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**

LUẬN ÁN TIẾN SỸ KỸ THUẬT

HÀ NỘI - 2023

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**

NGƯỜI HƯỚNG DẪN KHOA HỌC: **1.TS TRƯƠNG TRUNG KIÊN**

2. PGS.TS LÊ NHẬT THĂNG

HÀ NỘI - 2023

LỜI CAM ĐOAN

Tôi xin cam đoan các kết quả trình bày trong luận án là công trình nghiên cứu của tôi dưới sự hướng dẫn của các cán bộ hướng dẫn. Các số liệu, kết quả trình bày trong luận án là hoàn toàn trung thực và chưa được công bố trong bất kỳ công trình nào trước đây. Các kết quả sử dụng tham khảo đều đã được trích dẫn đầy đủ và theo đúng quy định.

Hà Nội, ngày tháng năm 2023

Tác giả

Vũ Lê Quỳnh Giang

LỜI CẢM ƠN

Trong quá trình nghiên cứu và hoàn thành luận án, nghiên cứu sinh đã nhận được nhiều sự giúp đỡ và đóng góp quý báu. Trước tiên, nghiên cứu sinh xin bày tỏ lòng biết ơn sâu sắc đến các Thầy hướng dẫn **TS. Trương Trung Kiên** và **PGS.TS. Lê Nhật Thăng**. Các Thầy không những là người hướng dẫn, giúp đỡ nghiên cứu sinh hoàn thành luận án này mà còn là người truyền thụ động lực, quyết tâm cho nghiên cứu sinh vượt qua những khó khăn trong quá trình nghiên cứu.

Tiếp theo, nghiên cứu sinh xin chân thành cảm ơn Khoa Sau đại học - Học viện Công nghệ Bưu chính Viễn Thông đã luôn tạo điều kiện, giúp đỡ để nghiên cứu sinh hoàn thành được luận án này. Nghiên cứu sinh xin chân thành cám ơn sâu sắc đến TS. Trần Hùng đã luôn hỗ trợ nghiên cứu sinh trong quá trình nghiên cứu.

Nhờ những ý kiến nhận xét và góp ý quí báu của các Thầy trong Hội đồng góp ý hội thảo luận án, bản luận án này đã được cải thiện đáng kể so với bản dự thảo luận án ban đầu. Tác giả xin chân thành cảm ơn các Thầy trong Hội đồng góp ý luận án trước bảo vệ về những chỉ dẫn quan trọng. Cuối cùng, nghiên cứu sinh xin gửi lời cảm ơn sâu sắc tới cơ quan, gia đình, bạn bè và đồng nghiệp đã luôn động viên, chia sẻ những khó khăn trong cuộc sống để nghiên cứu sinh đạt được những kết quả như hôm nay.

Mục lục

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	**Nghĩa Tiếng Anh**	**Nghĩa Tiếng Việt**
AWGN	Additive White Gaussian Noise	Tạp âm Gauss trắng cộng tính
BS	Base Station	Trạm gốc
CDF	Cumulative Distribution Function	Hàm phân bố xác suất
CR	Cognitive Radio	Vô tuyến nhận thức
CSI	Channel State Information	Thông tin trạng thái kênh truyền
DF	Decode and Forward	Giải mã và chuyển tiếp
ITU	International Telecommunications Union	Liên minh viễn thông quốc tế
IEEE	Institute of Electrical and Electronics Engineers	Viện kỹ thuật Điện và Điện tử
MAC	Medium Access Control	Điều khiển truy nhập
MIMO	Multi-Input Multi-Output	Đa đầu vào đa đầu ra
Massive MIMO	Massive Multi-Input Multi-Output	Đa đầu vào đa đầu ra cỡ rất lớn

MRC	Maximal Ratio Combining	Kết hợp tỉ số cực đại
LTE	Long Term Evolution	Tiến hóa dài hạn
LOS	Line-Of-Sight	Tầm nhìn thẳng
NLOS	Non-Line-Of-Sight	Không tầm nhìn thẳng
SOP	Secrecy Outage Probability	Xác suất dừng bảo mật
OFDM	Orthogonal Frequency-Division Multiplexing	Ghép kênh phân chia theo tần số trực giao
PSK	Phase-Shift Keying	Điều chế khóa dịch pha
PDF	Probability Density Function	Hàm mật độ xác suất
SNR	Signal-to-Noise Ratio	Tỉ số công suất tín hiệu trên công suất tạp âm
SINR	Signal to Interference plus Noise Ratio	Tỉ số công suất tín hiệu/ công suất nhiễu và tạp âm
Wi-Fi	Wireless Fidelity	Công nghệ mạng cục bộ không dây
WAP	Wi-Fi Protected Access	Chuẩn bảo mật được sử dụng trong mạng Wi-Fi
WEP	Wired Equivalent Privacy	Bảo mật tương đương với mạng có dây
ZF	Zero-Forcing	Cưỡng ép về không

Danh sách hình vẽ

DANH MỤC KÝ HIỆU TOÁN HỌC

Ký hiệu	Ý nghĩa
a	a là biến số vô hướng
$\mathbf{a}$	$\mathbf{a}$ là một véc-tơ
$\mathbf{A}$	$\mathbf{A}$ là một ma trận
a_{ij}	Phần tử hàng thứ i cột thứ j của ma trận $\mathbf{A}$
$\mathbf{A}^H$	Chuyển vị liên hợp phức (Hermitian transpose) của ma trận $\boldsymbol{A}$
$\mathbb{E}\{\cdot\}$	Kí hiệu của toán tử kì vọng
$f_X(\cdot)$	Hàm mật độ xác suất của X
$F_X(\cdot)$	Hàm phân bố tích lũy của X
$\mathcal{CN}(0, \sigma^2)$	Phân bố chuẩn với trung bình không và phương sai σ^2
η	Hệ số suy hao truyền sóng

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. Theo báo cáo của Ericsson [26], đến quý 4 năm 2022 thế giới có khoảng 8,2 tỷ thiết bị di động trên toàn cầu với tổng cộng 660 triệu tổng số đăng ký 5G hiện trên toàn thế giới. 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 [22, 55]. 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. Cụ thể, với bản chất mở của môi trường lan truyền sóng vô tuyến, mọi thiết bị nằm trong vùng phủ sóng của một máy phát đều có khả năng thu sóng vô tuyến truyền đi từ máy phát đó để cố gắng giải mã thông tin một cách bất hợp pháp. Ngoài ra 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 [59]. 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 truyền tin sử dụng nhiều ăng-ten ở cả máy phát và máy thu, gọi tắt là kỹ thuật MIMO đã được chuẩn hóa và sử dụng rộng rãi trong mạng WLAN thương mại (IEEE 802.11n/ac) và mạng di động tế bào (IEEE 802.16e /m, 3GPP LTE và LTE nâng cao). Ngoài ra, kỹ thuật định hướng búp sóng khi sử dụng nhiều ăng-ten thu phát giúp cải thiện tỉ số công suất tín hiệu trên công suất tạp âm của tín hiệu mong muốn, giảm xuyên nhiễu từ đó tăng hiệu suất sử dụng phổ. 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 [15, 79]. Masive MIMO là một cải tiến của kỹ thuật thông tin MIMO truyền thống vốn đã được tích hợp trong các mạng thông tin di động thế hệ thứ 4. Ý tưởng chính của kỹ thuật truyền dẫn này là sử dụng rất nhiều (có thể lên tới hàng trăm, hàng ngàn) ăng-ten ở trạm gốc để phục vụ đồng thời nhiều (có thể lên tới hàng chục, hàng trăm) thuê bao di động trên cùng một tài nguyên tần số và thời gian [53, 52]. Kỹ thuật này đã được 3GPP chấp nhận và đưa vào từ phiên bản 13 của họ công nghệ 3GPP LTE/LTE-Advanced/LTE-Advanced Pro [2] và được tích hợp vào họ công nghệ Vô tuyến mới cho 5G của 3GPP [50, 72, 69]. Kỹ thuật này hứa hẹn là một trong những công nghệ chủ chốt cho các mạng thông tin di động 5G, 6G (sau khi cấu hình lại) nhờ vào các tiềm năng như cải thiện hiệu quả sử dụng phổ tần và hiệu quả sử dụng năng lượng với sự triển khai chi phí thấp [48]. Bên cạnh các lợi ích tiềm năng này, kỹ thuật Massive MIMO cũng đặt ra các thách thức kỹ thuật mới cần phải vượt qua trước khi có thể áp dụng rộng rãi trên thực tế [59, 40, 94]. Ví dụ, 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. Đối với các phương pháp truyền thống, bảo mật của hệ thông mạng không dây đã được quan tâm và nghiên cứu ở các lớp khác nhau ở mô hình OSI. Như trong lớp liên kết thì sử dụng phương pháp bảo mật theo chuẩn bảo mật nâng cao, trong lớp ứng dụng thì sử dụng phương pháp bảo mật tương đương có dây/ Truy cập Wi-Fi được bảo vệ WEP/WAP... những phương pháp này đã được sử dụng trong các mạng truyền thông di động hiện nay. Tuy nhiên trong thực tế chứng minh, các giao thức bảo mật này đã bị vượt qua, đặc biệt đối với các thiết bị tấn công thông minh [94, 43]. Bên cạnh đó các giải pháp bảo mật truyền thống này sử dụng hệ thống mật mã dựa trên độ phức tạp của các thuật toán, các giải pháp này gặp nhiều khó khăn, hạn chế trong việc triển khai, trong việc quản lý và phân phối các khóa bảo mật. Ngoài ra, với sự phát triển nhanh chóng của các công nghệ tính toán, các hệ thống mật mã cũng phải đối mặt với nguy cơ bị phá vỡ và độ tin cậy của mã hóa sẽ không còn được đảm bảo. Ngày nay, bảo mật tại lớp vật lý đang là lĩnh vực được quan tâm nghiên cứu của các nhà khoa học trên khắp thế giới do có một số ưu điểm so với các phương pháp bảo mật truyền thông. Vì có độ trễ và độ phức tạp thấp, có khả năng triển khai tại lớp vật lý và áp dụng song song với các cơ chế bảo mật mã hóa hiện có ở các lớp trên, bảo mật lớp vật lý có khả năng cho phép truyền thông bảo mật và độ phức tạp tính toán thấp, đặc biệt hiệu có hiệu quả đối với các thiết bị mạng di động có tài nguyên hạn chế. Bảo mật tại lớp vật lý không yêu cầu các giả thiết về khả năng tính toán của các thiết bị nghe lén; kỹ thuật bảo mật tại lớp vật lý có khả năng mở rộng, có thể bổ sung hỗ trợ cho các kỹ thuật mã hóa truyền thống. Bên cạnh đó, bảo mật lớp vật lý bảo đảm an

toàn cho các pha truyền thông, còn kỹ thuật mật mã bảo vệ dữ liệu đã xử lý sau pha truyền thông. Việc nghiên cứu các tính chất bảo mật trong truyền thông ở lớp vật lý đã được đề cập đến trong công trình nghiên cứu của tác giả Wyner [92, 108]. Trong những năm gần đây, với sự phát triển của các công nghệ không dây như kỹ thuật MIMO, Massive MIMO, mmWave, NOMA, đã thu hút sự quan tâm của các nhà nghiên cứu và trở thành vấn đề quan trọng trong truyền thông thế hệ mới. Trong vấn đề an toàn thông tin của mạng thông tin di động, có hai vấn đề chính là tấn công chủ động và nghe trộm thụ động. Tấn công chủ động có thể là sự xâm nhập bất hợp pháp bằng cách giả mạo thông tin xác thực hoặc làm vô hiệu hóa hoạt động của hệ thống mạng bằng cách gây nhiễu để máy phát không thể truyền thông tin đến máy thu hợp pháp [61]. Đối với nghe lén thụ động, mục tiêu là thu thập và phá vỡ tính bí mật của thông tin, chặn dữ liệu và gây nhiễu cho truyền dẫn hợp pháp trong hệ thống thông tin di động [94, 43, 108, 61, 58]. Mặc dù đã có khá nhiều các công trình nghiên cứu với cách tiếp cận khác nhau, song vấn đề bảo mật thông tin trong truyền thông vẫn luôn là vấn đề mở. Với sự phát triển không ngừng của công nghệ trong hệ thống mạng thông tin di động, vấn đề bảo mật trong truyền thông sẽ có nhiều thách thức hơn nữa trong tương lai và chủ đề này trở thành một trong những lĩnh vực nghiên cứu quan trọng và liên tục. Những ý tưởng chính của bảo mật lớp vật lý là tận dụng những lợi thế của đặc tính kênh truyền và tính chất ngẫu nhiên của tín hiệu để hạn chế lượng thông tin mà các thiết bị không được cấp phép có thể thu thập và giải mã được. Dựa trên các mô hình lý thuyết và sử dụng phương pháp xử lý và mã hóa tín hiệu một cách phù hợp, bảo mật lớp vật lý có thể đảm bảo truyền thông an toàn mà không cần thiết lập các bộ khóa bí mật. Mặt khác,

trong các trường hợp cần thiết phải sử dụng khóa bí mật, bằng cách khai thác sự ngẫu nhiên và tính chất phức tạp của kênh truyền như cường độ tín hiệu, pha của tín hiệu sóng mang, điều chế góc, biên độ, tham số ngẫu nhiên Gauss,... Bảo mật lớp vật lý có khả năng cung cấp những phương pháp tiếp cận khác để thiết lập những khóa bí mật với mục tiêu làm giảm việc tính toán cho mã hóa tại lớp ứng dụng. Mạng thông tin di động luôn phải đối mặt với nhiều thách thức đo đặc điểm vật lý của kênh truyền. Với bản chất phát tự nhiên của kênh truyền vô tuyến, mạng thông tin di động do các thiết bị trong vùng phủ sóng của máy phát đều có khả năng thu và giải mã thông tin. Ngoài ra những vấn đề bảo mât khác phát sinh từ những nhược điểm của môi trường truyền dẫn tín hiệu như pha đinh đa đường, suy hao, nhiễu. Kết quả là những thiết bị bất hợp pháp có thể trích xuất thông tin truyền thông, có thể gây suy giảm hoặc gián đoạn hoạt động truyền thông của hệ thống [59]. Bên cạnh các giải pháp giải quyết vấn đề an ninh trong mạng thông tin di động theo cách tiếp cận truyền thống là sử dụng các kỹ thuật mã hóa để cảnh báo, ngăn chặn các thiết bị bất hợp pháp [33, 45]. Hiện nay, bảo mật lớp vật lý đã được bổ sung để nâng cao tính bảo mật thông tin và chống lại các cuộc tấn công nghe trộm trong mạng thông tin di động. Ý tưởng của cách tiếp cận bảo mật trong lớp vật lý cho mạng thông tin di động là dựa vào nguyên lý cơ bản của bảo mật dựa trên lý thuyết thông tin được giới thiệu bởi tác giả Shannon [77], tác giả đã đề xuất ra khái niệm bảo mật hoàn hảo. Tiếp theo cá nhà nghiên cứu đã đưa ra mô hình kênh nghe lén thụ động và chứng minh rằng việc truyền dữ liệu/ thông tin có thể đạt được bảo mật hoàn hảo nếu dung lượng kênh cấp phép lớn hơn dung lượng kênh bất hợp pháp mà không cần phải mã hóa dữ liệu [92]. Mô hình kênh nghe lén của được xem là nền

móng cho các nghiên cứu bảo mật thông tin tại lớp vật lý. Dung lượng bảo mật của kênh Gauss nghe lén được tính bằng hiệu dung lượng kênh Shannon giữa kênh chính và kênh nghe lén [66]. Khi đó dung lượng bảo mật là tốc độ tối đa có thể truyền tín hiệu mà vẫn đảm bảo rằng thiết bị nghe lén không thể giải mã thành công thông tin từ thiết bị phát gửi cho thiết bị thu.

Các nghiên cứu trước đây chủ yếu tập trung vào nghiên cứu các tiềm năng trong việc cải thiện hiệu quả sử dụng năng lượng của hệ thống này. Bảo mật cho hệ thống thông tin vô tuyến MIMO mới chỉ được nghiên cứu trong vài năm gần đây. Các kết quả nghiên cứu đã công bố trên thế giới đến nay cho hệ thống Massive MIMO xem xét cả ba trường hợp sau đây: i) chỉ có thiết bị tấn công chủ động [103, 43, 86, 91], ii) chỉ có thiết bị nghe lén thụ động [95, 105, 104, 8, 93, 100] và iii) có cả hai loại thiết bị trên [58, 73]. Các công trình này nghiên cứu một mô hình hệ thống Massive MIMO cụ thể trong đó một thuê bao liên lạc với trạm gốc khi có mặt thiết bị nghe lén thụ động/tấn công chủ động và trong điều kiện mô hình kênh truyền pha-đinh Rayleigh. Một số kết quả đã chứng minh trong điều kiện kênh truyền pha-đinh Rayleigh, thì thiết bị nghe lén thụ động hầu như không ảnh hướng đến dung lượng bảo mật của hệ thống. Tuy nhiên tình huống trở nên xấu hơn khi có mà thiết bị nghe lén nhận được độ lợi kênh truyền tốt hơn thiết bị được cấp phép khi mà thiết bị nghe lén ở gần trạm gốc hơn tại người dùng hợp pháp. Do đó bảo mật hoàn hảo trong truyền thông gần như không thể đạt được, vì thế cần xây dựng và thiết kế các biện pháp bảo mật để bảo đảm an toàn thông tin trong truyền thông. Các thiết bị nghe lén thường che giấu sự có mặt của chúng, do đó trạm gốc không có được thông tin trạng thái kênh truyền CSI của các thiết bị nghe lén. Vì vậy các công trình nghiên cứu đã dựa trên những ưu điểm

của hệ thống Masive MIMO, đó là trang bị mảng ăng-ten rất lớn ở trạm gốc để sử dụng các biện pháp nhằm phát hiện sự có mặt của các thiết bị nghe lén, từ đó trạm gốc có thể thực hiện những biện pháp bổ sung để bảo đảm an toàn trong truyền thông, hoặc quyết định tạm dừng pha truyền dữ liệu. Các công trình nghiên cứu đã đề xuất các biện pháp như việc nhận biết dao động nội của thiết bị nghe lén, sử dụng biện pháp lựa chọn ăng-ten tại trạm gốc, sử dụng hoa tiêu ngẫu nhiên để tính xác suất phát hiện của thiết bị nghe lén, tính xác suất cảnh báo sai. Đối với thiết bị nghe lén chuyển từ trạng thái nghe lén thụ động sang tấn công chủ động, các nghiên cứu này cũng đã trình bày phương pháp tính xác suất phát hiện và xác suất cảnh báo giả của hệ thống. Các kết quả tính toàn và mô phỏng cho thấy khi số lượng ăng ten tại trạm gốc càng lớn thì xác suất phát hiện càng lớn, và tiền gần về 1, và xác suất cảnh báo giả tiến dần về 0. Tuy nhiên trong điều kiện kênh truyền pha đinh Rice sẽ được nghiên cứu ảnh hưởng của thiết bị nghe lén thụ động như thế nào thì chưa được nghiên cứu nhiều. Đây cũng là hướng nghiên cứu mà NCS tập trung nghiên cứu.

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 Massive MIMO *khi có một thiết bị nghe lén thụ động trong điều kiện kênh truyền 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 xuất hiện *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. Ý nghĩa khoa học và thực tiễn

Ý nghĩa khoa học:

Luận án này góp phần bổ sung thêm các kết quả và sự kiến thức, kinh nghiệm

nghiên cứu về bài toán bảo mật lớp vật lý cho mạng Massive MIMO:

(1)Thiết lập biểu thức giải tích đánh giá dung lượng bảo mật của hệ thống thông tin vô tuyến MIMO cỡ rất lớn trong điều kiện kênh truyền pha đinh Rice không tương quan về không gian.

(2) Đề xuất một số giải pháp phát hiện nhiễu hoa tiêu gây ra bởi thiết bị tấn công chủ động cho hệ thống Masive MIMO trong điều kiện kênh truyền pha đinh Rice.

(3) Đề xuất phương pháp để cải tiến kỹ thuật phát hiện thiết bị bất hợp pháp trên phân tập thời gian.

Ý nghĩa thực tiễn:

Luận án cung cấp một số biện pháp có thể áp dụng để:

(1) Bảo vệ thông tin:

Bảo mật lớp vật lý giúp đảm bảo tính bí mật của dữ liệu được truyền trong mạng Massive MIMO. Điều này đồng nghĩa với việc ngăn chặn các kẻ tấn công không được phép truy cập vào thông tin nhạy cảm của người dùng, bảo vệ quyền riêng tư và đảm bảo tính bảo mật của dữ liệu trong quá trình truyền tin.

(2) Đối phó với nhiễu hoa tiêu:

Nhiễu hoa tiêu là hiện tượng xảy ra trong mạng truyền thông khi các tín hiệu truyền đi bị nhiễu do nhiều nguyên nhân khác nhau. Việc sử dụng bảo mật lớp vật lý trong hệ thống Massive MIMO giúp đối phó hiệu quả với nhiễu hoa tiêu, đồng thời đảm bảo tính bảo mật của thông tin truyền đi dù trong điều kiện xuất hiện nhiễu hoa tiêu.

(3) Tăng tính an toàn của mạng truyền thông:

Bảo mật lớp vật lý cung cấp một lớp bảo vệ bổ sung cho mạng Massive

MIMO, nâng cao tính an toàn của mạng truyền thông. Nếu chỉ dựa vào các biện pháp bảo mật ở các lớp mạng hay ứng dụng, hệ thống vẫn có thể bị tấn công từ lớp vật lý.

(4) Tăng khả năng chống lại các cuộc tấn công:

Bảo mật lớp vật lý cung cấp các phương pháp mã hóa, che giấu và chống lại các cuộc tấn công thông tin từ bên ngoài, bao gồm cả các cuộc tấn công từ thiết bị cố gắng giải mã, giả mạo hoặc đánh cắp thông tin truyền đi.

2. Các công trình nghiên cứu liên quan

Khi nói về bảo mật thông tin ở lớp vật lý, trước tiên chúng ta phải đề cập đến GS. Shannon, người đã đưa ra khái niệm bảo mật hoàn hảo trong nghiên cứu "Communications Theory of Secrecy Systems" [77]. Tiếp theo là Csiszas và Körner [20] đã chứng minh sự tồn tại loại mã hóa kênh để vừa hạn chế lỗi vừa đảm bảo an toàn thông tin. Trong nghiên cứu [33], đã mở rộng mô hình của Wyner [92] cho kênh Gauss và kết quả đã chỉ ra rằng bảo mật của hệ thống được bảo đảm nếu tốc độ truyền nhỏ hơn dung lượng bảo mật, có nghĩa là truyền ở tốc độ tối đa mà các thiết bị nghe lén không giải mã được thông tin. Do đó khả năng bảo mật thông tin bị phá vỡ khi kênh chính Gauss có tỷ số tín hiệu trên nhiễu lớn hơn kênh nghe trộm Gauss. Những nghiên cứu này bị giới hạn chủ yếu do dung lượng bảo mật chỉ lớn hơn không, khi truyền hợp pháp có tỷ số SNR lớn hơn kênh nghe lén. Ngoài ra tác giả Diffie và Hellman [33] đã công bố những nguyên tắc cơ bản về mã khóa công khai. Tuy nhiên, cho đến những năm gần đây bảo mật thông tin mới đã được các nhà nghiên cứu quan tâm và nghiên cứu một cách rộng rãi. Trong nghiên cứu này đã chứng minh rằng khi kênh hợp pháp kém hơn kênh nghe lén, thì có thể sử dụng mã khóa bí mật trên kênh truyền. Trong công bố [34], tác giả

Hero cùng các cộng sự đã nghiên cứu các kỹ thuật xử lý tín hiệu không gian và thời gian để bảo đảm an toàn thông tin cho các kênh truyền vô tuyến. Các kết quả trong bài báo của tác giả Bloch [13] và cộng sự đã nghiên cứu dung lượng dừng bảo mật của các kênh pha-đinh trong lý thuyết bảo mật thông tin ngay cả khi các thiết bị nghe lén có tỷ số tín hiệu trên nhiễu trung bình lớn hơn máy thu hợp pháp. 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 ăng-ten. Kỹ thuật Massive MIMO cũng đặt ra các thách thức kỹ thuật mới cần phải vượt qua trước khi có thể áp dụng rộng rãi trên thực tế đó là việc đảm bảo an toàn thông tin trong truyền thông Tác giả Jun Zhu và các cộng sự đã đề xuất việc sử dụng nhiễu nhân tạo để báo hiệu sự tiếp nhận của các thiết bị nghe lén. Thiết bị nghe lén thường bị động để che giấu sự tồn tại của chúng, và do đó CSI của nghe lén không thể có được bởi thiết bị phát. Trong trường hợp này, nhiều ăng-ten truyền có thể được khai thác để tăng cường bí mật bằng cách truyền đồng thời cả tín hiệu mang thông tin và nhiễu nhân tạo AN. Cụ thể, tiền mã hóa được sử dụng để làm cho nhiễu nhân tạo AN không ảnh hưởng đối với thiết bị hợp pháp trong khi làm suy giảm hiệu suất giải mã của thiết bị nghe lén. Những công trình tiêu biểu [105, 104, 106]. Ngoài ra nhóm nghiên cứu này cũng nghiên cứu vấn đề bảo mật với phần cứng không hoàn hảo trong hệ thống Massive MIMO khi triển khai của máy thu phát bao gồm các thành phần của phần cứng khác nhau, bao gồm các bộ chuyển đổi, bộ chuyển đổi, máy trộn và ampli. Mỗi thành phần trong số đó làm méo các tín hiệu một cách khác nhau. Các thành phần của phần cứng không hoàn hảo làm giảm khả năng của bộ thu phát. Phần cứng không hoàn hảo trên các hệ thống MIMO tác động của nhiễu pha có

nguồn gốc từ các dao động tự do chạy trên đường xuống của các hệ thống Massive MIMO đã được nghiên cứu trong cho các thiết kế tiền mã hóa tuyến tính khác nhau với mục tiêu tránh sự méo tín hiệu do các phi tuyến không tải ở máy phát. Tác giả Kapetanovic cùng các cộng sự đã ngiên cứu các thiết bị nghe trộm có thể được trang bị những biện pháp đối phó với khả năng tự bảo mật của lớp vật lý. Các thiết bị nghe trộm thể di chuyển hay tự định vị tới gần với người dùng được cấp phép để các kênh cho người dùng được cấp phép và các thiết bị nghe lén có tương quan cao. Trong trường hợp này, thì lợi thế kênh trực giao từ trạm gốc đến người dùng của mạng Massive MIMO không còn, và khả năng bảo mật sẽ bị giảm đi. Nhóm nghiên cứu đã đề xuất mô hình phát hiện sự có mặt của các thiết bị nghe trộm đó là sự dụng những tín hiệu N-PSK ngẫu nhiên [43].

Tác giả Li và các cộng sự đã nghiên cứu tạo khóa lớp vật lý dựa trên sự tương hỗ của kênh để thiết lập khóa bí mật cho nhiều người dùng trong các hệ thống mạng không dây Massive MIMO. Các tác giả cung cấp mô hình miền kênh truyền, trong đó các phần tử khác nhau đại diện cho độ lợi của kênh từ các hướng truyền khác nhau đến các hướng nhận khác nhau. Dựa trên mô hình kênh này, phân tích tỷ lệ khóa bí mật và rút ra biểu thức dạng đóng trong các điều kiện kênh độc lập [49].

Nghiên cứu về mạng di động thế hệ mới là một trong những hướng nghiên cứu đã thu hút được rất nhiều sự quan tâm của các nhà khoa học trong nước. Và hướng nghiên cứu về bảo mật tại lớp vật lý cho những mạng thông tin di động thế hệ mới còn chưa được công bố nhiều, nhưng hoàn toàn có thể liên hệ từ các vấn đề này để phát triển thành các nghiên cứu về bảo mật lớp vật lý. Tiêu biểu như hướng nghiên cứu sau:

Nhóm nghiên cứu của PGS. TS. Võ Nguyễn Quốc Bảo và PGS. TS. Trần Trung Duy tại Học viện Công nghệ Bưu chính Viễn thông, cơ sở ở thành phố Hồ Chí Minh, nghiên cứu khả năng sử dụng kỹ thuật truyền thông đa chặng và sử dụng các giao thức lựa chọn nút chuyển tiếp, thu thập năng lượng nhằm cải thiện dung lượng bảo mật cho hệ thống vô tuyến. Các kết quả nghiên cứu chỉ ra rằng sử dụng truyền thông đa chặng là một giải pháp hiệu quả và tối ưu hóa vị trí các nút chuyển tiếp trong sự tương quan với các thiết bị bất hợp pháp sẽ nâng cao đáng kể hiệu năng bảo mật của hệ thống đa chặng. Thu thập năng lượng tại các nút chuyển tiếp để tạo nhiễu nhân tạo sẽ tăng cường khả năng bảo mật lớp vật lý. Nhóm cũng nghiên cứu về khả năng lựa chọn các giao thức, kỹ thuật chuyển tiếp tín hiệu tại các nút chuyển tiếp, xem xét ảnh hưởng của nhiễu đồng kênh, phần cứng không hoàn hảo và thu thập năng lượng trong hệ thống vô tuyến và vô tuyến nhận thức, nhằm tăng cường khả năng bảo mật tại lớp vật lý, đồng thời so sánh khả năng bảo mật của hệ thống vào việc lựa chọn nút chuyển tiếp. Nhóm nghiên cứu của PGS. TS. Hà Đắc Bình tại Đại học Duy Tân, Đà Nẵng nghiên cứu bảo mật lớp vật lý của hệ thống vô tuyến trong các môi trường fading khác nhau, nâng cao hiệu quả bảo mật hệ thống với việc sử dụng kỹ thuật lựa chọn ăng-ten tại máy phát, đồng thời xem xét hiệu năng bảo mật của mạng vô tuyến nhận thức trong điều kiện có và không có sự hiện diện của các thiết bị nghe trộm của mạng thứ cấp. Nhóm nghiên cứu của GS.TS Trần Xuân Nam tại Học viện Kỹ thuật Quân sự, nghiên cứu về hệ thống vô tuyến chuyển tiếp MIMO và truyền thông cộng tác.

3. Đóng góp của luận án

Một số đóng góp chính của luận án có thể được tóm tắt như sau.

1. Đánh giá về khả năng bảo mật trong hệ mạng Massive MIMO trong điều kiện kênh truyền pha-đinh Rice không tương quan không gian và khi xuất hiện thiết bị nghe lén thụ động. Thiết lập biểu thức giải tích đánh giá dung lượng bảo mật của hệ thống Massive MIMO trong điều kiện kênh truyền pha-đinh Rice không tương quan về không gian.

2. Xây dựng thuật toán phát hiện, khu vực phát hiện và tính toán xác suất phát hiện và xác suất báo động giả khi với các kịch bản khác nhau của hệ thống Massive MIMO khi có thiết bị gây nhiễu chủ động.

3. Đề xuất giải pháp phát nâng cao xác suất 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 dựa trên phân tập thời gian.

4. Bố cục luận án

Luận án được tổ chức theo 4 chương, bố cục cụ thể như sau:

- Chương 1: NHỮNG VẤN ĐỀ CHUNG. Chương này trình bày các kiến thức tổng quan liên quan đến đề tài luận án để cung cấp kiến thức nền tảng giúp người đọc dễ theo dõi nội dung. Những kỹ thuật được trình bày ở các chương tiếp theo. Nội dung của chương này cũng nhằm mục tiêu giúp người đọc hình dung được bức tranh toàn cảnh các nghiên cứu liên quan đến đề tài luận án để từ đó có thể hiểu được ý nghĩa khoa học và ý nghĩa thực tiễn của các đóng góp khoa học của NCS

- 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 TRUYỀN PHA ĐINH RICE. Trong

chương này, luận án tập trung nghiên cứu hệ thống massive MIMO khi có mặt thiết bị nghe lén thụ động. Kết quả nghiên cứu của chương này đã được công bố trên công trình số 1,2

- Chương 3: NHIỄU HOA TIÊU TRONG HỆ THỐNG MASSIVE MIMO TRONG ĐIỀU KIỆN KÊNH TRUYỀN PHA ĐINH RICE. Chương 3 của luận án xây dựng mô hình và phân tích khu vực phát hiện, thuật toán phát hiện, tính xác suất phát hiện và xác suất báo động giả đối với thiết bị xâm nhập bất hợp pháp. Kết quả nghiên cứu được trình bày trong chương này đã được công bố trong các công trình số 3, 4
- Chương 4: CẢI THIỆN XÁC SUẤT PHÁT HIỆN VÀ XÁC SUẤT BÁO ĐỘNG GIẢ TRONG MẠNG MASSIVE MIMO. Chương 4 trình bày những đóng góp mới bao gồm việc đề xuất các phương pháp mới để cải thiện xác suất phát hiện đúng và giảm xác suất báo động giả trong mạng Massive MIMO, đồng thời thực hiện các phân tích và thử nghiệm để đánh giá hiệu quả của các giải pháp đề xuất. Kết quả nghiên cứu được trình bày trong chương này đã được công bố trong các công trình số 5,6

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. Theo báo cáo của Ericsson [26] sự tăng trưởng thuê bao 5G rất mạnh mẽ Đăng ký 5G tăng thêm 110 triệu trong quý 3 vào khoảng 870 triệu, và con số đó dự kiến sẽ đạt 1 tỷ thiết bị từ một số nhà cung cấp, với giá cả giảm nhanh hơn so với 4G và Trung Quốc triển khai 5G sớm và 5G sẽ trở thành công nghệ truy cập di động thống trị vào năm 2027. Thiết bị cầm tay 5G chiếm 23 phần trăm số lượng toàn cầu. 5G dự kiến sẽ là công nghệ truyền thông di động được triển khai nhanh nhất trong lịch sử và được dự báo sẽ phủ sóng khoảng 75% dân số thế giới vào năm 2027. Đến cuối năm 2028, 5 tỷ 5G đăng ký được dự báo trên toàn cầu, chiếm 55% của tất cả các thiết bị di động đăng ký. Tỷ lệ sử dụng thuê bao 5G là nhanh hơn cả 4G sau khi ra mắt vào năm 2009, với 5G dự kiến đạt 1 tỷ thuê bao sớm hơn 2 năm so với 4G. 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 cell, mảng ăng-ten bề mặt thông minh lên đến hàng ngàn ăng-ten, hàng triệu ăng-ten thông minh như

trong báo cáo của Ericsson. Để vượt qua được rào cản công nghệ này, mạng thông tin di động thế hệ thứ 5(5th Genaration - 5G), và những thế hệ tiếp theo [80] 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 đo đặc điểm vật lý của kênh truyền. Với bản chất phát tự nhiên của kênh truyền vô tuyến, mạng thông tin di động do các thiết bị trong vùng phủ sóng của máy phát đều có khả năng thu và giải mã thông tin. Ngoài ra những vấn đề bảo mật khác phát sinh từ những nhược điểm của môi trường truyền dẫn tín hiệu như pha-đinh đa đường, suy hao đường truyền, nhiễu. Kết quả là những thiết bị bất hợp pháp có thể trích xuất thông tin truyền thông, có thể gây suy giảm hoặc gián đoạn hoạt động truyền thông của hệ thống [59]. Kỹ thuật sử dụng rất nhiều ăng-ten tại trạm gốc là một trong những công nghệ chủ chốt cho các mạng thông tin di động 5G, 6G nhờ vào các tiềm năng như cải thiện hiệu quả sử dụng phổ tần và hiệu quả sử dụng năng lượng với sự triển khai chi phí thấp [48]. Bên cạnh các lợi ích tiềm năng này, kỹ thuật Massive MIMO cũng đặt ra các thách thức kỹ thuật mới cần phải vượt qua trước khi có thể áp dụng rộng rãi trên thực tế [58, 41, 42]. Ví dụ, 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 [59, 42]. Có nhiều giải pháp kỹ thuật đang được nghiên cứu để giải quyết thách thức kỹ thuật này, từ đó

có thể đề xuất các giải pháp kỹ thuật ở lớp vật lý để tăng cường tính bảo mật thông tin cho các mạng thông tin di động thế hệ mới, đặc biệt các mạng thông tin MIMO sử dụng rất nhiều ăng-ten ở trạm gốc, để làm tiền đề cho quá trình áp dụng vào thực tiễn. Tuy nhiên, khi các tiêu chuẩn cho mạng thông tin di động 5G được hoàn thiện và ban hành, còn rất nhiều vấn đề và thách thức kỹ thuật cần được nghiên cứu để vượt qua, và 6G đang trong quá trình nghiên cứu và triển khai thử nghiệm. Một trong những vấn đề kỹ thuật liên quan đang được quan tâm nhiều trên thế giới là tăng tính bảo mật và an toàn thông tin cho hệ thống thông tin MIMO sử dụng rất nhiều ăng-ten ở trạm gốc. Một cách tiếp cận để giải quyết vấn đề an toàn thông tin này là sử dụng các giải pháp bảo mật lớp vật lý. 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. Trong nghiên cứu này, nghiên cứu sinh sẽ tập trung nghiên cứu và lựa chọn mô hình hệ thống và mô hình toán học của hệ thống thông tin MIMO sử dụng rất nhiều ăng-ten ở trạm gốc khi bị tấn công. Tiếp đó, sẽ nghiên cứu các phương pháp tấn công hệ thống thông tin MIMO sử dụng rất nhiều ăng-ten ở trạm gốc. Trên cơ sở đó và tận dụng các kiến thức đã có về hệ thống thông tin Massive MIMO, NCS sẽ nghiên cứu đề xuất một giải pháp bảo mật lớp vật lý đối với một hoặc một số kiểu tấn công cụ thể và phân tích hiệu quả bảo mật tương ứng. Các phương pháp bảo mật tại các lớp phía trên trong mô hình mạng OSI đã được các nhà khoa học nghiên cứu và triển khai từ nhiều năm qua. Bảo mật lớp vật lý là một cách tiếp cận đang được quan tâm rộng rãi cho các mạng vô tuyến do có hiệu quả cao và do khả năng sẵn sàng kết hợp với các giải pháp bảo mật khác

Dữ liệu	Lớp	Phương pháp bảo mật
Data	Ứng dụng	Mã hóa
Data	Trình bày	
Data	Phiên	
Segments	Vận chuyển	Bảo mật lớp vận chuyển
Packets	Mạng	Bảo mật IP
Frames	Liên kết dữ liệu	Kiểm soát thu nhận
Bits	Vật lý	Bảo mật lớp vật lý

Bảng 1.1: Bảo mật ở các lớp trong mạng OSI

như mật mã hóa, không yêu cầu tính toán phức tạp. Ý tưởng chính của 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. Trên cơ sở đó, các giải pháp bảo mật lớp vật lý có thể được đề xuất để thiết bị thu hợp lệ có khả năng tách chính xác tín hiệu mong muốn bất chấp sự gây nhiễu của thiết bị tấn công chủ động trong khi thiết bị nghe lén thụ động không thể tách được tín hiệu mong muốn. Những vấn đề nghiên cứu kỹ thuật bảo mật tại lớp vật lý bao gồm:

- Nghiên cứu vấn đề an toàn thông tin này là sử dụng các giải pháp bảo mật lớp vật lý. 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.

- Nghiên cứu dựa trên ưu điểm khác của Massive MIMO, chưa được công nhận rộng rãi là tiềm năng của tự bảo mật lớp vật lý đối với các cuộc tấn

công nghe lén thụ động. Với tỷ lệ này truyền thông có thể được truyền tin cậy và an toàn mà không cần bất kỳ sử dụng của một hệ thống mã hóa chính thức nào. Tuy nhiên, với sự phát triển của công nghệ, các thiết bị nghe lén ED có thể được trang bị những biện pháp đối phó với khả năng tự bảo mật của lớp vật lý. Ví dụ, nó có thể di chuyển hay tự định vị tới gần với người dùng được cấp phép để các kênh cho người dùng được cấp phép và các thiết bị nghe trộm có tương quan cao. Trong trường hợp này, thì lợi thế kênh trực giao từ trạm gốc đến người dùng của mạng Massive MIMO không còn, và khả năng bảo mật sẽ bị giảm đi. Để chống lại việc này, cần đề xuất các giải pháp khác ở lớp vật lý để đảm bảo an toàn thông tin.

- Nghiên cứu kỹ thuật lựa chọn các nút chuyển giao để mạng để xác định dung lượng bảo mật, xác định xác suất dừng của hệ thống khi xuất hiện tấn công chủ động và nghe lén thụ động từ đó tối ưu hóa công suất thu phát trong hệ thống massive MIMO.

- Nghiên cứu kỹ thuật bảo mật trong hệ thống Massive MIMO với các thành phần phần cứng không hoàn hảo làm giảm khả năng của bộ thu phát.

Mạng thông tin di động luôn phải đối mặt với nhiều thách thức do đặc điểm vật lý tự nhiên của kênh truyền. Do bản chất phát sóng tự nhiên của kênh truyền vô tuyến, mạng thông tin di động dễ dàng bị tấn công, nghe trộm do bất kỳ người dùng nào trong vùng phủ sóng của trạm phát đều có khả năng thu và giải mã thông tin. Ngoài ra các vấn đề bảo mật khác phát sinh từ những nhược điểm của môi trường truyền dẫn tín hiệu. Kết quả là những

thiết bị bất hợp pháp có thể trích xuất thông tin truyền thông, có thể gây suy giảm hoặc gián đoạn hoạt động truyền thông của hệ thống [59]. Bên cạnh các giải pháp giải quyết vấn đề an ninh trong mạng thông tin di động theo cách tiếp cận truyền thống là sử dụng các kỹ thuật mã hóa để cảnh báo, ngăn chặn các thiết bị bất hợp pháp [33, 45]. Hiện nay, bảo mật lớp vật lý đã được bổ sung để nâng cao tính bảo mật thông tin và chống lại các cuộc tấn công/nghe lén trong mạng thông tin di động. Ý tưởng của cách tiếp cận bảo mật trong lớp vật lý cho mạng thông tin di động là dựa vào nguyên lý cơ bản của bảo mật dựa trên lý thuyết thông tin được giới thiệu bởi tác giả Shannon [77], tác giả đã đề xuất ra khái niệm bảo mật hoàn hảo. Tiếp theo đó tác giả Wyner đã đưa ra mô hình kênh nghe lén và chứng minh rằng việc truyền tải thông tin có thể đạt được bảo mật hoàn hảo nếu dung lượng kênh hợp pháp hơn hơn dung lượng kênh bất hợp pháp mà không cần phải mã hóa dữ liệu. Mô hình kênh nghe lén của Wyner được xem là nền móng cho các nghiên cứu bảo mật thông tin tại lớp vật lý. Phần lớn bảo mật lớp vật lý được xem xét dưới hình thức nghe lén thụ động tức là không truyền theo thứ tự để che dấu sự hiện diện của các thiết bị thu không hợp pháp.

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. Theo [45], dung lượng bảo mật của kênh nghe lén Gauss được tính bằng hiệu dung

lượng kênh Shannon giữa kênh chính và kênh nghe lén. Khi đó dung lượng bảo mật là tốc độ tối đa có thể truyền tín hiệu mà vẫn đảm bảo rằng thiết bị nghe lén không thể giải mã thành công các bản tin từ thiết bị phát gửi cho thiết bị thu.

$$\mathrm{C_{SC}} = \max\left\{\mathrm{C_{LU}} - \mathrm{C_{ED}}, 0\right\}] \tag{1.1}$$

Công thức (1.1) cho biết dung lượng bảo mật của hệ thống là giá trị lớn nhất của hiệu giữa dung lượng của kênh chính C_{LU} (1.2) và dung lượng kênh nghe lén C_{ED} (1.3) Theo định nghĩa Shannon ta có như sau

$$\mathrm{C_{LU}} = \frac{1}{2}\log(1 + \frac{P}{\sigma_m^2}) \tag{1.2}$$

$$C_{\mathrm{ED}} = \frac{1}{2}\log\left(1 + \frac{P}{\sigma_e^2}\right) \tag{1.3}$$

Từ (1.1) ta thấy tỉ số tín hiệu trên tạp âm của kênh hợp pháp lớn hơn kênh nghe lén, ngược lại dung lượng bảo mật bằng không. Điều này chứng tỏ ngay cả các thiết bị nghe lén thụ động cũng ảnh hướng đến dung lượng bảo mật của hệ thống. Ở phần tiếp theo sẽ trình bày về cách thức phát hiện các thiết bị nghe lén thụ động và tấn công chủ động.

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

Nếu dung lượng của kênh chính lớn hơn dung lượng kênh của kênh nghe lén thì ta có dung lượng bảo mật của hệ thông lớn hơn 0 và ngược lại, dung lượng bảo mật bằng 0 có nghĩa là truyền thông không bảo mật. Hiệu năng bảo mật của hệ thống được đánh giá chủ yếu thông qua ba tham số sau: Dung lượng bảo mật của hệ thống, xác suất dung lượng bảo mật khác không, xác suất dừng bảo mật.

a) Dung lượng bảo mật của hệ thống

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 dung thêm các biện pháp mã hóa. Theo định nghĩa, dung lượng bảo mật được xác định như 1.1.

b) Xác suất dung lượng bảo mật khác không

Xác suất dung lượng bảo mật khác không là xác suất khi dung lượng kênh chính lớn hơn dung lượng kênh nghe lén, điều đó có nghĩa tỉ số tín hiệu trên nhiễu SNR của kênh chính lớn hơn tỉ số tín hiệu trên nhiễu SNR của kênh nghe lén.

c) Xác suất dừng bảo mật của hệ thống

Gọi $R_s > 0$ là tốc độ bảo mật mong muốn của hệ thống. Xác suất dừng bảo mật của hệ thống là xác suất mà dung lượng bảo mật kênh tức thời C_s nhỏ hơn R_s . Nghĩa là

$$SOP = \Pr(C_s < R_s) \tag{1.4}$$

Ý nghĩa của xác suất dừng bảo mật là khi thiết lập một tốc độ bảo mật R_s, thiết bị phát giả định rằng dung lượng kênh nghe lén được cho bởi $C_m - R_s$. Nếu $R_s < C_s$ thì dung lượng của kênh nghe lén sẽ yếu hơn so với mức ước lượng của thiết bị phát, do đó mã hóa được sử dụng bởi thiết bị phát sẽ đảm bảo bảo mật thông tin cho truyền thông. Ngược lại $R_s > C_s$, theo nguyên lý bảo mật dựa trên lý thuyết thông tin thì tính bảo mật thông tin sẽ bị phá vỡ và thiết bị nghe lén của thể thu và giải mã thành công các bản tin được truyền đi từ máy phát. Từ các tham số đánh giá hiệu năng bảo mật của hệ thống trên, có thể thấy rằng để tăng dung lượng bảo mật của hệ thống ta

có thể tăng dung lượng kênh của kênh chính. Điều này có thể thực hiện một cách đơn giản là tăng công suất nguồn phát. Tuy nhiên, việc này cũng đồng nghĩa với việc tăng khả năng thu tín hiệu của các thiết bị nghe lén. Do đó để đảm bảo tính bảo mật thông tin trong truyền thông thì hệ thống cần có những giải pháp tối ưu hóa dung lượng kênh và hạn chế tối đa dung lượng của kênh nghe lén. Đó là những yêu cầu và thách thức của hướng nghiên cứu bảo mật thông tin lớp vật lý của mạng thông tin di động.

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 (có thể lên tới hàng ngàn) ăng-ten ở trạm gốc để phục vụ đồng thời nhiều (có thể lên tới hàng chục) thuê bao di động trên cùng một tài nguyên tần số [53, 52]. Kỹ thuật này là một trong những công nghệ chủ chốt cho các mạng thông tin di động 5G và 6G nhờ vào các tiềm năng như cải thiện hiệu quả sử dụng phổ tần và hiệu quả sử dụng năng lượng với sự triển khai chi phí thấp‘[48]. Tuy nhiên, bên cạnh các lợi ích tiềm năng này, kỹ thuật Massive MIMO cũng đặt ra các thách thức kỹ thuật mới cần phải vượt qua khi có thể áp dụng rộng rãi trong thực tế. Một số lợi ích cụ thể của hệ thống Massive MIMO như sau [52],[48],[74],[11]:

- Hệ thống Massive MIMO có thể tăng công suất từ 10 lần trở lên và đồng thời cải thiện hiệu suất năng lượng gấp 100 lần. Việc tăng công suất là kết quả của việc tối ưu ghép kênh không gian trong massive MIMO. Nguyên tắc cơ bản làm tăng đáng kể hiệu quả năng lượng có thể là với số lượng ăng ten lớn, năng lượng có thể được tập trung vào các vùng nhỏ

trong không gian.

- Hệ thống Massive MIMO có thể giảm đáng kể độ trễ trong truyền thông không dây. Tuy nhiên, hiệu suất của các hệ thống này thường bị hạn chế bởi hiện tượng pha-đinh, một hiện tượng có thể làm giảm cường độ tín hiệu tại một số thời điểm. Hiện tượng này xảy ra khi tín hiệu được gửi từ trạm gốc đi qua nhiều đường trước khi đến thiết bị đầu cuối, và tín hiệu này bị triệt tiêu do giao thoa với nhau. Điều này làm cho việc xây dựng các hệ thống truyền thông không dây có độ trễ thấp trở nên khó khăn. Nếu thiết bị đầu cuối bị ảnh hưởng bởi pha-đinh, nó phải chờ đợi cho đến khi kênh truyền thay đổi để có thể nhận dữ liệu. Tuy nhiên, 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. Theo luật số lớn, kênh gia cố để lập lịch cho việc sử dụng tần số. Với ghép kênh phân chia theo tần số trực giao OFDM, mỗi sóng mang con trong một hệ thống Massive MIMO về cơ bản sẽ có cùng một kênh. Mỗi thiết bị đầu cuối có thể được cung cấp toàn bộ băng thông, hoàn lại hầu hết các tín hiệu điều khiển dự phòng ở lớp vật lý.

- Massive MIMO làm gia tăng sự can thiệp của con người tạo ra và để cố ý gây nhiễu. Cố ý gây nhiễu hệ thống không dây ngày càng được chú ý và là mối đe dọa an ninh mạng nghiêm trọng. Thiết bị gây nhiễu,giả lập và thậm chí tắt hệ thống có thể được mua một cách dễ dàng.

- Do sự khan hiếm của băng thông, việc truyền thông tin theo tần số là

không khả thi. Vì vậy, cách duy nhất để cải thiện hiệu năng của mạng thông tin di động là sử dụng nhiều ăng-ten. Massive MIMO có khả năng cung cấp vượt mức có thể để hủy bỏ tín hiệu từ thiết bị gây nhiễu cố ý. Nếu Massive MIMO được triển khai bằng cách sử dụng các hoa tiêu đường lên để ước lượng kênh, sau đó thiết bị gây nhiễu thông minh có thể gây nhiễu với công suất truyền nhỏ hơn. Tuy nhiên, việc thực hiện bằng cách sử dụng chung ước lượng kênh và giải mã sẽ có thể làm giảm đáng kể vấn đề đó.

1.4.2. Thách thức của hệ thống Massive MIMO

Công nghệ MIMO đang trở nên hoàn thiện và được kết hợp thành chuẩn băng thông rộng không dây mới nổi như LTE. Về cơ bản, càng được trang bị nhiều ăng ten máy phát / máy thu, và mức độ tự do truyền thông tin thì hiệu suất tốt hơn cả về tốc độ dữ liệu và độ tin cậy của kênh truyền. Tuy nhiên, Công nghệ MIMO đòi hỏi sự phức tạp của phần cứng, năng lượng tiêu thụ xử lý tín hiệu, không gian vật lý để chứa ăng ten. Ngày nay, khi lưu lượng dữ liệu di động tăng theo cấp số nhân, cần tăng cường thêm dung lượng. Là một giải pháp cho nhu cầu công suất cao, Massive MIMO đã được nghiên cứu rộng rãi trong vài năm qua. Massive MIMO sử dụng hàng trăm ăng-ten tại trạm gốc phục vụ đồng số lượng nhỏ hơn nhiều của thiết bị đầu cuối. Số lượng thiết bị đầu cuối có thể được phục vụ đồng thời bị giới hạn. Với số lượng ăng-ten không giới hạn, công suất phát có thể được tạo ra nhỏ tùy ý và nhiễu có thể hạn chế tối đa hoặc biến mất, nhưng hiệu suất lại bị hạn chế bởi vấn đề nhiễu hoa tiêu [74]. 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 [52, 48, 75]. Ví dụ, 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. Về cơ bản, đảm bảo an toàn thông tin là một thách thức lớn không chỉ đối với riêng mạng thông tin Massive 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 [61, 18, 30, 41, 43, 42, 44, 87, 89, 96, 97, 106]. Có nhiều giải pháp kỹ thuật đang được nghiên cứu để giải quyết thách thức kỹ thuật này. Từ đó đề xuất các giải pháp kỹ thuật ở lớp vật lý để tăng cường tính bảo mật thông tin cho các mạng thông tin di động thế hệ mới, đặc biệt các mạng thông tin MIMO sử dụng rất nhiều ăng-ten ở trạm gốc, để làm tiền đề cho quá trình áp dụng vào thực tiễn. Xuất phát từ bốn ưu điểm cơ bản của mạng MU-MIMO truyền thống [48]:

- Tốc độ dữ liệu tăng lên, bởi vì càng nhiều ăng-ten, các luồng dữ liệu độc lập hơn có thể được gửi đi và nhiều thiết bị đầu cuối có thể được phục vụ đồng thời.
- 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.

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. Công nghệ MU-MIMO truyền thống cho mạng thông tin di động đang phát triển và được tích hợp vào gần đây và phát triển các chuẩn băng thông rộng không dây như 4G LTE và LTE-A. Càng nhiều ăng-ten hơn tại trạm gốc (hoặc thiết bị đầu cuối) thì hiệu suất tốt hơn ở chế độ song công phân chia theo thời gian. Tuy nhiên, số lượng ăng-ten được sử dụng hiện nay là hạn chế. Với hệ thống Massive MIMO sử dụng mảng ăng-ten với vài trăm ăng-ten, đồng thời phục vụ hàng chục thiết bị đầu cuối trong cùng một tài nguyên tần số. Điều này phát huy được những lợi ích của MIMO thông thường, nhưng trên quy mô lớn hơn nhiều. Nhìn chung, Massive MIMO là một yếu tố thúc đẩy sự phát triển của băng thông rộng trong tương lai (mạng cố định và di động) vì tiết kiệm năng lượng, an toàn, sử dụng phổ một cách hiệu quả hơn. Như vậy, Massive MIMO là một yếu tố hỗ trợ cho cơ sở hạ tầng IoT. Nhiều cấu hình và kịch bản triển khai khác nhau cho các mảng ăng ten thực tế được sử dụng bởi một hệ thống Massive MIMO. Massive MIMO dựa vào ghép kênh không gian và trạm gốc có đủ thông tin về kênh truyền, cả trên đường lên và đường xuống. Trên đường lên, trạm gốc dễ dàng để thực hiện bằng cách yêu cầu các thiết bị đầu cuối gửi hoa tiêu, dựa vào đó ước lượng kênh đáp ứng với từng thiết bị đầu cuối. Đường xuống thì sẽ khó khăn hơn trong môi trường có có tính di động cao. Trong các hệ thống MIMO thường, giống như tiêu chuẩn LTE, trạm gốc gửi các hoa tiêu thí điểm dựa trên đó các thiết bị đầu cuối lượng kênh, định lượng các ước tính thu được và gửi trở lại trạm gốc. Điều này sẽ không khả thi trong các hệ thống Massive MIMO, vì hai lý do.

- Kênh đối xứng

Cơ chế song công phân chia theo thời gian 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. Tuy nhiên, hệ thống các phần cứng trong trạm phát và thiết bị đầu cuối có thể không đối xứng giữa đường lên và đường xuống.

Đầu tiên, đường xuống tối ưu các hoa tiêu trực giao lẫn nhau giữa các ăng-ten. Điều này có nghĩa là thời gian cần thiết cho các hoa tiêu đường xuống lớn như số lượng ăng-ten, vì vậy với hệ thống Massive MIMO sẽ yêu cầu tài nguyên gấp hàng trăm lần so với tài nguyên hệ thống thông thường.

Thứ hai, số lượng phản hồi kênh mà mỗi thiết bị đầu cuối phải ước tính cũng là tỷ lệ thuận với số lượng ăng-ten trạm gốc. Do đó, thời gian mà đường lên cần thiết để thông báo cho trạm gốc về các phản hồi của kênh sẽ lớn hơn gấp trăm lần trong các hệ thống thông thường. Nói chung, giải pháp là hoạt động ở chế độ TDD và dựa vào về tính tương hỗ giữa các kênh đường lên và kênh đường xuống. Mặc dù chế độ song công phân chia theo tần số FDD có thể là có thể trong một số trường hợp nhất định [62].

- Nhiễu hoa tiêu

  Trước đây các nhà nghiên cứu đã xem xét vấn đề ở trường hợp đơn tế bào. Tuy nhiên, thực tế mạng bao gồm đa tế bào. Do phổ tần có sẵn còn hạn chế, mạng đa tế bào phải chia sẻ cùng một tài nguyên tần số. Do đó, một số vấn đề trên hệ tống đa tế bào cần được xem xét. 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. Vì thế, ước lượng kênh thu được trong một tế bào nhất định sẽ bị nhiễu bởi các hoa tiêu truyền dẫn tới người dùng trong các tế bào khác. Hiện tượng này, được gọi là nhiễu hoa tiêu, làm giảm hiệu suất hệ thống [41, 60, 18]. Tác động của nhiễu hoa tiêu là một hạn chế lớn vốn có của Massive MIMO. Nó không biến mất ngay cả khi số lượng ăng-ten tại BS tăng không giới hạn. Những nỗ lực đáng kể đã được thực hiện để làm giảm hiệu ứng này. Ước lượng kênh dựa trên phân tách giá trị riêng, khử nhiễu hoa tiêu, chẳng hạn như cũng như các chương trình tiền mã hóa bị giảm nhiễu được đề xuất trong [60, 63]. Bảo đảm an toàn thông tin trong nhiễu hoa tiêu cũng là một chủ đề được nhiều nhà khoa học đã và đang nghiên cứu.

- Phần cứng không hoàn hảo

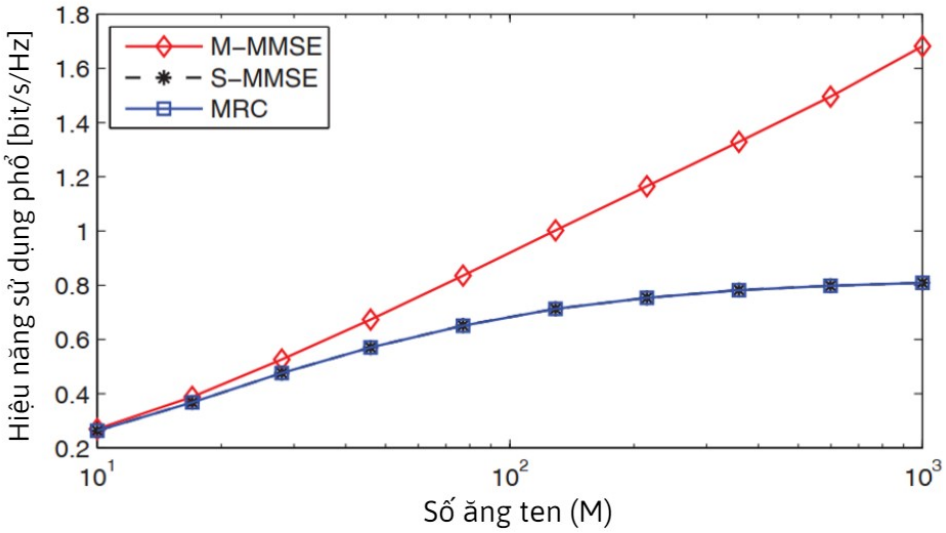
  Massive MIMO dựa trên luật số lớn đến trung bình, chịu sự can thiệp của nhiễu, pha-đinh ở một mức độ nào đó. Trong thực tế, Massive MIMO phải được được xây dựng với các thành phần với chi phí thấp. Điều này có thể có nghĩa là sự không hoàn hảo của phần cứng ngày càng lớn, đặc biệt là nhiễu pha và mất cân bằng pha của những phần cứng với chi phí thấp và tiết kiệm năng lượng, bộ chuyển đổi mang có độ nhiễu lượng tử hóa cao hơn. Bộ khuếch đại công suất sẽ bắt buộc phải sử dụng tín hiệu từ mức thấp đến trung bình trên mỗi ăng ten, là khả thi với lượng lớn ăng-ten máy phát. Với các vòng khóa pha chi phí thấp hoặc các bộ dao động tự do ở mỗi ăng-ten, có thể hạn chế nhiễu pha. Tuy nhiên, điều quan trọng là giai đoạn là thời điểm khi nhận được hoa tiêu và thời điểm

khi một tín hiệu dữ liệu nhận được tại mỗi ăng ten. Đây là chủ đề có tiềm năng lớn để nghiên cứu thiết kế các sơ đồ và bộ thu vật lý truyền thông thông minh thuật toán về nhiễu pha. Ngoài các vấn đề trên còn một số vấn đề đã và đang được các nhà nghiên cứu quan tâm như xử lý tín hiệu cần nhanh chóng và chuẩn xác, thách thức trong sử dụng phần cứng giá rẻ, vấn đề tiêu thụ năng lượng, không có thông tin trạng thái kênh truyền.

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. Trong cuốn sách [54], các tác giả đưa ra định nghĩa như sau: “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."

Có nhiều định nghĩa khác như sau về Massive MIMO , nhưng có định nghĩa được sử dụng phổ biến trong sách [9] "Massive MIMO là một hệ thống MIMO đa người dùng với M ăng ten tại trạm gốc và phục vụ một số người dùng K. Hệ thống được đặc trưng bởi $M \gg K$ và hoạt động ở chế độ TDD đối xứng hoàn hảo ở cả đường lên và đường xuống.” Lưu ý rằng định nghĩa



Hình 1.1: Hiệu năng sử dụng phổ của hệ thống Massive MIMO với số ăng-ten lớn. [10]

này không yêu cầu số lượng người dùng phải nhỏ theo bất kỳ nghĩa nào. Vì vậy, đối với câu hỏi lớn: Một trạm gốc cần bao nhiêu ăng-ten để trở nên vô cùng lớn "massive" ? Câu trả lời được đưa ra trong các nghiên cứu [10, 35, 64, 53] Các tác giả tập trung vào kênh đường lên và chứng minh rằng 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. Mô tả cụ thể các pha như sau:

- Pha huấn luyện đường lên: các thuê bao gửi tín hiệu hoa tiêu đường lên đã được quy định trước để trạm gốc ước lượng kênh truyền. Việc ước lượng kênh truyền cần phần chính xác để trạm gốc có thể tạo búp sóng

sao cho năng lượng sóng vô tuyến được tập trung vào đúng vị trí của thuê bao hợp lệ. Nói cách khác, nếu việc ước lượng kênh truyền không chính xác sẽ giảm công suất tín hiệu mong muốn và tăng công suất nhiễu đến các thuê bao khác.

- Pha truyền dữ liệu đường xuống

  Trạm gốc truyền dữ liệu đến các thuê bao. Ngoài tín hiệu mong muốn, mỗi thuê bao sẽ có thể nhận các tín hiệu không mong muốn, có thể từ trạm gốc nhưng dành cho thuê bao khác hoặc từ các nguồn phát tín hiệu ngoài.

- Pha truyền dữ liệu đường lên

  Các thuê bao truyền dữ liệu tới trạm gốc. Trạm gốc phải tách dữ liệu ứng với từng thuê bao để xử lý tiếp. Việc tách tín hiệu này có thể bị ảnh hưởng bởi dữ liệu ứng với các thuê bao khác hoặc bởi tín hiệu được truyền từ các nguồn phát tín hiệu ngoài.

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, đặc biệt các hệ thống hoạt động ở môi trường vô tuyến. Do đặc tính mở của môi trường truyền dẫn sóng vô tuyến, các thiết bị không hợp lệ, có thể làm ảnh ảnh hưởng đến tính bảo mật, tính toàn vẹn và tính sẵn có của thông tin 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. Về nguyên lý, thiết bị nghe

lén thụ động không thể bị phát hiện và thiết bị nghe lén thụ động cố gắng nghe tín hiệu đường xuống truyền từ trạm gốc tới một thuê bao hợp lệ.

- 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 và làm ảnh hưởng đến quá trình huấn luyện và ước lượng kênh và/ hoặc quá trình truyền dữ liệu giữa các thiết bị hợp lệ. Sự tác động này làm giảm hiệu năng hoạt động của hệ thống hợp lệ, thậm chí khiến hệ thống không thể hoạt động được. Trong hệ thống tấn công chủ động. Thiết bị tấn công chủ động sẽ đóng vai trò nguồn phát tín hiệu ngoài để truyền tín hiệu không mong muốn trong một trong ba pha được mô tả ở trên. Dù tác động ở pha nào thì thiết bị tấn công chủ động cũng sẽ làm ảnh hưởng tiêu cực tới hiệu năng hoạt động của hệ thống.

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, các tham số đánh giá dung lượng bảo mật của hệ thống để từ đó đưa ra giải pháp đảm bảo an toàn thông tin. Những vấn đề này là nền tảng để nghiên cứu sinh tìm hiểu, nghiên cứu sâu hơn và đưa ra những biện pháp nâng cao tính bảo mật của hệ thống Massive MIMO.

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. Do đặc tính mở của môi trường truyền dẫn sóng vô tuyến, các thiết bị xâm nhập không hợp lệ có thể làm ảnh hưởng đến tính bảo mật, tính toàn vẹn và sẵn có của thông tin bằng một trong 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. *Đóng góp của Chương 2 được trình bày trong công trình số 1,2.*

- **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.
- **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.

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. Theo định nghĩa, dung lượng bảo mật của hệ thống bằng hiệu số của tốc độ dữ liệu đạt được ở thiết bị thu hợp lệ và tốc độ dữ liệu nghe lén ở thiết bị nghe lén thụ động nếu hiệu số này không âm và bằng không nếu hiệu số này âm. Các kết quả nghiên cứu trước đây liên quan đến hệ thống chỉ có một thiết bị nghe lén thụ động giả thiết mô hình kênh pha-đinh Rayleigh, tức là giả thiết hệ số kênh truyền chỉ có thành phần không tầm nhìn thẳng NLOS. Các kết quả phân tích và mô phỏng với mô hình kênh pha-đinh Rayleigh khẳng định thiết bị nghe lén thụ động gần như không thể tách được tín hiệu từ trạm gốc, nếu số lượng ăng-ten tại trạm gốc đủ lớn [42]. Nói cách khác, dung lượng bảo mật của hệ thống sẽ tăng theo số lượng ăng-ten tại trạm gốc. Về lý thuyết, mô hình kênh pha-đinh Rice được giả thiết trong nghiên cứu này tổng quát hơn mô hình kênh pha-đinh Rayleigh vì có thêm thành phần truyền tầm nhìn thẳng LOS. [68, 38]. 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. Giả thiết cấu trúc khung vô tuyến đã được định trước và gồm có hai phần: i) phần đầu gồm τ_{p} dành cho quá trình huấn luyện và ước lượng hệ số kênh truyền đường lên và ii) phần còn lại dài $\tau_{\mathrm{d}} = \tau - \tau_{\mathrm{p}}$ ký hiệu được dùng để truyền dữ liệu đường xuống từ trạm gốc A tới thuê bao B.

Giả thiết kênh truyền vô tuyến có dạng pha đinh khối phẳng trên miền tần số, trong đó hệ số kênh truyền không thay đổi trong thời gian của một khung vô tuyến nhưng có thể thay đổi một cách độc lập từ khung vô tuyến này sang khung vô tuyến khác. Ký hiệu $\mathbf{h}_{\mathrm{B}} \in \mathbb{C}^{M\times 1}$ là vector hệ số kênh truyền đường lên từ thuê bao tới trạm gốc và $\mathbf{h}_{\mathrm{E}} \in \mathbb{C}^{M\times 1}$ là vec to hệ số kênh truyền đường lên từ thiết bị nghe lén tới trạm gốc. Giả thiết hệ số kênh truyền ở đường lên và đường xuống đối xứng hoàn hảo, tức là $\mathbf{h}_{\mathrm{B}}^{H}$, $\mathbf{h}_{\mathrm{E}}^{H} \in \mathbb{C}^{1\times M}$ là các vec tơ hệ số kênh truyền đường xuống tương ứng. Chúng ta giả thiết hệ số kênh truyền

tuân theo mô hình pha-đinh Rice không tương quan về không gian. Ký hiệu κ_X là hệ số Rice và β_{X} là hệ số pha-đinh phạm vi rộng của kênh truyền từ trạm gốc tới nút $\mathrm{X} \in \mathcal{X}$. 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

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

$$\alpha(\phi_{\mathrm{B}}, \phi_{\mathrm{E}}, M) = \frac{\sin(M\psi(\phi_{\mathrm{B}}, \phi_{\mathrm{E}}))}{\sin(\psi(\phi_{\mathrm{B}}, \phi_{\mathrm{E}}))}. \tag{2.5}$$

Sau một số phép biến đổi ta có

$$\mathbf{g}_{\mathrm{E}}^{H}\mathbf{g}_{\mathrm{B}} = \beta_{\mathrm{B,L}}^{1/2}\beta_{\mathrm{E,L}}^{1/2}e^{j\psi(\phi_{\mathrm{B}},\phi_{\mathrm{B}})}\alpha(\phi_{\mathrm{B}},\phi_{\mathrm{E}},M). \tag{2.6}$$

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

$$\mathbf{y}_{\mathrm{A}} = \sqrt{p_{\mathrm{p}}}\tau_{\mathrm{p}}\mathbf{h}_{\mathrm{B}} + \mathbf{n}_{\mathrm{A}}. \tag{2.7}$$

trong đó $\mathbf{n}_{\mathrm{A}} \sim \mathcal{CN}(\mathbf{0}, \sigma_{\mathrm{A}}^2\mathbf{I}_M)$ 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:

$$\hat{\mathbf{h}}_{\mathrm{B}} = \mathbf{g}_{\mathrm{B}} + \frac{\sqrt{p_{\mathrm{p}}}\beta_{\mathrm{B,N}}}{p_{\mathrm{p}}\tau_{\mathrm{p}}\beta_{\mathrm{B,N}} + \sigma_{\mathrm{A}}^2}(\mathbf{y}_{\mathrm{A}} - \sqrt{p_{\mathrm{p}}}\tau_{\mathrm{p}}\mathbf{g}_{\mathrm{B}}). \tag{2.8}$$

Theo tính chất trực giao của phương pháp MMSE, sai số ước lượng tương ứng là:

$$\tilde{\mathbf{h}}_{\mathrm{B}} = \mathbf{h}_{\mathrm{B}} - \hat{\mathbf{h}}_{\mathrm{B}}. \tag{2.9}$$

Chú ý rằng $\hat{\mathbf{h}}_{\mathrm{B}} \sim \mathcal{CN}(\mathbf{g}_{\mathrm{B}}, \hat{\beta}_{\mathrm{B,N}}\mathbf{I}_M)$ và $\tilde{\mathbf{h}}_{\mathrm{B}} \sim \mathcal{CN}(\mathbf{0}, \tilde{\beta}_{\mathrm{B,N}}\mathbf{I}_M)$ độc lập thống kê với nhau trong đó

$$\hat{\beta}_{\mathrm{B,N}} = \frac{p_{\mathrm{p}}\tau_{\mathrm{p}}\beta_{\mathrm{B,N}}^2}{p_{\mathrm{p}}\tau_{\mathrm{p}}\beta_{\mathrm{B,N}} + \sigma_{\mathrm{A}}^2}; \quad \tilde{\beta}_{\mathrm{B,N}} = \frac{\beta_{\mathrm{B,N}}\sigma_{\mathrm{A}}^2}{p_{\mathrm{p}}\tau_{\mathrm{p}}\beta_{\mathrm{B,N}} + \sigma_{\mathrm{A}}^2}. \tag{2.10}$$

Bên cạnh đó, ta có thể biểu diễn $\hat{\mathbf{h}}_{\mathrm{B}}$ và $\tilde{\mathbf{h}}_{\mathrm{B}}$ như sau

$$\hat{\mathbf{h}}_{\mathrm{B}} = \mathbf{g}_{\mathrm{B}} + \hat{\beta}_{\mathrm{B,N}}^{1/2}\hat{\mathbf{w}}_{\mathrm{B}}; \quad \tilde{\mathbf{h}}_{\mathrm{B}} = \tilde{\beta}_{\mathrm{B,N}}^{1/2}\tilde{\mathbf{w}}_{\mathrm{B}} \tag{2.11}$$

trong đó $\hat{\mathbf{w}}_{\mathrm{B}}$ và $\tilde{\mathbf{w}}_{\mathrm{B}}$ có cùng phân bố $\mathcal{CN}(\mathbf{0}, \mathbf{I}_M)$ và độc lập thống kê với nhau.

Trong pha truyền dữ liệu đường xuống, trạm gốc truyền tín hiệu x_{B}, trong đó $\mathbb{E}[x_{\mathrm{B}}] = 0, \mathbb{E}[|x_{\mathrm{B}}|^2] = 1$, tới nút B, nhưng bị nút E nghe lén. Ký hiệu p_{d}

là công suất phát ở đường xuống. Giả thiết trạm gốc sử dụng bộ tiền mã hóa kết hợp phát cực đại (MRT) có biểu thức

$$\mathbf{f}_{\mathrm{B}} = \frac{\hat{\mathbf{h}}_{\mathrm{B}}}{\xi}. \tag{2.12}$$

trong đó $\xi^2 = \mathbb{E}[\hat{\mathbf{h}}_{\mathrm{B}}^H \hat{\mathbf{h}}_{\mathrm{B}}] = (\beta_{\mathrm{B,L}} + \hat{\beta}_{\mathrm{B,N}})M$ là hệ số chuẩn hoá nhằm thỏa mãn điều kiện công suất phát trung bình cực đại tại trạm gốc $\mathbb{E}[|\mathbf{f}_{\mathrm{B}} x_{\mathrm{B}}|^2] \leq p_{\mathrm{d}}$. Tín hiệu thu được ở nút B và nút E lần lượt là

$$y_{\mathrm{B}} = \sqrt{p_{\mathrm{f}}} \mathbf{h}_{\mathrm{B}}^H \mathbf{f}_{\mathrm{B}} x_{\mathrm{B}} + n_{\mathrm{B}}. \tag{2.13}$$

$$y_{\mathrm{E}} = \sqrt{p_{\mathrm{f}}} \mathbf{h}_{\mathrm{E}}^H \mathbf{f}_{\mathrm{B}} x_{\mathrm{B}} + n_{\mathrm{E}}. \tag{2.14}$$

trong đó $n_{\mathrm{B}} \sim \mathcal{CN}(0, \sigma_{\mathrm{B}}^2)$ và $n_{\mathrm{E}} \sim \mathcal{CN}(0, \sigma_{\mathrm{E}}^2)$ 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

$$C_{\mathrm{SC}} = [R_{\mathrm{B}} - R_{\mathrm{E}}]^+. \tag{2.15}$$

trong đó $[x]^+ = \max x, 0$, R_{B} là tốc độ dữ liệu hợp lệ đạt được ở nút B và R_{E} là tốc độ dữ liệu nghe lén đạt được ở nút E. Mục 2.3.2 trình bày chi tiết phân tích tốc độ dữ liệu đạt được ở nút B trong khi Mục 2.3.3 trình bày chi tiết phân tích tốc độ dữ liệu đạt được ở nút B.

Chú ý rằng trạm gốc không truyền tín hiệu hoa tiêu đường xuống nên nút B và nút E không thể ước lượng hệ số kênh đường xuống tức thời. Trong

phần này, chúng ta chấp thuận phương pháp tiếp cận thường được sử dụng trong các tài liệu trước đây trong đó các nút này chỉ ước lượng được hệ số kênh truyền đường xuống hiệu dụng trung bình [40]. Cụ thể, nút B chỉ có được thông tin trạng thái kênh ở dạng $\mathbb{E}[\mathbf{h}_{\mathrm{B}}^{H}\mathbf{f}_{\mathrm{B}}]$. Tương tự, nút E chỉ có được thông tin trạng thái kênh ở dạng $\mathbb{E}[\mathbf{h}_{\mathrm{E}}^{H}\mathbf{f}_{\mathrm{B}}]$. Ngoài ra, Bổ đề sau đây sẽ được sử dụng nhiều trong quá trình xây dựng công thức giải tích dạng tường minh cho tốc độ dữ liệu đạt được ở nút B và nút E.

Bổ đề 2.3.1 *Cho* $\mathbf{a} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_M)$ *và ma trận chuẩn tắc* $\mathbf{B}$ *(tức là* $\mathbf{B}$ *thoả mãn điều kiện* $\mathbf{BB^H} = \mathbf{B}^H\mathbf{B}$*). Khi đó ta có*

$$\mathbb{E}[\mathbf{a}^H\mathbf{B}\mathbf{a}] = \mathrm{tr}\mathbf{B}. \tag{2.16}$$

$$\mathbb{E}[|\mathbf{a}^H\mathbf{B}\mathbf{a}|^2] = |\mathrm{tr}(\mathbf{B})|^2 + \mathrm{tr}(\mathbf{B}\mathbf{B}^H). \tag{2.17}$$

2.3.2. Tốc độ dữ liệu hợp lệ

Từ công thức (2.13) ta có thể viết lại biểu thức tín hiệu thu tại nút B như sau

$$y_{\mathrm{B}} = \sqrt{p_{\mathrm{d}}}\mathbb{E}[\mathbf{h}_{\mathrm{B}}^{H}\mathbf{f}_{\mathrm{B}}]x_{\mathrm{B}} + \sqrt{p_{\mathrm{d}}}(\mathbf{h}_{\mathrm{B}}^{H}\mathbf{f}_{\mathrm{B}} - \mathbb{E}[\mathbf{h}_{\mathrm{B}}^{H}\mathbf{f}_{\mathrm{B}}])x_{\mathrm{B}} + n_{\mathrm{B}}. \tag{2.18}$$

trong đó số hạng đầu tiên đóng vai trò là tín hiệu mong muốn để tách sóng kết hợp, số hạng thứ hai đóng vai trò nhiễu gây ra do sai số ước lượng hệ số kênh truyền đường xuống hiệu dụng và số hạng cuối cùng là tạp âm nhiệt. Để tìm một giới hạn dưới cho tỷ số công suất tín hiệu trên tổng công suất nhiễu và tạp âm SINR, ta xét trường hợp xấu nhất xảy ra khi số hạng thứ hai và số hạng thứ ba là các tín hiệu không tương quan. Khi đó, một giới hạn

dưới của SINR tại nút B được ký hiệu là η_{B} và được xác định như sau

$$\eta_{\mathrm{B}} = \frac{p_{\mathrm{d}}|\mathbb{E}[\mathbf{h}_{\mathrm{B}}^H \mathbf{f}_{\mathrm{B}} x_{\mathrm{B}}]|^2}{p_{\mathrm{d}}\mathbb{E}[|(\mathbf{h}_{\mathrm{B}}^H \mathbf{f}_{\mathrm{B}} - \mathbb{E}[\mathbf{h}_{\mathrm{B}}^H \mathbf{f}_{\mathrm{B}}])x_{\mathrm{B}}|^2] + \sigma_{\mathrm{B}}^2} \tag{2.19}$$

$$= \frac{p_{\mathrm{d}}|\mathbb{E}[\mathbf{h}_{\mathrm{B}}^H \mathbf{f}_{\mathrm{B}}]|^2}{p_{\mathrm{d}}(\mathbb{E}[|\mathbf{h}_{\mathrm{B}}^H \mathbf{f}_{\mathrm{B}}|^2] - |\mathbb{E}[\mathbf{h}_{\mathrm{B}}^H \mathbf{f}_{\mathrm{B}}]|^2) + \sigma_{\mathrm{B}}^2}. \tag{2.20}$$

Bổ đề 2.3.2 *Giá trị SINR hợp lệ η_{B} tỷ lệ tuyến tính với số ăng-ten tại trạm gốc M.*

Tốc độ dữ liệu đạt được tương ứng ở nút B hay thuê bao hợp lệ được định nghĩ như sau

$$R_{\mathrm{B}} = \log_2(1 + \eta_{\mathrm{B}}) = \log_2(1 + \bar{\eta_{\mathrm{B}}} M). \tag{2.21}$$

2.3.3. Tốc độ dữ liệu nghe lén đạt được

Từ công thức (2.14) ta có thể viết lại biểu thức tín hiệu thu tại nút E như sau

$$y_{\mathrm{E}} = \sqrt{p_{\mathrm{d}}}\mathbb{E}[\mathbf{h}_{\mathrm{E}}^H \mathbf{f}_{\mathrm{B}}]x_{\mathrm{B}} + \sqrt{p_{\mathrm{d}}}(\mathbf{h}_{\mathrm{E}}^H \mathbf{f}_{\mathrm{B}} - \mathbb{E}[\mathbf{h}_{\mathrm{E}}^H \mathbf{f}_{\mathrm{B}}])x_{\mathrm{B}} + n_{\mathrm{E}}. \tag{2.22}$$

Khi đó, một giới hạn dưới của SINR tại nút E được ký hiệu là η_{E} và được xác định như sau

$$\eta_{\mathrm{E}} = \frac{p_{\mathrm{d}}|\mathbb{E}[\mathbf{h}_{\mathrm{E}}^H \mathbf{f}_{\mathrm{B}} x_{\mathrm{B}}]|^2}{p_{\mathrm{d}}\mathbb{E}[|(\mathbf{h}_{\mathrm{E}}^H \mathbf{f}_{\mathrm{B}} - \mathbb{E}[\mathbf{h}_{\mathrm{E}}^H \mathbf{f}_{\mathrm{B}}])x_{\mathrm{B}}|^2] + \sigma_{\mathrm{B}}^2} \tag{2.23}$$

$$= \frac{p_{\mathrm{d}}|\mathbb{E}[\mathbf{h}_{\mathrm{E}}^H \mathbf{f}_{\mathrm{B}}]|^2}{p_{\mathrm{d}}(\mathbb{E}[|\mathbf{h}_{\mathrm{E}}^H \mathbf{f}_{\mathrm{B}}|^2] - |\mathbb{E}[\mathbf{h}_{\mathrm{E}}^H \mathbf{f}_{\mathrm{B}}]|^2) + \sigma_{\mathrm{B}}^2}. \tag{2.24}$$

Bổ đề 2.3.3 *Giá trị SINR nghe lén η_E được xác định bởi biểu thức sau*

$$\eta_{\mathrm{E}} = \bar{\eta}_{\mathrm{E}} \frac{|\alpha(\phi_{\mathrm{B}}, \phi_{\mathrm{E}}, M)|^2}{M}. \tag{2.25}$$

trong đó

$$\bar{\eta}_{\mathrm{E}} = \frac{p_{\mathrm{d}}\beta_{\mathrm{E,L}}\beta_{\mathrm{B,L}}}{p_{\mathrm{d}}\rho_{\mathrm{E}} + \sigma_{\mathrm{E}}^2(\beta_{\mathrm{B,L}} + \hat{\beta}_{\mathrm{B,N}})}. \tag{2.26}$$

Tốc độ dữ liệu đạt được tương ứng ở nút B hay thuê bao hợp lệ được định nghĩ như sau

$$R_{\mathrm{E}} = \log_2(1 + \eta_{\mathrm{E}}). \tag{2.27}$$

Phần này tập trung khảo sát và thảo luận một số tính chất của tốc độ dữ liệu hợp lệ đạt được tại nút B (tức là R_{B} được xác định bởi (2.21)) và tốc độ dữ liệu nghe lén đạt được tại nút E (tức là R_{E} được xác định bởi (2.27)) cũng như dung lượng bảo mật của hệ thống C_{SC} được xác định bởi (2.15). Cụ thể, Bổ đề 2.3.5 và Bổ đề 2.3.4 trình bày tính chất của giá trị SINR tại thiết bị nghe trộm η_{E} và dung lượng bảo mật của hệ thống C_{SC} trong các điều kiện khác nhau về quan hệ giữa Φ_{E} và Φ_{B}. Để tiện cho việc thảo luận, ký hiệu chênh lệch góc tới của thuê bao hợp lệ B và thiết bị nghe trộm B là $\Delta\Phi = |\Phi_{\mathrm{B}} - \Phi_{\mathrm{E}}|$.

Bổ đề 2.3.4 *Nếu $\Delta\Phi = 0$ thì η_{E} tỷ lệ tuyến tính với M. Ngoài ra thêm điều kiện, nếu M đủ lớn thì dung lượng bảo mật của hệ thống được xấp xỉ như sau*

$$C_{\mathrm{SC}} \approx \log_2(\bar{\eta}_{\mathrm{B}}/\bar{\eta}_{\mathrm{E}}). \tag{2.28}$$

Có thể thấy rằng khi thiết bị nghe lén và thiết bị thu hợp lệ có cùng góc tới đến trạm gốc (trên không gian hai chiều), tức là $\Phi_{\mathrm{E}} = \Phi_{\mathrm{B}}$, thì dung lượng bảo mật của hệ thống C_{SC} chỉ phụ thuộc vào các tham số pha-đinh phạm vi lớn và các tham số công suất nhưng không phụ thuộc vào số lượng ăng-ten tại trạm gốc M hay các góc tới Φ_{B} và Φ_{E}. Hiện tượng này xảy ra do thành phần truyền tầm nhìn thẳng $\mathbf{g}_{\mathrm{E}}$ và $\mathbf{g}_{\mathrm{B}}$ chỉ sai khác hệ số pha đinh phạm vi lớn nên $\mathbf{h}_{\mathrm{E}}$ và $\mathbf{h}_{\mathrm{B}}$ có tương quan chéo đủ lớn, khiến cho công suất tín hiệu mong muốn hiệu dụng mà thiết bị nghe lén nhận được từ trạm gốc đủ lớn để tách tín hiệu.

Bổ đề 2.3.5 *Nếu* $\Delta\Phi \neq 0$ *thì* $\eta_{\mathrm{E}} \to 0$ *và* $R_{\mathrm{E}} \to 0$ *khi* $M \to \infty$. *Khi đó dung lượng bảo mật* $C_{\mathrm{SC}} \to R_{\mathrm{B}} = \log_2(1 + \bar{\eta}_{\mathrm{B}})$ *khi* M *đủ lớn.*

Biết rằng, các kết quả nghiên cứu trước đây cho điều kiện kênh pha-đinh Rayleigh đã khẳng định rằng thiết bị nghe lén thụ động gần như không thể tách được thông tin phát từ trạm gốc tới thuê bao hợp lệ. Nói cách khác, thiết bị nghe lén thụ động gần như không ảnh hưởng tới dung lượng bảo mật của hệ thống. Lý do cho hiện tượng này là trong điều kiện kênh truyền pha-đinh Rayleigh với M đủ lớn thì $\mathbf{h}_{\mathrm{B}}$ và $\mathbf{h}_{\mathrm{E}}$ không chỉ có hệ số tương quan chéo thấp mà thậm chí còn trực giao với nhau. Chú ý rằng Bổ đề (2.3.5) cũng đưa ra một khẳng định hoàn toàn tương đồng trong điều kiện kênh pha-đinh Rice nếu cả $\Delta\Phi \neq 0$ và M đủ lớn. Có thể giải thích hiện tượng này như sau. Khi cả M đủ lớn thì độ phân giải không gian của mảng ăng-ten tại trạm gốc đủ nhỏ, điều này kết hợp với điều kiện $\Delta\Phi \neq 0$ thì các vec tơ hệ số kênh truyền $\mathbf{h}_{\mathrm{B}}$ và $\mathbf{h}_{\mathrm{E}}$ cũng sẽ có tương quan chéo thấp, khiến cho thiết bị nghe lén gần như không thu được tách được tín hiệu truyền từ trạm gốc.

2.4. Kết quả mô phỏng và tính toán số

Phần này cung cấp một số kết quả mô phỏng và tính toán số để kiểm chứng các kết quả phân tích giải tích đã trình bày ở Mục 2.3. Xét một mạng di động chỉ có một tế bào trong đó trạm gốc được đặt ở chính giữa tế bào trong khi thiết bị đầu cuối hợp lệ (nút B) và thiết bị nghe lén thụ động (nút E) được bố trí ngẫu nhiên trong tế bào. Giả thiết ảnh hưởng của hiệu ứng che chắn bị bỏ qua, khi đó hệ số suy hao đường truyền phạm vi lớn được tính

như sau [1, 72, 78]

$$\beta_{\mathrm{X,Y}} = 32.4 + 10 n_{\mathrm{Y}} \log_{10}(d_{\mathrm{3D,X}}) + 20 \log_{10}(f_{\mathrm{c}})$$

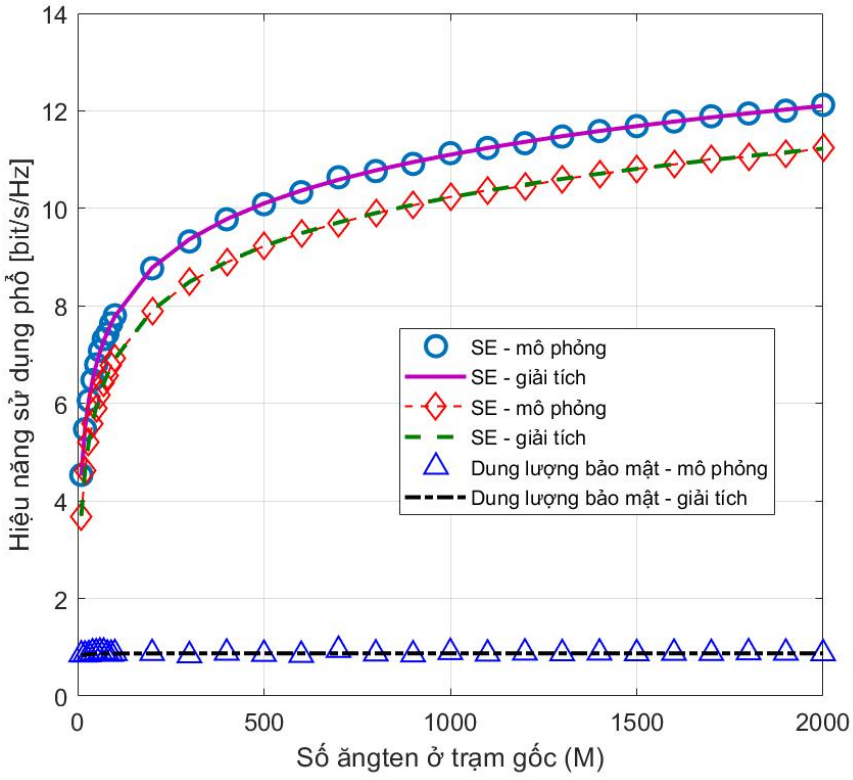
trong đó $X \in \mathcal{X}$, $Y \in \mathcal{Y} = \{\mathrm{L}, \mathrm{N}\}$, $d_{\mathrm{3D,X}}$ là khoảng cách tính theo mét từ trạm gốc đến nút X trong không gian 3 chiều, $f_{\mathrm{c}} = 3.5$ GHz là tần số sóng mang, n_{Y} là hệ số mũ suy hao đường truyền (PLE: path-loss exponent). Ngoài ra, $d_{\mathrm{3D,X}}$ được tính như sau $d_{\mathrm{3D,X}} = \sqrt{d_{\mathrm{2D,X}}^2 + (h_{\mathrm{A}} - h_{\mathrm{X}})^2}$ trong đó $d_{\mathrm{2D,X}}$ là khoảng cách từ trạm gốc tới nút X trong không gian 2 chiều, h_{A} là chiều cao của trạm gốc A, và h_{X} là chiều cao của nút X [1]. Không mất tính tổng quát, giả thiết $h_{\mathrm{A}} = 10$ [m] và $h_{\mathrm{B}} = h_{\mathrm{E}} = 1.5$ [m]. Bài báo xem xét môi trường cell lớn ở đô thị UMa, khi đó $n_{\mathrm{L}} = 2$ cho thành phần truyền tầm nhìn thẳng LOS và $n_{\mathrm{N}} = 2.9$ cho thành phần truyền không tầm nhìn thẳng NLOS [72, 78]. Theo [1], đối với môi trường UMa thì κ tính theo dB là một biến ngẫu nhiên Gauss $\mathcal{N}(9, 3.5)$. Để đơn giản, chúng ta giả thiết $\kappa_{\mathrm{B}} = \kappa_{\mathrm{E}} = 9$ [dB]. Giả thiết hệ thống hoạt động với băng thông 10 MHz, công suất phát ở trạm gốc là $p_{\mathrm{d}} = 46$ [dBm], công suất phát ở thiết bị đầu cuối hợp lệ là $p_{\mathrm{p}} = 24$ [dBm] và công suất tạp âm nhiệt là $N_0 = -174$ [dBm/Hz]. Tốc độ dữ liệu được tính cho một sóng mang con băng thông 15 [kHz]. Giả thiết khoảng cách giữa các ăng-ten lân cận tại trạm gốc bằng nửa bước sóng, tức là $d = 0.5$. Giả thiết hệ số tạp âm tại trạm gốc là 9 [dB/Hz] trong khi hệ số tạp âm tại nút B và tại nút E là 5 [dB/Hz]. Không mất tính tổng quát, giả thiết $\Phi_{\mathrm{B}} = 0$ [rad].

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

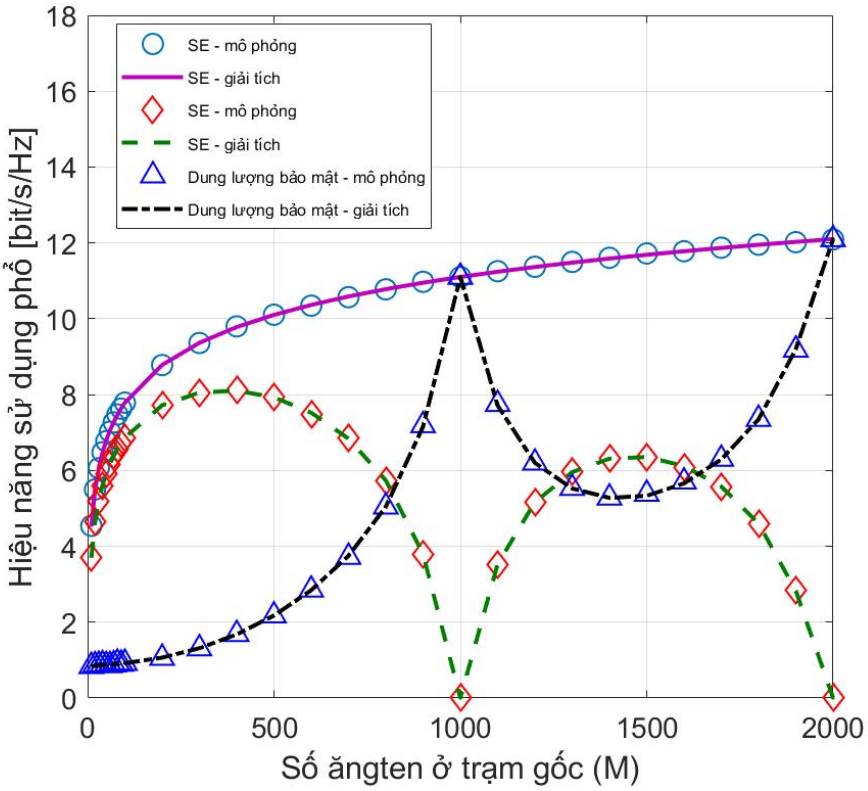
từ nút E và từ nút B đến trạm gốc đều là 300 [m], ii) hệ số mô hình kênh pha-đinh Rice là $\kappa_{\mathrm{B}} = \kappa_{\mathrm{E}} = 9$ [dB], và iii) kết quả mô phỏng được lấy trung bình của 150.000 mẫu. Hình 2.1 và Hình 2.2 trình bày kết quả mô phỏng và kết quả giải tích của tốc kết quả mô phỏng và kết quả phân tích giải tích của tốc độ dữ liệu hợp lệ R_{B}, tốc độ dữ liệu nghe lén R_{B} và dung lượng bảo mật C_{SC} dưới dạng hàm số của M tương ứng với khi $\Phi_{\mathrm{E}} = 0$ [rad] và $\Phi_{\mathrm{E}} = 0.002$ [rad]. Có thể thấy rằng các kết quả mô phỏng gần như nằm trên đường biểu diễn các kết quả phân tích giải tích tương ứng, tức là kết quả phân tích giải tích được đề xuất có độ chính xác cao và có thể được dùng thay thế cho kết quả mô phỏng. Trong cả hai hình 2.1 và 2.2, R_{B} luôn tăng theo hàm lôgarít của M, đúng như kết quả phân tích trong Mục 2.3.2. Hình 2.1 cho thấy R_{E} đều tăng theo hàm lôgarít đối với M trong khi C_{SC} gần như không đổi. Kết quả mô phỏng này hoàn toàn phù hợp với các khẳng định trong Bổ đề 2.3.4.

Hình 2.2 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. Đáng chú ý, có một số giá trị số ăng-ten ở trạm gốc khiến cho tốc độ dữ liệu nghe lén tiến sát bằng không và dung lượng bảo mật gần bằng tốc độ dữ liệu hợp lệ. Lý do là tại các giá trị M trên các vec tơ hệ số kênh truyền trực giao với nhau.

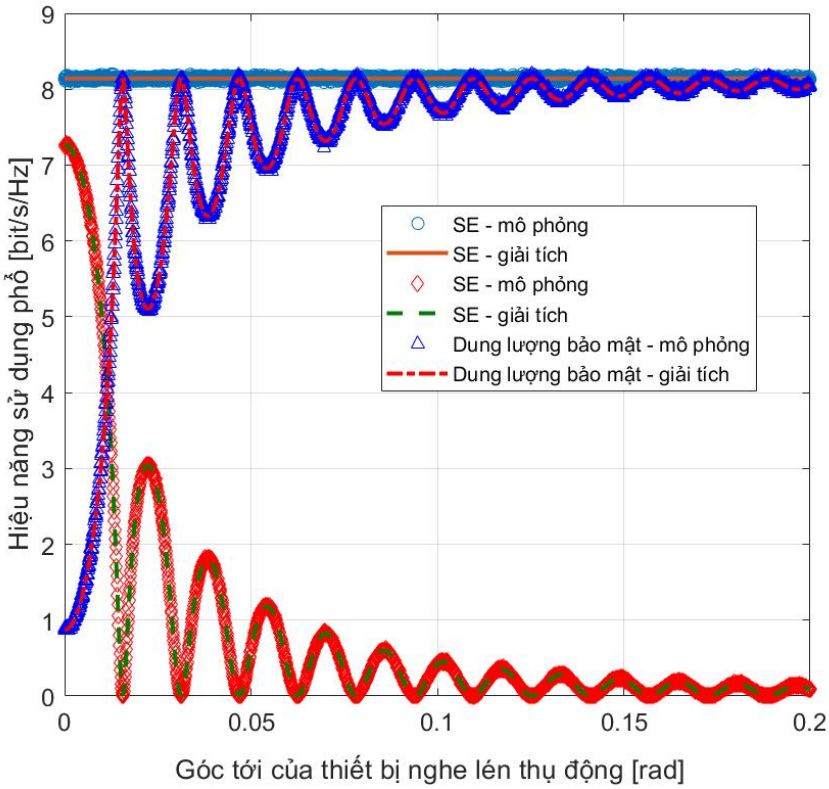
Hình 2.3 trình bày kết quả mô phỏng và kết quả phân tích giải tích của R_{B}, R_{E} và C_{SC} dưới dạng hàm số của Φ_{E} rad khi $M = 128$. Có thể thấy rằng khi góc tới Φ_{E} càng lớn, tức là $\Delta\Phi$ càng lớn, thì tốc độ dữ liệu nghe lén có xu hướng càng giảm. Điều này hợp lý vì khi $\Delta\Phi$ càng lớn thì tương quan chéo giữa các vec tơ hệ số kênh truyền càng nhỏ. Kết quả cho thấy của thành



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 M khi $\Phi_{\mathrm{E}} = \Phi_{\mathrm{B}} = 0$ [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 khi $\Phi_{\mathrm{E}} = \Phi_{\mathrm{B}} = 0.002$ [rad].



Hình 2.3: 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.

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, từ đó cho phép thiết bị nghe lén thụ động có thể ảnh hưởng lớn đến dung lượng bảo mật của hệ thống. Các kết quả trên được kiểm chứng bởi mô phỏng Monte Carlo trong các điều kiện mô phỏng khác nhau. Một số hướng nghiên cứu tiếp theo liên quan là nghiên cứu ảnh hưởng của thiết bị nghe lén thụ động khi trạm gốc sử dụng các phương pháp xử lý tín hiệu khác hoặc nghiên cứu ảnh hưởng của thiết bị tấn công chủ động trong điều kiện kênh truyền pha-đinh Rice.

2.5. Kết luận chương

Chương 2 của luận án đã khảo sát mô hình hệ thống MIMO cỡ rất lớn khi có thiết bị nghe lén thụ động, luận án đã đưa ra:

- Đánh giá dung lượng bảo mật của hệ thống mạng Massive MIMO trong điều kiện kênh truyền pha-đinh Rice không tương quan không gian, 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, từ đó cho phép thiết bị nghe lén thụ động có thể ảnh hưởng lớn đến dung lượng bảo mật của hệ thống.

Như vậy, với các kết quả giải tích mà nghiên cứu sinh đề xuất các biểu thức giải tích dạng tường minh cho dung lượng bảo mật của hệ thống thông tin vô tuyến Massive MIMO khi có mặt thiết bị nghe lén thụ động và dưới điều kiện kênh truyền pha-đinh Rice.

Chương 3

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

Việc gây nhiễu hoa tiêu không chỉ làm giảm khả năng bảo mật mà còn khó phát hiện. Trong chương 3 của luận án, NCS đã đề xuất một kỹ thuật, trong đó sử dụng hoa tiêu ngẫu nhiên N-PSK để phát hiện sự gây nhiễu hoa tiêu của thiết bị nghe lén thụ động trong các hệ thống Massive MIMO không tương quan không gian và trong điều kiện kênh truyền pha-đinh Rice. Kỹ thuật này chỉ cần hai khe thời gian đào tạo và không cần thông tin kênh truyền. Chương này, NCS xây dựng phương pháp phát hiện nhiễu hoa tiêu, phân tích 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 và đưa ra phương pháp tính xác suất phát hiện và xác suất báo động giả khi có thiết bị gây nhiễu. *Đóng góp của Chương 3 được trình bày trong công trình số 3,4*

- **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.

- **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.

3.1. Giới thiệu chung

Hệ thống Massive MIMO đã trở thành một trong những công nghệ quan trọng trong mạng 5G và những thế hệ tiếp theo sau khi cấu hình lại [53, 74, 39, 98, 75, 2, 6]. Nó có thể cung cấp nhiều lợi thế như tăng hiệu suất phổ và độ tin cậy, cải thiện chất lượng dịch vụ và phục vụ một số lượng lớn người dùng cùng một lúc, có thể kể đến một số ít. Cụ thể hơn, trong hệ thống Massive MIMO, BS thường được trang bị số lượng ăng ten lớn hơn để tạo ra nhiều bậc tự do hơn để phục vụ nhiều người dùng đồng thời [53]. Kết quả lý thuyết và triển khai thực tế đã chứng minh rằng kỹ thuật Massive MIMO đã cải thiện đáng kể hiệu suất hệ thống [65, 48, 83]. Tuy nhiên, do đặc tính phát sóng tự nhiên của tín hiệu không dây, các thiết bị bất hợp pháp có thể nghe lén và giải mã các thông điệp cho các mục đích không xác định. Rõ ràng, đây là một mối đe dọa nghiêm trọng đối với thông tin liên lạc an toàn và bảo mật [108].

Có hai loại tấn công chính trong truyền thông không dây: nghe lén thụ động và tấn công chủ động (gây nhiễu) [42]. Trong một cuộc tấn công thụ động, thiết bị không được cấp phép giữ im lặng để nghe lén các thông tin bí mật của người dùng hợp pháp, đây là một cuộc tấn công nguy hiểm vì rất khó phát hiện sự xuất hiện của kẻ tấn công. Trong một cuộc 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 để can thiệp vào ước tính kênh và / hoặc tín hiệu trực tiếp giữa những người dùng hợp pháp. Do đó, hiệu suất bảo mật của những người dùng hợp pháp bị giảm sút đáng kể, thậm chí bị gián đoạn do nhiễu có hại.

Nghiên cứu về bảo mật lớp vật lý dưới sự triển khai của công nghệ MIMO cỡ rất lớn đã thu hút nhiều nhà nghiên cứu để vượt qua mối đe dọa bảo mật trong mạng vô tuyến [105, 104, 86, 31, 91, 17, 14]. Các kết quả đã minh họa rằng việc bảo vệ truyền dẫn đường xuống có thể thực hiện được bằng cách sử dụng bộ lọc tiền mã hóa phù hợp và nhiễu nhân tạo AN được tạo ra tại BS. Dung lượng bảo mật có thể đạt được và xác suất dừng bảo mật được đề xuất cho các tình huống này để kiểm tra hoạt động của hệ thống. Bằng cách xem xét việc truyền đường xuống trong một hệ thống Massive MIMO đa tế bào, bốn bộ tiền mã hóa dữ liệu khác nhau và ba AN đã được nghiên cứu dưới số lượng ăng-ten của BS, thiết bị di động và thiết bị nghe lén là tiệm cận [104]. Tận dụng các công trình gần đây, J. Wang và các cộng sự đã cung cấp phân tích chuyên sâu về bảo mật do AN hỗ trợ MIMO cỡ rất lớn cho hàng loạt ăng-ten phân tán [86]. Kết quả cho thấy rằng số lượng ăng-ten phát tăng lên đến vô cùng lớn, ngưỡng dừng bảo mật trong các kênh truyền pha-đinh Rice phụ thuộc vào vị trí của người thiết bị nghe lén.

Đối với các thiết bị tấn công chủ động, trong [103], X. Zhou và các cộng sự đã nghiên cứu các chiến lược tấn công trong giai đoạn huấn luyện hoa tiêu. Các cuộc tấn công này ảnh hưởng trực tiếp đến những thiết bị hợp pháp để thay thế bộ tiền mã hóa của nó. Bằng cách thay đổi các vec tơ tiền mã hóa, hệ thống có thể tăng cường tín hiệu nhận được trong quá trình truyền dữ liệu với sự hiện diện của thiết bị gây nhiễu chủ động. Một cuộc tấn công bảo

mật mới đã được phát hiện thông qua hiện tượng nhiễu hoa tiêu. Trong [7], các tác giả đã nghiên cứu kênh đường xuống của hệ thống Massive MIMO đơn tế bào trong trường hợp những thiết bị tấn công có khả năng gây nhiễu và nghe lén. Một chiến lược định dạng chùm mới thiết lập bảo mật thông tin mà không cần mã hóa Wyner đã được đề xuất. Trong [25], T. T. Do và các cộng sự đã đề xuất các chiến lược chống gây nhiễu để chống lại những thiết bị gây nhiễu chủ động dựa trên việc truyền lại hoa tiêu. Kết quả mô phỏng đã minh họa rằng các chiến lược được đề xuất có thể cải thiện đáng kể hiệu suất bảo mật. Các công trình trước đây đã nghiên cứu các vấn đề trong đó các kênh chịu pha-đinh Rayleigh và người dùng thường có đầy đủ thông tin trạng thái kênh truyền. Tuy nhiên, trên thực tế, các kênh chứa các thành phần khác chứ không chỉ chứa các thành phần NLOS. Về mặt lý thuyết, các kênh pha-đinh Rice tổng quát hơn các kênh pha-đinh Rayleigh, vì chúng bao gồm thành phần LoS [67, 38]. Tuy nhiên, mô hình kênh Rice gây khó khăn cho việc phân tích khả năng bảo mật của hệ thống [86, 76]. Theo hiểu biết của NCS, đây là nghiên cứu đầu tiên về tấn công chủ động trong giai đoạn thử nghiệm hoa tiêu trên các kênh Rice. Bảo mật vật lý là một hướng nghiên cứu đầy hứa hẹn cho các mạng thế hệ thứ 5,6 và các thế hệ tiếp theo của các kênh pha-đinh Rice không tương quan về mặt không gian trong chế độ song công phân chia theo thời gian TDD. Dựa trên thực tế là các kênh lan truyền cần được ước lượng trong thực tế để phát hiện các tín hiệu mong muốn trong đường lên và xây dựng các vec tơ mã hóa chính xác trong đường xuống, một cuộc tấn công chủ động vào giai đoạn huấn luyện hoa tiêu có thể gây hại cho mạng không dây. Chúng ta chứng minh cách một thiết bị gây nhiễu có thể tấn công trong giai đoạn huấn luyện của hệ thống Massive MIMO với các

kênh pha-đinh Rice không tương quan về mặt không gian và hiển thị sơ đồ phát hiện sự hiện diện của thiết bị gây nhiễu. Dựa trên các đặc tính cơ bản của truyền thông trong mạng Massive MIMO, có thể coi các hiệu ứng gây nhiễu là nhiễu Gauss trắng cộng. Do đó, ngưỡng để phát hiện sự tồn tại của thiết bị gây nhiễu hoạt động được tính ở dạng biểu thức đóng với số lượng các ăng-ten đủ lớn tại trạm gốc. Trong phần này NCS đề xuất phương pháp mà không yêu cầu thông tin trạng thái kênh truyền và chỉ cần hai khe thời gian đào tạo để phát hiện hoạt động gây nhiễu. Các kết quả số cho thấy hiệu quả của việc phát hiện gây nhiễu hoạt động được đề xuất trên các cài đặt thông số hệ thống khác nhau. Hơn nữa, lợi ích của các thành phần NLOS chi phối đã được chứng thực. Đặc biệt, xác suất phát hiện được cải thiện khoảng 1,5 lần với sự hiện diện của các thành phần LOS, trong khi xác suất báo động giả được cải thiện hơn 10 lần.

Chi tiết hơn, nghiên cứu tập trung vào việc phát hiện hoạt động gây nhiễu trong hệ thống Massive MIMO kênh truyền pha-đinh Rice. Để phân tích hệ thống, cần nghiên cứu mô hình hệ thống trong đó BS được trang bị nhiều ăng ten và các cuộc tấn công gây nhiễu trong giai đoạn huấn luyện hoa tiêu đường lên. Theo đó, những nghiên cứu chính được tóm tắt như sau:

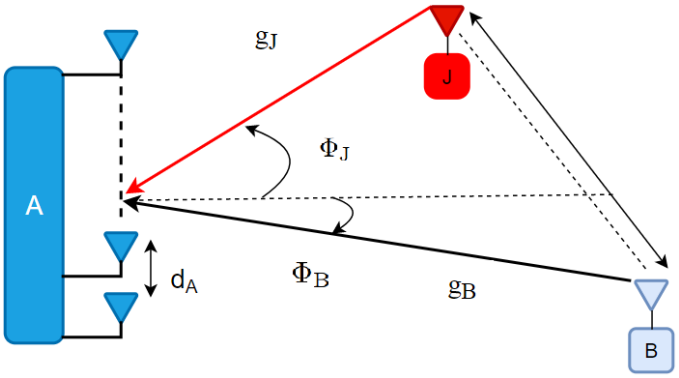
- Bảo mật lớp vật lý của hệ thống Massive MIMO dưới sự tấn công của một thiết bị gây nhiễu chủ động trong giai đoạn huấn luyện hoa tiêu. Sự ảnh hưởng của nhiễu bởi những thiết bị gây nhiễu chủ động trước tiên được phân tích cho một số lượng ăng-ten tại trạm gốc nhỏ. Các tác động của nhiễu và các cuộc tấn công gây nhiễu sau đó được quan sát rõ ràng khi số lượng ăng ten tại trạm gốc ngày càng lớn, thậm chí rất lớn.

- Trong phần này đề xuất một kế hoạch để phát hiện thiết bị gây nhiễu hoạt động bằng cách gây nhiễu hoa tiêu mà không cần có thông tin trạng thái kênh truyền. Quá trình phát hiện chỉ cần hai khe thời gian đào tạo để phát hiện sự xuất hiện của thiết bị gây nhiễu.
- 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.
- Trong nghiên cứu cũng đề xuất một sơ đồ phát hiện để phát hiện bộ gây nhiễu đang hoạt động. Ngay cả khi các góc tới (AOA) giống nhau, vẫn nhận được xác suất phát hiện rất cao và xác suất báo động sai thấp và có thể đạt đến 0 và có thể bỏ qua.

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). Lưu ý d_{BS} là khoảng cách giữa các ăng ten liền kề tại BS, $\bar{d}_{\mathrm{BS}} = 2\pi d_{\mathrm{BS}}/\lambda$ là khoảng cách giữa các ăng ten liền kề tại trạm gốc được chuẩn hóa, trong đó λ là bước sóng tương ứng với tần số sóng mang, d_k, $\forall k \in \mathcal{K}$, là khoảng cách từ trạm gốc đến UE_k [B,J]. θ_k, $\forall k \in \mathcal{K}$, là góc tạo bởi chùm tia nối từ BS đến người



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.

dùng $_k$ [B,J] và hướng búp sóng chính. Giá trị của θ_k là từ $-\pi$ đến π. Hình 3.1 biểu thị mô hình đó.

Giả sử mô hình kênh pha đinh khối phẳng trên miền tần số trong đó các hệ số kênh không thay đổi trong suốt thời gian của từng khung vô tuyến có các ký hiệu τ và thay đổi độc lập theo từng khung. Đặt $\mathbf{h}_{\mathrm{B}} \in \mathbb{C}^{N_{\mathrm{t}} \times 1}$ là vectơ hệ số kênh truyền giữa người dùng hợp pháp B và trạm gốc A. Gọi $\mathbf{h}_{\mathrm{J}} \in \mathbb{C}^{N_{\mathrm{t}} \times 1}$ là vec tơ hệ số kênh truyền giữa thiết bị bất hợp pháp J và trạm gốc A. Trong mô hình này, chúng ta xem xét mô hình kênh pha đinh Rice. Cụ thể, với mỗi vec tơ hệ số kênh truyền $\mathbf{h}_{\mathrm{X}}$, trong đó $\mathrm{X} \in \mathcal{X}$, được mô hình hóa và biểu diễn theo phân bố Gauss.

3.2.1. Mô hình truyền dẫn tầm nhìn thẳng LOS

Trong phần này, chúng ta trình bày mô hình truyền sóng 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.

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

3.2.2. Mô hình truyền dẫn không tầm nhìn thẳng NLOS

Ký hiệu $\mathbf{h}_k \in \mathbb{C}^{N_{\mathrm{t}} \times 1}$ 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

$\mathbf{h}_k \sim \mathcal{CN}(\mathbf{0}_{M\times 1}, \mathbf{R}_k)$, while $\mathbf{R}_k = \mathbb{E}[\mathbf{h}_k \mathbf{h}_k^H] \in \mathbb{C}^{M\times M}$ là ma trận tương quan không gian của vectơ truyền hệ số NLOS $\mathbf{h}_k$ trong đó $\mathrm{tr}(\mathbf{R}_k) = 1$. Ma trận tương quan không gian $\mathbf{R}_k$ có thể xác định theo mô hình sau Mô hình truyền cụm tán xạ:

Ký hiệu θ_k và σ_θ^2 là giá trị chính và phương sai của các góc tương ứng với vectơ kênh truyền, $p_\theta(\phi)$ là hàm mật độ phân bố xác suất của các góc tương ứng với các tia truyền sóng bị tán xạ trên cùng một cụm. Khi đó phần tử hàng m hàng cột n của $\mathbf{R}_k$ là $\forall m, n \in \{1, 2, \cdots, M\}$

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

Công thức dạng đóng của $[\mathbf{R}_k]_{m,n}$, tuân theo mô hình Laplace rút gọn. Ví dụ: nếu θ theo phân phối Laplace thì $[\mathbf{R}_k]_{m,n}$ xấp xỉ bằng (khi σ_θ nhỏ hơn 10^o) [27]

$$[\mathbf{R}_k]_{m,n} \approx \frac{\xi e^{j\bar{d}_{\mathrm{BS}}|m-n|\sin\theta_k}}{1 + \frac{\sigma_\theta^2}{2}[d_{\mathrm{BS}}(m-n)\cos\theta_j]^2}. \tag{3.3}$$

Từ các giả thiết trên ta xây dựng mô hình kênh đường lên của hệ thống. Ký hiệu $\mathbf{h}_{\mathrm{B}} \in \mathbb{C}^{M\times 1}$ là vectơ kênh truyền đường lên từ người dùng đến trạm

gốc và $\mathbf{h}_{\mathrm{J}} \in \mathbb{C}^{M\times 1}$ là vectơ kênh truyền đường lên từ thiết bị bất hợp pháp đến trạm gốc. Giả thiết mô hình kênh là đối xứng hoàn hảo TDD do đó $\mathbf{h}_{\mathrm{B}}^{H}, \mathbf{h}_{\mathrm{J}}^{H} \in \mathbb{C}^{1\times M}$.

Trong kịch bản nghiên cứu này, chúng ta giả thiết rằng κ_X hệ số Rice và β_{X} là độ số pha đinh trên quy mô lớn của kênh từ trạm gốc đến đích $\mathrm{X} \in \mathcal{X}$. Phần tương ứng với hệ số pha đinh quy mô lớn (LOS: Line-of-Sight)$\beta_{\mathrm{X,L}}$ và (NLOS: Non Line-of-Sight) $\beta_{\mathrm{X,N}}$ do

$$\beta_{\mathrm{X,L}} = \sqrt{\frac{\kappa_{\mathrm{X}}}{\kappa_{\mathrm{X}}+1}}\beta_{\mathrm{X}}; \quad \beta_{\mathrm{X,N}} = \sqrt{\frac{1}{\kappa_{\mathrm{X}}+1}}\beta_{\mathrm{X}}. \tag{3.4}$$

Khi đó vec tơ kênh truyền $\mathbf{h}_{\mathrm{X}}$ có phân bố là $\mathbf{h}_{\mathrm{X}} \sim \mathcal{CN}(\mathbf{g}_{\mathrm{X}}, \beta_{\mathrm{X,N}}\mathbf{I}_M)$ với $\mathrm{X} \in \mathcal{X}$ do

$$\mathbf{h}_{\mathrm{X}} = \mathbf{g}_{\mathrm{X}} + \sqrt{\beta_{\mathrm{X,N}}}\mathbf{w}_{\mathrm{X}}. \tag{3.5}$$

$\mathbf{g}_{\mathrm{X}}$ là hệ số LOS và $\mathbf{w}_{\mathrm{X}} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_M)$ là pha đinh phạm vi nhỏ. Do đó, vec tơ kênh truyền tương ứng với thành phần LOS từ trạm gốc đến các trạm $\mathrm{X} \in \mathcal{X}$ được cho bởi:

$$\mathbf{g}_{\mathrm{X}} = \beta_{\mathrm{X,L}}^{1/2}\left[1 \; e^{j2\pi d \sin\theta_{\mathrm{X}}} \; \cdots \; e^{j2\pi d(M-1)\sin\theta_{\mathrm{X}}}\right]^{T}. \tag{3.6}$$

trong đó θ_{X} là góc tới từ X đến BS và d là góc tới giữa trạm X đến BS và d là hàm khoảng cách giữa khoảng cách giữa các ăng ten và bước sóng. Chú ý là $\mathbf{g}_{\mathrm{X}}^{H}\mathbf{g}_{\mathrm{X}} = M\beta_{X,L}$ và $\forall X \in \mathcal{X}$. Để thuận tiện chúng ta ký hiệu. $\mathbf{g}_{\mathrm{X}}^{H}\mathbf{g}_{\mathrm{X}} = M\beta_{X,L}$ và $\forall X \in \mathcal{X}$.

$$\psi(\theta_{\mathrm{B}}, \theta_{\mathrm{J}}) = \pi d_{\mathrm{BJ}}(\sin\theta_{\mathrm{B}} - \sin\theta_{\mathrm{J}}) \tag{3.7}$$

$$\alpha(\theta_{\mathrm{B}}, \theta_{\mathrm{J}}, M) = \frac{\sin(M\psi(\theta_{\mathrm{B}}, \theta_{\mathrm{J}}))}{\sin(\psi(\theta_{\mathrm{B}}, \theta_{\mathrm{J}}))}. \tag{3.8}$$

Chúng ta có:

$$\mathbf{g}_{\mathrm{J}}^{H}\mathbf{g}_{\mathrm{B}} = \sqrt{\beta_{\mathrm{B,L}}\beta_{\mathrm{J,L}}}e^{j\psi(\theta_{\mathrm{B}},\theta_{\mathrm{J}})}\psi(\theta_{\mathrm{B}},\theta_{\mathrm{J}},M). \tag{3.9}$$

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. Trong đó $\mathbb{A}$ là tập hợp tất cả các tín hiệu. Hoa tiêu trong tập hợp $\mathbb{A}$ được biết đến công khai và thường được xác định theo tiêu chuẩn cho mô hình này và phù hợp trong thực tế. Vì vậy J có thể học và bắt chước để hoa tiêu được truyền bởi J có thể giống hệt với hoa tiêu được truyền bởi B. Gỉa thiết trong kịch bản nghiên cứu này B sử dụng bộ mã hóa N PSK trong tập hợp $\mathbb{A}$.

$$\mathbb{A} = \{e^{im2\pi/N} : 0 \leq m \leq (N-1)\}. \tag{3.10}$$

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

$$\mathbf{y}_{\mathrm{j}} = \sqrt{\mathrm{P_B}}\mathbf{p}_{\mathrm{j}}^{\mathrm{B}}\mathbf{h}_{\mathrm{AB}} + \sqrt{\mathrm{P_J}}\mathbf{p}_{\mathrm{j}}^{\mathrm{J}}\mathbf{h}_{\mathrm{AJ}} + \mathbf{n}_{\mathrm{j}}. \tag{3.11}$$

where $\mathbf{n}_j \sim \mathcal{CN}(\mathbf{0}, \sigma_j^2\mathbf{I}_{N_{\mathrm{t}}})$ là tạp âm nhiệt Gauss và

$$\mathbf{h}_{\mathrm{AB}} = \mathbf{g}_{\mathrm{B}} + \beta_{\mathrm{B,N}}^{1/2}\mathbf{w}_{\mathrm{B}}; \quad \mathbf{h}_{\mathrm{AJ}} = \mathbf{g}_{\mathrm{J}} + \beta_{\mathrm{J,N}}^{1/2}\mathbf{w}_{\mathrm{J}}. \tag{3.12}$$

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 $\mathrm{R_T^{11}} = \beta_{\mathrm{B}}\mathrm{M}$;

$\mathrm{R_T^{12}} = \sqrt{\beta_{\mathrm{B,N}}\beta_{\mathrm{J,N}}}\mathrm{e}^{\mathrm{j}\phi(\theta_{\mathrm{B}},\theta_{\mathrm{J}})}\alpha(\theta_{\mathrm{B}},\theta_{\mathrm{J}},\mathrm{M})$; $\mathrm{R_T^{21}} = [\mathrm{R_T^{12}}]^{\mathrm{H}}$; $\mathrm{R_T^{22}} = \beta_{\mathrm{J}}\mathrm{M}$.

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. Nếu BS nhận biết được các kênh và chúng khác nhau đáng kể, thì sẽ có sự khác biệt về cường độ tín hiệu so với dự kiến và tăng nguy cơ bị phát hiện. Phát hiện này tạo thành hệ thống phát hiện hoa tiêu ngẫu nhiên được mô tả bên dưới. 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.

$$\mathbf{y}_{\mathrm{j}} = \sqrt{P_{\mathrm{B}}}\mathbf{s}_{\mathrm{j}}^{\mathrm{B}}\mathbf{h}_{\mathrm{A,B}} + \sqrt{P_{\mathrm{J}}}\mathbf{s}_{\mathrm{j}}^{\mathrm{J}}\mathbf{h}_{\mathrm{A,J}} + \mathrm{n}_{j}, \tag{3.13}$$

Tích vô hướng của 2 vector nhận được:

$$\mathbf{z}_{12} = \frac{1}{M}\mathbf{y}_{1}^{\mathrm{H}}\mathbf{y}_{2}. \tag{3.14}$$

Chúng ta có:

$$\begin{aligned}\mathbf{z}_{12}^{\mathrm{J}} =& \frac{1}{M}\Big\{ P_{\mathrm{B}}(\mathbf{p}_{1}^{\mathrm{B}})^{\mathrm{H}}\mathbf{p}_{2}^{\mathrm{B}}\mathbf{R}_{T}^{11} + \sqrt{\mathrm{P_B P_J}}(\mathbf{p}_{1}^{\mathrm{B}})^{\mathrm{H}}\mathbf{p}_{2}^{\mathrm{J}}\mathbf{R}_{\mathrm{T}}^{12} \\ &+\sqrt{\mathrm{P_B P_J}}(\mathbf{p}_{1}^{\mathrm{J}})^{\mathrm{H}}\mathbf{p}_{2}^{\mathrm{B}}\mathbf{R}_{\mathrm{T}}^{12} + \mathrm{P_J}(\mathbf{p}_{1}^{\mathrm{J}})^{\mathrm{H}}\mathbf{p}_{2}^{\mathrm{J}}\mathbf{R}_{\mathrm{T}}^{22} \qquad (3.15)\\ &+\mathbf{N}_{12}^{\mathrm{J}}\Big\}. \qquad (3.16)\end{aligned}$$

Trong đó:

$$\begin{aligned}\mathbf{N}_{12}^{\mathrm{J}} =& \sqrt{P_{\mathrm{B}}}(\mathbf{p}_{1}^{\mathrm{B}})^{\mathrm{H}}\mathbf{h}_{\mathrm{A,B}}^{\mathrm{H}}\mathbf{n}_{2} + \sqrt{P_{\mathrm{J}}}(\mathrm{p}_{1}^{\mathrm{J}})^{\mathrm{H}}(\mathbf{h}_{\mathrm{A,J}})^{\mathrm{H}}\mathbf{n}_{2} \\ &+\sqrt{P_{\mathrm{B}}}\mathbf{p}_{2}^{\mathrm{B}}\mathbf{h}_{\mathrm{A,B}}\mathbf{n}_{1}^{\mathrm{H}} + \sqrt{P_{\mathrm{J}}}\mathbf{p}_{2}^{\mathrm{J}}\mathbf{h}_{\mathrm{A,J}}\mathbf{n}_{1} + \mathbf{n}_{1}^{\mathrm{H}}\mathbf{n}_{2}. \qquad (3.17)\end{aligned}$$

Chúng ta đưa ra cách phát hiện thiết bị nghe lén và tính toán xác suất phát hiện ra J.

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.

$$\mathbf{z}_{12}^{0} = \frac{1}{M} P_{\mathrm{B}} \left(\mathbf{p}_{1}^{\mathrm{B}}\right)^{\mathrm{H}} \mathbf{p}_{2}^{\mathrm{B}} \mathbf{h}_{\mathrm{A,B}}^{\mathrm{H}} \mathbf{h}_{\mathrm{A,B}}. \tag{3.18}$$

$$\mathbb{E}[\mathbf{z}_{12}^{0}] = \mathrm{P}_{\mathrm{B}} \beta_{\mathrm{B}} (\mathrm{p}_{1}^{\mathrm{B}})^{\mathrm{H}} \mathrm{p}_{2}^{\mathrm{B}}. \tag{3.19}$$

- 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.

Bổ đề 3.3.1 *Với mỗi cặp* $\mathbf{s}_j \in \mathbb{A}$ *trong* N*-PSK, khi đó* $\mathbf{p}_1^{\mathrm{H}} \mathbf{p}_2 \in N$*-PSK*

Chứng minh Bổ đề 3.3.1 *Tại mỗi thời điểm đào tạo thứ j,* B *và* J *được cung cấp* ${\mathbf{p}_j}^{\mathrm{B}} \in \mathbb{A}$ *và* ${\mathbf{p}_j}^{\mathrm{J}} \in \mathbb{A}$*, với toàn bộ tập hợp hoa tiêu thử nghiệm* $\mathbb{A}$*. Tập hợp hoa tiêu* $\mathbb{A}$ *được xác định trong suốt thời gian huấn luyện Ký hiệu hoa tiêu A là một tín hiệu* N*-PSK* $\mathbb{A} = e^{in_j 2\pi/N} : 0 \leq n_j \leq N-1 \; n_j \in (0, 1, ..., N-1)$*. Tại khe thời gian j = 1,2.*

Chúng ta có:

$$\begin{aligned} \mathbf{p}_1^{\mathrm{H}} \mathbf{p}_2 &= A_1 A_2 e^{j(n_2 - n_1)\frac{2\pi}{N}}, \\ [n_2 - n_1] &\in \{0, 1, ..., N-1\} \\ z = \arg \left|\mathbf{p}_1^{\mathrm{H}} \mathbf{p}_2\right| &= (n_2 - n_1) \frac{2\pi}{N} \end{aligned} \tag{3.20}$$

$\mathbf{z}$ *thuộc bộ* N*-PSK*

Từ bổ đề 3.3.1 chúng ta có: $(\mathbf{p}_1^{\mathrm{B}})^{\mathrm{H}}\mathbf{p}_2^{\mathrm{B}}$ là một tín hiệu N-PSK. Khi đó $\mathbb{E}[\mathbf{z}_{12}]$ thuộc tín hiệu PSK .

Dựa trên các công thức (3.14) và (3.19).

Nếu J không xuất hiện, thì $\mathrm{z}_{12}^{0} = \mathrm{y}_1^{\mathrm{H}}\mathrm{y}_2$ thuộc tín hiệu PSK .

Nếu J xuất hiện thì $\mathrm{z}_{12}^{\mathrm{J}} = \mathrm{y}_1^{\mathrm{H}}\mathrm{y}_2$ không thuộc PSK. Vì vậy trạm gốc dễ dàng phát hiện J Nếu để J không bị phát hiện thì $\mathrm{z}_{12}^{\mathrm{J}}$ phải thuộc tín hiệu PSK. Điều đó có nghĩa là $\mathrm{z}_{12}^{\mathrm{J}}$ cần phải nằm trên các đường N/2.

Dựa trên những quan sát này, có thể định nghĩa kỹ thuật phát hiện là: Khi $\mathrm{y}_1^{\mathrm{H}}\mathrm{y}_2$ nằm trên đường PSK. J không xuất hiện.

Tích vô hướng của Dựa trên những quan sát này, có thể định nghĩa kỹ thuật phát hiện là khi

$$\begin{aligned}\mathbb{E}\left[\mathbf{z}_{12}^{\mathrm{J}}\right] = \frac{1}{M}(\mathrm{p}_1^{\mathrm{B}})^{\mathrm{H}}\mathrm{p}_2^{\mathrm{B}}\,[&P_{\mathrm{B}}\mathrm{M}\beta_{\mathrm{B}}\\ &+\sqrt{P_{\mathrm{B}}P_{\mathrm{J}}}\beta_{\mathrm{B,N}}^{1/2}\beta_{\mathrm{J,N}}^{1/2}\mathrm{J}^{\mathrm{j}\theta(\theta_{\mathrm{B}},\theta_{\mathrm{J}})}\\ &\alpha(\theta_{\mathrm{B}},\theta_{\mathrm{J}},\mathrm{N_t})\left(\mathbf{p}_2^{\mathrm{B}}\right)^{\mathrm{H}}\left(\mathbf{p}_2^{\mathrm{J}}\right)\\ &+\sqrt{P_{\mathrm{B}}P_{\mathrm{J}}}\beta_{\mathrm{B,N}}^{1/2}\beta_{\mathrm{J,N}}^{1/2}\mathrm{J}^{\mathrm{j}\theta(\theta_{\mathrm{B}},\theta_{\mathrm{J}})}\\ &\alpha(\theta_{\mathrm{B}},\theta_{\mathrm{J}},\mathrm{N_t})\left(\mathbf{p}_1^{\mathrm{J}}\right)^{\mathrm{H}}\left(\mathbf{p}_1^{\mathrm{B}}\right)\\ &+P_{\mathrm{J}}\mathrm{M}\beta_{\mathrm{J}}\left(\mathbf{p}_2^{\mathrm{B}}\right)^{\mathrm{H}}\left(\mathbf{p}_1^{\mathrm{B}}\right)(\mathrm{p}_1^{\mathrm{J}})^{\mathrm{H}}\mathrm{p}_2^{\mathrm{J}}\Big]. \end{aligned} \tag{3.21}$$

Tích của tín hiệu PSK được tính trong $(\mathrm{p}_1^{\mathrm{X}})^{\mathrm{H}}\mathrm{p}_2^{\mathrm{X}}$. Tích vô hướng có góc vec tơ tích vô hướng có góc vec tơ (3.21) phải là góc của ký hiệu PSK. Nếu $\mathrm{p}_2^{\mathrm{J}} = \mathrm{p}_1^{\mathrm{J}}(\mathrm{p}_1^{\mathrm{B}})^{\mathrm{H}}\mathrm{p}_2^{\mathrm{B}}$. Trong trường hợp khác $\mathrm{p}_1^{\mathrm{J}}(\mathrm{p}_1^{\mathrm{B}})^{\mathrm{H}} \neq \mathrm{p}_2^{\mathrm{J}}(\mathrm{p}_2^{\mathrm{B}})^{\mathrm{H}}$ không trùng với bất kỳ góc nào của ký hiệu PSK. Trong trường hợp J tránh để không bị phát hiện, điều đó có nghĩa là J có thể đoán được hoa tiêu huấn luyện của B $\mathrm{p}_1^{\mathrm{J}}(\mathrm{p}_1^{\mathrm{B}})^{\mathrm{H}}\mathrm{p}_2^{\mathrm{B}}$ trong khung thời gian thứ hai. Bởi vì J có thể dự đoán được hoa

tiêu $\mathrm{p}_1^{\mathrm{J}}(\mathrm{p}_1^{\mathrm{B}})^{\mathrm{H}}\mathrm{p}_2^{\mathrm{B}}$ là tín hiệu PSK. Nhưng trong hầu hết các hệ thống thông tin liên lạc đều phải tính đến sự can nhiễu. Khi đó xác suất phát hiện thiết bị nghe lén sẽ thay đổi và xuất hiện xác suất báo động giả.

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

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

$$\begin{aligned}\mathbf{y}_1 =&\sqrt{P_{\mathrm{B}}}\mathbf{p}_1^{\mathrm{B}}\mathbf{h}_{\mathrm{A,B}} + \mathbf{n}_1,\\ \mathbf{y}_2 =&\sqrt{P_{\mathrm{B}}}\mathbf{p}_2^{\mathrm{B}}\mathbf{h}_{\mathrm{A,B}} + \mathbf{n}_2.\end{aligned} \tag{3.22}$$

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:

$$\mathrm{z}_{12}^0 = \frac{1}{\mathrm{M}}\left[\mathrm{P_B}(\mathrm{p}_1^{\mathrm{B}})^{\mathrm{H}}\mathrm{p}_2^{\mathrm{B}}\mathrm{h}_{\mathrm{A,B}}^{\mathrm{H}}\mathrm{h}_{\mathrm{A,B}} + \mathrm{N}_{12}^0\right]. \tag{3.23}$$

Trong đó

$$\begin{aligned}\mathrm{N}_{12}^0 = \frac{1}{\mathrm{M}}\Big[&\sqrt{\mathrm{P_B}}(\mathrm{p}_1^{\mathrm{B}})^{\mathrm{H}}\mathbf{h}_{\mathrm{A,B}}^{\mathrm{H}}\mathbf{n}_2 + \sqrt{\mathrm{P_B}}\mathrm{p}_2^{\mathrm{B}}\mathbf{n}_1^{\mathrm{H}}\mathbf{h}_{\mathrm{A,B}}\\ &+ \mathbf{n}_1^{\mathrm{H}}\mathbf{n}_2\Big].\end{aligned} \tag{3.24}$$

là nhiễu tương ứng. Giá trị nhỏ nhất của N_{12}^0 là $\mathbb{E}[\mathrm{N}_{12}^0] = 0$. Phương sai của N_{12}^0 là $\mathrm{S}_{\mathrm{J}}^0$

$$S_{\mathrm{J}}^0 = \frac{1}{\mathrm{M}}[2P_{\mathrm{B}}\mathrm{M}\beta_{\mathrm{B}}\sigma^2 + \sigma^4]. \tag{3.25}$$

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. Chúng ta tính tích vô

hướng của 2 vec tơ khi thiết bị nghe lén gây nhiễu hoa tiêu.

$$\begin{aligned}\mathbf{z}_{12}^{\mathrm{J}} = \frac{1}{M}\Big\{ & \mathrm{P_B}\left(\mathbf{p}_1^{\mathrm{B}}\right)^{\mathrm{H}} \mathrm{p}_2^{\mathrm{B}} \mathbf{h}_{\mathrm{A,B}}^{\mathrm{H}} \mathbf{h}_{\mathrm{A,B}} \\ & + \sqrt{\mathrm{P_B P_J}}\left(\mathbf{p}_1^{\mathrm{B}}\right)^{\mathrm{H}} \left(\mathbf{p}_2^{\mathrm{J}}\right) \left(\mathbf{h}_{\mathrm{A,B}}\right)^{\mathrm{H}} \mathbf{h}_{\mathrm{A,J}} \\ & + \sqrt{\mathrm{P_B} P_{\mathrm{J}}}\left(\mathbf{p}_1^{\mathrm{J}}\right)^{\mathrm{H}} \left(\mathbf{p}_2^{\mathrm{B}}\right) \mathbf{h}_{\mathrm{A,J}}^{\mathrm{H}} \mathbf{h}_{\mathrm{A,B}} \\ & + \mathrm{P_J}\left(\mathbf{p}_1^{\mathrm{J}}\right)^{\mathrm{H}} \left(\mathbf{p}_2^{\mathrm{J}}\right) \mathbf{h}_{\mathrm{A,J}}^{\mathbf{H}} \mathbf{h}_{\mathrm{A,J}} + \mathrm{N}_{12}^{\mathrm{J}} \Big\}. \end{aligned} \tag{3.26}$$

Trong đó:

$$\begin{aligned}\mathbf{N}_{12}^{\mathrm{J}} = & \sqrt{P_{\mathrm{B}}} \mathbf{p}_1 \mathbf{h}_{\mathrm{A,B}} \mathbf{n}_2 + \sqrt{P_{\mathrm{J}}} (\mathrm{p}_1^{\mathrm{B}})^{\mathrm{H}} (\mathbf{h}_{\mathrm{A,J}})^{\mathrm{H}} \mathbf{n}_2 \\ & + \sqrt{P_{\mathrm{B}}} \mathbf{p}_2 \mathbf{h}_{\mathrm{A,B}} \mathbf{n}_1^{\mathrm{H}} + \sqrt{P_{\mathrm{J}}} \mathbf{p}_2 \mathbf{h}_{\mathrm{A,J}} \mathbf{n}_1 + \mathbf{n}_1^{\mathrm{H}} \mathbf{n}_2. \end{aligned} \tag{3.27}$$

$$\begin{aligned}\mathbb{E}[\mathbf{z}_{12}^{\mathrm{J}}] = & \mathbb{E}\Bigg[\frac{1}{M} \Big\{ \mathrm{P_B} (\mathbf{p}_1^{\mathrm{B}})^{\mathrm{H}} \mathbf{p}_2^{\mathrm{B}} \mathbf{R}_T^{11} \\ & + \sqrt{\mathrm{P_B P_J}} (\mathbf{p}_1^{\mathrm{B}})^{\mathrm{H}} \mathbf{p}_2^{\mathrm{J}} \mathbf{R}_{\mathrm{T}}^{12} \\ & + \sqrt{\mathrm{P_B P_J}} (\mathbf{p}_1^{\mathrm{J}})^{\mathrm{H}} \mathbf{p}_2^{\mathrm{B}} \mathbf{R}_{\mathrm{T}}^{12} + \mathrm{P_J} (\mathbf{p}_1^{\mathrm{J}})^{\mathrm{H}} \mathbf{p}_2^{\mathrm{J}} \mathbf{R}_{\mathrm{T}}^{22} \Big\} \Bigg]. \end{aligned} \tag{3.28}$$

$\mathrm{N}_{12}^{\mathrm{J}}$ hội tụ với giá trị trung bình bằng 0 và phương sai là biến Gauss $S_{\mathrm{J}}^{\mathrm{M}}$

$$\begin{aligned} S_{\mathrm{M}}^{\mathrm{J}} = & \sigma^2 \Big\{ 2\mathrm{P_B R_T^{11}} + \sqrt{P_{\mathrm{B}} P_{\mathrm{J}}} [(\mathrm{p}_1^{\mathrm{B}})^{\mathrm{H}} \mathrm{p}_1^{\mathrm{J}} + (\mathrm{p}_2^{\mathrm{B}})^{\mathrm{H}} \mathrm{p}_2^{\mathrm{J}}] \mathrm{R}_{\mathrm{T}}^{12} \\ & + \sqrt{P_{\mathrm{B}} P_{\mathrm{J}}} [(\mathrm{p}_1^{\mathrm{J}})^{\mathrm{H}} \mathrm{p}_1^{\mathrm{B}} + (\mathrm{p}_2^{\mathrm{J}})^{\mathrm{H}} \mathrm{p}_2^{\mathrm{B}}] \mathrm{R}_{\mathrm{T}}^{21} \\ & + 2P_{\mathrm{J}} \mathrm{R}_{\mathrm{T}}^{22} + \sigma^2 \Big\}. \end{aligned} \tag{3.29}$$

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

Trong các phần trước, chúng tôi đã trình bày cách xây dựng tính năng phát hiện thiết bị nghe lén bất hợp pháp, tức là

BS quyết định phạm vi mà J có bị phát hiện gây nhiễu hay không dựa trên kết quả tính tích vô hướng $\mathrm{y_1^H y_2/M}$ nằm ngoài hay bên trong khu vực phát hiện từ tích vô hướng đã được tạo $\mathrm{z_{12}}$ trong công thức (3.23). 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 $\mathrm{y_1^H y_2/M}$ ở vị trí $r(D_{\mathrm{B}})$ cách một số đường PSK, thì J không gây nhiễu.

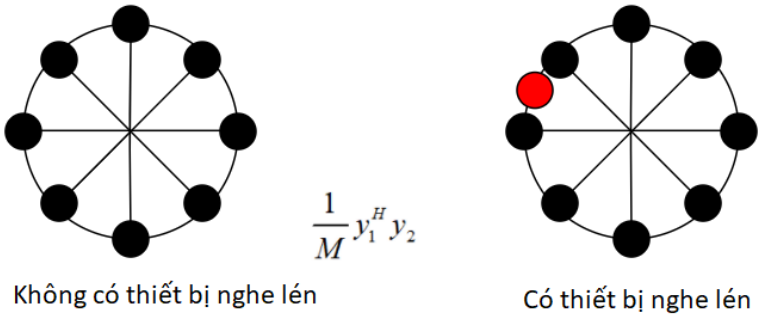
Phương sai $\mathrm{S_M^0}$ của nhiễu Gauss $\mathrm{N_{12}^0}$ tăng lên trong D_{B} với $r(D_{\mathrm{B}})$ giảm. Nhiễu Gauss có thể được hiển thị $\sqrt{S_{\mathrm{M}}^0}$ dưới dạng một vòng tròn có tâm quanh 0 , bán kính $r(D_{\mathrm{B}})$ trong không gian tín hiệu. Để phát hiện ra J, tích vô hướng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

$$s_M^0 = \frac{N_0}{M^2}(MN_0 + 2P_B\mathbf{R_T^{11}}). \tag{3.30}$$

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

Phần này cung cấp một số kết quả mô phỏng và tính toán số để kiểm chứng các kết quả phân tích giải tích. Xét một mạng di động đơn tế bào trong đó



Hình 3.2: Sơ đồ phát hiện phát hiện nhiễu hoa tiêu ngẫu nhiên. Đầu tiên B truyền các hoa tiêu PSK ngẫu nhiên. Sau quá trình xử lý tại BS, nếu không có J thì tích của hai tín hiệu nhận được phải là ký hiệu PSK. Ngược lại thì J có mặt.

trạm gốc được đặt ở chính giữa tế bào trong khi thiết bị đầu cuối hợp lệ (nút B) và thiết bị gây nhiễu chủ động (nút J) được bố trí ngẫu nhiên trong tế bào. Giả thiết ảnh hưởng của hiệu ứng che chắn bị bỏ qua, khi đó hệ số suy hao đường truyền phạm vi lớn được tính như sau [1, 72, 78]

$$\beta_{\mathrm{X,Y}} = 32.4 + 10 n_{\mathrm{Y}} \log_{10}(d_{\mathrm{3D,X}}) + 20 \log_{10}(f_{\mathrm{c}}).$$

trong đó $X \in \mathcal{X}$, $Y \in \mathcal{Y} = \{\mathrm{L}, \mathrm{N}\}$, $d_{\mathrm{3D,X}}$ là khoảng cách tính theo mét từ trạm gốc đến nút X trong không gian 3 chiều, $f_{\mathrm{c}} = 3.5$ GHz là tần số sóng mang, n_{Y} là hệ số mũ suy hao đường truyền. Ngoài ra, $d_{\mathrm{3D,X}}$ được tính như sau $d_{\mathrm{3D,X}} = \sqrt{d_{\mathrm{2D,X}}^2 + (h_{\mathrm{A}} - h_{\mathrm{X}})^2}$ trong đó $d_{\mathrm{2D,X}}$ là khoảng cách từ trạm gốc tới nút X trong không gian 2 chiều, h_{A} là chiều cao của trạm gốc A, và h_{X} là chiều cao của nút X [1]. Không mất tính tổng quát, giả thiết $h_{\mathrm{A}} = 10$ m và $h_{\mathrm{B}} = h_{\mathrm{J}} = 1.5$ m. Nghiên cứu này xem xét môi trường tế bào lớn ở đô thị, khi đó $n_{\mathrm{L}} = 2$ cho thành phần truyền tầm nhìn thẳng LOS và $n_{\mathrm{N}} = 2.9$ cho thành phần truyền không tầm nhìn thẳng NLOS [72, 78]. Theo [1], đối với môi trường UMa thì κ tính theo dB là một biến ngẫu nhiên Gauss $\mathcal{N}(9, 3.5)$. Để đơn giản, chúng ta giả thiết $\kappa_{\mathrm{B}} = \kappa_{\mathrm{J}} = 9$ dB. Giả thiết hệ thống hoạt

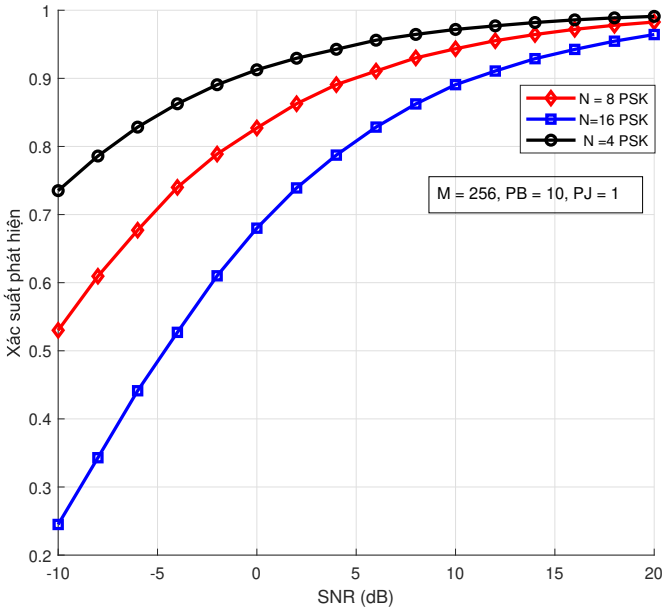
động với băng thông 10 MHz, công suất phát ở trạm gốc là $P_{\mathrm{d}} = 46$ dBm, công suất phát ở thiết bị đầu cuối hợp lệ là $P_{\mathrm{P}} = 24$ dBm và mật độ công suất tạp âm nhiệt là $N_0 = -174$ dBm/Hz. Tốc độ dữ liệu được tính cho một sóng mang con băng thông 15 kHz. Giả thiết khoảng cách giữa các ăng ten lân cận tại trạm gốc bằng nửa bước sóng, tứclà $d = 0.5$. Giả thiết hệ số tạp âm tại trạm gốc là 9 dB/Hz trong khi hệ số tạp âm tại nút B và tại nút J là 5 dB/Hz. Không mất tính tổng quát, giả thiết $\Phi_{\mathrm{B}} = 0$[rad].

Trước hết, chúng ta xem xét một kịch bản mô phỏng trong đó thiết bị gây nhiễu chủ động, hay nút J, 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 J và từ nút B đến trạm gốc đều là 300m, ii) hệ số mô hình kênh Rice là $\kappa_{\mathrm{B}} = \kappa_{\mathrm{J}} = 9$ dB , và iii) kết quả mô phỏng được lấy trung bình của 200.000 mẫu.

3.4.1. Sử dụng cặp hoa tiêu thử nghiệm trong một khung truyền vô tuyến

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.

Hình 3.3 cho biết xác suất phát hiện tỉ lệ với nhiễu SNR và trạm gốc được trang bị 256 ăng- ten, $\mathrm{P_B} = 24$ dBm, $\mathrm{P_J} = 24$ dBm, với khóa PSK lần lượt là $\mathrm{N} = [4, 8, 16]$- PSK. Trong đó SNR được tính bởi $\mathrm{SNR} = \frac{\mathrm{P_B}}{\mathrm{N_0}}$ in dB. Như dự đoán, xác suất phát hiện tăng SNR; trong miền SNR cao, xác suất phát hiện là 1. Trong [43], các tác giả đã chỉ ra rằng công suất truyền của J lớn hơn của người dùng hợp pháp B thì J dễ phát hiện hơn. Nhưng trong các kênh Massive MIMO với pha đinh Rice và số lượng ăng ten lớn hơn, không



Hình 3.3: 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

.

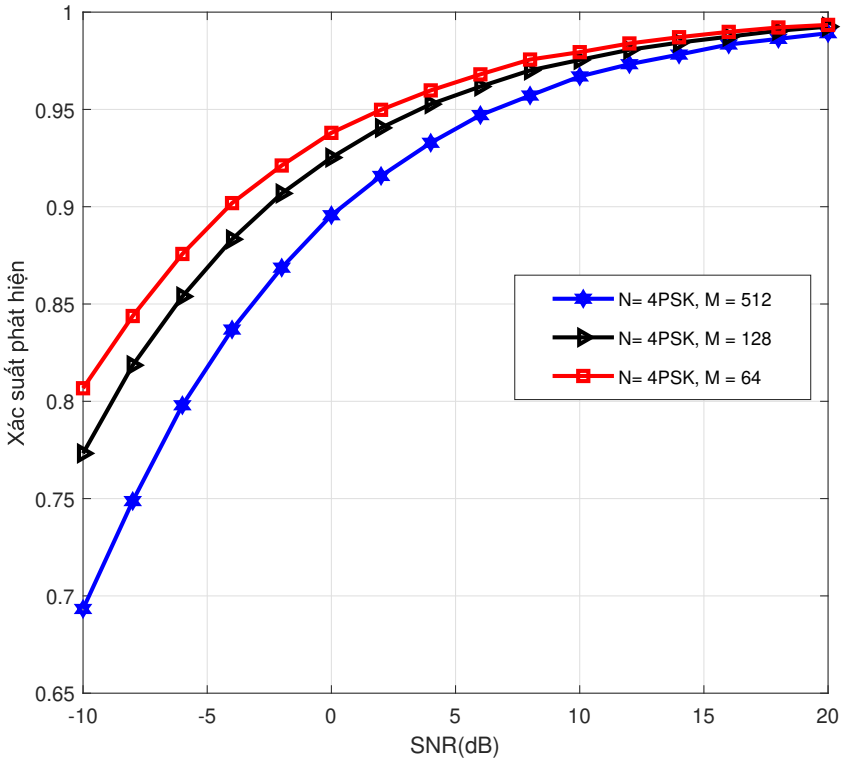
khó để phát hiện ra thiết bị tấn công gây nhiễu.

Hình vẽ 3.5 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

3.4.2. Sử dụng căp ngẫu nhiên hoa tiêu thử nghiệm trong một tập hoa tiêu thử nghiệm

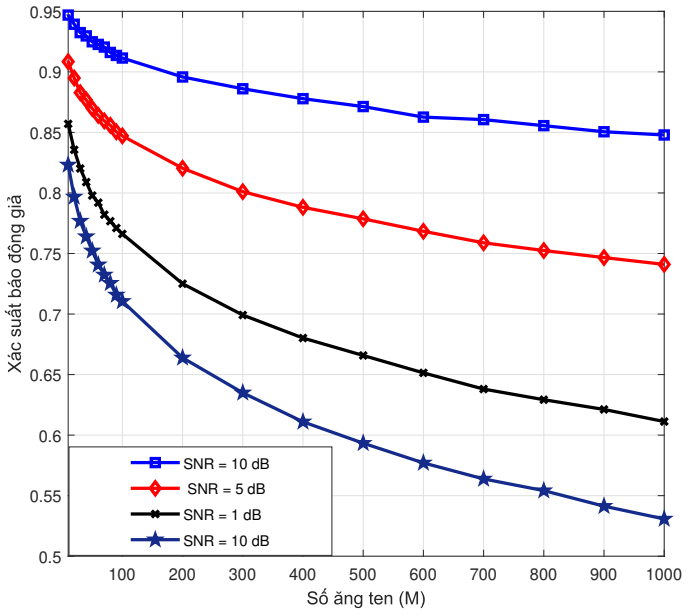
Khi chúng ta mở rộng nghiên cứu với kịch bản sử dụng một tập hợp hoa tiêu thử nghiệm và chọn ngẫu nhiên một cặp trong số đó. Hình 3.4 cho biết xác suất phát hiện tỉ lệ với SNR với khóa N = 4 PSK với số lương ăng ten thay đổi. Xác suất phát hiện tăng cao tỷ lệ thuận với SNR và tiến gần tới 1.

Hình 3.6 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

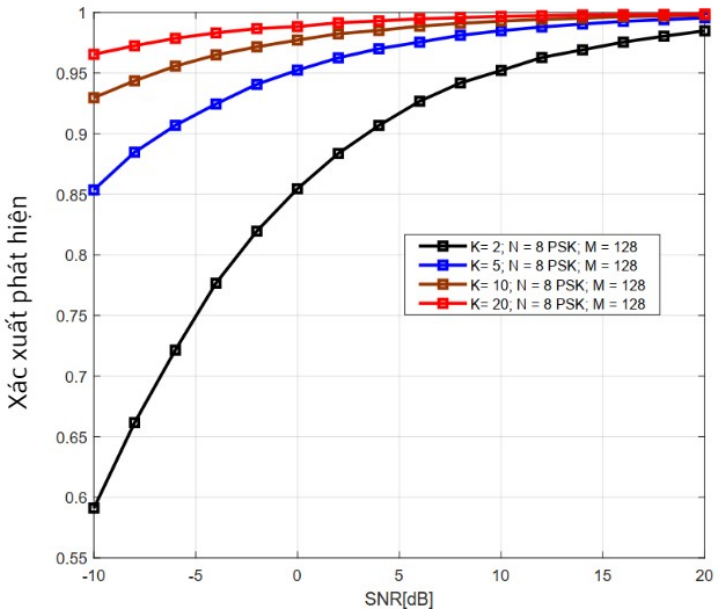


Hình 3.4: Xác suất phát hiện tỉ lệ với SNR cho trường hợp N = 4-PSK, P_B = 24 dBm, P_J = 24 dBm and Φ_B = 0.1 rad và Φ_J = 0.1 rad, d_B= 300 m, d_J = 200 m

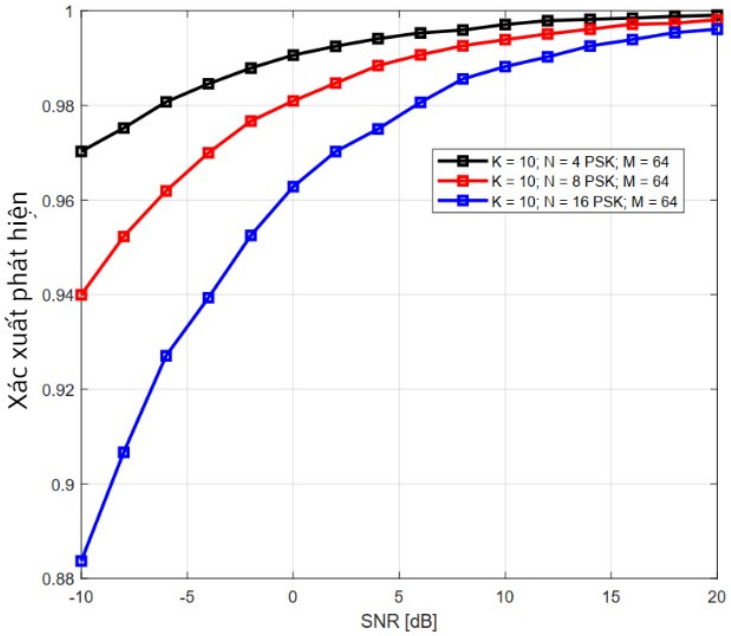
.



Hình 3.5: Xác suất báo động giả $\Phi_J = 0.1$ rad, $\Phi_B = 0.1$ rad, N = 16 PSK với M .



Hình 3.6: Xác suất phát hiện tỉ lệ với SNR với $M = 128$, $N = 8$ và các giá trị K khác nhau

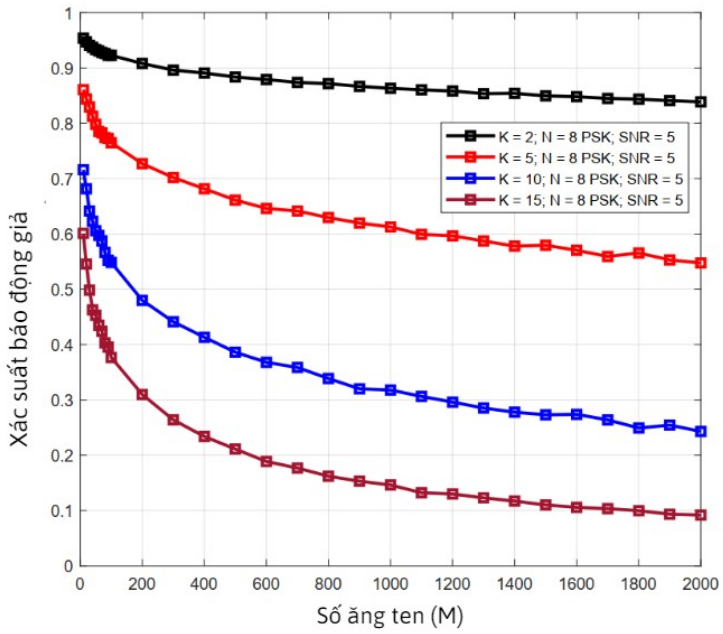


Hình 3.7: Xác suất phát hiện vs. SNR cho trường hợp K = 10, M = 64 ang ten, và N = 4; 8; 16-PSK

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 $K = 2$.

Hình 3.7 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.

Hình 3.8 trình bày xác suất báo động giả dưới dạng một hàm của ăng ten M tại trạm gốc khi sử dụng 8-PSK và SNR là 5 dB. Như dự đoán, xác suất báo động giả giảm theo số lượng ăng ten tại trạm gốc. Hơn nữa, kết quả này



Hình 3.8: Xác suất báo động giả N = 8 PSK , SNR=5; K = 2; 5; 10; 15 vs. M

.

cho thấy khả năng xảy ra báo động giả là tương đối thấp khi sử dụng đủ số lượng hoa tiêu thử nghiệm. Khi số lượng hoa tiêu đủ lớn, xác suất báo động giả sẽ nhanh chóng giảm đến 0. Điều này có nghĩa là thiết bị gây nhiễu có thể được phát hiện với xác suất rất cao bằng cách sử dụng một số lượng lớn hoa tiêu đào tạo cũng như một số lượng ăng ten đủ lớn.

3.5. Kết luận chương

Chương 3 của luận án đã khảo sát mô hình hệ thống Massive MIMO khi có thiết bị gây nhiễu hoặc tấn công chủ động, luận án đã đưa ra:

- Mô hình hệ thống khi có thiết bị gây nhiễu chủ động của mô hình Massive MIMO không tương quan trong điều kiện kênh truyền pha-đinh Rice.
- 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.
- Phương pháp tính xác suất phát hiện và xác suất báo động giả khi có thiết bị gây nhiễu trong những kịch bản khác nhau. Cách thức để nâng cao xác suất cảnh báo và giảm tối đa báo động giả.

Như vậy, với các kết quả giải tích mà nghiên cứu sinh đề xuất các kịch bản và mô hình khác nhau của hệ thống Massive MIMO dưới điều kiện kênh truyền pha-đinh Rice không tương quan về mặt không gian, đã đưa ra thuật toán phát hiện và cách xây dựng vùng phát hiện thiết bị gây nhiễu chủ động.

Chương 4
CẢI THIỆN XÁC SUẤT PHÁT HIỆN VÀ XÁC SUẤT BÁO ĐỘNG GIẢ TRONG HỆ THỐNG MASSIVE MIMO

Trong Chương 3 của luận án, NCS đã đề xuất một kỹ thuật để phát hiện hoạt động nhiễu hoa tiêu không chỉ làm giảm khả năng bảo mật mà còn khó phát hiện. Kỹ thuật này sử dụng ngẫu nhiên N-PSK trong các hệ thống Massive MIMO không tương quan không gian và trong điều kiện kênh truyền pha-đinh Rice. Phương pháp này chỉ yêu cầu hai giai đoạn đào tạo và không cần thông tin kênh truyền. 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. Trong chương này NCS đề xuất biện pháp để nâng cao xác suất phát hiện và giảm xác suất báo động giả thông qua những kịch bản sát với thực tế như thiết bị tấn công bất hợp pháp thông minh sẽ không lựa chọn xuất hiện tại những khe thời gian liên tiếp mà xuất hiện một cách ngẫu nhiên, và sử dụng một tập hợp nhiều hoa tiêu để nâng cao độ khó của việc dự đoán hoa tiêu của thiết bị bất hợp pháp. *Đóng góp của Chương 4 được trình bày trong công trình số 5,6.*

- **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," *Tạp chí Khoa học và Kỹ thuật - Học viện Kỹ*

thuật Quân sự , 2022, pp. 21-29

- **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," *IEEE Access*, vol. 10, 2022, pp. 125489-125498

4.1. Giới thiệu chung

Phân tập thời gian để chỉ các đơn vị đo thời gian nhỏ trong các hệ thống truyền thông. Phân tập thời gian là một phần quan trọng của kỹ thuật đa truy cập trong các mạng viễn thông. Phân tập thời gian giúp đảm bảo rằng quá trình truyền thông được thực hiện một cách chính xác và không xung đột trong các mạng di động. Phân tập thời gian đóng vai trò quan trọng trong việc phân biệt và đồng bộ hóa các tín hiệu và dữ liệu trên các kênh truyền thông. Đây cũng là lý do để NCS xây dựng phương pháp cải thiện xác suất phát hiện đúng và giảm thiểu xác suất báo động giả của hệ thống. 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 dựa trên phân tập thời gian.

- Sự gây nhiễu bởi những thiết bị gây nhiễu chủ động trước tiên được phân tích cho một số lượng ăng-ten tại trạm gốc nhỏ. Các tác động của nhiễu và các cuộc tấn công gây nhiễu sau đó được quan sát rõ ràng khi số lượng ăng-ten tại trạm gốc ngày càng lớn, thậm chí rất lớn.

- Trong phần này đề xuất một kế hoạch để phát hiện thiết bị gây nhiễu hoạt động bằng cách gây nhiễu hoa tiêu mà không cần có thông tin trạng

thái kênh truyền.

- Phân tích xây dựng vùng phát hiện của thiết bị gây nhiễu, đề xuất thêm thuật toán để tìm xác suất phát hiện và xác suất báo động giả dựa trên phân tập thời gian.

4.2. 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. Vì việc thu thập thông tin trạng thái kênh chính xác là điều tối quan trọng đối với trạm gốc để thực hiện phát hiện dữ liệu và thiết kế các vec tơ tiền mã hóa đường xuống. Do đó, một trong những chiến lược hiệu quả nhất để thiết bị bất hợp pháp J tấn công thông tin liên lạc hợp pháp là gây nhiễu ở giai đoạn đào tạo đường lên. Đặt $\mathcal{S}$ là tập hợp tất cả các hoa tiêu thử nghiệm ở kênh đường lên. Đối với hầu hết các thiết bị không dây được tiêu chuẩn hóa, bộ hoa tiêu thử nghiệm $\mathcal{S}$ được sử dụng bởi các thiết bị đầu cuối của người dùng hợp pháp thường được chỉ định rõ ràng trong thông số kỹ thuật.

Trong chương này, giả thiết $\mathcal{S}$ là một bộ mã N-PSK (phase-shift keying) với N ký hiệu được định nghĩa như sau $\mathcal{S} = \{e^{j2\pi m/N} : m \in \mathbb{Z}, 0 \leq m \leq N-1\}$.

Ngoài ra, hãy ký hiệu p_{X} là công suất truyền của thiết bị hợp pháp $X \in \mathcal{X}$ trong giai đoạn đào tạo hoa tiêu thử nghiệm đường lên. Trong phần này, giả định rằng p_{X} không thay đổi trong nhiều khung $\mathcal{NF}$.

Trong tập hợp hoa tiêu thử nghiệm $\ell \in \mathcal{K}_k$, chúng tôi giả định rằng thiết bị đầu cuối của người dùng hợp pháp B có thể truyền một hoa tiêu thử nghiệm

ngẫu nhiên $s_{\mathrm{B,k},\ell} \in \mathcal{S}$ để làm cho thiết bị đầu cuối của người dùng bất hợp pháp J không thể dự đoán trước được. Nói cách khác, tại bất kỳ thời điểm nào, thiết bị đầu cuối của người dùng bất hợp pháp J biết chính xác $\mathcal{S}$ nhưng nó không biết hoa tiêu thử nghiệm nào được truyền đi. Do đó, một trong những chiến lược tốt nhất mà thiết bị đầu cuối của thiết bị bất hợp pháp J có thể thực hiện là truyền một hoa tiêu thử nghiệm ngẫu nhiên $s_{\mathrm{J,k},\ell} \in \mathcal{S}$. Chúng ta có thể viết lại 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 $s_{\mathrm{J,k},\ell}, s_{\mathrm{B,k},\ell} \in \mathcal{S}$. Trong (4.1), (a) thu được vì $|s_{\mathrm{B,k},\ell}|^2 = 1$.

Giả thiết $\alpha_{k,\ell}$ làm tham số thỏa mãn $\alpha_{k,\ell} = 1$ nếu thiết bị đầu cuối của người dùng bất hợp pháp J truyền hoa tiêu thí điểm $\ell \in \mathcal{K}_k$. Ngược lại, $\alpha_{k,\ell} = 0$ nếu thiết bị đầu cuối của người dùng bất hợp pháp J không tấn công giai đoạn đào tạo thử nghiệm. 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 (AWGN) 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

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

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

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

Từ kết quả đạt được trong (4.1).

Một giả định rằng vị trí của trạm gốc và các thiết bị đầu cuối của người dùng không thay đổi qua nhiều khung truyền dẫn vô tuyến. Đối với khả năng định hướng phân tích, chúng ta giả định rằng các phần tử ăng-ten của trạm gốc A gọi chung là ULA. Vì vậy, chúng ta giả thiết $\bar{d}_{\mathrm{A}} = \pi d_{\mathrm{A}}/\lambda$ khoảng cách chuẩn hóa giữa các ăng-ten liền kề tại trạm gốc,λ là bước sóng tương ứng với tần số sóng mang. Hơn nữa, chúng ta ký hiệu d_{X} , $\forall \mathrm{X} \in \mathcal{X}$ khoảng cách từ trạm gốc đến người dùng X và $\theta_{\mathrm{X}} \in [-\pi, \pi]$, $\forall \mathrm{X} \in \mathcal{X}$ góc giữa đường nối trạm gốc với trạm người dùng X và hướng búp sóng chính của dải ăng-ten của trạm gốc. Mô hình hệ thống này đơn giản để NCS bắt đầu các kỹ thuật phân tích nhằm thu được những thông tin chi tiết có giá trị. Các mô hình phức tạp hơn, chẳng hạn như hệ thống đa người dùng, đa ăng-ten sẽ được nghiên cứu trong tương lai. 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 [82], chúng ta đạt được $\mathbf{g}_{\mathrm{X}}^{H}\mathbf{g}_{\mathrm{X}} = M, \forall \mathrm{X} \in \mathcal{X}$ và

$$\mathbf{g}_{\mathrm{J}}^{H}\mathbf{g}_{\mathrm{B}} = \psi(\theta_{\mathrm{B}}, \theta_{\mathrm{J}}, M) \tag{4.6}$$

$$= \frac{\sin(M\bar{d}_{\mathrm{A}}(\sin\theta_{\mathrm{B}} - \sin\theta_{\mathrm{J}}))}{\sin(\bar{d}_{\mathrm{A}}(\sin\theta_{\mathrm{B}} - \sin\theta_{\mathrm{J}}))} e^{j(M-1)\bar{d}_{\mathrm{A}}(\sin\theta_{\mathrm{B}} - \sin\theta_{\mathrm{J}})}. \tag{4.7}$$

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

$$\lim_{M\to\infty} \frac{|\psi(\theta_{\mathrm{B}}, \theta_{\mathrm{J}}, M)|}{M} = \begin{cases} 1, \text{nếu } \sin\theta_{\mathrm{B}} = \sin\theta_{\mathrm{J}}, \\ 0, \text{trường hợp khác.} \end{cases} \tag{4.8}$$

Trong phần này, giả thiết kênh truyền pha-đinh Rice không tương quan không gian [76]. Biểu thị κ_X là hệ số Rice và β_{X} là hệ số pha-đinh của $\mathbf{h}_{\mathrm{X}}$. Nhìn chung, κ_X và β_{X} không thay đổi trong nhiều khung vô tuyến liên tiếp. Nói cách khác độc lập với sự thay đổi của khung vô tuyến. Trong phần này, để hiểu rõ hơn,chúng tôi giả thiết rằng κ_X và β_{X} có được thông tin một cách hoàn hảo. Định nghĩa hệ số pha đinh phạm vi lớn tương ứng với thành phần LOS và thành phần NLOS của $\mathbf{h}_{\mathrm{X},k}$ là

$$\beta_{\mathrm{X,L}} = \frac{\kappa_{\mathrm{X}}}{\kappa_{\mathrm{X}}+1}\beta_{\mathrm{X}}; \quad \beta_{\mathrm{X,N}} = \frac{1}{\kappa_{\mathrm{X}}+1}\beta_{\mathrm{X}}. \tag{4.9}$$

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

$$\mathbf{h}_{\mathrm{X},k} = \beta_{\mathrm{X,L}}^{1/2}\mathbf{g}_{\mathrm{X}} + \beta_{\mathrm{X,N}}^{1/2}\mathbf{w}_{\mathrm{X},k} \tag{4.10}$$

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. Trong mô hình pha-đinh Rayleigh được xem xét trong các nghiên cứu trước là một trường hợp đặc biệt của mô hình nghiên cứu này vì nó có liên quan đến thành phần NLOS trong mô hình pha đinh Rice không tương quan, như là $\kappa_{\mathrm{X}} = 0$ và do đó $\beta_{\mathrm{X,L}} = 0$ và $\beta_{\mathrm{X,L}} = \beta_{\mathrm{X}}$ cho mọi $X \in \mathcal{X}$. Để thuận tiện, chúng ta ký hiệu $()_{\mathrm{Ri}}$ và $()_{\mathrm{Ra}}$ cho biết các tham số liên quan đến mô hình kênh pha-đinh Rice và Rayleigh pha đinh tương ứng.

4.3. Phương pháp phát hiện nhiễu hoa tiêu

Trong phần này, NCS đã đề xuất một phương pháp phát hiện nhiễu hoa tiêu thử nghiệm mới có tính đến các đặc điểm nổi bật của mô hình kênh pha-đinh Rice. Đầu tiên trình bày cách xác định khu vực phát hiện và thuật toán phát hiện. Sau đó, chứng minh rằng phương pháp phát hiện được đề xuất có khả năng tận dụng các đặc tính của kênh pha-đinh Rice để cung cấp xác suất phát hiện cao hơn so với phương pháp trước đó trong mô hình kênh pha-đinh Rayleigh. Tương tự, ta có $()_{\mathrm{J}}$ và $()_0$ chỉ ra các tham số khi thiết bị đầu cuối của người dùng bất hợp pháp J truyền các tín hiệu gây nhiễu và những tín hiệu đó khi J tương ứng không truyền tín hiệu gây nhiễu.

4.3.1. 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. Các cuộc tấn công có thể không xảy ra trong cùng một khung truyền dẫn hoặc trong hai khung truyền dẫn liên tiếp. Giả thiết rằng thiết bị gây nhiễu thông minh có thể xuất hiện ngẫu nhiên trong các khung truyền ngẫu nhiên để không bị dễ phát hiện nhất. 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:

$$z_{k,q} = \frac{1}{\sqrt{M}} \mathbf{y}_{k,\ell}^H \mathbf{y}_{q,u}. \tag{4.11}$$

Mặc dù (4.11) có biểu thức tương tự như những gì được đề xuất trong [43] cho mô hình kênh pha đinh Rayleigh, phương pháp được đề xuất của nghiên

cứu có tính mở rộng hơn vì nó không yêu cầu hai tín hiệu thử nghiệm phải trong cùng một khung truyền dẫn vô tuyến hoặc trong hai khung liên tiếp. 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:

$$a_{k,q} = \frac{1}{\sqrt{M}} \mathbf{f}^H_{q,u} \mathbf{f}_{k,\ell} \tag{4.12}$$

$$n_{k,q} = \frac{1}{\sqrt{M}} \left(\mathbf{f}^H_{q,u} \mathbf{n}_{k,\ell} + \mathbf{n}^H_{q,u} \mathbf{f}_{k,\ell} + \mathbf{n}^H_{q,u} \mathbf{n}_{k,\ell} \right). \tag{4.13}$$

Thay (4.4) vào (4.11) và sử dụng (4.12) và (4.13), chúng ta nhận được

$$z_{k,q} = a_{k,q} s_{\mathrm{B}} + n_{k,q}. \tag{4.14}$$

Chú ý rằng (4.14) có thể được coi là mối quan hệ đầu vào - đầu ra của kênh SISO trong đó s_{B} là ký hiệu N -PSK được truyền, $a_{k,q}$ tương đương hệ số kênh và $n_{k,q}$ là nhiễu tương đương .

Vì rất khó để xác định phân phối chính xác của $n_{k,q}$, chúng tôi áp dụng phương pháp tương tự như [43], trong đó chúng ta nghiên cứu thuộc tính thống kê khi M đủ lớn. 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 (4.11) - (4.14), chúng ta nhận thấy rằng

$$n_{k,q} = \frac{1}{\sqrt{M}} \mathbf{y}^H_{k,\ell} \mathbf{y}_{q,u} - a_{k,q} s_{\mathrm{B}}, \tag{4.15}$$

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

$$\lim_{M\to\infty} \frac{n_{k,q}}{\sigma_M} \xrightarrow{d} \mathcal{CN}(0,1). \tag{4.16}$$

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

$$\sigma_M^2 = \frac{N_0}{M}\left(\|\mathbf{f}_{q,u}\|^2 + \|\mathbf{f}_{k,\ell}\|^2 + MN_0\right). \tag{4.17}$$

Nói cách khác, khi M phát triển lớn, $n_{k,q}/\sigma_M$ hội tụ thành một biến ngẫu nhiên Gauss có giá trị phức với giá trị trung bình là 0 và phương sai σ_M^2. Kết quả số trong [43] cho thấy rằng giá trị gần đúng này tương đối chặt chẽ ngay cả đối với một số lượng nhỏ ăng-ten tại trạm gốc, ví dụ với số ăng-ten $M = 5$. Nói chung, phương sai nhiễu σ_M^2 phụ thuộc vào một số yếu tố, bao gồm sự xuất hiện của tín hiệu gây nhiễu, mô hình kênh và vị trí của hai hoa tiêu huấn luyện.

4.3.2. 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 (4.17) nhận được kết quả như sau:

$$\begin{aligned}\sigma_{\mathrm{Ri,J},M}^2 = \frac{N_0}{M}\Big(&\|\sqrt{p_{\mathrm{B}}}\mathbf{h}_{\mathrm{B},k} + \sqrt{p_{\mathrm{J}}}\mathbf{h}_{\mathrm{J},k}s_{k,\ell}\|^2 \\ &+ \|\sqrt{p_{\mathrm{B}}}\mathbf{h}_{\mathrm{B},q} + \sqrt{p_{\mathrm{J}}}\mathbf{h}_{\mathrm{J},q}s_{q,u}\|^2 + MN_0\Big).\end{aligned} \tag{4.18}$$

Chú ý rằng $\sigma_{\mathrm{Ri,J},M}^2$ trong (4.18) liên kết với σ_M^2 trong công thức (4.17), nhưng chỉ số dưới Ri, J chỉ ra rằng mô hình kênh được xem xét của là pha-đinh Rice và quá trình truyền thông bị tấn công gây nhiễu. Vì biểu thức (4.18) chứa các vec tơ kênh tức thời, nên việc quan sát các thuộc tính là không quan trọng. Tuy nhiên, những kết quả này với số ăng-ten giới hạn. Cụ thể, khi số ăng-ten

M rất lớn lớn, tức là $M \to \infty$, chúng ta có thể tính giá trị giới hạn của nó như sau:

$$\begin{aligned}\bar{\sigma}^2_{\mathrm{Ri,J}} &= \lim_{M\to\infty} \sigma^2_{\mathrm{Ri,J},M} \\ &= N_0\Big(2\bar{\beta}_{\mathrm{B},k,k} + 2\bar{\beta}_{\mathrm{J},k,k} + N_0 \\ &\quad + 2\sqrt{\bar{\beta}_{\mathrm{B},k,k}\bar{\beta}_{\mathrm{J},k,k}}\psi(\theta_{\mathrm{B}},\theta_{\mathrm{J}})\mathrm{Re}\{s_{k,\ell} + s_{q,u}\}\Big), \end{aligned} \tag{4.19}$$

được giới hạn từ phía trên nhờ định luật bảo toàn năng lượng và mức công suất phát hữu hạn. Trong (4.19), chúng ta định nghĩa cho mọi $\mathrm{X} \in \mathcal{X} = \{\mathrm{B}, \mathrm{J}\}$ như sau

$$\bar{\beta}_{\mathrm{X},k,q} = \begin{cases} p_{\mathrm{X}}\beta_{\mathrm{X}}, \text{nếu } k = q, \\ p_{\mathrm{X}}\beta_{\mathrm{X,L}}, \text{trường hợp khác.} \end{cases} \tag{4.20}$$

Do đó, hệ số kênh tương đương trong trường hợp này được cho là:

$$\begin{aligned} a_{\mathrm{Ri,J},k,q} = \frac{1}{\sqrt{M}}&(\sqrt{p_{\mathrm{B}}}\mathbf{h}_{\mathrm{B,q}} + \sqrt{p_{\mathrm{J}}}\mathbf{h}_{\mathrm{J,q}}s_{q,u})^H \\ &\times (\sqrt{p_{\mathrm{B}}}\mathbf{h}_{\mathrm{B,k}} + \sqrt{p_{\mathrm{J}}}\mathbf{h}_{\mathrm{J,k}}s_{k,\ell}), \end{aligned} \tag{4.21}$$

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 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

$$\begin{aligned}\bar{a}_{\mathrm{Ri,J},k,q} &= \lim_{M\to\infty} \frac{a_{\mathrm{Ri,J},k,q}}{\sqrt{M}} \\ &= \bar{\beta}_{\mathrm{B},k,q} + \bar{\beta}_{\mathrm{J},k,q}s^*_{q,u}s_{k,\ell} \\ &\quad + \sqrt{\bar{\beta}_{\mathrm{B},k,q}\bar{\beta}_{\mathrm{J},k,q}}\psi(\theta_{\mathrm{B}},\theta_{\mathrm{J}})(s^*_{q,u} + s_{k,\ell}), \end{aligned} \tag{4.22}$$

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.

4.3.3. Không có tín hiệu gây nhiễu chủ động

Để xem xét một cách tổng quát hơn, chúng ta xem xét mô hình hệ thống không bị có thiết bị tấn công. 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 (4.17) và (4.12), và ta có

$$a_{\mathrm{Ri},0,k,q} = \frac{1}{\sqrt{M}} \mathbf{h}^H_{\mathrm{B},q} \mathbf{h}_{\mathrm{B},k}, \tag{4.23}$$

$$\sigma^2_{\mathrm{Ri},0,M} = \frac{N_0}{M} \left(p_{\mathrm{B}} \|\mathbf{h}_{\mathrm{B},k}\|^2 + p_{\mathrm{B}} \|\mathbf{h}_{\mathrm{B},q}\|^2 + MN_0 \right). \tag{4.24}$$

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:

$$\bar{a}_{\mathrm{Ri},0,k,q} = \lim_{M\to\infty} \frac{|a_{\mathrm{Ri},0,k,q}|}{\sqrt{M}} = \bar{\beta}_{\mathrm{B},k,q} \tag{4.25}$$

$$\bar{\sigma}^2_{\mathrm{Ri},0} = \lim_{M\to\infty} \sigma^2_{\mathrm{Ri},0,M} = N_0 \left(2\bar{\beta}_{\mathrm{B},k,k} + N_0 \right). \tag{4.26}$$

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.

4.3.4. Thuật toán phát hiện

Chúng ta nhớ lại rằng $z_{k,q}$ có thể được coi là tín hiệu nhận được tương đương của kênh SISO với mối quan hệ đầu vào - đầu ra được cho trong công thức (4.11). Bây giờ chúng ta xây dựng vùng phát hiện dựa trên tích vô hướng $z_{k,q}$ để trạm gốc có thể quyết định xem liệu một thiết bị đầu cuối của người dùng bất hợp pháp có gây nhiễu cho các hoa tiêu mong muốn hay không. Lưu ý $z_{k,q}$ là tổng của ký hiệu N-PSK được chia tỷ lệ bởi $a_{\mathrm{Ri},0,k,q}$ và nhiễu Gauss với giá trị trung bình 0 và phương sai $\sigma^2_{\mathrm{Ri},0,M}$. Nhìn chung, trạm gốc chưa có ước lượng chính xác về hệ số suy hao quy mô nhỏ trước các giai đoạn huấn luyện. Điều này có nghĩa là nó không biết chính xác $a_{\mathrm{Ri},0,k,q}$ và $\sigma^2_{\mathrm{Ri},0,M}$ trước khi đưa ra quyết định về sự hiện diện của các tín hiệu gây nhiễu. Tuy nhiên, vì các thiết bị đầu cuối của người dùng không di chuyển trong một khoảng thời gian đủ dài, nên có thể xác nhận rằng trạm gốc có thể ước tính hệ số suy hao trên quy mô lớn β_{B} và $\beta_{\mathrm{B,L}}$ rất chính xác. Do đó, đối với một bộ điều chế N -PSK nhất định và cho số lượng ăng-ten đủ lớn M, chúng ta đề xuất các vùng phát hiện là các vòng tròn bán kính $\bar{\sigma}_{\mathrm{Ri},0}$ với các tâm tại các đường N-PSK được chia tỷ lệ với hệ số tỷ lệ chung là $\sqrt{M}\bar{a}_{\mathrm{Ri},0,k,q}$. Để giảm ảnh hưởng của nhiễu đối với độ chính xác của phát hiện, chúng ta cũng đề xuất lựa chọn một số hoa tiêu ngẫu nhiên K, trong đó các hoa tiêu $K \geq 2$, N-PSK được sử dụng cho mục đích phát hiện gây nhiễu. Dựa trên các vùng phát hiện này và việc sử dụng các hoa tiêu thử nghiệm K, chúng ta đề xuất phương pháp phát hiện sau:

- *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 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 $\mathcal{K}_q \in \mathcal{F}_u$, trạm gốc thực hiện các bước sau:

  3.1. Tính giá trị của tích vô hướng $z_{k,q}$.

  3.2. Tính $d_m = |z_{k,q} - \sqrt{M}\bar{a}_{\mathrm{Ri},0,k,q}e^{jm2\pi/N}|$ với mỗi $m \in 0, 1, \cdots, N-1$. Chú ý rằng d_m có thể được coi là khoảng cách từ hệ số vô hướng nhận được từ tín hiệu thứ m-th của N-PSK symbol

  3.3. Tính khoảng cách nhỏ nhất, được xác định là $d_{\min} = \min_{0 \le m \le (N-1)} d_m$.

  3.4. Nếu $d_{\min} < \bar{\sigma}_{\mathrm{Ri},0}$ sau đó trạm gốc quyết định rằng các hoa tiêu huấn luyện không bị gây nhiễu; nếu không, nó quyết định rằng chúng bị gây nhiễu, tức là tồn tại một thiết bị đầu cuối người dùng bất hợp pháp đang hoạt động.

- *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.

Nhấn mạnh rằng số lượng cặp được chọn càng lớn thì quyết định xác suất càng chính xác. Tuy nhiên, lợi ích đi kèm với chi phí cao hơn và phức tạp hơn về mặt tính toán. Cũng chú ý rằng việc sử dụng nhiều cặp hoa tiêu thử

nghiệm hơn để tận dụng sự đa dạng theo thời gian là một trong những điểm khác biệt chính giữa nghiên cứu này so với những nghiên cứu trước đây. Kết quả mô phỏng và tính toán số được trình bày ở phần sau.

4.3.5. 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. (4.27) cho $a_{k,q}$, khác 0, chúng ta nhận được:

$$\tilde{z}_{k,q} = s_{\mathrm{B}} + \frac{n_{k,q}}{a_{k,q}}. \tag{4.27}$$

Bán kính của mỗi vùng phát hiện được đề xuất tỷ lệ với
$D_{\mathrm{Ri},0,k,q} = \sigma^2_{\mathrm{Ri},0,k,q}/|a_{\mathrm{Ri},0,k,q}|^2$. Ngoài ra, bán kính của vòng tròn, nơi tỷ số $z_{k,q}$ xuất hiện với xác suất cao trong khi thiết bị gây nhiễu đang hoạt động, tỷ lệ với $D_{\mathrm{Ri,J},k,q} = \sigma^2_{\mathrm{Ri,J},k,q}/|a_{\mathrm{Ri,J},k,q}|^2$. Về nguyên tắc, xác suất phát hiện gần bằng 0 khi $D_{\mathrm{Ri,J},k,q} \leq D_{\mathrm{Ri},0,k,q}$ và nó tăng theo tỷ lệ $D_{\mathrm{Ri,J},k,q}/D_{\mathrm{Ri},0,k,q}$ khi $D_{\mathrm{Ri,J},k,q} > D_{\mathrm{Ri},0,k,q}$. Sau đó, $D_{\mathrm{Ri,J},k,q}/D_{\mathrm{Ri},0,k,q}$ càng lớn càng tốt. Đáng chú ý, chúng ta có thể biểu thị $D_{\mathrm{Ri,J},k,q}/D_{\mathrm{Ri},0,k,q} = D_{\mathrm{Ri,J},k,k}/D_{\mathrm{Ri},0,k,k}$ cho tất cả q. Điều này có nghĩa là hiệu suất của phương pháp được đề xuất cho phép linh hoạt trong việc kiểm tra sự tồn tại của các thiết bị gây nhiễu thường xuyên.

4.4. Kết quả mô phỏng

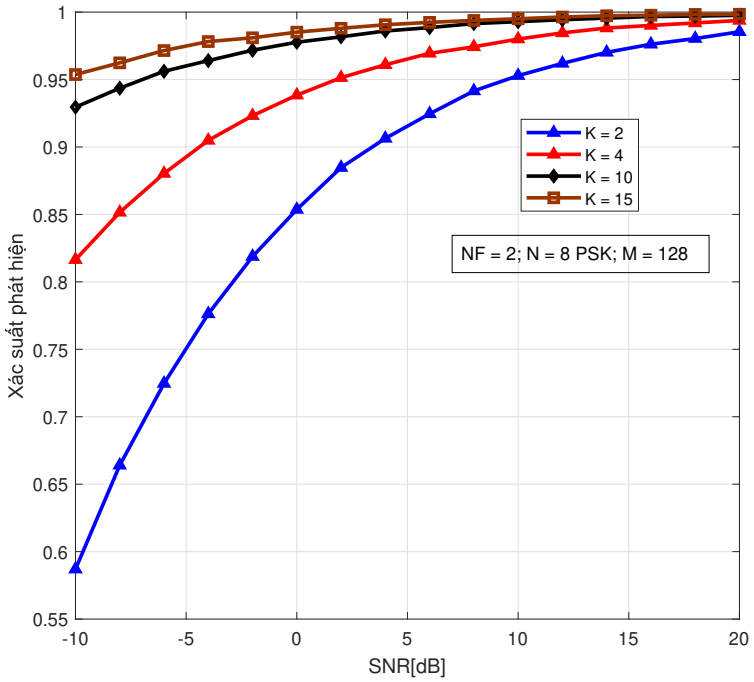
Phần này cung cấp một số kết quả mô phỏng và tính toán số để kiểm chứng các kết quả phân tích giải tích đã trình bày ở Mục 4.3. Trong kịch bản mô phỏng này NCS đã áp dụng phân tập thời gian để nâng cao xác suất phát hiện thiết bị tấn công và giảm xác suất báo động giả. Cụ thể sử dụng

tập hợp nhiều hoa tiêu ngẫu nhiên trong nhiều khung truyền vô tuyến dưới sự ảnh hưởng của góc tới.

Xét một mạng di động đơn tế bào trong đó trạm gốc được đặt ở chính giữa tế bào trong khi thiết bị đầu cuối hợp lệ (nút B) và thiết bị gây nhiễu chủ động (nút J) được bố trí ngẫu nhiên trong cell. Giả thiết ảnh hưởng của hiệu ứng che chắn bị bỏ qua, khi đó hệ số suy hao đường truyền phạm vi lớn được tính như sau [72, 78]

$$\beta_{\mathrm{X,Y}} = 32.4 + 10 n_{\mathrm{Y}} \log_{10}(d_{\mathrm{3D,X}}) + 20 \log_{10}(f_{\mathrm{c}}).$$

trong đó $X \in \mathcal{X}$, $Y \in \mathcal{Y} = \{\mathrm{L}, \mathrm{N}\}$, $d_{\mathrm{3D,X}}$ là khoảng cách tính theo mét từ trạm gốc đến nút X trong không gian 3 chiều, $f_{\mathrm{c}} = 3.5$ GHz là tần số sóng mang, n_{Y} là hệ số mũ suy hao đường truyền (PLE: path-loss exponent). Ngoài ra, $d_{\mathrm{3D,X}}$ được tính như sau $d_{\mathrm{3D,X}} = \sqrt{d_{\mathrm{2D,X}}^2 + (h_{\mathrm{A}} - h_{\mathrm{X}})^2}$ trong đó $d_{\mathrm{2D,X}}$ là khoảng cách từ trạm gốc tới nút X trong không gian 2 chiều, h_{A} là chiều cao của trạm gốc A, và h_{X} là chiều cao của nút X [1]. Không mất tính tổng quát, giả thiết $h_{\mathrm{A}} = 10$ m và $h_{\mathrm{B}} = h_{\mathrm{E}} = 1.5$ m. Nghiên cứu này xem xét môi trường cell lớn ở đô thị (UMa: Urban Macro), khi đó $n_{\mathrm{L}} = 2$ cho thành phần truyền tầm nhìn thẳng LOS và $n_{\mathrm{N}} = 2.9$ cho thành phần truyền không tầm nhìn thẳng NLOS [72, 78]. Theo [1], đối với môi trường UMa thì κ tính theo dB là một biến ngẫu nhiên Gauss $\mathcal{N}(9, 3.5)$. Để đơn giản, chúng ta giả thiết $\kappa_{\mathrm{B}} = \kappa_{\mathrm{E}} = 9$ dB. Giả thiết hệ thống hoạt động với băng thông 10 MHz, công suất phát ở trạm gốc là $p_{\mathrm{d}} = 46$ dBm, công suất phát ở thiết bị đầu cuối hợp lệ là $p_{\mathrm{P}} = 24$ dBm và mật độ công suất tạp âm nhiệt là $N_0 = -174$dBm/Hz. Tốc độ dữ liệu được tính cho một sóng mang con băng thông 15kHz. Giả thiết khoảng cách giữa các ăng-ten lân cận tại trạm gốc



Hình 4.1: Xác suất phát hiện tỉ lệ với SNR với số lượng hoa tiêu là $2, 4, 10, 15$, số khung truyền dẫn NF $= 2$, số PSK $= 8$, M $= 128$, $\mathrm{P_B} = 24$ dBm, $\mathrm{P_J} = 24$ dBm, and $\Phi_\mathrm{B} = 0$ rad và $\Phi_\mathrm{J} = 0.1$ rad

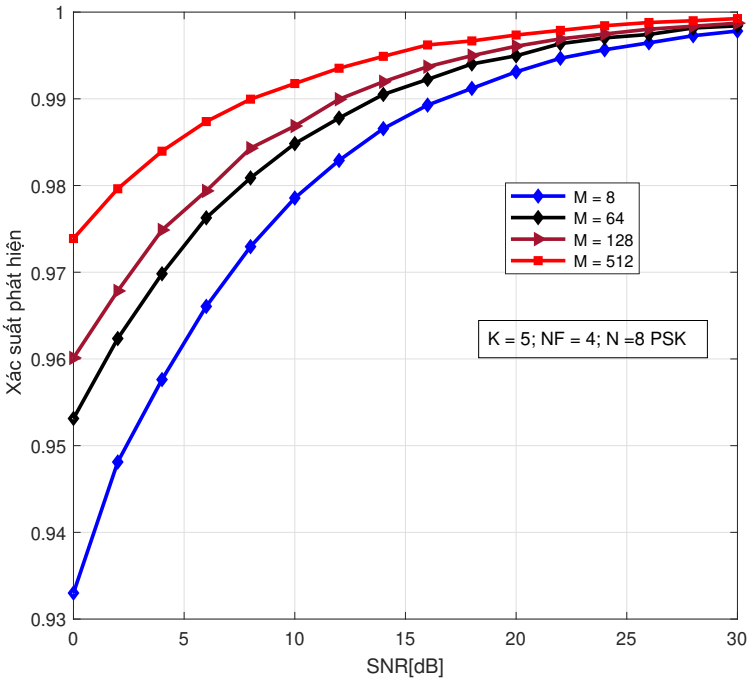
bằng nửa bước sóng, tứclà $d = 0.5$. Giả thiết hệ số tạp âm tại trạm gốc là 9dB/Hz trong khi hệ số tạp âm tại nút B và tại nút J là 5 dB/Hz. Không mất tính tổng quát, giả thiết $\Phi_\mathrm{B} = 0$[rad].

Trước hết, chúng ta xem xét một kịch bản mô phỏng trong đó thiết bị gây nhiễu chủ động, hay nút J, 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 J và từ nút B đến trạm gốc đều là 300m, ii) hệ số mô hình kênh Rician là $\kappa_\mathrm{B} = \kappa_\mathrm{J} = 9$ dB, và iii) kết quả mô phỏng được lấy trung bình của 200.000 mẫu.

Hình 4.1 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 K $\in$

$\{2, 4, 10, 15\}$. Sơ đồ điều chế được mô phỏng là 8 -PSK. Như mong đợi, xác suất phát hiện tăng với giá trị SNR, trong miền SNR cao, xác suất phát hiện đạt đến 1. Đáng chú ý, số lượng hoa tiêu thử nghiệm càng lớn thì xác suất phát hiện càng lớn. Ngay cả với SNR thấp $= -10$ [dB] và một số hoa tiêu thử nghiệm $K = 2$, xác suất phát hiện là khoảng 58%. Khi tăng số lượng hoa tiêu lên $K = 4$, xác suất phát hiện tăng lên rất nhiều lên 88% và dần dần tiến tới 1 với SNR cao. Nếu số lượng tín hiệu hoa tiêu vượt quá $K = 1$, xác suất phát hiện cuộc tấn công là rất cao. Nó vượt quá 93% và đạt gần một. Một khi hệ thống khai thác một số lượng đủ lớn các hoa tiêu thử nghiệm, thiết bị tấn công sẽ khó khăn hơn trong việc thu thập thông tin kênh truyền, mô phỏng hoa tiêu thử nghiệm của người dùng được cấp phép và tấn công vào quá trình truyền thông. Khi đó trạm gốc có thể dễ dàng phát hiện ra thiết bị tấn công. Kết quả cho thấy rằng trong truyền thông Massive MIMO với các kênh pha đinh Rice, hệ thống có thể khai thác một số lượng lớn các ăng-ten và một số hoa tiêu thử nghiệm thích hợp để phát hiện thành công người dùng bất hợp pháp với xác suất cao.

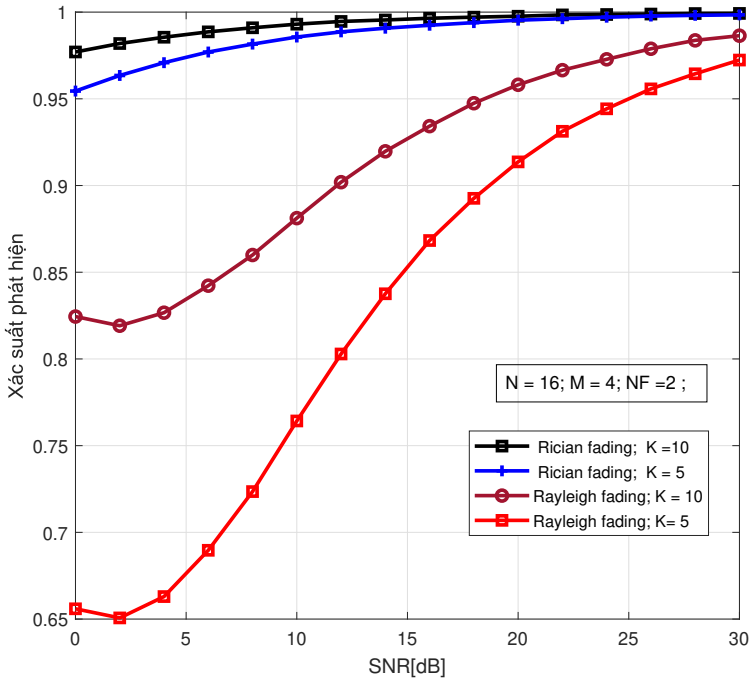
Hình. 4.2 hiển thị xác suất phát hiện so với các giá trị SNR khác nhau của hệ thống của chúng tôi cho $N = 8$ PSK và một số lượng ăng ten khác nhau tại BS. Xác suất phát hiện tăng theo giá trị SNR. Mặc dù xác suất phát hiện đã được cải thiện khoảng $0, 93$ với một vài ăng ten ở BS và bằng cách sử dụng số hoa tiêu thử nghiệm $K = 5$ chỉ trong 4 khung truyền dẫn. Khi BS được trang bị nhiều ăng ten hơn, ví dụ: với $M = 128$, xác suất phát hiện có thể lên đến $0, 96$. Theo xu hướng, xác suất phát hiện có thể gần bằng 1 khi có số lượng đủ lớn các ăng-ten tại BS. Ngoài ra, số lượng ăng ten BS cao hơn cung cấp xác suất phát hiện tốt hơn nhờ vào việc tăng cường kênh và



Hình 4.2: Xác suất phát hiện tỉ lệ với SNR với số hoa tiêu K = 5, số khung truyền dẫn là NF = 4, N = 8-PSK, $P_B = 1$, $P_J = 1$ and $\Phi_B = 0$ rad, and $\Phi_J = 0.1$ rad.

lan truyền thuận lợi [81].

Trong khi đó, Hình 4.3 so sánh xác suất phát hiện giữa các kênh pha-đinh Rayleigh và Rice dưới dạng một hàm của SNR với M = 4, K $\in \{5; 10\}$, NF = 2, N = 16, $P_B = 24$ [dBm], $P_J = 24$ [dBm], $\Phi_B = 0,1$ [rad] và $\Phi_J = 0,1$ [rad]. Với $K = 5$, đối với hệ thống trên mô hình kênh pha đinh Rayleigh, xác suất phát hiện được giới hạn thấp hơn 65% trong đó các tham số được xem xét và tốt hơn khi SNR tăng. Trong khi đó, với cùng số lượng hoa tiêu, trong mô hình kênh pha đinh Rice, xác suất phát hiện được cải thiện đáng kể với giới hạn thấp hơn của xác suất phát hiện 95%, tăng 30% so với mô hình kênh Rayleigh và nhanh chóng đạt đến 1 khi SNR tăng. Chúng ta quan sát thấy rằng xác suất phát hiện của hệ thống khi có các thành phần LOS là rất cao mặc dù BS được trang bị số ăng-ten không nhiều và ngay cả

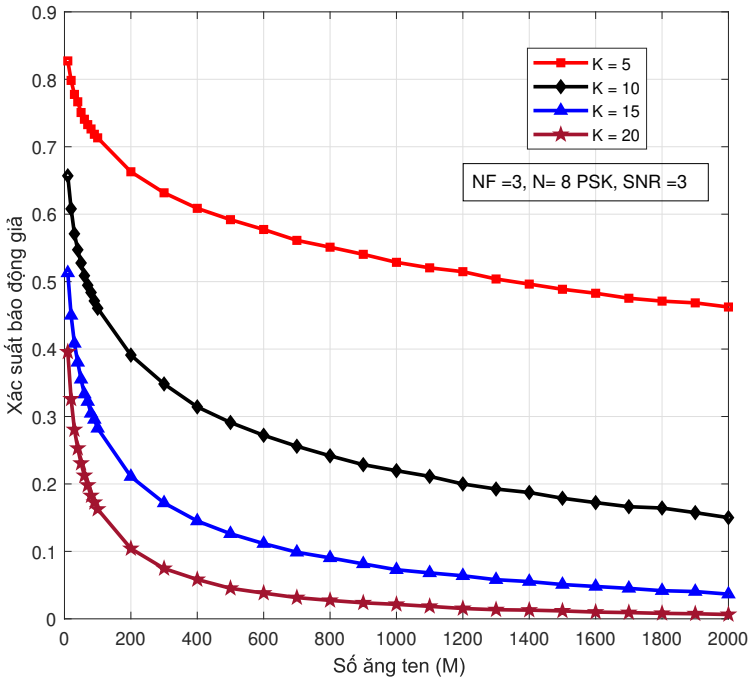


Hình 4.3: Xác suất phát hiện của kênh Rayleigh pha đinh và kênh truyền pha đinh Rice tỉ lệ với SNR, số ăng ten $M = 4$, số hoa tiêu thử nghiệm K $= 5; 10$, số khung truyền dẫn NF $= 2$, N $= 16$PSK, $P_B = 24$ dBm, $P_J = 24$ dBm and $\Phi_B = 0.1$ rad và $\Phi_J = 0.1$ rad.

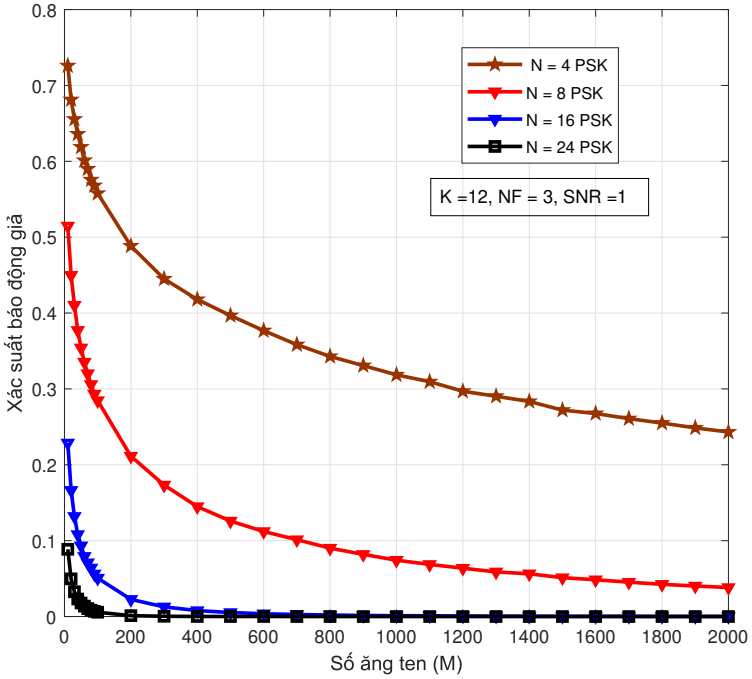
khi thiết bị tấn công có cùng góc đến (AOA) với người dùng.

Hình. 4.4 hiển thị xác suất báo động giả so với số lượng ăng-ten BS với N $= 8$, $\Phi_J = 0$ [rad] và $\Phi_B = 0,1$ [rad]. Số lượng hoa tiêu được chọn trong tập hợp $\{5, 10, 15, 20\}$ trong ba khung, tức là NF $= 3$. Như dự đoán, xác suất báo động giả giảm dần khi số lượng ăng ten BS tăng lên. Hơn nữa, tất cả các kết quả cho thấy xác suất báo động giả là tương đối thấp với một số lượng đủ lớn các hoa tiêu. Bên cạnh đó, xác suất báo động giả bằng 0 khi số lượng ăng-ten đủ lớn. Điều này có nghĩa là thiết bị gây nhiễu có thể được phát hiện một cách hiệu quả với xác suất rất cao thông qua việc sử dụng một số lượng lớn các hoa tiêu cũng như một số lượng lớn các ăng-ten.

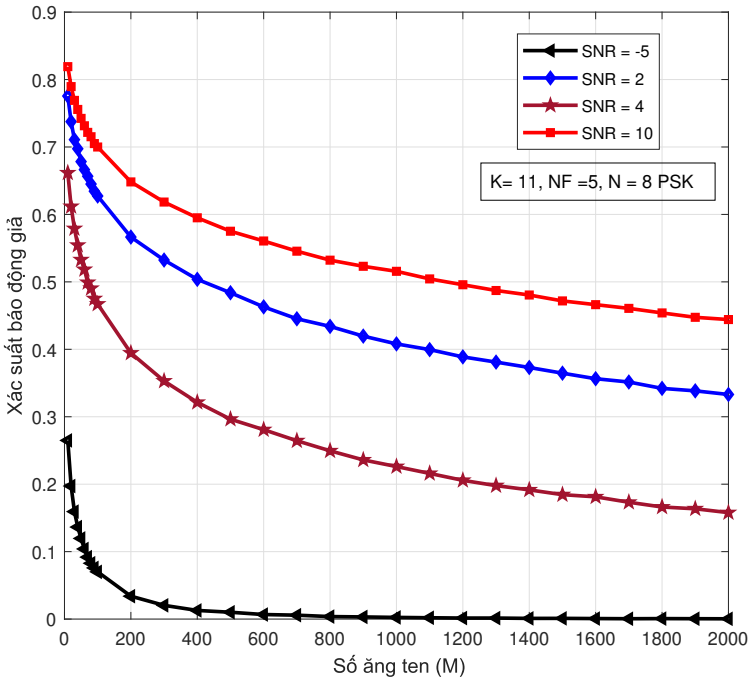
Hình. 4.5 trình bày xác suất báo động giả cho sau khi thiết lập thông số khác bao gồm $\Phi_J = 0$ [rad], $\Phi_B = 0,1$ [rad] với số PSK $= \{4, 8, 16, 24\}$, số



Hình 4.4: Xác suất cảnh báo sai tỉ lệ với M với số hoa tiêu là5, 10, 15, 20, SNR = 3 dB, số khung truyền dẫn NF = 3, với N = 8 PSK $\Phi_J = 0$ rad, $\Phi_B = 0.1$ rad.



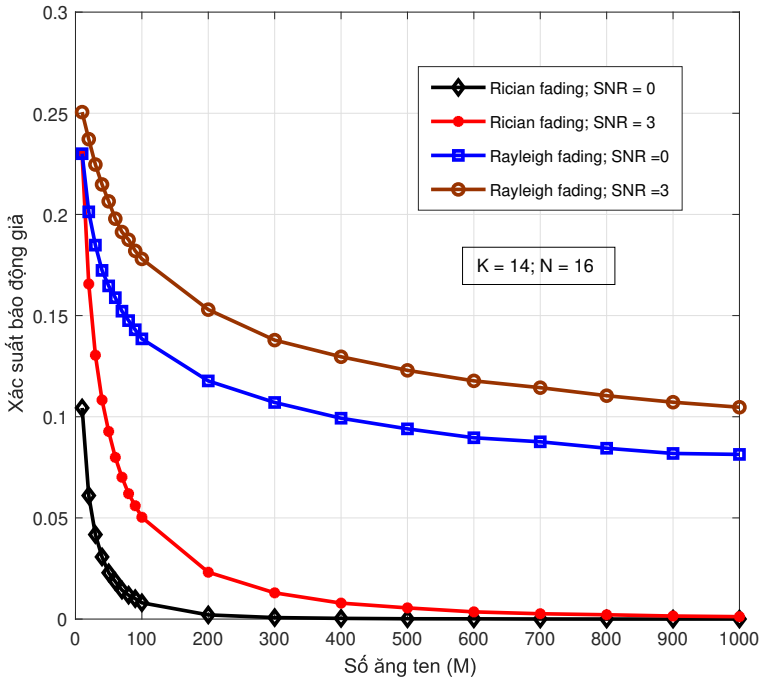
Hình 4.5: Xác suất cảnh báo sai tỉ lệ với số ăn-ten tại BS; PSK lần lượt là 4,8,16,24, số hoa tiêu là K = 12, số khung truyền dẫn NF = 3, $\Phi_J = 0$ rad, $\Phi_B = 0.1$ rad, SNR = 1 dB.



Hình 4.6: Xác suất báo động giả của kênh pha đinh Rice 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].

lượng hoa tiêu là K = 12 và trong 3 khung truyền dẫn khi số lượng ăng ten tăng lên. Hệ thống xác suất phát hiện rất cao khi SNR cao, và có xác suất báo động giả thấp hơn. Thậm chí xác suất báo động giả có thể đạt được rất thấp, gần bằng 0, nó có thể được coi là hệ thống hầu như không có báo động giả.

Hình. 4.7 cho thấy xác suất báo động giả giảm ngay cả khi $\Phi_J = 0$ rad, $\Phi_B = 0,1$ rad với SNR = -5, 2, 4, 10, số lượng hoa tiêu là K = 11 và trong 2 khung truyền dẫn khi số lượng ăng ten tăng lên. Các kết quả này cho thấy khi SNR thấp hệ thống có xác suất báo động giả ít hơn, thậm chí xác suất báo động giả gần bằng 0. Hình. 4.6 hiển thị kết quả của các kênh pha-đinh Rice. Những kết quả này đã chứng minh rằng trong các kênh pha-đinh Rice, xác suất báo động giả gần như bằng 0 trong khi số lượng ăng-ten tăng lên và



Hình 4.7: So sánh xác suất báo động giả của kênh truyền pha-đinh Rayleighvà kênh truyền pha-đinh Rice tỉ lệ với số ăng ten tại trạm gốc khi SNR $\in \{0, 3\}$ [dB] , K = 14, NF = 8, $N = 16$, $\Phi_J = 0.1$ [rad], $\Phi_B = 0.1$ [rad].

số khóa PSK đủ lớn.

Hình. 4.7 so sánh xác suất báo động giả của hệ thống trên các kênh pha-đinh Rayleigh và các kênh pha-đinh Rice với SNR $= 0; 3$ [dB], K $= 14$, NF $= 8$, N $= 16$, $P_B = 24$ [dBm], $P_J = 24$ [dBm], góc tới AoA của người dùng hợp pháp $\Phi_B = 0.1$ [rad] và góc tới AoA $\Phi_J = 0.1$ [rad] của thiết bị gây nhiễu tỉ lệ với số ăng-ten tại trạm gốc. Mặc dù góc AOA của thiết bị gây nhiễu và AOA của người dùng giống hệt nhau, tuy nhiên, xác suất báo động sai rất thấp. Trong các kịch bản đã xem xét của chúng tôi dưới các kênh pha-đinh Rice, xác suất báo động giả nhanh chóng tiến về 0 khi số lượng ăng ten BS tăng lên. Trong tất cả các tham số được thiết lập, hệ thống trên các kênh pha-đinh Rayleigh mang lại xác suất báo động cao hơn khoảng 10% so với xác suất báo động giả của hệ thống trên các kênh pha-đinh Rice. Đặc

biệt, kết quả chứng minh rằng xác suất báo động sai của khung được xem xét của chúng tôi nhỏ hơn đáng kể so với xác suất được xem xét trong [42]. Kết quả cho thấy lợi ích của một số lượng lớn ăng-ten trong việc bảo vệ người dùng hợp pháp khỏi các cuộc tấn công gây nhiễu.

4.5. 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 mô hình hệ thống Massive MIMO dưới điều kiện kênh truyền pha-đinh Rice, luận án đã đưa ra:

- Mô hình hệ thống khi có thiết bị gây nhiễu chủ động của mô hình Massive MIMO không tương quan trong điều kiện pha-đinh Rice.
- 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. Từ đó xây dựng khu vực phát hiện tấn công gây nhiễu của thiết bị bất hợp pháp.
- Phương pháp tính xác suất phát hiện và xác suất báo động giả khi có thiết bị gây nhiễu trong những kịch bản khác nhau. Đề xuất kỹ thuật để nâng cao xác suất cảnh báo và giảm tối đa báo động giả dựa trên phân tập thời gian.

Như vậy, với các kết quả giải tích mà nghiên cứu sinh đề xuất các kịch bản và mô hình khác nhau của hệ thống Massive MIMO dưới điều kiện kênh truyền pha-đinh Rice không tương quan về mặt không gian, đã đưa ra thuật toán phát hiện và cách xây dựng vùng phát hiện thiết bị gây nhiễu chủ động và kỹ thuật nâng cao độ tin cậy của phương pháp phát hiện dựa trên phân tập thời gian.

KẾT LUẬN VÀ HƯỚNG NGHIÊN CỨU TƯƠNG LAI

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 phương pháp tấn công trong mạng Massive MIMO, các tham số đánh giá dung lượng bảo mật của hệ thống để từ đó đưa ra giải pháp đảm bảo an toàn thông tin;

2. Thiết lập biểu thức giải tích đánh giá dung lượng bảo mật của hệ thống thông tin vô tuyến MIMO cỡ rất lớn trong điều kiện kênh truyền pha-đinh Rice không tương quan về không gian.

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 trong điều kiện kênh truyền pha-đinh Rice. Đề xuất thuật toán phát hiện và cách xây dựng vùng phát hiện thiết bị gây nhiễu chủ động.

4. Đề xuất những phương pháp nâng cao xác suất phát hiện và giảm thiểu báo động giả cho hệ thống Massive MIMO trong điều kiện kênh truyền pha-đinh Rice khi có thiết bị gây nhiễu chủ động dựa trên phân tập thời gian.

B. Hướng phát triển tiếp theo

Luận án đã có những đóng góp khoa học cho việc nghiên cứu sơ đồ phát

hiện thiết bị nghe lén và thiết bị gây nhiễu chủ động dựa trên việc truyền ngẫu nhiên các tín hiệu thí điểm đã được điều chế N -PSK. Sơ đồ phát hiện chỉ yêu cầu hai khe đào tạo thực hiện phát hiện tại trạm gốc mà không cần biết trước về các kênh tức thời. Nghiên cứu đã chỉ ra rằng thiết bị nghe lén thụ động không ảnh hưởng đến dung lượng bảo mật của hệ thống MIMO dưới điều kiện kênh truyền Rayleigh pha đinh, nhưng ảnh hưởng đến dung lượng bảo mật của hệ thống MIMO cỡ rất lớn dưới điều kiện kênh truyền pha-đinh Rice. Nghiên cứu đã đưa ra những khám phá để xác suất phát hiện chính xác cao tiệm cận với 1 và xác suất báo động giả thấp tiện cận 0. Kết quả số cho thấy sơ đồ phát hiện được đề xuất cung cấp xác suất phát hiện cao và xác suất báo động giả thấp hơn với nhiều cài đặt. Đây là một trong những hướng tiềm năng cho nghiên cứu trong tương lai. 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 truyền thông Massive MIMO với kênh truyền pha-đinh Rice tương quan về mặt 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 bị gây nhiễu chủ động.
- Nghiên cứu phương pháp phát hiện các thiết bị không được cấp phép trong hệ thống Massive MIMO cỡ rất lớn tương quan không gian đa người dùng.

DANH MỤC CÁC CÔNG TRÌNH ĐÃ CÔNG BỐ

- **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.
- **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,"*Tạp chí Khoa học và Kỹ thuật - Học viện Kỹ thuật Quân sự* , 2022, pp. 21-29
- **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)
- **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.
- **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.
- **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.

Tài liệu tham khảo

[1] 3GPP TR 38.901. *Study on channel model for frequencies from 0.5 to 100 GHz*. Technical Report v.15.0.0. 3GPP, June 2018.

[2] 3GPP TR 38.912. *Study on New Radio (NR) access technology (Release 15)*. Technical Report v.15.0.0. 3GPP, June 2018.

[3] A. Adhikary and A. Ashikhmin. "Uplink Massive MIMO for Channels with Spatial Correlation". In: *2018 IEEE Global Communications Conference (GLOBECOM)*. 2018, pp. 1–6.

[4] H. Akhlaghpasand et al. "Jamming Detection in Massive MIMO Systems". In: *IEEE Wireless Commun. Lett.* 7.2 (Apr. 2018), pp. 242–245. ISSN: 2162-2337.

[5] H. Akhlaghpasand et al. "Jamming Detection in Massive MIMO Systems". In: *IEEE Wireless Communications Letters* 7.2 (2018), pp. 242–245.

[6] I. F. Akyildiz, A. Kak, and S. Nie. "6G and Beyond: The Future of Wireless Communications Systems". In: *IEEE Access* 8 (2020), pp. 133995–134030.

[7] Y. O. Basciftci, C. E. Koksal, and A. Ashikhmin. "Securing massive MIMO at the physical layer". In: *2015 IEEE Conference on Communications and Network Security (CNS)*. 2015, pp. 272–280.

[8] A. Bereyhi et al. "On Robustness of Massive MIMO Systems Against Passive Eavesdropping under Antenna Selection". In: *Proc. of IEEE Global Commun. Conf. (GLOBECOM)*. Abu Dhabi, UAE, Dec. 2018.

[9] E. Bjornson, J. Hoydis, and L. Sanguinetti. *Massive MIMO Networks: Spectral, Energy, and Hardware Efficiency*. Vol. 11. 3-4. Foundations and Trends in Signal Processing, 2017.

[10] E. Björnson, J. Hoydis, and L. Sanguinetti. "Pilot contamination is not a fundamental asymptotic limitation in massive MIMO". In: May 2017, pp. 1–6.

[11] E. Björnson, E. G. Larsson, and T. L. Marzetta. "Massive MIMO: ten myths and one critical question". In: *IEEE Communications Magazine* 54.2 (2016), pp. 114–123.

[12] E. Björnson et al. *Massive MIMO is a Reality - What is Next? Five Promising Research Directions for Antenna Arrays*. Feb. 2019.

[13] M. Bloch et al. "Wireless Information-Theoretic Security". In: *IEEE Transactions on Information Theory* 54.6 (2008), pp. 2515–2534.

[14] J. Chen et al. "Resource Allocation for a Massive MIMO Relay Aided Secure Communication". In: *IEEE Transactions on Information Forensics and Security* 11.8 (2016), pp. 1700–1711.

[15] S Chen et al. "Wireless powered IoE for 6G: Massive access meets scalable cell-free massive MIMO". In: *China Communications* 17.12 (2020), pp. 92–109.

[16] X. Chen et al. "A Survey on Multiple-Antenna Techniques for Physical Layer Security". In: *IEEE Commun. Surveys Tutorials* 19.2 (2017), pp. 1027–1053.

[17] X. Chen et al. "Large-Scale MIMO Relaying Techniques for Physical Layer Security: AF or DF?" In: *IEEE Transactions on Wireless Communications* 14.9 (2015), pp. 5135–5146.

[18] X. Chen et al. "On Secrecy Performance of Multiantenna-Jammer-Aided Secure Communications With Imperfect CSI". In: *IEEE Transactions on Vehicular Technology* 65.10 (2016), pp. 8014–8024.

[19] Z. Chen and C. Yang. "Pilot Decontamination in Wideband Massive MIMO Systems by Exploiting Channel Sparsity". In: *IEEE Transactions on Wireless Communications* 15.7 (2016), pp. 5087–5100.

[20] I. Csiszar and J. Korner. "Broadcast channels with confidential messages". In: *IEEE Transactions on Information Theory* 24.3 (1978), pp. 339–348.

[21] H. Dang-The et al. "Impact of hardware impairments on secrecy performance of multi-hop relay networks in presence of multiple eavesdroppers". In: *Information and Computer Science (NICS)* (2016), pp. 113–118.

[22] P. de Figueiredo and Fe. Augusto. "An Overview of Massive MIMO for 5G and 6G". In: *IEEE Latin America Transactions* 20.6 (2022), pp. 931–940.

[23] W. Diffie and M. Hellman. "New directions in cryptography". In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654.

[24] F. F. Digham, M.-S. Alouini, and M. K. Simon. "On the Energy Detection of Unknown Signals Over Fading Channels". In: *IEEE Transactions on Communications* 55.1 (2007), pp. 21–24.

[25] T. T. Do et al. "Massive MIMO Pilot Retransmission Strategies for Robustification Against Jamming". In: *IEEE Wireless Communications Letters* 6.1 (2017), pp. 58–61.

[26] Ericsson Mobility. *Ericsson Mobility Report November 2022*. Ericsson Mobility Report v.15.0.0. 5G, 2022.

[27] A. Forenza, D. J. Love, and R. W. Heath Jr. "Simplified Spatial Correlation Models for Clustered MIMO Channels With Different Array Configurations". In: *IEEE Trans. Veh. Tech.* 56.4 (July 2007), pp. 1924–1934. ISSN: 0018-9545.

[28] R. S. Ganesan et al. "Integrating 3D Channel Model and Grid of Beams for 5G MIMO System Level Simulations". In: *Proc. of IEEE Veh. Tech. Conf.* IEEE. 2016, pp. 1–6.

[29] R. S. Ganesan et al. "Integrating 3D Channel Model and Grid of Beams for 5G mMIMO System Level Simulations". In: *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*. 2016, pp. 1–6.

[30] B. Gopalakrishnan and N. Jindal. "An analysis of pilot contamination on multi-user MIMO cellular systems with many antennas". In: *2011 IEEE 12th International Workshop on Signal Processing Advances in Wireless Communications*. 2011, pp. 381–385.

[31] K. Guo, Y. Guo, and G. Ascheid. "Security-Constrained Power Allocation in MU-Massive-MIMO With Distributed Antennas". In: *IEEE Transactions on Wireless Communications* 15.12 (2016), pp. 8139–8153.

[32] B. D. Ha et al. "Secure cognitive reactive decode-and-forward relay networks: With and without eavesdropper". In: *Wirel. Pers. Commun.* (2015).

[33] M. E. Hellman. "An overview of public key cryptography". In: *Communications Magazine, IEEE* 40 (June 2002), pp. 42–49.

[34] A. O. Hero. "Secure space-time communication". In: *IEEE Transactions on Information Theory* 49.12 (2003), pp. 3235–3249.

[35] J. Hoydis, S. ten Brink, and M. Debbah. "Massive MIMO in the UL/DL of Cellular Networks: How Many Antennas Do We Need?" In: *IEEE Journal on Selected Areas in Communications* 31.2 (2013), pp. 160–171.

[36] J. Hoydis et al. "Channel measurements for large antenna arrays". In: *2012 International Symposium on Wireless Communication Systems (ISWCS)*. 2012, pp. 811–815.

[37] D. Hu et al. "Secure Transmission in Multi-cell Multi-user Massive MIMO Systems with an Active Eavesdropper". In: *IEEE Wireless Commun. Lett.* (July 2018). ISSN: 2162-2337.

[38] Y. Hu, Y. Hong, and J. Evans. "Angle-of-Arrival-Dependent Interference Modeling in Rician Massive MIMO". In: *IEEE Trans. Veh. Tech.* 66.7 (July 2017), pp. 6171–6183. ISSN: 0018-9545.

[39] S. Jin, D. Yue, and H. H. Nguyen. "Spectral and Energy Efficiency in Cell-Free Massive MIMO Systems Over Correlated Rician Fading". In: *IEEE Systems Journal* (2020), pp. 1–12.

[40] J. Jose et al. “Pilot Contamination and Precoding in Multi-Cell TDD Systems”. In: *IEEE Trans. Wireless Commun.* 10.8 (Aug. 2011), pp. 2640–2651. ISSN: 1536-1276.

[41] J. Jose et al. “Pilot contamination and precoding in multi-cell TDD systems”. In: *IEEE Trans on Wireless Commun.* 10.8 (2011), pp. 2640–2651.

[42] D. Kapetanovic, G. Zheng, and F. Rusek. “Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks”. In: *IEEE Commun. Mag.* 53.6 (2015), pp. 21–27.

[43] D. Kapetanović et al. “Detection of pilot contamination attack using random training and massive MIMO”. In: *Proc. of IEEE Int. Symp. Personal, Indoor, Mobile Radio Commun. (PIMRC)*. Nov. 2013, pp. 13–18.

[44] M. Karlsson, E. Björnson, and E. G. Larsson. “Jamming a TDD Point-to-Point Link Using Reciprocity-Based MIMO”. In: *IEEE Transactions on Information Forensics and Security* 12.12 (2017), pp. 2957–2970.

[45] S. V. Kartalopoulos. “A primer on cryptography in communications”. In: *IEEE Communications Magazine* 44.4 (2006), pp. 146–151.

[46] D. Klinc et al. “LDPC for Physical Layer Security”. In: Jan. 2010, pp. 1–6.

[47] E. G. Larsson et al. “Massive MIMO for next generation wireless systems”. In: *IEEE Commun. Magazine* 52.2 (2014), pp. 186–195.

[48] E. G. Larsson et al. “Massive MIMO for Next GenerationWireless Systems”. In: *IEEE Communications Magazine* (2014), pp. 186–195.

[49] G. Li et al. “Sum Secret Key Rate Maximization for TDD Multi-User Massive MIMO Wireless Networks”. In: *IEEE Transactions on Information Forensics and Security* 16 (2021), pp. 968–982.

[50] S.-Y. Lien et al. “5G New Radio: Waveform, Frame Structure, Multiple Access, and Initial Access”. In: *IEEE Communications Magazine* 55.6 (2017), pp. 64–71.

[51] Y. Long et al. “Non-asymptotic analysis of secrecy capacity in massive MIMO system”. In: *Proc. of IEEE Int. Conf. Commun. (ICC)*. June 2015, pp. 4587–4592.

[52] T. L. Marzetta. “Massive MIMO: An introduction”. In: *Bell Labs Technical Journal* 20 (2015), pp. 11–22.

[53] T. L. Marzetta. “Noncooperative cellular wireless with unlimited numbers of base station antennas”. In: *IEEE Trans. on Wireless Commun.* 9.11 (2010), pp. 3590–3600.

[54] T.L. Marzetta et al. *Fundamentals of Massive MIMO*. United Kingdom: Cambridge University Press, 2016.

[55] M. Matthaiou et al. “The Road to 6G: Ten Physical Layer Challenges for Communications Engineers”. In: *IEEE Communications Magazine* 59.1 (2021), pp. 64–69.

[56] U. M. Maurer. “Secret key agreement by public discussion from common information”. In: *IEEE Transactions on Information Theory* 39.3 (1993), pp. 733–742.

[57] A. Mukherjee and A. L. Swindlehurst. “A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures”. In: *Proc. IEEE Asilomar Conf. on Signals, Systems and Computers*. Pacific Grove, U.S.A., Nov. 2011, pp. 265–269.

[58] A. Mukherjee and A. L. Swindlehurst. “Detecting passive eavesdroppers in the MIMO wiretap channel”. In: *2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 2012, pp. 2809–2812.

[59] A. Mukherjee et al. “Principles of physical layer security in multiuser wireless networks: A survey”. In: *IEEE Commun. Surveys & Tutorials* 16.3 (2014), pp. 1550–1573.

[60] R. R. Müller, L. Cottatellucci, and M. Vehkaperä. “Blind Pilot Decontamination”. In: *IEEE Journal of Selected Topics in Signal Processing* 8.5 (2014), pp. 773–786.

[61] A. Al-nahari. "Physical layer security using massive multiple-input and multiple-output: Passive and active eavesdroppers". In: *IET Communications* 10 (Jan. 2015).

[62] J. Nam et al. "Joint spatial division and multiplexing: Realizing massive MIMO gains with limited channel state information". In: *2012 46th Annual Conference on Information Sciences and Systems (CISS)*. 2012, pp. 1–6.

[63] H. Q. Ngo and E. G. Larsson. "EVD-based channel estimation in multicell multiuser MIMO systems with very large antenna arrays". In: *2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 2012, pp. 3249–3252.

[64] H. Q. Ngo and E. G. Larsson. "No Downlink Pilots Are Needed in TDD Massive MIMO". In: *IEEE Transactions on Wireless Communications* 16.5 (2017), pp. 2921–2935.

[65] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta. "Energy and Spectral Efficiency of Very Large Multiuser MIMO Systems". In: *IEEE Transactions on Communications* 61.4 (2013), pp. 1436–1449.

[66] F. Oggier and B. Hassibi. "The Secrecy Capacity of the MIMO Wiretap Channel". In: *IEEE Transactions on Information Theory* 57.8 (2011), pp. 4961–4972.

[67] O. Ozdogan, E. Bjornson, and E. G. Larsson. "Massive MIMO with Spatially Correlated Rician Fading Channels". In: *IEEE Trans. Commun.* (2018).

[68] Ö. Özdogan, E. Björnson, and E. G. Larsson. "Massive MIMO With Spatially Correlated Rician Fading Channels". In: *IEEE Transactions on Communications* 67.5 (2019), pp. 3234–3250.

[69] S. Parkvall et al. "NR: The New 5G Radio Access Technology". In: *IEEE Communications Standards Magazine* 1.4 (2017), pp. 24–30.

[70] T. Peng et al. "LSTM-Based Channel Prediction for Secure Massive MIMO Communications Under Imperfect CSI". In: *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*. 2020, pp. 1–6.

[71] N. D. T. Pham et al. "Security-reliability analysis for underlay cognitive radio networks with relay selection methods under impact of hardware noises". In: *Advanced Technologies for Communications (ATC)* (2016), pp. 174–179.

[72] T. S. Rappaport, S. Sun, and M. Shafi. "Investigation and comparison of 3GPP and NYUSIM channel model for 5G wireless communications". In: *Proc. of IEEE Veh. Tech. Conf. (VTC)*. Toronto, Canada, Sept. 2017.

[73] D. B. Rawat, K. Neupane, and M. Song. "A novel algorithm for secrecy rate analysis in massive MIMO system with target SINR requirements". In: *Proc. of IEEE Int. Conf. Computer Commun. (INFOCOM)*. Apr. 2016, pp. 53–58.

[74] F. Rusek et al. "Scaling Up MIMO: Opportunities and Challenges with Very Large Arrays". In: *IEEE Signal Processing Magazine* 30.1 (2013), pp. 40–60.

[75] L. Sanguinetti, E. Björnson, and J. Hoydis. "Toward Massive MIMO 2.0: Understanding Spatial Correlation, Interference Suppression, and Pilot Contamination". In: *IEEE Transactions on Communications* 68.1 (2020), pp. 232–257.

[76] L. Sanguinetti, A. Kammoun, and M. Debbah. "Theoretical Performance Limits of Massive MIMO with Uncorrelated Rician Fading Channels". In: *IEEE Trans. Commun.* (2018).

[77] C. E. Shannon. "Communication theory of secrecy systems". In: *The Bell System Technical Journal* 28.4 (1949), pp. 656–715.

[78] S. Sun et al. "Investigation of prediction accuracy, sensitivity, and parameter stability of large-scale propagation path loss models for 5G wireless communications". In: *IEEE Trans. Veh. Tech.* 65.5 (May 2016), pp. 2843–2860.

[79] S. Suyama et al. "Recent Studies on Massive MIMO Technologies for 5G Evolution and 6G". In: *2022 IEEE Radio and Wireless Symposium (RWS)*. 2022, pp. 90–93.

[80] S. Suyama et al. "Recent Studies on Massive MIMO Technologies for 5G Evolution and 6G". In: *2022 IEEE Radio and Wireless Symposium (RWS)*. 2022, pp. 90–93.

[81] C. V. Trinh, E. Björnson, and E. G. Larsson. "Joint pilot design and uplink power allocation in multi-cell massive MIMO systems". In: *IEEE Transactions on Wireless Communications* 17.3 (2018), pp. 2000–2015.

[82] C. V. Trinh et al. "Reconfigurable Intelligent Surface-Assisted Massive MIMO: Favorable propagation, channel hardening, and rank deficiency [Lecture Notes]". In: *IEEE Signal Processing Magazine* 39.3 (2022), pp. 97–104.

[83] VC. V. Trinh et al. "Uplink power control in massive MIMO with double scattering channels". In: *IEEE Transactions on Wireless Communications* 21.3 (2021), pp. 1989–2005.

[84] V. V. Veeravalli, Y. Liang, and A. M. Sayeed. "Correlated MIMO wireless channels: capacity, optimal signaling, and asymptotics". In: *IEEE Transactions on Information Theory* 51.6 (June 2005), pp. 2058–2072. ISSN: 1557-9654.

[85] G. Q. L. Vu and K. T. Truong. "Secret Capacity of Massive MIMO with a Passive Eavesdropper". In: *Journal of Research and Development on Information and Communication Technology* V-3.40 (Dec. 2018), p. 1.

[86] J. Wang et al. "Jamming-Aided Secure Communication in Massive MIMO Rician Channels". In: *IEEE Trans. Wireless Commun.* 14.12 (Dec. 2015), pp. 6854–6868. ISSN: 1536-1276.

[87] J. Wang et al. "Jamming-Aided Secure Communication in Massive MIMO Rician Channels". In: *IEEE Transactions on Wireless Communications* 14.12 (2015), pp. 6854–6868.

[88] Y. Wu et al. "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead". In: *IEEE J. Se. Areas Commun.* (2018).

[89] Y. Wu et al. "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead". In: *IEEE Journal on Selected Areas in Communications* 36.4 (2018), pp. 679–695.

[90] Y. Wu et al. "Secure Massive MIMO Transmission With an Active Eavesdropper". In: *IEEE Trans. Info. Theory* 62.7 (July 2016), pp. 3880–3900. ISSN: 0018-9448.

[91] Y. Wu et al. "Secure Transmission With Large Numbers of Antennas and Finite Alphabet Inputs". In: *IEEE Transactions on Communications* 65.8 (2017), pp. 3614–3628.

[92] A. D. Wyner. "The wire-tap channel". In: *The Bell System Technical Journal* 54.8 (1975), pp. 1355–1387.

[93] T. Yang et al. "Secure Massive MIMO Under Imperfect CSI: Performance Analysis and Channel Prediction". In: *IEEE Trans. Info. Forensics Security* (2018). ISSN: 1556-6013.

[94] C.-Y. Yeh and E. W. Knightly. "Feasibility of Passive Eavesdropping in Massive MIMO: An Experimental Approach". In: *Proc. of IEEE Conf. Commun. Network Security (CNS)*. Beijing, China, May 2018.

[95] C.-Y. Yeh and E. W. Knightly. "Feasibility of Passive Eavesdropping in Massive MIMO: An Experimental Approach". In: *2018 IEEE Conference on Communications and Network Security (CNS)*. 2018, pp. 1–9.

[96] A. Yener and S. Ulukus. "Wireless Physical-Layer Security: Lessons Learned From Information Theory". In: *Proc. the IEEE* 103.10 (Oct. 2015), pp. 1814–1825.

[97] A. Yener and S. Ulukus. "Wireless Physical-Layer Security: Lessons Learned From Information Theory". In: *Proceedings of the IEEE* 103.10 (2015), pp. 1814–1825.

[98] J. Zhang et al. "NOMA-Based Cell-Free Massive MIMO Over Spatially Correlated Rician Fading Channels". In: *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*. 2020, pp. 1–6.

[99] X. Zhang, D. Guo, and K. Guo. "Secure Performance Analysis for Multi-Pair AF Relaying Massive MIMO Systems in Ricean Channels". In: *IEEE Access* 6 (2018), pp. 57708–57720.

[100] X. Zhang, D. Guo, and K. Guo. "Secure Performance Analysis for Multi-Pair AF Relaying Massive MIMO Systems in Ricean Channels". In: *IEEE Access* 6 (2018), pp. 57708–57720.

[101] F. Zhou et al. “Artificial Noise Aided Secure Cognitive Beamforming for Cooperative MISO-NOMA Using SWIPT”. In: *IEEE Journal on Selected Areas in Communications* 36.4 (2018), pp. 918–931.

[102] X. Zhou, B. Maham, and A. Hjorungnes. “Pilot Contamination for Active Eavesdropping”. In: *IEEE Trans. Wireless Commun.* 11.3 (Mar. 2012), pp. 903–907. ISSN: 1536-1276.

[103] X. Zhou, B. Maham, and A. Hjorungnes. “Pilot Contamination for Active Eavesdropping”. In: *IEEE Transactions on Wireless Communications* 11.3 (2012), pp. 903–907.

[104] J. Zhu, R. Schober, and V. K. Bhargava. “Linear precoding of data and artificial noise in secure massive MIMO systems”. In: *IEEE Tran. Wireless Commun.* 15.3 (2016), pp. 2245–2261.

[105] J. Zhu, R. Schober, and V. K. Bhargava. “Secure transmission in multicell massive MIMO systems”. In: *IEEE Trans. Wireless Commun.* 13.9 (2014), pp. 4766–4781.

[106] J. Zhu et al. “Analysis and Design of Secure Massive MIMO Systems in the Presence of Hardware Impairments”. In: *IEEE Transactions on Wireless Communications* 16.3 (2017), pp. 2001–2016.

[107] J. Zhu et al. “Analysis and Design of Secure Massive MIMO Systems in the Presence of Hardware Impairments”. In: *IEEE Transactions on Wireless Communications* 16.3 (2017), pp. 2001–2016.

[108] Y. Zou et al. “A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends”. In: *Proc. of the IEEE* 104.9 (Sept. 2016), pp. 1727–1765.