HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Nguyễn Thị Kiều Diễm

GIẢI PHÁP XÁC THỰC DỰA TRÊN ĐỊNH DANH CHO CÁC AGENT TRONG HỆ THỐNG GIÁM SÁT MẠNG

CHUYÊN NGÀNH : HỆ THỐNG THÔNG TIN

MÃ SỐ: 8.48.01.04

TÓM TẮT LUẬN VĂN THẠC SĨ KỸ THUẬT

HÀ NỘI – 2019

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: PGS.TSKH. Hoàng Đăng Hải

Phản biện 1:……..

Phản biện 2: …….

Luận văn này sẽ được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc:…….giờ……ngày…..tháng…….năm……

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông

LỜI CẢM ƠN

Lời đầu tiên tôi xin gửi lời cảm ơn chân thành nhất đến thầy PGS. TSKH. Hoàng Đăng Hải đã tận tình chỉ bảo, hướng dẫn tôi trong suốt quá trình thực hiện luận văn này.

Tôi xin chân thành cảm ơn các thầy cô giáo đã giảng dạy và giúp đỡ tôi trong suốt thời gian học chương trình cao học. Các thầy cô đã trang bị cho tôi những kiến thức quý báu để làm hành trang cho tôi ứng dụng vào công việc hiện tại cũng như tương lai.

Tôi cũng xin gửi lời cảm ơn chân thành đến các bạn đồng môn, gia đình, bạn bè đã luôn ủng hộ, động viên, giúp đỡ và tạo điều kiện tốt cho tôi vượt qua những khó khăn để hoàn thành luận văn này.

LỜI CAM ĐOAN

Tôi xin cam đoan những vấn đề được trình bày trong luận văn "*Giải pháp xác thực dựa trên định danh cho các Agent trong hệ thống giám sát mạng*" là do sự tìm hiểu của cá nhân dưới sự hướng dẫn của **PGS. TSKH. Hoàng Đăng Hải**.

Tất cả những tham khảo từ các nghiên cứu liên quan đều được trích dẫn, nêu rõ nguồn gốc một cách rõ ràng từ danh mục tài liệu tham khảo trong luận văn. Trong luận văn này, tôi cam doan không sao chép nguyên bản tài liệu, công trình nghiên cứu của người khác mà không chỉ rõ về tài liệu tham khảo.

Hà Nội, ngày 01tháng 12 năm 2019

Tác giả luận văn

Nguyễn Thị Kiều Diễm

MỤC LỤC

MỞ ĐẦU

1. Lý do chọn đề tài:

Giám sát mạng là một nhu cầu thực tế của các nhà mạng. Trong một hệ thống giám sát mạng tập trung, các Agent (là các máy trinh sát) làm nhiệm vụ thu thập thông tin về tình trạng hoạt động của các thiết bị, mạng rồi chuyển về trung tâm giám sát để xử lý, phân tích, đưa ra cảnh báo về các nguy cơ tấn công, sự cố, lỗi,…

Một vấn đề thường đặt ra là các Agent có thực sự là thành viên của hệ thống giám sát hay không? Do vậy, một yêu cầu đặt ra là cần nghiên cứu giải pháp xác thực các Agent cho hệ thống giám sát mạng, nhằm xác định đúng Agent hợp pháp để cho phép truyền tin và cô lập Agent giả mạo.

2. Tổng quan về vấn đề nghiên cứu*:*

Cho đến nay, đã có nhiều kiến trúc hệ thống giám sát mạng tập trung ra đời. Kiến trúc chung của các hệ thống này thường gồm hai phần chính: 1) Các bộ thu thập dữ liệu thường được đặt tại vị trí giám sát hay tại đối tượng giám sát, 2) Bộ giám sát xử lý tập trung đặt tại trung tâm giám sát. Các Agent có thể là một thiết bị đặt tại đối tượng cần giám sát, hoặc một phần mềm được cài đặt trên đối tượng giám sát. Phạm vi bài luận văn xem xét các Agent dưới dạng một nút mạng trinh sát (thiết bị).

3. Mục đích nghiên cứu:

Xây dựng giải pháp xác thực dựa trên định danh cho các Agent trong hệ thống giám sát mạng tập trung với các mục đích cụ thể gồm:

- Xây dựng mô hình kiến trúc mạng giám sát phục vụ nghiên cứu giải pháp.
- Nghiên cứu phương pháp định danh cho các Agent.
- Nghiên cứu phương pháp xác thực cho các Agent.
- Xây dựng giải pháp xác thực dựa trên mã hóa định danh cho các Agent.
- Xây dựng cơ chế truyền tin bảo mật từ các Agent về trung tâm giám sát.

4. Đối tượng và phạm vi nghiên cứu:

Bài toán xác thực dựa trên định danh cho các agent trong hệ thống giám sát mạng. Đối tượng nghiên cứu là phương pháp xác thực, định danh, xác thực dựa trên định danh.

Phạm vi nghiên cứu: áp dụng cho xác thực các Agent trong một kiến trúc hệ thống giám sát tự xây dựng.

5. Phương pháp nghiên cứu:

- Nghiên cứu lý thuyết về hệ thống giám sát, vấn đề định danh, xác thực, mã hóa, các hệ mật mã phục vụ xác thực.
- Nghiên cứu các giải pháp, thuật toán, phương pháp liên quan đến định danh, xác thực qua khảo sát các tài liệu và công trình nghiên cứu trên thế giới và Việt Nam.
- Nghiên cứu về môi trường mô phỏng thử nghiệm.
- Thực hiện mô phỏng thử nghiệm cho giải pháp đưa ra.

Chương 1 - CƠ SỞ LÝ THUYẾT

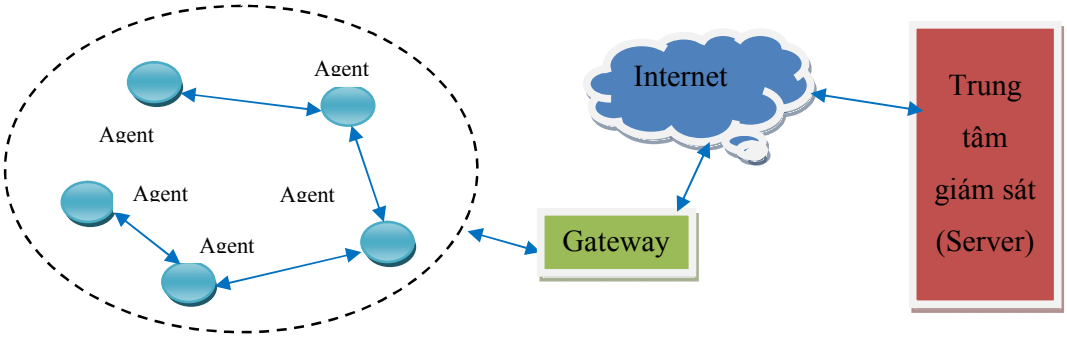
1.1. Giới thiệu chương

Chương này trình bày cơ sở lý thuyết về hệ thống giám sát mạng tập trung, các yêu cầu bảo mật, xác thực cho các Agent, phương pháp định danh, phương pháp xác thực, phương pháp mã hóa.

1.2. Giới thiệu chung về hệ thống giám sát mạng tập trung

Kiến trúc chung của các hệ thống theo dõi, giám sát mạng tập trung thường gồm hai phần chính: 1) Các bộ thu thập dữ liệu thường được đặt tại vị trí giám sát hay tại đối tượng giám sát, 2) Bộ giám sát xử lý tập trung đặt tại trung tâm giám sát [3]. Nhiệm vụ chính của các hệ thống theo dõi, giám sát là bảo vệ cho một hệ thống máy tính dựa trên việc phát hiện các dấu hiệu tấn công và đưa ra cảnh báo.

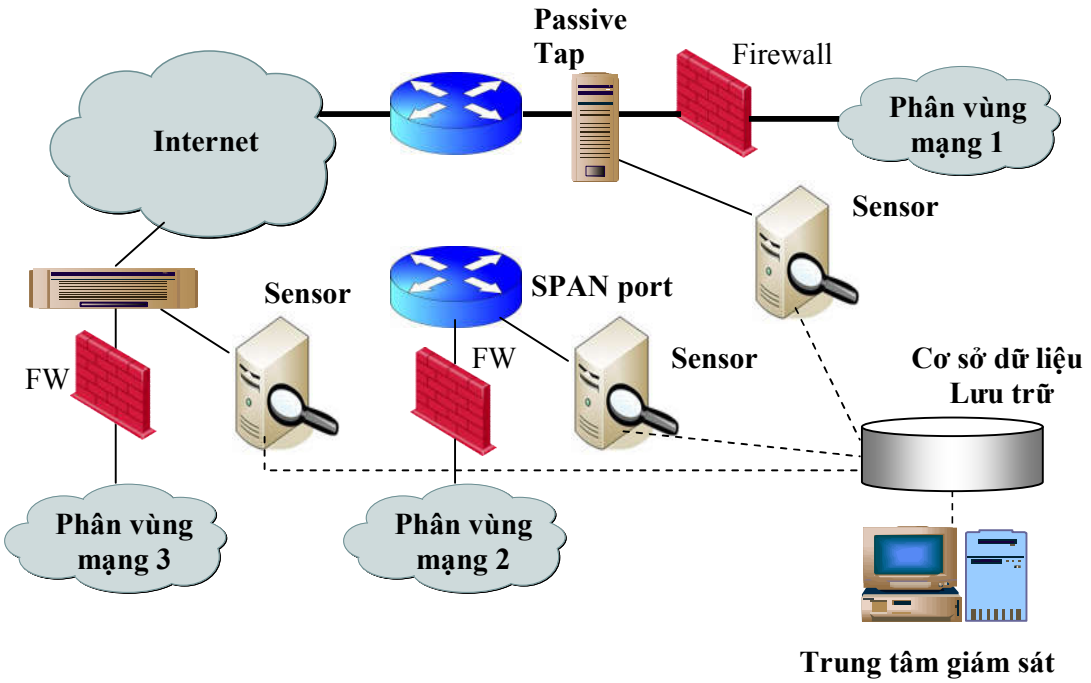
Các Agent có thể là một thiết bị đặt tại đối tượng cần giám sát, hoặc một phần mềm được cài đặt trên đối tượng giám sát.



Hình 1.2. Kiến trúc hệ thống giám sát mạng tập trung

Hình 1.2 là sơ đồ kiến trúc tổng quát của một hệ thống giám sát mạng với các Agent và trung tâm giám sát. Các Agent làm nhiệm vụ thu thập dữ liệu liên quan đến hoạt động của các đối tượng được giám sát (máy chủ Web, máy chủ, máy trạm, router), các sự

kiện tấn công và truyền về trung tâm giám sát. Hệ thống giám sát ở trung tâm làm nhiệm vụ: phân tích, phát hiện, cảnh báo và thống kê sự cố.



Hình 1.3. Kiến trúc hệ thống giám sát mạng tập trung cho nhiều phân vùng mạng

Hình 1.3. là một ví dụ về một hệ thống giám sát tập trung cho ba phân vùng mạng kết nối thông qua Internet với các bộ thu thập thông tin Sensor cài đặt tại các thiết bị (Phân vùng mạng 3), hoặc lấy dữ liệu trích xuất từ các cổng SPAN port của các bộ định tuyến (Phân vùng mạng 1 và 2).

1.3. Yêu cầu bảo mật, xác thực cho các Agent.

Trong một hệ thống giám sát mạng tập trung, các Agent (là các máy trinh sát) làm nhiệm vụ thu thập thông tin về tình trạng hoạt động của các thiết bị và mạng. Các thông tin thu thập được chuyển về trung tâm giám sát để xử lý, phân tích, đưa ra cảnh báo về các nguy cơ tấn công, sự cố, lỗi.

Câu hỏi đặt ra là các Agent có thực sự là thành viên của hệ thống giám sát hay không? Do vậy, cần đưa ra giải pháp xác thực Agent để phân biệt giả mạo. Phương pháp xác thực dựa trên định danh được đề xuất, có thể áp dụng cho Agent trong các mạng cảm biến không dây, mạng peer-to-peer, hoặc cho điện toán đám mây.

1.4. Phương pháp định danh (Identification)

Khái niệm về định danh: Người dùng cung cấp danh định của mình cho hệ thống.

Trong khoa học máy tính, định danh có thể là các mã dùng để đặt tên cho các thực thể (ID).

Mục đích của việc định danh: Xác định định danh cũng tương tự như việc xác định một "vật thể", nghĩa là tìm kiếm sự tồn tại và quyền hạn của vật thể, hoặc quyền hạn của người dùng đối với vật thể đó.

Về phương pháp xác định định danh: Có hai phương pháp điển hình nhất [18], đó là:

+ Phương pháp khai báo: Người dùng tự nhập thông tin về danh định (khai báo định danh).

+ Phương pháp sử dụng danh định số hóa: Phương pháp này khá phổ biến với việc sử dụng các dữ liệu số hóa thu được từ đối tượng.

- Danh định sinh trắc học (Biometric identity) có thể gồm: Dữ liệu nhận dạng khuôn mặt, dữ liệu Quét tròng mắt,dữ liệu hình học bàn tay, dữ liệu nhận dạng vân tay
- Danh định máy tính, thiết bị (Computer identity) bao gồm:Tên máy tính, tên thiết bị, địa chỉ MAC, địa chỉ IP
- Danh định số (Digital identity) gồm: Chứng nhận số, thẻ thông minh (Smart card)

1.5. Phương pháp xác thực

Khái niệm về xác thực: Người dùng cung cấp bằng chứng là danh định đó là đúng và phù hợp với mình.

Các phương pháp xác thực: Các phương pháp xác thực có thể được chia làm 3 loại chính, dữ trên cơ sở những dữ liệu sử dụng cho việc xác thực: 1) Những gì bạn biết, 2) Những gì bạn có, 3) Những gì thuộc về bạn.

+ Những gì bạn biết (Something you know):

+ Những gì bạn có (Something you have)

+ Những gì là chính bạn (Something you are):

+ Có thể kế hợp các phương pháp xác thực với nhau (2/3 phương pháp trên).

Một phương pháp xác thực tốt là phương pháp mà không dễ bị đoán hoặc bị làm giả

1.6. Phương pháp mã hóa (bí mật, công khai), các hệ mật mã

Để bảo mật thông tin trên đường truyền người ta sử dụng các phương pháp mã hoá. Dữ liệu bị biến đổi từ dạng nhận thức được sang dạng không nhận thức được theo một thuật toán nào đó và sẽ được biến đổi ngược lại ở trạm nhận (giải mã).

1.6.1. Phương pháp mã hóa bí mật (đối xứng)

- Mã hóa đối xứng là phương pháp mã hóa mà key mã hóa và key giải mã là như nhau (Sử dụng cùng một secret key để mã hóa và giải mã). Đây là phương pháp thông dụng

nhất hiện nay dùng để mã hóa dữ liệu truyền nhận giữa hai bên. Để thực hiện mã hóa thông tin giữa hai bên thì:

+ Đầu tiên bên gửi và bên nhận bằng cách nào đó sẽ phải thóa thuận secret key (khóa bí mật) được dùng để mã hóa và giải mã. .

+ Sau đó bên gửi sẽ dùng một thuật toán mã hóa với secret key tương ứng để mã hóa dữ liệu sắp được truyền đi. Khi bên nhận nhận được sẽ dùng chính secret key đó để giải mã dữ liệu.

- Vấn đề lớn nhất của phương pháp mã hóa đối xứng là làm sao để "thỏa thuận" secret key giữa bên gửi và bên nhận, vì nếu truyền secret key từ bên gửi sang bên nhận mà không dùng một phương pháp bảo vệ nào thì bên thứ ba cũng có thể dễ dàng lấy được secret key này.

- Các thuật toán mã hóa đối xứng thường gặp: DES, AES…

1.6.2. Phương pháp mã hóa công khai (Bất đối xứng)

- Mã hóa bất đối xứng là phương pháp mã hóa mà trong đó key mã hóa và key giải mã khác nhau. Nghĩa là key ta sử dụng để mã hóa dữ liệu sẽ khác với key ta dùng để giải mã dữ liệu. Tất cả mọi người đều có thể biết được public key, và có thể dùng public key này để mã hóa thông tin. Nhưng chỉ có người nhận mới nắm giữ private key, nên chỉ có người nhận mới có thể giải mã được thông tin.

- Để thực hiện mã hóa bất đối xứng thì:

+ Bên nhận sẽ tạo ra một cặp khóa (public key và private key). Bên nhận sẽ dữ lại private key và truyền cho bên gửi public key. Vì public key này là công khai nên có thể truyền tự do mà không cần bảo mật.

+ Bên gửi trước khi gửi dữ liệu sẽ mã hóa dữ liệu bằng thuật toán mã hóa bất đối xứng với key là public key từ bên nhận.

+ Bên nhận sẽ giải mã dữ liệu nhận được bằng thuật toán được sử dụng ở bên gửi, với key giải mã là private key.

- Điểm yếu lớn nhất của mã hóa bất đối xứng là tốc độ mã hóa và giải mã rất chậm so với mã hóa đối xứng, nếu dùng mã hóa bất đối xứng để mã hóa dữ liệu truyền – nhận giữa hai bên thì sẽ tốn rất nhiều chi phí.

Do đó, ứng dụng chính của mã hóa bất đối xứng là dùng để bảo mật secret key cho mã hóa đối xứng: Ta sẽ dùng phương pháp mã hóa bất đối xứng để truyền secret key của bên

gửi cho bên nhận. Và hai bên sẽ dùng secret key này để trao đổi thông tin bằng phương pháp mã hóa đối xứng.

- Thuật toán mã hóa bất đối xứng thường thấy: RSA.

1.6.3. Các hệ mật mã

- Có nhiều cách để phân loại hệ mật mã. Dựa vào cách truyền khóa có thể phân các hệ mật mã thành hai loại:

+ Hệ mật đối xứng (hay còn gọi là mật mã khóa bí mật): là những hệ mật dùng chung một khoá cả trong quá trình mã hoá dữ liệu và giải mã dữ liệu.
Do đó khoá phải được giữ bí mật tuyệt đối.

+ Hệ mật mã bất đối xứng (hay còn gọi là mật mã khóa công khai) : Hay còn gọi là hệ mật mã công khai, các hệ mật này dùng một khoá để mã hoá sau đó dùng một khoá khác để giải mã, nghĩa là khoá để mã hoá và giải mã là khác nhau. Các khoá này tạo nên từng cặp chuyển đổi ngược nhau và không có khoá nào có thể suy được từ khoá kia. Khoá dùng để mã hoá có thể công khai nhưng khoá dùng để giải mã phải giữ bí mật.

- Ngoài ra nếu dựa vào thời gian đưa ra hệ mật mã ta còn có thể phân làm hai loại: Mật mã cổ điển và mật mã hiện đại. Còn nếu dựa vào cách thức tiến hành mã thì hệ mật mã còn được chia làm hai loại là mã dòng và mã khối.

1.7. Kết luận chương

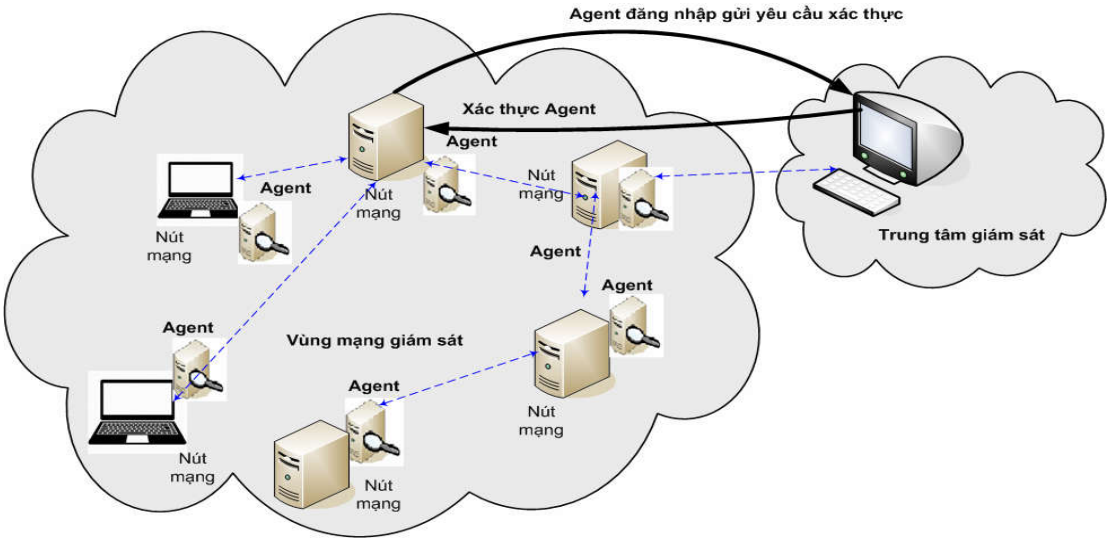
Bảo mật trong môi trường mạng vẫn đang là một thách thức lớn đối với các chuyên gia về bảo mật, nó quan trọng không kém gì vấn đề tối ưu năng lượng tiêu thụ, chi phí, cũng như khả năng kết nối không dây. Việc mã hóa, định danh và xác thực giúp hệ thống loại bỏ được các thiết bị giả mạo, đảm bảo các kết nối không bị hacker xâm nhập.

Chương 2 - GIẢI PHÁP XÁC THỰC DỰA TRÊN ĐỊNH DANH CHO CÁC AGENT

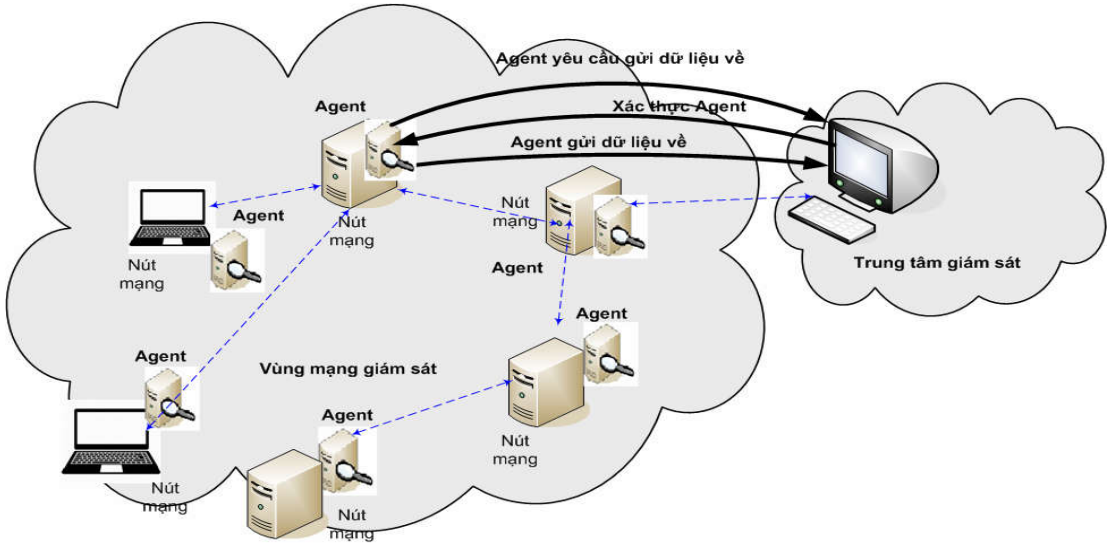
2.1. Giới thiệu chương

Dựa trên cơ sở lý thuyết về phương pháp định danh, phương pháp xác thực và phương pháp mã hóa đã trình bày trong chương 1, chương này đưa ra giải pháp xác thực dựa trên định danh cho các Agent trong hệ thống giám sát mạng tập trung.

2.2. Mô hình kiến trúc mạng giám sát tập trung sử dụng cho giải pháp



Hình 2.1. Sơ đồ hệ thống giám sát mạng tập trung với yêu cầu đăng nhập của Agent



Hình 2.2. Sơ đồ hệ thống giám sát mạng tập trung giai đoạn xác thực Agent và cho phép Agent gửi dữ liệu về trung tâm

Hệ giám sát mạng thường để kiểm tra băng thông sử dụng, kiểm tra hiệu suất của thiết bị, trạng thái của chúng. Hệ giám sát sẽ giúp định hướng trong môi trường phức tạp, đưa ra các báo cáo.

Hình 2.1 và 2.2 là sơ đồ kiến trúc tổng quát của một hệ thống giám sát mạng với các Agent và trung tâm giám sát. Các Agent làm nhiệm vụ thu thập dữ liệu liên quan đến hoạt động của các đối tượng được giám sát (máy chủ Web, máy chủ, máy trạm, router), các sự

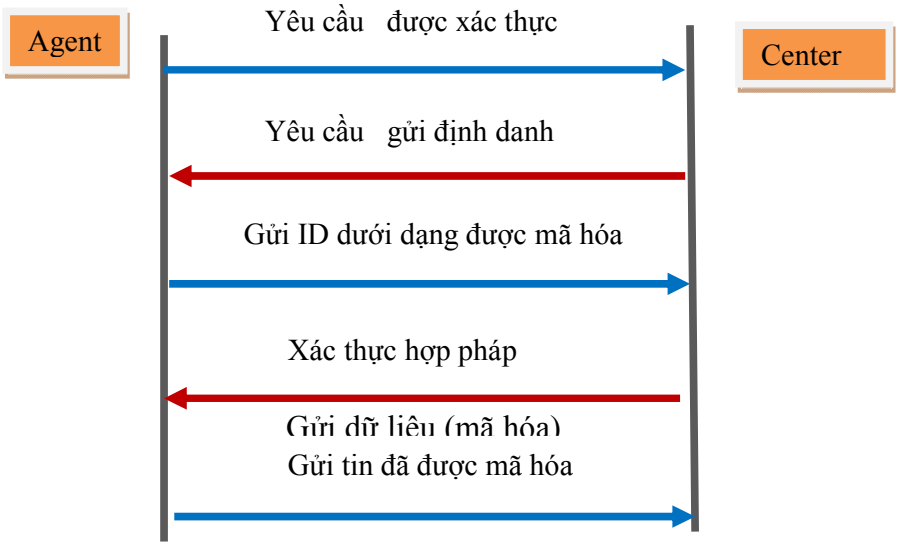
kiện tấn công và truyền về trung tâm giám sát. Hệ thống giám sát ở trung tâm làm nhiệm vụ: phân tích, phát hiện, cảnh báo và thống kê sự cố.

2.3. Định danh cho các Agent

Các Agent muốn truy cập vào hệ thống cần phải có một danh định để chứng minh được mình là một Agent hợp pháp chứ không phải là Agent giả mạo thông qua ID (username, password). Ví dụ, sử dụng phương thức "What you know", phương thức "What you have",phương thức "What you are". Cả ba phương thức nêu trên đều có thể sử dụng để định danh Agent duy nhất trên mạng và sử dụng để xác thực.

Trong luận văn này, ID để xác định Agent được sử dụng đơn giản là một tên định danh cho thiết bị trong mạng (Machine Name) có kèm theo mật khẩu truy nhập thiết bị. Trên cơ sở lý thuyết đã trình bày trong chương 1, bất kỳ dữ liệu nào của thiết bị cũng có thể được sử dụng để xác định định danh cho thiết bị.

*2.*4. Xây dựng lược đồ mã hóa theo định danh



Hình 2.3. Lược đồ mã hóa theo định danh

Hình 2.3 là lược đồ mã hóa cho định danh và xác thực sử dụng trong luận văn.

Các Agen thu thập thông tin và gửi về hệ thống:

- Agent gửi yêu cầu được xác thực về trung tâm
- Trung tâm yêu cầu Agent gửi định danh chứng minh là thành phần hợp pháp của hệ thống giám sát.
- Agent gửi về trung tâm ID đã được mã hóa

- Trung tâm đối chiếu kiểm tra với các ID của hệ thống và trả lời Agent đó là hợp pháp nếu ID đó tồn tại trong hệ thống và cho phép truyền tin .
- Agent gửi thông tin đã thu thập được dưới dạng mã hóa về trung tâm

2.5. Giải pháp xác thực dựa trên mã hóa định danh cho các Agent

2.5.1. Xác thực dùng khóa đối xứng (bí mật)

Phần sau đây trình bày về giải pháp xác thực dựa trên việc sử dụng mã khóa đối xứng. Nguyên tắc chung là ID của thiết bị (bao gồm tên, mật khẩu truy nhập) sẽ được mã hóa với khóa bí mật chỉ có trung tâm giám sát biết phục vụ cho việc giải mã và xác thực.

- **Mô tả phương thức sử dụng mã khóa bí mật:**

Mô tả cho phương thức sử dụng mã khóa bí mật như sau:

C: ciphertext (bản mã hóa cho bản tin M)

M: plaintext (bản rõ của bản tin, nghĩa là dữ liệu ID của thiết bị)

K_A: khóa của Alice (Agent)

$C = \{M\}_K$

K_{AB}: Khoá chung giữa Agent (Alice) và Centre (Bob)

Hình 2.4. Lược đồ mã hóa bí mật chung

➢ Giao thức xác thực lẫn nhau (mutual) dùng khóa đối xứng

Hình 2.5. Lược đồ mã hóa bí mật xác thực lẫn nhau

→Thông điệp ở bước 3 lặp lại từ bước 2: không thể xác thực người gửi

➢ Giao thức xác thực lẫn nhau cải tiến

Hình 2.6. Lược đồ mã hóa bí mật cải tiến

➢ Tấn công giao thức xác thực lẫn nhau cải tiến

Hình 2.7. Lược đồ tấn công mã hóa

➢ Giao thức xác thực lẫn nhau cải tiến khác

Hình 2.8. Lược đồ giao thức xác thực cải tiến

- **Phương thức sử dụng mã khóa bí mật kiểu cổ điển**

Mã hóa Caesa: Nhà quân sự người La Mã Julius Ceasar đã nghĩ ra phương pháp mã hóa một bản tin từ thế kỷ thứ 3 trước công nguyên: thay thế mỗi chữ trong bản tin bằng chữ đứng sau nó k vị trí trong bảng chữ cái.

Chúng ta hãy gán cho mỗi chữ cái một con số nguyên từ 0 đến 25:

Phương pháp Ceasar được biểu diễn như sau: với mỗi chữ cái p thay bằng chữ mã

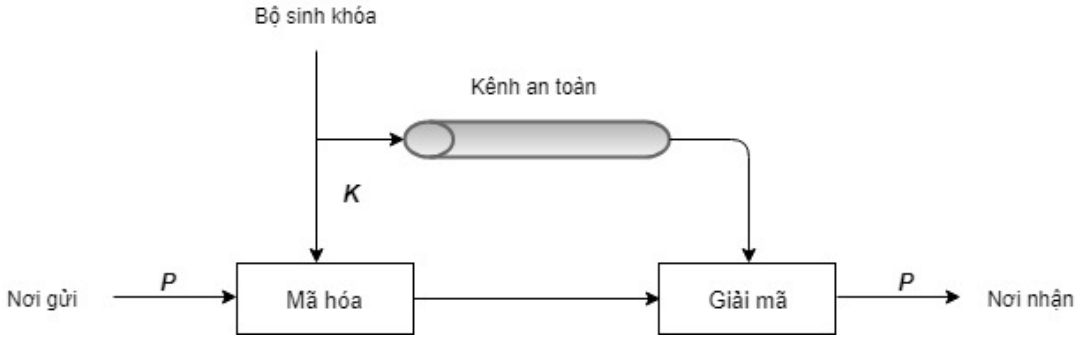
hóa C, trong đó: C = (p + k) mod 26 (trong đó mod là phép chia lấy số dư)

Quá trình giải mã đơn giản là: p = (C – k) mod 26

k được gọi là khóa. Khóa này dùng chung cho cả mã hóa và giải mã.

- **Cơ sở của phương thức sử dụng mã khóa đối xứng cơ bản**

Mô hình mã hóa đối xứng cơ bản.



Hình 2.9. Mô hình mã hóa đối xứng

Mô hình gồm 5 yếu tố:

- Bản rõ P (plain text)
- Thuật toán mã hóa E (encrypt algorithm)
- Khóa bí mật K (secret key)
- Bản mã C (cipher text)
- Thuật toán giải mã D (decrypt algorithm)

Trong đó: C = E (P, K) và P = D (C, K)

Thuật toán mã hóa và giải mã sử dụng chung một khóa, thuật toán giải mã là phép toán ngược của thuật toán mã hóa (trong mã hóa Ceasar, E là phép cộng còn D là phép trừ). Vì vậy mô hình trên được gọi là phương pháp mã hóa đối xứng. Các thuật toán mã hóa đỗi xứng được chia làm hai loại là mã hóa luồng và mã hóa khối.

2.5.2. Xác thực dùng khóa bất đối xứng (công khai)

Phần sau đây trình bày giải pháp xác thực với mã khóa bất đối xứng, sử dụng ID của thiết bị (bao gồm tên, mật khẩu truy nhập), thực hiện mã hóa với khóa bất đối xứng sử dụng 2 cặp khóa cho trung tâm giám sát biết phục vụ cho việc giải mã và xác thực.

- **Mô tả phương thức sử dụng mã khóa bất đối xứng**

C: ciphertext (Bản mã hóa)

M: plaintex (Bản rõ)

K_A: cặp khóa bí mật và công khai của Alice (Agent)

C = $\{M\}_{KA}$: mã hóa bằng khóa công khai của Alice (Agent)

M = $[C]_{KA}$: giải mã bằng khóa bí mật của Bob (Center)

S = [M]KA: ký lên M bằng khóa bí mật

$[\{M\}_{KA}]_{KA}$ = M

$\{[M]_{KA}\}_{KA}$ = M

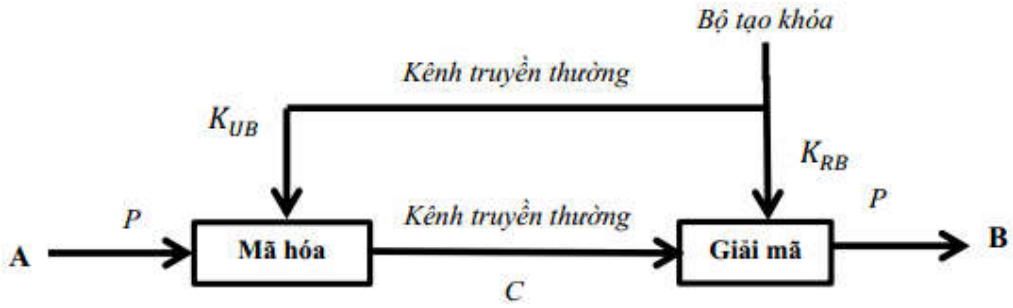
Hình 2.13. Ví dụ về sử dụng mã hóa bất đối xứng

Hệ mã hóa khóa bất đối xứng (hay còn gọi là hệ mã hóa khóa công khai). Hệ mã hóa này bao gồm một khóa dùng để mã hóa, còn gọi là khóa công khai (public key) và một khóa dùng để giải mã, còn gọi là khóa riêng (private key).

Giả sử khi A muốn gửi một thông điệp bí mật tới B, A tìm khóa công khai của B. A và B lần lượt có các cặp khóa bí mật và khóa công khai là K_{UA}, K_{RA}và K_{UB}, K_{RB}. Sau khi kiểm tra chắc chắc là chìa khóa công khai của B (thông qua chứng chỉ số của B), A

sẽ mã hoá thông điệp bằng khóa K_{UB} và gửi cho B. Khi B nhận được thông điệp đã mã hóa,

B dùng khóa K_{RB} để giải mã thông điệp. Mô hình hoạt động được thể hiện ở hình sau:



Hình 2.14. Mã hoá thông điệp sử dụng khoá công khai của B

Mô hình gồm 6 thành phần:

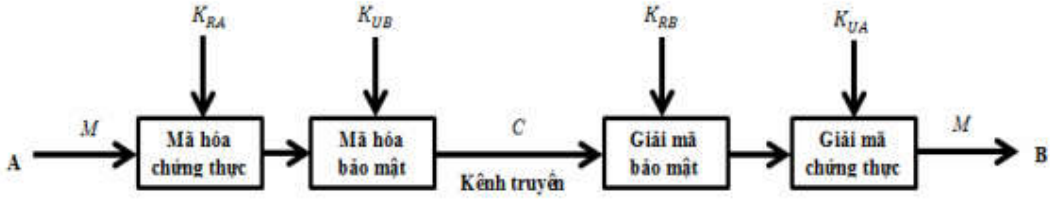
+ Bản rõ M.
+ Thuật toán mã hóa E (encrypt algorithm).
+ Khóa công khai K_{UB} của B.
+ Khóa bí mật K_{RB} của B.
+ Bản mã C (ciphertext).
+ Thuật toán giải mã D (decrypt algorithm)

Khi mã hóa bảo mật: A sẽ tính C = E (M, K_{UB}) để gửi cho B. Khi nhận được bản mã C chỉ có B mới có khóa riêng K_{RB} để giải mã đọc thông điệp của A gửi cho B: M = D (C, K_{RB}).

Khi mã hóa chứng thực: B sẽ tính C = E (M, K_{RB}) để gửi cho A. Khi nhận được bản mã C, A dùng khóa công khai K_{UB} của B để giải mã đọc thông điệp của B gửi cho A: M = D (C, K_{UB})

Như vậy, chỉ có B mới có khóa riêng K_{RB}để giải mã đọc thông điệp của A gửi cho B. Đảm bảo tính bí mật và nếu kẻ tấn công có được khóa bí mật K_{RB} của B thì B không thể chối bỏ trách nhiệm làm lộ khóa.

Tuy nhiên, với mô hình trên khi chỉ triển khai hệ mã hóa bất đối xứng cho mình B. Thì B không thể biết dữ liệu gửi đến có phải là A gửi hay không. Để giải quyết vấn đề trên, người ta kết hợp cả tính bảo mật và tính chứng thực bằng mô hình sau:



Hình 2.15. A và B cùng sử dụng hệ mã hóa bất đối xứng

Khi đó, nếu A gửi thông điệp M đến B sẽ tính: C = E (E (M, K_{RA}), K_{UB}) B nhận được bản mã C sẽ tính: M = D (D (C, K_{RB}), K_{UA})

Một số đặc điểm của mã hóa bất đối xứng:

Do sử dụng hai khóa mã hóa và giải mã khác nhau nên giúp đơn giản việc phân phối khóa giữa bên nhận cho bên gửi và khóa mã hóa có thể truyền trên kênh không an toàn mà không cần giữ bí mật.

Các thuật toán của hệ mã hóa bất đối xứng sử dụng khóa mã hóa là khóa công khai có độ dài khóa lớn, làm tăng khối lượng tính toán. Vì vậy, các thuật toán của hệ mã hóa bất đối xứng khó áp dụng cho các hệ thống có tài nguyên lưu trữ và năng lực tính toán hạn chế.

Một vấn đề nảy sinh là khả năng dễ bị tấn công dạng kẻ tấn công người đứng giữa.

Việc phát minh ra hệ mã hóa khóa bất đối xứng tạo ra một cuộc cách mạng trong công nghệ an toàn thông tin điện tử. Các thuật toán của hệ mã hóa đối xứng giải quyết được 2 vấn đề rất quan trọng mà các hệ mã hóa khác không giải quyết được là trao đổi khóa và xác thực. Tuy hệ mã hóa đối xứng ra đời lâu và có nhiều phát triển để đáp ứng yêu cầu an toàn thông tin, tuy nhiên vẫn còn tồn tại hai điểm yếu sau:

- Phải giữ bí mật khóa: Nếu bị lộ khóa cũng không có cơ sở để quy trách nhiệm bên gửi hay bên nhận làm lộ khóa.
- Quá trình trao đổi khóa giữa bên gửi và bên nhận: Cần phải có một kênh an toàn để trao đổi khóa trước khi trao đổi dữ liệu.

2.6. Kết luận chương

Việc xác định xem các Agent có được phép truyền tin hay không bao gồm các bước định danh và xác thực riêng biệt. Nhận dạng liên quan đến cách thức mà Agent cung cấp danh tính duy nhất của mình cho hệ thống. Danh tính có thể là tên hoặc một số. Danh tính phải là duy nhất để hệ thống có thể phân biệt giữa những Agent khác nhau.

Giải thuật mã hóa đối xứng hoặc bất đối xứng có khả năng chống được các cuộc tấn công trên Internet nói chung và tấn công nhằm vào các Agent nói riêng.

Chương 3 - KẾT QUẢ THỬ NGHIỆM

3.1. Giới thiệu chương

Chương này trình bày kết quả thử nghiệm cho giải pháp xác thực dựa trên định danh cho các Agent trong một hệ thống giám sát mạng tập trung..

3.1.1. Công cụ mô phỏng NS-2

NS-2 (Network Solution 2) là phần mềm mô phỏng mạng điều khiển sự kiện riêng rẽ hướng đối tượng. Bốn lợi ích lớn nhất của NS-2 phải kể đến đầu tiên là:

- Khả năng kiểm tra tính ổn định của các giao thức mạng đang tồn tại
- Khả năng đánh giá các giao thức mạng mới trước khi đưa vào sử dụng
- Khả năng thực thi những mô hình mạng lớn khó thực thi được trong thực tế
- Khả năng mô phỏng nhiều loại mạng khác nhau

NS-2 không chỉ hợp cho việc mô phỏng mà cho cả sự giả lập, điều này có nghĩa là nó có thể đưa chương trình mô phỏng vào trong mạng thực tế.

Hạn chế của NS-2 là thêm mới và chỉnh sửa các thành phần là không dễ dàng do cấu trúc của NS-2 đã được định hình sẵn. Cũng theo báo cáo thì tốc độ tính toán của NS-2 cũng khá chậm. Khó và mất rất nhiều thời gian để tiếp cận phần mềm.

3.1.2. Công cụ mô phỏng OPNET

OPNET là một công cụ mô phỏng mạng sự kiện mức cao. OPNET hỗ trợ mô phỏng mạng WSN tốt (cụ thể là tốt hơn NS2). OPNET là chương trình mô phỏng trên nền Windows được sử dụng rộng rãi. Nó được xây dựng dựa trên ngôn ngữ C++ và cung cấp môi trường ảo cho việc mô hình hóa, phân tích và dự đoán hiệu năng mạng, giúp mô hình hóa chính xác các ứng dụng, các máy chủ và nhiều công nghệ mạng. Hạn chế của OPNET là khó tiếp cận và cần có thời gian để tìm hiểu cũng như sử dụng thành thạo.

3.1.3. Công cụ mô phỏng Contiki/Cooja

Hệ điều hành Contiki được lập trình bằng ngôn ngữ C, hoạt động dựa trên cơ chế event - driven và có những đặc điểm phù hợp với các hệ thống nhúng và mạng cảm biến không dây. Bên cạnh đó, Contiki còn cung cấp những công cụ hỗ trợ mô phỏng với giao diện đơn giản, dễ sử dụng và hỗ trợ tốt những thiết bị trong thực tế, phục vụ những mục đích nghiên cứu, mô phỏng và triển khai những giao thức mới.

3.2. Giới thiệu tóm tắt về môi trường mô phỏng Contiki

3.2.1. Kiến trúc hệ thống của Contiki.

Kiến trúc hệ thống của contiki có dạng mô đun, với 4 thành phần cơ bản: Nhân, nạp chương trình, các thư viện và các quy trình, quy trình có thể là một dịch vụ hay chương trình ứng dụng. Một quy trình được định nghĩa bởi một hàm xử lý sự kiện và một tùy chọn hàm quản lý bầu chọn. Trong suốt quá trình biên dịch, hệ thống được phân thành hai phần: Chương trình lõi và nạp.

Lõi được biên dịch thành ảnh nhị phân đơn và lưu trữ trong các thiết bị, và nó thường không được sửa đổi sau khi triển khai. Các chương trình được nạp bởi chương trình nạp có chứa chương trình nhị phân hoặc bằng cách sử dụng cụm giao thức, hoặc sử dụng bộ nhớ kèm trực tiếp.

Nhân Contiki là một trình lập lịch sự kiện nhẹ gửi tới các tiến trình đang chạy và gọi các trình xử lý bầu chọn. Một quy trình chạy có thể được kích hoạt bởi các sự kiện gửi đi hoặc cơ chế bầu chọn. Nhân không chặn một xử lý sự kiện mà mà nó đã lập lịch. Do vậy các xử lý sự kiện phải chạy để hoàn thành hoặc sử dụng cơ chế nội bộ để đạt được sự ưu tiên.

3.2.2. Các tính năng của Contiki

Phân bổ và quản lý bộ nhớ: Contiki được thiết kế cho các hệ thống nhỏ có thể hoạt động chỉ với vài kb bộ nhớ khả dụng.

Nhận biết năng lượng: Contiki cung cấp một cơ chế ước tính năng lượng hệ thống để xem vị trí mà năng lượng bị tiêu hao.

Mô phỏng mạng Cooja: Cooja là mô phỏng mạng cung cấp bởi hệ điều hành Contiki. Có nhiều kiểu mote khác nhau có thể được mô phỏng ở mức phần cứng, cho phép ngươi dùng kiểm tra hành vi chính xác của mạng.

3.2.3. Ứng dụng mô phỏng Cooja

Cooja là phần mềm mô phỏng hệ thống mạng được tích hợp trong hệ điều hành Contiki. Công cụ này cho phép người sử dụng thay đổi các thông số như vị trí, phạm vi kết nối, tỉ lệ truyền gói thành công,… Nhờ đó người sử dụng có thể mô phỏng và đánh giá kết quả một cách hiệu quả hơn. Giao diện của chương trình thân thiện và dễ sử dụng.

3.3. Mô hình kiến trúc mạng mô phỏng với Contiki – Cooja

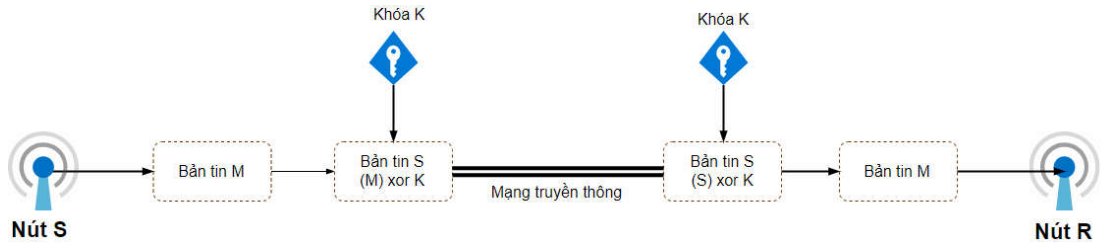
Mã hóa đối xứng được lựa chọn trong mô hình này vì một số đặc tính sau:

- Khá gọn nhẹ, tính toán nhanh.
- Đảm bảo được tính bảo mật, chứng thực, toàn vẹn, chống chối bỏ của một hệ truyền tin.

Mô tả bài toán: Truyền bản tin từ nút mạng S(Agent) đến nút mạng R (Center: Trung tâm giám sát) sử dụng phương pháp bảo mật đối xứng để mã hóa bản tin (Mã hóa định danh,và bản tin). Trong đó:

- Bên gửi: Nút S (Agent)
- Bên nhận: Nút R (Center)
- Bản tin cần rõ: M (Message)

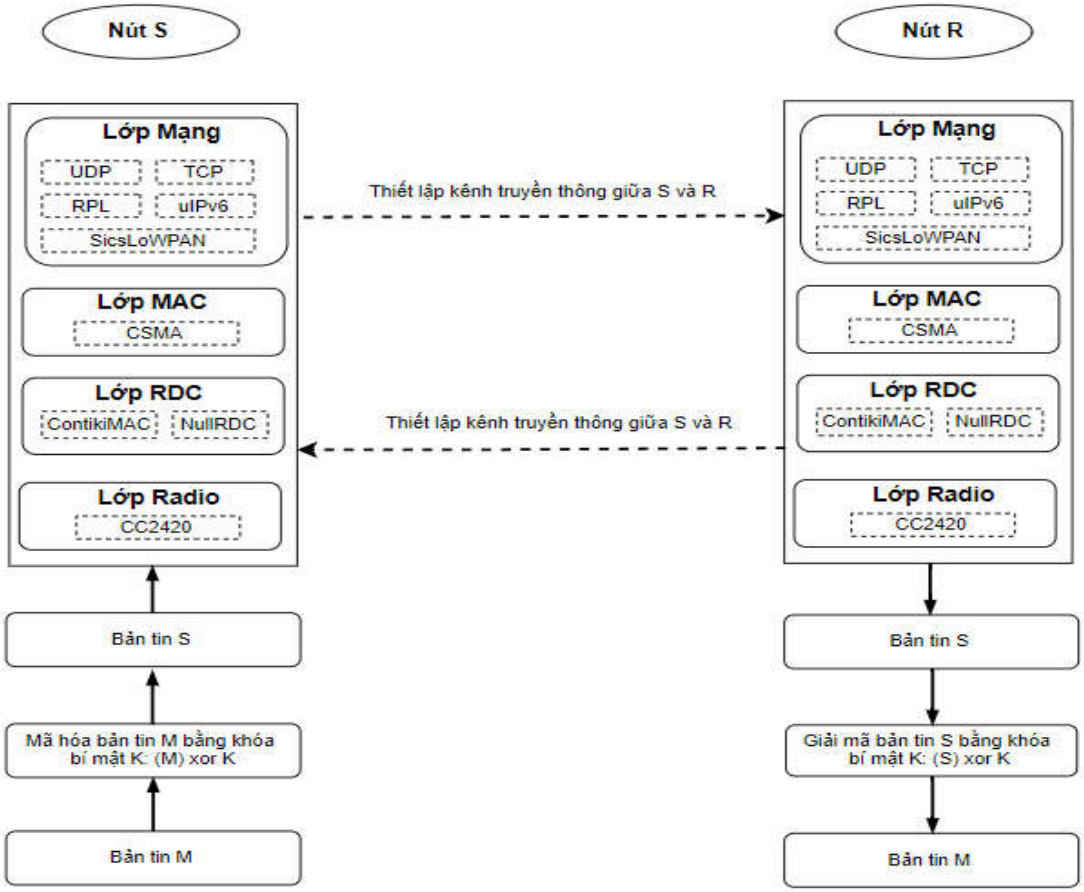
- Bản tin mã hóa: S (Symmetric)
- Khóa: K (Key)



Hình 3.5. Mô hình truyền tin giữa Agent và Center

Xây dựng các kịch bản mô phỏng thử nghiệm.

Kịch bản mô phỏng thử nghiệm xác thực dựa trên mã hóa định danh cho các Agent được hiện thông qua sơ đồ dưới đây:



Hình 3.6. Kịch bản thử nghiệm truyền tin bảo mật giữa Agent (Nút S) và Center (Nút R)

Giai đoạn 1: Xác thực giữa một cặp Agent và Center

Giai đoạn 2: Agent gửi các bản tin thu thập được về trung tâm

Các bước thực hiện: Thử nghiệm với một Agent và một server.

Bước 1: Setup a connection from Agent to Server

Bước 2: Agent has Agent ID key = "Here is Agent key ID"

Bước 3: Encryption using Symmetric key (Ks) for the "Agent ID key "and send to Server

Bước 4: Server decrypts "Agent ID key" using symmetric key and check for the correct "Agent ID key" of the Agent

Bước 5: If the authentication is successful -> Message transmission from Agent to server is enable!

If the authentication is failed ->Transmission from Agent to server is not permitted!

3.4. Các kết quả thử nghiệm

Thực hiện mô phỏng: Thử nghiệm với một Agent và một server.

Công cụ thực hiện mô phỏng: Sử dụng Cooja trên hệ điều hành Contiki để mô phỏng.

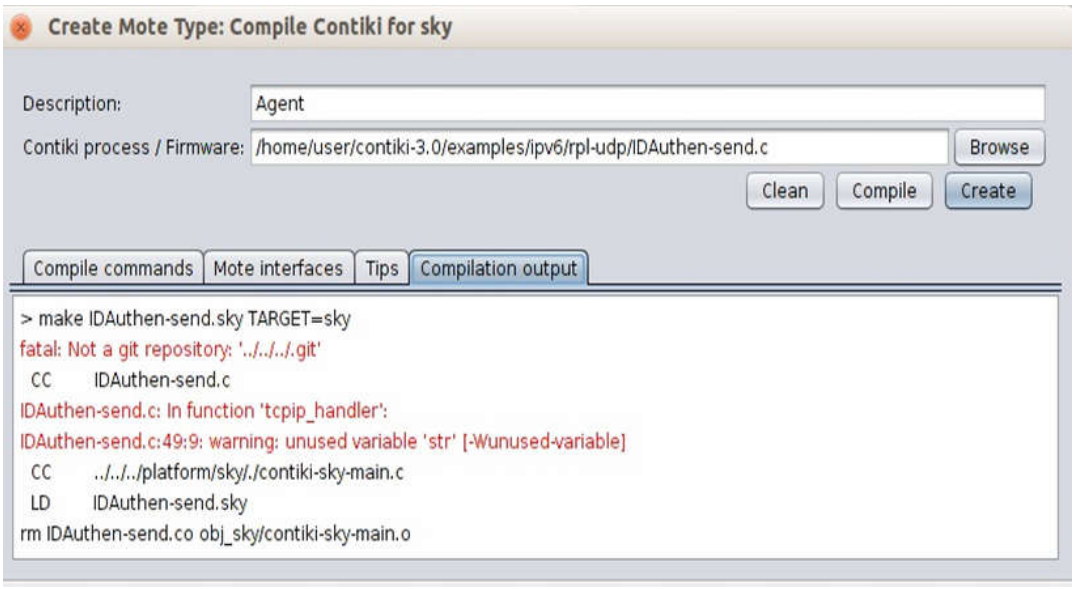
Quá trình thực hiện: Sử dụng 1 Agent và một Server (Trung tâm giám sát) để truyền tin sử dụng mã hóa đối xứng phân tích và đánh giá kết quả

Trong màn hình của Cooja ta tạo một chương trình mô phỏng bằng cách chọn File/ New khi đó xuất hiện cửa sổ Create new Simulation tại Simulation name ta đặt tên cho chương trình mô phỏng là Agent ID Authentication tiếp theo chọn Create để hoàn thành.

Tạo Agent: Trong cửa số Applications Places ta chọn Motes/ Add motes/ Create new mote type/ Sky mote.

Khi đó sẽ xuất hiện cửa số Create mote type: Contiki for sky. Tại đây ta đặt tên cho mote mới tại Description là Agent. Tiếp theo chọn Browse -> xuất hiện cửa sổ để ta lựa chọn:Home/user/contiki -3.0/examples/ipv6/rpl-udp/IDAuhen-Send.c

Tiếp theo chọn Compile để chạy; chọn Create để lựa chọn số Agent

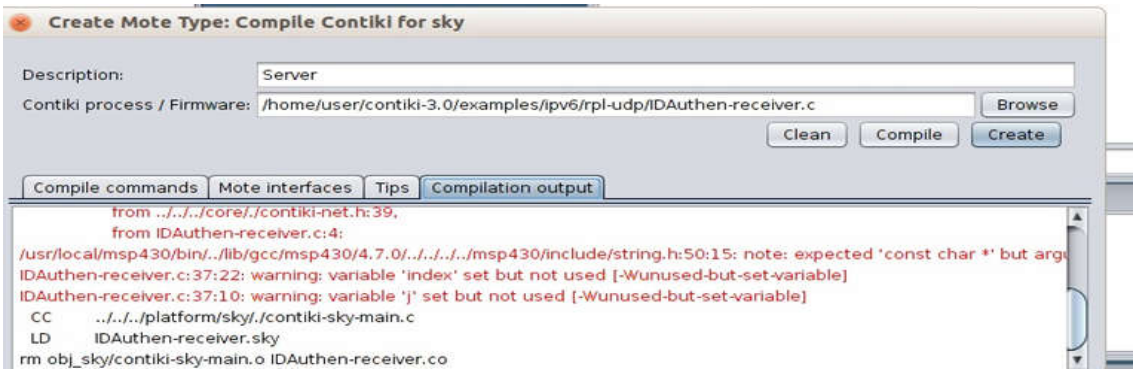


Hình 3.9. Tạo Agent

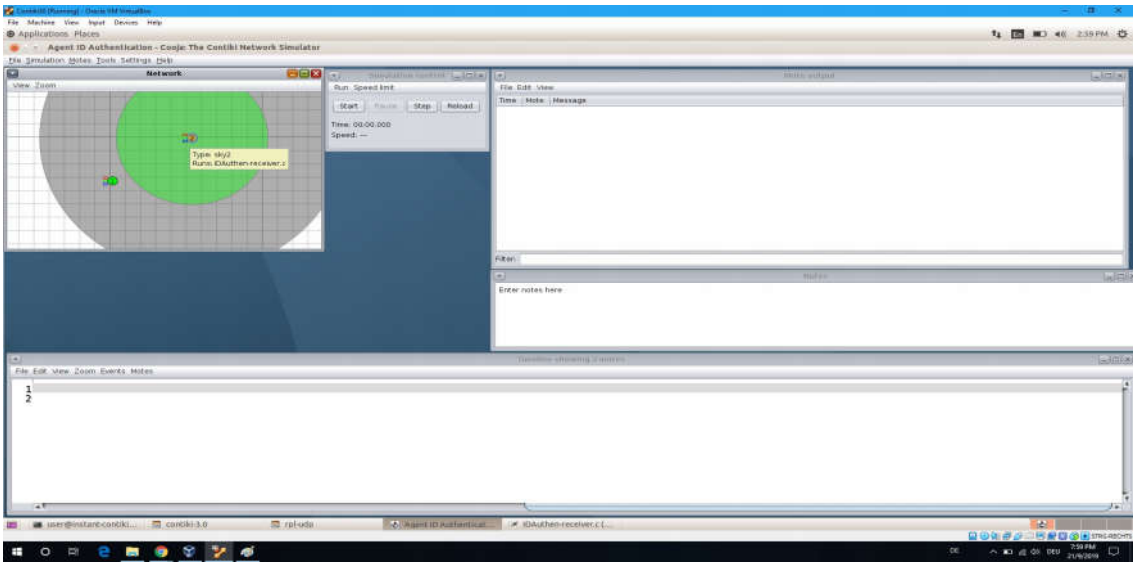
Tạo Server: Tương tự tạo Agent, Trong cửa số Applications Places ta chọn Motes/ Add motes/ Create new mote type/ Sky mote.

Khi đó sẽ xuất hiện cửa số Create mote type: Contiki for sky. Tại đây ta đặt tên cho mote mới tại Description là Server, tiếp theo chọn Browse khi đó xuất hiện cửa sổ để ta lựa chọn:Home/user/contiki -3.0/examples/ipv6/rpl-udp/IDAuhen-recelver.c

Tiếp theo chọn Compile để hoàn thành

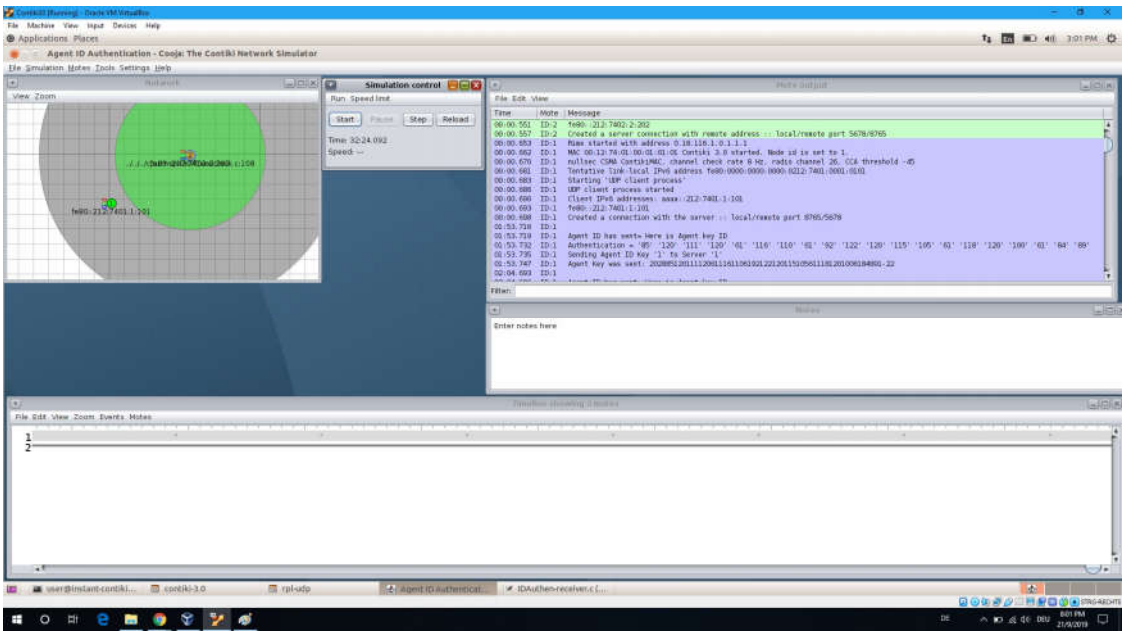


Hình 3.12. Tạo Server

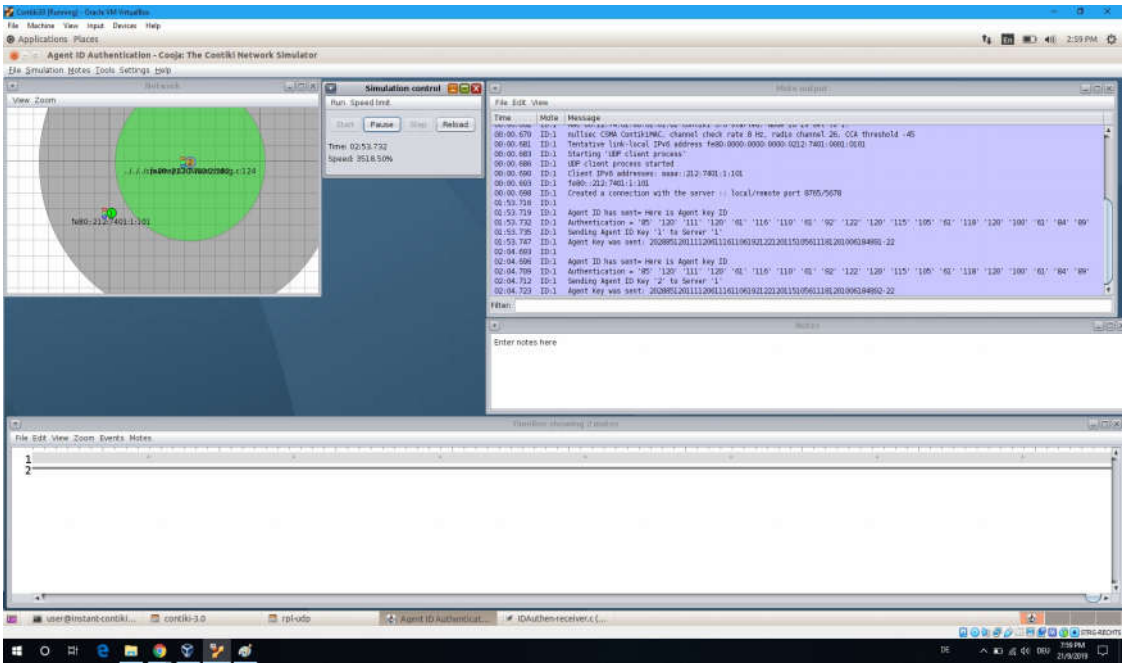


Hình 3.13. Hai mote được tạo để thực hiện mô phỏng: 1= Agent, 2 = Server

Kết quả quả thực hiện từ bước 1 đến bước 5: Quá trình xác thực dựa trên định danh



Hình 3.14. Quá trình xác thực dựa trên định danh



Hình 3.15. Quá trình xác thực dựa trên định danh

Kết quả:

- Mã hóa bằng mã đối xứng cho Agent ID key và gửi đến máy chủ
- Máy chủ giải mã "Agent ID key" bằng khóa đối xứng và kiểm tra "Agent ID key"có chính xác không
- Xác thực thành công cho phép truyền tin từ Agent tới trung tâm
- Truyền tin bảo mật giữa Agent và Server

3.5. Kết luận chương.

Giải pháp xác thực dựa trên định danh cho các Agent trong hệ thống giám sát mạng có thể góp phần đắc lực cho mục đích xác định đúng đối tượng hợp pháp thu thập thông tin, chuyển tiếp dữ liệu thu được về trung tâm xử lý.

KẾT LUẬN

Trong một hệ thống giám sát thường có rất nhiều Agent làm nhiệm vụ thu thập thông tin về tình trạng hoạt động của các thiết bị và mạng, đồng thời thu thập dữ liệu về các hành vi tấn công nhằm chuyển về trung tâm giám sát để xử lý, phân tích, đưa ra cảnh báo về các nguy cơ tấn công, sự cố, lỗi,…

Một nhu cầu thực tế đặt ra là cần xác định xem các Agent đó có phải thực sự là thành viên hợp pháp của hệ thống giám sát hay không. Một khả năng để giải quyết vấn đề này là sử dụng xác thực dựa trên định danh cho các Agent trong hệ thống giám sát mạng.

Giải pháp xác thực dựa trên định danh cho các Agent trong hệ thống giám sát mạng có thể góp phần đắc lực cho mục đích xác định đúng đối tượng hợp pháp thu thập thông tin, chuyển tiếp dữ liệu thu được về trung tâm xử lý.

Các kết quả đã đạt được trong bài luận văn gồm:

- Nghiên cứu về hệ thống giám sát mạng tập trung và các Agent thu thập thông tin giám sát, cơ sở lý thuyết cho định danh và xác thực, các phương pháp mã hóa bí mật và công khai có thể sử dụng cho xác thực các Agent trong hệ thống.
- Nghiên cứu xây dựng giải pháp xác thực dựa trên định danh cho các Agent trong hệ thống giám sát mạng tập trung với việc sử dụng ID (Machine Name, Password) cho các thiết bị Agent để định danh Agent, xây dựng các lược đồ mã hóa, thực hiện xác thực Agent dựa trên mã hóa ID theo phương thức sử dụng mã khóa bí mật và mã khóa công khai.
- Thực hiện thử nghiệm xác thực dựa trên định danh cho các Agent trong hệ thống giám sát mạng tập trung trên hệ thống mô phỏng Contiki-Cooja.

Hướng phát triển tiếp có thể là:

- Thử nghiệm gán định danh cho các Agent với các phương thức khác như sử dụng thẻ từ, hoặc sử dụng các dữ liệu duy nhất của Agent như địa chỉ MAC.
- Thử nghiệm mô phỏng quá trình xác thực và trao đổi thông tin giữa trung tâm giám sát với đồng thời nhiều Agent hơn.