TRANG THÔNG TIN LUẬN ÁN TIẾN SĨ

Tên đề tài luận án tiến sĩ: **Phát triển một số mô hình phát hiện bất thường mạng dựa trên học sâu và tổng hợp dữ liệu**

Chuyên ngành: **Hệ thống thông tin**

Mã số: **9.48.01.04**

Họ và tên NCS: **Bùi Công Thành**

Người hướng dẫn khoa học:

1. **PGS.TS. Hoàng Minh**
2. **PGS.TS. Nguyễn Quang Uy**

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

NHỮNG KẾT QUẢ MỚI CỦA LUẬN ÁN:

Sự phát triển nhanh chóng của hạ tầng và dịch vụ mạng máy tính trong những năm qua đã kéo theo sự bùng nổ các nguy cơ, đe doạ an ninh mạng. Nghiên cứu các giải pháp để phát hiện và ngăn chặn các tấn công mạng là nhiệm vụ thu hút sự quan tâm của rất nhiều nhà nghiên cứu, tiêu biểu là phát triển các mô hình phát hiện bất thường mạng (Network Anomaly Detection – NAD). Theo đó, mục đích luận án hướng đến nghiên cứu cải tiến các thuật toán phát hiện bất thường mạng, kết quả thể hiện thông qua các mô hình lý thuyết, sau đó cài đặt thực nghiệm để hỗ trợ kiểm chứng, đánh giá kết quả. Các kết quả đóng góp chính của luận án có thể được tóm tắt như sau.

(1) Luận án đã đề xuất được các mô hình phát hiện bất thường mạng dựa trên học sâu, các giải pháp có tên Clustering-Shrink AutoEncoder (KSAE) và Double-Shrink AutoEncoder (DSAE). Các giải pháp này được đề xuất để khắc phục một số hạn chế mà mô hình tiêu biểu SAE gặp phải, SAE được cho là hoạt động hiệu quả trên nhiều tập dữ liệu an ninh mạng. Trong đó, DSAE là mô hình NAD mới và có hướng đi khác với các phương pháp dựa trên mạng nơ-ron AutoEncoder, DSAE sử dụng đồng thời cả hai yếu tố là lỗi tái tạo (RE) và vector lớp ẩn làm cơ sở đưa ra độ đo bất thường. Kết quả thực nghiệm đã cho thấy, DSAE có thể phát hiện hiệu quả hơn với các tấn công mà mô hình tiêu biểu NAD dựa trên học sâu gặp khó. Các tấn công này được cho là có dữ liệu rất giống với dữ liệu bình thường, do vậy thường tạo ra khó khăn cho các mô hình phát hiện bất thường mạng.

(2). Luận án đã đề xuất được một phương pháp khung có tên là OFuseAD (One-Class Fusion-based Anomaly Detection), giải pháp cho phép giải quyết các hạn chế của các phương pháp đơn thường được cho là rất hiệu quả trên một vấn đề cụ thể, còn với các vấn đề khác thường không hiệu quả. OFuseAD

cung cấp một kiến trúc chung để xây dựng các mô hình tổng hợp dữ liệu trong điều kiện bài toán học bán giám sát (nghĩa là thường không sẵn có dữ liệu dương tính và nhãn tương ứng để giúp đánh giá giải pháp đề xuất). Giải pháp này gom lợi thể từ các phương pháp đơn NAD, mô hình có thể hoạt động mà không cần sự can thiệp của chuyên gia trong thiết lập ngưỡng, phù hợp với yêu cầu thực tiễn.

(3). Luận án đề xuất giải pháp ứng dụng phù hợp lý thuyết Dempster-Shafer (D-S) cho phát hiện bất thường mạng. Đã đề xuất được hàm có tên One-Class Basic Probability Assignment (OBPA), đây là vấn đề được cho là khó khăn khi ứng dụng lý thuyết D-S. Đã đề xuất được hàm DRC_AD, đây là giải pháp mở rộng của hàm kết hợp DRC trong lý thuyết D-S, giúp khắc phục hạn chế đang gặp phải.

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

(1). Mô hình khung OFuseAD có thể được ứng dụng cho các bài toán phát hiện bất thường khác, không chỉ riêng trong phạm vi NAD. Nhìn chung, OFuseAD có thể được xem xét ứng dụng cho các bài toán phân đơn lớp (OCC).

(2) Các kết quả của luận án về lý thuyết Dempster-Shafer như cách thiết lập hàm OBPA, luật DRC-AD có thể được cân nhắc ứng dụng.

(3) Luận án đề xuất một phương pháp mới để đánh giá độ tin cậy của các phương pháp OCC. Phương pháp này có thể được sử dụng như là chỉ số để so sánh độ tin cậy giữa các phương pháp đơn OCC.

(4) Ngoài các kết quả đạt được, luận án vẫn còn một số hạn chế như: việc xây dựng mô hình OFuseAD đang trên giả định các bộ phát hiện cục bộ đều quan sát đồng nhất một nguồn dữ liệu, do vậy làm cho mô hình có hạn chế về tính linh hoạt; OFuseAD sử dụng các phương pháp đơn dựa trên khoảng cách và dựa trên mật độ dẫn đến chi phí tính toán thường lớn.

(5) Một số hướng nghiên cứu phát triển tiếp theo như; với mô hình tổng hợp dữ liệu, có thể hướng đến sử dụng nhiều bộ phát hiện cục bộ; các loại bộ phát hiện có thể đa dạng hơn, bao gồm cả quyết định từ các chuyên gia, các ứng dụng an ninh mạng hoặc ngay cả thông tin có được từ các bộ phát hiện môi trường vật lý.

Xác nhận của đại diện tập thể	**Nghiên cứu sinh**
Người hướng dẫn khoa học	
PGS.TS. Hoàng Minh	**Bùi Công Thành**