(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6588562号
(P6588562)

(45)発行日　令和1年10月9日(2019.10.9)　(24)登録日　令和1年9月20日(2019.9.20)

(51)Int.Cl.		F I	
H04W 8/26	(2009.01)	H04W	8/26
H04W 12/06	(2009.01)	H04W	12/06
H04W 60/00	(2009.01)	H04W	60/00

請求項の数 48　(全 33 頁)

(21)出願番号	特願2017-545967(P2017-545967)
(86)(22)出願日	平成28年2月22日(2016.2.22)
(65)公表番号	特表2018-513581(P2018-513581A)
(43)公表日	平成30年5月24日(2018.5.24)
(86)国際出願番号	PCT/US2016/018860
(87)国際公開番号	WO2016/140823
(87)国際公開日	平成28年9月9日(2016.9.9)
審査請求日	平成31年2月8日(2019.2.8)
(31)優先権主張番号	62/128,724
(32)優先日	平成27年3月5日(2015.3.5)
(33)優先権主張国・地域又は機関	米国(US)
(31)優先権主張番号	14/808,862
(32)優先日	平成27年7月24日(2015.7.24)
(33)優先権主張国・地域又は機関	米国(US)

(73)特許権者　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　ス・ボム・イ
アメリカ合衆国・カリフォルニア・９２１２１・サン・ディエゴ・モアハウス・ドライヴ・５７７５

最終頁に続く

(54)【発明の名称】ワイヤレスネットワーク内の識別情報プライバシ

(57)【特許請求の範囲】

【請求項１】

ユーザ機器(UE)によるネットワークアクセスのための方法であって、

初期アタッチメッセージを用いて前記UEを識別するために、国際モバイル加入者識別情報(IMSI)の直接の代替としてプライバシモバイル加入者識別情報(PMSI)を前記UEからサービングネットワークを介してサーバに送るステップと、

次のPMSIおよびトラッキングインデックスを含む認証要求を前記サーバから受信するステップと、

前記UEによって、前記PMSIおよび前記トラッキングインデックスからUEベースの次のPMSIを導出するステップと、

前記UEによって、前記UEベースの次のPMSIと前記サーバから受信する前記次のPMSIとが一致することに応答して、前記サーバから受信する前記次のPMSIに対する肯定応答を生成するステップと、

前記肯定応答を前記UEから前記サーバに送るステップと

を含む方法。

【請求項２】

前記UEによって、初期PMSIに基づいてネットワークアクセスのための前記PMSIを判定するステップ

をさらに含む、請求項1に記載の方法。

【請求項３】

前記サーバへの前記UEの加入者登録中に前記初期PMSIを受信するステップ
をさらに含む、請求項2に記載の方法。
【請求項４】
前記サーバとの無線通信を介する加入者登録の後に前記初期PMSIをプロビジョニングするステップ
をさらに含む、請求項2に記載の方法。
【請求項５】
前記UEによって、提案されるPMSIを、前記UEにおいて生成される乱数または疑似乱数を含む数から生成するステップと、
前記UEによって、サーバ公開鍵を使用して、前記生成されたPMSIを暗号化するステップであって、前記サーバは、対応するサーバ秘密鍵を維持する、暗号化するステップと、
暗号化の後に前記生成されたPMSIを前記UEから前記サーバに送るステップと、
前記UEにおいて、前記初期PMSIとして前記生成されたPMSIを使用するために前記サーバから肯定応答を受信するステップと
をさらに含む、請求項4に記載の方法。
【請求項６】
生成する前記ステップより前に、一致があるかどうかを判定するために、前記UEベースの次のPMSIを前記認証要求の一部として受信された前記次のPMSIと比較するステップ
をさらに含む、請求項1に記載の方法。
【請求項７】
次のアタッチメッセージ内での使用のために、前記UEにおいて、確認された次のPMSIを記憶するステップ
をさらに含む、請求項1に記載の方法。
【請求項８】
前記認証要求を受信する前記ステップは、
匿名鍵を使用して前記認証要求内の前記次のPMSIを暗号化解除するステップであって、前記匿名鍵は、前記UEと前記サーバとの間で共有される秘密鍵から導出される、暗号化解除するステップ
をさらに含む、請求項1に記載の方法。
【請求項９】
前記次のPMSIが、PMSI生成鍵とともに前記PMSIに連結される前記トラッキングインデックスのハッシュを含む、請求項1に記載の方法。
【請求項１０】
ユーザ機器（UE）であって、
プライバシモバイル加入者識別情報(PMSI)を記憶するように構成されたメモリと、
初期アタッチメッセージを用いて前記UEを識別するために、国際モバイル加入者識別情報(IMSI)の直接の代替として前記PMSIをサービングネットを介してサーバに送り、
次のPMSIおよびトラッキングインデックスを含む認証要求を前記サーバから受信するように構成されたトランシーバと、
前記PMSIおよび前記トラッキングインデックスからUEベースの次のPMSIを導出し、
前記UEベースの次のPMSIと前記サーバから受信する前記次のPMSIとが一致することに応答して、前記サーバから受信する前記次のPMSIに対する肯定応答を生成する
ように構成されたプロセッサと
を含み、
前記トランシーバは、前記肯定応答を前記サーバに送るようにさらに構成される、ユーザ機器。
【請求項１１】
前記プロセッサは、
前記メモリ内に記憶された初期PMSIに基づいてネットワークアクセスのための前記PMSIを判定する

ようにさらに構成される、請求項10に記載のユーザ機器。
【請求項１２】
前記ユーザ機器は、前記サーバへの前記UEの加入者登録中に前記初期PMSIを受信する、請求項11に記載のユーザ機器。
【請求項１３】
前記ユーザ機器は、前記サーバとの無線通信を介する加入者登録の後に前記初期PMSIをプロビジョニングするように構成される、請求項11に記載のユーザ機器。
【請求項１４】
前記プロセッサは、提案されるPMSIを、前記UEにおいて生成される乱数または疑似乱数を含む数から生成し、サーバ公開鍵を使用して、前記生成されたPMSIを暗号化するようにさらに構成され、前記サービングネットワーク上の前記サーバは、対応するサーバ秘密鍵を維持し、
前記トランシーバは、暗号化の後に前記生成されたPMSIを前記サーバに送信し、前記初期PMSIとして前記生成されたPMSIを使用するために前記サーバから肯定応答を受信するようにさらに構成される、請求項13に記載のユーザ機器。
【請求項１５】
前記プロセッサは、
一致があるかどうかを判定するために、前記UEベースの次のPMSIを前記認証要求の一部として受信された前記次のPMSIと比較する
ようにさらに構成される、請求項10に記載のユーザ機器。
【請求項１６】
前記メモリは、次のアタッチメッセージ内での使用のために、前記次のPMSIを記憶するようにさらに構成される、請求項15に記載のユーザ機器。
【請求項１７】
前記プロセッサは、匿名鍵を使用して前記認証要求内の前記次のPMSIを暗号化解除するようにさらに構成され、前記匿名鍵は、前記UEと前記サーバとの間で共有される秘密鍵から導出される、請求項10に記載のユーザ機器。
【請求項１８】
ネットワーク上のサーバとのネットワークアクセスをセットアップするための方法であって、
初期アタッチメッセージからユーザ機器(UE)を識別するために、介在するサービングネットワーク内の1つまたは複数のネットワーク要素を介して前記UEから、国際モバイル加入者識別情報(IMSI)の直接の代替としてプライバシモバイル加入者識別情報(PMSI)を受信するステップと、
前記サーバによって、前記PMSIに基づいて次のPMSIを判定するステップと、
前記サーバから、認証の一部として、前記次のPMSIおよびトラッキングインデックスを含む認証情報を前記サービングネットワークに送信するステップと、
前記PMSIおよび前記トラッキングインデックスから前記UEによって導出されたUEベースの次のPMSIが前記サーバから送信される前記次のPMSIと一致することに応答して生成された肯定応答トークンを用いた、前記サーバから送信される前記次のPMSIに対する肯定応答を前記サービングネットワークを介して前記UEから受信するステップと
を含む方法。
【請求項１９】
前記サーバによって、初期PMSIに基づいてネットワークアクセスのための前記PMSIを判定するステップ
をさらに含む、請求項18に記載の方法。
【請求項２０】
前記サーバにおいて、前記サーバへの前記UEの加入者登録中に前記初期PMSIを受信するステップ
をさらに含む、請求項19に記載の方法。

【請求項２１】
前記UEから、提案される初期PMSIを受信するステップと、
前記サーバによって、前記UEにおいて対応するサーバ公開鍵によって暗号化された前記提案される初期PMSIをサーバ秘密鍵を使用して暗号化解除するステップと、
前記サーバによって、前記UEに関連する前記初期PMSIとして前記提案される初期PMSIを記憶するステップと、
前記UEに、前記初期PMSIとして前記提案される初期PMSIの肯定応答を送信するステップと
をさらに含む、請求項19に記載の方法。
【請求項２２】
前記サーバと前記UEとの間で共有される秘密鍵から匿名鍵を導出するステップと、
前記導出された匿名鍵を使用して前記認証情報内の前記次のPMSIを暗号化するステップと、
前記UEからの後続の初期アタッチメッセージに応答する際の使用のために前記サーバにおいて前記PMSIの代わりに前記次のPMSIを記憶するステップと
をさらに含む、請求項18に記載の方法。
【請求項２３】
判定する前記ステップは、
前記次のPMSIと異なるUEに関連する別の既存のPMSIとの間の衝突を検出するステップと、
前記トラッキングインデックスを増分し、前記次のPMSIおよび前記増分されたトラッキングインデックスに基づいて新しい次のPMSIを判定するステップと
をさらに含む、請求項18に記載の方法。
【請求項２４】
前記サーバがその上にあるホームネットワークとは別々の前記サービングネットワーク上のモビリティ管理エンティティ(MME)から、前記UEの前記IMSIの要求を受信するステップと、
前記要求に応答して、前記UEの前記IMSIの代わりに前記初期アタッチメッセージ内で使用された前記UEの前記PMSIを送るステップと
をさらに含む、請求項18に記載の方法。
【請求項２５】
前記初期アタッチメッセージに含まれる前記PMSIとの一致を1つまたは複数のデータベースから検索するステップと、
一致を突き止めないことに応答して、前記UEにおける更新されたPMSIの生成のために前記UEにおいて維持されるPMSIインデックスを前記UEが変更するための通知を送るステップと
をさらに含む、請求項18に記載の方法。
【請求項２６】
サーバであって、
ユーザ機器(UE)の複数のプライバシモバイル加入者識別情報(PMSI)を記憶するように構成されたデータベースと、
初期アタッチメッセージからUEを識別するために、介在するサービングネットワーク内の1つまたは複数のネットワーク要素を介して前記UEから、国際モバイル加入者識別情報(IMSI)の直接の代替としてプライバシモバイル加入者識別情報(PMSI)を受信するように構成されたトランシーバと、
前記PMSIに基づいて前記UEの次のPMSIを判定するように構成されたプロセッサと
を含み、
前記トランシーバは、認証の一部として、前記次のPMSIおよびトラッキングインデックスを含む認証情報を前記サービングネットワークに送信し、前記PMSIおよび前記トラッキングインデックスから導出されたUEベースの次のPMSIが前記トランシーバによって送信さ

れる前記次のPMSIと一致することに応答して生成された肯定応答トークンを用いた、前記トランシーバによって送信される前記次のPMSIに対する肯定応答を前記サービングネットワークを介して前記UEから受信するようにさらに構成される、サーバ。

【請求項２７】

前記プロセッサは、初期PMSIに基づいてネットワークアクセスのための前記PMSIを判定するようにさらに構成される、請求項26に記載のサーバ。

【請求項２８】

前記トランシーバは、前記サーバへの前記UEの加入者登録中に前記初期PMSIを受信するようにさらに構成される、請求項27に記載のサーバ。

【請求項２９】

前記トランシーバは、前記UEから、提案される初期PMSIを受信するようにさらに構成され、

前記プロセッサは、前記UEにおいて対応するサーバ公開鍵によって暗号化された前記提案される初期PMSIをサーバ秘密鍵を使用して暗号化解除し、前記UEに関連する前記初期PMSIとして前記提案される初期PMSIを記憶するようにさらに構成され、

前記トランシーバは、前記UEに、前記初期PMSIとして前記提案される初期PMSIの肯定応答を送信するようにさらに構成される、請求項27に記載のサーバ。

【請求項３０】

前記プロセッサは、前記サーバと前記UEとの間で共有される秘密鍵から匿名鍵を導出し、前記導出された匿名鍵を使用して前記認証情報内の前記次のPMSIを暗号化するようにさらに構成され、

前記データベースは、前記UEからの後続の初期アタッチメッセージに応答する際の使用のために前記PMSIの代わりに前記次のPMSIを記憶するようにさらに構成される、請求項26に記載のサーバ。

【請求項３１】

前記プロセッサは、前記判定の一部として、

前記次のPMSIと前記データベース内の異なるUEに関連する別の既存のPMSIとの間の衝突を検出し、

前記トラッキングインデックスを増分し、前記次のPMSIおよび前記増分されたトラッキングインデックスに基づいて新しい次のPMSIを判定する

ようにさらに構成される、請求項26に記載のサーバ。

【請求項３２】

前記トランシーバは、

前記サーバがその上にあるホームネットワークとは別々の前記サービングネットワーク上のモビリティ管理エンティティ(MME)から、前記UEの前記IMSIの要求を受信し、

前記要求に応答して、前記UEの前記IMSIの代わりに前記初期アタッチメッセージ内で使用された前記UEの前記PMSIを送る

ようにさらに構成される、請求項26に記載のサーバ。

【請求項３３】

前記プロセッサは、前記初期アタッチメッセージに含まれる前記PMSIとの一致を前記データベースから検索するようにさらに構成され、

前記トランシーバは、一致を突き止めないことに応答して、前記UEにおける更新されたPMSIの生成のために前記UEにおいて維持されるPMSIインデックスを前記UEが変更するための通知を送るようにさらに構成される、請求項26に記載のサーバ。

【請求項３４】

プログラムコードを記録した非一時的なコンピュータ可読媒体であって、前記プログラムコードは、

ユーザ機器(UE)に、初期アタッチメッセージを用いて前記UEを識別するために、国際モバイル加入者識別情報(IMSI)の直接の代替としてプライバシモバイル加入者識別情報(PMSI)をサービングネットワークを介して前記サーバに送らせるためのコードと、

前記UEに、次のPMSIおよびトラッキングインデックスを含む認証要求を前記サーバから受信させるためのコードと、
前記UEに、前記PMSIおよび前記トラッキングインデックスからUEベースの次のPMSIを導出させるためのコードと、
前記UEに、前記UEと前記サーバとの間でPMSI同期の一致があるかどうかを判定するために、前記UEベースの次のPMSIを前記認証要求の一部として受信された前記次のPMSIと比較させるためのコードと、
前記UEに、前記UEベースの次のPMSIと前記サーバから受信する前記次のPMSIとが一致することに応答して、前記サーバから受信する前記次のPMSIに対する肯定応答を生成させるためのコードと、
前記UEに、前記肯定応答を前記サーバに送らせるためのコードと
を含む、非一時的なコンピュータ可読媒体。
【請求項３５】
前記UEに、初期PMSIに基づいてネットワークアクセスのための前記PMSIを判定させるためのコード
をさらに含む、請求項34に記載の非一時的なコンピュータ可読媒体。
【請求項３６】
前記UEに、前記サーバへの前記UEの加入者登録中に前記初期PMSIを受信させるためのコード
をさらに含む、請求項35に記載の非一時的なコンピュータ可読媒体。
【請求項３７】
前記UEに、前記サーバとの無線通信を介する加入者登録の後に前記初期PMSIをプロビジョニングさせるためのコード
をさらに含む、請求項35に記載の非一時的なコンピュータ可読媒体。
【請求項３８】
前記UEに、提案されるPMSIを生成させるためのコードと、
前記UEに、サーバ公開鍵を使用して、前記生成されたPMSIを暗号化させるためのコードであって、前記サーバは、対応するサーバ秘密鍵を維持する、暗号化させるためのコードと、
前記UEに、暗号化の後に前記生成されたPMSIを前記サーバに送らせるためのコードと、
前記UEに、前記初期PMSIとして前記生成されたPMSIを使用するために前記サーバから肯定応答を受信させるためのコードと
をさらに含む、請求項37に記載の非一時的なコンピュータ可読媒体。
【請求項３９】
前記UEに、次のアタッチメッセージ内での使用のために、前記UEにおいて、確認された次のPMSIを記憶させるためのコード
をさらに含む、請求項34に記載の非一時的なコンピュータ可読媒体。
【請求項４０】
前記UEに、匿名鍵を使用して前記認証要求内の前記次のPMSIを暗号化解除させるためのコードであって、前記匿名鍵は、前記UEと前記サーバとの間で共有される秘密鍵から導出される、暗号化解除させるためのコード
をさらに含む、請求項34に記載の非一時的なコンピュータ可読媒体。
【請求項４１】
プログラムコードを記録した非一時的なコンピュータ可読媒体であって、前記プログラムコードは、
サーバに、初期アタッチメッセージからユーザ機器(UE)を識別するために、介在するサービングネットワーク内の1つまたは複数のネットワーク要素を介して前記UEから、国際モバイル加入者識別情報(IMSI)の直接の代替としてプライバシモバイル加入者識別情報(PMSI)を受信させるためのコードと、
前記サーバに、前記PMSIに基づいて次のPMSIを判定させるためのコードと、

前記サーバに、認証の一部として、前記次のPMSIおよびトラッキングインデックスを含む認証情報を前記サービングネットワークに送信させるためのコードと、
前記サーバに、前記PMSIおよび前記トラッキングインデックスから前記UEによって導出されたUEベースの次のPMSIが前記サーバから送信される前記次のPMSIと一致することに応答して生成された肯定応答トークンを用いた、前記サーバから送信される前記次のPMSIに対する肯定応答を前記サービングネットワークを介して前記UEから受信させるためのコードと
を含む、非一時的なコンピュータ可読媒体。
【請求項４２】
前記サーバに、初期PMSIに基づいてネットワークアクセスのための前記PMSIを判定させるためのコード
をさらに含む、請求項41に記載の非一時的なコンピュータ可読媒体。
【請求項４３】
前記サーバに、前記サーバへの前記UEの加入者登録中に前記初期PMSIを受信させるためのコード
をさらに含む、請求項42に記載の非一時的なコンピュータ可読媒体。
【請求項４４】
前記サーバに、前記UEから、提案される初期PMSIを受信させるためのコードと、
前記サーバに、前記UEにおいて対応するサーバ公開鍵によって暗号化された前記提案される初期PMSIをサーバ秘密鍵を使用して暗号化解除させるためのコードと、
前記サーバに、前記初期PMSIとして前記提案される初期PMSIの肯定応答を前記UEに送信させるためのコードと
をさらに含む、請求項42に記載の非一時的なコンピュータ可読媒体。
【請求項４５】
前記サーバに、前記サーバと前記UEとの間で共有される秘密鍵から匿名鍵を導出させるためのコードと、
前記サーバに、前記導出された匿名鍵を使用して前記認証情報内の前記次のPMSIを暗号化させるためのコードと、
前記サーバに、前記UEからの後続の初期アタッチメッセージに応答する際の使用のために前記サーバにおいて前記PMSIの代わりに前記次のPMSIを記憶させるためのコードと
をさらに含む、請求項41に記載の非一時的なコンピュータ可読媒体。
【請求項４６】
前記サーバに、前記次のPMSIを判定させるための前記コードが、
前記サーバに、前記次のPMSIと異なるUEに関連する別の既存のPMSIとの間の衝突を検出させるためのコードと、
前記サーバに、前記トラッキングインデックスを増分させ、前記次のPMSIおよび前記増分されたトラッキングインデックスに基づいて新しい次のPMSIを判定させるためのコードと
をさらに含む、請求項41に記載の非一時的なコンピュータ可読媒体。
【請求項４７】
前記サーバに、前記サーバがその上にあるホームネットワークとは別々の前記サービングネットワーク上のモビリティ管理エンティティ(MME)から、前記UEの前記IMSIの要求を受信させるためのコードと、
前記サーバに、前記要求に応答して、前記UEの前記IMSIの代わりに前記初期アタッチメッセージ内で使用された前記UEの前記PMSIを送らせるためのコードと
をさらに含む、請求項41に記載の非一時的なコンピュータ可読媒体。
【請求項４８】
前記サーバに、前記初期アタッチメッセージに含まれる前記PMSIとの一致を1つまたは複数のデータベースから検索させるためのコードと、
前記サーバに、一致を突き止めないことに応答して、前記UEにおける更新されたPMSIの

生成のために前記UEにおいて維持されるPMSIインデックスを前記UEが変更するための通知を送らせるためのコードと
をさらに含む、請求項41に記載の非一時的なコンピュータ可読媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
本願は、2015年3月5日に出願した米国特許仮出願第62/128724号、名称「Identity Privacy in Wireless Networks」の利益を主張する、2015年7月24日に出願した米国特許非仮出願第14/808862号の利益を主張するものであり、これらの特許出願の両方が、参照によってその全体が本明細書に組み込まれている。
【０００２】
本願は、ワイヤレス通信システムに関し、より具体的には、ワイヤレス通信中に加入者識別情報のプライバシを高めることに関する。
【背景技術】
【０００３】
ネットワークからサービスを受信するために、未知のユーザ機器(UE)は、ネットワークに登録し、または他の形でネットワークに知られるようになる必要がある。これは、ネットワークアタッチ手順を使用して達成される。アタッチ手順の一部として、UEは、その国際モバイル加入者識別情報(IMSI)を送る。IMSIは、UEが通信する(またはその代わりに通信する)すべてのネットワーク上でUEが使用する一意識別である。UEは、アタッチ要求とともにIMSIを送り、これらは、モビリティ管理エンティティ(MME)において受信される。
【０００４】
盗聴者および追跡からIMSIを保護することを試みて、一時モバイル加入者識別情報(TMSI)が、UEを最初に認証した後に使用され得る。TMSIは、特定のエリア区域にローカルであり、したがって、各エリア内で再割当されなければならない。さらに、TMSIは、UEが初期認証のためにIMSIを提供した後にまず割り当てられる(その結果、TMSIの割当は、UEの実際の識別情報に関連付けられ得るようになる)。時々、グローバル一意一時UE識別情報(GUTI)が、初期アタッチ要求内でIMSIの代わりに提供される。UEがIMSIの代わりにGUTIを送る場合に、MMEは、そのUEと以前に相互作用した可能性がある他のネットワーク要素に識別を要求する。UEが他のネットワーク要素に知られている場合には、これらの他のネットワーク要素は、IMSIを応答する。UEが知られていない場合には、MMEは、識別のためにIMSIを提供するようにUEに要求し、このIMSIは、その後、ロケーションレジスタを用いる更新手順に使用される。
【０００５】
上の手法のいずれの下であっても、IMSIは、まだ脆弱である。IMSIは、初期アタッチ要求内に含まれるか、認証されるために後に提供されなければならないかのいずれかである。したがって、IMSIは、無線トラフィックを介して受動的に監視され、ユーザ識別情報を判定するのに使用され得る。しばしば、アタッチ要求内のIMSIは、平文であり、IMSIを、監視に対してさらにより脆弱にする。UEがIMSIを送らないシナリオにおいてさえ、MMEは、それでも、他のネットワーク要素から実際のIMSIを入手し、複数の異なるネットワーク要素が、実際のIMSIを記憶する可能性がある(たとえば、MME、サービングゲートウェイ(S-GW)、および/またはPDNゲートウェイ(P-GW))。これは、IMSIを脆弱でサービングネットワークの信頼性に依存するままにする。
【発明の概要】
【課題を解決するための手段】
【０００６】
本開示の一態様によれば、ユーザ機器(UE)によるネットワークアクセスのための方法は、ネットワーク上のサーバに対して初期アタッチメッセージを用いてUEを識別するために、国際モバイル加入者識別情報(IMSI)ではなくプライバシモバイル加入者識別情報(PMSI)

をUEから送るステップと、次のPMSIを含む認証要求をサーバから受信するステップであって、次のPMSIは、PMSIから導出される異なる値である、受信するステップと、次のPMSIの受信の肯定応答をUEからサーバに送るステップとを含む。

【０００７】

本開示の追加の態様において、ユーザ機器は、プライバシモバイル加入者識別情報(PMSI)を記憶するように構成されたメモリと、ネットワーク上のサーバに対して初期アタッチメッセージを用いてUEを識別するために、国際モバイル加入者識別情報(IMSI)ではなくPMSIを送り、次のPMSIを含む認証要求をサーバから受信し、次のPMSIは、PMSIから導出される異なる値であるように構成されたトランシーバと、受信の肯定応答を生成するように構成されたプロセッサであって、トランシーバは、受信の肯定応答をサーバに送るようにさらに構成される、プロセッサとを含む。

【０００８】

本開示の追加の態様において、プログラムコードをその上に記録されたコンピュータ可読媒体は、ユーザ機器(UE)に、ネットワーク上のサーバに対して初期アタッチメッセージを用いてUEを識別するために、国際モバイル加入者識別情報(IMSI)ではなくプライバシモバイル加入者識別情報(PMSI)を送らせるためのコードと、UEに、次のPMSIを含む認証要求をサーバから受信させるためのコードであって、次のPMSIは、PMSIから導出される異なる値である、受信させるためのコードと、UEに、次のPMSIの受信の肯定応答をサーバに送らせるためのコードとを含む。

【０００９】

本開示の追加の態様において、ネットワーク上のサーバとのネットワークアクセスをセットアップするための方法は、初期アタッチメッセージからユーザ機器(UE)を識別するために、介在するサービングネットワーク内の1つまたは複数のネットワーク要素を介してUEから、国際モバイル加入者識別情報(IMSI)の代わりにプライバシモバイル加入者識別情報(PMSI)を受信するステップと、サーバによって、PMSIに基づいて次のPMSIを判定するステップと、サーバから、次のPMSIを含む認証要求を送信するステップと、次のPMSIの確認を含む受信の肯定応答をUEから受信するステップとを含む。

【００１０】

本開示の追加の態様において、サーバは、ユーザ機器(UE)の複数のプライバシモバイル加入者識別情報(PMSI)を記憶するように構成されたデータベースと、初期アタッチメッセージからUEを識別するために、介在するサービングネットワーク内の1つまたは複数のネットワーク要素を介してUEから、国際モバイル加入者識別情報(IMSI)の代わりにプライバシモバイル加入者識別情報(PMSI)を受信するように構成されたトランシーバと、PMSIに基づいてUEの次のPMSIを判定するように構成されたプロセッサとを含み、トランシーバは、次のPMSIを含む認証要求を送信し、次のPMSIの確認を含む受信の肯定応答を受信するようにさらに構成される。

【００１１】

本開示の追加の態様において、プログラムコードをその上に記録されたコンピュータ可読媒体は、サーバに、初期アタッチメッセージからユーザ機器(UE)を識別するために、介在するサービングネットワーク内の1つまたは複数のネットワーク要素を介してUEから、国際モバイル加入者識別情報(IMSI)の代わりにプライバシモバイル加入者識別情報(PMSI)を受信させるためのコードと、サーバに、PMSIに基づいて次のPMSIを判定させるためのコードと、サーバに、次のPMSIを含む認証要求を送信させるためのコードと、サーバに、次のPMSIの確認を含む受信の肯定応答をUEから受信させるためのコードとを含む。

【図面の簡単な説明】

【００１２】

【図１】本開示の様々な態様による、ワイヤレス通信ネットワークを示す図である。

【図２】本開示の実施形態による、例示的なUEを示すブロック図である。

【図３】本開示の実施形態による、例示的なサーバを示すブロック図である。

【図４】本開示の様々な態様による、例示的な送信器システムを示すブロック図である。

【図５】本開示の様々な態様による、ワイヤレスネットワーク内で識別情報プライバシをサポートするための、UEとサービングネットワークとホームネットワークとの間のいくつかのシグナリング態様を示すプロトコル図である。
【図６Ａ】本開示の様々な態様による、アタッチプロセスを開始するUEのための例示的な方法を示す流れ図である。
【図６Ｂ】本開示の様々な態様による、アタッチプロセス内で働くサーバのための例示的な方法を示す流れ図である。
【図７Ａ】本開示の様々な態様による、UEに関するPMSI初期化のための例示的な方法を示す流れ図である。
【図７Ｂ】本開示の様々な態様による、サーバに関するPMSI初期化のための例示的な方法を示す流れ図である。
【発明を実施するための形態】
【００１３】
添付図面に関連して下で示される詳細な説明は、様々な構成の説明として意図され、本明細書で説明される概念がその中で実践され得る唯一の構成を表すことは意図されていない。詳細な説明は、様々な概念の完全な理解を提供するために特定の詳細を含む。しかしながら、これらの具体的な詳細なしにこれらの概念が実践され得ることは当業者には明らかであろう。いくつかの場合に、そのような概念を不明瞭にすることを回避するために、周知の構造および構成要素は、ブロック図の形において示される。
【００１４】
本明細書で説明される技法は、CDMA、TDMA、FDMA、OFDMA、SC-FDMA、および他のネットワークなどの様々なワイヤレス通信ネットワークのために使用され得る。「ネットワーク」および「システム」という用語は、しばしば交換可能に使用される。CDMAネットワークは、Universal Terrestrial Radio Access(UTRA)、cdma2000、その他などの無線技術を実施することができる。UTRAは、Wideband CDMA(WCDMA（登録商標）)およびCDMAの他の変形を含む。cdma2000は、IS-2000規格、IS-95規格、およびIS-856規格を包含する。TDMAネットワークは、Global System for Mobile Communications(GSM（登録商標）)などの無線技術を実施することができる。OFDMAネットワークは、Evolved UTRA(E-UTRA)、Ultra Mobile Broadband(UMB)、IEEE 802.11(Wi-Fi)、IEEE 802.16(WiMAX)、IEEE 802.20、Flash-OFDMA、その他などの無線技術を実施することができる。UTRAおよびE-UTRAは、Universal Mobile Telecommunication System(UMTS)の一部である。3GPP Long Term Evolution(LTE)およびLTE-Advanced(LTE-A)は、E-UTRAを使用する、UMTSの新しいリリースである。UTRA、E-UTRA、UMTS、LTE、LTE-A、およびGSM（登録商標）は、「3rd Generation Partnership Project」(3GPP)という名称の組織からの文書内に記載されている。CDMA2000およびUMBは、「3rd Generation Partnership Project 2」(3GPP2)という名称の組織からの文書内に記載されている。本明細書で説明される技法は、上で言及されたワイヤレスネットワークおよび無線技術ならびに次世代(たとえば、第5世代(5G))ネットワークなどの他のワイヤレスネットワークおよび無線技術のために使用され得る。本開示の実施形態は、上に列挙されたネットワークおよび/またはこれから開発されるネットワークのうちの任意の1つまたは複数の上で使用され得る任意のタイプの変調方式を対象とする。
【００１５】
本開示の実施形態は、その代わりにプライバシモバイル加入者識別情報(PMSI)を提供することによって、ユーザ機器の国際モバイル加入者識別情報を保護するシステムおよび技法を導入する。一実施形態において、UEは、サービングネットワークに対してアタッチ要求を開始する。IMSIまたはサービングネットワーク上のある要素がそれでもIMSIにアクセスするのに使用できる関連する情報を提供するのではなく、UEは、アタッチ要求とともにPMSIを提供する。次いで、IMSIがUEとサーバとの間で要求されないように、PMSIが、プロセス全体を通じて使用される。一実施形態において、各PMSI(各UE用と特定のUEの異なる反復用との両方)は、お互いから一意である。これは、盗聴およびサービングネットワーク内のすべての潜在的に悪意のある要素からIMSIを保護する。この例を続けると、サービ

ングネットワークの要素は、UEのホームネットワーク上のサーバ(たとえば、ホーム加入者サーバ(HSS))に、認証情報要求の一部としてPMSIを渡す。HSSは、対応するUEを識別するためにPMSIを突き止め、ネットワーク要素に認証情報要求を供給する。応答の一部として、HSSは、UEが後続のアタッチ要求のために使用する次のPMSIを導出し、PMSI衝突をチェックし、UEに渡すためにサービングネットワーク内のネットワーク要素に次のPMSIおよびPMSIトラッキングインデックスを供給することもする。

【００１６】

次のPMSIおよびPMSIトラッキングインデックスは、暗号化された形において供給され得る。暗号化された形において、次のPMSIおよびPMSIトラッキングインデックスは、サービングネットワーク内の潜在的に悪意のあるネットワーク要素および盗聴から保護されたままになる。UEは、暗号化された次のPMSIおよびPMSIトラッキングインデックスを受信し、これらを暗号化解除することができる。UEは、UEおよびHSSが同期化されることを確認するために、次のPMSIのそれ自体のコピーを導出する。次のPMSIがUEとHSSとの間で同期化されることを確認した後に、UEは、肯定応答トークンをサーバに送る。次いで、UEおよびサーバは、それぞれ、現在のPMSI値および次のPMSI値のローカルコピーを更新する。HSSは、UEのPMSIのすべての反復を記憶する必要がない。その代わりに、HSSは、初期PMSI値および所望のPMSIトラッキングインデックス値に基づいてPMSIの任意の反復に達することができる。

【００１７】

さらなる実施形態において、初期PMSIは、UEとHSSとの間で合意され得る。一実施形態において、初期PMSIがUEのSIMカードにプロビジョニングされ、HSSに登録されるように、初期PMSIは、加入者登録時に合意される。別の実施形態において、UEは、加入者登録時にPMSIをプロビジョニングされるのではなく、HSSへの無線登録を開始する。UEは、初期PMSI値を生成し、HSSの公開鍵(または、UEとHSSとの間の他の共有される鍵)を使用して初期PMSI値を暗号化した後に、提案される初期PMSIをHSSに送ることができる。HSSは、対応する秘密鍵を用いてUEからの初期PMSIを暗号化解除し、PMSIが、HSSに登録された他の既存のPMSI値と衝突するかどうかを判定することができる。衝突がないことを確認した時に、HSSは、UEに対して初期PMSIを肯定応答し、UEが後にその第1のアタッチ要求を開始する時の使用のためにその初期PMSIを記憶することができる。

【００１８】

図1は、本開示の様々な態様による、ワイヤレス通信ネットワーク100を示す。ワイヤレス通信ネットワーク100は、複数のUE 102ならびに複数の基地局104を含むことができる。例示および説明の単純さのみのために、単一のUE 102および単一の基地局104が図1内に示されている。基地局104は、evolved Node B(eNodeB)を含むことができる。基地局は、ベーストランシーバ基地局またはアクセスポイントと呼ばれる場合もある。

【００１９】

基地局104は、図示のようにUE 102と通信する。UE 102は、アップリンクおよびダウンリンクを介して基地局104と通信することができる。ダウンリンク(または順方向リンク)は、基地局104からUE 102への通信リンクを指す。アップリンク(または逆方向リンク)は、UE 102から基地局104への通信リンクを指す。

【００２０】

UE 102は、ワイヤレス通信ネットワーク100全体に分散され得、UE 102は、静止またはモバイルとすることができる。UE 102は、端末、移動局、加入者ユニットなどと呼ばれる場合もある。UE 102は、セルラー電話、スマートフォン、携帯情報端末、ワイヤレスモデム、ラップトップコンピュータ、タブレットコンピュータなどとすることができる。ワイヤレス通信ネットワーク100は、本開示の様々な態様が適用されるネットワークの一例である。

【００２１】

やはり図1内に示されているのが、モビリティ管理エンティティ(MME)106である。MME 106は、加入者(たとえば、UE 102)に関する制御プレーン機能およびセッション管理の責任

を負うものとすることができる。たとえば、MME 106は、モビリティセッション管理ならびに他のネットワークへのハンドオーバ、ローミング、および加入者認証のサポートを提供することができる。MME 106は、少数の例を挙げると、UE 102の初期アタッチ中のS-GWの選択、非アクセス層(NAS)シグナリング、NASシグナリングセキュリティ、P-GW選択、専用ベアラ確立を含むベアラ管理機能、シグナリングトラフィックの合法的傍受(lawful interception)、および他の機能を支援することができる。MME 106および基地局104は、同一のサービングネットワーク108(たとえば、発展型パケットコア(EPC)の一部)内に存在することができる。理解されるように、サービングネットワーク108は、本開示の諸態様の議論の単純さのために図1内に示されていない多数の他のネットワーク要素を含む。

【００２２】

MME 106は、ホームネットワーク114内のサーバ112と通信する。一実施形態において、サーバ112は、とりわけ、ユーザ加入者情報を維持する1つまたは複数のデータベースを記憶し、更新する責任を負うホームロケーションレジスタ(HLR)を維持するホーム加入者サーバ(HSS)である。とりわけ、ホームネットワーク114内のサーバ112は、UE 102のIMSI(ユーザ識別/アドレッシング)のコピーを有する。サーバ112は、サービスサブスクリプション状態を識別するユーザプロファイル情報および/またはサービス品質(QoS)情報(たとえば、最大の許容されるビットレート、許容されるトラフィッククラスなど)をも維持することができる。サーバ112は、ユーザ識別情報鍵からのセキュリティ情報生成の管理およびHLR(および他のネットワークエンティティ)へのセキュリティ情報のプロビジョニングなど、認証機能をも含むことができる。セキュリティ情報を用いて、ネットワーク-UE認証が実行され得る。例示および説明の単純さのために、1つのサーバ112が図1内に示されている。ホームネットワーク114は、複数のHSSを含むことができる。たとえば、HSSの個数は、モバイル加入者の人数、機器容量、およびネットワーク編成に依存することができる。MME 106は、ネットワーク110を介してサーバ112と通信することができ、ネットワーク110は、理解されるように、様々なタイプの直接接続または間接接続とすることができる。

【００２３】

ワイヤレスネットワーク内で識別情報プライバシをサポートするためのUEとサービングネットワークとホームネットワーク(および関連するサーバ)との間のいくつかのシグナリング態様を示すプロトコル図を含む後続の図に関して下でより詳細に説明されるように、UE 102は、IMSIの除外に対してプライバシモバイル加入者識別情報(PMSI)を使用して、サービングネットワーク108およびホームネットワーク114と通信することができる。PMSIは、UE 102に特に関連付けられ、UE 102とサーバ112との両方によって維持される一意の数とすることができる。本開示の実施形態において、PMSIは、UE 102とサーバ112との両方によって合意される初期PMSIを含むことができる。UE 102がアタッチ要求を開始する各後続の時に、新しいPMSI値が要求の一部として供給されるように、UE 102のPMSIの特定の値は、1回使用され得る。UE 102およびサーバ112は、合意された初期PMSIおよびインデックスだけを記憶することができる。その結果、任意のPMSI値は、その後に初期PMSIと、UE 102とサーバ112との両方において特定のPMSIに達するために何回の導出反復が実行されなければならないのか(たとえば、UE 102およびサーバ112が、所与のセッションに使用される特定のPMSIに関して合意したままになるように)を記述するための特定のインデックス値の共有される知識とに基づいて導出され得る。

【００２４】

一例において、UE 102は、基地局104へのその初期アタッチ要求の一部として、IMSIではなくそのPMSIを送ることができる。次いで、基地局104は、UEのPMSIとともにアタッチ要求をMME 106に転送する。MME 106は、ホームネットワーク114内のサーバ112への認証情報要求内にPMSIを含める。サーバ112は、MME 106からの初期アタッチ要求/認証情報要求内で供給されたPMSIに基づいてUE 102を識別することができ、その結果、IMSIがサービングネットワーク108に供給される必要がなくなる。サーバ112からUE 102に戻る通信も、IMSIではなくPMSIに基づく/を含むはずである。通信経路内のこれらのステージのすべてに

おけるIMSIではなくPMSIの使用は、UE 102と基地局104との間での無線盗聴の危険性を低減し、IMSIではなくPMSIが記憶されるので、サービングネットワーク108内の任意のネットワーク要素からのUE 102のIMSIの入手可能性を除去する。

【００２５】

図2は、本開示の実施形態による、例示的なUE 102のブロック図である。UE 102は、上で説明された多数の構成のうちの任意の1つを有することができる。UE 102は、プロセッサ202、メモリ204、PMSIモジュール208、トランシーバ210、およびアンテナ216を含むことができる。これらの要素は、たとえば1つまたは複数のバスを介してお互いと直接的または間接的に通信していることができる。

【００２６】

プロセッサ202は、中央処理装置(CPU)、デジタル信号プロセッサ(DSP)、特定用途向け集積回路(ASIC)、コントローラ、フィールドプログラマブルゲートアレイ(FPGA)デバイス、別のハードウェアデバイス、ファームウェアデバイス、または図1に関して上で導入され、下でより詳細に議論される、UE 102を参照して本明細書で説明される動作を実行するように構成されたその任意の組合せを含むことができる。プロセッサ202は、コンピューティングデバイスの組合せ、たとえば、DSPとマイクロプロセッサとの組合せ、複数のマイクロプロセッサ、DSPコアに関連する1つまたは複数のマイクロプロセッサ、または任意の他のそのような構成としても実施され得る。

【００２７】

メモリ204は、キャッシュメモリ(たとえば、プロセッサ202のキャッシュメモリ)、ランダムアクセスメモリ(RAM)、磁気抵抗RAM(MRAM)、読取専用メモリ(ROM)、プログラマブル読取専用メモリ(PROM)、消去可能プログラマブル読取専用メモリ(EPROM)、電気的消去可能プログラマブル読取専用メモリ(EEPROM)、フラッシュメモリ、ソリッドステートメモリデバイス、ハードディスクドライブ、他の形の揮発性メモリおよび不揮発性メモリ、または異なるタイプのメモリの組合せを含むことができる。一実施形態において、メモリ204は、非一時的コンピュータ可読媒体を含む。メモリ204は、命令206を記憶することができる。命令206は、プロセッサ202によって実行された時に、プロセッサ202に、本開示の実施形態に関連してUE 102を参照して本明細書で説明される動作を実行させる命令を含むことができる。命令206は、コードと呼ばれる場合もある。「命令」および「コード」という用語は、任意のタイプのコンピュータ可読ステートメントを含むように、広く解釈されるべきである。たとえば、「命令」および「コード」という用語は、1つまたは複数のプログラム、ルーチン、サブルーチン、関数、手続きなどを指すことができる。「命令」および「コード」は、単一のコンピュータ可読ステートメント、または多数のコンピュータ可読ステートメントを含むことができる。

【００２８】

PMSIモジュール208は、本開示の様々な態様のために使用され得る。たとえば、PMSIモジュール208は、特定のUE 102のPMSIの初期プロビジョニングに用いられ得る。一実施形態において、PMSIは、UE 102のIMSIと同時にUE 102にプロビジョニングされ得る。たとえば、いくつかの場合に、PMSIは、図1内のサーバ112など、HSSへの加入者登録中にIMSIと一緒にプロビジョニングされる。このプロビジョニングは、製造の時にUE 102上のSIMカード内で行われ得る。別の実施形態において、IMSIは、PMSIがUE 102とサーバ112との間で合意される前にプロビジョニングされ得る。たとえば、UE 102およびサーバ112は、IMSIが既にUE 102にプロビジョニングされた後に、無線で第1の(初期)PMSIに合意することができる。PMSIが無線で合意される時に、UE 102は、提案される初期PMSI(下で図7Aに関してより詳細に議論される)を生成し、サーバ112によって供給された公開鍵を用いて、提案される初期PMSIを暗号化することができる。この形において、UE 102によって送信される提案される初期PMSIは、盗聴と、サービングネットワーク108内の潜在的に危険にさらされたネットワーク要素とから保護され得る。サーバ112は、対応する秘密鍵を維持し、提案される初期PMSIを暗号化解除することができる。サーバ112は、サーバ112によって維持されまたは他の形でホームネットワーク114内にある任意の他のUEのPMSIとの衝突がない

ことを検証するために、1つまたは複数のデータベースに対して提案される初期PMSIをチェックすることができる。

【００２９】

PMSIモジュール208は、PMSI肯定応答にさらに用いられ得る。上で述べたように、特定のPMSI値(初期PMSIに基づく)は、異なるPMSI値が後続のアタッチ要求のために提供されるように、所定の個数のアタッチ要求(たとえば、1つ、2つ、3つ、またはより多数)のためにのみ使用され得る。UE 102からのアタッチ要求に応答して、サーバ112は、「次のPMSI」すなわち後続セッション内で使用されるべき次のPMSI値を生成し、初期アタッチ要求に応答する認証要求の一部として次のPMSIをUE 102と共有することができる。UE 102のPMSIモジュール208は、記憶された初期PMSIおよびインクリメントされたインデックス(以下でさらに説明する)に基づいてそれ自体の次のPMSI値を計算し、ローカルな計算された次のPMSIをサーバ112から受信された次のPMSIと比較することができる。一致がある場合には、PMSIモジュール208は、UE 102に、サーバ112に次のPMSIを肯定応答する応答を生成させることができる。一致がない場合には、PMSIモジュール208は、再計算の後に値が一致するように、次のPMSIとともにサーバ112から受信されたインデックスを用いてそのローカルインデックスを更新することができる。

【００３０】

トランシーバ210は、モデムサブシステム212および無線周波数(RF)ユニット214を含むことができる。トランシーバ210は、基地局104などの他のデバイスと両方向に通信するように構成される。モデムサブシステム212は、変調およびコーディング方式(MCS)、たとえば、低密度パリティ検査(LDPC)コーディング方式、ターボコーディング方式、畳み込みコーディング方式などに従って、PMSIモジュール208からのデータを変調し、かつ/または符号化するように構成され得る。RFユニット214は、(アウトバウンド送信における)モデムサブシステム212からの変調された/符号化されたデータまたは基地局104などの別のソースから発する送信の変調された/符号化されたデータを処理する(たとえば、アナログ-デジタル変換またはデジタル-アナログ変換を実行するなど)ように構成され得る。トランシーバ210内に一緒に一体化されるものとして図示されているが、モデムサブシステム212およびRFユニット214は、UE 102が他のデバイスと通信することを可能にするためにUE 102において一緒に結合された別々のデバイスとすることができる。

【００３１】

RFユニット214は、1つまたは複数の他のデバイスへの送信のために、アンテナ216に変調されたデータおよび/または処理されたデータ、たとえばデータパケット(または、より一般的に、1つまたは複数のデータパケットおよびPMSI値を含む他の情報を含むことのできるデータメッセージ)を供給することができる。これは、たとえば、本開示の実施形態による、基地局104へのデータメッセージの送信を含むことができる。アンテナ216は、基地局104から送信されたデータメッセージをさらに受信し、トランシーバ210における処理および/または復調のために受信されたデータメッセージを供給することができる。図2は、アンテナ216を単一のアンテナとして図示するが、アンテナ216は、複数の送信リンクを維持するために、同様のまたは異なる設計の複数のアンテナを含むことができる。

【００３２】

図3は、本開示の実施形態による、例示的なサーバ112のブロック図である。サーバ112は、プロセッサ302、メモリ304、PMSIモジュール308、データベース310、およびトランシーバ312を含むことができる。これらの要素は、たとえば1つまたは複数のバスを介して互いに直接的または間接的に通信中であり得る。上で図1に関して述べたように、サーバ112は、2つの例だけを挙げるとホームロケーションレジスタおよび認証機能性を提供するHSSとすることができる。

【００３３】

プロセッサ302は、CPU、DSP、ASIC、コントローラ、FPGAデバイス、別のハードウェアデバイス、ファームウェアデバイス、または上で図1内で導入されたサーバ112を参照して本明細書で説明される動作を実行するように構成されたその任意の組合せを含むことがで

きる。プロセッサ302は、コンピューティングデバイスの組合せ、たとえば、DSPとマイクロプロセッサとの組合せ、複数のマイクロプロセッサ、DSPコアに関連する1つまたは複数のマイクロプロセッサ、または任意の他のそのような構成としても実施され得る。

【００３４】

メモリ304は、キャッシュメモリ(たとえば、プロセッサ302のキャッシュメモリ)、RAM、MRAM、ROM、PROM、EPROM、EEPROM、フラッシュメモリ、ソリッドステートメモリデバイス、1つまたは複数のハードディスクドライブ、他の形の揮発性メモリおよび不揮発性メモリ、または異なるタイプのメモリの組合せを含むことができる。一実施形態において、メモリ304は、非一時的コンピュータ可読媒体を含む。メモリ304は、命令306を記憶することができる。命令306は、プロセッサ302によって実行された時に、プロセッサ302に、本開示の実施形態に関連してサーバ112を参照して本明細書で説明される動作を実行させる命令を含むことができる。命令306は、コードと呼ばれる場合もあり、コードは、上で図2に関して議論したように、任意のタイプのコンピュータ可読ステートメントを含むように、広く解釈され得る。

【００３５】

PMSIモジュール308は、本開示の様々な態様のために使用され得る。たとえば、PMSIモジュール308は、特定のUE 102のPMSIの初期プロビジョニングに用いられ得る。一実施形態において、PMSIは、たとえば加入者登録中に、UE 102のIMSIと同時にプロビジョニングされ、データベース310内に記憶され得る。別の実施形態において、IMSIは、サーバ112とUE 102との間でPMSIが合意される前にプロビジョニングされ得る。たとえば、サーバ112は、IMSIが既にUE 102にプロビジョニングされた後に、UE 102からの無線で第1の(初期)PMSIに合意することができる。無線で合意される時に、サーバ112は、UE 102によって生成され、これから受信された提案される初期PMSI(下で図7Bに関してより詳細に議論される)を受信することができる。提案される初期PMSIは、サーバ112によってUE 102に供給された公開鍵を用いて暗号化されている場合がある。その結果、サーバ112は、対応する秘密鍵を使用して、提案される初期PMSIを暗号化解除することができる。この形において、PMSIは、盗聴と、サービングネットワーク108内の潜在的に危険にさらされたネットワーク要素とから保護され得る。サーバ112は、サーバ112によって維持されまたは他の形でホームネットワーク114内にある任意の他のUEのPMSIとの衝突がないことを検証するために、データベース310内のPMSI値に対して提案される初期PMSIをチェックすることができる。

【００３６】

PMSIモジュール308は、UE 102との初期アタッチ手順にさらに用いられ得る。サーバ112は、初期アタッチ要求とともに供給されたPMSIをUEから受信し、そのPMSIを、データベース310内に記憶されたPMSI値に対してチェックすることができる。UE 102からのアタッチ要求に応答して、サーバ112は、次のPMSIを生成し、初期アタッチ要求に応答する認証要求応答の一部として次のPMSIをUE 102に送信することができる。UE 102からの次のPMSIを肯定応答する応答の受信に応答して、PMSIモジュール308は、データベース310内に記憶されたPMSI値を更新する。たとえば、現在のPMSI値は、前のPMSI値になり、次のPMSI値は、UE 102からの後続のアタッチ要求などの後続の相互作用に利用される現在のPMSI値になる。

【００３７】

議論において、4つのPMSI値すなわち、(1)UE 102およびサーバ112が後続のPMSI値を導出するのに使用する、初期の合意されたPMSI値である初期PMSI、(2)現在のアタッチ要求手順内で使用されるPMSI値である現在のPMSI(たとえば、UE 102が初期アタッチ要求を初めて送る時に、現在のPMSIは、初期PMSIと等しいものとすることができるが、他の実施形態において、PMSIは、1回または複数回反復され得、その結果、初期PMSIは、初期アタッチ要求中であってもよりセキュアに保たれるようになる)、(3)現在のPMSIに先行するPMSIである前のPMSIまたは以前のPMSI(たとえば、前のアタッチ要求内で使用されたPMSIおよび/または現在のPMSIに達するのに使用されたPMSI)、および(4)現在のPMSIに続くPMSIである次のPMSI(たとえば、UE 102が任意の所与のサービングネットワーク108とともに開始

する次のアタッチ手順のためにPMSIが何になるべきかに関する合意に関してUE 102とサーバ112との両方によって導出されるPMSI)が、本明細書で参照される。

【００３８】

データベース310は、サーバ112、たとえば上で図1に関して言及したHLRによって維持される1つまたは複数のデータベースを含むことができる。データベース310は、ユーザ識別およびアドレッシング(たとえば、加入者のすべてまたはサブセットの、IMSI、PMSI(初期PMSI、現在のPMSI、以前のPMSI、および/または次のPMSIを含む)、PMSIトラッキングインデックス、および携帯電話番号を含む)、プロファイル情報(たとえば、サービスサブスクリプション状態)、ならびに各加入者に関連するセキュリティ情報(たとえば、セキュリティ鍵)などの加入者情報を追跡することができる。

【００３９】

トランシーバ312は、サーバ112が、ホームネットワーク114またはサービングネットワーク108内の他のネットワーク要素などの外部ソースからデータを送信し、受信するために通信することを可能にする。トランシーバ312は、ワイヤレス通信および/または有線通信を使用可能にすることができる。トランシーバ312は、認識されるように、たとえば、イーサネット（登録商標）接続、WiFi接続、または他のタイプのモデムおよび/もしくはRFサブシステムを含むことができる。

【００４０】

図4は、本開示のある種の態様による、MIMOシステム400における、例示的な送信器システム410(たとえば、基地局104)および受信器システム450(たとえば、UE 102)を示すブロック図である。送信器システム410において、複数のデータストリームのトラフィックデータが、データソース412から送信(TX)データプロセッサ414に供給される。トラフィックデータは、本開示の態様による1つまたは複数のMMEエンティティからの認証要求を含む、すべての形のトラフィックを含むことができる。

【００４１】

ダウンリンク送信において、たとえば、各データストリームは、それぞれの送信アンテナを介して送信される。TXデータプロセッサ414は、コーディングされたデータを提供するために、各データストリームのために選択された特定のコーディング方式に基づいて、そのデータストリームのトラフィックデータをフォーマットし、コーディングし、インターリーブする。

【００４２】

各データストリームのコーディングされたデータは、OFDM技法を使用して、パイロットデータと多重化され得る。パイロットデータ、たとえばパイロットシーケンスは、通常、既知の形において処理される既知のデータパターンであり、チャネル応答または他のチャネルパラメータを推定するために受信器システムにおいて使用され得る。パイロットデータは、パイロットシンボルにフォーマットされる場合がある。OFDMシンボル内のパイロットシンボルの個数およびパイロットシンボルの配置は、プロセッサ430によって実行される命令によって決定され得る。

【００４３】

次いで、各データストリームの多重化されたパイロットおよびコーディングされたデータは、変調シンボルを提供するために、そのデータストリームのために選択された特定の変調方式(たとえば、BPSK、QSPK、M-PSK、またはM-QAM)に基づいて変調される(すなわち、シンボルマッピングされる)。各データストリームのデータレート、コーディング、および変調は、プロセッサ430によって実行される命令によって決定され得る。各フレーム内のパイロットシンボルの個数およびパイロットシンボルの配置も、たとえば図2または図3に関して上で説明したように、プロセッサ430によって実行される命令によって決定され得る。送信器システム410は、たとえば図2または図3に関して上で説明したように、メモリ432をさらに含む。

【００４４】

次いで、すべてのデータストリームの変調シンボルが、TX MIMOプロセッサ420に供給さ

れ、TX MIMOプロセッサ420は、変調シンボルをさらに処理することができる(たとえば、OFDMに関して)。次いで、TX MIMOプロセッサ420は、N_T個の変調シンボルストリームをN_T個の送信器(TMTR)422_aから422_tに供給する。いくつかの実施形態において、TX MIMOプロセッサ420は、データストリームのシンボルおよびシンボルがそこから送信されるアンテナにビームフォーミング重みを適用する。送信器システム410は、ただ1つのアンテナを有する実施形態または複数のアンテナを有する実施形態を含む。

【００４５】

各送信器422は、1つまたは複数のアナログ信号を供給するためにそれぞれのシンボルストリームを受信し、処理し、さらに、MIMOチャネルを介する送信に適する変調された信号を供給するためにアナログ信号を条件付ける(たとえば、増幅し、フィルタリングし、アップコンバートする)。次いで、送信器422_aから422_tからのN_T個の変調された信号は、それぞれN_T個のアンテナ424_aから424_tから送信される。本明細書で説明される技法は、1つの送信アンテナだけを有するシステムにもあてはまる。1つのアンテナを使用する送信は、複数アンテナのシナリオよりも単純である。たとえば、単一アンテナのシナリオにおいては、TX MIMOプロセッサ420が不要である場合がある。

【００４６】

受信器システム450において、送信された変調された信号は、N_R個のアンテナ452_aから452_rによって受信され、各アンテナ452からの受信された信号は、それぞれの受信器(RCVR)454_aから454_rに供給される。各受信器454は、それぞれの受信された信号を条件付け(たとえば、フィルタリングし、増幅し、ダウンコンバートし)、サンプルを提供するために条件付けられた信号をデジタル化し、さらに、対応する「受信された」シンボルストリームを提供するためにサンプルを処理する。本明細書で説明される技法は、ただ1つのアンテナ452を有する受信器システム450の実施形態にもあてはまる。

【００４７】

次いで、RXデータプロセッサ460が、N_T個の検出されたシンボルストリームを供給するために、特定の受信器処理技法に基づいて、受信器454_aから454_rにN_R個の受信されたシンボルストリームを受信し、処理する。次いで、RXデータプロセッサ460は、データストリームのトラフィックデータを回復するために、必要に応じて、各検出されたシンボルストリームを復調し、デインターリーブし、復号する。回復されたトラフィックは、たとえば、本開示の態様による、MMEからの認証情報要求内の情報を含むことができる。RXデータプロセッサ460による処理は、送信器システム410においてTX MIMOプロセッサ420およびTXデータプロセッサ414によって実行される処理に対して相補的とすることができる。

【００４８】

RXデータプロセッサ460によって供給される情報は、プロセッサ470がチャネル状態情報(CSI)および他の情報などのレポートを作成して、TXデータプロセッサ438に供給することを可能にする。プロセッサ470は、CSIおよび/またはパイロット要求を含む逆方向リンクメッセージを定式化して、送信器システムに送信する。

【００４９】

プロセッサ470は、たとえば図2または図3内で説明されたプロセッサに関して上で説明されたように実施され得る。逆方向リンクメッセージに加えて、受信器システム450は、アタッチ要求と、肯定応答トークンと、通信セッションを確立するための他の情報ならびに通信セッション中のデータとを含む、他の様々なタイプの情報を送信することができる。メッセージは、TXデータプロセッサ438によって処理され、TX MIMOプロセッサ480によって変調され、送信器454_aから454_rによって条件付けられ、送信器システム410に戻って送信される。図示されているように、TXデータプロセッサ438は、データソース436から複数のデータストリーム用のトラフィックデータを受け取ることもできる。

【００５０】

送信器システム410において、受信器システム450からの変調された信号は、受信器システム450によって送信された逆方向リンクメッセージを抽出するために、アンテナ424によって受信され、受信器422によって条件付けられ、復調器440によって復調され、RXデータ

プロセッサ442によって処理される。その結果、データは、送信器システム410と受信器システム450との間で送られ、受信され得る。送信器システム410は、理解されるように、それが受信器システム450から受信する情報をそのサービングネットワーク内の他のネットワーク要素に送信し、サービングネットワーク内の1つまたは複数の他のネットワーク要素から情報を受信するのにも使用され得る。図4内に示された実施形態は、例示的であるのみであり、本開示の実施形態は、図4内に示されていない他の送信器システム/受信器システムに適用可能である。

【００５１】

図5は、本開示の様々な態様による、ワイヤレスネットワーク内で識別情報プライバシをサポートするための、UEとサービングネットワークとホームネットワークと(サーバと)の間のいくつかのシグナリング態様を示すプロトコル図である。議論の単純さのために、図5のプロトコル図内のアクションを説明する際に、図1内に示された要素(たとえば、UE 102、eNBとしての基地局104、MME 106、およびHSSとしてのサーバ112)を参照する。さらに、単純さのために、議論は、アタッチ手順のすべての態様ではなく、プロトコルフローのうちで本開示の実施形態の態様を説明する態様に焦点を合わせる(たとえば、議論は、TS 23.401 5.3.2.1に見られるものなどの多少のオーバーラップを伴う3GPP規格または他のアタッチ手順に加えて、またはこれとは異なる態様に焦点を合わせる)。

【００５２】

アクション502において、UE 102は、UE 102内に記憶された現在のPMSIにアクセスする。これが、UE 102がサービングネットワーク108にアタッチすることを初めて試みている時である場合には、現在のPMSIは、初期PMSIに対応する可能性がある(たとえば、PMSIが、UE 102のIMSIと同時にプロビジョニングされる場合、またはPMSIが、より後であるがアタッチ要求の前に合意された場合)。実施形態において、前のアタッチ手順が発生済みである場合またはサーバ112においてPMSI衝突によって必要とされる場合に、UE 102内に記憶された現在のPMSIは、前のアタッチ手順中にUEとサーバ112との間で合意された次のPMSIである。UE 102は、初期PMSI、現在のPMSI、以前のPMSI、および/または次のPMSIを含む1つまたは複数のPMSI値を記憶することができる。いくつかの場合に、現在のPMSIは、前のPMSI値とは別個の値として記憶される。

【００５３】

いくつかの実施形態において、UE 102は、以前のPMSIおよびPMSIトラッキングインデックスから現在のPMSIを導出する。たとえば、PMSIトラッキングインデックスは、初期PMSIとともに0に初期化され得、UE 102およびサーバ112がアタッチ手順を成功裡に完了するたびに、PMSIトラッキングインデックスは、UE 102とサーバ112との両方において固定値(たとえば、1)だけ増分され得る。したがって、UE 102およびサーバ112の各々は、現在使用中のPMSIの任意の反復に到達するのに使用され得る[初期PMSI、PMSIトラッキングインデックス]を記憶することができる。それぞれは、[現在のPMSI、PMSIトラッキングインデックス]をも記憶し、代わりに初期PMSIを参照する必要がある(たとえば、インデックス値がUE 102とサーバ112との間で一致しない場合)かどうかを判定するために、PMSIトラッキングインデックスに頼ることができる。

【００５４】

アクション504において、UE 102は、たとえば、基地局104に初期アタッチ要求を送信することによってサービングネットワーク108に初期アタッチ要求を送り、次いで、基地局104は、MME 106に転送する。初期アタッチ要求は、IMSIの代わりに現在のPMSI(または、サービングネットワーク108内の1つまたは複数の要素がUE 102のIMSIに関連付けるのに使用できる任意の他の値)を含む。

【００５５】

MME 106が、アクション504中に初期アタッチ要求を受信した後に、アクション506において、MME 106は、初期アタッチ要求内の情報をとり、認証情報要求をサーバ112に送る。認証情報要求は、現在のPMSIと、UE 102によってアクセスされているサービングネットワーク108を参照するシーケンス番号とを含むことができる。

【００５６】
アクション508において、サーバ112が、アクション506中に認証情報要求を受信した後に、サーバ112は、認証情報要求内に含まれるPMSIをチェックし、(とりわけ)1つまたは複数のデータベースに対してPMSIをチェックする。アクション508の一部として、サーバ112は、PMSIを暗号化解除する(PMSIが暗号化されている場合)。たとえば、サーバ112は、PMSIを暗号化するのに利用された公開鍵に関連する秘密鍵を使用してPMSIを暗号化解除することができる。サーバ112は、PMSIを、たとえば上で図3内で説明されたデータベース310内に記憶された値と比較する。サーバ112が、PMSI値の間の一致を見つける時に、サーバ112は、UE 102から受信された現在のPMSIに対応するIMSIに関してもチェックすることができる。

【００５７】
PMSI値の一致がある時には、アクション508の一部として、サーバ112(たとえば、PMSIモジュール308)は、MME 106への認証応答内に含めるために次のPMSIを導出することができる。一実施形態において、次のPMSIは、次のように導出される。PMSIトラッキングインデックスが、固定量、たとえば1だけ増分され、データベース310内に記憶された(MME 106からの認証情報要求内で識別される)現在のPMSI値に連結される。この値は、K_{PMSI}値と一緒に、別の導出関数への入力として含められる。K_{PMSI}は、PMSI生成鍵である。たとえば、K_{PMSI}は、入力として元の鍵K(たとえば、EPSマスタ鍵)およびPMSI導出コンテキストCTXを有する鍵導出関数(KDFF)を使用することによって作成され得る(たとえば、K_{PMSI}=KDF(K, CTX))。CTXは、コンテキスト、たとえば「PMSI generation」などの文字列とすることができ、鍵生成においてコンテキストを使用することによって、同一の鍵Kが、異なる鍵生成結果をもたらすために異なるコンテキストを組み込むことによるなど、異なる鍵を生成するのに使用され得る。

【００５８】
K_{PMSI}値およびインデックスを連結されたPMSIは、関数内で一緒にハッシュ化される(たとえば、(結果=HMAC(K_{PMSI}, PMSI|インデックス)、ただし、|は、連結演算子である))。関数の結果は、切り詰められ得、その結果、HMAC関数の出力(鍵付ハッシュメッセージ認証コード)が、固定された桁数(たとえば、9桁～10桁)に制限されるようになる。次いで、切り詰められた結果は、モバイルネットワークコード(MNC)およびモバイル国コード(MCC)と連結され得、結果の値が、次のPMSIになる。切詰の結果としてのこの値は、一実施形態において15桁の長さとすることができるが、他の長さ(より長いとより短いとの両方)が、本開示の範囲から逸脱せずに可能であることを理解されたい。全体的な動作は、一実施形態において次のように記述され得る。

次のPMSI=MCC|MNC|Truncate(HMAC(K_{PMSI}, PMSI|インデックス)) (式1)

【００５９】
一般的に言って、サーバ112は、PMSIトラッキングインデックスとともにPMSI(たとえば、初期PMSIおよび/または現在のPMSI)を記憶することができる。PMSIトラッキングインデックスは、サーバ112が、初期PMSIをx回繰り返してハッシュ化することによって初期PMSIから現在のPMSIを計算することを可能にし、ここで、xは、PMSIトラッキングインデックス値と等しい。PMSIトラッキングインデックスは、アカウンティングならびに衝突回避にも有用である。たとえば、サーバ112は、任意の他のUEのPMSIとの衝突がないことを検証するために、生成された次のPMSIを他の既知のPMSI値に対してチェックすることができる。衝突がない場合に、サーバ112は、インデックスを(たとえば1だけ)増分し、新しいPMSIを連結されたインデックス値を用いて式(1)を繰り返すことができる。

【００６０】
アクション510において、サーバ112は、生成された情報をとり、これを、MME 106に送られる認証情報応答内に組み込む。次のPMSIは、たとえばMME 106がUE 102とサーバ112との間で次のPMSIを見分けられなくするために、認証情報応答内の追加のセキュリティのために暗号化され得る。たとえば、次のPMSIは、K_{PMSI}および乱数(RAND)から導出される匿名鍵(anonymity key)を用いて暗号化される(たとえば、匿名鍵=function(K_{PMSI}, RAND))

。

【００６１】

匿名鍵は、K_{PMSI}および乱数RANDを入力として鍵導出関数に渡すことによって導出される。鍵導出関数は、3GPP規格(または将来の同等の/類似する規格)、たとえばf5*と一貫する任意の導出関数とすることができる。一実施形態において、鍵導出関数は、HMAC関数とすることができる。したがって、一実施形態において、匿名鍵は、HMAC(K_{PMSI}, RAND)によって導出され得る。代替実施形態において、匿名鍵は、初期サービングネットワーク108認証が使用可能にされる場合に、鍵暗号化鍵(KEK)とすることができる。

【００６２】

アクション510の一部として、サーバ112は、認証情報応答をMME 106に送ることができる。認証情報応答は、とりわけ、認証ベクトルと、暗号化された形の次のPMSI/PMSIトラッキングインデックス(その導出が上で説明された匿名関数によって暗号化される)とを含むことができる。一実施形態において、認証ベクトルは、それ自体が、認証トークン、期待される応答、乱数、およびローカルマスタ鍵K_{ASME}を含むことができる。したがって、認証ベクトルに関して伝統的に含まれ得るものに加えて、本開示の実施形態は、UE 102との同期化のために次のPMSIおよびPMSIトラッキングインデックスをも含む。MME 106は、認証ベクトルを記憶することができるが、いくつかの実施形態においては、暗号化されたPMSI/PMSIトラッキングインデックスを記憶しない。

【００６３】

アクション512において、MME 106は、認証要求をUE 102に送ることによって、UE 102との相互認証にかかわる。認証要求は、アクション510の認証情報応答から入手された情報をとる。たとえば、MME 106は、認証の一部として期待される応答を保持し、認証トークン上で乱数、eUTRAN鍵セット識別子(eKSI)、ならびに暗号化された次のPMSIおよびPMSIトラッキングインデックスを渡すことができる。

【００６４】

アクション514において、UE 102は、(MME 106との伝統的な相互認証手順に加えて)次のPMSIを確認し、サーバ112に返すための肯定応答トークンを生成する。これに関して、UE 102は、アクション512において受信された認証要求からの暗号化された次のPMSI値およびPMSIトラッキングインデックス値を暗号化解除する。UE 102が、サーバ112も有する(MME 106は有しない)共有される秘密鍵CTX(PMSI導出鍵)を有するので、UE 102は、次のPMSI値およびPMSIトラッキングインデックス値を暗号化解除することができる。

【００６５】

UE 102は、サーバ112によって生成された次のPMSIに対して比較するためにそれ自体で次のPMSIを導出して、それらが同期していることを確認する。UE 102は、次のPMSIトラッキングインデックスを用いて現在のPMSIをハッシュ化することによって、次のPMSIを導出することができる。代替案では、UE 102は、初期PMSIをx回繰り返してハッシュ化することによって次のPMSIを導出することができ、ここで、xは、PMSIトラッキングインデックス値(UE 102に関してローカルに保存されたまたはサーバ112から暗号化解除されたいずれか)と等しい。次いで、UE 102は、ローカルに導出された次のPMSIをサーバ112から受信された次のPMSIと比較する。値が一致する場合に、UE 102は、肯定応答トークンの生成に進むことができる。

【００６６】

2つの次のPMSI値が一致しない(たとえば、UE 102が、PMSIトラッキングインデックスのそれ自体のバージョンを使用する場合)場合には、UE 102およびサーバ112は、同期していない。これは、たとえば、UE 102からまたはUE 102へのメッセージが、輸送中に破棄された状況において発生する可能性がある。このシナリオにおいて、UE 102は、サーバ112から受信され、暗号化解除されたPMSIトラッキングインデックスに対応するようにそのPMSIトラッキングインデックスを更新することができる。次いで、UE 102は、次のPMSIを再導出し、サーバ112から受信され、暗号化解除された次のPMSIともう一度比較することができる。

【００６７】
後続のアタッチ手順の現在のPMSI値として使用される次のPMSIを確認して、UE 102は、肯定応答トークンの生成に進むことができる。肯定応答トークンは、暗号化されたシーケンス番号(同期化に使用される)およびMAC-A値を連結することによって生成され得る。暗号化態様は、UE 102とサーバ112との間で共有されるシーケンス番号を暗号化することを伴う。暗号化は、一実施形態において上でアクション510において説明された匿名鍵とは異なる別の匿名鍵(たとえば、ここでの匿名鍵は、3GPP規格または他の規格と一貫する異なる関数を使用して導出される)によって実行され得る。たとえば、シーケンス番号を暗号化するのに使用される匿名鍵自体は、入力として上で説明されたK_{PMSI}および乱数をとる様々な鍵導出関数のいずれかによって生成され得る。

【００６８】
暗号化されたシーケンス番号に連結されるMAC-A値は、入力として別の匿名鍵(たとえば、上で説明した別の匿名鍵のいずれとも異なる)、乱数を連結されたシーケンス番号、および認証管理フィールド(AMF)値をとるメッセージ認証関数(たとえば、f1*)から生成される。メッセージ認証関数において入力として使用される匿名鍵は、入力としてK_{PMSI}および乱数をとる別の鍵導出関数によって生成され得る。これらの関数および特定の入力は、議論の単純さのために説明される。理解されるように、他の関数およびこれらの関数への入力が、本開示の範囲から逸脱せずに使用され得る。

【００６９】
アクション516において、UE 102は、アクション514において生成された肯定応答トークンを、PMSI肯定応答メッセージとしてMME 106およびサーバ112に送り返す。PMSI肯定応答メッセージは、生成され、アクション514に関して上で説明された認証トークンならびに乱数(たとえば、上の鍵導出関数において使用されたものと同一の乱数)を含むことができる。一実施形態において、PMSI肯定応答メッセージは、ここで詳細には説明されないUE 102からMME 106へのアタッチ手順の他の態様(たとえば、暗号化されたオプション応答メッセージ)とともにピギーバックされ得る。MME 106において、PMSI肯定応答メッセージは、サーバ112に送られる別のメッセージ(たとえば、位置更新要求)とともに、MME 106からサーバ112へピギーバックされ得る。

【００７０】
アクション518において、肯定応答トークンの受信時に、サーバ112は、現在のPMSI値を用いて以前のPMSIを、次のPMSI値(UE 102に関して確認済みであり、したがって同期化されている)を用いて現在のPMSIを更新する。これは、アタッチ手順において使用されるPMSI値が、確立されたセッション中、たとえば他のMMEへのハンドオフ中にそれでもサーバ112とサービングネットワーク108とUE 102との間で使用され得るようにするために有用であり、その結果、UE 102の位置が、UE 102のIMSIを開示せずにサーバ112に関して正しく更新され得るようになる。次いで、アタッチ手順は、伝統的に実行される他の態様を含めるために継続することができるが、IMSIのすべての使用は、本開示によるPMSIの使用によって置換される。

【００７１】
たとえば上で図5に関して説明された、UE 102の成功裡の認証の後に、サーバ112は、いくつかの管轄区内の法律によって、図1内に示されたサービングネットワーク108などの要求するサービングネットワークにUE 102のIMSIを開示することを要求される場合がある。本開示の態様によれば、サーバ112は、これらの状況において、それでも、悪意のあるMME 106などの1つまたは複数の悪意のあるネットワーク要素の可能性に対して保護するために、IMSIの代わりにPMSIを供給することができる。

【００７２】
そのような要求は、次のように見える可能性がある(図5内には図示せず)。MME 106は、UE 102のIMSI要求をサーバ112に送ることができる。本開示の実施形態によれば、UE 102のIMSIは、アタッチ手順(またはハンドオーバ)中にMME 106によって受信されず、PMSIが受信されたので、MME 106は、K_{IMSI}暗号化鍵と一緒にUE 102に関連する受信されたPMSIを

含める。K_{IMSI}暗号化鍵は、入力としてK_{ASME}(アクセスセキュリティ管理エンティティ(Access Security Management Entity))およびIMSI検索キーを有するHMAC関数などの関数からの結果として生成され得る。K_{ASME}は、MME 106とサーバ112との両方に既知のMME 106基本鍵である。

【００７３】

IMSI要求に応答して、サーバ112は、IMSI応答を供給する。一実施形態において、サーバ112は、MME 106がIMSIに到達するための他の能力がない状態で、PMSIを送る。これを可能にすることができるのは、たとえば、サーバ112が、それでも、IMSI要求の対象であるUE 102のPMSIとIMSIとの間の関連付けを維持し、したがって、サーバ112がIMSIの使用と同一の情報にPMSIを使用してアクセスできるので、事実上、PMSIが、要求された妥当性検査を提供するからである。別の実施形態において、サーバ112は、PMSIならびにIMSIの暗号化されたバージョンを用いて応答する。たとえば、サーバ112は、PMSIとIMSIとの両方をとり、K_{IMSI}を使用してこれらを暗号化することができる。その結果、IMSIは、正当にK_{ASME}を所有するMME 106のみによって正しく暗号化解除され得る。

【００７４】

ここで図6Aに移ると、流れ図が、本開示の様々な態様による、PMSIを使用してアタッチプロセスを開始するUEのための例示的な方法600を示している。方法600は、サービングネットワーク108(たとえば、サービングネットワーク108の2つのネットワーク要素を示すために基地局104およびMME 106)と通信しているUE 102内で実施され得る。方法600は、議論の単純さのために特定のUE 102に関して説明されるが、本明細書で説明される態様が、複数のUE 102に適用可能とされ得ることを理解されたい。追加のステップが、方法600のステップの前、中、および後に提供され得ることと、説明されるステップの一部が、方法600の他の実施形態に関して置換されまたは除去され得ることとを理解されたい。

【００７５】

ステップ602において、UE 102は、ステップ604における初期アタッチ要求のために使用される現在のPMSIにアクセスする。上で図5に関して議論したように、現在のPMSIは、これがUE 102に関する最初のアタッチの試みである場合に、UE 102において(たとえば、メモリ204内に)記憶された初期PMSIとすることができる。他の実施形態において、前のアタッチ手順が発生済みである場合に、現在のPMSIは、前のアタッチ手順中にサーバ112とUE 102との間で確認された次のPMSIである。

【００７６】

ステップ604において、現在のPMSIが取り出された後に、UE 102は、現在のサービングネットワーク(たとえば、図1内に示された108)に初期アタッチ要求を送る。初期アタッチ要求は、IMSIまたはUE 102のIMSIを再構成するのに使用され得る他の値ではなく、取り出された現在のPMSIならびに他の情報を含む。初期アタッチ要求は、基地局104によって受信され得、基地局104は、この要求をMME 106に転送する。MME 106が初期アタッチ要求を受信した後に、MME 106は、初期アタッチ要求内の情報をとり、IMSIではなくPMSIとともに、認証情報要求をサーバ112に送る。

【００７７】

ステップ606において、UE 102は、サービングネットワーク108内のMME 106から(たとえば、基地局104を介して)認証要求を受信する(たとえば、上で図5のアクション512において説明したように)。認証要求は、サーバ112からの暗号化された次のPMSIおよびPMSIトラッキングインデックスを含むことができ、MME 106は、暗号化解除するための適当な鍵を有しないので、それにアクセスすることができない可能性がある。

【００７８】

ステップ608において、UE 102は、認証要求の一部としてMME 106から受信された次のPMSI値およびPMSIトラッキングインデックス値を暗号化解除する。UE 102は、上で図5のアクション508および514に関して説明したように、値を暗号化するのに使用された匿名鍵を生成する際にサーバ112が使用した共有される秘密鍵を有するので、次のPMSI値およびPMSIトラッキングインデックス値を暗号化解除することができる。

【００７９】
ステップ610において、UE 102は、独力で(すなわち、ステップ608において受信された次のPMSIおよびPMSIトラッキングインデックスに頼らずに)次のPMSI値を導出する。一実施形態において、UE 102は、UE 102において(たとえばメモリ204内に)記憶された以前のPMSI値およびPMSIトラッキングインデックス値に基づいて次のPMSI値を導出する。別の実施形態において、UE 102は、UE 102を用いて記憶された初期PMSI値およびPMSIトラッキングインデックスの現在の値に基づいて(たとえば、PMSIトラッキングインデックスの現在の値と等しい回数だけPMSI値をハッシュ化することによって)次のPMSI値を導出する。
【００８０】
ステップ612において、UE 102(たとえば、PMSIモジュール208に協力するプロセッサ202)は、ローカルに導出された次のPMSI値を受信され暗号化解除された次のPMSI値と比較する。
【００８１】
判断ステップ614において、ローカルに導出された次のPMSI値および受信され暗号化解除された次のPMSI値が一致しない場合には、方法600は、ステップ616に進み、ここで、UE 102は、サーバ112から受信され暗号化解除されたPMSIトラッキングインデックスの値と等しくなるようにPMSIトラッキングインデックスのローカルバージョンを更新する。次いで、方法600は、ステップ616からステップ610に戻って進み、ここで、プロセスは、上で説明したように継続する。
【００８２】
判断ステップ614に戻って、ローカルに導出された次のPMSI値および受信され暗号化解除された次のPMSI値が一致する場合には、方法600は、ステップ618に進む。
【００８３】
ステップ618において、UE 102(たとえば、PMSIモジュール208に協力するプロセッサ202)は、たとえば上で図5のアクション514に関して説明したように、サーバ112に送られる肯定応答トークンを生成する。
【００８４】
ステップ620において、UE 102は、たとえばサービングネットワーク108の1つまたは複数のネットワーク要素を介して、生成された肯定応答トークンをサーバ112に送る。また、UE 102は、たとえば現在のPMSI値(現在のアタッチ手順内で使用されるPMSI)を反映するように以前のPMSIを、同期化された次のPMSI値を反映するように現在のPMSIを更新することによって、そのローカルPMSI値を更新する。UE 102およびサービングネットワーク108は、理解されるように、通信セッションの確立を継続することができる。
【００８５】
図6Bは、本開示の様々な態様による、PMSIを使用するアタッチプロセス内のサーバのための例示的な方法630を示す流れ図である。方法630は、サービングネットワーク108と通信しているサーバ112(たとえば、サービングネットワーク108の1つのネットワーク要素の例を示すためにMME 106)内で実施され得る。方法630は、議論の単純さのためにサーバ112に関して説明されるが、本明細書で説明される態様が、複数のサーバ112に適用可能とされ得ることを理解されたい。追加のステップが、方法630のステップの前、中、および後に提供され得ることと、説明されるステップの一部が、方法630の他の実施形態に関して置換されまたは除去され得ることとを理解されたい。
【００８６】
ステップ632において、サーバ112は、サービングネットワーク108、たとえばMME 106から、UE 102のIMSIではなくUE 102によってMME 106に供給された現在のPMSIを含む認証情報要求を受信する。アクション506に関して上で説明したように、MME 106は、MME 106がUE 102から受信した初期アタッチ要求に基づいて認証情報要求を送る。
【００８７】
ステップ634において、サーバ112(たとえば、PMSIモジュール308およびデータベース310と協力するプロセッサ302)は、たとえば図5のアクション508に関して上で説明したよう

に、受信されたPMSIに対応する特定のUE 102を識別するために、サーバ112において既に維持されている(または、他所においてサーバ112によってアクセス可能な)PMSI値に対して受信されたPMSIをチェックする。

【００８８】

ステップ636において、一致を見つけた後に、サーバ112は、データベース310内に配置された(または他所においてサーバ112によってアクセス可能な)受信されたPMSIに関連するPMSIトラッキングインデックスを増分する。PMSIトラッキングインデックスは、サーバ112によって維持され、UEのPMSIレコードに関連して保持される。PMSIトラッキングインデックスは、上で説明したように、サーバ112が、UE 102とサーバ112との間で合意された初期PMSIに基づいてUE 102のPMSIの任意の反復を計算することを可能にする。PMSI値の任意の反復に達するこの能力は、サーバ112が様々なアカウンティング目的および課金目的を達成することをも可能にする。サーバ112は、サーバ112によって導出された可能な次のPMSI値と別のUE 102のためにサーバ112において既に維持されている別のPMSI値との間で衝突が発生する状況に対処するためにもPMSIトラッキングインデックスを使用する。一実施形態において、PMSIトラッキングインデックスは、例として1の値だけ増分され得る。

【００８９】

ステップ638において、サーバ112(たとえば、PMSIモジュール308と協力するプロセッサ302)は、次のPMSIを導出する。サーバ112は、たとえば上で図5内のアクション508に関して説明したように、ステップ632において認証情報要求内で受信された現在のPMSIならびにステップ636からの増分されたPMSIトラッキングインデックスに基づいて次のPMSIを導出することができる。同様に、サーバは、初期PMSI値およびPMSIトラッキングインデックス値に基づいて次のPMSIを導出することができる。

【００９０】

判断ステップ640において、サーバ112は、任意の他のUEのPMSIとの衝突がないことを検証するために、ステップ638において導出された次のPMSIを他の既知のPMSI値に対してチェックする。衝突がある場合には、方法630は、ステップ636に戻って進み、ここで、PMSIトラッキングインデックスが、もう一度増分され、次いで、次のPMSIが、新しいPMSIトラッキングインデックス値を用いてステップ638において導出される。

【００９１】

判断ステップ640に戻って、衝突がない場合には、方法630は、ステップ642に進む。ステップ642において、サーバ112は、たとえば図5のアクション508に関して上で説明したように、次のPMSI値および増分されたPMSIトラッキングインデックス値を暗号化する。図5において議論したように、暗号化された次のPMSI値およびPMSIトラッキングインデックス値は、認証ベクトルと一緒に認証情報応答に含まれ得る。

【００９２】

ステップ644において、サーバ112は、暗号化された次のPMSI値およびPMSIトラッキングインデックス値を含む認証情報応答をMME 106に送信する。次いで、MME 106は、UE 102との相互認証にかかわることができる。その相互認証の一部として、MME 106は、暗号化された次のPMSI値およびPMSIトラッキングインデックス値を、この情報をMME 106において暗号化解除することなく送信することができる。

【００９３】

UE 102が、たとえば図6Aのステップ608～616のうちの1つまたは複数に従って、次のPMSI値を確認した後に、方法630は、ステップ646に進む。ステップ646において、UE 102が、次のPMSI値を確認するか、他の形で同期化を完了した(たとえば、新しい提案される次のPMSI値を送ること、新しい次のPMSI値を要求すること、または受信され暗号化解除されたPMSIトラッキングインデックスの値を反映するようにそのローカルPMSIトラッキングインデックスを調整することによって)後に、サーバ112は、MME 106を介してUE 102から認証トークンを受信する。次いで、これに応答して、サーバ112は、そのPMSI情報を更新する(たとえば、サーバ112は、現在のPMSI値(現在のアタッチ手順内で使用されるPMSI値)を反映するように以前のPMSIを、および同期化された次のPMSI値を反映するように現在のPMSI

を更新する)。UE 102およびサービングネットワーク108は、理解されるように、通信セッションの確立を継続することができる。

【００９４】

ここで図7Aに移ると、流れ図が、本開示の様々な態様による、UEに関するPMSI初期化のための例示的な方法700を示す。方法700は、基地局104およびMME 106と通信しているUE 102内で実施され得る。方法700は、議論の単純さのために単一のUE 102に関して説明されるが、本明細書で説明される態様が、複数のUE 102に適用可能とされ得ることを理解されたい。追加のステップが、方法700のステップの前、中、および後に提供され得ることと、説明されるステップの一部が、方法700の他の実施形態に関して置換されまたは除去され得ることとを理解されたい。

【００９５】

ステップ702において、UE 102は、初期化プロセスを開始する。これは、UE 102のプロビジョニング(たとえば、本開示の態様によるIMSI値およびPMSI値の、UE 102のSIMカードへのプログラミング)の時またはより後の時に行われ得る。

【００９６】

判断ステップ704において、UE 102は、それがプロビジョニングの時に初期化されたPMSIを既に有するかどうかを判定する。これは、たとえば、プロセッサ202とメモリ204とPMSIモジュール208との間で協力して行われ得る。PMSIが既に初期化されている場合には、方法700は、ステップ716に進み、ここで、初期PMSIが記憶され、PMSI初期化方法700は終了する。PMSIがまだ初期化されていない場合には、方法700は、ステップ706に進む。

【００９７】

ステップ706において、プロセッサ202およびPMSIモジュール208は、一緒に協力し、提案される初期PMSIを生成する。提案される初期PMSIは、任意の様々な要因に基づくものとすることができる。一実施形態において、提案される初期PMSIは、UE 102のIMSIに基づき、たとえば、乱数または擬似乱数と組み合わされた1つまたは複数のハッシュ関数および/または反復に基づくものとすることができる。別の実施形態において、PMSIはUE 102のIMSIに基づくのではなく、少数の例を挙げれば乱数または擬似乱数に基づき、その結果、いかなる盗聴者も、PMSIからIMSIを導出できなくなる。

【００９８】

ステップ708において、プロセッサ202およびPMSIモジュール208は、一緒に協力し、ステップ706において生成された提案される初期PMSIを暗号化する。一実施形態において、PMSIは、サーバ112が以前のある時にUE 102と共有した公開鍵を使用して暗号化される。サーバ112は、受信時にPMSIを暗号化解除するための対応する秘密鍵を有する。

【００９９】

ステップ710において、UE 102は、トランシーバ210を介し、たとえば基地局104および/またはMME 106を介して暗号化されたPMSIをサーバ112に送信する。

【０１００】

ステップ712において、UE 102は、提案される初期PMSIの受信を肯定応答する応答をサーバ112から受信する(トランシーバ210を介して)。

【０１０１】

判断ステップ714において、プロセッサ202およびPMSIモジュール208は、一緒に協力し、サーバ112から受信された応答が、サーバ112が提案される初期PMSIを受け入れたことを示すかどうかを判定する。応答が、サーバ112が提案される初期PMSIを受け入れたことを示す場合には、方法700は、ステップ716に進み、ここで、初期PMSIが記憶され、方法700は終了する。応答が、サーバ112が提案される初期PMSIを受け入れなかったことを示す場合には、方法700は、ステップ706に戻って、拒絶されたばかりの初期PMSIとは異なる新しい提案される初期PMSIを生成する。提案される初期PMSIは、たとえば、そのPMSIと、たとえばサーバ112のデータベース310内に既に記憶されている、別の関連するUEの任意の他のPMSIとの間に衝突がある場合に、拒絶され得る。

【０１０２】

方法700は、UE 102とサーバ112との両方にとって同意可能なPMSIに達するまで繰り返され得る。代替実施形態において、判断ステップ714において、UE 102が、サーバ112が提案される初期PMSIを受け入れなかったと判定する場合に、UE 102は、サーバ112がUE 102のそれ自体の提案される初期PMSIを送ったかどうかを識別するために、サーバ112からの応答(ステップ712と同一のまたは異なる応答)を調べることもできる。この実施形態において、UE 102は、サーバ112からの提案される初期PMSIをチェックして、それがUE 102にとって許容できるものであるか否かを判定することができる。問題がなければ、UE 102は、サーバ112からの提案される初期PMSIを受け入れ、受入についてサーバ112に通知することができる。初期PMSIが合意された後に、初期PMSIは、後続使用のためにUE 102において記憶され、方法700はステップ716において終了する。

【０１０３】

図7Bは、本開示の様々な態様による、サーバに関するPMSIを使用するアタッチプロセスのための例示的な方法720を示す流れ図である。方法720は、議論の単純さのために単一のサーバ112および単一のUE 102に関して説明されるが、本明細書で説明される態様が、任意の個数のサーバ112および/またはUE 102に適用可能とされ得ることを理解されたい。追加のステップが、方法720のステップの前、中、および後に提供され得ることと、説明されるステップの一部が、方法720の他の実施形態に関して置換されまたは除去され得ることとを理解されたい。

【０１０４】

ステップ722において、サーバ112は、たとえばトランシーバ312を介して、UE 102から暗号化された提案される初期PMSIを受信する。

【０１０５】

ステップ724において、サーバ112は、たとえば、協力するプロセッサ302、メモリ304、およびPMSIモジュール308によって、受信されたPMSIを暗号化解除する。一実施形態において、受信されたPMSIは、サーバ112においてまたはサーバ112のために保持される秘密鍵に対応する公開鍵を用いてUE 102において暗号化された。

【０１０６】

ステップ726において、サーバ112は、受信され暗号化解除されたPMSIを、データベース310における(または、サーバ112における任意の他のデータベース内もしくは複数のUEに関するサーバ112によってアクセス可能な情報を維持する他所内の)他のUEに関して既に存在する他のPMSI値と比較する。

【０１０７】

ステップ728において、サーバ112は、受信された提案される初期PMSI値とサーバ112によって記憶されまたは他の形でアクセス可能な任意の他のPMSI値との間に衝突があるかどうかを判定する。

【０１０８】

判断ステップ730において、サーバ112は、ステップ728における判定に基づいて、提案される初期PMSIを受け入れるか否かを判断する。サーバ112が、提案される初期PMSIを受け入れる場合に、方法720は、ステップ734に進み、ここで、サーバ112は、初期PMSIの受入の肯定応答をUE 102に送り、初期PMSIをサーバ112においてデータベース310内に記憶し、その結果、初期PMSIがUE 102に関連付けられるようにする(たとえば、サーバ112がUE 102のために保持するレコードの一部として)。

【０１０９】

判断ステップ730において、サーバ112が、提案される初期PMSIを受け入れないと判定する場合には、方法720は、ステップ732に進み、ここで、サーバ112は、UE 102に新しいPMSIを要求し、サーバ112は、これをUE 102に送信し、応答を待つ。代替実施形態において、サーバ112は、その代わりに、提案される初期PMSIを自発的に生成し(判断ステップ730に応答して)、これを拒否とともにUE 102に送信することができる。

【０１１０】

情報および信号は、様々な異なる技術および技法のいずれかを使用して表現され得る。

たとえば、上記の説明全体にわたって参照される場合があるデータ、命令、コマンド、情報、信号、ビット、シンボル、およびチップは、電圧、電流、電磁波、磁場もしくは磁性粒子、光場もしくは光学粒子、またはそれらの任意の組合せによって表現され得る。

【０１１１】

本開示に関連して本明細書で説明される様々な例示的なブロックおよび方法は、汎用プロセッサ、DSP、ASIC、FPGAもしくは他のプログラマブル論理デバイス、ディスクリートゲート論理もしくはディスクリートトランジスタ論理、ディスクリートハードウェア構成要素、または本明細書で説明される機能を実行するように設計されたその任意の組合せを用いて実施されまたは実行され得る。汎用プロセッサはマイクロプロセッサとすることができるが、代替案において、プロセッサは、任意の従来のプロセッサ、コントローラ、マイクロコントローラ、または状態機械とすることができる。プロセッサは、コンピューティングデバイスの組合せ(たとえば、DSPおよびマイクロプロセッサの組合せ、複数のマイクロプロセッサ、DSPコアに関連する1つまたは複数のマイクロプロセッサ、または任意の他のそのような構成)としても実施され得る。

【０１１２】

本明細書で説明される機能は、ハードウェア、プロセッサによって実行されるソフトウェア、ファームウェア、またはその任意の組合せにおいて実施され得る。プロセッサによって実行されるソフトウェアにおいて実施される場合に、機能は、コンピュータ可読媒体上の1つまたは複数の命令またはコード上に記憶されまたは1つまたは複数の命令またはコードとして送信され得る。他の例および実施態様は、本開示の範囲内および添付の特許請求の範囲の範囲内にある。たとえば、ソフトウェアの性質に起因して、上で説明された機能は、プロセッサ、ハードウェア、ファームウェア、ハードワイヤリング、またはこれらのいずれかの組合せによって実行されるソフトウェアを使用して実施され得る。機能を実装する特徴は、機能の部分が異なる物理的位置において実施されるように分散されることを含めて、様々な位置に物理的に配置される場合もある。また、特許請求の範囲内を含めて、本明細書で使用される時に、項目のリスト(たとえば、「のうちの少なくとも1つ」または「のうちの1つまたは複数」などの句で終わる項目のリスト)内で使用される「または」は、たとえば、[A、B、またはCのうちの少なくとも1つ]のリストが、AまたはBまたはCまたはABまたはACまたはBCまたはABC(すなわち、AおよびBおよびC)を意味するような包括的リストを示す。

【０１１３】

本開示の実施形態は、サービングネットワークに対して、初期アタッチメッセージを用いてユーザ機器(UE)を識別するために、国際モバイル加入者識別情報(IMSI)ではなくプライバシモバイル加入者識別情報(PMSI)を送るための手段と、サービングネットワークと通信しているサーバによって判定された次のPMSIを含む認証要求をサービングネットワークから受信するための手段であって、次のPMSIは、PMSIから導出される、受信するための手段と、次のPMSIの受信の肯定応答をサービングネットワークを介してサーバに送るための手段とを含むUEを含む。

【０１１４】

UEは、以前のPMSIからPMSIを導出するための手段をさらに含み、以前のPMSIは、初期PMSIを含む。UEは、以前のPMSIからPMSIを導出するための手段をさらに含み、以前のPMSIは、初期PMSIから導出されるPMSI値を含む。UEは、UEによって、初期PMSIに基づいてネットワークアクセスのためのPMSIを判定するための手段をさらに含む。UEは、サーバへのUEの加入者登録中に初期PMSIを受信するための手段をさらに含む。UEは、サーバとの無線通信を介する加入者登録の後に初期PMSIをプロビジョニングするための手段をさらに含む。UEは、提案されるPMSIを生成するための手段と、サーバ公開鍵を使用して、生成されたPMSIを暗号化するための手段であって、サーバは、対応するサーバ秘密鍵を維持する、暗号化するための手段と、初期PMSIとして生成されたPMSIを使用するためにサーバから肯定応答を受信するための手段とをさらに含む。UEは、UEベースの次のPMSIを判定するための手段と、一致があるかどうかを判定するために、UEベースの次のPMSIを認証要求の一部として

受信された次のPMSIと比較するための手段とをさらに含む。UEは、一致があるとの判定に応答して肯定応答トークンを生成するための手段であって、受信の肯定応答は、肯定応答トークンを含む、生成するための手段と、次のアタッチメッセージ内での使用のために、UEにおいて、確認された次のPMSIを記憶するための手段とをさらに含む。UEは、匿名鍵を使用して認証要求内の次のPMSIを暗号化解除するための手段であって、匿名鍵は、UEとサーバとの間で共有される秘密鍵から導出される、暗号化解除するための手段をさらに含む。

【０１１５】

本発明の実施形態は、初期アタッチメッセージからユーザ機器(UE)を識別するために、介在するサービングネットワーク内の1つまたは複数のネットワーク要素を介してUEから、国際モバイル加入者識別情報(IMSI)の代わりにプライバシモバイル加入者識別情報(PMSI)を受信するための手段と、サーバによって、PMSIに基づいて次のPMSIを判定するための手段と、サーバから、次のPMSIを含む認証情報をサービングネットワークに送信するための手段であって、次のPMSIは、認証の一部としてサービングネットワークによってUEに中継される、送信するための手段と、次のPMSIの確認を含む受信の肯定応答をサービングネットワークを介してUEから受信するための手段とを含むサーバをさらに含む。

【０１１６】

サーバは、以前のPMSIから次のPMSIを導出する手段をさらに含み、以前のPMSIは、初期PMSIを含む。サーバは、以前のPMSIから次のPMSIを導出する手段をさらに含み、以前のPMSIは、初期PMSIから導出されるPMSI値を含む。サーバは、サーバによって、初期PMSIに基づいてネットワークアクセスのためのPMSIを判定するための手段をさらに含む。サーバは、サーバにおいて、サーバへのUEの加入者登録中に初期PMSIを受信するための手段をさらに含む。サーバは、UEから、提案される初期PMSIを受信するための手段と、サーバによって、UEにおいて対応するサーバ公開鍵によって暗号化された提案される初期PMSIをサーバ秘密鍵を使用して暗号化解除するための手段と、UEに、初期PMSIとしての提案される初期PMSIの肯定応答を送信するための手段とをさらに含む。サーバは、サーバとUEとの間で共有される秘密鍵から匿名鍵を導出するための手段と、導出された匿名鍵を使用して認証情報内の次のPMSIを暗号化するための手段と、肯定応答の一部として、次のPMSIを肯定応答する肯定応答トークンを受信するための手段と、UEからの後続の初期アタッチメッセージに応答する際の使用のためにサーバにおいてPMSIの代わりに次のPMSIを記憶するための手段とをさらに含む。サーバは、次のPMSIと異なるUEに関連する別の既存のPMSIとの間の衝突を検出するための手段と、PMSIインデックスを増分し、次のPMSIおよび増分されたPMSIインデックスに基づいて新しい次のPMSIを判定するための手段とをさらに含む。サーバは、サーバがその上にあるホームネットワークとは別々のサービングネットワーク上のモビリティ管理エンティティ(MME)から、UEのIMSIの要求を受信するための手段と、要求に応答して、UEのIMSIではなく初期アタッチメッセージ内で使用されたUEのPMSIを送るための手段とをさらに含む。サーバは、初期アタッチメッセージに含まれるPMSIとの一致を1つまたは複数のデータベースから検索するための手段と、一致を突き止めないことに応答して、UEにおける更新されたPMSIの生成のためにUEにおいて維持されるPMSIインデックスをUEが変更するための通知を送るための手段とをさらに含む。

【０１１７】

本開示の実施形態は、ユーザ機器(UE)によって、サービングネットワークにおいてアタッチすべきであると判定するステップと、UEの永久識別子(ID)の代わりに一時IDを含む初期アタッチメッセージをUEからサービングネットワークに送るステップであって、サービングネットワークの認証サーバ(HSS)とのセキュリティイコンテキストは、一時IDに基づいて確立される、送るステップとを含む、UEによるネットワークアクセスのための方法をさらに含む。

【０１１８】

この方法は、サービングネットワークのHSSによって判定された次の一時IDを含む認証要求をHSSから受信するステップであって、次の一時IDは、初期アタッチメッセージ内に

含まれる一時IDから導出される、受信するステップをさらに含む。この方法は、次の一時IDの受信の肯定応答をUEからサービングネットワークを介してHSSに送るステップをさらに含む。

【０１１９】

本発明の実施形態は、一時識別子(ID)を記憶するように構成されたメモリと、サービングネットワークにおいてアタッチすべきであると判定するように構成されたプロセッサと、UEの永久IDの代わりに一時IDを含む初期アタッチメッセージをサービングネットワークに送るように構成されたトランシーバであって、サービングネットワークの認証サーバ(HSS)とのセキュリティイコンテキストは、一時IDに基づいて確立される、トランシーバとを含むユーザ機器をさらに含む。

【０１２０】

UEは、トランシーバが、サービングネットワークのHSSによって判定された次の一時IDを含む認証要求をHSSから受信するようにさらに構成され、次の一時IDが、初期アタッチメッセージ内に含まれる一時IDから導出されることをさらに含む。UEは、プロセッサが、受信の肯定応答を生成するようにさらに構成され、トランシーバが、サービングネットワークを介してHSSに受信の肯定応答を送るようにさらに構成されることをさらに含む。

【０１２１】

本開示の実施形態は、ユーザ機器(UE)の永久識別子(ID)の代わりに一時IDを含む初期アタッチメッセージをUEからサービングネットワークを介して受信するステップと、一時IDに基づいてセキュリティコンテキストを確立するステップとを含む、ネットワーク上のサーバとのネットワークアクセスをセットアップする方法をさらに含む。

【０１２２】

この方法は、初期アタッチメッセージ内に含まれる一時IDに基づいて次の一時IDを判定するステップをさらに含む。この方法は、認証の一部として、次の一時IDを含む認証情報をサーバからサービングネットワークを介してUEに送信するステップをさらに含む。この方法は、次の一時IDの確認を含む受信の肯定応答をUEからサービングネットワークを介して受信するステップをさらに含む。

【０１２３】

本開示の実施形態は、ユーザ機器(UE)の永久識別子(ID)の代わりに一時IDを含む初期アタッチメッセージをUEからサービングネットワークを介して受信するように構成されたトランシーバと、一時IDに基づいてセキュリティコンテキストを確立するように構成されたプロセッサとを含むサーバをさらに含む。

【０１２４】

このサーバは、プロセッサが、初期アタッチメッセージ内に含まれる一時IDに基づいて次の一時IDを判定するようにさらに構成されることをさらに含む。このサーバは、トランシーバが、認証の一部として、次の一時IDを含む認証情報をサービングネットワークを介してUEに送信するようにさらに構成されることをさらに含む。このサーバは、トランシーバが、次の一時IDの確認を含む受信の肯定応答をUEからサービングネットワークを介して受信するようにさらに構成されることをさらに含む。

【０１２５】

当業者は、今はもう、手近な特定の応用例に依存して、本開示の趣旨および範囲から逸脱することなく、多数の修正形態、置換、および変形形態が、本開示のデバイスの材料、装置、構成、および使用の方法においておよびこれらに対して行われ得ることを了解する。このことに照らして、本明細書で図示され記載された特定の実施形態は、それらのいくつかの例によるものにすぎないため、本開示の範囲はそのような特定の実施形態の範囲に限定されるべきではなく、むしろ、下記に添付される特許請求の範囲およびそれらの機能的な均等物の範囲と完全に同じであるべきである。

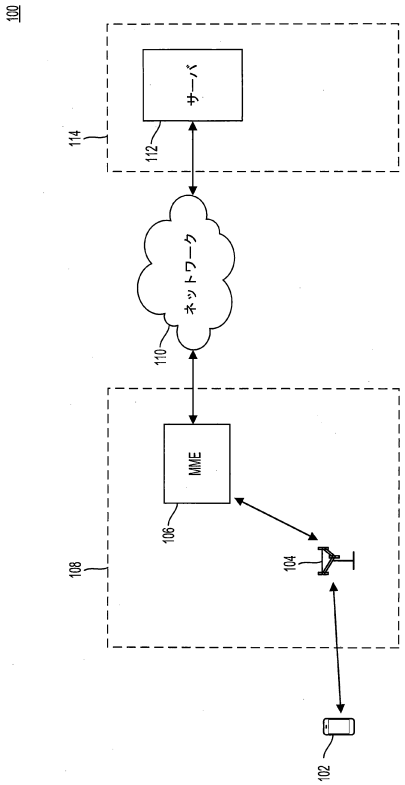
【符号の説明】

【０１２６】

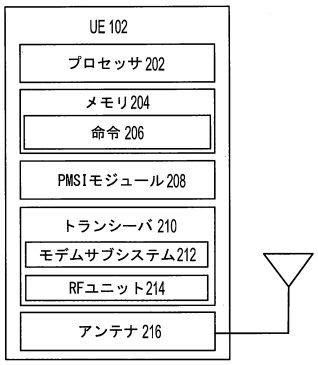
100　ワイヤレス通信ネットワーク

102 UE
104 基地局
106 モビリティ管理エンティティ(MME)
108 サービングネットワーク
110 ネットワーク
112 サーバ
114 ホームネットワーク
202 プロセッサ
204 メモリ
206 命令
208 PMSIモジュール
210 トランシーバ
212 モデムサブシステム
214 無線周波数(RF)ユニット
216 アンテナ
302 プロセッサ
304 メモリ
306 命令
308 PMSIモジュール
310 データベース
312 トランシーバ
400 MIMOシステム
410 送信器システム
412 データソース
414 送信(TX)データプロセッサ
420 TX MIMOプロセッサ
422_aから422_t 送信器(TMTR)、受信器
424_aから424_t アンテナ
430 プロセッサ
432 メモリ
436 データソース
438 TXデータプロセッサ
440 復調器
442 RXデータプロセッサ
450 受信器システムプロセッサ
452_aから452_r アンテナ
454_aから454_r 受信器(RCVR)、送信器
460 RXデータプロセッサ
470 プロセッサ
480 TX MIMOプロセッサ
600 方法
630 方法
700 方法
720 方法

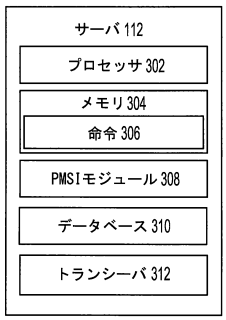
【図１】


100
サーバ
112
114
ネットワーク
110
MME
106
108
104
102

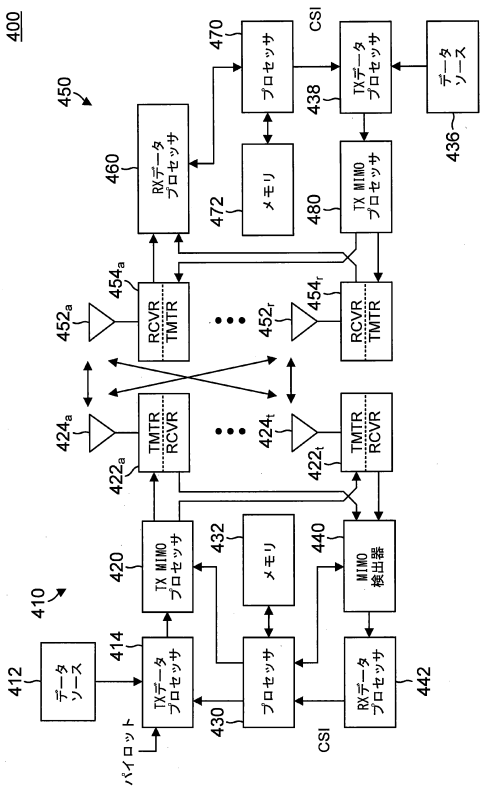
【図２】


UE 102
プロセッサ 202
メモリ 204
命令 206
PMSIモジュール 208
トランシーバ 210
モデムサブシステム 212
RFユニット 214
アンテナ 216

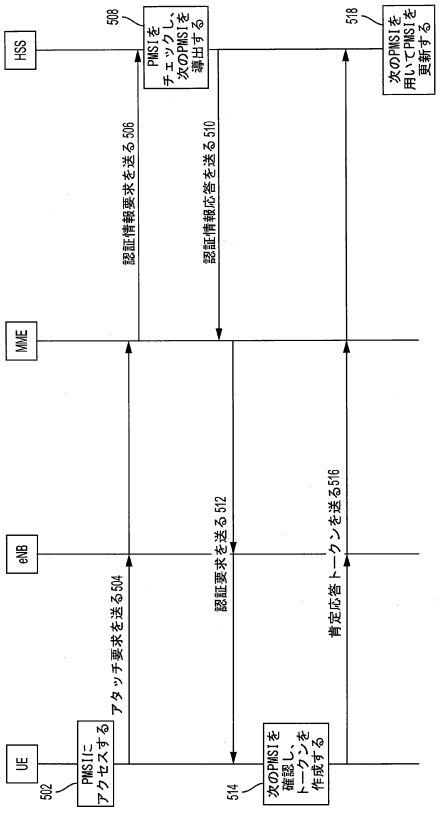
【図３】


サーバ 112
プロセッサ 302
メモリ 304
命令 306
PMSIモジュール 308
データベース 310
トランシーバ 312

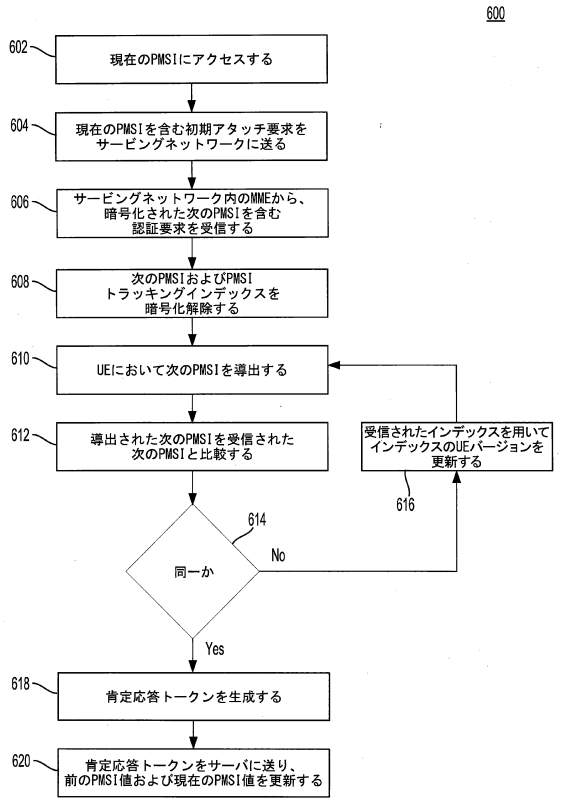
【図４】


400
450
460
RXデータプロセッサ
470
プロセッサ
CSI
438
TXデータプロセッサ
436
データソース
472
メモリ
480
TX MIMOプロセッサ
454a
454r
452a
452r
RCVR TMTR
424a
424t
422a
422t
TMTR RCVR
420
TX MIMOプロセッサ
432
メモリ
440
MIMO検出器
410
412
データソース
414
TXデータプロセッサ
430
プロセッサ
442
RXデータプロセッサ
パイロット
CSI

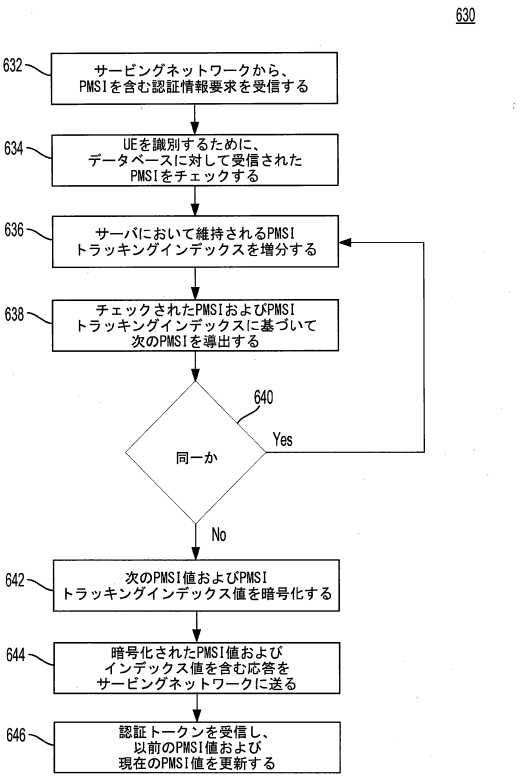
【図５】


HSS
MME
eNB
UE
508
PMSIをチェックし、次のPMSIを導出する
518
次のPMSIを用いてPMSIを更新する
認証情報要求を送る 506
認証情報応答を送る 510
アタッチ要求を送る 504
認証要求を送る 512
肯定応答トークンを送る 516
502
PMSIにアクセスする
514
次のPMSIを確認し、トークンを作成する

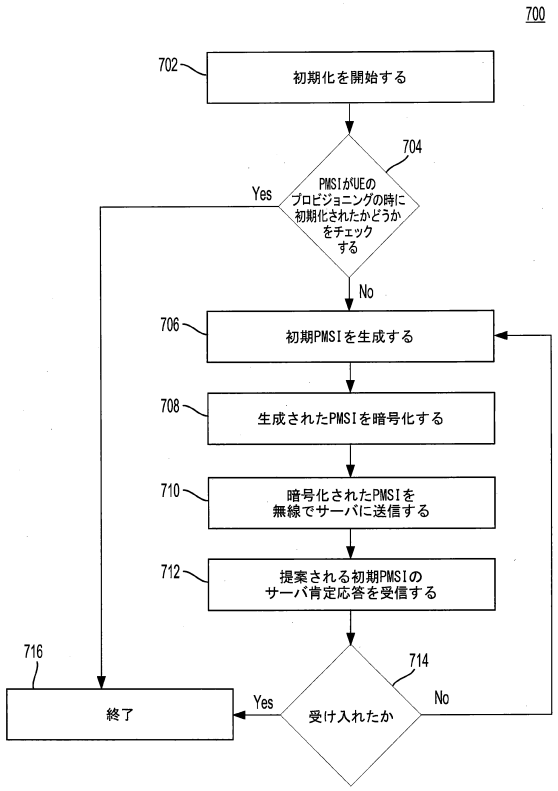
【図６Ａ】



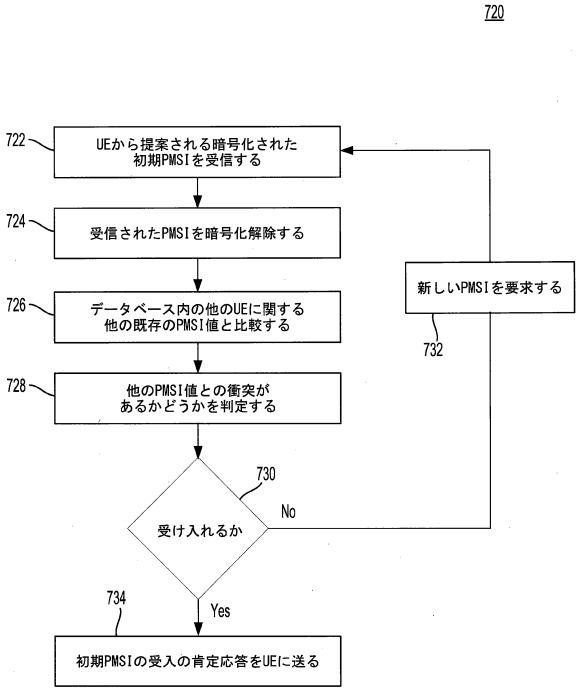
【図６Ｂ】



【図７Ａ】



【図７Ｂ】



フロントページの続き

早期審査対象出願

(72)発明者　アナンド・パラニガウンダー
アメリカ合衆国・カリフォルニア・９２１２１・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者　アドリアン・エドワード・エスコット
アメリカ合衆国・カリフォルニア・９２１２１・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者　ギャヴィン・バーナード・ホーン
アメリカ合衆国・カリフォルニア・９２１２１・サン・ディエゴ・モアハウス・ドライヴ・５７７５

審査官　松野　吉宏

(56)参考文献　特開２００９－０９４９４０（ＪＰ，Ａ）
米国特許出願公開第２００３／００２７５８１（ＵＳ，Ａ１）
国際公開第２０１３／１４０６８４（ＷＯ，Ａ１）
国際公開第２０１１／０３６４８４（ＷＯ，Ａ２）
国際公開第２０１４／０２０２３７（ＷＯ，Ａ１）
米国特許出願公開第２０１３／０３２４０８２（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｂ　７／２４　－　７／２６
Ｈ０４Ｗ　４／００　－　９９／００
３ＧＰＰ　ＴＳＧ　ＲＡＮ　ＷＧ１－４
ＳＡ　ＷＧ１－４
ＣＴ　ＷＧ１、４