# ĐÁNH GIÁ HIỆU NĂNG BẢO MẬT TRONG TRUYỀN THÔNG GIỮA VỆ TINH LEO VÀ HẠ TẦNG TRÊN CAO (HAPS)

**Nguyễn Thị Thu Nga**
Học viện Công nghệ Bưu Chính Viễn Thông

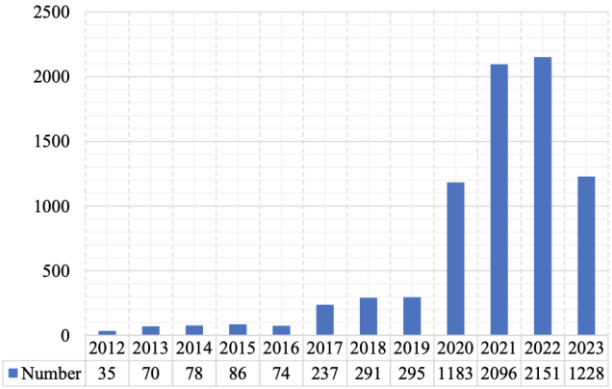
***Tóm tắt:*** Bài báo này tập trung nghiên cứu đánh giá hiệu năng bảo mật trong truyền thông quang giữa vệ tinh (LEO) và hạ tầng trên cao (HAPS). Cụ thể, nghiên cứu phân tích kịch bản nghe lén cho truyền thông đường xuống từ vệ tinh LEO đến HAPS. Để định lượng hiệu năng bảo mật của kịch bản, dung lượng bảo mật trung bình, xác suất dừng bảo mật, và thông lượng bảo mật được đưa ra dưới dạng công thức tường minh trong nghiên cứu này. Kết quả của nghiên cứu chứng tỏ rằng để tăng khả năng bảo mật của hệ thống ta có thể tăng công suất phát, giảm góc của chùm tia phân kỳ ở phía phát, tăng tốc độ ký hiệu, điều chỉnh tỷ lệ phân bố công suất.

***Từ khoá:*** Truyền thông quang vệ tinh (OpticsSatCom), HAP, LEO, Bảo mật lớp vật lý.

## I. GIỚI THIỆU:

Được thúc đẩy bởi sự phát triển bùng nổ của các thiết bị thông minh và sự gia tăng lưu lượng dữ liệu, khái niệm Thế hệ thứ sáu (6G) [1]–[3] nhằm mục đích xây dựng một mạng lưới toàn cầu tự chủ có chiều rộng lớn có khả năng hỗ trợ vùng phủ sóng liền mạch và các dịch vụ phổ biến. Bằng chứng là trong tài liệu [4], các tác giả đã đề xuất rằng các mạng không dây trong tương lai phải có khả năng giao tiếp liền mạch với các mạng mặt đất và vệ tinh. So với các vệ tinh Quỹ đạo Trái đất trung bình (MEO) và Quỹ đạo Trái đất địa tĩnh (GEO), các vệ tinh Quỹ đạo Trái đất thấp (LEO) [5]–[7] gần Trái đất hơn. Do đó, chúng phù hợp hơn để hỗ trợ truyền thông với độ trễ thấp trên toàn thế giới [8]. Ngoài ra, công nghệ thu hồi tên lửa và phóng đa vệ tinh đã giảm đáng kể chi phí phóng trung bình và thời gian triển khai. Như một lợi thế, hệ thống thông tin vệ tinh LEO (SCS) đã tìm thấy rất nhiều ứng dụng, bao gồm cả Internet Vạn vật Từ xa ( IoRT), thành phố thông minh và cứu hộ khẩn cấp [4].

Các vệ tinh LEO được phóng lần đầu tiên cách đây hơn 50 năm. Khái niệm về LEO SCS có thể bắt nguồn từ những năm 1990, khi Iridium [9], Globalstar [10] và Orbcomm được thiết kế để cung cấp dịch vụ thoại và dữ liệu có độ trễ thấp. Tuy nhiên, một số trong số chúng cuối cùng đã bị phá sản do chi phí cao, công nghệ chưa trưởng thành và khả năng truyền thông còn khiêm tốn. Nhưng nhờ sự phát triển của vật liệu tiên tiến, công nghệ tinh vi và quy mô nền kinh tế, một kỷ nguyên LEO SCS mới đã hé mở. Trong những năm gần đây, do nhu cầu ngày càng tăng [11], giảm chi phí [12] và tiến bộ công nghệ, các chòm sao lớn của LEO, như OneWeb, Starlink và Lightspeed, đang nỗ lực đổi mới để cung cấp dịch vụ cho 3 tỷ người còn lại chưa có quyền truy cập Internet.




*Hình 1. Số lượng vệ tinh LEO phóng từ năm 2012 đến quý 2 năm 2023.[4]*

Tại thời điểm viết bài, chúng có xu hướng phát triển theo hướng hệ thống hội tụ như được các chuyên gia dự đoán. Trong số đó, các vệ tinh có quỹ đạo cao có độ phân giải thấp và độ trễ cao hơn, làm cho chúng không phù hợp với lưu lượng lớn với độ trễ. Để thỏa mãn nhu cầu cao về công nghệ mới và tránh độ trễ lớn, việc sử dụng vệ tinh LEO đã thu hút được nhiều sự quan tâm. So với GEO và MEO, ngày nay LEO có mật độ đông đúc với hàng nghìn vệ tinh đang hoạt động do hiệu quả chi phí, độ trễ thấp hơn và tiêu thụ ít điện năng hơn. Từ năm 2012 đến quý II năm 2023, khoảng 7824 vệ tinh LEO đã được phóng thành công như được minh hoạ trong hình 1. Hệ thống truyền thông (SCS) đã có rất nhiều các ứng dụng, bao gồm Internet of Remote Things (IoRT), thành phố thông minh và cứu hộ khẩn cấp [4]. Do đó, các vệ tinh LEO được kỳ vọng sẽ là công nghệ then chốt hỗ trợ chính cho việc thực hiện truyền

Tác giả liên hệ: Nguyễn Thị Thu Nga,
Email: ngantt@ptit.edu.vn
Đến tòa soạn: 10/2023, chỉnh sửa: 11/2023, chấp nhận đăng: 12/2023.

thông trong không gian trong các mạng không dây trong tương lai do tiềm năng của chúng trong việc cung cấp liên lạc theo thời gian thực với tốc độ dữ liệu nâng cao và phạm vi phủ sóng rộng lớn.

Bên cạnh đó, một công nghệ được coi là hệ thống "giả" vệ tinh có độ bền cao, độ cao có thể cung cấp dịch vụ quan sát hoặc liên lạc tương tự như vệ tinh nhân tạo, và được biết tới với cái tên hạ tầng trên cao (HAPS). Nói chung, có hai lớp tương tác được hình dung như một phần của lớp mạng trên không. Một lớp con sẽ bao gồm các nút máy bay không người lái ở độ cao thấp (LAP) và lớp con thứ hai sẽ bao gồm các hệ thống hạ tầng trên cao (HAPS). HAPS là máy bay không người lái hoặc khinh khí cầu hoạt động ở tầng bình lưu có độ cao từ 17 - 20 km trong 32 giờ, có thể cung cấp những lợi ích đáng kể như phạm vi phủ sóng rộng lớn, chất lượng tín hiệu tốt hơn, độ tin cậy, thông lượng cao hơn, chi phí thấp hơn và độ trễ nhỏ hơn [6]. Hơn nữa, tầng bình lưu được coi là ít bị ảnh hưởng bởi điều kiện thời tiết khắc nghiệt và an toàn hơn cho các ứng dụng.

Hệ thống truyền thông vệ tinh (SatCom) theo truyền thống thường dựa trên tần số vô tuyến (RF). Tuy nhiên, hệ thống RF có xu hướng gặp nhiều các vấn đề bao gồm tắc nghẽn phổ tần, vấn đề cấp phép, nhiễu với các băng tần khác. Hơn nữa, RF SatCom dễ gặp rủi ro bảo mật hơn do nhiễu, điều này đặc biệt quan trọng đối với thông tin liên lạc quân sự. Truyền thông quang không gian tự do (FSO) đã loại bỏ được những vấn đề này. Trên thực tế, FSO SatCom mang lại nhiều lợi thế so với RF nhờ các đặc tính độc đáo của nó. Không giống như RF, FSO được coi là cung cấp băng thông cực cao, phổ không cần cấp phép, cải thiện bảo mật và triển khai dễ dàng. Trong FSO SatCom, điều cần thiết chính là kết nối tầm nhìn thẳng (LoS) và căn chỉnh chính xác giữa phát thu để đảm bảo truyền tin hoàn hảo.

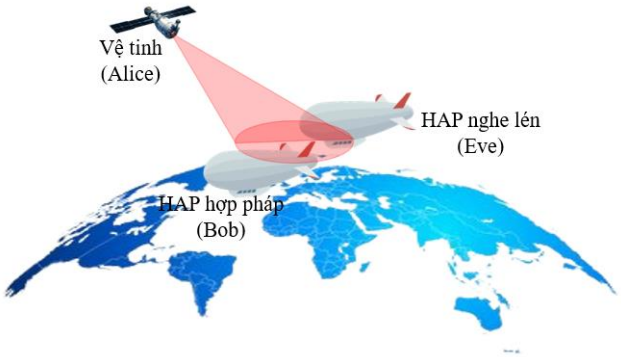
Tuy nhiên do truyền thông quang không dây là môi trường mở nên việc đảm bảo trao đổi thông tin một cách an toàn là một thách thức lớn. Hệ thống LEO - HAPS phải đối mặt với cả những cuộc tấn công an ninh và rủi ro về độ tin cậy. Các yêu cầu về an ninh và độ tin cậy của hệ thống này được đặt ra nhằm mục đích ngăn chặn cả hai loại đe dọa này, bao gồm cả việc nghe lén, gây nhiễu, va chạm, và các hình thức khác. Với số lượng vệ tinh ngày càng lớn trong môi trường mở thì việc nghe lén là một mối lo ngại. Để bảo vệ thông tin từ nghe lén, bảo mật lớp vật lý (PLS) dựa trên đặc điểm của kênh truyền đang dành được nhiều sự quan tâm nghiên cứu. PLS khám phá tính ngẫu nhiên của kênh không dây để đạt được tính bảo mật và xác thực [13].

B. Li và các cộng sự trong [14] đã khảo sát toàn diện về PLS cho hệ thống thông tin vệ tinh, cũng như thảo luận về những thách thức nghiên cứu liên quan mà kiến trúc mạng tích hợp mới nổi phải đối mặt. Cũng nghiên cứu về PLS, K. Guo, K. An, Y. Huang and B. Zhang trong [15] khảo sát hiệu năng bảo mật của các hệ thống thông tin vệ tinh có nhiều kẻ nghe lén. Đặc biệt, bằng cách tính đến tác động của suy hao đường truyền và hiện tượng che khuất ngẫu nhiên, các tác giả đã rút ra được các biểu thức dạng đóng cho PSPSC, SOP và ASC. Trong khi đó Wang and F. Zhou [16] lại khảo sát tính bảo mật lớp vật lý của mạng truyền thông vệ tinh di động mặt đất (LMS), trong đó nhiều người dùng hợp pháp và thiết bị nghe lén được xem xét trong hệ thống. Nghiên cứu cũng đưa ra các biểu thức dạng đóng của xác suất dừng bảo mật (SOP) và dung lượng bảo mật trung bình (ASC) dựa trên sơ đồ hợp tác người dùng được đề xuất khi có nghe lén. Nghiên cứu tính bảo mật lớp vật lý của truyền thông quang không gian tự do (FSO) với các tình huống nghe lén khác nhau được Y. Ai, A. Mathur và các cộng sự thực hiện trong [17]. Ba kịch bản thực tế khác nhau về việc nghe lén được xem xét bằng cách giả định những vị trí đặt khác nhau của kẻ nghe lén. Các biểu thức mới về khả năng bảo mật trung bình (ASC) và xác suất dừng bảo mật (SOP) được rút ra cho các kịch bản được xem xét. Kết quả cho thấy khi thiết bị nghe lén được đặt gần máy phát, điều kiện khí quyển sẽ có tác động ít đáng kể hơn đến hiệu suất bảo mật. Có thể thấy các nghiên cứu trước đây về nghe lén chủ yếu là cho hệ thống truyền thông quang không dây mặt đất hoặc hệ thống vệ tinh. Chính vì vậy, chúng tôi đề xuất mô hình và đánh giá thông lượng bảo mật trong truyền thông quang giữa vệ tinh và hạ tầng trên cao với các đóng góp như sau:

- Đưa ra một kịch bản nghe lén mới, hay còn gọi là thiết bị nghe lén (Eavesdropping), trong vấn đề tấn công bảo mật thụ động, cụ thể là HAPS đang nghe lén truyền thông giữa vệ tinh LEO và HAPS.
- Nghiên cứu tác động của tầng bình lưu đến bảo mật của hệ thống, cụ thể là chúng tôi xem xét sự ảnh hưởng của các đám mây băng (loại mà bay ở tầng cao trên 10 Km) tới sự suy giảm tín hiệu FSO.
- Phân tích hiệu năng bảo mật của truyền thông quang theo kịch bản thực tế. Truyền thông quang đường xuống (DL) giữa vệ tinh LEO và nút HAPS. Giả định HAPS nghe lén được đặt rất gần với máy thu hợp pháp HAPS, trong vùng diện tích của chùm tín hiệu quang thu được. Từ đó, nghiên cứu đánh giá thông lượng bảo mật trong truyền thông quang giữa vệ tinh LEO và hạ tầng trên cao HAP. Việc đánh giá được thực hiện thông qua xác suất dừng bảo mật (SOP) và dung lượng bảo mật trung bình (ASC).

Bài báo được tổ chức như sau: Phần I là giới thiệu chung trình bày về truyền thông quang không dây giữa vệ tinh – HAPS, vấn đề bảo mật của hệ thống và các nghiên cứu liên quan. Kênh và các mô hình hệ thống được trình bày ở Phần II. Phần III đưa ra mô hình giải tích phân tích dung lượng bảo mật trung bình, xác suất dừng bảo mật, và thông lượng bảo mật cho truyền thông quang không dây giữa vệ tinh và HAPS. Phần IV thảo luận về kết quả đạt được trong nghiên cứu này. Cuối cùng, phần V tóm lược những đóng góp chính cũng như kết quả chọn lọc của nghiên cứu.

## II. MÔ HÌNH HỆ THỐNG




*Hình 2. Kịch bản nghe lén của HAPS.*

Như trình bày ở trên, một yếu tố không thể thiếu trong việc xét truyền thông tin quang giữa vệ tinh và HAPS là tính toán đến độ suy giảm của đám mây đóng băng trên tầng cao (độ cao trên 10 Km). Trong khí quyển, mây được hình thành khi có những hạt mưa nhỏ hoặc tinh thể băng lơ lửng [18]. Các đám mây thường nằm ở độ cao khoảng 150 m so với bề mặt Trái đất [19]. Do cường độ nhỏ hơn mưa, Hàm lượng nước lỏng trong đám mây (CLWC) có thể ảnh hưởng đến sóng điện từ trên tần số hoạt động 10 GHz (đặc biệt ở vùng vi sóng và sóng milimet) [20]. Vì vậy, phần này minh họa phương pháp suy giảm đám mây do Liên minh Viễn thông Quốc tế-Truyền thông vô tuyến [19] nêu ra. Từ phương pháp này, hàm lượng nước lỏng, LWC, là một tham số cần thiết để xác định hiệu quả độ suy giảm trong khoảng từ 10 đến 200 GHz [20]. Tương tự, để phân tích giá trị xác suất suy giảm đám mây cần biết tổng hàm lượng nước lỏng trong mây, $M_c$ (mg/m$^3$) của khu vực nghiên cứu. Do đó, công trình này sử dụng Radar đo lượng mưa nhiệt đới để thu được giá trị trung bình 5 năm của $L$. Lượng suy hao do đám mây gây ra, $h_c$, được biểu thị bằng:

$$h_c = \exp(-\alpha d_c) \quad (1)$$

trong đó $d_c$ là quãng đường truyền FSO bị mây tác động, và $\alpha$ là hệ số suy giảm, cái mà được biểu diễn như sau

$$\alpha = \frac{3.91}{V}\left(\frac{\lambda}{550}\right)^{-q} \quad (2)$$

Trong đó $V = \frac{1.002}{(N_c M_c)^{0.6473}}$ là chỉ số tầm nhìn được đo theo đơn vị km, và trong đó $N_c$ là chỉ số loại mây và $M_c$ hàm lượng nước lỏng trong mây. $\lambda$ là bước sóng quang được đo theo đơn vị nm, và $q$ là hệ số của mô hình Kim [20].

Trong bài báo này, chúng tôi đề xuất một kịch bản mới về tấn công nghe lén trong không gian giữa các vệ tinh thuộc quỹ đạo LEO và HAPS. Như được hiển thị trong Hình 2, chúng tôi giả sử một vệ tinh LEO (kí hiệu là: S) giao tiếp với nút đích HAPS (kí hiệu là: H) khi có sự hiện diện của các thiết bị nghe lén là các HAPS xung quanh (kí hiệu là: E) nằm rất gần H. Ở đây, chúng tôi xét đường xuống (DL) từ S đến H, trong đó E nằm trong vùng diện tích thu được của chùm tín hiệu quang phát từ S để nó có thể nghe lén được chùm tia thu được. Trong ngữ cảnh này, thiết bị nghe lén E chỉ có thể thu được một phần nhỏ tín hiệu được truyền đi, trong khi đó máy thu hợp pháp sẽ thu được nhiều năng lượng hơn là $r_b$, trong đó $r_e + r_b \leq 1$ [13] với $r_e$, *và* $r_b$ lần lượt là phần diện tích thu được của thiết bị nghe lén và máy thu hợp pháp đã chuẩn hóa.

Lưu ý rằng các tham số $r_b$ và $r_e$ phụ thuộc vào kích thước khẩu độ của từng thiết bị cùng với góc phân kỳ chùm tia. Trong phân tích, chúng tôi giả định rằng vị trí của vệ tinh, HAPS và tàu vũ trụ nghe lén có thể được sử dụng để trích xuất thông tin vật lý của mô hình kênh đại diện cho thông tin trạng thái kênh [13]. Trong kịch bản giao tiếp S đến H, tín hiệu nhận được ở H là:

$$y_H = \sqrt{r_b P_S}\, I_H x_S + n_H \quad (3)$$

tín hiệu nhận được tại E là:

$$y_E = \sqrt{r_e P_S}\, I_E x_S + n_E \quad (4)$$

trong đó, $P_S$ biểu thị công suất phát của $S$. Bên cạnh đó, $I_H$, $I_E$ biểu thị bức xạ nhận được lần lượt tại $H$ và $E$. $x_S$, $x_H$ là các tín hiệu được truyền đi. Và, $n_H$, $n_S$ biểu thị nhiễu Gaussian trắng cộng (AWGN) với mật độ phổ công suất nhiễu $N_0$. Do đó, tỷ lệ tín hiệu trên nhiễu tức thời (SNR) tại $H$ là:

$$\gamma_H = \frac{r_b P_S h_c}{N_0} I_H^2 = \overline{\gamma_H} I_H^2 \quad (5)$$

trong đó

$$\overline{\gamma_H} = \frac{r_b P_S h_c}{N_0} \quad (6)$$

Xác định SNR trung bình tại H với

$$E[I_H^2] = 1 \quad (7)$$

và SNR tức thời tại E có thể được biểu thị tương tự sau khi thay đổi chỉ số dưới thành

$$\gamma_E = \frac{r_e P_J h_c}{N_0} I_E^2 = \overline{\gamma_E} I_E^2 \quad (8)$$

với

$$E[I_E^2] = 1 \quad (9)$$

Chúng tôi giả sử rằng nhiễu loạn gây ra Fading tuân theo phân bố EW. Phân bố EW đã được chứng minh là phù hợp nhất với các đường kính khẩu độ khác nhau đối với nhiễu loạn từ mức độ yếu đến mức độ mạnh, đặc biệt là khi tính trung bình khẩu độ được sử dụng để giảm thiểu hiện tượng tác động của nhiễu loạn và tăng hiệu năng tổng thể [13]. Vì thế hàm mật độ xác suất (PDF) của bức xạ $I$ cho nút $k$ trong đó $k \in \{H,E\}$ được biểu diễn như trong [13]. Hơn nữa, sự tích lũy hàm phân phối (CDF) của $\gamma_k$ có thể được biểu diễn dưới dạng [14]

$$F_{\gamma_k}(\gamma) = \sum_{p=0}^{\infty} \binom{\alpha_k}{p} (-1)^p exp\left[-p\left(\frac{\gamma}{\eta_k^2 \overline{\gamma}}\right)^{\frac{\beta k}{2}}\right] \quad (10)$$

trong đó $\alpha_k$, $\beta_k$ và $\eta_k$ tương ứng biểu thị các tham số hình dạng và tham số tỷ lệ, phụ thuộc vào chỉ số nhiễu loạn không khí [13]. Chỉ số nhiễu loạn $\delta_{I_{DL}}^2$ tại H có thể viết như sau:

$$\delta_{I_{DL}}^2 = exp\left[\frac{0.49\delta_R^2}{(1+1.11\delta_R^{\frac{12}{5}})^{\frac{5}{6}}} + \frac{0.51\delta_R^2}{(1+0.69\delta_R^{\frac{12}{5}})^{\frac{5}{6}}}\right] - 1 \quad (11)$$

trong đó, $\delta_R^2$ biểu thị phương sai Rytov được đưa ra trong [3], và nó phụ thuộc vào góc thiên đỉnh $\xi_H$ và tốc độ gió $w_H$. Với đường xuống DL, lỗi lệch chùm tia gây ra phải

được xem xét [13]. Vì vậy, chỉ số nhấp nháy $\delta_{I\,DL}^2$ có thể được viết như sau:

$$\delta_{I\,DL}^2 = 5.95(H_p - h_0)^2 sec^2(\xi_p)\left(\frac{2W_0}{r_0}\right)^{\frac{5}{3}}\left(\frac{\alpha_{pe}}{W_p}\right)^2 + exp\left[\frac{0.49\delta_{Bu}^2}{(1+(1.11+\Theta)\delta_{Bu}^{\frac{12}{5}})^{\frac{7}{6}}} + \frac{0.51\delta_{Bu}^2}{(1+0.69\delta_{Bu}^{\frac{12}{5}})^{\frac{5}{6}}}\right] - 1 \quad (12)$$

trong đó *Hp* là độ cao của S và E, $h_0$ là độ cao HAPS và $\xi_p$ là góc cực đại cho hướng xuống DL. $W_0$ là bán kính chùm tia tại H, tham số Fried $r_0$ phụ thuộc vào tốc độ gió $w_p$, $\alpha_{pe}$ biểu thị phương sai sai số định hướng do lệch chùm tia, $W_p$ là kích thước chùm tia tại S và E, và $\delta_{Bu}^2$ là phương sai Rytov trong truyền thông đường xuống DL [13].

## III. PHÂN TÍCH BẢO MẬT HỆ THỐNG

Trong phần này, chúng tôi phân tích hiệu năng bảo mật của kịch bản hệ thống dưới tình huống xem xét vấn đề tấn công bảo mật thụ động, cụ thể là có thiết bị nghe lén. Cụ thể hơn, các biểu thức dạng đóng của ASC, SOP, và ST được tính cho hướng xuống DL.

Theo lý thuyết thông tin định nghĩa dung lượng bảo mật $C_s$ là mức tối đa có thể đạt được tỷ lệ bảo mật được biểu thị như sau [14]:

$$C_s = \begin{cases} log_2(1+\gamma_H) - log_2(1+\gamma_E), & \gamma_H > \gamma_E \\ 0 & còn\ lại \end{cases} \quad (13)$$

với $\gamma_H$ , $\gamma_E$ lần lượt biểu thị SNR tức thời của máy thu chính và thiết bị nghe lén.

### *A. Dung lượng bảo mật trung bình*

Trong PLS, dung lượng bảo mật trung bình (ASC) là một tham số quan trọng để đánh giá hiệu năng bảo mật của hệ thống. Trong ngữ cảnh nghe lén đường xuống từ S đến H, chúng tôi giả sử rằng E được đặt rất gần với H. Do đó, có thể thu được ASC cho việc nghe lén DL bằng cách lấy trung bình $C_s$ như sau:

$$\bar{C_s} = \frac{1}{\ln(2)} E\left[\ln(1+\gamma_H) - \ln(1+\gamma_E)\right] \quad (14)$$

Bằng cách sử dụng bất đẳng thức Jensen, đối với các giá trị SNR cao, ASC có thể được viết lại là:

$$\bar{C_s} \cong \frac{1}{\ln(2)}\left[\ln(1+E[\gamma_H]) - \ln(1+E[\gamma_E])\right] \cong \frac{1}{\ln(2)}\left[\ln\left(1+\frac{r_b P_S}{N_0}\right) - \ln\left(1+\frac{r_e P_S}{N_0}\right)\right] \quad (15)$$

### *B. Xác suất dừng bảo mật*

Ngoài tham số ASC, một tham số quan trọng khác trong PLS là xác suất dừng bảo mật (SOP), tham số phù hợp nhất cho kịch bản nghe lén thụ động, trong đó nguồn không có bất kỳ thông tin nào về E. Cụ thể hơn, SOP xảy ra khi $C_s$ ở dưới mức độ bảo mật được xác định trước $R_s$. Do đó SOP có thể được thể hiện như sau:

$$P_{SO} = Pr[C_s \le R_s]. \quad (16)$$

Như đã đề cập ở trên, trong truyền thông đường xuống DL, E nằm rất gần H và biểu thức SOP có thể được viết là

$$P_{SO} = P_r[\gamma_H \le 2^{R_s} + 2^{R_s}\gamma_E - 1] = F_{\gamma_H}(2^{R_s} + 2^{R_s}\gamma_E - 1) \quad (17)$$

Qua đó, bằng cách sử dụng (17) SOP có thể được biểu diễn dưới dạng:

$$P_{SO} = \sum_{p=0}^{\infty}\binom{\alpha_E}{p}(-1)^p exp\left[-p\left(\frac{2^{R_s}+2^{R_s}\gamma_E-1}{\eta_H^2\gamma_H}\right)^{\frac{\beta_H}{2}}\right] \quad (18)$$

### *C. Thông lượng bảo mật*

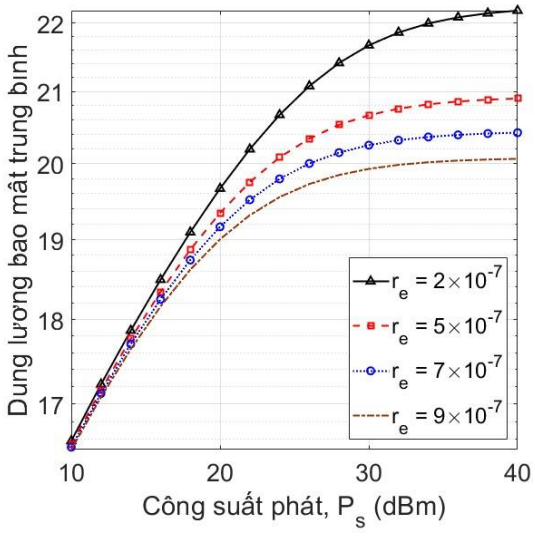
Một yếu tố không kém phần quan trọng trong việc đánh giá hiệu suất bảo mật của phương pháp đề xuất là thông lượng bảo mật (ST). Thông số này thường được áp dụng để mô tả hiệu quả của việc đảm bảo truyền thông đáng tin cậy và an toàn. Về mặt toán học, nó có thể được viết là [13]:

$$ST = R_s(1 - P_{SO}) \quad (19)$$

Các biểu thức của ST cho truyền thông đường xuống có thể dễ dàng thu được bằng cách thay (17) vào (18).

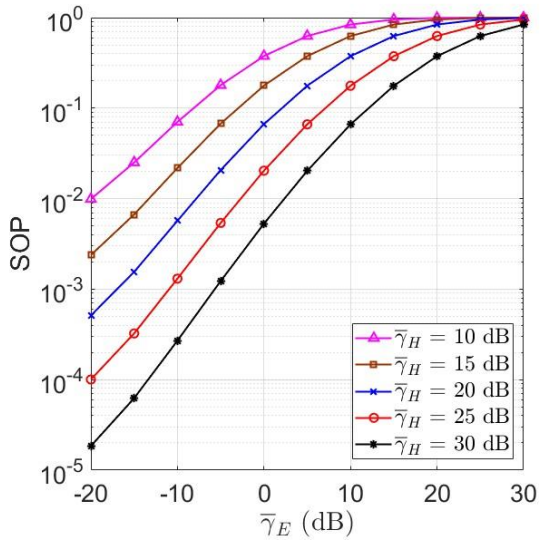
## IV. THẢO LUẬN KẾT QUẢ

Trong phần này, chúng tôi đánh giá hiệu năng bảo mật của vệ tinh bị nghe lén trong kịch bản được đề xuất. Chúng tôi xem xét các thông số như sau: vệ tinh LEO bay quanh quỹ đạo ở độ cao 500 km, trong khi HAPS nằm ở độ cao 20 km. Các góc thiên đỉnh được đặt bằng 30 độ, tốc độ gió được cho là $w_S = w_H = 65$ m/s và tốc độ bảo mật được đặt là $R_s = 0{,}01$ bit/s/Hz. Ngoài ra, các tham số được hiệu chỉnh trong từng ngữ cảnh sẽ được ghi chú trong từng kết quả.



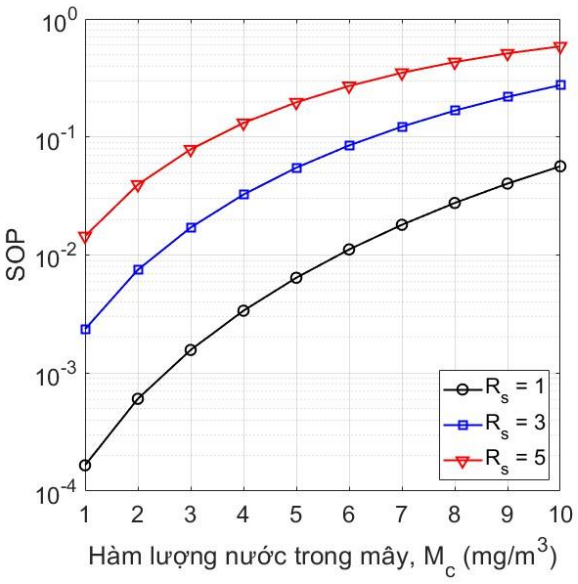

*Hình 3. Khảo sát dung lượng bảo mật trung bình với một khoảng công suất phát.*

Hình 3 khảo sát dung lượng bảo mật trung bình (ASC) của hệ thống được xem xét trong kịch bản nghe lén thụ động trên một dải công suất phát từ 10 dBm tới 40 dBm. Như đã nói trong kịch bản bảo mật hệ thống được xem xét, $r_b$ và $r_e$ tương ứng với kích thước khẩu độ của từng thiết bị cùng với góc phân kỳ chùm tia. Thêm vào đó, thiết bị nghe



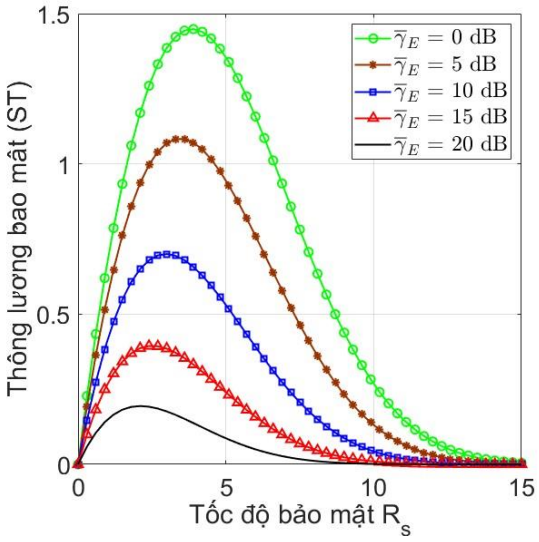

*Hình 4. Xem xét mối quan hệ giữa xác suất dừng bảo mật và SNR của máy nghe lén.*

lén E chỉ có thể thu được một phần nhỏ tín hiệu được truyền đi, trong khi đó máy thu hợp pháp sẽ thu được nhiều năng lượng hơn, do đó, 4 trường hợp của $r_e$ được xét với giá trị nhỏ. Qua kết quả ở đây, chúng ta cũng thấy được rằng ảnh hưởng của việc thu lén năng lượng của E ảnh hưởng lớn tới ASC. Từ kết quả, chúng ta có thể quan sát thấy rằng bằng việc giảm công suất phát hoặc tăng lượng công suất thu được của thiết bị nghe lén, về tổng thể thì ASC sẽ giảm. Ví dụ, với cùng một giá trị của $r_e = 5 \times 10^{-7}$, ASC sẽ giảm từ 20,6 (bits/s/Hz) xuống còn 19,4 (bits/s/Hz) khi ta giảm công suất phát từ 30 dBm về 20 dBm.




*Hình 5. Tác động của mây đến hiệu năng SOP*

Hình 4 cho thấy mối quan hệ giữa xác suất dừng bảo mật và SNR của thiết bị nghe lén trong 5 trường hợp khác nhau của SNR máy thu hợp pháp lần lượt là 10 dB, 15 dB, 20 dB, 25 dB, và 30 dB. Từ kết quả này, chúng ta có thể nhận định một cách nhanh chóng rằng khi SNR trung bình của thiết bị nghe lén tăng lên đã gián tiếp làm tăng xác suất dừng bảo mật. Tuy nhiên, trong những trường hợp này chúng ta có thể tăng SNR trung bình của máy thu hợp pháp




*Hình 6. Tác động của tốc độ bảo mật lên thông lượng bảo mật của hệ thống đã đề xuất.*

lên để có thể giảm xác suất dừng bảo mật. Để thực hiện được kĩ thuật này thì chúng ta có thể làm một trong hai cách sau: (1) chúng ta có thể tăng công suất phát để máy thu hợp pháp có thể thu được nhiều năng lượng hơn từ đó giảm được xác suất dừng bảo mật. Và (2) là tăng tỉ lệ thu tín hiệu, cụ thể ở đây chúng ta sẽ cố gắng tăng $r_b$. Để làm được điều đó chúng ta có thể tăng bán kính khẩu độ máy thu hợp pháp hoặc giảm góc phân kì ở phía phát để giảm diện tích thu từ đó giúp máy thu hợp pháp thu nhiều năng lượng hơn và đồng thời giảm được $r_e$ của máy nghe lén.

Hình 5 biểu diễn sự phụ thuộc của SOP vào hàm lượng nước trong mây trong ba trường hợp thay đổi của $R_s$. Từ kết quả này, ta nhận thấy rằng SOP có xu hướng tăng lên khi hàm lượng nước trong mây tăng lên. Bên cạnh đó, khi ta tăng tốc độ bảo mật lên thì SOP cũng có xu hướng tăng lên. Điều này có thể được giải thích qua công thức (18). Trong trường hợp $R_s$ có giá trị cao ($R_s$ = *5*), SOP tăng không quá nhanh như trong trường hợp $R_s$ có giá trị thấp ($R_s$ = *1*). Điều này cho thấy rằng, SOP có thể đạt ngưỡng bão hòa khi $R_s$ đạt tới giá trị vô cùng lớn.

Cuối cùng, hình 6 phân tích tác động của tốc độ bảo mật lên thông lượng bảo mật của hệ thống được xem xét trong kịch bản thiết bị nghe lén (HAPS) tiếp cận một máy thu hợp pháp (HAPS) trong các trường hợp tỉ lệ SNR của thiết bị nghe lén khác nhau. Như có thể quan sát thấy, ST tăng khi $R_s$ tăng đến một giá trị nhất định rồi giảm dần. Điều này là do sự phụ thuộc của ST trên $R_s$. ST tăng khi $R_s$ tương đối thấp. Tuy nhiên, khi $R_s$ vượt quá một giá trị ngưỡng cụ thể, hệ thống không thể đủ độ tin cậy và bảo mật. Cuối cùng, như mong đợi, việc giảm SNR trung bình của máy nghe lén sẽ cải thiện hiệu năng thông lượng bảo mật của hệ thống.

## V. KẾT LUẬN

Bài báo này đã giới thiệu phương pháp nghe lén vệ tinh, trong đó một tàu vũ trụ nghe lén vệ tinh LEO. Cụ thể, chúng tôi giả sử một vệ tinh LEO liên lạc với nút HAPS trong bối cảnh có một HAPS (thiết bị nghe lén) tấn công nằm rất gần máy thu hợp pháp. Các biểu thức dạng tường minh của SOP, ASC, và ST đã được đưa ra trong nghiên

cứu này. Ngoài ra, kết quả mô phỏng cho thấy truyền thông đường xuống từ vệ tinh đến HAPS an toàn . Thông qua các kết quả của nghiên cứu, chúng ta có thể thấy được rằng để tăng khả năng bảo mật của hệ thống chúng ta có thể tăng công suất phát, giảm góc của chùm tia phân kỳ ở phía phát, tăng tốc độ ký hiệu, điều chỉnh tỷ lệ phân bố công suất, etc.

Các hướng công việc trong tương lai có thể được tóm tắt như sau: Các kỹ thuật PLS chống lại những thiết bị nghe lén không dây như mã hóa nghe lén sẽ được nghiên cứu đồng thời khai thác các đặc điểm kênh cùng với kiến trúc bộ thu phát để hỗ trợ việc truyền dữ liệu giữa những người dùng hợp pháp. Cuối cùng, việc tối ưu hóa thông lượng bảo mật bằng cách điều chỉnh tỷ lệ bảo mật mục tiêu và tỷ lệ phân bổ công suất sẽ được thực hiện.

## TÀI LIỆU THAM KHẢO


[1] N. Yang and A. Shafie, “Terahertz communications for massive connectivity and security in 6G and beyond era,” IEEE Commun. Mag., Oct. 2022,

[2] C.-X. Wang, X. You, X. Gao et al., “On the road to 6G: Visions, requirements, key technologies, and testbeds,” IEEE Commun. SurveysTuts., vol. 25, no. 2, pp. 905–974, Second Quart. 2023.

[3] G. Karabulut Kurt et al., “A vision and framework for the high altitude platform station (HAPS) networks of the future,” IEEE Commun. Surv. Tut., vol. 23, no. 2, pp. 729–779, Apr.–Jun. 2021.

[4] P. Yue *et al*., "Low Earth Orbit Satellite Security and Reliability: Issues, Solutions, and the Road Ahead," in IEEE Communications Surveys & Tutorials, vol. 25, no. 3, pp. 1604-1652, thirdquarter 2023, doi: 10.1109/COMST.2023.3296160.

[5] Y.Ai, A. Mathur,G.D.Verma,L.Kong, ndM.Cheffena, “Comprehensive physical layer security analysis of FSO communications over Málaga channels,” IEEE Photon. J., vol. 12, no. 6, pp. 1–17, Dec. 2020.

[6] F. A. d’Oliveira, F. C. L. d. Melo, and T. C. Devezas, “High-altitude platforms–present situation and technology trends,” J. Aerosp. Technol. Manage., vol. 8, no. 3, pp. 249–262, 2016.

[7] Y. Shi, Y. Gao, and Y. Xia, “Secrecy performance analysis in internet of satellites: Physical layer security perspective,” in Proc. Int.Conf.Commun. China, 2020, pp. 1185–1189

[8] R. Boluda-Ruiz and K. Qaraqe, “Effect of misalignment error on secrecy outage capacity of FSO communication links,” in Proc. IEEE Wireless Commun. Netw. Conf., 2019, pp. 1–7.

[9] P. Wang, J. Zhang, X. Zhang, Z. Yan, B. G. Evans and W. Wang, "Convergence of Satellite and Terrestrial Networks: A Comprehensive Survey," in IEEE Access, vol. 8, pp. 5550-5588, 2020, doi: 10.1109/ACCESS.2019.2963223.

[10] Henri, Y. (2020). The OneWeb satellite system. In Handbook of Small Satellites: Technology, Design, Manufacture, Applications, Economics and Regulation (pp. 1091-1100). Cham: Springer International Publishing.

[11] Z. Tan, H. Qin, L. Cong and C. Zhao, "New Method for Positioning Using IRIDIUM Satellite Signals of Opportunity," in IEEE Access, vol. 7, pp. 83412-83423, 2019, doi: 10.1109/ACCESS.2019.2924470.

[12] F. J. Dietrich, P. Metzen and P. Monte, "The Globalstar cellular satellite system," in IEEE Transactions on Antennas and Propagation, vol. 46, no. 6, pp. 935-942, June 1998, doi: 10.1109/8.686783.

[13] O. B. Yahia, E. Erdogan, G. K. Kurt, I. Altunbas and H. Yanikomeroglu, "Optical Satellite Eavesdropping," in IEEE Transactions on Vehicular Technology, vol. 71, no. 9, pp. 10126-10131, Sept. 2022, doi: 10.1109/TVT.2022.3176119.

[14] B. Li, Z. Fei, C. Zhou and Y. Zhang, "Physical-Layer Security in Space Information Networks: A Survey," in IEEE Internet of Things Journal, vol. 7, no. 1, pp. 33-52, Jan. 2020, doi: 10.1109/JIOT.2019.2943900.

[15] K Guo, K. An, Y. Huang and B. Zhang, "Physical Layer Security of Multiuser Satellite Communication Systems With Channel Estimation Error and Multiple Eavesdroppers," in IEEE Access, vol. 7, pp. 96253-96262, 2019, doi: 10.1109/ACCESS.2019.2928751.

[16] R . Wang and F. Zhou, "Physical Layer Security for Land Mobile Satellite Communication Networks With User Cooperation," in IEEE Access, vol. 7, pp. 29495-29505, 2019, doi: 10.1109/ACCESS.2019.2902716.

[17] Y. Ai, A. Mathur, G. D. Verma, L. Kong and M. Cheffena, "Comprehensive Physical Layer Security Analysis of FSO Communications Over Málaga Channels," in IEEE Photonics Journal, vol. 12, no. 6, pp. 1-17, Dec. 2020, Art no. 7906617, doi: 10.1109/JPHOT.2020.3036244.

[18] O. M. Adewusi, T. V. Omotosho, M. L. Akinyemi, S. A. Akinwumi and O. O. Ometan, "Four Year Cloud Attenuation Study in a Tropical Station," 2019 IEEE International Symposium on Antennas and Propagation and USNC-URSI Radio Science Meeting, Atlanta, GA, USA, 2019, pp. 2105-2106, doi: 10.1109/APUSNCURSINRSM.2019.8889375.

[19] Olurotimi, Elijah Olusayo. "Combined tropospheric attenuation along satellite path at SHF and EHF bands in subtropical region." PhD diss., 2019.

[20] Hoang D. Le, Thang V. Nguyen, and Anh T. Pham, “cloud attenuation statistical model for satellite-based FSO communication,” IEEE Antennas wireless propagation letter, vol. 20, no. 5, pp. 643-647, 2021,doi: 10.1109/LAWP.2021.3058641.


## PERFORMANCE EVALUATION OF SECURITY IN COMMUNICATIONS BETWEEN LEO SATELLITES AND HIGH ALTITUDE PLATFORM STATIONS


***Abstract***: This paper focuses on studying and evaluating security performance in optical communications between satellites (LEO) and overhead infrastructure (HAPS). Specifically, the study analyzes the eavesdropping scenario for downlink communications from LEO satellites to HAPS. To quantify the security performance of the scenario, the average security capacity, security stall probability, and security throughput are given as explicit formulas in this study. Through the results of the study, we can see that to increase the security of the system we can increase the transmit power, reduce the angle of the divergent beam at the transmit side, and increase the symbol speed, adjust the power distribution ratio.

**Nguyễn Thị Thu Nga** nhận được bằng kỹ sư Điện tử và Viễn thông tại Đại học Bách Khoa Hà Nội, Việt Nam năm 1999 và bằng Thạc sĩ tại Đại học Công nghệ, Đại học Quốc gia Việt Nam năm 2005, nhận bằng tiến sĩ năm 2021 tại Học viện công nghệ Bưu chính Viễn Thông (PTIT). Cô hiện tại là giảng viên Khoa Viễn thông 1, Học viện công nghệ Bưu chính Viễn Thông. Mối quan tâm nghiên cứu hiện tại của cô là trong lĩnh vực truyền thông quang, thiết kế và đánh giá hiệu năng của các hệ thống truyền thông quang không dây.