|  |
| --- |
| **ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH**  **TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN**  ***KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG***  Logo  Description automatically generatedA picture containing text, vector graphics, clipart  Description automatically generated |
| ***MÔN HỌC: AN TOÀN MẠNG KHÔNG DÂY VÀ DI ĐỘNG***  **BÁO CÁO ĐỒ ÁN MÔN HỌC**  **ĐỀ TÀI: BẢO MẬT CHỐNG NGHE LÉN TẦNG VẬT LÝ** |
| **Giảng viên hướng dẫn:**  LÊ KIM HÙNG |
| **Sinh viên thực hiện:**  Võ Thị Thu Cúc - 19521296                            Võ Đức Khải - 19520617  Trần Nguyễn Đăng Khoa - 18520939                            Hoàng Văn Anh Đức - 20520890  ***TP. Hồ Chí Minh, tháng 06 năm 2022*** |
| MỤC LỤC  [**PHẦN 1: BẢO MẬT TẦNG VẬT LÝ KHÔNG DÂY NHẰM CHỐNG NGHE LÉN** 4](#_gjdgxs)  [**PHẦN 2: NỘI DUNG** 7](#_30j0zll)  [**A.**](#_1fob9te) **BẢO MẬT THEO TÍNH LÝ THUYẾT THÔNG TIN (INFORMATION-THEORETIC SECURITY) -** 20520890 7  [**B. BẢO MẬT HỖ TRỢ TIẾNG ỒN NHÂN TẠO.**](#_3znysh7) **-** 19521296 [16](#_3znysh7)  [**C. SECURITY-ORIENTED BEAMFORMING TECHNIQUES**](#_2et92p0) **-**18520939 [18](#_2et92p0)  [**D. ĐA DẠNG HÓA PHƯƠNG PHÁP BẢO MẬT**](#_tyjcwt) **-** 19520617  [21](#_tyjcwt)  [**PHẦN 3: KẾT LUẬN** 21](#_1t3h5sf) |

BÁO CÁO CHI TIẾT

# **PHẦN 1: BẢO MẬT TẦNG VẬT LÝ KHÔNG DÂY NHẰM CHỐNG NGHE LÉN**

* ***Mục đích***

-Trong phần này nói về chuyên ngành bảo mật tầng vật lý không dây. Chuyên ngành này đã được khám phá và nghiên cứu để giúp cho việc bảo vệ những giao tiếp không dây khỏi việc bị nghe lén

* ***Đường truyền trong mạng***

- Đường truyền không dây phát tín hiệu từ một nguồn tới điểm đích có thể có sự xuất hiện của bên nghe lén

* ***Tín hiệu***

- Khi tín hiệu radio được truyền từ nguồn, nhiều tín hiệu sẽ bị làm chậm và được chuyển tới đích đến thông qua phản xạ, tán xạ và nhiễu xạ sóng

* ***Hiệu ứng phân luồng***

- Do hiệu ứng phân luồng, những tín hiệu bị làm chậm có thể “constructively” hoặc “destructively”

\*\*

+ Constructive interference: 2 sóng kết hợp (chồng chéo) lên nhau thì sẽ tạo ra 1 sóng lớn hơn gọi là “constructive interference”

Overlapsed in the same place-“perfectly constructive” – “totally constructive”

+Destructive interference 2 sóng vs biên độ và tần số trái ngược nhau sẽ triệt tiêu lẫn nhau => Destructive interference

A picture containing icon

Description automatically generated

* ***Liên lạc vô tuyến***

+Trong thông tin liên lạc vô tuyến, đa luồng là hiện tượng lan truyền xảy ra trên tín hiệu vô tuyến đến anten thu bằng hai hoặc nhiều đường dẫn.

Nguyên nhân của đa đường bao gồm ống dẫn khí quyển, phản xạ tầng điện ly và khúc xạ, cũng như phản xạ từ các vùng nước và các vật thể trên cạn như núi và các tòa nhà.

Khi cùng một tín hiệu được nhận trên nhiều đường, nó có thể tạo ra nhiễu và lệch pha của tín hiệu. Sự can thiệp này gây ra sự mờ dần ( causes fading ); điều này có thể khiến tín hiệu vô tuyến trở nên quá yếu trong một số khu vực nhất định. Vì lý do này, hiệu ứng này còn được gọi là nhiễu đa đường hoặc méo đa đường.

<https://www.khanacademy.org/science/physics/light-waves/interference-of-light-waves/v/constructive-and-destructive-interference>

\*\*

* ***Sự giảm sút***

- Vì thế, sự giảm sút của tín hiệu trong không gian thay đổi theo thời gian, còn được gọi là sự phai đi và thường được xem là một tiến trình ngẫu nhiên

- Tín hiệu được nhận có thể bị giảm một cách đáng kể, đặc biệt là khi gặp phải chướng ngại vật (vd: cây cối,..) xuất hiện ở giữa nguồn và đích

- Do cách mà sóng radio được truyền đi, nguồn sóng có thể bị nghe lén , điều này có thể gây ra sự giảm sút của nhiều tín hiệu

* ***Cách xác định sự giảm sút***

- Có 3 dạng phân phối xác suất được dùng để xác định sự phai đi ngẫu nhiên của mạng không dây, bao gồm

Rayleigh [115], Rice [116] và Nakagami [117].

***Rayleigh Fading :*** <https://www.researchgate.net/publication/3195748_Rayleigh_fading_channels_in_mobile_digital_communication_systems_Part_I_Characterization>

\*\*

Mô hình mờ dần Rayleigh giả định rằng cường độ của tín hiệu đã đi qua một phương tiện truyền dẫn (còn được gọi là kênh giao tiếp) sẽ thay đổi ngẫu nhiên, hoặc mờ dần, theo phân phối Rayleig. Sự mờ dần của Rayleigh được xem là một mô hình hợp lý cho sự lan truyền tín hiệu tầng đối lưu và tầng điện ly cũng như ảnh hưởng của môi trường đô thị được xây dựng dày đặc đối với tín hiệu vô tuyến. Rayleigh Fading được áp dụng nhiều nhất khi không có sự lan truyền chi phối dọc theo đường ngắm giữa máy phát và máy thu. Nếu có một đường xác định (line of sight - hướng phải nhìn để có thể nhìn thấy một đối tượng cụ thể), Rician Fading có thể được áp dụng nhiều hơn

Trong đường truyền vô tuyến, tín hiệu RF  
từ máy phát có thể bị phản xạ từ các vật cản  
như đồi, nhà cửa, xe cộ…sinh ra nhiều đường  
tín hiệu đến máy thu (hiệu ứng đa đường) dẫn  
đến lệch pha giữa các tín hiệu đến máy thu  
làm cho biên độ tín hiệu thu bị suy giảm.

\*\*

***Rician Fading :***

<https://en.wikipedia.org/wiki/Rician_fading>

\*\*

Ricean fade là một mô hình cho sự bất thường trong quá trình truyền sóng vô tuyến gây ra bởi sự hủy một phần tín hiệu vô tuyến - tín hiệu đến máy thu bằng một số con đường khác nhau (do đó thể hiện nhiễu đa đường-multipath fading effect) và ít nhất một trong các đường dẫn đang thay đổi (kéo dài hoặc rút ngắn). Sự mờ dần ảo thuật xảy ra khi một trong các đường dẫn, thường là tín hiệu đường ngắm (line of sight) hoặc một số tín hiệu phản xạ mạnh, mạnh hơn nhiều so với các đường khác.

\*\*

Slide

***Hiện trạng***

***mô hình có triển vọng ?***

-Gần đây, bảo mật tầng vật lý đã được xem như một mô hình có triển vọng được thiết kể để tăng cường bảo mật của truyền dẫn không dây bằng cách sử dụng những đặc tính của các kênh truyền không dây

***The wire-tap channel***

-“The wire-tap channel”- Qua các tài liệu nghiên cứu , đã cho thấy sự bảo mật thông tin đáng tin cậy trên lý thuyết “reliable information-theoretic security” là khi mà kênh truyền tới bên nghe lén là một phiên bản kém hơn của kênh truyền chính từ nguồn đến đích

***The Gaussian wiretap channel***

-Trong “ The Gaussian wiretap channel” ,một thứ gọi là “Khả năng bảo mật”-secrecy capacity đã được phát triển và cho thấy sự khác biệt giữa băng thông (capacity) của kênh truyền chính và kênh truyền bị xâm nhập , khi mà “Khả năng bảo mật” này có tác dụng thì coi như sự bảo mật đáng tin cậy theo tính lý thuyết là có thể thực hiện được và ngược lại

\*\*\*\*\*\*\*\*\*\*\*\*

- Khả năng bảo mật, được định nghĩa là tốc độ thông tin tối đa mà nguồn có thể truyền đến người nhận mà người nghe trộm không thể thu được bất kỳ thông tin nào, là số liệu chính để đánh giá mức độ bảo mật của hệ thống FSO dựa trên bảo mật tầng vật lý.

(capacity) : the amount of data , a channel can transmit.

\*\*\*\*\*\*\*\*\*\*\*\*

slide

***Kết nối có dây thì sao ?***

Tuy nhiên, trong khi kết nối có dây thì (tín hiệu) thường không thay đổi theo thời gian, kết nối không dây thì lại bị ảnh hưởng bởi sự giảm sút tín hiệu ngẫu nhiên theo thời gian, dẫn đến sự giảm sút về chất lượng của “khả năng bảo mật” không dây, đặc biệt là khi kênh truyền chính gặp phải chướng ngại vật (vd: cây cối, nhà cửa,...) giữa nguồn và đích.

Vì thế, đã có nhiều dự án nghiên cứu về phương pháp bảo mật tầng vật lý, có thể được chia làm các loại chính như sau:

1. Bảo mật theo tính lý thuyết thông tin [119] – [125]
2. Bảo mật có trợ giúp tiếng ồn nhân tạo [126] – [130]
3. Phương pháp điều sóng theo hướng bảo mật [131] – [136]
4. Đa dạng hóa phương pháp bảo mật [42], [137]
5. Tạo khóa bí mật trong tầng vật lý [147] – [161]

Slide 1949

Đưa ra các khái niệm về bảo mật lý thuyết và bí mật thực tế để bảo vệ chống lại kẻ nghe trộm với sức mạnh tính toán vô hạn hoặc hữu hạn

**PHẦN 2: NỘI DUNG**

1. **BẢO MẬT THEO TÍNH LÝ THUYẾT THÔNG TIN (INFORMATION-THEORETIC SECURITY)**

***Phân tích***

**-**Bảo mật theo tính lý thuyết thông tin phân tích những giới hạn của những phương pháp bảo mật tầng vật lý về góc độ lý thuyết thông tin

***Shannon***

-Khái niệm của bảo mật theo tính lý thuyết thông tin được phát triển bởi Shannon[119]

***Hệ thống bí mật***

**-**Shannon đã định nghĩa một hệ thống bí mật ( secrecy system ) như một nhóm những sự chuyển đổi toán học của một không gian (tập hợp các thông điệp bản rõ) tới một không gian khác (tập hợp các mật mã có thể có) , nơi mà mỗi sự chuyển đổi tương ứng với việc mã hóa thông tin với sự hỗ trợ của khóa bí mật

**( có nghĩa là “secrecy system” bao gồm những loại mã hóa và giải mã khác nhau để che giấu thông tin khỏi attacker )**

**-**Hơn nữa, mỗi chuyển đổi là không suy biến (ko thay đổi nội dung), vì thế sự giải mã độc nhất là hoàn toàn có thể với điều kiện là khóa bí mật đã biết

**\*\***

***secrecy system includes*** :

1. Concealment systems : những phương pháp như như mực vô hình, che giấu một thông điệp trong một văn bản , hoặc trong một mật mã giả mạo che đậy hoặc các phương pháp khác mà sự tồn tại của thông báo là giấu giếm kẻ thù;
2. Privacy systems : ví dụ, đảo ngược giọng nói, trong đó thiết bị đặc biệt được yêu cầu để khôi phục thông điệp;
3. hệ thống bí mật "thực sự" nơi ý nghĩa của thông điệp được che giấu bởi mật mã, mật mã, v.v., mặc dù sự tồn tại của nó không bị che giấu, và giả định là kẻ thù có bất kỳ thiết bị đặc biệt nào cần thiết để đánh chặn và ghi lại tín hiệu được truyền đi.

Conclusion :Chúng tôi chỉ coi kiểu che giấu thứ ba chủ yếu là mối quan tâm chính , và là hệ thống quyền riêng tư một công nghệ nào đó

**\*\***

**\*\***

**Không suy biến : Một phép biến đổi tuyến tính có một nghịch đảo; nó có một nhân không gian rỗng ( it has a null space kernel ) chỉ bao gồm vectơ không**

**Kernel Space: Mã thực thi có quyền truy cập không hạn chế vào bất kỳ không gian địa chỉ nào của memory và tới bất kỳ phần cứng nào**

**Hạt nhân của một ánh xạ tuyến tính là không gian vectơ con của nguồn được ánh xạ tới vectơ không**

**\*\***

**slide**

***Communications theory of secrecy systems :***

***Lý thuyết truyền thông về hệ thống bí mật***

**-** Trong Communications theory of secrecy systems [119], ý tưởng về bảo mật theo lý thuyết và bảo mật thiết thực đã được giới thiệu và phát triển nhằm giúp cho việc chống lại những cuộc tấn công nghe lén, trong trường hợp bên tấn công có năng lực máy tính vô hạn hoặc có hạn

**-** [119] ” Communications theory of secrecy systems” đã cho thấy một hệ thống bảo mật hoàn hảo có thể được tạo ra, mặc dù sử dụng một chìa khóa bí mật có hạn, khi attacker có hiểu đc 1 phần nghĩa thì cũng không thể tìm ra được giải pháp độc nhất để giải mã (giải pháp không dùng private key)- sự không rõ nghĩa (equivocation) không tiệm cận 0

**-** Để giải thích thêm, sự không rõ nghĩa – (equivocation) được định nghĩa như là một đơn vị để tính sự không chắc chắn của attacker đối vối bản mã sau khi đánh chặn tin nhắn [119].

- Hệ thống bí mật ( secrecy system ) được phát triển bởi Shannon trong [119] dựa vào sự sử dụng của khóa bí mật. Tuy nhiên, việc ***quản lý khóa*** rất khó khăn ( chia sẻ khóa ) trong những mạng lưới không dây hoạt động mà không có một cơ sở hạ tầng cố định (vd: mạng không dây chỉ sử dụng khi cần thiết- wireless ad hoc networks) [32].

\*\*

Vd đối với “wireless ad hoc networks”

Có hệ thống cơ sở loại trừ (EBS) cung cấp một framework (khuôn khổ) để có thể mở rộng và quản lý nhóm khóa hiệu quả, trong đó số lượng khóa trên mỗi node và số lượng các thông điệp khóa lại (re-key message) có thể được điều chỉnh tương đối .

Tuy nhiên, các giải pháp dựa trên EBS có thể bị tấn công thông đồng (collusion attacks), trong đó một số bên có thể hợp tác để tiết lộ tất cả các khóa hệ thống và do đó chiếm được mạng

collusion attacks : chẳng hạn như thông đồng giữa một số bên để tiết lộ các nguyên tắc cơ bản của kế hoạch bảo mật được sử dụng

\*\*

***=> The wire-tap channel***

1975

-Vì thế, trong The wire-tap channel [33], Wyner đã nghiên cứu bảo mật có tính lý thuyết thông tin mà không cần sử dụng khóa bí mật và phân tích những giới hạn hoạt động của nó cho một kênh nghe lén không có bộ nhớ rời rạc (discrete memoryless wiretap channel) bao gồm một nguồn, một đích và một bên nghe lén

- **Nó đã đc chỉ ra trong [33] rằng một kênh truyền tin hoàn toàn an toàn là có thể thực hiện được, nếu như băng thông của kênh truyền chính dẫn từ nguồn tới đích cao hơn băng thông của kênh truyền dẫn từ nguồn tới bên nghe lén.**

\*\*

Channel capacity : là giới hạn chặt chẽ về tốc độ mà thông tin có thể được truyền qua một kênh truyền thông một cách đáng tin cậy.

\*\*

Nói cách khác, khi điều kiện của kênh truyền chính cao hơn điều kiện của kênh truyền bị xâm nhập, có khả năng nguồn và đích có thể trao đổi thông tin một cách an toàn

Leung et al 1978

- Trong [34], kết quả của Wyner được áp dụng xa hơn là tới kênh nghe lén Gaussian (Gaussian wiretap channel), nơi mà khái niệm của ‘năng lực bảo mật’-“secrecy capacity” được phát triển, cái này có thể phân biệt băng thông của kênh truyền chính với kênh truyền nghe lén

(34 k có tài liệu)

* **Nếu tần suất bảo mật ( secrecy rate ) được chọn thấp hơn khả năng bảo mật ( secrecy capacity ), sự truyền tin đảm bảo từ nguồn tới đích sẽ có thể đạt tới độ bí mật tuyệt đối**

**\*\***

**Khả năng bảo mật (secrecy capacity ) được định nghĩa là tốc độ mà một node truyền thông tin bí mật cho node khác.Hay tốc độ tối đa truyền giữa các node và bên nghe lén không thể “nghe” đc bất kì thông tin gì**

**Secrecy rate : một cuộc giằng co giữa kênh chính và kênh nghe lén. Nếu kênh chính có dung lượng lớn hơn thì Secrecy rate là dương, ngược lại là âm.**

**\*\***

-Trong mạng không dây, khả năng bảo mật ( secrecy capacity ) bị giảm chất lượng do hiệu ứng phai đi (fading effects) theo thời gian. Đây là bởi vì sự phai đi (fading) làm suy giảm tín hiệu được nhận tới đích , cái mà làm giảm băng thông của những kênh truyền này, từ đó dẫn đến sự giảm sút về chất lượng của “khả năng bảo mật”.

slide

***\*\* GIẢI PHÁP ĐỐI VS HIỆU ỨNG PHAI ĐI (fading process)***

TH1 : nguồn + nghe lén : nhiều ăng ten , đích chỉ có 1

***Nhóm hệ thống MIMO***

- Nhóm hệ thống MIMO được khẳng định rộng rãi là một cách hiệu quả để làm giảm hiệu ứng phai đi, đồng thời tăng cường “khả năng bảo mật” trong những môi trường không hiệu quả (môi trường có nhiều vật cản , …).

***2007***

***On the Gaussian MIMO Wiretap Channel***

Trong “On the Gaussian MIMO Wiretap Channel” [120], Khisti và những người khác đã nghiên một ngữ cảnh gọi là MISOME ( MISO ), khi mà cả bên nguồn và bên nghe lén đều được trang bị nhiều ăng ten, nhưng bên đích chỉ có 1 ăng ten. Coi như hệ số phai đi của mọi bên liên quan là không thay đổi và được biết giữa các bên (vd: nguồn, bên nghe lén, đích, ...), “Khả năng bảo mật” của ngữ cảnh MISOME có thể được phân biệt bằng các giá trị đặc trưng tổng quát của nó .

LÀ :

\*\*

***Noise***

Trong xử lý tín hiệu, nhiễu (noise) là một thuật ngữ chung để chỉ những sửa đổi không mong muốn (và nói chung là không xác định) mà tín hiệu có thể mắc phải trong quá trình thu, lưu trữ, truyền, xử lý hoặc chuyển đổi

***SNR***

SNR-Signal-to-noise ratio: là một thước đo được sử dụng trong khoa học và kỹ thuật để so sánh mức độ của tín hiệu mong muốn với mức độ nhiễu xung quanh

***Ngữ cảnh MISO*** :

+Sự ra đời : Khi kênh nghe lén của Wyner được khái quát cho trường hợp khi người gửi, người nhận và người nghe trộm có nhiều ăng-ten.

Thì ngữ cảnh MISO xem xét hai trường hợp:

Deterministic case và fading case.

Trong trường hợp xác định (deterministic case) , ma trận kênh của người nhận và người nghe trộm được cố định và tất cả đều biết các bên. Trong (fading case ) trường hợp mờ dần, kênh ma trận trải qua block fading và người gửi chỉ có thông tin tình trạng kênh của người nhận dự định (CSI) và thông tin thống kê về kênh của người nghe trộm. Đối với trường hợp xác định, một kế hoạch dựa trên (GSVD)- phân tích giá trị đơn lẻ tổng quát của ma trận kênh được đề xuất và hiển thị để đạt được khả năng bảo mật trong khi (SNR)- “mức độ của tín hiệu mong muốn với mức độ nhiễu xung quanh” cao. Khi người nhận dự kiến ​​chỉ có một ăng-ten (MISO case), khả năng bí mật được như mong đợi cho bất kỳ SNR nào.

/\*

Block fading là khi mà quá trình fading gần như không đổi trong 1 khoảng thời gian. Một kênh có thể bị 'làm mờ khối kép'-double block fading khi nó bị mờ dần theo khối trong cả miền thời gian và tần số

Trong đại số tuyến tính, phân rã giá trị kỳ dị tổng quát (GSVD) là tên của hai kỹ thuật khác nhau dựa trên sự phân rã giá trị kỳ dị. Hai phiên bản khác nhau vì một phiên bản phân tách hai (hoặc nhiều) ma trận và phiên bản kia sử dụng một tập hợp các ràng buộc áp đặt cho các vectơ số ít bên trái và bên phải.

\*/

***Khả năng giữ bí mật***

+Khả năng giữ bí mật bằng không khi và chỉ khi tỷ lệ giữa số ăng-ten của người nghe trộm với ăng ten người gửi ít nhất là hai, (số ăng ten của bên nghe trộm gấp đôi số ăng ten của bên phát)

mức tối ưu chương trình được coi là dựa trên "tiếng ồn nhân tạo" – “ artificial noise"

(min [ăng ten của (nghe lén/ bên phát)]=2)-ăng ten của ng nghe lén gấp đôi của transmitter

\*\*

SLIDE

Tăng cường bảo mật mạng không dây tầng vật lý

Nên nhớ rằng những thông tin về những phản hồi bất ngờ của bên nghe lén thường là không khả dụng,

***masked beamforming scheme***

Khisti và những đồng nghiệp [121] ủng hộ việc sử dụng một kế hoạch gọi là điều sóng ẩn ( masked beamforming scheme “vẫn trong MISOME case”)

- Nhằm tăng cường bảo mật mạng không dây tầng vật lý, khi mà không bị phụ thuộc vào thông tin về bên nghe lén để tìm phương hướng truyền tín hiệu ( tìm ra phương hướng để tránh các bên nghe lén nhưng trong trường hợp này thì k cần làm điều đó). Kế hoạch điều sóng không dây đã được cho thấy là có thể đạt tới mức bảo mật gần tối ưu với SNRs đủ cao. (SNR cao để gây nhiễu bên nghe lén ?)

\*\*

***SNRs***: mức độ của tín hiệu mong muốn với mức độ nhiễu xung quanh

SNR được định nghĩa là tỷ số giữa công suất tín hiệu và công suất nhiễu, thường được biểu thị bằng decibel. Tỷ lệ cao hơn 1: 1 cho thấy nhiều tín hiệu hơn là nhiễu

Masked beamforming scheme : phát ra năng lượng đẳng hướng theo mọi hướng và cho thấy rằng nó đạt được mức gần như tối ưu hiệu suất trong chế độ SNR cao

Nhiễu (noise) là nhiễu loạn không mong muốn trong tín hiệu điện. Tiếng ồn được tạo ra bởi rất nhiều các thiết bị điện tử khác nhau vì nó được tạo ra bởi một số hiệu ứng khác nhau. Trong các hệ thống truyền thông, nhiễu là một lỗi hoặc nhiễu ngẫu nhiên (random noise) không mong muốn của tín hiệu thông tin hữu ích

\*\*

* ***Rayleigh fading enviroment***

Hơn nữa, Khisti và những người khác đã mở rộng kết quả của họ đến những kênh truyền không dây thay đổi theo thời gian và phát triển cả mức trên và dưới (toàn diện) của “khả năng bảo mật-secrecy capacity” trong ngữ cảnh MISOME hoạt động trong môi trường phai đi Rayleigh. (Rayleigh fading enviroment)

***Tóm lại, nghiên cứu của Khisti và đồng nghiệp [121] tập trung chủ yếu vào việc thể hiện đặc tính “khả năng bảo mật” của kế hoạch điều sóng ẩn theo tính lý thuyết thông tin, thứ mà thuộc về chuyên ngành giải pháp bảo mật theo tính lý thuyết thông tin.***

**=>Conclusion [121] : *tăng thông lượng và độ tin cậy của hệ thống giúp bảo mật hơn. Nhiều trong số các hệ thống có một lợi ích phụ là cung cấp bảo mật. “ Nó là mối quan tâm để định lượng những lợi ích và xác định các ngữ cảnh ứng dụng tiềm năng.*** *“*

//////////////////////

slide

***Secure Transmission With Multiple Antennas***

Sau này, Khisti và đồng nghiệp “Secure Transmission With Multiple Antennas” [122] đã nghiên cứu bảo mật theo tính lý thuyết thông tin và đạt được với sự trợ giúp của nhiều ăng ten trong một tình huống , khi mà nguồn, đích và bên nghe lén được coi là có nhiều ăng ten.

\*\*

[122] :

//

Nó thiết lập sự tồn tại của một biểu thức tính toán và cho ra khả năng giữ bí mật của kênh MIMO .

Làm nổi bật vai trò hữu ích mà GSVD (phân tích giá trị đơn lẻ tổng quát) đóng vai trò cả trong việc tính toán công suất của kênh MIMO khi SNR cao và trong việc thiết kế các mã để tiếp cận băng thông này

//

Slide

***wire-tap chanel***

Kênh nghe lén (wire-tap chanel) là một mô hình lý thuyết thông tin để bảo mật lớp vật lý. Trong mô hình, có ba thiết bị đầu cuối — một người gửi, một người nhận và một người nghe trộm. Mục đích là khai thác cấu trúc của kênh quảng bá (broadcast chanel) để truyền thông điệp một cách đáng tin cậy đến máy thu, trong khi rò rỉ gần như không có thông tin nào đến bên nghe trộm.

\*\*

Họ xem xét hai trường hợp:

***Tình trạng kênh***

1. Trường hợp được đơn giản hóa và coi như hoàn hảo khi mà CSIs-Channel state information (tình trạng kênh) của cả hai đường dẫn chính và đường dẫn bị nghe lén là cố định .

***Ngữ cảnh thực tế***

1. Trường hợp thực tế- fading case ( the more practical fading scenario) . Trong đó những kênh truyền không dây bị ảnh hưởng bởi Rayleigh fading theo thời gian và nguồn gồm những kênh chính có CSI (tình trạng kênh) hoàn hảo và thông tin tình trạng kênh của kênh truyền nghe lén.

***khả năng bảo mật***

Trong trường hợp 1(xđ đc ý tưởng), họ sử dụng một phương pháp dựa vào GSVD-(phân tích giá trị đơn lẻ tổng quát) để tăng “khả năng bảo mật” trong khu vực có SNR cao.

Độ hiệu quả của kế hoạch GSVD được nghiên cứu sâu hơn trong ngữ cảnh có sự phai đi (fading scenario) và cho thấy (khả năng bảo mật) đạt 0 khi và chỉ khi ***“tỉ lệ ăng ten của bên nghe lén / ăng ten bên nguồn lớn hơn 2.”***

\*\*

**Secrecy rate : một cuộc giằng co giữa kênh chính và kênh nghe lén. Nếu kênh chính có dung lượng lớn hơn thì Secrecy rate là dương, ngược lại là âm.**

[123]

Slide

2009

***biểu thức dạng đóng***

Hơn nữa, trong [123], Chrysikos và đồng nghiệp nghiên cứu bảo mật không dây theo tính lý thuyết thông tin liên quan tới sự mất mát của “khả năng bảo mật”, thứ mà được dùng để mô tả “secrecy rate” lớn nhất, trong trường hợp sự mất mát là có thể xảy ra.

* Một biểu thức dạng đóng (closed -form) biểu thị sự mất mát của “khả năng bảo mật” được trích trong [123] bằng cách sử dụng một hệ thống chuỗi Taylor bậc 1 cho việc tính toán hàm mũ.

Một biểu thức dạng đóng (closed-form) : là một biểu thức toán học có thể được tính toán với số phép toán hữu hạn. Nó có thể chứa hằng số, biến số, một số phép toán "đã biết", và hàm số, nhưng thường không có giới hạn.

***Sự mất mát***

Sự mất mát ”khả năng bảo mật” có thể được tính toán cho một xác suất ngừng hoạt động nhất định và cho một môi trường lan truyền nhất định mất đi đường dẫn theo cơ số mũ, kênh chính trung bình SNR), cho phép ước tính với độ chính xác cao hơn các ranh giới của an toàn thông tin liên lạc

* Công thức tính

\*\*

SLIDE

***Kênh nghe lén MIMO -*** The MIMO wiretap channel

Kênh nghe lén MIMO có thể được coi là kênh phát MIMO, khi mà nguồn phát sóng những thông tin bí mật tới kênh đích và vô tình tới cả kênh nghe lén. Bảo mật tuyệt đối đạt được khi cả kênh nguồn và đích có thể giao tiếp một cách an toàn, trong khi vẫn giữ được những thông tin chung giữa nguồn và bên nghe lén bằng 0.

2011

***124 : The secrecy capacity of the MIMO wiretap channel***

Trong [124], Oggier và Hassibi phân tích “khả năng bảo mật” của những hệ thống được hỗ trợ bằng ăng ten bằng cách chuyển đổi kênh nghe lén (wire tap chennel) MIMO thành kênh phát sóng MIMO, trong đó số ăng ten của bên phát và nhận là ngẫu nhiên (vd: kênh đích và kênh nghe lén).

\*\*[124]

“Khả năng bảo mật” hoàn hảo của kênh phát sóng MIMO nhiều ăng-ten, trong đó số lượng ăng-ten là bất kì cho cả người gửi và 2 người nhận.

-Wyner cho thấy đối với các kênh không có bộ nhớ rời rạc rằng khả năng bảo mật hoàn hảo thực sự là sự khác biệt về thông tin lẫn nhau tương ứng giữa hai người dùng (2 người dùng gửi tin) , được tối đa hóa qua phân phối đầu vào

khả năng bảo mật hoàn hảo là sự khác biệt của hai phần thông tin chung của ng dùng và kẻ nghe trộm (không nghe lén đc toàn bộ nội dung) , phần của người dùng hợp pháp trừ phần của người nghe trộm = phần thông tin không chung, trong TH những thứ gửi đi đc tối ưu hóa trên ma trận hiệp phương sai đầu vào của người gửi.

***Gỉa định***

Giả định chính trong công việc này là người gửi biết các kênh của cả người dùng hợp pháp và người nghe trộm. Mặc dù đây có thể là một giả định hợp lý trong một số trường hợp, giả định thực tế hơn là người phát chỉ biết số liệu thống kê của người nghe trộm. Một vấn đề quan trọng là xác định khả năng bảo mật trong trường hợp này. Cuối cùng, nó cũng sẽ hữu ích để đưa ra các kế hoạch thực tế có thể đảm bảo bảo mật hoàn hảo khi máy phát chỉ có một phần CSI (tình trạng kênh) của người dùng hợp pháp.

\*\*

Nó được chứng minh rằng thông qua việc tối ưu ma trận phát, khả năng bảo mật của kênh nghe lén MIMO là sự khác biệt giữa băng thông của kênh nguồn-đến-đích với băng thông của kênh nguồn đến bên nghe lén.

Những kết quả trong [124] được cho rằng là kênh nguồn biết CSI ( tình trạng kênh) của cả kênh chính lẫn kênh nghe lén. Tuy nhiên, lời dự đoán này là không hợp lý trong các tình huống thực tế, vì bên nghe lén là bị động nên việc tính toán CSI của mỗi bên nghe lén là một thử thách lớn.

Một trường hợp thực tế hơn khi mà kênh nguồn chỉ có thông tin thống kê về CSI của những kênh nghe lén.

2011

=>Vì thế, He và đồng nghiệp [125] đã nghiên cứu một ngữ cảnh kênh nghe lén phát sóng MIMO hai bộ thu ( twin-receiver MIMO ), trong đó nguồn chính và đích chính được cho là không có thông tin gì về CSI của bên nghe lén.

\*\* **Extension**

Kênh nghe lén phát sóng MIMO hai đầu thu được coi là trạng thái kênh của người nghe trộm (thay đổi bất kì).

Kênh giữa người phát và hai người nhận hợp pháp là một kênh phát Gaussian MIMO không đổi (MIMO Gaussian broadcast channel)

Tài liệu tham khảo đã nghiên cứu một người dùng kênh nghe lén Gaussian MIMO và tìm thấy các” mức độ bảo mật tự do”- ” its secrecy degrees of freedom” của nó, đó là đặc điểm SNR cao của băng thông trong hình mẫu này

Tài liệu tham khảo cũng đã cung cấp mức độ bảo mật của vùng tự do khi phát sóng hai người nhận trên kênh Gaussian MIMO mà mỗi node hợp pháp có cùng số lượng ăng-ten

\*\*

Một thứ gọi là “khu vực mang tính bảo mật tự do”- “secrecy-degree-of-freedom region” được phát triển cho việc truyền phát không dây khi có sự hiện diện của một bên nghe lén. Đồng thời, một kế hoạch này dựa vào GSVD (phân tích giá trị đơn lẻ tổng quát) cũng đã được nêu lên nhằm đạt đến một “khu vực mang tính bảo mật tự do” tối ưu.

Các thông tin chính của bảo mật theo lý thuyết thông tin đc tổng hợp trong bảng 8

Text

Description automatically generated

## **B. BẢO MẬT HỖ TRỢ TIẾNG ỒN NHÂN TẠO.**

Bảo mật hỗ trợ tiếng ồn nhân tạo cho phép SN tạo ra các tín hiệu gây nhiễu cụ thể được gọi là tiếng ồn nhân tạo để chỉ người nghe trộm bị ảnh hưởng bất lợi bởi các tín hiệu gây nhiễu, trong khi DN dự định vẫn không bị ảnh hưởng.

Điều này dẫn đến việc giảm dung lượng của kênh nghe lén mà không ảnh hưởng đến dung lượng của kênh mong muốn và do đó dẫn đến khả năng bảo mật tăng lên, được định nghĩa là sự khác biệt giữa dung lượng của kênh chính và kênh nghe lén. Do đó, cải tiến bảo mật đạt được bằng cách sử dụng nhiễu nhân tạo.

Năn 2008, Goel và Negi đã xem xét một mạng không dây bao gồm SN, DN và một máy nghe trộm để điều tra những lợi ích của mô hình tạo tiếng ồn nhân tạo. Cụ thể hơn, SN phân bổ một phần công suất phát nhất định của nó để tạo ra tiếng ồn nhân tạo, do đó chỉ điều kiện kênh nghe lén bị suy giảm, trong khi đường truyền không dây mong muốn từ SN đến DN vẫn không bị ảnh hưởng bởi tiếng ồn nhân tạo. Để đáp ứng yêu cầu này, Goel và Negi đã đề xuất việc sử dụng nhiều ăng-ten để tạo ra tiếng ồn nhân tạo và chứng minh rằng số lượng ăng-ten phát tại SN phải nhiều hơn số lượng ăng-ten phát tại máy nghe trộm để đảm bảo rằng tiếng ồn nhân tạo sẽ không làm giảm chất lượng mong muốn. kênh truyền hình.

* Nó đã được chỉ ra rằng một khả năng bí mật khác có thể được đảm bảo để bảo mật truyền thông không dây bằng cách sử dụng tiếng ồn nhân tạo, ngay cả khi kẻ nghe trộm ở gần SN hơn DN.

Mặc dù bảo mật hỗ trợ tiếng ồn nhân tạo có khả năng đảm bảo bí mật của việc truyền tải không dây, điều này làm tốn chi phí, lãng phí tài nguyên công suất quý giá, vì một lần nữa, một lượng công suất nhất định phải được phân bổ để tạo ra nhiễu nhân tạo.

Năm 2010, Zhou an McKay đã kiểm tra thêm sự chia sẻ công suất phát tối ưu giữa tín hiệu truyền thông tin và nhiễu nhân tạo. Họ đã phân tích thông tin liên lạc nhiều ăng-ten an toàn dựa trên tiếng ồn nhân tạo và rút ra một biểu thức dung lượng bí mật dạng đóng cho các môi trường mờ dần, được sử dụng làm hàm mục tiêu để định lượng chia sẻ công suất tối ưu giữa tín hiệu thông tin và tiếng ồn nhân tạo. Việc chia sẻ quyền lực bình đẳng đơn giản được cho là một chiến lược không tối ưu, với điều kiện là những kẻ nghe trộm không cấu kết với nhau để cùng thực hiện việc đánh chặn. Hơn nữa, khi số lượng người nghe trộm tăng lên, cần phải phân bổ nhiều năng lượng hơn để tạo ra tiếng ồn nhân tạo

* Với sự hiện diện của CSI không hoàn hảo, người ta quan sát thấy rằng việc gán nhiều năng lượng hơn cho tiếng ồn nhân tạo để gây nhiễu những người nghe trộm có khả năng đạt được hiệu suất bảo mật tốt hơn so với việc tăng tốc độ truyền. công suất của tín hiệu thông tin mong muốn.

Tuy nhiên, công tác an ninh hỗ trợ tiếng ồn nhân tạo nói trên chủ yếu tập trung vào việc nâng cao năng lực bảo mật mà không xem xét đến các yêu cầu QoS của các doanh nghiệp hợp pháp. Do đó, để giải quyết vấn đề này, bảo mật hỗ trợ tiếng ồn nhân tạo dựa trên QoS- phương pháp tiếp cận đã được trình bày để giảm thiểu SINR tối đa có thể đạt được gặp phải ở những kẻ nghe trộm, đồng thời đảm bảo một SINR đạt yêu cầu tại DN dự định. Việc tối ưu hóa phân phối tiếng ồn nhân tạo được xây dựng dựa trên CSI của cả kênh chính và kênh nghe lén, được chứng minh là một vấn đề khó theo thời gian đa thức không xác định (NP-hard). Kỹ thuật SDR cổ điển được sử dụng để tính gần đúng lời giải của bài toán khó NP này. Liao và cộng sự đã chứng minh rằng kế hoạch bảo mật hỗ trợ tiếng ồn nhân tạo dựa trên QoS được đề xuất có khả năng bảo vệ hiệu quả chống lại các cuộc tấn công nghe trộm, đặc biệt là khi có một số lượng lớn người nghe trộm. Li và Ma đã đề xuất một sơ đồ bảo mật mạnh mẽ hỗ trợ tiếng ồn nhân tạo cho kênh nghe lén MISOME. Giả sử rằng SN có kiến ​​thức CSI hoàn hảo về các kênh chính, nhưng kiến ​​thức CSI không hoàn hảo về các kênh nghe lén, một bài toán tối ưu hóa đã được đặt ra để tối đa hóa tốc độ bí mật đối với cả hiệp phương sai của tín hiệu mong muốn và tiếng ồn nhân tạo, là bán vô hạn vấn đề tối ưu hóa và có thể được giải quyết với sự hỗ trợ của thuật toán tìm kiếm 1-D đơn giản. Nó chỉ ra rằng thiết kế tiếng ồn nhân tạo mạnh mẽ được đề xuất vượt trội hơn đáng kể so với các phương pháp tiếp cận không lọc thông thường về khả năng bí mật của nó.

Ngoài việc dựa vào nhiều ăng-ten để tạo ra tiếng ồn nhân tạo, các rơ le hợp tác cũng có thể được sử dụng để tạo ra tiếng ồn nhân tạo nhằm bảo vệ chống lại các cuộc tấn công nghe trộm. Năm 2012, Goeckel et al. nghiên cứu việc sử dụng các rơ le hợp tác cho tiếng ồn nhân tạo và đề xuất một giao thức truyền thông không dây bí mật, trong đó một rơ le nhắn tin được sử dụng để hỗ trợ truyền hợp pháp từ SN đến DN và một tập hợp các rơle can thiệp được sử dụng để tạo ra tiếng ồn nhân tạo được sử dụng để làm nhiễu những kẻ nghe trộm. Trọng tâm chính là xác định số lung Những kẻ nghe trộm có thể được dung thứ mà không ảnh hưởng đến bí mật thông tin liên lạc trong một mạng không dây hỗ trợ một số node hợp pháp nhất định. Nó được chỉ ra rằng nếu những kẻ nghe trộm được phân phối đồng đều và vị trí của chúng không xác định được đối với các node hợp pháp, thì số lượng người nghe trộm có thể chấp nhận được tăng tuyến tính với số lượng các node hợp pháp. Các kỹ thuật bảo mật hỗ trợ nhân tạo chính được tóm tắt trong Bảng 9.

Graphical user interface, text, application

Description automatically generated

Bảng 9

|  |  |  |
| --- | --- | --- |
| Năm | Tác giả | Đóng góp |
| 2008 | Goel et al | Đóng góp đã đề xuất việc sử dụng nhiều ăng-ten để tạo ra tiếng ồn nhân tạo và cho thấy rằng có thể đảm bảo khả năng bí mật khác không đối với thông tin liên lạc an toàn. |
| 2010 | Zhou et al | đã kiểm tra sự phân bổ công suất phát tối ưu giữa tín hiệu mang thông tin và nhiễu nhân tạo. |
| 2011 | Liao at al | đã đề xuất một phương pháp tiếp cận bảo mật hỗ trợ tiếng ồn nhân tạo dựa trên QoS để giảm thiểu SINR tối đa nhận được từ những người nghe trộm đồng thời đảm bảo nhận được một SINR thỏa đáng tại điểm đến đã định. |
| Li et al | đã nghiên cứu vấn đề tối đa hóa tốc độ bí mật tương ứng với hiệp phương sai tín hiệu mong muốn và hiệp phương sai tiếng ồn nhân tạo cho kênh nghe lén MISOME. |
| Goeckel et al | đã nghiên cứu việc sử dụng các rơ le hợp tác để tạo ra tiếng ồn nhân tạo và đề xuất một giao thức truyền thông không dây bí mật dựa trên rơ le.) |

## **C. SECURITY-ORIENTED BEAMFORMING TECHNIQUES**

Họ các kỹ thuật tạo chùm định hướng bảo mật cho phép SN truyền tín hiệu thông tin của nó theo một hướng cụ thể đến DN hợp pháp, do đó tín hiệu nhận được từ một kẻ nghe trộm (thường nằm ở một hướng khác với DN) bị nhiễu và do đó nó trở nên yếu. Do đó, RSS của DN sẽ trở nên cao hơn nhiều so với RSS của người nghe trộm với sự hỗ trợ của định hướng bảo mật, dẫn đến việc tăng cường khả năng bí mật (có lợi). Trong [131], Zhang và Gursoy đề xuất việc sử dụng các rơle hợp tác để tạo thành một hệ thống định dạng chùm dựa trên giả định đó là đơn giản hóa lý tưởng là có kiến thức CSI hoàn hảo về tất cả các kênh chính cũng như các kênh nghe lén và hình thành một giải mã-và- thiết kế dạng chùm dựa trên rơle chuyển tiếp để tối đa hóa (tỷ lệ)”mức độ” bí mật trong một giới hạn tổng công suất phát cố định. Bài toán công thức sau đó đã được giải quyết bằng cách sử dụng kỹ thuật lập trình bán nguyệt cổ điển và kỹ thuật lập trình hình nón bậc hai. [131] đã chỉ ra rằng phương pháp định dạng chùm được đề xuất có khả năng làm tăng đáng kể khả năng bí mật của truyền dẫn không dây.

Diagram, engineering drawing

Description automatically generated Chúng tôi xem xét một kênh liên lạc với nguồn S, đích D, máy nghe trộm E và M rơ le. Chúng tôi giả định rằng không có liên kết trực tiếp giữa S và D, và S và E. Chúng tôi cũng giả định rằng các rơle hoạt động đồng bộ bằng cách nhân các tín hiệu được truyền với trọng số phức tạp {w m} để tạo ra một chùm tia ảo điểm tới đích và kẻ nghe trộm. Trong mô hình này, nguồn S cố gắng truyền các thông điệp bí mật đến D với sự trợ giúp của các rơ le trong khi vẫn giữ cho kẻ nghe trộm E không biết thông tin. Rõ ràng là kênh của chúng tôi là mạng chuyển tiếp hai bước.

Trong [132], nhiều ăng-ten đã được sử dụng để định dạng chùm tia nhằm cải thiện khả năng bí mật có thể đạt được của các đường truyền không dây từ SN đến DN khi có kẻ nghe trộm. Trái ngược với công trình được trình bày trong [131], nơi kiến thức CSI hoàn hảo về kênh nghe lén được giả định, Mukherjee và Swindlehurst đã hình thành các thiết kế tạo chùm tối ưu trong [132] mà không dựa trên giả định đơn giản hóa lý tưởng về việc biết CSI của kẻ nghe trộm, mặc dù CSI chính xác của kênh chính trải dài từ SN đến DN vẫn được giả định là có sẵn. Tuy nhiên, CSI hoàn hảo của kênh chính thường không có sẵn ở SN. Cuối cùng, Mukherjee và Swindlehurst đã nghiên cứu thêm về tác động của CSI không hoàn hảo đối với hiệu suất bảo mật lớp vật lý có thể đạt được và trình bày một cặp sơ đồ tạo chùm mạnh mẽ có khả năng giảm thiểu ảnh hưởng của lỗi ước tính kênh. Nó chỉ ra rằng các kỹ thuật tạo chùm tia mạnh mẽ được đề xuất hoạt động tốt đối với các lỗi ước tính CSI vừa phải và do đó đạt được khả năng bảo mật cao hơn so với các phương pháp tiếp cận bảo mật có hỗ trợ tiếng ồn nhân tạo.

Ngoài Ra, Jeong et al. [133] đã nghiên cứu những lợi ích của việc truyền phát tia trong mạng chuyển tiếp khuếch đại và chuyển tiếp bao gồm SN, RN và DN, trong đó RN thực sự có khả năng cải thiện liên kết SN-to-DN, nhưng nó cũng có khả năng phát động một cuộc tấn công nghe lén bị động. Do đó, một cặp sơ đồ tạo chùm an toàn, cụ thể là bộ định dạng chùm bất hợp tác và bộ định dạng chùm an toàn hợp tác, đã được đề xuất để tối đa hóa khả năng bí mật của liên kết SN-to-DN. Các kết quả mô phỏng mở rộng đã được cung cấp để chứng minh rằng các sơ đồ tạo chùm tia an toàn được đề xuất có khả năng vượt trội hơn các phương pháp tiếp cận bảo mật thông thường về khả năng bảo mật có thể đạt được. Hơn nữa, trong [134], một phương pháp tiếp cận nhiều lớp khai thác nhiều luồng dữ liệu đồng thời của họ các tiêu chuẩn IEEE 802.11 hoạt động đã được nghĩ ra bằng cách sử dụng định dạng chùm không ép buộc, trong đó một AP được hỗ trợ bởi multiantenna được định cấu hình để sử dụng một trong các luồng dữ liệu của nó. để giao tiếp với người dùng mong muốn, trong khi các luồng dữ liệu còn lại đã bị khai thác để can thiệp tích cực vào những kẻ nghe trộm tiềm năng. Các đánh giá thử nghiệm mở rộng được thực hiện trong môi trường WLAN trong nhà thực tế, chứng minh rằng phương pháp tạo chùm tia không cưỡng bức được đề xuất luôn cấp SINR cho người dùng mong muốn, cao hơn 15 dB so với của người nghe trộm.

Đương nhiên, kỹ thuật định dạng chùm tia này cũng có thể được kết hợp với cách tiếp cận dựa trên tiếng ồn nhân tạo để tăng cường hơn nữa bảo mật lớp vật lý của các đường truyền không dây chống lại các cuộc tấn công nghe trộm. Do đó, trong [135], Qin et al. đã kiểm tra một dạng chùm tia chung và thiết kế hỗ trợ tiếng ồn nhân tạo để thu nhận thông tin liên lạc không dây an toàn từ SN đến DN khi có nhiều kẻ nghe trộm. Trọng số định dạng chùm và hiệp phương sai tiếng ồn nhân tạo được cùng nhau tối ưu hóa bằng cách giảm thiểu tổng công suất phát dưới một giới hạn tốc độ bảo mật mục tiêu cụ thể. Để giải thích thêm một chút, vấn đề thiết kế tạo chùm tia chung và thiết kế hỗ trợ tiếng ồn nhân tạo này đã được giải quyết bằng cách sử dụng phương pháp tối ưu hóa hai cấp, trong đó phương pháp thư giãn bán kỳ cổ điển và phương pháp dựa trên mặt cắt vàng [135] được sử dụng cho phần bên trong - tối ưu hóa cấp độ và tối ưu hóa cấp độ bên ngoài, tương ứng. Các kết quả số đã minh họa rằng sơ đồ tạo chùm tia chung và sơ đồ hỗ trợ tiếng ồn nhân tạo cải thiện đáng kể khả năng bí mật có thể đạt được của truyền dẫn không dây so với các phương pháp tạo chùm tia định hướng bảo mật thông thường.

Trong [136], Romero-Zurita et al. đã nghiên cứu việc sử dụng chung của tạo chùm tia không gian và tạo tiếng ồn nhân tạo để tăng cường bảo mật lớp vật lý có thể đạt được của kênh MISO khi có nhiều kẻ nghe trộm, trong đó không có kiến ​​thức CSI nào được sử dụng cho kênh nghe lén. Việc chia sẻ công suất tối ưu giữa tín hiệu thông tin và nhiễu nhân tạo đã được kiểm tra theo một yêu cầu xác suất bí mật được đảm bảo cụ thể. Bằng cách kết hợp các kỹ thuật định dạng chùm tia và tiếng ồn nhân tạo, cả tính bảo mật và độ tin cậy của đường truyền không dây đã được cải thiện đáng kể. Các kỹ thuật tạo chùm định hướng bảo mật chính được tóm tắt trong Bảng 10.

Graphical user interface, text, application

Description automatically generated

|  |  |  |
| --- | --- | --- |
| Năm | Tác giả | Đóng góp |
| 2010 | Zhang *et al.* [131] | đề xuất một sơ đồ định dạng chùm dựa trên chuyển tiếp hợp tác để tối đa hóa tỷ lệ bí mật với CSI hoàn hảo của các kênh chính và kênh ghi. |
| 2011 | Mukherjee *et al.* [132] | đã nghiên cứu thiết kế dạng chùm tia tối ưu trong các kênh nghe lén MIMO mà không cần biết kiến ​​thức về CSI của kẻ nghe trộm. |
| 2012 | Jeong *et al.* [133] | đã nghiên cứu dạng chùm phát trong các mạng chuyển tiếp không đáng tin cậy và đề xuất các phương án tạo chùm an toàn không hợp tác và các phương án tạo chùm an toàn hợp tác. |
| Romero-Zurita *et al.* [136] | Một sơ đồ tạo chùm không gian chung và nhiễu nhân tạo được đề xuất để cải thiện an ninh lớp vật lý. |

## **D. ĐA DẠNG HÓA PHƯƠNG PHÁP BẢO MẬT**

Phần này tập trung vào miêu tả sự đa dạng của các kỹ thuật được sử dụng để cải thiện bảo mật lớp vật lý của truyền không dây [137]. Trong trái ngược với các phương pháp tiếp cận hỗ trợ tiếng ồn nhân tạo, tiêu tán năng lượng bổ sung được gán cho tiếng ồn nhân tạo thế hệ, mô hình bảo mật hỗ trợ đa dạng là mục tiêu tăng cường bảo mật không dây mà không có bất kỳ sức mạnh nào khác. Theo truyền thống, các kỹ thuật đa dạng có được sử dụng để cải thiện khả năng tin cậy truyền đạt được, nhưng chúng cũng có tiềm năng đáng kể về mặt tăng cường bảo mật không dây chống nghe trộm các cuộc tấn công. Dưới đây chúng ta sẽ thảo luận về một số phương pháp tiếp cận đa dạng được hỗ trợ bởi sự đa dạng, bao gồm tính đa dạng được hỗ trợ bởi nhiều ăng-ten, tính đa dạng của nhiều người dùng và sự đa dạng hợp tác.

Phân tập phát nhiều ăng-ten hỗ trợ đã được chứng minh là tạo thành một phương tiện chiến đấu hiệu quả hiệu ứng mờ dần, do đó cũng làm tăng độ kín đáo của truyền dẫn không dây [138], [139]. Như hình trong hình dưới đây, với điều kiện SN có nhiều ăng-ten, ăng ten tối ưu có thể được kích hoạt để truyền tín hiệu mong muốn, tùy thuộc vào CSI của chính kênh và của kênh nghe lén có sẵn.

Diagram, engineering drawing

Description automatically generated

Cụ thể hơn, nếu CSI của cả kênh chính và của kênh nghe lén được biết đến tại SN, một tenna truyền cụ thể được liên kết với khả năng bí mật cao nhất có thể được chọn làm ăng ten tối ưu để truyền tín hiệu mong muốn, có tiềm năng cải thiện đáng kể khả năng bí mật của truyền dẫn không dây. Nếu chỉ CSI của kênh chính khả dụng, chúng tôi có thể chọn một kênh truyền ăng ten kết hợp với công suất kênh chính cao nhất để truyền tín hiệu mong muốn. Kể từ khi truyền lựa chọn ăng-ten hoàn toàn dựa trên CSI của kênh chính và kênh nghe lén thường lấn sâu vào kênh chính, dung lượng của kênh chính sẽ được tăng lên với sự hỗ trợ của lựa chọn ăng ten phát, trong khi không thể đạt được sự cải thiện dung lượng kênh nghe lén. Điều này cuối cùng dẫn đến việc tăng khả năng bí mật, như một lợi ích rõ ràng của việc truyền một lựa chọn teana.

Sự đa dạng đa người dùng của hình dưới đây cũng tạo thành một phương tiện hữu hiệu để cải thiện bảo mật lớp vật lý khi đối mặt với các cuộc tấn công nghe lén. Xét rằng BS phục vụ nhiều người dùng trong một mạng di động, một cơ chế đa truy cập trực tiếp, chẳng hạn như OFDMA của LTE hoặc CDMA của hệ thống 3G, cho phép nhiều người dùng để giao tiếp với BS. Đang cân nhắc OFDMA làm ví dụ, được cung cấp một khe cắm hoặc băng con của Diagram

Description automatically generated with medium confidence

Các sóng mang con OFDM, chúng ta nên xác định người dùng cụ thể nào được chỉ định để truy cập băng con cụ thể này cho truyền dữ liệu. Cụ thể hơn, một người dùng được kích hoạt với sự hỗ trợ của lập lịch đa người dùng để truy cập OFDM băng con và sau đó bắt đầu truyền tín hiệu của nó đến BS. Trong khi đó, do tính chất phát sóng của medium không dây, kẻ nghe trộm có thể chặn nguồn tin nhắn. Để bảo vệ hiệu quả mạng không dây truyền chống lại các cuộc tấn công nghe trộm, đa người dùng lập lịch phải được thiết kế để giảm thiểu dung lượng của kênh nghe lén, đồng thời tối đa hóa dung lượng của kênh chính [142]. Hành động này yêu cầu CSI của cả kênh chính và kênh nghe lén. Nếu chỉ CSI của kênh chính mới khả dụng, đa người dùng lập kế hoạch có thể được thiết kế để tối đa hóa chính dung lượng của kênh mà không có CSI của kênh nghe lén hiểu biết. Điều đáng nói là đa người dùng lập kế hoạch có khả năng cải thiện đáng kể dung lượng của kênh, trong khi dung lượng của kênh nghe lén vẫn giữ nguyên, dẫn đến chứng minh khả năng bí mật với sự hỗ trợ của đa dạng nhiều người dùng, ngay cả khi CSI của kênh nghe lén không xác định.

Thay vào đó, sự đa dạng hợp tác cũng có tiềm năng lớn trong việc bảo vệ đường truyền ít hơn chống lại các cuộc tấn công nghe trộm. Khi nào

xem xét một mạng không dây bao gồm một SN duy nhất, nhiều RN và một DN như trong hình dưới đây  
Diagram

Description automatically generated

Các điểm nối đa điểm có thể được khai thác để hỗ trợ sứ mệnh truyền tín hiệu từ SN sang DN. Để ngăn chặn kẻ nghe trộm chặn tín hiệu nguồn từ một quan điểm an ninh, lựa chọn chuyển tiếp tốt nhất xuất hiện như một phương tiện cải thiện bảo mật của đường truyền không dây chống lại các cuộc tấn công nghe trộm [145]. Cụ thể, một RN có khả năng giữ bí mật cao nhất (hoặc cao nhất dung lượng kênh chính nếu chỉ CSI của kênh chính là đã biết) được chọn để hỗ trợ truyền SN tới DN dự định. Bằng cách sử dụng lựa chọn RN tốt nhất, có thể đạt được mức tăng đa dạng hợp tác quan trọng có lợi cho vì lợi ích của việc tăng khả năng bí mật, một cách rõ ràng thể hiện lợi thế của lớp vật lý không dây

# **PHẦN 3: KẾT LUẬN**

**HẾT**