MÓDULO 6 - Proyecto Final

David López Pretel

11 de mayo de 2022

Índice

Índice de figuras

Índice de cuadros

Resumen

El objetivo de la detección de anomalías es identificar las observaciones que difieren significativamente de la mayoría de los datos. La detección de anomalías se aplica con frecuencia a las series temporales, que son datos con un componente temporal. Existen varias formas de abordar un problema de detección de anomalías para series temporales, sin embargo, hay muy pocas opciones para los problemas de detección de anomalías en series temporales multivariantes. Las técnicas con un mayor rendimiento en la tarea de detección de anomalías en series temporales son: Redes Neuronales Temporales (TNN) y Redes Neuronales Recurrentes (RNN).
`https://github.com/DLPretel/proyecto_final`

Palabras Clave— Detección de Anomalías, Series Temporales, Redes Neuronales

1. Introduccion

Para hacer un seguimiento de un sistema, se genera un conjunto de datos que refleja el comportamiento de dicho sistema. Cuando el sistema empieza a fallar por alguna razón, empiezan a aparecer anomalías en los datos. Por lo tanto, detectar estas anomalías en los datos permite saber si el sistema se enfrenta a un fallo [5, 1, 7]. La tarea de encontrar observaciones que difieren mucho del resto de los datos se conoce como detección de anomalías [5]. Las observaciones que comparten este comportamiento inusual suelen denominarse valores atípicos o anomalías. Hay una gran variedad de dominios en los que la detección de anomalías es útil, como la detección de intrusiones [13], las redes de sensores [14], la detección de fraudes con tarjetas de crédito [8], la atención sanitaria [6] o las anomalías industriales [3]. Por ejemplo, la detección de un comportamiento anómalo en un motor puede indicar que está próximo a fallar, por lo que detectar las anomalías antes de que se rompa puede reducir en gran medida los costes de reparación. La detección de anomalías es cada vez más importante debido a la relevancia de los beneficios que aporta y a la enorme variedad de dominios en los que puede aplicarse. Dado que las tareas de detección de anomalías suelen consistir en el seguimiento del comportamiento de un sistema a lo largo del tiempo, los datos rara vez son estáticos. El escenario más común es enfrentarse a una componente temporal en los datos.

Las series temporales son datos que tienen una componente temporal, es decir, cada observación no es independiente, sino que está relacionada en el tiempo. Las series temporales pueden clasificarse en univariantes, que tienen una sola característica, y multivariantes, que tienen más de una característica. La mayoría de las propuestas de series temporales se centran en las univariantes, por lo que no hay muchas alternativas en los problemas multivariantes. Las series temporales mostrarán valores diferentes en distintos periodos de tiempo sin que ello indique necesariamente una anomalía. Por ejemplo, un motor puede tener una temperatura más alta de lo normal en un instante de tiempo, pero ese sobrecalentamiento puede deberse simplemente a una mayor carga de trabajo y no a un fallo. Aprender el comportamiento de una serie temporal puede

servir para analizar datos futuros y así anticiparse a un fallo y prevenir posibles daños [21, 18]. Dentro de una serie temporal, una anomalía suele estar determinada por varios valores anómalos consecutivos en el tiempo [4], lo que supone un gran inconveniente para los problemas tradicionales de detección de anomalías, ya que tratan las anomalías sin tener en cuenta el componente temporal [20].

Teniendo en cuenta las características de los problemas de detección de anomalías descritas anteriormente, es conveniente hacer uso de un algoritmo que tenga en cuenta la componente temporal en los problemas de detección de anomalías en series temporales. Al enfrentarse a series temporales multivariantes, el estado del arte actual está poblado por redes neuronales recurrentes como las LSTMs y las GRUs [2]. Un algoritmo reciente y de buen rendimiento son las redes convolucionales temporales (TCN) [2, 15].

2. Estado del arte

2.1. Detección de anomalías

Una anomalía es una observación que no sigue el mismo patrón que el resto de los datos. La figura 1 muestra una representación gráfica de las anomalías en un conjunto de datos bidimensional. Los clusters C1 y C2 están compuestos por observaciones normales, ya que prácticamente todos los puntos pertenecen a estas dos regiones. El cluster C3 contiene muy pocas observaciones ya que es un cluster anómalo. Las observaciones O1, O2 están completamente aisladas y, por tanto, son instancias anómalas [5].

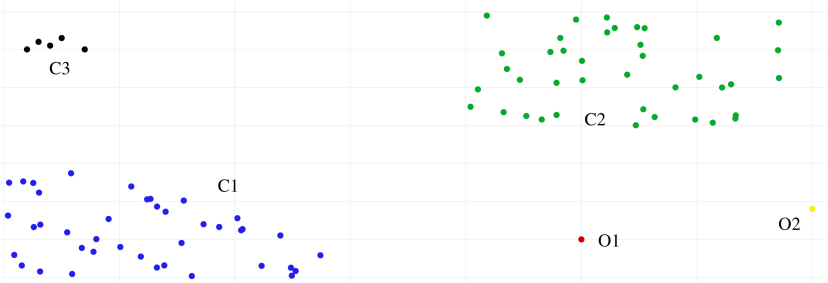

Figura 1: Ilustración de tipos de anomalías en un entorno de dos dimensiones

Podemos encontrar tres tipos diferentes de instancias anómalas [11]:

- Anomalía puntual: Es el escenario más frecuente en la detección de anomalías. Las instancias anómalas están completamente aisladas del resto. En la Figura 1, O1 y O2 son anomalías puntuales.
- Anomalía colectiva: La anomalía es una mezcla de varias instancias anómalas. Por ejemplo, la detección de un robo de tarjeta de crédito puede implicar la detección de varios extractos de cuentas bancarias.

- Anomalía contextual: Una instancia que no es anómala puede serlo dentro de un contexto determinado. Por ejemplo, si medimos la temperatura de un motor en un rango de 50 a 120 grados. Una temperatura de 80 grados parece completamente normal, pero si ese valor se da cuando el motor no tiene carga de trabajo, la temperatura estimada debería ser menor.

Las anomalías están relacionadas con el ruido, pero no hay que confundir ambos conceptos. El ruido tiene el mismo comportamiento descrito en la Figura 1, pero, el ruido no tiene interés para el analista de datos mientras que las anomalías sí lo tienen. El ruido se produce por una alteración de los datos, por lo que no refleja la distribución original de los mismos. Además, el ruido perjudica la calidad de los datos y esas observaciones deben ser fijadas o eliminadas [16, 9, 10]. Las anomalías son información valiosa que debe ser detectada, extraída y analizada.

La detección de anomalías se utiliza en una gran variedad de dominios, como las redes de sensores [14], la detección de intrusiones [13], las anomalías industriales [3], la detección de fraudes con tarjetas de crédito [8], la atención sanitaria [6], y mucho más [11]. El gran número de dominios que involucran el problema de la detección de anomalías, y el creciente número de sensores en todos los campos está haciendo que la detección de anomalías gane en popularidad.

En cuanto a la salida de un algoritmo de detección de anomalías, puede ser de dos tipos diferentes [5]:

- Etiquetas: El valor de retorno es una etiqueta binaria para cada instancia que indica qué instancias son normales y cuáles son anomalías.

- Scores: El valor de retorno es una puntuación de anomalía para cada instancia. Dicha puntuación indica la probabilidad de que una instancia sea anómala. También hay que estudiar qué puntuaciones son anómalas.

Como se ha mencionado anteriormente, nos centramos en la detección de anomalías en las series temporales. Una serie temporal es una colección de datos que sigue un orden cronológico. Algunas de sus características son: gran tamaño, alta dimensionalidad y actualización continua. Las series temporales han adquirido una gran importancia, ya que se utilizan en muchos ámbitos, como los datos diarios de temperatura, los datos semanales de ventas, las mediciones de los sensores de los motores u otras máquinas, etc.

Hay una gran variedad de aplicaciones en el ámbito del problema de la detección de anomalías. La detección de fraudes consiste en encontrar movimientos inusuales en aplicaciones comerciales como bancos, compañías telefónicas, tarjetas de crédito, etc [8]. La detección de intrusiones se refiere a la detección de actividades anómalas en una red informática [13]. Debido a la gran cantidad de flujo de información, puede producirse un elevado número de falsas alarmas. Esos movimientos inusuales están relacionados con intentos de robo de identidad o de una persona. Además, la detección de anomalías puede aplicarse en el mundo de la industria, detectando algunos daños en las estructuras, errores de

instrumentación de los sensores de los motores o comportamientos inesperados en los motores de una cadena de montaje [3].

Otras aplicaciones de interés son la detección de anomalías en datos de texto, la detección de anomalías en redes de sensores [14] o el procesamiento de imágenes [17].

2.2. Evaluación de los problemas de detección de anomalías

Para analizar el rendimiento de un algoritmo de detección de anomalías, se suelen utilizar cuatro métricas, que se representan en la matriz de confusión que se muestra en la Tabla 1. Tanto los verdaderos negativos como los verdaderos positivos son los valores más importantes y considerados, representan que el modelo está acertando en la predicción. El problema surge cuando el número de falsos positivos o falsos negativos es elevado. Hay dos medidas principales calculadas a partir de la matriz de confusión, la sensibilidad 1 que indica la capacidad de etiquetar como positivos los verdaderos positivos, y la especificidad 2 que indica la capacidad de etiquetar como negativos los verdaderos negativos.

$$\frac{TP}{TP + FN} \tag{1}$$

$$\frac{TN}{TN + FP} \tag{2}$$

Sin embargo, existe un equilibrio entre ambas medidas, ya que el aumento de una de ellas implica la disminución de la otra, por lo que encontrar el mejor ajuste posible es una tarea difícil y dependerá del problema a tratar qué medida tendrá prioridad.

Existe otro equilibrio entre TPs y la tasa de falsos positivos 3.

$$FPR = \frac{FP}{FP + TP} \tag{3}$$

El aumento de TPs suele dar lugar a un mayor FPR porque se da más importancia a las observaciones positivas y, por tanto, aunque se etiqueten correctamente más observaciones positivas, las observaciones negativas también se etiquetarán como positivas. Una característica distintiva de los problemas de detección de anomalías es que el número de observaciones normales es mucho mayor que el número de observaciones anómalas, por lo que intentar ajustar el modelo para centrarse en las observaciones anómalas da lugar a un incremento del número de falsos positivos, generando así alarmas innecesarias. Además, es posible que una observación sea etiquetada como positiva cuando no lo es en función de su contexto (dando lugar a un falso positivo), lo que es común cuando se trata de un problema de series temporales [12, 19].

		Predicción	
		Negativos	Positivos
Valor Real	Negativos	Verdaderos Negativos (TN)	Falsos Positivos (FP)
	Positivos	Falsos Negativos (FN)	Verdaderos Positivos (TP)

Cuadro 1: Matriz de confusión

Referencias

[1] Charu C. Aggarwal. *Outlier Analysis*. Springer Publishing Company, Incorporated, 2nd edition, 2016.

[2] Shaojie Bai, J Zico Kolter, and Vladlen Koltun. An empirical evaluation of generic convolutional and recurrent networks for sequence modeling. *arXiv preprint arXiv:1803.01271*, 2018.

[3] Barış Bayram, Taha Berkay Duman, and Gökhan Ince. Real time detection of acoustic anomalies in industrial processes using sequential autoencoders. *Expert Systems*, 38(1):e12564, 2021.

[4] Jacinto Carrasco, David López, Ignacio Aguilera-Martos, Diego García-Gil, Irina Markova, Marta García-Barzana, Manuel Arias-Rodil, Julián Luengo, and Francisco Herrera. Anomaly detection in predictive maintenance: A new evaluation framework for temporal unsupervised anomaly detection algorithms. *Neurocomputing*, 462:440–452, 2021.

[5] Varun Chandola, Arindam Banerjee, and Vipin Kumar. Anomaly detection: A survey. *ACM computing surveys (CSUR)*, 41(3):1–58, 2009.

[6] Rajendra Kumar Dwivedi, Rakesh Kumar, and Rajkumar Buyya. A novel machine learning-based approach for outlier detection in smart healthcare sensor clouds. *International Journal of Healthcare Information Systems and Informatics (IJHISI)*, 16(4):1–26, 2021.

[7] L. Erhan, M. Ndubuaku, M. Di Mauro, W. Song, M. Chen, G. Fortino, O. Bagdasar, and A. Liotta. Smart anomaly detection in sensor systems: A multi-perspective review. *Information Fusion*, 67:64–79, 2021.

[8] Javad Forough and Saeedeh Momtazi. Ensemble of deep sequential models for credit card fraud detection. *Applied Soft Computing*, 99:106883, 2021.

[9] Diego García-Gil, Julián Luengo, Salvador García, and Francisco Herrera. Enabling Smart Data: Noise filtering in Big Data classification. *Information Sciences*, 479:135 – 152, 2019.

[10] Diego García-Gil, Francisco Luque-Sánchez, Julián Luengo, Salvador García, and Francisco Herrera. From Big to Smart Data: Iterative ensemble filter for noise filtering in Big Data classification. *International Journal of Intelligent Systems*, 34(12):3260–3274, 2019.

[11] Markus Goldstein and Seiichi Uchida. A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. *PloS one*, 11(4):e0152173, 2016.

[12] Kyle Hundman, Valentino Constantinou, Christopher Laporte, Ian Colwell, and Tom Soderstrom. Detecting spacecraft anomalies using lstms and nonparametric dynamic thresholding. In *Proceedings of the 24th ACM SIGKDD international conference on knowledge discovery & data mining*, pages 387–395, 2018.

[13] Ilhan Firat Kilincer, Fatih Ertam, and Abdulkadir Sengur. Machine learning methods for cyber security intrusion detection: Datasets and comparative study. *Computer Networks*, 188:107840, 2021.

[14] Ivan Kraljevski, Frank Duckhorn, Constanze Tschöpe, and Matthias Wolff. Machine learning for anomaly assessment in sensor networks for ndt in aerospace. *IEEE Sensors Journal*, 21(9):11000–11008, 2021.

[15] Colin Lea, Rene Vidal, Austin Reiter, and Gregory D Hager. Temporal convolutional networks: A unified approach to action segmentation. In *European Conference on Computer Vision*, pages 47–54. Springer, 2016.

[16] Julián Luengo, Diego García-Gil, Sergio Ramírez-Gallego, Salvador García, and Francisco Herrera. *Big Data Preprocessing - Enabling Smart Data*. Springer, 2020.

[17] Guansong Pang, Chunhua Shen, Longbing Cao, and Anton Van Den Hengel. Deep learning for anomaly detection: A review. *ACM Comput. Surv.*, 54(2), 2021.

[18] Francesco Piccialli, Fabio Giampaolo, Edoardo Prezioso, David Camacho, and Giovanni Acampora. Artificial intelligence and healthcare: Forecasting of medical bookings through multi-source time-series fusion. *Information Fusion*, 74:1–16, 2021.

[19] Siddharth Sridhar and Manimaran Govindarasu. Model-based attack detection and mitigation for automatic generation control. *IEEE Transactions on Smart Grid*, 5(2):580–591, 2014.

[20] Nesime Tatbul, Tae Jun Lee, Stanley B. Zdonik, Mejbah Alam, and Justin Emile Gottschlich. Precision and recall for time series. In *Advances in Neural Information Processing Systems*, volume 31. Curran Associates, Inc., 2018.

[21] G Peter Zhang. Time series forecasting using a hybrid arima and neural network model. *Neurocomputing*, 50:159–175, 2003.