ĐẠI HỌC THÁI NGUYÊN

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

**TRầN THANH HÒA**

# NGHIÊN CỨU MỘT SỐ KỸ THUẬT PHÁT HIỆN XÂM NHẬP MẠNG BẰNG PHƯƠNG PHÁP SO KHỚP

**LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH**

**THÁI NGUYÊN – 2016**

ĐẠI HỌC THÁI NGUYÊN

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

**TRẦN THANH HÒA**

# NGHIÊN CỨU MỘT SỐ KỸ THUẬT PHÁT HIỆN XÂM NHẬP MẠNG BẰNG PHƯƠNG PHÁP SO KHỚP

**Chuyên ngành: Khoa học máy tính**

**Mã số: 60 48 0101**

## LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

***Người hướng dẫn khoa học*: TS. Nguyễn Ngọc Cương**

**THÁI NGUYÊN – 2016**

# LỜI CAM ĐOAN

Học viên xin cam đoan luận văn **"Nghiên cứu một số kỹ thuật phát hiện xâm nhập mạng bằng phương pháp so khớp"** là công trình nghiên cứu của cá nhân học viên tìm hiểu, nghiên cứu dưới sự hướng dẫn của TS. Nguyễn Ngọc Cương. Các kết quả là hoàn toàn trung thực, toàn bộ nội dung nghiên cứu của luận văn, các vấn đề được trình bày đều là những tìm hiểu và nghiên cứu của chính cá nhân học viên hoặc là được trích dẫn từ các nguồn tài liệu được trích dẫn và chú thích đầy đủ.

TÁC GIẢ LUẬN VĂN

**Trần Thanh Hòa**

# LỜI CẢM ƠN

Học viên xin bày tỏ lời cảm ơn chân thành tới tập thể các thầy cô giáo Viện công nghệ thông tin, các thầy cô giáo Trường Đại học Công nghệ thông tin và truyền thông - Đại học Thái Nguyên đã mang lại cho học viên kiến thức vô cùng quý giá và bổ ích trong suốt quá trình học tập chương trình cao học tại trường. Đặc biệt học viên xin bày tỏ lòng biết ơn sâu sắc tới thầy giáo TS.Nguyễn Ngọc Cương - Học viện an ninh đã định hướng khoa học và đưa ra những góp ý, gợi ý, chỉnh sửa quý báu, quan tâm, tạo điều kiện thuận lợi trong quá trình nghiên cứu hoàn thành luận văn này.

Cuối cùng, học viên xin chân thành cảm ơn các bạn bè đồng nghiệp, gia đình và người thân đã quan tâm, giúp đỡ và chia sẻ với học viên trong suốt quá trình học tập.

Do thời gian và kiến thức có hạn nên luận văn không tránh khỏi những thiếu sót nhất định. Học viên rất mong nhận được những sự góp ý quý báu của thầy cô và các bạn.

*Thái Nguyên, ngày 10 tháng 5 năm 2016*

HỌC VIÊN

**Trần Thanh Hòa**

# DANH MỤC CÁC HÌNH VẼ

# MỤC LỤC

# MỞ ĐẦU

## 1. Lý do chọn đề tài

Mạng Internet từ cuối thế kỷ XX đã mở ra một làn sóng mới về xu hướng phát triển của xã hội - thời đại của công nghệ thông tin và truyền thông, trong đó các  dịch vụ trực tuyến được phát triển mạnh mẽ như thương mại điện tử, thanh toán trực tuyến, kinh doanh, tài chính, công nghiệp, an ninh, y tế,…

Người sử dụng nhờ mạng Internet có thể truy cập, khai thác và chia sẻ thông tin mọi lúc mọi nơi, tuy nhiên Internet cũng là không gian rộng mở cho kẻ xấu lợi dụng thực hiện những vụ tấn công, truy cập trái phép vào các hệ thống máy tính và mạng của người dùng.

Phát hiện xâm nhập mạng là một trong các thành phần quan trọng trong hệ thống các giải pháp đảm bảo an ninh cho các mạng hiện đại

Hệ thống phát hiện xâm nhập mạng IDS (Intrusion Detection System) có nhiệm vụ phân tích các thông tin, theo dõi, phát hiện và ngăn chặn sự xâm nhập trái phép tài nguyên làm tổn hại đến tính bảo mật, tính toàn vẹn và tính sẵn sàng của hệ thống.

Hiện nay, trong việc phát triển hệ thống IDS có nhiều phương pháp để phát hiện xâm nhập vào hệ thống như:

- *Sử dụng phương pháp Bayes* với ý tưởng tính toán xác suất Bayes để có thể dịch chuyển ngược thời gian và tìm ra nguyên nhân của sự kiện, phù hợp cho việc tìm kiếm lý do cho một sự bất thường đặc biệt trong hành vi mạng.

- *Sử dụng mạng nơ ron nhân tạo* trên mô hình Kohonen’s Self Organizing features Map (SOM) và sử dụng máy học vectơ. Mục tiêu chính của việc sử dụng mạng nơ ron nhân tạo là cung cấp một phương pháp phân