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

LUẬN VĂN THẠC SỸ KỸ THUẬT

(Theo định hướng ứng dụng)

Hà Nội - 2021

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

LUẬN VĂN THẠC SỸ KỸ THUẬT

(Theo định hướng ứng dụng)

NGƯỜI HƯỚNG DẪN KHOA HỌC

PGS.TS.ĐẶNG THẾ NGỌC

Hà Nội - 2021

LỜI CAM ĐOAN

Tôi cam đoan đây là công trình nghiên cứu của riêng tôi.

Các số liệu, kết quả nêu trong luận văn là trung thực và chưa từng được ai công bố trong bất kỳ công trình nào khác.

Người viết luận văn

Nguyễn Thị Thuỳ Trang

LỜI CẢM ƠN

Luận văn này đã khép lại quá trình học tập, nghiên cứu của học viên tại Học viện Công nghệ Bưu chính Viễn thông. Học viên xin bày tỏ sự biết ơn sâu sắc tới Thầy hướng dẫn, PGS.TS.Đặng Thế Ngọc đã định hướng nghiên cứu và tận tình giúp đỡ, trực tiếp chỉ bảo trong suốt quá trình thực hiện luận văn. Đồng thời học viên cũng xin bày tỏ lòng biết ơn Lãnh đạo Học viện, các thầy cô của Khoa Đào tạo sau đại học, Khoa Viễn thông 1 tại Học viện Công nghệ Bưu chính Viễn thông.

Trân trọng!

Hà Nội, tháng 11 năm 2020

Học viên

Nguyễn Thị Thùy Trang

MỤC LỤC

DANH MỤC HÌNH ẢNH

DANH MỤC BẢNG BIỂU

THUẬT NGỮ VIẾT TẮT

Thuật ngữ	Thuật ngữ Tiếng Anh	Thuật ngữ Tiếng Việt
AES	Advanced Encryption Standard	Tiêu chuẩn mã hoá nâng cao
APD	Avalanche Photodiode	Điốt thu quang thác
ASE	Amplified Spontaneous Emission	Bộ phát xạ khuếch đại
AWGN	Additive White Gaussian Noise	Nhiễu Gauss trắng cộng
BPSK	Binary Phase Shift Keying	Điều chế pha nhị phân
CV	Continuous Variable	Biến liên tục
DD	Direct Detection	Tách sóng trực tiếp
DoF	Degrees of Freedom	Mức độ tự do
DPS	Differential-Phase-Shift	Khóa dịch pha nhị phân
DT	Double Threshold	Hai ngưỡng
DV	Discrete Variable	Biến rời rạc
FPGA	Field Programmable Gate Arrays	Vi mạch dùng cấu trúc mảng phần tử logic có thể lập trình
FSL	Free-space Loss	Suy hao không gian tự do
FSO	Free Space Optical	Truyền quang không gian tự do
GG	Gamma-Gamma	Phân phối Gamma-Gamma
HAP	High Altitude Platform	Hạ tầng trên cao
IM	Intensity Modulation	Điều chế cường độ
LED	Light Emitting Diode	Điot phát sáng
LEO	Low Earth Orbit	Quỹ đạo trái đất tầm thấp
LOS	Light Of Sight	Đường truyền thẳng
MG	Mixture-Gamma	Phân phối hỗn hợp Gamma
NEP	Noise Equivalent Power	Công suất tạp âm tương đương
OOK	On-Off Keying	Điều chế khóa đóng-mở
PAT	Pointing Acquisition Tracking	Bộ định hướng, bắt và bám
QBER	Quantum Bit Error rate	Tỷ lệ lỗi bit lượng tử

QICT	Quantum Communication and Information Technologies	Thông tin lượng tử và công nghệ truyền thông
QKD	Quantum Key Distrubution	Phân phối khoá lượng tử
QND	Quantum Not Destruction	Không phá huỷ lượng tử
QST	Quantum Status Transmission	Trạng thái lượng tử
RF	Radio Frequency	Tần số vô tuyến
RSA	Rivest–Shamir–Adleman	Mã hoá RSA
SIM	Subcarrier Intensity Modulation	Điều chế cường độ sóng mang phụ
SW	Switch	Chuyển mạch
TRNG	True Random number generator	Bộ tạo số ngẫu nhiên thực
UAV	Unmanned aerial vehicle	Phương tiện không người lái
URA	Unauthorized receiver attack	Tấn công máy thu trái phép

LỜI 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 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 [1]. 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) [2],[3].

Phân phối khóa lượng tử (QKD) là một phương thức truyền thông an toàn thực hiện một giao thức mật mã liên quan đến các thành phần của cơ học lượng tử. QKD cho phép người gửi và người nhận tạo ra một khóa bí mật ngẫu nhiên được chia sẻ mà chỉ họ biết, sau đó có thể được sử dụng để mã hóa và giải mã các thông điệp. Các giao thức phân phối khoá này dựa trên việc mã hoá thông tin lên các biến rời rạc (DV) như pha hay sự phân cực của photon. Nhược điểm của các giao thức này là tốc độ và hiệu quả của việc tách sóng từng photon tại phía thu bị hạn chế. Khác với các hệ thống DV, trong luận văn, mô hình QKD mã hoá thông tin khoá trên các biến liên tục như biên độ hay pha của xung ánh sáng cũng như cường độ sóng mang quang được điều chế.

Để phân phối khóa bí mật sử dụng giao thức DV/CV-QKD giữa Alice và Bob, các môi trường truyền dẫn khác nhau gồm mạng truyền thông sợi quang, truyền thông quang qua không gian (FSO) dưới mặt đất [4],[5] và FSO dựa trên vệ tinh đã được nghiên cứu một cách rộng rãi [6],[7]. 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 [8]. 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 [9]. 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 hạ tầng trên cao (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

Tóm tắt: Phân phối khóa lượng tử (QKD), một tên gọi khác của mật mã lượng tử, là ứng dụng tiên tiến nhất của công nghệ truyền thông và thông tin lượng tử (QICT). Giao thức QKD đầu tiên được đề xuất vào năm 1984, và kể từ đó, nhiều giao thức hơn đã được đề xuất. QKD sử dụng cơ học lượng tử để cho phép trao đổi an toàn các khóa mật mã. Để có độ tin cậy cao về tính bảo mật của các giao thức QKD, các giao thức đó phải được chứng minh là an toàn trước mọi cuộc tấn công. Trong chương này của luận văn sẽ thảo luận và trình bày các chứng cứ bảo mật của các giao thức QKD. Phân tích khả năng bảo mật của các giao thức QKD dựa trên các khái niệm vật lý cơ bản về lượng tử ứng dụng trong các giao thức phân phối khóa lượng tử khác nhau. Chương 1 luận văn cung cấp ngắn gọn nền tảng của QKD và cũng xác định các khái niệm cơ bản về bảo mật trong các giao thức QKD.

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 từ 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 như mô tả hình 1.1.

Hình 1.1: Mô hình phân phối khoá

Giả sử, Alice muốn gửi cho Bob một tin nhắn bí mật, như một bản giao dịch ngân hàng, thông tin chính trị….trên một kênh truyền thông có thể không an toàn. Để làm việc này, Alice và Bob phải chia sẻ một khóa bí mật – đó là một số nhị phân dài. Sau đó Alice có thể mã hóa tin nhắn của mình thành "mật mã" bằng một khóa chung với thuật toán mã hóa, ví dụ như AES. Mật mã sau đó có thể được truyền đi bằng một kênh dữ liệu bình thường, khi đó bên tấn công sẽ không thể hiểu được và Bob có thể sử dụng khóa đó để giải mã tin nhắn. Trái với phương pháp truyền thống của sự phân phối khóa, mật mã lượng tử đảm bảo sự an toàn của khóa đó. Khóa cũng có thể thường xuyên thay đổi, do đó làm giảm nguy cơ bị đánh cắp hoặc bị suy ra bởi một phép phân tích thống kê giải mã của mật mã.

Bất cứ phương pháp phân phối nào dựa trên con người cũng làm tổn hại các khóa do tự ý hoặc bị ép buộc tiết lộ. Trái lại, 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 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 thông tin đánh cắp trong tin nhắn mã hóa để suy luận ra khóa bí mật.

Các vấn đề còn tồn tại trong việc tạo và trao đổi khóa trong mã hóa khóa đối xứng và mã hóa không đối xứng được giải quyết bằng khái niệm phân phối khóa lượng tử (QKD).

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

Phân phối khóa lượng tử sử dụng các tính chất của cơ học lượng tử, dùng để phân phối khóa hệ mật mã đối xứng. Trước khi đến với phần mô tả về nguyên lý hoạt động của QKD, luận văn sẽ giới thiệu các khái niệm và nguyên tắc cơ bản cùng với mô tả về cơ học lượng tử được sử dụng để thực hiện phân phối khóa lượng

tử, từ những khái niệm vật lý cơ bản về cơ học lượng tử để khái quát hoá lên nguyên lý hoạt động của 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 tính chất vật lý đặc biệt của cơ học lượng tử đã đặt nền móng lý thuyết cho một lĩnh vực mới - thông tin và tính toán lượng tử. Những tính chất đặc biệt đó của thông tin lượng tử cũng xây dựng nên một cơ chế mật mã mới – mật mã lượng tử.

Mật mã lượng tử (Quantum Cryptography – QC) với những đặc tính hoàn toàn khác với các cơ chế mật mã truyền thống, cho phép đảm bảo sự an toàn vô điều kiện cho các thông điệp gửi trên mạng. Mặc dù xây dựng các máy tính lượng tử là rất phức tạp và chưa khả thi trong một tương lai gần, nhưng việc gửi và nhận thông tin lượng tử đã được thực hiện thành công trên các hạt ánh sáng (photon). Thực chất vật lý lượng tử đã tham gia từ lâu vào sự phát triển của Tin học và Công nghệ thông tin vì tính chất của các Transistor khắc trên các vi mạch của các máy tính cá nhân ngày nay, phát minh từ năm 1947 bởi Bardeen, Brattain và Shockley, chỉ có thể lý giải bằng lý thuyết vật lý lượng tử. Tuy nhiên phải đợi đến đầu những năm 80 của thế kỷ XX, các nhà vật lý mới có khả năng tác động và quan sát các đối tượng lượng tử đơn lẻ như photon, nguyên tử, i-on,… Chính khả năng tác động và quan sát các hạt cơ bản này là nguồn gốc ra đời của ngành thông tin lượng tử, trong đó các đối tượng lượng tử nguyên tố sẽ cho phép xây dựng vật lý các bit lượng tử hay qubit. 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: Người ta không bao giờ có thể xác định chính xác cả vị trí lẫn vận tốc của một hạt vào cùng một lúc. Nếu ta biết một đại lượng càng chính xác thì ta biết đại lượng kia càng kém chính xác.

Định lý không thể sao chép (no-clonning): Dựa trên nguyên lý bất định, vì không thể biết chắc chắn trạng thái một hệ thống lượng tử, nên không thể sao chép hoàn hảo một hệ thống lượng tử bất kỳ.

Tính chất vướng víu lượng tử (entanglement): Một hệ thống lượng tử có thể tương liên với một hay nhiều hệ thống lượng tử khác. Mỗi phân hệ sinh ngẫu nhiên ra trạng thái của mình và không một phân hệ nào có trạng thái cố định.

Từ lâu, các nhà vật lý đã biết rằng ánh sáng vừa có bản chất hạt, vừa có bản chất sóng. Một photon có thể xem như một điện trường thu nhỏ dao động. Hướng dao động của điện trường được định nghĩa là sự phân cực của photon. Một đặc tính của photon phân cực là khi người ta cho chúng đi qua một bộ lọc phân cực thì các photon, hoặc là bị bộ lọc hấp thụ, hoặc được truyền đi nhưng với sự phân cực của bộ lọc. Sau khi ra khỏi bộ lọc bị mất hoàn toàn thông tin về góc phân cực trước đó của photon, hay nói một cách khác, không thể sao lại trạng thái phân cực của một photon để thực hiện nhiều phép đo sự phân cực của photon với các bộ lọc phân cực khác nhau.

Như vậy, khi cho một chùm photon đi qua một bộ lọc phân cực, các photon thu được sẽ có cùng mặt phẳng phân cực của bộ lọc. Đây chính là nguyên tắc lập mã cho photon. Bộ lọc phân cực cũng được dùng để xác định trạng thái phân cực của photon. Ví dụ nếu nguồn photon chỉ gồm những photon có các góc phân cực 0° và 90° thì dùng một bộ lọc 0°, người ta có thể xác định được chính xác những photon 0° (qua) và 90° (không qua). Thao tác này gọi là phép đo phân cực của photon. Một cặp bộ lọc phân cực trực giao để lập mã hoặc đo photon được gọi là một cơ sở (base). Người ta có thể sử dụng một cơ sở như vậy để biểu diễn các giá trị 0 và 1 bằng các photon.

Hai cơ sở trực giao được sử dụng để mã hóa/đo các bit 0 và 1 cho các photon là: thẳng (0°/90°) - ký hiệu ⊕ và chéo (45°/135°) - ký hiệu ⊗. Trong hệ cơ sở thẳng, các photon có góc phân cực 0° được tương ứng với bit 1, photon có phân cực 90° với bit 0. Tương tự trong hệ cơ sở chéo, các bit này sẽ tương ứng với các photon có góc phân cực lần lượt là 45° và 135°. Theo lý thuyết, dễ thấy rằng nếu các photon không cùng cơ sở với bộ đo, chúng ta sẽ thu được kết quả hoàn toàn ngẫu nhiên.

Bằng những kết quả nghiên cứu mới, các nhà Vật lý đã chứng minh được rằng: việc sử dụng các tính chất kỳ lạ của vật lý lượng tử lại dẫn đến ứng dụng cụ thể đầu tiên của Thông tin lượng tử là truyền khóa mật mã hoàn toàn đảm bảo không thể tấn công.

b. Quantum bit (Qubit)

Một qubit (Quantum bit) hay bit lượng tử là một đơn vị thông tin lượng tử. Trong đó một qubit miêu tả một hệ cơ học lượng tử có hai trạng thái cơ bản thường được ký hiệu $|\psi_0\rangle$ và $|\psi_1\rangle$ tương ứng với hai trạng thái phân cực thẳng dọc và phân cực thẳng ngang của photon. Sự khác biệt so với *bit* cổ điển là trạng thái $|\psi\rangle$ cũng có thể ở dạng chồng chất cơ lượng tử của $|\psi_0\rangle$ và $|\psi_1\rangle$:

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

Đối với trạng thái chuẩn hóa $|\psi\rangle$, các biên độ phức α và β bị giới hạn bởi điều kiện chuẩn hóa $|\alpha^2|+|\beta^2|=1$. Phương trình này phù hợp với hai vectơ cơ sở bất kỳ $|\psi_0\rangle$ và $|\psi_1\rangle$ của không gian Hilbert hai chiều của trạng thái $|\psi\rangle$.

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.

Một khái niệm cần quan tâm khi nghiên cứu cơ học lượng tử là cơ sở. Cơ sở được tạo thành từ cặp đôi trực chuẩn. Điều đó có nghĩa là nếu hai trạng thái |φ⟩ và $|\psi\rangle$ trong cùng cơ sở * (có thể là cơ sở thẳng hoặc cơ sở chéo) luôn có tích vô hướng của hai vector bằng 0. Một trạng thái photon bất kỳ được đo trong cơ sở *, thì kết quả đo lường chỉ có thể cho là |φ⟩ hoặc $|\psi\rangle$.

Xét bốn trạng thái cơ bản của lượng tử là ↑, →, ↗, ↘, ta có tích vô hướng của hai vectơ trạng thái ↑ và → bằng 0. Như vậy cặp ↑, → được gọi là cặp đôi trực

chuẩn, cặp đôi này tạo lên cơ sở thẳng ⊕. Tương tự từ ↗, ↘ cũng là cặp đôi trực chuẩn tạo lên cơ sở chéo ⊗.

Khi đo lường lượng tử, một photon phân cực được sinh ra trong cơ sở nào sẽ được đo lường đúng trong cơ sở đó. Photon sinh ra trong cơ sở thẳng ⊕ và trạng thái phân cực của photon là ↑ hoặc → thì sau khi ta đo lường photon ta cũng được trạng thái phân cực là ↑ hoặc →. Cũng như vậy, photon sinh ra trong cơ sở chéo ⊗ và trạng thái phân cực của photon là ↗ hoặc ↘ thì sau khi ta đo lường photon ta cũng được trạng thái phân cực là ↗ hoặc ↘.

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

Phân phối khóa lượng tử sử dụng các tính chất của cơ học lượng tử nêu trên, dùng để phân phối khóa hệ mật mã đối xứng. Trong phân phối khóa lượng tử, sử dụng hai kênh truyền là kênh truyền lượng tử và kênh truyền thông thường. Kênh truyền lượng tử là kênh truyền sử dụng kỹ thuật lượng tử để truyền đi các qubit thông qua cáp quang hoặc không gian. Kênh truyền thông thường là kênh truyền công khai sử dụng kỹ thuật TCP/IP… 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 vào các photon phân cực (qubit), rồi chuyển các qubit này cho Bob. Bob thực hiện đo lường các qubit này, để thiết lập khóa ban đầu.

+ 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, nhưng Bob đo lường trong cơ sở khác.

+ 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 khoá” để đồng nhất khoá giữa Alice và Bob, hai bên thu được khoá đã làm mịn và tăng tính bảo mật làm giảm thông tin của Eve về khoá, họ thu được khoá cuối cùng.

1.2.3 Các giao thức phân phối khóa lượng tử

Các giao thức phân phối khóa khác nhau sẽ khác nhau cách trao đổi khóa trong thực tế. Một điểm khác biệt cơ bản để phân loại nhiều loại giao thức QKD hiện có là 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). Để hiểu rõ hơn về CV và DV có một ví dụ như sau, nếu có một máy phát hiện photon đơn lẻ, sẽ có các thời điểm là phát hiện và không phát hiện, ứng với trường hợp có photon chạm vào và không chạm vào máy phát hiện. Xét trên phương diện toán học, kết quả của máy phát hiện là tập hợp của việc (chạm, không chạm), số lượng kết quả đo được là rời rạc, do vậy có thuật ngữ DV. Mặt khác, nếu một máy phát hiện homodyne có điện trường của ánh sáng tới. Các kết quả đo của phép đo là hình chiếu của pha và biên độ của điện trường ánh sáng liên tục lên các trục cầu phương. Phép chiếu này mang lại một giá trị liên tục như một kết quả đo lường, do đó có thuật ngữ CV.

a. Giao thức phân phối khóa BB84

Phương pháp đầu tiên phân phối khóa mật mã trong những trạng thái lượng tử được đề xuất vào năm 1984 bởi các nhà vật lý lý thuyết Charles Bennett tại IBM và Gilles Brassard tại trường đại học Montreal, được biết đến là giao thức BB84. Trong giao thức, người gửi (Alice) truyền một chuỗi đơn photon phân cực đến người nhận (Bob), bằng cách tiến hành phép đo lượng tử và truyền thông công khai, người gửi có thể thiết lập một khóa chia sẻ và kiểm tra xem bên nghe lén (Eve) có chặn được bit nào thuộc khóa này trên đường đi hay không.

Giao thức BB84 không những cho phép chúng ta kiểm tra việc nghe trộm, mà còn đảm bảo Alice và Bob có thể thiết lập một khóa bí mật, dẫu cho Eve đã xác định được một số bit trong chuỗi nhị phân chia sẻ của Alice và Bob. Giao thức BB84 được Bennett và Brassard đề xuất năm 1984, tên của giao thức được lấy theo 2 chữ cái đầu của tên hai tác giả và năm phát minh BB84 là giao thức phân phối khóa lượng tử đầu tiên được đề xuất.

Trong giao thức BB84, Alice mã hóa mã hóa các bit cổ điển vào các photon phân cực trong hai cơ sở chéo và cơ sở thẳng. Nghĩa là khi nào Alice muốn gửi cho Bob một qubit, Alice sẽ chọn một trong bốn trạng thái của qubit được quy ước trong bảng 1.1. Sau đó Alice gửi các trạng thái này cho Bob thông qua kênh truyền lượng tử.

Bảng 1.1: Các cơ sở thẳng và chéo

Basis	0	1
+	↑	→
×	↗	↘

Bước đầu tiên trong BB84 là truyền lượng tử. Alice tạo một bit ngẫu nhiên (0 hoặc 1) và sau đó chọn ngẫu nhiên một trong hai cơ sở của Alice (trong trường hợp này là thẳng hoặc chéo) để truyền. Sau đó Alice chuẩn bị trạng thái phân cực photon tùy thuộc vào giá trị bit và cơ sở, như được minh họa trong bảng trên. Ví dụ, bit 0 được mã hóa theo cơ sở thẳng ⊕ như một trạng thái phân cực đứng, và bit 1 được mã hóa theo cơ sở chéo ⊗ như một trạng thái phân cực chéo. Alice sau đó truyền một photon đơn lẻ ở trạng thái được chỉ định cho Bob, sử dụng kênh truyền lượng tử. Quá trình này sau đó được lặp lại từ giai đoạn bit ngẫu nhiên, Alice ghi lại trạng thái lượng tử, cơ sở và thời gian của mỗi photon được gửi đi.

Theo cơ học lượng tử (đặc biệt là tính không xác định lượng tử), không có phép đo nào có thể phân biệt được giữa bốn trạng thái phân cực khác nhau, vì chúng không phải tất cả đều trực giao. Phép đo duy nhất có thể là giữa hai trạng thái trực giao bất kỳ (cơ sở trực chuẩn). Ví dụ, đo trong cơ sở thẳng cho kết quả ngang hoặc đứng. Nếu photon được tạo ra là ngang hoặc thẳng đứng (như là một trạng thái riêng) thì giá trị này đo được trạng thái chính xác, nhưng nếu photon được tạo là 45° hoặc 135° (các đường chéo) thì phép đo tuyến tính thay vào đó trả về ngang hoặc thẳng một cách ngẫu nhiên. Hơn nữa, sau phép đo này, photon bị phân cực ở trạng thái mà nó được đo (ngang hoặc thẳng), tất cả thông tin về phân cực ban đầu của photon sẽ bị mất đi.

Vì Bob không biết cơ sở mà các photon được mã hóa nên tất cả những gì Bob có thể làm là chọn một cơ sở ngẫu nhiên để đo, theo cơ sở thẳng hoặc chéo. 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.

Bảng 1.2: 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

Chuỗi bit ngẫu nhiên Alice	0	1	1	0	1	0	0	1
Cơ sở ngẫu nhiên của Alice	+	+	×	+	×	×	×	+
Phân cực photon Alice gửi Bob	↑	→	↘	↑	↘	↗	↗	→
Cơ sở đo ngẫu nhiên của Eve	+	×	+	+	×	+	×	+
Phân cực photon Eve đo, gửi Bob	↑	↗	→	↑	↘	→	↗	→
Cơ sở đo ngẫn nhiên của Bob	+	×	×	×	+	×	+	+
Phép đo phân cực của Bob(Alice gửi)	↑	↗	↘	↗	→	↗	→	→
Phép đo phân cực Bob (Eve gửi)	↑	↗	↗	↘	→	↗	↑	→
Cơ sở lập luận suy ra khóa								
Khóa chia sẻ an toàn	0		1			0		1
Lỗi trong khóa	✓		✗			✓		✓

Để kiểm tra sự hiện diện của bên nghe trộm, Alice và Bob bây giờ so sánh một tập hợp con được xác định trước của các chuỗi bit còn lại của họ. Nếu một bên thứ ba đã thu được bất kỳ thông tin nào về sự phân cực của các photon, điều này dẫn đến sai số trong các phép đo của Bob. Các điều kiện môi trường khác có thể gây ra lỗi tương tự. Nếu nhiều hơn *p* các bit khác nhau, họ hủy khóa và thử lại, có thể bằng một kênh lượng tử khác, vì không thể đảm bảo tính bảo mật của khóa được chọn sao cho nếu số lượng bit mà Eve biết ít hơn số này, thì khả năng khuếch đại bí mật có thể được sử dụng để giảm sự hiểu biết của Eve về khóa xuống một mức thấp hơn tùy ý với việc giảm độ dài của khóa.

Các trạng thái phân cực thẳng H, V, P và M của các photon đơn được chọn để mã hóa các bit khóa, trong đó H và P mã hóa giá trị bit 0, V và M mã hóa giá trị bit 1. Alice cần một thiết bị có khả năng tạo ra các photon đơn lẻ với sự phân cực được chuẩn bị chính xác, trong khi Bob phải có khả năng phát hiện các *qubit* được gửi đi và phân biệt các trạng thái phân cực khác nhau. Việc lựa chọn cơ sở chuẩn, cũng như giá trị bit đã chuẩn, cần phải hoàn toàn ngẫu nhiên. Các photon được gửi đến Bob qua kênh lượng tử và được đo ngẫu nhiên ở một trong hai cơ sở. Sau bước giao tiếp lượng tử này, Alice và Bob mỗi người nắm giữ các khóa thô không giống nhau có độ dài N.

Bước tiếp theo là quá trình sàng lọc khóa, 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. Nếu sự lựa chọn các bit khóa ngẫu nhiên giữa hai cơ sở với xác suất bằng nhau, lựa chọn của họ sẽ trùng khớp trung bình 50%. Do đó, các bit có cơ sở chuẩn và cơ sở đo lường khác nhau sẽ bị loại bỏ, dẫn đến khóa được sàng lọc có độ dài $l_{sift} = N/2$. Gọi là tỷ lệ lỗi bit lượng tử (QBER) xác định tỷ lệ giữa bit sai và bit sàng lọc và được định nghĩa như sau:

$$QBER = \frac{N_{wrong}}{N_{sifted}} \tag{1.2}$$

Lỗi trong chuỗi bit được trao đổi có thể do sự không hoàn hảo trong quá trình chuẩn hóa, trong quá trình truyền và phát hiện tín hiệu hoặc do sự hiện diện của bên

nghe trộm. Trong phân tích bảo mật, tất cả các lỗi đều do bên tấn công Eve này gây ra và do đó, QBER là thước đo cho lượng thông tin trên khóa mà bên nghe trộm có thể lấy được tối đa. Trong bước sửa lỗi các khóa đã sàng lọc của Alice và Bob được so sánh với nhau và các bit sai sót sẽ bị loại bỏ. Hiệu quả của thuật toán sửa lỗi được định lượng bằng hệ số $f_{EC} \geq 1$, trong đó $f_{EC} = 1$ là giới hạn Shannon. QBER được tính toán theo cách này sau đó được sử dụng để xóa tất cả thông tin mà Eve có thể có trên khóa đã sàng lọc và sửa chữa khóa trong quá trình khuếch đại khả năng bảo. Sau khi Alice và Bob loại bỏ tất cả các bit sai trong các khóa được sàng lọc và xóa thông tin của một bên nghe lén, họ nhận được một khóa an toàn. Giới hạn về tốc độ khóa an toàn được đưa ra như sau:

$$P_{\text{sec,max}} = R_{sift} \times \max\left[1-(f_{EC}+1)H_2(E), 0\right], \tag{1.3}$$

Giới hạn trên của tốc độ khóa an toàn được đưa ra với R_{sift} là tốc độ khóa được sàng lọc, tức là số lượng bit được sàng lọc nhân với tần số lặp lại của nguồn và chia cho số bit đã gửi *N*, $H_2(E)$ là nhị phân Shannon entropy của $E \equiv QBER$ đưa ra ước tính về lượng thông tin quan trọng mà bên tấn công có thể lấy được.

$$H_2(E) = -E\log_2(E) - (1-E)\log_2(1-E). \tag{1.4}$$

Có thể thấy QBER tối đa có thể chấp nhận được bằng cách tính giá trị tại đó phương trình (1.2) giảm về 0, được giá trị $E_{\max} \approx 11\%$.

- **Khả năng tấn công của Eve trong BB84**

Bởi vì Eve không thể sao chép các qubit mà Alice gửi cho Bob, nên cách duy nhất để có thông tin về khóa mà Alice gửi cho Bob là chặn những qubit đó và đo lường chúng trong một cơ sở nào đó và gửi một trạng thái lượng tử khác cho Bob. Theo cách này, Eve muốn Bob nghĩ rằng Eve nhận được trạng thái lượng tử này trực tiếp từ Alice. Để tránh bị phát hiện sự có mặt của mình trong phiên trao đổi khóa, Eve phải gửi cho Bob những trạng thái, sao cho tỷ lệ lỗi mà Alice và Bob tìm được là nhỏ nhất. Trong phần này luận văn sẽ đưa ra một vài khả năng có thể xảy ra khi Eve cố gắng lấy thông tin về khóa.

  - Eve đo lường trong cơ sở $\oplus$ hoặc $\otimes$

Khả năng này, Eve chặn các trạng thái được gửi từ Alice rồi đo lường những trạng thái này trong cơ sở ⊕ hoặc ⊗. Phân tích dưới đây sẽ chỉ ra rằng, khả năng lớn nhất khi Alice và Bob có cùng giá trị của bit sau đo lường nếu họ sử dụng cùng cơ sở là ¾. Eve gửi cho Bob trạng thái của qubit sau đo lường của Eve: Giả sử rằng Eve gửi cho Bob trạng thái sau đo lường trên qubit $|\psi\rangle$. Có hai khả năng có thể xảy ra là:

- Khả năng Eve đo lường $|\psi\rangle$ đúng cơ sở là ½. Như vậy sau phép đo lường, Eve có được giá trị của bit trùng với Alice và trạng thái của qubit sau đo lường vẫn là $|\psi\rangle$. Eve gửi tiếp $|\psi\rangle$ cho Bob, Bob đo lường $|\psi\rangle$ trong cùng cơ sở và nhận được giá trị của bit trùng với Alice với xác suất là 1. Như vậy trong trường hợp này, xác suất mà Alice và Bob thu được cùng một giá trị của bit là 1.
- Khả năng Eve đo lường $|\psi\rangle$ không đúng cơ sở là ½. Như vậy sau phép đo lường, trạng thái của qubit sau phép đo lường $|\psi\rangle$ phân cực trong cơ sở mà Eve đo lường. Tiếp đó Eve gửi $|\psi\rangle$ ' cho Bob, vì Bob đo lường cùng cơ sở với Alice nên một lần nữa qubit bị đo lường sai cơ sở. Sau phép đo lường của Bob, giá trị của bit mà Bob nhận được trùng với Alice là $\frac{1}{2}$. Như vậy trong trường hợp này, xác suất mà Alice và Bob thu được cùng một giá trị của bit là $\frac{1}{2}$.

=> Xác suất trung bình mà Alice và Bob thu được cùng một giá trị của bit trong trường hợp này là $\frac{1}{2}(1+\frac{1}{2})=\frac{3}{4}$.

Ví dụ: Giả sử Alice gửi một trạng thái $|\psi\rangle$ là ⟶ cho Bob. Eve chặn trên đường truyền lượng tử và đo lường qubit này.

- Nếu đo lường trong cơ sở ⊕. Kết quả phép đo lường sẽ cho Eve giá trị của bit 0 với xác suất là 1 và trạng thái của qubit sau đo lường vẫn là ⟶ . Eve

gửi trạng thái → cho Bob. Bob cũng đo lường trong cơ sở ⊕. Anh ta sẽ nhận được giá trị của bit là 0 với xác suất là 1.

- Nếu đo lường trong cơ sở ⊗. Kết quả phép đo lường sẽ cho Eve giá trị của bit 0 hoặc 1 với xác suất là như nhau và trạng thái của qubit sau đo lường là ↗ hoặc ↘. Eve gửi trạng thái đó cho Bob. Bob cũng đo lường trong cơ sở ⊗. Anh ta sẽ nhận được giá trị của bit là 0 hoặc 1 với xác suất là như nhau.

Những vị trí có cùng cơ sở nhưng lại thu được những giá trị của bit khác nhau sẽ được tìm thấy qua quá trình đánh giá tỷ lệ lỗi (vị trí được đánh dấu). Từ đó Alice và Bob sẽ quyết định xem phiên truyền khóa có an toàn không.

b. Giao thức phân phối khóa B92

Năm 1992, Charles Bennett đề xuất giao thức B92 trong bài báo của mình "Mật mã lượng tử sử dụng hai trạng thái không trực giao bất kỳ". Giao thức B92 là một phiên bản sửa đổi của giao thức BB84 với sự khác biệt chính giữa hai giao thức là trong khi giao thức BB84 sử dụng bốn trạng thái phân cực khác nhau của photon, giao thức B92 sử dụng hai trạng thái (một từ cơ sở thẳng, trạng thái phân cực H thông thường và một từ cơ sở chéo, quy ước + 45 ° trạng thái phân cực). Giao thức phân phối khóa của B92 không có nhiều khác biệt so với BB84, khác biệt chỉ xảy ra ở giai đoạn “phân phối, đo lường và biến đổi bit” và giai đoạn “so sánh cơ sở, thiết lập chuỗi bit kiểm tra và chuỗi bit khóa”. Giao thức B92 có thể được tóm tắt trong các bước sau:

- Bước 1: Alice gửi một chuỗi photon ở trạng thái phân cực H hoặc trạng thái phân cực + 45 ° được chọn ngẫu nhiên. Trạng thái H sẽ tương ứng với bit ‘0’ trạng thái + 45 ° sẽ tương ứng với bit ‘1’.
- Bước 2: Bob lựa chọn ngẫu nhiên giữa cơ sở thẳng và chéo, để đo độ phân cực của photon nhận được.
- Bước 3: Nếu Bob đang đo theo cơ sở thẳng, có hai trường hợp có thể xảy ra: nếu photon tới là phân cực H, thì kết quả đo sẽ là trạng thái H với xác suất 1 trong khi nếu photon tới là + 45 °phân cực, thì kết quả đo sẽ là trạng thái H

hoặc trạng thái V với xác suất 0,5. Do đó, nếu chỉ có kết quả là trạng thái V, Bob có thể tự tin suy ra rằng trạng thái phân cực tới của photon là '+ 45 °'.

Lập luận tương tự sẽ được áp dụng nếu Bob đang đo trên cơ sở chéo, trong đó kết quả đo của trạng thái - 45 ° sẽ chỉ ra rằng trạng thái phân cực tới của photon là 'H'.

Sau khi truyền chuỗi photon, Bob thông báo các trường hợp trong đó kết quả đo là 'V' hoặc '- 45 °' và phần còn lại bị loại bỏ bởi cả hai.

Những kết quả này có thể được sử dụng để tạo một chuỗi bit ngẫu nhiên giữa Alice và Bob. 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, bây giờ họ đã có thể tạo một khóa an toàn và đối xứng giữa họ. Một điểm tương phản quan trọng khác với giao thức BB84 là Bob không phải thông báo lựa chọn cơ sở trong giao tiếp sau truyền tải, tức là không cần sàng lọc. Bảng 1.3 sau đây cho thấy các trường hợp khác nhau về kết quả truyền và đo lường có thể có:

Bảng 1.3: Các trường hợp về kết quả truyền và đo lường trong giao thức B92

Alice		**Bob**		**Bit khóa**
Trạng thái lượng tử truyền đi	Giá trị bit	Cơ sở Bob lựa chọn ngẫu nhiên	Trạng thái lượng tử suy ra	
H	0	⊗	H	…
H	0	⊕	+	…
H	0	⊕	-	1
+	1	⊗	H	…
+	1	⊗	V	1
+	1	⊕	+	…

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

Hai giao thức phân phối khoá được phân tích ở trên đều sử dụng phương thức mã hoá biến rời rạc (DV), trong các hệ thống DV-QKD, thông tin khóa sẽ được mã hóa thành các trạng thái rời rạc của mỗi photon, việc cài đặt DV-QKD yêu cầu sử

dụng kỹ thuật phức tạp và giá thành khá cao là một trong những thách thức và khó khăn cho việc áp dụng vào thực tế. Mặt khác, với việc cài đặt CV-QKD, thông tin khóa được mã hóa dựa vào biện độ hoặc pha của xung ánh sáng, nghĩa là biến liên tục của các trạng thái kết hợp. Rõ ràng, so với phương thức DV-QKD, CV-QKD là giải pháp phù hợp hơn để thực hiện phân phối khóa bí mật vì phương pháp này phù hợp với các công nghệ truyền thông quang và cho tỷ lệ khóa bí mật cao hơn. Phần này sẽ giới thiệu giao thức phân phối khoá QKD phương thức CV-QKD sử dụng điều chế cường độ sóng mang con (SIM) với kỹ thuật điều chế BPSK. Giao thức phân phối khoá QKD trường hợp này được tóm tắt trong bốn bước sau:

- Bước 1: 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.
- Bước 2: Tại phía thu (Bob), tín hiệu thu được giải điều chế bằng cách nhân với tín hiệu đến từ bộ dao động nội có tần số là tần số của sóng mang con vô tuyến. 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). Hai mức ngưỡng $d_0$và d_1, được thiết lập tại phía Bob cho việc tách sóng tín hiệu. Nếu dòng tín hiệu nhận được nhỏ hơn d_0, bit “0” sẽ được quyết định. Nếu dòng tín hiệu nhận được lớn hơn d_1, bit “1” sẽ được quyết định. Trường hợp còn lại, bit “X” (không bit nào) được tạo ra. Điều đáng lưu ý ở đây là bit X bị loại bỏ.
- Bước 3: 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.
- Bước 4: 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. Trong các giao thức QKD, bên nghe trộm, không thể giữ một bản sao lượng tử hoàn hảo của các tín hiệu lượng tử vì không thể tồn tại các máy sao chép lượng tử hoàn toàn. Ngoài ra, bên nghe trộm còn bị ngăn chặn khỏi việc nghe trộm hoàn toàn, do định lý không nhân bản lượng tử không một phép đo lượng tử nào có thể được thực hiện mà không làm xáo trộn hệ thống lượng tử, trừ khi phép đo tương thích với trạng thái lượng tử. Đối với đặc tính độc đáo này, QKD đang trở thành một yếu tố thiết yếu của Internet lượng tử an toàn trong tương lai. Các giao thức phân phối khoá lượng tử đang được nghiên cứu rộng rãi hướng tới ứng dụng trong vệ tinh. Các giao thức QKD có thể được ứng dụng triển khai trong cả các liên kết truyền thông có dây tức là cáp quang và không dây tức là các liên kết giao tiếp quang không gian tự do (FSO). FSO đề cập đến sự truyền dẫn chùm tia sáng qua khí quyển (LOS), vốn linh hoạt hơn và rẻ hơn để triển khai so với sợi quang. Hơn nữa, FSO cũng cung cấp tốc độ dữ liệu cao và cung cấp các kết nối chống nhiễu, đặc biệt hấp dẫn cho các kịch bản triển khai trong môi trường không dây không đồng nhất siêu dày đặc thế hệ thứ năm (5G). FSO cũng là một công nghệ đầy hứa hẹn cho truyền thông từ vệ tinh tới mặt đất, qua đó các giao thức QKD có thể được sử dụng để cung cấp một mạng truyền thông toàn cầu thực sự an toàn.

1.4 Thách thức phân phối khoá lượng tử

Ngày nay, mức độ bảo mật cao được yêu cầu để truyền thông tin quan trọng cho các khối chính phủ, tư nhân và cá nhân. Như một biện pháp nâng cao mức độ bảo mật, hệ thống phân phối khóa lượng tử là lựa chọn tốt nhất để bảo vệ các thông tin quan trọng này vì QKD cung cấp bảo mật vô điều kiện. Trong thực tế có một vài vấn đề được coi là thách thức với các giao thức lượng tử ở trên sẽ được trình bày chi tiết trong các mục bên dưới.

1.4.1 Thiết bị

Trên thực tế, những hạn chế và sự không hoàn hảo về mặt kỹ thuật trong phần cứng được sử dụng sẽ mang lại cho Eve cơ hội thực hiện một số các kiểu tấn công khác dựa trên những điều không lý tưởng.

a. Nguồn quang

Nguồn quang mong muốn nhất cho ngành kỹ thuật và khoa học là nguồn photon đơn hoặc nguồn quang theo yêu cầu phát ra photon tại bất kỳ thời điểm tùy ý nào liên quan đến tốc độ truyền theo cách xác định (không theo xác suất), nghĩa là, theo trường hợp lý tưởng, 100% cho phát ra một photon nhất định và 0% cho nhiều photon được phát ra, trong số các tính năng mong muốn khác. Do đó, 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 vì phân tích xác suất được thực hiện dựa trên sự phân bố Poisson của tín hiệu quang. 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.

Do đó, đối với tất cả các nguồn quang đã đề cập, hiệu suất và các phần tử quang phi tuyến tính là một vấn đề quan trọng đối với thiết kế và chế tạo. Điều quan trọng là các nguồn quang học được mô tả phải phù hợp với các liên kết FSO trong đó hệ thống QKD hoàn chỉnh được triển khai, nghĩa là, việc hạn chế photon đơn là rất quan trọng để hỗ trợ khía cạnh an toàn vốn có trong hệ thống QKD.

Các thách thức đối với các nguồn quang thực tế liên quan đến băng tần viễn thông của thiết bị, băng thông hiện có, hiệu suất phát xạ và chế độ không gian tự do. Do đó, bước tiến quan trọng đặt ra một xu hướng rõ ràng dựa trên các nguồn quang hiệu quả ở các bước sóng viễn thông phổ biến (băng tần C). Mặc dù các nguồn băng tần O là có sẵn. Về cơ bản, hiệu suất được cải thiện của các nguồn quang học dựa trên việc sử dụng các vật liệu, cấu trúc và thiết bị lượng tử mới cho phép tạo ra trạng thái lượng tử gần lý tưởng. Công nghệ hiện tại chưa đủ tin cậy để tạo ra các hạt photon đơn. Các bộ phát photon có thể phát quá nhiều hoặc ít photon trên một đơn vị thời gian so với mức cần thiết, do đó Eve sẽ có cơ hội tốt cho việc chia sẻ

xung quanh quan sát một phần của các photon trong khi để cho phần còn lại tiếp tục truyền đến Bob.

b. Thiết bị đo photon

Máy đo photon đơn lý tưởng rất hữu ích trong các hệ thống QKD để phát hiện và phân giải (xác định) lượng photon trên mỗi thời gian quan sát (liên quan đến bit), tức là máy đo được kích hoạt để phát hiện một photon và xác định chính xác trạng thái lượng tử của một photon đơn. Định nghĩa này dựa trên giả thuyết về nguồn đơn photon lý tưởng. Rõ ràng, nguồn photon đơn và máy đo photon đơn lý tưởng để đảm bảo các mức độ bảo mật cụ thể dựa trên việc phát hiện bên thứ ba Eve làm nhiễu lượng photon được Alice truyền đi. Tuy nhiên, 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. Do đó, nhiều máy đo photon đơn thực tế có khả năng phân biệt giữa 0 photon trên một bit và nhiều hơn 0 photon trên một bit , nhưng chúng không phân giải lượng photon. Dựa trên những điều trên, các máy dò đơn photon được sử dụng phổ biến nhất là máy dò không phân giải số photon, tức là chúng có khả năng phát hiện photon nhưng không phân giải chính xác số lượng photon.

Những thách thức chính liên quan đến việc giảm thiểu nhiễu điện tử và tối đa hóa độ lợi của máy dò duy trì tốc độ truyền cao. Để làm được những điều đã nói ở trên, cần phải có các vật liệu mới. Đặc biệt, việc giảm thông số Noise Equivalent Power (NEP) cho phép phát hiện các photon có công suất thấp với băng thông điện tử khác nhau. Tuy nhiên, các máy đo quang mới đã được phát triển, các kỹ thuật phát hiện tiên tiến hơn ở phía thu, giúp giảm bớt việc sử dụng máy đo do khả năng khuếch đại và lọc phổ của kỹ thuật kết hợp.

c. Hệ thống vi xử lý

Hệ thống vi xử lý được triển khai trong các hệ thống QKD thông thường thực hiện các tác vụ cơ bản như: điều khiển cho các thiết bị khác nhau (ví dụ: bộ điều biến pha và biên độ, bộ tạo số ngẫu nhiên thực (TRNG), v.v.), cơ sở dữ liệu khóa lượng tử, thực hiện thuật toán cần chắt lọc, quy trình sàng lọc và khuếch đại tín hiệu. Đặc biệt, thuật toán này yêu cầu quyền truy cập vào cả kênh lượng tử và kênh

cổ điển. Do đó, hệ thống vi xử lý yêu cầu một số thông số kỹ thuật quan trọng để không làm giảm mức độ an toàn và tiết kiệm tốc độ khóa của hệ thống QKD. Đặc biệt, FPGA đã được sử dụng trong hệ thống QKD thời gian thực đạt tốc độ khóa bí mật ở 17 kb/s trong liên kết cáp quang 20 km. Rõ ràng các thông số kỹ thuật của FPGA ảnh hưởng đến hiệu suất của hệ thống QKD, do đó, các phương pháp đồng bộ hóa và jitter được cải thiện dựa trên các thiết bị với độ chính xác và tốc độ cao có thể giảm tỷ lệ lỗi bit lượng tử (QBER) và tăng tốc độ khóa bí mật cuối cùng.

Hệ thống vi xử lý phụ thuộc vào sự phát triển điện tử liên quan đến hiệu suất, tốc độ xử lý và thiết kế của Bảng mạch in được sử dụng trong các hệ thống vi xử lý khác nhau trong hệ thống vi xử lý. Trong số các thiết bị cần được cải tiến là bộ chuyển đổi cao cấp (Digital-to-Analog-Converter và Analog-to-Digital-Converter), các cổng xuất/nhập nhanh và bộ nhớ truy xuất nhanh. Mặt khác, một giao thức QKD được tối ưu hóa phải được lập trình trong các hệ thống vi xử lý, bao gồm các thuật toán khác nhau cần thiết trong các giai đoạn giao thức khác nhau, tức là, phát hiện và sửa mã lỗi, thực hiện một số hàm băm trong số các chức năng khác được sử dụng. 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

Nghiên cứu về các giao thức được sử dụng để phân phối khóa mật mã dựa trên các nguyên tắc của cơ học lượng tử đã có một sự bùng nổ lớn trong 10 năm qua. Nói chung, các giao thức QKD mô tả các nhiệm vụ hoặc bước cụ thể (tức là thuật toán) cần thiết để tạo ra tốc độ khóa bí mật lượng tử cuối cùng. Mặc dù các giao thức QKD được lập trình trong hệ thống hệ thống vi xử lý. Đặc biệt, các giao thức và hiệu suất của chúng phụ thuộc vào thông tin thống kê (các biến rời rạc và liên tục, DV và CV, tương ứng) liên quan đến trạng thái lượng tử được sử dụng.

Những thách thức hiện tại trong các giao thức QKD có liên quan đến các thông số hiệu suất của hệ thống QKD. Mặc dù mỗi giao thức sử dụng nguyên tắc bảo mật và trạng thái lượng tử khác nhau, nhưng vấn đề quan trọng nhất là tăng mức độ bảo

mật, tốc độ khóa bí mật và khoảng cách truyền khóa giữa Alice và Bob trong môi trường có bên thứ ba Eve. Thực tế khi một giao thức cụ thể có mức bảo mật cao và tốc độ khóa bí mật cụ thể cho các liên kết khoảng cách ngắn, thì giao thức khác có cùng mức bảo mật và tốc độ khóa bí mật cho các liên kết khoảng cách dài. Tuy nhiên một giao thức QKD yêu cầu các hệ thống vi xử lý khác, do đó, một giao thức giả định phức tạp đòi hỏi một thiết kế chi tiết và chặt chẽ, nghĩa là việc thiết lập thử nghiệm rất phức tạp. Vì vậy 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.

Mỗi giao thức QKD được mô tả về mặt lý thuyết, tuy nhiên, không gian tự do và các kênh khí quyển đòi hỏi sự cân bằng quan trọng quyết định giao thức phù hợp. Đặc biệt, giao thức BB84 đã được tối ưu hóa cho các liên kết FSO bị ảnh hưởng bởi nhiễu loạn khí quyển, cải thiện tốc độ khóa bí mật lên đến hơn 20%. Tuy nhiên, giao thức BB84 vẫn không thay đổi trong khi các hệ thống vi xử lý khác được sửa đổi. Trên thực tế, nhiều giao thức QKD đã được triển khai trong các liên kết FSO để chứng minh hiệu suất của chúng trong các điều kiện cụ thể.

1.4.3 Kỹ thuật và cấu trúc trong QKD

Các kỹ thuật và cấu trúc được sử dụng trong ngữ cảnh QKD liên quan đến các thiết lập, quy tắc hoạt động và thiết bị khác nhau thực hiện một giao thức cụ thể. Do đó, bước đầu tiên là chọn giao thức lượng tử và tiếp theo đưa ra cấu trúc chung có thể được đề xuất và thực hiện. Đặc biệt, cấu trúc bao gồm nguồn quang, bộ dò quang, bộ vi xử lý (những thách thức và xu hướng đã được đề cập) giữa các thiết bị cụ thể khác được kết nối với nhau để thực hiện một hệ thống QKD hoàn chỉnh. Mặt khác, các kỹ thuật là các quy tắc hoạt động mới để nâng cao hiệu suất hoàn chỉnh của hệ thống QKD. Mỗi giao thức được đề cập đã được kiểm chứng, bằng cách sử

dụng một kỹ thuật và cấu trúc cụ thể, chúng có thể được tìm thấy và phân tích trong các tài liệu tham khảo và các phân tích ở trên.

Nói chung, các cấu trúc và kỹ thuật cho phép cải thiện hiệu suất của hệ thống QKD-FSO. Do đó, việc thiết kế các kỹ thuật và cấu trúc cao cấp cho phép hỗ trợ một cách tốt hơn các đề xuất hệ thống QKD thực tế. Trên thực tế, những thách thức chính liên quan đến việc tối ưu hóa và cải thiện các hệ thống vi xử lý của hệ thống QKD-FSO (tức là các hệ thống con thứ cấp không được đề cập chi tiết như thấu kính, cấu trúc cơ học, kỹ thuật ghép kênh truy cập, trong số những hệ thống khác). Cuối cùng, 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 chương 1

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 1 cũng đã đưa ra những ưu điểm vượt trội của QKD so với mã hoá cổ điển thông thường, phân tích khả năng bảo mật của các giao thức QKD dựa trên các khái niệm vật lý cơ bản về lượng tử ứng dụng trong các giao thức phân phối khóa lượng tử khác nhau. Để phân phối khóa bí mật sử dụng giao thức DV/CV QKD giữa Alice và Bob, các môi trường truyền dẫn khác nhau gồm mạng truyền thông sợi quang, truyền qua không gian tự do dưới mặt đất/vệ tinh. Trong phạm vi của luận văn này, mô hình sẽ sử dụng môi trường FSO vệ tinh để thực hiện phân phối khoá. Mô hình này sẽ được phân tích chi tiết ở chương 3 của luận văn.

CHƯƠNG 2: MÔ HÌNH KÊNH QUANG KHÔNG GIAN TỰ DO

Tóm tắt: Hệ thống truyền thông RF ngày càng không đáp ứng đủ nhu cầu của người sử dụng do phổ tần số bị quá tải và tốc độ dữ liệu thấp. Công nghệ truyền thông quang không dây FSO ra đời như là một giải pháp giải quyết những khó khăn mà hệ thống truyền thông RF gặp phải khi hoạt động không cần cấp phép tần số và cung cấp tốc độ dữ liệu lên tới hàng chục Gbps. Trong chương này, luận văn trình bày khái niệm, mô hình hệ thống truyền thông sử dụng công nghệ FSO điển hình, so sánh giữa công nghệ FSO và công nghệ RF để thấy được những ưu điểm nổi bật khi triển khai hệ thống truyền thông FSO, đồng thời đưa ra mô hình sử dụng công nghệ FSO cho hệ thống truyền thông vệ tinh và hạ tầng trên cao đã được nghiên cứu và triển khai trên thế giới để chứng minh tính khả thi và những ưu điểm mà công nghệ này đem lại trong thực tế. Luận văn còn phân tích các yếu tố ảnh hưởng đến chất lượng truyền dẫn FSO là suy hao đường truyền và nhiễu loạn khí quyển.

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. "Không gian tự do" có nghĩa là không khí, không gian bên ngoài, chân không. FSO là công nghệ truyền thông tin, dữ liệu giữa 2 điểm sử dụng bức xạ quang như là tín hiệu mang tin và được truyền qua các kênh truyền tự do. Dữ liệu cần truyền được điều chế vào cường độ, pha, hoặc tần số của bức xạ quang mang tin. Một đường truyền dẫn FSO về cơ bản là đường truyền tầm nhìn thẳng (Light Of Sight- LOS), vì vậy để đảm bảo trao đổi thông tin thành công, yêu cầu máy thu và máy phát phải có thể "nhìn" thấy nhau một cách trực tiếp mà không có bất kỳ một chướng ngại vật nào trên đường truyền. Kênh truyền tự do có thể là trong không gian vũ trụ giữa các vệ tinh, dưới nước, trong khí quyển hoặc là sự kết hợp của các loại môi trường trên trong cùng một tuyến thông tin. FSO có thể đạt tới tốc độ 10 Gbps cho việc truyền

tải dữ liệu, thoại và truyền thông video. Hình 2.1 minh hoạ cho mô hình truyền thông sử dụng FSO.

Hình 2.1: Hệ thống truyền thông quang không dây

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

Thông tin quang trong môi trường tự do (FSO) là một công nghệ đã có từ lâu đời sử dụng sự truyền lan ánh sáng trong không gian để truyền tín hiệu giữa hai điểm.

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. Trong thí nghiệm của mình, Bell đã điều chế bức xạ của mặt trời với tín hiệu âm thanh và truyền đi qua khoảng cách khoảng 200 m. Máy thu được làm từ một chiếc gương parabol với một tế bào Selen đặt tại tiêu điểm. Tuy nhiên, thí nghiệm cho kết quả không thực sự tốt do thiết bị sử dụng thô sơ và sự gián đoạn tự nhiên của bức xạ mặt trời.

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. Hàng loạt các nghiên cứu về FSO đã được thực hiện từ những năm đầu 60 đến những năm 70, ví dụ như: truyền phổ của tín hiệu truyền hình qua khoảng cách 48 km sử sụng diode phát quang GaA được thực thi bởi cách nhà khoa học của học viện MIT năm 1962;

tháng 5 năm 1963, tín hiệu âm thanh được điều chế với laser He-NE đã đươc truyền qua 190km giữa 2 ngọn núi Panamint Ridge và San Gabriel tại Mỹ; truyền dẫn Laser trong không gian được sử dụng với mục đích thương mại lần đầu tiên được xây dựng ở Nhật Bản bởi công ty điện tử Nippon vào năm 1970 - là đường truyễn dẫn song công, sử dụng Laser He-Ne bước sóng 0.6328 μm, truyền thông tin giữa Yokohama và Tamagawa với khoảng cách 14km.

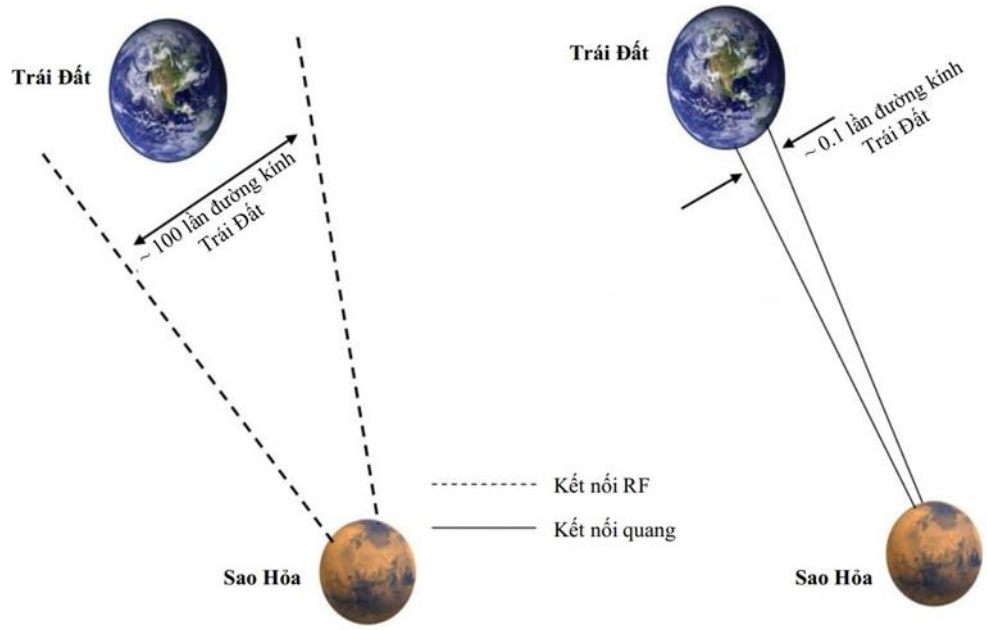
Từ thời điểm này trở đi, sự phát triển của FSO đã được nâng lên một bước tiến mới. Rất nhiều cuộc thí nghiệm đã được thực hiện trong các phòng nghiên cứu quân sự và không gian để có thể thực hiện kết nối FSO. Trong vòng vài thập kỷ vừa qua, công nghệ FSO đã được nghiên cứu và chứng minh một cách thành công là có thể được sử dụng trong truyền thông vũ trụ giữa các vệ tinh với tốc độ dữ liệu có thể lên tới 10 Gbps.

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. Dưới điều kiện thời tiết tốt, cửa sổ truyền dẫn trong không khí nằm trong vùng gần hồng ngoại (nằm từ 700 đến 1600 nm). Đối với hệ thống truyền thông RF, cửa số truyền dẫn nằm từ 30 mm đến 3 m. Do đó, bước sóng RF lớn hơn hàng nghìn lần so với bước sóng quang. 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 được đưa ra như sau [17]:

- **Băng thông điều chế lớn:** Khi tăng tần số sóng mang, dung lượng thông tin của hệ thống truyền thông sẽ được tăng lên. Trong hệ thống truyền thông RF, băng thông cho phép có thể lên tới 20% tần số sóng mang. Trong truyền thông quang, thậm chí khi băng thông chỉ chiếm 1% tần số sóng mang (≈1016 Hz), băng thông cho phép vẫn có thể lên tới 100 THz.
- **Độ phân kỳ của chùm sóng hẹp**: Độ phân kỳ của chùm sóng tỷ lệ với λ/D_R với λ là bước sóng của sóng mang và D_R là đường kính của khẩu độ. Do đó, độ trải rộng của chùm sóng quang sẽ hẹp hơn so với chùm sóng vô tuyến. Ví

dụ, độ phân kỳ chùm laser tại λ = 1550nm, D_R = 10 cm sẽ là 0,34 µrad. Mặt khác, tín hiệu tần số vô tuyến tại băng X sẽ có độ phân kỳ của chùm sóng là 67,2 µrad khi λ = 3 cm và D_R = 1 m. Hình 2.2 đưa ra sự so sánh về độ phân kỳ của chùm sóng cho tín hiệu quang và tín hiệu RF khi các tín hiệu được gửi từ Sao Hỏa về Trái Đất:



Hình 2.2: So sánh độ phân kỳ chùm sóng của tín hiệu RF và tín hiệu quang với tín hiệu gửi từ Sao Hỏa về Trái Đất

- **Công suất và khối lượng yêu cầu nhỏ hơn:** Với một mức công suất cho trước, cường độ quang tại phía thu sẽ nhiều hơn do độ phân kỳ của chùm sóng hẹp. Các thiết bị của hệ thống truyền thông FSO cũng nhỏ gọn hơn so với hệ thống truyền thông vô tuyến.
- **Hoạt động không cần cấp phép về tần số:** Trong hệ thống truyền thông RF, nhiễu từ các sóng mang lân cận luôn là một vấn đề đáng quan tâm do sự quá tải tại phổ tần số vô tuyến. Chính điều này khiến các cấp chính quyền phải quản lý phổ tần số vô tuyến bằng việc cấp phép tần số hoạt động cho các mục đích và ứng dụng khác nhau. Hệ thống truyền thông quang cho đến nay có thể hoạt động mà không cần cấp phép. Điều này giúp giảm thiểu chi phí thiết lập ban đầu và thời gian phát triển hệ thống.

- **An ninh:** Việc tách được chùm tín hiệu quang phát đi khó hơn nhiều so với tín hiệu RF do chùm tín hiệu quang có độ phân kỳ hẹp. Tuy nhiên, tín hiệu RF sẽ có vùng nghe trộm rộng hơn và có thể lên tới 64,37 km.

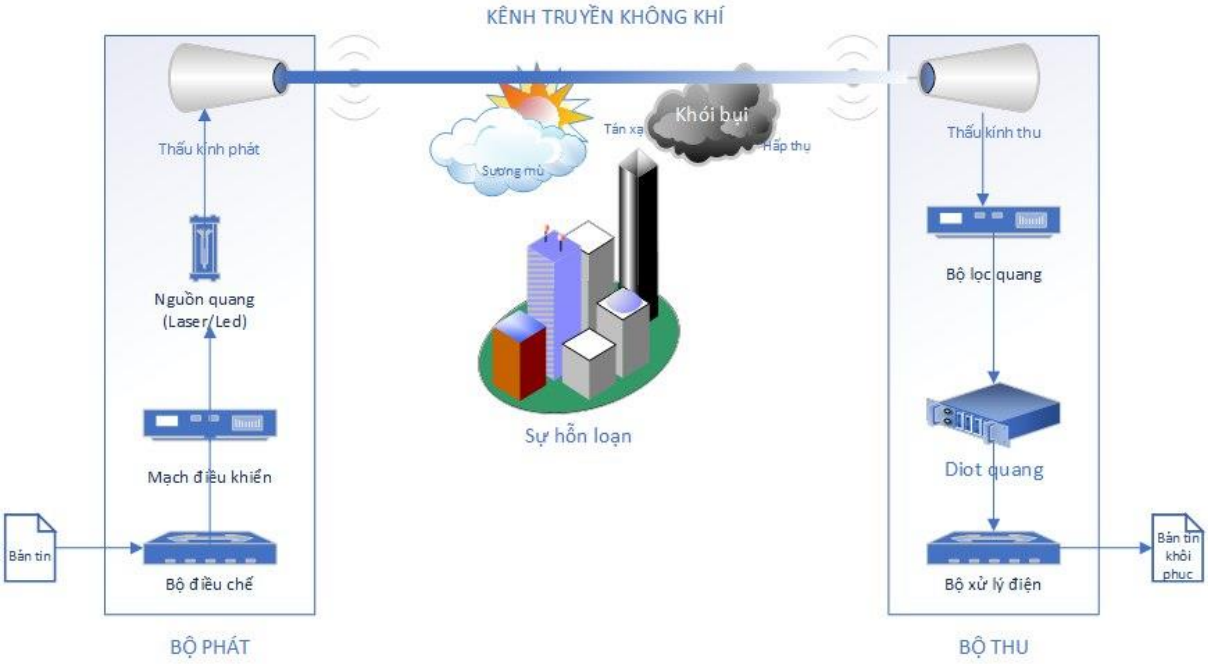
Ngoài những ưu điểm chính trên, hệ thống truyền thông FSO còn có những ưu điểm khác như linh hoạt và tiện lợi tại những địa điểm mà cáp quang không thể triển khai, dễ dàng mở rộng và tiết kiệm chi phí.

Bên cạnh những ưu điểm, hệ thống truyền thông FSO cũng tồn tại những nhược điểm. Hệ thống yêu cầu sự sắp đặt chặt chẽ giữa bộ phát và bộ thu do độ phân kỳ chùm sóng hẹp. Do ánh sáng không thể xuyên qua tường, đồi núi, tòa nhà cao tầng nên giữa bộ phát và bộ thu cần có một đường truyền tầm nhìn thẳng thoáng đãng và không có vật cản. Hiệu năng hệ thống truyền thông FSO cũng bị ảnh hưởng bởi điều kiện của không khí và sự phát xạ từ ánh sáng Mặt Trời.

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 như hình 2.3.

- **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. Các bộ phận thiết yếu trong bộ phát gồm: bộ điều chế, mạch điều khiển cho nguồn quang để ổn định sự phát quang và ống chuẩn trực hoặc thấu kính để tập hợp cũng như định hướng tín hiệu quang tới bộ thu. Phương thức điều chế thường được sử dụng là điều chế cường độ (Intensity Modulation – IM).
- **Kênh truyền**: Không khí chính là môi trường truyền dẫn của hệ thống truyền thông FSO. Do đó, kênh truyền sẽ bị ảnh hưởng bởi nhiều tác động môi trường không thể dự đoán trước như mây, tuyết, sương mù hoặc mưa. Các tác động đó không có đặc tính cố định và gây suy hao cũng như làm giảm chất lượng của tín hiệu thu. Kênh truyền chính là một trong những tác động hạn chế hiệu năng của hệ thống truyền thông FSO.



Hình 2.3: Mô hình hệ thống truyền thông FSO [17]

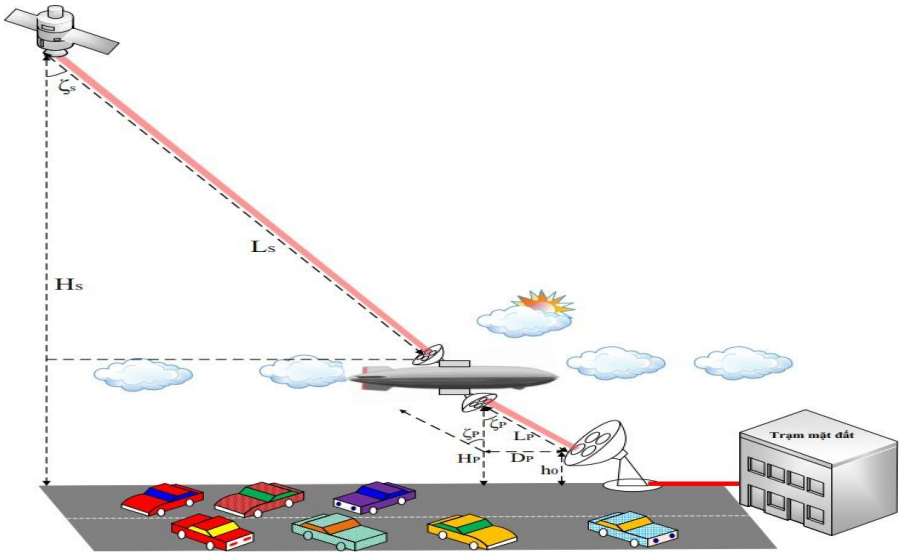
- **Bộ thu**: Chức năng chính của bộ thu là khôi phục lại bản tin phát ban đầu từ tín hiệu quang đi đến. Bộ thu bao gồm: thấu kính thu, bộ lọc quang, điốt thu quang và bộ giải điều chế. Thấu kính thu sẽ thu thập và tập trung tín hiệu quang thu được tới điốt thu quang. Bộ lọc quang loại bỏ ảnh hưởng của phát xạ nền và đưa tín hiệu tới điốt thu quang để chuyển đổi tín hiệu quang trở lại tín hiệu điện.

2.2 Mô hình kênh quang từ vệ tinh tới mặt đất

2.2.1 Giới thiệu

Hiện nay, hầu hết các hệ thống thông tin vệ tinh đều sử dụng tần số vô tuyến (RF) để thực hiện truyền thông. Tuy nhiên, tốc độ dữ liệu của các kết nối RF bị giới hạn trong khoảng vài trăm Mbps. Chính điều này đã thúc đẩy việc chuyển dịch từ sử dụng kết nối RF sang sử dụng kết nối truyền thông quang không dây qua không gian tự do (FSO). Các kết nối FSO có thể cung cấp tốc độ lên tới hàng chục Gbps và giải quyết tình trạng quá tải của trong phổ tần số RF. Trong những năm gần đây, sự triển khai các hệ thống truyền thông FSO trong kết nối giữa trạm mặt đất và vệ tinh, giữa vệ tinh với HAP và giữa HAP với trạm mặt đất đang thu hút nhiều sự

quan tâm của cả giới nghiên cứu và sự sử dụng thương mại nhờ vào các ưu điểm vượt trội của hệ thống truyền thông FSO như băng thông điều chế lớn, độ phân kỳ chùm sóng hẹp, công suất yêu cầu và khối lượng thiết bị nhỏ, tính định hướng cao, hoạt động không cần cấp phép về tần số và tính an ninh cao. Trong mục 2.2, luận văn sẽ mô tả sơ đồ khối của hệ thống truyền thông FSO chuyển tiếp quang dựa trên HAP kết nối vệ tinh LEO với trạm mặt đất trong Hình 2.4 - mô hình này sẽ được phân tích hiệu năng chi tiết trong chương 3.



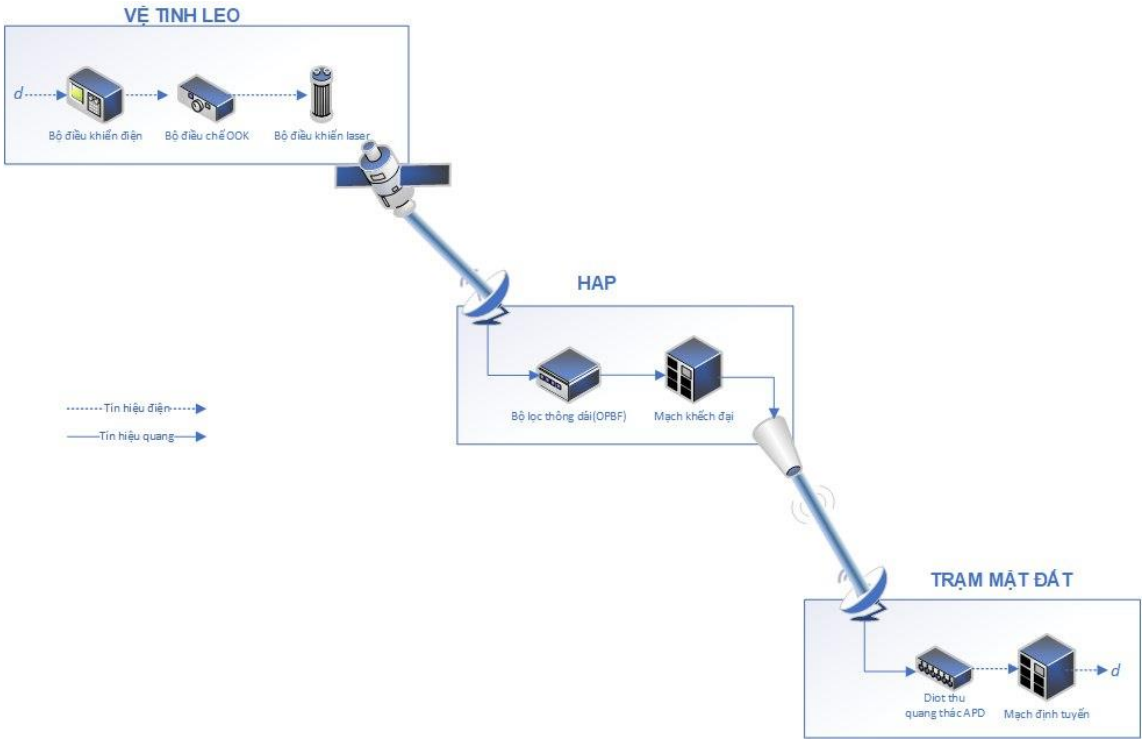
Hình 2.4: Hệ thống truyền thông FSO chuyển tiếp quang dựa trên HAP kết nối vệ tinh LEO và trạm mặt đất

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

Hệ thống bao gồm 3 phần được mô tả trong hình 2.5: 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.

- **Tại vệ tinh LEO:** dữ liệu nhị phân d (tín hiệu điện) được thực hiện điều chế khoá đóng – mở (On-off Keying – OOK) bằng việc gửi đi hoặc một xung quang hoặc không gửi gì cả trong một thời gian của một bit. Nếu d là bit “1”, nguồn phát quang laser điốt sẽ gửi đi một xung quang với công suất phát là P(S) tới HAP. Mặt khác, không ánh sáng nào được gửi đi nếu d là bit “0”.

Tín hiệu quang từ bộ phát sẽ được khuếch đại với độ lợi G_{TX}^{S} bằng việc sử dụng thấu kính bộ phát tại vệ tinh trước khi được gửi đến HAP thông qua kênh truyền FSO.



Hình 2.5: Sơ đồ khối hệ thống truyền thông FSO chuyển tiếp quang dựa trên HAP kết nối vệ tinh LEO với trạm mặt đất

- **Tại HAP:** tín hiệu quang thu được từ đầu ra của thấu kính bộ thu với độ lợi G_{RX}^{P} sẽ được chuyển qua một bộ lọc thông dải quang (OBPF) để giảm nhiễu nền. Tiếp theo, tín hiệu đã lọc được khuếch đại bằng bộ khuếch đại quang trong miền quang với hệ số khuếch đại G_A, sau đó tín hiệu được truyền qua thấu kính phát của HAP với độ lợi G_{TX}^{P} trước khi chuyển tiếp đến trạm mặt đất.
- **Tại trạm mặt đất (GS):** bộ thu sẽ sử dụng một điốt thu quang thác (Avalanche Photodiode – APD) để thực hiện chuyển đổi tín hiệu quang thu được thành dòng quang- điện. Sau đó, dòng quang điện này sẽ được so sánh với với mức ngưỡng của một mạch quyết định để khôi phục lại dữ liệu nhị phân ban đầu được gửi đi từ vệ tinh LEO. Bit "1" được quyết định tại đầu ra

mạch quyết định nếu cường độ dòng quang điện lớn hơn mức ngưỡng và nếu ngược lại thì bit "0" sẽ là bit nhận được tại đầu ra mạch quyết định.

Hệ thống truyền thông FSO kết nối vệ tinh LEO tới trạm mặt đất được chia thành hai chặng với chặng thứ nhất là từ vệ tinh LEO tới HAP và chặng tiếp theo là từ HAP tới trạm mặt đất. Mỗi chặng sẽ có mô hình kênh riêng biệt và được trình bày lần lượt như sau:

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. HAP được đặt ở độ cao 20 km so với bề mặt Trái Đất. Các vật thể khó có thể xuất hiện giữa vệ tinh LEO và HAP. Do đó, 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:

$$FSL = \frac{4\pi L_s}{\lambda} \tag{2.1}$$

với $L_s = (H_s - H_p)/cos(\xi_s)$ là khoảng cách truyền dẫn từ vệ tinh LEO đến HAP, trong đó: H_s và H_p lần lượt là độ cao của vệ tinh LEO, HAP; ξ_s là góc thiên đỉnh từ HAP tới vệ tinh, λ là bước sóng hoạt động của hệ thống.

Từ đó, công suất thu được tại HAP được tính toán như sau:

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

với G_{TX}^S là hệ số khuếch đại thấu kính bộ phát của vệ tinh LEO, G_{RX}^P là hệ số khuếch đại thấu kính bộ thu của HAP. Cường độ nhiễu loạn thường được xác định bởi chỉ số của thông số cấu trúc phản xạ C_n^2. Với độ cao lớn hơn 20 km, hằng số cấu trúc chỉ số phản xạ có thể giả sử bằng 0.

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. Khi tín hiệu quang đi qua bầu khí quyển, một số photon bị hấp thụ do một số thành phần như hơi nước, khí CO2, sương mù,…và năng lượng chuyển thành nhiệt năng. Trong khi đó, các photon khác đi qua bầu khí quyển không mất mát năng lượng nhưng hướng truyền lan ban đầu của chúng bị thay đổi do quá trình tán xạ. Suy hao khi truyền tín hiệu trong bầu khí quyển của hệ thống FSO là hệ quả của quá trình hấp thụ và tán xạ. Nồng độ của vật chất trong khí quyển gây ra việc suy hao tín hiệu khác nhau theo không gian và thời gian, và sẽ phụ thuộc vào điều kiện thời tiết của từng vùng. Để có thể dự đoán được dữ liệu suy hao quang từ dữ liệu tầm nhìn xa để ước tính sự khả thi của hệ thống truyền thông FSO, chúng ta cần biểu diễn được mối quan hệ giữa tầm nhìn xa và suy hao. Trong các nghiên cứu đã công bố, đã đưa ra một số mô hình mô tả mối quan hệ giữa tầm nhìn xa và suy hao quang. Để đặc tính hóa suy hao của tín hiệu quang qua môi trường truyền dẫn, " mức suy hao cụ thể" được sử dụng như một thuật ngữ với định nghĩa là mức suy hao trên một đơn vị độ dài với đơn vị dB/km.

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:

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

Trong đó $\gamma(\lambda)$ (tính theo đơn vị m^{-1}) là hệ số suy hao, h_l^a là suy hao tổng tại bước sóng λ. Hệ số suy hao là tổng của các hệ số hấp thụ và tán xạ từ hơi nước và các phân tử khí trong khí quyển, được tính như sau:

$$\gamma(\lambda) = \alpha_m(\lambda) + \alpha_a(\lambda) + \beta_m(\lambda) + \beta_a(\lambda) \tag{2.4}$$

Với $\alpha_m(\lambda)$: hệ số hấp thụ do hơi nước trong khí quyển

$\alpha_a(\lambda)$: hệ số hấp thụ do các phân tử khí trong khí quyển

$\beta_m(\lambda)$: hệ số tán xạ do hơi nước

$\beta_a(\lambda)$: hệ số tán xạ do các phần tử khí

Hấp thụ: xảy ra khi có sự tương tác giữa các photon và các phần tử trong không khí trong quá trình truyền lan. Một số photon bị hấp thụ và năng lượng của chúng biến thành nhiệt. Hệ số hấp thụ phụ thuộc rất nhiều vào các loại khí và mật độ của chúng. Sự hấp thụ phụ thuộc bước sóng và do đó có tính chọn lọc. Điều này dẫn tới bầu khí quyển có các vùng trong suốt – dải bước sóng có độ hấp thụ tối thiểu – được xem như là cửa sổ truyền. 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). Các loại tán xạ đối với các hạt khác nhau có mặt trong bầu khí quyển được tóm tắt trong Bảng 2.1.

Bảng 2.1: Bán kính và các loại tán xạ của các hạt điển hình tại λ = 850 nm [19]

Kiểu	**Bán kính (μm)**	x_0	**Loại tán xạ**
Phần tử khí	0,0001	0,00074	Rayleigh
Hạt bụi	0,01 – 1	0,074 – 7,4	Rayleigh – Mie
Hạt sương	1–20	7,4 – 147,8	Mie – hình học
Mưa	100 – 10000	740 – 74.000	Hình học
Tuyết	1000 – 5000	7400 – 37.000	Hình học
Mưa đá	5000 – 50000	37.000 – 370.000	Hình học

Kích thước hạt sương tương đối lớn so với dải bước sóng sử dụng trong FSO. Do đó, có thể coi sương mù là nguyên nhân chính gây tán xạ photon và nó góp phần vào sự suy giảm công suất quang. Tán xạ Mie sẽ được mô tả dựa trên các công thức thực nghiệm theo dải tầm nhìn V (tính theo đơn vị mét). Dải tầm nhìn là khoảng

cách mà một chùm sáng song song đi qua trong bầu khí quyển cho đến khi cường độ của nó giảm 2% so với giá trị ban đầu. Tầm nhìn được đo bằng một dụng cụ gọi là thiết bị đo truyền dẫn. Mô hình thực nghiệm phổ biến cho tán xạ Mie được cho bởi công thức (2.5) [18]:

$$\beta_a(\lambda) = \frac{3.91}{v}\left(\frac{\lambda}{550}\right)^{-\delta} \tag{2.5}$$

trong đó V là dải tầm nhìn (tính theo mét) và δ được biểu diễn như sau [18]:

Mô hình Kim

$$\delta = \begin{cases} 1.6 & V > 50 \\ 1.3 & 6 < V < 50 \\ 0.16V + 0.34 & 1 < V < 6 \\ V - 0.5 & 0.5 < V < 1 \\ 0 & v < 0.5 \end{cases}$$

Mô hình Kruse

$$\delta = \begin{cases} 1.6 & V > 50 \\ 1.3 & 6 < V < 50 \\ 0.586V^{1/3} & V < 6 \end{cases} \tag{2.6}$$

Bảng 2.2 dưới đây đưa ra giá trị của dải tầm nhìn dưới các điều kiện thời tiết khác nhau.

Bảng 2.2: Giá trị của dải tầm dưới các điều kiện thời tiết khác nhau

Điều kiện thời tiết	Dải tầm nhìn V(m)
Sương mù dày đặc	200
Sương mù trung bình	500
Sương mù nhẹ	770 – 1.000
Mưa lớn (25nm/h)	1.900 – 2.000
Mưa trung bình (12.5nm/h)	2.800 – 40.000
Khô ráo/Mưa bụi (0.25nm/h)	18.000 – 20.000
Rất khô ráo	23.000 – 50.000

Trong nghiên cứu của Al Naboulsi đã đưa ra công thức tính suy hao tầng bình lưu và suy hao bức xạ sương mù trong dải bước sóng 690 – 1550 nm và dải tầm nhìn trong dải 50 – 1000 m như sau:

$$\alpha_{drection}(\lambda) = \frac{0.11478\lambda + 3.8367}{V}$$
$$\alpha_{Radiation}(\lambda) = \frac{0.18126\lambda^2 + 0.13709\lambda + 3.7502}{V} \quad (2.7)$$

trong đó λ là bước sóng tính theo nm và tầm nhìn V tính theo mét. Tổn hao công suất do mưa và tuyết là thấp so với do tán xạ Mie.

2.4 Nhiễu loạn khí quyển

Bức xạ mặt trời bị hấp thụ bởi bề mặt Trái Đất làm cho không khí xung quanh bề mặt Trái Đất nóng hơn so với không khí tại những điểm cao hơn (so với mực nước biển). Lớp khí nóng này trở nên mỏng đi và bốc lên cao để hòa trộn một cách hỗn loạn với các vùng không khí lạnh hơn ở xung quanh, làm cho nhiệt độ không khí thay đổi một cách ngẫu nhiên. 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. Các mô hình này là một hàm của khoảng cách truyền dẫn của bức xạ quang qua môi trường khí quyển và được phân loại theo các mức độ yếu, trung bình và mạnh.Tuy nhiên, do sự phức tạp trong các mô hình toán học nhiễu loạn khí quyển, nên không có mô hình chung điển hình. Hai mô hình được sử dụng phổ biến nhất, đó là mô hình log- chuẩn và mô hình Gamma-Gamma.

Nhiễu loạn không khí dẫn tới sự biến đổi ngẫu nhiên của chỉ số khúc xạ khí quyển, n, dọc theo tuyến đường truyền dẫn của bức xạ quang qua môi trường khí quyển. Sự biến đổi chỉ số khúc xạ có nguyên nhân trực tiếp là sự biến đổi ngẫu nhiên của nhiệt độ khí quyển. Những sự thay đổi ngẫu nhiên về nhiệt độ là một hàm của áp suất khí quyển, độ cao so với mặt nước biển, và tốc độ gió. Mức độ nhỏ nhất và lớn nhất của các xoáy lốc trong khí quyển, tương ứng được gọi là kích thước cỡ

nhỏ (inner scale), l_0, và kích thước cỡ lớn (outer scale), L_0, của sự nhiễu loạn. l_0 thường nằm trong khoảng một vài milimet trong khi L_0 có thể lên tới vài mét.

Mối quan hệ giữa nhiệt độ không khí và chỉ số khúc xạ được xác định bởi công thức (2.8).

$$n = 1 + 77.6(1 + 7.52 \times 10^{-3} \lambda^2) \frac{P}{T_e} \times 10^{-6} \quad (2.8)$$

trong công thức này, n là chỉ số khúc xạ, T_e nhiệt độ (độ Kenvin), λ là bước sóng (nm), P là áp suất khí quyển (mbar).

Tốc độ thay đổi của chỉ số khúc xạ theo nhiệt độ được xác định bởi công thức (2.9).

$$-\frac{dn}{dT_e} = 7.8 \times 10^{-5} \frac{P}{T_e^2} \quad (2.9)$$

ở độ cao gần mực nước biển, $-\frac{dn}{dT_e} = 10^{-6} \times K^{-1}$

Trong khí quyển nhiễu loạn, một thông số quan trọng để đặc tính hóa lượng thay đổi của chỉ số khúc xạ là tham số cấu trúc chỉ số khúc xạ, C_n^2, được giới thiệu bởi Kolmogorov. Giá trị của C_n^2 thay đổi theo độ cao so với mặt nước biển, và có một mô hình thông dụng dùng để mô tả giá trị này, đó là mô hình Hufnagel- Valley (H-V) được cho theo công thức (2.10):

$$C_n^2(h') = 0.00549(\frac{v}{27})^2 (10^{-5} h')^{10} \exp(\frac{-h'}{1000}) + 2.7 \times 10^{-6} \exp(\frac{-h'}{1500}) + \hat{A} \exp(\frac{-h'}{100}) \quad (2.10)$$

Giá trị của C_n^2 thay đổi theo độ cao so với mặt nước biển, nhưng đối với môi trường quang lan truyền theo phương ngang thì chỉ số này được coi là khoảng hằng số, có giá trị từ 10^{-12} ($m^{-2/3}$)trong trường hợp kênh truyền có nhiễu loạn mạnh cho đến 10^{-17} ($m^{-2/3}$) trong trường hợp kênh truyền có nhiễu loạn yếu. Giá trị trung bình của tham số này khoảng 10^{-15} ($m^{-2/3}$).

2.4.1 Mô hình nhiễu loạn Log-chuẩn

σ_x^2 đặc trưng cho mức độ biến động biên độ trường trong khí quyển nhiễu loạn, được xác định thông qua tham số cấu trúc chỉ số khúc xạ, và cự ly truyền dẫn L theo các công thức (2.11):

$\sigma_x^2 = 0.56k_s^{7/6}\int_0^L C_n^2(x)(L-x)^{5/6}dx$ đối với sóng phẳng (2.11)

$\sigma_x^2 = 0.563k_s^{7/6}\int_0^L C_n^2(x)(x/L)^{5/6}(L-x)dx$ đối với sóng cầu.

Đối với trường phân cực ngang truyền qua môi trường nhiễu loạn, tham số cấu trúc chỉ số khúc xạ C_n^2 là hằng số, và phương sai log-cường độ trường (với giả thiết truyền lan sóng cầu) được xác định theo công thức (2.12):

$$\sigma_l^2 = 1.23C_n^2 k_s^{\frac{7}{6}} L^{\frac{11}{6}} \quad (2.12)$$

trong công thức (2.4), k_s là số bước sóng, nó nằm trong khoảng $2\frac{\pi}{L_0} \le k_s \le 2\pi/l_0$, L là cự ly truyền dẫn (m). Cường độ trường trong môi trường nhiễu loạn được xác định theo công thức (2.13):

$$I = \left|A(r)^2\right| \quad (2.13)$$

với A(r) là biên độ của trường trong môi trường nhiễu loạn.

Cường độ trường trong môi trường không nhiễu loạn được xác định như theo công thức (2.14):

$$I_0^2 = \left|A_0^2(r)\right| \quad (2.14)$$

với $A_0(r)$ là biên độ của trường không có nhiễu loạn.

Cường độ theo hàm log được cho bởi công thức (2.15):

$$I = \log_e\left|\frac{I}{I_0}\right| = 2X \quad (2.15)$$

trong công thức (2.15), X là sự biến đổi log-biên độ, I, I_0 lần lượt được xác định như trong công thức (2.13) và (2.14).

Từ công thức (2.15) ta có thể biến đổi để được công thức tinh I theo công thức (2.16):

$$I = I_0 \exp(I) \quad (2.16)$$

Để tìm được hàm mật độ xác suất bức xạ, thực hiện biến đổi $P(I) = P(X)\left|\frac{dX}{dl}\right|$

Ta được hàm phân bố log-chuẩn như trong công thức (2.17):

$$P(I) = \frac{1}{\sqrt{2\pi\sigma_l^2}} \frac{1}{I} \exp\left(\frac{(\ln(\frac{I}{I_0}) - E(l))^2}{2\sigma_l^2} \right) \quad (2.17)$$

trong công thức (2.16), trị trung bình log-cường độ E(l) = 2E(X), với E(X) là kì vọng của X.

Phương sai cường độ được tính bằng công thức (2.18):

$$\sigma_I^2 = I_0^2(\exp(\sigma_I^2) - 1) \quad (2.18)$$

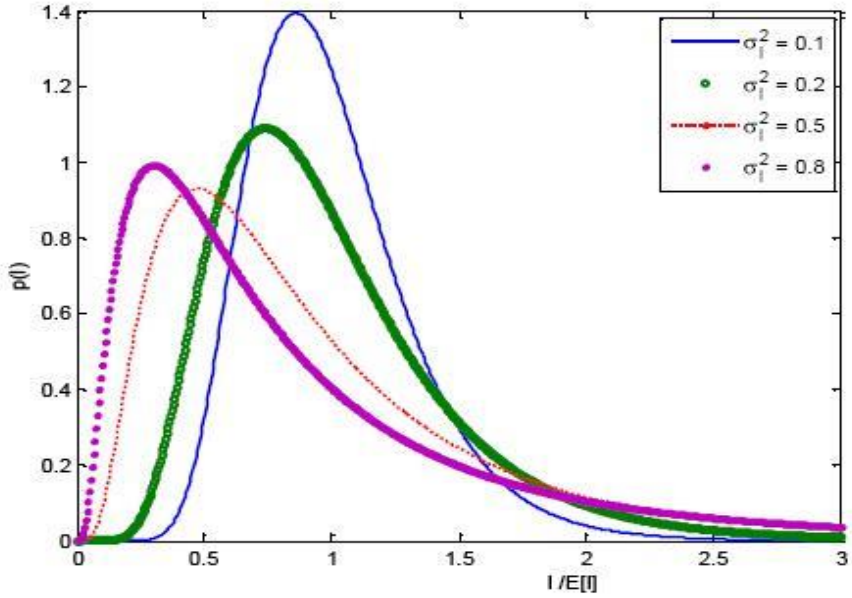
Như vậy ta có công thức phương sai chuẩn hóa cường độ hay còn gọi là chỉ số nhấp nháy S.I được xác định như công thức (2.19):

$$S.I = \sigma_N^2 = \frac{\sigma_I^2}{I_0^2} = \exp(\sigma_I^2) - 1 \quad (2.19)$$

Hàm mật độ xác suất log-chuẩn được thể hiện như trong Hình 2.6. Trong hình này, có thể thấy rằng, khi phương sai log-cường độ càng tăng thì phân bố càng trở nên sai lệch, không đều.

Giả thuyết Rytov(phương sai log-cường độ) được sử dụng để mô tả sự nhiễu loạn khí quyển và đã xét cho mô hình nhiễu loạn log-chuẩn. Giả thuyết này dự đoán rằng các tham số Rytov tăng không giới hạn theo tham số cấu trúc chỉ số khúc xạ hoặc độ dài đường truyền. Tuy nhiên, dựa trên các kết quả thử nghiệm được đề cập trong, dự đoán này đúng với trường hợp nhiễu loạn yếu, khi $\sigma_x^2 <= 0.3$. Khi cường độ nhiễu loạn tăng, do sự kết hợp của độ dài đường truyền tăng hoặc C_n^2 tăng, các xoáy nhiễu loạn tạo ra đa tán xạ không được tính đến trong mô hình Rytov.

Dựa trên các kết quả được đưa ra ở hình 2.6, chỉ số nhấp nháy *S.I* tăng tuyến tính với tham số Rytov trong vùng nhiễu loạn yếu và tiếp tục tăng đến giá trị cực đại lớn hơn 1. Vùng mà trong đó *S.I* đạt giá trị tối đa đặc trưng cho cường độ cao nhất của sự không đồng nhất. Sau đó *S.I* bắt đầu giảm do nhiễu.



Hình 2.6: Hàm mật độ log-chuẩn với E[I] =1 cho dãy giá trị của σ_I^2

2.4.2 Mô hình nhiễu loạn Gamma-gamma

Mô hình nhiễu loạn Gamma-Gamma được đề xuất bởi Andrews, sự thăng giáng của trường quang truyền qua khí quyển nhiễu loạn được giả thiết bao gồm các ảnh hưởng phạm vi nhỏ (tán xạ) và ảnh hưởng phạm vi lớn (khúc xạ). Các thăng giáng phạm vi lớn được tạo ra bởi các xoáy nhiễu loạn lớn hơn vùng tán xạ. Các xoáy nhiễu loạn kích thước nhỏ được giả định được điều chế bởi các xoáy nhiễu loạn kích thước lớn. Do đó, cường độ trường quang thu chuẩn hóa I được xác định là tích của hai quá trình ngẫu nhiên độc lập thống kê I_x và I_y, nó được biểu diễn theo công thức (2.20):

$$I = I_x I_y \tag{2.20}$$

I_x và I_y phát sinh từ các xoáy nhiễu loạn kích thước lớn và kích thước nhỏ, được đề xuất tuân theo phân bố Gamma. Hàm mật độ xác suất của chúng được xác định như trong công thức (2.21) và (2.22).

$$P(I_x) = \frac{\alpha(\alpha I_x)^{\alpha-1}}{\Gamma_\alpha} \exp(-\alpha I_x) \tag{2.21}$$

$$P(I_y) = \frac{\beta(\beta I_y)^{\beta-1}}{\Gamma_\beta} \exp(-\beta I_x) \tag{2.22}$$

Thay $I_y = I/I_x$ vào công thức (2.22) ta được công thức (2.23).

$$P(I/I_x) = \frac{\beta(\beta I/I_x)^{\beta-1}}{\Gamma_\beta}\exp(-\beta I/I_x); I>0 \quad (2.23)$$

trong đó I_x là giá trị trung bình của I.

Để nhận được phân bố cường độ vô điều kiện, xác suất có điều kiện p (I/I_x) được tính trung bình trên phân bố thống kê của I_x, được xác định theo (2.22) để có được hàm phân bố cường độ trường theo phân bố Gamma-gamma như sau [20]:

$$p(I) = \int_0^\infty p\left(\frac{I}{I_x}\right)p(I_x)dI_x = \frac{2(\alpha\beta)^{\frac{\alpha+\beta}{2}}}{\Gamma(\alpha)\Gamma(\beta)} I^{(\frac{\alpha+\beta}{2})-1} K_{\alpha-\beta}; I>0 \quad (2.24)$$

α và β lần luợt là số lượng hiệu dụng của các xoáy kích thước lớn và xoáy kích thước nhỏ của quá trình tán xạ. $K_n(.)$ là hàm Bessel sửa đổi loại 2 bậc n và $\Gamma(.)$ là hàm Gamma. Nếu trường quang tại máy thu được giả định là sóng phẳng, thì hai tham số α, β đặc trưng cho pdf của biến động cường độ theo các điều kiện khí quyển và được xác định như sau [20]:

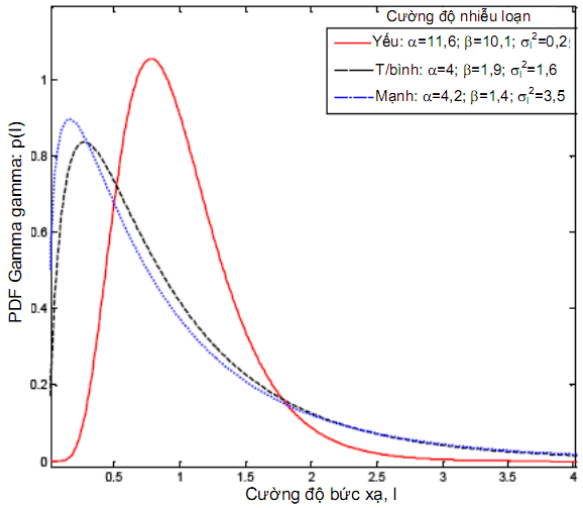
$$\alpha = \frac{1}{\exp\frac{0.49\sigma_l^2}{\left(1+1.11\sigma_l^{12/5}\right)^{7/6}}-1} \quad (2.25)$$

$$\beta = \frac{1}{\exp\frac{0.51\sigma_l^2}{\left(1+0.69\sigma_l^{12/7}\right)^{5/6}}-1} \quad (2.26)$$

Chỉ số nhấp nháy được xác định bởi công thức (2.27)

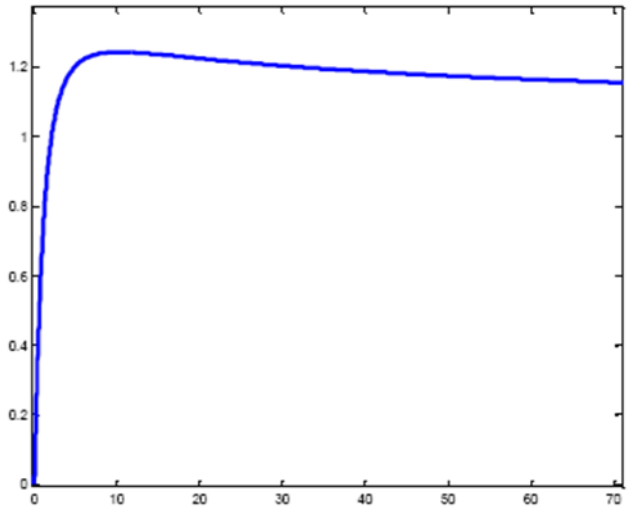
$$S.I = \exp\left(\frac{1}{\exp\frac{0.51\sigma_l^2}{\left(1+0.69\sigma_l^{12/5}\right)^{5/6}}} + \frac{1}{\exp\frac{0.49\sigma_l^2}{\left(1+1.11\sigma_l^{12/7}\right)^{7/6}}}\right)-1 \quad (2.27)$$

Phân bố xác suất Gamma cho kênh truyền nhiễu loạn yếu , trung bình và mạnh được thể hiện qua Hình 2.7.

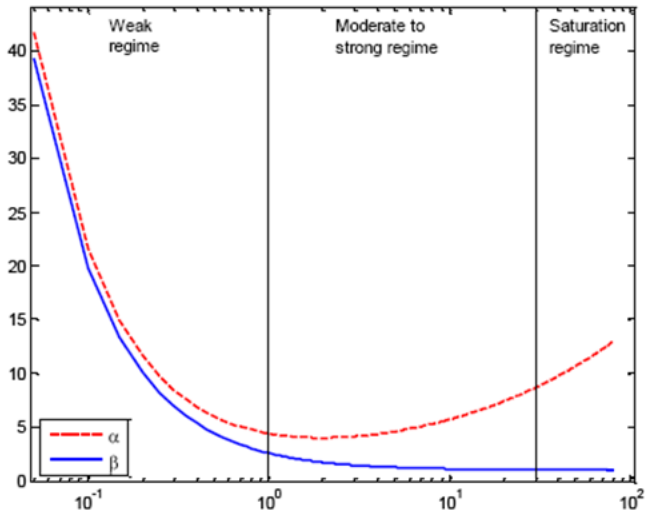


Hình 2.7: Hàm mật độ xác suất Gamma-Gamma cho ba chế độ nhiễu loạn khác nhau: yếu, trung bình và mạnh [16]

Mô hình nhiễu loạn Gamma-gamma theo (2.24) có giá trị cho tất cả các kịch bản nhiễu loạn từ yếu đến mạnh, các giá trị của α và β ở bất kỳ chế độ nào cũng được xác định theo (2.25). Hình 2.8 chỉ ra sự thay đổi của *S.I* là một hàm của tham số Rytov dựa trên (2.26), biểu đồ này chỉ ra rằng khi tham số Rytov tăng, *S.I* tiệm cận giá trị cực đại lớn hơn 1 và sau đó tiệm cận 1 khi nhiễu loạn gây ra phađinh tiệm cận chế độ bão hòa. Các giá trị của α và β theo các chế độ nhiễu loạn khác nhau được mô tả trong Hình 2.9. Trong chế độ nhiễu loạn rất yếu, $\alpha >> 1$ và $\beta >> 1$ như chỉ trong Hình 2.9, điều này có nghĩa số lượng hiệu dụng các xoáy kích thước lớn và xoáy kích thước nhỏ là rất lớn. Nhưng khi biến động cường độ bức xạ tăng (vượt quá $\sigma_l^2 = 0{,}2$) và chế độ tập trung được tiếp cận, thì α và β giảm đáng kể (như chỉ trong Hình 2.9). Ngoài chế độ tập trung (trung bình đến mạnh) và tiệm cận đến chế độ bão hòa, $\beta \to 1$ Điều này có nghĩa là số lượng hiệu dụng của các xoáy kích thước nhỏ giảm đến một giá trị xác định bởi bán kính kết hợp không gian của sóng ánh sáng [20]. Mặt khác, số lượng hiệu dụng của tán xạ khúc xạ rời rạc, α, lại tăng khi nhiễu loạn tăng và cuối cùng trở thành không giới hạn trong chế độ bão hòa như chỉ trong Hình 2.9.



Hình 2.8: S.I theo phương sai log-cường độ với $C_n^2 = 10^{-15}$ $m^{-2/3}$ và λ = 850 nm



Hình 2.9: Giá trị của α và β với các chế độ nhiễu loạn khác nhau: yếu, trung bình, mạnh và bão hòa

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 2 cũng đã đưa ra những so sánh giữa hệ thống truyền thông FSO và hệ thống truyền thông RF để thấy rõ được những ưu điểm nổi bật mà công nghệ FSO đem lại mô hình truyền

thông quang không dây FSO. Tuy nhiên, những tác động trong không khí như suy hao do điều kiện thời tiết và nhiễu loạn trong không khí sẽ ảnh hưởng đến hiệu năng của hệ thống truyền thông FSO. Đồng thời đưa ra mô hình sử dụng công nghệ FSO cho hệ thống truyền thông vệ tinh và hạ tầng trên cao, tại HAP sử dụng kỹ thuật chuyển tiếp để cải thiện hiệu năng hệ thống. Lợi ích của kỹ thuật chuyển tiếp đến hiệu năng hệ thống QKD dựa trên vệ tinh tới mặt đất sẽ được phân tích rõ hơn ở chương 3.

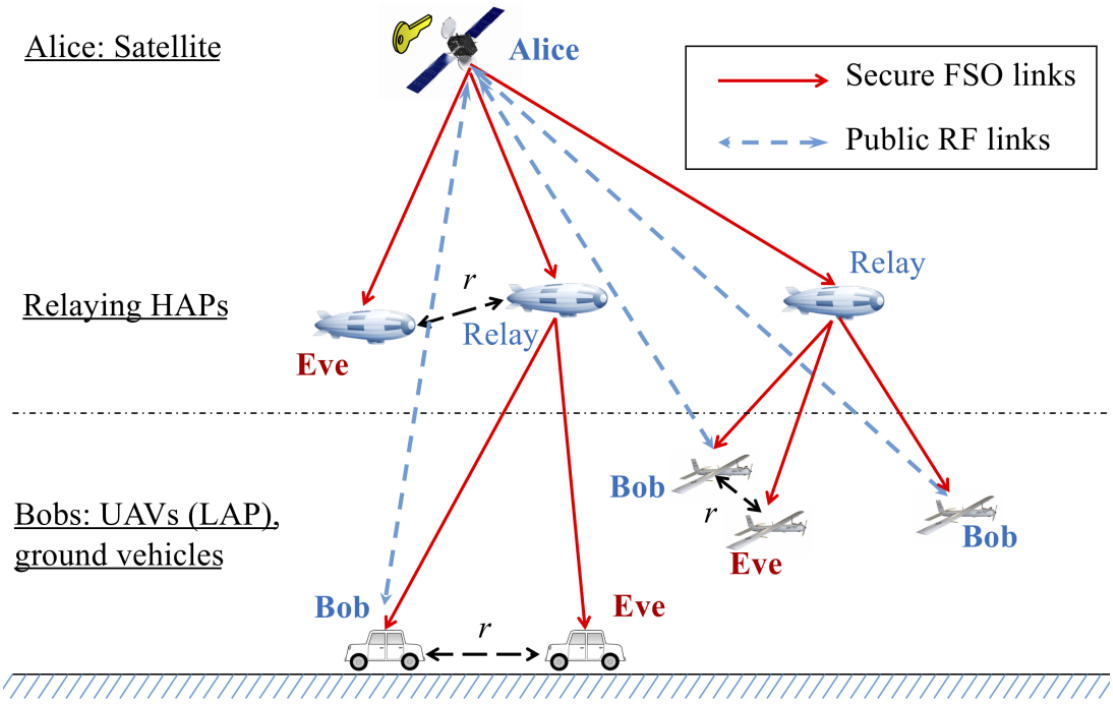
CHƯƠNG 3: PHÂN TÍCH HIỆU NĂNG HỆ THỐNG QKD DỰA TRÊN VỆ TINH SỬ DỤNG KỸ THUẬT CHUYỂN TIẾP

Tóm tắt: Chương này phân tích hiệu năng hệ thống phân phối khóa lượng tử (QKD) dựa trên vệ tinh sử dụng kỹ thuật chuyển tiếp. 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 thực hiện chức năng khuếch đại quang và chuyển tiếp (OAF). Luận văn 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. Mô hình sử dụng búp song dạng Gauss để đánh giá tác động của tổn hao hình học đối với tín hiệu mà người dùng hợp pháp nhận được và xác suất bị nghe trộm. Các kết quả xác nhận tính khả thi của hệ thống sử dụng kỹ thuật chuyển tiếp tại HAP.

3.1 Mô hình hệ thống QKD vệ tinh – mặt đất

Giao thức QKD được thực hiện trong hệ thống đề xuất được dựa trên SIM sử dụng khóa dịch pha nhị phân (SIM/BPSK). Mô hình của hệ thống QKD/FSO đề xuất được minh họa trong hình 3.1, cung cấp giải pháp phân phối khóa không dây cho các trạm di động (Bob), có thể là UAV, phương tiện giao thông hoặc bất kỳ trạm không dây nào. Khác với các hệ thống thông thường có kết nối trực tiếp từ vệ tinh, mô hình đề xuất sử dụng hạ tầng trên cao (HAP) làm trạm chuyển tiếp tín hiệu quang từ vệ tinh quỹ đạo trái đất thấp (LEO) (tức là Alice) đến các trạm di động. HAP có thể là khí cầu, khinh khí cầu, máy bay không người lái hoặc máy bay có người lái ở trên các đám mây ở độ cao điển hình từ 17 đến 25 km[21]. Hệ thống chuyển tiếp được hỗ trợ bởi HAP có các tính năng thuận lợi cho cả thông tin liên lạc vệ tinh và mặt đất, có chi phí vận hành hợp lý, bảo trì dễ dàng và triển khai nhanh chóng. Một tính năng quan trọng khác của hệ thống được đề xuất là việc sử dụng các hệ thống FSO tiêu chuẩn sử dụng điều chế cường độ sóng mang phụ (SIM) với khóa dịch pha nhị phân (BPSK) với tách sóng trực tiếp hai ngưỡng (DT/DD) giúp bắt chước trạng thái lượng tử truyền [9]. Ở HAP, cơ chế khuếch đại và chuyển tiếp (AF) quang được sử dụng để giảm độ phức tạp của phần cứng. Luận văn phân tích

tính toán tốc độ khóa bí mật ergodic xem xét ảnh hưởng của nhiễu loạn khí quyển và các nhiễu khác. Mô hình búp Gauss được sử dụng để đánh giá tác động của sự mở rộng. Luận văn xem xét hai tình huống nghe trộm khi bên nghe trộm được đặt gần nút chuyển tiếp (tức là HAP) hoặc khi nó ở gần Bob như hình 3.1 dưới đây:



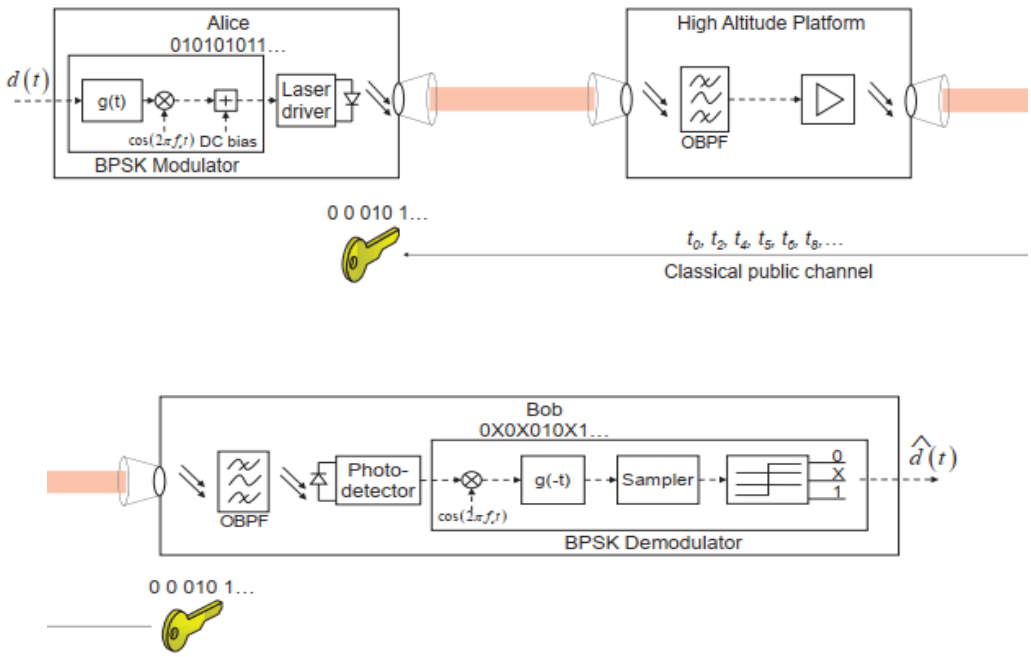
Hình 3.1: Mô hình hệ thống QKD/FSO dựa trên vệ tinh sử dụng kỹ thuật chuyển tiếp tại HAP

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 [2], 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" [22]. Tại trạm trung tâm (bộ phát của 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. Tiếp theo, tín hiệu BPSK, bao gồm cả giá trị âm và dương, được cộng thêm dòng định thiên DC vào trước khi điều chế với sóng quang liên tục được tạp ra bởi LED. LED chỉ có thể được điều chế bởi các tín hiệu dương nên tín hiệu BPSK

phải cộng thêm với dòng DC trước khi đưa vào điều chế. Sau đó, tín hiệu quang được truyền qua không gian qua HAP tới Bob.

Tại phía thu (Bob), tín hiệu thu được đưa qua bộ tách sóng APD. Sau đó, tín hiệu được giải điều chế bằng cách nhân với tín hiệu đến từ bộ dao động nội có tần số là tần số của sóng mang con vô tuyến. 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). Như chỉ ra trong hình 3.2, hai mức ngưỡng d_0 và d_1, được thiết lập tại phía Bob cho việc tách sóng tín hiệu. Nếu dòng tín hiệu nhận được nhỏ hơn d_0, bit "0" sẽ được quyết định. Nếu dòng tín hiệu nhận được lớn hơn d_1 , bit "1" sẽ được quyết định. Trường hợp còn lại, bit "x" (không bit nào) được tạo ra.



Hình 3.2: Sơ đồ khối của hệ thống FSO/QKD hỗ trợ chuyển tiếp HAP sử dụng SIM/BPSK và bộ thu DT / DD

Khi Bob khôi phục tín hiệu đã nhận, Bob sử dụng hai ngưỡng (DT) với quy tắc phát hiện là:

$$\text{Quyết định} = \begin{cases} 0\text{: } nếu\ (i \le d_0) \\ 1\text{: } nếu\ (i \ge d_1) \\ \text{X: } các\ trường\ hợp\ còn\ lại \end{cases} \qquad (3.1)$$

Trong đó X biểu thị trường hợp Bob không khôi phục bit đã truyền. Điều này tương tự như trường hợp lựa chọn cơ sở không chính xác trong giao thức BB84 ban đầu [5]. Hai mức của hai ngưỡng, d_0 và d_1, có thể được chọn đối xứng qua mức "không". Sau đó, các bước sau tương tự như trong giao thức BB84 gốc, bao gồm điều chế tín hiệu và khuếch đại tín hiệu, sẽ được thực hiện qua kênh công khai. Tính bảo mật của ý tưởng thiết kế này được giải thích như sau. Thứ nhất, độ sâu điều chế δ của các tín hiệu SIM/BPSK được chọn là đủ nhỏ để Eve không thể phân biệt hoàn toàn trạng thái được phát. Eve cũng có thể cố gắng sử dụng hai ngưỡng D-T như Bob, tuy nhiên, sự thăng giáng tín hiệu của Eve không tương quan với tín hiệu của Bob, do đó các bit khóa được tạo ra bởi Bob và Eve không khớp nhau. Nếu Eve cố giải mã khóa bằng cách sử dụng ngưỡng tối ưu $(D_e = 0)$, nó thu được các giá trị đo trong đó hai tín hiệu bị chồng chéo nhiều lên nhau, vì vậy nó sẽ phải chịu một tỷ lệ lỗi cao, do đó làm giảm sự hiểu biết về khóa có lợi cho Eve. Thứ hai, xác suất chọn lọc cũng có thể được điều khiển bởi Bob thông qua thiết lập hai ngưỡng D-T. Điều này có nghĩa là lượng thông tin được chia sẻ giữa Alice và Bob có thể được kiểm soát. Kết quả là, mô hình có thể đảm bảo tỷ lệ bí mật tích cực bằng cách điều chỉnh độ sâu điều chế và cài đặt D-T đúng cách để thông tin tương hỗ giữa Alice và Bob luôn lớn hơn thông tin Eve thu được theo các chiến lược nghe lén khác nhau.

3.1.2 Mô hình hệ thống

Sơ đồ khối của hệ thống FSO/QKD chuyển tiếp hỗ trợ HAP được đề xuất sử dụng SIM/BPSK và bộ thu DT/DD được trình bày trong Hình 3.2. 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 [21]. 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.

Tại vệ tinh, dữ liệu $d(t)$ của Alice được điều chế thành tín hiệu sóng mang phụ tần số vô tuyến (RF) bằng cách sử dụng điều chế BPSK. Độ lệch DC sẽ được

thêm vào tín hiệu sóng mang phụ $m(t)$ trước khi nó được sử dụng để điều chế chùm tia laze sóng liên tục vì $m(t)$ là sóng hình sin có cả giá trị âm và dương.

Công suất truyền từ Alice được định nghĩa như sau:

$$P_t^{(S)} = \frac{P}{2}\left[1+\delta m(t)\right] \tag{3.2}$$

trong đó P là công suất phát đỉnh, δ là độ sâu điều chế cường độ (IM), ($0 < \delta < 1$) để đảo ngược quá điều chế ($-1 < \delta m(t) < 1$).

Tín hiệu sóng mang con được mô tả như sau:

$$m(t) = A(t)g(t)\cos(2\pi f_c t + a_i \pi) \tag{3.3}$$

trong đó A là biên độ sóng mang con, g (t) là hàm định hình xung hình chữ nhật, f_c là tần số sóng mang phụ, và a_i với i ∈ {0; 1} biểu thị cho dữ liệu nhị phân thứ i theo bit "0" và bit "1". Công suất của m (t) được chuẩn hóa thành 1 để đơn giản hóa việc phân tích. Trước khi được gửi đến kênh FSO, tín hiệu quang phát sẽ được khuếch đại bởi thấu kính phát với độ lợi $G_{TX}^{(S)}$.

Tại HAP, công suất quang nhận được từ đầu ra của thấu kính bộ thu với độ lợi $G_{RX}^{(P)}$ được đưa qua bộ lọc thông dải quang (OBPF) để giảm nhiễu nền. Tiếp theo, tín hiệu đã lọc được khuếch đại trực tiếp bằng bộ khuếch đại quang trong miền quang. Độ lợi của bộ khuếch đại quang được ký hiệu là G_A. Sau đó, tín hiệu được khuếch đại đi đến thấu kính phát của máy phát HAP với độ lợi $G_{TX}^{(P)}$ trước khi được chuyển tiếp đến Bob. Cuối cùng, tín hiệu quang Bob nhận được từ HAP được truyền qua thấu kính với độ lợi $G_{RX}^{(G)}$ và OBPF sau đó được chuyển thành tín hiệu điện bằng bộ tách sóng quang (APD). Tín hiệu quang nhận được được chuyển đổi thành dòng tách quang. Sau đó Bob sử dụng một bộ giải điều chế RF tiêu chuẩn để giải điều chế ra tín hiệu d(t) . Đầu ra của APD có thể được biểu thị như sau:

$$i_r(t) = \Re M \frac{P_r^{(G)}}{2} h_a(t)[1 + \delta m(t)] + n(t) \tag{3.4}$$

trong đó $\Re = \frac{\eta q}{h\nu}$ là đáp ứng của APD với η là hiệu suất lượng tử, q là điện tích electron, h là hằng số Planck, ν là tần số quang và M là hệ số khuếch đại của APD.

Công suất nhận tại phía thu được xác định bằng:

$$P_r^{(G)0} = \frac{1}{FSL} P G_{TX}^{(S)} h_p^{(P)} G_{RX}^{(P)} G_A G_{TX}^{(P)} G_{RX}^{(G)} h_l h_p^{(G)} \tag{3.5}$$

trong đó FSL là tổn hao đường truyền giữa Alice và HAP được trình bày trong phần 3.2 $H_p^{(P)}$ là công suất do HAP thu được, h_l là tổn thất đường truyền giữa HAP và *GS*, $h_p^{(G)}$ là phần công suất được thu bởi Bob, và $h_a(t)$ là tham số trạng thái kênh FSO đặc trưng cho suy hao khí quyển của kênh truyền FSO giữa HAP và GS. $n(t)$ là tạp âm của máy thu. $i_r(t)$ được giải điều chế bằng cách trộn với bộ dao động nội có dạng $\cos(2\pi f_c t)$. Dòng tín hiệu sau giải điều chế được xác định như sau:

$$t(t) = \overline{i_r(t)\cos(2\pi f_c t)} = \begin{cases} i_0 = -\frac{1}{4}\Re M P_r^{(G)} \delta h_a(t) + n(t) \\ i_1 = \frac{1}{4}\Re M P_r^{(G)} \delta h_a(t) + n(t) \end{cases} \tag{3.6}$$

trong đó i_0 và i_1 biểu thị dòng tách quang tương ứng cho bit "0" và bit "1". Luận văn giả định rằng dòng tối là không đáng kể, nhiễu nhận được bao gồm nhiễu nổ, nhiễu nền và nhiễu phát xạ tự bộ phát xạ khuếch đại (ASE) được tạo ra bởi bộ khuếch đại quang học tại HAP. Chúng được mô hình hóa dưới dạng nhiễu Gauss trắng cộng (AWGN) với giá trị trung bình bằng không. Do đó, $n(t)$, là tổng của nhiễu nổ, nhiễu nền và nhiễu ASE, là nhiễu AWGN trung bình bằng 0 với tổng phương sai được xác định bởi (3.7):

$$\sigma_N^2 = \sigma_{sh}^2 + \sigma_b^2 + \sigma_{th}^2 + \sigma_a^2 \tag{3.7}$$

trong đó σ_{sh}^2 là phương sai của nhiễu nổ bị chi phối bởi công suất nhận được, σ_b^2 là phương sai của nhiễu nền, σ_{th}^2 là phương sai của nhiễu nhiệt, và σ_a^2 là phương sai của nhiễu ASE. Cuối cùng, tín hiệu giải điều chế được phát hiện bởi DT để tạo ra

các bit nhị phân “0”, “1” hoặc “x” (tức là không có bit nào được tạo) dựa trên quy tắc quyết định trong (3.1).

3.2 Kỹ thuật chuyển tiếp cho hệ thống QKD

Hệ thống QKD/FSO kết nối vệ tinh LEO tới trạm mặt đất sử dụng kỹ thuật chuyển tiếp được chia thành hai chặng với chặng thứ nhất là từ vệ tinh LEO tới HAP và chặng tiếp theo là từ HAP tới trạm mặt đất. Mỗi chặng sẽ có mô hình kênh riêng biệt và được trình bày lần lượt như sau:

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

Tham số cấu trúc chỉ số khúc xạ C_n^2, xác định cường độ nhiễu loạn, có thể được coi bằng 0 khi độ cao lớn hơn 30 km. Do đó, 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 hao suy hao không gian tự do và suy hao do lệch hướng búp sóng.

Suy hao không gian tự do: Vệ tinh truyền chùm tia laser qua không gian tự do đến HAP được đặt ở độ cao 20 km, kết nối này chủ yếu bị suy hao không gian tự do (FSL), có thể được biểu thị bằng:

$$FSL = (\frac{4\pi L_s}{\lambda})^2 \tag{3.8}$$

trong đó L_S là khoảng cách truyền giữa vệ tinh và HAP, có thể được tính là $L_S = (H_S - H_P)/\cos(\zeta_S)$, với λ là bước sóng hoạt động của hệ thống, H_S và H_P lần lượt là độ cao của vệ tinh và HAP, ζ_S là góc góc thiên đỉnh từ HAP tới vệ tinh.

Suy hao do lệch hướng búp sóng: Để đánh giá tác động của sự lệch hướng búp sóng quang do búp chính của anten thu hướng không đúng chùm tia phát xạ của anten phát luận văn xem xét khẩu độ thu bán kính tròn a^P và búp sóng quang được mô hình hóa theo mô hình phân bố Gauss tại máy thu. Phân bố cường độ tín hiệu phát chuẩn hóa theo không gian z từ máy phát đối với chùm Gauss có thể được biểu thị như sau:

$$I_{beam}(\rho; z) = \frac{2}{\pi\omega_z^2}\exp(-\frac{2\|\rho\|^2}{\omega_z^2}) \tag{3.9}$$

trong đó ρ là vectơ bán kính từ tâm búp sóng quang, ω_z là độ rộng búp sóng quang ở khoảng cách z [23]. Khoảng cách tương đối giữa tâm của máy thu và tâm của búp sóng thu được gây ra suy hao công suất do sự lệch hướng búp sóng. Suy hao lệch hướng búp sóng này với sai số định hướng q có thể được tính như công thức (3.10):

$$h_p^{(P)}(q;z) = \int_A I_{beam}(\rho - q; z)d\rho \quad (3.10)$$

trong đó $h_p^{(P)}(.)$ biểu thị phần công suất được thu bởi bộ thu và A là diện tích của bộ thu. Phương trình (3.10) có thể được ước lượng dưới dạng Gauss như sau:

$$h_p^{(P)}(r; a^{(P)}) \approx A_0^P \exp(-\frac{2r^2}{\omega_{zeq}^{2(P)}}) \quad (3.11)$$

trong đó $r = \|q\|$ là độ lớn của q, $v^{(P)} = \frac{\sqrt{\pi}a^{(P)}}{\sqrt{2}\omega_z^{(P)}}, A_0^{(P)} = \left[\text{erf}\,(v^{(P)})\right]^2$

và $\omega_{zeq}^{2(P)} = \omega_z^{2(P)} \frac{\sqrt{\pi}\text{erf}(\text{v}^{(P)})}{2v\exp(-v^{2(P)})}.A_0^{(P)}$ là công suất thu được tại r = 0 và $\omega_{zeq}^{(P)}$ là độ rộng búp tương đương ở HAP.

Công thức (3.11) được sử dụng để tính toán công suất quang nhận được tại nút chuyển tiếp dựa trên HAP cũng như tại bộ thu của Eve đặt gần HAP. Trong kịch bản nghe trộm này, máy thu của HAP nằm ở tâm chùm, tức là r = 0 trong khi công suất quang mà Eve nhận được tỷ lệ nghịch với r với r > 0.

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 tới GS. 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 $h = h_l h_P^{(G)} h_a$, 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.

Suy hao đường truyền, h_l: Suy hao khí quyển được xác định bởi Định luật Beer-Lambert theo hàm mũ được biểu thị như sau:

$$h_l = \exp(-\sigma L_p) \quad (3.12)$$

trong đó L_P, được định nghĩa là $L_P = H_P / \cos(\zeta_p)$, là khoảng cách truyền giữa HAP và nút mặt đất, H_P là độ cao của HAP, ζ_P là góc thiên đỉnh được xác định là góc hướng lan truyền từ HAP đến nút mặt đất, σ là hệ số suy giảm.

Suy hao lệch hướng búp sóng, $h_p^{(G)}$, suy hao gây ra bởi sự lệch hướng búp sóng quang do búp chính của anten thu hướng không đúng chùm tia phát xạ của anten phát từ HAP đến nút mặt đất (tức là Bob hoặc Eve) có thể được biểu thị tương tự theo phương trình (3.13) như sau:

$$h_p^{(G)}(r; a^{(G)}) \approx A_0^G \exp(-\frac{2r^2}{\omega_{zeq}^{2(G)}}) \tag{3.13}$$

trong đó $v^{(G)} = \dfrac{\sqrt{\pi} a^{(G)}}{\sqrt{2}\omega_z^{(G)}}$ với $a^{(G)}$ là bán kính của khẩu độ thu tại trạm mặt đất, $\mathrm{A}_0^{(G)} = \left[\mathrm{erf}(v^{(G)})\right]^2$ là phần công suất thu được tại r = 0 khi máy thu là của Bob và $\omega_{zeq}^{2(G)} = \omega_z^{2(G)} \dfrac{\sqrt{\pi}\,\mathrm{erf}(v^{(G)})}{2v\exp(-v^{2(G)})}$ là độ rộng tương ứng của chùm quang từ HAP đến trạm mặt đất.

Sự nhiễu loạn của khí quyển, h_a : Sự nhiễu loạn khí quyển là do sự kết hợp giữa không khí ấm và không khí lạnh hơn của các lớp trên. Chiết suất khí quyển phụ thuộc vào nhiệt độ và mật độ không khí cũng như thay đổi theo không gian và thời gian. Hiện tượng này dẫn đến tín hiệu tiêu hao dần và giảm hiệu suất hệ thống. Đối với các nhiễu loạn trung bình đến mạnh, phân phối Gamma-Gamma (GG) được sử dụng với $h_a > 0$ như (3.14):

$$fh_a(h_a) = \frac{2(\alpha\beta)^{\frac{\alpha+\beta}{2}}}{\Gamma(\alpha)\Gamma(\beta)} (h_a)^{(\frac{\alpha+\beta}{2})-1} K_{\alpha-\beta}(2\sqrt{\alpha\beta h_a}) \tag{3.14}$$

trong đó $K_{\alpha-\beta}(.)$ là hàm Bessel sửa đổi loại hai và bậc $(\alpha-\beta).\Gamma(\omega)\Gamma \triangleq \int_0^\infty t^{\omega-1}\exp(-t)dt$ là hàm Gamma, α và β lần lượt là số lượng hiệu dụng của các xoáy kích thước lớn và xoáy kích thước nhỏ của quá trình tán xạ

và được cho dưới dạng hàm của phương sai Rytov σ_R^2 như trong [24]. Trong trường hợp liên kết từ HAP đến trạm mặt đất, σ_R^2 có thể được đưa ra theo công thức (3.15):

$$\sigma_R^2 = 2.25k^{7/6}\sec^{11/6}(\zeta_P)\int_{h_0}^{H_P} C_n^2(h)(h-h_0)^{5/6}dh \tag{3.15}$$

trong đó $k = 2\pi/\lambda$ là số sóng và h_0 là độ cao của node mặt đất [25]. Độ lớn của nhiễu loạn được xác định bởi tham số cấu trúc chiết suất C_n^2. Nó sẽ thay đổi theo vị trí địa lý, độ cao và thời gian trong ngày. C_n^2 có thể được mô hình hóa bởi mô hình Hufnagel-Valley (H-V) để ước tính các cấu hình nhiễu loạn như [90]:

$$\begin{aligned} C_n^2(h) = 0.00594(\tfrac{\omega}{27}(10^{-5}\exp(-\tfrac{h}{1000}) + 2.7\times10^{-16}\exp(-\tfrac{h}{1500}) \\ +C_n^2(0)\exp(-\tfrac{h}{100}) \end{aligned} \tag{3.16}$$

trong đó *w* là vận tốc gió bình phương gốc, *h* là độ cao so với mặt đất, và $C_n^2(0) - 1.7\times10^{-14}m^{-2/3}$ là giá trị của C_n^2 tại mặt đất.

3.3 Phân tích hiệu năng hệ thống

Luận văn rút ra tốc độ khóa bí mật ergodic (*S*) của hệ thống được đề xuất trong trường hợp tấn công trái phép máy thu. Tốc độ khóa bí mật được định nghĩa là tốc độ truyền dẫn tối đa mà Eve không thể giải mã bất kỳ thông tin nào. Thông tin chung *I (A; B)* và *I (A; E)* là lượng thông tin được chia sẻ giữa Alice và Bob, và thông tin được chia sẻ giữa Alice và Eve. Chúng có thể được mô tả như công thức (3.17), (3.18):

$$I(A;B) = H(B) - H(B|A) \tag{3.17}$$

$$I(A;E) = H(E) - H(E|A) \tag{3.18}$$

trong đó $H(B)$ và $H(E)$ tương ứng biểu thị cho các entropy thông tin của Bob và Eve. $H(B|A)$ và $H(E|A)$ lần lượt đại diện cho entropy có điều kiện của Bob-Alice và Eve-Alice. Tốc độ khóa bí mật ergodic có thể được tính bằng cách tính đến thông tin tương hỗ $I(A;B)$ và $I(A;E)$ theo (3.19):

$$S = I(A;B) - I(A;E) \tag{3.19}$$

khi S dương, thông tin mà Eve thu thập sẽ bị giảm đi. Nếu không, bảo mật của hệ thống được đề xuất ở phần 3.2 bị đe dọa bởi Eve. Do đó S có thể được coi là tốc độ truyền tối đa mà bên nghe trộm không thể giải mã được bất kỳ thông tin nào.

Việc truyền thông tin giữa Alice và Bob có thể được mô hình hóa như một kênh xóa nhị phân (BEC) có lỗi [22], và do đó, thông tin giữa Alice và Bob $I(A;B)$ có thể được xác định theo (3.20):

$$\begin{aligned} I(A;B) &= p\log_2(p) + (1-p-q)\log_2(1-p-q) \\ &-(\alpha p + (1-\alpha)(1-p-q))\log_2(\alpha p + (1-\alpha)(1-p-q)) \\ &-(\alpha(1-p-q) + (1-\alpha)p)\log_2(\alpha(1-p-q) + (1-\alpha)p) \end{aligned} \tag{3.20}$$

ở đây, p và q là xác suất phát hiện đúng (ví dụ: $P_{A,B}(1,1)$) và sai (ví dụ: $P_{A,B}(1,0)$), tương ứng và có thể được biểu thị chung theo (3.21), (3.23):

$$P_{A,B}(a,0) - \frac{1}{2}\int_0^{\infty} Q\left(\frac{i_a - d_0}{\sigma_N}\right) f h_a(h_a) dh_a \tag{3.21}$$

$$P_{A,B}(a,1) - \frac{1}{2}\int_0^{\infty} Q\left(\frac{d_1 - i_a}{\sigma_N}\right) f h_a(h_a) dh_a \tag{3.22}$$

trong đó $a \in \{0,1\}, Q(.) \triangleq \frac{1}{\sqrt{2\pi}}\int_0^{\infty} \exp(-t^2/2)dt$ đại diện cho hàm Gauss Q, và i_a biểu thị các tín hiệu hiện tại nhận được cho bit "a" có thể được mô tả theo (3.23):

$$i_0 = -\frac{1}{4}\Re M P_r^{(G)} \delta h_a \text{ và } i_1 = -i_0 \tag{3.23}$$

trong đó $P_r^{(G)} = \frac{1}{FSL} P G_{TX}^{(S)} h_p^{(P)} G_{RX}^{(P)} G_A G_{TX}^{(P)} G_{RX}^{(P)} h_l$ là công suất đỉnh thu được ở Bob. Hai ngưỡng phát hiện d_0 và d_1 được xác định bằng cách sử dụng các lựa chọn DT như sau:

$$d_0 = E(i_0) - \varsigma\sqrt{\sigma_N^2} \text{ và } d_1 = E(i_1) - \varsigma\sqrt{\sigma_N^2} \tag{3.24}$$

trong đó ς là hệ số tỉ lệ hai ngưỡng, σ_N^2 là phương sai nhiễu và $E(i_a)$ là giá trị trung bình của i_a [22]. Ta coi $E[h_l h_a] = E[h_l] = h_l$ với $E[h_a] = 1$.

Bằng cách sử dụng phương pháp vuông góc Gauss-Laguerre $\int_0^\infty g(y)\exp(-y)dy \approx \sum_{i=q}^{M} v_i g(\tau_l)$ [26] các biểu thức dạng gần đúng cho xác suất chung trong (3.21) và (3.22) có thể được tính tương ứng theo (3.25), (3.26):

$$P_{A,B}(a,0) \approx \frac{1}{2}\sum_{i=1}^{N}\sum_{l=1}^{M} a_i\,\zeta_i^{-b_i} v_l \tau_l^{b_i-1} Q\left(\frac{\mp\frac{1}{4\times\zeta_i}\Re M P_r^{(G)}\delta\tau_l - d_0}{\sigma_{N-i,l}}\right) \quad (3.25)$$

$$P_{A,B}(a,1) \approx \frac{1}{2}\sum_{i=1}^{N}\sum_{l=1}^{M} a_i\,\zeta_i^{-b_i} v_l \tau_l^{b_i-1} Q\left(\frac{d_1 \pm\frac{1}{4\times\zeta_i}\Re M P_r^{(G)}\delta\tau_l}{\sigma_{N-i,l}}\right) \quad (3.26)$$

trong đó phương sai nhiễu $\sigma_{N-i,l}$ được biểu thị bằng phương trình (3.27)

$$\sigma_{N-i,l} = \sqrt{2qF_A M^2 \Re\left(\begin{matrix}\frac{1}{4\times\xi_i}\Re M P_r^{(G)}\delta\tau_\iota + \frac{1}{\xi_i}P_b^{(P)}P_{RX}^{(P)}G_A G_{TX}^{(P)}H_p^{(G)}G_{RX}^{(P)}h_l\tau_\iota \\ + \frac{1}{\xi_i}P_A G_{RX}^{(P)}G_A G_{TX}^{(P)}h_p^{(G)}G_{RX}^{(G)}h_l\tau_\iota + P_b^{(G)}P_{RX}^{(G)}\end{matrix}\right)\triangle f + \frac{4k_B T F_n}{R_l}\triangle f} \quad (3.27)$$

Trong các biểu thức dạng gần đúng này, a_i, b_i và ξ_i là các tham số của phân phối hỗn hợp-Gamma (MG) ước tính phân phối GG. N là số thành phần hỗn hợp. v_l và τ_l là các hệ số trọng số và các áp suất của đa thức Laguerre với M là số lần lặp để tích phân Laguerre gần đúng về mặt số học. Phép tính gần đúng này sẽ cho kết quả chính xác khi N = M = 10.

Giả sử rằng Eve sử dụng ngưỡng phát hiện $d_E = 0$ để tối đa hóa thông tin của nó và thông tin tương hỗ $I(A;E)$ có thể được biểu thị bằng (3.28):

$$I(A;E) = 1 + e\log_2(e) + (1-e)\log_2(1-e) \quad (3.28)$$

trong đó *e* biểu thị xác suất lỗi của Eve được xác định theo (3.29):

$$e = P_{A,E}(0,1) + P_{A,E}(1,0) \quad (3.29)$$

trong đó $P_{A,E}(0,1)$ và $P_{A,E}(1,0)$ là xác suất các bit được truyền bởi Alice mà bị Eve phát hiện sai khi sử dụng phát hiện ngưỡng tối ưu $d_E = 0$. Để có được $I(A;E)$, luận văn xem xét hai tình huống điển hình về vị trí của Eve, như được mô tả trong hình 3.1: Eve là một HAP trái phép hoặc Eve là một phương tiện trên mặt đất. Cả hai kịch bản đều thuộc loại tấn công máy thu trái phép (URA).

Kịch bản 1: Trong trường hợp này, tín hiệu nhận được bởi HAP trái phép không bị ảnh hưởng bởi nhiễu loạn khí quyển. Kết quả là $P_{A,E}(0,1)$ và $P_{A,E}(1,0)$ được tính như (3.30) và (3.31)::

$$P_{A,E}(0,1) = \frac{1}{2} Q\left(\frac{d_E + \frac{1}{4} P_r^{(E)} \delta}{\sigma_N^{(E)}}\right) \tag{3.30}$$

$$P_{A,E}(1,0) = \frac{1}{2} Q\left(\frac{\frac{1}{4} P_r^{(E)} \delta - d_E}{\sigma_N^{(E)}}\right) \tag{3.31}$$

trong đó $P_r^{(E)} = \frac{1}{FSL} \Re^{(E)} M^{(E)} P G_{TX}^{(S)} h_p^{(P)}(r; a^{(P)}) G_{RX}^{(E)}$ là công suất thu cực đại tại Eve, $\Re^{(E)} = \frac{\eta^{(E)} q}{h\nu}$ là mức độ phản hồi APD của Eve với $\eta^{(E)}$ là hiệu suất lượng tử và $M^{(E)}$ là độ lợi trung bình APD của Eve. $G_{RX}^{(E)}$ là độ lợi thấu kính của Eve. $\sigma_N^{2(E)}$ là phương sai nhiễu và được định nghĩa theo (3.32):

$$\sigma_N^{2(E)} = 2q\Re^{(E)} M^{2(E)} F_A \left(\frac{1}{4} P_r^{(E)} \delta + P_r^{(E)} G_{RX}^{(E)}\right) \triangle f + \frac{4 k_B T F_n}{R_L} \triangle f \tag{3.32}$$

Kịch bản 2: Trong trường hợp này, Eve nằm gần Bob, $P_{A,E}(0,1)$ và $P_{A,E}(1,0)$ có thể được biểu thị bằng (3.33), (3.34):

$$P_{A,E}(0,1) = \frac{1}{2} \int_0^\infty Q\left(\frac{d_E + \frac{1}{4} P_r^{(E)} \delta h_a}{\sigma_N^{(E)}}\right) f_{h_a}(h_a) dh_a \tag{3.33}$$

$$P_{A,E}(1,0) = \frac{1}{2} \int_0^\infty Q\left(\frac{\frac{1}{4} P_r^{(E)} \delta h_a - d_E}{\sigma_N^{(E)}}\right) f_{h_a}(h_a) dh_a \tag{3.34}$$

trong đó $P_r^{(E)}$ được xác định như sau:

$$P_r^{(E)} = \frac{1}{FSL} P G_{TX}^{(S)} h_p^{(P)} G_{RX}^{(P)} G_A G_{TX}^{(P)} h_p^{(G)}(r; a^{(E)}) G_{RX}^{(E)} h_l \tag{3.35}$$

$\sigma_N^{(E)}$ trong trường hợp này có thể được xác định theo (3.36):

$$\sigma_N^{2(E)} = 2q\Re^{(E)}M^{(E)}F_A\left(\begin{array}{l}\frac{1}{4}P_r^{(G)}\delta h_a + P_b^{(P)}G_{RX}^{(P)}G_A G_{TX}^{(P)}h_p^{(G)}(r;a^{(E)})G_{RX}^{(E)}h_l h_a \\ +P_b^{(P)}G_{RX}^{(P)} + P_a G_{TX}^{(P)}h_p^{(G)}(r;a^{(E)})G_{RX}^{(E)}h_l h_a\end{array}\right)\triangle f + \frac{4k_B T F_n}{R_L}\triangle f \quad (3.36)$$

3.4 Kết quả phân tích hiệu năng và bàn luận

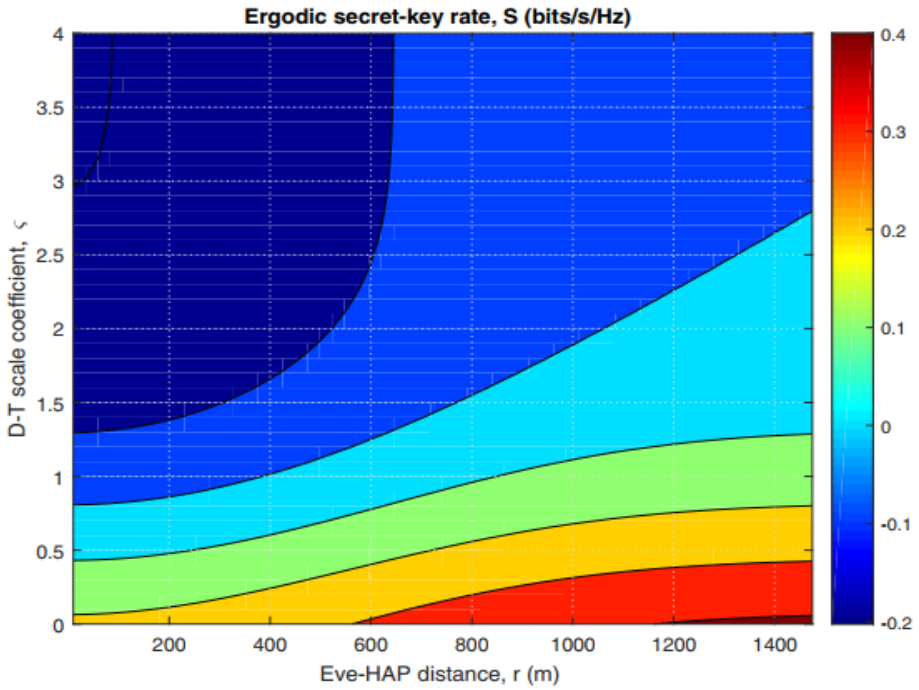
Trong phần này, luận văn phân tích hiệu năng của hệ thống được đề xuất qua tham số tốc độ khóa bí mật sai khi bị tấn công bởi người nhận trái phép. Luận văn sử dụng các thông số hệ thống như trong Bảng 3.1. Để xác nhận thiết kế, tốc độ khóa bí mật được khảo sát hai kịch bản tấn công như trong phân tích: (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).

Bảng 3.1: Các tham số của hệ thống

Tham số	Ký hiệu	Giá trị
Kênh FSO [27], [28]		
Tốc độ gió	ω	21 m/s
Phương sai của nhiễu		
Vệ tinh -> HAP	$\sigma_{b(P)}^2$	$4.435\times10^{-28}A^2/Hz$
Vệ tinh -> trạm mặt đất	$\sigma_{b(SG)}^2$	$7.7\times10^{-27}A^2/Hz$
HAP -> trạm mặt đất	$\sigma_{b(G)}^2$	$1.445\times10^{-25}A^2/Hz$
Hệ số suy hao	σ	$0.4km^{-1}$
Băng tần quang	B_0	125 GHz
Vệ tinh LEO (Alice) [29]		
Bước sóng	λ	1550 nm
Độ cao vệ tinh LEO	H_S	610 km
Góc thiên đỉnh	$\zeta_{(S)}$	50^o
Độ lợi thấu kính phát	G_{TX}^S	132 dB
Tốc độ bit	B	1 Gbps
Nút chuyển tiếp (HAP)		
Bước sóng	λ	1550 nm
Độ cao HAP	H_P	20 km
Góc thiên đỉnh	$\zeta_{(P)}$	50^o
Bán kính khẩu độ phát hiệu	$a^{(P)}$	0.05 m

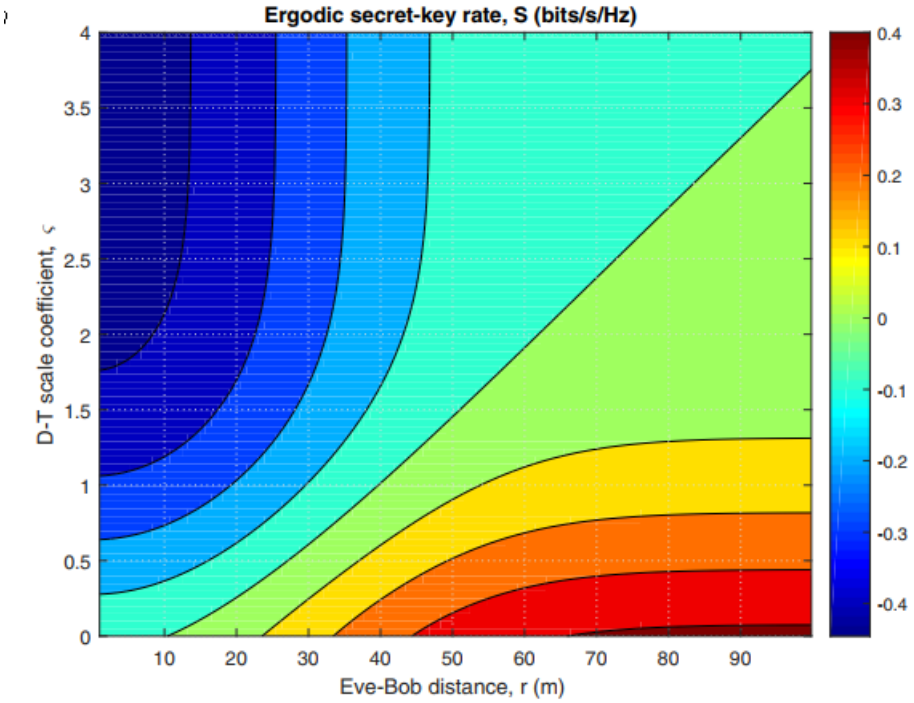
Tham số ASE	n_{sp}	5
Độ lợi thấu kính phát	$G_{TX}^{(P)}$	60 dB
Độ lợi thấu kính thu	$G_{RX}^{(P)}$	100 dB
Tốc độ bit	B	1 Gbps
Bob (Phương tiện hoặc UAV)		
Bán kính khẩu độ phát hiện	$a^{(G)}$	0.31 m
Độ lợi thấu kính thu	$G_{RX}^{(G)}$	121 dB
Hiệu suất lượng tử	η	0.62
Tỉ lệ hệ số i-on hoá	k_A	0.7
Hệ số nhiễu của bộ khuếch đại	F_n	2
Hệ số nhân thác	M	10
Điện trở	R_L	1000 Ω
Nhiệt độ	T	300 K
Eve (HAP hoặc phương tiện)		
Hiệu suất lượng tử	$\eta^{(E)}$	0.62
Hệ số nhân thác	$M^{(E)}$	10
Độ lợi thấu kính thu (Tình huống 1)	$G_{RX}^{(E)}$	204 dB
Độ lợi thấu kính thu (Tình huống 2)	$G_{RX}^{(E)}$	121 dB

Hình 3.3 và 3.4 cho thấy tốc độ khóa bí mật (*S*) so với khoảng cách giữa Eve và HAP ((Kịch bản 1) giữa Eve và Bob (Kịch bản 2) khi hệ số tỉ lệ DT có thể được điều chỉnh bởi Bob. Hệ số tỉ lệ DT xác định các mức ngưỡng như trong phương trình (3.24), giúp Bob ẩn đi tính ngẫu nhiên của các bit được phát hiện của Bob. Ở đây, luận văn sử dụng $P = 30dBm$, $\omega_z^{(P)} = 1475m$, $\omega_z^{(G)} = 50m$, và độ sâu IM δ = 0.4. Rõ ràng, tốc độ khóa bí mật tăng lên khi Eve ở xa HAP hoặc Bob. Điều này là do công suất quang thu được ở Eve giảm, do đó thông tin giữa Alice và Eve bị giảm.



Hình 3.3: Tốc độ khóa bí mật Ergodic (S) so với hệ số tỷ lệ DT (&) và khoảng cách của Eve từ HAP (r) trong kịch bản 1

Ngoài ra, với việc Bob điều chỉnh hệ số tỉ lệ DT Bob có thể nâng cao tính bảo mật với Alice. Ví dụ: khi Eve cách HAP gần 200m, Bob vẫn có thể đạt được tốc độ khóa bí mật 0,1 bit/giây/Hz nếu Bob đặt hệ số tỉ lệ δ = 0.5. Điều quan trọng cần lưu ý là, với tốc độ khóa này, hệ thống được đề xuất sử dụng hệ thống FSO tiêu chuẩn với tốc độ bit Gb/s vẫn có thể đảm bảo tốc độ tạo khóa đáng kể. Xét về khoảng cách xa với Eve, thì việc Eve tấn công đến vị trí của Bob sẽ khó hơn so với HAP, tức là Eve phải đến gần hơn nhiều để có được một số thông tin chung 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 = 1, 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.



Hình 3.4: Tốc độ khóa bí mật Ergodic (S) so với hệ số tỷ lệ DT (&) và khoảng cách của Eve từ Bob (UAV hoặc phương tiện) (r) trong kịch bản 2

3.5 Kết luận chương 3

Chương 3 luận văn đưa ra mô hình hệ thống QKD/FSO dựa trên vệ tinh sử dụng kỹ thuật chuyển tiếp tại HAP. Chương 3 đã phân tích từng thành phần hệ thống và nguyên lý hoạt động của hệ thống. 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 hai 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.

TÀI LIỆU THAM KHẢO

[1] A. I. Nurhadi and N. R. Syambas, “Quantum Key Distribution (QKD) Protocols: A Survey,” Proc. of the 4th International Conference on Wireless and Telematics (ICWT), Nusa Dua, 2018, pp. 1–5.

[2] C. H. Bennett and G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing,” Proc. of the IEEE International Conference on Computers, Systems,and Signal Processing, Bangalore, India, 1984, pp. 175–179.

[3] H. P. Yuen, “ Security of Quantum Key Distribution”, IEEE Access, vol. 4, pp. 724–749, 2016.

[4] P. V. Trinh and A. T. Pham, “Design and Secrecy Performance of Novel Two-way Free-space QKD Protocol using Standard FSO Systems,” IEEE International Conference on Communications (ICC), Paris, France, 2017,pp. 1–6.

[5] P. V. Trinh, T. V. Pham, N. T. Dang, H. V. Nguyen, S. X.Ng and A. T. Pham, “Design and Security Analysis of Quantum Key Distribution Protocol Over Free-Space Optics Using Dual-Threshold Direct-Detection Receiver,” IEEE Access, vol. 6, pp. 4159–4175, 2018.

[6] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S.Frick, and H Weinfurter, “Air-to-Ground Quantum Communication,” Nature Photonics, vol. 7, pp. 382–386,2013.

[7] R. Bedington, J. M. Arrazola, and A. Ling, “Progress in Satellite Quantum Key Distribution,” npj Quantum Information, vol. 3, no. 30, pp. 1–13, 2017.

[8] M. A. Khalighi and M. Uysal, “Survey on Free Space Optical Communication: A Communication Theory Perspective,” IEEE communications Surveys & Tutorials, vol. 16, no. 4, pp. 2231–2258, June 2014.

[9] M. Gabbi and S. Arnon, “Quantum key distribution by free space MIMO system,” IEEE/OSA J. Lightw. Technol., vol.24, no. 8, pp. 3114–3140, Aug. 2006.

[10] M. Safari and M. Uysal, “Relay-Assisted Quantum-Key Distribution Over Long Atmospheric Channels,” IEEE/OSA J. Lightw. Technol., vol. 27, no. 20, pp. 4508–4515, Oct.15, 2009.

[11]. Jacob Birkmann.”Towards Compact High-Altitude-Platform Based Quantum Key Distribution” 2019.

[12]. NIST, “Announcing the advanced encryption standard." Federal Information Processing Standards Publication, 197, 2001.

[13]. J. Katz and Y. Lindell, Introduction to modern cryptography. CRC press, 2014.

[14]. G. S. Vernam, “Secret signaling system." US PATENT US 1310719A, 1919.

[15]. D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, “Security of quantum key distribution with imperfect devices," in International Symposium on Information Theory, 2004. ISIT 2004. Proceedings., p. 136, IEEE, 2004.

[16]. A. Malik and P. Singh, “Free Space Optics: Current Applications and Future Challenges,” International Journal of Optics, vol. 2015, Article ID 945483, 7 pages, 2015.

[17]. H. Kaushal, V.K. Jain, S. Kar, Free Space Optical Communication, Springer, India, 2017

[18] Willebrand H. and Ghuman B.S., Free Space Optics: *Enabling optical connectivity in today’s network*, Indianapolis, IN, SAMS publishing, 2002.

[19] Ghassemlooy Z. and Popoola W. O., *Terrestrial Free-Space Optical Communications, Mobile and Wireless Communications Network Layer and Circuit Level Design*, Salma Ait Fares and Fumiyuki Adachi (Ed.), ISBN: 978-953-307-042-1, 2010.

[20] Al-Habash M. A., Andrews L. C., and Phillips R. L., “Mathematical model for the irradiance probability density function of a laser beam propagating through turbulent media,” *Optical Engineering*, vol. 40, no. 8, pp. 1554– 1562, Aug. 2001.

[21] F. Fidler et al., “Optical Communications for High-Altitude Platforms,” IEEE Journal of Selected Topics in Quantum Electronics, vol. 16, no. 5, pp. 1058–1070, Sept.-Oct. 2010.

[22] P. V. Trinh et: al, “Design and Security Analysis of Quantum Key Distribution Protocol over Free-Space Optics Using Dual-Threshold Direct-Detection Receiver”. IEEE Access, vol. 6, pp. 4159-4175, 2018.

[23]. B.E.A. Saleh and M.C. Teich, Fundamentals of Photonics. NewYork:Wiley, 1991.

[24]. Z. Ghassemlooy et al., “Free-Space Optical Communication Using Subearrier Modulation in Gamma-Gamma Atmospheric Turbulence,” 2007 9th ICTON, Rome, 2007, pp. 156–160.

[25]. Jing Ma, et al., “Performance analysis of satellite-to-ground downlink coherent optical communications with spatial diversity over GammaGamma atmospheric turbulence,” Appl. Opt., vol. 54, iss. 25, pp.7575–7585, Sept. 2015.

[26]. M. Abramowitz, I. A. Stegun, Handbook of mathematical functions, with formulas, graphs, and mathematical tables, 9th edition. New York, NY, USA: Dover, 1972.

[27]. S. R. Abdollahi et al. “An Optical Hard-Limiter for All-Optical Signal Processing,” 2017 UKSim-AMSS 19th Inter. Conference on Modelling & Simulation.

[28]. F. Fidler, Optical Communications from High Altitude Platforms (Dissertation), Inst. Commun. Radio-Frequency Eng., Vienna Univ. Technol., Austria, Sept. 2007. [Online].

[29]. F. Fidler, “Optical Backhaul Links between HAPs and Satellites in the Multi-Gigabit Regime,” 2008 IEEE Globecom Workshops, New Orleans, LO, 2008, pp. 1–5.