HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
-------***-------

NGUYỄN THỊ THUỲ TRANG

PHÂN TÍCH HIỆU NĂNG HỆ THỐNG PHÂN PHỐI KHÓA LƯỢNG TỬ DỰA TRÊN VỆ TINH SỬ DỤNG KỸ THUẬT CHUYỂN TIẾP

Chuyên ngành: Kỹ thuật viễn thông
Mã số: 8.52.02.08

TÓM TẮT LUẬN VĂN THẠC SỸ KỸ THUẬT

(Theo định hướng ứng dụng)

Hà Nội - 2021

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: PGS.TS Đặng Thế Ngọc

Phản biện 1: PGS.TS Nguyễn Nam Hoàng

Phản biện 2: TS. Nguyễn Ngọc Minh

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

Vào lúc: 9h30 ngày 09 tháng 01 năm 2021

Có thể tìm hiểu luận văn tại:

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

MỞ ĐẦU

Việc bảo mật thông tin ngày càng được quan tâm, đặc biệt là những thông tin được truyền qua cơ sở hạ tầng mạng Internet không được bảo mật. Phương pháp bảo mật phổ biến nhất là sử dụng khóa mật mã hóa bí mật dựa trên các thuật toán mật mã. Trong phương pháp này, bên gửi hợp pháp (Alice) và bên nhận hợp pháp (Bob) phải chia sẻ khóa bí mật qua kênh công khai không an toàn. Tuy nhiên, vấn đề nằm trong việc phân phối khóa nghĩa là làm sao hai bên gửi và nhận phải thông báo một cách bảo mật cho nhau về khóa bí mật được sử dụng để mã hóa thông tin. Để giải quyết được vấn đề này, rất nhiều giao thức phân phối khóa đã được đề xuất. Một trong những giao thức phân phối khóa nhận được nhiều sự quan tâm hiện nay là giao thức phân phối khóa lượng tử (QKD), trong đó hai bên gửi và nhận có thể trao đổi khóa bí mật qua kênh lượng tử, thậm chí cả khi có mặt của bên nghe trộm thứ ba (Eve).

Để phân phối khóa bí mật sử dụng giao thức DV/CV-QKD giữa Alice và Bob. Trong đó, phương pháp phân phối khóa lượng tử dựa trên sợi quang đã được nghiên cứu và rất nhiều ứng dụng đã được triển khai, nhưng đây chỉ là phương pháp sử dụng cho các đầu cuối cố định. Tuy nhiên, có rất nhiều ứng dụng thực tế, bao gồm cả trong đời sống hàng ngày hay trong quân đội, mà trong đó đầu cuối sử dụng là các thiết bị di động, ví dụ như các mạng xe cộ, đòi hỏi các giải pháp QKD vô tuyến. Trong bối cảnh đó, FSO, một hệ thống dễ thực thi và có chi phí hợp lý, có thể được sử dụng để truyền khóa lượng tử tới các trạm di động. Cũng như các hệ thống FSO khác, hệ thống QKD dựa trên FSO chịu rất nhiều ảnh hưởng của môi trường khí quyển như hấp thụ, tán xạ,... làm hạn chế khoảng cách truyền dẫn. Do vậy, sử dụng trạm chuyển tiếp là một giải pháp đã được đề xuất để mở rộng khoảng cách hoạt động của các hệ thống này. Nhận thấy tính thiết thực của đề tài, học viên xin chọn hướng nghiên cứu "Phân tích hiệu năng hệ thống phân phối khóa lượng tử dựa trên vệ tinh sử dụng kỹ thuật chuyển tiếp" làm đề tài cho luận văn tốt nghiệp thạc sỹ của mình. Mục tiêu chính mà luận văn hướng tới là phân tích hiệu năng qua các tham số hiệu năng của mô hình QKD/FSO dựa trên vệ tinh khi sử dụng kỹ thuật chuyển tiếp tại HAP. Tham

số hiệu năng mà luận văn hướng tới là tốc độ khoá bí mật. Bố cục luận văn gồm 3 chương chính:

Chương 1: Tổng quan về phân phối khoá lượng tử

Chương 2: Mô hình kênh quang không gian tự do

Chương 3: Phân tích hiệu năng hệ thống QKD dựa trên vệ tinh sử dụng kỹ thuật chuyển tiếp

Trong phần Kết luận, luận văn tóm tắt các kết quả nghiên cứu chính của luận văn cùng với những bàn luận xung quanh đóng góp mới cả về ưu điểm và hạn chế từ đó đưa ra những gợi mở cần tiếp tục nghiên cứu.

CHƯƠNG 1: TỔNG QUAN VỀ PHÂN PHỐI KHOÁ LƯỢNG TỬ

1.1 Vai trò của phân phối khoá lượng tử

Hiện nay có rất nhiều thuật toán mã hoá hiện đại như chuẩn mã hóa tiên tiến (AES) rất khó bị phá vỡ nếu như không có khóa, nhưng hệ thống này có một nhược điểm là khóa phải được biết cả hai phía. Như vậy mọi thuật toán mã hoá, bài toán truyền thông kín quy về bài toán làm sao phân phối những khóa này một cách an toàn – bản tin được mã hoá có thể được an toàn gửi đi theo một kênh công khai. Giải pháp cho bài toán này là sử dụng một đối tượng mang an toàn để vận chuyển khóa từ nơi gửi đến nơi nhận.

Mật mã lượng tử hay sự phân phối khóa lượng tử chính xác hơn, mang lại một phương pháp tự động phân phối các khóa bí mật bằng sợi quang truyền thông hoặc không gian tự do. Đặc trưng của phân phối khóa lượng tử là vốn dĩ an toàn: Giả sử rằng các định luật của thuyết lượng tử là đúng, thì chúng ta có thể chứng minh khóa đó không thể bị bên tấn công thu được mà không có sự phát hiện của người gửi và người nhận. Hơn nữa, phân phối khóa lượng tử cho phép khóa thay đổi thường xuyên, làm giảm nguy cơ mất trộm khóa hoặc "giải mã", trong đó bên nghe trộm phân tích các kiểu trong tin nhắn mã hóa để suy luận ra khóa bí mật.

1.2 Nguyên lý hoạt động giao thức phân phối khoá lượng tử

1.2.1 Các khái niệm vật lý cơ bản về cơ học lượng tử

a. Cơ sở vật lý hình thành mật mã lượng tử

Những nguyên lý cơ bản của vật lý lượng tử được sử dụng trong thông tin và mật mã lượng tử là:

Nguyên lý bất định của Heisenberg

Định lý không thể sao chép (no-clonning

Tính chất vướng víu lượng tử (entanglement

b. Quantum bit (Qubit)

Một qubit (Quantum bit) hay bit lượng tử là một đơn vị thông tin lượng tử. Trạng thái lượng tử được biểu diễn dưới dạng:

$$|\psi\rangle = \alpha|\psi_0\rangle + \beta|\psi_1\rangle \qquad (1.1)$$

c. Đo lường lượng tử

Đo lường lượng tử là hành động dùng các thiết bị trong lượng tử để quan sát trạng thái của các photon phân cực. Trong mật mã lượng tử, đo lường là một hành động không thể tách rời, dựa vào trạng thái phân cực của các photon để quyết định xem bit cổ điển tương ứng của trạng thái là 0 hay 1.

1.2.2 Nguyên lý hoạt động của giao thức phân phối khoá lượng tử

Mô hình phân phối khóa lượng tử giữa Alice (người gửi) và Bob (người nhận), tùy theo giao thức cụ thể được chia ra làm các bước cụ thể, nhưng nhìn chung gồm bốn giai đoạn:

+ Giai đoạn 1: Alice thực hiện mã hóa các bit cổ điển rồi chuyển các qubit này cho Bob. Bob thực hiện đo lường các qubit này.

+ Giai đoạn 2: Alice và Bob loại ra các bit mà Alice và Bob không sử dụng cùng cơ sở là các qubit được Alice tạo ra trong một cơ sở.

+ Giai đoạn 3: Alice và Bob đánh giá tỷ lệ lỗi. Nếu tỷ lệ lỗi lớn quá giới hạn lỗi họ sẽ hủy phiên truyền khóa và thực hiện lại phiên truyền khóa khác.

+ Giai đoạn 4: Alice và Bob sử dụng kỹ thuật "làm mịn khóa" để đồng nhất khóa giữa Alice và Bob, hai bên thu được khóa đã làm mịn khóa và "tăng tính bảo mật" làm giảm thông tin của Eve về khóa, họ thu được khóa cuối cùng.

1.2.3 Các giao thức phân phối khóa lượng tử

Dựa vào phương thức thông tin được mã hóa, QKD có thể được phân loại thành hai phương thức chính là biến rời rạc (discrete varable-DV) và biến liên tục (continous variable-CV).

a. Giao thức phân phối khoá BB84

Alice truyền một photon đơn lẻ ở trạng thái được chỉ định cho Bob, sử dụng kênh truyền lượng tử. Vì Bob không biết cơ sở mà các photon được mã hóa nên Bob chọn một cơ sở ngẫu nhiên để đo. Bob làm điều này cho mỗi photon nhận được, ghi lại thời gian, cơ sở đo lường được sử dụng và kết quả đo. Sau khi Bob đo tất cả các

photon, Bob liên lạc với Alice qua kênh cổ điển công khai. Alice và Bob trao đổi cơ sở dùng để phân cực và đo lường photon với nhau qua một kênh truyền thống đã được xác thực. Cả hai cùng loại bỏ các phép đo photon (bit) trong đó Bob sử dụng cơ sở khác của Alice, trung bình là một nửa, để lại một nửa số bit làm khóa chia sẻ.

b. Giao thức phân phối khoá B92

Alice gửi một chuỗi photon ở trạng thái phân cực H hoặc trạng thái phân cực +45° được chọn ngẫu nhiên. Bob lựa chọn ngẫu nhiên giữa cơ sở tuyến tính và đường chéo, để đo độ phân cực của photon nhận được. Để xác minh việc nghe trộm, Bob và Alice chia sẻ công khai một phần của chuỗi bit ngẫu nhiên được tạo và nếu lỗi vượt qua giới hạn có thể chấp nhận được, giao thức sẽ bị hủy bỏ. Nếu không, đã có thể tạo một khóa an toàn và đối xứng.

c. Giao thức phân phối khóa sử dụng SIM với kỹ thuật điều chế BPSK

Từ phía Alice, các bit nhị phân của khóa được chuyển sang hàm dạng xung chữ nhật (g(t)) và được điều chế lên sóng mang con RF sử dụng điều chế BPSK, trong đó bit “0” và “1” được biểu diễn bằng hai pha cách nhau 180 độ. Tại phía Bob sau khi giải mã, tín hiệu điện được qua bộ chỉnh xung (g(-t)), lấy mẫu và được quyết định là các bit “0”, “1”, hay “x” dựa trên bộ tách sóng hai ngưỡng (DT). Bob thông báo cho Alice về thời gian Bob tạo ra các bit từ những tín hiệu thu được thông qua kênh công cộng. Alice sẽ loại bỏ các bit tại thời điểm mà Bob tạo ra các giá trị không xác định. Các bit còn lại trong chuỗi bit sẽ tạo thành một chuỗi bit mới với tên gọi là khoá sàng lọc. Tương tự như giao thức BB84, tại bước này cũng sẽ thực hiện việc đối chiếu thông tin để hình thành nên một khóa bí mật không có lỗi.

1.3 Ứng dụng phân phối khoá lượng tử

Phân phối khóa lượng tử (QKD), là ứng dụng quan trọng nhất của mật mã lượng tử, hứa hẹn nguyên tắc bảo mật vô điều kiện dựa trên các định luật vật lý lượng tử.

1.4 Thách thức phân phối khoá lượng tử

1.4.1 Thiết bị

a. Nguồn quang

Nhiều nguồn quang có thể được coi là nguồn photon đơn nhưng thực tế dựa trên khái niệm xung laser mờ, tuy nhiên nguồn quang này không thể đảm bảo số lượng photon. Mặt khác, có những loại nguồn khác cũng được thử nghiệm, nhưng vẫn có sự khác biệt giữa lý thuyết và các thí nghiệm được sử dụng để tạo ra một photon.

b. Thiết bị đo photon

Do đặc điểm vật lý của vật liệu được sử dụng để sản xuất máy đo, có sự sai lệch giữa các thông số hiệu suất lý tưởng và thực tế.

c. Hệ thống vi xử lý

Hệ thống vi xử lý phụ thuộc vào sự phát triển điện tử liên quan đến hiệu suất cao liên quan đến xử lý tốc độ và thiết kế của bảng mạch in được sử dụng trong các hệ thống con khác nhau trong hệ thống vi xử lý. Do đó, bất kể thiết bị cao cấp nào được sử dụng trong hệ thống vi xử lý, nhà thiết kế cũng cần cố gắng tối ưu hóa mà không ảnh hưởng đến khả năng hoạt động của thiết bị.

1.4.2 Các giao thức QKD

Xu hướng của các giao thức đề cập đến việc đề xuất các giao thức QKD mới cho phép dễ dàng triển khai chúng trong các mạng thương mại quang, trong khi các thông số hiệu suất không đổi hoặc được cải thiện. Ngoài ra, một giao thức thứ nguyên cao được đề xuất để tăng dung lượng thông tin photon khi tốc độ photon bị hạn chế. Giao thức này dựa trên các cặp photon tương quan cho phép truyền thông tin bằng một chuỗi ký tự lớn.

1.4.3 Kỹ thuật và cấu trúc trong QKD

Xu hướng của hệ thống QKD-FSO liên quan đến cấu trúc và kỹ thuật là: tối đa hóa dung lượng kênh, tăng khoảng cách truyền dẫn và tăng tốc độ khóa bí mật, tăng hiệu quả tiêu thụ điện năng để hỗ trợ các nhiệm vụ trong thời gian dài hơn….

1.5 Kết luận

Nội dung Chương 1 đã trình bày tổng quan về các khái niệm cơ bản, vai trò, nguyên lý hoạt động, ứng dụng và thách thức của giao thức phân phối khoá lượng tử (QKD).

CHƯƠNG 2: MÔ HÌNH KÊNH QUANG KHÔNG GIAN TỰ DO

2.1 Mở đầu

FSO (Free Space Optics) là một công nghệ truyền thông quang không dây sử dụng laser hoặc điốt phát quang (Light Emitting Diode – LED) để truyền tín hiệu trong không gian tự do thay vì truyền qua sợi thủy tinh như trong mạng cáp quang.

2.1.1 Lịch sử phát triển công nghệ truyền thông quang không dây

Truyền thông tin quang trong môi trường tự do được đặt nền móng lần đầu tiên là bởi thí nghiệm Photophone thực hiện bởi Alexander Graham Bell vào năm 1880. Cột mốc quan trọng đánh dấu sự phát triển của công nghệ FSO đó là sự tìm ra các nguồn quang, mà quan trọng nhất là laser vào những năm 1960. Từ thời điểm này trở đi, sự phát triển của FSO đã được nâng lên một bước tiến mới.

2.1.2 So sánh hệ thống FSO với hệ thống RF

Hệ thống truyền thông FSO cung cấp nhiều ưu điểm hơn so với hệ thống truyền thông RF. Điểm khác biệt quan trọng giữa hai hệ thống đó là các bước sóng sử dụng. Tỷ lệ cao giữa các bước sóng dẫn đến những sự khác biệt của hệ thống truyền thông FSO so với hệ thống truyền thông RF như: băng thông điều chế lớn, độ phân kỳ của chùm sóng hẹp, công suất và khối lượng yêu cầu nhỏ hơn, hoạt động không cần cấp phép tần số.

2.1.3 Mô hình truyền thông quang không dây

Giống như bất kỳ công nghệ truyền thông khác, hệ thống truyền thông FSO gồm ba phần gồm bộ phát, kênh truyền và bộ thu:

Bộ phát: Chức năng chính của bộ phát là điều chế tín hiệu mang bản tin lên sóng mang quang để truyền qua không khí tới bộ thu.

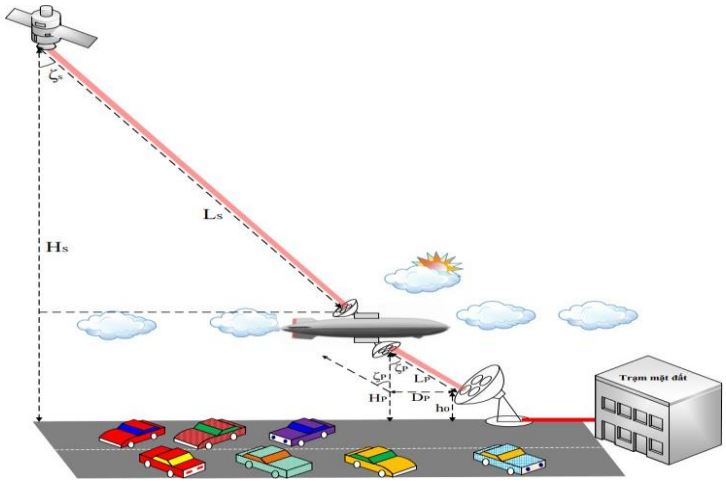
Kênh truyền: Không khí chính là môi trường truyền dẫn của hệ thống truyền thông FSO.

Bộ thu: Chức năng chính của bộ thu là khôi phục lại bản tin phát ban đầu từ tín hiệu quang đi đến.

2.2 Mô hình kênh quang từ vệ tinh tới mặt đất

2.2.1 Giới thiệu

Hình 2.1 dưới đây đưa ra mô hình hệ thống hệ thống truyền thông FSO chuyển tiếp quang dựa trên HAP kết nối vệ tinh LEO với trạm mặt đất – mô hình này sẽ được phân tích hiệu năng chi tiết trong chương 3.



Hình 2.1: Hệ thống truyền thông FSO chuyển tiếp quang dựa trên HAP kết nối vệ tinh LEO và trạm mặt đất

2.2.2 Hệ thống truyền thông FSO kết nối vệ tinh LEO với trạm mặt đất

Hệ thống bao gồm 3 phần: vệ tinh LEO đóng vai trò như bộ phát tại độ cao 610 km so với bề mặt Trái Đất; HAP đóng vai trò như một nút chuyển tiếp được trang bị một bộ thu phát; và bộ thu được đặt tại GS. Tín hiệu quang từ vệ tinh LEO sẽ được chuyển tiếp trong miền quang tại HAP trước khi tiếp tục gửi đến trạm mặt đất.

2.2.3 Mô hình kênh quang của kết nối từ vệ tinh LEO tới HAP

Tín hiệu từ vệ tinh LEO được truyền qua không gian tự do tới HAP. Suy hao không gian tự do (Free Space Loss – FSL) là tác nhân chính gây ra sự suy yếu tín hiệu thu được tại HAP và được biểu diễn như sau:

$$FSL = \frac{4\pi L_s}{\lambda} \qquad (2.1)$$

công suất thu được tại HAP được tính toán như sau:

$$P_r^{(P)} = \frac{P_t^{(S)} G_{TX}^S G_{RX}^P}{FSL} \qquad (2.2)$$

2.2.4 Mô hình kênh quang của kết nối từ HAP tới trạm mặt đất

Kênh không khí giữa HAP và GS bị ảnh hưởng bởi hai tác nhân chính gồm suy hao đường truyền và nhiễu loạn khí quyển. Cụ thể các ảnh hưởng của 2 tác nhân này sẽ được phân tích ở các mục 2.3, 2.4 dưới đây

2.3 Suy hao đường truyền

Hiệu năng của hệ thống truyền thông FSO bị ảnh hưởng bởi các tác động đa dạng từ môi trường như sương mù, tuyết, mưa và làm cho công suất của tín hiệu thu bị suy giảm.

Với một tuyến FSO trên mặt đất, cường độ tín hiệu thu được tại khoảng cách L từ bộ phát có quan hệ với cường độ tín hiệu phát theo quy luật Beer – Lambert như sau:

$$h_l^a = \frac{P_R}{P_T} = \exp\left[-\gamma(\lambda)L\right] \qquad (2.3)$$

Hấp thụ: xảy ra khi có sự tương tác giữa các photon và các phần tử trong không khí trong quá trình truyền lan. Các bước sóng sử dụng trong FSO về cơ bản được chọn để trùng với các cửa sổ truyền lan trong không khí, kết quả là hệ số suy hao bị chi phối chủ yếu bởi sự tán xạ do hơi nước, do đó có thể coi $\gamma(\lambda) \cong \beta_a(\lambda)$.

Tán xạ: là kết quả của việc phân bố lại góc của trường quang khi có và không có sự thay đổi bước sóng. Ảnh hưởng của tán xạ phụ thuộc vào bán kính r_m của các hạt (sương mù, hơi nước) gặp phải trong quá trình truyền lan. Một cách mô tả hiện tượng này là xét tham số kích cỡ $x_0 = 2\pi r_m/\lambda$. Nếu $x_0 << 1$ thì tán xạ là tán xạ Rayleigh, nếu $x_0 \approx 1$ là tán xạ Mie và nếu $x_0 >> 1$ thì tán xạ có thể thuộc loại khác (quang hình học).

2.4 Nhiễu loạn khí quyển

Sự không đồng nhất (gây ra nhiễu loạn không khí) là do các ô nhỏ rời rạc, hoặc các xoáy lốc với nhiệt độ khác nhau, hoạt động như những lăng kính khúc xạ có các

kích cỡ và chỉ số khúc xạ khác nhau. Sự tương tác giữa búp sóng quang và môi trường nhiễu loạn dẫn tới kết quả là pha và biên độ của trường quang mang thông tin thay đổi một cách ngẫu nhiên, làm cho hiệu năng của liên kết FSO bị suy giảm. Nhiễu loạn khí quyển được phân loại theo các mô hình phụ thuộc vào độ lớn của sự thay đổi chỉ số khúc xạ và sự không đồng nhất. Hai mô hình được sử dụng phổ biến nhất, đó là mô hình log- chuẩn và mô hình Gamma-Gamma.

2.4.1 Mô hình nhiễu loạn Log-chuẩn

Hàm phân bố log-chuẩn như trong công thức (2.4).

$$P(I) = \frac{1}{\sqrt{2\pi\sigma_l^2}} \frac{1}{I} \exp\left(\frac{(\ln(\frac{I}{I_0}) - E(l))^2}{2\sigma_l^2} \right) \tag{2.4}$$

2.4.2 Mô hình nhiễu loạn Gamma-gamma

Hàm phân bố cường độ trường theo phân bố Gamma-gamma như sau:

$$p(I) = \int_0^\infty p\left(\frac{I}{I_x}\right) p(I_x) dI_x = \frac{2(\alpha\beta)^{\frac{\alpha+\beta}{2}}}{\Gamma(\alpha)\Gamma(\beta)} I^{(\frac{\alpha+\beta}{2})-1} K_{\alpha-\beta}; I > 0 \tag{2.5}$$

2.5 Kết luận chương 2

Nội dung Chương 2 đã trình bày chi tiết về mô hình toán học của kênh truyền thông quang không dây FSO, trong đó mô hình hóa các ảnh hưởng của các tham số chính của kênh truyền lên cường độ tín hiệu quang tại phía thu.

CHƯƠNG 3: PHÂN TÍCH HIỆU NĂNG HỆ THỐNG QKD DỰA TRÊN VỆ TINH SỬ DỤNG KỸ THUẬT CHUYỂN TIẾP

3.1 Mô hình hệ thống QKD vệ tinh – mặt đất

3.1.1 Giao thức QKD dựa trên SIM/BPSK và DT/DD

Giao thức QKD được thực hiện trong hệ thống đề xuất được dựa trên SIM sử dụng khóa dịch pha nhị phân (SIM/BPSK), bộ thu DT/DD tương tự hoạt động của giao thức BB84 ban đầu, trong đó Alice tạo ra các tín hiệu được điều chế SIM/BPSK với độ sâu điều chế nhỏ $0<\delta<1$ theo các bit ngẫu nhiên nhị phân "0" và "1".

3.1.2 Mô hình hệ thống

Mô hình có ba phần chính: Vệ tinh LEO (tức là Alice), một HAP chuyển tiếp khuếch đại và chuyển tiếp tín hiệu và Bob (một chiếc xe) phát hiện tín hiệu nhận được từ HAP để khôi phục các khóa lượng tử được truyền từ Alice. HAP được trang bị hệ thống định hướng, thu nhận và theo dõi (PAT) để điều chỉnh HAP với các máy phát hoặc máy thu khác. Để đơn giản, mô hình đề xuất giả định rằng hệ thống PAT có sẵn tại HAP để Alice có thể phân phối khóa cho Bob một cách thuận lợi.

3.2 Kỹ thuật chuyển tiếp cho hệ thống QKD

3.2.1 Mô hình kênh của liên kết từ vệ tinh tới HAP

Ảnh hưởng của nhiễu loạn khí quyển có thể được bỏ qua và mô hình kênh giữa vệ tinh và HAP bao gồm hai loại tổn thất, suy hao không gian tự do và suy hao do lệch hướng búp sóng.

3.2.2 Mô hình kênh của liên kết HAP tới trạm mặt đất

Luận văn giả định rằng cả UAV và phương tiện mặt đất đều có chung một liên kết và được gọi là liên kết HAP-to-Ground. Sự suy hao đường truyền và nhiễu loạn của khí quyển là hai yếu tố chính ảnh hưởng đến liên kết. Trạng thái kênh khí quyển (h) có thể được biểu thị bằng 3 loại suy hao : trong đó h_l là suy hao đường đi, $h_p^{(G)}$ là suy hao lệch hướng búp sóng giữa HAP và phương tiện mặt đất, và h_a là nhiễu loạn khí quyển.

3.3 Phân tích hiệu năng hệ thống

Luận văn suy ra tốc độ khóa bí mật ergodic (S) của hệ thống được đề xuất trong trường hợp tấn công trái phép máy thu.

$$S = I(A;B) - I(A;E). \qquad (3.1)$$

Kịch bản 1: Trong trường hợp này, tín hiệu nhận được bởi HAP trái phép không bị ảnh hưởng bởi nhiễu loạn khí quyển.

Kịch bản 2: Trong trường hợp này, Eve nằm gần Bob.

3.4 Kết quả phân tích hiệu năng và bàn luận

Tốc độ khóa bí mật được khảo sát hai kịch bản tấn công như trong phân tích: (1) khi Eve tấn công búp sóng giữa Alice (vệ tinh) và HAP chuyển tiếp, (2) khi Eve tấn công vào búp sóng giữa HAP và Bob (UAV hoặc phương tiện).

Kết quả phân tích: tốc độ khóa bí mật tăng lên khi Eve ở xa HAP hoặc Bob. Điều này là do giảm công suất quang học do Eve thu thập được, do đó thông tin giữa Alice và Eve bị giảm. Ngoài ra, với việc Bob điều chỉnh hệ số thang đo DT Bob có thể nâng cao tính bảo mật với Alice. Cuối cùng, sử dụng các kết quả này, luận văn có thể xác định khoảng cách tối thiểu giữa Eve và HAP hoặc Bob mà có thể đảm bảo rằng hệ thống QKD được đề xuất được bảo mật (tức là S > 0). Ví dụ: khi Bob đặt hệ số tỷ lệ DT, Bob luôn có thể đảm bảo kênh an toàn với Alice bất cứ khi nào Eve cách HAP ít nhất 400m và cách Bob 40 m.

3.5 Kết luận

Mục đích chính của chương 3 là phân tích tốc độ khóa bí mật ergodic của hệ thống được đề xuất dưới tác động của các điều kiện khí quyển, bao gồm sự hấp thụ, tán xạ và nhiễu loạn khí quyển xuất hiện trong các kênh khí quyển trong 2 tình huống: bên nghe trộm gần nút chuyển tiếp và bên nghe trộm gần Bob hơn. Sử dụng các kết quả phân tích được, cuối cùng xác định được khoảng cách tối thiểu giữa Eve và HAP hoặc Bob để đảm bảo hệ thống QKD được bảo mật.

KẾT LUẬN

Nội dung luận văn đã đạt được mục tiêu đề ra là phân tích hiệu năng hệ thống phân phối khoá lượng tử dựa trên vệ tinh sử dụng kỹ thuật chuyển tiếp. Các kiến thức nền tảng và các kết quả nghiên cứu đã được trình bày trong luận văn với bố cục ba chương như sau: (1) Tổng quan về phân phối khoá lượng tử; (2) Mô hình kênh quang không gian tự do; (3) Phân tích hiệu năng hệ thống QKD dựa trên vệ tinh sử dụng kỹ thuật chuyển tiếp. Luận văn đã trình bày một cách tổng quan nhất về giao thức phân phối khoá lượng tử, các ưu điểm và thách thức đối với an toàn thông tin. Trình bày về mô hình truyền thông tin qua không gian tự do (FSO), các nguyên nhân chính làm suy giảm hiệu năng của hệ thống. Phân tích, đánh giá hiệu năng hệ thống phân phối khoá lượng tử dựa trên vệ tinh sử dụng kỹ thuật chuyển tiếp trong các tình huống giả lập khác nhau.

Luận văn cũng đã tìm hiểu, tham khảo và phân tích các kết quả tính toán tốc độ khoá bí mật trong hai trường hợp giả lập. Các kết quả đã cho thấy được những số liệu khả quan trong việc cải thiện hiệu năng hệ thống khi có các suy hao khác nhau như suy hao đường truyền, nhiễu nhiễu loạn khí quyển trong 2 điều kiện tấn công khác nhau: (1) bên nghe trộm ở gần nút chuyển tiếp; (2) bên nghe trộm ở gần Bob, cũng như xác định các phương pháp điều chế thích hợp cho hệ thống này là Phía phát sử dụng khóa dịch pha nhị phân điều chế cường độ sóng mang phụ (SIM) (BPSK) và sử dụng máy thu tách sóng trực tiếp/hai ngưỡng (DT/DD), HAP chuyển tiếp được trang bị nút chuyển tiếp khuếch đại quang và chuyển tiếp (OAF). Từ tốc độ khoá bí mật được phân tích, kết quả cuối cùng xác định được khoảng cách tối thiểu giữa Eve và HAP hoặc Bob để đảm bảo hệ thống QKD được bảo mật – mục tiêu bảo mật thông tin được hứa hẹn trong tương lai.