Tạp chí Khoa học Trường Đại học Bạc Liêu
BLU Journal of Science
ISSN: 2734-973X
Số 5(9), 02-11 (2024)

PHÂN TÍCH HIỆU NĂNG CỦA GIAO THỨC MIMO TAS/SC SỬ DỤNG MÃ FOUNTAIN TRÊN CÁC KÊNH FADING RAYLEIGH

PERFORMANCE ANALYSIS OF MIMO TAS/SC PROTOCOLS USING FOUNTAIN CODES OVER RAYLEIGH FADING CHANNELS

Nguyễn Thạc Dũng*, Nguyễn Đức Tuấn

Trường Đại học Thông tin liên lạc
* tcu@tsqtt.edu.vn

Ngày nhận bài: 07/8/2024
Ngày chấp nhận đăng: 20/9/2024

ABSTRACT

In this paper, we analyze performance of multiple input multiple output (MIMO) protocols ex ploiting Fountain Codes (FCs), where a transmitter (Alice) is equipped with multi-antennas using transmit antenna selection (TAS) technique to transmit its encoded packets to a legitimate receiver (Bob) in the presence of an eavesdropper (Eve). Moreover, both Bob and Eve nodes are equipped with multi-antenna receiver using selection combining (SC) method to decode the original information which is transmitted by Alice. To evaluate the performance of the proposed secure communication protocols, the article presents exact closed-form expressions for the success decoding probability and security performance (SS). To enhance security performance, the transmit power at A must be significantly reduced to degrade the eavesdropper's link quality. The paper also provides the interception probability (IP) and the average number of encoded packets (AP) over Rayleigh fading channels. To improve security performance, the appropriate number of antennas must be designed for both A and B. Moreover, power allocation at A should be optimized to transmit only the necessary amount required to block E, the entity attempting to eavesdrop on the original data from A. Finally, Monte Carlo simulations are conducted to verify the theoretical results..

Keywords: *Fountain codes, MIMO, TAS/SC, physical-layer security, Rayleigh fading channels.*

TÓM TẮT

Bài báo này phân tích hiệu năng của các giao thức MIMO sử dụng mã Fountain (FCs), trong đó một máy phát (Alice) được trang bị nhiều anten sử dụng kỹ thuật lựa chọn anten phát (TAS) để truyền các gói mã hóa đến một máy thu hợp pháp (Bob) trong bối cảnh có kẻ nghe trộm (Eve). Hơn nữa, cả Bob và Eve đều được trang bị máy thu nhiều anten sử dụng phương pháp kết hợp lựa chọn (SC), để giải mã thông tin gốc được truyền bởi Alice. Để đánh giá hiệu năng của các giao thức truyền thông bảo mật được đề xuất, bài báo đưa ra các biểu thức dạng đóng chính xác của xác suất giải mã thành công và bảo mật (SS) để cải thiện hiệu suất bảo mật, cần giảm đáng kể công suất phát tại A để giảm chất lượng liên kết của kẻ nghe lén; xác suất chặn (IP), và số lượng trung bình các gói mã hóa (AP) trên các kênh fading Rayleigh. Để cải thiện hiệu suất bảo mật cần thiết kế

Từ khóa: *Mã Foutain, MIMO, TAS/SC, bảo mật lớp vật lý, kênh fading Rayleigh.*

số lượng anten phù hợp cho cả A và B. Hơn nữa, việc phân bổ công suất tại A chỉ cần phát đủ mức cần thiết để ngăn chặn E, người cố gắng nghe lén dữ liệu gốc từ A. Sau đó, các mô phỏng Monte Carlo được thực hiện để kiểm chứng các kết quả lý thuyết.

1. Giới thiệu

Dựa trên đặc tính phát sóng của truyền thông vô tuyến, những kẻ nghe trộm có thể dễ dàng nghe lén và chặn dữ liệu truyền tải. Truyền thống, để đạt được truyền thông an toàn, các phương pháp mã hóa dựa vào quản lý và phân phối khóa bí mật đã được triển khai rộng rãi trong các hệ thống truyền thông thực tế ở các tầng cao hơn (B. Schneier, 1998) ví dụ, tầng ứng dụng. Tuy nhiên, các kỹ thuật này chưa xem xét đến khả năng của những kẻ nghe trộm, trong đó khả năng tính toán của họ có thể không giới hạn trong tương lai.

Bảo mật lớp vật lý PLS, (C. E. Shannon,1949; M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, 2008), (A. Wyner, 1975) đã được đề xuất gần đây như là một trong những giải pháp hiệu quả để tăng cường bảo mật trong các hệ thống truyền thông vô tuyến bằng cách khai thác các đặc tính của kênh vô tuyến. Ngoài ra, PLS có thể được sử dụng bổ sung cho các phương pháp mã hóa truyền thống. Trong (K. Cao, 2017) các tác giả đã đề xuất các phương án gây nhiễu hợp tác bằng cách truyền các tín hiệu nhiễu nhân tạo (AN) đến các kẻ nghe trộm để giảm chất lượng của các liên kết nghe trộm. Kết quả trong (J.-M. Kang, J. Yang, J. Ha, and Il-Min Kim, 2017) cho thấy rằng việc kết hợp các sơ đồ truyền thông đa dạng và kỹ thuật gây nhiễu đạt được chất lượng truyền thông dữ liệu an toàn tốt hơn so với các mạng hợp tác truyền thống mà không sử dụng tín hiệu gây nhiễu (H. Guo, 2017; N.-E. Wu and H.-J. Li, 2013). Để nâng cao khả năng bảo mật, các tác giả (T. T. Duy, T. Q. Duong, T. L. Thanh, and V. N. Q. Bao, 2015) đã đề xuất các sơ đồ lựa chọn bộ lặp cho truyền thông hợp tác dưới tác động của nhiễu đồng kênh và hiệu suất bảo mật của các mạng hợp tác vô tuyến nhận thức dưới mức cũng đã được nghiên cứu trong (T. T. Duy and P. N. Son, 2015). Hơn nữa, để cải thiện việc truyền tải an toàn trong truyền thông vô tuyến, PLS với các kênh MIMO nghe lén (T. Liu and S. Shamai ,2009; T. F. Wong, M. Bloch, 2009) cũng đã được nghiên cứu. Ngoài ra, một số công trình trong tài liệu (H. Alves, R. D. Souza, M. Debbah, and M. Bennis, 2012; N. Yang, H. Suraweera, I. Collings, and C. Yuen, 2013) đã chỉ ra rằng bằng cách sử dụng lựa chọn ăng-ten phát TAS tại bộ phát đa ăng-ten, lợi thế là bộ phát hợp pháp chỉ truyền chỉ số của ăng-ten có điều kiện kênh tốt nhất dựa trên tín hiệu phản hồi từ bộ thu hợp pháp. Mặc dù kẻ nghe lén có thể truy cập vào kênh phản hồi công khai, nhưng chỉ số ăng-ten này không phải là tối ưu đối với kẻ nghe lén. Vì vậy, điều này có thể cải thiện bảo mật với cấu trúc phần cứng đơn giản, giảm chi phí và tiêu thụ năng lượng nhưng vẫn đạt được đầy đủ đa dạng truyền thông (P. L. Yeoh, M. Elkashlan, and I. B. Collings, 2011)

Để khắc phục các vấn đề cơ bản trong truyền thông vô tuyến như tạp âm, fading, nhiễu giao thoa, bóng mờ và suy hao đường truyền, những yếu tố này thường xuyên thay đổi trong các kênh vô tuyến trong suốt thời gian truyền tải. Gần đây, mã Fountain FC, hay mã rateless (M. Luby, 2002; T. T. Duy and H. Y. Kong, 2014) đã thu hút sự chú ý lớn do khả năng thích ứng hiệu quả với nhiều điều kiện kênh khác nhau mà không cần biết thông tin trạng thái kênh CSI tại máy phát trước khi truyền các gói mã hóa và đã được áp dụng rộng rãi trong nhiều hệ thống truyền thông để cải thiện hiệu suất hệ thống. Trái ngược với các mã cố định tỉ lệ truyền thống, trong mã Fountain, một máy phát sử dụng bộ mã Fountain có thể tạo ra số lượng không giới hạn các gói mã hóa từ các ký hiệu nguồn của thông điệp gốc và truyền chúng đến các máy thu được chỉ định. Sau đó, máy thu thu thập các gói mã hóa này nếu thu đủ số lượng gói mã hóa, nó có thể giải mã và phục hồi thông điệp gốc. Tuy nhiên, do bản chất phát sóng của các truyền dẫn vô tuyến, những kẻ nghe trộm có thể dễ dàng chặn các gói mã hóa này để xây dựng lại dữ liệu nguồn. Vì vậy, thông tin bảo mật trở thành vấn đề quan trọng trong các hệ thống truyền thông

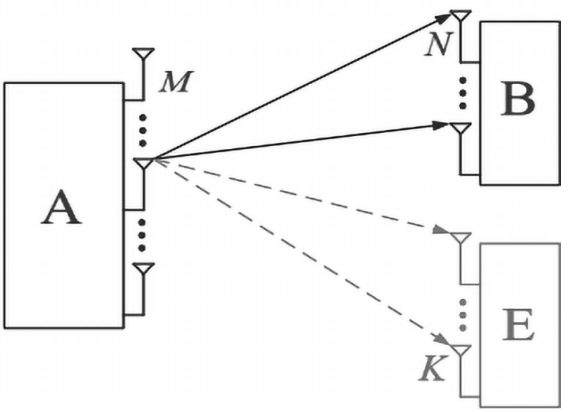
dựa trên FC.

Gần đây, có một số nghiên cứu trong tài liệu đã sử dụng FC để đạt được truyền thông an toàn (H. Niu, M. Iwai, K. Sezaki, L. Sun, and Q. Du, 2014; D. T. Hung, T. T. Duy, D. Q. Trinh, and V. N. Q. Bao, 2018). Trong (H. Niu, M. Iwai, K. Sezaki, L. Sun, and Q. Du, 2014), các tác giả đã phân tích một sơ đồ truyền tải an toàn khai thác FC, trong đó cả máy thu hợp pháp và kẻ nghe trộm sẽ cố gắng thu đủ số gói mã hóa để phục hồi dữ liệu gốc. Kết quả cho thấy truyền tải an toàn có thể đạt được nếu người dùng hợp pháp thu được đủ số gói Fountain trước kẻ nghe trộm tại cùng một thời điểm. Trong (W. Li, Q. Du, L. Sun, P. Ren, and Y. Wang, 2016), một cơ chế mã hóa Fountain động tại máy phát đã được đề xuất để tăng cường dữ liệu an toàn với tốc độ giải mã cao hơn cho người dùng hợp pháp và xác suất chặn thấp hơn cho kẻ nghe trộm. Trong (L. Sun, P. Ren, Q. Du, and Y. Wang, 2016), đã đề xuất một giao thức bảo mật của hệ thống relay hợp tác dựa trên FCs trong tình huống có kẻ nghe lén, và để cải thiện truyền thông an toàn, đã sử dụng một kế hoạch gây nhiễu hợp tác tạo ra tín hiệu nhiễu nhân tạo để giảm chất lượng tín hiệu thu tại kẻ nghe lén và hợp tác với nguồn để loại bỏ nhiễu tại điểm đích. Hơn nữa, ở (D. T. Hung, T. T. Duy, D. Q. Trinh, and V. N. Q. Bao, 2018) các tác giả đã đề xuất một giao thức chọn anten phát (TAS) sử dụng FC dưới tác động của các vấn đề về phần cứng. Để tăng cường hiệu suất bảo mật của hệ thống được đề xuất, một bộ gây nhiễu hợp tác được sử dụng để liên tục phát tín hiệu nhiễu nhân tạo đến kẻ nghe lén và loại bỏ nhiễu do nút gây nhiễu gây ra tại bộ thu hợp pháp. Ngoài ra, trong (Q. Du, Y. Xu, W. Li, and H. Song, 2018), các tác giả đã nghiên cứu các mạng đa điểm sử dụng FCs trên "Internet vạn vật" (IoT) để cải thiện hiệu suất bảo mật.

Trong bài báo đề xuất một giao thức MIMO TAS/SC khai thác FC để cải thiện hiệu năng bảo mật, trong đó nguồn (A) được trang bị nhiều anten và chọn anten tốt nhất để gửi các gói mã hóa đến đích (B) trong bối cảnh có kẻ nghe trộm (E) cố gắng nghe lén dữ liệu được phát từ nguồn. Cả điểm đích và các nút nghe trộm đều sử dụng nhiều anten và kỹ thuật kết hợp lựa chọn (SC) để giải mã thông tin gốc. Khi điểm đích có thể thu đủ số gói mã hóa để phục hồi thành công dữ liệu gốc, nó sẽ gửi một tín hiệu phản hồi đến nguồn để kết thúc việc truyền dữ liệu giữa nguồn và điểm đích. Truyền thông bảo mật có thể đạt được nếu nút nghe trộm không thu đủ số gói mã hóa cùng lúc, nó không thể giải mã dữ liệu gốc. Nếu không, thông tin gốc sẽ bị nghe lén. Để đánh giá hiệu năng bảo mật của các giao thức đề xuất, bài báo tính toán chính xác các biểu thức dạng đóng cho xác suất giải mã thành công, độ bảo mật (SS) và xác suất chặn (IP) trên các kênh fading Rayleigh. Hơn nữa, số lượng trung bình các gói mã hóa được nguồn (A) sử dụng cũng được đánh giá. Cuối cùng, thực hiện các mô phỏng Monte Carlo để kiểm chứng các kết quả lý thuyết. Bài báo được tổ chức như sau. Phần 2 mô tả mô hình hệ thống của các sơ đồ đề xuất. Phân tích hiệu năng bảo mật của các giao thức đề xuất trong Phần 3. Các kết quả mô phỏng được trình bày trong Phần 4. Cuối cùng, kết luận của bài báo này được đưa ra trong Phần 5.

2. Mô hình hệ thống

Hình 1: Mô hình hệ thống của các giao thức được đề xuất



Hình 1 trình bày một mô hình hệ thống vô tuyến của các giao thức truyền thông bảo mật, trong đó nguồn hợp pháp, Alice (A) với nhiều ăng-ten ($m = 1, 2, \ldots, M$) sử dụng giao thức TAS để gửi dữ liệu của mình đến điểm đích được chỉ định là Bob (B), trong bối cảnh có một kẻ nghe lén được gọi là Eve (E), người cố gắng nghe trộm dữ liệu được phát từ nút A. Liên kết dữ liệu giữa A và B được gọi là kênh chính, trong khi liên kết giữa A và E được gọi là kênh nghe lén.

Giả định rằng cả B và E đều được trang bị nhiều ăng-ten thu, nghĩa là (n = 1, 2, …, N) và (k = 1, 2, …, K) sử dụng phương pháp kết hợp lựa chọn (SC) để kết hợp các tín hiệu thu được. Trong FC, nguồn (A) chia dữ liệu gốc bảo mật của mình thành các gói L có cùng độ dài. Để tạo các gói được mã hóa thích hợp, một hoặc nhiều gói được chọn ngẫu nhiên từ các gói L này và thực hiện phép XOR với nhau. Tại mỗi khe thời gian, A sử dụng kỹ thuật TAS để phát mỗi gói mã hóa của mình đến B. Tuy nhiên, do tính chất phát sóng của kênh vô tuyến, các gói mã hóa này cũng sẽ dễ dàng được thu bởi nút E. Sau đó, cả B và E sẽ cố gắng giải mã các gói mã hóa đã thu và lưu trữ chúng vào bộ đệm của họ trong thời gian này. Hơn nữa, dữ liệu gốc được giả định là phục hồi thành công nếu các thiết bị thu này có thể thu đúng ít nhất H gói mã hóa, trong đó $H = (1 + \varepsilon) L$, với ε là độ dư thừa giải mã phụ thuộc vào thiết kế mã cụ thể (J. Castura and Y. Mao, 2007). Khi B có thể thu đủ số gói mã hóa để giải mã dữ liệu gốc từ A, nó sẽ gửi một thông báo phản hồi để thông báo cho A dừng phát dữ liệu. Đồng thời, nếu E không thu đủ các gói mã hóa để giải mã dữ liệu gốc, thì giao tiếp bảo mật được thực hiện. Ngược lại, thông tin gốc của A sẽ bị đánh chặn.

Tiếp theo, xem xét việc truyền dữ liệu tại một khe thời gian tùy ý. Giả sử $\lambda_{m,n}$ là độ lợi kênh giữa ăng-ten thứ m_{th} của A và ăng-ten thứ n_{th} của B, với m = 1, 2, …, M và n = 1, 2, …, N. Tương tự, chúng tôi ký hiệu $\varphi_{m,k}$ là độ lợi kênh giữa ăng-ten thứ m_{th} của A và ăng-ten thứ k_{th} của B, tương ứng, với k = 1, 2, …, K. Giả định rằng mô hình của các kênh là fading Rayleigh khối, có nghĩa là các hệ số kênh không đổi trong khe thời gian này nhưng thay đổi độc lập qua các khe thời gian khác nhau. Do đó, độ lợi kênh $\lambda_{m,n}$ và $\varphi_{m,k}$ là các biến ngẫu nhiên phân phối mũ (RVs), có các hàm phân phối tích lũy (CDF) được cho bởi:

$$\begin{aligned} F_{\gamma_{m,n}}(x) &= 1-\exp(-\lambda x), \\ F_{\varphi_{m,n}}(x) &= 1-\exp(-\Omega x), \end{aligned} \qquad (1)$$

trong đó $\lambda = 1/\mathrm{E}\{\gamma_{m,n}\}$, $\Omega = 1/\mathrm{E}\{\varphi_{m,n}\}$, và E {.} là toán tử kỳ vọng. A sử dụng ăng-ten thứ m_{th} để phát gói mã hóa của mình đến ăng-ten thứ n_{th} của B, và B sẽ kết hợp các tín hiệu thu được bằng cách sử dụng phương pháp SC. Do đó, tỷ lệ tín hiệu trên tạp (SNR) tức thời thu được tại B được cho bởi:

$$\Psi^{\mathrm{B}}_{m,n} = \max_{n=1,2,\ldots,N}\left(\frac{P_{\mathrm{A}}}{N_0}\gamma_{m,n}\right) = \frac{P_{\mathrm{A}}}{N_0}\max_{n=1,2,\ldots,N}\left(\gamma_{m,n}\right), \quad (2)$$

trong đó P_{A} là công suất phát tại ăng-ten thứ m_{th} của A (cũng là công suất phát tại các ăng-ten khác), N_0 là phương sai của nhiễu Gaussian tại B (giả định rằng tất cả các nhiễu Gaussian trắng cộng tại các thiết bị thu có phân phối Gaussian với trung bình bằng 0 và phương sai là N_0). Với kỹ thuật TAS tại A, nó sẽ chọn ăng-ten tốt nhất để phục vụ B, sử dụng công thức sau:

$$b = \arg\max_{m=1,2,\ldots,M}\left(\Psi^{\mathrm{B}}_{m,n}\right) \qquad (3)$$

trong đó b = 1, 2, …, M. Xét tại một khe thời gian tùy ý với phương pháp TAS/SC, SNR tức thời thu được tại B có thể được tính như sau:

$$\begin{aligned} \Psi^{\mathrm{B}}_{b} &= \max_{m=1,2,\ldots,M}\left(\Psi^{\mathrm{B}}_{m,n}\right) \\ &= \frac{P_{\mathrm{A}}}{N_0}\max_{m=1,2,\ldots,M}\max_{n=1,2,\ldots,N}\left(\gamma_{m,n}\right) \end{aligned} \quad (4)$$

Tương tự, SNR tức thời thu được tại E trong một khe thời gian tùy ý có thể được cho bởi:

$$\Psi^{\mathrm{E}}_{b} = \frac{P_{\mathrm{A}}}{N_0}\max_{k=1,2,\ldots,K}\left(\gamma_{b,k}\right). \qquad (5)$$

Tiếp theo, giả định rằng một gói mã hóa có thể được giải mã thành công nếu SNR thu được tại tất cả các thiết bị thu cao hơn hoặc bằng ngưỡng định trước, ký hiệu là γ_{th} . Nếu không, gói mã hóa không thể được giải mã thành công. Do đó, xác suất mà B không thể thu đúng một gói mã hóa được biểu diễn như sau:

$$\rho_{\mathrm{B}} = \Pr\left(\Psi^{\mathrm{B}}_{b} < \gamma_{\mathrm{th}}\right) = F_{\Psi^{\mathrm{B}}_{b}}\left(\gamma_{\mathrm{th}}\right), \qquad (6)$$

Tương tự, xác suất mà E không thể thu đúng một gói mã hóa được tính như sau:

$$\rho_{\mathrm{E}} = \Pr\left(\Psi^{\mathrm{E}}_{b} < \gamma_{\mathrm{th}}\right) = F_{\Psi^{\mathrm{E}}_{b}}\left(\gamma_{\mathrm{th}}\right), \qquad (7)$$

Hơn nữa, xác suất mà B và E có thể giải mã thành công một gói mã hóa được cho bởi 1- ρ_{B} và 1 - ρ_{E}, tương ứng. Lưu ý rằng xác suất giải mã thành công hay không thành công của một gói mã hóa tại mỗi khe thời gian là như nhau.

Trước khi xem xét các tham số hiệu suất hệ thống trong bài báo này, chúng tôi giả sử L_{A} là tổng số gói mã hóa được gửi bởi A. Tiếp theo, chúng tôi cũng ký hiệu L_{B} và L_{E} là số gói mã hóa

được thu đúng bởi B và E, tương ứng. Khi B thu đủ số gói mã hóa thì B ngay lập tức gửi tín hiệu phản hồi để thông báo cho A dừng phát dữ liệu của mình.

Hơn nữa, chúng tôi giả định rằng B có thể giải mã thành công dữ liệu gốc nếu B thu đủ H gói mã hóa. Do đó, xác suất mà B giải mã thành công và bảo mật (SS) có thể được công thức hóa như sau:

$$\mathrm{SS}=\Pr\left(L_{\mathrm{B}}=H, L_{\mathrm{E}}<H \,|\, L_{\mathrm{A}}\right), \quad (8)$$

Tiếp theo, xác suất đánh chặn (IP) mà E có thể thu các gói trước hoặc cùng lúc với B có thể được định nghĩa như sau:

$$\mathrm{IP}=\Pr\left(L_{\mathrm{E}}=H, L_{\mathrm{B}}\le H \,|\, L_{\mathrm{A}}\right), \quad (9)$$

Cuối cùng, chúng tôi xem xét số trung bình của các gói mã hóa được phát bởi A, có thể được biểu diễn chính xác như sau (xem phương trình (8)):

$$\mathrm{E}\{L_{\mathrm{A}}\}=\frac{H}{1-\rho_{\mathrm{B}}}. \quad (10)$$

3. Phân tích hiệu suất

3.1 Chuẩn bị toán học của ρ_{B} và ρ_{E}

Trong phần này, để thực hiện các kết quả toán học dẫn xuất từ (4), hãy xem xét biến ngẫu nhiên (RV) Z_1, $Z_1=\max\limits_{m=1,2,\ldots,M}\max\limits_{n=1,2,\ldots,N}\left(\gamma_{m,n}\right)$, có CDF của Z1 có thể được viết như sau:

$$F_{Z_1}(x)=\Pr(Z_1<x)$$
$$=\Pr\left(\max_{m=1,2,\ldots,M}\max_{n=1,2,\ldots,N}\left(\gamma_{m,n}\right)<x\right), \quad (11)$$

Áp dụng phương trình (22) của (T. T. Duy and P. N. Son, 2015), CDF của Z_1 có thể được tính như sau:

$$F_{Z_1}(x)=\left[F_{\gamma_{m,n}}(x)\right]^{MN}=\left(1-\exp(-\lambda x)\right)^{MN}. \quad (12)$$

Ngoài ra, thay thế (12) vào (4), chúng ta có thể viết lại CDF của Ψ_b^{B} như sau:

$$F_{\Psi_b^{\mathrm{B}}}(x)=\Pr\left(\Psi_b^{\mathrm{B}}<x\right)=\Pr\left(Z_1<\frac{N_0}{P_{\mathrm{A}}}x\right)$$
$$=F_{Z_1}\left(\frac{N_0}{P_{\mathrm{A}}}x\right)=\left(1-\exp\left(-\frac{\lambda N_0}{P_{\mathrm{A}}}x\right)\right)^{MN}. \quad (13)$$

Tương tự, từ (5), xem xét RV Z_2, trong đó $Z_2=\max\limits_{k=1,2,\ldots,K}\left(\gamma_{b,k}\right)$, có CDF của Z_2 có thể được biểu diễn như sau:

$$F_{Z_2}(x)=\Pr(Z_2<x)=\Pr\left(\max_{k=1,2,\ldots,K}\left(\gamma_{b,k}\right)<x\right)$$
$$=\left[F_{\gamma_{b,k}}(x)\right]^{K}=\left(1-\exp(-\Omega x)\right)^{K}. \quad (14)$$

Sử dụng (14) vào (5), hàm phân phối tích lũy (CDF) của Ψ_b^{E} được viết dưới dạng sau:

$$F_{\Psi_b^{\mathrm{E}}}(x)=\Pr\left(\Psi_b^{\mathrm{E}}<x\right)=\Pr\left(Z_2<\frac{N_0}{P_{\mathrm{A}}}x\right)$$
$$=F_{Z_2}\left(\frac{N_0}{P_{\mathrm{A}}}x\right)=\left(1-\exp\left(-\frac{\Omega N_0}{P_{\mathrm{A}}}x\right)\right)^{K}. \quad (15)$$

Thay thế CDF của Ψ_b^{B} và Ψ_b^{E} vào (6) và (7), ta có xác suất rằng cả B và E đều không thể thu đúng một gói mã hóa, tương ứng là:

$$\rho_{\mathrm{B}}=\left(1-\exp\left(-\frac{\lambda N_0}{P_{\mathrm{A}}}\gamma_{\mathrm{th}}\right)\right)^{MN}, \quad (16)$$

$$\rho_{\mathrm{E}}=\left(1-\exp\left(-\frac{\lambda N_0}{P_{\mathrm{A}}}\gamma_{\mathrm{th}}\right)\right)^{K}, \quad (17)$$

3.2 Xác suất giải mã thành công và bảo mật

Từ (8), xác suất tổng thể của SS có thể được viết như sau:

$$\mathrm{SS}=\sum_{L_{\mathrm{A}}=H}^{+\infty}\Pr\left(L_{\mathrm{B}}=H|L_{\mathrm{A}}\right)\mathrm{x}\sum_{G=0}^{H-1}\Pr\left(L_{\mathrm{E}}=G|L_{\mathrm{A}}\right) \quad (18)$$

trong đó $\Pr\left(L_{\mathrm{B}}=H \,|\, L_{\mathrm{A}}\right)$ là xác suất rằng B có thể thu đúng H gói mã hóa dưới điều kiện số lượng gói truyền tối đa của A là L_{A}. Ngoài ra, $\Pr\left(L_{\mathrm{B}}=H \,|\, L_{\mathrm{A}}\right)$ là xác suất rằng E có thể thu được G gói mã hóa cùng lúc, trong đó $(0\le G<H)$.

Sử dụng phương trình (8) của (T.T. Duy and H. Y. Kong, 2024), xác suất $\Pr\left(L_{\mathrm{B}}=H \,|\, L_{\mathrm{A}}\right)$ có thể được tính như sau:

$$\Pr\left(L_{\mathrm{B}}=H \,|\, L_{\mathrm{A}}\right)=C_{L_{\mathrm{A}}-1}^{L_{\mathrm{A}}-H}\left(1-\rho_{\mathrm{B}}\right)^{H}\left(\rho_{\mathrm{B}}\right)^{L_{\mathrm{A}}-H} \quad (19)$$

Tương tự, ta có xác suất $\Pr\left(L_{\mathrm{E}}=G \,|\, L_{\mathrm{A}}\right)$ là:

$$\Pr\left(L_{\mathrm{E}}=G \,|\, L_{\mathrm{A}}\right)=C_{L_{\mathrm{A}}}^{G}\left(1-\rho_{\mathrm{E}}\right)^{G}\left(\rho_{\mathrm{E}}\right)^{L_{\mathrm{A}}-G}, \quad (20)$$

Thay thế (19) và (20) vào (18), ta thu được biểu thức chính xác dưới dạng đóng của SS như sau:

$$\mathrm{SS}=\sum_{L_{\mathrm{A}}=H}^{+\infty}\left[C_{L_{\mathrm{A}}-1}^{L_{\mathrm{A}}-H}\left(1-\rho_{\mathrm{B}}\right)^{H}\left(\rho_{\mathrm{B}}\right)^{L_{\mathrm{A}}-H}\right]$$
$$\mathrm{x}\sum_{G=0}^{H-1}\left[C_{L_{\mathrm{A}}}^{G}\left(1-\rho_{\mathrm{E}}\right)^{G}\left(\rho_{\mathrm{E}}\right)^{L_{\mathrm{A}}-G}\right]. \quad (21)$$

3.3 Xác suất chặn

Tiếp theo, từ (9), ta có xác suất chặn (IP) có thể được viết như sau:

$$\mathrm{IP} = \sum_{L_\mathrm{A}=H}^{+\infty} \Pr\left(L_\mathrm{E}=H, L_\mathrm{B}=H \,|\, L_\mathrm{A}\right) \times \sum_{L_\mathrm{A}=H}^{+\infty} \Pr\left(L_\mathrm{E}=H, L_\mathrm{B}<H \,|\, L_\mathrm{A}\right)$$

$$= \sum_{L_\mathrm{A}=H}^{+\infty} \Pr\left(L_\mathrm{E}=H \,|\, L_\mathrm{A}\right) \times \left[\Pr\left(L_\mathrm{B}=H \,|\, L_\mathrm{A}\right) + \sum_{G=0}^{H-1} \Pr\left(L_\mathrm{B}=G \,|\, L_\mathrm{A}\right)\right], \quad (22)$$

trong đó $\Pr\left(L_\mathrm{E}=H \,|\, L_\mathrm{A}\right)$ là xác suất rằng E có thể thu thành công H gói mã hóa vào thời điểm này. Tương tự như (19), ta có thể được biểu diễn như sau:

$$\Pr\left(L_\mathrm{E}=H \,|\, L_\mathrm{A}\right) = C_{L_\mathrm{A}-1}^{L_\mathrm{A}-H} \left(1-\rho_\mathrm{E}\right)^H \left(\rho_\mathrm{E}\right)^{L_\mathrm{A}-H}, \quad (23)$$

Tiếp theo, xác suất $\Pr\left(L_\mathrm{B}=G \,|\, L_\mathrm{A}\right)$ trong (22) là:

$$\Pr\left(L_\mathrm{B}=G \,|\, L_\mathrm{A}\right) = C_{L_\mathrm{A}}^{G} \left(1-\rho_\mathrm{B}\right)^G \left(\rho_\mathrm{B}\right)^{L_\mathrm{A}-G}, \quad (24)$$

Thay thế (19), (23), và (24) vào (22), biểu thức chính xác dưới dạng đóng của IP có thể thu được như sau:

$$\mathrm{IP} = \sum_{L_\mathrm{A}=H}^{+\infty} \left[C_{L_\mathrm{A}-1}^{L_\mathrm{A}-H} \left(1-\rho_\mathrm{E}\right)^H \left(\rho_\mathrm{E}\right)^{L_\mathrm{A}-H} \right] \times \left[C_{L_\mathrm{A}-1}^{L_\mathrm{A}-H} \left(1-\rho_\mathrm{B}\right)^H \left(\rho_\mathrm{B}\right)^{L_\mathrm{A}-H} + \sum_{G=0}^{H-1} C_{L_\mathrm{A}}^{G} \left(1-\rho_\mathrm{B}\right)^G \left(\rho_\mathrm{B}\right)^{L_\mathrm{A}-G} \right] \quad (25)$$

3.4 Số lượng gói mã hóa trung bình

Biểu thức chính xác của số lượng gói mã hóa trung bình được phát bởi A được đưa ra chính xác như sau (xem phương trình (8) của (X. Wang, W. Chen, and Z. Cao, 2009): [31]):

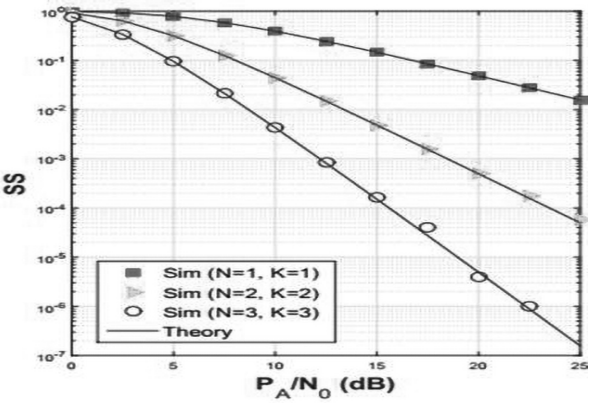
$$\mathrm{E}\{L_\mathrm{A}\} = \frac{H}{1-\rho_\mathrm{B}} = \frac{H}{1-\left(1-\exp\left(-\frac{\lambda N_0}{P_\mathrm{A}}\gamma_\mathrm{th}\right)\right)^{MN}} \quad (26)$$

4. Kết quả mô phỏng

Trong phần này, các mô phỏng Monte Carlo được trình bày để xác minh kết quả lý thuyết đề xuất. Để thực hiện các kết quả lý thuyết, trong tất cả các mô phỏng, chúng ta cố định tham số ngưỡng lỗi là $\gamma_\mathrm{th}=1$, số lượng gói mã Fountain cần thiết để khôi phục bộ dữ liệu gốc là 5 (H = 5), và chuỗi vô hạn được cắt bớt bởi 200, tức là (N_T = 200). Trong Hình 2, trình bày xác suất giải mã thành công và bảo mật (SS) như một hàm của tỷ số tín hiệu trên tạp (SNR) truyền P_A/N_0 (dB).

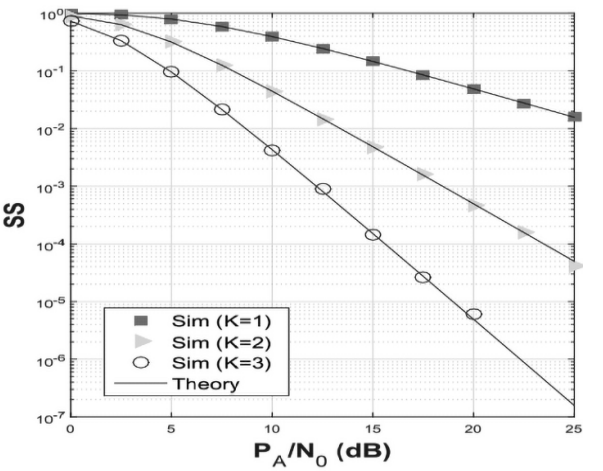
Trong mô phỏng này, cố định các tham số kênh như λ=0.5, Ω=1, và số lượng anten phát là 3 (M = 3). Trong hình này, có thể thấy rằng giá trị SS giảm khi giá trị P_A/N_0 (dB) tăng. Điều này là do khi tăng giá trị P_A/N_0 (dB), có nghĩa là tăng công suất truyền tại A, do đó khả năng chặn của E sẽ tăng lên.

Hình 2: Xác suất giải mã thành công và bảo mật (SS) như một hàm của SNR truyền P_A/N_0 (dB) khi M = 3, λ=0.5 và Ω=1.

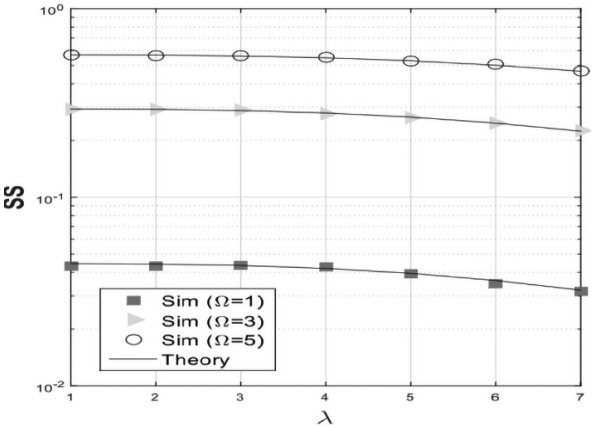


Ngược lại, SS tại B sẽ hội tụ về 1 ở công suất truyền thấp. Hơn nữa, khi công suất truyền tại A nhỏ hơn 0 dB, giá trị SS gần bằng 1, dữ liệu gốc có thể được giải mã và bảo mật thành công tại B.

Hình 3. SS dưới dạng hàm của P_A/N_0 trong (db) khi M = 2, N = 2, λ = 0.5 và Ω = 1.



Hình 4. SS dưới dạng hàm của λ khi P_A/N_0=10 (db), M = 2, N = 2 và K = 2.



Trong Hình 3, SS được hiển thị dưới dạng hàm (dB) với số lượng anten khác nhau tại E. Từ hình này, các tham số mô phỏng được cố định là $M = 2$, $N = 2$, λ = 0.5 và Ω = 1. Từ hình 4 thấy khi các anten thu tại E được trang bị với $K = 2$ và $K = 3$, giá trị của SS tệ hơn so với $K = 1$(Bảng 1). Do đó, để cải thiện hiệu suất bảo mật, cần giảm đáng kể công suất phát tại A để giảm chất lượng liên kết của kẻ nghe lén.

Bảng 1. Giá trị SS khi k=1,2,3

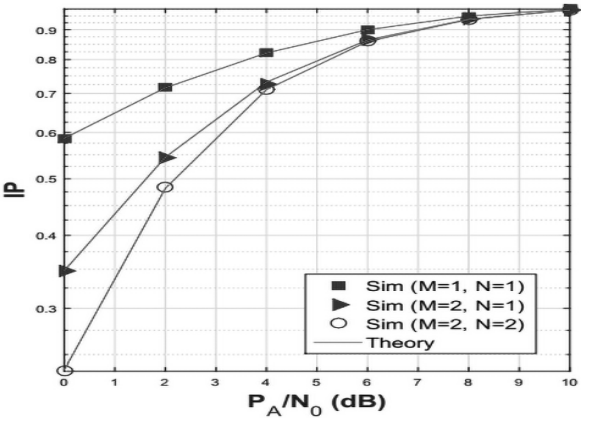
	M	N	λ	Ω	SS
K=1	2	2	0.5	1	$10^{-1.9}$
K=2	2	2	0.5	1	$10^{-4.3}$
K=2	2	2	0.5	1	$10^{-6.8}$

Trong Hình 4, SS được trình bày dưới dạng hàm của tham số kênh λ khi cố định các tham số mô phỏng như sau: P_A/N_0 = 10 (dB), $M = 2$; $N = 2$; và $K = 2$. Có thể thấy rằng hiệu suất bảo mật của các giao thức được đề xuất tăng đáng kể khi tăng Ω (bảng 2), điều này là do việc tăng Ω làm giảm chất lượng liên kết của kẻ nghe lén giữa A và E.

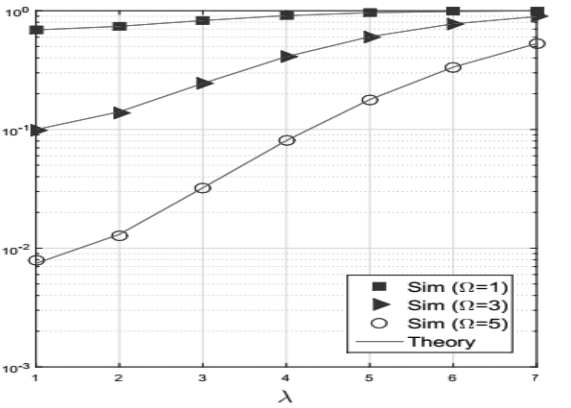
Bảng 2. Giá trị SS khi Ω =1,3,5

	M	N	λ	K	SS
Ω=1	2	2	1	2	$10^{-1.4}$
Ω=3	2	2	1	2	$10^{-0.5}$
Ω=5	2	2	1	2	$10^{-0.3}$

Hình 5. Xác suất bị chặn (IP) như một hàm của P_A/N_0(db) khi K = 2, λ = 0.5 và Ω = 1.



Hình 6. Xác suất bị chặn (IP) như một hàm của λ khi P_A/N_0= 5(db), M = 2, N = 2 và K=2



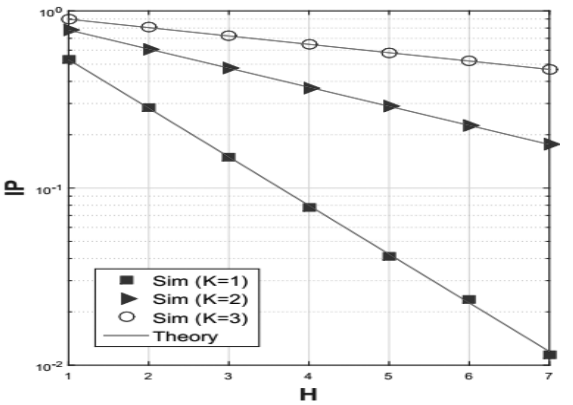
Trong Hình 5 minh họa xác suất chặn (IP) dưới dạng hàm của P_A/N_0 trong (dB) khi $K = 2$, λ = 0.5 và Ω = 1. Có thể quan sát rằng IP tăng đáng kể khi tăng giá trị của P_A/N_0 (bảng 3). Hơn nữa, trong ba trường hợp được khảo sát với việc thay đổi số lượng anten tại bộ phát và bộ thu qua kênh hợp pháp, tức là ($M = 2$, $N = 1$); ($M = 1$, $N = 1$) và ($M = 2$; $N = 2$); giá trị của IP là thấp nhất trong trường hợp ($M = 2$, $N = 2$). Điều này cho thấy lợi thế của các giao thức MIMO TAS/SC trong hệ thống bảo mật được đề xuất.

Bảng 3. Giá trị IP khi P_A/N_0 thay đổi

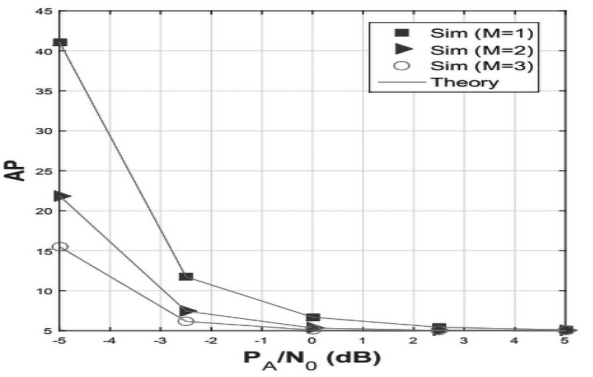
P_A/N_0	M	N	λ	Ω	IP
0	1	1	0.5	1	0.00
2	1	1	0.5	1	0.70
4	1	1	0.5	1	0.80
6	1	1	0.5	1	0.90
8	1	1	0.5	1	0.95
10	1	1	0.5	1	1.0

Trong Hình 6 tập trung vào IP như một hàm của λ với P_A/N_0 (dB) ($M = 2$, $N = 2$) và $K = 2$. Có thể thấy từ hình này, IP tăng khi tăng giá trị λ, điều này làm giảm chất lượng của các liên kết dữ liệu giữa A và B. Do đó, A cần gửi nhiều gói tin mã hóa hơn đến B với mục đích B có thể thu đủ H gói tin mã hóa để giải mã thông tin gốc, điều này cũng làm tăng khả năng chặn của kẻ nghe lén. Ngoài ra, IP giảm đáng kể khi tăng các tham số kênh của E, tức là trong mô phỏng này, giá trị của Ω từ 1 đến 5. Ngược lại, khi số lượng anten là 2 ($K = 2$), bộ thu bất hợp pháp thu được lợi ích đa dạng với phương pháp SC, điều này làm cho giá trị của xác suất chặn (IP) tăng nhanh khi các tham số kênh Ω giảm.

Hình 7. IP là hàm của H khi P_A/N_0= 5 (db), M = 3, N = 3, λ = 1 và Ω = 2



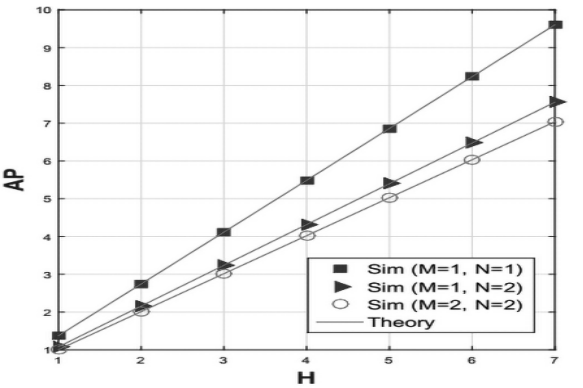
Hình 8. Số lượng trung bình các gói tin đã mã hóa (AP) là hàm của P_A/N_0 trong (db) khi N=3, K=3, λ = 1 và Ω = 0.5



Trong Hình 7, cho thấy IP như một hàm của H khi P_A/N_0 = 5 (dB), với các tham số cố định ($M = 3$, $N = 3$), λ = 1 và Ω = 2. Từ hình này cũng có thể thấy rằng IP trong Hình 5 giảm khi H tăng. Hơn nữa, khi tăng số lượng anten tại E từ 1 lên 3, giá trị IP tăng đáng kể.

Hình 8 minh họa số lượng gói tin mã hóa trung bình (AP) được phát bởi A như một hàm của P_A/N_0 (dB), với các tham số chính được cố định là ($N = 3$, $K = 3$), λ = 1 và Ω = 0.5. Trong hình này có thể quan sát rằng với công suất truyền thấp, cần nhiều gói tin mã hóa trung bình hơn để khôi phục dữ liệu gốc tại bộ thu khi tăng số lượng anten tại A từ 1 lên 3, dẫn đến giá trị AP giảm đáng kể. Tuy nhiên, khi tăng công suất phát tại A, AP giảm nhanh chóng và hội tụ về giá trị H.

Hình 9. AP là hàm của H khi P_A/N_0= 5 (db), K = 2, λ = 1 và Ω = 0.5



Hình 9 tập trung vào số lượng gói tin mã hóa trung bình (AP) như một hàm của số lượng gói tin mã hóa H khi P_A/N_0 = 5 (dB), $K = 2$, λ = 1 và Ω = 0.5. Có thể thấy, AP do A gửi tăng nhanh khi số lượng gói tin mã hóa H yêu cầu tại B tăng. Hơn nữa, khi thay đổi số lượng anten tại A và B, tức là ($M = 1$, $N = 1$), ($M = 1$, $N = 2$) và ($M = 2$, $N = 2$). Như được minh họa trong hình, AP trong trường hợp ($M = 2$, $N = 2$) là tốt nhất khi so sánh với các trường hợp còn lại, và giá trị AP bằng với giá trị H. Điều này cho thấy những lợi thế của các giao thức MIMO TAS/SC đề xuất.

5. Kết luận

Trong bài báo này đã đề xuất các giao thức MIMO TAS/SC sử dụng mã Fountain để nâng cao hiệu suất bảo mật của hệ thống. Đưa ra các biểu thức dạng đóng chính xác cho xác suất giải mã thành công và bảo mật (SS), xác suất bị chặn (IP), và số lượng gói tin mã hóa Fountain trung bình (AP) được gửi bởi A qua các kênh

suy hao Rayleigh. Các biểu thức lý thuyết đã được xác minh bằng các mô phỏng Monte Carlo. Kết quả cho thấy rằng các giao thức đề xuất vượt trội hơn so với các giao thức không sử dụng SC. Ngoài ra, để cải thiện hiệu suất bảo mật cần thiết kế số lượng anten phù hợp cho cả A và B. Hơn nữa, việc phân bổ công suất tại A chỉ cần phát đủ mức cần thiết để ngăn chặn E, người cố gắng nghe lén dữ liệu gốc từ A. Bên cạnh đó, cũng đã chỉ ra rằng việc tăng cường độ kênh qua kênh hợp pháp và giảm chất lượng liên kết của các kênh nghe lén có thể cải thiện hiệu suất bảo mật.

TÀI LIỆU KHAM KHẢO

A. Wyner (1975), "The Wire-tap channel,"*Bell Syst. Technol. J*., vol. 54, no. 8, pp. 1355-1387.

B. Schneier (1998), "Cryptographic design vulnerabilities," *Comput*., vol. 31, no. 9, pp. 29-31.

C. E. Shannon (1949), "Communication theory of secrecy systems," *Bell Syst. Technol. J*., vol. 28, pp. 656-715.

D. T. Hung, T. T. Duy, D. Q. Trinh, and V. N. Q. Bao (2018), "Secrecy performance evaluation of TAS protocol exploiting fountain codes and cooperative jamming under impact of hardware impairments, "in *Proc, The 2nd International Conference on Recent Advances in Signal Processing, Telecommunications and Computing*, pp. 164-169, Ho Chi Minh city, Vietnam.

H. Guo, Z. Yang, L. Zhang, J. Zhu, and Y. Zou (2017), "Power constrained secrecy rate maximization for joint relay and jammer selection assisted wireless networks," *IEEE Trans. Commun*., vol. 65, no. 5, pp. 2180-2193.

H. Alves, R. D. Souza, M. Debbah, and M. Bennis (2012), "Performance of transmit antenna selection physical layer se curity schemes," *IEEE Signal Process. Lett*., vol. 19, no. 6, pp. 372-375.

H. Niu, M. Iwai, K. Sezaki, L. Sun, and Q. Du (2014), "Ex ploiting fountain codes for secure wireless delivery," *IEEE Commun. Lett*., vol. 18, no. 5, pp. 777-780.

J.-M. Kang, J. Yang, J. Ha, and Il-Min Kim (2017), "Joint design of optimal precoding and cooperative jamming for multiuser secure broadcast systems," *IEEE Trans. Veh. Tech nol*., vol. 66, no. 11, pp. 10551-10556.

K. Cao, Y. Cai, Y. Wu, and W. Yang (2017), "Cooperative jamming for secure communication with nite alphabet in puts," *IEEE Commun. Lett*., vol. 21, no. 9, pp. 2025-2028.

L. Sun, P. Ren, Q. Du, and Y. Wang (2016), "Fountain-coding aided strategy for secure cooperative transmission in indus trial wireless sensor networks," *IEEE Transactions on Indus trial Informatics*, vol. 12, no. 1, pp. 291-300.

M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin (2008), "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515-2534.

M. Luby (2002), "LT codes," *in Proc. of the 43rd Annual IEEE Symp. On Foundations of Computer Science,* Vancouver, Canada, pp. 271-282.

N. Yang, H. Suraweera, I. Collings, and C. Yuen (2013), "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 254 259.

N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings (2013), "Transmit antenna selection for security enhance ment in MIMO wiretap channels," *IEEE Trans. Commun*., vol. 61, no. 1, pp. 144-154.

N.-E. Wu and H.-J. Li (2013), "Effect of feedback delay on se cure cooperative networks with joint relay and jammer se lection," *IEEE Commun. Lett*., vol. 2, no. 4, pp. 415-418.

P. L. Yeoh, M. Elkashlan, and I. B. Collings (2011) "Exact and asymptotic SER of distributed TAS/

MRC in MIMO relay networks," *IEEE Trans. Wireless Commun*., vol. 10, no. 3, pp. 751-756.

Q. Du, Y. Xu, W. Li, and H. Song (2018), "Security enhancement for multicast over internet of things by dynamically constructed fountain codes," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 8404219, pp. 1-11.

S. K. Leung-Yan-Cheong, and M. E. Hellman (1978), "The gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451-456.

T. T. Duy, T. Q. Duong, T. L. Thanh, and V. N. Q. Bao (2015), "Secrecy performance analysis with relay selection methods under impact of co-channel interference," *IET Commun*., vol. 9, no. 11, pp. 1427-1435.

T. T. Duy and P. N. Son (2015), "Secrecy performances of multicast underlay cognitive protocols with partial relay selec tion and without eaves dropper information," *KSII Trans. Internet and Inform. Syst*., vol. 9, no. 11, pp. 4623-4643.

T. Liu and S. Shamai (2009), "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547-2553.

T. F. Wong, M. Bloch, and J. M. Shea (2009), "Secret sharing over fast fading MIMO wiretap channels," *EURASIP J. Wireless Commun. Netw*., vol. 2009, pp. 506973/1-17.

T. T. Duy and H. Y. Kong (2014), "Secondaryspectrum access in cognitive radio networks using rateless codes over rayleigh fading channels," *Wireless Pers. Commun*., vol. 77, no. 2, pp. 963-978.

W. Li, Q. Du, L. Sun, P. Ren, and Y. Wang (2016), "Security enhanced via dynamic fountain code design for wireless delivery," *in Proc. of IEEE Wireless Communications and Networking Conference (WCNC2016)*, Doha, Quatar, pp. 1-6.

X. Wang, W. Chen, and Z. Cao (2009), "A rateless coding based multi-relay cooperative transmission scheme for cognitive radio networks," *in IEEE GLOBECOM*, Honolulu, HI, pp. 1-6