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

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

HÀ NỘI - 2019

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

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

NGƯỜI HƯỚNG DẪN KHOA HỌC

PGS. TSKH. HOÀNG ĐĂNG HẢI

HÀ NỘI - 2019

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

DANH MỤC CÁC THUẬT NGỮ, CHỮ VIẾT TẮT

Tên viết tắt	Tên Tiếng Anh	Tên Tiếng Việt
WSN	Wireless Sensor Network	Mạng cảm biến không dây
IOT	Internet of things	Internet vạn vật
DB	Database	Cơ sở dữ liệu
FW	Firewall	Tường lửa
K	Key	Khóa
P	Plain text	Bản rõ
C	Cipher Text	Bản mã
IP	Internet protocol	Giao thức Internet
MAC	Medium Access Control	Vỉ mạch kết nối mạng Internet
IPv6	Internet Protocol Version 6	Giao thức mạng Internet phiên bản 6
TCP/IP	Transmission Control Protocol/ Internet Protocol	Bộ giao thức liên mạng
DES	Data Encryption Standard	Chuẩn mã hóa dữ liệu
AES	Advanced Encryption Standard	Chuẩn mã hóa cấp cao
RSA	Rivest-Shamir-Adleman	Thuật toán mật mã khóa công khai
UDP	User Datagram Protocol	Giao thức sử dụng dữ liệu
RPL	Routing Protocol for Low power and Lossy Network	Phương pháp trao đổi khóa động dành cho mạng yếu và công suất thấp
PIN	Personal Identification Number	Mã số nhận dạng cá nhân
ID	Identification	Nhận dạng

DANH SÁCH HÌNH VẼ

MỞ ĐẦU

1. Lý do chọn đề tài:

Giám sát mạng là một nhu cầu thực tế của các nhà mạng nhằm mục đích theo dõi hoạt động của mạng, sớm phát hiện các lỗi, sự cố do tấn công mạng, suy giảm hoạt động của các thiết bị trên mạng, đưa ra cảnh báo nguy cơ và cung cấp thông tin hỗ trợ xử lý sự cố.

Đã có khá nhiều hệ thống giám sát mạng được phát triển và ứng dụng trong thực tiễn. 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,…

Một vấn đề thường đặt ra là các Agent có thực sự là thành viên của hệ thống giám sát hay không? Nếu không có cơ chế xác thực, một Agent có thể là một máy do kẻ tấn công cài vào mạng, thực hiện thu thập thông tin và chuyển về cho kẻ tấn công. Vấn đề xác thực Agent hợp pháp không phải luôn có trong mỗi hệ thống giám sát mạng hiện nay. Do vậy, một yêu cầu đặt ra là cần nghiên cứu giải pháp xác thực các Agent cho hệ thống giám sát mạng. Phương pháp xác thực dựa trên định danh đã được đề xuất áp dụng chủ yếu cho các mạng cảm biến không dây, mạng peer-to-peer, hoặc cho điện toán đám mây.

Yêu cầu đặt ra là cần nghiên cứu về giải pháp áp dụng phương pháp xác thực dựa trên định danh cho các Agent trong hệ thống giám sát mạng. Đó là chủ đề nghiên cứu của luận văn này.

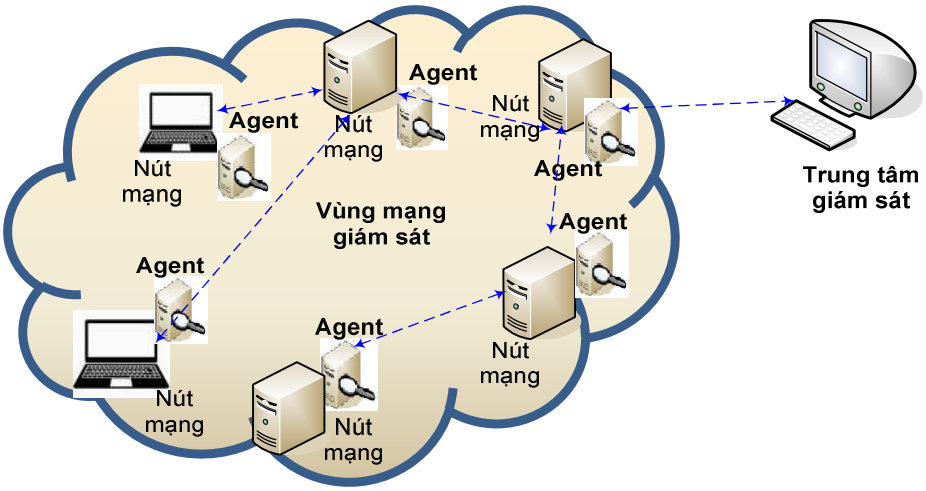
2. Tổng quan về vấn đề nghiên cứu:

Vấn đề nghiên cứu đặt ra là nghiên cứu một giải pháp xác thực dựa trên định danh cho các Agent trong hệ thống giám sát mạng. Phạm vi hệ thống giám sát có thể là trong một phần mạng thuộc một tổ chức, doanh nghiệp hoặc cho nhiều phân vùng mạng trên diện rộng. Vị trí giám sát có thể đặt tại thiết bị đầu cuối, máy chủ, hoặc nút mạng trung gian (ví dụ Router, Gateway,…). Kiến trúc giám sát có thể phân tán hoặc tập trung, song mô hình giám sát mạng tập trung là phổ biến. Đối

tượng giám sát có thể là một máy trạm, máy chủ hoặc một nút mạng bất kỳ, hoặc một máy chủ Web. Các mô hình giám sát mạng tập trung điển hình đã được khảo sát và trình bày trong các tài liệu như [1], [2], [3].

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 (còn gọi là máy trinh sát, thường gọi là Agent hay sensor) 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. Chi tiết về các công cụ giám sát đã được trình bày trong [1, 2, 3]. Chi tiết về Agent (hay sensor) thu thập thông tin được trình bày trong [3].

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).



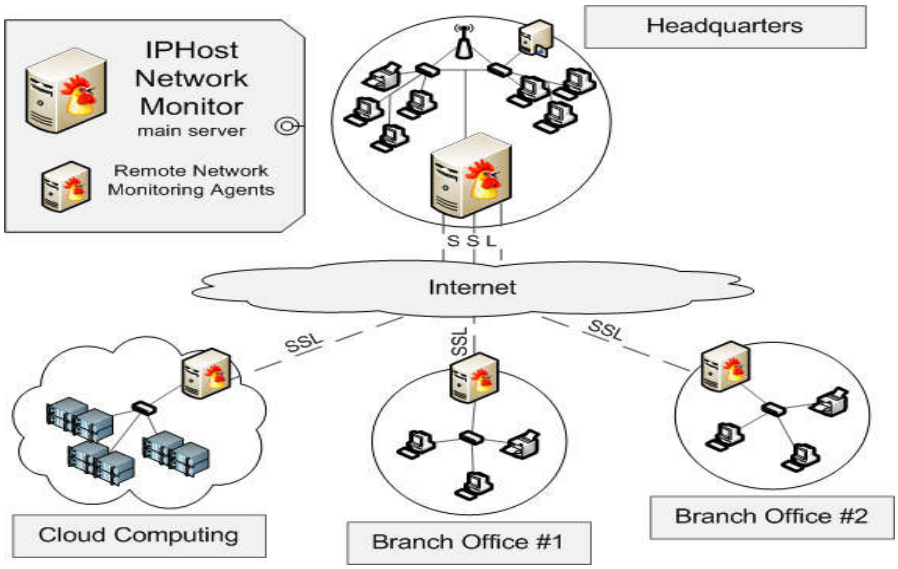
Hình 1. Kiến trúc hệ thống giám sát mạng tập trung

Hình 1 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 2 là ví dụ về một hệ thống giám sát tập trung cho ba phân vùng mạng. Phân vùng 1 (Cloud Computing) biểu thị hệ thống máy ảo của một cơ quan hoặc tổ

chức. Phân vùng 2 (Branch Office 1) và Phân vùng 3 (Branch Office 2) là hai miền mạng con (nghĩa là hai địa điểm làm việc) của một cơ quan hoặc tổ chức. Trung tâm điều hành của một cơ quan hoặc tổ chức đó đặt ở Headquarter. Các hệ thống mạng của 4 miền này được kết nối với nhau thông qua Internet (xem Hình 2).

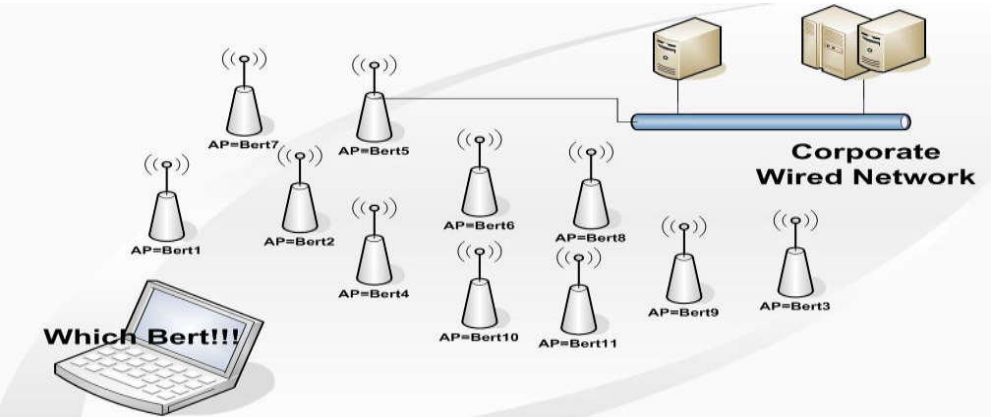
Hệ thống giám sát trung tâm được đặt tại miền Headquarter (có tên là IPHost Network Monitor như trên hình 2). Các Agent (remote Network Monitoring Agents) thu thập dữ liệu giám sát tại các miền mạng biểu thị bằng các máy tính có dấu màu đỏ).



Hình 2. Kiến trúc hệ thống giám sát mạng tập trung cho nhiều phân vùng mạng

Trong một hệ thống giám sát như vậy, tin tặc có thể đưa máy tính hoặc Agent tự tạo trà trộn vào hệ thống nhằm thu thập thông tin trái phép.

Hệ thống giám sát cần có cơ chế xác định đúng Agent hợp pháp thuộc hệ thống và chỉ có các Agent này mới có thể truyền dữ liệu về trung tâm giám sát. Nguy cơ tấn công có thể phát sinh khi một kẻ tấn công xâm nhập và cài một giả danh Agent của hệ thống. Mặt khác, dữ liệu truyền từ các Agent về trung tâm cũng cần được bảo vệ thích đáng bằng mã hóa.



Hình 3. Ví dụ về một trường hợp tấn công giả danh nút mạng truy nhập

Tài liệu [4] chỉ ra những khả năng tin tặc có thể sử dụng cài lén phần mềm để khai thác các lỗ hổng bảo mật trong hệ thống máy chủ Web trong hệ thống mạng của một tổ chức. Các tài liệu [5, 6] chỉ ra phương thức mã hóa cho truyền tin bảo mật giữa các nút mạng trong mạng IoT, sử dụng phương thức mã hóa đối xứng hoặc bất đối xứng.

Phương pháp xác thực dựa trên định danh đã được đề xuất khoảng chục năm trở lại đây, chủ yếu cho các mạng cảm biến, kết nối mạng peer-to-peer, hoặc cho điện toán đám mây. Phương pháp xác thực dựa trên định danh sẽ là một giải pháp khả thi cho bài toán quản lý xác thực Agent trong hệ thống giám sát mạng nêu trên và đó là chủ đề nghiên cứu của luận văn này.

Một số cơ chế xác thực dựa trên định danh có thể tham khảo trong các tài liệu [9 – 15].

Luận văn tập trung vào các trọng tâm nghiên cứu sau đây:

- Nghiên cứu tổng quan về kiến trúc hệ thống giám sát tập trung và các Agent.
- Nghiên cứu cơ sở lý thuyết cho phương pháp định danh và xác thực.
- Nghiên cứu xây dựng giải pháp xác thực dựa trên định danh cho các Agent.
- Vấn đề truyền tin bảo mật từ các Agent về trung tâm giám sát.
- Kết quả thử nghiệm (dự kiến với môi trường mô phỏng Contiki)

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.

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:

Bài sử dụng các phương pháp nghiên cứu sau:

- 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 về các giải pháp, thuật toán, phương pháp liên quan đến định danh, xác thực qua thu thập, 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

Như đã trình bày ở phần mở đầu, 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 (còn gọi là máy trinh sát, thường gọi là Agent hay sensor) 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].

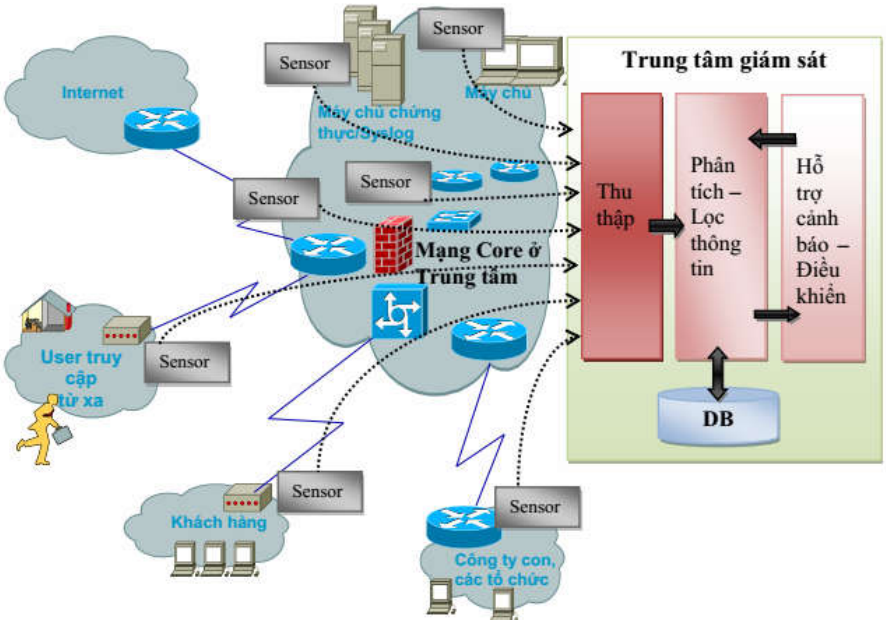
Nhiệm vụ chính của các hệ thống theo dõi, giám sát là bảo vệ cho một hệ thống máy tính dựa trên việc phát hiện các dấu hiệu tấn công và đưa ra cảnh báo.

Việc phát hiện các tấn công phụ thuộc vào số lượng và kiểu hành động thích hợp. Toàn bộ hệ thống cần phải được kiểm tra một cách liên tục. Dữ liệu được tạo ra từ các hệ thống phát hiện xâm nhập được kiểm tra một cách cẩn thận (đây là nhiệm vụ chính cho mỗi hệ thông theo dõi, giám sát) để phát hiện các dấu hiệu tấn công.

Khi một hành động xâm nhập được phát hiện, hệ thống theo dõi, giám sát đưa ra các cảnh báo đến các quản trị viên hệ thống về sự việc này. Bước tiếp theo được thực hiện bởi các quản trị viên hoặc có thể là bản thân hệ thống theo dõi, giám sát bằng cách lợi dụng các tham số đo bổ sung (các chức năng khóa để giới hạn các session, backup hệ thống, định tuyến các kết nối đến bẫy hệ thống, cơ sở hạ tầng hợp lệ,…).

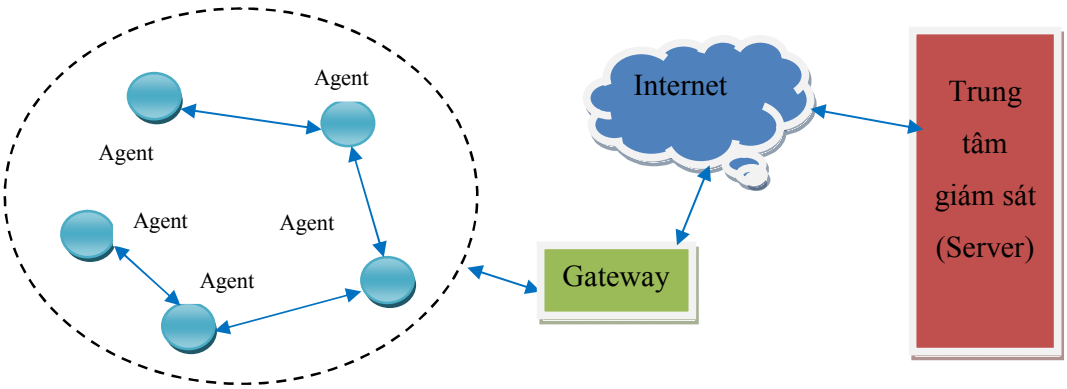
Giữa các nhiệm vụ hệ thống theo dõi, giám sát khác nhau, việc nhận ra kẻ xâm nhập là một trong những nhiệm vụ cơ bản. Nó cũng hữu dụng trong việc nghiên cứu mang tính pháp lý các tình tiết và việc cài đặt các bản vá thích hợp để

cho phép phát hiện các tấn công trong tương lai nhằm vào các cá nhân cụ thể hoặc tài nguyên hệ thống.



Hình 1.1. Mô hình hệ thống giám sát mạng cấp tỉnh

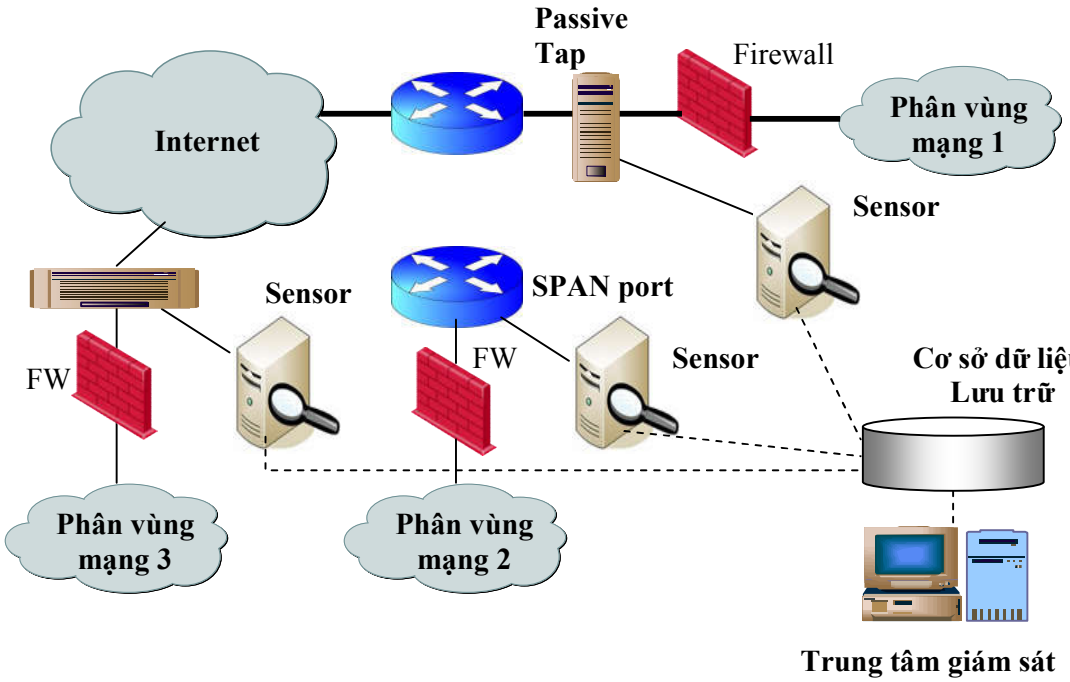
Các Agent có thể là một thiết bị đặt tại đối tượng cần giám sát, hoặc một phần mềm được cài đặt trên đối tượng giám sát.



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.

Giám sát mạng là một nhu cầu thực tế của các nhà mạng nhằm mục đích theo dõi hoạt động của mạng, sớm phát hiện các lỗi, sự cố do tấn công mạng, suy giảm hoạt động của các thiết bị trên mạng, đưa ra cảnh báo nguy cơ và cung cấp thông tin hỗ trợ xử lý sự cố.

Đã có khá nhiều hệ thống giám sát mạng được phát triển và ứng dụng trong thực tiễn. 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.

Một vấn đề thường đặt ra là các Agent có thực sự là thành viên của hệ thống giám sát hay không? Nếu không có cơ chế xác thực, một Agent có thể là một máy do kẻ tấn công cài vào mạng, thực hiện thu thập thông tin và chuyển về cho kẻ tấn công. Vấn đề xác thực Agent hợp pháp không phải luôn có trong mỗi hệ thống giám sát mạng hiện nay. Do vậy, một yêu cầu đặt ra là cần nghiên cứu giải pháp xác thực các Agent cho hệ thống giám sát mạng. Phương pháp xác thực dựa trên định danh đã được đề xuất áp dụng chủ yếu cho các mạng cảm biến không dây, mạng peer-to-peer, hoặc cho điện toán đám mây.

Yêu cầu đặt ra là cần nghiên cứu về giải pháp áp dụng phương pháp xác thực dựa trên định danh cho các Agent trong hệ thống giám sát mạng.

1.4. Phương pháp định danh (Identification)

Khái niệm về định danh:

Người dùng cung cấp danh định của mình cho hệ thống. Định danh là một tên dùng để xác thực một đối tượng duy nhất hay một lớp duy nhất của đối tượng, trong đó "đối tượng" hay lớp có thể là một ý tưởng, một đối tượng vật lý, hay vật chất vật lý. Định danh dược sử dụng rộng rãi trong hầu hết các hệ thống thông tin.

Trong khoa học máy tính, định danh có thể là các mã dùng để đặt tên cho các thực thể (ID). Về nguyên tắc, mỗi thuộc tính "duy nhất" cho một đối tượng đều có thể dùng làm định danh cho vật thể đó. Ví dụ: địa chỉ MAC (Medium Access Control) là duy nhất cho một vỉ mạch mạng, do đó có thể dùng làm định danh cho vỉ mạch liên kết mạng đó, và do đó cho cả máy tính đó. Hàm băm Hash là một giá trị duy nhất cho một tệp dữ liệu, một tệp văn bản, hay một ảnh. Do đó, hàm Hash tạo ra có thể dùng làm định danh cho tệp dữ liệu, tệp văn bản, hay ảnh gốc đó.

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 thể nêu hai phương pháp điển hình nhất [18], đó là:

+ Phương pháp khai báo:

Người dùng tự nhập thông tin về danh định tức khai báo định danh. Đây là phương pháp phổ biến nhất hiện nay.

Ví dụ về thông tin định danh là tên người (username), số tài khoản hoặc tên tài khoản (account, account name).

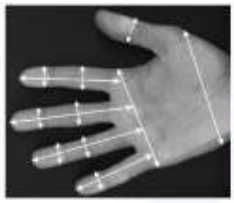
Để khai thác thông tin về định danh, kẻ tấn công có thể thực hiện như sau. Bước đầu tiên khi một hacker muốn xâm nhập vào một hệ thống là thu thập danh sách các người dùng hợp lệ của hệ thống sau đó dùng nó để tấn công hệ thống.

+ 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. Ví dụ như dữ liệu sinh trắc, dữ liệu về máy tính, các dữ liệu đặc trưng cho đối tượng khác.

- Danh định sinh trắc học (Biometric identity) có thể gồm:
  + Dữ liệu nhận dạng khuôn mặt (Facial recognition)
  + Dữ liệu Quét tròng mắt (Iris scanners)
  + Dữ liệu hình học bàn tay (Hand geometry)
  + Dữ liệu nhận dạng vân tay (Fingerprint)
  …

Dữ liệu sinh trắc còn có thể là bất kỳ dữ liệu nào khác của người dùng.


- Danh định máy tính, thiết bị (Computer identity) bao gồm:
  + Tên máy tính, tên thiết bị (ví dụ tên hãng, model, series,…)
  + Địa chỉ MAC (địa chỉ vỉ mạch kết nối mạng Internet)
  + Địa chỉ IP (địa chỉ giao thức Internet)
  ….
- Danh định số (Digital identity) gồm:
  + Chứng nhận số (Digital certificate)
  + 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. Xác thực là một hành động nhằm thiết lập hoặc chứng thực một cái gì đó (hoặc một người nào đó) đáng tin cậy. Trong an ninh máy tính, xác thực là một quy trình nhằm cố gắng xác minh nhận dạng số của phần truyền gửi thông tin trong giao thông liên lạc chẳng hạn như một yêu cầu đăng nhập. Phần gửi cần phải xác thực có thể là một người dùng sử dụng một máy tính, hay bản thân một máy tính hoặc một chương trình ứng dụng.

Mục đích của việc xác thực:

- Chứng minh danh định là hợp lệ và phù hợp với người dùng.
- Quyết định có cho phép người dùng truy cập vào tài nguyên của hệ thống hay không

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):

- Ví dụ:

  Password

  Số PIN (Personal Identification Number)

- Ưu điểm

  Tiện lợi

  Chi phí thấp

- Khuyết điểm

  Mức độ bảo mật phụ thuộc vào độ phức tạp của password

  Những vấn đề của password:

  Password yếu: dễ đoán (tên người dùng, ngày sinh nhật ,…)

  → Xây dựng chính sách password:

  - Độ dài
  - Có các ký tự đặc biệt (non-letter), có ký viết hoa, viết thường
  - Khác với username, các từ dễ đoán
  - Thay đổi password định kỳ

Cần cân bằng giữa: hacker khó đoán và người dùng có thể nhớ

Thu thập thông tin bất hợp pháp (Social engineering)

Các phần mềm gián điệp (spyware), keystroke logging

+ Những gì bạn có (Something you have)

- Thẻ thông minh (smart card): có bộ nhớ nhỏ và có khả năng thực hiện một vài tính toán
- Trong thẻ có lưu thông tin về người dùng và cả password.

  Người dùng có thể chọn những password phức tạp và thay đổi khi cần
- Địa chỉ MAC, địa chỉ IP

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

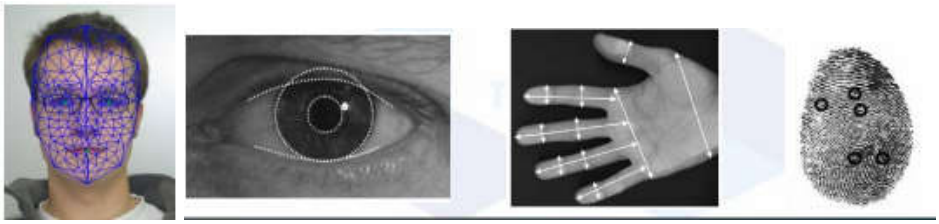
- Sử dụng các yếu tố sinh trắc học để xác thực.

  Nhận dạng khuôn mặt

  Quét tròng mắt

  Hình học bàn tay

  Nhận dạng vân tay



- Xác thực bằng sinh trắc học gồm 2 bước

  Đăng ký mẫu

  Nhận dạng
- Các lỗi xảy ra khi xác thực bằng sinh trắc học

Fraud rate: Tỷ lệ giả mạo, gian lận

False accept rate: Tỷ lệ chấp nhận sai sót

Insult rate: Tỉ lệ xúc phạm

False reject rate: Tỷ lệ từ chối sai sót

- Tỷ lệ lỗi sinh trắc học

  Fraud rate = Insult rate

  Vân tay (5%)

  Hình học bàn tay (0.1%)

  Tròng mắt (0.001%)

- Ưu điểm:

  Khó tấn công

- Khuyết điểm:

  Tốn kém: lưu trữ, xử lý

So sánh giữa các phương pháp xác thực, chúng ta có thể nhận thấy như sau:

+ Phương pháp xác thực tốt thì tốn kém

+ Phương pháp xác thực đơn giản thì có tốc độ nhanh hơn phương pháp phức tạp. Ví dụ, xác thực bằng mật khẩu nhanh hơn nhiều so với xác thực bằng sinh trắc học.
+ Hiệu quả của một phương pháp xác thực phụ thuộc vào độ phức tạp tính toán, tốc độ xác thực, tỷ lệ xác thực đúng/sai, khả năng tấn công.
Xét về khả năng bị tấn công, có thể thấy:
Biometrics < Smartcard < Password
Xét về chi phí:
Password < Smartcard < Biometrics
+ 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. Vì chỉ cần có secret key là có thể giải mã được, nên bên gửi và bên nhận cần làm một cách nào đó để cùng thống nhất về secret key.
- 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. Vì chỉ cần biết được secret key này thì bên thứ ba có thể giải mã được thông tin, nên thông tin này cần được bí mật truyền đi (bảo vệ theo một cách nào đó).

+ 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 (là hệ mật mã ra đời trước năm 1970) và mật mã hiện đại (ra đời sau năm 1970). Còn nếu dựa vào cách thức tiến hành mã thì hệ mật mã còn được chia làm hai loại là mã dòng (tiến hành mã từng khối dữ liệu, mỗi khối lại dựa vào các khóa khác nhau, các khóa này được sinh ra từ hàm sinh khóa, được gọi là dòng khóa) và mã khối (tiến hành mã từng khối dữ liệu với khóa như nhau).

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

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, người quản lý có thể sử dụng các báo cáo này để:

- Xác nhận việc tuân thủ quy định và chính sách
- Tiết kiệm chi phí tiềm lực bằng cách tìm nguồn dữ liệu dư thừa
- Xác định liên kết mạng diện rộng yếu và thắt cổ chai
- Xác định độ trễ mạng hoặc việc chuyển tải dữ liệu bị trễ
- Xác định sự bất thường trong mạng nội bộ.

Mỗi báo cáo của hệ giám sát có thể giúp nhà quản lý trả lời những câu hỏi khó khăn như:

- Giúp nhà thiết kế làm đơn giản hóa và đồng nhất hệ thống với chi phí thấp, giúp đưa ra quyết định thay thế các phân đoạn mạng với chi phí chấp nhận được.
- Hệ điều hành và các ứng dụng chạy trên server có cần thiết hay không?
- Mỗi máy trạm do ai sử dụng và lưu lượng băng thông của chúng?
- Làm thế nào để tăng hiệu suất của máy chủ?
- Thành phần nào trong mạng có dấu hiệu lỗi hoặc đang bị lỗi?
- Hệ thống có đang tận dụng triệt để tài nguyên?

Giám sát mạng cẩn thận cho phép nhà quản lý tất cả các thông tin họ cần để chứng minh việc nâng cấp mạng và mở rộng mạng là cần thiết để hỗ trợ doanh nghiệp thành công trong tương lai. Hệ giám sát mạng làm việc hiệu quả sẽ thông báo cho nhà quản lý

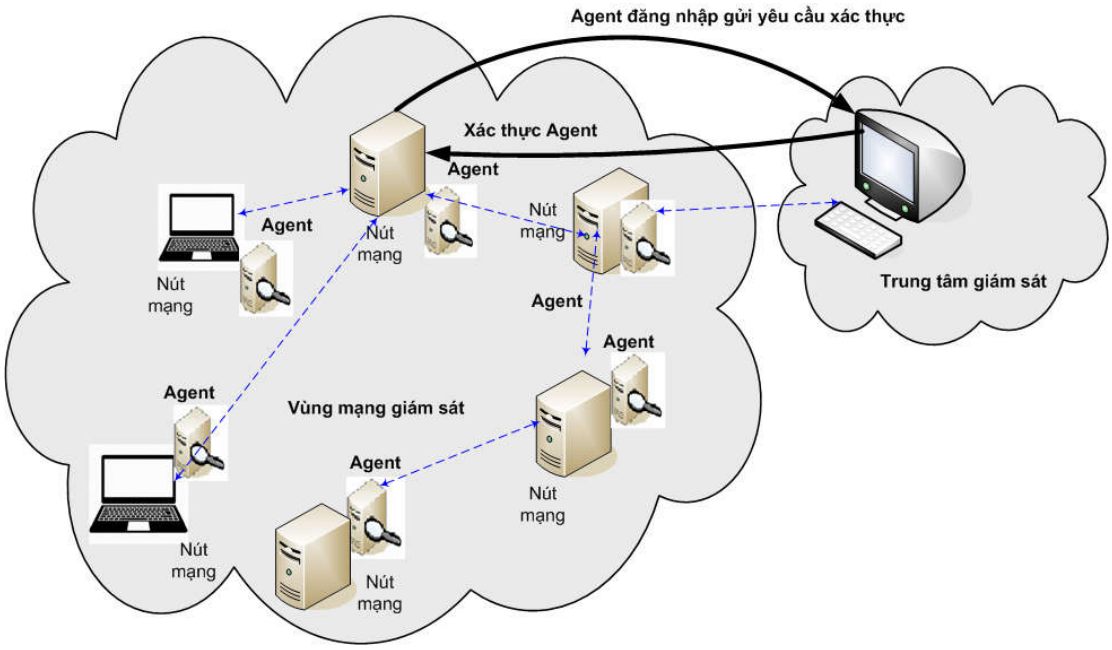
Đã có khá nhiều hệ thống giám sát mạng được phát triển và ứng dụng trong thực tiễn. Trong một hệ thống giám sát mạng tập trung, các Agent (là các máy trinh sát) làm nhiệm vụ thu thập thông tin về tình trạng hoạt động của các thiết bị và mạng. Các thông tin thu thập được chuyển về trung tâm giám sát để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

Một vấn đề, một Agent có thể là một máy do kẻ tấn công cài vào mạng, thực hiện thu thập thông tin và chuyển về cho kẻ tấn công. Vấn đề xác thực Agent hợp pháp không đặt ra là các Agent có thực sự là thành viên của hệ thống giám sát hay không? Nếu không có cơ chế xác thực phải luôn có trong mỗi hệ thống giám sát mạng hiện nay. Do vậy, một yêu cầu đặt ra là cần nghiên cứu giải pháp xác thực các Agent cho hệ thống giám sát mạng.

Ở luận văn này sẽ tập trung nghiên cứu về giải pháp xác thực dựa trên định danh cho các Agent trong hệ thống giám sát mạng.

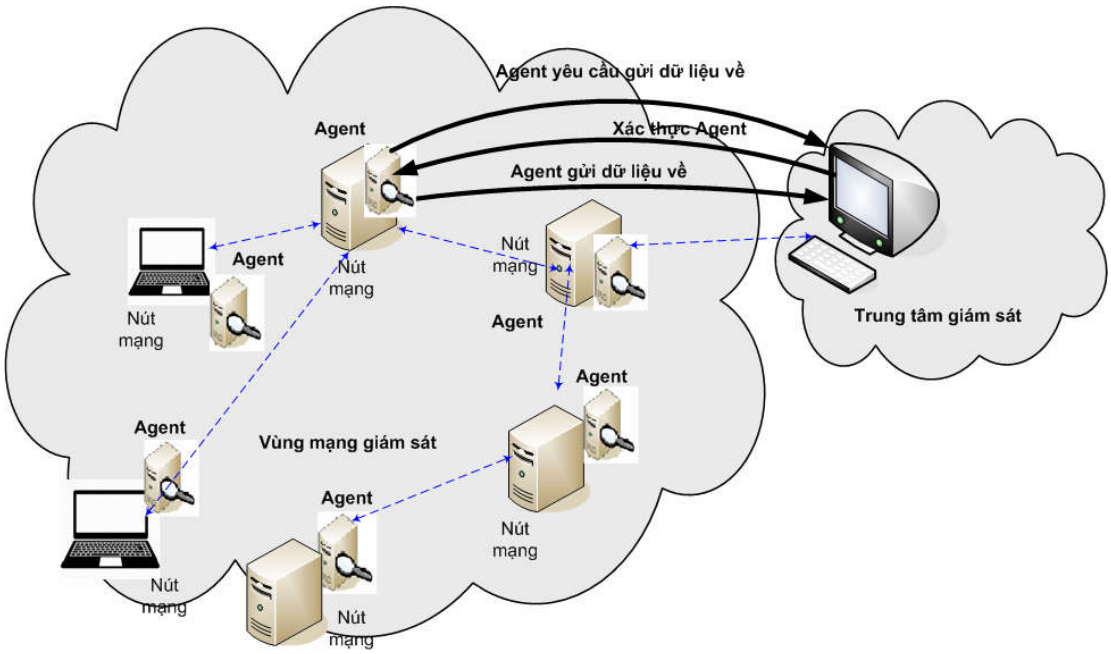
Hình 2.1 và 2.2 là sơ đồ kiến trúc tổng quát của một hệ thống giám sát mạng với các Agent và trung tâm giám sát. Các Agent làm nhiệm vụ thu thập dữ liệu liên quan đến hoạt động của các đối tượng được giám sát (máy chủ Web, máy chủ, máy trạm, router), các sự kiện tấn công và truyền về trung tâm giám sát. Hệ thống giám sát ở trung tâm làm nhiệm vụ: phân tích, phát hiện, cảnh báo và thống kê sự cố.

Trên hình 2.1 là sơ đồ hệ thống giám sát mạng tập trung với yêu cầu đăng nhập của Agent. Agent gia nhập vùng mạng giám sát (có thể được khai báo ban đầu, hoặc được cài đặt thêm vào mạng). Agent thực hiện gửi yêu cầu xác thực về trung tâm. Bước tiếp theo, trung tâm giám sát thực hiện việc xác thực Agent dựa trên thông tin về Agent có được. Nếu Agent là hợp lệ, trung tâm giám sát gửi xác thực tới Agent và lưu dữ liệu Agent đã xác thực tại trung tâm giám sát để quản lý.



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

Hình 2.2 là sơ đồ hệ thống giám sát mạng tập trung với Agent đã được xác thực sau khi gửi yêu cầu đăng nhập. Khi Agent thực hiện yêu cầu gửi dữ liệu thu thập được về trung tâm giám sát, bước xác thực Agent được diễn ra. Nếu quá trình xác thực thành công, trung tâm giám sát cho phép Agent gửi dữ liệu về. Nếu quá trình xác thực sai (Agent không phải là hợp pháp), Agent sẽ không được phép gửi dữ liệu. Khi đó Trung tâm giám sát sẽ phát hiện có một Agent giả mạo trên vùng mạng giám sát.



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

2.3. Định danh cho các Agent

Với một số lượng lớn các thiết bị tham gia vào việc giám sát trong mạng thì các chuyên gia bảo mật khuyến cáo một cách tiếp cận rất khác để bảo mật. Chúng ta cần đặt trọng tâm hơn vào việc xác định danh tính hay nói cách khác là định danh người dùng, thiết bị nếu chúng ta hi vọng giữ an toàn cho hệ thống.

Số lượng thiết bị và độ phức tạp của các tương tác: Khối lượng giao tiếp xảy ra giữa hàng ngàn thiết bị giám sát. Vì nó rất khác với bất kỳ thứ gì chúng ta đã thấy trước đây, nên rất khó lên kế hoạch trước. Các chuyên gia trong ngành và các quan chức chính phủ đang xem xét các tác động an ninh tiềm ẩn và đang nỗ lực để đảm bảo rằng các thiết bị được an toàn nhất có thể. Tuy nhiên, chúng ta sẽ thấy các tội phạm mạng nhắm mục tiêu và khai thác bất kỳ điểm yếu tiềm năng mới nào, điều này làm cho việc định danh trở nên thiết yếu.

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", ta có thể gán một tên (Machine Name) và một mật khẩu cho Agent như trong trường hợp trên.

Nếu sử dụng phương thức "What you have", ta có thể bổ sung một thẻ từ gắn với thiết bị và dùng dữ liệu của thẻ từ này để xác thực.

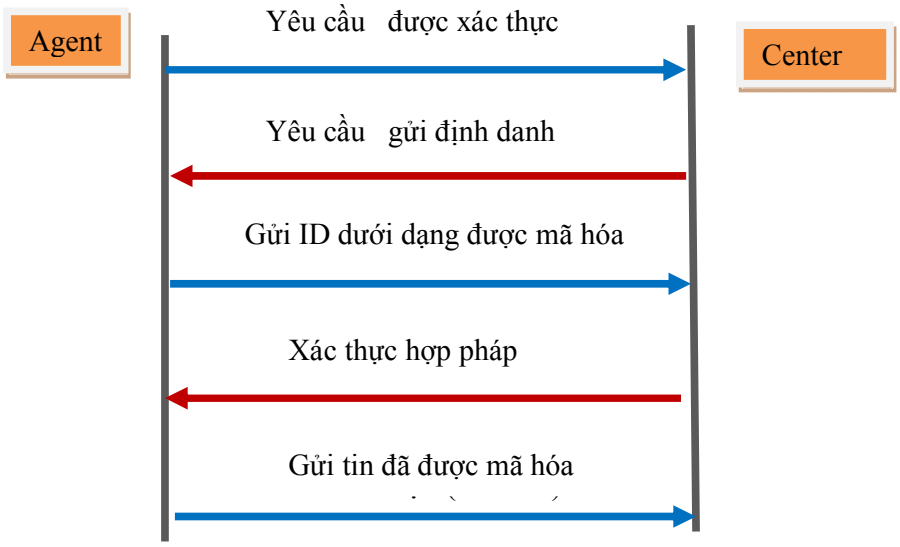
Nếu sử dụng phương thức "What you are", ta có thể sử dụng chính các dữ liệu có sẵn duy nhất của thiết bị (ví dụ như: mã hiệu, series sản xuất, địa chỉ MAC duy nhất,… của thiết bị) để xác thực.

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. Tuy nhiên, với mục đích là để mô tả giải pháp xác thực dựa trên định danh, luận văn sẽ không đi sâu vào các phương thức trên, mà giả thiết chỉ sử dụng dữ liệu định danh duy nhất có được đơn giản là thông qua tên máy và mật khẩu truy nhập.

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



Hình 2.3. Lược đồ mã hóa theo định danh

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)

Trong phần sau đây, luận văn sẽ 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:

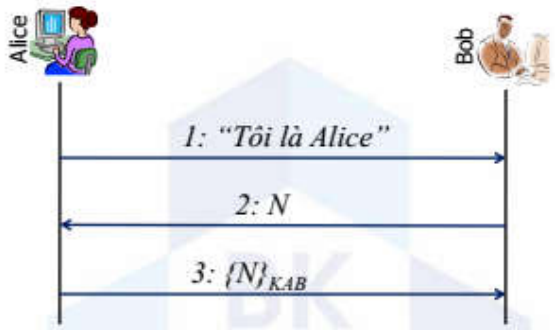
C: ciphertext (bản mã hóa cho bản tin M)

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

- Nhược điểm của việc sử dụng khóa bí mật:

Chỉ có Bob (Center) xác thực được Alice (Agent)

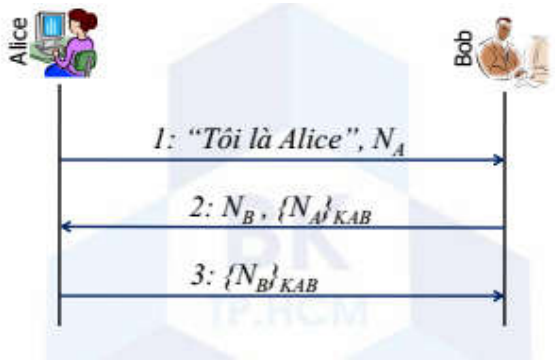
Alice (Agent) không biết có đúng là Bob (Center) không

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

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

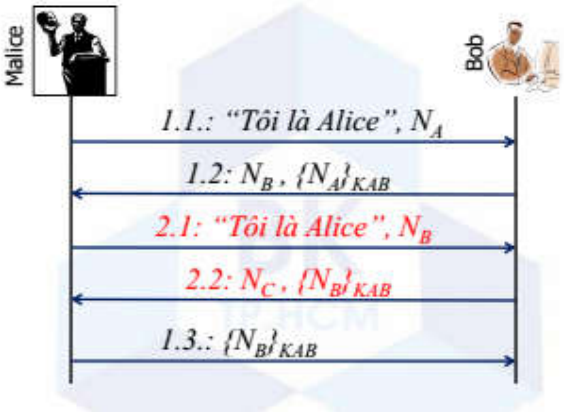
→Thông điệp ở bước 3 lặp lại từ bước 2: không thể xác thực người gửi

- 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:[6] 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. Giả sử chọn k = 3, ta có bảng chuyển đổi như sau:

Chữ ban đầu: a b c d e f g h i j k l m n o p q r s t u v w x y z

Chữ thay thế: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

(sau Z sẽ vòng lại là A, do đó x -> A, y -> B và z -> C)

Giả sử có bản tin gốc (bản rõ): Thank you very much

Như vậy bản tin mã hóa (bản mã) sẽ là: WLDQ BSX YHUB PXFK

Thay vì gửi trực tiếp bản rõ cho các cấp dưới, Ceasar gửi bản mã. Khi cấp dưới nhận được bản mã, tiến hành giải mã theo quy trình ngược lại để có được bản rõ. Như vậy nếu đối thủ của Ceasar có lấy được bản mã, thì cũng không hiểu được ý nghĩa của bản mã.

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

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

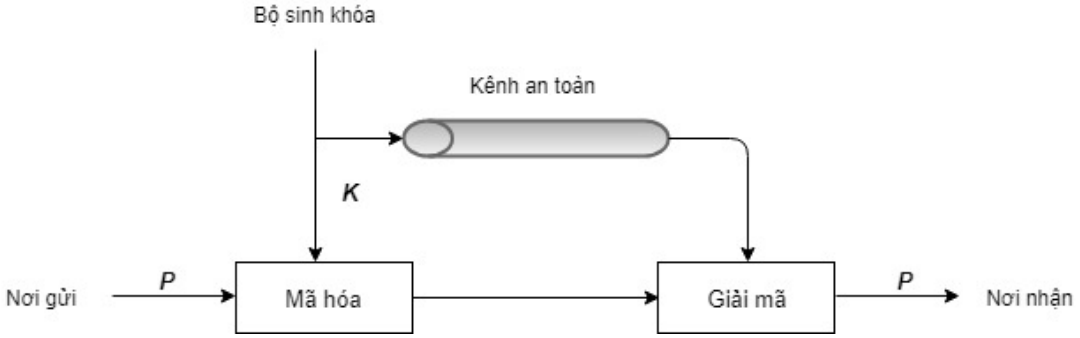
Phương pháp Ceasar được biểu diễn như sau: với mỗi chữ cái p thay bằng chữ mã hóa C, trong đó: $C = (p + k) \bmod 26$ (trong đó mod là phép chia lấy số dư)

Và quá trình giải mã đơn giản là: $p = (C - k) \bmod 26$

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 bất 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.

Bản mã C được gởi đi trên kênh truyền. Do bản mã C đã được biến đổi so với bản rõ P, cho nên những người thứ ba can thiệp vào kênh truyền để lấy được bản mã C, thì không hiểu được ý nghĩa của bản mã. Đây chính là đặc điểm quan trọng của mã hóa, cho phép đảm bảo tính bảo mật (confidentiality) của một hệ truyền tin.

Các đặc tính của mã hóa đối xứng:

- Tính bí mật của khóa: Mã hóa đối xứng đòi hỏi khóa phải được giữ bí mật giữa người gửi và người nhận trong quá trình truyền tin.
- Tính an toàn của hệ mã: Kẻ tấn công có thể dễ dàng suy ra được nếu tìm ra quy luật của hệ mã. Do đó một hệ mã hóa đối xứng được gọi là an toàn khi mã không bị phá hoặc vượt quá thời gian có thể phá mã.

Các thuật toán mã hóa đỗi xứng được chia làm hai loại là mã hóa luồng và mã hóa khối.

Mã hóa dòng: là loại mã hóa mà dữ liệu đầu vào sẽ được mã hóa từng đoạn bít có độ dài cố định với một chuỗi số ngẫu nhiên. Các thuật toán mã hóa luồng có tốc độ nhanh, thường được sử dụng trong các trường hợp khi khối lượng dữ liệu cần mã hóa không biết trước được.

Đặc điểm của mã hóa dòng

Kích thước một đơn vị mã hóa: Gồm k bít. Bản rõ được chia thành các đơn vị mã hóa có độ dài bằng độ dài của khóa:

$P \rightarrow p_o p_1 p_2 \dots p_{n-1}$ (p_i có độ dài k bit)

Bộ sinh dãy số ngẫu nhiên: Dùng một khóa K ban đầu để sinh ra các số ngẫu nhiên có kích thước bằng kích thước của đơn vị mã hóa:

$StreamCirpher(K) \rightarrow S = s_0 s_1 s_2 \dots s_{n-1}$ (s_i có độ dài k bit) và $s_0 = s_1 = s_2 = s_{n-1}$

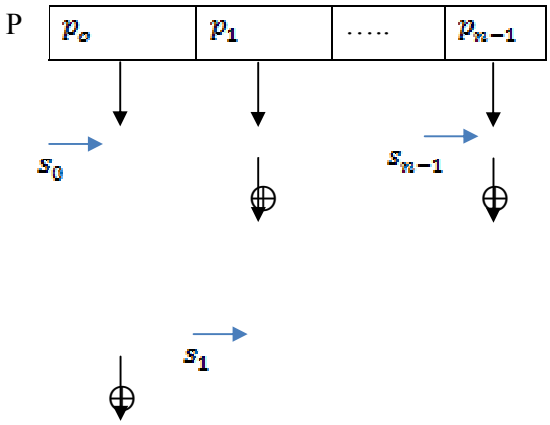
Bản mã: Gồm k bít. Mỗi đơn vị bản mã được tính bằng cách tính XOR một đơn vị mã hóa của bản rõ với khóa s.

$c_0 = p_0 \oplus s_0, c_1 = p_1 \oplus s_{1\dots} c_{n-1} = p_{n-1} \oplus s_{n-1}$

$C = c_o c_1 c_2 \dots c_{n-1}$ (c_i có độ dài k bit)

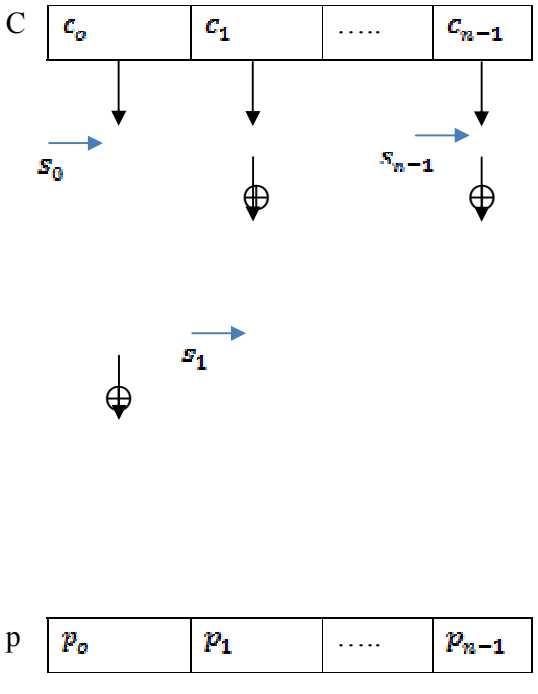
Quá trình mã hóa để tính bản mã C = P S và quá trình giải mã được thực hiện ngược lại, bản rõ P = C S. Quá trình mã hóa và giải mã được mô tả như hình sau:

Quá trình mã hóa



Hình 2.10. Quá trình mã hóa

Qúa trình giải mã



Hình 2.11. Mô hình mã hóa và giải mã dòng

Ta có thể thấy độ an toàn và tốc độ của mã hóa dòng phụ thuộc vào bộ sinh số ngẫu nhiên, nếu s_i có chiều dài ngắn thì dễ đoán, dễ vét cạn không đảm bảo an toàn, nếu s_i có chiều dài dài và độ dài bằng độ dài của bản tin P thì không thực tế và khó có thể thực hiện được. Vì vậy bộ sinh số của mã hóa dòng phải chọn độ dài hợp lý và cân bằng giữa hai điểm này nhưng vẫn phải đảm bảo độ dài an toàn cũng như độ ngẫu nhiên của dãy số S. Một số thuật toán dòng được sử dụng rộng rãi và phổ biến đó là: RC4, A5/1, A5/2, chameleon.

Mã hóa khối: Mã hóa luồng sử dụng XOR nên có một hạn chế đó là chỉ cần biết một cặp khối bản rõ và khối bản mã thì có thể suy ra được khóa và dùng nó để giải mã các khối bản khác. Vì vậy để chống phá mã người ta tìm cách làm cho P và C không có mối liên hệ về mặt toán học. Điều này chỉ thực hiện được khi ta lập được một bảng tra cứu ngẫu nhiên theo cặp các khối bản rõ và bản mã để mã hóa và giải mã

Ví dụ:

Bản rõ	**Bản mã**
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001

Hình 2.12. Ví dụ về mã hóa và giải mã khối

Có thể thấy, khóa là toàn bộ bảng trên, Các bên gửi và nhận phải biết tất cả bảng trên để có thể mã hóa và giải mã. Người phá mật mã, nếu biết một số cặp bản rõ và bản mã thì cũng chỉ biết được một phần khóa của bảng tra cứu trên, cũng không suy luận ra được các khối bản mã còn lại.

Tuy nhiên, mã khối an toàn lý tưởng là không thực tế và khả thi vì nếu kích thước khối lớn thì số dòng của bảng khóa cũng lớn và gây khó khăn cho việc lưu trữ cũng như trao đổi khóa giữa bên gửi và bên nhận. Giả sử kích thước khóa là 64 bít

thì số dòng của bảng khóa sẽ là 64 dòng và có 2^{64} bảng khóa có thể có. Một số thuật toán mã hóa khối trong hệ mã hóa đối xứng nổi tiếng và được sử dụng rộng rãi như: RC6, RC5, DES, 3-DES (Triple DES), AES, ECB, IDEA …

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

Trong phần sau đây, luận văn sẽ trình bày về giải pháp xác thực dựa trên việc sử dụng mã khóa bất đối xứng. Nguyên tắc chung tương tự như ở 2.5.1, nghĩa là 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) [6] là hệ mã hóa sử dụng một cặp khóa, được 2 nhà khoa học Diffie và Hellman đưa ra

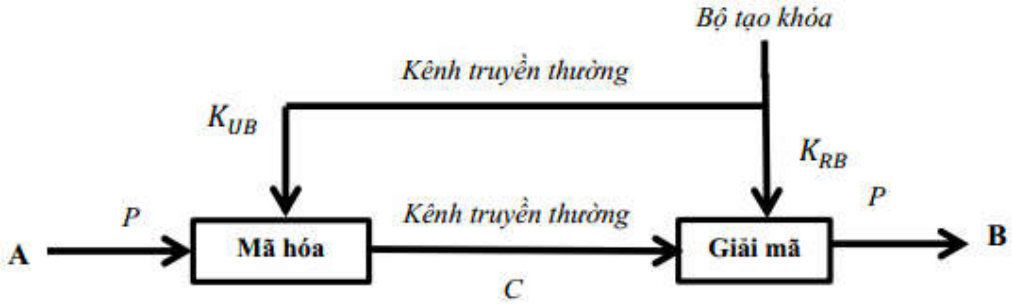
vào năm 1976. Hệ mã hóa này bao gồm một khóa dùng để mã hóa, còn gọi là khóa công khai (public key) và một khóa dùng để giải mã, còn gọi là khóa riêng (private key).

Vì vậy, hệ mã hóa bất đối xứng ra đời để giải quyết hai điểm yếu trên của mã hóa đối xứng. Trong hệ mã hóa này, hai khóa mã hóa và khóa giải mã là khác nhau, về mặt toán học thì từ khóa riêng có thể tính được khóa công khai nhưng từ khóa công khai khó có thể tính được khóa riêng. Khoá giải mã được giữ bí mật trong khi khoá mã hoá được công bố công khai. Một người bất kỳ có thể sử dụng khoá công khai để mã hoá tin tức, nhưng chỉ có người nào có đúng khoá giải mã mới có khả năng xem được bản rõ. Và khi cần chứng thực thì bên nhận sẽ dùng khóa bí mật của mình để mã hóa và bên gửi sẽ dùng khóa công khai để giải mã.

Giả sử khi A muốn gửi một thông điệp bí mật tới B, A sẽ 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)

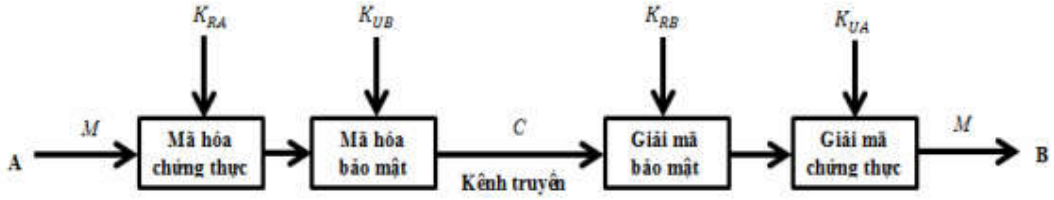
Trong đó:

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. Chỉ sử dụng duy nhất khóa công khai để mã hóa thông tin đối với các đối tượng khác nhau và số lượng đối tượng giao dịch không ảnh hưởng đến số lượng khóa.

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. Với cùng độ bảo mật, các thuật toán của hệ mã hóa bất đối xứng có khối lượng tính toán lớn hơn rất nhiều so với các thuật toán của hệ mã hóa đối xứng. 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 khác nảy sinh là khả năng dễ bị tấn công dạng kẻ tấn công người đứng giữa. Kẻ tấn công lợi dụng việc phân phối khóa công khai để giả mạo, thay đổi khóa công khai. Sau khi đã giả mạo được khóa công khai, kẻ tấn công đứng ở giữa 2 bên để nhận các gói tin, giải mã với cặp khóa công khai giả rồi lại mã hóa với khóa công khai đúng của nơi nhận và gửi đến nơi nhận để tránh bị phát hiện.

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 nhiên, các thuật toán của hệ mã hóa bất đối xứng có kích thước khóa mã hóa lớn làm tăng khối lượng tính toán nên nó khó được sử dụng độc lập. Vì vậy trong thực tế các mô hình bảo mật thường kết hợp các loại thuật toán với nhau để tận dụng các ưu điểm và hạn chế các điểm yếu. 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: Do cả bên gửi và bên nhận cùng dùng chung một khóa để mã hóa và giải mã nên cần phải giữ bí mật khóa này. 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. Điều này khó có thể thực hiện được và tốn kém chi phí để xây dựng được một kênh truyền an toàn.

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. Việc thử nghiệm được thực hiện trên cơ sở một công cụ mô phỏng hệ thống mạng có sẵn. Mạng giám sát được thiết lập bao gồm 1 nút mạng làm trung tâm giám sát, các nút mạng khác mô phỏng các Agent trong vùng mạng được giám sát. Quá trình xác thực được thực hiện trên cơ sở trao đổi thông tin định danh và sử dụng các phương thức mã hóa khóa bí mật và khóa công khai như đã trình bày trong chương 2.

Hiện nay có rất nhiều công cụ mô phỏng mạng khác nhau trên nhiều phương diện, có thể kể đến như là Contiki/Cooja, OPNET, QualNet, NS-2, NS-3, OMNet++, REAL, SSFNet,…Trong khuôn khổ luận văn này, phần tiếp theo chỉ xin giới thiệu một số công cụ mô phỏng điển hình.

3.1.1. Công cụ mô phỏng NS-2

NS-2 (Network Solution 2) [6] là phần mềm mô phỏng mạng điều khiển sự kiện riêng rẽ hướng đối tượng, được phát triển tại UC Berkely, viết bằng ngôn ngữ C++ và OTcl. NS-2 mô phỏng các chức năng và giao thức mạng có dây cũng như không dây (ví dụ: các thuật toán định tuyến, TCP, UDP).

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 mà gần như ta không thể thực thi được trong thực tế
- Khả năng mô phỏng nhiều loại mạng khác nhau

NS-2 là phần mềm mã nguồn mở và chạy ổn định trong cả 2 môi trường Windowns và Linux. NS-2 sử dụng 2 ngôn ngữ lập trình: ngôn ngữ lập trình hệ thống C++ và Ngôn ngữ kịch bản (OTcl - Object oriented Tool Command Language).

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. Những đối tượng trong chương trình mô phỏng có khả năng đưa các lưu lượng thực vào trong chương trình mô phỏng và đưa một phần lưu lượng trong 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. Việc này có nghĩa là về khả năng kiểm tra các thuật toán hoặc mô phỏng các thuật toán mới của NS-2 không bằng được so với các công cụ mô phỏng khác. Cũng theo báo cáo thì tốc độ tính toán của NS-2 cũng khá chậm. Đối với người mới bắt đầu sử dụng thì cũng rất khó và mất rất nhiều thời gian để tiếp cận phần mềm.

3.1.2. Công cụ mô phỏng OPNET

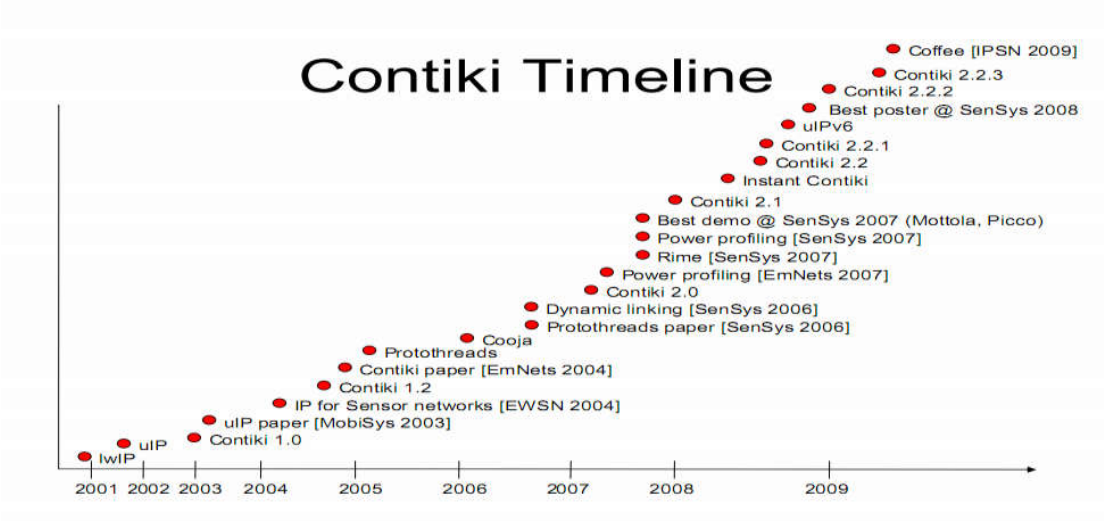
OPNET [6]là một công cụ mô phỏng mạng sự kiện mức cao. OPNET hỗ trợ mô phỏng mạng WSN tốt (cụ thể là tốt hơn NS2). Một đặc điểm nữa là OPNET tuy là phần mềm thương mại, nhưng miễn phí cho các trường Đại học hay Học viện. Và kể từ phiên bản 14.5 trở đi OPNET có hỗ trợ thư viện cho Zigbee. Tuy thư viện này không đầy đủ như bản miêu tả kỹ thuật của Zigbee Alliance 2006, nhưng rất phù hợp với các sản phẩm bán ra của các hãng như TI, Freescale, Atmel, hay Microchip… là chỉ hỗ trợ phương thức giao tiếp CSMA/CA không chia khe.

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 chương trình mô phỏng này 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 là hệ điều hành mã nguồn mở, được nghiên cứu, thiết kế và phát triển bởi một nhóm các nhà phát triển từ viện khoa học máy tính Thụy Điển, người đứng đầu là Adam Dunkels. Nhóm phát triển Contiki gồm nhiều thành

viên đến từ SICS, CISCO, cùng nhiều tổ chức và các trường đại học khác trên thế giới. Hệ điều hành Contiki được thiết kế cho các vi điều khiển có bộ nhớ nhỏ, với thông số 2KB RAM và 40KB ROM. Nhờ đó, Contiki được sử dụng cho các hệ thống nhúng và các ứng dụng trong mạng cảm biến không dây. Contiki bắt đầu được nghiên cứu từ năm 2001 và phát hành phiên bản đầu tiên Contiki 1.0 năm 2003. Hình 3.1 cho thấy lịch sử phát triển của Contiki trong những năm qua. Phiên bản hiện nay của Contiki là 2.4, với nhiều thay đổi, bổ sung và phát triển vượt bậc. Trong thực tế, Contiki đã được ứng dụng trong nhiều dự án như giám sát đường hầm xe lửa, theo dõi nước trong biển Baltic,… Nhiều cơ chế, ý tưởng trong Contiki đã được ứng dụng rộng rãi trong công nghiệp. Điển hình như mô hình uIP được phát hành năm 2001 đã được sử dụng trong hệ thống ứng dụng của hàng trăm công ty trong các lĩnh vực hàng hải, thông tin vệ tinh, khai thác dầu mỏ,…; mô hình Protothreads được công bố lần đầu tiên năm 2005, đến nay đã được sử dụng trong nhiều ứng dụng như bộ giải mã kỹ thuật số và thiết bị cảm biến rung không dây.



Hình 3.1. Lịch sử hệ điều hành Contiki

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:

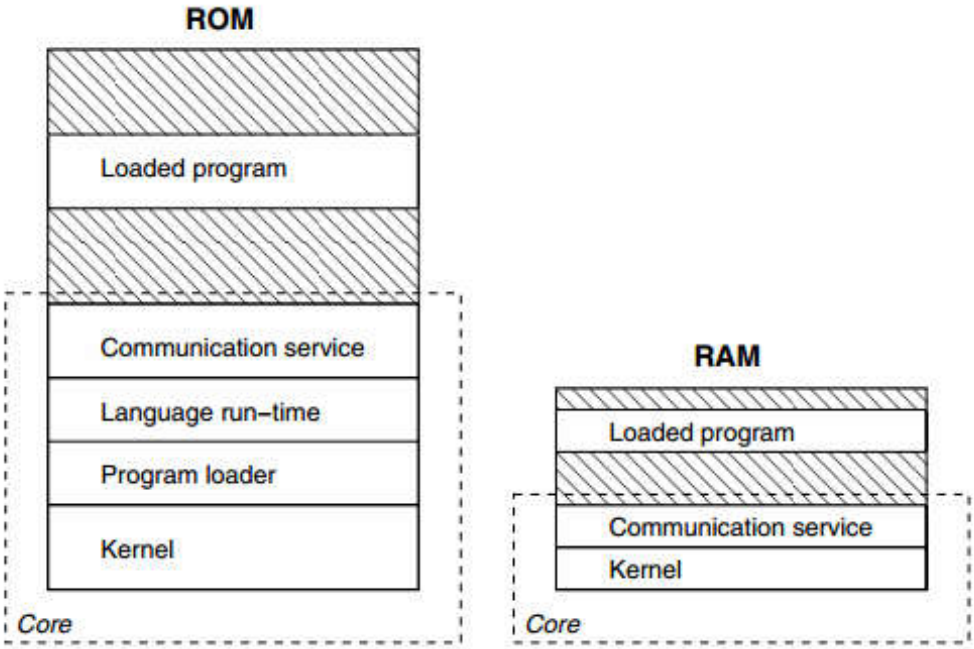
- Contiki được chia thành nhiều modul hoạt động độc lập. Nhờ đó các ứng dụng có thể sử dụng các modul một cách linh động và chỉ load những modul cần thiết.
- Cơ chế hoạt động điều khiển sự kiện làm giảm năng lượng tiêu hao và hạn chế dung lượng bộ nhớ cần sử dụng.
- Có thể sử dụng IP trong mạng cảm biến thông qua uIP stack được xây dựng dựa trên nền TCP/IP.
- Có những modul cho phép ước lượng và quản lý năng lượng một cách hiệu quả.
- Các giao thức tương tác giữa các lớp và các node trong mạng dễ dàng hơn.
- Sử dụng RIME stack phục vụ các giao thức dành cho mạng năng lượng thấp một cách hiệu quả.

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.



Hình 3.2. Phân vùng lõi và chương trình 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.

Hai sự kiện được nhân Contiki hỗ trợ là các sự kiện đồng bộ và các sự kiện không đồng bộ. Các sự kiện đồng bộ gửi ra ngay lập tức tới quy trình đích và đã được lên lịch trong khi các sự kiện không đồng bộ được sắp xếp và gưi đi sau đó.

Cơ chế bầu chọn trong nhân của Contiki bao gồm các sự kiện ưu tiên cao mà đã được lập lịch ở giữa mỗi sự kiện không đồng bộ. Nó sử dụng bởi các quy trình hoạt động gần phần cứng để nhận các cập nhật trạng thái.

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. Cấu hình Contiki tiêu chuẩn yêu cầu 2 kb RAM, 40 kb ROM, do vậy nó có hiệu suất bộ nhớ cao và cung cấp một bộ các quy tắc cấp phát bộ nhớ. Contiki hỗ trợ quản lý bộ nhớ động và liên kết động các chương trình, sử dụng quản lý cấp phát bộ nhớ với nhiệm vụ chính là giữ giải phóng bộ nhớ cấp phát từ việc phân mảnh bằng cách phân cụm bộ nhớ khi các khối được giải phóng.

Mạng IP đầy đủ: Contiki cung cấp cụm mạng IP đầy đủ, mỗi ứng dụng có thể sử dụng cả IPv4 và IPv6.

Nhận biết năng lượng: Contiki được thiết kết cho hệ thống năng lượng cực thấp mà nó có thể chạy cả năm với một đôi phi AA. Nó không cung cấp bất kỳ chức năng tiết kiệm năng lượng nào. Việc tiết kiệm năng lượng bằng cách đưa thiết bị về chế độ ngủ hoặc khác phải được thực hiện bởi các ứng dụng. Tuy nhiên Contiki cung cấp một cơ chế ước tính năng lượng hệ thống để xem vị trí mà năng lượng bị tiêu hao.

6LoWPAN, RPL, CoAP: Contiki hỗ trợ các giao thức IETF chuẩn hiện nay cho mạng IPv6 công suất thấp: Giao thức định tuyến đa bước nhảy 6LoWPAN, RPL, và giao thức tầng ứng dụng an toàn CoAP.

RPL là giao thức định tuyến được thiết kế cho các mạng tổn hao công suất thấp LLNs (Low Power And Lossy Networks) với các nút mạng có tài nguyên hạn chế và được kết nối với nhau bởi các liên kết tổn hao (dễ bị mất mát bản tin).

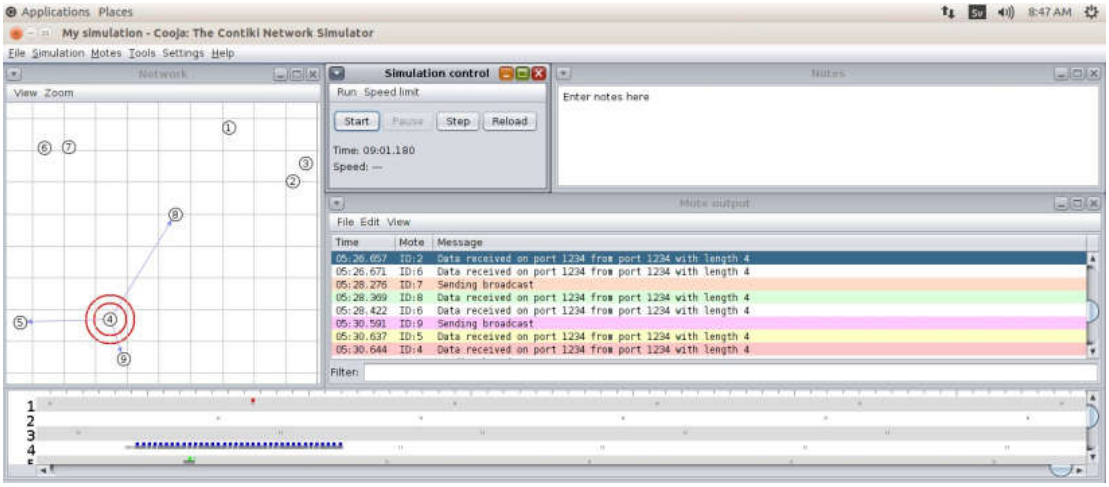
Mô phỏng mạng Cooja: Cooja là mô phỏng mạng cung cấp bởi hệ điều hành Contiki. Có nhiều kiểu mote khác nhau có thể được mô phỏng ở mức phần cứng, cho phép ngươi dùng kiểm tra hành vi chính xác của mạng.

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.

Dưới đây là giao diện của chương trình mô phỏng bằng Cooja:



Hình 3.3. Giao diện chương trình Cooja

Từ hình có thể nhận thấy giao diện của chương trình thân thiện và dễ sử dụng, với một màn hình cho phép hiển thịc các quá trình hoạt động của node, có khả năng thay đổi vị trí, phạm vi phủ sóng của mỗi node. Bên cạnh đó Cooja cung cấp một số các cửa sổ theo dõi sự kiện như Log listener, Radio listener cho phép người sử dụng tìm kiếm những sự kiện theo một số thông số nhất định, theo dõi sự giao tiếp giữa một số node cụ thể, ….Có thể nói, đây là một công cụ mô phỏng khá trực quan và dễ sử dụng, phục vụ tốt cho quá trình nghiên cứu, mô phỏng, đánh giá.

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

Truyền thông tin bảo mật đã phát triển từ rất sớm và có nhiều giải pháp khác nhau để bảo đảm bảo thông tin từ người gửi đến người cần nhận được an toàn bảo mật. Tuy nhiên các giải pháp bảo mật truyền thống nhiều khi khó áp dụng vào các nút mạng do các nút này được thiết kế nhỏ, bộ nhớ ít, pin có hạn và năng lực xử lý hạn chế.

Mô hình truyền tin bảo mật đối với các nút mạng cũng vì thế cần phải thiết kế gọn nhẹ nhưng vẫn đảm bảo bảo mật cơ bản của một hệ truyền tin truyền thống. Mã hóa đối xứng được lựa chọn trong mô hình này vì một số đặc tính sau:

- Mã hóa đối xứng khá gọn nhẹ, tính toán nhanh.
- Mã hóa đỗi xứng vẫn đảm bảo được tính bảo mật, chứng thực, toàn vẹn, tính không từ chối 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:

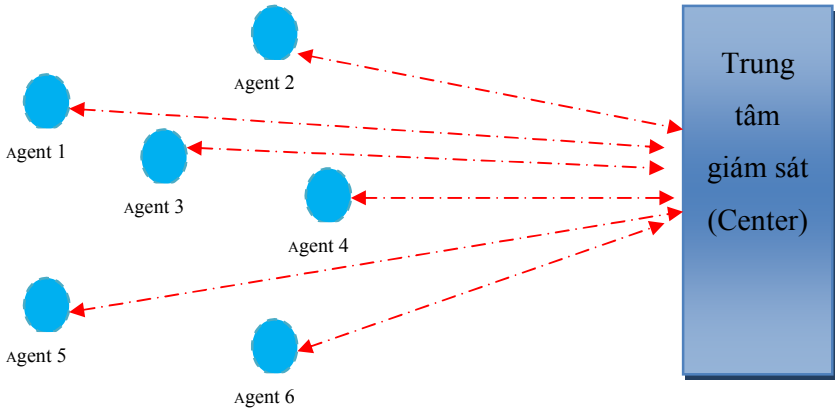
- Bên gửi: Nút S (Agent)
- Bên nhận: Nút R (Center)
- Bản tin cần rõ: M (Message)
- Bản tin mã hóa: S (Symmetric)
- Khóa: K (Key)

Trước khi có thể truyền tin thu thập được về trung tâm giám sát. Agent cần chứng minh được mình là một thành phần hợp pháp của hệ thống giám sát:

Agent gửi yêu cầu xác thực về trung tâm, khi đó trung tâm sẽ yêu cầu Agent gửi ID (định danh) để xác thực.

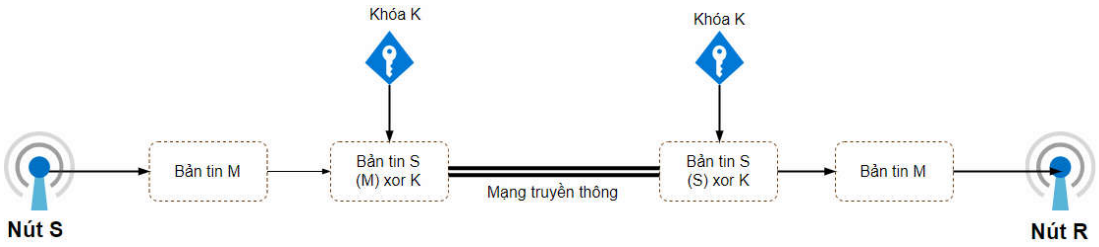
Agent muốn gửi ID đến (Center), nó sử dụng khóa bí mật K để mã hóa ID thành S và gửi qua Mạng truyền thông. Khi Đến phía server, nó sử dụng khóa bí mật K đã biết trước để giải mã S thành ID ban đầu sau đó kiểm tra xem ID đó có tồn tại trong hệ thống không

Nếu có nó sẽ gửi tin báo cho Agent và cho phép truyền tin. Agent sẽ gửi tin thu thập được về trung tâm dưới dạng đã được mã hóa.



Hình 3.4.. Sơ đồ hệ thống mạng giám sát với nhiều Agent và một trung tâm

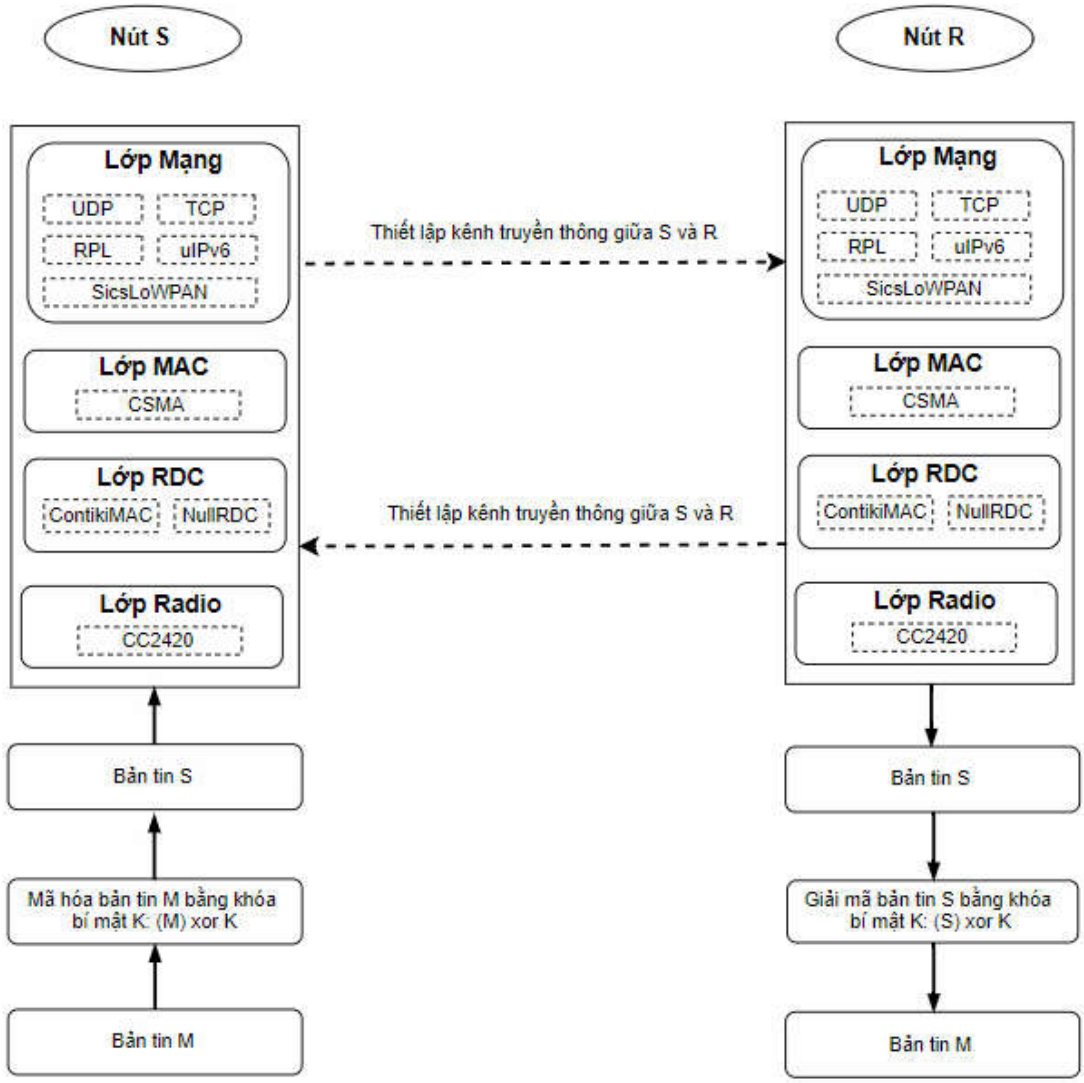
Mô hình mô phỏng truyền tin bảo mật: Nút mạng S (Agent) muốn gửi bản tin M đến Nút mạng R (Centers), nó sử dụng khóa bí mật K để mã hóa bản tin M thành bản tin S và gửi qua Mạng truyền thông. Khi Đến phía nút mạng R, nó sử dụng khóa bí mật K đã biết trước để giải mã bản tin S thành bản tin M ban đầu.



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)

σ

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

Sau khi Agent gửi yêu cầu được xác thực về trung tâm và trung tâm yêu cầu Agent gửi định danh chứng minh là thành phần hợp pháp của hệ thống giám sát. Agent sẽ gửi về trung tâm ID đã được mã hóa. ID đã được mã hóa sẽ đi từ tầng ứng dụng tầng trên xuống tầng Mạng truyền đi qua lớp Mac, lớp RDC và lớp Radio về Center. Tại Center thông tin về ID mà Agent gửi sang sẽ đi từ tầng Mạng đến tầng ứng dụng qua lớp Mac, RDC và Radio để giải mã và đối chiếu với các ID có trong

hệ thống. Nếu tồn tại ID mà Agent vừa gửi sang thì Center sẽ trả lời xác thực và cho phép truyền tin

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

Agent gửi thông tin đã thu thập được dưới dạng mã hóa về trung tâm từ trình ứng dụng xuống tầng Mạng truyền đi qua lớp Mac, lớp RDC và lớp Radio về Center. Tại Center thông tin mà Agent gửi sang sẽ đi từ tầng Mạng đến tầnng ứng dụng qua lớp Mac, RDC và Radio để giải mã phân tích và xử lý.

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

Bước 1: thiết lập kênh truyền thông giữa Agent và trung tâm giám sát.

Bước 2: Thiết lập Agent ID key

Bước 3: Mã hóa bằng mã đối xứng cho Agent ID key và gửi đến máy chủ

Bước 4: Máy chủ giải mã "Agent ID key" bằng khóa đối xứng và kiểm tra "Agent ID key"có chính xác không

Bước 5: Nếu xác thực thành công cho phép truyền tin từ Agent tới trung tâm. Nếu xác thực thất bại Agent không được phép truyền tin về trung tâm giám sát

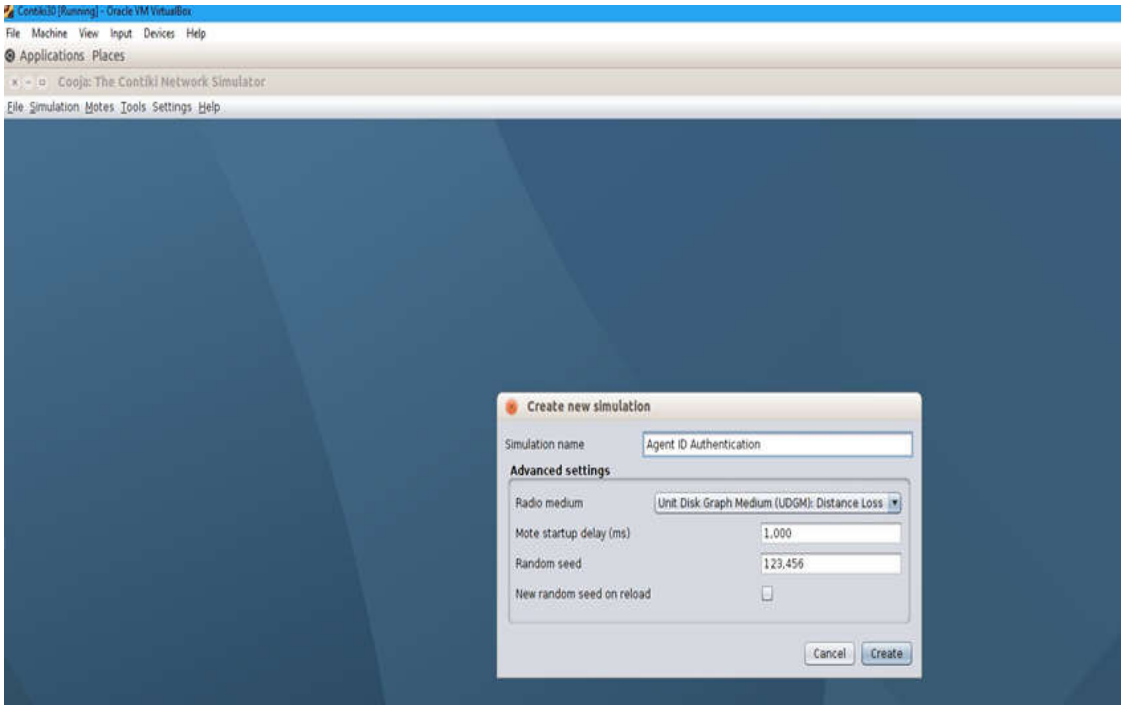
3.4. Các kết quả thử nghiệm

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

Công cụ thực hiện mô phỏng: Để mô phỏng xác thực dựa trên mã hóa định danh cho các agent trong mạng giám sát tập trung, trong khuôn khổ luận văn này xin đề cập đến việc sử dụng công cụ Cooja trên hệ điều hành Contiki để mô phỏng.

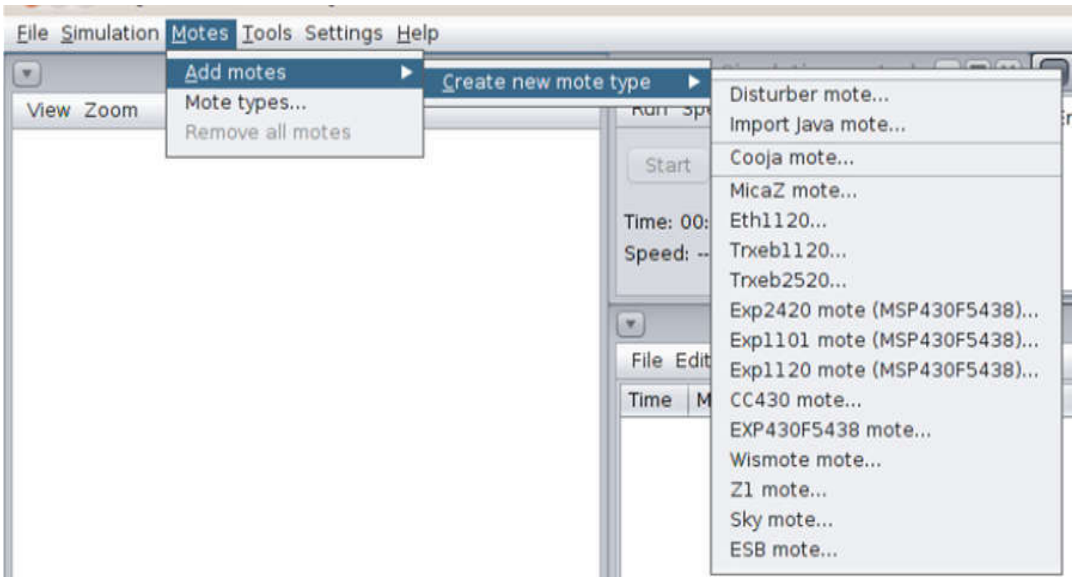
Quá trình thực hiện: Trong quá trình thực hiện mô phỏng sẽ sử dụng 1 Agent và một Server (Trung tâm giám sát) để truyền tin sử dụng mã hóa đối xứng phân tích và đánh giá kết quả, trong đó có một nút gửi là Agent và nút nhận là Server

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.



Hình 3.7. Tạo mới một chương trình mô phỏng

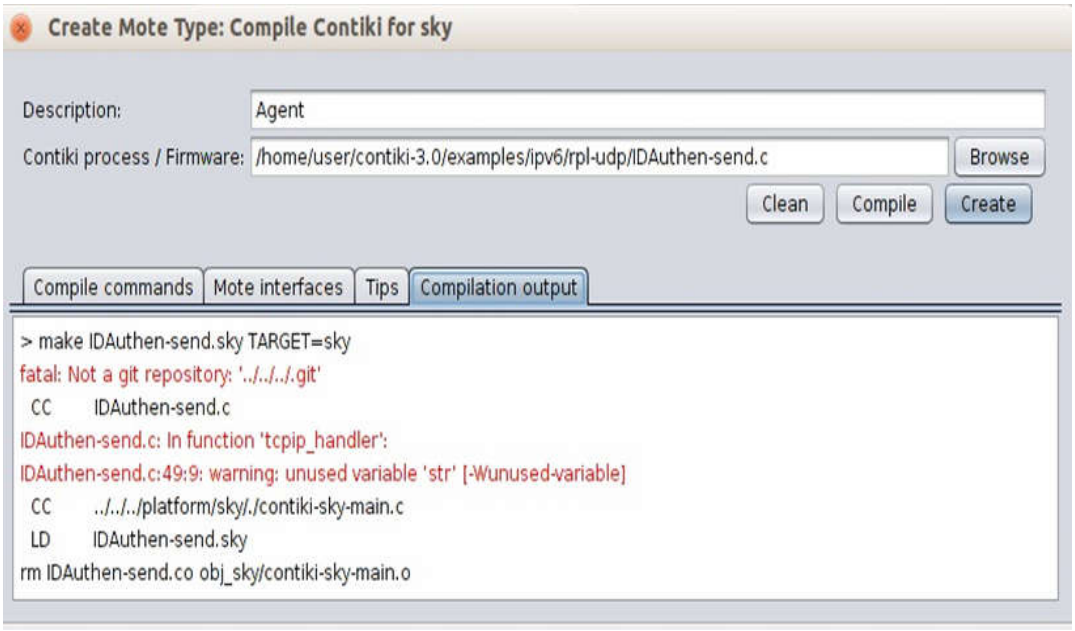
Tạo Agent: Trong cửa số Applications Places ta chọn Motes/ Add motes/ Create new mote type/ Sky mote.



Hình 3.8. Tạo mote mới

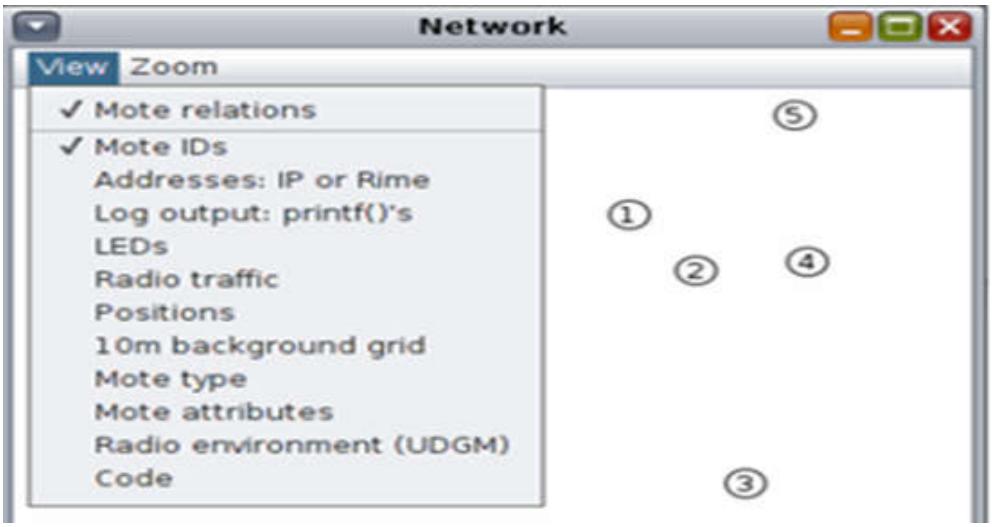
Khi đó sẽ xuất hiện cửa số Create mote type: Contiki for sky. Tại đây ta đặt tên cho mote mới tại Description là Agent tiếp theo chọn Browse khi đó xuất hiện cửa sổ để ta lựa chọn:Home/user/contiki -3.0/examples/ipv6/rpl-udp/IDAuhen-Send.c

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



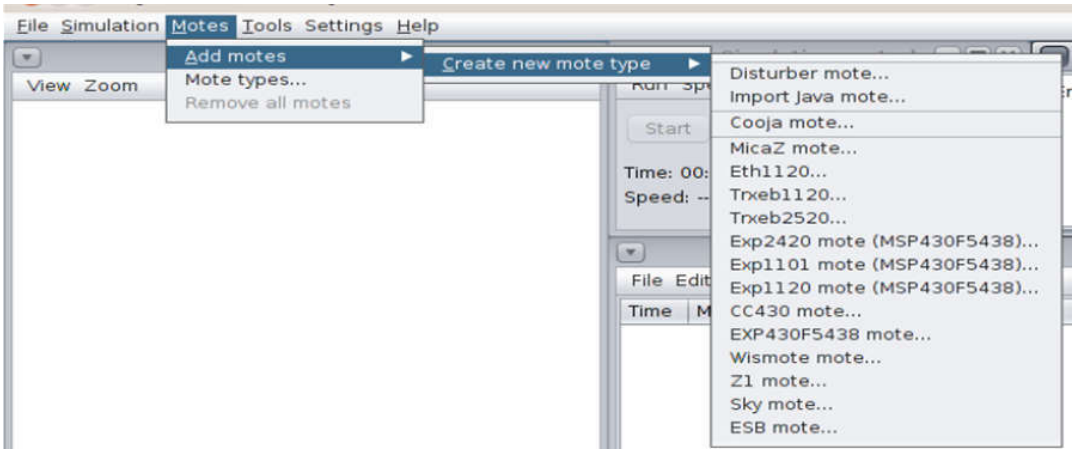
Hình 3.9. Tạo Agent

Tiếp theo click View và lựa chọn cách hiển thị cho các Agent



Hình 3.10. Chọn cách hiển thị các Agent

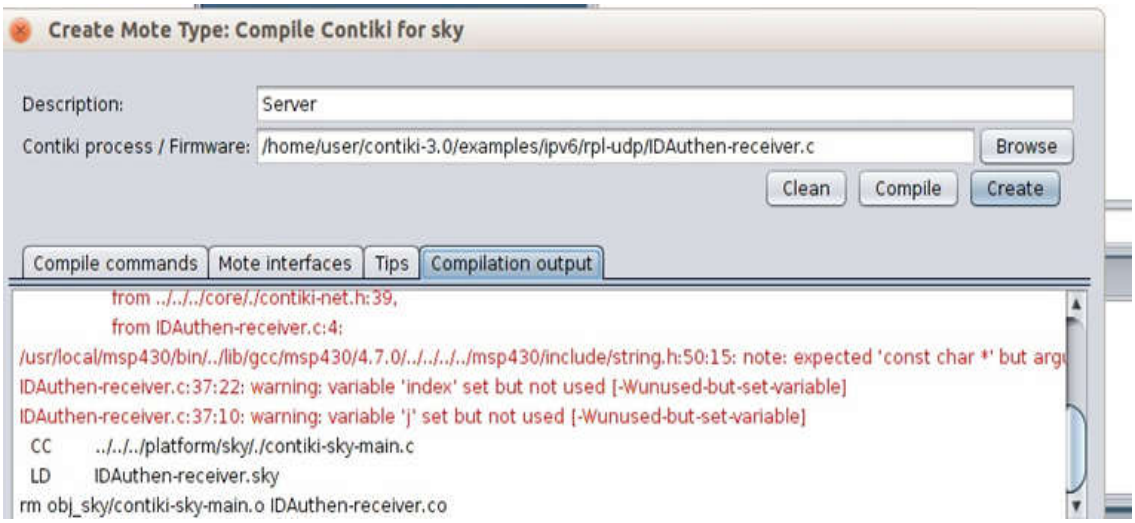
Tạo Server: Tương tự tạo Agent, Trong cửa số Applications Places ta chọn Motes/ Add motes/ Create new mote type/ Sky mote.



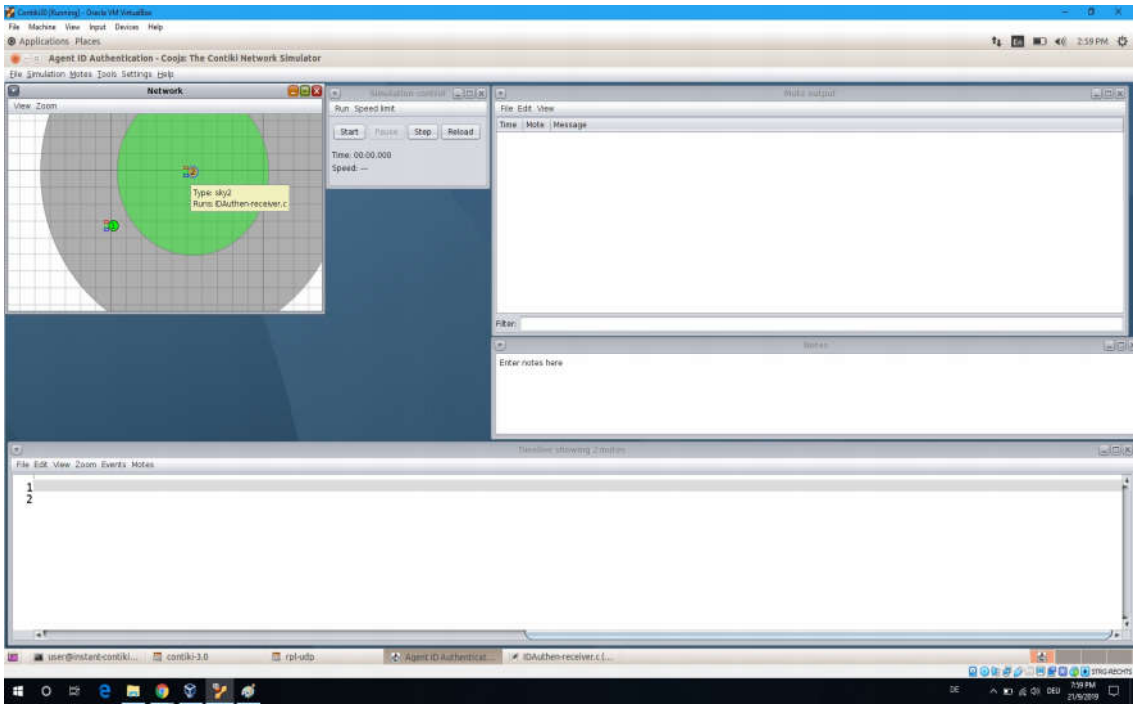
Hình 3.11. Tạo mote mới

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

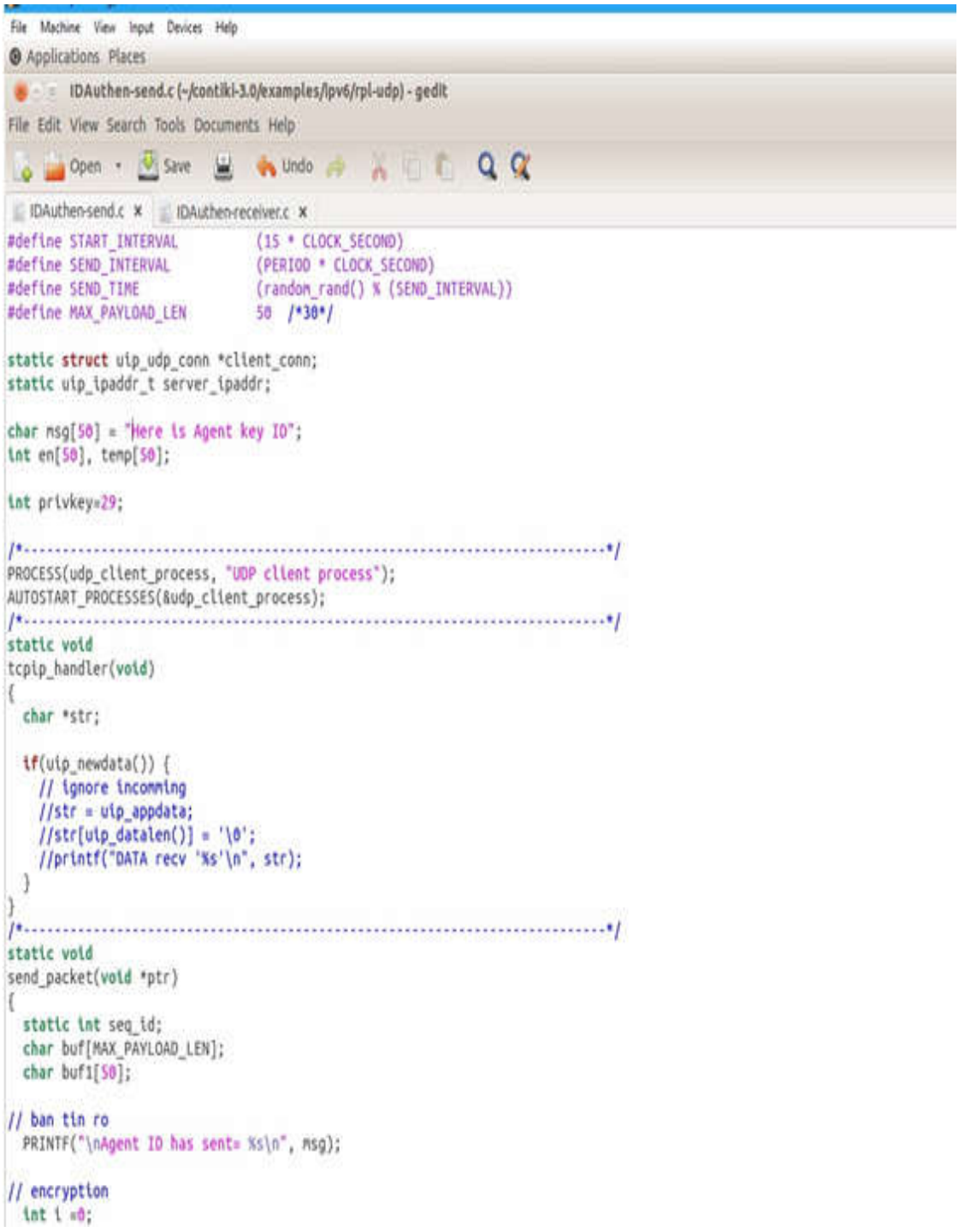


Hình 3.12. Tạo Server



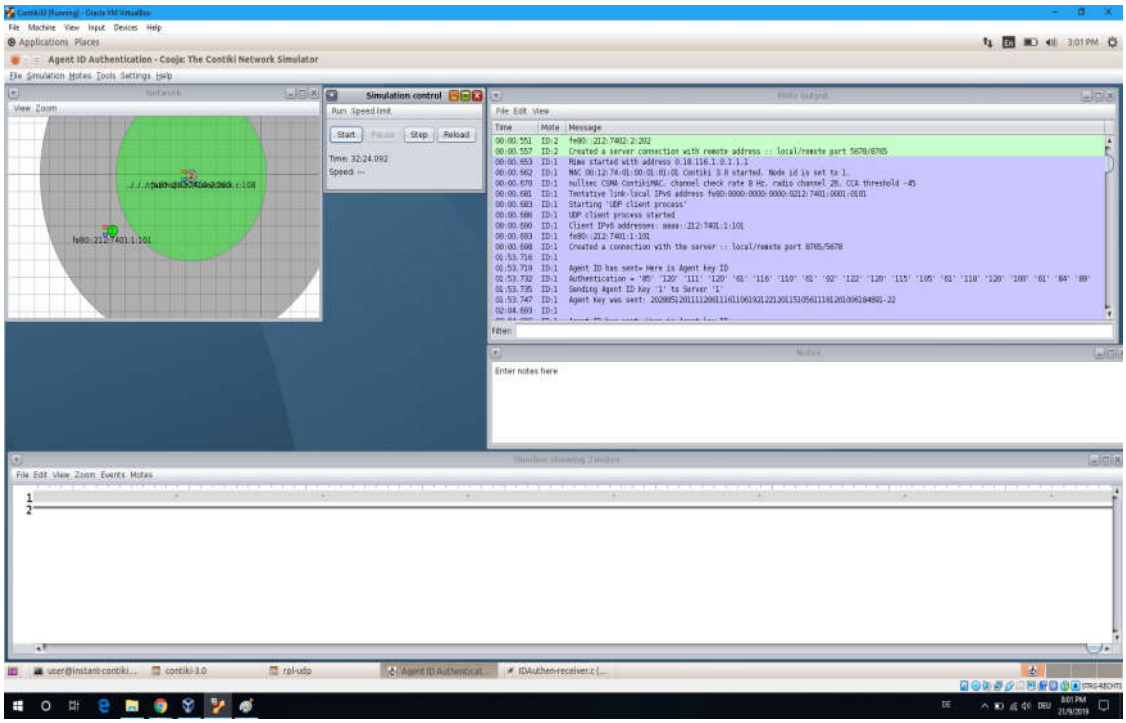
Hình 3.13. Hai mote được tạo để thực hiện mô phỏng: 1= Agent, 2 = Server

Chương trình của nút gửi và nhận như sau:

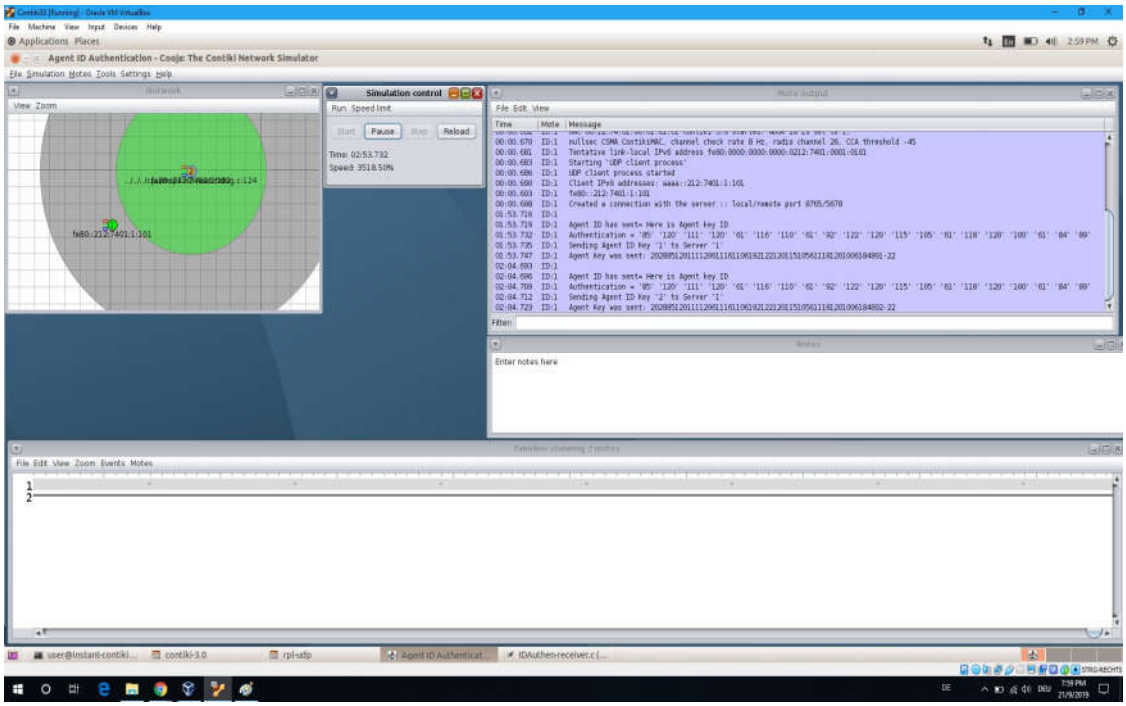



```
static struct uip_udp_conn *server_conn;

PROCESS(udp_server_process, "UDP server process");
AUTOSTART_PROCESSES(&udp_server_process);
/*---------------------------------------------------------------------------*/
static void
tcpip_handler(void)
{
  char *appdata;
  int dn[50];
  int i, j=0, len=0, index, seqNo=0;
  int privkey=29;

  if(uip_newdata()) {
    appdata = (char *)uip_appdata;

    index = uip_datalen(); // index=chieu dai ca goi tin
    len = appdata[0]; // len=do dai ban tin msg
]
    for(i=0; i<len; i++)
      {
        dn[i]=appdata[i+2]^privkey;
      }

    dn[i]='\n';
    j = strlen(dn);
    seqNo = appdata[i+2];

    PRINTF("\nAccept Agent ID Key '%d' from Agent '%d':\n", seqNo, UIP_IP_BUF->srcipaddr.u8[sizeof(UIP_IP_BUF->srcipaddr.u8) - 1]);

    PRINTF("Ma nhan duoc = ");
    for(i=0; i<len+4; i++)
      {
        PRINTF("%d", appdata[i]); // ban tin ma hoa nhan duoc
      }

    PRINTF("\nAgent ID Key was authenticated = ");
       for(i=0; i<len; i++)
         {
           printf("%c", dn[i]);
```

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.

Một giải pháp xác thực dựa trên định danh cho các Agent trong hệ thống giám sát mạng sẽ đóng vai trò rất quan trọng trong việc phát hiện, cảnh báo tấn công xâm nhập bất hợp pháp vào hệ thống. Nhờ có cảnh báo sớm về Agent giả mạo, chúng ta có thể xác định được địa chỉ nơi cài đặt Agent, nguy cơ gây ra sự cố và cô lập Agent giả mạo đó để giảm thiểu tối đa những thiệt hại mà kẻ tấn công gây ra.

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.

PHỤ LỤC

Hướng dẫn cài đặt và sử dụng hệ điều hành Contiki/ Cooja

1. Tải hệ điều hành Contiki/Cooja và VMware Player

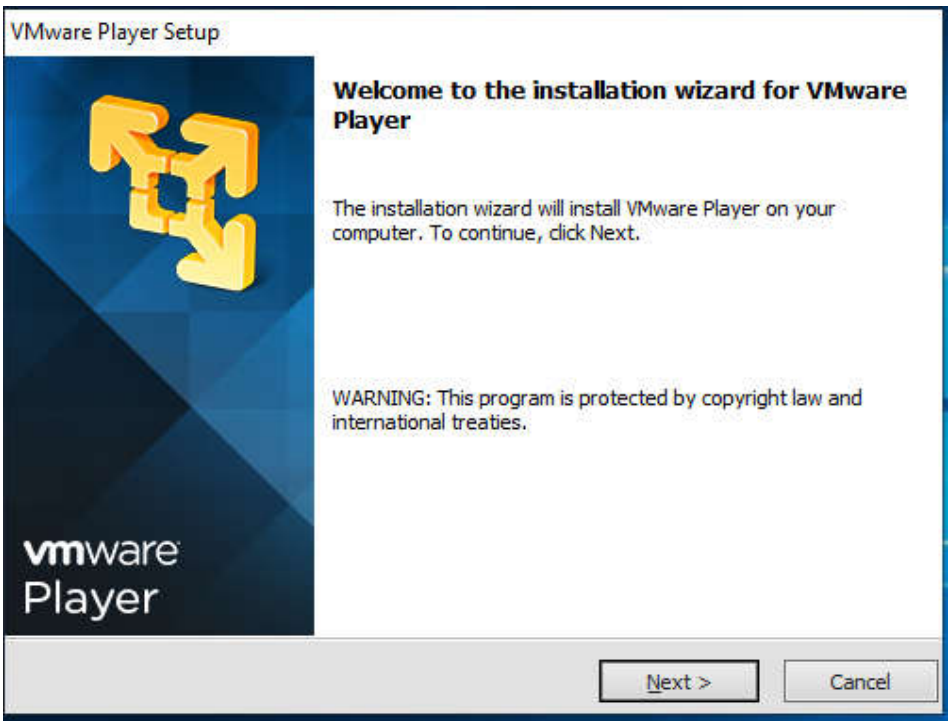
Tải hệ điều hành Contiki/Cooja từ trang chủ: http://www.contiki-os.org/

Tải phiên bản VMware Player tại địa chỉ :

https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_player/6_0

2. Cài đặt VMware Player:

Sau khi tải tệp về máy tính, nháy đúp chuột vào file "*VMware-player-6.0.7-2844087.exe*" để tiến hành cài đặt.

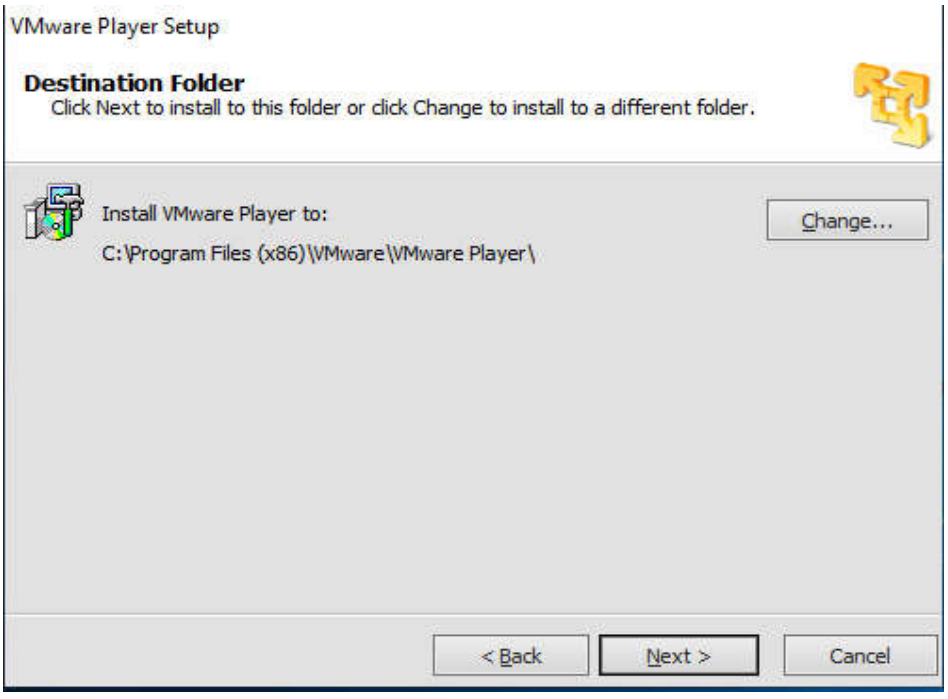


Hình 1. Cửa sổ cài đặt 1

Tiếp theo chọn "*Next*"

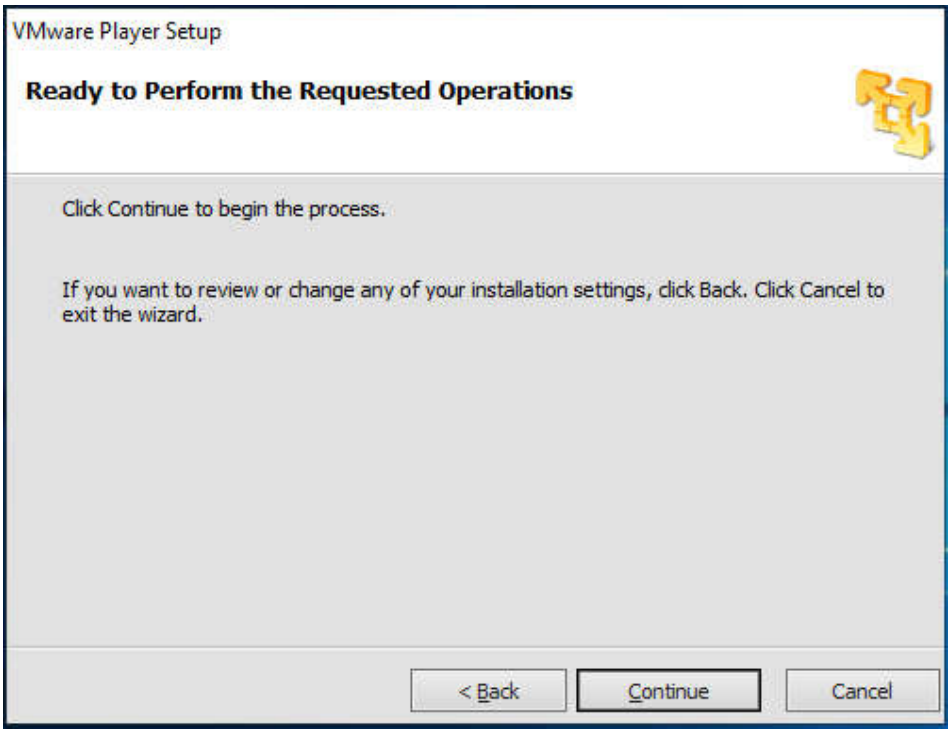
Hình 2 . Cửa sổ cài đặt 2

Bấm chọn "*I accept the terms in the license agreement*" và chọn "*Next*"



Hình 3 . Cửa sổ cài đặt 3

Chọn "*Next*", và bấm "Next" một số bước tiếp theo.

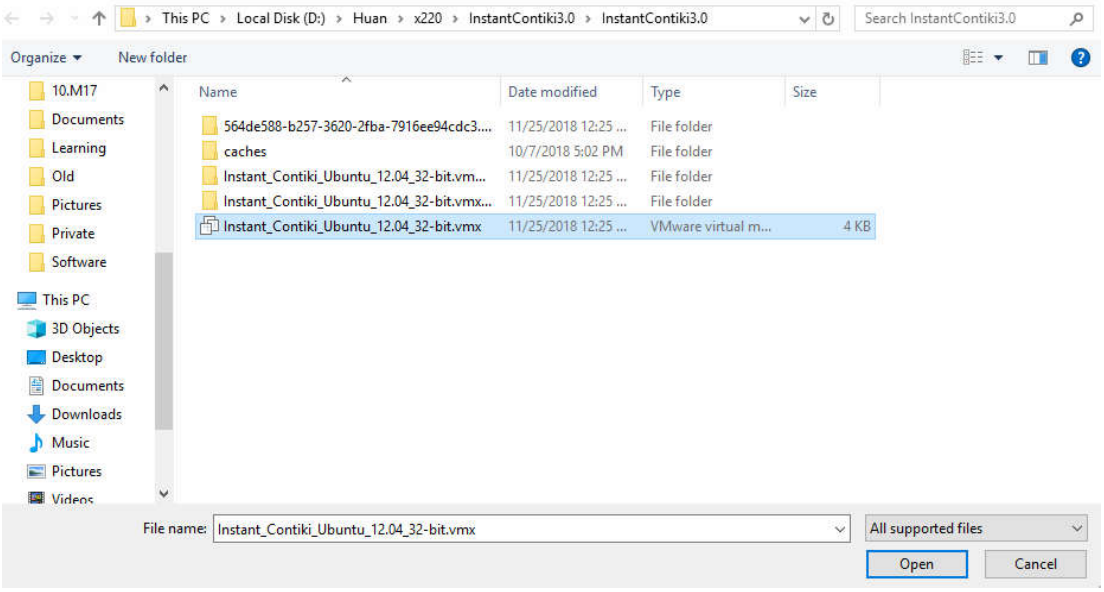


Hình 4 . Cửa sổ cài đặt 4

Bấm "*Continue*" để tiếp tục quá trình cài đặt và bấm *"Finish"* để kết thúc.

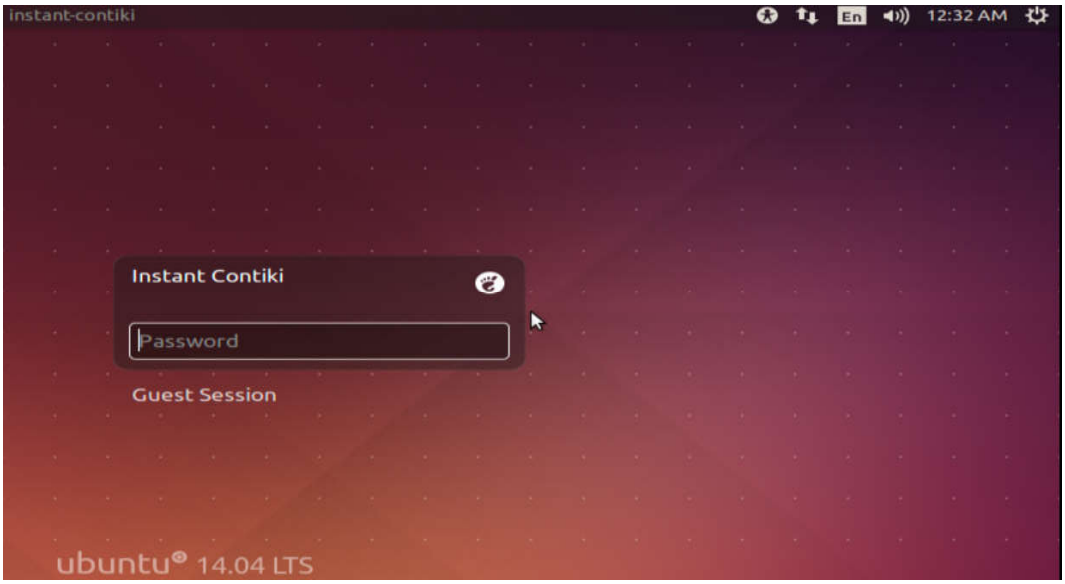
3. Chạy hệ điều hành Contiki/Cooja trên máy ảo VMware Player.

Giải nén và mở file “Instant_Contiki_Ubuntu_12.04_32-bit.vmx”



Hình 5. Mở tệp chạy Contiki/Cojja

Màn hình Ubuntu xuất hiện như sau:

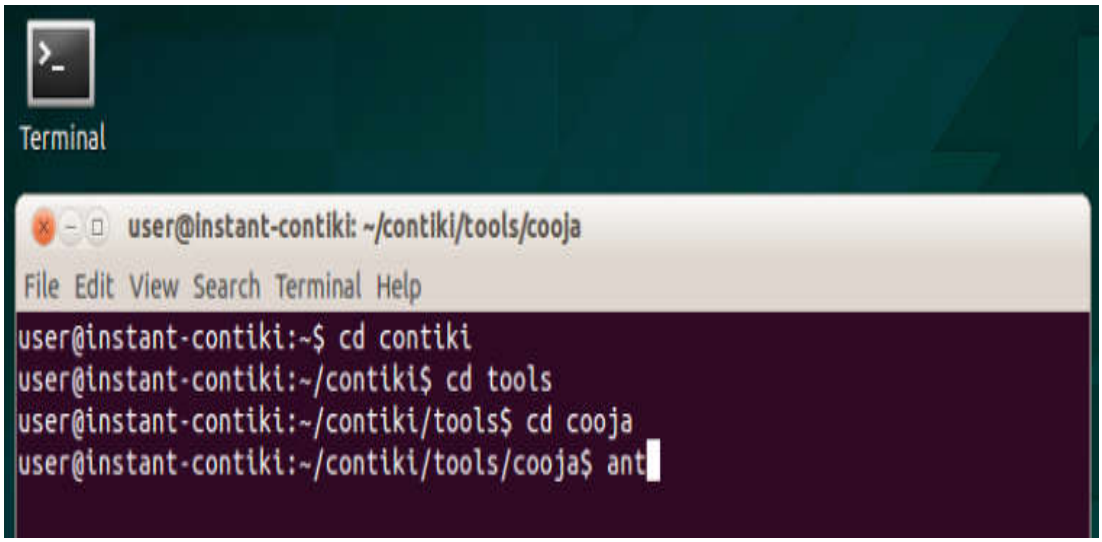


Hình 6. Màn hình chào mừng của Ubuntu 14.04 LTS

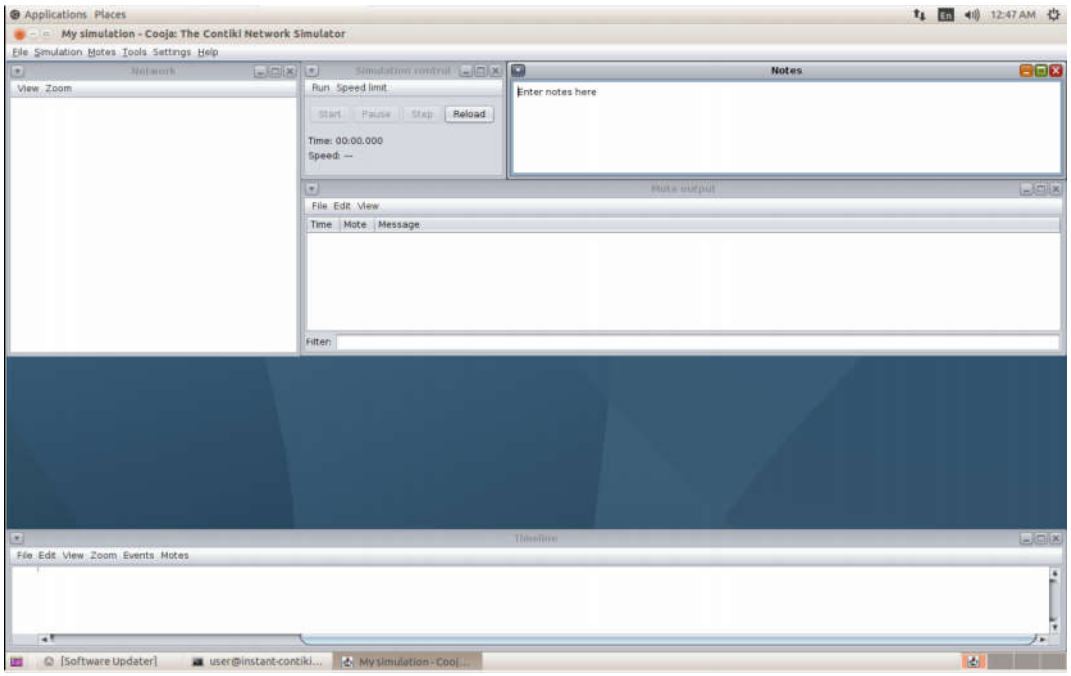
Nhập password là “user”, ta thấy cửa sổ hệ điều hành

Hình 7. Màn hình chính của Ubuntu 14.04 LTS

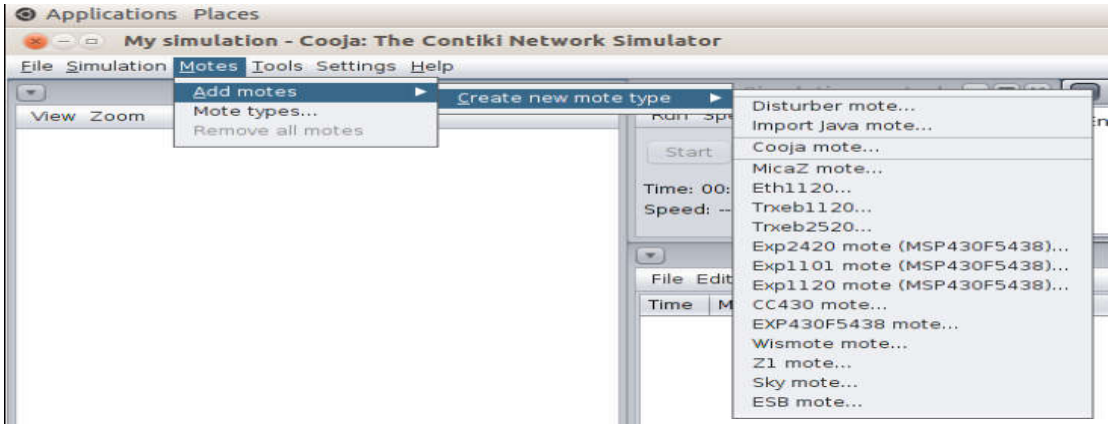
Mở công cụ mô phỏng Cooja trên Contiki bằng cách nháy đúp vào biểu tượng Terminal trên màn hình và gõ các lệnh như trong hình để khởi động công cụ Cooja:



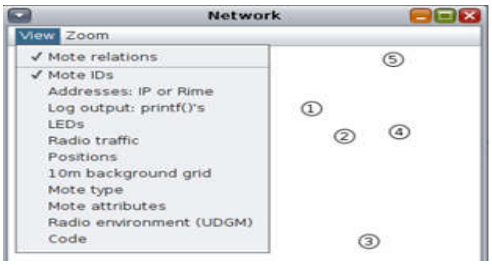
Màn hình của Cooja khi tạo mới một chương trình mô phỏng bằng cách bấm vào File/New

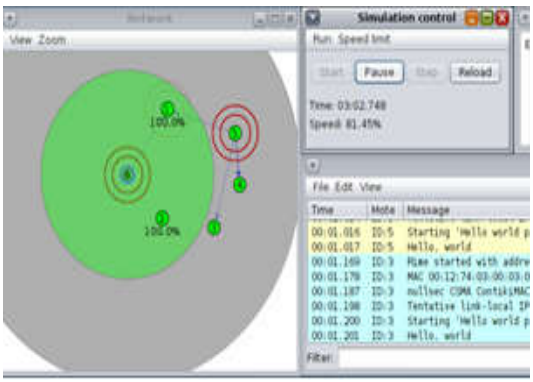


Thêm các Mote:



Một số lựa chọn hiển thị các Mote





DANH MỤC CÁC TÀI LIỆU THAM KHẢO

1. Tiếng việt

[1] Vũ Kim Cương, Phân tích đánh giá một số công cụ giám sát mạng và thử nghiệm với bộ công cụ Cacti. Luận văn thạc sỹ. Học viện CNBCVT 2014. Người hướng dẫn: PGS.TSKH. Hoàng Đăng Hải.

[2] Lê Quang Hưng, Hệ thống theo dõi, giám sát an ninh toàn mạng máy tính cấp tỉnh. Luận văn thạc sỹ. Học viện CNBCVT 2009. Người hướng dẫn: PGS.TSKH. Hoàng Đăng Hải.

[3] Nguyễn Quốc Thắng, Nghiên cứu xây dựng sensor thu thập thông tin an toàn mạng. Luận văn thạc sỹ. Học viện CNBCVT 2009. Người hướng dẫn: PGS.TSKH. Hoàng Đăng Hải.

[4] Nguyễn Thị Thơm, Mô hình và phương pháp kiểm tra lỗ hổng bảo mật trang Web. Luận văn thạc sỹ. Học viện CNBCVT 2015. Người hướng dẫn: PGS.TSKH. Hoàng Đăng Hải.

[5] Nguyễn Văn Thắng, Nghiên cứu, thử nghiệm phương thức trao đổi khóa động cho định danh và xác thực trong mạng IOT. Luận văn thạc sỹ. Học viện CNBCVT 2018. Người hướng dẫn: PGS.TSKH. Hoàng Đăng Hải.

[6] Trần Văn Huấn, Nghiên cứu, thử,nghiệm truyền tin bảo mật giữa các nút mạng IOT. Luận văn thạc sỹ. Học viện CNBCVT 2018. Người hướng dẫn: PGS.TSKH. Hoàng Đăng Hải.

2. Tiếng Anh

[7] A.B.Rabiah, K.K. Ramakrishnan, E. Liri, K. Kar. A Lightweight Authentication and Key Exchange Protocol for IoT. Proc of Workshop on Decentralized IoT Security and Standards. Jan 2018.

[8] H.Li, Y.S. Dai, B. Yang. Identity-Based Cryptography for Cloud Security. IACR Cryptology ePrint Archive 2011.

[9] O. Salman, S. Abdallah, I.H. Elhajj, A. Chehab, A. Kayssi. Identity-based authentication scheme for the Internet of Things. Proc of IEEE Symposium on Computers and Communications, June 2016.

[10] Adam Dunkels, Bjorn Gronvall, Thiemo Voigt (2004), "Contiki - a Lightweight and Flexible Operating System for Tiny Networked Sensors" 29th Annual IEEE International Conference on Local Computer Networks, 16-18 Nov.2004

[11] P. Shiva Kumar, Rinki Sharma, G.Varaprasad "Dynamic key management method for wireless sensor networks". 9th IEEE International Conference on Wireless and Optical Communications Networks (WOCN). India, 22-29 September 2012.

[12] Chien-Lung Hsu, Yu-Han Chen, Huang-Chia Lu, Tzu-Hsien Chuang, Tzu-Wei Lin "A Dynamic Identity End-to-End Authentication Key Exchange Protocol for IOT Environments". Twelfth International Conference on Digital Information Management (ICDIM). Japan, 12-14 Sept. 2017.

[13] Samet Kalyoncu. "Wireless Solutions and Authentication Mechanisms for Contiki Based Internet of Things Networks". Halmstadt University Report 2013. http://www.diva-portal.org/smash/record.jsf?pid=diva_2_3A767847 & dswid =7106

[14] Ayaz Hassan Moon, Ummer Iqbal, G. Mohluddin Bhat "Authenticated key exchange protocol for Wireless Sensor Networks". Elsevier Procedia Computer Science, Vol.89, 2016, pp.90-98.

[15] Yunlei Zhao "Identity-Concealed Authenticated Encryption and Key Exchange". CCS '16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria, 24-28 Oct. 2016. Pp. 1464-1479

3. Websites

[16] http://www.contiki-os.org/

[17] https://github.com

[18] http://antoanthongtin.vn/

[19] http://anrg.usc.edu/contiki/index.php/Contiki_tutorials

[20] https://securitybox.vn/4896/phan-loai-cac-phuong-phap-ma-hoa/