

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4690423号
(P4690423)

(45) 発行日 平成23年6月1日 (2011.6.1)

(24) 登録日 平成23年2月25日 (2011.2.25)

(51) Int.Cl.	F I
HO4W 12/12 (2009.01)	HO4Q 7/00 186
HO4W 8/18 (2009.01)	HO4Q 7/00 150
HO4M 11/00 (2006.01)	HO4M 11/00 303

請求項の数 21 (全 15 頁)

(21) 出願番号	特願2007-551758 (P2007-551758)	(73) 特許権者	598036300
(86) (22) 出願日	平成17年1月24日 (2005.1.24)		テレフオンアクチーボラゲット エル エム エリクソン (パブル)
(65) 公表番号	特表2008-529330 (P2008-529330A)		スウェーデン国 ストックホルム エスー
(43) 公表日	平成20年7月31日 (2008.7.31)		164 83
(86) 国際出願番号	PCT/IB2005/000103	(74) 代理人	100076428
(87) 国際公開番号	W02006/077449		弁理士 大塚 康德
(87) 国際公開日	平成18年7月27日 (2006.7.27)	(74) 代理人	100112508
審査請求日	平成19年12月25日 (2007.12.25)		弁理士 高柳 司郎
		(74) 代理人	100115071
			弁理士 大塚 康弘
		(74) 代理人	100116894
			弁理士 木村 秀二
		(74) 代理人	100130409
			弁理士 下山 治

最終頁に続く

(54) 【発明の名称】 コアネットワークの方法及び装置

(57) 【特許請求の範囲】

【請求項1】

コアネットワーク (102) を保護する方法であって、
無認可移動体アクセスネットワーク内あるいは汎用アクセスネットワーク (100) 内のネットワークコントローラ (116) で、移動局 (104) のモバイルアイデンティティを含むメッセージ (302、402) を受信する (202) ステップと、
前記ネットワークコントローラ (116) で、前記受信したモバイルアイデンティティが該ネットワークコントローラ (116) に記憶されているモバイルアイデンティティとマッチするか判定する (206) ステップと、
前記受信したモバイルアイデンティティが前記移動局 (104) に関連付けて記憶されているモバイルアイデンティティとマッチしないときは、前記ネットワークコントローラ (116) で、前記メッセージ (302、402) を破棄する (210) ステップとを備え、
前記モバイルアイデンティティは、国際移動体加入者アイデンティティ、一時移動体加入者アイデンティティあるいはパケット一時移動体加入者アイデンティティであり、
前記移動局 (104) は、前記ネットワークコントローラ (116) への登録時に使用された前記国際移動体加入者アイデンティティと同一の国際移動体加入者アイデンティティのみを使用することが許可されており、かつ前記移動局 (104) は、前記コアネットワーク (102) によって割当られた前記一時移動体加入者アイデンティティあるいは前記パケット一時移動体加入者アイデンティティと同一の前記一時移動体加入者アイデンテ

10

20

ィティあるいは前記パケット一時移動体加入者アイデンティティを使用することが許可されてい、

前記記憶されているモバイルアイデンティティの1つは、前記移動局（104）と前記無認可移動体アクセスネットワーク内あるいは汎用アクセスネットワーク（100）との間のセキュア接続の確立時に使用される国際移動体加入者アイデンティティであり、

前記一時移動体加入者アイデンティティあるいは前記パケット一時移動体加入者アイデンティティは、前記コアネットワーク（102）によって、前記移動局（104）に割当られる

ことを特徴とする方法。

【請求項2】

10

前記受信したモバイルアイデンティティが前記移動局（104）に関連付けて記憶されているモバイルアイデンティティとマッチするときは、前記メッセージ（302、402）を処理する（208）ステップを更に備える

ことを特徴とする請求項1に記載の方法。

【請求項3】

前記メッセージ（302、402）は、アップリンクメッセージ（302）あるいはダウンリンクメッセージ（402）である

ことを特徴とする請求項1に記載の方法。

【請求項4】

前記アップリンクメッセージ（302）は、移動交換局（112）、あるいは汎用パケット無線サービスサポートノードから受信される

20

ことを特徴とする請求項3に記載の方法。

【請求項5】

前記受信したメッセージ（302、402）が登録リクエストであるときは、前記ネットワークコントローラ（116）で、前記受信したモバイルアイデンティティを記憶し（512）、該受信したメッセージ（302、402）を処理するステップを更に備える

ことを特徴とする請求項1に記載の方法。

【請求項6】

前記受信したメッセージ（302、402）がダウンリンクメッセージ（402）であり、かつ前記受信したモバイルアイデンティティが前記移動局（104）に対する新規のモバイルアイデンティティであると、前記ネットワークコントローラ（116）で、該受信したモバイルアイデンティティを記憶し（610）、かつ該受信したメッセージ（302、402）を処理する（608）ステップを更に備える

30

ことを特徴とする請求項1に記載の方法。

【請求項7】

前記ダウンリンクメッセージ（402）の受領、応答確認あるいは完了するアップリンクメッセージが受信される（714）まで、前記ネットワークコントローラ（116）で、前記受信したモバイルアイデンティティは記憶されない（716）

ことを特徴とする請求項6に記載の方法。

【請求項8】

40

前記受信したメッセージ（302、402）を破棄する（210、516）ステップは、更に、

前記移動局を抹消する（518）ステップと、

所定期間、前記移動局（104）に関連付けられているインターネットプロトコルアドレスをブラックリストに掲載する（520）ステップと、

前記破棄されたメッセージと、前記移動局の抹消をシステムオペレータに通知する（522）ステップと、

前記破棄されたメッセージと、前記移動局の抹消についての情報をログに記録する（524）ステップと

を備えることを特徴とする請求項1に記載の方法。

50

【請求項 9】

前記受信したメッセージは、モビリティ管理メッセージ、汎用パケット無線サービスモビリティ管理メッセージ、あるいは U M A あるいは無認可無線リソースメッセージであることを特徴とする請求項 1 に記載の方法。

【請求項 10】

前記ネットワークコントローラ (116) は、無認可移動体アクセスネットワーク (100) 内の無認可ネットワークコントローラ (U N C) (116)、あるいはコアネットワーク (102) と通信する汎用アクセスネットワーク (100) 内の汎用アクセスネットワークコントローラ (116) である

ことを特徴とする請求項 1 に記載の方法。

10

【請求項 11】

コアネットワーク (102) を保護するためのコンピュータ可読媒体上で実現されるコンピュータプログラムであって、

無認可移動体アクセスネットワークあるいは汎用アクセスネットワーク (100) 内のネットワークコントローラ (116) で、移動局 (104) のモバイルアイデンティティを含むメッセージ (302、402) を受信する (202) ためのコードセグメントと、

前記ネットワークコントローラ (116) で、前記受信したモバイルアイデンティティが該ネットワークコントローラ (116) に記憶されているモバイルアイデンティティとマッチするか判定する (206) ためのコードセグメントと、

前記受信したモバイルアイデンティティが前記移動局 (104) に関連付けて記憶されているモバイルアイデンティティとマッチしないときは、前記ネットワークコントローラ (116) で、前記メッセージ (302、402) を破棄する (210) ためのコードセグメントとを備え、

20

前記モバイルアイデンティティは、国際移動体加入者アイデンティティ、一時移動体加入者アイデンティティあるいはパケット一時移動体加入者アイデンティティであり、

前記移動局 (104) は、前記ネットワークコントローラ (116) への登録時に使用された前記国際移動体加入者アイデンティティと同一の国際移動体加入者アイデンティティのみを使用することが許可されており、かつ前記移動局 (104) は、前記コアネットワーク (102) によって割当られた前記一時移動体加入者アイデンティティあるいは前記パケット一時移動体加入者アイデンティティと同一の前記一時移動体加入者アイデンティティあるいは前記パケット一時移動体加入者アイデンティティを使用することが許可されて、

30

前記記憶されているモバイルアイデンティティの 1 つは、前記移動局 (104) と前記無認可移動体アクセスネットワーク内あるいは汎用アクセスネットワーク (100) との間のセキュア接続の確立時に使用される国際移動体加入者アイデンティティであり、

前記一時移動体加入者アイデンティティあるいは前記パケット一時移動体加入者アイデンティティは、前記コアネットワーク (102) によって、前記移動局 (104) に割当られる

ことを特徴とするコンピュータプログラム。

【請求項 12】

40

前記受信したモバイルアイデンティティが前記移動局 (104) に関連付けて記憶されているモバイルアイデンティティとマッチするときは、前記メッセージ (302、402) を処理する (208) ためのコードセグメントを更に備える

ことを特徴とする請求項 11 に記載のコンピュータプログラム。

【請求項 13】

前記受信したメッセージ (302、402) が登録リクエストであるときは、前記ネットワークコントローラ (116) で、前記受信したモバイルアイデンティティを記憶し (512)、該受信したメッセージ (302、402) を処理するためのコードセグメントを更に備える

ことを特徴とする請求項 11 に記載のコンピュータプログラム。

50

【請求項 1 4】

前記受信したメッセージ（302、402）がダウンリンクメッセージ（402）であり、かつ前記受信したモバイルアイデンティティが前記移動局（104）に対する新規のモバイルアイデンティティであると、前記ネットワークコントローラ（116）で、該受信したモバイルアイデンティティを記憶し（610）、かつ該受信したメッセージ（302、402）を処理する（608）ためのコードセグメントを更に備える

ことを特徴とする請求項11に記載のコンピュータプログラム。

【請求項 1 5】

前記ダウンリンクメッセージの受領、応答確認あるいは完了するアップリンクメッセージが受信される（714）まで、前記ネットワークコントローラ（116）で、前記受信したモバイルアイデンティティは記憶されない（716）

ことを特徴とする請求項14に記載のコンピュータプログラム。

【請求項 1 6】

データ記憶デバイスと、移動局（104）のモバイルアイデンティティを含むメッセージ（302、402）を受信する（202）該データ記憶デバイスに通信可能に接続されているプロセッサとを備える、コアネットワーク（102）を保護するための、無認可移動体アクセスネットワークあるいは汎用アクセスネットワーク（100）内のネットワークコントローラ（116）であって、

前記データ記憶デバイスは、移動局とモバイルアイデンティティとの関係を記憶し、

前記プロセッサは、前記受信したモバイルアイデンティティが前記記憶されているモバイルアイデンティティとマッチするか判定し（206）、前記受信したモバイルアイデンティティが前記移動局（104）に関連付けて記憶されているモバイルアイデンティティとマッチしないときは、前記メッセージ（302、402）を破棄し（210）、

前記モバイルアイデンティティは、国際移動体加入者アイデンティティ、一時移動体加入者アイデンティティあるいはパケット一時移動体加入者アイデンティティであり、

前記移動局（104）は、前記ネットワークコントローラ（116）への登録時に使用された前記国際移動体加入者アイデンティティと同一の国際移動体加入者アイデンティティのみを使用することが許可されており、かつ前記移動局（104）は、前記コアネットワーク（102）によって割当られた前記一時移動体加入者アイデンティティあるいは前記パケット一時移動体加入者アイデンティティと同一の前記一時移動体加入者アイデンティティあるいは前記パケット一時移動体加入者アイデンティティを使用することが許可されて、

前記記憶されているモバイルアイデンティティの1つは、前記移動局（104）と前記無認可移動体アクセスネットワーク内あるいは汎用アクセスネットワーク（100）との間のセキュア接続の確立時に使用される国際移動体加入者アイデンティティであり、

前記一時移動体加入者アイデンティティあるいは前記パケット一時移動体加入者アイデンティティは、前記コアネットワーク（102）によって、前記移動局（104）に割当られる

ことを特徴とするネットワークコントローラ（116）。

【請求項 1 7】

当該ネットワークコントローラ（116）は、無認可ネットワークコントローラ（116）あるいは汎用アクセスネットワークコントローラである

ことを特徴とする請求項16に記載のネットワークコントローラ（116）。

【請求項 1 8】

前記プロセッサは、前記受信したモバイルアイデンティティが前記移動局（104）に関連付けて記憶されているモバイルアイデンティティとマッチするときは、前記メッセージ（302、402）を処理する（208）

ことを特徴とする請求項16に記載のネットワークコントローラ（116）。

【請求項 1 9】

前記プロセッサは、前記受信したメッセージ（302、402）が登録リクエストであ

10

20

30

40

50

るときは、前記受信したモバイルアイデンティティを記憶し（５１２）、該受信したメッセージ（３０２、４０２）を処理する

ことを特徴とする請求項１６に記載のネットワークコントローラ（１１６）。

【請求項２０】

前記プロセッサは、前記受信したメッセージ（３０２、４０２）がダウンリンクメッセージ（４０２）であり、かつ前記受信したモバイルアイデンティティが前記移動局（１０４）に対する新規のモバイルアイデンティティであると、該受信したモバイルアイデンティティを記憶し（６１０）、かつ該受信したメッセージ（３０２、４０２）を処理する（６０８）

ことを特徴とする請求項１６に記載のネットワークコントローラ（１１６）。 10

【請求項２１】

前記ダウンリンクメッセージ（４０２）の受領、応答確認あるいは完了するアップリンクメッセージが受信される（７１４）まで、前記受信したモバイルアイデンティティは記憶されない（７１６）

ことを特徴とする請求項２０に記載のネットワークコントローラ（１１６）。

【発明の詳細な説明】

【技術分野】

【０００１】

発明の分野

本発明は、一般的には、移動通信の分野に関するものであり、より詳しくは、無認可移動体アクセスネットワーク内の移動局のモバイルアイデンティティ（移動体アイデンティティ：mobile identity）をチェックすることによってコアネットワークを保護するための方法及び装置に関するものである。 20

【０００２】

背景技術

無認可移動体アクセス（UMA：unlicensed network controller）仕様は、移動局（MS：mobile station）がUNC-SGWに向けてのIPsecセキュア接続を確立する場合、また、MSがUNCで登録する場合には、無認可ネットワークコントローラ（UNC：unlicensed network controller）及び無認可ネットワークコントローラセキュアゲートウェイ（UNC-SGW：unlicensed network controller secure gateway）が、同一の国際移動体加入者アイデンティティ（IMSI：International Mobile Subscriber Identity）が使用されていることをチェックすることを勧告している。これらの場合の両方において、MSはIMSIをUNC-SGWとUNCそれぞれへ提供する。また、これらの勧告の実装は、依然としてコアネットワークが攻撃を受けやすい状態にある。 30

【０００３】

このことは、汎用アクセスネットワーク（GAN：Generic Access Network）として知られる、「A及びGbインタフェースへの汎用アクセス」に対する第３世代パートナシッププロジェクト（3GPP）標準における場合にもあてはまる。3GPP技術仕様書43.318（ステージ２）及び44.318（ステージ３）を参照されたい。ここで、3GPP仕様書の汎用アクセスネットワークコントローラ（GANC：generic access network controller）は、UMA仕様のUNCと等価であることに注意されたい。同様に、3GPP仕様の汎用アクセスネットワークコントローラセキュアゲートウェイ（GANC-SEGW：generic access network controller secure gateway）は、UMA仕様のUNC-SGWと等価である。 40

【０００４】

例えば、MSは、複数の一時移動体加入者アイデンティティ（TMSI：Temporary Mobile Subscriber Identities）あるいは複数のパケット一時移動体加入者アイデンティティ（P-TMSI：Packet Temporary Mobile Subscriber Identities）を使用して、複数のMS群、例えば、SIMカードリーダー及びUMAクライアントを備えるパーソナルコンピュータ（PC）をエミュレートすることができる。また、敵対的なMSは、位置更新 50

あるいはIMS I 消去メッセージをコアネットワークに向けて送信することで、MS レベルでのサービス拒否（DoS：denial-of-service）攻撃の類を発生させることができる（呼の終了が失敗する等）。従って、移動局がコアネットワークと通信する場合に、それらによって使用されるモバイルアイデンティティ（IMS I、TMS I 及びP-TMS I の少なくともいずれか）をチェックすることによって、コアネットワークを保護する方法及び装置が必要とされている。

米国特許出願第2003/0081607A1号公報（2003年5月1日）は、GPRSネットワーク内のサービスノード間、例えば、在圏GPRSサポートノード（SGSN）とゲートウェイGPRSサポートノード（GGSN）間のGPRSトンネリングプロトコル（GTP）パケットのフィルタ処理を行うための方法を開示している。このGTPフィルタは、GTPパケット／メッセージを検査し、解析し、そしてフィルタ処理を実行し、そして、様々な条件を満足しないパケットを破棄する。但し、このGTPフィルタは、IMS I アドレスのチェックを実行し、すべてのフィルタリングがGPRSサービスノードで実行され、このノードは、コアネットワークの内部あるいはその周辺に存在する。

ゴパル、チャン及びワンによる、IEEEの論文「3Gモバイルネットワーク用のユーザプレーンファイアウォール」（2003年、IEEE、ISBN：0-7803-7954-3）は、GGSNでのファイアウォールを開示している。このファイアウォールは、無線ネットワーク内での攻撃を防止するための理想的な位置に配置されている。このファイアウォールは、フィルタ及びポリシー／ルールを使用して、悪意のあるメッセージを識別し、かつそれらを破棄する。すべてのフィルタリングはGGSNで実行され、これは、コアネットワークの周辺に存在する。

米国特許出願第2002/0032029A1（2002年3月14日）は、多国間電気通信ネットワーク内でパケットデータを送信するためのシステムを開示している。このシステムは、第1国の電気通信ネットワークを介して転送される、特定の移動局に対応するデータパケットを検出し、第1国の電気通信ネットワークと、少なくとも第2国の電気通信ネットワーク間で送信される、特定の移動局に対応するデータパケットを検出するためのデバイス及び方法を含んでいる。

2004年12月23日に出版されている国際特許出願WO2004/112328A1は、通信システム内のMBMSサービスを用いて、UEのルートエリア更新を実行する方法を開示している。これは、新規のU-GGSNと旧SGSN／新SGSN間の対話、加えて、M-GGSNと旧SGSN／新SGSN間の対話を信号でやり取りしている。UEは、新規のRAへ進入した後、MBMSサービスを使用することを継続することができる。MBMSをサポートしないSGSNは、MBMSサービスをUEへ間接的にも提供することができる。U-GGSNは、ポイントツーポイントPSモードで、MBMSサービスをUEへ提供することができる。つまり、UE、SGSN及びGGSN内のMBMSコンテキストは一貫して維持されている。

【0005】

発明の要約

本発明は、移動局（MS）がコアネットワークと通信する場合に、それらによって使用されるモバイルアイデンティティ（国際移動体加入者アイデンティティ（IMS I）、一時移動体加入者アイデンティティ（TMS I）及びパケット一時移動体加入者アイデンティティ（P-TMS I）の少なくともいずれか）をチェックすることによって、コアネットワークを保護する方法及び装置を提供する。簡単に説明すると、（登録後の）MSに関連付けて記憶されている移動体識別子に対応しない移動体識別子を含むメッセージは破棄される。このようなメッセージが一旦破棄されると、様々な予防及び報告動作を行うことができる。それゆえ、MSは、1つのIMS I、1つのTMS I及び1つのP-TMS Iを使用することだけが許可されている。その結果、本発明は、悪意のある、かつ不完全なMS実装からコアネットワークを保護する。本発明は、無認可移動体アクセスネットワーク（UMAN）及びGANの両方に適用可能である。

【0006】

より詳しくは、本発明は、MSのモバイルアイデンティティを含むメッセージを受信し、かつ受信したモバイルアイデンティティが移動局に関連付けて記憶されているモバイルアイデンティティとマッチしないときは、メッセージを破棄することによって、コアネットワークを保護するための方法を提供する。受信したモバイルアイデンティティがMSに関連付けて記憶されているモバイルアイデンティティとマッチするときは、メッセージが処理される。モバイルアイデンティティは、IMSI、TMSIあるいはP-TMSIであり得る。メッセージは、アップリンクメッセージあるいはダウンリンクメッセージであり得る、これには、例えば、モビリティ管理（MM）メッセージ、汎用パケット無線サービス（GPRS）モビリティ管理（GMM）メッセージ、あるいはUMAあるいは無認可無線リソース（URR）メッセージ（MSとUNC間でのみ使用される）がある。本発明は、コンピュータ可読媒体上で実現されるコンピュータプログラムとして実現することができる。ここで、このコンピュータ可読媒体では、様々な方法ステップが1つ以上のコードセグメントによって実現される。

10

【0007】

加えて、本発明は、プロセッサと通信可能に接続されているデータ記憶デバイスを含む装置を提供する。このデータ記憶デバイスは、MSとモバイルアイデンティティとの関係を記憶する。このプロセッサは、MSのモバイルアイデンティティを含むメッセージを受信し、かつその受信したモバイルアイデンティティがMSに関連付けて記憶されているモバイルアイデンティティとマッチしないときは、メッセージを破棄する。この装置は、典型的には、無認可移動体アクセスネットワーク（UMAN）内の無認可ネットワークコントローラ（UNC）、あるいはコアネットワーク（102）と通信する汎用アクセスネットワーク（GAN）内の汎用アクセスネットワークコントローラ（GANC）である。

20

【0008】

発明の詳細

本発明の様々な実施形態の実施及び使用については以下で詳細に説明するが、本発明は、様々な特殊な状況に広く実施することができる、多くの適用可能な発明の概念を提供することが理解されるべきである。本明細書で説明する特定の実施形態は、本発明を実施し、かつ使用するための特定の方法を単に例示しているに過ぎず、本発明の範囲を制限するものではない。

【0009】

本発明の理解を容易にするために、いくつかの用語を以下に定義する。本明細書で定義される用語は、本発明に関連する分野の当業者によって一般に理解される意味を有している。例えば、英語の不定冠詞「a」、「an」及び定冠詞「the」は単一のエンティティのみを参照することを意図するものではなく、図示のために使用することができる特定例の一般的な分類を含むことを意味するものである。本明細書の用語は、本発明の特定の実施形態を説明するために使用されるが、請求項で説明されるもの以外は、その使用は本発明を制限するものではない。

30

【0010】

本発明は、移動局（MS）がコアネットワークと通信する場合に、それらによって使用されるモバイルアイデンティティ（国際移動体加入者アイデンティティ（IMSI）、一時移動体加入者アイデンティティ（TMSI）及びパケット一時移動体加入者アイデンティティ（P-TMSI）の少なくともいずれか）をチェックすることによって、コアネットワークを保護する方法及び装置を提供する。簡単に説明すると、（登録後の）MSに関連付けて記憶されている移動体識別子に対応しない移動体識別子を含むメッセージは破棄される。このようなメッセージが一旦破棄されると、様々な予防及び報告動作を行うことができる。それゆえ、MSは、1つのIMSI、1つのTMSI及び1つのP-TMSIを使用することだけが許可されている。その結果、本発明は、悪意のある、かつ不完全なMS実装からコアネットワークを保護する。本発明は、無認可移動体アクセスネットワーク（UMAN）及びGANの両方に適用可能であることに注意されたい。

40

【0011】

50

ここで、図1を参照すると、無認可移動体アクセス（UMA）ネットワーク（UMAN）あるいは汎用アクセスネットワーク（GAN）100と、コアネットワーク102間でのモバイルアイデンティティの使用を示す代表的なシグナリングシーケンスが示されている。MS104がUNC-SGWあるいはGANC-SEGW106に向けてIPsecセキュア接続108を確立する場合には、EAP-SIMあるいはEAP-AKAを使用して、無認可ネットワークコントローラのセキュアゲートウェイ（UNC-SGW）あるいは汎用アクセスネットワークコントローラのセキュアゲートウェイ（GANC-SEGW）106へ、MS104はIMSIを提供する。UNC-SGWあるいはGANC-SEGW106は、周知のシグナリング及び認証プロトコル（認証、認可及びアカウントリング（AAA）インフラストラクチャ114）を使用して、HLR110でこのIMSIを認証する110。また、MS104がUNCあるいはGANC116に登録する場合118、無認可ネットワークコントローラ（UNC）あるいは汎用アクセスネットワークコントローラ（GANC）116へも、MS104はIMSIを提供する。加えて、MS104はコアネットワーク102（例えば、MSC112）と通信する場合（120）、MS104は、IMSI、TMSIあるいはP-TMSIを使用して自身を識別する。

【0012】

登録118を行う場合に、TMSIとP-TMSIはUNCあるいはGANC116には報告されないことに注意されたい。TMSIとP-TMSIは、位置エリア内にのみ意義を有している。位置エリア外では、TMSIとP-TMSIは、一義的なアイデンティティを提供するために、位置エリア識別子（LAI）と組み合わせられなければならない。通常は、TMSIあるいはP-TMSIの再割当は、少なくとも位置エリアの各変更地点で実行される。このような選択は、ネットワークオペレータに任せられている。

【0013】

モバイルアイデンティティは、MS104とMSC/訪問先位置レジスタ（VLR）112間の以下のモビリティ管理（MM）メッセージで使用される。

【0014】

MS104からMSC/VLR112へ（アップリンクメッセージ）：

位置更新リクエスト（LOCATION UPDATING REQUEST）

アイデンティティ応答（IDENTITY RESPONSE）

CMサービスリクエスト（CM SERVICE REQUEST）

IMSI消去指示（IMSI DETACH INDICATION）

CM再確立リクエスト（CM RE-ESTABLISHMENT REQUEST）

MSC/VLR112からMS104へ（ダウンリンクメッセージ）：

TMSI再割当コマンド（TMSI REALLOCATION COMMAND）

位置更新受領（LOCATION UPDATING ACCEPT）

モバイルアイデンティティは、MS104からMSC/VLR112へのページング応答（PAGING RESPONSE）メッセージでも使用される。UNCあるいはGANC116は、それゆえ、MS104とMSC/VLR112間で送信されるMMメッセージでチェックを実行することができる。

【0015】

図2を参照すると、本発明に従うコアネットワーク102を保護する方法200を示すフローチャートが示されている。ブロック202で、UNCあるいはGANC116は、MS104のモバイルアイデンティティを含むメッセージを受信する。ブロック204で、UNCあるいはGANC116は、MS104に関連付けて記憶されているモバイルアイデンティティと受信したモバイルアイデンティティを比較することによって、その受信したモバイルアイデンティティが正常であるか判定する。判定ブロック206での判定として、その受信したモバイルアイデンティティが正常である場合、ブロック208で、その受信したメッセージが処理される（例えば、転送等）。一方、判定ブロック206での判定として、受信したモバイルアイデンティティが正常でない場合、ブロック210で、その受信したメッセージは破棄される。モバイルアイデンティティは、IMSI、TMSI、P-TMSI

IあるいはP-TMSIであり得る。その受信したメッセージは、アップリンクメッセージあるいはダウンリンクメッセージであり得る、これには、例えば、モビリティ管理（MM）メッセージ、汎用パケット無線サービス（GPRS）モビリティ管理（GMM）メッセージ、あるいはUMAあるいは無認可無線リソース（URR）メッセージ（MS104とUNC116間でのみ使用される）がある。

【0016】

UNCあるいはGANC116は、レイヤ違反を実行することによって、即ち、コアネットワーク102に向けてMS104から送信される上位レイヤメッセージに忍び込ませる（sneaking）ことによって、MS104のモバイルアイデンティティが正常であることを判定し、UNCあるいはGANC116に登録するために使用されているIMSIと同一のIMSIをMS104が使用しているか確認する。TMSI値はMSC/VLR112によって割当られ、またP-TMSI値はSGSNによって割当られているので、UNCあるいはGANC116は、MS104がMSC112によって割当られている値を使用していることをチェックすることができる。これは、コアネットワーク102によって送信される上位レイヤダウンリンクメッセージをチェックすることによって再度実行して、TMSI値あるいはP-TMSI値のどちらがMS104に割当られているかを確認することができ、更に、その上位レイヤアップリンクメッセージをチェックすることによって、MS104が実際に割当られているTMSI値あるいはP-TMSI値を使用していることを確認することができる。

【0017】

本発明は、UNCあるいはGANC116のような装置として実現することができ、この装置は、プロセッサと通信可能に接続されているデータ記憶デバイスを含んでいる。このデータ記憶デバイスは、モバイルアイデンティティとMS104との関係を記憶している。このプロセッサは、MS104のモバイルアイデンティティを含むメッセージを受信し202、受信したモバイルアイデンティティがMS104に関連付けて記憶されているモバイルアイデンティティとマッチしないときはそのメッセージを破棄する210。プロセッサは、プレプロセッサ、フィルタあるいはこの装置内の他の処理デバイスであり得る。このデータ記憶デバイスは、メモリ、ディスクドライブ、ハードドライブ等であり得る。

【0018】

ここで、図3を参照すると、アップリンクメッセージ302に関して、本発明の実施形態を使用するシグナリングシーケンス300が示されている。UNCあるいはGANC116はモバイルアイデンティティを含むアップリンクメッセージ302を受信すると、UNCあるいはGANC116はモバイルアイデンティティをチェックする304。アップリンクメッセージ302が登録リクエスト（即ち、新規MS104）である場合、UNCあるいはGANC116は、その受信したモバイルアイデンティティを記憶し、それをMS104と関連づけ、そして、その受信したメッセージを処理する（即ち、登録を実行する）。チェック304が失敗する場合—その受信したモバイルアイデンティティがMS104に関連付けて記憶されているモバイルアイデンティティとマッチしない場合、メッセージが破棄される302。一方、チェック304が成功する場合—その受信したモバイルアイデンティティがMS104に関連付けて記憶されているモバイルアイデンティティとマッチする場合—あるいはモバイルアイデンティティが検出不能である場合、UNCあるいはGANC116は、メッセージ302を処理する（例えば、メッセージを転送する306）。モバイルアイデンティティは、MS104とSGSN間の、いくつかのGMMメッセージ、GPRSモビリティ管理（GMM）メッセージで検出不能である可能性がある。これは、それらが、LLCレイヤ上で暗号化されて送信される場合があり、かつUNCあるいはGANC116が容易にそのメッセージを忍び込ませることができないからである。例えば、ルーティングエリア更新リクエスト（ROUTING AREA UPDATE REQUEST）メッセージは、通常暗号化されずに送信され、かつUNCあるいはGANC116はそのメッセージをチェックすることができる。

【0019】

より詳しくは、アップリンクメッセージ302がIMSIを含んでいる場合、UNCあるいはGANC116はそのIMSIが、登録中にMS104によって提供されるものと同一であることをチェックする。同一である場合、そのメッセージ306はコアネットワークへ転送される。異なる場合、そのメッセージは破棄される。UNCあるいはGANC116は、MS104を抹消し、MS104によって使用されているIPアドレスを一時的にブラックリストに掲載することができる。その他の動作として、オペレータへアラームを通知すること、及びイベントのログを記録することが含んでいても良い。

【0020】

アップリンクメッセージ302にTMSIあるいはP-TMSIを含んでいて、かつUNCあるいはGANC116が、MS104に対するTMSIあるいはP-TMSIを記憶していない場合、TMSIあるいはP-TMSIがMS104コンテキストに記憶される。一方、UNCあるいはGANC116がこのMS104に対するTMSIあるいはP-TMSIを既に記憶している場合、UNCあるいはGANC116はこれらのTMSIあるいはP-TMSI値が同一であることをチェックする。これらが同一である場合、メッセージ306はコアネットワークへ転送される。それらが異なる場合、そのメッセージは破棄される。また、UNCあるいはGANC116は、MS104を抹消し、MS104によって使用されているIPアドレスを一時的にブラックリストに掲載することができる。その他の動作として、オペレータへアラームを通知すること、及びイベントのログを記録することが含んでいても良い。

【0021】

図4を参照すると、ダウンリンクメッセージ402に関して、本発明の実施形態を使用するシグナリングシーケンス400が示されている。UNCあるいはGANC116はモバイルアイデンティティを含むダウンリンクメッセージ402を受信すると、UNCあるいはGANC116はモバイルアイデンティティをチェックする404。ダウンリンクメッセージ402がMS104に対する新規の（新規に割り当てられているあるいは変更されている）モバイルアイデンティティを含んでいると、UNCあるいはGANC116はその受信したモバイルアイデンティティを記憶し、それをMS104と関連付け、そして、その受信したメッセージを処理する（即ち、そのメッセージ406をMS104へ転送する）。チェック404が、モバイルアイデンティティがMS104に対して既に記憶されている（既に存在している）と判定する場合、その受信したメッセージは処理される（即ち、そのメッセージ406がMS104へ転送される）。選択的には、ダウンリンクメッセージ402の受領、応答確認あるいは完了するアップリンクメッセージが受信されるまで、モバイルアイデンティティを記憶せずに保持することができる。

【0022】

例えば、ダウンリンクメッセージ402がTMSI再割当コマンド（TMSI REALLOCATION COMMAND）である場合、UNCあるいはGANC116は割り当てられたTMSI値をMS104コンテキストに記憶する。ダウンリンクメッセージは、MS104コンテキストに関連付けられているシグナリング接続において受信される。TMSI再割当完了（TMSI REALLOCATION COMPLETE）メッセージがMS104から受信されるまで、TMSIのMS104への記憶は遅延させることもできる。同様に、ダウンリンクメッセージ402が位置更新受領（LOCATION UPDATING ACCEPT）であり、かつ新規のTMSIがMS104へ割り当てられている場合、UNCあるいはGANC116はその割り当てられているTMSI値をMS104コンテキストに記憶する。TMSI再割当完了（TMSI REALLOCATION COMPLETE）メッセージがMS104から受信されるまで、TMSIのMS104コンテキストへの記憶は遅延させることもできる。P-TMSI再割当コマンド（P-TMSI REALLOCATION COMMAND）に対する処理は、同様に処理される。

【0023】

図5を参照すると、アップリンクメッセージに関して、本発明の実施形態に従う方法500を示すフローチャートが示されている。ブロック502で、アップリンクメッセージ

10

20

30

40

50

が受信される。判定ブロック504の判定として、その受信したメッセージがMSのモバイルアイデンティティを含んでいない（あるいは検出不能である）場合、ブロック506で、アップリンクメッセージが処理される（例えば、転送される、実行される等）。一方、判定ブロック504の判定として、アップリンクメッセージがMSのモバイルアイデンティティを含んでいて、判定ブロック508の判定として、そのモバイルアイデンティティがIMSIであり、判定ブロック510の判定として、そのアップリンクメッセージが登録リクエストである場合、ブロック512で、IMSIが記憶され、MSと関連付けられ、そしてMSが登録される。一方、判定ブロック510の判定として、アップリンクメッセージが登録リクエストでなく、判定ブロック514の判定として、受信したIMSIがMSに関連付けて記憶されているIMSIとマッチする場合、ブロック506で、そのメッセージが通常に処理される。一方、判定ブロック514の判定として、受信したIMSIがMSに関連付けて記憶されているIMSIとマッチしない場合、ブロック516で、メッセージが破棄される。UNCあるいはGANC116は次の動作のいずれかあるいはすべてを実行しても良い。：ブロック518で、MSを抹消する。ブロック520で、所定期間、MSに関連付けているIPアドレスをブラックリストに掲載する。ブロック522で、破棄されたメッセージと移動局の抹消をシステムオペレータに通知する。ブロック524で、破棄されたメッセージ及び移動局の抹消についての情報をログに記録する。

【0024】

一方、判定ブロック508の判定として、モバイルアイデンティティがTMSIあるいはP-TMSIであり、判定ブロック526の判定として、TMSIあるいはP-TMSIがMSに対してまだ記憶されていない場合、ブロック528で、TMSIあるいはP-TMSIが記憶され、MSと関連付けられ、ブロック506で、メッセージが通常に処理される。一方、判定ブロック526の判定として、TMSIあるいはP-TMSIがMSに対して既に記憶されていて、判定ブロック530の判定として、受信したTMSIあるいはP-TMSIがMSに関連付けて記憶されているTMSIあるいはP-TMSIとマッチする場合、ブロック506で、メッセージが通常に処理される。一方、判定ブロック530の判定として、受信したTMSIあるいはP-TMSIがMSに関連付けて記憶されているTMSIあるいはP-TMSIとマッチしない場合、ブロック516で、メッセージが破棄される。UNCあるいはGANC116は次の動作のいずれかあるいはすべてを実行しても良い。：ブロック518で、MSを抹消する。ブロック520で、所定期間、MSに関連付けているIPアドレスをブラックリストに掲載する。ブロック522で、破棄されたメッセージと移動局の抹消をシステムオペレータに通知する。ブロック524で、破棄されたメッセージ及び移動局の抹消についての情報をログに記録する。

【0025】

図6を参照すると、ダウンリンクメッセージに関して、本発明の実施形態に従う方法600を示すフローチャートが示されている。ブロック602で、ダウンリンクメッセージが受信される。判定ブロック604の判定として、そのダウンリンクメッセージがMSに対するTMSIあるいはP-TMSIを含んでいない（あるいは検出不可能である）場合、ブロック606で、そのダウンリンクメッセージが処理される（例えば、転送される、実行される等）。一方、判定ブロック604の判定として、ダウンリンクメッセージがMSに対するTMSIあるいはP-TMSIを含んでいて、判定ブロック608の判定として、TMSIあるいはP-TMSIが新規でない場合（即ち、UNCあるいはGANC116が既にTMSIあるいはP-TMSIを記憶していて、それをMSと関連付けている）、ブロック606で、ダウンリンクメッセージが通常に処理される。一方、判定ブロック608の判定として、TMSIあるいはP-TMSIが新規である場合、ブロック610で、TMSIあるいはP-TMSIが記憶され、MSと関連付けられ、ブロック606で、そのメッセージが通常に処理される。

【0026】

図7を参照すると、ダウンリンクメッセージに関して、本発明の別の実施形態に従う方法700を示すフローチャートが示されている。ブロック702で、ダウンリンクメッセ

10

20

30

40

50

ージが受信される。判定ブロック704の判定として、そのダウンリンクメッセージがMSに対するTMSIあるいはP-TMSIを含んでいない（あるいは検出不可能である）場合、ブロック706で、そのダウンリンクメッセージが処理される（例えば、転送される、実行される等）。一方、判定ブロック704の判定として、ダウンリンクメッセージがMSに対するTMSIあるいはP-TMSIを含んでいて、判定ブロック708の判定として、TMSIあるいはP-TMSIが新規でない場合（即ち、UNCあるいはGANC116が既にTMSIあるいはP-TMSIを記憶していて、それをMSと関連付けている）、ブロック706で、ダウンリンクメッセージが通常に処理される。一方、判定ブロック708の判定として、TMSIあるいはP-TMSIが新規である場合、ブロック710で、TMSIあるいはP-TMSIが保持され、ブロック712で、そのメッセージが通常に処理される。ブロック714で、保持されているTMSIあるいはP-TMSIを含む受信したダウンリンクメッセージの受領、応答確認あるいは完了するアップリンクメッセージが受信されるまで、TMSIあるいはP-TMSIが保持される。

10

【0027】

上述の任意の方法は、コンピュータ可読媒体上で実現されるコンピュータプログラムとして実現することができる。ここで、このコンピュータ可読媒体では、様々な方法ステップが1つ以上のコードセグメントによって実現される。

【0028】

本願発明の範囲は、明細書に記載されている処理、機器、製造物、合成物、手段、方法及ぶステップの特定の実施形態に制限されるものと意図されるものではない。

20

【図面の簡単な説明】**【0029】**

【図1】UMAネットワークとコアネットワーク間のモバイルアイデンティティの使用を示すシグナリングシーケンスを示す図である。

【図2】本発明に従うコアネットワークを保護する方法を示すフローチャートである。

【図3】アップリンクメッセージに関して、本発明の実施形態を使用するシグナリングシーケンスを示す図である。

【図4】ダウンリンクメッセージに関して、本発明の実施形態を使用するシグナリングシーケンスを示す図である。

【図5】アップリンクメッセージに関して、本発明の実施形態に従う方法を示すフローチャートである。

30

【図6】ダウンリンクメッセージに関して、本発明の実施形態に従う方法を示すフローチャートである。

【図7】ダウンリンクメッセージに関して、本発明の他の実施形態に従う方法を示すフローチャートである。

【図 1】

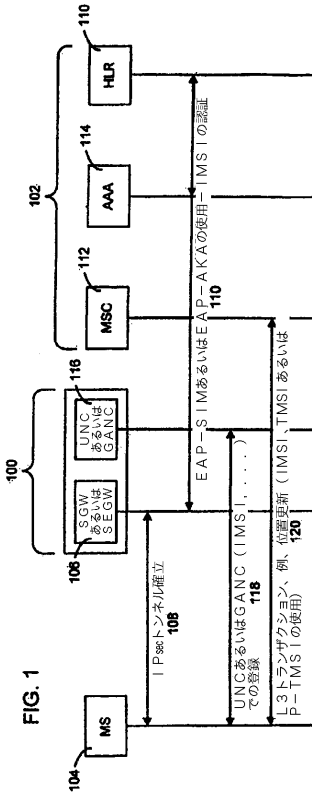


FIG. 1

【図 2】

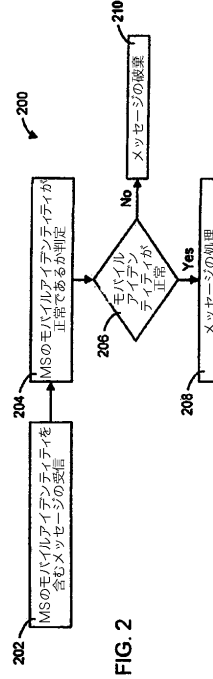


FIG. 2

【図 3】

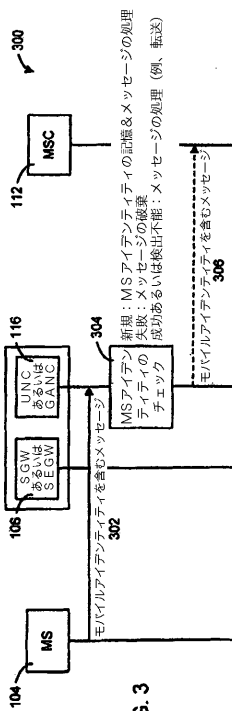


FIG. 3

【図 4】

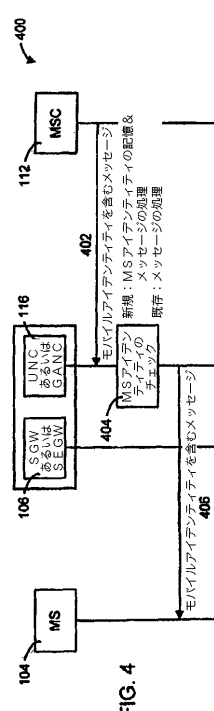
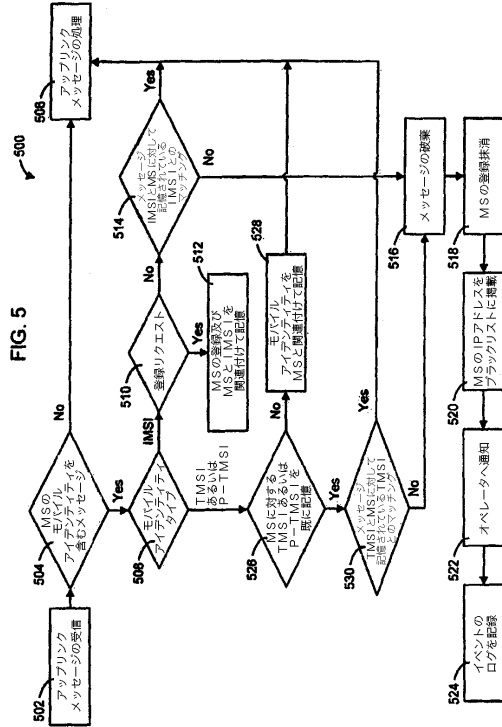
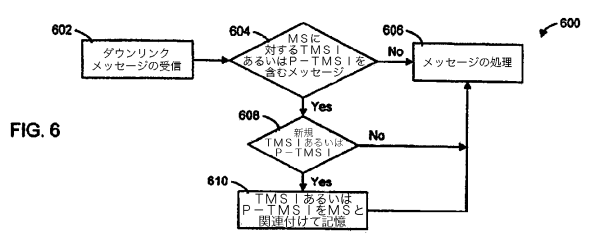


FIG. 4

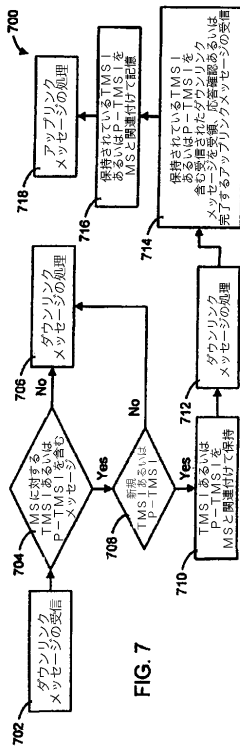
【図 5】



【図 6】



【図 7】



フロントページの続き

- (72)発明者 ビックベルイ, ヤリ, タピオ
スウェーデン国 イェーマ エスー153 38, スベルセタースベージェン 12
- (72)発明者 ニランダー, トーマス
スウェーデン国 ベルムデ エスイー139 34, ヘグトルプスベージェン

審査官 石原 由晴

- (56)参考文献 米国特許出願公開第2003/0081607 (US, A1)
特表2002-532988 (JP, A)
特開平11-127468 (JP, A)
特開2004-215118 (JP, A)
特開2002-271874 (JP, A)

- (58)調査した分野(Int.Cl., DB名)
- | | |
|------|------------|
| H04B | 7/24-7/26 |
| H04W | 4/00-99/00 |
| H04M | 11/00 |