TẠP CHÍ KHOA HỌC ĐẠI HỌC KHÁNH HÒA
tapchikhoahoc@ukh.edu.vn

NGHIÊN CỨU BẢO MẬT LỚP VẬT LÝ SỬ DỤNG MÃ FOUNTAIN VỚI KỸ THUẬT CHỌN LỰA ANTEN PHÁT

Nguyễn Thạc Dũng, Đặng Xuân Hải, Đinh Công Hùng, Nguyễn Văn Anh, Nguyễn Đức Tuấn, Tạ Hữu Long

Trường Đại học Thông tin liên lạc

Tóm tắt: *Trong bài báo này, chúng tôi đề xuất mô hình bảo mật lớp vật lý sử dụng mã Fountain với kỹ thuật chọn lựa anten phát tại trạm gốc (BS). Trong mô hình đề xuất, một trạm gốc (BS) đa anten truyền dữ liệu đến một người dùng hợp pháp (D), trong sự xuất hiện của một người nghe lén bất hợp pháp (E), với giả sử rằng cả D và E là các thiết bị đầu cuối được trang bị đơn anten. Chúng tôi đưa ra các biểu thức dạng tường minh của xác suất giải mã và bảo mật thông tin thành công (SS) tại nút đích, xác suất đánh chặn (IP) tại nút nghe lén và số lượng các gói mã hóa trung bình được phát bởi BS (ANEP) trên kênh truyền pha-đinh Rayleigh. Cuối cùng, chúng tôi thực hiện mô phỏng Monte Carlo để kiểm chứng các biểu thức toán học đã tìm ra.*

Từ khóa: *Mã Fountain, kỹ thuật chọn lựa anten phát, bảo mật lớp vật lý, kênh truyền pha-đinh Rayleigh.*

1. Giới thiệu

Ngày nay, bảo mật trong thông tin vô tuyến đã thu hút được nhiều sự quan tâm, do tính chất phát sóng quảng bá tự nhiên của kênh truyền vô tuyến làm cho việc truyền dữ liệu dễ dàng bị tấn công [1]. Để bảo đảm an toàn thông tin, nhiều thuật toán mã hóa và giải mã dữ liệu đã được triển khai tại lớp ứng dụng dựa trên nhiều giả thuyết khác nhau, như giả sử rằng liên kết giữa máy phát và máy thu tại lớp vật lý là không lỗi, không trễ để đảm bảo độ tin cậy của việc truyền dữ liệu, trong khi những kẻ nghe lén bị giới hạn về khả năng tính toán và thiếu các thuật toán hiệu quả để giải mã thông tin. Tuy nhiên, giả định này đang bị suy yếu cùng với việc phát triển các thuật toán hiệu quả cũng như việc tăng lên khả năng tính toán của các thiết bị thông tin hiện đại, ví dụ như máy tính lượng tử. Chính những giới hạn này là động lực thúc đẩy để nhiều nhà nghiên cứu gần đây đã tập trung thảo luận về các vấn đề bảo mật thông tin tại lớp vật lý (Physical Layer Security: PLS) nhằm đạt được bảo mật bằng cách khai thác đặc tính riêng biệt của các kênh truyền vô tuyến khác nhau, như nhiễu nhiệt, nhiễu và tính chất thay đổi của các kênh pha-đinh [2]. Khái niệm về PLS lần đầu tiên được giới thiệu bởi Shannon [3], và sau đó được mở rộng bởi Wyner [4], với điều kiện bảo mật hoàn hảo được phân tích dựa trên quan điểm của lý thuyết thông tin tương lai.

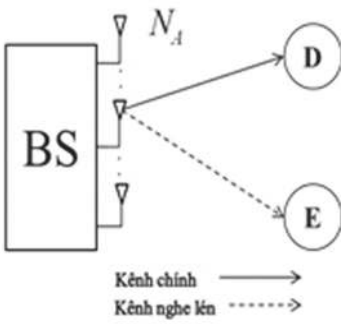
Trong những năm gần đây, đã có nhiều công trình nghiên cứu về PLS ở các góc độ khác nhau nhằm nâng cao hiệu năng bảo mật trong truyền thông vô tuyến. Đặc biệt, kỹ thuật chọn lựa anten phát (Transmit Antenna Selection: TAS) đã được nghiên cứu rộng rãi do độ phức tạp thực hiện thấp của các chuỗi tần số vô tuyến (Radio Frequence Chains) trong khi vẫn đạt được bậc phân tập đầy đủ [5], [6], [7]. Các tác giả trong [8], đã phân tích hiệu năng bảo mật của các kênh nghe lén MIMO với kỹ thuật TAS được thực hiện tại máy phát và các phương pháp kết hợp tín hiệu thu khác nhau. Trong [9], đã nghiên cứu TAS với mã hóa Alamouti và phân bổ công suất trong các kênh nghe lén MIMO. Hơn nữa, trong [10] đã khảo sát hiệu năng bảo mật của hệ thống với giao thức TAS và kết hợp tỷ số tối đa (Maximal Ratio Combining: MRC) với tín hiệu phản hồi không hoàn hảo. Tiếp đến, trong [11], các tác giả đã khảo sát hiệu năng bảo mật của các mạng đa người dùng đường xuống với nhiễu nhân tạo bằng việc thiết kế phân bổ công suất tối ưu để tối đa tổng dung lượng dừng bảo mật của hệ thống. Trong [12], để tăng mức độ bảo mật của kênh hợp pháp, các phương pháp lựa chọn nút gây nhiễu cơ hội khác nhau đã được đề xuất trong các mạng nghe lén đa người dùng. Trong [13], một phương pháp lựa chọn người dùng tối ưu trong các mạng chuyển tiếp đa người dùng với gây nhiễu cộng tác đã được phân tích dựa vào biểu thức tốc độ dừng bảo mật được đưa ra.

Hơn nữa, các kỹ thuật chọn lựa nút chuyển tiếp, chuyển tiếp cộng tác, truyền thông đa chặng và gây nhiễu nhân tạo cũng đã được khai thác rộng rãi để cải thiện PLS trong truyền thông vô tuyến [14], [15], [16], [17]. Một trong những vấn đề cơ bản trong thông tin vô tuyến là tăng thông lượng một cách hiệu quả trong các kênh truyền biến đổi theo thời gian. Nhìn chung, việc truyền tín hiệu trên các kênh vô tuyến phải đối mặt với rất nhiều thách thức đó là sự suy giảm nghiêm trọng về chất lượng kênh truyền, bao gồm nhiễu, pha-đinh, suy hao đường truyền, hiện tượng bóng mờ,.. thay đổi trong suốt quá trình truyền. Do đó, để đạt được thông lượng cao, các hệ thống vô tuyến cần phải thích ứng với tất cả các điều kiện kênh truyền khác nhau. Để giải quyết những vấn đề trên, thì mã Fountain (Fountain codes: FCs), hay mã Rateless (Rateless codes) [18], [19], có thể thích ứng với các điều kiện kênh truyền mà không cần biết thông tin trạng thái kênh (Channel State Information: CSI) tại máy phát. Máy phát sử dụng bộ mã hóa Fountain có thể tạo ra các symbol được mã hóa không giới hạn, phụ thuộc vào chất lượng kênh tức thời của máy thu. Máy thu nhận các symbol được mã hóa một cách hiệu quả và kết thúc quá trình nhận cho đến khi có thể giải mã thành công bản tin gốc, có nghĩa rằng tốc độ thay đổi phụ thuộc vào CSI tức thời [20], [21]. Ngoài ra, bằng cách sử dụng FCs, máy thu chỉ gửi một bít thông tin đến máy phát để bắt đầu quá trình truyền bản tin mới. Tuy nhiên, do đặc tính quảng bá tự nhiên của thông tin vô tuyến, những kẻ nghe lén có thể dễ dàng đánh chặn những gói tin được mã hóa này để giải mã bản tin gốc.

Do đó, bảo mật là vấn đề rất quan trọng trong các hệ thống vô tuyến sử dụng FCs. Khác với các mô hình đã xét trong [22] sử dụng kỹ thuật TAS nhằm nâng cao hiệu năng bảo mật, xem xét dưới điều kiện tác động của nhiễu đồng kênh, dựa vào biểu thức dạng chính xác của xác suất giải mã và bảo mật thông tin thành công được đưa ra. Trong bài báo này, chúng tôi xem xét mô hình hệ thống mà trong đó việc tái sử dụng tần số trong mạng được phân bổ phổ tần một cách phù hợp, nên không xảy ra hiện tượng giao thoa đồng kênh giữa các thiết bị trong mạng. Trong mô hình đề xuất khai thác FCs, một trạm gốc (BS) sử dụng kỹ thuật TAS để đạt được chất lượng kênh truyền tốt nhất trên kênh chính, nhằm thực hiện giải mã các gói tin mã hóa và bảo mật dữ liệu được gửi đi, trong khi đó cả máy thu hợp pháp (D) và máy nghe lén (E) là các thiết bị đơn ăntên. Để đánh giá hiệu năng bảo mật của hệ thống, chúng tôi đưa ra các biểu thức dạng chính xác của xác suất giải mã và bảo mật thông tin thành công (Probability of Successful and Secure: SS), xác suất đánh chặn (Intercept Probability: IP) và số lượng các gói mã hóa trung bình được phát bởi BS (Average Number of Encoded Packets: ANEP) trên kênh truyền pha-đinh Rayleigh. Những biểu thức toán học này sẽ được kiểm chứng thông qua các mô phỏng máy tính. Phần còn lại của bài báo được tổ chức như sau: Trong phần II, chúng tôi miêu tả mô hình hệ thống được đề xuất. Trong phần III, chúng tôi đánh giá hiệu năng bảo mật của hệ thống. Phần IV cung cấp các kết quả mô phỏng và phân tích lý thuyết. Cuối cùng, chúng tôi kết luận bài báo trong phần V

2. Mô hình hệ thống

Như được thể hiện trong Hình 1, mô hình hệ thống đề xuất bao gồm một trạm gốc (Base Station: BS) muốn truyền dữ liệu đến một nút đích (Destination: D) trên kênh chính, trong sự xuất hiện của một nút nghe lén (Eavesdropper: E) đang cố gắng nghe lén các gói tin được mã hóa để giải mã dữ liệu gốc từ trạm gốc. Chúng tôi cũng giả sử rằng tất cả các thiết bị đầu cuối trong mạng đều được trang bị đơn anten và hoạt động theo chế độ bán song công (halfduplex). Hệ thống sử dụng FCs, dữ liệu gốc của BS có thể chia thành T gói có độ dài bằng nhau, rồi mã hóa một cách thích hợp bằng cách chọn ngẫu nhiên một hoặc một số gói từ T gói này để thực hiện XOR với nhau nhằm tạo ra các gói Fountain. Tại cuối mỗi khe thời gian, D và E sẽ cố gắng giải mã các gói Fountain nhận được và giả sử rằng các máy thu này có thể giải mã thành công bản tin gốc nếu chúng nhận chính xác ít nhất H gói Fountain, với $H = (1+\varepsilon)T$ và ε là hằng số phụ thuộc vào việc thiết kế mã [21]. Ngay sau khi nhận thành công H gói Fountain, D sẽ gửi một tin nhắn ACK để thông báo cho BS dừng phát các gói tin mã hóa. Trong trường hợp này, nếu E không thể đạt được đủ số lượng các gói Fountain cần thiết, thì nó không thể giải mã được bản tin gốc.



Hình 1. Mô hình nghiên cứu đề xuất

Ngược lại, thông tin gốc của BS bị đánh chặn. Với việc xem xét quá trình truyền dữ liệu tại một khe thời gian bất kỳ. Chúng tôi giả sử rằng mô hình kênh truyền được sử dụng trong bài báo là kênh pha-đinh phẳng biến đổi chậm, có nghĩa là hệ số kênh truyền sẽ không thay đổi trong một khe thời gian nhưng thay đổi độc lập giữa các khe thời gian khác nhau. Để thuận tiện cho việc thể hiện các ký hiệu toán học, ta sẽ bỏ qua ký hiệu chỉ số thời gian trên các hệ số kênh truyền. Do vậy, ta ký hiệu h_n là hệ số kênh truyền giữa anten phát thứ n của BS và D, với $n = 1; 2; :::; N_A$. Mặt khác, ta cũng giả sử rằng

kênh truyền giữa các thiết bị là kênh pha-đinh Rayleigh và các hệ số kênh truyền h_n có phân bố độc lập và đồng nhất với nhau (independent and identically distributed: iid). Tiếp theo, g_n được ký hiệu là hệ số kênh truyền của anten phát thứ n của BS và E, tương ứng. Do các hệ số kênh truyền có phân bố Rayleigh, nên độ lợi kênh truyền có phân bố hàm mũ và ta ký hiệu các độ lợi như sau: $\gamma D,n = |h_n|^2$, $\gamma E,n = |g_n|^2$. Hơn nữa, ta cũng ký hiệu λ_D, λ_E lần lượt là các tham số đặc trưng của độ lợi kênh truyền (cụ thể bằng nghịch đảo giá trị trung bình của độ lợi kênh truyền).

$$\lambda_D = \frac{1}{\gamma D,n}, \lambda_E = \frac{1}{\gamma E,n} \quad (1)$$

Từ biểu thức (1), ta biểu diễn hàm phân phối tích lũy (Cumulative Distribution Function: CDF) của biến ngẫu nhiên phân bố mũ X như sau:

$$F(x) = 1 - \exp(-\omega x), \quad (2)$$

Với $X \in \{\gamma D,n, \gamma E,n\}$ và $\omega \in \{\lambda_D, \lambda_E\}$

Tại một khe thời gian bất kỳ, BS sẽ chọn ăntен tốt nhất của mình để truyền các gói Fountain đến D theo phương pháp chọn lựa ăntен phát tốt nhất [23], như sau:

$$b^* : \gamma D,b^* = \max(\gamma D,n), n = 1,2,.....,N_A \quad (3)$$

trong đó, b^* là chỉ số ăntен tốt nhất được chọn để phát dữ liệu tại BS, vì chất lượng kênh truyền giữa ăntен này và D là tốt nhất. Từ công thức (3), hàm CDF của $\gamma D,b^*$ được đưa ra như sau:

$$F_{\gamma D,b^*}(x) = \prod_{n=1}^{N_A} F_{\gamma D,n}(x)$$
$$= (1 - \exp(-\lambda_{D,x}))^{N_A}$$
$$= 1 + \sum_{n=1}^{N_A} (-1)^n C_{N_A}^n \exp(-n\lambda_{D,x}) \quad (4)$$

Tiếp theo, ta xây dựng công thức tính tỷ số tín hiệu trên nhiễu (Signal to Noise Ratio: SNR) đạt được tại cả D và E như sau:

$$\Psi_D = \frac{P_{BS\gamma D,b^*}}{N_0} = \Delta\gamma D,b^*, \quad (5)$$

$$\Psi_E = \frac{P_{BS\gamma E,b^*}}{N_0} = \Delta\gamma E,b^*, \quad (6)$$

với P_{BS} là công suất phát của BS, N_0 là phương sai nhiễu cộng tại máy thu (giả sử tất cả các nhiễu cộng đều có phân bố Gauss với giá trị trung bình bằng 0 và phương sai bằng N_0), $\Delta = P_{BS} / N_0$ là SNR phát. Tiếp theo, giả sử rằng một gói tin mã hóa có thể được giải mã thành công nếu tỷ số SNR nhận được tại máy thu lớn hơn một ngưỡng γ_{th} cho trước. Ngược lại, gói dữ liệu mã hóa sẽ không được nhận thành công. Vậy nên, xác suất mà cả D và E không thể nhận chính xác một gói mã hóa được cho bởi:

$$\rho_D = P_r(\Psi_D \le \gamma_{th}),$$
$$\rho_E = P_r(\Psi_E \le \gamma_{th}). \quad (7)$$

Mặt khác, xác suất để cả D và E có thể nhận chính xác một gói dữ liệu sẽ lần lượt là $1 - \rho_D$ và $1 - \rho_E$. Trước tiên, ta tính giá trị của ρ_D như sau:

$$\rho_D = P_r(\Delta\gamma D,b^* \le \gamma_{th}) = P_r(\gamma D,b^* \le \frac{\gamma_{th}}{\Delta})$$
$$= F_{\gamma D,b^*}\left(\frac{\gamma_{th}}{\Delta}\right) \quad (8)$$

Thay hàm CDF của $\gamma D,b^*$ trong (4) vào (8), ta có:

$$\rho_D = 1 + \sum_{n=1}^{N_A} (-1)^n C_{N_A}^n \exp(-n\lambda_D \frac{\gamma_{th}}{\Delta}) \quad (9)$$

Tương tự, ta có giá trị của ρ_E được tính như sau:

$$\rho_E = P_r(\Delta\gamma E,b^* \le \gamma_{th})$$
$$= P_r(\gamma E,b^* \le \frac{\gamma_{th}}{\Delta})$$
$$= F_{\gamma E,b^*}\left(\frac{\gamma_{th}}{\Delta}\right) \quad (10)$$

Thay hàm CDF của $\gamma E,b^*$ trong (2) vào (10), ta được:

$$\rho_E = 1 - \exp\left(-\lambda_E \frac{\gamma_{th}}{\Delta}\right). \quad (11)$$

3. Đánh giá hiệu năng hệ thống

Chúng ta ký hiệu L_{BS} là tổng số gói Fountain mà BS gửi đến D và L_D là số gói Fountain mà D có thể nhận đúng để khôi phục bản tin gốc $(L_D = H)$. Lưu ý rằng, L_{BS} luôn luôn lớn hơn hoặc bằng số gói Fountain được yêu cầu (H) và BS có thể phát số lượng gói Fountain rất lớn nếu như chất lượng kênh truyền giữa BS và D là xấu. Ngược lại, nếu như chất lượng kênh truyền giữa BS và D là tốt, thì ta kỳ vọng rằng D có thể nhận đủ H gói Fountain sau H khe thời gian $(L_{BS} = H)$. Một cách tương tự, chúng ta cũng ký hiệu L_E là số lượng gói tin mà E nhận đúng trong L_{BS} khe thời gian và chúng ta cũng mong đợi rằng L_E nhỏ hơn H để E không thể giải

mã thành công bản tin gốc của BS. Như đã đề cập ở trên, ta có xác suất giải mã và bảo mật thông tin thành công (Probability of Successful and Secure: SS) có thể được định nghĩa như sau:

$$SS = P_r\left(L_D = H, L_E < H\right) \quad (12)$$

Kế tiếp, xác suất đánh chặn (Intercept Probability: IP) tại E được viết như sau:

$$IP = P_r\left(L_E = H, L_D < H\right) \quad (13)$$

Cuối cùng, số lượng các gói Fountain trung bình được phát bởi BS là $E\{L_A\}$:

A. Xác suất giải mã và bảo mật thông tin thành công (Probability of Successful and Secure: SS)

Từ biểu thức (12), ta có biểu thức dạng chính xác của xác suất giải mã và bảo mật thông tin thành công, như sau:

$$SS = \sum_{L_{BS}=H}^{+\infty}\left[C_{L_{BS}-1}^{L_{BS}-H}\left(1-\rho_D\right)^H\left(\rho_D\right)^{L_{BS}-H}\right]\times\left[\sum_{L_E=0}^{H-1}C_{L_{BS}}^{L_E}\left(\rho_E\right)^{L_{BS}-L_E}\left(1-\rho_E\right)^{L_E}\right] \quad (14)$$

Để thể hiện các kết quả lý thuyết, ta cần phải cắt chuỗi vô cùng trong (14) bằng một giá trị hữu hạn nào đó. Thật vậy, ta có thể viết lại biểu thức (14) dưới dạng như sau:

$$SS \approx \sum_{L_{BS}=H}^{N_T}\left[C_{L_{BS}-1}^{L_{BS}-H}\left(1-\rho_D\right)^H\left(\rho_D\right)^{L_{BS}-H}\right]\times\left[\sum_{L_E=0}^{H-1}C_{L_{BS}}^{L_E}\left(1-\rho_E\right)^{L_E}\left(\rho_E\right)^{L_{BS}-L_E}\right] \quad (15)$$

Trong biểu thức (15), N_T là một hằng số và khi N_T đủ lớn thì giá trị của SS sẽ hội tụ về giá trị chính xác.

B. Xác suất đánh chặn (Intercept Probability: IP)

Tương tự, từ công thức (13), ta có biểu thức chính xác của xác suất đánh chặn tại nút nghe lén như sau:

$$IP = C_{L_{BS}-1}^{L_{BS}-H}C_{L_{BS}-1}^{L_{BS}-H}\left(\rho_D\right)^{L_{BS}-H}\left(1-\rho_D\right)^H\left(\rho_E\right)^{L_{BS}-H} \times\left(1-\rho_E\right)^H + C_{L_{BS}-1}^{L_{BS}-H}\left(1-\rho_E\right)^H\left(\rho_E\right)^{L_{BS}-H}\text{ x} \times\left[\sum_{u=0}^{H-1}C_{L_{BS}}^{u}\left(\rho_D\right)^{L_{BS}-u}\left(1-\rho_D\right)^u\right]. \quad (16)$$

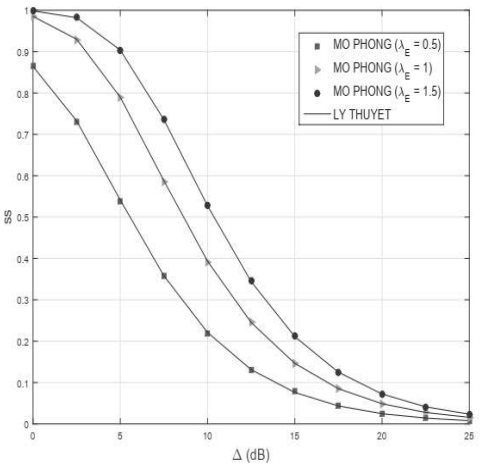
C. Số lượng các gói mã hóa trung bình được phát bởi BS (Average Number of Encoded Packets: ANEP)

Biểu thức chính xác của số lượng các gói Fountain trung bình được phát bởi trạm gốc (BS) cho bởi như sau (xem [24, eq. (8)])

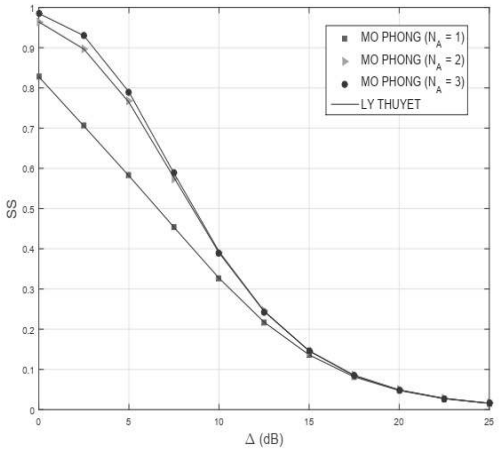
$$E\{L_A\} = \frac{H}{1-\rho_D} = \frac{H}{1-\left(1-\exp\left(-\frac{\lambda_D N_0}{P_{BS}}\gamma_{th}\right)\right)^{N_A}} \quad (17)$$

4. Kết quả mô phỏng và lý thuyết

Trong phần này, chúng tôi thực hiện các mô phỏng Monte-Carlo để kiểm chứng các biểu thức toán học đã được đưa ra ở trong phần III. Trong tất cả các mô phỏng, chúng tôi cố định ngưỡng dừng γ_{th} bằng 1, số gói mã hóa Fountain cần thiết phải đạt được để khôi phục lại dữ liệu gốc là $H = 5$ và giá trị của N_T được cố định bằng 500.



Hình 3. SS là một hàm của Δ (dB) khi λ_D = 0.5 và λ_E = 1:

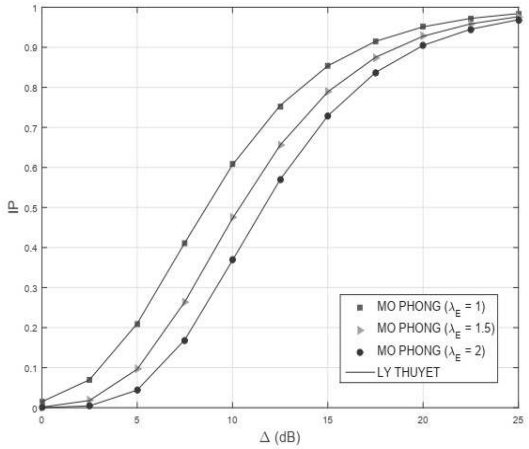


Hình 2. SS là một hàm của Δ (dB) khi λ_D = 0.5 và N_A = 3.

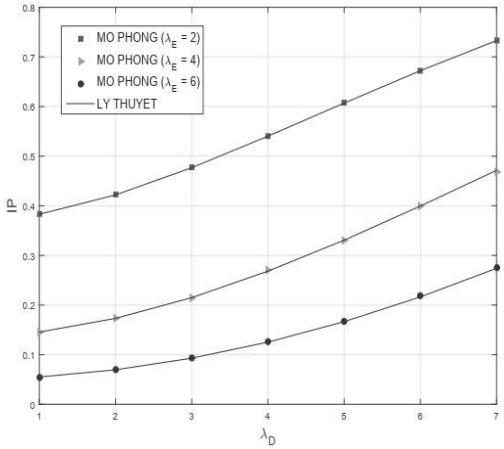
Trong Hình 2, giá trị của SS được thể hiện như là một hàm của SNR phát Δ ($\Delta = P_{BS}/N_0$) (dB) khi thay đổi các tham số đặc trưng kênh truyền của kênh nghe lén lần lượt là: $\lambda_E = 0,5$, $\lambda_E = 1$, và $\lambda_E = 1.5$. Ta cố định tham số đặc trưng kênh truyền

trên kênh chính $\lambda_D = 0.5$; số ăntен phát được trang bị tại BS là $N_A = 3$. Quan sát hình vẽ, ta thấy rằng xác suất giải mã và bảo mật thông tin thành công (SS) giảm nhanh khi tăng giá trị của Δ. Điều này có nghĩa là khi tăng Δ hay tăng mức công suất phát tại BS thì khả năng nghe lén của E sẽ tăng lên, đồng thời khả năng giải mã thành công thông tin gốc tại D tăng lên. Mặt khác, khi giá trị $\lambda_E = 1.5$ tại mức công suất phát là 0 dB, thì giá trị của SS gần bằng 1, có nghĩa là thông tin gốc sẽ được giải mã và bảo mật thành công tại D. Hơn nữa, như thể hiện trong Hình 2, thì giá trị của SS tăng khi λ_E tăng.

Hình 3, tiếp tục thể hiện giá trị của SS theo Δ ($\Delta = P_{BS} / N_0$) (dB), khi cố định $\lambda_D = 0.5$ và $\lambda_E = 1$. Như ta có thể quan sát, giá trị của SS giảm khi Δ tăng. Mặt khác, khi tăng số lượng anten tại máy phát N_A = (1 ÷ 3) thì tại mức công suất phát nhỏ hơn 15 dB, giá trị SS tăng lên. Tuy nhiên, khi tăng công suất phát Δ thì giá trị SS sẽ hội tụ khi tăng N_A.

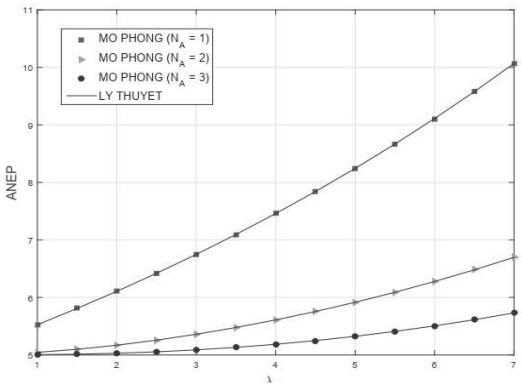


Hình 4. IP là một hàm của Δ (dB) khi λ_D = 0.5 và N_A = 3

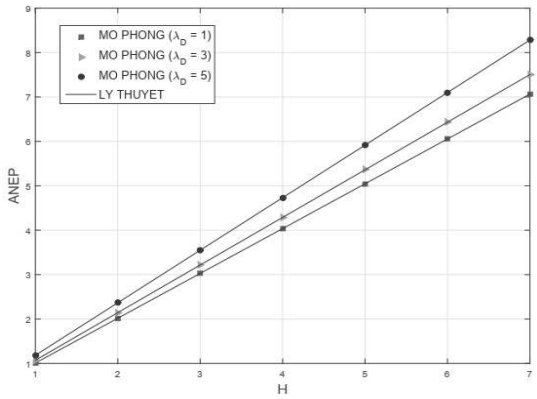


Hình 5. IP vẽ theo λ_D khi Δ = 10 (dB) và N_A = 2.

Trong Hình 4, chúng tôi vẽ giá trị của IP theo Δ ($\Delta = P_{BS} / N_0$) (dB), khi cố định $\lambda_D = 0.5$ và $N_A = 3$. Nhìn từ hình vẽ ta thấy rằng, giá trị của IP tăng khi Δ tăng. Tuy nhiên, tại mức công suất phát Δ nhỏ hơn 0 (dB), thì IP tiệm cận về giá trị không, có nghĩa rằng thông tin gốc được bảo mật thành công. Mặt khác, khi tăng λ_E, đồng nghĩa với chất lượng kênh nghe lén xấu, giá trị của IP giảm. Trong Hình 5, chúng tôi khảo sát ảnh hưởng của tham số đặc trưng kênh truyền lên giá trị của IP khi Δ = 10 (dB) và N_A = 2. Như ta có thể định lượng, IP sẽ giảm khi λ_E lớn. Hơn nữa, giá trị của IP tăng khi λ_D tăng.



Hình 6. Số lượng gói tin mã hóa trung bình (ANEP) được phát bởi BSlà một hàm của λ_D khi Δ = 10 (dB).



Hình 7. ANEP là một hàm của *H* khi N_A = 2.

Trong Hình 6, số lượng các gói tin mã hóa trung bình (ANEP) được phát bởi BS được vẽ theo hàm của λD khi cố định Δ = 10 (dB), với số ăntен phát khác nhau tại BS, cụ thể $N_A = 1, 2, 3$. Như

được thể hiện trong Hình 6, ANEP tăng khi tăng λ_D và khi *N*A được trang bị tại BS tăng thì ANEP giảm. Hình 7, chúng tôi tiếp tục thể hiện ANEP là một hàm của *H* khi cố định $N_A = 2$ và thay đổi các tham số đặc trưng của kênh chính, cụ thể $\lambda_D = 1, 3, 5$ .Nhìn vào hình vẽ ta thấy rằng, ANEP tăng khi tăng số gói Fountain được yêu cầu (*H*) tại D để có thể giải mã thành công thông tin gốc và ANEP giảm khi giảm λ_D . Hơn nữa, khi chất lượng kênh chính là xấu thì BS có thể phát nhiều gói tin mã hóa tới D, điều này sẽ làm tăng số khe thời gian được sử dụng và thời gian trễ của hệ thống. Như chúng ta quan sát từ Hình 2 đến Hình 7, các kết quả phân tích lý thuyết và kết quả mô phỏng hoàn toàn trùng khít nhau, điều này thể hiện tính chính xác của các kết quả phân tích.

5. Kết luận

Trong bài báo này, chúng tôi đã đề xuất và đánh giá hiệu năng bảo mật lớp vật lý sử dụng mã Fountain với kỹ thuật TAS tại trạm gốc (BS). Chúng tôi đưa ra các biểu thức dạng chính xác của xác suất giải mã và bảo mật thông tin thành công (SS) tại nút đích (D), xác suất đánh chặn (IP) tại nút nghe lén (E) và số lượng các gói mã hóa trung bình được phát bởi BS. Các kết quả đã thể hiện rằng, để đạt được hiệu năng bảo mật của hệ thống thì yêu cầu công suất phát của BS phải nhỏ và cần tăng số lượng anten phát tại BS một cách thích hợp. Mặt khác, hiệu năng bảo mật của hệ thống phụ thuộc rất lớn bởi các tham số đặc trưng của kênh truyền.

Trong hầu hết các công trình nghiên cứu trước về bảo mật lớp vật lý thì phần cứng của thiết bị trong mạng được giả sử là hoàn hảo. Tuy nhiên,trong thực tế, phần cứng của các thiết bị vô tuyến luôn là không hoàn hảo do nhiễu pha, sự không cân bằng I/Q và các bộ khuếch đại phi tuyến. Bảo mật lớp vật lý sử dụng mã fountain với kỹ thuật chọn lựa anten phát được áp dụng trong điều kiện phần cứng khiếm khuyết, kỹ thuật này được ứng dụng cho những mạng truyền thông vô tuyến như mạng cảm biến, mạng ad-hoc hay mạng IoT phổ biến hiện nay.

Với phương pháp sử dụng mã fountain với kỹ thuật chọn lựa anten phát để nâng cao hiệu năng bảo mật của hệ thống thì cần phải giảm số lần truyền các gói mã hóa và tăng số anten tại nút nguồn thứ cấp SS một cách phù hợp để nâng cao chất lượng của kênh hợp pháp.

TÀI LIỆU THAM KHẢO

1. Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in mimo wiretap channels using general-order transmit antenna selection with outdated csi," *IEEE Trans. Commun.*, vol. 63, no. 8, pp. 2959–2971, Aug. 2015.
2. M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*,vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
3. C. E. Shannon, "Communication theory of secrecy systems," *BellSyst. Technol. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
4. D. Wyner, "The wire-tap channel," *Bell Syst. Technol. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
5. F. A. Khan, K. Tourki, M.-S. Alouini, and K. A. Qaraqe, "Outage and ser performance of spectrum sharing system with tas/mrc," in *Communications Workshops (ICC), Proc. IEEE Commun. Conf.*, Budapest, Hungary, Jun. 2013, pp. 381–385. [6]
6. F. A. Khan, K. Tourki, M. Alouini, and K. A. Qaraqe, "Performance analysis of a power limited spectrum sharing system with tas/mrc," *IEEE Trans. Signal Process.*, vol. 62, no. 4, pp. 954–967, Feb. 2014.
7. K. Tourki, F. A. Khan, K. A. Qaraqe, H.-C. Yang, and M.-S. Alouini, "Exact performance analysis of mimo cognitive radio systems using transmit antenna selection," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 3, pp. 425–438, Mar. 2014.
8. N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in mimo wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.
9. S. Yan, N. Yang, R. Malaney, and J. Yuan, "Transmit antenna selection with alamouti coding and power allocation in mimo wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3,pp. 1656–1667, Mar. 2014.
10. J. Xiong, Y. Tang, D. Ma, P. Xiao, and K.-K. Wong, "Secrecy performance analysis for tas-mrc system with imperfect feedback," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 8, pp. 1617–1629, Aug. 2015.
11. N. Li, X. Tao, H. Wu, J. Xu, and Q. Cui, "Large-system analysis of artificial-noise-assisted communication in the multiuser downlink: Ergodic secrecy sum rate and optimal power allocation," *IEEETrans. Veh. Technol.*, vol. 65, no. 9, pp. 7036–7050, Sept. 2016.

12. J. H. Lee and W. Choi, "Multiuser diversity for secrecy communications using opportunistic jammer selection: Secure dof and jammer scaling law," *IEEE Trans. Signal Process.*, vol. 62, no. 4, pp. 828–839, Feb. 2014.
13. S.-I. Kim, I.-M. Kim, and J. Heo, "Secure transmission for multiuse relay networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp.3724–3737, Jul. 2015.
14. T. T. Duy, T. Q. Duong, T. L. Thanh, and V. N. Q. Bao, "Secrecy performance analysis with relay selection methods under impact of co-channel interference," *IET Communications*, vol. 9, no. 11, pp.1427–1435, Jul. 2015.
15. D. T. Hung, T. T. Duy, D. Q. Trinh, V. N. Q. Bao, and T. Hanh, "Impact of hardware impairments on secrecy performance of multihop relay networks in presence of multiple eavesdroppers," in *TheThird Nafosted Conference on Information and Computer Science(NICS2016)*, Danang city, Vietnam, Sep. 2016, pp. 113–118.
16. T. T. Phu, D. T. Hung, T. D. Tran, and M. Voznák, "Analysis of ˇ probability of non-zero secrecy capacity for multi-hop networks in presence of hardware impairments over nakagami-m fading channels," *RadioEngineering*, vol. 25, no. 4, pp. 774–782, Dec. 2016.
17. P. T. Tin, T. T. Duy, P. T. Tran, and M. Voznak, "Secrecy performance of joint relay and jammer selection methods in cluster networks: With and without hardware noises," in *The InternationalConference on Advanced Engineering–Theory and Applications (AETA2016)*, Busan, Korea, Dec. 2016, pp. 769–779.
18. M. Luby, "Lt codes," in *Proc. 43rd Annual IEEE Symp. on Foundations of Computer Science*, Vancouver, Canada, Nov. 2002, pp. 271–282.

A. Shokrollahi, "Raptor codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 6, pp. 2551–2567, Jun. 2006.

19. J. Castura and Y. Mao, "Rateless coding for wireless relay channels," *IEEE Trans. Wireless Commun.*, vol. 6, no. 5, pp. 1638–1642, May2007.
20. T. T. Duy and H. Y. Kong, "Secondary spectrum access in cognitive radio networks using rateless codes over rayleigh fading channels," *Wireless Pers. Commun.*, vol. 77, no. 2, pp. 963–978, Jul. 2014.
21. D. T. Hung, T. T. Duy, V. N. Q. Bao, D. Q. Trinh, and T. Hanh, "Phân tích hiệu năng mô hình truyền Đường xuống sử dụng kỹ thuật chọn lựa Ăntен phát và mã fountain dưới sự Ảnh hưởng của nhiễu Đồng kênh," in *Hội thảo Quốc gia 2017 về điện tử, Truyền thôngvà Công nghệ Thông tin (REV-ECIT 2017)*, TP. HCM, Viet Nam, 12/ 2017, pp. 270–274.
22. P. T. D. Ngoc, T. T. Duy, V. N. Q. Bao, and H. V. Khuong, "Đánh giá hiệu năng mạng vô tuyến nhận thức dạng nền với tas/sc và suy hao phần cứng," *Hội thảo Quốc gia 2015 về điện tử, Truyền thông và Công nghệ Thông tin (REV-ECIT 2015)*, pp. 477–481, 12/ 2015.
23. X. Wang, W. Chen, and Z. Cao, "A rateless coding based multi-relay cooperative transmission scheme for cognitive radio networks," in *IEEE GLOBECOM*, Honolulu, HI, Dec. 2009, pp. 1–6

PHYSICAL SECURITY USING FOUNTAIN CODES WITH ANTENNA SELECTION TECHNIQUE

Nguyen Thac Dung, Dang xuan Hai, Dinh Cong Hung, Nguyen Van Anh, Nguyen Duc Tuan, Ta Huu Long

Telecommunication University

Summary: *In this article, we propose a physical security model using Fountain codes with the antenna selection technique at the base station (BS). In the proposed model, a base station (BS) with multi antenna transmits data to a legitimate user (D), in the appearance of an illegal eavesdropper (E), assuming that both D and E are the terminal equipments with single antenna. We give explicit expressions of decrypted probability and successful information security (SS) at the destination node, interception probability (IP) at the eavesdropping node and the average number of encrypted packets transmitted by BS (ANEP) on the Rayleigh fading channel. Finally, we perform a Monte Carlo simulation to verify the mathematical expressions found.*

Keywords: *Fountain codes, antenna selection technique, physical security, Rayleigh fading channel.*