XVII Congreso Galego de Estatística e Investigación de Operacións
Ourense, 23 - 25 de outubro de 2025

Medición de incertidumbre en detección de anomalías

Celia Melendi Ortega[1], Marta Sestelo Pérez[2,3] y Pablo Cereijo García[1]

[1] Fundación Centro Tecnolóxico de Telecomunicacions de Galicia (Gradiant), 36214 Vigo, España
[2] Departamento de Estadística e I.O. (Universidade de Vigo) y Grupo SiDOR, 36310 Vigo, España
[3] Centro de Investigación y Tecnología de Galicia (CITMAga) 15782 Santiago de Compostela, Vigo

RESUMEN

La fiabilidad de los sistemas de detección de anomalías se ve limitada por la ausencia de mecanismos que cuantifiquen la incertidumbre en sus predicciones, lo que dificulta su aplicación en dominios críticos como la ciberseguridad. Este trabajo estudia distintas técnicas de medición de incertidumbre aplicadas a modelos no supervisados de detección de anomalías, específicamente a *Isolation Forest* y *Extended Isolation Forest*. Se analizan métodos de predicción conformal (*split* y *cross*-conformal) y *ExCeeD*. Además, se ha desarrollado una implementación propia basada en *bootstrap* para obtener estimaciones de probabilidad de que una observación este correctamente clasificada. Posteriormente, para la evaluación de las distintas técnicas se emplea un conjunto de datos de tráfico de red. Los resultados obtenidos muestran que es posible complementar la detección clásica con medidas de incertidumbre que proporcionan información estadística adicional, mejorando la interpretabilidad de los modelos y proporcionando, o bien garantías estadísticas sobre las detecciones realizadas, o una métrica adicional que permite priorizar las distintas alertas y mejorar la toma de decisiones frente a estas.

Palabras y frases clave: Medición de incertidumbre, anomalía, probabilidad, p valores, métodos conformal, confianza.

REFERENCIAS

Bates, S., Candès, E., Lei, L., Romano, Y., y Sesia, M. (2023). Testing for outliers with conformal p-values. The Annals of Statistics, 51(1). doi: 10.1214/22-AOS2244

Hennhöfer, O., y Preisach, C. (2024). Uncertainty quantification in anomaly detection with cross-conformal p-values.

Perini, L., Vercruyssen, V., y Davis, J. (2021). Quantifying the confidence of anomaly detectors in their example-wise predictions. En F. Hutter, K. Kersting, J. Lijffijt, y I. Valera (Eds.), *Machine learning and knowledge discovery in databases* (pp. 227–243). Cham: Springer International Publishing.