PHÁT HIỆN TẤN CÔNG DDOS ĐỐI KHÁNG BẰNG MÔ HÌNH GAN VỚI BỘ PHÂN BIỆT KÉP (GAN-DD)

Kiều Hồng Khang - 240201042

[1] Trường ĐH……

[2] University of Science HCMC, Vietnam

[3] National Institute of Informatics

What ?

Ứng dụng mô hình GAN với Bộ phân biệt đối xử kép (GAN-DD) để phát hiện các cuộc tấn công DDoS, trong đó:

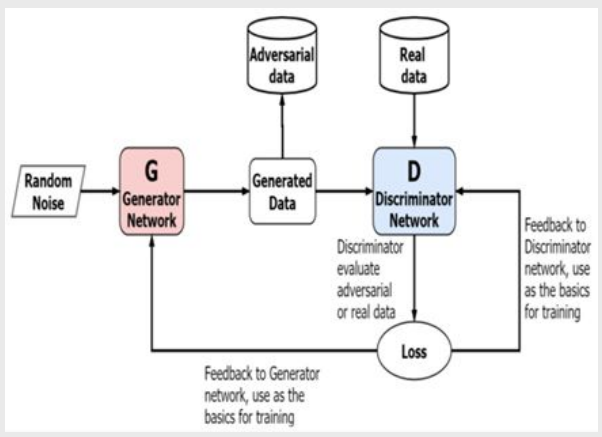
- Nghiên cứu và phát triển mô hình GAN-DD.
- Đánh giá hiệu quả của mô hình GAN-DD
- So sánh hiệu quả của mô hình GAN-DD với các phương pháp phát hiện tấn công DDoS truyền thống.

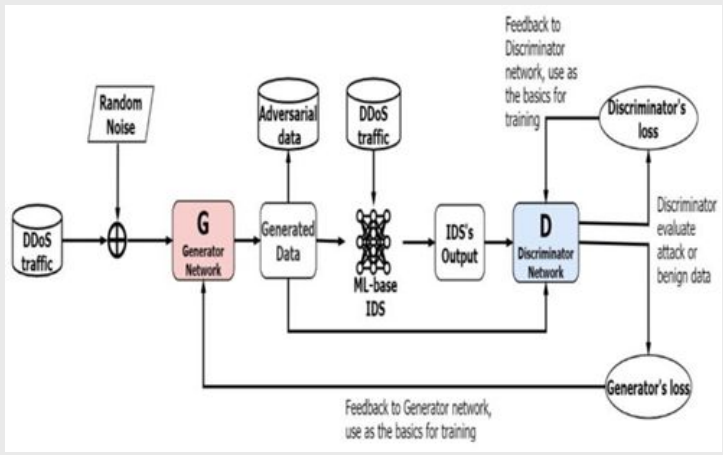
Why ?

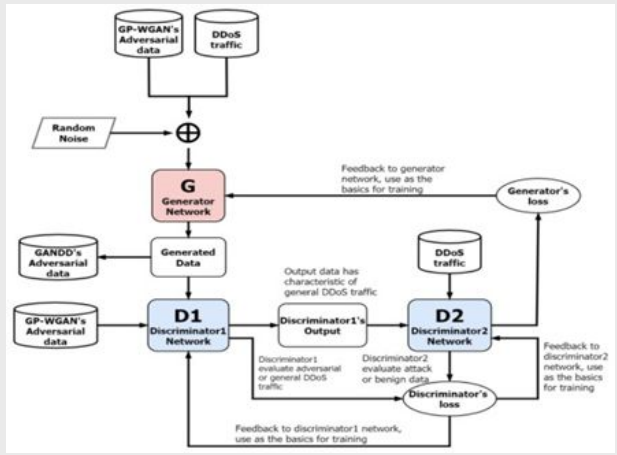
- Các cuộc tấn công DDoS đang ngày càng gia tăng về tần suất, cường độ và độ phức tạp.
- Các phương pháp phát hiện hiện tại (ML/DL) vẫn còn hạn chế trước các kỹ thuật tấn công đối kháng (adversarial attacks).
- Mô hình GAN-DD hứa hẹn mang lại hiệu quả phát hiện tốt hơn nhờ khả năng học sâu và chống lại dữ liệu giả mạo.

Overview

Mô hình GAN → Mô hình WGAN-GP → Mô hình GAN-DD





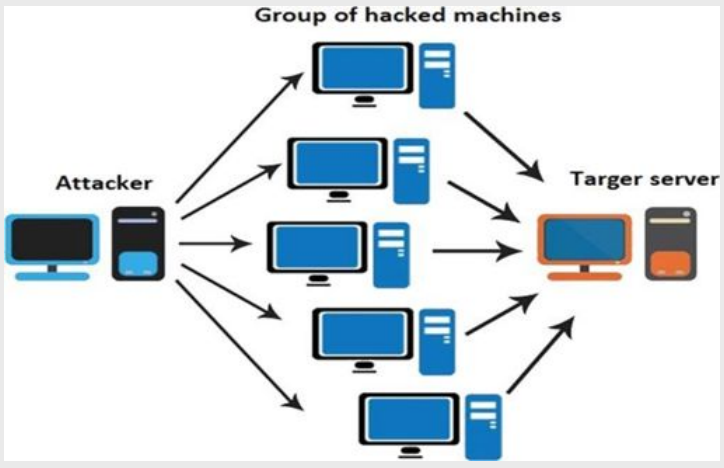


Description

1. Tìm hiểu các phương pháp phát hiện tấn công DDoS truyền thống

Phân tích so sánh ưu và nhược điểm của các phương pháp phát hiện tấn công DDoS hiện có theo:

- Phát hiện dựa trên quy tắc.
- Phát hiện dựa trên thống kê
- Phát hiện dựa trên máy học.



2. Tìm hiểu mô hình GAN-DD

Kiến trúc và nguyên tắc hoạt động của mô hình GAN-DD

Ứng dụng GAN-DD vào phát hiện tấn công DDoS theo phương pháp:

- Thu thập dữ liệu: Thu thập dữ liệu lưu lượng truy cập mạng và dữ liệu tấn công DDoS từ các nguồn khác nhau
- Xử lý dữ liệu: Làm sạch, chuyển đổi và chuẩn hóa dữ liệu để đảm bảo chất lượng dữ liệu phù hợp cho việc huấn luyện mô hình
- Huấn luyện mô hình GAN-DD: Thiết lập cấu trúc mô hình, chọn thuật toán tối ưu hóa và huấn luyện mô hình GAN-DD

3. Triển khai mô hình GAN-DD

- Triển khai mô hình GAN-DD: Triển khai mô hình GAN-DD vào hệ thống phát hiện tấn công DDoS thực tế.
- Đánh giá mô hình GAN-DD: Tiến hành đánh giá hiệu quả phát hiện tấn công DDoS của mô hình GAN-DD, bao gồm tính chính xác, độ nhạy và độ đặc trưng.
- Phân tích thách thức và giải pháp: Xác định các thách thức khi ứng dụng GAN-DD vào phát hiện tấn công DDoS

NII

KIỀU HỒNG KHANG – University of Science HCMC, Vietnam

TEL : 0368458614 Email : Khangkh.19@grad.uit.edu.vn