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

特許第5054772号
(P5054772)

(45)発行日　平成24年10月24日(2012.10.24)　(24)登録日　平成24年8月3日(2012.8.3)

(51)Int.Cl.　F I
H04W 12/04 (2009.01)　H04Q 7/00 182

請求項の数 22 (全 18 頁)

(21)出願番号	特願2009-523298 (P2009-523298)
(86)(22)出願日	平成19年8月9日 (2007.8.9)
(65)公表番号	特表2010-500803 (P2010-500803A)
(43)公表日	平成22年1月7日 (2010.1.7)
(86)国際出願番号	PCT/EP2007/058284
(87)国際公開番号	WO2008/019989
(87)国際公開日	平成20年2月21日 (2008.2.21)
審査請求日	平成21年2月5日 (2009.2.5)
(31)優先権主張番号	102006038037.1
(32)優先日	平成18年8月14日 (2006.8.14)
(33)優先権主張国	ドイツ(DE)

(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　100061815
弁理士　矢野　敏雄
(74)代理人　100094798
弁理士　山崎　利臣

最終頁に続く

(54)【発明の名称】アクセス専用キーを提供する方法およびシステム

(57)【特許請求の範囲】

【請求項１】

移動端末機(1)とアクセスネットワーク(2)のノードとの間でのデータ伝送を保安するためのアクセス専用キーを提供するための方法であって、

前記移動端末機(1)のアクセス認証が成功した後、前記移動端末機(1)のホームネットワーク(4)に設けられている認証サーバ(4A)がセッションキーを生成し、

該セッションキーからベースキーが導出され、アクセスネットワーク(2)またはホームネットワーク(4)に設けられているインタワーキングプロキシサーバ(7)に伝送され、

該インタワーキングプロキシサーバは伝送されたベースキーからアクセス専用キーを導出し、前記アクセスネットワーク(2)のノードに提供する方法。

【請求項２】

請求項１記載の方法であって、

前記セッションキーはMSK(Master Session Key)キーまたはEMSK(Extended Master Session Key)キーにより形成される方法。

【請求項３】

請求項１記載の方法であって、

前記ベースキーは前記セッションキーから、所定の第1の誘導関数によって導出される方法。

【請求項４】

請求項３記載の方法であって、

前記第1の誘導関数は、HMAC-SHA1誘導関数、HMAC-SHA256誘導関数、HMAC-MD5誘導関数、 SHA1誘導関数、SHA-256誘導関数またはMD5誘導関数により形成される方法。

【請求項５】

請求項１記載の方法であって、

前記ベースキーの導出は、前記セッションキーと符合文字列(ストリング)に依存して行われる方法。

【請求項６】

請求項１記載の方法であって、

移動端末機の認証は、認証サーバにおいてEAPプロトコルを用いて行われる方法。

【請求項７】

請求項１記載の方法であって、

移動端末機の認証は、認証サーバにおいてUMTS-AKAプロトコルを用いて行われる方法。

【請求項８】

請求項１記載の方法であって、

移動端末機の認証は、認証サーバにおいてHTTPダイジェストAKAプロトコルを用いて行われる方法。

【請求項９】

請求項１記載の方法であって、

認証サーバとインタワーキングプロキシサーバとの間のデータ伝送は、Diameterプロトコルまたは Radiusプロトコルによって行われる方法。

【請求項１０】

請求項１記載の方法であって、

アクセスネットワークはWiMaxネットワークにより形成される方法。

【請求項１１】

請求項１記載の方法であって、

ホームネットワークは3GPPネットワークにより形成される方法。

【請求項１２】

請求項１記載の方法であって、

伝送されたベースキーからインタワーキングプロキシサーバによって、第2の誘導関数を用いてモバイルIPルートキーが導出される方法。

【請求項１３】

請求項１２記載の方法であって、

前記第2の誘導関数は、HMAC-SHA1誘導関数、HMAC-SHA256誘導関数、HMAC-MD5誘導関数、 SHA1誘導関数、SHA-256誘導関数またはMD5誘導関数により形成される方法。

【請求項１４】

請求項１３記載の方法であって、

前記導出されたモバイルIPルートキーから第3の誘導関数によって、移動端末機とアクセスネットワークのノードとの間のデータ伝送を保安するためのアクセス専用キーが導出される方法。

【請求項１５】

請求項１４記載の方法であって、

前記第3の誘導関数は、HMAC-SHA1誘導関数、HMAC-SHA256誘導関数、HMAC-MD5誘導関数、 SHA1誘導関数、SHA-256誘導関数またはMD5誘導関数により形成される方法。

【請求項１６】

請求項１記載の方法であって、

アクセスネットワーク(2)のノードと移動端末機(1)との間の種々異なるデータ伝送区間に対して、それぞれ1つの所属のアクセス専用キーが導出される方法。

【請求項１７】

請求項１記載の方法であって、

移動端末機(1)は前記アクセス認証の成功後、同様にセッションキーを生成し、該セッ

ションキーからアクセス専用キーを導出する方法。
【請求項１８】
ベースキーを提供するための認証サーバ(4A)であって、前記ベースキーから移動端末機(1)とアクセスネットワーク(2)のノードとの間でのデータ伝送を保安するためのアクセス専用キーが導出され、
前記認証サーバ(4A)は、前記移動端末機(1)のホームネットワークに設けられており、移動端末機(1)のアクセス認証が成功した後セッションキーを生成し、該セッションキーから誘導関数によってベースキーを導出し、アクセスネットワーク(2)またはホームネットワーク(4)に設けられているインタワーキングプロキシサーバ(7)に提供する認証サーバ。
【請求項１９】
請求項１８記載の認証サーバであって、
前記誘導関数は、HMAC-SHA1誘導関数、HMAC-SHA256誘導関数、HMAC-MD5誘導関数、 SHA1誘導関数、SHA-256誘導関数またはMD5誘導関数により形成される認証サーバ。
【請求項２０】
移動端末機(1)とアクセスネットワーク(2)のノードとの間でのデータ伝送を保安するためのアクセス専用キーを提供するためのインタワーキングプロキシサーバ(7)であって、
前記インタワーキングプロキシサーバ(7)はアクセスネットワーク(2)またはホームネットワーク(4)に設けられており、前記移動端末機(1)のホームネットワークに設けられている認証サーバ(4a)から伝送されたベースキーからアクセス専用キーを導出し、アクセスネットワーク(2)のノードに提供するインタワーキングプロキシサーバ。
【請求項２１】
複数のアクセスネットワーク(2)と、移動端末機(1)の少なくとも1つのホームネットワーク(4)とを備えるデータ伝送システムであって、
前記ホームネットワーク(4)の認証サーバ(4A)が、移動端末機(1)のアクセス認証が成功した後セッションキーを生成し、該セッションキーから共通のベースキーを導出し、
該ベースキーは前記アクセスネットワーク(2)に伝送され、
該アクセスネットワークはそれぞれ1つのインタワーキングプロキシサーバ(7)を有しており、
該インタワーキングプロキシサーバは少なくとも1つのアクセス専用キーを前記伝送されたベースキーから導出し、
該アクセス専用キーは、前記移動端末機とそれぞれのアクセスネットワーク(2)のノードとの間のデータ伝送区間を保安するために設けられているものであるデータ伝送システム。
【請求項２２】
請求項２１記載のデータ伝送システムであって、
前記アクセスネットワーク(2)の各ノードに対して所属のアクセス専用キーが、前記伝送されたベースキーからインタワーキングプロキシサーバ(7)によって導出されるデータ伝送システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、移動端末機とアクセスネットワークノードとの間でのデータ伝送を保安するためのアクセス専用キーを提供する方法およびシステムに関する。
【背景技術】
【０００２】
TCP/IPプロトコルを用いるインターネットは、モバイル分野のためにより高度なプロトコルを開発するためのプラットフォームを提供する。インターネットプロトコルは広く普及しているので、相応のプロトコル拡張によってモバイル環境のために、大きな適用範囲を開発することができる。しかしながら従来のインターネットプロトコルは本来的にモバ

イルでの使用のために構想されていない。従来のインターネットのパケット交換においては、固定のコンピュータ間でパケットが交換され、これらのパケットのネットワークアドレスは変化せず、またこれらのパケットが異なるサブネットワーク間で伝送されることもない。移動端末機ないしモバイルコンピュータを備えた無線ネットワークにおいては、モバイルコンピュータMS(移動局)が種々のネットワークに組み込まれることが多い。DHCP(動的ホスト構成プロトコル；Dynamic Host Configuration Protocol)は、相応のサーバを用いてネットワーク内のコンピュータへのIPアドレスおよび別のコンフィギュレーションパラメータの動的な割当てを実現する。ネットワークにリンクされるコンピュータにはDHCPプロトコルにより任意のIPアドレスが自動的に割り当てられる。モバイルコンピュータにDHCPがインストールされると、このコンピュータはDHCPプロトコルによるコンフィギュレーションをサポートするローカルネットワークのエリア内で動作しなければならない。DHCPプロトコルでは動的なアドレス設定が実現される。すなわち任意のIPアドレスが自動的に所定時間の間、割り当てられる。この時間の経過後には、モバイルコンピュータMSによるリクエストが新たに行われなければならないか、またはIPアドレスを別のやり方で割り当てることができる。

【０００３】

DHCPにより、マニュアルによるコンフィギュレーションを行うことなくモバイルコンピュータMSをネットワークに組み込むことができる。その前提として単にDHCPサーバが提供されれば良い。モバイルコンピュータMSはローカルネットワークのサービスを利用することができ、例えば中央に記憶されているデータファイルを利用することができる。しかしながら、モバイルコンピュータMS自体がサービスを提供する場合には、潜在的なサービスユーザがそのモバイルコンピュータMSを発見することはできない。なぜならば、そのモバイルコンピュータのIPアドレスはモバイルコンピュータが組み込まれるネットワーク毎に変わるからである。同様のことは、IPコネクションが確立されている間にIPアドレスが変わる場合にも発生する。これによりコネクションが中断される。したがってモバイルIPの場合には、モバイルコンピュータMSに他のネットワークにおいても維持されるIPアドレスが割り当てられる。従来のIPネットワーク変化の場合には、IPアドレス設定を相応に適合させることが必要であった。IPアドレスおよび従来の自動的なコンフィギュレーションメカニズムが恒常的に適合される場合、確立しているコネクションがIPアドレスの変更の際に遮断される。MIPプロトコル(RFC2002，RFC2977，RFC3344，RFC3846，RFC3957，RFC3775，RFC3776，RFC4285)は移動端末機MSのモビリティをサポートする。従来のIPプロトコルにおいては、移動端末機MSは、IPサブネットワークが変化する都度、自身のIPアドレスを適合させなければならなかった。これは移動端末機MSにアドレッシングされたデータパケットを正確にルーティングするためである。確立したTCPコネクションを維持するために、移動端末機MSは自身のIPアドレスを保持しなければならない。なぜならば、アドレス変更によりコネクションが遮断されるからである。MIPプロトコルにより2つのアドレス間で、すなわち恒久的なホームアドレスと一時的な気付アドレス(Care-Of-Address)との間でトランスパレントなコネクションが実現される。気付アドレスとは、その時点において移動端末機MSにアクセスすることができるIPアドレスである。

【０００４】

ホームエージェント(Home Agent)HAは、移動端末機MSが本来のホームネットワーク内に存在しない場合における、この移動端末機MSのエージェントである。ホームエージェントにはモバイルコンピュータMSの現在地に関する情報が恒常的に通知される。ホームエージェントHAは通常の場合、移動端末機のホームネットワーク内のルータの構成要素である。移動端末機MSがホームネットワーク外に存在する場合には、ホームエージェントHAは移動端末機MSがログインできる機能を提供する。この場合ホームエージェントHAは、この移動端末機MSにアドレッシングされたデータパケットを、移動端末機MSの現在のサブネットワークに転送する。

【０００５】

フォーリンエージェント(Foreign Agent)FAは、移動端末機MSが移動しているサブネッ

トワーク内に存在する。フォーリンエージェントFAは到来したデータパケットを移動端末機MSないしモバイルコンピュータMSに転送する。フォーリンエージェントFAはいわゆるフォーリンネットワーク(訪問先のネットワーク)内に存在する。フォーリンエージェントFAも通常の場合、ルータの構成要素である。フォーリンエージェントFAはすべての管理モバイルデータパケットを、移動端末機MSとそのホームエージェントHAとの間でルーティングする。フォーリンエージェントFAはホームエージェントHAから送信され、トンネリングされたIPデータパケットをアンパックし、そのデータを移動端末機MSに転送する。

【０００６】

移動端末機MSのホームアドレスは、この移動端末機MSに恒常的にアクセスすることができるアドレスである。ホームアドレスは、ホームエージェントHAと同一のアドレスプレフィクスを有する。ここで気付アドレスは、移動端末機MSがフォーリンネットワークにおいて使用するIPアドレスである。

【０００７】

ホームエージェントHAはいわゆるモビリティ結合テーブル(MBT: Mobility Binding Table)を管理する。このテーブル内のエントリは、移動端末機MSの2つのアドレス、すなわちホームアドレスと気付アドレスを相互に対応付け、データパケットを相応にリルートするために使用される。

【０００８】

MBTテーブルはホームアドレス、気付アドレス、およびこの対応付けが有効である期間(ライフタイム)についての情報に関するエントリを含む。

【０００９】

図１は、従来技術によるモビリティ結合テーブルMBTの一例を示す。

【００１０】

フォーリンエージェントFAは、訪問者リストないしビジターリスト(VL：Visitor List)を有し、このリストはその時点においてフォーリンエージェントFAのIPネットワーク内に存在する移動端末機MSに関する情報を包含する。

【００１１】

図２は、従来技術によるその種の訪問者リストの一例を示す。

【００１２】

モバイルコンピュータMSをネットワークに組み込むためには、モバイルコンピュータMSは先ず自身がホームネットワーク内にいるのか外部ネットワーク内にいるのかを識別しなければならない。付加的に移動端末機MSは、サブネットワーク内のどのコンピュータがホームエージェントもしくはフォーリンエージェントであるかを識別しなければならない。これらの情報はいわゆるエージェント発見(Agent Discovery)によって求められる。

【００１３】

続く登録によって移動端末機MSは自身の現在地を自身のホームエージェントHAに通知することができる。このためにモバイルコンピュータないし移動端末機MSはホームエージェントに目下の気付アドレスを送信する。登録のためにモバイルコンピュータMSは登録リクエスト(Registration-Request)ないし登録要求をホームエージェントに送信する。ホームエージェントHAは気付アドレスを自身のリストに登録し、登録リプレイ(Registration Reply)ないし登録応答により応答する。もっともこの場合、安全性に関する問題が存在する。原理的にはいずれのコンピュータもホームエージェントHAに登録リクエストを送信することができるので、簡単にホームエージェントHAに、コンピュータが別のネットワーク内を移動しているかのように認識させることができてしまう。つまり外部のコンピュータはモバイルコンピュータないし移動端末機のすべてのデータパケットを受け取ることが可能であり、このことを送信器が識別することもない。これを阻止するために、モバイルコンピュータMSおよびホームエージェントHAは共通の秘密キーを使用する。モバイルコンピュータMSが自身のホームネットワークに戻ると、このモバイルコンピュータMSはホームエージェントHAにおける登録が抹消される。なぜならばモバイルコンピュータMSはすべてのデータパケットを自身で受け取ることができるからである。モバイル無線ネットワークはこ

とに以下のセキュリティ特性を有していなければならない。情報に対するアクセスは所望の通信パートナに対してのみ許可される。すなわち伝送されるデータに対して不所望な傍受者によるアクセスは許可されない。したがってモバイル無線ネットワークは秘匿(Confidentiality)特性を有していなければならない。さらに認証性が与えられていなければならない。認証性(Authenticity)により通信パートナは、所望の通信パートナとの通信が実際に確立されたか、または部外者が通信パートナと称しているかを一義的に識別することができる。認証をメッセージ毎またはコネクション毎に実施することができる。コネクションを基礎として認証が行われる場合には、セッション(Session)の開始時に一度だけ通信パートナが識別される。セッションのさらなる経過に関しては、後続のメッセージが依然として相応の送信器に由来することが前提とされる。もちろん、通信パートナの同一性が確定されている場合であっても、すなわち通信パートナが認証されている場合であっても、この通信パートナはすべてのリソースへのアクセスが許可されない、もしくはネットワークを介するすべてのサービスの利用が許可されない場合もある。この場合においては、相応の許可はこの通信パートナが前もって認証されることを前提とする。

【００１４】

モバイルデータネットワークにおいては、メッセージがエアインタフェースを介して比較的長い区間を伝送されるので、潜在的な攻撃者はこれらのメッセージに容易にアクセスすることができる。したがってモバイル無線データネットワークにおいてはセキュリティの側面が非常に重要な役割を担う。データネットワークにおける安全性を高めるための重要な手段は暗号化技術である。暗号化によって、権限のない第三者がデータにアクセスできることなく、保安されていない通信経路、例えばエアインタフェースを介してデータを伝送することができる。暗号化のためにデータ、すなわちいわゆる平文が暗号化アルゴリズムにより暗号文に変換される。この暗号文を保安されていないデータ伝送チャネルを介して伝送し、続けて復号ないし解読することができる。

【００１５】

非常に有望な無線アクセス技術としてWiMax(Worldwide Interoperability for Microwave Access)が新たな標準として提案されており、これはIEEE802.16無線伝送のために使用される。WiMaxにより送信局は100Mbit/秒のデータレートで50kmまでの領域をカバーすることができる。

【００１６】

図３は、WiMax無線ネットワークに関する基準モデルを示す。移動端末機MSは、アクセスネットワーク(ASN：Access Serving Network)内に存在する。アクセスネットワークASNは少なくとも１つの訪問先ネットワーク(VCSN：Visited Connectivity Service Network)ないし中間ネットワークを介してホームネットワークHCSN(Home Connectivity Service Network)と接続されている。種々異なるネットワークがインタフェースないし基準点Rを介して相互に接続されている。移動局MSのホームエージェントHAは、ホームネットワーク(HCSN)または訪問先ネットワーク(VCSN)内に存在する。

【００１７】

WiMaxは、モバイルIPの2つの実現バリエーションを支援する。すなわち、移動局MS自体がMIPクライアント機能を実現するクライアントMIP(CMIP)と、MIPクライアント機能がWiMaxアクセスネットワークASNによって実現されているプロキシMIP(PMIP)の2つである。このためにASN内に設けられている機能性はプロキシモバイルノード(PMN)またはPMIPクライアントと称される。これによって自身ではMIPをサポートしない移動局MSもMIPを使用することができる。

【００１８】

図４は、ホームエージェントHAが訪問先ネットワークVCSN内に存在する場合の従来技術によるプロキシMIP(PMIP)におけるコネクション確立を示す。

【００１９】

移動端末機MSと基地局BSとの間の無線コネクションが確立された後に、先ずアクセス認証が行われる。認証、許可および課金の機能はいわゆるAAAサーバによって行われる(AAA

：Authentication Authorization and Accounting)。移動端末機MSとホームネットワークのAAAサーバ(HAAA)との間で認証メッセージが交換され、この認証メッセージによりホームエージェントHAのアドレスおよび認証キーが取得される。ホームネットワーク内の認証サーバは、加入者のプロフィールデータを有する。AAAサーバは、移動端末機の加入者識別子を含む認証リクエストメッセージを受け取る。AAAサーバはアクセス認証が成功すると、移動端末機MSとアクセスネットワークASNの基地局BSとの間のデータ伝送区間を保安するためにMSKキー(MSK：Master Session Key)を生成する。このMSKキーはホームネットワークのAAAサーバから中間ネットワークCSNを介してアクセスネットワークASNに伝送される。

【００２０】

アクセス認証後には、図４から見て取れるように、DHCPプロキシサーバがアクセスネットワークASNでコンフィギュレートされる。IPアドレスおよびホストコンフィギュレーションがすでにAAA応答メッセージに含まれている場合には、すべての情報がDHCPプロキシサーバにダウンロードされる。

【００２１】

認証および許可が成功すると、移動局ないし移動端末機MSがDHCP発見メッセージ(discovery message)を送信し、またIPアドレスの割当てが行われる。

【００２２】

移動端末機MSがネットワークに組み込まれると、この移動端末機MSは自分がホームネットワークにいるか外部ネットワークにいるかを認識できなければならない。さらにこの移動端末機MSは、どのコンピュータがそれぞれのネットワーク内でホームエージェントもしくはフォーリンエージェントであるかを識別しなければならない。これらの情報はいわゆるエージェント発見(Agent Discovery)によって求められる。エージェント発見には2種類がある。すなわち、エージェント広告(Agent Advertisement)とエージェント誘導(Agent Solicitation)がある。

【００２３】

エージェント広告ではエージェント、すなわちホームエージェントまたはフォーリンエージェントが周期的に同報メッセージをサブネットワークのすべてのコンピュータもしくは移動端末機に送信する。所定の期間に同報メッセージを聴取したコンピュータはいずれも、それぞれのサブネットワークにおけるエージェントを識別することができる。

【００２４】

移動端末機が新たに起動される場合、一般的に次のエージェント広告を待機することは実際的ではない。移動端末機MSは、今現在どのサブネットワーク内にいるかを即座に知らなければならない。したがっていわゆるエージェント誘導においては、移動端末機MSが、エージェント広告を実施せよとの要求をそれぞれのサブネットワークのすべてのコンピュータに送信する。移動端末機MSはエージェント誘導によって、エージェントを即座に識別することを強制することができ、これにより待機時間が格段に短縮される。エージェント誘導は、例えばパケット損失またはネットワーク切り換えの際にエージェント広告が行われない場合にも実施される。エージェント発見により、移動端末機MSは自身がホームネットワーク内にいるか、フォーリンネットワーク内にいるかを識別することもできる。エージェント広告メッセージ内のパケット情報に基づき、移動端末機MSは自身のホームエージェントHAを識別する。移動端末機MSがフォーリンネットワークからのメッセージパケットを受信すると、この移動端末機MSは自身の現在地が最後の広告以降に変化したか否かを付加的に識別することができる。移動端末機MSが広告メッセージを受信しない場合、この移動端末機MSは、ホームネットワーク内におり、かつホームエージェントHAは妨害されていないことをとりあえず前提にする。そして移動端末機MSはこの前提を確認するために、ネットワークのルータとコンタクトを取ることを試みる。移動端末機MSが自身のホームネットワーク内にいない場合には、この移動端末機MSはDHCPサーバにアクセスし、サブネットワークのアドレスを取得することを試みる。この試みが成功すると、移動端末機MSはこのアドレスをいわゆる共有気付アドレス(Colocated Care-of-Adresse)として使用し、ホー

ムエージェントHAとコンタクトを取る。共有気付アドレスはフォーリンネットワーク内の移動端末機MSに割り当てられたアドレスであり、ホームエージェントHAにも通知される。ネットワークベースのモビリティ管理(PMIP)と端末機ベースのモビリティ管理(CMIP)は区別される。端末機ベースのモビリティ管理CMIPは、端末機モバイルIP(MIP)を支援する。

【００２５】

図４は従来のネットワークベースのモビリティ管理(PMIP)におけるコネクション確立を示し、図５は従来の端末機ベースのモビリティ管理(CMIP)におけるコネクション確立を示す。

【００２６】

移動端末機MSとネットワークとの間でコネクションが確立されると、ホームネットワークの認証サーバ(H-AAA)は加入者の認証が成功した後に認証確認メッセージ(SUCCESS)を送信する。認証確認メッセージは、認証クライアントに加入者の認証が成功したことを通知する。

【００２７】

プロキシMIPないしネットワークベースのモビリティ管理(PMIP)では移動端末機はモバイルIPをサポートしない、もしくは相応のMIPソフトウェアが移動端末機MSで起動されない。

【００２８】

これに対してクライアントMIP(CMIP)ないし端末機ベースのモビリティ管理においては、モバイルIPがそれぞれの端末機ないし移動局MSによってサポートされる。

【００２９】

プロキシMIPでは、移動端末機MSはDHCPサーバによって割り当てられたIPアドレスしか識別しない。移動端末機MSの気付アドレスはこの移動端末機MSには既知ではなく、PMIPクライアント、フォーリンエージェントFAならびにホームエージェントHAに既知である。これに対してクライアントMIPでは、移動端末機MSは自身の両方のIPアドレス、すなわちホームアドレスも気付アドレスも識別する。

【００３０】

図４，５から分かるように、IPアドレスの割当て後にはMIP登録が行われる。このMIP登録の際に、ホームエージェントHAには移動端末機MSの現在地に関する情報が通知される。登録のために移動端末機MSまたは相応のPMIPクライアントは、目下の気付アドレスを含む登録リクエストをホームエージェントHAに送信する。ホームエージェントHAは気付アドレスを自身が管理するリストに登録し、登録応答(Registration Reply)により応答する。基本的に各コンピュータはホームエージェントHAに登録リクエストを送信することができるので、コンピュータまたは移動端末機MSは、別のネットワーク内を移動しているかのようにホームエージェントHAに簡単に認識させることができてしまう。これを阻止するために、移動端末機MSもホームエージェントHAも共通の秘密キー、すなわちモバイルIPキー(MIP-KEY)を使用する。

【００３１】

プロキシMIP(PMIP)では登録リクエスト(MIPRRQ)が、アクセスネットワークASN内のPMIPクライアントからフォーリンエージェントFAを介してホームエージェントHAに伝送される。図４に示されているように、ホームエージェントHAには所属の認証サーバH-AAAにより加入者用のキーが割り当てられ、ホームエージェントHAはこのキーをMIP登録応答(MIP Registration Reply)と共に伝送する。

【００３２】

図５に示されているように、端末機ベースのモビリティ管理(CMIP)では、登録リクエストメッセージ(MIPRRQ)が、移動端末機MSからフォーリンエージェントFAを介してホームエージェントHAに直接送信される。

【００３３】

WiMaxアクセスネットワークでは、モバイルIP(CMIP)の他にプロキシモバイルIP(PMIP)も使用され、これにより自身はモバイルIPクライアント機能を有していないクライアント

のためにモバイル管理を可能にしている。PMIPでは、アクセスネットワークにプロキシモバイルIPクライアントが設けられており、このプロキシモバイルIPクライアントはクライアントのために代理でMIPシグナリングを行う。これらのモバイルプロトコルは、WiMaxでは2つのアクセスネットワークASN間のハンドオーバ、ないしは2つのネットワークアクセスプロバイダNAP間のハンドオーバのために使用される。ここで所属のWiMaxホームエージェントは選択的に、WiMaxホームネットワークHCSNまたは訪問先WiMaxネットワーク(VCSN)に存在することができる。WiMaxでは、ホームネットワークHCSNにホームAAAサーバが存在し、このホームAAAサーバはユーザと共有の長期暗号キーと別の使用パラメータを知っていることが前提である。

【００３４】

登録の際にWiMaxホームエージェントは、WiMaxホームAAAサーバに保安パラメータ、例えば一時的暗号キーを問い合わせる。このことは、権限のあるクライアントだけがホームエージェントに登録することができるようにし、MIPシグナリングを保安するために必要である。移動端末機が認証サーバとともに実行する認証およびキー取決めプロトコルの一部として、移動端末機もこの保安パラメータを導出することができる。WiMaxアクセスネットワークでは、いわゆるEMSKキー(Extended Master Session Key)からAMSKないしはモバイルIPルートキー(MIP-RK)が導出され、作成される。このモバイルIPルートキーから、続いて別のキーが導出される。この別のキーは、モバイルノードないしはフォーリンエージェントFAとホームエージェントHAとの間の種々の通信区間を保安するためのものである。ここでは種々のモバイルIPバージョン、例えばモバイルIP V6およびモバイルIP V4が、固有のキーによってクライアントモバイルIPの場合とプロキシモバイルIPの場合に対してそれぞれ導出される。

【００３５】

従来のWiMaxアクセスネットワークでは、別形式のネットワークとのインタワーキングないしは共同作業がサポートされていない。

【００３６】

図６は、WiMaxアクセスネットワークと3GPPホームネットワークとの従来技術による相互作用を示す。図６から分かるように、WiMaxアクセスネットワークには認証プロキシサーバ(AAA-Relay)が設けられており、これはインタワーキングユニットIWUを3GPPホームネットワークへのインタフェースとして有する。認証プロキシサーバは、3GPPネットワークとのインタワーキングの場合に、キー作成とキー導出を引き受ける。このキー作成とキー導出は、加入者のネットワークエントリーの枠内で、加入者ないしは移動端末機に対してプロキシモバイルIPを起動するために必要である。プロキシモバイルIPの場合、プロキシモバイルIPクライアントは、WiMaxホームネットワークWiMax-CSNのASNゲートウェイないしは認証プロキシサーバ内に存在する。このWiMaxホームネットワークWiMax-CSNは、図６に示されるように3GPPネットワークと接続されている。したがってプロキシモバイルIPでは、インタワーキングユニットIWUがモバイルIPキー(MIP-Key)を、ネットワークエントリーの際にプロキシモバイルIPクライアントとホームエージェントとの間の区間を保安するために生成する。ここでプロキシモバイルIPクライアントは有利には、ASNゲートウェイ内に存在し、したがってアクセスネットワークインフラストラクチャの一部を形成する。したがってプロキシモバイルIPでは、3GPP認証サーバを変更することは不要であり、3GPP認証サーバはWiMaxアクセスネットワークの仕様を満たす必要はない。

【００３７】

クライアントプロキシモバイルIPでは、とりわけWiMaxアクセスネットワークと3GPPホームネットワークとの間のインタワーキングがサポートされていない。現在のところ、保安パラメータをクライアントないしは移動端末機に転送するための固有のプロトコルは存在しない。その理由は、移動端末機がこの保安パラメータを、従来の処理では認証およびキー取決めプロトコルから導出するからである。

【発明の概要】

【発明が解決しようとする課題】

【００３８】
したがって本発明の課題は、移動端末機とアクセスネットワークのノードとの間でのデータ伝送を保安するためのアクセス専用キーを提供する方法およびシステムを開示することであり、これはホームネットワークの認証サーバがモビリティ管理をサポートしない場合でもクライアントIP(CMIP)を可能にする。
【課題を解決するための手段】
【００３９】
本発明は、移動端末機とアクセスネットワークのノードとの間でのデータ伝送を保安するためのアクセス専用キーを提供するための方法を開示する。ここでは、移動端末機の認証の際に認証サーバがセッションキーを生成し、このセッションキーからベースキーが導出され、インタワーキングプロキシサーバに伝送され、このインタワーキングプロキシサーバは伝送されたベースキーからアクセス専用キーを導出し、アクセスネットワークのノードに提供する。
【発明の効果】
【００４０】
本発明の方法の有利な実施形態では、セッションキーはMSK(Master Session Key)キーまたはEMSK(Extended Master Session Key)キーにより形成される。
【００４１】
したがって本発明の方法では、保安の理由からホームネットワークの認証サーバ(AAA)から離れてはならないローカルマスタセッションキー(MSKないしはEMSK)が、擬似ベースキーないしはベースキーの導出のために利用され、引き続きインタワーキングプロキシサーバに伝送される。そしてインタワーキングプロキシサーバは受信したベースキーから必要なアクセス専用キーを、所定のキー階層にしたがい導出し、アクセスネットワークのそれぞれのノードのために提供する。
【００４２】
本発明による方法の有利な実施形態においては、認証サーバが移動端末機のホームネットワーク内に存在する。
【００４３】
本発明の方法の実施形態では、ベースキーがセッションキーから、所定の第1の誘導関数によって導出される。
【００４４】
この第1の誘導関数は有利には、HMAC-SHA1誘導関数、HMAC-SHA256誘導関数、HMAC-MD5誘導関数、 SHA1誘導関数、SHA-256誘導関数またはMD5誘導関数により形成される。
【００４５】
本発明の方法の有利な実施形態では、ベースキーの導出は、セッションキーと符合文字列(ストリング)に依存して行われる。
【００４６】
本発明の方法の有利な実施形態では、移動端末機の認証は認証サーバにおいてEAPプロトコルによって行われる。
【００４７】
本発明の方法の別の有利な実施形態では、移動端末機の認証は認証サーバにおいてUMTS-AKAプロトコルによって行われる。
【００４８】
本発明の方法の択一的な実施形態では、移動端末機の認証は認証サーバにおいてHTTPダイジェストAKAプロトコルによって行われる。
【００４９】
本発明の方法の別の実施形態では、認証サーバとインタワーキングプロキシサーバとの間のデータ伝送は、DiameterプロトコルまたはRadiusプロトコルによって行われる。
【００５０】
本発明の方法の有利な実施形態では、アクセスネットワークはWiMaxネットワークによ

って形成される。
【００５１】
本発明の方法の有利な実施形態では、ホームワークは3GPPネットワークによって形成される。
【００５２】
本発明の方法の有利な実施形態では、伝送されたベースキーからインタワーキングプロキシサーバによって第2の誘導関数を用いてモバイルIPルートキーが導出される。
【００５３】
この第2の誘導関数は有利には、HMAC-SHA1誘導関数、HMAC-SHA256誘導関数、HMAC-MD5誘導関数、 SHA1誘導関数、SHA-256誘導関数またはMD5誘導関数により形成される。
【００５４】
本発明の方法の有利な実施形態では、導出されたモバイルIPルートキーから第3の誘導関数によって、移動端末機とアクセスネットワークのノードとの間のデータ伝送を保護するためのアクセス専用キーが導出される。
【００５５】
この第3の誘導関数は有利には、HMAC-SHA1誘導関数、HMAC-SHA256誘導関数、HMAC-MD5誘導関数、 SHA1誘導関数、SHA-256誘導関数またはMD5誘導関数である。
【００５６】
本発明の方法の実施形態では、アクセスネットワークのノードと移動端末機との間の種々のデータ伝送区間のために、それぞれ1つの所属のアクセス専用キーが導出される。
【００５７】
本発明の方法の実施形態では、移動端末機が認証の際に同様にセッションキーを生成し、そこからアクセス専用キーを導出する。
【００５８】
本発明さらには、ベースキーを提供するための認証サーバを開示するものであり、このベースキーから移動端末機とアクセスネットワークのノードとの間でのデータ伝送を保安するためのアクセス専用キーを導出することができる。ここでは、
認証サーバが移動端末機の認証の際にセッションキーを生成し、そこから誘導関数によってベースキーを導出し、インタワーキングプロキシサーバに提供する。
【００５９】
本発明さらには、移動端末機とアクセスネットワークのノードとの間でのデータ伝送を保安するためのアクセス専用キーを提供するインタワーキングプロキシサーバを開示する。ここでは、インタワーキングプロキシサーバは、認証サーバから伝送されたベースキーからアクセス専用キーを導出し、アクセスネットワークのノードに提供する。
【００６０】
本発明さらに、複数のアクセスネットワークと、移動端末機の少なくとも1つのホームネットワークとを備えるデータ伝送システムに関する。ここではホームネットワークの認証サーバが、移動端末機の認証の際にセッションキーを生成し、そこから共通のベースキーを導出し、このベースキーがアクセスネットワークに伝送され、このアクセスネットワークはインタワーキングプロキシサーバを有しており、このインタワーキングプロキシサーバは少なくとも1つのアクセス専用キーを伝送されたベースキーから導出し、このアクセス専用キーは、移動端末機とそれぞれのアクセスネットワークのノードとの間のデータ伝送区間を保安するために設けられている。
【００６１】
移動端末機とアクセスネットワークのノードとの間でのデータ伝送を保安するためのアクセス専用キーを提供するための本発明方法および本発明のシステムの有利な実施形態の詳細について、本発明の主要な特徴を示す添付図面を参照して説明する。
【図面の簡単な説明】
【００６２】
【図１】従来技術のモビリティエントリーを示す図である。

【図２】従来技術による訪問者リストを示す。
【図３】WiMax無線ネットワークに対する基準モデルを示す。
【図４】従来技術によるプロキシMIP(PMIP)におけるコネクション確立を示す。
【図５】従来技術によるクライアントMIP(CMIP)におけるコネクション確立を示す。
【図６】WiMaxアクセスネットワークと3GPPホームネットワークとの従来技術による相互作用(インタワーキング)を示す。
【図７】アクセス専用キーを提供するための本発明のシステムの実施形態のブロック回路図である。
【図８】アクセス専用キーを提供するための本発明の方法の実施形態を示す信号線図である。
【図９】アクセス専用キーを提供するための本発明の方法の実施形態を示す別の信号線図である。
【発明を実施するための形態】
【００６３】
図７は、アクセス専用キーを提供するための本発明による方法を使用することができるネットワークアーキテクチャを示す。移動端末機1(MS＝移動局)は、インタフェースR1を介してアクセスネットワーク2(ASN= Access Service Network)に接続されている。アクセスネットワーク2は、インタフェースR3を介して訪問先ネットワーク3(VCSN=訪問先のコネクティビティサービスネットワーク；Visited Connectivity Service Network)に接続されている。この訪問先ネットワーク3は、インタフェースR5を介してホームネットワーク4(HCSN=ホームコネクティビティサービスネットワーク；Home Connectivity Service Network)と接続されている。
【００６４】
移動端末機1が第1のアクセスネットワーク2から第2のアクセスネットワーク2'に移動すると、第1のアクセスネットワークと第2のアクセスネットワークとの間で引渡し(ハンドオーバ)が行われる。この引渡し(ハンドオーバ)はWiMax仕様において「マクロモビリティ管理；Macro Mobility Management」または「R3モビリティ；R3 Mobility」もしくは「インタASNモビリティ；Inter ASN Mobility」と称される。訪問先ネットワーク3およびホームネットワーク4は、それぞれアクセスサービスプロバイダ(ASP；Access Service Provider)のネットワークまたはインターネットに接続されている。
【００６５】
各アクセスネットワーク2は複数の基地局6を有し、それらの基地局6はインタフェースR6を介してASNゲートウェイノード５に接続されている。図６に示されているASNゲートウェイノード5はオーセンティケータ5A、MIPフォーリンエージェント5Bおよびオプションとして PMIPクライアント5C、ならびにオプションとしてインタワーキングプロキシユニット7を有する。各訪問先ネットワーク3には、図６に示されているようにAAAサーバ3Aが設けられている。同様にホームネットワーク4にはオーセンティケータ4Aならびにホームエージェント4Bが設けられている。択一的実施形態では、インタワーキングユニット7もホームネットワーク4に設けられている。
【００６６】
移動端末機1に関しては2つのケースを区別することが重要である。つまり、移動端末機1が自身でモバイルIPをサポートし、かつ固有のCMIPクライアントを有するケースと、移動端末機1がモバイルIPをサポートせず、かつアクセスネットワーク2のゲートウェイノード5におけるPMIPクライアント5Cを必要とするケースである。
【００６７】
図８は、本発明による方法の実施形態を説明するための信号線図を示す。
ここでインタワーキングユニット7は、第1の実施形態ではアクセスネットワーク2に、または択一的実施形態ではホームネットワーク4に設けられている。本発明の方法ではアクセス専用キーが、移動端末機1とアクセスネットワーク2の任意のノードとの間のデータ伝送を保安するために提供される。ここで移動端末機1の認証の際に、移動端末機4のホーム

ネットワーク4に存在する認証サーバ4Aがセッションキーを生成し、このセッションキーからベースキーを導出し、このベースキーがインタワーキングプロキシサーバ1に、図７に示したように伝送される。インタワーキングプロキシサーバ7は受信したベースキーから必要なアクセス専用キーを、誘導関数を用いて導出し、アクセスネットワーク2のそれぞれのノードのために提供する。伝送されるベースキーが導出されるセッションキーは、実施形態ではMSK(Master Session Key)キーまたはEMSK(Extended Master Session Key)キーにより形成される。図８に示すように、認証サーバ4Aは、擬似EMSKないしは共通のベースキーをHMAC-SHA1誘導関数によって拡張マスタセッションキーEMSKから導出する。択一的実施形態でこの誘導関数は、HMAC-SHA256誘導関数、HMAC-MD5誘導関数、 SHA1誘導関数、SHA-256誘導関数またはMD5誘導関数により形成される。導出されたベースキーないしは擬似キーは、EAP成功メッセージで、マスタセッションキーMSKとともにインタワーキングユニット7に伝送される。このインタワーキングユニット7は、たとえばインタワーキングプロキシサーバとして構成されている。

【００６８】

本発明の別の実施形態では、ベースキーないしは擬似キーPEMSKの導出が、セッションキーMSKおよび/またはEMSKに依存して、かつ付加的に符合文字列ないしはストリングに依存して、すなわち次のバリエーションの1つに相応して行われる：

PEMSK = H(MSK, EMSK, "ストリング")、

PEMSK = H(MSK, "ストリング")、

PEMSK = H(EMSK, "ストリング")。

【００６９】

図８に示した実施形態で、移動端末機1の認証はEAPデータ伝送プロトコルによって行われる。択一的実施形態で、移動端末機の認証は認証サーバ4Aにおいて、UMTS-AKAプロトコルまたはHTTPダイジェストAKAプロトコルによって行われる。認証サーバ4Aとインタワーキングプロキシサーバ7との間のデータ伝送は有利には、DiameterプロトコルまたはRadiusプロトコルによって行われる。

【００７０】

導出されたベースキーないしは擬似キーは、キー階層での中間段階である。このベースキーは共通のベースキーとして、種々のアクセスネットワーク2に設けられた種々のインタワーキングプロキシサーバ1にも伝送される。アクセスネットワーク2は例えばWiMaxネットワークである。認証サーバ4Aが設けられているホームネットワーク4は、例えば3GPPネットワークである。

【００７１】

図８に示されているようにインタワーキングプロキシサーバ7が伝送されたベースキーPEMSKを受け取ると直ちに、このインタワーキングプロキシサーバは第2の誘導関数を用いてモバイルIPルートキーIMP-RKを生成する。この第2の誘導関数も同様に、HMAC-SHA1誘導関数、HMAC-SHA256誘導関数、HMAC-MD5誘導関数、 SHA1誘導関数、SHA-256誘導関数またはMD5誘導関数とすることができる。別の実施形態では、別の誘導関数ないしは暗号キー誘導関数KDFを使用することができる。このようにして導出されたモバイルIPルートキーIMP-RKから、キー階層に相応してさらなるアクセス専用キーを、移動端末機1とアクセスネットワーク2のノードとの間のデータ伝送を保安するために導出することができる。この第3の誘導関数も例えば、HMAC-SHA1誘導関数、HMAC-SHA256誘導関数、HMAC-MD5誘導関数、SHA1誘導関数、SHA-256誘導関数またはMD5誘導関数とすることができる。

【００７２】

モバイルIPルートキーIMP-RKは、そこからアプリケーションキーないしはアクセス専横キーを生成するために使用される。例えば：

MN-HA-MIP4 = H (MIP-RK, "ストリング"|HA-IP)

MN-HA-CMIP6 = H (MIP-RK, "ストリング"|HA-IP)

MN-FA = H (MIP-RK, "ストリング"|FA-IP) そして

FA-H = H (MIP-RK, "ストリング"|FA-IP|HA-IP|NONCE)。

【００７３】
符合"|"は、部分符合文字列の連続に対するものである。
【００７４】
キー導出はさらに、PMIPV4とCMIPV4に対して別個のキーを導出するように変更することができる。例えば：
MN-HA-CMIP4 = H(MIP-RK, "CMIP4MNHA"|HA-IP)
MN-HA-PMIP4 = H(MIP-RK, "PMIP4MNHA"|HA-IP)。
【００７５】
アクセスネットワーク2のノードと移動端末機との間の種々のデータ伝送区間のそれぞれに対してこのようにして、所属のアクセス専用キーをモバイルIPルートキーIMP-RKから導出することができ、このモバイルIPルートキーIMP-RKは伝送されたベースキーから導出される。
【００７６】
本発明の方法では、加入者のための、EAPベースのネットワークエントリーの枠内でこれまでのキー導出が拡張され、インタワーキングプロキシサーバ7がアクセスネットワークに、CMIPに適するキーを提供するようになり、このキーは場合によりPMIPにも使用可能であるようになる。本発明の方法では、ベースキーないしは擬似キーが、MSKおよび/またはEMSKおよび/または別の入力、例えば符合文字列から適切なキー誘導関数KDFを用い、認証サーバによって導出される。
【００７７】
図９は、本発明による方法の基礎となる原理を説明するための信号チャートである。移動端末機1の認証の際には認証およびキー取決めプロトコル、例えばRadiusまたはDiameterに基づくEAPを用いて、保安サーバないしは認証サーバ4Aが第1のネットワークでベースキーないしは擬似キーないしは擬似一次暗号キーを、一時的暗号キーTKS、例えばマスタセッションキーMSKないしはEMSKに基づいて生成する。誘導関数により導出された擬似キーは引き続き、第2のネットワークにあるインタワーキングプロキシサーバ1に伝送される。ここでは各認証サーバないしはノード8，9に対して別の誘導関数からアクセス専用キーが導出される。続いて、各アプリケーションサーバ8，9はインタワーキングプロキシサーバ7から、導出されたアクセス専用キーを受け取る。引き続き、伝送されたキーを用いて端末機1とそれぞれのアプリケーションサーバ8，9との間のデータ伝送区間が暗号で保護される。
【００７８】
本発明の方法により、認証サーバ、例えばWLANサーバまたは3GPPサーバをWiMaxアクセスネットワークのために使用することができる。この認証サーバは、WiMaxアクセスネットワークにより期待されるCMIP/PMIP機能性を提供する必要はなく、ベースキーをセッションキーから導出するという機能性だけを拡張すればよい。本発明の方法の利点は、WiMaxアクセスネットワークにおいてCMIPのケースもサポートされ、したがってマクロモビリティに関する制限が回避されることである。本発明の方法で、WiMazxネットワークは、WiMaxネットワークにインタワーキングプロキシサーバ7を設けることは例外として、それ以上の変更は必要ない。移動端末機1、認証サーバならびにインタワーキングプロキシサーバ7は、どのベースキーないし擬似キーを自分が使用するかを知る。これにより、種々異なるMIPキー(Bootstrapping-Varianten)をWiMaxネットワーク内でサポートすることができる。本発明の方法では、例えば3GPPネットワークから発するキーマテリアルが、WiMaxネットワークに対するキーマテリアルに変換され、WiMaxネットワークは形成されたキーを、適合を行うことなしに使用することができる。
【００７９】
本発明の方法の実施形態では、本発明による認証機能性がWiMaxネットワークの外でも、例えば3GPPネットワークでも確立される。本発明の方法によって、将来的にWiMax-3GPPインタワーキングが可能となり、これによりWiMaxネットワークでの制限が生じることもない。本発明の方法のさらなる利点は、種々のネットワーク間のインタワーキングに容易

に拡張することができ、任意のアプリケーションに対してキーを提供するように拡張できることである。本発明の方法では、インタワーキングプロキシサーバ7だけが、どのアプリケーション専用キーを提供しなければならず、これをどのように導出するかを知ればよい。したがって本発明の方法では、ホーム認証サーバが、接続されたすべての種々異なるネットワークに対してそれぞれ所要のキーを生成する必要はない。したがって本発明の方法では比較的簡単に、種々異なるネットワークをフレキシブルにホームネットワークに接続することができる。

【００８０】

本発明の方法では、移動端末機1が認証の際に同様にセッションキーを生成し、相応にしてそこからアクセス専用キーを導出する。

【図１】

従来技術

モビリティ結合テーブル

ホームアドレス	気付アドレス	ライフタイム (ms)
131.192.180.42	129.142.23.42	100
213.123.24.140	172.23.142.49	150
・・・	・・・	・・・

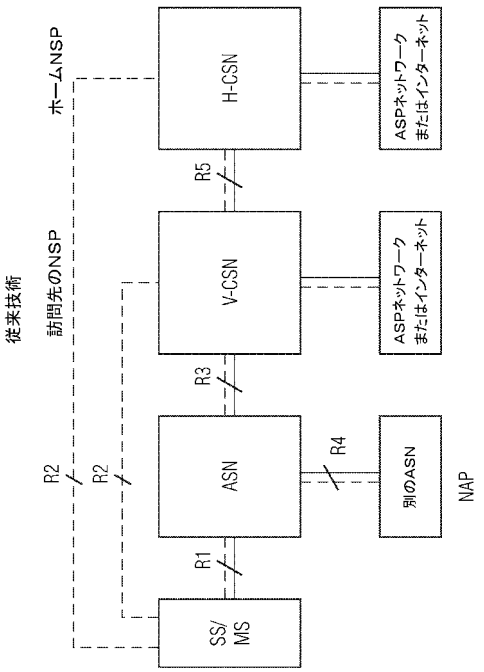
【図２】

従来技術

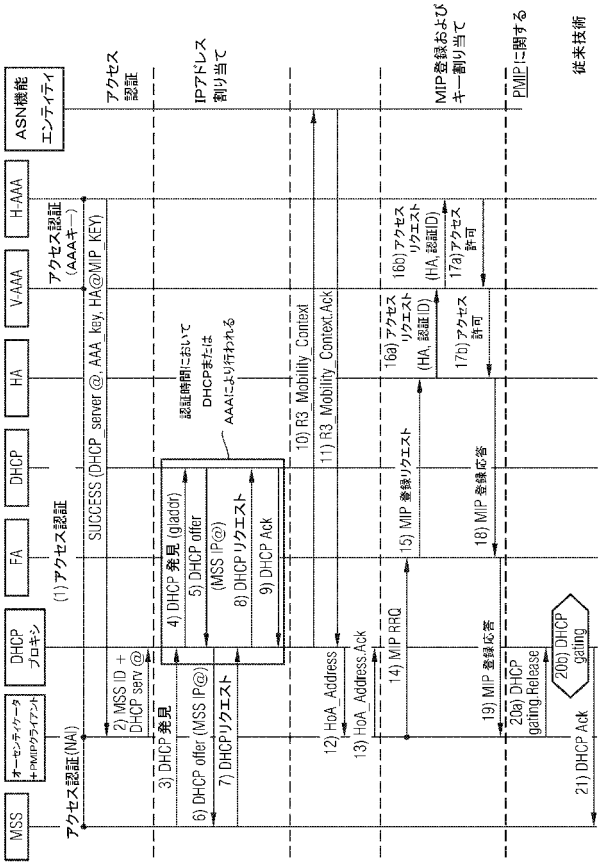
訪問者リスト

ホームアドレス	ホームエージェントアドレス	メディアアドレス	ライフタイム
131.192.180.42	129.142.23.42	08-00-46-26-75-6A	100
213.123.24.140	172.23.142.49	00-02-B3-77-43-00	150
・・・	・・・	・・・	・・・

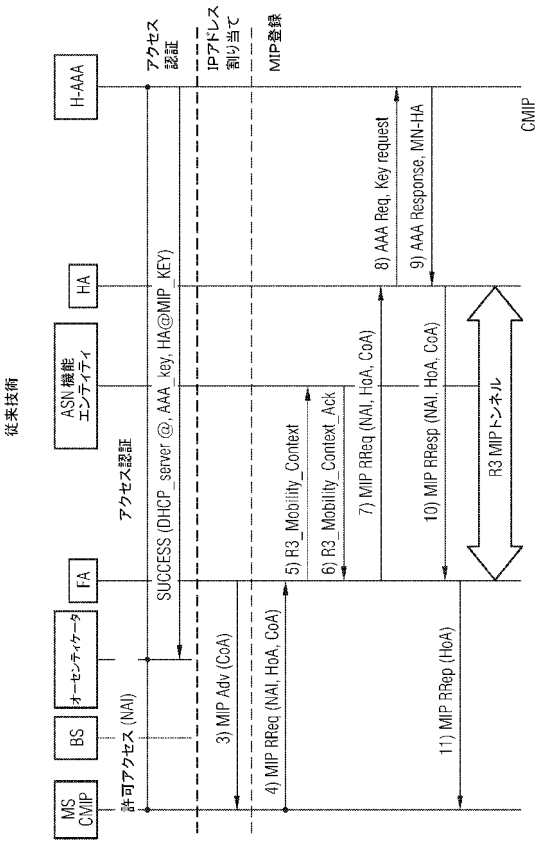
【図３】



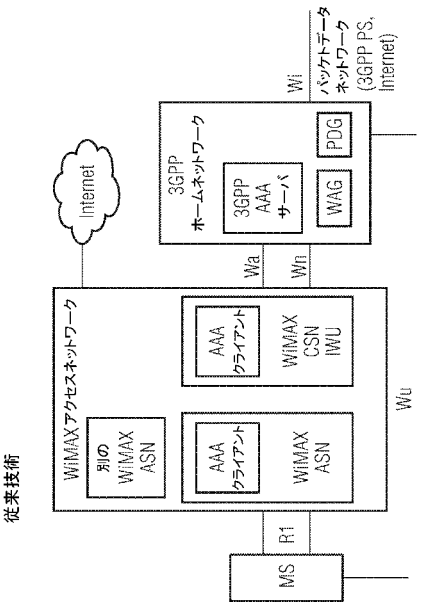
【図４】


MSS
オーセンティケータ+PMIPクライアント
DHCP プロキシ
FA
DHCP
HA
V-AAA
H-AAA
ASN機能 エンティティ
アクセス認証
IPアドレス 割り当て
MIP登録および キー割り当て
PMIPに関する
従来技術
アクセス認証(NAI)
(1) アクセス認証
SUCCESS (DHCP_server @, AAA_key, HA@MIP_KEY)
アクセス認証 (AAAキー)
2) MSS ID + DHCP serv @
3) DHCP 発見
4) DHCP 発見 (giador)
5) DHCP offer (MSS IP@)
6) DHCP offer (MSS IP@)
7) DHCPリクエスト
8) DHCP リクエスト
9) DHCP Ack
認証時間において DHCPまたは AAAにより行われる
10) R3_Mobility_Context
11) R3_Mobility_Context.Ack
12) HoA_Address
13) HoA_Address.Ack
14) MIP RRQ
15) MIP 登録リクエスト
16a) アクセス リクエスト (HA, 認証ID)
16b) アクセス リクエスト (HA, 認証ID)
17a) アクセス 許可
17b) アクセス 許可
18) MIP 登録応答
19) MIP 登録応答
20a) DHCP gating Release
20b) DHCP gating
21) DHCP Ack

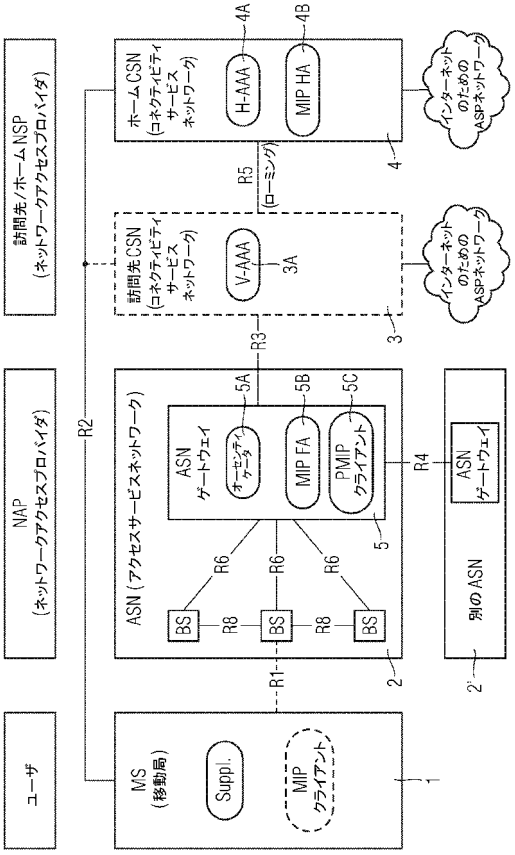
【図５】


従来技術
MS CMIP
BS
オーセンティケータ
FA
ASN機能 エンティティ
HA
H-AAA
アクセス認証
IPアドレス 割り当て
MIP登録
CMIP
許可アクセス (NAI)
アクセス認証
SUCCESS (DHCP_server @, AAA_key, HA@MIP_KEY)
3) MIP Adv (CoA)
4) MIP RReq (NAI, HoA, CoA)
5) R3_Mobility_Context
6) R3_Mobility_Context_Ack
7) MIP RReq (NAI, HoA, CoA)
8) AAA Req, Key request
9) AAA Response, MN-HA
10) MIP RResp (NAI, HoA, CoA)
11) MIP RRep (HoA)
R3 MIPトンネル

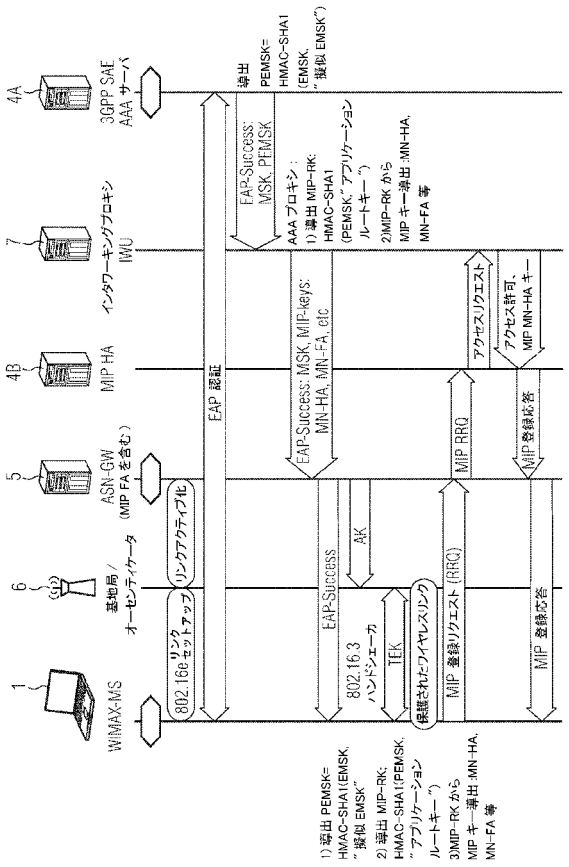
【図６】


従来技術
Internet
WiMAXアクセスネットワーク
別の WiMAX ASN
AAA クライアント
WiMAX ASN
AAA クライアント
WiMAX CSN IWU
Wu
MS
R1
3GPP ホームネットワーク
3GPP AAA サーバ
WAG
PDG
Wa
Wn
Wi
パケットデータ ネットワーク (3GPP PS, Internet)

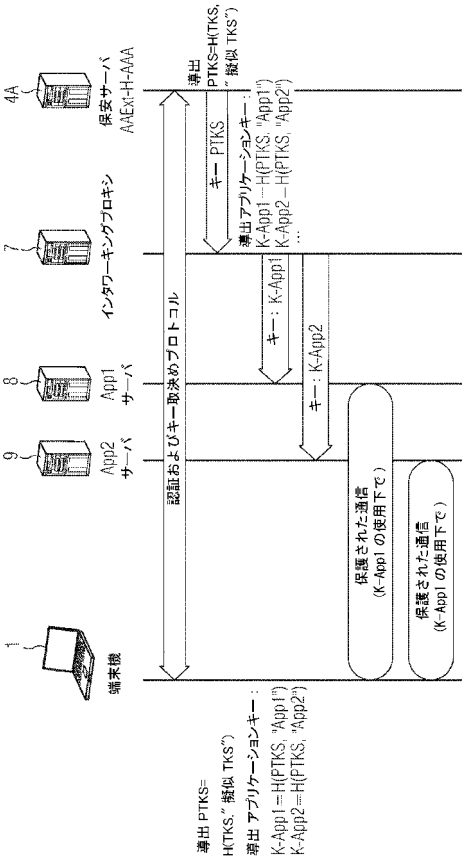
【図７】


ユーザ
訪問先/ホーム NSP (ネットワークアクセスプロバイダ)
NAP (ネットワークアクセスプロバイダ)
MS (移動局)
Suppl.
MIP クライアント
ASN (アクセスサービスネットワーク)
ASN ゲートウェイ
オーセンティケータ
MIP FA
PMIP クライアント
BS
別の ASN
訪問先CSN (コネクティビティ サービス ネットワーク)
V-AAA
ホーム CSN (コネクティビティ サービス ネットワーク)
H-AAA
MIP HA
インターネットのための ASPネットワーク
R1
R2
R3
R4
R5 (ローミング)
R6
R8
1
2
2'
3
3A
4
4A
4B
5
5A
5B
5C

【図８】


1
WiMAX-MS
6
基地局 / オーセンティケータ
5
ASN-GW (MIP FA を含む)
4B
MIP HA
7
インタワーキングプロキシ IWU
4A
3GPP SAE AAA サーバ
802.16e リンクセットアップ
リンクアクティブ化
EAP 認証
EAP-Success
802.16.3 ハンドシェーカ
TEK
保護されたワイヤレスリンク
AK
EAP-Success: MSK, MIP-keys: MN-HA, MN-FA, etc
EAP-Success: MSK, PEMSK
導出 PEMSK= HMAC-SHA1 (EMSK, "擬似 EMSK")
AAA プロキシ: 1) 導出 MIP-RK: HMAC-SHA1 (PEMSK, "アプリケーション ルートキー ") 2)MIP-RK から MIP キー導出 :MN-HA, MN-FA 等
MIP RRQ
MIP 登録リクエスト (RRQ)
アクセスリクエスト
アクセス許可, MIP MN-HA キー
MIP 登録応答
MIP 登録応答
1)導出 PEMSK= HMAC-SHA1(EMSK, "擬似 EMSK" 2) 導出 MIP-RK: HMAC-SHA1(PEMSK, "アプリケーション ルートキー ") 3)MIP-RK から MIP キー導出 :MN-HA, MN-FA 等

【図９】


1
端末機
9
App2 サーバ
8
App1 サーバ
7
インタワーキングプロキシ
4A
保安サーバ AAExt-H-AAA
認証およびキー取決めプロトコル
導出 PTKS= H(TKS," 擬似 TKS")
キー PTKS
導出アプリケーションキー : K-App1=H(PTKS, "App1") K-App2=H(PTKS, "App2")
キー : K-App1
キー : K-App2
保護された通信 (K-App1 の使用下で)
保護された通信 (K-App1 の使用下で)
導出 PTKS= H(TKS," 擬似 TKS")
導出 アプリケーションキー : K-App1=H(PTKS, "App1") K-App2=H(PTKS, "App2")

フロントページの続き

(74)代理人 100099483
弁理士 久野 琢也
(74)代理人 100112793
弁理士 高橋 佳大
(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 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 ライナー ファルク
ドイツ連邦共和国 エアディング パークシュトラーセ ４３
(72)発明者 ギュンター ホルン
ドイツ連邦共和国 ミュンヘン プレラートーツィストルーシュトラーセ １２
(72)発明者 ディルク クレーゼルベルク
ドイツ連邦共和国 ミュンヘン ペスタロッツィシュトラーセ ２７

審査官 久松 和之

(56)参考文献 特表２００５－５３０２７７（ＪＰ，Ａ）
特表２００８－５０６３１７（ＪＰ，Ａ）
特表２００８－５２９３６８（ＪＰ，Ａ）
特開２００２－２３２４１８（ＪＰ，Ａ）
特開２００５－２１０６３９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04B 7/24 - 7/26
H04W 4/00 - 99/00