x

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

LUẬN ÁN TIẾN SĨ KỸ THUẬT

Hà Nội, 2023

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

LUẬN ÁN TIẾN SĨ KỸ THUẬT

NGƯỜI HƯỚNG DẪN KHOA HỌC:

1. PGS.TS. Đặng Thế Ngọc

2. PGS.TS. Lê Hải Châu

Hà Nội, 2023

LỜI CAM ĐOAN

Nghiên cứu sinh xin cam đoan đây là công trình nghiên cứu của chính mình. Các số liệu, kết quả trong luận án là trung thực và chưa từng được công bố trong bất cứ công trình của bất kỳ tác giả nào khác. Tất cả các kế thừa của các tác giả khác đã được trích dẫn.

Người cam đoan

Phan Thị Thu Hằng

LỜI CẢM ƠN

Trong quá trình nghiên cứu và hoàn thành luận án này, nghiên cứu sinh đã nhận được nhiều sự giúp đỡ và đóng góp quý báu.

Lời đầu tiên, nghiên cứu sinh xin được bày tỏ sự biết ơn sâu sắc tới các Thầy hướng dẫn, PGS.TS. Đặng Thế Ngọc và PGS.TS. Lê Hải Châu, đã định hướng và liên tục hướng dẫn nghiên cứu sinh thực hiện các nhiệm vụ nghiên cứu trong suốt quá trình thực hiện luận án. Đặc biệt, sự hướng dẫn tận tình và những ý kiến quý báu từ PGS.TS. Đặng Thế Ngọc đã giúp nghiên cứu sinh rất nhiều trong việc hoàn thiện luận án.

Nghiên cứu sinh xin được gửi lời cảm ơn chân thành tới Ban lãnh đạo, các Thầy/Cô của Khoa Đào tạo sau đại học và Khoa Viễn thông 1 của Học viện Công nghệ Bưu chính Viễn thông đã tạo điều kiện thuận lợi để nghiên cứu sinh hoàn thành nhiệm vụ. Nghiên cứu sinh trân trọng cảm ơn Trường Đại học Công nghiệp Hà Nội, đơn vị chủ quản, đã cho phép và tạo điều kiện cho nghiên cứu sinh được tham gia và hoàn thành chương trình đào tạo tiến sĩ. Nghiên cứu sinh cũng xin bày tỏ lòng cảm ơn sâu sắc đến TS. Vũ Trung Kiên, TS. Tống Văn Luyên, những người luôn hỗ trợ nghiên cứu sinh trong thời gian hoàn thành nghiên cứu. Xin chân thành cảm ơn Ban chủ nhiệm Khoa Điện tử và các anh chị em đồng nghiệp thuộc Khoa Điện tử, trường Đại học Công nghiệp Hà Nội đã luôn tạo mọi điều kiện giúp nghiên cứu sinh hoàn thành luận án.

Xin được bày tỏ lòng cảm ơn tới gia đình đã kiên trì chia sẻ và động viên nghiên cứu sinh trong suốt quá trình thực hiện nội dung luận án.

Hà Nội, tháng 3 năm 2023

MỤC LỤC

BẢNG DANH MỤC CÁC HÌNH VẼ

BẢNG DANH MỤC CÁC BẢNG BIỂU

BẢNG THUẬT NGỮ VIẾT TẮT

Từ viết tắt	Tiếng Anh	Tiếng Việt
A		
ACK	Acknowledgment	Tín hiệu báo nhận thành công
AES	Advanced Encryption Standard	Chuẩn mã hóa dữ liệu nâng cao
AIoT	Artificial Intelligence of Things	Internet vạn vật kết hợp với trí tuệ nhân tạo
APD	Avalanche Photo Diode	Đi-ốt quang thác
ARQ	Automatic Repeat Request	Yêu cầu phát lại tự động
B		
BPF	Band Pass Filter	Bộ lọc thông dải
BPSK	Binary Phase Shift Keying	Điều chế khóa dịch pha nhị phân
C		
CDM	Code Division Mutiplexing	Ghép kênh phân chia theo mã
CDMA	Code Division Multiple Access	Đa truy nhập phân chia theo mã
CV-QKD	Continuous Variable-Quantum Key Distribution	Phân phối khóa lượng tử biến liên tục
CS-QKD	Coherent State-Quantum Key Distribution	Phân phối khóa lượng tử trạng thái kết hợp

CW	Continuous Wave	Sóng liên tục
D		
DES	Data Encryption Standard	Tiêu chuẩn mã hóa dữ liệu
DT/HD	Dual Threshold/Heterodyne Detection	Máy thu tách sóng kiểu heterodyne sử dụng cơ chế tách ngưỡng kép
DTMC	Discrete-Time Markov Chain	Chuỗi Markov rời rạc theo thời gian
DV-QKD	Discrete Variable-Quantum Key Distribution.	Phân phối khóa lượng tử biến rời rạc
E		
EM	External Modulator	Bộ điều chế ngoài
F		
FEC	Forward Error Correction	Sửa lỗi hướng phát
FPGA	Field-Programmable Gate Array	Mảng cổng lập trình được theo trường
FSO	Free Space Optics	Quang không gian tự do
FSP	Free Space Photonics	Quang không gian tự do
G		
GPU	Graphics Processing Unit	Bộ xử lý đồ họa
H		
HAP	High Altitude Platform	Hạ tầng trên cao

HUP	Heisenberg Uncertainly Principle	Nguyên lý bất định Heisenberg
I		
IIoT	Industrial Internet of Things	Internet vạn vật ứng dụng trong công nghiệp
IoT	Internet of Things	Internet vạn vật
ITU	International Telecommunication Union	Hiệp hội Viễn thông quốc tế
IR	Infrared Radiation	Phát xạ hồng ngoại
L		
LO	Local Oscillator	Bộ dao động nội
LoS	Line of Sight	Tầm nhìn thẳng
LPF	Low Pass Filter	Bộ lọc thông thấp
M		
MZM	March-Zehnder Modulator	Bộ điều chế March-Zehnder
N		
NACK	Negative-Acknowledgment	Tín hiệu báo nhận không thành công
O		
ODEMUX	Optical Demultiplexing	Tách kênh quang
OFDM	Orthogonal Frequency Division Multiplexing	Ghép kênh phân chia theo tần số trực giao
OMUX	Optical Multiplexing	Ghép kênh quang

OTP	One Time Password	Mật khẩu dùng một lần
OW	Optical Wireless	Quang không dây
P		
PIN	P-Intrisic-N	Loại đi-ốt tách quang có thêm lớp tự dẫn
PQC	Post Quantum Cryptography	Mật mã hậu lượng tử
Q		
QA-DTMC	Queue-Associated DTMC	Chuỗi Markov rời rạc thời gian kết nối hàng đợi
QBER	Quantum Bit Error Rate	Tỷ lệ lỗi bit lượng tử
QKD	Quantum Key Distribution	Phân phối khóa lượng tử
QPSK	Quadrature Phase Shift Keying	Điều chế khóa dịch pha cầu phương
QPSK-DT/HD	Quadrature Phase Shift Keying-Dual Threshold/ Heterodyne Detection	Hệ thống QKD có bên phát sử dụng kiểu điều chế QPSK, bên thu dùng tách sóng kiểu heterodyne và cơ chế tách ngưỡng kép
QPSK-DT/DD	Quadrature Phase Shift Keying-Dual Threshold/ Direct Detection	Hệ thống QKD có bên phát sử dụng kiểu điều chế QPSK, bên thu dùng tách sóng kiểu trực tiếp và cơ chế tách ngưỡng kép
QKER	Quantum Key Error Rate	Tỷ lệ lỗi khóa lượng tử

QSD/PP	Quantum State Determination/ Performance Parameters	Bộ xác định trạng thái lượng tử/ Các tham số hiệu năng
QSP	Quantum State Preparation	Bộ chuẩn bị trạng thái lượng tử
R		
RF	Radio Frequency	Tần số vô tuyến
S		
S/P	Serial/Parallel	Chuyển đổi nối tiếp/song song
SCM	Sub Carrier Multiplexing	Ghép kênh sóng mang phụ
SIM	Subcarrier Intensity Modulation	Điều chế cường độ sóng mang phụ
SIM/BPSK-DT	Subcarrier Intensity Modulation/ Binary Phase Shift Keying-Dual Threshold	Hệ thống QKD có máy phát sử dụng điều chế cường độ sóng mang phụ dựa trên BPSK và máy thu sử dụng cơ chế tách ngưỡng kép
SKR	Secret Key Rate	Tốc độ khóa bí mật
SNR	Signal-to-Noise Ratio	Tỷ số tín hiệu trên nhiễu
W		
WDM	Wave Division Multiplexing	Ghép kênh phân chia theo bước sóng

DANH MỤC CÁC KÝ HIỆU

a	Hệ số tính trong trường hợp suy hao do tuyết
a_d	Khẩu độ tách sóng tại trạm mặt đất
a_R	Bán kính thấu kính thu
A	Diện tích mặt thu của bộ thu
A_0	Tỷ lệ công suất thu được tại $r = 0$
$A_t(t)$	Biên độ trường quang của xung Gauss ở phía phát
$A_r(t)$	Biên độ trường quang nhận được ở phía thu
b	Hệ số tính trong trường hợp suy hao do tuyết
$Be\,(Df)$	Băng thông hiệu dụng của bộ thu
B_0	Băng thông quang
C	Kích thước của bộ nhớ đệm tại trạm chuyển tiếp
$C_n^2(h)$	Tham số cấu trúc chỉ số khúc xạ
D	Đường kính aperture của máy thu
d_1	Ngưỡng tách quang tại máy thu trong trường hợp không dùng trạm chuyển tiếp
d_0	Ngưỡng tách quang tại máy thu trong trường hợp không dùng trạm chuyển tiếp
$d^{(A)}t$	Chuỗi bit ngẫu nhiên được tạo ra bởi bộ tạo khóa sẽ được đưa ra bộ phát
$d_0^{(AR)}$	Ngưỡng tách quang tại máy thu trong trường hợp dùng trạm chuyển tiếp

$d_1^{(AR)}$	Ngưỡng tách quang tại máy thu trong trường hợp dùng trạm chuyển tiếp
D_β	Khoảng cách truyền dẫn trong môi trường khí quyển
D_S	Khoảng cách truyền dẫn trong môi trường không gian tự do
e	Hệ số Euler
$E\left[I_x^{(AR)}\right]$	Giá trị trung bình của dòng tín hiệu thu được
E_{Rx}	Tín hiệu quang thu được tại máy thu
f_c	Tần số sóng mang quang
f_{IF}	Tần số trung tần
f_{LO}	Tần số của bộ dao động nội
g	Hệ số suy hao trong môi trường khí quyển phụ thuộc khoảng cách của tầm nhìn.
$\mathrm{G}(.)$	Hàm Gamma
G_{Tx}	Độ khuếch đại của thấu kính tại bên phát
$G_T^{(A)}$	Độ khuếch đại của thấu kính phát tại vệ tinh
$G_R^{(R)}$	Độ khuếch đại của thấu kính thu tại trạm chuyển tiếp
$G_T^{(R)}$	Độ khuếch đại của thấu kính phát tại trạm chuyển tiếp
$G_R^{(B)}$	Độ khuếch đại của thấu kính thu tại trạm mặt đất
H	Tốc độ chuỗi bit đến bộ đệm
h	Suy hao kênh bao gồm suy hao không gian tự do và suy hao khí quyển
$\tilde{h}$	Hằng số Plank
H_a	Độ cao tầng khí quyển
H_G	Độ cao của trạm mặt đất
h_a	Suy hao do khí quyển
h_l	Suy hao do trải rộng chùm tia

h_f	Ảnh hưởng của pha-đinh do nhiễu loạn khí quyển
H_S	Độ cao của vệ tinh
I_d	Dòng điện tối
I_{decod}	Dòng điện sau giải mã
i_n	Dòng điện nhiễu
I_p	Tín hiệu điện tại đầu ra của APD
k	Số kênh ở trạng thái đang gửi bit "1"
K	Số lượng kênh ghép trong hệ thống QKD-FSO sử dụng kỹ thuật CDMA
k_b	Số bước sóng trường quang
k_B	Hằng số Boltzmann
k_1	Hệ số tính toán cho suy hao do mưa
k_2	Hệ số tính toán cho suy hao do mưa
Kn(.)	Hàm Bessel sửa đổi loại 2 bậc n
L_a	Khoảng cách truyền dẫn trong môi trường khí quyển
l_{bs}	Độ dài của một chuỗi bit ngẫu nhiên.
L_{FS}	Suy hao trong không gian tự do
M_A	Hệ số nhân thác lũ của APD
M	Số lần tối đa trạm chuyển tiếp phát lại một chuỗi bit
M_w	Số lượng bước sóng quang trong phương pháp ghép kênh kiểu WDM
m_L	Số lần truyền lại của một chuỗi bit
N	Số lượng sóng mang phụ trong phương pháp ghép kênh kiểu SCM
N_c	Tổng số kênh được ghép trong phương pháp ghép kênh kiểu SCM-WDM
n_L	Số chuỗi bit xếp hàng tại bộ đệm của Ruby

$P_{A,B}(i,j)$	Xác suất mà tại một thời điểm bit ở bên Alice là "*i*" nhưng bit bên Bob là "*j*"
$P_{B/A}(j/i)$	Xác suất mà Bob nhận được bit "*j*" trong khi Alice gửi đi bit "*i*"
P_{Eve}	Xác suất mà Eve phát hiện đúng các bit được truyền đi từ Alice
P_{error}	Xác suất có một số bit lỗi trong khóa chọn lọc
P_L	Ma trận chuyển đổi
P_{LO}	Công suất của bộ dao động nội
P_R	Công suất thu
P_{sift}	Xác suất chọn lọc
P_T	Công suất phát
$P_T^{(RB)}$	Công suất phát tại phía phát của trạm chuyển tiếp
$p^{(ar)}$	Xác suất khi có một chuỗi bit trong một khe thời gian xác định
$p^{(no)}$	Xác suất không có một chuỗi bit đến trong một khe thời gian xác định
$p_{j(q_D,s_L,m_L),(Success)}$	Xác suất một chuỗi bit có thể được nhận một cách thành công tại khe thời gian thứ *j*
q	Điện tích điện tử
q_D	Chiều dài hàng đợi của Ruby
Q(.)	Hàm Q Gauss
R	Tốc độ mưa
r	Độ lệch giữa tâm bộ thu và tâm vết búp sóng
R_b	Tốc độ bit
R_L	Giá trị điện trở tải
S	Tốc độ tuyết
s_L	Trạng thái của đường truyền

T_e	Nhiệt độ tại máy thu
t_Q	Trễ hàng đợi tại bộ đệm của Ruby
x	Hệ số nhiễu trội của APD
x_c	Giá trị tương quan chéo
X	Phân cực xiên
V	Tầm nhìn thấy
η	Hiệu suất lượng tử
ζ	Góc thiên đỉnh
θ	Góc phân kỳ của chùm tia
θ_h	Góc của độ cao trên đường chân trời
$\mathcal{R}$	Đáp ứng của bộ tách quang
λ	Bước sóng quang
α	Tham số hiệu dụng của môi trường truyền dẫn tán xạ
α_{snow}	Suy hao do tuyết gây ra
α_{rain}	Suy hao do mưa gây ra
β	Tham số hiệu dụng của môi trường truyền dẫn tán xạ
ρ	Hệ số tỷ lệ ngưỡng kép tại máy thu trong trường hợp không dùng trạm chuyển tiếp
β_l	Hệ số suy hao khí quyển
ν	Tốc độ gió
σ_n	Tổng phương sai nhiễu
σ_R^2	Phương sai Rytov
τ_{bs}	Thời gian truyền một chuỗi bit
τ_0	Khoảng thời gian mà điều kiện nhiễu loạn khí quyển không thay đổi
$\mathcal{D}$	Độ trễ lớn nhất mà đường truyền ARQ cho phép
$\varsigma^{(AR)}$	Hệ số tỷ lệ tại bộ tách ngưỡng kép của trạm chuyển tiếp

$\varsigma^{(RB)}$	Hệ số tỷ lệ tại bộ tách ngưỡng kép của trạm mặt đất trong trường hợp dùng trạm chuyển tiếp
$\varsigma_W^{(RB)}$	Hệ số tỷ lệ của bộ tách ngưỡng kép tại trạm mặt đất trong trường hợp nhiễu loạn khí quyển yếu
$\varsigma_S^{(RB)}$	Hệ số tỷ lệ của bộ tách ngưỡng kép tại trạm mặt đất trong trường hợp nhiễu loạn khí quyển mạnh.
μ	Độ sâu điều chế
ω	Trọng lượng của mã
ω_c	Tần số góc của sóng mang quang
γ	Hệ số suy hao theo thời tiết
ϕ_A	Kết hợp pha của hai nhánh bộ điều chế Mach-Zehnder
ϕ_B	Pha của tín hiệu được tạo ra ở máy thu
ϕ_1	Pha của nhánh thứ nhất trong bộ điều chế Mach-Zehnder
ϕ_2	Pha của nhánh thứ hai trong bộ điều chế Mach-Zehnder
ϕ_{LO}	Pha của bộ dao động nội
Σ	Tổng của một phép toán
Π	Tích của một phép toán
$\approx$	Tương đương (Biểu thức)
$\cong$	Hàm tương đương
$\triangleq$	Bằng nhau theo định nghĩa

MỞ ĐẦU

Bảo mật thông tin ngày càng trở thành vấn đề quan trọng và cần quan tâm khi truyền thông, đặc biệt là những thông tin được truyền qua cơ sở hạ tầng mạng Internet không được bảo mật. Các phương pháp bảo mật khi truyền thông tin hiện nay chủ yếu dựa trên tính bí mật của khóa được mã hóa. Mức độ bảo mật sẽ phụ thuộc vào độ phức tạp của thuật toán được dùng để mã hóa khóa và độ dài của khóa. Các thuật toán càng khó, độ dài của khóa càng lớn thì tính bảo mật của khóa càng được đảm bảo. Tuy nhiên, với sự ra đời của các máy tính lượng tử với tốc độ xử lý lớn gấp nhiều lần máy tính hiện nay, nếu một hệ thống bảo mật chỉ dựa vào tính phức tạp của thuật toán hoàn toàn có thể bị phá khóa [57, 77, 78].

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 [22, 72]. Động lực cơ bản cho nghiên cứu QKD là theo lý thuyết thông tin của Shannon [73], bảo mật vô điều kiện (bảo mật hoàn hảo) có thể đạt được khi sử dụng khóa đối xứng đủ dài và chỉ một lần [30]. Vấn đề đặt ra là yêu cầu cần phải có một kênh an toàn để truyền khóa từ bên phát tới bên thu. Do đó, nếu đảm bảo một phương thức bảo mật để phân phối khóa, chúng ta có thể đạt được bảo mật vô điều kiện để phân phối khóa an toàn giữa hai bên hợp pháp trong các mạng truyền thông cho dù có sự hiện diện của kẻ nghe lén**.** 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). DV-QKD có nhiều ưu điểm về tính bảo mật tuy nhiên do máy thu DV-QKD yêu cầu sử dụng các thiết bị tách đơn photon phức tạp và đắt tiền, tốc độ truyền khóa nhỏ nên DV-QKD khó thực hiện trong thực tế. CV-QKD có ưu điểm về khả năng tương thích với các hệ thống truyền thông

quang đã có và tốc độ khóa cao. CV-QKD ngày càng thu hút được sự quan tâm của cộng đồng các nhà nghiên cứu bởi những ưu điểm mà nó mang lại.

Nguyên lý hoạt động của một hệ thống QKD bao gồm hai giai đoạn là truyền thông lượng tử và thống nhất khóa. Giai đoạn truyền thông lượng tử bao gồm ba bước là: (1) Chuẩn bị trạng thái lượng tử, (2) Truyền trạng thái lượng tử và (3) Đo trạng thái lượng tử để lấy thông tin. Một giao thức phân phối khóa lượng tử gồm bốn bước, bao gồm: (1) Bên phát chọn ngẫu nhiên một trong hai trạng thái phân cực để mã hóa mỗi một bit nhị phân trong khóa thô truyền đi; (2) Bên thu thực hiện việc tách và xác định giá trị bit thu được bằng việc lựa chọn ngẫu nhiên phân cực; (3) Bên thu trao đổi thông tin với bên phát về phân cực được sử dụng để giải mã các bit thu được, bên phát sẽ báo cho bên thu biết phân cực mà bên thu dùng là đúng hay sai và tạo khóa chọn lọc và (4) Sửa lỗi và tạo ra khóa bí mật. Trong đó, bước 1 và 2 của giao thức phân phối khóa lượng tử thuộc về giai đoạn một trong hoạt động của một hệ thống QKD là truyền thông lượng tử. Bước 3 và 4 của giao thức phân phối khóa sẽ thuộc về giai đoạn hai, thống nhất khóa, giai đoạn này sử dụng kênh riêng có xác thực để chia sẻ các thông tin về chọn và tạo khóa.

Ngoài ra**,** việc truyền thông tin không chỉ giới hạn trong một quốc gia hay một tổ chức mà phải đáp ứng trong một khoảng cách lớn như giữa các quốc gia trong hệ thống thông tin toàn cầu. 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 phạm vi toàn cầu.

Để có thể đáp ứng yêu cầu truyền khóa có tốc độ đủ lớn, tỷ lệ lỗi bit lượng tử đủ nhỏ đảm bảo cho quá trình sửa lỗi bên phía thu, khoảng cách lớn ở quy mô toàn cầu thì hệ thống phân phối khóa lượng tử qua không gian tự do QKD-FSO cần vượt qua nhiều thách thức. Các thách thức xuất hiện là do các nguyên nhân: nhiễu và tạp âm tại bên phát và bên thu [11, 43]; sự can thiệp của kẻ nghe lén; những ảnh hưởng của môi trường không gian tự do; sự thăng giáng của cường độ tín hiệu quang thu được; sự lệch hướng giữa thấu kính phát và thấu kính thu. Trong đó, những yếu tố ảnh

hưởng của môi trường không gian tự do có thể kể đến như: suy hao trên đường truyền có giá trị lớn, phụ thuộc vào yếu tố môi trường và thời tiết (sương mù, mưa, tuyết, gió); đặc biệt là tác động của điều kiện khí quyển, bao gồm sự hấp thụ, tán xạ và nhiễu loạn khí quyển. Do ảnh hưởng của các yếu tố đã nêu ở trên, hiệu năng của hệ thống QKD-FSO sử dụng vệ tinh sẽ bị hạn chế và cần có các biện pháp để nâng cao hiệu năng hệ thống nhằm phục vụ cho mục đích truyền khóa trong hệ thống QKD toàn cầu.

Xuất phát từ nhu cầu cần thiết phải nâng cao hiệu năng của hệ thống QKD-FSO và tận dụng những ưu điểm của hệ thống phân phối khóa lượng tử biến liên tục CV-QKD, 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.

Luận án sẽ tập trung xây dựng các mô hình toán học để phân tích, đánh giá hiệu năng hệ thống QKD-FSO với các tham số hệ thống, điều kiện đường truyền và đề xuất các giải pháp cải thiện hiệu năng truyền dẫn FSO khác nhau cho hệ thống CV-QKD. Kết quả nghiên cứu của luận án sẽ phục vụ cho những nghiên cứu tiếp theo như thiết kế hệ thống, đánh giá tính khả thi của hệ thống đề xuất, xác định điều kiện hoạt động tin cậy của hệ thống đề xuất ở điều kiện cụ thể. Ý nghĩa thực tiễn đạt được của luận án thể hiện ở các giải pháp mà luận án đề xuất nhằm cải thiện hiệu năng, cụ thể là giảm tỷ lệ lỗi bit lượng tử, tăng cự ly truyền dẫn, tăng tốc độ truyền khóa lượng tử cho hệ thống truyền khóa lượng tử qua không gian tự do QKD-FSO. Từ đó góp phần thúc đẩy quá trình triển khai ứng dụng hệ thống truyền khóa lượng tử trong truyền thông.

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.

Đối tượng nghiên cứu của luận án là truyền dẫn quang qua không gian tự do trong hệ thống phân phối khóa lượng tử biến liên tục và hiệu năng của hệ thống này. **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.

Để đạt được mục tiêu nghiên cứu đã nêu ở trên, các **nhiệm vụ nghiên cứu** trong quá trình thực hiện luận án được xác định bao gồm: (1) nghiên cứu tổng quan về hệ thống phân phối khóa lượng tử qua không gian tự do dựa trên vệ tinh, (2) đề xuất áp dụng các giải pháp cải thiện hiệu năng truyền dẫn FSO trong hệ thống phân phối khóa lượng tử biến liên tục dựa trên vệ tinh và (3) kiểm chứng về hiệu năng của các giải pháp đã đề xuất. Cụ thể, trong phần tổng quan về hệ thống phân phối khóa lượng tử qua không gian tự do QKD-FSO, luận án tập trung vào khảo sát, phân tích, đánh giá các kết quả nghiên cứu của các tác giả đi trước có nghiên cứu liên quan đến hiệu năng của hệ thống phân phối khóa lượng tử để rút ra những hạn chế và tìm ra hướng nghiên cứu của riêng mình. Tiếp theo, luận án sẽ đề xuất các giải pháp nâng cao hiệu năng của hệ thống. Cuối cùng, luận án sẽ thực hiện kiểm chứng các giải pháp

đã đề xuất dựa trên việc xây dựng các mô hình toán học và kết quả khảo sát hiệu năng dựa trên công cụ phần mềm Matlab.

Trên cơ sở các nhiệm vụ nghiên cứu đã nêu ở trên, **phương pháp nghiên cứu** được nghiên cứu sinh áp dụng trong luận án là nghiên cứu lý thuyết, dựa trên lý thuyết thông tin và nguyên lý truyền thông lượng tử. Các công cụ toán học và xác suất được sử dụng trong việc xây dựng mô hình toán học phân tích hiệu năng của hệ thống QKD-FSO. Công cụ phần mềm được sử dụng trong việc khảo sát và đưa ra các kết quả phân tích hiệu năng. Cụ thể, phương pháp nghiên cứu lý thuyết được sử dụng cho các nghiên cứu về phân phối khóa lượng tử, nguyên lý hoạt động của các phần tử trong hệ thống truyền dẫn khóa lượng tử qua không gian tự do như tạo khóa/khôi phục khóa, điều chế/giải điều chế tín hiệu, phát/thu quang. Phương pháp nghiên cứu lý thuyết kết hợp với công cụ toán học, xác xuất và phần mềm được sử dụng trong việc khảo sát, đánh giá hiệu năng các hệ thống phân phối khóa lượng tử qua không gian đã đề xuất.

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 có tiêu đề "***Tổng quan về truyền dẫn khóa lượng tử qua không gian tự do***" trình bày về giao thức BB84, giao thức nền tảng của phân phối khóa lượng tử; những đặc điểm của QKD biến liên tục (CV-QKD), những ưu điểm của CV-QKD so với QKD biến rời rạc (DV-QKD); đường truyền quang qua không gian tự do có sử dụng vệ tinh; các yếu tố ảnh hưởng tới hiệu năng truyền dẫn quang trong hệ thống phân phối khóa lượng tử biến liên tục qua không gian tự do QKD-FSO. Nội dung chính của Chương sẽ tập trung khảo sát các nghiên cứu liên quan đến cải thiện hiệu năng truyền dẫn quang qua không gian tự do của hệ thống phân phối khóa lượng tử biến liên tục để từ đó xác định các hạn chế của các nghiên cứu đã có và đề xuất hướng nghiên cứu, phạm vi nghiên cứu cũng như phương thức tiếp cận của luận án.

Chương 2 có tiêu đề "***Hệ thống QKD-FSO biến liên tục dựa trên điều chế***

pha" trình bày về mô hình toán học của kênh truyền FSO khi xem xét các yếu tố suy hao, ảnh hưởng của pha-đinh do nhiễu loạn khí quyển; giải pháp truyền dẫn quang qua không gian tự do trong hệ thống phân phối khóa lượng tử biến liên tục CV-QKD dựa trên điều chế pha. Nội dung trình bày trong phần giải pháp đề xuất sẽ bao gồm thiết kế hệ thống QKD-FSO dựa trên vệ tinh sử dụng phương thức truyền dẫn khóa lượng tử dựa trên điều chế pha; sử dụng phương pháp phân tích lý thuyết với các công cụ giải tích và xác suất xây dựng công thức tính các tham số hiệu năng; khảo sát, đánh giá hiệu năng truyền dẫn quang của hệ thống phân phối khóa lượng tử biến liên tục qua không gian tự do dựa trên điều chế pha. Đóng góp của luận án trong Chương này là đề xuất phương thức truyền dẫn khóa lượng tử dựa trên điều chế pha cầu phương (Quadrature Phase Shift Keying – QPSK) kết hợp với bộ tách sóng kiểu heterodyne và cơ chế tách ngưỡng kép. Kết quả nghiên cứu của Chương 2 đã được công bố trên 01 bài báo tại *Hội nghị quốc tế ISCIT 2019* [C2] (bài báo nhận được giải bài báo xuất sắc của hội nghị); 01 bài báo công bố trên tạp chí quốc tế ISI (*Photonic Network Communications*, vol. 42, no. 1, pp. 27-39, July 2021) [J1]; 01 bài báo công bố trên tạp chí *Khoa học và Công nghệ* [J3].

Chương 3 có tiêu đề "***Cải thiện hiệu năng hệ thống QKD-FSO sử dụng kỹ thuật truyền lại khóa và chuyển tiếp***" tập trung trình bày về 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 CV-QKD bằng việc sử dụng kỹ thuật truyền lại khóa với yêu cầu phát lại tự động (Automatic Repeat Request – ARQ) và kỹ thuật chuyển tiếp dựa trên hạ tầng trên cao (High Altitude Platforms – HAP). Nội dung của Chương tập trung xây dựng mô hình toán học phân tích hiệu năng hệ thống đã đề xuất dựa trên việc sử dụng mô hình chuỗi Markov hai trạng thái. Chương này sẽ phân tích và đánh giá hai kịch bản. Ở kịch bản thứ nhất, hệ thống QKD-FSO sử dụng kỹ thuật truyền lại khóa theo phương pháp ARQ tại vệ tinh. Trong khi đó, kịch bản thứ hai với hệ thống QKD-FSO sử dụng kết hợp kỹ thuật chuyển tiếp dựa trên hạ tầng trên cao HAP với kỹ thuật truyền lại khóa theo phương pháp ARQ tại trạm chuyển tiếp. Các đóng góp của luận

án được trình bày trong Chương 3 đã được công bố trong *Hội nghị quốc tế về các công nghệ tiên tiến trong truyền thông IEEE ATC 2020* [C1] và 01 bài báo đăng trên tạp chí quốc tế ISI xếp hạng Q2 (*Photonic Network Communications*, vol. 42, no. 1, pp. 27-39, July 2021) [J1].

Chương 4 có tiêu đề "***Hệ thống QKD-FSO đa kênh đa người sử dụng***" tập trung trình bày về giải pháp sử dụng kỹ thuật ghép kênh sóng mang phụ (Subcarrier Multiplexing – SCM) với kỹ thuật ghép kênh quang phân chia theo bước sóng (Wave Division Mutiplexing – WDM) để cải thiện hiệu năng truyền dẫn quang qua không gian tự do trong hệ thống phân phối khóa lượng tử biến liên tục CV-QKD. Nội dung cụ thể bao gồm thiết kế mô hình hệ thống QKD-FSO dựa trên vệ tinh sử dụng kỹ thuật ghép kênh WDM và SCM; xây dựng công thức tính toán các tham số hiệu năng; khảo sát, đánh giá hiệu năng của truyền dẫn quang đối với giải pháp đề xuất . Khả năng hỗ trợ đa người dùng kết hợp với việc cải thiện hiệu năng an ninh của hệ thống QKD-FSO cũng được khảo sát với kỹ thuật đa truy nhập phân chia theo mã quang (Code Division Multiple Access – CDMA). Đóng góp của luận án được trình bày trong Chương 4 đã được công bố trong 01 bài báo đăng trên tạp chí *Khoa học và công nghệ quân sự* [J2] và 01 bài báo đăng và đăng trên tạp chí quốc tế Scopus xếp hạng Q2, *Opt. Continuum*, vol. 2, no. 2, pp. 289-302, Feb. 2023 [J4].

Trong nội dung của phần **Kết luận** sẽ trình bày tóm tắt các kết quả nghiên cứu chính của luận án cùng với những tự nhận xét của NCS về những ưu điểm và hạn chế của các đóng góp mới, từ đó đề xuất hướng nghiên cứu tiếp theo trong tương lai.

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

Tóm tắt

Nội dung của Chương trình bày về sự cần thiết của hệ thống phân phối khóa lượng tử trong truyền thông ngày nay, nguyên tắc tạo và truyền khóa ở bên phát, khôi phục khóa chọn lọc ở bên thu của giao thức BB84, hệ thống phân phối khóa lượng tử qua đường truyền quang qua không gian tự do và các yếu tố ảnh hưởng tới hiệu năng của hệ thống này. Nội dung chính của Chương sẽ tập trung khảo sát các nghiên cứu liên quan đến hiệu năng hệ thống phân phối khóa lượng tử qua không gian tự do để từ đó tìm ra các hạn chế của các nghiên cứu trước đây và đề xuất hướng nghiên cứu, phạm vi nghiên cứu và phương thức tiếp cận của luận án.

1.1. Giới thiệu chung về bảo mật thông tin và mã hóa dữ liệu

Bảo mật thông tin là các biện pháp nhằm phục vụ cho việc trao đổi hay lưu giữ thông tin một cách an toàn và bí mật. Mô hình bảo mật thông tin có thể phân loại theo hai hướng chính như sau: Bảo vệ thông tin trong quá trình truyền thông tin trên kênh truyền và bảo vệ hệ thống xử lý tín hiệu ở cả phía phát và phía thu khỏi sự xâm nhập của những kẻ truy nhập bất hợp pháp.

Để xem xét những vấn đề về bảo mật thông tin liên quan đến truyền thông tin trên kênh truyền, giả sử có ba nhân vật tên lần lượt là Alice, Bob và Eve. Alice và Bob thực hiện trao đổi thông tin với nhau, còn Eve là kẻ nghe lén, đặt thiết bị can thiệp vào kênh truyền tin giữa Alice và Bob. Các loại hành động tấn công của Eve có thể gây ảnh hưởng đến quá trình truyền tin giữa Alice và Bob là: xem trộm thông tin, thay đổi nội dung bản tin, mạo danh và phát lại bản tin. Một hệ thống truyền tin được gọi là an toàn và bảo mật thì phải có khả năng chống lại được các nguy cơ tấn công kể trên. Do đó, một hệ thống truyền tin phải có các đặc tính sau: tính bảo mật, tính chứng thực và tính không từ chối.

Mã hóa dữ liệu hay còn gọi là mật mã dữ liệu là một công cụ thiết yếu để bảo

mật dữ liệu. Mã hóa dữ liệu phải đáp ứng được các yêu cầu bảo mật của một hệ thống truyền tin. Một bộ mã hóa dữ liệu sẽ được đặc trưng bởi một bộ bao gồm các tham số (P, C, K, E, D, K'), với:

P: Thông tin gốc được gửi đi (**P**laintext).

C: Bản mã gửi đi trên đường truyền (**C**iphertext).

K: Khóa phục vụ cho việc mã hóa dữ liệu (**K**ey)

E: Thuật toán mã hóa dữ liệu (**E**ncrypt Algorithm).

D: Thuật toán giải mã dữ liệu (**D**ecrypt Algorithm).

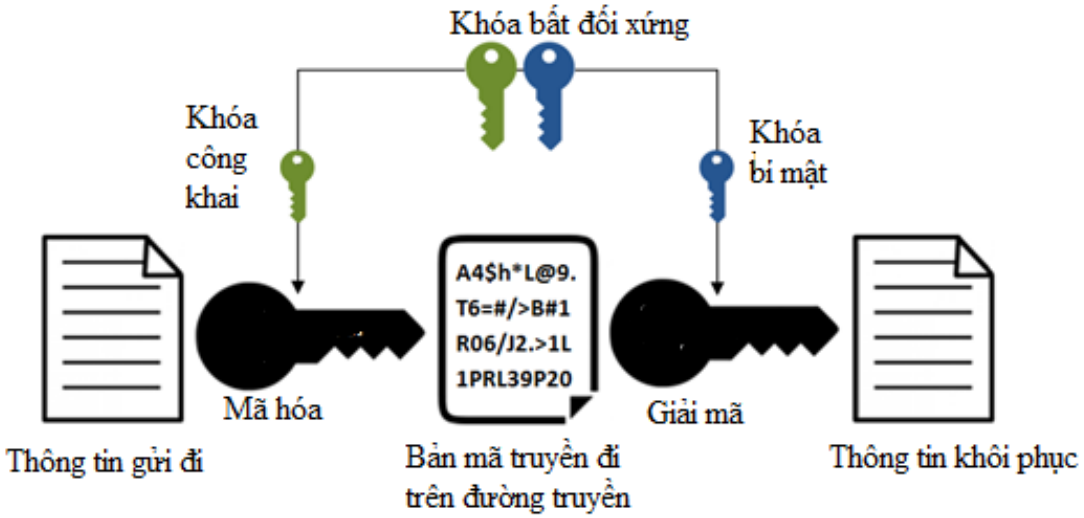
K': Khóa phục vụ cho việc giải mã dữ liệu (**K**ey).

Trong đó:

C = E (P,K)

P = D (C,K')

Ngày nay, có rất nhiều phương pháp mã hóa dữ liệu được sử dụng nhưng có thể chia chúng theo hai loại chính là: mã hóa bất đối xứng và mã hóa đối xứng.

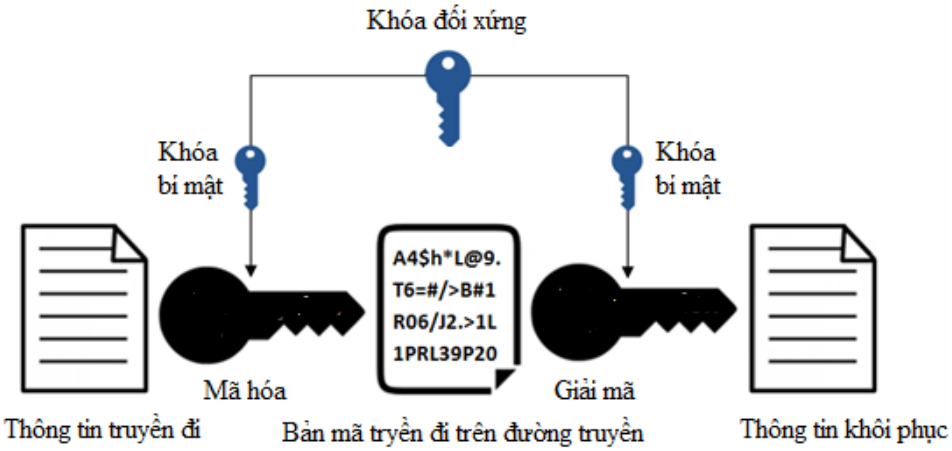


Hình 1. 1. Mã hóa bất đối xứng

Mã hóa bất đối xứng hay còn gọi là phương pháp **mã hóa công khai** được minh họa trong Hình 1.1. Trong phương pháp này, có hai khóa khác nhau được dùng

để để mã hóa và giải mã dữ liệu (K ≠ K'). Bên phát sử dụng khóa công khai để mã hóa, bên thu sử dụng khóa bí mật để giải mã. Khóa bí mật sẽ không được truyền, khóa công khai sẽ được truyền đi cùng với dữ liệu thông qua mạng Internet hay một mạng truyền thông nào đó [18].

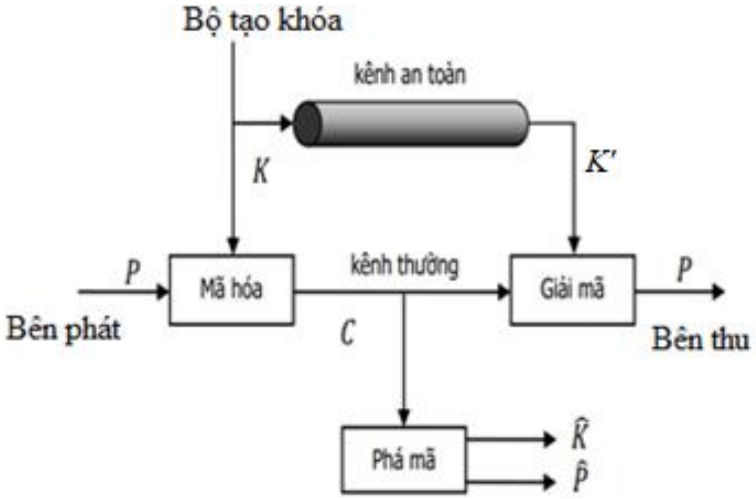
Mã hóa bất đối xứng được sử dụng trong các giao tiếp hàng ngày qua Internet. Một số phương pháp mã hóa theo phương pháp này là RSA, DSA, Elgaman, Knapsack. Mã hóa bất đối xứng có ưu điểm là độ bảo mật cao do khóa bí mật không bao giờ được truyền. Vì vậy, sẽ không có hiện tượng khóa bị phá trên đường truyền bởi những người dùng không hợp pháp và hạn chế được vấn đề bảo mật phát sinh khi truyền khóa do chỉ truyền khóa công khai. Ngoài ra, phương pháp này có khả năng cung cấp các chữ ký số giúp tăng được tính bảo mật. Tuy nhiên, phương pháp mã hóa bất đối xứng có nhược điểm là tốc độ xử lý của bên phát và bên thu khá chậm.



Hình 1. 2. Mã hóa đối xứng

Trong khi đó, **mã hóa đối xứng** (Hình 1.2) hay còn gọi là phương pháp **mã hóa khóa bí mật** là phương pháp mã hóa mà bên phát và bên thu dùng chung một khóa để mã hóa và giải mã dữ liệu K = K' (Hình 1.3). Do thuật toán giải mã ngược với thuật toán mã hóa nên phương pháp có tên là mã hóa đối xứng. Khóa bí mật có thể là các số, các từ hay các ký tự theo một cách ngẫu nhiên và được trộn với thông tin cần gửi đi theo một thuật toán nào đó để làm thay đổi nội dung bản tin cần gửi [18].

Đặc tính quan trọng đầu tiên của mã hóa đối xứng là khóa phải được giữ bí mật giữa người gửi và người nhận, hay nói cách khác khóa phải được phân phối một cách an toàn từ người gửi đến người nhận. Đặc tính quan trọng thứ hai của một hệ mã hóa đối xứng là có thể đạt được bảo mật vô điều kiện của hệ mã khi sử dụng khóa đối xứng đủ dài và chỉ một lần [30]. Tính bảo mật vô điều kiện của hệ mã đạt được khi hệ mã không thể bị phá mã (điều kiện lý tưởng) hoặc thời gian phá mã là bất khả thi. Một số phương pháp mã hóa sử dụng phương pháp này là DES, AES, RC4, RC5, RC6 Blowfish. Các thuật toán được sử dụng rộng rãi trong phương pháp này là AES-128, AES-192, AES-256.



Hình 1. 3. Mô hình hệ thống mã hóa đối xứng

Ưu điểm của phương pháp mã hóa đối xứng là tốc độ nhanh. Do khóa không truyền cùng dữ liệu nên khả năng dữ liệu bị giải mã là bằng không nếu như khóa được đảm bảo về tính bảo mật. Phương pháp mã hóa này sử dụng tính chứng thực bảo mật để cải thiện sự nhận diện của bên thu. Chỉ bên thu hợp pháp có khóa bảo mật mới có thể giải mã được dữ liệu. Nhược điểm lớn nhất của phương pháp này là cả bên phát và bên thu đều phải tham gia vào quá trình trao đổi khóa để mã hóa dữ liệu trước khi dữ liệu có thể giải mã ở bên thu. Khóa bí mật phải được truyền tới bên thu trước khi dữ liệu được truyền đi. Vấn đề đặt ra của phương pháp này là vấn đề truyền khóa từ bên phát tới bên thu: yêu cầu cần phải có một kênh an toàn để truyền khóa từ bên phát tới bên thu. Nhờ có các ưu điểm vượt trội về tốc độ, tính giản đơn và bảo mật tốt, mã

hóa đối xứng hiện được sử dụng rộng rãi trong rất nhiều ứng dụng từ bảo mật khi truy cập Internet cho tới bảo vệ dữ liệu lưu trữ trên các máy chủ điện toán đám mây.

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

Phân phối khóa được coi là vấn đề quan trọng của mật mã. Để đảm bảo tính bảo mật khi truyền thông qua các kênh thông thường, điều cần thiết là các khóa bí mật phải được phân phối một cách an toàn. Ngay cả khi thuật toán mã hóa được sử dụng là không thể phá vỡ, thông tin truyền đi cũng dễ bị tấn công nếu các khóa không được đảm bảo an toàn. Các thuật toán càng khó, độ dài của khóa càng lớn thì tính bảo mật của khóa càng được đảm bảo. Tuy nhiên, với sự ra đời của các máy tính lượng tử với tốc độ xử lý lớn gấp nhiều lần máy tính hiện nay nếu một hệ thống bảo mật chỉ dựa vào tính phức tạp của thuật toán hoàn toàn có thể bị phá khóa. Giả sử, hệ thống sử dụng kiểu mã AES với chiều dài khóa là 128 bit, nếu có hệ thống tính toán đủ mạnh để kiểm tra 1.000 tỷ khóa trong một giây thì để kiểm tra toàn bộ các khóa có thể có, phải mất 10,79 nghìn tỷ năm. Tuy nhiên, nếu sử dụng máy tính lượng tử, thời gian để bẻ khóa chỉ mất khoảng sáu tháng.

Theo hiệp hội Viễn thông quốc tế (International Telecommunication Union - ITU), có ba cách khả thi để chống lại các cuộc tấn công từ máy tính lượng tử [37]:

- Cải tiến hệ thống tiền lượng tử hiện tại: Tăng gấp đôi kích thước khóa hiện tại để có thể chống lại thuật toán Grover bằng cách tăng tốc độ lên căn bậc hai cho các thuật toán tìm kiếm lượng tử so sánh trên máy tính cổ điển**.** Tuy nhiên, điều này chỉ phù hợp với các hệ thống sử dụng mã hóa đối xứng.

- Thiết kế hệ thống khóa công khai mới: Sử dụng các vấn đề toán học mới chưa bị bẻ khóa bởi các thuật toán lượng tử hiện tại, ví dụ: các thuật toán mã hóa dựa trên mã và dựa trên kiểu mạng tinh thể, thường được gọi là mật mã hậu lượng tử PQC. Tuy nhiên, ngay cả nếu những vấn đề toán học mới đó được chứng minh là mạnh mẽ chống lại các thuật toán lượng tử hiện tại, chúng cũng có thể sẽ không an toàn trước các thuật toán lượng tử sẽ được tạo ra trong tương lai.

- Sử dụng hệ thống phân phối khóa lượng tử QKD để thay thế cơ chế trao đổi khóa dựa trên khóa công khai: Tính bảo mật của phân phối khóa lượng tử QKD dựa trên các nguyên tắc vật lý lượng tử của ánh sáng [30, 72] có thể tránh được một cách hiệu quả các mối đe dọa được gây ra do sự gia tăng hiệu năng tính toán hoặc thuật toán "backdoors" mà các thuật toán khóa công khai truyền thống phải đối mặt. QKD đã được chứng minh là có khả năng chống lại các thuật toán lượng tử được tạo ra trong tương lai [6].

Như vậy, để giải quyết vấn đề về kênh an toàn khi truyền khóa, có thể thực hiện bảo mật ngay tầng vật lý khi truyền khóa bằng cách sử dụng phân phối khóa lượng tử QKD.

Mật mã lượng tử hay cụ thể hơn là **phân phối khóa lượng tử QKD** là phương pháp chỉ dựa trên luật của lớp vật lý mà không sử dụng các thuật toán để mã hóa dữ liệu. QKD có những ưu điểm đáp ứng được nhu cầu bảo mật của các hệ thống truyền tin trong tương lai:

- Không giống như các hệ thống cổ điển, 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.
- Nếu như các hệ thống bảo mật cổ điển không thể phát hiện được sự có mặt của kẻ xâm nhập trái phép thì 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. Điều này có được là do đặc tính duy nhất và dễ bị thay đổi của photon, nếu có bên thứ ba cố tình đọc hay sao chép các photon theo bất kỳ một cách nào đó sẽ làm thay đổi trạng thái cả photon [48].

Vì những lý do này, QKD trở thành một thành phần không thể thiếu trong các kiến trúc của hệ thống thông tin lượng tử trong tương lai, đó là những hệ thống bao gồm cả những thuật toán cổ điển dựa trên lượng tử và các phương pháp mật mã lượng tử. Hiện nay, QKD là phương pháp phân phối khóa đang thu hút được nhiều sự quan tâm của các chuyên gia bảo mật dữ liệu trên toàn thế giới trong bối cảnh có sự phát

triển mạnh mẽ của các máy tính lượng tử [6]. QKD là cơ sở để phát triển một hệ thống Internet lượng tử trên quy mô toàn cầu, một hệ thống mà người sử dụng có thể truy cập vào các máy tính lượng tử từ một khoảng cách rất xa thông qua Internet lượng tử. Các ứng dụng tiềm năng của QKD bao gồm các hệ thống thông tin yêu cầu bảo mật cao như hệ thống Smart Grid, hệ thống thông tin tài chính hay các hệ thống phòng thủ quốc gia…[33]. Mô hình ứng dụng hệ thống QKD được minh họa trong Hình 1.4.

Hình 1. 4. Mô hình ứng dụng hệ thống QKD

1.2.2. Các kiểu tấn công có thể xảy ra đối với hệ thống QKD

-***Tấn công kiểu xen giữa (man in the middlie attack)***: Trong các cuộc tấn công kiểu xen giữa, Eve giả làm Bob đối với Alice và Eve giả làm Alice đối với Bob. Do đó, trong hệ thống QKD yêu cầu phải có sự chứng thực của Alice và Bob với nhau.

-***Chặn và gửi lại thông tin (intercept-resend attack)***: Với các cuộc tấn công kiểu chặn và gửi lại thông tin, Eve giải mã ra các trạng thái lượng tử được gửi bởi Alice (Eve sẽ đoán theo cách giống như cách thức Bob thực hiện) và sau đó thay đổi trạng thái và phân cực gửi tới Bob. Điều này gây ra lỗi trong khóa mà Bob và Alice đang chia sẻ. Xác suất mà Eve chọn sai phân cực để giải mã là 50% và nếu Bob giải mã các photon bị chặn này với phân cực mà Alice gửi, Bob sẽ nhận được một kết quả ngẫu nhiên, một kết quả sai sẽ có xác suất là 50%. Xác suất một photon bị chặn tạo ra một lỗi trong khóa sẽ là 50% × 50% = 25%. Nếu Alice và Bob so sánh *n* bit trong

khóa đang chia sẻ (sau đó sẽ hủy chúng vì chúng không còn tính bảo mật nữa) thì xác suất nhận ra sự có mặt của Eve là 1- $(3/4)^n$ [54].

Ví dụ: Để phát hiện ra sự có mặt của Eve với xác suất là 0.9999999 thì Alice và Bob phải so sánh 72 bit.

-***Tấn công chia nhỏ số photon***: Eve sẽ chia một photon đơn hay một số lượng nhỏ các photon từ mỗi một bit truyền dẫn trên đường truyền cho việc giải mã và cho phép phần còn lại đi tới Bob. Điều này cho phép Eve giải mã các photon mà Eve đang có mà không làm ảnh hưởng tới các photon mà Bob đang giải mã. Cách giải quyết mà một số nghiên cứu đưa ra là phát đi các xung là mồi nhử để Alice và Bob có thể phát hiện được một cuộc tấn công kiểu chia nhỏ số photon.

-***Từ chối dịch vụ***: Cuộc tấn công thực hiện bằng cách cắt hay khóa đường truyền. Giải pháp được sử dụng để khắc phục các cuộc tấn công kiểu này là phát triển mạng QKD để có thể định tuyến lại thông tin bằng cách đường truyền thay thế khi bị gián đoạn.

-***Tấn công kiểu Trojan-house:*** Eve thăm dò bằng việc gửi đi một ánh sáng từ một kênh lượng tử và phân tích đường phản xạ. Các nghiên cứu gần đây đã chứng minh rằng Eve phát hiện được trạng thái pha mà Bob sử dụng với xác suất lên tới 90%.

1.2.3. Phân loại hệ thống QKD

Tùy thuộc vào cách thức thông tin được mã hóa, có thể phân loại QKD theo 2 loại chính là: QKD biến rời rạc (Discrete-Variable Quantum Key Distribution – DV-QKD) và QKD biến liên tục (Continuous-Variable Quantum Key Distribution – CV-QKD).

1.2.3.1 QKD biến rời rạc DV-QKD

Trong các hệ thống DV-QKD, thông tin về khóa được mã hóa vào các trạng thái rời rạc của mỗi một photon như pha hay phân cực và được biết như các tính chất của photon. Các photon sau khi mã hóa được truyền qua kênh lượng tử và các thiết bị tách photon đơn sẽ được sử dụng để tách các photon ở phía thu [30]. Tuy nhiên DV-QKD đòi hỏi kỹ thuật phức tạp và chi phí lớn, đây thực sự là những thách thức đối với phương pháp này. Ngoài ra, trong truyền thông sử dụng cáp quang truyền thống, để có thể truyền tín hiệu đi xa, người ta có thể dùng các bộ lặp trên đường truyền để

khắc phục hiện tượng suy hao tín hiệu, tăng được khoảng cách truyền dẫn. Tuy nhiên, nếu truyền tín hiệu trên kênh lượng tử, yêu cầu cần phải có các bộ lặp lượng tử được trang bị các bộ nhớ lượng tử. Công nghệ hiện nay chưa thực hiện được điều này [56]. Do đó, đây cũng là một hạn chế của DV-QKD. Giao thức BB84, giao thức có thể được coi là cơ sở trong phân phối khóa lượng tử, là giao thức QKD biến liên tục.

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 [24]. 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 [47].

Việc sử dụng phương thức mã hóa thông tin lượng tử cần truyền đi của CV-QKD thay vì kiểu các thông tin rời rạc của photon đã tạo ra một hướng tiếp cận mới cho các nghiên cứu về QKD. CV-QKD đã được chứng minh là đạt được độ bảo mật về mặt lý thuyết ngang với DV-QKD trong nghiên cứu [69] được công bố năm 2009 và nghiên cứu [47] công bố năm 2020. Các giao thức kiểu CV-QKD thể hiện một lợi thế lớn so với DV-QKD, đó là CV-QKD chỉ yêu cầu các công nghệ viễn thông tiêu chuẩn, điều này giúp cho hệ thống sử dụng giao thức CV-QKD dễ thực hiện hơn [51]. Thay vì phải sử dụng máy thu kiểu tách, đếm photon chuyên dụng như ở DV-QKD, CV-QKD chỉ yêu cầu sử dụng máy thu kiểu tách sóng coherent (homodyne hoặc heterodyne), đây là kiểu máy thu được sử dụng phổ biến trong truyền thông quang học truyền thống [24]. Các máy thu kiểu tách sóng coherent đem lại lợi thế về khía cạnh có thể đạt được tốc độ khóa cao hơn so với hệ thống sử dụng các giao thức DV-QKD [85]. Điều này chính là điểm khác biệt lớn giữa DV-QKD và CV-QKD khi xét trên khía cạnh cấu trúc máy thu. Ngoài ra, CV-QKD còn mang đến những ưu điểm vượt trội so với DV-QKD về mặt chi phí xử lý dữ liệu cũng như chi phí cho cả hệ thống [62].

Đã có nhiều nghiên cứu và đề xuất về các giao thức CV-QKD [12, 27, 32, 35, 49, 51, 52, 87, 88, 96, 97, 103, 104], các giao thức đề xuất đều dựa trên nguyên tắc cơ bản của mã hóa lượng tử trong giao thức BB84 do Bennett và Brassard đề xuất năm 1984 nhưng cũng có những sự thay đổi để phù hợp với các mục đích đề ra. Các giao thức CV-QKD đã được nghiên cứu cho đến hiện nay có thể phân loại theo các tiêu chí khác nhau. Nếu phân loại theo kiểu của bộ tách sóng sử dụng có loại giao thức sử dụng kiểu heterodyne và kiểu giao thức sử dụng kiểu homodyne. Nếu phân loại theo kiểu điều chế sẽ có giao thức cho các trạng thái đơn mode là Gauss hay không Gauss. Nếu phân loại theo các trạng thái phục vụ cho việc mã hóa thông tin có giao thức cho các trạng thái coherent đơn mode hay giao thức cho các trạng thái coherent 2 mode. Ngoài ra, có thể phân loại các giao thức CV-QKD theo kiểu của phương pháp sửa lỗi sử dụng. Trong các loại giao thức CV-QKD đã đề xuất, có loại dễ thực hiện hơn các loại khác nhưng cũng có loại đạt được tính bảo mật cao hơn các loại còn lại.

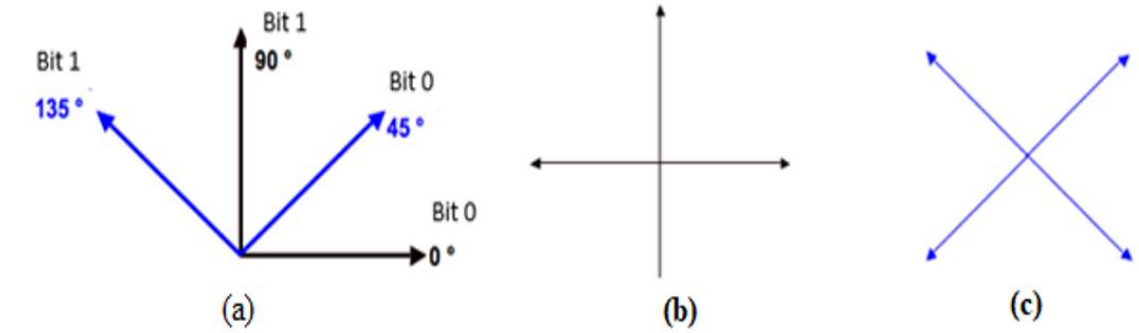
Giải pháp phòng chống tấn công được sử dụng trong các hệ thống CV-QKD

Trong CV-QKD, với sự hỗ trợ của Alice, Bob cũng có khả năng phát hiện sự tấn công đánh chặn và gửi lại của Eve vào quá trình truyền khóa giữa Alice và Bob. Cụ thể, Bob có thể tiết lộ một phần ngẫu nhiên các phép đo của Bob và Alice có thể cho Bob biết Alice đã gửi trạng thái nào cho phần ngẫu nhiên đó. Điều này cho phép Bob chỉ định đúng các giá trị đo lường của mình ở trạng thái phù hợp. Sau đó, Bob có thể vẽ biểu đồ phân phối và tính toán phương sai của phân phối. Nếu phương sai này khác phương sai dự kiến của trạng thái kết hợp giới hạn nhiễu lượng tử, Bob biết rằng đã xảy ra sự cố trong quá trình truyền và cho rằng Eve đã tác động các trạng thái lượng tử trên đường đi.

1.2.4. Giao thức BB84

Giao thức BB84 là giao thức QKD đầu tiên, giao thức này được đề xuất năm 1984 bởi Charles Bennet và Gilles Brassard. Giao thức BB84 dựa trên nguyên lý bất định của Heisenberg [10]. Cho tới ngày nay, BB84 vẫn là một trong những giao thức quan trọng nhất và là cơ sở cho các giao thức khác dựa trên nguyên lý bất định của

Heisenberg như B92, SSP hay SARG04. Ý tưởng cơ bản của giao thức là Alice truyền một khóa bí mật ngẫu nhiên tới Bob bằng việc gửi một chuỗi các photon, các bit trong khóa ngẫu nhiên này được mã hóa bằng sự phân cực của các photon. Nguyên lý bất định của Heisenberg đảm bảo rằng kẻ xâm nhập trái phép Eve không thể đo được các photon này và truyền chúng tới Bob mà không làm ảnh hưởng tới trạng thái của photon, cả Alice và Bob sẽ biết được sự hiện diện của Eve khi Eve cố gắng tìm cách xâm nhập trái phép vào đường truyền. Trong trường hợp này, khóa đang dùng sẽ bị hủy và một khóa mới sẽ được tạo ra để truyền.



Hình 1. 5. Mã hóa các bit trong giao thức BB84:(a)Sự phân cực của các photon, (b) Sự phân cực thẳng, (c) Sự phân cực xiên

Hình 1.5 mô tả cách mã hóa một bit vào trạng thái phân cực của một photon trong giao thức BB84. Chúng ta định nghĩa một bit là có giá trị là "0" khi trạng thái phân cực của photon là 0^0 (phân cực thẳng +) hoặc 45^0 (phân cực xiên X). Tương tự như vậy, bit có giá trị là "1" là khi trạng thái phân cực của photon là 90^0 (phân cực thẳng) hoặc 135^0 (phân cực xiên).

Bảng 1. 1. Ví dụ về tạo khóa chọn lọc trong giao thức BB84

Chuỗi bit của Alice	**0**	**1**	**1**	**0**	**1**	**0**	**0**	**1**
Hệ phân cực của Alice dùng để mã hóa	+	+	X	+	X	X	X	+
Trạng thái phân cực của Alice	→	↑	↖	→	↖	↗	↗	↑

Hệ phân cực của Bob dùng để giải mã.	+	X	X	X	X	X	+	+
Trạng thái phân cực của Bob dùng để giải mã.	→	↖	↖	↗	↖	↗	→	↑
Alice báo cho Bob biết hệ phân cực Bob dùng để giải mã đúng hoặc sai	Đúng	Sai	Đúng	Sai	Đúng	Đúng	Sai	Đúng
Khóa chọn lọc được tạo ra	**0**		**1**		**1**	**0**		**1**

Quá trình tạo khóa chọn lọc trong giao thức BB84 được minh họa ở Bảng 1.1.

Alice sẽ thực hiện truyền thông tin về khóa thô với Bob qua kênh lượng tử. Alice bắt đầu chọn các bit và trạng thái phân cực một cách ngẫu nhiên, hoặc theo kiểu phân cực thẳng hoặc theo kiểu phân cực xiên để mã hóa cho mỗi một bit trong chuỗi bit ngẫu nhiên tạo ra. Alice sẽ truyền mỗi một photon với một trạng thái phân cực tương ứng với mỗi bit tới Bob. Quá trình này nằm trong bước 1 của giao thức QKD BB84.

Khi các photon sau mã hóa được truyền tới Bob, Bob sẽ sử dụng các lăng kính tách tia để đọc các thông tin đã được mã hóa của các photon này. Với mỗi photon nhận được, Bob sẽ đọc trạng thái phân cực của photon bằng cách chọn ngẫu nhiên trạng thái phân cực. Với một photon, nếu trạng thái phân cực của Bob chọn trùng với trạng thái phân cực của Alice, Bob có thể giải mã được bit mà Alice gửi. Nếu Bob chọn sai trạng thái, không trùng với trạng thái phân cực của photon mà Alice gửi đi, Bob sẽ không thể giải mã được bit đó. Quá trình này nằm trong bước 2 của giao thức QKD BB84.

Bob sẽ gửi cho Alice thông tin về phân cực mà Bob sử dụng để xác định trạng thái của photon, Alice gửi phản hồi về các phân cực đúng và không đúng của Bob qua kênh công khai. Alice và Bob sẽ loại bỏ những bit tương ứng với các photon mà Bob sử dụng sai trạng thái phân cực để giải mã. Với giả thiết không có lỗi xảy ra hoặc không có bên thứ ba tác động vào photon, Bob và Alice sẽ thống nhất tạo ra một

chuỗi các bit được gọi là khóa chọn lọc. Quá trình này nằm trong bước 3 của giao thức QKD BB84.

Bảng 1.1 là mô tả một chuỗi bit Alice chọn phát đi, các trạng thái phân cực mà Alice dùng để mã hóa các bit, các trạng thái phân cực Bob dùng để giải mã và khóa chọn lọc được tạo ra sau khi Bob và Alice loại bỏ đi các bit mà Bob sử dụng sai trạng thái phân cực để giải mã. Trước khi quá trình kết thúc, Alice và Bob sẽ thực hiện thống nhất dựa trên một chuỗi ngẫu nhiên các bit để so sánh nhằm đảm bảo tính nhất quán. Nếu chuỗi bit là không thống nhất, chúng sẽ bị loại bỏ và các bit còn lại sẽ tạo thành khóa bí mật để chia sẻ giữa Alice và Bob. Trong trường hợp không có nhiễu hay quá trình giải mã không xảy ra lỗi, sự không thống nhất của các bit được so sánh sẽ chỉ ra sự có mặt của Eve trên kênh lượng tử. Đó là do Eve đang cố gắng tìm cách giải mã các photon được gửi từ Alice đi trước khi chúng tới Bob, cho dù Eve không có quyền truy cập. Eve bị phát hiện vì nguyên tắc không nhân bản lượng tử đảm bảo rằng Eve không thể nhân bản được một phần nào của các trạng thái mà Eve không biết. Bởi vì Eve không thể biết được chính xác trạng thái pha nào mà Alice dùng để mã hóa bit nên Eve bắt buộc phải đoán. Nếu Eve sử dụng trạng thái phân cực sai để giải mã, nguyên lý bất định của Heisenberg đảm bảo rằng các thông tin bị mã hóa trong các trạng thái phân cực khác sẽ bị mất. Do đó, khi các photon tới Bob, các trạng thái phân cực mà Bob sử dụng để giải mã là ngẫu nhiên và xác suất mà Bob giải mã sai là 50%. Giả sử xác suất Eve chọn sai phân cực là 50% để giải mã thì 25% các bit Bob giải mã được sẽ khác với Alice. Nếu Eve thực hiện giải mã trên tất cả các bit thì sau khi có n bit so sánh giữa Alice và Bob, khả năng giải mã thành công của Eve sẽ bị giảm xuống và xác suất Eve sẽ giải mã sai là $(¾)^n$ [54].

Trong trường hợp có lỗi xảy ra khi truyền khóa, các thông tin về phát hiện lỗi và sửa lỗi sẽ được sử dụng để sửa các lỗi này và tạo nên khóa không lỗi. Cuối cùng, Alice và Bob sử dụng các hàm băm để tạo ra một khóa mới, ngắn hơn sao cho Eve có được rất ít thông tin về khóa. Quá trình này được gọi là khuếch đại tính bảo mật. Quá trình này nằm trong bước 4 của giao thức QKD BB84.

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.

1.3.Truyền thông quang trong không gian tự do FSO

Quang không gian tự do FSO (Free Space Optics) còn có tên gọi là FSP (Free Space Photonics) hoặc quang không dây OW (Optical Wireless) liên quan đến việc truyền thông tin bằng ánh sáng trong dải tần nhìn thấy hoặc ánh sáng hồng ngoại trong môi trường không khí. So với hệ thống truyền thông sử dụng đường truyền sóng điện từ (Radio Frequence RF), một hệ thống FSO có những ưu điểm sau: có thể đạt được tốc độ truyền tải và tính bảo mật của dữ liệu cao, kích thước của anten nhỏ (gần bằng 1/10 lần kích thước của anten trong hệ thống sử dụng đường truyền sóng điện từ), mức tiêu thụ điện năng nhỏ (gần bằng 1/2 lần so với các thiết bị trong hệ thống sử dụng đường truyền sóng điện từ), không cần sử dụng cáp quang hay phải xin cấp phép dải phổ truyền như khi truyền sóng điện từ, tài nguyên băng thông còn lớn [17]. Theo công bố của nghiên cứu [79] vào tháng 10 năm 2021, hệ thống FSO có thể đạt tốc độ truyền dữ liệu tới 160 Gb/s. Ánh sáng mà hệ thống FSO truyền có thể tạo ra từ các đi-ốt phát quang (Light-Emitting Diode – LED) hoặc từ các đi-ốt laser (Laser Diode – LD). Các hệ thống FSO có bước sóng hoạt động trong dải từ 780 tới 1600 nm và sử dụng các bộ chuyển đổi quang sang điện và điện sang quang. Khi hệ thống FSO truyền ánh sáng laser, nguyên tắc hoạt động của hệ thống cũng giống như truyền tín hiệu quang sử dụng sợi quang, sự khác biệt duy nhất chỉ là môi trường truyền thông tin. Ánh sáng truyền qua không khí với tốc độ nhanh hơn khi nó truyền qua sợi quang, do đó người ta thường phân loại FSO như một tuyến thông tin quang có tốc độ truyền là tốc độ ánh sáng. FSO cũng được xem xét như một phương pháp thay thế cho việc truyền sóng điện từ theo tuyến truyền có tầm nhìn thẳng (Line of Sight – LoS) [44]. Kiểu truyền quang không dây phổ biến hiện nay là kiểu truyền mặt đất-mặt đất và kiểu truyền mặt đất-vệ tinh-mặt đất.

Một hệ thống truyền quang không dây được minh họa trong Hình 1.6, sẽ bao gồm ba thành phần chính là:

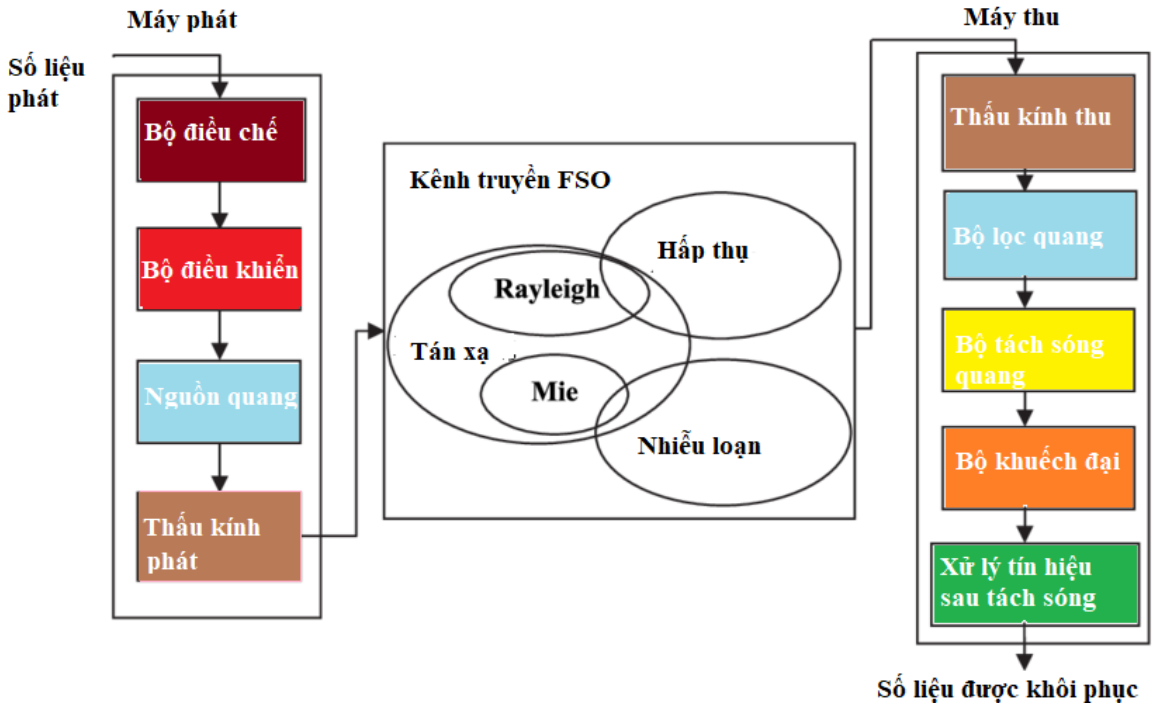
Bên phát để phát đi các thông tin được mã hóa dưới dạng ánh sáng thông qua môi trường không khí dựa trên luật Beer-Lambert. Bộ phát sử dụng phương thức điều chế cường độ theo kiểu điều chế trực tiếp hoặc điều chế pha/tần số/trạng thái phân cực thông qua bộ điều chế ngoài (bộ điều chế ngoài Mach Zehnder hay cách tử Bragg…). Tốc độ dữ liệu đạt được sau điều chế cao hơn khi sử dụng bộ điều chế ngoài so với bộ điều chế trực tiếp. Thấu kính phát sẽ tập hợp các tín hiệu sau điều chế từ nguồn quang sau đó phát tín hiệu quang này qua môi trường khí quyển để tín hiệu tới được bên phía thu.

Kênh truyền quang trong không gian tự do FSO bao gồm các yếu tố ảnh hưởng đến chất lượng đường truyền như: mây, mưa, khói bụi, nhiệt độ, sương mù, nhiễu loạn khí quyển,…Do tín hiệu truyền trên đường truyền là tín hiệu quang nên tín hiệu ở đầu vào kênh truyền thể hiện ở dạng công suất thay vì dạng biên độ như trong kênh nhiễu Gauss thông thường. Tín hiệu quang ở đầu vào kênh truyền sẽ có hai đặc trưng là (1) Tín hiệu không âm và (2) Giá trị trung bình của tín hiệu không vượt quá mức công suất tối đa quy định.

Bên thu để giải mã các tín hiệu quang về tín hiệu gốc truyền đi. Tín hiệu quang thu được là tổng hợp của tín hiệu quang phát đi, nhiễu, méo tín hiệu, bức xạ nền. Thấu kính thu được dùng để tập trung trường quang thu được. Kích thước của thấu kính thu và công suất tín hiệu thu sẽ xác định được lượng ánh sáng đưa vào bộ tách quang. Nếu gọi A là diện tích mặt thu của bộ thu, phương sai nhiễu lượng tử tỷ lệ thuận với A và công suất tín hiệu điện thu được tỷ lệ với A^2. Do đó, nếu tăng diện tích mặt thu A thì tăng được tỷ số tín hiệu trên nhiễu (Signal to Noise Ratio – SNR) của bộ thu, tuy nhiên, tăng A đồng nghĩa với việc tham số điện dung của bộ thu tăng lên. Khi điện dung của bộ thu tăng, băng thông của máy thu sẽ bị giảm đi. Trong hệ thống QKD-FSO, nếu kẻ nghe lén Eve có diện tích mặt thu thật lớn thì khả năng thu khóa chính xác sẽ cao hơn bên thu hợp lệ Bob. Tuy nhiên, việc tăng diện tích bề mặt thu không

làm tăng khả năng trùng nhau giữa khóa chọn lọc của Eve và Bob do sự khác nhau về việc thiết lập ngưỡng kép tại máy thu cũng như điều kiện kênh truyền của Eve và Bob không hoàn toàn giống nhau. Các phần tử chính trong bộ thu bao gồm:

- Thấu kính thu: Có nhiệm vụ tập trung trường quang trong không gian.
- Bộ lọc quang: Có tác dụng làm giảm bức xạ nền.
- Bộ tách sóng quang: Có chức năng chuyển đổi tín hiệu quang thành tín hiệu điện. Bộ tách quang có thể dùng loại PIN hoặc đi-ốt quang thác (Avalanche Photo Diode – APD).
- Xử lý sau tách sóng: Có nhiệm vụ khuếch đại, lọc, xử lý tín hiệu điện để đảm bảo tính chính xác của tín hiệu khôi phục.



Hình 1. 6. Sơ đồ khối của hệ thống FSO

Dựa vào cách thức hoạt động, có thể phân loại quá trình tách tín hiệu phía thu thành hai loại chính là:

- **Tách sóng trực tiếp**: Sử dụng cường độ hoặc công suất bức xạ quang đến bộ thu để tách tín hiệu. Cường độ tín hiệu điện thu được sau bộ tách quang tỷ lệ với

cường độ hay công suất quang ở đầu vào. Ưu điểm của kiểu tách sóng trực tiếp là đơn giản, phù hợp với hệ thống quang sử dụng phương pháp điều chế cường độ.

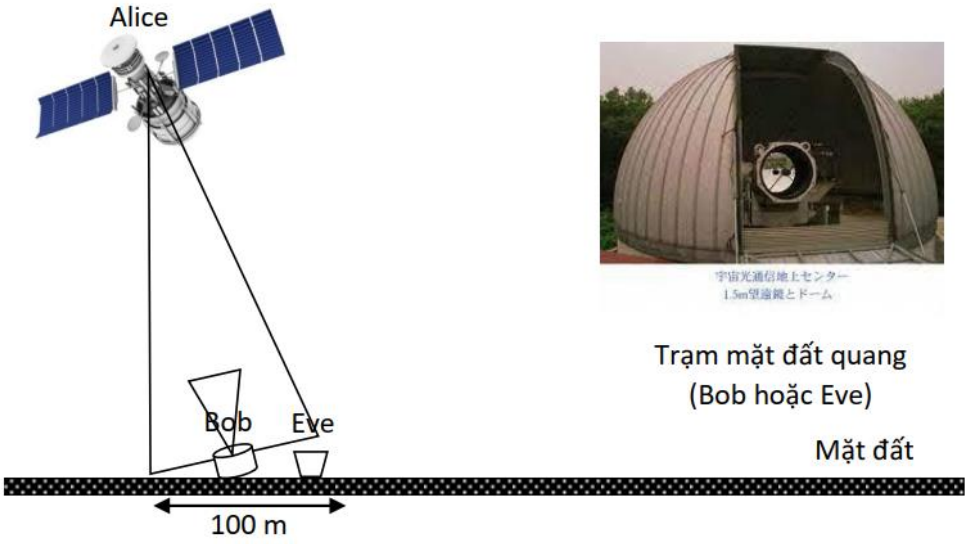
- **Tách sóng coherent**: Dựa trên nguyên tắc trộn các sóng ánh sáng. Trường tín hiệu quang tới sẽ được trộn với trường tín hiệu quang nội được tạo ra bởi máy thu. Nếu tần số của bộ dao động nội bằng tần số trường tín hiệu quang tới, bộ thu được gọi là **homodyne**. Nếu hai tần số này khác nhau, bộ thu được gọi là **heterodyne**. Một điều đáng chú ý là không có yêu cầu về pha của bộ dao động nội trong các máy thu quang kiểu coherent phải trùng với pha của tín hiệu trường quang đến. Đây là điều khác biệt của máy thu coherent quang với máy thu coherent trong truyền thông vô tuyến truyền thống. Bộ thu coherent có ưu điểm là dễ dàng khuếch đại tần số trung tần, khi điều chỉnh công suất bộ dao động nội ở máy thu thì tỷ số SNR có thể tăng theo.

1.4. Truyền thông quang trong không gian tự do sử dụng vệ tinh

Truyền thông quang trong không gian tự do FSO đang phát triển và hứa hẹn mang lại đường truyền tốc độ dữ liệu cao hơn một cách đáng kể, cùng với đó kích thước, trọng lượng của thiết bị cũng như công suất thấp hơn nếu so với truyền thông vô tuyến truyền thống. Tuy nhiên, giải pháp sử dụng FSO mặt đất chỉ có thể hỗ trợ khoảng cách truyền ngắn. FSO sử dụng vệ tinh đã được nghiên cứu trong nhiều thập kỷ gần đây và được tin tưởng mạnh mẽ sẽ thực hiện được nhiệm vụ liên lạc trong một khoảng cách truyền dẫn dài như giữa các quốc gia với nhau. Vệ tinh sẽ làm nhiệm vụ chuyển tiếp thông tin trong các hệ thống QKD-FSO. Trong truyền thông quang không dây sử dụng vệ tinh, sự phân kỳ của chùm tia hẹp trong truyền thông FSO sẽ yêu cầu tính định hướng chính xác cao hơn với tính chính xác trong định hướng truyền thông vô tuyến. Độ chính xác điển hình thường rơi vào một vài trăm μrad [45]. Khi tính định hướng cao đã được bảo đảm, các trạm phát Alice nằm trên vệ tinh sử dụng trong truyền thông FSO cũng không phải lo lắng về việc can nhiễu giữa các đường truyền với nhau. Do đó, mỗi một vệ tinh có thể đáp ứng được lượng băng thông như mong muốn.

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

Có thể hoặc sử dụng đường truyền cáp quang hoặc đường truyền quang không dây để phân phối khóa bí mật trong hệ thống CV-QKD giữa phía phát và phía thu. Tuy nhiên, hệ thống QKD sử dụng cáp quang bị giới hạn trong vài trăm km với tốc độ truyền khóa rất thấp do suy hao và các vấn đề về bảo toàn tính phân cực [22]. Theo công bố nghiên cứu năm 2021, Mirko Pittaluga và các cộng sự đã thử nghiệm thành công hệ thống phân phối khóa lượng tử qua kênh cáp quang có chiều dài đường truyền lên tới 605 km [64]. So với sợi quang, hiệu ứng tán sắc của các đường truyền FSO là không đáng kể, do đó sự phân cực của photon khi lan truyền trong khí quyển được bảo toàn, hệ thống truyền quang không dây linh động và mang lại chi phí thấp hơn. Để tăng khoảng cách truyền dẫn, hệ thống QKD-FSO có thể sử dụng các khinh khí cầu nhưng phương thức này chỉ hỗ trợ cho các khoảng cách truyền dẫn không dài. Việc sử dụng vệ tinh làm phương tiện chuyển tiếp là một giải pháp để tăng cự ly truyền dẫn đạt được xa hơn nữa, đáp ứng được xu hướng toàn cầu hóa mạng QKD trong tương lai.



Hình 1. 7. Kịch bản truyền tín hiệu từ Alice đến Bob với sự có mặt của Eve

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 còn có lợi thế về khả năng an ninh. Một điều quan trọng cần chú ý là hình thức tấn công người

ở giữa rất khó thực hiện đối với hệ thống QKD-FSO dựa trên vệ tinh với lý do như sau: Hệ thống FSO hoạt động dựa trên nguyên tắc truyền dẫn tầm nhìn thẳng (LOS), do búp sóng laser có kích thước hẹp nên yêu cầu nghiêm ngặt về việc đồng chỉnh, giữ thẳng hướng giữa bộ thu và bộ phát. Nhờ đặc tính đó và hệ thống FSO vẫn luôn được coi là có khả năng an ninh cao hơn các hệ thống truyền thông sử dụng sóng vô tuyến khác. Như minh họa trong Hình 1.7, Eve muốn thu lén được tín hiệu từ Alice, Eve phải nằm trong vùng phủ (footprint) của Alice. Với hệ thống FSO vệ tinh thực tế đang được triển khai, ví dụ SOTA tại NICT (Nhật Bản) [16], đường kính footprint chỉ trong khoảng 100 m và kích thước trạm mặt đất khá lớn (đường kính thấu kính thu cỡ 50 cm kèm theo hệ thống dò, bắt và bám tín hiệu) thì việc phát hiện có trạm thu lén là hết sức dễ dàng bằng mắt thường hoặc camera an ninh.

Ngoài ra, để tăng cường tính an ninh của hệ thống QKD-FSO, trong các hệ thống CV-QKD thường lựa chọn các tham số của hệ thống như tham số công suất phát nhỏ, đủ để máy thu hợp pháp tách được bit với QBER đạt yêu cầu tối thiểu. Mức công suất phát nhỏ được sử dụng với mục đích thông qua ảnh hưởng của nhiễu tạp để kẻ thu lén Eve khó có thể thu được chính xác toàn bộ chuỗi bit. Eve muốn thu được chính xác chuỗi bit tương ứng với chuỗi trạng thái pha đã phát đi, cần có giả thiết là nhiễu tạp đủ nhỏ. Tuy nhiên, trong thực tế, ảnh hưởng mạnh của nhiễu loạn khí quyển và các loại nhiễu tạp trong máy thu quang như tạp âm lượng tử, tạp âm ánh sáng nền, tạp âm nhiệt…sẽ khiến cho Eve khó tách chính xác được toàn bộ chuỗi bit. Nếu Eve cũng sử dụng máy thu coherent, Eve sẽ phải sử dụng laser dao động nội công suất lớn và tạp âm lượng tử do laser dạo động nội gây ra đã được chứng minh là mạnh hơn rất nhiều so với tạp âm lượng tử do tín hiệu quang thu được. Khác với hệ thống thông tin sử dụng sợi quang, tạp âm ánh sáng nền có ảnh hưởng mạnh với hệ thống truyền thông quang qua không gian tự do FSO do ánh sáng mặt trời và các nguồn ánh sáng khác lọt vào bộ thu quang.

Đường truyền FSO phải đối mặt với một số ảnh hưởng đến từ môi trường không gian tự do, 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)

Tỷ lệ lỗi bit lượng tử được định nghĩa là tỉ số của xác suất mà Bob phát hiện sai bit "0" và "1" (P_{error}) với xác suất chọn lọc P_{sift}. P_{sift} là xác suất Bob có thể quyết định các bit nhận được là "0" hoặc "1", đó chính là xác suất mà Bob sử dụng cùng trạng thái phân cực cơ sở như Alice để đo các photon thu, từ đó Bob giải mã chuỗi bit được gọi là khóa lọc. P_{error} là xác suất mà có một số bit sai trong khóa chọn lọc, gây ra bởi đường truyền, tạp âm và/hoặc sự can thiệp của Eve . P_{error} là xác suất mà Bob tách sai, nghĩa là khi Alice gửi đi bit "1", Bob lại giải mã ra kết quả là "0" và ngược lại. Theo đó, QBER được biểu diễn như sau [30]:

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

với:

$$P_{error=}\, P_{A,B}(0,1) + P_{A,B}(1,0) \tag{1.2}$$

$$P_{sift=}\, P_{A,B}(0,1) + P_{A,B}(1,0) + P_{A,B}(0,0) + P_{A,B}(1,1) \tag{1.3}$$

với:

$P_{A,B}(i,j)$ là xác suất mà tại một thời điểm bit ở bên Alice là "*i*" nhưng bit bên Bob là "*j*" và được xác định theo công thức:

$$P_{A,B} = P_A(i)P_{B|A}(j|i) \tag{1.4}$$

trong đó, $P_A(i)$=1/2 là xác suất mà Alice gửi đi bit "0" hay bit "1" được giả sử là bằng nhau. $P_{B|A}(j|i)$ là xác suất mà Bob nhận được bit "*j*" trong khi Alice gửi đi bit "*i*". QBER sẽ xác định tỷ lệ lỗi bit trong khóa chọn lọc. QBER có giá trị khác nhiều so với giá trị tỷ lệ lỗi bit BER là 10^{-9} thường được biết đến trong truyền thông quang.

QBER được dùng để phân biệt với tỷ lệ lỗi bit (Bit Error Rate – BER) dùng trong truyền thông quang thông thường.

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. 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, được tính như sau:

$$S = I(A;B) - I(A;E) \tag{1.5}$$

trong đó, $I(A;B)$ và $I(A;E)$ là tương ứng là lượng thông tin mà Alice và Bob, Alice và Eve chia sẻ.

Giả thiết, bit "0" và "1" có xác suất truyền như nhau, thông tin được chia sẻ giữa Alice và Bob được tính theo công thức như sau [36]:

$$\begin{aligned} I(A;B) = p\log_2(p) + (1-p-q)\log_2(1-p-q) \\ -\ (1-q)\log_2(1-q) + 1 - q \end{aligned} \tag{1.6}$$

Trong công thức (1.6): $p=P_{A,B}(0,0)=P_{A,B}(1,1)$;

$$q=0{,}5-P_{A,B}(0,0)-P_{A,B}(0,1).$$

Thông tin chung giữa Alice và Eve được tính theo công thức (1.7):

$$I(A;E) = 1 + p_e\log_2(p_e) + (1-p_e)\log_2(1-p_e) \tag{1.7}$$

trong đó, p_e là xác suất mà Eve phát hiện đúng các bit được truyền đi từ Alice, p_e được xác định như sau:

$$p_e = 0.5 - P_{A,E}(0,1) = 0.5\,P_{A,E}(1,0) \tag{1.8}$$

Khoảng cách đường truyền giữa máy phát và máy thu

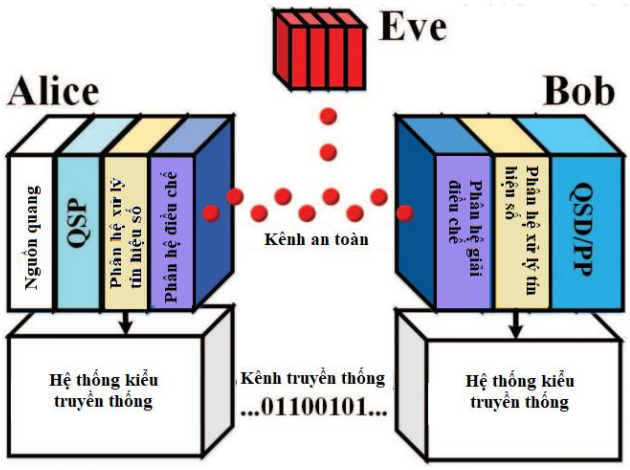
Trong hệ thống QKD-FSO, Alice được đặt trên vệ tinh và Bob nằm ở phía trạm mặt đất. Đường truyền giữa Alice và Bob trong hệ thống QKD-FSO là đường truyền trong tầm nhìn thẳng. Độ dài của khoảng cách đường truyền giữa phía phát và phía

thu bị ảnh hưởng bởi các yếu tố thuộc môi trường truyền dẫn như suy hao trong không gian tự do, suy hao khí quyển và đặc biệt là nhiễu loạn khí quyển.

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. Hình 1.7 mô tả cấu trúc của hệ thống QKD-FSO theo các phân hệ con.

Mặc dù hệ thống QKD được cho là đạt được bảo mật vô điều kiện dựa trên các định luật của cơ học lượng tử, nhưng công nghệ thiết kế phần cứng của hệ thống cũng có những giới hạn nhất định, chính những giới hạn này làm tính bảo mật của hệ thống có thể khác so với tính bảo mật lý thuyết của hệ thống. Trong thực tế, những hạn chế về mặt kỹ thuật và sự không hoàn hảo của phần cứng được kẻ nghe lén Eve tận dụng để thực hiện một số cuộc tấn công vào hệ thống [40].



Hình 1. 8. Cấu trúc hệ thống QKD-FSO theo các phân hệ con

1.7.1. Nguồn quang

Nguồn quang có một số yêu cầu về đặc tính vật lý và kỹ thuật quan trọng. Các tham số ảnh hưởng tới hiệu năng của hệ thống QKD-FSO là độ rộng búp sóng quang, trạng thái quang lượng tử được tạo ra bởi nguồn, độ ổn định bước sóng quang. Đối với tất cả các nguồn quang được sử dụng, hiệu suất và các phần tử quang phi tuyến tính là một vấn đề quan trọng đối với thiết kế và sản xuất. Hơn nữa, các nguồn quang

cũng phải phù hợp với đường truyền FSO trong hệ thống QKD-FSO. Do đó, việc sử dụng xung ánh sáng yếu là kỹ thuật phổ biến cho các ứng dụng FSO. Về cơ bản, hiệu suất của các nguồn quang học được cải thiện dựa trên việc sử dụng các vật liệu, cấu trúc mới, các thiết bị lượng tử cho phép tạo ra trạng thái lượng tử gần như lý tưởng.

1.7.2. Các bộ tách quang

Nhiễu điện và độ lợi của bộ tách quang ảnh hưởng đến tốc độ truyền dẫn. Để có thể giảm nhiễu điện và tối đa hóa độ lợi của bộ tách quang, các vật liệu mới trong chế tạo bộ tách quang và các cải thiện trong thiết kế cho bộ tách quang được sử dụng. Khả năng tách sóng một tín hiệu tới của một bộ tách sóng quang bị hạn chế bởi các sự thăng giáng của tín hiệu và nhiễu. Nếu công suất tín hiệu quang tới nhỏ hơn công suất nhiễu, các tín hiệu sẽ không thể được phân biệt một cách rõ ràng. Hai loại nguồn nhiễu quan trọng nhất trong bộ thu quang là nhiễu lượng tử và nhiễu nhiệt. Nhiễu lượng tử xuất hiện do tính chất ngẫu nhiên của quá trình chuyển đổi photon thành điện tử và nhiễu nhiệt xuất hiện do chuyển động ngẫu nhiên của các electron, nó luôn tồn tại ở bất kỳ nhiệt độ xác định nào. Thực tế, bên cạnh việc có nhiều bộ tách quang mới được nghiên cứu và áp dụng thì bên phía thu vẫn có thể sử dụng kỹ thuật tách sóng coherent do ưu điểm về tính khuếch đại và lọc phổ sẵn có của kỹ thuật coherent.

1.7.3. Các giao thức QKD

Các giao thức QKD mô tả các tác vụ hoặc bước cụ thể (thuật toán) cần thiết để tạo ra khóa lượng tử cuối cùng là khóa bí mật. Các giao thức và hiệu suất của chúng phụ thuộc vào thông tin thống kê (biến rời rạc DV hay biến liên tục CV) liên quan đến trạng thái lượng tử được sử dụng.

Mỗi một loại giao thức QKD có một nguyên lý bảo mật cụ thể, hoặc là dựa vào nguyên lý bất định Heisenberg (điển hình là giao thức BB84, B92) hoặc là dựa vào hiệu ứng rối lượng tử (ví dụ giao thức E91). Giao thức BB84 sử dụng 4 trạng thái phân cực để mã hóa thông tin khóa và giao thức B92 chỉ cần sử dụng 2 trạng thái phân cực không vuông góc để mã hóa thông tin khóa cần truyền đi. Trong giao thức E91, việc sử dụng các trạng thái của lượng tử để trao đổi khóa giống cơ bản với giao

thức BB84. Tuy nhiên, thay vì Alice gửi các photon đã được mã hóa cho Bob, một trạm trung gian sẽ gửi một cặp photon được mã hóa, trong đó một photon gửi cho Bob và một photon gửi cho Alice. Trong thực tế, một số giao thức tăng tính bảo mật, đạt được tốc độ truyền khóa nhất định trong một khoảng cách truyền ngắn, một số giao thức khác lại cải thiện về khoảng cách truyền dẫn mà không cải thiện được tính bảo mật của hệ thống.

1.7.4. Các kỹ thuật và cấu trúc trong QKD

Các kỹ thuật và cấu trúc được sử dụng trong QKD liên quan đến các thiết lập khác nhau, các quy luật và các thiết bị để thực thi một giao thức QKD cụ thể nào đó. Khi triển khai một hệ thống QKD-FSO, bước đầu tiên là chọn lựa giao thức QKD, tiếp theo cấu trúc chung của hệ thống được đề xuất và thực hiện. Các kỹ thuật là những quy tắc hoạt động để nâng cao hiệu năng của một hệ thống QKD-FSO. Việc lựa chọn giao thức QKD phù hợp, các kỹ thuật xử lý tín hiệu như mã hóa, ghép kênh,.. hay việc các kỹ thuật trong cải tiến về thiết bị như bộ tách sóng quang, bộ cải thiện độ chính xác trong sự định hướng giữa trạm phát và trạm thu …đều góp phần cải thiện hiệu năng của một hệ thống QKD-FSO.

1.7.5. Kênh truyền FSO

Kênh truyền FSO trong hệ thống QKD-FSO có ảnh hưởng rất lớn đến hiệu năng của toàn hệ thống. Ảnh hưởng của kênh truyền FSO chủ yếu đến từ nguyên nhân môi trường truyền dẫn. Ngoài hiện tượng tuyết và mưa gây suy hao trên đường truyền quang trong hệ thống QKD-FSO, đường truyền FSO còn chịu ảnh hưởng mạnh bởi hiện tượng sương mù và nhiễu loạn khí quyển. Ngoài ra, nhiễu dòng tối và nhiễu nền của quá trình bức xạ quang cũng có thể dẫn tới giảm hiệu năng của kênh truyền FSO trong hệ thống QKD-FSO.

1.7.6. Phân hệ xử lý tín hiệu số

Phân hệ xử lý tín hiệu số được triển khai trong các hệ thống QKD-FSO thông thường được tạo thành từ các nhiệm vụ cơ bản, cụ thể như: bộ điều biến biên độ/pha, bộ tạo số ngẫu nhiên thực, thực hiện các thuật toán để bảo mật, sửa lỗi .. trong quá

trình chia sẻ khóa giữa Alice và Bob. Phân hệ xử lý tín hiệu số yêu cầu một số thông số kỹ thuật quan trọng để đảm bảo mức độ bảo mật và đảm bảo tốc độ truyền khóa của hệ thống QKD. Các thông số kỹ thuật của các mảng cổng lập trình được theo trường (Field Programmble Gate Array – FPGA) sử dụng trong phân hệ xử lý tín hiệu số có tác động đến hiệu suất của hệ thống QKD. Việc đồng bộ hóa được cải thiện dựa trên các thiết bị chính xác và tốc độ cao có thể làm giảm tỷ lệ lỗi bit lượng tử QBER và tăng tốc độ khóa bí mật được chia sẻ. Ngoài ra, tốc độ khóa bí mật có mối quan hệ quan trọng với hiệu suất của các phân hệ xử lý số ngẫu nhiên. Các module cho các giai đoạn cụ thể của giao thức được sử dụng (sàng lọc, sửa lỗi,..) cũng hỗ trợ nâng cao hiệu năng của hệ thống QKD.

Như vậy, có thể nhận thấy nếu xét một cách toàn diện, các tham số liên quan đến các phân hệ con trong toàn bộ hệ thống QKD-FSO đều có ảnh hưởng tới hiệu năng của hệ thống nhưng do phạm vi nghiên cứu của đề tài, luận án sẽ xem xét tới ảnh hưởng của các yếu tố gây suy hao trên kênh truyền, nhiễu loạn khí quyển, tạp âm tại máy thu, phương thức truyền dẫn sẽ được sử dụng trong giao thức CV-QKD.

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, các nghiên cứu về truyền thông sợi quang và truyền thông quang qua không gian FSO đã và đang được tiến hành tại nhiều trường Đại học và Viện nghiên cứu. Về công nghệ FSO, các công trình nghiên cứu liên quan bao gồm nghiên cứu nâng cao chất lượng tuyến thông tin quang không dây mặt đất trong điều kiện khí hậu Việt Nam [2]; nghiên cứu cải thiện hiệu năng hệ thống FSO mặt đất [23, 63, 86]. Nghiên cứu ứng dụng công nghệ FSO trong thông tin vệ tinh [92]. Tuy nhiên, các nghiên cứu nêu trên chỉ tập trung vào ứng dụng công nghệ FSO trong việc truyền tải các bit số liệu.

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. Hiện tại, trên các trang Web về an ninh mạng của Việt Nam cũng chỉ có các bài giới thiệu chung về khái niệm phân phối khóa lượng tử qua không gian tự do, liệt kê các kết quả đạt được trong triển khai thử nghiệm của một số nước trên thế giới.

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.

Hệ thống QKD-FSO trên mặt đất.

Việc sử dụng các hệ thống FSO trên mặt đất cho QKD đã được nghiên cứu [28, 60, 84, 85]. Tuy nhiên, giải pháp này chỉ có thể hỗ trợ cho phân phối khóa lượng tử với khoảng cách truyền từ máy phát tới máy thu là ngắn.

Năm 2016, Alberto Carrasco-Casado và các cộng sự tại Tây Ban Nha đã tiến hành thử nghiệm hệ thống phân phối khóa lượng tử qua không gian tự do QKD-FSO tại Madrid (Tây Ban Nha) với khoảng cách giữa bên phát và bên thu là 300 m, chạy thử hệ thống trong vòng 24 giờ cho ra kết quả tỷ lệ QBER dao động trong khoảng từ 0,02 đến 0,08. Đây là con số khá lớn, không thể áp dụng trong một hệ thống thực tế [5].

Vào năm 2017, cuộc trình diễn thử nghiệm QKD đầu tiên từ trạm phát mặt đất đến máy bay đang di chuyển đã được ghi nhận với khoảng cách 3 – 10 km và tạo ra các khóa bí mật có chiều dài 868 KB, tỷ lệ lỗi QBER từ 0,03 đến 0,05 [66].

Hệ thống QKD-FSO dựa trên vệ tinh

Các nghiên cứu về tính khả thi của truyền thông lượng tử qua vệ tinh đã được tiến hành từ thập kỷ trước trong các nghiên cứu [15, 21, 41, 82, 89, 91]. Sự kiện lần đầu hoàn thành triển khai QKD từ vệ tinh đến mặt đất được thực hiện tại Trung Quốc với vệ tinh Micius đã đánh dấu một cột mốc quan trọng trong hướng nghiên cứu này. Cuối năm 2017, BB84 đã được triển khai thành công qua các liên kết từ vệ tinh Micius

đến các trạm mặt đất ở Trung Quốc và Áo. Các khóa được kết hợp và kết quả đã được sử dụng để truyền hình ảnh và video giữa Bắc Kinh (Trung Quốc) và Vienna (Áo) [65]. Trong nghiên cứu của [100] tại Trung Quốc, một đường truyền lượng tử được thiết lập từ vệ tinh Micius ở quỹ đạo tầm thấp LEO tới ba trạm mặt đất ở Delingha, Urumqi và Lijiang. Khoảng cách từ Delingha đến Lijiang là 1203 km, tổng chiều dài đường truyền khi có sự tham gia của vệ tinh dao động từ 1600 km đến 2400 km. Nghiên cứu này sử dụng giao thức QKD dựa trên kiểu rối lượng tử.

Cũng vào năm 2017, Robert Bedington, Juan Miguel Arrazola1 và Alexander Ling đã tiến hành thử nghiệm mô hình truyền khóa lượng tử QKD qua vệ tinh sử dụng cửa sổ quang 800 nm [9]. Thử nghiệm được tiến hành trên nhiều kịch bản đường truyền khi đường kính ăng-ten tại trạm phát/thu mặt đất là 1 m, đường kính ăng-ten của trạm thu/phát trên vệ tinh có đường kính 30 cm, vệ tinh ở quỹ đạo địa tĩnh (Geosynchronous Equatorial Orbit – GEO) hay quỹ đạo Trái đất tầm thấp (Low Earth Orbit – LEO). Thử nghiệm đạt được cự ly truyền lớn nhất là 40.000 km, tốc độ truyền khóa khá nhỏ (lớn nhất là 220 Kb/s khi suy hao quang là 0 dB và bằng 0 Kb/s khi suy hao quang trên đường truyền là 20 dB), tỷ lệ lỗi QBER lớn (nhỏ nhất là 0,02 khi suy hao quang là 0 dB và lên tới 0,11 khi suy hao quang là 30 dB, đặc biệt khi suy hao quang là 60 dB, tỷ lệ QBER đạt tới con số là 0,5). Ngoài ra, thử nghiệm cũng có cấu trúc máy thu lớn vì sử dụng phương thức mã hóa DV-QKD.

Năm 2020, trong nghiên cứu [47] các tác giả sử dụng giao thức CS-QKD, máy thu kiểu homodyne và kiểu heterodyne cho đường truyền từ vệ tinh xuống trạm mặt đất, nghiên cứu đạt được kết quả có tốc độ truyền khóa xấp xỉ 866 Mb/s.

Trong công bố năm 2021 của nghiên cứu [20], nhóm nghiên cứu sử dụng giao thức CV-QKD với đề xuất phân tích dữ liệu dựa trên việc chia nhỏ quỹ đạo đã cải thiện được tốc độ tạo khóa bí mật, hệ thống sử dụng vệ tinh trên quỹ đạo LEO, có đường truyền từ vệ tinh tới trạm mặt đất là 2000 km.

Cũng trong năm 2021, nghiên cứu [46] tập trung vào kỹ thuật xác định tối ưu cấu hình các vệ tinh để có thể phủ sóng liên tục và cân bằng được giữa số vệ tinh cần

dùng với tốc độ truyền thông tin lượng tử.

Các nghiên cứu cải thiện hiệu năng hệ thống QKD-FSO.

Năm 2017, nhóm nghiên cứu tại trường đại học Southampton (Mỹ) kết hợp với nhóm nghiên cứu tại trường đại học Aizu (Nhật Bản) đề xuất hệ thống NC-CQKD-FSO cho truyền khóa lượng tử qua không gian tự do với kết quả cải thiện về tốc độ truyền khóa cũng như giảm tỷ lệ lỗi QBER [60].

Năm 2018, tại phòng nghiên cứu US Naval Research Laboratory tại Washington đã thử nghiệm hệ thống QKD-FSO với việc sử dụng bộ phản xạ retro hình mắt mèo tại phía phát để mã hóa các trạng thái lượng tử dưới dạng điều chế biên độ, bước sóng làm việc từ 1532nm đến 1537nm [68]. Thử nghiệm này cho phép giảm nhỏ công suất tại phía máy thu, có khả năng chống được các cuộc tấn công dạng "Trojan horse" tuy nhiên tỷ lệ QBER đạt được nhỏ nhất là 0,05. Giá trị QBER đạt được trong thử nghiệm là khá lớn, không khả thi khi triển khai hệ thống trong thực tế.

Để giảm được hệ số lỗi bit lượng tử QBER, nghiên cứu [14] đã đề xuất sử dụng phương pháp sửa lỗi hướng phát (Forward Error Correction – FEC) trong quá trình sửa lỗi khi nhận được khóa ở bên thu và [4] đã nghiên cứu phát triển dựa trên nguyên tắc này.

Trong nghiên cứu [85], phương pháp điều chế cường độ sóng mang phụ (Subcarrier Intensity Modulation – SIM) sử dụng khóa dịch pha nhị phân (Binary Phase Shift Keying – BPSK) được đề xuất cho hệ thống phân phối khóa lượng tử QKD-FSO.

Trong khi đó nghiên cứu của [19] và [67] sử dụng sóng mang trực tiếp thay vì sóng mang phụ RF, tín hiệu được điều chế theo phương pháp điều chế khóa dịch pha QPSK và sử dụng máy thu tách sóng kiểu homodyne.

Trong nghiên cứu của Lopez-Leyva JA [38], để giảm ảnh hưởng của nhiễu loạn khí quyển tới hiệu năng của đường truyền FSO trong hệ thống QKD-FSO, nhóm nghiên cứu sử dụng mã kiểm tra chẵn lẻ mật độ thấp (Low Density Parity Check –

LDPC) có độ lợi của mã thay đổi theo mức độ nhiễu loạn khí quyển. Kết quả cho thấy tốc độ truyền khóa được duy trì trong một dải của mức độ nhiễu loạn khí quyển.

Năm 2019, trong nghiên cứu [39], các tác giả đã sử dụng phương pháp điều chế 2PolSK-BPSK, hệ thống hoạt động ở bước sóng 1550,1 nm, cả Alice và Bob đều sử dụng bộ tạo các chuỗi số ngẫu nhiên, tỷ lệ lỗi bit lượng tử đạt được có giá trị từ 0,001 đến 0,5.

Trong công bố năm 2020, nghiên cứu [95] đã sử dụng phương pháp bù pha trên thực nghiệm độ dài kênh truyền không dây thực tế là 150m trong khu vực ký túc xá của đại học Shanghai Jiao Tong với máy phát đặt tại tầng 4 của tòa nhà SEIEE và máy thu đặt tại tầng 2 của tòa nhà khác ở gần đó.

Năm 2021, trong nghiên cứu [50] đã sử dụng cải thiện hiệu năng hệ thống bằng cách sử dụng bộ khuếch đại tuyến tính lai ghép, độ dài đường truyền tối đa đạt được là 120 km.

Theo kết quả được công bố vào tháng 12 năm 2021, nhóm tác giả của nghiên cứu [7] đã cải thiện hiệu năng hệ thống QKD-FSO bằng cách sử dụng phương pháp điều chế vị trí xung đa mức MMPM dựa trên giao thức cơ sở BB84 với kịch bản sử dụng điều chế từ 2 đến 16 mức, các điều kiện nhiễu loạn đường truyền khác nhau, khoảng cách đường truyền từ 1 đến 4 km, tốc độ cao nhất của khóa thô và khóa bí mật là 85 Mb/s.

Nghiên cứu về hệ thống QKD đa kênh

Mặc dù đã có rất nhiều các nghiên cứu lý thuyết và thực nghiệm về QKD nhưng các nghiên cứu này tập trung chủ yếu vào các hệ thống QKD đơn kênh. Lý do chính là các hệ thống QKD thường sử dụng QKD biến rời rạc DV-QKD, thông tin khóa được mã hóa vào trạng thái rời rạc của một photon. Các hệ thống sử dụng DV-QKD đòi hỏi phải sử dụng các thiết bị tách đơn photon phức tạp và khó thực hiện trong cả các hệ thống thông tin quang đơn kênh và đa kênh. Một hệ thống ghép kênh phân chia theo bước sóng WDM ba kênh sử dụng đồng thời đi-ốt quang thác và bộ thu đơn photon đã được thử nghiệm và đạt được tốc độ truyền khóa bí mật là 208 Kb/s qua

45 km sợi quang thường với mức suy hao 14,5 dB [101]. Ngược lại, trong các hệ thống CV-QKD, việc mã hóa thông tin vào các trạng thái kết hợp của các xung ánh sáng yếu hoặc sóng mang phụ dễ thực hiện hơn. Đó là do các hệ thống CV-QKD tương thích với các công nghệ viễn thông quang tiêu chuẩn và cho phép tốc độ tạo khóa cao hơn [31, 36, 94]. Tận dụng ưu điểm của CV-QKD, Jian Fang và các cộng sự đã đề xuất hệ thống CV-QKD đa kênh sử dụng ghép kênh sóng mang phụ SCM. Hệ thống cho phép phân phối nhiều kênh CV-QKD độc lập qua sợi quang với một nguồn laser và nhiều bộ điều chế pha [25]. Tương tự, kỹ thuật ghép kênh phân chia theo tần số trực giao (Orthogonal Frequency Division Multiplexing – OFDM) cũng được đề xuất cho hệ thống CV-QKD từ vệ tinh tới trạm mặt đất thông qua kênh quang không gian tự do FSO [55]. Giải pháp này cũng sử dụng nhiều sóng mang phụ truyền tải song song thay vì truyền dẫn đơn kênh.

Năm 2020, Sharma và các cộng sự trong nghiên cứu [75] đã đề xuất sử dụng kỹ thuật đa truy nhập theo mã cho lượng tử. Trong năm 2021, nhóm nghiên cứu của Rezai đã đề xuất mạng đa truy nhập phân chia theo mã cho lượng tử dựa trên mã hóa và giải mã quang phổ của các xung ánh sáng lượng tử [70].

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, điều này dẫn tới hệ thống chỉ thực hiện trong thử nghiệm tại các phòng nghiên cứu, chưa áp dụng trong thực tế được.

- 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. Trong khi đó các máy thu của hệ thống QKD sử dụng giao thức DV-QKD thường có kiến trúc khá phức tạp, đòi hỏi sử dụng các phần tử quang có cấu trúc đặc biệt, có giá thành cao,

yêu cầu nghiêm ngặt trong thiết kế. Điều đáng chú ý, các hệ thống QKD sử dụng giao thức DV-QKD không có tính tương thích với các hệ thống truyền thông quang đã có. Với nghiên cứu cải tiến hiệu năng của nghiên cứu [85] cho CV-QKD, tín hiệu SIM/ BPSK yêu cầu sử dụng bộ điều chế sóng mang phụ tần số vô tuyến (RF), điều này dẫn tới sự phức tạp của hệ thống. Nghiên cứu [99] tận dụng ưu điểm của CV-QKD, sử dụng bộ điều chế dựa trên phương pháp điều chế pha kiểu QPSK nhưng chỉ áp dụng cho hệ thống phân phối khóa lượng tử sử dụng cáp quang, chưa có tiến hành nghiên cứu áp dụng cho hệ thống QKD-FSO. Nghiên cứu [38] sử dụng mã thích nghi LDPC tuy duy trì được tốc độ truyền khóa nhưng yêu cầu về phần cứng để xử lý tín hiệu phức tạp.

- Với các phương pháp cải thiện về giảm hệ số QBER bằng phương pháp sử dụng mã sửa sai FEC tận dụng ưu điểm của kỹ thuật FEC là không yêu cầu gửi lại thông tin. Dựa trên nguyên tắc của kỹ thuật FEC, bên phát sẽ phải thêm thông tin phục vụ cho mục đích phát hiện lỗi và sửa lỗi vào chuỗi bit mang thông tin về khóa cần gửi đi, điều đó cho phép bên nhận có thể tự kiểm tra và sửa lỗi (nếu có) gây ra do kênh truyền. Phương pháp sử dụng mã sửa lỗi FEC gặp phải vấn đề lớn là độ phức tạp trong các thuật toán nhằm mục đích giảm được số lượng các bit phục vụ cho mục đích sửa sai được cộng thêm vào cùng với dữ liệu. Hơn nữa, mã sửa lỗi FEC cũng không đủ mạnh để đảm bảo độ tin cậy khi khoảng cách đường truyền từ vệ tinh tới mặt đất là lớn.

- Việc sử dụng một trong các kỹ thuật ghép kênh đã được khảo sát ở trên, về cơ bản, đã giúp cải thiện tốc độ truyền khóa của hệ thống QKD. Tuy nhiên, chưa đạt được sự cải thiện vượt trội về tốc độ truyền khóa bí mật của các hệ thống QKD đa kênh. Việc mã hóa và giải mã trong các nghiên cứu [75] và [70] yêu cầu việc xử lý tín hiệu phức tạp và không phù hợp cho việc tích hợp trong các hệ thống viễn thông đã có. Phần lớn các công trình nghiên cứu chỉ hỗ trợ truyền dẫn khóa cho một người sử dụng, các hệ thống truyền dẫn khóa lượng tử nhiều người sử dụng 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, hướng nghiên cứu sẽ tập trung vào đề xuất áp dụng và chứng minh 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. Cụ thể, luận án sẽ tập trung vào các hướng nghiên cứu sau::

(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. Phương thức truyền dẫn luận án đề xuất sẽ sử dụng kiểu mã hóa thông tin khóa như trong giao thức kiểu CV-QKD, nhằm tận dụng những ưu điểm của giao thức CV-QKD: tương thích với các hệ thống truyền thông quang đã có, giá thành rẻ, tốc độ khóa cao, cấu trúc máy thu đơn giản. Nguyên lý thiết lập mức công suất nhỏ kết hợp với ngưỡng kép và điều chế pha để thông qua ảnh hưởng của nhiễu tạp tạo ra khả năng an ninh cho hệ thống phân phối khóa lượng tử biến liên tục CV-QKD.

(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 nhằm giảm tỉ lệ lỗi bit lượng tử QBER và tỉ lệ lỗi khóa lượng tử QKER, tăng khoảng cách đường truyền từ máy phát đến máy thu.

(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.

Giải pháp cải thiện hiệu năng thứ nhất được đề xuất trong luận án là phương thức truyền dẫn quang trong không gian tự do trong hệ thống phân phối khóa lượng tử dựa trên nguyên tắc của CV-QKD, phương thức truyền dẫn này sẽ sử dụng: **(1)**

phương pháp điều chế QPSK trong việc mã hóa các bit bên phát vào ánh sáng laser truyền đi dựa trên nền tảng là giao thức BB84 và **(2)** kết hợp với máy thu quang sử dụng bộ tách sóng kiểu heterodyne và cơ chế tách ngưỡng kép. Hiệu năng của hệ thống sẽ được phân tích dưới sự ảnh hưởng của nhiễu máy thu và suy hao kênh.

Phương thức truyền dẫn mà luận án đề xuất sẽ dùng sóng mang quang để điều chế tín hiệu cần truyền đi. Việc sử dụng sóng mang quang giúp cho hệ thống QKD-FSO có tính tương thích với các hệ thống truyền thông quang truyền thống.

Máy thu quang kiểu tách sóng heterodyne được dùng để cải thiện độ nhạy của máy thu và do đó quá trình giải mã tín hiệu sẽ đạt được sự chính xác cao hơn so với máy thu sử dụng kiểu tách sóng trực tiếp, kết quả là hệ số lỗi bit lượng tử QBER được cải thiện so với việc dùng máy thu sử dụng kiểu tách sóng trực tiếp. Hệ số QBER nhỏ để có thể đảm bảo được tốc độ truyền khóa 100 Mb/s (tăng so với các hệ thống hiện nay) trong hệ thống FSO 10 Gb/s. Cơ chế tách ngưỡng kép của bộ tách sóng bên thu giúp hình thành các bit “0”, bit “1”, bit “X” giống như việc tái tạo thông tin trong giao thức cơ sở BB84.

Giải pháp cải thiện hiệu năng thứ hai được đề xuất trong luận án là sử dụng: **(1)** kỹ thuật ARQ trong việc phát lại các chuỗi bit phát không thành công **(2)** trạm chuyển tiếp dựa trên hạ tầng trên cao HAP với bộ nhớ đệm được trang bị tại trạm chuyển tiếp và **(3)** mô hình chuỗi Markov hai trạng thái để mô tả trạng thái kênh truyền FSO từ HAP tới trạm mặt đất khi phân tích đánh giá hiệu năng. Hiệu năng của hệ thống cũng được đánh giá trong điều kiện nhiễu loạn khí quyển yếu hay mạnh.

Kỹ thuật ARQ sẽ truyền lại các khóa bị lỗi để đảm bảo độ tin cậy của các khóa lượng tử. Ưu điểm của việc sử dụng ARQ là kỹ thuật này không yêu cầu các thuật toán phức tạp để giảm nhỏ số lượng các bit dùng cho mục đích sửa sai đồng thời đảm bảo độ tin cậy khi truyền khóa trong điều kiện khoảng cách đường truyền từ vệ tinh tới trạm mặt đất lớn.

Kỹ thuật chuyển tiếp được dùng để tăng cường chất lượng của đường truyền vật lý từ vệ tinh tới trạm mặt đất. Trạm chuyển tiếp đặt tại HAP sẽ khôi phục lại và

chuyển tiếp khóa lượng tử truyền từ vệ tinh xuống trạm mặt đất. Do đó, tỷ lệ lỗi bit lượng tử QBER sẽ được giảm xuống đáng kể.

Bộ nhớ đệm được trang bị tại trạm chuyển tiếp sẽ được sử dụng để lưu trữ và truyền lại khóa lượng tử nếu quá trình truyền khóa không thành công. Việc sử dụng bộ nhớ đệm tại trạm chuyển tiếp sẽ làm giảm trễ truyền dẫn khi phân phối khóa.

Mô hình chuỗi Markov hai trạng thái được sử dụng để phân tích hiệu năng của hệ thống. Mô hình này đã được công nhận rộng rãi là cách tiếp cận linh hoạt về mặt toán học và chính xác về mặt logic với truyền thông không dây [76].

Giải pháp cải thiện hiệu năng thứ ba được đề xuất là kỹ thuật phân phối khóa lượng tử đa kênh dựa trên vệ tinh sử dụng: **(1)** kỹ thuật ghép kênh sóng mang phụ SCM và **(2)** kỹ thuật phân chia theo bước sóng WDM.

Hiệu năng của hệ thống cũng sẽ được xem xét trong các điều kiện tạp âm và nhiễu loạn khí quyển khác nhau.

Kỹ thuật ghép kênh sóng mang phụ SCM sẽ thực hiện điều chế N luồng bit được tạo ra từ vệ tinh sau quá trình chuyển đổi nối tiếp/song song vào N sóng mang phụ nhờ bộ điều chế dịch pha nhị phân BPSK.

Kỹ thuật ghép kênh theo bước sóng WDM sẽ kết hợp mỗi nhóm N sóng mang phụ và điều chế vào một trong M_w bước sóng được tạo ra bởi nguồn laser thông qua bộ điều chế ngoài và M_w bước sóng được ghép lại nhờ bộ ghép kênh quang (Optical Mutiplexing – OMUX).

Bằng phương pháp kênh sóng mang phụ SCM và ghép kênh theo bước sóng, hiệu năng hệ thống được cải thiện nhờ giảm hệ số lỗi bit lượng tử QBER dưới sự ảnh hưởng của tạp âm, nhiễu và trong các điều kiện nhiễu loạn khác nhau. Đặc biệt, hệ thống có thể cung cấp tốc độ khóa bí mật (Secret Key Rate – SKR) hàng Gbit/s. Đây là khả năng mà các hệ thống QKD đơn kênh và các hệ thống QKD đa kênh trước đây không thực hiện được. Khả năng cung cấp SKR tốc độ Gbit/s có vai trò rất quan trọng

trong việc tạo ra các khóa bí mật chia sẻ có độ dài lớn nhằm tạo ra khả năng an ninh vô điều kiện cho các hệ thống truyền thông trong tương lai.

Để tăng khả năng hỗ trợ đa người dùng kết hợp với việc cải thiện hiệu năng an ninh của hệ thống QKD-FSO, giải pháp hệ thống QKD-FSO sử dụng kỹ thuật đa truy nhập phân chia theo mã quang (Code Division Multiple Access – CDMA) cũng được luận án đề xuất.

Kết luận Chương 1

Nội dung của Chương 1 đã trình bày khái quát về giao thức BB84, giao thức cơ sở trong truyền khóa lượng tử; hệ thống phân phối khóa lượng tử QKD nói chung và hệ thống phân phối khóa lượng tử biến liên tục nói riêng; mô hình, nguyên lý hoạt động, các tham số hiệu năng và các yếu tố ảnh hưởng tới truyền dẫn quang qua không gian tự do trong hệ thống phân phối khóa lượng tử biến liên tục. Ngoài ra, tình hình nghiên cứu trong và ngoài nước liên quan đến các hệ thống QKD-FSO nói chung và cải thiện hiệu năng truyền dẫn quang qua không gian tự do trong hệ thống phân phối khóa lượng tử biến liên tục nói riêng cũng đã được phân tích, đánh giá. Thông qua đó, các hạn chế của các nghiên cứu trước đây đã được chỉ ra. Trên cơ sở những hạn chế này, hướng nghiên cứu của luận án đã được xác định là 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 dựa trên kỹ thuật điều chế QPSK và máy thu coherent kiểu tách sóng heterodyne; kỹ thuật ARQ và dùng chuyển tiếp HAP cho hệ thống QKD-FSO đơn kênh dựa trên vệ tinh, dùng mô hình Markov hai trạng thái để mô tả kênh truyền FSO từ trạm chuyển tiếp HAP đến máy thu; kỹ thuật dùng ghép kênh sóng mang phụ kết hợp SCM với ghép kênh quang theo bước sóng WDM cho hệ thống QKD-FSO đa kênh dựa trên vệ tinh và kỹ thuật đa truy nhập phân chia theo mã quang hỗ trợ cho hệ thống QKD-FSO đa người dùng, tăng cường tính bảo mật của hệ thống. Các giải pháp cải thiện hiệu năng được đề cập ở trên sẽ lần lượt được trình bày chi tiết trong nội dung của Chương 2, Chương 3 và Chương 4 của luận án.

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

Tóm tắt

Chương 2 trình bày về mô hình toán học của kênh truyền FSO khi xem xét các yếu tố suy hao bao gồm: suy hao trong không gian tự do, suy hao do khí quyển, suy hao do trải rộng chùm tia và ảnh hưởng của pha-đinh do nhiễu loạn khí quyển. Nội dung chính của Chương 2 là đề xuất 01 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. Giải pháp truyền dẫn đề xuất sẽ dựa trên nguyên tắc của điều chế pha QPSK ở phía máy phát để mã hóa các thông tin cần truyền kết hợp với sử dụng máy thu quang sử dụng bộ tách sóng coherent kiểu heterodyne với cơ chế tách sóng hai ngưỡng. Các thông tin về khóa sẽ được mã hóa trong bốn trạng thái coherent của sóng mang quang. Máy thu quang sử dụng bộ tách sóng coherent kiểu heterodyne để tăng độ nhạy máy thu quang, từ đó hiệu năng của cả hệ thống sẽ được cải thiện. Kết quả nghiên cứu của chương 2 đã được công bố trên 01 bài báo quốc tế ISI [J1]; 01 bài báo tại hội thảo quốc tế ISCIT 2019 [C2] (bài báo nhận được giải Best Paper của hội nghị); 01 bài báo trên tạp chí Khoa học và công nghệ [J3].

2.1. Mô hình kênh truyền FSO

Trước hết, 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. Ảnh hưởng của nhiễu loạn khí quyển là không đáng kể khi độ cao đủ lớn [34]. Trong mô hình toán học của kênh truyền được sử dụng trong luận án, độ cao H_β được sử dụng như một ngưỡng để xác định yếu tố suy hao trong không gian tự do hay suy hao do khí quyển đóng vai trò chính trong suy hao công suất của tín hiệu thu được.

2.1.1. Suy hao trong không gian tự do

Chùm tia laser được truyền từ vệ tinh tại độ cao H_s xuyên qua không gian tự do tới trạm mặt đất đặt tại độ cao H_G. Suy hao trong không gian tự do từ độ cao H_s tới H_β được xác định bằng công thức [34]:

$$L_{FS} = \left(\frac{4\pi D_s}{\lambda}\right)^2 \tag{2.1}$$

Với D_S là khoảng cách truyền dẫn trong môi trường không gian tự do, có thể được tính theo công thức:

$$D_S = \frac{(H_S - H_\beta)}{cos\zeta} \tag{2.2}$$

Với ζ là góc thiên đỉnh. λ là bước sóng quang.

2.1.2. Suy hao do khí quyển

Trong quá trình truyền tín hiệu quang qua bầu khí quyển của Trái đất, tín hiệu quang sẽ phải tương tác với hơi nước và các phần tử khí khác nhau tồn tại trong bầu khí quyển. Hiện tượng hấp thụ và tán xạ là nguyên nhân chính gây ra suy hao khí quyển. Hấp thụ khí quyển là hiện tượng phụ thuộc vào bước sóng của tín hiệu quang truyền qua bầu khí quyển. Nếu bước sóng tín hiệu quang trong khu vực hồng ngoại và nhìn thấy được, hấp thụ phân tử nước, carbon dioxide, ozon là nguyên nhân chính gây ra suy hao khí quyển. Trong điều kiện trời trong, hệ số hấp thụ phân tử phụ thuộc bước sóng được đưa ra ở Bảng 2.1 [45].

Bảng 2. 1. Một số giá trị tiêu biểu của các hệ số hấp thụ phân tử

Số thứ tự	Bước sóng (nm)	Hấp thụ phân tử (dB/km)
1	550	0,13
2	690	0,01
3	850	0,41
4	1550	0,01

Đa số các hệ thống truyền quang qua không gian tự do lựa chọn tín hiệu quang có bước sóng làm việc trong cửa sổ 780-850 nm và 1520-1600 nm.

Tán xạ ánh sáng cũng là một trong những nguyên nhân gây suy giảm hiệu năng hệ thống truyền quang qua không gian tự do. Tùy thuộc theo kích thước của hạt khí quyển so với bước sóng quang là nhỏ hơn hay tương đương bước sóng quang sẽ có tán xạ Rayleigh hay tán xạ Mie tương ứng. Các hạt không khí, khói mù, các phân tử gây ra tán xạ Rayleigh. Phần tử khí, sương mù là các yếu tố gây ra tán xạ Mie. Giống như hiện tượng hấp thụ, hiện tượng tán xạ cũng phụ thuộc vào bước sóng làm việc của tín hiệu quang. Tán xạ Rayleigh chiếm ưu thế nếu bước sóng làm việc của tín hiệu quang nằm trong vùng nhìn thấy và tia cực tím. Tán xạ Rayleigh có thể được bỏ qua nếu bước sóng làm việc của tín hiệu quang gần vùng bức xạ hồng ngoại (Infrared Radiation – IR). Tán xạ Mie chiếm ưu thế nếu bước sóng làm việc của tín hiệu quang nằm ở vùng bức xạ hồng ngoại hoặc dài hơn.

Sương mù

Sương mù được coi là thách thức chính đối với truyền thông quang không dây. Sương mù được tạo ra do hơi nước được tập hợp từ những giọt nước nhỏ có đường kính vài trăm micro mét. Thông qua sự kết hợp của các hiện tượng hấp thụ, tán xạ và phản xạ của ánh sáng khi truyền qua sương mù, ánh sáng có thể bị thay đổi đặc tính truyền lan hoặc bị ngăn cản hoàn toàn sự truyền lan. Điều này có thể dẫn đến mật độ công suất của búp sóng phát bị suy giảm. Trong điều kiện truyền thông quang trong sương mù dày đặc, khi tầm nhìn thậm chí còn ít hơn 50 m, độ suy giảm có thể đạt tới giá trị hơn 350 dB/km [59]. Sương mù có thể tồn tại ở độ cao 400m so với bề mặt Trái đất. Suy hao do sương mù có thể được dự đoán bằng cách áp dụng lý thuyết tán xạ Mie.

Mưa

Những hạt mưa có kích thước lớn hơn đáng kể (100 đến 10.000 μm) so với bước sóng được sử dụng trong truyền thông quang không dây nên ảnh hưởng của mưa không rõ rệt như ảnh hưởng của sương mù. Suy hao do mưa nhẹ (2,5 mm/giờ) đến mưa lớn (25 mm/giờ) từ 1 dB/km đến 10 dB/km khi truyền thông quang có các bước sóng xung quanh 850 nm và 1500 nm [81, 90].

Suy hao do mưa α_{rain} (dB/km) cho truyền thông quang trong không gian tự do có thể được tính theo công thức [81]

$$\alpha_{rain} = k_1 R^{k_2} \quad (2.3)$$

Với R là tốc độ mưa tính bằng mm/giờ và k_1, k_2 là các tham số mô hình có giá trị phụ thuộc vào kích thước hạt mưa và nhiệt độ mưa. Những cơn mưa kèm theo đám mây thấp sẽ có suy hao lớn, để khắc phục hiện tượng này có thể sử dụng nguồn quang có công suất lớn, quỹ công suất quang lớn hơn 30 dB.

Tuyết

Suy hao do tuyết gây ra với đường truyền quang qua không gian tự do nhỏ hơn suy hao gây ra do sương mù nhưng lớn suy hao gây ra do mưa vì kích thước của tuyết nhỏ hơn kích thước của mưa, lớn hơn kích thước của sương mù. Với suy hao có nguyên nhân do tuyết, có thể phân loại thành suy hao do tuyết khô và suy hao do tuyết ướt gây ra. Suy hao do tuyết α_{snow} (dB/km) cho truyền thông quang trong không gian tự do có thể được tính theo công thức [71]:

$$\alpha_{snow} = aS^b \quad (2.4)$$

Trong đó, S là tốc độ tuyết (mm/ giờ); a và b là các giá trị xác định với từng trường hợp tuyết ướt hoặc tuyết khô.

Trường hợp tuyết ướt: a = 1,02.10^{-4}+ 3,78; b = 0,72;

Trường hợp tuyết khô: a = 5,42.10^{-5}+5,49; b = 1,38;

Suy hao khí quyển được tính dựa trên luật Beer - Lambert [74]:

$$h_a = \frac{P_R}{P_T} = exp(-\gamma(\lambda) D_\beta) \quad (2.5)$$

với $\gamma(\lambda)$ là hệ số suy hao phụ thuộc thời tiết, có đơn vị là m^{-1}, h_a là suy hao tổng tại bước sóng λ, D_β là khoảng cách truyền dẫn trong môi trường khí quyển và được xác định theo công thức:

$$D_\beta = \frac{(H_\beta - H_G)}{cos\zeta} \quad (2.6)$$

2.1.3. Suy hao do trải rộng chùm tia và sự lệch hướng

Duy trì định hướng giữa bộ phát và bộ thu đóng vai trò quan trọng trong việc đảm bảo sự thành công của việc truyền tín hiệu giữa trạm thu và trạm phát. Vấn đề về duy trì định hướng thực sự là yêu cầu khó khăn khi hệ thống QKD-FSO yêu cầu truyền dẫn trong tầm nhìn thẳng, sử dụng búp sóng quang hẹp, phân tán góc để truyền. Một số nguyên nhân cơ bản gây ra sự lệch hướng giữa trạm thu và trạm phát trong các hệ thống QKD-FSO có thể kể ra như sau:

- Sự trôi búp sóng quang: Sự trôi búp sóng quang xảy ra khi tồn tại luồng gió hỗn loạn (gió xoáy) có kích thước lớn hơn đường kính của búp sóng quang, luồng gió hỗn loạn này gây ra sự dịch chuyển chậm nhưng đáng kể của búp sóng quang. Các hoạt động địa chấn gây ra sự dịch chuyển tương đối giữa vị trí của bộ phát và bộ thu quang cũng có thể gây ra hiện tượng trôi búp sóng.

- Gió, đặc biệt khi các thiết bị thu/phát được đặt trên các tòa nhà cao tầng. Sự dao động của tòa nhà là một quá trình ngẫu nhiên và nó có thể dẫn tới hậu quả lệch hướng giữa trạm mặt đất và vệ tinh.

- Sự thay đổi về kích thước, hình dạng của các phần khung đỡ thấu kính phát và thu do hiện tượng dãn nhiệt. Sự dãn nhiệt có đặc tính chu kỳ theo ngày hoặc mùa, có thể dự đoán được.

Để đánh giá suy hao tín hiệu quang do ảnh hưởng của sự lệch hướng, búp sóng quang được mô hình hóa theo mô hình phân bố Gauss với phân bố cường độ tín hiệu phát chuẩn hóa theo không gian tại khoảng cách $D_{SG} = (H_S - H_G)/\cos(\zeta)$ từ phía phát tới phía thu và được tính theo công thức [8]:

$$I_{beam}(\rho_A;\, D_{SG}) = \frac{2}{\pi\omega_D^2}\exp(-\frac{2\|\rho\|^2}{\omega_D^2}), \tag{2.7}$$

Với ω_D là độ rộng búp sóng quang tại khoảng cách D_{SG}. ρ_A là vector hướng từ tâm của búp sóng quang tới ||. || xác định biểu thức của chuẩn Euclid. Với độ lệch hướng r giữa tâm khẩu độ thu và tâm của footprint búp sóng quang trên mặt phẳng chứa bộ thu, tổn hao hình học do sự trải rộng chùm tia tại phía thu kết hợp với ảnh hưởng của lệch hướng được xác định:

$$h_l\,(r;\,D_{SG}) = \int_A I_{beam}(\rho_A - r; D_{SG}\,)d\rho_A \tag{2.8}$$

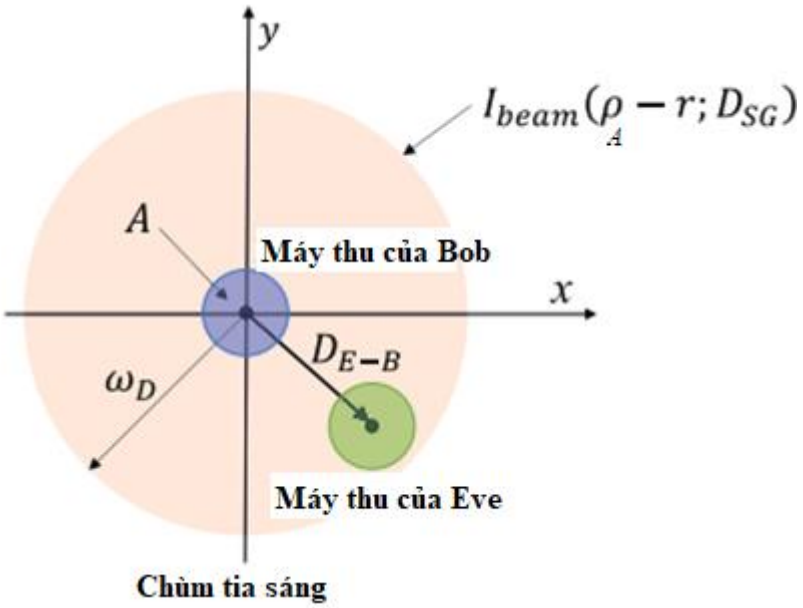
Với A là diện tích của vùng thu tại máy thu. Biểu thức Gauss của $h_l(.)$ được viết theo công thức [26]:

$$h_l\,(r;\,D_{SG}) \approx A_0 exp\left(-\frac{2r^2}{\omega_{D_{eq}}^2}\right) \tag{2.9}$$

Với: $\omega_{D_{eq}}^2 = \omega_D^2 \frac{\sqrt{\pi} erv(v)}{2v\exp(-v^2)}$ xác định chiều rộng chùm tia tương đương tại trạm mặt đất.

$A_0 = [\mathrm{erf}(v)]^2$ và $v = \frac{\sqrt{\pi} a_d}{\sqrt{2}\omega_D}$

a_d là khẩu độ tách sóng tại trạm mặt đất. A_0 biểu thị lượng công suất thu được khi r=0.



Hình 2. 1. Chùm tia tại mặt đất và vị trí máy thu của Bob và Eve.

Công thức (2.7) dùng để xác định công suất quang thu được bởi máy thu hoặc tại kẻ nghe lén (Eve). Trong kịch bản có máy thu không hợp pháp đặt gần Bob (trong chùm tia sáng) để lấy trộm khóa lượng tử như trong minh họa ở Hình 2.1. Chúng ta

giả thiết rằng máy thu Bob đặt tại trung tâm của chùm tia (r=0) và $r = D_{E-B}$ là khoảng cách giữa Eve và Bob. Công suất quang nhận được tỷ lệ nghịch với r. Tại trạm mặt đất, lượng công suất quang thu được ở Bob và Eve tương ứng là $h_l(0; D_{SG})$ và $h_l(D_{E-B}, D_{SG})$.

2.1.4. Ảnh hưởng của pha-đinh do nhiễu loạn khí quyển

Nhiễu loạn khí quyển là hiện tượng ngẫu nhiên, phụ thuộc vào tốc độ gió, áp suất khí quyển, độ cao, sự thay đổi của hệ số khúc xạ của môi trường. Nguyên nhân gây ra sự nhiễu loạn khí quyển là do sự thay đổi của áp suất và nhiệt độ trên đường truyền dẫn quang không dây. Những sự thay đổi này tạo ra những xoáy lốc nhiễu loạn có kích thước và mật độ thay đổi nhanh kéo theo chỉ số khúc xạ của môi trường truyền dẫn bị thay đổi nhanh. Các xoáy lốc nhiễu loạn sẽ đóng vai trò như những thấu kính có đặc tính thay đổi theo thời gian gây ra tỷ lệ lỗi bit của các hệ thống QKD-FSO tăng mạnh, đặc biệt ở các khoảng thời gian có ánh sáng mặt trời. Tùy theo mối quan hệ giữa kích thước của xoáy lốc nhiễu loạn và kích thước chùm tia sẽ gây ra những hậu quả khác nhau. Nếu kích thước của xoáy lốc nhiễu loạn lớn hơn kích thước của chùm tia, nhiễu loạn khí quyển sẽ gây ra hiện tượng lệch chùm tia ra khỏi đường truyền một cách ngẫu nhiên, gây ra lỗi đường truyền. Nếu kích thước của xoáy lốc nhỏ hơn kích thước của chùm tia sẽ gây ra hiện tượng nhấp nháy của tín hiệu quang thu được. Đó chính là hiện tượng thăng giáng cường độ tín hiệu quang thu được theo thời gian và không gian.

Ngoài ra, nhiễu loạn khí quyển cũng có thể tạo ra sự thay đổi phân cực ánh sáng và sự dãn rộng của xung quang. Sự thay đổi phân cực ánh sáng sẽ làm suy giảm công suất trung bình của chùm quang. Sự dãn rộng của xung quang là do hiện tượng truyền đa đường khi chùm tia quang truyền qua các xoáy lốc hỗn loạn của bầu khí quyển. Sự dãn rộng của xung quang sẽ gây ra sự hạn chế về băng thông và tốc độ dữ liệu.

Cả hai trường hợp nhiễu loạn khí quyển yếu và mạnh đều được xem xét trong khảo sát về hiệu năng của các phương pháp đề xuất. Nhiễu loạn khí quyển được biểu thị bằng hệ số kênh (h_f), được mô hình hóa dưới dạng phân phối Gamma-Gamma với hàm phân bố xác suất (Probability Density Function – PDF). Trong truyền thông

FSO, phân bố Gamma-Gamma (GG) được sử dụng rộng rãi để đại diện cho sự nhiễu loạn từ yếu đến mạnh [7]. Hàm phân bố xác suất PDF của h_f với điều kiện $h_f > 0$ được xác định như sau [61]:

$$f_{h_f}(h_f) = \frac{2K_{\alpha-\beta}(\alpha\beta)^{\frac{\alpha+\beta}{2}}}{\Gamma(\alpha)\Gamma(\beta)}\left(2\sqrt{\alpha\beta h_f}\right)(h_f)^{\left(\frac{\alpha+\beta}{2}\right)-1} \tag{2.10}$$

Với α, β tương ứng là các tham số mô tả sự ảnh hưởng của dòng xoáy quy mô lớn và quy mô nhỏ của nhiễu loạn khí quyển. $K_{\alpha-\beta}(.)$ là hàm Bessel sửa đổi loại thứ hai được mô tả bởi $K_v(.)$. Bậc (α-β) và $\Gamma(.)$ đại diện cho hàm Gamma được định nghĩa: $\Gamma(m) = \int_0^\infty t^{m-1}e^{-t}dt$. Giả thiết, sóng được truyền là sóng phẳng, α và β có thể được tính xấp xỉ bởi công thức [29]:

$$\begin{cases} \alpha \cong \left[\exp\left(\dfrac{0.49\sigma_R^2}{\left(1+1.11\sigma_R^{\frac{12}{5}}\right)^{\frac{7}{6}}}\right)-1\right]^{-1} \\ \beta \cong \left[\exp\left(\dfrac{0.51\sigma_R^2}{\left(1+0.69\sigma_R^{\frac{12}{5}}\right)^{\frac{5}{6}}}\right)-1\right]^{-1} \end{cases} \tag{2.11}$$

Với σ_R^2 là phương sai Rytov, trong trường hợp đường truyền theo phương nghiêng từ vệ tinh tới trạm mặt đất, phương sai Rytov và có thể được biểu diễn bằng công thức (khi xác định đường truyền quang từ khoảng cách độ cao của vệ tinh là H_β tới khoảng cách độ cao của trạm mặt đất H_G) [55]:

$$\sigma_R^2 = 2.25k_b^{\frac{7}{6}}\sec(\zeta)^{\frac{11}{6}}\int_{H_G}^{H_\beta} C_n^2(h)(h-H_G)^{\frac{5}{6}}dh, \tag{2.12}$$

với $k_b = 2\pi/\lambda$ là số bước sóng trong trường quang và $C_n^2(h)$ là tham số cấu trúc chỉ số chiết suất phụ thuộc vào độ cao so với mặt nước biển, đặc trưng cho cường độ của

nhiễu loạn. Mô hình Hufnagel- Valley (H-V) có thể được dùng để xác định các điều kiện nhiễu loạn [55]:

$$C_n^2(h) = 0{,}00594\left(\frac{v}{27}\right)^2 (10^{-5}h)^{10}\exp\left(-\frac{h}{1000}\right) + 2{,}7\times 10^{-16}\exp\left(-\frac{h}{1500}\right) + C_n^2(0)\exp\left(-\frac{h}{100}\right) \quad (2.13)$$

trong đó, v là tốc độ gió (tính theo đơn vị m/s), h là độ cao so với mặt nước biển (tính theo đơn vị m), $C_n^2(0)$ là giá trị của C_n^2 tại mặt đất (tính theo đơn vị $m^{-2/3}$).

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

Luận án sẽ đề xuất phương thức truyền dẫn quang qua không gian tự do trong hệ thống phân phối khóa lượng tử CV-QKD. Phương thức truyền dẫn được đề xuất cho hệ thống QKD-FSO sử dụng điều chế pha kiểu QPSK ở bên phía phát và ở phía thu của sẽ sử dụng máy thu kiểu tách sóng heterodyne dựa trên cơ chế tách ngưỡng kép. Việc sử dụng bộ điều chế sóng mang phụ quang ở luận án đề xuất sẽ khắc phục được sự phức tạp của hệ thống khi sử dụng tín hiệu SIM/BPSK với yêu cầu sử dụng bộ điều chế sóng mang phụ tần số vô tuyến điện như trong nghiên cứu [85].

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

Nguyên lý cơ bản của phương thức truyền dẫn đề xuất là sử dụng các trạng thái pha của sóng mang quang để mã hóa các bit trong chuỗi khóa như minh họa trong Hình vẽ 2.2. Phương thức này 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].

Bước 1: Tại phía phát, Alice chọn ngẫu nhiên 1 trong 2 base A_1 hoặc A_2 để mã hóa mỗi một bit nhị phân vào một trong hai giá trị ϕ_A của sóng mang quang. Trong đó ϕ_A được tính theo công thức:

$$\phi_A = (\phi_1 + \phi_2)/2 \quad (2.14)$$

ϕ_A là kết hợp pha của hai nhánh bộ điều chế Mach-Zehnder (MZM) có pha lần lượt là ϕ_1 và ϕ_2. Bốn giá trị pha ϕ_A của sóng mang quang chính là bốn trạng thái pha trong điều chế QPSK tương đương với bốn trạng thái phân cực trong giao thức BB84.

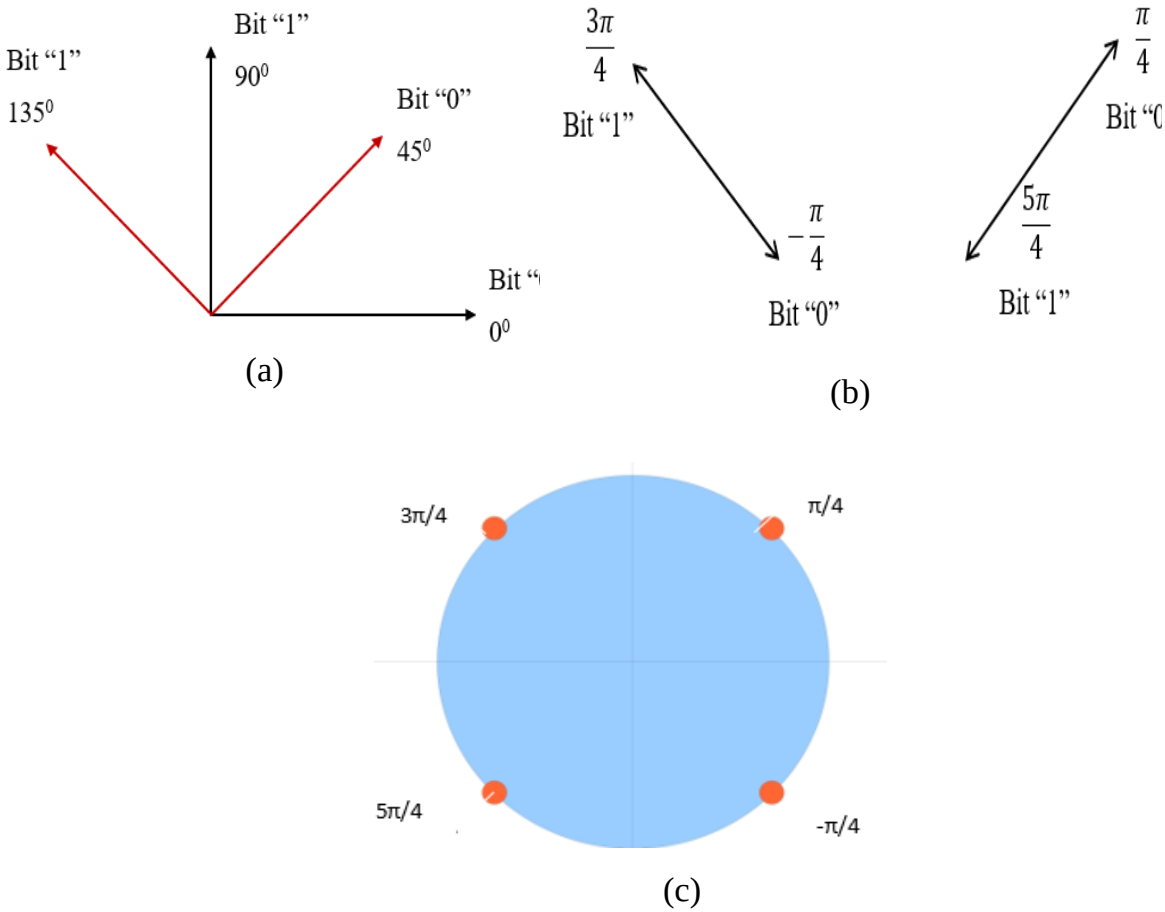
Bước 2: Tại máy thu Bob, tín hiệu nhận được từ Alice với pha ϕ_A được trộn với tín hiệu được tạo ra tại Bob có pha là ϕ_B. Bob sẽ chọn pha ϕ_B một cách ngẫu nhiên từ một trong hai base là B_1 và B_2 với B_1 có pha là $\phi_B = \pi/4$ và B_2 có pha là $\phi_B = -\pi/4$.

Alice và Bob chọn cùng base nếu Alice chọn A_i và Bob chọn B_i với $i\epsilon\{1,2\}$. Kết quả là, dòng điện tại đầu ra của tách quang trong bộ thu sẽ nhận được một trong ba giá trị là I_0, 0, I_1 tương đương với bit "0", "X", và bit "1" một cách tương ứng. Bit "X" xuất hiện trong trường hợp không bit nào được tạo ra. Bit "X" trong trường hợp này phản ánh trong một hệ thống truyền dẫn QKD có ba loại bit là "1", "0" và "X" thay vì một hệ thống truyền dẫn thông thường chỉ có hai loại bit là "1" và "0". Bit "X" xuất hiện trong phương thức truyền dẫn CV-QKD đề xuất tương ứng với bit "X" tạo ra trong giao thức gốc BB84 loại DV-QKD.

Bước 3: Bob thông báo với Alice qua kênh truyền thống công khai các thời điểm mà Bob có thể tạo ra các bit nhị phân "0" hay "1" từ các tín hiệu tách được. Alice cũng bỏ đi các giá trị bit ở các vị trí tương ứng với Bob tạo ra bit không xác định. Các bit còn lại trong chuỗi bit tạo ra một chuỗi bit mới dùng để chia sẻ giữa Alice và Bob, chuỗi bit mới này được gọi là **khóa chọn lọc**.

Bước 4: Giống như giao thức BB84, bước này sẽ thực hiện phát hiện lỗi và sửa lỗi, sau đó tạo ra khóa bí mật không lỗi. Trong quá trình này, Alice và Bob sử dụng các hàm băm để tạo ra một khóa mới, ngắn hơn nhằm mục đích Eve có được rất ít thông tin về khóa.

Bảng 2.2 mô tả các pha ở bên phát được dùng trong mã hóa các bit của khóa cần truyền đi, các pha ở bên thu được dùng để giải mã từ tín hiệu thu được và các bit thông tin của khóa sau quá trình giải mã.



Hình 2. 2. (a) Các pha được dùng trong giao thức BB84 truyền thống. (b) Các pha được dùng trong giao thức QKD sử dụng phương thức truyền dẫn khóa đề xuất. (c) Biểu đồ chòm sao được dùng trong phương thức truyền dẫn khóa đề xuất.

Bảng 2. 2. Các pha dùng trong mã hóa, giải mã và các bit kết quả tương ứng.

Base	**Bit**	ϕ_1	ϕ_2	ϕ_A	**Base**	ϕ_B	ϕ_A-ϕ_B	***I***	**Bit**
A_1	0	0	$\frac{\pi}{2}$	$\frac{\pi}{4}$	B_1	$\frac{\pi}{4}$	0	I_0	0
A_1	0	0	$\frac{\pi}{2}$	$\frac{\pi}{4}$	B_2	$-\frac{\pi}{4}$	$\frac{\pi}{2}$	0	X
A_1	1	π	$\frac{3\pi}{2}$	$\frac{5\pi}{4}$	B_1	$\frac{\pi}{4}$	π	I_1	1
A_1	1	π	$\frac{3\pi}{2}$	$\frac{5\pi}{4}$	B_2	$-\frac{\pi}{4}$	$-\frac{\pi}{2}$	0	X

A_2	0	0	$-\frac{\pi}{2}$	$-\frac{\pi}{4}$	B_1	$\frac{\pi}{4}$	$-\frac{\pi}{2}$	0	X
A_2	0	0	$-\frac{\pi}{2}$	$-\frac{\pi}{4}$	B_2	$-\frac{\pi}{4}$	0	I_0	0
A_2	1	π	$\frac{\pi}{2}$	$\frac{3\pi}{4}$	B_1	$\frac{\pi}{4}$	$\frac{\pi}{2}$	0	X
A_2	1	π	$\frac{\pi}{2}$	$\frac{3\pi}{4}$	B_2	$-\frac{\pi}{4}$	π	I_1	1

Nội dung Bảng 2.3 là so sánh các bước thực hiện của giao thức cơ sở BB84 với giao thức CV-QKD sử dụng phương thức truyền dẫn khóa luận án đề xuất. Bước một của giao thức được thực hiện tại máy phát với việc mã hóa các bit trong chuỗi bit truyền đi vào sóng mang quang bằng phương thức điều chế QPSK. Bước hai của giao thức được thực hiện tại máy thu bằng việc sử dụng pha ngẫu nhiên ϕ_B của máy thu kết hợp với cơ chế tách ngưỡng kép. Bằng việc sử dụng cơ chế tách ngưỡng kép, bit "X" được tạo ra khi Alice chọn A_i để mã hóa và Bob chọn B_j ($i \neq j$) để tách và xác định giá trị của bit thu được.

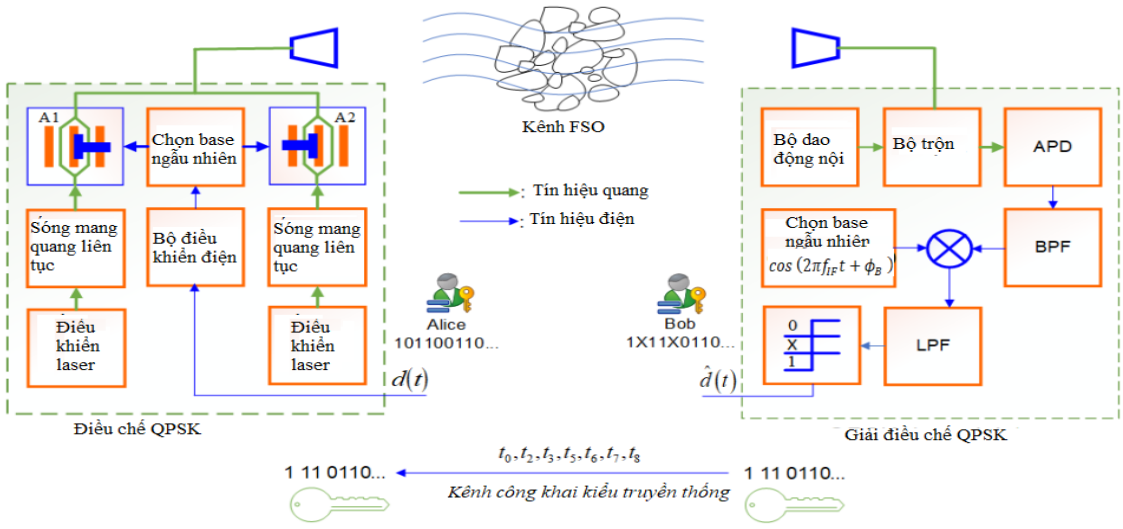
Bảng 2. 3. So sánh các bước thực hiện của giao thức cơ sở BB84 với giao thức CV-QKD sử dụng phương thức truyền dẫn đề xuất.

Bước	**Giao thức cơ sở BB84.**	**Giao thức QKD sử dụng phương thức truyền dẫn khóa luận án đề xuất.**
1	Alice chọn một cách ngẫu nhiên một trong hai trạng thái phân cực để mã hóa mỗi một bit nhị phân.	**Alice chọn ngẫu nhiên một trong hai base** A_1 hoặc A_2 để mã hóa mỗi một bit nhị phân vào một trong hai giá trị của sóng mang quang.
2	Bob thực hiện tách và xác định giá trị bit thu được	Bob lập các giá trị của ϕ_B **bằng cách chọn một cách ngẫu nhiên một trong hai base**

	bằng việc lựa chọn ngẫu nhiên trạng thái của nó.	B_1 ($\phi_B = \pi/4$) hoặc B_2 ($\phi_B = -\pi/4$) để xác định các giá trị bit thu được.
3	Khóa chọn lọc được tạo ra.	Khóa chọn lọc được tạo ra.
4	Sửa lỗi và tạo ra các khóa không lỗi. Tạo ra khóa mới ngắn hơn.	Sửa lỗi và tạo ra các khóa không lỗi. Tạo ra khóa mới ngắn hơn.

2.2.2. Mô hình hệ thống đề xuất

Hình 2.3 mô tả sơ đồ khối của hệ thống QKD-FSO dựa trên vệ tinh sử dụng giao thức CV-QKD có điều chế QPSK ở phía phát và máy thu sử dụng bộ tách sóng kiểu heterodyne và cơ chế tách ngưỡng kép vì các ưu điểm của máy thu tách sóng heterodyne, cơ chế tách ngưỡng kép giúp hình thành các bit "0", "1" và bit "X" như trong giao thức gốc BB84.



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.

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.

Nguyên tắc hoạt động của hệ thống đề xuất:

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. Tại mỗi bộ điều chế MZM, pha của sóng mang quang tại mỗi một nhánh có giá trị tùy thuộc theo giá trị bit là "0" hay "1" như Bảng 2.2. Tín hiệu đầu ra của bộ điều chế MZM là tổng hợp của tín hiệu quang từ hai nhánh, tạo nên pha của Alice là ϕ_A.

Tại máy thu, tín hiệu quang nhận được sẽ trộn với sóng quang liên tục (Continuous Wave – CW) được tạo ra bởi bộ dao động quang nội (Local Ossilator – LO). Tín hiệu sau trộn được chuyển thành tín hiệu điện nhờ các đi-ốt quang thác APD. Tín hiệu điện sau đó được lọc bởi một bộ lọc thông dải để loại bỏ các tín hiệu không mong muốn trong khi các thành phần hữu ích tại tần số trung tần được giữ lại để đưa vào quá trình tiếp theo. Tiếp theo, dòng điện tại đầu ra của bộ lọc thông dải (Band Pass Filter – BPF) sẽ được nhân với tín hiệu tham chiếu dạng $\cos(2\pi f_{IF}t + \phi_B) = \cos(2\omega_{IF}t + \phi_B)$. Hai base dùng để giải mã của Bob được chọn ngẫu nhiên bằng cách thiết lập pha của tín hiệu tham chiếu. Tín hiệu sau giải mã sau đó được lọc bởi bộ lọc thông thấp (Low Pass Filter – LPF) để khôi phục tín hiệu băng gốc. Cuối cùng, 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

Tại đầu ra của bên phát Alice, có 4 giá trị khác nhau của ϕ_A tương đương với 4 trạng thái pha của mô hình điều chế pha QPSK. Tín hiệu với pha được chọn lựa ngẫu nhiên được biểu diễn theo công thức:

$$E_{Tx}(t) = \sqrt{P_T}\exp[i(2\pi f_c t + \phi_A)] \quad (2.15)$$

với P_T là công suất phát và f_c là tần số của sóng mang quang.

Xem xét đường truyền xuống từ vệ tinh tới trạm mặt đất. Giả thiết vệ tinh và trạm mặt đất ở các độ cao lần lượt là H_s và H_G. Với góc thiên đỉnh ζ, khoảng cách đường truyền từ vệ tinh tới trạm mặt đất tính theo công thức:

$$L = \frac{H_S - H_G}{\cos\zeta} \quad (2.16)$$

Hệ số suy hao kênh h bao gồm suy hao không gian tự do và suy hao khí quyển được tính theo công thức:

$$h = G_{Tx}\frac{A}{\pi(L\theta)^2}exp(-\gamma(\lambda)D_\beta)G_{Rx} = G_{Tx}G_{Rx}\frac{A}{\pi(L\theta)^2}h_a \quad (2.17)$$

Trong công thức (2.17), $A=\pi a_R^2$ là diện tích thu và a_R là bán kính của thấu kính thu, θ là góc phân kỳ của chùm tia, $\gamma(\lambda)$ là hệ số suy hao khí quyển phụ thuộc thời tiết, G_{Tx} và G_{Rx} lần lượt là các độ khuếch đại của các thấu kính tại bên phát và bên thu và D_β là khoảng cách truyền dẫn trong môi trường khí quyển. Giả thiết rằng dưới độ cao H_β, suy hao chính xảy ra là suy hao khí quyển và D_β được xác định theo công thức (2.6).

Tại máy thu, tín hiệu quang thu được tính theo công thức:

$$E_{Rx}(t) = \sqrt{P_R}\,exp[i(2\pi f_c t + \phi_A)] \quad (2.18)$$

với $P_R=P_T.h$ là công suất thu.

Tương tự, tín hiệu quang được tạo ra bởi bộ dao động nội LO được tính theo công thức:

$$E_{LO}(t) = \sqrt{P_{LO}}\,exp[i(2\pi f_{LO} t)] \quad (2.19)$$

Trong công thức (2.19), P_{LO}, f_{LO} lần lượt là công suất, tần số của bộ dao động nội. Theo mô hình tách sóng kiểu heterodyne, hai tín hiệu được trộn tại đầu vào của APD và tín hiệu điện tại đầu ra của APD được tính theo công thức sau:

$$I_p = \Re M_A |E_{Rx} + E_{LO}|^2$$

$$= \Re M_A \{(P_R + P_{LO}) + 2\sqrt{P_R P_{LO}} \cos[2\pi f_{IF} t + \phi_A]\} + i_n \quad (2.20)$$

với $f_{IF} = f_c - f_{LO}$ là tần số trung tần, f_c là tần số sóng mang quang, q là điện tích điện tử, i_n là dòng điện nhiễu, M_A, $\Re$ tương ứng là hệ số nhân thác lũ và đáp ứng của APD, $\Re = \frac{\eta q}{\tilde{h} f_c}$, với η là hiệu suất lượng tử, $\tilde{h}$ là hằng số Plank. Sau đó, tín hiệu sẽ được lọc bởi bộ lọc thông dải, bộ lọc này chỉ cho tần số trung tần đi qua. Quá trình giải mã được thực hiện bởi việc nhân thành phần tần số trung tần với $\cos(2\pi f_{IF} t + \phi_B)$. Dòng điện sau giải mã được tính toán theo công thức:

$$I_{decod}(t) = 2M_A \Re \sqrt{P_R P_{LO}} \cos[2\pi f_{IF} t + \phi_A] \cos[2\pi f_{IF} t + \phi_B] + i_n$$

$$= M_A \Re \sqrt{P_R P_{LO}} \cos[4\pi f_{IF} t + \phi_A + \phi_B] + M_A \Re \sqrt{P_R P_{LO}} \cos[\phi_A - \phi_B] + i_n \quad (2.21)$$

Sau đó, tín hiệu sau giải mã được lọc bởi bộ lọc thông thấp LPF để loại bỏ thành phần không mong muốn $4f_{IF}$. Kết quả là, dòng điện tại đầu vào của bộ tách ngưỡng kép có thể biểu thị theo công thức:

$$I = M_A \Re \sqrt{P_R P_{LO}} \cos[\phi_A - \phi_B] + i_n \quad (2.22)$$

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, với:

$$I_0 = M_A \Re \sqrt{P_R P_{LO}} \quad (2.23)$$

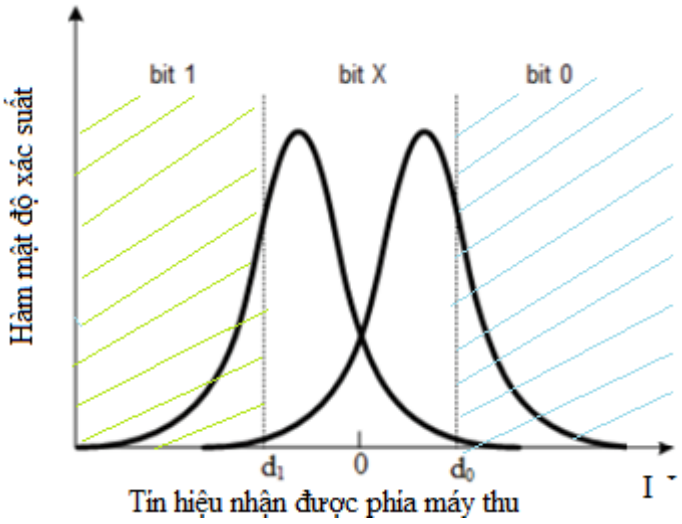
$$I_1 = -M_A \Re \sqrt{P_R P_{LO}} \quad (2.24)$$

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.

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:

$$\text{Giá trị bit} = \begin{cases} 1 \text{ nếu } I \leq d_1 \\ 0 \text{ nếu } I \geq d_0 \\ X \quad \text{trong trường hợp còn lại} \end{cases} \tag{2.25}$$

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



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.

Gọi P_{sift} là xác suất chọn lọc, đó là khi Bob sử dụng cùng base với Alice để giải mã chuỗi bit của khóa chọn lọc và P_{error} là xác suất có một số lượng các bit lỗi trong khóa chọn lọc do lỗi. Tỷ lệ lỗi bit lượng tử trong khóa chọn lọc được tính theo công thức (1.1). P_{sift} và P_{error} được tính theo công thức (1.2) và (1.3).

Các thành phần nhiễu được xem xét trong nội dung đề xuất bao gồm nhiễu dòng tối, nhiễu nhiệt và nhiễu nổ, những nhiễu này được thống kê dưới dạng các biến ngẫu nhiên Gauss với giá trị trung bình bằng 0. Theo luật của bộ tách sóng sử dụng cơ chế ngưỡng kép, các xác suất hợp $P_{A,B}(a,0)$ và $P_{A,B}(a,1)$ với a $\in \{0,1\}$ được tính như sau:

$$P_{A,B}(a,0) = \frac{1}{2} Q\left(\frac{d_0 - I_a}{\sigma_n}\right) \tag{2.26}$$

$$P_{A,B}(a,1) = \frac{1}{2} Q\left(\frac{I_{a-} d_1}{\sigma_n}\right) \tag{2.27}$$

Trong công thức (2.26) và (2.27), I_0 và I_1 được tính theo công thức (2.24) và (2.25); $d_0=\rho I_o$, $d_1=\rho I_1$ lần lượt là hai ngưỡng của bộ tách ngưỡng kép và ρ là hệ số tỷ lệ ngưỡng kép; hàm Q Gauss được tính theo công thức:

$$Q(.) \triangleq \frac{1}{\sqrt{2\pi}} \int_0^{\infty} \exp\left(-\frac{t^2}{2}\right) dt \tag{2.28}$$

và σ_n là tổng phương sai nhiễu, trong đó nhiễu nổ được tính theo [3]

$$\sigma_n = 2qM_A{}^{2+x}(\Re P_{LO} + I_d)\Delta f + \frac{4k_BT}{R_L}\Delta f \tag{2.29}$$

Trong công thức (2.29), q là điện tích electron, T là nhiệt độ của máy thu, I_d là dòng điện tối, x là hệ số nhiễu dư của APD, R_L là điện trở tải, k_B là hằng số Boltzmann, Δf là băng thông của máy thu, M_A là hệ số nhân thác lũ của APD.

Nhiễu nổ xuất hiện trong cả công suất quang thu được và cả trong công suất bộ dao động nội. Tuy nhiên P_{LO} lớn hơn rất nhiều P_R, do đó, nhiễu nổ phụ thuộc tín hiệu sẽ được bỏ qua.

2.2.4. Kết quả khảo sát hiệu năng hệ thống

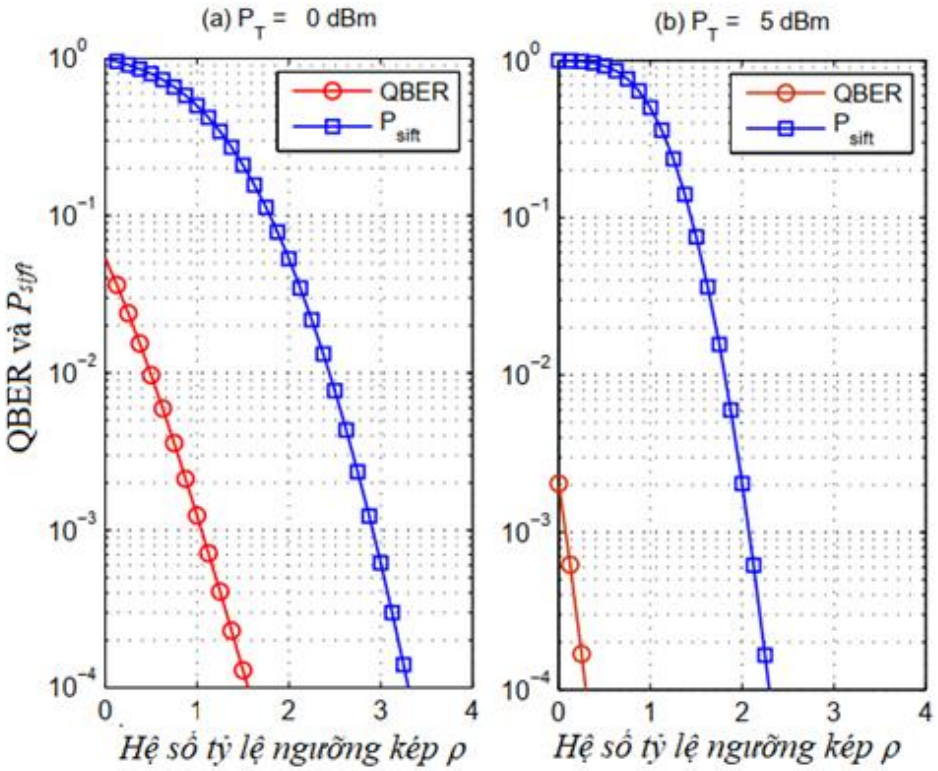
Mục này khảo sát giá trị của QBER và P_{sift} với các tham số chính của hệ thống để đánh giá tính khả thi của hệ thống phân phối khóa lượng tử biến liên tục qua không gian tự do dựa trên vệ tinh sử dụng phương thức truyền dẫn quang đề xuất dựa trên kỹ thuật điều chế QPSK ở phía phát và cơ chế tách ngưỡng kép ở phía thu. Luận án sẽ xác định các tiêu chí để thiết lập máy thu tại trạm mặt đất nhằm đảm bảo các điều kiện về an ninh khi có các cuộc tấn công trái phép. 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$\leq 10^{-3}$. $P_{sift} \geq 10^{-2}$ để máy thu hợp lệ Bob có đủ thông tin từ Alice, yêu cầu này tương đương với yêu cầu tốc độ khóa đạt được từ vài chục đến vài trăm Mb/s. QBER$\leq 10^{-3}$ để các lỗi của khóa sẽ được sửa tại máy thu bằng cách sử dụng các mã sửa lỗi (nếu có xảy ra lỗi).

Kết quả của việc phân tích hiệu năng thu được khi sử dụng các tham số và hằng số được liệt kê trong Bảng 2.4. QBER và P_{sift} được tính theo công thức (1.1) và (1.2) với các xác suất kết hợp được tính theo công thức (2.27) và (2.28). Các tham số trong Bảng 2.4 liên quan đến bộ thu phát quang được tham khảo từ [3] và các tham số liên quan đến trạm vệ tinh, trạm mặt đất dựa trên những thông số trong hệ thống truyền dẫn sử dụng đường truyền FSO dựa trên vệ tinh [82]. Giá trị $C_n^2(0) = 5 \times 10^{-15}$ $(m^{-2/3})$ và $C_n^2(0) = 7 \times 10^{-12}$ $(m^{-2/3})$ tương ứng với điều kiện nhiễu loạn khí quyển yếu và mạnh [58].

Bảng 2. 4. Bảng các tham số mô phỏng hệ thống QKD-FSO dựa trên vệ tinh sử dụng điều chế QPSK và cơ chế tách ngưỡng kép.

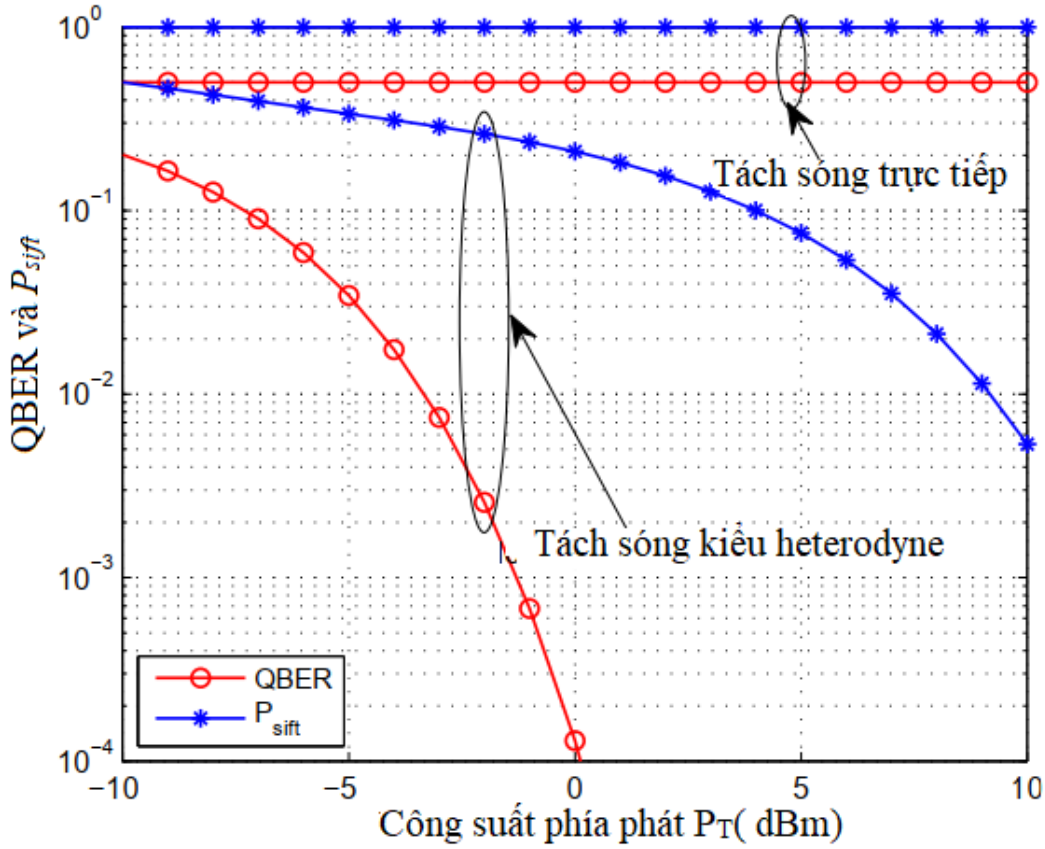
Tham số	**Ký hiệu**	**Giá trị**
Hằng số Boltzmanm	k_B	$1{,}38 \times 10^{-23}$ W/K/Hz
Điện tích electron	Q	$1{,}6 \times 10^{-19}$ C
Điện trở tải	R_L	50Ω
Nhiệt độ máy thu	T	298 K
Đáp ứng của APD	$\Re$	0,8
Hệ số nhiễu trội của APD	x	0,8 (InGaAs APD)
Hệ số nhân thác lũ của APD	M_A	10
Đường kính aperture của phía thu	D	0,02 m
Dòng điện tối	I_d	3 nA
Góc phân kỳ	θ	10^{-3} rad
Hệ số suy hao khí quyển	γ	0,43 dB/km
Bước sóng hoạt động	λ	1550 nm
Độ cao vệ tinh	H_S	600 km
Độ cao của trạm mặt đất	H_G	5 m
Độ cao tầng khí quyển	H_β	20 km
Góc thiên đỉnh	ζ	50˚
Bán kính phần thu	a_R	0,25 m

Độ khuếch đại của thấu kính phía phát	G_{Tx}	20 dB
Độ khuếch đại của thấu kính phía thu	G_{Rx}	20 dB
Tốc độ bit	R_b	10 Gb/s



Hình 2. 5. QBER và P_{sift} phụ thuộc vào các giá trị của hệ số tỷ lệ ngưỡng kép ρ khi P_{LO}= 0 dBm.

Ở Hình 2.5, trước tiên luận án khảo sát QBER và P_{sift} phụ thuộc hệ số tỷ lệ ngưỡng kép với hai giá trị của công suất phát là 0 dBm và 5 dBm. Có thể dễ dàng nhận thấy rằng xác suất Bob giải mã bit "1" hay bit "0" sai sẽ giảm khi khoảng cách của hai ngưỡng d_0 và d_1 lớn, ví dụ hệ số tỷ lệ ngưỡng kép lớn được sử dụng. Khi hệ số tỷ lệ tăng, P_{error} giảm, do đó kéo theo QBER và P_{sift} cũng giảm. Từ kết quả của Hình 2.5(a), có thể nhận thấy hệ số tỷ lệ được khuyến nghị nằm trong khoảng từ 1,2 đến 2,4 để giữ $P_{sift} \geq 10^{-2}$ và QBER $\leq 10^{-3}$. Khi công suất máy phát tăng tới 5 dBm như ở Hình 2.5 (b), giá trị của QBER và P_{sift} đều giảm. Do đó, hệ số tỷ lệ ngưỡng kép được khuyến nghị giảm tới 1,8 để đạt được $P_{sift} \geq 10^{-2}$.



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

Hình 2.6 đưa ra kết quả khảo sát QBER và P_{sift} khi hệ số tỷ lệ ngưỡng kép là cố định ở giá trị 1,5 và công suất máy phát P_T thay đổi. Qua kết quả khảo sát này, 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. Nội dung của Chương tập trung chính vào các đóng góp của luận án.

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. Phương thức truyền dẫn mà luận án đề xuất 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. Việc thiết lập mức công suất phát nhỏ kết hợp sử dụng máy thu ngưỡng kép và điều chế pha để thông qua ảnh hưởng của nhiễu tạp tạo ra khả năng an ninh cho hệ thống CV-QKD. Việc lựa chọn giá trị $P_{sift} \geq 10^{-2}$ nhằm mục đích đảm bảo tính bảo mật của hệ thống khi có cuộc tấn công trái phép từ Eve xảy ra.

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".

Hiệu năng của hệ thống truyền khóa lượng tử biến liên tục sử dụng phương thức truyền dẫn quang đề xuất được khảo sát khi có ảnh hưởng của nhiễu tại máy thu và suy hao kênh truyền. Kết quả phân tích hiệu năng đã chứng minh rằng hệ thống đề xuất đã đạt được tỷ lệ lỗi bit lượng tử QBER thấp (QBER $\leq 10^{-3}$) và tốc độ khóa chọn lọc đủ lớn, có thể đạt tới giá trị 100 Mb/s. Ngoài ra, phương thức truyền dẫn quang cho hệ thống phân phối khóa lượng tử biến liên tục đề xuất sử dụng điều chế pha kiểu QPSK yêu cầu sóng mang quang để điều chế giúp cho hệ thống tương thích với các hệ thống truyền thông quang truyền thống. Máy thu sử dụng tách sóng kiểu heterodyne giúp cải thiện độ nhạy của máy thu, có thể cải thiện đáng kể giá trị QBER so với máy thu loại tách sóng trực tiếp.

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 như các hệ thống được đề xuất trong nội dung của Chương 3 và Chương 4 của luận án 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

Tóm tắt

Nội dung của Chương 3 là giải pháp cải thiện hiệu năng hệ thống QKD-FSO dựa trên vệ tinh sử dụng kỹ thuật truyền lại khóa theo phương pháp yêu cầu phát lại tự động ARQ và kỹ thuật chuyển tiếp dựa trên hạ tầng trên cao HAP. Nội dung của Chương cũng trình bày về mô hình chuỗi Markov hai trạng thái được sử dụng để phân tích hiệu năng của hệ thống đã đề xuất. Hai kịch bản sẽ được xem xét khi đánh giá hiệu năng hệ thống đề xuất. Ở kịch bản thứ nhất, hệ thống QKD-FSO sử dụng kỹ thuật ARQ ngay tại vệ tinh. Ở kịch bản thứ hai với hệ thống QKD-FSO sử dụng kết hợp kỹ thuật chuyển tiếp dựa trên hạ tầng trên cao HAP với kỹ thuật ARQ tại trạm chuyển tiếp. Mô hình giải tích phân tích hiệu năng của hệ thống đề xuất dưới ảnh hưởng của các tham số đường truyền cũng đã được xây dựng. Kết quả nghiên cứu của Chương 3 đã được công bố trên 01 bài báo quốc tế ISI [J1] và 01 bài báo hội nghị ATC 2020 [C1].

3.1 Đặt vấn đề

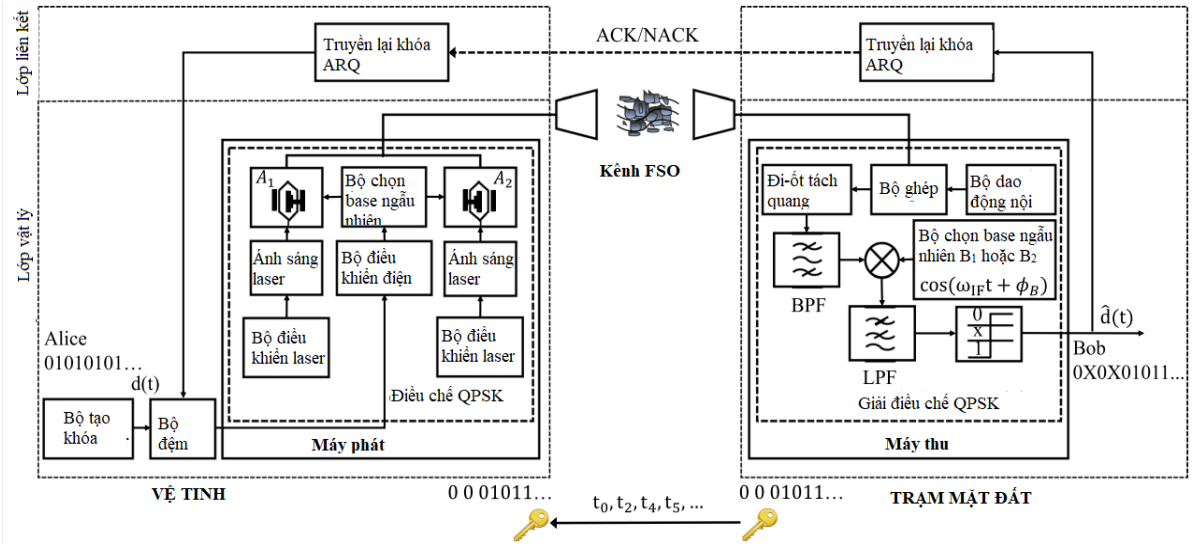
Hiệu năng của các hệ thống QKD-FSO dựa trên vệ tinh bị suy giảm bởi các yếu tố của kênh truyền từ Alice tới Bob như sự tán xạ, hấp thụ và nhiễu loạn khí quyển [53, 89] . Do đó, cho dù không có sự xuất hiện của kẻ nghe lén, tỷ lệ lỗi khóa có thể có giá trị lớn trong trường hợp nhiễu loạn khí quyển mạnh. Để giảm tỷ lệ lỗi của khóa, có thể sử dụng phương pháp sửa lỗi theo hướng phát FEC trong quá trình phát hiện lỗi và sửa lỗi ở bên phía thu như trong nghiên cứu [14] và [98]. Tuy nhiên, việc sử dụng phương pháp FEC có nhược điểm là yêu cầu thuật toán phức tạp để tối ưu hóa các bit cộng vào cho mục đích phát hiện lỗi và sửa lỗi. Hơn nữa, các kỹ thuật chỉ dựa trên phương pháp sửa lỗi theo hướng phát không đủ mạnh để đảm bảo tính tin cậy trong đường truyền có khoảng cách truyền lớn như từ vệ tinh tới các trạm mặt đất.

Luận án đề xuất giải pháp sử dụng kỹ thuật truyền lại khóa theo phương pháp yêu cầu phát lại tự động ARQ. Kỹ thuật ARQ sẽ truyền lại các khóa không truyền thành công để đảm bảo độ tin cậy của hệ thống. Kỹ thuật ARQ không yêu cầu các thuật toán phức tạp như FEC để điều khiển lỗi nhưng nó có thể gây ra độ trễ lớn vì khoảng cách của đường truyền là lớn khi khóa được truyền lại từ vệ tinh. Để giảm độ trễ khi truyền khóa, luận án đề xuất sử dụng bộ nhớ đệm tại vệ tinh để lưu trữ và truyền lại các khóa khi cần.

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.



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

Giả thiết phía phát là Alice được đặt tại vệ tinh và phía thu là Bob đặt tại trạm mặt đất. Các khóa bí mật được truyền từ Alice tới Bob thông qua kênh an toàn FSO trong khi đường phản hồi phục vụ truyền lại khóa từ Bob về Alice được gửi thông qua kênh RF công khai.

Tại phía phát bộ điều khiển điện tạo ra hai loại thông tin điều khiển phụ thuộc vào giá trị "1" hoặc "0" của các bit nhị phân từ chuỗi dữ liệu d(t). Thông tin điều khiển sẽ được dùng để chọn lựa pha của tín hiệu quang ở đầu ra của các bộ điều chế Mach-Zehnder. Bộ chọn base ngẫu nhiên sẽ lựa chọn tín hiệu quang tại đầu ra của một trong hai bộ điều chế Mach-Zehnder tương ứng với một trong hai base A_1 hoặc A_2 một cách ngẫu nhiên để mã hóa các bit của dữ liệu cần truyền đi vào pha của sóng mang quang được tạo ra từ đi-ốt laser. Tại mỗi bộ điều chế Mach-Zehnder, pha của sóng mang quang tại mỗi nhánh được xác định bởi giá trị bit là "0" hay "1" như trong Bảng 2.2. Tín hiệu tại đầu ra của bộ điều chế Mach-Zehnder là kết hợp của tín hiệu quang ở hai nhánh của bộ điều chế, tạo nên pha của tín hiệu phát đi từ Alice là ϕ_A.

Tại phía thu, tín hiệu quang nhận được sẽ được trộn với tín hiệu quang liên tục được tạo ra bởi bộ dao động quang nội LO. Một vòng khóa pha quang được sử dụng để giữ đồng bộ pha giữa bộ dao động quang nội LO và tín hiệu quang nhận được. Tín hiệu sau khi trộn được chuyển đổi thành dòng điện nhờ đi-ốt tách quang APD. Tín hiệu điện thu được sau đi-ốt APD sẽ tiếp tục được lọc bởi bộ lọc thông dải BPF để loại bỏ các tín hiệu không mong muốn và giữ lại toàn bộ các thành phần tần số trung tần hữu ích đi tới phần xử lý tiếp theo. Tiếp theo, tín hiệu trung tần tại đầu ra của BPF sẽ được nhân với tín hiệu tham chiếu $\cos(2\pi f_{IF}t+\phi_B)$. Hai base được Bob dùng để giải mã cũng được chọn lựa ngẫu nhiên bằng cách thiết lập pha của tín hiệu tham chiếu. Tín hiệu sau giải mã được đưa qua bộ lọc thông thấp LPF để khôi phục tín hiệu ở băng tần cơ bản. Cuối cùng, một bộ tách ngưỡng kép được sử dụng để quyết định bit sau giải mã có giá trị là "1" hoặc "0" hoặc "X".

3.2.2. Giao thức CV-QKD sử dụng

Giao thức QKD sử dụng là QKD dựa trên điều chế pha kiểu QPSK và cơ chế tách ngưỡng kép ở phía thu như đã mô tả ở mục 2.2 của Chương 2. 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. Giống như các bước thực hiện trong giao thức BB84 gốc, các thông tin phục vụ cho phát hiện lỗi và sửa lỗi sẽ được thêm vào vào khóa chọn lọc để bên thu có thể tiến hành phát hiện lỗi, sửa lỗi sau khi giải mã các thông tin nhận được từ Alice. Tuy nhiên, thay vì sử dụng kỹ thuật sửa lỗi theo hướng phát FEC, trong mô hình đề xuất của luận án sử dụng kỹ thuật phát lại tự động ARQ.

3.2.3. Kỹ thuật ARQ

Để giảm tỷ lệ mất khóa, kỹ thuật phát lại khóa sẽ được sử dụng ở lớp liên kết. Tại vệ tinh, chuỗi bit ngẫu nhiên $d(t)$ được tạo ra bởi bộ tạo khóa, trước tiên sẽ được xếp hàng tại bộ đệm. Sau đó, bộ đệm sẽ chuyển chuỗi bit này đến phần đầu của hàng đợi để tới máy phát. Chuỗi bit được truyền qua kênh truyền FSO tới máy thu ở trạm mặt đất. Thủ tục phát hiện lỗi trong ARQ có thể thực hiện tương tự như cơ chế FEC đã được sử dụng trong bước 4 của giao thức BB84. Cụ thể, sau bước 3 khi Alice và Bob thống nhất các bit chọn lọc sử dụng làm khóa, Alice tính checksum của các bit này và gửi cho Bob qua kênh công khai. Bob cũng tính checksum các bit khóa của mình rồi so sánh với checksum nhận được từ Alice. Nếu kết quả so sánh giống nhau, Bob gửi tín hiệu báo nhận thành công ACK (Acknowledgment – ACK) cho Alice, ngược lại, Bob sẽ gửi tín hiệu báo nhận không thành công NACK (Negative Acknowledgment – NACK). Do giới hạn của luận án, coi các bước 3 và 4 của giao thức CV-QKD liên quan tới các bước báo hiệu không có sai sót nên kỹ thuật ARQ đề xuất trong luận án sử dụng các hai thủ tục ACK và NACK. Các tín hiệu ACK hoặc NACK được gửi từ Bob tới Alice thông qua kênh RF công khai truyền thống. Nếu Alice nhận được tín hiệu ACK, Alice sẽ loại bỏ chuỗi bit đã phát khỏi bộ đệm. Nếu Alice nhận được tín hiệu NACK, Alice sẽ truyền lại chuỗi bit đã phát không thành công. Nếu gọi M là số lần tối đa cho phép truyền lại một chuỗi bit của Alice, chuỗi

bit sẽ bị loại bỏ khỏi bộ đệm sau khi được Bob nhận thành công hoặc sau *M* lần truyền lại nhưng đều bị lỗi. Chuỗi bit không thể gửi thành công tới phía thu có thể do bộ nhớ đệm bị tràn hoặc chuỗi bit đã bị loại bỏ sau *M* lần truyền lại đều bị lỗi.

3.2.4. Phân tích hiệu năng hệ thống

3.2.4.1. Phân tích hiệu năng lớp vật lý

A. Hệ thống QKD sử dụng điều chế QPSK và máy thu sử dụng tách sóng kiểu heterodyne và cơ chế tách ngưỡng kép

Tín hiệu quang với trạng thái pha được chọn lựa ngẫu nhiên phía Alice được biểu diễn theo công thức (2.13). Tín hiệu quang này được đưa tới thấu kính phát và được truyền qua kênh FSO, tín hiệu nhận được ở phía thu tại trạm mặt đất sẽ được biểu diễn theo công thức:

$$E_{Rx}(t) = \sqrt{P_R}\, exp[i(2\pi f_c t + \phi_A) \tag{3.1}$$

Trong công thức (3.1), $P_R = \frac{1}{L_{FS}} G_T P_T h_a h_l h_f G_R$ là công suất tín hiệu quang thu được ở phía thu; G_T, G_R tương ứng là độ khuếch đại của thấu kính phía phát và phía thu; L_{FS}, h_a, h_l, h_f tương ứng là suy hao trong không gian tự do, suy hao do khí quyển, suy hao do trải rộng chùm tia và ảnh hưởng của fading do nhiễu loạn khí quyển.

Tín hiệu quang nhận được ở máy thu E_{Rx} sẽ được trộn với tín hiệu quang liên tục được tạo ra ở bộ dao động nội. Tín hiệu quang được tạo ra ở bộ dao động nội được biểu diễn theo công thức (2.20). Tín hiệu quang này sẽ được chuyển đổi sang tín hiệu dòng điện bởi đi-ôt tách quang APD và tiếp tục được đi qua bộ lọc thông dải để lọc các tín hiệu không mong muốn. Tín hiệu điện sau khi nhân với tín hiệu tham chiếu được tín hiệu dòng điện sau giải mã là I_{decod}. Dòng điện I_{decod} sau khi qua bộ lọc thông thấp sẽ thu được tín hiệu dòng điện là *I*. Giá trị của *I* được tính theo công thức (2.23). Cuối cùng tín hiệu được đi qua bộ tách ngưỡng kép để quyết định giá trị của bit thu được là "1" hoặc "0" hặc "X". Luật của bộ tách ngưỡng kép tuân theo công thức (2.26).

B. Tỷ số lỗi bit lượng tử

Tỷ số lỗi bit lượng tử QBER được tính theo công thức (1.1) với P_{error} *và* P_{sift} được tính theo công thức (1.2) và (1.3).

Xác suất kết hợp của Alice-Bob qua kênh pha-đinh được mô tả bởi công thức sau:

$$\begin{cases} P_{A,B}(a,0) = \dfrac{1}{2}\displaystyle\int_0^{\infty} Q\left(\frac{d_0 - I_a}{\sigma_n}\right) f_{h_f}(h_f)dh_f \\ P_{A,B}(a,1) = \dfrac{1}{2}\displaystyle\int_0^{\infty} Q\left(\frac{I_a - d_1}{\sigma_n}\right) f_{h_f}(h_f)dh_f \end{cases} \quad (3.2)$$

với $P_{A,B}(a,b)$ là xác suất kết hợp mà Alice gửi bit "*a*" và Bob giải mã ra bit "*b*" với $a,b \in \{0,1\}$. Q(.) là hàm Q Gauss được biểu diễn ở công thức (2.29) và σ_n là tổng phương sai nhiễu được tính theo công thức (2.30). I_0 và I_1 là dòng điện thu được tại máy thu không có nhiễu được xác định theo công thức (2.24) và (2.25).

Để xác định các giá trị ngưỡng kép d_0 và d_1, luận án đề xuất chọn giá trị ngưỡng xác định theo công thức của nghiên cứu [85] như sau:

$$d_0 = E[i_0] + \rho\sqrt{\sigma_n} \quad (3.3)$$

$$d_1 = E[i_1] - \rho\sqrt{\sigma_n} \quad (3.4)$$

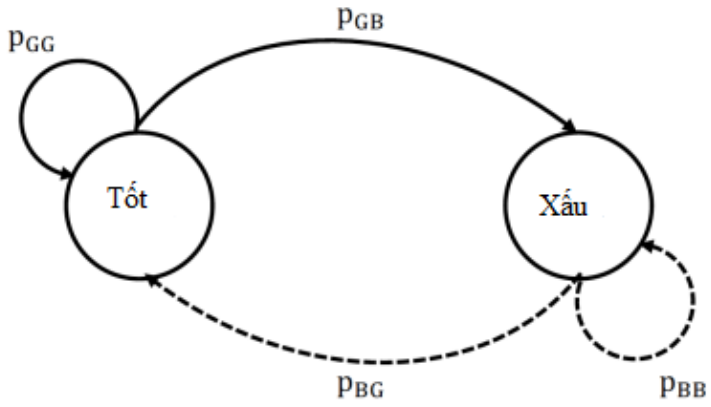
Với ρ là hệ số tỷ lệ ngưỡng kép tại bộ tách ngưỡng kép. Khi $E[h_f] = 1, E[i_a]$ là giá trị trung bình của i_a có thể được biểu diễn theo công thức sau:

$$\begin{cases} E[i_0] = M_A \Re \sqrt{\dfrac{1}{L_{FS}} P_T P_{LO} G_T G_R h_a h_l}, \\ E[i_1] = -M_A \Re \sqrt{\dfrac{1}{L_{FS}} P_T P_{LO} G_T G_R h_a h_l}. \end{cases} \quad (3.5)$$

3.2.4.2. Phân tích hiệu năng lớp liên kết

A. Mô hình trạng thái kênh lượng tử

Chuỗi Markov hai trạng thái được đề xuất để mô tả sự chuyển đổi trạng thái của kênh lượng tử. Mô hình này được sử dụng rộng rãi trong việc toán học hóa các kênh truyền không dây [76].



Hình 3. 2. Mô hình chuyển đổi trạng thái 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) như minh họa ở Hình 3.2. Một trạng thái đường truyền được xem là tốt khi mà tất cả các khóa chọn lọc được truyền qua mà không có lỗi. Nếu tất cả các lần truyền đều lỗi, trạng thái đường truyền sẽ là xấu.

Từ công thức tính QBER ở (1.1), xác suất thu đúng của 1 bit trong khóa chia sẻ được xác định là 1- QBER.

Khóa thu được ở bên thu là đúng khi và chỉ khi tất cả các bit ở trong khóa chia sẻ được thu đúng. Với chiều dài của chuỗi bit ngẫu nhiên là l_{bs}, xác suất bên thu tách được các bit "0" và "1" là P_{sift}, xác suất thu đúng của 1 khóa sẽ là $(1 - \text{QBER})^{l_{bs}P_{sift}}$.

Do đó, tỷ lệ lỗi khóa lượng tử (Quantum Key Error – QKER) được tính theo công thức như sau:

$$\mathrm{QKER} = 1 - (1 - \mathrm{QBER})^{l_{bs}P_{sift}} \tag{3.6}$$

Thông qua QKER, các xác suất chuyển đổi của trạng thái kênh có thể được tính như sau:

$$\begin{cases} P_{GG} = \mathrm{QKER}\left(1 - \dfrac{\tau_{bs}}{\tau_0}\right), \\ P_{BB} = (1 - \mathrm{QKER})\left(1 - \dfrac{\tau_{bs}}{\tau_0}\right), \\ p_{BG} = 1 - p_{BB}, \\ p_{GB} = 1 - p_{GG}, \end{cases} \tag{3.7}$$

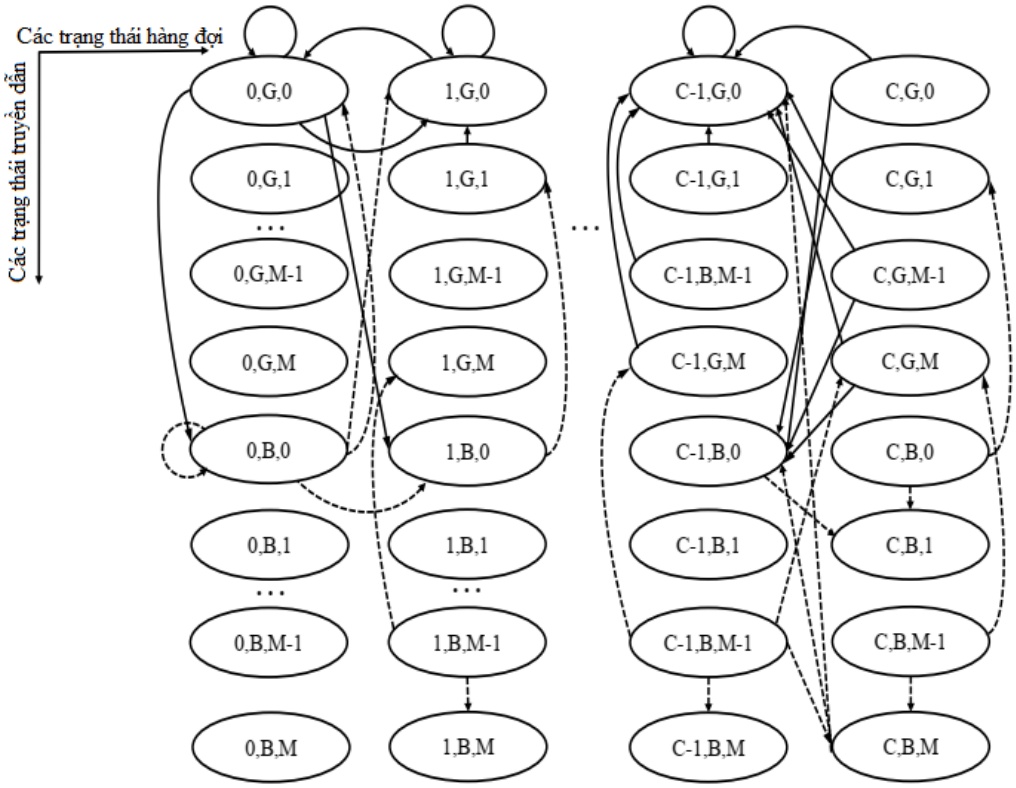
Trong công thức (3.7), $\tau_{bs} = \frac{l_{bs}}{R_b}$ là thời gian truyền một chuỗi bit, đó chính là độ lớn của một khe thời gian; R_b là tốc độ bit của hệ thống; $\tau_0 = \frac{\sqrt{\lambda D_\beta}}{\nu}$ là khoảng thời gian mà điều kiện nhiễu loạn không thay đổi với D_β là độ dài của đường truyền trong môi trường khí quyển, ν là vận tốc gió trung bình, λ là bước sóng quang.

B. Chuỗi Markov rời rạc thời gian liên kết hàng đợi

Tại vệ tinh, chuỗi bit được tạo ra và đưa vào bộ đệm với thông lượng H (chuỗi/giây). Quá trình Bernoulli tĩnh được dùng để mô hình hóa quá trình đến bộ đệm của chuỗi bit. Do đó, $H\tau_{bs}$ và 1-$H\tau_{bs}$ tương ứng là các xác suất có một chuỗi bit hoặc không có một chuỗi bit đến một khe thời gian xem xét. Trong một khe thời gian cho trước, đường truyền FSO giữ ổn định tại trạng thái hiện tại. Một chuỗi bit được truyền tới bộ phát của Alice tại thời điểm bắt đầu của khe thời gian nếu hàng đợi không rỗng. Một chuỗi bit sẽ bị loại bỏ tại thời điểm cuối của mỗi khe thời gian nếu việc truyền được thành công.

Tại thời điểm đầu tiên của mỗi khe thời gian, một chuỗi Markov rời rạc thời gian (Discrete Time Markov Chain – DTMC) ba chiều có thể được xác định bởi (n_L, s_L, m_L). Trong đó, $n_L \in [0, C]$ là số chuỗi bit xếp hàng tại bộ đệm của Alice, trạng thái của đường truyền được biểu diễn bằng $s_L \in [B, G]$, m_L là số lần truyền lại của một chuỗi bit. Chuỗi Markov rời rạc thời gian ba chiều đề xuất được gọi là DTMC

liên kết hàng đợi (Queue - Associated DTMC). Các trạng thái có cả m_L>1 và n_L=0 là không thể tồn tại. Sự chuyển các trạng thái của QA-DTMC được mô tả trong Bảng 3.1 và Hình 3.3.



Hình 3. 3. Sự chuyển đổi các trạng thái của QA-DTMC.

Bảng 3. 1. Sự chuyển trạng thái của DTMC.

Trạng thái hiện tại	**Trạng thái tiếp theo**	**Xác suất chuyển đổi**
(0,*B*,0)	(1, *B*, 0)	$H\tau_{bs}p_{BB}$
	(1, *G*, 0)	$H\tau_{bs}p_{BG}$
	(0, *B*, 0)	$(1-H\tau_{bs})p_{BB}$
	(0, *G*, 0)	$(1-H\tau_{bs})p_{BG}$
(*n*,*B*,*m*)	(*n*+1, *B*, *m*+1)	$H\tau_{bs}p_{BB}$
n∈[1, *C*-1]	(*n*+1, *G*, *m*+1)	$H\tau_{bs}p_{BG}$
m ∈[1, *M*-1]	(*n*, *B*, *m*+1)	$(1-H\tau_{bs})p_{BB}$
	(*n*, *G*, *m*+1)	$(1-H\tau_{bs})p_{BG}$

(n, B, m) n∈[1, C-1]	(n, B, 0) (n, G, 0) (n-1, B, 0) (n-1, G, 0)	$H\tau_{bs}p_{BB}$ $H\tau_{bs}p_{BG}$ $(1-H\tau_{bs})p_{BB}$ $(1-H\tau_{bs})p_{BG}$
(C, B, m) m ∈[1, M-1]	(C, B, m+1) (C, G, m+1)	p_{BB} p_{BG}
(C, B, M)	(C-1, B, *0*) (C-1, G, *0*)	p_{BB} p_{BG}
(*0*,*G*,*0*)	(1, B, 0) (1, G, 0) (0, B, 0) (0, G, 0)	$H\tau_{bs}p_{GB}$ $H\tau_{bs}p_{GG}$ $(1-H\tau_{bs})p_{GB}$ $(1-H\tau_{bs})p_{GG}$
(n, G, m) n ∈[1, C-1] m ∈[0, M]	(n, B, 0) (n, G, 0) (n-1, B, 0) (n-1, G, 0)	$H\tau_{bs}p_{GB}$ $H\tau_{bs}p_{GG}$ $(1-H\tau_{bs})p_{GB}$ $(1-H\tau_{bs})p_{GG}$
(C, G, m) m ∈[0, M]	(C-1, B, 0) (C-1, G, 0)	p_{GB} p_{GG}

C. Tỷ lệ mất khóa

Xác suất của trạng thái bền trong DTMC liên kết hàng đợi được biểu diễn bằng $\pi(n_L, s_L, m_L)$ và được xác định bằng cách giải hệ phương trình sau:

$$\begin{cases} \Pi^T P_L = \Pi^T \\ \sum_{n_L=0}^{C} \sum_{s_L \epsilon \{B,G\}} \sum_{m_L=0}^{M} \pi(C, s_L, m_L) = 1, \end{cases} \quad (3.8)$$

với Π=[$\pi(n_L, s_L, m_L)$]; P_L là ma trận chuyển đổi với kích thước $(C+1) \times 2 \times (M+1)$ và các thành phần của nó được chỉ ra trong cột thứ 3 của Bảng 3.1. Phương trình (3.8) được giải nhờ các phương pháp đại số bao gồm phép lặp Jacobi và khử Gauss [42] . Π có thể được xác định như sau:

$$\Pi = [\pi(0,G,0), \pi(1,G,0), \ldots\ldots, \pi(C,G,M), \pi(0,B,0), \pi(1,B,0), \ldots\ldots \pi(C,B,M)], \quad (3.9)$$

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:

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

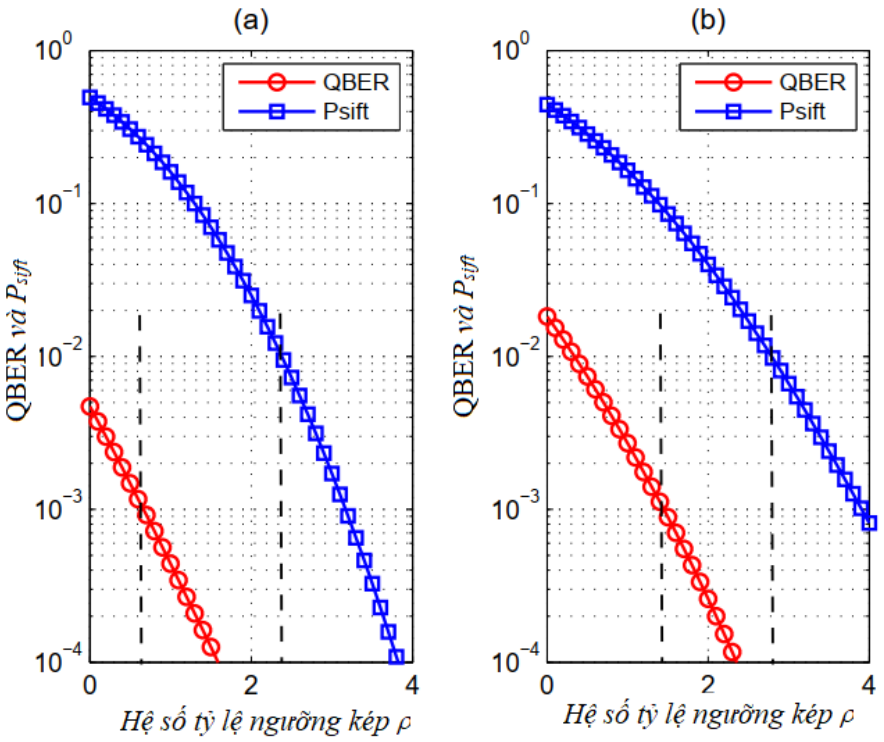
3.2.5. Kết quả khảo sát hiệu năng hệ thống

Trong phần này, luận án sẽ xác định tập tham số để thiết lập cho máy thu tại Bob để đảm bảo các điều kiện đảm bảo an ninh khi có các cuộc tấn công vào máy thu. Các hệ số và các tham số chính của hệ thống được liệt kê trong Bảng 3.2, các tham số liên quan đến bộ thu phát quang được tham khảo từ [3] và các tham số liên quan đến trạm vệ tinh, trạm mặt đất dựa trên những thông số trong hệ thống truyền dẫn sử dụng đường truyền FSO dựa trên vệ tinh [83]. Chiều dài chuỗi bit của khóa chia sẻ (khóa thô) dựa trên điều kiện QBER≤10^{-3} và $P_{sift} \geq 10^{-2}$. QBER, P_{sift}, KLR lần lượt được tính theo các công thức (1.1), (1.2), (1.3) và (3.10), trong đó các xác suất kết hợp được tính theo công thức (3.2). Giá trị $C_n^2(0) = 5 \times 10^{-15}$ $(m^{-2/3})$ và $C_n^2(0) = 7 \times 10^{-12}$ $(m^{-2/3})$ tương ứng với nhiễu loạn khí quyển yếu và mạnh được sử dụng cho khảo sát.

Bảng 3. 2. Các hằng số và các tham số hệ thống dùng trong khảo sát hiệu năng hệ thống đề xuất

Tham số	**Ký hiệu**	**Giá trị**
Các tham số chung		
Hằng số Boltzmann	k_B	1,38 × 10^{-23} W/K/Hz
Điện tích electron	q	1,6 × 10^{-19} C
Điện trở tải	R_L	50 Ω

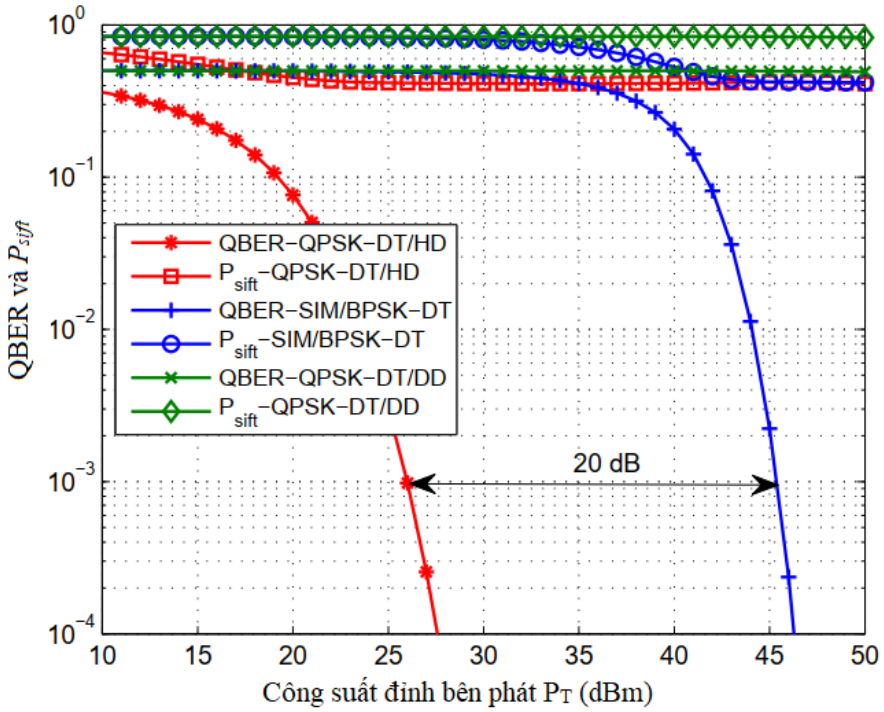
Nhiệt độ máy thu	T	298K
Hệ số nhiễu trội của APD	x	0,8 (Điôt APD loại InGaAS)
Tốc độ bit của hệ thống	R_b	10 Gb/s
Hệ số nhân thác lũ của APD	M_A	10
Dòng điện tối	I_d	3 nA
Đáp ứng của APD	$\Re$	0,8
Các tham số kênh		
Bước sóng quang	λ	1550 nm
Vận tốc gió	v	21 m/s
Góc thiên đỉnh	ζ	50^0
Hệ số suy hao	γ	0,43 dB/km
Bán kính của khẩu độ tách sóng	a_r	0,31 m
Độ rộng của chùm tia tại trạm mặt đất	ω_D	50m
Độ cao vệ tinh	H_s	600 km
Độ cao trạm mặt đất	H_G	5m
Độ cao khí quyển	H_β	20 km
Độ khuếch đại của thấu kính phát	G_T	120 dB
Độ khuếch đại của thấu kính thu	G_R	121 dB
Các tham số lớp liên kết		
Thông lượng	H	185 chuỗi/s
Chiều dài của một chuỗi bit	l_{bs}	3×10^6 bit



Hình 3. 4. QBER và P_{sift} tại máy thu phụ thuộc vào hệ số tỷ lệ ngưỡng kép trong điều kiện nhiễu loạn khí quyển (a) yếu và (b) mạnh với P_T=25 dBm và P_{LO}= 0dBm.

Kết quả khảo sát sự phụ thuộc của tham số hiệu năng QBER và P_{sift} vào hệ số tỷ lệ ngưỡng kép trong điều kiện nhiễu loạn khí quyển khác nhau ở Hình 3.4 cho thấy xác suất máy thu tách nhầm bit là nhỏ khi hệ số tỷ lệ ngưỡng kép lớn được sử dụng, lúc này sự khác biệt giữa hai ngưỡng d_0 và d_1 là lớn. Do đó, P_{error} giảm khi hệ số tỷ lệ ngưỡng kép tăng, QBER và P_{sift} cũng giảm. Việc Bob cần phải thu đủ lượng thông tin từ Alice là rất quan trọng. Mục tiêu của việc thiết kế hệ thống là cung cấp P_{sift} bằng hoặc lớn hơn 10^{-2} để máy thu Bob có đủ thông tin từ Alice, tương đương với yêu cầu tốc độ khóa đạt được là từ vài chục đến vài trăm Mb/s. Hơn nữa, hệ thống cần giữ giá trị QBER$\leq 10^{-3}$ sao cho các lỗi của khóa sẽ được sửa tại máy thu nếu lỗi xảy ra bằng cách sử dụng các mã sửa lỗi. Dựa trên những yêu cầu về giá trị của QBER và P_{sift}, có thể thấy hệ số tỷ lệ ngưỡng kép của bộ tách sóng ngưỡng kép được khuyến nghị nằm trong khoảng $0,7 \leq \rho \leq 2,4$ trong điều kiện nhiễu loạn khí quyển yếu (Hình 3.4 (a)) và $1,4 \leq \rho \leq 2,8$ trong điều kiện nhiễu loạn khí quyển mạnh (Hình 3.4.(b)).

Trong thực tế, máy thu có thể thiết lập hệ số tỷ lệ ngưỡng kép của bộ tách ngưỡng kép dựa trên thông tin về trạng thái kênh được tính bằng cách sử dụng các tín hiệu pilot.

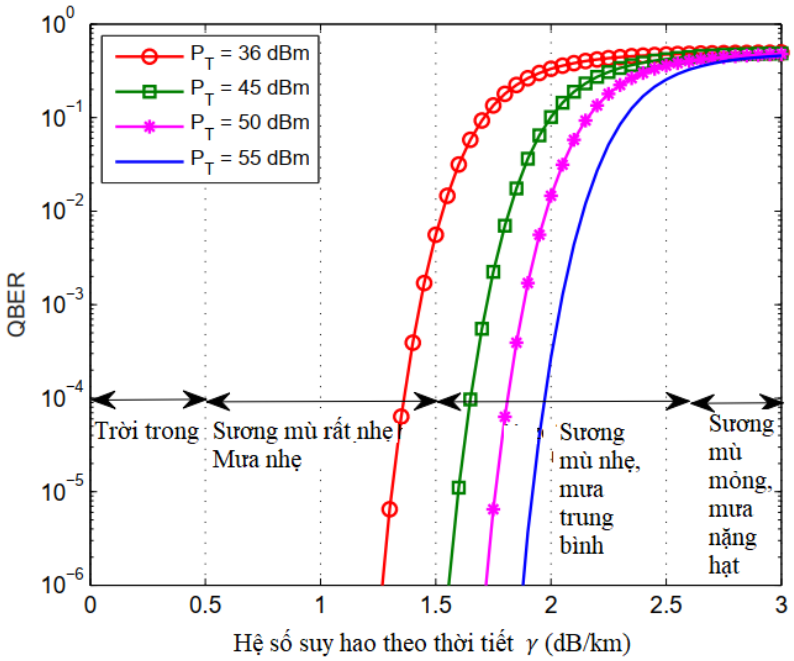


Hình 3. 5. QBER và P_{sift} phụ thuộc vào công suất đỉnh bên phát P_T trong điều kiện nhiễu loạn khí quyển yếu trong ba trường hợp: QPSK-DT/HD (ρ=0,7 và P_{LO}=0 dBm), QPSK-DT/DD (ρ=0,7) và SIM/BPSK-DT (ρ=0,9)

Hình 3.5 là kết quả khảo sát QBER và P_{sift} tại máy thu trong điều kiện nhiễu loạn khí quyển yếu phụ thuộc vào công suất đỉnh của máy phát P_T. Để thuận tiện cho việc so sánh, ba mô hình điều chế/ tách sóng được sử dụng là mô hình QPSK-DT/HD quang, QPSK-DT/DD và SIM/BPSK-DT. Trong tất cả ba loại hệ thống QKD, độ lớn P_{sift} đều đáp ứng yêu cầu $P_{sift} \geq 10^{-2}$. Tuy nhiên, máy thu có kiểu tách sóng heterodyne mang lại kết quả QBER tốt nhất. Hệ thống QKD sử dụng loại QPSK-DT/HD quang có QBER nhỏ nhất so với hệ thống QKD sử dụng loại QPSK-DT/DD và SIM/BPSK-DT. Kết quả khảo sát ở Hình 3.5 cũng xác định công suất phát yêu cầu để QBER tại máy thu đảm bảo yêu cầu QBER$\leq 10^{-3}$. Trong trường hợp sử dụng QPSK-DT/HD quang, công suất nhỏ nhất tại máy thu được yêu cầu là 25 dBm trong khi giá trị này

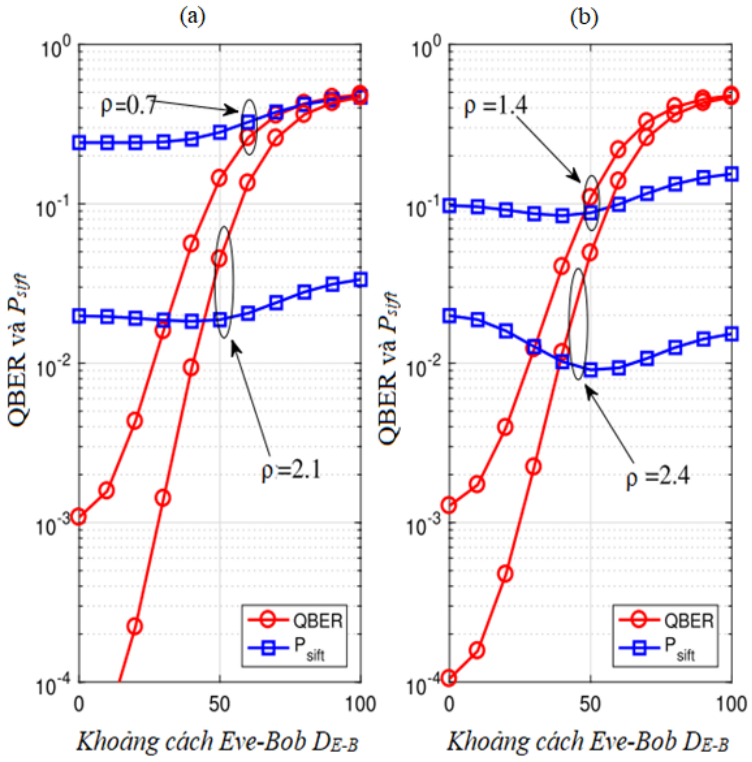
là 45 dBm (tương ứng với 20 dB) trong trường hợp hệ thống QKD sử dụng SIM/BPSK-DT.

Hình 3.6 là kết quả khảo sát sự thay đổi của QBER tại máy thu theo các hệ số suy giảm khác nhau. Kịch bản cho khảo sát là công suất đỉnh phía phát trong bốn trường hợp có giá trị lần lượt là 36 dBm, 45 dBm, 50 dBm, 55 dBm; điều kiện nhiễu loạn khí quyển mạnh; hệ số tỷ lệ ngưỡng kép của bộ tách ngưỡng kép được đặt là 1,4. Độ khuếch đại của các thấu kính phát và thu trong khảo sát lần lượt là G_T= 130 dB và G_R= 131 dB. Điều kiện thời tiết sẽ được xác định thông qua các hệ số suy hao và có ảnh hưởng rõ rệt tới hệ số QBER tại máy thu. Bằng việc xác định giá trị của công suất phát phù hợp, hệ thống đề xuất có thể làm việc tốt trong các điều kiện thời tiết khác nhau. Ví dụ, khi P_T= 45 dBm, QBER tại máy thu $\leq 10^{-3}$ có thể được đảm bảo trong điều kiện hệ số suy hao thời tiết $0 \leq \gamma \leq 0{,}5$, mưa nhỏ và điều kiện thời tiết sương mù nhẹ $0{,}5 \leq \gamma \leq 1{,}53$. Tuy nhiên, một dải giá trị lớn của công suất sẽ được yêu cầu trong điều kiện sương mù nhiều hơn hoặc mưa trung bình $1{,}54 \leq \gamma \leq 2{,}68$ để hệ thống có thể đáp ứng được tham số hiệu năng QBER như yêu cầu.



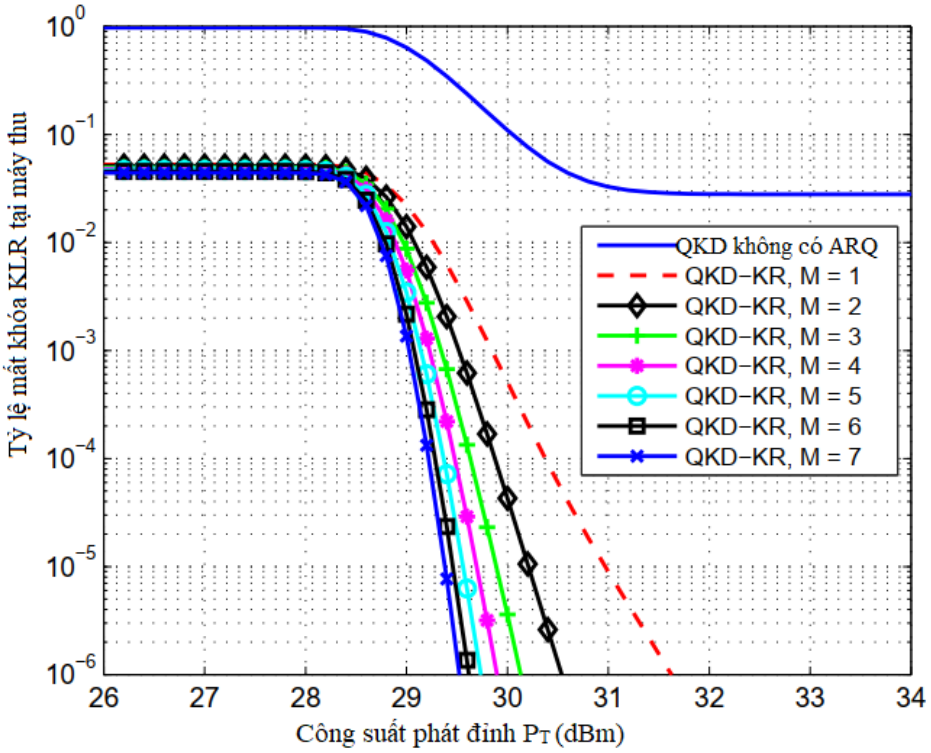
Hình 3. 6. Hệ số QBER phụ thuộc các hệ số suy giảm thời tiết khác nhau (γ) trong điều kiện nhiễu loạn khí quyển mạnh với P_{LO}= 0 dBm, G_T=130 dB và G_R= 131 dB.

Hình 3.7 là kết quả khảo sát sự phụ thuộc của QBER và P_{sift} với khoảng cách của Eve và Bob ($D_{E\text{-}B}$) trong các điều kiện nhiễu loạn khí quyển yếu (a) và mạnh (b). Trường hợp xấu nhất là trường hợp Eve có hệ số tỷ lệ ngưỡng kép của máy thu cùng giá trị với Bob. Rõ ràng, các điều kiện ràng buộc về độ bảo mật của hệ thống QKD sẽ được điều chỉnh bởi các vị trí của Eve. Đặc biệt, QBER tại Eve sẽ nhỏ khi Eve được đặt gần Bob và do đó, Eve có thể tách được một cách không hợp pháp khóa mà Alice đã gửi cho Bob. Do đó, QBER tại Eve phải lớn hơn giá trị 10^{-2} để đảm bảo Eve không tách đúng được khóa thậm chí cả trong trường hợp Eve có mã sửa lỗi. Dựa trên yêu cầu này, khoảng cách tối thiểu giữa Eve và Bob để đảm bảo điều kiện bảo mật là 30 m trong cả điều kiện nhiễu loạn khí quyển yếu và mạnh. Eve có thể giảm QBER bằng cách tăng hệ số tỷ lệ của bộ tách ngưỡng kép, tuy nhiên điều này đồng nghĩa với việc giảm P_{sift} và kết quả là lượng thông tin mà Eve thu được từ Alice cũng giảm.



Hình 3. 7. QBER và P_{sift} tại Eve phụ thuộc vào khoảng cách D_{E_B} giữa Eve và Bob trong điều kiện nhiễu loạn khí quyển yếu (ρ=0,7 và 2,1) và nhiễu loạn khí quyển mạnh (ρ=1,4 và 2,4) với P_T=25 dBm, P_{LO}= 0 dBm.

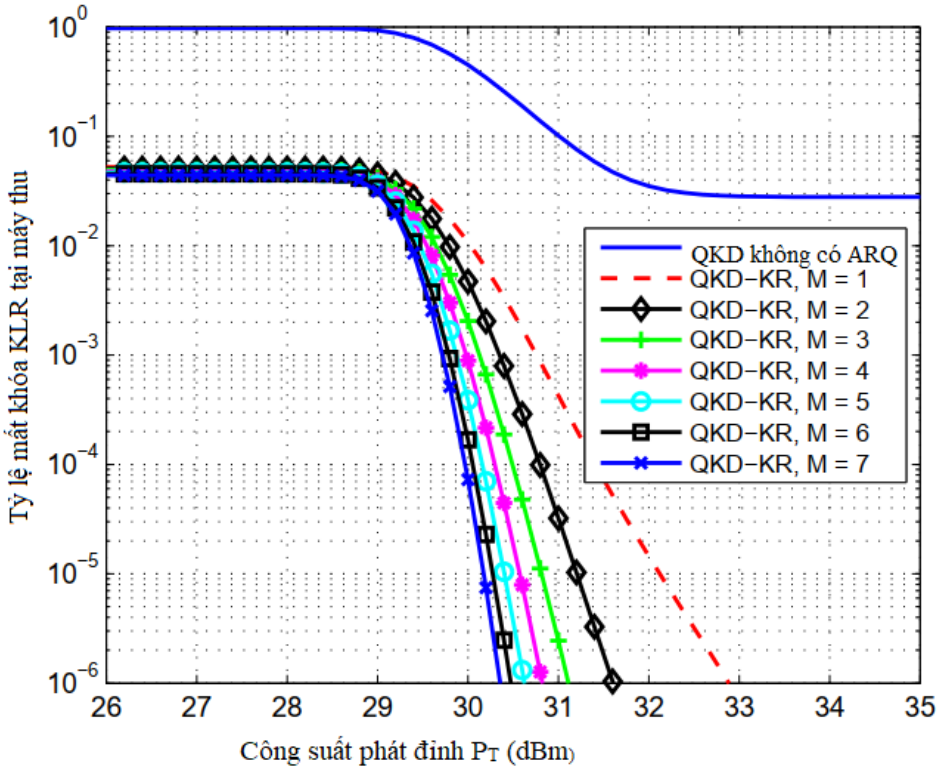
Kết quả khảo sát hiệu năng hệ thống đánh giá thông qua tham số tỷ lệ mất khóa ở phía máy thu với các điều kiện khác nhau của hệ thống bao gồm công suất đỉnh phía phát P_T và số lần tối đa được phép truyền lại một chuỗi bit.



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 3.8 là kết quả khảo sát tỷ lệ mất khóa KLR tại Bob phụ thuộc vào công suất đỉnh phía phát P_T khi P_{LO} = 0 dBm và và hệ số tỷ lệ ρ = 0,7 trong điều kiện nhiễu loạn khí quyển yếu $C_n^2(0) = 5 \times 10^{-15}$. Khảo sát sẽ thực hiện so sánh KLR của hệ thống QKD không sử dụng kỹ thuật phát lại khóa với hệ thống QKD có số lần phát lại khóa tối đa là M= {1,2,3,4,5,6,7}. Hệ thống không sử dụng kỹ thuật ARQ có kết quả KLR cao do nhiễu loạn khí quyển. Đặc biệt, giá trị KLR nhỏ nhất đạt được là 3 $\times 10^{-12}$ 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. Điều này vô cùng quan trọng trong trường hợp nhiễu loạn khí quyển mạnh bởi vì lúc này công suất phát lớn hơn sẽ được yêu cầu.



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

Hình 3.9 là kết quả khảo sát tỷ lệ mất khóa KLR tại Bob phụ thuộc vào công suất đỉnh phía phát P_T khi P_{LO}= 0 dBm và và hệ số tỷ lệ ρ=1,4 trong điều kiện nhiễu loạn khí quyển mạnh $C_n^2(0) = 7 \times 10^{-12}$. Kết quả của khảo sát cho thấy tại giá trị KLR =10^{-6} độ lợi về mặt công suất là 2 dB khi số lần truyền lại tối đa được phép tăng từ 1 đến 4. Điều này đạt được vì với số lần truyền lại tối đa được phép lớn hơn có thể bù khóa mất do nguyên nhân công suất phát nhỏ hơn. Tuy nhiên, độ lợi về mặt công suất chỉ là 0,5 dB khi giá trị của *M* tăng từ 4 lên 7. Do đó, độ lợi về mặt công suất khi giá trị *M* lớn hơn 4 là không đáng kể. Hơn nữa, việc truyền lại khóa cũng gây ra trễ nên *M* lớn hơn 4 không được khuyến khích chọn.

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.

Thứ nhất, kẻ nghe lén Eve có thể thu được chính xác chuỗi bit tương ứng với chuỗi trạng thái pha đã phát đi, cần có giả thiết là nhiễu tạp đủ nhỏ.

Trong quá trình thiết kế, lựa chọn các tham số của hệ thống QKD-FSO đề xuất dựa trên điều chế QPSK ở phía phát, luận án đã tiến hành khảo sát để đưa ra khuyến nghị lựa chọn tham số công suất phát nhỏ. Giá trị công suất phát này đủ để máy thu hợp pháp Bob tách được chuỗi bit với tham số QBER đạt yêu cầu tối thiểu. Kết quả khảo sát ở Hình 3.5 đã xác định công suất phát nhỏ nhất là 25 dBm để tham số hiệu năng QBER tại máy thu đảm bảo $QBER \leq 10^{-3}$. Mức công suất phát nhỏ được sử dụng với mục đích thông qua ảnh hưởng của nhiễu tạp sẽ khiến kẻ nghe lén Eve khó có thể thu được chính xác toàn bộ chuỗi bit mà Alice phát đi.

Thứ hai, trong một dải rộng các giá trị ngưỡng kép được thiết lập ở máy thu, xác suất Eve biết được giá trị ngưỡng kép mà Bob sử dụng là rất nhỏ. Nếu Bob và Eve sử dụng giá trị ngưỡng kép khác nhau, số lượng bit chọn lọc và vị trí các bit chọn lọc mà Bob và Eve nhận được sẽ khác nhau. Ngoài ra, đặc tính kênh truyền quang qua không gian giữa Alice và Bob khác đặc tính kênh truyền giữa Alice và Eve, đặc biệt dưới sự ảnh hưởng ngẫu nhiên của nhiễu loạn khí quyển phụ thuộc và không gian và tạp âm ngẫu nhiên ở máy thu. Kết quả là, ví dụ Alice phát đi 20 bit có thứ tự từ 1 đến 20, Bob sau khi loại bỏ nhận được 4 bit có thứ tự là 1, 3, 12, 19 và Eve nhận được 5 bit có thứ tự lần lượt là 2, 7, 12, 16, 20. Trong trường hợp này, dù Eve có phát hiện được nhiều bit hơn nhưng vị trí các bit không trùng hoàn toàn với vị trí các bit mà Bob thu được do đó Eve không đánh cắp được khóa. Trong tính toán này còn chưa tính tới trường hợp có các bit lỗi trong số các bit nhận được.

Thứ ba, hình thức tấn công người ở giữa khó thực hiện đối với hệ thống QKD-FSO dựa trên vệ tinh vì hệ thống QKD-FSO hoạt động dựa trên nguyên tắc truyền

dẫn tầm nhìn thẳng LoS, do búp sóng laser có kích thước hẹp nên giữa thấu kính phát và thấu kính thu phải thỏa mãn yêu cầu về việc đồng chỉnh, giữ thẳng hướng giữa bộ phát và bộ thu. Eve muốn thu lén được tín hiệu từ Alice, Eve phải nằm trong vùng phủ footprint của Alice. Với kích thước đường kính footprint nhỏ (0,5m), kích thước trạm mặt đất khá lớn (đường kính thấu kính thu 0,62m) như trong Bảng 3.2 kèm theo hệ thống dò, bắt và bám tín hiệu thì việc phát hiện có trạm thu lén là hết sức dễ dàng bằng mắt thường hoặc camera an ninh.

Luận án giả thiết khi xảy ra tình huống xấu, Eve thu lén tín hiệu mà Bob không biết và đã khảo sát QBER của Eve với khoảng cách giữa Bob và Eve thay đổi như chỉ ra trong Hình 3.7. QBER tại Eve đạt giá trị lớn hơn 10^{-2} khi khoảng cách giữa Eve và Bob lớn hơn 30m, giá trị QBER này để đảm bảo Eve không tách đúng được khóa thậm chí cả trong trường hợp Eve có mã sửa lỗi. Tuy nhiên, ngay cả trong trường hợp này, Eve cũng không thể phát lại cho Bob vì Bob hướng thấu kính thu tới vệ tinh và không nhận được tín hiệu quang laser từ Eve. Trong trường hợp Eve sử dụng vệ tinh ở quỹ đạo thấp hơn hoặc các trạm hạ tầng trên cao HAP, kích thước lớn của các trạm này sẽ chắn búp sóng laser có kích thước hẹp từ Alice đến Bob và Bob bị gián đoạn tín hiệu thu và có thể phát hiện kẻ tấn công Eve ở giữa.

Với hệ thống QPSK đề xuất trong luận án, nguy cơ tấn công này có thể lượng hóa thông qua xác suất Eve thu được chính xác trạng thái pha của toàn bộ chuỗi bit phát đi. Với tốc độ truyền dẫn xấp xỉ Gbit/s kèm theo công suất phát thấp, ảnh hưởng của nhiễu loạn khí quyển và các loại nhiễu tạp như đã đề cập ở trên, xác suất này là rất nhỏ.

Thực tế luận án cũng đã khảo sát xác suất chọn lọc (P_{sift}), xác suất Eve tách được bit 0 hoặc 1, và tỉ lệ lỗi bit lượng tử của Eve ($\mathrm{QBER_{Eve}}$). Từ hai tham số này sẽ tính xác suất Eve có thể thu chính xác chuỗi khóa thô có độ dài N theo công thức:

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

Công thức này xuất phát từ điều kiện Eve tách được bit 0 hoặc 1 trong N bit của chuỗi khóa thô và tất cả các bit đó đều không bị lỗi. Từ công thức này, 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. 3. 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 và QBER = 2×10^{-3} P_{Eve} = **$2{,}3 \times 10^{-90}$**	P_{sift} = 0,3 và QBER = $1{,}5\times10^{-1}$ P_{Eve} = **1×10^{-76}**
Nhiễu loạn mạnh	P_{sift} = 0,1 và QBER = 2×10^{-3} P_{Eve} = **$6{,}8 \times 10^{-129}$**	P_{sift} = 0,09 và QBER = 1×10^{-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 năng 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

Việc đầu tiên để tăng cường độ mạnh của đường truyền vật lý là sử dụng kỹ thuật chuyển tiếp dựa trên hạ tầng trên cao HAP như minh họa ở Hình 3.10. Trong kỹ thuật này, một trạm chuyển tiếp được đặt tại HAP để khôi phục các khóa lượng tử được truyền từ vệ tinh tới, sau đó trạm chuyển tiếp sẽ tiếp tục phát lại các khóa lượng tử đã khôi phục tới trạm mặt đất. Kỹ thuật sử dụng trạm chuyển tiếp dựa trên hạ tầng trên cao HAP giúp cho khóa lượng tử được tái tạo tại trạm chuyển tiếp, do đó tỷ lệ lỗi khóa lượng tử sẽ được giảm đi.

Hình 3. 10. Hệ thống QKD-FSO có vệ tinh sử dụng kỹ thuật chuyển tiếp dựa trên hạ tầng trên cao HAP và kỹ thuật truyền lại khóa theo phương pháp ARQ.

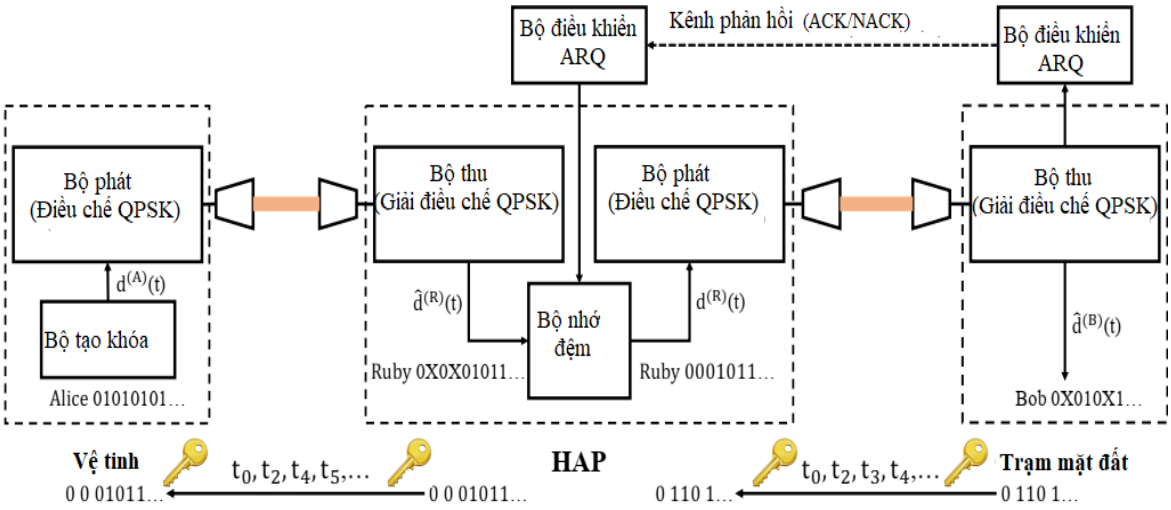
Việc tiếp theo để cải thiện hiệu năng hệ thống là sử dụng kỹ thuật truyền lại khóa theo phương pháp ARQ. Để giảm độ trễ do khoảng cách của đường truyền là lớn khi khóa được truyền lại từ vệ tinh xuống trạm chuyển tiếp, luận án đề xuất sử dụng bộ nhớ đệm tại HAP để lưu trữ và truyền lại các khóa khi cần. Do khoảng cách từ HAP tới trạm mặt đất nhỏ hơn nhiều so với khoảng cách từ vệ tinh tới trạm mặt đất nên độ trễ được giảm đi một cách đáng kể.

3.3.1. Mô hình hệ thống đề xuất

Hình 3.11 là sơ đồ khối của hệ thống mà luận án đề xuất bao gồm một vệ tinh (Alice), một trạm chuyển tiếp dựa trên hạ tầng trên cao HAP (Ruby) và một trạm mặt đất (Bob). Trạm mặt đất sẽ nhận tín hiệu quang từ trạm chuyển tiếp để khôi phục lại các khóa được truyền từ Alice đến. Một kênh quang truyền thống sẽ được sử dụng cho đường truyền tín hiệu phản hồi ARQ. Hệ thống trong Hình 3.11 được phát triển từ hệ thống đã đề xuất trong Hình 3.1. Hệ thống này sử dụng kết hợp cả kỹ thuật ARQ và kỹ thuật chuyển tiếp dựa trên hạ tầng trên cao HAP. Nhược điểm của kỹ thuật ARQ là làm tăng độ trễ, đặc biệt khi truyền lại khóa từ vệ tinh, với giải pháp truyền lại khóa từ trạm chuyển tiếp, trễ truyền dẫn sẽ giảm. Ngoài ra, kỹ thuật HAP giúp cho

khóa lượng tử được tái tạo tại trạm chuyển tiếp, từ đó lỗi khóa lượng tử sẽ giảm, hiệu năng của hệ thống sẽ được cải thiện.

Tại vệ tinh, chuỗi bit ngẫu nhiên $d^{(A)}t$ được tạo ra bởi bộ tạo khóa sẽ được điều chế tại bộ điều chế quang QPSK, sau đó đưa ra thấu kính phát. Tín hiệu quang từ bộ phát của Alice sẽ được truyền thẳng tới bộ giải điều chế quang QPSK tại trạm chuyển tiếp Ruby. Bộ điều chế và bộ giải điều chế quang theo kiểu điều chế/giải điều chế QPSK đã được mô tả chi tiết ở giải pháp đề xuất trong Chương 2 của luận án. Tín hiệu quang truyền đi được khuếch đại bởi một thấu kính có độ khuếch đại $G_T^{(A)}$ và được truyền tới trạm chuyển tiếp HAP qua một kênh an toàn FSO.



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.

Tại trạm chuyển tiếp tại hạ tầng trên cao HAP, tín hiệu quang nhận được từ Alice trước tiên sẽ được đi qua thấu kính thu có độ khuếch đại $G_R^{(R)}$, tiếp theo tín hiệu sẽ được đưa tới bộ giải điều chế QPSK để tách sóng quang chuỗi bit. Máy thu sử dụng cơ chế tách ngưỡng kép để xác định các bit “0”, “1” hoặc các bit “X”.

Trên đường truyền vệ tinh-HAP, suy hao trong không gian tự do được xác định là yếu tố suy hao chính làm suy giảm chất lượng của tín hiệu thu được tại trạm chuyển tiếp dẫn tới tỷ lệ lỗi khóa lượng tử QKER có giá trị nhỏ. Nếu Ruby nhận khóa chọn

lọc không thành công, Ruby sẽ hủy khóa ngay lập tức mà không sử dụng kỹ thuật FEC. Nếu Ruby thu được khóa chọn lọc thành công và không có lỗi, khóa chọn lọc trở thành khóa bí mật được chia sẻ giữa Alice và Ruby. Sau đó, khóa sẽ được đưa vào bộ nhớ đệm của Ruby. Bộ nhớ đệm của Ruby sẽ chuyển khóa này tới đầu của hàng đợi để đưa tới điều chế tại bộ điều chế QPSK. Tín hiệu sau điều chế quang QPSK tại phía Ruby sẽ được đưa qua thấu kính phát của HAP có độ khuếch đại là $G_T^{(R)}$.

Tại trạm mặt đất, tín hiệu quang thu được sẽ đi qua thấu kính thu có độ khuếch đại $G_R^{(B)}$ và bộ giải điều chế QPSK. Tại trạm mặt đất, chuỗi bit cũng được giải mã bởi bộ thu sử dụng cơ chế tách ngưỡng kép. Bob sẽ thông báo cho cả Alice và Ruby về khoảng thời gian mà Bob tạo ra các bit nhị phân. Kết quả là, một chuỗi bit xác định (khóa chọn lọc) được chia sẻ giữa Alice, Bob và Ruby.

Như vậy, quá trình Alice và Bob thống nhất khóa chọn lọc có thể tóm tắt như sau: Alice gửi khóa thô sơ cấp tới trạm chuyển tiếp Ruby; trạm chuyển tiếp Ruby gửi các bit chọn lọc lần thứ nhất (khóa thô thứ cấp) tới Bob sau khi xóa đi các bit không xác định; Bob thỏa thuận với Ruby về vị trí các bit chọn lọc lần hai trong chuỗi bit khóa thô thứ cấp nhận được từ trạm chuyển tiếp. Tiếp theo, trạm chuyển tiếp thỏa thuận với Alice về vị trí các bit chọn lọc trong chuỗi khóa thô sơ cấp nhận được từ Alice. Nhờ đó Bob và Alice thống nhất được khóa chọn lọc.

3.3.2. Kỹ thuật truyền lại khóa

Giả thiết rằng nhiễu loạn khí quyển là yếu tố xuất hiện chính trong đường truyền HAP-mặt đất, kỹ thuật ARQ được sử dụng giữa Ruby và Bob để cải thiện hiệu năng của hệ thống. Nếu khóa chọn lọc được Bob nhận thành công và không có lỗi, Bob sẽ gửi một bản tin ACK cho cả Alice và Ruby ngay lập tức. Tại bộ nhớ đệm của Ruby, Ruby sẽ xóa các bit tương ứng với các bit trong khóa chọn lọc đã được nhận thành công. Nếu Bob không thành công trong việc nhận khóa chọn lọc, Ruby sẽ truyền lại chuỗi bit tương ứng với khóa chọn lọc được nhận không thành công này. Nếu gọi M là số lần tối đa cho phép Ruby phát lại một chuỗi bit, một chuỗi bit được xác định là bị rớt nếu sau M lần Ruby cố gắng phát lại không thành công, một bản tin NACK sẽ

được Bob gửi đi cho cả Ruby và Alice đồng thời bộ nhớ đệm của Ruby cũng xóa các bit tương ứng với khóa đã được cố gắng gửi đi *M* lần nhưng không thành công này.

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. Tỷ lệ mất khóa được xác định bằng tỷ số giữa chuỗi bit mất trên tổng số chuỗi được phát đi. Tỷ lệ trễ vượt ngưỡng được xác định bằng chuỗi bit nhận được có độ trễ vượt quá ngưỡng cho trước.

A. Tỷ lệ lỗi khóa lượng tử

Tỷ lệ lỗi bit lượng tử QBER được xác định bằng tỷ lệ của các bit lỗi của khóa chọn lọc, được định nghĩa theo công thức (1.1).

Trong trường hợp của hệ thống đề xuất, P_{sift} là xác suất mà Ruby và/ hoặc Bob có thể tách các bit "0" và "1" dựa trên quy luật của bộ tách sóng ngưỡng kép. P_{sift} tính theo công thức (1.2).

Đường truyền vệ tinh-HAP

Suy hao trong không gian tự do là nguyên nhân chính trong việc làm suy giảm chất lượng tín hiệu quang tại phía thu. Các xác suất kết hợp của Alice-Ruby thông qua đường truyền FSO được xác định như sau:

$$\begin{cases} P_{A,R}(a,0) = \frac{1}{2} Q\left(\frac{d_0^{(AR)} - I_a^{(AR)}}{\sigma_N}\right), \\ P_{A,R}(a,1) = \frac{1}{2} Q\left(\frac{I_a^{(AR)} - d_1^{(AR)}}{\sigma_N}\right), \end{cases} \tag{3.12}$$

Trong công thức (3.12), Q(.) là hàm Q Gauss được tính theo công thức (2.20); I_a là dòng điện tín hiệu của Ruby và/ hoặc Bob tương ứng với bit "a". I_a được xác định như sau:

$$\begin{cases} I_0^{(AR)} = M_A \Re \sqrt{\dfrac{1}{L_{FS}} G_T^{(A)} P_T^{(AR)} G_R^{(R)} P_{LO}} \\ I_1^{(AR)} = -M_A \Re \sqrt{\dfrac{1}{L_{FS}} G_T^{(A)} P_T^{(AR)} G_R^{(R)} P_{LO}} \end{cases} \quad (3.13)$$

Trong công thức (3.13), $P_T^{(AR)}$ là công suất phát; P_{LO}là công suất của bộ dao động nội LO; $M_A, \Re$ tương ứng là hệ số nhân thác lũ và hệ số đáp ứng của đi-ốt quang thác APD; L_{FS} là suy hao trong không gian tự do; $G_T^{(A)}$ và $G_R^{(R)}$ lần lượt là độ khuếch đại của thấu kính phát phía Alice và độ khuếch đại của thấu kính thu phía Ruby.

Hai ngưỡng tách quang $d_0^{(AR)}$ và $d_1^{(AR)}$ trong công thức (3.12) được xác định như sau:

$$\begin{cases} d_0^{(AR)} = E\left[I_0^{(AR)}\right] + \rho^{(AR)}\sqrt{\sigma_n^2} \\ d_1^{(AR)} = E\left[I_1^{(AR)}\right] - \rho^{(AR)}\sqrt{\sigma_n^2} \end{cases} \quad (3.14)$$

trong đó, $\rho^{(AR)}$ là hệ số tỷ lệ ngưỡng kép, $E\left[I_x^{(AR)}\right]$ là giá trị trung bình của $I_x^{(AR)}$, σ_n là tổng phương sai nhiễu và được xác định theo công thức (2.30).

Tỷ lệ lỗi khóa lượng tử $QKER^{(AR)}$ với các khóa được hình thành từ $l_{bs}P_{sift}^{(AR)}$ các bit nhận được. Tỷ lệ lỗi khóa lượng tử sẽ được tính theo công thức:

$$\mathrm{QKER}^{(\mathrm{AR})} = 1 - (1 - \mathrm{QBER}^{(AR)})^{l_{bs}P_{sift}^{(AR)}} \quad (3.15)$$

trong đó l_{bs} là độ dài của một chuỗi bit ngẫu nhiên.

Đường truyền HAP-trạm mặt đất:

Xác suất kết hợp của Ruby-Bob được mô tả bởi công thức sau:

$$\begin{cases} P_{R,B}(a,0) = \dfrac{1}{2}\displaystyle\int_0^{\infty} Q\left(\dfrac{d_0^{(RB)} - I_a^{(RB)}}{\sigma_N}\right) f_{h_f}(h_f)dh_f \\ P_{R,B}(a,1) = \dfrac{1}{2}\displaystyle\int_0^{\infty} Q\left(\dfrac{I_a^{(RB)} - d_1^{(RB)}}{\sigma_N}\right) f_{h_f}(h_f)dh_f \end{cases} \tag{3.16}$$

với:

$$\begin{aligned} I_0^{(RB)} &= M_A \Re \sqrt{G_T^{(R)} P_T^{(RB)} G_R^{(B)} P_{LO} h_a h_l h_f} \\ I_1^{(RB)} &= -M_A \Re \sqrt{G_T^{(R)} P_T^{(RB)} G_R^{(B)} P_{LO} h_a h_l h_f} \end{aligned} \tag{3.17}$$

Trong công thức (3.17), $P_T^{(RB)}$ là công suất phát tại phía phát của Ruby; $G_T^{(R)}$ và $G_R^{(B)}$ lần lượt là độ khuếch đại của thấu kính phát phía Ruby và độ khuếch đại thấu kính thu phía Bob; h_a, h_l, h_f lần lượt là suy hao khí quyển, suy hao do trải rộng chùm tia và nhiễu loạn khí quyển. Tại trạm mặt đất, bộ thu sử dụng cơ chế tách ngưỡng kép cũng được sử dụng với hệ số tỷ lệ ngưỡng kép là $\rho^{(RB)}$. Tỷ lệ lỗi khóa lượng tử được xác định bằng công thức:

$$\mathrm{QKER}^{(\mathrm{RB})} = 1 - (1 - \mathrm{QBER}^{(\mathrm{RB})})^{l_{bs} P_{sift}^{(AR)} P_{sift}^{(RB)}} \tag{3.18}$$

B. Sự chuyển đổi các trạng thái đường truyền.

Các xác suất chuyển trạng thái của các trạng thái đường truyền được tính theo công thức:

$$\begin{cases} P_{GG} = \left(1 - \mathrm{QKER}^{(\mathrm{AR})}\right)\left(1 - \mathrm{QKER}^{(\mathrm{RB})}\right)\left(1 - \dfrac{\tau_{bs}}{\tau_0}\right), \\ P_{BB} = \left(1 - \mathrm{QKER}^{(\mathrm{AR})}\right)\left(\mathrm{QKER}^{(\mathrm{RB})}\right)\left(1 - \dfrac{\tau_{bs}}{\tau_0}\right), \\ p_{BG} = 1 - p_{BB}, \\ p_{GB} = 1 - p_{GG}, \end{cases} \tag{3.19}$$

với τ_{bs} là thời gian truyền một chuỗi bit, τ_0 là khoảng thời gian mà điều kiện nhiễu loạn không thay đổi. Cách xác định τ_{bs} và τ_0 đã được trình bày trong công thức (3.7).

C. Tỷ lệ mất khóa

Tại phía thu của Ruby, chuỗi bit được mã hóa $\hat{d}^{(R)}(t)$ được chuyển tới bộ đệm với tốc độ H (chuỗi bit/ giây). Quá trình Bernoulli tĩnh được dùng để mô hình hóa quá trình đến của chuỗi bit. Nếu gọi $p^{(ar)}$ và $p^{(no)}$ tương ứng là xác suất khi một chuỗi bit đến hoặc không có một chuỗi bit đến trong một khe thời gian xác định thì $p^{(ar)}$ và $p^{(no)}$ được tính theo công thức:

$$p^{(ar)} = (1 - QBER^{(AR)})H\tau_{bs} \tag{3.20}$$

$$p^{(no)} = (1 - QBER^{(AR)})(1 - H\tau_{bs}) \tag{3.21}$$

Trong một khe thời gian cho trước, đường truyền FSO giữ ổn định tại trạng thái hiện tại. Một chuỗi bit được truyền tới bộ phát của Ruby tại thời điểm bắt đầu của khe thời gian nếu hàng đợi không rỗng. Một chuỗi bit sẽ bị loại bỏ tại thời điểm cuối của mỗi khe thời gian nếu việc truyền được thành công.

Tại thời điểm đầu tiên của mỗi khe thời gian, một chuỗi Markov rời rạc thời gian ba chiều có thể được xác định bởi (n_L, s_L, m_L). Trong đó, $n_L \in [0, C]$ là số chuỗi bit xếp hàng tại bộ đệm của Ruby, trạng thái của đường truyền được biểu diễn bằng $s_L \in [B, G]$, m_L là số lần truyền lại của một chuỗi bit. Tỷ lệ mất khóa do nguyên nhân các lần truyền lại đều không thành công và do bộ nhớ đệm của Ruby bị tràn được tính theo công thức (3.10). Bảng 3.3 minh họa sự chuyển trạng thái của DTMC.

Bảng 3. 4. Sự chuyển trạng thái của DTMC

Trạng thái hiện tại	**Trạng thái tiếp theo**	**Xác suất chuyển đổi**
(0,*B*,0)	(1,*B*,0)	$p^{(ar)}p_{BB}$
	(1,*G*,0)	$p^{(ar)}p_{BG}$
	(0,*B*,0)	$p^{(no)}p_{BB}$
	(0,*G*,0)	$p^{(no)}p_{BG}$
(*n*,*B*,*m*)	(*n*+1, *B*, *m*+1)	$p^{(ar)}p_{BB}$
n∈[1, *C*-1]	(*n*+1, *G*, *m*+1)	$p^{(ar)}p_{BG}$
m ∈[1, *M*-1]	(*n*, *B*, *m*+1)	$p^{(no)}p_{BB}$

	$(n, G, m+1)$	$p^{(no)}p_{BG}$
(n, B, m) $n \in [1, C-1]$	$(n, B, 0)$ $(n, G, 0)$ $(n-1, B, 0)$ $(n-1, G, 0)$	$p^{(ar)}p_{BB}$ $p^{(ar)}p_{BG}$ $p^{(no)}p_{BB}$ $p^{(no)}p_{BG}$
(C, B, m) $m \in [1, M-1]$	$(C, B, m+1)$ $(C, G, m+1)$	p_{BB} p_{BG}
(C, B, M)	$(C-1, B, 0)$ $(C-1, G, 0)$	p_{BB} p_{BG}
$(0, G, 0)$	$(1, B, 0)$ $(1, G, 0)$ $(0, B, 0)$ $(0, G, 0)$	$p^{(ar)}p_{GB}$ $p^{(ar)}p_{GG}$ $p^{(no)}p_{GB}$ $p^{(no)}p_{GG}$
(n, G, m) $n \in [1, C-1]$ $m \in [0, M]$	$(n, B, 0)$ $(n, G, 0)$ $(n-1, B, 0)$ $(n-1, G, 0)$	$p^{(ar)}p_{GB}$ $p^{(ar)}p_{GG}$ $p^{(no)}p_{GB}$ $p^{(no)}p_{GG}$
(C, G, m) $m \in [0, M]$	$(C-1, B, 0)$ $(C-1, G, 0)$	p_{GB} p_{GG}

D. Phân tích hiệu năng trễ

Xem xét khoảng thời gian khi mà một chuỗi bit đến bộ nhớ của Ruby, một chuỗi Markov rời rạc thời gian ba chiều kết nối chuỗi bit được đề xuất. (n_D, s_D, m_D) mô tả trạng thái hiện tại của chuỗi bit, với $n_D \in [1, q_D], s_D \in [B, G]$ và $m_D \in [0, M]$. Số chuỗi bit xếp hàng tại hàng đợi tại bộ nhớ đệm của Ruby ngoại trừ chuỗi bit đang được truyền là $n_D - 1$. s_D là trạng thái hiện tại của đường truyền và m_D là số lần truyền lại của chuỗi bit hiện tại. q_D là chiều dài hàng đợi của Ruby bao gồm cả chuỗi đang được truyền. Tại thời điểm cuối của quá trình DTMC, một trạng thái (lỗi hoặc thành công) tương đương với chuỗi bit hiện tại bị rớt sau M lần cố gắng truyền lại

hoặc khôi phục mà không có lỗi, được xác định bởi Bảng 3.4 mô tả tất cả các khả năng chuyển đổi của bước tiếp theo.

(q_D, s_L, m_L) là trạng thái đầu tiên kết nối với trạng thái hiện tại của chuỗi bit.

$p_{j(q_D,s_L,m_L),\ (Success)}$ là khả năng một chuỗi bit có thể được nhận một cách thành công tại khe thời gian thứ j. Xác suất điều kiện mà trễ hàng đợi của mỗi chuỗi bit thu được lớn hơn $\mathcal{D}/\mathcal{T}_{bs}$ khe thời gian có thể được biểu diễn bằng công thức:

$$\Pr\left\{t_Q > \frac{\mathcal{D}}{\tau_{bs}} | ((q_D, s_L, m_L)\right\} = \frac{\sum_{j=\frac{\mathcal{D}}{\tau_{bs}}+2}^{q_D(M+1)} p_{j_{(q_D,s_L,m_L),\ (Success)}}}{\sum_{j=q_D}^{q_D(M+1)} p_{j_{(q_D,s_L,m_L),\ (Success)}}} \qquad (3.22)$$

với $\mathcal{D}$ là độ trễ lớn nhất mà đường truyền ARQ cho phép và t_Q là trễ hàng đợi của bộ đệm của Ruby.

Bảng 3. 5. Xác suất chuyển đổi trạng thái của một chuỗi bit QKD khi sử dụng mô hình chuỗi Markov rời rạc thời gian 3 chiều kết nối.

Trạng thái hiện tại	**Trạng thái tiếp theo**	**Xác suất chuyển đổi**
(q_D, B, m_L) $q_D \in (1,B]$, $m_L \in [0,M)$	(q_D, B, m_L +1) (q_D, G, m_L +1)	p_{BB} p_{BG}
(q_D, B, M) $q_D \in (1,B]$	(q_D - 1, B, 0) (q_D - 1, G, 0)	p_{BB} p_{BG}
(1, B, m_L) $m_L \in [0,M)$	(1, B, m_L+1) (1, G, m_L+1)	p_{BB} p_{BG}
(1,B,M)	*Lỗi*	1
(q_D, G, m_L) $q_D \in (1,B]$, $m_L \in [0,M]$	(q_D -1, B, 0) (q_D -1, G, 0)	p_{GB} p_{GG}
(1, G, m_L) $m_L \in$ [0,M]	*Thành công*	1

Dựa vào xác suất trạng thái tĩnh của DTMC kết nối hàng đợi QKD đề xuất, chúng ta có thể có được xác suất của mỗi một trạng thái ban đầu liên kết với một chuỗi bit được xem xét theo công thức:

$$\Pr = \{(q_D, s_L, m_L)\} = \pi(q_D - 1, s_L, m_L)/\pi_v \quad (3.23)$$

trong đó:

$$\pi_v = \sum_{s_L \in \{B,G\}} \pi\,(0, s_L, 0) + \sum_{q_D=2}^{C} \sum_{s_L \in [B,G]} \sum_{m_L=0}^{M} \pi\,(q_D - 1,\ s_L, m_L) \quad (3.24)$$

Trong công thức (3.24), $\pi\,(q_D - 1, s_L, m_L)$ được biểu diễn như trong Bảng 3.2.

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

$$\Pr\left\{t_Q > \frac{\mathcal{D}}{\tau_{bs}}\right\} = Pr\left\{t_Q > \frac{\mathcal{D}}{\tau_{bs}} |\ (q_D, s_L, m_L)\right\} Pr\{(q_D, s_L, m_L)\}$$

$$= \frac{1}{\pi_v}\left[\sum_{s_L \in \{B,G\}} Pr\left\{t_Q > \frac{\mathcal{D}}{\tau_{bs}} |\ (0, s_L, 0)\right\} \pi(0, s_L, 0) + \right.$$

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

3.3.4. Kết quả khảo sát hiệu năng hệ thống

Nhằm đánh giá tính khả thi của hệ thống CV-QKD đã đề xuất, trong phần này, các tham số hiệu năng như tỷ lệ mất khóa KLR và tỷ lệ trễ vượt ngưỡng được xem xét. Các tham số khác của hệ thống sử dụng trong các tính toán mô phỏng được cho ở trong Bảng 3.5. Các tham số liên quan đến bộ thu phát quang được tham khảo từ [3] và các tham số liên quan đến trạm vệ tinh, trạm mặt đất dựa trên những thông số trong hệ thống truyền dẫn sử dụng đường truyền FSO dựa trên vệ tinh có sử dụng chuyển tiếp [93]. KLR và tỷ lệ trễ vượt ngưỡng lần lượt được tính theo các công thức (3.10) và công thức (3.25), trong đó các xác suất kết hợp được tính theo công thức (3.12) và (3.16). Hai kịch bản nhiễu loạn được xem xét trong các kết quả nghiên cứu

bao gồm nhiễu loạn yếu $C_n^2(0) = 5\times10^{-15}$ ($m^{-2/3}$) và nhiễu loạn mạnh $C_n^2(0) = 7\times10^{-12}$ ($m^{-2/3}$).

Bảng 3. 6. Bảng các tham số dùng trong khảo sát hiệu năng hệ thống QKD-FSO có vệ tinh sử dụng kỹ thuật chuyển tiếp HAP và kỹ thuật ARQ.

Tham số	**Ký hiệu**	**Giá trị**
Các tham số chung		
Hằng số Boltzmann	k_B	$1{,}38\times10^{-23}$ W/K/Hz
Điện tích electron	q	$1{,}6\times10^{-19}$ C
Điện trở tải	R_L	50 Ω
Nhiệt độ máy thu	T	298K
Hệ số nhiễu trội của APD	x	0,8 (Điôt APD loại InGaAS)
Tốc độ bit của hệ thống	R_b	10 Gb/s
Bước sóng quang	λ	1550 nm
Vận tốc gió	v	21 m/s
Hệ số nhân thác lũ của APD	M_A	10
Dòng điện tối	I_d	3 nA
Đáp ứng của APD	$\Re$	0,8
Các tham số của lớp vật lý		
Công suất của bộ dao động nội	P_{LO}	0 dBm
Công suất phát	P_T	7 dBm
Độ khuếch đại của thấu kính phát tại vệ tinh	$G_T^{(A)}$	115 dB
Độ khuếch đại của thấu kính phát tại HAP	$G_T^{(R)}$	5 dB
Độ khuếch đại của thấu kính thu tại HAP	$G_R^{(R)}$	105 dB

Độ khuếch đại của thấu kính thu tại trạm mặt đất	$G_R^{(B)}$	5 dB
Hệ số tỷ lệ của bộ tách ngưỡng kép		
Vệ tinh tới HAP	$\rho^{(AR)}$	0,4
HAP tới trạm mặt đất (Nhiễu loạn yếu)	$\rho_W^{(RB)}$	0,7
HAP tới trạm mặt đất (Nhiễu loạn mạnh)	$\rho_S^{(RB)}$	1,4
Các tham số của lớp liên kết		
Chiều dài của một chuỗi bit	l_{bs}	5×10^7 bit
Độ trễ tối đa	$\mathcal{D}$	80 ms

Trong phần kết quả khảo sát hiệu năng, luận án sẽ so sánh hiệu năng của ba hệ thống: (1) hệ thống sử dụng cả kỹ thuật chuyển tiếp dựa trên HAP và kỹ thuật ARQ, (2) hệ thống chỉ sử dụng kỹ thuật ARQ, (3) hệ thống không sử dụng kỹ thuật ARQ và kỹ thuật chuyển tiếp dựa trên HAP. Hệ thống (3) là hệ thống thông thường và hệ thống (1), (2) là hệ thống sử dụng các kỹ thuật đã đề xuất.

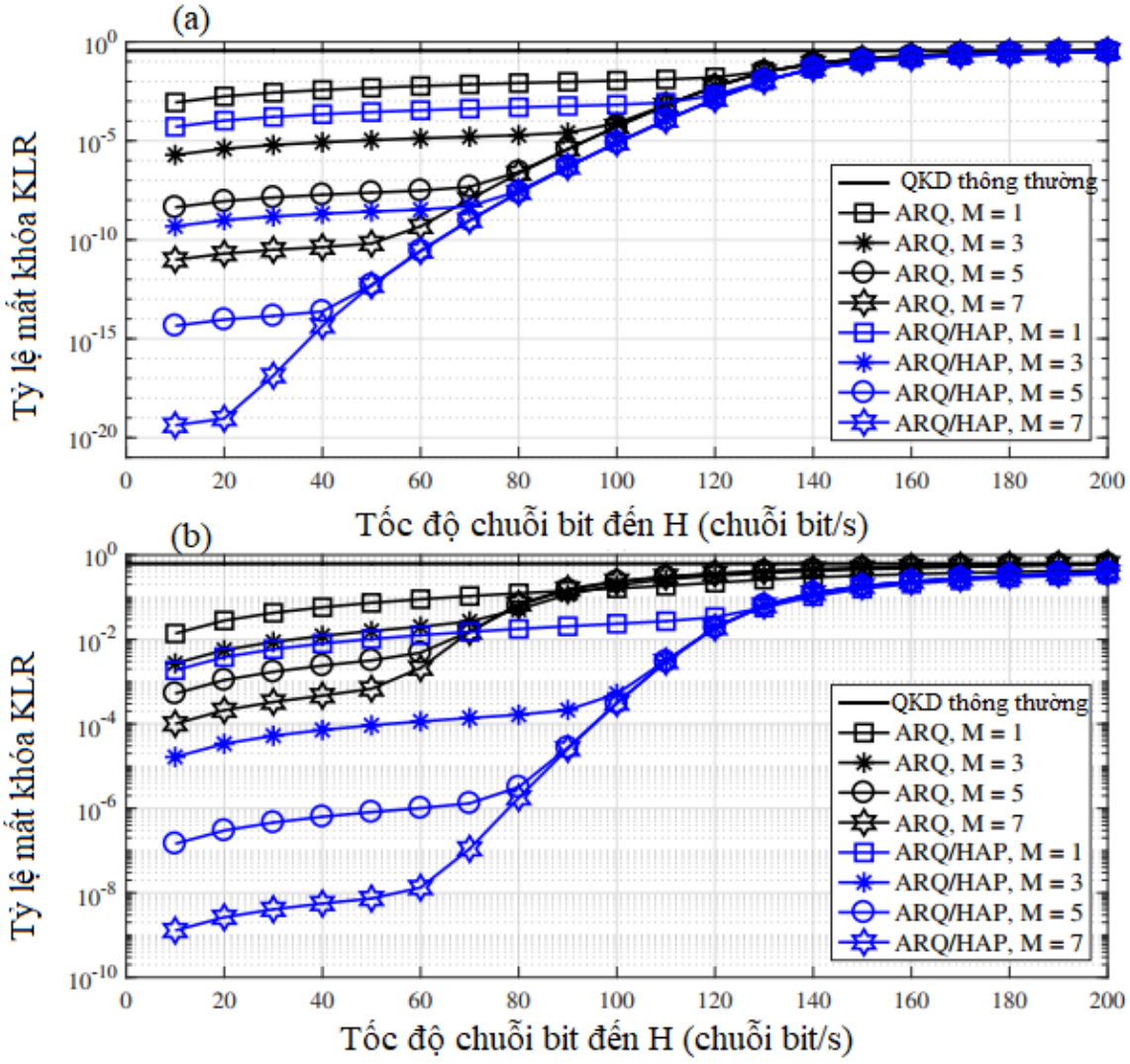
Công suất phát của hệ thống không sử dụng kỹ thuật chuyển tiếp là P_T được thiết lập bằng với công suất phát yêu cầu từ vệ tinh xuống HAP và HAP tới trạm mặt đất trong hệ thống sử dụng kỹ thuật chuyển tiếp, nghĩa là $P_T = P_T^{(AR)} + P_T^{(RB)}$.

A. Tỷ lệ mất khóa

Hình 3.12 (a) và Hình 3.12 (b) mô tả mối quan hệ của tỷ lệ mất khóa KLR với tốc độ chuỗi bit đến *H* tương ứng với điều kiện nhiễu loạn khí quyển yếu và điều kiện nhiễu loạn khí quyển mạnh. Qua kết quả khảo sát thu được, chúng ta có thể dễ dàng nhận thấy, tỷ lệ mất khóa KLR của hệ thống không sử dụng kỹ thuật chuyển tiếp và kỹ thuật ARQ là tương đối cao mặc dù độ khuếch đại của thấu kính phát phía vệ tinh và độ khuếch đại của thấu kính thu phía mặt đất có thể tăng lên tới 130 dB hoặc 135 dB tương ứng với các điều kiện nhiễu loạn của khí quyển.

Tỷ lệ mất khóa có thể cải thiện nhờ vào việc sử dụng kỹ thuật ARQ, đặc biệt khi kỹ thuật này được dùng kết hợp với kỹ thuật chuyển tiếp sử dụng hạ tầng trên cao

HAP. Ưu điểm của việc kết hợp hai kỹ thuật này được so sánh với khi hệ thống chỉ sử dụng kỹ thuật ARQ sẽ được xem xét một cách độc lập, đặc biệt khi số lần cho phép phát lại một chuỗi bit là M cao hơn.



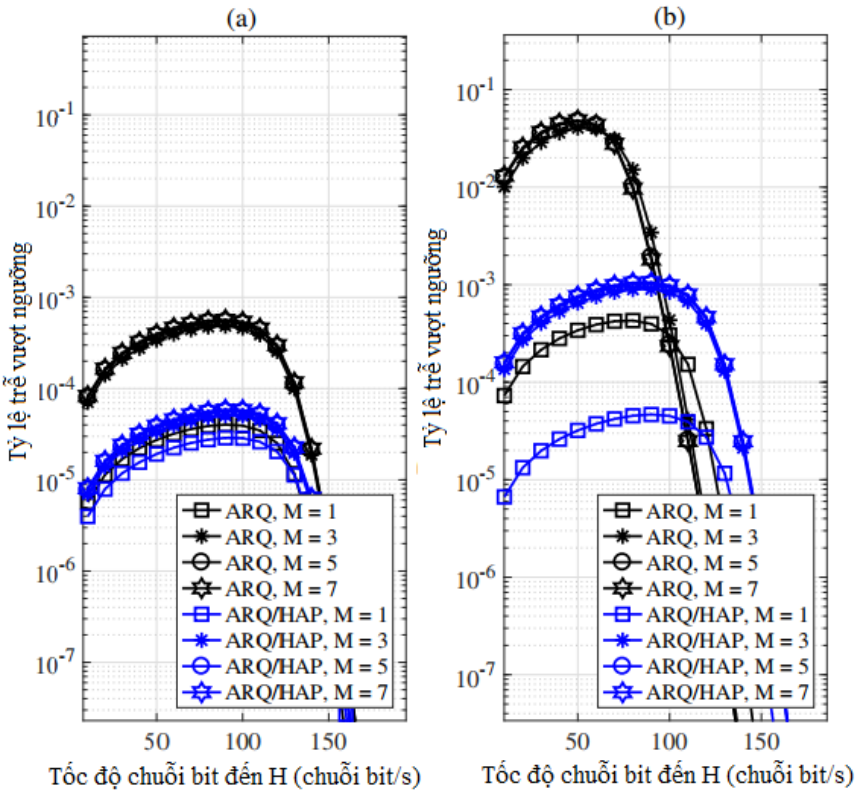
Hình 3. 12. Tỷ lệ mất khóa KLR theo tốc độ chuỗi bit đến H với điều kiện nhiễu loạn khí quyển yếu (a) và mạnh (b), kích thước bộ nhớ đệm C= 10 chuỗi bit.

Trong Hình 3.12, với giá trị của số lần chuỗi bit được phép phát lại *M*=3, tỷ lệ chuỗi bit đến lớn nhất tương ứng với tỷ lệ mất khóa KLR= 10^{-2} là 120 chuỗi bit/ giây đối với hệ thống sử dụng cả kỹ thuật ARQ và HAP và 50 chuỗi bit/giây trong trường hợp hệ thống chỉ sử dụng kỹ thuật ARQ. Tuy nhiên, 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.

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.

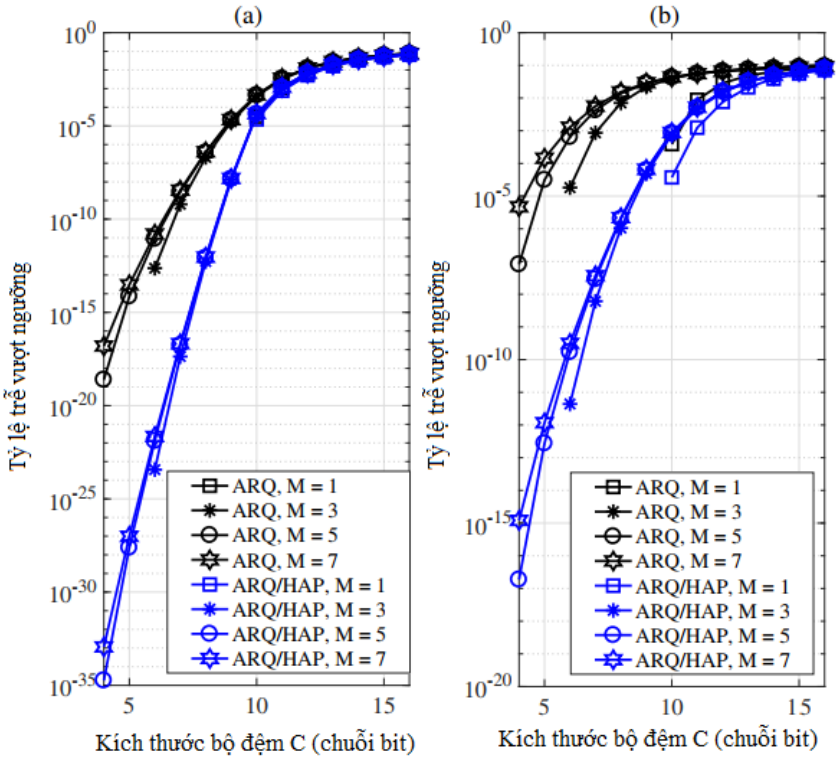


Hình 3. 13. Tỷ lệ trễ vượt ngưỡng theo tốc độ chuỗi bit đến với điều kiện nhiễu loạn khí quyển yếu (a) và mạnh (b), kích thước bộ nhớ đệm C=10 chuỗi bit.

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 quả này có được là do chuyển tiếp dựa trên hạ tầng trên cao HAP là một kỹ thuật hiệu quả trong việc giảm tỷ lệ lỗi khóa và số lần cho phép truyền lại một chuỗi bit trong kỹ thuật ARQ gây ra trễ. Việc tăng số lần cho phép truyền lại một chuỗi bit cũng làm tăng độ trễ.

Kết quả trong Hình 3.13 cũng cho thấy tỷ lệ trễ vượt ngưỡng thay đổi một cách rõ rệt khi thay đổi tỷ lệ chuỗi bit đến. Tại thời điểm ban đầu, do tỷ lệ chuỗi bit đến cao dẫn đến độ trễ hàng đợi cao nên tỷ lệ chuỗi vượt ngưỡng tăng với tỷ lệ chuỗi bit đến. Độ trễ giảm khi tỷ lệ chuỗi bit đến đạt tới một giá trị xác định. Tuy nhiên, trong trường hợp này, các chuỗi bit bị hủy bởi vì bộ nhớ đệm bị tràn, do đó tỷ lệ các chuỗi bit nhận được thành công bị giảm đi.



Hình 3. 14. Tỷ lệ trễ vượt ngưỡng với kích thước bộ nhớ đệm trong điều kiện nhiễu loạn khí quyển yếu (a) và mạnh (b), tốc độ chuỗi bit đến H= 60 chuỗi/giây.

Hình 3.14 mô tả mối quan hệ giữa tỷ lệ trễ vượt ngưỡng với kích cỡ của bộ nhớ đệm trong các điều kiện nhiễu loạn khí quyển. Chúng ta có thể nhận thấy một cách rõ ràng, khi kích thước bộ nhớ đệm tăng lên sẽ giảm tỷ lệ mất khóa KLR. Để

đảm bảo tỷ lệ trễ vượt ngưỡng ở dưới một ngưỡng xác định cần thiết phải xác định kích cỡ tối đa của bộ nhớ đệm. Trong trường hợp hệ thống sử dụng cả kỹ thuật ARQ và chuyển tiếp dựa trên hạ tầng trên cao HAP, hoạt động trong điều kiện nhiễu loạn khí quyển mạnh, kích cỡ lớn nhất của bộ nhớ đệm là 10 chuỗi với tỷ lệ trễ vượt ngưỡng là 10^{-3}. Giá trị này tương đương với các giá trị khác nhau của *M*, với *M* là số lần tối đa một chuỗi bit được phát lại. Giá trị của tỷ lệ trễ vượt ngưỡng là nhỏ trong điều kiện nhiễu loạn khí quyển yếu, trong khi các giá trị *M* khác nhau nhiều trong điều kiện nhiễu loạn khí quyển. Nguyên nhân là do điều kiện nhiễu loạn khí quyển mạnh dẫn tới tỷ lệ mất khóa KLR cao nên số lần được phép truyền lại một chuỗi bit có ảnh hưởng hơn tới tỷ lệ mất khóa. Với cùng một kích thước bộ nhớ đệm, tỷ lệ trễ vượt ngưỡng nhỏ hơn trong trường hợp nhiễu loạn khí quyển yếu.

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.

Kịch bản thứ nhất, hệ thống QKD-FSO chỉ sử dụng kỹ thuật ARQ tại phía phát. Hiệu năng của hệ thống được cải thiện một cách đáng kể, đặc biệt trong các điều kiện nhiễu loạn khí quyển mạnh. Hệ thống QKD sử dụng QPSK-DT/HD được đề xuất đạt QBER thấp hơn nhiều so với hệ thống SIM/BPSK-DT [85]. Với cùng QBER, hệ thống đề xuất trong luận án yêu cầu công suất phát thấp hơn 20 dB. Hệ thống QKD sử dụng ARQ có tỷ lệ mất khóa (truyền không thành công) là 10^{-6} thấp hơn rất nhiều so với tỷ lệ mất khóa là 10^{-1} của hệ thống không sử dụng ARQ, xét trong cùng một điều kiện công suất phát. Tuy nhiên, nhược điểm của kỹ thuật ARQ là làm tăng độ trễ, đặc biệt khi truyền lại khóa từ vệ tinh.

Kịch bản thứ hai, hệ thống QKD-FSO sử dụng cả kỹ thuật chuyển tiếp hạ tầng trên cao và kỹ thuật ARQ tại trạm chuyển tiếp. Với giải pháp truyền lại khóa từ trạm

chuyển tiếp, trễ truyền dẫn sẽ giảm, đồng thời hiệu năng hệ thống được cải thiện. Tính khả thi của hệ thống đề xuất được chứng minh qua kết quả tỷ lệ mất khóa KLR nhỏ (giảm tới 10^{-9} trong điều kiện nhiễu loạn khí quyển mạnh và 10^{-20} trong điều kiện nhiễu loạn khí quyển yếu) và tỷ lệ trễ vượt ngưỡng giảm nhỏ. Để đạt được tỷ lệ trễ vượt ngưỡng đáp ứng yêu cầu đặt ra thì cần phải xác định tỷ lệ chuỗi bit đến cũng như kích thước bộ nhớ đệm tương ứng.

Giải pháp đề xuất ở Chương 3 có thể ứng dụng trong trường hợp các hệ thống QKD-FSO đơn kênh dựa trên vệ tinh nhằm phục vụ cho mạng QKD-FSO toàn cầu trong tương lai. Đối với các hệ thống QKD-FSO đa kênh, giải pháp đề xuất cải thiện hiệu năng sẽ được trình bày ở nội dung của Chương 4 của luận án.

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

Tóm tắt

Nội dung của Chương 4 đề xuất 02 giải pháp hệ thống QKD-FSO đa kênh đa người sử dụng dựa trên vệ tinh. Giải pháp thứ nhất sử dụng kỹ thuật ghép kênh phân chia theo bước sóng WDM và ghép kênh theo sóng mang phụ SCM nhằm tăng tốc độ khóa bí mật SKR của hệ thống QKD-FSO đa kênh dựa trên vệ tinh. Giải pháp thứ hai cho hệ thống QKD-FSO hỗ trợ đa người dùng sử dụng kỹ thuật CDMA quang. Việc xây dựng mô hình giải tích, xác suất và khảo sát hiệu năng của hệ thống đề xuất cũng được trình bày chi tiết trong nội dung của chương. Tham số hiệu năng tỷ lệ lỗi bit lượng tử QBER, xác suất chọn lọc P_{sift}, tốc độ khóa bí mật SKR được khảo sát với các thông số khác nhau của hệ thống như hệ số tỷ lệ ngưỡng kép, tốc độ bit và tổng số lượng kênh sóng mang phụ, điều kiện nhiễu loạn khí quyển trung bình và nhiễu loạn mạnh. Đồng thời, ảnh hưởng của các loại tạp âm máy thu và nhiễu xuyên kênh cũng được tính đến trong trong mô hình phân tích hiệu năng.

Kết quả nghiên cứu của Chương 4 đã được công bố trong 01 bài báo đăng trên tạp chí Nghiên cứu Khoa học và Công nghệ quân sự [J2] và 01 bài báo quốc tế [J4].

4.1. Mở đầu

Việc nghiên cứu các hệ thống QKD đã được triển khai với việc sử dụng đường truyền bằng cáp quang hoặc không gian tự do. Kênh truyền không gian tự do có ưu điểm cung cấp một lớp vật lý linh hoạt hơn cho các ứng dụng khác nhau, đặc biệt trong việc kết nối giữa hai người dùng đầu cuối chuyển động [13]. Tuy nhiên, phân phối khóa lượng tử QKD qua kênh không gian tự do bị ảnh hưởng bởi các hiện tượng hấp thụ, tán xạ, nhiễu loạn khí quyển. Các hiện tượng này đã làm giảm tốc độ truyền khóa SKR của một hệ thống QKD. Do đó, để đạt được tốc độ truyền khóa lớn trong một khoảng đường truyền dài ở chế độ đơn kênh thực sự là thách thức lớn đối với hệ thống QKD kiểu đơn kênh [80]. Theo lý thuyết, tốc độ truyền khóa có thể cải thiện

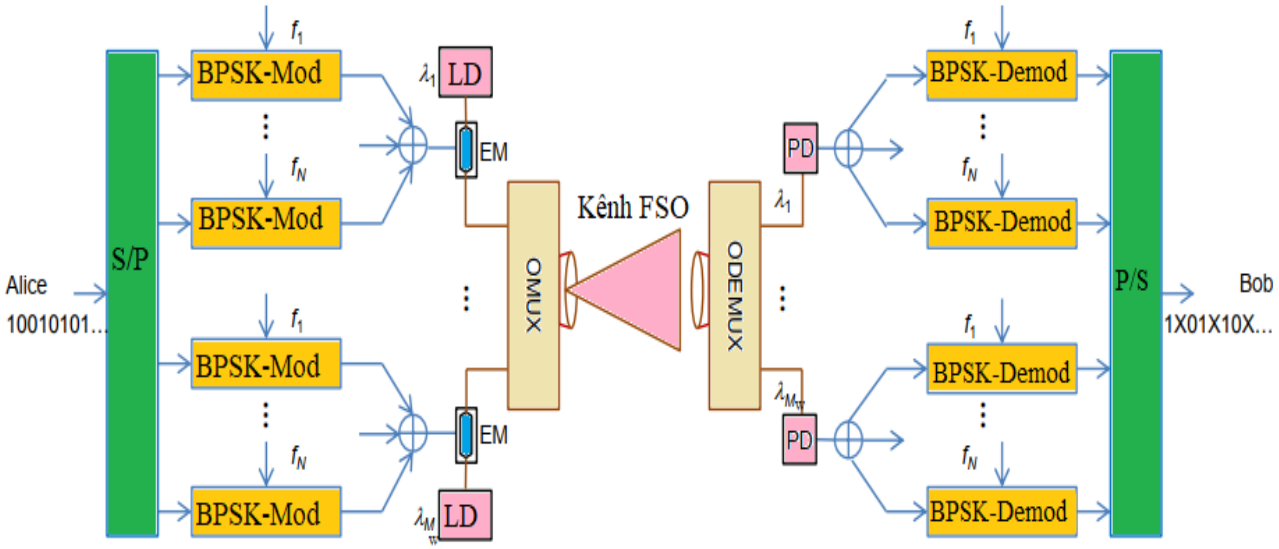
bằng cách tăng tốc độ truyền chuỗi bit ngẫu nhiên phát đi. Tuy nhiên, sự suy yếu của đường truyền vật lý sẽ có ảnh hưởng nhiều hơn tới hệ thống QKD với tốc độ truyền bit lớn, kéo theo tỷ lệ lỗi bit lượng tử QBER sẽ cao hơn. Giải pháp tăng SKR bằng cách sử dụng tốc độ truyền cao hơn cũng yêu cầu bộ tách sóng có băng thông rộng và tốc độ xử lý dữ liệu cao hơn. Một giải pháp để tăng tốc độ khóa là sử dụng kỹ thuật ghép kênh. Kỹ thuật ghép kênh cho phép phân phối các khóa bí mật độc lập thông qua một đường truyền vật lý. Việc sử dụng kỹ thuật ghép kênh không chỉ tăng tốc độ khóa mà còn hỗ trợ cho việc phân phối khóa tới đa người dùng. Giải pháp sử dụng các phương pháp ghép kênh là một giải pháp đang thu hút được nhiều sự quan tâm, nghiên cứu [25].

Một số nghiên cứu cải thiện tốc độ khóa bí mật SKR bằng phương pháp ghép kênh đã được tiến hành [25, 105]. Các nghiên cứu này, về cơ bản, đã giúp cải thiện tốc độ truyền khóa của hệ thống QKD. Tuy nhiên, nhằm đạt được sự cải thiện vượt trội về tốc độ truyền khóa bí mật của các hệ thống QKD, luận án đề xuất hệ thống CV-QKD đa kênh từ vệ tinh sử dụng kết hợp hai kỹ thuật ghép kênh SCM và WDM (SCM-WDM). Trong đó, chuỗi bit khóa trước tiên được phân thành nhiều luồng song song để điều chế lên các sóng mang phụ. Tiếp theo, mỗi nhóm N sóng mang phụ sẽ được kết hợp lại để điều chế một nguồn quang laser ở một bước sóng xác định. Với số lượng bước sóng là M_w, trong điều kiện không có xuyên nhiễu giữa các kênh, tốc độ truyền khóa có thể tăng tối đa $N \times M_w$ lần. Nhằm đánh giá tính khả thi của hệ thống đề xuất, luận án sử dụng phương pháp phân tích lý thuyết với các công cụ giải tích và xác suất nhằm xây dựng các công thức tính toán tốc độ khóa bí mật SKR và tỷ lệ lỗi bit lượng tử QBER của hệ thống. Các thông số này được đánh giá trong điều kiện hệ thống chịu tác động của nhiễu loạn khí quyển.

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

Mô hình hệ thống QKD-FSO đa kênh sử dụng kỹ thuật SCM-WDM từ vệ tinh tới trạm mặt đất được minh họa như trong Hình 4.1. Hệ thống trong Hình 4.1 được luận án đề xuất với mục đích tăng tốc độ khóa sử dụng kỹ thuật ghép kênh, hỗ trợ phân phối khóa tới đa người dùng bằng cách sử dụng kết hợp kỹ thuật ghép kênh SCM và WDM.



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

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. Khóa thô là chuỗi bit ngẫu nhiên được tạo ra tại vệ tinh sẽ được phân thành $N \times M_w$ luồng song song nhờ bộ chuyển đổi nối tiếp/song song (S/P), mỗi luồng sẽ được mã hóa biến liên tục vào một sóng mang phụ (f_i, $1 \le i \le N$) nhờ bộ điều chế khóa dịch pha nhị phân (BPSK-Mod), tiếp theo mỗi nhóm N sóng mang phụ sẽ được kết hợp lại và điều chế vào một trong số M_w bước sóng (λ_j, $1 \le j \le M_w$) được tạo ra bởi nguồn laser LD thông qua bộ điều chế ngoài (EM). M_w bước sóng được ghép lại nhờ bộ ghép kênh quang OMUX. Tín hiệu quang đầu ra bộ OMUX được đưa tới thấu kính phát và truyền qua kênh FSO tới trạm mặt đất. Tại trạm mặt đất, tín hiệu quang thu được bởi thấu kính thu trước tiên được đưa qua bộ tách kênh theo bước sóng quang (Optical Demultiplexing – ODEMUX) để tách ra M_w kênh bước sóng riêng biệt. Mỗi kênh bước sóng được

chuyển đổi thành tín hiệu điện nhờ một đi-ôt tách quang PD trước khi đưa qua N bộ giải điều chế khóa dịch pha nhị phân BPSK để tách ra N chuỗi bit chọn lọc. $N \times M_w$ chuỗi bit chọn lọc được kết hợp lại nhờ bộ chuyển đổi song song/nối tiếp P/S để khôi phục khóa chọn lọc đã được Alice và Bob thống nhất sử dụng trong quá trình mã hóa và khóa chọn lọc này sẽ được dùng cho việc giải mã dữ liệu ở bên máy thu.

4.2.2. Giao thức CV-QKD sử dụng

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. Giao thức CV-QKD này đã được đề xuất và khảo sát cho kịch bản hệ thống QKD đơn kênh FSO mặt đất [85]. Trong Hình 4.1, mã hóa lượng tử biến liên tục được thực hiện tại khối điều chế BPSK, phần giải mã và tách ngưỡng kép được thực hiện tại khối tách sóng BPSK.

Trước tiên, tại vệ tinh (Alice), một chuỗi nhị phân ngẫu nhiên $d(t)$ được tạo ra, chuyển sang định dạng xung và sau đó được điều chế bởi kỹ thuật BPSK. Trong phương pháp điều chế BPSK hệ thống sử dụng, một sóng mang phụ có hai pha khác biệt nhau 180^0 được sử dụng để biểu thị các bit "0" và "1". Công thức biểu diễn tín hiệu BPSK tại kênh sóng mang phụ thứ i như sau:

$$S_i(t) = A(t)\, g(t) \cos\left(2\pi f_i t + a_k \pi\right) \tag{4.1}$$

trong đó, $A(t)$ là biên độ sóng mang, $g(t)$ là hàm định dạng xung hình chữ nhật, f_i là tần số sóng mang và $a_k \in \{0, 1\}$ là bit nhị phân thứ k. Để đơn giản hóa việc phân tích, công suất $S(t)$ được giả định là một. Sau đó, cả giá trị dương và âm của tín hiệu BPSK được cộng thêm dòng thiên áp một chiều DC. Lý do là đi-ốt laser LD được sử dụng để tạo ra sóng quang liên tục chỉ có thể được điều chế bởi các tín hiệu dương. Sau điều chế quang, công suất phát của búp sóng laser được biểu diễn như sau:

$$P_S(t) = \frac{P_p}{2}\left[1 + \mu \sum_{i=1}^{N} S_i(t)\right] \tag{4.2}$$

Trong công thức (4.2), P_p là công suất phát đỉnh, μ là độ sâu điều chế cường độ (0

$< \mu <$ 1). Sau đó, tín hiệu được ghép theo bước sóng, khuếch đại bởi thấu kính phát với hệ số khuếch đại G_{Tx} và được truyền qua kênh truyền FSO.

Tại máy thu của trạm mặt đất (Bob), một đi-ốt quang thác APD được sử dụng để chuyển đổi tín hiệu quang thành tín hiệu điện. Dòng tách quang cho mỗi kênh sóng mang phụ có thể được biểu diễn như sau:

$$i_p(t) = \Re M_A h_t \frac{P_R}{2}\left[1+\gamma S_i(t)\right] + i_n(t) \tag{4.3}$$

Trong công thức (4.3), $\Re$ là đáp ứng và M_A là hệ số nhân thác lũ của APD; h_t là hệ số kênh đặc trưng cho kênh FSO; $i_n(t)$ là dòng điện tạp âm máy thu và P_R là công suất thu cực đại tại trạm mặt đất.

Sau khi giải điều chế BPSK, tín hiệu từ các thành phần tần số cao bị loại bỏ bằng cách sử dụng bộ lọc thông thấp LPF. Đầu ra của LPF là tín hiệu băng tần cơ sở mong muốn như sau [85]:

$$\begin{cases} i_0 = -\dfrac{1}{4}\Re M_A \mu h_t P_R + i_n(t) \\ i_1 = +\dfrac{1}{4}\Re M_A \mu h_t P_R + i_n(t) \end{cases} \tag{4.4}$$

với i_0 và i_1 lần lượt là dòng điện thu được tương ứng với khi phát bit "0" và bit "1". Tổng phương sai tạp âm bao gồm tạp âm lượng tử, tạp âm nhiệt và nhiễu xuyên kênh được biểu diễn như sau:

$$\begin{aligned} \sigma_n^2 &= 2qM_A^2 F_A \Re\left(P_R + P_b\right) B_e \\ &\quad + \frac{4k_B T}{R_L} F_n B_e + 2(NM_{\mathrm{w}} - 1) B_e \tau_c \Re^2 C_X P_R^2 \end{aligned} \tag{4.5}$$

Trong công thức (4.5), q là điện tích của electron; $B_e = R_b/2$ là băng thông nhiễu hiệu dụng; R_b là tốc độ bit; k_B là hằng số Boltzmann; T là nhiệt độ của máy thu; R_L là điện trở tải; $F_A = k_A M_A + (2 - 1/M_A)(1 - k_A)$ với k_A là hệ số ion hóa của APD [3]; $\tau_c = 1/B_o$ với B_o là độ rộng băng thông quang; C_X là tỉ số công suất xuyên kênh; $\Re$ là đáp ứng của APD; M_A là hệ số nhân thác lũ của APD; F_n là hệ số tạp âm. Nhiễu xuyên kênh gây ra bởi sự giao thoa giữa (N - 1) kênh sóng mang phụ còn lại trong hệ thống

lên kênh sóng mang phụ đang xét. Trong công thức (4.5), nhiễu xuyên kênh được xét trong trường hợp xấu nhất, có ảnh hưởng mạnh nhất, pha của tín hiệu từ các kênh khác trùng với pha của tín hiệu kênh sóng mang phụ đang xét.

Tín hiệu sau khi giải điều chế được đưa qua một bộ tách ngưỡng kép DT gồm hai mức ngưỡng d_0 và d_1. Bộ tách ngưỡng kép sẽ so sánh giá trị của tín hiệu điện thu được với các mức ngưỡng, từ đó sẽ quyết định giá trị bit tương ứng ở đầu ra. Có ba trường hợp xảy ra đối với tín hiệu điện đưa vào bộ tách ngưỡng kép, bao gồm: nhỏ hơn d_0, lớn hơn d_1 và nằm giữa hai ngưỡng d_0 và d_1. Nhờ sử dụng ngưỡng kép, máy thu có thể quyết định tương ứng các bit nhận được là "0", "1" hoặc "X". Sự xuất hiện của "X" trong chuỗi bit khôi phục thể hiện một số bit khi chuyển từ Alice tới Bob không được khôi phục thành công. Đây chính là tính chất đặc trưng cho kênh lượng tử. Sau khi kết thúc quá trình khôi phục bit, Bob thông báo cho Alice biết vị trí chính xác của các bit trong chuỗi được khôi phục thành công, bit "0" hoặc "1", qua kênh công khai. Dựa trên thông báo của Bob, Alice chỉ tạo khóa chọn lọc dựa trên các bit ở các vị trí được khôi phục thành công.

4.2.3. Phân tích hiệu năng hệ thống

Tỷ lệ lỗi bit lượng tử QBER được định nghĩa như công thức (1.1). Với hệ thống CV-QKD xem xét trong nghiên cứu này, P_{sift} tương ứng với xác suất mà Bob có thể tách các bit "0" và "1" nhờ sử dụng bộ tách ngưỡng kép, P_{error} là xác suất mà Bob quyết định sai là "0" khi bit "1" được phát và ngược lại. Các xác suất này được tính thông qua các xác suất hợp giữa Alice và Bob theo công thức (1.2) và (1.3)

Xét đến ảnh hưởng của pha-đinh do nhiễu loạn khí quyển, xác suất kết hợp giữa A và B được tính như sau:

$$\begin{aligned} P_{A,B}(a,0) &= \frac{1}{2}\int_0^{\infty} Q\left(\frac{I_a - d_0}{\sigma_n}\right) f_{h_f}(h_f)\,dh_f \\ P_{A,B}(a,1) &= \frac{1}{2}\int_0^{\infty} Q\left(\frac{d_0 - I_a}{\sigma_n}\right) f_{h_f}(h_f)\,dh_f \end{aligned}, \qquad (4.6)$$

trong đó $Q(.)$ là hàm Q dạng Gauss và I_a là ký hiệu dòng điện tín hiệu thu cho bit "a" được xác định như sau:

$$\begin{aligned} I_0 &= -\Re M_A \mu h_t P_R \\ I_1 &= +\Re M_A \mu h_t P_R \end{aligned}. \tag{4.7}$$

Để xác định các giá trị ngưỡng d_0 và d_1, luận án đề xuất thiết lập giá trị cho các ngưỡng này như sau:

$$\begin{aligned} d_0 &= E\left[i_0\right] + \rho\sigma_n \\ d_1 &= E\left[i_1\right] - \rho\sigma_n \end{aligned}, \tag{4.8}$$

Trong đó ρ là hệ số tỷ lệ ngưỡng kép và E[.] là hàm giá trị trung bình. Vì $E[h_t]$ = 1 nên giá trị trung bình của I_a có thể biểu diễn như sau[85]:

$$\begin{aligned} E\left[i_0\right] &= -\Re M_A \mu P_R \\ E\left[i_1\right] &= +\Re M_A \mu P_R \end{aligned} \tag{4.9}$$

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

$$SKR = R_b P_{sift} N_C \tag{4.10}$$

Trong đó R_b là tốc độ bit đường truyền, P_{sift} là xác suất chọn lọc, $N_C = N \times M_w$ là tổng số lượng kênh sóng mang phụ trong hệ thống.

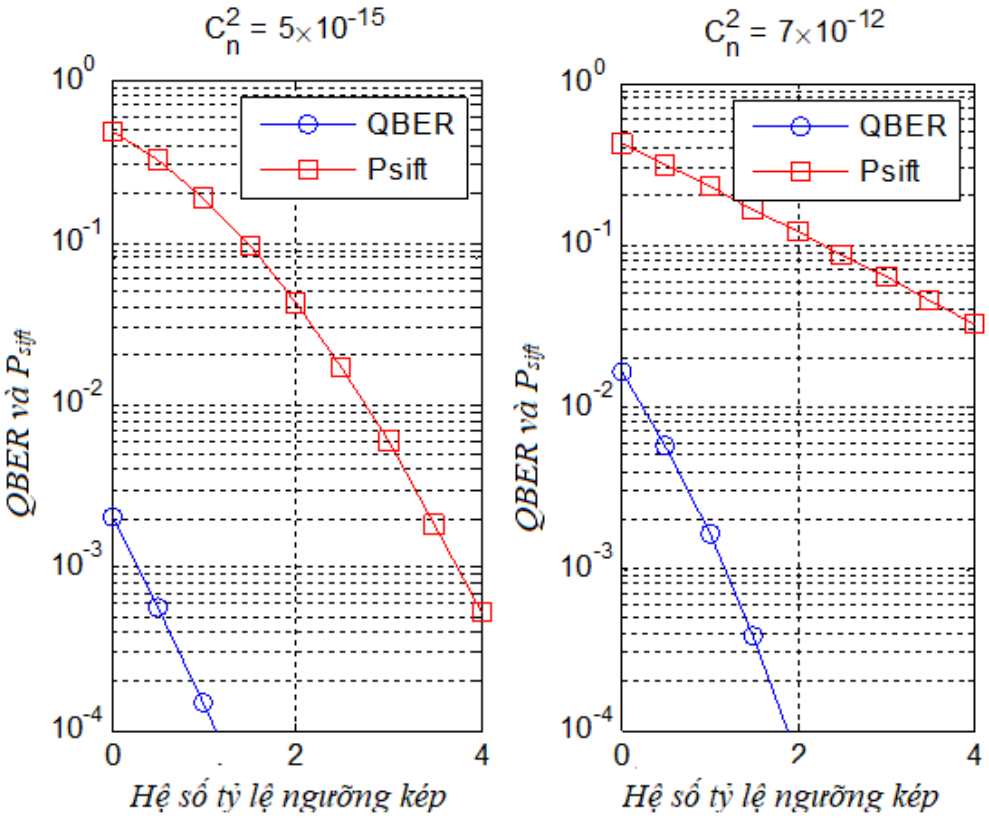
4.2.4. Kết quả khảo sát hiệu năng hệ thống

Nhằm đánh giá tính khả thi của hệ thống CV-QKD đa kênh đã đề xuất, trong phần này, các tham số hiệu năng QBER, P_{sift} và tốc độ khóa bí mật KLR được khảo sát theo các tham số hệ thống như hệ số tỷ lệ ngưỡng kép, tốc độ bit và tổng số lượng kênh sóng mang phụ. QBER, P_{sift}, KLR được tính theo công thức (1.1), (1.2), (1.3), (4.10), trong đó các xác suất kết hợp được tính theo công thức (4.8). Các tham số khác của hệ thống sử dụng trong các tính toán được cho ở trong Bảng 4.1. Các tham

số liên quan đến bộ thu phát quang được tham khảo từ [3] và các tham số liên quan đến trạm vệ tinh, trạm mặt đất dựa trên những thông số trong hệ thống truyền dẫn sử dụng đường truyền FSO dựa trên vệ tinh [82] . Hai kịch bản nhiễu loạn được xem xét trong các kết quả nghiên cứu bao gồm nhiễu loạn yếu $C_n^2(0) = 5\times10^{-15}$ ($m^{-2/3}$) và nhiễu loạn mạnh $C_n^2(0) = 7\times10^{-12}$ ($m^{-2/3}$).

Bảng 4. 1. Bảng các tham số dùng trong khảo sát hiệu năng hệ thống QKD-FSO có vệ tinh sử dụng kỹ thuật SCM-WDM.

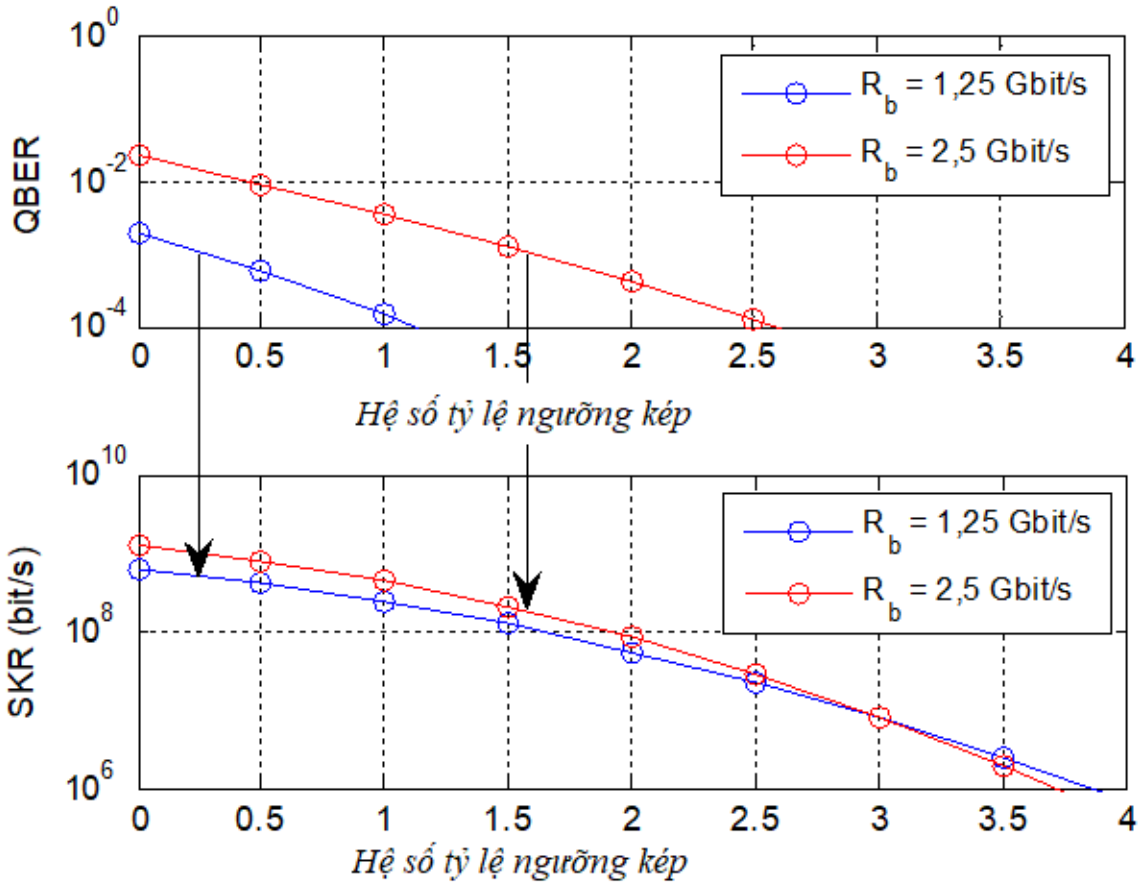
Tên	**Ký hiệu**	**Giá trị**
Điện trở tải	R_L	50 Ω
Nhiệt độ máy thu	T	298 K
Hệ số ion hóa	k_A	0,7 (InGaAs APD)
Bước sóng trung tâm	λ	1550 nm
Vận tốc gió	v	21 m/s
Đáp ứng APD	$\Re$	0,8
Hệ số nhân thác lũ của APD	M_A	15
Công suất ánh sáng nền	P_b	-40 dBm
Hệ số tạp âm	F_n	2
Công suất thu	P_R	- 30 dBm
Tỉ số công suất xuyên kênh	C_X	-20 dB
Độ cao vệ tinh	H_S	600 km
Độ cao trạm mặt đất	H_G	20 m



Hình 4. 2. QBER và P_{sift} theo hệ số tỷ lệ ngưỡng kép với R_b = 1,25 Gbit/s và N_C = 4

Hình 4.2 khảo sát QBER và P_{sift} theo hệ số tỷ lệ ngưỡng kép trong hai điều kiện nhiễu loạn. Kết quả cho thấy trong cả hai trường hợp, hệ thống đề xuất trong nghiên cứu này đều có thể đảm bảo tỷ lệ lỗi bit lượng tử yêu cầu dưới 10^{-3} thông qua việc lựa chọn hệ số tỷ lệ ngưỡng kép phù hợp. Ngưỡng QBER $\leq 10^{-3}$ được lựa chọn để đảm bảo chuỗi bit khóa chọn lọc không bị lỗi khi các kỹ thuật mã hóa sửa lỗi được sử dụng. Kết quả mô phỏng ở Hình 4.2 cũng thể hiện QBER và P_{sift} giảm khi hệ số tỷ lệ của bộ tách ngưỡng kép tăng.

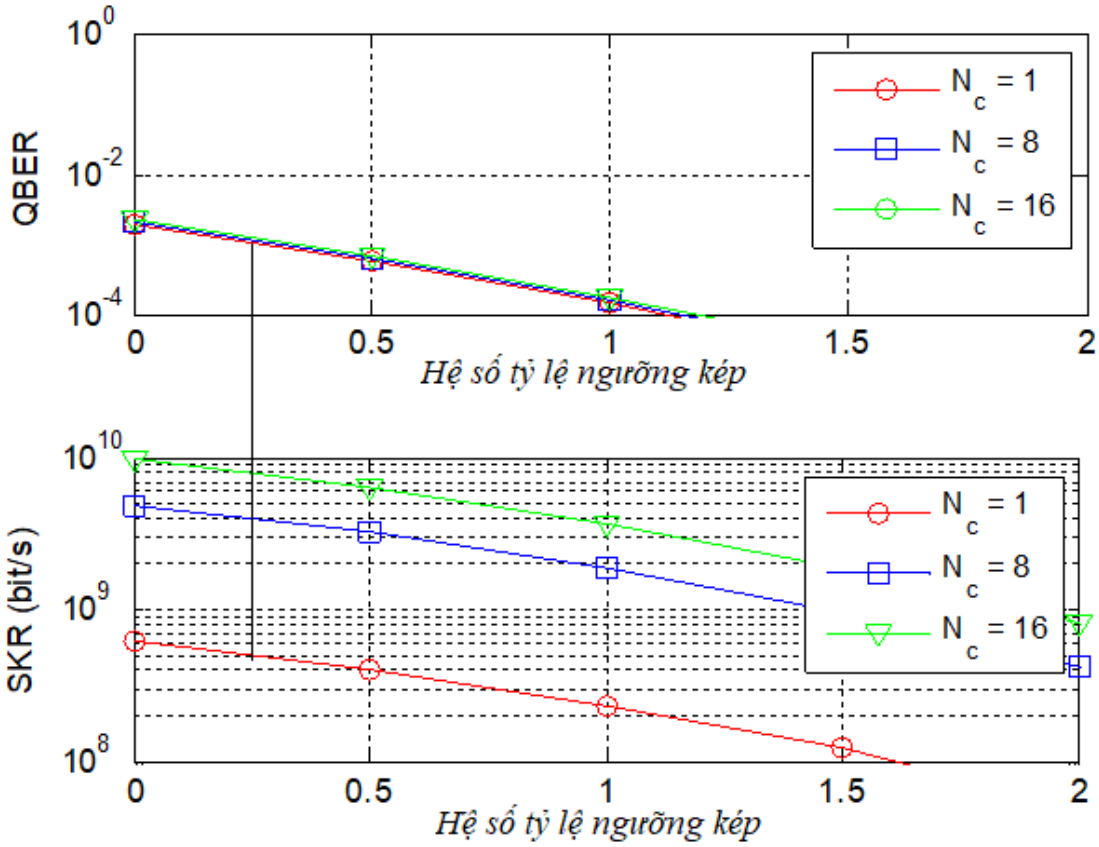
Trong khi việc giảm QBER đem lại hiệu năng tốt hơn thì việc giảm P_{sift} sẽ dẫn đến giảm độ dài khóa chọn lọc và tốc độ khóa. Hình 4.2 cũng cho thấy, tỉ số ngưỡng kép tại QBER = 10^{-3} sẽ tương ứng với P_{sift} đạt 40% với trường hợp nhiễu loạn yếu và 10% trong với hợp nhiễu loạn mạnh.



Hình 4. 3. QBER và SKR theo hệ số tỷ lệ ngưỡng kép trong trường hợp nhiễu loạn khí quyển yếu với N_C = 1

Trong Hình 4.3, QBER và tốc độ truyền khóa được khảo sát theo hệ số tỷ lệ của bộ tách ngưỡng kép trong điều kiện nhiễu loạn trung bình và xét trong trường hợp truyền dẫn đơn kênh. Giải pháp tăng tốc độ khóa bí mật thông qua việc tăng tốc độ bit truyền dẫn trên mỗi kênh cũng được khảo sát trong kết quả này. Xét trường hợp R_b = 1,25 Gbit/s, hệ số tỷ lệ của bộ tách ngưỡng kép có giá trị tối thiểu là 0,25 nhằm đạt được QBER ≤ 10^{-3}. Tốc độ khóa cực đại ứng với QBER = 10^{-3} là 500 Mbit/s. Khi hệ số tỷ lệ của bộ tách ngưỡng kép tăng, QBER giảm, tuy nhiên tốc độ khóa cũng giảm tương ứng do P_{sift} giảm. Cụ thể, tại QBER = 10^{-4}, tốc độ khóa lượng tử giảm xuống còn 200 Mbit/s. Khi tốc độ bit tăng, QBER tăng do băng thông máy thu được mở rộng dẫn đến công suất tạp âm tăng. Tương ứng với R_b = 2,5 Gbit/s, tốc độ khóa cực đại là 200 Mbit/s tại QBER = 10^{-3}. Như vậy, việc tăng tốc độ bit truyền dẫn từ

1,25 Gbit/s lên 2,5 Gbit/s khiến cho SKR cực đại giảm từ 500 Mbit/s xuống 200 Mbit/s, không giúp cải thiện SKR của hệ thống. Giải pháp truyền dẫn đa kênh SCM-WDM sẽ giúp giải quyết vấn đề này.



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. Trong kết quả này, tốc độ bit được cố định tại R_b = 1,25 Gbit/s và tổng số lượng kênh sóng mang phụ được tăng dần, N_C = 1 (đơn kênh), 8 và 16. Mặc dù số lượng kênh tăng làm tăng ảnh hưởng của nhiễu xuyên kênh nhưng không làm tăng đáng kể QBER. 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

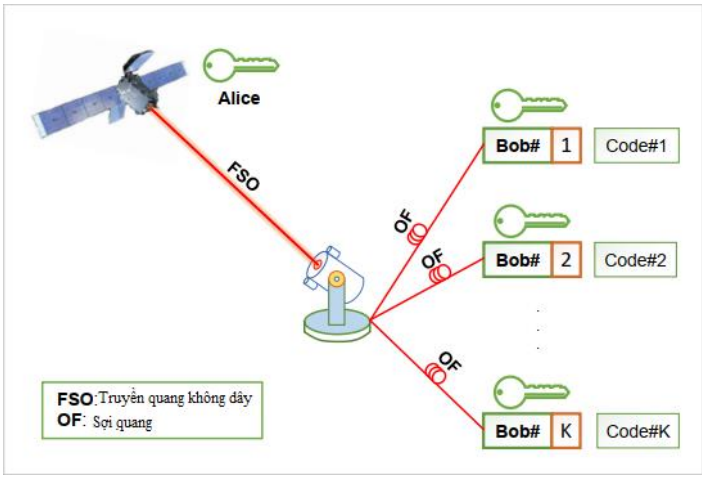
đảm bảo tính bảo mật cao của thông tin được trao đổi qua mạng.

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

Động lực cho giải pháp sử dụng kỹ thuật đa truy nhập phân chia theo mã của luận án là ưu điểm của kỹ thuật ghép kênh phân chia theo mã CDM. Trong giải pháp này, hệ thống QKD dùng vệ tinh sẽ sử dụng kỹ thuật CDM, kỹ thuật này không chỉ hỗ trợ đa người dùng mà còn tăng tính bảo mật cho hệ thống. Trong đề xuất hệ thống CV-QKD đa người dùng với kỹ thuật CDMA, kỹ thuật điều chế cường độ sẽ được sử dụng ở phía phát và máy thu tách sóng trực tiếp sử dụng cơ chế tách ngưỡng kép được sử dụng ở bên thu. Cấu trúc của hệ thống trong giải pháp này là đơn giản.

4.3.1. Mô hình hệ thống đề xuất

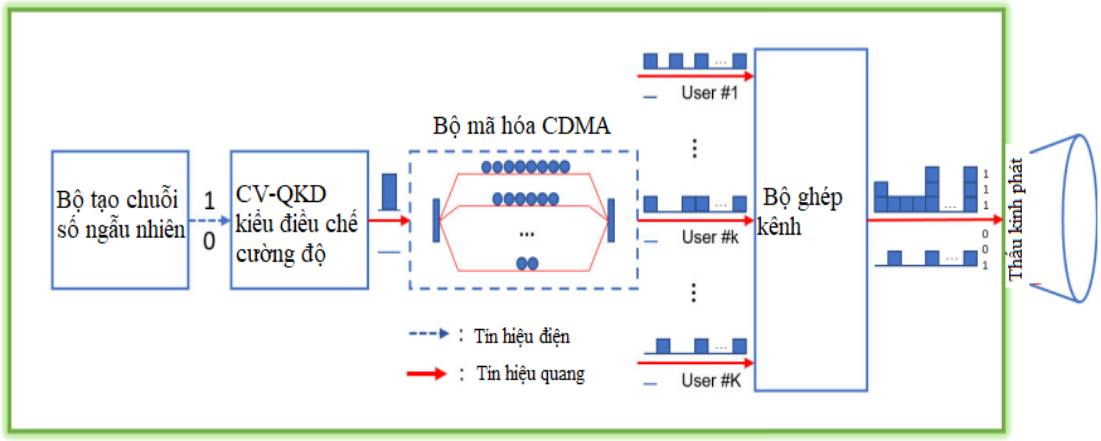
Hình 4.5 là mô hình của hệ thống CV-QKD luận án đề xuất dựa trên vệ tinh sử dụng kỹ thuật phân chia theo mã CDM. Kỹ thuật CDM không chỉ hỗ trợ đa người dùng mà còn tăng tính bảo mật cho hệ thống. Hình 4.6 (a) và (b) mô tả chi tiết sơ đồ khối của máy thu và máy phát trong mô hình hệ thống đã đề xuất ở Hình 4.5.



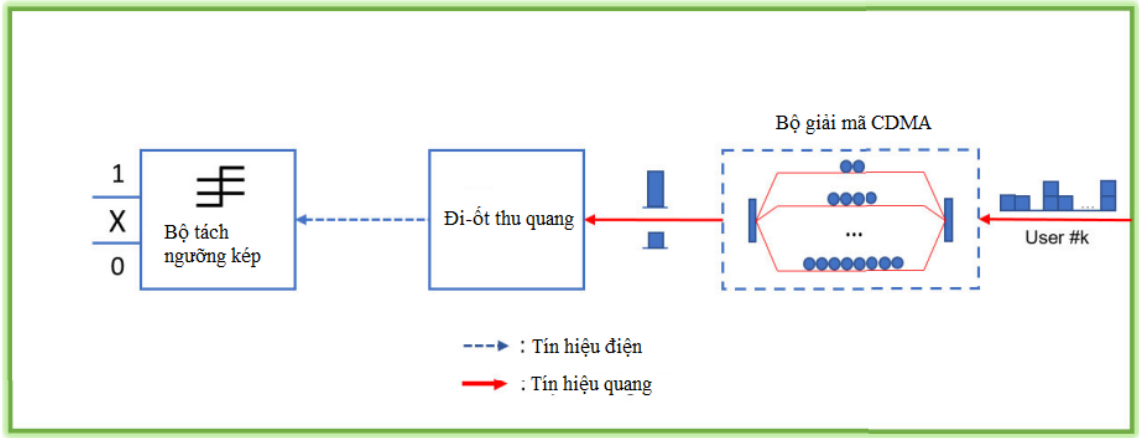
Hình 4. 5. Mô hình hệ thống CV-QKD dựa trên vệ tinh sử dụng kỹ thuật phân chia theo mã

Máy phát Alice nằm trên vệ tinh thực hiện truyền khóa với một trạm mặt đất thông qua kênh truyền quang không dây. 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. Trạm

mặt đất sẽ chuyển các khóa tới đa người dùng (Các máy thu Bob trong Hình vẽ 4.5) ở cự ly gần thông qua các đường truyền quang. Mỗi một máy thu sẽ sử dụng bộ tách sóng kiểu trực tiếp với cơ chế tách ngưỡng kép được dùng để khôi phục các khóa. Do giao thức QKD sử dụng trong hệ thống dựa trên các hệ thống quang không dây tiêu chuẩn nên kẻ nghe lén thực hiện kiểu tấn công đơn giản ở lớp vật lý sẽ có hiệu quả nhất. Trong kịch bản này, kẻ nghe lén sẽ thực hiện cuộc tấn công trái phép bằng cách định vị máy thu trái phép Eve trong phạm vi gần chùm tia và/ hoặc phía sau máy thu Bob.



a. Máy phát



b. Máy thu

Hình 4. 6. Sơ đồ khối của: (a) máy phát, (b) máy thu trong hệ thống CV-QKD dựa trên vệ tinh sử dụng kỹ thuật phân chia theo mã.

Hình 4.6 (a) và 4.6 (b) mô tả sơ đồ khối máy phát và máy thu trong hệ thống CV-QKD sử dụng kỹ thuật phân chia theo mã thực hiện điều chế kiểu cường độ. CV-QKD kiểu này có thể triển khai được trong các hệ thống quang tiêu chuẩn với cấu hình đơn giản, độ bảo mật cao.

Quá trình chia sẻ khóa giữa Alice và Bob:

Alice tạo ra một chuỗi ngẫu nhiên và truyền tín hiệu quang với mức công suất là 0 hoặc μP_r tùy thuộc vào giá trị bit phát đi là "0" hay là "1", với μ là độ sâu điều chế, $0 < \mu < 1$. Bob sẽ nhận tín hiệu quang và khôi phục lại giá trị các bit đã được phát đi. Bob sẽ thông báo cho Alice các khoảng thời gian mà Bob có thể khôi phục được các bit nhị phân từ tín hiệu quang thu được. Alice sẽ loại bỏ các giá trị ở các khoảng thời gian mà Bob không tạo được các bit. Tiếp theo, Alice và Bob chia sẻ một chuỗi bit có giá trị xác định, đó chính là khóa chọn lọc. μ có giá trị nhỏ sao cho hai trạng thái coherent tương đương với bit "0" và bit "1" là không trực giao với nhau. Do đó, kẻ nghe lén Eve không thể phân biệt được hoàn toàn trạng thái được truyền.

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.

Bộ tách ngưỡng kép được sử dụng để khôi phục các bit "0", "1" và "X". Luật của bộ tách ngưỡng kép được sử dụng trong đề xuất này như sau:

$$Giá\ trị\ bit = \begin{cases} 0\ nếu\ I \le d_0 \\ 1\ nếu\ I \ge d_1 \\ X\ \ trường\ hợp\ còn\ lại \end{cases} . \quad (4.11)$$

Việc Bob thông báo cho Alice các khoảng thời gian Bob tạo ra các bit "0" hoặc "1" được thực hiện thông qua kênh công khai, ví dụ như có thể sử dụng kênh vô tuyến. Phía máy phát cũng loại bỏ các giá trị bit tại các khoảng thời gian mà phía máy thu không khôi phục được các bit "0" và "1". Các bit còn lại tạo thành khóa chọn lọc và được chia sẻ giữa máy phát và máy thu. Chiều dài của khóa chọn lọc được thể hiện thông qua tham số P_{sift}, đó chính là khả năng mà Bob có thể tách được bit "0" và bit "1". P_{sift} lớn sẽ dẫn tới khóa chọn lọc dài và tốc độ khóa lớn.

4.3.3. Mô hình kênh truyền

Đường truyền FSO từ vệ tinh đến trạm mặt đất chịu ảnh hưởng của các yếu tố chính như suy hao do khí quyển, suy hao do trải rộng chùm tia và lỗi định hướng, nhiễu loạn khí quyển.

Suy hao do khí quyển của một tín hiệu quang là suy hao của tín hiệu quang bị ảnh hưởng bởi các điều kiện của khí quyển, đặc biệt là sự xuất hiện của các hạt gây ra hiện tượng hấp thụ và tán xạ. Có thể coi sương mù là nguyên nhân chính gây tán xạ photon và nó góp phần vào sự suy giảm công suất quang vì kích thước hạt sương tương đối lớn so với dải bước sóng sử dụng trong FSO. Một kỹ thuật đơn giản để mô hình hóa toán học suy hao do khí quyển là dựa trên tầm nhìn. Dải tầm nhìn là khoảng cách mà chùm tia sáng song song đi qua bầu khí quyển cho đến khi cường độ của nó giảm 2% so với giá trị ban đầu. Sự phụ thuộc của suy hao do khí quyển vào tầm nhìn V (km) và bước sóng λ (μm) được biểu diễn theo công thức [90]:

$$\gamma_0 = 10 \log_{10}(e) \frac{3.912}{V} \left(\frac{\lambda}{0.55}\right)^{-g(V)} \quad (4.12)$$

Trong công thức (4.12), e là hệ số Euler, $g(V)$ là hệ số suy hao trong khi quyển phụ thuộc tầm nhìn và được tính theo công thức sau trong mô hình Kruse:

$$g(V) = \begin{cases} 1{,}6 & với\ V > 50\ km \\ 1{,}3 & với\ 6\ km < V < 50\ km \\ 0{,}585V^{1/3} & với\ V < 6\ km \end{cases} \quad (4.13)$$

Công thức (4.13) phù hợp cho việc tính toán suy giảm dọc theo một đường truyền thông thường tới bề mặt Trái đất, khi mà tán xạ Mie là chủ yếu và hấp thụ tín hiệu quang có thể bỏ qua. Khi xem xét một đường truyền quang tới bề mặt Trái đất không theo kiểu thông thường, suy hao nghiêng đường truyền do suy hao khí quyển được tính theo công thức:

$$h_{al} = \gamma_0 \int_0^{\infty} \exp(-\frac{l \sin(\theta_h)}{H_a})\, dl, \quad (4.14)$$

với θ_h là góc của độ cao trên đường chân trời và H_a là chiều cao phía trên mà ảnh hưởng của suy giảm do khí quyển là không đáng kể.

Suy hao do trải rộng chùm tia, lỗi định hướng và ảnh hưởng của pha-đinh do nhiễu loạn khí quyển đã được trình bày ở mục 2.1 của luận án.

4.3.4. Phân tích hiệu năng hệ thống

Tại phía Bob, tín hiệu quang nhận được được phân chia thành *K* nhánh tương đương với *K* kênh. Tại mỗi một nhánh, một bộ giải mã được sử dụng để tách kênh tín hiệu mong muốn. Tín hiệu này được biểu diễn bằng biểu thức sau:

$$E_s(t) = \omega\sqrt{P_r}\exp(\omega_c t + \phi_d) + kx_c\sqrt{P_r}\exp(\omega_c t + \phi_i) \quad (4.15)$$

Trong công thức (4.15), ω là trọng lượng mã; k là số kênh hoạt động, đó chính là các kênh đang gửi đi bit "1"; x_c là giá trị tương quan chéo phụ thuộc vào loại của tập mã được sử dụng; kx_c phản ánh số các xung nhiễu từ các kênh khác; ω_c và ϕ_d, ϕ_i là tương ứng tần số và pha của sóng mang quang; P_r là công suất quang thu được. Mối quan hệ giữa công suất quang thu được với công suất quang phát đi được biểu diễn bởi công thức:

$$P_r = \mu P_t h_a h_l G_{Tx} G_{Rx} \quad (4.16)$$

với G_{Tx} , G_{Rx} tương ứng là độ khuếch đại của thấu kính phát và thấu kính thu; μ là độ sâu điều chế; P_t là công suất quang phát đi; h_a, h_l tương ứng là suy hao do khí quyển và suy hao do mở rộng chùm tia, lệch hướng.

Sau khi được giải mã, tín hiệu thu được sẽ được chuyển đổi từ tín hiệu dạng quang sang tín hiệu dạng điện nhờ đi-ốt quang thác. Biểu thức toán học cho dòng điện thu được ở đầu ra đi-ốt quang thác trong trường hợp Alice gửi bit "0" và bit "1" được biểu diễn theo công thức sau:

$$I_1(k) = \Re M_A(\omega + kx_c)P_r + i_n(t) \tag{4.17}$$

$$I_o(k) = \Re M_A kx_c P_r + i_n(t) \tag{4.18}$$

với $\Re$, M_A tương ứng là đáp ứng và hệ số thác lũ của đi-ốt quang thác APD; i_n là dòng điện nhiễu gây ra bởi nhiễu nổ, nhiễu nền và nhiễu nhiệt. Theo lý thuyết, dòng điện nhiễu có thể được mô hình hóa như một biến ngẫu nhiên Gauss với trung bình bằng không. Phương sai của dòng điện nhiễu trong trường hợp bit "0" và bit "1" được xác định bằng công thức sau:

$$\sigma_1(k)^2 = 2q\Re {M_A}^2 F_A(\omega P_r + kx_c P_r + P_b)B + \frac{4k_B T_e}{R_L} F_n B, \tag{4.19}$$

$$\sigma_0(k)^2 = 2q\Re {M_A}^2 F_A(kx_c P_r + P_b)B + \frac{4P_b T}{R_L} F_n B, \tag{4.20}$$

Trong công thức (4.19) và (4.20), q là điện tích electron; F_n là hệ số nhiễu của máy thu; B là băng thông nhiễu hiệu dụng và có thể xấp xỉ với tốc độ bit R_b; P_b là công suất nền; k_B là hằng số Boltzmann; $T_e$là nhiệt độ tuyệt đối tại máy thu; R_L là điện trở tải; F_A được tính theo công thức:

$$F_A = M_A x + (2 - \left(\frac{1}{M_A}\right))(1 - x) \tag{4.21}$$

với x là hệ số nhiễu trội của APD.

Khi Alice truyền một chuỗi bit ngẫu nhiên trong một kênh, có thể giả thiết xác suất truyền các bit "1" và các bit "0" của các kênh là như nhau và đều bằng ½. Theo

luật tách ngưỡng kép, các khả năng Bob tách bit "0" là $P_{A,B}(a,0)$ và tách bit "1" là $P_{A,B}(a,1)$ với $a \in \{0,1\}$ được xác định theo các công thức như sau:

$$P_{A,B}(a,0) = \frac{1}{2}\sum_{k=0}^{K-1} p(k) Q\left(\frac{I_a(k)-d_0}{\sigma_n(k)}\right) \quad (4.22)$$

$$P_{A,B}(a,1) = \frac{1}{2}\sum_{k=0}^{K-1} p(k) Q\left(\frac{d_1-I_a(k)}{\sigma_n(k)}\right) \quad (4.23)$$

Trong công thức (4.22) và (4.23), d_0 và d_1 tương ứng là các ngưỡng tách bit "0" và bit "1"; $Q(.)$ là hàm Q Gauss; $p(k)$ là xác suất mà k của K-1 kênh nhiễu đồng thời là "1", tuân theo phân bố nhị thức, $p(k)$ được xác định theo công thức:

$$p(k) = \binom{K-1}{k} 2^{-(K-1)} \quad (4.24)$$

các giá trị ngưỡng d_0 và d_1 được xác định theo công thức (3.3) và (3.4); P_{error} và P_{sift} được tính theo công thức (1.2) và (1.3).

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

$$SKR = K\, P_{sift} R_b \quad (4.25)$$

4.3.5. Kết quả khảo sát hiệu năng hệ thống

Luận án thực hiện khảo sát tham số hiệu năng của hệ thống CV-QKD đề xuất sử dụng kỹ thuật CDM với một tập các tham số như hệ số ngưỡng kép, độ sâu điều chế, số kênh, công suất phát...như trong Bảng 4.2.

Các tham số liên quan đến bộ thu phát quang được tham khảo từ [3] và các tham số liên quan đến trạm vệ tinh, trạm mặt đất dựa trên những thông số trong hệ thống truyền dẫn sử dụng đường truyền FSO dựa trên vệ tinh. Nhiễu loạn khí quyển được xem xét trong khảo sát là nhiễn loạn khí quyển ở mức độ trung bình. Kỹ thuật CDM được thực hiện dựa trên mã nguyên tố với trọng lượng mã là 7 và giá trị tương quan chéo lớn nhất là 2 [102].

Các tham số hiệu năng của hệ thống CV-QKD đề xuất cần được khảo sát bao gồm QBER, P_{sift} tại máy thu hợp lệ Bob và phía kẻ nghe lén Eve. Ngoài ra, tốc độ

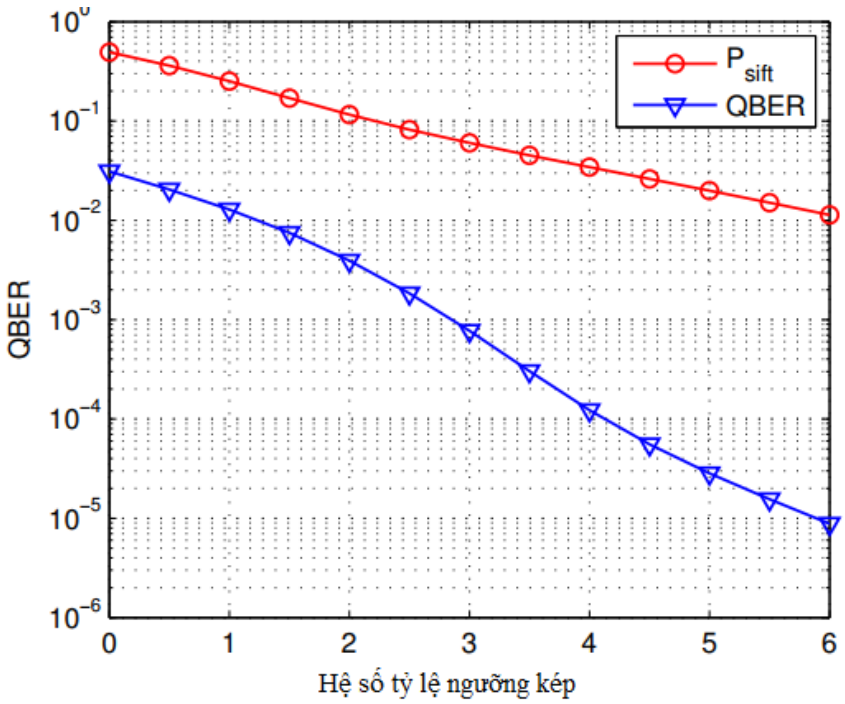
truyền khóa bí mật SKR của hệ thống cũng được khảo sát để đánh giá tính khả thi của hệ thống đã đề xuất. QBER, P_{sift}, SKR lần lượt được tính theo các công thức (1.1), (1.2), (1.3) và (4.25), trong đó các xác suất kết hợp được tính theo công thức (4.22) và (4.23).

Bảng 4. 2. Bảng các tham số dùng trong khảo sát hiệu năng hệ thống QKD-FSO có vệ tinh sử dụng kỹ thuật đa truy nhập ghép kênh theo mã.

Tên	**Ký hiệu**	**Giá trị**
Điện trở tải	R_L	50 Ω
Hằng số Boltzmann	k_B	$1{,}38 \times 10^{-23}$ W/K/Hz
Điện tích electron	q	$1{,}6 \times 10^{-19}$ C
Tốc độ bit	R_b	1 Gb/s
Hệ số ion hóa	k_A	0,7 (Với APD loại InGaAS)
Bước sóng	λ	1550 nm
Vận tốc gió	v	21 m/s
Đáp ứng APD	$\Re$	0,8
Nhiệt độ tại máy thu	T_e	298 K
Hệ số nhân thác lũ của APD	M_A	15
Công suất nền	P_b	-40 dBm
Bán kính khẩu độ tách sóng	a	0,31 m
Độ rộng chùm tia tại trạm mặt đất	ω_D	50 m
Góc phương vị	ζ	60^0
Nhiễu loạn khí quyển tại mặt đất	$C_n^2(0)$	$1{,}7 \times 10^{-14} m^{-2/3}$

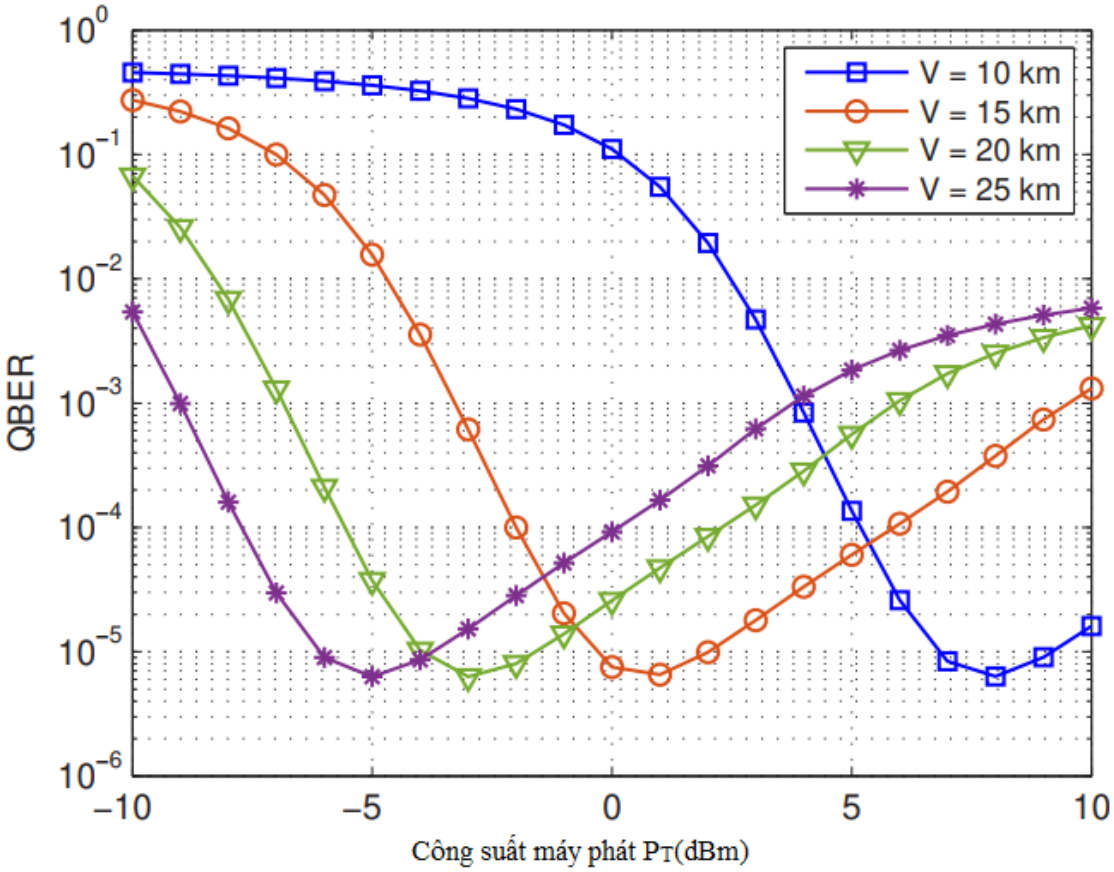
Độ cao vệ tinh	H_S	600 km
Độ cao trạm mặt đất	H_G	5 m
Độ khuếch đại thấu kính phát	G_T	15 dB
Độ khuếch đại thấu kính thu	G_R	25 dB

Với hệ thống đã thiết kế, một trong những tham số quan trọng cần xác định là hệ số tỷ lệ ngưỡng kép. Hình 4.6 là kết quả khảo sát các tham số hiệu năng QBER và P_{sift} tại phía thu Bob theo giá trị của hệ số tỷ lệ ngưỡng kép trong trường hợp công suất phát P_T=-2dBm, độ sâu điều chế μ=0,2 và số kênh là 3. Độ sâu điều chế được chọn là 0,2 với mục đích để kẻ nghe lén Eve chịu tỷ lệ lỗi QBER lớn và nhận được các thông tin về khóa ít đi. Giá trị của hệ số tỷ lệ ngưỡng kép phản ánh sự khác biệt giữa hai ngưỡng của bộ tách ngưỡng kép nên nếu giá trị hệ số tỷ lệ ngưỡng kép tăng thì giá trị QBER sẽ giảm. Tuy nhiên, khi đó giá trị của P_{sift} cũng giảm đi. Qua kết quả khảo sát ở Hình 4.6, giá trị nhỏ nhất của hệ số tỷ lệ ngưỡng kép để đảm bảo giá trị QBER $\leq 10^{-3}$ là 2,9, tại giá trị này của hệ số tỷ lệ ngưỡng kép, giá trị P_{sift} là 6 $\times 10^{-2}$.



Hình 4. 7. QBER và P_{sift} tại phía thu Bob phụ thuộc vào giá trị của hệ số tỷ lệ ngưỡng kép khi P_T=-2dBm, độ sâu điều chế μ=0,2, số kênh là 3.

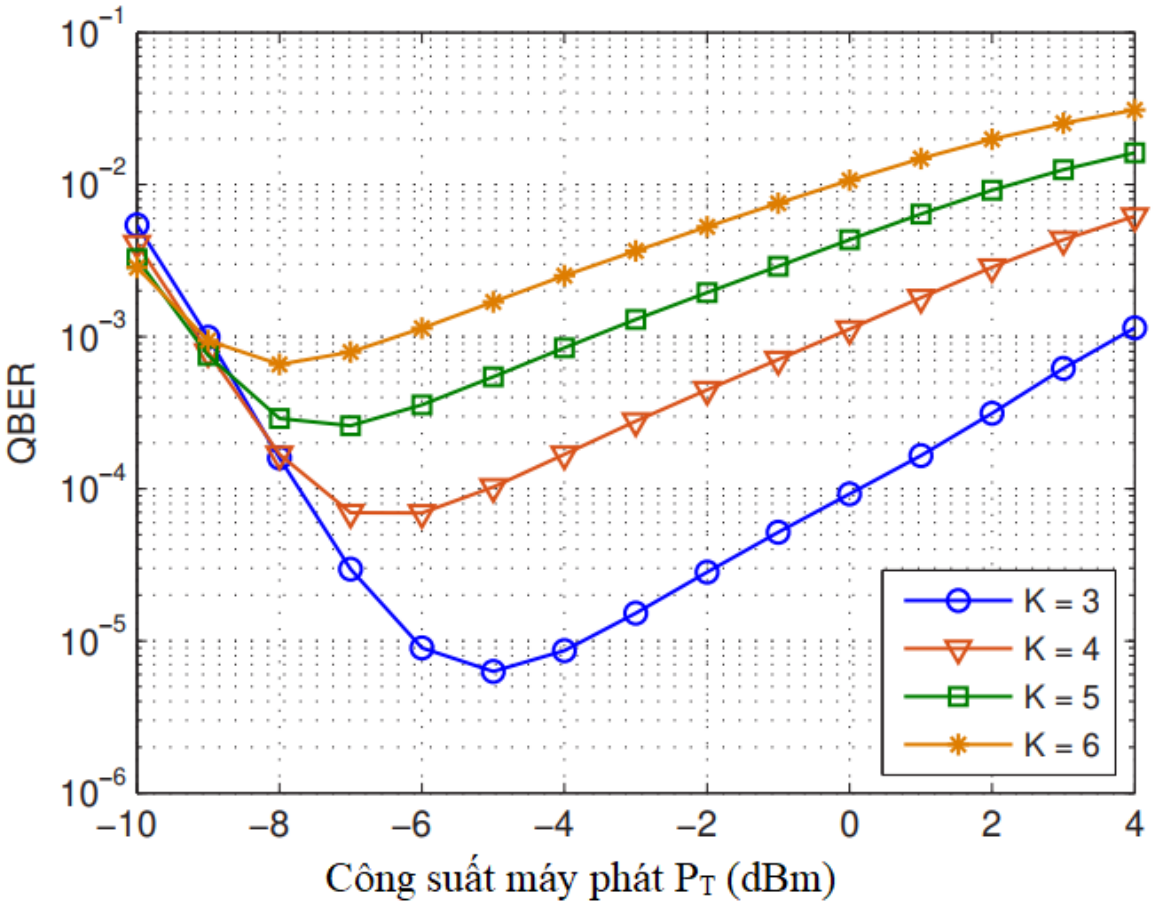
Hình 4.8 là kết quả khảo sát sự phụ thuộc của QBER vào công suất phát trong điều kiện số người dùng là 3 và hệ số tỷ lệ ngưỡng kép là 5. Luận án khảo sát trên các điều kiện khác nhau của tầm nhìn, cụ thể V=10 km, V= 15 km, V= 20 km và V= 25 km. Khi suy hao khí quyển tăng với tầm nhìn giảm, hệ thống có thể đạt được mục tiêu QBER≤10^{-3} bằng việc tăng công suất phát. Theo kết quả khảo sát ở Hình 4.8, khi tầm nhìn giảm từ 25 km xuống 10 km, công suất máy phát cần thiết phải tăng từ -9 dBm tới 4 dBm để duy trì được QBER≤10^{-3} .



Hình 4. 8. Sự phụ thuộc của QBER tại máy thu Bob theo công suất phát trong trường hợp số người sử dụng là 3 và hệ số ngưỡng kép là 5.

Hình 4.9 là kết quả thu được khi khảo sát giá trị của QBER tại máy thu hợp lệ Bob theo công suất phát trong trường hợp số người dùng thay đổi từ là 3 đến 6, độ sâu điều chế μ=0,2 và hệ số tỷ lệ ngưỡng kép là 5. Có thể dễ dàng nhận thấy, đồ thị QBER thu được có thể chia làm hai vùng. Ở vùng thứ nhất, ảnh hưởng của số người

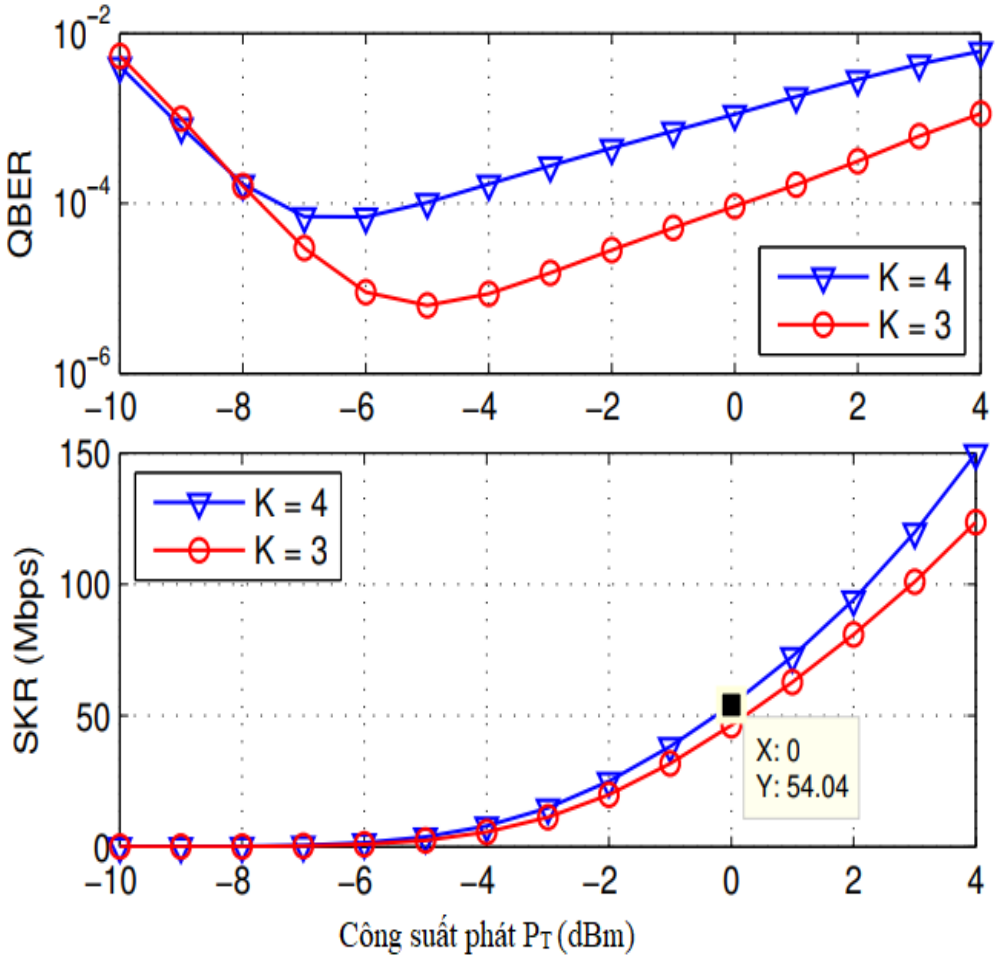
sử dụng là không đáng kể, do đó giá trị của QBER giảm khi công suất phát tăng. Ở vùng thứ hai, ảnh hưởng của số người sử dụng là đáng kể, giá trị của QBER tăng theo công suất phát. Giá trị của công suất phát tương ứng với giá trị nhỏ nhất của QBER trên đồ thị thu được ở Hình 4.9 có thể coi là giá trị tối ưu. Tuy nhiên, giá trị công suất phát tối ưu này còn phụ thuộc vào số người dùng. Với số lượng người dùng là 3, công suất phát tối ưu sẽ là -5dBm. Khi số lượng người dùng tăng lên 5, giá trị công suất phát tối ưu sẽ giảm tới -7dBm do sự gia tăng về số lượng người dùng.



Hình 4. 9. QBER tại Bob theo công suất phát trong trường hợp người dùng thay đổi từ 3 đến 6, độ sâu điều chế μ=0,2 và hệ số tỷ lệ ngưỡng kép ρ=5

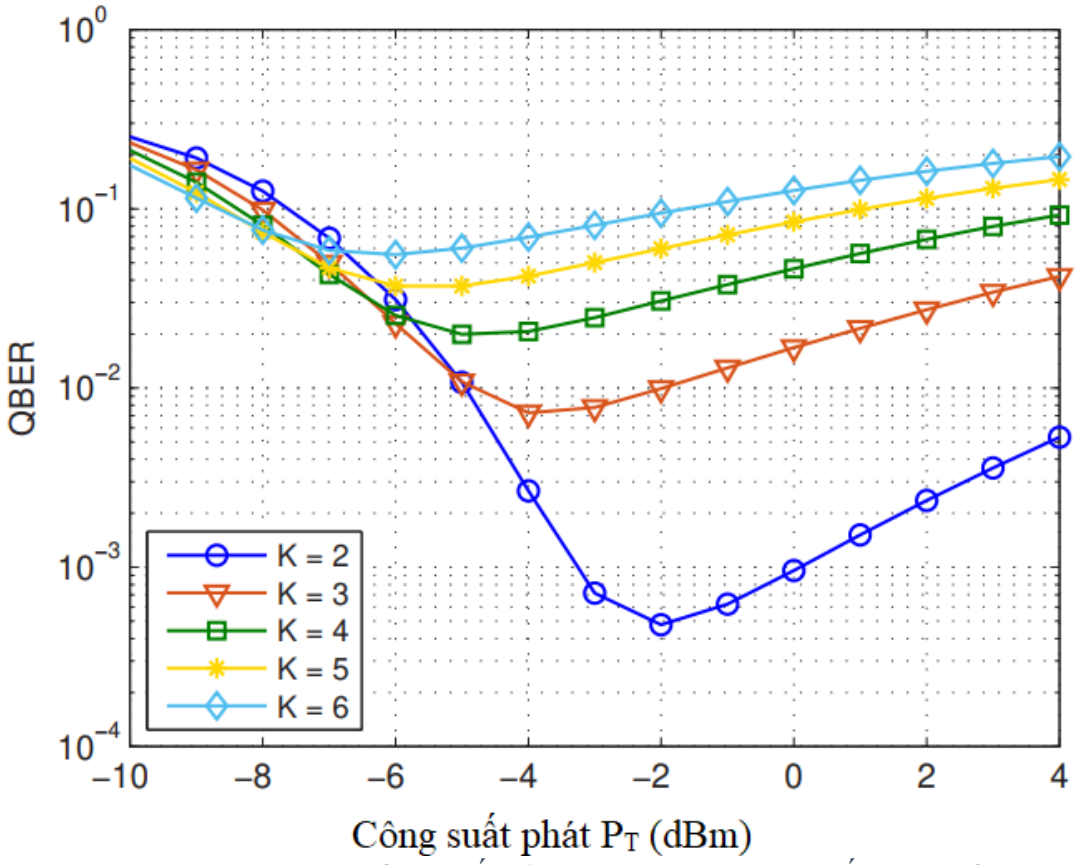
Tốc độ truyền khóa là một tham số đánh giá hiệu năng của hệ thống phân phối khóa đề xuất. Theo công thức (4.27), giá trị của tốc dộ truyền khóa phụ thuộc vào giá trị của P_{sift}. Hình 4.10 là kết quả khảo sát giá trị QBER và SKR của hệ thống đề xuất

theo công suất phát khi hệ số tỷ lệ ngưỡng kép là 5. Có thể dễ dàng nhận thấy, giá trị của SKR tăng cùng với giá trị công suất phát tăng. Tuy nhiên, số lượng bit trong khóa chọn lọc thu được không chỉ là các bit của chuỗi khóa phát đi đã được tách và giải mã đúng mà còn bao gồm cả những bit của chuỗi khóa phát đi đã bị tách và giải mã sai giá trị. Do đó, giá trị của SKR nên được xác định bởi giá trị lớn nhất của QBER. Ví dụ, trong trường hợp số người dùng là 3, giá trị QBER lớn nhất là 10^{-3}, công suất phát giới hạn là 4 dBm, giá trị lớn nhất SKR đạt được là 123,7 Mb/s. Trong trường hợp số người sử dụng là 4, giá trị SKR lớn nhất mà hệ thống đạt được giảm xuống tới 54 Mb/s do sự gia tăng của số người sử dụng. Công suất phát nên chọn trong trường hợp này là 0 dBm.



Hình 4. 10. QBER và SKR theo công suất phát khi hệ số tỷ lệ ngưỡng kép ρ=5

Một vấn đề cần quan tâm tới trong hệ thống QKD đề xuất là hiệu năng về mặt an ninh khi có mặt của kẻ nghe lén Eve. Trong nghiên cứu này, luận án giả thiết Eve có cùng cơ chế thu như bên thu hợp pháp Bob, tuy nhiên sai mã. Công suất mà Eve nhận được phụ thuộc vào giá trị của tương quan chéo, tương quan chéo có giá trị lớn nhất là 2 trong khảo sát của luận án. Hình 4.11 là kết quả khảo sát giá trị QBER tại Eve theo giá trị của công suất phát trong trường hợp hệ số tỷ lệ ngưỡng kép là 4, độ sâu điều chế là 0,2 và số lượng người sử dụng thay đổi từ 2 đến 4.

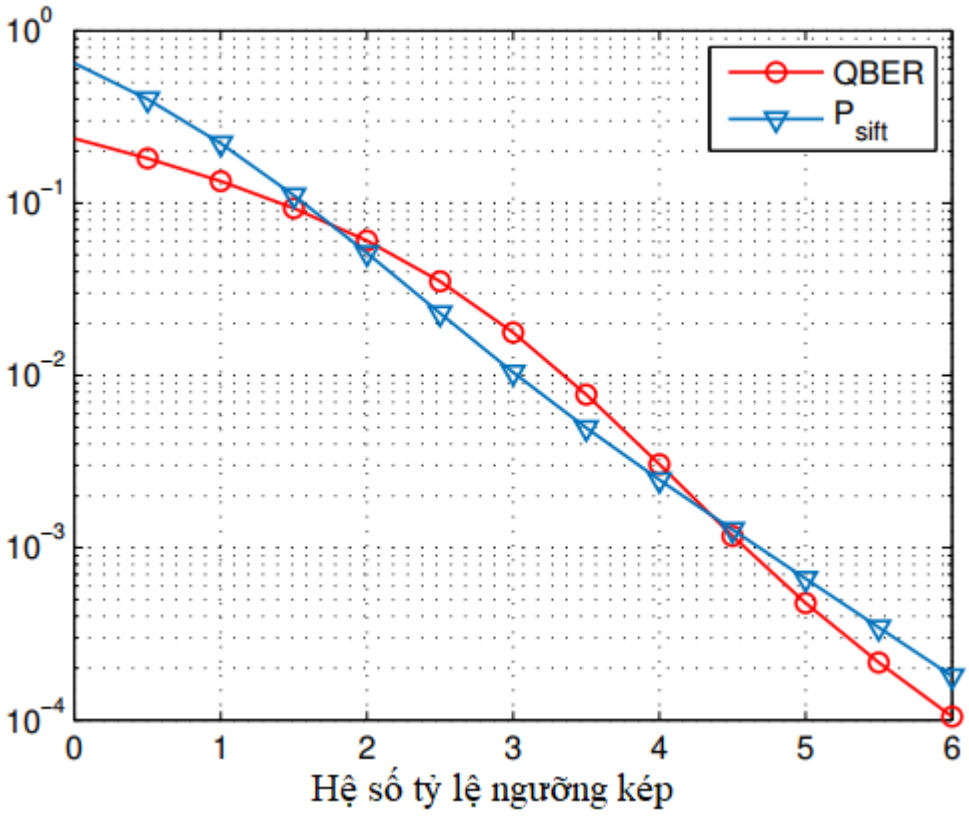


Hình 4. 11. QBER tại Eve theo công suất phát trong trường hợp số người dùng thay đổi

Qua kết quả khảo sát ở Hình 4.11, có thể nhận thấy kẻ nghe lén Eve có giá trị QBER cao hơn, đặc biệt khi số lượng người dùng lớn. Điều này nghĩa là số lượng người dùng tăng có ảnh hưởng tích cực tới hiệu năng an ninh của hệ thống QKD đề xuất. Tuy nhiên, QBER tại Eve vẫn lớn hơn 10^{-3} trong trường hợp số người dùng là

2. Với giá trị QBER lớn như vậy, Eve không thể sửa được các bit bị lỗi ngay cả trường hợp biết mã sửa lỗi.

Hình 4.12 là kết quả khảo sát trong trường hợp Eve thay đổi hệ số tỷ lệ ngưỡng kép nhằm thu được giá trị QBER thấp. Trường hợp xấu nhất là trường hợp ứng với số người sử dụng là 2. Kết quả khảo sát cho thấy, Eve có thể thiết lập hệ số tỷ lệ ngưỡng kép lớn hơn 4,5 để thu được QBER có giá trị nhỏ hơn 10^{-3}. Tuy nhiên, trong trường hợp này P_{sift} có giá trị nhỏ hơn 10^{-3}. Điều đó có nghĩa là tổng số bit Eve giải mã được nhỏ hơn tổng số bit mà Bob giải mã được. Do vậy, Eve không thể khôi phục được khóa chia sẻ giữa Alice và Bob.



Hình 4. 12. QBER và P_{sift} tại Eve khi thay đổi hệ số tỷ lệ ngưỡng kép

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. Tính khả thi của giải pháp đề xuất đã được đánh giá thông qua các kết quả phân tích hiệu năng. Các kết quả cho thấy rằng, hệ thống QKD đa kênh đã đề xuất có thể đảm bảo yêu cầu về QBER dưới sự ảnh hưởng của tạp âm, nhiễu và trong các điều kiện nhiễu loạn khác nhau. Đặc biệt, hệ thống có thể cung cấp tốc độ truyền khóa hàng Gbit/s, điều mà các hệ thống QKD đơn kênh và các hệ thống QKD đa kênh trước đây không thực hiện được. Khả năng cung cấp SKR tốc độ Gbit/s có vai trò rất quan trọng trong việc tạo ra các khóa bí mật chia sẻ có độ dài lớn nhằm tạo ra khả năng an ninh vô điều kiện cho các hệ thống truyền thông trong tương lai. Giải pháp QKD đa kênh dựa trên SCM-WDM có thể được ứng dụng trong việc phân phối khóa lượng tử từ vệ tinh tới đồng thời nhiều trạm mặt đất nhằm tạo ra mạng QKD có quy mô toàn cầu. Tuy nhiên, giải pháp QKD đa kênh đề xuất gây tốn băng thông và công suất của hệ thống. Trong các hệ thống QKD-FSO do sử dụng quang để truyền thông tin về khóa, băng thông rộng nên nhược điểm về băng thông có thể được coi là không quan trọng.

-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. Bằng việc chọn giá trị của hệ số tỷ lệ ngưỡng kép phù hợp, giá trị tỷ lệ lỗi QBER và P_{sift} đảm bảo được yêu cầu đề ra với một hệ thống QKD và hỗ trợ được nhiều người dùng. Giải pháp đề xuất có ý nghĩa thiết thực trong việc tạo ra mạng QKD với nhiều người dùng trong thực tế.

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. Toàn bộ các kiến thức nền tảng và các kết quả nghiên cứu đã được trình bày chi tiết trong luận án với bố cục gồm 04 Chương như sau: 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. Các kết quả đóng góp mới về khoa học của luận án có thể phân thành ba nhóm như sau:

1. 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

Luận án đã đề xuất phương thức truyền dẫn khóa lượng tử với điều chế pha kiểu QPSK ở phía phát kết hợp sử dụng máy thu tách sóng kiểu heterodyne và cơ chế tách ngưỡng kép. So với các nghiên cứu đã có, phương thức truyền dẫn khóa lượng tử đề xuất sử dụng điều chế quang kiểu QPSK, không yêu cầu sử dụng bộ điều chế sóng mang phụ tần số vô tuyến RF đã dẫn tới hệ thống đơn giản hơn, tương thích với truyền thông quang truyền thống.

2. 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.

Đóng góp này cũng có thể được tách thành hai nội dung như sau:

– Thứ nhất là đề xuất hệ thống sử dụng kỹ thuật chuyển tiếp dựa trên hạ tầng trên cao HAP và kỹ thuật phát lại khóa theo kiểu yêu cầu phát lại tự động tại trạm chuyển tiếp. Các kỹ thuật chuyển tiếp dựa trên hạ tầng trên cao hay ARQ không mới

và được sử dụng trong truyền thông truyền thống nhưng chưa được đề xuất trong hệ thống phân phối khóa lượng tử QKD-FSO.

– Thứ hai là xây dựng mô hình giải tích để tính toán các tham số hiệu năng như tỷ lệ mất khóa KLR, tỷ lệ trễ vượt ngưỡng. Các mô hình toán học đã có từ trước không thể áp dụng trong việc tính toán các tham số hiệu năng của hệ thống đề xuất do các mô hình này chỉ sử dụng bit "0" và bit "1". Mô hình toán học mà luận án xây dựng được sử dụng trong trường hợp hệ thống truyền khóa lượng tử với kênh truyền dẫn có đầu vào rời rạc (4 trạng thái), và đầu ra của kênh truyền dẫn có xóa do có khả năng xuất hiện của một trong ba bit là "1", "0" hoặc "X" sau tách sóng ở bên thu.

3. Đề xuất các giải pháp truyền dẫn đa kênh đa người sử dụng cho hệ thống phân phối khóa lượng tử biến liên tục qua không gian tự do

Luận án đã đề xuất 02 giải pháp truyền dẫn cho hệ thống QKD-FSO đa kênh.

- Thứ nhất**,** hệ thống QKD-FSO sử dụng kỹ thuật phân phối khóa lượng tử đa kênh từ vệ tinh sử dụng (1) kỹ thuật ghép kênh sóng mang phụ SCM và (2) kỹ thuật phân chia theo bước sóng WDM. Kỹ thuật SCM và WDM đã phát triển và triển khai ở các hệ thống truyền thông nhưng việc kết hợp cả hai kỹ thuật này dùng cho hệ thống QKD-FSO chưa được nghiên cứu.

- Thứ hai, hệ thống QKD-FSO sử dụng 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.

Hướng phát triển của luận án:

Những giải pháp cải thiện hiệu năng mà luận án đề xuất có thể ứng dụng trong hệ thống QKD-FSO đơn kênh và đa kênh dựa trên vệ tinh. Tuy nhiên trong luận án, các nghiên cứu chưa đánh giá chi tiết và định lượng tất cả các nguy cơ tấn công hệ thống truyền khóa từ phía Eve cũng như xem xét các ảnh hưởng và nguy cơ mất an ninh do quá trình báo hiệu ở bước 3 và bước 4 của giao thức QKD gây ra. Do đó, các nghiên cứu tiếp theo trong tương lai 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.

Ngoài ra, trong xu thế phát triển mạnh mẽ hiện nay của hệ thống QKD có quy mô toàn cầu với sự xuất hiện của các mạng QKD bao gồm nhiều trạm QKD, đa dạng kiểu cấu hình kết nối, cung cấp nhiều loại hình dịch vụ, yêu cầu tính linh động cao thì việc đề xuất hệ thống và đưa ra các giải pháp cải thiện hiệu năng cho hệ thống QKD được định nghĩa bằng phần mềm là cần thiết. Mạng QKD được định nghĩa bằng phần mềm sẽ cho phép tự động hóa việc cung cấp các dịch vụ trong một cơ sở hạ tầng mạng QKD có sẵn, điều này giúp cho các nhà khai thác dịch vụ tránh khỏi việc triển khai các dịch vụ mới bằng cách can thiệp thủ công hoặc phải sử dụng các dịch vụ được cung cấp bởi các nhà cung cấp độc quyền.

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-variable quantum key distribution systems using code-division multiple access"***, Optics Continuum, vol. 2, no. 2, pp. 289-302, Feb. 2023. DOI: 10.1364/OPTCON.474509

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.

TÀI LIỆU THAM KHẢO

Tiếng Việt

1. Lê Minh Thanh (2008), "Mô phỏng mật mã lượng tử theo giao thức BB84", *Khoa học Tự nhiên và Công nghệ* 24, tr. 238-247.
2. Nguyễn Văn Tuấn, Nguyễn Ngọc Dương, Phan Vĩnh Vương (2012), "Nâng cao chất lượng tuyến thông tin quang không dây trong điều kiện khí hậu Việt Nam", *Khoa học và Công nghệ, Đại học Đà Nẵng*, 54(5), tr. 79-86.

Tiếng Anh

3. Agrawal, G.P. (2002), *Fiber-optic communication systems*, Wiley.
4. Ai, X., Malaney, R., and Ng, S. X. (2020), "A Reconciliation Strategy for Real-Time Satellite-Based QKD", *IEEE Communications Letters*. 24(5), pp. 1062-1066.
5. Alberto Carrasco-Casado, Verónica Fernández, Natalia Denisenko (2016), "Free-space quantum key distribution", *Optical Wireless Communications - An Emerging Technology*, Springer International Publishing.
6. Alléaume, R., et al. (2014), "Using quantum key distribution for cryptographic purposes: A survey", *Theoretical Computer Science*. 560, pp. 62-81.
7. Alshaer, N., Nasr, M. E., and Ismail, T. (2021), "Hybrid MPPM-BB84 Quantum Key Distribution Over FSO Channel Considering Atmospheric Turbulence and Pointing Errors", *IEEE Photonics Journal*. 13(6), pp. 1-9.
8. Bahaa E. A. Saleh, Malvin Carl Teich (2019), *Fundamentals of Photonics*, 3 rd ed, Wiley, New York.
9. Bedington, Robert, Arrazola, Juan Miguel, and Ling, Alexander (2017), "Progress in satellite quantum key distribution", *npj Quantum Information*. 3(1), p. 30.
10. Bennett, Charles H. and Brassard, Theor. Comput. Sci. (2014), "Quantum cryptography: Public key distribution and coin tossing". 560, pp. 7-11.

11. Bloom, Scott, et al. (2003), "Understanding the performance of free-space optics [Invited]", *Journal of Optical Networking*. 2(6), pp. 178-200.
12. Borelli, L. F. M., et al. (2016), "Quantum key distribution using continuous-variable non-Gaussian states", *Quantum Information Processing*. 15(2), pp. 893-904.
13. Bourgoin, Jean-Philippe, et al. (2015), "Free-space quantum key distribution to a moving receiver", *Optics Express*. 23(26), pp. 33437-33447.
14. Buttler, W. T., et al. (2003), "Fast, efficient error reconciliation for quantum cryptography", *Physical Review A*. 67(5), pp. 052303-0523038.
15. Calderaro, Luca, et al. (2018), "Towards quantum communication from global navigation satellite system", *Quantum Science and Technology*. 4(1), p. 015012.
16. Carrasco-Casado, Alberto and Mata-Calvo, Ramon (2020), "Space Optical Links for Communication Networks", *Springer Handbook of Optical Networks*, Springer International Publishing, Cham, pp. 1057-1103.
17. Chaleshtory, Z. N., et al. (2017), "Experimental Investigation of Environment Effects on the FSO Link With Turbulence", *IEEE Photonics Technology Letters*. 29(17), pp. 1435-1438.
18. Chandra, S., et al. (2014), "A comparative survey of Symmetric and Asymmetric Key Cryptography", *2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE)*, pp. 83-93.
19. Costa e Silva, M. B., et al. (2006), Homodyne QPSK Detection for Quantum Key Distribution, *Optical Amplifiers and Their Applications/Coherent Optical Technologies and Applications*, Optical Society of America, Whistler, p. CFA2.
20. Dequal, Daniele, et al. (2021), "Feasibility of satellite-to-ground continuous-variable quantum key distribution", *npj Quantum Information*. 7(1), p. 3.

21. Dequal, Daniele, et al. (2016), "Experimental single-photon exchange along a space link of 7000 km", *Physical Review A*. 93(1), p. 010301.
22. Diamanti, Eleni, et al. (2016), "Practical challenges in quantum key distribution", *npj Quantum Information*. 2(1), p. 16025.
23. Duyen, Trung Ha, Trong, Tuan Do, and T., Anh Pham (2014), "Pointing error effects on performance of free-space optical communication systems using SC-QAM signals over atmospheric turbulence channels", *AEU - International Journal of Electronics and Communications*. 68(9), pp. 869-876.
24. Eleni Diamanti and Leverrier, Anthony (2015), "Distributing Secret Keys with Quantum Continuous Variables: Principle, Security and Implementations", *Entropy*. 17(pp. 6072-6092).
25. Fang, Jian, Huang, Peng, and Zeng, Guihua (2014), "Multichannel parallel continuous-variable quantum key distribution with Gaussian modulation", *Physical Review A*. 89(2), p. 022315.
26. Farid, A. A. and Hranilovic, S. (2007), "Outage Capacity Optimization for Free-Space Optical Links With Pointing Errors", *Journal of Lightwave Technology*. 25(7), pp. 1702-1710.
27. Fossier, S., et al. (2009), "Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers", *Journal of Physics B: Atomic, Molecular and Optical Physics*. 42(11), p. 114014.
28. Gabay, M. and Arnon, S. (2006), "Quantum key distribution by a free-space MIMO system", *Journal of Lightwave Technology*. 24(8), pp. 3114-3120.
29. Ghassemlooy, Z., Popoola, W. O., and Leitgeb, E. (2007), Free-Space Optical Communication Using Subearrier Modulation in Gamma-Gamma Atmospheric Turbulence, *2007 9th International Conference on Transparent Optical Networks*, pp. 156-160.
30. Gisin, Nicolas, et al. (2002), "Quantum cryptography", *Reviews of Modern Physics*. 74(1), pp. 145-195.

31. Grosshans, Frédéric and Grangier, Philippe (2002), "Continuous Variable Quantum Cryptography Using Coherent States", *Physical Review Letters*. 88(5), p. 057902.
32. Guo, Ying, et al. (2017), "Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction", *Physical Review A*. 95(3), p. 032304.
33. Haitjema, Mart (2007), A Survey of the Prominent Quantum Key Distribution Protocols, [Online] Available at: Quantum Key Distribution - QKD (wustl.edu)
34. Hemmati, Hamid (2020), *Near-earth laser communications*, CRC Press, 466.
35. Huang, Peng, et al. (2013), "Performance improvement of continuous-variable quantum key distribution via photon subtraction", *Physical Review A*. 87(1), p. 012317.
36. Ikuta, Takuya and Inoue, Kyo (2016), "Intensity modulation and direct detection quantum key distribution based on quantum noise", *New Journal of Physics*. 18(1), p. 013018.
37. ITU (March 2020), *XSTR-SEC-QKD Security considerations for quantum key distribution network*. [Online] Available at: ITU-T Rec. Technical Report Corrigendum 1 (04/2021) XSTR-SEC-QKD Security considerations for quantum key distribution network Corrigendum 1
38. J.A López-Leyva, A. Arvizu-Mondragon, J. Santos-Aguilar,R. Ramos-Garcia (2017), "Improved performance of the cryptographic key distillation protocol of an FSO/CV-QKD system on a turbulent channel using an adaptive LDPC encoder", *Revista Mexicana de Física* 63, pp. 268-274.
39. Josue, A. Lopez-Leyva, et al. (2019), "FSO/CV-QKD/QBaudSK system based on 2PolSK-BPSK scheme considering dynamical atmospheric conditions", *Proc.SPIE*.

40. Josue Aaron Lopez-Leyva, Ariana Talamantes-Alvarez, Miguel A. Ponce-Camacho, Edith Garcia-Cardenas and Eduardo Alvarez-Guzman (November 5th, 2018), *Quantum Cryptography in Advanced Networks*, Intechopen, 72.
41. Juan Yin, Yuan Cao, Shu-Bin Liu, Ge-Sheng Pan, Jin-Hong Wang, Tao Yang, Zhong-Ping Zhang, Fu-Min Yang, Yu-Ao Chen, Cheng-Zhi Peng, and Jian-Wei Pan (2013), "Experimental quasi-single-photon transmission from satellite to earth", *Opt. Express*. 21(20032-20040).
42. Jurado-Navas, Antonio, et al. (2017), "Fade statistics of turbulent optical links", *EURASIP Journal on Wireless Communications and Networking*. 2017(1), p. 112.
43. Karp S., Gagliardi R. M., Moran S. E., and Stotts L. B. (1988), *Optical Channels: fibers, clouds, water and the atmosphere*, Plenum Press, New York.
44. Kashif, H., Khan, M. N., and Altalbe, A. (2020), "Hybrid Optical-Radio Transmission System Link Quality: Link Budget Analysis", *IEEE Access*. 8, pp. 65983-65992.
45. Kaushal, H. and Kaddoum, G. (2017), "Optical Communication in Space: Challenges and Mitigation Techniques", *IEEE Communications Surveys & Tutorials*. 19(1), pp. 57-96.
46. Khatri, Sumeet, et al. (2021), "Spooky action at a global distance: analysis of space-based entanglement distribution for the quantum internet", *npj Quantum Information*. 7(1), p. 4.
47. Kish, S. P., et al. (2020), "Feasibility assessment for practical continuous variable quantum key distribution over the satellite-to-Earth channel", *Quantum Engineering*. 2.
48. L, Ajay (May 2016), "Survey of Most Prominent Quantum Key Distribution Protocols", *International Research Journal of Engineering and Technology*. 03(05), pp. 1330-1333.

49. Leverrier, Anthony and Grangier, Philippe (2011), "Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation", *Physical Review A*. 83(4), p. 042312.
50. Li, Yin, et al. (2021), "Continuous-Variable Quantum Key Distribution Based on Heralded Hybrid Linear Amplifier with a Local Local Oscillator", *Entropy*. 23(11).
51. Li, Yong-Min, et al. (2017), "Continuous variable quantum key distribution", *Chinese Physics B*. 26(4), p. 040303.
52. Li, Zhengyu, et al. (2016), "Non-Gaussian postselection and virtual photon subtraction in continuous-variable quantum key distribution", *Physical Review A*. 93(1), p. 012310.
53. Liao, Sheng-Kai, et al. (2018), "Satellite-Relayed Intercontinental Quantum Network", *Physical Review Letters*. 120(3), p. 030501.
54. Lomonaco, Samuel J. (1999), "A quick glace at quantum cryptography", *Cryptologia*. 23(1), pp. 1-41.
55. Ma, Jing, et al. (2015), "Performance analysis of satellite-to-ground downlink coherent optical communications with spatial diversity over Gamma - Gamma atmospheric turbulence", *Applied Optics*. 54(25), pp. 7575-7585.
56. Manuel Erhard, et al. (2021), "How to choose the best QKD network technology: Three different satellite based scenarios compared", *International Conference on Space Optics*, https://doi.org/10.1117/12.2599218.
57. Mavroeidis, Vasileios, et al. (2018), "The Impact of Quantum Computing on Present Cryptography", *International Journal of Advanced Computer Science and applications*, 9(3), http://dx.doi.org/10.14569/IJACSA.2018.090354
58. Motlagh, A. C., et al. (2008), The effect of atmospheric turbulence on the performance of the free space optical communications, *2008 6th International Symposium on Communication Systems, Networks and Digital Signal Processing*, pp. 540-543.

59. Nadeem, F., et al. (2010), "Continental Fog Attenuation Empirical Relationship from Measured Visibility Data", *Radioengineering*. 19 (4), pp. 596-600.

60. Nguyen, H. V., et al. (2017), "Network Coding Aided Cooperative Quantum Key Distribution Over Free-Space Optical Channels", *IEEE Access*. 5, pp. 12301-12317.

61. Nor, N. A. M., et al. (2015), Investigation of moderate-to-strong turbulence effects on free space optics — A laboratory demonstration, *2015 13th International Conference on Telecommunications (ConTEL)*, pp. 1-5.

62. Oesterling, L., Hayford, D., and Friend, G. (2012), Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information, *2012 IEEE Conference on Technologies for Homeland Security (HST)*, pp. 156-161.

63. Pham, Hien T. and Dang, Ngoc T. (2017), "Performance improvement of spatial modulation-assisted FSO systems over Gamma---Gamma fading channels with geometric spreading", *Photonic Netw. Commun*. 34, pp. 213–220.

64. Pittaluga, Mirko (2021), *Quantum-encrypted information transmitted over fiber more than 600 kilometers long*, accessed, [Online] Available at: https://phys.org/news/2021-10-quantum-encrypted-transmitted-fiber-kilometers.html.

65. Popkin, Gabriel (2017), "China's quantum satellite achieves 'spooky action' at record distance". [Online] Available at: https://quantum.ustc.edu.cn/web/index.php/en/node/447

66. Pugh, C. J., et al. (2017), "Airborne demonstration of a quantum key distribution receiver payload", *2017 Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC)*, pp. 1-1.

67. Q. Xu, M. Sabban, P. Gallion and F. Mendieta, Quantum key distribution system using dual-threshold homodyne detection,, *2008 IEEE International Conference on Research, Innovation and Vision for the Future in Computing and Communication Technologies*, Ho Chi Minh City, pp. 1-8.

68. Rabinovich, William S., et al. (2018), "Free space quantum key distribution using modulating retro-reflectors", *Optics Express*. 26(9), pp. 11331-11351.

69. Renner, R. and Cirac, J. I. (2009), "de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography", *Physical Review Letters*. 102(11), p. 110504.

70. Rezai, M. and Salehi, J. A. (2021), "Quantum CDMA Communication Systems", *IEEE Transactions on Information Theory*. 67(8), pp. 5526-5547.

71. Salamah, Salem H., et al. (2018), "The Effects of Power Control on Free-Space Optical Communications during Snowfall and Rainfall", *International Journal of Communications, Network and System science*. 11, pp. 216-227.

72. Scarani, Valerio, et al. (2009), "The security of practical quantum key distribution", *Reviews of Modern Physics*. 81(3), pp. 1301-1350.

73. Shannon, Claude E. (1949), "Communication Theory of Secrecy Systems", *Bell System Technical Journal*.

74. Sharma, M., Chadha, D., and Chandra, V. (2016), "High-altitude platform for free-space optical communication: Performance evaluation and reliability analysis", *Journal of Optical Communications and Networking*. 8(8), pp. 600-609.

75. Sharma, Vishal and Banerjee, Subhashish (2020), "Quantum communication using code division multiple access network", *Optical and Quantum Electronics*. 52(8), p. 381.

76. Shen, H., Cai, L., and Shen, X. (2006), "Performance analysis of TFRC over wireless link with truncated link-level ARQ", *IEEE Transactions on Wireless Communications*. 5(6), pp. 1479-1487.

77. Shor, P. W. (1994), Algorithms for quantum computation: discrete logarithms and factoring, *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 124-134.

78. Shor, Peter W. (1997), "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", *SIAM Journal on Computing*. 26(5), pp. 1484-1509.

79. Singh, H., et al. (2021), "Design and Analysis of High-Speed Free Space Optical (FSO) Communication System for Supporting Fifth Generation (5G) Data Services in Diverse Geographical Locations of India", *IEEE Photonics Journal*. 13(5), pp. 1-12.

80. Sun, Xiaole, Djordjevic, Ivan B., and Neifeld, Mark A. (2016), "Multiple spatial modes based QKD over marine free-space optical channels in the presence of atmospheric turbulence", *Optics Express*. 24(24), pp. 27663-27673.

81. Suriza, A. Z., et al. (2013), "Proposed parameters of specific rain attenuation prediction for Free Space Optics link operating in tropical region", *Journal of Atmospheric and Solar-Terrestrial Physics*. 94, pp. 93-99.

82. Takenaka, Hideki, et al. (2017), "Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite", *Nature*. 11(8), pp. 502-508.

83. Toyoshima, Morio, et al. (2012), "Results of Kirari optical communication demonstration experiments with NICT optical ground station (KODEN) aiming for future classical and quantum communications in space", *Acta Astronautica*. 74, pp. 40-49.

84. Trinh, P. V. and Pham, A. T. (2017), Design and secrecy performance of novel two-way free-space QKD protocol using standard FSO systems, *2017 IEEE International Conference on Communications (ICC)*, pp. 1-6.

85. Trinh, P. V., et al. (2018), "Design and Security Analysis of Quantum Key Distribution Protocol Over Free-Space Optics Using Dual-Threshold Direct-Detection Receiver", *IEEE Access*. 6, pp. 4159-4175.

86. Truong, L. D., et al. (2017), "Topology design and cross-layer optimization for FSO mesh networks impaired by atmospheric turbulence and misalignment fading", *Journal of Optical Communications and Networking*. 9(12), pp. 1097-1107.

87. Usenko, Vladyslav C. and Filip, Radim (2016), "Trusted Noise in Continuous-Variable Quantum Key Distribution: A Threat and a Defense", *Entropy*. 18(1).

88. Usenko, Vladyslav C. and Grosshans, Frédéric (2015), "Unidimensional continuous-variable quantum key distribution", *Physical Review A*. 92(6), p. 062337.

89. Vallone, Giuseppe, et al. (2015), "Experimental Satellite Quantum Communications", *Physical Review Letters*. 115(4), p. 040502.

90. Vavoulas, Alexander, Sandalidis, Harilaos G, and Varoutas, Dimitris (2012), "Weather Effects on FSO Network Connectivity", *Journal of Optical Communications and Networking*. 4(10), pp. 734-740.

91. Villoresi, Paolo, et al. (2008), "Experimental verification of the feasibility of a quantum channel between space and Earth", *New Journal of Physics*. 10, p. 033038.

92. Vu, Minh Q., et al. (2018), "Performance enhancement of LEO-to-ground FSO systems using All-optical HAP-based relaying", *Physical Communication*. 31, pp. 218-229.

93. Vu, Minh Quang, Dang, Ngoc T., and Pham, Anh Tuan IEEE 89th Vehicular Technology Conference (2019), "HAP-Aided Relaying Satellite FSO/QKD Systems for Secure Vehicular Networks", pp. 1-6.

94. Wang, Chao, et al. (2016), "Practical security of continuous-variable quantum key distribution with finite sampling bandwidth effects", *Physical Review A*. 93(2), p. 022315.

95. Wang, Shiyu, et al. (2020), "Phase compensation for free-space continuous-variable quantum key distribution", *Optics Express*. 28(8), pp. 10737-10745.
96. Wang, Xu-Yang, et al. (2013), "Four-State Modulation Continuous Variable Quantum Key Distribution over a 30-km Fiber and Analysis of Excess Noise", *Chinese Physics Letters*. 30(1), p. 010305.
97. Wang, Xuyang, et al. (2017), "Experimental study on all-fiber-based unidimensional continuous-variable quantum key distribution", *Physical Review A*. 95(6), p. 062330.
98. X.Ai, R.Malane and S.X.Ng (2020), "A recoiliation strategy for real-time satellite-base QKD", *IEEE Wireless Commun. Lett.* 24, p. 5.
99. Xu, Q., et al. (2008), Quantum key distribution system using dual-threshold homodyne detection, *2008 IEEE International Conference on Research, Innovation and Vision for the Future in Computing and Communication Technologies*, pp. 1-8.
100. Yin, Juan, et al. (2017), "Satellite-based entanglement distribution over 1200 kilometers", *Science*. 356(6343), pp. 1140-1144.
101. Yoshino, Ken-ichiro, et al. (2012), "High-speed wavelength-division multiplexing quantum key distribution system", *Optics Letters*. 37(2), pp. 223-225.
102. Zhang, Jianguo, Sharma, A. B., and Kwong, Wing C. (2000), "Cross-correlation and system performance of modified prime codes for all-optical CDMA applications", *Journal of Optics*. 2(5), pp. L25-L29.
103. Zhang, Yi-Chen, et al. (2014), "Improvement of two-way continuous-variable quantum key distribution using optical amplifiers", *Journal of Physics B: Atomic, Molecular and Optical Physics*. 47(3), p. 035501.
104. Zhang, Yichen, et al. (2015), "Noiseless Linear Amplifiers in Entanglement-Based Continuous-Variable Quantum Key Distribution", *Entropy*. 17(7).
105. Zhao, Wei, et al. (2018), "Performance analysis of the satellite-to-ground continuous-variable quantum key distribution with orthogonal frequency

division multiplexed modulation", *Quantum Information Processing*. 18(1), p. 39.