(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ

(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ

(11) **1-0036499**

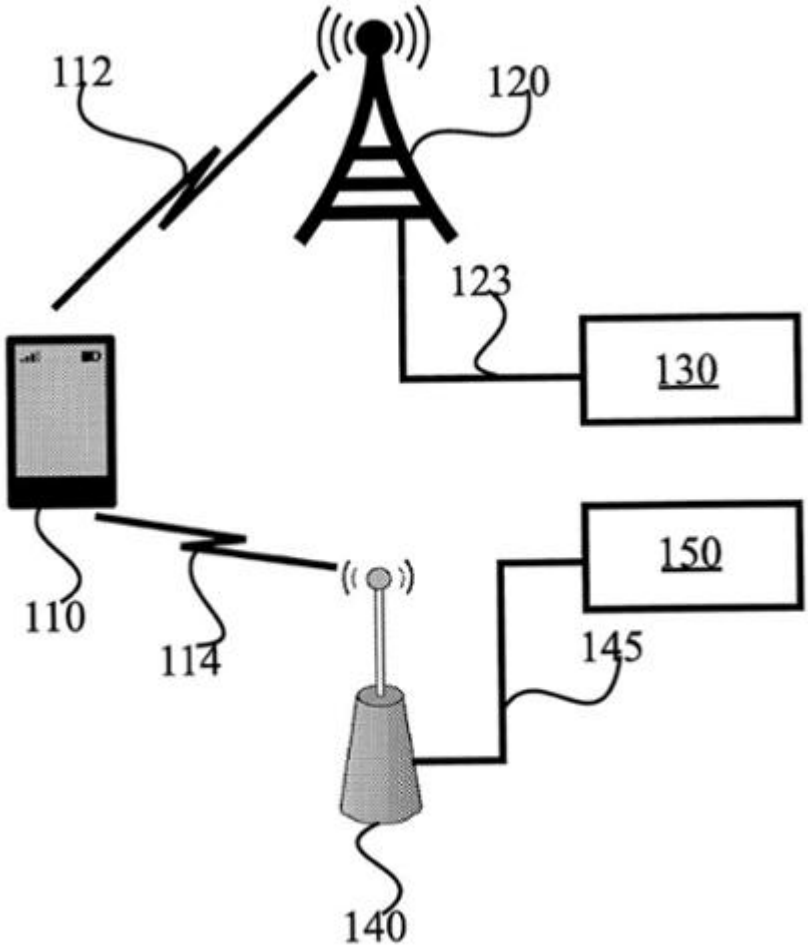
(51)[7] **H04L 9/32**; H04W 12/06; G06F 21/44; H04L 9/18

(13) **B**

(21) 1-2018-02017
(22) 16/10/2015
(86) PCT/FI2015/050701 16/10/2015
(87) WO 2017/064361 20/04/2017
(45) 25/07/2023 424
(43) 25/09/2018 366A
(73) Nokia Technologies Oy (FI)
Karaportti 3, FI-02610 Espoo, Finland
(72) KOSKIMIES, Olli Oskari (FI).
(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) THIẾT BỊ VÀ PHƯƠNG PHÁP XÁC THỰC TIN NHẮN VÀ VẬT GHI

(57) Sáng chế đề cập đến thiết bị bao gồm ít nhất một lõi xử lý, ít nhất một bộ nhớ bao gồm mã chương trình máy tính, ít nhất một bộ nhớ và mã chương trình máy tính được tạo cấu hình để, bằng ít nhất một lõi xử lý, làm cho thiết bị ít nhất thực hiện biên dịch, từ thông tin được bao gồm trong tin nhắn nhận được trong thiết bị, chuỗi bit bảo vệ, chuỗi bit bảo vệ này bao gồm phần thứ nhất và phần thứ hai, nhận dạng người gửi tin nhắn dựa trên việc nhận dạng khóa bảo mật mà giải mã phần thứ nhất thành chuỗi bit gốc được bao gồm trong tin nhắn, và xác minh chuỗi bit bảo vệ đã được làm tăng so với chuỗi bit bảo vệ trong tin nhắn trước đó từ cùng người gửi.


112
120
123
130
150
110
114
145
140

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực xác thực tin nhắn, ví dụ trong môi trường không dây.

Tình trạng kỹ thuật của sáng chế

Trong truyền thông điện tử, như truyền thông điện tử nối dây hoặc không dây, việc đảm bảo tính xác thực của tin nhắn có thể rất quan trọng. Ví dụ, khi truyền thông thông tin nhạy cảm, như thông tin liên quan đến sức khỏe, tài chính cá nhân, truyền thông cá nhân, những kế hoạch của doanh nghiệp, những kết quả tài chính của doanh nghiệp chưa được công bố hoặc thông tin về tính bảo mật công cộng, mà tính xác thực của tin nhắn có thể là quan trọng. Hơn nữa, ngay cả khi khi truyền thông chỉ để, ví dụ, mở các cửa được khóa bằng điện, thì sự xác thực của nguồn gốc gói tin có thể là quan trọng trong việc ngăn ngừa những người không được phép không đi qua những cửa này.

Để bảo vệ chống lại tấn công phát lại, trong đó kẻ tấn công ghi lại gói tin đã truyền thông và sau đó tái tạo lại gói tin này, bộ đếm hoặc dấu thời gian có thể được sử dụng. Ví dụ, khi mà cửa được khóa bằng điện được mở bằng cách truyền một gói tin phù hợp, trang bị cho gói tin này với bộ đếm hoặc dấu thời gian giúp bảo vệ chống lại việc phát lại các tin nhắn đã được ghi, do tin nhắn được phát lại sẽ bao gồm dấu thời gian cũ, cho phép vừa phát hiện việc cố tình lừa gạt vừa loại bỏ gói tin được phát lại.

Để bảo vệ chống lại gói tin giả mạo, ví dụ, gói tin đã ghi lại được sửa đổi để tạo ra dấu thời gian mới hơn được bao gồm trong gói tin này, các gói tin đã truyền thông có thể bao gồm các giá trị hàm băm. Trong những trường hợp này, hàm băm có thể được dẫn xuất từ các nội dung của gói tin, bao gồm dấu thời gian, và bí mật được chia sẻ giữa bộ phát và người nhận. Việc thay đổi dấu thời gian sẽ làm cho hàm băm không còn tương ứng với các nội dung của gói tin, cho phép phát hiện sự giả mạo bằng cách tái dẫn xuất hàm băm tại đầu bộ thu và so sánh hàm băm đã tái dẫn xuất này với hàm băm được bao gồm trong tin nhắn. Kẻ tấn công không sở hữu bí mật được chia sẻ này sẽ không biết cách thay đổi giá trị hàm băm được bao gồm trong gói tin đã ghi lại như vậy để làm cho giá trị hàm băm này trùng khớp với dấu thời gian đã thay đổi.

Hàm băm có thể được dẫn xuất bằng cách sử dụng, ví dụ, thuật toán hàm băm mật mã như thuật toán hàm băm bảo mật 1, SHA-1. SHA-1 xuất ra giá trị hàm băm có 160 bit làm một đầu ra.

Bản chất kỹ thuật của sáng chế

Sáng chế được xác định bởi các chỉ báo trong các điểm yêu cầu bảo hộ độc lập. Một số phương án cụ thể được xác định trong các điểm yêu cầu bảo hộ phụ thuộc.

Theo khía cạnh thứ nhất, sáng chế đề xuất thiết bị bao gồm ít nhất một lõi xử lý, ít nhất một bộ nhớ bao gồm mã chương trình máy tính, ít nhất một bộ nhớ và mã chương trình máy tính này được tạo cấu hình để, bằng ít nhất một lõi xử lý, làm cho thiết bị ít nhất thực hiện biên dịch, từ thông tin được bao gồm trong tin nhắn nhận được trong thiết bị, một chuỗi bit bảo vệ, chuỗi bit bảo vệ này bao gồm phần thứ nhất và phần thứ hai, nhận dạng người gửi tin nhắn dựa trên việc nhận dạng một khóa bảo mật mà giải mã phần thứ nhất thành chuỗi bit gốc được bao gồm trong tin nhắn, và xác minh chuỗi bit bảo vệ đã được làm tăng so với chuỗi bit bảo vệ trong tin nhắn trước đó từ cùng một người gửi.

Theo khía cạnh thứ hai, sáng chế đề xuất thiết bị bao gồm ít nhất một lõi xử lý, ít nhất một bộ nhớ bao gồm mã chương trình máy tính, ít nhất một bộ nhớ và mã chương trình máy tính này được tạo cấu hình để, bằng ít nhất một lõi xử lý, làm cho thiết bị ít nhất thực hiện biên dịch tin nhắn để truyền, tin nhắn này bao gồm chuỗi bit bảo vệ được bố trí trong phần thứ nhất và phần thứ hai, lựa chọn chuỗi bit bảo vệ bằng cách làm tăng chuỗi bit bảo vệ đã sử dụng trước đây, và mã hóa, sử dụng khóa bảo mật, phần thứ nhất và phần thứ nhất này bao gồm trong tin nhắn ở cả hai dạng mã hóa và chưa mã hóa.

Theo khía cạnh thứ ba, sáng chế đề xuất phương pháp bao gồm các bước: biên dịch, từ thông tin được bao gồm trong tin nhắn nhận được trong một thiết bị, một chuỗi bit bảo vệ, chuỗi bit bảo vệ này bao gồm phần thứ nhất và phần thứ hai, nhận dạng người gửi tin nhắn dựa trên việc nhận dạng khóa bảo mật mà sử dụng để giải mã phần thứ nhất thành chuỗi bit gốc được bao gồm trong tin nhắn, và xác minh chuỗi bit bảo vệ đã được làm tăng so với chuỗi bit bảo vệ trong tin nhắn trước đó từ cùng một người gửi.

Theo khía cạnh thứ tư, sáng chế đề xuất phương pháp bao gồm các bước: biên dịch tin nhắn để truyền, tin nhắn này bao gồm chuỗi bit bảo vệ được bố trí trong phần

thứ nhất và phần thứ hai, lựa chọn chuỗi bit bảo vệ bằng cách làm tăng chuỗi bit bảo vệ đã sử dụng trước đây, mã hóa, sử dụng khóa bảo mật, phần thứ nhất và phần thứ nhất này được bao gồm trong tin nhắn ở cả hai dạng mã hóa và chưa mã hóa

Theo khía cạnh thứ năm, sáng chế đề xuất thiết bị bao gồm các phương tiện để biên dịch, từ thông tin được bao gồm trong tin nhắn nhận được trong thiết bị, chuỗi bit bảo vệ, chuỗi bit bảo vệ này bao gồm phần thứ nhất và phần thứ hai, các phương tiện để nhận dạng người gửi tin nhắn dựa trên việc nhận dạng khóa bảo mật mà sử dụng để giải mã phần thứ nhất thành chuỗi bit gốc được bao gồm trong tin nhắn, và các phương tiện để xác minh chuỗi bit bảo vệ đã được làm tăng so với chuỗi bit bảo vệ trong tin nhắn trước đó từ cùng người gửi.

Theo khía cạnh thứ sáu, sáng chế đề xuất thiết bị bao gồm các phương tiện để biên dịch tin nhắn để truyền, tin nhắn bao gồm chuỗi bit bảo vệ được bố trí trong phần thứ nhất và phần thứ hai, các phương tiện để lựa chọn chuỗi bit bảo vệ bằng cách làm tăng chuỗi bit bảo vệ đã sử dụng trước đây, các phương tiện để mã hóa, sử dụng khóa bảo mật, phần thứ nhất và các phương tiện để đưa vào trong tin nhắn phần thứ nhất ở cả hai dạng mã hóa và chưa mã hóa.

Theo khía cạnh thứ bảy, sáng chế đề xuất phương tiện cố định đọc được bằng máy tính có tập hợp các lệnh đọc được bằng máy tính được lưu trữ trên các phương tiện này mà, khi được thực thi bằng ít nhất một bộ xử lý, sẽ làm cho thiết bị ít nhất thực hiện biên dịch, từ thông tin được bao gồm trong tin nhắn nhận được trong thiết bị, chuỗi bit bảo vệ, chuỗi bit bảo vệ này bao gồm phần thứ nhất và phần thứ hai, nhận dạng người gửi tin nhắn dựa trên việc nhận dạng khóa bảo mật mà sử dụng để giải mã phần thứ nhất thành chuỗi bit gốc được bao gồm trong tin nhắn, và xác minh chuỗi bit bảo vệ đã được làm tăng so với chuỗi bit bảo vệ trong tin nhắn trước đó từ cùng một người gửi.

Theo khía cạnh thứ tám, sáng chế đề xuất phương tiện cố định đọc được bằng máy tính mà tập hợp các lệnh đọc được bằng máy tính được lưu trữ trên các phương tiện này mà, khi được thực thi bằng ít nhất một bộ xử lý, sẽ làm cho thiết bị ít nhất thực hiện biên dịch tin nhắn để truyền, tin nhắn này bao gồm chuỗi bit bảo vệ được bố trí trong phần thứ nhất và phần thứ hai, lựa chọn chuỗi bit bảo vệ bằng cách làm tăng chuỗi bit bảo vệ đã sử dụng trước đây, mã hóa, sử dụng khóa bảo mật, phần thứ nhất phần thứ nhất này được bao gồm trong tin nhắn ở cả hai dạng mã hóa và chưa mã hóa.

Theo khía cạnh thứ chín, sáng chế đề xuất chương trình máy tính được tạo cấu hình để thực hiện phương pháp theo ít nhất một trong các khía cạnh thứ ba và thứ tư.

Mô tả vắn tắt các hình vẽ

Fig.1 minh họa hệ thống theo ít nhất một số phương án của sáng chế;

Fig.2 minh họa định dạng tin nhắn theo ít nhất một số phương án của sáng chế;

Fig.3 minh họa thiết bị ví dụ có khả năng hỗ trợ ít nhất một số phương án của sáng chế;

Fig.4 minh họa việc báo hiệu theo ít nhất một số phương án của sáng chế;

Fig.5 là lưu đồ thứ nhất minh họa phương pháp thứ nhất theo ít nhất một số phương án của sáng chế, và

Fig.6 là lưu đồ thứ hai minh họa phương pháp thứ hai theo ít nhất một số phương án của sáng chế.

Mô tả chi tiết sáng chế

Bằng cách bao gồm trong tin nhắn, chuỗi bit bảo vệ, như bộ đếm hoặc dấu thời gian, được chia thành hai phần, việc xác thực tin nhắn có thể được hỗ trợ. Cụ thể, phần thứ nhất của chuỗi bit bảo vệ có thể được tạo ra trong tin nhắn dưới dạng văn bản gốc theo cả hai định dạng chưa mã hóa và định dạng mã hóa. Phần thứ hai của chuỗi bit bảo vệ có thể được tạo ra ở nơi khác trong tin nhắn, ví dụ theo định dạng chưa mã hóa. Do vậy, bộ thu mà nó sở hữu tổ hợp các khóa bí mật có thể thử lần lượt các khóa bảo mật, để tìm ra khóa bí mật nào đã được sử dụng để mã hóa định dạng văn bản gốc của phần thứ nhất của chuỗi bit bảo vệ trong tin nhắn thành định dạng mã hóa của phần thứ nhất của chuỗi bit bảo vệ trong tin nhắn. Khóa bảo mật được nhận biết có liên hệ với mã đồng nhất của người gửi, sau đó được xem như mã đồng nhất của nút đã gửi tin nhắn. Trường địa chỉ người gửi có thể được sử dụng, ít nhất là theo từng phần, đối với chuỗi bit bảo vệ, hay nói khác đi thì trường địa chỉ người gửi có thể được thiết đặt, ít nhất là theo từng phần, thành một phần của chuỗi bit bảo vệ.

Chuỗi bit bảo vệ, cả hai phần cùng nhau, có thể tăng dần giữa các tin nhắn từ cùng một người gửi, để bảo vệ chống lại các cuộc tấn công phát lại. Việc xác thực tin nhắn có thể tiếp tục bao gồm việc kiểm tra chuỗi bit bảo vệ trong tin nhắn, bao gồm cả

hai phần, được tăng lên lên tương ứng với một phần trước, ví dụ như một tin nhắn liên tiếp trước liền kề, từ cùng một người nhận. Ở đây, thuật ngữ tăng dần cũng có thể, nếu có, cũng đề cập đến sự giảm dần, cả hai ví dụ về làm tăng.

Fig.1 minh họa một hệ thống phù hợp với ít nhất một số phương án của sáng chế. Hệ thống trên Fig.1 bao gồm thiết bị 110, có thể bao gồm thiết bị khóa điện, thiết bị cá nhân, điện thoại di động, điện thoại thông minh, thiết bị phablet, máy tính bảng, máy tính xách tay, máy tính để bàn hoặc loại thiết bị phù hợp khác, ví dụ. Thiết bị 110 có thể được tạo cấu hình để truyền tải tin nhắn. Các tin nhắn như vậy có thể được định dạng theo một lược đồ được xác định trước, ví dụ, thành các cấu trúc dữ liệu bao gồm một hoặc nhiều trường bit. Các trường bit có thể có độ dài được xác định trước, ví dụ 32 bit, 8 bit hoặc 160 bit. Các trường bit có thể có độ dài khác nhau.

Các tin nhắn được truyền từ thiết bị 110 có thể đến đích của chúng thông qua giao diện vô tuyến 112 và trạm gốc 120 chẳng hạn. Trong ví dụ được minh họa, trạm gốc 120 được bố trí để hoạt động theo tiêu chuẩn truyền thông di động, hoặc công nghệ, chẳng hạn như, phát triển lâu dài, LTE, đa truy cập phân chia theo mã băng rộng, WCDMA hoặc tiêu chuẩn tạm thời 95, IS- 95. Giao diện vô tuyến 112 được bố trí theo công nghệ tương tự như trạm gốc 120. Nơi được truyền qua giao diện vô tuyến 112 và trạm gốc 120, các tin nhắn bắt nguồn từ thiết bị 110 có thể được chuyển đến người nhận 130 thông qua kết nối 123, có thể bao gồm, ví dụ, một giao diện nối dây như Ethernet hoặc giao diện không dây ít nhất một phần.

Ngoài ra, hoặc bổ sung, để nhắn tin qua trạm gốc 120, thiết bị 110 có thể được bố trí để truyền tin nhắn qua điểm truy cập 140. Trong trường hợp này, tin nhắn được chuyển đến người nhận 150 qua giao diện vô tuyến 114, điểm truy cập 140 và kết nối 145. Kết nối 145 có thể là nối dây hoặc ít nhất là một phần không dây. Giao diện vô tuyến 114 và điểm truy cập 140 có thể được tạo cấu hình để hoạt động theo công nghệ không di động, chẳng hạn như Bluetooth, Bluetooth năng lượng thấp, BTLE, mạng cục bộ không dây, WLAN hoặc khả năng tương tác toàn cầu với truy cập vi sóng, WiMAX chẳng hạn.

Các giao diện vô tuyến 112 và 114 có thể là hai chiều, nói cách khác, bao gồm một đường lên được bố trí để truyền tải thông tin từ thiết bị 110 đến trạm gốc 120 hoặc điểm truy cập 140 và bao gồm đường xuống được bố trí để truyền tải thông tin về thiết

bị 110. Kết nối 123 và/hoặc 145 tương tự như vậy có thể là hai chiều.

Người nhận 130 và người nhận 150 có thể, tùy thuộc vào phương án, là cùng một người nhận hoặc hai người nhận riêng biệt. Trong một số phương án, người nhận 130 được tích hợp vào hoặc với trạm gốc 120. Trong một số người nhận 150 được tích hợp vào hoặc với điểm truy cập 140. Người nhận 130 và/hoặc người nhận 150 có thể bao gồm máy chủ, ví dụ hoặc thiết bị điều khiển được tạo cấu hình kiểm soát một quá trình, chẳng hạn như một cơ chế mở cửa hoặc quá trình công nghiệp, ví dụ. Trong một số phương án, thiết bị 110 được tạo cấu hình để truyền thông chỉ sử dụng một công nghệ. Ví dụ, nơi thiết bị 110 bao gồm một thiết bị khóa điện, nó có thể được tạo cấu hình để truyền thông với BTLE, chỉ bằng cách gửi tin nhắn đến một thiết bị điều khiển và nhận phản hồi từ đó. Ngoài ra, hoặc cách khác, thiết bị truyền thông không dây 110 có thể được tạo cấu hình để truyền tải tin nhắn bằng kết nối nối dây.

Người nhận tin nhắn, ví dụ như người nhận 130 hoặc người nhận 140, có thể được tạo cấu hình để thực hiện các bước để đảm bảo tính bảo mật của nhắn tin giữa chính nó và người gửi, chẳng hạn như thiết bị 110. Việc đảm bảo tính bảo mật có thể bao gồm ít nhất một trong số việc sử dụng mã hóa để hiển thị nội dung tin nhắn không thể tiếp cận đối với người nghe trộm, xác minh tính xác thực của tin nhắn và bảo vệ chống lại các cuộc tấn công phát lại. Xác minh tính xác thực hoặc xác thực, một tin nhắn có thể bao gồm tăng cường độ tin cậy rằng tin nhắn được tạo bởi bộ phát chính xác. Các cuộc tấn công lặp lại bao gồm các cuộc tấn công trong đó kẻ tấn công ghi lại một tin nhắn xác thực được truyền đi, ví dụ như khi nó đi qua giao diện vô tuyến, và sau đó truyền tin nhắn được ghi lại. Vì tin nhắn được ghi lại ban đầu là xác thực và do đó có các đặc trưng của một tin nhắn xác thực, các biện pháp cụ thể có thể cần phải được thực hiện để đảm bảo tin nhắn được ghi lại không được người nhận chấp nhận.

Việc mã hóa nội dung có thể bao gồm việc cung cấp nội dung làm đầu vào cho thuật toán mã hóa và truyền nội dung được mã hóa được cung cấp từ thuật toán mã hóa làm đầu ra. Ví dụ về thuật toán mã hóa là thuật toán mã hóa đối xứng và thuật toán mã hóa khóa công khai. Ví dụ về các thuật toán mã hóa đối xứng bao gồm triple-DES và chuẩn mã hóa tiên tiến, AES, trong khi các ví dụ về thuật toán mã hóa khóa công khai bao gồm thuật toán RSA và ElGamal.

Việc xác thực có thể bao gồm việc xác minh đặc trưng xác thực của tin nhắn. Ví

dụ, nội dung của một tin nhắn có thể được báo hiệu mã hóa bằng cách sử dụng một hệ thống mật mã khóa công khai, trong đó một khóa riêng được sử dụng để ký và một khóa công khai tương ứng có thể sử dụng trong việc xác minh chữ ký. Ngoài ra, hoặc bổ sung, hàm băm có thể được sử dụng để dẫn xuất giá trị băm, như nội dung của tin nhắn và bí mật được chia sẻ, được cung cấp cho hàm băm và giá trị băm được lấy từ hàm băm làm đầu ra. Bí mật được chia sẻ có thể bao gồm khóa mã hóa bí mật trong đó khóa mã hóa bí mật được chia sẻ với người nhận tin nhắn mong muốn. Hàm băm có thể bao gồm một hàm băm mật mã, ví dụ. Giá trị băm có thể được bao gồm trong tin nhắn, cho phép người nhận tái dẫn xuất hàm băm bằng nội dung tin nhắn và bí mật được chia sẻ, để kiểm tra người gửi đã sở hữu bí mật được chia sẻ bằng cách so sánh giá trị băm được tái dẫn xuất với giá trị băm trong tin nhắn. Ví dụ về hàm băm bao gồm SHA-1, SHA-2, SHA-3 và MD5. Giá trị băm có thể được bao gồm trong toàn bộ tin nhắn, hoặc một phần. Trong trường hợp giá trị băm được bao gồm một phần, phần được bao gồm này có thể được gọi là giá trị băm đã cắt ngắn, có thể bao gồm một tập hợp con các bit của toàn bộ giá trị băm.

Bảo vệ chống lại các cuộc tấn công phát lại có thể bao gồm việc cung cấp tin nhắn bằng chuỗi bit bảo vệ, chẳng hạn như bộ đếm hoặc dấu thời gian. Dấu thời gian có thể bao gồm chỉ báo của thời gian khi tin nhắn được biên soạn hoặc gửi và xác minh dấu thời gian để bảo vệ chống lại phát lại có thể bao gồm so sánh dấu thời gian với thời gian hiện tại có sẵn cho người nhận. Trong trường hợp thời gian hiện tại trễ hơn thời gian được chỉ báo trong dấu thời gian nhiều hơn một khoảng thời gian ngưỡng, dấu thời gian có thể được coi là không xác minh. Vì việc truyền và nhận tin nhắn mất thời gian hữu hạn và đồng hồ của bộ phát và người nhận có thể không được căn chỉnh hoàn hảo, dấu thời gian có thể khác nhau theo khoảng thời gian ngưỡng từ thời điểm hiện tại và vẫn vượt qua xác minh. Trong một số phương án, người nhận được tạo cấu hình để từ chối tin nhắn từ cùng một bộ phát trong trường hợp dấu thời gian được xây dựng lại không lớn hơn dấu thời gian của tin nhắn trước đó từ cùng một bộ truyền. Dấu thời gian giống với dấu thời gian trong tin nhắn trước có thể là chỉ báo của tin nhắn được phát lại.

Trong một số phương án, trong đó dấu thời gian được tăng lên lên chỉ tương đối hiếm khi, ví dụ như một lần thứ hai, nó có thể xảy ra rằng các tin nhắn xác thực và không được phát lại liên tiếp có cùng dấu thời gian. Trong các phương án như vậy, người nhận có thể được tạo cấu hình để chấp nhận các tin nhắn như vậy. Ưu điểm của dấu thời gian

tăng dần chậm là thông tin dấu thời gian trong tin nhắn có thể được truyền tải bằng cách sử dụng các bit tương đối ít.

Dấu thời gian đầy đủ, được biểu thị dưới dạng biến nhị phân, có thể mất ít nhất 4 byte khoảng trống. Một byte là tám bit. Một giá trị băm điển hình mất 8 byte. Tổng cộng, một dấu thời gian và giá trị băm có thể lấy ít nhất 12 byte trong một tin nhắn. Việc xác minh bộ đếm có thể bao gồm việc kiểm tra xem bộ đếm đã được làm tăng từ các tin nhắn trước đó từ cùng một người gửi chưa. Trong trường hợp người nhận đã nhận được một tin nhắn từ người gửi có cùng giá trị bộ đếm, tin nhắn có thể bị từ chối như một tin nhắn được phát lại.

Trong trường hợp thiết bị 110 sử dụng định dạng tin nhắn phù hợp với sơ đồ được xác định trước khi truyền, kích thước tin nhắn tổng thể có thể được thiết lập và không thể sửa đổi được bằng thiết bị 110. Trong các phương án khác, thiết bị 110 có thể ở mức độ nào đó sửa đổi kích thước của tin nhắn. Trong trường hợp chuỗi bit bảo vệ và/hoặc giá trị băm có thể được lưu trữ trong tin nhắn bằng cách sử dụng ít bit hơn, một phần lớn hơn của tin nhắn có thể được sử dụng để truyền thông nội dung thực tế, thay vì thông tin bảo mật như dấu thời gian và giá trị băm. Ngay cả khi kích thước tin nhắn có thể được thay đổi bởi thiết bị 110, việc truyền thông ít bit tiêu thụ ít năng lượng hơn và mất ít thời gian hơn truyền thông nhiều bit hơn, thu được lợi thế so với truyền thông nhiều bit hơn.

Khi tái định dạng một định dạng tin nhắn hiện có sang một sử dụng mới, bao gồm thông tin trong định dạng tin nhắn không được chỉ báo ban đầu cho nó có thể trở thành có thể bằng cách sử dụng ít bit hơn cho chuỗi bit bảo vệ và/hoặc sử dụng giá trị băm. Ví dụ, khi một định dạng tin nhắn có nội dung không thể bị xóa hoặc thay thế, và dấu thời gian và giá trị băm, sử dụng ít bit hơn cho dấu thời gian và/hoặc sử dụng giá trị băm có thể tạo ra một khoảng trống vài bit có thể sử dụng cho mục đích mới chẳng hạn như, chẳng hạn như chỉ báo trạng thái cho biết trạng thái thiết bị 110 hoặc vị trí của thiết bị 110.

Thỉnh thoảng một tin nhắn có thể được để lại trong trường hợp nội dung cần thiết của nó có thể được truyền đi trong một tin nhắn khác. Ví dụ, nếu thay vì truyền định kỳ dữ liệu cảm biến và dữ liệu định vị trong các tin nhắn riêng biệt, dữ liệu cảm biến có thể được bao gồm trong tin nhắn định vị, có thể tiết kiệm năng lượng đáng kể nếu có thể bỏ

qua tin nhắn dữ liệu cảm biến chuyên dụng. Điều này có thể được thực hiện bằng cách giảm số bit được sử dụng cho chuỗi bit bảo vệ và/hoặc giá trị băm sử dụng trong các tin nhắn định vị. Một sửa đổi như vậy đặc biệt hữu ích khi cần có dữ liệu cảm biến và định vị ở cùng tần số, hoặc ví dụ như chu kỳ.

Trong một số phương án, một số bit được phân bổ cho một giá trị băm có thể được chọn tự động phụ thuộc vào các yêu cầu bảo mật liên quan đến tin nhắn. Ví dụ, khi yêu cầu bảo mật thấp hơn áp dụng cho một tin nhắn cụ thể, có thể sử dụng giá trị băm rút gọn, rút gọn, giải phóng một số bit khác cho nội dung tin nhắn. Trong những trường hợp này, rủi ro lớn hơn một chút là giá trị băm giả mạo sẽ vô tình đúng, tuy nhiên, theo yêu cầu bảo mật thấp hơn, điều này có thể chấp nhận được.

Sau khi chọn một chuỗi bit bảo vệ thích hợp cho một tin nhắn được truyền đi, chuỗi bit bảo vệ có thể được tách ra, khi biên dịch tin nhắn truyền trong thiết bị 110, thành hai phần, phần thứ nhất và phần thứ hai. Phần thứ nhất có thể tương ứng với một tập hợp các bit có trọng số cao nhất của chuỗi bit bảo vệ, và phần thứ hai có thể tương ứng với một tập hợp các bit có trọng số thấp nhất của chuỗi bit bảo vệ. Việc ghép nối phần thứ nhất và phần thứ hai với nhau có thể tạo ra chuỗi bit bảo vệ ban đầu trong toàn bộ. Ví dụ, phần thứ hai có thể được bao gồm trong tin nhắn trong phần phụ tải. Ví dụ: phần thứ nhất có thể được bao gồm trong tin nhắn trong phần tiêu đề. Phần thứ nhất có thể được bao gồm trong trường địa chỉ, chẳng hạn như trường tiêu đề địa chỉ người gửi, chẳng hạn như trường tiêu đề địa chỉ người gửi Bluetooth.

Thiết bị 110 có thể được tạo cấu hình thêm để mã hóa phần thứ nhất, và được bao gồm trong tin nhắn cũng là phiên bản được mã hóa của phần thứ nhất của chuỗi bit bảo vệ. Do đó, tin nhắn có thể bao gồm phần thứ nhất được mã hóa, phần thứ nhất không được mã hóa và phần thứ hai. Đối với một tin nhắn tiếp theo, chuỗi bit bảo vệ được làm tăng, ví dụ như được tăng lên lên. Khi việc làm tăng ảnh hưởng ban đầu đến các bit có trọng số thấp nhất, phần thứ nhất không bị ảnh hưởng bởi sự làm tăng, nhưng cuối cùng phần thứ hai sẽ lặp lại và khiến phần thứ nhất thay đổi, thay đổi hiệu quả địa chỉ người gửi trong tin nhắn trong các phương án được lưu trữ trong tin nhắn trong trường địa chỉ người gửi.

Người nhận có thể đã lưu trữ trong đó, hoặc có quyền truy cập vào, một bộ khóa bí mật của những người gửi khác nhau, chẳng hạn như thiết bị 110. Sau khi nhận được

tin nhắn từ người gửi, người nhận có thể cố gắng giải mã phần thứ nhất được mã hóa ban đầu bằng một trong những chìa khóa bí mật, và để so sánh phần thứ nhất được giải mã do đó được giải mã với phần thứ nhất không được mã hóa trong tin nhắn. Trong trường hợp các phần thứ nhất khớp với nhau, có nghĩa là, chúng có cùng chuỗi bit, người gửi đã sử dụng khóa bí mật thứ nhất trong mã hóa phần thứ nhất và người gửi là một nút được kết hợp với khóa bí mật thứ nhất. Nói cách khác, người nhận có thể thiết lập danh tính của người gửi. Mặt khác, trong trường hợp các phần thứ nhất không khớp, người nhận có thể giải mã phần thứ nhất được mã hóa bằng phần thứ hai của khóa bí mật và thực hiện lại so sánh, v.v. cho đến khi một khóa bí mật được tìm thấy trong số các khóa bí mật, không mã hóa phần thứ nhất được mã hóa sao cho nó khớp với phiên bản không được mã hóa của phần thứ nhất trong tin nhắn. Do đó, danh tính của người gửi có thể được thiết lập. Cách khác để giải mã phần thứ nhất được mã hóa, người nhận có thể được tạo cấu hình để tìm khóa bí mật chính xác bằng cách mã hóa phần thứ nhất không được mã hóa.

Khi danh tính của người gửi được thiết lập, các tin nhắn tiếp theo có thể được xử lý bằng cách quan sát phần thứ nhất và/hoặc phần thứ nhất được mã hóa giống như trước đây. Trường hợp người nhận xác định rằng, do sự làm tăng của chuỗi bit bảo vệ, phần thứ nhất sẽ thay đổi, người nhận có thể dẫn xuất trước phần thứ nhất được mã hóa sau đó, vì người nhận đã biết khóa bí mật chính xác và có thể dự đoán phần thứ nhất không được mã hóa. Việc dẫn xuất trước có thể bao gồm việc làm tăng phần thứ nhất lên một và sau đó mã hóa nó bằng khóa bí mật được liên kết với người gửi.

Trong một số phương án, người nhận có thể xác định rằng nó có, ít nhất là trong giây lát, khả năng xử lý dự phòng. Đáp lại việc xác định khả năng xử lý dự phòng, người nhận có thể dự đoán phần thứ nhất được mã hóa tiếp theo cho ít nhất một người gửi và tùy chọn cho tất cả người gửi mà người nhận gần đây đã nhận được ít nhất một tin nhắn hoặc người nhận đang hoạt động truyền thông. Việc dự đoán các phần thứ nhất được mã hóa có thể đặc biệt thuận lợi khi một người nhận duy nhất truyền thông với nhiều người gửi, ví dụ bằng cách nhận tin nhắn từ người gửi.

Trong trường hợp xác minh hoặc xác thực không thành công, ví dụ đáp ứng giá trị băm được dẫn xuất bởi người nhận không khớp với giá trị băm, hoặc giá trị băm đã cắt ngắn, trong tin nhắn, một tin nhắn phản hồi có thể được người nhận gửi đến người gửi, tin nhắn phản hồi bao gồm một chỉ báo của thời gian theo đồng hồ của người nhận.

Sau đó, người gửi có thể đặt thời gian theo thời gian được chỉ ra trong tin nhắn phản hồi để căn chỉnh đồng hồ hoặc nếu người gửi có thời gian chính, truyền chỉ báo thời gian chính đến người nhận để căn chỉnh đồng hồ. Các tin nhắn được sử dụng để căn chỉnh đồng hồ có thể được truyền mà không có dấu thời gian riêng biệt. Các tin nhắn được sử dụng để căn chỉnh đồng hồ có thể bao gồm một chỉ báo như đối với người nhận dự định của tin nhắn, ví dụ như thông tin nhận dạng nút. Các tin nhắn này có thể được mã hóa, ký và/hoặc cung cấp với các giá trị băm được dẫn xuất từ nội dung để ngăn chặn các cuộc tấn công dựa trên tin nhắn liên kết đồng hồ.

Nói chung, khi bắt đầu truyền thông ban đầu, một số ngẫu nhiên có thể được sử dụng làm điểm bắt đầu trong bộ đếm. Điều này có thể làm tăng độ mạnh mã hóa của giải pháp.

Ví dụ: nếu kẻ trộm có thể xác định ID Bluetooth của thẻ nội dung được gắn với một thiết bị đắt tiền bằng cách ghi lại khi thiết bị được sử dụng rõ ràng trong bệnh viện, kẻ trộm có thể tạo máy quét để xác định xem thiết bị có ở trong một phòng lưu trữ cụ thể hay không, mà không cần phải mở cửa, làm cho chúng ăn cắp thiết bị dễ dàng hơn nhiều. Do đó, danh tính của người gửi có thể được bảo vệ, chẳng hạn như, ví dụ, sử dụng các phương pháp được mô tả ở đây.

Fig.2 minh họa một định dạng tin nhắn phù hợp với ít nhất một số phương án của sáng chế. Định dạng là một gói quảng cáo Bluetooth 200. Gói 200 quảng cáo được chia thành phần mở đầu 202, từ đồng bộ 204, đơn vị dữ liệu giao thức, PDU, 206 và kiểm tra dự phòng tuần hoàn, CRC, 208. Phần mở đầu có thể là chiều dài 8 bit, ví dụ như từ đồng bộ 32 bit và bit CRC 24 bit.

PDU 206 có thể được chia nhỏ thành tiêu đề 210 có 16 bit và trường phụ tải 212 chẳng hạn. Tiêu đề 210 có thể bao gồm loại tiêu đề gói quảng cáo Bluetooth, chẳng hạn như ADV_NONCONN_IND chẳng hạn. Trường phụ tải 212 có thể được chia nhỏ thành trường AdvA tương ứng với địa chỉ Bluetooth của thiết bị quảng cáo có 48 bit, 214 và cấu trúc dữ liệu quảng cáo 216 có chiều dài thay đổi. Địa chỉ Bluetooth 214 có thể bao gồm một trường băm 218, ví dụ 24 bit, một trường prand ngẫu nhiên 220, ví dụ có 22 bit, và một trường "10" 222 có hai bit đó, ví dụ. Được bao gồm trong cấu trúc dữ liệu 216 có thể là trường 224, lưu trữ phần thứ hai của chuỗi bit bảo vệ. Phần thứ nhất của chuỗi bit bảo vệ có thể được lưu trữ ít nhất một phần trong trường prand 220, ví dụ, và

một phiên bản mã hóa của phần thứ nhất trong trường băm 218 chẳng hạn.

Trường tổng kiểm tra (checksum) 208 có thể được bỏ qua khi giá trị băm được bao gồm trong tin nhắn, vì việc kiểm tra băm có thể được sử dụng để bộc lộ lỗi bit xảy ra trong quá trình truyền, nói cách khác, hàm băm có thể hoạt động hiệu quả như một hàm tổng kiểm tra. Trong một số phương án, trường tổng kiểm tra 208 được giữ lại trong tin nhắn nhưng một hàm tổng kiểm tra khác được bỏ qua, dựa vào thay vào đó ít nhất một phần vào giá trị băm. Ví dụ, trường tổng kiểm tra 208 có thể cần phải tuân thủ một tiêu chuẩn truyền thông. Giá trị băm có thể được tính toán dựa trên khóa bí mật của thiết bị và nội dung tin nhắn, bao gồm cả địa chỉ thiết bị. Điều này có nghĩa là toàn bộ chuỗi bit bảo vệ, cả phần có trọng số thấp nhất và phần có trọng số cao nhất, có thể được bao gồm trong phép tính băm. Giá trị băm, hoặc giá trị băm cắt ngắn, có thể được bao gồm trong tin nhắn ở một vị trí thích hợp, mà không cần phải là một trường được định nghĩa rõ ràng trong một đặc tả như một trường giá trị băm. Thay vào đó, giá trị băm hoặc giá trị băm cắt ngắn có thể nằm trong trường phụ tải, ví dụ, cùng với thông tin khác.

Thay vì sử dụng bộ đếm, dấu thời gian có thể được sử dụng làm chuỗi bit bảo vệ. Dấu thời gian có thể bao gồm 4 byte, là 32 bit, ví dụ. Dấu thời gian có thể được biểu thị dưới dạng thời gian UNIX, giây kể từ tháng 1 năm 1970 chẳng hạn. Trong trường hợp này, 22 bit có trọng số cao nhất của dấu thời gian có thể được lưu trữ trong địa chỉ thiết bị và 10 bit được lưu trữ trong phụ tải tin nhắn. Sử dụng lược đồ này, địa chỉ thiết bị thay đổi cứ 17 phút một lần trong trường hợp một tin nhắn được gửi mỗi giây. Trong lược đồ này, hai tin nhắn liên tiếp có thể nhận được cùng một dấu thời gian, vì vậy người nhận phải chấp nhận các tin nhắn có dấu thời gian giống như dấu thời gian nhận được cao nhất từ cùng một người gửi, ít nhất là cho đến khi sự chênh lệch với đồng hồ treo tường tăng quá lớn.

Ví dụ trong đó chuỗi bit bảo vệ là bộ đếm, giả sử giá trị bộ đếm hiện tại của người gửi là 12345. Trong nhị phân, đó là 11000000111001. Giả sử ta gán 10 bit cho phần có trọng số thấp nhất của bộ đếm. 10 bit có trọng số thấp nhất của giá trị bộ đếm, theo dạng nhị phân, là 0000111001. Phần có trọng số cao nhất, được sử dụng làm phần ngẫu nhiên trong địa chỉ thiết bị, là 1100, do đó 22 bit của phần ngẫu nhiên trong địa chỉ thiết bị là 0000000000000000001100. Người gửi bao gồm phụ tải tin nhắn phần có trọng số thấp nhất của bộ đếm, phần thứ hai của chuỗi bit bảo vệ, 0000111001 và giá trị băm được tính từ ít nhất địa chỉ thiết bị, nội dung tin nhắn bao gồm phần có trọng số thấp nhất của

bộ đếm và khóa bí mật của thiết bị. Nếu có, nói rằng, 10 byte, là 80 bit, tổng thể có sẵn trong tin nhắn, ta sử dụng 10 bit cho bộ đếm, có nghĩa là 70 bit có thể được sử dụng cho giá trị băm, có thể được cắt ngắn. Điều này sẽ có được nhiều hơn 6 bit so với mức tối thiểu 8 byte, là 64 bit, làm giảm khả năng va chạm đáng kể.

Người nhận tin nhắn sau đó có thể kiểm tra xem địa chỉ thiết bị có nằm trong số các địa chỉ đã biết không. Nếu có, người nhận tra cứu khóa bí mật được liên kết như được mô tả ở trên. Nếu không, người nhận sẽ thử mọi khóa bí mật mà nó biết để mã hóa phần ngẫu nhiên của địa chỉ thiết bị và kiểm tra xem kết quả có khớp với phần băm của địa chỉ thiết bị hay không. Nếu có, thì người gửi là người gửi được liên kết với khóa bí mật đó. Người nhận sau đó tạo lại bộ đếm bằng cách ghép phần có trọng số cao nhất, là phần ngẫu nhiên của địa chỉ thiết bị, 00000000000000000000, với phần có trọng số thấp nhất, là bộ đếm trong phần thân tin nhắn, 0000111001, nhận được 00000000000000000011000000111001, mà là 12345 trong hệ thập phân.

Sau đó người nhận có thể tính giá trị băm giống như người gửi, sử dụng ít nhất địa chỉ thiết bị, nội dung tin nhắn bao gồm phần có trọng số thấp nhất của bộ đếm và bí mật được chia sẻ được lưu trữ cho người gửi đó và so sánh kết quả với băm giá trị trong tin nhắn. Vì tất cả các giá trị được sử dụng để tính toán băm đều giống nhau, kết quả phù hợp và tin nhắn được xác thực.

Người nhận cũng có thể xác minh toàn bộ bộ đếm, có nghĩa là phần nối của phần có trọng số cao nhất trong địa chỉ thiết bị và phần có trọng số thấp nhất trong phụ tải lớn hơn giá trị bộ đếm đã lưu cuối cùng nhận được từ cùng một người gửi, có thể cho phép chuyển qua như được mô tả trước đó. Nếu không, tin nhắn là bản phát lại hoặc sao chép và bị từ chối. Nếu có, tin nhắn được chấp nhận và giá trị bộ đếm trong tin nhắn được lưu dưới dạng giá trị bộ đếm mới cho người gửi đó.

Fig.3 minh họa một thiết bị ví dụ có khả năng hỗ trợ ít nhất một số phương án của sáng chế. Được minh họa là thiết bị 300, có thể bao gồm, ví dụ, thiết bị 110 hoặc người nhận trên Fig.1. Được bao gồm trong thiết bị 300 là bộ xử lý 310, có thể bao gồm, ví dụ, bộ xử lý đơn hoặc đa lõi trong đó một bộ xử lý lõi đơn bao gồm một lõi xử lý và một bộ xử lý đa lõi bao gồm nhiều lõi xử lý. Bộ xử lý 310 có thể bao gồm nhiều bộ xử lý. Một lõi xử lý có thể bao gồm, ví dụ, một lõi xử lý Cortex-A8 được sản xuất bởi ARM Holdings hoặc một lõi xử lý Steamroller được sản xuất bởi Advanced Micro Devices

Corporation. Bộ xử lý 310 có thể bao gồm ít nhất một bộ xử lý Qualcomm Snapdragon và/hoặc bộ xử lý Intel Atom. Bộ xử lý 310 có thể bao gồm ít nhất một mạch tích hợp dành riêng cho ứng dụng, ASIC. Bộ xử lý 310 có thể bao gồm ít nhất một mảng cổng lập trình được dạng trường, FPGA. Bộ xử lý 310 có thể là phương tiện để thực hiện các bước phương pháp trong thiết bị 300. Bộ xử lý 310 có thể được tạo cấu hình, ít nhất một phần bằng các lệnh của máy tính, để thực hiện các thao tác.

Thiết bị 300 có thể bao gồm bộ nhớ 320. Bộ nhớ 320 có thể bao gồm bộ nhớ truy cập ngẫu nhiên và/hoặc bộ nhớ vĩnh viễn. Bộ nhớ 320 có thể bao gồm ít nhất một chip RAM. Ví dụ, bộ nhớ 320 có thể bao gồm bộ nhớ trạng thái rắn, từ, quang và/hoặc bộ nhớ toàn ký. Bộ nhớ 320 có thể ít nhất một phần có thể truy cập được tới bộ xử lý 310. Bộ nhớ 320 có thể ít nhất một phần được bao gồm trong bộ xử lý 310. Bộ nhớ 320 có thể là phương tiện để lưu trữ thông tin. Bộ nhớ 320 có thể bao gồm các lệnh máy tính mà bộ xử lý 310 được tạo cấu hình để thực thi. Khi các lệnh máy tính được tạo cấu hình để khiến bộ xử lý 310 thực hiện một số hành động nhất định được lưu trữ trong bộ nhớ 320, và thiết bị 300 được tạo cấu hình để chạy theo hướng của bộ xử lý 310 sử dụng các lệnh máy tính từ bộ nhớ 320, bộ xử lý 310 và/hoặc ít nhất một lõi xử lý có thể được coi là được tạo cấu hình để thực hiện các tác vụ nhất định. Bộ nhớ 320 có thể ít nhất một phần được bao gồm trong bộ xử lý 310. Bộ nhớ 320 có thể ít nhất là một phần bên ngoài thiết bị 300 nhưng có thể truy cập vào thiết bị 300.

Thiết bị 300 có thể bao gồm bộ phát 330. Thiết bị 300 có thể bao gồm một bộ thu 340. Bộ phát 330 và bộ thu 340 có thể được tạo cấu hình để truyền và nhận, tương ứng, thông tin phù hợp với ít nhất một tiêu chuẩn di động hoặc không di động. Bộ phát 330 có thể bao gồm nhiều hơn một bộ phát. Bộ thu 340 có thể bao gồm nhiều hơn một bộ thu. Bộ phát 330 và/hoặc bộ thu 340 có thể được tạo cấu hình để hoạt động theo các tiêu chuẩn hệ thống truyền thông di động toàn cầu, GSM, đa truy cập phân chia theo mã băng rộng, WCDMA, phát triển lâu dài, LTE, IS-95, mạng cục bộ không dây, WLAN, Ethernet và/hoặc khả năng tương tác toàn cầu với truy cập vi sóng, WiMAX chẳng hạn.

Thiết bị 300 có thể bao gồm truyền thông gần trường, NFC, bộ thu phát 350. Bộ thu phát NFC 350 có thể hỗ trợ ít nhất một công nghệ NFC, chẳng hạn như NFC, Bluetooth, Wibree hoặc các công nghệ tương tự.

Thiết bị 300 có thể bao gồm giao diện người dùng, giao diện người dùng, 360.

UI 360 có thể bao gồm ít nhất một màn hình, bàn phím, màn hình cảm ứng, bộ rung được bố trí để báo hiệu cho người dùng bằng cách khiến thiết bị rung 300, loa và micrô. Người dùng có thể vận hành thiết bị 300 qua UI 360, ví dụ như mở cửa, chấp nhận cuộc gọi điện thoại, để gọi điện thoại hoặc gọi điện viđeo, duyệt Internet, quản lý tệp kỹ thuật số được lưu trữ trong bộ nhớ 320 hoặc trên đám mây có thể truy cập thông qua bộ phát 330 và bộ thu 340, hoặc thông qua bộ thu phát NFC 350 và/hoặc để chơi trò chơi, chẳng hạn.

Thiết bị 300 có thể bao gồm hoặc được bố trí để chấp nhận môđun nhận dạng người dùng 370. Môđun nhận dạng người dùng 370 có thể bao gồm, ví dụ, môđun nhận dạng thuê bao, SIM, thẻ có thể lắp đặt trong thiết bị 300. Môđun nhận dạng người dùng 370 có thể bao gồm thông tin xác định sự đăng ký của người dùng thiết bị 300. Môđun nhận dạng người dùng 370 có thể bao gồm thông tin mật mã có thể sử dụng để kiểm tra danh tính của người dùng thiết bị 300 và/hoặc để tạo điều kiện mã hóa thông tin được truyền thông và sự thanh toán của người dùng thiết bị 300 cho truyền thông được thực hiện qua thiết bị 300.

Bộ xử lý 310 có thể được trang bị bộ phát được bố trí thông tin đầu ra từ bộ xử lý 310, thông qua các dây dẫn điện bên trong thiết bị 300, đến các thiết bị khác được bao gồm trong thiết bị 300. Bộ phát này có thể bao gồm bộ phát bus nối tiếp được bố trí, ví dụ, xuất ra thông tin qua ít nhất một dây dẫn điện tới bộ nhớ 320 để lưu trữ trong đó. Ngoài một bus nối tiếp, bộ phát có thể bao gồm một bộ phát bus song song. Tương tự, bộ xử lý 310 có thể bao gồm một bộ thu được bố trí để nhận thông tin trong bộ xử lý 310, thông qua các dây dẫn điện bên trong thiết bị 300, từ các thiết bị khác được bao gồm trong thiết bị 300. Bộ thu như vậy có thể bao gồm một bộ thu bus nối tiếp được bố trí để, ví dụ, thu thông tin qua dây ít nhất một dẫn điện từ bộ thu 340 để xử lý trong bộ xử lý 310. Ngoài một bus nối tiếp, bộ thu có thể bao gồm một bộ thu bus song song.

Thiết bị 300 có thể bao gồm các thiết bị khác không được minh họa trên Fig.3. Ví dụ, khi thiết bị 300 bao gồm một điện thoại thông minh, nó có thể bao gồm ít nhất một camera kỹ thuật số. Một số thiết bị 300 có thể bao gồm một camera mặt sau và camera mặt trước, trong đó camera mặt sau có thể được dùng để chụp ảnh kỹ thuật số và camera mặt trước cho điện thoại viđeo. Thiết bị 300 có thể bao gồm cảm biến vân tay được bố trí để xác thực, ít nhất một phần, người dùng thiết bị 300. Trong một số phương án, thiết bị 300 thiếu ít nhất một thiết bị được mô tả ở trên. Ví dụ: một số thiết bị 300 có

thể thiếu bộ thu phát NFC 350 và/hoặc môđun nhận dạng người dùng 370.

Bộ xử lý 310, bộ nhớ 320, bộ phát 330, bộ thu 340, bộ thu phát NFC 350, UI 360 và/hoặc mô đun nhận dạng người dùng 370 có thể được kết nối với nhau bằng các dây dẫn điện bên trong thiết bị 300 theo nhiều cách khác nhau. Ví dụ, mỗi thiết bị nói trên có thể được kết nối riêng với một bus chính bên trong thiết bị 300, để cho phép các thiết bị trao đổi thông tin. Tuy nhiên, vì người có hiểu biết trung bình trong lĩnh vực kỹ thuật tương ứng sẽ hiểu rằng, đây chỉ là một ví dụ và tùy thuộc vào phương án, các cách kết nối khác nhau ít nhất hai trong số các thiết bị nói trên có thể được chọn mà không trệch khỏi phạm vi của sáng chế.

Fig.4 minh họa báo hiệu phù hợp với ít nhất một số phương án của sáng chế. Trên trục thẳng đứng được bố trí thiết bị 110, người nhận 150 và thiết bị 4XX. Thiết bị 110 và người nhận 150 có thể tương ứng với cấu trúc giống như trong hệ thống trên Fig.1. Thiết bị 4XX có thể là thiết bị được kiểm soát, ít nhất một phần, bởi người nhận 150. Ví dụ, thiết bị 4XX có thể bao gồm cửa bị khóa điện tử hoặc thiết bị điều khiển quá trình công nghiệp được bố trí theo chức năng, ít nhất là một phần, theo hướng nhận được từ người nhận 150.

Bước 410 bao gồm truyền, từ thiết bị 110, một tin nhắn đến người nhận 150. Tin nhắn có thể được truyền tải thông qua một phương tiện nối dây hoặc không dây thích hợp, chẳng hạn như cổng nối tiếp đa năng, USB, cáp hoặc kết nối Bluetooth. Tin nhắn này có thể bao gồm dấu thời gian cắt ngắn và/hoặc giá trị băm đã cắt ngắn, như được trình bày ở trên.

Ở bước 420, người nhận 150 xác minh tin nhắn nhận được ở bước 410. Xác minh ở bước 420 có thể bao gồm việc xác định danh tính của thiết bị 110 đã gửi tin nhắn, như mô tả ở trên và kiểm tra chuỗi bit bảo vệ phù hợp với chuỗi bit bảo vệ của ngay trước đó, tức là, tin nhắn trước đó từ thiết bị 110 trong chuỗi các tin nhắn từ thiết bị 110. Trong trường hợp chuỗi bit bảo vệ nhỏ hơn hoặc bằng chuỗi bit bảo vệ trước ngay lập tức, người nhận 150 có thể từ chối tin nhắn. Việc xác minh có thể tiếp tục bao gồm tái dẫn xuất một giá trị băm từ các nội dung của tin nhắn và bí mật được chia sẻ với thiết bị 110. Sau đó có thể kiểm tra xem giá trị băm được tái dẫn xuất có phù hợp với giá trị băm hay giá trị băm cắt ngắn được bao gồm trong tin nhắn đã nhận hay không. Trong trường hợp băm được xác minh thành công, người nhận 150 có thể có sự tin tưởng tốt rằng tin nhắn

là xác thực từ thiết bị 110 và không được phát lại.

Đáp lại việc xác minh thành công, người nhận 150 có thể, ở bước 430, lệnh cho thiết bị 4XX thực hiện một hành động, có thể là một hành động mà thiết bị 110 được yêu cầu trong tin nhắn của bước 410. Đáp ứng, ở bước 440, thiết bị 4XX thực hiện hành động.

Ở bước 450, thiết bị 110 truyền tin nhắn thứ hai đến người nhận 150. Tin nhắn có thể có các trường nội dung tương tự như tin nhắn được truyền ở bước 410. Tại thời điểm tin nhắn của bước 450 được truyền đi, đồng hồ của thiết bị 110 đã lệch so với đồng hồ ở người nhận 150, với hậu quả là khi tin nhắn được xác minh trong người nhận 150, chuỗi bit bảo vệ được xây dựng lại, trong ví dụ này là dấu thời gian, có thể thất bại so với thời gian từ đồng hồ có sẵn cho người nhận 150.

Đáp lại sự thất bại trong xác minh ở người nhận 150, một tin nhắn có thể được gửi trở lại thiết bị 110, ở bước 460, tin nhắn này bao gồm một chỉ báo của một thời gian hiện tại theo đồng hồ của người nhận 150. Thời gian của người nhận 150 được đặt làm thời gian hiện tại của thiết bị 110 ở bước 470, do đó căn chỉnh đồng hồ của thiết bị 110 với thiết bị của người nhận 150.

Fig.5 là biểu đồ lưu lượng thứ nhất minh họa phương pháp thứ nhất phù hợp với ít nhất một số phương án của sáng chế. Các bước của phương pháp được minh họa có thể được thực hiện trong thiết bị người nhận, ví dụ, hoặc trong một thiết bị điều khiển được tạo cấu hình để điều khiển hoạt động của thiết bị nhận, khi được cấy vào đó.

Bước 510 bao gồm biên dịch, từ thông tin được bao gồm trong một tin nhắn nhận được trong một thiết bị, một chuỗi bit bảo vệ, chuỗi bit bảo vệ bao gồm phần thứ nhất và phần thứ hai. Bước 520 bao gồm việc xác định người gửi tin nhắn dựa trên việc xác định một khóa bí mật giải mã phần thứ nhất thành một chuỗi bit gốc được bao gồm trong tin nhắn. Phần thứ nhất có thể xuất hiện trong tin nhắn, dưới dạng mã hóa, trong một trường dữ liệu khác với chuỗi bit văn bản tương ứng với phần thứ nhất được giải mã. Bước 530 bao gồm việc xác minh chuỗi bit bảo vệ đã được làm tăng đối với chuỗi bit bảo vệ trong một tin nhắn trước đó từ cùng một người gửi.

Fig.6 là biểu đồ dòng thứ hai minh họa phương pháp thứ hai phù hợp với ít nhất một số phương án của sáng chế. Các bước của phương pháp được minh họa có thể được thực hiện trong thiết bị người gửi, ví dụ hoặc trong thiết bị điều khiển được tạo cấu hình

để kiểm soát hoạt động của thiết bị người nhận, khi được cấy vào đó.

Một số ưu điểm nhất định có thể được cung cấp bởi các phương án khác nhau của sáng chế. Ví dụ: lượng khoảng trống cần thiết trong tin nhắn để bảo vệ phát lại có thể bị giảm, đồng thời cho phép ẩn danh thông tin người gửi tin nhắn. Việc ẩn danh cho phép tuân thủ các yêu cầu bảo vệ nghiêm ngặt hơn. Khoảng trống được tiết kiệm có thể được sử dụng trong các tin nhắn định vị để tăng sức mạnh của băm bảo vệ tính toàn vẹn, và/hoặc lưu trữ dữ liệu cảm biến trong các tin nhắn định vị, làm giảm số lượng tin nhắn cần gửi và do đó giảm tiêu thụ năng lượng và tăng tuổi thọ pin nơi thiết bị được cấp nguồn pin. Khoảng trống được tiết kiệm có thể được sử dụng để tăng độ dài của dữ liệu định vị trong tin nhắn, điều này có thể làm tăng hiệu suất định vị. Sử dụng một số phương án của sáng chế có thể cho phép thực hiện một sự cân bằng tốt giữa bảo vệ tính toàn vẹn của tin nhắn và độ mạnh xác thực, tuổi thọ pin và hiệu suất định vị.

Một ưu điểm khác của các phương án nhất định của sáng chế là các địa chỉ thiết bị ẩn danh có thể được thực hiện tương thích với đặc tả Bluetooth, để chúng có thể được xử lý bởi các thiết bị Bluetooth tuân thủ tiêu chuẩn. Điều này có thể hữu ích vì nó cho phép các hệ thống của bên thứ ba nhận ra danh tính người gửi nếu chúng được cấp phép với các khóa bí mật và danh tính của các thiết bị.

Điều này được hiểu rằng các phương án của sáng chế được bộc lộ không giới hạn ở các cấu trúc cụ thể, các bước quy trình, hoặc các vật liệu được bộc lộ trong sáng chế, nhưng được mở rộng tương đương như được công nhận bởi những người có hiểu biết trung bình trong lĩnh vực kỹ thuật tương ứng. Cũng nên hiểu rằng thuật ngữ được sử dụng trong sáng chế chỉ được sử dụng cho mục đích mô tả các phương án cụ thể và không có ý định giới hạn.

Tham chiếu xuyên suốt toàn bộ bản mô tả cho một phương án hoặc phương án có nghĩa là đặc điểm, cấu trúc hoặc đặc tính cụ thể được mô tả liên quan đến phương án được bao gồm trong ít nhất một phương án của sáng chế. Do đó, sự xuất hiện của các cụm từ "trong một phương án" hoặc "trong phương án" ở những nơi khác nhau trong toàn bộ bản mô tả không nhất thiết phải đề cập đến cùng một phương án. Trường hợp sự tham chiếu được thực hiện cho một giá trị số bằng cách sử dụng một thuật ngữ như, ví dụ, khoảng hoặc đáng kể, giá trị số chính xác cũng được bộc lộ.

Như được sử dụng ở đây, nhiều mục, phần tử cấu trúc, phần tử cấu tạo và/hoặc

vật liệu có thể được trình bày trong một danh sách chung để thuận tiện. Tuy nhiên, các danh sách này nên được hiểu là mỗi thành viên trong danh sách được xác định riêng lẻ như một thành viên riêng biệt và duy nhất. Vì vậy, không có thành viên riêng biệt nào trong danh sách như vậy nên được hiểu là tương đương chính thức với bất kỳ thành viên nào khác trong cùng một danh sách chỉ dựa trên bản trình bày của chúng trong một nhóm chung mà không có chỉ báo ngược lại. Ngoài ra, các phương án và ví dụ khác nhau của sáng chế có thể được đề cập trong sáng chế cùng với các lựa chọn thay thế cho các thành phần khác nhau của chúng. Điều này được hiểu rằng các phương án, ví dụ và các phương án thay thế này không được hiểu là tương đương chính thức với nhau, nhưng được coi là các biểu diễn riêng biệt và độc lập của sáng chế.

Hơn nữa, các dấu hiệu, cấu trúc hoặc đặc điểm được mô tả có thể được kết hợp theo bất kỳ cách phù hợp nào trong một hoặc nhiều phương án. Trong phần mô tả sau đây, nhiều chi tiết cụ thể được cung cấp, chẳng hạn như ví dụ về độ dài, độ rộng, hình dạng, v.v., để cung cấp một sự hiểu biết thấu đáo về phương án của sáng chế. Tuy nhiên, người có hiểu biết trong lĩnh vực kỹ thuật tương ứng sẽ nhận ra rằng sáng chế có thể được thực hành mà không có một hoặc nhiều chi tiết cụ thể hoặc với các phương pháp, thành phần, vật liệu khác. Ví dụ, các cấu trúc, vật liệu hoặc hoạt động đã biết không được hiển thị hoặc mô tả chi tiết để tránh làm khó hiểu các khía cạnh của sáng chế.

Mặc dù các ví dụ nêu trên là minh họa về các nguyên tắc của sáng chế trong một hoặc nhiều ứng dụng cụ thể, nhưng sẽ trở nên rõ ràng với những người có hiểu biết trung bình trong lĩnh vực kỹ thuật rằng có thể thực hiện nhiều thay đổi về hình thức, cách sử dụng và chi tiết thực hiện mà không cần sử dụng khả năng sáng tạo, và không trệch khỏi các nguyên lý và khái niệm của sáng chế. Theo đó, sáng chế không nhằm bị giới hạn, ngoại trừ bởi bộ yêu cầu bảo hộ được nêu dưới đây.

Các động từ "bao gồm" và "gồm có" được sử dụng trong sáng chế như là những giới hạn mở mà không loại trừ cũng không yêu cầu sự tồn tại của các dấu hiệu chưa được nêu. Các dấu hiệu được nêu trong các điểm yêu cầu bảo hộ phụ thuộc kết hợp được tự do trừ khi có quy định rõ ràng khác. Hơn nữa, nó được hiểu rằng việc sử dụng "một", nghĩa là, dạng số ít, xuyên suốt sáng chế không loại trừ dạng số nhiều.

Khả năng ứng dụng trong công nghiệp

Ít nhất một số phương án của sáng chế có khả năng áp dụng trong việc xác thực

tin nhắn.

Danh mục các từ viết tắt

AAA	Định nghĩa
BTLE	Bluetooth năng lượng thấp (Bluetooth-low energy)
IS-95	Tiêu chuẩn tạm thời 95 (Interim Standard 95)
LTE	Phát triển dài hạn (Long Term Evolution)
PDU	Đơn vị dữ liệu giao thức (Protocol Data Unit)
SHA-1	Thuật toán hàm băm bảo mật 1 (Secure Hash Algorithm 1)
USB	Cổng nối tiếp đa năng (Universal Serial Port)
WiMAX	Khả năng tương tác toàn cầu với truy cập vi sóng (Worldwide Interoperability For Microwave Access)
WLAN	Mạng cục bộ không dây (Wireless Local Area Network)
WCDMA	Đa truy cập phân chia theo mã băng rộng (Wideband Code Division Multiple Access)

Danh mục các số chỉ dẫn

110	Thiết bị
120	Trạm gốc
130	Người nhận
140	Điểm truy cập
150	Người nhận
112 và 114	Giao diện vô tuyến
123 và 145	Kết nối
200	Gói tin quảng bá Bluetooth năng lượng thấp (Bluetooth low energy advertisement packet) (Fig.2)
202 – 228	Các trường có trong gói tin quảng bá Bluetooth năng lượng thấp 200

300 – 370	Cấu trúc được minh họa trên Fig.3
410 – 470	Các bước của quá trình báo hiệu được minh họa trên Fig.4
510 – 540	Các bước của phương pháp được minh họa trên Fig.5
610 – 640	Các bước của phương pháp được minh họa trên Fig.6

YÊU CẦU BẢO HỘ

1. Thiết bị xác thực tin nhắn bao gồm ít nhất một lõi xử lý, ít nhất một bộ nhớ bao gồm mã chương trình máy tính, ít nhất một bộ nhớ và mã chương trình máy tính được tạo cấu hình để, bằng ít nhất một lõi xử lý, làm cho thiết bị ít nhất thực hiện:

biên dịch, từ thông tin được bao gồm trong tin nhắn nhận được trong thiết bị, chuỗi bit bảo vệ, chuỗi bit bảo vệ bao gồm phần thứ nhất và phần thứ hai, phần thứ nhất bao gồm đoạn các bit có trọng số cao nhất của chuỗi bit bảo vệ và phần thứ hai bao gồm đoạn các bit có trọng số thấp nhất của chuỗi bit bảo vệ;

nhận dạng người gửi tin nhắn dựa trên việc nhận dạng khóa bí mật mà giải mã phần thứ nhất thành chuỗi bit gốc được bao gồm trong tin nhắn;

xác minh rằng số được thể hiện bởi cả hai phần cùng nhau của chuỗi bit bảo vệ đã được tăng lên hoặc được giảm xuống so với chuỗi bit bảo vệ trong tin nhắn trước đó từ cùng một người gửi, và

xác định phần thứ nhất tiếp theo mà sẽ được liên kết với tập hợp các tin nhắn trong tương lai từ người gửi, khi tăng chuỗi bit bảo vệ sẽ khiến cho phần thứ nhất thay đổi.

2. Thiết bị theo điểm 1, trong đó chuỗi bit gốc khác biệt với phần thứ nhất và phần thứ hai.

3. Thiết bị theo điểm 1, trong đó chuỗi bit bảo vệ bao gồm bộ đếm hoặc dấu thời gian.

4. Thiết bị theo điểm 1, trong đó phần thứ nhất được bao gồm trong trường địa chỉ của tin nhắn.

5. Thiết bị theo điểm 4, trong đó trường địa chỉ là trường địa chỉ người gửi.

6. Thiết bị theo điểm 1, trong đó ít nhất một bộ nhớ và mã chương trình máy tính được tạo cấu hình để, với ít nhất một lõi xử lý, khiến cho thiết bị xác định phần thứ nhất tiếp theo đáp lại sự xác định rằng thiết bị này có khả năng tính toán dự phòng.

7. Thiết bị theo điểm 1, trong đó ít nhất một bộ nhớ và mã chương trình máy tính được tạo cấu hình để, với ít nhất một lõi xử lý, khiến cho thiết bị xác định tập hợp các phần thứ nhất tiếp theo, mỗi phần thứ nhất tiếp theo trong tập hợp này tương

ứng với một người gửi riêng biệt, đáp lại sự xác định rằng thiết bị này có khả năng tính toán dự phòng.

8. Phương pháp xác thực tin nhắn được thực hiện bằng máy tính sử dụng ít nhất một hoặc nhiều bộ xử lý phần cứng, phương pháp này bao gồm các bước:

biên dịch, từ thông tin được bao gồm trong tin nhắn nhận được thông qua mạng máy tính trong thiết bị, chuỗi bit bảo vệ, chuỗi bit bảo vệ bao gồm phần thứ nhất và phần thứ hai, phần thứ nhất bao gồm đoạn các bit có trọng số cao nhất của chuỗi bit bảo vệ và phần thứ hai bao gồm đoạn các bit có trọng số thấp nhất của chuỗi bit bảo vệ;

nhận dạng, sử dụng ít nhất một hoặc nhiều bộ xử lý phần cứng, người gửi tin nhắn dựa trên việc nhận dạng mã bảo mật dùng cho giải mã phần thứ nhất thành chuỗi bit gốc được bao gồm trong tin nhắn;

xác minh, sử dụng ít nhất một hoặc nhiều bộ xử lý phần cứng, rằng số được thể hiện bởi cả hai phần cùng nhau của chuỗi bit bảo vệ đã được tăng lên hoặc được giảm xuống so với chuỗi bit bảo vệ trong tin nhắn trước đó từ cùng một người gửi, và

xác định phần thứ nhất tiếp theo mà sẽ được liên kết với tập hợp các tin nhắn trong tương lai từ người gửi, khi tăng chuỗi bit bảo vệ sẽ khiến cho phần thứ nhất thay đổi.

9. Phương pháp theo điểm 8, trong đó chuỗi bit gốc khác biệt với phần thứ nhất và phần thứ hai.

10. Phương pháp theo điểm 8, trong đó chuỗi bit bảo vệ bao gồm bộ đếm hoặc dấu thời gian.

11. Phương pháp theo điểm 8, trong đó phần thứ nhất được bao gồm trong trường địa chỉ của tin nhắn.

12. Vật ghi lâu dài đọc được bằng máy tính lưu tập hợp các lệnh đọc dược bằng máy tính trên đó để, khi được thực thi bởi ít nhất một bộ xử lý, khiến cho thiết bị ít nhất thực hiện:

biên dịch, từ thông tin được bao gồm trong tin nhắn nhận được trong thiết bị, chuỗi bit bảo vệ, chuỗi bit bảo vệ bao gồm phần thứ nhất và phần thứ hai, phần thứ nhất bao gồm đoạn các bit có trọng số cao nhất của chuỗi bit bảo vệ và phần thứ hai bao

gồm đoạn các bit có trọng số thấp nhất của chuỗi bit bảo vệ;

nhận dạng người gửi tin nhắn dựa trên việc nhận dạng khóa bí mật mà giải mã phần thứ nhất thành chuỗi bit gốc được bao gồm trong tin nhắn;

xác minh rằng số được thể hiện bởi cả hai phần cùng nhau của chuỗi bit bảo vệ đã được tăng lên hoặc được giảm xuống so với chuỗi bit bảo vệ trong tin nhắn trước đó từ cùng một người gửi, và

xác định phần thứ nhất tiếp theo mà sẽ được liên kết với tập hợp các tin nhắn trong tương lai từ người gửi, khi tăng chuỗi bit bảo vệ sẽ khiến cho phần thứ nhất thay đổi.

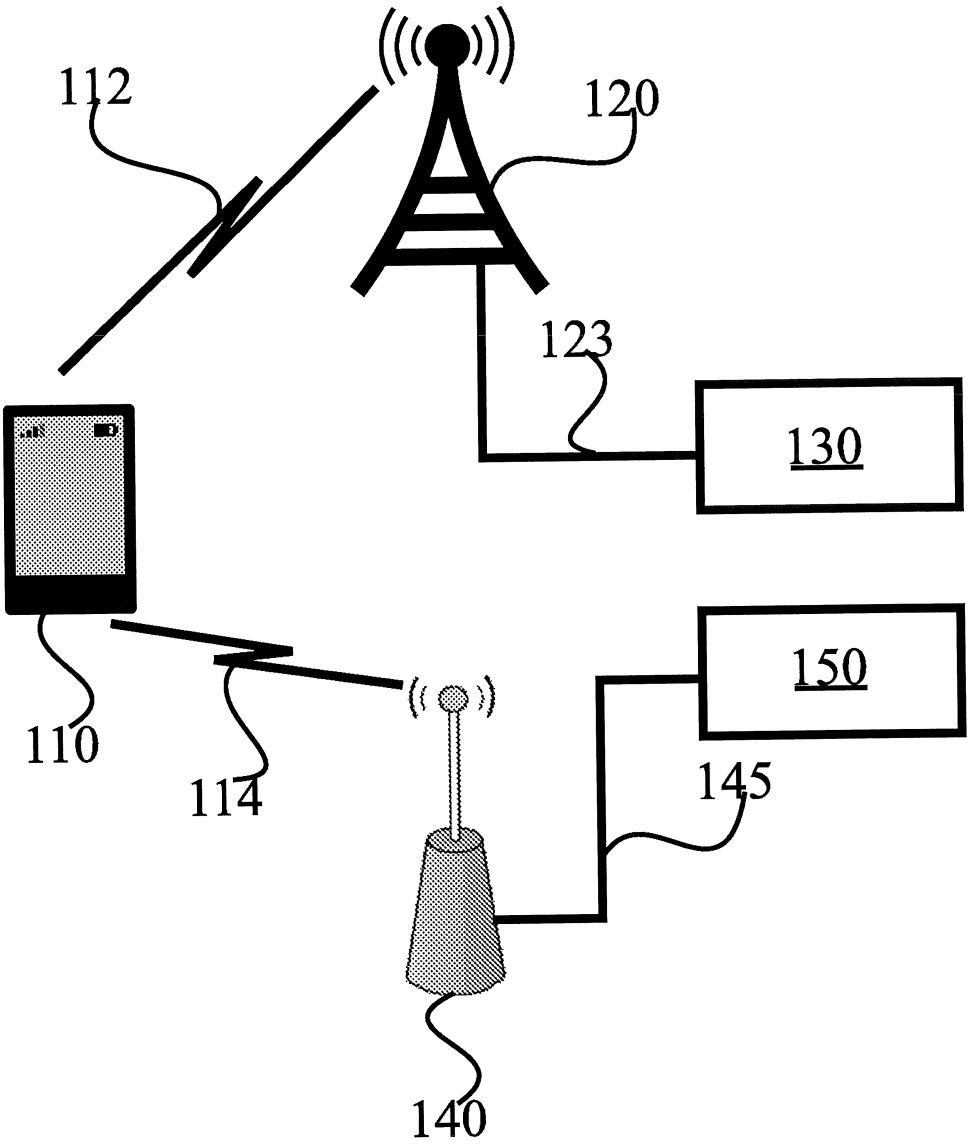


Fig.1

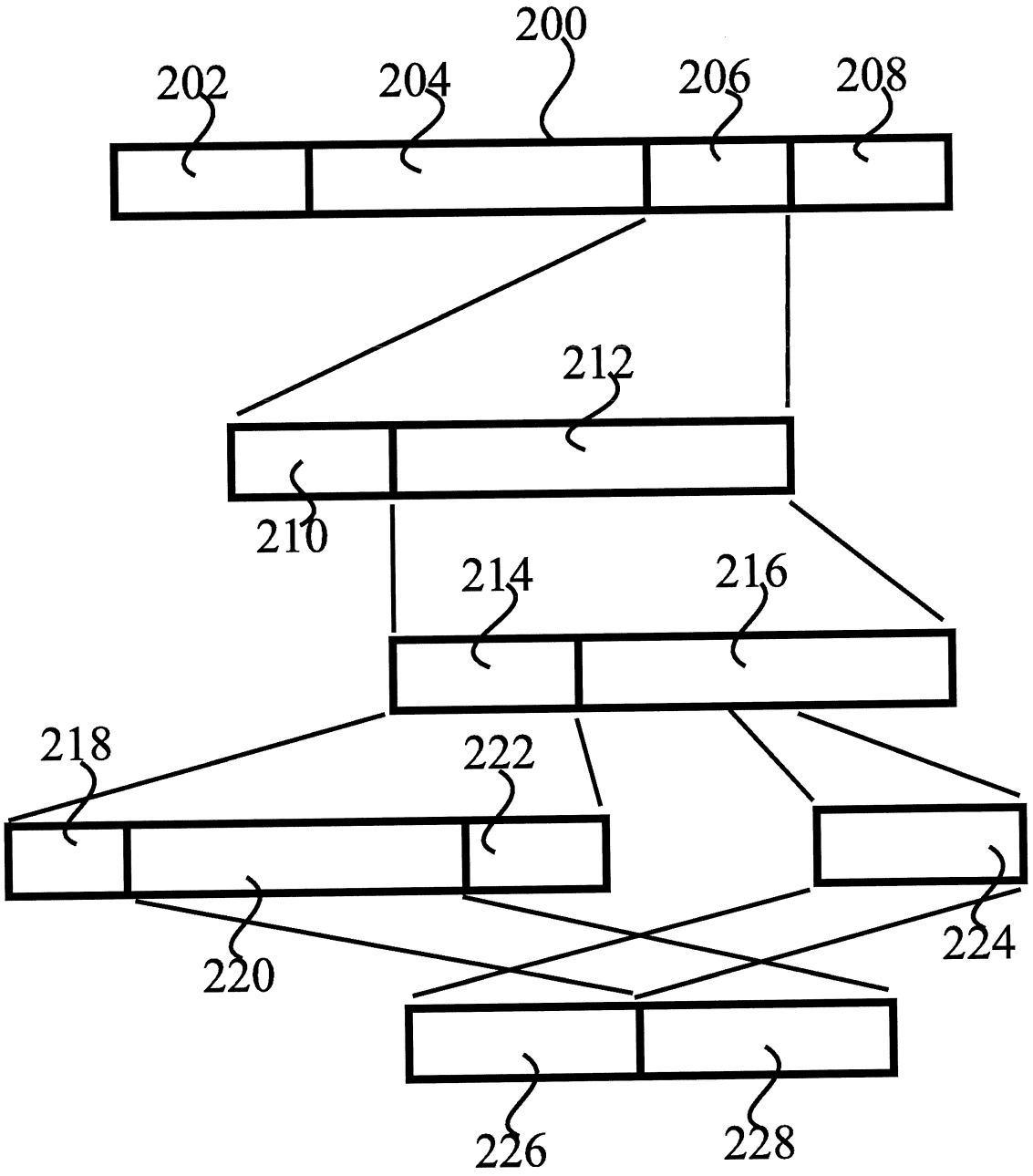


Fig.2

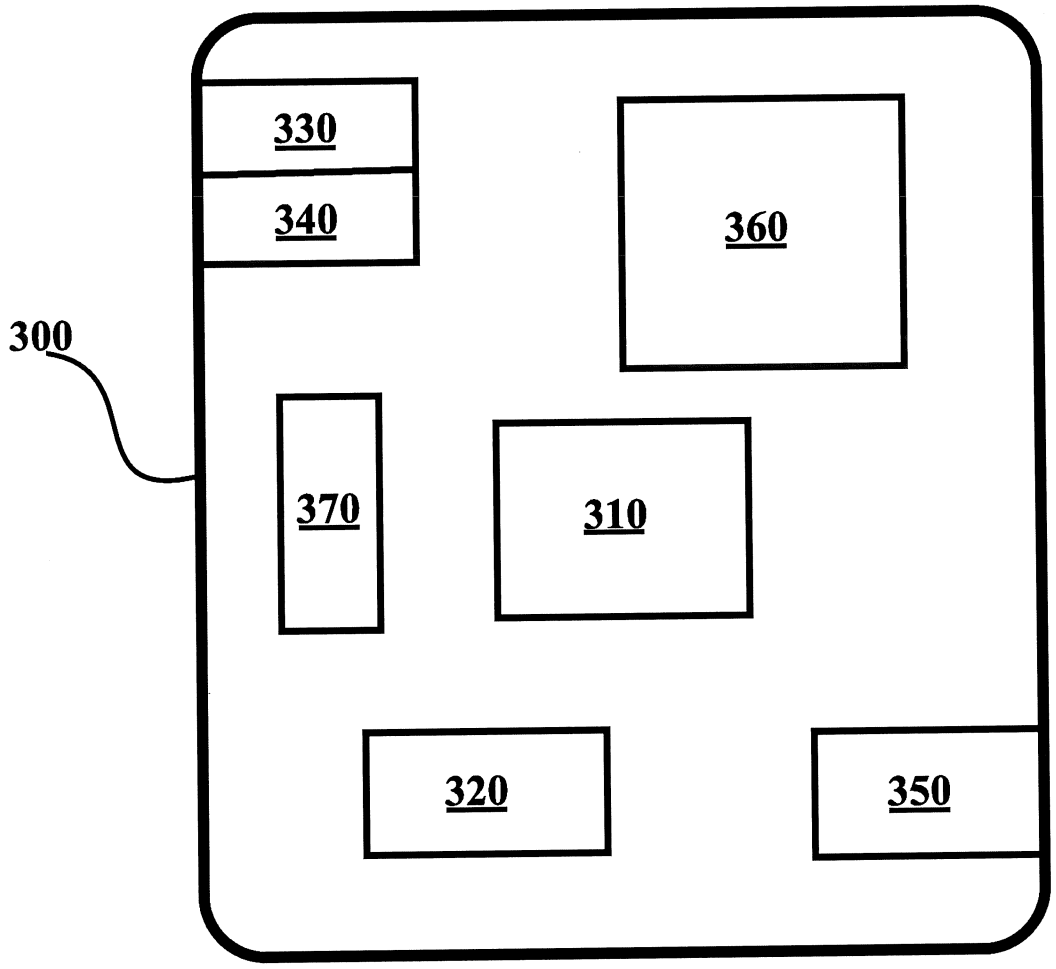


Fig.3

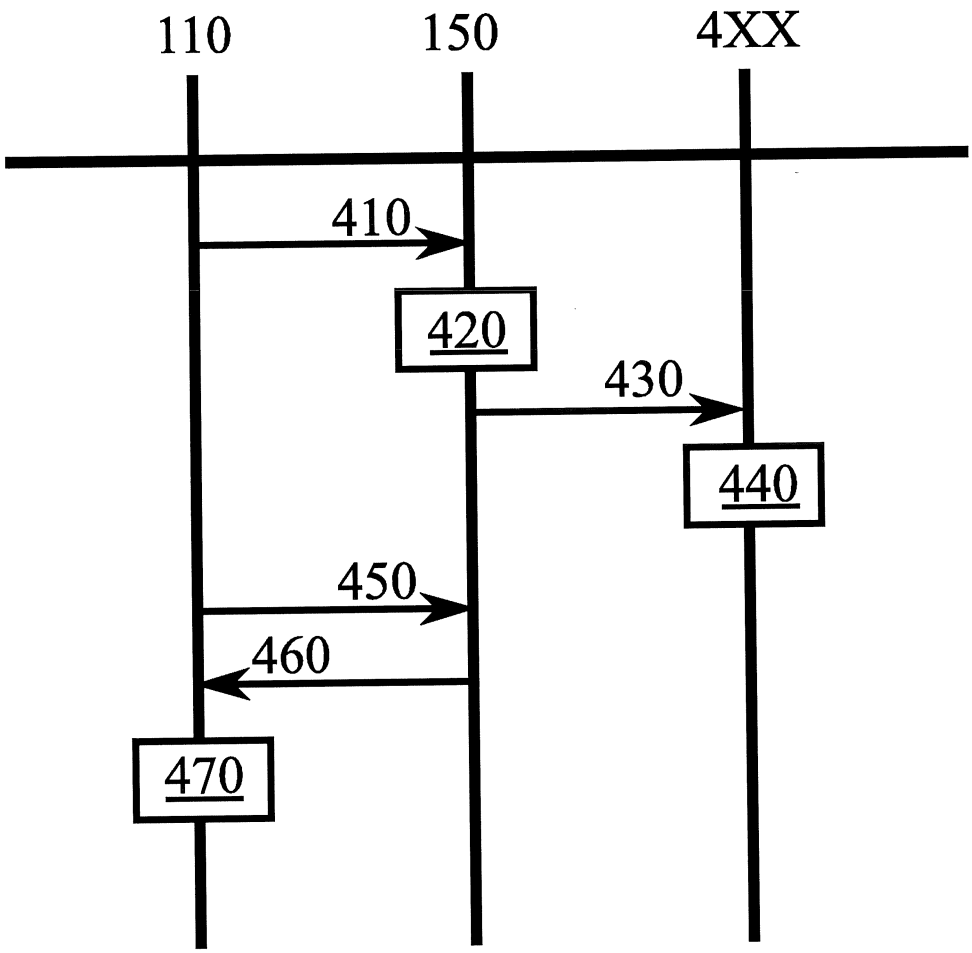


Fig.4

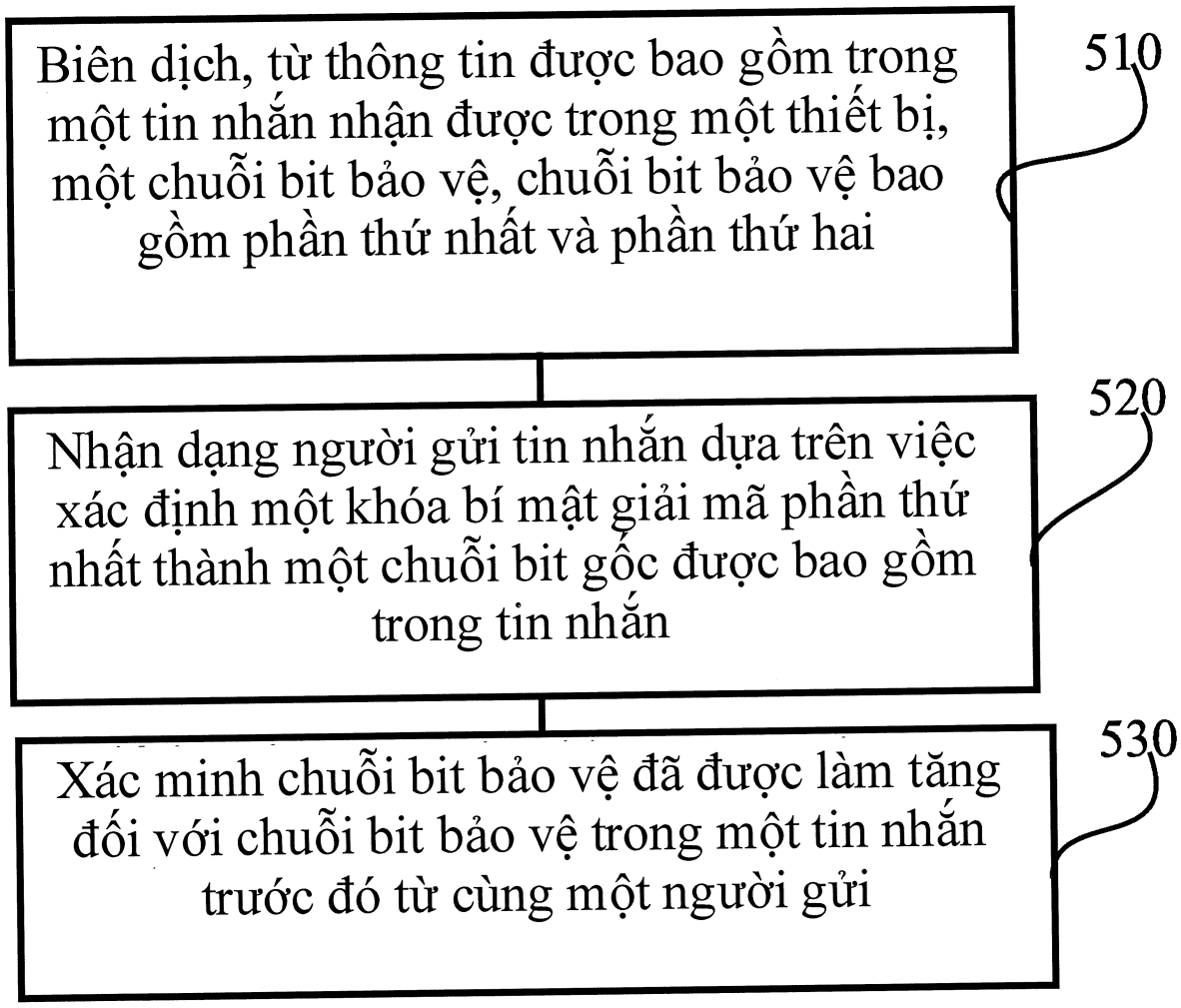

Biên dịch, từ thông tin được bao gồm trong một tin nhắn nhận được trong một thiết bị, một chuỗi bit bảo vệ, chuỗi bit bảo vệ bao gồm phần thứ nhất và phần thứ hai
510
Nhận dạng người gửi tin nhắn dựa trên việc xác định một khóa bí mật giải mã phần thứ nhất thành một chuỗi bit gốc được bao gồm trong tin nhắn
520
Xác minh chuỗi bit bảo vệ đã được làm tăng đối với chuỗi bit bảo vệ trong một tin nhắn trước đó từ cùng một người gửi
530

Fig.5

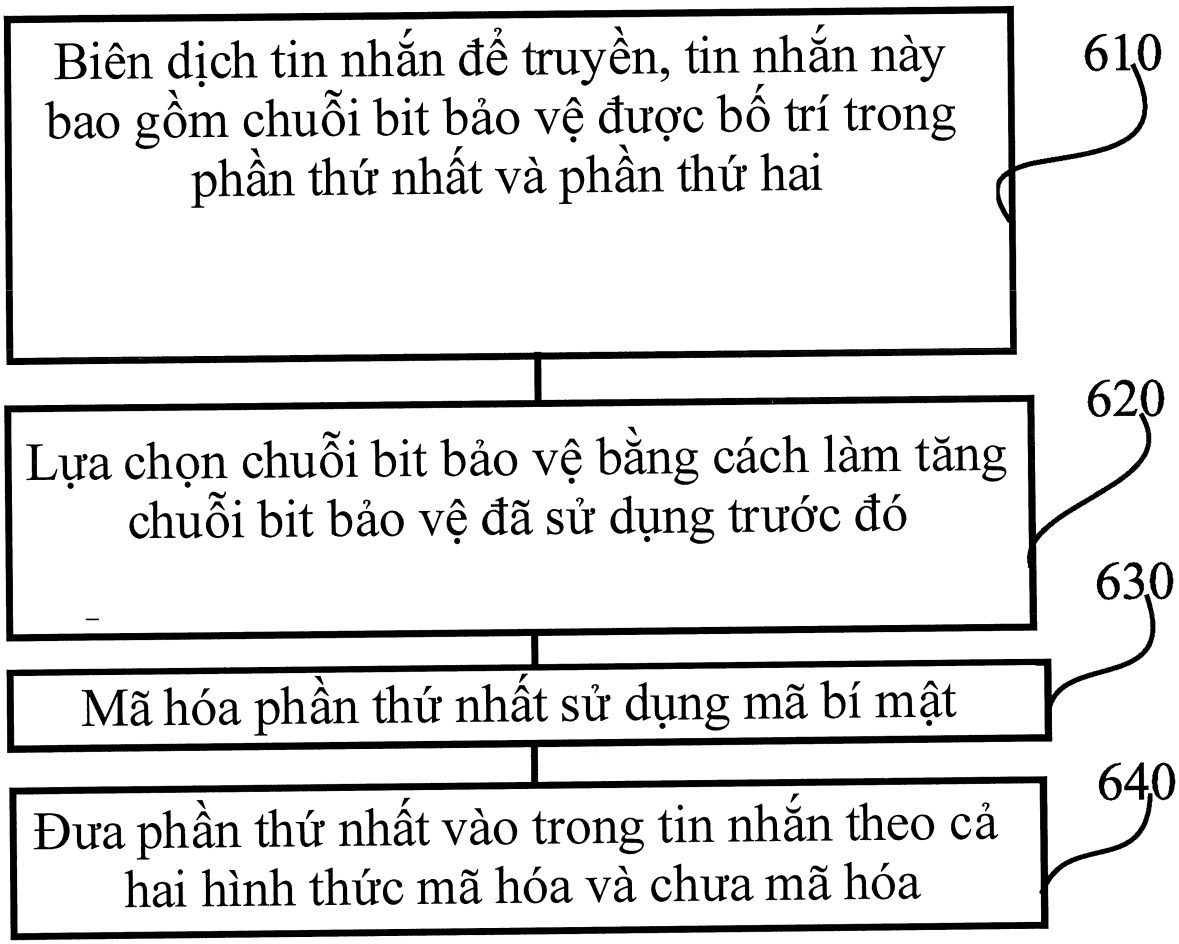

Biên dịch tin nhắn để truyền, tin nhắn này bao gồm chuỗi bit bảo vệ được bố trí trong phần thứ nhất và phần thứ hai
610
Lựa chọn chuỗi bit bảo vệ bằng cách làm tăng chuỗi bit bảo vệ đã sử dụng trước đó
620
Mã hóa phần thứ nhất sử dụng mã bí mật
630
Đưa phần thứ nhất vào trong tin nhắn theo cả hai hình thức mã hóa và chưa mã hóa
640

Fig.6