TRANG THÔNG TIN LUẬN ÁN TIẾN SĨ

Tên đề tài luận án tiến sĩ: **Giải pháp phát hiện nhanh các Hot-IP trong hệ thống mạng và ứng dụng**

Chuyên ngành: **Hệ thống thông tin**

Mã số: **62.48.01.04**

Họ và tên NCS: **Huỳnh Nguyên Chính**

Người hướng dẫn khoa học:

1. PGS. TS. Nguyễn Đình Thúc
2. TS. Tân Hạnh

Cơ sở đào tạo: Học viện Công nghệ Bưu chính Viễn thông

NHỮNG KẾT QUẢ MỚI CỦA LUẬN ÁN

1. Đề xuất giải pháp phát hiện các Hot-IP trên mạng dựa trên thử nhóm bất ứng biến và một số kỹ thuật kết hợp để nâng cao hiệu quả của giải pháp. Trong đó, kỹ thuật tính toán song song được sử dụng trong bước tính vector kết quả của các nhóm thử, kiến trúc phân tán được sử dụng trong các hệ thống mạng đa vùng để cảnh báo sớm từ các vùng phát hiện được Hot-IP, lựa chọn kích thước ma trận phù hợp ở vị trí triển khai giải pháp nhằm giảm áp lực tính toán. Lý thuyết nền tảng cho phương pháp đề xuất là sử dụng phương pháp nối mã để xây dựng tường minh ma trận phân cách. Nhờ đó, không gian lưu trữ được tối ưu thay vì phải lưu trữ toàn ma trận có kích thước lớn.
2. Đề xuất hai thuật toán cải tiến "*online Hot-IP detecting*" và "*online Hot-IP preventing*" để giảm thời gian tính toán phát hiện các Hot-IP trực tuyến. Điểm khác biệt của thuật toán cải tiến là các nhóm thử đến ngưỡng không cần phải cập nhật tiếp tục, danh sách các địa chỉ IP nghi ngờ được xác định và khởi tạo bộ đếm tương ứng, các cập nhật đối với các IP có mặt trong danh sách nghi ngờ được thực hiện thay vì phải cập nhật trong tập rất lớn tất cả các các bộ đếm của các nhóm thử dựa vào ma trận phân cách.
3. Mô hình hóa 4 bài toán ứng dụng: (1) phát hiện các đối tượng có khả năng là các nguồn phát tán sâu Internet, (2) phát hiện các thiết bị có khả năng đang hoạt động bất thường, (3) phát hiện các đối tượng có khả năng là mục tiêu hay nguồn phát trong tấn công từ chối dịch vụ về bài toán phát hiện Hot-IP và (4) giám sát hoạt động của các Hot-IP kết hợp với theo dõi tài nguyên mạng để điều phối hay hạn chế hoạt động của các luồng dữ liệu chứa các Hot-IP này. Kỹ thuật được sử dụng là phân tích luồng dữ liệu dựa vào địa chỉ IP nguồn và đích trong các gói tin kết hợp với theo dõi tài nguyên hệ thống làm dữ liệu đầu vào trong thuật toán phát hiện các Hot-IP.

CÁC ỨNG DỤNG, KHẢ NĂNG ỨNG DỤNG TRONG THỰC TIỄN HOẶC NHỮNG VẤN ĐỀ CÒN BỎ NGỎ CẦN TIẾP TỤC NGHIÊN CỨU:

Khả năng ứng dụng trong thực tiễn

Trong bối cảnh hiện nay, các hình thức tấn công trên mạng ngày càng phổ biến, đặc biệt là tấn công từ chối dịch vụ (DoS/DDoS), phát tán sâu mạng, việc xây dựng các giải pháp nhằm phát hiện và hạn chế các hoạt động tấn công, phá hoại trên mạng là cấp thiết. Luận án đã đề xuất giải pháp phát hiện các địa chỉ IP có tần suất xuất hiện cao trên mạng (gọi là Hot-IP), từ đó ứng dụng vào việc phòng chống các hoạt động tấn công trên mạng như tấn công DoS/DDoS, phát tán sâu Internet,…Do vậy, đề tài luận án có khả năng được áp dụng vào thực tiễn rất lớn.

Những vấn đề còn bỏ ngỏ cần tiếp tục nghiên cứu

Luận án đã trình bày một giải pháp hoàn chỉnh về phát hiện các Hot-IP trên mạng và một số ứng dụng trong lĩnh vực an ninh mạng. Bên cạnh việc áp dụng giải pháp vào thực tiễn, đặc biệt là triển khai giải pháp trên phần cứng, hướng nghiên cứu mở tiếp theo là kết hợp phân tích một số yếu tố khác trong dòng dữ liệu để nhận dạng, phân loại nguy cơ từ bài toán phát hiện các Hot-IP này.

Xác nhận của người hướng dẫn khoa học **Nghiên cứu sinh**

NGUYỄN ĐÌNH THÚC TÂN HẠNH HUỲNH NGUYÊN CHÍNH