ỨNG DỤNG MÔ HÌNH LSTM ĐƯỢC SỬ DỤNG ĐỂ PHÂN LOẠI TẤN CÔNG DDOS

TRƯƠNG CÔNG BÌNH

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

Mục tiêu

Chúng tôi ứng dụng mô hình trong việc phát hiện và phòng chống DDoS. Trong đó mục tiêu hướng đến :

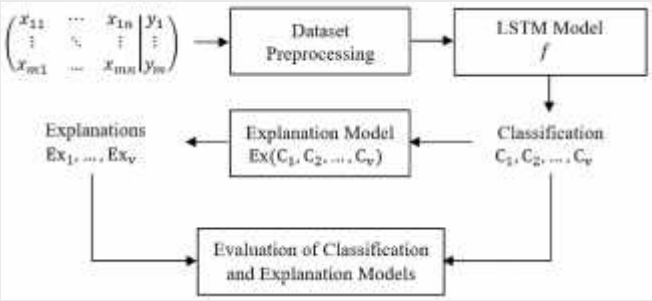
- Tăng cường khả năng thích ứng với các loại tấn công mới
- Hỗ trợ việc phân tích dữ liệu và ra quyết định
- Phát triển các hệ thống phòng chống DDoS hiệu quả hơn

Lý do chọn đề tài ?

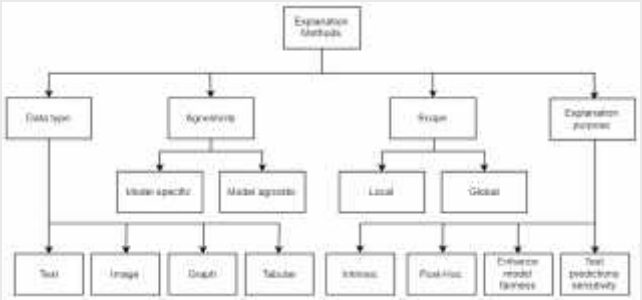
– Đánh giá hiệu suất LSTM trong việc phát hiện các loại tấn công DDoS khác nhau bằng cách sử dụng các bộ dữ liệu CIC được sử dụng phổ biến và công khai

– Việc phân loại chính xác lưu lượng mạng giúp phát hiện sớm các cuộc tấn công DDoS và thực hiện các biện pháp phòng thủ kịp thời

TỔNG QUAN



Phương pháp phát hiện và giải thích kiến trúc



Kiến trúc mô hình phân loại LSTM

MÔ TẢ

Nội Dung

- Mô hình LSTM cho phân loại tấn công DDoS thường bao gồm các thành phần sau:
- Lớp thu thập dữ liệu: Dữ liệu lưu lượng truy cập mạng được ghi lại, bao gồm các tính năng như địa chỉ IP nguồn và đích, cổng, giao thức, byte được truyền.
- Lớp tiền xử lý dữ liệu: Xử lý trước dữ liệu: Dữ liệu được thu thập được làm sạch, chuẩn hóa và định dạng để tương thích với LSTM.
- Lớp LSTM: Bao gồm nhiều lớp nơ-ron LSTM được kết nối với nhau. Các nơ-ron LSTM có khả năng học hỏi các phụ thuộc thời gian trong dữ liệu lưu lượng mạng.
- Lớp phân loại: Phân loại dữ liệu đầu vào là lưu lượng truy cập bình thường hay tấn công DDoS.
- Sử dụng mô hình LSTM để phân loại 17 loại tấn công DDoS

Phương Pháp

- **LIME (Local Interpretable Model-Agnostic Explanations)**
- LIME tạo ra các mô hình giải thích cục bộ xấp xỉ mô hình LSTM bằng một mô hình tuyến tính đơn giản trong vùng lân cận của điểm dữ liệu được giải thích.
- Mô hình tuyến tính này được đào tạo trên một tập dữ liệu nhỏ được tạo ra từ điểm dữ liệu được giải thích và các điểm dữ liệu lân cận.
- Các trọng số của mô hình tuyến tính được sử dụng để xác định các đặc điểm quan trọng nhất cho dự đoán của LSTM tại điểm dữ liệu được giải thích.
- **SHAP (SHapley Additive exPlanations):**
- SHAP sử dụng phân bố Shapley để phân bổ mức độ ảnh hưởng của mỗi đặc điểm đối với dự đoán của LSTM.
- Phân bố Shapley là một phương pháp phân bổ giá trị công bằng cho mỗi người chơi trong một trò chơi hợp tác.
- Trong ngữ cảnh giải thích mô hình, mỗi đặc điểm được coi là một người chơi và giá trị Shapley của nó đại diện cho mức độ ảnh hưởng của nó đối với dự đoán.
- **Anchor:**
- Anchor tìm kiếm các điểm dữ liệu lân cận với điểm dữ liệu được giải thích có cùng dự đoán với LSTM.
- Các điểm dữ liệu này được gọi là "anchor" và được sử dụng để giải thích dự đoán của LSTM tại điểm dữ liệu được giải thích.
- Anchor có thể được sử dụng để so sánh điểm dữ liệu được giải thích với các điểm dữ liệu tương tự khác và xác định các đặc điểm khác biệt.
- **LORE (Local Optimal Reconstruction Explanation):**
- LORE sử dụng phương pháp tối ưu hóa cục bộ để tìm kiếm một tập con nhỏ các đặc điểm có thể tái tạo dự đoán của LSTM tại điểm dữ liệu được giải thích.
- Tập con này được gọi là "LORE" và được sử dụng để giải thích dự đoán của LSTM.
- LORE có thể được sử dụng để xác định các đặc điểm quan trọng nhất cho dự đoán của LSTM tại điểm dữ liệu được giải thích.

Kết Quả Đạt Được

- Mô hình LSTM đạt được độ chính xác cao trong việc phân loại các cuộc tấn công DDoS.
- Các phương pháp giải thích giúp hiểu rõ cách thức hoạt động của mô hình LSTM.
- 51 đặc điểm quan trọng được xác định để phân loại tấn công DDoS.
- Phương pháp LIME đạt hiệu suất tốt nhất về độ chính xác mô tả (DA) và độ thưa thớt mô tả (DS).

NII

TRƯƠNG CÔNG BÌNH -Trường Đại học Công nghệ thông tin TPHCM

TEL : 0909934728 Email : binhtc.18@grad.uit.edu.vn