THÔNG TIN LUẬN ÁN

Tên luận án: **TĂNG CƯỜNG KHẢ NĂNG PHÒNG CHỐNG TẤN CÔNG TRONG MẠNG SDN**

Ngành: **Công nghệ Thông tin**

Mã số: **9480201**

Họ tên: **PHAN THẾ DUY**

Cán bộ hướng dẫn: **TS. PHẠM VĂN HẬU và PGS.TS. LÊ ĐÌNH DUY**

Cơ sở đào tạo: **TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN – ĐHQG TP.HCM**

TÓM TẮT

Luận án nghiên cứu và xây dựng khung liên kết phát hiện xâm nhập và săn tìm mối đe dọa trong mạng khả lập trình (Software-Defined Networking – SDN) thông qua mô hình học liên kết (Federated Learning - FL). Cách tiếp cận này giúp nâng cao hiệu quả phát hiện và ngăn chặn các tấn công mạng mới xuất hiện trong môi trường SDN phân tán, nơi có sự tham gia của nhiều tổ chức. Trong mô hình này, các máy khách huấn luyện đại diện cho các bên tham gia hệ thống học liên kết, chẳng hạn như các máy huấn luyện được quản lý bởi các Trung tâm Điều hành An ninh Mạng (Security Operation Center - SOC) vận hành SDN. Khi đó, việc triển khai các hệ thống phát hiện xâm nhập (Intrusion Detection System – IDS) dựa trên FL mang lại nhiều lợi ích trong việc bảo vệ dữ liệu nhạy cảm, nhưng cũng gặp phải một số điểm yếu và rào cản về bảo mật từ các bên tham gia không tin cậy. Do đó, luận án tập trung vào mục tiêu tăng cường các khía cạnh bảo mật cốt lõi trong phát triển bộ khung IDS dựa trên học liên kết (Federated Learning - FL), vừa khai thác lợi thế của FL trong bảo vệ dữ liệu nhạy cảm, vừa xử lý các thách thức bảo mật trọng yếu của các hệ thống sử dụng FL trong bối cảnh an ninh mạng. Luận án đã đạt được bốn đóng góp nổi bật, bao gồm:

- Tăng cường khả năng chống tấn công riêng tư (Privacy Attack) thông qua việc phát triển cơ chế đảm bảo tin cậy và quyền riêng tư: Luận án đề xuất một cơ chế nhằm đảm bảo tính tin cậy và bảo vệ quyền riêng tư dữ liệu trong quá trình huấn luyện mô hình học máy liên kết cho các ứng dụng phát hiện xâm nhập và săn tìm mối đe dọa trên mạng SDN. Giải pháp này ngăn chặn chia sẻ dữ liệu nhạy cảm và đảm bảo tính an toàn khi tổng hợp các bản cập nhật mô hình từ nhiều nguồn.
- Tăng cường khả năng chống tấn công đầu độc (Poisoning Attack) thông qua giải pháp phát hiện và loại bỏ tấn công đầu độc mô hình liên kết phát hiện xâm nhập: Luận án giới thiệu phương pháp ngăn ngừa tấn công đầu độc mô hình toàn cục bằng cách phân tích không gian tiềm ẩn của các bản cập nhật từ các máy khách huấn luyện cục bộ, nhằm nâng cao tính bảo mật cho mô hình học máy liên kết.
- Tăng cường khả năng chống tấn công trốn tránh (Evasion Attack) thông qua cơ chế đánh giá tính bền vững và kháng nhiễu cho hệ thống phát hiện xâm nhập: Luận án xây dựng mô hình sử dụng mạng sinh đối kháng để thử nghiệm các mẫu tấn công mới, qua đó đánh giá và đảm bảo hiệu quả phát hiện và ngăn chặn các cuộc tấn công, góp phần tăng cường tính bền vững của hệ thống IDS trong mạng SDN.
- Tăng cường khả năng chống tấn công lạm dụng truy cập (Abuse Attack) từ các ứng dụng mạng không đáng tin cậy với mô hình kiểm soát truy cập phi tập trung cho ứng dụng mạng SDN: Luận án đề xuất và thực nghiệm một mô hình quản lý truy cập dựa trên blockchain, nhằm quản lý quyền truy cập một cách an toàn và đảm bảo an ninh trong quá trình giám sát, thu thập trạng thái hệ thống mạng.

Những đóng góp này không chỉ nâng cao hiệu quả phòng chống tấn công trong mạng SDN mà còn củng cố tính an toàn và bảo mật thông tin trong bối cảnh mạng của nhiều tổ chức có sự cộng tác.

Về công bố khoa học, trong thời gian thực hiện và hoàn thành luận án, NCS đã công bố 08 bài báo khoa học, trong đó: 05 bài báo đăng tại các tạp chí uy tín (05 bài báo tạp chí SCIE xếp hạng Q1) và ba bài báo khoa học đăng tại các hội nghị quốc tế uy tín.

CÁN BỘ HƯỚNG DẪN		NGHIÊN CỨU SINH
Phạm Văn Hậu	**Lê Đình Duy**	**Phan Thế Duy**