

NGHIÊN CỨU HIỆU NĂNG BẢO MẬT LỚP VẬT LÝ CHO MẠNG CHUYỂN TIẾP LAI GHÉP VỆ TINH-MẶT ĐẤT DƯỚI SỰ TÁC ĐỘNG CỦA NHIỀU ĐỒNG KÊNH VÀ NHIỀU PHẦN CỨNG

Đặng Thế Hùng*, Lê Chu Khấn[†], Nguyễn Văn Toàn[#], Đỗ Quốc Trinh*

* Học Viện Kỹ Thuật Quân Sự

[†]Học Viện Công Nghệ Bưu Chính Viễn Thông cơ sở tại TP. Hồ Chí Minh

[#] Đại Học Thông Tin Liên Lạc, Thành Phố Nha Trang

Tóm tắt: Bài báo này nghiên cứu mạng chuyển tiếp lai ghép vệ tinh-mặt đất với sự xuất hiện của một thiết bị nghe lén. Trong mô hình nghiên cứu, dữ liệu từ vệ tinh sẽ được gửi xuống các trạm mặt đất, và một trong các trạm mặt đất sẽ làm nhiệm vụ chuyển tiếp dữ liệu này đến một nhóm các người dùng hợp pháp. Thiết bị nghe lén được đặt ở vị trí thích hợp để có thể nghe lén trực tiếp từ vệ tinh hoặc nghe lén từ trạm chuyển tiếp mặt đất được chọn. Để có thể bảo mật dữ liệu, bài báo đề xuất triển khai các trạm tạo nhiễu nhân tạo gần các trạm mặt đất và gần những người dùng hợp pháp để tạo nhiễu lên thiết bị nghe lén. Mặt khác, các trạm tạo nhiễu này có thể phối hợp với các trạm mặt đất và những người dùng hợp pháp để khử giao thoa do chúng tạo ra. Hơn thế nữa, nhiễu gây ra do khiếm khuyết phần cứng tại những người dùng hợp pháp, và giao thoa đồng kênh do quá trình tái sử dụng tần số cũng được xem xét khi đánh giá và phân tích hiệu năng của mô hình. Cụ thể, bài báo đưa ra các công thức toán học đánh giá chính xác xác suất dừng tại những người dùng hợp pháp, và xác suất giải mã thành công dữ liệu (xác suất chặn) tại thiết bị nghe lén. Cuối cùng, các kết quả sẽ được thể hiện để thấy được những xu hướng hiệu năng của mô hình nghiên cứu, cũng như sự tác động của các thông số hiệu năng.

Từ khóa: Mạng chuyển tiếp lai ghép vệ tinh-mặt đất, bảo mật lớp vật lý, khiếm khuyết phần cứng, giao thoa đồng kênh, xác suất dừng, xác suất chặn.

I. GIỚI THIỆU

Thông tin vệ tinh hay truyền thông vệ tinh (satellite communications) [1] đang nhận được nhiều sự quan tâm của các nhà nghiên cứu trong và ngoài nước. Sự phát triển của thông tin vệ tinh mang lại nhiều lợi ích trong đời sống xã hội hiện nay như thương mại, y tế, giáo dục, giao thông, v.v. Bởi khả năng cung cấp đa dạng các dịch vụ, khả năng kết nối nhanh chóng, ổn định với tốc độ cao, thông tin vệ tinh đang trở thành một lĩnh vực đầy tiềm năng trong hiện tại và tương lai gần. Trong thông tin

vệ tinh, một trạm mặt đất (terrestrial station) có thể liên lạc với bất cứ trạm mặt đất nào khác thông qua các vệ tinh được phóng lên quỹ đạo. Do đó, vệ tinh đóng vai trò như thiết bị chuyển tiếp cho các trạm dưới mặt đất. Trong công trình [2], các tác giả đánh giá xác suất dừng (OP: Outage Probability) cho mạng truyền thông giữa hai trạm mặt đất thông qua vệ tinh. Với sự xuất hiện của LOS (Line of Sight), độ lợi kênh truyền giữa các trạm mặt đất và vệ tinh được mô tả bằng các biến ngẫu nhiên có phân phối Shadowed-Rician [2]. Hơn nữa, các tác giả trong tài liệu [2] cũng quan tâm đến sự ảnh hưởng của nhiễu gây ra bởi khiếm khuyết phần cứng (HIs: Hardware Impairments). Như đã đề cập và phân tích trong các công bố [2]-[4], nhiễu pha, sự mất cân bằng I/Q, bộ khuếch đại không tuyến tính, v.v., gây ra HIs và làm suy giảm đáng kể hiệu năng của hệ thống. Trong công trình [5], nhóm tác giả nghiên cứu và phân tích hiệu năng của mạng chuyển tiếp lai ghép vệ tinh-mặt đất (HSTRN: Hybrid Satellite-Terrestrial Relay Network). Trong mạng HSTRN, bởi vì các thiết bị đầu cuối không thể trực tiếp nhận dữ liệu từ vệ tinh (do bị che khuất), nên các trạm mặt đất được triển khai để làm nhiệm vụ chuyển tiếp dữ liệu từ vệ tinh đến các thiết bị này. Tương tự như [2], công trình [5] cũng nghiên cứu sự tác động của HIs lên hiệu năng OP của mạng HSTRN. Hơn nữa, trong tài liệu [5], một hoặc nhiều trạm mặt đất được chọn để chuyển tiếp dữ liệu từ vệ tinh đến người dùng. Tương tự [5], mô hình HSTRN kết hợp với kỹ thuật chọn lựa trạm mặt đất được đề xuất trong công trình [6] để nâng cao hiệu năng OP của mạng. Điểm mới của công trình [6] đó là nhóm tác giả khảo sát sự ảnh hưởng của việc thông tin trạng thái kênh truyền đã thay đổi (outdated channel state information (CSI)) trong tiến trình chọn lựa trạm chuyển tiếp mặt đất tốt nhất, cũng như đề xuất áp dụng kỹ thuật kết hợp tỷ lệ tối đa (MRC: Maximal Ratio Combining) cho các trạm mặt đất được trang bị nhiều anten.

Do tính chất quảng bá của kênh thông tin, bảo mật là vấn đề then chốt trong thông tin vệ tinh nói riêng và trong truyền thông vô tuyến nói chung. Gần đây, kỹ thuật bảo mật lớp vật lý (PLS: Physical-Layer Security) [7]-[8] đang trở thành một chủ đề "nóng" bởi sự đơn giản nhưng hiệu quả trong bảo mật thông tin. Kỹ thuật PLS sử dụng các yếu tố của kênh vật lý như khoảng cách, chất lượng

Tác giả liên hệ: Đặng Thế Hùng
Email: danghung8384@gmail.com

Đến tòa soạn: 11/2020, chỉnh sửa: 12/2020, chấp nhận đăng: 12/2020.

kênh truyền, giao thoa và nhiễu để bảo mật dữ liệu. Trong công trình [8], kỹ thuật tạo nhiễu nhân tạo (cooperative jamming (CJ) technique) được thực hiện để làm giảm tỷ số SNR (Signal-to-Noise Ratio) đạt được tại các nút nghe lén. Trong kỹ thuật CJ [8]-[9], các nút tạo nhiễu (jammer) sẽ được sử dụng để phát nhiễu lên các nút nghe lén, và mặt khác, chúng sẽ hợp tác với các thiết bị thu hợp pháp để khử giao thoa gây ra. Do đó, kỹ thuật CJ sẽ làm giảm đáng kể chất lượng kênh nghe lén, trong khi vẫn giữ nguyên chất lượng của kênh dữ liệu. Để đánh giá hiệu năng bảo mật của các kỹ thuật PLS, dung lượng bảo mật (Secrecy Capacity) [8]-[9] thường được sử dụng. Dung lượng bảo mật là một đại lượng không âm và được tính bằng hiệu giữa dung lượng kênh dữ liệu và dung lượng kênh nghe lén. Khác với [8]-[9], các tài liệu [10]-[11] đánh giá sự đánh đổi giữa bảo mật và độ tin cậy của việc truyền dữ liệu thông qua đại lượng xác suất chặn (IP: Intercept Probability) của kênh nghe lén và xác suất dừng OP của kênh dữ liệu.

Vấn đề bảo mật thông tin trong truyền thông vệ tinh-mặt đất cũng đang là chủ đề mới. Trong tài liệu [12], nhóm tác giả nghiên cứu quá trình truyền dữ liệu giữa một vệ tinh và một trạm mặt đất, với sự xuất hiện của một nhóm các thiết bị nghe lén. Để đánh giá hiệu năng bảo mật, nhóm tác giả trong [12] đã phân tích xác suất dung lượng bảo mật khác không (Probability of Non-zero Secrecy Capacity) cho mô hình. Công trình [13] nghiên cứu mô hình PLS cho truyền thông vệ tinh-mặt đất với nhiều trạm thu mặt đất và nhiều trạm nghe lén. Các tác giả trong [13] đã đề xuất mô hình cộng tác cho các trạm thu mặt đất nhằm nâng cao độ tin cậy của việc nhận dữ liệu từ vệ tinh. Mặt khác, tài liệu [13] cũng xem xét hai mô hình nghe lén phổ biến trong PLS, đó là mô hình các nút nghe lén độc lập (non-colluding scheme), và mô hình nghe lén cộng tác (colluding scheme). Khác với [12]-[13], công trình [14] khảo sát mô hình truyền vệ tinh-mặt đất ngẫu nhiên, trong đó người dùng hợp pháp và người nghe lén xuất hiện ngẫu nhiên trong vùng phủ của vệ tinh. Trong tài liệu [15], các tác giả nghiên cứu hiệu năng bảo mật của mạng HSTRN với sự xuất hiện của nhiều người nghe lén. Cụ thể hơn, trạm mặt đất trong [15] sẽ chuyên tiếp dữ liệu từ vệ tinh đến người dùng sử dụng kỹ thuật giải mã chuyên tiếp (DF: Decode and Forward) hoặc khuếch đại chuyên tiếp (AF: Amplify and Forward). Mô hình của công trình [15] được phát triển thành mô hình với nhiều người dùng và nhiều người nghe lén được đề xuất trong công trình [16]. Nhóm tác giả của công trình [16] cũng đã đưa ra mô hình chuyên tiếp AF và kỹ thuật chọn lựa người dùng hợp pháp tốt nhất. Tổng quát hơn các công trình [15] và [16], tài liệu [17] nghiên cứu mô hình HSTRN với nhiều trạm chuyên tiếp mặt đất, nhiều nút thu hợp pháp và nhiều nút nghe lén. Hơn thế nữa, các tác giả của [17] đề xuất các giao thức chọn lựa trạm chuyên tiếp và người dùng tối ưu, đồng thời cũng khảo sát cả mô hình nghe lén độc lập và nghe lén hợp tác. Trong mô hình HSTRN được nghiên cứu trong công trình [18], nút nghe lén có thể nghe lén thông tin trực tiếp từ vệ tinh và từ các trạm chuyên tiếp mặt đất. Do đó, để giảm xác suất dừng bảo mật, các tác giả của [18] đã đưa ra các giải pháp chọn lựa nút chuyên tiếp hiệu quả để nâng cao chất lượng cho kênh dữ liệu.

Bài báo này nghiên cứu vấn đề PLS cho mạng HSTRN, trong đó một trong những trạm mặt đất sẽ được chọn để gửi dữ liệu quảng bá từ vệ tinh đến một nhóm

các người dùng, sử dụng kỹ thuật DF. Để bảo mật thông tin khi có sự xuất hiện của trạm nghe lén dưới mặt đất, bài báo đề xuất áp dụng kỹ thuật tạo nhiễu nhân tạo CJ. Cụ thể, các trạm tạo nhiễu sẽ được triển khai để đảm bảo sự truyền dữ liệu an toàn giữa vệ tinh và các trạm mặt đất, và giữa trạm mặt đất được chọn và những người dùng hợp pháp. Những điểm mới, điểm khác biệt so với các công trình hiện có, và những đóng góp chính của bài báo sẽ được tóm tắt như bên dưới:

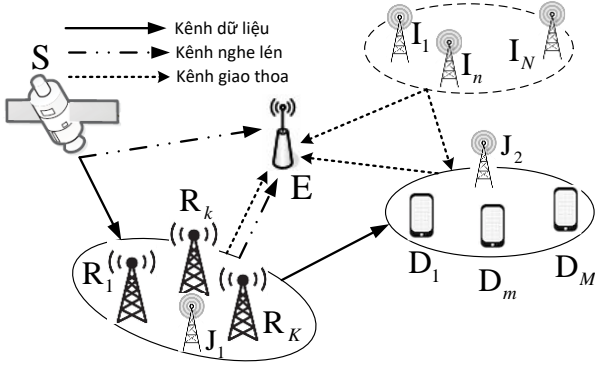
- Điểm khác biệt đầu tiên khi so sánh với các công trình liên quan [15]-[18], đó là bài báo này đề xuất kỹ thuật tạo nhiễu nhân tạo để bảo vệ thông tin nhận được tại các trạm mặt đất và những người dùng hợp pháp. Điểm mới tiếp theo trong mô hình đề xuất là mô hình quảng bá đa người dùng, trong đó vệ tinh gửi dữ liệu đồng thời đến một nhóm người dùng mong muốn. Thật vậy, mô hình đề xuất này khác với mô hình chọn lựa người dùng tốt nhất để truyền dữ liệu trong các tài liệu [16]-[17].
- Bài báo nghiên cứu mô hình thực tế khi phần cứng tại những người dùng hợp pháp là không hoàn hảo. Hơn nữa, giao thoa đồng kênh (CI: Co-channel Interference) do quá trình tái sử dụng tần số dưới mặt đất cũng được xem xét khi đánh giá hiệu năng OP và IP của mô hình. Đây cũng là những điểm mới của bài báo khi so sánh với các công trình liên quan [15]-[18].
- Bên cạnh việc đề xuất mô hình mới, đóng góp quan trọng khác của công trình này là đưa ra các biểu thức toán học đánh giá chính xác OP cho kênh dữ liệu và IP cho kênh nghe lén. Các công thức đưa ra đều ở dạng tường minh (closed form) nên có thể được sử dụng hiệu quả trong quá trình phân tích và tối ưu hệ thống.
- Các kết quả được đưa ra để cho thấy những ưu điểm nổi bật của mô hình đề xuất, cũng như cho thấy được xu hướng các hiệu năng theo sự thay đổi của các thông số hệ thống.

Phần còn lại của bài báo được tổ chức như sau: trong phần II, nguyên lý hoạt động của mô hình hệ thống nghiên cứu sẽ được trình bày. Trong phần III, bài báo đánh giá các thông số hiệu năng OP và IP bằng các biểu thức toán học. Phần IV cung cấp các kết quả phân tích lý thuyết. Cuối cùng, các kết luận và hướng phát triển được đưa ra trong phần V.

II. MÔ HÌNH HỆ THỐNG

Hình 1 mô tả mô hình mạng HSTRN được nghiên cứu trong bài báo. Trong mô hình này, vệ tinh S đóng vai trò là nút nguồn muốn gửi dữ liệu đến M nút đích, ký hiệu là D_1, D_2, \dots, D_M , với $M \geq 1$. Do bị che khuất, các nút đích này không thể nhận trực tiếp dữ liệu từ vệ tinh, và do đó, các trạm chuyên tiếp mặt đất sẽ chuyên tiếp dữ liệu từ vệ tinh đến các đích. Như trong Hình 1, ta giả sử có K trạm mặt đất, ký hiệu là R_1, R_2, \dots, R_K , ($K \geq 1$), sẽ thu dữ liệu từ vệ tinh S, rồi tiến hành gửi dữ liệu đến các nút đích, theo phương pháp giải mã và chuyên tiếp (DF). Trong mạng, xuất hiện một nút nghe lén E; nút này đang cố gắng nghe lén dữ liệu của vệ tinh gửi đến các nút đích. Nút E sẽ chọn vị trí thích hợp để nghe lén dữ liệu trực tiếp từ vệ tinh và từ các trạm chuyên

tiếp mặt đất. Để bảo mật dữ liệu theo kỹ thuật CJ, các trạm tạo nhiễu nhân tạo, được ký hiệu là J_1 và J_2 , sẽ lần lượt được triển khai gần các trạm chuyển tiếp mặt đất và gần các nút đích. Ta cũng giả sử rằng các nút đích và nút nghe lén chịu ảnh hưởng của nhiễu đồng kênh gây ra bởi N nguồn giao thoa được ký hiệu I_1, I_2, \dots, I_N , với $N \geq 1$. Sự xuất hiện của các nguồn giao thoa là do việc sử dụng tái sử dụng tần số dưới mặt đất.



Hình 1. Mô hình bảo mật lớp vật lý trong HSTRN.

Bảng 1. Tóm tắt các ký hiệu toán học

Ký hiệu	Ý nghĩa
K	Số trạm mặt đất
M	Số người dùng hợp pháp
N	Số nguồn gây giao thoa đồng kênh
$P_X (X \in \{S, R, J_1, J_2, I\})$	Công suất phát của nút phát X
σ_0^2	Phương sai của nhiễu cộng
$\Delta_X (X \in \{S, R, J_1, J_2\})$	Tỷ số SNR phát bằng P_X / σ_0^2
$h_{X,Y}, l_{X,Y} (X, Y \in \{S, R_k, J_1, J_2, I_n, E\})$	Hệ số kênh giữa X và Y
κ^2	Mức suy hao phản cứng

Xét sự truyền dữ liệu ở pha đầu tiên, trong đó vệ tinh S gửi dữ liệu xuống các trạm mặt đất. Cùng lúc đó, nút E nghe lén dữ liệu và trạm J_1 phát nhiễu nhân tạo lên nút E. Bởi vì J_1 ở gần các trạm $R_k (k = 1, 2, \dots, K)$, nên J_1 và R_k có thể phối hợp với nhau để loại bỏ giao thoa mà J_1 gây ra cho R_k (xem các tài liệu [8]-[10]). Do đó, tín hiệu nhận được tại R_k trong pha đầu tiên này được viết ra như sau:

$$y_{R_k} = \sqrt{P_S} h_{S,R_k} x + n_{R_k}, \quad (1)$$

với P_S là công suất phát của S, h_{S,R_k} là hệ số kênh truyền giữa S và R_k , x là tín hiệu của S, n_{R_k} là nhiễu Gauss trắng cộng tính (AWGN: Additive White Gaussian Noise) tại R_k với giá trị trung bình bằng 0 và phương sai bằng

σ_0^2 . Để đơn giản về mặt ký hiệu, ta sẽ dùng ký hiệu σ_0^2 cho phương sai của AWGN tại tất cả các thiết bị thu.

Từ công thức (1), tỷ số SNR đạt được tại R_k để giải mã dữ liệu của vệ tinh S được viết ra như sau:

$$\gamma_{R_k} = \frac{P_S |h_{S,R_k}|^2}{\sigma_0^2} = \Delta_S X_{R_k}, \quad (2)$$

với $\Delta_S = P_S / \sigma_0^2$ và $X_{R_k} = |h_{S,R_k}|^2$ là độ lợi kênh truyền.

Tương tự [2], [18], độ lợi kênh X_{R_k} sẽ có phân phối Shadowed-Rician, và hàm mật độ xác suất (PDF: Probability Density Function) của X_{R_k} được viết như sau:

$$f_{X_{R_k}}(x) = \frac{1}{2b_k} \left(\frac{2m_k b_k}{2m_k b_k + \Omega_k} \right)^{m_k} \exp\left(-\frac{x}{2b_k}\right) \times {}_1F_1\left(m_k; 1; \frac{\Omega_k x}{2b_k(2m_k b_k + \Omega_k)}\right), \quad (3)$$

với Ω_k là công suất trung bình của thành phần LOS trong liên kết giữa S và R_k , $2b_k$ là công suất trung bình của thành phần đa đường (multi-path), m_k là tham số đặc trưng Nakagami của kênh truyền, và ${}_1F_1(\cdot; \cdot; \cdot)$ là hàm confluent hypergeometric [19]. Để thuận tiện cho việc ký hiệu và phân tích, ta giả sử rằng các liên kết S- R_k là độc lập và đồng đều, cụ thể: $\Omega_k = \Omega_R$, $b_k = b_R$, $m_k = m_R$ với $\forall k$.

Bởi vì nút nghe lén E không thể loại bỏ giao thoa do nút tạo nhiễu J_1 gây ra nên tín hiệu nhận được tại E được viết ra như sau:

$$y_E = \sqrt{P_S} h_{S,E} x + \sqrt{P_{J_1}} l_{J_1,E} u_1 + n_E, \quad (4)$$

với P_{J_1} là công suất phát của nút tạo nhiễu J_1 , $h_{S,E}$ là hệ số kênh truyền giữa S và E, u_1 là tín hiệu của J_1 , n_E là AWGN tại E với giá trị trung bình bằng 0 và phương sai bằng σ_0^2 .

Từ công thức (4), tỷ số SINR (SINR: Signal-to-Interference-plus-Noise Ratio) đạt được tại E để giải mã dữ liệu từ vệ tinh là:

$$\gamma_E = \frac{P_S |h_{S,E}|^2}{P_{J_1} |l_{J_1,E}|^2 + \sigma_0^2} = \frac{\Delta_S X_E}{\Delta_{J_1} Z_{J_1} + 1}, \quad (5)$$

với $\Delta_{J_1} = P_{J_1} / \sigma_0^2$, $X_E = |h_{S,E}|^2$ và $Z_{J_1} = |l_{J_1,E}|^2$. Tương tự, độ lợi kênh X_E cũng có phân phối Shadowed-Rician, và hàm PDF của X_E được viết ra như sau:

$$f_{X_E}(x) = \frac{1}{2b_E} \left(\frac{2m_E b_E}{2m_E b_E + \Omega_E} \right)^{m_E} \exp\left(-\frac{x}{2b_E}\right) \times {}_1F_1\left(m_E; 1; \frac{\Omega_E x}{2b_E(2m_E b_E + \Omega_E)}\right), \quad (6)$$

với Ω_E là công suất trung bình của thành phần LOS, $2b_E$ là công suất trung bình của thành phần đa đường (multi-path), m_E là tham số đặc trưng Nakagami của kênh truyền.

Đối với liên kết giữa J_1 và E, kênh truyền này được mô hình bằng kênh pha đỉnh Rayleigh. Do đó, độ lợi kênh Z_{J_1} sẽ có phân phối mũ với hàm PDF như sau:

$$f_{Z_{J_1}}(z) = \lambda_{J_1,E} \exp(-\lambda_{J_1,E}z), \quad (7)$$

với $\lambda_{J_1,E}$ bằng nghịch đảo giá trị trung bình của Z_{J_1} . $\lambda_{J_1,E}$ cũng được gọi là tham số đặc trưng của biến ngẫu nhiên có phân phối mũ Z_{J_1} .

Giả sử rằng, các thiết bị thu R_k và E sẽ giải mã thành công dữ liệu nếu tỷ số SNR (SINR) đạt được tại các nút này lớn hơn một ngưỡng xác định trước, ký hiệu là $\omega_{1,th}$. Ngược lại, nếu tỷ số SNR (SINR) tại R_k và E thấp hơn ngưỡng $\omega_{1,th}$ thì R_k và E không thể giải mã thành công dữ liệu.

Sau quá trình giải mã dữ liệu, trong K trạm mặt đất, sẽ có một số trạm giải mã thành công dữ liệu từ vệ tinh S, và những trạm còn lại sẽ giải mã không thành công. Không mất tính tổng quát, ta có thể giả sử rằng có v trạm giải mã thành công, đó là R_1, R_2, \dots, R_v , và những trạm giải mã không thành công là $R_{v+1}, R_{v+2}, \dots, R_K$, với $0 \leq v \leq K$. Do đó, xác suất để xảy ra sự kiện số trạm giải mã thành công bằng v được viết ra như sau:

$$\begin{aligned} Q_v &= \Pr \left(\begin{array}{l} \gamma_{R_1} \geq \omega_{1,th}, \dots, \gamma_{R_v} \geq \omega_{1,th}, \\ \gamma_{R_{v+1}} < \omega_{1,th}, \dots, \gamma_{R_K} < \omega_{1,th} \end{array} \right) \\ &= \left[\prod_{u=1}^v \Pr(\gamma_{R_u} \geq \omega_{1,th}) \right] \times \left[\prod_{u=v+1}^K \Pr(\gamma_{R_u} < \omega_{1,th}) \right] \quad (8) \\ &= \left[1 - \Pr(\gamma_{R_u} < \omega_{1,th}) \right]^v \times \left[\Pr(\gamma_{R_u} < \omega_{1,th}) \right]^{K-v}. \end{aligned}$$

Ta xét trường hợp đặc biệt $v=0$, tức là không có trạm chuyển tiếp R_k nào có thể nhận được thành công dữ liệu từ vệ tinh. Trong trường hợp này, sẽ không có bất cứ trạm nào có thể chuyển tiếp dữ liệu đến các nút đích, và hệ thống sẽ bị dừng trong trường hợp này. Ngược lại, với $v \geq 1$, thì một trong các trạm chuyển tiếp thành công sẽ được chọn để chuyển tiếp dữ liệu từ vệ tinh đến các nút đích (phương pháp chọn trạm chuyển tiếp tốt nhất để phục vụ các nút đích sẽ được trình bày cụ thể trong pha thứ hai).

Xét sự giải mã dữ liệu tại nút nghe lén E; nút này giải mã thành công khi $\gamma_E \geq \omega_{1,th}$; và không thành công khi $\gamma_E < \omega_{1,th}$. Khi mà E giải mã thành công, điều này cũng có nghĩa là dữ liệu đã bị mất bảo mật.

Trước khi mô tả việc truyền nhận dữ liệu trong pha 2, chúng ta có một số lưu ý sau: đầu tiên, bởi vì các thiết bị như vệ tinh, các trạm mặt đất và nút nghe lén thường được trang bị với các phần cứng đắt tiền, do đó, ta có thể giả sử rằng nhiễu gây ra do khiếm khuyết tại các thiết bị này là rất nhỏ và có thể bỏ qua (xem tài liệu [20]). Kế tiếp,

ta cũng giả sử không có nhiễu đồng kênh tác động lên các trạm chuyển tiếp mặt đất cũng như nút nghe lén trong pha đầu tiên, bởi không có sự tái sử dụng đối với các băng tần sử dụng trong vệ tinh.

Xét pha thứ hai; giả sử rằng trạm R_k được chọn để gửi dữ liệu đến các đích D_m ($m=1, 2, \dots, M$). Nút nghe lén E cũng sẽ cố gắng nghe lén và giải mã dữ liệu được gửi đi từ trạm R_k . Dưới sự tác động của nhiễu phần cứng tại đích D_m và giao thoa đồng kênh từ các nguồn nhiễu I_n ($n=1, 2, \dots, N$), tín hiệu nhận được tại đích D_m được viết ra như sau:

$$z_{D_m} = \sqrt{P_R} h_{R_k, D_m} (x + \chi_{D_m}) + \sum_{n=1}^N \sqrt{P_I} l_{I_n, D_m} w_n + n_{D_m}. \quad (9)$$

Trong công thức (9), P_R là công suất phát của trạm R_k (giả sử tất cả các trạm chuyển tiếp mặt đất có công suất phát giống nhau), và P_I là công suất phát của các nguồn nhiễu đồng kênh. h_{R_k, D_m} và l_{I_n, D_m} lần lượt là kênh pha đỉnh Rayleigh của các liên kết $R_k \rightarrow D_m$ và $I_n \rightarrow D_m$. w_n là tín hiệu của I_n , n_{D_m} là AWGN tại D_m với giá trị trung bình bằng 0 và phương sai bằng σ_0^2 . χ_{D_m} là nhiễu gây ra do khiếm khuyết phần cứng tại D_m . Như đã được đề cập trong các công trình [3], [4], [10], [20], χ_{D_m} cũng là một biến ngẫu nhiên có phân bố Gauss với giá trị trung bình bằng 0 và phương sai là κ^2 , với κ^2 là một hằng số mô tả mức khiếm khuyết phần cứng. Trong trường hợp mà phần cứng là lý tưởng thì $\kappa^2 = 0$.

Từ công thức (9), tỷ số SINR đạt được tại nút đích D_m để giải mã dữ liệu nhận được từ R_k sẽ được viết ra như sau:

$$\begin{aligned} \varphi_{R_k, D_m} &= \frac{P_R |h_{R_k, D_m}|^2}{\kappa^2 P_R |h_{R_k, D_m}|^2 + \sum_{n=1}^N P_I |l_{I_n, D_m}|^2 + \sigma_0^2} \\ &= \frac{\Delta_R Y_{D_m}}{\kappa^2 \Delta_R Y_{D_m} + \sum_{n=1}^N \Delta_I T_{I_n, D_m} + 1} \end{aligned} \quad (10)$$

$$\text{với } \Delta_R = P_R / \sigma_0^2, \quad \Delta_I = P_I / \sigma_0^2, \quad Y_{D_m} = |h_{R_k, D_m}|^2, \quad T_{I_n, D_m} = |l_{I_n, D_m}|^2.$$

Ta cũng lưu ý rằng trong pha thứ hai này, nút tạo nhiễu J_2 cũng đang phát nhiễu lên nút nghe lén E. Tuy nhiên, do J_2 được đặt gần các nút đích D_m , nên J_2 và D_m có thể phối hợp với nhau để loại bỏ giao thoa mà J_2 gây ra [8]-[10].

Đối với các độ lợi kênh Y_{D_m} và T_{I_n, D_m} , chúng đều có phân phối mũ và hàm PDF của Y_{D_m} và T_{I_n, D_m} lần lượt được viết ra như sau:

$$f_{Y_{D_m}}(y) = \lambda_{R_k, D_m} \exp(-\lambda_{R_k, D_m} y), \quad (11)$$

$$f_{T_{I_n, D_m}}(t) = \lambda_{I_n, D_m} \exp(-\lambda_{I_n, D_m} t), \quad (12)$$

với λ_{R_k, D_m} và λ_{I_n, D_m} lần lượt là các tham số đặc trưng của các biến ngẫu nhiên Y_{D_m} và T_{I_n, D_m} .

Giả sử các biến ngẫu nhiên Y_{D_m} và T_{I_n, D_m} là độc lập và đồng đều, ta có: $\lambda_{R_k, D_m} = \lambda_{R, D}$ và $\lambda_{I_n, D_m} = \lambda_{I, D}$ với $\forall m, n, k$. Bây giờ, các công thức (11) và (12) sẽ được viết lại như sau:

$$f_{Y_{D_m}}(y) = \lambda_{R, D} \exp(-\lambda_{R, D} y), \quad (13)$$

$$f_{T_{I_n, D_m}}(t) = \lambda_{I, D} \exp(-\lambda_{I, D} t). \quad (14)$$

Bởi vì dữ liệu từ vệ tinh được gửi quảng bá đến M người dùng nên ta sẽ quan tâm đến người dùng có SINR thấp nhất (xem [21]), cụ thể:

$$D_r : \varphi_{R_k, D_r} = \min_{m=1, 2, \dots, M} (\varphi_{R_k, D_m}), \quad (15)$$

với $r=1, 2, \dots, M$. Như đã đề cập trong [21], nút D_r là nút đích có SINR thấp nhất, và sẽ là nút được quan tâm trong mạng quảng bá bởi vì xác suất dừng tại nút này sẽ là lớn nhất. Hơn thế nữa, nếu nút D_r giải mã thành công dữ liệu thì tất cả những nút còn lại cũng sẽ giải mã thành công dữ liệu.

Từ công thức (15), bài báo đề xuất phương pháp chọn trạm chuyển tiếp tốt nhất để phục vụ cho M người dùng như sau:

$$\begin{aligned} R_k : \varphi_{R_k, D_r} &= \max_{u=1, 2, \dots, v} (\varphi_{R_u, D_r}) \\ &= \max_{u=1, 2, \dots, v} \left(\min_{m=1, 2, \dots, M} (\varphi_{R_u, D_m}) \right). \end{aligned} \quad (16)$$

Công thức (16) có nghĩa là trạm chuyển tiếp nhận được dữ liệu từ vệ tinh thành công trong pha đầu ($1 \leq k \leq v$) và cung cấp tỷ số SINR lớn nhất cho đích D_r sẽ được chọn.

Xét nút nghe lén E trong pha thứ hai này; tín hiệu nhận được tại E sẽ là:

$$\begin{aligned} z_E &= \sqrt{P_R} h_{R_k, E} x + \sum_{n=1}^N \sqrt{P_I} l_{I_n, E} w_n \\ &+ \sqrt{P_{J_2}} l_{J_2, E} u_2 + n_E, \end{aligned} \quad (17)$$

với P_{J_2} là công suất phát của J_2 , $h_{R_k, E}$, $l_{I_n, E}$ và $l_{J_2, E}$ lần lượt là kênh pha đỉnh Rayleigh của các liên kết $R_k \rightarrow E$, $I_n \rightarrow E$ và $J_2 \rightarrow E$, u_2 là tín hiệu nhiễu gây ra bởi J_2 .

Từ công thức (17), tỷ số SINR đạt được tại nút nghe lén E sẽ được viết ra như sau:

$$\begin{aligned} \varphi_E &= \frac{P_R |h_{R_k, E}|^2}{P_{J_2} |l_{J_2, E}|^2 + \sum_{n=1}^N P_I |l_{I_n, E}|^2 + \sigma_0^2} \\ &= \frac{\Delta_R Y_E}{\Delta_{J_2} Z_{J_2} + \sum_{n=1}^N \Delta_I T_{I_n, E} + 1}, \end{aligned} \quad (18)$$

với $\Delta_{J_2} = P_{J_2} / \sigma_0^2$, $Y_E = |h_{R_k, E}|^2$, $T_{I_n, E} = |l_{I_n, E}|^2$ và $Z_{J_2} = |l_{J_2, E}|^2$.

Tương tự, các độ lợi kênh Y_E , $T_{I_n, E}$ và Z_{J_2} đều có phân phối mũ. Cũng với giả sử rằng các kênh pha đỉnh Rayleigh là độc lập và đồng đều, hàm PDF của Y_E , $T_{I_n, E}$ và Z_{J_2} sẽ lần lượt được viết ra như sau:

$$f_{Y_E}(y) = \lambda_{R, E} \exp(-\lambda_{R, E} y), \quad (19)$$

$$f_{T_{I_n, E}}(t) = \lambda_{I, E} \exp(-\lambda_{I, E} t), \quad (20)$$

$$f_{Z_{J_2}}(z) = \lambda_{J_2, E} \exp(-\lambda_{J_2, E} z). \quad (21)$$

Tương tự như trên, các thiết bị thu D_m và E có thể giải mã thành công dữ liệu nếu tỷ số SINR đạt được tại các nút này lớn hơn một ngưỡng xác định trước, ký hiệu là $\omega_{2, th}$. Ngược lại, nếu tỷ số SINR tại D_m và E thấp hơn ngưỡng $\omega_{1, th}$ thì D_m và E không thể giải mã thành công dữ liệu.

Sử dụng công thức (16), xác suất dừng của kênh dữ liệu sẽ được đánh giá như sau:

$$\begin{aligned} OP_v &= \Pr(\varphi_{R_k, D_r} < \omega_{2, th}) \\ &= \Pr\left(\max_{u=1, 2, \dots, v} \left(\min_{m=1, 2, \dots, M} (\varphi_{R_u, D_m})\right) < \omega_{2, th}\right) \\ &= \prod_{u=1}^v \Pr\left(\min_{m=1, 2, \dots, M} (\varphi_{R_u, D_m}) < \omega_{2, th}\right) \\ &= \prod_{u=1}^v \left[1 - \Pr\left(\min_{m=1, 2, \dots, M} (\varphi_{R_u, D_m}) \geq \omega_{2, th}\right)\right] \\ &= \prod_{u=1}^v \left[1 - \prod_{m=1}^M \Pr(\varphi_{R_u, D_m} \geq \omega_{2, th})\right]. \end{aligned} \quad (22)$$

Công thức (22) định nghĩa xác suất dừng OP như sau: trong điều kiện có v ($v \geq 1$) trạm chuyển tiếp mặt đất giải mã thành công dữ liệu từ vệ tinh, thì xác suất dừng là xác suất mà nút đích D_r không thể giải mã thành công dữ liệu mà trạm chuyển tiếp được chọn R_k gửi đến. Điều này cũng tương đương với sự kiện trong M nút đích có ít nhất một nút không thể giải mã thành công dữ liệu.

Tương tự như các nút đích, sự giải mã dữ liệu tại E sẽ thành công khi $\varphi_E \geq \omega_{2, th}$; và không thành công khi $\varphi_E < \omega_{2, th}$. Trong trường hợp mà E giải mã thành công dữ liệu nhận được từ R_k , dữ liệu cũng sẽ bị mất bảo mật.

III. ĐÁNH GIÁ HIỆU NĂNG HỆ THỐNG

A. Xác suất dừng (OP)

Tổng xác suất dừng của mô hình nghiên cứu được viết ra như sau:

$$OP = Q_0 + \sum_{v=1}^K C_K^v \times Q_v \times OP_v, \quad (23)$$

Trong (23), Q_0 là xác suất mà tất cả các trạm mặt đất không thể giải mã thành công dữ liệu từ vệ tinh, Q_v là xác suất có v trạm chuyển tiếp mặt đất giải mã thành công dữ liệu, OP_v là xác suất hệ thống bị dừng ở pha thời gian thứ hai, và hệ số C_K^v xuất hiện do có tất cả C_K^v cách chọn v trạm chuyển tiếp thành công từ tập K trạm chuyển tiếp. Từ các công thức (2) và (8), Q_v được viết dưới dạng sau:

$$Q_v = \left[1 - \Pr \left(X_{R_u} < \frac{\omega_{1,th}}{\Delta_S} \right) \right]^v \times \left[\Pr \left(X_{R_u} < \frac{\omega_{1,th}}{\Delta_S} \right) \right]^{K-v} \quad (24)$$

$$= \left[1 - F_{X_{R_u}} \left(\frac{\omega_{1,th}}{\Delta_S} \right) \right]^v \times \left[F_{X_{R_u}} \left(\frac{\omega_{1,th}}{\Delta_S} \right) \right]^{K-v},$$

với $F_U(\cdot)$ là hàm phân phối tích lũy (CDF: Cumulative Distribution Function) của biến ngẫu nhiên U . Thật vậy, từ hàm PDF đưa ra trong công thức (3), ta có thể tìm được hàm CDF cho X_{R_u} như sau:

$$F_{X_{R_u}}(x) = \int_0^x f_{X_{R_u}}(t) dt. \quad (25)$$

Kết hợp các công thức (3), (24) và (25), Q_v sẽ được tính chính xác như sau:

$$Q_v = \left[1 - \int_0^{\frac{\omega_{1,th}}{\Delta_S}} \left(\frac{1}{2b_R} \left(\frac{2m_R b_R}{2m_R b_R + \Omega_R} \right)^{m_R} \exp\left(-\frac{t}{2b_R}\right) \right) \times {}_1F_1 \left(m_R; 1; \frac{\Omega_R t}{2b_R (2m_R b_R + \Omega_R)} \right) dt \right]^v \quad (26)$$

$$\times \left[\int_0^{\frac{\omega_{1,th}}{\Delta_S}} \left(\frac{1}{2b_k} \left(\frac{2m_k b_k}{2m_k b_k + \Omega_R} \right)^{m_k} \exp\left(-\frac{t}{2b_k}\right) \right) \times {}_1F_1 \left(m_k; 1; \frac{\Omega_R t}{2b_k (2m_k b_k + \Omega_R)} \right) dt \right]^{K-v}.$$

Từ công thức (26), Q_0 có thể được tính như sau:

$$Q_0 = \left[1 - \int_0^{\frac{\omega_{1,th}}{\Delta_S}} \left(\frac{1}{2b_R} \left(\frac{2m_R b_R}{2m_R b_R + \Omega_R} \right)^{m_R} \exp\left(-\frac{t}{2b_R}\right) \right) \times {}_1F_1 \left(m_R; 1; \frac{\Omega_R t}{2b_R (2m_R b_R + \Omega_R)} \right) dt \right]^K. \quad (27)$$

Tiếp đến, ta tính xác suất dừng OP_v ; kết hợp các công thức (10) và (22), ta có thể viết:

$$OP_v = \prod_{u=1}^v \left[1 - \prod_{m=1}^M \Pr \left(\frac{\Delta_R Y_{D_m}}{\underbrace{\kappa^2 \Delta_R Y_{D_m} + \sum_{n=1}^N \Delta_I T_{I_n, D_m} + 1}_{Q_m}} \geq \omega_{2,th} \right) \right] \quad (28)$$

$$= \prod_{u=1}^v \left[1 - \prod_{m=1}^M Q_m \right].$$

Xét xác suất Q_m trong (28), ta có:

$$Q_m = \Pr \left((1 - \kappa^2 \omega_{2,th}) \Delta_R Y_{D_m} \geq \sum_{n=1}^N \Delta_I T_{I_n, D_m} \omega_{2,th} + \omega_{2,th} \right). \quad (29)$$

Quan sát công thức (29), ta thấy rằng nếu $1 - \kappa^2 \omega_{2,th} \geq 1$ thì $Q_m = 0$, và do đó $OP_v = 1$. Xét trường hợp $1 - \kappa^2 \omega_{2,th} < 1$, Q_m được đưa về dạng sau:

$$Q_m = \Pr \left(Y_{D_m} \geq \rho_1 \sum_{n=1}^N T_{I_n, D_m} + \rho_2 \right) \quad (30)$$

$$= \int_0^{+\infty} \left(1 - F_{Y_{D_m}} \left(\rho_1 \sum_{n=1}^N x_n + \rho_2 \right) \right) \prod_{n=1}^N f_{T_{I_n, D_m}}(x_n) dx_n,$$

với

$$\rho_1 = \frac{\Delta_I \omega_{2,th}}{(1 - \kappa^2 \omega_{2,th}) \Delta_R}, \quad \rho_2 = \frac{\omega_{2,th}}{(1 - \kappa^2 \omega_{2,th}) \Delta_R}. \quad (31)$$

Trong công thức (30), hàm CDF $F_{Y_{D_m}} \left(\rho_1 \sum_{n=1}^N x_n + \rho_2 \right)$ được viết ra như sau:

$$F_{Y_{D_m}} \left(\rho_1 \sum_{n=1}^N x_n + \rho_2 \right) = 1 - \exp(-\lambda_{R,D} \rho_2) \times \exp\left(-\lambda_{R,D} \rho_1 \sum_{n=1}^N x_n\right). \quad (32)$$

Thay (12) và (32) vào (30), sau khi tính tích phân, ta đạt được công thức (33) như sau:

$$Q_m = \exp(-\lambda_{R,D} \rho_2) \prod_{n=1}^N \frac{\lambda_{I,D}}{\lambda_{I,D} + \lambda_{R,D} \rho_1} \quad (33)$$

$$= \left(\frac{\lambda_{I,D}}{\lambda_{I,D} + \lambda_{R,D} \rho_1} \right)^N \exp(-\lambda_{R,D} \rho_2).$$

Thay (33) vào (28), xác suất dừng OP_v được tính chính xác như sau:

$$OP_v = \prod_{u=1}^v \left[1 - \prod_{m=1}^M \left(\left(\frac{\lambda_{I,D}}{\lambda_{I,D} + \lambda_{R,D} \rho_1} \right)^N \exp(-\lambda_{R,D} \rho_2) \right) \right] \quad (34)$$

$$= \left[1 - \left(\frac{\lambda_{I,D}}{\lambda_{I,D} + \lambda_{R,D} \rho_1} \right)^{M \times N} \exp(-M \lambda_{R,D} \rho_2) \right]^v.$$

Cuối cùng, thay (26), (27) và (34) vào (23), ta sẽ có được công thức tính chính xác xác suất dừng của kênh dữ liệu.

B. Xác suất chặn (IP)

Xác suất mất bảo mật hay xác suất chặn (IP) là xác suất mà nút nghe lén E có thể giải mã thành công dữ liệu của vệ tinh, hoặc trực tiếp từ vệ tinh hoặc từ trạm chuyên tiếp được chọn R_k . Thật vậy, ta có thể đưa ra công thức tính xác suất chặn tại E như sau:

$$\begin{aligned} IP &= \Pr(\gamma_E \geq \omega_{1,th} \cup \varphi_E \geq \omega_{2,th}) \\ &= 1 - \Pr(\gamma_E < \omega_{1,th}) \times \left(Q_0 + \sum_{v=1}^K C_K^v Q_v \Pr(\varphi_E < \omega_{2,th}) \right). \end{aligned} \quad (34)$$

Công thức (34) có nghĩa rằng chỉ cần nút nghe lén giải mã thành công dữ liệu trong pha 1 hoặc pha 2 thì dữ liệu sẽ bị mất bảo mật ($\gamma_E \geq \omega_{1,th} \cup \varphi_E \geq \omega_{2,th}$). Xác suất này cũng cũng tương đương với 1 trừ đi xác suất mà nút nghe lén E không thể đạt được dữ liệu mong muốn trong cả pha thứ nhất ($\gamma_E < \omega_{1,th}$) và pha thứ hai ($Q_0 + \sum_{v=1}^K C_K^v Q_v \Pr(\varphi_E < \omega_{2,th})$).

Xét xác suất $\Pr(\gamma_E < \omega_{1,th})$, kết hợp với công thức (5), ta có:

$$\begin{aligned} \Pr(\gamma_E < \omega_{1,th}) &= \Pr\left(X_E < \frac{\Delta_{J_1} \omega_{1,th}}{\Delta_S} Z_{J_1} + \frac{\omega_{1,th}}{\Delta_S}\right) \\ &= \int_0^{+\infty} F_{X_E}(\xi_1 z + \xi_2) f_{Z_{J_1}}(z) dz, \end{aligned} \quad (35)$$

với

$$\xi_1 = \frac{\Delta_{J_1} \omega_{1,th}}{\Delta_S}, \xi_2 = \frac{\omega_{1,th}}{\Delta_S}. \quad (36)$$

Kết hợp với công thức (6) và (7), công thức (35) được viết lại dưới dạng sau:

$$\begin{aligned} \Pr(\gamma_E < \omega_{1,th}) &= \int_0^{+\infty} \lambda_{J_1,E} \exp(-\lambda_{J_1,E} z) \\ &\times \int_0^{\xi_1 z + \xi_2} \left[\frac{1}{2b_E} \left(\frac{2m_E b_E}{2m_E b_E + \Omega_E} \right)^{m_E} \exp\left(-\frac{x}{2b_E}\right) \right. \\ &\left. \times {}_1F_1\left(m_E; 1; \frac{\Omega_E x}{2b_E(2m_E b_E + \Omega_E)}\right) \right] dx dz. \end{aligned} \quad (37)$$

Kế tiếp, ta tính xác suất $\Pr(\varphi_E < \omega_{2,th})$ trong công thức (34); sử dụng công thức (18), ta có:

$$\begin{aligned} \Pr(\varphi_E < \omega_{2,th}) &= \Pr\left(\frac{\Delta_R Y_E}{\Delta_{J_2} Z_{J_2} + \sum_{n=1}^N \Delta_I T_{I_n,E} + 1} < \omega_{2,th}\right) \\ &= \Pr\left(Y_E < \frac{\Delta_{J_2} \omega_{2,th}}{\Delta_R} Z_{J_2} + \frac{\Delta_I \omega_{2,th}}{\Delta_R} \sum_{n=1}^N T_{I_n,E} + \frac{\omega_{2,th}}{\Delta_R}\right) \\ &= \Pr\left(Y_E < \omega_3 Z_{J_2} + \omega_4 \sum_{n=1}^N T_{I_n,E} + \omega_5\right), \end{aligned} \quad (38)$$

với

$$\omega_3 = \frac{\Delta_{J_2} \omega_{2,th}}{\Delta_R}, \omega_4 = \frac{\Delta_I \omega_{2,th}}{\Delta_R}, \omega_5 = \frac{\omega_{2,th}}{\Delta_R}. \quad (39)$$

Tiếp đến, ta tiếp tục viết công thức (38) dưới dạng sau:

$$\begin{aligned} \Pr(\varphi_E < \omega_{2,th}) &= \int_0^{+\infty} F_{Y_E}\left(\omega_3 x_0 + \omega_4 \sum_{n=1}^N x_n + \omega_5\right) \\ &\times f_{Z_{J_2}}(x_0) dx_0 \prod_{n=1}^N f_{T_{I_n,E}}(x_n) dx_n. \end{aligned} \quad (40)$$

Thay các hàm CDF và PDF đã có vào công thức (40), sau một số phép tính tích phân, ta đạt được:

$$\begin{aligned} \Pr(\varphi_E < \omega_{2,th}) &= 1 - \\ &\frac{\lambda_{J_2,E}}{\lambda_{J_2,E} + \lambda_{R,E} \omega_3} \exp(-\lambda_{R,E} \omega_5) \times \prod_{n=1}^N \frac{\lambda_{I_n,E}}{\lambda_{I_n,E} + \lambda_{R,E} \omega_4} \\ &= 1 - \frac{\lambda_{J_2,E}}{\lambda_{J_2,E} + \lambda_{R,E} \omega_3} \left(\frac{\lambda_{I_n,E}}{\lambda_{I_n,E} + \lambda_{R,E} \omega_4} \right)^N \exp(-\lambda_{R,E} \omega_5). \end{aligned} \quad (41)$$

Cuối cùng, thay (26), (27) và (41) vào (34), ta có được công thức tính chính xác của IP.

IV. KẾT QUẢ VÀ THẢO LUẬN

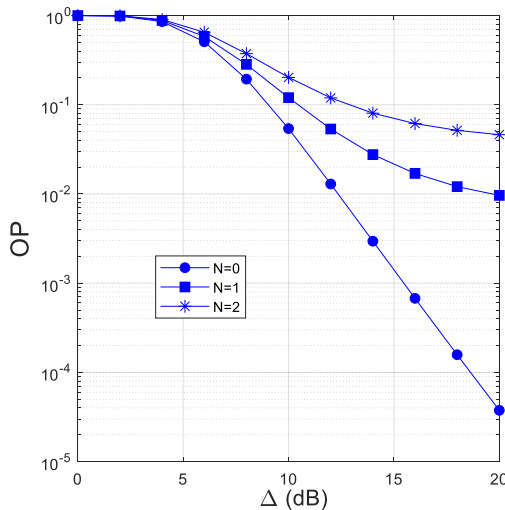
Trong phần này, các kết quả lý thuyết sẽ được đưa ra nhằm đánh giá và phân tích các hiệu năng OP và IP của hệ thống. Trong tất cả các hình vẽ trong mục này, các tham số kênh truyền Shadowed-Rician sẽ được thiết lập như sau: $m_R = m_E = 10.1$, $b_R = b_E = 0.126$ và $\Omega_R = \Omega_E = 0.835$ [5], [15], [18], [22]. Để đơn giản trong việc mô tả và phân tích các xu hướng hiệu năng hệ thống, ta có thể cố định các tham số hệ thống như sau: $\sigma_0^2 = 1$, $P_S = P_R = P_I = P$, $P_{J_1} = P_{J_2} = P_J = 0.5P_S$, $\lambda_{R,D} = \lambda_{R,E} = \lambda_{J_1,E} = \lambda_{J_2,E} = 0.1$, $\lambda_{I,D} = \lambda_{I,E} = 10$. Trong các hình vẽ, ta sử dụng: $\Delta_S = \Delta_R = \Delta_I = \Delta$ và $\omega_{1,th} = \omega_{2,th} = \omega_{th}$. Bài báo dùng phần mềm máy tính MATHEMATICA để tính các giá trị của OP và IP, và phần mềm MATLAB để vẽ các kết quả.

Hình 2 vẽ xác suất dừng theo Δ (dB) với số nguồn giao thoa N khác nhau khi số lượng trạm mặt đất (K) bằng 3, số lượng người dùng (M) là 4, mức khiếm khuyết tại các nút đích hợp pháp (κ^2) bằng 0.01 và ngưỡng dừng (ω_{th}) bằng 5. Như được quan sát trong Hình 2, xác suất dừng giảm khi tăng Δ và giảm số lượng nguồn giao

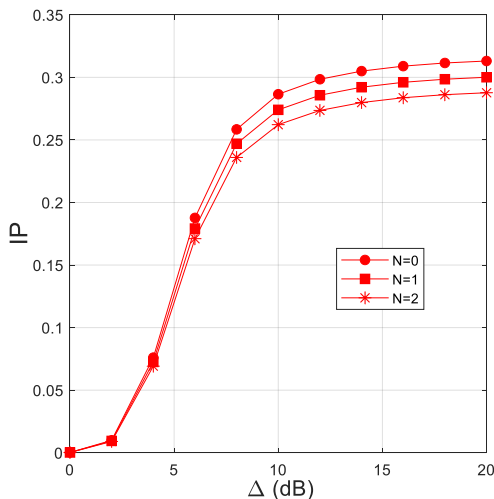
thoa. Trong trường hợp $N=0$, OP của hệ thống nhỏ hơn đáng kể khi so với các trường hợp có 01 hoặc 02 nguồn giao thoa.

Hình 3 vẽ xác suất chặn (IP) tại nút nghe lén E theo Δ (dB). Các thông số trong Hình 2 và Hình 3 là giống nhau. Như ta có thể quan sát trong Hình 3, giá trị IP tăng khi tăng Δ và giảm số lượng nguồn giao thoa.

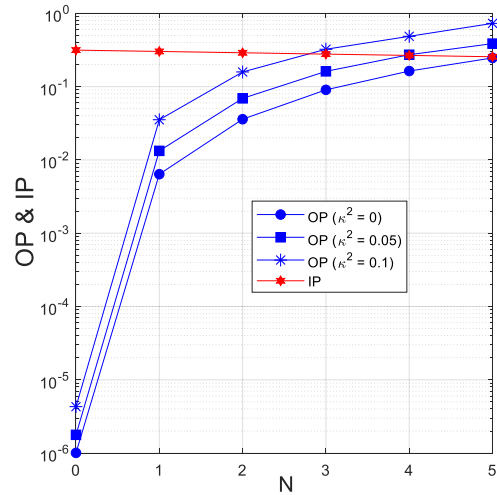
Từ Hình 2 và 3, ta thấy có sự đánh đổi giữa độ tin cậy của việc truyền dữ liệu (OP) và khả năng bảo mật dữ liệu của hệ thống. Ví dụ: khi hệ thống sử dụng công suất phát lớn, việc truyền dữ liệu sẽ đáng tin cậy hơn (OP nhỏ hơn), tuy nhiên dữ liệu sẽ dễ bị mất bảo mật hơn (IP lớn hơn). Ý nghĩa của việc nghiên cứu sự đánh đổi giữa OP và IP đó là chúng ta có thể dựa vào các giá trị OP và IP để tối ưu hóa hệ thống. Ví dụ: hệ thống hoạt động trong môi trường không có giao thoa đồng kênh ($N=0$) và chất lượng dịch vụ yêu cầu là: $OP \leq 0.001$, thì nhìn vào Hình 2, ta thấy giá trị của Δ vào khoảng 16 dB là tốt nhất để giá trị OP là nhỏ nhất có thể.



Hình 2. OP vẽ theo Δ (dB) với $K=3$, $M=4$, $\kappa^2=0.01$ và $\omega_{th}=5$.



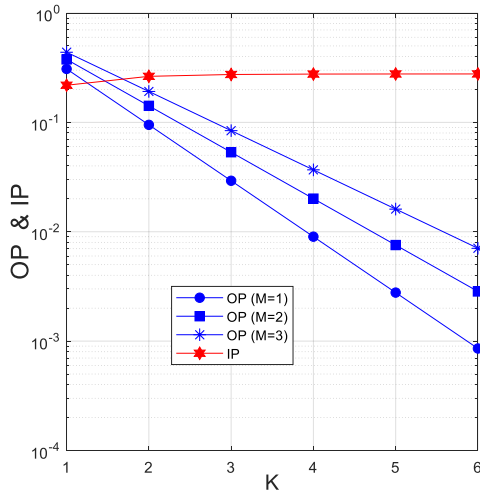
Hình 3. IP vẽ theo Δ (dB) với $K=3$, $M=4$, $\kappa^2=0.01$ và $\omega_{th}=5$.



Hình 4. OP và IP vẽ theo N với $K=3$, $M=4$, $\Delta=25$ (dB) và $\omega_{th}=5$.

Hình 4 vẽ OP và IP theo số nguồn giao thoa N với các giá trị khác nhau của mức khiếm khuyết phần cứng (κ^2) và với $K=3$, $M=4$, $\Delta=25$ (dB) và $\omega_{th}=5$. Như chúng ta có thể dự đoán giá trị của OP sẽ tăng khi số nguồn nhiễu tăng, trong khi IP sẽ giảm. Như ta có thể thấy trong Hình 4, giá trị OP tăng nhanh theo N , trong khi IP chỉ giảm nhẹ. Đó là vì nút nghe lén E chịu ảnh hưởng chính bởi các trạm tạo nhiễu nhân tạo J_1 và J_2 . Thật vậy, do độ lợi kênh trung bình từ J_1 và J_2 đến E lớn hơn so với từ các nguồn nhiễu I_n ($n=1, 2, \dots, N$) nên sự tác động của nhiễu gây ra bởi J_1 và J_2 lên E là đáng kể hơn. Cũng trong Hình 4, ta cũng quan sát được sự ảnh hưởng của khiếm khuyết phần cứng tại các nút đích tác động lên giá trị của OP. Như quan sát, OP tăng khi κ^2 tăng.

Hình 5 vẽ OP và IP theo số nguồn trạm chuyển tiếp K với các giá trị khác nhau của số lượng nút đích M và với $N=1$, $\kappa^2=0.01$, $\Delta=10$ (dB) và $\omega_{th}=5$. Như ta có thể quan sát, xác suất dừng OP của hệ thống giảm mạnh khi tăng số trạm chuyển tiếp từ 1 lên 7. Đó là vì khi tăng giá trị của K sẽ nâng cao độ tin cậy của việc truyền-nhận dữ liệu ở cả hai pha. Tuy nhiên, xác suất dừng hệ thống tăng khi số nút đích tăng lên do yêu cầu tất cả những người dùng đều đạt được dữ liệu thành công. Đối với giá trị IP, giá trị này tăng nhẹ khi tăng giá trị của K . Bởi vì khi số trạm mặt đất tăng sẽ tăng xác suất có ít nhất một trạm mặt đất giải mã thành công dữ liệu từ vệ tinh, và do đó tăng xác suất nút nghe lén có thể nghe lén ở pha thứ hai. Tuy nhiên, do ở cả hai pha, kỹ thuật CJ đều được sử dụng nên sự tăng của IP là không đáng kể.



Hình 5. OP và IP vẽ theo K với $N=1$, $\kappa^2=0.01$, $\Delta=10$ (dB) và $\omega_{th}=5$.

V. KẾT LUẬN

Bài báo đã nghiên cứu sự đánh đổi giữa bảo mật và độ tin cậy cho mô hình chuyển tiếp lai ghép vệ tinh-mặt đất với sự ảnh hưởng của nhiễu đồng kênh và khiếm khuyết phần cứng. Đề nâng cao sự ổn định của sự truyền dữ liệu từ vệ tinh đến những người dùng hợp pháp, bài báo đề xuất triển khai nhiều trạm chuyển tiếp mặt đất và phương pháp chọn trạm chuyển tiếp tốt nhất để phục vụ những người dùng. Đề nâng cao hiệu quả bảo mật ở lớp vật lý, kỹ thuật tạo nhiễu nhân tạo đã được áp dụng để bảo vệ dữ liệu ở cả hai pha truyền. Bên cạnh việc đề xuất mô hình mới, bài báo cũng đã đưa ra các công thức đánh giá chính xác các thông số hiệu năng của hệ thống. Các kết quả đạt được trong bài báo cũng cho thấy rằng có sự đánh đổi giữa OP và IP. Hơn nữa, sự tác động của các thông số quan trọng như công suất phát, số trạm mặt đất, số nguồn nhiễu đồng kênh, mức khiếm khuyết phần cứng lên hiệu năng của hệ thống cũng đã được phân tích kỹ. Trong tương lai, các mô hình tổng quát như mô hình với các nút được trang bị nhiều anten, mô hình với sự xuất hiện của nhiễu thiết bị nghe lén hợp tác, mô hình kênh truyền pha định tổng quát như Nakagami- m , Rician, sẽ được nghiên cứu.

LỜI CẢM ƠN

Nghiên cứu này được tài trợ bởi Học Viện Công Nghệ Bưu Chính Viễn Thông Cơ Sở Thành Phố Hồ Chí Minh với mã số đề tài 07-HV-2020-RD_VT2.

TÀI LIỆU THAM KHẢO

- [1] B. Evans, M. Werner, E. Lutz, M. Bousquet, G.E. Corazza, G. Maral and R. Rumeau, "Integration of Satellite and Terrestrial Systems in Future Multimedia Communications," IEEE Wireless Communications, vol. 12, no. 5, pp. 72-80, Oct. 2005.
- [2] K. Guo, D. Guo, Y. Huang, X. Wang and B. Zhang, "Performance Analysis of a Dual-Hop Satellite Relay Network with Hardware Impairments," in Proc. of 25th Wireless and Optical Communication Conference (WOCC), Chengdu, China, pp. 1-5, May 2016.
- [3] E. Bjornson, M. Matthaiou and M. Debbah, "A New Look at Dual-Hop Relaying: Performance Limits With Hardware

Impairments," IEEE Transactions on Communications, vol. 61, no. 11, pp. 4512-4525, Nov. 2013.

- [4] T. T. Duy, et al., "Proactive Relay Selection with Joint Impact of Hardware Impairment and Co-channel Interference," IEEE Transactions on Communications, vol. 63, no. 5, pp. 1594-1606, May 2015.
- [5] H. Wu, Y. Zou, W. Cao, Z. Chen, T. A. Tsiftsis, M. R. R. Bhatnagar and R. C. De Lamare, "Impact of Hardware Impairments on Outage Performance of Hybrid Satellite-Terrestrial Relay Systems," IEEE Access, vol. 7, pp. 35103- 35112, Mar. 2019.
- [6] C. Zhang, H. Lin, Y. Huang and L. Yang, "Performance of Integrated Satellite-Terrestrial Relay Network with Relay Selection and Outdated CSI," IEEE Access, vol. 8, pp. 169652-169662, Sept. 2020.
- [7] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan and S. Shetty, "Physical Layer Security in Wireless Cooperative Relay Networks: State of the Art and Beyond," IEEE Communications Magazine, vol. 53, no. 12, pp. 32-39, Dec. 2015.
- [8] H. D. Hung, T. T. Duy and M. Voznak, "Secrecy Outage Performance of Multi-hop LEACH Networks using Power Beacon Aided Cooperative Jamming With Jammer Selection Methods," AEU-International Journal of Electronics and Communications vol. 124, ID 153357, Sept. 2020.
- [9] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan and T. Q. Duong, "Relay Selection for Security Enhancement in Cognitive Relay Networks," IEEE Wireless Communications Letters, vol. 4, no. 1, pp. 46-49, Feb. 2015.
- [10] P. T. Tin, et. al, "Rateless Codes based Secure Communication Employing Transmit Antenna Selection and Harvest-To-Jam under Joint Effect of Interference and Hardware Impairments," Entropy, vol. 21, no. 7, ID 700, Jul. 2019.
- [11] P. Yan, Y. Zou, X. Ding and J. Zhu, "Energy-Aware Relay Selection Improves Security-Reliability Tradeoff in Energy Harvesting Cooperative Cognitive Radio Systems," IEEE Transactions on Vehicular Technology, vol. 69, no. 5, pp. 5115-5128, May 2020.
- [12] Y. Li, K. An, T. Liang and X. Yan, "Secrecy Performance of Land Mobile Satellite Systems with Imperfect Channel Estimation and Multiple Eavesdroppers," IEEE Access, vol. 7, pp. 31751-31761, Mar. 2019.
- [13] R. Wang and F. Zhou, "Physical Layer Security for Land Mobile Satellite Communication Networks With User Cooperation," IEEE Access, vol. 7, pp. 29495-29505, Mar. 2019.
- [14] Y. Zhang, J. Ye, G. Pan and M. -S. Alouini, "Secrecy Outage Analysis for Satellite-Terrestrial Downlink Transmissions," IEEE Wireless Communications Letters, vol. 9, no. 10, pp. 1643-1647, Oct. 2020.
- [15] Q. Huang, M. Lin, K. An, J. Ouyang and W. Zhu, "Secrecy Performance of Hybrid Satellite-Terrestrial Relay Networks in the Presence of Multiple Eavesdroppers," IET Communications, vol. 12, no. 1, pp. 26-34, Jan. 2018.
- [16] V. Bankey and P. K. Upadhyay, "Ergodic Secrecy Capacity Analysis of Multiuser Hybrid Satellite-Terrestrial Relay Networks with Multiple Eavesdroppers," in Proc. of 2019 IEEE International Conference on Communications Workshops (ICC Workshops), Shanghai, China, 2019, pp. 1-6.
- [17] V. Bankey and P. K. Upadhyay, "Physical Layer Security of Multiuser Multirelay Hybrid Satellite-Terrestrial Relay Networks," IEEE Transactions on Vehicular Technology, vol. 68, no. 3, pp. 2488-2501, Mar. 2019.
- [18] W. Cao, Y. Zou, Z. Yang and J. Zhu, "Relay Selection for Improving Physical-Layer Security in Hybrid Satellite-

Terrestrial Relay Networks," IEEE Access, vol. 6, pp. 65275-65285, Oct. 2018.

- [19] I. S. Gradshteyn and I. M. Ryzhik, "Table of Intergals, Series, and Products. 7th ed. Academic Press, 2007.
- [20] M. Matthaiou, A. Papadogiannis, E. Bjornson, M. Debbah, "Two-Way Relaying Under the Presence of Relay Transceiver Hardware Impairments," IEEE Communications Letters, vol. 17, no. 6, pp. 1136-1139, Jun. 2013.
- [21] T. T. Duy, P. N. Son, "Secrecy Performances of Multicast Underlay Cognitive Protocols with Partial Relay Selection and without Eavesdropper's Information," KSII Transactions on Internet and Information Systems, vol. 9, no. 11, pp. 4623-4643, Nov. 2015.
- [22] M. K. Arti and M. R. Bhatnagar, "Making Two-Way Satellite Relaying Feasible: A Differential Modulation Based Approach," IEEE Communications Letters, vol. 18, no. 7, p. 1187-1190, Jul. 2014.

SECRECYPERFORMANCE ANALYSIS FOR HYBRID SATELLITE-TERRESTRIAL RELAY NETWORKS UNDER IMPACT OF CO-CHANNEL INTERFERENCE AND HARDWARE IMPAIRMENTS

Abstract: In this paper, we study secrecy performance of hybrid satellite-terrestrial relay network in presence of an eavesdropper. In the proposed protocol, a satellite sends its data to terrestrial stations, and one of successful terrestrial stations is selected to transmit the data to a group of authorized destinations. The eavesdropper can overhear the data from the satellite and the selected terrestrial station. To protect the transmitted data, cooperative jamming technique is employed, where the jammer stations are delayed to generate jamming noises to the eavesdropper. Moreover, the terrestrial stations and the authorized destinations can cooperative with the jammer stations to remove the generated noises. This paper also considers joint impact of hardware impairments at the authorized destinations and co-channel interference caused by frequency reuse operation on the system performance. We derive exact expressions of outage probability at the authorized destinations and intercept probability at the eavesdropper. Finally, the results are presented to show the performance trends as well as the impact of the system parameters.

Keywords: Hybrid Satellite-Terrestrial Relay Network, Physical-layer security, hardware impairments, co-channel interference, outage probability, intercept probability.



Đặng Thế Hùng nhận bằng kỹ sư Viễn thông tại Đại học thông tin liên lạc, Nha Trang, Khánh Hoà vào năm 2006, và nhận bằng Thạc Sĩ Kỹ Thuật Viễn Thông tại Học viện Công nghệ Bưu chính Viễn thông cơ sở tại TP. Hồ Chí Minh vào năm 2014. Th.S. Đặng Thế Hùng hiện tại đang làm nghiên cứu sinh tại Học viện Kỹ thuật Quân sự. Hướng nghiên cứu

đang quan tâm bao gồm: thông tin vô tuyến, bảo mật lớp vật lý, thông tin vệ tinh.

Email:
danghung8384@gmail.com



Lê Chu Khản tốt nghiệp đại học chính qui ngành kỹ thuật điện- điện tử năm 1996, tại trường đại học sư phạm kỹ thuật TP. HCM. Tốt nghiệp thạc sỹ kỹ thuật tại đại học bách khoa, đại học quốc gia TP HCM vào 05/2004. Th.S. Lê Chu Khản hiện đang công tác tại Khoa Viễn Thông 2, Học viện Công nghệ Bưu chính Viễn thông, cơ sở tại TP. Hồ Chí Minh. Hướng nghiên cứu đang quan tâm bao gồm: thông tin vô tuyến, thông tin vệ tinh.

Email:
lckhan@ptithcm.edu.vn



Nguyễn Văn Toàn nhận bằng kỹ sư vô tuyến điện tại Đại học thông tin liên lạc, Nha Trang, Khánh Hoà vào năm 2007, và nhận bằng Thạc Sĩ Kỹ thuật Viễn thông tại Học viện Công nghệ Bưu chính Viễn thông cơ sở tại TP. Hồ Chí Minh vào năm 2013. Th.S. Nguyễn Văn Toàn hiện đang công tác tại Đại học thông tin liên lạc, Nha Trang, Khánh Hoà. Hướng nghiên cứu đang quan tâm bao gồm: thông tin vô tuyến, thông tin vệ tinh.

Email:
toan.nguyenvan@tcu.edu.vn



PGS.TS. Đỗ Quốc Trình nhận bằng Tiến sĩ điện tử Viễn thông tại Học viện Kỹ thuật Quân sự vào năm 2003 và Phó giáo sư năm 2013. PGS Đỗ Quốc Trình hiện đang công tác tại Học viện Kỹ thuật Quân sự. Hướng nghiên cứu đang quan tâm bao gồm: thông tin vô tuyến, mã hóa, thông tin di động, kỹ thuật trải phổ.

Email:
trinhdq@mta.edu.vn