**V. 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

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 nút 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 nút truyền thông tin bí mật cho nút khác.Hay tốc độ tối đa truyền giữa các nút 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 nút 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