-The open communications environment makes wireless transmissions are more vulnerable than wired communications to malicious attacks, including both passive eavesdropping for data interception and active jamming for disrupting legitimate transmissions

( Môi trường giao tiếp mở làm cho truyền không dây dễ bị tấn công hơn so với truyền thông có dây, bao gồm cả nghe trộm thụ động để đánh chặn dữ liệu và gây nhiễu chủ động cho làm gián đoạn đường truyền hợp pháp )

-the art in physical-layer security, is an emerging technique of securing the open communications environment against eavesdropping attacks at the physical layer. Several physical-layer security techniques are reviewed and compared, including information-theoretic security, artificial-noise-aided security, security-oriented beamforming, diversity-assisted security, and physical-layer key generation approaches.

( nghệ thuật trong bảo mật lớp vật lý, là một kỹ thuật mới nổi để bảo vệ môi trường truyền thông mở chống lại các cuộc tấn công nghe trộm ở lớp vật lý. Một số lớp vật lý các kỹ thuật bảo mật được xem xét và so sánh, bao gồm bảo mật lý thuyết thông tin, bảo mật hỗ trợ tiếng ồn nhân tạo, định hướng bảo mật định hướng chùm tia, bảo mật được hỗ trợ đa dạng, và các cách tiếp cận tạo khóa lớp vật lý. )

-wireless networks are prone to malicious attacks,

including eavesdropping attack [24], DoS attack [25],

spoofing attack [26], MITM attack [27], message falsification/injection attack [28], etc

( mạng không dây dễ bị tấn công nguy hiểm, bao gồm cả tấn công nghe lén [24], tấn công DoS [25], tấn công giả mạo [26], tấn công MITM [27], tấn công giả mạo / đưa vào thư [28], v.v. )

-Wyner examined a discrete memoryless wiretap channel consisting of a source, a destination as well as an eavesdropper and proved that perfectly secure transmission can be achieved, provided that the channel capacity of the main link from the source to the destination is higher than that of the wiretap link from the source to the eavesdropper

( Wyner đã kiểm tra một kênh nghe lén không có bộ nhớ rời rạc bao gồm nguồn, đích cũng như người nghe trộm và đã chứng minh rằng có thể đạt được đường truyền hoàn toàn an toàn, miễn là dung lượng kênh của liên kết chính từ nguồn đến điểm đến cao hơn điểm đến của liên kết nghe lén từ nguồn đến người nghe trộm )

-Wyner’s results were extended from the discrete memoryless wiretap channel to the Gaussian wiretap channel, where the notion of a so-called secrecy capacity was developed, which was shown to be equal to the difference between the channel capacity of the main link and that of the wiretap link

( Kết quả của Wyner được mở rộng từ kênh nghe lén không có bộ nhớ rời sang kênh nghe lén Gaussian, nơi khái niệm về cái gọi là khả năng giữ bí mật đã được phát triển, được chứng minh là bằng với sự khác biệt giữa dung lượng kênh của liên kết chính và của liên kết nghe lén )

- If the secrecy capacity falls below zero, the transmissions from the source to the destination become insecure and the eavesdropper would become capable of intercepting the source’s transmissions [35], [36].

( Nếu khả năng giữ bí mật giảm xuống dưới 0, truyền từ nguồn đến đích trở thành không an toàn và kẻ nghe trộm sẽ có khả năng chặn đường truyền của nguồn [35], [36] )

- To improve the attainable transmission security, it is of importance to increase the secrecy capacity by exploiting sophisticated signal processing techniques, such as the artificial-noise-aided security [37]–[39], security-oriented beamforming [40], [41], security-oriented diversity approaches [42], [43] and so on.

( Để cải thiện bảo mật đường truyền, thì tăng secrecy capacity bằng cách khai thác các kỹ thuật xử lý tín hiệu phức tạp là rất quan trọng , chẳng hạn như bảo mật hỗ trợ nhiễu nhân tạo [37] - [39], định hướng chùm tia bảo mật [40], [41], phương pháp tiếp cận phân tập định hướng bảo mật [42], [43], v.v. )

- physical-layer security is emerging as an effective paradigm conceived for improving the security of wireless communications against eavesdropping attacks by exploiting the physical layer characteristics of wireless channels.

( bảo mật lớp vật lý đang nổi lên như một mô hình hiệu quả được hình thành để cải thiện tính bảo mật của truyền thông không dây chống lại các cuộc tấn công nghe trộm bằng cách khai thác các đặc tính lớp vật lý của các kênh không dây. )

- in wireless networks, the information is exchanged among authorized users, but this process is vulnerable to various malicious threats owing to the broadcast nature of the wireless medium. The security requirements of wireless networks are specified for the sake of protecting the wireless transmissions against wireless attacks, such as eavesdropping attack

( trong mạng không dây, thông tin được trao đổi giữa những người dùng được ủy quyền, nhưng quá trình này dễ bị ảnh hưởng bởi các mối đe dọa độc hại khác nhau do bản chất phát sóng của phương tiện không dây. Yêu cầu bảo mật của mạng không dây được xác định cho lợi ích của việc bảo vệ các đường truyền không dây chống lại tấn công không dây, chẳng hạn như tấn công nghe trộm,.. )

Diagram

Description automatically generated

- due to the broadcast nature of radio propagation, the physical layer of wireless transmission is extremely vulnerable to both eavesdropping and jamming attacks. This necessitates the development of physical-layer security as a complement to conventional upper-layer security protocols

( do bản chất phát sóng của truyền thanh, lớp vật lý của đường truyền không dây cực kỳ dễ bị tấn công nghe trộm và gây nhiễu. Cái này đòi hỏi sự phát triển của bảo mật lớp vật lý như một bổ sung cho các giao thức bảo mật lớp trên thông thường )

- when the wiretap channel spanning from the source to the eavesdropper is a degraded version of the main channel between the source and the destination.

( khi mà kênh nghe lén trải dài từ nguồn đến máy nghe trộm là phiên bản đã xuống cấp của kênh chính giữa nguồn và đích. )

A. Physical-Layer Attacks

- the broadcast nature of wireless communications makes its physical layer extremely vulnerable to eavesdropping and jamming attacks, which are two main types of wireless physical-layer attacks.

( Cách phát sóng nguyên bản của truyền thông không dây làm cho nó lớp vật lý cực kỳ dễ bị nghe trộm và các cuộc tấn công gây nhiễu, đó là hai loại mạng không dây chính tấn công lớp vật lý. )

More specifically, the eavesdropping attack refers to an unauthorized user attempting to intercept the data transmission between legitimate users.

( Cụ thể hơn, cuộc tấn công nghe lén đề cập đến một người dùng trái phép cố gắng chặn việc truyền dữ liệu giữa những người dùng hợp pháp. )

In wireless networks, as long as an eavesdropper lies in the transmit coverage area of the source node, the wireless communications session can be overheard by the eavesdropper.

( Trong mạng không dây, miễn là kẻ nghe trộm nằm trong vùng phủ sóng truyền khu vực của nút nguồn, phiên giao tiếp không dây có thể bị nghe trộm nghe trộm. )

To maintain confidential transmission, typically cryptographic techniques relying on secret keys are adopted for preventing eavesdropping attacks from intercepting the data transmission

(để duy trì việc truyền tải bí mật, thông thường các kỹ thuật mật mã dựa trên các khóa bí mật được áp dụng cho ngăn chặn các cuộc tấn công nghe trộm ngăn chặn truyền dữ liệu )

To be specific, the SN and the DN share a secret key, and the so-called plaintext is first encrypted at SN, leading to the ciphertext, which is then transmitted to DN.

( Cụ thể, SN và DN chia sẻ một khóa bí mật và cái gọi là bản rõ được mã hóa đầu tiên tại SN, dẫn đến văn bản mật mã, sau đó truyền đến DN. )

In this case, even if an eavesdropper overhears the ciphertext transmission, it remains difficult to extract the plaintext from the ciphertext without the secret key

( Trong trường hợp này, ngay cả khi kẻ nghe trộm nghe trộm được quá trình truyền bản mã, vẫn rất khó để trích xuất bản rõ từ bản mã mà không có chìa khóa bí mật )

A picture containing table

Description automatically generated

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

V. WIRELESS PHYSICAL-LAYER SECURITY AGAINST EAVESDROPPING

Diagram

Description automatically generated

-Fig. 17 shows a wireless scenario transmitting from a source to a destination in the presence of an eavesdropper, where the main and wiretap links refer to the channels spanning from the source to the destination and the eavesdropper, respectively.

( Hình 17 cho thấy một thiết bị không dây truyền từ nguồn đến đích trong sự hiện diện của một kẻ nghe trộm, trong đó chính và liên kết nghe lén đề cập đến các kênh trải dài từ nguồn tới đích và tới người nghe trộm, tương ứng. )

As shown in Fig. 17, when a radio signal is transmitted from the source, multiple differently delayed signals will be received at the destination via different propagation paths due to the signal reflection, diffraction and scattering experienced.

( Như thể hiện trong Hình 17, khi tín hiệu vô tuyến được truyền từ nguồn, nhiều lần bị trễ khác nhau tín hiệu sẽ được nhận tại điểm đến thông qua đường lan truyền do phản xạ tín hiệu, nhiễu xạ và rải rác có kinh nghiệm )

Owing to the multipath effects, the differently delayed signal components sometimes add constructively, sometimes destructively

( Do các hiệu ứng đa đường, các thành phần tín hiệu bị trễ khác nhau đôi khi thêm vào một cách như khuôn mẫu, đôi khi ngẫu nhiên )

Hence, the attenuation of the signal that propagated through the space fluctuates in time, which is referred to as fading and it is usually modeled as a random process

( Do đó, sự suy giảm của tín hiệu đã truyền thông qua không gian dao động trong thời gian, được đề cập đến như mờ dần và nó thường được mô hình hóa như một quá trình ngẫu nhiên )

The signal received at the destination may be attenuated significantly, especially when a deep fade is encountered, due to the shadowing in the presence of obstacles (e.g., trees) between the source and destination

( Tín hiệu nhận được tại điểm đến có thể bị suy giảm đáng kể, đặc biệt là khi gặp phải hiện tượng mờ dần, do bóng mờ khi có chướng ngại vật (ví dụ: cây) giữa nguồn và đích

)

Moreover, due to the broadcast nature of radio propagation, the source signal may be overheard by the eavesdropper, which also experiences a multipath fading process

( Hơn thế nữa, do bản chất phát sóng của truyền thanh, tín hiệu nguồn có thể bị kẻ nghe trộm nghe lén, cũng trải qua quá trình mờ dần nhiều đường- a multipath fading process )

- when a radio signal is transmitted from the source, multiple differently delayed signals will be received at the destination via different propagation paths due to the signal reflection, diffraction and scattering experienced.

( khi một tín hiệu radio được truyền từ nguồn, nhiều lần bị trễ khác nhau tín hiệu sẽ được nhận tại điểm đến thông qua đường lan truyền do phản xạ tín hiệu, nhiễu xạ và rải rác có kinh nghiệm. )

- it was shown that reliable information-theoretic security can be achieved when the wiretap channel spanning from the source to the eavesdropper is a degraded version of the main channel between the source and the destination.

( nó đã được chỉ ra rằng bảo mật thông tin-lý thuyết có thể đạt được, khi kênh nghe lén trải dài từ nguồn đến máy nghe trộm là phiên bản đã xuống cấp của kênh chính giữa nguồn và đích. )

- when the wiretap channel spanning from the source to the eaves-dropper is a degraded version of the main channel between the source and the destination.

( khi kênh nghe lén trải dài từ nguồn đến eaves-dropper là một phiên bản đã xuống cấp của kênh chính giữa nguồn và đích. )

- a so-called secrecy capacity was developed and shown as the difference between the capacity of the main channel and that of the wiretap channel, where a positive secrecy capacity means that reliable information-theoretic security is possible and vice versa.

( Cái gọi là năng lực bí mật được phát triển và thể hiện như là sự khác biệt giữa dung lượng của kênh chính và của kênh nghe lén, nơi có khả năng giữ bí mật tích cực có nghĩa là khả năng bảo mật lý thuyết-thông tin đáng tin cậy và ngược lại. )

However, in contrast to wired channels that are typically time-invariant, wireless channels suffer from time-varying random fading, which results in significant degradation of the wireless secrecy capacity, especially when a deep fade is encountered in the main channel due to shadowing by obstacles (e.g., buildings, trees, etc.) appearing between the source and the destination

( Tuy nhiên, trái ngược với các kênh có dây thường bất biến theo thời gian, các kênh không dây bị “phai màu ngẫu nhiên thay đổi theo thời gian”, dẫn đến suy giảm đáng kể khả năng bảo mật không dây ,đặc biệt là khi gặp phải sự mờ dần trong kênh chính do bị che khuất bởi các chướng ngại vật (ví dụ: tòa nhà, cây cối, v.v.) xuất hiện giữa nguồn và Nơi Đến )

1. Information-Theoretic Security

I.Khái niệm

- Một hệ thống mật mã được coi là **có tính bảo mật về mặt lý thuyết thông tin** (còn được gọi là **bảo mật vô điều kiện** ) nếu hệ thống được bảo mật trước kẻ thù với tài nguyên và thời gian tính toán không giới hạn. Ngược lại, một hệ thống phụ thuộc vào chi phí tính toán của phân tích mật mã để được bảo mật (và do đó có thể bị phá vỡ bởi một cuộc tấn công với khả năng tính toán không giới hạn) được gọi là tính toán, hoặc có điều kiện, an toàn.

II.Tổng quát

-Một giao thức mã hóa với bảo mật thông tin-lý thuyết là không thể phá vỡ ngay cả với sức mạnh tính toán vô hạn. Các giao thức được chứng minh là an toàn thông tin về mặt lý thuyết có khả năng chống lại sự phát triển trong tương lai của máy tính. Khái niệm truyền thông an toàn về mặt lý thuyết được đưa ra vào năm 1949 bởi nhà toán học người Mỹ Claude Shannon , một trong những người sáng lập ra lý thuyết thông tin ( information theory ) cổ điển , người đã sử dụng nó để chứng minh hệ thống đệm một lần ( one-time pad ) là an toàn. Các hệ thống mật mã an toàn về mặt lý thuyết thông tin đã được sử dụng cho các thông tin liên lạc nhạy cảm nhất của chính phủ, chẳng hạn như điện tín ngoại giao ( diplomatic cables ) và thông tin liên lạc quân sự cấp cao.

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

<https://en.wikipedia.org/wiki/One-time_pad>

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

Có một loạt các nhiệm vụ mật mã mà bảo mật thông tin-lý thuyết là một yêu cầu hữu ích và có ý nghĩa. Một vài trong số này là:

1. Các kế hoạch chia sẻ bí mật ( [Secret sharing](https://en.wikipedia.org/wiki/Secret_sharing) ) như của Shamir ( Shamir's ) được bảo mật thông tin về mặt lý thuyết (và cũng an toàn tuyệt đối) ở chỗ có ít hơn số lượng chia sẻ bí mật cần thiết sẽ không cung cấp thông tin về bí mật.

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

<https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing>

1. Nói chung hơn, các giao thức tính toán đa bên an toàn (  [secure multiparty computation](https://en.wikipedia.org/wiki/Secure_multiparty_computation)  ) thường có tính bảo mật về mặt lý thuyết thông tin.

<https://en.wikipedia.org/wiki/Secure_multi-party_computation>

1. Việc truy xuất thông tin cá nhân ( Private information retrieval ) với nhiều cơ sở dữ liệu có thể đạt được với sự riêng tư về mặt lý thuyết thông tin cho truy vấn của người dùng.

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

1. Mã hóa đối xứng có thể được xây dựng theo một khái niệm lý thuyết thông tin về bảo mật được gọi là bảo mật entropi ( entropic security ) , giả định rằng kẻ thù hầu như không biết gì về thông điệp được gửi đi. Mục đích ở đây là để ẩn tất cả các chức năng của bản rõ hơn là tất cả thông tin về nó.

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

1. Mật mã lý thuyết thông tin là an toàn lượng tử ( quantum-safe )

<https://en.wikipedia.org/wiki/Post-quantum_cryptography>

III. Mã hóa lớp vật lý

Các thuật toán giới hạn kỹ thuật ( Technical limitations Algorithms ) được bảo mật về mặt tính toán hoặc có điều kiện (tức là chúng không an toàn về mặt lý thuyết thông tin) phụ thuộc vào các giới hạn tài nguyên. Ví dụ, RSA dựa vào khẳng định rằng việc bao thanh toán các số lượng lớn là khó

Một khái niệm yếu hơn về bảo mật, được định nghĩa bởi Aaron D. Wyner , đã thiết lập một lĩnh vực nghiên cứu hiện đang phát triển mạnh được gọi là mã hóa lớp vật lý. Nó khai thác kênh không dây vật lý để bảo mật bằng kỹ thuật truyền thông, xử lý tín hiệu và mã hóa. Bảo mật là có thể chứng minh , không thể phá vỡ và có thể định lượng (tính bằng bit / giây / hertz).

Công việc mã hóa lớp vật lý ban đầu của Wyner vào những năm 1970 đã đặt ra vấn đề Alice – Bob – Eve, trong đó Alice muốn gửi một tin nhắn cho Bob mà không cho Eve giải mã nó. Nếu kênh từ Alice đến Bob tốt hơn về mặt thống kê so với kênh từ Alice đến Eve, thì điều đó đã chứng minh rằng có thể giao tiếp an toàn. Đó là trực giác, nhưng Wyner đã đo lường tính bí mật trong các thuật ngữ lý thuyết thông tin xác định khả năng giữ bí mật, về cơ bản là tốc độ mà Alice có thể truyền thông tin bí mật cho Bob. Ngay sau đó, Imre Csiszár và Körner cho thấy rằng có thể giao tiếp bí mật ngay cả khi Eve có một kênh thống kê tốt hơn Alice so với Bob. Ý tưởng cơ bản của phương pháp lý thuyết thông tin ( Information-theoretic ) để truyền các thông điệp bí mật một cách an toàn (không sử dụng khóa mã hóa) đến một người nhận hợp pháp là sử dụng tính ngẫu nhiên vốn có của phương tiện vật lý (bao gồm tiếng ồn và dao động kênh do mờ dần) và khai thác sự khác biệt giữa kênh tới người nhận hợp pháp và kênh tới người nghe trộm để mang lại lợi ích cho người nhận hợp pháp. Các kết quả lý thuyết gần đây hơn liên quan đến việc xác định khả năng bí mật và phân bổ công suất tối ưu ( in broadcast fading channels ) . Có một số lưu ý là không thể tính toán được nhiều dung lượng trừ khi có giả định rằng Alice biết kênh dẫn đến Eve. Nếu biết được điều đó, Alice có thể chỉ cần đặt một null theo hướng của Eve. Khả năng bí mật đối với MIMO và nhiều kẻ nghe lén thông đồng là công việc đang diễn ra gần đây hơn, và những kết quả như vậy vẫn đưa ra giả định không hữu ích về kiến ​​thức thông tin trạng thái kênh của kẻ nghe trộm.

Song song với công việc đó trong cộng đồng lý thuyết thông tin là công việc trong cộng đồng anten, được gọi là điều chế anten trực tiếp trường gần hoặc điều chế định hướng. Người ta đã chỉ ra rằng bằng cách sử dụng một mảng ký sinh , điều chế được truyền theo các hướng khác nhau có thể được điều khiển một cách độc lập. Bí mật có thể được thực hiện bằng cách làm cho các điều chế theo hướng không mong muốn khó giải mã. Việc truyền dữ liệu điều chế định hướng đã được thực nghiệm chứng minh bằng cách sử dụng một mảng theo từng giai đoạn ( phased array ) . Những người khác đã chứng minh điều chế định hướng với mảng chuyển mạch và thấu kính liên hợp pha

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

Loại điều chế hướng đó ( directional modulation ) thực sự là một tập con của sơ đồ mã hóa nhiễu nhân tạo cộng tính của Negi và Goel. Một sơ đồ khác sử dụng các ăng ten phát có thể định cấu hình lại theo mẫu ( pattern-reconfigurable ) cho Alice được gọi là nhiễu nhân ( multiplicative noise ) tạo có thể định cấu hình lại (RMN) bổ sung cho nhiễu nhân tạo cộng tính. Cả hai hoạt động tốt cùng nhau trong mô phỏng kênh mà Alice hoặc Bob không biết gì về những kẻ nghe trộm.

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

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

IV. Thỏa thuận khóa bí mật

Các công việc khác nhau được đề cập trong phần trước, theo cách này hay cách khác, sử dụng tính ngẫu nhiên hiện diện trong kênh không dây để truyền tải các thông điệp an toàn về mặt lý thuyết. Ngược lại, chúng ta có thể phân tích xem người ta có thể trích xuất bao nhiêu bí mật từ chính sự ngẫu nhiên dưới dạng một khóa bí mật ( secret key. ) . Đó là mục tiêu của thỏa thuận khóa bí mật .

Trong dòng công việc này, được bắt đầu bởi Maurer và Ahlswede và Csiszár, mô hình hệ thống cơ bản loại bỏ bất kỳ hạn chế nào đối với các kế hoạch giao tiếp và giả định rằng người dùng hợp pháp có thể giao tiếp hai chiều, công khai, noiseless và kênh xác thực miễn phí. Mô hình này sau đó đã được mở rộng cho nhiều người dùng và một” noisy channel “trong số những người khác.

1. Information-Theoretic Security

Bảo mật lý thuyết thông tin kiểm tra giới hạn cơ bản của các biện pháp bảo mật lớp vật lý từ một quan điểm thông tin-lý thuyết. Khái niệm của bảo mật lý thuyết thông tin được Shannon tiên phong ở [119], nơi lý thuyết cơ bản về hệ thống bí mật được phát triển với trọng tâm là cấu trúc và tính chất toán học. Cụ thể, Shannon đã định nghĩa một hệ thống bí mật như một tập hợp các phép biến đổi toán học của một khoảng trắng (tập hợp các thông báo văn bản rõ ràng hợp pháp) vào một không gian khác (tập hợp các mật mã có thể có), trong đó mỗi phép biến đổi tương ứng với sự kết hợp thông tin với sự hỗ trợ của một khóa bí mật . Hơn thế nữa, sự biến đổi là không cần chú ý để có cách giải mã duy nhất trở nên khả thi , với điều kiện là khóa bí mật là đã biết. Trong [119], các khái niệm về bí mật lý thuyết và bí mật thực tế đã được giới thiệu, đã được phát triển để dễ dàng bảo vệ chống lại các cuộc tấn công nghe trộm, khi một kẻ thù được cho là có vô hạn hoặc thực tế hơn là sức mạnh tính toán hữu hạn.

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

- the notions of theoretical secrecy and practical secrecy were introduced, which was developed for the ease of guarding against eavesdropping attacks when an adversary is assumed to have the either infinite or more practically finite computing power

( các khái niệm về bí mật lý thuyết và bí mật thực tế đã được giới thiệu, đã được phát triển để dễ dàng bảo vệ chống lại các cuộc tấn công nghe trộm, khi một kẻ thù được cho là có vô hạn hoặc thực tế hơn sức mạnh tính toán hữu hạn )

- QoS-based artificial-noise-aided security the scheme is capable of efficiently guarding against eavesdropping attacks, especially in the presence of a large number of eavesdroppers

( Bảo mật hỗ trợ tiếng ồn nhân tạo dựa trên QoS chương trình có khả năng bảo vệ hiệu quả chống lại các cuộc tấn công nghe trộm, đặc biệt là khi có sự hiện diện của một lượng lớn số người nghe trộm )

- relying on multiple antennas for artificial noise generation, cooperative relays may also be utilized for producing artificial noise to guard against eavesdropping attacks

( dựa vào nhiều ăng-ten để tạo ra tiếng ồn nhân tạo, các rơle 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 )

-