Detección de Anomalías en BGP usando Machine Learning

Carlos Marcelo Martinez

Workshop IA en Sistemas Ciber-Físicos
Nov 2024 - Feb 2025

Introducción

- El protocolo BGP es crítico para la conectividad global de Internet.
- Es vulnerable a incidentes como secuestro de rutas, filtraciones y errores de configuración.
- Este trabajo explora el uso de Machine Learning para detectar anomalías en BGP.

Objetivos

- Identificar incidentes históricos relevantes de BGP.
- Extraer datos de BGP y generar conjuntos de datos procesables.
- Aplicar técnicas de aprendizaje automático para detectar anomalías.

Fuentes de Datos

- Datos obtenidos de:
  - **RIPE RIS**: Conjunto de datos de enrutamiento global.
  - **RouteViews**: Datos de sesiones BGP en múltiples puntos de la red.
- Procesamiento usando **BGPStream** para extraer features.

Algoritmos Utilizados

- **Supervisado**:
  - Regresión Logística.
  - Árboles de Decisión y Random Forest.
- **No Supervisado**:
  - One-Class SVM.
  - Local Outlier Factor (LOF).

One-Class SVM

- **¿Qué es?**
  - Algoritmo de aprendizaje no supervisado basado en máquinas de soporte vectorial.
  - Modela los datos normales y detecta outliers como desviaciones significativas.
- **Resultados obtenidos:**
  - Identificó correctamente intervalos anómalos en eventos conocidos.
  - Ajuste de umbrales fue necesario para mejorar la precisión.
  - Detectó anomalías en eventos como el apagón de Moscú 2005 y la filtración de Level 3.

Local Outlier Factor (LOF)

- **¿Qué es?**
  - Algoritmo basado en la densidad de vecinos cercanos.
  - Mide cuán aislado está un punto respecto a su vecindario.
- **Resultados obtenidos:**
  - Detectó con precisión eventos anómalos sin necesidad de datos etiquetados.
  - Menos sensible a outliers extremos que One-Class SVM.
  - Se observó un buen rendimiento en la detección de filtraciones de prefijos.

Resultados

- Los modelos supervisados sufrieron de **desbalanceo de clases** y bajo **recall**.
- Los métodos no supervisados (One-Class SVM y LOF) lograron detectar intervalos anómalos con mayor precisión.
- Se identificó que las ventanas de tiempo cortas (**6 segundos**) mejoraban la detección de anomalías.

Casos de Estudio

- **Apagón de Moscú 2005**: Impacto en el tráfico de Internet.
- **Filtración de rutas de Level 3 (2017)**: Afectación masiva en EE.UU.
- **Incidente de Rostelecom (2020)**: Filtración de miles de prefijos europeos.

Conclusiones

- Machine Learning es una herramienta prometedora para la detección de anomalías en BGP.
- Los modelos no supervisados son más efectivos, pero requieren ajuste fino.
- Es necesario mejorar la precisión de los datos y explorar estrategias de detección en tiempo real.

Trabajo Futuro

- Implementación en tiempo real con **Kafka** y **procesamiento de streaming**.
- Mejora en la selección de features para detectar anomalías con menor cantidad de prefijos afectados.
- Desarrollo de modelos explicables que diferencien entre ataques, fallas de red y cambios benignos.

¡Gracias!

¿Preguntas?

Contacto:
carlos@cagnazzo.uy
carlos@lacnic.net