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

特許第5392879号
(P5392879)

(45)発行日　平成26年1月22日(2014.1.22)　(24)登録日　平成25年10月25日(2013.10.25)

(51)Int.Cl.		F I	
H04W 12/06	(2009.01)	H04W 12/06	
H04W 12/04	(2009.01)	H04W 12/04	
H04W 4/08	(2009.01)	H04W 4/08	
G06F 21/44	(2013.01)	G06F 21/20	144C

請求項の数 23　(全 37 頁)

(21)出願番号	特願2013-504105 (P2013-504105)
(86)(22)出願日	平成23年4月12日 (2011.4.12)
(65)公表番号	特表2013-527673 (P2013-527673A)
(43)公表日	平成25年6月27日 (2013.6.27)
(86)国際出願番号	PCT/CN2011/072651
(87)国際公開番号	WO2011/127810
(87)国際公開日	平成23年10月20日 (2011.10.20)
審査請求日	平成24年11月21日 (2012.11.21)
(31)優先権主張番号	201010149674.X
(32)優先日	平成22年4月12日 (2010.4.12)
(33)優先権主張国	中国(CN)

(73)特許権者　504277388
▲ホア▼▲ウェイ▼技術有限公司
中華人民共和国５１８１２９広東省深▲セン▼市龍岡区坂田華為本社ビル
(74)代理人　100146835
弁理士　佐伯　義文
(74)代理人　100140534
弁理士　木内　敬二
(72)発明者　▲張▼　▲麗▼佳
中華人民共和国５１８１２９広東省深▲セン▼市龍岡区坂田華為本社ビル
(72)発明者　▲許▼　怡▲シャン▼
中華人民共和国５１８１２９広東省深▲セン▼市龍岡区坂田華為本社ビル

最終頁に続く

(54)【発明の名称】通信デバイスを認証するための方法および装置

(57)【特許請求の範囲】
【請求項１】
マシン型通信MTCデバイスを認証するための方法であって、
グループ識別子を含む、認証されるべきMTCデバイスによって送信されたアタッチ要求を受信するステップと、
前記グループ識別子に結び付けられた第1のグループ認証ベクトルがローカルに存在するかどうかを判定するステップと、
前記グループ識別子に結び付けられた前記第1のグループ認証ベクトルが存在する場合に、前記第1のグループ認証ベクトルにしたがって、認証されるべき前記MTCデバイスを認証し、認証されるべき前記MTCデバイスに関するシステム鍵を生成するステップと、
を含み、
前記グループ識別子は、認証されるべき前記MTCデバイスが位置するMTCグループのグループ識別子であり、
前記第1のグループ認証ベクトルは、前記MTCグループ内のMTCデバイスを認証するために使用される認証ベクトルであることを特徴とする方法。
【請求項２】
前記第1のグループ認証ベクトルが存在しない場合に、
前記グループ識別子にしたがってサーバから前記第1のグループ認証ベクトルを取得するステップと、
前記グループ識別子と取得された第1のグループ認証ベクトルの間の結び付けの関係を

確立するステップと、
前記第1のグループ認証ベクトルにしたがって、認証されるべき前記MTCデバイスを認証し、認証されるべき前記MTCデバイスに関するシステム鍵を生成するステップと、
をさらに含むことを特徴とする請求項1に記載の方法。
【請求項３】
前記方法が、ユニバーサル移動体通信システムUMTSネットワークに適用されるとともに、前記方法が、前記UMTSネットワークの在圏ロケーションレジスタVLRによって実行され、前記サーバが、前記UMTSネットワークのホームロケーションレジスタHLRであるか、または
前記方法が、ロングタームエボリューションLTEネットワークに適用されるとともに、前記方法が、前記LTEネットワークのモビリティ管理エンティティMMEによって実行され、前記サーバが、前記LTEネットワークのホーム加入者システムHSSであることを特徴とする請求項2に記載の方法。
【請求項４】
前記MTCグループ内の各MTCデバイスは、デバイス特性を有し、
前記デバイス特性は、前記MTCグループ内の前記MTCデバイスを一意的に識別するために使用され、
前記アタッチ要求は、認証されるべき前記MTCデバイスを識別するために使用される第2のデバイス特性をさらに含み、
前記グループ識別子に結び付けられた前記第1のグループ認証ベクトルがローカルに存在するかどうかを判定する前記ステップの後、前記方法が、
前記第2のデバイス特性が、ローカルに記憶された第1のデバイス特性と同じであるかどうかを判定するステップと、
前記第2のデバイス特性が前記ローカルに記憶された第1のデバイス特性と異なる場合に、前記第1のグループ認証ベクトルにしたがって、認証されるべき前記MTCデバイスを認証し、認証されるべき前記MTCデバイスの前記システム鍵を生成する前記ステップを実行するステップと、
をさらに含み、
前記第1のデバイス特性は、前記グループ識別子と前記第1のグループ認証ベクトルの両方に結び付けられたデバイス特性であることを特徴とする請求項1から3のいずれか一項に記載の方法。
【請求項５】
認証されるべき前記MTCデバイスの前記第2のデバイス特性が前記ローカルに記憶された第1のデバイス特性と同じである場合に、
前記MTCグループ内の前記MTCデバイスを認証するために使用される第2のグループ認証ベクトルを、前記グループ識別子にしたがって取得するステップと、
前記グループ識別子と、前記第2のデバイス特性と、取得された第2のグループ認証ベクトルとの間の結び付けの関係を確立するステップと、
前記取得された第2のグループ認証ベクトルおよび前記第2のデバイス特性よって生成された期待される応答番号にしたがって、認証されるべき前記MTCデバイスを認証し、認証されるべき前記MTCデバイスのシステム鍵を生成するステップと、
をさらに含むことを特徴とする請求項4に記載の方法。
【請求項６】
前記第1のグループ認証ベクトルにしたがって、認証されるべき前記MTCデバイスを認証し、認証されるべき前記MTCデバイスの前記システム鍵を生成する前記ステップが、
前記第1のグループ認証ベクトルおよび前記第2のデバイス特性にしたがって期待される応答番号を生成するステップと、
認証されるべき前記MTCデバイスが、グループ認証情報にしたがってネットワークを認証し、前記第2のデバイス特性にしたがってデバイス側の鍵を生成するように、認証されるべき前記MTCデバイスに前記グループ認証情報を送信するステップと、

認証されるべき前記MTCデバイスによって前記第2のデバイス特性にしたがって生成された応答番号を受信するステップと、
前記応答番号および前記期待される応答番号にしたがって、認証されるべき前記MTCデバイスを認証するステップと、
前記第1のグループ認証ベクトルおよび前記第2のデバイス特性にしたがってネットワーク側の鍵を生成するステップと、
を含み、
前記グループ認証情報は、前記第1のグループ認証ベクトル内の情報であることを特徴とする請求項4または5に記載の方法。
【請求項７】
MTCデバイスを認証するための方法であって、
MTCグループ内のプライマリMTCデバイスとネットワーク側の間の認証が成功した後、前記MTCグループ内の第2のMTCデバイスによって送信されたアタッチ要求を受信するステップと、
前記プライマリMTCデバイスによって、前記第2のMTCデバイスを認証し、前記グループ認証ベクトルを使用することによって前記第2のMTCデバイスに関するシステム鍵を生成するステップと、
前記プライマリMTCデバイスによって、前記システム鍵を前記第2のMTCデバイスに送信するステップと、
を含み、
前記プライマリMTCデバイスと前記ネットワーク側の間の認証のプロセスで生成された認証ベクトルは、前記MTCグループのグループ認証ベクトルとみなされることを特徴とする方法。
【請求項８】
前記MTCグループ内の前記プライマリMTCデバイスと前記ネットワーク側の間の認証が成功した後、
前記グループ認証ベクトルと前記MTCグループのグループ識別子の間の結び付けの関係を確立するステップをさらに含み、
前記第2のMTCデバイスによって送信された前記アタッチ要求を受信する前記ステップが、前記グループ識別子および前記第2のMTCデバイスのデバイス特性を含むとともに、前記第2のMTCデバイスによって送信された前記アタッチ要求を受信するステップを含み、
前記プライマリMTCデバイスと前記ネットワーク側の間の認証の前記プロセスで生成された前記グループ認証ベクトルを使用することによって前記第2のMTCデバイスに関する前記システム鍵を生成する前記ステップが、前記アタッチ要求で伝達された前記グループ識別子に結び付けられた前記グループ認証ベクトルを取得するステップと、
前記グループ認証ベクトルおよび前記第2のMTCデバイスの前記デバイス特性を使用することによって前記第2のMTCデバイスに関する前記システム鍵を生成するステップと、
を含むことを特徴とする請求項7に記載の方法。
【請求項９】
前記グループ識別子および前記第2のMTCデバイスの前記デバイス特性を含み、前記第2のMTCデバイスによって送信された前記アタッチ要求を受信する前記ステップの後、
前記ネットワーク側が、前記グループ認証ベクトルおよび前記第2のMTCデバイスの前記デバイス特性を使用することによって前記第2のMTCデバイスに関する前記システム鍵を生成するように、前記アタッチ要求を前記ネットワーク側に転送するステップをさらに含むことを特徴とする請求項8に記載の方法。
【請求項１０】
MTCデバイスを認証するための方法であって、
MTCグループ内のプライマリMTCデバイスによって、ネットワーク側にアタッチ要求を送信するステップと、
前記プライマリMTCデバイスと前記ネットワーク側の間の認証を実行し、認証プロセス

で生成されたグループ認証ベクトル、および認証されるべき前記その他のMTCデバイスの前記デバイス特性を使用することによって、認証されるべき前記その他のMTCデバイスに関するシステム鍵を生成するステップと、
前記プライマリMTCデバイスが、認証されるべき前記その他のMTCデバイスを正常に認証した後、前記プライマリMTCデバイスによって、認証されるべき前記その他のMTCデバイスに前記システム鍵を送信するステップと、
を含み、
前記アタッチ要求が、前記MTCグループのグループ識別子、および前記MTCグループ内の認証されるべきその他のMTCデバイスのデバイス特性を含むことを特徴とする方法。
【請求項１１】
前記アタッチ要求が、前記プライマリMTCデバイスのデバイス特性をさらに含み、
前記プライマリMTCデバイスと前記ネットワーク側の間で前記認証を実行する前記ステップは、前記プライマリMTCデバイスの前記デバイス特性にしたがって前記プライマリMTCデバイスと前記ネットワーク側の間の認証を実行するとともに、前記プライマリMTCデバイスのシステム鍵を生成するステップを含むことを特徴とする請求項10に記載の方法。
【請求項１２】
グループ識別子を含む、認証されるべきMTCデバイスによって送信されたアタッチ要求を受信するように構成された第1の受信ユニットと、
前記第1の受信ユニットによって受信された前記グループ識別子に結び付けられた第1のグループ認証ベクトルが存在するときに、前記第1のグループ認証ベクトルにしたがって、認証されるべき前記MTCデバイスを認証し、認証されるべき前記MTCデバイスのシステム鍵を生成するように構成された第1の認証ユニットと、
を含み、
前記グループ識別子は、認証されるべき前記MTCデバイスが位置するMTCグループのグループ識別子であることを特徴とするネットワーク側のエンティティ。
【請求項１３】
前記第1のグループ認証ベクトルが存在しないときに、前記第1の受信ユニットによって受信された前記グループ識別子にしたがってサーバから前記第1のグループ認証ベクトルを取得するように構成された第1の取得ユニットと、
前記第1の受信ユニットによって受信された前記グループ識別子と、前記第1の取得ユニットによって取得された前記第1のグループ認証ベクトルとの間の結び付けの関係を確立するように構成された第1の確立ユニットと、
前記第1の取得ユニットによって取得された前記第1のグループ認証ベクトルにしたがって、認証されるべき前記MTCデバイスを認証し、認証されるべき前記MTCデバイスのシステム鍵を生成するように構成された第2の認証ユニットと、
をさらに含むことを特徴とする請求項12に記載のネットワーク側のエンティティ。
【請求項１４】
前記第1の受信ユニットによって受信された前記アタッチ要求が認証されるべき前記MTCデバイスを識別するために使用される第2のデバイス特性をさらに含む場合に、前記第2のデバイス特性が、ローカルに記憶された第1のデバイス特性と同じであるかどうかを判定するように構成された判定ユニットをさらに含み、
前記第1のデバイス特性は、前記グループ識別子と前記第1のグループ認証ベクトルの両方に結び付けられたデバイス特性であることを特徴とする請求項12または13に記載のネットワーク側のエンティティ。
【請求項１５】
認証されるべき前記MTCデバイスの前記第2のデバイス特性が、前記ローカルに記憶された第1のデバイス特性と同じであるとき、前記第1の受信ユニットによって受信された前記グループ識別子にしたがって、前記MTCグループ内のMTCデバイスを認証するために使用される第2のグループ認証ベクトルを取得するように構成された第2の取得ユニットと、
前記第1の受信ユニットによって受信された前記グループ識別子と、前記第2のデバイス

特性と、前記第2の取得ユニットによって取得された前記第2のグループ認証ベクトルとの間の結び付けの関係を確立するように構成された第2の確立ユニットと、
前記第2の取得ユニットによって取得された前記第2のグループ認証ベクトルおよび前記第1の受信ユニットによって受信された前記第2のデバイス特性によって生成された期待される応答番号にしたがって、認証されるべき前記MTCデバイスを認証し、認証されるべき前記MTCデバイスのシステム鍵を生成するように構成された第3の認証ユニットと、
をさらに含むことを特徴とする請求項14に記載のネットワーク側のエンティティ。
【請求項１６】
前記第1の認証ユニットが、
前記第1のグループ認証ベクトルおよび前記第1の受信ユニットによって受信された前記第2のデバイス特性にしたがって期待される応答番号を生成するように構成された第1の生成ユニットと、
認証されるべき前記MTCデバイスが、グループ認証情報にしたがってネットワークを認証し、前記第2のデバイス特性にしたがってデバイス側の鍵を生成するように、認証されるべき前記MTCデバイスに前記グループ認証情報を送信するように構成された第1の送信ユニットと、
認証されるべき前記MTCデバイスによって前記第2のデバイス特性にしたがって生成された応答番号を受信するように構成された第2の受信ユニットと、
前記第2の受信ユニットによって受信された前記応答番号および前記第1の生成ユニットによって生成された前記期待される応答番号にしたがって、認証されるべき前記MTCデバイスを認証するように構成された第1の認証サブユニットと、
前記第1のグループ認証ベクトルおよび前記第1の受信ユニットによって受信された前記第2のデバイス特性にしたがってネットワーク側の鍵を生成するように構成された第2の生成ユニットと、
を含み、
前記グループ認証情報は、前記第1のグループ認証ベクトル内の情報であることを特徴とする請求項14または15に記載のネットワーク側のエンティティ。
【請求項１７】
前記ネットワーク側のエンティティが、ユニバーサル移動体通信システムUMTSネットワークの在圏ロケーションレジスタVLRまたはロングタームエボリューションLTEネットワークのモビリティ管理エンティティMMEであることを特徴とする請求項12から16のいずれか一項に記載のネットワーク側のエンティティ。
【請求項１８】
MTCデバイスを認証するためのデバイスであって、
デバイスとネットワーク側の間の認証が成功した後、デバイスが位置するMTCグループ内の第2のMTCデバイスによって送信されたアタッチ要求を受信するように構成された第3の受信ユニットと、
前記第2のMTCデバイスを認証し、デバイスと前記ネットワーク側の間の認証のプロセスで生成されたグループ認証ベクトルを使用することによって前記第2のMTCデバイスに関するシステム鍵を生成するように構成された第4の認証ユニットと、
前記第4の認証ユニットによって生成された前記システム鍵を前記第2のMTCデバイスに送信するように構成された第2の送信ユニットと、
を含むことを特徴とするデバイス。
【請求項１９】
前記デバイスと前記ネットワーク側の間の前記認証が成功した後、前記グループ認証ベクトルと、前記MTCグループのグループ識別子との間の結び付けの関係を確立するように構成された第3の確立ユニットをさらに含むことを特徴とする請求項18に記載のデバイス。
【請求項２０】
前記第3の受信ユニットによって受信された前記アタッチ要求が、前記グループ識別子

および前記第2のMTCデバイスのデバイス特性を含むとき、前記第4の認証ユニットが、
前記第3の受信ユニットによって受信された前記グループ識別子に結び付けられた前記グループ認証ベクトルを取得するように構成された第3の取得ユニットと、
前記第3の取得ユニットによって取得された前記グループ認証ベクトルおよび前記第3の受信ユニットによって受信される前記第2のMTCデバイスの前記デバイス特性を使用することによって前記第2のMTCデバイスに関するシステム鍵を生成するように構成された第3の生成ユニットと、
を含むことを特徴とする請求項19に記載のデバイス。
【請求項２１】
前記ネットワーク側が、前記グループ認証ベクトルおよび前記第2のMTCデバイスの前記デバイス特性を使用することによって前記第2のMTCデバイスに関する前記システム鍵を生成するように、前記第3の受信ユニットによって受信された前記アタッチ要求を前記ネットワーク側に転送するように構成された転送ユニットをさらに含むことを特徴とする請求項20に記載のデバイス。
【請求項２２】
MTCデバイスを認証するためのデバイスであって、
アタッチ要求をネットワーク側に送信するように構成された第3の送信ユニットと、
デバイスと前記ネットワーク側の間で相互認証を実行し、グループ認証ベクトルおよび認証されるべき前記MTCデバイスの前記デバイス特性を使用することによって、認証されるべき前記MTCデバイスに関するシステム鍵を生成するように構成された第5の認証ユニットと、
デバイスが、認証されるべき前記MTCデバイスを正常に認証した後、前記第5の認証ユニットによって生成された前記システム鍵を認証されるべき前記MTCデバイスに送信するように構成された第4の送信ユニットと、
を含み、
前記アタッチ要求は、デバイスが位置するMTCグループのグループ識別子、および前記MTCグループ内の認証されるべきMTCデバイスのデバイス特性を含み、
前記グループ認証ベクトルが、デバイスと前記ネットワーク側の間の認証のプロセスで生成されることを特徴とするデバイス。
【請求項２３】
前記第3の送信ユニットによって送信された前記アタッチ要求が前記デバイスのデバイス特性を含むときに、前記デバイスの前記デバイス特性にしたがって前記デバイスのシステム鍵を生成するように構成された第4の生成ユニットをさらに含むことを特徴とする請求項22に記載のデバイス。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、無線通信の分野に関し、具体的には、通信デバイスを認証するための方法および装置に関する。
【０００２】
本出願は、2010年4月12日に中国専利局に出願され、「METHOD AND APPARATUS FOR AUTHENTICATING COMMUNICATION DEVICE」と題された中国特許出願第201010149674.X号の優先権を主張するものであり、この中国特許出願は、参照によりその全体が本明細書に組み込まれる。
【背景技術】
【０００３】
マシン型通信(Machine Type Communication, MTC)デバイスは、MTCデバイスとネットワーク側の間の相互認証が成功した後にだけネットワーク側と通信することができる。第3世代パートナーシッププロジェクト(3rd Generation Partnership Project, 3GPP)規格においては、グループに基づく属性が、MTCデバイスの分散に対して提示され、つまり、同

じ地理的位置に位置するMTCデバイスが同じ属性を有するか、または同じユーザに属するMTCデバイスがグループとみなされる可能性がある。MTCデバイスのグループは、直接ネットワークにアクセスすることができ、ゲートウェイを通じてネットワークにアクセスすることもできる。

【０００４】

従来技術において、各MTCデバイスは、国際移動体加入者識別番号(International Mobile Subscriber Identity, IMSI)を有し、識別情報IMSIは、一意的である。MTCデバイスとネットワーク側の間の相互認証のプロセスにおいて、ネットワーク側は、MTCデバイスの一意的なIMSIに対応する基本鍵(basic key)Kにしたがって認証ベクトル(Authentication Vector, AV)を生成し、AVにしたがってMTCデバイスとネットワーク側の間の相互認証を完了する。異なるMTCデバイスは、相互認証を完了するために、異なるIMSIに対応する異なる基本鍵Kを使用することによって異なる認証ベクトルAVを生成する。

【０００５】

MTCデバイスの数が多いので、既存の認証方法が採用される場合、多数のMTCデバイスが短期間にネットワークにアクセスするとき、認証プロセス中に生成されるシグナリングのトラフィックが、急速に増大し、ネットワークの混雑をもたらす。

【発明の概要】

【発明が解決しようとする課題】

【０００６】

本発明の実施形態は、多数のMTCデバイスが短期間にネットワークにアクセスする場合に各MTCデバイスが効果的に認証され得るように、通信デバイスを認証するための方法および装置を提供する。

【課題を解決するための手段】

【０００７】

上述の目的を達成するために、本発明の実施形態は、以下の技術的な解決策を採用する。

【０００８】

MTCデバイスを認証するための方法は、

グループ識別子を含み、認証されるべきMTCデバイスによって送信されたアタッチ要求を受信するステップであって、グループ識別子が、認証されるべきMTCデバイスが位置するMTCグループのグループ識別子である、ステップと、

グループ識別子に結び付けられた第1のグループ認証ベクトルがローカルに存在するかどうかを判定するステップと、

存在する場合に、第1のグループ認証ベクトルにしたがって、認証されるべきMTCデバイスを認証し、認証されるべきMTCデバイスのシステム鍵(system key)を生成するステップと、を含む。

【０００９】

MTCデバイスを認証するための方法は、

MTCグループ内のプライマリMTCデバイス(primary MTC device)とネットワーク側の間の認証が成功した後、MTCグループ内の第2のMTCデバイスによって送信されたアタッチ要求を受信するステップと、

第2のMTCデバイスを認証し、プライマリMTCデバイスとネットワーク側の間の認証のプロセスで生成されたグループ認証ベクトルを使用することによって第2のMTCデバイスに関するシステム鍵を生成するステップと、

システム鍵を第2のMTCデバイスに送信するステップと、を含む。

【００１０】

MTCデバイスを認証するための方法は、

MTCグループ内のプライマリMTCデバイスによって、ネットワーク側にアタッチ要求を送信するステップであって、アタッチ要求が、MTCグループのグループ識別子、およびMTCグループ内の認証されるべきその他のMTCデバイスのデバイス特性を含む、ステップと、

プライマリMTCデバイスとネットワーク側の間の認証を実行し、認証されるべきその他のMTCデバイスのデバイス特性およびグループ認証ベクトルを使用することによって、認証されるべきその他のMTCデバイスに関するシステム鍵を生成するステップであって、グループ認証ベクトルが、プライマリMTCデバイスとネットワーク側の間の認証のプロセスで生成される、ステップと、

プライマリMTCデバイスが、認証されるべきその他のMTCデバイスを正常に認証した後、プライマリMTCデバイスによって、認証されるべきその他のMTCデバイスにシステム鍵を送信するステップと、を含む。

【００１１】

ネットワーク側のエンティティは、

グループ識別子を含み、認証されるべきMTCデバイスによって送信されたアタッチ要求を受信するように構成された第1の受信ユニットであって、グループ識別子が、認証されるべきMTCデバイスが位置するMTCグループのグループ識別子である、第1の受信ユニットと、

第1の受信ユニットによって受信されたグループ識別子に結び付けられた第1のグループ認証ベクトルが存在するときに、第1のグループ認証ベクトルにしたがって、認証されるべきMTCデバイスを認証し、認証されるべきMTCデバイスのシステム鍵を生成するように構成された第1の認証ユニットと、を含む。

【００１２】

MTCデバイスを認証するためのデバイスは、

デバイスとネットワーク側の間の認証が成功した後、デバイスが位置するMTCグループ内の第2のMTCデバイスによって送信されたアタッチ要求を受信するように構成された第3の受信ユニットと、

第2のMTCデバイスを認証し、デバイスとネットワーク側の間の認証のプロセスで生成されたグループ認証ベクトルを使用することによって第2のMTCデバイスに関するシステム鍵を生成するように構成された第4の認証ユニットと、

第4の認証ユニットによって生成されたシステム鍵を第2のMTCデバイスに送信するように構成された第2の送信ユニットと、を含む。

【００１３】

MTCデバイスを認証するためのデバイスは、

アタッチ要求をネットワーク側に送信するように構成された第3の送信ユニットであって、アタッチ要求は、デバイスが位置するMTCグループのグループ識別子、およびMTCグループ内の認証されるべきMTCデバイスのデバイス特性を含む、第3の送信ユニットと、

デバイスとネットワーク側の間で相互認証を実行し、グループ認証ベクトル、および認証されるべきMTCデバイスのデバイス特性を使用することによって、認証されるべきMTCデバイスに関するシステム鍵を生成するように構成された第5の認証ユニットであって、グループ認証ベクトルが、デバイスとネットワーク側の間の認証のプロセスで生成される、第5の認証ユニットと、

デバイスが、認証されるべきMTCデバイスを正常に認証した後、第5の認証ユニットによって生成されたシステム鍵を認証されるべきMTCデバイスに送信するように構成された第4の送信ユニットと、を含む。

【００１４】

本発明の実施形態において提供されるMTCデバイスを認証するための方法および装置においては、グループ認証ベクトルが、MTCグループによって共有されるグループ識別子を通じて取得され、グループ内の認証されるべきMTCデバイスが、グループ認証ベクトルを通じて認証されるか、またはシステム鍵が、グループ認証ベクトルを通じてグループ内の認証されたMTCデバイスに対して生成され、それによって、認証プロセスまたはシステム鍵を生成するプロセスにおいて異なるMTCデバイスに対して異なる認証ベクトルが生成されることが必要であるという問題を回避し、したがって、シグナリングのトラフィックが大幅に削減され、多数のMTCデバイスが短期間にネットワークにアクセスする場合であっ

てもネットワークの混雑が引き起こされない。本発明の実施形態で提供されるMTCデバイスを認証するための方法および装置によって、多数のMTCデバイスが短期間にネットワークにアクセスする場合に、各MTCデバイスが、やはり効果的に認証され得る。

【図面の簡単な説明】

【００１５】

【図１】グループに基づくMTCデバイスがネットワークにアクセスする第1のシナリオの図である。

【図２】グループに基づくMTCデバイスがネットワークにアクセスする第2のシナリオの図である。

【図３】グループに基づくMTCデバイスがネットワークにアクセスする第3のシナリオの図である。

【図４】本発明の第1の実施形態によるMTCデバイスを認証するための方法の流れ図である。

【図５】本発明の第1の実施形態がUMTSネットワークに適用される概略的な流れ図である。

【図６】本発明の第1の実施形態がLTEネットワークに適用される概略的な流れ図である。

【図７】本発明の第2の実施形態によるMTCデバイスを認証するための方法の流れ図である。

【図８】本発明の第2の実施形態がUMTSネットワークに適用される概略的な流れ図である。

【図９】本発明の第2の実施形態がLTEネットワークに適用される概略的な流れ図である。

【図１０】本発明の第3の実施形態によるMTCデバイスを認証するための方法の流れ図である。

【図１１】本発明の第3の実施形態がUMTSネットワークに適用される概略的な流れ図である。

【図１２】本発明の第3の実施形態がLTEネットワークに適用される概略的な流れ図である。

【図１３】本発明の第4の実施形態によるMTCデバイスを認証するための方法の流れ図である。

【図１４】本発明の第4の実施形態がUMTSネットワークに適用される概略的な流れ図である。

【図１５】本発明の第4の実施形態がLTEネットワークに適用される概略的な流れ図である。

【図１６】本発明の一実施形態によるネットワーク側のエンティティの第1の概略的な構造図である。

【図１７】本発明の一実施形態によるネットワーク側のエンティティの第2の概略的な構造図である。

【図１８】本発明の一実施形態によるネットワーク側のエンティティの第3の概略的な構造図である。

【図１９】本発明の一実施形態によるネットワーク側のエンティティの概略的な構造図内の第1の認証ユニット1302の概略的な構造図である。

【図２０】本発明の一実施形態によるMTCデバイスを認証するためのデバイスの第1の概略的な構造図である。

【図２１】本発明の一実施形態によるMTCデバイスを認証するためのデバイスの第2の概略的な構造図である。

【図２２】本発明の一実施形態によるMTCデバイスを認証するためのデバイスの第4の認証ユニット1402の概略的な構造図である。

【図２３】本発明の一実施形態によるMTCデバイスを認証するためのデバイスの第3の概略的な構造図である。

【図２４】本発明の別の実施形態によるMTCデバイスを認証するためのデバイスの概略的

な構造図である。
【図２５】本発明の別の実施形態によるネットワーク側のエンティティの概略的な構造図である。
【発明を実施するための形態】
【００１６】
図1、図2、および図3は、本発明の実施形態が基づくMTCグループの3つのあり得るシナリオを示し、番号1がMTCデバイスを表し、番号2がMTCゲートウェイを表す。図1において、MTCデバイス1のグループは、3GPPネットワークに直接アクセスする。MTCゲートウェイは、ネットワークアーキテクチャで必要とされず、各MTCデバイスは、相互認証がMTCデバイスとネットワークの間で実行された後にだけネットワークと通信することができる。図2において、MTCデバイスのグループは、MTCゲートウェイ2を通じて3GPPネットワークにアクセスするが、ネットワーク側は、ゲートウェイに接続された各MTCデバイスを識別することができる。つまり、ネットワーク側からすると、MTCゲートウェイは、通常のMTCデバイスと等価であり、通常のMTCデバイスのすべての機能を有する。グループ内の各MTCデバイスからすると、MTCゲートウェイは、グループ内のその他のMTCデバイスに外部接続チャネルを提供する。各MTCデバイスおよびMTCゲートウェイは、認証が成功した後にだけネットワーク側と通信することができる。図3において、MTCデバイスのグループは、MTCゲートウェイ2を通じて3GPPネットワークにアクセスするが、ネットワーク側は、MTCゲートウェイだけを識別することができるが、ゲートウェイに接続されたMTCデバイスを識別することはできない。MTCゲートウェイは、相互認証がMTCデバイスとネットワークの間で実行された後にだけネットワークと通信することができる。MTCゲートウェイ2は、ゲートウェイ機能を有するMTCデバイスである可能性がある。
【００１７】
従来技術において多数のMTCデバイスがネットワークにアクセスする場合にシグナリングのトラフィックの増大によって引き起こされるネットワークの混雑の問題を解決するために、本発明の実施形態は、通信デバイスを認証するための方法および装置を提供する。
【００１８】
図4に示されるように、本発明の第1の実施形態によるMTCデバイスを認証するための方法は、以下を含む。
【００１９】
ステップ101: グループ識別子を含み、認証されるべきMTCデバイスによって送信されたアタッチ要求を受信し、グループ識別子は、認証されるべきMTCデバイスが位置するMTCグループのグループ識別子である。
【００２０】
この実施形態において、認証されるべきMTCデバイスは、ネットワークと通信する必要があり、MTCグループ内にあるMTCデバイスである。MTCデバイスがネットワークにアクセスする前に、MTCデバイスとネットワークの間の相互認証が実行される必要があり、システム鍵が生成される必要がある。この実施形態においては、グループ識別子が、各MTCグループに対して設定され、グループ識別子は、一意的であり、Group IMSIによって表される可能性があり、異なるMTCグループは、異なるGroup IMSIを有する。
【００２１】
ステップ102: グループ識別子に結び付けられた（bound）第1のグループ認証ベクトルがローカルに存在するかどうかを判定する。
【００２２】
この実施形態において、グループ認証ベクトルは、MTCグループ内のMTCデバイスを認証するために使用される認証ベクトルを指し、MTCグループ内の認証されるべき複数のMTCデバイスが、認証のためのグループ認証ベクトルを共有することができる。第1のグループ認証ベクトルは、MTCデバイスが、ネットワークにアクセスする最初のMTCデバイスであり、MTCグループ内にある場合に、当該MTCデバイスとネットワークの間の相互認証のプロセスにおいて生成される。第1のグループ認証ベクトルは、同じMTCグループに属する別のMT

Cデバイスが、ネットワークにアクセスする必要があるときにグループ認証ベクトルを素早く発見することができ、グループ認証ベクトルを再生成する必要がないように、グループ識別子に結び付けられる。ネットワークにアクセスする最初のMTCデバイスであるMTCデバイスは、MTCグループ内のMTCデバイスがそれまでネットワークにアクセスしていない場合に、ネットワークにアタッチ要求を送信する最初のMTCデバイスであるMTCデバイスを指す。

【００２３】

ステップ103: 存在する場合に、第1のグループ認証ベクトルにしたがって、認証されるべきMTCデバイスを認証し、認証されるべきMTCデバイスのシステム鍵を生成する。

【００２４】

この実施形態において、認証されるべきMTCデバイスのシステム鍵は、ネットワーク側の鍵およびデバイス側の鍵を含む。

【００２５】

本発明の実施形態において提供されるMTCデバイスを認証するための方法においては、グループ認証ベクトルが、MTCグループによって共有されるグループ識別子を通じて取得され、グループ内の認証されるべきMTCデバイスが、グループ認証ベクトルを通じて認証され、システム鍵が生成され、それによって、認証し、システム鍵を生成するプロセスにおいて異なるMTCデバイスに対して異なる認証ベクトルが生成されることが必要であるという問題を回避し、したがって、シグナリングのトラフィックが大幅に削減され、多数のMTCデバイスが短期間にネットワークにアクセスする場合であってもネットワークの混雑が避けられる。また、1つのグループ識別子を共有することは、15ビットのIMSIがMTCデバイスの数が多いときに使用するのに不十分であるという問題も解決する。本発明の実施形態で提供されるMTCデバイスを認証するための方法によって、多数のMTCデバイスが短期間にネットワークにアクセスする場合に、各MTCデバイスが、効果的に認証され得る。

【００２６】

さらに、ステップ102において、グループ識別子に結び付けられた第1のグループ認証ベクトルがローカルに存在しないと判定される場合、第1のグループ認証ベクトルを取得することが必要とされ、これは、具体的には、以下のステップを含む。

【００２７】

ステップ1021: グループ識別子にしたがってサーバから第1のグループ認証ベクトルを取得する。

【００２８】

この実施形態において、サーバは、ネットワーク側の特定のサーバである。例えば、ユニバーサル移動体通信システム(Universal Mobile Telecommunication System, UMTS)ネットワークにおいては、サーバは、ホームロケーションレジスタ(Home Location Register, HLR)であり、ロングタームエボリューション(Long Term Evolution, LTE)ネットワークにおいては、サーバは、ホーム加入者システム(Home Subscriber System, HSS)である。

【００２９】

ステップ1022: グループ識別子と取得された第1のグループ認証ベクトルの間の結び付け(binding)の関係を確立する。

【００３０】

この実施形態において、結び付けの関係を確立する目的は、取得された第1のグループ認証ベクトルが、同じMTCグループ内のその他のMTCデバイスを認証し、システム鍵を生成するために直接使用可能であり、毎回再取得されることを必要としないことを可能にすることである。

【００３１】

さらに、ステップ101で受信されるアタッチ要求は、第2のデバイス特性（device characteristic）も含み得る。MTCグループにおいて、デバイス特性は、MTCグループ内でMTCデバイスを一意的に識別することができる。第2のデバイス特性は、認証されるべきMTCデバ

イスを識別するために使用されるパラメータである。第2のデバイス特性は、認証されるべきMTCデバイスの位置パラメータである可能性があり、認証されるべきMTCデバイスを一意的に識別することができる別のパラメータである可能性もある。アタッチ要求が第2のデバイス特性を含むとき、および第1のグループ認証ベクトルがローカルに存在すると判定された後、方法は、さらに以下のステップを含む。

【００３２】

第2のデバイス特性が、ローカルに記憶された第1のデバイス特性と同じであるかどうかが判定され、第1のデバイス特性は、最初にネットワークにアクセスし、MTCグループ内にあるMTCデバイスのデバイス特性であり、第1のデバイス特性は、グループ識別子および第1のグループ認証ベクトルに結び付けられており、第2のデバイス特性は、グループ内の別のMTCデバイスのデバイス特性である。第2のデバイス特性が、ローカルに記憶された第1のデバイス特性と異なるとき、つまり、認証されるべきMTCデバイスが、ネットワークにアクセスする最初のMTCデバイスであるMTCデバイスではないときは、第1のグループ認証ベクトルにしたがって、認証されるべきMTCデバイスが認証され、認証されるべきMTCデバイスのシステム鍵が生成される。第2のデバイス特性が、ローカルに記憶された第1のデバイス特性と同じであるとき、つまり、認証されるべきMTCデバイスが、ネットワークにアクセスする最初のMTCデバイスであるMTCデバイスであるときは、グループ認証ベクトルが、グループ識別子にしたがって再取得され、再取得されたグループ認証ベクトルは、第2のグループ認証ベクトルと呼ばれ、第2のグループ認証ベクトルは、毎回グループ認証ベクトルが取得されるときに使用される乱数が異なるので、第1のグループ認証ベクトルとはやはり異なる。次いで、グループ識別子と、第2のデバイス特性と、取得された第2のグループ認証ベクトルとの間の結び付けの関係が確立され、第2のグループ認証ベクトルおよび第2のデバイス特性によって生成された期待される応答番号にしたがって、認証されるべきMTCデバイスが認証され、認証されるべきMTCデバイスのシステム鍵が、第2のグループ認証ベクトルおよび第2のデバイス特性にしたがって生成される。

【００３３】

当業者に本発明の第1の実施形態で提供される技術的な解決策をより明瞭に理解させるために、第1の実施形態で提供される技術的な解決策が、特定の応用のシナリオを通じて以下で詳細に説明される。

【００３４】

図5に示されるように、本発明の第1の実施形態によるMTCデバイスを認証するための方法は、図1に示された第1のシナリオに適用され得る。この実施形態においては、MTCデバイスのグループが、1つの識別情報Group IMSIと、その識別情報に対応する1つの基本鍵Kとを共有する。グループ内の第1のMTCデバイスがネットワークにアクセスするとき、MTCデバイスとネットワークの間の相互認証が実行され、システム鍵が生成される。別のMTCデバイスがネットワークにアクセスするとき、第1のMTCデバイスによって取得されたグループ認証ベクトルが、当該デバイスとネットワークの間の相互認証を実行し、システム鍵を生成するために再使用される。第1のMTCデバイスは、MTCグループ内のMTCデバイスがそれまでネットワークにアクセスしていない場合に、ネットワークにアタッチ要求を最初に送信するMTCデバイスを指す。UMTSネットワークにおいて、この方法は、以下のステップを含む。

【００３５】

ステップ201: 第1のMTCデバイスが、在圏ロケーションレジスタ(Visited Location Register, VLR)にアタッチ要求を送信し、アタッチ要求は、グループ内のデバイスによって共有される識別情報Group IMSIと、第1のMTCデバイスのデバイス特性device position 1と、タイムスタンプtime stamp 1とを含み、time stampは、アタッチ要求が送信される時間に基づいて生成される。device positionは、MTCデバイスグループ内の各デバイスの位置を示し、各デバイスのデバイス特性として使用される。デバイス特性は、MTCデバイスのグループを所有するユーザによって指定される可能性があり、オペレータは、登録段階でデバイス特性を知らされる可能性がある。あるいは、MTCデバイスのグループ内の特定

のデバイスが、登録中にMTCデバイスのグループの情報をオペレータに知らせ、次に、オペレータが、デバイス特性を各MTCデバイスに割り当てる。もちろん、別の特徴も、デバイス特性として選択される可能性があり、ここでは1つ1つ列挙されない。

【００３６】

ステップ202: 第1のMTCデバイスのアタッチ要求を受信した後、VLRが、Group IMSIとグループ認証ベクトルの間に結び付けの関係が存在するかどうかを調べる、つまり、Group IMSIに結び付けられた認証ベクトルが存在するかどうかを判定する。

【００３７】

そのMTCデバイスが第1のMTCデバイスであるので、結び付けの関係は存在せず、新しいグループ認証ベクトルが取得される必要がある。

【００３８】

ステップ203: VLRが、認証ベクトル要求をホームロケーションレジスタ(Home Location Register, HLR)に送信し、要求は、Group IMSIを含む。

【００３９】

ステップ204: HLRが、Group IMSIにしたがって対応する基本鍵Kを発見し、グループ認証ベクトルAV = (RAND, XRES, CK, IK, AUTH)を生成し、ここで、RANDは乱数を示し、XRESは期待される応答番号を示し、CKは暗号化鍵を示し、IKは完全性鍵(integrity key)を示し、AUTHは認証トークンを示す。HLRは1つのAVを生成する可能性があり、一群のAVを生成する可能性もあり、1つのAVまたは複数のAVをVLRに送信する可能性があることに留意されたい。VLRは、1つのAVを繰り返し使用するか、または一群のAVを循環的に使用して、MTCデバイスを認証することができる。

【００４０】

ステップ205: HLRが、AVおよび事前に定義された関数FをVLRに送信する。

【００４１】

関数FはVLRにおいて直接構成される可能性もあり、後のステップにおいてシステム鍵またはデバイスの期待される応答番号などのパラメータを計算するために使用されることに留意されたい。

【００４２】

ステップ206: VLRが、AVおよび関数Fを記憶し、AVと、第1のMTCデバイスのデバイス特性device position 1と、グループ内のデバイスによって共有される識別情報Group IMSIとの間の結び付けの関係を確立し、次に、関数Fを使用することによって第1のMTCデバイスの期待される応答番号XRES device 1 = F (device position 1, time stamp 1, XRES)を計算し、ここで、device position 1は、ステップ202で受信されたパラメータであり、XRESは、グループ認証ベクトルAVのパラメータである。

【００４３】

ステップ207: VLRが、グループ認証情報を第1のMTCデバイスに送信し、グループ認証情報は、AVから取得されたパラメータであり、乱数RANDおよび認証トークンAUTHを含む。

【００４４】

ステップ208: グループ認証情報を受信した後、第1のMTCデバイスが、認証トークンAUTHを調べ、AUTHが正しい場合、第1のMTCデバイスによって実行されたネットワーク側の認証を完了し、第1のMTCデバイスの応答番号RES device 1 = F (device position 1, time stamp 1, RES)と、第1のMTCデバイスの暗号化鍵CK device 1 = F (device position 1, time stamp 1, CK)と、第1のMTCデバイスの完全性鍵IK device 1 = F (device position 1, time stamp 1, IK)とを計算する。

【００４５】

ステップ209: 第1のMTCデバイスが、RES device 1を含むデバイス認証情報をVLRに送信する。

【００４６】

ステップ210: VLRが、XRES device 1が、受信されたRES device 1に等しいかどうかを調べ、それらが等しい場合、第1のMTCデバイスのアタッチ要求を受け入れ、ネットワーク

によって実行された第1のMTCデバイスの認証を完了し、ネットワーク側の鍵CK device 1 = F (device position 1, time stamp 1, CK)およびIK device 1 = F (device position 1, time stamp 1, IK)を計算する。

【００４７】

ステップ211: VLRが、第1のMTCデバイスとネットワークの間の相互認証を完了するために、アタッチ要求が受け入れられることを示すメッセージを第1のMTCデバイスに送信する。

【００４８】

ステップ212: 第2のMTCデバイスが、VLRにアタッチ要求を送信し、メッセージは、device position 2、time stamp 2、およびGroup IMSIを含む。

【００４９】

ステップ213: 第2のMTCデバイスのアタッチ要求を受信した後、VLRが、Group-IMSIとAVの間に結び付けの関係が存在するかどうかを調べ、存在しない場合、HLRからの新しいAVを要求し、存在する場合、アタッチ要求内のdevice position 2が、Group-IMSIおよびAVに結び付けられたdevice positionと同じであるかどうかを調べ、同じでない場合、既存のAVを使用することによって第2のMTCデバイスを認証し、同じである場合、HLRからの新しいAVを要求する。

【００５０】

このステップにおいて、そのMTCデバイスが第2のMTCデバイスであるので、新しいAVを求めることは必要とされない。第1のMTCデバイスが求めるAVが、認証を実行するために直接使用され、システム鍵が生成される。方法は、第1のMTCデバイスを認証するための方法と同じであり、ここで再び繰り返して説明されない。

【００５１】

第2のMTCデバイスを認証するための上述の方法において、ネットワークにアクセスする2番目のMTCデバイスであるMTCデバイスは、説明のための例とみなされる。しかし、方法は、現在のMTCグループ内でアタッチ要求を送信する2番目のMTCデバイスであるMTCデバイスを認証することに限定されず、方法は、MTCグループ内で、第1のMTCデバイスを除いて、アタッチ要求をその後送信するすべてのその他のMTCデバイスに適用可能である。

【００５２】

タイムスタンプtime stampに加えて、乱数RANDなどの別のパラメータが、システム鍵を生成するためにやはり使用され得ることに留意されたい。VLRによって実行される部分的な機能(例えば、関数Fを用いてXRES device、CK device、およびIK deviceを計算すること、ならびにGroup IMSIとAVの間の結び付けの関係を調べること)は、HLRで実行される可能性もある。ネットワークにアクセスする最初のMTCデバイスであるMTCデバイスがシャットダウンされ、一方、その他のMTCデバイスは引き続きネットワーク側と通信する必要があるとき、VLRは、ネットワークにアクセスする最初のMTCデバイスであるMTCデバイスがシャットダウンされる場合にその他のMTCデバイスが新しいAVを取得することができることを保証するために、ネットワークにアクセスする最初のMTCデバイスであるMTCデバイスのシャットダウン記録を記憶する必要がある。

【００５３】

図6に示されるように、上述の方法は、ロングタームエボリューション(Long Term Evolution, LTE)ネットワークにも適用され得る。違いは、UMTSネットワークのVLRがLTEネットワークのモビリティ管理エンティティ(Mobility Management Entity, MME)に対応し、UMTSネットワークのHLRが、LTEネットワークのホーム加入者システム(Home Subscriber System, HSS)に対応する点にある。方法は、以下を含む。

【００５４】

ステップ301: 第1のMTCデバイスが、MMEにアタッチ要求を送信し、アタッチ要求は、グループ内のデバイスによって共有される識別情報Group IMSIと、第1のMTCデバイスのデバイス特性device position 1と、タイムスタンプtime stamp 1とを含み、time stampは、アタッチ要求が送信される時間に基づいて生成される。

【００５５】
ステップ302: 第1のMTCデバイスのアタッチ要求を受信した後、MMEが、Group IMSIと認証ベクトルAVの間に結び付けの関係が存在するかどうかを調べる、つまり、Group IMSIに結び付けられた認証ベクトルが存在するかどうかを判定する。そのMTCデバイスが第1のMTCデバイスであるので、結び付けの関係は存在せず、新しい認証ベクトルAVが取得される必要がある。
【００５６】
ステップ303: MMEが、認証ベクトル要求をホーム加入者システム(Home Subscriber System, HSS)に送信し、要求は、Group IMSIを含む。
【００５７】
ステップ304: HSSが、Group IMSIにしたがって対応するKを発見し、認証ベクトルAV = (RAND, AUTH, XRES, K_{ASME})を生成し、HSSは、1つのAVを生成する可能性があり、一群のAVを生成する可能性もあり、1つのAVまたは複数のAVをMMEに送信する可能性があり、MMEは、1つのAVを繰り返し使用するか、または一群のAVを循環的に使用して、MTCデバイスを認証することができる。
【００５８】
ステップ305: HSSが、AVおよび事前に定義された関数FをMMEに送信する。関数FはMMEにおいて直接構成される可能性もあることに留意されたい。
【００５９】
ステップ306: MMEが、AVおよび関数Fを記憶し、AVと、第1のMTCデバイスのデバイス特性device position 1と、グループ内のデバイスによって共有される識別情報Group IMSIとの間の結び付けの関係を確立し、次いで、関数Fを使用することによって、第1のMTCデバイスの期待される応答番号XRES device 1 = F (device position 1, time stamp 1, XRES)を計算する。
【００６０】
ステップ307: MMEが、グループ認証情報を第1のMTCデバイスに送信し、グループ認証情報は、乱数RANDおよび認証トークンAUTHを含む。
【００６１】
ステップ308: グループ認証情報を受信した後、第1のMTCデバイスが、認証トークンAUTHを調べ、AUTHが正しい場合、第1のMTCデバイスによって実行されたネットワーク側の認証を完了し、第1のMTCデバイスの応答番号RES device 1 = F (device position 1, time stamp 1, RES)およびパラメータK_{ASME} device 1 = F (Device position 1, time stamp 1, K_{ASME})を計算する。
【００６２】
ステップ309: 第1のMTCデバイスが、RES device 1を含むデバイス認証情報をMMEに送信する。
【００６３】
ステップ310: MMEが、XRES device 1が、受信されたRES device 1に等しいかどうかを調べ、それらが等しい場合、第1のMTCデバイスのアタッチ要求を受け入れ、ネットワークによって実行された第1のMTCデバイスの認証を完了し、ネットワーク側のK_{ASME} device 1 = F (Device position 1, time stamp 1, K_{ASME})を計算する。
【００６４】
ステップ311: MMEが、第1のMTCデバイスとネットワークの間の相互認証を完了するために、アタッチ要求が受け入れられることを示すメッセージを第1のMTCデバイスに送信する。
【００６５】
ステップ312: 第2のMTCデバイスが、MMEにアタッチ要求を送信し、メッセージは、device position 2、time stamp 2、およびGroup IMSIを含む。
【００６６】
ステップ313: 第2のMTCデバイスのアタッチ要求を受信した後、MMEが、Group-IMSIとA

Vの間に結び付けの関係が存在するかどうかを調べ、存在しない場合、HSSからの新しいAVを要求し、存在する場合、アタッチ要求内のdevice position 2が、Group-IMSIおよびAVに結び付けられたdevice positionと同じであるかどうかを調べ、同じでない場合、既存のAVを使用することによって第2のMTCデバイスを認証し、同じである場合、HSSからの新しいAVを要求する。

【００６７】

このステップにおいて、そのMTCデバイスが第2のMTCデバイスであるので、新しいAVを求めることは必要とされない。第1のMTCデバイスが求めるAVが、認証のために直接使用され、システム鍵が生成される。方法は、第1のMTCデバイスを認証するための方法と同じであり、ここで再び繰り返して説明されない。

【００６８】

第2のMTCデバイスを認証するための上述の方法において、ネットワークにアクセスする2番目のMTCデバイスであるMTCデバイスは、説明のための例とみなされる。しかし、方法は、現在のMTCグループ内でアタッチ要求を送信する2番目のMTCデバイスであるMTCデバイスを認証することに限定されず、方法は、MTCグループ内で、第1のMTCデバイスを除いて、アタッチ要求をその後送信するすべてのMTCデバイスに適用可能である。

【００６９】

タイムスタンプtime stampに加えて、乱数RANDなどの別のパラメータが、システム鍵を生成するためにやはり使用され得ることに留意されたい。MMEによって実行される部分的な機能(例えば、関数Fを使用することによってXRES deviceおよびK_{ASME} deviceを計算すること)は、HSSで実行される可能性もある。ネットワークにアクセスする最初のMTCデバイスであるMTCデバイスがシャットダウンされ、一方、その他のMTCデバイスは引き続きネットワーク側と通信する必要があるとき、MMEは、ネットワークにアクセスする最初のMTCデバイスであるMTCデバイスがシャットダウンされる場合にその他のMTCデバイスが新しいAVを取得することができることを保証するために、ネットワークにアクセスする最初のMTCデバイスであるMTCデバイスのシャットダウン記録を記憶する必要がある。

【００７０】

本発明の実施形態において提供されるMTCデバイスを認証するための方法においては、グループ認証ベクトルが、MTCグループによって共有されるグループ識別子を通じて取得され、グループ内の認証されるべきMTCデバイスが、グループ認証ベクトルを通じて認証され、システム鍵が生成され、それによって、認証し、システム鍵を生成するプロセスにおいて異なるMTCデバイスに対して異なる認証ベクトルが生成されることが必要であるという問題を回避し、したがって、シグナリングのトラフィックが大幅に削減され、多数のMTCデバイスが短期間にネットワークにアクセスする場合であってもネットワークの混雑が避けられる。また、1つのグループ識別子を共有することは、15ビットのIMSIがMTCデバイスの数が多いときに使用するのに不十分であるという問題も解決する。本発明の実施形態で提供されるMTCデバイスを認証するための方法によって、多数のMTCデバイスが短期間にネットワークにアクセスする場合に、各MTCデバイスが、やはり効果的に認証され得る。

【００７１】

図7に示されるように、本発明の第2の実施形態によるMTCデバイスを認証するための方法は、以下を含む。

【００７２】

ステップ401: MTCグループ内のプライマリMTCデバイスとネットワーク側の間の認証が成功した後、MTCグループ内の第2のMTCデバイスによって送信されたアタッチ要求を受信する。

【００７３】

この実施形態において、プライマリMTCデバイスは、MTCグループ内のゲートウェイである可能性があり、指定されたMTCデバイスである可能性もある。プライマリMTCデバイスとネットワーク側の間の相互認証が実行され、次に、プライマリMTCデバイスが、グループ

内の認証されるべきその他のMTCデバイスを認証する。

【００７４】

ステップ402: 第2のMTCデバイスを認証し、プライマリMTCデバイスとネットワーク側の間の認証のプロセスで生成されたグループ認証ベクトルを使用することによって第2のMTCデバイスに関するシステム鍵を生成する。

【００７５】

この実施形態において、第2のMTCデバイスは、グループ内のプライマリMTCデバイスを除く任意のMTCデバイスであり、システム鍵は、グループ認証ベクトルを再使用することによって第2のMTCデバイスに対して生成される。

【００７６】

ステップ403: システム鍵を第2のMTCデバイスに送信する。

【００７７】

この実施形態において、システム鍵は、ネットワーク側の鍵およびデバイス側の鍵を含み、プライマリMTCデバイスによって第2のMTCデバイスに送信される鍵は、第2のMTCデバイスのデバイス側の鍵である。

【００７８】

本発明の実施形態において提供されるMTCデバイスを認証するための方法においては、MTCグループ内のプライマリMTCデバイスとネットワーク側の間の相互認証が最初に実行され、システム鍵が、それらの相互認証プロセスで生成されたグループ認証ベクトルを使用することによって、グループ内のその他の正常に認証されたMTCデバイスに対して生成され、それによって、異なるMTCデバイスに対してシステム鍵を生成するために異なる認証ベクトルを使用することが必要とされる従来技術の問題を回避する。この実施形態で提供される方法によって、シグナリングのトラフィックが大幅に削減され、多数のMTCデバイスが短期間にネットワークにアクセスする場合であってもネットワークの混雑がやはり避けられる。

【００７９】

さらに、グループ内のプライマリMTCデバイスとネットワーク側の間の認証が成功した後、認証プロセスにおいて生成されたグループ認証ベクトルと、グループ識別子との間の結び付けの関係が確立され、したがって、グループ内の認証されるべきその他のMTCデバイスが、MTCデバイスのグループ識別子およびデバイス特性(第2のMTCデバイスのデバイス特性と呼ばれる)を含むアタッチ要求をプライマリMTCデバイスに送信するときに、グループ認証ベクトルをグループ識別子にしたがって素早く発見することができ、グループ認証ベクトルおよびMTCデバイスのデバイス特性が、MTCデバイスのシステム鍵を生成するために使用され得る。

【００８０】

当業者に本発明の第2の実施形態で提供される技術的な解決策をより明瞭に理解させるために、第2の実施形態で提供される技術的な解決策が、特定の応用のシナリオを通じて以下で詳細に説明される。

【００８１】

図8に示されるように、本発明の第2の実施形態によるMTCデバイスを認証するための方法は、図2に示された第2のシナリオおよび図3に示された第3のシナリオに適用され得る。この実施形態においては、MTCデバイスのグループが、1つの識別情報Group IMSIと、1つの対応する基本鍵Kとを共有する。グループ内のMTCゲートウェイがネットワークにアクセスするとき、MTCゲートウェイとネットワークの間の相互認証が実行され、システム鍵が生成される。MTCゲートウェイは、グループ内のその他のMTCデバイスを認証し、MTCゲートウェイによって取得されたAVを再使用することによって鍵を生成し、その他のMTCデバイスに鍵を割り当てる役割を負う。UMTSネットワークにおいて、この方法は、以下のステップを含む。

【００８２】

ステップ501: MTCゲートウェイが、VLRにアタッチ要求を送信し、要求は、グループ内

のデバイスによって共有される識別情報Group IMSIと、MTCゲートウェイのデバイス特性device positionと、time stampとを含み、time stampは、アタッチ要求が送信される時間に基づいて生成される。

【００８３】

ステップ502: VLRが、認証ベクトルAV要求をHLRに送信し、要求は、Group IMSIを含む。

【００８４】

ステップ503: HLRが、Group IMSIにしたがって対応するKを発見し、認証ベクトルAV = (RAND, XRES, CK, IK, AUTH)を生成し、ここで、RANDは乱数を示し、XRESは期待される応答番号を示し、CKは暗号化鍵を示し、IKは完全性鍵を示し、AUTHは認証トークンを示す。

【００８５】

ステップ504: HLRが、AVおよび事前に定義された関数FをVLRに送信する。関数FはVLRにおいて直接構成される可能性もあり、後のステップにおいてシステム鍵またはデバイスの期待される応答番号などのパラメータを計算するために使用されることに留意されたい。

【００８６】

ステップ505: VLRが、AVおよび関数Fを記憶し、AVと、MTCゲートウェイのデバイス特性device positionと、グループ内のデバイスによって共有される識別情報Group IMSIとの間の結び付けの関係を確立し、次に、関数Fを使用することによってMTCゲートウェイの期待される応答番号XRES device = F (device position, time stamp, XRES)を計算し、ここで、device positionは、ステップ502で受信されたパラメータであり、XRESは、グループ認証ベクトルAVのパラメータである。

【００８７】

ステップ506: VLRが、グループ認証情報をMTCゲートウェイに送信し、グループ認証情報は、乱数RANDおよび認証トークンAUTHを含む。

【００８８】

ステップ507: グループ認証情報を受信した後、MTCゲートウェイが、認証トークンAUTHを調べ、AUTHが正しい場合、MTCゲートウェイによって実行されたネットワーク側の認証を完了し、MTCゲートウェイの応答番号RES device = F (device position, time stamp, RES)と、MTCゲートウェイの暗号化鍵CK device = F (device position, time stamp, CK)と、MTCゲートウェイの完全性鍵IK、IK device = F (device position, time stamp, IK)とを計算する。

【００８９】

ステップ508: MTCゲートウェイが、RES deviceを含むデバイス認証情報をVLRに送信する。

【００９０】

ステップ509: VLRが、XRES deviceが、受信されたRES deviceに等しいかどうかを調べ、それらが等しい場合、MTCゲートウェイのアタッチ要求を受け入れ、ネットワークによって実行されたMTCゲートウェイの認証を完了し、ネットワーク側の鍵CK device = F (device position, time stamp, CK)およびIK device = F (device position, time stamp, IK)を計算する。

【００９１】

ステップ510: VLRが、MTCゲートウェイとネットワークの間の相互認証を完了するために、アタッチ要求が受け入れられることを示すメッセージをMTCゲートウェイに送信する。

【００９２】

ステップ511: グループ内の別のMTCデバイスが、MTCゲートウェイにアタッチ要求を送信し、メッセージは、MTCデバイスのdevice position 2、time stamp 2、およびGroup IMSIを含む。

【００９３】

ステップ512: グループ内の別のMTCデバイスのアタッチ要求を受信した後、MTCゲート

ウェイがMTCデバイスを認証する。

【００９４】

ステップ513: MTCゲートウェイがMTCデバイスを正常に認証する場合、MTCゲートウェイが、MTCデバイスのアタッチ要求をVLRに送信し、アタッチ要求は、Group IMSI、time stamp 2、およびdevice position 2を含む。

【００９５】

ステップ514: VLRが、Group IMSIにしたがってステップ505で受信されたAVを発見し、ネットワーク側の鍵CK device 2= F (device position 2, time stamp 2, CK)およびIK device 2 = F (device position 2, time stamp 2, IK)を計算する。

【００９６】

ステップ515: MTCゲートウェイが、MTCデバイスのデバイス特性device position 2にしたがってデバイス側の鍵CK device 2= F (device position 2, time stamp 2, CK)およびIK device 2 = F (device position 2, time stamp 2, IK)を計算する。

【００９７】

ステップ516: MTCゲートウェイが、生成されたデバイス側の鍵CK device 2およびIK device 2をMTCデバイスに割り当てる。

【００９８】

MTCゲートウェイは、MTCデバイスのグループ内のプライマリデバイスである可能性もあり、それは、認証され、ネットワークにアクセスする最初のMTCデバイスであることに留意されたい。タイムスタンプtime stampに加えて、乱数RANDなどの別のパラメータが、システム鍵を生成するためにやはり使用され得る。

【００９９】

図9に示されるように、上述の方法は、LTEネットワークにおいても適用され得る。違いは、UMTSネットワークのVLRがLTEネットワークのMMEに対応し、UMTSネットワークのHLRがLTEネットワークのHSSに対応する点にある。具体的な実装方法は、以下のように説明される。

【０１００】

ステップ601: MTCゲートウェイが、MMEにアタッチ要求を送信し、要求は、グループ内のデバイスによって共有される識別情報Group IMSIと、MTCゲートウェイのデバイス特性「device position」と、time stampとを含み、time stampは、アタッチ要求が送信される時間に基づいて生成される。

【０１０１】

ステップ602: MMEが、認証ベクトルAV要求をHSSに送信し、要求は、Group IMSIを含む。

【０１０２】

ステップ603: HSSが、Group IMSIにしたがって対応するKを発見し、認証ベクトルAV = (RAND, AUTH, XRES, K_{ASME})を生成する。

【０１０３】

ステップ604: HSSが、AVおよび事前に定義された関数FをMMEに送信する。

【０１０４】

ステップ605: MMEが、AVおよび関数Fを記憶し、AVと、MTCゲートウェイのデバイス特性device positionと、グループ内のデバイスによって共有される識別情報Group IMSIとの間の結び付けの関係を確立し、次いで、関数Fを使用することによって、MTCゲートウェイの期待される応答番号XRES device = F (device position, time stamp, XRES)を計算する。

【０１０５】

ステップ606: MMEが、グループ認証情報をMTCゲートウェイに送信し、グループ認証情報は、乱数RANDおよび認証トークンAUTHを含む。

【０１０６】

ステップ607:　グループ認証情報を受信した後、MTCゲートウェイが、認証トークンAUT

Hを調べ、AUTHが正しい場合、MTCゲートウェイによって実行されたネットワーク側の認証を完了し、MTCゲートウェイの応答番号RES device = F (device position, time stamp, RES)およびパラメータK_{ASME} device = F (Device position, time stamp, K_{ASME})を計算する。

【０１０７】

ステップ608: MTCゲートウェイが、RES deviceを含むデバイス認証情報をMMEに送信する。

【０１０８】

ステップ609: MMEが、XRES deviceが、受信されたRES deviceに等しいかどうかを調べ、それらが等しい場合、MTCゲートウェイのアタッチ要求を受け入れ、ネットワークによって実行されたMTCゲートウェイの認証を完了し、ネットワーク側のK_{ASME} device = F (Device position, time stamp, K_{ASME})を計算する。

【０１０９】

ステップ610: MMEが、MTCゲートウェイとネットワークの間の相互認証を完了するために、アタッチ要求が受け入れられることを示すメッセージをMTCゲートウェイに送信する。

【０１１０】

ステップ611: グループ内の別のMTCデバイスが、MTCゲートウェイにアタッチ要求を送信し、メッセージは、MTCデバイスのdevice position 2、time stamp 2、およびGroup IMSIを含む。

【０１１１】

ステップ612: グループ内の別のMTCデバイスのアタッチ要求を受信した後、MTCゲートウェイがMTCデバイスを認証する。

【０１１２】

ステップ613: MTCゲートウェイがMTCデバイスを正常に認証する場合、MTCゲートウェイが、MTCデバイスのアタッチ要求をMMEに送信し、アタッチ要求は、Group IMSIおよびdevice position 2を含む。

【０１１３】

ステップ614: Group IMSIにしたがって、MMEが、ステップ605で受信されたAVを発見し、ネットワーク側のK_{ASME} device 2 = F (Device position 2, time stamp 2, K_{ASME})を計算する。

【０１１４】

ステップ615: MTCゲートウェイが、MTCデバイスのデバイス特性device position 2にしたがってデバイス側のK_{ASME} device 2= F (Device position 2, time stamp 2, K_{ASME})を計算する。

【０１１５】

ステップ616: MTCゲートウェイが、生成されたデバイス側のK_{ASME} device 2をMTCデバイスに割り当てる。

【０１１６】

MTCゲートウェイは、MTCデバイスのグループ内のプライマリデバイスである可能性もあり、それは、認証され、ネットワークにアクセスする最初のMTCデバイスであることに留意されたい。タイムスタンプtime stampに加えて、乱数RANDなどの別のパラメータが、システム鍵を生成するためにやはり使用され得る。

【０１１７】

本発明の実施形態において提供されるMTCデバイスを認証するための方法においては、MTCグループ内のプライマリMTCデバイスとネットワーク側の間の相互認証が最初に実行され、システム鍵が、それらの相互認証プロセスで生成されたグループ認証ベクトルを使用することによって、グループ内のその他の正常に認証されたMTCデバイスに対して生成され、それによって、異なるMTCデバイスに対してシステム鍵を生成するために異なる認証ベクトルを使用することが必要とされる従来技術の問題を回避する。この実施形態で提供

される方法によって、シグナリングのトラフィックが大幅に削減され、多数のMTCデバイスが短期間にネットワークにアクセスする場合であってもネットワークの混雑が避けられる。

【０１１８】

図10に示されるように、本発明の第3の実施形態によるMTCデバイスを認証するための方法は、以下を含む。

【０１１９】

ステップ701: MTCグループ内のプライマリMTCデバイスが、ネットワーク側にアタッチ要求を送信し、アタッチ要求は、MTCグループのグループ識別子、およびMTCグループ内の認証されるべきその他のMTCデバイスのデバイス特性を含む。

【０１２０】

この実施形態においては、認証されるべき1つまたは複数のその他のMTCデバイスが、MTCグループ内に存在し得る。プライマリMTCデバイスは、バッチ処理を実行するように機能し、異なるMTCデバイスは、同じグループ識別子および異なるデバイス特性に対応する。システム鍵を生成する後続のプロセスにおいて、異なるデバイス特性にしたがって異なるMTCデバイスに対して異なるシステム鍵が生成され、それによって、システムのセキュリティを保証し、処理の効率を改善する。

【０１２１】

ステップ702: プライマリMTCデバイスとネットワーク側の間の認証を実行し、グループ認証ベクトル、および認証されるべきその他のMTCデバイスのデバイス特性を使用することによって、認証されるべきその他のMTCデバイスに関するシステム鍵を生成し、グループ認証ベクトルは、プライマリMTCデバイスとネットワーク側の間の認証のプロセスで生成される。

【０１２２】

ステップ703: プライマリMTCデバイスが、認証されるべきその他のMTCデバイスを正常に認証した後、プライマリMTCデバイスが、認証されるべきその他のMTCデバイスにシステム鍵を送信する。

【０１２３】

この実施形態において、システム鍵は、ネットワーク側の鍵およびデバイス側の鍵を含み、プライマリMTCデバイスによって、認証されるべきMTCデバイスに送信される鍵は、それらのデバイス側の鍵である。

【０１２４】

本発明の実施形態において提供されるMTCデバイスを認証するための方法においては、グループ認証ベクトルが、MTCグループによって共有されるグループ識別子を通じて取得され、システム鍵が、グループ内の認証されるべきすべてのMTCデバイスに対して、グループ認証ベクトルを通じて生成され、生成されたシステム鍵が、MTCデバイスに割り当てられ、それによって、異なるMTCデバイスに対してシステム鍵を生成するために異なる認証ベクトルが使用される必要があるために大量のシグナリングのトラフィックが生成されるという従来技術の問題を回避する。この実施形態で提供される方法によって、シグナリングのトラフィックが大幅に削減され、多数のMTCデバイスが短期間にネットワークにアクセスする場合であってもネットワークの混雑が避けられる。また、1つのグループ識別子を共有することは、15ビットのIMSIがMTCデバイスの数が多いときに使用するのに不十分であるという問題も解決する。

【０１２５】

当業者に本発明の第3の実施形態で提供される技術的な解決策をより明瞭に理解させるために、第3の実施形態で提供される技術的な解決策が、特定の応用のシナリオを通じて以下で詳細に説明される。

【０１２６】

図11に示されるように、本発明の第3の実施形態によるMTCデバイスを認証するための方法は、図2に示された第2のシナリオおよび図3に示された第3のシナリオに適用され得る。

この実施形態においては、MTCデバイスのグループが、1つの識別情報Group IMSIと、1つの対応する基本鍵Kとを共有する。グループ内のMTCゲートウェイがネットワークにアクセスするとき、MTCゲートウェイとネットワークの間の相互認証が実行され、グループ内の認証されるべきその他のMTCデバイスのデバイス特性が、ネットワーク側に一回送信され、システム鍵が、認証ベクトルAVを再使用することによってグループ内のその他のMTCデバイスに対して生成される。MTCゲートウェイは、グループ内のその他のMTCデバイスを認証し、グループ内のその他のMTCデバイスに鍵を割り当てる役割を負う。UMTSネットワークにおいて、この方法は、以下のステップを含む。

【０１２７】

ステップ801: MTCゲートウェイが、VLRにアタッチ要求を送信し、要求は、グループ内のデバイスによって共有される識別情報Group IMSIと、time stampと、グループ内のMTCデバイスのデバイス特性device position 1、device position 2、device position 3...とを含み、time stampは、アタッチ要求が送信される時間に基づいて生成される。

【０１２８】

ステップ802: VLRが、認証ベクトルAV要求をHLRに送信し、要求は、Group IMSIと、device position nによって示されるグループ内のMTCデバイスのデバイス特性device position 1、device position 2、device position 3...とを含む。

【０１２９】

ステップ803: HLRが、Group IMSIにしたがって対応するKを発見し、認証ベクトルAV = (RAND, XRES, CK, IK, AUTH)を生成し、ここで、RANDは乱数を示し、XRESは期待される応答番号を示し、CKは暗号化鍵を示し、IKは完全性鍵を示し、AUTHは認証トークンを示し、HLRが、グループ内のデバイスのデバイス特性「device position n」を使用することによって各デバイスのネットワーク側の暗号化鍵CK device n = F (device position n, time stamp, CK)およびネットワーク側の完全性鍵IK device n = F (device position n, time stamp, IK)を計算する。

【０１３０】

ステップ804: HLRが、AVと、事前に定義された関数Fと、各MTCデバイスのネットワーク側の暗号化鍵CK deviceと、各MTCデバイスのネットワーク側の完全性鍵IK deviceとをVLRに送信する。もちろん、関数Fは、VLRにおいて直接構成される可能性もある。

【０１３１】

ステップ805: VLRが、AVと、関数Fと、各デバイスのネットワーク側の暗号化鍵CK deviceと、各デバイスのネットワーク側の完全性鍵IK deviceとを記憶する。

【０１３２】

ステップ806: VLRが、グループ認証情報をMTCゲートウェイに送信し、グループ認証情報は、乱数RANDおよび認証トークンAUTHを含む。

【０１３３】

ステップ807:　グループ認証情報を受信した後、MTCゲートウェイが、認証トークンAUTHを調べ、AUTHが正しい場合、MTCゲートウェイによって実行されたネットワーク側の認証を完了し、応答番号RES、暗号化鍵CK、および完全性鍵IKを計算する。

【０１３４】

ステップ808: MTCゲートウェイが、RESを含むデバイス認証情報をVLRに送信する。

【０１３５】

ステップ809: VLRが、XRESが、受信されたRESに等しいかどうかを調べ、それらが等しい場合、MTCゲートウェイのアタッチ要求を受け入れ、ネットワークによって実行されたMTCゲートウェイの認証を完了する。

【０１３６】

ステップ810: VLRが、MTCゲートウェイとネットワークの間の相互認証を完了するために、アタッチ要求が受け入れられることを示すメッセージをMTCゲートウェイに送信する。

【０１３７】

ステップ811: MTCゲートウェイが、ステップ807において計算される各MTCデバイスのCK、IK、およびデバイス特性device position nにしたがって各MTCデバイスの暗号化鍵CK device n = F (device position n, time stamp, CK)およびIK device n = F (device position n, time stamp, IK)を計算する。

【０１３８】

ステップ812: MTCゲートウェイが、グループ内の各MTCデバイスを認証する。

【０１３９】

ステップ813: 認証が成功する場合、MTCゲートウェイが、ステップ811において計算されるCK device nおよびIK device nを対応するMTCデバイスに割り当てる。

【０１４０】

MTCゲートウェイは、MTCデバイスのグループ内のプライマリデバイスである可能性もあり、それは、認証され、ネットワークにアクセスする最初のMTCデバイスであることに留意されたい。time stampに加えて、乱数RANDなどの別のパラメータが、システム鍵を生成するためにやはり使用され得る。

【０１４１】

図12に示されるように、上述の方法は、LTEネットワークにおいても適用され得る。違いは、UMTSネットワークのVLRがLTEネットワークのMMEに対応し、UMTSネットワークのHLRがLTEネットワークのHSSに対応する点にある。具体的な実装方法は、以下のように説明される。

【０１４２】

ステップ901: MTCゲートウェイが、MMEにアタッチ要求を送信し、要求は、グループ内のデバイスによって共有される識別情報Group IMSIと、time stampと、グループ内のMTCデバイスのデバイス特性device position 1、device position 2、device position 3...とを含み、time stampは、アタッチ要求が送信される時間に基づいて生成される。

【０１４３】

ステップ902: MMEが、認証ベクトルAV要求をHSSに送信し、要求は、Group IMSIと、device position nによって示されるグループ内のMTCデバイスのデバイス特性device position 1、device position 2、device position 3...とを含む。

【０１４４】

ステップ903: HSSが、Group IMSIにしたがって対応するKを発見し、認証ベクトルAV = (RAND, AUTH, XRES, K_{ASME})を生成し、グループ内の各デバイスのデバイス特性device position nを使用することによって各デバイスのネットワーク側のK_{ASME} device n = F (Device position n, time stamp, K_{ASME})を計算する。

【０１４５】

ステップ904: HSSが、AVと、事前に定義された関数Fと、各MTCデバイスのネットワーク側のK_{ASME} deviceとをMMEに送信する。

【０１４６】

ステップ905: MMEが、AVと、関数Fと、各MTCデバイスのネットワーク側のK_{ASME} deviceとを記憶する。

【０１４７】

ステップ906: MMEが、グループ認証情報をMTCゲートウェイに送信し、グループ認証情報は、乱数RANDおよび認証トークンAUTHを含む。

【０１４８】

ステップ907: グループ認証情報を受信した後、MTCゲートウェイが、認証トークンAUTHを調べ、AUTHが正しい場合、MTCゲートウェイによって実行されたネットワーク側の認証を完了し、応答番号RESおよびデバイス側のK_{ASME}を計算する。

【０１４９】

ステップ908: MTCゲートウェイが、RESを含むデバイス認証情報をMMEに送信する。

【０１５０】

ステップ909: MMEが、XRESが、受信されたRESに等しいかどうかを調べ、それらが等し

い場合、MTCゲートウェイのアタッチ要求を受け入れ、ネットワークによって実行されたMTCゲートウェイの認証を完了する。

【０１５１】

ステップ910: MMEが、MTCゲートウェイとネットワークの間の相互認証を完了するために、アタッチ要求が受け入れられることを示すメッセージをMTCゲートウェイに送信する。

【０１５２】

ステップ911: MTCゲートウェイが、ステップ907において計算される各MTCデバイスのK_{ASME}およびデバイス特性device position nにしたがって各MTCデバイスのK_{ASME} device n = F (device position n, time stamp, K_{ASME})を計算する。

【０１５３】

ステップ912: MTCゲートウェイが、グループ内の各MTCデバイスを認証する。

【０１５４】

ステップ913: 認証が成功する場合、MTCゲートウェイが、ステップ911において計算されたK_{ASME} device nを対応するMTCデバイスに割り当てる。

【０１５５】

MTCゲートウェイは、MTCデバイスのグループ内のプライマリデバイスである可能性もあり、それは、認証され、ネットワークにアクセスする最初のMTCデバイスであることに留意されたい。time stampに加えて、乱数RANDなどの別のパラメータが、システム鍵を生成するためにやはり使用され得る。

【０１５６】

本発明の実施形態において提供されるMTCデバイスを認証するための方法においては、グループ認証ベクトルが、MTCグループによって共有されるグループ識別子を通じて取得され、システム鍵が、グループ内の認証されるべきその他のMTCデバイスに対して、グループ認証ベクトルを通じて一回生成され、生成されたシステム鍵が、MTCデバイスに割り当てられ、それによって、異なるMTCデバイスに対してシステム鍵を生成するために異なる認証ベクトルが使用される必要があるために大量のシグナリングのトラフィックが生成されるという従来技術の問題を回避する。この実施形態で提供される方法によって、シグナリングのトラフィックが大幅に削減され、多数のMTCデバイスが短期間にネットワークにアクセスする場合であってもネットワークの混雑が避けられる。また、1つのグループ識別子を共有することは、15ビットのIMSIがMTCデバイスの数が多いときに使用するのに不十分であるという問題も解決する。

【０１５７】

図13に示されるように、本発明の第4の実施形態によるMTCデバイスを認証するための方法は、以下を含む。

【０１５８】

ステップ1001: グループ識別子およびデバイス特性を含むアタッチ要求を受信し、グループ識別子は、認証されるべきMTCデバイスが位置するMTCグループのグループ識別子であり、デバイス特性は、認証されるべきMTCデバイスのデバイス特性である。

【０１５９】

ステップ1002: グループ識別子およびデバイス特性にしたがって、認証されるべきMTCデバイスの認証ベクトルを取得する。

【０１６０】

ステップ1003: 認証ベクトルおよびデバイス特性にしたがって、認証されるべきMTCデバイスを認証し、認証されるべきMTCデバイスに関するシステム鍵を生成する。

【０１６１】

本発明の実施形態において提供されるMTCデバイスを認証するための方法においては、認証ベクトルが、1つのグループ識別子を共有することによって取得され、それによって、15ビットのIMSIがMTCデバイスの数が多いときに使用するのに不十分であるという問題を解決する。また、異なるデバイス特性にしたがって異なるMTCデバイスに対して異なる

システム鍵が生成され、それによって、システムのセキュリティを保証し、処理の効率を改善する。本発明の実施形態で提供されるMTCデバイスを認証するための方法によって、多数のMTCデバイスが短期間にネットワークにアクセスする場合に、各MTCデバイスが、やはり効果的に認証され得る。

【０１６２】

当業者に本発明の第4の実施形態で提供される技術的な解決策をより明瞭に理解させるために、第4の実施形態で提供される技術的な解決策が、特定の応用のシナリオを通じて以下で詳細に説明される。

【０１６３】

図14に示されるように、本発明の第4の実施形態によるMTCデバイスを認証するための方法は、図1に示された第1のシナリオに適用され得る。この実施形態においては、MTCデバイスのグループが、1つの識別情報Group IMSIを共有し、識別情報Group IMSIおよびデバイス特性device positionが、異なる基本鍵Kに対応する。グループ内の各MTCデバイスは、Group IMSIおよびデバイス特性device positionを通じてネットワークにアクセスする。MTCデバイスは、異なるKに基づいて認証され、システム鍵が生成される。UMTSネットワークにおいて、この方法は、以下のステップを含む。

【０１６４】

ステップ1101: MTCデバイスが、VLRにアタッチ要求を送信し、アタッチ要求は、グループ内のデバイスによって共有される識別情報Group IMSIと、MTCデバイスのデバイス特性「device position」とを含む。

【０１６５】

ステップ1102: VLRが、認証ベクトルAV要求をHLRに送信し、要求は、Group IMSIおよびdevice positionを含む。

【０１６６】

ステップ1103: HLRが、Group IMSIおよびdevice positionにしたがって対応する基本鍵Kを発見し、事前に定義された関数Fを使用することによってAV = (RAND, XRES device, CK, IK, AUTH)を生成し、ここで、XRES device = F (device position, XRES)である。

【０１６７】

ステップ1104: HLRが、AVおよび事前に定義された関数FをVLRに送信する。関数FはVLRにおいて直接構成される可能性もあることに留意されたい。

【０１６８】

ステップ1105: VLRが、AVおよび関数Fを記憶する。

【０１６９】

ステップ1106: VLRが、認証情報をMTCデバイスに送信し、認証情報は、乱数RANDおよび認証トークンAUTHを含む。

【０１７０】

ステップ1107:　認証情報を受信した後、MTCデバイスが、認証トークンAUTHを調べ、AUTHが正しい場合、MTCデバイスによって実行されたネットワーク側の認証を完了し、MTCデバイスの応答番号RES device = F (device position, RES)と、MTCデバイスの暗号化鍵CK device = F (device position, CK)と、MTCデバイスの完全性鍵IK device = F (device position, IK)とを計算する。

【０１７１】

ステップ1108: MTCデバイスが、RES deviceを含むデバイス認証情報をVLRに送信する。

【０１７２】

ステップ1109: VLRが、XRES deviceが、受信されたRES deviceに等しいかどうかを調べ、それらが等しい場合、MTCデバイスのアタッチ要求を受け入れ、ネットワークによって実行されたMTCデバイスの認証を完了し、ネットワーク側の鍵CK device = F (device position, CK)およびIK device = F (device position, IK)を計算する。

【０１７３】

ステップ1110: VLRが、MTCデバイスとネットワークの間の相互認証を完了するために、

アタッチ要求が受け入れられることを示すメッセージをMTCデバイスに送信する。

【０１７４】

図15に示されるように、上述の方法は、LTEネットワークにおいても適用され得る。違いは、UMTSネットワークのVLRがLTEネットワークのMMEに対応し、UMTSネットワークのHLRがLTEネットワークのHSSに対応する点にある。具体的な実装方法は、以下のように説明される。

【０１７５】

ステップ1201: MTCデバイスが、MMEにアタッチ要求を送信し、アタッチ要求は、グループ内のデバイスによって共有される識別情報Group IMSIと、MTCデバイスのデバイス特性「device position」とを含む。

【０１７６】

ステップ1202: MMEが、認証ベクトルAV要求をHSSに送信し、要求は、Group IMSIおよびdevice positionを含む。

【０１７７】

ステップ1203: HSSが、Group IMSIおよびdevice positionにしたがって対応する基本鍵Kを発見し、事前に定義された関数Fを使用することによってAV = (RAND, AUTH, XRES device, K_{ASME})を生成し、ここで、XRES device = F (device position, XRES)である。

【０１７８】

ステップ1204: HSSが、AVおよび事前に定義された関数FをMMEに送信する。関数FはMMEにおいて直接構成される可能性もあることに留意されたい。

【０１７９】

ステップ1205: MMEが、AVおよび関数Fを記憶する。

【０１８０】

ステップ1206: MMEが、認証情報をMTCデバイスに送信し、認証情報は、乱数RANDおよび認証トークンAUTHを含む。

【０１８１】

ステップ1207: 認証情報を受信した後、MTCデバイスが、認証トークンAUTHを調べ、AUTHが正しい場合、MTCデバイスによって実行されたネットワーク側の認証を完了し、MTCデバイスの応答番号RES device = F (device position, RES)およびMTCデバイスのK_{ASME} device = F (device position, K_{ASME})を計算する。

【０１８２】

ステップ1208: MTCデバイスが、RES deviceを含むデバイス認証情報をMMEに送信する。

【０１８３】

ステップ1209: MMEが、XRES deviceが、受信されたRES deviceに等しいかどうかを調べ、それらが等しい場合、MTCデバイスのアタッチ要求を受け入れ、ネットワークによって実行されたMTCデバイスの認証を完了し、ネットワーク側のK_{ASME} device = F (device position, K_{ASME})を計算する。

【０１８４】

ステップ1210: MMEが、MTCデバイスとネットワークの間の相互認証を完了するために、アタッチ要求が受け入れられることを示すメッセージをMTCデバイスに送信する。

【０１８５】

本発明の実施形態において提供されるMTCデバイスを認証するための方法においては、認証ベクトルが、1つのグループ識別子を共有することによって取得され、それによって、15ビットのIMSIがMTCデバイスの数が多いときに使用するのに不十分であるという問題を解決する。また、異なるデバイス特性にしたがって異なるMTCデバイスに対して異なるシステム鍵が生成され、それによって、システムのセキュリティを保証し、処理の効率を改善する。本発明の実施形態で提供されるMTCデバイスを認証するための方法によって、多数のMTCデバイスが短期間にネットワークにアクセスする場合に、各MTCデバイスが、やはり効果的に認証され得る。

【０１８６】

図16に示されるように、本発明の実施形態は、
グループ識別子を含み、認証されるべきMTCデバイスによって送信されたアタッチ要求を受信するように構成された第1の受信ユニット1301であって、グループ識別子が、認証されるべきMTCデバイスが位置するMTCグループのグループ識別子である、第1の受信ユニット1301と、
第1の受信ユニット1301によって受信されたグループ識別子に結び付けられた第1のグループ認証ベクトルが存在するときに、第1のグループ認証ベクトルにしたがって、認証されるべきMTCデバイスを認証し、認証されるべきMTCデバイスに関するシステム鍵を生成するように構成された第1の認証ユニット1302とを含むネットワーク側のエンティティをさらに提供する。

【０１８７】
さらに、図17に示されるように、ネットワーク側のエンティティは、
第1のグループ認証ベクトルが存在しないときに、第1の受信ユニット1301によって受信されたグループ識別子にしたがってサーバから第1のグループ認証ベクトルを取得するように構成された第1の取得ユニット1303と、
第1の受信ユニット1301によって受信されたグループ識別子と、第1の取得ユニット1303によって取得された第1のグループ認証ベクトルとの間の結び付けの関係を確立するように構成された第1の確立ユニット1304と、
第1の取得ユニット1303によって取得された第1のグループ認証ベクトルにしたがって、認証されるべきMTCデバイスを認証し、認証されるべきMTCデバイスに関するシステム鍵を生成するように構成された第2の認証ユニット1305とをさらに含む。

【０１８８】
さらに、図18に示されるように、ネットワーク側のエンティティは、
第1の受信ユニット1301によって受信されたアタッチ要求が認証されるべきMTCデバイスを識別するために使用される第2のデバイス特性をさらに含むときに、第2のデバイス特性が、ローカルに記憶された第1のデバイス特性と同じであるかどうかを判定するように構成された判定ユニット1306であって、第1のデバイス特性は、グループ識別子と第1のグループ認証ベクトルの両方に結び付けられたデバイス特性である、判定ユニット1306をさらに含む。

【０１８９】
さらに、図18に示されるように、ネットワーク側のエンティティは、
認証されるべきMTCデバイスの第2のデバイス特性が、ローカルに記憶された第1のデバイス特性と同じであるとき、第1の受信ユニット1301によって受信されたグループ識別子にしたがって、MTCグループ内のMTCデバイスを認証するために使用される第2のグループ認証ベクトルを取得するように構成された第2の取得ユニット1307と、
第1の受信ユニット1301によって受信されたグループ識別子と、第2のデバイス特性と、第2の取得ユニット1307によって取得された第2のグループ認証ベクトルとの間の結び付けの関係を確立するように構成された第2の確立ユニット1308と、
第2の取得ユニット1307によって取得された第2のグループ認証ベクトルおよび第1の受信ユニット1301によって受信された第2のデバイス特性によって生成された期待される応答番号にしたがって、認証されるべきMTCデバイスを認証し、第2の取得ユニット1307によって取得された第2のグループ認証ベクトルおよび第1の受信ユニット1301によって受信された第2のデバイス特性にしたがって、認証されるべきMTCデバイスのシステム鍵を生成するように構成された第3の認証ユニット1309とをさらに含む。

【０１９０】
図19に示されるように、第1の認証ユニット1302は、
第1のグループ認証ベクトルおよび第1の受信ユニット1301によって受信された第2のデバイス特性にしたがって期待される応答番号を生成するように構成された第1の生成ユニット13021と、
認証されるべきMTCデバイスが、グループ認証情報にしたがってネットワークを認証し

、第2のデバイス特性にしたがってデバイス側の鍵を生成するように、認証されるべきMTCデバイスにグループ認証情報を送信するように構成された第1の送信ユニット13022であって、グループ認証情報は、第1のグループ認証ベクトル内の情報である、第1の送信ユニット13022と、

認証されるべきMTCデバイスによって第2のデバイス特性にしたがって生成された応答番号を受信するように構成された第2の受信ユニット13023と、

第2の受信ユニット13023によって受信された応答番号および第1の生成ユニット13021によって生成された期待される応答番号にしたがって、認証されるべきMTCデバイスを認証するように構成された第1の認証サブユニット13024と、

第1のグループ認証ベクトル、および第1の受信ユニット1301によって受信される第2のデバイス特性にしたがってネットワーク側の鍵を生成するように構成された第2の生成ユニット13025とを含む。

【０１９１】

上述のユニットの具体的な実装方法に関しては、ステップ201～213またはステップ301～313で説明された方法が参照可能であり、これらのステップは、ここで再び繰り返して説明されない。

【０１９２】

本発明の実施形態で提供されるネットワーク側のエンティティにおいては、グループ認証ベクトルが、MTCグループによって共有されるグループ識別子を通じて取得され、グループ内の認証されるべきすべてのMTCデバイスが、グループ認証ベクトルを通じて認証され、システム鍵が生成され、それによって、認証し、システム鍵を生成するプロセスにおいて異なるMTCデバイスに対して異なる認証ベクトルが生成されることが必要であるという問題を回避し、したがって、シグナリングのトラフィックが大幅に削減され、多数のMTCデバイスが短期間にネットワークにアクセスする場合であってもネットワークの混雑が避けられる。また、1つのグループ識別子を共有することは、15ビットのIMSIがMTCデバイスの数が多いときに使用するのに不十分であるという問題も解決する。本発明の実施形態で提供されるネットワーク側のエンティティによって、多数のMTCデバイスが短期間にネットワークにアクセスする場合に、各MTCデバイスが、やはり効果的に認証され得る。

【０１９３】

図20に示されるように、本発明の実施形態は、

デバイスとネットワーク側の間の認証が成功した後、デバイスが位置するMTCグループ内の第2のMTCデバイスによって送信されたアタッチ要求を受信するように構成された第3の受信ユニット1401と、

第2のMTCデバイスを認証し、デバイスとネットワーク側の間の認証のプロセスで生成されたグループ認証ベクトルを使用することによって第2のMTCデバイスに関するシステム鍵を生成するように構成された第4の認証ユニット1402と、

第4の認証ユニット1402によって生成されたシステム鍵を第2のMTCデバイスに送信するように構成された第2の送信ユニット1403とを含む、MTCデバイスを認証するためのデバイスをさらに提供する。

【０１９４】

さらに、図21に示されるように、MTCデバイスを認証するためのデバイスは、

デバイスとネットワーク側の間の認証が成功した後、グループ認証ベクトルと、MTCグループのグループ識別子との間の結び付けの関係を確立するように構成された第3の確立ユニット1404をさらに含む。

【０１９５】

さらに、図22に示されるように、第4の認証ユニット1402は、

第3の受信ユニット1401によって受信されたグループ識別子に結び付けられたグループ認証ベクトルを取得するように構成された第3の取得ユニット14021と、

第3の取得ユニット14021によって取得されたグループ認証ベクトル、および第3の受信ユニット1401によって受信される、第2のMTCデバイスのデバイス特性を使用することによ

って第2のMTCデバイスに関するシステム鍵を生成するように構成された第3の生成ユニット14022とを含む。

【０１９６】

さらに、図23に示されるように、MTCデバイスを認証するためのデバイスは、

ネットワーク側が、グループ認証ベクトルおよび第2のMTCデバイスのデバイス特性を使用することによって第2のMTCデバイスに関するシステム鍵を生成するように、第3の受信ユニット1401によって受信されたアタッチ要求をネットワーク側に転送するように構成された転送ユニット1405をさらに含む。

【０１９７】

上述のユニットの具体的な実装方法に関しては、ステップ501～516またはステップ601～616で説明された方法が参照可能であり、これらのステップは、ここで再び繰り返して説明されない。

【０１９８】

本発明の実施形態において提供されるMTCデバイスを認証するためのデバイスにおいては、MTCグループ内のプライマリMTCデバイスとネットワーク側の間の相互認証が最初に実行され、システム鍵が、それらの相互認証プロセスで生成されたグループ認証ベクトルを使用することによって、グループ内のその他の正常に認証されたMTCデバイスに対して生成され、それによって、異なるMTCデバイスに対してシステム鍵を生成するために異なる認証ベクトルを使用することが必要とされる従来技術の問題を回避する。この実施形態で提供されるデバイスによって、シグナリングのトラフィックが大幅に削減され、多数のMTCデバイスが短期間にネットワークにアクセスする場合であってもネットワークの混雑が避けられる。

【０１９９】

図24に示されるように、本発明の実施形態は、

アタッチ要求をネットワーク側に送信するように構成された第3の送信ユニット1501であって、アタッチ要求が、デバイスが位置するMTCグループのグループ識別子、およびMTCグループ内の認証されるべきMTCデバイスのデバイス特性を含む、第3の送信ユニット1501と、

デバイスとネットワーク側の間で相互認証を実行し、グループ認証ベクトル、および認証されるべきMTCデバイスのデバイス特性を使用することによって、認証されるべきMTCデバイスに関するシステム鍵を生成するように構成された第5の認証ユニット1502であって、グループ認証ベクトルが、デバイスとネットワーク側の間の認証のプロセスで生成される、第5の認証ユニット1502と、

デバイスが、認証されるべきMTCデバイスを正常に認証した後、第5の認証ユニット1502によって生成されたシステム鍵を認証されるべきMTCデバイスに送信するように構成された第4の送信ユニット1503とを含む、MTCデバイスを認証するためのデバイスをさらに提供する。

【０２００】

さらに、MTCデバイスを認証するためのデバイスは、

第3の送信ユニット1501によって送信されたアタッチ要求がデバイスのデバイス特性を含むときに、デバイスのデバイス特性にしたがってデバイスのシステム鍵を生成するように構成された第4の生成ユニット1504をさらに含む。

【０２０１】

上述のユニットの具体的な実装方法に関しては、ステップ801～813またはステップ901～913で説明された方法が参照可能であり、これらのステップは、ここで再び繰り返して説明されない。

【０２０２】

本発明の実施形態において提供されるMTCデバイスを認証するためのデバイスにおいては、グループ認証ベクトルが、MTCグループによって共有されるグループ識別子を通じて取得され、システム鍵が、グループ内の認証されるべきすべてのMTCデバイスに対して、

グループ認証ベクトルを通じて生成され、生成されたシステム鍵が、MTCデバイスに割り当てられ、それによって、異なるMTCデバイスに対してシステム鍵を生成するために異なる認証ベクトルが使用される必要があるために大量のシグナリングのトラフィックが生成されるという従来技術の問題を回避する。この実施形態で提供されるデバイスによって、シグナリングのトラフィックが大幅に削減され、多数のMTCデバイスが短期間にネットワークにアクセスする場合であってもネットワークの混雑が避けられる。また、1つのグループ識別子を共有することは、15ビットのIMSIがMTCデバイスの数が多いときに使用するのに不十分であるという問題も解決する。

【０２０３】

図25に示されるように、本発明の実施形態は、

グループ識別子およびデバイス特性を含むアタッチ要求を受信するように構成された第4の受信ユニット1601であって、グループ識別子は、認証されるべきMTCデバイスが位置するMTCグループのグループ識別子であり、デバイス特性は、認証されるべきMTCデバイスのデバイス特性である、第4の受信ユニット1601と、

第4の受信ユニット1601によって受信されるグループ識別子およびデバイス特性にしたがって、認証されるべきMTCデバイスの認証ベクトルを取得するように構成された第4の取得ユニット1602と、

第4の取得ユニット1602によって取得された認証ベクトルおよび第4の受信ユニット1601によって受信されたデバイス特性にしたがって、認証されるべきMTCデバイスを認証し、認証されるべきMTCデバイスのシステム鍵を生成するように構成された第6の認証ユニット1603とを含むネットワーク側のエンティティをさらに提供する。

【０２０４】

上述のユニットの具体的な実装方法に関しては、ステップ1101～1110またはステップ1201～1210で説明された方法が参照可能であり、これらのステップは、ここで再び繰り返して説明されない。

【０２０５】

本発明の実施形態で提供されるネットワーク側のエンティティにおいては、認証ベクトルが、1つのグループ識別子を共有することによって取得され、それによって、15ビットのIMSIがMTCデバイスの数が多いときに使用するのに不十分であるという問題を解決する。また、異なるデバイス特性にしたがって異なるMTCデバイスに対して異なるシステム鍵が生成され、それによって、システムのセキュリティを保証し、処理の効率を改善する。本発明の実施形態で提供されるネットワーク側のエンティティによって、多数のMTCデバイスが短期間にネットワークにアクセスする場合に、各MTCデバイスが、やはり効果的に認証され得る。

【０２０６】

本発明で提供される技術的な解決策は、MTCデバイスを認証する技術分野に適用され得る。

【０２０７】

当業者は、上述の実施形態による方法のステップのすべてまたは一部が、関連するハードウェアに指示するプログラムによって実装され得ることを理解するに違いない。プログラムは、ROM/RAM、磁気ディスク、またはコンパクトディスクなどのコンピュータ可読ストレージ媒体に記憶され得る。

【０２０８】

上述の説明は、本発明の特定の実装方法であるに過ぎないが、本発明の保護範囲を限定するように意図されていない。本発明で開示された技術的範囲内で当業者によって容易に想到され得るすべての変更または置き換えは、本発明の保護範囲内に入るべきである。したがって、本発明の保護範囲は、特許請求の範囲の保護範囲にしたがうべきである。

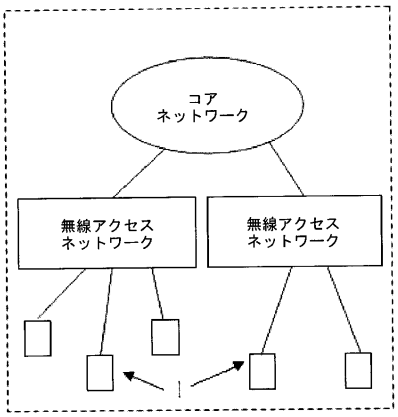
【符号の説明】

【０２０９】

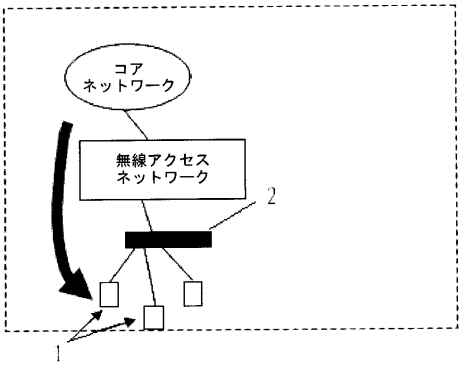
１　MTCデバイス

2 MTCゲートウェイ
1301 第1の受信ユニット
1302 第1の認証ユニット
1303 第1の取得ユニット
1304 第1の確立ユニット
1305 第2の認証ユニット
1306 判定ユニット
1307 第2の取得ユニット
1308 第2の確立ユニット
1309 第3の認証ユニット
1401 第3の受信ユニット
1402 第4の認証ユニット
1403 第2の送信ユニット
1404 第3の確立ユニット
1405 転送ユニット
1501 第3の送信ユニット
1502 第5の認証ユニット
1503 第4の送信ユニット
1601 第4の受信ユニット
1602 第4の取得ユニット
1603 第6の認証ユニット
13021 第1の生成ユニット
13022 第1の送信ユニット
13023 第2の受信ユニット
13024 第1の認証サブユニット
13025 第2の生成ユニット
14021 第3の取得ユニット
14022 第3の生成ユニット

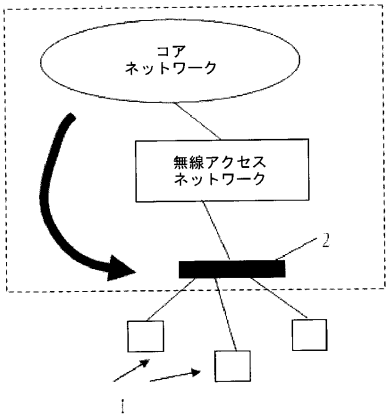
【図１】



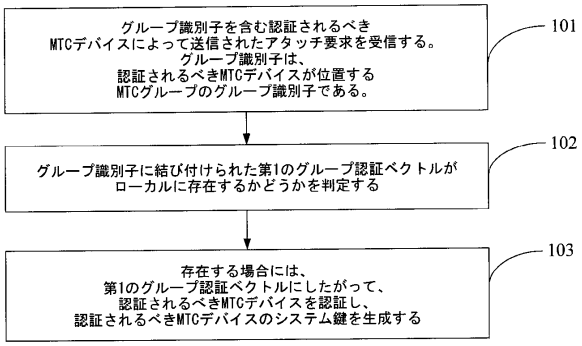
【図２】



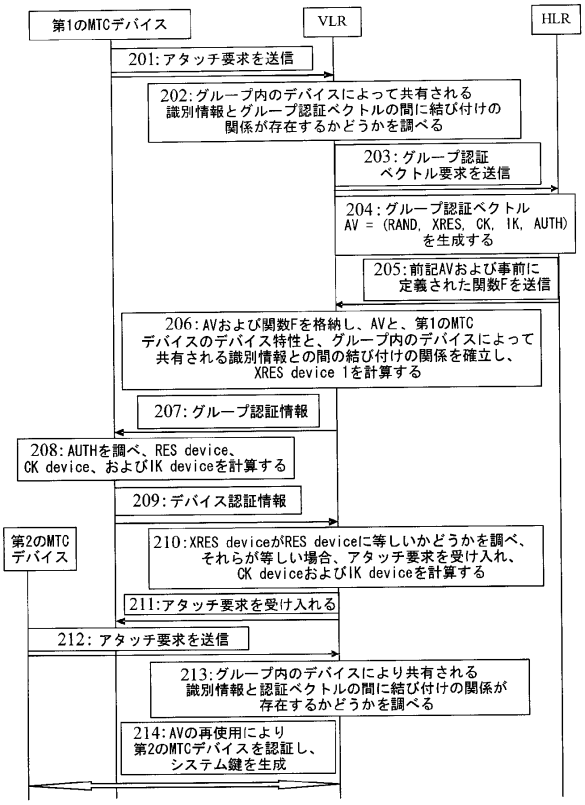
【図３】



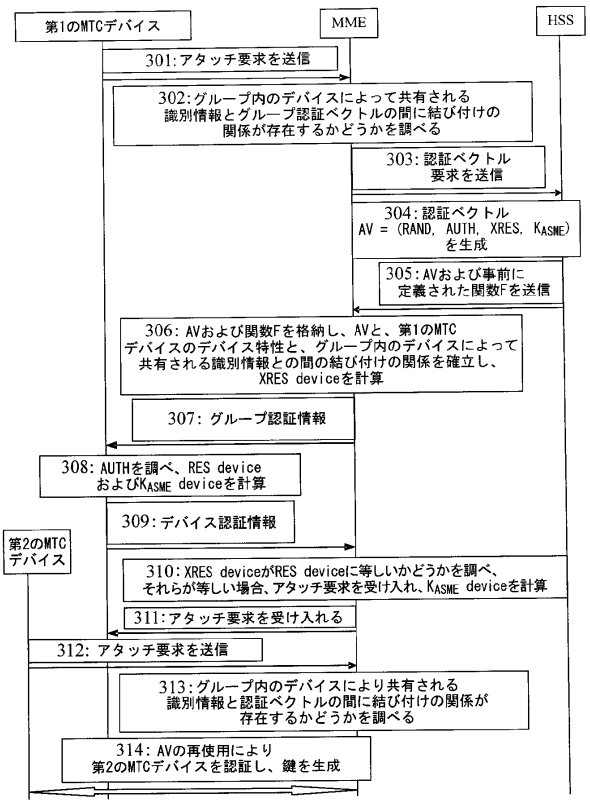
【図４】



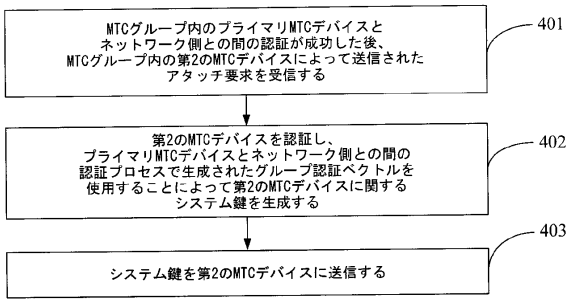
【図５】



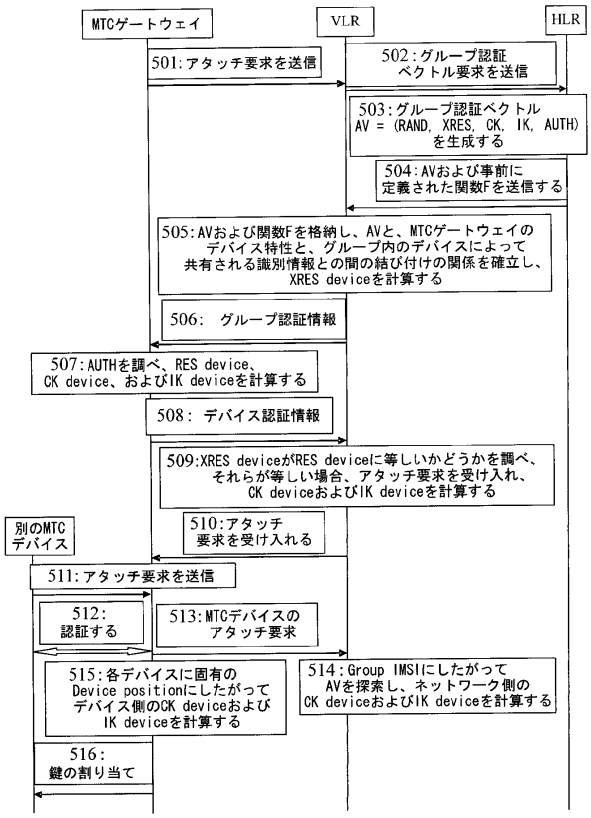
【図６】



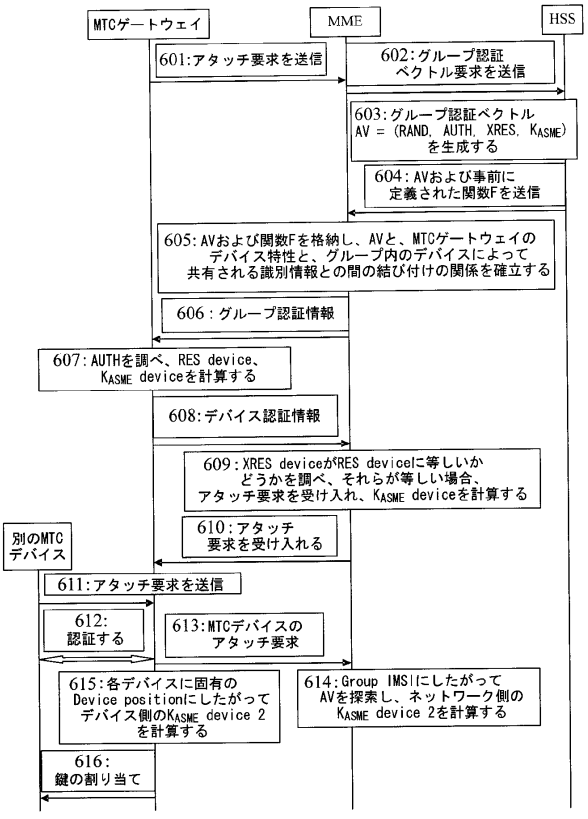
【図７】


MTCグループ内のプライマリMTCデバイスと
ネットワーク側との間の認証が成功した後、
MTCグループ内の第2のMTCデバイスによって送信された
アタッチ要求を受信する
401
第2のMTCデバイスを認証し、
プライマリMTCデバイスとネットワーク側との間の
認証プロセスで生成されたグループ認証ベクトルを
使用することによって第2のMTCデバイスに関する
システム鍵を生成する
402
システム鍵を第2のMTCデバイスに送信する
403

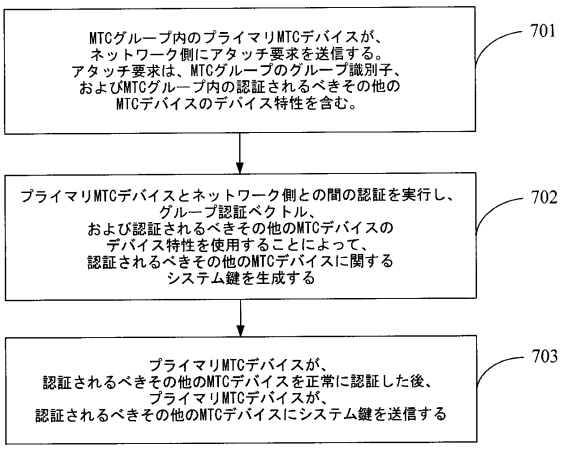
【図８】


MTCゲートウェイ
VLR
HLR
501:アタッチ要求を送信
502:グループ認証
ベクトル要求を送信
503:グループ認証ベクトル
AV = (RAND, XRES, CK, IK, AUTH)
を生成する
504:AVおよび事前に
定義された関数Fを送信する
505:AVおよび関数Fを格納し、AVと、MTCゲートウェイの
デバイス特性と、グループ内のデバイスによって
共有される識別情報との間の結び付けの関係を確立し、
XRES deviceを計算する
506: グループ認証情報
507:AUTHを調べ、RES device、
CK device、およびIK deviceを計算する
508: デバイス認証情報
509:XRES deviceがRES deviceに等しいかどうかを調べ、
それらが等しい場合、アタッチ要求を受け入れ、
CK deviceおよびIK deviceを計算する
別のMTC
デバイス
510:アタッチ
要求を受け入れる
511:アタッチ要求を送信
512:
認証する
513:MTCデバイスの
アタッチ要求
514:Group IMSIにしたがって
AVを探索し、ネットワーク側の
CK deviceおよびIK deviceを計算する
515:各デバイスに固有の
Device positionにしたがって
デバイス側のCK deviceおよび
IK deviceを計算する
516:
鍵の割り当て

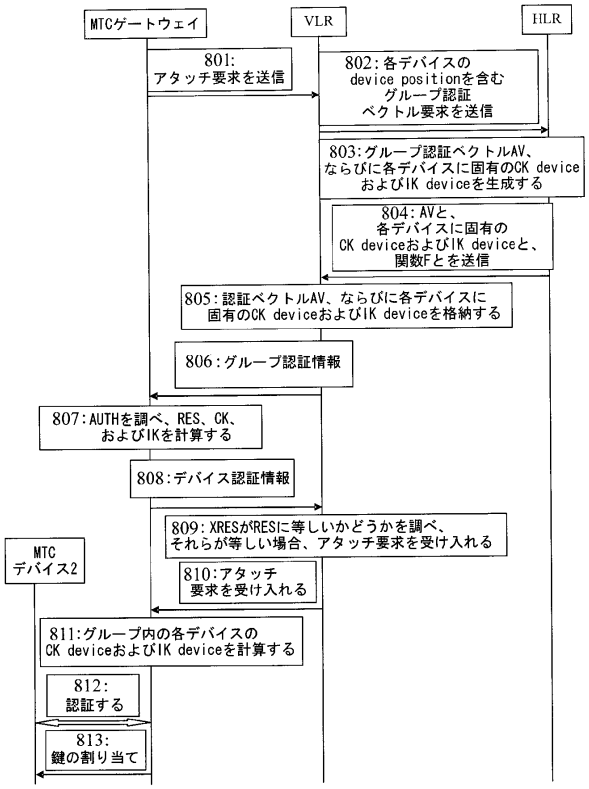
【図９】


MTCゲートウェイ
MME
HSS
601:アタッチ要求を送信
602:グループ認証
ベクトル要求を送信
603:グループ認証ベクトル
AV = (RAND, AUTH, XRES, KASME)
を生成する
604:AVおよび事前に
定義された関数Fを送信
605:AVおよび関数Fを格納し、AVと、MTCゲートウェイの
デバイス特性と、グループ内のデバイスによって
共有される識別情報との間の結び付けの関係を確立する
606:グループ認証情報
607:AUTHを調べ、RES device、
KASME deviceを計算する
608:デバイス認証情報
609:XRES deviceがRES deviceに等しいか
どうかを調べ、それらが等しい場合、
アタッチ要求を受け入れ、KASME deviceを計算する
610:アタッチ
要求を受け入れる
別のMTC
デバイス
611:アタッチ要求を送信
612:
認証する
613:MTCデバイスの
アタッチ要求
614:Group IMSIにしたがって
AVを探索し、ネットワーク側の
KASME device 2を計算する
615:各デバイスに固有の
Device positionにしたがって
デバイス側のKASME device 2
を計算する
616:
鍵の割り当て

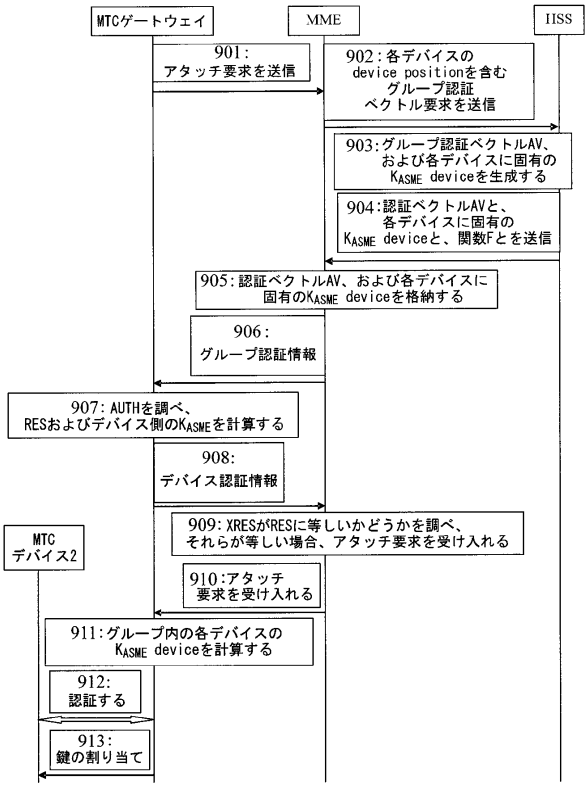
【図１０】


MTCグループ内のプライマリMTCデバイスが、
ネットワーク側にアタッチ要求を送信する。
アタッチ要求は、MTCグループのグループ識別子、
およびMTCグループ内の認証されるべきその他の
MTCデバイスのデバイス特性を含む。
701
プライマリMTCデバイスとネットワーク側との間の認証を実行し、
グループ認証ベクトル、
および認証されるべきその他のMTCデバイスの
デバイス特性を使用することによって、
認証されるべきその他のMTCデバイスに関する
システム鍵を生成する
702
プライマリMTCデバイスが、
認証されるべきその他のMTCデバイスを正常に認証した後、
プライマリMTCデバイスが、
認証されるべきその他のMTCデバイスにシステム鍵を送信する
703

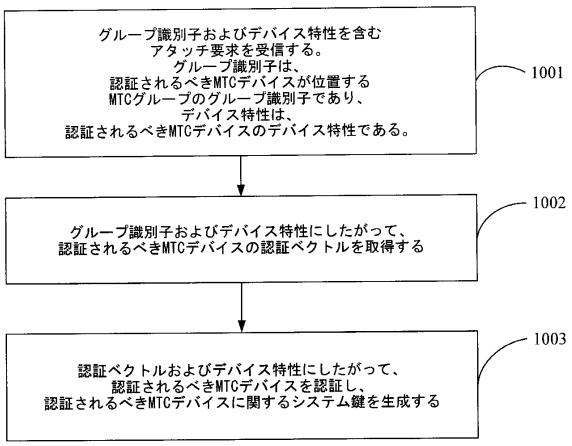
【図１１】



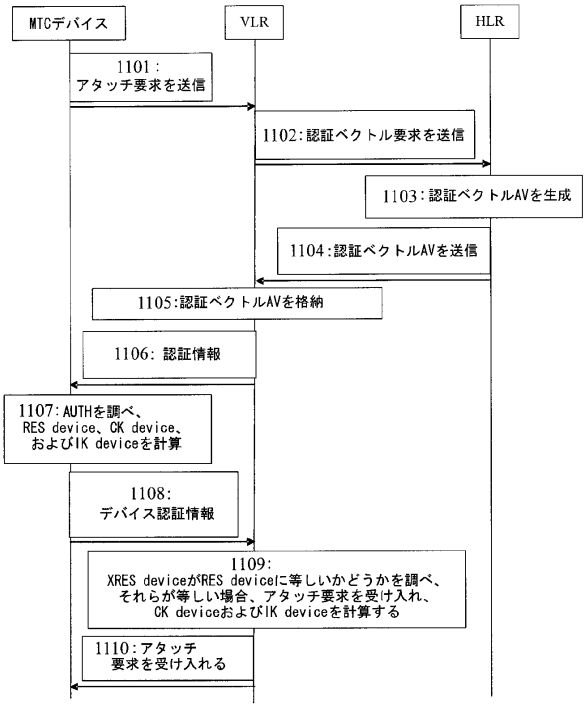
【図１２】



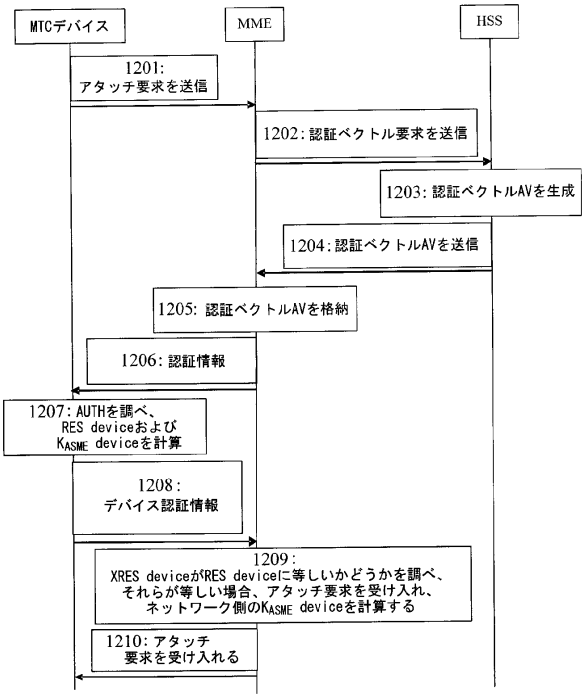
【図１３】



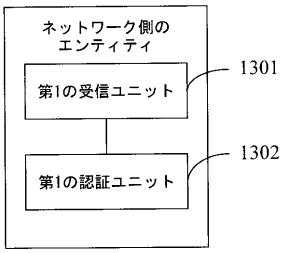
【図１４】



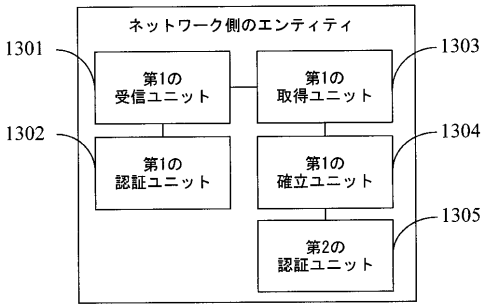
【図１５】



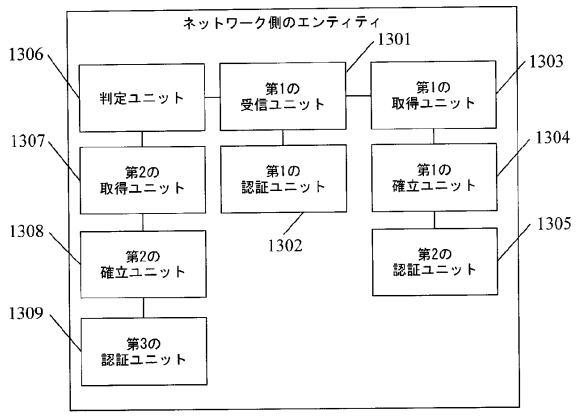
【図１６】



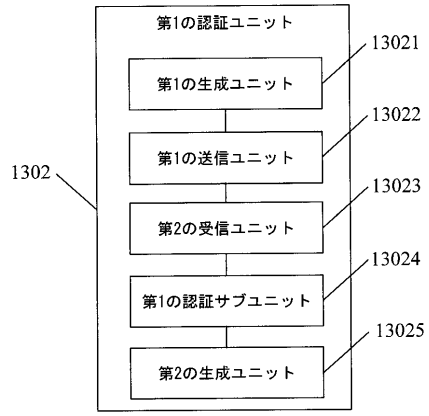
【図１７】



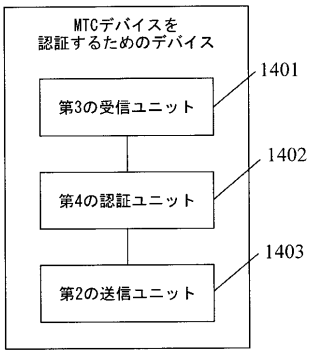
【図１８】



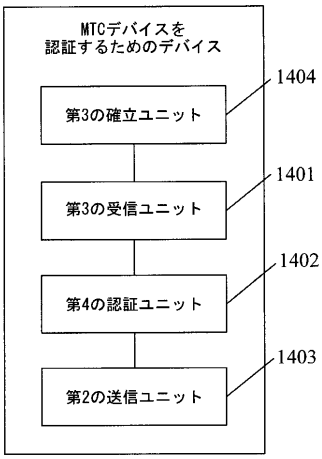
【図１９】



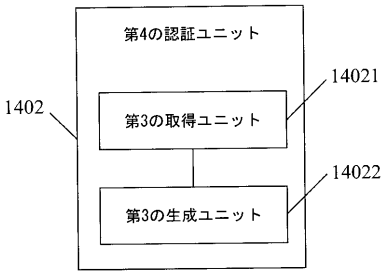
【図２０】



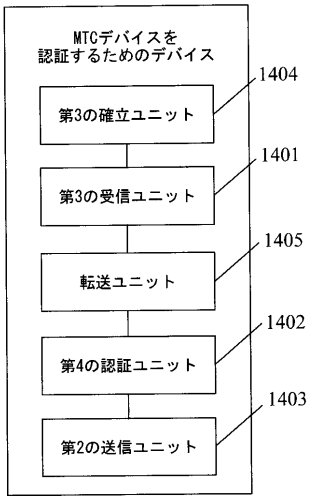
【図２１】



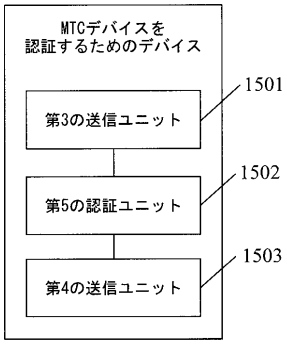
【図２２】



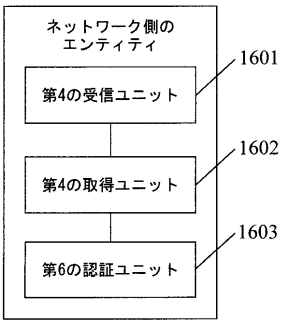
【図２３】



【図２４】



【図２５】



フロントページの続き

(72)発明者　黄　迎新
中華人民共和国５１８１２９広東省深▲セン▼市龍岡区坂田華為本社ビル
(72)発明者　▲劉▼　▲シャオ▼寒
中華人民共和国５１８１２９広東省深▲セン▼市龍岡区坂田華為本社ビル
(72)発明者　メリオー・ローレンス
中華人民共和国５１８１２９広東省深▲セン▼市龍岡区坂田華為本社ビル

審査官　望月　章俊

(56)参考文献　Motorola, On applicability of "group-based MTC features" to RAN2, 3GPP Tdoc R2-102142, 3GPP, ２０１０年　4月　6日
Samsung, RAN enhancements for Machine-type Communicaiton, 3GPP R2-100537, 3GPP, ２０１２年　1月１８日
3GPP TR23.888 V0.3.2, 3GPP, ２０１０年　3月

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｗ４／００－Ｈ０４Ｗ９９／００
Ｈ０４Ｂ７／２４－Ｈ０４Ｂ７／２６
Ｇ０６Ｆ２１／４４