ĐẠI HỌC QUỐC GIA HÀ NỘI

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

HOÀNG VĂN TÂN

NGHIÊN CỨU MÔ HÌNH ĐẢM BẢO AN TOÀN TRUYỀN TIN DỰA TRÊN CHỮ KÝ SỐ VÀ CHỨNG CHỈ SÔ

LUẬN VĂN THẠC SỸ CÔNG NGHỆ KỸ THUẬT ĐIỆN TỬ TRUYỀN THÔNG

HÀ NỘI 2016

ĐẠI HỌC QUỐC GIA HÀ NỘI

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

HOÀNG VĂN TÂN

NGHIÊN CỨU MÔ HÌNH ĐẢM BẢO AN TOÀN TRUYỀN TIN DỰA TRÊN CHỮ KÝ SỐ VÀ CHỨNG CHỈ SÔ

Ngành: Công nghệ Kỹ thuật Điện tử, Truyền thông

Chuyên ngành: Kỹ thuật điện tử

Mã số: 60520203

LUẬN VĂN THẠC SỸ CÔNG NGHỆ KỸ THUẬT ĐIỆN TỬ TRUYỀN THÔNG

HƯỚNG DẪN KHOA HỌC: PGS. TS Trịnh Anh Vũ

HÀ NỘI 2016

LỜI CAM ĐOAN

Tôi xin cảm đoan luận văn tốt nghiệp "**Nghiên cứu mô hình đảm bảo an toàn truyền tin dựa trên chữ ký số và chứng chỉ sô**" là công trình nghiên cứu của riêng tác giả. Các số liệu, kết quả mô phỏng trình bày trong luận văn là hoàn toàn trung thực, chưa từng được công bố trong bất kỳ công trình nào khác.

Trong luận văn có tham khảo một số tài liệu như đã nêu trong phần tài liệu tham khảo

Tác giả luận văn

Hoàng Văn Tân

LỜI CẢM ƠN

Để hoàn thành được luận văn này, đầu tiên tôi được gửi lời cảm ơn chân thành và sâu sắc đến PGS.TS Trịnh Anh Vũ – Giảng viên Đại học Công nghệ, Đại học Quốc gia Hà nội. Thầy đã định hướng nội dung đề tài nghiên cứu và tận tình hướng dẫn, góp ý để em hoàn thành luận văn này.

Tiếp theo, tôi cũng xin gửi lời cảm ơn sâu sắc tới các thầy, các cô trong khoa và bộ môn Thông tin vô tuyến đã giúp đỡ, tạo điều kiện tốt nhất và giúp đỡ tôi trong quá trình học tập, nghiên cứu tại trường.

Cuối cùng, tôi xin gửi lời cảm ơn chân thành đến bố mẹ tôi và những người thân, những người đã luôn ủng hộ, động viên tôi về cả vật chất và tinh thần để tôi có thể hoàn thành luận văn.

Mặc dù có nhiều cố gắng, tuy nhiên luận văn bao gồm lượng lý thuyết rộng và nhiều kiến thức mới, thời gian và kiến thức còn hạn chế nên không tránh khỏi những thiếu sót. Em rất mong nhận được nhận xét phê bình, góp ý của các thầy cô để em hoàn thiện hơn luận văn.

Em xin chân thành cảm ơn.!

Hà Nội, ngày tháng năm 2016

Học viên

Hoàng Văn Tân

TÓM TẮT

Hiện nay với xu thế kết nối internet vạn vật (IoT - Internet of Things) nhiều hệ thống mạng cảm biến không dây được xây dựng phát triển để người quản lý, chỉ huy có thể trực tiếp theo dõi, giám sát nhiều đối tượng khác nhau, trên cơ sở đó có thể hành động hay ra quyết định kịp thời. Tuy nhiên yếu điểm của hệ thống cảm biến là bị hạn chế về tài nguyên và năng lực tính toán nên khả năng bảo mật đơn lẻ hay áp dụng các chương trình, giao thức bảo vệ, đảm bảo an toàn thông tin là khó khả thi.

Luận văn này dựa trên những nguyên tắc chung của truyền tin bảo mật dữ liệu và các mô hình an toàn dựa trên chứng chỉ số và chữ ký số. Nội dung luận văn đưa ra mô hình phân phối khóa Blom và phân tích và mô phỏng đánh giá một số mô hình Blom cải tiến khi được áp dụng vào mạng cảm biến không dây.

Mô hình phân phối khóa Blom cho phép bất kỳ cặp nút mạng nào đều có thể tìm được khóa riêng. Mô hình Blom yêu cầu một số nguyên tố q, một ma trận công khai P và một ma trận bí mật S. Trong đó, ma trận S là ma trận bí mật và ngẫu nhiên, ma trận P là ma trận công khai có dạng là ma trận Vandermonde. Tuy nhiên, ma trận Vandermonde có giá trị phần tử lớn, gây khó khăn trong tính toán và lưu trữ. Vì vậy, luận văn có tìm hiểu một số đề xuất cải tiến mô hình Blom bằng cách thay thế ma trận Vandermonde bằng ma trận ngẫu nhiên, ma trận Hadamard và ma trận liền kề vô hướng. Các kết quả mô phỏng khi áp dụng các cải tiến đều cho kết quả tốt, phù hợp với lý thuyết. Luận văn cũng có đưa ra đề xuất thay thế ma trận Vandermode bằng ma trận kề có hướng và có kết quả mô phỏng đánh giá. Kết quả mô phỏng phù hợp với lý thuyết và có kết quả ngang bằng với các đề xuất cải tiến trước đây.

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

LỜI GIỚI THIỆU

Mô hình đảm bảo an toàn truyền tin trong luận văn này tập trung trên mạng cảm biến không dây. Như chúng ta đều biết hiện nay với xu thế kết nối internet vạn vật (IoT - Internet of Things) nhiều hệ thống mạng cảm biến không dây được xây dựng phát triển để người quản lý, chỉ huy có thể trực tiếp theo dõi, giám sát các sự kiện diễn biến của nhiều đối tượng khác nhau, trên cơ sở đó có thể hành động hay ra quyết định kịp thời. Tuy nhiên yếu điểm của hệ thống cảm biến nói chung là bị hạn chế về tài nguyên và năng lực tính toán nên khả năng bảo mật đơn lẻ hay áp dụng các chương trình, giao thức bảo vệ, đảm bảo an toàn thông tin là khó khả thi, không thể như các thiết bị như smart phone hay các hệ thống mạng, hệ thống servers. Trong khi các dữ liệu thu thập được của các cảm biến có thể rất nhạy cảm và cần bảo mật cao (như hệ thống theo dõi sức khỏe cá nhân, hệ thống giám sát môi trường, quân sự…).

Đề tài "Nghiên cứu mô hình đảm bảo an toàn truyền tin dựa trên chữ ký số và chứng chỉ số" dựa trên những nguyên tắc chung của truyền tin bảo mật dữ liệu, nguyên tắc xác nhận tư cách người truy cập (chứng chỉ số) và người cấp phát dữ liệu (chữ ký số) để vận dụng trong mạng cảm biến không dây với tính đặc thù về hạn chế tài nguyên xử lý ở mỗi nút mạng, đồng thời đưa ra những kịch bản mô phỏng tương ứng để chứng minh ưu điểm của các đề xuất nghiên cứu phát triển. Nội dung luận văn gồm 4 chương, trình bày các vấn đề sau:

Chương 1: Tổng quan về mật mã học và mã hóa

Chương 1: Giới thiệu tổng quan về mật mã học và mã hóa, các yêu cầu chức năng của mã hóa. Đồng thời tìm hiểu và phân tích các ưu điểm, nhược điểm về mô hình hoạt động của hệ mã hóa đối xứng, hệ mã hóa bất đối xứng và một số mô hình mã hóa hiện đại.

Chương 2: Mạng cảm biến không dây và các vấn đề bảo mật

Chương 2: Giới thiệu, trình bày khái niệm cơ bản về mạng cảm biến không dây, về kiến trúc của mạng cảm biến không dây. Chương 2 cũng tìm hiểu về các yêu cầu an toàn bảo mật trong mạng cảm biến không dây và đưa ra những thách thức khi triển khai các phương pháp đảm bảo an toàn thông tin trong mạng cảm biến không dây.

Chương 3: Mô hình Blom

Chương 3 giới thiệu về mô hình bảo mật Blom trong mạng cảm biến không dây, các bước bắt tay xác thực nút mạng và trao đổi khóa khi áp dụng mô hình Blom vào mạng cảm biến không dây.

Chương 4: Các mô hình Blom cải tiến

Chương 4 đưa ra và phân tích một số phương pháp cải tiến mô hình Blom từ trước và cũng có đề xuất cải tiến mô hình Blom nhằm giảm thời gian tính toán và giảm dung lượng bộ nhớ lưu trữ của nút mạng.

Em rất mong nhận được nhận xét phê bình, góp ý của các thầy cô để em hoàn thiện hơn.

Em xin chân thành cảm ơn.!

CHƯƠNG I: TỔNG QUAN VỀ MẬT MÃ HỌC VÀ MÃ HÓA

1.1. TỔNG QUAN VỀ MẬT MÃ HỌC VÀ MÃ HÓA

1.1.1. Khái niệm mật mã học và mã hóa

Mật mã trước hết là một loại hoạt động nhằm giữ bí mật thông tin. Kỹ thuật mật mã được thể hiện thông qua việc biến đổi thông tin rõ nghĩa thành những đoạn ký tự mã hóa có dạng ngẫu nhiên không rõ nghĩa. Từ đó đạt được hai mục tiêu:

+ Một là, làm cho kẻ tin tặc đánh cắp thông tin không biết cách giải mã nên không thể thu được thông tin có ý nghĩa từ chuỗi ký tự ngẫu nhiên.
+ Hai là, kẻ tin tặc không có khả năng làm giả thông tin để giả mạo người gửi.

Khoa học nghiên cứu kỹ thuật mật mã gọi là mật mã học, mật mã học bao gồm hai lĩnh vực là: mật mã học lập mã và mật mã học phân tích.

+ Mật mã học lập mã là ngành học nghiên cứu mã hóa thông tin để thực hiện che giấu thông tin.
+ Mật mã học phân tích là ngành học nghiên cứu và phân tích việc giải mã.

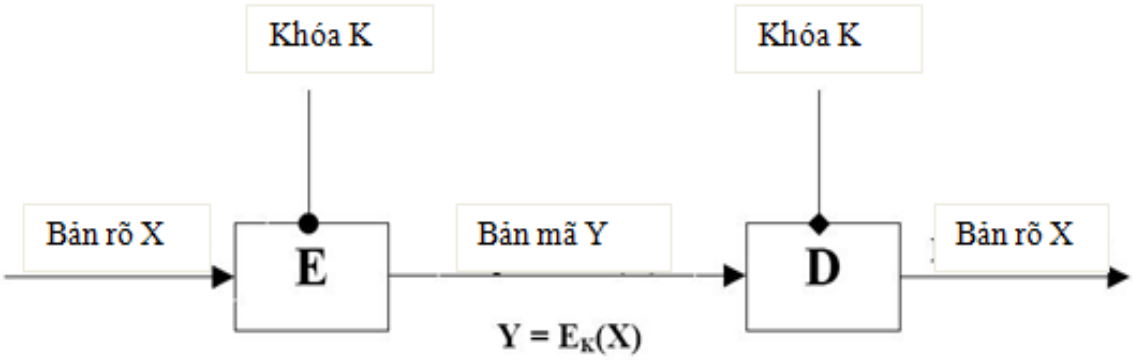
Mã hóa là một quá trình dùng để biến đổi thông tin từ dạng này sang dạng khác và ngăn chặn những đối tượng không được phép có thể xem được thông tin. Bản thân việc mã hóa không ngăn chặn được việc đánh cắp thông tin, nó chỉ làm biến dạng thông tin để cho dù có bị đánh cắp thì cũng không thể xem được nội dung thông tin.

Thông tin trước khi chuyển đổi được gọi là bản rõ, thông tin sau khi chuyển đổi được gọi là bản mật. Quá trình chuyển đổi thông tin từ dạng bản rõ sang dạng bản mật được gọi là quá trình mã hóa và ngược lại, quá trình chuyển đổi thông tin từ dạng bản mật sang dạng bản rõ được gọi là quá trình giải mã. Để thực hiện được một quá trình mã hóa và giải mã, ta còn cần có một *thuật toán* và *khóa mật mã* để

biến bản tin rõ thành bản mật và một thuật toán làm ngược lại biến bản mật cùng với khoá mật mã thành bản rõ. Các thuật toán đó được gọi tương ứng là thuật toán mã hóa và thuật toán giải mã. Các thuật toán này thường không nhất thiết phải giữ bí mật, cái cần được giữ bí mật là *khóa mật mã.* Một hệ mã hóa tiêu biểu được định nghĩa gồm 5 thành phần (P, C, K, E, D), trong đó:

+ P là tập hữu hạn các các bản rõ.
+ C tập hữu hạn các bản mã.
+ K là tập hữu hạn các khoá.
+ E là tập các hàm mã hóa.
+ D là tập các hàm giải mã.

Với mỗi khóa k ∈ K, có một hàm mã hóa ek ∈ E, ek : P → C và một hàm giải mã dk∈ D, đk: C → P sao cho dk(ek(x)) = x , ∀ x ∈ P. Mô hình quá trình mã hóa và giải mã chi tiết như hình sau:



Hình 1.1: Quá trình mã hóa và giải mã (Nguồn: https://voer.edu.vn)

Ví dụ: Người gửi A muốn gửi một văn bản đến người nhận B, A phải tạo cho văn bản đó một bản mã mật tương ứng và thay vì gửi văn bản rõ thì A chỉ gửi bản mật cho B, B nhận được bản mật và khôi phục lại dạng bản rõ để hiểu được thông tin mà A gửi. Do văn bản gửi đi thường được chuyển qua các đường công khai nên người ngoài có thể "lấy trộm" hoặc "xem trộm", nhưng vì đó là bản mật mã nên kẻ

lấy cắp không đọc hiểu được; Còn A có thể biến đổi bản rõ thành bản mã mật và B có thể giải bản mã mật thành bản rõ để hiểu được là do hai người đã có một thoả thuận về khoá để mã hóa và giải mã, chỉ với khoá này thì A mới tạo được bản mã mật từ bản rõ và B mới khôi phục được bản rõ từ bản mã mật. Khoá này được gọi là khoá mật mã.

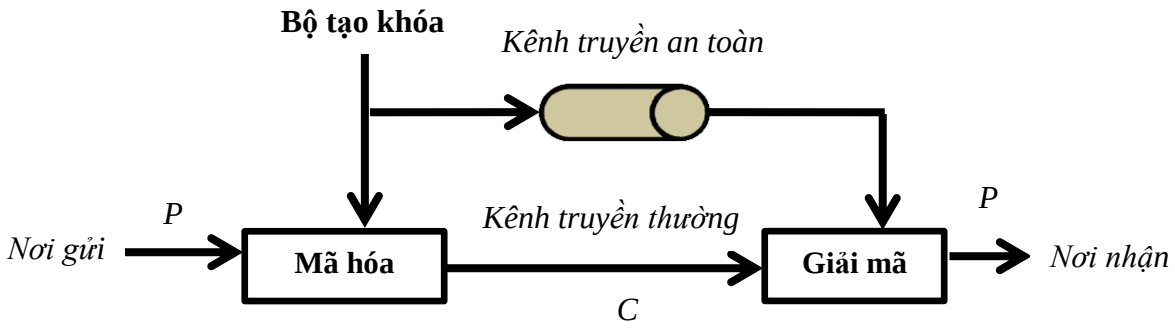
1.1.2. Chức năng của mã hóa

- *Đảm bảo tính bí mật:* Chức năng này giải quyết vấn đề bảo vệ thông tin chống lại sự tìm hiểu nội dung thông tin từ các đối tượng không có quyền truy cập nội dung hay tìm hiểu nội dung. Chỉ có những đối tượng có quyền truy cập và có khóa hợp lệ mới có thể truy cập và đọc được thông tin.
- *Đảm bảo tính toàn vẹn:* Chức năng này đảm bảo khả năng phát hiện sự sửa đổi thông tin trái phép. Việc đảm bảo toàn vẹn dữ liệu cần phải có các phương pháp đơn giản và tin cậy, không gây lãng phí tài nguyên đường truyền. Hiện nay, việc sử dụng các hàm băm một chiều được sử dụng rất hiệu quả. Dữ liệu gửi đi được đính kèm thêm giá trị hàm băm của dữ liệu gốc bên nhận sẽ tính lại giá trị băm của dữ liệu gốc nhận được, nếu giá trị hàm băm tính được và giá trị hàm băm của bên gửi đính kèm là giống nhau, chứng tỏ dữ liệu nhận được là toàn vẹn không bị thay đổi.
- *Đảm bảo tính xác thực:* Chức năng này có chức năng xác minh thông tin, nguồn gốc thông tin của bên gửi, đảm bảo quyền hợp pháp của chủ thể gửi và nhận thông tin, chống sự giả mạo. Ví dụ như việc sử dụng mã PIN cá nhân trong các giao dịch ngân hàng.
- *Đảm bảo tính chống từ chối:* Chức năng này đảm bảo xác định rõ trách nhiệm của các chủ thể trong việc quản lý, phân phối khóa đồng thời làm rõ được nguồn gốc của thông tin khi trao đổi, chống chối bỏ trách nhiệm.

1.2. CÁC HỆ MÃ HÓA TIÊU BIỂU

1.2.1. Hệ mã hóa đối xứng

Hệ mã hóa đối xứng (hay còn gọi là hệ mã hóa khóa bí mật) là hệ mã hóa sử dụng chung một khóa cho việc mã hóa và giải mã. Trước khi dùng hệ mã hóa đối xứng, người gửi và người nhận phải thỏa thuận thuật toán và khóa dùng để mã hóa hay giải mã qua một kênh an toàn. Nơi gửi sẽ dùng khóa đã thỏa thuận và một thuật toán mã hóa đã thỏa thuận trước để mã hóa thông điệp. Phía nhận sẽ sử dụng khóa đã thỏa thuận và một thuật toán giải mã đã thỏa thuận để giải mã. Độ an toàn của hệ mã hóa loại này phụ thuộc vào khóa. Hệ mã hóa đối xứng tổng quan được biểu diễn bằng mô hình sau:



Hình 1.2: Mô hình hệ mã hóa đối xứng [4]

Mô hình trên gồm 5 thành phần:

+ Bản rõ P (plaintext)
+ Thuật toán mã hóa E (encrypt algorithm)
+ Khóa bí mật K (secret key)
+ Bản mã C (ciphertext)
+ Thuật toán giải mã D (decrypt algorithm)

Trong đó: C = E (P, K)

P = D (C, K)

Các thuật toán sử dụng trong hệ mã hóa đối xứng được chia ra làm hai loại: Mã hóa luồng (stream ciphers) và Mã hóa khối (block ciphers).

- *Mã hóa luồng*

Mã hóa luồng 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. Ví dụ trong kết nối không dây.

Mã hóa luồng có các đặc điểm sau:

- *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 $\rightarrow p_0p_1p_2p_3$ ... p_{n-1} (p_i: có độ dài là k bít)

- *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:

  StreamCipher(K) $\rightarrow$ S = $s_0s_1s_2s_3$ ... s_{n-1} (s_i: có độ dài là k bít)

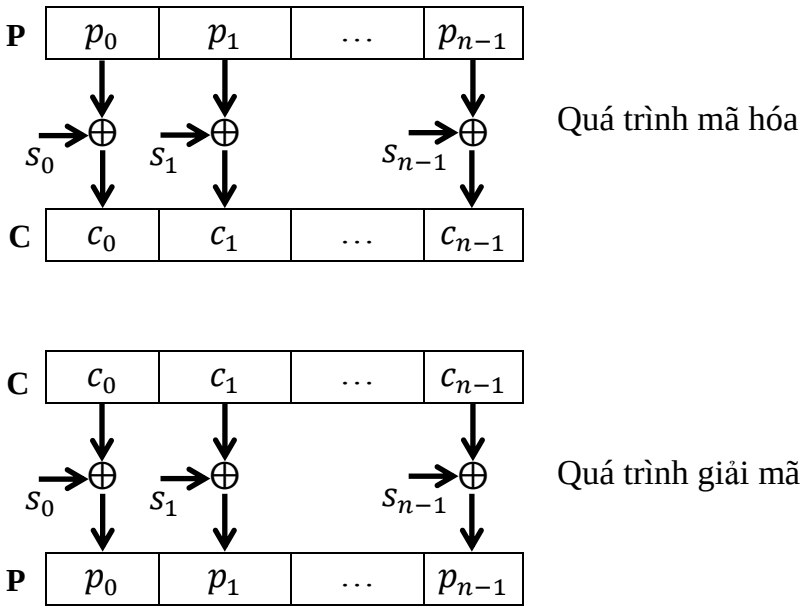
  Và $s_0 = s_1 = s_2 = s_3 = \ldots = s_{n-1}$

- *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.

  $c_0 = p_0 \oplus s_0, c_1 = p_1 \oplus s_1, \ldots\ c_{n-1} = p_{n-1} \oplus s_{n-1}$

  C = $c_0c_1c_2c_3$ ... c_{n-1} (c_i: có độ dài là k bít)

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



Hình 1.3: Mô hình mã hóa và giải mã của mã hóa luồng [2]

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

- *Mã hóa khối*

Mã hóa luồng có hạn chế là chỉ cần biết một cặp khối bản rõ và khối bản mã, người ta có thể suy ra được khóa và dùng nó để giải mã các khối bản mã khác của bản tin. Do đó để chống việc phá mã thì người ta phải làm cho P và C không có mối liên hệ nào về 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
000	101
001	100
010	110
011	001
100	111
101	011
110	000
111	010

Khi đó, khóa là toàn bộ bảng trên, cả hai bên gửi và bên nhận đều phải biết toàn bộ bảng trên để thực hiện mã hóa và giải mã. Đối với kẻ tấn công, nếu biết một số cặp bản rõ và bản mã thì cũng chỉ biết được một phần khóa của bảng tra cứu trên. Do đó không thể giải mã được các khối bản mã còn lại.

Tuy nhiên, 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 2^{64} dòng và có $2^{64}!$ bảng khóa có thể có. Lúc đó kích thước khóa là rất lớn và việc phá mã là điều khó có thể. Do đó mã hóa khối an toàn lý tưởng là điều không khả thi trong thực tế. Một số thuật toán mã hóa khối trong hệ mã hóa đối xứng nổi tiếng và được sử dụng rộng dải như: RC6, RC5, DES, 3-DES (Triple DES), AES, ECB, IDEA …

➢ *Các tính chất của hệ mã hóa đối xứng*

- Các thuật toán của hệ mã hóa đối xứng có tốc độ tính toán nhanh, độ an toàn cao, độ dài khóa ngắn.
- Các thuật toán của hệ mã hóa đối xứng sử dụng một khóa chung cho cả bên gửi và bên nhận. Do đó các thuật toán này không cần giữ bí mật thuật toán, cái cần giữ bí mật là khóa bí mật dùng để mã hóa và giải mã. Do đó sự hạn chế của các thuật toán của hệ mã hóa đối xứng nảy sinh trong việc phân phối khóa và đảm bảo an toàn trong quản lý và sử dụng khóa.

+ Đảm bảo an toàn trong quản lý và sử dụng khóa: Do khả năng các khóa có thể bị phát hiện bởi thám mã trong quá trình trao đổi hoặc sử dụng khóa. Vì vậy, chúng cần được đảm bảo an toàn trong khi sử dụng và có cơ chế đổi khóa thường xuyên. Điều này cũng phụ thuộc lớn vào ý thức người dùng.
+ Đảm bảo an toàn trong phân phối khóa: Khi trao đổi khóa giữa người gửi và người nhận, khóa có thể bị lộ bởi rất nhiều nguyên nhân. Việc này đòi hỏi phải có phương thức phân phối khóa an toàn và hiệu quả.
+ Số lượng khóa lớn: Với mỗi cặp kết nối giữa bên gửi với bên nhận khác nhau sẽ có một khóa riêng để mã hóa. Do vậy, gây khó khăn trong việc sinh khóa và lưu trữ khóa khi số lượng kết nối lớn.

1.2.2. Hệ mã hóa bất đối xứng

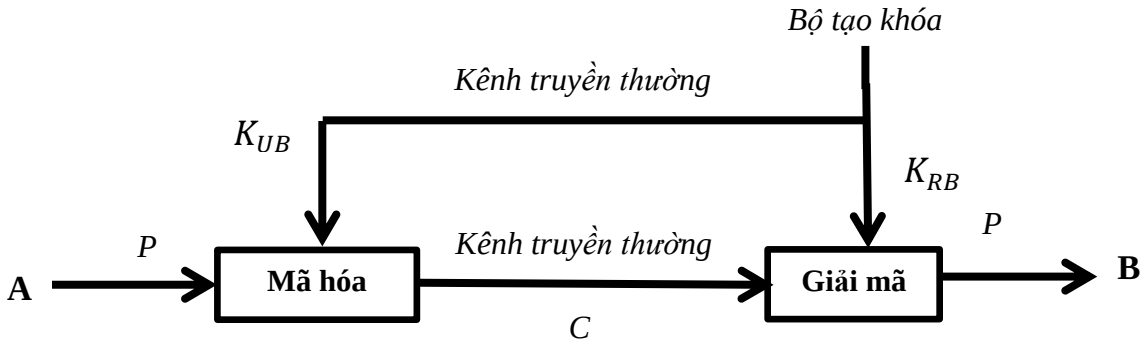
Hệ mã hóa khóa bất đối xứng (hay còn gọi là hệ mã hóa khóa công khai) là hệ mã hóa sử dụng một cặp khóa, được 2 nhà khoa học Diffie và Hellman đưa ra vào năm 1976. Hệ mã hóa này bao gồm một khóa dùng để mã hóa, còn gọi là khóa công khai (public key) và một khóa dùng để giải mã, còn gọi là khóa riêng (private key).

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.
- Vấn đề 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.

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 1.4: A mã hoá thông điệp sử dụng khoá công khai của B [2]

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.

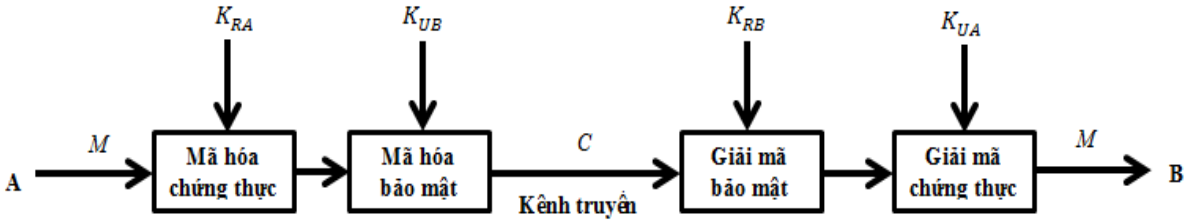
+ Bản mã C (ciphertext).
+ Thuật toán giải mã D (decrypt algorithm).

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 1.5: A và B đều sử dụng hệ mã hóa bất đối xứng [2]

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})

➢ *Các tính chất của hệ mã hóa bất đối xứng:*

- Các thuật toán của hệ mã hóa bất đối xứng sử dụng khóa mã hóa và khóa giải mã khác nhau 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.
- Do các thuật toán mã hóa của hệ mã hóa bất đối xứng có khóa công khai được công bố công khai trên mạng. Nên không thể đảm bảo khóa công khai có đúng là của đối tượng cần liên lạc hay không? Vấn đề xác thực được giải quyết bằng việc, yêu cầu các chủ thể cung cấp chứng chỉ số do các tổ chức cung cấp chứng chỉ số được công nhận như: VNPT, Viettel, FPT, GeoTrust Global, DigiCert ...
- Một vấn đề khác nảy sinh là khả năng dễ bị tấn công dạng kẻ tấn công người đứng giữa (MITM - Man In The Middle). 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

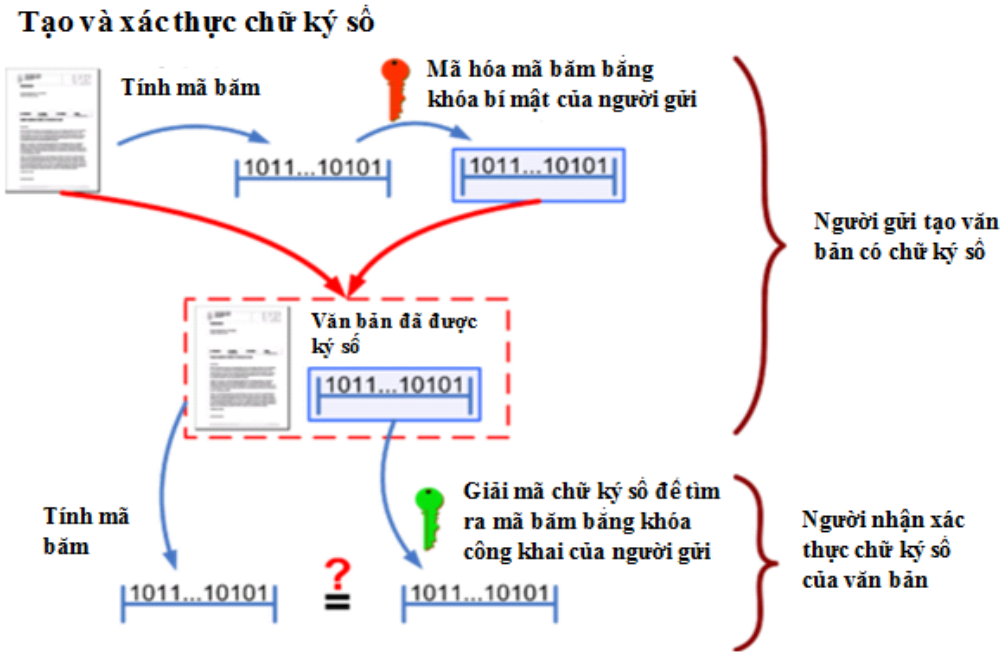
được là trao đổi khóa và xác thực. Tuy nhiên, các thuật toán của hệ mã hóa bất đối xứng có kích thước khóa mã hóa lớn làm tăng khối lượng tính toán nên nó khó được sử dụng độc lập. Vì vậy trong thực tế các mô hình bảo mật thường kết hợp các loại thuật toán với nhau để tận dụng các ưu điểm và hạn chế các điểm yếu.

1.2.3. Một số ứng dụng thực tế

Thực tế, một số ứng dụng, giao thức mã hóa phải kết hợp nhiều mô hình, nhiều hệ mã hóa, nhiều thuật toán đảm bảo an toàn thông tin với nhau để tận dụng được thế mạnh và khắc phục được các điểm yếu của các hệ mã hóa. Một số ứng dụng, giao thức mã hóa được sử dụng rộng dải như: chứng chỉ số, chữ ký số.

- *Chữ ký số (Chữ ký điện tử)*

Chữ ký số là thông tin đi kèm theo dữ liệu gửi đi nhằm mục đích xác định được chủ nhân của dữ liệu. Chữ ký số hoạt động dựa trên hệ mã hóa bất đối xứng, mô hình tạo và kiểm tra chữ ký số như sau:



Hình 1.6: Sơ đồ tạo và kiểm tra chữ ký số (nguồn: https://vi.wikipedia.org)

Bên gửi sẽ dùng một thuật toán tính hàm băm để tìm ra một bản "tóm tắt" của văn bản cần gửi. Sau đó, mã hóa bản "tóm tắt" này bằng khóa bí mật của bên gửi và đính kèm với văn bản trước khi gửi đi. Bên nhận dùng khóa công khai của bên gửi để tính ra bản "tóm tắt" từ bản "tóm tắt" đã mã hóa, đồng thời cũng tính bản "tóm tắt" từ văn bản nhận được. So sánh giữa hai bản tóm tắt, nếu giống nhau chứng tỏ văn bản được tạo và ký nhận bởi đúng người gửi và văn bản không bị sửa đổi. Nếu hai bản này khác nhau thì văn bản nhận được đã bị thay đổi sau khi ký hoặc chữ ký số không được tạo ra bởi khóa bí mật của người gửi hợp pháp.

- *Chứng chỉ số*

Chứng chỉ số là một tệp tin điện tử dùng để xác minh danh tính của một chủ thể là cá nhân, một máy chủ hay của một công ty … trên internet. Chứng chỉ số giống như chứng minh nhân dân, hộ chiếu hay nhưng giấy tờ dùng để xác minh cho một chủ thể duy nhất. Và việc cấp chứng chỉ số cũng phải do một tổ chức đứng ra chứng nhận nhưng thông tin của chủ thể cung cấp là chính xác. Tổ chức này được gọi là nhà cung cấp chứng chỉ số (CA – Certificate Authority).

Chứng chỉ số hoạt động dựa trên hệ mã hóa bất đối xứng, một chứng chỉ số bao gồm các thông tin: khóa công khai, tên, địa chỉ của chủ thể sở hữu, hạn sử dụng và CA cung cấp chứng chỉ. Chứng chỉ số có chứa cả chữ ký số của CA đã cấp chứng chỉ số, điều này đảm bảo chứng chỉ số được đảm bảo không bị giả mạo.

1.3. Kết luận chương

Trong nội dung chương 1, luận văn đã đưa ra các khái niệm cơ bản về mật mã và mã hóa. Nội dung chương đã đưa ra và phân tích các mô hình mã hóa và giải mã của các hệ mã hóa đối xứng và hệ mã hóa bất đối xứng từ đó thấy được các ưu nhược điểm của từng mô hình mã hóa. Nội dung chương 1 cũng đã giới thiệu được một số ứng dụng của các hệ mã hóa như: chứng chỉ số, chữ ký số.

CHƯƠNG II: MẠNG CẢM BIẾN KHÔNG DÂY VÀ CÁC VẤN ĐỀ BẢO MẬT

2.1. ĐỊNH NGHĨA

Mạng cảm biến không dây (WSN – Wireless Sensor Networks) bao gồm một tập hợp các thiết bị, các cảm biến sử dụng các kết nối với nhau để phối hợp thực hiện nhiệm vụ thu thập thông tin dữ liệu phân tán với quy mô lớn và trong bất kỳ điều kiện vật lý nào.

Các nút trong mạng cảm biến không dây thường là các thiết bị đơn giản, nhỏ gọn, giá thành thấp… và có số lượng lớn. Mạng cảm biến không dây được phát triển và dùng trong nhiều ứng dụng khác nhau như: theo dõi môi trường, khí hậu, do thám, giám sát, phát hiện trong quân sự, sức khỏe … Do vậy mạng cảm biến không dây được phân bổ không có mô hình mạng.

Mạng cảm biến không dây có một số đặc điểm sau:

- Có khả năng tự tổ chức, yêu cầu ít hoặc không cần sự can thiệp của con người.
- Có khả năng chịu lỗi cao.
- Có khả năng mở rộng.
- Triển khai với số lượng lớn và có sự kết hợp giữa các nút mạng.
- Truyền thông không tin cậy, quảng bá trong phạm vi hẹp.
- Cấu hình mạng thay đổi thường xuyên, phụ thuộc vào mức độ dịch chuyển, hư hỏng hay mở rộng các nút mạng.
- Bị giới hạn về kích thước, năng lượng, công suất phát, bộ nhớ và năng lực tính toán.

Chính những đặc điểm trên đã đưa ra yêu cầu thay đổi và thiết kế cảm biến để phù hợp hơn với chức năng khi triển khai.

2.2. ĐẶC ĐIỂM CỦA CẢM BIẾN KHÔNG DÂY

Như các đặc điểm, tính chất của mạng cảm biến không dây đã nêu, nên việc thiết kế, chế tạo một cảm biến cũng bị nhiều ràng buộc:

2.2.1. Kích thước vật lý nhỏ

Kích thước và công suất tiêu thụ luôn chi phối khả năng xử lý, lưu trữ và tương tác của các thiết bị cơ sở. Việc thiết kế các phần cứng cho mạng cảm biến phải chú trọng đến giảm kích cỡ đồng thời phải đảm bảo công suất tiêu thụ và nguồn cung cấp phù hợp với yêu cầu về khả năng hoạt động. Khi thiết kế cảm biến, việc sử dụng phần mềm phải tạo ra các hiệu quả để bù lại các hạn chế của phần cứng.

2.2.2. Hoạt động đồng thời với độ tập trung cao

Hoạt động chính của các thiết bị trong mạng cảm biến là đo lường và vận chuyển các dòng thông tin với khối lượng xử lý thấp, gồm các hoạt động nhận lệnh, dừng, phân tích và đáp ứng. Vì dung lượng bộ nhớ trong nhỏ nên cần tính toán rất kỹ về khối lượng công việc cần xử. Một số hoạt động xử lý nhiều thì cảm biến xử lý lâu và khó đáp ứng tính năng thời gian thực. Do đó, các nút mạng phải thực hiện nhiều công việc đồng thời và cần phải có sự tập trung xử lý cao độ.

2.2.3. Khả năng liên kết vật lý và điều khiển hạn chế

Tính năng điều khiển ở các nút cảm biến không dây cũng như sự phức tạp của chức năng xử lý, lưu trữ và chuyển mạch trong mạng cảm biến không dây thấp hơn so với các hệ thống thông thường. Ví dụ, trong bộ cảm biến cung cấp một giao diện đơn giản kết nối trực tiếp tới một bộ vi điều khiển (đảm bảo tiêu thụ điện thấp nhất). Ngược lại, các hệ thống thông thường, với các hoạt động xử lý phân tán, đồng thời kết hợp với nhiều thiết bị trên nhiều mức điều khiển được liên kết với nhau bằng một cấu trúc bus phức tạp.

2.2.4. Đa dạng trong thiết kế và ứng dụng

Các thiết bị cảm biến có khuynh hướng được sản xuất dành riêng cho ứng dụng cụ thể, tức là mỗi loại thiết kế, mỗi loại phần cứng chỉ hỗ trợ riêng cho ứng dụng của nó. Vì có một phạm vi ứng dụng rất rộng nên cảm biến cũng có rất nhiều kiểu thiết bị vật lý khác nhau. Với mỗi thiết bị cảm biến, điều quan trọng là phải tích hợp được phần mềm để có được ứng dụng từ phần cứng. Như vậy, các loại thiết bị này cần một sự điều chỉnh phần mềm ở một mức độ nào đó để có được hiệu quả sử dụng phần cứng cao.

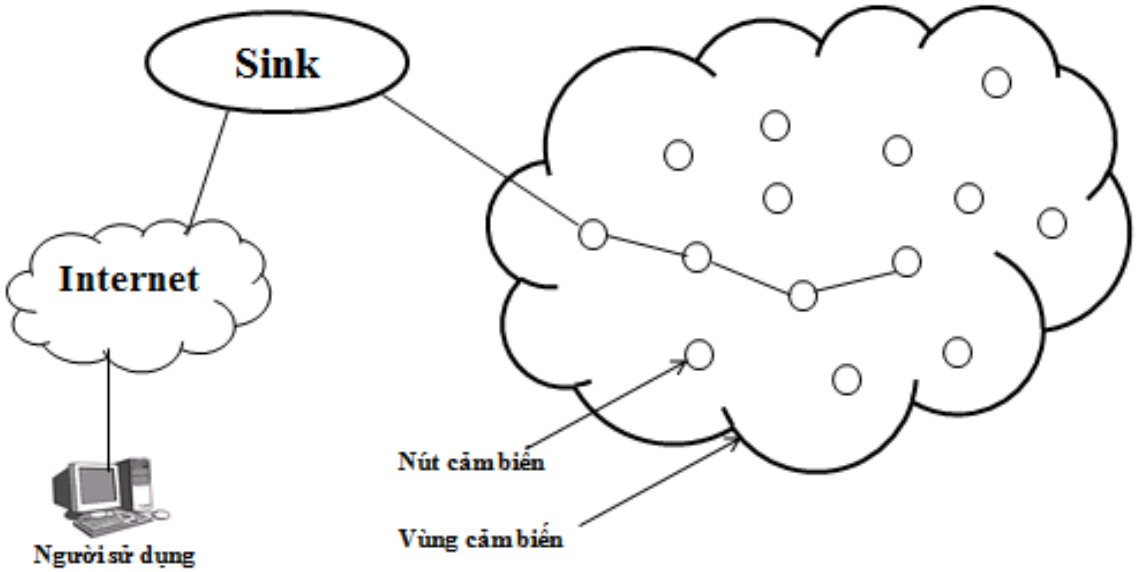
2.2.5. Hoạt động tin cậy

Các thiết bị có số lượng lớn, được triển khai trong phạm vi rộng với một ứng dụng cụ thể. Việc áp dụng các kỹ thuật mã hóa sửa lỗi truyền thống nhằm tăng độ tin cậy của các cảm biến bị giới hạn bởi kích thước, nguồn và công suất. Việc tăng độ tin cậy của các cảm biến là điều cốt yếu. Thêm vào đó, chúng ta có thể tăng độ tin cậy của ứng dụng bằng khả năng chấp nhận và khắc phục được sự hỏng hóc của một vài cảm biến đơn lẻ. Như vậy, hệ thống hoạt động trên từng nút đơn không những mạnh mẽ mà còn dễ dàng phát triển các ứng dụng phân tán tin cậy.

2.3. MÔ HÌNH MẠNG CẢM BIẾN KHÔNG DÂY

Một mạng cảm biến không dây bao gồm rất nhiều nút được triển khai ở gần hoặc bên trong đối tượng cần thăm dò để thu thập thông tin. Vị trí các cảm biến không cần định trước vì vậy nó cho phép triển khai ngẫu nhiên trong các vùng không thể tiếp cận hoặc các khu vực nguy hiểm. Khả năng tự tổ chức mạng và cộng tác làm việc của các cảm biến là đặc trưng cơ bản của mạng. Với số lượng lớn các cảm biến được triển khai gần nhau thì truyền thông đa liên kết được lựa chọn để công suất tiêu thụ là nhỏ nhất (so với truyền thông đơn liên kết) và mang lại hiệu quả truyền tín hiệu tốt hơn so với truyền khoảng cách xa.

Cấu trúc cơ bản của mạng cảm biến không dây được thể hiện ở hình sau.



Hình 2.1: Cấu trúc cơ bản của mạng cảm biến không dây
(nguồn: http://automation.net.vn)

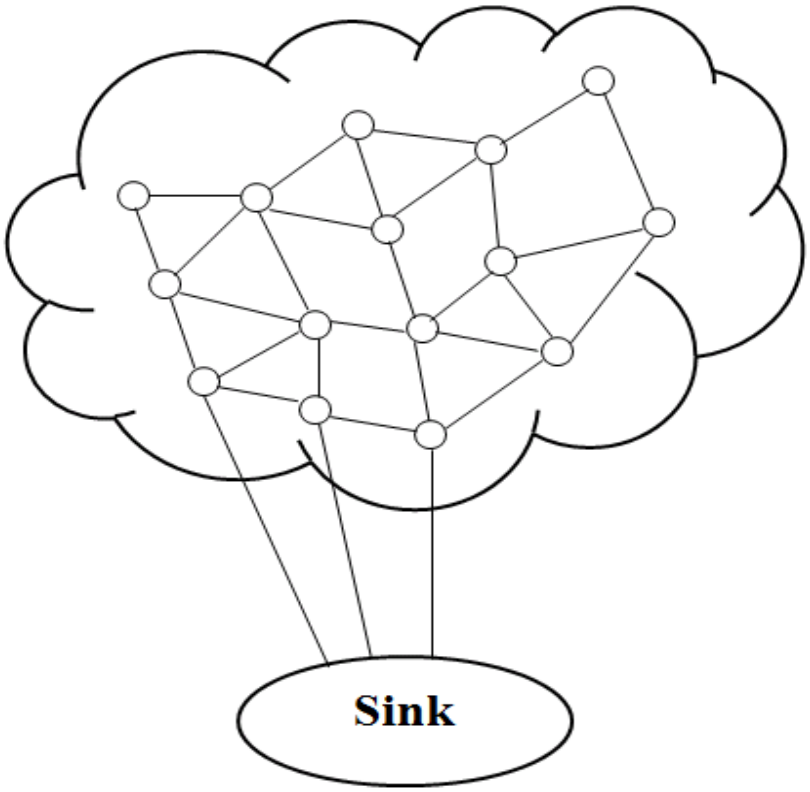
Các nút cảm biến được triển khai trong môi trường cần quan sát, thu thập thông tin. Mỗi nút cảm biến được triển khai phân tán trong mạng và có khả năng thu thập thông số liệu, định tuyến gửi số liệu về bộ thu nhận (Sink) để chuyển tới người dùng (User) và định tuyến chuyển các bản tin mang theo yêu cầu từ nút Sink đến các nút cảm biến. Nút sink có thể kết nối trực tiếp với người dùng hoặc gián tiếp thông qua mạng Internet hay vệ tinh.

Nút sink có thể là thực thể bên trong mạng (là một nút cảm biến) hoặc ngoài mạng. Thực thể ngoài mạng có thể là một thiết bị thực như máy tính xách tay tương tác với mạng cảm biến hoặc là một thiết bị có chức năng chuyển thông tin từ các nút trong mạng ra bên ngoài.

Về mặt phân loại, mạng cảm biến không dây chia thành 2 dạng cấu trúc: Cấu trúc phẳng và Cấu trúc phân cấp.

2.3.1. Cấu trúc phẳng

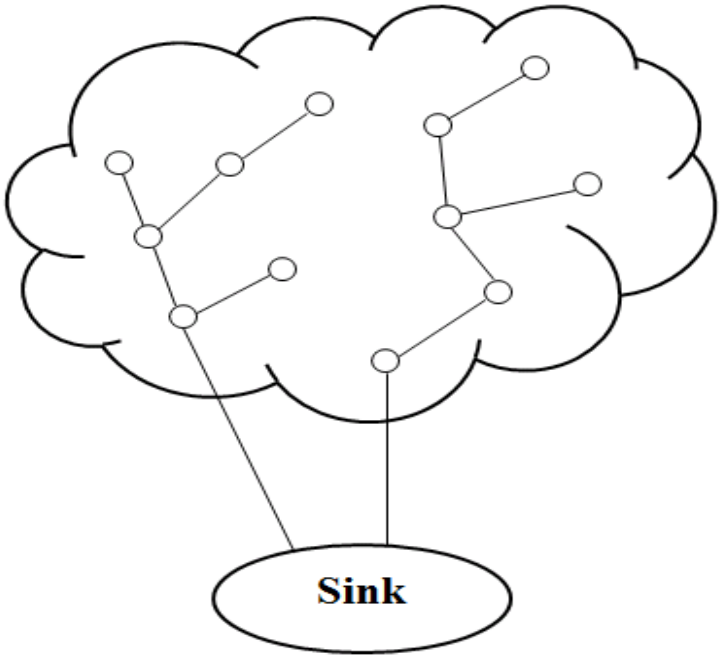
Trong mô hình cấu trúc phẳng, tất cả các nút đều ngang hàng và đồng nhất trong hình dạng và chức năng. Các nút giao tiếp với sink qua multi-hop sử dụng các nút ngang hàng làm bộ tiếp song. Với phạm vi truyền cố định, các nút gần sink hơn sẽ đảm bảo vai trò của bộ tiếp sóng đối và được phân bổ lượng nguồn lớn.



Hình 2.2: Cấu trúc phẳng của mạng cảm biến không dây
(nguồn: www.intechopen.com)

2.3.2. Cấu trúc phân cấp

Trong cấu trúc cấp, các cụm nút cảm biến được tạo ra, các nút cảm biến trong cùng một cụm gửi dữ liệu single-hop hay multi-hop (tùy thuộc vào kích cỡ cụm) đến một nút được định sẵn, được gọi là nút chủ. Trong cấu trúc này các nút tạo thành một hệ thống có phân cấp bậc mà ở đó mỗi nút ở một mức nhiệm vụ đã được xác định trước.



Hình 2.3: Cấu trúc tầng của mạng cảm biến không dây
(nguồn: www.intechopen.com)

Mạng có cấu trúc phân cấp hoạt động hiệu quả hơn cấu trúc phẳng do:

- Cấu trúc phân cấp giúp giảm được chi phí cho mạng xác định được các tài nguyên để phân bổ để hoạt động hiệu quả.
- Do định sẵn chức năng của các nút cảm biến, nên việc nâng cấp khả năng tính toán hay thay đổi kiến trúc, thiết kế của nút sẽ nâng cao được hiệu suất sử dụng và tuổi thọ của nút.

2.4. YÊU CẦU BẢO MẬT TRONG MẠNG CẢM BIẾN KHÔNG DÂY

Do đặc điểm bị hạn chế về kích thước, tài nguyên, năng lực tính toán và năng lượng của các nút cảm biến. Nên để đảm bảo an toàn thông tin trong truyền tin của mạng cảm biến không dây, cần phải có phương pháp mã hóa và giải mã có tốc độ nhanh, tốn ít tài nguyên. Tuy nhiên, vẫn phải đảm bảo độ an toàn như độ dài khóa, độ lớn của không gian khóa và không gian khóa đủ lớn để tránh bị tấn công vét cạn.

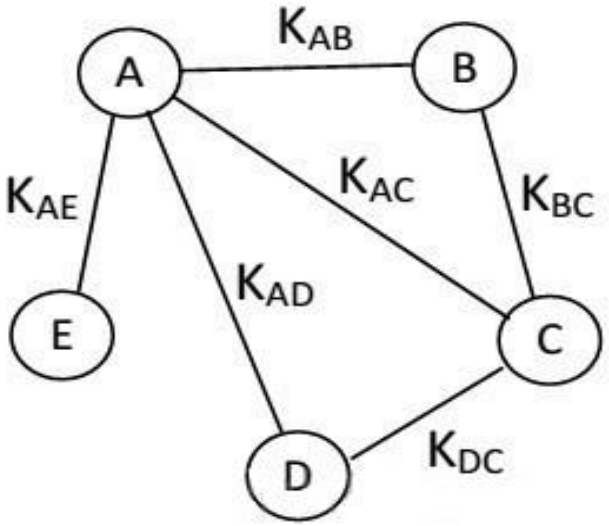
Cũng như các hệ thống khác, khi triển khai các phương pháp đảm bảo an toàn thông tin cho mạng cảm biến không dây sẽ nảy sinh các hạn chế như: độ dài khóa hạn chế, mất an toàn trong việc phân phối khóa và đảm bảo an toàn trong quản lý, sử dụng khóa.

- Độ dài khóa: Do các nút cảm biến bị hạn chế về tài nguyên và năng lực tính toán, nên độ dài khóa quá dài sẽ không khả thi khi áp dụng cho mạng. Khi độ dài khóa ngắn thì dễ bị tấn công vét cạn.
- Đảm bảo an toàn trong phân phối khóa: Trong mạng cảm biến không dây, các nút cảm biến truyền thông với nhau đều trên kênh truyền không an toàn. Vì vậy, khi trao đổi khóa giữa người gửi và người nhận, khóa có thể bị lộ bởi rất nhiều nguyên nhân. Việc này đòi hỏi phải có phương thức phân phối khóa an toàn.
- Đảm bảo an toàn trong quản lý, sử dụng khóa: Do khả năng các khóa có thể bị lộ trong khi sử dụng hay khi triển khai hệ thống. Do vậy phải có phương pháp quản lý và trao đổi khóa hiệu quả.

Do đặc điểm và các hạn chế về tài nguyên phần cứng nên phương pháp mã hóa áp dụng cho mạng cảm biến không dây khả thi nhất là phương pháp mã hóa đối xứng. Tuy nhiên, trong mạng cảm biến không dây có số lượng nút cảm biến trong mạng là lớn và các thuật toán mã hóa khóa đối xứng sử dụng khóa chung cho cả bên gửi và bên nhận nên các hạn chế khi triển khai mã hóa khóa đối xứng được thể hiện rõ như sau:

- Độ dài khóa bị giới hạn: Do tài nguyên phần cứng bị hạn chế, nên khi sử dụng các số lớn làm khóa phải tính toán tránh bị tràn.
- Hạn chế trong việc quản lý và sử dụng khóa: Do mạng cảm biến không dây có số lượng các nút cảm biến rất lớn. Trong khi đó, thuật toán mã hóa đối xứng

đòi hỏi mỗi cặp nút cảm biến phải có một khóa riêng. Giả sử trong mạng có N nút cảm biến và mỗi cặp người sử dụng cần có một khóa bí mật riêng, như vậy cần có $\frac{N(N-1)}{2}$ khóa. Do vậy sẽ dẫn đến khó khăn cho việc lưu trữ vì có quá nhiều khóa phải nhớ.



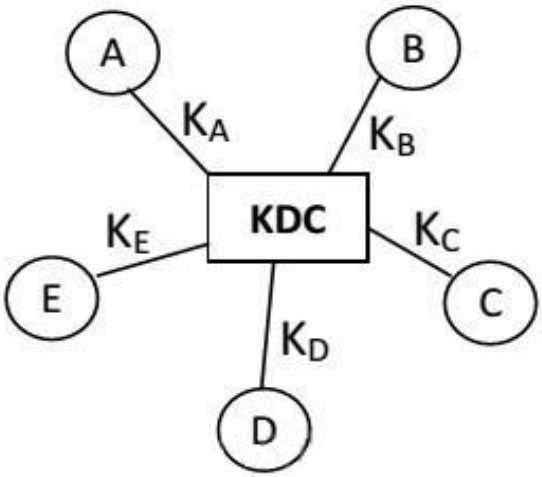
Hình 2.4: Các khóa riêng giữa các nút [4]

- Khó khăn trong việc phân phối: Do hạn chế về tài nguyên phần cứng nên khóa sử dụng không được quá dài, điều này đồng nghĩa với việc khóa có khả năng bị phá khi kẻ tấn công sử dụng phương pháp vét cạn. Điều này đòi hỏi phải có phương thức quản lý và phân phối khóa hiệu quả khi số lượng nút lớn và thời gian cần thay đổi khóa ngắn.

  Do vậy phương pháp trao đổi khóa bằng trung tâm phân phối khóa (Key Distribution Center – KDC) giúp đơn giản hóa vấn đề này. Đây chính là mô hình mà Domain Controller trên hệ điều hành windows đang triển khai.

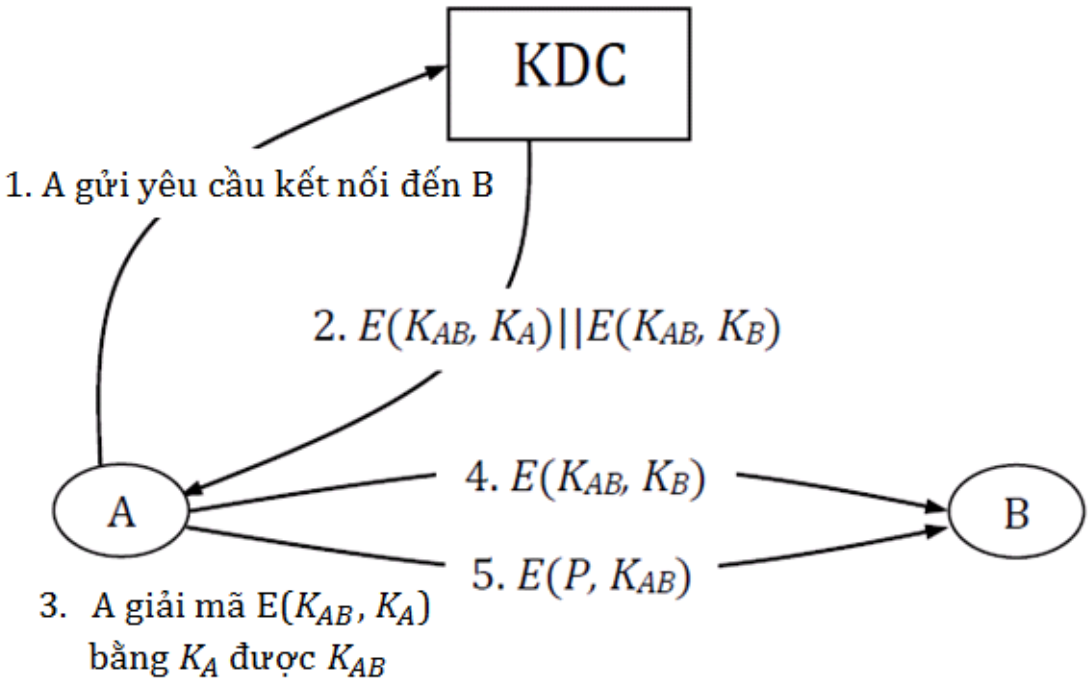
  Trong mô hình sử dụng KDC, mỗi người sử dụng chỉ cần có một khóa bí mật với KDC. Còn khóa dùng để trao đổi dữ liệu giữa các người sử dụng với nhau sẽ do KDC cung cấp khi có yêu cầu. Như vậy, nút mạng chỉ cần lưu 1 khóa duy

nhất và việc thay đổi khóa sẽ chỉ do KDC thay đổi. Mô hình trao đổi khóa sử dụng KDC như sau:



Hình 2.5: Mô hình trao đổi khóa tập trung [4]

Giả sử, nút A và B chỉ có khóa bí mật với KDC. Nếu A cần trao đổi dữ liệu với B thì phải thiết lập khóa chung giữa A và B, các bước như sau:



Hình 2.6: Quá trình trao đổi khóa bí mật khi triển khai mô hình KDC [4]

Bước 1: A gửi yêu cầu muốn trao đổi dữ liệu với B cho KDC.

Bước 2: KDC tạo một khóa bí mật K_{AB} và mã hóa thành 2 bản. Một bản được mã hóa với khóa bí mật của A E(K_{AB}, K_A), một bản được mã hóa với khóa bí mật của B E(K_{AB}, K_B).

Bước 3: A sẽ giải mã E(K_{AB}, K_A) bằng K_A để có được K_{AB}.

Bước 4: A gửi đi E(K_{AB}, K_B) cho B, B dùng K_B để giải mã để có được K_{AB}.

Bước 5: A và B trao đổi với nhau bằng khóa bí mật K_{AB}.

2.5. KẾT LUẬN CHƯƠNG

Trong nội dung chương 2, luận văn đưa ra các khái niệm về mạng cảm biến không dây. Nội dung chương đã đưa ra và phân tích những đặc điểm của mạng cảm biến không dây và thách thức khi áp dụng các mô hình mã hóa đảm bảo an toàn thông tin vào mạng cảm biến không dây.

CHƯƠNG III: MÔ HÌNH BLOM

3.1. MÔ HÌNH BLOM

Năm 1985, Blom đã đưa ra một mô hình phân phối khóa, mà sau đây được gọi là mô hình Blom. Mô hình cho phép bất kỳ cặp nút mạng nào đều có thể tìm được khóa riêng. Mô hình Blom yêu cầu một số nguyên tố q, một ma trận công khai P và một ma trận bí mật S.

Trong mô hình này, một mạng có n nút cảm biến và có chỉ số an toàn t, t bé hơn n và được chọn sao cho t $\geq \frac{n}{2} + 1$ [5].Chỉ số an toàn t thể hiện số lượng kết nối tối đa của một nút mạng với các nút khác trong mạng. Nếu có ít nhất t+1 nút bị lộ khóa riêng mới có thể lộ tất cả các khóa của mạng. Giá trị của t càng lớn càng an toàn cho mạng, tuy nhiên cũng làm tăng mức độ tính toán cũng như dung lượng bộ nhớ để lưu trữ thông tin.

Do giá trị của khóa chung và khóa riêng đều nằm trong tập G(q). Vì vậy, số nguyên tố q quyết định độ dài khóa và không gian khóa chung giữa hai nút. Để đảm bảo giá trị khóa giữa các nút là khác nhau và độ dài khóa đủ lớn đòi hỏi giá trị q lớn. Tuy nhiên, giá trị q lớn làm tăng giá trị của các phần tử trong các ma trận, làm tăng khối lượng tính toán.

Giả sử ta cần triển khai một mạng cảm biến không dây có n nút mạng, tất cả các cảm biến đều cần trao đổi thông tin bí mật với nhau. Mô hình bảo mật cần triển khai cho mạng là hệ mã hóa khóa đối xứng (ví dụ như: DES, AES …). Như vậy, toàn bộ mạng cần phải có $\frac{n(n-1)}{2}$ khóa khác nhau cho các cặp kết nối giữa các nút cảm biến trong mạng với nhau. Do các nút cảm biến bị hạn chế về tài nguyên và năng lực xử lý, nên cần phải có một trung tâm quản lý khóa tập trung. Trung tâm quản lý khóa phải truyền n(n-1) khóa đến n nút mạng bằng kênh truyền bí mật.

Ban đầu, nút mạng cơ sở xây dựng một ma trận P có kích thước (t+1) x n,trong đó n là kích thước của mạng, t là chỉ số an toàn và một số nguyên tố q. P được *công khai* cho tất cả các nút mạng và được xây dựng bằng ma trận Vandermonde, điều này đảm bảo cột bất kỳ trong t+1 cột của P đều là *độc lập tuyến tính*.

$$P = \begin{bmatrix} 1 & 1 & 1 & & 1 \\ a_1 & a_2 & a_3 & \cdots & a_n \\ a_1^2 & a_2^2 & a_3^2 & & a_n^2 \\ & \vdots & & \ddots & \vdots \\ a_1^t & a_2^t & a_{n3}^t & \cdots & a_n^t \end{bmatrix} \quad (a_i \neq a_j \text{ nếu } i \neq j \text{ và } a_i \neq 0)$$

Sau đó, nút mạng cơ sở chọn một ma trận đối xứng ngẫu nhiên S trên tập G(q) có kích thước (t+1) x (t+1). Trong đó, ma trận *S là bí mật* và chỉ có nút mạng cơ sở mới biết. Sau đó tính ma trận khóa chung A = $(S.P)^T$, vì ma trận S là đối xứng nên ta có:

K = A.P = $(S.P)^T$. P = P^T. S^T. P = P^T. S.P = P^T. A = P^T. A^T =$(A.P)^T$ = K^T

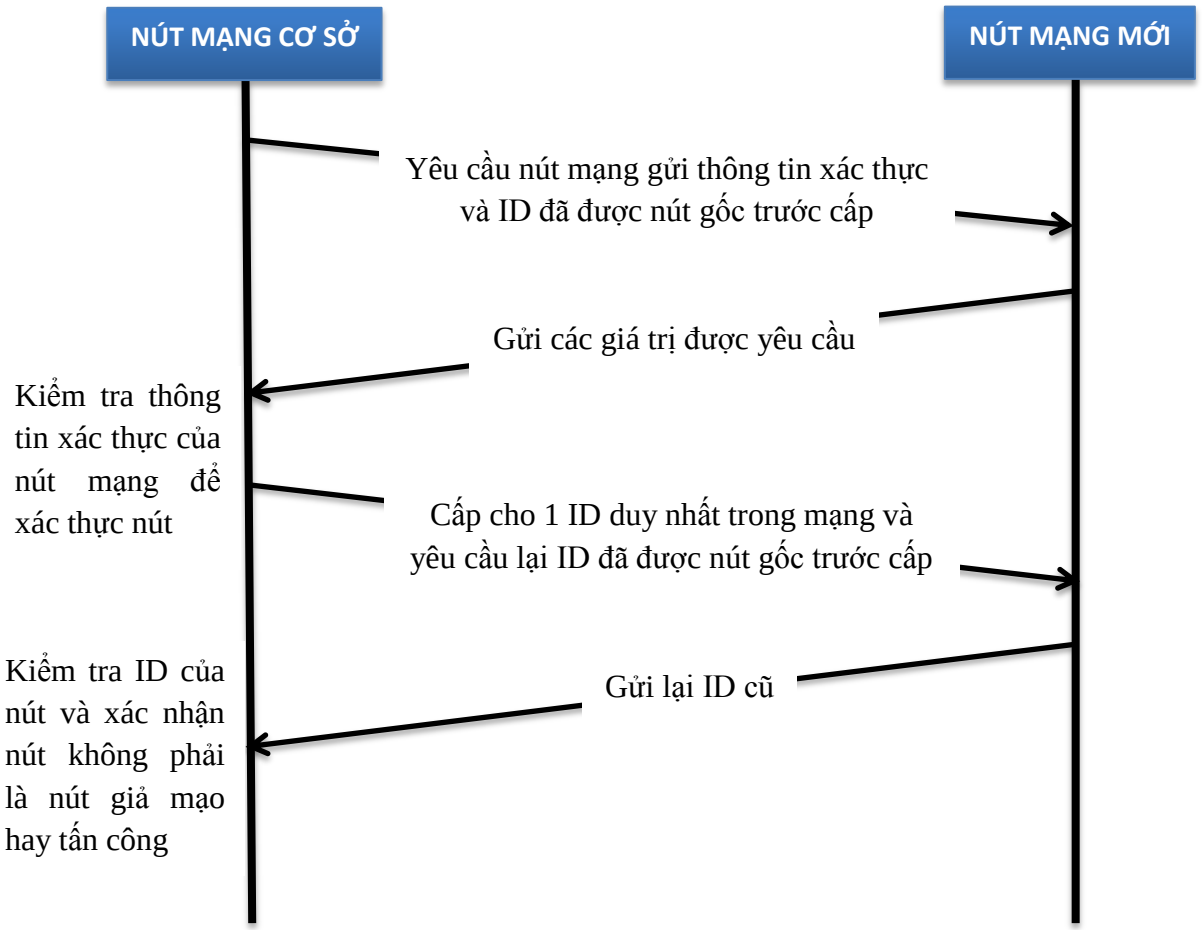
Qua chứng minh ta thấy rằng: K = K^T, như vậy ma trận K là ma trận đối xứng. Do vậy mọi phần tử trong ma trận K ở hàng thứ i và cột thứ j luôn bằng một phần tử khác trong K nằm ở hàng thứ j và cột thứ i, tức là K_{ij} = K_{ji}. Do đó ma trận K luôn tạo nên một cặp K_{ij} và K_{ji} có giá trị bằng nhau và được sử dụng như khóa chung cho nút i và nút j.

Như vậy, để có thể tạo khóa chung giữa 2 nút bất kỳ, các nút sẽ lấy giá trị khóa riêng của mình là một hàng tương ứng với ID của nút trên ma trận khóa riêng A. Sau đó nhân với hàng tương ứng với số ID của nút mạng cần kết nối trên ma trận công khai P. Khóa riêng A của nút mạng chỉ có nút mạng có ID trùng với số hàng mới biết được, nên đảm bảo chỉ có nút mạng có ID đúng mới có thể có khóa A đúng và tính đúng được khóa chung.

3.2. CÁC BƯỚC BẮT TAY VÀ THIẾT LẬP KHÓA CHUNG

Ngay từ ban đầu triển khai mạng, nút mạng cơ sở sẽ gán cho mỗi nút mạng một ID duy nhất và ID này được thông báo công khai cho tất cả các nút mạng khác biết trước khi tính toán các ma trận để phân phối khóa. Khi các nút mạng nhận được ID của mình, nó sẽ thông báo lại cho nút mạng cơ sở biết các thông tin của nút đã dùng để xác thực với nút cơ sở để nút cơ sở biết được đã cấp đúng ID cho nút.

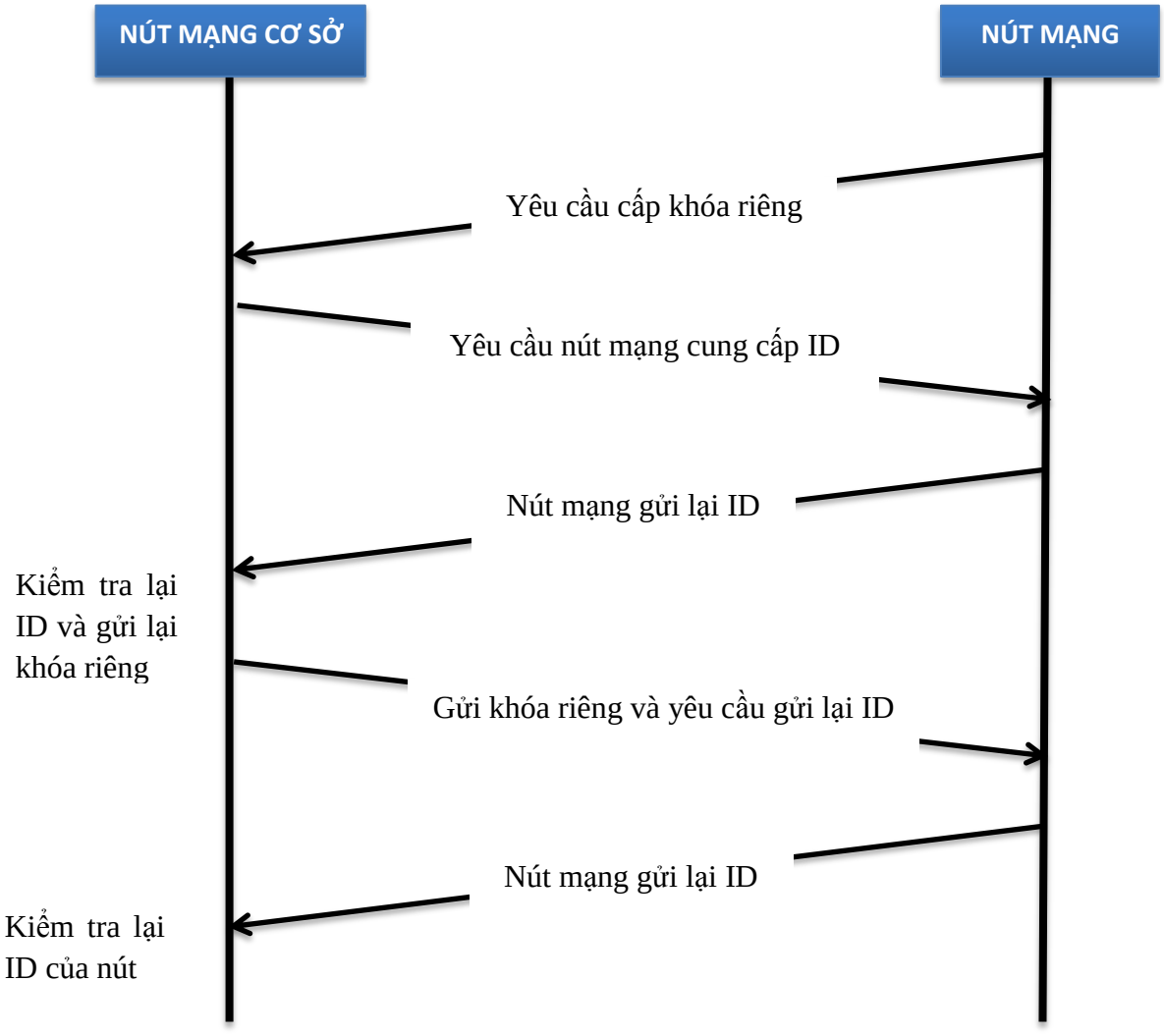
Nếu có một nút mạng xâm nhập ngay từ đầu triển khai hay để phân biệt nút mới vào mạng là tin cậy hay không. Nút mạng cơ sở sẽ yêu cầu nút mạng cung cấp các thông tin của nút mạng để kiểm tra. Các bước chi tiết được mô tả như hình sau:



Hình 3.1: Quá trình thêm nút mạng mới [7]

Sau khi đăng ký ID cho các nút mạng, nút mạng cơ sở sẽ xây dựng một ma trận công khai P và gửi quảng bá cho tất cả các nút mạng. Đồng thời cũng đưa ra một ma trận bí mật S chỉ có nút mạng cơ sở biết được ma trận này. Nút mạng cơ sở sẽ tính tiếp ma trận A = $(S.P)^T$. Các hàng của ma trận A được gọi là khóa riêng của các nút mạng có id tương ứng và được gửi cho các nút mạng khi có yêu cầu.

Giả sử, nếu nút mạng A cần giao tiếp với nút mạng B, nút mạng A và B sẽ yêu cầu nút mạng cơ sở cung cấp khóa riêng cho A và B. Các bước cấp khóa riêng chi tiết như sau:

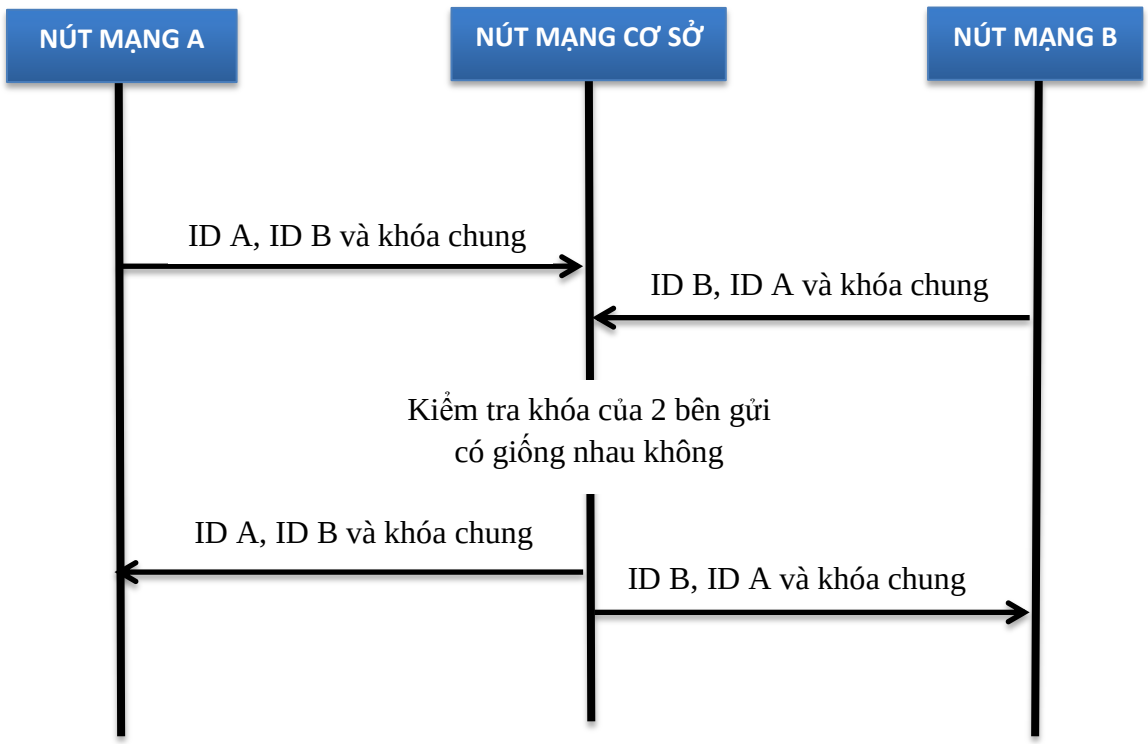


Hình 3.2: Quá trình gửi khóa riêng cho nút mạng [7]

Nút gốc yêu cầu nút mạng gửi lại ID cũ lần 2 sau khi cấp khóa riêng cho nút để kiểm tra xem khóa riêng gửi đúng nút có ID đã yêu cầu không. Trong quá trình gửi khóa riêng, nút cơ sở phát hiện ra ID của nút mạng là giả mạo. Nút cơ sở sẽ dừng việc bắt tay và gửi quảng bá cho tất cả các nút mạng để ngăn chặn tất cả thông tin trao đổi giữa các nút trong mạng với nút giả mạo.

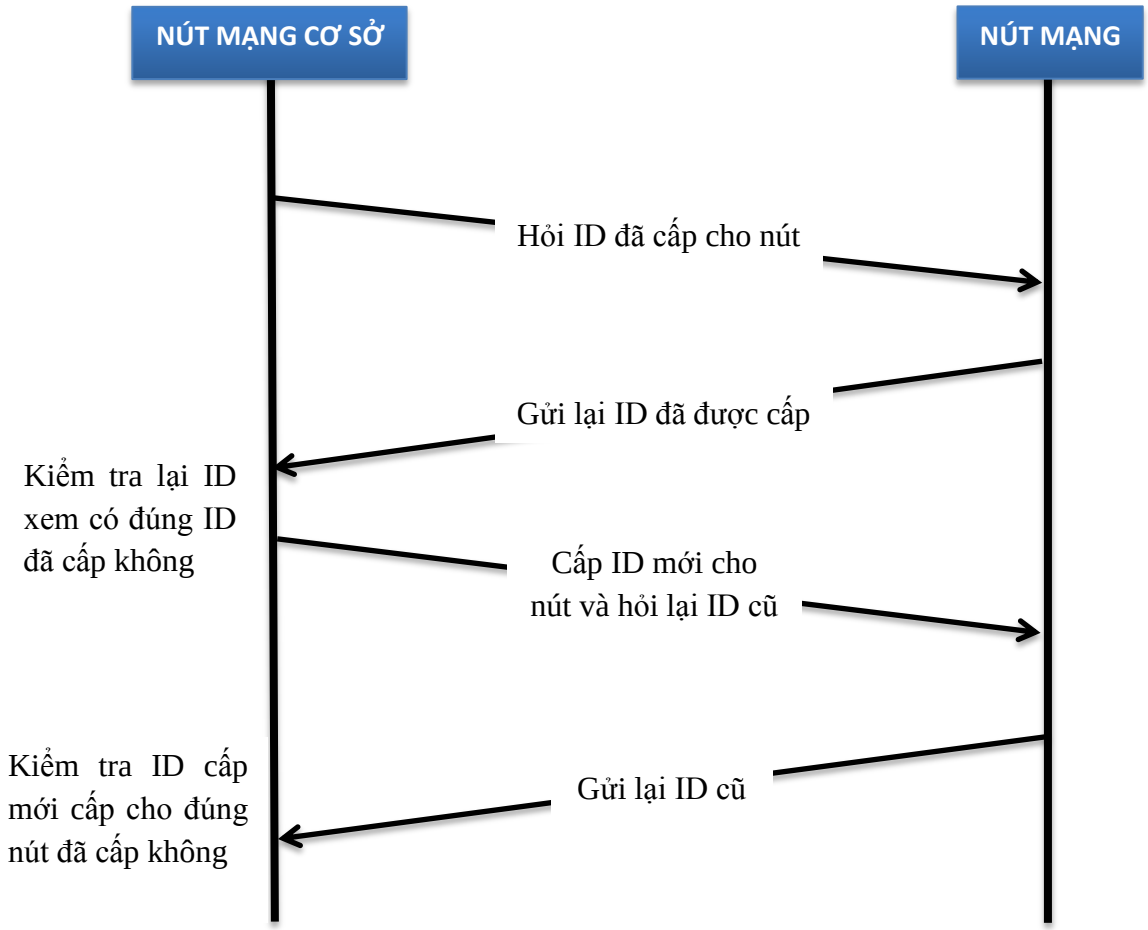
Sau khi có được khóa riêng, nút A và nút B sẽ tính được khóa chung của nút A với nút B bằng cách nhân khóa riêng (hàng tương ứng với ID của nút mạng trên ma trận A) với cột tương ứng của ID nút mạng cần kết nối đến trong ma trận công khai P (tính A.P).

Khi khóa chung đã được thiết lập tại 2 nút. Trước khi giao tiếp với nhau, 2 nút sẽ gửi thông tin cho nút mạng cơ sở để xác thực lại thông tin.



Hình 3.3: Quá trình xác thực lại trước khi gửi dữ liệu giữa 2 nút [7]

Nếu nút cơ sở thay đổi ma trận bí mật, nút cơ sở sẽ yêu cầu các nút mạng cập nhật ID mới, các bước thực hiện như sau:



Hình 3.4: Quá trình cập nhật lại ID mới cho nút mạng [7]

3.3. VÍ DỤ

Một mạng cảm biến không dây gồm 8 cảm biến (n=8), chỉ số an toàn t = 8/2= 4 và một số nguyên tố q = 31.

Ta tính ma trận Vandermonde có kích thước 8×5

$$V = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 & 7^2 & 8^2 \\ 1 & 2^3 & 3^3 & 4^3 & 5^3 & 6^3 & 7^3 & 8^3 \\ 1 & 2^4 & 3^4 & 4^4 & 5^4 & 6^4 & 7^4 & 8^4 \end{bmatrix}$$

Ta tính được ma trận công khai P bằng ma trận V chia lấy dư cho q. Ma trận này được gửi quảng bá cho tất cả các nút mạng

$$P = V \ mod \ q = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 9 & 16 & 25 & 5 & 18 & 2 \\ 1 & 8 & 27 & 2 & 1 & 30 & 2 & 16 \\ 1 & 16 & 19 & 8 & 5 & 25 & 14 & 4 \end{bmatrix}$$

Chọn một ma trận bí mật S, S là ma trận đối xứng (trong ví dụ này giới hạn các phần tử của ma trận S nhỏ hơn 15). Ma trận này chỉ có nút gốc biết

$$S = \begin{bmatrix} 9 & 8 & 7 & 0 & 9 \\ 8 & 0 & 1 & 0 & 11 \\ 7 & 1 & 7 & 1 & 6 \\ 0 & 0 & 1 & 10 & 3 \\ 9 & 11 & 6 & 3 & 10 \end{bmatrix}$$

Nút gốc tính ma trận khóa riêng A = $(S.P)^T$ mod q.

$$S.P = \begin{bmatrix} 33 & 91 & 329 & 271 & 315 & 424 & 146 & 205 \\ 20 & 66 & 292 & 46 & 82 & 309 & 35 & 80 \\ 22 & 64 & 240 & 212 & 194 & 341 & 131 & 176 \\ 14 & 58 & 244 & 50 & 114 & 111 & 59 & 192 \\ 39 & 111 & 405 & 275 & 373 & 429 & 149 & 253 \end{bmatrix} \text{ mod } 31$$

$$= \begin{bmatrix} 2 & 29 & 19 & 23 & 5 & 21 & 22 & 19 \\ 20 & 4 & 13 & 15 & 20 & 30 & 4 & 18 \\ 22 & 2 & 23 & 26 & 8 & 0 & 7 & 21 \\ 14 & 27 & 27 & 19 & 21 & 18 & 28 & 6 \\ 8 & 18 & 2 & 27 & 1 & 26 & 25 & 5 \end{bmatrix}$$

Suy ra: $A = (S.P)^T = \begin{bmatrix} 2 & 20 & 22 & 14 & 8 \\ 29 & 4 & 2 & 27 & 18 \\ 19 & 13 & 23 & 27 & 2 \\ 23 & 15 & 26 & 19 & 27 \\ 5 & 20 & 8 & 21 & 1 \\ 21 & 30 & 0 & 18 & 26 \\ 22 & 4 & 7 & 28 & 25 \\ 19 & 18 & 21 & 6 & 5 \end{bmatrix}$

Sau khi tính được ma trận A, mỗi nút mạng sẽ được nhận khóa riêng của mình theo ID của nút tương ứng với hàng trong ma trận A. Giả sử nút mạng có ID là 2 cần trao đổi thông tin với nút mạng có ID là 8. Khi đó nút có ID 2 chỉ cần lấy khóa riêng của mình (hàng 2 trong ma trận A) nhân với cột 8 trong ma trận P. Ở nút 8 cũng làm tương tự.

$$K_{2,8} = A_2.P_8 = [29 \quad 4 \quad 2 \quad 27 \quad 18] \begin{bmatrix} 1 \\ 8 \\ 2 \\ 16 \\ 4 \end{bmatrix} = 35848 \bmod 31 = 12$$

$$K_{8,2} = A_8.P_2 = [19 \quad 18 \quad 21 \quad 6 \quad 5] \begin{bmatrix} 1 \\ 2 \\ 4 \\ 8 \\ 16 \end{bmatrix} = 49488 \bmod 31 = 12$$

Ta có thể tính toàn bộ ma trận khóa K = A.P để thấy rằng ma trận K là ma trận đối xứng ($K_{ij} = K_{ji}$)

$$K = A.P \bmod q = \begin{bmatrix} 4 & 18 & 22 & 17 & 24 & 2 & 24 & 7 \\ 18 & 24 & 15 & 1 & 3 & 4 & 9 & 12 \\ 22 & 15 & 16 & 25 & 22 & 25 & 27 & 5 \\ 17 & 1 & 25 & 11 & 21 & 13 & 14 & 3 \\ 24 & 3 & 22 & 21 & 30 & 0 & 10 & 4 \\ 2 & 4 & 25 & 13 & 0 & 6 & 24 & 1 \\ 24 & 9 & 27 & 14 & 10 & 24 & 0 & 17 \\ 7 & 12 & 5 & 3 & 4 & 1 & 17 & 11 \end{bmatrix}$$

3.4. NHẬN XÉT

Mô hình Blom đã giải quyết được sự hạn chế lưu trữ và tính toán của các nút cảm biến. Thay vì các nút cảm biến phải tự trao đổi, tính toán khóa thì nút cơ sở sẽ thực hiện nhiệm vụ này và nút mạng chỉ cần lưu một hàng trong ma trận bí mật A (khóa riêng của nút) và một cột trong ma trận công cộng P để tính khóa. Việc quản lý và phân phối khóa tập trung giúp nâng cao khả năng bảo mật, mở rộng mạng hay thay đổi khóa khi cần.

Trong mô hình Blom, các nút mạng sử dụng các thông tin của nhà sản xuất gán cho ban đầu để xác thực với nút cơ sở. Khi đã được xác thực, nút mạng sẽ nhận được ID do nút cơ sở cấp và dùng để xác thực trước khi nhận khóa trong quá trình làm việc trong mạng. Các thông tin này được sử dụng như một chứng chỉ số và chứng chỉ số này được tạo bởi nhà sản xuất và nút cơ sở nhằm đảm bảo tính hợp lệ và chống giả mạo của nút mạng.

Khi được cấp phát khóa riêng, các nút mạng sẽ tính được khóa bảo mật. Khóa riêng được tính cả 2 bên gửi và bên nhận và được gửi lại để xác nhận cho nút cơ sở. Nút cơ sở sẽ tính lại khóa riêng giữa hai nút nếu giá trị khóa của hai nút như nhau là đúng. Khóa này như một chữ ký số, đảm bảo chỉ có nút có khóa riêng và khóa công khai đúng thì mới có thể tính được khóa đúng.

Việc sử dụng ma trận công khai và ma trận bí mật để tính ra khóa chung giữa các nút mạng có ý nghĩa như chứng chỉ số. Cả 2 nút mạng đều có thể tính được khóa bảo mật chung nhờ việc tính khóa riêng của mình với khóa công khai của nút mạng cần kết nối. Tuy nhiên, chỉ có nút mạng có khóa riêng đúng mới có thể tính được khóa chung đúng và khóa được xác nhận lại bởi nút cơ sở.

Tuy nhiên, việc sử dụng ma trận Vandermonde để tính toán làm cho việc lưu trữ và tính toán ở nút mạng cơ sở trở nên khó khăn. Với mô hình Blom đưa ra, ma

trận công khai ban đầu là ma trận vandermonde có hạng là n×t. Nếu mạng có quy mô n nút mạng thì số hạng lớn nhất trong ma trận Vandermonde sẽ là n^t (t là chỉ số an toàn). Nếu chọn chỉ số an toàn t có giá trị lớn sẽ làm kích thước của ma trận công khai P tăng, làm tăng bộ nhớ của nút cần sử dụng và khối lượng tính toán khóa cũng tăng lên.

3.5. TỔNG KẾT CHƯƠNG

Trong chương 3, luận văn đã mô tả được mô hình hoạt động và lấy ví dụ cho mô hình Blom. Nội dung chương đã đưa ra và phân tích được các ưu điểm, các vấn đề mà mô hình Blom giải quyết được khi áp dụng mô hình mã hóa khóa đối xứng vào mạng cảm biến không dây. Nội dung chương cũng đã đưa ra các thách thức, hạn chế của mô hình Blom khi áp dụng vào mạng cảm biến không dây.

CHƯƠNG IV: CÁC MÔ HÌNH BLOM CẢI TIẾN

4.1. CÁC MÔ HÌNH BLOM CẢI TIẾN

Mô hình Blom đã tạo nên một bước đột phá quan trọng trong việc đảm bảo an toàn bảo mật cho mạng cảm biến không dây. Mô hình Blom phù hợp với mô hình, kiến trúc mạng cảm biến không dây và giải quyết được các vấn đề tồn tại của mạng cảm biến không dây khi áp dụng các phương án đảm bảo an toàn thông tin.

Tuy nhiên, do các hạn chế về năng lượng, tài nguyên và năng lực tính toán của các nút mạng cảm biến. Nên cần phải cải tiến mô hình Blom để tăng tốc độ tính toán và giảm dung lượng bộ nhớ lưu trữ của nút mạng. Vì vậy, để tối ưu mô hình Blom đã có một số đề xuất sau:

- Thay thế ma trận công khai P là ma trận Vandermonde thành ma trận Adjacency [5].
- Thay thế ma trận công khai P là ma trận Vandermonde thành ma trận Hadamard [6].
- Thay thế ma trận công khai P là ma trận Vandermonde thành một ma trận ngẫu nhiên và đảm bảo các cột trong ma trận là độc lập tuyến tính với nhau [7].

Ngoài ra, trong đề xuất [6] cũng tính toán mô phỏng để đưa ra được chỉ số an toàn t. Việc chỉ ra giới hạn t giúp giảm số lượng ô nhớ để lưu trữ ma trận P và cũng nâng cao được một phần tốc độ tính toán của mô hình Blom. Để hiểu rõ hơn các cải tiến [5, 6, 7] ta sẽ thực hiện phân tích và mô phỏng các cải tiến.

4.1.1. Mô hình Blom sử dụng ma trận Adjacency

Với mô hình Blom sử dụng ma trận Adjacency (ma trận kề), các phần tử trong ma trận bao gồm các giá trị 1 và 0. Ma trận kề được sử dụng trong tính toán đồ thị, nó ánh xạ từ các đường kết nối giữa các điểm trong đồ thị vào trong ma trận. giả

sử, với các điểm i và j có kế nối với nhau, khi ánh xạ sang ma trận kề thì vị trí hàng i cột j và hàng j cột i sẽ có giá trị bằng 1 và ngược lại, nếu không có kết nối giá trị ánh xạ sang đồ thị sẽ là 0.

Khi sử dụng ma trận kề vào mô hình Blom, nó sẽ giảm được mức độ tính toán và giảm dung lượng khi lưu trữ. Trong cải tiến [5] ma trận Adjacency là loại ma trận vô hướng, nên ma trận Adjacency là ma trận đối xứng.

Ví dụ: Một mạng có số nút là 4, chọn hệ số an toàn t=3 và số nguyên tố q=31

Ta có ma trận M = $\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ và ma trận S = $\begin{bmatrix} 10 & 6 & 5 & 1 \\ 6 & 7 & 10 & 7 \\ 5 & 10 & 6 & 6 \\ 1 & 7 & 6 & 9 \end{bmatrix}$

Tính ma trận P bằng cách thay thế các phần tử có giá trị 0 bằng q-1 =30

Nên P = $\begin{bmatrix} 1 & 1 & 30 & 30 \\ 1 & 1 & 1 & 30 \\ 30 & 1 & 30 & 1 \\ 30 & 30 & 1 & 30 \end{bmatrix}$ $\rightarrow$ A = $(S.P)^T$ mod q = $\begin{bmatrix} 16 & 13 & 15 & 8 \\ 21 & 23 & 21 & 14 \\ 7 & 14 & 16 & 16 \\ 5 & 10 & 6 & 6 \end{bmatrix}$

Suy ra: ma trận khóa K = A.P mod q = $\begin{bmatrix} 29 & 13 & 21 & 15 \\ 13 & 3 & 6 & 21 \\ 21 & 6 & 30 & 16 \\ 15 & 21 & 16 & 6 \end{bmatrix}$

4.1.2. Mô hình Blom sử dụng ma trận Hadamard

Ma trận Hadamard là ma trận có dạng.

$$H_m = \begin{bmatrix} H_{m-1} & H_{m-1} \\ H_{m-1} & -H_{m-1} \end{bmatrix}$$ Trong đó: h_{ij} = 1 hoặc h_{ij} = -1

Với mô hình Blom sử dụng ma trận Hadamard, các phần tử trong ma trận bao gồm các giá trị 1 và -1. Nó sẽ giảm được mức độ tính toán và giảm dung lượng khi lưu trữ.

Ví dụ: Một mạng có số nút là 4, chọn hệ số an toàn t=3 và số nguyên tố q=31

Ta có ma trận H = $\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$ và ma trận S = $\begin{bmatrix} 1 & 10 & 9 & 1 \\ 10 & 1 & 2 & 3 \\ 9 & 2 & 2 & 2 \\ 1 & 3 & 2 & 9 \end{bmatrix}$

Tính ma trận P

P = H mod q = $\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 30 & 1 & 30 \\ 1 & 1 & 30 & 30 \\ 1 & 30 & 30 & 1 \end{bmatrix}$ $\rightarrow$ A = $(S.P)^T$ mod q = $\begin{bmatrix} 21 & 16 & 15 & 15 \\ 30 & 8 & 7 & 22 \\ 1 & 6 & 7 & 24 \\ 14 & 10 & 7 & 5 \end{bmatrix}$

Suy ra: ma trận khóa K = A.P mod q = $\begin{bmatrix} 5 & 5 & 7 & 5 \\ 5 & 7 & 9 & 6 \\ 7 & 9 & 7 & 12 \\ 5 & 6 & 12 & 2 \end{bmatrix}$

4.1.3. Mô hình Blom sử dụng ma trận ngẫu nhiên.

Với mô hình dùng ma trận P bất kỳ, nó sẽ giảm được thời gian tính toán và độ lớn của các phần tử trong ma trận so với việc dùng ma trận Vandermonde mà vẫn đảm bảo tính chất đối xứng của ma trận K.

Ví dụ: Một mạng có số nút là 4, chọn hệ số an toàn t=3 và số nguyên tố q=31

Ta có ma trận P = $\begin{bmatrix} 5 & 4 & 0 & 7 \\ 0 & 5 & 7 & 7 \\ 4 & 6 & 3 & 0 \\ 3 & 3 & 6 & 6 \end{bmatrix}$ và ma trận S = $\begin{bmatrix} 2 & 1 & 2 & 6 \\ 1 & 7 & 3 & 7 \\ 2 & 3 & 2 & 11 \\ 6 & 7 & 11 & 6 \end{bmatrix}$

Tính ma trận A = $(S.P)^T$ mod q = $\begin{bmatrix} 25 & 20 & 6 & 7 \\ 30 & 12 & 13 & 30 \\ 20 & 24 & 1 & 6 \\ 26 & 22 & 0 & 17 \end{bmatrix}$

Suy ra: ma trận khóa K = A.P mod q = $\begin{bmatrix} 6 & 5 & 21 & 27 \\ 5 & 20 & 14 & 12 \\ 21 & 14 & 10 & 19 \\ 27 & 12 & 19 & 29 \end{bmatrix}$

Để đánh giá được hiệu quả của các đề xuất cải tiến trong [5, 6, 7], ta cần tiến hành các mô phỏng đánh giá.

4.2. MÔ PHỎNG

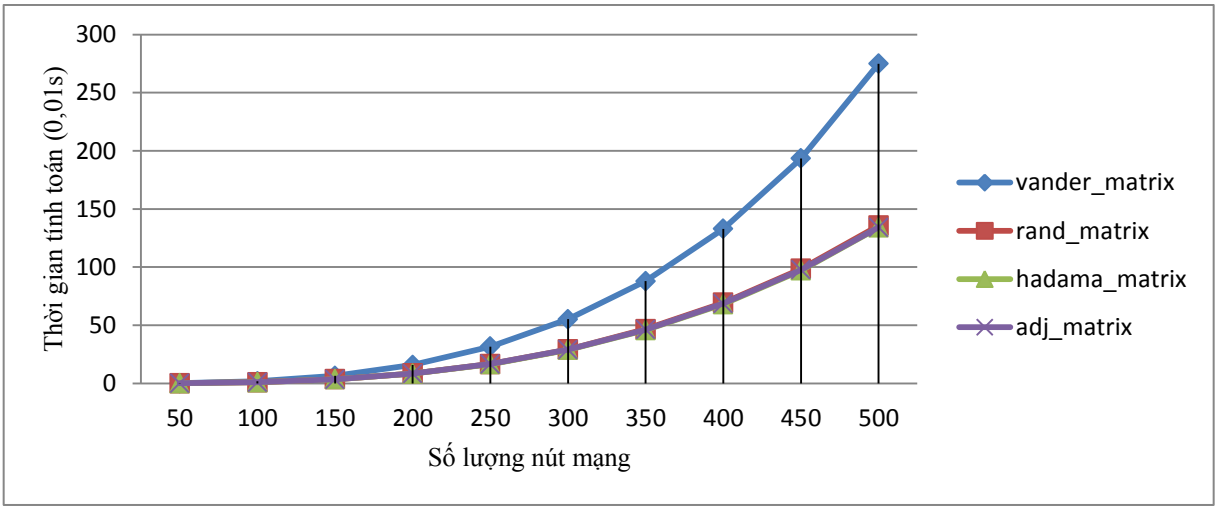
Trong các cải tiến [5, 6, 7], các tác giả đã lấy ví dụ và chứng minh được tính chất của mô hình Blom không thay đổi khi áp dụng các cải tiến. Tuy nhiên, các mô phỏng trong [5, 6, 7] chỉ đánh giá được các cải tiến riêng lẻ với mô hình Blom mà chưa so sánh chung giữa các cải tiến với nhau và với mô hình Blom. Mặt khác, trong các cải tiến [5, 6, 7] các mô phỏng chỉ đưa ra đánh giá độ phức tạp tính toán mà chưa đưa ra được việc áp dụng các cải tiến đem lại lợi ích như thế nào.

Vì vậy, để đánh giá các phương án cải tiến mô hình Blom trong [5, 6, 7], ta xây dựng chương trình tính toán khóa theo mô hình Blom để đánh giá độc lập với tác giả. Chương trình xây dựng bằng phần mềm NetBeans và ngôn ngữ lập trình Java. Chương trình có các giá trị đầu vào là ma trận công khai P và ma trận bí mật S. Thông tin đầu ra là ma trận khóa chung K và thời gian tính toán. Ta đánh giá thời gian tính toán giữa mô hình Blom sử dụng ma trận Vandermonde so với mô hình Blom khi áp dụng các cải tiến trong [5, 6, 7].

Kịch bản mô phỏng:

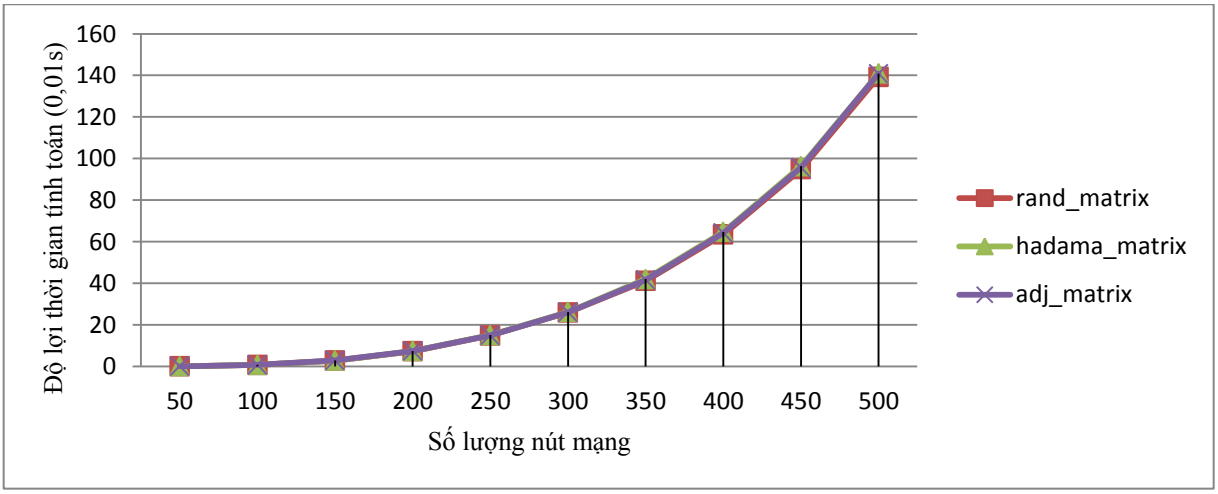
Ta thực hiện mô phỏng với một mạng có số nút mạng thay đổi từ 0 đến 500 và có bước là 50, hệ số an toàn $t = \frac{n}{2} + 1$, số nguyên tố q=1181. Thực hiện mô phỏng so sánh thời gian tính toán khóa với các ma trận P khác nhau với cùng ma trận S có kích thước (t+1 x t+1), giá trị các phần tử trong S được giới hạn từ 0 đến q. Mô

phỏng được thực hiện 100 lần và lấy kết quả thời gian tính toán trung bình. Kết quả thu được như hình dưới, với chiều dọc là thời gian tính toán (đơn vị 0,01s), chiều ngang là số nút của mạng (độ lớn của ma trận P). Kết quả mô phỏng như sau:



Hình 4.1: Thời gian tính toán của mô hình Blom và các cải tiến [5, 6, 7]

Ta thấy, thời gian tính toán khi áp dụng các cải tiến trong [5, 6, 7] thấp hơn thời gian tính toán khi sử dụng ma trận Vandermonde. Khi số nút tăng lên lợi thế thời gian càng tăng. Để so sánh được ưu mức độ hiệu quả giữa các mô hình Blom cải tiến, ta so sánh độ lợi về thời gian khi áp dụng các cải tiến trong [5, 6, 7] so với sử dụng ma trận Vandermonde trong hình sau.



Hình 4.2: Độ lợi thời gian tính toán khi áp dụng mô hình cải tiến [5, 6, 7]

Hình 3.2 thể hiện cho ta thấy độ lợi về thời gian khi áp dụng các cải tiến trong [5, 6, 7]. Ở đây, giá trị càng cao thì độ lợi về thời gian càng lớn càng hiệu quả. Ta thấy khi áp dụng các cải tiến thay thế ma trận Vandermonde bằng các ma trận cải tiến trong [5, 6, 7] thì hiệu quả về thời gian gần tương đương nhau, khi số nút lớn thì ma trận Hadamard cho kết quả tốt hơn.

Ta thấy, mô phỏng đã chỉ ra được thời gian tính toán và so sánh được độ lợi về thời gian khi áp dụng các cải tiến [5, 6, 7] so với mô hình Blom sử dụng ma trận Vandermonde. Kết quả mô phỏng khi áp dụng các cải tiến trong [5, 6, 7] đều cho kết quả thời gian tính toán tốt hơn so với khi áp dụng ma trận Vandermonde và kết quả này cũng phù hợp với ý nghĩa kết quả mô phỏng được công bố trong [5, 6, 7].

Như ta đã biết, trong mô hình Blom có sử dụng 2 ma trận đầu vào là ma trận công khai P và ma trận bí mật S. Ma trận bí mật S phải là ma trận đối xứng để đảm bảo ma trận khóa K là ma trận đối xứng. Ma trận P có điều kiện là các cột độc lập tuyến tính với nhau từng cột một. Và dựa vào kết quả mô phỏng đánh giá các cải tiến trong [5, 6, 7], luận văn có đề xuất cải tiến thêm bằng cách áp dụng cả ma trận ngẫu nhiên và ma trận Adjacency để thay thế ma trận Vandermonde. Tức là sử dụng loại ma trận Adjacency có hướng cho ma trận P (gọi là ma trận cải tiến), ma trận P sẽ là ma trận ngẫu nhiên gồm các số nhị phân, đảm bảo tính chất độc lập tuyến tính theo cột và không phải là ma trận đối xứng.

Việc sử dụng ma trận cải tiến là ma trận gồm các số nhị phân làm ma trận P thay thế ma trận Vandermonde nhằm các mục đích sau:

- Ma trận bao gồm các số nhị phân sẽ giảm dung lượng bộ nhớ cần lưu trữ, có thể chỉ lưu vị trí của các phần tử khác 0 mà không cần phải lưu cả ma trận.
- Sử dụng các số nhị phân trong ma trận giúp giảm thời gian tính toán khi tính khóa.

Ví dụ: Một mạng có số nút là 4, chọn hệ số an toàn t=3 và số nguyên tố q=31

Ta có ma trận cải tiến M = $\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$ và ma trận S = $\begin{bmatrix} 15 & 17 & 8 & 9 \\ 17 & 11 & 27 & 0 \\ 8 & 27 & 12 & 16 \\ 9 & 0 & 16 & 20 \end{bmatrix}$

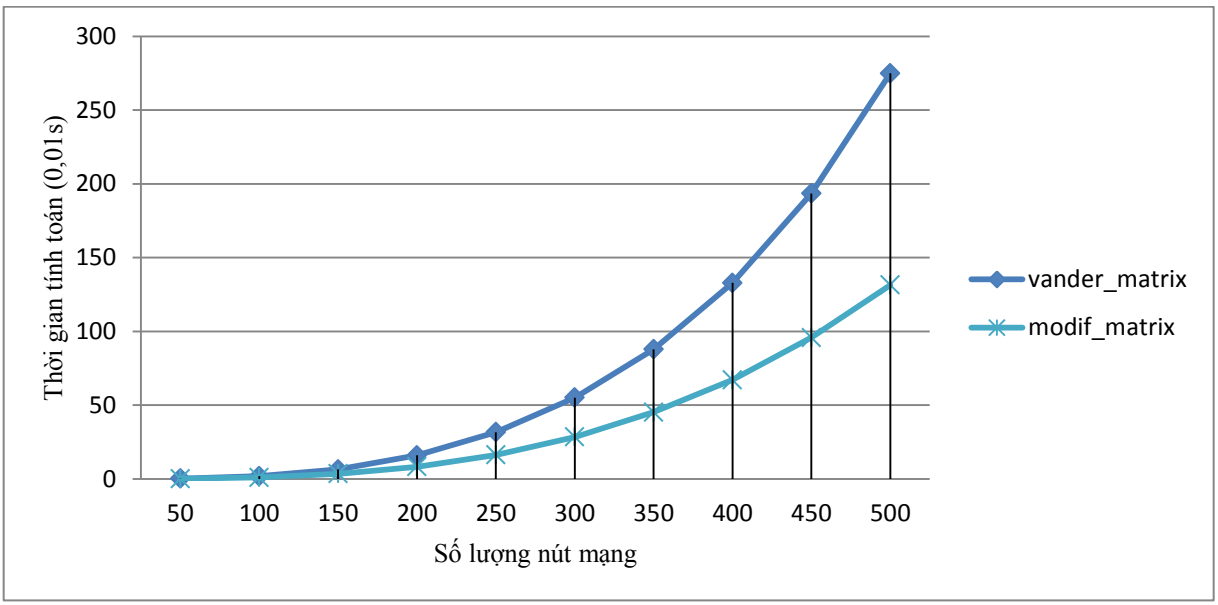
Ma trận P = M

Suy ra: A = $(S.P)^T$ mod q = $\begin{bmatrix} 15 & 17 & 8 & 9 \\ 1 & 13 & 5 & 14 \\ 18 & 24 & 1 & 14 \\ 23 & 13 & 20 & 25 \end{bmatrix}$

Suy ra: ma trận khóa K = A.P mod q = $\begin{bmatrix} 15 & 1 & 18 & 23 \\ 1 & 20 & 2 & 6 \\ 18 & 2 & 26 & 19 \\ 23 & 6 & 19 & 12 \end{bmatrix}$

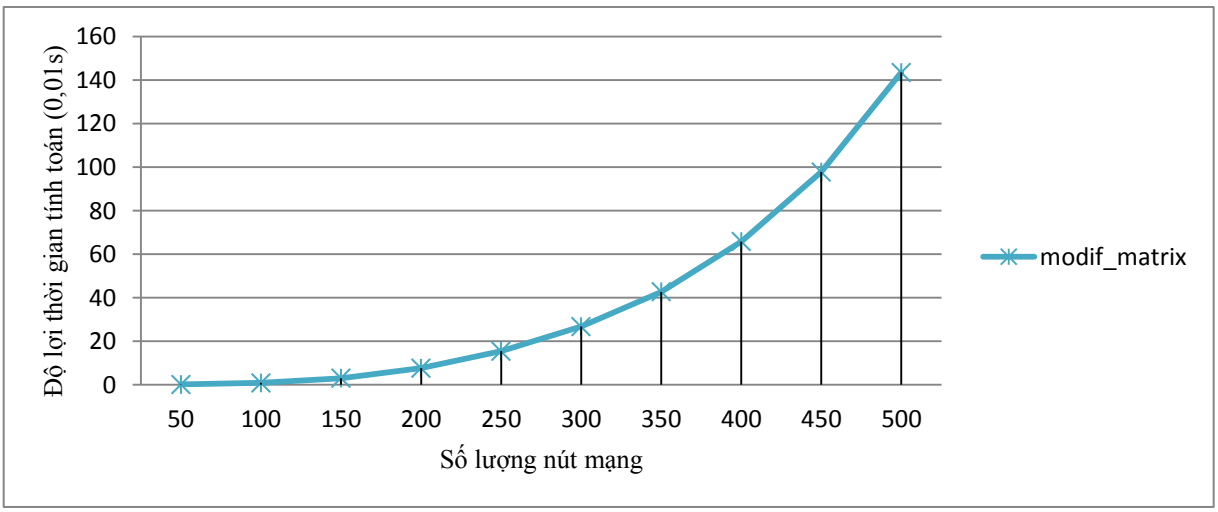
Để đánh giá hiệu quả khi thay thế ma trận ma trận cải tiến với Vandermonde, ta tiến hành mô phỏng so sánh thời gian tính toán khóa giữa mô hình Blom sử dụng ma trận Vandermonde và ma trận cải tiến.

Ta thực hiện mô phỏng với một mạng có số nút mạng thay đổi từ 0 đến 500 và có bước là 50 nút, hệ số an toàn $t = \frac{n}{2} + 1$, số nguyên tố q=1181. Thực hiện mô phỏng 100 lần và lấy kết quả thời gian tính toán trung bình. Kết quả thu được như hình dưới, với chiều dọc là thời gian tính toán (đơn vị 0,01s), chiều ngang là số nút của mạng. Kết quả mô phỏng như sau:



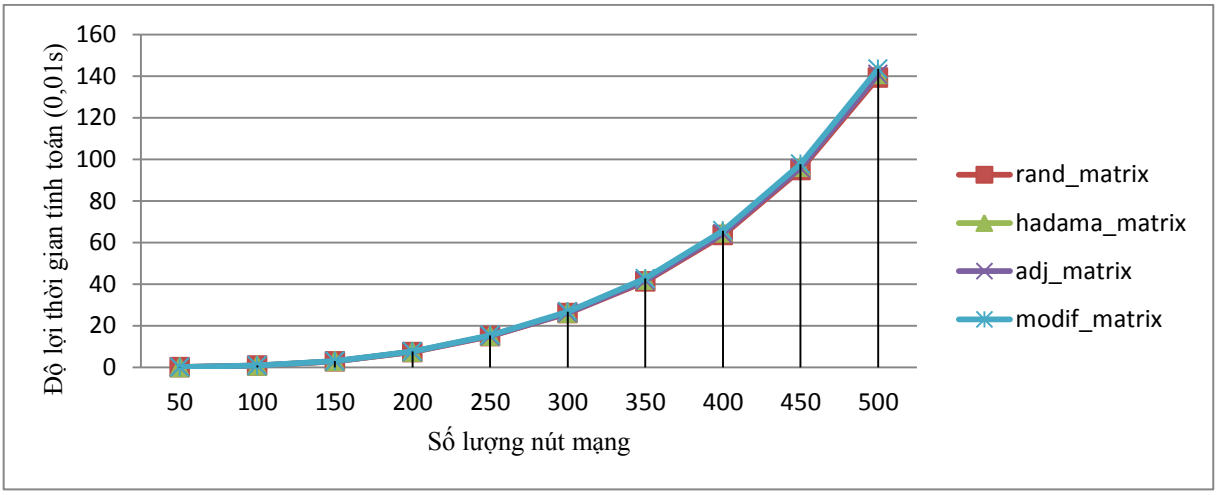
Hình 4.3: Thời gian tính toán giữa ma trận Vandermonde và ma trận cải tiến

Ta thấy, thời gian tính toán khi thay thế ma trận Vandermonde bằng ma trận cải tiến có thời gian tính toán thấp khi sử dụng ma trận Vandermonde. Khi số nút trong mạng càng tăng, thời gian chênh lệch càng tăng. Để thấy được hiệu quả về thời gian khi sử dụng ma trận cải tiến, ta tính độ lợi thời gian khi sử dụng ma trận cải tiến với ma trận Vandermonde như sau.



Hình 4.4: Độ lợi thời gian tính toán khi áp dụng ma trận cải tiến

Ta thực hiện so sánh độ lợi thời gian khi sử dụng ma trận cải tiến với các ma trận trong [5, 6, 7].



Hình 4.5: Độ lợi thời gian tính toán giữa ma trận cải tiến và các cải tiến [5, 6, 7]

Ta thấy độ lợi thời gian khi sử dụng ma trận cải tiến và các ma trận trong cải tiến [5, 6, 7] gần như xấp xỉ nhau. Và độ lợi thời gian so với khi sử dụng ma trận Vandermonde tăng nhanh khi độ lớn của mạng tăng.

4.3. TỔNG KẾT CHƯƠNG

Trong chương 4, luận văn đã tìm hiểu lấy ví dụ và mô phỏng đánh giá một số cải tiến để tối ưu cho mô hình Blom. Đồng thời luận văn cũng đưa ra đề xuất cải tiến mô hình Blom khi đưa ma trận ngẫu nhiên gồm các số nhị phân thay thế ma trận Vandermonde và có chương trình đánh giá mô hình cải tiến đề xuất với mô hình Blom sử dụng ma trận Vandermonde và các mô hình cải tiến trước đó.

Việc áp dụng ma trận cải tiến mà luận văn đề xuất cho mô hình Blom có thể làm giảm được dung lượng bộ nhớ cần để lưu trữ ma trận P. Đồng thời, khi các phần tử trong ma trận là các số nhị phân giúp giảm thời gian tính toán khi tính khóa. Kết quả mô phỏng cũng cho thấy, thời gian tính toán khi áp dụng ma trận đề xuất xấp xỉ so với khi áp dụng các cải tiến trong [5, 6, 7].

KẾT LUẬN

Luận văn với đề tài "Nghiên cứu mô hình đảm bảo an toàn truyền tin dựa trên chữ ký số và chứng chỉ số" có các kết quả chính như sau:

1/. Tìm hiểu nghiên cứu các vấn đề sau:

+ Tìm hiểu về mã hóa và mật mã học.
+ Tìm hiểu về các mô hình hệ mã hóa đối xứng, hệ mã hóa bất đối xứng và một số mô hình mã hóa hiện đại.
+ Tìm hiểu về mạng cảm biến không dây, các điểm yếu và yêu cầu khi triển khai mã hóa cho mạng cảm biến không dây.
+ Tìm hiểu về mô hình phân phối khóa Blom, đã đưa ra được các đánh giá và một số cách nâng cao hiệu năng và tốc độ tính toán khi áp dụng mô hình phân phối khóa Blom vào mạng cảm biến không dây.

2/. Thử nghiệm chương trình để đánh giá ưu điểm và mức độ cải tiến về tốc độ của các mô hình Blom cải tiến khi áp dụng vào mạng cảm biến không dây.

3/. Đề xuất sử dụng ma trận nhị phân để nâng cao tốc độ cũng như giảm được dung lượng bộ nhớ lưu trữ và có chương trình mô phỏng đánh giá với các cải tiến trước đó.

DANH MỤC CÁC TỪ VIẾT TẮT

- IoT – Internet of Things: Internet kết nối vạn vật.
- KDC – Key Distribution Center: Trung tâm phân phối khóa tập trung.
- DES – Data Encryption Standard: Thuật toán tiêu chuẩn mã hóa dữ liệu
- AES – Advanced Encryption Standard: Thuật toán tiêu chuẩn mã hóa tiên tiến
- ECB – Electronic Code Book: Thuật toán bảng tra mã điện tử, là một phương pháp mã hóa khối
- IDEA – International Data Encryption Algorithm: Là một phương pháp mã hóa khối
- P – Plaintext: Văn bản, thông tin ở dạng rõ
- E – Encrypt algorithm: Thuật toán mã hóa
- D – Decrypt algorithm: Thuật toán giải mã
- MITM – Man In The Middle: Tấn công người đứng giữa
- CA – Certificate Authority: Trung tâm cung cấp chứng chỉ số
- WSN – Wireless Sensor Networks: Mạng cảm biến không dây
- Sink: Bộ thu nhận

TÀI LIỆU THAM KHẢO

Tài liệu tiếng việt

[1] GS.TS Nguyễn Bình, "Giáo trình Cơ sở mật mã học", Khoa Kỹ thuật Điện tử 1, Học Viện Công Nghệ Bưu Chính Viễn Thông, 2013, 237 trang.

[2] Trần Minh Văn, "Bài giảng an toàn và bảo mật thông tin", Khoa Công nghệ thông tin, Đại hoc Nha trang, 2008, 184 trang.

[3] https://manthang.wordpress.com/2012/07/22/co-ban-ve-mat-ma-hoc-1/

[4] https://anninhmang.net/phan-tich-mang/

Tài liệu tiếng anh

[5] Suraj Sukumar, "Computational Analysis of Modified Blom's Scheme", 2013, 12 pages.

[6] Rohith Singi Reddy, "Key mangament in wireless sensor networks using a modified Blom scheme", Computer Science Department, Oklahoma State University, American, 2011, 9 pages.

[7] Divya Harika Nagabhyrava, "Efficient key generation for dynamic Blom's scheme", Bachelor of Technology in Computer Science, Jawaharlal Nehru Technological University, India, 2014, 17 pages.

[8] Anna Ha'c, "Wireless Sensor Network Designs", University of Hawaii at Manoa, Honolulu, USA, John Wiley & Sons Ltd, 2003

[9] Edgar H.Callaway Jr, "Wireless Sensor Networks: Architectures and Protocols", A CRC Press Company, 2004.

[10] John A. Stankovic, "Wireless Sensor Networks", Department of Computer Science, University of Virginia, 2006.