BỘ THÔNG TIN VÀ TRUYỀN THÔNG

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

PHAN THỊ THU HẰNG

NGHIÊN CỨU CẢI THIỆN HIỆU NĂNG TRUYỀN DẪN QUANG QUA KHÔNG GIAN TỰ DO TRONG HỆ THỐNG PHÂN PHỐI KHÓA LƯỢNG TỬ BIẾN LIÊN TỤC

Chuyên ngành: Kỹ thuật Viễn thông

Mã số: 9.52.02.08

TÓM TẮT LUẬN ÁN TIẾN SĨ KỸ THUẬT

Hà Nội - 2023

Công trình hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học:

PGS.TS. Đặng Thế Ngọc

PGS.TS. Lê Hải Châu

Phản biện 1: **GS.TS. Vũ Văn Yêm**

Phản biện 2: **PGS. TS. Lê Trung Thành**

Phản biện 3: **TS. Vũ Tuấn Lâm**

Luận án được bảo vệ trước hội đồng chấm luận án cấp Học viện họp tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

vào hồi: ngày tháng năm 2023 Có thể tìm hiểu luận án tại:

1. Thư viện Quốc gia Việt Nam

2. Thư viện Học viện Công nghệ Bưu chính Viễn thông

MỞ ĐẦU

Một trong những giải pháp khả thi để bảo mật Internet trong tương lai là sử dụng phân phối khóa lượng tử (Quantum Key Distribution – QKD) khi truyền tin. QKD là phương pháp phân phối khóa bí mật dựa trên vật lý lượng tử thay vì sử dụng độ phức tạp của các thuật toán trong toán học như các phương pháp phân phối khóa truyền thống [21, 70]. Dựa theo cách ánh xạ thông tin khóa cần truyền đi vào biến rời rạc hay biến liên tục, có hai loại QKD là QKD biến rời rạc (Discrete Variable – Quantum Key Distribution – DV-QKD) và QKD biến liên tục (Continuous Variable – Quantum Key Distribution – CV-QKD). CV-QKD có ưu điểm về khả năng tương thích với các hệ thống truyền thông quang đã có và tốc độ khóa cao. Ngoài ra, sử dụng vệ tinh để phân phối khóa lượng tử tới các trạm mặt đất thông qua kênh quang không gian tự do (Free Space Optics – FSO) là một giải pháp hứa hẹn tạo ra một mạng QKD có quy mô toàn cầu. Để có thể đáp ứng yêu cầu truyền khóa trong một khoảng cách dài, có tốc độ đủ lớn, tỷ lệ lỗi bit lượng tử đủ nhỏ đảm bảo cho quá trình sửa lỗi bên phía thu thì hệ thống truyền dẫn quang qua không gian tự do trong hệ thống phân phối khóa lượng tử biến liên tục cần vượt qua nhiều thách thức. Những thách thức này đến từ các yếu tố như kẻ nghe lén, nhiễu tại bên thu, ảnh hưởng của môi trường không gian tự do, đặc biệt là tác động của điều kiện khí quyển, bao gồm sự hấp thụ, tán xạ và nhiễu loạn khí quyển. Xuất phát từ nhu cầu này, nghiên cứu sinh đã quyết định lựa chọn đề tài "**Nghiên cứu cải thiện hiệu năng truyền dẫn quang qua không gian tự do trong hệ thống phân phối khóa lượng tử biến liên tục**" cho luận án của mình.

Mục tiêu chính mà luận án hướng tới là đề xuất và đánh giá tính khả thi của các giải pháp cải thiện hiệu năng truyền dẫn quang

qua không gian tự do trong hệ thống phân phối khóa lượng tử biến liên tục dưới ảnh hưởng của môi trường truyền dẫn (nhiễu loạn, suy hao, ..), nhiễu tại bên thu và sự có mặt của kẻ nghe lén.

Phạm vi nghiên cứu giới hạn với các hệ thống truyền khóa lượng tử biến liên tục qua không gian tự do trong đó giả thiết vệ tinh là nút tin cậy đóng vai trò tạo và phân phối khóa tới các trạm mặt đất. Hệ thống được nghiên cứu ở kịch bản đơn kênh và đa kênh. Nội dung nghiên cứu của luận án sẽ giới hạn trong bước 1 và bước 2 của giao thức phân phối khóa lượng tử, đó là truyền dẫn khóa lượng tử. Luận án sẽ nghiên cứu các giải pháp cải thiện hiệu năng truyền dẫn khóa thô trong giai đoạn đầu tiên của giao thức QKD, với mục tiêu đề xuất các hệ thống truyền dẫn khóa lượng tử giữa bên phát Alice và bên thu hợp lệ Bob có tỷ lệ lỗi bit lượng tử và xác suất chọn lọc đạt yêu cầu thiết kế. Các thủ tục xảy ra ở các bước tiếp theo của giao thức giả thiết không có sai sót và không ảnh hưởng tới tham số hiệu năng của hệ thống truyền dẫn khóa lượng tử.

Các tham số hiệu năng của hệ thống được đánh giá và khảo sát trong luận án này là tỷ lệ lỗi bit lượng tử (Quantum Bit Error Rate – QBER), xác suất chọn lọc P_{sift}, tốc độ khóa bí mật (Secret Key Rate – SKR), tỷ lệ mất khóa (Key Loss Rate – KLR) và tỷ lệ trễ vượt ngưỡng.

Bố cục của luận án bao gồm 4 Chương cùng với phần mở đầu, kết luận, phụ lục, danh mục các báo cáo khoa học đã được công bố của nghiên cứu sinh.

Chương 1: Tổng quan về truyền dẫn khóa lượng tử qua không gian tự do.

Chương 2: Hệ thống QKD-FSO biến liên tục dựa trên điều

chế pha.

Chương 3: Cải thiện hiệu năng hệ thống QKD-FSO sử dụng kỹ thuật truyền lại khóa và chuyển tiếp.

Chương 4: Hệ thống QKD-FSO đa kênh đa người sử dụng.

CHƯƠNG 1. TỔNG QUAN VỀ TRUYỀN DẪN KHÓA LƯỢNG TỬ QUA KHÔNG GIAN TỰ DO

1.2. Hệ thống phân phối khóa lượng tử QKD

1.2.1. Sự cần thiết của hệ thống phân phối khóa lượng tử QKD

Với sự ra đời của các máy tính lượng tử với tốc độ xử lý lớn gấp nhiều lần các máy tính hiện nay, nếu một hệ thống bảo mật chỉ dựa vào tính phức tạp của các thuật toán thì hoàn toàn có thể bị phá khóa. Để giải quyết vấn đề về kênh an toàn khi truyền khóa, có thể thực hiện bảo mật ngay tại tầng vật lý bằng cách phân phối khóa lượng tử QKD. QKD có những ưu điểm đáp ứng được nhu cầu bảo mật của các hệ thống truyền tin trong tương lai: (1) QKD không cho phép kẻ xâm nhập trái phép trên đường truyền khóa lấy được các tín hiệu lượng tử được truyền đi nhờ vào nguyên tắc không nhân bản của cơ chế lượng tử và (2) bên phát hoặc bên thu của hệ thống QKD hoàn toàn có thể phát hiện được sự can thiệp của kẻ xâm nhập trái phép.

1.2.3. Phân loại hệ thống QKD

1.2.3.2 QKD biến liên tục CV-QKD

Trong các hệ thống CV-QKD, các thông tin được mã hóa vào biên độ và/hoặc pha của xung ánh sáng yếu đã được điều chế hoặc sóng mang RF/quang, … đó là các biến liên tục của các trạng thái kết hợp [23]. So sánh với DV-QKD thì CD-QKD có ưu điểm: tốc độ truyền khóa cao, việc sử dụng máy thu kiểu heterodyne và homodyne đều đem lại hiệu quả và tiết kiệm chi phí, tương thích với các kênh truyền quang không dây [46].

1.2.4. Giao thức BB84

Quá trình tạo khóa chọn lọc trong giao thức BB84 có bốn bước. Bước thứ nhất và thứ hai nằm trong giai đoạn đầu tiên là truyền thông lượng tử của hệ thống QKD. Bước thứ ba và thứ tư thuộc giai đoạn thứ hai, giai đoạn có sử dụng kênh riêng có xác thực để chia sẻ các thông tin về chọn và tạo khóa bí mật.

1.5. Hệ thống phân phối khóa lượng tử biến liên tục sử dụng vệ tinh

Có thể đường truyền quang không dây để phân phối khóa bí mật trong hệ thống CV-QKD giữa phía phát và phía thu. Việc sử dụng vệ tinh làm phương tiện chuyển tiếp là một giải pháp để tăng cự ly truyền dẫn đạt được xa. Ngoài lợi thế về khoảng cách đường truyền giữa trạm phát và trạm thu được kéo dài, hệ thống phân phối khóa lượng tử qua kênh truyền quang không dây có sử dụng vệ tinh còn có lợi thế về khả năng an ninh. Hình thức tấn công người ở giữa rất khó thực hiện đối với hệ thống QKD-FSO dựa trên vệ tinh. Tuy nhiên, một đường truyền FSO phải đối mặt với một số ảnh hưởng đến từ môi trường không gian tự do, nhiễu bên phía thu,.. những ảnh hưởng này làm hạn chế đáng kể tới tốc độ truyền khóa tối đa đạt được, cũng như làm giảm khoảng cách đường truyền từ phía phát tới phía thu của một hệ thống QKD-FSO sử dụng vệ tinh.

1.6. Các tham số đánh giá hiệu năng của hệ thống QKD-FSO

Tỷ lệ lỗi bit lượng tử (Quantum Bit Error Ratio – QBER)

QBER được biểu diễn như sau [29]:

$$\mathrm{Q_{BER}} = \frac{P_{error}}{P_{sift}} \tag{1.1}$$

Tốc độ khóa bí mật

Tốc độ khóa bí mật Ergodic, kí hiệu là S, cho biết mức độ bảo mật của hệ thống đề xuất.

$$S = I(A;B) - I(A;E) \quad (1.5)$$

Khoảng cách đường truyền giữa máy phát và máy thu

Trong hệ thống QKD-FSO, Alice được đặt trên vệ tinh và Bob nằm ở phía trạm mặt đất. Đường truyền giữa Alice và Bob trong hệ thống QKD-FSO là đường truyền trong tầm nhìn thẳng.

1.7. Các yếu tố ảnh hưởng tới hiệu năng truyền dẫn quang qua không gian tự do trong hệ thống phân phối khóa lượng tử biến liên tục.

Trong hệ thống QKD-FSO, hiệu quả làm việc của mỗi một phân hệ đều có thể ảnh hưởng đến hiệu năng toàn hệ thống. Các yếu tố gây ảnh hưởng tới hiệu năng truyền dẫn quang qua không gian tự do trong hệ thống phân phối khóa lượng tử biến liên tục bao gồm: nguồn quang, các bộ tách quang, giao thức QKD sử dụng, các kỹ thuật và cấu trúc sử dụng trong hệ thống QKD, kênh truyền FSO, phân hệ xử lý tín hiệu số.

1.8. Các công trình nghiên cứu liên quan đến đề tài luận án.

1.8.1. Các công trình nghiên cứu trong nước

Theo tìm hiểu của nghiên cứu sinh, ở Việt Nam, nghiên cứu về QKD được thực hiện ở mức độ tìm hiểu về giao thức BB84 và thực hiện mô phỏng mật mã lượng tử của giao thức này [1]. Các nghiên cứu về phân phối khóa lượng tử qua hệ thống thông tin quang nói chung

và hệ thống QKD qua không gian tự do nói riêng còn chưa được quan tâm nghiên cứu.

1.8.2. Các công trình nghiên cứu trên thế giới

Trong thập kỷ qua, trên thế giới đã có nhiều nghiên cứu dành cho việc thiết kế và triển khai các hệ thống QKD-FSO, tuy nhiên vẫn còn những thách thức trong việc thực hiện các hệ thống QKD không gian tự do đảm bảo hiệu năng và độ tin cậy cao. Các hướng nghiên cứu chính về hệ thống QKD-FSO bao gồm:

(1) Hệ thống QKD-FSO trên mặt đất (2) Hệ thống QKD-FSO dựa trên vệ tinh (3) Các nghiên cứu cải thiện hiệu năng hệ thống QKD-FSO (4) Nghiên cứu về hệ thống QKD đa kênh

1.9. Nhận xét về công trình nghiên cứu của các tác giả khác và hướng nghiên cứu của luận án

1.9.1 Nhận xét về công trình nghiên cứu của các tác giả khác

Dựa trên quá trình khảo sát và phân tích các nghiên cứu đã có, nghiên cứu sinh nhận thấy có một số vấn đề chưa được giải quyết, cụ thể như sau:

Tỷ lệ lỗi bit lượng tử của các hệ thống QKD-FSO đã được đề xuất và thử nghiệm còn khá cao, tốc độ truyền khóa còn thấp. Các cải thiện chủ yếu tập trung ở phần cứng của hệ thống và cải thiện hiệu năng cho các hệ thống QKD sử dụng giao thức DV-QKD là chủ yếu. Việc sử dụng một trong các kỹ thuật ghép kênh đã được khảo sát chưa đạt được sự cải thiện vượt trội về tốc độ truyền khóa bí mật của các hệ thống QKD đa kênh. Phần lớn các công trình nghiên cứu chỉ hỗ trợ truyền dẫn khóa cho một người dùng, các hệ thống truyền dẫn khóa lượng tử đa người dùng chưa được quan tâm nghiên cứu.

1.9.2. Hướng nghiên cứu của luận án

Trên cơ sở kết quả phân tích các hạn chế của các nghiên cứu liên quan, các hướng nghiên được đề xuất trong luận án này bao gồm:

(1) Đề xuất phương thức truyền dẫn quang qua không gian tự do trong hệ thống phân phối khóa lượng tử biến liên tục dựa trên kỹ thuật điều chế QPSK vào sóng mang quang ở bên phát và sử dụng tách sóng kiểu heterodyne kết hợp cơ chế tách ngưỡng kép ở bên thu. **(2)** Nghiên cứu và đề xuất giải pháp cải thiện hiệu năng hệ thống truyền dẫn quang qua không gian tự do trong hệ thống phân phối khóa lượng tử biến liên tục sử dụng kỹ thuật truyền lại khóa ARQ kết hợp với chuyển tiếp dựa trên hạ tầng trên cao HAP. **(3)** Nghiên cứu và đề xuất giải pháp cải thiện tốc độ khóa trong hệ thống truyền dẫn quang qua không gian tự do trong hệ thống phân phối khóa lượng tử biến liên tục đa kênh sử dụng kỹ thuật ghép kênh phân chia theo bước sóng quang WDM và ghép kênh sóng mang phụ SCM. Hỗ trợ đa người sử dụng trong hệ thống QKD-FSO với kỹ thuật đa truy nhập phân chia theo mã quang.

CHƯƠNG 2. HỆ THỐNG QKD-FSO BIẾN LIÊN TỤC DỰA TRÊN ĐIỀU CHẾ PHA

2.1. Mô hình kênh truyền FSO

Luận án sẽ xem xét việc biểu diễn toán học cho một kênh truyền FSO xác định, bao gồm bốn thành phần: Suy hao trong không gian tự do (L_{FS}), suy hao do khí quyển h_a, suy hao do sự trải rộng chùm tia h_l và ảnh hưởng của pha-đinh do nhiễu loạn khí quyển h_f.

2.2. Hệ thống QKD-FSO biến liên tục dựa trên điều chế pha

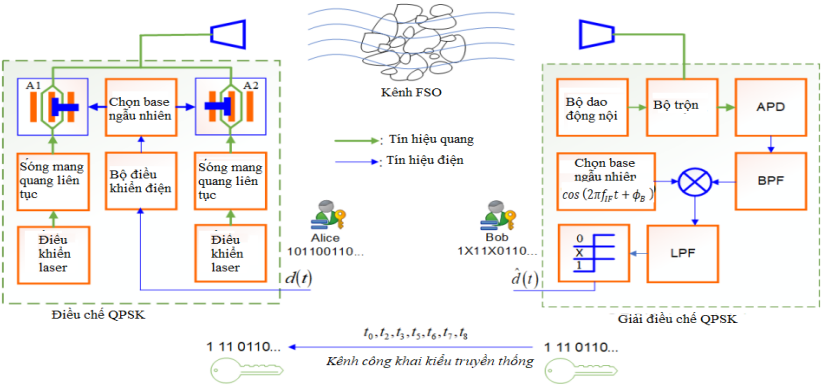
2.2.1. Mã hóa bit lượng tử sử dụng điều chế pha cầu phương QPSK

Phương thức luận án dựa trên điều chế pha kiểu QPSK ở bên phát và cơ chế tách ngưỡng kép ở bên thu và được phát triển dựa trên các bước thực hiện trong một giao thức BB84 truyền thống [10].

2.2.2. Mô hình hệ thống đề xuất

Giả sử rằng bên phát Alice ở vệ tinh và bên thu Bob ở mặt đất. Bên phát và bên thu sẽ được kết nối với nhau thông qua kênh truyền không gian tự do.

Hình 2. 3. Sơ đồ khối hệ thống QKD-FSO dựa trên vệ tinh sử dụng giao thức CV- QKD có kiểu điều chế QPSK ở phía phát kết hợp phía thu sử dụng tách sóng kiểu heterodyne và bộ tách ngưỡng kép.



Tại phía phát, dòng dữ liệu nhị phân d(t) sẽ được đưa vào bộ điều khiển để tạo ra các xung điều khiển điện với biên độ phù hợp với bộ điều chế Mach-Zehnder nhằm tạo ra các trạng thái pha tương ứng với sóng mang quang. Bộ chọn base sẽ chọn ngẫu nhiên một trong hai bộ điều chế MZM tương đương với base A_1 và A_2 để mã hóa dữ liệu nhị phân vào sóng mang quang được tạo ra từ đi-ốt laser. Ở bên thu, hai base dùng để giải mã của Bob được chọn ngẫu nhiên bằng cách thiết lập pha của tín hiệu tham chiếu và một bộ tách sóng dựa trên cơ

chế ngưỡng kép được sử dụng để quyết định giá trị bit thu được là "1", "0" hay "X".

2.2.3. Phân tích hiệu năng hệ thống

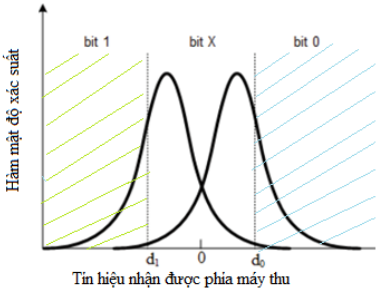
Dòng điện sau giải mã được tính toán theo công thức:

$$I_{decod}(t) = M_A\Re\sqrt{P_R P_{LO}}\cos[4\pi f_{IF}t + \phi_A + \phi_B] + M_A\Re\sqrt{P_R P_{LO}}\cos[\phi_A - \phi_B] + i_n \quad (2.22)$$

Dòng điện tại đầu vào của bộ tách ngưỡng kép có thể biểu thị theo công thức:

$$I = M_A\Re\sqrt{P_R P_{LO}}\cos[\phi_A - \phi_B] + i_n \quad (2.23)$$

Trong trường hợp lý tưởng không có sự ảnh hưởng của nhiễu, I nhận một trong ba giá trị là I_0, 0, và I_1 tùy theo giá trị của ϕ_A và ϕ_B như trong Bảng 2.1. Do ảnh hưởng của nhiễu, I bị thay đổi và hàm mật độ xác suất PDF của I được vẽ ở Hình 2.4, hai đỉnh của phân bố dòng điện tương đương với bit "0" và bit "1" của Alice.



Hình 2. 4. Hàm phân bố mật độ xác suất của tín hiệu Bob nhận được với d_o và d_1 là hai giá trị ngưỡng của bộ tách ngưỡng kép.

Hai ngưỡng d_1 và d_0 được sử dụng để quyết định bit "0", "X" và bit "1". Luật của bộ quyết định ngưỡng như sau:

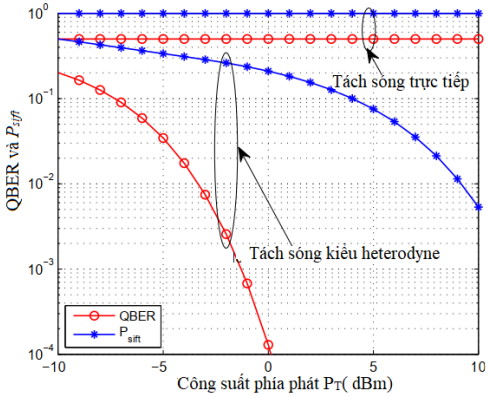
$$\text{Giá trị bit} = \begin{cases} 1 \text{ nếu } I \leq d_1 \\ 0 \text{ nếu } I \geq d_0 \\ X \quad \text{trong trường hợp còn lại} \end{cases} \tag{2.1}$$

với "X" tương đương với trường hợp không có bit được tạo ra.

2.2.4. Kết quả khảo sát hiệu năng hệ thống

Mục tiêu của đề xuất là hệ thống phân phối khóa lượng tử biến liên tục qua không gian tự do có các tham số hiệu năng $P_{sift} \geq 10^{-2}$ và QBER$\leq 10^{-3}$.

Luận án khảo sát giá trị của QBER và P_{sift} để đánh giá tính khả thi của hệ thống QKD-FSO biến liên tục dựa trên vệ tinh sử dụng phương thức truyền dẫn quang đề xuất dựa trên kỹ thuật điều chế QPSK ở phía phát và cơ chế tách ngưỡng kép ở phía thu.



Hình 2. 6. Giá trị QBER và P_{sift} tại phía thu Bob phụ thuộc vào công suất phía phát khi ρ= 1,5

Qua kết quả khảo sát Hình 2.6 , có thể xác định được khoảng giá trị của công suất máy phát để cho cả QBER và P_{sift} thỏa mãn điều kiện yêu cầu $P_{sift} \geq 10^{-2}$ và QBER $\leq 10^{-3}$. Khoảng giá trị này được khuyến nghị từ -1,25 dBm tới 8dBm. Hình 2.6 cũng chỉ ra ưu điểm

của máy thu sử dụng tách sóng kiểu heterodyne so với máy thu tách sóng trực tiếp khi máy thu sử dụng tách sóng kiểu heterodyne đạt được giá trị QBER thấp hơn.

Kết luận Chương 2

Nội dung Chương 2 đã trình bày về mô hình toán học của kênh FSO khi kể đến các yếu tố suy hao và ảnh hưởng của pha-đinh do nhiễu loạn khí quyển. Đóng góp thứ nhất với đề xuất phương thức truyền dẫn quang qua không gian tự do trong hệ thống phân phối khóa lượng tử CV-QKD bao gồm phương pháp điều chế pha kiểu QPSK ở bên phát và máy thu sử dụng tách sóng kiểu heterodyne kết hợp cơ chế tách ngưỡng kép. Đóng góp thứ hai là xây dựng mô hình giải tích để tính toán các tham số hiệu năng QBER và P_{sift}. Mô hình giải tích mà luận án xây dựng ở chương này dùng để tính toán trong trường hợp hệ thống QKD-FSO với khả năng xuất hiện của ba bit là "1", "0" và "X" thay vì các hệ thống thông thường chỉ sử dụng hai bit là bit "0" và bit "1".

Phương thức truyền dẫn quang đề xuất ở Chương 2 có thể được sử dụng trong các hệ thống QKD-FSO dựa trên vệ tinh để tăng khoảng cách truyền dẫn từ phía phát tới phía thu, đáp ứng được cho hệ thống QKD có quy mô toàn cầu.

CHƯƠNG 3. CẢI THIỆN HIỆU NĂNG HỆ THỐNG QKD-FSO SỬ DỤNG KỸ THUẬT TRUYỀN LẠI KHÓA VÀ CHUYỂN TIẾP

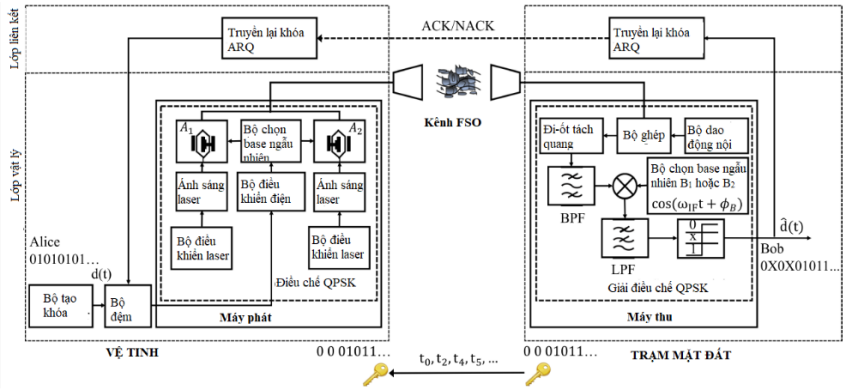
3.2. Hệ thống phân phối khóa lượng tử biến liên tục dựa trên vệ tinh sử dụng kỹ thuật truyền lại khóa kiểu ARQ

3.2.1. Mô hình hệ thống đề xuất

Hình 3.1 mô tả hệ thống CV-QKD dựa trên vệ tinh sử dụng: (1)

kỹ thuật điều chế QPSK ở bên phát (2) máy thu sử dụng bộ tách sóng kiểu heterodyne kết hợp cơ chế tách ngưỡng kép (3) kỹ thuật ARQ tại vệ tinh. Hệ thống đề xuất có hai chức năng chính là: (1) truyền khóa bí mật thông qua kênh FSO và (2) thực hiện thủ tục truyền lại khóa để cải thiện hiệu năng của cả hệ thống.

Giao thức QKD sử dụng là QKD dựa trên điều chế pha kiểu QPSK và cơ chế tách ngưỡng kép ở phía thu. Do sự xuất hiện của các yếu tố không mong muốn trên kênh truyền và có thể có sự có mặt của kẻ nghe lén nên các khóa chọn lọc có thể có lỗi, mô hình đề xuất của luận án sử dụng kỹ thuật phát lại tự động ARQ.



Hình 3. 1. Sơ đồ khối hệ thống CV-QKD dựa trên vệ tinh sử dụng kỹ thuật truyền lại khóa kiểu ARQ.

3.2.4. Phân tích hiệu năng hệ thống

Chuỗi Markov hai trạng thái được đề xuất để mô tả sự chuyển đổi trạng thái của kênh lượng tử. Trong mô hình trạng thái kênh lượng tử đề xuất, khoảng thời gian được chia thành các khe, một khe thời gian tương đương với khoảng thời gian truyền đi một chuỗi bit. Đường truyền sẽ chuyển đổi giữa các trạng thái xấu (B) và tốt (G). Quá trình

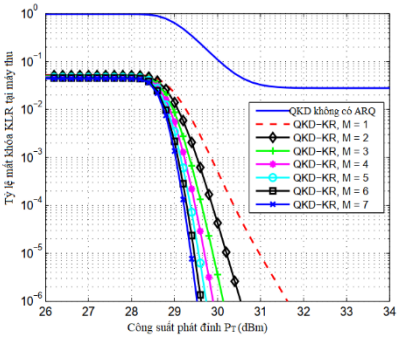
Bernoulli tĩnh được dùng để mô hình hóa quá trình đến bộ đệm của chuỗi bit.

Tỷ lệ mất khóa (Key Loss Rate - KLR) do nguyên nhân các lần truyền lại đều không thành công cũng như do bộ nhớ đệm của Alice bị tràn được mô tả bằng công thức sau:

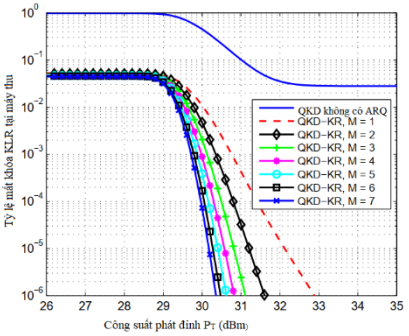
$$\mathrm{KLR} = \sum_{n_L=0}^{C-1} \pi(n_L, B, M) + \sum_{s_L \in [B,G]} \sum_{m_L=0}^{M} \pi(C, s_L, m_L) \quad (3.10)$$

3.2.5. Kết quả khảo sát hiệu năng hệ thống

Kết quả khảo sát hiệu năng hệ thống đánh giá thông qua tham số tỷ lệ mất khóa KLR ở phía máy thu với các điều kiện khác nhau của hệ thống bao gồm công suất đỉnh phía phát P_T, số lần tối đa được phép truyền lại một chuỗi bit, điều kiện nhiễu loạn khí quyển yếu và mạnh.



Hình 3. 8 Tỷ lệ mất khóa KLR tại máy thu phụ thuộc vào công suất đỉnh phía phát P_T trong điều kiện nhiễu loạn khí quyển yếu, P_{LO}= 0 dBm và hệ số tỷ lệ ngưỡng kép ρ=0,7



Hình 3. 9. Tỷ lệ mất khóa KLR tại máy thu phụ thuộc vào công suất đỉnh phía phát P_T trong điều kiện nhiễu loạn khí quyển mạnh, P_{LO}= 0 dBm và hệ số tỷ lệ ngưỡng kép ρ=1,4

Giá trị KLR nhỏ nhất đạt được là 3×10^{-12} khi công suất phát đỉnh lớn. Giá trị của KLR sẽ giảm khi số lần phát lại tăng lên. Với một giá trị KLR cho trước, việc tăng số lần phát lại tối đa cho phép kéo theo sự giảm công suất phát yêu cầu.

3.2.6. Khả năng an ninh của hệ thống đề xuất

Luận án hướng tới mục tiêu thiết kế hệ thống phân phối khóa lượng tử qua không gian tự do nhằm hạn chế khả năng thu đúng và giảm xác suất chọn lọc (xác suất phát hiện được bit) của kẻ nghe lén.

Xác suất Eve có thể thu chính xác chuỗi khóa thô có độ dài N theo công thức:

$$P_{Eve} = [P_{sift} \times (1 - \mathrm{QBER_{Eve}})]^N \quad (3.11)$$

Từ công thức (3.11) và theo kết quả khảo sát tại Hình 3.7 của luận án, xác suất Eve P_{Eve} thu được chính xác toàn bộ chuỗi bit khóa thô có độ dài $N = 128$ bit như sau:

Bảng 3. 1. Xác suất Eve thu chính xác toàn bộ chuỗi bit của khóa thô có chiều dài N=128 bit

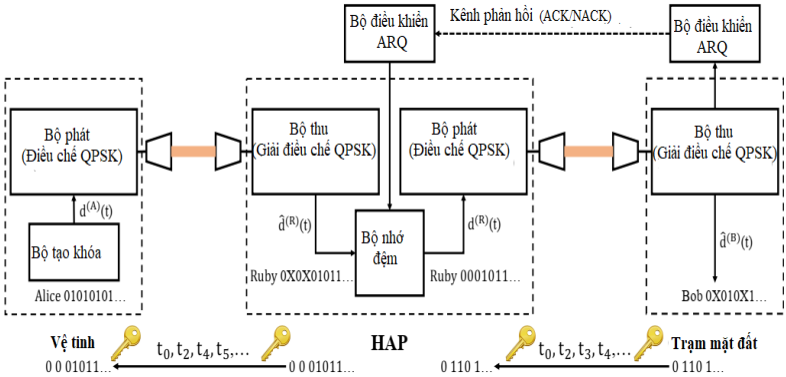
Khoảng cách Eve-Bob	***L* = 15 m**	***L* = 50 m**
Nhiễu loạn yếu	$P_{sift} = 0{,}25$ $\mathrm{QBER} = 2\times10^{-3}$ $P_{Eve} =$ **$2{,}3 \times 10^{-90}$**	$P_{sift} = 0{,}3$ $\mathrm{QBER} = 1{,}5\times10^{-1}$ $P_{Eve} =$ **1×10^{-76}**
Nhiễu loạn mạnh	$P_{sift} = 0{,}1$ $\mathrm{QBER} = 2\times10^{-3}$ $P_{Eve} =$ **$6{,}8 \times 10^{-129}$**	$P_{sift} = 0{,}09$ $\mathrm{QBER} = 1\times10^{-1}$ $P_{Eve} =$ **$1{,}9 \times 10^{-140}$**

Kết quả trên cho thấy, xác suất Eve có thể thu chính xác chuỗi khóa là rất nhỏ, đủ đảm bảo khả jnăng an toàn của hệ thống đề xuất

khi bị tấn công với hình thức thu lén. Đặc biệt với chiều dài khóa tăng lên 256 bit, 512 bit hoặc lớn hơn, xác suất này càng giảm mạnh.

3.3. Hệ thống QKD-FSO sử dụng kỹ thuật truyền lại khóa và chuyển tiếp

3.3.1. Mô hình hệ thống đề xuất



Hình 3. 11. Sơ đồ khối hệ thống QKD-FSO dựa trên vệ tinh sử dụng kỹ thuật chuyển tiếp dựa trên HAP và kỹ thuật phát lại khóa ARQ.

3.3.3. Phân tích hiệu năng hệ thống

Các tham số hiệu năng được xem xét và đánh giá bao gồm tỷ lệ mất khóa KLR và tỷ lệ trễ vượt ngưỡng.

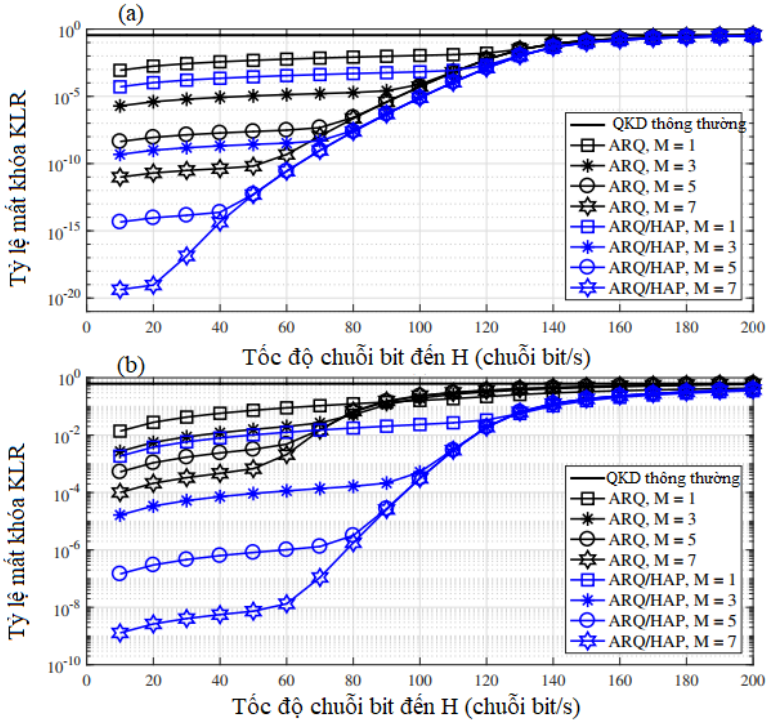
Xác suất trễ hàng đợi vượt quá $\frac{\mathcal{D}}{\tau_{bs}}$ khe thời gian có thể tính theo công thức:

$$\Pr\left\{t_Q > \frac{\mathcal{D}}{\tau_{bs}}\right\} = Pr\left\{t_Q > \frac{\mathcal{D}}{\tau_{bs}} \mid (q_D, s_L, m_L)\right\} Pr\{(q_D, s_L, m_L)\}$$
$$= \frac{1}{\pi_v}\left[\sum_{s_L\in\{B,G\}} Pr\left\{t_Q > \frac{\mathcal{D}}{\tau_{bs}} \mid (0, s_L, 0)\right\}\pi(0, s_L, 0) + \right.$$
$$\left.\sum_{q_D=2}^{C}\sum_{s_L\in[B,G]}\sum_{m_L=0}^{M} Pr\left\{t_Q > \frac{\mathcal{D}}{\tau_{bs}} \mid (q_D - 1, s_L, m_L)\right\}.\pi\,(q_D - 1, s_L, m_L)\right] \quad (3.25)$$

3.3.4. Kết quả khảo sát hiệu năng hệ thống

A. Tỷ lệ mất khóa

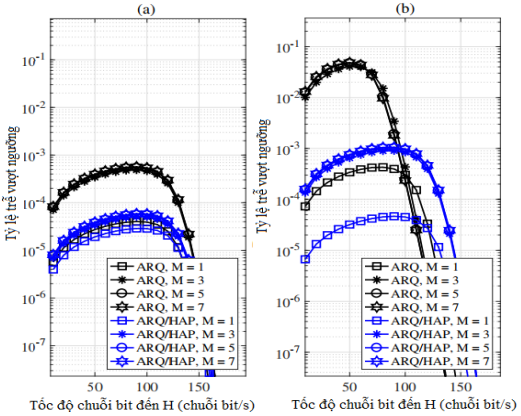
Việc sử dụng cả kỹ thuật ARQ và kỹ thuật chuyển tiếp chỉ cải thiện tỷ lệ mất khóa KLR trong trường hợp tỷ lệ chuỗi bit đến là nhỏ. Khi tỷ lệ chuỗi bit đến đạt đến một giá trị xác định, việc sử dụng kết hợp cả kỹ thuật ARQ và kỹ thuật chuyển tiếp không mang lại hiệu quả vì xác suất bộ nhớ đệm của Ruby đầy sẽ tăng lên. Việc sử dụng kết hợp cả hai kỹ thuật ARQ và chuyển tiếp được khuyến nghị khi tỷ lệ chuỗi bit đến là H<180 cho cả hai điều kiện nhiễu loạn khí quyển là yếu và mạnh.



Hình 3. 12. Tỷ lệ mất khóa KLR theo tốc độ chuỗi bit đến H với điều kiện nhiễu loạn khí quyển yếu (a) và mạnh (b), kích thước bộ nhớ đệm C= 10 chuỗi bit.

B. Tỷ lệ trễ vượt ngưỡng

Tỷ lệ trễ vượt ngưỡng quan hệ với tỷ lệ chuỗi bit đến *H* trong các điều kiện nhiễu loạn khí quyển khác nhau được xem xét trong Hình 3.13.



Hình 3. 13. Tỷ lệ trễ vượt ngưỡng theo tốc độ chuỗi bit đến với điều kiện nhiễu loạn khí quyển yếu (a) và mạnh (b), kích thước bộ nhớ đệm C=10 chuỗi bit.

Dựa vào kết quả của khảo sát trong Hình 3.13, chúng ta có thể dễ dàng nhận thấy tỷ lệ trễ vượt ngưỡng trong trường hợp hệ thống sử dụng cả kỹ thuật ARQ và chuyển tiếp nhỏ hơn trong trường hợp hệ thống chỉ sử dụng kỹ thuật ARQ, đặc biệt trong điều kiện nhiễu loạn khí quyển mạnh

Kết luận Chương 3

Chương 3 đã đề xuất hệ thống phân phối khóa lượng tử QKD-FSO dựa trên vệ tinh sử dụng kỹ thuật truyền lại khóa theo phương pháp yêu cầu lặp lại tự động ARQ kết hợp với kỹ thuật chuyển tiếp dựa trên hạ tầng trên cao HAP và mô hình chuỗi Markov hai trạng thái dùng cho việc phân tích một cách toàn diện cho hai chỉ số hiệu suất quan trọng là tỷ lệ mất khóa KLR và tỷ lệ trễ vượt ngưỡng cho hệ

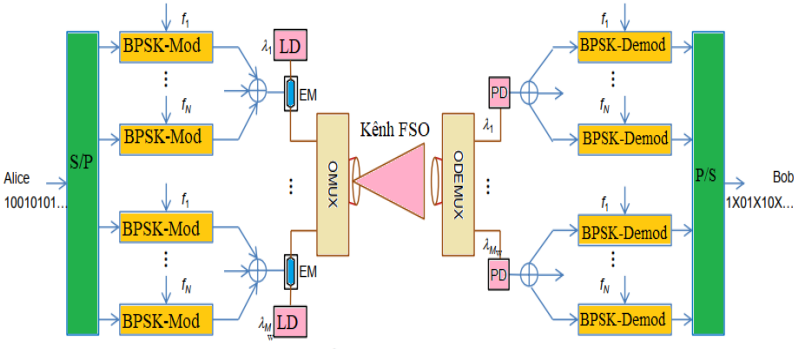
thống đề xuất. Nội dung của Chương 3 đã đưa ra hai kịch bản để khảo sát, đánh giá hiệu năng của hệ thống đề xuất nhằm kết luận về tính khả thi của hệ thống đã đề xuất.

CHƯƠNG 4. HỆ THỐNG QKD-FSO ĐA KÊNH ĐA NGƯỜI SỬ DỤNG

4.2. Hệ thống QKD-FSO sử dụng kỹ thuật ghép kênh sóng mang phụ SCM và ghép kênh phân chia theo bước sóng WDM

4.2.1. Mô hình hệ thống đề xuất

Máy phát được đặt tại vệ tinh và máy thu đặt tại trạm mặt đất, máy phát và máy thu được kết nối với nhau qua kênh quang không gian tự do. Trong đề xuất này luận án sử dụng giao thức QKD biến liên tục dựa trên kỹ thuật điều chế sóng mang phụ sử dụng khóa dịch pha nhị phân BPSK và cơ chế tách ngưỡng kép ở phía thu.



Hình 4. 1. Mô hình hệ thống QKD đa kênh sử dụng SCM-WDM

4.2.3. Phân tích hiệu năng hệ thống

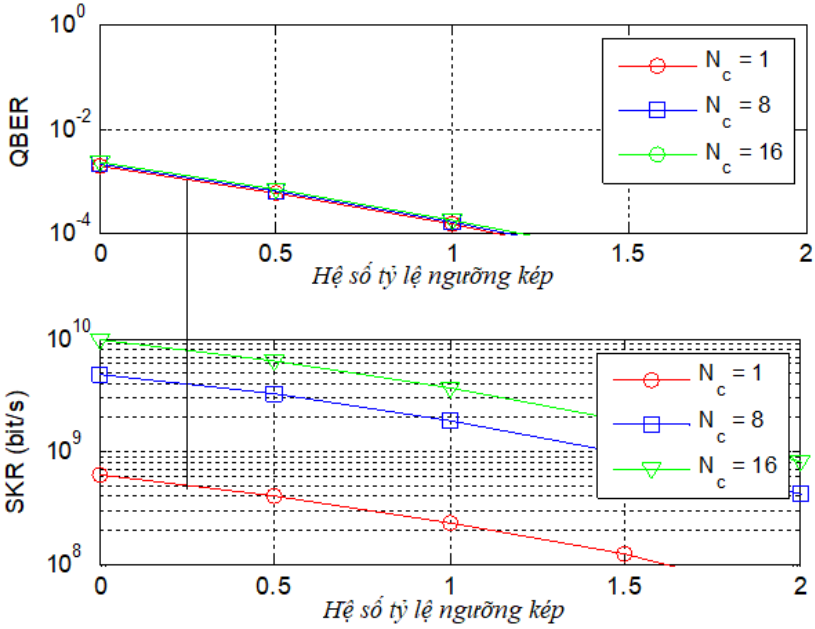
Luận án đề xuất thiết lập giá trị cho các ngưỡng d_0 và d_1 của bộ tách ngưỡng kép như sau:

$$d_0 = E[i_0] + \rho\sigma_n, \quad d_1 = E[i_1] - \rho\sigma_n \tag{4.10}$$

Giả thiết mã hóa sửa lỗi được sử dụng để đảm bảo không xảy ra lỗi trong chuỗi bit khóa chọn lọc, tốc độ khóa bí mật khi đó được định nghĩa như sau

$$SKR = R_b P_{sift} N_C \tag{4.12}$$

4.2.4. Kết quả khảo sát hiệu năng hệ thống



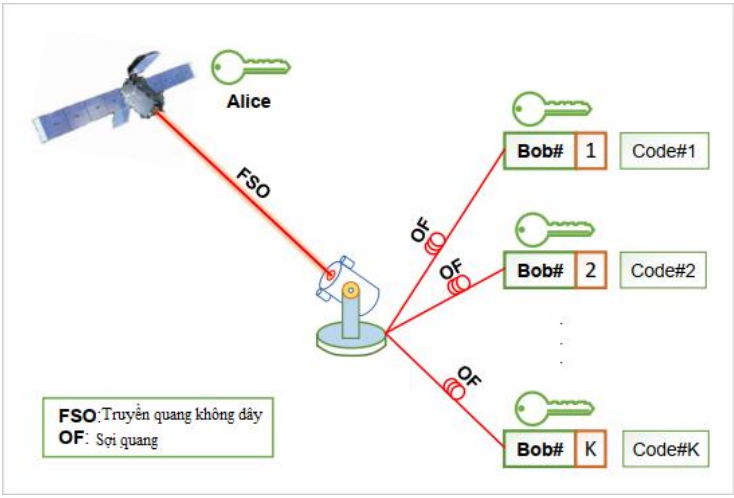
Hình 4. 4. QBER và SKR theo hệ số tỷ lệ ngưỡng kép trong trường hợp nhiễu loạn khí quyển yếu với R_b = 1,25 Gbit/s

Khả năng cải thiện SKR thông qua giải pháp QKD đa kênh được khảo sát trong Hình 4.4 với điều kiện nhiễu loạn yếu. Kết quả Hình 4.4 cũng cho thấy, tốc độ khóa cực đại trong trường hợp hệ thống QKD đơn kênh là 500 Mbit/s. Xét hệ thống QKD đa kênh với số lượng kênh

là 8 và 16, tốc độ khóa cực đại tương ứng là 4 Gbit/s và 8 Gbit/s. Tốc độ Gbit/s ở hệ thống QKD đa kênh cải thiện hơn rất nhiều so với hệ thống QKD đơn kênh và có thể đáp ứng được yêu cầu sử dụng các khóa có độ dài lớn nhằm đảm bảo tính bảo mật cao của thông tin được trao đổi qua mạng.

4.3. Hệ thống CV-QKD đa người sử dụng với kỹ thuật CDMA quang

4.3.1. Mô hình hệ thống đề xuất



Hình 4. 5. Mô hình hệ thống CV-QKD dựa trên vệ tinh sử dụng kỹ thuật phân chia theo mã

Các khóa được tạo ra ở vệ tinh và được phân phối tới các trạm mặt đất nhờ vào máy phát theo kiểu điều chế cường độ. Tại các trạm mặt đất, máy thu tách sóng kiểu trực tiếp với cơ chế tách ngưỡng kép được dùng để khôi phục các khóa.

Trong hệ thống CV-QKD sử dụng CDM, một chuỗi chip bao

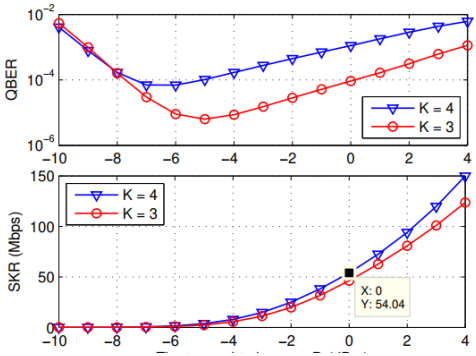
gồm các chip “0” và “1” được biểu diễn cho bit “1” và không có tín hiệu nào được truyền đi nếu bit được truyền có giá trị là “0”. Mỗi một bộ mã hóa CDM bao gồm ω dây trễ quang với thời gian trễ được thiết lập theo mã được gán cho kênh. ω là trọng lượng mã, đó chính là số lượng của chip “1” trong chuỗi mã. Các tín hiệu được mã hóa từ đầu ra của các bộ mã hóa CDM được tổng hợp lại và truyền qua tới máy thu qua kênh truyền FSO. Bộ giải mã CDM tại phía thu cũng được tạo thành từ các dây trễ quang. Tuy nhiên, thời gian trễ được thiết lập trong bộ giải mã sẽ phải đảm bảo cho ω các xung quang xuất hiện tại đầu ra của bộ giải mã cùng một thời điểm. Các xung quang từ các kênh không mong muốn với các thời gian trễ không phù hợp với bộ giải mã sẽ bị loại bỏ. Sau đó, quá trình chuyển đổi tín hiệu quang thành tín hiệu dòng điện xảy ra nhờ đi-ốt tách quang.

4.3.4. Phân tích hiệu năng hệ thống

Tốc độ khóa bí mật SKR được tính theo công thức:

$$SKR = K\, P_{sift} R_b \tag{4.27}$$

4.3.5. Kết quả khảo sát hiệu năng hệ thống



Hình 4. 8. QBER và SKR theo công suất phát khi hệ số tỷ lệ ngưỡng kép $\rho = 5$

Giá trị của SKR tăng cùng với giá trị công suất phát tăng. Hệ thống đề xuất có thể đạt được tốc độ truyền khóa bí mật trên 100 Mb/s, đồng thời với QBER ≤ 10^{-3} với giá trị công suất phát thích hợp.

Kết luận Chương 4

Nội dung Chương 4 đã trình bày 02 đóng góp của luận án trong việc đề xuất sử dụng kỹ thuật ghép kênh và hỗ trợ đa người dùng.

- Thứ nhất, kết hợp kỹ thuật ghép kênh sóng mang phụ và ghép kênh phân chia theo bước sóng nhằm cải thiện tốc độ truyền khóa bí mật của hệ thống CV-QKD từ vệ tinh

-Thứ hai, kỹ thuật đa truy nhập phân chia theo mã quang (Code Division Multiple Access – CDMA) với khả năng hỗ trợ đa người dùng kết hợp với việc cải thiện hiệu năng an ninh của hệ thống QKD-FSO. Tính khả thi của giải pháp đề xuất đã được đánh giá thông qua kết quả phân tích hiệu năng.

KẾT LUẬN

Nội dung luận án đã đạt được mục tiêu đề ra là nghiên cứu, tìm kiếm các giải pháp cải thiện hiệu năng truyền dẫn quang qua không gian tự do trong hệ thống truyền khóa lượng tử biến liên tục dưới ảnh hưởng của môi trường truyền dẫn (nhiễu loạn, suy hao, ..), nhiễu tại bên phát và bên thu, sự có mặt của kẻ nghe lén.

Các kết quả đóng góp mới về khoa học của luận án có thể phân thành ba nhóm như sau:

- Đề xuất phương thức truyền dẫn quang qua không gian tự do trong hệ thống truyền khóa lượng tử kiểu biến liên tục CV-QKD dựa trên điều chế pha.
- Đề xuất giải pháp cải thiện hiệu năng truyền dẫn quang qua không gian tự do trong hệ thống phân phối khóa lượng tử biến

liên tục sử dụng kỹ thuật truyền lại khóa và chuyển tiếp.

- Đề xuất các giải pháp truyền dẫn đa kênh đa người sử dụng cho hệ thống phân phối khóa lượng tử QKD-FSO đa kênh đa người sử dụng.

Hướng phát triển của luận án là sẽ tập trung vào việc xem xét, đánh giá mức độ an ninh của hệ thống QKD với các kiểu tấn công từ phía Eve cũng như các ảnh hưởng của quá trình báo hiệu và nghiên cứu đề xuất hệ thống và các giải pháp cải thiện hiệu năng trong một mạng QKD được định nghĩa bằng phần mềm.

CÁC CÔNG TRÌNH KHOA HỌC ĐÃ CÔNG BỐ

BÀI BÁO KHOA HỌC

[J1] Nam D. Nguyen, Hang T. T. Phan, Hien T. T. Pham, Vuong V. Mai, Ngoc T. Dang, "***Reliability improvement of satellite-based quantum key distribution systems using retransmission scheme***", *Photonic Network Communications*, vol. 42, no.1, Jun. 2021, page 27-39, doi:10.1007/s11107-021-00934-y.

[J2] Phan Thị Thu Hằng, Đặng Tiến Sỹ, Phạm Thị Thúy Hiền, Đặng Thế Ngọc, "***Hệ thống phân phối khóa lượng tử đa kênh từ vệ tinh sử dụng SCM-WDM***", *Tạp chí Nghiên cứu Khoa học và Công nghệ quân sự,* số 72, 04 – 2021, trang 35-43**.**

[J3] Phan Thị Thu Hằng, ***" Mô hình hóa kênh truyền quang không dây sử dụng vệ tinh khi xem xét các yếu tố ảnh hưởng tới hiệu năng kênh truyền",*** *Tạp chí Khoa học và Công nghệ,* số 58, 05-2022, trang 154-158.

[J4] Hang.T.T.Phan, Minh B. Vu, Hien T.T.Pham, Ngoc T. Dang, "***Satellite continuous-quantum key distribution systems using code-division multiple access"***, Optics Continuum, vol. 2, no. 2, pp. 289-302, Feb. 2023. DOI: 10.1364/OPTCON.4745092023.

HỘI NGHỊ KHOA HỌC

[C1] Nam D. Nguyen, Hang T. T. Phan, Hien T. T. Pham, Vuong V. Mai, and Ngoc T. Dang, "***Performance Enhancement of Satellite QKD-FSO systems using HAP-based Relaying and ARQ***", In the Proc. of *2020 International Conference on Advanced Technologies*

for Communications (ATC), Nha Trang, Vietnam, Oct. 2020, pp. 12-17, doi: 10.1109/ATC50776.2020.9255472.

[C2] Minh B. Vu, Hien T. T. Pham, Anh T. Do, Hang T. T. Phan, Ngoc T. Dang, "***Satellite-based Free-Space Quantum Key Distribution Systems using QPSK Modulation and Heterodyne Detection Receiver***", *2019 19th International Symposium on Communications and Information Technologies (ISCIT)*, Ho Chi Minh, Vietnam, Sep. 2019, pp. 265-270, doi: 10.1109/ISCIT.2019.8905206.