NGHIÊN CỨU HIỆU NĂNG BẢO MẬT MẠNG VÔ TUYẾN NHẬN THỨC DẠNG NỀN CỘNG TÁC SỬ DỤNG MÃ FOUNTAIN

Nguyễn Văn Hiền*, Trần Trung Duy*, Trần Đình Thuần*
*Khoa Viễn Thông 2, Học Viện Công Nghệ Bưu Chính Viễn Thông cơ sở tại TP. Hồ Chí Minh

Tóm tắt: Trong bài báo này, chúng tôi nghiên cứu phương pháp bảo mật lớp vật lý (Physical-Layer Security) cho mạng vô tuyến nhận thức dạng nền (Underlay Cognitive Radio Network) sử dụng mã Fountain. Trong mô hình nghiên cứu, nguồn thứ cấp và nút chuyển tiếp thứ cấp hiệu chỉnh công suất phát để đảm bảo chất lượng dịch vụ của mạng sơ cấp không bị ảnh hưởng. Sử dụng mã Fountain, nút nguồn liên tục gửi các gói mã hoá đến nút đích, và nút đích có thể khôi phục lại dữ liệu của nguồn nếu nút này nhận đủ một lượng tối thiểu các gói mã hoá. Hơn nữa, nếu nút chuyển tiếp có thể tích luỹ đủ số lượng gói mã hoá để giải mã dữ liệu nguồn trước nút đích, nút chuyển tiếp sẽ thay nút nguồn gửi các gói mã hoá đến nút đích. Trong mạng thứ cấp, một nút nghe lén xuất hiện, và cố gắng đạt được dữ liệu của nút nguồn. Nếu nút nghe lén có thể nhận đủ số lượng gói mã hoá, nút này cũng có thể giải mã thành công dữ liệu nguồn, và trong trường hợp này, việc truyền dữ liệu xem như bị mất bảo mật. Do đó, hiệu năng của mô hình nghiên cứu được đánh giá thông qua hai thông số quan trọng: i) xác suất dừng (OP: Outage Probability) là xác suất mà nút đích không thể nhận đủ số lượng gói mã hoá để giải mã thành công dữ liệu nguồn; ii) xác suất mất bảo mật (IP: Insecure Probability) là xác suất mà nút nghe lén nhận đủ số lượng gói mã hoá để giải mã dữ liệu nguồn. Chúng tôi đưa ra các công thức đánh giá chính xác hiệu năng OP và IP của mạng thứ cấp trên kênh truyền fading Rayleigh, dưới sự ảnh hưởng của giao thoa đồng kênh đến từ mạng sơ cấp. Các công thức toán học đều được kiểm chứng sự chính xác thông qua mô phỏng Monte Carlo. Các kết quả cho thấy có sự đánh đổi giữa bảo mật và độ tin cậy trong việc truyền dữ liệu. Hơn nữa, mô hình nghiên cứu có thể đạt được các hiệu năng tốt hơn khi so sánh với mô hình truyền trực tiếp giữa nguồn thứ cấp và đích thứ cấp.

Từ khóa: Mã Fountain, vô tuyến nhận thức dạng nền, bảo mật lớp vật lý, xác suất dừng, xác suất mất bảo mật, truyền thông cộng tác.

I. GIỚI THIỆU

Gần đây, bảo mật lớp vật lý (Physical-layer security) [1]-[3] đang nhận được sự quan tâm đặc biệt của các nhà nghiên cứu trong và ngoài nước. Trong phương pháp bảo mật tiềm năng này, các yếu tố như kênh truyền, khoảng cách và nhiễu được sử dụng để bảo vệ sự truyền-nhận thông tin giữa các thiết bị thu-phát, trước sự nghe lén của các thiết bị thu không hợp pháp. Trong bảo mật lớp vật lý, các nhà nghiên cứu định nghĩa thông số dung lượng bảo mật (secrecy capacity), bằng hiệu giữa dung lượng của kênh dữ liệu và dung lượng của kênh nghe lén. Hơn nữa, dung lượng bảo mật là một đại lượng không âm. Do đó, để nâng cao dung lượng bảo mật hay nâng cao hiệu năng bảo mật, hệ thống cần tăng cường dung lượng của kênh dữ liệu và/hoặc giảm dung lượng của kênh nghe lén. Trong các công trình [4]-[6], các mô hình thu-phát phân tập MIMO (Multiple Input Multiple Output) được đề xuất để nâng cao chất lượng kênh dữ liệu, và do đó cũng nâng cao dung lượng bảo mật. Trong trường hợp các thiết bị không thể trang bị nhiều ăntен, chuyển tiếp cộng tác [7] thường được áp dụng, trong đó các nút đơn ăntен sẽ chia sẽ ăntен của mình để tạo thành hệ thống MIMO ảo. Trong các tài liệu [8]-[9], các tác giả đề xuất những mô hình chuyển tiếp cộng tác hiệu quả nhằm nâng cao hiệu năng bảo mật của mạng. Các công trình [10]-[11] kết hợp giữa chuyển tiếp và chọn lựa nút chuyển tiếp để nâng cao hơn nữa chất lượng của kênh dữ liệu. Trong bảo mật lớp vật lý, tạo nhiễu lên các thiết bị nghe lén cũng là một phương pháp hiệu quả để bảo mật thông tin. Trong kỹ thuật này, nút gây nhiễu (jammer) sẽ phát nhiễu lên các thiết bị nghe lén, đồng thời phối hợp với các thiết bị thu hợp pháp trong mạng để khử nhiễu gây ra [12]-[13]. Mặc dù các mô hình sử dụng tạo nhiễu đạt được hiệu năng bảo mật cao hơn khi so sánh với các mô hình không sử dụng tạo nhiễu, tuy nhiên việc triển khai kỹ thuật này rất phức tạp vì yêu cầu sự đồng bộ cao giữa nút tạo nhiễu, nút phát và nút thu. Khác với các công trình [4]-[13], các tác giả trong [14]-[15] đánh giá hiệu năng của các mô hình bảo mật lớp vật lý thông qua xác suất dừng (OP) tại nút thu hợp pháp và xác suất chặn (Intercept Probability) tại nút nghe lén. Các công trình [14] và [15] cũng phân tích sự đánh đổi giữa bảo mật thông tin và độ tin cậy của việc truyền thông tin thông qua sự tương quan của hai thông số hiệu năng OP và IP.

Vô tuyến nhận thức (CR: Cognitive Radio) ra đời nhằm giải quyết bài toán khan hiếm phổ tần, và cũng là giải pháp sử dụng phổ tần hiệu quả hơn [16]. Trong vô tuyến nhận thức, người dùng sơ cấp (Primary User) sẽ được cấp phép sử dụng phổ tần bất cứ lúc nào, trong khi người dùng thứ cấp (Secondary User) chỉ được sử dụng phổ tần khi chất lượng dịch vụ của mạng sơ cấp không bị ảnh hưởng. Thông thường, người dùng thứ cấp phải thăm dò sự xuất hiện của người dùng sơ cấp để sử dụng những băng tần không đang bị chiếm giữ. Tuy nhiên, một khi

Tác giả liên hệ: Trần Trung Duy
email: trantrungduy@ptithcm.edu.vn
Đến tòa soạn: 11/2020, chỉnh sửa: 12/2020, chấp nhận đăng: 12/2020.

người dùng sơ cấp trở lại sử dụng băng tần, người dùng thứ cấp phải lập tức chuyển sang sử dụng băng tần trống khác. Do đó, nhược điểm phương pháp thăm dò người dùng sơ cấp là phức tạp, đồng bộ cao, khả năng thăm dò chính xác, sự chuyển đổi kênh truyền nhanh chóng và không đảm bảo tính liên tục cho mạng thứ cấp. Các tác giả trong công bố [17] đề xuất mô hình vô tuyến nhận thức dạng nền (Underlay CR), trong đó người dùng thứ cấp được phép sử dụng cùng băng tần với người dùng sơ cấp. Tuy nhiên, người dùng thứ cấp phải hiệu chỉnh công suất phát để đảm bảo chất lượng dịch vụ của mạng sơ cấp không bị ảnh hưởng. Trong các công trình [17]-[18], công suất phát của thiết bị phát thứ cấp phải được hiệu chỉnh theo thông tin trạng thái kênh truyền (CSI: Channel State Information) tức thời giữa thiết bị này với người dùng sơ cấp sao cho giao thoa gây lên người dùng sơ cấp không được vượt qua một ngưỡng quy định trước. Tuy nhiên, việc ước lượng chính xác CSI tức thời khó đạt được trong thực tế vì cần sự phối hợp giữa hai mạng sơ cấp và thứ cấp, cần nhiều thời gian để ước lượng, cũng như cần đáp ứng nhanh chóng với sự thay đổi của kênh fading [19]. Trong tài liệu [20], các tác giả giới thiệu phương pháp hiệu chỉnh công suất phát đơn giản hơn cho các thiết bị phát thứ cấp, đó là hiệu chỉnh theo giá trị trung bình của độ lợi kênh đến người dùng sơ cấp. Cụ thể, công suất phát của nút phát thứ cấp sẽ được tính toán sao cho xác suất dừng tại người dùng sơ cấp luôn nhỏ hơn một ngưỡng xác định trước.

Mã Rateless hay mã Fountain [21]-[22] đang được nghiên cứu trong thời gian gần đây bởi sự đơn giản trong thiết kế và khả năng thích ứng với các điều kiện kênh truyền mà không cần biết CSI tại thiết bị phát. Trong mã Fountain, dữ liệu gốc của nguồn sẽ được chia thành các gói nhỏ, và nguồn sẽ tạo ra các gói mã hoá bằng cách XOR một vài các gói nhỏ này. Sau đó, nguồn sẽ liên tục gửi các gói mã hoá đến đích, cho đến khi đích nhận đủ một số lượng gói mã hoá tối thiểu để khôi phục lại dữ liệu nguồn. Tuy nhiên, bảo mật cũng là một vấn đề quan trọng trong việc sử dụng mã Fountain bởi vì các thiết bị nghe lén có thể nhận được các gói mã hoá và tiến hành giải mã để đạt được dữ liệu của nguồn. Trong các công trình [23]-[26], các tác giả đề xuất các mô hình bảo mật lớp vật lý cho các hệ thống truyền thông vô tuyến sử dụng mã Fountain. Như đã được đề cập trong các công trình [23]-[24], dữ liệu nguồn có thể được bảo mật nếu nút đích có thể đạt được đủ số gói mã hoá trước nút nghe lén. Cụ thể, sau khi nhận đủ số gói mã hoá, nút đích lập tức gửi thông báo đến nút nguồn để yêu cầu nút nguồn dừng việc gửi các gói mã hoá. Bởi vì nút đích đã nhận đủ số gói mã hoá nên nút này có thể giải mã thành công dữ liệu gốc, trong khi nút nghe lén không thể khôi phục được do chưa nhận đủ số gói yêu cầu. Tài liệu [25] đưa ra mô hình chuyển tiếp hợp tác sử dụng một nút tạo nhiễu để làm giảm chất lượng tín hiệu đạt được tại nút nghe lén. Tuy nhiên, như đã đề cập ở trên, việc triển khai kỹ thuật tạo nhiễu rất phức tạp bởi cần một sự đồng bộ cao giữa tất cả các nút.

Trong bài báo này, chúng tôi đề xuất mô hình bảo mật lớp vật lý sử dụng mã Fountain cho mạng chuyển tiếp cộng tác trong môi trường vô tuyến nhận thức dạng nền. Sau khi hiệu chỉnh công suất phát nhằm đảm bảo xác suất dừng của mạng sơ cấp luôn thấp hơn hoặc bằng một ngưỡng xác định trước, nút nguồn thứ cấp gửi các gói mã hoá đến nút đích thứ cấp. Cùng lúc đó, nút chuyển tiếp thứ cấp cũng sẽ nhận các gói mã hoá từ nút nguồn. Ngay khi nút đích nhận đủ số lượng gói mã hoá, nút này sẽ yêu cầu nút nguồn (hoặc nút chuyển tiếp) dừng việc truyền, rồi tiến hành khôi phục dữ liệu gốc. Trong trường hợp, nút chuyển tiếp có thể nhận đủ số lượng gói trước nút đích, nút chuyển tiếp sẽ thay nút nguồn gửi các gói mã hoá đến nút đích. Cũng xuất hiện trong mạng thứ cấp, nút nghe lén cũng cố gắng nhận các gói mã hoá để đạt được dữ liệu của nguồn. Với sự ràng buộc thời gian trễ tối đa, tổng số lần truyền các gói mã hoá tại nguồn và nút chuyển tiếp không được vượt quá một giá trị cho trước. Vì vậy, sau số lần truyền tối đa này, nếu nút đích không thể nhận đủ số gói mã hoá thì xem như nút đích bị dừng (không thể giải mã thành công dữ liệu nguồn). Hơn nữa, trong quá trình truyền dữ liệu, nếu nút nghe lén có thể nhận đủ số lượng gói mã hoá, thì dữ liệu nguồn xem như bị mất bảo mật. Do đó, hai thông số hiệu năng xác suất dừng (OP) và xác suất mất bảo mật (IP) sẽ được đánh giá đồng thời trong bài báo này.

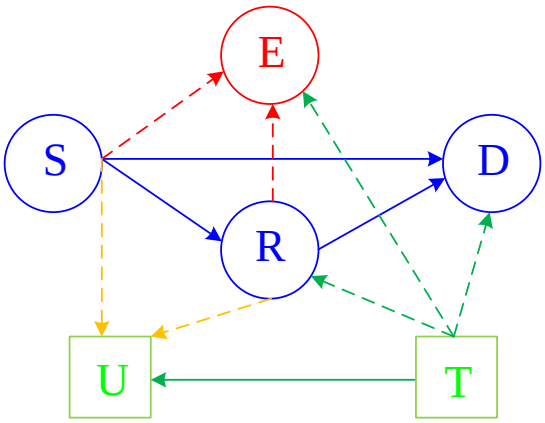
Sau đây, chúng tôi trình bày những công trình chính liên quan đến chủ đề của bài báo. Hơn nữa, những điểm mới và điểm khác biệt giữa bài báo này và những công bố trước đây sẽ được phân tích kỹ. Đầu tiên, các công trình liên quan [23]-[24] chỉ nghiên cứu các mô hình truyền trực tiếp giữa nguồn và đích, và không nghiên cứu mô hình chuyển tiếp. Tương tự như vậy, các công bố [26]-[28] cũng nghiên cứu hệ thống truyền thông trực tiếp giữa nguồn và đích, sử dụng các kỹ thuật phân tập thu-phát MIMO. Các tác giả trong công trình [25] đã đề xuất mô hình chuyển tiếp cộng tác, trong đó nút chuyển tiếp sẽ giúp đỡ nút nguồn chuyển tiếp từng gói mã hoá đến nút đích. Khác với công trình [25], nút chuyển tiếp trong bài báo này đóng vai trò chuyển tiếp dữ liệu của nguồn khi nút này tích luỹ đủ gói mã hoá trước nút đích. Hơn thế nữa, mô hình trong công trình [25] cũng không nghiên cứu về mạng vô tuyến nhận thức. Tài liệu [29] nghiên cứu mô hình bảo mật sử dụng mã Fountain trong mạng vô tuyến nhận thức dạng nền dưới sự tác động của khiếm khuyết phần cứng và nhiễu từ mạng sơ cấp. Khác với [29], bài báo này xét đến mạng chuyển tiếp, trong khi công trình [29] nghiên cứu mô hình truyền trực tiếp giữa nguồn và đích.

Tiếp đến, những đóng góp và những kết quả đạt được trong bài báo sẽ được tóm tắt. Đóng góp đầu tiên là việc đề xuất mô hình chuyển tiếp cộng tác nhằm nâng cao độ tin cậy của sự truyền dữ liệu trong mạng vô tuyến nhận thức dạng nền. Đóng góp thứ hai của bài báo là đưa ra biểu thức tính chính xác xác suất dừng (OP) và xác suất mất bảo mật (IP) của mạng thứ cấp trên kênh truyền fading Rayleigh. Hơn nữa, các công thức toán học đều được kiểm chứng sự chính xác thông qua mô phỏng Monte Carlo. Kế tiếp, các kết quả đạt được cho thấy mô

hình đề xuất đạt được hiệu năng xác suất dừng tốt hơn hẳn mô hình truyền trực tiếp giữa nguồn và đích. Đối với hiệu năng IP, mô hình đề xuất có thể đạt được giá trị IP thấp hơn (hoặc lớn hơn không đang kể) khi so sánh với mô hình truyền trực tiếp. Cuối cùng, sự ảnh hưởng của các tham số hệ thống (như tổng số lần truyền gói mã hoá tối đa và vị trí của nút chuyển tiếp) cũng sẽ được nghiên cứu kỹ trong bài báo này.

Phần còn lại của bài báo được tổ chức như sau: Phần II trình bày nguyên lý hoạt động của mô hình đề xuất. Trong phần III, bài báo đánh giá các hiệu năng OP và IP của mô hình đề xuất bằng các công cụ toán học. Phần IV đưa ra các kết quả phân tích lý thuyết được kiểm chứng bằng mô phỏng. Cuối cùng, các kết luận và hướng phát triển được thảo luận trong phần V.

II. MÔ HÌNH HỆ THỐNG



Hình 1. Mô hình nghiên cứu.

Mô hình đề xuất được mô tả trong Hình 1, trong đó hai mạng sơ cấp và thứ cấp sử dụng cùng băng tần, và do đó, gây giao thoa đồng kênh lên nhau. Trong mạng sơ cấp, thiết bị phát (T) đang truyền dữ liệu đến thiết bị thu (U). Trong mạng thứ cấp, nút nguồn (S) đang gửi các gói mã hoá đến nút chuyển tiếp (R) và nút đích (D), trong khi nút nghe lén (E) đang nghe lén dữ liệu được gửi đi. Giả sử rằng tất cả các nút đều chỉ có 01 ăntен, và hoạt động ở chế độ bán song công (half duplex).

Nút nguồn S chia dữ liệu gốc thành các gói nhỏ có kích thước bằng nhau. Sau đó, một số lượng các gói nhỏ này sẽ được chọn một cách ngẫu nhiên, và XOR lại với nhau để tạo thành những gói mã hóa. Trong các gói mã hoá, các thành phần mào đầu (Overhead) và các bit kiểm tra có thể được thêm vào để phục vụ cho việc giải mã tại các thiết bị thu như R và D. Các gói mã hoá sẽ liên tục được gửi đến R và D, và cũng bị nghe lén bởi E. Giả sử, sự truyền dữ liệu giữa nguồn và đích bị giới hạn về thời gian trễ, cụ thể số lần truyền các gói mã hoá tối đa không được vượt qua $N_{\max}$. Điều này có nghĩa là sau $N_{\max}$ lần truyền các gói mã hoá thì S và R không được gửi thêm lần nào nữa vì đã quá thời gian trễ quy định. Để giải mã thành công dữ liệu của nguồn, các nút R, D và E phải tích luỹ ít nhất H gói mã hoá, $H \le N_{\max}$. Hơn nữa, ngay khi đích D nhận đủ H gói mã hoá, nút này sẽ gửi thông điệp ACK đến nguồn S để thông báo, và nguồn S sẽ dừng việc truyền các gói mã hoá. Trong trường hợp, nút R nhận đủ H gói mã hoá trước nút đích, R cũng gửi thông báo ACK đến S. Kế tiếp, R sẽ thay S truyền các gói mã hoá đến D. Việc nút chuyển tiếp thay thế nút nguồn có những điểm lợi sau đây: thứ nhất, nút chuyển tiếp chia sẽ tải với nút nguồn; thứ hai, nút chuyển tiếp ở gần nút đích hơn nên việc truyền dữ liệu đến đích sẽ tốt hơn. Cũng vậy, nút đích tiếp tục tích luỹ các gói mã hoá cho đến khi nhận đủ số lượng, và cũng sẽ gửi ACK đến nút chuyển tiếp để thông báo. Trong trường hợp, đích D không thể nhận đủ H gói mã hoá sau $N_{\max}$ lần truyền thì D xem như bị dừng. Trong trường hợp nút nghe lén E có thể đạt được ít nhất H gói mã hoá trong suốt quá trình truyền dữ liệu thì xem như dữ liệu của nguồn bị mất bảo mật.

Giả sử kênh truyền giữa hai nút X và Y là kênh fading Rayleigh, với $(\mathrm{X},\mathrm{Y}) \in \{\mathrm{S},\mathrm{R},\mathrm{D},\mathrm{T},\mathrm{U}\}$. Ta cũng giả sử kênh truyền giữa hai nút này không thay đổi trong suốt quá trình truyền một gói mã hoá. Ta ký hiệu γ_{XY} là độ lợi kênh giữa X và Y, và γ_{XY} sẽ là một biến ngẫu nhiên có phân phối mũ [7]-[10] với hàm mật độ xác suất và hàm phân bố tích luỹ lần lượt là

$$\begin{aligned} f_{\gamma_{\mathrm{XY}}}(x) &= \lambda_{\mathrm{XY}} \exp(-\lambda_{\mathrm{XY}} x), \\ F_{\gamma_{\mathrm{XY}}}(x) &= 1 - \exp(-\lambda_{\mathrm{XY}} x), \end{aligned} \tag{1}$$

ở đây, $f_U(.)$ và $F_U(.)$ lần lượt là hàm mật độ xác suất và hàm phân bố tích luỹ của biến ngẫu nhiên U, λ_{XY} là tham số đặc trưng của γ_{XY}, và được biểu diễn bằng công thức sau (xem [7]-[9]):

$$\lambda_{\mathrm{XY}} = (d_{\mathrm{XY}})^{\beta}, \tag{2}$$

ở đây, d_{XY} là khoảng cách giữa X và Y, và β là hệ số suy hao đường truyền có giá trị từ 2 đến 8.

Xét sự truyền dữ liệu giữa hai nút sơ cấp T và U; nếu mạng thứ cấp cũng đang sử dụng phổ tần thì tỷ số tín hiệu trên giao thoa và nhiễu (SINR: Signal-to-Interference-plus-Noise Ratio) đạt được tại U được biểu diễn bằng công thức sau:

$$\Phi_{\mathrm{TU}} = \frac{P_{\mathrm{T}} \gamma_{\mathrm{TU}}}{P_{\mathrm{A}} \gamma_{\mathrm{AU}} + \sigma_0^2}. \tag{3}$$

Trong công thức (3), P_{T} là công suất phát của nút phát sơ cấp T, P_{A} là công suất phát của nút phát thứ cấp A ($\mathrm{A} \in \{\mathrm{S},\mathrm{R}\}$), và σ_0^2 là phương sai của nhiễu Gauss trắng cộng tính tại nút thu U (giả sử nhiễu Gauss trắng cộng tính tại các thiết bị thu đều có giá trị trung bình bằng 0 và phương sai bằng σ_0^2). Cũng trong (3), $P_{\mathrm{A}} \gamma_{\mathrm{AU}}$ là giao thoa đồng kênh do nút A gây lên nút U.

Xác suất dừng của mạng sơ cấp được định nghĩa là xác suất mà tỷ số SINR đạt được tại nút U nhỏ hơn một ngưỡng ψ_{P} cho trước. Từ công thức (3), xác suất dừng được viết như sau:

$$\begin{aligned} \mathrm{OP} &= \Pr(\Phi_{\mathrm{TU}} < \psi_{\mathrm{P}}) = \Pr\left(\frac{P_{\mathrm{T}} \gamma_{\mathrm{TU}}}{P_{\mathrm{A}} \gamma_{\mathrm{AU}} + \sigma_0^2} < \psi_{\mathrm{P}}\right) \\ &= \int_0^{+\infty} F_{\gamma_{\mathrm{TU}}}\left(\frac{P_{\mathrm{A}} \psi_{\mathrm{P}}}{P_{\mathrm{T}}} x + \frac{\psi_{\mathrm{P}} \sigma_0^2}{P_{\mathrm{T}}}\right) f_{\gamma_{\mathrm{AU}}}(x)\, dx. \end{aligned} \tag{4}$$

Kết hợp với công thức (1), xác suất dừng trong công thức (4) được tính chính xác như sau:

$$\mathrm{OP}=1-\frac{\lambda_{\mathrm{AU}}P_{\mathrm{T}}}{\lambda_{\mathrm{AU}}P_{\mathrm{T}}+\lambda_{\mathrm{TU}}\psi_{\mathrm{P}}P_{\mathrm{A}}}\exp\left(-\frac{\lambda_{\mathrm{TU}}\sigma_0^2\psi_{\mathrm{P}}}{P_{\mathrm{T}}}\right). \quad (5)$$

Tiếp đến, nút phát thứ cấp A phải hiệu chỉnh công suất phát $\left(P_{\mathrm{A}}\right)$ để chất lượng dịch vụ của mạng sơ cấp không bị ảnh hưởng, cụ thể: $\mathrm{OP}\le\varepsilon_{\mathrm{OP}}$ [20], với $\varepsilon_{\mathrm{OP}}$ là giá trị được quy định bởi mạng sơ cấp. Bằng cách giải phương trình $\mathrm{OP}=\varepsilon_{\mathrm{OP}}$, ta đạt được nghiệm sau đây:

$$P_{\mathrm{A}}=\left(\frac{1}{1-\varepsilon_{\mathrm{OP}}}\exp\left(-\frac{\lambda_{\mathrm{TU}}\sigma_0^2\psi_{\mathrm{P}}}{P_{\mathrm{T}}}\right)-1\right)\frac{\lambda_{\mathrm{AU}}}{\lambda_{\mathrm{TU}}\psi_{\mathrm{P}}}P_{\mathrm{T}}. \quad (6)$$

Bởi vì công suất phát là đại lượng không âm, nên từ công thức (6), công suất phát lớn nhất của S và R lần lượt được đưa ra bằng các biểu thức sau:

$$\begin{cases}P_{\mathrm{S}}=\left[\left(\frac{1}{1-\varepsilon_{\mathrm{OP}}}\exp\left(-\frac{\lambda_{\mathrm{TU}}\sigma_0^2\psi_{\mathrm{P}}}{P_{\mathrm{T}}}\right)-1\right)\frac{\lambda_{\mathrm{SU}}}{\lambda_{\mathrm{TU}}\psi_{\mathrm{P}}}P_{\mathrm{T}}\right]^+\\ P_{\mathrm{R}}=\left[\left(\frac{1}{1-\varepsilon_{\mathrm{OP}}}\exp\left(-\frac{\lambda_{\mathrm{TU}}\sigma_0^2\psi_{\mathrm{P}}}{P_{\mathrm{T}}}\right)-1\right)\frac{\lambda_{\mathrm{RU}}}{\lambda_{\mathrm{TU}}\psi_{\mathrm{P}}}P_{\mathrm{T}}\right]^+\end{cases} \quad (7)$$

Trong công thức (7), ta sử dụng hàm $\left[x\right]^+=\max\left(x,0\right)$. Ta cũng lưu ý rằng việc hiệu chỉnh công suất phát của nút S và nút R được thực hiện trước khi sự truyền dữ liệu bắt đầu.

Xét sự truyền của một gói mã hoá từ nút phát thứ cấp A $\left(\mathrm{A}\in\left\{\mathrm{S},\mathrm{R}\right\}\right)$; tỷ số SINR đạt được nút thu thứ cấp B, $\left(\mathrm{B}\in\left\{\mathrm{R},\mathrm{D},\mathrm{E}\right\}\right)$, được tính như sau:

$$\Phi_{\mathrm{AB}}=\frac{P_{\mathrm{A}}\gamma_{\mathrm{AB}}}{P_{\mathrm{T}}\gamma_{\mathrm{TB}}+\sigma_0^2}. \quad (8)$$

Trong công thức (8), $P_{\mathrm{T}}\gamma_{\mathrm{TB}}$ là thành phần giao thoa đồng kênh do nút sơ cấp T gây lên nút thu thứ cấp B. Nếu tỷ số SINR Φ_{AB} nhỏ hơn một ngưỡng xác định trước ψ_{S}, ta giả sử rằng nút thu thứ cấp B không thể giải mã thành công gói mã hoá nhận được từ A. Ngược lại, nếu $\Phi_{\mathrm{AB}}\ge\psi_{\mathrm{S}}$, thì gói mã hoá được giải mã thành công. Tương tự các công thức (4) và (5), ta tính được xác suất mà một gói mã hoá gửi đi từ A và không thể giải mã thành công bởi B là:

$$\begin{aligned}\rho_{\mathrm{AB}}&=\int_0^{+\infty}F_{\gamma_{\mathrm{AB}}}\left(\frac{P_{\mathrm{T}}\psi_{\mathrm{S}}}{P_{\mathrm{A}}}x+\frac{\psi_{\mathrm{S}}\sigma_0^2}{P_{\mathrm{A}}}\right)f_{\gamma_{\mathrm{TB}}}\left(x\right)dx\\&=1-\frac{\lambda_{\mathrm{TB}}P_{\mathrm{A}}}{\lambda_{\mathrm{TB}}P_{\mathrm{A}}+\lambda_{\mathrm{AB}}P_{\mathrm{T}}\psi_{\mathrm{S}}}\exp\left(-\frac{\lambda_{\mathrm{TU}}\psi_{\mathrm{S}}}{P_{\mathrm{A}}}\right).\end{aligned} \quad (9)$$

Và xác suất một gói mã hoá được gửi từ A và được giải mã thành công tại B sẽ là:

$$\overline{\rho_{\mathrm{AB}}}=1-\rho_{\mathrm{AB}}=\frac{\lambda_{\mathrm{TB}}P_{\mathrm{A}}}{\lambda_{\mathrm{TB}}P_{\mathrm{A}}+\lambda_{\mathrm{AB}}P_{\mathrm{T}}\psi_{\mathrm{S}}}\exp\left(-\frac{\lambda_{\mathrm{TU}}\psi_{\mathrm{S}}}{P_{\mathrm{A}}}\right). \quad (10)$$

III. PHÂN TÍCH HIỆU NĂNG HỆ THỐNG

Trong mục này, bài báo sẽ phân tích hiệu năng OP và IP của mô hình đề xuất (ký hiệu CT: Cooperative Transmission), và so sánh với mô hình truyền trực tiếp (ký hiệu DT: Direct Transmission). Ta ký hiệu n_{R}, n_{D} và n_{E} lần lượt là số gói mã hoá nhận được tại R, D và E sau khi quá trình truyền các gói mã hoá kết thúc, và n_{S} là số gói mã hoá mà nguồn S đã gửi đi.

A. OP của mô hình CT

Trong mô hình đề xuất CT, đích D sẽ bị dừng trong ba trường hợp sau:

- *Trường hợp 1*: nút nguồn S gửi tất cả $N_{\max}$ gói mã hoá tuy nhiên nút đích D không thể nhận đủ M gói để khôi phục dữ liệu gốc. Trong trường hợp này, xác suất dừng được viết như sau:

$$\mathrm{OP}_1=\Pr\left(n_{\mathrm{S}}=N_{\max},n_{\mathrm{D}}<H,n_{\mathrm{R}}\le H\right). \quad (11)$$

Trong công thức (11), số lượng gói mã hoá đạt được tại nút chuyển tiếp R cũng không được vượt qua *H*. Nếu số lượng gói mã hoá nhận được tại R là bằng *H* thì gói mã hoá thành công thứ *H* của nút R phải nhận tại lần phát cuối cùng của nút nguồn S. Từ lập luận trên, xác suất dừng OP_1 được tính chính xác bởi:

$$\begin{aligned}\mathrm{OP}_1=&\left[\sum_{n_{\mathrm{D}}=0}^{H-1}C_{N_{\max}}^{n_{\mathrm{D}}}\left(\overline{\rho_{\mathrm{SD}}}\right)^{n_{\mathrm{D}}}\left(\rho_{\mathrm{SD}}\right)^{N_{\max}-n_{\mathrm{D}}}\right]\\&\times\left[\begin{array}{l}C_{N_{\max}-1}^{H-1}\left(\overline{\rho_{\mathrm{SR}}}\right)^{H}\left(\rho_{\mathrm{SR}}\right)^{N_{\max}-H}\\+\sum_{n_{\mathrm{R}}=0}^{H-1}C_{N_{\max}}^{n_{\mathrm{R}}}\left(\overline{\rho_{\mathrm{SR}}}\right)^{n_{\mathrm{R}}}\left(\rho_{\mathrm{SR}}\right)^{N_{\max}-n_{\mathrm{R}}}\end{array}\right].\end{aligned} \quad (12)$$

Trong công thức (12), bởi vì đích D không đạt đủ ít nhất H gói mã hoá, nên giá trị của n_{D} chỉ đi từ 0 đến $H-1$, cụ thể: $0\le n_{\mathrm{D}}\le H-1$. Hơn nữa, trong $N_{\max}$ lần truyền dữ liệu của nguồn S, số cách chọn n_{D} lần nút đích nhận gói mã hoá thành công là $C_{N_{\max}}^{n_{\mathrm{D}}}$. Cũng trong công thức (12), $C_{N_{\max}-1}^{\mathrm{H}-1}\left(\overline{\rho_{\mathrm{SR}}}\right)^{\mathrm{H}}\left(\rho_{\mathrm{SR}}\right)^{N_{\max}-\mathrm{H}}$ là xác suất mà nút chuyển tiếp R đạt được *H* gói mã hoá, và gói mã hoá thứ *H* nhận thành công ở lần truyền cuối cùng của nguồn S.

- *Trường hợp 2*: nút chuyển tiếp R đạt được *H* gói mã hoá trước nút chuyển tiếp D. Trong trường hợp này, số lần truyền tối đa mà nút R có thể thực hiện là $N_{\max}-n_{\mathrm{S}}$. Gọi m_{D} là số gói mã hoá mà nút đích D cần phải tích luỹ thêm để đạt được đủ *H* gói. Xác suất dừng của trường hợp 2 này được đưa ra bằng công thức sau:

$$\mathrm{OP}_2=\Pr\left(\begin{array}{l}H\le n_{\mathrm{S}}<N_{\max},n_{\mathrm{R}}=H,\\n_{\mathrm{D}}<H,m_{\mathrm{D}}>N_{\max}-n_{\mathrm{S}}\end{array}\right). \quad (13)$$

Công thức (13) có nghĩa rằng nút đích không thể nhận đủ *H* gói mã hoá vì số lượng gói cần phải nhận thêm từ R là m_{D} trong khi số lần truyền tối đa của R lại nhỏ hơn m_{D}. Trong trường hợp này, nút R không cần

thiết gửi tiếp các gói mã hoá đến nút D nữa. Do đó, xác suất dừng được tính chính xác như sau:

$$\mathrm{OP}_2 = \sum_{n_\mathrm{S}=H}^{N_{\max}-1}\left[\begin{array}{l} C_{n_\mathrm{S}-1}^{H-1}\left(\overline{\rho_{\mathrm{SR}}}\right)^{H}\left(\rho_{\mathrm{SR}}\right)^{n_\mathrm{S}-H} \\ \times \sum\limits_{m_\mathrm{D}=N_{\max}-n_\mathrm{S}+1}^{H} C_{n_\mathrm{S}}^{H-m_\mathrm{D}}\left(\overline{\rho_{\mathrm{SD}}}\right)^{H-m_\mathrm{D}}\left(\rho_{\mathrm{SD}}\right)^{n_\mathrm{S}-H+m_\mathrm{D}} \end{array}\right]. \quad (14)$$

Trong công thức (14), số gói mã hoá mà đích D đã nhận thành công từ nguồn S sau khi nguồn dừng việc truyền dữ liệu là $H-m_\mathrm{D}$.

- *Trường hợp 3*: nút chuyển tiếp R đạt được H gói mã hoá trước nút chuyển tiếp D và $m_\mathrm{D} \le N_{\max}-n_\mathrm{S}$. Tuy nhiên, nút D không thể nhận đủ m_D gói mã hoá từ nút chuyển tiếp R sau khi nút R sử dụng hết những lần truyền dữ liệu còn lại. Xác suất dừng trong trường hợp này được đưa ra bằng công thức sau:

$$\mathrm{OP}_3 = \Pr\left(\begin{array}{l} H \le n_\mathrm{S} < N_{\max}, n_\mathrm{R} = \mathrm{H}, \\ m_\mathrm{D} \le N_{\max}-n_\mathrm{S}, n_\mathrm{D} < \mathrm{H} \end{array}\right). \quad (15)$$

Do đó, OP_3 được tính chính xác như sau:

$$\mathrm{OP}_3 = \sum_{n_\mathrm{S}=H}^{N_{\max}-1}\left[\begin{array}{l} C_{n_\mathrm{S}-1}^{H-1}\left(\overline{\rho_{\mathrm{SR}}}\right)^{H}\left(\rho_{\mathrm{SR}}\right)^{n_\mathrm{S}-H} \\ \times\left(\begin{array}{l} \sum\limits_{m_\mathrm{D}=1}^{N_{\max}-n_\mathrm{S}} C_{n_\mathrm{S}}^{H-m_\mathrm{D}}\left(\overline{\rho_{\mathrm{SD}}}\right)^{H-m_\mathrm{D}}\left(\rho_{\mathrm{SD}}\right)^{n_\mathrm{S}-H+m_\mathrm{D}} \\ \times \sum\limits_{q_\mathrm{D}=0}^{m_\mathrm{D}-1} C_{N_{\max}-n_\mathrm{S}}^{q_\mathrm{D}}\left(\overline{\rho_{\mathrm{RD}}}\right)^{q_\mathrm{D}}\left(\rho_{\mathrm{RD}}\right)^{N_{\max}-n_\mathrm{S}-q_\mathrm{D}} \end{array}\right) \end{array}\right]. \quad (16)$$

Trong công thức (16), q_D là số gói mã hoá mà nút đích D có thể đạt được từ nút chuyển tiếp R. Bởi vì, $0 \le q_\mathrm{D} < m_\mathrm{D}$ nên nút đích D sẽ không thể đạt đủ H gói mã hoá.

Kết hợp các công thức (12), (14) và (16), tổng xác suất dừng của mô hình CT được tính như sau:

$$\mathrm{OP}_{\mathrm{CT}} = \mathrm{OP}_1 + \mathrm{OP}_2 + \mathrm{OP}_3. \quad (17)$$

B. IP của mô hình CT

Xác suất mất bảo mật của mô hình đề xuất CT sẽ được tính trong bốn trường hợp như bên dưới:

- *Trường hợp 1*: nút nguồn S gửi tất cả $N_{\max}$ gói mã hoá và nút nghe lén E có thể nhận ít nhất H gói mã hoá. Do đó, xác suất mất bảo mật là:

$$\mathrm{IP}_1 = \Pr\left(n_\mathrm{S} = N_{\max}, n_\mathrm{D} \le \mathrm{H}, n_\mathrm{R} \le \mathrm{H}, n_\mathrm{E} \ge H\right). \quad (18)$$

Trong công thức (18), bất kể nút đích D có nhận đủ H gói mã hoá hay không thì dữ liệu của nguồn cũng mất bảo mật bởi vì $n_\mathrm{E} \ge H$. Trong trường hợp nút D hoặc nút R nhận đủ H gói mã hoá thì gói mã hoá thứ H phải nhận ở lần truyền cuối cùng của nguồn S. Từ đó, IP_1 được tính chính xác như sau:

$$\mathrm{IP}_1 = \left[\begin{array}{l} C_{N_{\max}-1}^{H-1}\left(\overline{\rho_{\mathrm{SD}}}\right)^{H}\left(\rho_{\mathrm{SD}}\right)^{N_{\max}-H} \\ +\sum\limits_{n_\mathrm{D}=0}^{H-1} C_{N_{\max}}^{n_\mathrm{D}}\left(\overline{\rho_{\mathrm{SD}}}\right)^{n_\mathrm{D}}\left(\rho_{\mathrm{SD}}\right)^{N_{\max}-n_\mathrm{D}} \end{array}\right] \times \left[\begin{array}{l} C_{N_{\max}-1}^{H-1}\left(\overline{\rho_{\mathrm{SR}}}\right)^{H}\left(\rho_{\mathrm{SR}}\right)^{N_{\max}-H} \\ +\sum\limits_{n_\mathrm{R}=0}^{H-1} C_{N_{\max}}^{n_\mathrm{R}}\left(\overline{\rho_{\mathrm{SR}}}\right)^{n_\mathrm{R}}\left(\rho_{\mathrm{SR}}\right)^{N_{\max}-n_\mathrm{R}} \end{array}\right] \times \sum_{n_\mathrm{E}=H}^{N_{\max}} C_{N_{\max}}^{n_\mathrm{E}}\left(\overline{\rho_{\mathrm{SE}}}\right)^{H}\left(\rho_{\mathrm{SE}}\right)^{N_{\max}-H}. \quad (19)$$

- *Trường hợp 2*: nút đích D có thể nhận được đủ H gói mã hoá trước khi nguồn S gửi hết $N_{\max}$ lần. Điều này có nghĩa là nút nguồn S sẽ dừng việc truyền mà không cần sử dụng $N_{\max}$ lần truyền. Hơn nữa, số lượng gói mã hoá nhận được tại nút chuyển tiếp cũng không thể vượt qua H gói. Cũng vậy, dữ liệu của nguồn sẽ mất bảo mật nếu như $n_\mathrm{E} \ge H$. Do đó, IP trong trường hợp này sẽ là:

$$\mathrm{IP}_2 = \Pr\left(H \le n_\mathrm{S} < N_{\max}, n_\mathrm{R} \le H, n_\mathrm{D} = H, n_\mathrm{E} \ge H\right). \quad (20)$$

Tiếp đến, IP_2 được tính chính xác như sau:

$$\mathrm{IP}_2 = \sum_{n_\mathrm{S}=H}^{N_{\max}-1}\left\{\begin{array}{l} C_{n_\mathrm{S}-1}^{H-1}\left(\overline{\rho_{\mathrm{SD}}}\right)^{H}\left(\rho_{\mathrm{SD}}\right)^{n_\mathrm{S}-H} \\ \times\left[\begin{array}{l} C_{n_\mathrm{S}-1}^{H-1}\left(\overline{\rho_{\mathrm{SR}}}\right)^{H}\left(\rho_{\mathrm{SR}}\right)^{n_\mathrm{S}-H} \\ +\sum\limits_{n_\mathrm{R}=0}^{H-1} C_{n_\mathrm{S}}^{n_\mathrm{R}}\left(\overline{\rho_{\mathrm{SR}}}\right)^{n_\mathrm{R}}\left(\rho_{\mathrm{SR}}\right)^{n_\mathrm{S}-n_\mathrm{R}} \end{array}\right] \\ \times \sum\limits_{n_\mathrm{E}=\mathrm{H}}^{n_\mathrm{S}} C_{n_\mathrm{S}}^{n_\mathrm{E}}\left(\overline{\rho_{\mathrm{SE}}}\right)^{n_\mathrm{E}}\left(\rho_{\mathrm{SE}}\right)^{n_\mathrm{S}-n_\mathrm{E}} \end{array}\right\}. \quad (21)$$

- *Trường hợp 3*: nút chuyển tiếp R đạt được H gói mã hoá trước nút đích D, trong khi nút đích vẫn chưa nhận đủ H gói, và nút E đã nhận ít nhất H gói mã hoá từ nguồn S. Do đó, xác suất mất bảo mật trong trường hợp này là:

$$\mathrm{IP}_3 = \Pr\left(H \le n_\mathrm{S} < N_{\max}, n_\mathrm{R} = H, n_\mathrm{D} < H, n_\mathrm{E} \ge H\right). \quad (22)$$

Từ công thức (22), ta có công thức (23) như sau:

$$\mathrm{IP}_3 = \sum_{n_\mathrm{S}=H}^{N_{\max}-1}\left[\begin{array}{l} C_{n_\mathrm{S}-1}^{H-1}\left(\overline{\rho_{\mathrm{SR}}}\right)^{H}\left(\rho_{\mathrm{SR}}\right)^{n_\mathrm{S}-H} \\ \times\sum\limits_{n_\mathrm{D}=0}^{H-1} C_{n_\mathrm{S}}^{n_\mathrm{D}}\left(\overline{\rho_{\mathrm{SD}}}\right)^{n_\mathrm{D}}\left(\rho_{\mathrm{SD}}\right)^{n_\mathrm{S}-n_\mathrm{D}} \\ \times\sum\limits_{n_\mathrm{E}=H}^{n_\mathrm{S}} C_{n_\mathrm{S}}^{n_\mathrm{E}}\left(\overline{\rho_{\mathrm{SE}}}\right)^{n_\mathrm{R}}\left(\rho_{\mathrm{SE}}\right)^{n_\mathrm{S}-n_\mathrm{E}} \end{array}\right]. \quad (23)$$

- *Trường hợp 4*: nút chuyển tiếp R đạt được H gói mã hoá trước nút đích D, nút đích D và nút nghe lén E vẫn chưa nhận đủ H gói mã hoá. Trong trường hợp này, để nút chuyển tiếp R tiếp tục gửi các gói mã hoá đến đích D thì $m_\mathrm{D} \le N_{\max}-n_\mathrm{S}$. Do đó, nút E tiếp tục nghe lén các gói mã hoá từ nút R và đạt được đủ H gói sau khi sự truyền dữ liệu giữa R và D kết thúc. Xác suất mất bảo mật trong trường hợp này được viết dưới dạng sau:

$$\mathrm{IP}_4 = \Pr\begin{pmatrix} H \le n_\mathrm{S} < N_{\max}, n_\mathrm{R} = H, \\ m_\mathrm{D} \le N_{\max} - n_\mathrm{S}, p_\mathrm{E} < H, n_\mathrm{E} \ge H \end{pmatrix}. \quad (24)$$

Trong công thức (24), p_E là số gói mã hoá mà nút E nhận được từ nguồn S. Tiếp đến, ta tính chính xác IP_4 như trong công thức (25) ở đầu trang kế tiếp. Trong công thức này, t_R là số lần truyền gói dữ liệu của nút R.

Từ các công thức (19), (21), (23) và (25), xác suất mất bảo mật của mô hình CT được đưa ra như sau:

$$\mathrm{IP}_{\mathrm{CT}} = \mathrm{IP}_1 + \mathrm{IP}_2 + \mathrm{IP}_3 + \mathrm{IP}_4. \quad (26)$$

C. OP và IP của mô hình DT

Trong mô hình DT, nút nguồn S sẽ gửi tất cả các gói mã hoá đến đích D mà không cần sự trợ giúp của nút chuyển tiếp. Cũng vậy, một khi nút đích D nhận đủ H gói mã hoá thì nguồn S sẽ dừng việc truyền dữ liệu. Tương tự với các phân tích ở trên, xác suất dừng của mô hình DT được tính chính xác như sau:

$$\mathrm{OP}_{\mathrm{DT}} = \sum_{n_\mathrm{D}=0}^{H-1} C_{N_{\max}}^{n_\mathrm{D}} \left(\overline{\rho_{\mathrm{SD}}}\right)^{n_\mathrm{D}} \left(\rho_{\mathrm{SD}}\right)^{N_{\max}-n_\mathrm{D}}. \quad (27)$$

Đối với xác suất mất bảo mật, ta xét hai trường hợp: i) nút đích D không thể nhận đủ H gói sau $N_{\max}$ lần truyền của nguồn nhưng nút nghe lén E đã nhận ít nhất H gói; ii) nút đích D nhận đủ H gói và nút nghe lén E cũng đã nhận ít nhất H gói. Do đó, ta có thể biểu diễn xác suất mất bảo mật trong mô hình DT như sau:

$$\begin{aligned} \mathrm{IP}_{\mathrm{DT}} &= \Pr\left(n_\mathrm{S} = N_{\max}, n_\mathrm{D} < H, n_\mathrm{E} \ge H\right) \\ &\quad + \Pr\left(n_\mathrm{S} \le N_{\max}, n_\mathrm{D} = H, n_\mathrm{E} \ge H\right). \end{aligned} \quad (28)$$

Từ công thức (28), ta có:

$$\begin{aligned} \mathrm{IP}_{\mathrm{DT}} &= \sum_{n_\mathrm{D}=0}^{H-1} C_{N_{\max}}^{n_\mathrm{D}} \left(\overline{\rho_{\mathrm{SD}}}\right)^{n_\mathrm{D}} \left(\rho_{\mathrm{SD}}\right)^{N_{\max}-n_\mathrm{D}} \\ &\quad \times \sum_{n_\mathrm{E}=H}^{N_{\max}} \left(\overline{\rho_{\mathrm{SE}}}\right)^{n_\mathrm{E}} \left(\rho_{\mathrm{SE}}\right)^{N_{\max}-n_\mathrm{E}} \\ &\quad + \sum_{n_\mathrm{S}=H}^{N_{\max}} C_{n_\mathrm{S}-1}^{H-1} \left(\overline{\rho_{\mathrm{SD}}}\right)^{H} \left(\rho_{\mathrm{SD}}\right)^{n_\mathrm{S}-H} \\ &\quad \times \sum_{n_\mathrm{E}=H}^{n_\mathrm{S}} C_{n_\mathrm{S}}^{n_\mathrm{E}} \left(\overline{\rho_{\mathrm{SE}}}\right)^{n_\mathrm{E}} \left(\rho_{\mathrm{SE}}\right)^{n_\mathrm{S}-n_\mathrm{E}}. \end{aligned} \quad (29)$$

IV. KẾT QUẢ MÔ PHỎNG VÀ LÝ THUYẾT

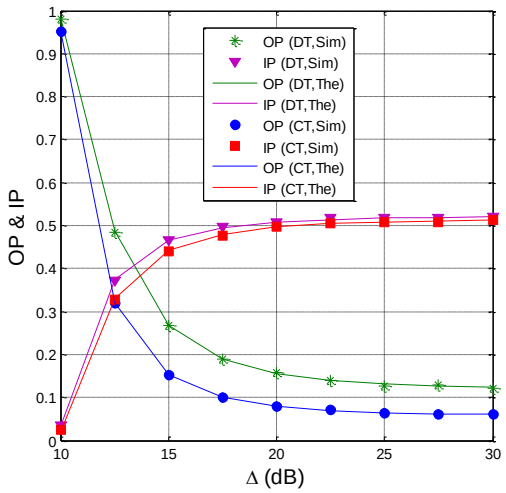
Trong mục này, mô phỏng Monte Carlo được thực hiện để kiểm chứng các công thức đã đưa ra trong mục III. Môi trường mô phỏng là mặt phẳng hai chiều Oxy, trong đó các nút được đặt ở các vị trí sau: $\mathrm{S}(0,0)$, $\mathrm{R}(x_\mathrm{R},0)$, $\mathrm{D}(1,0)$, $\mathrm{T}(0.5,1.5)$ và $\mathrm{U}(0.5,0.75)$, với $0 < x_\mathrm{R} < 1$. Trong các kết quả mô phỏng (Sim: Simulation) và lý thuyết (The: Theory), để tập trung phân tích xu hướng hiệu năng của các mô hình nghiên cứu, một số tham số hệ thống được cố định như sau: $\beta = 3$, $\psi_\mathrm{P} = 1$ và $\varepsilon_{\mathrm{OP}} = 0.05$. Ta cũng lưu ý rằng, các biểu thức đạt được trong bài báo được đưa ra dưới dạng tường minh và được biểu diễn bằng các công thức dạng chữ. Do đó, các công thức đạt được có thể được sử dụng cho tất cả các giá trị khác nhau của các tham số hệ thống trong thực tế.

Hình 2 vẽ xác suất dừng (OP) và xác suất mất bảo mật (IP) theo tỷ số SNR phát Δ(dB) $\left(\Delta = P_\mathrm{T}/\sigma_0^2\right)$ với $H = 4$, $N_{\max} = 6$, $\psi_\mathrm{S} = 0.1$ và $x_\mathrm{R} = 0.5$. Quan sát từ Hình 2, ta thấy mô hình CT đạt được giá trị OP và IP thấp hơn mô hình DT. Có nghĩa rằng mô hình chuyển tiếp cộng tác đạt được hiệu quả bảo mật và độ tin cậy của việc truyền dữ liệu tốt hơn mô hình truyền trực tiếp. Hình 2 cũng cho thấy rằng khi tăng Δ thì OP của cả hai mô hình đều giảm, tuy nhiên IP lại tăng. Bởi vì khi tăng Δ thì công suất phát P_T cũng tăng, dẫn đến SNR đạt được tại nút chuyển tiếp, nút đích và nút nghe lén đều tăng. Do đó, OP của hệ thống giảm nhưng IP của hệ thống lại tăng. Để thấy được ưu điểm của mô hình CT, ta xét ví dụ sau: trong mô hình DT, để đạt được OP < 0.2 thì $\Delta \approx 17.5$ dB, và giá trị IP ở mức gần 0.5. Tuy nhiên, để đạt được OP < 0.2, thì mô hình CT chỉ cần $\Delta \approx 14$ dB, và IP vào khoảng 0.38. Do đó, công suất phát P_T cần được hiệu chỉnh để có thể đạt được OP mong muốn, cũng như giảm giá trị IP xuống mức thấp nhất có thể.

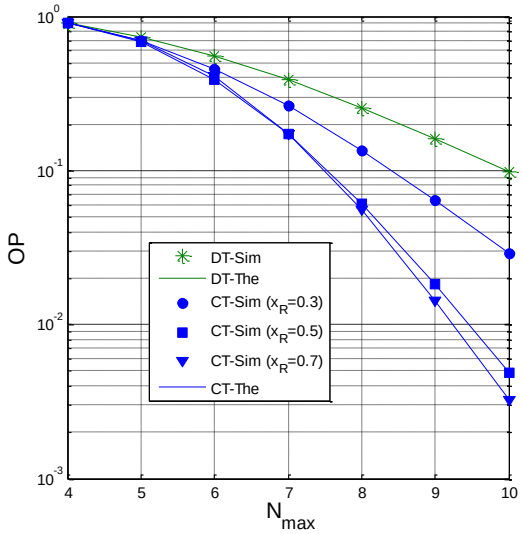
Hình 3 và 4 lần lượt thể hiện xác suất dừng (OP) và xác suất mất bảo mật (IP) của mô hình CT và DT theo $N_{\max}$ với $\Delta = 20$ (dB), $H = 4$ và $\gamma_\mathrm{S} = 0.25$. Quan sát từ Hình 3, ta thấy rằng khi tăng giá trị $N_{\max}$, xác suất dừng của hai mô hình CT và DT đều giảm. Đó là vì với $N_{\max}$ lớn, thì xác suất nút đích tích luỹ đủ H gói mã hoá sẽ tăng lên, và vì vậy, xác suất dừng tại D sẽ giảm. Hình 3 cũng cho ta thấy OP của mô hình CT giảm nhanh hơn mô hình DT khi giá trị $N_{\max}$ tăng. Cũng quan sát từ Hình 3, khi tăng $N_{\max}$, OP của mô hình CT giảm nhanh hơn OP của mô hình DT. Hơn nữa, ta cũng quan sát được rằng vị trí của nút chuyển tiếp cũng ảnh hưởng đáng kể đến giá trị OP của mô hình CT. Như ta có thể thấy, OP của mô hình CT có giá trị lớn khi đặt nút chuyển tiếp ở vị trí $x_\mathrm{R} = 0.3$. Mặt khác, trong trường hợp $x_\mathrm{R} = 0.5$ và $x_\mathrm{R} = 0.7$, các giá trị OP tại đích D chênh lệch không nhiều.

Đối với giá trị IP trong Hình 4, ta cũng thấy rằng giá trị này tăng khi $N_{\max}$ tăng. Như đã giải thích ở trên, giá trị $N_{\max}$ tăng sẽ làm tăng xác suất nút nghe lén nhận đủ số gói mã hoá, và do đó, xác suất mất bảo mật cũng tăng. Hơn nữa, $N_{\max}$ càng lớn thì thời gian trễ cũng sẽ tăng. Ta cũng thấy từ Hình 4 rằng, vị trí của nút chuyển tiếp cũng ảnh hưởng đến khả năng nghe lén của nút E. Ví dụ: khi $N_{\max} = 5$, IP thấp nhất khi $x_\mathrm{R} = 0.3$, tuy nhiên khi $N_{\max} = 7$ thì IP thấp nhất khi $x_\mathrm{R} = 0.7$. Hình 4 cũng cho ta thấy IP của mô hình CT có thể đạt giá trị thấp hơn khi so sánh với mô hình DT. Mặc dù, giá trị IP biến thiên theo sự thay đổi của x_R và $N_{\max}$, tuy nhiên sự chênh lệch hiệu năng giữa mô hình CT và DT là không quá lớn.

$$\mathrm{IP}_4 = \sum_{n_E=H}^{N_{\max}-1}\sum_{n_S=H}^{N_{\max}-1}\left\{ C_{n_S-1}^{H-1}\left(\overline{\rho_{SR}}\right)^{H}\left(\rho_{SR}\right)^{n_S-H} \times \sum_{p_E=0}^{H-1}\left[C_{p_E}^{n_S}\left(\overline{\rho_{SE}}\right)^{p_E}\left(\rho_{SE}\right)^{n_S-p_E} \times \sum_{m_D=1}^{N_{\max}-n_S} C_{n_S}^{H-m_D}\left(\overline{\rho_{SD}}\right)^{H-m_D}\left(\rho_{SD}\right)^{n_S-H+m_D} \times \left(\sum_{q_D=0}^{m_D-1} C_{N_{\max}-n_S}^{q_D}\left(\overline{\rho_{RD}}\right)^{q_D}\left(\rho_{RD}\right)^{N_{\max}-n_S-q_D} \times C_{N_{\max}-n_S}^{n_E-p_E}\left(\overline{\rho_{RE}}\right)^{n_E-p_E}\left(\rho_{RD}\right)^{N_{\max}-n_S-n_E+p_E} + \sum_{t_R=m_D}^{N_{\max}-n_S} C_{t_R-1}^{m_D-1}\left(\overline{\rho_{RD}}\right)^{m_D}\left(\rho_{RD}\right)^{t_R-m_D} \times C_{t_R}^{n_E-p_E}\left(\overline{\rho_{RE}}\right)^{n_E-p_E}\left(\rho_{RD}\right)^{t_R-n_E+p_E} \right) \right] \right\}. \quad (25)$$



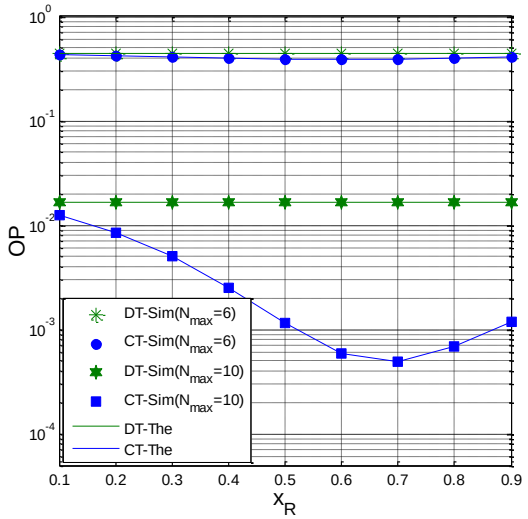
Hình 2. OP và IP vẽ theo Δ (dB) với $H=4$, $N_{\max}=6$, $\psi_S=0.1$ và $x_R=0.5$.



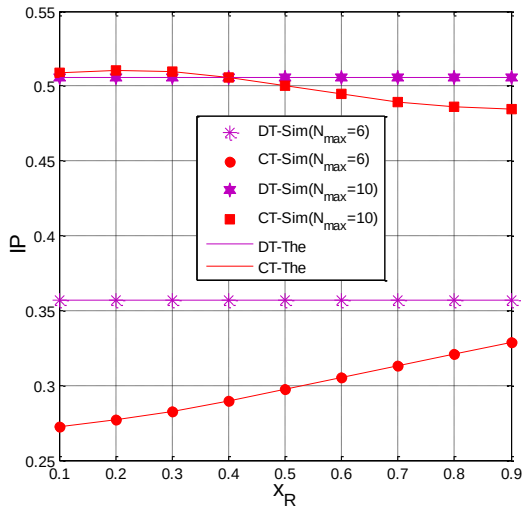
Hình 3. OP vẽ theo $N_{\max}$ với $\Delta=20$ (dB), $H=4$ và $\gamma_S=0.25$.

Hình 5 và 6 khảo sát sự ảnh hưởng vị trí nút chuyển tiếp lên các giá trị OP và IP của mô hình CT khi $\Delta=20$ (dB), $H=5$ và $\psi_S=0.1$. Hình 5 cho ta thấy rằng vị trí nút R ảnh hưởng đáng kể lên giá trị OP của mô hình CT, và xác suất dừng của mô hình CT luôn thấp hơn mô hình DT. Như ta quan sát, tồn tại vị trí của nút R để OP trong mô hình CT đạt giá trị nhỏ nhất. Ví dụ: khi $N_{\max}=10$ thì vị trí tối ưu của nút R trong Hình 5 là $x_R=0.7$.

Hình 6 cũng cho ta thấy rằng vị trí nút R ảnh hưởng đến khả năng nghe lén của nút E trong mô hình CT. Với $N_{\max}=10$, ta quan sát rằng sự biến thiên của IP theo x_R là khá phức tạp. Mặc khác, khi $N_{\max}=6$, IP của mô hình CT luôn tăng khi x_R tăng từ 0.1 lên 0.9.



Hình 5. OP vẽ theo x_R với $\Delta=20$ (dB), $H=5$ và $\psi_S=0.1$.



Hình 6. IP vẽ theo x_R với $\Delta=20$ (dB), $H=5$ và $\psi_S=0.1$.

Những Hình 2-6 cho ta thấy kết quả mô phỏng và lý thuyết trùng với nhau, điều này kiểm chứng tính chính xác của các kết quả phân tích.

V. KẾT LUẬN

Bài báo đề xuất mô hình chuyển tiếp công tác để nâng cao độ tin cậy và khả năng bảo mật của mạng thứ cấp, sử dụng mã Fountain, khi so sánh với mô hình truyền trực tiếp giữa nguồn và đích. Các kết quả cũng cho thấy rằng có một sự đánh đổi giữa bảo mật thông tin và độ tin cậy của việc truyền tin. Do đó, trong quá trình thiết kế hệ thống, các tham số quan trọng như công suất phát, số lần truyền gói mã hoá tối đa hay vị trí nút chuyển tiếp cần được thiết kế một cách tối ưu.

Trong tương lai, chúng tôi sẽ phát triển mô hình đề xuất theo hướng nhiều nút chuyển tiếp cộng tác, cũng như đề xuất các phương pháp chọn lựa nút chuyển tiếp hiệu quả để nâng cao hơn nữa hiệu năng OP của hệ thống. Ngoài ta, kỹ thuật tạo nhiễu lên thiết bị nghe lén cũng sẽ được nghiên cứu áp dụng để bảo vệ tốt hơn dữ liệu nguồn.

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 05-HV-2020-RD_VT2.

TÀI LIỆU THAM KHẢO

[1] A. D. Wyner, “The Wire-Tap Channel,” The Bell System Technical Journal vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] R. Liu, I. Maric, P. Spasojevic, R. D. Yates, "Discrete Memoryless Interference and Broadcast Channels With Confidential Messages: Secrecy Rate Regions," IEEE Transactions on Information Theory, vol. 54, no. 6, pp. 2493-2507, Jun. 2008.

[3] J. Zhang, Trung Q. Duong, R. Woods, A. Marshall, “Securing Wireless Communications of the Internet of Things From The Physical Layer, An Overview,” Entropy, vol. 19, no. 8, (420) Aug. 2017.

[4] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, I. B. Collings, "Transmit Antenna Selection for Security Enhancement in MIMO Wiretap Channels," IEEE Transactions on Communications, vol. 61, no. 1, pp. 144-154, Jan. 2013.

[5] N. Yang, H. A. Suraweera, I. B. Collings, C. Yuen, "Physical Layer Security of TAS/MRC With Antenna Correlation," IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 254-259, Jan. 2013.

[6] H. Zhao, Y. Tan, G. Pan, Y. Chen, N. Yang, "Secrecy Outage on Transmit Antenna Selection/Maximal Ratio Combining in MIMO Cognitive Radio Networks," IEEE Transactions on Vehicular Technology, vol. 65, no. 12, pp. 10236-10242, Dec. 2016.

[7] J. N. Laneman, D. N. C. Tse and G. W. Wornell, "Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior," IEEE Transactions on Information Theory, vol. 50, no. 12, pp. 3062-3080, Dec. 2004.

[8] C. Cai, Y. Cai, W. Yang, W. Yang, "Secure Connectivity Using Randomize-and-Forward Strategy in Cooperative Wireless Networks," IEEE Communications Letters, vol. 17, no. 7, pp. 1340-1343, Jul. 2013.

[9] P. N. Son, H. Y. Kong, "Cooperative Communication With Energy-Harvesting Relays Under Physical Layer Security," IET Communications, vol. 9, no. 17, pp. 2131-2139, Nov. 2015.

[10] T. T. Duy, T. Q. Duong, T. L. Thanh, 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.

[11] L. Fan, X. Lei, N. Yang, T. Q. Duong, G. K. Karagiannidis, "Secure Multiple Amplify-and-Forward Relaying With Cochannel Interference," IEEE Journal of Selected Topics in Signal Processing, vol. 10, no. 8, pp. 1494-1505, Dec. 2016.

[12] L. Dong, Z. Han, A. P. Petropulu, H. V. Poor, “Improving Wireless Physical Layer Security via Cooperating Relays,” IEEE Transactions on Signal Processing, vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[13] S. Jia, J. Zhang, H. Zhao, R. Zhang, “Relay Selection for Improved Security in Cognitive Relay Networks with Jamming,” IEEE Wireless Communications Letters, vol. 6, no. 5, pp. 662-665, Oct. 2017.

[14] X. Ding, T. Song, Y. Zou, X. Chen, L. Hanzo, "Security-Reliability Tradeoff Analysis of Artificial Noise Aided Two-Way Opportunistic Relay Selection," IEEE Transactions on Vehicular Technology, vol. 66, no. 5, pp. 3930-3941, May 2017.

[15] X. Ding, Y. Zou, F. Ding, D. Zhang, G. Zhang, "Opportunistic Relaying Against Eavesdropping for Internet-of-Things: A Security-Reliability Tradeoff Perspective," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8727-8738, Oct. 2019.

[16] J. Mitola, G. Q. Maguire, “Cognitive Radio: Making Software Radios More Personal,” IEEE Personal Communications, vol. 6, no. 4, pp. 13-18, Aug. 1999.

[17] J. Hong, B. Hong, T. W. Ban, W. Choi, "On the Cooperative Diversity Gain in Underlay Cognitive Radio Systems," IEEE Transactions on Communications, vol. 60, no. 1, pp. 209-219, Jan. 2012.

[18] C. Xu, M. Zheng, W. Liang, H. Yu, Y. Liang, "Outage Performance of Underlay Multihop Cognitive Relay Networks With Energy Harvesting," IEEE Communications Letters, vol. 20, no. 6, pp. 1148-1151, Jun. 2016.

[19] V. N. Q. Bao, T. Q. Duong, C. Tellambura, "On the Performance of Cognitive Underlay Multihop Networks with Imperfect Channel State Information," IEEE Transactions on Communications, vol. 61, no. 12, pp. 4864-4873, Dec. 2013.

[20] P. T. D. Ngoc, T. T. Duy, H. V. Khuong, "Outage Performance of Cooperative Cognitive Radio Networks under Joint Constraints of Co-Channel Interference, Intercept Probability and Hardware Imperfection," EAI Transactions on Industrial Networks and Intelligent Systems, vol. 6, no. 19, pp. 1-8, Jun. 2019.

[21] M. Luby, "LT Codes," in Proc. of The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings., Vancouver, BC, 2002, pp. 271-280.

[22] A. Shokrollahi, "Raptor Codes," IEEE Transactions on Information Theory, vol. 52, no. 6, pp. 2551-2567, Jun. 2006.

[23] H. Niu, M. Iwai, K. Sezaki, L. Sun and Q. Du, "Exploiting Fountain Codes for Secure Wireless Delivery," IEEE Communications Letters, vol. 18, no. 5, pp. 777-780, May 2014.

[24] W. Li, Q. Du, L. Sun, P. Ren, Y. Wang, "Security Enhanced via Dynamic Fountain Code Design for Wireless Delivery," in Proc. of 2016 IEEE Wireless Communications and Networking Conference, Doha, 2016, pp. 1-6.

[25] L. Sun, P. Ren, Q. Du, and Y. Wang, “Fountain-Coding Aided Strategy for Secure Cooperative Transmission in Industrial Wireless Sensor Networks,” IEEE Trans. Industrial Inform., vol. 12, no. 1, pp. 291-300, Feb. 2016.

[26] D. T. Hung, T. T. Duy, D. Q. Trinh and V. N. Q. Bao, "Secrecy Performance Evaluation of TAS Protocol Exploiting Fountain Codes and Cooperative Jamming under Impact of Hardware Impairments," in Proc. of the 2nd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing, pp. 164-169, HoChiMinh city, VietNam.

[27] P. T. Tin, N. N. Tan, N. Q. Sang, T. T. Duy, T. T. Phuong, M. Voznak, "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, (700), Jul. 2019.

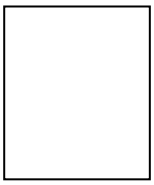
[28] D. T. Hung, T. T. Duy, T. T. Phuong, D. Q. Trinh, T. Hanh, "Performance Comparison between Fountain Codes-Based Secure MIMO Protocols with and without Using Non-Orthogonal Multiple Access," Entropy, vol. 21, no. 10, (928), Oct. 2019.

[29] D. T. Hung, T. T. Duy, D. Q. Trinh, "Nghiên Cứu Hiệu Năng Truyền Bảo Mật Sử Dụng Mã Fountain Trong Mạng Vô Tuyến Nhận Thức Dưới Sự Tác Động Của Khiếm Khuyết Phần Cứng," Tạp Chí Nghiên Cứu Khoa Học và Công Nghệ Quân Sự, số 59, pp. 58-69, 02/2019.

PERFORMANCE EVALUATION OF SECURE COOPERATIVE COMMUNICATION PROTOCOL IN UNDERLAY COGNITIVE RADIO NETWORKS USING FOUNTAIN CODES

Abstract: In this paper, we evaluate performance of a secure cooperative communication protocol in underlay cognitive radio network using Fountain codes. In the proposed protocol, a secondary source and a secondary relay have to adjust their transmit power to guarantee quality of service of a primary network. Employing Fountain codes, the source sends encoded packets to the relay and destination. If the destination can receive a sufficient number of the encoded packets, it will recover the source data correctly. Moreover, if the relay can obtain enough number of the encoded packet before the destination, it (instead of the source) will send the encoded packets to the destination. In the secondary network, an eavesdropper attempts to decode the source data illegally. Also, if the eavesdropper obtains enough number of the encoded packets, the data transmission is insecure. For performance evaluation, we focus on two important metrics: i) OP (Outage Probability) is probability that the destination cannot receive enough number of the encoded packets for the data recovery; ii) IP (Insecure Probability) is probability that the source data is intercepted by the eavesdropper or the probability that the eavesdropper can accumulate encoded packets sufficiently. We derive exact closed-form expressions of OP and IP for the secondary network over Rayleigh fading channel, under impact of co-channel interference from the primary network. All the derived formulas are verified by computer simulations using Monte Carlo method. The obtained results present that there is a trade-off between OP and IP. In addition, the proposed protocol can obtain better OP and IP performance as compared with the direct transmission protocol that does not employ cooperative communication.

Keywords: *Fountain codes, underlay cognitive radio, physical-layer security, outage probability, intercept probability, cooperative communication.*



Nguyễn Văn Hiền nhận bằng Kỹ Sư vào năm 2004 tại Học Viện Công Nghệ BCVT cơ sở tahi Tp. HCM. KS. Nguyễn Văn Hiền hiện đang công tác tại Khoa Viễn Thông 2, thuộc Học Viện Công Nghệ Bưu Chính Viễn Thông cơ sở tại TP. Hồ Chí Minh. Hướng nghiên cứu hiện tại: IoT, mạng máy tính và truyền thông vô tuyến.

Email:nvhien@ptithcm.edu.vn

Trần Trung Duy nhận bằng tiến Sỹ vào năm 2013 tại Đại Học Ulsan, Hàn Quốc. TS. Trần Trung Duy hiện đang công tác tại Khoa Viễn Thông 2, thuộc Học Viện Công Nghệ Bưu Chính Viễn Thông cơ sở tại TP. Hồ Chí Minh. Hướng nghiên cứu hiện tại: truyền thông vô tuyến.

Email:
trantrungduy@ptithcm.edu.vn

Trần Đình Thuần nhận bằng Thạc Sỹ vào năm 1998 tại ĐH Bách Khoa Hà Nội, Việt Nam. Th.S. Trần Đình Thuần hiện đang công tác tại Khoa Viễn Thông 2, thuộc Học Viện Công Nghệ Bưu Chính Viễn Thông cơ sở tại TP. Hồ Chí Minh. Hướng nghiên cứu hiện tại: IoT và mạng máy tính.

Email:
tdthuan@ptithcm.edu.vn