Lección 1. El problema de la detección de anomalías

UCO ONLINE

La detección de anomalías

Definición del problema de detección de anomalías

La detección de anomalías es un área donde se están realizado muchos avances en las últimas décadas, en parte gracias al avance de la minería de datos y el aprendizaje automático. Así como el gran crecimiento de las tecnologías informáticas que está permitiendo que puedan abordarse problemas que antes eran inimaginables.

Las anomalías surgen en numerosos campos de estudio, incluyendo medicina, finanzas, ciberseguridad, sociología y astronomía. En algunas áreas, las anomalías indican un comportamiento problemático, por ejemplo, transacciones inusuales con una tarjeta de crédito. En algunas otras áreas, pueden ser indicadores de resultados positivos, por ejemplo, ventas inesperadamente más altas dentro de una organización minorista. En otros casos, pueden indicar fenómenos mal entendidos u objetos o procesos desconocidos, desencadenando la exploración de nuevas ideas que enriquecen el campo de la investigación científica. Todas las áreas comparten que son eventos que son relevantes estudiar.

A veces una metodología de detección de anomalías exitosa en un dominio también puede tener éxito en un área de estudio completamente nueva, y el conocimiento del primero puede permitir avances más rápidos en el segundo. Es por tanto importante tener una comprensión firme de los principios y algoritmos de detección de anomalías y comprender el alcance de su aplicabilidad.

1. Definición de anomalía

Según la Real Academia Española (RAE), encontramos las siguientes dos acepciones relacionadas con los temas que se abordan en este curso:

> *1. f. Desviación o discrepancia de una regla o de un uso.*
> *2. f. Defecto de forma o de funcionamiento.*

En línea con estas definiciones, nosotros vamos a definir la detección de anomalías [2] como el problema de encontrar eventos u observaciones en los datos que no se ajustan al comportamiento esperado (figura 1). Estos eventos u observaciones diferentes, a menudo se denominan anomalías, valores atípicos, observaciones discordantes, excepciones o peculiaridades en diferentes dominios de aplicación. No obstante, los términos más ampliamente utilizados son anomalías y valores atípicos (outliers), que son los son dos términos más ampliamente utilizados en el contexto de la detección de anomalías [1,3].

Figura 1. Una posible anomalía

La relevancia que tiene la detección de anomalías radica en que normalmente se traducen en información significativa (y a menudo crítica) en una amplia variedad de dominios de aplicación. Por ejemplo, una observación anormal en el tráfico de una red informática podría significar una intrusión en la red que está enviando datos confidenciales a un destino no autorizado. Una anomalía en una imagen de una resonancia puede indicar la presencia de tumores malignos. Una anomalía en las transacciones de compra de una tarjeta de crédito podría indicar un fraude o finalmente, una anomalía en las señales del sensor de una nave espacial podría significar un fallo en algún componente de la nave [2]. Como se puede ver, son eventos que no ocurren habitualmente, pero cuando ocurren pueden tener graves consecuencias en el dominio de aplicación.

La detección de valores atípicos o anomalías, debido a su gran relevancia, es un área que lleva mucho tiempo estudiándose, así encontramos estudios que se remontan al siglo XIV. En sus inicios, la mayoría de los estudios eran realizados por la comunidad estadística. Con el tiempo, se han ido desarrollando nuevas métricas y actualmente, debido al avance que está teniendo la ciencia de datos y la inteligencia artificial, los métodos aprendizaje automático y la minería de datos son las técnicas más ampliamente utilizadas.

En la figura 2 se muestra un ejemplo de anomalías en un conjunto de datos bidimensionales simple. Los datos tienen dos regiones normales, C1 y C2, ya que la mayoría de las observaciones se encuentran en estas dos regiones. Los puntos que están muy alejados de estas regiones, por ejemplo, puntos A1 y A3, se pueden considerar anomalías.

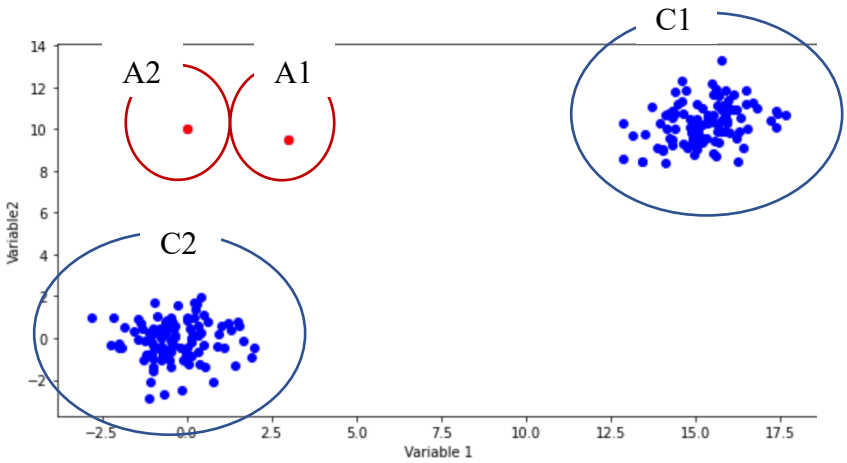


Figura 2. Ejemplo de anomalías

1.1 Anomalías y valores atípicos

En la definición anterior se han hablado de dos conceptos con los que habitualmente se referencian a las anomalías "valores atípicos" y "anomalías", cuando estamos trabajando en este campo, ambos términos son muchas veces intercambiados y es interesante pararnos un momento a comentar los posibles matices que pueden tener [3].

Las anomalías significan irregularidades en el dominio de aplicación donde ocurren. En la mayoría de los casos, la detección de anomalías está destinada a comprender eventos raros que no se habían producido antes. Un método que permite realizar esta tarea puede crear un modelo de los datos normales y aplicar las futuras observaciones con el modelo, si no coincide, se trata de una anomalías. Sin embargo, como veremos en este tema, la definición de normalidad difiere en función del dominio del problema y del tiempo, por lo que el problema de la detección de anomalías resulta ser un proceso complicado. Otro enfoque genérico consiste en buscar valores atípicos en un conjunto de datos que nos permita identificar eventos raros en nuestros datos. En este contexto, gran parte de la investigación relacionada con la detección de valores atípicos ha evolucionado en el contexto de la detección de anomalías.

La detección de valores atípicos tiene varias implicaciones útiles en varias aplicaciones de la vida real. La detección exitosa de valores atípicos ayuda a una mejor determinación de los escenarios anómalos donde el sistema subyacente puede tender a funcionar mal o puede exhibir algún comportamiento inesperado. Por lo tanto, la detección de valores atípicos en los datos conduce a la identificación de anomalías en sistemas reales. Puede haber diferencias sutiles entre un valor atípico y una anomalía en la forma en que se perciben en una aplicación concreta. Sin embargo, desde el punto de vista de la minería de datos y tal y como la vamos a trabajar en este curso, estos dos tipos de definiciones muestran características similares en términos de su desviación de la normalidad y no haremos una distinción específica entre estos dos tipos de objetos.

2. Retos en la detección de anomalías

La detección de anomalía no es un problema trivial. Partiendo de la definición anterior, una anomalía es un patrón u observación que no se ajusta al comportamiento normal que se esperaba. De acuerdo con esta definición, un enfoque directo que nos permitiría abordarla sería definir la región que represente el comportamiento normal y definir como anómalo cualquier observación en los datos que no pertenezca a la región considerada normal. No obstante, distintos factores hacen que este problema sea muy complejo de resolver y que dependa mucho del dominio de aplicación [2]:

- Definir una región de los datos que se considere normal y que abarque todos los comportamientos normales posibles es muy complejo. Además, el límite entre el comportamiento normal y anómalo a menudo no se conoce y no está totalmente definido. Así, una observación anómala que se encuentra cerca del límite podría ser realmente normal, y viceversa.

- Cuando las anomalías son el resultado de acciones malintencionadas, los atacantes a menudo se adaptan para hacer que las observaciones anómalas parezcan normales, lo que hace que la tarea de definir el comportamiento normal sea más difícil.

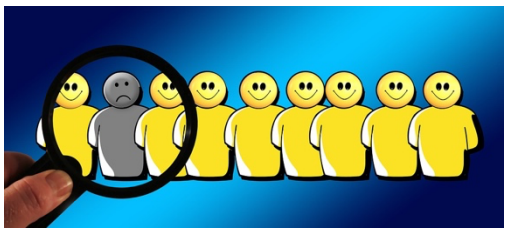
- En muchos dominios, el comportamiento normal va evolucionando y una región de los datos que se considere normal ahora, podría no ser muy representativa en el futuro (figura 3).

- La noción exacta de una anomalía es diferente según el dominio de aplicación. Por ejemplo, en el dominio médico una pequeña desviación de lo normal (por ejemplo, fluctuaciones en la temperatura corporal) podría ser una anomalía, mientras que una desviación similar en los valores de la bolsa (por ejemplo, las fluctuaciones en el valor de una acción) podría considerarse como normal. Por lo tanto, aplicar una técnica desarrollada en un dominio y aplicarla a otro, no es algo directo.

- Por definición, lo que se quiere detectar es un evento u observación que no es frecuente, con lo que se suele tener poca información sobre las anomalías y muchas veces ni se conoce. Así, la disponibilidad de datos etiquetados para entrenamiento/validación de modelos usados por las técnicas de detección anomalías suele ser un problema importante.

- A menudo, los datos contienen ruido (se trata solamente de datos que no se han almacenado correctamente), pero tienden a ser similares a las anomalías reales y por lo tanto es difícil de distinguir y es necesario valorarlas para poder tomar una decisión acerca de ellas.

a) Lo anómalo es estar feliz.



b) Lo anómalo es estar triste.

Figura 3. Cambio de lo que se considera anómalo

Debido a todas estas características, se puede comprender que el problema de detección de anomalías no es nada fácil de resolver. De hecho, la mayoría de las técnicas de detección de anomalías existentes resuelven un problema específico que viene definido por la naturaleza de los datos, la disponibilidad de datos etiquetados (se tienen identificados casos anómalos y casos normales) y el tipo de anomalías a ser detectado. Actualmente, la detección de anomalías comparte conceptos de diversas disciplinas como la estadística, el aprendizaje automático, la minería de datos y la teoría espectral.

1.3 Tipos de anomalías

Una anomalía dentro del campo de la Ciencia de Datos puede clasificarse ampliamente en tres categorías [2]:

- Anomalía puntual: corresponden a anomalías de datos individuales que pueden considerarse anómalos con respecto al resto de datos. Es el tipo de anomalía con el que más se ha trabajado, en estos casos un evento/observación concreto puede considerarse como anómalo con respecto al resto de datos.

  En la Figura 2, los puntos A1 y A2 se encuentran fuera del límite de las regiones normales y, por lo tanto, son anomalías puntuales.

  Para relacionarlo con una aplicación real, se puede considerar el problema de la detección de fraudes con tarjetas de crédito. Cada punto se correspondería con una transacción de la tarjeta de crédito de una persona. Por simplicidad, si cada dato se define solamente usando como característica la cantidad gastada. La transacción donde el total gastado es muy alto en comparación con el resto de los gastos que se consideran normales para esa persona, se podría considerar una anomalía puntual.

- Anomalía contextual: corresponde a anomalías debido al contexto de la observación. De este modo, un evento es anómalo en un contexto específico (pero no considerado de forma individual). La noción de contexto es inducida por cierta estructura del conjunto de datos y debe ser una especificación del problema. Para detectar este tipo de anomalías, cada evento debe tener definidos dos atributos:

  - Atributo contextual: los atributos contextuales se utilizan para determinar el contexto (o vecindario) para ese evento. Por ejemplo, en eventos representados por conjuntos de datos espaciales, la longitud y la latitud de una ubicación son los atributos contextuales. En series temporales, el tiempo sería un atributo contextual que determina la posición de un evento en toda la secuencia.

  - Atributo de comportamiento: los atributos de comportamiento definen las características no contextuales del evento. Por ejemplo, en eventos representados por conjunto de datos espaciales que describen la lluvia promedio de todo el mundo, los litros de lluvia que han caído en un determinado lugar sería un atributo de comportamiento.

El comportamiento anómalo se determina utilizando los valores de los atributos de comportamiento dentro de un contexto específico. Una observación puede ser una anomalía contextual en un determinado contexto, pero un evento idéntico (en términos de atributos de comportamiento) podría considerarse normal en un contexto diferente. La correcta identificación de los atributos contextuales y de comportamiento es crucial en los métodos de detección de anomalías que trabajan con anomalías contextuales. Estas anomalías se exploran con mayor frecuencia en conjuntos de datos de series temporales y espaciales.

La Figura 3 (obtenida de [2]) muestra un ejemplo de una serie temporal que muestra la temperatura mensual de una zona en los últimos años. Una temperatura de dos grados podría ser normal durante el invierno (en el momento t1) en ese lugar, pero el mismo valor durante el verano (en el momento t2) sería una anomalía.

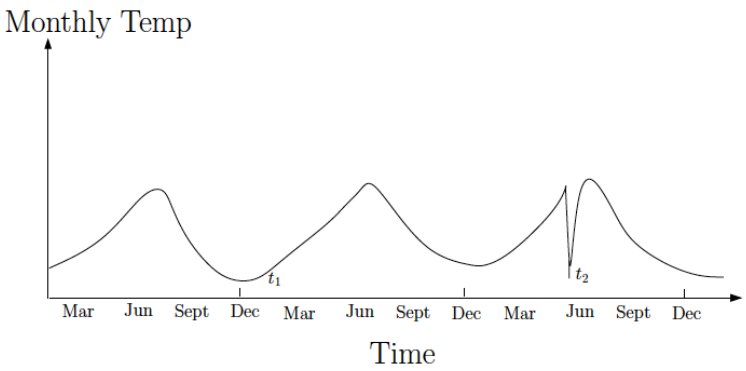


Figura 3. Anomalía contextual en t2 [2].

Un ejemplo similar se puede encontrar en el dominio de detección de fraudes con tarjetas de crédito. El atributo contextual en el dominio de la tarjeta de crédito puede ser el momento de la compra. Supongamos que un individuo generalmente tiene una factura de compras semanal de 100 euros, excepto durante la semana de Navidad que llega a 1000 euros. Una nueva compra de 1000 euros en una semana en julio será considerada una anomalía contextual, ya que no se ajusta al comportamiento normal del individuo en el contexto del tiempo (aunque la misma cantidad gastada durante la semana de Navidad se considerará normal).

Para poder aplicar métodos que detecten este tipo de anomalías es fundamental tener disponibilidad de atributos contextuales. En algunos casos definir un contexto es sencillo y, por lo tanto, aplicar una técnica de detección de anomalías contextuales tiene sentido. En los casos en lo que no se puede definir ese contexto, no podrán utilizarse.

- Anomalía colectiva: un conjunto de eventos anómalos determina que existe una anomalía. Los datos individuales en una anomalía colectiva pueden no ser anomalías por sí mismos, pero su aparición conjunta sí.

  La Figura 4 (obtenida de [2]) muestra la salida de un electrocardiograma humano. La región resaltada denota una anomalía porque existe el mismo valor bajo para un tiempo anormalmente largo (correspondiente a una contracción auricular prematura). Ese bajo valor por sí mismo, en un instante solamente, no es una anomalía.

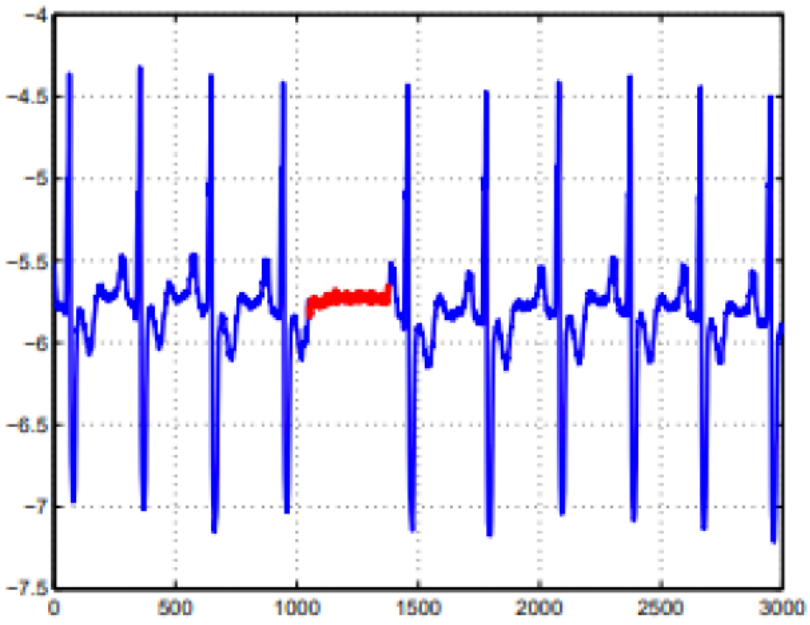


Figura 4. Salida de electrocardiograma humano con anomalía colectiva [2]

Cabe señalar que, si bien las anomalías puntuales pueden ocurrir en cualquier conjunto de datos, las anomalías colectivas solo pueden ocurrir en conjuntos de datos en los que los eventos que se estudian están relacionados. En contraste, la ocurrencia de anomalías contextuales depende de la disponibilidad de atributos del contexto en los datos. Una anomalía puntual o una anomalía colectiva también puede ser una anomalía contextual si se analiza con respecto a un contexto. Por lo tanto, una anomalía puntual o una anomalía colectiva se puede transformar en un problema de detección de anomalía contextual si se incorpora información de contexto.

Referencias

[1] C.C. Aggarwal. “Outlier analysis second edition”. Springer International Publishing, 2º edicion, 465 páginas. 2016.
[2] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3), 1-58.
[3] K. G. Mehrotra, C. K. Mohan, H. Huang. “Anomaly detection principles and algorithms”. Springer International Publishing, 1º edición, 217 páginas. 2017.