Detección Robusta por Grupos de Señales Primarias en Redes de Radio Cognitiva

Mercedes Jiménez Blasco
Internet Interdisciplinary Institute
Universitat Oberta de Catalunya
Email: mjimenezbl@uoc.edu

José Mut Rojas
Internet Interdisciplinary Institute
Universitat Oberta de Catalunya
Email: jmutr@uoc.edu

Helena Rifà-Pous
Internet Interdisciplinary Institute
Universitat Oberta de Catalunya
Email: hrifa@uoc.edu

***Resumen*—La radio cognitiva es una tecnología inalámbrica propuesta para usar eficientemente los recursos del espectro radioeléctrico permitiendo así reducir la carga existente en las bandas de frecuencia de uso libre. Las redes de radio cognitiva son capaces de escanear el espectro y adaptar sus parámetros para operar en las bandas no ocupadas. Para evitar interferir con usuarios con licencia que operan en un determinado canal, la sensibilidad de las redes tiene que ser muy alta. Ello se consigue con métodos de detección cooperativos. Los métodos de detección cooperativa actuales tienen una carencia de robustez ya sea frente a ataques puntuales o continuos. En este artículo presentamos un método de fusión por grupos que tiene presente el comportamiento de los usuarios a corto y largo plazo. Al realizar la fusión de los datos, el método se basa en dar mayor peso a los grupos de usuarios con mayor unanimidad en sus decisiones. Los resultados de las simulaciones prueban que en presencia de atacantes el método de fusión por grupos propuesto consigue una detección superior a otros métodos, cumpliendo los requisitos de sensibilidad mínimos de las redes de radio cognitiva incluso con un 12 % de usuarios reiteradamente maliciosos o un 10 % de atacantes puntuales.**

I. Introducción

Los numerosos servicios de redes inalámbricas disponibles hoy en día han producido un aumento en la demanda de espectro radioeléctrico. Los recursos de espectro son limitados y están controlados por agencias gubernamentales que otorgan licencias para su uso. Sólo una pequeña parte del espectro se puede usar de forma libre, y esta banda está cada día más sobrecargada. Por contra, el uso de otras frecuencias no supera el 15 %. Así pues, como ha manifestado la Federal Communicacitions Commission (FCC) [3] el reparto y uso actual del espectro es ineficiente.

Las redes de radio cognitiva están surgiendo como una tecnología clave para llevar a cabo una gestión más óptima del ancho de banda disponible [1]. Se caracterizan por tener la capacidad de escuchar el uso que se hace del espectro y adaptar consecuentemente sus parámetros de comunicación para aprovechar los huecos libres que existen en muchas de las frecuencias licenciadas. Ello permite a los usuarios compartir el espectro de forma oportunista y evitar colisiones tanto con los servicios licenciados -televisión, telefonía móvil, etc.-, como con otros usuarios sin licencia que quieren aprovechar el ancho de banda libre de la red. Las entidades y usuarios que ofrecen o consumen servicios con licencia son denominados usuarios primarios dado que tienen prioridad en el uso de la red, mientras que los usuarios sin licencia se conocen como usuarios secundarios. Actualmente el estándar de radio cognitiva que se está desarrollando es el IEEE 802.22 que opera sobre las bandas de frecuencia de los servicios de televisión y está dirigido a formar redes de área regional.

El requisito principal de los sistemas de radio cognitiva es evitar interferir a los usuarios primarios. Sin embargo, dicha tarea es complicada debido a la propia naturaleza del medio inalámbrico. Las señales pueden sufrir desvanecimientos profundos debido al efecto multicamino o porque han atravesado un medio con alta atenuación. Este efecto puede ocasionar el problema del terminal oculto en el que un nodo secundario falla en la detección de una señal primaria. Para evitar errores, la sensibilidad de las radios cognitivas debe ser mucho mayor que la de los receptores primarios. Desarrollar sensores que individualmente garanticen los requisitos de sensibilidad que exige una radio cognitiva es muy costoso. Es por ello que las soluciones comúnmente adoptadas pasan por utilizar otra estrategia: la detección cooperativa [4].

Las técnicas de detección cooperativas combinan los resultados de la monitorización espectral que han realizado varios usuarios secundarios individualmente y obtienen una decisión final acerca de la presencia de un usuario primario en la banda de operación. Dado que el efecto multicamino y el ensombrecimiento son factores locales que degradan la detección de sólo algunos nodos de la red, los esquemas detección cooperativa permiten mitigar dichos efectos, obteniendo así un aumento en la probabilidad de detección del usuario primario. Sin embargo, este paradigma conlleva unos riesgos de seguridad, ya que los nodos pueden reportar información falsa que altere la decisión del estado final del espectro.

Aunque en la literatura hay múltiples propuestas sobre métodos de detección cooperativos, pocos de ellos consideran la presencia de usuarios maliciosos en la red que envíen datos erróneos a propósito. Los que lo hacen, requieren generalmente información *a priori* sobre las condiciones del entorno, ya sea el perfil de los nodos del sistema, las características de la señal y el ruido, la frecuencia de ocupación de los canales, etc.

En este artículo, se propone un nuevo método de fusión de detección cooperativa para radios cognitivas que no asume el conocimiento previo del contexto y que es robusto frente a ataques maliciosos. El algoritmo propuesto utiliza las deci-

siones locales de los múltiples nodos y los divide en cuatro grupos según su factor de aciertos en pasadas detecciones, considerando tanto los resultados obtenidos a corto y largo plazo. Los grupos toman una decisión basándose en la detección de la mayoría de sus miembros. Finalmente, las decisiones de los grupos son fusionadas teniendo en cuenta la reputación global del grupo y su unanimidad en la decisión.

El resto del artículo está organizado de la siguiente forma. En la sección II, se describen aspectos generales sobre la detección cooperativa de señales primarias y sobre métodos básicos de fusión cooperativa. El método de fusión de datos por grupos propuesto se explica en la sección III. En la sección IV, los resultados de las simulaciones verifican el funcionamiento del método propuesto comparado con métodos básicos. Finalmente, la sección V presenta las conclusiones del artículo.

II. Técnicas de detección cooperativas

En esta sección presentaremos, en primer lugar, aspectos generales sobre las técnicas de detección cooperativas y, en segundo lugar, describiremos los métodos de fusión cooperativos básicos más usados.

Una red de radio cognitiva está formada por un grupo de usuarios secundarios que escanean periódicamente su entorno radioeléctrico para detectar la presencia de usuarios primarios. Los usuarios secundarios se encuentran bajo diferentes condiciones de atenuación.

La mayoría de técnicas de detección cooperativas utilizan un centro de fusión que recoge los datos enviados por los nodos secundarios acerca de los resultados de su detección local. El centro de fusión ejecuta un determinado método de fusión sobre los datos para obtener la decisión final.

Los métodos de fusión utilizados por el centro de fusión se pueden clasificar en dos tipos: métodos de fusión de datos multi-nivel (soft-combining) y métodos de fusión de datos binarios (hard-combining). Los primeros fusionan información sobre la medida realizada por cada nodo. La fusión proporciona datos muy ajustados pero el volumen de datos que se requiere que los nodos envíen al centro de fusión es muy elevado. Por otro lado, los métodos de fusión de datos binarios realizan la fusión de las decisiones locales sobre si existe o no usuario primario. Cada una de las decisiones locales se envían al centro de fusión en forma binaria. La principal ventaja de estos métodos es que reducen la cantidad de datos enviados.

Los métodos detallados en este artículo emplean datos binarios para realizar la fusión. Antes de presentar los diferentes métodos propuestos para implementar la detección cooperativa, vamos a describir dos parámetros que son importantes a la hora de evaluar el funcionamiento de una determinada técnica de fusión de datos.

El primer parámetro es la probabilidad de detección y se define como la probabilidad de acierto en la detección de un usuario primario. Esta probabilidad indica cómo de bueno es el método evitando las interferencias al usuario primario. Cuando la probabilidad de detección es alta, conseguimos un nivel elevado de protección de la señal primaria. El segundo parámetro es la probabilidad de falsa alarma y representa la probabilidad de detectar un usuario primario cuando en realidad éste no existe. Cuanto menor sea la probabilidad de falsa alarma, el uso de los canales libres será más eficiente.

II-A. Métodos de fusión de datos binarios

En este apartado introducimos las principales técnicas de fusión de datos binarios existentes para detección cooperativa.

Las reglas OR, AND o Mayoría son los métodos de fusión de datos más básicos y se adaptan a cualquier situación [8]. Estas técnicas deciden sobre la ocupación del canal sumando cada una de las decisiones de los N nodos del sistema (u_i) y comparando el resultado con un umbral. En función del valor del umbral de decisión, estaremos hablando de las reglas AND, OR o Mayoría.

La regla OR declara que el usuario primario está presente si al menos uno de los nodos ha detectado al usuario primario:

$$\text{Si} \begin{cases} \sum_{i=1}^{N} u_i \geq 1 & \Rightarrow \text{ señal primaria presente} \\ \text{Otro;} & \Rightarrow \text{ señal primaria absente} \end{cases}$$

En la regla AND el umbral de decisión para declarar que existe usuario primario es el total de nodos N:

$$\text{Si} \begin{cases} \sum_{i=1}^{N} u_i = N & \Rightarrow \text{ señal primaria presente} \\ \text{Otro;} & \Rightarrow \text{ señal primaria absente} \end{cases}$$

En la regla de fusión por Mayoría se declara el canal ocupado cuando como mínimo la mitad de los nodos hayan detectado al usuario primario:

$$\text{Si} \begin{cases} \sum_{i=1}^{N} u_i \geq \frac{1}{2}N & \Rightarrow \text{ señal primaria presente} \\ \text{Otro;} & \Rightarrow \text{ señal primaria absente} \end{cases}$$

Otra posibilidad para fusionar los datos del análisis del espectro se basa en realizar el Likelihood Ratio Test (LRT) y de ese modo obtener una decisión final óptima. Al modelar el proceso de fusión como un problema probabilístico es necesario disponer de información adicional, a parte de conocer las decisiones locales de los nodos. En particular, se deberán conocer: la probabilidad *a priori* de u_i cuando la decisión final es que no hay usuario primario ($P(u_i|H_0)$) y la probabilidad *a priori* de u_i cuando se decide que existe usuario primario ($P(u_i|H_1)$). El cálculo del LRT se realiza según la siguiente expresión:

$$\prod_i \frac{P\left(u_i \mid H_1\right)}{P\left(u_i \mid H_0\right)} \begin{matrix} H_1 \\ > \\ < \\ H_0 \end{matrix} \lambda$$

donde H_0 representa la hipótesis de que el canal está libre y H_1 de que está ocupado. El resultado del LRT se compara con un determinado umbral λ para obtener la decisión final (H_0 o H_1). Este método deberá ser utilizado en entornos más

estáticos y donde se conozcan determinados parámetros del sistema.

La detección colaborativa permite obtener un análisis de las bandas frecuenciales libres más preciso que una única detección local. Sin embargo, el buen funcionamiento de estos métodos puede estar afectado por los siguientes problemas.

En primer lugar, las señales que reciben los nodos secundarios pueden llegar severamente atenuadas o simplemente puede ocurrir que el terminal secundario no funcione correctamente y realice un análisis del espectro erróneo. Estas causas provocan equivocaciones en la decisión del nodo al detectar la señal primaria.

En segundo lugar, puede ocurrir que el sistema contenga usuarios maliciosos. Este tipo de nodos envían información falsa al centro de fusión alterando los resultados de sus medidas del espectro para alterar la decisión final. Este tipo de ataques conduce a equivocaciones cuando se realiza el algoritmo de fusión de datos. Algunos de los efectos que esto puede producir son el error de falsa alarma o fallo de detección. El caso de falsa alarma reduce el rendimiento del sistema. Sin embargo, el caso de fallo de detección tiene consecuencias más serias porque puede provocar interferencias a los usuarios primarios.

Como resultado de estos problemas recientemente se han investigado nuevos métodos de fusión que implementan contramedidas para atenuar los efectos de los ataques de falsificación de datos o los efectos de equipos defectuosos que inconscientemente envían resultados incorrectos.

Lim et al. presentan un método de fusión de datos binarios que utiliza vectores de confianza y reputaciones [5]. El vector de confianza es un índice asignado por el propio nodo según la confianza que él tiene de la precisión del resultado de sus medidas. La reputación representa la precisión de un nodo en su historial de medidas respecto a las decisiones finales.

En primer lugar, un nodo escanea el espectro, toma una decisión sobre la ocupación del canal, y determina un valor de confianza. Luego, el nodo modifica el valor del vector de confianza con un signo positivo si el nodo decidió que el canal estaba ocupado y con signo negativo en el caso contrario.

A continuación, los nodos envían al centro de fusión sus decisiones locales junto con el nuevo valor de confianza. El centro de fusión agrupa todos los resultados utilizando la regla de fusión por mayoría ponderada con pesos. Los pesos representan la reputación de cada nodo, de manera que se asignan pesos mayores a los nodos más fiables. Por consecuencia, las decisiones de estos nodos contribuyen en mayor medida a la decisión final.

La decisión final u se obtiene según la siguiente expresión

$$u = \begin{cases} 1, & \text{si} \quad \sum_i c_i w_i \geq 0 \\ 0, & \text{si} \quad \sum_i c_i w_i < 0 \end{cases}$$

donde c_i es el vector de confianza para un usuario i y w_i el factor de reputación.

Existen otros métodos de fusión binaria y cooperativos que han sido propuestos con el objetivo de reducir el efecto de nodos maliciosos ([6], [2], [9]) pero su ámbito de aplicación no es tan genérico por requerir el conocimiento de cierta información de entorno.

III. Método de fusión en grupos propuesto

Los métodos de fusión de datos binarios propuestos hasta ahora han sido diseñados para entornos inalámbricos muy estáticos y en los que la presencia de atacantes es limitada. En concreto, sólo se asume la presencia de atacantes de tipo SIEMPRE-SI (siempre dicen que la banda del espectro a analizar está ocupada) y de tipo SIEMPRE-NO (siempre dicen que la banda del espectro a analizar está libre). Sin embargo, nodos que normalmente prestan un buen servicio a la comunidad con una detección fiable de los canales espectrales, pueden sesgar su visión del sistema en el momento en el que son ellos mismos los que necesitan un canal de comunicaciones. Un nodo egoísta puede manipular el sistema y decir que un canal está ocupado cuando en realidad no es así, por el simple hecho de poder ocupar él este canal sin tener que compartirlo con los demás nodos de la comunidad. También puede darse el caso que un nodo malicioso informe que un canal está libre cuando está ocupado, por el simple hecho de interferir y provocar una denegación de servicio a los nodos primarios.

En este artículo, proponemos un método de fusión de datos que tiene en cuenta el comportamiento y la reputación de los usuarios a largo plazo, pero que también está preparado para soportar los cambios bruscos del entorno y por consecuencia, de las decisiones incoherentes de los nodos. Para ello clasificamos los nodos en grupos según su comportamiento pasado. Los grupos toman una decisión basándose en la detección de la mayoría de sus miembros. Finalmente, las decisiones de los grupos son fusionadas dando mayor peso a los grupos de usuarios que más han acertado en pasadas detecciones y que presentan mayor unanimidad de voto en la decisión actual.

III-A. Clasificación de los nodos

Definimos la reputación de un nodo como un valor que mide los aciertos a largo término de sus decisiones de detección, esto es, cuando la decisión local del nodo y la global del sistema coinciden. La reputación $r_i \in [0, 1]$ de un nodo i es:

$$r_i = \frac{\sum_{k=1}^{N_i} a_i}{N_i}$$

donde a_i es el número de aciertos del nodo i sobre un total de N_i detecciones.

Por otro lado, definimos la estabilidad de un nodo como un valor que ilustra los cambios contextuales o de conducta de un nodo en un corto instante de tiempo. Calculamos la estabilidad e_i a partir de los aciertos de detección de un nodo i en un corto espacio de tiempo correspondiente a 4 iteraciones de detección:

$$e_i = \frac{\sum_{k=N_i-3}^{N_i} a_i(k)}{4}$$

donde $a_i(k)$ es una función que retorna 0 o 1 cuando el nodo i en el instante de tiempo k falla o acierta la detección del nodo primario, respectivamente.

A partir de la reputación r_i y la estabilidad e_i, un nodo i obtiene un factor de incidencia $w_i \in [0,1]$ en la decisión:

$$w_i = r_i \cdot e_i$$

III-B. Algoritmo de decisión

Los nodos hacen la detección del espectro y envían al centro de fusión la decisión local $d_i = \{-1, 1\}$ para indicar que la banda está libre (-1) o ocupada (1). El algoritmo de fusión propuesto está basado en la regla de fusión por mayoría, pero en lugar de tratar por igual las decisiones de todos los nodos, el sistema las pondera según el factor de incidencia de los nodos y el grado de unanimidad de la decisión.

En primer lugar el centro de fusión ordena los nodos que participan en la detección cooperativa de forma ascendente según el valor de su factor de incidencia. Luego clasifica los nodos en cuatro cuartiles (G_1, G_2, G_3 y G_4). Los valores de corte de los cuartiles (λ_{12}, λ_{23}, y λ_{34}) vienen determinados por el factor de incidencia de los nodos que ocupan las posiciones al $25\,\%$, $50\,\%$ y $75\,\%$ de la longitud de la lista, respectivamente. Así, los nodos son clasificados en grupos según el valor de su factor de incidencia de la siguiente forma:

$$\text{Si} \begin{cases} 0 \leq w_i \leq \lambda_{34}; & \Rightarrow \quad u_i \in G_4 \\ \lambda_{34} < w_i \leq \lambda_{23}; & \Rightarrow \quad u_i \in G_3 \\ \lambda_{23} < w_i \leq \lambda_{12}; & \Rightarrow \quad u_i \in G_2 \\ \lambda_{12} < w_i \leq 1; & \Rightarrow \quad u_i \in G_1 \end{cases}$$

El centro de fusión agrega los datos reportados por los diferentes nodos de la siguiente manera:

$$\begin{aligned} \gamma \quad = \quad & \overline{G_1} + (1 - |\overline{G_1}|)\overline{G_2} + (1 - |\overline{G_1}|)(1 - |\overline{G_2}|)\overline{G_3} + \\ & (1 - |\overline{G_1}|)(1 - |\overline{G_2}|)(1 - |\overline{G_3}|)\overline{G_4} \end{aligned}$$

con $\overline{G_x}$ el promedio de las decisiones locales recibidas por el grupo G_x.

Siendo $\overline{G_x}$ el promedio de un grupo de valores $\{-1, 1\}$, el rango de valores que puede tomar esta variable está entre -1 y 1. $|\overline{G_1}| = 1$ cuando la decisión de todos los nodos del grupo G_x sea unánime; $|\overline{G_1}| = 0$ cuando la disparidad de decisiones entre los nodos del grupo G_x sea máxima, es decir, haya la mitad de los nodos que decidan que la banda del espectro sobre la que han hecho la detección está libre, y la otra mitad de los nodos decidan que está ocupada.

El algoritmo de decisión considera principalmente las decisiones de los nodos que están en el grupo G_1 para tomar la decisión final, ya que son los nodos que gozan de una mayor reputación y tienen estabilidad en el sistema. Sin embargo, cuando las decisiones de este grupo son muy dispares (esto es, el promedio de los datos en valor absoluto es bajo), el peso de este grupo baja y las decisiones de los grupos G_2, G_3 y G_4 toman más fuerza. Como se ha hecho con G_1 se analiza la uniformidad de las decisiones de cada grupo G_x y se pondera consecuentemente la incidencia de este grupo en la decisión final.

La decisión global se toma en función del valor γ resultante. Si $\gamma < 0$ se considera que el canal está libre. Sino, el canal está ocupado.

Una vez el centro de fusión ha tomado una decisión sobre la ocupación del canal, la reputación y la estabilidad de los nodos del sistema es actualizada.

IV. Simulaciones

En esta sección se ilustran los resultados de las simulaciones realizadas con el esquema propuesto a través de las curvas ROC. Las curvas ROC representan los pares de probabilidad de detección (sensibilidad) frente probabilidad de falsa alarma para diferentes umbrales de decisión.

Las simulaciones se han realizado con 50 usuarios secundarios distribuidos aleatoriamente sobre una área de $500m$x$500m$ considerando un medio con obstáculos y propagación multicamino. Todos los nodos secundarios utilizan un detector de energía para monitorizar el espectro. Por lo tanto, la SNR que recibe cada usuario es diferente y consecuentemente su capacidad de detección. El centro de fusión utiliza en cada caso uno de los métodos de fusión descritos en las secciones II y III.

Se ha analizado la capacidad de detección para diferentes métodos de detección cooperativos de uso general, que no requieren un conocimiento *a priori* sobre el contexto de aplicación.

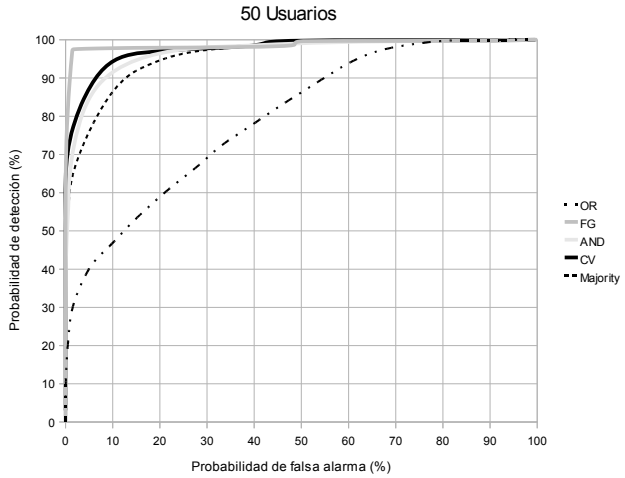

Figura 1. Gráfica ROC. Detección cooperativa con 50 nodos

En la Fig.1 se comparan los diferentes métodos: la regla AND (referida como AND), la regla OR (referida como OR), la regla de fusión por mayoría (referida como Majority), el método con vectores de confianza (referido como CV) y el método de fusión por grupos propuesto (referido como FG). Los resultados muestran que el método propuesto supera al resto de algoritmos de fusión. Para una probabilidad de falsa alarma del 10 % este esquema consigue una probabilidad de detección mayor al 10 % que en el esquema de fusión por mayoría.

La curva ROC evidencia que un aumento de la probabilidad de detección va en detrimento de la probabilidad de falsa

alarma y viceversa, lo que implica que la selección del umbral exige un compromiso entre estos dos conceptos. Para conseguir los requisitos mínimos de sensibilidad y probabilidad de falsa alarma estipulados por el estándar IEEE 802.22 los valores deben ser, respectivamente, mayor al 90 % y menor al 10 % [7].

El segundo escenario de simulación que se ha analizado mantiene las mismas características de red que en el caso anterior, pero se han añadido usuarios maliciosos del tipo Siempre-No que atacan reiteradamente. Para evaluar el comportamiento de cada método, se ha fijado un umbral de detección para cada algoritmo que maximice la dupla de la probabilidad de detección y la probabilidad de falsa alarma en un escenario libre de atacantes. A partir de aquí, se ha analizado la probabilidad de detección del sistema a medida que se han ido añadiendo atacantes a la red. La Fig.2 evidencia que la regla AND es el método menos robusto frente a este tipo de ataques, ya que experimenta la mayor disminución. Por otro lado, se observa como el método propuesto cumple el estándar con una probabilidad de detección del 90 % para un porcentaje de atacantes menor al 12 %. Para un porcentaje de atacantes mayor al 20 % no podemos asegurar probabilidad de detección, aunque dependiendo de la configuración de los nodos ésta puede ser positiva. En cuanto a la probabilidad de detección del método de fusión por mayoría y del método con vectores de confianza podemos decir que decrecen suavemente, pero éstos no cumplen el requisito del estándar para una proporción mayor al 2 % de atacantes.

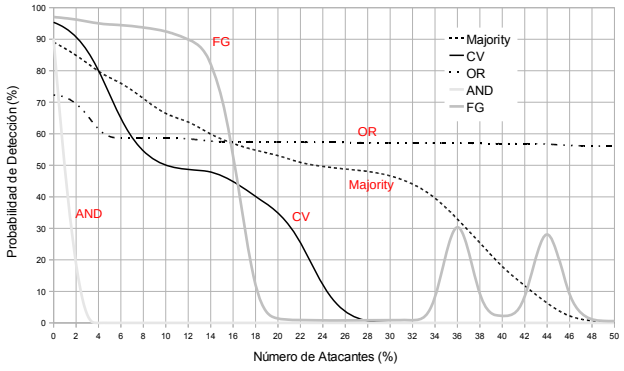

Figura 2. Probabilidad de detección con nodos atacantes

Por último, hemos simulado un escenario con atacantes que actúan por ráfagas. En general los nodos tienen un buen comportamiento en el sistema y por lo tanto gozan de buena reputación, pero puntualmente pueden lanzar un ataque cuando ven que el éxito de éste les puede reportar algún beneficio. Las gráficas que se muestran en Fig.3, Fig.4 y Fig.5, representan la probabilidad de detección del sistema en un periodo de 40 iteraciones. Los nodos tienen un comportamiento correcto durante las 10 primeras iteraciones, pero entre el intervalo de 10 a 30 un determinado número de nodos falsifica sus datos reportando que el canal está libre. Finalmente, después de la iteración número 30, todos los nodos vuelven a enviar al centro de fusión los datos de detección correctos. Las características de la red se mantienen como en los anteriores casos, y siempre hay presencia de un nodo primario en la red.

La Fig.3, la Fig.4 y la Fig.5 representan todas la probabilidad de detección frente al número de iteraciones para un porcentaje del 10 %, del 20 % y del 40 % de atacantes, respectivamente. En las tres gráficas durante el intervalo que se produce la ráfaga de ataques, todos los métodos disminuyen su probabilidad de detección y después de este periodo vuelven a recuperar los valores iniciales.

Comparando las tres gráficas observamos que los métodos de fusión por grupos, con vectores de confianza y por mayoría, empeoran su comportamiento a medida que aumenta la proporción de atacantes. Cuando esta proporción es baja, del 10 % o del 20 %, el método propuesto supera la regla de fusión por mayoría. En particular, para un 10 % de atacantes, el método de fusión por grupos reacciona correctamente manteniéndose en una probabilidad de detección alrededor del 90 % y cumpliendo así las especificaciones del estándar.

Si comparamos este último caso de atacantes puntuales con el caso de atacantes Siempre-No reiterativos (Fig.2), apreciamos que los métodos de fusión sin memoria (como la OR, AND y Mayoría) no presentan comportamientos diferentes entre los dos casos. En cuanto al método con vectores de confianza, tiene probabilidades de detección menores que el método de fusión por mayoría. El método con confianza no está diseñado para tener en cuenta ataques puntuales, el centro de fusión considera correctos los informes que envían los atacantes que habían obtenido buenas reputaciones antes de atacar. El método de fusión por grupos propuesto reacciona correctamente frente a ataques puntuales. Observamos en la Fig.4 como la probabilidad de detección se encuentra alrededor del 70 %. Mientras que para el mismo porcentaje de atacantes reiterativos el método no es capaz de detectar al usuario primario.

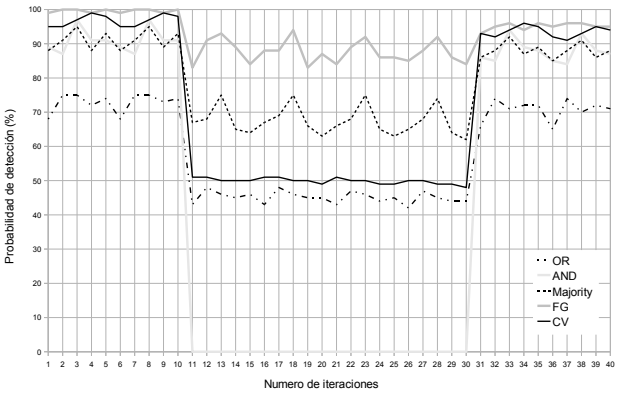

Figura 3. Probabilidad de detección con un 10 % de atacantes puntuales

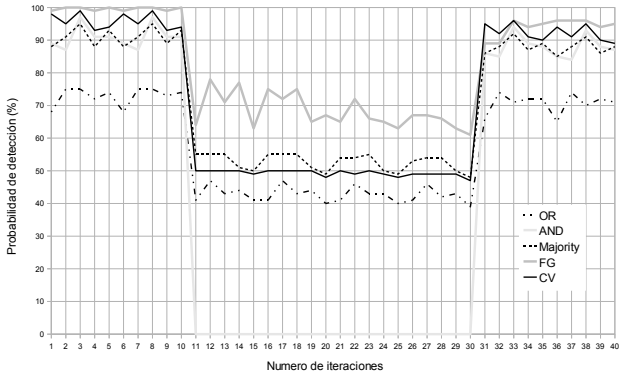

Figura 4. Probabilidad de detección con un 20 % de atacantes puntuales

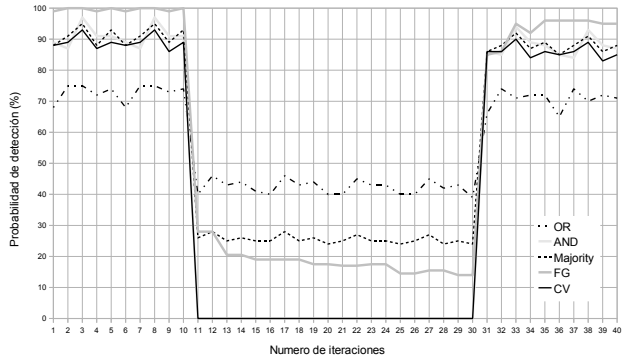

Figura 5. Probabilidad de detección con un 40 % de atacantes puntuales

V. Conclusiones

En este trabajo se ha descrito un esquema de detección colaborativo por grupos con el objetivo de mejorar la sensibilidad y robustez de una red de radio cognitiva. Los resultados de las simulaciones muestran que el algoritmo propuesto ofrece una mejor probabilidad de detección frente a otros algoritmos con unas características de rendimiento similares. En un trabajo futuro se analizará la robustez del esquema en otros contextos y para diferentes volúmenes de nodos.

Agradecimientos

Este trabajo ha sido financiado parcialmente por el Ministerio de Industria, Turismo y Comercio con el proyecto AVANZA TSI-020100-2009-374 SAT2, y por el Ministerio de Ciencia e Innovación y los fondos FEDER con los proyectos TSI2007-65406-C03-03 E-AEGIS y CONSOLIDER CSD2007-00004 ARES.

Referencias

[1] I.F. Akyildiz, W.Y. Lee, M.C. Vuran, and S. Mohanty. Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey. *Computer Networks*, 50(13):2127–2159, 2006.

[2] Ruiliang Chen, Jung-Min Park, and Kaigui Bian. Robust distributed spectrum sensing in cognitive radio networks. In *INFOCOM. The 27th Conference on Computer Communications. IEEE*, pages 1876–1884, April 2008.

[3] S.P.T. Force. Spectrum policy task force report. *Federal Communications Commission ET Docket 02*, 135, 2002.

[4] A. Ghasemi and E.S. Sousa. Opportunistic spectrum access in fading channels through collaborative sensing. *Journal of Communications*, 2(2):71, 2007.

[5] Sunmin Lim, Hoiyoon Jung, and Myung Sun Song. Cooperative spectrum sensing for ieee 802.22 wran system. In *Proceedings of 18th Internatonal Conference on Computer Communications and Networks (ICCCN).*, pages 1–5, Aug. 2009.

[6] Tao Qin, Han Yu, Cyril Leung, Zhiqi Shen, and Chunyan Miao. Towards a trust aware cognitive radio architecture. *SIGMOBILE Mob. Comput. Commun. Rev.*, 13(2):86–95, 2009.

[7] C.R. Stevenson, C. Cordeiro, E. Sofer, and G. Chouinard. Functional requirements for the 802.22 WRAN standard. *IEEE 802.22-05/0007r48*, pages 802–22, Nov. 2006.

[8] E. Visotsky, S. Kuffner, and R. Peterson. On collaborative detection of tv transmissions in support of dynamic spectrum sharing. In *IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN).*, pages 338–345, Nov. 2005.

[9] Wenzhong Wang, Weixia Zou, Zheng Zhou, and Yabin Ye. Detection fusion by hierarchy rule for cognitive radio. In *Cognitive Radio Oriented Wireless Networks and Communications. CrownCom. 3rd International Conference on*, pages 1–5, May 2008.