MỘT GIẢI PHÁP TĂNG DUNG LƯỢNG HỆ THỐNG PHÂN PHỐI KHÓA LƯỢNG TỬ QUA HỆ THỐNG LAI GHÉP QUANG VÔ TUYẾN

Phạm Anh Thư
Học Viện Công Nghệ Bưu chính Viễn thông

Tóm tắt – Mô hình truyền khóa lượng tử trên hệ thống lai ghép quang vô tuyến được xem là một trong những giải pháp có nhiều ưu điểm như cung cấp khoảng cách truyền dẫn dài, mềm dẻo, linh động và dễ dàng mở rộng và do đó được các nhà nghiên cứu và triển khai quan tâm đặc biệt trong những năm gần đây. Tuy nhiên, hiệu năng về mặt dung lượng hệ thống vẫn còn là một vấn đề cần được xem xét và cải thiện. Trong bài báo này, chúng tôi đề xuất một giải pháp cải thiện dung lượng của hệ thống phân phối khóa lượng tử qua hệ thống lai ghép quang vô tuyến, đó là sử dụng sợi quang đa lõi (MCF). Khóa lượng tử từ bên gửi (Alice) được truyền qua sợi quang đa lõi tới trạm trung gian (BS) và sau đó được chuyển tiếp tới các trạm di động (Bob) qua kênh vô tuyến. Giao thức QKD được thực thi bằng cách dựa trên điều chế cường độ sóng mang con sử dụng khóa dịch pha nhị phân, và bộ thu hai ngưỡng được sử dụng để giải mã. Hiệu năng hệ thống về mặt tỉ lệ lỗi bit lượng tử và tốc độ khóa bí mật của hệ thống được phân tích dưới ảnh hưởng của rất nhiều các tham số lớp vật lý đến từ bộ thu, phần mạng quang và kênh vô tuyến. Các tham số này bao gồm suy hao kênh vô tuyến, suy hao kênh quang, xuyên nhiễu trong sợi MCF và nhiễu bộ thu. Ngoài ra, bài báo còn xét đến hiệu năng của hệ thống khi có mặt của kẻ tấn công (Eve). Tính khả thi của hệ thống QKD đề xuất được thể hiện trong các kết quả của bài báo này.

Từ khóa – Phân phối khóa lượng tử (QKD), sợi quang đa lõi (MCF), điều chế cường độ sóng mang con (SIM), tỉ lệ lỗi bit lượng tử (QBER).

I. GIỚI THIỆU CHUNG

Trong kỉ nguyên số, khi mà lưu lượng dữ liệu đang tăng lên một cách nhanh chóng trên toàn cầu, khối dữ liệu lớn, còn được gọi là dữ liệu thô, đang đứng trước rất nhiều nguy cơ bảo mật. Vấn đề an toàn của việc gửi giữ liệu giữa các hệ thống mạng phụ thuộc vào các cơ chế bảo vệ. Mặc dù, có rất nhiều các cơ chế bảo mật thông tin đã được sử dụng cho các hệ thống mạng khác nhau, một yêu cầu bắt buộc với các cơ chế này đó là an toàn khóa phải được bảo mật cao bởi nó ảnh hưởng trực tiếp tới hoạt động an toàn của các hệ thống mạng.

Tác giả liên hệ: Phạm Anh Thư,
Email: thupa@ptit.edu.vn
Đến tòa soạn: 10/2023, chỉnh sửa: 11/2023, chấp nhận đăng: 12/2023.

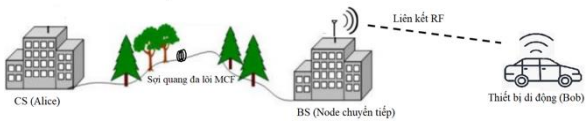
Như một phương pháp mới đảm bảo việc truyền dẫn an toàn thông tin, công nghệ phân phối khóa lượng tử QKD cung cấp giải pháp an toàn cao cho việc chia sẻ các khóa bí mật giữa các bên gửi (Alice) và bên nhận (Bob), dưới sự có mặt của kẻ tấn công (Eve), kẻ mong muốn lấy được khoá để phá mã hệ thống, đã thu hút được rất nhiều các nhà nghiên cứu và triển khai mạng trên thế giới. Hơn thế, công nghệ này còn được thử nghiệm thành công trong rất nhiều lĩnh vực. Việc bảo mật các khóa được phân phối bằng cách sử dụng QKD dựa trên các luật lượng tử và có thể được thực thi đơn giản bởi sử dụng các trạng thái pha hoặc phân cực của các photon đơn, còn được gọi là QKD biến rời rạc (DV-QKD). Sơ đồ sử dụng DV-QKD có thể được triển khai để phân phối các khóa một cách an toàn giữa các nút hợp pháp. Tuy nhiên, phương pháp tiếp cận này có một số hạn chế như khoảng cách truyền dẫn bị hạn chế và tốc độ khóa bí mật thấp. Hơn nữa, các công nghệ được sử dụng trong các hệ thống DV-QKD khá khác với các công nghệ được sử dụng trong các hệ thống truyền thông truyền thống. Để khắc phục các nhược điểm này, hệ thống CV-QKD với các ưu điểm như khả năng đạt được tốc độ phân phối khóa bí mật cao đã được quan tâm một cách đặc biệt. Ngoài ra, so với hệ thống DV-QKD, hệ thống CV-QKD có thể tận dụng được các công nghệ đang sử dụng trong các mạng viễn thông truyền thống.

Gần đây, các công nghệ ghép kênh như WDM, ghép kênh phân chia theo pha và phân cực đã được đề xuất triển khai trong các hệ thống CV-QKD để nâng cao hiệu năng của các hệ thống này [1-3]. Tuy nhiên, các công nghệ ghép kênh này yêu cầu các thiết bị phức tạp chứ không phải thiết bị thương mại và tốc độ khóa bí mật của các hệ thống này cũng vẫn thấp hơn nhiều so với yêu cầu của các hệ thống thực tế. Trong mấy năm gần đây, công nghệ ghép phân chia theo không gian (SDM) sử dụng nhiều kênh không gian để tăng dung lượng hệ thống đã được đề xuất để đáp ứng được nhu cầu lưu lượng lớn [4-6]. Một cách tiếp cận thực tế của công nghệ SDM là sử dụng sợi quang đa lõi (MCF) gồm nhiều lõi sợi quang được sử dụng làm các kênh song song để truyền các tín hiệu một cách độc lập. Sợi MCF hoàn toàn có thể được sử dụng như là môi trường truyền dẫn để tăng dung lượng của hệ thống QKD, và khắc phục được tốc độ khóa bí mật thấp trong các hệ thống dựa trên sợi quang đơn mode truyền thống [7-9].

Cho đến nay, một số các kịch bản thử nghiệm liên quan đến việc sử dụng sợi MCF cho hệ thống CV-QKD đã được công bố. Trong [10], các tác giả đã đề xuất một hệ

thống truyền đồng thời tín hiệu khóa và dữ liệu qua cùng sợi đa lõi. Hệ thống này đã được thử nghiệm một cách thành công. Các kết quả trong đề xuất chỉ ra rằng có sự suy giảm nhẹ về hiệu năng của hệ thống. Tuy nhiên, phương pháp để tăng được tốc độ khóa bí mật lại không được đề cập đến trong hệ thống này. Gần đây hơn, một thử nghiệm về hệ thống CV-QKD sử dụng sợi MCF [11] đã được báo cáo. Trong báo cáo này, các nhà nghiên cứu đã đề xuất hệ thống CV-QKD dựa trên sợi MCF để tăng tốc độ khóa bí mật. Các kết quả trong [11] chỉ ra rằng có sự suy giảm hiệu năng hệ thống do suy hao của thiết bị FIFO. Hơn nữa, tổng tốc độ khóa bí mật có thể được cải thiện một cách rõ ràng. Tuy nhiên, các bước sóng phân bố cho mỗi kênh lượng tử trong mỗi lõi MCF là khác nhau và do đó ảnh hưởng của nhiễu xuyên kênh của sợi MCF chưa được xem xét.

Trong bài báo này, mô hình truyền khóa lượng tử trên hệ thống lai ghép quang sử dụng sợi đa lõi MCF và vô tuyến (RoMCF/QKD) được đề xuất. Ưu điểm của kiến trúc đề xuất này là có thể cung cấp khoảng cách truyền dẫn dài hơn, mềm hẻo hơn và có khả năng mở rộng. Hệ thống phân phối khóa QKD đề xuất có thể được ứng dụng cho các mạng di động trong việc phân phối khóa bí mật từ các trạm trung tâm (CS) tới các nút di động (MN) trong đó BS sẽ đóng vai trò là nút chuyển tiếp. Sợi đa lõi trong mô hình này được sử dụng để kết nối CS và BS trong khi giữa BS và MN là các liên kết vô tuyến RF ở băng sóng MMW (Hình 1). Hiệu năng về tỉ lệ lỗi bit lượng tử (*QBER*) và tốc độ khóa bí mật (*SKR*) của hệ thống RoMCF/QKD đề xuất được phân tích dưới ảnh hưởng của rất nhiều các tham số lớp vật lý đến từ bộ thu, xuyên nhiễu trong sợi MCF và kênh vô tuyến.



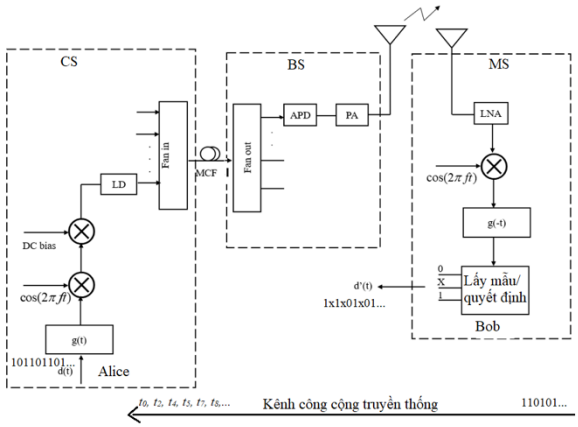
Hình 1 Mô hình phân phối khóa lượng tử QKD trên hệ thống lai ghép quang vô tuyến (RoMCF/QKD)

Phần còn lại của bài báo được bố cục như sau. Mô hình hệ thống đề xuất được giới thiệu trong phần 2. Trong phần 3, hiệu năng của hệ thống về mặt tỉ lệ lỗi bit lượng tử và tốc độ khóa bí mật sẽ được phân tích. Phần 4 chỉ ra các kết quả mô phỏng số và các đánh giá về các kết quả này. Cuối cùng, phần 5 sẽ là phần kết luận của bài báo.

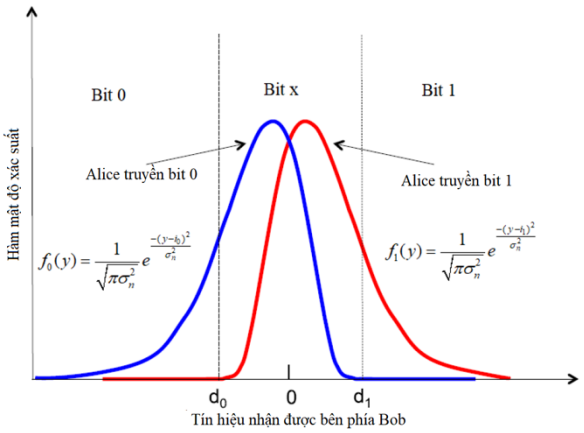
II. MÔ HÌNH HỆ THỐNG

Sơ đồ khối của hệ thống RoMCF/QKD đề xuất được chỉ ra trong hình 2. Hệ thống đề xuất bao gồm ba phần chính, bên gửi khóa (bên Alice), trạm chuyển tiếp khóa (BS) và bên nhận khóa (bên Bob) sẽ nhận tín hiệu khóa và khôi phục khóa ban đầu được truyền đi từ Alice. Giao thức QKD được thực thi trong mô hình đề xuất được dựa trên điều chế sóng mang con SIM sử dụng khóa dịch pha nhị phân (SIM-BPSK).

Như chỉ ra trong hình 2, tại bộ phát của Alice, các bit nhị phân của khóa d(t) được chuyển sang hàm dạng xung chữ nhật (*g(t)*) và được điều chế lên sóng mang con RF sử dụng điều chế BPSK, trong đó bit "0" và "1" được biểu diễn bằng hai pha cách nhau 180 độ. Tiếp theo, tín hiệu BPSK, bao gồm cả giá trị âm và dương, được cộng thêm dòng định thiên DC vào trước khi điều chế với sóng quang liên tục được tạo ra bởi LD. LD chỉ có thể được điều chế bởi các tín hiệu dương nên tín hiệu BPSK phải cộng thêm với dòng DC trước khi đưa vào điều chế. Sau đó, tín hiệu quang từ mỗi LD được ghép vào một lõi xác định của sợi quang đa lõi có *W* lõi với chiều dài sợi là *L* bằng cách sử dụng thiết bị FAN-IN, và sau đó được truyền qua sợi đa lõi tới trạm chuyển tiếp BS. Khi tín hiệu tới BS, tín hiệu thu được trước tiên được tách ra khỏi sợi MCF nhờ thiết bị FAN-OUT và được chuyển tới bộ tách sóng APD để chuyển đổi thành tín hiệu điện. Sau đó, tín hiệu điện được khuếch đại bởi bộ khuếch đại PA rồi gửi tới anten phát để phát đến bên thu Bob. Tại phía thu Bob, tín hiệu điện thu được được chuyển qua bộ khuếch đại tạp âm thấp LNA, sau đó được giải điều chế bằng cách nhân với tín hiệu đến từ bộ dao động nội có tần số là tần số của sóng mang con vô tuyến.



Hình 2. Hệ thống RoFSK/QKD lai ghép sử dụng SIM-BPSK và bộ thu DT.



Hình 3: Tách sóng hai ngưỡng tại phía Bob

Sau khi giải mã, tín hiệu điện được qua bộ chỉnh xung (*g(-t)*), lấy mẫu và được quyết định là các bit "0", "1", hay "x" dựa trên bộ tách sóng hai ngưỡng (DT). Như chỉ ra trong hình 3, hai mức ngưỡng d_0 và d_1, được thiết lập tại phía Bob cho việc tách sóng tín hiệu. Nếu dòng tín hiệu nhận được nhỏ hơn d_0, bit "0" sẽ được quyết định. Nếu dòng tín hiệu nhận được lớn hơn d_1, bit "1" sẽ được quyết định. Trường hợp còn lại, bit "x" (không bit nào) được tạo ra [13].

Cuối cùng, Bob thông báo cho Alice biết các thời điểm mà các bit "0" và "1" được tạo ra qua kênh công khai truyền thống. Sau đó Alice loại bỏ các giá trị bit tại thời điểm mà Bob không tạo ra bit. Từ đây, Alice và Bob chia

sẻ một chuỗi bit giống hệt nhau, gọi là khóa chọn lọc. Bằng cách thu ước lượng CSI tại máy thu, d_0 và d_1 có thể được điều chỉnh, do đó xác suất chọn lọc tại máy thu của Bob có thể được điều khiển.

III. HIỆU NĂNG CỦA HỆ THỐNG ĐỀ XUẤT

Trong phần này, dòng tín hiệu và nhiễu tại phía thu của Bod được tính toán trước. Sau đó, hiệu năng của hệ thống về mặt tỉ lệ lỗi bít lượng tử (*QBER*) được tính dựa trên xác suất lỗi và số bit khóa được sử dụng. Hơn nữa, tốc độ khóa bí mật cũng sẽ được xem xét trong phần này.

A. Hiệu năng hệ thống

Như chỉ ra trong mô hình hệ thống đề xuất (Hình 2), các bit khóa, chuỗi các bit nhị phân ngẫu nhiên "0" hoặc "1", được điều chế BPSK với sóng mang, sau đó được biến đổi thành tín hiệu quang nhờ điều chế cường độ với độ sâu điều chế nhỏ. Công suất thu được của chùm laser được điều chế có thể biểu diễn như sau

$$P_t(t) = \frac{P_0}{2}\left[1 + mS(t)\right] \qquad (1)$$

Trong đó, P_0 là công suất phát đỉnh, m là độ sâu điều chế cường độ với $0 < m < 1$. $S_t(t) = A(t)g(t)\cos(2\pi f_c t + a_i\pi)$, trong đó $A(i)$ biên độ sóng mang, $g(t)$ hàm tạo xung chữ nhật, f_c là tần số sóng mang, và $a_i \in \{0,1\}$ là bit nhị phân thứ i. Giả thiết công suất $S(t)$ được chuẩn hóa thành đơn vị cho việc phân tích đơn giản hơn.

Tín hiệu quang được điều chế sau mỗi LD được ghép vào một lõi cụ thể trong sợi quang đa lõi gồm W lõi bằng cách sử dụng thiết bị FAN-IN có xuyễn nhiễu thấp và suy hao thấp. Các tín hiệu quang sau đó được truyền qua sợi quang MCF có W lõi và chiều dài L tới trạm chuyển tiếp BS nơi có thiết bị FAN-OUT được sử dụng để tách các tín hiệu quang khỏi sợi đa lõi.

Tại BS, tín hiệu quang thu tại đầu ra của thiết bị FAN-OUT sẽ được chuyển qua bộ lọc thông dải quang (OBPF) để giảm nhiễu nền. Sau đó, tín hiệu quang đã lọc được biến đổi ngược lại thành tín hiệu điện nhờ bộ tách sóng APD. Dòng tín hiệu điện sau APD có thể được mô tả như sau

$$i_p(t) = \Re M_A \frac{\sqrt{P_{or}^{BS}}}{2}\left[1 + mS(t)\right] + n_{BS}(t), \qquad (2)$$

Trong đó, $\Re$ và M_A là đáp ứng và hệ số khuếch đại của APD, tương ứng, $n_{rB(t)}$ là dòng nhiễu tại bộ thu BS. P_{or}^{BS} là công suất thu đỉnh tại BS được tính bởi

$$P_{or}^{BS} = P_o \exp(\alpha L), \qquad (3)$$

trong đó α là hệ số suy hao của sợi quang và L là chiều dài của sợi quang đa lõi.

Khi truyền qua sợi quang MCF, tín hiệu quang trên mỗi lõi chịu nhiễu xuyên lõi (*XT*) gây ra bởi các lõi kế cận. Để đơn giản, chúng tôi giả thiết sợi quang MCF là đồng nhất (nghĩa là tất cả các lõi có cùng kích thước và chỉ số khúc xạ). Xét 1 lõi bất kỳ (giả sử lõi i), xuyên nhiễu giữa hai lõi là tỉ số công suất đầu ra trong lõi i ghép từ lõi j trên công suất đầu ra của lõi xuyên nhiễu j [14]. Vì vậy, xuyên nhiễu giữa lõi i và j trong sợi MCF được tính như sau [14]:

$$XT_{ij} = \frac{2\kappa^2 R_{bd}}{\beta \Lambda_{ij}} L, \qquad (4)$$

trong đó Λ_{ij} là khoảng cách giữa hai lõi (core pitch), R_{bd} là bán kính uốn cong, β là hằng số truyền, κ là hệ số ghép mode.

Trong sợi MCF W lõi đồng nhất, các lõi sợi được sắp xếp theo hình vòng. Tổng xuyên nhiễu trong mỗi lõi là như nhau và được tính như sau:

$$P_{XT} = \sum_{\substack{j=1 \\ j\neq i}}^{W} P_{ij} = \sum_{\substack{j=1 \\ j\neq i}}^{W} XT_{ij} P_{or}^{BS}, \qquad (5)$$

Tín hiệu quang đầu ra mỗi lõi được biến đổi thành tín hiệu điện. Bên cạnh các dòng tín hiệu điện này, có dòng nhiễu xuất hiện tại đầu ra APD. Dòng nhiễu này bao gồm các nhiễu thành phần, giả sử có cùng phân bố Gaussian, là nhiễu nổ, nhiễu nhiệt, nhiễu xuyên kênh và nhiễu phách (beat noise) gây ra giữa tín hiệu mong muốn và nhiễu xuyên kênh. Kết quả là, tổng công suất nhiễu sau mỗi APD có thể được biểu diễn như sau:

$$\sigma_{BS}^2 = \sigma_s^2 + \sigma_{XT}^2 + \sigma_{sig-XT}^2 + \sigma_{th}^2 + \sigma_{ASE}^2 + \sigma_{sig-ASE}^2 + \sigma_{XT-ASE}^2, \qquad (6)$$

trong đó, σ_s^2, σ_{XT}^2, σ_{sig-XT}^2, σ_{th}^2 là công suất nhiễu nổ, xuyên nhiễu, nhiễu phách và nhiễu nhiệt, tương ứng. Các thành phần nhiễu này được tính cụ thể như sau:

$$\sigma_s^2 = 2qM^2 F_A B(\Re P_{or} + I_d + \Re P_{XT} + \Re P_{ASE}), \qquad (7)$$

$$\sigma_{XT}^2 = (\Re P_{XT})^2, \qquad (8)$$

$$\sigma_{sig-XT}^2 = 4\Re^2 P_{or} P_{XT} \cos^2 \beta L, \qquad (9)$$

$$\sigma_{th}^2 = \frac{4K_B T}{R_L} B, \qquad (10)$$

$$\sigma_{sig-ASE}^2 = 2\Re^2 P_{or}\left[n_{sp}(M-1)hf_0 B_0\right], \qquad (11)$$

$$\sigma_{XT-ASE}^2 = 2\Re^2 P_{XT}\left[n_{sp}(M-1)hf_0 B_0\right], \qquad (12)$$

trong đó, q là điện tích electron, B là băng tần nhiễu hiệu dụng, I_d là dòng tối, K_B là hằng số Boltzmann, T là nhiệt độ máy thu, R_L là điện trở tải. B_0, n_{sp}, h, f_0 là băng tần của tín hiệu quang, hệ số phát xạ tự phát, hằng số plank và tần số của sóng ánh sáng tương ứng. F_A là hệ số nhiễu trội của APD. F_A được tính như sau [19]

$$F_A(M_A) = k_A M_A + (1-k_A)(2 - 1/M_A), \qquad (13)$$

Trong đó, k_A là tỉ lệ ion hóa.

Sau đó, tín hiệu RF từ BS được truyền tới bên phía thu của Bob, tại đây tín hiệu BPSK được giải điều chế bằng cách trộn với tín hiệu từ bộ dao động nội có dạng $\cos(2\pi f_c t)$. Dòng tín hiệu sau giải điều chế có thể được biểu diễn là

$$i_d(t) = i_p(t)\sqrt{h_w}\cos(2\pi f_c t) + n_{MN}(t), \qquad (14)$$

Trong đó, $h_w = G_{Tx}G_{Rx}/P_L$ là hệ số kênh của kênh vô tuyến với G_{Tx} và G_{Rx} là hệ số khuếch đại của anten phát và thu; P_L là tổng suy hao của liên kết vô tuyến. Tổng suy hao này được tính theo đơn vị dB bởi $P_L = 20\log(4\pi f_c d/c) + \gamma d$, trong đó d là khoảng cách liên kết vô tuyến và γ là hệ số suy hao tổng. $n_{MN}(t)$ là nhiễu tại bộ thu có biến thiên là $\sigma^2_{MN} = KTB_n/R_L$. Bằng

cách sử dụng bộ lọc thông thấp để loại bỏ các thành phần tần số cao như f_c hay $2f_c$, tín hiệu băng gốc có thể thu được tại đầu ra của bộ lọc LPF được xác định bởi

$$r(t)=\begin{cases} i_0 = -\frac{1}{4}\Re M_A\sqrt{P_{or}^{BS}}\,m\sqrt{h_w}+n_{BS}(t)\sqrt{h_w}+n_{MN}(t) \\ i_1 = +\frac{1}{4}\Re M_A\sqrt{P_{or}^{BS}}\,m\sqrt{h_w}+n_{BS}(t)\sqrt{h_w}+n_{MN}(t) \end{cases}, \quad (15)$$

Trong đó, i_0 và i_1 là tín hiệu nhận được tương ứng với bit "0" và "1". Tổng biến thiên nhiễu được tính như sau $\sigma_n^2=\sigma_{BS}^2h_w+\sigma_{MN}^2$. Tiếp theo, tín hiệu sau giải điều chế được chuyển tới bộ tách sóng hai ngưỡng để quyết định bit nào nhận được "0", "1", hay "x" như chỉ ra trong hình 3.

B. Tỉ lệ lỗi bit lượng tử

Tỉ lệ lỗi bít lượng tử được định nghĩa là tỉ số xác suất mà Bob phát hiện sai bit "0" và "1" (P_{err}) trên xác suất mà Bob có thể quyết định các bit nhận được là "0" và "1" (P_{sift}) [20]. Theo đó, *QBER* có thể được biểu diễn như sau

$$\mathrm{QBER}=\frac{P_{err}}{P_{sift}}, \quad (16)$$

Trong đó, P_{err} và P_{sift} được tính như sau

$$\begin{aligned} P_{err} &= P_{A,B}(0,1)+P_{A,B}(1,0) \\ P_{sift} &= P_{A,B}(0,0)+P_{A,B}(0,1)+P_{A,B}(1,0)+P_{A,B}(1,1) \end{aligned}, \quad (17)$$

Trong đó, $P_{A,B}(\mathrm{i},\mathrm{j})$ là xác suất mà tại 1 thời điểm bit ở bên Alice là "*i*" nhưng bit bên Bob là "*j*". Xác suất này có thể được tính như là $P_{A,B}(\mathrm{i},\mathrm{j})=P_A(i)P_{(B/A)}(j|i)$, trong đó $P_A(i)=1/2$ và $P_{(B/A)}(j|i)$ là xác suất mà Bob nhận được bit "*j*" trong khi Alice gửi đi bit "*i*". Dựa trên nguyên lý tách sóng hai ngưỡng, xác suất của $P_{(B/A)}(j|i)$ có thể được mô tả gần đúng như sau:

$$\begin{aligned} P_{B|A}(0|0) &= \frac{1}{\sigma_n\sqrt{2\pi}}\int_{-\infty}^{d_0}\exp\left(-\frac{(y-i_0)^2}{2\sigma_n^2}\right)dy=\frac{1}{2}\mathrm{erfc}\left(\frac{i_0-d_0}{\sigma_n\sqrt{2}}\right) \\ P_{B|A}(0|1) &= \frac{1}{\sigma_n\sqrt{2\pi}}\int_{-\infty}^{d_0}\exp\left(-\frac{(y-i_1)^2}{2\sigma_n^2}\right)dy=\frac{1}{2}\mathrm{erfc}\left(\frac{i_1-d_0}{\sigma_n\sqrt{2}}\right) \\ P_{B|A}(1|0) &= \frac{1}{\sigma_n\sqrt{2\pi}}\int_{d_1}^{\infty}\exp\left(-\frac{(y-i_0)^2}{2\sigma_n^2}\right)dy=\frac{1}{2}\mathrm{erfc}\left(\frac{d_1-i_0}{\sigma_n\sqrt{2}}\right) \\ P_{B|A}(1|1) &= \frac{1}{\sigma_n\sqrt{2\pi}}\int_{-\infty}^{d_0}\exp\left(-\frac{(y-i_1)^2}{2\sigma_n^2}\right)dy=\frac{1}{2}\mathrm{erfc}\left(\frac{d_1-i_1}{\sigma_n\sqrt{2}}\right) \end{aligned}, \quad (18)$$

Để điều chỉnh được giá trị của hai ngưỡng tách sóng, hệ số *k* được thêm vào và hai giá trị ngưỡng được định nghĩa như sau

$$\begin{aligned} d_0 &= E[i_0]-k\sqrt{\sigma_n^2} \\ d_1 &= E[i_1]+k\sqrt{\sigma_n^2} \end{aligned}, \quad (19)$$

Trong đó $E[i_0]$ và $E[i_1]$ là giá trị trung bình của i_0 và i_1.

C. Tốc độ khóa bí mật

Tốc độ khóa bí mật Egodic, 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 Eva không thể giải mã bất kỳ thông tin nào, được tính như sau

$$S=I(A;B)-I(A;E), \quad (20)$$

Trong đó, $I(A;B)$ và $I(A;E)$ là lượng thông tin chia sẻ giữa Alice và Bob, và giữa Alice và Eve tương ứng. Với giả thiết rằng xác suất truyền bit "0" và "1" là xảy ra bằng nhau, thông tin chia sẻ giữa Alice và Bob có thể được tính như sau [20]

$$\begin{aligned} I(A;B) = {} & p\log_2(p)+(1-p-q)\log_2(1-p-q) \\ & -(1-q)\log_2(1-q)+1-q \end{aligned}, \quad (21)$$

Trong đó, $p = P_{A,B}(0,0) = P_{A,B}(1,1)$ and $q = P_{A,B}(0,x) = P_{A,B}(1,x) = 0.5 - P_{A,B}(0,0) - P_{A,B}(0,1)$.

Thông tin chung giữa Alice và Eve có thể tính bằng [16]

$$I(A;E)=1+p_e\log_2(p_e)+(1-p_e)\log_2(1-p_e), \quad (22)$$

Trong đó, p_e là xác suất mà Eve phát hiện đúng các bit được truyền đi từ Alice, có thể được tính là $p_e = 0.5 - P_{A,E}(0,1) = 0.5 - P_{A,E}(1,0)$. Ngoài ra, xác suất lỗi của Eve được tính như sau

$$\mathrm{QBER}_{Eve}=P_{A,E}(0,1)+P_{A,E}(1,0), \quad (23)$$

Trong đó, $P_{A,E}(0,1)$ và $P_{A,E}(1,0)$ là xác suất lỗi mà Eve quyết định sai bit nhận được từ Alice. Giả sử rằng Eve sử dụng tách sóng đơn ngưỡng, đây là mô hình tách sóng thường dung cho máy thu quang. Xác suất lỗi có thể được tính như sau [21]

$$\begin{aligned} P_{A,E}(0,1) &= P_A(0)P_{E|A}(1|0)=\frac{1}{4}\mathrm{erfc}\left(\frac{d_E-i_0}{\sigma_n\sqrt{2}}\right) \\ P_{A,E}(1,0) &= P_A(1)P_{E|A}(0|1)=\frac{1}{4}\mathrm{erfc}\left(\frac{i_1-d_E}{\sigma_n\sqrt{2}}\right) \end{aligned}. \quad (24)$$

Trong đó $d_E = 0$ là ngưỡng tách sóng tại bộ thu của Eve (như hình 3).

IV. KẾT QUẢ MÔ PHỎNG SỐ

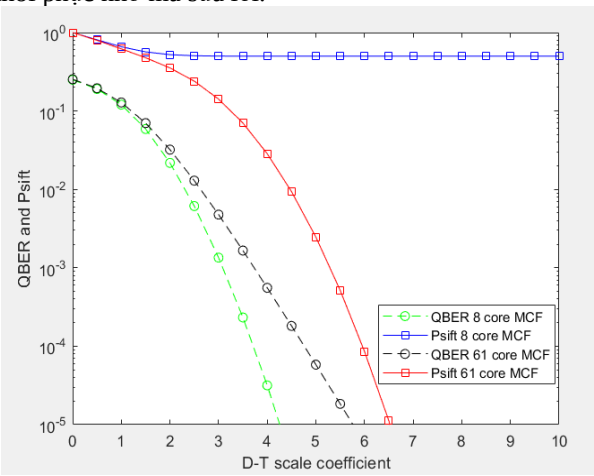
Trong phần này, các kết quả khảo sát hiệu năng hệ thống gồm *QBER* và *S* sẽ được trình bày dựa trên các công thức giải tích trong phần trên. QBER tại bộ thu của Bob và của Eve được xem xét phụ thuộc vào rất nhiều tham số của hệ thống như công suất phát quang (*Pt*) và hệ số ngưỡng D-T, core pitch, độ dài sợi quang MCF, khoảng cách vô tuyến đến Bob. Ngoài ra, QBER tại Eve cũng được xem xét để khẳng định độ an toàn của hệ thống. Các tham số và hằng số được liệt kê trong Bảng 1.

Bảng 1: Tham số hệ thống và hằng số

Tên tham số, hằng số	Ký hiệu	Giá trị
Các tham số và hằng số chung		
Hằng số Boltzmann	K	1.38×10^{-23}
Điện tích	q	$1.6\times 10^{-19}C$
Vận tốc ánh sáng	c	3×10^8 m/s
Khả năng chịu tải	R_L	$50\,\Omega$
Tốc độ bit	R_b	1 Gb/s
Nhiệt độ	T	300 K
Bước sóng	λ	1550 nm
Hệ số tạp âm	F_n	5 dB
Các thông số của bộ thu phát quang học		
Chỉ số điều chế	m	0.2 A/W

Suy hao sợi quang	α	0.2 dB/km
Đáp ứng PD	$\Re$	0.6 A/W
Tỷ lệ ion hoá	k_A	0.7
Băng thông FWHM của tia laser	$\Delta\upsilon_m$	12.75 MHz
Hệ số ghép mode	κ	0.02
Bán kính uốn	R_{bd}	0.1 m
Hằng số lan truyền	β	rad/micromet
Các tham số của RF		
Tần số RF	f_c	26GHz
Hệ số suy hao	γ	4dB/km
Hệ số khuếch đại anten phát	G_{Tx}	28 dB
Hệ số khuếch đại anten thu	G_{Rx}	28 dB

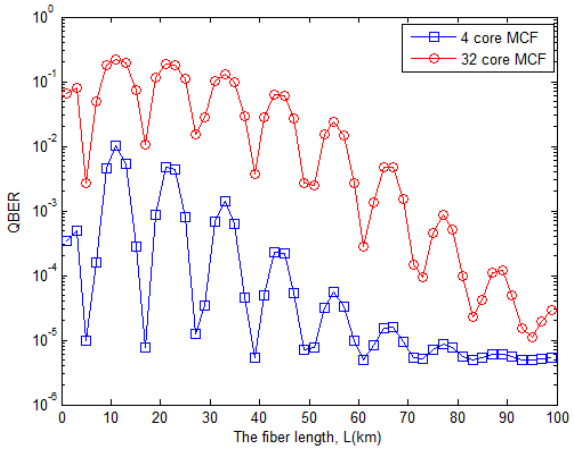
Hệ số ngưỡng là một trong những các thông số quan trọng nhất mà các nhà điều hành mạng cần xem xét khi thiết kế hệ thống. Do đó, trong hình 4 tỉ lệ lỗi bit lượng tử *QBER* và *Psift* được thể hiện là một hàm của hệ số ngưỡng tại máy thu của Bob. *Psift* phải lớn hơn hoặc bằng 10^{-2} để Bob có thể nhận được từ Alice với tốc độ Mbps khi tốc độ truyền đạt đến Gb/s. Ngoài ra, *QBER* được giữ ở mức thấp hơn hoặc bằng 10^{-3} để các lỗi bit có thể được khôi phục nhờ mã sửa lỗi.



Hình 4: QBER và Psift tại phía Bob phụ thuộc vào hệ số ngưỡng khi Pt = 5 dBm, L = 100 km, và dAB = 300m.

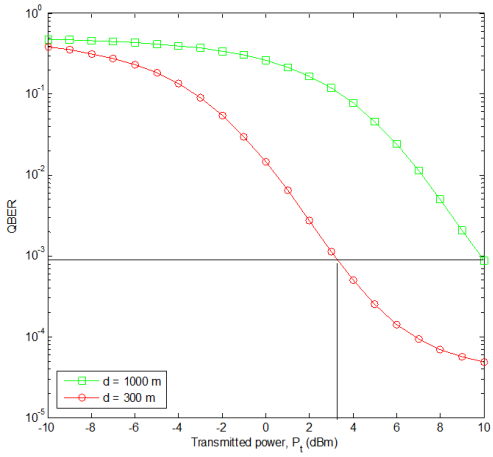
Như chỉ ra trong hình 4, để đáp ứng các yêu cầu nêu trên, hệ số ngưỡng D-T phải lớn hơn 3.2 trong trường hợp sử dụng 8 sợi đa lõi lõi, và trong phạm vi 4 và 5 trong trường hợp sử dụng sợi đa lõi 61 lõi. Sự khác biệt trong hệ số ngưỡng D-T là do nhiễu xuyên kênh lớn xảy ra trong sợi MCF 61 lõi.

Tiếp theo, để biết được chiều dài sợi quang MCF (*L*) ảnh hưởng đến hiệu năng hệ thống như thế nào, QBER tại Bob được khảo sát phụ thuộc vào độ dài sợi quang MCF với *Pt* = 5 dBm, M_A = 5 và khoảng cách giữa BS và Bob (*d*) bằng 300 m như trong hình 5. Từ kết quả mô phỏng ta có thể thấy, để *QBER* nhỏ hơn 10^{-3} với khoảng cách sợi quang MCF 4 lõi, vị trí bộ thu của Bob nên tránh tại một số khoảng cách ví dụ như khoảng 11-16 km hay 20-25 km. Còn đối với sợi 32 lõi, *QBER* của hệ thống chỉ đạt được yêu cầu với khoảng cách sợi quang trong dải khoảng 60-62 km hoặc lớn hơn khoảng 70 km. Lý do của việc nên tránh tại một số khoảng cách sợi quang là vì nhiễu phách gây ra sau APD phụ thuộc vào hàm *cos* như trong công thức (9).

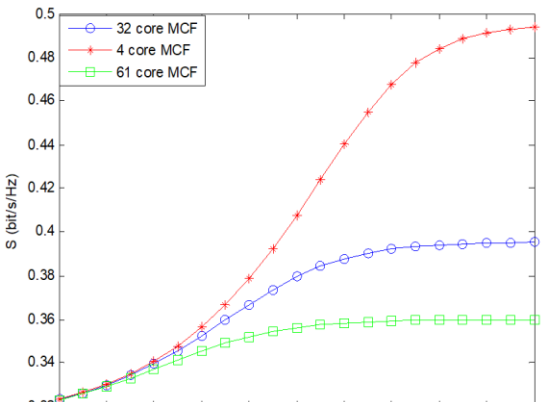


Hình 5: QBER phụ thuộc vào khoảng cách sợi quang MCF với Pt = 5 dBm, MA = 5, dAB = 300m.

Hình 6 biểu diễn ảnh hưởng của công suất phát quang và khoảng cách vô tuyến giữa BS và Bob lên QBER của hệ thống trong trường hợp sử dụng sợi MCF 32 lõi và khoảng cách sợi MCF lên tới 80km. Như hình vẽ chỉ ra, với khoảng cách vô tuyến giữa BS và Bob ở mức 300m thì công suất phát yêu cầu khoảng 3.2 dBm, trong khi công suất phát yêu cầu đến 10 dBm cho khoảng cách vô tuyến ở mức 1000 m.



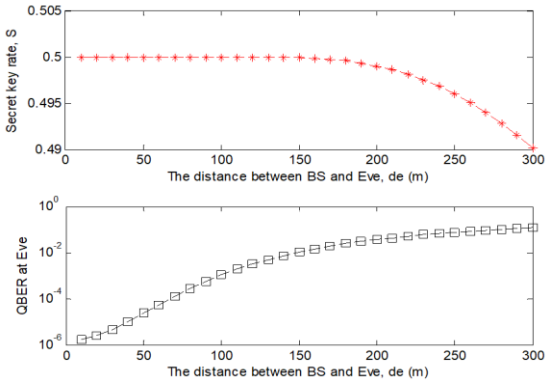
Hình 6: QBER phụ thuộc vào công suất phát khi chiều dài sợi 32 lõi dài 80 km, MA =5



Hình 7: Tốc độ khóa bí mật phụ thuộc vào công suất phát, khi khoảng cách sợi đa lõi dài 80 km.

Tiếp đó, Hình 7 mô tả tốc độ khóa bí mật phụ thuộc vào công suất phát, khi khoảng cách sợi đa lõi dài 80 km. Ba loại sợi đa lõi khác nhau được xem xét bao gồm 4 lõi, 32 lõi và 61 lõi. Tốc độ khóa bí mật phụ thuộc nhiều vào loại sợi đa lõi, cụ thể với sợi càng ít lõi thì tốc độ khóa bí mật đạt được càng cao với công suất phát khoảng từ 0 dBm trở đi. Điều này có thể lý giải do xuyên nhiễu ở sợi MCF nhiều lõi cao hơn nhiều so với sợi MCF ít lõi.

Cuối cùng, trong hình 8, Tốc độ khóa bí mật và QBER của Eve được khảo sát phụ thuộc vào khoảng cách vô tuyến giữa BS và Eve. Nhận thấy rằng tốc độ khóa bí mật ergodic giảm và QBER tại Eve tăng khi khoảng cách vô tuyến giữa BS và Eve tăng. Do vậy, khi khoảng cách vô tuyến này càng xa thì Eve có QBER cao và do đó khả năng sửa lỗi của Eve là khó.



Hình 8: Tốc độ khóa bí mật Ergodic và QBER tại Eve phụ thuộc vào khoảng cách vô tuyến giữa BS và Eve khi khoảng cách sợi 4 lõi dài 80 km.

V. KẾT LUẬN

Bài báo đã đề xuất giải pháp tăng dung lượng hệ thống phân phối khóa lượng tử qua hệ thống lai ghép quang vô tuyến sử dụng điều chế cường độ sóng mang con với tín hiệu BPSK và bộ thu tách sóng hai ngưỡng. Các mô tả toán học cho các phân tích bảo mật của hệ thống đề xuất được phân tích. Tỉ lệ lỗi bít lượng tử và tốc độ khóa bí mật biến thiên theo các tham số lớp vật lý được xem xét. Các kết quả mô phỏng số chứng tỏ rằng hệ thống đề xuất có thể đạt được các mục tiêu bảo mật mong muốn bao gồm QBER nhỏ hơn 10^{-3} và tốc độ khóa chọn lọc đạt được tại tốc độ Mbps. Các kết quả cho thấy hệ thống lai ghép quang vô tuyến là giải pháp hiệu quả để phân phối khóa lượng tử tới các thiết bị di động.

TÀI LIỆU THAM KHẢO

[1] L.-J. Wang, K.-H. Zou, W. Sun, Y. Mao, Y.-X. Zhu, H.-L. Yin, Q. Chen, Y. Zhao, F. Zhang, T.-Y. Chen, and J.-W. Pan, ‘‘Long-distance copropagation of quantum key distribution and terabit classical optical data channels,’’ Phys. Rev. A, Gen. Phys., vol. 95, no. 1, Jan. 2017, Art. no. 012301.

[2] S. Kleis, J. Steinmayer, R. H. Derksen, and C. G. Schaeffer, ‘‘Experimental investigation of heterodyne quantum key distribution in the S-Band embedded in a commercial DWDM system,’’ in Proc. Opt. Fiber Commun. Conf. (OFC), 2019, pp. 1–3, Paper. Th1J.3.

[3] F. Karinou, H. H. Brunner, C.-H.-F. Fung, L. C. Comandar, S. Bettelli, D. Hillerkuss, M. Kuschnerov, S. Mikroulis, D. Wang, C. Xie, M. Peev, and A. Poppe, ‘‘Toward the integration of CV quantum key distribution in deployed optical networks,’’ IEEE Photon. Technol. Lett., vol. 30, no. 7, pp. 650–653, Apr. 1, 2018.

[4] P. J. Winzer, ‘‘Spatial multiplexing in fiber optics: The 10X scaling of Metro/Core capacities,’’ Bell Labs Tech. J., vol. 19, pp. 22–30, Sep. 2014.

[5] R. S. Luís, B. J. Puttnam, J. M. D. Mendinueta, W. Klaus, J. Sakaguchi,Y. Awaji, T. Kawanishi, A. Kanno, and N. Wada, ‘‘OSNR penalty of selfhomodyne coherent detection in spatial-division-multiplexing systems,’’ IEEE Photon. Technol. Lett., vol. 26, no. 5, pp. 477–479, Mar. 1, 2014.

[6] X. Pang, ‘‘High-speed SDM interconnects with directly-modulated .5-μm VCSEL enabled by low-complexity signal processing techniques,’’ in Proc. Signal Process. Photon. Commun., vol. 2018, pp. 1–2, Paper. Sp

[7] J. F. Dynes, S. J. Kindness, S. W.-B. Tam, A. Plews, A. W. Sharpe, M. Lucamarini, B. Fröhlich, Z. L. Yuan, R.V. Penty, and A. J. Shields, “Quantum key distribution over multicore fiber,” Opt. Express 24(8), 8081-8087 (2016).

[8] G. Cañas, N. Vera, J. Cariñe, P. González, J. Cardenas, P. W. R. Connolly, A. Przysiezna, E. S. Gómez, M. Figueroa, . Vallone, P. Villoresi, T. Ferreira da Silva, G. B. Xavier, and G. Lima, “High-dimensional decoystate quantum key distribution over multicore telecommunication fibers,” Phys. Rev. A 96, 022317 (2017).

[9] Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, “High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits,” npj Quantum Information 3, 25 (2017).

[10] T. A. Eriksson et al., “Coexistence of continuous variable quantum key distribution and 7×12.5 Gbit/s classical channels,” in Proc. IEEE Photon. Soc. Summer Top. Meeting Ser. (SUM), Jul. 2018, pp. 71–72.

[11] F. Li, H. Zhong, Y. Wang, Y. Kang, D. Huang, and Y. Guo, “Performance analysis of continuous-variable quantum key distribution with multi-core fiber,” Appl. Sci., vol. 8, no. 10, p. 1951, 2018.

[12] Tobias A. Eriksson, Benjamin J. Puttnam,..., “Crosstalk Impact on Continuous Variable Quantum Key Distribution in Multicore Fiber Transmission,” IEEE PHOTONICS TECHNOLOGY LETTERS, VOL. 31, NO. 6, MARCH 15, 2019

[13] Thu A. Pham, Nga T. T. Nguyen, and Ngoc T. Dang, “Quantum Key Distribution over Hybrid Fiber-Wireless System for Mobile Networks” In the Proc. of the ACM Eighth International Symposium on Information and Communication Technology (SoICT 2019), Hanoi-Halong, Vietnam, Dec. 2019, pp. 236-241.

[14] T Hayashi, T Taru, O Shimakawa, T Sasaki, E Sasaoka, Design and fabrication of ultra-low crosstalk and low-loss multi-core fiber, Optics express, Vol.19, No.17, 2011.

[15] Masanori Koshiba, Kunimasa Saitoh, Katsuhiro Takenaga, and Shoichiro Matsuo, “Multi-core fiber design and analysis: coupled-mode theory and coupled-power theory,” Opt. Express 19, B102-B111 (2011).

[16] M. Koshiba, K. Saitoh, K. Takenaga, and S. Matsuo, “Multi-core fiber design and analysis: coupled mode theory and coupled-power theory,” Optics Express, vol.19, no.16, pp.B102-B111, 2011.

[17] D. Marcuse, “Derivation of coupled power equations,” Bell Syst. Tech. J. 51, 229–237, 1972.

[18] Ahmed E. A. Farghal, Performance analysis of core-multiplexed spectral amplitude coded OCDMA PON, Journal of Optical Communications and Networking, Vol. 8, Iss. 9, Sept. 2016.

[19] Govind P. A. Fiber-Optic Communications Systems. John Wiley & Sons 2002, Third Edition, Inc. ISBNs: 0-471-21571-6 (Hardback); 0-471-22114-7 (Electronic).

[20] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum Cryptography” Rev. Mod. Phys., vol. 74, pp. 145–195, 2002

[21] P. V. Trinh, T. V. Pham, N. T. Dang, H. V. Nguyen, S. X. Ng and A. T. Pham, “Design and security analysis of quantum key distribution protocol over free-space optics using dual-threshold direct-detection receiver,” IEEE Access, vol. 6, pp. 4159–4175, 2018.

A SOLUTION TO INCREASE THE CAPACITY OF QUANTUM KEY DISTRIBUTION SYSTEMS BY USING RADIO-OPTICAL HYBRID SYSTEM

Abstract - The quantum key transmission model on the radio-optical hybrid system is considered one of the solutions with many advantages such as providing long transmission distances, flexibility, and easy expansion.Therefore, the model has been received special attention from many researchers and implementers in recent years. However, performance in terms of system capacity is still an issue that needs to be considered and improved. In this paper, we propose a solution to improve the capacity of the quantum key distribution system through the radio-optical hybrid system, which is to use multi-core optical fiber (MCF). The quantum key from the sender (Alice) is transmitted over the multicore fiber to the intermediate station (BS) and then forwarded to the mobile stations (Bob) over the radio channel. The QKD protocol is implemented by relying on subcarrier intensity modulation using binary phase shift keying, and a two-threshold receiver is used for decoding. The system performance in terms of quantum bit error rate and secret key rate of the system is analyzed under the influence of many physical layer parameters coming from the receiver, optical network part and radio channel. These parameters include radio channel loss, optical channel loss, crosstalk in the MCF fiber, and receiver noise. In addition, the article also considers the performance of the system in the presence of an attacker (Eve). The feasibility of the proposed QKD system is demonstrated in the results of this paper.

Keywords – Quantum key distribution (QKD), Multicore Fiber (MCF), Subcarrier Intensity Modulation (SIM), Quantum Bit Error Rate (QBER).

Phạm Anh Thư nhận bằng kỹ sư điện tử viễn thông của Học viện Công nghệ Bưu chính Viễn thông (PTIT), Việt Nam, năm 2003, và bằng Thạc sĩ Kỹ thuật Viễn thông của Học viện Công nghệ Hoàng gia Melbourne, Australia, năm 2008. Cô nhận học vị Tiến sĩ về Kỹ thuật viễn thông tại PTIT năm 2019. Hiện nay, cô là giảng viên khoa Viễn thông1, Học viện công nghệ bưu chính viễn thông. Các lĩnh vực nghiên cứu chính bao gồm mạng truyền thông, truyền sóng vô tuyến qua sợi quang và an toàn mạng thông tin.

.