(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4976548号
(P4976548)
(45)発行日　平成24年7月18日(2012.7.18)　(24)登録日　平成24年4月20日(2012.4.20)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 675A
H04W 12/06 (2009.01)　　H04Q 7/00 183
H04L 9/08 (2006.01)　　H04L 9/00 601C

請求項の数 17　(全 17 頁)

(21)出願番号　特願2010-513633 (P2010-513633)
(86)(22)出願日　平成20年8月27日 (2008.8.27)
(65)公表番号　特表2010-533390 (P2010-533390A)
(43)公表日　平成22年10月21日 (2010.10.21)
(86)国際出願番号　PCT/CN2008/072165
(87)国際公開番号　WO2009/030155
(87)国際公開日　平成21年3月12日 (2009.3.12)
審査請求日　平成21年12月24日 (2009.12.24)
(31)優先権主張番号　200710145703.3
(32)優先日　平成19年8月31日 (2007.8.31)
(33)優先権主張国　中国 (CN)
(31)優先権主張番号　200710151700.0
(32)優先日　平成19年9月26日 (2007.9.26)
(33)優先権主張国　中国 (CN)

早期審査対象出願

(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　100089037
弁理士　渡邊　隆
(74)代理人　100110364
弁理士　実広　信哉
(72)発明者　何　承▲東▼
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　石田　信行

最終頁に続く

(54)【発明の名称】端末が移動するときにセキュリティ機能を折衝するための方法、システム、および装置

(57)【特許請求の範囲】
【請求項１】
端末が移動するときにセキュリティ機能を折衝するための方法であって、移動局(UE)が、第2/第3世代(2G/3G)ネットワークからロングタームエボリューション(LTE)ネットワークに移動するとき、
移動性管理エンティティ(MME)が、前記UEから送られたトラッキングエリアアップデート(TAU)要求メッセージを受け取り、かつ前記UEによりサポートされる非アクセスシグナリング(NAS)セキュリティアルゴリズムと、認証ベクトル関連鍵、もしくは前記認証ベクトル関連鍵により導出されるルート鍵とを取得するステップと、
前記MMEが、前記UEによりサポートされる前記NASセキュリティアルゴリズムに従ってNASセキュリティアルゴリズムを選択し、前記認証ベクトル関連鍵または前記ルート鍵によりNAS保護鍵を導出し、かつ前記選択されたNASセキュリティアルゴリズムを運ぶメッセージを前記UEに送るステップと、
前記UEが、その認証ベクトル関連鍵によりNAS保護鍵を導出するステップと
を含む方法。
【請求項２】
前記MMEが前記UEによりサポートされる前記NASセキュリティアルゴリズムを取得する前記ステップが、
前記MMEが、前記UEから送られた前記TAU要求メッセージから、前記UEによりサポートされるセキュリティ機能情報を取得するステップを含み、前記TAU要求メッセージが、前記U

Eによりサポートされる前記NASセキュリティアルゴリズムを含む、請求項1に記載の方法。

【請求項３】

前記MMEが前記UEによりサポートされる前記NASセキュリティアルゴリズムを取得する前記ステップが、

前記MMEが、サービス汎用パケット無線サービス(GPRS)サポートノード(SGSN)から送られた移動性管理コンテキスト応答メッセージから、前記UEによりサポートされるセキュリティ機能情報を取得するステップを含み、前記移動性管理コンテキスト応答メッセージが、前記UEによりサポートされる前記NASセキュリティアルゴリズムを含む、請求項1に記載の方法。

【請求項４】

前記MMEが前記認証ベクトル関連鍵を取得する前記ステップが、

前記MMEが、SGSNから送られた移動性管理コンテキスト応答メッセージから、前記認証ベクトル関連鍵を取得するステップを含み、また

前記MMEが、前記認証ベクトル関連鍵により導出される前記ルート鍵を取得する前記ステップが、

前記MMEが、前記SGSNから送られた前記移動性管理コンテキスト応答メッセージから、前記認証ベクトル関連鍵により導出される前記ルート鍵を取得するステップを含む、請求項1に記載の方法。

【請求項５】

前記SGSNが、前記2Gネットワークの SGSNであるとき、前記認証ベクトル関連鍵は少なくとも、暗号化鍵Kc、または前記暗号化鍵Kcに対して一方向変換が行われた後に得られた値を含み、あるいは

前記SGSNが、前記3Gネットワークの SGSNであるとき、前記認証ベクトル関連鍵は少なくとも、完全性鍵IKおよび暗号化鍵CKを、または前記IKおよび前記暗号化鍵CKに対して一方向変換が行われた後に得られた値を含む、請求項4に記載の方法。

【請求項６】

前記SGSNが、前記2Gネットワークの SGSNであるとき、前記認証ベクトル関連鍵により導出される前記ルート鍵が、暗号化鍵Kc、または前記暗号化鍵Kcに基づいて一方向に変換された値により前記SGSNによって導出されて、次いで、前記MMEに送られ、あるいは

前記SGSNが、前記3Gネットワークの SGSNであるとき、前記認証ベクトル関連鍵により導出される前記ルート鍵が、完全性鍵IKおよび暗号化鍵CK、または前記完全性鍵IKおよび前記暗号化鍵CKに対して一方向変換が行われた後に得られた値により前記SGSNによって導出されて、次いで、前記MMEに送られる、請求項4に記載の方法。

【請求項７】

前記MMEが前記認証ベクトル関連鍵により導出される前記ルート鍵を取得する前記ステップが、

前記MMEが、認証および鍵共有(AKA)手順を介して、前記認証ベクトル関連鍵により導出される前記ルート鍵を直接取得するステップを含む、請求項1に記載の方法。

【請求項８】

前記MMEおよび前記UEがそれぞれ、前記認証ベクトル関連鍵により前記NAS保護鍵を導出する前記ステップが、

前記MMEおよび前記UEが、前記認証ベクトル関連鍵により前記ルート鍵を導出し、次いで、前記導出されたルート鍵により前記NAS保護鍵を導出するステップを含む、請求項1に記載の方法。

【請求項９】

前記MMEが前記選択されたNASセキュリティアルゴリズムを運ぶメッセージを前記UEに送る前記ステップの前に、

前記MMEが前記選択されたNASセキュリティアルゴリズムを運ぶ前記メッセージに対して完全性保護を実施するステップと、

前記UEが、前記選択されたNASセキュリティアルゴリズムを運ぶ前記メッセージを受け取った後に、前記選択されたNASセキュリティアルゴリズムを運ぶ前記メッセージに対して実施された前記完全性保護が、前記導出されたNAS保護鍵に従って正しいかどうかを検出するステップと
をさらに含む、請求項1に記載の方法。
【請求項１０】
前記選択されたNASセキュリティアルゴリズムを運ぶ前記メッセージが、前記UEによりサポートされる前記セキュリティ機能情報をさらに運び、また
前記UEが、前記受け取った前記UEによりサポートされるセキュリティ機能情報が、前記UEにサポートされたセキュリティ機能情報と矛盾していないかどうかを判定することにより、劣化攻撃が行われたかどうかを判定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１１】
前記選択されたNASセキュリティアルゴリズムを運ぶ前記メッセージが、前記UEによりサポートされる前記セキュリティ機能情報をさらに運び、また
前記UEが、前記受け取った前記UEによりサポートされるセキュリティ機能情報が、前記UEによりサポートされるセキュリティ機能情報と矛盾していないかどうかを判定することにより、劣化攻撃が行われたかどうかを判定するステップをさらに含む、請求項3に記載の方法。
【請求項１２】
端末が移動するときにセキュリティ機能を折衝するためのシステムであって、移動局(UE)と移動性管理エンティティ(MME)とを備え、
前記UEが、トラッキングエリアアップデート(TAU)要求メッセージを前記MMEに送り、前記MMEから送られた、選択された非アクセスシグナリング(NAS)セキュリティアルゴリズムを運ぶメッセージを受け取り、認証ベクトル関連鍵によりNAS保護鍵を導出するように適合されており、
前記MMEが、前記UEから送られた前記TAU要求メッセージを受け取り、認証ベクトル関連鍵、もしくは前記認証ベクトル関連鍵により導出されるルート鍵と、前記UEによりサポートされるNASセキュリティアルゴリズムとを取得し、前記UEによりサポートされる前記NASセキュリティアルゴリズムに従ってNASセキュリティアルゴリズムを選択して、前記選択されたNASセキュリティアルゴリズムを運ぶメッセージを生成して前記UEに送信し、前記取得された認証ベクトル関連鍵もしくは前記ルート鍵によりNAS保護鍵を導出するように適合される、システム。
【請求項１３】
前記MMEがさらに、前記UEによりサポートされるセキュリティ機能情報を取得し、前記UEに送られる前記選択されたNASセキュリティアルゴリズムを運ぶメッセージ中で、前記UEによりサポートされる前記セキュリティ機能情報を搬送し、
前記UEがさらに、前記MMEから送られた前記UEによりサポートされる前記セキュリティ機能情報が、前記UEによりサポートされるセキュリティ機能と矛盾していないかどうかを判定することにより、劣化攻撃が行われたかどうかを判定する、請求項12に記載のシステム。
【請求項１４】
取得モジュール、選択モジュール、および鍵導出モジュールを備え、
前記取得モジュールが、移動局(UE)から送られたトラッキングエリアアップデート(TAU)要求メッセージを受け取り、認証ベクトル関連鍵、もしくは前記認証ベクトル関連鍵により導出されるルート鍵と、前記UEによりサポートされる非アクセスシグナリング(NAS)セキュリティアルゴリズムとを取得するように適合され、
前記選択モジュールが、前記UEによりサポートされ、かつ前記取得モジュールにより取得された前記NASセキュリティアルゴリズムに従ってNASセキュリティアルゴリズムを選択し、前記選択されたNASセキュリティアルゴリズムを運ぶメッセージを生成して前記UEに

送信するように適合され、
前記鍵導出モジュールが、前記取得モジュールにより取得された、前記認証ベクトル関連鍵、もしくは前記認証ベクトル関連鍵により導出される前記ルート鍵と、前記選択モジュールにより選択された前記NASセキュリティアルゴリズムとにより、NAS保護鍵を導出するように適合される移動性管理エンティティ(MME)。
【請求項１５】
前記取得モジュールが、前記UEによりサポートされるセキュリティ機能情報をさらに取得し、また前記選択モジュールが、前記選択されたNASセキュリティアルゴリズムを運ぶ前記メッセージ中で、前記UEによりサポートされ、かつ前記取得モジュールにより取得された前記セキュリティ機能情報をさらに搬送する、請求項14に記載のMME。
【請求項１６】
更新モジュール、鍵導出モジュール、ストレージモジュール、および検出モジュールを備え、
前記更新モジュールが、前記UEによりサポートされ、かつ前記ストレージモジュール中に記憶されたセキュリティ機能情報を運ぶトラッキングエリアアップデート(TAU)要求メッセージを移動性管理エンティティ(MME)に送り、また前記MMEから送られた、選択された非アクセスシグナリング(NAS)セキュリティアルゴリズムを運ぶメッセージを受け取るように適合され、
前記鍵導出モジュールが、認証ベクトル関連鍵、および前記更新モジュールにより受信された前記NASセキュリティアルゴリズムによりNAS保護鍵を導出するように適合され、
前記ストレージモジュールが、前記UEによりサポートされる前記セキュリティ機能情報を記憶するように適合され、
前記検出モジュールが、前記UEによりサポートされかつ前記MMEから受け取ったセキュリティ機能情報が、前記UEによりサポートされかつ前記ストレージモジュールに記憶された前記セキュリティ機能情報と矛盾していることを検出した場合、劣化攻撃が行われたと判定するように適合される移動局(UE)。
【請求項１７】
前記MMEから送られた、前記選択されたNASセキュリティアルゴリズムを運ぶ前記メッセージが、前記UEによりサポートされるセキュリティ機能情報をさらに運ぶ、請求項16に記載のUE。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
本出願は、2007年8月31日に出願された中国特許出願第200710145703.3号、および2007年9月26日に出願された中国特許出願第200710151700.0号に対する優先権を主張する2008年8月27日に出願された国際出願第PCT/CN2008/072165号の継続出願であり、それらをすべて参照により本明細書にその全体を組み込む。
【０００２】
本発明は、無線通信技術の分野に関し、より詳細には、端末が移動するときにセキュリティ機能を折衝するための方法およびシステム、MME (mobility management entity:移動性管理エンティティ)、ならびにUE (user equipment:移動局)に関する。
【背景技術】
【０００３】
無線ネットワークは、無線アクセスネットワークおよびコアネットワークを含む。LTE (long term evolution)無線ネットワークのコアネットワークは、MMEを含む。MMEは、第2/第3世代(2G/3G)ネットワークのSGSN (service GPRS (general packet radio service) support node)のものと同様の機能を有しており、主として、移動性管理およびユーザ認証を担当する。2G/3GまたはLTE無線ネットワークにおいて、UEがアイドル状態にあるとき、UEは、SGSNまたはMMEと、それぞれ、NAS (non-access signaling:非アクセスシグナリン

グ)セキュリティ機能を折衝する必要がある。セキュリティ機能は、NASシグナリング暗号化アルゴリズム、対応するNAS完全性保護鍵Knas-int、NAS完全性保護アルゴリズム、および対応するNAS機密性保護鍵Knas-encを含み、それらは、UEとシステムの間のシグナリング送信のために使用され、それにより、UEシグナリングの正常な受信と、通信システムのセキュリティとを保証することができる。

【０００４】

2GのGERAN (GSM (global system for mobile communications) edge radio access network)、または3GのUTRAN (UMTS (universal mobile telecommunications system) terrestrial radio access network)にアクセスしているUEがアイドル状態に移ると、UEは、LTE無線アクセスネットワークのトラッキングエリアに移ることができ、したがって、UEはLTEを介して再度ネットワークにアクセスすることができる。この時点で、TAU (tracking area update:トラッキングエリアアップデート)手順が行われる、すなわち、異種ネットワーク間でTAU手順が行われる。手順中、UEのためにセキュリティ機能折衝を行うエンティティが、例えば、SGSNからMMEへと変わり、またエンティティは異なるセキュリティ機能を有する可能性があるので、UEとネットワーク間のその後の対話の安全性を保証するために、セキュリティ機能折衝手順を再度行うことが必要である。LTEネットワークの場合、セキュリティ機能折衝は、NAS機密性保護アルゴリズムおよびNAS完全性保護アルゴリズム、RRC (radio resource control)機密性保護アルゴリズムおよびRRC完全性保護アルゴリズム、ならびにUP (user plane:ユーザプレーン)機密性保護アルゴリズムのネゴシエーションを含むことに留意されたい。

【０００５】

アイドル状態中のUEにより開始されるTAU手順の場合は、NAS機密性保護アルゴリズム、NAS完全性保護アルゴリズム、および対応するNAS保護鍵の折衝を解決する必要がある。

【０００６】

本発明の実施中に、本発明者は、異種ネットワーク間におけるTAU手順中にセキュリティ機能を折衝するための方法を従来技術では見出すことができず、したがって、UEが、2G/3GネットワークからLTEネットワークに移動するとき、セキュリティ機能折衝を行うことができず、UEとネットワーク間のその後の対話の安全性を保証できないことを発見した。

【発明の概要】

【発明が解決しようとする課題】

【０００７】

したがって、本発明は、端末が移動するときにセキュリティ機能を折衝するための方法を対象とし、2G/3GネットワークからLTEネットワークに移動するとき、アイドル状態にあるUEがセキュリティ機能を折衝できるようにする。

【０００８】

本発明は、端末が移動するときにセキュリティ機能を折衝するためのシステムをさらに対象とし、2G/3GネットワークからLTEネットワークに移動するとき、アイドル状態にあるUEがセキュリティ機能を折衝できるようにする。

【０００９】

本発明は、MMEをさらに対象とし、2G/3GネットワークからLTEネットワークに移動するとき、アイドル状態にあるUEがセキュリティ機能を折衝できるようにする。

【００１０】

本発明は、UE装置をさらに対象とし、2G/3GネットワークからLTEネットワークに移動するとき、アイドル状態にあるUEがセキュリティ機能を折衝できるようにする。

【課題を解決するための手段】

【００１１】

諸目的を達成するために、本発明の技術的な解決策が以下のように実施される。

【００１２】

端末が移動するときにセキュリティ機能を折衝するための方法が提供され、この方法は、以下の諸ステップを含む。

【００１３】
MMEは、UEから送られたTAU要求メッセージを受け取り、UEによりサポートされるNASセキュリティアルゴリズムと、認証ベクトル関連鍵、もしくは認証ベクトル関連鍵により導出されるルート鍵とを取得する。
【００１４】
MMEは、UEによりサポートされるNASセキュリティアルゴリズムに従ってNASセキュリティアルゴリズムを選択し、認証ベクトル関連鍵またはルート鍵によりNAS保護鍵を導出し、選択されたNASセキュリティアルゴリズムを運ぶメッセージをUEに送る。
【００１５】
UEは、その認証ベクトル関連鍵によりNAS保護鍵を導出する。
【００１６】
端末が移動するときにセキュリティ機能を折衝するためのシステムが提供され、このシステムは、UEおよびMMEを含む。
【００１７】
UEは、TAU要求メッセージをMMEに送り、MMEから送られた、選択されたNASセキュリティアルゴリズムを運ぶメッセージを受け取り、認証ベクトル関連鍵によりNAS保護鍵を導出するように適合される。
【００１８】
MMEは、UEから送られたTAU要求メッセージを受け取り、認証ベクトル関連鍵、もしくは認証ベクトル関連鍵により導出されるルート鍵と、UEによりサポートされるNASセキュリティアルゴリズムとを取得し、UEによりサポートされるNASセキュリティアルゴリズムに従ってNASセキュリティアルゴリズムを選択して、選択されたNASセキュリティアルゴリズムを運ぶメッセージを生成してUEに送信し、取得された認証ベクトル関連鍵もしくはルート鍵によりNAS保護鍵を導出するように適合される。
【００１９】
取得モジュール、選択モジュール、および鍵導出モジュールを含むMMEが提供される。
【００２０】
取得モジュールは、UEから送られたTAU要求メッセージを受け取り、認証ベクトル関連鍵、もしくは認証ベクトル関連鍵により導出されるルート鍵と、UEによりサポートされるNASセキュリティアルゴリズムとを取得するように適合される。
【００２１】
選択モジュールは、UEによりサポートされ、かつ取得モジュールにより取得されたNASセキュリティアルゴリズムに従ってNASセキュリティアルゴリズムを選択し、選択されたNASセキュリティアルゴリズムを運ぶメッセージを生成し、メッセージをUEに送信するように適合される。
【００２２】
鍵導出モジュールは、取得モジュールにより取得された認証ベクトル関連鍵、もしくは認証ベクトル関連鍵により導出されるルート鍵と、選択モジュールにより選択されたNASセキュリティアルゴリズムとにより、NAS保護鍵を導出するように適合される。
【００２３】
更新モジュール、鍵導出モジュール、ストレージモジュール、および検出モジュールを含むUEが提供される。
【００２４】
更新モジュールは、UEによりサポートされ、かつストレージモジュール中に記憶されたセキュリティ機能情報を運ぶTAU要求メッセージをMMEに送り、またMMEから送られた、選択されたNASセキュリティアルゴリズムを運ぶメッセージを受け取るように適合される。
【００２５】
鍵導出モジュールは、認証ベクトル関連鍵、および更新モジュールにより受信されたNASセキュリティアルゴリズムによりNAS保護鍵を導出するように適合される。
【００２６】

ストレージモジュールは、UEによりサポートされるセキュリティ機能情報を記憶するように適合される。

【００２７】

検出モジュールは、UEによりサポートされかつMMEから受け取ったセキュリティ機能情報が、UEによりサポートされかつストレージモジュールに記憶されたセキュリティ機能情報と矛盾していることを検出した場合、劣化攻撃(degradation attack)が行われたと判定するように適合される。

本発明は、また、端末が移動するときにセキュリティ機能を折衝するための方法であって、移動局(UE; user equipment)が、第2/第3世代(2G/3G)ネットワークからロングタームエボリューション(LTE; long term evolution)ネットワークに移動するとき、

移動性管理エンティティ(MME; mobility management entity)が、前記UEから送られたトラッキングエリアアップデート(TAU; tracking area update)要求メッセージを受け取り、かつ前記UEによりサポートされる非アクセスシグナリング(NAS; non-access signaling)セキュリティアルゴリズムと、認証ベクトル関連鍵、もしくは前記認証ベクトル関連鍵により導出されるルート鍵とを取得するステップと、

前記MMEが、前記UEによりサポートされる前記NASセキュリティアルゴリズムに従ってNASセキュリティアルゴリズムを選択し、前記認証ベクトル関連鍵または前記ルート鍵によりNAS保護鍵を導出し、かつ前記選択されたNASセキュリティアルゴリズムを運ぶメッセージを前記UEに送るステップとを含む方法である。

【００２８】

本発明の技術的な解決策では、MMEは、UEから送られたTAU要求メッセージを受け取り、認証ベクトル関連鍵、もしくは認証ベクトル関連鍵により導出されるルート鍵と、UEによりサポートされるNASセキュリティアルゴリズムとを取得し、次いで、UEによりサポートされるNASセキュリティアルゴリズムに従ってNASセキュリティアルゴリズムを選択し、選択されたNASセキュリティアルゴリズムを運ぶメッセージを生成し、かつそのメッセージをUEに送信し、それにより、UEおよびMMEがNASセキュリティアルゴリズムを共用することを可能にする。さらに、MMEは、認証ベクトル関連鍵、もしくは認証ベクトル関連鍵により導出されるルート鍵によりNAS保護鍵を導出し、またUEは、認証ベクトル関連鍵によりNAS保護鍵を導出し、それにより、MMEおよびUEがNAS保護鍵を共用することを可能にする。このような方法で、2G/3GネットワークからLTEネットワークに移動するとき、UEは、MMEとNASセキュリティアルゴリズムおよびNAS保護鍵を折衝することができ、したがって、異種ネットワーク間のTAU手順におけるセキュリティ機能折衝プロセスが達成され、それにより、UEとネットワーク間のその後の対話の安全性を保証することができる。

【００２９】

さらに、本発明を、UEがLTEネットワーク内で移動する場合のセキュリティ機能折衝手順に適用することも可能である。

【図面の簡単な説明】

【００３０】

【図１】端末が移動するときにセキュリティ機能を折衝するための本発明の第1の実施形態による方法の流れ図である。

【図２】端末が移動するときにセキュリティ機能を折衝するための本発明の第2の実施形態による方法の流れ図である。

【図３】端末が移動するときにセキュリティ機能を折衝するための本発明の第3の実施形態による方法の流れ図である。

【図４】端末が移動するときにセキュリティ機能を折衝するための本発明の実施形態によるシステムの構造図である。

【発明を実施するための形態】

【００３１】

本発明の諸実施形態で提供される、端末が移動するときにセキュリティ機能を折衝するための方法では、UEが、2G/3GネットワークからLTEネットワークに移動するとき、MMEは、UEから送られたTAU要求メッセージを受け取り、かつUEによりサポートされるNASセキュリティアルゴリズムと、認証ベクトル関連鍵、もしくは認証ベクトル関連鍵により導出されるルート鍵とを取得する。次いで、MMEは、UEによりサポートされるNASセキュリティアルゴリズムに従ってNASセキュリティアルゴリズムを選択し、認証ベクトル関連鍵、もしくはその認証ベクトル関連鍵により導出されるルート鍵によりNAS保護鍵を導出し、選択されたNASセキュリティアルゴリズムを運ぶメッセージをUEに送信する。UEは、認証ベクトル関連鍵によりNAS保護鍵を導出する。

【００３２】

本発明の実施形態は、特有の実施形態および添付の図面を参照して、以下で詳細に述べる。

【００３３】

UEがUTRAN/GERANにアクセスした後にアイドル状態に入ったと仮定する。この場合、LTEネットワークのトラッキングエリアに移動すると、UEはTAU手順を開始する。

【００３４】

図1は、端末が移動するときにセキュリティ機能を折衝するための本発明の第1の実施形態による方法の流れ図である。図1を参照すると、本方法は以下の諸ステップを含む。

【００３５】

ステップ100で、UEは、TAU要求をMMEに送る。

【００３６】

このステップでは、UEは、LTE無線アクセスネットワークのeNB (evolved Node B)を介して新しいMMEにTAU要求を送る。説明の便宜上、eNBを介するUEとMMEとの間の通信は、以下の説明では、UEとMMEの間の通信に簡略化している。

【００３７】

このステップで、UEからMMEに送られるTAU要求は、当業者に知られたTMSI (temporary mobile subscriber identity:仮の移動局識別子)など、いくつかのパラメータを運ぶだけではなく、UEによりサポートされるセキュリティ機能情報も運ぶことができる。セキュリティ機能情報は、NASセキュリティアルゴリズム(NAS完全性保護アルゴリズムおよび/またはNAS機密性保護アルゴリズム)を含み、またRRCセキュリティアルゴリズム(RRC完全性保護アルゴリズムおよび/またはRRC機密性保護アルゴリズム)、またはUPセキュリティアルゴリズム(機密性保護アルゴリズム)を含むこともできる。

【００３８】

ステップ101～102で、MMEは、UEによりサポートされるNASセキュリティアルゴリズムを取得し、移動性管理コンテキスト要求メッセージをSGSNに送る。メッセージを受け取った後、SGSNは、認証ベクトル関連鍵を運ぶ移動性管理コンテキスト応答メッセージをMMEに送る。

【００３９】

ステップ100で、UEが、MMEに送られたTAU要求中で、UEによりサポートされるNASセキュリティアルゴリズムを伝えなかった場合、移動性管理コンテキスト要求メッセージを受け取った後に、SGSNは、UEによりサポートされるNASセキュリティアルゴリズムを照会し、照会されたUEによりサポートされるNASセキュリティアルゴリズムを、MMEに送られる移動性管理コンテキスト応答メッセージ中で搬送する。NASセキュリティアルゴリズムは、NAS完全性保護アルゴリズムおよび/またはNAS機密性保護アルゴリズムである。

【００４０】

UEが、2GネットワークからLTEネットワークのトラッキングエリアに移動するとき、上記プロセスにおけるSGSNは、2GネットワークのSGSNであり、また認証ベクトル関連鍵は少なくとも、暗号化鍵Kc、またはKcに対して一方向変換が行われた後に得られた値Kc'を含む。UEが、3GネットワークからLTEネットワークのトラッキングエリアに移動するとき、上記プロセスのSGSNは、3GネットワークのSGSNであり、また認証ベクトル関連鍵は少なく

とも、完全性鍵IKおよび暗号化鍵CK、またはIKおよびCKに対して一方向変換が行われた後の値IK'およびCK'を含む。

【００４１】

一方向変換とは、ターゲットのパラメータを得るために、元のパラメータを特定のアルゴリズムを用いることにより変換する変換手順を指すが、ターゲットのパラメータにより、元のパラメータを得ることはできない。例えば、Kcに関しては、アルゴリズムｆ(Kc)を用いることによりKc'が取得されるが、Kcを、どんな逆変換アルゴリズムを用いてもKc'から導出できない場合、その変換は一方向変換である。

【００４２】

ステップ103で、MMEは、UEによりサポートされるNASセキュリティアルゴリズム、およびMMEによりサポートされるNASセキュリティアルゴリズム、ならびにシステムにより許容されるNASセキュリティアルゴリズムに従って、新しいNASセキュリティアルゴリズムを選択し、認証ベクトル関連鍵によりルート鍵Kasmeを導出し、次いで、KasmeによりNAS保護鍵を導出する。NAS保護鍵は、NAS完全性保護鍵Knas-intおよび/またはNAS機密性保護鍵Knas-encを含む。

【００４３】

ステップ104で、MMEは、選択されたNASセキュリティアルゴリズムを運ぶTAU受入れメッセージを生成する。

【００４４】

このステップで、MMEはさらに、TAU受入れメッセージに対してNAS完全性保護を実施することができる。例えば、MMEは、ステップ103で得られたNAS完全性保護鍵Knas-int、TAU受入れにおける情報、および選択されたNASセキュリティアルゴリズム中のNAS完全性保護アルゴリズムに従って、NAS完全性保護のメッセージ認証コード(NAS-MAC)の値を導出し、次いで、その値をTAU受入れメッセージで運び、TAU受入れメッセージをUEに送る。

【００４５】

このステップにおけるTAU受入れメッセージはさらに、UEによりサポートされるセキュリティ機能情報を運ぶことができる。

【００４６】

ステップ105で、UEは、MMEにより選択されたNASセキュリティアルゴリズムを運ぶTAU受入れメッセージを受け取り、折衝されたNASセキュリティアルゴリズムを取得し、次いで、その現在の認証ベクトル関連鍵(例えば、元のネットワークが3Gである場合は、IKおよびCK、またはIKおよびCKにより導出されたIK'およびCK'、あるいは元のネットワークが2Gである場合は、KcまたはKcにより導出されたKc')によりルート鍵Kasmeを導出し、さらに、ルート鍵によりNAS保護鍵を導出する。NAS保護鍵は、NAS完全性保護鍵Knas-int、および/またはNAS機密性保護鍵Knas-encを含む。

【００４７】

このステップで、UEはさらに、TAU受入れメッセージに対して行われた完全性保護が正しいかどうかを検出することができる。正しくない場合、現在のセキュリティ機能折衝は失敗したと判定し、セキュリティ機能折衝手順を再度開始することができる。例えば、UEは、導出されたNAS機密性保護鍵Knas-enc、TAU受入れにおける情報、およびTAU受入れメッセージ中で運ばれたNAS完全性保護アルゴリズムによりNAS-MACを導出し、次いで、導出されたNAS-MACが、TAU受入れメッセージ中で運ばれたNAS-MACと同じものであるかどうかを比較する。同じであれば、メッセージは、送信中に変更されていないことを示すが、同じではない場合、送信中にメッセージが変更されていると考えられ、したがって、現在のセキュリティ機能折衝は失敗したと判定される。

【００４８】

ステップ104で、TAU受入れメッセージがさらに、UEによりサポートされるセキュリティ機能情報を運ぶ場合、このステップで、UEはさらに、UEによりサポートされ、かつTAU受入れメッセージ中で運ばれるセキュリティ機能情報を、UE中に記憶されたセキュリティ機能情報と比較することができる。2つのものが、互いに矛盾しない場合、劣化攻撃が行わ

れていないと判定され、そうではなくて矛盾する場合は、劣化攻撃が行われており、現在のセキュリティ機能折衝が失敗したと判定され、セキュリティ機能折衝手順を再度開始することができ、それにより、劣化攻撃を阻止することができる。

【００４９】

劣化攻撃に対しては、UEは、2つのセキュリティアルゴリズム、すなわち、高強度(high strength)アルゴリズムA1および低強度(low strength)アルゴリズムA2を同時にサポートし、MMEもまた2のアルゴリズムをサポートするものと仮定される。この方法では、高強度アルゴリズムA1が、UEとMMEの間で折衝されるべきである。しかし、UEが、UEによりサポートされるセキュリティ機能情報をMMEへと送る経路中で、攻撃者が、例えば、低強度アルゴリズムA2だけが維持されるなど、UEのセキュリティ機能情報を変更した場合、あるいはMMEがNASセキュリティアルゴリズムを選択するとき、UEによりサポートされるセキュリティ機能情報が攻撃者により変更されて、低強度アルゴリズムA2だけが維持される場合、MMEは、低強度アルゴリズムA2を選択し、それをUEに送ることができるだけである。すなわち、UEとMMEの間の折衝を通して、高強度アルゴリズムA1ではなくて、低強度アルゴリズムA2が得られ、したがって、攻撃者は、より容易に攻撃を行うことが可能になり、それがいわゆる劣化攻撃である。本発明の実施形態では、MMEは、UEによりサポートされるセキュリティ機能情報をUEに送り、UEは、送られたUEによりサポートされるセキュリティ機能情報が、UEによりサポートされるセキュリティ機能情報と矛盾していないかどうかを検出し、それにより、劣化攻撃を検出し、さらに阻止する。

【００５０】

MMEが、ステップ103で、認証ベクトル関連鍵によりNAS保護鍵を最終的に導出する手順は、ステップ104およびステップ105に関していずれの時間的な順序にも限定されず、その手順は、ステップ104の前に実施することが可能であり、またはステップ104とステップ105の間で、あるいはステップ105の後に実施することも可能である。

【００５１】

上記プロセスで、MMEおよびUEはまた、ルート鍵を導出し、次いで、そのルート鍵によりNAS保護鍵を導出することを必要とせず、認証ベクトル関連鍵により、NAS保護鍵を直接導出することもできる。

【００５２】

上記プロセスで、認証ベクトル関連鍵によりNAS保護鍵を導出するために、UEにより使用される導出方法は、認証ベクトル関連鍵によりNAS保護鍵を導出するためにネットワーク側で使用される方法と同じでなければならないことを当業者であれば理解されたい。導出法は、任意の一方向変換、例えば、Kasme=f (IK、CK、他のパラメータ)、Knas-enc=f (Kasme、NAS機密性保護アルゴリズム、他のパラメータ)、およびKnas-int=f (Kasme、NAS完全性保護アルゴリズム、他のパラメータ)を使用することができる。

【００５３】

さらに、本発明のこの実施形態を強調表示するために、セキュリティに関係しない手順は、上記プロセスにおいて、ステップ102とステップ104の間で除外されている。

【００５４】

上記プロセスを介して、UEおよびMMEは、NASセキュリティアルゴリズムおよびNAS保護鍵を共用することができ、それにより、NASセキュリティ機能の折衝を実施することができる。

【００５５】

図2は、端末が移動するときにセキュリティ機能を折衝するための本発明の第2の実施形態による方法の流れ図である。図2を参照すると、本方法は以下の諸ステップを含む。

【００５６】

ステップ200は、ステップ100と同じであり、したがって、その説明をここでは除外する。

【００５７】

ステップ201～203で、MMEは、UEによりサポートされるNASセキュリティアルゴリズムを

取得し、コンテキスト要求メッセージをSGSNに送る。コンテキスト要求メッセージを受け取った後、SGSNは、その認証ベクトル関連鍵によりルート鍵を導出し、次いで、ルート鍵を運ぶコンテキスト応答メッセージをMMEに送る。

【００５８】

本発明の他の実施形態では、ステップ200で、UEが、MMEに送られたTAU要求中で、UEによりサポートされるNASセキュリティアルゴリズムを伝えなかった場合、移動性管理コンテキスト要求メッセージを受け取った後に、SGSNは、UEによりサポートされるNASセキュリティアルゴリズムを照会し、照会されたUEによりサポートされるNASセキュリティアルゴリズムを、MMEに送られる移動性管理コンテキスト応答メッセージ中で搬送する。NASセキュリティアルゴリズムは、NAS完全性保護アルゴリズムおよび/またはNAS機密性保護アルゴリズムである。

【００５９】

UEが、2GネットワークからLTEネットワークのトラッキングエリアに移動するとき、上記プロセスにおけるSGSNは、2GネットワークのSGSNであり、またルート鍵は、Kcにより、またはKcに対して一方向変換が行われた後に取得されたKc'により、SGSNによって導出されるルート鍵Kasmeである。UEが、3GネットワークからLTEネットワークのトラッキングエリアに移動するとき、上記プロセスのSGSNは、3GネットワークのSGSNであり、ルート鍵は、IKおよびCK、またはIKおよびCKに対して一方向変換が行われた後のIK'およびCK'により、SGSNによって導出されたKasmeである。

【００６０】

ステップ204で、MMEは、UEによりサポートされるNASセキュリティアルゴリズム、およびMMEによりサポートされるNASセキュリティアルゴリズム、ならびにシステムにより許容されるNASセキュリティアルゴリズムに従って、新しいNASセキュリティアルゴリズムを選択し、次いで、ルート鍵によりNAS保護鍵を導出する。NAS保護鍵は、NAS完全性保護鍵Knas-intおよび/またはNAS機密性保護鍵Knas-encを含む。

【００６１】

ステップ205で、MMEは、選択されたNASセキュリティアルゴリズムを運ぶTAU受入れメッセージを生成する。

【００６２】

このステップで、MMEはさらに、TAU受入れメッセージに対してNAS完全性保護を実施することができる。このステップにおけるTAU受入れメッセージはさらに、UEによりサポートされるセキュリティ機能情報を運ぶことができる。

【００６３】

ステップ206で、UEは、MMEにより選択されたNASセキュリティアルゴリズムを運ぶTAU受入れメッセージを受け取り、折衝されたNASセキュリティアルゴリズムを取得し、次いで、その現在の認証ベクトル関連鍵(例えば、元のネットワークが3Gである場合は、IKおよびCK、またはIKおよびCKにより導出されたIK'およびCK'、あるいは元のネットワークが2Gである場合は、KcまたはKcにより導出されたKc')によりルート鍵Kasmeを導出し、さらに、ルート鍵によりNAS保護鍵を導出する。NAS保護鍵は、NAS完全性保護鍵Knas-int、および/またはNAS機密性保護鍵Knas-encを含む。

【００６４】

このステップで、UEはさらに、TAU受入れメッセージに対して行われた完全性保護が正しいかどうかを検出することができる。正しくない場合、現在のセキュリティ機能折衝は失敗したと判定し、セキュリティ機能折衝手順を再度開始することができる。

【００６５】

本発明の他の実施形態では、ステップ205で、TAU受入れメッセージがさらに、UEによりサポートされるセキュリティ機能情報を運ぶ場合、このステップで、UEはさらに、TAU受入れメッセージ中で運ばれる、UEによりサポートされるセキュリティ機能情報を、UEによりサポートされるセキュリティ機能情報と比較することができる。2つのものが、互いに矛盾しない場合、劣化攻撃が行われていないと判定され、そうではなくて矛盾する場合は

、劣化攻撃が行われており、現在のセキュリティ機能折衝が失敗したと判定され、セキュリティ機能折衝手順を、再度開始することができ、それにより、劣化攻撃を阻止することができる。

【００６６】

本発明の他の実施形態では、MMEが、ステップ204で、ルート鍵によりNAS保護鍵を導出する手順は、ステップ205およびステップ206に関していずれの時間的な順序にも限定されず、その手順は、ステップ205の前に実施することが可能であり、またはステップ205とステップ206の間で、あるいはステップ206の後に実施することも可能である。

【００６７】

上記のプロセスで、認証ベクトル関連鍵によりNAS保護鍵を導出するために、UEにより使用される導出方法は、認証ベクトル関連鍵によりNAS保護鍵を導出するために、ネットワーク側で使用される方法と同じでなくてはならないことを当業者であれば理解されたい。

【００６８】

上記プロセスを介して、UEおよびMMEは、NASセキュリティアルゴリズムおよびNAS保護鍵を共用することができ、それにより、NASセキュリティ機能の折衝を実施することができる。

【００６９】

図3は、端末が移動するときにセキュリティ機能を折衝するための本発明の第3の実施形態による方法の流れ図である。図3を参照すると、本方法は、以下の諸ステップを含む。

【００７０】

ステップ300は、ステップ100と同じであり、したがって、その説明をここでは除外する。

【００７１】

ステップ301～302で、MMEは、移動性管理コンテキスト要求および応答メッセージを介して、SGSNから、UEによりサポートされるNASセキュリティアルゴリズムを取得する。

【００７２】

本発明の他の実施形態では、ステップ300で、UEが、MMEに送られたTAU要求中で、UEによりサポートされるNASセキュリティアルゴリズムを伝えなかった場合、移動性管理コンテキスト要求メッセージを受け取った後、SGSNは、UEによりサポートされるNASセキュリティアルゴリズムを照会し、照会されたUEによりサポートされるNASセキュリティアルゴリズムを、MMEに送られる移動性管理コンテキスト応答メッセージ中で搬送する。NASセキュリティアルゴリズムは、NAS完全性保護アルゴリズムおよび/またはNAS機密性保護アルゴリズムである。

【００７３】

ステップ303で、MMEは、AKA (authentication and key agreement:認証および鍵共有)手順を介して、HSS (home subscriber server:ホーム加入者サーバ)から認証ベクトル関連鍵により導出されるルート鍵Kasmeを取得する。

【００７４】

ステップ304で、MMEは、UEによりサポートされるNASセキュリティアルゴリズム、およびMMEによりサポートされるNASセキュリティアルゴリズム、ならびにシステムにより許容されるNASセキュリティアルゴリズムに従って、新しいNASセキュリティアルゴリズムを選択し、次いで、Kasmeにより他のNAS保護鍵を導出する。NAS保護鍵は、完全性保護鍵Knas-intおよびNAS機密性保護鍵Knas-encを含む。

【００７５】

ステップ305で、MMEは、選択されたNASセキュリティアルゴリズムを運ぶNAS SMC (security mode command)要求メッセージを生成し、UEに送る。SMC要求メッセージは、TAU受入れメッセージ中で運ぶことができる。

【００７６】

このステップで、MMEはさらに、SMC受入れメッセージに対してNAS完全性保護を実施す

ることができる。例えば、MMEは、ステップ304で得られたNAS完全性保護鍵Knas-int、SMC要求メッセージ中の情報、および選択されたNASセキュリティアルゴリズム中のNAS完全性保護アルゴリズムに従って、NAS完全性保護のメッセージ認証コード(NAS-MAC)の値を導出し、次いで、その値をSMC要求メッセージで運び、SMC要求メッセージをUEに送る。

【００７７】

このステップにおけるSMC要求メッセージはさらに、UEによりサポートされるセキュリティ機能情報を運ぶことができる。

【００７８】

ステップ306で、UEは、MMEにより選択されたNASセキュリティアルゴリズムを運ぶSMC要求メッセージを受け取り、UEによりサポートされかつMMEにより選択されたNASセキュリティアルゴリズムを取得し、次いで、そのAKA手順で取得された現在の認証ベクトル関連鍵によりルート鍵を導出し、ルート鍵によりNAS保護鍵を導出する。NAS保護鍵は、NAS完全性保護鍵Knas-intおよびNAS機密性保護鍵Knas-encを含む。

【００７９】

この実施形態では、このステップで、UEはさらに、TAU受入れメッセージに対して行われた完全性保護が正しいかどうかを検出することができる。正しくない場合、現在のセキュリティ機能折衝は失敗したと判定し、セキュリティ機能折衝手順を再度開始することができる。例えば、UEは、導出されたNAS機密性保護鍵Knas-enc、TAU受入れメッセージ中の情報、およびTAU受入れメッセージ中で運ばれたNAS完全性保護アルゴリズムによりNAS-MACを導出し、次いで、導出されたNAS-MACが、TAU受入れメッセージ中で運ばれたNAS-MACと同じものであるかどうかを比較する。同じであれば、メッセージは、送信中に変更されていないことを示すが、同じではない場合、送信中にメッセージが変更されていると考えられ、したがって、現在のセキュリティ機能折衝は失敗したと判定される。

【００８０】

本発明の他の実施形態では、ステップ305で、SMC要求メッセージがさらに、UEによりサポートされるセキュリティ機能情報を運ぶ場合、このステップで、UEはさらに、UEによりサポートされ、かつSMC要求メッセージ中で運ばれるセキュリティ機能情報を、UEによりサポートされるセキュリティ機能情報と比較することができる。2つのものが互いに矛盾しない場合、劣化攻撃が行われていないと判定され、そうではなくて矛盾する場合は、劣化攻撃が行われており、現在のセキュリティ機能折衝が失敗したと判定され、セキュリティ機能折衝手順を再度開始することができ、それにより、劣化攻撃を阻止することができる。

【００８１】

ステップ307で、UEは、SMC完了応答メッセージをMMEに送る。SMC完了応答メッセージは、TAU完了メッセージ中で運ぶこともできる。

【００８２】

ステップ308で、MMEは、TAU受入れメッセージを返す。

【００８３】

本発明の他の実施形態では、ステップ305で、SMC要求メッセージを、TAU受入れメッセージ中で運ぶことによってUEに送るときは、ステップ308は、ステップ305と組み合わされる。

【００８４】

ステップ309で、UEは、TAU完了メッセージを返す。

【００８５】

本発明の他の実施形態では、ステップ307で、SMC完了応答メッセージがTAU完了メッセージ中で運ばれるときは、ステップ309は、ステップ307と組み合わされる。

【００８６】

上記のプロセスを通して、NASセキュリティ機能の折衝が行われる。

【００８７】

本発明の諸実施形態による方法中の諸ステップのすべてまたは一部は、関連するハード

ウェアに命令するプログラムにより実施することができ、またプログラムは、ROM（読取り専用メモリ)/RAM（ランダムアクセスメモリ)、磁気ディスク、または光ディスクなど、コンピュータで読取り可能なストレージ媒体中に記憶することができることを当業者であれば理解されたい。

【００８８】

図4は、端末が移動するときにセキュリティ機能を折衝するための本発明の実施形態によるシステムの構造図である。図4を参照すると、システムは、UEおよびMMEを含む。

【００８９】

UEは、TAU要求メッセージをMMEに送り、MMEから送られた、選択されたNASセキュリティアルゴリズムを運ぶメッセージを受け取り、かつ認証ベクトル関連鍵によりNAS保護鍵を導出するように適合される。

【００９０】

MMEは、UEから送られたTAU要求メッセージを受け取り、認証ベクトル関連鍵、もしくは認証ベクトル関連鍵により導出されるルート鍵とUEによりサポートされるNASセキュリティアルゴリズムとを取得し、UEによりサポートされるNASセキュリティアルゴリズムに従ってNASセキュリティアルゴリズムを選択し、選択されたNASセキュリティアルゴリズムを運ぶメッセージを生成してUEに送り、かつ取得された認証ベクトル関連鍵、もしくは認証ベクトル関連鍵により導出されるルート鍵によってNAS保護鍵を導出するように適合される。

【００９１】

システムでは、MMEはさらに、UEによりサポートされるセキュリティ機能情報を取得し、さらに、UEに送られる選択されたNASセキュリティアルゴリズムを運ぶメッセージ中で、UEによりサポートされるセキュリティ機能情報を搬送し、またUEはさらに、UEによりサポートされ、MMEから送られたセキュリティ機能情報が、UEによりサポートされるセキュリティ機能情報と矛盾していないかどうかを判定することにより、劣化攻撃が行われたかどうかを判定する。

【００９２】

具体的には、MMEは、取得モジュール、選択モジュール、および鍵導出モジュールを含む。

【００９３】

取得モジュールは、UEから送られたTAU要求メッセージを受け取り、認証ベクトル関連鍵、もしくは認証ベクトル関連鍵により導出されるルート鍵と、UEによりサポートされるNASセキュリティアルゴリズムとを取得するように適合される。選択モジュールは、UEによりサポートされ、取得モジュールにより取得されたNASセキュリティアルゴリズムに従ってNASセキュリティアルゴリズムを選択し、選択されたNASセキュリティアルゴリズムを運ぶメッセージを生成し、UEに送るように適合される。鍵導出モジュールは、取得モジュールにより取得された認証ベクトル関連鍵、もしくは認証ベクトル関連鍵により導出されるルート鍵と、選択されたNASセキュリティアルゴリズムとにより、NAS保護鍵を導出するように適合される。

【００９４】

取得モジュールはさらに、UEによりサポートされるセキュリティ機能情報を取得し、また選択モジュールはさらに、UEによりサポートされ、取得モジュールにより取得されたセキュリティ機能情報を、選択されたNASセキュリティアルゴリズムを運ぶメッセージ中で搬送する。

【００９５】

UEは、更新モジュール、鍵導出モジュール、ストレージモジュール、および検出モジュールを含む。

【００９６】

更新モジュールは、UEによりサポートされ、ストレージモジュール中に記憶されたセキュリティ機能情報を運ぶTAU要求メッセージをMMEに送り、MMEから送られた、選択されたN

ASセキュリティアルゴリズムを運ぶメッセージを受け取るように適合される。鍵導出モジュールは、認証ベクトル関連鍵、および更新モジュールにより受信された、選択されたNASセキュリティアルゴリズムにより、NAS保護鍵を導出するように適合される。ストレージモジュールは、UEによりサポートされるセキュリティ機能情報を記憶するように適合される。検出モジュールは、UEによりサポートされ、MMEから受け取ったセキュリティ機能情報が、UEによりサポートされ、ストレージモジュール中に記憶されたセキュリティ機能情報と矛盾することを検出したとき、劣化攻撃が行われたと判定するように適合される。MMEから送られた、選択されたNASセキュリティアルゴリズムを運ぶメッセージはさらに、UEによりサポートされるセキュリティ機能情報を搬送する。

【００９７】

本発明の諸実施形態で提供される技術的な解決策においては、MMEは、UEから送られたTAU要求メッセージを受け取り、UEによりサポートされるNASセキュリティアルゴリズムと、認証ベクトル関連鍵、もしくは認証ベクトル関連鍵により導出されるルート鍵とを取得し、次いで、UEによりサポートされるNASセキュリティアルゴリズムに従ってNASセキュリティアルゴリズムを選択し、選択されたNASセキュリティアルゴリズムを運ぶメッセージを生成してUEに送り、それにより、UEおよびMMEがNASセキュリティアルゴリズムを共用できるようになることが上記の説明から理解される。さらに、UEおよびMMEは、認証ベクトル関連鍵、もしくは認証ベクトル関連鍵により導出されるルート鍵によってNAS保護鍵を導出し、それにより、MMEおよびUEがNAS保護鍵を共用することが可能になる。このような方法で、2G/3GネットワークからLTEネットワークに移動するとき、UEは、NASセキュリティアルゴリズムおよびNAS保護鍵について、MMEと折衝することができ、したがって、異種ネットワーク間のTAU手順におけるセキュリティ機能折衝プロセスが達成され、それにより、UEとネットワーク間のその後の対話の安全性が保証される。

【００９８】

本発明によれば、劣化攻撃をさらに阻止することができる。MMEはまた、TAU受入れメッセージを介して、UEによりサポートされるセキュリティ機能情報を返し、UEは、UEによりサポートされるセキュリティ機能情報が、UEによりサポートされる現在のセキュリティ機能情報と矛盾していないかどうかを検出する。矛盾していない場合、現在のセキュリティ機能折衝が成功し、折衝を通して得られたNASセキュリティアルゴリズムおよびNAS保護鍵を使用することができる。矛盾する場合、劣化攻撃が行われ、現在のセキュリティ機能折衝が失敗し、セキュリティ機能折衝を再度行う必要があると判定される。上記の解決策によれば、UEによりサポートされるセキュリティ機能情報が、UEによりサポートされるセキュリティ機能情報をMMEが取得する前に攻撃されたかどうかを検出することができ、それにより、劣化攻撃を阻止し、かつUEとネットワーク間のその後の対話の安全性を保証することができる。

【００９９】

上記の説明は、単に、本発明の好ましい実施形態に過ぎず、本発明の保護範囲を限定することを意図するものではない。本発明の趣旨および原理を逸脱することなく行われる変更、均等な置換え、および改良はいずれも本発明の保護範囲に含まれる。

【図１】

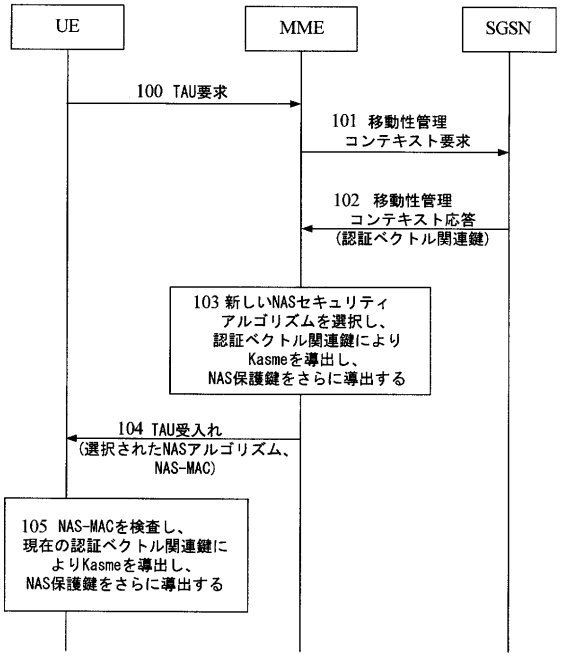

FIG. 1

【図２】

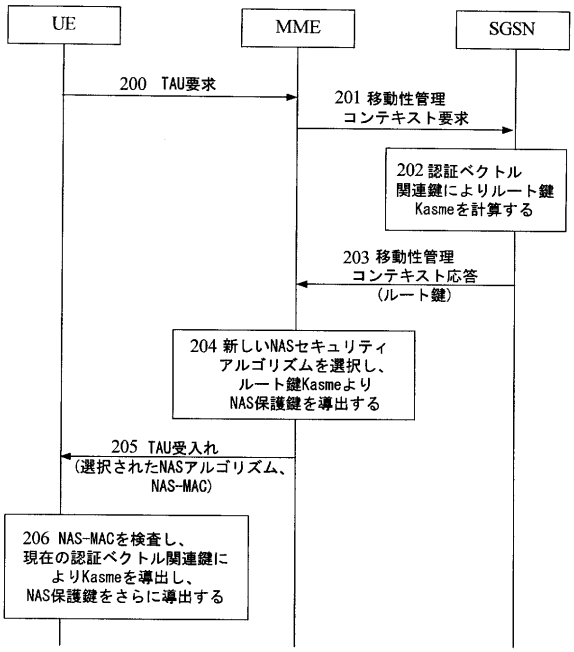

FIG. 2

【図３】

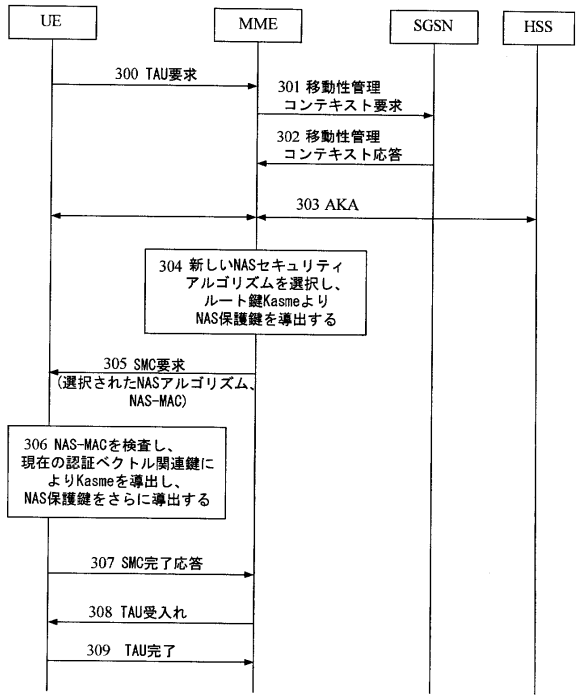

FIG. 3

【図４】

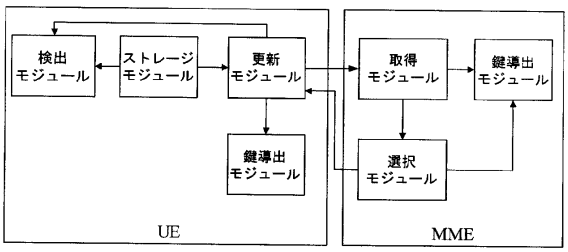

FIG. 4

フロントページの続き

(56)参考文献 特表２０１０－５２８５５９（ＪＰ，Ａ）
特表２０１０－５２１９０５（ＪＰ，Ａ）
特表２００９－５４０７２１（ＪＰ，Ａ）
特表２００９－５３１９５２（ＪＰ，Ａ）
欧州特許出願公開第２２１４４４４（ＥＰ，Ａ１）
3GPP TR 33.821 V0.2.0，２００７年 ４月

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/32
H04L 9/08
H04W 12/06