DETECTION OF ADVERSARIAL DDOS ATTACKS USING GENERATIVE ADVERSARIAL NETWORKS WITH DUAL DISCRIMINATORS (GANDD)

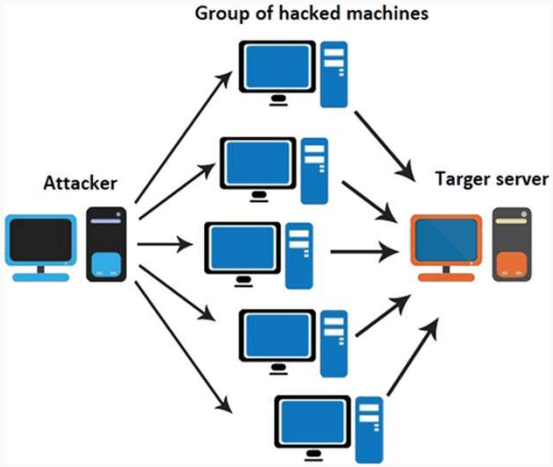
NGUYỄN THÀNH TÂM - 230201053

Tóm tắt

- Lớp: CS2205.APR2023
- Link Github: https://github.com/nguyentam88/TamNT-CS2205.APR2023
- Link YouTube video: https://youtu.be/w2dThVfun5E

Nguyễn Thành Tâm

Giới thiệu



- Sự gia tăng về tần suất, cường độ và độ phức tạp của cuộc tấn công DDoS.
- Hạn chế về huấn luyện, thu thập dữ liệu, đánh giá và kiểm tra của các phương pháp ML và DL.
- Kỹ thuật tấn công mới là tấn công DDoS với lưu lượng tấn công mạng đối nghịch.
- Mô hình GANDD là giải pháp mới dựa trên mô hình GAN với thiết kế gồm bộ phân biệt đối xử kép giúp cải thiện khả năng phát hiện tấn công DDoS.

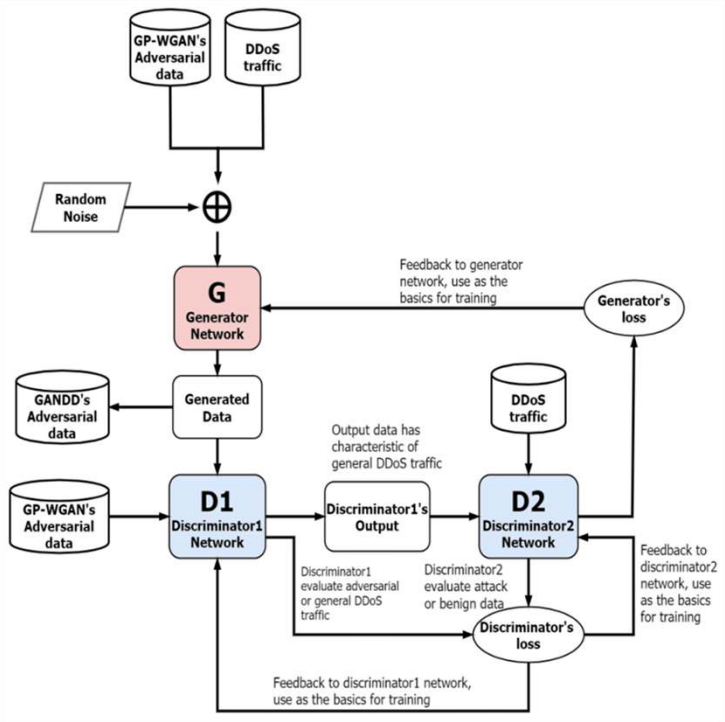
Mục tiêu

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

Nội dung và Phương pháp

Nội dung:

- Khảo sát các phương pháp phát hiện tấn công DDoS truyền thống.
- Tìm hiểu mô hình GANDD.
- So sánh GANDD với các biến thể khác của mô hình GAN
- Ứng dụng GANDD vào phát hiện tấn công DDoS.
- Đánh giá hiệu quả của GANDD.
- Phân tích thách thức và giải pháp.



Nội dung và Phương pháp

Phương Pháp:

- Thu thập dữ liệu.
- Xử lý dữ liệu.
- Huấn luyện mô hình GANDD.
- Triển khai mô hình GANDD.
- Đánh giá mô hình GANDD.

Kết quả dự kiến

Việc ứng dụng GANDD (Generative Adversarial Networks with Dual Discriminators) vào phát hiện tấn công DDoS mang lại nhiều kết quả mong đợi bao gồm:

- Phát triển mô hình GANDD có khả năng phát hiện tấn công DDoS.
- Đánh giá chi tiết hiệu quả của mô hình GANDD trong việc phân biệt lưu lượng tấn công DDoS với lưu lượng bình thường.
- So sánh hiệu quả của mô hình GANDD với các phương pháp phát hiện tấn công DDoS truyền thống.
- Xác định các thách thức và đề xuất giải pháp khi ứng dụng.

Tài liệu tham khảo

[1]. Goodfellow, I.J.; Pouget-Abadie, J.; Mirza, M.; Xu, B.; Warde-Farley, D.; Ozair, S.; Courville, A.; Bengio, Y. Generative adversarial networks. In Proceedings of the 27th International Conference on Neural Information Processing Systems, Montreal, QC, Canada, 8–13 December 2014; Volume 2, 2672–2680.

[2]. Gulrajani, I.; Ahmed, F.; Arjovsky, M.; Dumoulin, V.; Courville, A.C. Improved training of Wasserstein GANs. In Proceedings of the 31st International Conference on Neural Information Processing Systems, Long Beach, CA, USA, 4–9 December 2017; 5769–5779

[3]. Nguyen, T.D.; Le, T.; Vu, H.; Phung, D. Dual Discriminator Generative Adversarial Nets. In Proceedings of the Advances in Neural Information Processing Systems 30, Long Beach, CA, USA, 4–9 December 2017; pp. 2667–2677.

[4]. Zhang, X.; Zhao, Y.; Zhang, H. Dual-discriminator GAN: A GAN way of profile face recognition. In Proceedings of the 2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), Dalian, China, 27–29 June 2020; 162–166