modo, una prueba de manipulaciones fraudulentas, es que el mecanismo de identificación debe ser incorporado en los dispositivos de los usuarios secundarios de redes cognitivas.

4.4.4. Autenticación

La autenticación es una garantía de que la comunicación de la entidad es la que dice ser. El principal objetivo de un esquema de autenticación es prevenir que usuarios no autorizados tengan acceso a los sistemas protegidos. Se trata de un procedimiento necesario para verificar tanto la identidad de una entidad y la autoridad.
Desde la perspectiva del proveedor de servicios, la autenticación protege el proveedor de servicios de intrusiones no autorizadas en el sistema, para lo cual, emplean certificados de autoridad que aseguran la protección de la información, esto a su vez, hace los usuarios de estos servicios tengan confianza al momento de emplearlos.

En las redes de radio cognitivas, hay un requisito inherente a la distinción entre los usuarios primarios y secundarios. Por lo tanto, la autentificación se puede considerar como uno de los requisitos básicos para las redes cognitivas. En las redes cognitivas centralizadas, donde las estaciones base primarias y secundarias están conectadas con una red troncal por cable, puede ser más fácil su autentificación. Sin embargo, en redes cognitivas distribuidas con un número de usuarios secundarios dispersos sobre un área geográfica grande, el abastecimiento de las funcionalidades de un certificado de autentificación puede ser absolutamente un desafío.

4.4.5. Autorización

Las entidades en la red tienen diversos tipos de autorización. Por ejemplo, el punto de acceso inalámbrico tiene la autorización de eliminar a un usuario que podría ser malicioso. Otros usuarios en la red no tienen este privilegio. La política del control de acceso a la red describe el nivel de autorización para cada una de las entidades. En el contexto de redes cognitivas, se tiene un requisito único de la autorización llamada autorización condicional. Es condicional, porque los usuarios secundarios están autorizados a transmitir en las bandas sólo con licencia, siempre y cuando no interfieran con los usuarios primarios de comunicación en esa banda. Como es difícil determinar exactamente cuál de los usuarios secundarios es responsable de las interferencias perjudiciales para transmisión de los usuarios primarios, este tipo de autorización es difícil de aplicar y más aún en una configuración distribuida. La autorización condicional, por lo tanto, plantea un desafío único en el acceso al espectro dinámico.

4.4.6. Confidencialidad

La confidencialidad está estrechamente vinculada con la integridad. Si bien la integridad asegura que los datos en tránsito no han sido modificados, la confidencialidad protege la información a usuarios no autorizados. Esto se logra con el uso de algoritmos de cifrado y encriptación de los datos que se transmiten con una clave secreta que se comparte sólo con los beneficiarios. Dicha clave puede descifrar y leer los datos.

Dado que el medio inalámbrico está abierto a los intrusos, IEEE 802.11 utiliza un estándar de cifrado avanzado (AES) con protocolo CCMP modo contador, para cifrar los datos, como una capa adicional de seguridad en la capa de enlace. Sabemos que, el ruido en el medio inalámbrico, es propenso a generar errores, sin embargo, empleando el ruido es posible, plantear un desafío único en los mecanismos de confidencialidad e integridad.

Esto se debe a que casi todas las técnicas de integridad y confidencialidad se basan en cifras que son sensibles a los errores del canal. Esta característica de la sensibilidad bajo condiciones ruidosas acciona las retransmisiones excesivas que consumen un gran ancho de banda de la red. Este problema es mayor en las redes cognitivas, donde el acceso de los usuarios secundarios a la red es oportunista y la disponibilidad del espectro no está garantizada.

4.4.7. No repudiación

Las técnicas de la no repudiación evitan que tanto el remitente como el receptor no nieguen un mensaje transmitido. Por lo tanto, cuando se envía un mensaje, el receptor puede probar que el mensaje fue enviado por el remitente. Del mismo modo, cuando se recibe un mensaje, el remitente puede probar que el mensaje fue recibido por el presunto receptor. En el ajuste de la red de radio cognitiva, si identifican a los usuarios secundarios que violan el protocolo, las técnicas de la no repudiación se pueden utilizar para probar la mala conducta y para prohibir el acceso a la red a los usuarios malintencionados.

4.5. Cuestiones inherentes de confiabilidad

A continuación se señalan algunas de las cuestiones inherentes de confiabilidad en las redes de radio cognitiva.

4.5.1. Alta sensibilidad a las señales del usuario primario

Para prevenir interferencia a los usuarios primarios con licencia, los usuarios secundarios deben detectar en primer lugar, las transmisiones primarias. Para asegurar una alta probabilidad de hasta el 99% de la ausencia de interferencias a los usuarios primarios, los requisitos a la sensibilidad son rigurosos y se colocan en los dispositivos detectores secundarios sin licencia.

Hay dos formas importantes para detectar en la transmisión un usuario principal: a base de energía y basado en la detección de la forma de onda. A base de energía no requiere ningún conocimiento de los principales usuarios de la señal de transmisión. Sin embargo, esta técnica de detección es propensa a falsas detecciones y el tiempo de detección suele ser más largo cuando la señal es de baja potencia.

La detección basada en la forma de onda es aplicada cuando la información sobre los patrones de la forma de onda y la señal de la transmisión de los usuarios primarios se sabe. Esto hace que las técnicas de detección de forma de onda realicen una mejor

detección que la técnica basada en energía. Sin embargo, en muchos casos, los patrones de la señal de transmisión del usuario primario la desconocen los usuarios secundarios.

Por otra parte, los mandatos de la FCC, como uno de los requisitos de las redes cognitivas es predecir el nivel de interferencia alrededor de los receptores del usuario principal y mantenerla por debajo de umbral. Sin embargo, suele ser difícil asegurar el cumplimiento del requisito de sensibilidad, hacia las señales del usuario primario en las redes cognitivas.
Esta alta sensibilidad basada en energía, incrementa las detecciones falsas, provocando el uso ineficaz del espectro.

4.5.2. Localización desconocida del receptor primario

Una cuestión que ha recibido muy poca atención hasta el momento es la falta de conocimiento de la ubicación de los receptores primarios. Con el fin de reducir al mínimo la interferencia a la red del usuario primario, los transmisores secundarios necesitan conocer las localizaciones de los receptores primarios.
La mayoría de los modelos de intervención que han sido estudiados, proponen que, para reducir al mínimo el nivel de interferencia, es necesario conocer la ubicación de los receptores primarios. Estas terminales ocultas pueden ocasionar problemas en las redes cognitivas.
Algunos estudios recientes han estudiado esta cuestión y propuesto técnicas que pueden utilizarse para detectar receptores primarios. Detectando la salida de energía del receptor. Sin embargo, aún queda por hacer, una importante labor para proteger los receptores primarios contra la interferencia accidental causada por los usuarios secundarios.

4.5.3. Requisito de Sincronización

Los usuarios secundarios en redes de radio cognitivas centralizadas realizan operaciones de detección a una gran velocidad entre los periodos de las transmisiones, por ejemplo, IEEE.802.22.
Estas mediciones se retransmiten a la estación base, esta agrega y determina la presencia de transmisiones de usuarios primarios. Por lo tanto, la sincronización a tiempo entre los usuarios secundarios, es un requisito importante para detectar la presencia de los usuarios primarios. Incluso si un usuario secundario no está sincronizado con el resto de los usuarios secundarios, todos los demás usuarios secundarios, transmitirían esa información a la estación base.
La estación base después, podrá determinar, que transmisión del usuario primario está disponible o cual no, también puede bloquear las transmisiones del usuario secundario en esa banda de frecuencia. La sincronización entre los usuarios secundarios es más difícil de lograr en algunas bandas del espectro como las bandas de la televisión.

4.5.4. Carencia del canal de control común

A diferencia de otra infraestructura orientada a las redes inalámbricas, las redes cognitivas carecen de un canal de control determinado. Por lo tanto, tan pronto como arranca un usuario secundario, es necesario iniciar una búsqueda de señales de control

en toda la banda espectral. Esta operación necesita ejecutarse durante el restablecimiento de la conexión móvil, es decir, cuando los usuarios secundarios se trasladen al área de cobertura de una estación base existente para el área de cobertura de otra estación base.

4.5.5. Protocolos y utilidades basados en un mismo modelo

Las funciones para uso general en muchos protocolos de acceso al espectro coordinado, se basan generalmente en un mismo modelo. Este modelo se basa en una sociedad donde los usuarios tienen una aversión de la desigualdad. Estos modelos no asumen ninguna estructura centralizada de gobierno, por lo que la aplicación de las normas depende de la participación voluntaria de sus compañeros. Sin embargo, en realidad, esta situación rara vez existe, ya que algunas entidades malintencionadas tienden a violar dichos códigos.

Este modelo está diseñado para fines egoístas como la adquisición de mayor ancho de banda, así como obtener más recursos o bien para bloquear intencionalmente a otros que quieren conseguir recursos específicos. Por lo tanto, se deben emplear modelos más robustos que detecten el comportamiento malintencionado. Estos, deben emplearse para diseñar protocolos de acceso coordinados en las redes cognitivas.

4.6. Descripción de las principales capas en las Redes de Radio Cognitivas

4.6.1. Capa Física

La capa física es la encargada de transmitir los bits de información por la línea o medio utilizado para la transmisión. Se ocupa de las propiedades físicas y características eléctricas de los diversos componentes, de la velocidad de transmisión, si esta es unidireccional o bidireccional. Así mismo, se encarga también, de aspectos de mecanismos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas.
En las redes cognitivas, la capa física tiene la capacidad de transmitir en diferentes frecuencias a través de la mayor parte de la banda del espectro radioeléctrico. Esto hace que la capa física en las redes cognitivas sea más compleja, en comparación con las redes inalámbricas convencionales. Por lo tanto, cuando la transmisión de una banda de frecuencia se cambia a otra banda de frecuencia, el proceso de cambio incurre en un retraso considerable en la capa física de las redes cognitivas.

4.6.2. Capa de Enlace

El objetivo principal de la capa de enlace consiste en transferir los datos hacia y desde la capa física a la capa de red. Especifica cómo se organizan los datos cuando se transmiten en un medio particular. Además del direccionamiento local, se ocupa de la detección y control de errores ocurridos en la capa física, del control de acceso a dicha capa y de la integridad de los datos y fiabilidad de transmisión. Para esto se agrupa la información a transmitir en bloques, e incluye a cada uno una suma de control, que permitirá al receptor comprobar su integridad. Los datagramas recibidos son comprados

por el receptor. Si algún datagrama se ha corrompido se envía un mensaje de control al remitente solicitando su reenvió.
La capa de enlace proporciona los medios funcionales que permiten la fragmentación de datos, corrección de errores y modulación.

4.6.3. Capa de Red

La capa de red es responsable de la entrega de paquetes de nodo a nodo. La capa de red proporciona los medios operativos para realizar el enrutamiento, el control de flujo y la calidad de servicio (QoS). El enrutamiento se refiere a la selección de trayectorias a lo largo de la red a través de la cual se transmiten datos desde el origen al destino. Cada nodo en la red es responsable de mantener la información de enrutamiento sobre sus nodos vecinos. Cuando una conexión necesita ser establecida, cada nodo determina cual de sus vecinos debe ser el siguiente en la trayectoria hacia el destino. Algunos de los protocolos de enrutamiento usados en entorno inalámbrico, por ejemplo, el enrutamiento dinámico (DSR) y ad-hoc sobre la demanda de la distancia del vector (AODV) de la fuente. Un nodo malintencionado en la trayectoria puede interrumpir el enrutamiento por la incorrecta información de enrutamiento a sus vecinos o por la reorientación de los paquetes en la dirección equivocada.

4.6.4. Capa de Transporte

La capa de transporte establece los requisitos funcionales para la transferencia de datos entre dos hosts de extremo a extremo. Es el principal responsable del control de flujo, de la recuperación de errores de punto a punto y del control de la congestión. Hay dos protocolos principales que operan en la capa de transporte, el Protocolo de datagramas de usuario (UDP) y el Protocolo de control de transporte (TCP). El UDP es sin conexión, mientras que TCP tiene una conexión orientada y garantiza la entrega de paquetes. El rendimiento de TCP suele medirse por un parámetro llamado tiempo de viaje de ida y vuelta (RTT). Los errores en el entorno inalámbrico pueden causar la pérdida de paquetes, que a su vez desencadena en las retransmisiones. Además, los frecuentes cambios de banda del espectro por los usuarios secundarios, debido al espectro handoff en el aumento de capa de enlace, aumentan el RTT. Además, diferentes nodos secundarios operan en diferentes bandas de frecuencia y las bandas cambian constantemente., es por esto que el RTT para una conexión TCP en redes cognitivas tenga una alta variación.

4.6.5. Capa de Aplicación

La capa de aplicación es la última capa del modelo. Esta proporciona las aplicaciones para los usuarios de los dispositivos de comunicación. Algunos de los servicios básicos de la capa de aplicación incluyen el protocolo de transferencia de archivos (FTP), Telnet, correo electrónico y recientemente streaming. Por lo tanto, cualquier ataque contra las capas: física, enlace, red de transporte, puede repercutir negativamente en la capa de aplicación. Uno de los parámetros más importantes en la capa de aplicación es la calidad de servicio (QoS). Esto es especialmente importante para aplicaciones de

streaming. En la capa física y de enlace, los retrasos al espectro handoff. Para la capa de red los ataques provocan desvíos innecesarios de rutas, debido a los ataques y retrasos se crea una degradación de QoS en los protocolos de la capa de aplicación.

4.7. Ataques a las redes de radio cognitiva

Un ataque contra las redes cognitivas se define de las siguientes maneras:

1) Una interferencia inaceptable a los usuarios primarios autorizados.
2) Oportunidades perdidas para los usuarios secundarios.

Un ataque puede ser cuando un número mínimo de adversarios que aunque realizan operaciones mínimas, estas causan daño y pérdidas para los usuarios primarios y secundarios en la red. A continuación se describirán algunos ataques de problemas de confiabilidad en varias de las capas de las redes cognitivas. Las capas que se describirán son: Capa física, Capa de enlace, Capa de transporte, Capa de aplicación, así como los ataques que se presentan entre las capas, ya que a pesar de que estos ataques son específicos a cada capa, estos a su vez pueden afectar a otras capas.

4.7.1. Ataques de la capa física

a) Ataque intencional (Jamming)

Este es uno de los tipos de ataque más comunes, que se pueden ser realizados por los usuarios secundarios en las redes de radio cognitiva.
El usuario secundario ataca interfiriendo de forma malintencionada y continua, en una banda con licencia a los usuarios primarios y secundarios. Dicho ataque se puede amplificar por el uso de alta potencia de transmisión, transmitida en varias bandas espectrales.
Aunque las técnicas basadas en la detección de la energía y las técnicas de triangulación, se pueden utilizar para detectar este ataque, el tiempo que tarda en identificar al y el usuario malintencionado, afecta seriamente el rendimiento de la red. El ataque se puede hacer más peligroso por un usuario secundario malintencionado móvil que realiza el ataque en un área geográfica y que se desplazan a otra área antes de ser capturado.

b) *Ataque del receptor primario*

La falta de conocimiento acerca de la ubicación de los receptores primarios puede ser utilizada por una entidad malintencionada, causando interferencias perjudiciales.

El ataque se produce cuando el usuario primario que está más cerca del receptor primario participa en un protocolo de colaboración y envió de transmisiones a usuarios secundarios, para que esta sea detectada por el usuario malintencionado.
A pesar de la interferencia se mantenga por debajo del umbral en algún otro punto en el espacio, ésta todavía causaría interferencia continua al receptor bloqueando de manera eventual las transmisiones primarias. Por otra parte a veces los usuarios

secundarios olvidan que son ellos quienes pueden generar las interferencias al receptor primario.

c) Ataque de amplificación a la sensibilidad

Con el fin de evitar interferencias en la red primaria, algunas técnicas de detección del usuario primario tienen una mayor sensibilidad hacia las transmisiones primarias. Esto da lugar a detecciones falsas trayendo consigo oportunidades perdidas para los usuarios secundarios. Una entidad malintencionada puede amplificar la sensibilidad y, por tanto, el número de oportunidades perdidas para reproducir la transmisión primaria. ¿Qué hace que este ataque más perjudicial?, es que incluso un adversario con una baja potencia de transmisión puede transmitir en los límites de la banda del espectro y todavía causar a los usuarios secundarios que operan en múltiples bandas del espectro un sin fin de pérdidas de oportunidades provocando un uso ineficiente del espectro.

d) Ataque secundario traslapado del usuario

En las redes cognitivas centralizadas y distribuidas, las redes múltiples secundarias pueden coexistir en la misma región geográfica. En tales casos, las transmisiones de entidades malintencionadas en una red pueden causar daño a los usuarios primarios y secundarios de la otra red. Este tipo de ataque es difícil de prevenir porque las entidades malintencionadas pueden no estar bajo control directo de la estación base de los usuarios de la red o de los usuarios de la red que corre peligro.

4.7.2. Ataques en la capa de enlace

a) Ataque para uso general

Un usuario secundario malintencionado es capaz de ajustar los parámetros para un uso general, aumentando el ancho de banda. Si los usuarios secundarios y/o las estaciones base no son capaces de detectar este tipo de comportamiento anormal, puede provocar la privación del medio de transmisión para otros usuarios secundarios. Por ejemplo, algunos autores proponen una función para uso general que sea utilidad a los usuarios secundarios para determinar el ancho de banda en términos de potencia de transmisión, con la restricción de que la interferencia debido a las transmisiones secundarias en los receptores primarios este por debajo del umbral. El problema se analiza como un juego de interés público y las soluciones para lograr un equilibrio óptimo global que determine las transmisiones adecuadas para los usuarios secundarios, por ejemplo, si un usuario malintencionado cambia su función de uso general para transmitir a una potencia mayor, dará lugar a que otros usuarios obtengan menos ancho de banda. Algunos usuarios secundarios tal vez ni siquiera puedan transmitir.

b) Ataque de detección asíncrono

En lugar de sincronizar la actividad de detección con otros usuarios secundarios de la red, un usuario malintencionado puede transmitir asíncrono, cuando otros usuarios secundarios están realizando operaciones de detección. Si la estación base u otros usuarios secundarios consideran esto como una transmisión de un usuario

primario, después esto podría dar lugar a oportunidades perdidas. Este ataque puede ser más eficiente transmitiendo sólo durante los periodos de detección.

c) Ataque falso

Para los protocolos que confían en los usuarios secundarios que intercambian información. La falsa información de un grupo de usuarios malintencionados puede hacer que los usuarios secundarios tomen acciones inapropiadas, para así modificar los objetivos del protocolo. Por ejemplo, considere la posibilidad de un escenario representado en la Figura 4. En esta red cognitiva descentralizada, conformada por cinco usuarios secundarios, S1,..., S5, se asocian con una estación base secundaria. El usuario secundario S2 está más cercano a una estación base secundaria. Supongamos que el usuario secundario S2 es malintencionado y cuando la estación base primaria comienza a usar su licencia autorizada para ingresar al espectro y S2 la detecta pero no revela esta la información a otros usuarios secundarios, además el usuario secundario S1 se encuentra fuera de la región de la base principal y por lo tanto no percibe la presencia del receptor primario. Del mismo modo, los usuarios secundarios S3, S4 y S5 tampoco han podido detectar la presencia del receptor primario. Ahora, cualquier transmisión de S1, S3, S4 y S5 puede causar interferencias perjudiciales en la transmisión a los receptores primarios de la estación base primaria. Un ataque similar es posible en una red de radio cognitiva centralizada.

4.7.3. Ataques de la capa de red

Varios ataques de enrutamiento se han descubierto en redes inalámbricas ad hoc, la mayoría de los ataques se pueden clasificar en dos categorías:

1) Ataques en la interrupción de rutas.
2) Ataques en el consumo de recursos.

Algunos de los ejemplos de los ataques de enrutamiento es el ataque llamado “agujero negro” donde un nodo malintencionado atrae a los paquetes de cada nodo, el atacante selecciona los paquetes así como dos pares de nodos con una conexión privada entre los dos pares. Este ataque suele ser peligroso ya que puede evitar ser descubierto, la mayoría de estos ataques se previenen usando protocolos seguros como Ariadne, los cuales utilizan mecanismos de encriptación para garantizar la integridad de la información de enrutamiento y la autenticidad de los nodos. Aunque la mayor parte de los problemas de la capa de enlace en las redes LAN inalámbricas se han estudiado, referente a la seguridad en la capa de enlace en las redes cognitivas aun no se ha realizado.
A continuación se muestran algunos ataques en la capa de enlace aplicados en las redes cognitivas.

a) Ataque NEPA

NEPA tiene la capacidad de hacer que al menos un nodo se comporte de manera malintencionada en la red. El propósito de este nodo consiste en aumentar la interferencia en los canales primarios con mayor tráfico de información.

La mayor parte del tiempo, los enlaces son afectados durante toda la trayectoria a través de la ruta de nodos malintencionados hacia la puerta de enlace por cable; por lo tanto, el ataque lleva el nombre de un ataque de parásito.
En condiciones normales de operación de asignación de canales, un nodo asigna la menor carga para los canales de sus interfaces y transmite la información más reciente a sus vecinos dentro del dominio. Un nodo comprometido lanza el NEPA asignando sus interfaces a los canales primarios. Sin embargo, no informa a sus vecinos sobre este cambio, esto da lugar al uso de canales con interferencia, disminución del ancho de banda y un menor rendimiento

b) Ataque CEPA

El ataque CEPA es un caso especial del ataque NEPA, con una ligera modificación en la estrategia de ataque. Un nodo comprometido lanza el ataque CEPA cambiando todas las interfaces del canal prioritario que está siendo utilizado. Sin embargo, la gravedad de este ataque hace que su detección sea fácil.

c) Ataque LORA

El ataque LORA maneja información engañosa sobre las asignaciones del espectro y la transmite a todos los vecinos para impulsar la red en un estado cuasi-estable. Puesto que la asignación del canal del nodo comprometido no se cambia realmente, este ataque es perceptiblemente diferente al NEPA y CEPA, de igual modo es un tipo de ataque mucho más fuerte y barato. El ataque LORA es relativamente más grave porque el efecto se propaga a una gran parte de la red, más allá de los vecinos del nodo comprometido, alterando la capacidad de transmisión de tráfico de los distintos nodos, en un tiempo de duración considerable. Se pone en marcha el ataque cuando el nodo comprometido transmite la información engañosa de la asignación del canal, forzando a los otros nodos a ajustar sus asignaciones del canal. Esto puede generar una serie de cambios, incluso en la asignación del canal de los nodos no vecinos. Este ataque crea la ilusión de que los canales tienen una intensa carga de información, creando una confusión en la selección de canales.

4.7.4. Ataques en la capa de transporte

Inusualmente algunas veces los viajes de ida y vuelta, con frecuencia provoca que se produzcan retransmisiones en la capa de transporte que implican períodos de sesiones en redes cognitivas cortas. Esto da lugar a un gran número de sesiones que son iniciadas para cualquier uso dado. La mayor parte de la capa de transporte como los protocolos de seguridad SSL y TLS emplean claves criptográficas al comienzo de cada período de sesiones. Las redes cognitivas tienen un mayor número de sesiones, por tanto, el número de los principales establecimientos aumentará la probabilidad de utilizar la misma clave dos veces. Las repeticiones pueden ser explotadas para romper el cifrado del sistema subyacente.

Por ejemplo, los protocolos WEP y TKIP se utilizan en la capa de enlace de IEEE 802.1, son vulnerables a los ataques de repetición. El protocolo CCMP es más reciente y fuerte, y está diseñado para demorar las repeticiones en las claves. Sin embargo, la mayoría de los protocolos de seguridad utilizada por debajo de la capa de red se ha

diseñado teniendo en cuenta el número total de sesiones que normalmente se producen en redes LAN inalámbricas.

4.7.5. Ataques entre capas

Los ataques entre capas se refieren a las operaciones malintencionadas realizadas en una capa para causar violaciones de seguridad en otra capa. Para las redes cognitivas, se requiere de una mayor interacción entre las distintas capas del protocolo de comunicación. Por esta razón se necesita poner mayor atención en los ataques entre capas.
Este ataque se realiza en la capa de red, pero afecta el rendimiento de la capa de transporte, en concreto el protocolo TCP. El objetivo de este ataque es reducir el rendimiento del protocolo TCP. Hay tres variantes de este ataque: desorden, variación de la caída y del retardo. El ataque de desorden provoca que los paquetes se reordenen de manera intencional y periódicamente, mientras estos pasan por un nodo malintencionado.

Este ataque se aprovecha de la vulnerabilidad de los paquetes desordenados del protocolo TCP, este acciona retransmisiones y degrada rendimiento de procesamiento. La segunda variante es el ataque de caída del paquete, donde el nodo malintencionado altera por fracción de segundos los paquetes. Sin embargo, los paquetes son escogidos de manera inteligente por el adversario para poder coincidir con la ventana de la transmisión del TCP, provocando a veces un rendimiento nulo en el protocolo.
La tercera variante del ataque es el retardo, aquí están los paquetes al azar, ya que demora en pasar a través de un nodo malintencionado. Esto hace que el tiempo de TCP no se considere válido lo que se traduce en congestión e inferencias. Aunque estos ataques son principalmente propuestas para redes inalámbricas ad hoc, puede ser aplicado a las redes cognitivas descentralizadas.
Por último, proponen una cuarta variante en este tipo de ataque, donde el atacante realiza operaciones en la capa de enlace para atacar la capa de transporte. Para realizar este ataque, el atacante hace que el nodo víctima cognitivo para cambiar de una a otra banda de frecuencias (utilizando cualquiera de los ataques de la capa de enlace), lo que provoca un retraso considerable en la red de transporte y demás capas. Si se realiza observando activamente el tráfico de TCP, puede hacer que existan retrasos en las sesiones de ida y vuelta, perjudicando el rendimiento del protocolo.
Todos los ataques mencionados anteriormente son difíciles de detectar en la capa de red, y por ende permite los ataques en a capa de transporte.

4.8. Arquitecturas de redes cognitivas

Algunas de las arquitecturas de las redes cognitivas son:

- Arquitectura Nautilus.
- Arquitectura DIMSUMnet.
- Arquitectura IEEE 802.22.
- Arquitectura de Radio Cognitiva OCRA basada en OFDM.

4.8.1. Arquitectura Nautilus

Nautilus es un marco de coordinación distribuido, escalable y eficiente para las redes ad hoc del espectro abierto. El marco de Nautilus se refiere a la falta de un canal de control común en las arquitecturas de redes cognitivas. Existen algunos planes de colaboración en el acceso al espectro que no confían en una entidad centralizada o un canal de control común. Para las redes cognitivas móviles se emplea una asignación distribuida del espectro, basada en una negociación local, donde los usuarios móviles negocian la asignación del espectro dentro de los grupos de un mismo organismo local. Los recursos son limitados para los dispositivos cognitivos, por lo que, se propone una regla basada en la gestión del espectro, en donde los usuarios tengan acceso al espectro sin licencia de acuerdo con observaciones locales del espectro.

4.8.2. Arquitectura DIMSUMnet

La arquitectura se basa en un corredor del espectro gestione permanentemente las bandas con licencia (denominado acceso coordinado de bandas (JCA)). Las estaciones de base secundarias se colocan con los encargados de acceso a la red denominados RANMANs. RANMANs se encarga de negociar con los agentes de arrendamiento del espectro la asignación del espectro apropiada para las estaciones de base secundarias.
El corredor del espectro, que mantiene una base de datos de las bandas de frecuencias disponibles en la actualidad, responde a RANMANs con frecuencias e intervalos de tiempos asignados del espectro.
Después de que las bandas del espectro se asignen a las estaciones base secundarias, se informa a los usuarios secundarios conectados con esas estaciones base para cambiar a las bandas de frecuencia correspondientes. Puesto que DIMSUMnet es una arquitectura centralizada, con la detección del espectro realizada por una entidad centralizada, los mecanismos de seguridad son más fáciles de ejecutar y de adherirse.
La detección de ataques que son posibles en IEEE 802.22 son más difíciles de aplicar en DIMSUMnet. Sin embargo, como el espectro de función de control se realiza por una sola entidad, la información sobre la disponibilidad del espectro puede no ser tan precisa como en el caso de detección distribuida realizado por el IEEE 802.22. La información inexacta del espectro puede ser una edición de confiabilidad primaria en el caso de DIMSUMnet.

4.8.3. Arquitectura IEEE 802.22

IEEE 802.22 es un estándar para las redes de inalámbricas regionales (WRAN) que utilizan la frecuencia UHF y VHF, las bandas de televisión entre el 54 y 862 MHz. IEEE 802.22 ayuda a gestionar las estaciones base con una característica única de detección distribuida. Para realizar la detección distribuida, la estación base da la instrucción a los usuarios secundarios de los dispositivos cognitivos, para que puedan detectar de manera síncrona las bandas espectrales para el uso del usuario primario.
Estos resultados son sensores periódicamente recogidos por la estación base, que realiza la totalización de los resultados para determinar la presencia y ausencia de los principales usuarios en cada una de las bandas del espectro bajo licencia. Por lo tanto, el IEEE 802.22 se basa en la detección síncrona.

Este requisito puede ser una fuente de vulnerabilidad. En este caso, la entidad malintencionada transmite durante el período de detección y provoca que los usuarios segundarios detecten la actividad del usuario primario. Esto da lugar a un manejo ineficiente de los recursos del espectro. A veces se proporciona una solución que consiste en una firma digital, que ayuda a las estaciones base para identificar las señales primarias originales y de este modo evitar las que sean enviadas por entidades malintencionadas.

4.8.4. Arquitectura de Radio Cognitiva OCRA basada en OFDM

La red OCRA se basa en la tecnología OFDM. Se consideran las arquitecturas de red cognitivas centralizadas y distribuidas. Para tomar decisiones sobre la detección del espectro, OCRA emplea una técnica de OFDM, basada en la gestión del espectro, esta se basa en la capa física que permite el reparto del espectro de modo dual. Este tipo de reparto del espectro permite el acceso a las redes existentes, así como la coordinación entre los usuarios cognitivos. OCRA propone utilizar una nueva técnica de rutas entre capas. Para aumentar la confiabilidad y QoS, las conexiones múltiples de la capa de transporte se establecen sobre las bandas no contiguas del espectro.

4.9. Direcciones futuras

Algunas de las direcciones futuras que deben adoptarse para hacer que las redes de radio cognitiva sean seguras consiste en el desarrollo de protocolos de seguridad, ya que algunas veces estos requieren que se trabaje en la encriptación de la información.

4.9.1. Uso de protocolos de seguridad existentes

Los servicios de seguridad que se aplican en redes inalámbricas, telefonía celular, también pueden aplicarse en las redes cognitivas. En arquitecturas de redes inalámbricas centralizadas, la red troncal de cable normalmente es un medio. Por lo tanto, existen fuertes mecanismos de seguridad que protegen a esta red. Las redes inalámbricas deben estar protegidas por el aire. Como las redes celulares están centralizadas, las soluciones de seguridad existentes en las redes celulares (3G en particular) se podría utilizar como modelo para garantizar la seguridad en redes cognitivas.
En las redes celulares, la identidad del usuario es obtenida usando una entidad temporal llamada identidad móvil del usuario. La autentificación se realiza por medio de un mecanismo de respuesta que emplea llaves secretas. Este mecanismo se basa en integridad.

Para la telefonía celular una entidad el indica a otra que sabe algo sin revelar la información. Para esto se empela un acuerdo de autentificación y de la llave UMTS. El secreto es proporcionado usando el algoritmo secreto f8 y la llave de encriptación secreta, que se intercambia como parte del proceso.
La integridad es proporcionada usando el algoritmo de la integridad f9 y la llave de integridad. Un bloque de cifrado conocido como Kasumi es la piedra angular de los algoritmos f8 y f9. Kasumi opera en bloques de 64 bits y utiliza uno de 128 bits de clave

secreta. Una configuración similar podría ser utilizado en redes cognitivas centralizadas para establecer los requisitos básicos de seguridad entre los usuarios secundarios y la estación base secundaria.

En redes descentralizadas, los usuarios secundarios se comunican entre sí con más de uno o más saltos. Debido a la falta de infraestructura, estas redes también se denominan redes ad-hoc. Este tipo de redes suelen emplear un mecanismo de seguridad de dos niveles. Un nivel de seguridad se proporciona en la capa de enlace de cada salto para proteger de la comunicación y el otro nivel de seguridad se emplea en la red de transporte o de la capa de aplicación para proteger la comunicación de extremo a extremo. Dos operaciones más complicadas de las redes inalámbricas ad hoc son las gestión del espectro y la seguridad en la trayectoria. Las redes descentralizadas cognitivas podrían utilizar los mecanismos de seguridad empleados en las redes inalámbricas ad-hoc. Algunas de las cuestiones, tales como la falta de un canal de control y el uso de diversas bandas de frecuencias por los diferentes usuarios secundarios pueden imponer restricciones adicionales sobre los actuales protocolos de seguridad.

4.9.2. Uso de cifrados

La mayor parte de los ataques realizados en la capa de enlace implican una entidad enmascarada malintencionada como un usuario principal. Por lo tanto la identificación del usuario primario es primordial para las redes centralizadas y descentralizadas. Recientemente se ha propuesto una firma digital que se puede ser utilizada, por los usuarios secundarios para distinguir transmisiones primarias malintencionadas. La mayor parte de la investigación se basa en el uso de cifrados criptográficos para resolver los problemas de seguridad de las redes cognitivas.

4.9.3. Mecanismos de seguridad reactivos

Los mecanismos de seguridad que detectan actividad malintencionada de las redes cognitivas, necesitan ser desarrolladas. Por ejemplo, los mecanismos que pueden detectar inusualmente las bandas del espectro son útiles para evitar la interferencia del espectro y los ataques. Los mecanismos de detección combinados con los mecanismos de la no repudiación permiten a los usuarios secundarios identificar y bloquear a usuarios malintencionados.

4.9.4. Enfoque del espectro

Hay dos maneras para manejar la movilidad del espectro y los retardos asociados. Una de ellas es hacer que el espectro que detecta, sea rápido de analizar y transparente para los protocolos de la capa superior. Sin embargo, el espectro de detección y los procesos handoff en sus etapas de inicio, llevarán un largo tiempo en lograr avances.
Otra manera es la metodología entre capas para incorporar la movilidad del espectro como información de estado en los protocolos que funcionan en las capas superiores. Aunque este enfoque aumente las dependencias entre las capas, hará consciente al protocolo para que disponga de una mejor defensa contra los ataques a los protocolos de la capa superior de las redes cognitivas. Por ejemplo, la ruta debe considerar la banda operacional del espectro, sus características de frecuencia. En la capa de transporte debe

considerar el efecto handoff del espectro en el tiempo de viaje de ida y vuelta, y ajustar la ventana de retransmisión correspondiente.

4.9.5. Desarrollo analógico de protocolos primitivos

Uno de los retos es la incorporación de mecanismos de seguridad en redes cognitivas es que en algunas bandas de frecuencias como la televisión, las estaciones base primarias transmiten señales analógicas (con la excepción de HDTV). Puesto que la mayor parte de los protocolos primitivos criptográficos funcionan en el dominio digital, puede incluso no ser posible incorporarlos en señales análogas de la TV. Por lo tanto, los protocolos primitivos criptográficos que trabajan en dominios análogos necesitan ser desarrollados.

4.9.6. Uso de protocolos de seguridad primitivos y ligeros

Si los usuarios secundarios en redes cognitivas móviles tienen equipos con potencia de procesamiento limitada, al igual que los recursos, sería un desafío proporcionar la capacidad de radio cognitiva y de seguridad en tiempo real. Los protocolos de seguridad ligeros necesitan ser desarrollados para la energía y los entornos de recursos limitados.