Estimación Probabilística del Riesgo en Redes Eléctricas ante Ataques MaDIoT: Un Enfoque Multicapa

Farid Bagheri-Gisour Marandyn, Néstor Rodríguez-Pérez, Mario Castro Ponce, Lukas Sigrist, Gregorio López López
Instituto de Investigación Tecnológica, Universidad Pontificia Comillas, Calle de Alberto Aguilera, 23, 28015 Madrid
{fbagherigisour, nrodriguezp, marioc, lsigrist, gllopez}@comillas.edu

Resumen- **Este artículo presenta una propuesta de modelo para la estimación del nivel de riesgo de una red eléctrica dada a ser afectada por un ataque de tipo MaDIoT (*Manipulation of Demand via IoT*). Para conseguir dicho objetivo, se emplea un diseño multicapa donde la estimación del riesgo global de la red parte de la estimación de riesgo a nivel de dispositivo, a través del estudio de vulnerabilidades conocidas proporcionadas mediante OSINT, seguido de la estimación de riesgo de compromiso de cierta potencia de un nodo de la red, mediante la generación por Monte Carlo de dos funciones de densidad de probabilidad marginales para dos escenarios extremos (*best-case, worst-case*), y finalizando por la estimación del riesgo global de la red, a través de la categorización en niveles de la función de densidad de probabilidad conjunta obtenida mediante simulaciones en PowerFactory de diferentes escenarios de nodos para dos modelos de red (IEEE9, IEEE39). Asimismo, el artículo muestra y compara los resultados obtenidos utilizando diferentes algoritmos de *machine learning*, destacando los que proporcionan mejores resultados.**

***Index Terms*- análisis de riesgo, ciberseguridad, redes eléctricas, aprendizaje máquina, *clustering*, *Manipulation of Demand via IoT*.**

Tipo de contribución: *Investigación original*

I. Introducción

Las redes eléctricas modernas enfrentan nuevas amenazas ciberfísicas debido a la proliferación de dispositivos del Internet de las Cosas (IoT) conectados al sistema eléctrico. De entre las amenazas que surgen debido a la implementación de nuevos sistemas IoT, emerge un ejemplo crítico de amenazas que son los denominados ataques MaDIoT (*Manipulation of Demand via IoT*) [1]. En estos ataques, un atacante controla en masa dispositivos IoT de alto consumo (como aires acondicionados, calefactores, cargadores de vehículo eléctrico, etc.) con el objetivo de alterar drásticamente la demanda eléctrica. Estos ataques coordinados pueden provocar efectos tales en la red como inestabilidades de frecuencia y desconexión de generadores [2], sobrecarga de líneas, resonancias y apagones en cascada [1] y/o aumento de los costos operativos [1].

Dado la potencial severidad de los ataques MaDIoT, ha sido crucial desde el mundo de la ciberseguridad, entre otras, la evaluación del riesgo asociado al incremento de dispositivos de IoT (sobre todo de alto consumo) en las diferentes redes eléctricas. Para ello, la literatura aborda este análisis en términos de probabilidad de que ocurra un ataque exitoso [3] y consecuencias esperadas en caso de que ocurra [4-5].

Las metodologías tradicionales de análisis de riesgos se basan en fases predefinidas (identificación de activos, evaluación de amenazas, evaluación de riesgos) y, a menudo, carecen de actualización dinámica, lo que las hace insuficientes para manejar amenazas en constante evolución. La literatura reciente propone metodologías de Evaluación Dinámica de Riesgos (DRA, por sus siglas en inglés), que incorporan fuentes de datos en tiempo real tales como: sistemas de seguridad (IDS/IPS/SIEM) [6-13], datos históricos de vulnerabilidades, como CVSS [12-13], [14-17], conocimiento del sistema, para evaluar continuamente los riesgos [18-19] y conocimiento experto, para la toma de decisiones [20]. Además, los enfoques que aprovechan el aprendizaje automático (por ejemplo, redes bayesianas, redes neuronales) [6-12], [20] y modelos híbridos [21-22] que combinan datos cuantitativos y cualitativos han mostrado resultados prometedores [23].

En este aspecto, la gran mayoría de estudios se centran en metodologías cuantitativas, donde los diferentes sistemas de información y seguridad son utilizados como fuentes principales para poder suministrar de datos a los modelos propuestos. Solo una pequeña parte de los estudios observados en la materia platean sistemas basados en metodologías cualitativas y, por orden de utilización, el último sería los métodos híbridos, provocando que se carezca de propuestas con un mapeo continuo y multicapa desde las vulnerabilidades de cada dispositivo IoT hasta el impacto operativo en la red eléctrica.

Este artículo se centra en el estudio de la probabilidad de que un ataque MaDIoT tenga efecto en la red eléctrica de estudio (IEEE9 e IEEE39) y, asimismo, en la conversión de esa probabilidad en una categoría de riesgo asociado (escalar, acotada), en tiempo real.

Con dicho objetivo en mente, se plantea un modelo multicapa subdividido en 3 tareas principales: estimación del riesgo a nivel de dispositivo, estimación del riesgo de potencia comprometida a nivel de nodo de red y estimación del riesgo global de la red eléctrica bajo estudio.

En referencia a la primera tarea, la estimación del riesgo de los dispositivos se obtiene en función de lo descrito en el artículo [24], donde a través del estudio de las vulnerabilidades asociadas a dichos dispositivos y mediante el enriquecimiento de sus características conocidas (firmware, versión, *vendor*, etc.) por fuentes OSINT como el NIST NVD, se permite conocer el riesgo asociado a ese dispositivo.

Con relación a la segunda tarea, el riesgo de compromiso de cierta potencia de un nodo es obtenida a través de la generación de su función densidad de probabilidad (PDF) marginal de compromiso de potencia. Esta PDF, al no poder ser obtenida empíricamente de antemano, ya que no se conocen los dispositivos a priori, se construye a través de

simulaciones por Monte Carlo de dos escenarios extremos, a los que denominamos *best-case* y *worst-case*. Estos escenarios son implementados mediante dos variables aleatorias que los modelan.

Por lo que se refiere a la tercera tarea, la estimación del riesgo global de la red, se generó una subdivisión de éste en dos flujos: *offline* y *online*.

En la parte *offline* se desarrollan dos tareas: el proceso relativo a la obtención de la PDF conjunta de compromiso de la red de estudio, descrita mediante las cargas deslastradas y/o protecciones activadas y la categorización de esas PDFs conjuntas en niveles de riesgo. Esta categorización en niveles de riesgo se realiza mediante la creación de umbrales (para cada una de las características que describen la PDF conjunta), a través del estudio y selección de diferentes modelos de *clustering*

Por último, en la parte *online*, se desarrolla el flujo encargado de determinar, en tiempo real, esa categoría de riesgo asociado a la red. Para ello, se ingesta las entradas relativos a los dispositivos que posee la red y la propia topología de la red y se pasan a comparar con las simulaciones de los diferentes casos de la parte offline, obteniendo el valor de riesgo asociado.

II. METODOLOGÍA

El diseño del modelo propuesto (véase Fig. 1) consta de una arquitectura que engloba, a alto nivel, 3 bloques diferenciados (A, B y C) que, aunque trabajen de manera conjunta al formar parte del mismo flujo de datos, realizan tareas diferenciadas unas de otras, las cuales se listan a continuación:

- **Bloque A**: Subproceso encargado de la ingesta de los ficheros relativos a las características de los dispositivos (tipología, producto, marca, versión, geolocalización, CPE y potencia máxima) y a la topología de la red (actualmente relativa a los modelos IEEE9 y IEEE39).
- **Bloque B**: Subproceso encargado del enriquecimiento de los ficheros ingestados en el Bloque A referentes a los dispositivos. Este segundo bloque se realiza según lo descrito en [24].
- **Bloque C**: Subproceso encargado de determinar y categorizar el riesgo global de la red eléctrica. Dicho bloque se subdivide a su vez en dos tareas interrelacionadas y dependientes: estimación del riesgo de compromiso de cierta potencia de un nodo y estimación del riesgo global de la red eléctrica.

Con el objetivo de poder calcular a tiempo real el riesgo asociado a la red (y previamente a la de los nodos particulares), las subtareas del Bloque C se dividen en dos flujos paralelos, a las que denominamos *offline* y *online.*

El flujo *offline* es el encargado de realizar todos los cálculos a priori necesarios para tener una base empírica con la que poder realizar la clasificación del riesgo. Estos cálculos son referentes a:

- Generación de las PDFs marginales de los dos casos extremos (*best-case, worst-case*).
- Utilización de las PDFs marginales para la simulación en PowerFactory de los efectos en red relativos a cargas deslastradas y protecciones activadas. Los datos obtenidos permiten constituir la PDF conjunta de la red.
- Empleo de la PDF conjunta de la red para calcular y establecer umbrales en cada una de las características que la componen.
- Estimación de la categoría de riesgo (escalar, acotado) de la red a partir de los umbrales establecidos anteriormente.

Fig. 1: Arquitectura de estimación y categorización de riesgo propuesta.

En contraposición, el flujo *online* es el encargado de gestionar todo el ciclo de datos en tiempo real, utilizando según corresponda, los valores previos obtenidos en el flujo *offline,* con el objetivo de generar la categoría de riesgo asociada a la red de estudio. Para ello, se definen los siguientes pasos:

- Cálculo de la PDF marginal de los nodos a tiempo real en base a los valores de riesgo de cada uno de los dispositivos que componen el nodo, recogido en el fichero enriquecido del Bloque B.
- Comparación iterativa de la PDF marginal de cada nodo obtenida en el flujo *online* con las dos PDFs marginales de los escenarios *best-case*, *worst-case* definidos y generados en el flujo *offline.*
- Selección en base a la comparación de las PDFs marginales y de la PDF conjunta de la red que corresponda a los escenarios (*best-case*, *worst-case*) seleccionados por cada nodo.
- Adquisición de los umbrales asociados a la PDF conjunta seleccionada, calculadas en el flujo *offline*.
- Obtención de la categoría de riesgo asociada a la red.

En aras de precisar cada uno de los pasos que se realizan en ambas ramas, se detalla en las siguientes secciones los diferentes hitos que se han listado anteriormente.

A. Offline - Generación de las PDFs marginales de los casos escenario de los nodos

Como consecuencia de que no se posee información a priori relativa a la cantidad y características de los dispositivos que conforman la red bajo estudio, se generan dos casos de escenarios extremos con los que poder modelar los nodos: *best-case, worst-case*. El objetivo de estos escenarios es crear dos contextos de ataque diferenciados que pueda sufrir una red: uno en el que el ataque no suponga una gran amenaza (pocos dispositivos, con un riesgo bajo de compromiso y una potencia baja) y otro en el que el ataque sí suponga una amenaza considerable (muchos dispositivos, con un riesgo alto de compromiso y una potencia alta).

Para la conformación de estos escenarios, se realiza la configuración de una variable aleatoria que se caracteriza por medio de tres distribuciones:

- **Cantidad de dispositivos**: Modelado a través de una distribución uniforme $X \sim \mathcal{U}(a, b)$, siendo *Best-case* $X \sim \mathcal{U}(5, 100)$ y *Worst-case* $X \sim \mathcal{U}(100, 2000)$.
- **Probabilidad de compromiso del dispositivo**: Modelado a través de una distribución $Y \sim \text{Bernoulli}(p)$ donde p queda definido a través de una distribución uniforme $p \sim \mathcal{U}(a, b)$. En el *Best-case*: p $\sim \mathcal{U}(0, 0.3)$ y en el *Worst-case*: $p \sim \mathcal{U}(0.7,1)$.
- **Potencia comprometida del dispositivo**: Modelado a través de una distribución uniforme $Z \sim \mathcal{U}(a, b)$ con un rango para el *Best-case* $Z \sim \mathcal{U}(0.001, 0.1)$ MW y para el *Worst-case* $Z \sim \mathcal{U}(0.1,0.5)$ MW.

Tras caracterizar la variable aleatoria que modela los nodos en cada uno de los escenarios establecidos, mediante simulaciones por Monte Carlo, se realiza el cálculo de la PDF y posteriormente de la función densidad de probabilidad acumulada (CDF). Las simulaciones Monte Carlo constan de 1.000.000 de iteraciones para caso. Todos los valores fueron normalizados en función de la P_{max} de cada uno de los nodos de los modelos de red eléctrica utilizados.

B. Offline – Generación de la PDF conjunta de la red

El objetivo de esta subtarea es generar la PDF conjunta de la red para que pueda ser caracterizada y poder estimar su riesgo.

Como no se posee información a priori relativa a la topología de la red de estudio (está vendrá definida posteriormente en la rama *online*, si es proporcionada, al igual que los dispositivos), fue necesario definir modelos de redes eléctricas a analizar. Como aproximación para este estudio, se seleccionar los modelos de red IEEE9 e IEEE39, ampliamente utilizados en investigación. Dichos modelos de red poseen, respectivamente, 3 y 19 nodos con demanda conectada.

Utilizando la herramienta de simulación DIgSILENT PowerFactory, por cada modelo de red y por cada tipo de escenario de nodo, se pasó a generar las simulaciones que nos permitan poder generar la PDF conjunta. Para el modelo IEEE9 (3 nodos con demanda) se establecen 1000 simulaciones para cada uno de los casos escenario: *best-case*, *worst-case* y *mix-case* (siendo esta, combinación de las 2 anteriores) y por cada nodo. Análogamente, para el modelo IEEE39 (19 nodos con demanda), se establecen 1000 simulaciones para cada uno de los mismos casos escenario y por cada nodo (excepto *mix-case*, que solo tendrá configuración de 19 nodos debido a la explosión combinatoria).

De los resultados de las simulaciones se utilizan las cargas deslastradas (MW) y las protecciones activas (subfrecuencia, sobrefrecuencia, subtensión, sobretensión), para generar la PDF conjunta, ya que proporcionan información de contingencia ante anomalías en la red (sobrecarga) e interpretación directa con posteriores valores de umbrales.

C. Offline – Cálculo de los umbrales en las características objetivo

Dentro de la metodología aplicada, los umbrales se tienen que definir para poder delimitar rangos de valores dentro de cada una de las características que se seleccionan en la PDF conjunta de la red. A esos rangos de valores, posteriormente se le asociará un nivel de riesgo.

Para poder establecer cuáles son los umbrales que mejor ajusten esos rangos de valores, se utilizaron y compararon diferentes algoritmos de agrupamiento (clustering) para obtener la mejor aproximación. En concreto, los algoritmos de agrupamiento empleados incluyeron K-Means++, GMM y DBSCAN para la generación de los diferentes clústeres.

Los algoritmos de agrupamiento en sí no proporcionan directamente los umbrales entre los clústeres, sino que identifican los clústeres y sus centroides. Para determinar los umbrales dentro de este marco, se calculó el valor medio de las distancias entre los centroides (o medias, en el caso de los algoritmos probabilísticos) de los clústeres ordenados de forma consecutiva para las características seleccionadas (deslastre de cargas, protecciones activas).

D. Offline – Estimación del riesgo de la red en base a los umbrales

La estimación del riesgo de la red estará determinada en función de los valores de las características seleccionadas arrojadas por las simulaciones. Lo que hay que determinar es la asociación de esos valores numéricos con una categoría o nivel de riesgo. Esta asociación se realizó utilizando los umbrales como *proxy*. El proceso, es el siguiente:

1. Por cada una de los modelos de *thresholding*, se utilizan los valores de los *thresholds* para separar las PDFs de las características en rangos.
2. De forma ordenada e incremental, se asocian esos rangos de valores a niveles de riesgo (de menor a mayor riesgo).
3. Un evento, proveniente del flujo online será comparado con las diferentes PDFs de las características de estudio del modelo de red que provenga el evento.
4. La comparación con todas las características provoca la conformación de un vector de Riesgo ($\text{Risk}_{\text{vector}}$)
5. El valor final de riesgo de red será el valor máximo de ese vector de riesgo: $\max(Risk_{vector})$

E. Online – Generación de la PDF marginal de los nodos en tiempo real

Con respecto a la rama *online*, para poder obtener la estimación del riesgo de la red a tiempo real, es necesario calcular las PDFs marginales de cada nodo en función de los datos que se ingesten del Bloque B.

Uno de los métodos matemáticos posibles para calcular una PDF mixta compuesta de múltiples variables aleatorias con sus propias PDFs es utilizar la operación convolución.

Con ello y mediante la utilización de la *Fast Fourier Transform* (FFT), que mejora la eficiencia del cálculo de la convolución, se realiza el cálculo de la PDF marginal en tiempo real por cada uno de los nodos. El proceso de cálculo es el siguiente:

1. Cada uno de los dispositivos se modelan como una variable de Bernoulli, cuyos valores son los relativos a no comprometer potencia (0 MW) o comprometer la potencia máxima del dispositivo ($P_{maxdisp}$). La probabilidad de compromiso se calculó a partir de la valoración de riesgo calculada en el Bloque B.
2. Modelados los dispositivos mediante las distribuciones, se pasa a calcular la PDF marginal del nodo aplicando la FFT. El resultado es la obtención de la PDF del nodo.

El procedimiento es posteriormente aplicado a cada uno de los nodos que conforman la red. El proceso se sintetiza en la Fig. 2

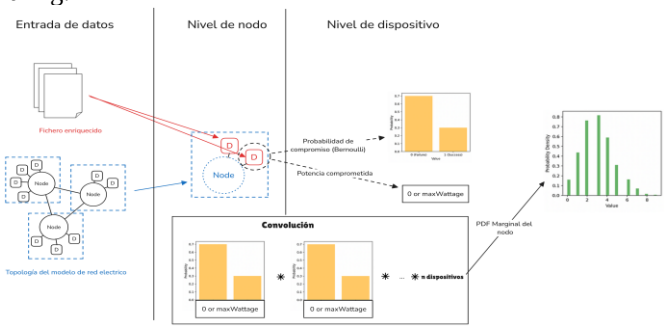

Fig. 2: Online - Esquemático del proceso de generación de la PDF marginal en tiempo real.

F. Online – Estimación del riesgo global a tiempo real

La estimación del riesgo global en la rama *online* se apoyará en lo ya realizado en su contraparte *offline*. Al haber obtenido las diferentes PDFs marginales para cada uno de los nodos, se propone es el siguiente proceso (véase Fig. 3):

- Por cada una de las PDFs marginales obtenidas en el flujo *online*, se utiliza la divergencia de Kullback-Leibler para compararlo con los 2 escenarios elaborados en la parte *offline*, seleccionando la más semejante. Este proceso se realiza para todos los nodos.
- Habiendo obtenido a que caso es más semejante por cada nodo, se obtienen todas las simulaciones realizadas para esa configuración, promediando los valores.
- La simulación promediada obtenida es la utilizada para poder identificar, dentro de los rangos de valores generados por los umbrales, a cuál pertenece.
- Conociendo el rango del valor al cual pertenece, se consigue el nivel de riesgo, ya que previamente, en la parte *offline*, ya se había realizado esa asociación.

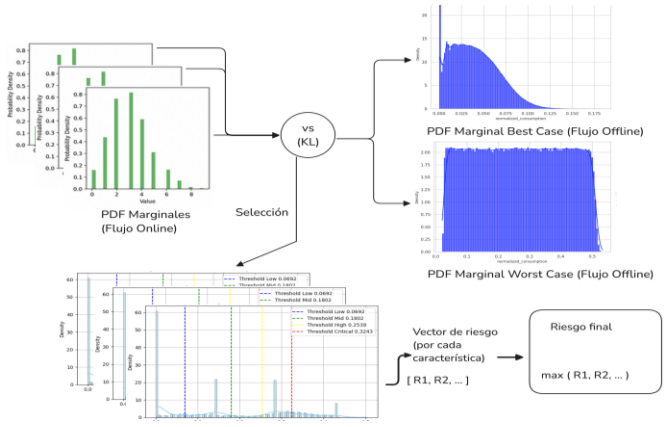

Fig. 3: Online – Esquemático del flujo de estimación riesgo global

III. RESULTADOS

Para evaluar el desempeño de la metodología propuesta, se analizaron los resultados de la estimación del riesgo global en las redes de estudio IEEE9 e IEEE39, considerando los distintos escenarios de ataque.

Inicialmente, se presentan los mapas de calor (Fig. 4 y Fig. 5) que ilustran la asignación de categorías de riesgo (eje X) en función de los diferentes casos (eje Y) para los modelos de thresholding aplicados en el flujo *offline*.

Las categorías de riesgo que se asignan son valores numéricos enteros positivos (empezando por 0). El conjunto de valores de los mapas de calor indica la cantidad de simulaciones realizadas para cada tipo de caso.

La Fig. 4 muestra, la estimación del riesgo que realizan los diferentes modelos para la red IEEE9. En estos mapas de calor se observa que:

- Los casos escenario *best-case* siempre son valorados con el nivel de riesgo más bajo. Esto permite indicar que el aporte de riesgo a la red al ser atacado por este tipo de caso es mínimo.
- Los casos escenario *mix-case* son siempre valorados de igual forma que su contraparte del escenario *worst-case*, en cualquier modelo. Debido a que el aporte en riesgo del *best-case* es mínimo, el aporte en riesgo en la red proviene casi exclusivamente de los nodos que se simularon bajo el escenario *worst-case*.
- Los casos escenario *worst-case* difieren en la estimación del riesgo en función del modelo empleado. El umbral de DBSCAN es más disperso, mientras que los umbrales de K-Means++ y GMM proporcionan una estimación más progresiva.

La Fig. 5 se centra exclusivamente en los escenarios de peor caso para la red IEEE39 debido a las similitudes observadas con los comportamientos del *best-case* y *mix-case* de IEEE9 (Fig. 4). Las observaciones de estos mapas de calor describen que todas las metodologías de umbrales basadas en agrupamiento generan una estimación progresiva y diagonal. Específicamente, el umbral de K-Means++ y el umbral de GMM tienden a la sobreestimación (valores por encima de la diagonal), mientras que el umbral de DBSCAN tiende a la subestimación (valores por debajo de la diagonal).

Con el objetivo de sintetizar los resultados obtenidos y poder escoger la modalidad que mejor permite calcular valores de umbrales, en la Tabla I se desglosan las propiedades observadas por cada una de ellas.

Durante todo el análisis comparativo (véase Fig. 4, Fig. 5, Tabla I) se observó que el algoritmo GMM demostró consistentemente una superior variabilidad intra-caso y dispersión inter-caso, adaptándose eficazmente a las distribuciones de datos reales.

A diferencia de otros métodos de agrupamiento, GMM ofrece transiciones suaves de umbrales entre los niveles de riesgo, lo que da lugar a una categorización más coherente y representativa de los escenarios de ataque MaDIoT, lo que llevó a su selección.

IV. CONCLUSIONES

Este artículo muestra que la metodología multicapa que se propone para la estimación de riesgo global en las redes de estudio IEEE9 y IEEE39 al ser atacadas por ataques MaDIoT es explicativa y consistente con un análisis clásico de riesgo.

Se puede apreciar que tanto la recopilación e inventariado de los dispositivos presentes en el Bloque A, como el análisis de vulnerabilidades y riesgo de dichos dispositivos en el Bloque B son propios de la literatura clásica del análisis de riesgo. Sin embargo, la metodología propuesta presenta novedades en el bloque C, al utilizar métodos probabilísticos y metodologías de *thresholding* para estimar niveles de riesgo. Estas metodologías, aun difiriendo significativamente respecto a metodologías más clásicas, sí que permiten la

misma interpretación con respecto a valores de riesgo provistos empíricamente.

No obstante, es necesario evaluar la metodología presentada con un mayor número de modelos de red diferentes, con el fin de ampliar su validación.

AGRADECIMIENTOS

Este trabajo fue desarrollado en el marco del Proyecto eFORT, proyecto financiado por el programa de Investigación e Innovación Horizonte Europa de la Unión Europea bajo el Grant Agreement No. 101075665.

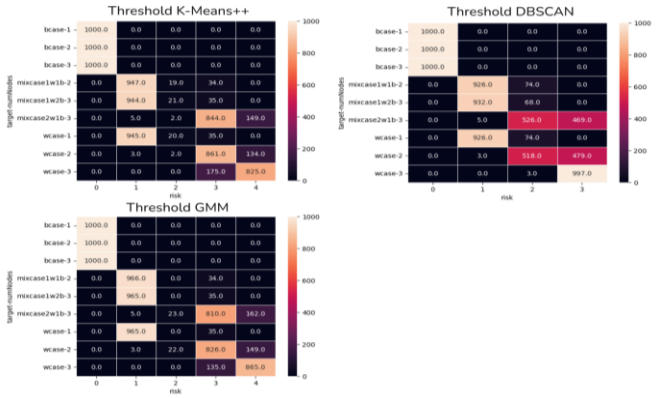

Fig. 4: Mapas de calor por cada modelo de *thresholding* en la red IEEE9 (*best-case*, *mix-case*, *worst-case*).

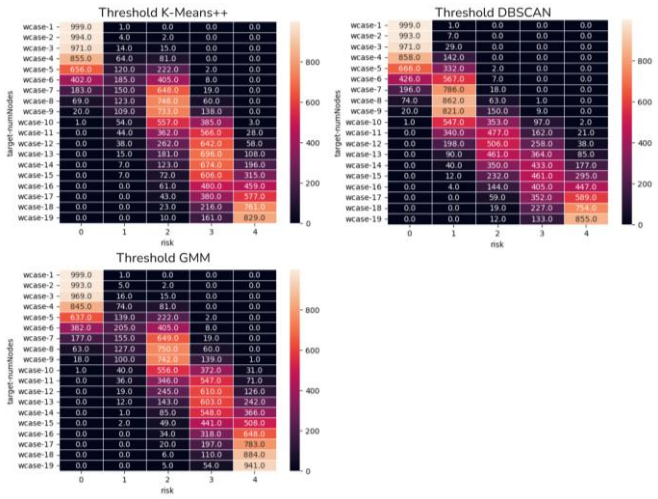

Fig. 5: Mapas de calor por cada modelo de *thresholding* en la red IEEE39 (*worst-case*).

Tabla I
SELECCIÓN DE MODELO DE THRESHOLDING

Modelo	Propiedades
Threshold K-Means++	Mejora en la variabilidad intracaso y dispersión intercaso, pero inferior a GMM. Generación de clústeres esféricos, sin adaptación a la forma real.
Threshold DBSCAN	Mejora en la variabilidad intracaso y dispersión intercaso en ciertas redes, pero inconsistente. Imposibilidad de ajuste en la cantidad de thresholds generados, ya que está basado en otros parámetros. Clasificación de ciertos valores como ruido
Threshold GMM	Variabilidad intracaso y dispersión mejor ajustada intercaso. Mejora en la transición suave intracaso. Permite adaptarse a la forma del clúster.

REFERENCIAS

[1] S. Soltan, P. Mittal, y H. V. Poor, «BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid», 2018.

[2] S. Maleki, S. Pan, S. Lakshminarayana, y C. Konstantinou, «Survey of Load-Altering Attacks Against Power Grids: Attack Impact, Detection and Mitigation», 29 de octubre de 2024.

[3] J. Ospina, X. Liu, C. Konstantinou, y Y. Dvorkin, «On the Feasibility of Load-Changing Attacks in Power Systems During the COVID-19 Pandemic», *IEEE Access*, vol. 9, pp. 2545-2563, 2021.

[4] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, y Z. Li, «Power System Risk Assessment in Cyber Attacks Considering the Role of Protection Systems», *IEEE Trans. Smart Grid*, pp. 1-1, 2016.

[5] N. Rodríguez-Pérez, J. Matanza Domingo, L. Sigrist, J. L. Rueda Torres, and G. López López. Confronting the Threat: Analysis of the Impact of MaDIoT Attacks in Two Power System Models. Energies, 16(23), 7732, 2023.

[6] H. Cam y P. Mouallem, «Mission assurance policy and risk management in cybersecurity», *Environ. Syst. Decis.*, vol. 33, n.º 4, pp. 500-507, dic. 2013.

[7] H. Cam, «Risk assessment by dynamic representation of vulnerability, exploitation, and impact», presentado en SPIE Defense + Security,p. 945809, may 2015.

[8] Q. Zhang, C. Zhou, N. Xiong, Y. Qin, X. Li, y S. Huang, «Multimodel-Based Incident Prediction and Risk Assessment in Dynamic Cybersecurity Protection for Industrial Control Systems», *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 46, n.º 10, pp. 1429-1444, oct. 2016.

[9] Q. Zhang, C. Zhou, Y.-C. Tian, N. Xiong, Y. Qin, y B. Hu, «A Fuzzy Probability Bayesian Network Approach for Dynamic Cybersecurity Risk Assessment in Industrial Control Systems», *IEEE Trans. Ind. Inform.*, vol. 14, n.º 6, pp. 2497-2506, jun. 2018.

[11] Q. Zhu, Y. Zhao, L. Fei, y C. Zhou, «A Dynamic Decision-Making Approach for Cyber-Risk Reduction in Critical Infrastructure», en *IEEE 8th Annual International Conference on CYBER Technology*, jul. 2018.

[12] J. K. Debnath y D. Xie, «CVSS-based Vulnerability and Risk Assessment for High Performance Computing Networks», en *2022 IEEE International Systems Conference (SysCon)*, abr. 2022, pp. 1-8.

[13] I. Kotenko y E. Doynikova, «Security metrics for risk assessment of distributed information systems», en *IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS)*, sep. 2013, pp. 646-650.

[14] K. Huang, C. Zhou, Y.-C. Tian, W. Tu, y Y. Peng, «Application of Bayesian network to data-driven cyber-security risk assessment in SCADA networks», en *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, pp. 1-6. nov. 2017,

[15] Y. Qin, Y. Peng, K. Huang, C. Zhou, y Y.-C. Tian, «Association Analysis-Based Cybersecurity Risk Assessment for Industrial Control Systems», *IEEE Syst. J.*, vol. 15, n.º 1, pp. 1423-1432, mar. 2021.

[16] S. Abraham y S. Nair, «A Novel Architecture for Predictive CyberSecurity Using Non-homogenous Markov Models», en *2015 IEEE Trustcom/BigDataSE/ISPA*, ago. 2015, pp. 774-781.

[17] Q. Hong *et al.*, «An information security risk assessment method based on conduct effect and dynamic threat», *8th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, nov. 2017, pp. 782-786.

[18] G. Gonzalez-Granadillo *et al.*, «Dynamic risk management response system to handle cyber threats», *Future Gener. Comput. Syst.*, vol. 83, pp. 535-552, jun. 2018.

[19] P. K. Vaddi, Y. Zhao, y C. Smidts, «Dynamic Probabilistic Risk Assessment for Cyber Security Risk Analysis in Nuclear Reactors.», 2022.

[20] «CPS Information Security Risk Evaluation Based on Blockchain and Big Data», *Teh. Vjesn. - Tech. Gaz.*, vol. 25, n.º 6, dic. 2018.

[21] Z. Wang, L. Chen, S. Song, P. X. Cong, y Q. Ruan, «Automatic cyber security risk assessment based on fuzzy fractional ordinary differential equations», *Alex. Eng. J.*, vol. 59, n.º 4, pp. 2725-2731, ago. 2020.

[22] K. Yan, X. Liu, Y. Lu, y F. Qin, «A Cyber-Physical Power System Risk Assessment Model Against Cyberattacks», *IEEE Syst. J.*, vol. 17, n.º 2, pp. 2018-2028, jun. 2023.

[23] G. Gonzalez-Granadillo *et al.*, «Automated Cyber and Privacy Risk Management Toolkit», *Sensors*, vol. 21, n.º 16, Art. n.º 16, ene. 2021.

[24] V. G. Fernández, N. Rodrígºuez Pérez, R. G. Miñarro, J. M. Domingo, R. P. Hielscher, y G. López López, «Dynamic risk assessment tool for customer IoT infrastructures for Smart Grids», en *2023 JNIC Cybersecurity Conference (JNIC)*, jun. 2023, pp. 1-4.