BỘ THÔNG TIN VÀ TRUYỀN THÔNG

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

VŨ LÊ QUỲNH GIANG

NGHIÊN CỨU BẢO MẬT LỚP VẬT LÝ CHO HỆ THỐNG MASSIVE MIMO VỚI KÊNH PHA ĐINH RICE

Chuyên ngành: Kỹ thuật Viễn thông

Mã số: 9.52.02.08

TÓM TẮT LUẬN ÁN TIẾN SĨ KỸ THUẬT

Hà Nội - 2023

CÔNG TRÌNH ĐƯỢC HOÀN THÀNH TẠI
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG - BỘ THÔNG TIN VÀ TRUYỀN THÔNG.

Người hướng dẫn khoa học: 1. TS. Trương Trung Kiên

2. PGS.TS Lê Nhật Thăng

Phản biện 1:

Phản biện 2:

Phản biện 3:

Luận án sẽ được bảo vệ trước Hội đồng đánh giá luận án cấp Học viện theo Quyết định số ... ngày ... tháng ... năm ... của Giám đốc Học viện Công Nghệ Bưu chính Viễn thông, họp tại Học viện Công Nghệ Bưu chính Viễn thông vào hồi ... giờ ... ngày ..... tháng ... năm ...

Có thể tìm hiểu luận án tại:
- Thư viện Quốc gia Việt Nam
- Thư viện Công Nghệ Bưu chính Viễn thông.

DANH MỤC CÁC CÔNG TRÌNH SỬ DỤNG TRONG LUẬN ÁN

1. **J1: Vũ Lê Quỳnh Giang**, Trương Trung Kiên, "Dung lượng bảo mật của hệ thống MIMO cỡ rất lớn khi có thiết bị nghe lén thụ động," *Journal of Research and Development on Information and Communication Technology,* V-3 no. 40, pp. 1-10, Dec. 2018.
2. **C1: Vũ Lê Quỳnh Giang**, Trương Trung Kiên,"Nghiên cứu tính tương quan không gian cho mô hình kênh MIMO cỡ rất lớn," *National Conference on Electronics, Communications and Information Technology (REV-ECIT),* pp. 29–37, Dec. 2019.
3. **C2: Giang. Q. L Vu**, T. Le Nhat and K. T. Truong, "Physical Layer Security of Massive MIMO Spatially-uncorrelated Rician Channels," *2021 International Conference on Advanced Technologies for Communications (ATC)*, 2021, pp. 22-27.
4. **C3: Giang. Q. L. Vu**, H. Tran and K. T. Truong, "Jammer Detection by Random Pilots in Massive MIMO Spatially-uncorrelated Rician Channels," *2021 8th NAFOSTED Conference on Information and Computer Science (NICS)*, 2021, pp. 440-445.
5. **J2: Giang. Q. L. Vu**,, Trung-Kien Truong, Trong- Minh Hoang , "A Study on Physical Layer Security of Massive MIMO in the Rician Fading Channel Consideration,"Journal of Military Science and Technology - Academy of Military Science and Technology , 2022, pp. 21-29
6. **J3: G. Q. L. Vu** , H. Tran, T. V. Chien, L. N. Thang and K. T. Truong, "Attacker Detection in Massive MIMO Systems Over Spatially Uncorrelated Rician Fading Channels," in IEEE Access, vol. 10, 2022, pp. 125489-125498 (ISI Q1)

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN CỦA LUẬN ÁN

A. Một số kết quả đạt được của luận án

1. Trình bày những kiến thức chung về bảo mật lớp vật lý trong mạng thông tin di động nói chung và mạng Massive MIMO nói riêng, các giải pháp đảm bảo an toàn thông tin;

2. Thiết lập biểu thức giải tích đánh giá dung lượng bảo mật của hệ thống Massive MIMO kênh pha-đinh Rice.

3. Đề xuất một số giải pháp phát hiện nhiễu hoa tiêu gây ra bởi thiết bị bất hợp pháp trong hệ thống thông tin vô tuyến Massive MIMO kênh pha-đinh Rice.

4. Đề xuất những phương pháp nâng cao xác suất phát hiện và giảm thiểu báo động giả cho hệ thống Massive MIMO dựa trên phân tập thời gian.

B. Hướng phát triển tiếp theo Kế thừa kết quả của luận án và các nghiên cứu có liên quan nghiên cứu sinh thấy rằng có thể phát triển vấn đề nghiên cứu theo các hướng như sau:

- Nghiên cứu ảnh hưởng của một hoặc nhiều bộ thiết bị gây nhiễu hoạt động trong hệ thống Massive MIMO với kênh truyền pha-đinh Rice tương quan không gian.

- Nghiên cứu ảnh hưởng của tương quan không gian trong mạng Massive MIMO khi có thiết bị nghe lén.

- Nghiên cứu ảnh hưởng của tương quan không gian trong mạng Massive MIMO khi có thiết bịTtấn công chủ động .

- Nghiên cứu phương pháp phát hiện các thiết bị không được cấp phép trong hệ thống Massive MIMO tương quan không gian đa người dùng.

MỞ ĐẦU

1. Hoàn cảnh nghiên cứu

Hiện nay các thiết bị di động cùng với yêu cầu về băng thông đường truyền ngày càng cao. Dự kiến đăng ký 5G được dự báo sẽ đạt 4,4 tỷ vào năm 2027 chiếm một nửa số thuê bao di động. Các công nghệ đang sử dụng không thể đáp ứng được nhu cầu kết nối cho một số lượng lớn thiết bị đa dạng về chủng loại cũng như công nghệ đa truy cập. Để vượt qua được rào cản công nghệ này, mạng thông tin di động thế hệ thứ 5, 6 và những thế hệ tiếp theo được mong đợi có thể giải quyết vấn đề này. Tuy nhiên, mạng thông tin di động luôn phải đối mặt với nhiều thách thức kỹ thuật do đặc điểm của kênh truyền vật lý. Những vấn đề bảo mật khác phát sinh từ các đặc điểm của môi trường lan truyền sóng vô tuyến như pha-đinh đa đường, suy hao đường truyền và nhiễu. Kết quả là những thiết bị bất hợp pháp có thể trích xuất thông tin truyền thông, có thể gây suy giảm hiệu năng truyền nhận thông tin hoặc gián đoạn hoạt động truyền tin của hệ thống. Để tăng tốc độ dữ liệu có thể sử dụng nhiều ăng-ten tại phía phát/thu hoặc sử dụng phương pháp định hướng búp sóng hoặc tăng băng thông tín hiệu. Kỹ thuật thông tin MIMO sử dụng rất nhiều ăng-ten ở trạm gốc (thường được biết đến với tên tiếng Anh là "Massive MIMO") là một trong các kỹ thuật truyền dẫn vô tuyến ứng cử quan trọng cho mạng 5G, 6G. Luận án này tập trung vào vấn đề bảo mật lớp vật lý trong mạng thông tin di động nói chung và hệ thống Massive MIMO trong điều kiện kênh truyền pha đinh Rice nói riêng qua việc đánh giá dung lượng bảo mật của hệ thống từ đó đưa ra giải pháp đảm bảo an toàn thông tin.

2. Mục đích nghiên cứu

Mục đích của luận án là đưa ra một số kết quả mới về : Các biện pháp bảo mật lớp vật lý của mạng Massive MIMO và cách phát hiện nhiễu hoa tiêu, tính xác suất phát hiện thiết bị không cấp phép cho các bài toán về bảo mật lớp vật lý đối với các thiết bị nghe lén thụ động và tấn công chủ động.

3. Đối tượng và phạm vi nghiên cứu

3.1. Đối tượng nghiên cứu.

Luận án nghiên cứu các bài toán bảo mật tại lớp vật lý, nghe lén thụ động và tấn công chủ động trong hệ thống Massive MIMO.Nghiên cứu ảnh hưởng đến dung lượng bảo mật của hệ thống khi có một thiết bị nghe lén thụ động trong

điều kiện pha đinh Rice. Nghiên cứu phương pháp phát hiện nhiễu hoa tiêu, xây dựng thuật toán toán phát hiện, tính xác suất phát hiện đúng và xác suất báo động giả khi có thiết bị chủ động tấn công

3.2. Phạm vi nghiên cứu.

Luận án tập trung nghiên cứu các bài toán sau:

- Bài toán về ảnh hưởng của thiết bị nghe lén thụ động của hệ thống Massive MIMO không tương quan trong điều kiện kênh truyền pha-đinh Rice.

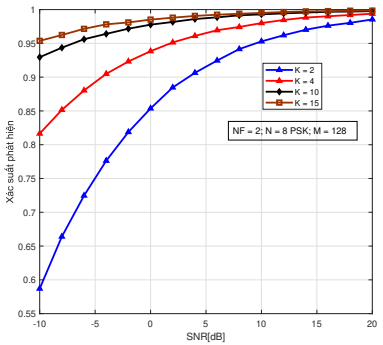
- Bài toán về xây dựng thuật toán phát hiện thiết bị tấn công cho hệ thống Massive MIMO trong điều kiện kênh truyền pha đinh Rice khi sử dụng khóa PSK ở kênh đường lên.

- Kỹ thuật nâng cao bảo mật cho hệ thống Massive MIMO trong điều kiện kênh truyền pha đinh Rice qua nhiễu hoa tiêu và phân tập thời gian.

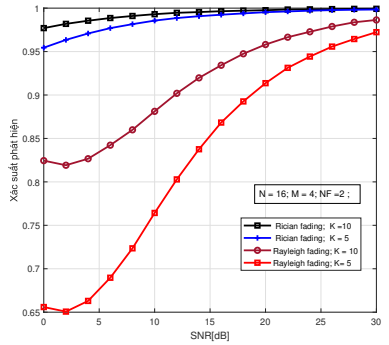
4. Đóng góp của luận án

- Đánh giá về khả năng bảo mật trong hệ mạng Massive MIMO trong điều kiện kênh truyền pha-đinh Rice khi xuất hiện thiết bị nghe lén. - Xây dựng thuật toán phát hiện, khu vực phát hiện và tính toán xác suất phát hiện và xác suất báo động giả có thiết bị gây nhiễu chủ động. - Đề xuất giải pháp phát nâng cao xác suất phát hiện nhiễu hoa tiêu dựa trên phân tập thời gian.

5. Bố cục luận án Luận án bao gồm: Mở đầu; Kết luận và hướng phát triển của luận án; Danh mục các công trình công bố và Tài liệu tham khảo. Luận án chia thành 4 chương như trình bày tiếp theo.

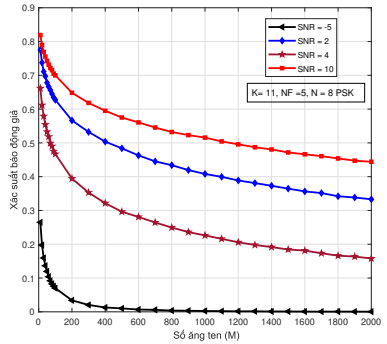


((a)) số lượng hoa tiêu là $2, 4, 10, 15$, số khung truyền dẫn NF $= 2$, số PSK $= 8$, M $= 128$, $P_B = 24$ dBm, $P_J = 24$ dBm, and $\Phi_B = 0$ rad và $\Phi_J = 0.1$ rad

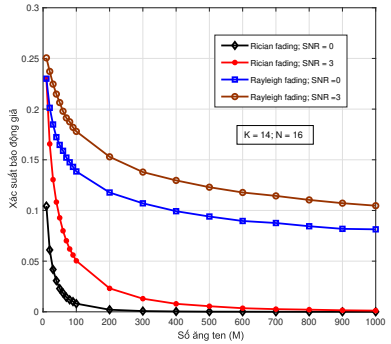


((b)) Xác suất phát hiện của kênh Rayleigh pha đinh và kênh truyền pha đinh Rice tỉ lệ với SNR, $M = 4$, K $= 5; 10$, NF $= 2$, N $= 16$ PSK, $P_B = P_J = 24$ dBm,$\Phi_B = \Phi_J = 0.1$ rad.

Hình 4.1: Xác suất phát hiện của kênh Rayleigh pha đinh/ và kênh truyền pha đinh Rice



((a)) Xác suất báo động giả theo số ăng-ten và SNR là -5, 2, 4, 10, số hoa tiêu K $= 11$, số khung truyền dẫn vô tuyến NF $= 5$, PSK $= 8$, $\Phi_J = 0$ [rad], $\Phi_B = 0.1$ [rad].



((b)) So sánh xác suất báo động giả của kênh Rayleigh và kênh Rice tỉ lệ với số ăng ten khi SNR $\in \{0, 3\}$ [dB] , K $= 14$, NF $= 8$, $N = 16$, $\Phi_J = 0.1$ [rad], $\Phi_B = 0.1$ [rad].

là phải chọn 2 khung truyền vô tuyến liên tiếp. Bước 3: Với mỗi cặp hoa tiêu huấn luyện khung vô tuyến $\mathcal{K}_k \in \mathcal{F}_l$ và khung truyền $\mathcal{K}_q \in \mathcal{F}_u$ Bước 4: Dựa trên phần lớn kết quả phát hiện của các cặp đã chọn, trạm gốc xác định sự hiện diện của thiết bị gây nhiễu. Bước 5: Trạm gốc quyết định rằng xuất hiện các thiết bị tấn công qua một khoảng thời gian dựa trên phần lớn kết quả phát hiện ngẫu nhiên của các cặp được chọn.

4.2.5 Phân tích xác suất phát hiện

Trong phần này, chúng ta phân tích xác suất phát hiện của phương pháp đề xuất khi số lượng ăng-ten M tại trạm gốc rất lớn để có được những có những nghiên cứu sâu về tác động của mô hình kênh. Chia cả hai phần của công thức. (4.19) cho $a_{k,q}$, khác 0, chúng ta nhận được:

$$\tilde{z}_{k,q} = s_{\mathrm{B}} + \frac{n_{k,q}}{a_{k,q}}. \tag{4.19}$$

Bán kính của mỗi vùng phát hiện được đề xuất tỷ lệ với $D_{\mathrm{Ri},0,k,q} = \sigma^2_{\mathrm{Ri},0,k,q}/|a_{\mathrm{Ri},0,k,q}|^2$.

4.3 Kết quả mô phỏng

Phần này cung cấp một số kết quả mô phỏng và tính toán số để kiểm chứng các kết quả phân tích giải tích Hình. 4.2(b) so sánh xác suất báo động giả của hệ thống trên các kênh pha-đinh Rayleigh và các kênh pha-đinh Rice với $\mathrm{SNR} = 0;3$ [dB], $\mathrm{K} = 14$, $\mathrm{NF} = 8$, $\mathrm{N} = 16$, $\mathrm{P_B} = 24$ [dBm], $\mathrm{P_J} = 24$ [dBm], góc tới AoA của người dùng hợp pháp $\Phi_{\mathrm{B}} = 0.1$ [rad] và góc tới AoA $\Phi_{\mathrm{J}} = 0.1$ [rad] của thiết bị gây nhiễu tỉ lệ với số ăng-ten tại trạm gốc. Hình 4.1(a) hiển thị xác suất phát hiện cho các giá trị khác nhau của SNR khi trạm gốc được trang bị 128 ăng ten. Công suất phát là $\mathrm{P_B} = \mathrm{P_J} = 24$ dBm . Chúng tôi xem xét các số lượng hoa tiêu thử nghiệm khác nhau $\mathrm{K} \in \{2, 4, 10, 15\}$. Sơ đồ điều chế được mô phỏng là 8 -PSK. Trong khi đó, Hình 4.1(b) so sánh xác suất phát hiện giữa các kênh pha-đinh Rayleigh và Rice dưới dạng một hàm của SNR với $\mathrm{M} = 4$, $\mathrm{K} \in \{5; 10\}$, $\mathrm{NF} = 2$, $\mathrm{N} = 16$, $\mathrm{P_B} = 24$ [dBm], $\mathrm{P_J} = 24$ [dBm], $\Phi_{\mathrm{B}} = 0,1$ [rad] và $\Phi_{\mathrm{J}} = 0,1$ [rad].

4.4 Kết luận chương

Chương 4 của luận án đã đưa ra biện pháp nâng cao độ chính xác khi phát hiện có thiết bị gây gây nhiễu chủ động trên phân tập thời gian.

Chương 1

NHỮNG VẤN ĐỀ CHUNG VỀ BẢO MẬT LỚP VẬT LÝ VÀ MẠNG THÔNG TIN DI ĐỘNG MASSIVE MIMO

Hiện nay sự bùng nổ của các thiết bị di động cùng với yêu cầu về băng thông đường truyền ngày càng cao. Các công nghệ đang sử dụng không thể đáp ứng được nhu cầu kết nối cho một số lượng lớn thiết bị đa dạng về chủng loại cũng như công nghệ truy nhập. Các nhà nghiên cứu cũng như các công ty viễn đông đã và đang bắt tay vào nghiên cứu 6G dựa trên những cải biến của công nghệ 5G như sử dụng công nghệ massive MIMO không tế bào, mảng ăng-ten bề mặt thông minh lên đến hàng ngàn ăng-ten. Việc phục vụ đồng thời nhiều thuê bao qua môi trường vô tuyến đặt ra một thách thức rất lớn trong việc bảo đảm an toàn thông tin.

1.1 Bảo mật lớp vật lý trong mạng thông tin di động

Đảm bảo an toàn thông tin là một thách thức lớn không chỉ đối với riêng mạng thông tin MIMO sử dụng rất nhiều ăng-ten ở trạm gốc mà còn đối với rất cả các mạng thông tin di động thế hệ mới Ý tưởng chính của cách tiếp cận này là tận dụng đặc điểm kênh truyền đặc biệt và số chiều không gian dư thừa có được nhờ vào việc sử dụng rất nhiều ăng-ten ở trạm gốc để chống việc nghe trộm hoặc tấn công ngay ở lớp vật lý. Những vấn đề nghiên cứu kỹ thuật bảo mật tại lớp vật lý bao gồm:

- Tận dụng đặc điểm kênh truyền đặc biệt và số chiều không gian dư thừa có được nhờ vào việc sử dụng rất nhiều ăng-ten ở trạm gốc để chống việc nghe trộm hoặc tấn công ngay ở lớp vật lý.
- Nghiên cứu dựa trên ưu điểm khác của Massive MIMO, với sự phát triển của công nghệ, các thiết bị nghe lén có thể được trang bị những biện pháp đối phó với khả năng tự bảo mật của lớp vật lý.
- Nghiên cứu kỹ thuật lựa chọn các nút chuyển giao để mạng để xác định dung lượng bảo mật.
- Nghiên cứu kỹ thuật bảo mật trong hệ thống Massive MIMO với các thành phần phần cứng không hoàn hảo.

1.2 Kênh nghe lén Gauss

Trong mô hình kênh nghe lén Gauss, thiết bị phát sẽ mã hóa bản tin thành mã, sau đó được gửi qua kênh truyền có nhiễu Gauss, phía thiết bị thu sẽ giải mã tín hiệu thu được thành bản tin, bên cạnh đó thiết bị nghe lén cũng thu được tín hiệu từ thiết bị phát và giải mã được bản tin trong môi trường kênh truyền có nhiễu Gauss tương ứng với kênh chính và kênh nghe lén.

1.3 Tham số đánh giá dung bảo mật của hệ thống thông tin di động

i)Dung lượng bảo mật của hệ thống. ii) Xác suất dung lượng bảo mật khác không. iii) Xác suất dừng bảo mật của hệ thống.

1.4 Hệ thống Massive MIMO

1.4.1 Lợi ích của hệ thống Massive MIMO

Massive MIMO là một kỹ thuật thông tin vô tuyến dựa trên ý tưởng sử dụng rất nhiều ăng-ten ở trạm gốc để phục vụ đồng thời nhiều thuê bao di động trên cùng một tài nguyên tần số. Hệ thống Massive MIMO có thể tăng công suất và đồng thời cải thiện hiệu suất năng lượng . Hệ thống Massive MIMO có thể giảm đáng kể độ trễ trong truyền thông không dây. Hệ thống Massive MIMO dựa trên luật số lớn và định hướng tia để tránh hiện tượng pha đinh, giúp đạt được độ trễ thấp mà không bị giới hạn bởi pha-đinh. Massive MIMO đơn giản hóa việc đa truy cập. Massive MIMO làm gia tăng sự can thiệp của con người tạo ra và để cố ý gây nhiễu. Cách thức để cải thiện hiệu năng của mạng thông tin di động là sử dụng nhiều ăng-ten.

1.4.2 Thách thức của hệ thống Massive MIMO

Kỹ thuật Massive MIMO được xem là một cải tiến của kỹ thuật thông tin MIMO truyền thống dựa trên nền tảng sử dụng nhiều trong thực tế Xuất phát từ bốn ưu điểm cơ bản của mạng MU-MIMO truyền thống:

- Tốc độ dữ liệu tăng lên, bởi vì càng nhiều ăng-ten.
- Nâng cao độ tin cậy, bởi vì càng nhiều ăng ten thì có đường truyền càng khác biệt tín hiệu có thể truyền qua.
- Cải thiện hiệu quả năng lượng, bởi vì các trạm gốc có thể tập trung năng lượng và hướng vào các thiết bị đầu cuối được.
- Giảm nhiễu vì trạm gốc có thể tránh được các hướng truyền vào những nơi can nhiễu.

được J đoán ra có thể khớp với các ký hiệu được truyền bởi B hay không, tức là: $s_{q,u} = s_{k,\ell}$. Chúng ta có

$$\bar{a}_{\mathrm{Ri,J},k,q} = \lim_{M\to\infty} \frac{a_{\mathrm{Ri,J},k,q}}{\sqrt{M}} \tag{4.16}$$

quan sát khi $s_{q,u} = s_{k,\ell}$, xảy ra xác suất là $1/N$, $\bar{a}_{\mathrm{Ri,J},k,q}$ là một đại lượng vô hướng với mọi k và q. Trong trường hợp này, xác suất phát hiện là $z_{k,q}$ bị ô nhiễm nằm trong vòng tròn bán kính $\bar{\sigma}_{\mathrm{Ri,J}}$ và có tâm là khóa N-PSK được chia tỷ lệ bằng $\bar{a}_{\mathrm{Ri,J},k,q}$. Ngược lại, dưới dạng $s_{q,u} \neq_{k,\ell}$, xuất hiện với xác suất $(N-1)/N$, thì $\bar{a}_{\mathrm{Ri,J},k,q}$ là một đại lượng vô hướng phức tạp. Kết quả là giá trị $z_{k,q}$ bị ô nhiễm nằm trong vòng tròn bán kính $\bar{\sigma}_{\mathrm{Ri,J}}$ và căn giữa là biểu tượng N -PSK được chia tỷ lệ bằng $|\bar{a}_{\mathrm{Ri,J},k,q}|$ và được quay một góc nhất định.

4.2.3 Không có tín hiệu gây nhiễu chủ động

Khi thiết bị đầu cuối của người dùng bất hợp pháp J không truyền tín hiệu trong cả hai pha huấn luyện, chúng ta có $\alpha_{k,\ell} = \alpha_{q,u} = 0$. Biểu thị $\sigma^2_{0,M}$ giá trị tương ứng của σ^2_M và thay thế $\alpha_{k,\ell} = \alpha_{q,u} = 0$ vào (4.14) ta có

$$a_{\mathrm{Ri},0,k,q} = \frac{1}{\sqrt{M}} \mathbf{h}^H_{\mathrm{B},q} \mathbf{h}_{\mathrm{B},k}; \quad \sigma^2_{\mathrm{Ri},0,M} = \frac{N_0}{M} \left(p_{\mathrm{B}} \|\mathbf{h}_{\mathrm{B},k}\|^2 + p_{\mathrm{B}} \|\mathbf{h}_{\mathrm{B},q}\|^2 + MN_0 \right). \tag{4.17}$$

Bằng cách sử dụng các thuộc tính của mô hình kênh pha-đinh được cung cấp trong phần trước và thực hiện một số bước tính toán, chúng ta thu được các kết quả sau:

$$\bar{a}_{\mathrm{Ri},0,k,q} = \lim_{M\to\infty} \frac{|a_{\mathrm{Ri},0,k,q}|}{\sqrt{M}} = \bar{\beta}_{\mathrm{B},k,q}; \quad \bar{\sigma}^2_{\mathrm{Ri},0} = \lim_{M\to\infty} \sigma^2_{\mathrm{Ri},0,M} = N_0 \left(2\bar{\beta}_{\mathrm{B},k,k} + N_0 \right). \tag{4.18}$$

Mặc dù cả hai kết quả thu được đều được giới hạn là $M \to \infty$, chúng cho thấy sự khác biệt. Cụ thể hơn, $\bar{a}_{\mathrm{Ri},0,k,q}$ là một hàm của các vị trí của các hoa tiêu huấn luyện, nhưng $\bar{\sigma}^2_{\mathrm{Ri},0}$ thì không phải.

4.2.4 Thuật toán phát hiện

Bước 1: Trong một số khung truyền vô tuyến liên tiếp $\mathcal{F}> = 1$, trạm gốc chọn một số cặp hoa tiêu huấn luyện khác nhau từ tập các hoa tiêu huấn luyện K. Lưu ý rằng số cặp ký hiệu huấn luyện tối đa là $K(K-1)/2$. Bước 2: Chọn 2 khung truyền vô tuyến ngẫu nhiên $\mathcal{F}_l$, $\mathcal{F}_u$ trong $\mathcal{F}$. Chú ý rằng không cần thiết

Mặc dù (4.9) có biểu thức tương tự như những gì được đề xuất trong. Trước hết định nghĩa $s_{\mathrm{B}} = s^*_{\mathrm{B},q,u} s_{\mathrm{B},k,\ell}$, và s_{B} là một tín hiệu N-PSK bởi vì cả $s^*_{\mathrm{B},q,u}$ và $s_{\mathrm{B},k,\ell}$ đều là tín hiệu N-PSK. Để thuận tiện, đặt các biến mới như sau:

$$a_{k,q} = \frac{1}{\sqrt{M}} \mathbf{f}^H_{q,u} \mathbf{f}_{k,\ell}; \quad n_{k,q} = \frac{1}{\sqrt{M}} \left(\mathbf{f}^H_{q,u} \mathbf{n}_{k,\ell} + \mathbf{n}^H_{q,u} \mathbf{f}_{k,\ell} + \mathbf{n}^H_{q,u} \mathbf{n}_{k,\ell} \right). \tag{4.10}$$

Thay (4.4) vào (4.9) và (4.10), chúng ta nhận được

$$z_{k,q} = a_{k,q} s_{\mathrm{B}} + n_{k,q}. \tag{4.11}$$

Vì rất khó để xác định phân phối chính xác của $n_{k,q}$. Để triển khai các vec tơ kênh truyền và các hoa tiêu thử nghiệm đã truyền, cả $\mathbf{f}_{q,u}$ và $\mathbf{f}_{k,\ell}$ đều được xác định rõ ràng. Dựa trên (4.9) - (4.11), chúng ta nhận thấy rằng

$$n_{k,q} = \frac{1}{\sqrt{M}} \mathbf{y}^H_{k,\ell} \mathbf{y}_{q,u} - a_{k,q} s_{\mathrm{B}}, \tag{4.12}$$

trong đó $\mathbf{y}_{k,\ell}$ và $\mathbf{y}_{q,u}$ là hai vector Gauss độc lập kích thước M với phương sai $N_0 \mathbf{I}_M$, trong đó $\mathbf{f}_{k,\ell} s_{\mathrm{B},k,\ell}$ và $\mathbf{f}_{q,u} s_{\mathrm{B},q,u}$, tương ứng. Tiếp theo sau là $\mathbf{E}[n_{k,q}] = 0$. Bởi vì $n_{k,q}$ là tổng của giá trị phức biến Gauss M, chúng ta thu được kết quả sau bằng cách áp dụng định lý giới hạn trung tâm Lyapunov

$$\lim_{M \to \infty} \frac{n_{k,q}}{\sigma_M} \xrightarrow{d} \mathcal{CN}(0,1). \tag{4.13}$$

trong đó phương sai σ^2_M được xác định như dưới và sẽ được chứng minh là hữu hạn khi M tăng lên rất lớn

$$\sigma^2_M = \frac{N_0}{M} \left(\|\mathbf{f}_{q,u}\|^2 + \|\mathbf{f}_{k,\ell}\|^2 + M N_0 \right). \tag{4.14}$$

4.2.2 Khi có tín hiệu gây nhiễu chủ động

Khi tín hiệu gây nhiễu tồn tại trong cả hai hoa tiêu huấn luyện, tức là $\alpha_{k,\ell} = \alpha_{q,u} = 1$, thay các giá trị vào (4.14) nhận được kết quả như sau: Hệ số kênh tương đương trong trường hợp này được cho là:

$$a_{\mathrm{Ri,J},k,q} = \frac{1}{\sqrt{M}} (\sqrt{p_{\mathrm{B}}} \mathbf{h}_{\mathrm{B,q}} + \sqrt{p_{\mathrm{J}}} \mathbf{h}_{\mathrm{J,q}} s_{q,u})^H \times (\sqrt{p_{\mathrm{B}}} \mathbf{h}_{\mathrm{B,k}} + \sqrt{p_{\mathrm{J}}} \mathbf{h}_{\mathrm{J,k}} s_{k,\ell}), \tag{4.15}$$

điều này phụ thuộc vào việc hai hoa tiêu thử nghiệm có nằm trong cùng một khung truyền dẫn hay không. Nó cũng phụ thuộc vào việc hoa tiêu thử nghiệm

Tất cả những cải tiến không thể đạt được đồng thời và phải đòi hỏi những yêu cầu về điều kiện truyền và phát nhưng những ưu điểm trên là những ưu điểm chung. Điều này sẽ không khả thi trong các hệ thống Massive MIMO, vì hai lý do.

- Kênh đối xứng: Cơ chế TDD phụ thuộc vào tính đối xứng của kênh. Bản thân kênh truyền về cơ bản là đối xứng, trừ khi việc truyền sóng bị ảnh hưởng bởi vật liệu với từ tính khác.
- Nhiễu hoa tiêu: Trong các hệ thống đa tế bào, chúng ta không thể chỉ định các hoa tiêu trực giao cho tất cả người dùng trong tất cả các tế bào. Hoa tiêu trực giao phải được tái sử dụng lại từ tế bào này sang tế bào khác. Hiện tượng này, được gọi là nhiễu hoa tiêu, làm giảm hiệu suất hệ thống.
- Phần cứng không hoàn hảo Massive MIMO dựa trên luật số lớn đến trung bình, chịu sự can thiệp của nhiễu, pha-đinh ở một mức độ nào đó. Trong thực tế, Massive MIMO phải được được xây dựng với các thành phần với chi phí thấp.

1.4.3 Hệ thống Massive MIMO với số ăng-ten vô cùng lớn

Massive MIMO là gì? Thuật ngữ này đã được sử dụng cho nhiều hệ thống khác nhau và điểm chung duy nhất dường như là hệ thống MIMO đa người dùng với từ vài đến vô số ăng-ten. Massive MIMO là hệ thống đa người dùng MIMO có nhiều lợi thế và có khả năng mở rộng. Có những sự khác biệt cơ bản giữa Massive MIMO và MIMO truyền thống. Thứ nhất, chỉ trạm gốc mới có thông tin trạng thái kênh truyền. Thứ hai, số ăng-ten tại trạm gốc M thường lớn hơn rất nhiều so với số lượng người dùng, mặc dù không nhất thiết phải như vậy. Thứ ba, đối xứng hoàn hảo cả trên kênh đường lên và kênh đường xuống. Những đặc điểm này làm cho Massive MIMO có khả năng mở rộng với số lượng ăng-ten trạm gốc. Với sự kết hợp MMSE đa tế bào, hiệu suất phổ tăng lên không giới hạn khi số lượng ăng ten tăng lên, ngay cả trong trường hợp nhiễu hoa tiêu, với một điều kiện độc lập tuyến tính giữa ma trận kênh hiệp phương sai.

1.5 Bảo mật lớp vật lý trong hệ thống Massive MIMO

1.5.1 Nguyên lý hoạt động của hệ thống Massive MIMO

Có thể thấy, nguyên lý hoạt động của hệ thống Massive MIMO cơ bản gồm 3 pha: i) pha huấn luyện đường lên, ii) pha truyền dữ liệu đường xuống và iii) pha truyền dữ liệu đường lên.

1.5.2 Các phương pháp tấn công trong hệ thống Massive MIMO

Đảm bảo an toàn thông tin là một vấn đề quan trọng và thiết yếu trong các hệ thống thông tin, các thiết bị không hợp lệ, có thể làm ảnh ảnh hưởng đến tính bảo mật, bằng một trong hai phương pháp sau:
- Nghe lén thụ động: Thiết bị nghe lén thụ động chỉ cố gắng tách tín hiệu từ sóng vô tuyến mang thông tin nhận được từ thiết bị phát.
- Tấn công chủ động: Thiết bị tấn công chủ động không chỉ cố gắng tách tín hiệu được truyền từ thiết bị phát mà còn tự phát đi tín hiệu để gây nhiễu.

1.6 Kết luận

Chương 1 đã trình bày những kiến thức chung về bảo mật lớp vật lý trong mạng thông tin di động nói chung và mạng Massive MIMO nói riêng, các phương pháp tấn công trong mạng Massive MIMO. Những vấn đề này là nền tảng để NCS tìm hiểu, nghiên cứu và đưa ra những biện pháp nâng cao tính bảo mật của hệ thống Massive MIMO.

và hoa tiêu thử nghiệm nhận được là $\mathbf{y}_{k,\ell}$ trong (4.2) có thể được viết lại như sau

$$\mathbf{y}_{k,\ell} = \mathbf{f}_{k,\ell} s_{\mathrm{B},k,\ell} + \mathbf{n}_{\mathrm{k},\ell}, \tag{4.4}$$

Theo giả định ULA tại trạm gốc, phản hồi mảng $\mathbf{g}_{\mathrm{X}} \in \mathbb{C}^{M\times 1}$ của vectơ kênh $\mathbf{h}_{\mathrm{X},k}$ độc lập với khung vô tuyến k và được tính như sau:

$$\mathbf{g}_{\mathrm{X}} = \left[1, e^{j2\bar{d}_{\mathrm{A}}\sin\theta_{\mathrm{X}}}, \cdots, e^{j2\bar{d}_{\mathrm{A}}(M-1)\sin\theta_{\mathrm{X}}}\right]^T. \tag{4.5}$$

Khai thác những đặc tính của hệ thống Massive MIMO, chúng ta đạt được $\mathbf{g}_{\mathrm{X}}^H \mathbf{g}_{\mathrm{X}} = M, \forall \mathrm{X} \in \mathcal{X}$ và

$$\mathbf{g}_{\mathrm{J}}^H \mathbf{g}_{\mathrm{B}} = \psi(\theta_{\mathrm{B}}, \theta_{\mathrm{J}}, M) = \frac{\sin(M\bar{d}_{\mathrm{A}}(\sin\theta_{\mathrm{B}} - \sin\theta_{\mathrm{J}}))}{\sin(\bar{d}_{\mathrm{A}}(\sin\theta_{\mathrm{B}} - \sin\theta_{\mathrm{J}}))} e^{j(M-1)\bar{d}_{\mathrm{A}}(\sin\theta_{\mathrm{B}} - \sin\theta_{\mathrm{J}})}. \tag{4.6}$$

Chúng ta có thể phân tích qua việc quan sát giới hạn của $\psi(\theta_{\mathrm{B}}, \theta_{\mathrm{J}})$ khi $M \to \infty$ như sau

$$\lim_{M\to\infty} \frac{|\psi(\theta_{\mathrm{B}}, \theta_{\mathrm{J}}, M)|}{M} = \begin{cases} 1, \text{nếu} \quad \sin\theta_{\mathrm{B}} = \sin\theta_{\mathrm{J}}, \\ 0, \text{trường hợp khác.} \end{cases} \tag{4.7}$$

Sau đó, vector kênh truyền tức thời $\mathbf{h}_{\mathrm{X},k}$ được phân tích thành hai thành phần LOS và NLOS như sau:

$$\mathbf{h}_{\mathrm{X},k} = \beta_{\mathrm{X,L}}^{1/2} \mathbf{g}_{\mathrm{X}} + \beta_{\mathrm{X,N}}^{1/2} \mathbf{w}_{\mathrm{X},k} \tag{4.8}$$

trong đó $\beta_{\mathrm{X,L}}^{1/2} \mathbf{g}_{\mathrm{X}} \in \mathbb{C}^{M\times M}$ là thành phần LOS và $\beta_{\mathrm{X,N}}^{1/2} \mathbf{w}_{\mathrm{X}} \in \mathbb{C}^{M\times M}$ với $\mathbf{w}_{\mathrm{X}} \sim \mathcal{CN}(\mathbf{0}_{M\times 1}, \mathbf{I}_{M\times M})$ là thành phần NLOS.

4.2 Phương pháp phát hiện nhiễu hoa tiêu

4.2.1 Phương pháp phát hiện

Để phương pháp phát hiện sát với thực tế, trong phần này của luận án nghiên cứu sử dụng một thuật toán kết hợp với phân tập thời gian. Một phương pháp sử dụng giá trị vô hướng mới được định nghĩa là tích được chia tỷ lệ nhận được của hai các tín hiệu nhận ngẫu nhiên. $l \in \mathcal{K}_k$ trong khung truyền dẫn $\mathcal{F}_l$ và $u \in \mathcal{K}_q$ trong khung truyền dẫn $\mathcal{F}_u$ như sau:

$$z_{k,q} = \frac{1}{\sqrt{M}} \mathbf{y}_{k,\ell}^H \mathbf{y}_{q,u}. \tag{4.9}$$

Chương 4

CẢI THIỆN XÁC SUẤT PHÁT HIỆN VÀ XÁC SUẤT BÁO ĐỘNG GIẢ TRONG HỆ THỐNG MASSIVE MIMO

Trong Chương 4 này, NCS đã xây dựng một phương pháp để để cải thiện độ tin cậy của xác suất phát hiện và giảm thiểu xác suất báo động giả của hoa tiêu trong các kịch bản có sự tham gia của các thiết bị gây nhiễu chủ động dựa trên phân tập thời gian. *Đóng góp của Chương 4 được trình bày trong công trình số J2, J3* . Theo đó, những nghiên cứu chính được tóm tắt như sau: Xây dựng những kịch bản có khả năng xảy ra khi có thiết bị tấn công, nâng cao độ chính xác của phương pháp phát hiện dựa trên phân tập thời gian.

4.1 Mô hình hệ thống

Giả định rằng quá trình truyền giữa người dùng hợp pháp B và trạm gốc được đồng bộ hóa hoàn hảo. Theo đó, trạm gốc biết hoa tiêu huấn luyện trong quá trình truyền ở pha đường lên. Ký hiệu $\mathcal{K}_k$ là tập chỉ mục của các ký hiệu đó trong khung vô tuyến k. Chúng ta có thể viết như sau:

$$s_{\mathrm{J,k},\ell} \overset{(a)}{=} s_{\mathrm{J,k},\ell} s^{*}_{\mathrm{B,k},\ell} s_{\mathrm{B,k},\ell} = s_{k,\ell} s_{\mathrm{B,k},\ell}, \tag{4.1}$$

trong đó $s_{k,\ell} = s_{\mathrm{J,k},\ell} s^{*}_{\mathrm{B,k},\ell} \in \mathcal{S}$ và $s_{\mathrm{J,k},\ell}, s_{\mathrm{B,k},\ell} \in \mathcal{S}$. Giao thức truyền được xem xét cho biết rằng sự gây nhiễu hoa tiêu chỉ xảy ra trong ký hiệu huấn luyện $\ell \in \mathcal{K}_k$ như $\alpha_{k,\ell} = 1$. Tín hiệu hoa tiêu thử nghiệm nhận được tại BS tương ứng với hoa tiêu thử nghiệm $\ell \in \mathcal{K}_k$, ký hiệu là $\mathbf{y}_{k,\ell} \in \mathbb{C}^{M\times 1}$ được cho là:

$$\mathbf{y}_{k,\ell} = \sqrt{p_{\mathrm{B}}}\mathbf{h}_{\mathrm{B,k}} s_{\mathrm{B},k,\ell} + \alpha_{k,\ell}\sqrt{p_{\mathrm{J}}}\mathbf{h}_{\mathrm{J,k}} s_{\mathrm{J},k,\ell} + \mathbf{n}_{\mathrm{k},\ell}, \tag{4.2}$$

Trong đó $\mathbf{n}_{k,\ell} \in \mathbb{C}^{M\times 1}$ nhiễu Gauss trắng cộng tại trạm gốc trong quá trình gửi hoa tiêu thử nghiệm $\ell \in \mathcal{K}_k$, được phân phối dưới dạng $\mathbf{n}_{k,\ell} \sim \mathcal{CN}(\mathbf{0}_{M\times 1}, \sigma^2\mathbf{I}_M)$. Để giải quyết (4.2), đặt $\mathbf{f}_{k,\ell} \in \mathbb{C}^{M\times 1}$ là vectơ hệ số kênh truyền tương ứng, là định nghĩa là

$$\mathbf{f}_{k,\ell} = \sqrt{p_{\mathrm{B}}}\mathbf{h}_{\mathrm{B,k}} + \alpha_{k,\ell}\sqrt{p_{\mathrm{J}}}\mathbf{h}_{\mathrm{J,k}} s_{k,\ell}. \tag{4.3}$$

Chương 2

DUNG LƯỢNG BẢO MẬT CỦA HỆ THỐNG KHI CÓ THIẾT BỊ NGHE LÉN THỤ ĐỘNG ĐỐI VỚI HỆ THỐNG MASSIVE MIMO TRONG ĐIỀU KIỆN KÊNH PHA ĐINH RICE

Bảo mật lớp vật lý có thể kết hợp với các giải pháp bảo mật ở lớp trên để đảm bảo an ninh thông tin trong mạng thông tin vô tuyến. Có hai phương pháp sau: nghe lén thụ động, tấn công chủ động. Cụ thể, thiết bị nghe lén thụ động chỉ cố gắng tách tín hiệu từ sóng vô tuyến mang thông tin nhận được từ thiết bị phát. Về nguyên lý, thiết bị nghe lén thụ động không thể bị phát hiện. Trong Chương 2, luận án đề xuất một phương pháp đánh giá ảnh hưởng của thiết bị nghe lén lên dung lượng bảo mật của hệ thống.

2.1 Những thách thức của nghe lén thụ động trong mạng Massive MIMO

Bảo mật lớp vật lý trong các hệ thống thông tin vô tuyến là xem xét các yếu tố ở lớp vật lý như tạp âm nhiệt, hệ số pha-đinh của kênh truyền và các kỹ thuật xử lý tín hiệu ảnh hưởng như thế nào đến khả năng bảo mật thông tin được truyền qua kênh vật lý khi có mặt các thiết bị xâm nhập. Trong chương này tập trung nghiên cứu dung lượng bảo mật lớp vật lý trong hệ thống thông tin Massive MIMO khi có mặt thiết bị nghe lén thụ động trong điều kiện kênh pha-đinh Rice không tương quan về không gian. Các kết quả nghiên cứu trước đây đã chỉ ra rằng với điều kiện kênh truyền pha-đinh Rayleigh, việc sử dụng rất nhiều ăng ten ở trạm gốc giúp hệ thống thông tin Massive MIMO có khả năng tự bảo mật trước thiết bị nghe lén thụ động.

2.2 Mô hình hệ thống

Xem xét một hệ thống Massive MIMO với trạm gốc (ký hiệu là A) đang phục vụ một thuê bao hợp lệ (ký hiệu là nút B) với sự có mặt của một thiết bị nghe trộm thụ động (ký hiệu là E), tức là thiết bị này không phát tín hiệu trong suốt thời gian được xem xét của hệ thống. Trong khi trạm gốc A có M ăng ten thì thuê bao B và thiết bị nghe lén E chỉ có một ăng-ten. Để tiện trình

bày, chúng ta ký hiệu $\mathcal{X} = \{\mathrm{B}, \mathrm{E}\}$ là tập chỉ số nút. Giả thiết hệ thống hoạt động ở chế độ song công phân chia theo thời gian TDD với khung truyền dẫn vô tuyến dài τ ký hiệu. Các hệ số pha-đinh phạm vi rộng ứng với thành phần truyền tầm nhìn thẳng LOS $\beta_{\mathrm{X,L}}$ và thành phần truyền không tầm nhìn thẳng NLOS $\beta_{\mathrm{X,N}}$ được tính như sau

$$\beta_{\mathrm{X,L}} = \sqrt{\frac{\kappa_X}{\kappa_X + 1}}\beta_{\mathrm{X}}; \quad \beta_{\mathrm{X,N}} = \sqrt{\frac{1}{\kappa_X + 1}}\beta_{\mathrm{X}}. \tag{2.1}$$

Khi đó vector hệ số kênh truyền từ trạm gốc tới nút X có phân bố như sau $\mathbf{h}_{\mathrm{X}} \sim \mathcal{CN}(\mathbf{g}_{\mathrm{X}}, \beta_{\mathrm{X,N}}\mathbf{I}_M)$ for $\mathrm{X} \in \mathcal{X}$ và được biểu diễn dưới dạng

$$\mathbf{h}_{\mathrm{X}} = \mathbf{g}_{\mathrm{X}} + \beta_{\mathrm{X,N}}^{1/2}\mathbf{w}_{\mathrm{X}}. \tag{2.2}$$

trong đó $\mathbf{g}_{\mathrm{X}}$ là vec tơ hệ số kênh truyền ứng với thành phần truyền sóng tầm nhìn thẳng và $\mathbf{w}_{\mathrm{X}} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_M)$ là vector hệ số kênh truyền pha-đinh phạm vi nhỏ. Để tiện tính toán, giả thiết mảng anten tại trạm gốc A được phân bố tuyến tính đều (ULA: Uniform Linear Array). Việc mở rộng ra các dạng hình học khác của mảng ăng-ten này không quá phức tạp. Khi đó, vec tor hệ số truyền tầm nhìn thẳng từ trạm gốc tới nút $\mathrm{X} \in \mathcal{X}$ được tính như sau

$$\mathbf{g}_{\mathrm{X}} = \beta_{\mathrm{X,L}}^{1/2}\left[1 \; e^{j2\pi d \sin\phi_{\mathrm{X}}} \; \cdots \; e^{j2\pi d(M-1)\sin\phi_{\mathrm{X}}}\right]^T. \tag{2.3}$$

trong đó ϕ_{X} là góc tới từ nút X tới trạm gốc và d là tỷ số giữa khoảng cách giữa các phần tử ăng-ten kề nhau ở trạm gốc chia cho bước sóng. Chú ý rằng $\mathbf{g}_{\mathrm{X}}^H\mathbf{g}_{\mathrm{X}} = M\beta_{X,L}$ với $\forall X \in \mathcal{X}$. Để tiện trình bày, ta định nghĩa một số tham số như sau

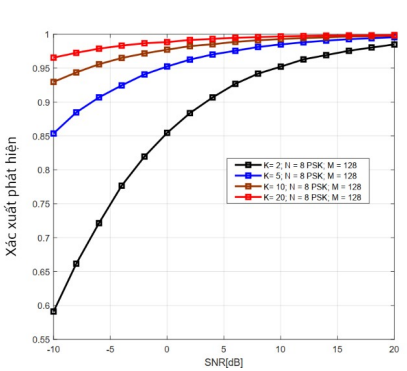
$$\psi(\phi_{\mathrm{B}}, \phi_{\mathrm{E}}) = \pi d(\sin\phi_{\mathrm{B}} - \sin\phi_{\mathrm{E}}); \quad \alpha(\phi_{\mathrm{B}}, \phi_{\mathrm{E}}, M) = \frac{\sin(M\psi(\phi_{\mathrm{B}}, \phi_{\mathrm{E}}))}{\sin(\psi(\phi_{\mathrm{B}}, \phi_{\mathrm{E}}))}. \tag{2.4}$$

Sau một số phép biến đổi ta có

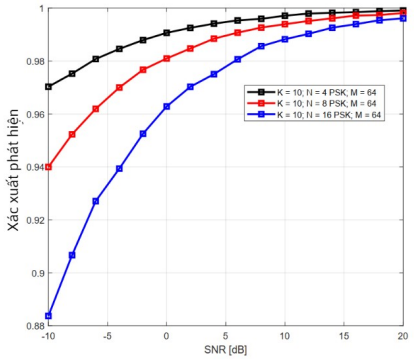
$$\mathbf{g}_{\mathrm{E}}^H\mathbf{g}_{\mathrm{B}} = \beta_{\mathrm{B,L}}^{1/2}\beta_{\mathrm{E,L}}^{1/2}e^{j\psi(\phi_{\mathrm{B}}, \phi_{\mathrm{B}})}\alpha(\phi_{\mathrm{B}}, \phi_{\mathrm{E}}, M). \tag{2.5}$$

Trong pha huấn luyện và ước lượng kênh, nút B truyền một tín hiệu hoa tiêu với công suất phát p_{p}. Tín hiệu huấn luyện sau khi tiền xử lý là

$$\mathbf{y}_{\mathrm{A}} = \sqrt{p_{\mathrm{p}}}\tau_{\mathrm{p}}\mathbf{h}_{\mathrm{B}} + \mathbf{n}_{\mathrm{A}}. \tag{2.6}$$



((a)) Xác suất phát hiện tỉ lệ với SNR với $M = 128$, $N = 8$ và các giá trị K khác nhau.



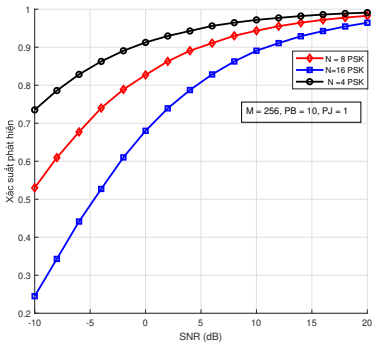
((b)) Xác suất phát hiện vs. SNR cho trường hợp K = 10, M = 64 ang ten, và N = 4; 8; 16-PSK

Hình 3.4: Xác suất phát hiện vs. SNR

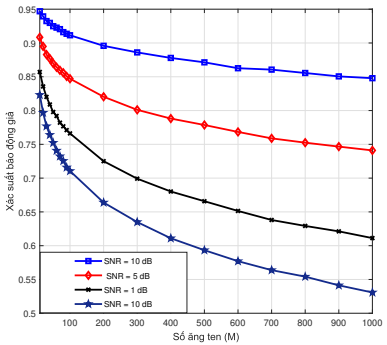
Hình 3.4(b) trình bày xác suất phát hiện như một hàm của SNR với một số khóa N -PSK khi trạm gốc chỉ có $M = 64$ ăng ten. Lưu ý rằng xác suất phát hiện cũng tăng theo SNR và rất gần bằng 1 khi SNR lớn hơn 15 dB. Từ quan sát này, chúng ta có thể kết luận rằng bằng cách sử dụng đủ số lượng hoa tiêu thử nghiệm, trạm gốc không cần sử dụng quá nhiều ăng ten cho mục đích phát hiện thiết bị gây nhiễu.

3.5 Kết luận chương

Chương 3 Phân tích các kịch bản xảy ra khi có các thiết bị gây nhiễu chủ động. Xây dựng thuật toán phát hiện thiết bị tấn công gây nhiễu. Xây dựng phạm vi phát hiện tấn công gây nhiễu của thiết bị bất hợp pháp. Đề xuất một số giải pháp phát hiện nhiễu hoa tiêu gây ra bởi thiết bị tấn công chủ động trong hệ thống Massive MIMO trong điều kiện kênh truyền pha-đinh Rice.



((a)) Xác suất phát hiện tỉ lệ SNR với M = 256, P_B = 24 dBm, P_J = 24 dBm, $\Phi_B = 0.1$ rad và $\Phi_J = 0.1$ rad.



((b)) Xác suất báo động giả $\Phi_J = 0.1$ rad, $\Phi_B = 0.1$ rad, N = 16 PSK với M.

Hình 3.3: Xác suất phát hiện và xác suất báo động giả

Hình 3.3(a) cho biết xác suất phát hiện tỉ lệ với nhiễu SNR và trạm gốc được trang bị 256 ăng- ten, P_B = 24 dBm, P_J = 24 dBm, với khóa PSK lần lượt là N = [4, 8, 16]- PSK. Trong đó SNR được tính bởi SNR = $\frac{P_B}{N_0}$ in dB. Như dự đoán, xác suất phát hiện tăng SNR; trong miền SNR cao, xác suất phát hiện là 1. Hình vẽ 3.3(b) cho thấy xác suất báo động giả giảm đi khi số lượng ăng-ten tại trạm gốc tăng lên, ngay ngay cả khi góc tới của thiết bị tấn công tương đương với góc tới của người dùng hợp pháp $\Phi_J = 0.1$ rad, $\Phi_B = 0.1$ rad và thay đổi số SNR = [-1, 1, 5, 10] dB

3.4.1 *Sử dụng căp ngẫu nhiên hoa tiêu thử nghiệm trong một tập hoa tiêu thử nghiệm*

Khi chúng ta mở rộng nghiên cứu với kịch bản sử dụng một tập hợp hoa tiêu thử nghiệm và chọn ngẫu nhiên một cặp trong số đó.

Hình 3.4(a) hiển thị xác suất phát hiện dưới dạng hàm SNR khi trạm gốc có $M = 128$ ăng ten và sử dụng 8 -PSK. Như dự đoán, xác suất phát hiện tăng lên với SNR; trong miền SNR cao, xác suất phát hiện là 1. Đáng chú ý, ngay cả với một số lượng nhỏ hoa tiêu thử nghiệm, ví dụ: $K = 5$, phương pháp cũng đạt được xác suất phát hiện thiết bị gây nhiễu rất cao, cao hơn nhiều so với việc chỉ sử dụng một cặp hoa tiêu, tức là $K = 2$.

trong đó $\mathbf{n}_A \sim \mathcal{CN}(\mathbf{0}, \sigma_A^2 \mathbf{I}_M)$ là tạp âm nhiệt AWGN có công suất σ_A^2. Giả thiết trạm gốc áp dụng kỹ thuật ước lượng bình phương trung bình tối thiểu (MMSE) để nhận được một ước lượng hệ số kênh truyền tới nút B như sau:

$$\hat{\mathbf{h}}_B = \mathbf{g}_B + \frac{\sqrt{p_p}\beta_{B,N}}{p_p \tau_p \beta_{B,N} + \sigma_A^2}(\mathbf{y}_A - \sqrt{p_p}\tau_p \mathbf{g}_B). \quad (2.7)$$

Theo tính chất trực giao của phương pháp MMSE Trong pha truyền dữ liệu đường xuống, trạm gốc truyền. Tín hiệu thu được ở nút B và nút E lần lượt là

$$y_B = \sqrt{p_f}\mathbf{h}_B^H \mathbf{f}_B x_B + n_B.; \quad y_E = \sqrt{p_f}\mathbf{h}_E^H \mathbf{f}_B x_B + n_E. \quad (2.8)$$

trong đó $n_B \sim \mathcal{CN}(0, \sigma_B^2)$ và $n_E \sim \mathcal{CN}(0, \sigma_E^2)$ là tạp âm Gauss trắng cộng độc lập thống kê với nhau.

2.3 Phân tích dung lượng bảo mật

2.3.1 *Định nghĩa và cách tiếp cận*

Dung lượng bảo mật của hệ thống là tốc độ dữ liệu tối đa có thể truyền từ trạm gốc tới thuê bao hợp lệ, tức là nút B, một cách tin cậy và bảo mật mà không cần dùng thêm các biện pháp mã hoá. Theo định nghĩa, dung lượng bảo mật được xác định như sau: $C_{SC} = [R_B - R_E]^+$.

2.3.2 *Tốc độ dữ liệu hợp lệ*

Biểu thức tín hiệu thu tại nút B như sau

$$y_B = \sqrt{p_d}\mathbb{E}[\mathbf{h}_B^H \mathbf{f}_B]x_B + \sqrt{p_d}(\mathbf{h}_B^H \mathbf{f}_B - \mathbb{E}[\mathbf{h}_B^H \mathbf{f}_B])x_B + n_B. \quad (2.9)$$

Khi đó, một giới hạn dưới của SINR tại nút B được ký hiệu là η_B và được xác định như sau

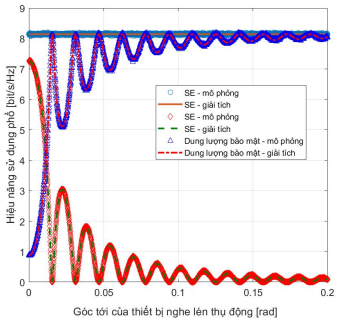
$$\eta_B = \frac{p_d|\mathbb{E}[\mathbf{h}_B^H \mathbf{f}_B x_B]|^2}{p_d\mathbb{E}[|(\mathbf{h}_B^H \mathbf{f}_B - \mathbb{E}[\mathbf{h}_B^H \mathbf{f}_B])x_B|^2] + \sigma_B^2} = \frac{p_d|\mathbb{E}[\mathbf{h}_B^H \mathbf{f}_B]|^2}{p_d(\mathbb{E}[|\mathbf{h}_B^H \mathbf{f}_B|^2] - |\mathbb{E}[\mathbf{h}_B^H \mathbf{f}_B]|^2) + \sigma_B^2}. \quad (2.10)$$

2.3.3 *Tốc độ dữ liệu nghe lén đạt được*

Từ công thức (2.8) ta có thể viết lại biểu thức tín hiệu thu tại nút E như sau

$$y_E = \sqrt{p_d}\mathbb{E}[\mathbf{h}_E^H \mathbf{f}_B]x_B + \sqrt{p_d}(\mathbf{h}_E^H \mathbf{f}_B - \mathbb{E}[\mathbf{h}_E^H \mathbf{f}_B])x_B + n_E. \quad (2.11)$$

Khi đó, một giới hạn dưới của SINR tại nút E được ký hiệu là η_E



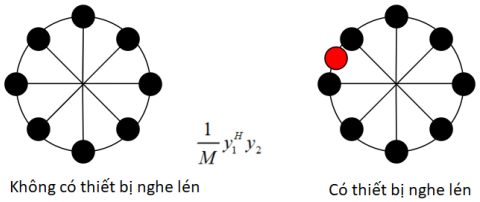
Hình 2.1: Kết quả mô phỏng và kết quả phân tích giải tích của R_{B}, R_{E} và C_{SC} dưới dạng hàm số của Φ_{E}[rad] khi M = 128.

2.4 Kết quả mô phỏng và tính toán số

Trước hết, chúng ta xem xét một kịch bản mô phỏng trong đó thiết bị nghe lén thụ động, hay nút E, đặt khá sát thiết bị đầu cuối hợp lệ, hay nút B. Một số các tham số mô phỏng của kịch bản này như sau: i) khoảng cách từ nút E và từ nút B đến trạm gốc đều là 300 [m], ii) hệ số mô hình kênh pha-đinh Rice là $\kappa_{\mathrm{B}} = \kappa_{\mathrm{E}} = 9$ [dB], và iii) kết quả mô phỏng được lấy trung bình của 150.000 mẫu. Hình 2.2(b) cho thấy khi $\Phi_{\mathrm{E}} \neq \Phi_{\mathrm{B}}$ thì cả R_{E} và C_{SC} thay đổi không đơn điệu theo M. Khi số ăng-ten ở trạm gốc nhỏ thì tốc độ dữ liệu nghe lén gần sát với tốc độ dữ liệu hợp lệ, khiến cho dung lượng bảo mật thấp. Khi số ăng-ten ở trạm gốc tăng lên thì tốc độ dữ liệu nghe lén giảm dần. Hình 2.1 trình bày kết quả mô phỏng và kết quả phân tích giải tích của R_{B}, R_{E} và C_{SC} dưới dạng hàm số của Φ_{E} rad khi $M = 128$. Có thể thấy rằng khi góc tới Φ_{E} càng lớn, tức là $\Delta\Phi$ càng lớn, thì tốc độ dữ liệu nghe lén có xu hướng càng giảm.

2.5 Kết luận chương

Chương 2 Đánh giá dung lượng bảo mật của hệ thống mạng Massive MIMO trong điều kiện kênh truyền pha-đinh Rice khi có thiết bị nghe lén thụ động. Khảo sát và chứng minh thành phần truyền tầm nhìn thẳng có thể làm cho tương quan chéo giữa các vec tơ hệ số kênh truyền giữa trạm gốc và các thiết bị đủ lớn.



Hình 3.2: Sơ đồ phát hiện phát hiện nhiễu hoa tiêu ngẫu nhiên.

Chúng ta xem xét $\mathrm{p}_1^{\mathrm{J}}(\mathrm{p}_1^{\mathrm{B}})^{\mathrm{H}}$ và $\mathrm{p}_2^{\mathrm{J}}(\mathrm{p}_2^{\mathrm{B}})^{\mathrm{H}}$. Nếu dấu bằng xảy ra thì $S_{\mathrm{M}}^{\mathrm{J}}$ bằng với một ký hiệu PSK cộng với $\mathrm{N}_{12}^{\mathrm{J}}$. Do đó, trong trường hợp này, tình huống tương tự với tình huống của J và khả năng phát hiện ra J bị giảm. Ngược lại, $S_{\mathrm{M}}^{\mathrm{J}}$ có sự khác biệt so với tín hiệu PSK sẽ tương đương với việc thêm N_{12}^{J}.

3.3.3 Xây dựng phạm vi phát hiên thiết bị bất hợp pháp

BS quyết định phạm vi mà J có bị phát hiện gây nhiễu hay không dựa trên kết quả tính tích vô hướng $\mathrm{y}_1^{\mathrm{H}}\mathrm{y}_2/\mathrm{M}$ nằm ngoài hay bên trong khu vực phát hiện từ tích vô hướng đã được tạo z_{12} trong công thức (3.8). Tổng tương đương với vô hướng ký hiệu vô hướng $D_{\mathrm{B}} = P_{\mathrm{B}}\beta_{\mathrm{B}}$ và nhiễu Gauss, BS quyết định rằng nếu $\mathrm{y}_1^{\mathrm{H}}\mathrm{y}_2/\mathrm{M}$ ở vị trí $r(D_{\mathrm{B}})$ cách một số đường PSK, thì J không gây nhiễu.

Phương sai $\mathrm{S}_{\mathrm{M}}^0$ của nhiễu Gauss N_{12}^0 tăng lên trong D_{B} với $r(D_{\mathrm{B}})$ giảm. Nhiễu Gauss có thể được hiển thị $\sqrt{S_{\mathrm{M}}^0}$ dưới dạng một vòng tròn có tâm quanh 0 , bán kính $r(D_{\mathrm{B}})$ trong không gian tín hiệu. Để phát hiện ra J, tích vô hướng được tạo ra bởi trạm gốc

$$s_M^0 = \frac{N_0}{M^2}(MN_0 + 2P_B\mathbf{R}_{\mathbf{T}}^{\mathbf{11}}). \tag{3.10}$$

Để phát hiện J, trạm gốc tuân theo thuật toán sau:
Với mỗi phần thực tương ứng của $y_{12} = \frac{(y_1^H y_2)}{M}$ Tính $|y_{12} - xv|$ với $r(x)$ Những khả năng có thể xảy ra : Trường hợp 1: $|y_{12} - xv| > r(x)$ Trạm gốc thông báo J vắng mặt ; Trường hợp 2: $|y_{12} - xv| < r(x)$ Trạm gốc thông báo J xuất hiện gây nhiễu

3.4 Kết quả mô phỏng

Trong kịch bản mô phỏng, trên kênh truyền Rice pha đinh chỉ sử dụng 1 cặp hoa tiêu trong một khung truyền vô tuyến để phát hiện thiết bị gây nhiễu.

3.3 Tấn công sử dụng nhiễu hoa tiêu ở kênh đường lên

Việc trạm gốc xác định chính xác nguồn gốc của hoa tiêu là vô cùng khó khăn. Chúng ta muốn nhấn mạnh rằng kỹ thuật của này không yêu cầu về thông tin trạng thái kênh truyền. Các tín hiệu nhận được trong suốt thời gian huấn luyện.

$$\mathbf{y}_{\mathrm{j}} = \sqrt{P_{\mathrm{B}}}\mathbf{s}_{\mathrm{j}}^{\mathrm{B}}\mathbf{h}_{\mathrm{A,B}} + \sqrt{P_{\mathrm{J}}}\mathbf{s}_{\mathrm{j}}^{\mathrm{J}}\mathbf{h}_{\mathrm{A,J}} + \mathrm{n}_{j}, \tag{3.5}$$

3.3.1 Sơ đồ phát hiện hoa tiêu ngẫu nhiên khi không bị can nhiễu

Trước tiên, chúng ta đã loại bỏ nhiễu khỏi tín hiệu nhận được để chứng minh nguyên tắc này. Tích được biến đổi như sau.

$$\mathbf{z}_{12}^{0} = \frac{1}{M} P_{\mathrm{B}} \left(\mathbf{p}_{1}^{\mathrm{B}}\right)^{\mathrm{H}} \mathbf{p}_{2}^{\mathrm{B}} \mathbf{h}_{\mathrm{A,B}}^{\mathrm{H}} \mathbf{h}_{\mathrm{A,B}}. \tag{3.6}$$

Nếu J không có mặt, ký hiệu N-PSK được chia tỷ lệ của BS sẽ nhận được là z_{12}. BS nhận được z_{12}^{J} khi có mặt J và J không được phát hiện khi z_{12}^{J} là tín hiệu tỷ lệ N-PSK. Điều này cho thấy rằng z_{12}^{J} nằm trên một trong các đường PSK.

3.3.2 Sơ đồ phát hiện nhiễu hoa tiêu ngẫu nhiên dưới sự ảnh hưởng của nhiễu

Trong cả hai khung thời gian, khi thiết bị nghe lén không hoạt động, các tín hiệu nhận được tại trạm gốc là.

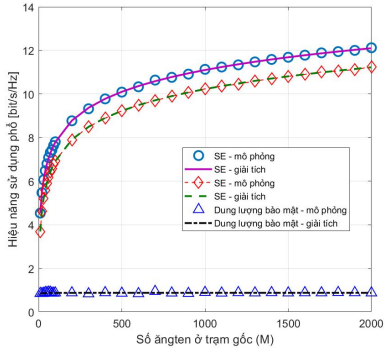
$$\mathbf{y}_1 = \sqrt{P_{\mathrm{B}}}\mathbf{p}_1^{\mathrm{B}}\mathbf{h}_{\mathrm{A,B}} + \mathbf{n}_1; \quad \mathbf{y}_2 = \sqrt{P_{\mathrm{B}}}\mathbf{p}_2^{\mathrm{B}}\mathbf{h}_{\mathrm{A,B}} + \mathbf{n}_2. \tag{3.7}$$

Nếu thiết bị nghe lén vắng mặt trong cả 2 khe thời gian, thì tích vô hướng của tín hiệu nhận được y_{12}^{0} là:

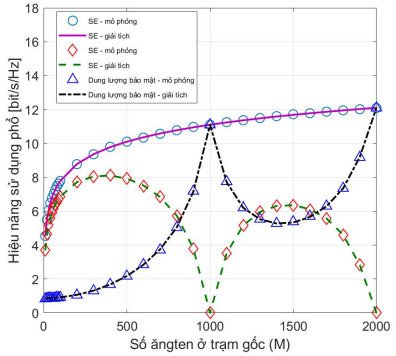
$$\mathrm{z}_{12}^{0} = \frac{1}{\mathrm{M}}\left[\mathrm{P_B}(\mathrm{p}_1^{\mathrm{B}})^{\mathrm{H}}\mathrm{p}_2^{\mathrm{B}}\mathrm{h}_{\mathrm{A,B}}^{\mathrm{H}}\mathrm{h}_{\mathrm{A,B}} + \mathrm{N}_{12}^{0}\right]. \tag{3.8}$$

Khi không có thiết bị nghe lén, z_{12}^{0} thuộc tín hiệu PSK cộng thêm nhiễu Gauss trung bình bằng không và phương sai là S_{J}^{0}.

$$\begin{aligned} S_{\mathrm{M}}^{\mathrm{J}} =& \sigma^2\Big\{2\mathrm{P_B R_T^{11}} + \sqrt{P_{\mathrm{B}}P_{\mathrm{J}}}[(\mathrm{p}_1^{\mathrm{B}})^{\mathrm{H}}\mathrm{p}_1^{\mathrm{J}} + (\mathrm{p}_2^{\mathrm{B}})^{\mathrm{H}}\mathrm{p}_2^{\mathrm{J}}]\mathrm{R_T^{12}} \\ &+\sqrt{P_{\mathrm{B}}P_{\mathrm{J}}}[(\mathrm{p}_1^{\mathrm{J}})^{\mathrm{H}}\mathrm{p}_1^{\mathrm{B}} + (\mathrm{p}_2^{\mathrm{J}})^{\mathrm{H}}\mathrm{p}_2^{\mathrm{B}}]\mathrm{R_T^{21}} + 2P_{\mathrm{J}}\mathrm{R_T^{22}} + \sigma^2\Big\}. \end{aligned} \tag{3.9}$$



((a)) Kết quả mô phỏng và kết quả phân tích giải tích của R_{B}, R_{E} và C_{SC} dưới dạng hàm số của M khi $\Phi_{\mathrm{E}} = \Phi_{\mathrm{B}} = 0$ [rad]. .



((b)) Kết quả mô phỏng và kết quả phân tích giải tích của R_{B}, R_{E} và C_{SC} dưới dạng hàm số của M khi $\Phi_{\mathrm{E}} = \Phi_{\mathrm{B}} = 0.002$ [rad].

Hình 2.2: Kết quả mô phỏng và kết quả phân tích giải tích của R_{B}, R_{E} và C_{SC} dưới dạng hàm số của M

Chương 3

PHÁT HIỆU NHIỄU HOA TIÊU TRONG HỆ THỐNG MASSIVE MIMO TRONG ĐIỀU KIỆN KÊNH PHA-ĐINH RICE

Việc gây nhiễu hoa tiêu không chỉ làm giảm khả năng bảo mật mà còn khó phát hiện. Kỹ thuật phát hiện thiết bị bất hợp pháp chỉ cần hai khe thời gian đào tạo và không cần thông tin kênh truyền. Đóng góp của Chương 3 được trình bày trong công trình số 3,4

3.1 Giới thiệu chung

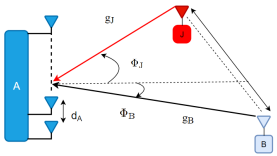
Trong tấn công chủ động, những kẻ tấn công không chỉ giải mã các tín hiệu truyền từ máy phát mà còn tạo ra các tín hiệu gây nhiễu. Những nghiên cứu chính được tóm tắt như sau: Phân tích xây dựng khu vực phát hiện của thiết bị gây nhiễu, đề xuất thêm thuật toán để tìm xác suất phát hiện và xác suất báo động giả. Đề xuất một sơ đồ phát hiện để phát hiện bộ gây nhiễu đang hoạt động.

3.2 Mô hình hệ thống

Hãy xem xét một hệ thống Masive MIMO đơn tế bào trong đó một trạm gốc truyền thông hợp pháp với người dùng B khi có sự hiện diện của một thiết bị nghe bất hợp pháp J. Cả hai đều trang bị đơn một ăng ten. Để thuận tiện chúng ta ký hiệu như sau $\mathcal{X} = \{\mathrm{B}, \mathrm{J}\}$ trong Hình 3.1. Mặc dù đây là một mô hình hệ thống đã được đơn giản hóa bằng cách chỉ xem xét hai người dùng, kết quả của mô hình này có thể dễ dàng mở rộng cho các trường hợp có nhiều người dùng. BS trang bị M ăng ten, trong khi $M \gg 2$. Để thuận tiện, chúng ta xét mảng ăng-ten của trạm cơ sở A là Mảng tuyến tính đồng nhất (ULA). Hình 3.1 biểu thị mô hình đó.

Mô hình truyền dẫn tầm nhìn thẳng LOS của vectơ kênh truyền của hệ thống $\mathbf{g}_k$, $\forall k \in \mathcal{K}$. Trong đó $\mathbf{a}_{\mathrm{BS}}(\theta) \in \mathbb{C}^M \times 1$ là vectơ của ăng ten M tại BS theo hướng tương ứng với sóng góc lan truyền θ. Lưu ý $\bar{\mathbf{g}}_k \in \mathbb{C}^M \times 1$ là lan truyền LOS $\mathbf{g}_k$ với $k \in \mathbf{K}$. khi đó $\bar{\mathbf{g}}_k$ được xác định như sau.

$$\bar{\mathbf{g}}_k = \frac{1}{\sqrt{M}} \left[1 \; e^{j\bar{d}_{\mathrm{BS}} \sin\theta} \; \cdots \; e^{j\bar{d}_{\mathrm{BS}}(M-1)\sin\theta}\right]^T. \tag{3.1}$$



Hình 3.1: Mô hình hệ thống, trong đó trạm gốc A truyền thông với người dùng B và thiết bị nghe lén bất hợp pháp J.

Mô hình truyền dẫn không tầm nhìn thẳng NLOS Ký hiệu $\mathbf{h}_k \in \mathbb{C}^{N_t \times 1}$ hệ số kênh truyền không tầm nhìn thẳng NLOS $\mathbf{h}_k$, $\forall k \in \mathcal{K}$. Trong môi trường truyền sóng giàu tán xạ chúng ta giả thiết $\mathbf{h}_k \sim \mathcal{CN}(\mathbf{0}_{M\times 1}, \mathbf{R}_k)$, trong đó $\mathbf{R}_k = \mathbb{E}[\mathbf{h}_k \mathbf{h}_k^H] \in \mathbb{C}^{M\times M}$ là ma trận tương quan không gian của vectơ truyền hệ số NLOS $\mathbf{h}_k$ trong đó $\mathrm{tr}(\mathbf{R}_k) = 1$.Khi đó phần tử hàng m hàng cột n của $\mathbf{R}_k$ là $\forall m, n \in \{1, 2, \cdots, M\}$

$$[\mathbf{R}_k]_{m,n} = \xi \int_{-\pi}^{\pi} e^{j\bar{d}_{\mathrm{BS}} \sin(\theta_k + \phi)} p_\theta(\phi) d\phi. \tag{3.2}$$

Trong pha đường lên, người dùng hợp pháp B truyền tín hiệu hoa tiêu đường lên với công suất là P_{B} và P_{J} là công suất truyền của thiết bị nghe lén bất hợp pháp. $\mathbf{p}_j{}^{\mathrm{x}} \in \mathbb{A}$ là những hoa tiêu được truyền đi bởi người dùng hợp pháp B và thiết bị nghe lén J trong cùng khe thời gian đào tạo j.

Tín hiệu hoa tiêu nhận được tiền xử lý trước tại trạm gốc là

$$\mathbf{y}_{\mathrm{j}} = \sqrt{\mathrm{P_B}}\mathbf{p}_{\mathrm{j}}^{\mathrm{B}}\mathbf{h}_{\mathrm{AB}} + \sqrt{\mathrm{P_J}}\mathbf{p}_{\mathrm{j}}^{\mathrm{J}}\mathbf{h}_{\mathrm{AJ}} + \mathbf{n}_{\mathrm{j}}. \tag{3.3}$$

trong đó $\mathbf{n}_j \sim \mathcal{CN}(\mathbf{0}, \sigma_j^2 \mathbf{I}_{N_t})$ là tạp âm nhiệt Gauss và

$$\mathbf{h}_{\mathrm{AB}} = \mathbf{g}_{\mathrm{B}} + \beta_{\mathrm{B,N}}^{1/2}\mathbf{w}_{\mathrm{B}}; \quad \mathbf{h}_{\mathrm{AJ}} = \mathbf{g}_{\mathrm{J}} + \beta_{\mathrm{J,N}}^{1/2}\mathbf{w}_{\mathrm{J}}. \tag{3.4}$$

Giả thiết trạm gốc sử dụng phương pháp bình phương tối thiểu MMSE để ước lượng kênh. Để thuận tiện, ký hiệu $\mathrm{R_T^{11}}$ là tích được xác định là $\mathbf{h}_{\mathrm{AB}}^{\mathrm{H}}\mathbf{h}_{\mathrm{AB}}$, $\mathrm{R_T^{12}}$ là tích $\mathbf{h}_{\mathrm{AB}}^{\mathrm{H}}\mathbf{h}_{\mathrm{AJ}}$, $\mathrm{R_T^{21}}$ là tích $\mathbf{h}_{\mathrm{AJ}}^{\mathrm{H}}\mathbf{h}_{\mathrm{AB}}$ and $\mathrm{R_T^{22}}$ là tích $\mathbf{h}_{\mathrm{AJ}}^{\mathrm{H}}\mathbf{h}_{\mathrm{AJ}}$.
Chúng ta có $\mathrm{R_T^{11}} = \beta_{\mathrm{B}}\mathrm{M}$; $\mathrm{R_T^{12}} = \sqrt{\beta_{\mathrm{B,N}}\beta_{\mathrm{J,N}}}\mathrm{e}^{\mathrm{j}\phi(\theta_{\mathrm{B}},\theta_{\mathrm{J}})}\alpha(\theta_{\mathrm{B}}, \theta_{\mathrm{J}}, \mathrm{M})$; $\mathrm{R_T^{21}} = [\mathrm{R_T^{12}}]^{\mathrm{H}}$; $\mathrm{R_T^{22}} = \beta_{\mathrm{J}}\mathrm{M}$.