Detección de anomalías

Diplomatura en Ciencia de Datos,
Aprendizaje Automático y sus Aplicaciones
FaMAF-UNC
agosto 2018

Basado en filminas de Arindam Banerjee, Varun Chandola, Vipin Kumar, Jaideep Srivastava y Aleksandar Lazarevic

https://www.siam.org/meetings/sdm08/TS2.ppt

Qué es una anomalía

Un patrón en los datos que no conforma al comportamiento esperado

- outliers, excepciones, peculiaridades, sorpresa, etc.

Se traducen en entidades de la vida real muy importantes

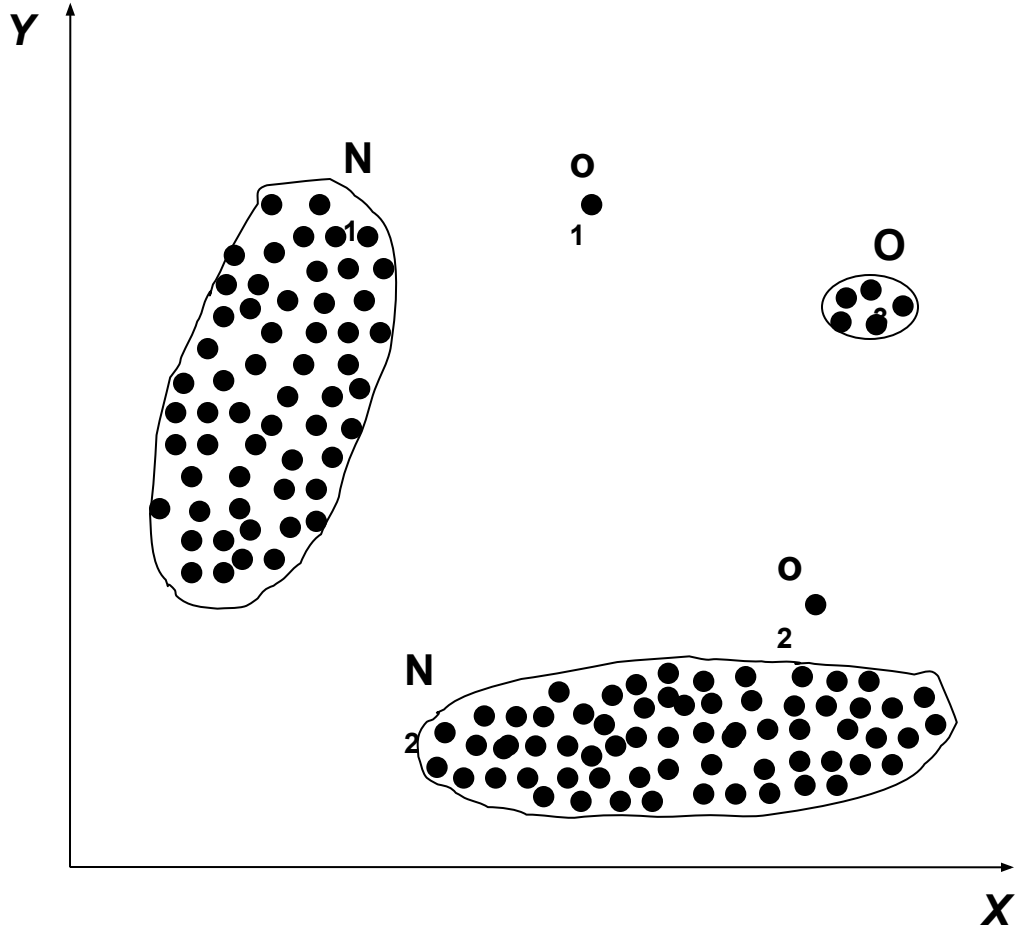
- Intrusiones cibernéticas
- Fraude en tarjeta de crédito

Ejemplo

N1 y N2 son regiones de comportamiento normal

o1 y o2 son anomalías

Los puntos de la región O3 son anomalías



Problemas relacionados

Rare Class Mining

Chance discovery

Novelty Detection

Exception Mining

Noise Removal

Black Swan

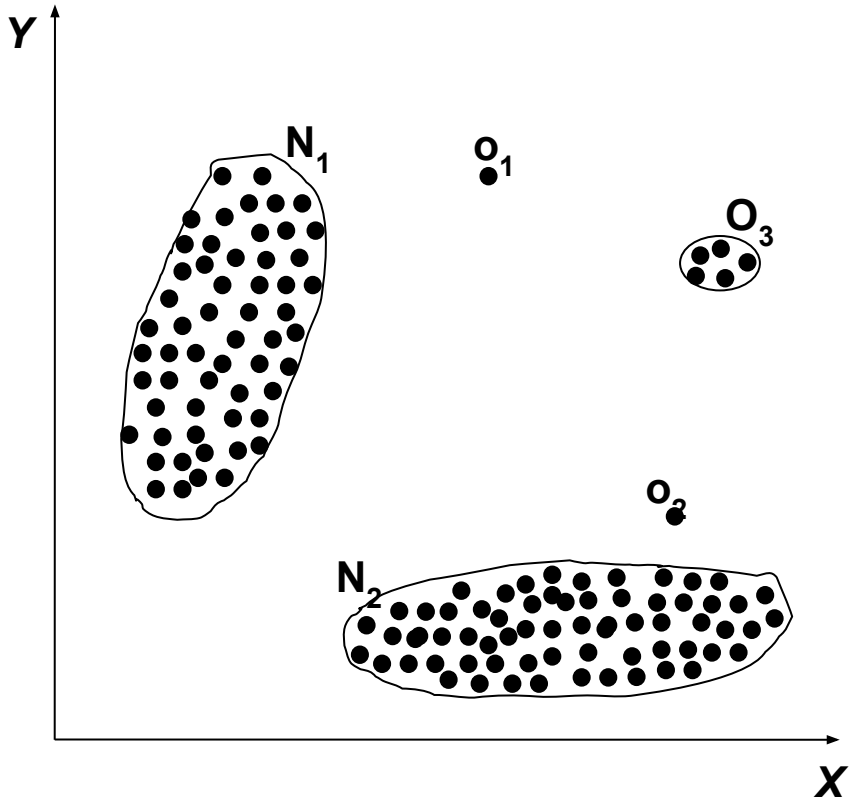
Retos clave

- Definir una región normal representativa
- La frontera entre comportamiento normal y anómalo no es precisa
- El comportamiento normal cambia a través del tiempo
- La idea de outlier depende del dominio
- Disponibilidad de datos
- Adversarios maliciosos
- Ruido

Tipos de anomalía

- Puntuales
- Contextuales
- Colectivas

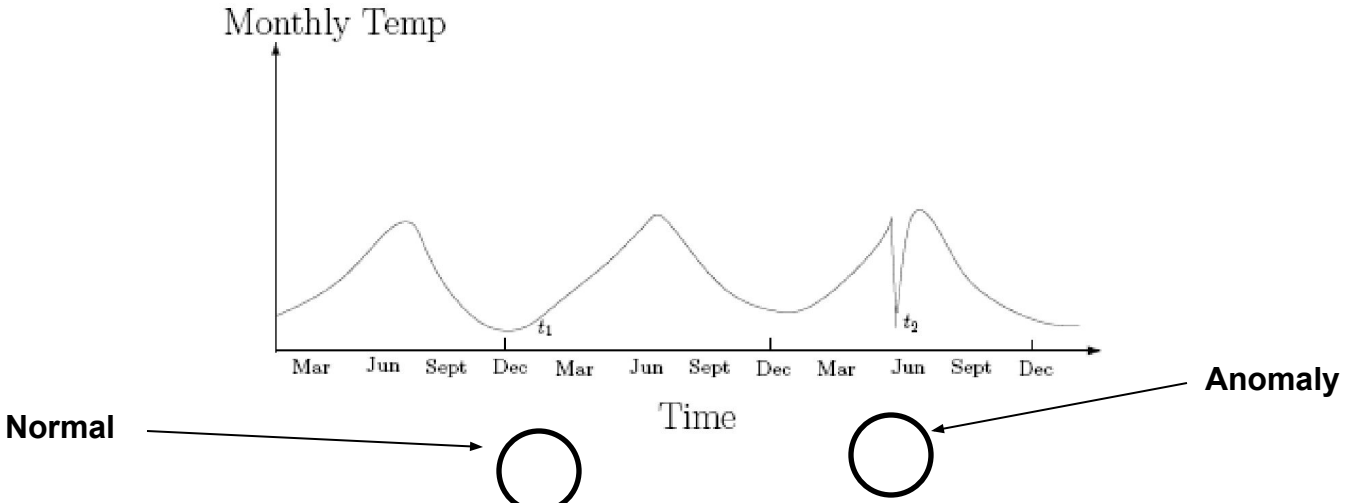
Anomalías puntuales



Anomalías contextuales

Una instancia es anómala en un contexto

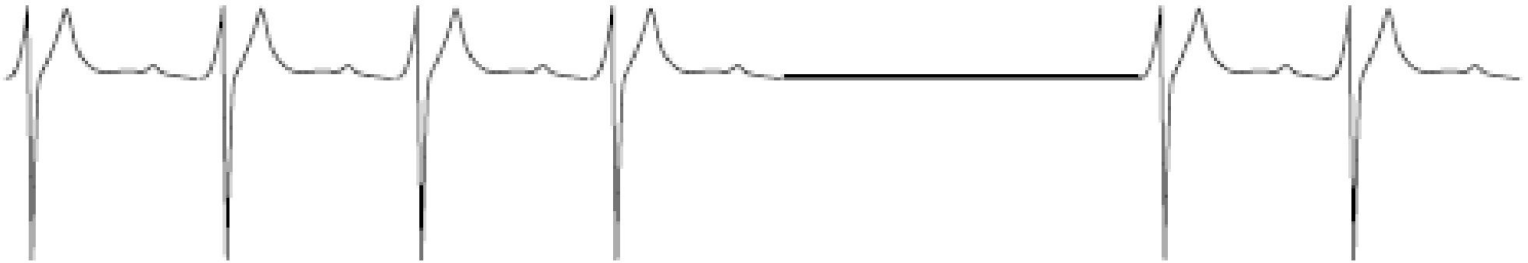
- Requiere definir “contexto”
- *conditional anomalies*



Anomalías colectivas

Una colección de instancias que es anómala

- Las instancias individuales no son anómalas por sí mismas
- Requiere definir cuándo las instancias están relacionadas
- Datos secuenciales, espaciales, en grafo



Evaluación

Se asigna a cada instancia una etiqueta “normal” o “anormal”, o un nivel de normalidad

- Accuracy dá valores muy altos (la clase mayoritaria es muy grande)
- Cobertura (proporción de detección) - proporción entre el número de anomalías detectadas y el número de anomalías existentes
- Proporción de falsos positivos
- AUC: Área bajo la curva de ROC, un balance entre la cobertura y la proporción de falsos positivos

Aplicaciones

Network intrusion detection

Insurance / Credit card fraud detection

Healthcare Informatics / Medical diagnostics

Industrial Damage Detection

Image Processing / Video surveillance

Novel Topic Detection in Text Mining

...

Técnicas basadas en clasificación

Se entrena un clasificador para eventos normales y raros, basándose en datos etiquetados

- Se pueden generar los eventos raros artificialmente, como en PU learning
- El modelo tiene que tratar adecuadamente clases desbalanceadas

Dificultades:

- Etiquetas para la clase normal y anómala
- No se detectan anomalías desconocidas o emergentes

Algunos trucos para usar clasificación en detección de anomalías

- Over-sampling de la clase minoritaria hasta balancear las clases ➜ No aumenta la información pero aumenta el coste de error de clasificación
- Undersampling de la clase mayoritaria
- Generar anomalías artificiales
  - Cercanos a regiones donde se encuentran anomalías
  - En regiones poco pobladas

Técnicas no supervisadas

- Usando k-nn: los puntos con menos vecinos en su radio (regiones poco pobladas, poca densidad) son anomalías
- Las anomalías pertenecen a clusters chicos, o a la periferia de clusters grandes
- Asumir que los datos están generados por una distribución, y determinar los outliers como los puntos con menos probabilidad dentro de la distribución
- Los puntos con mayor entropía en el dataset (requieren más bits para ser descritos)
- Usando PCA: los outliers tienen variabilidad en los componentes menos importantes
- Visualización