Nghiên cứu một số phương pháp chế áp tín hiệu Wifi tiêu chuẩn IEEE 802.11 dưới 6 GHz

Lê Hải Triều, Trương Chí Kiên, Ngô Thu Hiền

***Tóm tắt*— Ra đời năm 1980 theo tiêu chuẩn IEEE 802.11, mạng không dây Wifi (Wireless Fidelity) hỗ trợ mở rộng mạng có dây và dần dần đã trở thành thành phần quan trọng của cơ sở hạ tầng viễn thông trong xã hội. Hiện nay, hệ thống hạ tầng mạng Wifi ngày càng trở nên quan trọng khi ứng dụng của nó đã giúp cho việc kết nối nhanh chóng với các nguồn thông tin, nắm bắt sự kiện, tin tức hiệu quả. Tuy nhiên, mạng Wifi đã bị lợi dụng để tiến hành các hoạt động gián điệp, khủng bố, phá hoại, thực hiện các hành vi phạm tội như thu thập thông tin bất hợp pháp, định vị vị trí, điều khiển từ xa, tấn công khủng bố, đặc biệt là tuyên truyền xuyên tạc, kích động chống phá Đảng, Nhà nước của các thế lực thù địch, các tổ chức tội phạm gây ảnh hưởng đến an ninh quốc gia, mất an toàn thông tin thường xuyên diễn ra tại các khu vực bảo vệ sự kiện nhạy cảm. Trong bài báo này, nhóm tác giả tập trung vào việc nghiên cứu một số phương pháp chế áp tín hiệu Wifi tại các khu vực bảo vệ các sự kiện nhạy cảm nhằm đề xuất lựa chọn giải pháp phù hợp nhất xử lý kịp thời không để xuất hiện những tình huống xấu.**

***Abstract*— Launched in 1980 according to the IEEE 802.11 standard, Wifi (Wireless Fidelity) wireless network supports the expansion of wired networks and has gradually become an important component of telecommunications infrastructure in society. Currently, Wifi network infrastructure is becoming increasingly important as its application has helped quickly connect to information sources, capture events and news effectively. However, the Wifi network has been exploited to conduct espionage, terrorism, sabotage, and criminal acts such as illegally collecting information, locating relatively accurate locations, and controlling remotely, illegally collecting information, terrorist attacks, especially distorted propaganda and incitement against the Party and Government of Vietnam by hostile forces and criminal organizations that affect national security, causing information insecurity that frequently occurs in sensitive event protection areas. In this article, the authors focus on researching a number of methods to jam Wifi signals in sensitive event protection areas to propose the most appropriate solution to promptly handle and prevent incidents from occurring bad situations arise.**

Từ khóa— an toàn thông tin, Wifi, chế áp, bộ phát Wifi, tiêu chuẩn.

Keyworks— information security; Wifi; jamming; Wifi router; standard.

I. GIỚI THIỆU VỀ TIÊU CHUẨN WIFI

Mạng Wifi là mạng không dây chiếm ưu thế nhất trong hạ tầng kết nối cho các dịch vụ Internet tầm ngắn, dung lượng cao và được triển khai rộng rãi ở các khu vực công cộng như khu chung cư, nhà ở, văn phòng, trường học, khu trung tâm thương mại và sân bay, nhà hàng, khách sạn, các nơi tổ chức sự kiện trong nước và quốc tế có tầm ảnh hưởng đến chính trị - xã hội. Hiện nay, mạng Wifi sử dụng các tiêu chuẩn IEEE 802.11 a/b/g/n/ac/ax để hoạt động. Các tiêu chuẩn này được áp dụng trong các thiết bị đầu cuối thương mại khác nhau như điện thoại thông minh, máy tính xách tay, máy in, máy ảnh và tivi thông minh [2].

- *Tiêu chuẩn 802.11:* Năm 1997, IEEE đã giới thiệu tiêu chuẩn mạng không dây đầu tiên và đặt tên nó là 802.11. Khi đó, tốc độ hỗ trợ

Bài báo được gửi báo cáo trước đó tại Hội thảo quốc gia VNICT 2023, sau đó gửi Tạp chí vào ngày 17/9/2023. Bài báo được nhận xét bởi phản biện thứ nhất vào ngày 04/10/2023 và được chấp nhận đăng ngày 10/10/2023. Bài báo được nhận xét bởi phản biện thứ hai ngày 29/9/2023 và được chấp nhận đăng ngày 10/10/2023.

tối đa của mạng này chỉ là 2 Mbps với băng tần 2,4 GHz.

- *Tiêu chuẩn 802.11b:* Vào tháng 7/1999, tiêu chuẩn 802.11b ra đời và hỗ trợ tốc độ lên đến 11 Mbps. Chuẩn này cũng hoạt động tại băng tần 2,4 GHz nên dễ bị can nhiễu từ các thiết bị điện tử khác cùng dùng chung băng tần.

- *Tiêu chuẩn 802.11a:* Song song với quá trình hình thành tiêu chuẩn b, tiêu chuẩn 802.11a phát ở tần số cao hơn là 5 GHz nhằm tránh bị nhiễu từ các thiết bị khác. Tốc độ xử lý của tiêu chuẩn đạt 54 Mbps, tuy nhiên tiêu chuẩn này khó xuyên qua các vật cản, ví dụ như bức tường,…

- *Tiêu chuẩn 802.11g:* Tiêu chuẩn 802.11g có tốc độ cao hơn so với chuẩn b, hoạt động ở tần số 2,4 GHz. Tốc độ xử lý đã được nâng lên 54 Mbps.

- *Tiêu chuẩn 802.11n:* Ra mắt năm 2009 và là tiêu chuẩn phổ biến nhất hiện nay nhờ sự vượt trội hơn so với tiêu chuẩn 802.11.b và 802.11.g. Tiêu chuẩn này hỗ trợ tốc độ tối đa lên đến 300 Mbps, hoạt động trên cả băng tần 2,4 GHz và 5 GHz.

- *Tiêu chuẩn 802.11ac:* Đây là tiêu chuẩn được IEEE giới thiệu vào đầu năm 2013, hoạt động ở băng tần 5 GHz. Tiêu chuẩn này cho tốc độ cao nhất lên đến 1730 Mpbs.

- *Tiêu chuẩn 802.11ax:* Đây là tiêu chuẩn Wifi 6 được cập nhật năm 2019. Wifi 6 có tốc độ nhanh hơn, dung lượng lớn hơn và hiệu suất năng lượng được cải thiện tốt hơn so với các kết nối không dây trước đây.

- *Tiêu chuẩn Wifi 6E:* Đã được cung cấp ra thị trường, tuy nhiên do giá cả và thiết bị đầu cuối còn ít hỗ trợ nên chưa phổ biến. Đây là phiên bản nâng cấp của Wifi 6, bổ sung thêm băng tần số 6 GHz.

- *Tiêu chuẩn Wifi 7:* Đang được thử nghiệm và dự kiến năm 2024 sẽ ra mắt, bổ sung băng tần số 7.25 GHz.

Bảng 1 tóm tắt các tham số kỹ thuật của một số tiêu chuẩn Wifi đang sử dụng rộng rãi tại Việt Nam. Mặc dù Wifi 6E đã phát hành từ năm 2021, tuy nhiên hiện nay số lượng thiết bị đầu cuối hỗ trợ cũng như các thiết bị phát sóng 6E còn hạn chế. Trong tất cả các địa điểm đo khảo sát mạng Wifi (phần II), nhóm tác giả đều chưa thấy xuất hiện tần số của Wifi 6E ở 6 GHz, do vậy nhóm tác giả chưa đề cập nghiên cứu trong bài báo này.

Theo Thông tư số 08/2021/TT-BTTTT ngày 14/10/2021 của Bộ Thông tin và Truyền thông quy định "Danh mục thiết bị vô tuyến điện được miễn giấy phép sử dụng tần số vô tuyến điện, điều kiện kỹ thuật và khai thác kèm theo", trong đó băng tần sử dụng cho mạng

BẢNG 1. THAM SỐ KỸ THUẬT CỦA MỘT SỐ TIÊU CHUẨN WIFI

Thế hệ tiêu chuẩn Wifi từ 2007 đến nay					
	Wifi 4	**Wifi 5**	**Wifi 6**	**Wifi 6E**	**Wifi 7**
Năm phát hành	2007	2013	2019	2021	2024
Tiêu chuẩn IEEE	802.11n	802.11ac	802.11ax		802.11 be
Tốc độ dữ liệu tối đa	1,2 Gbps	3,5 Gbps	9,6 Gbps		46 Gbps
Băng tần số	2,4 và 5 GHz	5 GHz	2,4 và 5 GHz	6 GHz	2,4 GHz, 5 GHz, 6 GHz và 7,25 GHz
Bảo mật	WPA2	WPA2	WPA3		WPA3
Băng thông	20, 40 MHz	20, 40, 80, 80+80, 160 MHz	20, 40, 80, 80+80, 160 MHz		Lên đến 320 MHz
Điều chế	64-QAM, OFDM	256-QAM, OFDM	1024-QAM, OFDMA		4096-QAM, OFDMA
Kiểu ăng-ten	4x4 MIMO	4x4 MIMO, DL MU-MIMO	8x8 MIMO, UL/DL MU-MIMO		16x16 MIMO, UL/DL MU-MIMO

Wifi là 2.4 GHz và 5 GHz được miễn giấy phép sử dụng [28].

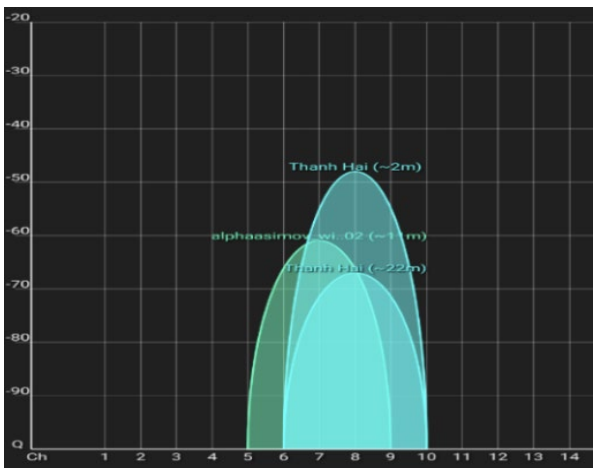
Cụ thể là băng tần số 2.4 GHz trong dải tần số từ 2400 đến 2483,5 MHz, băng tần số 5 GHz gồm 3 dải tần số sau: từ 5150 đến 5350 MHz, từ 5470 đến 5725 MHz và từ 5725 đến 5850 MHz. Do vậy, nhóm tác giả sử dụng thuật ngữ chung băng tần 2.4 GHz và 5 GHz đối với tín hiệu Wifi dưới 6 GHz trong nghiên cứu này.

II. MỘT SỐ KẾT QUẢ ĐO WIFI TẠI HÀ NỘI

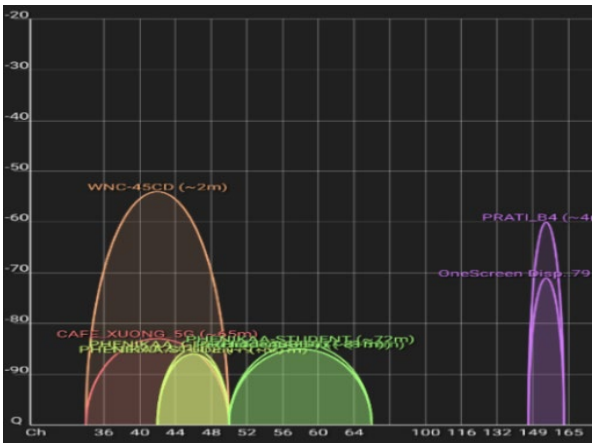
Để đánh giá phổ tần số và công suất tương đối của các băng tần Wifi hiện có, nhóm tác giả sử dụng ứng dụng phần mềm Wifi Analyzer mã nguồn mở [26, 27], cài đặt trên điện thoại 5G, các phần mềm NetSpot, Acrylic Analyzer, SignifiAgent cài đặt trên Laptop và đối chiếu kết quả với máy thu đo tín hiệu Oscor Green. Nhóm tác giả tiến hành đo kiểm tra ở một số địa diểm và thu được kết quả như hình 1, 2, 3.

Dựa vào kết quả đo được có thể đánh giá, hiện tại hầu hết sóng Wifi phổ biến đều hoạt động trong băng tần số là 2.4 GHz và 5 GHz. Công suất truyền của các thiết bị thu/phát thường nhỏ hơn 100 mW. Vì vậy, các phương pháp thực hiện chế áp Wifi sẽ tập trung vào băng tần 2.4 GHz và 5 GHz.

A. Kết quả đo tại Đại học Phenikka, Hà Đông



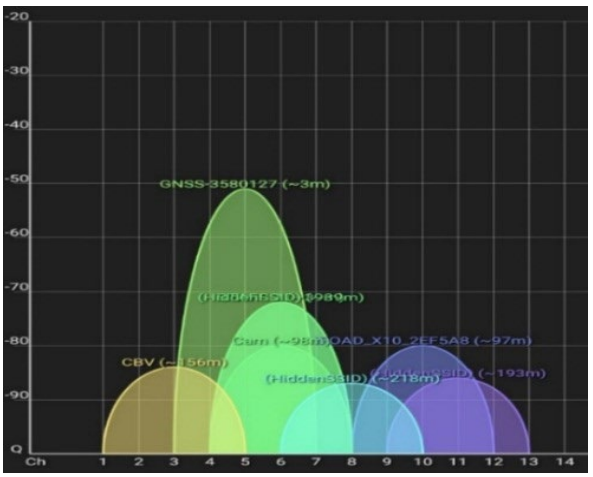
(a)



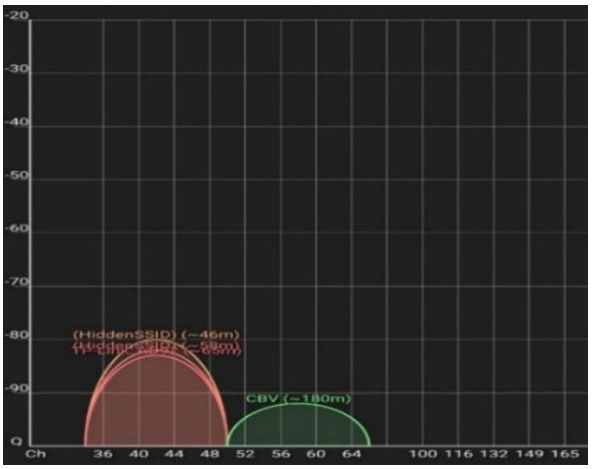
(b)

Hình 1. Băng 2.4 GHz tập trung ở kênh 6,7,8 (a) và băng 5 GHz tập trung ở kênh 44, 56, 150 (b)

B. Kết quả đo tại khu vực Sân vận động Mỹ Đình, Nam Từ Liêm



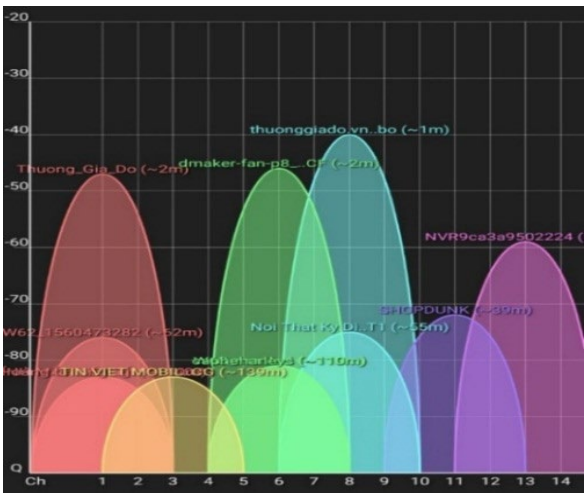
(a)



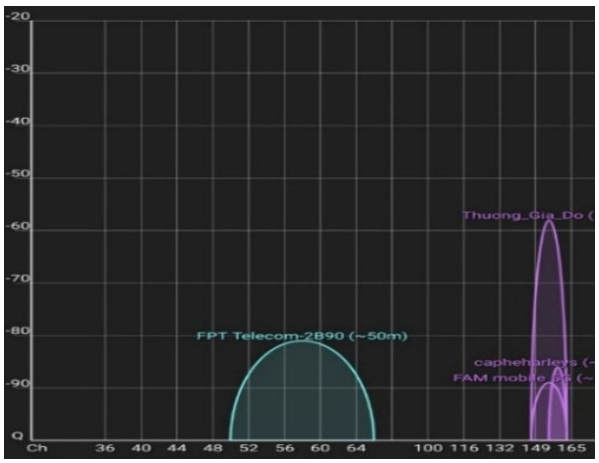
(b)

Hình 2. Băng 2.4 GHz tập trung ở kênh 5,6,10 (a) và băng 5 GHz tập trung ở kênh 44, 56 (b)

C. Kết quả đo tại Xuân Thuỷ, Cầu Giấy



(a)



(b)

Hình 3. Băng 2.4 GHz tập trung ở tất cả các kênh (a) và băng 5 GHz tập trung ở kênh 56, 150 (b)

Kết quả đo, kiểm tra các mạng Wifi tại một số địa điểm nêu trên không thể hiện tính phổ biến, chỉ nhằm phục vụ nghiên cứu thiết kế, chế tạo thiết bị chế áp tín hiệu Wifi, trước mắt thực hiện ở chế áp tần số dưới 6 HGz.

III. Một số nguy cơ và thách thức mất an toàn thông tin của việc lợi dụng Wifi

A. Nguy cơ

Những ưu điểm Wifi trong đời sống và công việc hàng ngày rất rõ ràng và thực tế. Tuy nhiên, công nghệ này đã bị kẻ xấu lợi dụng vào những hành vi vi phạm pháp luật và có xu hướng ngày càng gia tăng. Việc lợi dụng Wifi ở các khu vực bảo vệ, các sự kiện nhạy cảm để thực hiện các hành vi gây ảnh hưởng đến an ninh quốc gia, an toàn thông tin là rất lớn. Sóng Wifi là phương tiện được sử dụng để phát tán rộng rãi các thông tin ở khu vực bảo vệ các sự kiện nhạy cảm như tòa án, trụ sở cơ quan nhà nước, nơi diễn ra các hội nghị cấp cao, các sự kiện quốc tế, trong nước lớn,… Có thể kể ra một số nguy cơ chính sau:

- Việc lợi dụng sóng Wifi để điều khiển các thiết bị thu thập thông tin bất hợp pháp, có khả năng hoạt động trong phạm vi rộng mà ta khó nhận diện hoặc phát hiện tại những khu vực cần đảm bảo an ninh an toàn thông tin [16, 17].

- Wifi và bluetooth đều có thể được sử dụng để định vị vị trí tương đối chính xác, vì vậy những yếu nhân, những vị khách quan trọng của quốc gia,… có thể dễ dàng bị tấn công bởi các loại vũ khí công nghệ cao ở bất cứ vị trí nào và vào bất cứ thời điểm nào [18].

- Ngoài ra, có những thiết bị/phần mềm được cài đặt kết nối bộ định tuyến Wifi với điện thoại để điều khiển từ xa. Trong thời đại Internet vạn vật, nguy cơ sử dụng mạng Wifi để thực hiện những cuộc tấn công khủng bố mọi lúc mọi nơi là hoàn toàn có thể xảy ra và rất dễ dàng để thực hiện [19].

- Những hành vi mà các đối tượng có thể sử dụng là dùng các thiết bị thu phát, ghi âm, ghi hình có trang bị công nghệ Wifi để thu tin bất hợp pháp, có thể là lấy tin từ các cuộc họp, xâm phạm đời tư cá nhân hoặc gian lận trong các kỳ thi. Nhiều thiết bị thu, ghi lén sử dụng công nghệ Wifi đã được phát triển tới mức tinh vi, điểm nổi bật của các thiết bị siêu nhỏ này là có khả năng hoạt động độc lập có thể xem trên điện thoại và máy tính [20, 21].

- Trong lĩnh vực quốc phòng an ninh, các cơ quan đặc biệt nước ngoài sử dụng thiết bị đặc biệt thu, lợi dụng mạng Wifi để thực hiện thu thập thông tin của đối phương vẫn diễn ra dưới nhiều hình thức [22].

- Đặc biệt, trước sự bùng nổ của thiết bị bay không người lái hiện nay (TBBKNL), nguy cơ

gây mất an toàn an ninh đang bị đe dọa nghiêm trọng. Khoảng cách giữa TBBKNL với người điều khiển có thể lên đến hàng chục km, muốn chế áp ta phải xác định được vị trí của người điều khiển hoặc TBBKNL. Mặc dù TTBKNL cùng sử dụng các băng tần Wifi 2.4 GHz và 5 GHz, nhưng chế áp nó cần được thực hiện bằng giải pháp riêng. Trong khuôn khổ bài báo này, nhóm tác giả không đề cập đến phương pháp chế áp TBBKNL [23, 24].

B. Thách thức

Đảng, Nhà nước ta đã có nhiều chủ trương, chính sách đẩy mạnh nghiên cứu, ứng dụng, phát triển công nghệ bảo đảm quốc phòng, an ninh phục vụ phát triển kinh tế - xã hội. Nhiều chính sách, pháp luật được ban hành như: Luật An ninh mạng; Luật An toàn thông tin mạng; Luật Bảo vệ bí mật nhà nước và các văn bản hướng dẫn thi hành, các chủ trương về bảo vệ Tổ quốc trên không gian mạng. Một số thách thức đặt ra như sau [25]:

- An ninh quốc gia bị đe dọa khi sự phát triển của mạng xã hội đã tạo môi trường thuận lợi cho các hoạt động tác động, chuyển hóa chính trị, khủng bố trong và ngoài nước.

- Mất kiểm soát trên không gian mạng nếu không được kiểm soát chặt chẽ sẽ có thể gây ảnh hưởng nghiêm trọng đến mọi lĩnh vực trong xã hội.

- Đối mặt với các cuộc tấn công mạng quy mô lớn, gây thiệt hại nghiêm trọng.

- Các hệ thống thông tin quan trọng về an ninh quốc gia bị tấn công. Có thể phá hủy, gây đình trệ hoạt động của các lĩnh vực trọng yếu, thậm chí làm tê liệt các hoạt động của tổ chức, cơ quan.

C. Giải pháp an ninh, an toàn cho mạng Wifi

Có nhiều cách tiếp cận giải pháp bảo đảm an ninh, an toàn cho mạng Wifi nhằm phòng và chống các nguy cơ như đã trình bày trước đó, như tăng cường mật khẩu Wifi, sử dụng các bộ tường lửa, thường xuyên rà quét các lỗ hổng của bộ định tuyến, các thiết bị thu phát có đăng ký sử dụng hợp pháp, quản lý truy cập thông tin [29, 30]. Tuy nhiên, đó là các giải pháp được thực hiện thường xuyên, liên tục và chuyên biệt ở các khu vực cố định. Còn đối với các khu vực bảo vệ các sự kiện nhạy cảm, vị trí tạm thời không cố định, trong một khoảng thời gian không dài cần lựa chọn phương pháp chế áp liên tín hiệu Wifi phù hợp nhất. Do đó, đòi hỏi nghiên cứu tìm hiểu các phương pháp chế áp tín hiệu Wifi là yêu cầu cấp thiết.

IV. Cơ chế hoạt động của một số phương pháp chế áp wifi dưới 6 ghz

Chế áp Wifi được định nghĩa là làm gián đoạn truyền thông không dây bằng cách giảm tỷ lệ tín hiệu trên tạp âm ở phía máy thu thông qua việc phát các tín hiệu gây nhiễu. Đã có rất nhiều nghiên cứu đăng trên các tạp chí khoa học trên thế giới đề cập đến các phương pháp chế áp Wifi, có thể chia thành 2 nhóm như sau:

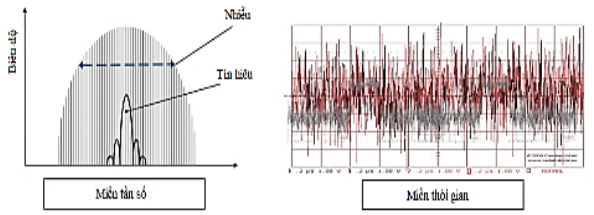
- *Nhóm 1. Phương pháp chế áp cơ bản:* Trong đó, có một số phương pháp phổ biến như chế áp liên tục, chế áp đánh lừa, chế áp ngẫu nhiên và chế áp phản ứng, chế áp bằng quét tần số,…

- *Nhóm 2. Phương pháp chế áp nâng cao:* Trong đó, tập trung vào các giải pháp chế áp riêng đối với một số giao thức xử lý tín hiệu của mạng Wifi.

A. Phương pháp chế áp cơ bản

1. Chế áp liên tục

Phương pháp này sử dụng thiết bị phát nhiễu công suất lớn chế áp tín hiệu Wifi mỗi khi hoạt động. Các cuộc tấn công chế áp liên tục không chỉ phá hủy khả năng nhận thông tin của thiết bị thu, bằng cách gây nhiễu công suất cao cho quá trình truyền dữ liệu mà còn ngăn thiết bị thu truy cập kênh bằng cách liên tục chiếm giữ kênh. Kiểu tấn công này tuy không hiệu quả về năng lượng và dễ phát hiện nhưng lại rất dễ phát động và có thể ngăn chặn toàn bộ liên lạc của các mạng Wifi trong phạm vi ảnh hưởng [3, 4].



Hình 4. Minh họa phương pháp chế áp liên tục

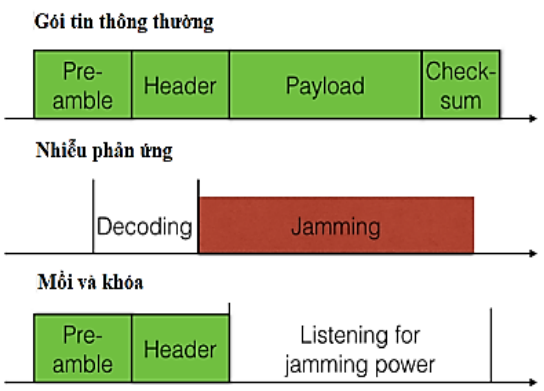
2. Chế áp ngẫu nhiên và chế áp định kỳ

Chế áp ngẫu nhiên là phương pháp chế áp mà thiết bị phát tín hiệu chế áp trong các khoảng thời gian ngẫu nhiên và chuyển sang trạng thái nghỉ trong thời gian còn lại. Trong khi đó, chế áp định kỳ là một biến thể của chế áp ngẫu nhiên, khi thiết bị chế áp phát tín hiệu và nghỉ trong một chu kỳ đặt trước.

Phương pháp chế áp này cho phép thiết bị chế áp tiết kiệm năng lượng hơn so với phương pháp chế áp liên tục. Tuy nhiên, nó kém hiệu quả hơn trong khả năng phá hoại so với phương pháp chế áp liên tục [6].

3. Chế áp phản ứng

Tấn công chế áp phản ứng còn được gọi là cuộc tấn công chế áp nhận biết kênh, trong đó thiết bị chế áp phát nhiễu vô tuyến mỗi khi phát hiện có các gói trao đổi thông tin được truyền trong mạng.



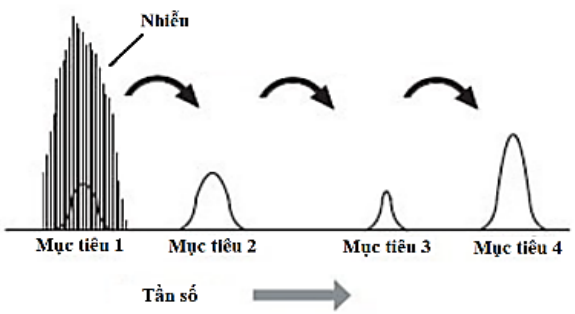
Hình 5. Chế áp phản ứng gây khó khăn cho việc đo mức công suất nhiễu

Chế áp phản ứng được coi là một chiến lược tấn công tiết kiệm năng lượng vì thiết bị chế áp chỉ hoạt động khi có truyền dữ liệu trong mạng. Tuy nhiên, phương pháp này yêu cầu các ràng buộc về thời gian rất chặt chẽ (ví dụ: dưới 1 ký tự OFDM, 4μs) để thực hiện nhiệm vụ trong thực tế vì nó cần phải chuyển từ chế độ nghe sang chế độ phát nhiễu một cách nhanh chóng [7].

4. Chế áp quét tần số

Trong liên lạc vô tuyến, có nhiều kênh được sử dụng cho liên lạc Wifi trên các băng tần ISM.

Đối với một thiết bị chế áp chi phí thấp, nó bị hạn chế bởi mạch phần cứng của thiết bị (ví dụ: tốc độ lấy mẫu ADC rất cao và bộ khuếch đại công suất băng thông rộng) để tấn công đồng thời một lượng lớn các kênh. Các cuộc tấn công chế áp quét tần số đã được đề xuất để khắc phục hạn chế này, sao cho thiết bị chế áp có thể nhanh chóng chuyển đổi (ví dụ: trong phạm vi 10 μs) sang các kênh khác nhau [8].

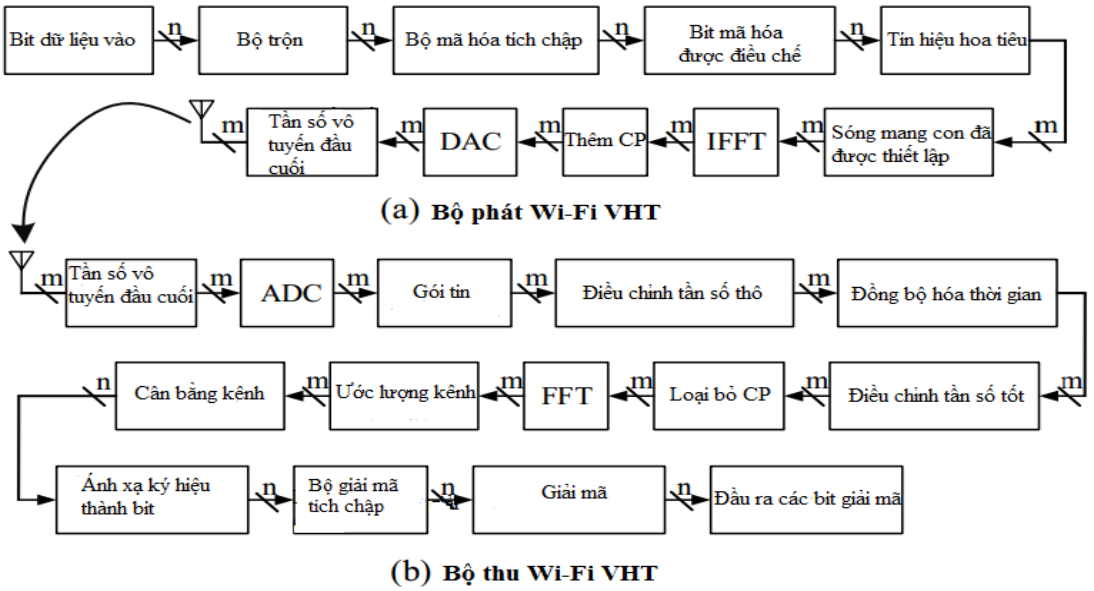


Hình 6. Minh họa chế áp quét tần số

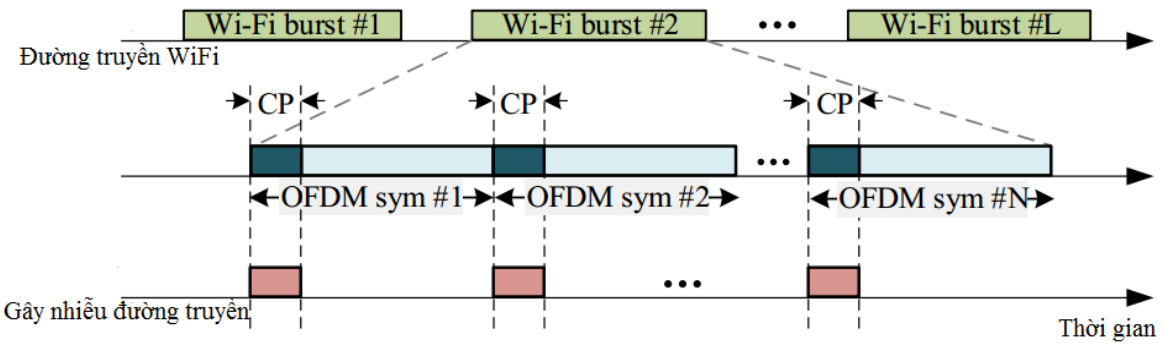
B. Phương pháp chế áp nâng cao

1. Chế áp quá trình đồng bộ hóa thời gian hoặc tần số

Hình 7 mô tả quá trình xử lý tín hiệu băng cơ sở cho một bộ thu phát Wifi 802.11, trong đó đồng bộ hóa thời gian là một khâu quan trọng của bộ thu Wifi để giải mã gói dữ liệu. Các phương pháp chế áp khác nhau đã được nghiên cứu nhằm ngăn cản sự thu thập định thời tín hiệu và làm gián đoạn thủ tục phát hiện phần mở đầu của gói tin, chẳng hạn như tấn công làm giả phần mở đầu, tấn công vô hiệu hóa phần mở đầu và tấn công làm biến dạng phần mở đầu [9-11].



Hình 7. Sơ đồ xử lý tín hiệu băng cơ sở cho một bộ phát (a) thu (b) Wifi 802.11 [12] ($n \leq 4$ và $m \leq 8$)



Hình 8. Gây nhiễu vào tiền tố tuần hoàn (CP) [13]

Đối với bộ thu Wifi, độ lệch tần số sóng mang có thể khiến các sóng mang con lệch khỏi tính trực giao lẫn nhau, dẫn đến nhiễu liên kênh và suy giảm tỷ số tín trên tạp. Ngoài ra, độ lệch tần số sóng mang có thể gây ra độ lệch pha không mong muốn cho các tín hiệu được điều chế, do đó làm giảm hiệu suất giải điều chế tín hiệu. Trong giao tiếp Wifi, độ lệch tần số được ước tính bằng cách so sánh tín hiệu mở đầu nhận được trong miền thời gian. Do đó, các phương pháp chế áp phần mở đầu sử dụng để ngăn đồng bộ hóa thời gian cũng có thể được dùng để phá hủy các chức năng hiệu chỉnh bù tần số.

2. Chế áp vào ước tính kênh

Như thể hiện trong Hình 7, ước tính kênh và cân bằng kênh là các mô-đun cần thiết cho bộ thu Wifi. Bất kỳ sự cố nào trong hoạt động của chúng đều có thể dẫn đến kết quả giải mã khung bị sai. Bộ thu Wifi sử dụng chuỗi mở đầu ở miền tần số nhận được để ước tính đáp ứng tần số kênh của mỗi sóng mang con. Một phương pháp tự nhiên để tấn công các mô-đun ước tính kênh và cân bằng kênh là can thiệp vào tín hiệu mở đầu.

3. Chế áp vào tiền tố tuần hoàn CP (Cyclic Prefix)

Hầu hết các hệ thống truyền thông không dây đều sử dụng điều chế ghép kênh phân chia theo tần số trực giao OFDM (Orthogonal Frequency Division Multiplexing) ở lớp vật lý và mọi ký hiệu OFDM đều có CP. Hình 8 trình bày phương pháp chế áp vào CP. Các nhà nghiên cứu đã chỉ ra rằng chế áp CP là một cách

tiếp cận khả thi và hiệu quả để phá vỡ bất kỳ giao tiếp OFDM như là Wifi. Lỗi CP có thể làm sai lệch đầu ra của bộ cân bằng kênh tuyến tính. Hơn nữa, các nhà nghiên cứu cũng chỉ ra rằng chế áp CP tiết kiệm hơn 80% năng lượng so với chế áp liên tục để kéo đường truyền Wifi xuống [13]. Tuy nhiên, chế áp trên CP rất khó thực hiện vì nó yêu cầu thiết bị chế áp phải ước tính chính xác thời gian truyền mạng [9].

4. Chế áp vào quá trình tạo chùm tia MU-MIMO (Multi User-Multiple Input and Multiple Output)

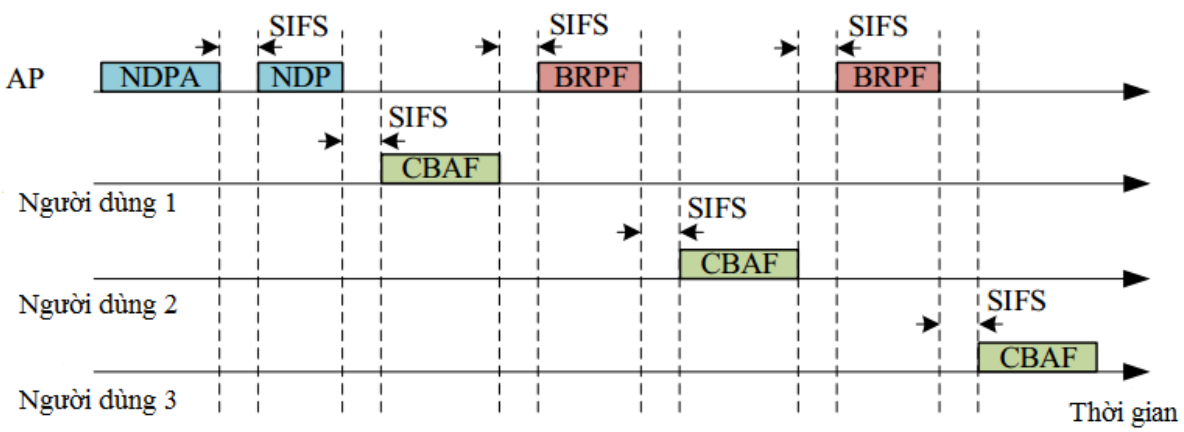
Do sự bất đối xứng của cấu hình ăng-ten tại một điểm truy cập và các thiết bị khách mà nó phục vụ trong mạng Wifi, gần đây các công nghệ Wifi (ví dụ: IEEE 802.11ac và IEEE 802.11ax) hỗ trợ nhiều thiết bị truyền MIMO (MU-MIMO) trong đường xuống của chúng, trong đó một điểm truy cập nhiều ăng-ten có thể phục vụ đồng thời nhiều người dùng một ăng-ten (hoặc nhiều ăng-ten) bằng cách sử dụng kỹ thuật tạo chùm tia [2].

Để thiết kế bộ tiền mã hóa tạo chùm tia (hay còn gọi là ma trận tạo chùm tia), yêu cầu điểm truy cập Wifi phải xác định được số lượng các kênh giữa các ăng-ten của nó và tất cả người dùng. Theo tiêu chuẩn IEEE 802.11ac, quy trình xác định kênh trong truyền thông Wifi VHT được quy định theo ba bước sau: Đầu tiên, điểm truy cập phát một gói tin tới các thiết bị trong mạng. Thứ hai, mỗi thiết bị sẽ tính toán xác định kênh của mình thông qua gói tin nhận được. Thứ ba, mỗi thiết bị trong mạng thông báo kết quả ước tính kênh của nó cho điểm truy cập.

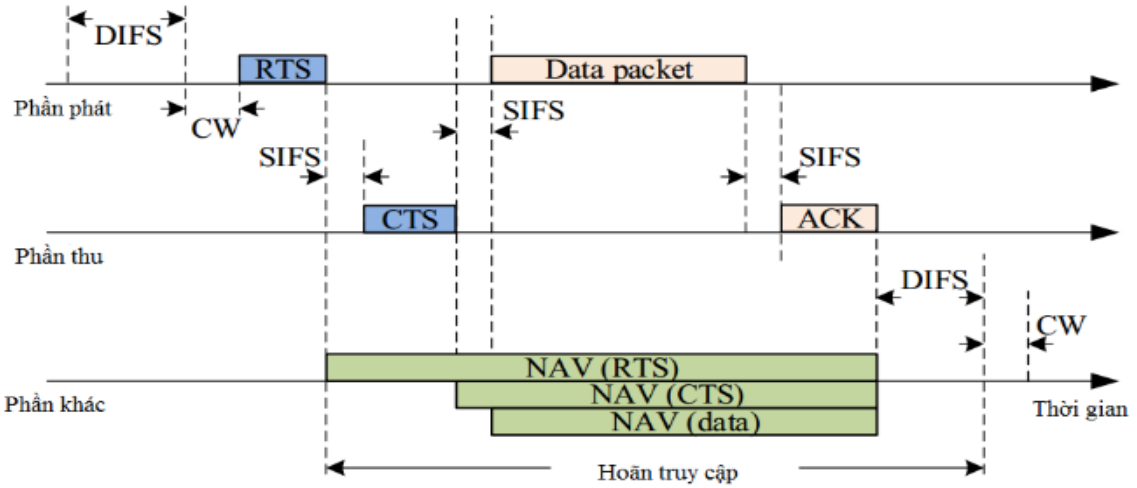
Hình 9 cho thấy giao thức tạo chùm tin trong mạng Wifi VHT. Điểm truy cập AP (Access Point) phát một gói thông báo (NDPA) để chuẩn bị kênh cho các quá trình tạo chùm và định kênh. Sau tín hiệu NDPA, AP phát một gói dữ liệu rỗng (NDP) dưới dạng gói thông báo. Thiết bị trong mạng sử dụng phần mở đầu được truyền trong NDP để tính toán đáp ứng tần số kênh trên mỗi sóng mang phụ. Sau đó, kỹ thuật xoay Givens thường được sử dụng, trong đó một loạt các gói được gửi trở lại AP dưới dạng khung hành động tạo chùm nén (CBAF), thay vì ma trận kênh ước tính ban đầu. AP sử dụng khung thăm dò báo cáo định dạng chùm (BRPF) để quản lý việc truyền báo cáo giữa những người dùng.

5. Chế áp vào giao thức MAC (Media Access Control)

Một loạt các phương pháp chế áp lớp MAC, còn được gọi là các phương pháp chế áp thông minh [14, 15] nhằm mục đích làm giảm hiệu suất của giao tiếp Wifi. Mục tiêu chính của các phương pháp chế áp thông minh là làm hỏng các gói điều khiển như gói CTS (Clear To Send) và ACK (Acknowledgement) được sử dụng bởi giao thức MAC Wifi (Hình 10).



Hình 9. Giao thức tạo chùm tin trong mạng Wifi 802.11 VHT



Hình 10. Giao thức RTS/CTS trong mạng Wifi 802.11 [12]

Đối với cuộc tấn công CTS, bộ chế áp chờ cho đến khi gói RTS (Request To Send) được truyền bởi một thiết bị đang hoạt động, đợi một khe thời gian SIFS từ khi kết thúc RTS và làm kẹt gói CTS. Không giải mã được gói CTS đơn giản là dừng truyền dữ liệu. Chế áp truyền gói ACK cũng tương tự như vậy. Khi bộ phát không thể nhận gói ACK, nó sẽ truyền lại gói dữ liệu. Quá trình truyền lại tiếp tục cho đến khi đạt đến giới hạn TCP hoặc lệnh hủy bỏ được đưa ra. Chế áp thông minh cũng có thể nhắm mục tiêu tới gói dữ liệu, nơi bộ chế áp phát hiện RTS và CTS và gửi tín hiệu gây nhiễu theo một khe thời gian SIFS.

Ngoài ra, các cuộc chế áp lớp MAC có thể được thiết kế để giữ cho thiết bị luôn bận, ngăn các thiết bị khác truy cập vào kênh bằng cách gửi gói RTS giả để chiếm kênh trong thời gian dài nhất có thể [16].

C. Đánh giá

1. Phương pháp chế áp nâng cao

Các phương pháp chế áp nâng cao tương đối phức tạp, đòi hỏi các kiến thức chuyên sâu về cấu trúc lõi của lớp MAC và lớp vật lý cũng như phương thức truyền nhận tín hiệu của thiết bị thu phát Wifi. Tuy nhiên, hiệu quả của các phương pháp này lại không cao, không thể đồng thời chế áp toàn bộ các thiết bị thu phát sử dụng băng tần Wifi trong một khu vực rộng lớn. Việc nghiên cứu các phương pháp chế áp nâng cao sẽ là một trong các định hướng nghiên cứu chuyên sâu khác, phục vụ cho mục tiêu đa dạng hóa sản phẩm chế áp, phù hợp với các địa điểm bảo đảm an ninh, an toàn thông tin khác.

2. Phương pháp chế áp cơ bản

Phương pháp này không yêu cầu người sử dụng có hiểu biết sâu về mạng Wifi. Trong số đó, chế áp liên tục là một phương pháp chế áp khả thi và hiệu quả hơn cả, thiết bị chế áp phát nhiễu công suất lớn, không đổi tần số khi hoạt động. Lý do phương pháp này tối ưu nhất đó là thời gian triển khai ngắn, hiệu quả chế áp có thể đạt 100% trong phạm vi phủ sóng chế áp, đảm bảo an ninh, an toàn, ngăn chặn toàn bộ việc phát tán, thu thập thông tin, kiểu chế áp này dễ phát động và có thể làm hỏng quá trình liên lạc của mạng đến mức chặn toàn bộ liên lạc trong phạm vi ảnh hưởng mỗi khi hoạt động.

3. Lựa chọn phương pháp

Trên thị trường hiện nay, các thiết bị chế áp sóng vô tuyến nói chung và thiết bị chế áp Wifi nói riêng hầu hết đều sử dụng phương pháp chế áp liên tục để hoạt động. Dựa trên nguyên lý vận hành đơn giản, chế áp liên tục mang lại độ tin cậy và hiệu quả cao, đây chính là phương pháp phù hợp nhất với mục đích bảo đảm an

ninh, an toàn thông tin cho các khu vực bảo vệ sự kiện nhạy cảm, thời gian hoạt động ngắn, địa điểm chế áp cơ động, phạm vi chế áp phụ thuộc vào yêu cầu, triển khai trong thực tế nhanh, không cần cài đặt hệ thống phức tạp, quá trình vận hành, bảo dưỡng, sửa chữa thiết bị đơn giản và đạt yêu cầu công tác.

V. KẾT LUẬN

Nghiên cứu được nhóm tác giả thực hiện nhằm tìm hiểu các tiêu chuẩn 802.11 hiện đang sử dụng cho mạng Wifi và thời gian sắp tới. Nhóm tác giả đã trình bày một số nguy cơ và thách thức mà Wifi, bluetooth và các thiết bị thu phát khác (sử dụng chung băng tần 2.4 GHz và 5 GHz) có thể bị lợi dụng nhằm mục đích thực hiện các hành vi vi phạm pháp luật, gây mất an toàn, an ninh cho các cá nhân và tổ chức tại khu vực bảo vệ sự kiện nhạy cảm. Từ đó tìm hiểu cơ chế hoạt động của một số phương pháp chế áp tín hiệu Wifi tiêu chuẩn IEEE 802.11 dưới 6 GHz. Qua thực tiễn nghiên cứu công nghệ, thiết kế chế tạo các các sản phẩm chế áp vô tuyến phục vụ công tác công an trong các các sự kiện lớn của đất nước diễn ra từ trước đến nay, nhóm tác giả đã đề xuất phương pháp chế áp liên tục tín hiệu Wifi là phù hợp nhất, khả thi trong thực tế, và cũng đã được hầu hết các lực lượng bảo vệ an ninh trên thế giới sử dụng.

Nhóm tác giả cùng các đồng nghiệp tại Viện Khoa học và công nghệ, Bộ Công an đã xây dựng, hoàn thiện và tham mưu cho lãnh đạo Bộ Công an ký ban hành Tiêu chuẩn cơ sở trong lĩnh vực an ninh số 102:2022/BCA năm 2022 đối với thiết bị chế áp sóng Wifi băng tần số 2.4 GHz công suất nhỏ dưới 3W dùng để áp dụng trang bị đối với các phòng họp nhỏ. Thiết bị chế áp tín hiệu Wifi băng tần số 2.4GHz công suất nhỏ đã được nhóm tác giả hoàn thiện và triển khai thực tế tại một số phòng họp ở công an tỉnh và địa phương.

Hướng nghiên cứu tiếp theo của nhóm tác giả là hoàn thiện thiết bị chế áp tín hiệu Wifi tiêu chuẩn IEEE 802.11 dưới 6 GHz và đón đầu tiêu chuẩn Wifi 6E và Wifi 7.

TÀI LIỆU THAM KHẢO

[1]. IEEE standard for information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks-specific requirements - part 11, (2013). Wireless LAN medium access control (MAC) and physical layer (PHY) specifications - Amendment 4: Enhancements for very high throughput for operation in bands below 6 GHz, *IEEE Std 802.11ac(TM)*, pp. 1–425.

[2]. K. Grover, A. Lim, and Q. Yang, (2014) Jamming and anti-jamming techniques in wireless networks: a survey, *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 17, no. 4, pp. 197–215.

[3]. K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, (2010), Denial of service attacks in wireless networks: The case of jammers, *IEEE Communications surveys & tutorials*, vol. 13, no. 2, pp. 245–257.

[4]. I. Broustis, K. Pelechrinis, D. Syrivelis, S. V. Krishnamurthy, and L. Tassiulas, (2009), FIJI: Fighting implicit jamming in 802.11 WLANs, *Proceedings of International Conference on Security and Privacy in Communication Systems*, pp. 21–40, Springer.

[5]. E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, (2013), Performance of IEEE 802.11 under jamming, *Mobile Networks and Applications*, vol. 18, no. 5, pp. 678–696.

[6]. Y. Cai, K. Pelechrinis, X. Wang, P. Krishnamurthy, and Y. Mo, (2013), Joint reactive jammer detection and localization in an enterprise Wifi network, *Computer Networks*, vol. 57, no. 18, pp. 3799–3811.

[7]. S. Bandaru, (2014), Investigating the effect of jamming attacks on wireless LANs, *International Journal of Computer Applications*, vol. 99, no. 14, pp. 5–9.

[8]. C. Shahriar, M. La Pan, M. Lichtman, T. C. Clancy, R. McGwier, R. Tandon, S. Sodagari, and J. H. Reed, (2014), PHY-layer resiliency in OFDM communications: A tutorial, *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 292–314.

[9]. M. J. La Pan, T. C. Clancy, and R. W. McGwier, (2012), Jamming attacks against OFDM timing synchronization and signal acquisition, *Proceedings of IEEE Military Communications Conference (MILCOM)*, pp. 1–7.

[10]. M. J. La Pan, T. C. Clancy, and R. W. McGwier, (2016), Physical layer orthogonal frequency-division multiplexing acquisition and timing synchronization security, *Wireless Communications and Mobile Computing*, vol. 16, no. 2, pp. 177–191.

[11]. E. Perahia and R. Stacey, (2013), Next generation wireless LANs: 802.11n and 802.11ac. *Cambridge university press*.

[12]. A. L. Scott, (2011), Effects of cyclic prefix jamming versus noise jamming in OFDM signals, *Air Force Institute of Technology Graduate School of Engineering and Management*.

[13]. D. Thuente and M. Acharya, (2006), Intelligent jamming in wireless networks with applications to 802.11b and other networks, *Proceedings of IEEE Military Communications Conference (MILCOM)*, vol. 6, p. 100.

[14]. M. Acharya, T. Sharma, D. Thuente, and D. Sizemore, (2004), Intelligent jamming in 802.11b wireless networks, *Proceedings of OPNETWORK*. Washington DC, USA: OPNET.

[15]. R. Negi and A. Rajeswaran, (2005), DoS analysis of reservation based MAC protocols, *Proceedings of IEEE International Conference on Communications (ICC)*, vol. 5, pp. 3632–3636.

[16]. Lunox, Đánh cắp thông tin qua Wifi – Evil Twin", https://codelearn.io/sharing/danh-cap-thong-tin-qua-wifi-evil-twin.

[17]. Philip Bates, "5 Ways Hackers Use Public Wi-Fi to Steal Your Identity", https://www.makeuseof.com/tag/5-ways-hackers-can-use-public-wi-fi-steal-identity/.

[18]. A.S. Ja'afar, N.M.Z. Hashim, A.A.M. Isa, N.A. Ali#4, A.M. Darsono. (8/2013), Analysis of indoor location and positioning via wi-fi signals at FKEKK, UTeM, *International Journal of Engineering and Technology,* 5(4): 3570-3579.

[19]. Krishi Chowdhary, "How to Spy on Devices Connected to My Wifi | Top 10 Wifi Spy Apps Reviewed",https://www.techopedia.com/spy/how-to-spy-on-devices-connected-to-my-wifi.

[20]. Lê Nam, "Thiết bị gian lận thi cử, rao bán tràn lan trên chợ ảo", https://kinhtedothi.vn/thiet-bi-gian-lan-thi-cu-rao-ban-tran-lan-tren-cho-ao.html.

[21]. Brian F., "Best Hidden Recording Devices For 2023", https://spycentre.com/blogs/news/top-5-hidden-voice-recorders-of-2017-review.

[22]. Privacyinternational.org, "Communications Surveillance", https://privacyinternational.org/explainer/1309/communications-surveillance.

[23]. C. S. Liang, "Terrorist Digitalis: Preventing Terrorists from Using Emerging Technologies", https://www.gcsp.ch/publications/terrorist-digitalis-preventing-terrorists-using-emerging-technologies.

[24]. Measuring the Impact of Terrorism, (2023), GLOBAL TERRORISM INDEX 2023, *Istitute for Economics & Peace.*

[25]. GS. TS. Tô Lâm, (2020), Đảm bảo an ninh mạng trong tình hình mới, Tạp chí Cộng sản.

[26]. www.github.com/noohkvm/meterview.

[27]. https://github.com/jjoe64/GraphView/wiki.

[28].Chinhphu.vn, "Thông tư số 08/2021/TT-BTTTT của Bộ Thông tin và Truyền thông: Quy định Danh mục thiết bị vô tuyến điện được miễn giấy phép sử dụng tần số vô tuyến điện, điều kiện kỹ thuật và khai thác kèm theo", https://vanban.chinhphu.vn/default.aspx?pageid=27160&docid=204286.

[29]. Hung, N. V., Mai, Đang T., & Tung, N. T. (2023). Network attack classification framework based on Autoencoder model and online stream analysis technology. *Journal of Science and Technology on Information Security*, *1*(18), 3-19, https://doi.org/10.54654/isj.v1i18.938.

[30]. Khanh, T. V., Tu, N. V., & Ho, T. P. . (2022). Some issues about upgrading and developing high-speed local IP network encryption devices. *Journal of Science and Technology on Information Security*, 1(15), 46-55, https://doi.org/10.54654/isj.v1i15.838.

SƠ LƯỢC VỀ TÁC GIẢ

Lê Hải Triều

Đơn vị công tác: Phòng Kỹ thuật điện tử nghiệp vụ, Viện Khoa học và công nghệ, Bộ Công an.

Email: lht295@gmail.com

Quá trình đào tạo: Tốt nghiệp Học viện Kỹ thuật quân sự năm 1996; Tốt nghiệp Thạc sĩ năm 2004; Tiến sĩ chuyên ngành Kỹ thuật viễn thông năm 2019.

Hướng nghiên cứu hiện nay: Thiết kế, chế tạo các thiết bị nghe nhìn nghiệp vụ, chế áp thông tin vô tuyến công suất vừa và nhỏ; phát hiện và chế áp thiết bị bay không người lái; công nghệ sinh trắc học; trí tuệ nhân tạo.

Trương Chí Kiên

Đơn vị công tác: Phòng Kỹ thuật điện tử nghiệp vụ, Viện Khoa học và công nghệ, Bộ Công an.

Email: kientc82@gmail.com

Quá trình đào tạo: Tốt nghiệp Thạc sĩ chuyên ngành Kỹ thuật điều khiển và tự động hóa tại Học viện Kỹ thuật quân sự năm 2017.

Hướng nghiên cứu hiện nay: Thiết kế, chế tạo các thiết bị thu phát nghiệp vụ, chế áp thông tin vô tuyến công suất nhỏ.

Ngô Thu Hiền

Đơn vị công tác: Phòng Kỹ thuật điện tử nghiệp vụ, Viện Khoa học và công nghệ, Bộ Công an.

Email: hiennt1611@gmail.com

Quá trình đào tạo: Tốt nghiệp Thạc sĩ chuyên ngành Kỹ thuật viễn thông tại Đại học Giao thông vận tải năm 2022.

Hướng nghiên cứu hiện nay: Thiết kế, chế tạo các thiết bị thu phát, nghe nhìn nghiệp vụ, chế áp thông tin vô tuyến công suất nhỏ.