TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 19 No. 3, Septiembre-Diciembre, 2020, p.23-37 ISSN 1729-3804

EL RADIO COGNITIVO EN LA GUERRA ELECTRÓNICA

Rafael Galindo Mier[1]
Instituto de Investigación y Desarrollo de Telecomunicaciones, LACETEL, Ave. 1 de mayo esquina a Ave. Boyeros
e-mail: galindo@lacetel.cu

RESUMEN

La guerra electrónica (EW) incluye todas las acciones que usan armas de energía electromagnética, estas para controlar el espectro electromagnético para efectuar amenazas. La realización de EW en áreas urbanas busca lograr los mismos resultados que en otros entornos. Una consideración importante en las áreas urbanas son los efectos colaterales en partes de la infraestructura crítica urbana que dependen del espectro electromagnético para el servicio. Mientras que los expertos de EW han reconocido por mucho tiempo la importancia de la contribución de EW a la guerra moderna, recientemente EW se ha integrado sagazmente en el pensamiento de la guerra moderna. La tecnología de radio cognitivo (CR) ha demostrado ser una solución tentadora para promover la eficiencia del espectro y aliviar los problemas de escasez de este. La capacidad cognitiva del CR se utiliza para la monitorización de algunas bandas de frecuencia de interés de conjunto con técnicas innovadoras de radio de espectro ensanchado por salto de frecuencia (FHSS) para identificar los espacios o agujeros del espectro evitando interferir a los usuarios primarios existentes. El objetivo de este artículo es, luego de una extensa encuesta de los materiales publicados, proporcionar una visión actualizada sobre el rol del CR en la EW.

PALABRAS CLAVES: Guerra electrónica, interferencia provocada o jamming, radio cognitivo, salto de frecuencia.

COGNITIVE RADIO IN THE ELECTRONIC WARFARE

ABSTRACT

Electronic warfare (EW) includes all actions that use electromagnetic energy weapons, to control the electromagnetic spectrum to carry out threats. Performing EW in urban areas seeks to achieve the same results as in other settings. An important consideration in urban areas is collateral effects on parts of critical urban infrastructure that depend on the electromagnetic spectrum for service. While EW experts have long recognized the importance of EW's contribution to modern warfare, recently EW has been cleverly integrated into modern warfare thinking. Cognitive radio (CR) technology has proven to be a tempting solution for promoting spectrum efficiency and alleviating spectrum shortage issues. The cognitive capacity of the CR is used for the monitoring of some frequency bands of interest in conjunction with innovative techniques of frequency hopping spread spectrum (FHSS) radio to identify the spaces or holes of the spectrum avoiding interfering with the existing primary users. The aim of this article is, after an extensive survey of published materials, to provide an updated view on the role of the RC in EW.

KEYWORDS: Electronic Warfare, jamming, cognitive radio, frequency hopping.

1. INTRODUCCIÓN

Hoy en día, los sistemas FHSS se han utilizado ampliamente en comunicaciones civiles y militares, pero de alguna manera sus beneficios se verían potencialmente neutralizados por un bloqueo de seguimiento (FOJ-Follow-on jamming) con escaneo de banda ancha y capacidades de respuesta interferente o de bloqueo que cubran el período de salto. El concepto FOJ es en realidad implícitamente análogo a una comunicación con características de conocimiento del espectro y ubicación, escuchar, actuar, así como auto adaptación. El alto valor de la relación de percepción cognitiva (RCP) significa un alto conocimiento del espectro, pero una baja coexistencia.

El concepto central para un sistema de comunicaciones seguro es protegerse contra bloqueos e interceptores no intencionados o intencionados, obligarlos a cambiar los parámetros del sistema o trabajar fuera de las regiones aceptables prescritas, y simultáneamente mantener el rendimiento seguro del sistema. La organización de este artículo es la siguiente: la Sección 2 está dedicada a los conceptos básicos de la guerra electrónica (EW), la Sección 3 describe los tipos de bloqueadores (jammers), la Sección 4 ofrece las tecnologías bloqueadoras (jamming) y anti-bloqueadoras (anti-jamming), la Sección 5 está dedicada a la detección de señales bloqueadoras, la Sección 6 presenta sistemas de comunicaciones anti-jamming, la Sección 7 analiza la capacidad de detección del espectro a través de esquemas de escaneo específicos, la Sección 8 ofrece el rendimiento anti-jaming de las redes de radio cognitivos (CRN), la Sección 9 ofrece los resultados de Simulaciones de dos Redes de Radio Cognitivos (CRN-Cognitive Radio Network) típicas y en la Sección 10 damos algunas conclusiones finales.

Manuscrito recibido:24-07-2020, aceptado: 27-08-2020
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

2. GUERRA ELECTRÓNICA

La guerra electrónica de comunicación (EW, por sus siglas en inglés) es el nombre que se aplica a las actividades realizadas para lograr la intercepción o la denegación de comunicaciones. Consiste en tres componentes principales: Ataque electrónico (EA), Soporte electrónico (ES), Protección electrónica (EP).

El ataque electrónico (EA) es la nueva denominación de lo que solía llamarse contramedidas electrónicas (ECM). Es el uso de señales activas para evitar que un sistema de comunicación intercambie información de manera efectiva. En este artículo solo abordaremos el ataque electrónico. En general (aunque no exclusivamente) se acepta que (EA) consiste en tres actividades principales: (1) jamming o bloqueo, (2) engaño y (3) energía dirigida (DE). De los tres principios principales de la información: relevancia, precisión y oportunidad [1], el jamming está destinado principalmente a abordar el último. Si la información se intercambia con éxito, es poco lo que puede hacer el jamming para afectar directamente la relevancia y precisión de esa información. Sin embargo, las actividades de jamming pueden afectar la oportunidad del intercambio de información, al menos temporalmente, reduciendo ese intercambio. El jamming también puede afectar la relevancia de la información, porque si llega al destino previsto demasiado tarde para ser utilizada, la información se vuelve irrelevante. Ni el soporte electrónico (ES) ni la protección electrónica (EP) serán abordados en este artículo.

3. TIPOS DE JAMMERS

Las redes inalámbricas juegan un papel importante en el logro de la comunicación ubicua, donde los dispositivos de red embebidos en el entorno proporcionan conectividad y servicios continuos, mejorando así la calidad de vida humana. Sin embargo, debido a la naturaleza expuesta de los enlaces inalámbricos, las redes inalámbricas actuales pueden ser atacadas fácilmente por la tecnología de jamming. El jamming en redes inalámbricas se define como la interrupción de las comunicaciones inalámbricas existentes al disminuir la relación señal / ruido en el lado del receptor a través de la transmisión de señales inalámbricas interferentes. El jamming es diferente de las interferencias regulares de la red, porque consiste en el uso deliberado de señales inalámbricas en un intento de interrumpir las comunicaciones, mientras que la interferencia se refiere a formas involuntarias de interrupciones. Para comprender cómo un jammer ataca las redes inalámbricas y cómo evitar el jamming para lograr una comunicación eficiente, investigamos los tipos de jammers existentes. La clasificación detallada de diferentes jammers se puede encontrar en la Fig. 1 [2].

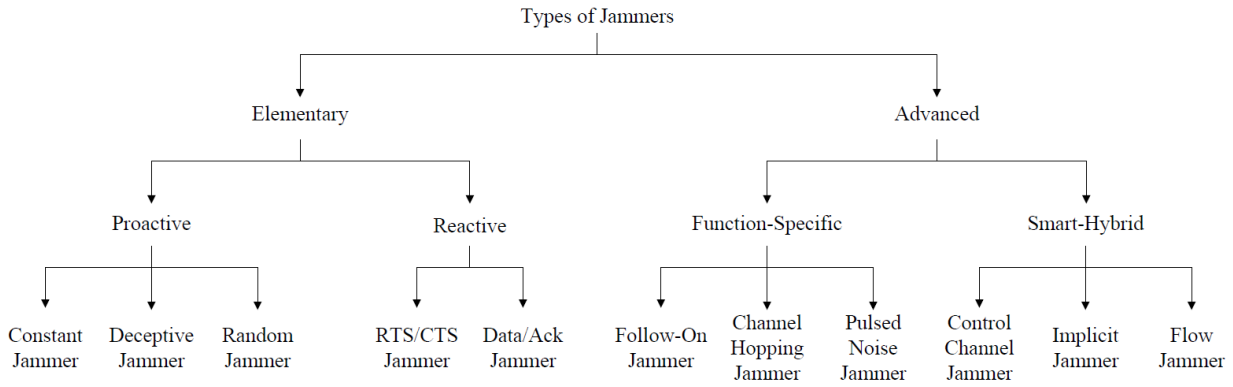

Figura 1: Tipos de jammers en redes inalámbricas [2].

Básicamente, un jammer puede ser elemental o avanzado según su funcionalidad. Los jammers elementales, los dividimos en dos subgrupos: proactivos y reactivos. Los avanzados también se clasifican en dos subtipos: de función específica e híbridos-inteligentes.

El jammer proactivo transmite señales de jamming (bloqueo) independientemente de si hay o no comunicación de datos en una red. Envía paquetes o bits aleatorios en el canal en el que está operando, poniendo a todos los demás nodos en ese canal en modos no operativos. Sin embargo, no cambia de canales y opera en un solo canal hasta que se agota su energía. Hay tres tipos básicos de jammers proactivos: constante, engañoso y aleatorio.

El jammer reactivo [3] comienza a bloquear (jamming) solo cuando observa que hay actividad en la red en un determinado canal. Como resultado, un jammer reactivo compromete la recepción de un mensaje. Puede interrumpir paquetes pequeños y grandes. Como tiene que monitorizar constantemente la red, el jammer reactivo es menos eficiente energéticamente que el jammer aleatorio. Sin embargo, es mucho más difícil detectar un jammer reactivo que un jammer proactivo, porque la relación de entrega de paquetes (PDR-packet delivery ratio) no se puede determinar con precisión en la práctica.

El bloqueo (jamming) de función específica se implementa al tener una función predeterminada. Además de ser proactivos o reactivos, pueden trabajar en un solo canal para conservar energía o bloquear (jamming) múltiples canales y maximizar el rendimiento del bloqueo (jamming) independientemente del uso de energía. Incluso cuando los jammers de función específica están bloqueando un solo canal a la vez, ellos no están fijos en ese canal y pueden

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 19 No. 3, Septiembre-Diciembre, 2020, p.23-37 ISSN 1729-3804

cambiar sus canales de acuerdo con su funcionalidad específica. Los llamamos inteligentes debido a su naturaleza de bloqueo eficiente y efectiva. El objetivo principal de estos jammers es aumentar su efecto de bloqueo en la red que intentan bloquear. Además, también se cuidan a sí mismos conservando su energía. En redes muy grandes colocan suficiente energía en el lugar correcto para obstaculizar el ancho de banda de comunicación para toda la red o una parte importante de ella. Cada bloqueador de este tipo puede implementarse como proactivo y reactivo, por lo tanto, híbrido.

4. TECNOLOGÍAS JAMMING Y ANTI-JAMMING (J/AJ)

Es importante comprender cómo los bloqueadores (jammers) desplegados por los enemigos pueden interrumpir las redes inalámbricas críticas, ya que pueden permitirnos mejorar la solidez de la red subyacente [4]. Si bien hay más tipos de tecnologías de comunicación (J/AJ) [5], las dos predominantes en el uso generalizado son el espectro ensanchado (SS) de secuencia directa (DSSS) y el espectro ensanchado de salto de frecuencia (FHSS). Un tercer tipo, llamado salto de tiempo (TH), también está disponible y, como técnica para lograr AJ, está comenzando a emerger como una técnica viable.

Los sistemas de espectro ensanchado de secuencia directa DSSS difunden la señal digital portadora de información a través de un ancho de banda amplio y ese ancho de banda completo se ocupa instantáneamente, es decir, la señal se extiende por todo el ancho de banda al mismo tiempo. Tomar una señal de datos de energía limitada y difundir esa energía a través de un ancho de banda muy amplio hace que la energía presente en cualquier frecuencia particular o banda de frecuencia pequeña, sea minúscula. A menudo es tan pequeña como para estar por debajo del ruido térmico a esa frecuencia. Los receptores que simplemente examinan el espectro a la frecuencia apropiada de operación de dichos sistemas de comunicación confundirán la señal como ruido y detectarán fallas. Se requiere un procesamiento de señal especial para extraer la señal.

A diferencia del DSSS, en los sistemas FHSS la señal de datos de banda estrecha en cualquier instante dado, ocupa un solo canal, generalmente de banda estrecha. En la banda baja de VHF, tradicionalmente la canalización de frecuencia ha sido de 25 kHz, aunque esta se está reduciendo. Por lo tanto, el sistema FHSS en cualquier instante está ocupando este ancho de banda. En la banda de baja frecuencia de VHF hay alrededor de 2.400 canales disponibles, y los sistemas generalmente están diseñados para utilizar algunos subconjuntos de estos.

En los sistemas de comunicación FHSS, la señal de información de banda estrecha modula una señal portadora, y la frecuencia de la señal portadora se cambia frecuentemente. Además de proporcionar un grado de baja probabilidad de intercepción (LPI) y baja probabilidad de explotación (LPE), los sistemas FHSS disfrutan de la ventaja de la diversidad de frecuencia, que ayuda a mitigar el desvanecimiento dependiente de la frecuencia y los trayectos múltiples. Una de las técnicas de codificación más simples para frecuencia de desplazamiento múltiple (MFSK) es dividir la energía de un símbolo (E_s), en m símbolos secundarios de igual energía, también llamados chips, y transmitir estos símbolos secundarios a diferentes frecuencias que saltan independientemente.

FHSS se puede dividir en espectro ensanchado por salto de frecuencia rápido (FFHSS) y espectro ensanchado por salto de frecuencia lento (SFHSS). Esta distinción normalmente se basa en la cantidad de bits de datos enviados en el tiempo de espera (dwell) de un salto particular. Si hay varios bits de datos en un salto, se llama SFHSS, mientras que, si hay varios saltos para cada bit de datos, se llama FFHSS. La línea divisoria entre SFHSS y FFHSS es un bit por salto o, equivalentemente, un salto por bit.

Para el salto rápido de frecuencia, la frecuencia de salto está determinada por L_F, donde cada uno de los símbolos secundarios de L_F representa un salto diferente y, por lo tanto, una frecuencia de salto diferente. La estructura de canal para FFHSS se ilustra en la Fig. 2. Cada bit de datos se transmite a varias frecuencias (en este caso, $L_F = 4$). Esto tiene varias ventajas. Su mayor desventaja en relación con SFHSS es la complejidad de la implementación. Para una comunicación de voz efectiva, generalmente se requieren 16,000 bps (aunque esto se está reduciendo con las técnicas modernas de codificación de fuente).

Para $L_F = 4$, como en este ejemplo, y suponiendo que se requieren algunos bits para la administración del sistema (aproximadamente 1,000 bps), la velocidad de datos del canal sería de aproximadamente 68,000 bps. Dependiendo de la modulación utilizada, esto podría causar que el ancho de banda del canal requerido, en muchas situaciones, sea demasiado grande para relaciones de señal a ruido SNR razonables. La Fig. 3 muestra la estructura del detector para sistemas BFSK -FFHSS no coherentes con la llamada decodificación de decisión difícil.

La estructura de canal para los sistemas SFHSS se muestra en la Fig. 4 y en la Fig.5 la estructura del detector del receptor para BFSK no coherente con decodificación de decisión difícil, múltiplo de la velocidad de datos R.

El rendimiento de un sistema BFSK de salto de frecuencia lento, en cualquier frecuencia dada, es el mismo que el rendimiento de un sistema BFSK que no está saltando. En este caso, en cada salto, se transmiten varios bits.

La estructura del detector de un receptor se muestra en la Fig. 5, que es un radiómetro incoherente. Esta estructura es similar a la del detector BFSK- FFHSS no coherente, excepto que faltan las sumas de las muestras de las frecuencias

de L_F en la salida. Se toma una decisión en cada bit sobre si se envió una marca o un espacio. Al pasar a través de los filtros de paso de banda hay ruido y posiblemente una señal de bloqueo provocada (jamming). Pasando a través de los filtros pasa banda está el ruido y también la señal en ese instante. Las salidas del filtro se detectan con un dispositivo de ley cuadrática y luego se muestrea formando las señales muestreadas r_{1k} y r_{2k}, k = 1, 2, …, L_S, donde L_S es el número de bits por salto. La muestra marca (MARK) se resta de la muestra espacial (SPACE) formando el test estadístico *z*. Si z es menor que cero, se declara marca, y si *z* es mayor que cero, se declara espacio.

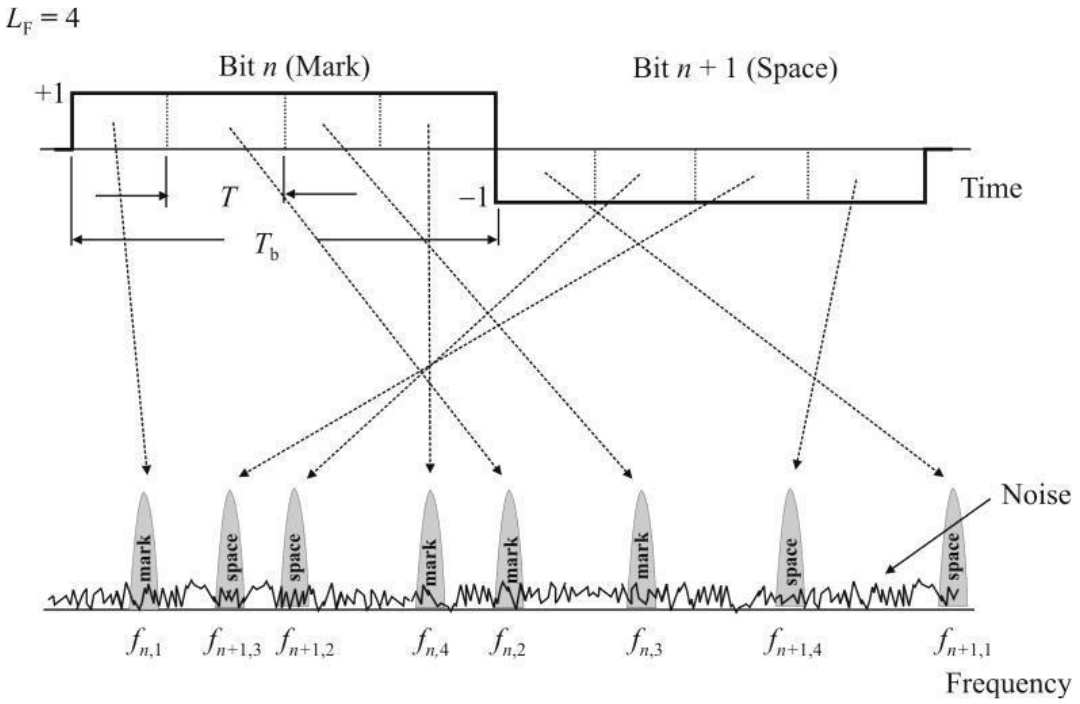

Figura 2: Estructura de canal con FFHSS [5].

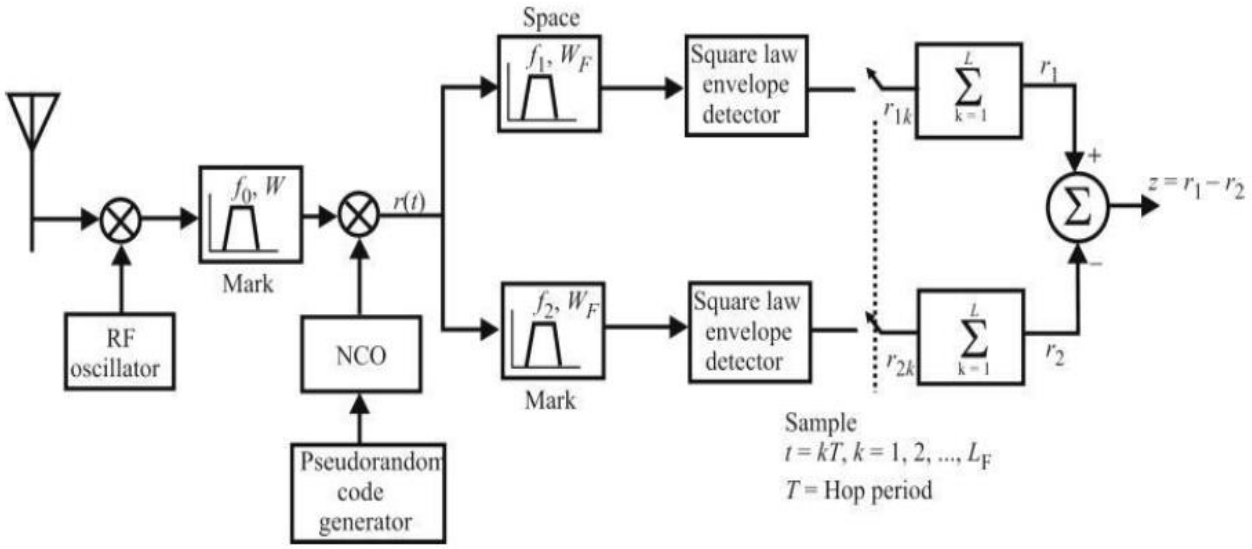

Figura 3: Receptor FFHSS y detector BFSK no coherente [5].

5. DETECCIÓN DE SEÑAL BLOQUEADORA

Se trata de inhibir o prevenir el bloqueo electrónico. La detección de señales tiene el propósito de controlar al atacante o "jammer". Los receptores de escaneo miden la energía en un ancho de banda (relativamente) estrecho mientras se sintonizan en un ancho de banda más amplio.

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 19 No. 3, Septiembre-Diciembre, 2020, p.23-37 ISSN 1729-3804

Hay dos tipos de estos receptores: barrido superheterodino, y barrido compresivo. El primero generalmente tiene un ancho de banda instantáneo mucho más estrecho que el segundo y, por lo tanto, una resolución de frecuencia más fina. Por otro lado, los segundos son considerablemente más rápidos que los primeros y, por lo tanto, poseen una probabilidad de detección mucho mayor cuando la sensibilidad y el rango dinámico no son problemas. Un receptor compresivo realiza una exploración rápida continua en un rango de frecuencia de interés [6].

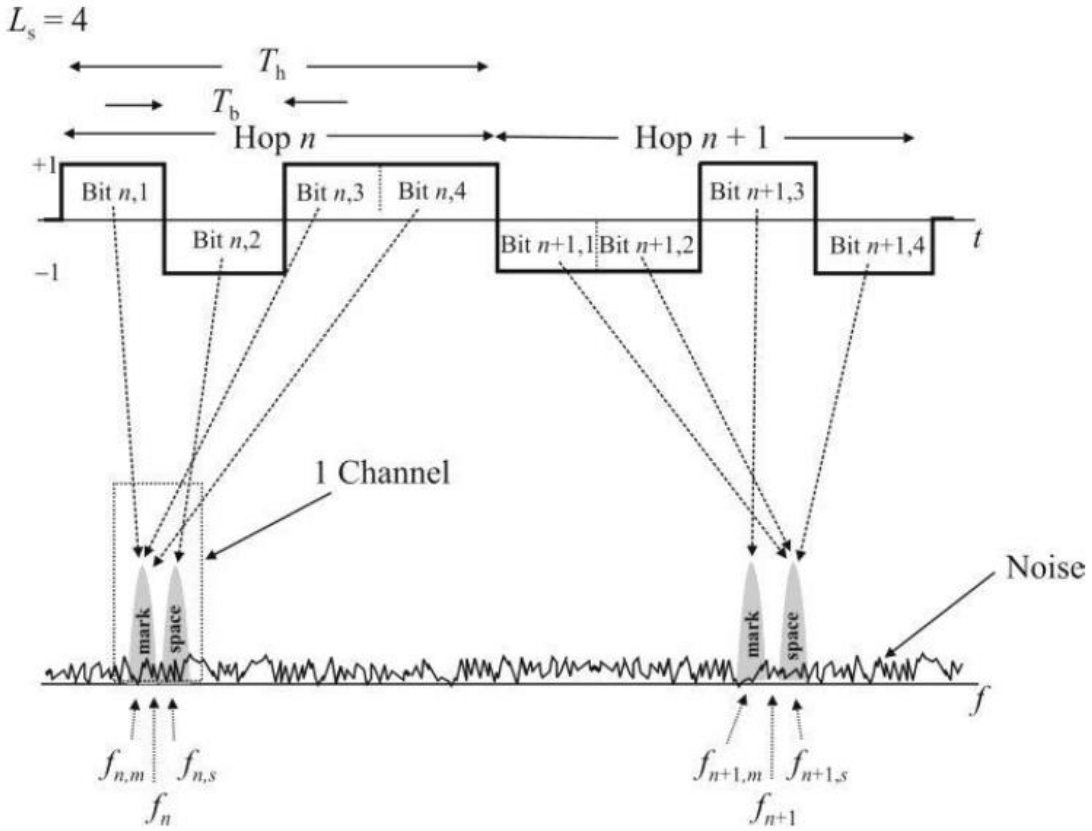

Figura 4: Estructura de canal para sistemas SFHSS [5].

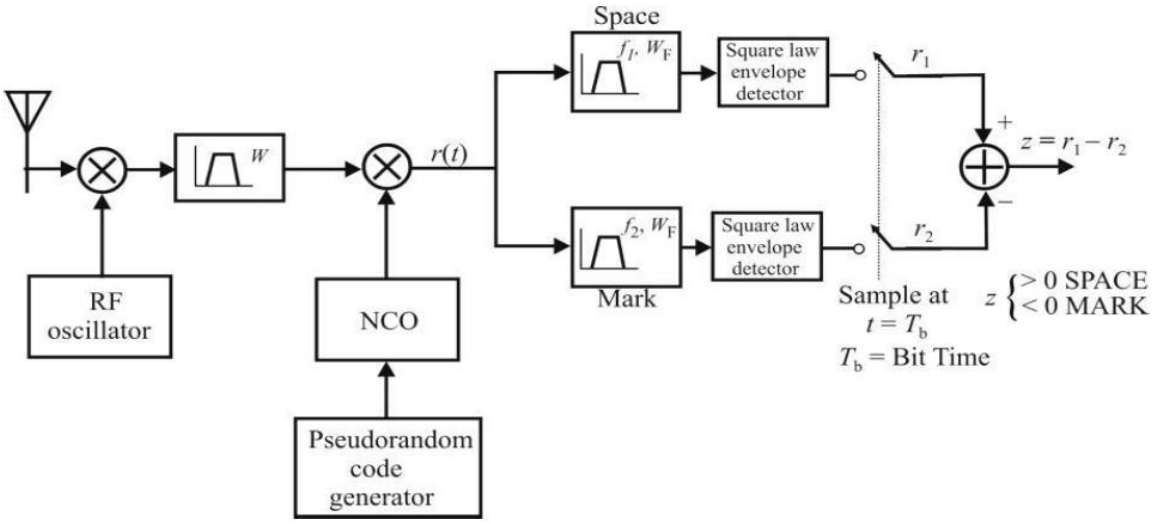

Figura 5: Estructura del receptor para BFSK no coherente [5].

En el caso de los sistemas de espectro ensanchado (SS), esa región de interés sería el ancho de banda de cada canal (W_{ss}) o una fracción sustancial de él. Estos receptores pueden barrer o escanear varios cientos de MHz en microsegundos, lo que facilita una alta probabilidad de rendimiento de detección.

Para detectar la presencia de una señal de FHSS, el combinador de banco de filtros (FBC) y el combinador de banco de filtros de banda parcial PB FBC son los métodos más comunes. Sin embargo, como ya se mencionó, simplemente detectar solo la presencia de señal rara vez es suficiente en espectros congestionados. Dado que el propósito de la detección es localizar a un jammer si hay una señal presente, casi siempre es necesario medir parámetros basados en la energía en el canal para realizar la decisión de salto.

La medición de los parámetros apropiados depende de alguna manera en determinar la frecuencia a la que el transmisor ha saltado. La banda de frecuencia completa sobre la cual los objetivos saltan se puede monitorizar simultáneamente con uno de los tipos de receptores ya mencionados. Una vez que se detecta nueva energía en alguna frecuencia, se deben realizar mediciones para determinar si ese es el objetivo de interés porque, por lo general, se producirán varias alarmas de energías nuevas si hay muchos objetivos presentes, que con asiduidad cambian de frecuencia. Por lo tanto, la "clasificación de la señal" (identificación del patrón de modulación) se vuelve importante.

Las arquitecturas específicas para estos receptores dependen del tipo de señal y el objetivo de detección. Para señales SFHSS, la detección óptima requiere buscar en todos los patrones de datos posibles, ya que muchos bits de datos están contenidos dentro de cada tiempo de espera (dwell). Por otro lado, para FFHSS, hay muchos tiempos de espera (dwells) por bit de datos y solo es necesario buscar sobre las posibles frecuencias de espera.

En general, ninguna de estas arquitecturas es prácticamente realizable. Sin embargo, ellas forman los casos limitantes de qué rendimiento es posible. Estas arquitecturas suponen que la información de época de temporización está disponible en el receptor y los tiempos de integración del receptor están alineados con ella. La arquitectura óptima del receptor para objetivos SFHSS (múltiples bits por salto) se ilustra en la Fig. 6, mientras que la de las señales FFHSS (múltiples saltos por bit) se muestra en la Fig. 7.

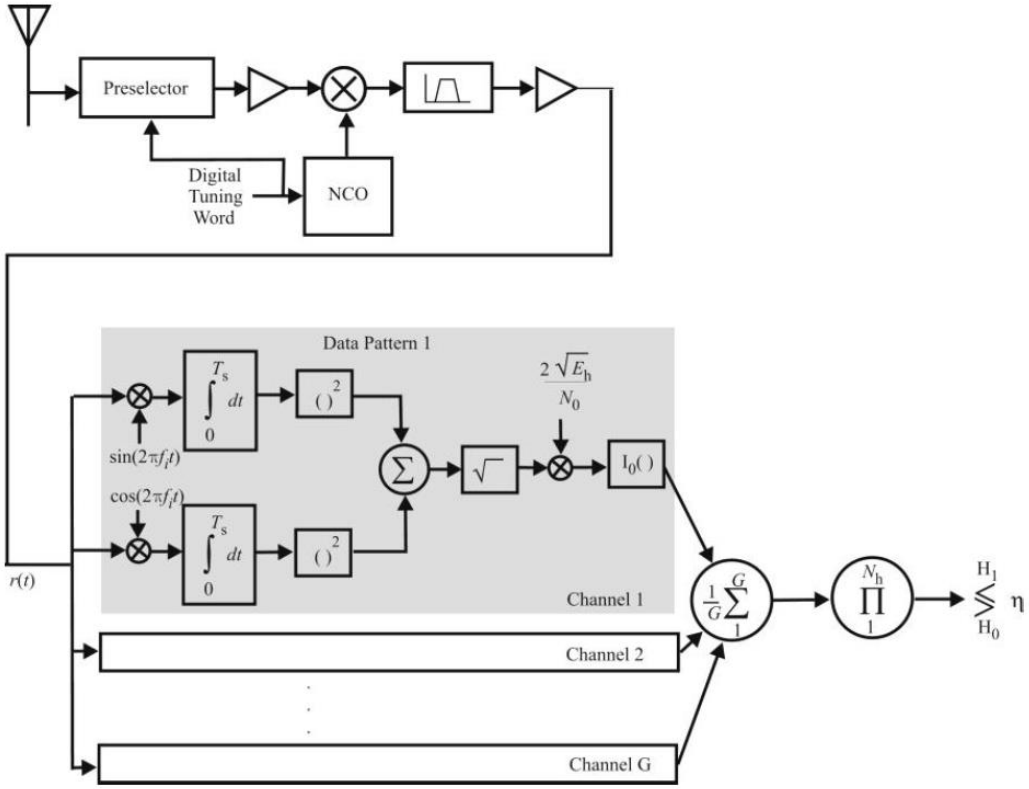

Figura 6: Arquitectura del receptor para clasificar señales SFHSS [5].

6. SISTEMAS DE COMUNICACIÓN ANTIJAMING (AJ)

Estrictamente hablando, la tecnología de comunicación AJ se refiere a la capacidad de combatir el jamming en un sistema de comunicación. Estar totalmente libre de los efectos del jamming de RF en un entorno de comunicación inalámbrica es un objetivo poco realista. Dadas las circunstancias apropiadas, todos los sistemas de RF pueden ser bloqueados. Las técnicas comunes para la implementación de AJ consisten en formas de ocultar una señal para que un interceptor o un intruso casual no sepa que la señal está allí, como por ejemplo moverla rápidamente en el espectro de frecuencia para que los receptores de intercepción de banda estrecha tradicionales no vean la identifiquen. Ya sea que la intención sea interceptar comunicaciones o negar la posibilidad de efectuar las mismas, en una relación de confrontación obviamente hay un interés por impedir el éxito de la comunicación.

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 19 No. 3, Septiembre-Diciembre, 2020, p.23-37 ISSN 1729-3804

Los sistemas de comunicación deben protegerse contra intercepciones no autorizadas o contra interrupciones o corrupción en entornos electromagnéticos complicados. En general, se utilizan tres categorías de seguridad para delinear los sistemas de comunicación inalámbrica, como se muestra en la Fig. 8, es decir, INFOSEC, COMSEC y TRANSEC [7]. La seguridad de la información (INFOSEC) es la que combate contra el acceso no autorizado o la modificación de la información; la seguridad de las comunicaciones (COMSEC) es la que mantiene seguras las comunicaciones importantes. La seguridad de transmisión (TRANSEC) es aquella que hace que sea difícil para alguien interceptar o interferir las comunicaciones. Para los usuarios no intencionados o intencionados, las estrategias básicas para apoderarse y paralizar a la víctima de la comunicación son detectar, interceptar, explotar y bloquear las señales de comunicación.

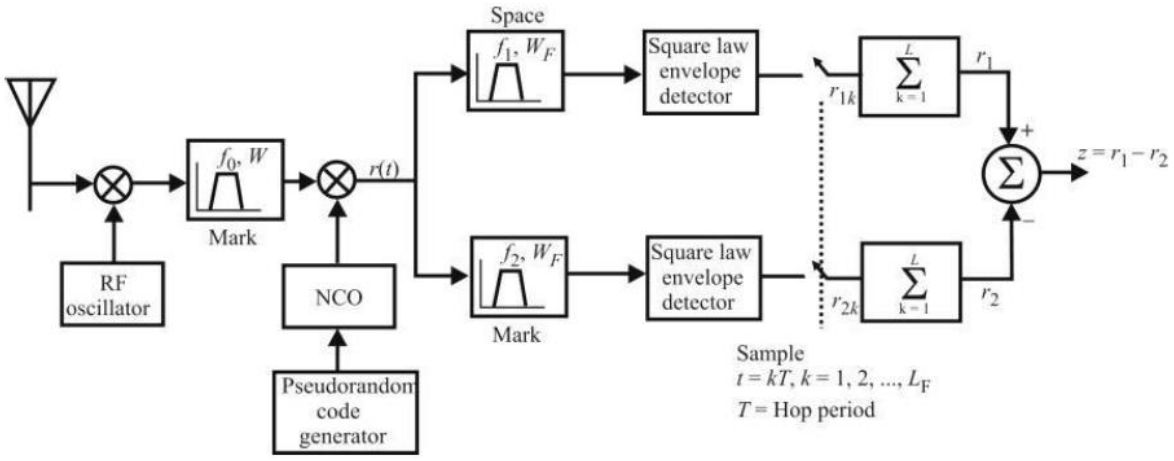

Figura 7: Arquitectura del receptor para clasificar señales FFHSS [5].

Para la víctima, las medidas básicas para contrarrestar estas estrategias son diseñar un sistema con capacidades de TRANSEC. Es decir, baja probabilidad de detección, intercepción y explotación (LPD / I / E), y con capacidad de seguridad de recepción, es decir, AJ o resistente al jamming.

En estas circunstancias como se mencionó anteriormente, no es sencillo realizar evaluaciones y decisiones sabias y prudentes para comunicaciones seguras con capacidades concurrentes de (AJ) y (LPD / I / E). Se necesita obtener un modelo de análisis y métricas para evaluar de manera efectiva un tipo especial de jammer, con detección en tiempo real (o casi concurrente), (escaneo o barrido pasivo) y capacidad de transmisión, (llamado repetidor o follow-on jammer) para un sistema de comunicación con salto de frecuencia (FH).

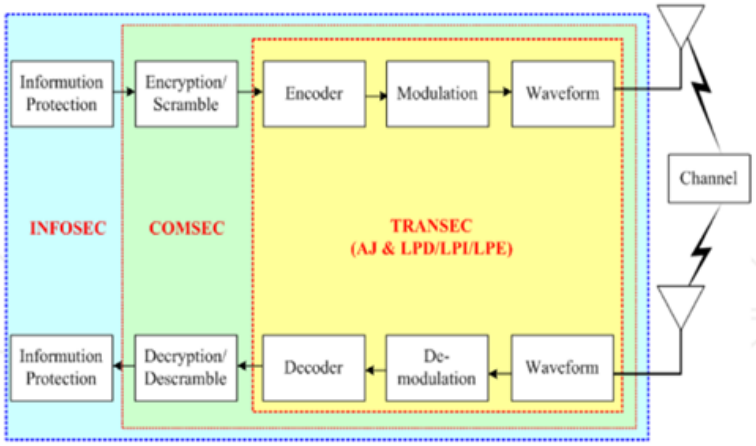

Figura 8: Esquema de seguridad de la comunicación inalámbrica [7].

Finalmente, en base a lo anterior, también se desea que esté disponible una técnica de detección de espectro como esta, especialmente para una comunicación (FH) por radio cognitivo (CR). La tecnología (CR) ha demostrado ser una solución tentadora para promover la eficiencia del espectro y aliviar los problemas de escasez de espectro. Sin embargo, la capacidad cognitiva no solo se puede realizar mediante la monitorización en algunas bandas de frecuencia de interés, sino que también se requieren técnicas más innovadoras para capturar los huecos del espectro con variaciones

temporales, frecuenciales o espaciales. Estas técnicas se aplican en entornos de radio sofisticados de espectro ensanchado de salto de frecuencia rápido (FFHSS), y evitan interferencias con los usuarios primarios (PU) existentes.

Hoy en día, los sistemas FHSS se han utilizado ampliamente en comunicaciones civiles y militares, pero sus beneficios se verían potencialmente neutralizados por un bloqueo de seguimiento (FOJ) con escaneo de banda ancha y capacidades de respuesta interferente que cubran el período de salto. El concepto (FOJ) es en realidad implícitamente análogo a una comunicación CR con características de conocimiento y ubicación del espectro, el concepto de detectar, aprender y luego actuar mediante la auto-reconfiguración de los parámetros de radio.

7. CAPACIDAD DE DETECCIÓN DEL ESPECTRO A TRAVÉS DE ESQUEMAS DE ESCANEO ESPECÍFICOS

En esta sección, investigaremos más a fondo un tipo de jamming especial con características de exploración y transmisión en tiempo real, es decir, capacidades de detección concurrente y de jamming, el cual está diseñado inherentemente para contrarrestar un sistema de comunicación por salto de frecuencia (FH). Este debería ser un buen objetivo de referencia para evaluar el rendimiento del sistema de espectro ensanchado (FHSS) teniendo en cuenta las características de transmisión y recepción simultáneamente. Además, se investigan las métricas de probabilidad de jamming efectivo para esquemas de exploración específicos (FOJ), que serán buenas cifras de mérito para evaluar el rendimiento del sistema de comunicación (FH) y (CR).

Modelo de probabilidad de jamming (FH)

La Fig. 9 muestra el diagrama de bloques básico de la función (FOJ) básica con los tiempos de proceso asignados para obtener señales "víctima" entrantes e implementar jamming. El parámetro jT_z es el tiempo analítico total necesario para obtener la frecuencia de salto, τ_r es el tiempo de activación total necesario para sintetizar y amplificar un tono de señal repetidora o ruido para bloquear (jam) la señal "víctima". Este tiempo está compuesto por los tiempos de proceso del sintetizador de frecuencia, amplificador de potencia y bancos de filtros.

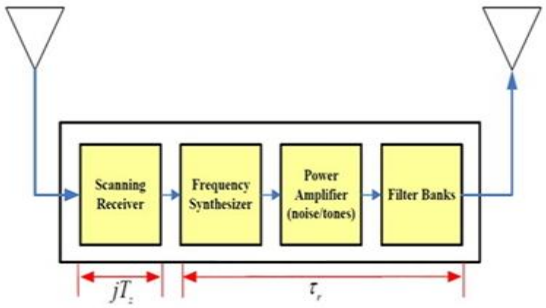

Figura 9: Diagrama de bloques de funciones de FOJ básico [7].

En general, los tiempos procesados para estos tres parámetros están en el orden de ms, μs, y ns (nanosegundos), respectivamente. Además, el retardo de propagación o el tiempo de diferencia (τ_d), que depende de las posiciones relativas, debe incluirse para un análisis de probabilidad de bloqueo efectivo (effective jamming).

Por ejemplo, si la diferencia de rango (ΔR) es de 30 km, el tiempo de diferencia de propagación τ_d será de alrededor de 100 μs, mucho más que el tiempo de respuesta τ_r. Por lo tanto, en esta circunstancia, se puede suponer que este parámetro es cero en comparación con otros parámetros más grandes. La Fig. 10 muestra el desglose efectivo del tiempo de permanencia del jamming para (FOJ).

De la Fig.10 podemos apreciar:

Tr representa el tiempo de retardo total del proceso de jamming y el tiempo de propagación (= $\tau_r + \Delta\tau d$), T_l describe el tiempo de latencia (= $jTz + T_r$) y T_j representa el tiempo de "permanencia efectiva" (effective dwell time) del jamming (= $T_h - T_l$), con lo cual

$$T_l = jT_z + (\tau_r + \Delta\tau_d) = jT_z + T_r, \quad (1)$$

$$T_j = T_h - (jT_z + T_r) = T_t - jT_z. \quad (2)$$

Las ventanas de escaneo disponibles durante el intervalo de espera de salto se definen como *m,* que se representa como:

$$m = \left|\frac{T_h - T_r}{T_z}\right| = \left|\frac{T_t}{T_z}\right| \quad (3)$$

donde T_z representa el tiempo de trama de análisis por ventana de exploración W_s del jammer. De ello se deduce que el FOJ puede analizar a lo sumo *m* ventanas de escaneo durante el intervalo de permanencia individual, T_h (single dwell interval). El número de ventanas de escaneo disponible en el ancho de banda del sistema F_H se define como *n* y se representa como:

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 19 No. 3, Septiembre-Diciembre, 2020, p.23-37 ISSN 1729-3804

$$n = \left|\frac{W}{W_s}\right|, \quad (4)$$

donde W representa el ancho de banda de salto de un sistema FH y W_s representa la ventana de exploración del jammer. Sea k el número de ventanas de exploración que el FOJ analiza en el intervalo de permanencia. Es evidente que:

$$k = min.(m, n), \quad (5)$$

lo cual significa que se selecciona el más pequeño de m o n como el número analizado de ventanas escaneadas. Supongamos que un sistema FH opera solo en el ancho de banda W y que el FOJ conoce los parámetros del sistema FH y también los momentos de cambios de canal.

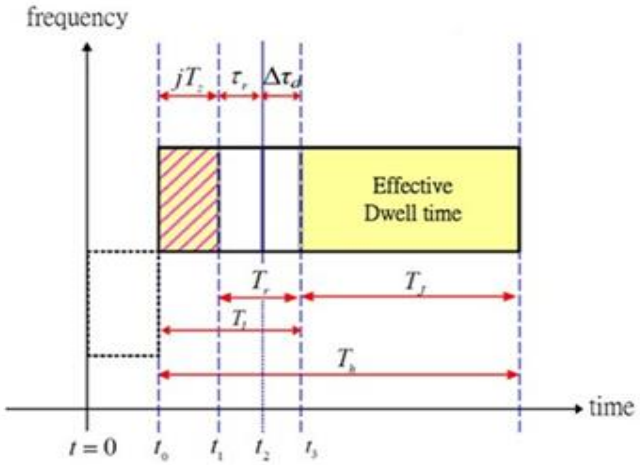

Figura 10: Tiempo de permanencia efectivo (T_J) y desglose del tiempo de latencia para la operación de la Unidad de Radio Cognitivo (CRU o CR node) [7].

Por lo tanto, exactamente en estos momentos ($t = 0$), el jammer iniciará la búsqueda del canal real. Cuando el terminal FH transmite en la ventana de exploración j-th, esta transmisión se encuentra en el momento $t_0 = jT_z$. Sea t_1 el momento en que el receptor de exploración encuentre el canal de transmisión real del sistema FH. Sea t_2 el momento en que el FOJ inicia el bloqueo del canal encontrado. Sea t_3 el momento en que la señal iniciada del FOJ llega al sitio del receptor del canal encontrado, es decir, el receptor FH está bloqueado en el momento t_3.

Modelos de escaneo

Se explorarán dos esquemas denominados escaneo o barrido uniforme y escaneo o barrido secuencial y se tomarán como medidas de escaneo, para escanear y rastrear las señales entrantes de salto de frecuencia, lo suficientemente rápido como para implantar ruido efectivo o bloqueo de tonos a partir de entonces. Además, también se examinará el caso de respuesta demorada ($T_r \neq 0$) para estos dos esquemas de exploración.

Esquema uniforme de escaneo (U-scan)

Se explorará y se utilizará una técnica de escaneo uniforme como la medida de escaneo, para escanear y rastrear las señales entrantes de salto de frecuencia, lo suficientemente rápido como para implantar señales de transmisión a partir de entonces. El CR node analiza todas las ventanas de exploración al azar, con probabilidad uniforme p_u (T_J) = 1 / n; y p_u (T_J) = (n-k) / n es la probabilidad de que el sistema FH opere en la ventana de escaneo que no se analiza. Después de una larga derivación de las ecuaciones, la relación de permanencia efectiva (h_u) y la tasa de exploración (R_{su}) para la técnica de exploración uniforme se pueden expresar mediante las siguientes ecuaciones:

$$h_u = \frac{\bar{T}_j}{T_h}, \quad (6)$$

$$R_{su} = \frac{W_s}{T_z}. \quad (7)$$

Esquema secuencial de escaneo

Se tomará un esquema de escaneo secuencial como medida de escaneo para escanear las señales de salto de frecuencia entrantes, de manera lo suficientemente rápida como para implantar, si es permisible, la señal de transmisión del CR node. Basado en las definiciones básicas como se mencionó anteriormente, si el CR node analiza todas las ventanas de exploración al azar con percepción secuencial p_s (T_J) = 1 / (n + 1-j), entonces p_s (T_J) = (n-k) / (n + 1-j) será la percepción no analizada en la ventana de escaneo. Por lo tanto, la relación de tiempo de permanencia efectiva (h_s) y la velocidad de exploración mediante un esquema de exploración secuencial se expresan mediante las ecuaciones (8) y (9), respectivamente.

$$h_s = \frac{\bar{T}_j}{T_h}, \tag{8}$$

$$R_{sh} = \frac{W_s}{T_z}. \tag{9}$$

La Fig. 11 muestra los resultados de comparación de la probabilidad efectiva de jamming (h) frente a la tasa de salto (R_h) para los esquemas de exploración uniforme (U-) y secuencial (S-). Bajo las mismas condiciones de tiempo de encuadre (T_z), se observa obviamente que el esquema de exploración *S* es mejor que el esquema de exploración *U* para una tasa de salto fija. Por ejemplo, el valor de probabilidad de bloqueo efectivo será de alrededor de 0.8 y 0.5 si R_h = 500Hz y T_z = 100 μs para el esquema de exploración S y U, respectivamente. Desde otro punto de vista, el esquema de exploración *S* tendrá una mejor capacidad de detección de velocidad de salto (650Hz) que el esquema de exploración *U* (500Hz) si la probabilidad efectiva de jamming se fija en 0.5.

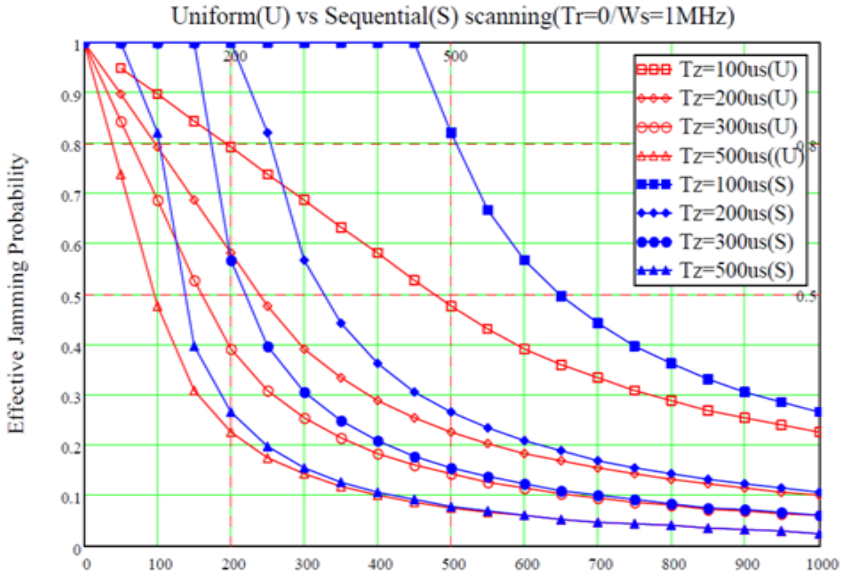

Figura 11. Probabilidad efectiva de bloqueo versus tasa de salto con valores de T_z especificados [7].

8. RENDIMIENTO ANTI-JAMING DE LAS REDES DE RADIO COGNITIVOS (CRN)

En esta sección, nos enfocamos en el rendimiento anti-jamming en un nodo de la Red con Radio Cognitivo CRN. Por un lado, los jammers pueden mejorar en gran medida su capacidad de bloqueo al explotar la tecnología de radio cognitivo, especialmente las funciones flexibles de capa física (PHY) y capa (MAC). Por el contrario, el CR node puede volverse más susceptible a los ataques de jamming debido a algunos requisitos únicos en la capa física y MAC, como el requisito de desocupación del canal al detectar cualquier señal de usuario primario (PU). Por otro lado, la capacidad de saltar entre muchos canales le da al CR node una ventaja única de mejorar su rendimiento anti-jamming. Por lo tanto, el rendimiento anti-jamming es un tema de investigación nuevo e interesante en las redes (CRN).

Modelo de transmisión CR node y modelo jammer

Como se muestra en la Fig. 12, una transmisión típica de un CR node implica la transmisión de un paquete de datos (en un intervalo de datos) seguido de un período de sensado del usuario primario (PU) (en un intervalo de sensado). Si el PU se detecta como ausente, el nodo continúa usando este canal; de lo contrario, el CR node cambia a otro canal. Si la transmisión de un paquete de datos está bloqueada, el CR node iniciará el cambio de canal a través de una secuencia de sincronización, configuración de canal, protocolo de enlace y procedimiento de configuración de red, antes de que el paquete de datos pueda transmitirse nuevamente. El CR node puede tener muchos canales para seleccionar, dependiendo de la actividad del PU. La gran cantidad de canales es una de las principales ventajas del CR node para combatir el bloqueo.

Hacemos las siguientes suposiciones sobre el jammer. 1) El jammer utiliza dispositivos que tienen capacidades similares a los CR nodes, incluido el sensado del espectro y el transceptor RF. El jammer podría utilizar varios dispositivos de jamming, dependiendo de qué tan fuerte sea el atacante o qué costo el jammer está dispuesto a pagar para bloquear la comunicación. 2) Cuando el CR node cambia a un nuevo canal, tomará algún tiempo para que un jammer sense el espectro y descubra qué canal está usando este CR node. Específicamente, si este período de tiempo es más largo que el período de tiempo que el CR node pasa en un canal, entonces la única alternativa para el jammer es seleccionar aleatoriamente canales para bloquear. Por lo tanto, la velocidad de conmutación de canales del CR node afecta directamente su capacidad anti-jam mientras al mismo tiempo afecta la eficiencia de su ancho de banda de transmisión. 3) También asumimos que los jammers no conocen las claves secretas que el CR node está utilizando para la selección y comunicación de canales.

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 19 No. 3, Septiembre-Diciembre, 2020, p.23-37 ISSN 1729-3804

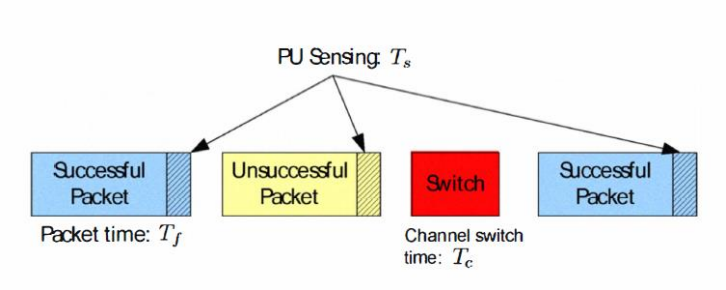

Figura 12. Ilustración de una sesión de transmisión de un CR node [8].

Suponemos que el jammer o bloqueador tiene la misma potencia de transmisión $P_J = P_s$ que el CR node. Hay varias formas para que el jammer realice bloqueo o jamming, desde el bloqueo convencional (que utiliza toda la potencia de transmisión para bloquear un canal) hasta enfoques de bloqueo o jamming más inteligentes. Por lo general, el jammer no conoce el canal utilizado por el CR node, por lo que tiene que bloquear aleatoriamente algunos de los canales. Además, el jammer puede usar el cambio rápido de canales para bloquear más canales dentro de una ranura, pero a un nivel de señal de bloqueo relativamente más bajo. El número total de canales que puede transmitir un jammer depende de la relación entre la longitud del intervalo de datos y la longitud del intervalo de bloqueo. Obviamente, al bloquear simultáneamente más canales, es más probable que el jammer golpee el canal utilizado por el CR node, pero el CR node sufrirá menos bloqueo o jamming. Convencionalmente, el bloqueo es exitoso solo si la señal a interferencia más la relación de ruido (SINR) del CR node es menor que cierto umbral. Por lo tanto, el número de canales bloqueados simultáneamente no puede ser demasiado grande en la práctica.

Sin embargo, un jammer inteligente puede bloquear / interferir selectivamente solo la ranura de detección del PU. Mientras la señal de bloqueo emitida a la ranura de detección del PU haga que la SNR sea mayor que el umbral de detección, el CR node debe desocupar el canal y cambiar a uno nuevo.

Tipos de estrategia de jamming

Por lo tanto, hay tres estrategias típicas de bloqueo para el jammer: J1 Estrategia de fuerte bloqueo donde el propósito es bloquear completamente cualquier transmisión; J2 Estrategia de bloqueo ligero donde el propósito es inyectar una leve señal en el período de tiempo de sensado del canal para hacer que el CR node cambie de canal; J3 Estrategia de bloqueo inteligente donde el propósito es bloquear tanto las ranuras de sensado del canal como la de cambio de canal.

En general, el desempeño del CR node viene dado por el Rendimiento del Nodo y por la Probabilidad de Bloquear K veces el canal correcto del CR node. Para evitar una tediosa derivación de fórmulas, solo utilizaremos las expresiones de estos dos parámetros.

Rendimiento del CR node bajo una estrategia de fuerte bloqueo

En este caso, el Rendimiento de la transmisión del CR node se reduce a:

$$R = \frac{1-P[J]P[\gamma<\Gamma_0]}{1+\frac{T_c}{T_f}P[J]\,P[\gamma<\Gamma_0]}. \tag{10}$$

La Probabilidad de Bloquear K veces el canal correcto del CR node es:

$$P[J] = 1 - \sqrt[\frac{T_f}{T_j}]{\left(1 - \frac{M_w\,(1-p_{jf})\,(1-p_{cf})}{M_c\;M_j}\right)}\,, \tag{11}$$

donde P_s es la potencia de transmisión del CR node (más exactamente, la potencia de la señal recibida en el receptor del CR node), P_J es la potencia de transmisión del jammer (o más exactamente, la potencia de la señal de bloqueo recibida por el receptor del CR node), N es ruido, T_f es el período de tiempo de transmisión del CR node, y T_J es el período de tiempo de bloqueo.

Como se muestra en la Fig. 12, consideramos una sola sesión de la transmisión del CR node donde este conduce la transmisión de datos durante T_f segundos a la velocidad de datos unitaria. Si no está bloqueado, continúa realizando otra sesión de transmisión. Si está bloqueado, entonces el CR node necesita pasar otro tiempo T_c para cambiar a un nuevo canal y retransmitir el paquete de datos usando otra sesión con una duración T_f. Dado que el jammer normalmente no puede seguir perfectamente la conmutación de canales del CR node, podemos suponer razonablemente que esta próxima sesión de transmisión será exitosa.

Rendimiento del CR node bajo estrategia de bloqueo ligero

Aquí, consideramos otra posible estrategia de bloqueo del jammer, es decir, la Estrategia J2: el jammer utiliza una pequeña potencia de transmisión para bloquear el CR node. Aunque el poder de bloqueo es muy pequeño y

normalmente no impide la transmisión exitosa del paquete de datos, de toda manera hará que el CR node cambie de canal, ya que los CR nodes pueden tomar la señal de bloqueo como la señal del usuario primario (PU).

Considere la sesión de transmisión del CR node como se muestra en la Fig. 12. Cada ranura de paquete de datos tiene transmisión durante T_f. Al final de cada ranura de transmisión de paquetes de datos, hay una pequeña ranura T_s utilizada para que el CR node realice el sensado del espectro para ver si hay un usuario primario (PU) activo. Si se detecta el usuario primario, este canal debe quedar vacante. El tiempo de cambio de canal T_c puede ser corto o largo, dependiendo de la realización del sistema. Por ejemplo, un tiempo de desocupación de canal típico es inferior a 0,5 segundos. En un escenario de comunicación normal, dado que el usuario primario puede volverse activo en un canal previamente vacante con muy baja probabilidad, la conmutación de canales también ocurre con una probabilidad extremadamente baja. Como resultado, incluso si la longitud de la ranura del paquete de datos T_f es pequeña, mucho menor que el tiempo de conmutación T_c, la reducción del rendimiento sigue siendo muy pequeña. Sin embargo, en caso de bloqueo, será completamente diferente, ya que el objetivo del bloqueo es tratar de aumentar la frecuencia de cambio de canal.

Suponemos que la SNR de comunicación requerida del CR node es Γ_0, que también es el nivel máximo de bloqueo que puede crear el jammer. También suponemos que la sensibilidad de sensado mínima del CR node (para detectar al usuario primario) es una SNR de Γ_{min}. Por lo general, $\Gamma_{min} \ll \Gamma_0$. También suponemos que el jammer no puede bloquear el procedimiento de conmutación de canales, porque los CR nodes pueden simplemente saltarse cualquier bloqueo durante esta fase, o esta fase es conducida por alguna transmisión especial de espectro ensanchado, por lo que la interferencia a los usuarios primarios es baja. Durante un período de tiempo fijo T, el jammer tiene una energía de transmisión total P_sT x 1 (potencia de transmisión CR node por longitud de paquete de datos por un canal). Como el jammer puede usar una potencia de transmisión más baja en este caso, puede bloquear múltiples canales en lugar de un canal. Además, es posible que no necesite permanecer en el mismo canal durante todo el período del paquete, sino que permanecerá en el mismo conjunto de canales solo por el tiempo T_J, donde el tiempo de bloqueo es $T_J \ll T$.

Además, dado que consideramos solo el caso de potencia de bloqueo extremadamente baja, la energía de bloqueo gastada en la fase de transmisión del paquete de datos generalmente no importa. Lo que importa es la energía de bloqueo gastada dentro de T_s. Como resultado, generalmente no tiene sentido que el jammer bloquee el mismo canal durante demasiado tiempo (de hecho, se puede demostrar que un bloqueo de tiempo más corto es mejor que un bloqueo de tiempo prolongado en este caso). Por lo tanto, suponemos que:

$$T_j < T_s, \tag{12}$$

con lo cual el número total de canales G que el jammer puede bloquear simultáneamente se obtiene a partir de la siguiente ecuación:

$$P_j T_j G \leq P_s T, \tag{13}$$

donde P_J es la potencia de bloqueo por canal, T_J es el período de bloqueo por canal, P_s es la potencia de transmisión más alta del CRN y del jammer, T es una longitud de ranura.

Rendimiento del Nodo CR node bajo estrategia de bloqueo inteligente

Aquí, consideramos otra posible estrategia de bloqueo del jammer, es decir, la Estrategia J3: el jammer utiliza una potencia de transmisión de nivel medio para bloquear el CR node. El objetivo es bloquear la ranura de detección del espectro y la ranura de conmutación de canales. Al inyectar una señal de bloqueo en la ranura de detección de canal, el CR node tendrá que realizar una conmutación de canal, lo que le hace desperdicia tiempo y reduce su rendimiento. Esto es similar al caso J2. Sin embargo, en esta nueva estrategia de bloqueo, el jammer también intenta bloquear el procedimiento de cambio de canal. Aquí el objetivo es bloquear el comienzo del procedimiento de conmutación de canales para romper el protocolo de enlace realizado por los CR nodes. Como sabemos, este intercambio es fundamental para los CR nodes porque pueden tener un conocimiento asimétrico sobre los canales disponibles. Con anterioridad vimos que, la longitud de la ranura del conmutador de canal T_c puede ser pequeña. Pero si esto se bloquea con éxito, el CR node tiene que usar un procedimiento más lento para reiniciar las comunicaciones. Por lo tanto, tenemos que introducir una longitud de ranura de conmutación de canal mucho mayor T_w en este caso.

9. RESULTADOS DE LAS SIMULACIONES

Aquí, se simulan los resultados de los análisis derivados anteriormente. Además, se simulan los dos sistemas de redes CRN típicas, a través del análisis de sus CR nodes: Cl. El sistema comercial IEEE 802.22 que explota los agujeros del espectro en los canales de transmisión de TVD (TV White Spaces); C2 El sistema militar XG (Next Generation) de DARPA.

El primer sistema presenta una trama de datos larga T_f, ranuras de conmutación de canal largas T_c, T_w y un número menor de canales disponibles M_w. Por otro lado, el segundo sistema presenta una trama de datos corta T_f, una gran cantidad de canales M_w disponibles y ranuras de conmutación de canales relativamente cortas T_c, T_w. Tengamos en cuenta que la diferencia entre T_c y T_w depende de si la comunicación de control entre los CR nodes está bloqueada o no. Si no está bloqueada, el tiempo de cambio de canal es relativamente corto, o sea T_c. Si esta comunicación de

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 19 No. 3, Septiembre-Diciembre, 2020, p.23-37 ISSN 1729-3804

control está bloqueada, entonces debido a la información asimétrica sobre los canales disponibles entre los CR nodes, la duración del tiempo de conmutación del canal T_w será mucho mayor.

Denotamos los sistemas similares al IEEE 802.22 como "CR Modelo 1", mientras que el sistema similar XG como "CR Modelo 2". Al simular estos dos modelos CR nodes diferentes, podemos ver fácilmente cómo los parámetros del protocolo CR node afectan el rendimiento anti-jamming bajo diversas estrategias de bloqueo.

Para el Modelo 1 de CR, utilizamos los siguientes parámetros: M = 10, M_w = 5, $p_{jf} = P_{jp} = P_{cf} = P_{cp}$ = 0.05, T_f = 60, T_w = 30, T_c = 0.5, T_s = 0.025, Γ_0 = 15dB, Γmin = -15 dB, G = 10, P_s = -80 dBm, N = -100 dBm. En todas las simulaciones, la duración del intervalo de bloqueo T_J es variable. Derivamos el rendimiento y la probabilidad de bloqueo con varios T_J. De esta manera, podemos ver la importancia de que el jammer seleccione los mejores parámetros de bloqueo además de la estrategia de bloqueo. En el primer experimento, simulamos los dos modelos de CR nodes bajo la estrategia de bloqueo J1. Los resultados se muestran en la Fig. 13 (a) y (b).

En el primer experimento, simulamos los dos modelos de CR nodes bajo la Estrategia J1 de Jamming. Los resultados se muestran en la Fig. 13. Las curvas marcadas como "teoría" denotan resultados de análisis teóricos, calculados por las ecuaciones (12) y (13). Las curvas marcadas como "sim" denotan los resultados de la simulación, o los resultados obtenidos mediante la simulación de un gran número de sesiones de transmisión de CR nodes en las sesiones de bloqueo. De la Fig. 13, podemos ver claramente que los resultados del análisis coinciden bien con los resultados de la simulación, lo que indica la validez de las expresiones de análisis. Además, a partir de la figura, podemos ver claramente que, al usar una gran cantidad de canales, el CR node puede mitigar efectivamente los bloqueadores con la estrategia de bloqueo J1, ya que el rendimiento normalizado es casi unitario, mientras que la probabilidad de bloqueo es casi 0. Esto significa que la transmisión es confiable incluso si hay múltiples bloqueadores en lugar de un bloqueador como lo analizamos y simulamos.

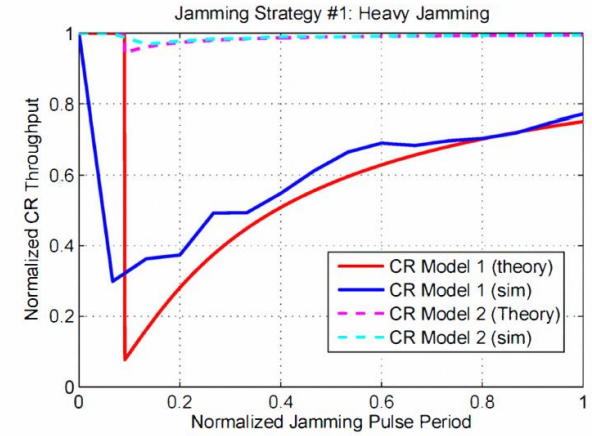

Fig.13 (a). Rendimiento CR node con estrategia de bloqueo J1 [8].

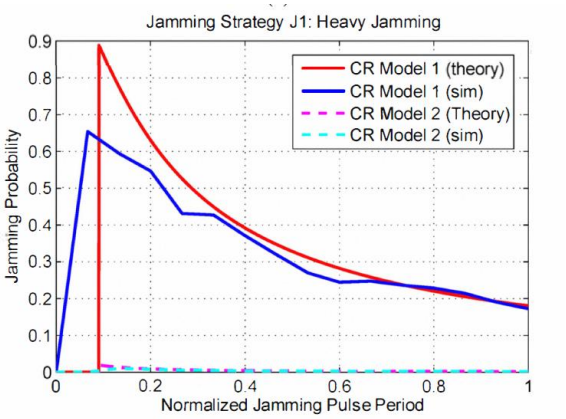

Fig.13 (b). Probabilidad de bloqueo con estrategia de bloqueo J1 [8].

Por otro lado, si el número de canales es pequeño, la transmisión se puede bloquear con éxito siempre que la longitud de la ranura de bloqueo del jammer se elija con cuidado. De hecho, con múltiples jammers, es bastante flexible que los jammers elijan sus longitudes de ranura de bloqueo. Desde el punto de vista del jammer, la estrategia de fuerte bloqueo J1 puede no ser una buena estrategia de jamming.

En el segundo experimento, simulamos los dos modelos de nodes bajo la Estrategia J2 de Jamming. Los resultados se muestran en la Fig. 14. Aunque la probabilidad de bloqueo es alta (lo que significa que con alta probabilidad el jammer puede inyectar señales de bloqueo en los canales utilizados por el CR node), el rendimiento puede no reducirse demasiado para el CR node modelo l. Sin embargo, el CR node modelo 2 puede bloquearse fácilmente en este caso. Esto puede explicarse porque toda la transmisión de datos puede pasar, y el único efecto de reducción del rendimiento se debe al procedimiento de cambio de canal.

Dado que el modelo 1 de CR node tiene una longitud de ranura de datos relativamente larga, pero una longitud de ranura de conmutación de canal relativamente pequeña, su rendimiento puede no verse gravemente afectado. Esto es completamente diferente del modelo 2 de CR node, donde la longitud de la ranura de datos es pequeña. Téngase en cuenta que se supone que el CR node siempre puede encontrar un canal al cual desalojar, incluso para el modelo 1 de CR node con un pequeño número de canales a los que saltar.

Este resultado indica la importancia de optimizar las longitudes de ranura de varias ranuras de la capa MAC. Esto también indica que el ataque de emulación de usuario primario (PUE) convencional se puede tratar fácilmente ajustando las longitudes de las ranuras, siempre que siempre haya canales de reserva para usar.

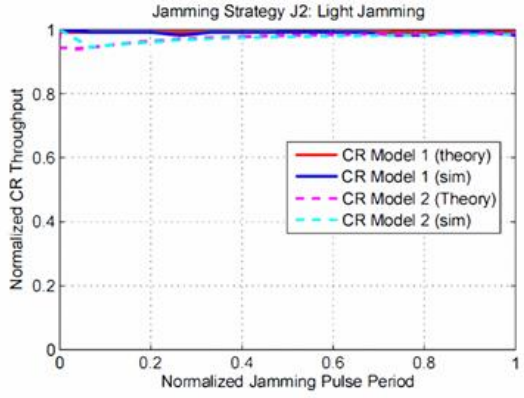

Fig.14 (a). Rendimiento CR node con estrategia de bloqueo J2 [8].

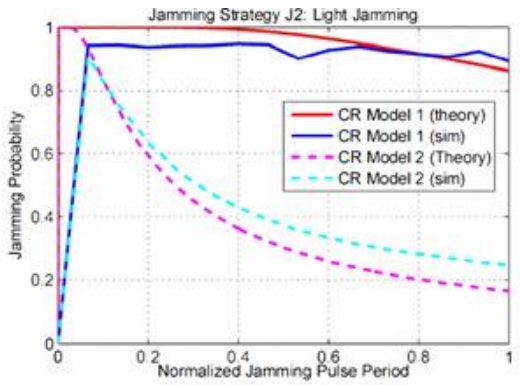

Fig.14 (b). Probabilidad de bloqueo con estrategia de bloqueo J2 [8].

En el tercer experimento, simulamos los dos modelos de CR nodes bajo la Estrategia de bloqueo inteligente J3. Los resultados se muestran en la Fig. 15. A partir del resultado, podemos ver claramente que esta es la mejor estrategia de bloqueo en términos de los jammers, ya que ninguno de los modelos puede tener transmisiones confiables siempre que el jammer elija el período de bloqueo adecuadamente. De la figura, podemos ver que un solo jammer puede hacer que ambos modelos de CR nodes reduzcan su rendimiento al 50% -70%. Por lo tanto, algunos jammers pueden bloquear fácilmente las transmisiones de los CR nodes. Aquí es cuando el CR node realmente puede sufrir bloqueos, lo que indica que el diseño anti-jamming es un problema difícil para el CR node.

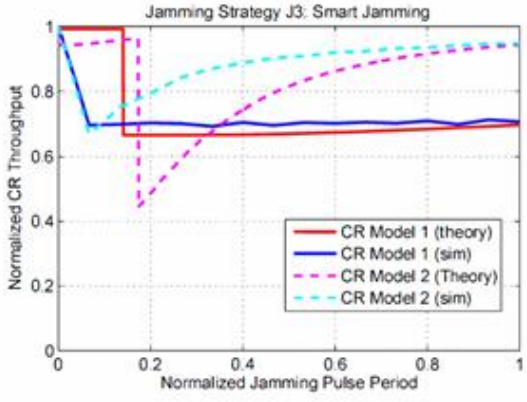

Figura 15 (a). Rendimiento CR node con estrategia de bloqueo J3 [8].

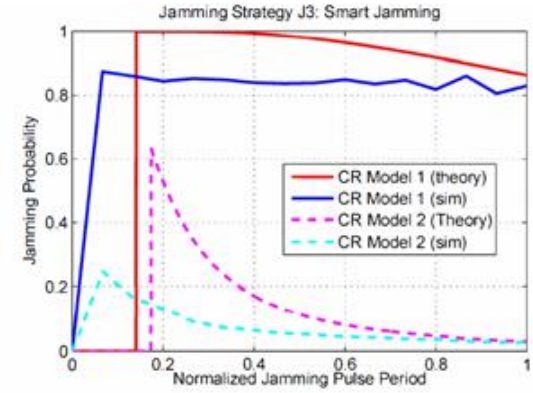

Figura 15 (b). Probabilidad de bloqueo con estrategia de bloqueo J3[8].

10. CONCLUSIONES

En este artículo presentamos técnicas de bloqueo y anti-bloqueo (anti-jamming) en redes inalámbricas. Creemos que hemos contribuido clasificando y resumiendo varios enfoques y discutiendo temas de investigación abierta en este campo. Arístides Mpitziopoulus propone, en su artículo ¨An effective defensive node against jamming attacks in sensor networks¨, la utilización de forma híbrida de las técnicas de espectro extendido de secuencia directa (DSSS) y el espectro extendido de salto de frecuencia (FHSS). DSSS utiliza un ancho de banda más amplio para la transmisión de señal, mientras que FHSS proporciona evitar las interferencias.

Existe un esquema híbrido DSSS y FFHSS, llamado nodo Hermes [9], para tratar los ataques de interferencia en las redes de sensores. El nodo Hermes realiza 1,000, 000 saltos por segundo (FHSS) para evitar los bloqueadores de seguimiento rápido (FOJ). DSSS se utiliza para hacer que el atacante detecte las señales de datos como ruido blanco, lo que evita que el atacante detecte la banda de radio de comunicación. El nodo Hermes usa 55 canales de frecuencia para FHSS y 275MHz de ancho de banda para espectro ensanchado en DSSS. Este tipo de configuración es un reto para el desempeño y seguridad del Radio Cognitivo (CR).

Los resultados indican que el anti-jamming es una tarea desafiante para el CR node. El CR node necesita usar más canales y mejorar la capacidad anti-jamming del procedimiento de detección del PU para mitigar los ataques de interferencia.

Revista Telemática. Vol. 19 No. 3, Septiembre-Diciembre, 2020, p.23-37 ISSN 1729-3804

REFERENCIAS

[1] USA Congressional Research Service. "Defense Primer: Electronic Warfare". www.crs.gov | 7-5700. September 2019.

[2] Grover, Kanica; Lim, Alvin; Yang, King. "Jamming and anti-jamming techniques in wireless networks: a survey". International Journal of Ad Hoc and Ubiquitous Computing. Volume 17 Issue 4, December 2014.

[3] Lichtman, Marc; Clancy, T. Charles; Reed, Jeffrey H. "Reactive Jammer Piggybacking: Achieving Antifragile Electronic Warfare". Milcom - Waveforms and Signal Processing. IEEE 2016.

[4] SaiDhiraj Amuru, Member, IEEE; Harpreet S. Dhillon, Member, IEEE; Buehrer, R. Michael, Senior Member, IEEE. "On Jamming Against Wireless Networks". Transactions on Wireless Communications. 2016.

[5] Poisel, Richard. "Modern Communications. Jamming Principles and Techniques". Artech House. 2011.

[6] Nawaz, Tassadaq; Marcenaro, Lucio; Regazzoni, Carlo S. "Cyclostationary-based jammer detection for wideband radios using compressed sensing and artificial neural network". International Journal of Distributed Sensor Networks. Vol. 13(12). 2017.

[7] Wang, Cheng-Xiang, "Adaptation from Transmission Security (TRANSEC) to Cognitive Radio Communication, Advances in Cognitive Radio Systems". INTECH. Croatia. 2012.

[8] Xiaohua, Li; Wednel, Cadeau. "ANTI-JAMMING PERFORMANCE OF COGNITIVE RADIO NETWORKS". State University of New York at Binghamton. 2011.

[9] Kirti, Sharma; Shobha, Bhatt. "Jamming Attack – A Survey". International Journal of Recent Research Aspects. ISSN: 2349-7688, Vol. 5, Issue 1, March 2018, pp. 74-80

CONFLICTO DE INTERESES

No hay conflicto de intereses con ninguna institución.

SOBRE EL AUTOR

Nacido en La Habana, el 9 de mayo de 1943. Graduado como Ingeniero Eléctrico de la Universidad Tecnológica de La Habana (CUJAE) en 1968. Graduado de Maestría en Ciencias en 1977, en la especialidad de Telecomunicaciones, de las Universidades CUJAE y Toronto, identificador ORCID 0000-0002-5546-3497. En 1980 fue nombrado Director de Ciencia y Técnica del MINCOM y Constructor Principal por la República de Cuba del Sistema Único de Medios Digitales de Conmutación y Transmisión del COMECOM. Investigador Titular desde 1982. Entre 1982 y 1990 fue tutor de múltiples tesis de ingeniería o maestría en ciencias, y publicó numerosos artículos sobre las telecomunicaciones, estudios empresariales o macroeconomía. En 1998 fue honrado con la Distinción de Cuadro Destacado del Estado y el Gobierno de la República de Cuba. Entre 1990 y 2003 fue nombrado Director General de la primera compañía celular cubana: CUBACEL. Ha participado como orador en múltiples eventos científicos internacionales y nacionales, relacionados con la UIT, las Naciones Unidas, el Banco Mundial y el COMECOM. Ha obtenido múltiples premios nacionales e internacionales. Actualmente es Investigador Titular del Instituto de Investigación y Desarrollo de Telecomunicaciones ¨LACETEL¨.

CONTRIBUCIONES DE LOS AUTORES

Este trabajo fue conformado por un único autor con la totalidad del contenido aquí presente a su cargo.