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

特許第4944904号
(P4944904)

(45)発行日　平成24年6月6日(2012.6.6)　(24)登録日　平成24年3月9日(2012.3.9)

(51)Int.Cl.		F I		
H04L 9/14	(2006.01)	H04L	9/00	641
H04L 9/32	(2006.01)	H04L	9/00	675A
H04W 12/10	(2009.01)	H04Q	7/00	185
H04W 8/04	(2009.01)	H04Q	7/00	142
H04W 12/02	(2009.01)	H04Q	7/00	181

請求項の数 16　(全 13 頁)　最終頁に続く

(21)出願番号　特願2008-553725 (P2008-553725)
(86)(22)出願日　平成19年1月31日(2007.1.31)
(65)公表番号　特表2009-526455 (P2009-526455A)
(43)公表日　平成21年7月16日(2009.7.16)
(86)国際出願番号　PCT/EP2007/050936
(87)国際公開番号　WO2007/090774
(87)国際公開日　平成19年8月16日(2007.8.16)
審査請求日　平成20年8月6日(2008.8.6)
(31)優先権主張番号　102006006072.5
(32)優先日　平成18年2月9日(2006.2.9)
(33)優先権主張国　ドイツ(DE)

前置審査

(73)特許権者　390039413
シーメンス　アクチエンゲゼルシヤフト
Ｓｉｅｍｅｎｓ　Ａｋｔｉｅｎｇｅｓｅｌｌｓｃｈａｆｔ
ドイツ連邦共和国　Ｄ－８０３３３　ミュンヘン　ヴィッテルスバッハープラッツ　２
Ｗｉｔｔｅｌｓｂａｃｈｅｒｐｌａｔｚ　２，　Ｄ－８０３３３　Ｍｕｅｎｃｈｅｎ，　Ｇｅｒｍａｎｙ
(74)代理人　100099483
弁理士　久野　琢也
(74)代理人　100112793
弁理士　高橋　佳大

最終頁に続く

(54)【発明の名称】モバイルインタネットプロトコルに準拠して交換されるメッセージの真正性を保証する方法

(57)【特許請求の範囲】
【請求項１】
モバイルノードとホームエージェントとのあいだでモバイルインタネットプロトコルに準拠して交換されるメッセージの真正性を保証するために、使用される暗号化法をモバイルノードとホームエージェントとのあいだで一致させる、
メッセージの真正性を保証する方法において、
モバイルノードは、自身の支援している複数の暗号化法を含む登録要求を形成し、第１の暗号化法によって該登録要求の真正性を保証し、さらに、真正性を保証した登録要求をホームエージェントへ送信し、
ホームエージェントは、送信されてきた登録要求の真正性を検査し、該登録要求の真正性を確認した場合に、当該のモバイルノードとのあいだで共通に支援されている第２の暗号化法を選択し、共通の第２の暗号化法を選択したことを報告する登録返信を当該のモバイルノードへ送信する
ことを特徴とするメッセージの真正性を保証する方法。
【請求項２】
前記ホームエージェントは、前記登録要求が真正でないことを検出した場合に、前記登録要求を拒絶する登録返信をモバイルノードへ送信する、請求項１記載の方法。
【請求項３】
前記登録返信は当該のホームエージェントの支援する暗号化法に関する情報を含む、請求項１または２記載の方法。

【請求項４】
前記ホームエージェントは、前記登録返信の真正性を自身の選択した暗号化法によって保証する、請求項１から３までのいずれか１項記載の方法。
【請求項５】
前記モバイルノードは前記登録返信の真正性を検査する、請求項４記載の方法。
【請求項６】
前記ホームエージェントは、前記モバイルノードを登録して登録返信により当該のモバイルノードの登録が有効になされたことを表示し、選択した暗号化法によって当該のモバイルノードとのあいだに少なくとも１つのメッセージセキュリティアソシエーションを形成する、請求項１から５までのいずれか１項記載の方法。
【請求項７】
前記ホームエージェントは、共通の暗号化法を選択できなかった場合、第２の暗号化法として前記第１の暗号化法を選択する、請求項１から６までのいずれか１項記載の方法。
【請求項８】
前記モバイルノードは、前記登録返信に含まれている情報に基づいて共通の暗号化法を選択し、選択した暗号化法によって当該のホームエージェントとのあいだに少なくとも１つのメッセージセキュリティアソシエーションを形成する、請求項７記載の方法。
【請求項９】
共通の第２の暗号化法を用いて、前記モバイルノードと前記ホームエージェントとのあいだでの別のメッセージ交換の真正性を保証する、請求項１から８までのいずれか１項記載の方法。
【請求項１０】
前記第１の暗号化法および前記第２の暗号化法は複数のメッセージオーセンティケーションコードおよび複数のリプレイプロテクションスタイルを含む、請求項１から９までのいずれか１項記載の方法。
【請求項１１】
前記登録要求および／または前記登録返信を平文で伝送する、請求項１から１０までのいずれか１項記載の方法。
【請求項１２】
前記登録要求および／または前記登録返信は前記第１の暗号化法および／または前記共通の第２の暗号化法に関する示唆を含む、請求項１１記載の方法。
【請求項１３】
前記第１の暗号化法は前記モバイルノードと前記ホームエージェントとのあいだの先行のデータ交換から既知となる、請求項１から１２までのいずれか１項記載の方法。
【請求項１４】
前記モバイルノードおよび前記ホームエージェントは共通の秘密鍵を有する、請求項１から１３までのいずれか１項記載の方法。
【請求項１５】
前記モバイルノードに代わって外部エージェントと前記ホームエージェントとがメッセージを交換する、請求項１から１４までのいずれか１項記載の方法。
【請求項１６】
前記ホームエージェントに代わって外部エージェントと前記モバイルノードとがメッセージを交換する、請求項１から１４までのいずれか１項記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、モバイルノードとホームエージェントとのあいだでモバイルインタネットプロトコルに準拠して交換されるメッセージの真正性を保証する方法に関する。
【０００２】
インタネットプロトコルIPｖ４は定置のコンピュータと交換ノードとのあいだの有線通

信のために開発された。ラップトップコンピュータやＰＤＡなどのモバイル機器が或るコンピュータネットワークから別のコンピュータネットワークへ移動したときに同時に固定のＩＰアドレスを取得できるようにするために、"インタネットエンジニアリングタスクフォース"ＩＥＴＦによってネットワークプロトコル"ＩＰｖ４のためのＩＰモビリティサポート"、略称"モバイルＩＰ"が構想されたのである。モバイルＩＰは"Request For Comments"ＲＦＣ３３４４に規定されており、モバイル加入者機によるインタネットコネクションの規格として利用されている。

【０００３】

モバイルＩＰでは、"モバイルノード"とは、或るネットワークから別のネットワークへアクセスを変更するコンピュータまたはルータを意味する。"ホームエージェント"とは、モバイルノードのホームネットワークへ接続されており、当該のモバイルノードの位置情報を管理しているルータのことである。また"外部エージェント"とは、モバイルノードに対して外部ネットワークへのルーティングサービスを行い、ホームエージェントからモバイルエージェントへのデータパケットの転送を担当しているルータのことである。

【０００４】

モバイルノードが外部ネットワークに接続されたことが明らかとなると、当該のモバイルノードは外部ネットワーク内の"気付アドレス"を要求する。気付アドレスは外部エージェントの公示（外部エージェント気付アドレス）から求められるかまたはＤＨＣＰ（共通気付アドレス）を介して求められる。当該のモバイルノードはホームエージェントでの新たな気付アドレスによって登録される。ホームエージェントに到来するデータパケットはＩＰｔｏＩＰカプセルによってモバイルホストへ転送される。ホームネットワークへ戻って来た後、当該のモバイルノードはホームエージェントへコンタクトを取ってそこで登録を行う。

【０００５】

外部エージェントを利用する場合は登録のために次の各ステップが必要である。すなわち、まず、モバイルノードはホームエージェントのアドレスを付した"登録要求"を外部エージェントへ送信する。外部エージェントは当該の登録要求をホームエージェントへ転送する。その後、ホームエージェントは"登録返信"を外部エージェントへ送信し、外部エージェントは登録を許可するかまたは拒絶する。続いて、外部エージェントは登録返信をモバイルノードへ引き渡す。外部エージェントが存在しない場合、登録には２つのステップが必要なだけである。すなわち、まずモバイルノードが登録要求をホームエージェントへ送信する。続いて、ホームエージェントが登録返信によってモバイルノードへ応答するのである。

【０００６】

モバイルノードは登録要求においてその時点での気付アドレス（すなわち外部ネットワークにおいて当該のモバイルノードのアドレスとして通用するアドレス）をホームエージェントに報告するので、当該の登録要求を不正操作に対して保護しなければならない。例えば攻撃者が登録要求内の気付アドレスを変更したとすると、ホームエージェントはモバイルノードにデータパケット全体を送信することができず、攻撃者の定めたアドレスへこれを送信することになる。登録メッセージの真正性は保証されなければならない。つまり、登録メッセージの内容の変更も送信者の偽装も許してはならない。

【０００７】

真正性を保護するために、モバイルＩＰではいわゆる"モビリティセキュリティアソシエーション"ＭＳＡが通信機対ごとに設けられる。ここでの通信機対はたいていの場合ホームエージェントおよびモバイルノードから成るが、外部エージェントとホームエージェントとのあいだまたは外部エージェントとモバイルノードとのあいだにもモビリティセキュリティアソシエーションは存在しうる。通信機対のあいだでは各方向に複数の異なるモビリティセキュリティアソシエーションが存在しうる。ただしこのとき実際には２つの方向に対して唯一のモビリティセキュリティアソシエーションが用いられる。モビリティセキュリティアソシエーションＭＳＡは通信機対のあいだのセキュリティ関係式の集合体で

あって、真正性を保護するために利用すべき暗号化法および鍵を表している。モビリティセキュリティアソシエーションの個々のセキュリティ関係式は"セキュリティパラメータインデクス"ＳＰＩにより特徴づけられている。

【０００８】

セキュリティ関係式の暗号化法はそれぞれ１つずつ真正性確認アルゴリズムおよび"リプレイプロテクションスタイル"を含んでいる。

【０００９】

標準の真正性確認アルゴリズムとしてＨＭＡＣ－ＭＤ５が挙げられる。これは、ＭＤ５アルゴリズムをベースとして、"メッセージオーセンティケーションコード"ＭＡＣすなわちハッシュ値を保護すべきメッセージに関する秘密鍵によって計算するアルゴリズムである。メッセージが変更されていたり他の鍵が用いられていたりする場合、メッセージオーセンティケーションコードＭＡＣを新たに計算すると不正操作ないし送信者偽装が証明される。ＨＭＡＣ－ＭＤ５以外の別の真正性確認アルゴリズムを用いることもできる。

【００１０】

リプレイプロテクションは旧い登録要求の再使用防止に用いられる。タイムスタンプの付されたリプレイプロテクションでは送信側通信機によって時刻がメッセージに添付され、受信側通信機は当該のメッセージが所定の時刻よりも旧いものでないかどうかを検査できる。"Ｎｏｎｃｅ"（ナンバーユーズドオンリーワンス）の付されたリプレイプロテクションでは、送信側通信機から受信側通信機へ送られる全てのメッセージに送信のたびに新たな乱数が添付される。このとき送信側通信機は受信側通信機が同じ数を次の連絡で返送してくるかどうかを検査する。もちろん他のリプレイプロテクションスタイルを用いることもできる。タイムスタンプ、"Ｎｏｎｃｅ"その他のリプレイプロテクションスタイルによって形成された値は、送信側通信機によって登録メッセージのＩＤフィールドにエントリされ、受信側通信機によって検査される。

【００１１】

メッセージを認証するためにモバイルＩＰｖ４が設けられており、送信側通信機はメッセージの保護すべき部分に関するセキュリティパラメータインデクスＳＰＩおよびメッセージオーセンティケーションコードＭＡＣを含む"オーセンティケーションエクステンション"をメッセージに添付する。モバイルノードとホームエージェントとのあいだのオーセンティケーションエクステンションは"モバイルホームオーセンティケーションエクステンション"ＭＨＡＥと称される。受信側通信機は、セキュリティパラメータインデクスＳＰＩによって識別されるモビリティセキュリティアソシエーションＭＳＡにアクセスしてそこから利用すべき真正性確認アルゴリズムおよびリプレイプロテクションスタイルを求めることにより、真正性を検査する。その後、受信側通信機はメッセージオーセンティケーションコードＭＡＣを計算し、得られた結果と受信メッセージに含まれているメッセージオーセンティケーションコードＭＡＣとが一致するかどうかを確認する。旧いメッセージの再使用を防止するため、登録メッセージのＩＤフィールドに含まれるリプレイプロテクションスタイルの値も検査される。

【００１２】

モバイルＩＰでは種々の真正性確認アルゴリズムおよびリプレイプロテクションスタイルを使用することができるので、通信機対は利用すべき真正性確認アルゴリズムおよびリプレイプロテクションスタイルを指定しなければならない。

【００１３】

このための手段として、利用すべき真正性確認アルゴリズムおよびリプレイプロテクションスタイルを予め定めておき、モバイルノードおよびホームエージェントをこれにしたがって構成することが考えられる。ただしこの手段には次のような欠点がある。すなわち、そもそも、多数のモバイルノードおよび複数のホームエージェントを有する大きなネットワークでは全ての通信機対を手動で構成しなおすことはきわめて煩雑である。このことは最初のコンフィグレーションのケースにも当てはまるし、いちど構成された暗号化法の脆弱性が明らかとなって全ての通信機対においてこれを置換しなければならないケースに

も当てはまる。しかも、モバイルノードないしホームエージェントで支援されている暗号化法が未知である場合、例えば３ＧＰＰ（Third Generation Partnership Project）のワイヤレスローカルエリアネットワークＷＬＡＮにおけるローミングの際には、短時間で通信機対の双方に支援されている暗号化法を求めることはできない。したがって、適切な共通の真正性確認アルゴリズムおよびリプレイプロテクションスタイルを定めることもこれにしたがって２つの通信機を構成することも不可能である。

【００１４】

こうした欠点を改善するには、通信機対によって当該のネットワークで利用すべき暗号化法を選択することが挙げられる。ＲＦＣ３９５７"Authentication, Authorization and Accounting (AAA) Registration Keys for Mobile IPv4"によれば、モバイルノード、ホームエージェントないし外部エージェント間でのモビリティセキュリティアソシエーションＭＳＡはモバイルノードおよびホームＡＡＡサーバ間での"ＡＡＡセキュリティアソシエーション"から導出される。真正性確認アルゴリズムおよびリプレイプロテクションスタイルは登録メッセージの"キージェネレーションエクステンション"においてホームＡＡＡサーバからモバイルノードおよびホームエージェントへ伝送される。同様のプロセスがＤｉａｍｅｔｅｒＡＡＡサーバによるＲＦＣ４００４の"Diameter Mobile IPv4 Application"にも記載されている。これらのプロセスによれば、ネットワークから暗号化法を求めることができる。ただし、ここには、各モバイルノードがどのような真正性確認アルゴリズムおよびリプレイプロテクションスタイルを支援しているかがネットワークにとって一般に未知であるという欠点が存在する。したがって、例えば、ネットワークの定めた最新の暗号化法を支援していない旧いモバイルノードは、確実に受け入れられる暗号化法を支援していたとしても、それが旧いものであるかぎり、当該のネットワークと通信できない。

【００１５】

また別の改善手段として、暗号化法を一方側で求めるのではなく、通信機対のあいだで協議して取り決めることが考えられる。ＲＦＣ３３２９の"Security Mechanism Agreement for the Session Initiation Protocol (SIP)"からは、支援している暗号化法のリストをサーバへ送信するプロセスが記載されている。これに応じて、サーバは、自身の支援している暗号化法のリストを含む呼びかけ（Challenge）をクライアントへ送信する。クライアントは最も高い優先順位を付して共通の暗号化法を選択する。攻撃者がリストを改ざんしたり偽装したりするのを回避するために、サーバは弱い暗号化法のみを支援し、通信機対は相応の弱い暗号化法の指定に続いて、リストをもう一度保護して伝送する。相手方通信機は選択された暗号化法を作動し、サーバによって支援されている暗号化法を含むリストをサーバへ送信する。サーバはリストの真正性を検査し、これによりオリジナルリストが改ざんされていないことが保証される。さらに別の協議メカニズムとして"インタネットキーエクスチェンジ"ＩＫＥ（ＩＰｓｅｃ－ＩＫＥ）も公知である。ただし、この方法では最初のメッセージが保護されずに伝送されるため、モバイルＩＰではそのまま利用することができず、最初のメッセージに対して別の真正性保護手段が必要となるという欠点がある。また、支援される暗号化法を含むリストを２回伝送しなければならないという欠点も存在する。

【００１６】

したがって、本発明の課題は、モバイルノード、ホームエージェントないし外部エージェント間で相互に支援される暗号化法を知らせあい、共通の暗号化法を選択し、モバイルインタネットプロトコルに準拠して交換されるメッセージの真正性を保証する方法を提供することである。

【００１７】

この課題は、モバイルノードとホームエージェントとのあいだでモバイルインタネットプロトコルに準拠して交換されるメッセージの真正性を保証するために、使用される暗号化法をモバイルノードとホームエージェントとのあいだで一致させる、本発明の方法により解決される。

【００１８】
暗号化法が予め設定および構成されないことにより、モバイルノードおよびホームエージェントで支援されている種々の暗号化法によりダイナミックかつ効率的に大きなネットワークを構成することができる。また、メッセージセキュリティアソシエーションにとって最適な暗号化法が選択される。つまり、一方で双方の通信機に共通の強い暗号化法を用いることができ、他方で強い暗号化法が双方の通信機で共通に支援されていない場合には弱い暗号化法も利用可能となる。さらに、本発明の方法によれば、信用を失った暗号化法を大きなコストをかけずに置換することができる。
【００１９】
本発明の実施形態によれば、モバイルインタネットプロトコルはモバイルＩＰｖ４プロトコルである。
【００２０】
本発明の実施形態によれば、モバイルノードは自身の支援する暗号化法に関する情報を含む登録要求を形成する。ついで、モバイルノードは当該の登録要求の真正性を第１の暗号化法により保証する。続いて、モバイルノードは真正性の保証された登録要求をホームエージェントへ送信し、ホームエージェントは当該の登録要求の真正性を検査する。
【００２１】
ＲＦＣ３３４４に準拠したモバイルＩＰとは異なり、モバイルノードの形成した登録要求は当該のモバイルノードの支援する複数の暗号化法に関する情報を含んでおり、これによりホームエージェントに当該の情報が既知となる。さらに、第１の登録要求の真正性がモバイルＩＰと同様に保証されるので、モバイルノードの支援する複数の暗号化法に関する情報が改ざんされていたり当該の登録要求が他のソースから到来していたりしないかどうかを識別することができる。
【００２２】
本発明の実施形態によれば、ホームエージェントは登録要求が真正でないことを検出した場合に登録要求を拒絶する登録返信をモバイルノードへ送信する。
【００２３】
登録要求の内容が変更されていたり送信側通信機が不正に操作されていたり、または再使用が行われていたりした場合には、ホームエージェントは当該のモバイルノードの登録を許可しない。
【００２４】
本発明の実施形態によれば、ホームエージェントは登録要求の真正性を確認した場合に共通の第２の暗号化法を選択しこれを報告する登録返信をモバイルノードへ送信する。
【００２５】
ホームエージェントは、唯一の暗号化法を定めるのではなく、共通の暗号化法が複数利用されている場合には、有利な暗号化法を選択することができる。
【００２６】
本発明の実施形態によれば、登録返信はホームエージェントの支援する暗号化法に関する情報を含む。
【００２７】
ホームエージェントの支援する暗号化法に関する情報により、モバイルノードでは、あらためて登録要求するとき、当該の暗号化法のうちの１つを登録要求の真正性を保証する共通の第１の暗号化法として用いることができる。
【００２８】
本発明の実施形態によれば、ホームエージェントは登録返信の真正性を自身の選択した暗号化法によって保証する。
【００２９】
このようにして登録返信の内容および送信者は不正操作に対して保護される。これにより、例えば弱い暗号化法しか支援されないために攻撃者によって暗号化法に関する情報が恣意的に変更されるというおそれがなくなる。

【００３０】
本発明の実施形態によれば、モバイルノードは登録返信の真正性を検査する。
【００３１】
登録返信の真正性が検査されることにより、モバイルノードは登録返信に挙げられている暗号化法が第三者によって不正操作されていたり選択されていたりせず、ホームエージェントから不変のまま到来したものであることを確認することができる。
【００３２】
本発明の実施形態によれば、ホームエージェントは、登録要求の真正性を確認できた場合、当該のモバイルノードを登録して登録返信により当該のモバイルノードの登録が有効になされたことを表示し、選択した暗号化法によって当該のモバイルノードとのあいだに少なくとも１つのメッセージセキュリティアソシエーションを形成する。
【００３３】
本発明の方法によれば、２つのメッセージのやり取りのみで支援されている暗号化法に関する情報交換の真正性を保証し、最適な暗号化法を選択して相応のメッセージセキュリティアソシエーションを形成することができる。
【００３４】
本発明の実施形態によれば、ホームエージェントは、共通の暗号化法を選択できなかった場合、第２の暗号化法として第１の暗号化法を選択する。
【００３５】
本発明の実施形態によれば、モバイルノードは、登録返信に含まれている情報に基づいて共通の暗号化法を選択し、選択した暗号化法によってホームエージェントとのあいだに少なくとも１つのメッセージセキュリティアソシエーションを形成する。
【００３６】
本発明の実施形態によれば、モバイルノードとホームエージェントとのあいだでの別のメッセージ交換の真正性を保証するために、共通の第２の暗号化法が用いられる。
【００３７】
共通の第２の暗号化法は有利な暗号化法である。一方ではセキュリティに関して強い暗号化法を選択することができるし、他方では暗号化法としては弱いけれどもモバイルノードとホームエージェントとのあいだの確実な通信を可能にする暗号化法を選択することもできる。
【００３８】
本発明の実施形態によれば、第１の暗号化法および第２の暗号化法は複数のメッセージオーセンティケーションコードＭＡＣおよび複数のリプレイプロテクションスタイルを含む。
【００３９】
メッセージオーセンティケーションコードにより、登録要求ないし登録返信およびこれらに含まれる暗号化法に関する情報が不正操作されていないこと、ならびに、ＩＤすなわち送信元アドレスおよび宛先アドレスが変更されていないことが保証される。また、タイムスタンプまたはＮｏｎｃｅなどのリプレイプロテクションスタイルにより、登録返信が先行の登録要求に対応していること、ならびに、旧い登録メッセージの再使用が回避されていることが保証される。
【００４０】
本発明の実施形態によれば、登録要求および／また登録返信は平文で伝送される。
【００４１】
このようにすれば、ホームエージェントはモバイルノードで支援されている暗号化法を登録要求から読み出し、モバイルノードはホームエージェントで支援されている暗号化法を登録返信から読み出すことができる。
【００４２】
本発明の実施形態によれば、登録要求および／また登録返信は第１の暗号化法に関する示唆を含む。

【００４３】
登録要求ないし登録返信が平文で伝送されるので、真正性確認に用いられた第１の暗号化法についての示唆を添付することにより、モバイルノードないしホームエージェントに対して、メッセージの真正性を保証した真正性確認アルゴリズム、リプレイプロテクションスタイルおよび鍵を報告し、これらを検査することができる。
【００４４】
本発明の実施形態によれば、第１の暗号化法はモバイルノードとホームエージェントとのあいだの先行のデータ交換から既知となる。
【００４５】
第１の暗号化法は、登録要求および登録返信などの先行の合意または協議から既知となるか、或いは、同じネットワーク内の他のホームエージェントまたは同様の有利なアルゴリズムないしリプレイプロテクションスタイルを有するホームエージェントから取得される。このようにすれば、最初の登録要求が未知の真正性確認アルゴリズムまたは未知のリプレイプロテクションスタイルを含んでいるために拒絶されるというケースがほぼ排除される。
【００４６】
本発明の実施形態によれば、モバイルノードおよびホームエージェントは共通の秘密鍵を利用する。
【００４７】
真正性確認アルゴリズムに基づいてメッセージオーセンティケーションコードの計算の際に考慮される秘密鍵により、こうしたコードが対応するモバイルノードまたはホームエージェントのみで計算されることが保証される。
【００４８】
本発明の実施形態によれば、ホームエージェントに代わって外部エージェントとモバイルノードとがメッセージを交換する。
【００４９】
本発明の実施形態によれば、モバイルノードに代わって外部エージェントとホームエージェントとがメッセージを交換する。
【００５０】
このようにすれば、本発明により、モバイルノードと外部エージェントとのあいだないしホームエージェントと外部エージェントとのあいだでメッセージの真正性が保証される。
【００５１】
以下に本発明を図示の実施例に則して詳細に説明する。
【００５２】
図１にはモバイルノードとホームエージェントとのあいだで暗号化法を一致させる本発明の方法の実施例のフローチャートが示されている。図２には本発明の登録要求のフィールドの実施例が示されている。
【００５３】
図１には、モバイルノードとホームエージェントとのあいだでモバイルＩＰｖ４に準拠して交換されるメッセージの真正性を保証するために暗号化法を一致させる実施例のフローチャートが示されている。真正性を保証する暗号化法は真正性確認アルゴリズムおよびリプレイプロテクションスタイルから成る。真正性確認アルゴリズムは例えばＨＭＡＣ－ＭＤ５であり、ここでは１２８ｂｉｔ長の対称鍵によってメッセージオーセンティケーションコードが計算される。鍵は例えばＲＦＣ３９５７によって交換される。また３ＧＰＰネットワークでは鍵はＧＢＡ（Generic bootstraping architecture）に基づくプロセスによって交換される。リプレイプロテクションスタイルとしては、モバイルＩＰに規定されているタイムスタンプまたはＮｏｎｃｅが用いられる。もちろんメッセージの真正性を支援する他の方法を用いることもできる。
【００５４】

本発明の方法は、モバイルノード、ホームエージェントないし外部エージェント間でメッセージを交換する際にメッセージの真正性を保証するために用いられる。この場合、ＦＨＡＥ（Foreign Home Authentication Extention）およびモバイルＩＰにおいて規定されＦＨＡＥに添付されたＭＦＡＥ（Mobili Foreign Authentication Extention）が必要となる。本発明の方法はメッセージの真正性を保証する暗号化法を協議するためのモバイルＩＰとして用いることもできる。フローチャートの個々のステップは入れ替え、補充および省略が可能である。

【００５５】

ステップ１でモバイルノードおよびホームエージェントはメッセージセキュリティアソシエーションの形成を開始する。本発明では、必要な情報の全て、例えば秘密鍵などが既に存在しており、メッセージセキュリティアソシエーションの完成には共通の暗号化法すなわち真正性確認アルゴリズムおよびリプレイプロテクションスタイルのみが必要であるということを前提としている。

【００５６】

ステップ２では、モバイルノードは自身の支援する暗号化法に関する情報を含む登録要求を形成する。そしてモバイルノードは当該の登録要求の真正性を第１の暗号化法により保証する。当該の暗号化法は当該のモバイルノードによって相手方のホームエージェントが支援している確率が高いとして選択されたものである。この選択は例えば相手方のホームエージェントまたは同じネットワーク内の同様の暗号化法を有する他のホームエージェントとの先行の交渉から得られた情報に基づいて行われる。真正性の保証された登録要求は当該のモバイルノードから平文でホームエージェントへ送信されるので、ホームエージェントは当該の登録要求から真正性の保証に用いられた第１の暗号化法に関する示唆を取り出すことができる。

【００５７】

ステップ５の問い合わせにおいて、ホームエージェントは自身が第１の暗号化法を支援しているか否かを検査する。支援していない場合には、当該のホームエージェントは登録要求の真正性を検査しない。この場合、攻撃者がモバイルノードの支援している暗号化法に関する情報を不正に操作しうる状況および／またはホームエージェントが送信者をチェックできない状況など、セキュリティにとってクリティカルな事態が生じたことになるからである。

【００５８】

ステップ６では、ホームエージェントは登録要求を拒絶する旨の登録返信を形成する。この場合、拒絶はモバイルＩＰに準拠したエラーメッセージであってもよいし、新たに定義したエラーメッセージであってもよい。当該の登録返信はモバイルノードおよびホームエージェントが共通に支援している暗号化法によって真正性を保証され、ホームエージェントからモバイルノードへ送信される。ホームエージェントは当該の登録返信に自身の支援している暗号化法に関する情報を含めて送信し、モバイルノードはステップ２であらためて登録要求を行う際に、リストから新たな第１の暗号化法を選択し、これによって新たな登録要求を保護する。

【００５９】

ステップ１０の問い合わせにおいて、ホームエージェントは当該の登録要求が真正であるか否かを検査する。この検査は、モバイルノードによって選択された第１の暗号化法がホームエージェントの支援しているものであることから可能となっている。

【００６０】

登録要求が真正でない場合、これは当該の登録要求が例えば攻撃者によって不正に操作されているということを意味する。このとき、ホームエージェントは、ステップ１１において、登録要求を拒絶する旨の登録返信を形成する。当該の登録返信は、こうしたケースのために設けられたモバイルＩＰのエラーメッセージまたは新たに定義されたエラーメッセージを含むほか、さらに、当該のホームエージェントの支援している暗号化法に関する情報を含む。ホームエージェントは、第１の暗号化法で登録返信の真正性を保証した後、

当該の登録返信を、ステップ２であらためて登録しようと試みているモバイルノードへ送信する。

【００６１】

ホームエージェントによって登録要求が真正であると確認された場合には、ホームエージェントはステップ２０において当該のモバイルノードを当該のネットワークに登録する。

【００６２】

ステップ２５の問い合わせにおいて、ホームエージェントはモバイルノードによって支援されている暗号化法に関する情報と自身の支援している暗号化法とを比較し、第１の暗号化法のほかに他の共通の暗号化法が存在するかどうかを求める。こうして、例えば第１の暗号化法として幾分弱くても広汎に用いられている暗号化法を登録要求の保護に選択し、その後で、モバイルノードおよびホームエージェントの双方に共通の強い別の暗号化法を選択することができる。

【００６３】

共通の別の暗号化法を求めることができない場合、ステップ２６において、ホームエージェントは第１の暗号化法を第２の暗号化法として選択する。

【００６４】

共通の別の暗号化法を求めることができた場合、ステップ３０において、ホームエージェントは自身にとって有利な共通の暗号化法を第２の暗号化法として選択する。

【００６５】

ステップ３１において、ホームエージェントはメッセージセキュリティアソシエーションを自身の側で選択した暗号化法によって完成させる。続いてホームエージェントは、自身の選択した暗号化法に関する情報（示唆）を含む登録返信を形成し、この東麓返信を選択した第２の共通の暗号化法によって保護し、当該の登録返信をモバイルノードへ送信する。他のエラーが発生しなければ、当該の登録返信は登録が有効に行われたことを表す。

【００６６】

ステップ３２では、モバイルノードが、登録要求からホームエージェントの選択した第２の共通の暗号化法を取り出し、これによって登録返信の真正性を検査する。

【００６７】

ステップ４０の問い合わせにおいて、モバイルノードは当該の登録返信が有効な登録を表示しているかどうかを検査する。

【００６８】

登録が有効に行われなかった場合、モバイルノードはあらためて登録を試みる。ステップ４１では、モバイルノードは例えば登録返信のエラーコードからエラーの原因を導き出し、これを補正する。例えば暗号化法が指定されていてエラーが発生している場合には、モバイルノードは次の登録要求において暗号化法の他のリストを提示することができる。また、拒絶は、モバイルノードの制御不能な他のエラー、例えば長すぎる登録要求による時間切れや多数の登録要求による混雑を原因としても行われうる。これらの場合には補正は必要ない。あらためての登録の試行が再びステップ２で開始される。

【００６９】

ステップ５０の問い合わせは、登録返信によって登録が有効に行われたことが表示された場合に行われる。ステップ５０の問い合わせでは、ホームエージェントがモバイルノードに対して共通の第２の暗号化法の利用を設定したか否かが判別される。

【００７０】

ホームエージェントがモバイルノードに対して自身の選択した第２の共通の暗号化法の利用を設定しなかった場合、モバイルノードはステップ５１において第２の暗号化法をみずから求める。この場合モバイルノードは自身の選択した暗号化法によってメッセージセキュリティアソシエーションを完成させる。このようにすれば、ホームエージェントおよびモバイルノードがメッセージの認証に異なる暗号化法を利用しても、双方の側で互いに選択した暗号化法を利用することができる。

【００７１】
ホームエージェントがモバイルノードに対して自身の選択した第２の共通の暗号化法の利用を設定した場合、モバイルノードはステップ６０においてホームエージェントの選択した暗号化法によってメッセージセキュリティアソシエーションを完成させる。この場合、実際にはホームエージェントおよびモバイルノードの双方がメッセージセキュリティアソシエーションに対して同じ暗号化法を利用することになる。
【００７２】
モバイルノードとホームエージェントとのあいだにメッセージセキュリティアソシエーションが形成された後、付加的にステップ６１において、形成されたメッセージセキュリティアソシエーションによってただちに保護された新たな登録を行い、当該のメッセージセキュリティアソシエーションが双方の側で有効に形成されているか否かを検査してもよい。
【００７３】
ＲＦＣ３３２９に規定されたセッション開始プロトコルＳＩＰのセキュリティメカニズムアグリーメントプロシージャなどの公知の方法とは異なり、本発明の方法では、モバイルノードの支援している暗号化法に関する情報もホームエージェントの支援している暗号化法に関する情報も送信する必要はない。なぜなら登録要求および登録返信の真正性が既に保証されており、不正操作のおそれが排除されているからである。共通に支援されている暗号化法は全部で２つのメッセージ、すなわちモバイルノードからホームエージェントへのメッセージおよびホームエージェントからモバイルノードへのメッセージのみで一致させることができる。
【００７４】
図２には、本発明の方法で用いられる登録要求のフィールドの実施例が示されている。当該の登録要求はＩＰヘッダＩＰ，ＵＤＰヘッダＵＤＰおよびモバイルＩＰフィールドを有する。ＩＰヘッダにはＩＰ送信元アドレス、ＩＰ宛先アドレスおよびＩＰライフタイムが含まれている。ＵＤＰヘッダ（ユーザデータグラムプロトコルヘッダ）には送信元ポートおよび宛先ポートが含まれている。モバイルＩＰフィールドは固定長のフィールドＡＬ，ＩＤおよび所定の延長部（エクステンション）から成る。
【００７５】
フィールドＡＬは、タイプ、ライフタイム、モバイルノードのＩＰアドレス、ホームエージェントのＩＰアドレスおよび気付アドレスなどの登録要求の一般的な情報を含む。ＩＤフィールドには、登録返信を登録要求に対応させる識別子が含まれており、この識別子にはリプレイプロテクションＲＰに対する情報が含まれる。
【００７６】
延長部は、モバイルノードの支援している暗号化法をエントリする新たなフィールドＫＶと、使用される暗号化法に関する示唆をエントリする新たなフィールドＨＷと、ＭＨＡＥ（Mobile Home Authentication Extension）とを含み、これにより最新の登録要求の真正性が保護される。
【００７７】
ＭＨＡＥ（Mobile Home Authentication Extension）はタイプＴＹＰ，延長部の長さＬＥＮ，セキュリティパラメータインデクスＳＰＩおよびメッセージオーセンティケーションコードＭＡＣを含む。メッセージオーセンティケーションコードＭＡＣは、暗号化ユニットＫＥにおいて選択された当該のモバイルノードおよびホームエージェントのみに既知の真正性確認アルゴリズムＡＡおよび対称鍵ＫＥＹにより、フィールドＡＬ，ＩＤ，ＫＶ，ＨＷ，ＴＹＰ，ＬＥＮ，ＳＰＩから計算される。これらのフィールドのうち１つでも変更されると、受信側通信機は他のメッセージオーセンティケーションコードを計算し、伝送されたメッセージオーセンティケーションコードＭＡＣと比較することにより不正操作の有無を識別する。登録要求は平文で送信され、ホームエージェントはモバイルノードの支援している暗号化法ＫＶおよび示唆ＨＷを読み出すことができる。
【００７８】

本発明の方法のための登録返信は図２に示した登録要求に類似しており、新たなフィールドＫＶ，ＨＷを含む。

【図面の簡単な説明】

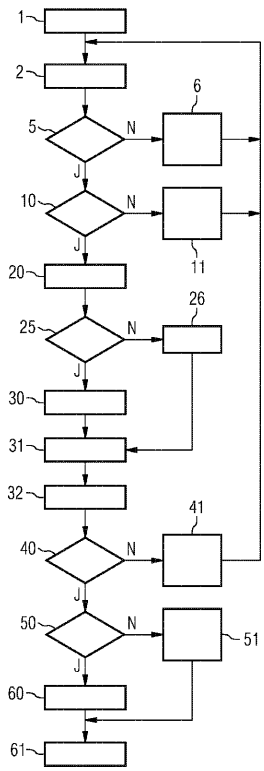
【００７９】

【図１】モバイルノードとホームエージェントとのあいだで暗号化法を一致させる本発明の方法の実施例のフローチャートである。

【図２】本発明の登録要求のフィールドの実施例を示す図である。

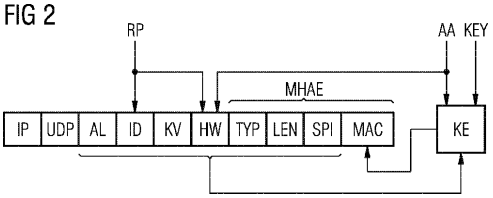
【図１】

FIG 1



【図２】

FIG 2



フロントページの続き

(51)Int.Cl. F I
G09C 1/00 (2006.01) G09C 1/00 640D

(74)代理人 100128679
弁理士 星 公弘
(74)代理人 100135633
弁理士 二宮 浩康
(74)代理人 100156812
弁理士 篠 良一
(74)代理人 100114890
弁理士 アインゼル・フェリックス＝ラインハルト
(72)発明者 ヴォルフガング ビュッカー
ドイツ連邦共和国 ノイビーベルク ヴァルキューレンシュトラーセ 24
(72)発明者 ヴォルフガング グレーティング
ドイツ連邦共和国 オーバーハウゼン エーゲルスフルトシュトラーセ 24
(72)発明者 ヨアヒム クロース
ドイツ連邦共和国 ミュンヘン ウェアデンフェルスシュトラーセ 11

審査官 青木 重徳

(56)参考文献 特表２００２－５２０７０８（ＪＰ，Ａ）
特開２００４－０４０５５５（ＪＰ，Ａ）
特表２０００－５１６７３４（ＪＰ，Ａ）
国際公開第２００５／０３６８１３（WO，Ａ１）
欧州特許出願公開第０１４１４２１２（ＥＰ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/14
G09C 1/00
H04L 9/32
H04W 8/04
H04W 12/02
H04W 12/10