UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA:
INGENIERÍA ELECTRÓNICA

Trabajo de titulación previo a la obtención del título de:
INGENIERO ELECTRÓNICO

TEMA:
ANÁLISIS DE POSIBLES VULNERABILIDADES DE ACCESO EN ENTORNOS DE RADIO COGNITIVA PARA ENTENDER LAS FALENCIAS DE SEGURIDAD DE ESTA TECNOLOGÍA, EN BASE A UN MODELAMIENTO MATEMÁTICO

AUTOR:
SANTIAGO VINICIO ARAUJO FLORES

TUTOR:
MANUEL RAFAEL JAYA DUCHE

Quito, Septiembre 2016

Declaratoria de coautoría del docente tutor

Yo, declaro que bajo mi dirección y asesoría fue desarrollado el trabajo de titulación ANÁLISIS DE POSIBLES VULNERABILIDADES DE ACCESO EN ENTORNOS DE RADIO COGNITIVA PARA ENTENDER LAS FALENCIAS DE SEGURIDAD DE ESTA TECNOLOGÍA, EN BASE A UN MODELAMIENTO MATEMÁTICO realizado por Santiago Vinicio Araujo Flores, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana para ser considerados como trabajo final de titulación.

Quito, Septiembre 2016

Manuel Rafael Jaya Duche

C.I:1710631035

Cesión de derechos de autor

Yo Santiago Vinicio Araujo Flores, con documento de identificación N° 1717547614, manifiesto mi voluntad y cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del trabajo de grado/titulación intitulado: ANÁLISIS DE POSIBLES VULNERABILIDADES DE ACCESO EN ENTORNOS DE RADIO COGNITIVA PARA ENTENDER LAS FALENCIAS DE SEGURIDAD DE ESTA TECNOLOGÍA, EN BASE A UN MODELAMIENTO MATEMÁTICO, mismo que ha sido desarrollado para optar por el título de: Ing. Electrónica, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

.....

Santiago Vinicio Araujo Flores
Cédula: 1717547614
Fecha: Septiembre, 2016

ANÁLISIS DE POSIBLES VULNERABILIDADES DE ACCESO EN ENTORNOS DE RADIO COGNITIVA PARA ENTENDER LAS FALENCIAS DE SEGURIDAD DE ESTA TECNOLOGÍA, EN BASE A UN MODELAMIENTO MATEMÁTICO

Santiago Araujo[1], Rafael Jaya[2]

Resumen

El presente trabajo tiene como objetivo analizar las posibles vulnerabilidades de los entornos de red de radio cognitiva (RRC), porque es necesario entender cuáles serían los retos de esta nueva tecnología a enfrentar el nivel de seguridades, el estudio se enfocara en el análisis de los ataques bizantinos que es un tipo de ataque a nivel de capa de enlace que se produce en el momento de monitorización cooperativa del espectro, se utilizó Matlab para elaborar los casos de modelamiento de investigación para pruebas en diferentes escenarios de uso de espectro radioeléctrico, en base a una ecuación establecida por A. S. R. Priyank Anand, para entender como los usuarios maliciosos pueden utilizar la RRC para realizar ataques desde los nodos secundarios y generar falsos informes de uso del medio.

Al aplicar el modelo se pudo observar que efectivamente la probabilidad de ataque aumenta hasta en un 99% al aumentar el número de usuarios deshonestos y tomando en cuenta un rango de probabilidad de mentir de dichos usuarios del 70% al 100%, esto denota las graves falencias de seguridad de dicho entorno en el caso reportes para detección de usuarios licenciados, por otro lado, dicha probabilidad varia en una proporción de 0% a 30% si se toma en cuenta el número de usuarios maliciosos M que intervienen en la comunicación.

Palabras Clave: RRC, Nodos, Usuario Licenciado, Espectro Radioeléctrico, Matlab.

Abstract

This paper aims to analyze potential vulnerabilities environments cognitive radio (RRC), because you need to understand what would be the challenges of this new technology to face the level of assurance, the study will focus on the analysis of Byzantine attacks which is a type of attack level link layer that occurs at the time of cooperative monitoring the spectrum, Matlab was used to develop cases modeling research to test different scenarios using radio spectrum, based on a established by equation, to understand how malicious users can use the RRC to carry out attacks from the child nodes and generate false reports of use of the medium.

In applying the model was observed that indeed the likelihood of attack increases up to 99% by increasing the number of rogue users and taking into account a range of probability of lying of those users from 70% to 100%, this shows the serious security flaws in that environment reports for case detection licensed users, on the other hand that probability varies at a rate of 0% to 30% if we take into account the number of malicious users M involved in communication.

Keywords: CRN, FC, Nodos, User Licensed, Radio Spectrum Matlab.

[1] Estudiante de Ingeniería Electrónica - Universidad Politécnica Salesiana, Egresado - UPS - sede Quito
Email: saraujof0@est.ups.edu.ec

[2] Magister en Redes de Información y Conectividad, Ingeniero en Electrónica y Telecomunicaciones, Profesor de Ingeniería Electrónica - UPS - sede Quito
Email: mjaya@ups.edu.ec

1. Introducción

Según [1] las comunicaciones inalámbricas actuales se enfrentan a un grave problema de saturación de espectro radioeléctrico, es por ese motivo que radio cognitiva llega como una solución para la optimización del uso del mismo, sin embargo, el espectro concesionado está siendo subutilizado y en algunos casos no se lo usa, en el caso de ciertas bandas explotadas por algunas operadoras de televisión sufren variación temporales o geográficas de utilización entre un 15% y un 85%.

Una red radio cognitiva (RRC) es una radio que puede cambiar sus parámetros del transmisor basado en interacción con el entorno en que se opera [2], en otras palabras, las antenas transmisoras y receptoras de telecomunicaciones dejarán de ser elementos pasivos y pasarán a ser elemento activos, lo cual da una gran ventaja sobre el espectro radioeléctrico, los transmisores reconfigurables darán acceso a millones de nuevos usuarios a la red.

"En cuanto a la Seguridad, esto es inherente al funcionamiento mismo del paradigma de Radio Cognitiva, ya que el hecho de monitorizar el tráfico de un usuario legítimo por parte de un usuario no legítimo en sí mismo ya compromete la seguridad y la privacidad del primer usuario. Esto es, el censado del espectro del usuario licitado facilita información sobre su patrón de tráfico, el volumen, la ocupación de espectro, e incluso del enrutamiento" [1].

Esta nueva tecnología busca en general optimizar el acceso y uso de dicho recurso, pero este se enfrenta a grandes retos como son las seguridades de los usuarios licenciados que ya tienen la concesión legal de dicho espectro, y al momento de ingresar nuevos usuarios a utilizar sus frecuencias quedarían vulnerables ante los mismos, en la Fig. 1.1, Se ilustran diversos aspectos de la tarea de detección de espectro [3].

Bajo esta perspectiva radio cognitiva es una tecnología de capa de enlace para acceso dinámico al espectro (Dynamic Spectrum Access: DSA), orientada a facilitar la transmisión de radio en capa física [4], con una tecnología inalámbrica de reconfiguración [1].

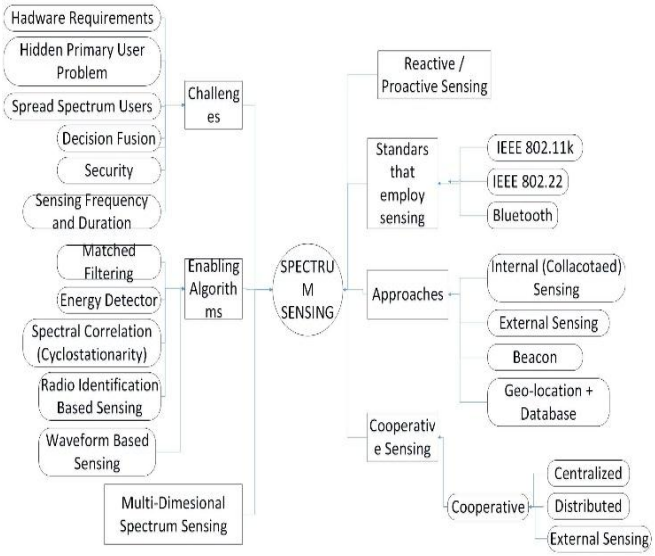

Fig. 1.1 Varios aspectos de la detección del espectro de radio cognitiva [3].

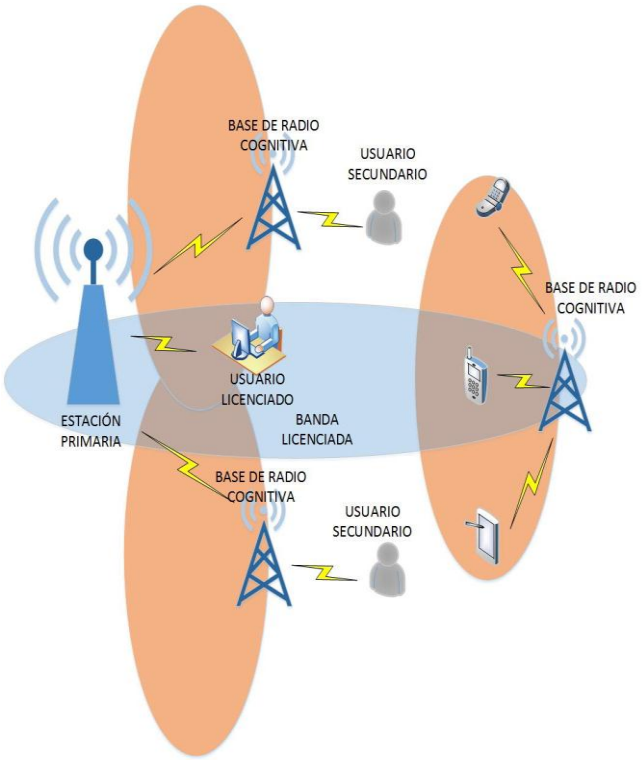

Fig. 1.2 Esquema de red de radio cognitiva.

El objetivo de este proyecto es estudiar los ataques bizantinos y su comportamiento en diferentes escenarios para los cuales se asumirán parámetros de estudio como probabilidad de acceso tanto de usuarios licenciados con usuarios no licenciados y usuarios maliciosos.

1.1 Amenazas de seguridades de Radio Cognitiva

La seguridad es un aspecto clave para el desarrollo de las redes cognitivas, tanto en entornos civiles como militares (dentro del estándar IEEE 802.22 [5] [6]).

Entre los principales tipos de ataque para los cuales es necesario investigar posibles contramedidas se tienen los siguientes [7]:

• Ataques OFA (del inglés, Object Function Attacks), destinados a afectar a los algoritmos de aprendizaje de los dispositivos de radio cognitiva.

• Ataques "cross-layer", entre la capa física/enlace y la capa de transporte, destinados a afectar al protocolo de transporte saturando la red.

• Ataques PUE (del inglés, Primary User Emulation), en los que se imita la transmisión producida por un elemento primario para evitar la transmisión en la misma banda por parte de un elemento secundario, ver Fig 1.3.

• Ataques de censado en general, en el caso de redes cognitivas basadas en el paradigma de censado cooperativo, un posible atacante puede introducir información falsa con el objetivo de afectar a la operatividad general de la red.

Los ataques a radios cognitivas plantean un gran problema de seguridad para la privacidad de los usuarios, en general las redes inalámbricas son más vulnerables a ataques a nivel de capa física (spoofing, jamming, MitM…), según [8], y esto hace que RRC sea más vulnerable en términos de control de acceso poniendo en juego la integridad de los datos y privacidad de los usuarios.

1.1.1 Ataque Bizantino

Se trata de un tipo de ataque de censado en el que los usuarios maliciosos [9] tratan de tomar ventaja sobre el uso del espectro [10] ya sea frente a otros usuarios o simplemente para interrumpir el proceso de la comunicación de los usuarios honestos [11].

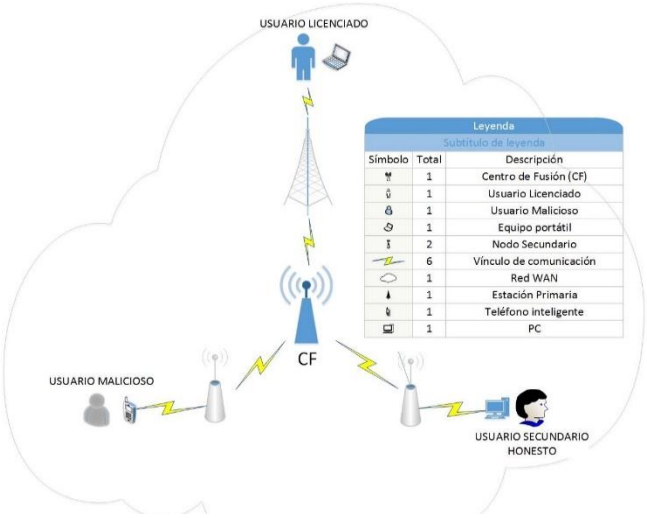

Fig. 1.3 Esquema de ataque PUE por ataque de usuario malicioso.

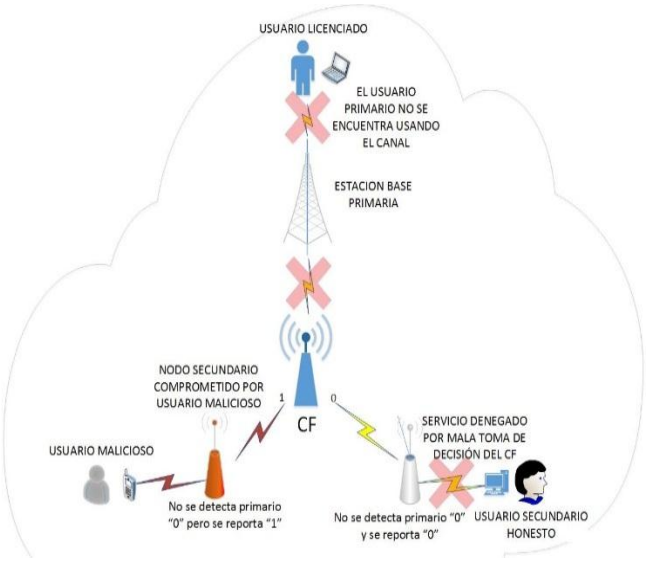

Fig. 1.4 Esquema de ataque bizantino por ataque de usuario malicioso.

El escenario de la Fig. 1.4, se puede observar como un usuario malicioso irrumpe la comunicación para promover un mal reporte de estado por parte del

nodo y de esta manera genere un falso positivo o falsos negativos por parte del CF (Centro de Fusión).

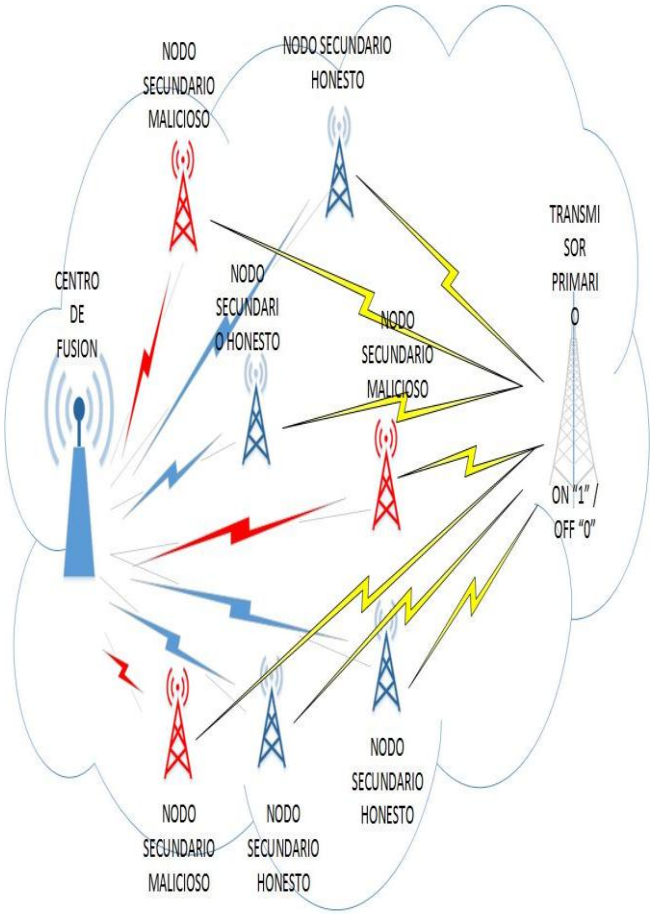

Fig. 1.5 Esquema de ataque bizantino por ataque de varios nodos maliciosos.

La red de la Fig. 1.5 se usará un escenario en el que se trata un esfuerzo en conjunto de los nodos locales para la detección del usuario licenciado, es decir, cada nodo a nivel local envía un reporte del análisis de ocupación de canal del usuario primario, para estos resultados sean analizados en conjunto por CF, por lo tanto, cada nodo reportará un "1" si el canal se encuentra ocupado o un "0" si el canal se encuentra desocupado, al final el que toma la decisión es el CF.

1.1.2 Casos de evaluación en ataques bizantinos

Para el caso de la creación de los entornos de simulación se usará el software matemático Matlab [12], el programa se basa la simulación de las ecuaciones de fusión para calcular la afectación en porcentaje del sistema global de reportes del CF.

en la siguiente investigación se tratarán los cuatro escenarios posibles, que son:

1.1.3 Escenario con usuario primario sin usuarios maliciosos

Se utilizó para este escenario la ecuación probabilística de fusión para la detección de falsas alarmas definida por [13] [14] [15].

$$Q_d^B = \sum_{i=l}^{M} \binom{M}{i} (P_d^B)^i (1 - P_d^B)^{M-i} \quad (1)$$

$$Q_{md} = \sum_{i=0}^{B_1} \binom{H}{i} {P_d}^i (1 - P_d)^{H-i} \sum_{j=0}^{B_2} \binom{M}{j} (f_2)^j (1 - f_2)^{(M-j)} \sum_{k=0}^{B_2} \binom{M-j}{k} (f_3)^k (1 - f_3)^{(M-j-k)} \quad (2)$$

De donde:

$$B_1 = \min(H, N-1)$$
$$B_2 = \min(M, N-1-i)$$
$$B_3 = \min(M-j, N-1-i-j)$$

$$f_2 = (P_d * P_l)$$
$$f_3 = (1 - P_d) * (1 - P_l)$$

Q_d= Probabilidad de detección total del sistema (la decisión final del Centro de Fusión)
Q_{md}= Probabilidad total de reportarla ausencia de primarios cuando si existen (la decisión final del Centro de Fusión).
B_i= Valor mínimo entre el número de nodos secundarios honestos y el número total de nodos secundarios.
f_2= Probabilidad de que nos encontremos en el caso en el que un nodo malicioso detecte un primario, pero decida mentir.
f_3= Probabilidad de que nos encontremos en el caso en el que un nodo malicioso detecte un primario, pero decida no mentir.

Tabla 1. Especificaciones de las diferentes variables y constantes a utilizar.

Parámetro	Descripción	Valor
N	Número total de nodos secundarios	100
M	Número de nodos secundarios maliciosos	0- 60
H	Número de nodos secundarios honestos	40 - 100
L	Umbral del centro de fusión	N/2
Pd	Probabilidad de detección por parte de los nodos secundarios honestos	0.9
Pf	Probabilidad de falsa alarma por parte de los nodos secundarios honestos	0.1
Pl	Probabilidad de mentir por parte de los nodos maliciosos	0.7 – 1

Los valores de Pd y Pf son los requeridos por el estándar IEEE 802.22 [16].

Los valores de Pl varían de 0.7 a 1, ya que estos son los valores en los que las probabilidades se ven afectadas de forma considerable, para el resto de valores la presencia de usuarios deshonestos no altera la decisión del Centro de Fusión CF.

Para las simulaciones se usará el método del umbral ya que este es el menos restrictivo y es el que más se acerca a la realidad del funcionamiento del medio de acceso al espectro, tomaremos las variables H y M, Tabla 1, de donde concluimos que:

$$H = N - M \qquad (3)$$

1.2.4 Escenario sin usuario primario y sin usuarios maliciosos

En este escenario el objetivo es calcular la probabilidad global de falsa alarma, aquí se detecta el número de casos en que el sistema ha decidido reportar la presencia de un usuario primario sin haberlo, producido por informes locales erróneos, sin necesariamente ser maliciosos.
Se usará la ecuación de probabilidad de falsa alarma Qfa dada por [13].

$$Q_{fa}^{B} = \sum_{i=l}^{M} \binom{M}{i} \left(P_{fa}^{B}\right)^{i} \left(1 - P_{fa}^{B}\right)^{M-i} \quad (4)$$

1.2.5 Escenario con usuario primario y M usuarios maliciosos

En este escenario se analiza el entorno de radio cognitiva con la inclusión de usuarios maliciosos, siendo así la red comprometida por dichos atacantes que decidirán o no falsificar información de reporte.
Para el análisis de dicho escenario se utilizó la ecuación dada por [15], ver Ec. (2)

En esta expresión Ec. (2) se tiene tres posibles opciones, la primera sumatoria tiene en cuenta los casos en que los nodos no comprometidos realizan *miss detection,* en el segundo sumatorio representa el escenario en el que un nodo malicioso decida mentir acerca de si existe o no un usuario primario, y por último el tercer sumatorio implica los casos en el que se detecta usuario primario pero los usuarios maliciosos deciden no mentir.

1.2.6 Escenario sin usuario primario y M usuarios maliciosos

En este caso se puede observar el escenario en el cual no existe ningún usuario primario usando el espectro, pero la influencia de los usuarios maliciosos hace que se emita un reporte erróneo por parte del FC en función de la variación de la probabilidad de mentir Pl.

$$Q_{fa} = 1 - \sum_{i=0}^{B_1} \binom{H}{i} {P_f}^{i} (1 - P_f)^{H-i} \sum_{j=0}^{B_2} \binom{M}{j} (f_4)^{j} (1 - f_4)^{(M-j)} \sum_{k=0}^{B_2} \binom{M-j}{k} (f_5)^{k} (1 - f_5)^{(M-j-k)} \quad (5)$$

De donde:

$$f_4 = (1 - P_f) * P_l$$
$$f_5 = P_f * (1 - P_l)$$

Q_{fa}= Probabilidad de falsa alarma (la decisión final del Centro de Fusión)
f_4= Probabilidad de que un nodo malicioso no detecta primario, pero decide mentir
f_5= Probabilidad de que el usuario malicioso detecta al primario erróneamente (debido a Pf) y decide no mentir

En la Ecuación (5) se toma en cuenta el caso en que los usuarios generan falsas alarmas en la primera sumatoria, el caso en que los nodos maliciosos no detectan al usuario primario pero está decidido a mentir en la segunda sumatoria, y al final representamos el caso en el que el usuario maliciosos detecta al primario erróneamente debido a la probabilidad de falsa alarma P_f y decide mentir.

2. Obtención de resultados

Previo a estos análisis se hace una breve referencia del diagrama de flujo de dichos programas en cuestión, ver Fig. 1.6.

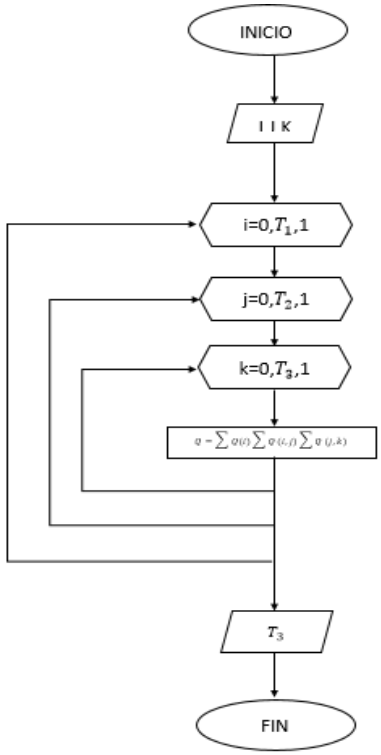

Fig. 1.6 Diagrama de flujo de la ecuación de probabilidad de detección o falsa alarma de usuario licenciado.

En base a las ecuaciones mostradas con anterioridad se procedió a generar el programa para la simulación en Matlab de cada uno de los escenarios en cuestión, obteniendo así los siguientes resultados.

CASO 1

Tabla 2. Datos obtenidos de la simulación del primer escenario con usuario primario sin usuarios maliciosos.

	Qd (Probabilidad de detección total del sistema)	**Qmd (Probabilidad total de reportar ausencia de primarios)**
N=10, l=6	0,9984	0,0018
N=20, l=11	1	0.000867
N=30, l=16	1	0,0005428
N=40, l=21	1	0,0004296
N=50, l=26	1	0,00039013
N=60, l=31	1	0,00037637
N=70, l=36	1	0,00037157
N=80, l=41	1	0,0003699
N=90, l=46	1	0,00036931
N=100, l=51	1	0,00036911

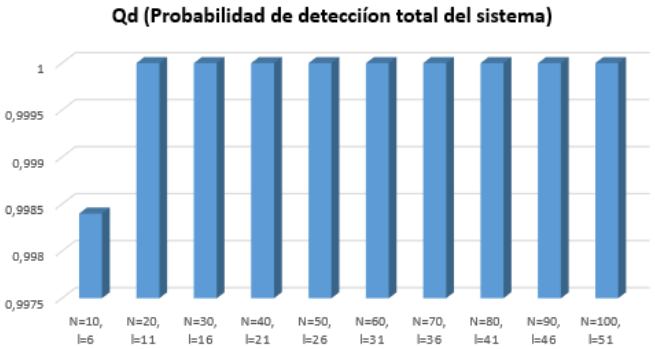

Fig. 1.6 Gráfica de probabilidad porcentual de detección total del sistema.

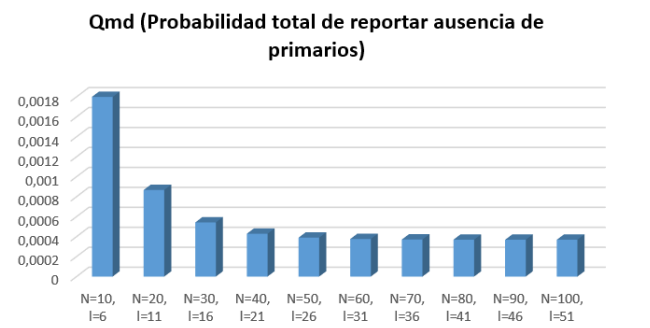

Fig. 1.7 Gráfica de probabilidad porcentual total de reportar ausencia de usuario primario

CASO 2

Tabla 3. Datos obtenidos de la simulación del segundo escenario sin usuario primario sin usuarios maliciosos.

	Qfa (Probabilidad de falsa alarma)
N=10, l=6	1,47E-04
N=20, l=11	7,09E-07
N=30, l=16	3,66E-09
N=40, l=21	1,96E-11
N=50, l=26	1,07E-13
N=60, l=31	5,99E-16
N=70, l=36	3,38E-18
N=80, l=41	1,92E-20
N=90, l=46	1,10E-22
N=100, l=51	6,32E-25

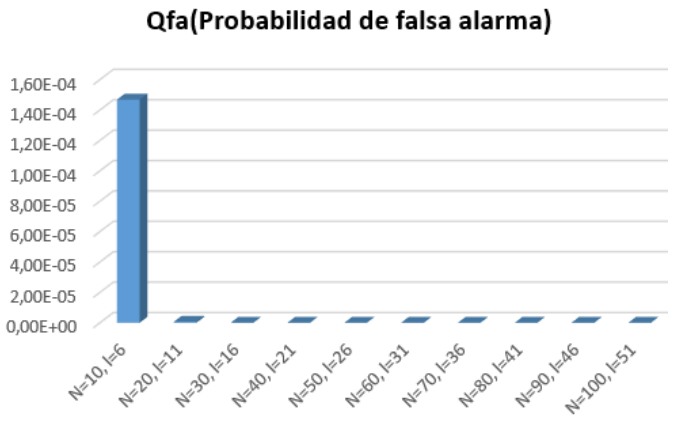

Fig. 1.8 Gráfica de probabilidad porcentual de reportar falsa alarma

CASO 3

Tabla 4. Datos obtenidos de la simulación del tercer escenario con usuario primario y M usuarios maliciosos y un Pl=(0.7 - 1).

	Qmd (Probabilidad total de reportar ausencia de primarios con N=100; Pl=0,7; l=51)	**Qmd (Probabilidad total de reportar ausencia de primarios con N=100; Pl=0,8; l=51)**	**Qmd (Probabilidad total de reportar ausencia de primarios con N=100; Pl=0,9; l=51)**	**Qmd (Probabilidad total de reportar ausencia de primarios con N=100; Pl=1; l=51)**
M=0	0	0	0	0
M=10	9,05E-18	1,09E-17	1,28E-17	1,45E-13
M=20	5,57E-12	7,11E-12	8,62E-12	9,95E-12
M=30	5,48E-07	7,40E-07	9,31E-07	1,10E-06
M=40	0,00322094	0,00459541	0,00599783	0,00719081
M=50	0,22711967	0,34251818	0,46396272	0,56692594
M=60	0,3572702	0,56952535	0,80064862	0,99711351

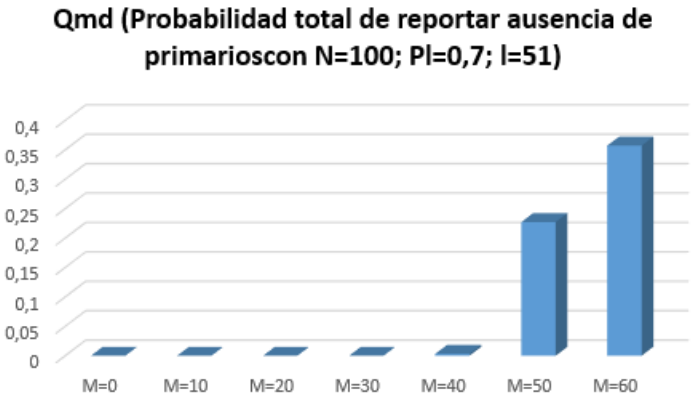

Fig. 1.9 Gráfica de probabilidad porcentual de reportar ausencia de primario con Pl=0.7

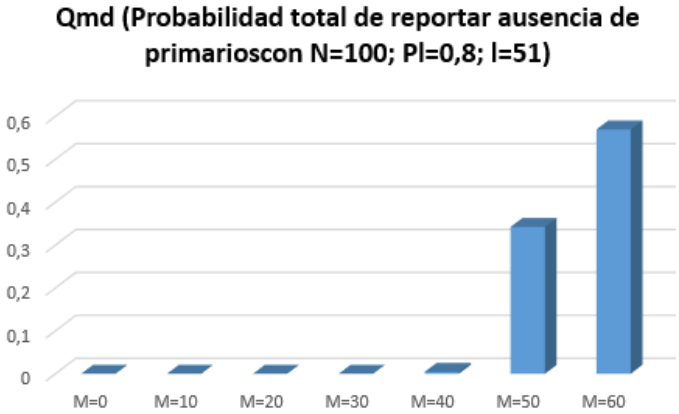

Fig. 1.10 Gráfica de probabilidad porcentual de reportar ausencia de primario con Pl=0.8

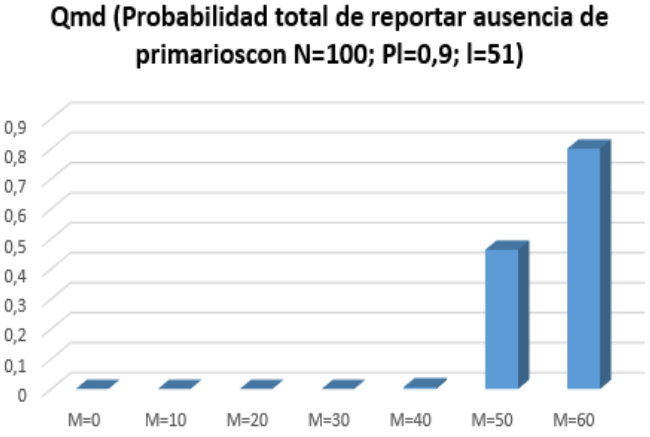

Fig. 1.11 Gráfica de probabilidad porcentual de reportar ausencia de primario con Pl=0.9

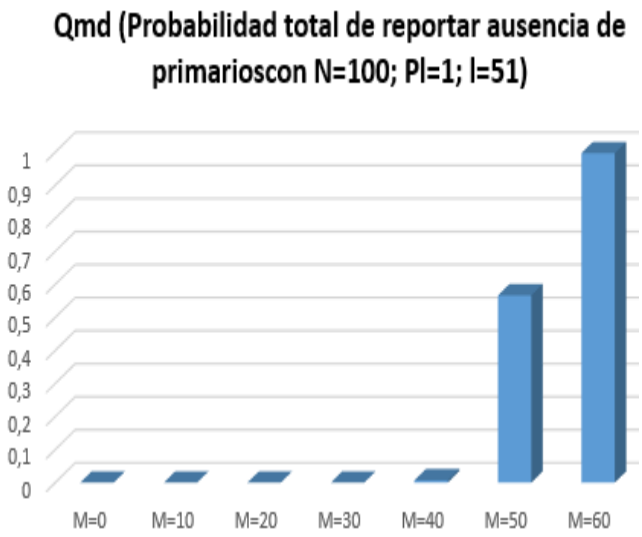

Fig. 1.12 Gráfica de probabilidad porcentual de reportar ausencia de primario con Pl=1

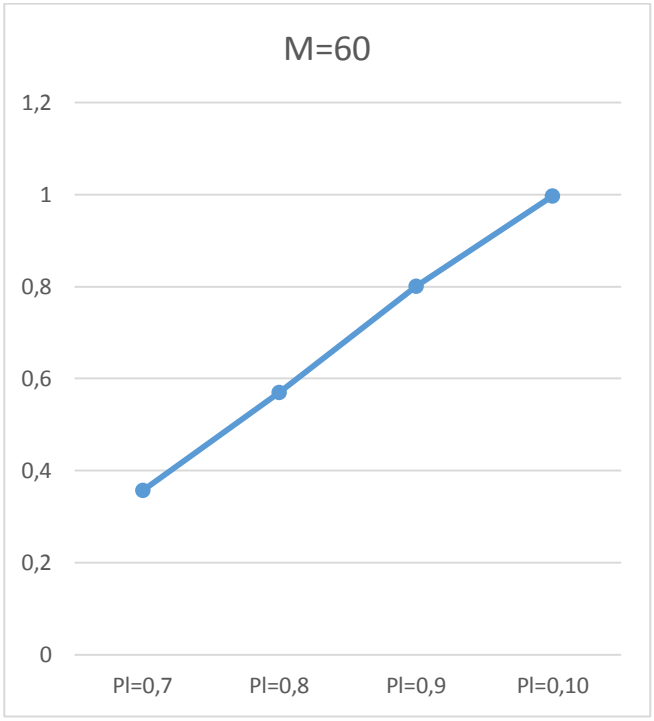

Fig. 1.13 Gráfica de probabilidad porcentual comparativa de reportar ausencia de primario con variación de Pl=(0,7 - 1).

En la Fig. 1.13, se puede observar la influencia del valor de la probabilidad de mentir por parte de los usuarios deshonestos a medida que aumenta el porcentaje Pl del 70% a 100% se ve un incremento considerable en la probabilidad de reportar ausencia de primarios Qmd, de un 35,7% hasta un 99,7%, esto debido a que se hicieron pruebas en el rango de Pl de 0% y al 100% y se pudo observar que en valores de Pl menores al 70% el nivel de afectación en el Qmd es menor al 20% y por lo tanto estos valores no afectan en la toma de decisión del CF.

CASO 4

Tabla 5. Datos obtenidos de la simulación del tercer escenario sin usuario primario y M usuarios maliciosos.

	Qfa (Probabilidad de falsa alarma N=100; Pl=0,7; l=51)	**Qfa (Probabilidad de falsa alarma N=100; Pl=0,8; l=51)**	**Qfa (Probabilidad de falsa alarma N=100; Pl=0,9; l=51)**	**Qfa (Probabilidad de falsa alarma N=100; Pl=1; l=51)**
M=0	0	0	0	0
M=10	1,69E-14	2,04E-14	2,39E-14	2,70E-14
M=20	1,84E-13	2,34E-13	2,84E-13	3,28E-13
M=30	1,59E-08	2,15E-08	2,71E-08	3,18E-08
M=40	0,00012362	0,00017638	0,0002302	0,000276
M=50	0,03815166	0,05753636	0,07793668	0,095235
M=60	0,32812398	0,52306329	0,73533149	0,915793

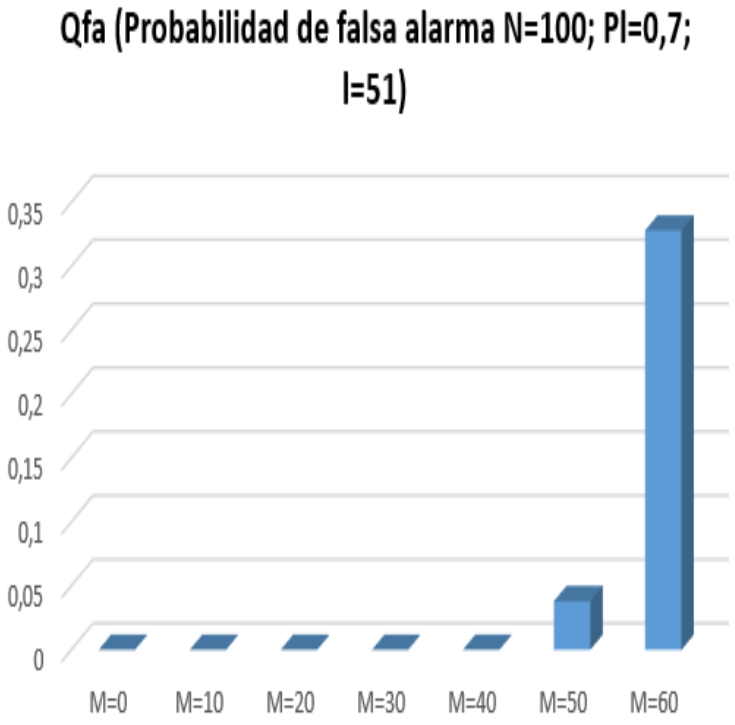

Fig. 1.14 Gráfica de probabilidad porcentual de reportar falsa alarma con Pl=0.7

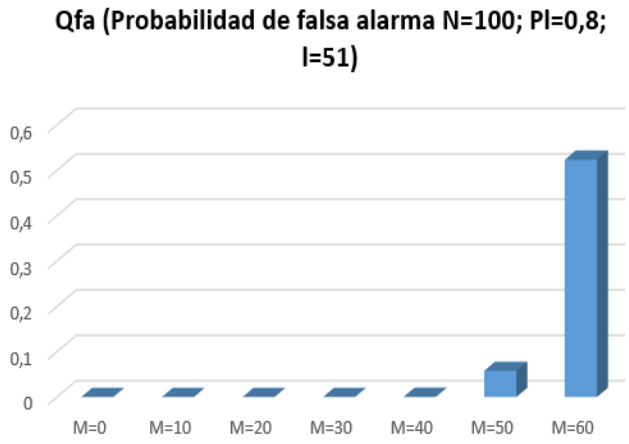

Fig. 1.15 Gráfica de probabilidad porcentual de reportar falsa alarma con Pl=0.8

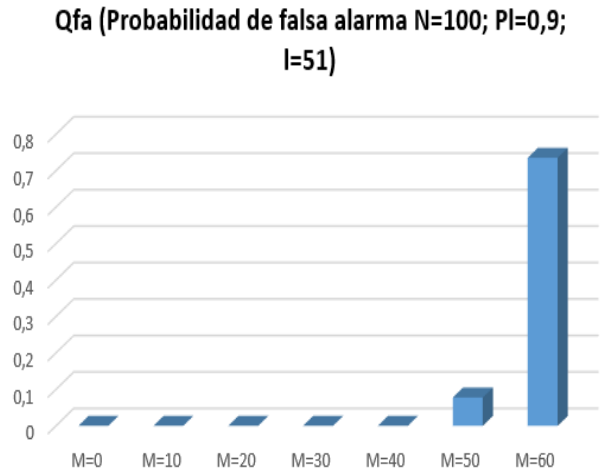

Fig. 1.16 Gráfica de probabilidad porcentual de reportar falsa alarma con Pl=0.9

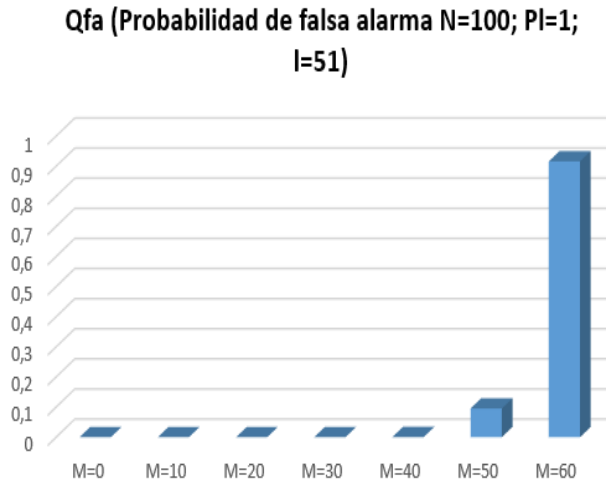

Fig. 1.17 Gráfica de probabilidad porcentual de reportar falsa alarma con Pl=1

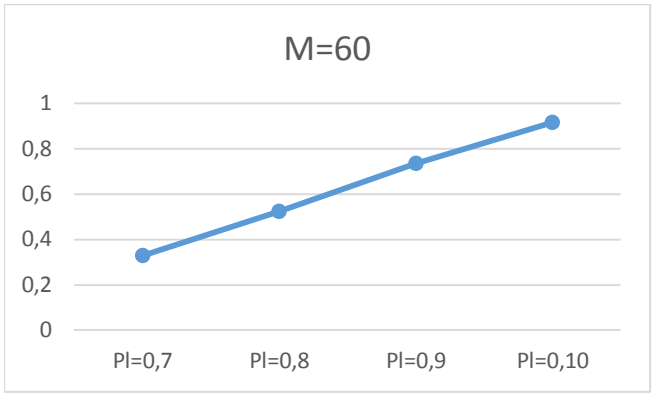

Fig. 1.18 Gráfica de probabilidad porcentual comparativa de reportar falsa alarma con Pl=(0,7 - 1).

En la Fig. 1.18, se puede observar la influencia del valor de la probabilidad de mentir por parte de los usuarios deshonestos a medida que aumenta el porcentaje Pl del 70% a 100%, se ve un incremento considerable en la probabilidad de reportar ausencia de primarios desde un 32,8% hasta un 91,6%.

3. Resultados y Discusión

Los análisis presentados a continuación son realizados tomando en cuenta los casos de mayor afectación al sistema de Radio Cognitiva (RC), en base a cada uno de los escenarios presentados anteriormente.

3.1. CASO 1

En la Fig. 1.6, se puede observar que la probabilidad de detección total del sistema es siempre un valor cercano al 100%, esto se debe claramente a la ausencia de usuarios maliciosos (M=0), pues este factor no se toma en la primera ecuación, y la probabilidad de detección que es equivalente al 90%, acorde al estándar IEEE 802.22, y dejando con esto un rango de error de reporte erróneo por parte de los usuarios secundarios honestos del 10%.

En la Fig. 1.7, se tiene que la probabilidad porcentual total de reportar ausencia de usuario primario es aproximadamente nula tendiendo al

0.18% y un reporte de probabilidad de detección total del sistema de 99,84%, en el caso de tener la menor cantidad de usuarios (N=10), esto se debe también a la ausencia de usuario maliciosos (M=0), por lo que este valor no se lo toma en cuenta en la ecuación mencionada, al igual que en el caso anterior se utilizó una probabilidad de detección del 90% por parte general del sistema en conjunto.

3.2. CASO 2

En la Fig. 1.8, se tiene la probabilidad porcentual de falsa alarma y observamos que es equivalente al 0,0147% en otras palabras, el nivel de afectación total del sistema es nulo ya que esta probabilidad se acerca a 0%, esto como en el caso anterior se debe a la falta de usuarios maliciosos y la utilización de una probabilidad de falsa alarma del 10% por parte de los usuarios secundarios, como dice el estándar IEEE 802.22.

3.3. CASO 3

En la Fig. 1.9, se tiene una la probabilidad porcentual de 35.72% de reportar ausencia de primario con una probabilidad de mentir del Pl=70%, en el caso de tener una probabilidad de detección del 90%, con un valor considerable de usuarios secundarios maliciosos M= 60.

En la Fig. 1.10, se tiene una probabilidad porcentual de 56.95% de reportar ausencia de primario con una probabilidad de mentir del Pl=80%, en el caso de tener una probabilidad de detección del 90%, con un valor considerable de usuarios secundarios maliciosos M= 60.

En la Fig. 1.11, se tiene una probabilidad porcentual de 80.06% de reportar ausencia de primario con una probabilidad de mentir del Pl=90%, en el caso de tener una probabilidad de detección del 90%, con un valor considerable de usuarios secundarios maliciosos M= 60.

En la Fig. 1.12, se tiene una probabilidad porcentual de 99.71% de reportar ausencia de primario con una probabilidad de mentir del Pl=100%, en el caso de tener una probabilidad de detección del 90%, con un valor considerable de usuarios secundarios maliciosos M= 60.

3.4. CASO 4

En la Fig. 1.14, se calculó la probabilidad porcentual de reportar falsa alarma de 32.81% con una probabilidad de mentir por parte de los usuarios secundarios maliciosos de Pl=70%, en el caso de tener una probabilidad de falsa alarma del 10%, con un valor considerable de usuarios secundarios maliciosos de M=60.

En la Fig. 1.15, se calculó la probabilidad porcentual de reportar falsa alarma de 52.30% con una probabilidad de mentir por parte de los usuarios secundarios maliciosos de Pl=80%, en el caso de tener una probabilidad de falsa alarma del 10%, con un valor considerable de usuarios secundarios maliciosos de M=60.

En la Fig. 1.16, se calculó la probabilidad porcentual de reportar falsa alarma de 73.53% con una probabilidad de mentir por parte de los usuarios secundarios maliciosos de Pl=90%, en el caso de tener una probabilidad de falsa alarma del 10%, con un valor considerable de usuarios secundarios maliciosos de M=60.

En la Fig. 1.17, se calculó la probabilidad porcentual de reportar falsa alarma de 91.57% con una probabilidad de mentir por parte de los usuarios secundarios maliciosos de Pl=100%, en el caso de tener una probabilidad de falsa alarma del 10%, con un valor considerable de usuarios secundarios maliciosos de M=60.

En general, se puede ver en las gráficas comparativas del tercer y cuarto caso, ver Fig. 1.13 y Fig1.18, que la variación de las probabilidades tanto en el caso de la ausencia o la no ausencia de usuarios licenciados, es proporcional a la probabilidad de mentir que tienen los usuarios maliciosos, pues de esta manera se obtuvo que en el reporte falso de usuarios primario del caso 3 es de 99,7% con el 100% de casos de usuarios

maliciosos que desearon mentir, mientras que en el reporte de ausencia del primario del caso 4 se obtuvo el 91,57% con el 100% de casos de usuarios que desearon mentir, cabe recalcar que estos valores porcentuales son calculados de manera independiente y no tienen ninguna correlación pues pertenecen a dos ecuaciones diferentes.

4. Conclusiones

En el presente trabajo de investigación se analizaron dos casos particulares el uno en ambiente ideal sin la intervención de usuarios maliciosos y el otro un caso real en el que ya intervienen usuarios maliciosos, de aquí se puede concluir que para el caso ideal, mientras el número de usuarios en general del sistema es mayor al 10% la afectación a la probabilidad de detección total es de un 100%, y que la probabilidad de falsa alarma es 0%, no obstante en el segundo caso donde ya intervienen usuarios maliciosos, la probabilidad total de reportar ausencia de primarios es del 99,7% aun cuando estos si existan, esto cuando el 100% de usuarios maliciosos desea mentir o sea en las peores condiciones de infiltración, mientras la probabilidad de falsa alarma es del 91,57% aun cuando los usuarios primarios si existan, para cuando el 100% de usuarios maliciosos desea mentir y se toma en cuenta un 60% de usuarios maliciosos en la red. Con estos parámetros, es importante recalcar las falencias de seguridad que se observan en dicho sistema de RRC, por lo que se tiene que aumentar dicha seguridad para aplacar los valores de vulnerabilidad, penetración y afectación del sistema de RRC hacia los usuarios licenciados ya que estos propensos a ataques en conformidad aumentan los usuarios secundarios maliciosos y los reportes erróneos por parte de los usuarios secundarios honestos, ante esto, se tienen el planteamiento que las antenas ya son inteligentes para este nuevo tipo de tecnología y pasan a ser elementos activos en la comunicación, es por eso que se propone mejorar mediante software las seguridades en CF, se deben generar códigos y filtros para la detección oportuna de usuarios maliciosos en la red y es ahí donde se debe tomar en cuenta los resultados de esta investigación en todos los diferentes escenarios analizados y de esta manera disminuir el nivel de afectación de los mismos en la toma de decisión por parte del CF.

5. Referencias

[1] P. J. R. Roig, «Control Adaptativo de Admisión e Interferencia en redes de Radio Cognitiva con Tráfico Elástico,» *Master Universitario en Tecnologias, Sistema y Redes de Comunicación Universidad Politécnica de Valencia,* p. 42, 2012.

[2] A. W. (. B. D. C. (. B. S. M. M. (. B. D. W. (. B. Robert W. Brodersen (UC Berkeley), «A COGNITIVE RADIO APPROACH FOR USAGE OF VIRTUAL UNLICENSED SPECTRUM,» *CORVUS,* nº 4, 2005.

[3] T. Y. ¨. a. H. ¨. Arslan, «A Survey of Spectrum Sensing Algorithms for Cognitive Radio Applications,» *IEEE,* p. 15, 2009.

[4] H. K. A. W. M. A. A. K. KANG G. SHIN, «COGNITIVE RADIOS FOR DYNAMIC SPECTRUM ACCESS: FROM CONCEPT TO REALITY,» *UNIVERSITY OF MICHIGAN,* 2012.

[5] K. G. S. X. H. Alexander W, «Secure Cooperative Sensing in IEEE 802.22 WRANs Using Shadow Fading Correlation,» *IEEE,* p. 14, 2011.

[6] L. S. Committee, «Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands,» *IEEE Computer Society ,* 2015.

[7] C. A. H. y. L. Giupponi, «RADIO Y REDES COGNITIVAS,» *White paper – AEI eMOV ,* p. 20, 2010.

[8] M. H. ,. D. M. a. L. D. S. Bhagavathy

Nanthini, «Attacks in Cognitive Radio Networks (CRN) — A Survey,» *Indian Joournal of Science & Technology,* p. 7, 2014.

[9] H. L. Y. (. S. a. Z. H. Wenkai Wang, «Securing Collaborative Spectrum Sensing against Untrustworthy Secondary Users in Cognitive Radio Networks,» *EURASIP Journal on Advances in Signal Processing,* p. 15, 2010.

[10] K.-H. K. J. P. S. K. G. S. Alexander W, «Opportunistic Spectrum Access for Mobile Cognitive Radios,» *IEEE,* p. 9, 2011.

[11] V. M. a. L. T. Stefano Marano, «Distributed Detection in the Presence of Byzantine Attacks,» *IEEE,* 2009.

[12] H. Moore, MATLAB para ingenieros, México: PEARSON, Prentice Hall, 2007.

[13] A. S. R. Priyank Anand, «Collaborative Spectrum Sensing in the Presence of Byzantine Attacks in Cognitive Radio Networks,» *IEEE Transactions on Signal Processing* , p. 9, Feb. 2011.

[14] H. D. Xiaofan He, «A Byzantine Attack Defender in Cognitive Radio Networks: the Conditional Frequency Check,» *IEEE,* 2015.

[15] C. Chen, «Robust and secure spectrum sensing in cognitive,» *The University of Toledo Digital Repository,* p. 104, 2013.

[16] E. A. D. S. f. I. T.--.-T. a. i. e. b. s. W. R. A. N. (WRAN), «Specific requirements Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands Amendment,» *IEEE,* pp. 1-316, 2015.

6. Agradecimiento

El presente trabajo, primeramente, me gustaría agradecerte a Dios por bendecirme para llegar hasta donde he llegado, y por darme una familia que he de admirar y querer el resto de mi vida como lo he hecho hasta ahora, y que gracias a ellos he logrado conseguir mis metas en la vida, a la Universidad Politécnica Salesiana por darme la oportunidad de estudiar y ser un profesional, y mediante esto ser un ente útil a nuestra sociedad, a mi tutor, Msc. Rafael Jaya por su esfuerzo y dedicación, quien, con sus conocimientos, su experiencia, su paciencia y su motivación ha logrado en mí que pueda terminar este proyecto de titulación con éxito, también a mis profesores que durante toda mi carrera aportaron con un granito de arena a mi formación tanto personal como profesional, son muchas las personas que han formado parte de mi vida estudiantil a las que me encantaría agradecerles su amistad, consejos, apoyo, ánimo y compañía en los momentos más difíciles de mi vida, sin importar en donde estén quiero darles las gracias por formar parte de mí, por todo lo que me han brindado y por todas sus bendiciones.