(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) **1-0022613**

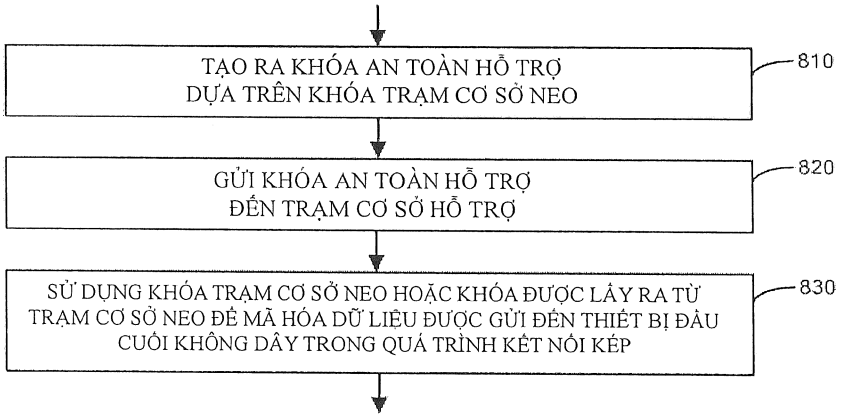
(51)[7] **H04L 29/06**, H04W 12/04, 36/00

(13) **B**

(21) 1-2015-02759
(22) 30.01.2014
(86) PCT/SE2014/050122 30.01.2014
(87) WO2014/120077 07.08.2014
(30) 61/758,373 30.01.2013 US
(45) 25.12.2019 381
(43) 26.10.2015 331
(73) TELEFONAKTIEBOLAGET L M ERICSSON (PUBL) (SE)
SE-164 83 Stockholm, Sweden
(72) WAGER, Stefan (SE), VIRKKI, Vesa (FI), TEYEB, Oumer (ET), JOHANSSON, Niklas (SE), NORRMAN, Karl (SE)
(74) Công ty Luật TNHH T&G (TGVN)

(54) THIẾT BỊ ĐẦU CUỐI KHÔNG DÂY VÀ PHƯƠNG PHÁP TRONG THIẾT BỊ ĐẦU CUỐI KHÔNG DÂY ĐỂ TẠO RA KHÓA AN TOÀN

(57) Sáng chế đề cập đến các kỹ thuật tạo ra tập hợp các khóa mã hóa an toàn để được sử dụng cho truyền thông giữa thiết bị đầu cuối không dây và trạm cơ sở hỗ trợ trong kịch bản kết nối kép. Phương pháp ví dụ bao gồm bước tạo ra (810) khóa an toàn hỗ trợ đối với trạm cơ sở hỗ trợ, dựa trên khóa trạm cơ sở neo. Khóa an toàn hỗ trợ được tạo ra được gửi (820) đến trạm cơ sở hỗ trợ, để sử dụng bởi trạm cơ sở hỗ trợ trong việc mã hóa lưu lượng dữ liệu được gửi đến thiết bị đầu cuối không dây hoặc trong việc tạo ra một hoặc nhiều khóa an toàn hỗ trợ bổ sung để mã hóa lưu lượng dữ liệu được gửi đến thiết bị đầu cuối không dây trong khi thiết bị đầu cuối không dây được kết nối kép vào trạm cơ sở neo và trạm cơ sở hỗ trợ. Khóa trạm cơ sở neo, hoặc khóa được lấy ra từ khóa trạm cơ sở neo, được sử dụng (830) để mã hoá dữ liệu được gửi đến thiết bị đầu cuối không dây bởi trạm cơ sở neo.



Lĩnh vực kỹ thuật được đề cập

Nói chung, sáng chế đề cập đến mạng viễn thông không dây, và cụ thể hơn là đề cập đến các kỹ thuật để xử lý khóa an toàn trong các bối cảnh kết nối kép, tức là, các bối cảnh trong đó thiết bị đầu cuối di động được kết nối một cách đồng thời vào nhiều trạm cơ sở.

Tình trạng kỹ thuật của sáng chế

Trong hệ thống vô tuyến mạng tế bào thông thường, thiết bị đầu cuối di động (còn được gọi là trang thiết bị người dùng, các UE, thiết bị đầu cuối không dây, và/hoặc các trạm di động) truyền thông nhờ RAN (radio access network - mạng truy cập vô tuyến) với một hoặc nhiều mạng lõi, mà cung cấp việc truy cập đến các mạng dữ liệu, như Internet, và/hoặc đến PSTN (public-switched telecommunications network - mạng viễn thông chuyển mạch công cộng). RAN phủ sóng diện tích địa lý mà được chia thành các diện tích mạng tế bào, với từng diện tích mạng tế bào được phục vụ bởi trạm cơ sở vô tuyến (còn được gọi là trạm cơ sở, nút RAN, "NodeB", và/hoặc NodeB được cải thiện hoặc "eNodeB"). Diện tích mạng tế bào là diện tích địa lý mà trên đó việc phủ sóng vô tuyến được cung cấp bởi trang thiết bị trạm cơ sở ở phía trạm cơ sở. Trạm cơ sở truyền thông thông qua các kênh truyền thông vô tuyến với thiết bị đầu cuối không dây nằm trong phạm vi của trạm cơ sở.

Các nhà vận hành hệ thống truyền thông mạng tế bào đã bắt đầu cung cấp các dịch vụ dữ liệu dải rộng di động dựa trên, ví dụ, WCDMA (Wideband Code-Division Multiple Access - đa truy cập phân mã dải rộng), HSPA (High-Speed Packet Access - truy cập gói tốc độ cao), và các công nghệ không dây LTE (Long Term Evolution - tiến triển dài hạn). Được khuyến khích bằng cách đưa vào các thiết bị mới được thiết kế đối với các ứng dụng dữ liệu, các yêu cầu thực hiện của người dùng cuối tiếp tục gia tăng. Việc làm thích ứng gia tăng của dải rộng di động dẫn đến việc tăng đáng kể về lưu lượng được xử lý bởi các mạng dữ liệu không dây tốc độ cao. Do đó, mong muốn có các kỹ thuật cho phép các nhà vận hành mạng tế bào quản lý các mạng một cách hiệu quả hơn.

Các kỹ thuật để cải thiện việc thực hiện liên kết xuống có thể bao gồm các kỹ thuật truyền đa anten MIMO (Multiple-Input-Multiple-Output - nhiều đầu vào-nhiều đầu ra), truyền thông đa dòng, triển khai đa vật mang, v.v.. Khi các hiệu quả quang phổ cho liên kết có thể là tiến gần đến các giới hạn lý thuyết, các bước tiếp theo có thể bao gồm việc cải thiện các hiệu quả quang phổ trên một diện tích đơn vị. Các hiệu quả khác đối với các mạng không dây có thể đạt được, ví dụ, bằng cách thay đổi tôpô của các mạng truyền thống để làm tăng tính đồng nhất của kinh nghiệm của người dùng qua toàn bộ tế bào. Một cách tiếp cận là thông qua việc triển khai các mạng được gọi là không đồng nhất.

Mạng đồng nhất là mạng của trạm cơ sở (còn được gọi là NodeB, NodeB được cải thiện, hoặc eNB) trong cách bố trí theo kế hoạch, cung cấp các dịch vụ truyền thông đối với tập hợp các thiết bị đầu cuối người dùng (còn được gọi là các nút trang thiết bị người dùng, các UE, và/hoặc thiết bị đầu cuối không dây), trong đó tất cả các trạm cơ sở thường có các mức truyền năng lượng tương tự, các mẫu anten, các nền nhiễu của bộ nhận, và/hoặc kết nối đổi hướng ngược lại đến mạng dữ liệu. Hơn nữa, tất cả các trạm cơ sở trong mạng đồng nhất có thể thường đưa ra truy cập không giới hạn đến thiết bị đầu cuối người dùng trong mạng, và từng trạm cơ sở có thể phục vụ thô cùng số lượng thiết bị đầu cuối người dùng. Các hệ thống truyền thông không dây mạng tế bào hiện nay trong phạm trù này có thể bao gồm, ví dụ, GSM (Global System for Mobile communication - hệ thống truyền thông di động toàn cầu), WCDMA, HSDPA (High Speed Downlink Packet Access - truy cập gói liên kết xuống tốc độ cao), LTE (Long Term Evolution - tiến triển dài hạn), WiMAX (Worldwide Interoperability for Microwave Access - hệ thống truy cập vi ba có tính tương tác toàn cầu), v.v..

Trong mạng không đồng nhất, trạm cơ sở năng lượng thấp (còn được gọi là LPN (low power node - nút năng lượng thấp), các nút micro, các nút pico, các nút femto, các nút chuyển tiếp, các nút đơn vị vô tuyến từ xa, các nút RRU, các tế bào nhỏ, các RRU, v.v.) có thể được triển khai dọc theo hoặc làm vật phủ đến trạm cơ sở vĩ mô được lập kế hoạch và/hoặc được đặt đều đặn. Do đó, MBS (macro base station - trạm cơ sở vĩ mô) có thể cung cấp dịch vụ trên diện tích mạng tế bào vĩ mô tương đối

lớn, và từng LPN có thể cung cấp dịch vụ đối với diện tích mạng tế bào LPN tương đối nhỏ tương ứng nằm trong diện tích mạng tế bào vĩ mô tương đối lớn.

Năng lượng được truyền bởi LPN có thể là tương đối nhỏ, ví dụ, 2 Oát, so với năng lượng được truyền bởi trạm cơ sở vĩ mô, mà có thể là 40 Oát đối với trạm cơ sở vĩ mô thông thường. LPN có thể được triển khai, ví dụ, để giảm/loại trừ (các) lỗ trống phủ sóng trong việc phủ sóng được cung cấp bởi trạm cơ sở vĩ mô, và/hoặc đến lưu lượng không tải từ trạm cơ sở vĩ mô, như làm tăng dung lượng ở vị trí lưu lượng cao hoặc được gọi là điểm nóng. Do năng lượng truyền thấp hơn và kích cỡ vật lý thấp hơn của nó, LPN có thể tạo ra sự linh hoạt cao hơn đối với việc thu nhận ở vị trí.

Do đó, mạng không đồng nhất tạo dấu hiệu triển khai nhiều tầng của các HPN (high-power node - nút năng lượng cao), như trạm cơ sở vĩ mô, và các nút năng lượng thấp (các LPN), như trạm cơ sở được gọi là pico hoặc các nút pico. Các LPN và các HPN trong vùng được đưa ra của mạng không đồng nhất có thể hoạt động trên cùng tần số, trong trường hợp đó, việc triển khai có thể được gọi là triển khai đồng nhất đồng kênh, hoặc trên các tần số khác nhau, trong trường hợp đó, việc triển khai có thể được gọi là liên tần số hoặc vật mang phức hoặc phức tần số triển khai đồng nhất.

3GPP (Third Generation Partnership Project - dự án đối tác thế hệ thứ 3) đang tiếp tục phát triển các đặc tả đối với các dấu hiệu tiên tiến và cải thiện trong bối cảnh hệ thống viễn thông không dây thế hệ thứ tư đã được biết đến là LTE (Tiến triển dài hạn). Trong Phiên bản 12 của các đặc tính LTE và xa hơn, các cải thiện khác liên quan đến các nút năng lượng thấp và các triển khai đồng nhất sẽ được xem xét ở dưới ô bảo vệ của các hoạt động "cải thiện tế bào nhỏ". Một số hoạt động này sẽ tập trung vào việc đạt tới mức độ thậm chí là lớn hơn của hoạt động giao diện giữa tầng vĩ mô và các tầng năng lượng thấp, bao gồm thông qua việc sử dụng tập hợp các các kỹ thuật và công nghệ được gọi là "kết nối tầng kép" hoặc đơn giản là "kết nối kép".

Như được thể hiện trên Fig.1, kết nối kép ngụ ý rằng thiết bị có các kết nối đồng thời với cả hai tầng vĩ mô và các tầng năng lượng thấp. Fig.1 minh họa một ví dụ về mạng không đồng nhất trong đó thiết bị đầu cuối di động 101 sử dụng các dòng phức, ví dụ, dòng trạm từ trạm cơ sở vĩ mô (hoặc "eNB trạm") 401A và dòng hỗ trợ từ trạm cơ sở pico (hoặc là "eNB hỗ trợ") 401B. Ghi nhận rằng, thuật ngữ này có thể biến

đổi - trạm cơ sở neo và trạm cơ sở hỗ trợ trong cấu hình giống như được thể hiện trên Fig.1 đôi khi có thể được gọi là các trạm cơ sở "chủ" và "tớ" hoặc theo các tên gọi khác. Còn nên ghi nhận rằng, trong khi thuật ngữ "neo/hỗ trợ" và "chủ/tớ" tạo ra mối quan hệ có thứ bậc giữa trạm cơ sở liên quan trong bối cảnh kết nối kép, nhiều nguyên lý và các kỹ thuật kết hợp với kết nối kép có thể được áp dụng để triển khai các bối cảnh trong đó không có mối quan hệ có thứ bậc này, ví dụ, giữa các trạm cơ sở ngang hàng. Do đó, trong khi thuật ngữ "trạm cơ sở neo" và "trạm cơ sở hỗ trợ" được sử dụng trong bản mô tả này, nên được hiểu rằng các kỹ thuật và thiết bị được mô tả trong bản mô tả này không chỉ giới hạn ở các phương án mà sử dụng thuật ngữ này, cũng không nhất thiết chỉ giới hạn ở các phương án có mối quan hệ có thứ bậc được đề xuất bởi Fig.1.

Kết nối kép có thể ngụ ý, trong các phương án và/hoặc các bối cảnh khác nhau:

• Kiểm soát và tách dữ liệu trong đó, ví dụ, kiểm soát việc phát tín hiệu đối với tính di động được cung cấp nhờ tầng vĩ mô đồng thời làm kết nối dữ liệu tốc độ cao được cung cấp nhờ tầng năng lượng thấp.

• Việc tách giữa liên kết xuống và liên kết lên, trong đó kết nối liên kết xuống và liên kết lên được cung cấp nhờ các tầng khác nhau.

• Tính đa dạng để kiểm soát việc phát tín hiệu, trong đó kiểm soát nguồn vô tuyến (RRC) việc phát tín hiệu có thể được cung cấp nhờ đa liên kết, còn cải thiện việc thực hiện tính di động.

Hỗ trợ vĩ mô bao gồm kết nối kép có thể tạo ra một vài lợi ích:

• Hỗ trợ được cải thiện đối với tính di động - bằng cách duy trì điểm neo di động trong tầng vĩ mô, như được mô tả trên đây, có thể duy trì tính di động liền một mạch giữa các tầng vĩ mô và các tầng năng lượng thấp, cũng như giữa các nút năng lượng thấp.

• Truyền phụ phí thấp từ tầng năng lượng thấp - bằng cách chỉ truyền thông tin đòi hỏi đối với kinh nghiệm người dùng riêng, có thể tránh được phụ phí đến từ việc hỗ trợ tính di động trong chế độ không tải trong tầng diện tích cục bộ, chẳng hạn.

• Cân bằng tải hiệu quả năng lượng - bằng cách ngắt các nút năng lượng thấp khi không diễn ra sự truyền dữ liệu, có thể giảm tiêu thụ năng lượng của tầng năng lượng thấp.

• Tối ưu hóa theo liên kết - bằng cách lựa chọn điểm kết thúc đối với liên kết lên và liên kết xuống một cách riêng rẽ, việc lựa chọn nút có thể được tối ưu hóa đối với từng liên kết.

Một trong số các vấn đề trong việc sử dụng kết nối kép là cách để ánh xạ cho các DRB (data radio bearer - vật mang dữ liệu vô tuyến) lần lượt lên trên dòng neo và dòng hỗ trợ. Một lựa chọn để tách rời các DRB giữa 2 trạm cơ sở, như được thể hiện trên Fig.1, là để giữ mặt phẳng kiểm soát (RRC) trong eNB neo và phân phối các thực thể PDCP sao cho một vài trong số chúng là trong eNB neo và một vài trong số chúng trong eNB hỗ trợ. Như được thảo luận chi tiết hơn dưới đây, cách tiếp cận này có thể tạo ra một số lợi ích quan trọng về hiệu quả của hệ thống. Tuy nhiên, cách tiếp cận này gây ra các vấn đề liên quan đến việc xử lý khóa an toàn mà được sử dụng đối với tính cẩn mật và việc bảo vệ tính tổng thể của dữ liệu được truyền đến và từ thiết bị đầu cuối di động.

Bản chất kỹ thuật của sáng chế

Trong các hệ thống LTE, tầng RRC (Radio Resource Control - kiểm soát tài nguyên vô tuyến) tạo cấu hình các thực thể PDCP (Packet Data Convergence Protocol - giao thức hội tụ dữ liệu gói) với các khóa mã hóa và dữ liệu cấu hình, như dữ liệu chỉ ra các thuật toán an toàn nên được áp dụng liên quan đến vật mang vô tuyến tương ứng. Trong kịch bản kết nối kép, tầng RRC có thể được xử lý ngoại lệ bởi nút neo, trong khi các thực thể PDCP có thể được điều khiển trong từng loại trong số các loại nút trạm cơ sở neo và hỗ trợ. Khi trạm cơ sở neo và trạm cơ sở hỗ trợ có thể được ứng dụng trong các nút riêng rẽ về mặt vật lý, giả thuyết rằng RRC có thể tạo cấu hình các thực thể PDCP nhờ các API (application program interface - giao diện chương trình ứng dụng) bên trong không còn giữ được nữa.

Các phương án làm ví dụ được bộc lộ trong bản mô tả này được định hướng theo việc tạo ra tập hợp các khóa mã hoá an toàn để được sử dụng cho truyền thông giữa thiết bị đầu cuối không dây trong kết nối kép và eNB hỗ trợ. Trong một số

phương án, khóa cơ sở dùng cho eNB hỗ trợ được tạo ra từ khóa an toàn của eNB neo. Khi đó, khóa cơ sở có thể được sử dụng để tạo ra khóa dùng cho sự truyền thông an toàn giữa thiết bị đầu cuối không dây và eNB hỗ trợ.

Các phương án về các kỹ thuật được bộc lộ bao gồm, ví dụ, phương pháp, phù hợp để ứng dụng trong nút mạng, để tạo ra khóa an toàn cho các sự truyền thông an toàn giữa thiết bị đầu cuối không dây và trạm cơ sở neo và giữa thiết bị đầu cuối không dây và trạm cơ sở hỗ trợ, trong đó thiết bị đầu cuối không dây được hoặc sắp được kết nối kép vào trạm cơ sở neo và trạm cơ sở hỗ trợ. Phương pháp làm ví dụ bao gồm bước tạo ra khóa an toàn hỗ trợ đối với trạm cơ sở hỗ trợ, dựa ít nhất một phần trên khóa trạm cơ sở neo. Khi đó, khóa an toàn hỗ trợ được tạo ra được gửi đến trạm cơ sở hỗ trợ, để sử dụng bởi trạm cơ sở hỗ trợ trong việc mã hóa lưu lượng dữ liệu được gửi đến thiết bị đầu cuối không dây hoặc trong việc tạo ra một hoặc nhiều khóa an toàn hỗ trợ bổ sung để mã hóa lưu lượng dữ liệu được gửi đến thiết bị đầu cuối không dây bởi trạm cơ sở hỗ trợ, trong khi thiết bị đầu cuối không dây được kết nối kép vào trạm cơ sở neo và trạm cơ sở hỗ trợ. Khóa trạm cơ sở neo, hoặc khóa được lấy ra (derived) từ khóa trạm cơ sở neo, được sử dụng để mã hóa dữ liệu được gửi đến thiết bị đầu cuối không dây bởi trạm cơ sở neo trong khi thiết bị đầu cuối không dây được kết nối kép vào trạm cơ sở neo và trạm cơ sở hỗ trợ.

Còn được bộc lộ trong bản mô tả này là phương pháp khác để tạo ra khóa an toàn hỗ trợ đối với trạm cơ sở hỗ trợ. Giống như phương pháp được tổng kết trên đây, phương pháp này còn phù hợp để ứng dụng trong nút mạng, để tạo ra khóa an toàn cho các sự truyền thông an toàn giữa thiết bị đầu cuối không dây và trạm cơ sở neo và giữa thiết bị đầu cuối không dây và trạm cơ sở hỗ trợ, trong đó thiết bị đầu cuối không dây được hoặc sắp được kết nối kép vào trạm cơ sở neo và trạm cơ sở hỗ trợ. Tuy nhiên, trong phương pháp này, phương pháp có thể được tiến hành trong nút mạng khác với trạm cơ sở neo, sử dụng khóa chính mà có thể không được biết đến đối với trạm cơ sở neo.

Theo phương pháp làm ví dụ thứ hai này, khóa an toàn chính được chia sẻ giữa nút mạng và thiết bị đầu cuối không dây. Khóa này có thể không được biết đến đối với trạm cơ sở neo, trong một số phương án. Phương pháp tiếp tục với việc tạo ra khóa an

toàn hỗ trợ đối với trạm cơ sở hỗ trợ, dựa ít nhất một phần trên khóa an toàn chính. Khi đó, khóa an toàn hỗ trợ được tạo ra được gửi đến trạm cơ sở hỗ trợ, để sử dụng bởi trạm cơ sở hỗ trợ trong việc mã hóa lưu lượng dữ liệu được gửi đến thiết bị đầu cuối không dây hoặc trong việc tạo ra một hoặc nhiều khóa an toàn hỗ trợ bổ sung để mã hóa lưu lượng dữ liệu được gửi đến thiết bị đầu cuối không dây bởi trạm cơ sở hỗ trợ trong khi thiết bị đầu cuối không dây được kết nối kép vào trạm cơ sở neo và trạm cơ sở hỗ trợ. Trong một số phương án, khóa an toàn hỗ trợ được tạo ra được gửi một cách trực tiếp đến trạm cơ sở hỗ trợ sao cho trạm cơ sở neo không phải là phần dấu hiệu của khóa, trong khi trong các phương án khác, khóa an toàn hỗ trợ được tạo ra được gửi đến trạm cơ sở hỗ trợ một cách gián tiếp, nhờ trạm cơ sở neo.

Các phương án khác của công nghệ được bộc lộ trong bản mô tả này bao gồm thiết bị nút mạng và thiết bị đầu cuối di động, từng loại được tạo cấu hình để thực hiện một trong số các phương pháp làm ví dụ được tổng kết trên đây hoặc các dạng biến đổi của nó.

Mô tả vắn tắt các hình vẽ

Fig.1 là sơ đồ minh họa một ví dụ về việc triển khai kết nối kép không đồng nhất với dòng neo và dòng hỗ trợ đồng thời đến thiết bị đầu cuối di động.

Fig.2 là hình vẽ minh họa các thành phần của kiến trúc hệ thống E-UTRAN.

Fig.3 là hình vẽ minh họa các chi tiết của kiến trúc giao thức trạm cơ sở trong kịch bản kết nối kép.

Fig.4 là hình vẽ minh họa thứ bậc lấy khóa ra dựa trên khóa trạm cơ sở neo.

Fig.5 là hình vẽ minh họa thứ bậc lấy khóa ra dựa trên khóa MME.

Fig.6 là sơ đồ tiến trình minh họa phương pháp làm ví dụ như được thực hiện bởi một nút mạng ví dụ.

Fig.7 là sơ đồ tiến trình minh họa phương pháp làm ví dụ như được thực hiện bởi thiết bị đầu cuối không dây.

Từng hình vẽ trong số các hình vẽ Fig.8 và Fig.9 minh họa sơ đồ tiến trình tương ứng với các phương án làm ví dụ theo sáng chế.

Fig.10 là sơ đồ khối minh họa một thiết bị làm trạm cơ sở neo làm ví dụ theo sáng chế.

Fig.11 là sơ đồ khối minh họa thiết bị nút mạng làm ví dụ khác theo sáng chế.

Fig.12 minh họa các thành phần của một thiết bị đầu cuối không dây làm ví dụ được tạo cấu hình theo một số phương án được bộc lộ theo sáng chế.

Mô tả chi tiết sáng chế

Sáng chế sẽ sẽ được mô tả một cách đầy đủ hơn dưới đây có tham khảo đến các hình vẽ kèm theo, trong đó các ví dụ về các phương án của sáng chế được thể hiện. Tuy nhiên, sáng chế có thể được biểu hiện ở nhiều dạng khác nhau và không được hiểu là bị giới hạn vào các phương án được nêu trong bản mô tả này. Tốt hơn là, các phương án này được đề xuất sao cho bản mô tả này sẽ là toàn thiện và đầy đủ, và chuyển tải đầy đủ phạm vi của sáng chế đến người có hiểu biết trung bình trong lĩnh vực. Còn nên ghi nhận rằng, các phương án này không loại trừ lẫn nhau. Các thành phần từ một phương án có thể được ngầm giả thiết là có mặt hoặc được sử dụng trong một phương án khác.

Chỉ với các mục đích minh họa và giải thích, các phương án này và các phương án khác của sáng chế được mô tả trong bản mô tả này trong bối cảnh vận hành trong mạng truy cập vô tuyến (RAN) mà truyền thông trên các kênh truyền thông vô tuyến với thiết bị đầu cuối di động (còn được gọi là thiết bị đầu cuối không dây hoặc các UE). Như được sử dụng trong bản mô tả này, thiết bị đầu cuối di động, thiết bị đầu cuối không dây, hoặc UE có thể bao gồm thiết bị bất kỳ mà nhận dữ liệu từ mạng truyền thông, và có thể bao gồm, nhưng không chỉ giới hạn ở, điện thoại di động (điện thoại "mạng tế bào"), laptop/máy tính xách tay, máy tính bỏ túi, máy tính cầm tay, máy tính để bàn, thiết bị máy với máy (M2M) hoặc thiết bị dạng MTC, bộ cảm biến với giao diện truyền thông không dây, v.v..

UMTS (Universal Mobile Telecommunications System - hệ thống viễn thông di động vạn năng) là hệ thống truyền thông di động thế hệ thứ ba, mà cải tiến từ GSM (Global System for Mobile Communications - hệ thống truyền thông di động toàn cầu), và nhằm cung cấp các dịch vụ truyền thông di động được cải thiện dựa trên công nghệ WCDMA (Wideband Code Division Multiple Access - đa truy cập phân mã dải

rộng). UTRAN, viết tắt cho mạng truy cập vô tuyến mặt đất UMTS, là thuật ngữ chung đối với cơ cấu kiểm soát của Nút B và cơ cấu kiểm soát mạng Vô tuyến mà tạo ra mạng truy cập vô tuyến UMTS. Do đó, UTRAN cơ bản là mạng truy cập vô tuyến sử dụng đa truy cập phân mã dải rộng (WCDMA) đối với các UE.

Dự án đối tác thế hệ thứ 3 (3GPP) đã đảm nhận để phát triển hơn nữa UTRAN và GSM dựa trên các công nghệ mạng truy cập vô tuyến. Về vấn đề này, các đặc tính đối với mạng truy cập vô tuyến mặt đất vạn năng tiên tiến (E-UTRAN) diễn ra trong phạm vi 3GPP. Mạng truy cập vô tuyến mặt đất vạn năng tiên tiến (E-UTRAN) bao gồm tiến triển dài hạn (LTE) và SAE (System Architecture Evolution - tiến triển kiến trúc hệ thống).

Ghi nhận rằng, mặc dù thuật ngữ học từ LTE được sử dụng chung trong bản mô tả này cho các phương án làm ví dụ theo sáng chế, điều này không nên được xem là giới hạn phạm vi của sáng chế chỉ đối với các hệ thống này. Các hệ thống không dây khác, bao gồm các biến đổi và các kế thừa của các hệ thống WCDMA và LTE 3GPP, WiMAX (hệ thống truy cập vi ba có tính tương tác toàn cầu), UMB (Ultra Mobile Broadband - Dải rộng siêu di động), HSDPA (Truy cập gói liên kết xuống tốc độ cao), GSM (Hệ thống truyền thông di động toàn cầu), v.v., còn có thể có lợi từ việc khai thác các phương án của sáng chế được bộc lộ trong bản mô tả này.

Còn ghi nhận rằng, thuật ngữ học này như trạm cơ sở (cũng được dùng để chỉ Nút B, eNodeB, hoặc Nút B tiên tiến) và thiết bị đầu cuối không dây hoặc thiết bị đầu cuối di động (cũng được dùng để chỉ nút trang thiết bị người dùng hoặc UE) nên được xem là không giới hạn và không ngụ ý mối quan hệ thứ bậc nào đó giữa 2 loại này. Nhìn chung, trạm cơ sở (ví dụ, "Nút B" hoặc "eNodeB") và thiết bị đầu cuối không dây (ví dụ, "UE") có thể được xem là các ví dụ về các thiết bị truyền thông khác nhau tương ứng mà truyền thông với nhau trên kênh vô tuyến không dây.

Trong khi các phương án được thảo luận trong bản mô tả này có thể tập trung vào các phương án làm ví dụ trong đó các giải pháp được mô tả được áp dụng trong các mạng không đồng nhất mà bao gồm hỗn hợp của các trạm cơ sở năng lượng tương đối cao (ví dụ, trạm cơ sở "vĩ mô", mà còn có thể được gọi là trạm cơ sở diện tích rộng hoặc các nút mạng trên diện tích rộng) và các nút năng lượng tương đối thấp (ví dụ,

trạm cơ sở "pico", mà còn có thể được gọi là trạm cơ sở diện tích cục bộ hoặc các nút mạng diện tích cục bộ), các kỹ thuật được mô tả có thể được áp dụng trong dạng phù hợp bất kỳ của mạng, bao gồm cả cấu hình không đồng nhất và đồng nhất. Do đó, trạm cơ sở liên quan trong các cấu hình được mô tả có thể là tương tự hoặc đồng dạng với nhau, hoặc có thể là khác khi xét đến năng lượng truyền, số lượng các anten của cơ cấu truyền-cơ cấu nhận, năng lượng xử lý, các đặc tính của cơ cấu nhận và cơ cấu truyền, và/hoặc khả năng vật lý hoặc chức năng bất kỳ khác.

E-UTRAN (Evolved UMTS Terrestrial Radio Access Network - Mạng truy cập vô tuyến mặt đất UMTS tiên tiến) bao gồm Nút B được cải thiện được gọi là trạm cơ sở (eNB hoặc eNodeB), tạo ra mặt phẳng người dùng E-UTRA và kết thúc giao thức mặt phẳng kiểm soát hướng theo UE. eNB được kết nối với nhau sử dụng giao diện X2. eNB còn được kết nối bằng cách sử dụng giao diện S1 đến EPC (Evolved Packet Core - Lõi gói tiên tiến), cụ thể hơn là đến MME (Mobility Management Entity - Thực thể quản lý tính di động) bởi giao diện S1-MME và đến cổng nối mạng dịch vụ (S-GW) bởi giao diện S1-U. Giao diện S1 hỗ trợ mối quan hệ nhiều-nhiều giữa MME/S-GW và eNB. Hình ảnh đơn giản của kiến trúc E-UTRAN được minh họa trên Fig.2.

eNB 210 giữ các chức năng như quản lý tài nguyên vô tuyến (RRM), kiểm soát vật mang vô tuyến, kiểm soát nhận vào, nén đầu của dữ liệu mặt phẳng người dùng hướng theo cổng nối mạng dịch vụ, và/hoặc đường đi của dữ liệu mặt phẳng người dùng hướng theo cổng nối mạng dịch vụ. MME 220 là nút kiểm soát mà xử lý việc phát tín hiệu giữa UE và CN (mạng lõi). Các chức năng rõ rệt của MME 220 liên quan đến quản lý kết nối và quản lý vật mang, mà được xử lý nhờ giao thức địa tầng không truy cập (NAS). S-GW 230 là điểm trạm đối với tính di động UE, và còn bao gồm các chức năng khác như dữ liệu đệm DL (liên kết xuống) tạm thời trong khi UE được đánh số trang, đường đi của gói và chuyển đến eNB bên phải, và/hoặc thu thập thông tin để tải và chắc chắn đúng luật. Cổng nối mạng PDN (P-GW, không được thể hiện trên Fig.2) là nút chịu trách nhiệm đối với việc định rõ địa chỉ UE IP, cũng như thực thi QoS (Quality of Service - chất lượng của dịch vụ) (như được thảo luận tiếp sau đây). Người đọc tham khảo 3GPP TS 36.300 và các tham khảo trong đó để có chi tiết hơn về các chức năng của các nút khác nhau.

Trong việc mô tả các phương án khác nhau theo sáng chế, thuật ngữ không giới hạn nút mạng vô tuyến có thể được dùng để chỉ dạng bất kỳ của UE phục vụ nút mạng và/hoặc được kết nối vào nút mạng khác hoặc yếu tố mạng hoặc nút vô tuyến bất kỳ từ đó UE nhận tín hiệu. Các ví dụ về các nút mạng vô tuyến là Nút B, BS (base station - trạm cơ sở), nút vô tuyến MSR (multi-standard radio - vô tuyến nhiều tiêu chuẩn) như cơ cấu kiểm soát mạng, của BS MSR, eNodeB, RNC (radio network controller - cơ cấu kiểm soát mạng vô tuyến), cơ cấu kiểm soát trạm cơ sở, phần chuyển tiếp, phần chuyển tiếp kiểm soát nút đono, BTS (base transceiver station - trạm thu phát cơ sở), AP (access point - điểm truy cập), chương trình chuyển vận không dây, các điểm truyền, các nút truyền, RRU (remote radio unit - bộ phận vô tuyến từ xa), RRH (remote radio head - đầu vô tuyến từ xa), các nút trong DAS (distributed antenna system - hệ thống anten phân phối), v.v..

Trong một số trường hợp, một thuật ngữ chung hơn "nút mạng" được sử dụng; thuật ngữ này có thể tương ứng với dạng bất kỳ của một nút mạng vô tuyến hoặc bất kỳ nút mạng mà truyền thông với ít nhất một nút mạng vô tuyến. Các ví dụ về các nút mạng là nút mạng vô tuyến bất kỳ được nêu trên đây, các nút mạng lõi (ví dụ, MSC, MME, v.v.), O&M, OSS, SON, nút định vị (ví dụ, E-SMLC), MDT, v.v..

Trong việc mô tả một số phương án, thuật ngữ trang thiết bị người dùng (UE) được sử dụng, và để chỉ dạng bất kỳ của thiết bị truyền thông không dây với một nút mạng vô tuyến trong hệ thống truyền thông mạng tế bào hoặc di động. Các ví dụ về các UE là các thiết bị đích, các UE thiết bị-đến-thiết bị, các UE dạng máy hoặc các UE có khả năng giao tiếp máy-đến-máy, các PDA, máy tính bàn được tạo khả năng không dây, thiết bị đầu cuối di động, điện thoại thông minh, LEE (laptop embedded equipped - máy tính xách tay được gắn vào được trang bị), LME (laptop mounted equipment - trang thiết bị gắn với máy tính xách tay), khóa điện tử USB, CPE (customer premises equipment - trang thiết bị theo ý khách hàng), v.v.. Thuật ngữ "thiết bị đầu cuối di động" như được sử dụng trong bản mô tả này nên được hiểu thường là trao đổi lẫn nhau với thuật ngữ UE như được sử dụng trong bản mô tả này và trong các đặc tính khác nhau được phổ biến bởi 3GPP, nhưng không nên được hiểu là chỉ giới hạn ở các thiết bị tuân theo các tiêu chuẩn 3GPP.

Các phương án làm ví dụ được thể hiện trong bản mô tả này được định hướng cụ thể về việc tạo ra khóa khi ngăn xếp giao thức Uu LTE được tách rời giữa tế bào vĩ mô và tế bào eNB hỗ trợ. Các kỹ thuật và thiết bị có thể áp dụng chung hơn về việc tạo ra khóa trong các bối cảnh kết nối kép khác.

Như đã ghi nhận trên đây, một lựa chọn để tách rời vật mang dữ liệu vô tuyến (các DRB) giữa 2 trạm cơ sở trong kịch bản kết nối kép là để giữ mặt phẳng kiểm soát, được điều khiển bằng giao thức kiểm soát tài nguyên vô tuyến (RRC), trong eNB trạm, trong khi phân phối các thực thể PDCP (Packet Data Convergence Protocol - giao thức hội tụ dữ liệu gói), mà được kết hợp với riêng vật mang vô tuyến, sao cho một hoặc nhiều trong số chúng được kết thúc trong eNB neo và một hoặc nhiều trong số chúng trong eNB hỗ trợ.

Tầng RRC tạo cấu hình tất cả các thực thể PDCP mà nó được kết hợp. Điều này được minh họa trên Fig.3, mà chỉ ra một ví dụ về kiến trúc giao thức đối với phức kết nối.

Cụ thể hơn, RRC tạo cấu hình các thực thể PDCP với các khóa mã hóa và dữ liệu cấu hình, như dữ liệu chỉ ra các thuật toán an toàn nên được áp dụng liên quan đến vật mang vô tuyến tương ứng. Đối với các kết nối kết hợp với thiết bị đầu cuối di động được đưa ra, RRC tạo cấu hình tất cả các thực thể PDCP đối với lưu lượng mặt phẳng người dùng (DRB) với một và cùng khóa mã hóa, KUP-enc, và tất cả các thực thể PDCP đối với lưu lượng mặt phẳng kiểm soát (SRB) với một và cùng khóa mã hóa, KRRC-enc, và một và cùng khóa bảo vệ tính tổng thể, KRRC-int. Đối với các DRB được sử dụng để bảo vệ dữ liệu giữa eNB đono cho và nút chuyển tiếp, RRC còn tạo cấu hình cho các DRB với khóa bảo vệ tính tổng thể, KUP-int.

Khi eNB neo và eNB hỗ trợ có thể được ứng dụng trong các nút vật lý riêng rẽ, giả thuyết rằng RRC có thể tạo cấu hình các thực thể PDCP nhờ các giao diện chương trình ứng dụng bên trong (các API) không còn giữ được nữa. Điều này có nghĩa là, tình huống hiện hành trong đó dữ liệu cấu hình an toàn có thể là giả thiết để được giữ an toàn bên trong môi trường an toàn vật lý của eNB không còn nữa. Thay vào đó, thực thể RRC trong eNB neo phải tạo cấu hình các thực thể PDCP trong eNB hỗ trợ, mà ở bên ngoài môi trường an toàn của eNB neo.

eNB neo và eNB hỗ trợ được sử dụng trong bản mô tả này để xác định các vai trò khác nhau của eNB từ UE hoặc thiết bị đầu cuối không dây tương ứng. Thừa nhận rằng, đây chỉ là một ví dụ đặt tên và chúng còn có thể được gọi là gì đó khác, như phần neo và phần tăng cường, chủ và tớ, hoặc đơn giản là eNB_1 và eNB_2.

Thiết kế an toàn của LTE thường tạo ra việc chia thành ngăn của các chức năng an toàn. Việc chia thành ngăn này có ý định để đảm bảo rằng nếu kẻ tấn công làm hỏng tính an toàn của một chức năng, thì chỉ chức năng đó bị ảnh hưởng. Ví dụ, có một khóa được sử dụng cho mã hóa của giao thức RRC và khóa khác được sử dụng cho việc bảo vệ tính tổng thể của giao thức RRC. Nếu kẻ tấn công làm hỏng khóa mã hóa, thì hắn có thể giải mã và đọc tất cả các tin nhắn RRC. Tuy nhiên, khi khóa tích hợp khác với khóa mã hóa, kẻ tấn công không thể làm biến đổi hoặc đưa vào các tin nhắn RRC.

Một khía cạnh khác của cách tiếp cận chia thành ngăn được sử dụng trong LTE đó là từng loại eNB sử dụng bộ khóa riêng. Cơ cở hợp lý cho điều này đó là cách tiếp cận này đảm bảo rằng kẻ tấn công đột nhập vào một eNB không nhận được thông tin bất kỳ về dữ liệu được truyền giữa thiết bị đầu cuối không dây và eNB khác về mặt vật lý khác. Trong kịch bản kết nối kép, khi đó, để duy trì đặc tính làm hỏng thành một nút RAN vật lý, tức là, eNB, không giúp trong việc tấn công nút RAN khác, eNB hỗ trợ nên sử dụng bộ khóa của chính nó, riêng rẽ với bộ khóa được sử dụng trong eNB neo.

Kiến trúc kết nối kép có thể mở 3 đường mới để tấn công an toàn tiềm năng, phụ thuộc vào các kỹ thuật được làm thích ứng để xử lý khóa an toàn và các thông số. Trước tiên, việc chuyển cấu hình an toàn và khóa mã hóa từ eNB neo vào eNB hỗ trợ đề xuất điểm ở đó kẻ tấn công có thể nghe trộm hoặc có thể làm biến đổi khóa và dữ liệu cấu hình. Thứ hai, kẻ tấn công có thể đột nhập về mặt vật lý vào eNB hỗ trợ, và nghe trộm hoặc làm biến đổi khóa và dữ liệu cấu hình ở đó. Ngoài ra, kẻ tấn công đột nhập về mặt vật lý vào eNB hỗ trợ có thể đọc, làm biến đổi hoặc xen lạc lõng dữ liệu mặt phẳng người dùng đối với thiết bị bất kỳ đầu cuối không dây được kết nối vào eNB hỗ trợ. Thứ ba, kẻ tấn công có thể truy cập và làm biến đổi dữ liệu mặt phẳng người dùng khi eNB hỗ trợ việc gửi và nhận nó. Điều này là đúng không kể nếu dữ liệu mặt phẳng người dùng chạy giữa eNB hỗ trợ và eNB neo, giữa eNB hỗ trợ và S-GW, hoặc nếu dữ liệu bị làm hỏng đến Internet cục bộ trong eNB hỗ trợ.

Các phương án làm ví dụ được bộc lộ trong bản mô tả này được định hướng theo việc tạo ra tập hợp khóa mã hoá an toàn để được sử dụng cho truyền thông giữa thiết bị đầu cuối không dây trong kết nối kép và eNB hỗ trợ. Trong một số phương án, khóa cơ sở đối với eNB hỗ trợ được tạo ra từ khóa an toàn của eNB neo. Khi đó, khóa cơ sở có thể được sử dụng để tạo ra các khóa cho sự truyền thông an toàn giữa thiết bị đầu cuối không dây và eNB hỗ trợ.

Thiết lập khóa đối với eNB hỗ trợ

Trong LTE, bộ khóa trong eNB bao gồm K_{eNB}, và $K_{UP\text{-}enc}$, $K_{RRC\text{-}enc}$ và $K_{RRC\text{-}int}$. Phụ thuộc vào các chức năng nào eNB hỗ trợ cung cấp, bộ khóa cần thiết bởi eNB hỗ trợ sẽ là khác nhau. Khi eNB hỗ trợ sẽ ít nhất kết thúc việc mã hóa mặt phẳng người dùng, là hữu dụng để thiết lập khóa mã hóa mà eNB hỗ trợ chia sẻ với thiết bị đầu cuối không dây. Nếu eNB hỗ trợ sẽ cung cấp các dịch vụ đối với các nút chuyển tiếp, ở đó còn nhu cầu đối với khóa tích hợp để bảo vệ các DRB mà mang lưu lượng mặt phẳng kiểm soát của nút chuyển tiếp. Kể từ đây là hữu dụng để thiết lập khóa cơ sở đối với eNB hỗ trợ, tương tự với K_{eNB}, từ đó khóa khác có thể được lấy ra. Kể từ phần trên đây, việc trình bày sẽ về thiết lập khóa cơ sở, được gọi là $K_{assiting\_eNB}$, nhưng với cùng lý do có thể được áp dụng hiển nhiên cho trường hợp trong đó, ví dụ, chỉ khóa mã hóa được thiết lập.

Fig.4 chỉ ra cách $K_{assiting\_eNB}$ có thể được tạo ra dựa trên K_{eNB} của eNB neo. Hình vẽ thể hiện thứ bậc khóa có thể đối với eNB hỗ trợ. Trong ví dụ này, eNB hỗ trợ và thiết bị đầu cuối không dây chia sẻ các khóa $K_{assiting\_eNB}$, $K_{assiting\_eNB\text{-}enc}$ và $K_{assiting\_eNB\text{-}int}$, tất cả trong số đó được lấy ra trực tiếp hoặc gián tiếp từ K_{eNB} đối với eNB neo.

Các mũi tên trên Fig.4 chỉ ra các ứng dụng của các KDF (Key Derivation Function - hàm lấy khóa ra). KDF có thể, đối với tất cả các mục đích thực tế, được xem là hàm một chiều. Như được biết rõ đối với những người quen với các kỹ thuật mã hóa, hàm một chiều là dễ dàng tính toán bằng máy tính theo hướng chuyển (hướng của mũi tên), nhưng bằng máy tính không thể làm được việc đảo ngược. Hàm ý của điều này đó là truy cập đến mức thấp hơn khóa trong thứ bậc khóa không đưa ra thông tin hữu dụng bất kỳ về khóa khi lên cao hơn về thứ bậc. Một ví dụ về KDF là chức

năng HMAC-SHA256, là KDF được sử dụng trong hệ LTE và trong nhiều hệ thống 3GPP khác.

Ví dụ cụ thể nằm trên Fig.4. Nếu khóa $K_{assiting\_eNB}$ được tạo ra trong eNB neo và được gửi đến eNB hỗ trợ, khi đó eNB hỗ trợ có truy cập đến $K_{assiting\_eNB}$ và khóa mã hóa và khóa tích hợp mà nó được lấy ra từ đó. Tuy nhiên, sẽ không có truy cập đến K_{eNB}.

Bởi vì có giả thiết rằng, các KDF là đã được biết đến, eNB trạm nút, mặt khác, sẽ có truy cập đến tất cả khóa được sử dụng bởi eNB hỗ trợ. Điều này làm hỏng nguyên lý chia thành ngăn nếu nó được dịch ra theo nghĩa nghiêm ngặt nhất của nó. Tuy nhiên, mức an toàn trong bối cảnh này tương tự mức an toàn thu được ở sự chuyển giao X2, là sự chuyển giao trong LTE mà được xử lý không có sự bao hàm của Thực thể quản lý tính di động (MME). Ở sự chuyển giao X2, eNB nguồn tính toán khóa mới dựa trên KeNB được sử dụng hiện hành và cung cấp khóa mới cho eNB đích. Một ví dụ khác của tình huống tương tự xuất hiện trong bối cảnh của các nút chuyển tiếp. Trong trường hợp của các nút chuyển tiếp, eNB đono tác động làm S1-proxy đối với nút chuyển tiếp. Kết quả là, eNB đono có truy cập đến tất cả các khóa được sử dụng bởi nút chuyển tiếp. Bởi vì tình huống an toàn là tương tự với một vài tình huống đã xuất hiện trong các mạng LTE, việc sử dụng K_{eNB} làm vật liệu khóa cơ sở đối với $K_{assiting\_eNB}$ có thể được xem là chấp nhận được từ quan điểm an toàn.

Thứ bậc khóa được thể hiện trên Fig.4 có thể được dùng có lợi trong kịch bản kết nối kép trong đó eNB neo kiểm soát các thực thể PDCP trong eNB hỗ trợ, tức là, eNB neo có thể thiết lập mới các thực thể PDCP, xóa chúng và khởi động lại các thực thể PDCP bị xóa trước đó. eNB neo và thiết bị đầu cuối di động (ví dụ, LTE UE) sẽ từng loại được lấy ra từ $K_{assiting\_eNB}$ từ KeNB như điều này: $K_{assiting\_eNB}$ = KDF(KeNB, other_params).

Để tránh được khả năng của tấn công đã được biết rõ mà khai thác việc truyền được lặp lại của dữ liệu được mã hóa mà mang dữ liệu cơ bản đã được biết đến, nên đảm bảo rằng $K_{assiting\_eNB}$ "mới" mỗi lần mà thực thể PDCP sử dụng lại cùng các giá trị COUNT. Do đó, tốt hơn là việc lấy ra $K_{assiting\_eNB}$ nên bao gồm thông số làm mới thích hợp. Một cách để đạt được tính mới là sử dụng nhiều trình tự COUNT PDCP mà được

kết hợp với thông điệp RRC được xác định trước nào đó, như lệnh thức an toàn RRC sau cùng hoặc lệnh chuyển giao, hoặc một trong các yếu cầu tạo lại cấu hình RRC hoặc các tin nhắn đầy đủ mà được sử dụng để thiết lập các thực thể PDCP trong eNB hỗ trợ. Số trình tự kết hợp với các tin nhắn RRC khác, tất nhiên có thể được sử dụng thay thế. Các lựa chọn khác để kết hợp việc làm mới vào việc tạo ra $K_{assiting\_eNB}$ bao gồm gửi "số này" mới từ thiết bị đầu cuối không dây đến eNB neo hoặc eNB hỗ trợ, từ eNB neo hoặc eNB hỗ trợ đến thiết bị đầu cuối không dây (hoặc cả hai hướng) trong (các) các thông điệp RRC được xác định trước nào đó hoặc các tin nhắn giao thức khác. Số này là số được tạo ra ngẫu nhiên (giả danh-), với xác xuất đủ cao, sẽ duy nhất khi xét đến K_{eNB}.

Bất kể thông số làm mới nào khi đó được bao gồm trong việc lấy ra $K_{assiting\_eNB}$ hoặc trong việc lấy ra của khóa được lấy ra từ $K_{assiting\_eNB}$. Còn có thể sử dụng lại các yếu tố thông tin hiện hành trong các tin nhắn RRC hoặc thông tin mà được truyền từ eNB neo hoặc eNB hỗ trợ trong các cụm hệ thống thông tin. Thông tin bất kỳ có thể được sử dụng chỉ cần là nó đưa ra đầu vào duy nhất (thống kê) với xác xuất đủ cao.

Thiết kế có thể thực hiện được khác là eNB neo được lấy ra từ $K_{assiting\_eNB}$ từ K_{eNB} không có thông số làm mới bất kỳ. Theo cách tiếp cận thay thế này, nếu eNB hỗ trợ hoặc eNB neo phát hiện ra rằng COUNT PDCP trong eNB hỗ trợ sắp bọc quanh, eNB neo bắt đầu làm mới lại KeNB khóa nhờ sự chuyển giao nội tế bào. Kết quả của sự chuyển giao nội tế bào đó là thiết bị đầu cuối không dây và eNB neo không chỉ làm mới lại K_{eNB}, mà cả $K_{assiting\_eNB}$; $K_{assiting\_eNB}$ có thể được tính toán lại theo cùng cách như nó được lấy ra lần đầu tiên. Cách tiếp cận này có thể đòi hỏi rằng, eNB hỗ trợ phải thông tin cho eNB neo về COUNT PDCP mà sắp được sử dụng lại.

Việc chuyển $K_{assiting\_eNB}$ từ eNB neo thành eNB hỗ trợ có thể được thực hiện trên kênh kiểm soát giữa cả 2 loại này. Kênh kiểm soát phải có tính cẩn mật và tính tổng thể được bảo vệ như đã được nêu.

Các thông số khác với các thông số được đề cập rõ ràng còn có thể được đưa vào KDF, trong các phương án khác nhau của các kỹ thuật được mô tả trên đây. Các thông số có thể được đặt trong trình tự bất kỳ trong số các trình tự khác nhau. Ngoài ra, bất kỳ một hoặc nhiều trong số các thông số đối với KDF có thể được biến đổi

trước khi được đưa vào KDF. Ví dụ, tập hợp các thông số P1, P2, …, Pn, đối với số n không âm, có thể được biến đổi bằng cách trước tiên chạy thông qua hàm số chuyển *f* và kết quả của nó, tức là, *f*(P1, P2, …, Pn), được đưa vào KDF.

Trong một ví dụ về việc lấy khóa ra, thông số P1 trước tiên được biến đổi trước khi được đưa vào KDF để tính khóa được gọi là "output_key": output_key = KDF(f(P1), P2), trong đó *f* là chức năng tùy ý nào đó hoặc chuỗi của các chức năng và P1 và P2 là các thông số được đưa vào. Thông số P2, ví dụ, có thể là 0, 1 hoặc nhiều thông số khác hơn, ví dụ, được sử dụng để ràng buộc khóa đến bối cảnh nào đó. Các thông số có thể được đưa vào làm các thông số riêng hoặc có thể được ghép cùng nhau và khi đó được đưa vào trong thông số đưa vào riêng đến KDF. Thậm chí khi các biến số của KDF như các biến số được sử dụng, cốt lõi của ý tưởng được duy trì là như nhau.

Không kể cách tiếp cận thiết lập khóa được sử dụng, quy trình chuyển giao hiện hành thường là không bị tác động khi việc xử lý trên thiết bị đầu cuối di động với kết nối kép vào trạm cơ sở khác, không kể dạng của trạm cơ sở đích. eNB neo có thể kéo mạnh xuống DRB trong eNB hỗ trợ và tiến hành sự chuyển giao cho trạm cơ sở đích theo các đặc tính kỹ thuật hiện hành.

Khi xử lý trên thiết bị đầu cuối không dây cho eNB đích và eNB hỗ trợ đích, việc lấy ra của khóa K_{eNB} và $K_{assiting\_eNB}$ có thể được thực hiện một cách riêng rẽ.

Lấy khóa ra dựa trên K_{ASME}

Thay cho việc sử dụng khóa cơ sở của nút neo làm cơ sở để tạo ra $K_{assiting\_eNB}$, khóa kết hợp với nút khác trong mạng không dây và đã được biết đến cho thiết bị đầu cuối di động có thể được sử dụng thay thế. Ví dụ, sử dụng K_{ASME} làm vật liệu khóa cơ sở đối với $K_{assiting\_eNB}$, như được thể hiện trên Fig.5, cho phép đối với mức an toàn cao hơn, so với việc sử dụng K_{eNB}được mô tả trên đây. Như thấy được trên Fig.5, $K_{assiting\_eNB}$ có thể được lấy ra từ K_{ASME}, và khóa mã hóa và khóa tích hợp đối với eNB hỗ trợ được lấy ra từ $K_{assiting\_eNB}$ tạo thành.

K_{ASME} là khóa được thiết lập nhờ sự xác thực thuê bao trong LTE, và nó được chia sẻ giữa MME và thiết bị đầu cuối không dây. Nếu $K_{assiting\_eNB}$ được lấy ra từ

K_{ASME} và MME làm cho eNB hỗ trợ với $K_{assiting\_eNB}$ này một cách trực tiếp, khi đó nút neo không có truy cập đến $K_{assiting\_eNB}$ hoặc khóa mã hóa và khóa tích hợp được lấy ra từ nó. Trong trường hợp này, khi đó, nguyên lý chia thành ngăn được thảo luận trên đây được tham gia vào với nghĩa nghiêm ngặt hơn.

Dựa trên việc lấy ra $K_{assiting\_eNB}$ trên K_{ASME} đòi hỏi rằng MME được làm nhận biết được khi eNB hỗ trợ cần truy cập đến khóa, và còn đòi hỏi rằng có đường truyền thông giữa 2 loại này. Xem MME có nhận biết được khi thiết bị đầu cuối không dây được kết nối với eNB hỗ trợ (và kể từ đây khóa là cần thiết) và xem có đường tín hiệu giữa MME hay không và eNB hỗ trợ phụ thuộc vào cách thức eNB hỗ trợ được kiểm soát. Nếu các điều kiện này không thỏa mãn, việc sử dụng K_{ASME} làm cơ sở vật liệu khóa là kém hữu dụng, mặc dù vẫn còn có thể, bởi vì MME sẽ phải gửi $K_{assiting\_eNB}$ đến nút neo, mà, đến lượt, cung cấp nó cho eNB hỗ trợ. Tất nhiên, trong bối cảnh này, nút neo có truy cập đến $K_{assiting\_eNB}$.

Sử dụng K_{ASME} làm phương tiện cơ sở của vật liệu khóa mà $K_{assiting\_eNB}$ được lấy ra từ K_{ASME} nhờ sử dụng khóa lấy ra chức năng $K_{assiting\_eNB}$= KDF(K_{ASME}, [other_params]), trong đó other_params tùy chọn có thể bao gồm một hoặc nhiều thông số làm mới.

Như được mô tả trên đây, khi cơ cấu đếm gói PDCP (COUNT PDCP) được thiết lập lại, khóa mã hóa và khóa tích hợp nên được làm mới lại. Nếu cùng khóa được sử dụng với cùng COUNT PDCP, ở đó sẽ là sử dụng lại dòng khóa, và một cách tiềm năng, thực hiện lại tấn công có thể. Do đó, MME và thiết bị đầu cuối không dây có thể bao gồm thông số làm mới trong việc lấy khóa ra. Ví dụ, cùng thông số làm mới như thông số được sử dụng khi K_{eNB} được lấy ra đối với nút neo (eNB). Thông số làm mới được sử dụng cho việc lấy K_{eNB} ra có thể phụ thuộc vào tình huống. Thông số làm mới có thể bao gồm các số này (các số ngẫu nhiên được sử dụng một lần) mà MME và thiết bị đầu cuối không dây trao đổi. Các khả năng khác là cơ cấu đếm gói như COUNT liên kết xuống hoặc liên kết lên NAS, hoặc cơ cấu đếm được đưa vào mới mà được truyền hoặc là từ thiết bị đầu cuối không dây đến MME hoặc từ MME đến thiết bị đầu cuối không dây. Một hạn chế với cơ cấu đếm được đưa vào mới đó là nếu nó đưa ra đồng bộ, có thể được đồng bộ lại bởi cơ chế đồng bộ lại mới.

Các thông số khác có thể cũng được bao gồm trong việc lấy $K_{assiting\_eNB}$ ra. Ví dụ, việc nhận diện của eNB hỗ trợ hoặc tế bào mà eNB hỗ trợ sử dụng có thể được sử dụng làm tín hiệu được đưa vào. Điều này là tương tự với việc K_{eNB} được liên kết vào cách nhận diện tế bào. Mục đích còn có thể là chia thành ngăn tiếp với các phạm vi an toàn tiềm năng.

Một khi MME lấy ra $K_{assiting\_eNB}$, MME còn phải chuyển nó thành eNB hỗ trợ. Việc chuyển $K_{assiting\_eNB}$ thành eNB hỗ trợ có thể được xử lý theo một trong 2 cách, hoặc là trực tiếp thành eNB hỗ trợ, hoặc gián tiếp, bởi trước tiên chuyển $K_{assiting\_eNB}$ thành eNB và khi đó để cho eNB chuyển nó thành eNB hỗ trợ khi cần thiết.

Thường là một ưu điểm an toàn để chuyển $K_{assiting\_eNB}$ trực tiếp từ MME thành eNB hỗ trợ. Theo cách này, chỉ có MME, eNB hỗ trợ và thiết bị đầu cuối không dây biết khóa. Nếu việc phát tín hiệu để thiết lập kết nối giữa eNB hỗ trợ và thiết bị đầu cuối không dây là sao cho MME có liên quan, khi đó điều này được ưu tiên.

Một dạng thay đổi khác là đối với MME để gửi $K_{assiting\_eNB}$ đến eNB, mà đơn giản chuyển $K_{assiting\_eNB}$ thành eNB hỗ trợ. Cách tiếp cận này có hạn chế về mặt an toàn trong đó eNB giờ đây còn là dấu hiệu của $K_{assiting\_eNB}$. Tuy nhiên, nếu cách tiếp cận có thể là hữu dụng, nếu không có đường phát tín hiệu trực tiếp giữa MME và eNB hỗ trợ và K_{ASME} là vật liệu khóa được sử dụng làm cơ sở đối với việc lấy ra $K_{assiting\_eNB}$.

Phương pháp làm ví dụ

Theo các ví dụ được nêu chi tiết được mô tả trên đây, sẽ đánh giá được rằng, các hình vẽ Fig.6 và Fig.7 là sơ đồ tiến trình mô tả các vận hành làm ví dụ mà có thể được lấy bởi nút mạng và thiết bị đầu cuối không dây, tương ứng, trong đó mạng có thể là trạm cơ sở neo hoặc MME, trong các phương án khác nhau. Sơ đồ tiến trình được minh họa bao gồm một số vận hành mà được minh họa với các đường viền đậm và một số vận hành mà được minh họa với đường nét rời. Các vận hành mà được bao gồm ở các đường viền đậm là các vận hành mà được bao gồm trong các phương án làm ví dụ rộng nhất. Các vận hành mà được bao gồm ở đường nét rời là các phương án làm ví dụ mà có thể được bao gồm trong, hoặc một phần của, hoặc còn là các vận hành khác mà có thể được lấy ngoài các vận hành của các phương án làm ví dụ rộng hơn. Do đó, các vận hành được thể hiện ở các đường nét rời có thể được xem là "tùy ý" với nghĩa là chúng có thể

không xuất hiện trong từng ví dụ về trong từng phương án của quy trình được minh họa. Còn nên đánh giá được rằng, các vận hành của Fig.6 và Fig.7 chỉ được đề xuất làm ví dụ.

Cụ thể hơn, Fig.6 minh họa quy trình để tạo ra khóa an toàn hỗ trợ để sử dụng bởi trạm cơ sở hỗ trợ trong kịch bản kết nối kép. Quy trình được thể hiện trên Fig.6 có thể được ứng dụng trong nút mạng, như trong trạm cơ sở neo (ví dụ, eNB neo LTE) hoặc trong mạng khác nào đó, như MME. Như được thể hiện ở khối 10, nút mạng trước tiên xác định nhu cầu đối với khóa an toàn hỗ trợ để được tạo ra. Điều này có thể được khởi động bằng cách thiết lập kịch bản kết nối kép, chẳng hạn. Khi đáp ứng với việc xác định này, nút mạng tạo ra khóa an toàn hỗ trợ, dựa ít nhất một phần trên khóa an toàn chính. Điều này được thể hiện ở khối 12. Như được giải thích chi tiết trên đây, khóa an toàn chính này có thể là, trong các phương án khác nhau, khóa cơ sở nút neo (ví dụ, K_{eNB}) hoặc khóa khác mà đã được biết đến cho nút mạng và cho thiết bị đầu cuối di động quan tâm, như khóa MME (ví dụ, K_{ASME}).

Việc tạo ra khóa an toàn hỗ trợ có thể kết hợp việc sử dụng KDF, ví dụ, chức năng mã hóa một chiều, cũng như một hoặc nhiều thông số làm mới, như được thể hiện ở các khối 12 và 16. Danh mục các thông số làm mới mà đã được sử dụng có thể được duy trì trong một số phương án, như được thể hiện ở khối 17.

Như được thể hiện ở khối 18, khi đó, khóa an toàn hỗ trợ được tạo ra được gửi đến trạm cơ sở hỗ trợ. Trong một số trường hợp, như được nêu chi tiết trên đây, khóa an toàn hỗ trợ khi đó được sử dụng để tạo ra một hoặc nhiều khóa bổ sung để bảo vệ dữ liệu được chuyển đến và từ thiết bị đầu cuối di động, mặc dù khóa an toàn hỗ trợ có thể được sử dụng trực tiếp cho các mục đích này, trong một số phương án.

Fig.7 minh họa phương pháp tương ứng như có thể được tiến hành ở thiết bị đầu cuối di động. Như được thể hiện ở khối 30, thiết bị đầu cuối di động tạo ra khóa an toàn hỗ trợ, dựa ít nhất một phần trên cùng khóa an toàn chính, được sử dụng bởi nút mạng trên Fig.6. Một lần nữa, khóa an toàn chính này có thể là, trong các phương án khác nhau, khóa cơ sở nút neo (ví dụ, K_{eNB}) hoặc khóa khác mà đã được biết đến cho nút mạng và cho thiết bị đầu cuối di động quan tâm, như khóa MME (ví dụ, K_{ASME}). Việc tạo ra khóa an toàn hỗ trợ có thể kết hợp việc sử dụng KDF, ví dụ, chức năng mã

hóa một chiều, cũng như một hoặc nhiều thông số làm mới, như được thể hiện ở các khối 32 và 34. Danh mục thông số làm mới mà đã được sử dụng có thể được duy trì trong một số phương án, như được thể hiện ở khối 17.

Như được thể hiện ở khối 36, khi đó, khóa an toàn hỗ trợ được tạo ra được áp dụng cho việc bảo vệ dữ liệu được gửi đến và từ trạm cơ sở hỗ trợ. Trong một số trường hợp, như được nêu chi tiết trên đây, khóa an toàn hỗ trợ được sử dụng để tạo ra một hoặc nhiều khóa bổ sung để bảo vệ dữ liệu được chuyển đến và từ thiết bị đầu cuối di động, mặc dù khóa an toàn hỗ trợ có thể được sử dụng trực tiếp cho các mục đích này, trong một số phương án.

Như được thảo luận trên đây, khóa an toàn hỗ trợ có thể được tạo ra từ nút neo khóa hoặc từ khóa an toàn tương ứng với nút khác, như MME, trong các phương án khác nhau. Các hình vẽ Fig.8 và Fig.9 là các sơ đồ tiến trình tương ứng lần lượt với hai bối cảnh này. Các phương pháp này có thể được tiến hành trong mạng LTE, ví dụ, nhưng còn có thể được áp dụng cho các mạng không dây khác mà dùng kết nối kép.

Do đó, Fig.8 minh họa phương pháp, phù hợp để ứng dụng trong nút mạng, để tạo ra khóa an toàn cho các sự truyền thông an toàn giữa thiết bị đầu cuối không dây và trạm cơ sở neo và giữa thiết bị đầu cuối không dây và trạm cơ sở hỗ trợ, trong đó thiết bị đầu cuối không dây được hoặc sắp được kết nối kép vào trạm cơ sở neo và trạm cơ sở hỗ trợ. Như được thể hiện ở khối 810, phương pháp được minh họa bao gồm việc tạo ra khóa an toàn hỗ trợ đối với trạm cơ sở hỗ trợ, dựa ít nhất một phần trên khóa trạm cơ sở neo. Như được thể hiện ở khối 820, khi đó, khóa an toàn hỗ trợ được tạo ra được gửi đến trạm cơ sở hỗ trợ, để sử dụng bởi trạm cơ sở hỗ trợ trong việc mã hóa lưu lượng dữ liệu được gửi đến thiết bị đầu cuối không dây hoặc trong việc tạo ra một hoặc nhiều khóa an toàn hỗ trợ bổ sung để mã hóa lưu lượng dữ liệu được gửi đến thiết bị đầu cuối không dây bởi trạm cơ sở hỗ trợ trong khi thiết bị đầu cuối không dây được kết nối kép vào trạm cơ sở neo và trạm cơ sở hỗ trợ. Như được thể hiện ở khối 830, khóa trạm cơ sở neo, hoặc khóa được lấy ra từ khóa trạm cơ sở neo, được sử dụng để mã hóa dữ liệu được gửi đến thiết bị đầu cuối không dây bởi trạm cơ sở neo trong khi thiết bị đầu cuối không dây được kết nối kép vào trạm cơ sở neo và trạm cơ sở hỗ trợ.

Trong một số phương án của phương pháp được minh họa trên Fig.8, khóa an toàn hỗ trợ được tạo ra bao gồm khóa an toàn hỗ trợ cơ sở để sử dụng trong việc tạo ra một hoặc nhiều khóa an toàn hỗ trợ bổ sung để mã hóa lưu lượng dữ liệu được gửi đến thiết bị đầu cuối không dây bởi trạm cơ sở hỗ trợ. Trong một số phương án từ các phương án này, trạm cơ sở neo và thiết bị đầu cuối di động có thể từng loại được lấy ra từ khóa mã hóa, hoặc khóa tích hợp, hoặc cả hai, từ khóa trạm cơ sở neo, và sử dụng khóa hoặc các khóa được lấy ra để bảo vệ dữ liệu được gửi đến hoặc được nhận từ thiết bị đầu cuối không dây bởi trạm cơ sở neo trong khi thiết bị đầu cuối không dây được kết nối kép vào trạm cơ sở neo và trạm cơ sở hỗ trợ.

Trong một số phương án được thể hiện trên Fig.8, mà tạo ra khóa an toàn hỗ trợ bao gồm việc lấy ra khóa an toàn hỗ trợ từ khóa trạm cơ sở neo sử dụng hàm một chiều. Hàm một chiều có thể là hàm mã hóa HMAC-SHA-256, trong một số phương án. Trong một số phương án này và trong một số phương án khác, việc tạo ra khóa an toàn hỗ trợ còn dựa trên thông số làm mới.

Trong một số phương án, phương pháp được minh họa còn có thể bao gồm việc phát hiện rằng, thông số COUNT của giao thức hội tụ gói Dữ liệu (PDCP) trong trạm cơ sở hỗ trợ sắp bọc quanh và, khi đáp ứng, bắt đầu việc làm mới khóa trạm cơ sở neo và tính toán lại khóa an toàn hỗ trợ.

Trong một số phương án, khóa an toàn hỗ trợ đơn được sử dụng để tạo ra tập hợp các khóa để sử dụng trong tất cả các vật mang dữ liệu vô tuyến. Trong các phương án khác, khóa an toàn hỗ trợ phức có thể được sử dụng, trong trường hợp đó vận hành tạo ra được mô tả trên đây được lặp lại đối với mỗi trong số nhiều vật mang dữ liệu vô tuyến được thiết lập giữa thiết bị đầu cuối không dây và trạm cơ sở hỗ trợ, sao cho khóa an toàn hỗ trợ tạo thành là khác đối với mỗi vật mang dữ liệu vô tuyến. Các phức của một vài khóa tạo thành có thể được gửi đồng thời, trong một số phương án.

Fig.9 là sơ đồ tiến trình minh họa phương pháp khác để tạo ra khóa an toàn hỗ trợ đối với trạm cơ sở hỗ trợ. Giống như phương pháp được thể hiện trên Fig.8, quy trình của Fig.9 là phù hợp để ứng dụng trong nút mạng, để tạo ra khóa an toàn cho các sự truyền thông an toàn giữa thiết bị đầu cuối không dây và trạm cơ sở neo và giữa thiết bị đầu cuối không dây và trạm cơ sở hỗ trợ, trong đó thiết bị đầu cuối không dây

được hoặc sắp được kết nối kép vào trạm cơ sở neo và trạm cơ sở hỗ trợ. Tuy nhiên, trong phương pháp này, phương pháp có thể được tiến hành trong nút mạng khác với trạm cơ sở neo, sử dụng khóa chính mà có thể không được biết đến đối với trạm cơ sở neo.

Như được thể hiện ở khối 910, phương pháp được minh họa bao gồm việc chia sẻ khóa an toàn chính với thiết bị đầu cuối không dây. Khóa này có thể không được biết đến đối với trạm cơ sở neo, trong một số phương án. Một ví dụ là khóa K_{ASME} được thảo luận trên đây, mà được chia sẻ giữa MME LTE và thiết bị đầu cuối di động.

Như được thể hiện ở khối 920, phương pháp tiếp tục với việc tạo ra khóa an toàn hỗ trợ đối với trạm cơ sở hỗ trợ, dựa ít nhất một phần trên khóa an toàn chính. Khi đó, khóa an toàn hỗ trợ được tạo ra được gửi đến trạm cơ sở hỗ trợ, như được thể hiện ở khối 930, để sử dụng bởi trạm cơ sở hỗ trợ trong việc mã hóa lưu lượng dữ liệu được gửi đến thiết bị đầu cuối không dây hoặc trong việc tạo ra một hoặc nhiều khóa an toàn hỗ trợ bổ sung để mã hóa lưu lượng dữ liệu được gửi đến thiết bị đầu cuối không dây bởi trạm cơ sở hỗ trợ trong khi thiết bị đầu cuối không dây được kết nối kép vào trạm cơ sở neo và trạm cơ sở hỗ trợ. Trong một số phương án, khóa an toàn hỗ trợ được tạo ra được gửi trực tiếp đến trạm cơ sở hỗ trợ sao cho trạm cơ sở neo không là dấu hiệu của khóa, trong khi, trong các phương án khác, khóa an toàn hỗ trợ được tạo ra được gửi đến trạm cơ sở hỗ trợ một cách gián tiếp, nhờ trạm cơ sở neo.

Trong một số phương án, khóa an toàn hỗ trợ được tạo ra bao gồm khóa an toàn hỗ trợ cơ sở để sử dụng trong việc tạo ra một hoặc nhiều khóa an toàn hỗ trợ bổ sung để mã hóa lưu lượng dữ liệu được gửi đến thiết bị đầu cuối không dây bởi trạm cơ sở hỗ trợ. Trong một số phương án này và trong một số phương án khác, việc tạo ra khóa an toàn hỗ trợ bao gồm việc lấy ra khóa an toàn hỗ trợ từ khóa trạm cơ sở neo sử dụng hàm một chiều. Hàm một chiều có thể là hàm mã hóa HMAC-SHA-256, chẳng hạn. Như được thảo luận chi tiết trên đây, việc tạo ra khóa an toàn hỗ trợ có thể là còn dựa trên thông số làm mới, trong một số phương án.

Phương án thực hiện phần cứng làm ví dụ

Một vài trong số các kỹ thuật và các phương pháp được mô tả trên đây có thể được ứng dụng nhờ sử dụng mạch xử lý dữ liệu điện tử và mạch vô tuyến hoặc mạch

giao diện khác được bố trí trong nút mạng, như trạm cơ sở neo hoặc trong MME, trong khi các dạng khác có thể được ứng dụng nhờ sử dụng mạch vô tuyến và mạch xử lý dữ liệu điện tử được bố trí trong thiết bị đầu cuối không dây.

Fig.10 minh họa cấu hình nút làm ví dụ về trạm cơ sở neo 401A mà có thể tiến hành một số phương án làm ví dụ được mô tả trong bản mô tả này. Trạm cơ sở neo 401A có thể bao gồm mạch vô tuyến hoặc cổng truyền thông 410A mà có thể được tạo cấu hình để nhận và/hoặc truyền các số đo, dữ liệu, các lệnh, và/hoặc các tin nhắn truyền thông. Trạm cơ sở neo 401A còn có thể bao gồm mạch giao diện mạng 440A mà có thể được tạo cấu hình để nhận hoặc gửi các mạng truyền thông, ví dụ, đến và từ các nút mạng khác. Nên đánh giá được rằng, mạch vô tuyến hoặc cổng truyền thông 410A có thể được bao gồm là số lượng bất kỳ của việc thu phát, nhận, và/hoặc các cơ cấu hoặc mạch truyền. Còn đánh giá được rằng, mạch vô tuyến hoặc truyền thông 410A có thể ở dạng cổng truyền thông vào hoặc ra bất kỳ đã được biết đến trong ngành. Mạch vô tuyến hoặc truyền thông 410A và/hoặc mạng giao diện 440A có thể bao gồm mạch RF và mạch xử lý dải cơ sở, chi tiết về chúng được biết rõ đối với những người quen với thiết kế trạm cơ sở.

Trạm cơ sở neo 401A còn có thể bao gồm mạch hoặc bộ phận xử lý 420A mà có thể được tạo cấu hình để thực hiện các hoạt động liên quan đến việc tạo ra khóa an toàn hỗ trợ (ví dụ, khóa an toàn đối với eNB hỗ trợ), như được mô tả trong bản mô tả này. Mạch xử lý 420A có thể có dạng cơ cấu tính toán phù hợp bất kỳ, ví dụ bộ vi xử lý, DSP (digital signal processor - bộ xử lý tín hiệu số), FPGA (field programmable gate array - mảng cổng lập trình được theo trường), hoặc ASIC (application specific integrated circuit - mạch tích hợp chuyên dụng), hoặc dạng mạch bất kỳ khác. Trạm cơ sở neo 401A còn có thể bao gồm mạch hoặc bộ nhớ 430A mà có thể có dạng phù hợp bất kỳ của bộ nhớ đọc được bằng máy tính và có thể có dạng khả biến hoặc không khả biến. Bộ nhớ 430A có thể được tạo cấu hình để lưu trữ thông tin được nhận, được truyền, và/hoặc thông tin bất kỳ liên quan đến việc tạo ra khóa an toàn hoặc thông số làm mới, các thông số thiết bị, các ưu tiên truyền thông, và/hoặc các lệnh thực thi được của chương trình.

Các chức năng thông thường của mạch xử lý 420A, ví dụ, khi được tạo cấu hình với mã chương trình phù hợp được lưu trữ trong bộ nhớ 430A, bao gồm sự điều biến và sự mã hóa tín hiệu được truyền và sự giải điều biến và sự giải mã các tín hiệu được nhận. Trong một số phương án của sáng chế, mạch xử lý 420A được làm thích ứng, sử dụng mã chương trình phù hợp được lưu trữ trong bộ nhớ lưu trữ chương trình 430A, ví dụ, để thực hiện một trong các kỹ thuật được mô tả trên đây để xử lý khóa an toàn trong kịch bản kết nối kép. Tất nhiên, sẽ đánh giá được rằng, không phải tất cả các bước của các kỹ thuật này cần thiết được thực hiện trong bộ vi xử lý đơn hoặc thậm chí trong mô đun đơn.

Sẽ đánh giá được rằng, mạch xử lý 420A, như được làm thích ứng với mã chương trình được lưu trữ trong chương trình và bộ nhớ dữ liệu 430A, có thể ứng dụng sơ đồ tiến trình của Fig.8 (hoặc dạng biến đổi của nó) sử dụng cách bố trí của "các mô đun" chức năng, trong đó các mô đun là các chương trình máy tính hoặc các phần của chương trình máy tính thực thi trên mạch của bộ xử lý 420A. Do đó, thiết bị 401A có thể được hiểu là bao gồm giao diện truyền thông 440A được tạo cấu hình để truyền thông với trạm cơ sở hỗ trợ, và còn bao gồm một vài mô đun chức năng được ứng dụng trong mạch xử lý 420A. Các mô đun chức năng này bao gồm: mô đun tạo ra để tạo ra khóa an toàn hỗ trợ đối với trạm cơ sở hỗ trợ, dựa ít nhất một phần trên khóa trạm cơ sở neo; mô đun gửi để gửi đến trạm cơ sở hỗ trợ, sử dụng mạch giao diện, khóa an toàn hỗ trợ được tạo ra, để sử dụng bởi trạm cơ sở hỗ trợ trong việc mã hóa lưu lượng dữ liệu được gửi đến thiết bị đầu cuối không dây hoặc trong việc tạo ra một hoặc nhiều khóa an toàn hỗ trợ bổ sung để mã hóa lưu lượng dữ liệu được gửi đến thiết bị đầu cuối không dây bởi trạm cơ sở hỗ trợ trong khi thiết bị đầu cuối không dây được kết nối kép vào trạm cơ sở neo và trạm cơ sở hỗ trợ; và mô đun mã hóa để sử dụng khóa trạm cơ sở neo, hoặc khóa được lấy ra từ khóa trạm cơ sở neo, để mã hoá dữ liệu được gửi đến thiết bị đầu cuối không dây bởi trạm cơ sở neo trong khi thiết bị đầu cuối không dây được kết nối kép vào trạm cơ sở neo và trạm cơ sở hỗ trợ.

Fig.11 minh họa cấu hình nút làm ví dụ về nút quản lý tính di động 505A (ví dụ, MME, SGSN, S4-SGSN) mà có thể tiến hành một số phương án làm ví dụ được mô tả trong bản mô tả này. Nút quản lý tính di động 505A có thể bao gồm mạch giao diện hoặc cổng truyền thông 510A mà có thể được tạo cấu hình để nhận và/hoặc

truyền các số đo, dữ liệu, các lệnh, và/hoặc các tin nhắn truyền thông. Nên đánh giá được rằng, mạch vô tuyến hoặc cổng truyền thông 510A có thể được bao gồm là số lượng bất kỳ của việc thu phát, nhận, và/hoặc các cơ cấu hoặc mạch truyền. Còn đánh giá được rằng, mạch vô tuyến hoặc truyền thông 510A có thể ở dạng cổng truyền thông vào hoặc ra bất kỳ đã được biết đến trong ngành. Mạch giao diện hoặc truyền thông 510A có thể bao gồm mạch RF và mạch xử lý dải cơ sở (không được thể hiện trên hình vẽ).

Nút quản lý tính di động 505A còn có thể bao gồm mạch hoặc bộ phận xử lý 520A mà có thể được tạo cấu hình để thực hiện các hoạt động liên quan đến việc tạo ra khóa an toàn hỗ trợ (ví dụ, khóa an toàn đối với eNB hỗ trợ), như được mô tả trong bản mô tả này. Mạch xử lý 520A có thể có dạng bộ phận tính toán phù hợp bất kỳ, ví dụ bộ vi xử lý, bộ xử lý tín hiệu số (DSP), mảng cổng lập trình được dạng trường (FPGA), hoặc mạch tích hợp chuyên dụng (ASIC), hoặc dạng mạch bất kỳ khác. Nút quản lý tính di động 505A còn có thể bao gồm mạch hoặc bộ nhớ 530A mà có thể có dạng phù hợp bất kỳ của bộ nhớ đọc được bằng máy tính và có thể có dạng khả biến hoặc không khả biến. Bộ nhớ 530A có thể được tạo cấu hình để lưu trữ thông tin được nhận, được truyền, và/hoặc thông tin bất kỳ liên quan đến việc tạo ra khóa an toàn hoặc thông số làm mới, các thông số thiết bị, các ưu tiên truyền thông, và/hoặc các lệnh thực thi được của chương trình để sử dụng bởi mạch xử lý 520A.

Trong một số phương án của sáng chế, mạch xử lý 520A được làm thích ứng, sử dụng mã chương trình phù hợp được lưu trữ trong bộ nhớ lưu trữ chương trình 530A, ví dụ, để thực hiện một trong các kỹ thuật được mô tả trên đây để xử lý khóa an toàn trong kịch bản kết nối kép. Tất nhiên, sẽ đánh giá được rằng, không phải tất cả các bước của các kỹ thuật này cần thiết được thực hiện trong bộ vi xử lý đơn hoặc thậm chí trong mô đun đơn.

Sẽ đánh giá được rằng, mạch xử lý 520A, như được làm thích ứng với mã chương trình được lưu trữ trong bộ nhớ dữ liệu và chương trình 530A, có thể thực hiện tiến trình trên Fig.9 (hoặc dạng biến đổi của nó) sử dụng cách bố trí của "các mô đun" chức năng, trong đó các mô đun là các chương trình máy tính hoặc các phần của chương trình máy tính thực thi trên mạch của bộ xử lý 520A. Do đó, thiết bị 501A có

thể được hiểu là bao gồm giao diện truyền thông 540A được tạo cấu hình để truyền thông với trạm cơ sở hỗ trợ, và còn bao gồm một vài mô đun chức năng được ứng dụng trong mạch xử lý 520A. Các các mô đun chức năng này bao gồm: mô đun chia sẻ để chia sẻ khóa an toàn chính với thiết bị đầu cuối không dây; mô đun tạo ra để tạo ra khóa an toàn hỗ trợ đối với trạm cơ sở hỗ trợ, dựa ít nhất một phần trên khóa an toàn chính; và mô đun gửi để gửi đến trạm cơ sở hỗ trợ, thông qua mạch giao diện, khóa an toàn hỗ trợ được tạo ra, để sử dụng bởi trạm cơ sở hỗ trợ trong việc mã hóa lưu lượng dữ liệu được gửi đến thiết bị đầu cuối không dây hoặc trong việc tạo ra một hoặc nhiều khóa an toàn hỗ trợ bổ sung để mã hóa lưu lượng dữ liệu được gửi đến thiết bị đầu cuối không dây bởi trạm cơ sở hỗ trợ trong khi thiết bị đầu cuối không dây được kết nối kép vào trạm cơ sở neo và trạm cơ sở hỗ trợ. Fig.12 minh họa cấu hình nút làm ví dụ về thiết bị đầu cuối không dây 505B mà có thể được tạo cấu hình để thực hiện một số phương pháp làm ví dụ được mô tả trong bản mô tả này. Thiết bị đầu cuối không dây 505B có thể bao gồm mạch giao diện hoặc cổng truyền thông 510B mà có thể được tạo cấu hình để nhận và/hoặc truyền các số đo, dữ liệu, các lệnh, và/hoặc các tin nhắn truyền thông. Nên đánh giá được rằng, mạch vô tuyến hoặc cổng truyền thông 510B có thể được bao gồm với số lượng bất kỳ của các bộ phận hoặc mạch thu phát, nhận, và/hoặc truyền. Còn đánh giá được rằng, mạch vô tuyến hoặc truyền thông 510B có thể ở dạng cổng truyền thông vào hoặc ra bất kỳ đã được biết đến trong lĩnh vực. Mạch giao diện hoặc truyền thông 510B có thể bao gồm mạch RF và mạch xử lý dải cơ sở (không được thể hiện trên hình vẽ).

Thiết bị đầu cuối không dây 505B còn có thể bao gồm mạch hoặc bộ phận xử lý 520B mà có thể được tạo cấu hình để thực hiện các hoạt động liên quan đến việc tạo ra khóa an toàn hỗ trợ (ví dụ, khóa an toàn đối với eNB hỗ trợ), như được mô tả trong bản mô tả này. Mạch xử lý 520B có thể có dạng cơ cấu tính toán phù hợp bất kỳ, ví dụ bộ vi xử lý, bộ xử lý tín hiệu số (DSP), mảng cổng lập trình được dạng trường (FPGA), hoặc mạch tích hợp chuyên dụng (ASIC), hoặc dạng bất kỳ khác của mạch. Thiết bị đầu cuối không dây 505B còn có thể bao gồm bộ nhớ hoặc mạch 530B mà có thể có dạng phù hợp bất kỳ của bộ nhớ đọc được bằng máy tính và có thể có dạng khả biến hoặc không khả biến. Bộ nhớ 530B có thể được tạo cấu hình để lưu trữ thông tin được nhận, được truyền, và/hoặc thông tin bất kỳ liên quan đến việc tạo ra khóa an

toàn hoặc thông số làm mới, các thông số thiết bị, các ưu tiên truyền thông, và/hoặc các lệnh thực thi được của chương trình.

Do đó, trong các phương án khác nhau của sáng chế, các mạch xử lý, như các mạch xử lý 520A và 520B và các mạch bộ nhớ tương ứng của chúng 530A và 530B, được tạo cấu hình để thực hiện một hoặc nhiều kỹ thuật được mô tả chi tiết trên đây. Các phương án khác có thể bao gồm các trạm cơ sở và/hoặc các nút mạng khác mà bao gồm một hoặc nhiều mạch xử lý này. Trong một số trường hợp, các mạch xử lý này được tạo cấu hình với mã chương trình phù hợp, được lưu trữ trong một hoặc nhiều thiết bị bộ nhớ phù hợp, để ứng dụng một hoặc nhiều kỹ thuật được mô tả trong bản mô tả này. Tất nhiên, sẽ đánh giá được rằng, không phải tất cả các bước của các kỹ thuật này cần thiết được thực hiện trong bộ vi xử lý đơn hoặc thậm chí trong mô đun đơn.

Người có hiểu biết trung bình trong lĩnh vực sẽ đánh giá được rằng, các biến đổi khác nhau có thể được tạo cho các phương án được mô tả trên đây mà không vượt quá phạm vi của sáng chế. Ví dụ, mặc dù các phương án của sáng chế đã được mô tả với các ví dụ mà bao gồm hệ thống truyền thông tuân thủ các tiêu chuẩn LTE được đặc trưng cho 3GPP, nên ghi nhận rằng, các giải pháp được thể hiện có thể cũng được áp dụng tốt cho các mạng khác mà hỗ trợ kết nối kép. Do đó, các phương án đặc hiệu được mô tả trên đây nên được xem là ví dụ tốt hơn là giới hạn phạm vi của sáng chế. Tất nhiên, bởi vì không thể mô tả từng tổ hợp của các thành phần hoặc các kỹ thuật có thể hiểu được, người có hiểu biết trung bình trong lĩnh vực sẽ đánh giá được rằng, sáng chế có thể được ứng dụng theo các cách khác với các cách được đưa ra cụ thể trong bản mô tả này, mà không tách rời các đặc tính cơ bản của sáng chế. Do đó, các phương án theo sáng chế được xem là ở trong tất cả khía cạnh là để minh họa và không giới hạn sáng chế.

Trong phần mô tả của các phương án khác nhau của sáng chế, được hiểu là, thuật ngữ học được sử dụng trong bản mô tả này là đối với mục đích mô tả các phương án cụ thể và không có ý định để giới hạn sáng chế. Trừ phi có quy định khác, tất cả thuật ngữ (bao gồm các thuật ngữ khoa học và kỹ thuật) được sử dụng trong bản mô tả này có cùng nghĩa như thường được hiểu bởi người có hiểu biết trung bình trong lĩnh

vực mà sáng chế thuộc về. Sẽ còn được hiểu là, các thuật ngữ, như các thuật ngữ được xác định trong các từ điển thường được sử dụng, nên được dịch ra là có nghĩa mà phù hợp với nghĩa của chúng trong bối cảnh của bản mô tả này và tài liệu liên quan và sẽ không được dịch ra trong nghĩa được lý tưởng hóa hoặc hình thức thái quá được xác định riêng như vậy trong bản mô tả này.

Khi yếu tố được dùng để chỉ "được kết nối", "được ghép đôi", "đáp ứng", hoặc các dạng biến đổi của nó với yếu tố khác, nó có thể trực tiếp được kết nối, được ghép đôi, hoặc đáp ứng với yếu tố khác hoặc các yếu tố can thiệp có thể có mặt. Ngược lại, khi yếu tố được dùng để chỉ "trực tiếp được kết nối", "trực tiếp được ghép đôi", "trực tiếp đáp ứng", hoặc các dạng biến đổi của nó với yếu tố khác, ở đó không có các yếu tố can thiệp có mặt. Các số giống nhau là để chỉ các yếu tố giống nhau trong toàn bộ bản mô tả. Hơn nữa, "được ghép đôi", "được kết nối", "đáp ứng", hoặc các dạng biến đổi của nó như được sử dụng trong bản mô tả này có thể bao gồm được ghép đôi, được kết nối, hoặc đáp ứng không dây. Như được sử dụng trong bản mô tả này, các giới từ số ít không xác định và xác định số có hàm ý bao gồm cả các dạng số nhiều, trừ khi bối cảnh được quy định khác. Các chức năng hoặc các kiến trúc đã được biết rõ thì có thể không cần được mô tả chi tiết nữa để cho ngắn gọn và/hoặc rõ ràng. Thuật ngữ "và/hoặc" bao gồm tổ hợp bất kỳ và tất cả tổ hợp của một hoặc nhiều mục được liệt kê kết hợp.

Sẽ được hiểu rằng, mặc dù thuật ngữ thứ nhất, thứ hai, thứ ba, v.v. có thể được sử dụng trong bản mô tả này để mô tả các yếu tố/các vận hành khác nhau, các yếu tố/các vận hành này không nên chỉ giới hạn ở thuật ngữ này. Thuật ngữ này chỉ được sử dụng để phân biệt một yếu tố/hoạt động với yếu tố/hoạt động khác. Do đó, yếu tố/hoạt động thứ nhất trong một số phương án có thể cho tên gọi là yếu tố/hoạt động thứ hai trong các phương án khác mà không lệch khỏi nội dung của sáng chế. Các số tham khảo giống nhau hoặc các chỉ định tham khảo giống nhau sẽ biểu hiện cùng các yếu tố hoặc các yếu tố tương tự trong toàn bộ bản mô tả.

Như được sử dụng trong bản mô tả này, thuật ngữ "bao gồm", "việc bao gồm", "sự bao gồm", "gồm có", "việc gồm có ", "sự gồm có ", "có", "việc có", hoặc các dạng biến đổi của chúng được kết thúc mở, và bao gồm một hoặc nhiều dấu hiệu, số

nguyên, các yếu tố, các bước, các thành phần hoặc các chức năng được nêu nhưng không ngăn sự có mặt hoặc bổ sung của một hoặc nhiều dấu hiệu, số nguyên, các yếu tố, các bước, các thành phần, các chức năng hoặc các nhóm khác của nó. Hơn nữa, như được sử dụng trong bản mô tả này, dạng viết tắt chung "e.g." được dịch là “ví dụ”, mà được lấy ra từ cụm từ Latin "exempli gratia," có thể được sử dụng để giới thiệu hoặc đặc trưng hóa ví dụ chung hoặc các ví dụ về vấn đề được đề cập trước đây, và không có ý định để giới hạn vấn đề này. Dạng viết tắt chung "i.e." được dịch là “tức là”, mà được lấy ra từ từ cụm từ Latin "id est," có thể được sử dụng để chỉ định vấn đề cụ thể từ việc kể ra chung hơn.

Các phương án làm ví dụ được mô tả trong bản mô tả này việc tham khảo đến các sơ đồ khối và/hoặc minh họa sơ đồ tiến trình của các phương pháp, các thiết bị ứng dụng máy tính (các hệ thống và/hoặc các thiết bị) và/hoặc các sản phẩm chương trình máy tính. Được hiểu là khối minh họa trên sơ đồ khối và/hoặc sơ đồ tiến trình, và tổ hợp của các khối minh họa trên các sơ đồ khối và/hoặc sơ đồ tiến trình, có thể được thực hiện bởi các lệnh của chương trình máy tính mà được thực hiện bởi một hoặc nhiều mạch máy tính. Các lệnh của chương trình máy tính này có thể được cung cấp đến mạch của bộ xử lý của mạch máy tính với mục đích chung, mạch máy tính với mục đích cụ thể, và/hoặc mạch xử lý dữ liệu có thể lập trình khác để sản xuất ra máy, sao cho các lệnh, mà thực thi nhờ bộ xử lý của máy tính và/hoặc thiết bị xử lý dữ liệu có thể lập trình khác, các transito biến đổi hoặc kiểm soát, các giá trị được lưu trữ trong các vị trí bộ nhớ, và các thành phần phần cứng khác trong phạm vi mạch này để thực hiện các chức năng/hoạt động được đặc trưng hóa trong một hoặc nhiều khối của sơ đồ khối/sơ đồ tiến trình, và nhờ đó tạo ra phương tiện (chức năng) và/hoặc kiến trúc để thực hiện các chức năng/hoạt động được đặc trưng hóa trong (các) khối của sơ đồ khối và/hoặc sơ đồ tiến trình.

Các lệnh của chương trình máy tính này còn có thể được lưu trữ trong môi trường đọc được bởi máy tính xác thực mà có thể điều khiển máy tính hoặc thiết bị xử lý dữ liệu có thể lập trình khác để thực hiện chức năng theo cách cụ thể, sao cho các lệnh được lưu trữ trong môi trường đọc được bởi máy tính sản xuất ra vật phẩm sản xuất bao gồm các lệnh mà thực hiện các chức năng/hoạt động được đặc trưng hóa trong một hoặc nhiều khối của sơ đồ khối/sơ đồ tiến trình. Do đó, các phương án của

sáng chế có thể được biểu hiện trong phần cứng và/hoặc trong phần mềm (bao gồm vi chương trình, phần mềm thường trú, vi mã, v.v.) chạy trên bộ xử lý như bộ xử lý tín hiệu số, mà có thể được gọi chung là "mạch," "mô đun" hoặc các dạng biến đổi của nó.

Còn nên ghi nhận rằng, trong một số ứng dụng khác nhau, các chức năng/hoạt động được nêu trong các khối có thể làm xuất hiện ngoài thứ tự được nêu trong sơ đồ tiến trình. Ví dụ, hai khối được thể hiện kế tiếp có thể thực tế được thực thi cơ bản là đồng thời hoặc các khối đôi khi có thể được thực thi theo trình tự nghịch đảo, phụ thuộc vào chức năng/hoạt động liên quan. Hơn nữa, chức năng ở khối đã cho của sơ đồ tiến trình và/hoặc sơ đồ khối có thể được phân tách thành nhiều khối và/hoặc chức năng của hai hoặc nhiều hơn hai khối trên sơ đồ tiến trình và/hoặc sơ đồ khối có thể ít nhất được tích hợp một phần. Cuối cùng, các khối khác có thể được bổ sung/được chèn vào giữa các khối được minh họa, và/hoặc các khối/hoạt động có thể được bỏ qua mà không lệch khỏi phạm vi của sáng chế. Hơn nữa, mặc dù một số sơ đồ bao gồm các mũi tên trên các đường truyền thông để chỉ ra hướng truyền thông chính, nhưng cần hiểu là truyền thông có thể diễn ra hướng ngược lại với các mũi tên được mô tả.

Nhiều thay đổi và biến đổi có thể được tạo đối với các phương án mà về cơ bản không lệch khỏi các nguyên lý của sáng chế. Tất cả các thay đổi và các biến đổi này được dự định nằm trong trong phạm vi bảo hộ của sáng chế. Do đó, đối tượng được bộc lộ trên đây được xem là để minh họa, và không giới hạn, và các ví dụ kèm theo của các phương án được nhằm bao hàm tất cả các biến đổi này, các cải thiện, và các phương án khác, mà nằm trong trong ý đồ và phạm vi bảo hộ của sáng chế. Do đó, đến phạm vi tối đa được cho phép bởi luật, phạm vi của sáng chế được xác định bởi cách hiểu rộng nhất được phép của sáng chế, và sẽ không bị hạn chế hoặc giới hạn bởi phần mô tả chi tiết trên đây.

YÊU CẦU BẢO HỘ

1. Phương pháp trong thiết bị đầu cuối không dây (505B), để tạo ra khóa an toàn cho các sự truyền thông an toàn giữa thiết bị đầu cuối không dây (505B) và trạm cơ sở hỗ trợ, trong đó thiết bị đầu cuối không dây (505B) được hoặc sắp được kết nối kép vào trạm cơ sở neo và trạm cơ sở hỗ trợ, trong đó khóa an toàn chính được biết đối với trạm cơ sở neo và thiết bị đầu cuối không dây (505B), phương pháp này bao gồm các bước:

tạo ra khóa an toàn hỗ trợ, dựa ít nhất một phần trên khóa an toàn chính;

sử dụng khóa an toàn hỗ trợ trong việc tạo ra một hoặc nhiều khóa an toàn hỗ trợ bổ sung để mã hóa lưu lượng dữ liệu, trong đó lưu lượng dữ liệu được gửi từ thiết bị đầu cuối không dây (505B) đến trạm cơ sở hỗ trợ trong khi thiết bị đầu cuối không dây (505B) được kết nối kép vào trạm cơ sở neo và trạm cơ sở hỗ trợ.

2. Phương pháp theo điểm 1, trong đó khóa an toàn hỗ trợ được tạo ra bao gồm khóa an toàn hỗ trợ cơ sở để sử dụng trong việc tạo ra một hoặc nhiều khóa an toàn hỗ trợ bổ sung để mã hóa lưu lượng dữ liệu được gửi đến thiết bị đầu cuối không dây (505B) bởi trạm cơ sở hỗ trợ.

3. Phương pháp theo điểm 1 hoặc 2, trong đó bước tạo ra khóa an toàn hỗ trợ bao gồm lấy ra khóa an toàn hỗ trợ từ khóa chính sử dụng hàm một chiều.

4. Phương pháp theo điểm 3, trong đó hàm một chiều là hàm mã hóa HMAC-SHA-256.

5. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 4, trong đó bước tạo ra khóa an toàn hỗ trợ còn dựa trên thông số làm mới.

6. Thiết bị đầu cuối không dây (505B), để tạo ra khóa an toàn cho các sự truyền thông an toàn giữa thiết bị đầu cuối không dây (505B) và trạm cơ sở hỗ trợ, thiết bị đầu cuối không dây (505B) bao gồm mạch giao diện (510B), mạch xử lý (520B), và bộ nhớ (530B), trong đó thiết bị đầu cuối không dây (505B) được tạo cấu hình để được kết nối kép vào trạm cơ sở neo và trạm cơ sở hỗ trợ, và trong đó mạch xử lý (520B) được tạo cấu hình để:

tạo ra khóa an toàn hỗ trợ, dựa ít nhất một phần trên khóa an toàn chính mà được biết đối với trạm cơ sở neo và thiết bị đầu cuối không dây (505B);

sử dụng khóa an toàn hỗ trợ trong việc tạo ra một hoặc nhiều khóa an toàn hỗ trợ bổ sung để mã hóa lưu lượng dữ liệu, trong đó lưu lượng dữ liệu được gửi từ thiết bị đầu cuối không dây (505B) đến trạm cơ sở hỗ trợ trong khi thiết bị đầu cuối không dây (505B) được kết nối kép vào trạm cơ sở neo và trạm cơ sở hỗ trợ.

7. Thiết bị đầu cuối không dây (505B) theo điểm 6, trong đó mạch xử lý (520B) còn được tạo cấu hình để tạo ra khóa an toàn hỗ trợ nhờ lấy ra khóa an toàn hỗ trợ từ khóa chính sử dụng hàm một chiều.

8. Thiết bị đầu cuối không dây (505B) theo điểm 7, trong đó hàm một chiều là hàm mã hóa HMAC-SHA-256.

9. Thiết bị đầu cuối không dây (505B) theo điểm bất kỳ trong số các điểm từ 6 đến 8, trong đó mạch xử lý (520B) còn được tạo cấu hình để tạo ra khóa an toàn hỗ trợ dựa trên thông số làm mới.

10. Thiết bị đầu cuối không dây (505B) theo điểm bất kỳ trong số các điểm từ 6 đến 9, thiết bị này còn được tạo cấu hình để lưu trữ khóa chính và/hoặc khóa an toàn hỗ trợ trong bộ nhớ (530B).

11. Thiết bị đầu cuối không dây (505B) theo điểm 9 hoặc 10, thiết bị này còn được tạo cấu hình để lưu trữ thông số làm mới trong bộ nhớ (530B).

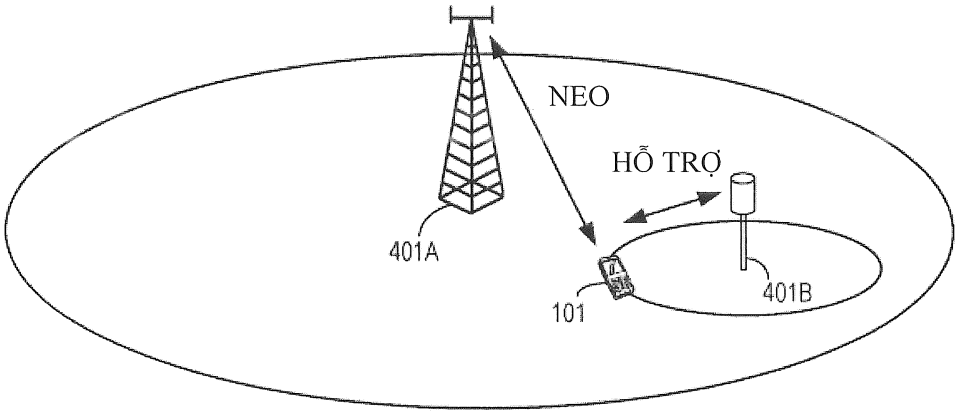


FIG. 1

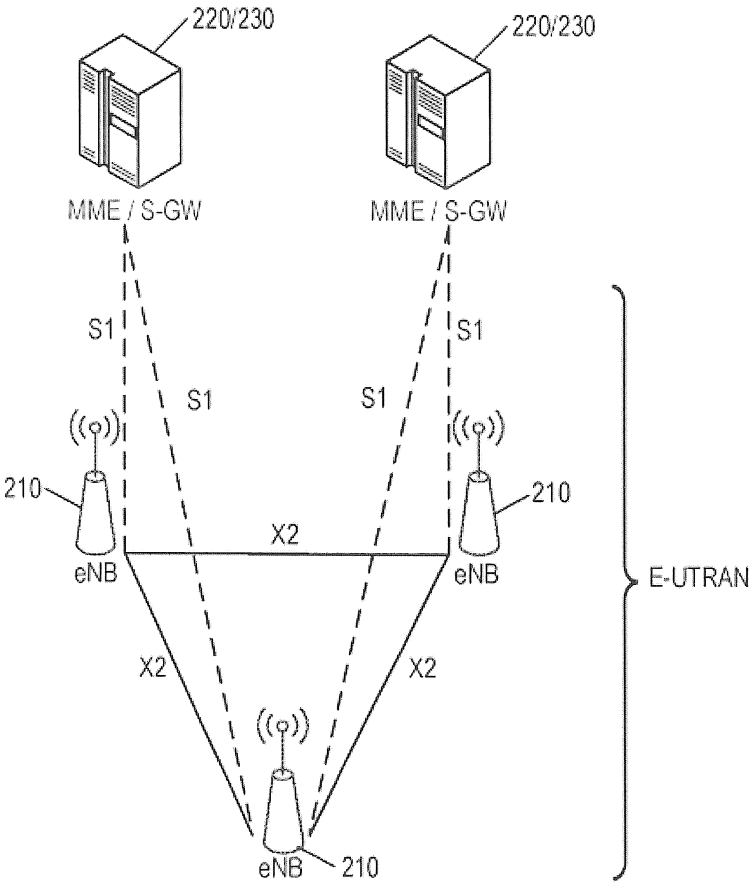

220/230
220/230
MME / S-GW
MME / S-GW
S1
S1
S1
S1
210
210
X2
eNB
eNB
X2
X2
eNB
210
E-UTRAN

FIG. 2

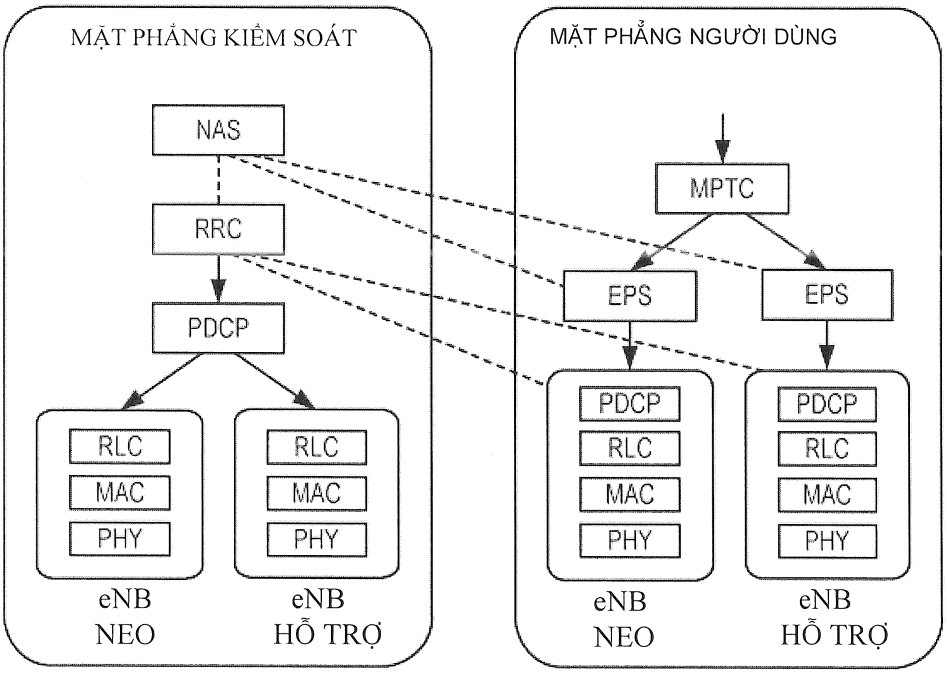

MẶT PHẲNG KIỂM SOÁT
MẶT PHẲNG NGƯỜI DÙNG
NAS
RRC
PDCP
MPTC
EPS
EPS
RLC
MAC
PHY
RLC
MAC
PHY
PDCP
RLC
MAC
PHY
PDCP
RLC
MAC
PHY
eNB
NEO
eNB
HỖ TRỢ
eNB
NEO
eNB
HỖ TRỢ

FIG. 3

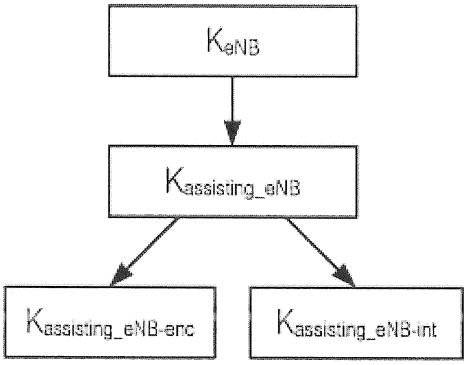

KeNB
Kassisting_eNB
Kassisting_eNB-enc
Kassisting_eNB-int

FIG. 4

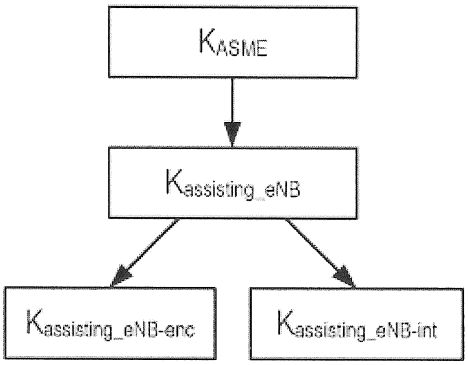

KASME
Kassisting_eNB
Kassisting_eNB-enc
Kassisting_eNB-int

FIG. 5

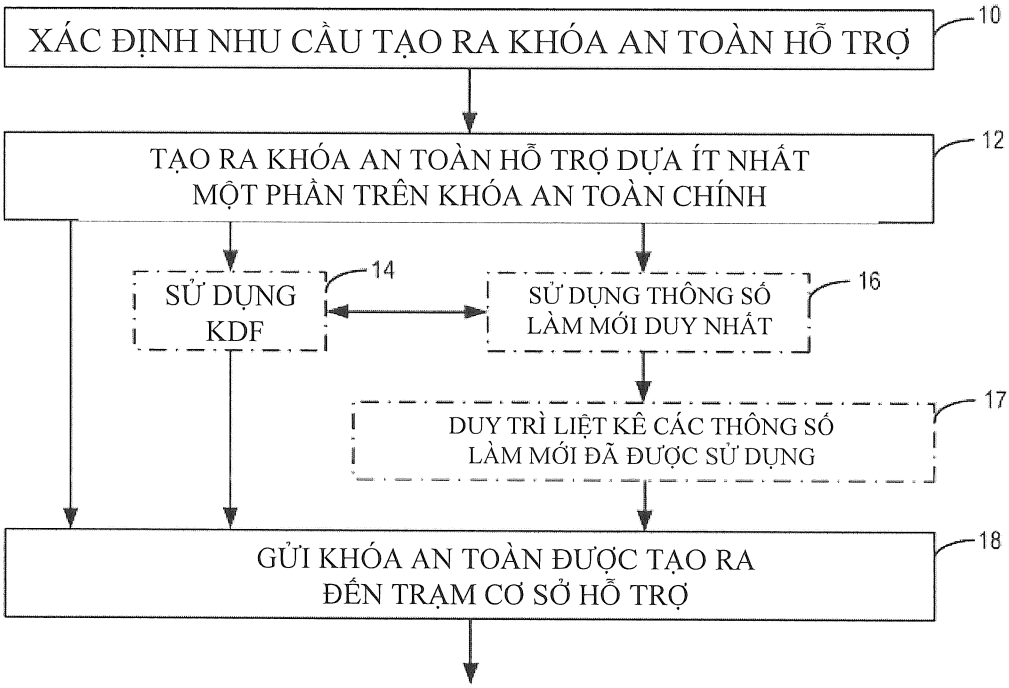

XÁC ĐỊNH NHU CẦU TẠO RA KHÓA AN TOÀN HỖ TRỢ
10
TẠO RA KHÓA AN TOÀN HỖ TRỢ DỰA ÍT NHẤT MỘT PHẦN TRÊN KHÓA AN TOÀN CHÍNH
12
SỬ DỤNG KDF
14
SỬ DỤNG THÔNG SỐ LÀM MỚI DUY NHẤT
16
DUY TRÌ LIỆT KÊ CÁC THÔNG SỐ LÀM MỚI ĐÃ ĐƯỢC SỬ DỤNG
17
GỬI KHÓA AN TOÀN ĐƯỢC TẠO RA ĐẾN TRẠM CƠ SỞ HỖ TRỢ
18

FIG. 6

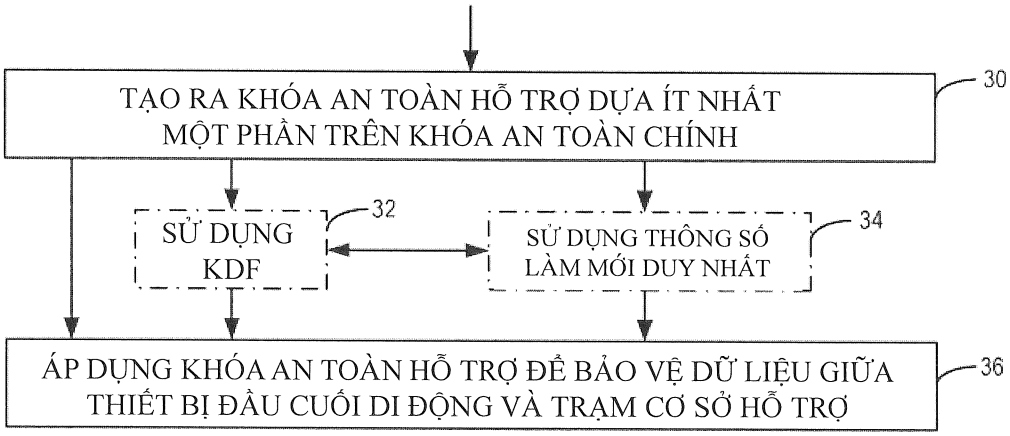

TẠO RA KHÓA AN TOÀN HỖ TRỢ DỰA ÍT NHẤT MỘT PHẦN TRÊN KHÓA AN TOÀN CHÍNH
30
SỬ DỤNG KDF
32
SỬ DỤNG THÔNG SỐ LÀM MỚI DUY NHẤT
34
ÁP DỤNG KHÓA AN TOÀN HỖ TRỢ ĐỂ BẢO VỆ DỮ LIỆU GIỮA THIẾT BỊ ĐẦU CUỐI DI ĐỘNG VÀ TRẠM CƠ SỞ HỖ TRỢ
36

FIG. 7

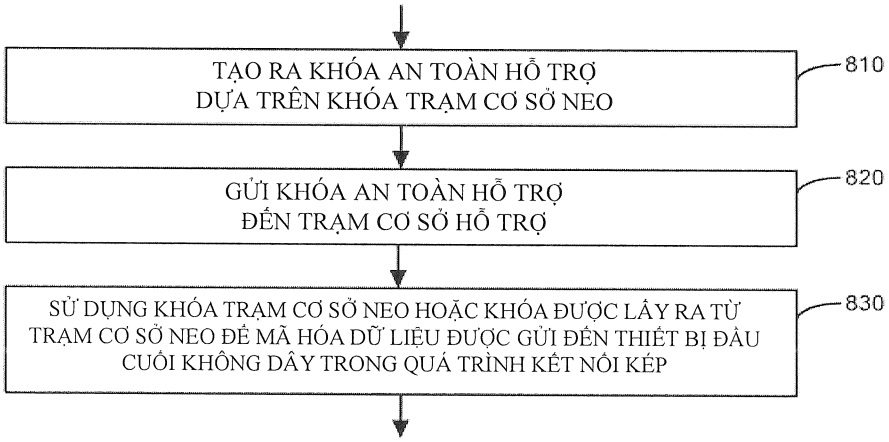

TẠO RA KHÓA AN TOÀN HỖ TRỢ
DỰA TRÊN KHÓA TRẠM CƠ SỞ NEO
810
GỬI KHÓA AN TOÀN HỖ TRỢ
ĐẾN TRẠM CƠ SỞ HỖ TRỢ
820
SỬ DỤNG KHÓA TRẠM CƠ SỞ NEO HOẶC KHÓA ĐƯỢC LẤY RA TỪ
TRẠM CƠ SỞ NEO ĐỂ MÃ HÓA DỮ LIỆU ĐƯỢC GỬI ĐẾN THIẾT BỊ ĐẦU
CUỐI KHÔNG DÂY TRONG QUÁ TRÌNH KẾT NỐI KÉP
830

FIG. 8

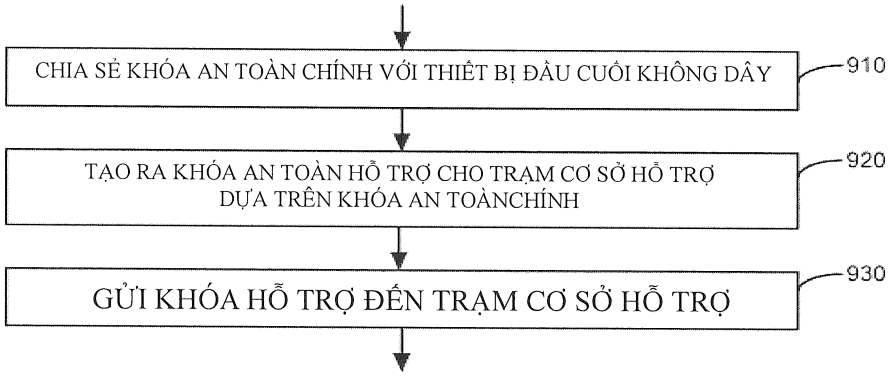

CHIA SẺ KHÓA AN TOÀN CHÍNH VỚI THIẾT BỊ ĐẦU CUỐI KHÔNG DÂY
910
TẠO RA KHÓA AN TOÀN HỖ TRỢ CHO TRẠM CƠ SỞ HỖ TRỢ
DỰA TRÊN KHÓA AN TOÀNCHÍNH
920
GỬI KHÓA HỖ TRỢ ĐẾN TRẠM CƠ SỞ HỖ TRỢ
930

FIG. 9

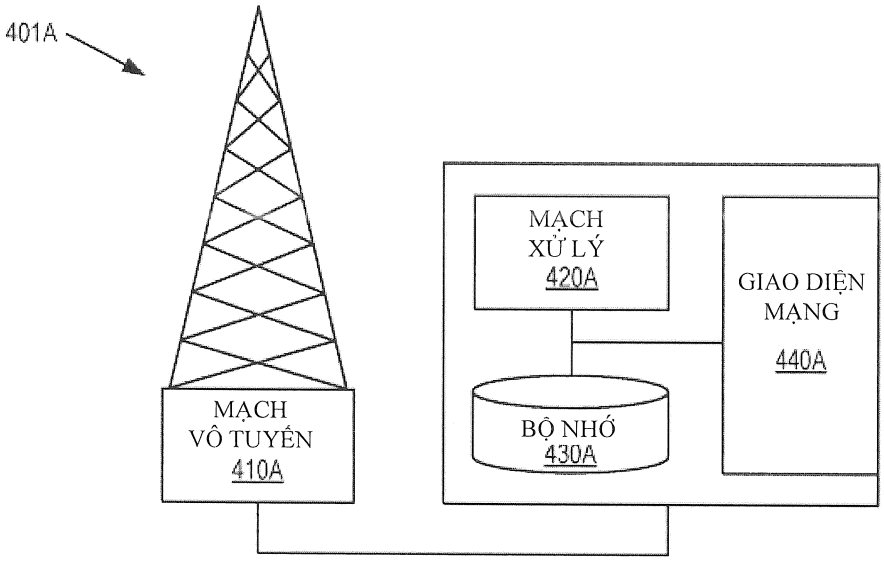

401A
MẠCH
VÔ TUYẾN
410A
MẠCH
XỬ LÝ
420A
BỘ NHỚ
430A
GIAO DIỆN
MẠNG
440A

FIG. 10

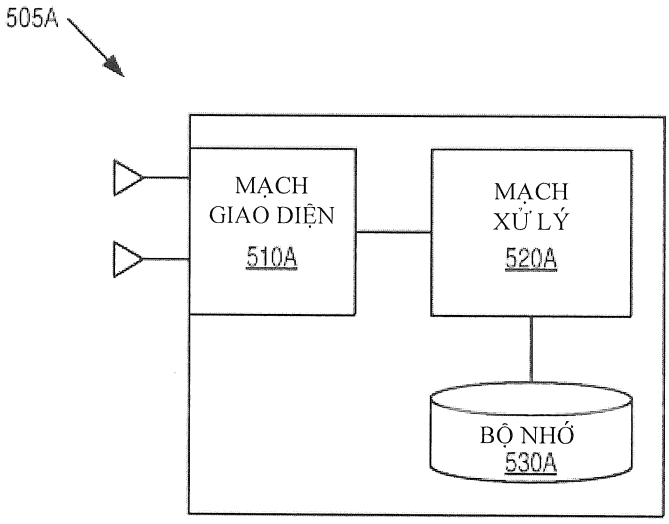

505A
MẠCH
GIAO DIỆN
510A
MẠCH
XỬ LÝ
520A
BỘ NHỚ
530A

FIG. 11

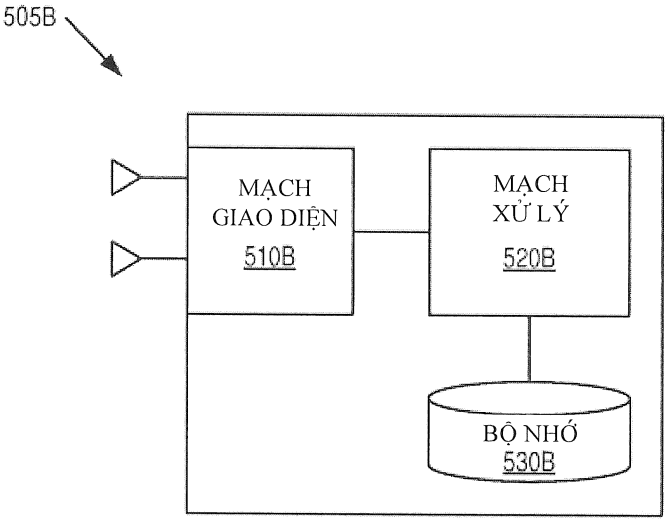

505B
MẠCH
GIAO DIỆN
510B
MẠCH
XỬ LÝ
520B
BỘ NHỚ
530B

FIG. 12