TRANG THÔNG TIN LUẬN ÁN TIẾN SĨ

Tên đề tài luận án tiến sĩ: **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

Họ và tên NCS: Phan Thị Thu Hằng

Khóa đào tạo: 2018-2021

Người hướng dẫn khoa học:

1. PGS. TS Đặng Thế Ngọc

2. PGS. TS Lê Hải Châu

Cơ sở đào tạo: Học viện Công nghệ Bưu chính Viễn thông

NHỮNG KẾT QUẢ MỚI CỦA LUẬN ÁN:

Luận án đề cập tổng quát về phân phối khóa lượng tử nói chung và phân phối khóa lượng tử biến liên tục nói riêng; truyền thông quang không dây dựa trên vệ tinh; phân phối khóa lượng tử biến liên tục sử dụng truyền dẫn quang qua không gian tự do. Từ những nội dung này, luận án khẳng định sự cần thiết của việc cải thiện hiệu năng truyền dẫn quang qua không gian tự do trong hệ thống phân phối khóa lượng tử biến liên tục. Kết quả đưa ra trong luận án là các giải pháp nâng cao hiệu năng truyền dẫn quang qua không gian tự do trong hệ thống phân phối khóa lượng tử biến liên tục đơn kênh và đa kênh đảm bảo các tiêu chí như: tỷ lệ lỗi bit lượng tử QBER nhỏ đảm bảo cho quá trình sửa lỗi bên phía thu; tốc độ khóa bí mật đủ lớn khi xem xét tới các yếu tố ảnh hưởng tới điều kiện truyền dẫn như: nhiễu loạn khí quyển, các thành phần gây suy hao tín hiệu và nhiễu tại máy thu; đảm bảo được an ninh của hệ thống trong một số điều kiện cụ thể khi có kẻ nghe lén xuất hiện. Đóng góp mới của quá trình nghiên cứu thể hiện trong luận án 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.

CÁC ỨNG DỤNG, KHẢ NĂNG ỨNG DỤNG TRONG THỰC TIỄN HOẶC NHỮNG VẤN ĐỀ CÒN BỎ NGỎ CẦN TIẾP TỤC NGHIÊN CỨU

Những nghiên cứu của luận án có thể xem xét để ứng dụng trong các hệ thống QKD có quy mô toàn cầu nhằm đảm bảo tính bảo mật của truyền thông trong điều kiện hiện nay. Liên quan đến những đề xuất mới của luận án, có thể liệt kê những vấn đề cần nghiên cứu trong các công trình tiếp theo như sau:

(1) 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.

(2) 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 mạng QKD được định nghĩa bằng phần mềm và các giải pháp cải thiện hiệu năng trong một mạng QKD được định nghĩa bằng phần mềm sẽ trở nên 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.

Xác nhận của đại diện tập thể

Người hướng dẫn khoa học	Nghiên cứu sinh
PGS.TS Đặng Thế Ngọc	Phan Thị Thu Hằng