

# Ataque de envenenamiento e inundación de ARP en SDN

Publicado: 7 de abril de 2022 | Versión 2 | DOI: 10.17632/yxzh9fbvbj.2  
Colaboradores: Nisha Ahuja, Gaurav Singal, Debajyoti Mukhopadhyay

## descripción

Es un conjunto de datos específicos de SDN generados mediante el emulador de mininet y utilizados para la clasificación del tráfico por aprendizaje automático y algoritmos de aprendizaje profundo. Una topología de árbol con profundidad y valor de abanico de tres se emula en Mininet y utilizado con fines experimentales. Un total de 27 hosts y 13 conmutadores están conectados a un controlador Ryu único. La simulación de red se ejecuta para benignos y tráfico de ataque donde el tráfico de ataque es una colección de veneno ARP y ataque de inundación ARP.

Descargar todos los 1,77 MB



## Archivos

 ARP Poison, ataque a inundaciones Dataset.csv

17 MB



## Pasos para reproducir

Un total de 15 características están disponibles en el conjunto de datos que incluye switch-id, in\_port, out\_port, src\_mac\_eth, dest\_mac\_eth que es Dirección MAC de origen y destino en la capa Ethernet, src\_mac\_arp, dest\_mac\_arp, que es Dirección MAC de origen y destino en la capa ARP, IP de origen, IP de destino, código de operación que se divide en cuatro tipos (1 solicitud de ARP, respuesta de 2 ARP, solicitud de 3 de ICMP, respuesta de 4 ICMP), número de los mensajes Packet\_in generados durante la transmisión de tráfico, Protocolo que especifica 0 para ARP y 1 para ICMP, Pkt pérdida que especifique la pérdida de paquetes durante la transmisión de tráfico, rtt (avg) especifique el tiempo promedio de ida y vuelta, tiempo total que especifique el tiempo total para toda la operación de ping que también incluye el tiempo de retardo. La última columna indica la etiqueta de clase que indica si el tipo de tráfico es benigno o malicioso. Tráfico benigno tiene etiqueta 0 y tráfico malicioso tiene etiqueta 1 o 2 dependiendo de ARP el tráfico de veneno tiene etiqueta 1 y el tráfico de inundación de ARP tiene etiqueta 2. La simulación de red se ejecuta durante 250 minutos y 1.04.345 filas de datos se recoge. La simulación de red se ejecuta durante 300 minutos y se recopilan 1.34.000 filas de datos. La simulación se ejecuta de nuevo para un intervalo definido y se pueden recopilar más datos. Los datos se generan tomando el registro de tráfico benigno y tráfico de ataque. El tráfico de ataque estaba compuesto por veneno ARP y ataques de inundación de ARP. Por lo tanto, en total hay tres clases de tráfico (benigno, veneno ARP y ataque de inundación ARP) presentes en el conjunto de datos. Este conjunto de datos se puede utilizar con cualquier modelo de aprendizaje automático para la clasificación del tráfico.

## Instituciones

Universidad Bennett

## categorías

Seguridad de red

## Licencia

CC POR 4.0

[más información](#)

## Métricas del conjunto de datos

Uso	
Vistas:	720
Descargas:	123


 [VER DETALLES](#) >

## Última versión

Versión 2  
Publicado: 7 de abril de 2022  
DOI: 10.17632/yxzh9fbvbj.2

**Cita este conjunto de datos**

Ahuja, Nisha; Singal, Gaurav; Mukhopadhyay, Debajyoti (2022), “ARP Poisoning and Flood attack in SDN”, Mendeley Data, V2, doi: 10.17632/yxzh9fbvbj.2

 Copiar al portapapeles

## Versiones anteriores

Versión 1 31 de marzo de 2022

## Comparación de versiones

 [Comparar versiones](#)