



(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) Cộng hòa xã hội chủ nghĩa Việt Nam (VN) (11) CỤC SỞ HỮU TRÍ TUỆ



1-0048350

(51)^{2021.01} H04L 29/06; H04B 7/06; H04W 52/52; (13) B
H04W 12/03; H04W 12/041; H04B
7/0413

(21) 1-2022-01476 (22) 01/09/2020
(86) PCT/US2020/048923 01/09/2020 (87) WO 2021/061355 A1 01/04/2021
(30) 16/583,005 25/09/2019 US
(45) 25/07/2025 448 (43) 25/07/2022 412A
(73) QUALCOMM INCORPORATED (US)
ATTN: International IP Administration 5775 Morehouse Drive San Diego, California
92121-1714 (US)
(72) YUNUSOV, David (IL); TOUBOUL, Assaf (IL); KUTZ, Gideon Shlomo (IL);
LANDIS, Shay (IL).
(74) Công ty TNHH Quốc tế D & N (D&N INTERNATIONAL CO.,LTD.)

(54) PHƯƠNG PHÁP, THIẾT BỊ KHÔNG DÂY, VÀ MÁY TRUYỀN THÔNG KHÔNG
DÂY VÀ PHƯƠNG TIỆN BẮT BIẾN ĐỌC ĐƯỢC BẰNG MÁY TÍNH

(21) 1-2022-01476

(57) Nói chung một số khía cạnh của sáng chế đề cập đến phương pháp, máy, thiết bị không dây để truyền thông không dây và phương tiện bất biến đọc được bằng máy tính. Theo một số khía cạnh, thiết bị không dây có thể nhận tín hiệu được điều hướng chùm từ thiết bị truyền. Thiết bị không dây có thể ước lượng tổng có trọng số dựa ít nhất một phần vào một hoặc nhiều hệ số liên quan đến các khiếm khuyết gắn với thiết bị truyền, vị trí không gian của thiết bị không dây, và/hoặc tương tự. Thiết bị không dây có thể xác định khóa mật mã dựa ít nhất một phần vào tỷ lệ giữa nhiều hệ số trong tổng có trọng số, và một hoặc nhiều cuộc truyền thông giữa thiết bị không dây và thiết bị truyền có thể được bảo mật dựa trên khóa mật mã. Sáng chế còn đề cập đến rất nhiều khía cạnh khác.

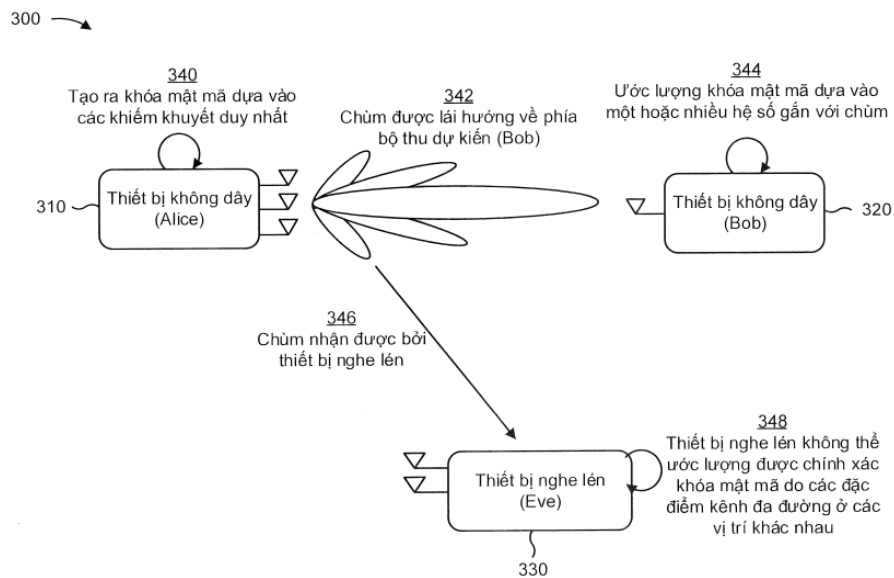


Fig.3

Lĩnh vực kỹ thuật được đề cập

Nói chung, các khía cạnh của sáng chế đề cập đến truyền thông không dây và đến các kỹ thuật và máy lấy dấu hiệu đặc trưng lớp vật lý dựa trên khiếm khuyết. Một số kỹ thuật và thiết bị được mô tả ở đây có thể sử dụng dấu hiệu đặc trưng lớp vật lý dựa trên khiếm khuyết và/hoặc một hoặc nhiều đặc điểm kênh đa đường nhiều đầu ra nhiều đầu vào (multiple input multiple output - MIMO) để tạo ra khóa mật mã mà không được dùng chung trong phiên trao đổi khóa.

Tình trạng kỹ thuật của sáng chế

Các hệ thống truyền thông không dây được triển khai rộng rãi để cung cấp các dịch vụ viễn thông khác nhau chẳng hạn như điện thoại, video, dữ liệu, gửi tin nhắn và phát rộng. Các hệ thống truyền thông không dây thông thường có thể sử dụng các công nghệ đa truy cập có khả năng hỗ trợ truyền thông với nhiều người dùng bằng cách dùng chung các tài nguyên hệ thống sẵn có (chẳng hạn, băng thông, công suất phát, và/hoặc tương tự). Ví dụ về các công nghệ đa truy cập như vậy bao gồm các hệ thống đa truy cập phân chia theo mã (code division multiple access - CDMA), các hệ thống đa truy cập phân chia theo thời gian (time division multiple access - TDMA), các hệ thống đa truy cập phân chia theo tần số (frequency division multiple access - FDMA), các hệ thống đa truy cập phân chia theo tần số trực giao (orthogonal frequency division multiple access - OFDMA), các hệ thống đa truy cập phân chia theo tần số một sóng mang (single-carrier frequency divisional multiple access - SC-FDMA), các hệ thống đa truy cập phân chia theo mã đồng bộ phân chia theo thời gian (time division synchronous code division multiple access - TD-SCDMA), và hệ thống phát triển dài hạn (Long Term Evolution - LTE). LTE/LTE cải tiến là tập hợp các cải tiến đối với chuẩn di động Hệ thống Viễn thông Di động Toàn cầu (Universal Mobile Telecommunications System - UMTS) được ban hành bởi Dự án Đối tác Thế hệ Thứ ba (Third Generation Partnership Project - 3GPP).

Mạng truyền thông không dây có thể bao gồm một số trạm gốc (base station - BS) mà có thể hỗ trợ truyền thông cho một số thiết bị người dùng (user equipment - UE). UE có thể truyền thông với BS qua đường xuống và đường lên. Đường xuống (hay liên kết xuôi) chỉ liên kết truyền thông từ BS đến UE, và đường lên (hay liên kết ngược) chỉ liên

kết truyền thông từ UE đến BS. Như sẽ được mô tả chi tiết hơn dưới đây, BS có thể được gọi là Nút B, gNB, điểm truy cập (access point - AP), đầu vô tuyến, điểm thu phát (transmit receive point - TRP), BS vô tuyến mới (new radio - NR), nút B 5G, và/hoặc các thuật ngữ tương tự.

Các công nghệ đa truy cập trên đây đã được ứng dụng trong các chuẩn viễn thông khác nhau để cung cấp một giao thức chung mà cho phép các thiết bị người dùng khác nhau truyền thông ở mức thành phố, quốc gia, khu vực và thậm chí toàn cầu. Vô tuyến mới (New radio - NR), còn được gọi là 5G, là tập hợp các cải tiến của chuẩn di động LTE được ban hành bởi Dự án Đối tác Thế hệ Thứ ba (3GPP). NR được thiết kế để hỗ trợ tốt hơn cho truy cập Internet băng rộng di động bằng cách cải tiến hiệu quả phổ, giảm chi phí, cải thiện các dịch vụ, sử dụng phổ mới, và tích hợp tốt hơn với các chuẩn mở khác bằng cách sử dụng kỹ thuật ghép kênh phân chia theo tần số trực giao (orthogonal frequency division multiplexing - OFDM) có tiền tố vòng (cyclic prefix - CP) (CP-OFDM) trên đường xuống (downlink - DL), sử dụng CP-OFDM và/hoặc SC-FDM (ví dụ, còn gọi là OFDM trải trên biến đổi Fourier rời rạc (discrete Fourier transform spread OFDM - DFT-s-OFDM) trên đường lên (uplink - UL), cũng như hỗ trợ điều hướng chùm sóng, công nghệ anten nhiều đầu vào nhiều đầu ra (multiple-input multiple-output - MIMO) và gộp sóng mang. Tuy nhiên, do nhu cầu truy cập băng rộng di động tiếp tục tăng, nên cần cải tiến thêm công nghệ LTE và NR. Tốt hơn là, các cải tiến này nên ứng dụng được cho nhiều công nghệ đa truy cập và các chuẩn viễn thông mà có sử dụng các công nghệ này.

Bản chất kỹ thuật của sáng chế

Theo một số khía cạnh, sáng chế đề xuất phương pháp truyền thông không dây, được thực hiện bởi thiết bị không dây, có thể bao gồm các bước: nhận tín hiệu được điều hướng chùm từ thiết bị truyền; ước lượng tổng có trọng số dựa ít nhất một phần vào nhiều hệ số kết hợp với tín hiệu được điều hướng chùm, trong đó nhiều hệ số bao gồm một hoặc nhiều hệ số liên quan đến một hoặc nhiều khiếm khuyết gắn với thiết bị truyền và một hoặc nhiều hệ số phụ thuộc vào vị trí không gian của thiết bị không dây; xác định khóa mật mã dựa ít nhất một phần vào tỷ lệ giữa nhiều hệ số trong tổng có trọng số kết hợp với tín hiệu được điều hướng chùm; và bảo mật một hoặc nhiều cuộc truyền thông giữa thiết bị không dây và thiết bị truyền dựa ít nhất một phần vào khóa mật mã.

Theo một số khía cạnh, sáng chế đề xuất thiết bị không dây để truyền thông không dây có thể bao gồm bộ nhớ và một hoặc nhiều bộ xử lý nối với bộ nhớ. Bộ nhớ và một

hoặc nhiều bộ xử lý có thể được tạo cấu hình để: nhận tín hiệu được điều hướng chùm từ thiết bị truyền; ước lượng tổng có trọng số dựa ít nhất một phần vào nhiều hệ số kết hợp với tín hiệu được điều hướng chùm, trong đó nhiều hệ số bao gồm một hoặc nhiều hệ số liên quan đến một hoặc nhiều khiếm khuyết gắn với thiết bị truyền và một hoặc nhiều hệ số phụ thuộc vào vị trí không gian của thiết bị không dây; xác định khóa mật mã dựa ít nhất một phần vào tỷ lệ giữa nhiều hệ số trong tổng có trọng số kết hợp với tín hiệu được điều hướng chùm; và bảo mật một hoặc nhiều cuộc truyền thông giữa thiết bị không dây và thiết bị truyền dựa ít nhất một phần vào khóa mật mã.

Theo một số khía cạnh, sáng chế đề xuất phương tiện bất biến đọc được bằng máy tính có thể lưu trữ một hoặc nhiều lệnh để truyền thông không dây. Một hoặc nhiều lệnh, khi được thực thi bởi một hoặc nhiều bộ xử lý của thiết bị không dây, có thể khiến cho một hoặc nhiều bộ xử lý: nhận tín hiệu được điều hướng chùm từ thiết bị truyền; ước lượng tổng có trọng số dựa ít nhất một phần vào nhiều hệ số kết hợp với tín hiệu được điều hướng chùm, trong đó nhiều hệ số bao gồm một hoặc nhiều hệ số liên quan đến một hoặc nhiều khiếm khuyết gắn với thiết bị truyền và một hoặc nhiều hệ số phụ thuộc vào vị trí không gian của thiết bị không dây; xác định khóa mật mã dựa ít nhất một phần vào tỷ lệ giữa nhiều hệ số trong tổng có trọng số được kết hợp với tín hiệu được điều hướng chùm; và bảo mật một hoặc nhiều cuộc truyền thông giữa thiết bị không dây và thiết bị truyền dựa ít nhất một phần vào khóa mật mã.

Theo một số khía cạnh, sáng chế đề xuất máy truyền thông không dây có thể bao gồm: phương tiện nhận tín hiệu được điều hướng chùm từ thiết bị truyền; phương tiện ước lượng tổng có trọng số dựa ít nhất một phần vào nhiều hệ số kết hợp với tín hiệu được điều hướng chùm, trong đó nhiều hệ số bao gồm một hoặc nhiều hệ số liên quan đến một hoặc nhiều khiếm khuyết gắn với thiết bị truyền và một hoặc nhiều hệ số phụ thuộc vào vị trí không gian của máy; phương tiện xác định khóa mật mã dựa ít nhất một phần vào tỷ lệ giữa nhiều hệ số trong tổng có trọng số được kết hợp với tín hiệu được điều hướng chùm; và phương tiện bảo mật một hoặc nhiều cuộc truyền thông giữa máy và thiết bị truyền dựa ít nhất một phần vào khóa mật mã.

Các khía cạnh thường bao gồm phương pháp, máy, hệ thống, sản phẩm chương trình máy tính, phương tiện bất biến đọc được bằng máy tính, thiết bị người dùng, trạm gốc, thiết bị truyền thông không dây, và/hoặc hệ thống xử lý như được mô tả một cách cơ

bản trong bản mô tả này có tham chiếu đến và được minh họa bằng bản mô tả và hình vẽ kèm theo.

Các phần trên đây đã mô tả tương đối rộng các dấu hiệu và ưu điểm kỹ thuật của các ví dụ theo sáng chế để phân mô tả chi tiết sau đây có thể được hiểu rõ hơn. Các dấu hiệu và ưu điểm khác sẽ được mô tả sau đây. Khái niệm và các ví dụ cụ thể được bộc lộ có thể dễ dàng được dùng làm cơ sở để sửa đổi hoặc thiết kế các kết cấu khác để thực hiện các mục đích tương tự của sáng chế. Các kết cấu tương đương như vậy không nằm ngoài phạm vi của phân yêu cầu bảo hộ kèm theo. Các đặc điểm của các khái niệm được bộc lộ ở đây, cả cấu tạo và phương pháp hoạt động của chúng, cùng với các ưu điểm kèm theo sẽ được hiểu rõ hơn qua phần mô tả sau đây khi được xem xét cùng với các hình vẽ kèm theo. Mỗi hình vẽ được đưa ra nhằm mục đích minh họa và mô tả, và không nhằm xác định giới hạn của các yêu cầu bảo hộ.

Mô tả vắn tắt các hình vẽ

Do đó, các dấu hiệu nêu trên của sáng chế có thể được hiểu chi tiết, phân mô tả cụ thể hơn, được nêu vắn tắt trên đây, có thể có được bằng cách tham chiếu đến các khía cạnh, một số khía cạnh trong số các khía cạnh này được minh họa trên các hình vẽ kèm theo. Tuy nhiên, cần lưu ý rằng các hình vẽ kèm theo chỉ minh họa một số khía cạnh điển hình của sáng chế và do đó không được coi là giới hạn phạm vi của sáng chế, do phần mô tả có thể bao gồm các khía cạnh khác có hiệu quả ngang nhau. Các số chỉ dẫn giống nhau trên các hình vẽ khác nhau có thể nhận dạng các phần tử giống hoặc tương tự nhau.

Fig.1 là sơ đồ khối minh họa ví dụ về mạng truyền thông không dây, theo các khía cạnh khác nhau của sáng chế;

Fig.2 là sơ đồ khối minh họa ví dụ về trạm gốc truyền thông với UE trong mạng truyền thông không dây, theo các khía cạnh khác nhau của sáng chế.

Fig.3 là sơ đồ minh họa ví dụ về phương án thực hiện trong đó hai thiết bị không dây tạo ra khóa mật mã một cách độc lập dựa trên dấu hiệu đặc trưng lớp vật lý duy nhất, theo các khía cạnh khác nhau của sáng chế.

Fig.4 là sơ đồ minh họa ví dụ về quy trình được thực hiện, ví dụ, bằng thiết bị không dây, theo các khía cạnh khác nhau của sáng chế.

Mô tả chi tiết sáng chế

Sau đây, các khía cạnh khác nhau của sáng chế được mô tả đầy đủ hơn dựa vào các hình vẽ kèm theo. Tuy nhiên, sáng chế có thể được thể hiện ở nhiều dạng khác nhau và không nên được hiểu là bị giới hạn ở cấu trúc hoặc chức năng cụ thể bất kỳ nào được nêu xuyên suốt bản mô tả này. Đúng hơn là, các khía cạnh này được bộc lộ để bản mô tả sáng chế trở nên toàn diện và hoàn chỉnh, và sẽ truyền đạt đầy đủ phạm vi của sáng chế đến người có hiểu biết trung bình trong lĩnh vực kỹ thuật này. Dựa trên các nguyên lý được đề xuất ở đây, người có hiểu biết trung bình trong lĩnh vực kỹ thuật này có thể thấy rằng phạm vi của sáng chế dự kiến bao gồm mọi khía cạnh của sáng chế được đề xuất ở đây, cho dù được thực hiện độc lập hay kết hợp với bất kỳ khía cạnh nào khác của sáng chế. Ví dụ, máy có thể được triển khai hoặc phương pháp có thể được thực hiện nhờ sử dụng một số khía cạnh bất kỳ được đề xuất ở đây. Ngoài ra, phạm vi của sáng chế dự kiến bao gồm máy hoặc phương pháp mà được thực hiện bằng cách sử dụng cấu trúc, chức năng khác, hoặc cấu trúc và chức năng bổ sung hoặc nằm ngoài các khía cạnh khác nhau của sáng chế được nêu ở đây. Cần phải hiểu rằng mọi khía cạnh của sáng chế bộc lộ ở đây có thể được thể hiện bằng một hoặc nhiều phần tử nêu trong yêu cầu bảo hộ.

Theo một số khía cạnh, các hệ thống viễn thông sẽ được trình bày có dựa vào các máy và kỹ thuật khác nhau. Các máy và kỹ thuật này sẽ được mô tả trong phần mô tả chi tiết dưới đây và được minh họa trên các hình vẽ kèm theo bởi các khối, modul, bộ phận, mạch, bước, quy trình, thuật toán, khác nhau và/hoặc tương tự (được gọi chung là “phần tử”). Các phần tử này có thể được thực hiện nhờ sử dụng phần cứng, phần mềm, hoặc tổ hợp của chúng. Việc các phần tử như vậy được triển khai dưới dạng phần cứng hay phần mềm phụ thuộc vào các ràng buộc ứng dụng và thiết kế cụ thể được áp dụng cho toàn bộ hệ thống.

Cần lưu ý là mặc dù các khía cạnh có thể được mô tả ở đây bằng cách sử dụng thuật ngữ thường liên quan đến công nghệ không dây 3G và/hoặc 4G, nhưng các khía cạnh của sáng chế có thể được áp dụng trong các hệ thống truyền thông dựa trên thế hệ khác, như 5G và sau này, bao gồm cả các công nghệ NR.

Fig.1 là sơ đồ minh họa mạng không dây 100 trong đó các khía cạnh của sáng chế có thể được thực hiện. Mạng không dây 100 có thể là mạng LTE hoặc một mạng không dây khác nào đó, như mạng 5G hoặc NR chẳng hạn. Mạng không dây 100 có thể bao gồm một số BS 110 (được thể hiện trên hình vẽ là BS 110a, BS 110b, BS 110c và BS 110d) và các thực thể mạng khác. BS là thực thể truyền thông với các thiết bị người dùng (UE) và

có thể cũng được gọi là trạm gốc, BS NR, nút B, gNB, nút B (NB) 5G, điểm truy cập, điểm thu phát (transmit receive point - TRP), và/hoặc tương tự. Mỗi BS có thể cung cấp sự phủ sóng truyền thông cho một vùng địa lý cụ thể. Trong 3GPP, thuật ngữ “ô” có thể chỉ vùng phủ sóng của BS và/hoặc hệ thống con BS phục vụ vùng phủ sóng này, tùy thuộc vào ngữ cảnh mà thuật ngữ này được dùng.

BS có thể cung cấp vùng phủ sóng truyền thông cho ô macro, ô pico, ô femto, và/hoặc loại ô khác. Ô macro có thể phủ sóng một vùng địa lý tương đối rộng (chẳng hạn, có bán kính vài kilômet) và có thể cho phép các UE có đăng ký thuê bao dịch vụ truy cập không hạn chế. Ô pico có thể bao phủ một vùng địa lý tương đối nhỏ và có thể cho phép các UE là thuê bao dịch vụ truy cập không hạn chế. Ô femto có thể phủ sóng một vùng địa lý tương đối nhỏ (ví dụ, trong nhà) và có thể cho phép các UE có kết nối với ô femto này truy cập hạn chế (ví dụ, các UE trong nhóm thuê bao kín (closed subscriber group - CSG)). BS dùng cho ô macro có thể được gọi là BS macro. BS dùng cho ô pico có thể được gọi là BS pico. BS dùng cho ô femto có thể được gọi là BS femto hoặc BS trong nhà. Trong ví dụ thể hiện trên Fig.1, BS 110a có thể là BS macro dùng cho ô macro 102a, BS 110b có thể là BS pico dùng cho ô pico 102b, và BS 110c có thể là BS femto dùng cho ô femto 102c. BS có thể hỗ trợ một hoặc nhiều (ví dụ, ba) ô. Các thuật ngữ “eNB”, “trạm gốc”, “BS NR”, “gNB”, “TRP”, “AP”, “nút B”, “NB 5G”, và “ô” có thể được dùng thay thế cho nhau trong bản mô tả này.

Theo một số khía cạnh, ô có thể không nhất thiết là ô cố định, và vùng địa lý của ô có thể di chuyển theo vị trí của BS di động. Theo một số khía cạnh, các BS có thể được kết nối với nhau và/hoặc với một hoặc nhiều BS hoặc nút mạng khác (không được thể hiện trên hình vẽ) trong mạng truy cập 100 qua một số loại giao diện backhaul như kết nối vật lý trực tiếp, mạng ảo, và/hoặc tương tự bằng cách sử dụng mạng truyền tải thích hợp bất kỳ.

Mạng không dây 100 có thể cũng bao gồm các trạm chuyển tiếp. Trạm chuyển tiếp là thực thể có thể thu cuộc truyền dữ liệu từ trạm phía trên (ví dụ, BS hoặc UE) và gửi cuộc truyền dữ liệu cho trạm phía dưới (ví dụ, UE hoặc BS). Trạm chuyển tiếp có thể cũng là UE mà có thể chuyển tiếp các cuộc truyền cho các UE khác. Trong ví dụ thể hiện trên Fig.1, trạm chuyển tiếp 110d có thể truyền thông với BS macro 110a và UE 120d để hỗ trợ truyền thông giữa BS 110a và UE 120d. Trạm chuyển tiếp cũng có thể được gọi là BS chuyển tiếp, trạm gốc chuyển tiếp, bộ phận chuyển tiếp, và/hoặc tương tự.

Mạng không dây 100 có thể là mạng không đồng nhất bao gồm các BS thuộc nhiều kiểu khác nhau, ví dụ, các BS macro, các BS pico, các BS femto, các BS chuyển tiếp, và/hoặc tương tự. Các loại BS khác nhau này có thể có mức công suất truyền khác nhau, vùng phủ sóng khác nhau, và mức độ ảnh hưởng khác nhau đối với nhiễu trong mạng không dây 100. Ví dụ, các BS macro có thể có mức công suất truyền cao (ví dụ, từ 5 đến 40 Watt) trong khi các BS pico, các BS femto, và các BS chuyển tiếp có thể có các mức công suất truyền thấp hơn (ví dụ, từ 0,1 đến 2 Watt).

Bộ điều khiển mạng 130 có thể nối với tập hợp các BS và có thể cung cấp sự điều phối và điều khiển cho các BS này. Bộ điều khiển mạng 130 có thể truyền thông với các BS qua backhaul không dây hoặc có dây. Các BS có thể cũng truyền thông với nhau, (ví dụ, trực tiếp hoặc gián tiếp) qua backhaul không dây hoặc có dây.

Các UE 120 (ví dụ, 120a, 120b, 120c) có thể được phân tán khắp mạng không dây 100, và mỗi UE có thể cố định hoặc di động. UE cũng có thể được gọi là thiết bị đầu cuối truy cập, thiết bị đầu cuối, trạm di động, đơn vị thuê bao, trạm và/hoặc các thuật ngữ tương tự. UE có thể là điện thoại di động (ví dụ, điện thoại thông minh), thiết bị số hỗ trợ cá nhân (personal digital assistant - PDA), modem không dây, thiết bị truyền thông không dây, thiết bị cầm tay, máy tính xách tay, điện thoại không dây, trạm vòng cục bộ không dây (wireless local loop - WLL), máy tính bảng, máy ảnh, thiết bị trò chơi điện tử, máy tính netbook, máy tính bảng thông minh, máy tính siêu mỏng, thiết bị hoặc dụng cụ y tế, cảm biến/thiết bị sinh trắc học, thiết bị mang theo được (đồng hồ thông minh, quần áo thông minh, kính thông minh, dây đeo cổ tay thông minh, trang sức thông minh (ví dụ, nhẫn thông minh, vòng đeo tay thông minh), thiết bị giải trí (ví dụ, thiết bị nghe nhạc hoặc xem video hoặc vô tuyến vệ tinh), thành phần hoặc cảm biến trên xe, đồng hồ đo/cảm biến thông minh, thiết bị sản xuất công nghiệp, thiết bị hệ thống định vị toàn cầu hoặc thiết bị thích hợp khác bất kỳ được tạo cấu hình để truyền thông qua phương tiện không dây hoặc có dây.

Một số UE có thể được xem là các UE truyền thông kiểu máy (machine-type communication - MTC) hoặc truyền thông kiểu máy phát triển hoặc cải tiến (evolved hoặc enhanced machine-type communication - eMTC). Các UE MTC và eMTC bao gồm, ví dụ, robot, thiết bị bay không người lái, thiết bị từ xa, bộ cảm biến, máy đo, thiết bị giám sát, thẻ vị trí, và/hoặc tương tự, có thể truyền thông với trạm gốc thiết bị khác (ví dụ, thiết bị từ xa), hoặc một thực thể nào đó khác. Nút không dây có thể cung cấp, ví dụ, khả năng kết nối cho hoặc đến mạng (ví dụ, mạng diện rộng như Internet hoặc mạng kiểu ô) qua liên kết

truyền thông có dây hoặc không dây. Một số UE có thể được xem là thiết bị internet vạn vật (Internet-of-Thing - IoT), và/hoặc có thể được cài đặt như thiết bị internet vạn vật băng hẹp (narrowband internet of things - NB-IoT). Một số UE có thể được xem là thiết bị đặt tại cơ sở của khách hàng (Customer Premises Equipment - CPE). UE 120 có thể được đưa vào bên trong vỏ chứa các thành phần của UE 120, như các thành phần xử lý, các thành phần bộ nhớ, và/hoặc các thành phần tương tự.

Nói chung, số lượng mạng không dây bất kỳ có thể được triển khai trong một vùng địa lý cho trước. Mỗi mạng không dây có thể hỗ trợ một công nghệ truy cập vô tuyến (radio access technology - RAT) cụ thể và có thể hoạt động trên một hoặc nhiều tần số. RAT cũng có thể được dùng để chỉ công nghệ vô tuyến, giao diện không gian, và/hoặc tương tự. Tần số cũng có thể được gọi là sóng mang, kênh tần số, và/hoặc tương tự. Mỗi tần số cũng có thể hỗ trợ một RAT trong một vùng địa lý nhất định để tránh nhiễu giữa các mạng không dây có các RAT khác nhau. Trong một số trường hợp, các mạng RAT NR hoặc 5G có thể được triển khai.

Theo một số khía cạnh, hai hoặc nhiều UE 120 (ví dụ, được thể hiện dưới dạng UE 120a và UE 120e) có thể truyền thông trực tiếp nhờ sử dụng một hoặc nhiều kênh liên kết phụ (ví dụ, mà không cần sử dụng trạm gốc 110 làm trung gian để truyền thông với nhau). Ví dụ, các UE 120 có thể truyền thông bằng cách dùng các cuộc truyền ngang hàng (peer-to-peer - P2P), cuộc truyền từ thiết bị đến thiết bị (device-to-device -D2D), giao thức từ phương tiện đến tất cả (vehicle-to-everything -V2X) (ví dụ, có thể bao gồm giao thức từ phương tiện đến phương tiện (vehicle-to-vehicle - V2V), giao thức từ phương tiện đến cơ sở hạ tầng (vehicle-to-infrastructure -V2I), và/hoặc các giao thức tương tự), mạng kiểu lưới, và/hoặc mạng tương tự. Trong trường hợp này, UE 120 có thể thực hiện các thao tác lập lịch, các thao tác chọn tài nguyên, và/hoặc các thao tác khác được mô tả trong phần khác trong bản mô tả này là được thực hiện bởi trạm gốc 110.

Như đã nêu trên, Fig.1 được đưa ra làm ví dụ. Các ví dụ khác có thể khác với những gì được mô tả trên Fig.1.

Fig.2 thể hiện sơ đồ khối của thiết kế 200 của trạm gốc 110 và UE 120, mà có thể là một trong các trạm gốc và một trong các UE trên Fig.1. Trạm gốc 110 có thể được trang bị T anten từ 234a đến 234t, và UE 120 có thể được trang bị R anten từ 252a đến 252r, trong đó nói chung $T \geq 1$ và $R \geq 1$

Ở trạm gốc 110, bộ xử lý truyền 220 có thể nhận dữ liệu từ nguồn dữ liệu 212 cho một hoặc nhiều UE, chọn một hoặc nhiều sơ đồ điều chế và mã hóa (modulation and coding schemes - MCS) cho mỗi UE dựa ít nhất một phần vào chỉ báo chất lượng kênh (channel quality indicator - CQI) nhận được từ UE, xử lý (ví dụ, mã hóa và điều chế) dữ liệu cho mỗi UE dựa ít nhất một phần vào (các) MCS được chọn cho UE, và cung cấp các ký hiệu dữ liệu cho tất cả các UE. Bộ xử lý truyền 220 cũng có thể xử lý thông tin hệ thống (ví dụ, cho thông tin phân chia nguồn bán tĩnh (semi-static resource partitioning information - SRPI), và/hoặc tương tự) và thông tin điều khiển (ví dụ, các yêu cầu CQI, cấp phép, báo hiệu lớp trên, và/hoặc tương tự) và cung cấp các ký hiệu hao tổn và các ký hiệu điều khiển. Bộ xử lý truyền 220 cũng có thể tạo ra các ký hiệu tham chiếu cho các tín hiệu tham chiếu (ví dụ, tín hiệu tham chiếu riêng của ô (cell-specific reference signal - CRS) và các tín hiệu đồng bộ hóa (ví dụ, tín hiệu đồng bộ hóa sơ cấp (primary synchronization signal - PSS) và tín hiệu đồng bộ hóa thứ cấp (secondary synchronization signal - SSS)). Bộ xử lý nhiều đầu vào nhiều đầu ra (multiple-input multiple-output - MIMO) truyền (truyền - TX) 230 có thể thực hiện xử lý không gian (ví dụ, tiền mã hóa) trên các ký hiệu dữ liệu, ký hiệu điều khiển, ký hiệu hao tổn, và/hoặc các ký hiệu tham chiếu, nếu có thể, và có thể cung cấp T dòng ký hiệu đầu ra cho T bộ điều chế (modulator - MOD) từ 232a đến 232t. Mỗi bộ điều chế 232 có thể xử lý dòng ký hiệu đầu ra tương ứng (ví dụ, cho OFDM, và/hoặc tương tự) để thu nhận dòng mẫu đầu ra. Mỗi bộ điều chế 232 có thể còn xử lý (ví dụ, chuyển đổi sang tín hiệu tương tự, khuếch đại, lọc và biến đổi tăng tần số) dòng mẫu đầu ra để thu nhận tín hiệu đường xuống. T tín hiệu đường xuống từ các bộ điều chế từ 232a đến 232t có thể được truyền lần lượt qua T anten từ 234a đến 234t. Theo các khía cạnh khác nhau được mô tả chi tiết hơn dưới đây, các tín hiệu đồng bộ hóa có thể được tạo ra bằng việc mã hóa vị trí để truyền thông tin bổ sung.

Tại UE 120, các anten từ 252a đến 252r có thể nhận các tín hiệu đường xuống từ trạm gốc 110 và/hoặc các trạm gốc khác và có thể cung cấp các tín hiệu nhận được lần lượt cho các bộ giải điều chế (demodulator - DEMOD) từ 254a đến 254r. Mỗi bộ giải điều chế 254 có thể làm thích ứng (ví dụ, lọc, khuếch đại, biến đổi giảm tần số, và số hóa) tín hiệu nhận được để thu nhận các mẫu đầu vào. Mỗi bộ giải điều chế 254 có thể còn xử lý các mẫu đầu vào (ví dụ, đối với OFDM, và/hoặc tương tự) để thu nhận các ký hiệu nhận được. Bộ dò MIMO 256 có thể thu được các ký hiệu đã nhận từ tất cả R bộ giải điều chế từ 254a đến 254r, thực hiện dò MIMO trên các ký hiệu đã nhận nếu có thể, và cung cấp các ký hiệu

dò được. Bộ xử lý nhận 258 có thể xử lý (ví dụ, giải điều chế và giải mã) các ký hiệu dò được, cung cấp dữ liệu giải mã của UE 120 cho vùng dữ liệu 260, và cung cấp thông tin điều khiển đã giải mã và thông tin hệ thống cho bộ điều khiển/bộ xử lý 280. Bộ xử lý kênh có thể xác định công suất nhận được của tín hiệu tham chiếu (reference signal received power - RSRP), chỉ báo cường độ tín hiệu nhận được (received signal strength indicator - RSSI), chất lượng nhận được của tín hiệu tham chiếu (reference signal received quality - RSRQ), chỉ báo chất lượng kênh (channel quality indicator - CQI), và/hoặc các thông tin tương tự. Theo một số khía cạnh, một hoặc nhiều thành phần của UE 120 có thể được đưa vào trong vỏ.

Trên đường lên, tại UE 120, bộ xử lý truyền 264 có thể nhận và xử lý dữ liệu từ nguồn dữ liệu 262 và thông tin điều khiển (ví dụ, cho các báo cáo bao gồm RSRP, RSSI, RSRQ, CQI, và/hoặc tương tự) từ bộ điều khiển/bộ xử lý 280. Bộ xử lý truyền 264 có thể cũng tạo ra các ký hiệu tham chiếu cho một hoặc nhiều tín hiệu tham chiếu. Các ký hiệu từ bộ xử lý truyền 264 có thể được tiền mã hóa bởi bộ xử lý MIMO TX 266 nếu có thể, được xử lý thêm bởi các bộ điều chế 254a đến 254r (ví dụ, đối với DFT-s-OFDM, CP-OFDM, và/hoặc tương tự), và được truyền đến trạm gốc 110. Tại trạm gốc 110, các tín hiệu đường lên từ UE 120 và các UE khác có thể được nhận bởi anten 234, được xử lý bởi các bộ giải điều chế 232, được phát hiện bởi bộ dò MIMO 236 nếu có thể, và được xử lý thêm bởi bộ xử lý nhận 238 để thu nhận dữ liệu đã giải mã và thông tin điều khiển do UE 120 gửi. Bộ xử lý nhận 238 có thể cung cấp dữ liệu đã giải mã cho bộ góp dữ liệu 239 và thông tin điều khiển đã giải mã cho bộ điều khiển/bộ xử lý 240. Trạm gốc 110 có thể bao gồm đơn vị truyền thông 244 và truyền thông đến bộ điều khiển mạng 130 qua đơn vị truyền thông 244. Bộ điều khiển mạng 130 có thể bao gồm đơn vị truyền thông 294, bộ điều khiển/bộ xử lý 290, và bộ nhớ 292.

Bộ điều khiển/bộ xử lý 240 của trạm gốc 110, bộ điều khiển/bộ xử lý 280 của UE 120, bộ điều khiển/bộ xử lý 290 của bộ điều khiển mạng 130, và/hoặc (các) thành phần khác bất kỳ trên Fig.2 có thể thực hiện một hoặc nhiều kỹ thuật liên quan đến dấu hiệu đặc trưng lớp vật lý dựa trên khiếm khuyết. Ví dụ, như được mô tả chi tiết hơn ở nơi khác trong bản mô tả này, bộ điều khiển/bộ xử lý 240 của trạm gốc 110, bộ điều khiển/bộ xử lý 280 của UE 120, bộ điều khiển/bộ xử lý 290 của bộ điều khiển mạng 130 và/hoặc (các) thành phần khác bất kỳ trên Fig.2 có thể thực hiện một hoặc nhiều kỹ thuật để sử dụng dấu hiệu đặc trưng lớp vật lý dựa trên khiếm khuyết và/hoặc một hoặc nhiều đặc điểm kênh đa

đường MIMO để tạo ra khóa mật mã mà không được dùng chung trong phiên trao đổi khóa. Ví dụ, bộ điều khiển/bộ xử lý 240 của trạm gốc 110, bộ điều khiển/bộ xử lý 280 của UE 120, và/hoặc (các) thành phần khác bất kỳ trên Fig.2 có thể thực hiện hoặc quản lý các hoạt động của, ví dụ, quy trình 400 trên Fig.4, và/hoặc các quy trình khác như được mô tả ở đây. Các bộ nhớ 242, 282, 292 có thể lưu trữ lần lượt dữ liệu và các mã chương trình cho trạm gốc 110, UE 120 và bộ điều khiển mạng 130. Theo một số khía cạnh, bộ nhớ 242, bộ nhớ 282, và/hoặc bộ nhớ 292 có thể bao gồm phương tiện bất biến đọc được bằng máy tính lưu trữ một hoặc nhiều lệnh để truyền thông không dây. Ví dụ, một hoặc nhiều lệnh, khi được thực thi bởi một hoặc nhiều bộ xử lý của trạm gốc 110, UE 120, bộ điều khiển mạng 130, và/hoặc tương tự có thể thực hiện hoặc quản lý các hoạt động của, ví dụ, quy trình 400 trên Fig.4 và/hoặc các quy trình khác như được mô tả ở đây. Bộ lập lịch 246 có thể lập lịch các UE để truyền dữ liệu trên đường xuống và/hoặc đường lên.

Theo một số khía cạnh, trạm gốc 110, UE 120, bộ điều khiển mạng 130 và/hoặc tương tự có thể bao gồm phương tiện nhận tín hiệu được điều hướng chùm từ thiết bị truyền, phương tiện để ước lượng tổng có trọng số dựa ít nhất một phần vào nhiều hệ số kết hợp với tín hiệu được điều hướng chùm, phương tiện xác định khóa mật mã dựa ít nhất một phần vào tỷ lệ giữa nhiều hệ số trong tổng có trọng số được kết hợp với tín hiệu được điều hướng chùm, phương tiện bảo mật một hoặc nhiều cuộc truyền thông giữa máy và thiết bị truyền dựa ít nhất một phần vào khóa mật mã, và/hoặc tương tự. Theo một số khía cạnh, các phương tiện như vậy có thể bao gồm một hoặc nhiều thành phần của trạm gốc 110 được mô tả trên Fig.2, như anten 234, DEMOD 232, bộ dò MIMO 236, bộ xử lý nhận 238, bộ điều khiển/bộ xử lý 240, bộ xử lý truyền 220, bộ xử lý TX MIMO 230, MOD 232, anten 234, và/hoặc tương tự. Ngoài ra hoặc cách khác, các phương tiện như vậy có thể bao gồm một hoặc nhiều thành phần của UE 120 được mô tả dựa vào Fig.2, như bộ điều khiển/bộ xử lý 280, bộ xử lý truyền 264, bộ xử lý TX MIMO 266, MOD 254, anten 252, DEMOD 254, bộ dò MIMO 256, bộ xử lý nhận 258, và/hoặc tương tự. Ngoài ra, hoặc theo cách khác, các phương tiện như vậy có thể bao gồm một hoặc nhiều thành phần của bộ điều khiển mạng 290 được mô tả dựa vào Fig.2, như bộ điều khiển/bộ xử lý 290, bộ nhớ 292, đơn vị truyền thông 294, và/hoặc tương tự.

Như đã nêu ở trên, Fig.2 được đưa ra làm ví dụ. Các ví dụ khác có thể khác với những gì được mô tả trên Fig.2.

Khi hai thiết bị truyền thông qua kênh không dây trong mạng không dây (ví dụ, mạng LTE, mạng NR, và/hoặc tương tự), lưu lượng được truyền qua kênh không dây có thể được mã hóa hoặc cách khác được mã hóa bằng cách sử dụng khóa mật mã. Ví dụ, các kỹ thuật bảo mật thường được triển khai trong các mạng không dây bằng cách sử dụng kỹ thuật mã hóa truyền nhận đã biết dựa vào kỹ thuật mã hóa lớp cao hơn với khóa mật mã được dùng chung giữa các thiết bị điểm cuối và được dùng để mã hóa văn bản gốc thành văn bản mã hóa và để giải mã văn bản mã hóa thành văn bản gốc. Do đó, để bảo mật kênh không dây và cho phép truyền thông bảo mật qua kênh không dây, các thiết bị điểm cuối có thể thực hiện phiên trao đổi khóa khi bắt đầu phiên truyền thông để dàn xếp hoặc trao đổi (các) khóa mật mã sẽ được dùng trong phiên truyền thông. Trong các giao thức bảo mật dựa trên phiên trao đổi khóa, nhu cầu trao đổi (các) khóa mật mã được dùng trong phiên truyền thông là một điểm yếu mà người dùng trái phép (ví dụ, người nghe lén) có thể khai thác. Ví dụ, nếu người dùng trái phép có thể truy cập (các) khóa mật mã, thì người dùng trái phép có thể giải mã dữ liệu mà được truyền trong phiên truyền thông. Nói cách khác, nếu hai thiết bị không thể thiết lập trao đổi khóa ban đầu an toàn, thì các thiết bị sẽ không thể truyền thông an toàn qua kênh không dây mà không có nguy cơ thông tin truyền thông qua kênh không dây bị chặn và giải mã bởi bên thứ ba trái phép đã thu được khóa bí mật trong quá trình trao đổi khóa ban đầu.

Một số khía cạnh được mô tả ở đây cung cấp các kỹ thuật và máy để tạo ra khóa mật mã tại các thiết bị không dây khác nhau theo cách phối hợp mà không cần các thiết bị không dây dùng chung một cách rõ ràng khóa mật mã hoặc tham số bất kỳ được dùng để tạo khóa mật mã. Ví dụ, một hoặc nhiều thành phần trong đường truyền tương tự có thể được kết hợp với tập hợp các khiếm khuyết hoặc dấu hiệu nhân tạo (ví dụ, độ tuyến tính của bộ khuếch đại công suất, băng tần bên dư (residual sideband - RSB) phụ thuộc tần số, độ dịch tần số, và/hoặc tương tự) là duy nhất đối với một thiết bị cụ thể, do đó thiết bị nhất định bất kỳ có thể có dấu hiệu đặc trưng tần số vô tuyến (radio frequency - RF) duy nhất mà có thể được dùng để tạo ra khóa mật mã. Ví dụ, tập hợp khiếm khuyết hoặc dấu hiệu nhân tạo nói chung có thể thay đổi từ thiết bị này sang thiết bị khác sao cho tập hợp khiếm khuyết hoặc dấu hiệu nhân tạo có thể là duy nhất theo nghĩa là tập hợp khiếm khuyết hoặc dấu hiệu nhân tạo đó có thể hiếm gặp hoặc không bao giờ giống nhau ở hai thiết bị khác nhau. Hơn nữa, một số kỹ thuật và máy được mô tả ở đây có thể sử dụng kỹ thuật điều hướng chùm sóng để truyền tín hiệu được điều hướng chùm hướng đến bộ thu dự kiến qua

kênh đa đường MIMO, và tín hiệu được điều hướng chùm có thể được kết hợp với tập hợp các hệ số trước méo kỹ thuật số (digital pre-distortion - DPD) (ví dụ, pha kênh, pha điều hướng chùm sóng, và/hoặc tương tự) khác nhau tại các vị trí không gian khác nhau.

Ví dụ, như được mô tả ở đây, tín hiệu được điều hướng chùm thường có thể đề cập đến tín hiệu được truyền từ thiết bị có nhiều anten, và tín hiệu được điều hướng chùm có thể được lái theo một hướng cụ thể (ví dụ, hướng đến bộ thu dự kiến) bằng cách điều khiển tín hiệu được truyền từ nhiều anten. Do đó, như được mô tả chi tiết hơn ở đây, thiết bị truyền có nhiều anten phát có thể tạo ra khóa mật mã dựa trên một hoặc nhiều khiếm khuyết liên quan đến một hoặc nhiều thành phần (ví dụ, bộ khuếch đại công suất) trong đường truyền tương tự, và thiết bị truyền có thể sử dụng kỹ thuật điều hướng chùm sóng để lái chùm (ví dụ, tín hiệu được điều hướng chùm) hướng đến vị trí không gian của bộ thu dự kiến qua kênh đa đường MIMO. Như được mô tả chi tiết hơn dưới đây, bộ thu dự kiến có thể ước lượng tổng có trọng số kết hợp với chùm và sử dụng tổng có trọng số để suy ra khóa mật mã giống như thiết bị truyền, dựa trên một hoặc nhiều hệ số liên quan đến các khiếm khuyết kết hợp với một hoặc nhiều thành phần trong đường truyền tương tự và một số đặc tính nhất định mà các hệ số DPD của chùm có được khi bộ thu dự kiến được bố trí về mặt không gian tại hoặc gần tâm của chùm được lái hướng đến bộ thu dự kiến.

Theo cách này, các thiết bị không dây (ví dụ, thiết bị truyền và bộ thu dự kiến) có thể sử dụng khóa mật mã để bảo mật một hoặc nhiều cuộc truyền thông qua kênh đa đường MIMO mà không phải thực hiện phiên trao đổi khóa hoặc theo cách khác là dùng chung một cách rõ ràng khóa mật mã hoặc (các) tham số được dùng để tạo ra khóa mật mã. Hơn nữa, vì các hệ số DPD ở các vị trí không gian khác nhau là khác nhau nên thiết bị nghe lén ở vị trí vật lý khác không thể ước lượng một cách chính xác một hoặc nhiều hệ số liên quan đến các khiếm khuyết gắn với một hoặc nhiều thành phần trên đường truyền tương tự giữa các thiết bị không dây 310, 320 và do đó không thể tạo ra khóa mật mã được dùng để bảo mật một hoặc nhiều cuộc truyền thông giữa các thiết bị không dây 310, 320.

Fig.3 là sơ đồ minh họa phương án làm ví dụ 300 trong đó hai thiết bị không dây tạo ra khóa mật mã một cách độc lập dựa trên dấu hiệu đặc trưng lớp vật lý duy nhất, theo một số khía cạnh của sáng chế. Ví dụ, như được mô tả chi tiết hơn ở đây, hai thiết bị không dây có thể tạo ra khóa mật mã một cách độc lập dựa trên một hoặc nhiều khiếm khuyết mà là duy nhất đối với một hoặc nhiều thành phần trên đường truyền RF tương tự giữa các thiết bị không dây. Ví dụ, trong phương án thực hiện làm ví dụ 300 được thể hiện trong

hình vẽ trên Fig.3, thiết bị không dây thứ nhất 310 (Alice) và thiết bị không dây thứ hai 320 (Bob) thiết lập phiên truyền thông an toàn mà được bảo vệ chống lại truy cập trái phép của thiết bị nghe lén 330 (Eve). Nói chung, thiết bị không dây thứ nhất 310 và thiết bị không dây thứ hai 320 có thể tương ứng với trạm gốc và UE truyền thông qua đường lên và đường xuống, một cặp UE truyền thông qua liên kết phụ, cặp thiết bị mạng (ví dụ, trạm gốc, bộ điều khiển mạng, máy chủ, và/hoặc tương tự) truyền thông qua liên kết backhaul không dây, và/hoặc tương tự.

Trong phương án thực hiện làm ví dụ 300 được thể hiện trên Fig.3, thiết bị không dây thứ nhất 310 có thể tương ứng với bộ phát nhiều anten phát tín hiệu được điều hướng chùm (ở đây có thể được gọi đơn giản là chùm) được lái hướng đến thiết bị không dây thứ hai 320, thiết bị này có một hoặc nhiều anten thu. Nói chung, nhiều anten phát có thể được kết hợp với một hoặc nhiều bộ khuếch đại công suất phi tuyến tính. Cụ thể hơn, trong bộ khuếch đại công suất tuyến tính, tín hiệu đầu ra thường tỷ lệ thuận với tín hiệu đầu vào, còn bộ khuếch đại công suất phi tuyến tính có thể tạo ra tín hiệu đầu ra không tỷ lệ thuận với tín hiệu đầu vào. Ví dụ, trong thiết bị không dây có nhiều anten phát, mỗi anten được kết hợp với một hoặc nhiều bộ khuếch đại công suất phi tuyến tính, tín hiệu đầu ra từ mỗi bộ khuếch đại công suất phi tuyến tính có thể được biểu diễn như sau:

$$PA_n = x + a_n|x|^2x$$

trong đó n là chỉ số của bộ khuếch đại công suất phi tuyến tính, x là tín hiệu đầu vào của bộ khuếch đại công suất phi tuyến tính, a_n là hệ số biểu diễn lượng phi tuyến tính trong bộ khuếch đại công suất (ví dụ, tùy thuộc vào công suất được cung cấp cho bộ khuếch đại công suất phi tuyến tính), và số hạng bậc cao hơn $a_n|x|^2x$ là nhân Volterra đại diện cho độ phi tuyến tính của bộ khuếch đại công suất. Nói chung, giá trị của hệ số a_n có thể giống nhau hoặc khác nhau đối với mỗi bộ khuếch đại công suất. Ví dụ, như được mô tả chi tiết hơn ở đây, giá trị của hệ số a_n có thể được điều khiển một cách độc lập đối với mỗi bộ khuếch đại công suất (ví dụ, dựa trên các đặc tính duy nhất được kết hợp với bộ khuếch đại công suất, các mức công suất được cung cấp cho bộ khuếch đại công suất và/hoặc tương tự). Hơn nữa, mặc dù ví dụ trên biểu thị sự phi tuyến tính của bộ khuếch đại công suất sử dụng một nhân Volterra, trong một số khía cạnh, sự phi tuyến tính đối với một hoặc nhiều bộ khuếch đại công suất có thể được biểu diễn bằng cách sử dụng một hoặc nhiều nhân Volterra bổ sung (ví dụ, $b_n|x|^4x$ và/hoặc tương tự). Do đó, theo một số khía cạnh, tín hiệu

đầu ra từ mỗi bộ khuếch đại công suất phi tuyến tính thường có thể bao gồm số hạng tuyến tính (ví dụ, x trong ví dụ ở trên), và các số hạng phi tuyến tính lượng thích hợp bất kỳ (hoặc nhân Volterra) để đại diện cho loại trạng thái phi tuyến tính, hiệu ứng, đặc tính, thuộc tính và/hoặc tương tự thích hợp bất kỳ gắn với một hoặc nhiều thành phần trên đường truyền RF tương tự giữa các thiết bị không dây 310, 320. Ví dụ, trong ví dụ trên đây, $a_n|x|^2x$ có thể đại diện cho mối quan hệ phi tuyến tính giữa công suất đầu vào và công suất đầu ra kết hợp với bộ khuếch đại công suất, mặc dù (các) nhân Volterra có thể biểu diễn hoặc theo cách khác mô hình hóa các loại trạng thái phi tuyến tính thích hợp khác, như hiệu ứng bộ nhớ khiến cho các đặc tính của bộ khuếch đại công suất thay đổi như hàm của các mức đầu vào trước đây và/hoặc tương tự.

Như thể hiện trên Fig.3 và theo số chỉ dẫn 340, thiết bị không dây thứ nhất 310 có thể tạo ra khóa mật mã được dùng để bảo mật một hoặc nhiều cuộc truyền thông với thiết bị không dây thứ hai 320, dựa trên một hoặc nhiều khiếm khuyết duy nhất mà tạo ra dấu hiệu đặc trưng RF duy nhất cho thiết bị không dây thứ nhất 310. Ví dụ, như được mô tả ở đây, các khiếm khuyết duy nhất có thể bao gồm các độ phi tuyến tính của các bộ khuếch đại công suất được biểu diễn theo cách được mô tả ở trên. Ngoài ra, hoặc theo cách khác, theo một số khía cạnh, các khiếm khuyết duy nhất có thể bao gồm RSB phụ thuộc vào tần số liên quan đến sự không phù hợp giữa các thành phần trong pha (in-phase - I) và vuông góc (quadrature - Q), độ dịch tần số hoặc tạp âm pha dao động liên quan đến độ dịch của bộ dao động từ tần số danh định (ví dụ, do lão hóa thành phần, thay đổi nhiệt độ, sự thay đổi điện áp phân cực, và/hoặc tương tự), và/hoặc các dấu hiệu nhân tạo thích hợp khác trong đường truyền tương tự cung cấp dấu hiệu đặc trưng RF duy nhất cho một thiết bị không dây cụ thể.

Theo một số khía cạnh, khi (các) khiếm khuyết duy nhất được thiết bị không dây thứ nhất 310 sử dụng để tạo ra khóa mật mã liên quan đến độ phi tuyến tính của bộ khuếch đại công suất, khóa mật mã có thể tương ứng với giá trị trung bình của các hệ số phi tuyến tính trên toàn bộ các bộ khuếch đại công suất trong đường truyền tương tự cụ thể (ví dụ, các bộ khuếch đại công suất được kết hợp với nhiều anten phát trong một chuỗi phát đã cho). Ví dụ, theo một số khía cạnh, khóa mật mã được tạo ra bởi thiết bị không dây thứ nhất 310 và được dùng để bảo mật một hoặc nhiều cuộc truyền thông với thiết bị không dây thứ hai 320 có thể được biểu diễn như sau:

$$\frac{1}{n} \sum_n a_n$$

trong đó n là chỉ số của mỗi bộ khuếch đại công suất phi tuyến tính và a_n là hệ số biểu thị lượng phi tuyến tính trên mỗi bộ khuếch đại công suất. Ví dụ, như thể hiện bởi số chỉ dẫn 342, thiết bị không dây thứ nhất 310 có thể truyền chùm mà được lái hướng đến bộ thu dự kiến (thiết bị không dây thứ hai 320), và nói chung chùm có thể được truyền bằng cách sử dụng nhiều anten phát được gắn với nhiều bộ khuếch đại công suất, mỗi trong số chúng có thể được kết hợp với một hệ số phi tuyến tính khác a_n vì mỗi bộ khuếch đại công suất có thể có các đặc tính phi tuyến tính duy nhất. Do đó, giá trị trung bình của các hệ số phi tuyến tính trên tất cả các bộ khuếch đại công suất có thể được dùng làm khóa mật mã, và như thể hiện bằng số chỉ dẫn 344, thiết bị không dây thứ hai 320 có thể ước lượng khóa mật mã dựa trên một hoặc nhiều hệ số kết hợp với chùm mà được truyền bởi thiết bị không dây thứ nhất 310. Ví dụ, để lái chùm hướng về phía thiết bị không dây thứ hai 320, thiết bị không dây thứ nhất 310 có thể điều khiển pha điều hướng chùm sóng, biên độ tương đối, và/hoặc tương tự kết hợp với tín hiệu tại mỗi anten phát để tạo ra mẫu có cấu trúc và nhiễu giảm mà dẫn đến tín hiệu kết hợp một cách nhất quán tại vị trí không gian của thiết bị không dây thứ hai 320. Do đó, thiết bị không dây thứ hai 320 có thể ước lượng khóa mật mã mà được tạo ra bởi thiết bị không dây thứ nhất 310 dựa trên một số hệ số kết hợp với chùm nhận được từ thiết bị không dây thứ nhất 310, có thể bao gồm một hoặc nhiều hệ số liên quan đến một hoặc nhiều khiếm khuyết (ví dụ, phi tuyến tính) chỉ được kết hợp với nhiều bộ khuếch đại công suất ở thiết bị không dây thứ nhất 310 và một hoặc nhiều hệ số phụ thuộc vào vị trí không gian của thiết bị không dây thứ hai 320.

Ví dụ, như đề cập ở trên, thiết bị không dây thứ nhất 310 có thể truyền chùm mà được hướng về phía thiết bị không dây thứ hai 320 bằng cách sử dụng nhiều anten phát, mỗi anten này được kết hợp với một hoặc nhiều bộ khuếch đại công suất, và số hạng n có thể là số lượng anten phát. Do đó, theo một số khía cạnh, tín hiệu mang trong chùm được nhận bởi thiết bị không dây thứ hai 320 có thể được biểu diễn như sau:

$$y_{Bob} = \sum_n h_n \theta_n (x + a_n |x|^2 x)$$

trong đó h_n là pha kênh giữa thiết bị không dây thứ hai 320 và anten phát thứ n ở thiết bị không dây thứ nhất 310, θ_n là pha điều hướng chùm sóng được áp dụng cho anten phát thứ n (ví dụ, để lái chùm hướng về phía góc phương vị cụ thể mà dẫn đến chùm kết

hợp một cách nhất quán tại vị trí không gian của thiết bị không dây thứ hai 320) và $(x + a_n|x|^2x)$ là tín hiệu đầu ra từ bộ khuếch đại công suất thứ n , như được mô tả ở trên. Do đó, tín hiệu nhận được bởi thiết bị không dây thứ hai 320 có thể tương ứng với tổng có trọng số dựa trên một số hệ số mà phụ thuộc vào một hoặc nhiều khiếm khuyết kết hợp với thiết bị không dây thứ nhất 310 (ví dụ, độ phi tuyến tính của bộ khuếch đại công suất trong ví dụ hiện tại), các pha điều hướng chùm sóng được áp dụng ở thiết bị không dây thứ nhất 310 để lái chùm hướng về phía thiết bị không dây thứ hai 320 và các pha kênh phụ thuộc vào một hoặc nhiều đặc điểm kênh đa đường MIMO giữa thiết bị không dây thứ nhất 310 và thiết bị không dây thứ hai 320 (ví dụ, các vật cản, bề mặt phản xạ, và/hoặc các vật thể khác trong môi trường tác động đến cách thức truyền tín hiệu giữa thiết bị không dây thứ nhất 310 đến thiết bị không dây thứ hai 320).

Theo một số khía cạnh, thiết bị không dây thứ hai 320 có thể ước lượng khóa mật mã dựa trên tỷ lệ giữa nhiều hệ số trong tổng có trọng số liên quan đến tín hiệu nhận được. Ví dụ, theo một số khía cạnh, thiết bị không dây thứ hai 320 có thể ước lượng khóa mật mã theo tỷ lệ của một hoặc nhiều hệ số bậc ba với một hoặc nhiều hệ số bậc nhất, như sau:

$$\frac{\sum_n \theta_n a_n h_n}{\sum_n \theta_n h_n}$$

Theo một số khía cạnh, do chùm được truyền bởi thiết bị không dây thứ nhất 310 được lái hướng về phía vị trí không gian của thiết bị không dây thứ hai 320, nên các tín hiệu được truyền từ nhiều anten của thiết bị không dây thứ nhất 310 có thể kết hợp một cách nhất quán tại vị trí không gian của thiết bị không dây thứ hai 320. Ví dụ, khi chùm được định hướng hoặc lái về phía một góc phương vị cụ thể trong không gian, các tín hiệu tạo nên chùm có thể kết hợp một cách nhất quán theo góc phương vị cụ thể đó, trong trường hợp này tương ứng với vị trí không gian của thiết bị không dây thứ hai 320. Nói cách khác, thiết bị không dây thứ nhất 310 điều chỉnh hoặc điều khiển giá trị θ_n để đảm bảo rằng chùm sẽ kết hợp một cách nhất quán tại vị trí không gian của thiết bị không dây thứ hai 320, nhờ đó dẫn đến thuộc tính $\theta_n h_n \approx 1$ cho mỗi anten phát. Do đó, theo tỷ lệ trên, các số hạng $\theta_n h_n$ có thể đơn giản hóa thành một, dẫn đến thiết bị không dây thứ hai 320 ước lượng khóa mật mã như sau:

$$\frac{\sum_n a_n}{n}$$

về cơ bản tương đương với khóa mật mã được tạo ra ở thiết bị không dây thứ nhất 310. Hơn nữa, theo một số khía cạnh, chùm có thể không được chia vào hoặc định tâm một cách chính xác tại vị trí không gian của thiết bị không dây thứ hai 320 (ví dụ, do các đặc điểm kênh đa đường). Do đó, theo một số khía cạnh, thiết bị không dây thứ hai 320 có thể lượng hóa các hệ số khác nhau trong tổng có trọng số và ước lượng khóa mật mã dựa trên các hệ số đã lượng tử hóa, để giảm đến mức thấp nhất xác suất ước lượng không chính xác khóa mật mã.

Theo một số khía cạnh, như thể hiện thêm trên Fig.3, và theo số chỉ dẫn 346, thiết bị nghe lén 330 cũng có thể nhận chùm được truyền bởi thiết bị không dây thứ nhất 310. Tuy nhiên, như được thể hiện bởi số chỉ dẫn 348, thiết bị nghe lén 330 không thể ước lượng khóa mật mã chính xác vì chùm được lái hướng về phía thiết bị không dây thứ hai 320 (chứ không phải về phía thiết bị nghe lén 330), do đó ít nhất là hệ số pha kênh sẽ khác ở thiết bị nghe lén 330 do các đặc điểm kênh đa đường khác nhau. Cụ thể, theo cách tương tự như mô tả ở trên, tín hiệu mang trong chùm nhận được bởi thiết bị nghe lén 330 có thể được biểu diễn như sau:

$$y_{Eve} = \sum_n g_n \theta_n (x + a_n |x|^2 x)$$

trong đó g_n là pha kênh giữa anten thu của thiết bị nghe lén 330 và anten phát thứ n ở thiết bị không dây thứ nhất 310. Do đó, khi cố gắng ước lượng khóa mật mã là tỷ lệ của một hoặc nhiều hệ số bậc ba với một hoặc nhiều hệ số bậc nhất, thiết bị nghe lén 330 có thể ước lượng khóa mật mã như sau:

$$\frac{\sum_n \theta_n a_n g_n}{\sum_n \theta_n g_n}$$

Trong trường hợp này, vì chùm không được lái hướng về phía thiết bị nghe lén 330, tích của θ_n và g_n không bằng một, do đó thiết bị nghe lén 330 không thể ước lượng chính xác khóa mật mã $\frac{\sum_n a_n}{n}$. Hơn nữa, ngay cả khi thiết bị nghe lén 330 bằng cách nào đó có thể thu được giá trị h_n (ví dụ, pha kênh giữa anten thu ở thiết bị không dây thứ hai 320 và anten phát thứ n ở thiết bị không dây thứ nhất 310), thiết bị nghe lén 330 vẫn không thể sử dụng giá trị h_n để thu được khóa mật mã chính xác. Ví dụ, ngay cả khi thiết bị nghe lén 330 biết về kênh không dây nghịch đảo giữa thiết bị không dây thứ nhất 310 và thiết bị không dây thứ hai 320, thiết bị nghe lén 330 chỉ có quyền truy cập vào tổng có trọng số

$\frac{\sum_n \theta_n a_n g_n}{\sum_n \theta_n g_n}$ và không thể ước lượng khóa mật mã $\frac{\sum_n a_n}{n}$ mà không biết về các giá trị của các hệ số riêng.

Nói cách khác, để ước lượng chính xác khóa mật mã là $\frac{\sum_n a_n}{n}$, thiết bị nghe lén 330 sẽ phải ước lượng chính xác mỗi trong số θ_n , a_n , và h_n một cách riêng rẽ, còn bộ thu dự kiến (thiết bị không dây thứ hai 320) có thể sử dụng một anten thu duy nhất để ước lượng duy nhất tổng có trọng số, để thu được khóa mật mã chính xác dựa trên chùm kết hợp một cách nhất quán tại vị trí không gian của thiết bị không dây thứ hai 320. Thiết bị nghe lén 330 sẽ phải sử dụng dây anten thu tức là tối thiểu bằng số lượng anten phát được dùng ở thiết bị không dây thứ nhất 310 để xây dựng một cách rõ ràng tổng dựa trên các ước lượng riêng về θ_n , a_n , và h_n . Việc này sẽ cực kỳ tốn kém đối với nhiều kẻ nghe lén tiềm ẩn, nhất là khi thiết bị không dây thứ nhất 310 là trạm gốc sóng milimet sử dụng 64, 128 hoặc 256 anten phát. Ngay cả khi thiết bị nghe lén 330 sử dụng dây anten thu đủ lớn (ví dụ, N anten thu), thiết bị nghe lén 330 cần phải tính toán các hệ số của ma trận $N \times N$ để ước lượng riêng θ_n , a_n , và h_n . Ví dụ, giả sử thiết bị nghe lén 330 thu được tín hiệu không tạp âm và số lượng anten thu và phát bằng nhau, tín hiệu nhận được tại anten thứ m của thiết bị nghe lén 330 là:

$$y_{Eve,m} = \sum_n g_{m,n} \theta_n (x + a_n |x|^2 x)$$

trong đó $g_{m,n}$ là phản hồi kênh giữa anten phát thứ n ở thiết bị không dây thứ nhất 310 và anten thu thứ m ở thiết bị nghe lén 330, có thể được viết dưới dạng ma trận như sau:

$$y_{Eve} = G(x + \underline{a}|x|^2 x)$$

trong đó $\underline{a} = [a_0, \dots, a_{(Tx-1)}]^T$ và G là ma trận MIMO (ví dụ, được điều hướng chùm sóng) với phần tử $g_{m,n} \theta_n$ ở hàng thứ m và cột thứ n giữa thiết bị không dây thứ nhất 310 và thiết bị nghe lén 330. Trong trường hợp này, thiết bị nghe lén 330 chỉ có thể ước lượng:

$$G^{-1} y_{Eve} = (x + \underline{a}|x|^2 x)$$

và thiết bị nghe lén 330 chỉ có thể ước lượng chính xác khóa mật mã nếu \underline{a} được ước lượng một cách hoàn hảo, việc này thực tế là không thể do các yêu cầu về tỷ lệ tín hiệu trên nhiễu (signal-to-noise ratio - SNR). Ví dụ, ngoài việc yêu cầu số lượng anten thu bằng

hoặc nhiều hơn số lượng anten phát được dùng ở thiết bị không dây thứ nhất 310, việc ước lượng G là rất khó khi có nhiều anten phát do các giới hạn ngân sách liên kết. Ngược lại, bộ thu dự kiến (thiết bị không dây thứ hai 320) không cần ước lượng các phần tử của H ma trận kênh vì tích θ_n và h_n đơn giản hóa thành một (1), dựa trên chùm được lái hướng về vị trí không gian của bộ thu dự kiến. Tương tự, giới hạn ngân sách nhiều và liên kết có thể ngăn không cho thiết bị nghe lén 330 ước lượng chính xác tất cả các phần tử \underline{a} vì việc ước lượng của các phần tử riêng trên mỗi anten yêu cầu SNR ở thiết bị nghe lén 330 là $20 \log_{10}(Tx)$ cao hơn SNR ở thiết bị không dây thứ hai 320, trong đó Tx là số lượng anten phát được dùng bởi thiết bị không dây thứ nhất 310 (ví dụ, giả sử rằng 128 anten phát được thiết bị không dây thứ nhất 310 sử dụng, SNR ở thiết bị nghe lén 330 sẽ cần khoảng 40dB cao hơn so với SNR ở thiết bị không dây thứ hai 320, mà trên thực tế là không thể đạt được). Cụ thể, SNR phải cao hơn ở thiết bị nghe lén 330 vì thiết bị nghe lén 330 không nhận được độ lợi điều hướng chùm sóng mà thiết bị không dây thứ hai 320 trải qua do các tín hiệu kết hợp một cách nhất quán tại vị trí không gian của thiết bị không dây thứ hai 320.

Do đó, vì thiết bị nghe lén 330 không thể ước lượng hoặc theo cách khác thu được khóa mật mã, nên khóa mật mã có thể được dùng để bảo mật một hoặc nhiều cuộc truyền thông giữa thiết bị không dây thứ nhất 310 và thiết bị không dây thứ hai 320. Ví dụ, theo một số khía cạnh, thiết bị không dây thứ nhất 310 có thể sử dụng khóa mật mã để mã hóa thông tin cần truyền cho thiết bị không dây thứ hai 320 và thiết bị không dây thứ hai 320 có thể sử dụng khóa mật mã để giải mã thông tin nhận được từ thiết bị không dây thứ nhất 310. Tương tự, thiết bị không dây thứ hai 320 có thể sử dụng khóa mật mã để mã hóa thông tin cần truyền cho thiết bị không dây thứ nhất 310, và thiết bị không dây thứ nhất 310 có thể sử dụng khóa mật mã để giải mã thông tin nhận được từ thiết bị không dây thứ hai 320.

Ngoài ra, hoặc theo cách khác, khóa mật mã có thể được dùng làm cơ chế xác thực để kiểm tra danh tính của thiết bị truyền. Ví dụ, vì các giá trị θ_n , a_n , và h_n được biết đến hoặc theo cách khác được tạo cấu hình ở thiết bị không dây thứ nhất 310, thiết bị không dây thứ nhất 310 có thể truyền tổng có trọng số $\frac{\sum_n \theta_n a_n h_n}{\sum_n \theta_n h_n}$ dưới dạng chữ ký kết hợp với một hoặc nhiều bản tin được truyền trong chùm đến thiết bị không dây thứ hai 320 (ví dụ, theo cách tương tự như chữ ký điện tử được tạo ra bằng cách sử dụng khóa riêng trong khóa công khai hoặc hệ mật mã không đối xứng). Theo cách này, thiết bị không dây thứ hai 320 có thể tính toán một cách độc lập tổng có trọng số dựa trên chùm được nhận qua

một hoặc nhiều anten thu, và so sánh phép tính của tổng có trọng số với chữ ký nhận được từ thiết bị không dây thứ nhất 310. Theo cách này, nếu phép tính của tổng có trọng số khớp với chữ ký nhận được từ thiết bị không dây thứ nhất 310, thiết bị không dây thứ hai 320 có thể xác minh tính hợp pháp của thiết bị truyền và/hoặc phát hiện khi chùm đang được thiết bị gian lận truyền đi (ví dụ, như trong một cuộc tấn công xen giữa) nếu phép tính tổng có trọng số khác chữ ký đi kèm với cuộc truyền chùm. Hơn nữa, vì cơ chế lấy dấu hiệu đặc trưng được mô tả ở đây được dựa trên tổng có trọng số bao gồm một hoặc nhiều hệ số DPD liên quan đến pha kênh, pha điều hướng chùm sóng, và/hoặc tương tự, thiết bị không dây thứ hai 320 không cần phải được đặt ở tâm của chùm để tính toán chữ ký dự kiến của thiết bị không dây thứ nhất 310. Hơn nữa, vì thiết bị nghe lén 330 và thiết bị không dây thứ nhất 310 ở các vị trí không gian khác nhau, nên thiết bị nghe lén 330 không thể tạo ra chùm truyền với pha kênh h_n ngay cả khi thiết bị nghe lén 330 bằng cách nào đó thu được giá trị tổng có trọng số $\frac{\sum_n \theta_n a_n h_n}{\sum_n \theta_n h_n}$.

Theo một số khía cạnh, để tăng bảo mật qua các mức ngẫu nhiên bổ sung, thiết bị không dây thứ nhất 310 có thể tạo ra một hoặc nhiều dạng sóng để sử dụng một hoặc nhiều khiếm khuyết mà tạo ra dấu hiệu đặc trưng duy nhất của thiết bị không dây thứ nhất 310 theo cách có kiểm soát. Ví dụ, trong một số khía cạnh, thiết bị không dây thứ nhất 310 có thể tạo cấu hình hoặc theo cách khác điều khiển các giá trị cho a_n mỗi bộ khuếch đại công suất bằng cách sử dụng các mức công suất đầu vào khác nhau, các mức nguồn khác nhau, và/hoặc tương tự cho mỗi bộ khuếch đại công suất. Do đó, trong pha thiết lập khóa, thiết bị không dây thứ nhất 310 có thể truyền với các mức công suất khác nhau trên mỗi bộ khuếch đại công suất, việc này có thể dẫn đến sự kết hợp cụ thể a_n được dùng làm khóa mật mã hoặc dấu hiệu đặc trưng để xác thực vì giá trị a_n đối với bộ khuếch đại công suất cụ thể có thể thường phụ thuộc vào độ lùi công suất liên quan đến điểm bão hòa của bộ khuếch đại công suất. Ví dụ, nếu tín hiệu được truyền ở mức công suất đủ để lùi khỏi điểm bão hòa của bộ khuếch đại công suất, thì a_n có thể có giá trị nhỏ và bộ khuếch đại công suất có thể xử lý một cách tuyến tính hoặc có số hạng phi tuyến tính nhỏ. Tuy nhiên, nếu công suất được tăng đến mức tiệm cận điểm bão hòa của bộ khuếch đại công suất, thì giá trị a_n có thể tăng lên. Do đó, bằng cách thay đổi các mức công suất mà mỗi bộ khuếch đại công suất được vận hành (ví dụ, từ 0 đến mức công suất tiệm cận điểm bão hòa của bộ khuếch đại công suất), thiết bị không dây thứ nhất 310 có thể sử dụng kết hợp cụ thể a_n để

điều khiển các bộ khuếch đại công suất nào đóng góp vào việc thiết lập khóa mật mã hoặc dấu hiệu đặc trưng, phần đóng góp mà mỗi bộ khuếch đại công suất thực hiện để thiết lập khóa mật mã hoặc dấu hiệu đặc trưng, và/hoặc tương tự. Hơn nữa, kết hợp cụ thể a_n được dùng trong pha thiết lập khóa không được lặp lại trong các cuộc truyền thông bình thường giữa thiết bị không dây thứ nhất 310 và thiết bị không dây thứ hai 320, để ngăn không cho thiết bị nghe lén 330 thu được cuộc truyền thông giữa các thiết bị không dây 310, 320.

Như đã nêu trên, Fig.3 được đưa ra làm ví dụ. Các ví dụ khác có thể khác với ví dụ được mô tả liên quan đến Fig.3.

Fig.4 là sơ đồ minh họa quy trình 400 làm ví dụ được thực hiện, ví dụ, bằng thiết bị không dây, theo các khía cạnh khác nhau của sáng chế. Quy trình ví dụ 400 là ví dụ trong đó thiết bị không dây (ví dụ, trạm gốc 110, UE 120, bộ điều khiển mạng 130, thiết bị không dây 310, thiết bị không dây 320 và/hoặc tương tự) thực hiện các hoạt động để tạo ra khóa mật mã dựa ít nhất một phần vào một hoặc nhiều khiếm khuyết liên quan đến dấu hiệu đặc trưng lớp vật lý duy nhất.

Như thể hiện trên Fig.4, theo một số khía cạnh, quy trình 400 có thể bao gồm bước nhận tín hiệu được điều hướng chùm từ thiết bị truyền (khối 410). Ví dụ, thiết bị không dây (ví dụ, sử dụng anten 234, DEMOD 232, bộ dò MIMO 236, bộ xử lý nhận 238, bộ điều khiển/bộ xử lý 240, anten 252, DEMOD 254, bộ dò MIMO 256, bộ xử lý nhận 258, bộ điều khiển/bộ xử lý 280, bộ điều khiển/bộ xử lý 290, đơn vị truyền thông 294, và/hoặc tương tự) có thể nhận tín hiệu được điều hướng chùm từ thiết bị truyền, như được mô tả ở trên.

Như thể hiện thêm trên Fig.4, theo một số khía cạnh, quy trình 400 có thể bao gồm ước lượng tổng có trọng số dựa ít nhất một phần vào nhiều hệ số kết hợp với tín hiệu được điều hướng chùm, trong đó nhiều hệ số bao gồm một hoặc nhiều hệ số liên quan đến một hoặc nhiều khiếm khuyết gắn với thiết bị truyền và một hoặc nhiều hệ số phụ thuộc vào vị trí không gian của thiết bị không dây (khối 420). Ví dụ, thiết bị không dây (ví dụ, sử dụng bộ điều khiển/bộ xử lý 240, bộ điều khiển/bộ xử lý 280, bộ điều khiển/bộ xử lý 290 và/hoặc tương tự) có thể ước lượng tổng có trọng số dựa ít nhất một phần vào nhiều hệ số kết hợp với tín hiệu được điều hướng chùm, như mô tả ở trên. Theo một số khía cạnh, nhiều hệ số bao gồm một hoặc nhiều hệ số liên quan đến một hoặc nhiều khiếm khuyết gắn với thiết bị truyền và một hoặc nhiều hệ số phụ thuộc vào vị trí không gian của thiết bị không dây.

Như được trình bày thêm trên Fig.4, theo một số khía cạnh, quy trình 400 có thể bao gồm việc xác định khóa mật mã dựa ít nhất một phần vào tỷ lệ giữa nhiều hệ số trong tổng có trọng số được kết hợp với tín hiệu được điều hướng chùm (khối 430). Ví dụ, thiết bị không dây (ví dụ, sử dụng bộ điều khiển/bộ xử lý 240, bộ điều khiển/bộ xử lý 280, bộ điều khiển/bộ xử lý 290 và/hoặc tương tự) có thể xác định khóa mật mã dựa ít nhất một phần vào tỷ lệ giữa nhiều hệ số trong tổng có trọng số kết hợp với tín hiệu được điều hướng chùm, như được mô tả ở trên.

Như được trình bày thêm trên Fig.4, theo một số khía cạnh, quy trình 400 có thể bao gồm bước bảo mật một hoặc nhiều cuộc truyền thông giữa thiết bị không dây và thiết bị truyền, dựa ít nhất một phần vào khóa mật mã (khối 440). Ví dụ, thiết bị không dây (ví dụ, sử dụng anten 234, DEMOD 232, bộ dò MIMO 236, bộ xử lý nhận 238, bộ điều khiển/bộ xử lý 240, bộ xử lý truyền 220, bộ xử lý TX MIMO 230, MOD 232, anten 252, DEMOD 254, bộ dò MIMO 256, bộ xử lý nhận 258, bộ điều khiển/bộ xử lý 280, bộ xử lý truyền 264, bộ xử lý TX MIMO 266, MOD 254, bộ điều khiển/bộ xử lý 290, đơn vị truyền thông 294 và/hoặc tương tự) có thể bảo mật một hoặc nhiều cuộc truyền thông giữa thiết bị không dây và thiết bị truyền dựa ít nhất một phần vào khóa mật mã, như được mô tả ở trên.

Quy trình 400 có thể bao gồm các khía cạnh bổ sung, như một khía cạnh bất kỳ hoặc kết hợp bất kỳ của các khía cạnh được mô tả dưới đây và/hoặc liên quan đến một hoặc nhiều quy trình khác được mô tả trong bản mô tả này.

Theo khía cạnh thứ nhất, tín hiệu được điều hướng chùm kết hợp một cách nhất quán tại vị trí không gian của thiết bị không dây.

Theo khía cạnh thứ hai, một mình hoặc kết hợp với khía cạnh thứ nhất, một hoặc nhiều khiếm khuyết gắn với thiết bị truyền bao gồm các mức độ phi tuyến tính gắn với một hoặc nhiều bộ khuếch đại công suất.

Theo khía cạnh thứ ba, một mình hoặc kết hợp với một hoặc nhiều khía cạnh trong số khía cạnh thứ nhất và thứ hai, khóa mật mã dựa ít nhất một phần vào độ phi tuyến tính trung bình giữa nhiều bộ khuếch đại công suất.

Theo khía cạnh thứ tư, một mình hoặc kết hợp với một hoặc nhiều khía cạnh trong số các khía cạnh từ thứ nhất đến thứ ba, một hoặc nhiều khiếm khuyết gắn với thiết bị

truyền bao gồm băng tần bên dư phụ thuộc vào tần số được kết hợp với một hoặc nhiều bộ khuếch đại công suất.

Theo khía cạnh thứ năm, một mình hoặc kết hợp với một hoặc nhiều khía cạnh trong số các khía cạnh từ thứ nhất đến thứ tư, một hoặc nhiều khiếm khuyết kết hợp với thiết bị truyền bao gồm độ dịch tần số kết hợp với một hoặc nhiều bộ khuếch đại công suất.

Theo khía cạnh thứ sáu, một mình hoặc kết hợp với một hoặc nhiều khía cạnh trong số các khía cạnh từ thứ nhất đến thứ năm, một hoặc nhiều hệ số phụ thuộc vào vị trí không gian của thiết bị không dây bao gồm pha kênh giữa thiết bị không dây và một hoặc nhiều anten phát tại thiết bị truyền, và pha điều hướng chùm sóng được áp dụng tại mỗi anten trong số một hoặc nhiều anten phát.

Theo khía cạnh thứ bảy, một mình hoặc kết hợp với một hoặc nhiều khía cạnh trong số các khía cạnh từ thứ nhất đến thứ sáu, một hoặc nhiều hệ số liên quan đến một hoặc nhiều khiếm khuyết gắn với thiết bị truyền dựa ít nhất một phần vào các mức công suất truyền kết hợp với tín hiệu được điều hướng chùm.

Theo khía cạnh thứ tám, một mình hoặc kết hợp với một hoặc nhiều khía cạnh trong số các khía cạnh từ thứ nhất đến thứ bảy, thiết bị không dây lượng tử hóa nhiều hệ số, và khóa mật mã được xác định dựa ít nhất một phần vào nhiều hệ số đã lượng tử hóa.

Theo khía cạnh thứ chín, một mình hoặc kết hợp với một hoặc nhiều khía cạnh trong số các khía cạnh từ thứ nhất đến thứ tám, việc bảo mật một hoặc nhiều cuộc truyền thông giữa thiết bị không dây và thiết bị truyền bao gồm một hoặc nhiều trong số giải mã thông tin nhận được từ thiết bị truyền bằng cách sử dụng khóa mật mã, mã hóa thông tin được truyền đến thiết bị truyền bằng cách sử dụng khóa mật mã, hoặc xác thực danh tính của thiết bị truyền bằng cách sử dụng khóa mật mã.

Theo khía cạnh thứ mười, một mình hoặc kết hợp với một hoặc nhiều khía cạnh trong số các khía cạnh từ thứ nhất đến thứ chín, tín hiệu được điều hướng chùm bao gồm một hoặc nhiều nhân Volterra đại diện cho một hoặc nhiều khiếm khuyết gắn với thiết bị truyền.

Mặc dù Fig.4 thể hiện các khối ví dụ của quy trình 400, nhưng theo một số khía cạnh, quy trình 400 có thể bao gồm các khối bổ sung, ít khối hơn, các khối khác, hoặc các

khối được bố trí khác với các khối thể hiện trên Fig.4. Ngoài ra, hoặc theo cách khác, hai hoặc nhiều trong số các khối của quy trình 400 có thể được thực hiện song song.

Phần mô tả trên đây cung cấp sự minh họa và mô tả, nhưng không được hiểu là hết mọi khía cạnh hoặc giới hạn các khía cạnh ở dạng cụ thể được bộc lộ. Các cải biến và thay đổi có thể được thực hiện dựa trên phần bộc lộ trên đây hoặc có thể đạt được từ việc thực hành các khía cạnh này.

Như được dùng ở đây, thuật ngữ "thành phần" dự kiến được hiểu theo nghĩa rộng là phần cứng, firmware, và/hoặc tổ hợp của phần cứng và phần mềm. Như được dùng ở đây, bộ xử lý được thực thi trong phần cứng, firmware hoặc tổ hợp của phần cứng và phần mềm.

Như được dùng ở đây, việc đáp ứng ngưỡng có thể, tùy thuộc vào ngữ cảnh, chỉ giá trị lớn hơn ngưỡng, lớn hơn hoặc bằng ngưỡng, nhỏ hơn ngưỡng, nhỏ hơn hoặc bằng ngưỡng, bằng ngưỡng, không bằng ngưỡng, và/hoặc tương tự.

Rõ ràng là các hệ thống và/hoặc phương pháp, được mô tả ở đây, có thể được thực hiện theo các hình thức khác nhau của phần cứng, firmware, hoặc tổ hợp của phần cứng và phần mềm. Mã phần cứng hoặc phần mềm điều khiển chuyên dụng thực tế được dùng để thực thi các hệ thống và/hoặc phương pháp này là không giới hạn ở các khía cạnh này. Do đó, hoạt động và trạng thái của các hệ thống và/hoặc các phương pháp được mô tả ở đây mà không tham chiếu đến mã phần mềm cụ thể —nên hiểu rằng phần mềm và phần cứng có thể được thiết kế để thực thi các hệ thống và/hoặc phương pháp này dựa, ít nhất một phần, vào phần mô tả ở đây.

Mặc dù các tổ hợp cụ thể của các dấu hiệu được nêu trong các yêu cầu bảo hộ và/hoặc bộc lộ trong bản mô tả này, nhưng các tổ hợp này không được dự tính để giới hạn sự bộc lộ của các khía cạnh khác nhau. Thực tế, nhiều đặc điểm này có thể được kết hợp theo các cách không được nêu cụ thể trong yêu cầu bảo hộ và/hoặc bộc lộ trong bản mô tả. Mặc dù từng điểm yêu cầu bảo hộ phụ thuộc liệt kê dưới đây có thể phụ thuộc trực tiếp vào duy nhất một yêu cầu bảo hộ, nhưng sự bộc lộ của các khía cạnh khác nhau bao gồm từng điểm yêu cầu bảo hộ phụ thuộc kết hợp với từng điểm yêu cầu bảo hộ khác trong bộ yêu cầu bảo hộ. Cụm từ đề cập đến “ít nhất một trong” danh sách các hạng mục chi tổ hợp bất kỳ của các hạng mục này, bao gồm cả các thành phần đơn. Ví dụ, “ít nhất một trong số: a, b, hoặc c” được dự tính bao gồm a, b, c, a-b, a-c, b-c, và a-b-c, cũng như tổ hợp bất kỳ có

nhiều phần tử giống nhau (ví dụ, a-a, a-a-a, a-a-b, a-a-c, a-b-b, a-c-c, b-b, b-b-b, b-b-c, c-c, và c-c-c hoặc thứ tự khác bất kỳ của a, b, và c).

Không có phân tử, hoạt động hoặc lệnh nào được dùng ở đây nên được hiểu là quan trọng hoặc thiết yếu trừ khi được mô tả rõ như vậy. Ngoài ra, như được dùng ở đây, từ chỉ số lượng là "một" nhằm bao gồm một hoặc nhiều hạng mục, và có thể được dùng hoán đổi với từ chỉ số lượng là "một hoặc nhiều". Hơn nữa, như được dùng ở đây, thuật ngữ "tập hợp" và "nhóm" được dự kiến để bao gồm một hoặc nhiều hạng mục (ví dụ, các hạng mục liên quan, các hạng mục không liên quan, tổ hợp của các hạng mục liên quan và không liên quan, và/hoặc tương tự), và có thể được dùng hoán đổi với "một hoặc nhiều". Trường hợp chỉ có một mục định nói đến, thuật ngữ "chỉ một" hoặc từ ngữ tương tự được dùng. Ngoài ra, như được dùng trong bản mô tả này, các thuật ngữ "có" và/hoặc tương tự ý muốn nói đến các thuật ngữ không giới hạn. Ngoài ra, cụm từ "dựa vào" được dự kiến có nghĩa "dựa, ít nhất một phần, vào" trừ khi được quy định khác rõ ràng.

YÊU CẦU BẢO HỘ

1. Phương pháp truyền thông không dây được thực hiện bằng thiết bị không dây, phương pháp này bao gồm các bước:

nhận tín hiệu được điều hướng chùm từ thiết bị truyền;

ước lượng tổng có trọng số dựa ít nhất một phần vào nhiều hệ số kết hợp với tín hiệu được điều hướng chùm, trong đó nhiều hệ số bao gồm một hoặc nhiều hệ số liên quan đến một hoặc nhiều khiếm khuyết gắn với thiết bị truyền và một hoặc nhiều hệ số phụ thuộc vào vị trí không gian của thiết bị không dây;

xác định khóa mật mã dựa ít nhất một phần vào tỷ lệ giữa nhiều hệ số trong tổng có trọng số được kết hợp với tín hiệu được điều hướng chùm; và

bảo mật một hoặc nhiều cuộc truyền thông giữa thiết bị không dây và thiết bị truyền dựa ít nhất một phần vào khóa mật mã.

2. Phương pháp theo điểm 1, trong đó tín hiệu được điều hướng chùm kết hợp một cách nhất quán tại vị trí không gian của thiết bị không dây.

3. Phương pháp theo điểm 1, trong đó một hoặc nhiều khiếm khuyết gắn với thiết bị truyền bao gồm mức độ phi tuyến tính kết hợp với một hoặc nhiều bộ khuếch đại công suất.

4. Phương pháp theo điểm 1, trong đó khóa mật mã dựa ít nhất một phần vào độ phi tuyến tính trung bình giữa nhiều bộ khuếch đại công suất.

5. Phương pháp theo điểm 1, trong đó một hoặc nhiều khiếm khuyết gắn với thiết bị truyền bao gồm các băng tần bên dư phụ thuộc vào tần số được kết hợp với một hoặc nhiều bộ khuếch đại công suất.

6. Phương pháp theo điểm 1, trong đó một hoặc nhiều khiếm khuyết gắn với thiết bị truyền bao gồm các độ dịch tần số liên quan đến một hoặc nhiều bộ khuếch đại công suất.

7. Phương pháp theo điểm 1, trong đó một hoặc nhiều hệ số phụ thuộc vào vị trí không gian của thiết bị không dây bao gồm pha kênh giữa thiết bị không dây và một hoặc nhiều anten phát tại thiết bị truyền, và pha điều hướng chùm sóng được áp dụng tại mỗi anten trong số một hoặc nhiều anten phát.

8. Phương pháp theo điểm 1, trong đó một hoặc nhiều hệ số liên quan đến một hoặc nhiều khiếm khuyết gắn với thiết bị truyền được dựa ít nhất một phần vào mức công suất truyền liên quan đến tín hiệu được điều hướng chùm.

9. Phương pháp theo điểm 1, phương pháp này còn bao gồm bước lượng tử hóa nhiều hệ số, trong đó khóa mật mã được xác định dựa ít nhất một phần vào nhiều hệ số đã lượng tử hóa.

10. Phương pháp theo điểm 1, trong đó bước bảo mật một hoặc nhiều cuộc truyền thông giữa thiết bị không dây và thiết bị truyền bao gồm một hoặc nhiều trong số giải mã thông tin nhận được từ thiết bị truyền bằng cách sử dụng khóa mật mã, mã hóa thông tin được truyền đến thiết bị truyền bằng cách sử dụng khóa mật mã, hoặc xác thực danh tính của thiết bị truyền bằng cách sử dụng khóa mật mã.

11. Phương pháp theo điểm 1, trong đó tín hiệu được điều hướng chùm bao gồm một hoặc nhiều nhân Volterra đại diện cho một hoặc nhiều khiếm khuyết gắn với thiết bị truyền.

12. Thiết bị không dây để truyền thông không dây bao gồm:

bộ nhớ; và

một hoặc nhiều bộ xử lý ghép nối với bộ nhớ, bộ nhớ và một hoặc nhiều bộ xử lý được tạo cấu hình để:

nhận tín hiệu được điều hướng chùm từ thiết bị truyền;

ước lượng tổng có trọng số dựa ít nhất một phần vào nhiều hệ số kết hợp với tín hiệu được điều hướng chùm, trong đó nhiều hệ số bao gồm một hoặc nhiều hệ số liên quan đến một hoặc nhiều khiếm khuyết gắn với thiết bị truyền và một hoặc nhiều hệ số phụ thuộc vào vị trí không gian của thiết bị không dây;

xác định khóa mật mã dựa ít nhất một phần vào tỷ lệ giữa nhiều hệ số trong tổng có trọng số được kết hợp với tín hiệu được điều hướng chùm; và

bảo mật một hoặc nhiều cuộc truyền thông giữa thiết bị không dây và thiết bị truyền dựa ít nhất một phần vào khóa mật mã.

13. Thiết bị không dây theo điểm 12, trong đó tín hiệu được điều hướng chùm kết hợp một cách nhất quán tại vị trí không gian của thiết bị không dây.

14. Thiết bị không dây theo điểm 12 trong đó một hoặc nhiều khiếm khuyết kết hợp với thiết bị truyền bao gồm mức độ phi tuyến tính kết hợp với một hoặc nhiều bộ khuếch đại công suất.
15. Thiết bị không dây theo điểm 12, trong đó khóa mật mã dựa ít nhất một phần vào độ phi tuyến tính trung bình giữa nhiều bộ khuếch đại công suất.
16. Thiết bị không dây theo điểm 12, trong đó một hoặc nhiều khiếm khuyết gắn với thiết bị truyền bao gồm các băng tần bên dư phụ thuộc vào tần số được kết hợp với một hoặc nhiều bộ khuếch đại công suất.
17. Thiết bị không dây theo điểm 12, trong đó một hoặc nhiều khiếm khuyết gắn với thiết bị truyền bao gồm độ dịch tần số kết hợp với một hoặc nhiều bộ khuếch đại công suất.
18. Thiết bị không dây theo điểm 12, trong đó một hoặc nhiều hệ số phụ thuộc vào vị trí không gian của thiết bị không dây bao gồm pha kênh giữa thiết bị không dây và một hoặc nhiều anten phát tại thiết bị truyền, và pha điều hướng chùm sóng được áp dụng tại mỗi anten trong số một hoặc nhiều anten phát.
19. Thiết bị không dây theo điểm 12, trong đó một hoặc nhiều hệ số liên quan đến một hoặc nhiều khiếm khuyết gắn với thiết bị truyền dựa ít nhất một phần vào mức công suất truyền kết hợp với tín hiệu được điều hướng chùm.
20. Thiết bị không dây theo điểm 12, trong đó bộ nhớ và một hoặc nhiều bộ xử lý còn được tạo cấu hình để lượng tử hóa nhiều hệ số, trong đó khóa mật mã được xác định dựa ít nhất một phần vào nhiều hệ số đã lượng tử hóa.
21. Thiết bị không dây theo điểm 12, trong đó bộ nhớ và một hoặc nhiều bộ xử lý, khi bảo mật một hoặc nhiều cuộc truyền thông giữa thiết bị không dây và thiết bị truyền, được tạo cấu hình thêm để thực hiện một hoặc nhiều trong số giải mã thông tin nhận được từ thiết bị truyền bằng cách sử dụng khóa mật mã, mã hóa thông tin được truyền đến thiết bị truyền bằng cách sử dụng khóa mật mã, hoặc xác thực danh tính của thiết bị truyền bằng cách sử dụng khóa mật mã.

22. Thiết bị không dây theo điểm 12, trong đó tín hiệu được điều hướng chùm bao gồm một hoặc nhiều nhân Volterra đại diện cho một hoặc nhiều khiếm khuyết liên quan đến thiết bị truyền.

23. Phương tiện bất biến đọc được bằng máy tính lưu trữ một hoặc nhiều lệnh để truyền thông không dây, một hoặc nhiều lệnh này bao gồm:

một hoặc nhiều lệnh mà, khi được thực thi bởi một hoặc nhiều bộ xử lý của thiết bị không dây, khiến cho một hoặc nhiều bộ xử lý:

nhận tín hiệu được điều hướng chùm từ thiết bị truyền;

ước lượng tổng có trọng số dựa ít nhất một phần vào nhiều hệ số kết hợp với tín hiệu được điều hướng chùm, trong đó nhiều hệ số bao gồm một hoặc nhiều hệ số liên quan đến một hoặc nhiều khiếm khuyết gắn với thiết bị truyền và một hoặc nhiều hệ số phụ thuộc vào vị trí không gian của thiết bị không dây;

xác định khóa mật mã dựa ít nhất một phần vào tỷ lệ giữa nhiều hệ số trong tổng có trọng số được kết hợp với tín hiệu được điều hướng chùm; và

bảo mật một hoặc nhiều cuộc truyền thông giữa thiết bị không dây và thiết bị truyền dựa ít nhất một phần vào khóa mật mã.

24. Phương tiện bất biến đọc được bằng máy tính theo điểm 23, trong đó tín hiệu được điều hướng chùm kết hợp một cách nhất quán tại vị trí không gian của thiết bị không dây.

25. Phương tiện bất biến đọc được bằng máy tính theo điểm 23, trong đó một hoặc nhiều khiếm khuyết gắn với thiết bị truyền bao gồm mức độ phi tuyến tính kết hợp với một hoặc nhiều bộ khuếch đại công suất.

26. Phương tiện bất biến đọc được bằng máy tính theo điểm 23, trong đó khóa mật mã được dựa ít nhất một phần vào độ phi tuyến tính trung bình giữa nhiều bộ khuếch đại công suất.

27. Phương tiện bất biến đọc được bằng máy tính theo điểm 23, trong đó một hoặc nhiều khiếm khuyết liên quan đến việc truyền bao gồm các băng tần bên dư phụ thuộc vào tần số kết hợp với một hoặc nhiều bộ khuếch đại công suất.

28. Phương tiện bất biến đọc được bằng máy tính theo điểm 23, trong đó một hoặc nhiều khiếm khuyết gắn với thiết bị truyền bao gồm các độ dịch tần số gắn với một hoặc nhiều bộ khuếch đại công suất.

29. Phương tiện bất biến đọc được bằng máy tính theo điểm 23, trong đó một hoặc nhiều hệ số phụ thuộc vào vị trí không gian của thiết bị không dây bao gồm pha kênh giữa thiết bị không dây và một hoặc nhiều anten phát tại thiết bị truyền, và pha điều hướng chùm sóng được áp dụng tại mỗi anten trong số một hoặc nhiều anten phát.

30. Phương tiện bất biến đọc được bằng máy tính theo điểm 23, trong đó một hoặc nhiều hệ số liên quan đến một hoặc nhiều khiếm khuyết gắn với thiết bị truyền được dựa ít nhất một phần vào mức công suất truyền liên quan đến tín hiệu được điều hướng chùm.

31. Phương tiện bất biến đọc được bằng máy tính theo điểm 23, trong đó một hoặc nhiều lệnh, khi được thực thi bởi một hoặc nhiều bộ xử lý, còn khiến cho một hoặc nhiều bộ xử lý lượng tử hóa nhiều hệ số, trong đó khóa mật mã được xác định dựa ít nhất một phần vào nhiều hệ số đã lượng tử hóa.

32. Phương tiện bất biến đọc được bằng máy tính theo điểm 23, trong đó một hoặc nhiều lệnh khiến cho một hoặc nhiều bộ xử lý bảo mật một hoặc nhiều cuộc truyền thông giữa thiết bị không dây và thiết bị truyền còn khiến cho một hoặc nhiều bộ xử lý thực hiện một hoặc nhiều trong số giải mã thông tin nhận được từ thiết bị truyền bằng cách sử dụng khóa mật mã, mã hóa thông tin được truyền đến thiết bị truyền bằng cách sử dụng khóa mật mã, hoặc xác thực danh tính của thiết bị truyền bằng cách sử dụng khóa mật mã.

33. Phương tiện bất biến đọc được bằng máy tính theo điểm 23, trong đó tín hiệu được điều hướng chùm bao gồm một hoặc nhiều nhân Volterra đại diện cho một hoặc nhiều khiếm khuyết liên quan đến thiết bị truyền.

34. Máy truyền thông không dây bao gồm:

phương tiện nhận tín hiệu được điều hướng chùm từ thiết bị truyền;

phương tiện ước lượng tổng có trọng số dựa ít nhất một phần vào nhiều hệ số kết hợp với tín hiệu được điều hướng chùm, trong đó nhiều hệ số bao gồm một hoặc nhiều hệ số liên quan đến một hoặc nhiều khiếm khuyết gắn với thiết bị truyền và một hoặc nhiều hệ số phụ thuộc vào vị trí không gian của máy;

phương tiện xác định khóa mật mã dựa ít nhất một phần vào tỷ lệ giữa nhiều hệ số trong tổng có trọng số kết hợp với tín hiệu được điều hướng chùm; và

phương tiện bảo mật một hoặc nhiều cuộc truyền thông giữa máy và thiết bị truyền dựa ít nhất một phần vào khóa mật mã.

35. Máy theo điểm 34, trong đó tín hiệu được điều hướng chùm kết hợp một cách nhất quán tại vị trí không gian của máy.

36. Máy theo điểm 34, trong đó một hoặc nhiều khiếm khuyết gắn với thiết bị truyền bao gồm mức độ phi tuyến tính kết hợp với một hoặc nhiều bộ khuếch đại công suất.

37. Máy theo điểm 34, trong đó khóa mật mã được dựa ít nhất một phần vào độ phi tuyến tính trung bình giữa nhiều bộ khuếch đại công suất.

38. Máy theo điểm 34, trong đó một hoặc nhiều khiếm khuyết gắn với thiết bị truyền bao gồm các băng tần bên dư phụ thuộc vào tần số kết hợp với một hoặc nhiều bộ khuếch đại công suất.

39. Máy theo điểm 34, trong đó một hoặc nhiều khiếm khuyết gắn với thiết bị truyền bao gồm các độ dịch tần số kết hợp với một hoặc nhiều bộ khuếch đại công suất.

40. Máy theo điểm 34, trong đó một hoặc nhiều hệ số phụ thuộc vào vị trí không gian của máy bao gồm pha kênh giữa máy và một hoặc nhiều anten phát tại thiết bị truyền, và pha điều hướng chùm sóng được áp dụng tại mỗi anten trong số một hoặc nhiều anten phát.

41. Máy theo điểm 34, trong đó một hoặc nhiều hệ số liên quan đến một hoặc nhiều khiếm khuyết gắn với thiết bị truyền được dựa ít nhất một phần vào mức công suất truyền kết hợp với tín hiệu được điều hướng chùm.

42. Máy theo điểm 34 còn bao gồm phương tiện lượng hóa nhiều hệ số, trong đó khóa mật mã được xác định dựa ít nhất một phần vào nhiều hệ số đã lượng tử hóa.

43. Máy theo điểm 34, trong đó phương tiện bảo mật một hoặc nhiều cuộc truyền thông giữa máy và thiết bị truyền bao gồm một hoặc nhiều phương tiện trong số phương tiện giải mã thông tin nhận được từ thiết bị truyền bằng cách sử dụng khóa mật mã, phương tiện mã hóa thông tin được truyền đến thiết bị truyền bằng cách sử dụng khóa mật mã, hoặc phương tiện xác thực danh tính của thiết bị truyền bằng cách sử dụng khóa mật mã.

44. Máy theo điểm 34, trong đó tín hiệu được điều hướng chùm bao gồm một hoặc nhiều nhân Volterra đại diện cho một hoặc nhiều khiếm khuyết gắn với thiết bị truyền.

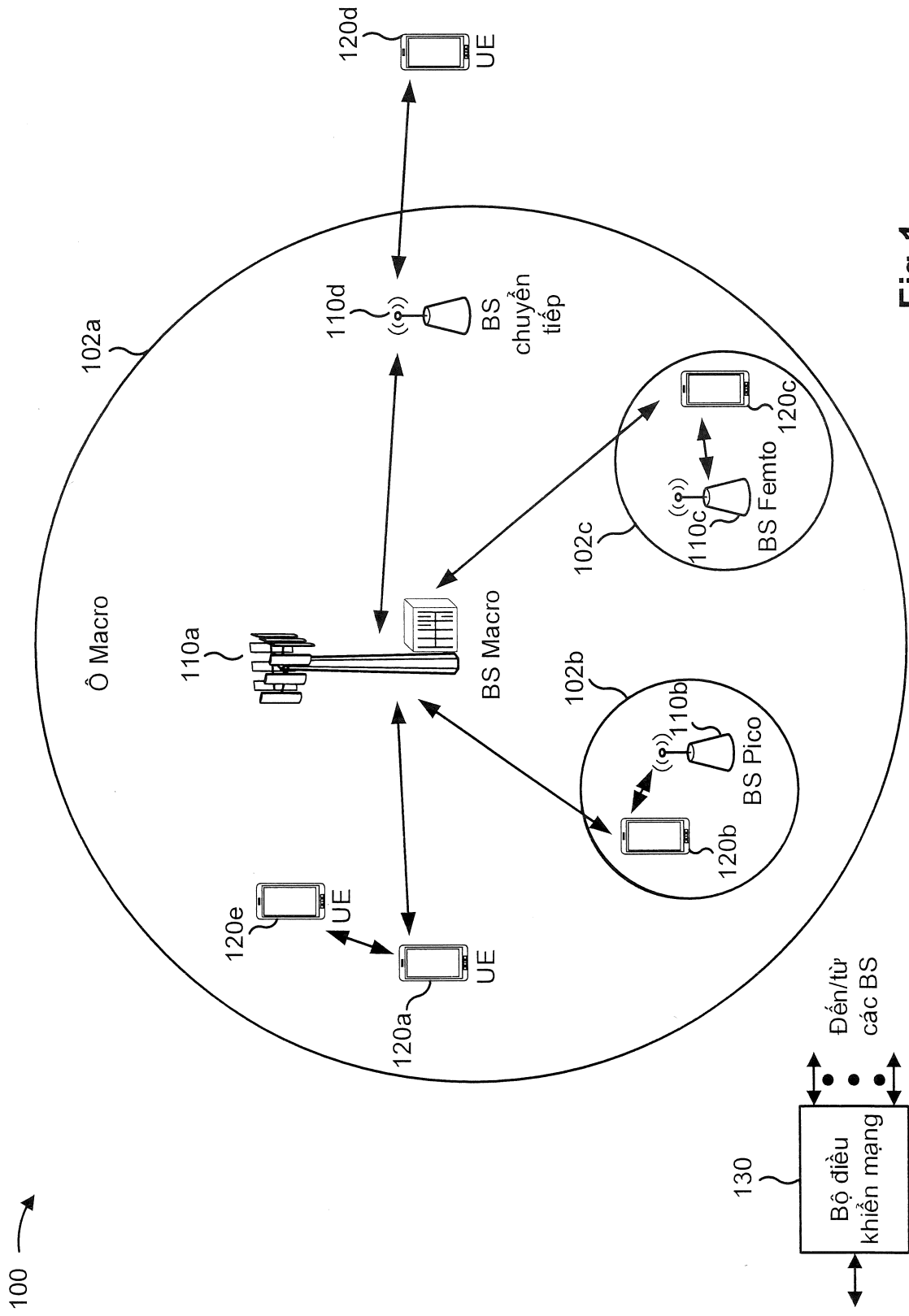


Fig.1

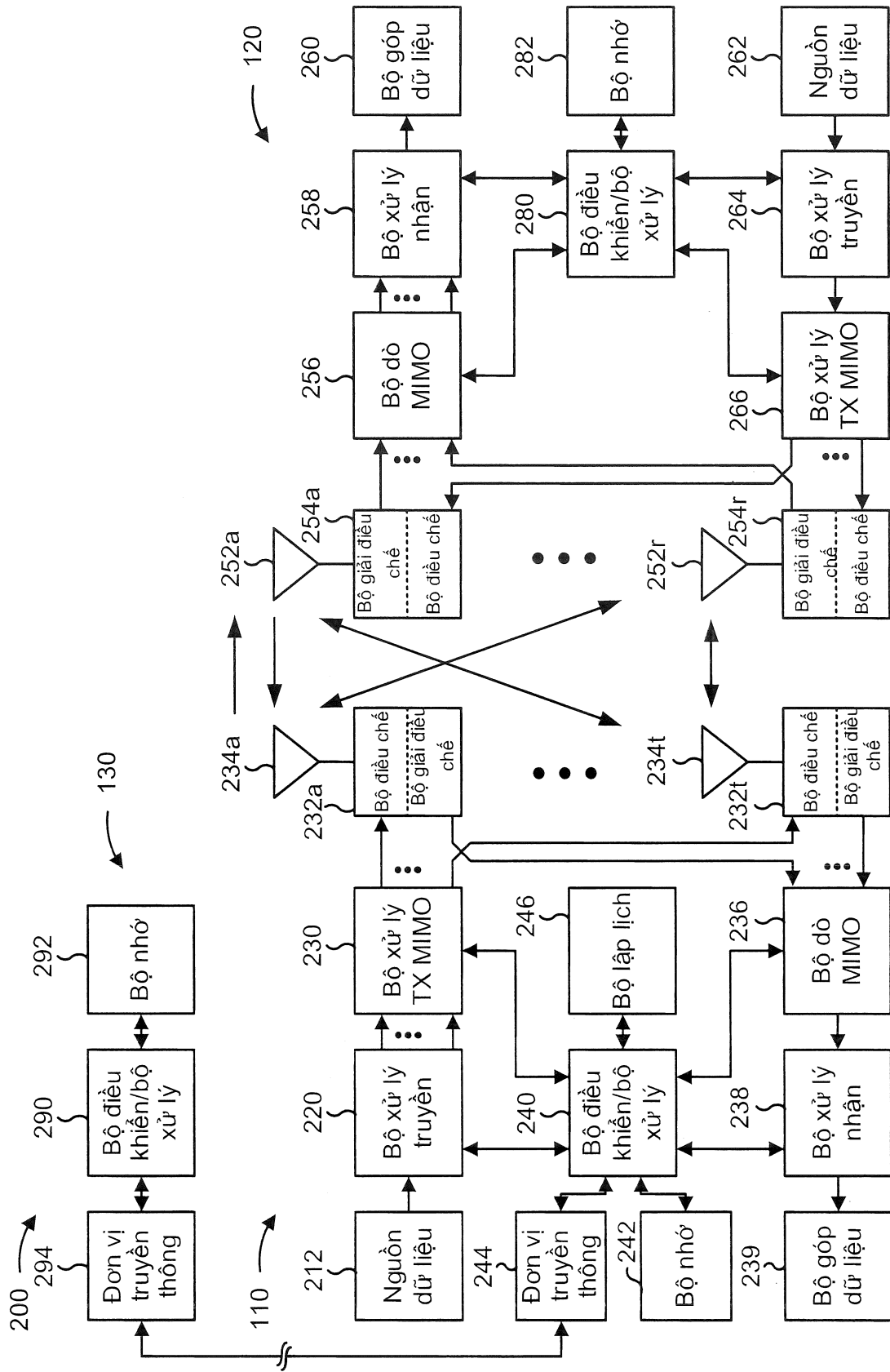


Fig.2

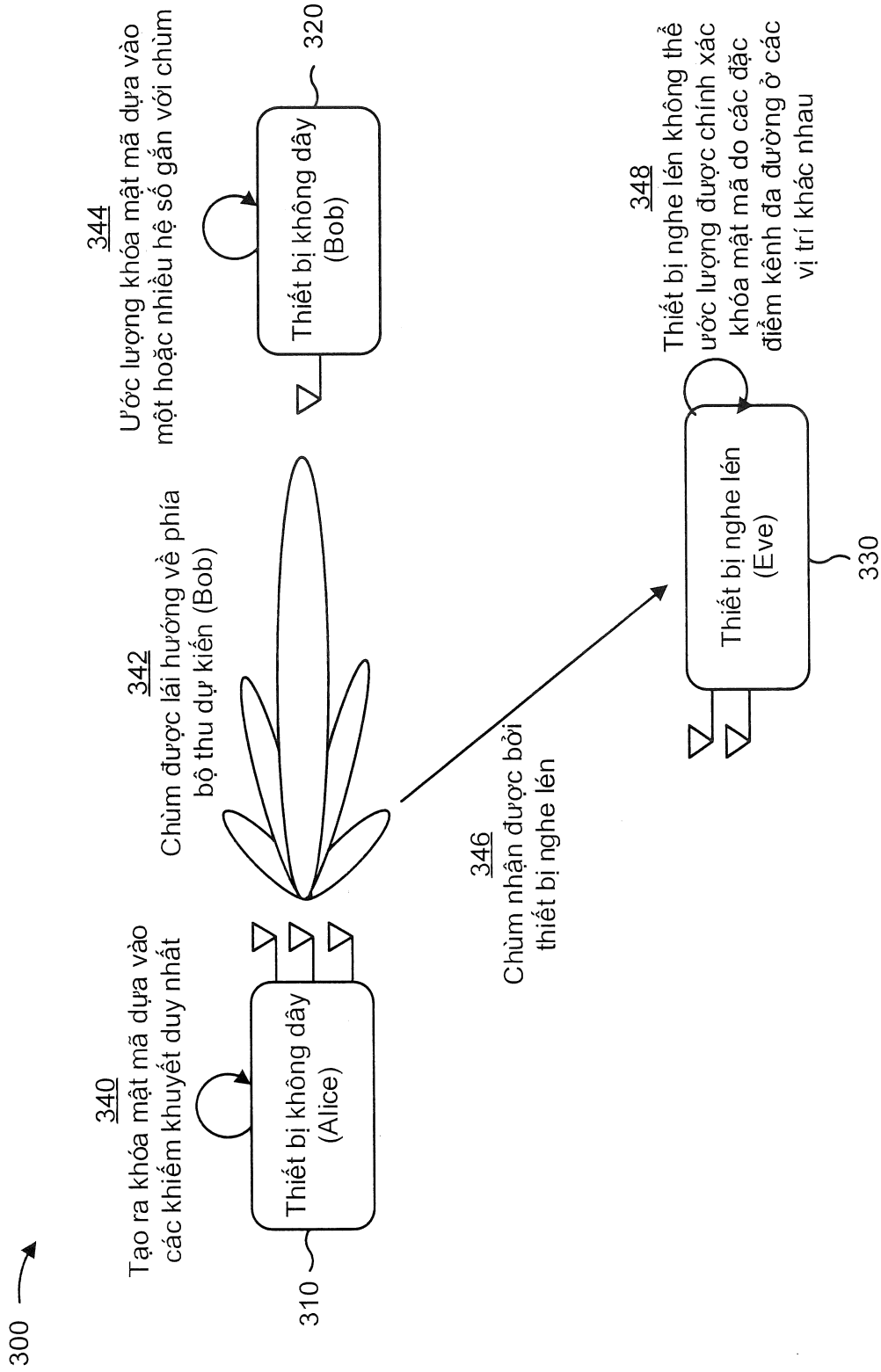


Fig.3

400 →

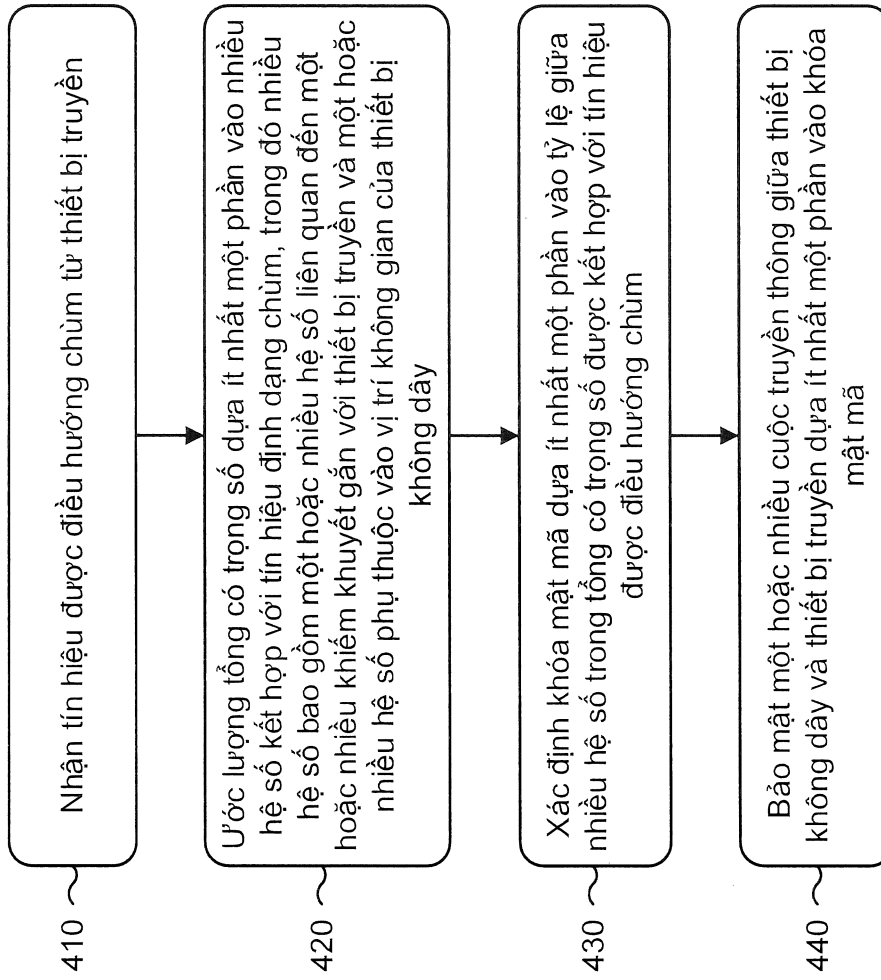


Fig. 4