PHÂN TÍCH KẾT NỐI AN TOÀN VÀ SỐ CHẶNG CỦA MẠNG TÙY BIẾN ĐA CHẶNG KHI CÓ NHỮNG THIẾT BỊ NGHE LÉN THÔNG ĐỒNG

Lê Thế Dũng[1*], Lê Ngọc Dùng[2]

[1]*Trường Đại học FPT Tp. Hồ Chí Minh*
[2] *Trường Đại học Công nghệ Đồng Nai*
*Tác giả liên hệ: Lê Thế Dũng, *dunglt96@fe.edu.vn*

THÔNG TIN CHUNG

Ngày nhận bài: 11/08/2024

Ngày nhận bài sửa: 13/09/2024

Ngày duyệt đăng: 30/09/2024

TỪ KHOÁ

Kết nối an toàn;
Mạng tùy biến đa chặng;
Số chặng;
Thiết bị nghe lén thông đồng.

TÓM TẮT

Tính kết nối và số chặng kết nối là hai thuộc tính quan trọng của mạng tùy biến đa chặng. Khi xem xét vấn đề bảo mật, việc thiết lập đường truyền đa chặng an toàn là một thách thức vì một nút trung gian có liên kết với các nút ở phía trước có thể không an toàn để nhận dữ liệu từ các nút đó và ngược lại. Để phân tích đặc tính này, chúng tôi sử dụng đồ thị hình học ngẫu nhiên để mô hình hóa mạng tùy biến đa chặng có sự hiện diện của nhiều thiết bị nghe lén trong trường hợp bảo mật xấu nhất là khi thiết bị nghe lén thông đồng với nhau. Tiếp theo, chúng tôi đề xuất phương pháp phân tích dựa trên mô phỏng để có được các điểm về tính kết nối, phân bố số chặng và số chặng trung bình trong nhiều kịch bản đánh giá khác nhau. Kết quả mô phỏng cho thấy rằng tính kết nối đạt giá trị bão hòa là 0,93 khi mật độ nút hợp pháp là $1,88\times10^{-3}$ nút/m^2. Ngoài ra tham số hình dạng của kênh fading Nakagami chỉ làm tính kết nối giảm 5,62% so với 29,96% của mật độ nút nghe lén. Các kết quả trong bài báo này cung cấp những thông tin có giá trị trong việc thiết kế và đánh giá mạng tùy biến đa chặng có xét đến bảo mật.

1. GIỚI THIỆU

Mạng không dây tùy biến (AHWN) là mạng không dây phi tập trung, bao gồm nhiều nút di động không dây tạo thành mạng tạm thời mà không sử dụng bất kỳ cơ sở hạn tầng cố định hoặc quản trị tập trung (Sarkar et al., 2013). Tùy theo những ứng dụng cụ thể, mạng AHWN có thể được phân loại thành mạng cảm biến không dây trong đó nhiều cảm biến chuyên dụng được phân tán trên bề mặt để ghi lại các điều kiện vật lý của môi trường xung quanh (Agarkar et al., 2020). Trái ngược với mạng AHWN, trong mạng cảm biến không dây, dữ liệu được thu thập tại mỗi cảm biến được chuyển tiếp đến một nút trung tâm của mỗi nhóm cảm biến (Rekha et al., 2020). Do tất cả các nút không dây đều thực hiện truyền thông rộng rãi nên mạng AHWN dễ bị nghe lén và tấn công mạo danh. Thông thường các thuật toán mật mã đối xứng được sử dụng để bảo vệ tính bảo mật và xác thực của thông tin liên lạc. Các thuật toán mã hóa cấp bit này có một số nhược điểm, chẳng hạn như bảo vệ chuẩn hóa trong các mạng không dây công cộng có thể không đủ an toàn

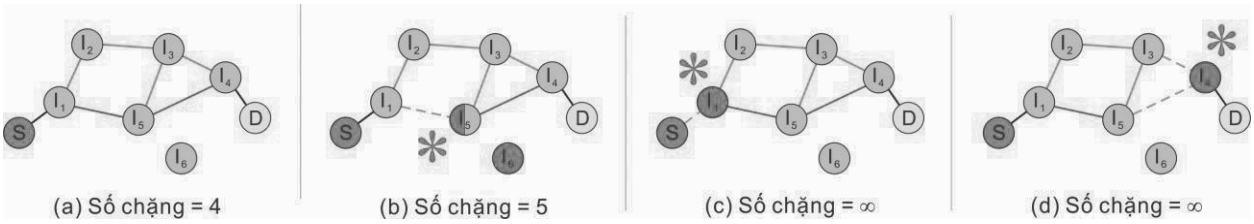
và ngay cả khi có các giao thức xác thực và mã hóa nâng cao chúng vẫn yêu cầu các ràng buộc mạnh và chi phí cao. Đặc biệt trong các mạng không dây động như mạng AHWN, nơi các nút di động có thể ngẫu nhiên tham gia và rời khỏi mạng bất cứ lúc nào, vấn đề phân phối chìa khóa cho các hệ thống mật mã đối xứng trở nên khó khăn hơn. Hơn nữa, tất cả các kỹ thuật mã hóa dựa trên khóa đều dựa trên giả định rằng về mặt tính toán, chúng không khả thi để giải mã nếu không có thông tin về chìa khóa bí mật. Tuy nhiên, do sự tiến bộ nhanh chóng của công nghệ máy tính, kẻ tấn công có thể thực hiện tìm kiếm khóa toàn diện (còn gọi là tấn công brute-force) với hy vọng cuối cùng sẽ đoán đúng chìa khóa. Do đó, một cơ chế bảo mật thay thế, cụ thể là bảo mật lý thuyết thông tin hoặc bảo mật lớp vật lý (PLS), đã được giới thiệu. Phương pháp bảo mật mới này tập trung vào khả năng bảo mật của các kênh không dây. Việc áp dụng các kỹ thuật bảo mật lớp vật lý cho mạng AHWN so với các kỹ thuật mật mã truyền thống có hai ưu điểm. Đầu tiên, các kỹ thuật bảo mật lớp vật lý không dựa vào độ phức tạp của tính toán mà khai thác tính ngẫu nhiên vốn có của nhiễu và các kênh truyền thông để hạn chế lượng thông tin mà nút nghe lén có thể trích xuất. Thứ hai, các phương pháp bảo mật lớp vật lý có thể thực hiện giao tiếp bí mật qua các kênh không dây mà không cần sử dụng khóa mã hóa; do đó, chúng rất phù hợp với mạng AHWN vì không cần thêm các gói tin điều khiển.

Lịch sử của PLS bắt đầu từ phân tích lý thuyết thông tin bảo mật của Shannon (Shannon, 1949), sau đó được phát triển thành công trình của Wyner về kênh nghe lén (Wyner, 1975), trong đó máy phát muốn truyền đạt các thông điệp riêng tư qua kênh chính trong khi nút nghe lén cố gắng truy cập bất hợp pháp vào kênh liên lạc này. Gần đây, việc phân tích PLS của các mạng quy mô lớn đã thu hút được nhiều sự chú ý của các nhà nghiên cứu. Không giống như với mạng điểm-đến-điểm, việc giao tiếp giữa các nút trong các mạng quy mô lớn phụ thuộc rất nhiều vào vị trí và tương tác giữa các nút.

2. ĐỘNG LỰC VÀ ĐÓNG GÓP

Như đã trình bày ở trên, mặc dù các tính năng về khả năng kết nối hoặc số chặng của đường truyền đa chặng trong mạng không dây đã được tìm hiểu rộng rãi, nhưng có rất ít nghiên cứu tập trung vào việc phân tích đồng thời hai đặc tính cơ bản này. Cụ thể, trong bài báo (Ibrahim et al., 2021) các tác giả nghiên cứu hiệu suất của hai kỹ thuật định tuyến phù hợp cho mạng mmWave, cụ thể là kỹ thuật số chặng tối thiểu (MHC) và kỹ thuật chuyển tiếp LoS gần nhất đến đích với MHC (NLR-MHC). Các mô hình phân tích được cung cấp để đánh giá hiệu suất của hai kỹ thuật định tuyến này bằng các công cụ từ hình học ngẫu nhiên. Các tác giả trong bài báo (Li et al., 2022) đưa ra một biểu thức phân phối số chặng trong một mạng tùy biến hữu hạn theo các giao thức định tuyến số chặng tối thiểu. Bằng cách sử dụng phân phối nút theo quy trình điểm nhị thức, mạng được cung cấp trong bài báo là một vùng giới hạn với tất cả các nút được phân phối ngẫu nhiên và đồng đều. Trong bài báo (Xiao et al., 2021), tác động của va chạm gói tin trong lớp điều khiển truy cập kênh truyền (MAC) đối với xác suất kết nối của mạng kết nối phương tiện giao thông. Điểm chung của tất cả các công trình được đề cập ở trên là đều bỏ qua vấn đề về kết nối an toàn. Để truyền thông phù hợp trong một số trường hợp, kết nối giữa hai nút trong mạng tùy biến không dây phải đáp ứng cả hai ràng buộc về suy giảm công suất tín hiệu nhận được và tính bảo mật của liên kết. Mặt khác, vì các đường truyền trong mạng tùy biến không dây thường bao gồm nhiều chặng nên việc đảm bảo sự an toàn cho đường truyền đa chặng là rất khó khăn (Chen et al., 2018). Chúng ta nên lưu ý rằng điều kiện để có liên kết không dây giữa hai nút không phụ thuộc vào điều kiện để đảm bảo liên kết này an toàn. Ví dụ, liên kết không dây giữa hai nút tồn tại, nhưng liên kết đó có thể không an toàn để truyền thông và ngược lại. Do đó, việc thiết lập các đường truyền đa chặng an toàn trong các mạng động như trong mạng tùy biến không dây cực kỳ phức tạp vì một nút trung gian có thể được kết nối với một tập hợp

nhất định các nút trước đó và chỉ an toàn để nhận dữ liệu từ một tập hợp khác các nút trước đó. Trong bài báo (Zheng et al., 2022), mặc dù các tác giả đã đề xuất một giải pháp đó là nút hợp pháp gửi tín hiệu gây nhiễu với một xác suất nhất định để đánh bại những nút nghe lén và phân tích xác suất mất kết nối và xác suất mất bảo mật để đánh giá độ tin cậy của đường truyền, tuy nhiên các tác giả không phân tích ảnh hưởng của các yếu tố này lên số chặng của đường truyền. Trong phần sau, chúng tôi sẽ đưa ra một ví dụ cụ thể, cho thấy hiệu ứng kết hợp của bảo mật và fading kênh ảnh hưởng đến số chặng và đặc điểm kết nối của đường truyền giữa hai nút hợp pháp được chọn ngẫu nhiên làm nút nguồn và nút đích.



Hình 1.Tác động của nút nghe lén lên số chặng và tính kết nối của đường truyền giữa nút nguồn (S) và nút đích (D) hợp pháp.

Hình 1 minh họa sự xuất hiện của nút nghe lén (được biểu thị là dấu hoa thị màu đỏ) ảnh hưởng lớn đến số chặng và kết nối của đường truyền đa chặng ngắn nhất giữa nút nguồn (S) và nút đích (D) hợp pháp trong mạng AHWN. Cụ thể, trong Hình 1(a), khi không có nút nghe lén trong mạng, đường truyền ngắn nhất từ S đến D là S $\rightarrow$ I1 $\rightarrow$ I5 $\rightarrow$ I4 $\rightarrow$ D, có số chặng là 4. Tuy nhiên, vì nút nghe lén tồn tại gần I5 như trong Hình 1(b), đường truyền ngắn nhất từ S đến D sẽ là S $\rightarrow$ I1 $\rightarrow$ I2 $\rightarrow$ I3 $\rightarrow$ I4 $\rightarrow$ D, có số chặng là 5. Lưu ý rằng tương tự như trường hợp trong Hình 1(a), I6 không có liên kết không dây với những nút hợp lệ khác do hiện tượng fading của kênh truyền. Hơn nữa,I6 không an toàn (được thể hiện bằng nền đỏ) để nhận dữ liệu từ bất kỳ nút hợp pháp nào. Ngược lại, I5 không an toàn để nhận dữ liệu từ I1 (tức là kết nối I1 − I5 không thỏa mãn ràng buộc bảo mật), nhưng an toàn để nhận dữ liệu từ I3. Do đó, I5 được biểu diễn dưới dạng một nửa vòng tròn xanh nửa vòng tròn đỏ. Trong trường hợp tệ nhất, không có đường truyền thông tin an toàn nào từ S đến D vì I1 không an toàn để nhận dữ liệu từ S như trong Hình 1(c) và I4 không an toàn để nhận dữ liệu từ I3 và I5 như trong Hình 1(d). Tóm lại, tùy thuộc vào điều kiện kênh, một liên kết không dây giữa hai nút hợp pháp được thiết lập hoặc an toàn để gửi dữ liệu. Các thuộc tính này độc lập; do đó, một nút hợp pháp có thể kết nối với một nút hợp pháp khác, nhưng liên kết không dây giữa chúng có thể không an toàn để gửi dữ liệu và ngược lại. Do đó, khả năng kết nối và số chặng của các đường truyền bảo mật đa chặng trong mạng AHWN cực kỳ phức tạp vì đường truyền bảo mật đa chặng giữa S và D chỉ có thể thiết lập thành công nếu nút dùng trung gian hợp pháp đều có ít nhất một liên kết không dây an toàn.

Từ quan sát trên, chúng tôi quan tâm đến việc đưa ra một nghiên cứu sâu sắc về số chặng và đặc điểm kết nối của đường truyền đa bước của mạng AHWN có xét đến bảo mật. Để hoàn thành nhiệm vụ này, chúng tôi đề xuất một phương pháp phân tích dựa trên mô phỏng có thể cho ra phân phối số chặng, số chặng trung bình và khả năng kết nối của mạng AHWN đa chặng dưới các ràng buộc bảo mật. Những đóng góp chính của bài báo này có thể được tóm tắt như sau:

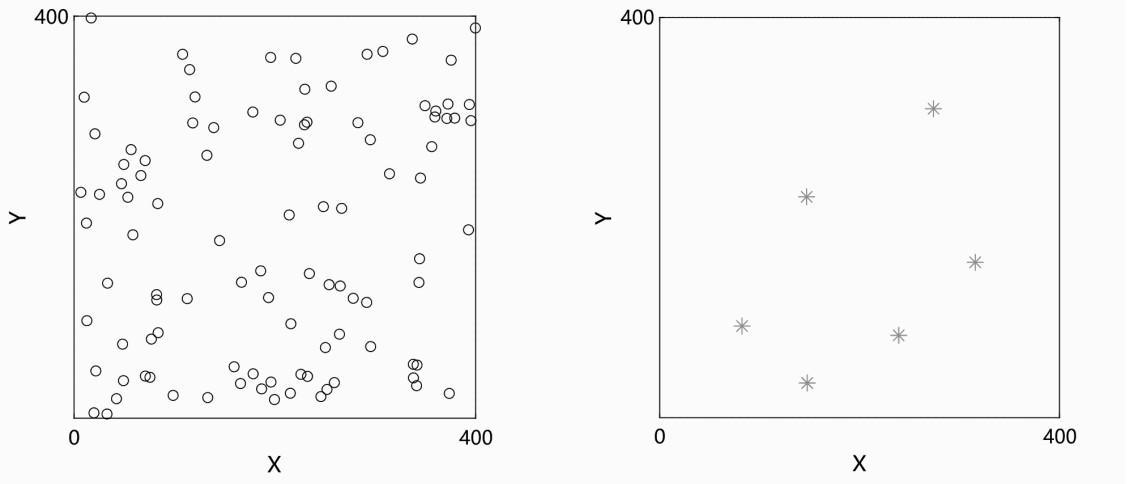
Khác với các công trình trước đây chỉ xét đến tính kết nối bảo mật (Zheng et al., 2022) hoặc số chặng (Ibrahim et al., 2021), (Li et al., 2022) của các đường truyền đa chặng hoặc nghiên cứu cả hai thông số này (Dung et al., 2018) mà không tính đến vấn đề bảo mật, trong bài báo này chúng tôi phân tích số chặng và tính

kết nối của đường đường dẫn đa chặng giữa hai nút hợp pháp bất kỳ dưới sự hiện của nhiều nút nghe lén phân bố ngẫu nhiên trong mạng.

Chúng tôi sử dụng đồ thị truyền thông bảo mật để mô hình hóa mạng AHWN có xét đến bảo mật với vị trí ngẫu nhiên của nút hợp pháp và nút nghe lén và fading kênh thay đổi. Sau đó, chúng tôi đề xuất một phương pháp để phân tích kỹ lưỡng đặc tính của số chặng và khả năng kết nối của mạng AHWN này dưới tác động của nhiều yếu tố khác nhau như chế độ hoạt động thông đồng của nút nghe lén, điều kiện kênh (mức độ nghiêm trọng của fading biên độ tín hiệu), giao thức định tuyến và mật độ nút hợp pháp và nút nghe lén.

Bảng 1. Đặc điểm chính của công trình trong bài báo này và các công trình nghiên cứu đã được công bố của các tác giả khác.

Công trình nghiên cứu	Đặc điểm				
	Có xem xét tính bảo mật?	Có phân tích tính kết nối?	Có phân tích số chặng trung bình?	Mô hình kênh truyền	Chế độ hoạt động của nút nghe lén
(Zheng et al., 2022)	Có	Có	Không	Rayleigh	Không thông đồng
(Ibrahim et al., 2021),	Có	Có	Không	Không gian tự do	Không thông đồng
(Li et al., 2022)	Không	Không	Có	Không gian tự do	–
(Dung et al., 2018)	Không	Có	Có	Nakagami	–
Bài báo này	Có	Có	Có	Nakagami	Thông đồng



(a) Nút hợp pháp, $\rho_l = 100/400^2 = 6{,}25\times10^{-4}$ nút/m^2. (b) Nút nghe lén, $\rho_e = 6/400^2 = 3{,}75\times10^{-5}$ nút/m^2.

Hình 2. Vị trí ngẫu nhiên của nút hợp pháp và nút nghe lén theo phân phối Poisson với mật độ nút khác nhau.

Chúng tôi cung cấp các đặc điểm riêng biệt của số chặng và khả năng kết nối cũng như mối quan hệ giữa chúng trong kịch bản đánh giá khác nhau để tìm ra một số thông tin mới và có

giá trị cho việc thiết kế và đánh giá mạng tùy biến đa chặng có xét đến bảo mật.

Để làm rõ sự khác biệt giữa công trình nghiên cứu của chúng tôi trong bài báo này và các công trình nghiên cứu đã được công bố của các tác giả khác, chúng tôi cung cấp tóm tắt các đặc điểm chính của các công trình nghiên cứu này trong Bảng 1.

Phần còn lại của bài báo này được tổ chức như sau. Mục 3 mô tả mô hình hệ thống, bao gồm phân phối nút, kênh không dây và kết nối an toàn được sử dụng trong bài báo này. Mục 4 trình bày phương pháp phân tích dựa trên mô phỏng được đề xuất để phân tích số lượng hop và đặc điểm kết nối của đường truyền đa chặng giữa hai nút hợp lệ ngẫu nhiên trong mạng AHWN khi có sự hiện diện của những nút nghe lén thông đồng. Mục 5 trình bày các kết quả và thảo luận về số chặng trung bình và kết nối của mạng AWHN thu được từ nhiều kịch bản mô phỏng khác nhau. Cuối cùng, một số nhận xét kết luận được đưa ra trong Mục 6.

3. MÔ HÌNH HỆ THỐNG

3.1. Phân bố nút

Tất cả các nút không dây bao gồm nút hợp pháp và nút nghe lén trong mạng AHWN được xem xét trong bài báo này được giả định được phân bố ngẫu nhiên trong một khu vực hình vuông $A = a \times a$ theo phân phối đồng đều với mật độ nút $\rho = N/A$, trong đó N là số lượng nút ($N = N_l$ đối với nút hợp pháp và $N = N_e$ đối với nút nghe lén). Từ đó xác suất một nút nằm trong một diện tích nhỏ δ là $p = \delta/A$. Sau đó, số lượng nút q nằm trong δ tuân theo phân phối nhị thức với hàm khối xác suất (pmf) được đưa ra bởi

$$P(Q=q)=\frac{N}{q!(N-q)}p^q(1-p)^{N-q}. \quad (1)$$

Theo biểu thức (1), khi $A \to \infty$ và các thông số khác không đổi, phân phối nhị thức có thể được xấp xỉ thành phân phối Poisson, tức là,

$$P(Q=q)=\frac{\eta^q}{q!}e^{-\eta}, \quad (2)$$

Trong đó $\eta = E(Q) = \rho\delta$ với $\rho = \rho_l = N_l/a^2$ và $\rho = \rho_e = N_e/a^2$ tương ứng với mật độ nút của nút hợp pháp và nút nghe lén.

Hình 2 minh họa vị trí ngẫu nhiên của nút hợp pháp và nút nghe lén trong một khu vực hình vuông có kích thước 400 m ×400 m theo phân phối Poisson với mật độ nút lần lượt là $\rho_l = 100/400^2 = 6{,}25\times10^{-4}$ nút/m^2 và $\rho_e = 6/400^2 = 3{,}75\times10^{-5}$ nút/m^2.

3.2. Kênh truyền không dây

Kết nối không dây giữa hai nút trong mạng AHWN được xem xét trong bài báo này được đặc tả bằng suy hao đường truyền quy mô lớn và fading Nakagami-*m* quy mô nhỏ. Đối với fading Nakagami-*m*, hàm mật độ xác suất (pdf) của biên độ tín hiệu U tại nút thu là

$$f_U(u)=\frac{2}{\Gamma(m)}\left(\frac{m}{\Omega}\right)^m u^{2m-1}\exp\left(-\frac{mu^2}{\Omega}\right), \quad (3)$$

Trong đó $\Gamma(\cdot)$ là hàm Gamma và $\Omega = E(u^2)$ là công suất trung bình của tín hiệu nhận được, phản ánh mức độ giãn của fading Nakagami-*m*.

Lưu ý rằng thông số tham số hình dạng m của fading Nakagami-m biểu thị mức độ nghiêm trọng của fading biên độ tín hiệu nhận được. Đặc biệt khi $m = 1$, fading Nakagami trở thành fading Rayleigh, tức là,

$$f_U(u)=\frac{2u}{\Omega}\exp\left(-\frac{u^2}{\Omega}\right), \quad (4)$$

Với $m < 1$ biểu thị mức độ fading nghiêm trọng hơn fading Rayleigh và ngược lại.

Như vậy dưới tác động chung của suy hao đường truyền quy mô lớn và fading Nakagami quy mô nhỏ, công suất nhận được P_r ($P_r = P_{rl}$ tại máy thu hợp lệ và $P_r = P_{re}$ tại máy nghe lén) đối với công suất truyền P_t cụ thể được cho bởi

$$P_r = u^2 \frac{1}{d^\alpha} P_t \,, \tag{5}$$

Trong đó d là khoảng cách giữa hai nút, α là hệ số suy hao đường truyền.

Từ biểu thức (5), sự suy giảm công suất tín hiệu có thể được tính như sau

$$\gamma(d) = \frac{P_t}{P_r} = \frac{d^\alpha}{u^2} \,, \tag{6}$$

Và được thể hiện theo đơn vị dB là

$$\begin{aligned} \gamma(d)_{\text{dB}} &= 10\log\left(\frac{P_t}{P_r}\right) \\ &= \alpha 10\log_{10}(d) - 20\log_{10}(u). \end{aligned} \tag{7}$$

Theo định nghĩa, liên kết không dây giữa nút tồn tại nếu độ suy giảm công suất tín hiệu nhận được tại máy thu nhỏ hơn hoặc bằng ngưỡng nhất định γ_{th}, đó là $\gamma \le \gamma_{\text{th}}$.

3.3. Kết nối an toàn

Khác với những công trình trước đây về mạng AHWN đa chặng với phân tích kết nối giữa các nút không có ràng buộc bảo mật, bài báo này xem xét mạng AHWN đa chặng, trong đó các giao tiếp giữa những nút hợp pháp được thực hiện dưới sự hiện diện của nhiều nút nghe lén thông đồng. Đây là trường hợp bảo mật xấu nhất khi tất cả những nút nghe lén trao đổi tin nhắn và cùng nhau xử lý các tin nhắn đã nhận của chúng tại một đơn vị xử lý trung tâm. Khi đó công suất tín hiệu nhận được kết hợp tại mỗi nút nghe lén sau khi xử lý tập trung là

$$P_{re} = \sum_{e \in G_e} u_e^2 \frac{1}{d_e^\alpha} P_t, \tag{8}$$

Trong đó G_e là tập hợp tất cả những nút nghe lén được phân bố trong mạng.

Bảo mật lớp vật lý được sử dụng như một tiêu chí để đánh giá kết nối giữa hai nút có an toàn hay không. Cụ thể, theo định nghĩa của bảo mật lớp vật lý, kết nối giữa một máy phát hợp pháp và một máy thu hợp pháp được đảm bảo an toàn nếu sự khác biệt giữa dung lượng Shannon của kênh máy phát hợp pháp-máy thu hợp pháp (hay còn gọi là kênh hợp pháp) và dung lượng Shannon của kênh nghe lén là dương (Pinto et al., 2008), tức là,

$$\log_2\left(1 + \frac{P_{rl}}{\sigma_l^2}\right) - \log_2\left(1 + \frac{P_{re}}{\sigma_e^2}\right) > 0 \,, \tag{9}$$

Trong đó σ_l^2 và σ_e^2 là độ lệch công suất nhiễu của kênh hợp pháp và kênh nghe lén.

Sau khi thực hiện một số biến đổi đại số, công thức (9) trở thành

$$\frac{P_{rl}}{P_{re}} > \beta \,, \tag{10}$$

Trong đó $\beta = \sigma_l^2 / \sigma_e^2$ là tỷ lệ bảo mật. Nói cách khác, liên kết không dây giữa hai nút hợp pháp là an toàn nếu tỷ lệ công suất nhận được tại máy thu hợp pháp P_{rl} so với công suất nhận được tại máy nghe lén P_{re} lớn hơn tỷ lệ bảo mật β.

Đường truyền đa chặng an toàn kết nối hai nút hợp pháp được tạo thành một số liên kết không dây an toàn. Việc thiết lập đường truyền đa chặng an toàn này dựa trên giao thức định tuyến luôn tiến về phía trước (GF) với hai quy tắc sau: (i) mọi nút hợp pháp đều chọn các nút hàng xóm an toàn gần đích hơn chính nó làm các nút chuyển tiếp; (ii) nếu một nút hợp pháp không thể tìm thấy một nút hàng xóm an toàn ở chặng tiếp theo gần đích hơn chính nó, thì đường truyền từ nút đó đến đích không tồn tại. Tiêu chí được sử dụng để xác định xem một nút có an toàn hay không để tham gia chuyển tiếp dữ liệu được xác định bởi biểu thức (10).

4. PHƯƠNG PHÁP PHÂN TÍCH DỰA TRÊN MÔ PHỎNG ĐƯỢC ĐỀ XUẤT

Trong phần này, chúng tôi đề xuất một phương pháp phân tích dựa trên mô phỏng có thể sử dụng các đặc điểm của mật độ nút, kênh không dây, giao thức định tuyến, chế độ hoạt động của nút nghe lén và yêu cầu bảo mật được mô tả trong Mục 3 làm tham số đầu vào.

Hình 3. Cấu trúc của phương pháp phân tích dựa trên mô phỏng được đề xuất.

Cấu trúc của phương pháp phân tích dựa trên mô phỏng được đề xuất được trình bày trong Hình 3. Nó bao gồm hai phần chính: phần đầu tiên là một thuật toán có thể cho ra trạng thái kết nối và số chặng tương ứng của đường truyền an toàn ngắn nhất giữa hai nút hợp pháp ngẫu nhiên, trong khi phần thứ hai là một thuật toán khác sử dụng kết quả đầu ra của thuật toán đầu tiên để trả về kết nối đường truyền tổng thể và số chặng trung bình. Mô tả chi tiết về hai phần này sẽ được cung cấp trong các tiểu mục sau đây.

4.1. Các hoạt động của thuật toán thứ nhất

Mục tiêu chính của thuật toán này là tìm tất cả các đường truyền đa chặng khả dụng giữa hai nút hợp pháp ngẫu nhiên và cung cấp số chặng của đường truyền ngắn nhất. Thuật toán này sử dụng vị trí của những nút hợp pháp trong đồ thị nút hợp pháp $G(\rho_l)$, vị trí của những nút nghe lén trong đồ thị nút nghe lén $G(\rho_e)$, điều kiện kênh không dây (α, m, Ω), ngưỡng suy giảm tín hiệu γ_{th}và tỷ lệ bảo mật β.

So với thuật toán tìm đường ngắn nhất của Dijkstra (Johnsonbaugh, 2009), thuật toán được đề xuất không cần đồ thị được kết nối làm thông số đầu vào. Do đó, nó hữu ích cho mạng AHWN khi mạng được kết nối có thể không phải lúc nào cũng khả dụng do tính di động của nút và chất lượng liên kết không dây thay đổi nhanh chóng. Hình 4 trình bày mã giả của thuật toán này. Quy trình hoạt động của nó sẽ được tóm tắt trong các giải thích từng bước sau đây.

- **Bước 1:** Dựa trên thông tin đồ thị nút hợp pháp $G(\rho_l)$, vị trí của những nút nghe lén trong đồ thị nút nghe lén $G(\rho_e)$, điều kiện kênh không dây (α, m, Ω), ngưỡng suy giảm tín hiệu γ_{th} và tỷ lệ bảo mật β, thuật toán này bắt đầu kiểm tra kết nối trực tiếp giữa nút nguồn và nút đích có khả dụng và an toàn hay không (tham khảo Dòng 2–5). Cụ thể, nếu độ suy giảm tín hiệu tại nút đích nhỏ hơn hoặc bằng ngưỡng, tức là $\gamma(src, dest) \leq \gamma_{th}$, nút đích có thể giao tiếp trực tiếp với nguồn. Tiếp theo, tính bảo mật của giao tiếp trực tiếp này được kiểm tra bằng cách sử dụng tiêu chí trong biểu thức (10) với công suất nhận được tại mỗi thiết bị nghe lén được đưa ra bởi biểu thức (8). Thuật toán trả ra *hop count* = 1 nếu điều kiện thiết lập liên kết và điều kiện bảo mật liên kết đều được thỏa mãn (tham khảo Dòng 8). Nếu không, nó sẽ trả về *hop count* = ∞ và dừng thực thi (tham khảo Dòng 6).

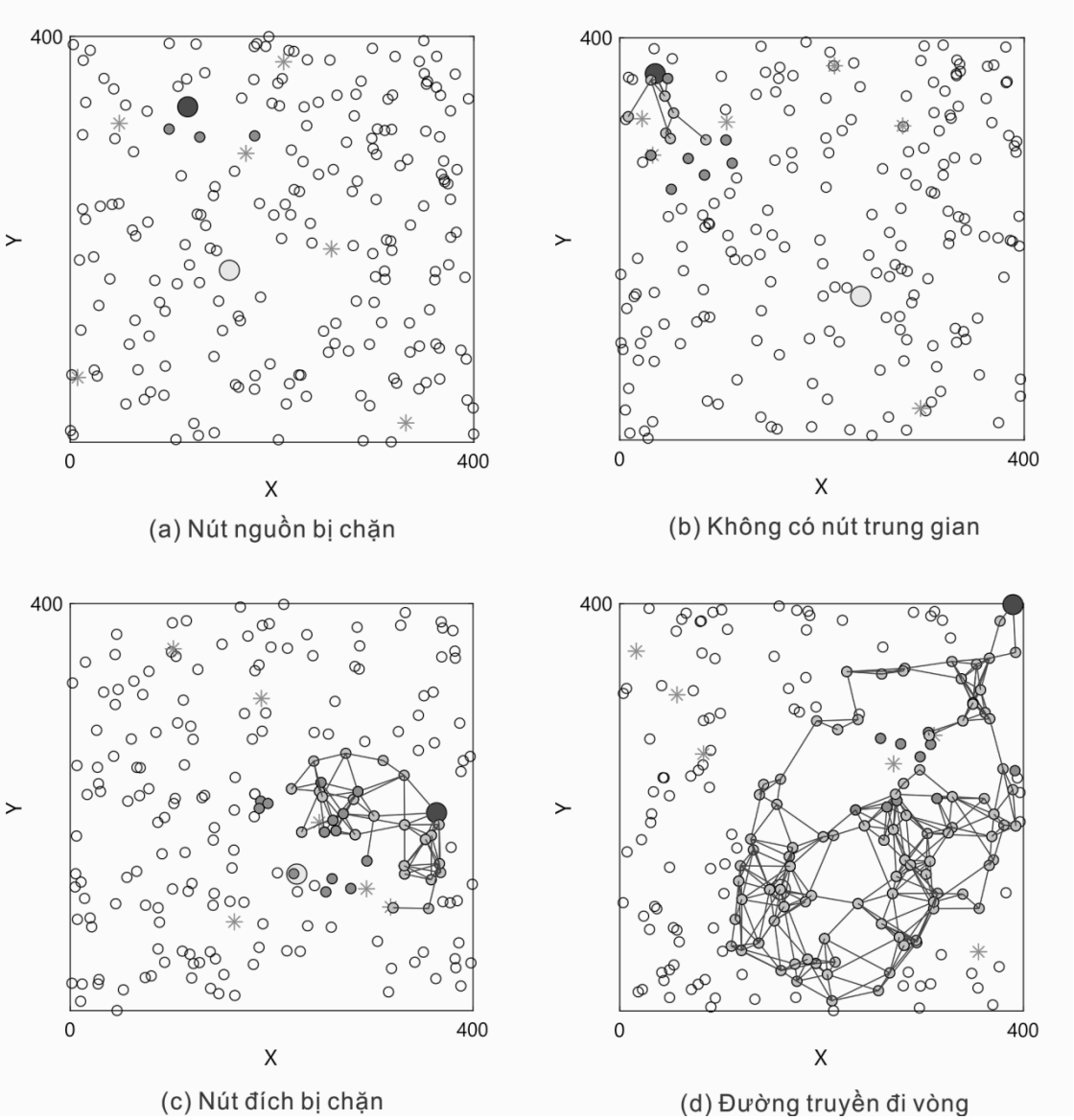
- **Bước 2:** Nếu liên kết bảo mật trực tiếp giữa nguồn và đích không tồn tại, thuật toán sẽ tìm kiếm tất cả các đường truyền đa chặng có thể giữa chúng. Khi bắt đầu quá trình này, tất cả các nút con bảo mật của nút nguồn (tức là nút nguồn sử dụng giao thức định tuyến GF để xác định các nút lân cận có liên lạc không dây bảo mật với nó) được tìm. Nếu nút nguồn không có bất kỳ nút con nào, thì rõ ràng là không thể thiết lập được đường truyền từ nút nguồn đến nút đích; do đó *hop count* = ∞ (tham khảo Dòng 10–12). Nếu không, các nút con bảo mật của nguồn được thêm vào danh sách *gonna_chk_nodes* để chúng sẽ được kiểm tra dần sau đó. Đồng thời, thông tin (ID nút, *hop count* = 1) của các nút con bảo mật này của nguồn được ghi lại trong bảng *hopcount_cache*.

```
1  SecAHWN_HC(G(ρl), G(ρe),α,m, Ω,γthv,β)
2      if γ(src, dest) ≤ γth then
3          Prl(src,dest) = Eq. (5);
4          Pre(src,eave) = Eq. (8);
5          if Prl(src,dest)/Pre(src,eave) ≤ β then
6              hop count = Inf;
7          else
8              hop count = 1;
9      else
10         Find secure child nodes of src;
11         if secure child nodes of src = ∅ then
12             hop count = Inf;
13         else
14             Add secure child nodes of src to gonna_chk_nodes list;
15             Store node IDs and hop count = 1 of these nodes into hopcount_cache table;
16             while (gonna_chk_nodes ≠ ∅)
17                 for each chk_node in gonna_chk_nodes
18                     Get the hop count of chk_node from hopcount_cache and assign to hc_chk_node;
19                     Find secure child nodes of chk_node and put into child_nodes list;
20                     for each chd_node in child_nodes
21                         if chd_node ∉ already_chk_node then
22                             Add the ID and current hop count of chd_node, i.e., hc_chk_node + 1, to already_chk_node;
23                             Add chd_node to gonna_chk_nodes;
24                         else
25                             if the current hop count of chd_node < previous one in already_chk_node then
26                                 Update hop count of chd_node in already_chk_node with the current one;
27                                 Add chd_node to gonna_chk_nodes;
28                     Remove chk_node from gonna_chk_nodes;
29                     if dest ∈ already_chk_node then
30                         hop count = hop count of from src to dest; break;
31             if dest ∉ already_chk_node then
32                 hop count = Inf;
33     return (hop count)
```

Hình 4. Mã giả của thuật toán thứ nhất để lấy số chặng và tính kết nối của đường dẫn đa chặng giữa hai nút hợp lệ ngẫu nhiên.

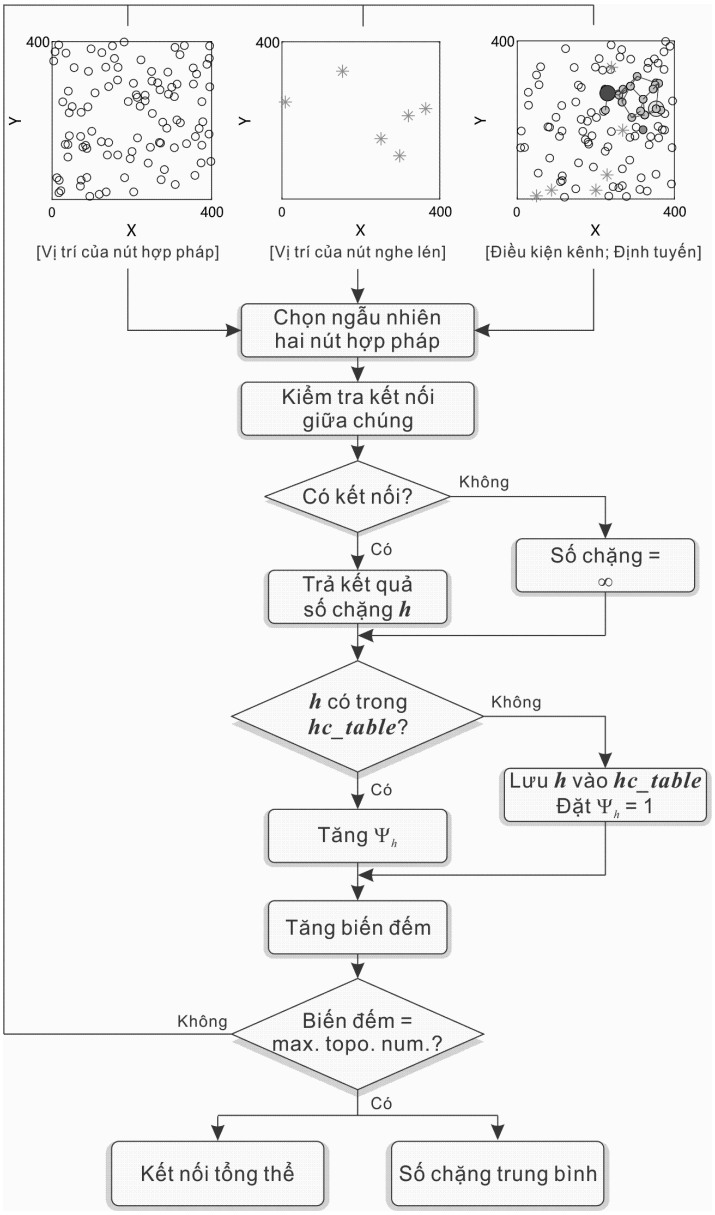
• **Bước 3:** Đối với mỗi nút con an toàn của các nút được lưu trữ trong *gonna_chk_nodes*, nếu số chặng đến nó chưa được biết, số chặng mới này sẽ được tăng thêm một, tức là *hc_chk_node* = *hc_chk_node* + 1, trong *hopcount_cache* và ID nút của nó được thêm vào *gonna_chk_nodes* (tham khảo Dòng 22–23). Trong trường hợp số chặng đến nút con an toàn này đã tồn tại trong *hopcount_cache*, nhưng số chặng mới nhất nhỏ hơn số chặng trước đó, số chặng đến nút con an toàn này sẽ được thay thế bằng giá trị nhỏ hơn và ID của nó được thêm vào danh sách *gonna_chk_nodes* (tham khảo Dòng 26–27). Sau khi một nút được kiểm tra để tìm các nút con an toàn của nó, nút đó sẽ bị xóa khỏi danh sách *gonna_chk_nodes*. Tất cả các quy trình từ Dòng 17–28 được lặp lại miễn là danh sách *gonna_chk_nodes* không trống. Nếu có thể đến nút đích trong thời gian này, thuật toán sẽ dừng thực thi và trả về số chặng của đường truyền ngắn nhất giữa nút nguồn và nút đích (tham khảo Dòng 29–30). Nếu không, thuật toán sẽ trả về số chặng = ∞.

Lưu ý rằng thuật toán này mang tính phổ quát và có thể được sử dụng để có được số chặng giữa hai nút ngẫu nhiên trong mạng AHWN đa chặng không có bảo mật bằng cách loại bỏ tác động của nút nghe lén, tức là đặt $N_e = 0$.



Hình 5. Minh họa các trạng thái kết nối giữa một nút hợp pháp nguồn và một hợp pháp đích được chọn ngẫu nhiên; a = 400 m, N_l = 200, N_e = 6, α = 3, m = 1, Ω = 1, β = 1, γ_{th} = 50 dB.

Thuật toán trên được thực hiện bằng phần mềm mô phỏng MATLAB và bốn trường hợp trạng thái kết nối có thể xảy ra được trình bày trong Hình 5. Hai nút hợp pháp ngẫu nhiên được chọn làm nút nguồn và nút đích. Chúng được biểu diễn lần lượt bằng chấm xanh và chấm vàng, trong khi những nút hợp pháp không an toàn được biểu diễn bằng chấm đỏ. Cần lưu ý rằng một nút hợp pháp đóng vai trò là nút chuyển tiếp không an toàn cho một nút hợp pháp nào đó có thể là nút chuyển tiếp an toàn cho một nút hợp pháp khác tùy thuộc vào điều kiện bảo mật của liên kết không dây giữa chúng. Hình 5(a) trình bày trường hợp nút nguồn bị chặn vì tất cả các nút lân cận của nó đều không an toàn để liên lạc. Chỉ có một nút đáp ứng được ràng buộc bảo mật, nhưng nút này không thể thiết lập bất kỳ liên kết không dây nào với các nút khác. Do đó, đường truyền từ nút nguồn đến nút đích không khả dụng. Các đường truyền đa chặng giữa nút nguồn và nút đích cũng không thể được thiết lập do không cómnút trung gian khả dụng (Hình 5(b)) hoặc nút đích bị chặn (Hình 5(c)).



Hình 6. Lưu đồ quy trình hoạt động của thuật toán thứ hai để có được kết nối tổng thể và pmf của phân phối số chặng.

Những vấn đề này là do tác động kết hợp của ràng buộc bảo mật và fading, tức là một nút an toàn để giao tiếp, nhưng nó không có liên kết không dây với các nút trước đó hoặc ngược lại. Khi một nút nguồn có thể giao tiếp với một nút đích, đường truyền giữa chúng thường có nhiều chặng (ví dụ: 11 chặng như thể hiện trong Hình 5(d)) vì nó phải đi vòng qua các nút trung gian không an toàn.

4.2. Các hoạt động của thuật toán thứ hai

Thuật toán này nhằm mục đích thu được kết nối tổng thể và số chặng trung bình bằng cách khai thác kết quả củathuật toán trước được trình bày trong Tiểu mục 4.1. Đặc biệt, thuật toán này thu thập số chặng và trạng thái kết nối của đường truyền ngắn nhất giữa hai nút hợp pháp tùy ý trong mỗi cấu trúc mạng ngẫu nhiên và đưa ra số chặng trung bình từ một số lượng lớn các cấu trúc mạng. Lưu đồ quy trình hoạt động của thuật toán này được mô tả trong Hình 6 và có thể được tóm tắt như sau:

- **Bước 1:** Đầu tiên một diện tích mạng vuông được tạo ra. Tiếp theo N_l nút hợp pháp và N_e nút nghe lén được triển khai ngẫu nhiên trong diện tích mạng này theo phân phối đồng đều.

- **Bước 2:** Sau khi hai nút hợp pháp ngẫu nhiên được chọn làm nút nguồn và nút đích, thuật toán đầu tiên sẽ kiểm tra trạng thái kết nối giữa chúng. Nếu có ít nhất một đường truyền giữa nút nguồn và nút đích, thuật toán sẽ trả về số chặng của đường truyền ngắn nhất. Đường truyền ngắn nhất là đường truyền có số chặng nhỏ nhất trong tất cả các đường truyền đa chặng khả dụng.

- **Bước 3:** Đối với mỗi cấu trúc mạng, số chặng h của đường truyền ngắn nhất và số đường truyền có số chặng là h, Ψ_h, được ghi vào một ma trận hai cột *hc_table*. Trong trường hợp nếu giá trị hop count h không tồn tại trong *hc_table* nó sẽ được thêm vào *hc_table* và Ψ_h tương ứng sẽ được đặt thành 1. Nếu không, sẽ được tăng thêm 1.

Quá trình trên được lặp lại Ψ lần cho mỗi tham số hệ thống đánh giá. Trong mỗi lần chạy, các vị trí ngẫu nhiên của nút hợp pháp và nút nghe lén được tạo mới và hai nút hợp pháp tùy ý được chọn làm nguồn và đích. Sau khi kiểm tra với Ψ cấu trúc mạng, thông tin trong ma trận *hc_table* được sử dụng để có được pmf của phân phối số chặng. Cụ thể, pmf này là hợp của các xác suất của tất cả các đường truyền h-chặng có thể có trong Ψ cấu trúc mạng. Mỗi xác suất được tính là tỷ lệ giữa số lượng cấu trúc mạng có đường truyền ngắn nhất h-chặng, Ψ_h, và tổng số cấu trúc mạng được đánh giá, Ψ. Về mặt toán học, pmf của phân phối số chặng có thể được biểu diễn như sau:

$$p_H(h) = \bigcup_{h=1}^{H_{\max}} \frac{\Psi_h}{\Psi} \tag{11}$$

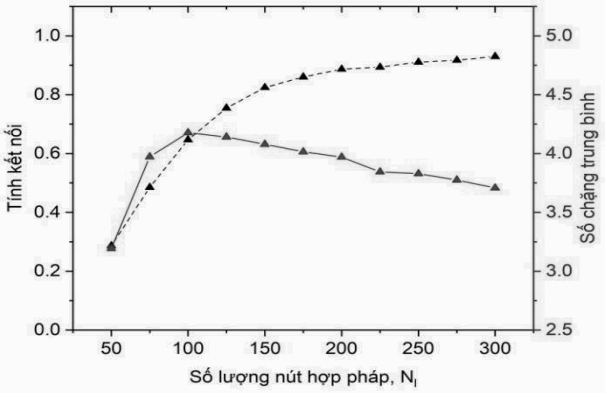
Lời bình: Xét về độ phức tạp, thuật toán thứ nhất có độ phức tạp là $O(n^2)$ do có hai vòng lặp trong quá trình lựa chọn các nút trung gian của các đường truyền đa chặng khả dụng. Trong khi đó, độ phức tạp của thuật toán thứ hai chỉ là $O(n)$ do chỉ có một vòng lặp khi lấy thông tin các giá trị trong mảng.

5. KẾT QUẢ VÀ THẢO LUẬN

Trong phần này, nhiều kết quả mô phỏng khác nhau được cung cấp để điều tra đặc tính của kết nối an toàn và số chặng trung bình trong mạng AHWN. Cụ thể, chúng tôi thực hiện phương pháp phân tích dựa trên mô phỏng được đề xuất trên chương trình mô phỏng MATLAB. Nút hợp pháp và nút lén được phân bố ngẫu nhiên trong một khu vực mạng 400 m × 400 m. Trong các tiểu mục sau, chúng tôi đưa ra nhiều kịch bản đánh giá khác nhau để nghiên cứu toàn diện số chặng và đặc tính kết nối của đường truyền đa chặng trong mạng AHWN.

5.1. Tác động của mật độ nút hợp pháp

Hình 7 minh họa tính kết nối và số chặng trung bình của đường truyền ngắn nhất giữa hai nút hợp pháp ngẫu nhiên thay đổi theo số lượng nút hợp pháp N_l. Chúng tôi tăng N_l từ 50 lên 300 để đặc trưng cho mật độ nút hợp pháp thưa thớt, vừa phải và dày đặc. Các tham số khác được đặt như sau: số lượng nút nghe lén $N_e = 5$, hệ số suy hao đường truyền $\alpha = 3$, mức độ giãn của đường truyền fading Nakagami $\Omega = 4$, ngưỡng bảo mật $\beta = 1$, ngưỡng suy giảm tín hiệu $\gamma_{th} = 50$ dB.

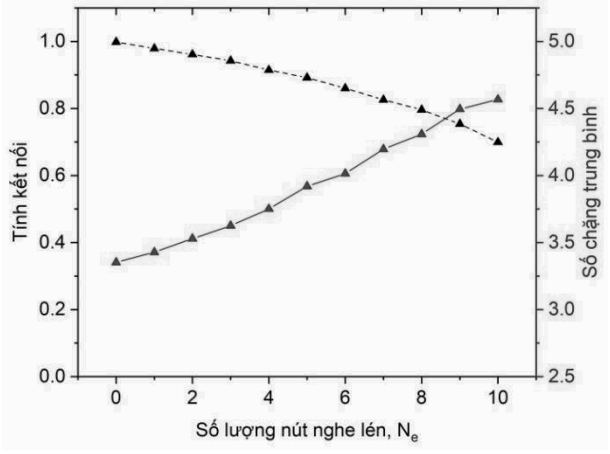


Hình 7. Tính kết nối và số chặng trung bình của đường truyền ngắn nhất giữa hai nút hợp pháp ngẫu nhiên thay đổi theo số lượng nút hợp pháp N_l. $a = 400$ m, $N_e = 6$, $\alpha = 3$, $m = 1$, $\Omega = 4$, $\beta = 1$, $\gamma_{th} = 50$ dB.

Như quan sát từ Hình 7, tính kết nối của đường truyền đa chặng tăng nhanh khi N_l tăng từ 50 đến 175 và sau đó tăng chậm trong phạm vi còn lại của N_l, đạt giá trị lớn nhất bằng 0,93 khi $N_l = 300$. Trong khi đó số chặng trung bình có giá trị thấp nhất bằng 3,19 khi $N_l = 50$ do mật độ nút hợp pháp quá thấp để có được đường truyền dài. Số chặng trung bình đạt giá trị tối đa bằng 4,18 khi $N_l = 50$ và sau đó giảm dần khi N_l tiếp tục tăng do mật độ nút hợp pháp ngày càng lớn để tạo thành những đường truyền ngắn hơn.

5.2. Tác động của mật độ nút nghe lén

Hình 8 mô tả tính kết nối và số chặng trung bình của đường truyền ngắn nhất giữa hai nút hợp pháp ngẫu nhiên so với số lượng nút nghe lén N_e. Chúng tôi thay đổi N_e từ 0 đến 10. Lưu ý rằng $N_e = 0$ tương ứng với trường hợp truyền thông không có mối đe dọa về bảo mật (Dung et al., 2018).

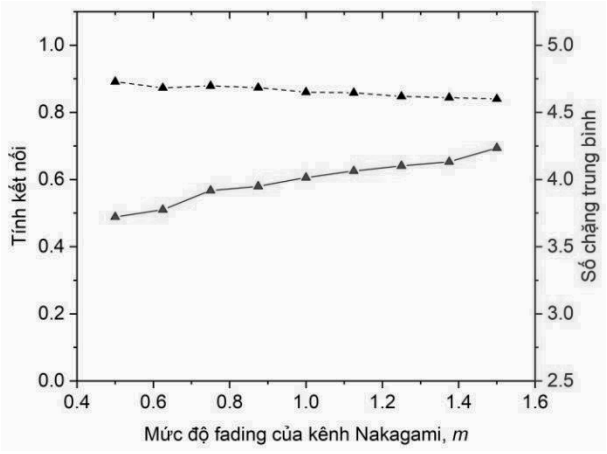


Hình 8. Tính kết nối và số chặng trung bình của đường truyền ngắn nhất giữa hai nút hợp pháp thay đổi theo số lượng nút nghe lén N_e. a = 400 m, $N_l = 175$, $\alpha = 3$, $m = 1$, $\Omega = 4$, $\beta = 1$, $\gamma_{th} = 50$ dB.

Từ Hình 8, chúng ta có thể thấy khi không có nút nghe lén trong mạng AHWN, gần như luôn có đường truyền giữa hai nút nguồn và đích hợp pháp, đó là tính kết nối ≈ 1. Khi số lượng nút nghe lén tăng, khả năng không thiết lập được các đường truyền đa chặng cũng tăng do sự gia tăng số lượng các nút trung gian không an toàn không được phép tạo thành các đường truyền này. Cụ thể là tính kết nối giảm còn 0.7 khi $N_e = 10$, giảm 30% so với trường hợp $N_e = 0$. Đồng thời, đường truyền thông tin phải dài hơn do phải đi vòng để tránh các nút trung gian không an toàn, làm cho số chặng trung bình tăng từ 3.35 lên 4.57 khi N_e tăng từ 0 đến 10.

5.3. Tác động của mức độ fading của kênh Nakagami-*m*

Hình 9 cho thấy tính kết nối và số chặng trung bình của đường truyền ngắn nhất giữa hai nút hợp pháp thay đổi theo mức độ fading m của kênh truyền Nakagami. Thông số hình dạng m của phân bố Nakagami thay đổi từ 0.5 đến 1.5 để phản ánh mức độ fading nghiêm trọng hơn hay ít nghiêm trọng hơn so với kênh truyền Rayleigh.



Hình 9. Tính kết nối và số chặng trung bình của đường truyền ngắn nhất giữa hai nút hợp pháp thay đổi theo mức độ fading m của kênh Nakagami. a = 400 m, $N_l = 175$, $N_e = 6$, $\alpha = 3$, $\Omega = 4$, $\beta = 1$, $\gamma_{th} = 50$ dB.

Chúng ta có thể thấy trong Hình 9 là khi m tăng từ 0.5 lên 1.5, tính kết nối của đường truyền đa chặng giảm nhẹ, từ 0.89 xuống 0.84. Trong khi đó, số chặng trung bình tăng khá nhiều, từ 3.72 lên 4.24. Đặc điểm này xuất hiện do việc tăng m làm cho fading quy mô nhỏ bớt nghiêm trọng hơn. Nói cách khác, ảnh hưởng của suy hao đường truyền quy mô lớn trở nên chiếm ưu thế hơn. Từ đó xác suất có đường

truyền dài trở nên lớn hơn trong khi xác suất có đường truyền vừa và ngắn nhỏ đi. Ngoài ra, tác động của mức độ fading của kênh Nakagami-*m* không ảnh hưởng nhiều đến tính kết nối và số chặng trung bình so với tác động của mật độ nút hợp pháp và nút nghe lén.

6. KẾT LUẬN

Ý tưởng trong bài báo này đến từ việc tìm hiểu cách mối quan hệ độc lập giữa điều kiện thiết lập kết nối và điều kiện bảo mật của kết nối ảnh hưởng đến số chặng và đặc điểm kết nối của đường truyền đa chặng giữa hai nút hợp lệ ngẫu nhiên trong mạng AHWN. Để có câu trả lời cho vấn đề này, chúng tôi đã đề xuất một phương pháp phân tích dựa trên mô phỏng lấy thông tin về vị trí của nút hợp lệ và nút nghe lén, điều kiện kênh không dây và chế độ hoạt động của nút nghe lén làm đầu vào. Dựa trên kết quả thử nghiệm từ nhiều kịch bản đánh giá khác nhau, một số kết luận quan trọng có thể được rút ra như sau:

- Việc tiếp tục tăng mật độ nút hợp pháp không cải thiện đáng kể chất lượng của đường truyền đa chặng. Ngoài ra, mật độ nút hợp pháp cao chỉ giúp giảm thêm số chặng trung bình của đường truyền đa chặng nhưng không làm tăng tính kết nối của đường truyền đa chặng do sự hiện diện của các nút nghe lén.

- Việc có càng nhiều nút nghe lén hơn trong mạng dẫn đến tính kết nối của đường truyền đa chặng liên tục giảm và làm số chặng trung bình liên tục tăng, khác với trường hợp đạt đến giá trị bão hòa của tính kết nối khi tăng số lượng nút hợp pháp.

- Tác động của mức độ fading của kênh Nakagami-m đến tính kết nối và số chặng trung bình có mức độ thấp hơn so với tác động của mật độ nút hợp pháp và nút nghe lén.

TÀI LIỆU THAM KHẢO

Agarkar, P. T., Chawan, M. D., P. T. Karule, &P. R. Hajare. (2020). A comprehensive survey onrouting schemes and challenges in wireless sensor networks (WSN). *International Journal of Computer Networks and Applications (IJCNA) 7*(6), 193–207.

Chen, G., Coon, J. P.,&Tajbakhsh, S. E. (2018). Secure routing formultihop ad hoc networks with inhomogeneous eavesdropper clusters. *IEEE Transactions on Vehicular Technology 67*(11), 10660 – 10670.

Dung, L. T., & Choi, S. G. (2018). Simulation modeling and analysis of the hop count distribution in cognitive radio ad-hoc networks with beamforming. *Simulation Modelling Practice and Theory 84*, 1–18.

Ibrahim, M., & HamoudaW. (2021). Performance analysis of minimum hop count-based routing techniques in millimeter wave networks: A stochastic geometry approach. *IEEE Transactions on Communications 69*(12), 8304 – 8318.

Johnsonbaugh, R. (2009). Discrete Mathematics. *Pearson Education*.

Li, S., Hu, X., Jiang, T., ZhangR., Yang, L., & Hu H. (2022). Hop Count Distribution for Minimum Hop-Count Routing in Finite Ad Hoc Networks. *IEEE Transactions on Wireless Communications 21*(7), 5317 – 5332.

Lu, J., He D.,&Wang, Z. (2022). Secure routing in multihop ad-hoc networks with SRR-based reinforcement learning. *IEEE Wireless Communications Letters 11*(2), 362 – 366.

Pinto, P. C., Barros, J., & Win,M.Z. (2008). Physical-layer security in stochastic wirelessnetworks. *Proceedings of 11th IEEE ICCS 2008*, 974–979.

Pramitarini, Y., Perdana, R., Shim, K.,&An, B. (2024). Exploiting secure multi-hop transmissions with NOMA networks: Performance analysis. *Proceedings of IEEE ICAIIC 2024*, 359 – 364.

Rekha, & Gupta, R. (2020). Cluster head election in wireless sensor network: A comprehensive study and future directions. *International Journal of*

Computer Networks and Applications (IJCNA) 7(6), 178–192.

Sarkar, S. K., Basavaraju, T., & PuttamadappaC. (2013). Ad Hoc Mobile Wireless Networks: Principles, Protocols, and Applications. *CRC Press*.

Shannon, C.E. (1949). Communication theory of secrecy system. *The Bell System Technical Journal 28*(4), 656–71.

Wang, H. M., Zhang, Y., Zhang, X., & Li Z. (2020). Secrecy and covert communications against UAV surveillance via multi-hop networks. *IEEE Transactions on Communications 68*(1), 389 – 401.

Wyner, A. D. (1975). The wire-tap channel. *The Bell System Technical Journal 54*(8), 1355–1387.

Xiao, H., Xiaolan L., ZhangQ.,& ChronopoulosA. T. (2021) Connectivity probability analysis for freeway vehicle scenarios in vehicular networks. *Wireless Networks 17*, 465–474.

Zheng, T.X., Chen, X., Wang, C., Wong, K.-K., & Yuan J. (2022). Physical layer security in large-scale random multiple access wireless sensor networks: A stochastic geometry approach. *IEEE Transactions on Communications 70*(6), 4038 – 4051.

ANALYSIS OF SECURE CONNECTIVITY AND HOP COUNT OF AD-HOC NETWORKS WITH COLLUDING EAVESDROPPERS

Le The Dung[1*], Le Ngoc Dung[2]

[1]*FPT University Ho Chi Minh City*
[2] *Dong Nai Technology University*
*Corresponding author: Le The Dung, *dunglt96@fe.edu.vn*

GENERAL INFORMATION

Received date: 11/08/2024

Revised date: 13/09/2024

Accepted date: 30/09/2024

KEYWORD

Colluding eavesdropper;

Hop count;

Multi-hop ad-hoc wireless network;

Secure connectivity.

ABSTRACT

Connectivity and hop count are two important properties of multi-hop wireless ad-hoc networks (AHWN). When considering security, establishing a secure multi-hop path is challenging because an intermediate node that is connected to the previous nodes may not be safe enough to receive data from those nodes and vice versa. To analyze this property, we use stochastic geometry graphs to model the AHWN with multiple eavesdroppers in the worst-case scenario where the eavesdroppers collude with each other. Next, we propose a simulation-based analysis method to obtain the path connectivity, hop count distribution, and average hop count under various evaluation scenarios. The simulation results show that the connectivity reaches a saturated value of 0.93 when the legitimate node density is $1{,}88\times10^{-3}$ node/m^2. In addition, the shape parameter of the Nakagami fading channel only reduces the connectivity by 5.62% compared to 29.96% of the eavesdropper density. The results of this paper provide valuable information on the design and evaluation of security-aware multi-hop AHWNs.