ĐẠI HỌC QUỐC GIA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN

NGUYỄN MINH PHÚC

NGHIÊN CỨU MÔ HÌNH QUẢN LÝ MẠNG CỤC BỘ VÀ ĐÁM MÂY SỬ DỤNG CÔNG NGHỆ TÁC TỬ DI ĐỘNG

Chuyên ngành: Quản lý Hệ thống Thông tin

Mã số: 9480205.01QTD

TÓM TẮT LUẬN ÁN TIẾN SĨ CÔNG NGHỆ THÔNG TIN

Hà Nội – 2026

Công trình được hoàn thành tại: Viện Công nghệ thông tin, Đại học Quốc gia Hà Nội.

Người hướng dẫn khoa học:

1. PGS. TS. Nguyễn Ái Việt

2. TS. Trần Quý Nam

Phản biện 1: PGS.TS Nguyễn Việt Anh

Phản biện 2: PGS. TS Trần Thị Lượng

Phản biện 3: PGS.TS Nguyễn Thanh Tùng

Luận án được bảo vệ trước Hội đồng cấp DHQG chấm luận án tiến sĩ họp tại Phòng 505, nhà E3, Viện Công nghệ thông tin, 144 Xuân Thuỷ, Cầu Giấy, Hà Nội vào hồi 8h30 ngày 18 tháng 03 năm 2026.

Có thể tìm hiểu luận án tại:

Thư viện Quốc gia Việt Nam

CHƯƠNG MỞ ĐẦU

1. Lý do chọn đề tài

Đề tài nghiên cứu được phát triển từ các chuyên đề nghiên cứu tác tử di động của Nghiên cứu sinh, đồng thời được định hướng bởi bối cảnh ứng dụng của các hệ thống quản lý nội dung và truy cập từ xa trong môi trường mạng cục bộ và Internet, trong đó yêu cầu trọng tâm là bảo đảm truy cập an toàn giữa mạng cục bộ (LAN -Local Area Network) và Internet [6], [7]. Mục tiêu của bối cảnh ứng dụng này là hình thành bộ giải pháp cho phép người dùng truy cập Internet từ mạng cục bộ và truy cập các dịch vụ nội bộ từ Internet một cách an toàn; vì vậy, quản trị mạng an toàn là một cấu phần quan trọng của hệ thống. Trên cơ sở đó, các chuyên đề về tác tử di động tập trung nghiên cứu việc sử dụng tác tử di động để hỗ trợ quản trị mạng an toàn, đáp ứng nhu cầu của quản trị viên trong giám sát, hỗ trợ kỹ thuật và khắc phục sự cố từ xa. Để hạn chế nguy cơ bị lợi dụng quyền truy cập dẫn đến xâm nhập trái phép, công nghệ tác tử di động được đề xuất tích hợp trong một kiến trúc an toàn, an ninh mạng [5].

Các kết quả nghiên cứu của các chuyên đề liên quan [3–6] có thể tiếp tục mở rộng để áp dụng cho nhiều loại mạng khác nhau như mạng di động, mạng định nghĩa bởi phần mềm (SDN – Software Defined Network), mạng 5G và IoT (Internet of Things) những lĩnh vực đang có nhu cầu thực tiễn lớn trong nước và quốc tế. Đặc biệt, trong quá trình dịch chuyển hạ tầng từ mạng cục bộ lên điện toán đám mây (Cloud Computing) của các doanh nghiệp, quản trị mạng trở thành vấn đề then chốt và đòi hỏi lời giải cho các thách thức an ninh mạng phức tạp trong giai đoạn quá độ.

Xuất phát từ yêu cầu trên về việc xây dựng một giải pháp đồng bộ, luận án xác định giải quyết 2 vấn đề trọng tâm là mô hình quản trị và công nghệ truy cập. Vấn đề thứ nhất, Trong mô hình quản trị, việc sử dụng cơ sở thông tin quản trị (MIB) đã trở thành tiêu chuẩn. Điều đó đòi hỏi có một mô hình kiến trúc có khả năng cập nhật MIB thường xuyên mà không cần xây dựng lại hệ thống phần mềm, đảm bảo hệ thống hoạt động không bị gián đoạn. Vấn đề thứ hai là việc sử dụng công nghệ bảo đảm an toàn cho ứng dụng quản trị hệ thống. Các quản trị viên hỗ trợ sự cố trong mạng cục bộ hay đám mây từ xa thường phải truy cập vào trong mạng. Do đó, các tài nguyên trong mạng có nguy cơ bị tấn công bằng các hành vi không được phép, nếu quyền truy cập bị lộ lọt. Một kịch bản thường xảy ra là từ một thiết bị, quản trị viên còn cần phải truy cập vào các thiết bị khác để thu thập một số lượng lớn thông tin để khắc phục sự cố. Điều đó kéo theo việc toàn bộ mạng có nguy cơ mất an toàn. Luận án này giải quyết hai vấn đề nêu trên để xây dựng một giải pháp quản trị mạng cục bộ trong quá trình dịch chuyển lên mạng đám mây an toàn dựa trên công nghệ tác tử. Vấn đề thứ nhất được giải quyết bằng phương pháp kiến trúc để kết hợp các chuẩn quản trị mạng SNMP và CMIP. Vấn đề thứ hai được giải quyết bằng công nghệ tác tử và một giải pháp tăng cường tính an toàn của các công nghệ tác tử nguồn mở.

2. Mục đích (hoặc mục tiêu) và nhiệm vụ nghiên cứu

Mục tiêu nghiên cứu tập trung vào các vấn đề cốt lõi sau:

- Nội dung 1: Nghiên cứu và cải tiến đặc tả quản lý mạng trên nền tảng tác tử di động

- Nội dung 2: Nghiên cứu công nghệ tác tử di động và ứng dụng công nghệ tác tử

- Nội dung 3: Nghiên cứu và xây dựng bộ khung ứng dụng trên nền tác tử di động theo chuẩn FIPA

- Nội dung 4: Xây dựng và nâng cao an toàn thông tin và bảo mật cho hệ thống mạng dựa trên nền tảng công nghệ tác tử di động và đảm bảo an toàn thông tin cho nền tảng tác tử di động.

3. Đối tượng và phạm vi nghiên cứu

- Tích hợp các giao thức quản lý mạng SNMP, CMIP và các giao thức quản lý mạng khác.

- Ứng dụng công nghệ tác tử di động vào trong thực tế, và ứng dụng công nghệ tác tử vào trong lĩnh vực quản lý mạng.

- Cải tiến bộ khung ứng dụng trên nền tác tử di động theo chuẩn FIPA.

- Cải tiến kỹ thuật cho đặc tả quản lý mạng trên nền tảng tác tử di động.

- Đề xuất mô hình ứng dụng tác tử và nâng cao an toàn bảo mật cho hệ thống quản lý mạng dựa trên nền tảng công nghệ tác tử di động, đảm bảo an toàn thông tin cho nền tảng tác tử di động.

4. Phương pháp nghiên cứu

- Dựa trên các tài liệu nghiên cứu về công nghệ tác tử di động, ứng dụng tác tử di động, bộ khung ứng dụng tác tử di động và dựa trên nghiên cứu mã nguồn từ các bộ khung ứng dụng tác tử di động để xây dựng, kế thừa và nâng cấp bộ khung ứng dụng tác tử di động.

- Nghiên cứu từ các chuẩn quốc tế về chuẩn về quản lý mạng SNMPv1, SNMPv2, SNMPv3 và chuẩn CMISE/CMIP theo chuẩn OSI, chuẩn về ngôn ngữ giao tiếp giữa các bộ giao thức trừu tượng ASN.1/GDMO và các chuẩn về thông tin quản lý MIBv1, MIBv2, tác tử di động FIPA,... Từ nghiên cứu các chuẩn quốc tế, tiến hành thực nghiệm để cải tiến kỹ thuật, đặc tả

kỹ thuật để xây dựng bộ giao thức bảo mật cho hệ thống thông tin và quản lý mạng dựa trên nền tảng tác tử.

- Thử nghiệm các kết quả nghiên cứu trên hệ thống Lab giả lập; trong trường hợp điều kiện cho phép, có thể triển khai thử nghiệm giải pháp trên hệ thống thông tin tại đơn vị đang công tác và một số công ty CNTT.

5. Đóng góp của luận án

Nghiên cứu này tập trung vào việc giải quyết hai vấn đề chính nhằm xây dựng một hệ thống quản trị mạng cục bộ và đám mây an toàn, hiệu quả dựa trên nền tảng tác tử di động.

Vấn đề thứ nhất tập trung vào việc đề xuất mô hình quản lý mạng cục bộ và đám mây trên nền tảng tác tử di động. Mô hình này tận dụng tính linh hoạt và khả năng tự động hóa của công nghệ tác tử để quản lý hiệu quả các tài nguyên mạng trong cả môi trường truyền thống và đám mây. Bên cạnh đó, nghiên cứu cũng đề xuất các cải tiến kỹ thuật cho nền tảng tác tử di động, bao gồm tối ưu hóa quy trình thực thi, nâng cao khả năng tương tác giữa các tác tử, và cải thiện các cơ chế bảo mật như mã hóa dữ liệu, xác thực danh tính và quản lý quyền truy cập.

Vấn đề thứ hai: bao gồm việc đề xuất giải pháp kết nối giữa hai giao thức quản lý mạng SNMP và CMIP. Giải pháp này nhằm tận dụng ưu điểm của cả hai giao thức: SNMP với tính đơn giản và phổ biến, cùng CMIP với khả năng quản lý phức tạp và tính bảo mật cao. Đồng thời, nghiên cứu cũng đề xuất một mô hình phát hiện xâm nhập IDS tích hợp trên nền tảng SDN để nâng cao tính an toàn và bảo mật cho hệ thống mạng cục bộ và đám mây. Mô hình này kết hợp các kỹ thuật giám sát, phân tích hành vi mạng và phản ứng tự động nhằm ngăn chặn các mối đe dọa tiềm ẩn.

6. Bố cục luận án

Luận án gồm các phần sau:

Phần mở đầu trình bày lý do chọn đề tài; Giới thiệu mục tiêu, đối tượng, phạm vi và phương pháp nghiên cứu; Ý nghĩa khoa học của đề tài; Trình bày bố cục luận án.

Chương 1 trình bày tổng quan về quản lý mạng, bài toán quản lý mạng cục bộ và đám mây, nền tảng tác tử di động và ứng dụng Công nghệ tác tử di động và các giao thức trong quản lý mạng, ứng dụng của tác tử di động vào quản lý hệ thống mạng.

Chương 2 trình bày đề xuất Mô hình kiến trúc Quản lý mạng cục bộ và đám mây trên nền tảng tác di động giúp cho việc quản trị mạng mạng Cụ bộ và đám mây hiệu quả và tối ưu.

Chương 3 trình bày về kỹ thuật ứng dụng tác tử di động để nâng cao an toàn bảo mật thông tin cho hệ thống mạng cục bộ và đám mây, đồng thời đề xuất cải tiến và nâng cao an toàn bảo mật cho nền tác tử di động.

Phần kết luận nêu những đóng góp chính của luận án, các hướng phát triển nghiên cứu tiếp theo và những vấn đề quan tâm của tác giả; danh mục các công trình đã được công bố của liên quan tới nội dung luận án; danh sách tài liệu tham khảo được sử dụng trong luận án.

CHƯƠNG 1: TỔNG QUAN VỀ QUẢN LÝ MẠNG CỤC BỘ VÀ ĐÁM MÂY

1.1. Bài toán dịch chuyển mạng cục bộ (LAN) lên đám mây (Cloud)

Bài toán dịch chuyển mạng cục bộ lên đám mây phức tạp và yêu cầu giải pháp toàn diện. Trong đó, các nội dung cần giải quyết là vấn đề bảo mật dữ liệu và hệ thống, đảm bảo hiệu suất và độ trễ, khả năng tích hợp hệ thống và tương thích, khả năng quản lý tài nguyên giám sát hoạt động và tuân thủ pháp lý, chi phí vận hành.

Luận án tập trung vào nghiên cứu 2 nội dung chính là đảm bảo an toàn thông tin cho hệ thống thông tin và quản lý mạng hiệu quả.

1.1.1 Vấn đề đảm bảo an toàn thông tin trong dịch chuyển mạng cục bộ lên đám mây

Trong đảm bảo an toàn thông tin, Một số vấn đề chính bao gồm bảo mật dữ liệu, bảo vệ hệ thống, duy trì quyền riêng tư, kiểm soát truy cập và đảm bảo tính sẵn sàng của dịch vụ. Đồng thời, cũng đưa ra yêu cầu về xây dựng kiến trúc an toàn thông tin và đảm bảo an toàn cho kiến trúc các hệ thống thông tin:

- Nguy cơ đe dọa an toàn khi dịch chuyển lên đám mây
- Yêu cầu xây dựng Kiến trúc và chuẩn hoá an toàn mạng trong thiết kế hệ thống
- Vấn đề an toàn và kiến trúc để đảm bảo an toàn mạng cho hệ thống thông tin

1.1.2 Vấn đề quản trị mạng hiệu quả cho mạng cục bộ và đám mây

Đối với vấn đề quản trị mạng một số vấn đề phát sinh đối với quản trị mạng cục bộ và đám mây như:

- Vấn đề quản trị các mạng với giao thức SNMP và CMIP
- Vấn đề quản trị mạng bằng công nghệ tác tử
- Vấn đề đảm bảo an toàn cho môi trường tác tử di động

1.2 Tổng quan các nghiên cứu về quản trị mạng cục bộ và đám mây

Từ những vấn đề phát sinh trên, việc phân tích nghiên cứu tổng quan về quản trị mạng cục bộ và đám mây để đề xuất giải pháp cho bài toán quản lý mạng khi dịch chuyển từ mạng cục bộ sang đám mây:

- Nghiên cứu sử dụng giao thức SNMP
- Nghiên cứu mô hình và tối ưu quản trị mạng mới
- Nghiên cứu về giám sát hệ thống
- Nghiên cứu về mạng SDN

1.3 Tổng quan ứng dụng tác tử di động vào quản trị mạng cục bộ và đám mây

Phân tích các bài báo nghiên cứu ứng dụng Tác tử di động trong quản trị mạng và tính hiệu quả, ưu điểm, nhược điểm khi triển khai tác tử di động trong quản trị mạng trong thực tiễn.

1.4 Tổng quan ứng dụng tác tử di động trong quản lý và bảo mật mạng cục bộ và đám mây

Phân tích các bài báo nghiên cứu về các vấn đề bảo mật khi ứng dụng Tác tử di động trong quản trị mạng.

Qua phân tích các bài báo nghiên cứu trên, Luận án tập trung vào việc giải quyết hai vấn đề chính để xây dựng một giải pháp quản trị mạng cục bộ trong quá trình di chuyển lên mạng đám mây một cách an toàn, hiệu quả dựa trên công nghệ tác tử và đảm bảo an toàn thông tin cho hệ thống.

1.5 Kết luận vấn đề nghiên cứu

Thông qua nội dung tổng quan và đánh giá các hiện trạng nghiên cứu, tác giả nhận thấy một số nội dung cần nghiên cứu và đóng góp khoa học để nâng cao hiệu quả cho hệ thống mạng cục bộ và đám mây, đồng thời đảm bảo an toàn thông tin và bảo mật:

1. Đề xuất một phương pháp kiến trúc kết hợp hai chuẩn quản trị mạng phổ biến là SNMP và CMIP dựa trên nền tảng tác tử di động.

2. Vấn đề về nâng cao tính an toàn bảo mật cho nền tảng tác tử di động và sử dụng nền tảng tác tử di động để đảm bảo an toàn cho các hệ thống thông tin.

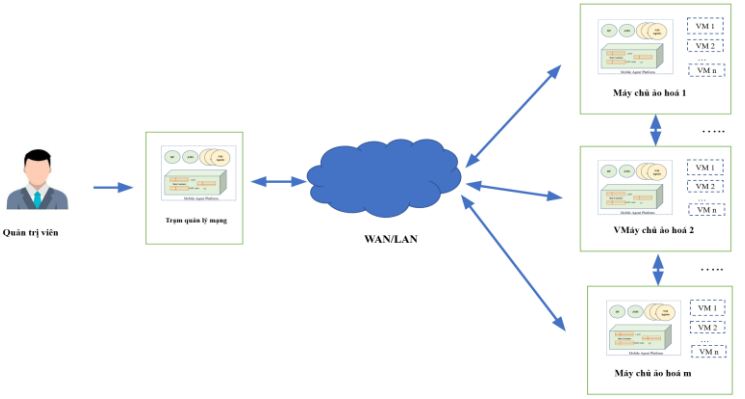
CHƯƠNG 2 XÂY DỰNG MÔ HÌNH TÁC TỬ DI ĐỘNG QUẢN LÝ MẠNG TRÊN MẠNG CỤC BỘ VÀ ĐÁM MÂY

2.1 Xây dựng Mô hình quản lý mạng cục bộ và đám mây dựa trên tác tử di động (CNMMA)

2.2 Kiến trúc mô hình CNMMA

Các thành phần của Mô hình CNMMA bao gồm các thành phần cốt lõi cơ bản như trong hình 2.1:

- Nền tảng tác tử di động
- Máy chủ quản lý mạng ảo hóa
- Trạm quản lý mạng (NMS)
- Quản lý mạng tác tử di động (NMMA)



Hình 2.1: Kiến trúc mô hình CNMMA

2.3 Tích hợp giao thức SNMP và CMIP cho Tác tử di động trong quản lý mạng

2.3.1 Tác tử di động proxy cho quản lý mạng

Tác nhân proxy Mobile Agent (MA) được đề xuất cung cấp mô phỏng các dịch vụ CMIS bằng cách ánh xạ chúng đến các thông điệp SNMP tương ứng. Nó cho phép quản lý các đối tượng Internet MIB-II bằng trình quản lý CMIP hỗ trợ giao thức quản lý mạng CMIP và các dịch vụ CMIS.

Proxy MA thực hiện các chức năng sau:

- Quản lý thiết lập/giải phóng kết nối với trình quản lý CMIP.

- Truyền dữ liệu giữa người quản lý CMIP và tác nhân Internet bao gồm: chuyển các đơn vị dữ liệu giao thức phản hồi và chỉ báo CMIP (PDU) với trình quản lý CMIP; chuyển yêu cầu SNMP và tin nhắn phản hồi với đại lý Internet.

- Chức năng mô phỏng dịch vụ proxy như:

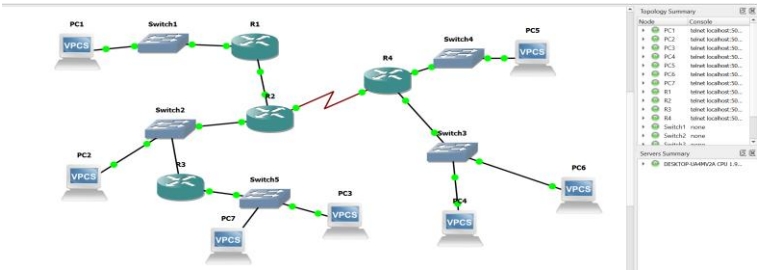
+ Ánh xạ CMIS sang SNMP

+ Ánh xạ SNMP sang CMIS

Proxy MA duy trì một tệp cấu hình trong kho dữ liệu chung để bảo toàn thông tin trong quá trình truyền tin nhắn.

2.3.2 Trình mô phỏng quản lý mạng

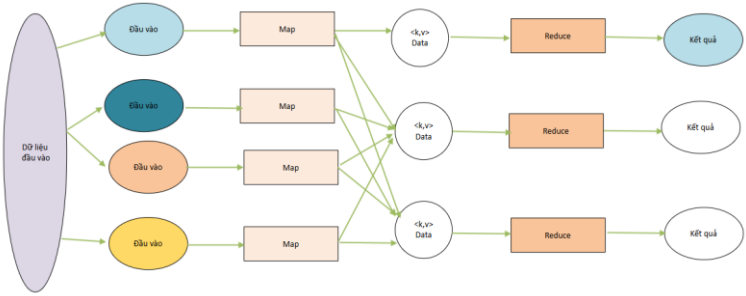
Để thử nghiệm nguyên mẫu giao thức CMIP và lý thuyết về Mô hình CNMMA dẫn tới một trình mô phỏng mạng dựa trên GNS3 và tạo kết nối từ mô phỏng nối mạng đến PC ảo hóa vật lý cài đặt khung nền tảng tác tử di động để thử nghiệm tạo và di chuyển tác tử Quản lý mạng trên nền tảng Tác tử di động.



Hình 2.10: Trình mô phỏng quản lý mạng bằng GNS3

Tối ưu tốc độ di chuyển tác tử di động sử dụng Tác tử di động

- MapReduce Module Unit: Xem xét một hệ thống bao gồm một tập hợp các *ứng dụng phân tán* N A = *A1, A2, ..., AN* chạy trên một tập hợp các nút thợ M (quy trình cảm biến) *W = W1, W2, ..., WM.* Mỗi ứng dụng phân tán *Aj* được biểu diễn dưới dạng biểu đồ dòng chảy (thể hiện trong Hình 2.12) bao gồm một số tác vụ ánh xạ (T^{jap}) và một số tác vụ giảm ($T^{jreduce}$) thực hiện song song trên nhiều nút thợ. Ngoài ra, mỗi ứng dụng A_j có thời hạn $Deadline_j$, là khoảng thời gian, bắt đầu từ thời điểm ứng dụng được gửi đến hệ thống, trong đó ứng dụng sẽ hoàn thành [60].



Hình 2.11: Thuật toán giảm xử lý dữ liệu cảm biến bằng cách sử dụng MapReduce

2.4. Đánh giá hiệu năng khi áp dụng mô hình tác tử di động trong quản lý mạng

2.4.1 Tính chi phí quản lý mạng

Để tính toán chi phí của mô hình CNMMA sử dụng tác tử di động để quản lý mạng, chi phí sau những cân nhắc tính toán đã được tính đến.

2.4.2. Chi phí quản lý mạng cho mô hình Client/Server (C/S) tập trung dựa trên SNMP

Đối với mô hình quản lý mạng dựa trên mô hình Máy chủ khách, chi phí của n thiết bị mạng thăm dò là:

$$C_{c/s} = \sum_{i=0}^{n} K_{0,i} * \left(S_{yêu\ cầu} + S_{hồi\ đáp}\right) \quad (2.1)$$

Trong đó,

- $K_{0,i}$: Hệ số chi phí của liên kết từ trình quản lý (vị trí 0) đến thiết bị thứ i.
- $S_{yêu\ cầu}$: Kích thước gói tin yêu cầu SNMP.
- $S_{hồi\ đáp}$: Kích thước gói tin phản hồi SNMP.

Nếu p là số lần thăm dò nốt mạng được thực hiện trong một khoảng thời gian, chẳng hạn như một giờ, sau đó tính chi phí quản lý mạng cho việc đó thì chi phí khoảng thời gian là:

$$C_{c/s} = \left(\sum_{i=0}^{n} \quad K_{0,i} * \left(S_{yêu\ cầu} + S_{hồi\ đáp}\right)\right) * p \qquad (2.2)$$

2.4.3 Chi phí quản lý mạng cho quản lý tác tử di động

Đối với mô hình quản lý mạng dựa trên Tác tử di động [97] chi phí một lần di chuyển tác tử qua mạng gồm N+1 nút (với N0 đóng vai trò là nút quản lý trung tâm) là:

$$C_{MA} = \left(\sum_{i=0}^{N-1} \quad K_{i,i+1} * (S_{MA} + i * D)\right) + K_{N,0} * (S_{MA} + N * D) \quad (2.3)$$

Trong đó:

- $K_{i,j}$: Hệ số chi phí của liên kết giữa nút i và j.
- S_{MA}: Kích thước của tác tử di động.
- D: Kích thước thông tin thu thập của Tác tử di động tại mỗi nút.

Nếu p là số lần thăm dò được thực hiện trong một khoảng thời gian để quản lý mạng thì chi phí quản lý cho khoảng thời gian đó là:

$$C_{MA} = \left\{\left(\sum_{i=0}^{N-1} \quad K_{i,i+1} * (S_{MA} + i * D)\right) + K_{N,0} * (S_{MA} + N * D)\right\} * p \quad (2.4)$$

2.4.4 Chi phí quản lý mạng cho mô hình CNMMA

Tổng chi phí:

$$C_{CNMMA} = C_{CNMMAD} + C_{CNNMAP} \qquad (2.5)$$

Trong đó:

- C_{CNMMAD}: Chi phí khám phá mạng và triển khai các trình quản lý.
- C_{CNMMAP}: Chi phí thăm dò để kiểm tra trạng thái mạng ở cấp cao nhất.

- Chi phí triển khai ban đầu từ cấp quản lý cao nhất (được coi là điểm khởi đầu để khám phá mạng):

$$C_{MA} = \sum_{k} \quad \left(\frac{L}{h=1}\right) \sum_{i=0}^{M-1} \quad F_{h,j} * S_{MA} \qquad (2.6)$$

- Chi phí thăm dò:

$$C_{MA} = \sum_k \left(\frac{L}{h=1}\right) \sum_{i=0}^{M-1} F_{h,j}\,(MA_{yêu\ cầu}) + \sum_{j=1}^{Q} C_Q \quad (2.7)$$

- *Chi phí theo mô hình phẳng cho miền thứ Q*

  $C_Q = MDA_s * (R_Q + 1) * K_Q$ (2.8)

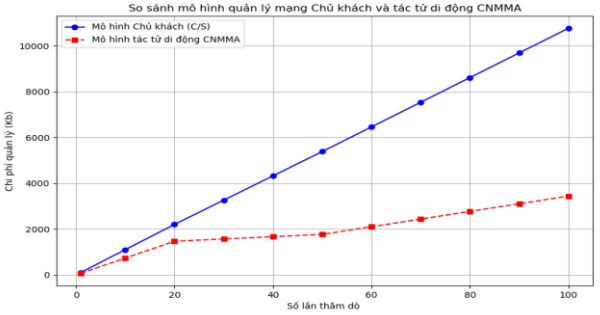
- MDA_s: Kích thước của Tác tử di động
- R_Q: Số nút được quản lý trong miền Q.
- K_Q: Hệ số chi phí liên kết của miền Q.

Nếu thăm dò p lần trong một khoảng thời gian:

$C_{CNMMA} = (C_{CNMMAD} + C_{CNMMAP}) * p$ (2.9)

2.5 So sánh và đánh giá giá chi phí mạng

Để tính toán chi phí quản lý mạng cần định nghĩa các tham số sau để so sánh và đánh giá chi phí quản lý mạng



Hình 2.14: Biểu đồ so sánh chi phí quản lý mạng

Kết luận:

Chi phí quản lý mạng sử dụng Tác tử di động tiết kiệm chi phí hơn so với mô hình Chủ khách, đặc biệt chi phí sẽ giảm và hiệu quả hơn nếu số lượt thăm dò lớn.

CHƯƠNG 3: NÂNG CAO AN TOÀN BẢO MẬT CHO TÁC TỬ DI ĐỘNG

3.1 Nguy cơ bảo mật trên công nghệ tác tử di động

Mối đe doạ về an toàn bảo mật có thê được phân ra thành 4 hạng mục cơ bản sau:

1. Tác tử tới nền tảng (**Agent to Platform)**: Hạng mục này liên quan đến mối đe doạ của tác tử tới một nền tảng cụ thể.

2. Nền tảng tới tác tử (**Platform to Agent):** Hạng mục này liên quan đến mối đe doạ nền tảng tới tác tử

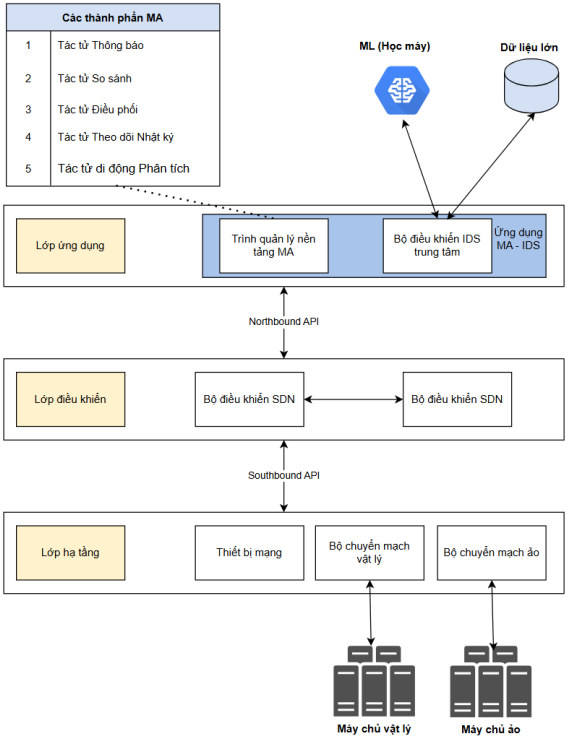
3. Tác tử tới tác tử (**Agent to Agent):** Hạng mục này liên quan đến mối đe doạ giữa các tác tử với nhau

4. Nền tảng tới nền tảng (**Platform to Platform):** Hạng mục này liên quan đến mối de doạ giữa các nền tảng chứa các tác tử di động.

3.7 Đề xuất mô hình Khung hệ thống phát hiện xâm nhập phân tán tác tử di động (MA-DIDS)

Một mô hình mới cho các hệ thống phát hiện xâm nhập là việc triển khai MA trong các hệ thống mạng SDN.

IDS - CC và MAP Manager tạo thành hai phần chính của Khung hệ thống phát hiện xâm nhập phân tán tác tử di động (MA-DIDS) được đề xuất, như được mô tả trong hình dưới đây.



Hình 3.2: Khung hệ thống phát hiện xâm nhập phân tán tác tử di động (MA-DIDS) trong SDN.

Tổng quan kiến trúc khung hệ thống phát hiện xâm nhập

Kiến trúc hệ thống gồm 3 lớp trên nền tảng kiến trúc SDN tiêu chuẩn gồm 3 lớp riêng biệt:

- Lớp hạ tầng: là lớp vật lý và ảo hóa, bao gồm các máy chủ vật lý, máy chủ ảo, cùng với các thiết bị mạng như thiết bị chuyển mạch vật lý và ảo hoá. Lớp này là nền tảng thực thi các yêu cầu từ lớp trên.
- Lớp điều khiển: là bộ não của mạng, chứa thành phần trọng tâm là Bộ điều khiển SDN (SDN Controller), giao tiếp với lớp hạ tầng

thông qua giao diện lập trình ứng dụng hướng nam (Southbound API) để cấu hình và điều khiển luồng dữ liệu mạng. Đồng thời, nó cung cấp giao diện hướng bắc (Northbound API) để lớp ứng dụng có thể ra quyết định và gửi yêu cầu xuống.

- Lớp ứng dụng: là lớp cao nhất, nơi chứa logic nghiệp vụ và các ứng dụng thông minh. Đối với kiến trúc này, đây chính là nơi hệ thống MA-IDS hoạt động.

Phân tích chi tiết các thành phần chính

Hệ thống Tác tử di động (Mobile Agent - MA)

- Đây là hạt nhân độc đáo của kiến trúc, giúp hệ thống trở nên linh hoạt và chủ động. Thay vì một hệ thống giám sát tập trung và bị động, các tác tử là những chương trình nhỏ, có khả năng tự di chuyển qua các nút mạng để thu thập thông tin và thực thi nhiệm vụ.
- MA Platform Manager (Trình quản lý Nền tảng Tác tử): Là môi trường để quản lý vòng đời của các tác tử, bao gồm việc tạo, triển khai, điều phối và hủy bỏ chúng.

Các thành phần của Tác tử Di động (MA Components)

- Log Tracking Agent (LTA - Tác tử Theo dõi Nhật ký): Nhiệm vụ chính là di chuyển đến các máy chủ ảo (VM) để thu thập nhật ký hệ thống (system logs), thông tin về các hoạt động mạng và sự kiện hệ điều hành. Sau đó, nó báo cáo dữ liệu này về Trung tâm Điều khiển IDS.
- Analysis Mobile Agent (Tác tử Di động Phân tích): Tác tử này nhận dữ liệu thô từ LTA để thực hiện phân tích sơ bộ, lọc nhiễu và tìm kiếm các dấu hiệu bất thường ban đầu.
- Comparator Agent (Tác tử So sánh): So sánh các hoạt động đáng ngờ đã được phát hiện với cơ sở dữ liệu mẫu xâm nhập đã

biết. Nếu có sự trùng khớp, nó sẽ xác nhận đây là một cuộc tấn công đã biết.

- Mobile Agent Coordinator (Tác tử Điều phối): Là chỉ huy trưởng của các tác tử khác. Nó chịu trách nhiệm điều phối hoạt động, gửi các tác tử đến đúng vị trí cần thiết và đảm bảo luồng xử lý thông tin diễn ra một cách chính xác.
- Notify Agent (Tác tử Thông báo): Khi một cuộc tấn công được xác nhận (bởi Comparator Agent hoặc bởi mô hình Học máy), tác tử này sẽ được kích hoạt để gửi cảnh báo ngay lập tức đến quản trị viên hệ thống thông qua ứng dụng MA-IDS.

Trung tâm Điều khiển IDS

- Đây là trung tâm thần kinh của toàn bộ hệ thống an ninh, nơi hội tụ thông tin và ra quyết định.
- Chức năng: Nhận toàn bộ dữ liệu từ MA Platform Manager (do các tác tử báo cáo về) và kết quả phân tích từ khối Học máy.
- MA-IDS App: Là ứng dụng giao diện cho quản trị viên, hiển thị các cảnh báo, trạng thái hệ thống, và cho phép họ tương tác, điều tra các sự cố.
- Quản lý trạng thái: Trung tâm Điều khiển IDS chịu trách nhiệm cập nhật và duy trì trạng thái của từng máy ảo trong mạng.

Cơ sở dữ liệu & Dữ liệu lớn (Database & Big Data)

Hệ thống cần một kho dữ liệu lớn để lưu trữ và phân tích, bao gồm nhiều cơ sở dữ liệu với các chức năng riêng biệt:

- Cơ sở dữ liệu mẫu xâm nhập: Đây là cơ sở dữ liệu chứa các "chữ ký" (signatures) hoặc mẫu của các cuộc tấn công đã biết. Notify Agent và Comparator Agent sử dụng dữ liệu này để so sánh và xác định các mối đe dọa quen thuộc.
- Cơ sở dữ liệu sự kiện: Toàn bộ nhật ký hệ thống và các sự kiện do Log Tracking Agent (LTA) báo cáo về được lưu trữ tại đây

dưới dạng Dữ liệu lớn (Big Data). Đây là nguồn dữ liệu đầu vào cho khối Học máy.

- Cơ sở dữ liệu trạng thái máy ảo: Được cập nhật bởi Trung tâm điều khiển IDS, cơ sở dữ liệu này theo dõi trạng thái của mỗi máy ảo, có thể ở một trong ba trạng thái: bình thường (normal), bị xâm phạm (compromised), hoặc đang di chuyển (migrated).

Học máy & Khai thác dữ liệu (Machine Learning & Data Mining)

- Module này cung cấp trí thông minh để phát hiện các mối đe dọa mới, chưa từng được biết đến (zero-day attacks) dựa trên các hành vi bất thường.
- Cơ chế hoạt động: Mô hình học máy được áp dụng trên tập dữ liệu lớn bao gồm các cuộc tấn công đã được phát hiện trước đây, nhật ký hệ thống và dữ liệu do LTA thu thập. Từ đó, mô hình sẽ "học" được thế nào là hành vi "bình thường" của mạng. Bất kỳ hoạt động nào lệch khỏi trạng thái bình thường này sẽ bị coi là đáng ngờ.
- Đào tạo mô hình: Các nhà khoa học dữ liệu sử dụng các bộ dữ liệu công khai có sẵn để đào tạo mô hình. Một trong những bộ dữ liệu phổ biến nhất cho việc phát hiện xâm nhập dựa trên sự bất thường là NSL-KDD. Đây là phiên bản cải tiến của bộ dữ liệu KDD99, bao gồm các loại tấn công điển hình như:

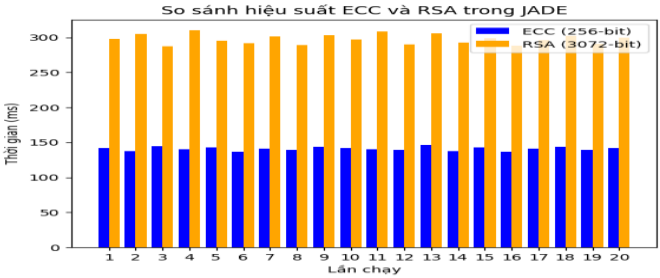
+ DoS (Denial of Service): Tấn công từ chối dịch vụ.
+ Probe: Tấn công thăm dò, quét cổng.
+ U2R (User to Root): Tấn công leo thang đặc quyền từ người dùng thường lên quản trị viên.
+ R2L (Remote to Local): Tấn công truy cập từ xa vào máy cục bộ.

3.9 Đánh giá thử nghiệm so sánh hiệu suất giữa mã hoá truyền tin nền tảng Tác tử di động sử dụng thuật toán ECC và RSA

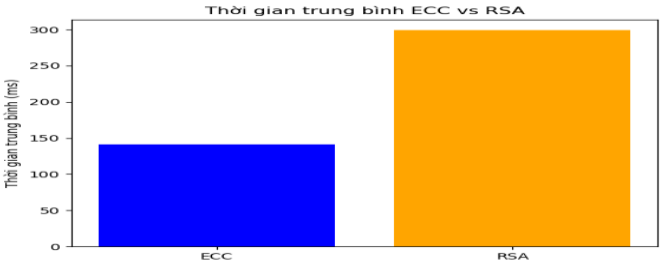
3.9.1 Bộ dữ liệu thử nghiệm

Dữ liệu thời gian (đơn vị: milliseconds) được thu thập từ 20 lần chạy cho mỗi cài đặt thuật toán ECC và RSA và số lượng gửi 1000 bản tin.

Biểu đồ so sánh hiệu suất mã hoá truyền tin nền tảng Tác tử di động sử dụng thuật toán ECC và RSA như Hình 3.4.



Hình 3.3: Biểu đồ so sánh hiệu suất ECC và RSA trong môi trường Tác tử di động



Hình 3.4: Thời gian trung bình giữa ECC và RSA

So sánh hiệu suất:

- **Tỷ lệ:** $RSA/ECC = \frac{\text{RSA}}{\text{ECC}} = \frac{298{,}55}{140{,}95} \approx 2{,}12$

- ECC nhanh hơn RSA khoảng 2,12 lần trong thử nghiệm.

3.11 Đánh giá thử nghiệm so sánh giữa Baseline IDS và MA-DIDS

3.11.2 Các bộ thực nghiệm

- Thực nghiệm 1: Đánh giá độ chính xác phát hiện (True Positive Rate & False Positive Rate).

- Mục tiêu: Xác định khả năng phát hiện chính xác và tỉ lệ cảnh báo sai của hai hệ thống Baseline IDS và MA-DIDS.

- Cách cài đặt: Mỗi hệ thống được chạy 30 lần, thời gian mỗi lần 5 giây. Dữ liệu tấn công và bình thường được trộn ngẫu nhiên để đảm bảo độ tin cậy 95%. Các chỉ số thu thập: True Positive Rate (TPR), False Positive Rate (FPR).

Bảng 3.12: Bảng số liệu so sánh đánh giá độ chính xác phát hiện tấn công xâm nhập giữa Baseline IDS và MA-DIDS

Chỉ số	Baseline	MA-DIDS	Cải thiện
True Positive Rate	99,2%	99,3%	0,2%
False Positive Rate	41,7%	15,6%	-62,7%

- Phân tích: MA-DIDS gần như giữ nguyên TPR nhưng giảm mạnh FPR tới 62,7%. Điều này chứng tỏ hệ thống MA-DIDS có khả năng lọc nhiễu tốt hơn, hạn chế cảnh báo sai.

- Kết luận: MA-DIDS có hiệu quả vượt trội về độ chính xác, đặc biệt trong việc giảm cảnh báo sai so với Baseline.

Thực nghiệm 2: Đánh giá độ tin cậy phân loại (Precision & F1-Score)

- Mục tiêu: So sánh khả năng phân loại đúng và cân bằng giữa độ chính xác và độ bao phủ của hai mô hình.

- Cách cài đặt: Sử dụng cùng tập dữ liệu kiểm thử với 30 mẫu. Đo các chỉ số: Precision, F1-Score (trung bình 30 lần).

Bảng 3.13: Bảng số liệu so sánh đánh giá độ tin cậy phân loại giữa Baseline IDS và MA-DIDS

Chỉ số	Baseline	MA-DIDS	Cải thiện
Precision	85,4%	95,6%	11,8%
F1-Score	90,7%	97,1%	7,0%

- Phân tích: MA-DIDS cải thiện Precision đáng kể (+11,8%), cho thấy ít cảnh báo sai hơn. F1-Score tăng 7% thể hiện sự cân bằng giữa độ chính xác và độ bao phủ.

- Kết luận: Hệ thống MA-DIDS đáng tin cậy hơn trong việc phân loại đúng các tấn công và giảm lỗi cảnh báo.

Thực nghiệm 3: Đánh giá hiệu suất hệ thống (Thời gian, CPU, Memory, Thread)

- Mục tiêu: So sánh mức tiêu thụ tài nguyên và tốc độ phản hồi của hai hệ thống.

- Cách cài đặt: Cùng cấu hình phần cứng, mỗi test chạy 5 giây × 30 lần. Đo các chỉ số: thời gian phát hiện, sử dụng CPU, Memory, và Thread count.

Bảng 3.14: Bảng số liệu so sánh đánh giá hiệu suất giữa Baseline IDS và MA-DIDS

Chỉ số	**Baseline**	**MA-DIDS**	**Chênh lệch**
Detection Time	16,6 ms	40,8 ms	+146,3%
Memory Usage	28,0%	38,5%	+37,4%
CPU Usage	46,9%	92,5%	+97,1%
Thread Count	5,5	27,9	+411,6%

- Phân tích: MA-DIDS tiêu tốn nhiều tài nguyên hơn do cơ chế tác tử di động phân tán (do overhead của nền tảng). Thời gian phát hiện chậm hơn do nhiều bước xử lý hợp tác giữa các tác tử.

- Kết luận: MA-DIDS phù hợp cho môi trường có tài nguyên mạnh, và đòi hỏi độ chính xác cao và phân tích sâu trong khi Baseline IDS vẫn đáp ứng cho hệ thống giới hạn tài nguyên

KẾT LUẬN

Luận án tập trung vào việc giải quyết hai vấn đề chính để xây dựng một giải pháp quản trị mạng cục bộ trong quá trình di chuyển lên mạng đám mây một cách an toàn, dựa trên công nghệ tác tử.

Vấn đề thứ nhất được giải quyết thông qua việc đề xuất một kiến trúc kết hợp hai chuẩn quản trị mạng phổ biến là SNMP (Simple Network Management Protocol) và CMIP (Common Management Information Protocol). SNMP được sử dụng để quản lý các thiết bị mạng đơn giản và thực hiện các tác vụ cơ bản, trong khi CMIP được áp dụng cho các hệ thống phức tạp yêu cầu tính bảo mật cao. Một lớp trung gian (middleware) được triển khai để tích hợp hai giao thức này, đảm bảo tính tương thích và hiệu quả trong quá trình quản trị mạng. Đồng thời, đề xuất mô hình quản lý mạng ứng dụng Công nghệ tác tử di động.

Vấn đề thứ hai liên quan đến việc tăng cường tính an toàn cho công nghệ tác tử nguồn mở. Giải pháp đề xuất bao gồm mã hóa dữ liệu bằng các thuật toán ECC thay thế cho thuật toán AES và RSA, xác thực và quản lý danh tính thông qua PKI cho nền tảng tác tử di động, và tích hợp hệ thống giám sát và phát hiện xâm nhập (IDS) ứng dụng tác tử di động để thực hiện cập nhật

và vá lỗi tự động, cũng như áp dụng cơ chế quản lý quyền truy cập dựa trên vai trò (RBAC). Kết quả là một hệ thống quản trị mạng linh hoạt, an toàn, phù hợp với xu hướng chuyển đổi số và di chuyển lên Cloud hiện nay.

Tác tử di động là một hướng nghiên cứu công nghệ mới, và được thừa nhận rộng rãi và ngay lập tức đã thu hút sự quan tâm ngày càng lớn của giới nghiên cứu cũng như giới công nghiệp trong lĩnh vực Công Nghệ Thông Tin. Trong thập kỉ đầu của thế kỷ 21, đây là khoảng thời gian bùng nổ trong lĩnh vực nghiên cứu về công nghệ tác tử nói chung và tác tử di động nói riêng, rất nhiều bộ khung tác tử được phát triển, các chuẩn về tác tử cũng được xây dựng và phát hành. Lĩnh vực nghiên cứu công nghệ tác tử rất rộng từ những lĩnh vực có thể áp dụng ngay trong thực tiễn như điện toán di động, tài liệu động, lấy dữ liệu từ xa, quản trị hệ thống mạng…cho đến những lĩnh vực mới như điện toán đám mây, điện toán môi trường bao quanh.

Mặc dù, trong lĩnh vực nghiên cứu công nghệ tác tử thu được thành tựu lớn và quan trọng nhưng việc áp dụng công nghệ vào trong thực tiễn vẫn còn ít, chưa có nhiều phần mềm ứng dụng công nghệ tác tử nổi bật bởi các ứng dụng truyền thống (theo mô hình máy trạm/máy chủ). Nguyên nhân của tình trạng trên là sự lo ngại về công nghệ mới, tính an toàn và bảo mật của công nghệ tác tử cũng cần phải được xem xét và phát triển hơn nữa.

Do vậy, việc nghiên cứu và làm chủ công nghệ tác tử là một vấn đề rất quan trọng nói chung và trong việc xây dựng hệ thống quản lý mạng và hứa hẹn sẽ là bước đột phá trong việc xây dựng mô hình quản lý mạng cho hệ thống mạng và điện toán đám mây hiện nay. Mặt khác, ngoài việc làm chủ công nghệ tác tử thì môi trường tác tử, khung ứng dụng để triển khai tác tử và sự đảm

bảo tính an toàn bảo mật cho hệ thống tác tử là một vấn đề trọng yếu để đưa công nghệ tác tử vào triển khai trong thực tế.

Kết quả chính của luận án:

Thứ nhất, nghiên cứu và đưa ra bộ điều hợp cho phép kết hợp cả 2 giao thức SNMP và CMIP cũng như đưa bộ kết nối này vào 2 giao thức này vào ứng dụng trong nền tảng tác tử di động và đề xuất mô hình quản lý mạng cho mạng cục bộ và đám mây sử dụng nền tảng tác tử di động là Mô hình CNMMA giúp quản lý hiệu quả lưu lượng đám mây với tiết kiệm chi phí, băng thông mạng hơn và cung cấp giải pháp bảo mật cho việc quản lý mạng.

Thứ hai, đề xuất các phương thức nâng cao an toàn bảo mật nền tảng tác tử di động qua sử dụng thuật toán mã hoá nhỏ gọn và đơn giản hơn và đề xuất xây dựng mô hình bộ Khung phát hiện xâm nhập hệ thống mạng dựa trên nền tảng Tác tử di động.

Hướng phát triển của luận án:

Thứ nhất, tiếp tục mở rộng, nghiên cứu nâng cao an toàn bảo mật và cải tiến kỹ thuật cho nền tảng tác tử di động để có thể ứng dụng các tác tử di động vào trong thực tế.

Thứ hai, nghiên cứu và ứng dụng Trí tuệ nhân tạo vào nền tảng tác tử di động như cải tiến về thuật toán tối ưu, và dò tìm vị trí của tác tử di động, quản lý mạng cục bộ và đám mây tự động.

DANH MỤC CÔNG TRÌNH TÁC GIẢ ĐÃ CÔNG BỐ

[CT1]. Nguyen Minh Phuc, Nguyen Ai Viet, Tran Quy Nam, Cloud network management model based on Mobile Agent, Proceeding of Conference FAIR 2020, DOI: 10.15625/vap.2020.00150, (2020).

[CT2]. Nguyen Minh Phuc, Nguyen Ai Viet, Tran Quy Nam, Enhanced security and performance of the Smart Traffic Management System VNSMAPS by using Mobile Agent and Map Reduce, Proceeding of Conference FAIR 2021, DOI: 10.15625/vap.2021.0100, (2021).

[CT3]. Nguyen Minh Phuc; Nguyen Ai Viet; Tran Quy Nam; Long Cu Kim; Vijender Kumar Solanki, "Enhanced SDN Security Using Mobile Agent" in Creative Approaches Towards Development of Computing and Multidisciplinary IT Solutions for Society, Wiley, 2024, pp.25-36, doi: 10.1002/9781394272303.ch3

[CT4]. Nguyen Minh Phuc, Nguyen Ai Viet, Tran Quy Nam, Integration of SNMP and CMIP protocol for Mobile Agent in LAN and Cloud Network Management, (2024), The International Scientific Journal Current Research # 45 (227), November 2024, International Scientific Journal Actual Research (apni.ru), ISSN 2713-1513.

[CT5]. Nguyen Minh Phuc, Nguyen Ai Viet, Tran Quy Nam, CNNMA model for enhancing security and network performance in LAN and Cloud Network Management, (2025), The International Scientific Journal Current Research #1 (287), December 2025, International Scientific Journal Actual Research (apni.ru), ISSN 2713-1513.