Desarrollo de un modelo para la detección de ataques SSDF en redes de radio cognitiva móvil integrando técnicas de inteligencia artificial

Ing. Lina María Yara Cifuentes, Ing. Ernesto Cadena Muñoz, Ph.D., Ing. Rafael Cubillos Sánchez, M.Sc.,
Ing. Armando Mateus Rojas, M.Sc.,
Facultad de Ingeniería Electrónica, Universidad Santo Tomás, Bogotá D.C.
lina.cifuentesyar@usantotomas.edu.co, ecadenam@udistrital.edu.co, rafaelcubillos@usantotomas.edu.co,
armandomateus@usantotomas.edu.co.

Este producto se presenta para optar al título de Magíster en Ingeniería Electrónica.

Resumen - Las redes de radio cognitiva móvil (MCRNs) permiten el acceso dinámico al espectro mediante la técnica de detección cooperativa del espectro (CSS), pero presentan vulnerabilidades frente a ataques de falsificación de datos de detección del espectro (SSDF). Diversos estudios han abordado este problema mediante técnicas de aprendizaje automático, modelos de confianza y métodos híbridos. Este artículo presenta los principales resultados de un modelo híbrido que integra máquina de vectores de soporte (SVM), el algoritmo K-Nearest Neighbors (KNN) y un sistema de reputación basado en la distribución Beta para identificar usuarios maliciosos. La validación experimental mediante radio definida por software (SDR) demuestra probabilidades de detección superiores al 90 %, una reducción significativa de falsas alarmas y una mayor robustez en condiciones de movilidad y con bajos valores de relación señal-ruido (SNR).

Palabras clave: MCRN, SSDF, aprendizaje automático, SVM, KNN, reputación, SDR.

Abstract - Mobile Cognitive Radio Networks (MCRNs) enable dynamic spectrum access through the Cooperative Spectrum Sensing (CSS) technique; however, they present vulnerabilities to Spectrum Sensing Data Falsification (SSDF) attacks. Various studies have addressed this problem using machine learning techniques, trust models, and hybrid methods. This article presents the main results of a hybrid model that integrates Support Vector Machines (SVM), the K-Nearest Neighbors (KNN) algorithm, and a reputation system based on the Beta distribution to identify malicious users. Experimental validation using Software Defined Radio (SDR) demonstrates detection probabilities above 90%, a significant reduction in false alarms, and greater robustness under mobility conditions and low Signal-to-Noise Ratio (SNR) values.

Keywords: Mobile Cognitive Radio Networks, SSDF Attack, Cooperative Spectrum Sensing, Machine Learning, Reputation Systems, SDR.

I. Introducción

El crecimiento acelerado de los dispositivos inalámbricos y de los servicios móviles ha incrementado significativamente la demanda del espectro radioeléctrico. En respuesta a este desafío, las MCRN han surgido como una solución prometedora para mejorar la eficiencia en el uso del espectro mediante el acceso dinámico a bandas subutilizadas asignadas a usuarios primarios [1], [2]. En este tipo de redes, los usuarios secundarios (SUs) realizan un proceso de CSS para identificar la presencia de usuarios primarios (PUs) y aprovechar los espacios espectrales disponibles.

Sin embargo, el carácter cooperativo del CSS introduce vulnerabilidades de seguridad. Una de las amenazas más relevantes es el ataque SSDF, también conocido como ataque bizantino, en el que nodos maliciosos envían reportes falsos al Fusion Center (FC) para alterar la toma de decisiones globales del sistema [3]. Este tipo de ataque puede provocar decisiones incorrectas sobre la ocupación del espectro, generando interferencias con los usuarios primarios o impidiendo el acceso legítimo de los SUs.

Diversos trabajos han abordado este problema mediante técnicas de detección basadas en el aprendizaje automático, modelos de confianza y algoritmos de detección de anomalías [7], [13], [22], [24], [30]. Aunque estos enfoques han mostrado resultados prometedores, muchos han sido diseñados para redes cognitivas estáticas y presentan limitaciones en entornos móviles, donde la movilidad de los nodos, las variaciones del canal y los cambios en la disponibilidad del espectro generan escenarios más complejos.

En este contexto, el objetivo de este trabajo es desarrollar y evaluar un modelo híbrido para la detección de ataques SSDF en redes MCRN, integrando técnicas de aprendizaje automático y mecanismos de reputación que mejoren la confiabilidad del proceso de detección de espectro cooperativa.

Por lo anterior, las principales contribuciones de este artículo se relacionan a continuación:

1) Propuesta de un modelo híbrido de detección que combina clasificadores supervisados (SVM y KNN) con un sistema de reputación basado en la distribución Beta para identificar usuarios secundarios maliciosos.

2) Integración de la información física del canal, como la energía recibida y la SNR, en el proceso de clasificación para mejorar la precisión de la detección.

3) Validación experimental del modelo propuesto mediante un entorno de pruebas basado en SDR, que permite evaluar el desempeño del sistema en condiciones reales de comunicación

y en presencia de atacantes.

4) Los resultados obtenidos muestran que la combinación de técnicas de aprendizaje automático con mecanismos de reputación mejora significativamente la capacidad de detección de ataques SSDF y reduce la tasa de falsas alarmas, incluso en escenarios con condiciones adversas de señal y la presencia de múltiples usuarios maliciosos.

En ese contexto, el artículo se organiza de la siguiente manera: la Sección II describe el modelo de detección propuesto. La Sección III presenta la metodología y el entorno experimental empleados. La Sección IV analiza los resultados obtenidos y discute el desempeño del sistema. Finalmente, la Sección V presenta las conclusiones del estudio.

II. Modelo Propuesto

A. Arquitectura del sistema

La arquitectura híbrida del sistema se muestra en la Fig. 1. Cada SU transmite al FC los parámetros físicos del canal, principalmente la energía y la SNR, siguiendo el esquema de detección cooperativa descrito en [2] y [6]. Estos datos se procesan mediante módulos de aprendizaje automático y de reputación para generar la decisión global.

Figura 1. *Modelo general de detección para el proceso de entrenamiento (fuente: propia).*

B. Extracción de características

La detección de energía es una técnica ampliamente utilizada en redes cognitivas debido a su baja complejidad y a su eficiencia en entornos dinámicos [34]. En ese sentido, el estadístico principal utilizado como entrada al modelo es el indicado en la ecuación (1):

$$y_i = \sum_{t=1}^{N} |y_i(t)|^2 \tag{1}$$

Donde: (y_i) representa la energía recibida por el usuario secundario (i).

C. Sistema de reputación

Los mecanismos de confianza basados en distribuciones Beta se han utilizado para mitigar ataques SSDF dinámicos y evaluar la confiabilidad de los SUs [13], [21]. En este trabajo, el puntaje de reputación se define como se muestra en la ecuación (2):

$$R_i = \frac{r_i + 1}{r_i + s_i + 2} \tag{2}$$

Donde:
R_i: Es el valor de reputación del usuario secundario i, utilizado para ponderar su contribución a la toma de decisiones globales del sistema.
r_i: El número de reportes correctos del usuario i, que coinciden con la decisión del FC.
s_i: El número de reportes incorrectos o discrepancias del usuario i.
i: El índice que identifica al SU en la red.

D. Clasificación Híbrida (SVM + KNN)

El uso de clasificadores supervisados ha demostrado alta precisión en la detección de anomalías en redes cognitivas [24], mientras que los métodos basados en vecinos cercanos permiten capturar relaciones no lineales en entornos dinámicos [30].

En este caso, mediante el clasificador SVM se establece la frontera de decisión como se muestra en la ecuación (3):

$$f(\vec{x}) = sign\Big(\sum_{=1}^{l} \alpha_i y_i K(\vec{x_j}, \vec{x_i}) + b\Big) \tag{3}$$

Donde:
$K(\cdot,\cdot)$: función kernel.
$yj \in -1, +1$: etiqueta de clase.
αj: multiplicadores de Lagrange.
b: término de sesgo (bias).

Por su parte, KNN evalúa la similitud entre reportes mediante distancia euclidiana, como se muestra en la ecuación (4):

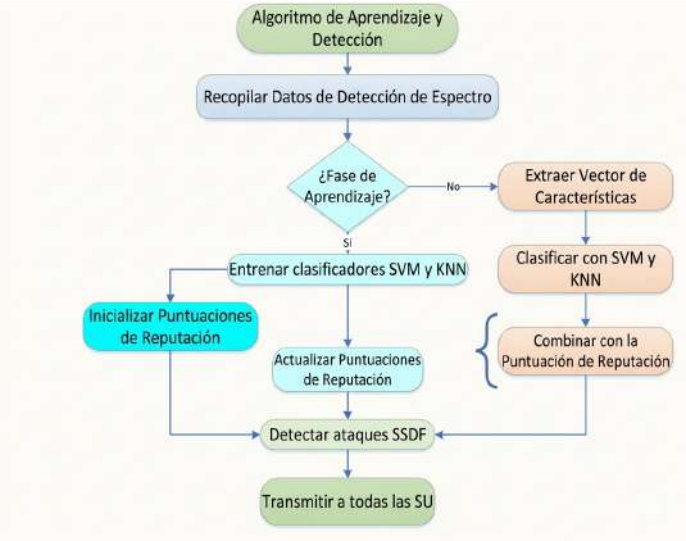
$$d(x_i, x_j) = \sqrt{\sum_{j=1}^{n} (x_j - x_{ik})^2} \tag{4}$$

Donde: x_j es el vector de características de la j-ésima muestra de entrenamiento. A partir de estos vectores, el modelo de detección KNN asigna la clase que aparece con mayor frecuencia entre los k vecinos más cercanos mediante un esquema de votación mayoritaria.

III. Metodología y escenario experimental

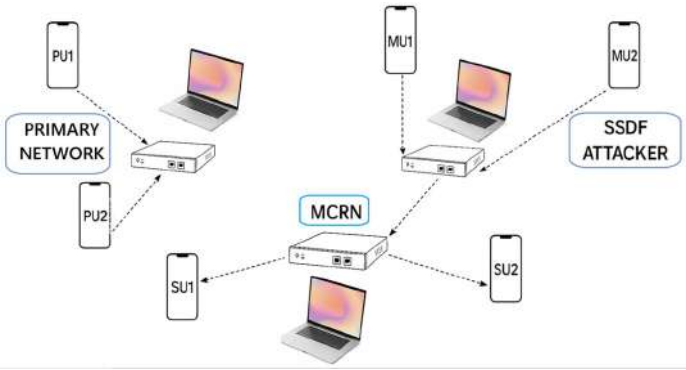
El flujo general del proceso de aprendizaje y detección se muestra en la Fig. 2. En esta propuesta, el diseño experimental sigue metodologías de validación con SDR empleadas en estudios recientes sobre redes cognitivas móviles [5], [31].

Figura 2. *Diagrama de flujo del proceso de aprendizaje y detección (fuente: elaboración propia).*



Para la validación experimental de la propuesta, se implementó un banco de pruebas compuesto por dispositivos RTL-SDR, radios NI USRP-2922, la plataforma GNU Radio y smartphones comerciales, como se muestra en la Fig. 3. A partir de este entorno, se recopilaron aproximadamente 10.000 muestras en la banda de 850 MHz, considerando escenarios con y sin ataques SSDF. En este proceso, la energía de la señal y la SNR se utilizaron como variables principales para el análisis y la construcción del modelo de detección.

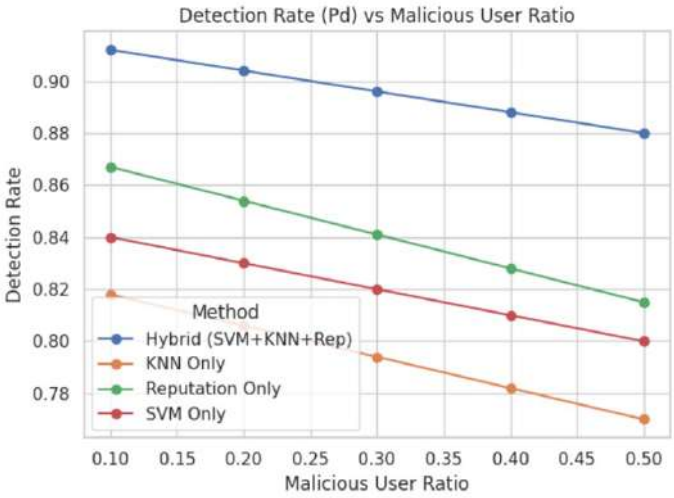
Figura 3. *Banco de pruebas para experimentos con SDR (fuente: elaboración propia).*



IV. Resultados Experimentales

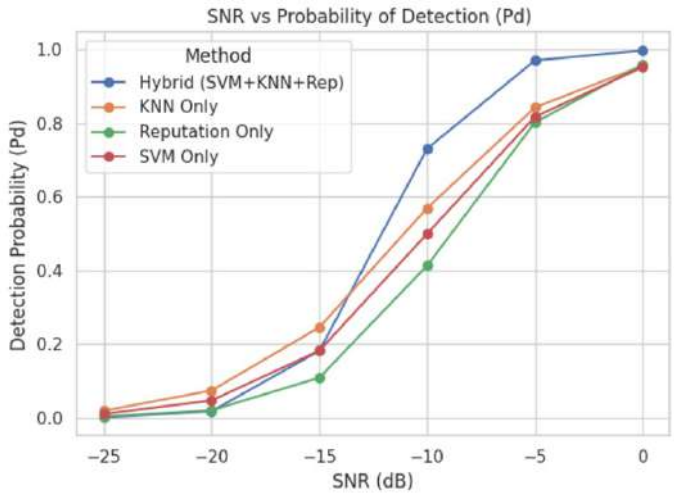
La Fig. 4 muestra la tasa de detección del modelo híbrido frente a diferentes proporciones de usuarios maliciosos, manteniendo probabilidades superiores a 0.88 incluso ante una alta presencia de atacantes.

Figura 4. *Tasa de detección del modelo híbrido vs. proporción de usuarios maliciosos (fuente: elaboración propia).*



La Fig. 5 muestra la probabilidad de detección en función del SNR, lo que evidencia mejoras significativas frente a clasificadores individuales en condiciones adversas, resultados que coinciden con enfoques basados en aprendizaje profundo y en métricas de Received Signal Strength (RSS) [31], [32].

Figura 5. *Probabilidad de detección vs. SNR (fuente: elaboración propia).*



Los resultados relevantes obtenidos en esta investigación son:

1) Con SVM se alcanzó una precisión superior al 96%.

2) Con KNN se obtuvieron tasas de detección superiores al 88%.

3) El modelo híbrido alcanzó una exactitud global aproximada del 94%.

V. Discusión

El uso combinado del aprendizaje automático y de la reputación permite una evaluación multicapa que mejora la confiabilidad del CSS. Mientras que SVM proporciona estabilidad

en la frontera de decisión [24], KNN permite adaptabilidad ante variaciones del entorno [30] y el sistema de reputación introduce una memoria histórica del comportamiento de los usuarios [7], [13].

VI. Conclusiones

Se presentó un modelo híbrido para la detección de ataques SSDF en MCRNs que integra el aprendizaje automático y mecanismos de confianza. La validación experimental mediante SDR confirma mejoras significativas en la precisión, la reducción de falsas alarmas y la robustez frente a condiciones dinámicas, lo que fortalece la seguridad de la detección en CSS.

Reconocimiento

Los autores agradecen a la Universidad Santo Tomás la financiación del proyecto de investigación a través del Proyecto FODEIN 2024, así como el apoyo para el APC. Asimismo, se reconoce a la Universidad Distrital Francisco José de Caldas por la provisión de los dispositivos y recursos tecnológicos utilizados en el desarrollo experimental de esta investigación. La metodología, el software y la arquitectura de hardware del modelo propuesto fueron concebidos por L. M. Yara Cifuentes y E. Cadena Muñoz. El diseño experimental fue desarrollado por E. Cadena Muñoz, L. M. Yara Cifuentes y R. Cubillos Sánchez. La ejecución de los experimentos fue realizada por L. M. Yara Cifuentes, E. Cadena Muñoz y R. Cubillos Sánchez. El análisis de resultados, la revisión y la edición del manuscrito fueron realizados por L. M. Yara Cifuentes, E. Cadena Muñoz y R. Cubillos Sánchez. Todos los autores participaron en la discusión de los resultados y en la revisión del documento, y aprobaron la versión final del artículo.

Referencias

[1] S. Solanki, V. Dehalwar, y J. Choudhary, Deep learning for spectrum sensing in cognitive radio, Symmetry, vol. 13, n.o 1, p. 147, 2021.

[2] G. Manoranjan, M. Chandan, G. Karthik, R. Satpathy, y S. Sugumaran, Security against ssdf attacks using novel attack mitigation mechanism for cognitive radio networks, en 2021 Fourth International Conference on Electrical, Computer and Communication Technologies (ICECCT), IEEE, 2021, pp. 1-6.

[3] A. Paul, A. K. Mishra, S. Shreevastava, y A. K. Tiwari, Deep reinforcement learning based reliable spectrum sensing under SSDF attacks in cognitive radio networks, J. Netw. Comput. Appl., vol. 205, p. 103454, 2022.

[4] R. Sarmah, A. Taggu, y N. Marchang, Detecting Byzantine attack in cognitive radio networks using machine learning, Wirel. Netw., vol. 26, n.o 8, pp. 5939-5950, 2020.

[5] S. Banerjee, T. Singh, y K. R. Singh, Mitigation of spectrum sensing data falsification attack (ssdf) in cognitive radio network, J. Inst. Eng. India Ser. B, vol. 103, n.o 4, pp. 1249-1257, 2022.

[6] R. Wan, L. Ding, N. Xiong, y X. Zhou, Mitigation strategy against spectrum-sensing data falsification attack in cognitive radio sensor networks, Int. J. Distrib. Sens. Netw., vol. 15, n.o 9, p. 1550147719870645, 2019.

[7] A. Ahmadfard, A. Jamshidi, y A. Keshavarz-Haddad, Probabilistic spectrum sensing data falsification attack in cognitive radio networks, Signal Process., vol. 137, pp. 1-9, 2017.

[8] S. Chatterjee y P. S. Chatterjee, A comparison based clustering algorithm to counter SSDF attack in CWSN, en 2015 International Conference on Computational Intelligence and Networks, IEEE, 2015, pp. 194-195.

[9] X. Zhi, Y. Cao, y X. Liu, Anti-Dynamic SSDF Attack Scheme Based on Credit Mechanism, en 2024 4th International Conference on Electronic Information Engineering and Computer (EIECT), IEEE, 2024, pp. 875-879.

[10] R. Kumar, A. Parmar, K. Captain, y J. Patel, Reinforcement learning for performance improvement in cooperative spectrum sensing, Phys. Commun., vol. 59, p. 102112, 2023.

[11] A. Antoinette y S. Buvaneswari, Security and Energy Management in Cooperative Spectrum Sensing, Procedia Comput. Sci., vol. 230, pp. 716-724, 2023.

[12] L. P. Rachakonda, M. Siddula, y V. Sathya, A comprehensive study on IoT privacy and security challenges with focus on spectrum sharing in Next-Generation networks (5G/6G/beyond), High-Confid. Comput., p. 100220, 2024.

[13] M. Liu, L. Liu, D. Xu, y L. Zhang, Cognitive IoT Collusion SSDF Attack Detection Based on FP-Growth Algorithm, J. Netw. Syst. Manag., vol. 33, n.o 2, p. 25, 2025.

[14] J. Feng, M. Zhang, Y. Xiao, y H. Yue, Securing cooperative spectrum sensing against collusive SSDF attack using XOR distance analysis in cognitive radio networks, Sensors, vol. 18, n.o 2, p. 370, 2018.

[15] F. Zardosht, M. Derakhtian, A. Jamshidi, y H. Eshaghi, Recognition and elimination of SSDF attackers in cognitive radio networks, Telecommun. Syst., vol. 81, n.o 1, pp. 53-66, 2022.

[16] Y. Liu, A. H. Shaikh, y W. M. Khoso, Impact of Spectrum Sensing Data Falsification Attack and Imperfect Reporting Channel on Cooperative Spectrum Sensing, en 2023 9th International Conference on Computer and Communications (ICCC), IEEE, 2023, pp. 470-474.

[17] T. Peng, Y. Chen, J. Xiao, Y. Zheng, y J. Yang, Improved soft fusion-based cooperative spectrum sensing defense against SSDF attacks, en 2016 International Conference on Computer, Information and Telecommunication Systems (CITS), IEEE, 2016, pp. 1-5.

[18] L. Li, F. Li, y J. Zhu, A method to defense against cooperative SSDF attacks in Cognitive Radio Networks, en 2013 IEEE International Conference on Signal Processing, Communication and Computing (ICSPCC 2013), IEEE, 2013, pp. 1-6.

[19] P. S. Chatterjee, Systematic survey on SSDF attack and detection mechanism in cognitive wireless sensor network, en 2021 International Conference on Intelligent Technologies (CONIT), IEEE, 2021, pp. 1-5.

[20] Y. Fu y Z. He, An online learning approach for cooperator selection in CSS under SSDF attack, IEEE Commun. Lett., vol. 26, n.o 7, pp. 1479-1483, 2022.

[21] A. A. Reddy, V. S. A. Gandlapalli, K. V. Sai, y R. B. Battula, Secure spectrum sensing in CRNs: A study on SSDF attacks and countermeasure using USRP, en 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE, 2024, pp. 1-5.

[22] D. Yao, S. Yuan, Z. Lv, D. Wan, y W. Mao, An enhanced cooperative spectrum sensing scheme against SSDF attack based on Dempster-Shafer evidence theory for cognitive wireless sensor networks, IEEE Access, vol. 8, pp. 175881-175890, 2020.

[23] S. Liu, Q. Liu, J. Gao, y J. Guan, Attacker-exclusion scheme for cooperative spectrum sensing against SSDF attacks based on accumulated suspicious level, en 2011 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems, IEEE, 2011, pp. 239-243.

[24] A. A. Sharifi y M. J. M. Niya, Defense against SSDF attack in cognitive radio networks: Attack-aware collaborative spectrum sensing approach, IEEE Commun. Lett., vol. 20, n.o 1, pp. 93-96, 2015.

[25] Z. Cheng, J. Zhang, T. Song, J. Hu, y X. Bao, Detection strategy against restricted SSDF attack with potential interaction assistance, IEEE Trans. Cogn. Commun. Netw., vol. 7, n.o 2, pp. 553-566, 2020

[26] X. Wu, Z. Tang, Y. Lu, D. Wu, H. Xiao, y Y. Tang, Cooperative spectrum sensing method against spectrum sensing data falsification attack, en 2023 24st Asia-Pacific Network Operations and Management Symposium (APNOMS), IEEE, 2023, pp. 66-70.

[27] S. Nath, N. Marchang, y A. Taggu, Mitigating SSDF attack using K-Medoids clustering in cognitive radio networks, en 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2015, pp. 275-282.

[28] F. Ye, X. Zhang, y Y. Li, Comprehensive reputation-based security mechanism against dynamic SSDF attack in cognitive radio networks, Symmetry, vol. 8, n.o 12, p. 147, 2016.

[29] P. Bai, X. Zhang, y F. Ye, Reputation-based Beta reputation system against SSDF attack in cognitive radio networks, en 2017 Progress in Electromagnetics Research Symposium-Fall (PIERS-FALL), IEEE, 2017, pp. 792-799.

[30] A. S. S. Musuvathi, J. F. Archbald, T. Velmurugan, D. Sumathi, S. Renuga Devi, y K. Preetha, Efficient improvement of energy detection technique in cognitive radio networks using K-nearest neighbour (KNN) algorithm, EURASIP J. Wirel. Commun. Netw., vol. 2024, n.o 1, p. 10, 2024.