**V. BẢO MẬT TẦNG VẬT LÝ KHÔNG DÂY NHẰM CHỐNG NGHE LÉN**

Trong phần này, chúng ta sẽ 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. Hình 17 cho thấy một tình huống khi đường truyền không dây phát tín hiệu từ một nguồn tới điểm đích có sự xuất hiện của bên nghe lén. Hình có thể hiện đường dẫn chính từ nguồn tới đích và một đường dẫn bị xâm nhập bởi bên nghe lén. Như trong hình 17, khi tín hiệu radio được truyền từ nguồn, nhiều tín hiệu bị làm chậm khác sẽ được chuyển tới đích đến thông qua phản xạ, tán xạ và nhiễu xạ sóng. Do hiệu ứng phân luồng, những tín hiệu đã được làm chậm có thể sẽ có ích hoặc gây hại. 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,..) ở giữa nguồn và đích. Hơn nữa, do cách mà sóng radio được truyền đi, nguồn sóng có thể bị nghe lén. Thông thường sẽ có 3 dạng lan truyền xác suất được dùng để xác định sự phai đi ngẫu nhiên không dây, bao gồm Rayleigh [115], Rice [116] và Nakagami [117].

Diagram

Description automatically generated

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 [33], [34], [118]. Chính xác hơn, [33] đã cho thấy sự bảo mật đáng tin cậy là có thể thực hiện được theo lý thuyết, khi mà kênh truyền bị xâm nhập từ nguồn tới bên nghe lén là một phiên bản kém hơn của kênh truyền chính từ nguồn đến đích. Trong [34], một thứ gọi là “băng thông ưu tiên” đã được phát triển và cho thấy như là sự khác biệt giữa sức chứa của kênh truyền chính và kênh truyền bị xâm nhập, khi mà “băng thông ưu tiên” 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. Tuy nhiên, trong khi kết nối có dây thì thường không thay đổi theo thời gian, kết nối không dây thì lại bị ảnh hưởng bởi sự phai đi ngẫu nhiên theo thời gian, dẫn đến sự giảm sút về chất lượng của “băng thông ưu tiên” 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]

Những phương pháp bảo mật nêu trên được tóm gọn lại trong hình 18. Sau đây, chúng ta sẽ tìm hiểu thêm về những chủ đề bảo mật tầng vật lý trên.

1. **Bảo mật theo tính lý thuyết thông tin**

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. Khái niệm về bảo mật theo tính lý thuyết thông tin được phát triển bởi Shannon trong [119], khi mà nguyên lý đơn giản của những hệ thống ưu tiên được phát triển với sự nhấn mạnh về cấu trúc và đặc tính toán học.

Rõ hơn là, Shannon đã định nghĩa một hệ thống ưu tiên như một nhóm những sự chuyển đổi toán học của một không gian à (nhóm tin nhắn dưới dạng kí tự thường) tới một không gian khác (nhóm mật mã). Mỗi sự chuyển đổi tương ứng với sự mã hóa thông tin với sự trợ giúp của khóa bí mật. Hơn nữa, mỗi chuyển đổi là không suy biến, vì thế sự giải mã độc nhất là hoàn toàn có thể nếu như biết khóa bí mật.

Trong [199], ý tưởng về bảo mật theo lý thuyết và bảo mật thiết thực đã được giới thiệu và phát triển nhằm giúp trong 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] đã cho thấy một hệ thống ưu tiên có thể được tạo ra, mặc dù sử dụng một chìa khóa bí mật có hạn, khi bên xâm nhập không thể tìm ra được giải pháp độc nhất để giải mã. Để giải thích thêm, lượng mật mã được định nghĩa như là một đơn vị để tính sự không chắc chắn của bên xâm nhập khi phán đoán mật mã sau khi lấy được tin nhắn [119].

Hệ thống ưu tiên 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 trong những mạng lưới không dây hoạt động không có một cơ sở hạ tầng cố định (vd: mạng không dây chỉ sử dụng khi cần thiết) [32]. Vì thế, trong [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 để xây dựng một kênh truyền bị xâm nhập bí mật không dùng bộ nhớ bao gồm một nguồn, một đích và một bên nghe lén. Nó đã cho thấy 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.

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.

Trong [34], kết quả của Wyner được áp dụng xa hơn tới kênh xâm nhập Gaussian, nơi mà khái niệm của băng thông ưu tiên được phát triển, cái mà phân biệt băng thông của kênh truyền chính với kênh truyền bị xâm nhập.

Nếu tần suất ưu tiên được chọn dưới băng thông ưu tiên, sự truyền tin đảm bảo từ nguồn tới đích sẽ có thể đạt tới độ bí mật tuyệt đối.

Trong mạng không dây, kênh truyền ưu tiên bị giảm chất lượng do sự phai đi dựa trên thời gian. Đây là bởi vì sự yếu đi của tín hiệu được nhận tới một đích đến chính thống, cái mà làm giảm băng thông của những kênh truyền chính thống này, từ đó dẫn đến sự giảm sút về chất lượng của “khả năng bảo mật”.

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 băng thông ưu tiên trong những môi trường không hiệu quả. Trong [120], Khisti và những người khác đã nghiên cứu một trường hợp gọi là MISOME, 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, ...), băng thông ưu tiên của tình huống MISOME có thể được phân biệt bằng trị riêng của nó

. Nên nhớ rằng những thông tin được biết về những phản hồi bất ngờ của bên nghe lén thường là không khả dụng, Khisti và những người khác [121] ủng hộ việc sử dụng một kế hoạch gọi là điều sóng ẩn nhằm tăng cường bảo mật tầng vật lý không dây, khi mà thông tin về bên nghe lén không bị phụ thuộc để tìm phương hướng truyền tín hiệu. 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.

Hơn nữa, Khisti và những người khác đã mở rộng kết quả của họ đến những kênh truyền không dây dựa vào thời gian và phát triển cả mức trên và dưới của băng thông ưu tiên trong tình huống MISOME hoạt động trong môi trường phai đi Rayleigh. Tóm lại, nghiên cứu của Khisti và đồng nghiệp [121] tập trung chủ yếu vào việc thể hiện đặc tính băng thông ưu tiên 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.

Sau này, Khisti và đồng nghiệp [122] đã nghiên cứu bảo mật theo tính lý thuyết thông tin đạt được với sự trợ giúp của nhiều ăng ten trong một tình huống chung hơn, khi mà nguồn, đích và bên nghe lén được coi là có nhiều ăng ten. Họ xem xét hai trường hợp: 1) Trường hợp được đơn giản hóa và coi như hoàn hảo. Trong đó CSIs của cả hai đường dẫn chính và đường dẫn bị xâm nhập là cố định và được biết bởi các bên liên quan. 2) Trường hợp phai đi thực tế. Trong đó những kênh truyền không dây bị ảnh hưởng bởi sự phai đi theo thời gian Rayleigh. Nguồn gồm những kênh chính có CSI hoàn hảo và thông tin CSI của kênh truyền bị xâm nhập.

Trong trường hợp 1, họ sử dụng một phương pháp dựa vào GSVD để tăng băng thông ưu tiên trong khu vực có SNR cao. Độ hiệu quả của kế hoạch GSVD được nghiên cứu sâu hơn trong trường hợp có sự phai đi và cho thấy băng thông ưu tiên đạt 0 khi và chỉ khi tỉ lệ ăng ten của bên nghe lén với ăng ten bên nguồn lớn hơn 2. 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 băng thông ưu tiên, thứ mà được dùng để mô tả tỉ lệ ưu tiên lớn nhất trong trường hợp sự mất mát là có thể xảy ra. Một biểu thức dạng đóng của mất mát trong băng thông ưu tiên được trích trong [123] bằng cách sử dụng một hệ thống Taylor cơ bản cho việc tính toán hàm mũ.

Kênh truyền bị xâm nhập MIMO có thể được gọi là kênh phát MIMO, khi mà kênh nguồn phát sóng những thông tin bí mật tới kênh đích lẫn kên bị nghe lén. Bảo mật tuyệt đối được đạt tới 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. Trong [124], Oggier và Hassibi phân tích băng thông ưu tiên của những hệ thống được hỗ trợ bằng ăng ten bằng cách chuyển đổi kênh xâm nhập 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). Nó được chứng minh rằng thông qua việc tối ưu ma trận phát, băng thông ưu tiên của kênh xâm nhập sẽ bị phát hiện bởi sự khác biệt giữa băng thông của kênh nguồn-đến-đích với băng thông của kênh nguồn đến bên nghe lén. Những kết quả lấy trong [124] được cho là dựa vào sự dự đoán được đơn giản hóa rằng kênh nguồn biết CSI của cả kênh chính lẫn kênh nghe lén. Tuy nhiên, lời dự đoán này là NGU XUẨN trong những trường hợp thực tế, vì bên nghe lén là bị động nên việc tính toán CSI của bên nghe lén là một thử thách lớn. Việc nghiên cứu một trường hợp thực tế hơn đang rất được quan tâm, khi mà kênh nguồn chỉ có thông tin về CSI của kênh nghe lén theo thông số. Vì thế, He và đồng nghiệp [125] đã nghiên cứu một trường hợp kênh nghe lén có kênh nhận MIMO đôi, trong đó nguồn chính và đích chính được cho là không có thông tin gì về CSI của bên nghe lén. Một thứ gọi là “khu vực mang tính bảo mật tự do” được phát triển cho việc truyền phát không dây khi có sự hiện diện của một bên nghe lén. Đồng thời, một kế hoạch dựa vào GSVD cũng đã được nêu lên nhằm đạt đến một “khu vực mang tính bảo mật tự do” tối ưu. Những phương pháp bảo mật theo tính lý thuyết thông tin đã được tóm gọn lại trong Bảng 8.