

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号
特許第4965737号
(P4965737)

(45) 発行日 平成24年7月4日 (2012. 7. 4)

(24) 登録日 平成24年4月6日 (2012. 4. 6)

(51) Int. Cl.

F I

HO 4 W 12/08 (2009. 01) HO 4 Q 7/00 1 8 4

HO 4 W 36/08 (2009. 01) HO 4 Q 7/00 3 0 6

請求項の数 8 (全 18 頁)

(21) 出願番号	特願2011-501740 (P2011-501740)	(73) 特許権者	598036300
(86) (22) 出願日	平成20年8月25日 (2008. 8. 25)		テレフオンアクチーボラゲット エル エ
(65) 公表番号	特表2011-515984 (P2011-515984A)		ム エリクソン (パブル)
(43) 公表日	平成23年5月19日 (2011. 5. 19)		スウェーデン国 スtockホルム エスー
(86) 国際出願番号	PCT/SE2008/050957		1 6 4 8 3
(87) 国際公開番号	W02009/120122	(74) 代理人	100095957
(87) 国際公開日	平成21年10月1日 (2009. 10. 1)		弁理士 亀谷 美明
審査請求日	平成23年8月1日 (2011. 8. 1)	(74) 代理人	100096389
(31) 優先権主張番号	61/040, 269		弁理士 金本 哲男
(32) 優先日	平成20年3月28日 (2008. 3. 28)	(74) 代理人	100101557
(33) 優先権主張国	米国 (US)		弁理士 萩原 康司
早期審査対象出願		(74) 代理人	100128587
			弁理士 松本 一騎

最終頁に続く

(54) 【発明の名称】 ハンドオーバーの間における不正操作されまたは欠陥のある基地局の識別

(57) 【特許請求の範囲】

【請求項 1】

ユーザ機器（UE；303）のハンドオーバーに関連して、ソース基地局（400）として動作する不正操作されまたは欠陥のある基地局を検出できるようにするための、ターゲット基地局（401）として動作する通信ネットワークの基地局内での方法であって：

優先度順に前記UEと通信する場合に使用することを許可されるアルゴリズムをリスト化する、優先順位付きアルゴリズムリスト（PAL）を、ネットワークノードから受信するステップ（600）と；

前記2つの基地局間でハンドオーバーされる前記UEについて、UEセキュリティケイパビリティ（SCAP）を前記ソース基地局から受信するステップ（601）と；

前記UE SCAPによると前記UEによってサポートされ、かつ前記ターゲット基地局によりサポートされている前記アルゴリズムの中から、前記PALによると最も高い優先度を有する少なくとも1つのアルゴリズムを選択するステップ（602）と；

を含み、

前記ハンドオーバーに先立って前記UEの前記UE SCAPを予め記憶している移動性管理エンティティ（MME）へ、前記ソース基地局から受信された前記UE SCAPをパススイッチメッセージにビジーバックすることによりレポートし、それにより、前記MMEが予め記憶している前記UE SCAPの少なくとも一部とレポートされた前記UE

SCAPとを比較して、不正操作されまたは欠陥のある基地局を検出できるようにするステップ（603）

を特徴とする方法。

【請求項 2】

前記 P A L は、複数の U E について使用されるグローバル P A L である、請求項 1 に記載の方法。

【請求項 3】

前記グローバル P A L は、前記ネットワークのオペレーション&メンテナンスシステムから前記基地局へ配信される、請求項 2 に記載の方法。

【請求項 4】

前記グローバル P A L は、前記ネットワークノードを介して、前記基地局へ配信される、請求項 2 に記載の方法。

【請求項 5】

ターゲット基地局へのユーザ機器 (U E) のハンドオーバに関連して、ソース基地局として動作する不正操作されまたは欠陥のある基地局を検出するための、通信ネットワークの移動性管理エンティティ (M M E) 内の方法であって：

優先度順に前記 U E のために許可されるアルゴリズムをリスト化する、優先順位付きアルゴリズムリスト (P A L) を予め記憶するステップ (8 0 0) と；

U E セキュリティケイパビリティ (S C A P) を、前記ハンドオーバに先立って前記 U E から受信しおよび記憶するステップ (8 0 1) と；

を含み、

前記ハンドオーバの間に前記ソース基地局から前記ターゲット基地局へ送信された、前記ターゲット基地局によりパススイッチメッセージにピギーバックされる前記 U E の U E

S C A P を、前記ターゲット基地局から受信するステップ (8 0 2) と；

不正操作されまたは欠陥のある基地局を検出するために、記憶された前記 U E S C A P の少なくとも一部を、前記ターゲット基地局から受信された前記 U E S C A P と比較することにより、前記ターゲット基地局から受信された前記 U S S C A P を検証するステップ (8 0 3) と；

を特徴とする方法。

【請求項 6】

前記 P A L は、前記ネットワークのオペレーション&メンテナンスシステム (O & M) から受信される、請求項 5 に記載の方法。

【請求項 7】

ユーザ機器 (U E) のハンドオーバに関連して、ソース基地局 (4 0 0) として動作する不正操作されまたは欠陥のある基地局を検出できるようにするための、ターゲット基地局として動作できる通信ネットワークの基地局 (4 0 1) であって：

優先度順に前記 U E と通信する場合に使用することを許可されるアルゴリズムをリスト化する、優先順位付きアルゴリズムリスト (P A L) を、ネットワークノードから受信し、および、前記 2 つの基地局間でハンドオーバされる前記 U E について、U E セキュリティケイパビリティ (S C A P) を前記ソース基地局から受信するための受信手段 (5 0 1) と；

前記 U E S C A P によると前記 U E によってサポートされ、かつ前記基地局によりサポートされている前記アルゴリズムの中から、前記 P A L によると最も高い優先度を有する少なくとも 1 つのアルゴリズムを、前記 P A L から選択するための選択手段 (5 0 2) と；

を備え、

前記ハンドオーバに先立って前記 U E の前記 U E S C A P を予め記憶している移動性管理エンティティ (M M E) (2 0 0) へ、送信手段 (5 0 4) を介して、前記ソース基地局から受信された前記 U E S C A P をパススイッチメッセージにピギーバックすることによりレポートし、それにより、前記 M M E が予め記憶している前記 U E S C A P の少なくとも一部とレポートされた前記 U E S C A P とを比較して、不正操作されまたは欠陥のある基地局を検出できるようにするためのレポート手段 (5 0 3)

10

20

30

40

50

を特徴とする基地局。

【請求項 8】

ターゲット基地局（401）へのユーザ機器（UE；300）のハンドオーバに関連して、ソース基地局（301）として動作する不正操作されまたは欠陥のある基地局を検出するための、通信ネットワークの移動性管理エンティティ（MME）（200）であって：

優先度順に前記UEのために許可されるアルゴリズムをリスト化する優先順位付きアルゴリズムリスト（PAL）を予め記憶し、並びに、前記ハンドオーバに先立って前記UEから受信されるUEセキュリティケイパビリティ（SCAP）を記憶するための記憶手段（702）；

を備え、

前記ハンドオーバの間に前記ソース基地局から前記ターゲット基地局へ送信された、前記ターゲット基地局によりパススイッチメッセージにピギーバックされる前記UEのUE SCAPを、前記ターゲット基地局から受信するための受信手段（701）と；

不正操作されまたは欠陥のある基地局を検出するために、記憶された前記UE SCAPの少なくとも一部を、前記ターゲット基地局から受信された前記UE SCAPと比較することにより、前記ターゲット基地局から受信された前記UE SCAPを検証するための検証手段（203）と；

を特徴とするMME。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、セルラー通信ネットワークにおける、不正操作されまたは欠陥のある基地局の検出に関する。

【背景技術】

【0002】

3GPPは、現在、3Gネットワークの延長であるLTE（Long Term Evolution）を規格化している。LTEでは、ユーザプレーンおよび無線リソースコントロールのデータの、暗号化並びに完全性保護は、この文脈ではevolved Node B（eNB）と通常呼ばれる基地局により実行される。端末、すなわちユーザ機器（UE）の通信リンクが、あるeNBから別のeNBへハンドオーバされる場合、ソースeNBは、UEによってサポートされるアルゴリズム、およびネットワークによりユーザのために許可されるアルゴリズムについて、ターゲットeNBに通知する。ネットワークにより許可され、UEおよびターゲットeNBによってサポートされるアルゴリズムの中から、ターゲットeNBは、次に、所定の選択基準に従って、最良と考えられるアルゴリズムを選択する。

【0003】

かかる状況では、危殆化された（compromised）ソースeNBは、ユーザがサポートし、ネットワークが許可するアルゴリズム、および／またはネットワークがサポートするアルゴリズムの優先順位を示すリストを改変し得る。ターゲットeNBが、これらのリストの信頼性を検証する可能性はないため、ターゲットeNBは、悪意のあるソースeNBがターゲットeNBをだまして、脆弱で、場合によっては壊れたアルゴリズムを選択させているかを、検出できない。かかるアタックセットアップは、典型的に、ビディングダウンアタック（bidding-down attack）と呼ばれる。

【0004】

3GPP内のセキュリティワーキンググループは、この種のビディングダウンアタックを検出のためのソリューションを提供することに合意した。

【0005】

現在のハンドオーバのシグナリングが、どのように構成され得るかの理解のために、先行技術に従ったかかる手続きが、ここで、図1のシグナリング図を参照して説明される。説明されるハンドオーバのシグナリングは、2008年5月の技術仕様TS 36.30

10

20

30

40

50

0、"3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2"に準拠する。

【0006】

最初のステップ1:1では、ソースeNB101は、エリア制限情報に従って、UEメ
ジヤメント手続きを構成する。ステップ1:2からステップ1:5で示されるとおり、U
E100は、UE100が現在属するeNB101、すなわち、ハンドオーバーの状況の場合
にはソースeNBと呼ばれるサービングeNBへの、メジヤメントレポートを、準備し
、送信する。そこで、UE100は、周辺のeNBの強さを測定し、結果をレポートする
。次のステップ1:6で示されるとおり、サービングeNB101は、選択されたターゲ
ットeNB102へUE100をハンドオーバーすることを決定する。次のステップ1:7
に示されるとおり、ソースeNB101は、次に、ターゲットeNB102へ必要な情報
を送信して、ターゲットeNBにハンドオーバーをリクエストする。別のステップ1:8で
示されるとおり、この段階で、ターゲットeNB102は、流入制御手続きを実行し得る
。その後、ステップ1:9で示されるとおり、ターゲットeNB102は、リクエストを
受け取り、それに応じて、ソースeNB101は、ターゲットeNBに属するUEへハンド
オーバーコマンド送信する。そして、別のステップ1:11で示されるとおり、ソースe
NB101は、UE100へ、ハンドオーバーコンファームメッセージを送信する。次のステ
ップ1:12-1:18では、例えば同期を含むハンドオーバーの準備が、UE100と
ターゲットeNB102との間で実行される。ターゲットeNB102が、ステップ1:
19で送信されるハンドオーバーコンファームメッセージを受信すると、次のステップ1:
20で示されるとおり、ターゲットeNB102は、UE100の新たな位置について、
コアネットワーク内の移動性管理エンティティ(MME)104に通知する。最後のステ
ップ1:29に示されるとおり、UE100に送信され、およびUE100から受信される
全てのデータが、ターゲットeNB102を介して実行されることを、次のステップ1:
21-1:28で、MMEが、保証する。

【0007】

しかしながら、上記手続きによると、MME103がステップ1:20のパススイッチ
リクエスト(path switch request)の中で受信した情報が、正確で、信頼できること
を、MME103が、検証する方法はない。上記の問題を扱うための3GPPセキュリ
ティワーキンググループ(SA WG3)内の議論では、現在2つのソリューションが存在
する。1つは、Nokia、Nokia Siemens Networksによる、2008年2月25日-29
日のS3-080169(P-CR)"AS algorithms selection mismatch indicati
on"内で提供される。要するに、このドキュメントにて説明されているソリューションは
、ハンドオーバーの手続きを実行する前に、UEが、そのセキュリティケイパビリティを、
移動性管理エンティティ(MME)へレポートしており、そして、MMEが、許可される
アルゴリズムのセットをUEに送信することを、提案する。MMEは、さらに、UEによ
ってサポートされるアルゴリズムのみを含む、優先順位付けされたアルゴリズムのリスト
を、サービングeNBへ送信する。サービングeNBは、使用するために、これらのアル
ゴリズムの中から1つを選択する。ハンドオーバーの手続きの間に、UEが、ターゲットセ
ル内で使用するために選択されたアルゴリズムが、許可されるアルゴリズムのセットに含
まれていないことに気付くと、UEは、これをMMEにレポートする。レポートには、ミ
スマッチが検出された最初のセルのセルアイデンティティ(セルID)が、含まれる。し
かしながら、この方法には、ターゲットeNBまたはUEは、ソースeNBが、ネットワ
ークの許可されたアルゴリズムのリスト内におけるアルゴリズムの順番を改変したかを検
出できないという問題がある。さらに、UEが説明されたイベントをMMEへレポートす
ることを可能とする、新たなノンアクセスストラタム(NAS)の手続きが、必要とされる
ため、必要とされるレポートのメカニズムは、複雑である。このメカニズムを使うことは
、また、UEとターゲットeNBとの間のエアインターフェース上でのさらなる負荷をも

たらず。

【0008】

同じ問題への別のソリューションは、Ericssonによる、2008年2月25日－29日のS3-080054"AS algorithm policy handling"で提案されており、基本的に以下のステップからなる：

1. UEは、そのUEセキュリティケイパビリティ（UE SCAP）、すなわちUEによりサポートされるアルゴリズムを、MMEへ送信する。
2. MMEは、ここではMME__prio__listと呼ばれる、優先度順のアルゴリズムのリストを選択する。
3. MMEは、MME__prio__listおよびUE SCAPを、サービングeNBへ送信する。
4. MMEは、完全性が保護されたMME__prio__listおよびUE SCAPを、UEへ送信する。
5. ターゲットeNBは、O&M__allowed__setと呼ばれる、リスト化された許可されるアルゴリズムのセットを伴って、オペレーション&メンテナンス（O&M）を介して構成される。
6. ターゲットeNBは、UE SCAP、MME__prio__listおよびO&M__allowed__setの3つ全ての中から識別され得るアルゴリズムを選択する。
7. UEは、そのMME__prio__listおよびUE SCAPを、ターゲットeNBへレポートする。
8. UEから受信されたMME__prio__listおよびUE SCAPが、ソースeNBから受信されたものと同じでないとターゲットeNBが判定すると、ターゲットeNBは、ビディングダウンアタックが発生したと推定し、適切な対応をとり得る。

【0009】

しかしながら、このソリューションは、UEが、ハンドオーバーコンファームコマンドの中でターゲットeNBへ情報を提供しなければならないため、各eNB内で構成される別々のアルゴリズムのリストを必要とするだけではなく、また、確立された無線リンク上での帯域幅の使用を増加させる。

【0010】

また、Ericssonによる、2007年7月10日－13日のS3-070554"Bidding down attack at eNB to eNB active mode handover"が、この問題を扱う。様々なソリューションが提案され、例えば、UEがMMEに選択されたアルゴリズムを通知し、それによりMMEはミスマッチを検出するためにUEのケイパビリティとおよびeNBのケイパビリティとアルゴリズムを比較することができるという、ソリューションが提案されている。しかしながら、マッチは、ソースeNBから受信されたUEのケイパビリティに関する情報が修正されなかったことを必ずしも意味しない。さらに、S3-070554に示されるそのようなUEに基づくアプローチは、UEとMMEとの間の追加のメッセージを伴い、そのようなメッセージは、UEの複雑さを増大させる。

【発明の概要】

【0011】

本発明の目的は、上記問題を解決することであり、少なくとも上記の問題のいくつかを解決することである。さらに具体的に、本発明の目的は、不正操作されまたは欠陥のある基地局から発生するセキュリティ機能上へのビディングダウンアタックを検出するための改善された手続きを提供することである。

【0012】

一実施形態によると、ユーザ機器（UE；303）のハンドオーバーに関連して、ソース基地局として動作する不正操作されまたは欠陥のある基地局を検出できるようにするための、ターゲット基地局として動作する通信ネットワークの基地局内での方法が、提供される。上記方法は、

一優先度順に上記UEと通信する場合に使用することを許可されるアルゴリズムをリスト

化している、優先順位付きアルゴリズムリスト（PAL）を、上記ネットワークから受信するステップと；

－上記ソース基地局から上記ターゲット基地局へハンドオーバされる上記UEについて、UEセキュリティケイパビリティ（SCAP）関連情報を上記ソース基地局から受信するステップと；

－上記UE SCAP関連情報によると上記UEによってサポートされ、かつ上記ターゲット基地局によりサポートされている上記アルゴリズムの中から、上記PALによると最も高い優先度を有する少なくとも1つのアルゴリズムを選択するステップと；

－上記UEの上記UE SCAPのナレッジを有するコアネットワークノードへ、受信された上記UE SCAP関連情報をレポートし、それにより、上記コアネットワークノードが上記UE SCAP関連情報を使用して、不正操作されまたは欠陥のある基地局を検出できるようにするステップと；

を含む。

【0013】

本発明のさらなる形態は、ターゲット基地局へのユーザ機器（UE）のハンドオーバに関連して、ソース基地局として動作する不正操作されまたは欠陥のある基地局を検出するための、通信ネットワークのコアネットワークノード内の方法に関する。上記方法は、

－優先度順に上記UEのために許可されるアルゴリズムをリスト化する、優先順位付きアルゴリズムリスト（PAL）を、上記ネットワークから受信しおよび記憶するステップと；

－UEセキュリティケイパビリティ（SCAP）を、上記UEから受信しおよび記憶するステップと；

－上記ハンドオーバ手続きの間に上記ソース基地局から上記ターゲット基地局へ予めレポートされた、上記UEのUE SCAP関連情報を、上記ターゲット基地局から受信するステップと；

－不正操作されまたは欠陥のある基地局を検出するために、記憶された上記UE SCAPの少なくとも一部を、上記UE SCAP関連情報と比較することにより、上記ターゲット基地局から受信された上記US SCAP関連情報を検証するステップと；

を含む。

【0014】

本発明のさらに別の形態は、ユーザ機器（UE）のハンドオーバに関連して、ソース基地局として動作する不正操作されまたは欠陥のある基地局を検出できるようにするための、ターゲット基地局として動作できる通信ネットワークの基地局に関する。上記基地局は、

－優先度順に上記UEと通信する場合に使用することを許可されるアルゴリズムをリスト化する、優先順位付きアルゴリズムリスト（PAL）を、上記ネットワークから受信し、および、上記2つの基地局間でハンドオーバされる上記UEについて、UEセキュリティケイパビリティ（SCAP）関連情報を上記ソース基地局から受信するための受信手段と；

－上記UE SCAP関連情報によると上記UEによってサポートされ、かつ上記基地局によりサポートされている上記アルゴリズムの中から、上記PALによると最も高い優先度を有する少なくとも1つのアルゴリズムを、上記PALから選択するための選択手段（502）と；

－送信手段（504）を介して、上記UEの上記UE SCAPのナレッジを有するコアネットワークノード（200）へ、受信された上記UE SCAP関連情報をレポートし、それにより、上記コアネットワークノードが上記UE SCAP関連情報を使用して、不正操作されまたは欠陥のある基地局を検出できるようにするためのレポート手段（503）と；

を備える。

【0015】

本発明のさらに別の形態は、ターゲット基地局へのユーザ機器（UE）のハンドオーバーに関連して、ソース基地局として動作する不正操作されまたは欠陥のある基地局を検出するための、通信ネットワークのコアネットワークノードに関する。上記コアネットワークは、

－優先度順に上記UEのために許可されるアルゴリズムをリスト化する優先順位付きアルゴリズムリスト（PAL）を上記ネットワークから受信し、および上記PALを記憶し、UEセキュリティケイパビリティ（SCAP）を上記UEから受信し、および上記UE SCAPを記憶し、並びに、上記ハンドオーバーの間に上記ソース基地局から上記ターゲット基地局へ予めレポートされた上記UEのUE SCAP関連情報を上記ターゲット基地局から受信するための受信手段と；

－不正操作されまたは欠陥のある基地局を検出するために、記憶された上記UE SCAPの少なくとも一部を、上記UE SCAP関連情報と比較することにより、上記ターゲット基地局から受信された上記UE SCAP関連情報を検証するための検証手段（203）と；

を備える。

【0016】

コアネットワークノードは、典型的には移動性管理エンティティ（MME）である。

【0017】

全てのUEについて同じPALが使用される場合、グローバルPALは、オペレーション&メンテナンスシステムから直接的にネットワーク内の各基地局および例えばMMEのようなコアネットワークノードへ、ネットワークから伝達され得る。あるいは、グローバルPALはコアネットワークノードへ伝達され、そしてコアネットワークノードがグローバルPALをネットワーク内の全ての基地局へ配信してもよい。

【0018】

同じPALがネットワークのある部分へ送信されるが、ネットワークの別の部分は異なるPALを有することも、可能である。あるいは、PALは、UEによりサポートされていることが知られているあるアルゴリズムのみを含み得るように、各UEにとってユニークである。そのような場合、UEにユニークなPALは、ソース基地局を介してネットワークからターゲット基地局へ配信される。

【0019】

さらに、全ての基地局はPALによって正しい優先順位に気付くため、および、ターゲットセル内で使用するために選択されたアルゴリズムが許可されたアルゴリズムのセットの中にないことを検出することに加えて、本発明はさらにセット内のアルゴリズムの中のビディングダウンアタックを検出するため、本発明は高い精度を提供する。

【0020】

さらに、提案されるメカニズムは、基地局に関する独自の構成が必要ないため、実装しやすい。さらに、提案される検証メカニズムに関連付けられる全ての情報は既に存在するメッセージ上でpiggy-backed（piggy-backed）され得るため、新たなシグナリング手続きは必要とされない。例えば、ターゲット基地局がパススイッチメッセージをMMEのようなコアネットワークノードへ送信する場合、ターゲット基地局はソース基地局から受信されるUE SCAPをこのメッセージ上でpiggy-backする。この点において、ターゲット基地局から受信されるUE SCAPが、コアネットワークノード内に記憶されているUE SCAPとマッチするかを、コアネットワークノードは検証し得る。ミスマッチがある場合に、コアネットワークノードは1つ以上の適切な対応をとるように構成され得る。ソースeNBのIDもパススイッチメッセージ上でpiggy-backedされてもよく、それによりコアネットワークノードは、どのeNBが不正を行いまたは正常に機能していないかを判定することができる。UEは説明された手続きに参与する必要はなく、したがって要求される端末の複雑さを軽減している。端末とeNBとの間の独自のシグナリングはこの目的のために必要とされないため、提案されるメカニズムを実行する場合、無線リソースもより効率的に利用される。

10

20

30

40

50

【0021】

本発明の他の目的、有利な点、および新規の特徴は、添付の図面と併せて考えられて、以下の本発明の詳細な説明から明らかになるであろう。

【図面の簡単な説明】

【0022】

本発明は、例示的な実施形態により、および以下の添付の図面を参照して、より詳細に説明される：

【図1】先行技術に従って、ハンドオーバー手続きに関連付けられるシグナリングを説明する、シグナリング図である。

【図2a】グローバル優先順位付きアルゴリズムリスト(PAL)をネットワークの基地局へ配信するための代替オプションを説明する、単純化されたスキームである。

【図2b】グローバル優先順位付きアルゴリズムリスト(PAL)をネットワークの基地局へ配信するための代替オプションを説明する、単純化されたスキームである。

【図3】一実施形態に従って、どのようにUE SCAPが配信され得るかを説明する、シグナリング図である。

【図4】一実施形態に従って、悪意のあるソースeNBを検出するステップを含むハンドオーバー手続きを説明する、シグナリング図である。

【図5】一実施形態に従って、図4のハンドオーバー手続きを実行するように適合される基地局を説明する、ブロック図である。

【図6】一実施形態に従って、不正操作されまたは欠陥のある基地局の検出を支援するターゲット基地局によって実行されるステップを説明する、フローチャートである。

【図7】一実施形態に従って、不正操作されまたは欠陥のある基地局を検出できるように適合されるコアネットワークノードを説明する、ブロック図である。

【図8】一実施形態に従って、不正操作されまたは欠陥のある基地局を検出するためにコアネットワークノードによって実行されるステップを説明する、フローチャートである。

【発明を実施するための形態】

【0023】

簡潔に説明すると、本発明は、ハンドオーバー手続きの間に、不正操作されまたは欠陥のある基地局を検出するための方法についてのものである。本発明は、また、提案される方法を実行するように適合されるコアネットワークノード、および提案される方法の実行を支援するように適合される基地局についてのものである。ここでの説明は、E-UTRANの設定で提供されとしても、中心となるネットワークノードが、無線基地局とUEとの間のリンクの保護のために1つ以上のアルゴリズムを選択する任意の種類の無線基地局に、アルゴリズムの選択肢のセットを提供する、任意のシステムに同様に適用できることに、留意すべきである。したがって、以下のE-UTRANの設定は、専ら、提案される本発明の1つの適用の1つの説明例とみなされるべきである。特に、情報がハンドオーバーに関与するエンティティの間で送信される、例において言及される特定のメッセージは、専ら、実例とみなされるべきであり、したがって、他の代替となるメッセージが、代わりに使用され得ることに留意する。

【0024】

ここではeNBと呼ばれる2つの基地局間におけるUEセッションのハンドオーバーに関与する、1つの提案される方法が、以下に説明される実施形態に従って示されることができ、上記方法は以下の主なステップを含む：

1. 許可されるアルゴリズムのリストは、通信ネットワークのeNBへ提供される。このリストは、特定の優先度に従って順序付けられる。典型的に、最も高い優先度を有するアルゴリズムが、使用に最も望ましい。これ以降、このリストは、優先順位付きアルゴリズムリスト(PAL)と呼ばれる。PALは、UEごとにユニークなリスト、または全てのUEとともにグローバルに使用されるリストであり得る。

2. UEが、ネットワークに接続し、UEによりサポートされるアルゴリズム、すなわち、UEセキュリティケイパビリティ(以下、UE SCAPという)を提供すると、サー

10

20

30

40

50

ピング eNB は、サービング eNB によってサポートされ、PAL によると最も高い優先度を有するアルゴリズムを、選択する。

3. ハンドオーバーの間に、ソース eNB は、ターゲット eNB へ UE SCAP を提供し、ターゲット eNB は、UE SCAP 内に存在し、ターゲット eNB によってサポートされるアルゴリズムから、PAL によると最も高い優先度を有するアルゴリズムを選択する。

4. ハンドオーバーの後に、UE およびターゲット eNB は、次の通信におけるステップ 3 においてターゲット eNB によって選択されたアルゴリズムを使用する。

5. ターゲット eNB は、ソース eNB がハンドオーバー手続きの間に UE SCAP を不正操作しなかったことを検証する MME へ、UE SCAP をレポートする。

10

【0025】

当然ながら、危殆化されたソース eNB は、選択されたアルゴリズムを UE に与える前に、選択されたアルゴリズムを改変する可能性がある。しかしながら、これは、ターゲット eNB および UE が、異なるアルゴリズムを使用するという結果を招き、したがって、接続は、ゴミとなる。そのような状況では、eNB は、3GPP 内の現在の仕様によると、UE をリリースする。UE は、UE が送信するデータを有するとすぐに新たな接続を確立することにより、反応する。同様に、ネットワークが UE に送信するデータを有する場合に、UE は、呼び出される。したがって、そのようなシナリオの影響は、続かない。

【0026】

上記の例は、1つのアルゴリズムの選択についてのものであるが、説明された手続きが使用されて、異なる目的のための様々な種類のアルゴリズムが選択され得ることは、当業者にとって明らかである。例えば、同じメカニズムを使用して、あるアルゴリズムは、完全性保護のために選択され得るが、一方で、あるアルゴリズムは、暗号化の目的のために選択される。

20

【0027】

以下に、提案される検出メカニズムの方法のステップが、限定されない例を参照して、より詳細に説明される。

【0028】

上記のとおり、優先順位付きアルゴリズムリスト (PAL) は、アルゴリズムが使用にどの程度望ましいかに従って順位付けられるアルゴリズムのリストである。このリストは、典型的に、ネットワークの運用者によって構成され、実装の選択に依存する。以下にさらに詳細に説明されるとおり、リストは、ネットワークによりカバーされる様々なエリア内で、様々な方法で構成され得る。

30

【0029】

一般的に、eNB への PAL の配信について、考えるべき2つの主なケースがある。最初のケースでは、PAL は、UE ごとにユニークである。そのようなケースでは、PAL は、典型的に、各 UE によってサポートされることが既知であるアルゴリズムのみを含む。この情報は、UE の IMEI または類似のものから推定される、各 UE の UE SCAP、および、誤って実装され、または廃止予定であるアルゴリズムに関するナレッジから、導き出され得る。説明される例によると、各 UE の UE コンテキストが、eNB 内で確立されると、UE にユニークな PAL は、サービング eNB へ配信される。以下、この種類の PAL は、UE にユニークな PAL と呼ばれる。

40

【0030】

別のケースは、代わりに、ネットワーク内の全ての UE とともに使用される共通の PAL についてのものである。そのようなシナリオでは、PAL は、eNB 内における UE コンテキストの確立前の任意の時間に、任意の eNB へ配信され得る。以後、この種類の PAL は、グローバル PAL と呼ばれる。

【0031】

この種類の PAL が、通信ネットワークの eNB へ配信され得る、様々な方法がある。1つのソリューションの候補が、図 2a にて説明されている。セキュリティポリシーがネ

50

ットワーク内でどのように扱われているかに応じて、O & Mインターフェース 201 を介して MME 200 内でこのリストを構成し、MME 200 に、そのコントロールの下で、eNB 203 a、b、c へ PAL 202 を配信させることが、望ましい。

【0032】

1つの代替となるソリューションが、図 2 b に示されている。図 2 b は、どのように、O & M システム 201 が、代わりに、PAL 202 を用いて、eNB 203 a、b、c を直接的に構成するように設定され得るかを説明している。

【0033】

UE がネットワークに属し、または、例えば、MME の再配置、若しくは IDLE モードモビリティのために、MME 内ではじめて知られる場合、UE は、ネットワークの MME に、UE SCAP を通知し、または、MME は、UE が以前に接続されていた MME から、UE SCAP を取得する。

【0034】

図 3 は、一実施形態に従ったそのような原理を示す。一実施形態では、UE 300 がサービング eNB 301 とセキュリティを確立する場合、UE 300 の UE SCAP は、サービング eNB 301 に行き着く。最初のステップ 3:1 では、UE 300 は、MME 200 へ UE SCAP を送信する。次のステップ 3:2 で示されるとおり、MME は、記憶手段で UE SCAP を記憶し、次のステップ 3:3 で、UE SCAP は、サービング eNB 301 へ提供される。以下で説明されるとおり、例えば、UE SCAP が使用されて、UE にユニークな PAL がフィルタリングされる場合に、MME 200 から eNB 301 への UE SCAP の伝達は、暗黙的であり得る。そのようなケースでは、ステップ 3:3 a で、フィルタリングされた PAL も、サービング eNB 301 へ提供される。任意のステップ 3:3 に示されるとおり、UE にユニークな PAL も、例えば、NAS Security Mode Command を介して、MME 200 と UE 300 との間のセキュアなメッセージの中で、UE 300 へ配信され得る。

【0035】

次のステップ 3:4 に示されるとおり、ステップ 3:3 で送られた UE SCAP および PAL に基づいて、サービング eNB 301 は、アルゴリズムを選択する。アルゴリズムが選択された後に、UE 300 およびサービング eNB 301 は、選択されたアルゴリズムによって保護されたデータを交換することができる。最後のステップ 3:5 で示されるとおり、これは、データ送信手続きとして説明されている。

【0036】

また、グローバル PAL を使用する場合、MME は、ある UE について 1 つ以上のアルゴリズムをブロックするために、UE SCAP を修正し得る。そのようなシナリオでは、元の UE SCAP は、UE 300 へ送信される一方、MME 200 は、ステップ 3:3 で、サービング eNB 301 へ、修正された UE SCAP を送信し得る。

【0037】

ハンドオーバーでの MME の再配置のケースでは、ソース MME は、ターゲット MME へ UE SCAP を提供し得る。また、このケースでは、当然ながら、UE が、ネットワークに UE SCAP を再度送信する必要はない。これは、専ら、どのように情報が UE からネットワークへ送信されるかの例としての役目を果たす。留意すべき重要事項は、MME が UE についての SCAP を記憶することである。

【0038】

以前に参照した TS 36.300 に示されるとおり、eNB 間のハンドオーバーの間に、ソース eNB は、ハンドオーバーリクエストコマンドの中で、UE SCAP を、ターゲット eNB へ伝達している。

【0039】

ターゲット eNB をだまして、ソース eNB が正常に動作する場合にターゲット eNB が選択するよりも望ましくないアルゴリズムを使わせる、悪意のある eNB について、唯一の可能性は、UE SCAP、または PAL が UE にユニークな PAL である場合の P

10

20

30

40

50

ALを、改変することである。よって、一実施形態に従った、ハンドオーバの間に悪意のあるソースeNBを検出するための手続きが、ここで、図4を参照してより詳細に説明される。

【0040】

図1のステップ1：1に対応する最初のステップ4：1で、メジャメントレポートが、UE300からソースeNB400へフォワードされる。次のステップ4：2で示されるとおり、これらのレポートに基づいて、ソースeNB400は、ターゲットeNB401へ、ハンドオーバ（HO）リクエストを送信する。HOリクエストは、MMEから、または、eNB400が以前のハンドオーバでターゲットeNBとして動作していた場合には、別のeNBから、eNB400へ予め送信されたUE SCAPを含む。以前に言及されたとおり、HOリクエストは、UE SCAPに加えて、PALも含み得る。PALおよび／またはUE SCAPが、ハッシュ値として、eNB400へ提供される場合、PALおよび／またはUE SCAPの関連するハッシュ値が、実際のリストの代わりに、HOリクエストの中で送信される。別のステップ4：3で示されるとおり、PALおよび／またはUE SCAPに基づいて、ターゲットeNB401は、ソースeNBが正常に動作していると仮定して、アルゴリズムを選択する。

【0041】

ターゲットeNB401は、選択されたアルゴリズムの標識を含むHOリクエスト確認応答（acknowledgement）で、ここでソースeNBを表すeNB400に応答する。これは、図4のステップ4：4で示される。次のステップ4：5で、ソースeNB400は、選択されたアルゴリズムの標識を含むハンドオーバコマンドを、UE300へ送信する。別のステップ4：6で示されるとおり、UE300とターゲットeNB401との間のトラフィックは、以後、選択されたアルゴリズムにより保護される。次のステップ4：7で、UE300は、その後、実行されたターゲットeNB401へのハンドオーバを確認する。無線ネットワークの視点からハンドオーバが完了すると、ターゲットeNB401は、UE300が位置を変更したことをMMEに通知するために、UE SCAPを含むパススイッチメッセージ（path switch message）、典型的にはパススイッチリクエストを、MME200へ送信する。これは、ステップ4：8で示されている。UE SCAPは、パススイッチメッセージ上でピギーバックされ得る。ターゲットeNB401が、HO手続きの前にPALを持っていなかった場合、または、PALがUEにとってユニークである、すなわち、UEにユニークなPALを生成するために、PALが、UE SCAPを使用してMME200によってフィルタリングされ、したがって、ステップ4：2で、ソースeNB400からターゲットeNB401へ提供された場合、PALも、パススイッチメッセージへ追加される。これを行う理由は、PALがソースeNBによって不正操作されなかったことを、検証することができるためである。上記のように、各PALおよび／または各UE SCAPを表すハッシュ値は、各リストの代わりに、パススイッチメッセージへ追加され得る。サービングeNBへ予め送信されたUE SCAPが、修正されたUE SCAPであった場合、この修正されたUE SCAPが、ステップ4：2でターゲットeNBへ、ステップ4：8でMME200へ、送信される。

【0042】

ステップ4：9で示されるとおり、MME200が、ターゲットeNB401からパススイッチメッセージを取得すると、MME200は、UE SCAPが、MMEに既に記憶されているものと同一であることを検証することができる。また、UEにユニークなPALも送信された場合、MME200は、UEにユニークなPALが、MMEに記憶されたPALのコピーとマッチすることを検証し得る。次のステップ4：10で示されるとおり、これらのチェックのいずれかが失敗する場合、MMEは、適切な対応をとり得る。そのような適切な対応は、例えば、ネットワークからUEをリリースし、イベントをロギングし、およびO&Mシステムへアラームをあげることを含み得る。

【0043】

別の代替となる実施形態によると、提案されるソリューションは、MMEへ各値そのも

10

20

30

40

50

のをレポートする代わりに、UE SCAP、および、場合によってはまたPALのレポートを、US SCAP、および、適用できる場合にはPALのハッシュ値で、置き換えることにより、さらに効率的にされ得る。そのようなケースでは、UE SCAP/PALは、ターゲットeNB401によって、ハッシュ値を計算される。UE SCAP/PALの代わりに、ハッシュ値が、ステップ4：8で、パススイッチリクエストの中でMME200へ送信される。そして、ステップ4：9で行われる比較は、各PALおよび／または各UE SCAPのハッシュ値に基づいて行われる。

【0044】

ハッシュ値のサイズは、検出されない誤ったUE SCAPの可能性を十分に低くする程度に大きく選択され得る。典型的には、ハッシュ値のためのビット数は、圧縮されたUE SCAPそのものより少なくなるように選択される。MMEは、最初のUE SCAPのハッシュ値も保持し得る。この設定では、UE SCAPの2つのハッシュ値のみが、比較される必要があり、実際のUE SCAPそのものは、比較される必要がない。PALが、ターゲットeNBからMMEへ送信される必要がある場合に、同様の策が、使用され得る。

10

【0045】

事前の計算を通して、2つの異なるUE SCAPが同一のハッシュ値を持つことが、MME200によって発見される場合、MMEは、UE SCAPおよびMMEが選択するオフセットのハッシュ値を計算するように構成され得る。上記オフセットは、例えば、ここでは、MME__OFFS列と呼ばれる、32ビット列と連結されたUE SCAPである。MME__OFFS列は、その後、図3のステップ3：3で、MME200によって、UE SCAPまたはPALとともに、サービングeNB301へ送信される。この列は、その後、比較のステップ4：9でも使用される前に、図4のステップ4：2および4：8で、各UE SCAPまたは各PALとともに送信され、したがって、異なるリストの相互の区別を可能とする。

20

【0046】

ステップ4：8で、オフセット値が、UE SCAPおよびオフセットのハッシュとともに、ターゲットeNBによって、MMEへレポートバックされる場合、セキュリティは、さらに強化され得る。この代替となる実施形態に従って結合された列であっても、UE SCAPのリストそのものよりも短くなり得る。

30

【0047】

ハッシュ値は、任意の従来技術を使用して、生成され、識別され得る。したがって、これらの手続きは、本明細書でさらに詳細に説明されない。適しているハッシュ関数の例は、例えば、ハッシュ関数の出力列の切捨て(truncation)を可能とする、SHA1、RIPMD-160の任意の切捨てバージョンであり得る。

【0048】

どのeNBが、いずれかのリストを不正操作したかを知ること、関心であるかもしれない。これは、ステップ4：8で送信されるパススイッチリクエストの中にソースeNBのアイデンティティ(eNB ID)も含むことによって、達成され得る。代わりに、MMEは、このメッセージを介するのとは違う別の方法で、ソースeNBを識別することが可能であり得る。ソースeNBのeNB IDが、MMEへ提供される場合、そのような情報は、やはり注意して扱われるべきである。eNB IDに基づいて誤っていると思われるeNBに、ネットワークへのアクセスを自動的に禁止する代わりに、情報が、なるべく登録され、eNBは、チェックされるべきである。この理由は、悪意のあるeNBは、正常に動作するeNBを禁止するために、偽造されたパススイッチメッセージを送信し得るということである。したがって、例えば、アラームをあげ、疑わしいソースeNBをチェックするためにフィールド技術者を送り出すことが、より適切であると思われる。

40

【0049】

上記手続きのステップに従って悪意のあるソースeNBを識別するために、コアネットワークノード(典型的には、MME)を支援する基地局(典型的には、eNB)は、それ

50

に応じて適合されなければならない。1つの例示的な実施形態に従って、ターゲット基地局として動作することができる、そのような基地局が、ここで、図5を参照してより詳細に説明される。

【0050】

ターゲット基地局の機能性を基地局に提供するために適合される、この例で説明された基地局の手段に加えて、基地局は、現在の環境に応じて、基地局がソース基地局として動作することを含む追加の基地局関連タスクを扱うことを可能とする、追加の従来型の手段も備えることは、理解されるべきである。しなしながら、簡単にするために、本明細書に示されるメカニズムの理解のために必要のない任意の手段は、省略された。基地局401は、PALおよび／またはUE SCAPを含むHOLリクエストをソース基地局400から受信するように適合される、従来型の受信手段501を、備える。受信手段501は、また、MMEのようなコアネットワークノード200からグローバルPALを受信するように適合され得る。基地局401は、受信手段501へ提供される情報に基づいて、および、PALが、MME200から予め受信された場合には、この情報にも基づいて、基地局がサポートするアルゴリズムの1つを選択するように適合される、選択手段502も備える。

10

【0051】

選択手段502が、アルゴリズムを選択すると、選択手段502は、選択手段へ提供される各情報、すなわちPALおよび／またはUE SCAPのMMEへのレポートを始めるように適合される。レポートは、従来型の送信手段504を介して、パススイッチリクエストによって、MMEへ情報を送信するレポート手段503によって実行される。基地局のレポート手段503は、また、図4のステップ4：2で示されるとおり、基地局がソース基地局として動作している場合に、基地局からターゲット基地局へハンドオーバーされるUEについてのUE SCAP／PALを提供するように、構成される。

20

【0052】

ハッシュ値のレポートが、適用される場合は、レポート手段は、また、送信手段504を介してコアネットワークノード200へレポートされるUE SCAP／PALのハッシュ値を提供するように適合される。そのようなハッシュの機能性は、そのために適合される任意の従来技術を使用して、提供され得る。

【0053】

不正操作されまたは欠陥のある基地局の検出でコアネットワークノードを支援する場合における、上記基地局の機能は、図6で説明されているとおり、ブロック図で説明され得る。

30

【0054】

最初のステップ600では、基地局は、ハンドオーバーの前にネットワークの全ての基地局へ送信されるグローバルPALであり得るPAL、または、図4を参照して上記で説明されたPALのように、ハンドオーバー手続きの間にソース基地局から送信されるPALを受信する。

【0055】

次のステップ601では、基地局は、ハンドオーバーが実行される予定であるUEから、UE SCAPを受信する。次のステップ602では、基地局は、PALおよびUE SCAPを使用して、1つ以上のアルゴリズムを選択する。最後のステップ603では、基地局は、UE SCAP、および場合によってはまたPALを、MMEへレポートし、MMEが必要な検証の目的でこの情報を使用できるようにする。

40

【0056】

また、説明された実施形態でMMEとして例示された、コアネットワークノードは、それに応じて適合されなければならない。したがって、1つの例示される実施形態に従って、そのようなコアネットワークノードが、ここで、図7を参照してさらに詳細に説明される。基地局と類似して、本明細書の焦点にある発見メカニズムの理解のために必要のない任意の手段を省略するために、説明されるコアネットワークノードのアーキテクチャは、

50

単純化される。

【0057】

コアネットワークノード200は、UE300およびターゲット基地局401の両方からUE SCAPを受信するように適合される、従来型の受信手段701を備える。受信手段は、また、図2aまたは2bのいずれか一方を参照して上記で示されたとおり、ネットワークからPALを受信するように、適合される。コアネットワークノード200は、上記のとおりUEから受信されたUE SCAPを記憶するための記憶手段702も備える。ターゲット基地局401から受信されるUE SCAPは、検証手段703へフォワードされる。検証手段703は、対応する記憶された値と受信された値を比較するように適合される。コアネットワークノード200は、図3aまたは3bを参照して上記に示されたとおり、サービング基地局と通信するように適合される、送信手段704も備える。ハッシュ値が使用される場合は、検証手段203は、また、例示された実施形態によると、特定のUEのPALおよび／またはUE SCAPのための各ハッシュ値を生成するように適合される。そのような検証手段は、ターゲット基地局から受信されるハッシュ値を、記憶されたUE SCAPまたはPALの相当するハッシュ値と比較するように、さらに適合される。さらに、検証ユニットは、また、同一のハッシュ値を識別するための機能性、および、ハッシュ値を相互に区別するためのオフセット値を生成し、後の段階では、そのような値を比較するための機能性を備えるように適合され得る。上記のとおり、そのような生成および比較の機能性、並びにオフセット値を扱うための機能性は、任意の従来技術を使用して、提供され得る。したがって、この技術は、この例示されたコアネットワークノードのアーキテクチャで、さらに説明されない。パススイッチリクエストの中でコアネットワークノードへ提供される情報の処理からの出力に応じて、送信手段は、任意の他の適切なノードと通信するように適合され得る。検証手段203は、疑わしい誤った、または不正操作される基地局の検出に従って、適切なさらなる処理が実行されることを可能とするために、レポートノード705へ1つ以上のメッセージを生成し、フォワードするように、構成され得る。

【0058】

図8では、1つの例示的な実施形態に従って、より詳細に、ブロックスキームが、コアネットワークノードの動作を説明する。最初のステップ800で、上記のとおり、コアネットワークノード200は、典型的にはO&Mから、PALを受信し、記憶する。

【0059】

次のステップ801で、ノードは、UEからUE SCAPを受信し、記憶する。次のステップ802に示されたとおり、UEが、まさにHOを経験しようとしていると、ネットワークノードは、また、ターゲット基地局から、UE SCAPを受信する。両方のUE SCAPは、次のステップ803で、比較される。ステップ804で示されたとおり、ミスマッチが認識される場合、条件付きステップ805で示されたとおり、コアネットワークノードは、適切な対応をとる。一方で、比較が、成功に終わる場合、手続きは、最後のステップ806で終了する。

【0060】

本実施形態は、全ての点において、限定ではなく、例示として、みなされるべきである。したがって、本発明は、本発明の本質的な特徴から逸脱しない、ここで具体的に説明された方法以外の方法でも、実施され得ることが、理解されるべきである。

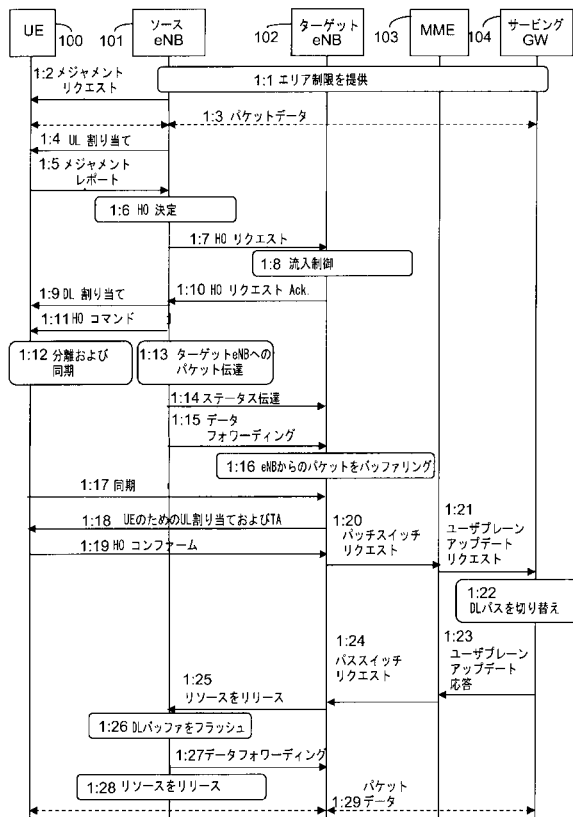
【0061】

(略語のリスト)

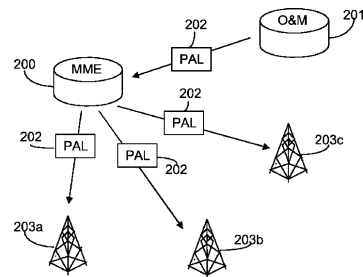
eNB	LTEの無線基地局
LTE	ロングタームエボリューション (Long Term Evolution)
MME	移動性管理エンティティ
NAS	ノンアクセスストラタム
O&M	オペレーション&メンテナンス
PAL	優先順位付きアルゴリズムリスト

SCAP UEセキュリティケイパビリティ
UE ユーザ機器

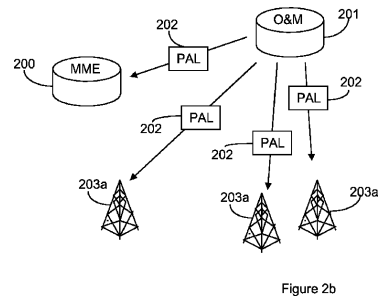
【図 1】



【図 2 a】



【図 2 b】



【図 3】

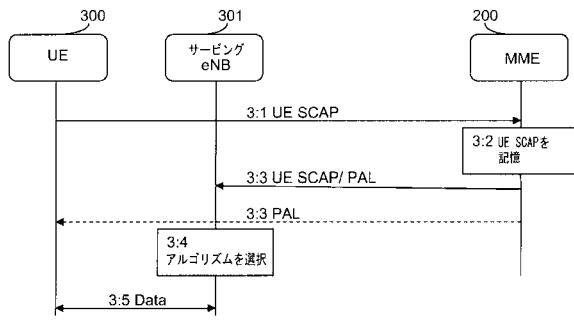


Figure 3

【図 4】

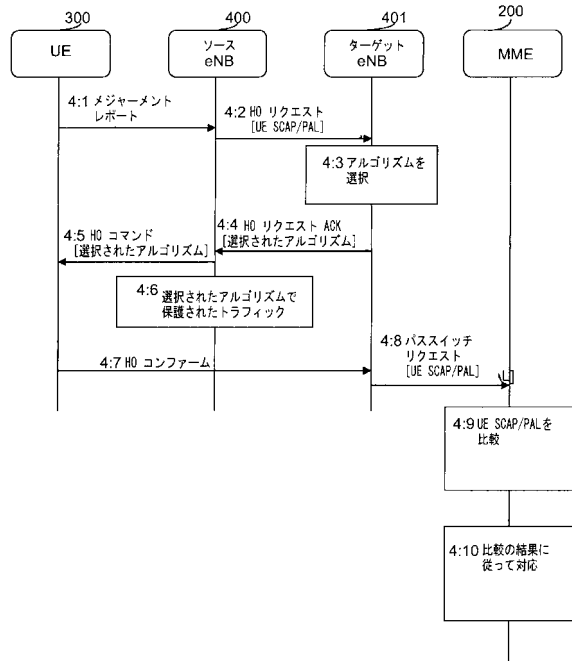


Figure 4

【図 5】

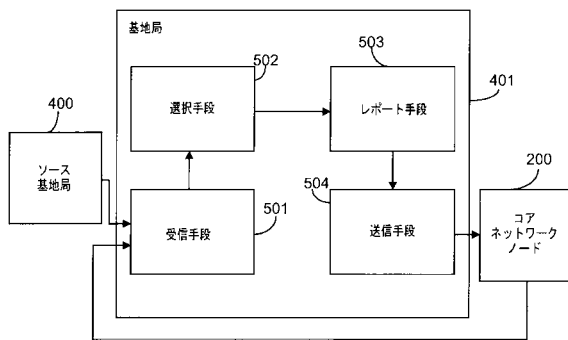


Figure 5

【図 7】

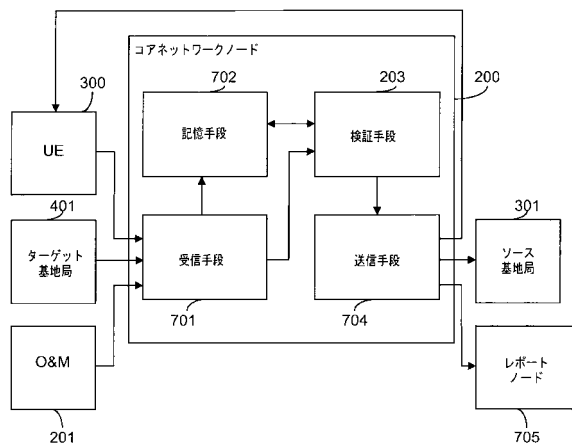


Figure 7

【図 6】

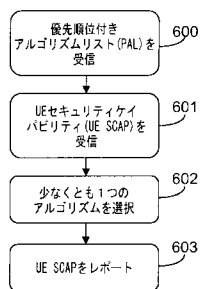


Figure 6

【図 8】

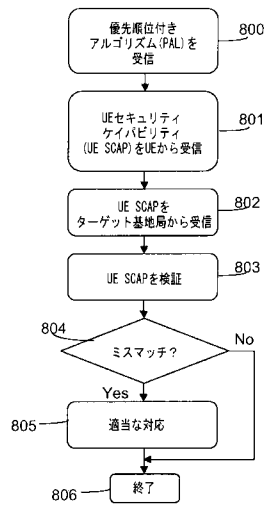


Figure 8

フロントページの続き

- (72)発明者 ノルマン、カール
スウェーデン王国 エスー１１６ ２８ ストックホルム スティグベルグスガタン ３２エー
- (72)発明者 スミーツ、ベルナルド（ベン）
スウェーデン王国 エスー２４７ ５１ ダルビー ダルバッカヴェーゲン １１
- (72)発明者 ブロム、ロルフ
スウェーデン王国 エスー１７５ ６８ イェールフェーラ スヴェールドヴェーゲン ２

審査官 廣川 浩

- (56)参考文献 特開２００７－２６７１２０（ＪＰ，Ａ）
Ericsson, "Bidding down attack at eNB to eNB active mode handover", S3-070554, 3GPP TS
G SA WG3 Meeting#48, ２００７年 ７月１３日, URL, http://www.3gpp.org/ftp/tsg_sa/wg3_security/TSGS3_48_Montreal/Docs/S3-070554.zip

- (58)調査した分野(Int.Cl., DB名)

H04B 7/24- 7/26

H04W 4/00-99/00