【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成24年4月19日(2012.4.19)

【公表番号】特表2010-533390(P2010-533390A)
【公表日】平成22年10月21日(2010.10.21)
【年通号数】公開・登録公報2010-042
【出願番号】特願2010-513633(P2010-513633)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｈ０４Ｗ　12/06　(2009.01)
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ａ
Ｈ０４Ｑ　7/00　１８３
Ｈ０４Ｌ　9/00　６０１Ｃ

【手続補正書】
【提出日】平成24年3月1日(2012.3.1)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【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。