(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2005-524255
(P2005-524255A)
(43)公表日　平成17年8月11日(2005.8.11)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04Q 7/38	H04B	7/26	109R	5J104
H04L 9/08	H04L	12/56	100D	5K030
H04L 9/14	H04L	9/00	641	5K067
H04L 12/56	H04L	9/00	601E	

審査請求 未請求　予備審査請求 有　（全 26 頁）

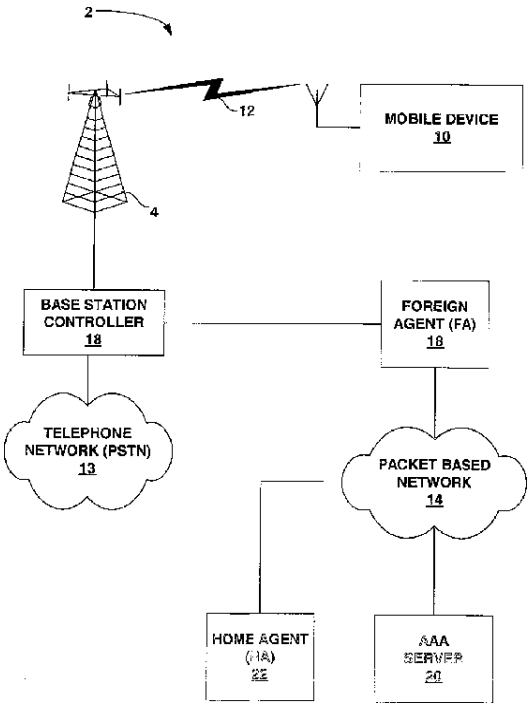
(21)出願番号　特願2003-585398 (P2003-585398)
(86)(22)出願日　平成15年4月4日 (2003.4.4)
(85)翻訳文提出日　平成16年11月10日 (2004.11.10)
(86)国際出願番号　PCT/US2003/010512
(87)国際公開番号　WO2003/088617
(87)国際公開日　平成15年10月23日 (2003.10.23)
(31)優先権主張番号　60/370,442
(32)優先日　平成14年4月5日 (2002.4.5)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　60/407,469
(32)優先日　平成14年8月29日 (2002.8.29)
(33)優先権主張国　米国 (US)

(71)出願人　595020643
クゥアルコム・インコーポレイテッド
ＱＵＡＬＣＯＭＭ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100109830
弁理士　福原　淑弘

最終頁に続く

(54)【発明の名称】移動無線システムにおけるキー更新

(57)【要約】
【課題】移動無線システムにおけるキー更新。
【解決手段】本開示は、移動ＩＰネットワーク内で用いるためのセキュリティキー更新方式を記述する。更新方式は、移動デバイスおよび移動デバイスを認証するサーバ計算機間のセキュリティキー更新を容易にするために実行することが可能である。この中に記述された技術は、更新ルーチン期間中の可能性のあるメッセージ損失、更新ルーチン期間中の移動デバイス故障、あるいは移動ネットワークセッティングにおいて典型的に遭遇する他の問題を考慮に入れるような方法で、セキュリティキー更新を容易にすることが可能である。このようにして、技術はセキュリティキー更新のための強力な方式を与えることが可能であり、そしてネットワークセキュリティを改善することが可能である。



【特許請求の範囲】
【請求項１】
方法であって、
ネットワークに対するアクセスのための第１の登録要求を受信し、なお第１の登録要求はキーを用いて形成されており、
第１の登録要求に対応した、ネットワークにアクセスするためにはキー更新が必要であることを示す第１の回答を送出し、
新しいキーを含む第２の登録要求を受信し、
新しいキーは第２の登録要求に対応して受信されたことを示す第２の回答を送出し、
新しいキーは他の第２の登録要求を受信するときに、ネットワークへのアクセスを許可するに先立って受信されたことを示す他の第２の回答を再送出し、
第３の登録要求を受信し、なお第３の登録要求は新しいキーを用いて形成されており、そして
第３の登録要求に続いてネットワークに対するアクセスを許可する
ことを含む方法。
【請求項２】
ここで、第２の登録要求は新しいキーおよびトークンを含み、そして第２の回答はトークンを含む、請求項１記載の方法。
【請求項３】
さらに、ネットワークへのアクセスの許可に先立って他の第１の登録要求を受信するときは、他の第１の回答を再送出することを含む、請求項１記載の方法。
【請求項４】
さらに、新しいキーを用いて形成されていなかった登録要求を受信するときは、第２の回答の送出後に他の第１の回答を再送出することを含む、請求項１記載の方法。
【請求項５】
さらに、
第２の登録要求を受信するときは新しいキーを保管し、そして
第３の登録要求の受信後に認証に用いるための新しいキーを引き渡す
ことを含む、請求項１記載の方法。
【請求項６】
方法であって、
ネットワークに対するアクセスを要求するために、キーを用いて形成された第１の登録要求を送出し、
ネットワークにアクセスするためにはキー更新が必要であることを示す第１の回答を受信し、
第１の回答に対応して新しいキーを含む第２の登録要求を送出し、
ネットワークにアクセスするためにはキー更新が必要であることを示す、他の第１の回答を受信し、
他の第１の回答の受信に対応して、新しいキーを含む他の第２の登録要求を送出し、
第２の登録要求に対応して、新しいキーが受信されたことを示す第２の回答を受信し、
新しいキーを用いて形成された第３の登録要求を送出し、そして
第３の登録要求に続いてネットワークにアクセスする
ことを含む方法。
【請求項７】
さらに、定義された時間の総量内に第２の回答が受信されない場合は、第２の要求を再送出することを含む、請求項６記載の方法。
【請求項８】
デバイスであって、
データで変調された信号を受信する受信機と、
データで変調された信号を送出する送信機と、そして

デバイスのためにセキュリティキーを更新するためのキー更新論理と、なおデバイスは
送信機は、ネットワークに対してアクセスを要求するために、キーを用いて形成された第１の登録要求を送出し、
受信機は、ネットワークにアクセスするためにはキー更新が必要であることを示す、第１の登録要求に対応した第１の回答を受信し、
キー更新論理は、第１の回答に対応して新しいキーを発生し、
送信機は、新しいキーを含む第２の登録要求を送出し、
受信機は、ネットワークにアクセスするためにはキー更新が必要であることを示す、他の第１の回答を受信し、
送信機は、他の第１の回答の受信に対応して新しいキーを含む他の第２の登録要求を送出し、
受信機は、第２の登録要求に対応して第２の回答を受信し、なお第２の回答は新しいキーが受信されたことを示しており、
送信機は、新しいキーを用いて形成された第３の登録要求を送出し、そして
デバイスは、第３の登録要求に続いてネットワークへのアクセスを得る
ように配置されている、
を含むデバイス。

【請求項９】
さらに、送信機によって送出される信号上にデータを変調する変調ユニットおよび、受信機によって受信された信号からデータを復調する復調ユニットを含む、請求項８記載のデバイス。

【請求項１０】
ここで、送信機および受信機は一体化されたトランシーバーを含み、そしてここで変調ユニットおよび復調ユニットは一体化されたモデムを含む、請求項８記載のデバイス。

【請求項１１】
ここで、デバイスは移動電話、ラップトップ計算機、デスクトップ計算機、パーソナルディジタルアシスタント（ＰＤＡ）、データ端末、およびデータ収集デバイスを含むグループから選択される、請求項８記載のデバイス。

【請求項１２】
サーバであって、
データパケットを受信する受信機と、
データパケットを送信する送信機と、
移動インターネットプロトコル（移動ＩＰ）ネットワーク内の移動デバイスに関する認証、許可、課金処理を与えるための、認証、許可、および課金処理（ＡＡＡ）ユニットと、そして
キー更新ルーチンを制御するためのキー更新論理と、なおサーバは
受信機は、キーを用いて形成された第１の登録要求を受信し、なお第１の登録要求は移動ＩＰネットワークへのアクセスを要求しており、
送信機は、ネットワークにアクセスするためにはキー更新が必要であることを示す、第１の登録要求に対応した第１の回答を送出し、
送信機は、サーバがネットワークへのアクセスを許可するに先立って、他の第１の登録要求を受信する受信機に対応して他の第１の回答を再送出し、
受信機は、新しいキーを含む第２の登録要求を受信し、
送信機は、第２の登録要求に対応して第２の回答を送出し、なお第２の回答は新しいキーが受信されたことを示しており、
受信機は、新しいキーを用いて形成された第３の登録を受信し、そして
サーバは、第３の登録要求に対応して移動デバイスに対してネットワークへのアクセスを許可する
ように配置されている、
を含むサーバ。

【請求項１３】
サーバはさらに、サーバがネットワークへのアクセスを許可するに先立って、他の第２の登録要求を受信する受信機に対応して、送信機が他の第２の回答を再送出するように配置されている、請求項１２記載のサーバ。
【請求項１４】
サーバはさらに、送信機は第２の回答を送出する後に、新しいキーを含まない登録要求を受信する受信機に対応して、他の第１の回答を再送出するように配置されている、請求項１２記載のサーバ。
【請求項１５】
装置であって、移動デバイスに
ネットワークへのアクセスを要求するためにキーを用いて形成された第１の登録要求を送出し、
第１の登録要求に対応した第１の回答を受信するときは第２の登録要求を送出し、なお第１の回答はネットワークにアクセスするためにはキー更新が必要であることを示しており、なお第２の登録要求は新しいキーを含んでおり、
他の第１の回答を受信するときは他の第２の登録要求を再送出し、そして
第２の登録要求に対応した第２の回答を受信するときは、新しいキーを用いて形成された第３の登録要求を送出する、なお第２の回答は新しいキーが受信されたことを示しており、
ことを行わせるディジタル回路を含む装置。
【請求項１６】
ディジタル回路はさらに、移動デバイスに、定義された時間の総量内に第２の回答を受信していないことに対応して、第２の要求を再送出することを行わせる、請求項１５記載の装置。
【請求項１７】
ここで、装置は移動デバイス内で実行するステートマシンを含み、そしてここで第２の登録要求は新しいキーおよびトークンを含み、そしてここで第２の回答はトークンを含む、請求項１５記載の装置。
【請求項１８】
装置であって、サーバに
第１の登録要求に対応して第１の回答を送出し、なお第１の登録要求はキーを用いて形成されており、そして第１の回答はネットワークにアクセスするためにはキー更新が必要であることを示しており、
第２の登録要求に対応して第２の回答を送出し、なお第２の登録要求は新しいキーを含んでおり、そして第２の回答は新しいキーが受信されたことを示しており、
ネットワークアクセスを許可するのに先立って、他の第２の登録要求に対応した他の第２の回答を送出し、
第３の登録要求に対応してネットワークへのアクセスを許可する、なお第３の登録要求は新しいキーを用いて形成されており、
ことを行わせるディジタル回路を含む装置。
【請求項１９】
ディジタル回路はさらに、サーバに、ネットワークへのアクセスの許可に先立って他の第１の登録要求を受信するときは、他の第１の回答を再送出することを行わせる、請求項１８記載の装置。
【請求項２０】
ディジタル回路はさらに、サーバに、新しいキーを含まない登録要求を受信するときは、第２の回答を送出する後に他の第１の回答を再送出することを行わせる、請求項１８記載の装置。
【請求項２１】
ここで、装置はサーバ内で実行するステートマシンを含み、そしてここで第２の登録要

求は新しいキーおよびトークンを含み、そして第２の回答はトークンを含む、請求項１８記載の装置。

【請求項２２】

計算機が読み出し可能な媒体であって、移動デバイス内で実行される場合は移動デバイスに、

ネットワークへのアクセスを要求するために、キーを用いて形成された第１の登録要求を送出し、

第１の登録要求に対応した第１の回答を受信するときは第２の登録要求を送出し、なお第１の回答は、ネットワークにアクセスするためにはキー更新が必要であることを示しており、なお第２の登録要求は新しいキーを含んでおり、

他の第１の回答を受信するときは他の第２の登録要求を再送出し、そして

第２の登録要求に対応した第２の回答を受信するときは、新しいキーを用いて形成された第３の登録要求を送出する、なお第２の回答は新しいキーが受信されたことを示しており、

ことを行わせるプログラムコードを含む媒体。

【請求項２３】

さらに、移動デバイス内で実行される場合は、移動デバイスに、定義された時間の総量内に第２の回答を受信しないことに対応して、第２の要求を再送出することを行わせるプログラムコードを含む、請求項２２記載の計算機により読み出し可能な媒体。

【請求項２４】

ネットワークサーバ内で実行される場合はサーバに、

第１の登録要求に対応して第１の回答を送出し、なお第１の登録要求はキーを用いて形成されており、そして第１の回答はネットワークにアクセスするためにはキー更新が必要であることを示しており、

第２の登録要求に対応して第２の回答を送出し、なお第２の登録要求は新しいキーを含んでおり、そして第２の回答は新しいキーが受信されたことを示しており、

ネットワークアクセスの許可に先立って、他の第２の登録要求に対応した他の第２の回答を送出し、そして

第３の登録要求に対応してネットワークへのアクセスを許可する、なお第３の登録要求は新しいキーを用いて形成されており

ことを行わせるプログラムコードを含む、計算機が読み出し可能な媒体。

【請求項２５】

さらに、サーバ内で実行される場合はサーバに、ネットワークへのアクセスを許可するに先立って他の第１の登録要求を受信するときは、他の第１の回答を再送出することを行わせるプログラムコードを含む、請求項２４記載の計算機が読み出し可能な媒体。

【請求項２６】

さらに、サーバ内で実行される場合はサーバに、新しいキーを含まない登録要求を受信するときは、第２の回答を送出する後に他の第１の回答を再送出することを行わせるプログラムコードを含む、請求項２４記載の計算機が読み出し可能な媒体。

【請求項２７】

システムであって、

移動デバイスと、および

ネットワークサーバと、

ネットワークへのアクセスを要求するために、ネットワークサーバにキーを用いて形成された第１の登録要求を送出するように配置されている移動デバイスと、

キー更新状態に置かれるときは、第１の登録要求に対応した第１の回答を送出するよう配置されているネットワークサーバと、なお第１の回答はネットワークにアクセスするためにはキー更新が必要であることを示しており、

第１の回答を受信するときは更新キー状態に移行し、そして第１の回答に対応した第２の登録要求を送出するように、さらに配置されている移動デバイスと、なお第２の登録要

求は新しいキーを含んでおり、
第２の登録要求を受信するときは更新承認状態に移行し、そして第２の登録要求に対応した第２の回答を送出するように、さらに配置されているネットワークサーバと、なお第２の回答は新しいキーが受信されたことを示しており、
第２の回答を受信するときはキー有効状態に移行し、そして第２の回答に対応した第３の登録要求を送出するように、さらに配置されている移動デバイスと、なお第３の登録要求は新しいキーを用いて形成されており、そして
第３の登録要求を受信するときはキーＯＫ状態に移行し、そして第３の登録要求に対応して移動デバイスに対してネットワークへのアクセスを許可するように、さらに配置されているネットワークサーバと
を含むシステム。
【請求項２８】
さらに、移動デバイスからネットワークサーバへの要求を解釈しそして進め、そしてネットワークサーバから移動デバイスへの回答を解釈しそして進めるエージェントを含む、請求項２７記載のシステム。
【請求項２９】
装置であって、
ネットワークへのアクセスを要求するために、キーを用いて形成された第１の登録要求を送出するための手段と、
第１の登録要求に対応した第１の回答を受信するための手段と、なお第１の回答はネットワークにアクセスするためにはキー更新が必要であることを示しており、
第２の登録要求を送出するための手段と、なお第２の登録要求は新しいキーを含んでおり、
他の第１の回答の受信に対応して他の第２の登録要求を再送出するための手段と、
第２の登録要求に対応して第２の回答を受信するための手段と、なお第２の回答は新しいキーが受信されたことを示しており、
第３の登録要求を送出するための手段と、なお第３の登録要求は新しいキーを用いて形成されており、そして
第３の登録要求に続いて、ネットワークにアクセスするための手段と
を含む装置。
【請求項３０】
装置であって、
ネットワークへのアクセスを要求する第１の登録要求を受信するための手段と、なお第１の登録要求はキーを用いて形成されており、
第１の登録要求に対応した第１の回答を送出するための手段と、なお第１の回答はネットワークにアクセスするためにはキー更新が必要であることを示しており、
第２の登録要求を受信するための手段と、なお第２の登録要求は新しいキーを含んでおり、
第２の登録要求に対応した第２の回答を送出するための手段と、なお第２の回答は新しいキーが受信されたことを示しており、
他の第２の登録要求の受信に対応して他の第２の回答を送出するための手段と、
第３の登録要求を受信するための手段と、なお第３の登録要求は新しいキーを用いて形成されており、そして
第３の登録要求に対応してネットワークへのアクセスを許可するための手段と
を含む装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、移動無線ネットワークプロトコルをサポートするように配置された移動デバイス、および移動ネットワーク環境における移動デバイスに関する、認証(authenticatio

n)、許可(authorization)、および課金処理(accounting)（ＡＡＡ：authentication、authorization、and accounting）のために配置されたサーバに関する。

【背景技術】

【０００２】

通信ネットワークにおいて、ネットワークノードはネットワーク通信プロトコルを用いてデータを交換する。インターネットプロトコル（ＩＰ：Internet Protocol）は、ネットワークノード間のパケットデータ通信(packetized data communication)を容易にするネットワーク通信プロトコルの一例である。移動ＩＰは、パケットに基づいたネットワークにおいて移動計算デバイスの使用を容易にするプロトコルの一例である。換言すれば、移動ＩＰプロトコルはネットワーク内のノード移動を可能にする。移動ＩＰプロトコルを動かすことが可能な移動計算デバイスの例は、セルラ電話および衛星電話等の移動電話、ラップトップ計算機、パーソナルディジタルアシスタント（ＰＤＡ：personal digital assistant）、データ端末、データ収集デバイス、および他の計算デバイスである。

【０００３】

移動ＩＰは移動デバイスが、ウエブ拾い読み(web browsing)、Ｅメール、メッセージングあるいは類似のもの等の、パケットに基づいた通信応用と組み合わせられたパケットを送出し、そして受信することを可能とする。パケットに基づいたネットワークは典型的には、ネットワーク内のデバイスを識別するために、インターネットの場合におけるＩＰアドレス等のネットワークアドレスを使用する。データはこれらのＩＰアドレスに基づいてデバイスに対しておよび（デバイス）から発送される。しかしながら、移動デバイスはネットワーク内の異なった位置に移動することが可能である。この理由で移動ＩＰはパケットを、移動デバイスの現在の所属位置からトンネリング処理によって(via a tunneling process)再送されることを可能にしている。

【０００４】

移動ＩＰにおいては、移動デバイスはホームエージェント（ＨＡ：home agent）に割り当てられる。そしてそれは典型的には、移動デバイスのホームサブネットワーク上のルータ、あるいは他のエンティティである。移動デバイスがホームから離れる場合は、それ（移動デバイス）は外部エージェント（ＦＡ：foreign agent）を割り当てられることが可能である。外部エージェントは典型的には、移動デバイスが、訪問したサブネットワークに所属される場合はそれに対してルーティングサービスを与える、移動デバイスが訪問したサブネットワーク上のルータである。

【０００５】

移動デバイスのホームアドレスに送出された情報は、トンネリングとして参照される処理によって外部エージェントを経由して移動デバイスに再送されることが可能である。とくに、一度移動デバイスが外部エージェントを経由して登録されるときは、ホームエージェント（ＨＡ）はパケットを外部エージェントにトンネルする。ＦＡはそこでパケットを移動デバイスに配送することが可能である。とくに、ＦＡが移動デバイスから登録回答（ＲＲＰ：registration reply）を受信する場合は、ＲＲＰパケットのホームアドレスフィールドを読み出すことによってその発送テーブルを更新する。このように、ＨＡからＦＡにトンネルされたパケットは移動デバイスに正しく配送されることが可能である。さらに、外部エージェントは移動デバイスからネットワークに所属する他のデバイスにパケットを送出するための、省略時ルータ(default router)として動作することが可能である。

【０００６】

ＡＡＡサーバは認証、許可、および課金処理機能を実行するサーバ計算機として参照される。ＡＡＡサーバは典型的には、インターネットサービスプロバイダ（ＩＳＰ：Internet service provider）によって維持される。移動ＩＰにおいては、ＡＡＡサーバは移動デバイスがネットワークにアクセスすることを認証し、そして許可することが可能であり、そして請求目的のための課金処理情報を与えることが可能である。

【０００７】

ＩＳ‐８３５ネットワークにおいては、ネットワークにアクセスするために、移動デバ

イスは外部エージェント（ＦＡ）に対して、セキュリティキーを用いて形成されている登録要求（ＲＲＱ：registration request）を送出する。とくに、セキュリティキーは、移動デバイスのユーザを認証するために使用することが可能である。たとえば、移動デバイスは、パスワード認証プロトコル（ＰＡＰ：password authentication protocol）に従ってキーを送信することが可能であり、あるいは、不確実な(insecure)システムにおいてはキーを用いて形成されたオーセンティケータ値(authenticator value)を発生するかも知れない。たとえば、移動デバイスはセキュリティキーを用いたチャレンジハンドシェーク認証プロトコル（ＣＨＡＰ：challenge handshake authentication protocol）に対する応答を発生するかも知れない。

【０００８】

いずれの場合においても、移動デバイスがセキュリティキーを用いて形成されたＲＲＱを送出する後に、ＦＡはＲＲＱをアクセス要求（ＡＲＱ：access request）に変換し、そしてＡＲＱをＡＡＡサーバに送出する。ＦＡはそこでもしもＡＡＡがアクセスを許可する場合は、登録要求をＨＡに進める。パケットトンネリングはそこで、パケットをＨＡからＦＡに配送するために使用することが可能となり、そしてＦＡはパケットを移動デバイスに配送することが可能となる。

【０００９】

ある場合には移動デバイスのセキュリティキーを変更することが望まれるかも知れない。たとえば、もしも異端の(maverick)デバイスがキーへのアクセスを得た場合、その異端のデバイスは無許可のユーザとして、パケットに基づいたネットワークにアクセスすることが可能であるかも知れない。この開示においては、“異端のデバイス”は、他のデバイスのセキュリティキーを用いてネットワークにアクセスし、あるいはアクセスすることを試みるデバイスを参照する。もしも成功する場合、異端のデバイスは移動デバイスを装うことが可能であるかも知れない。なお悪い場合、異端のデバイスは他のユーザになりすましてインターネットにアクセスし、そしてサイバー犯罪、サイバーテロリズムあるいは類似のことを実行するためにセキュリティキーを使用するかも知れない。その結果、知られている異端の脅威に対応して、あるいは可能性のある異端の脅威に先んじそして妨害するために周期的な基準等によって、移動デバイスのセキュリティキーを変更することがしばしば望まれる。

【発明の開示】

【課題を解決するための手段】

【００１０】

本開示は、移動ＩＰネットワークにおける使用のためのセキュリティキー更新方式に向けられている。更新方式は、移動デバイスおよび移動デバイスを認証するサーバ計算機間のセキュリティキー更新を容易にするために実行することが可能である。この中に記述された技術は、更新ルーチン期間中の可能性のあるメッセージ損失、更新ルーチン期間中の移動デバイス故障、あるいは移動ネットワーク環境において典型的に遭遇する他の問題を考慮に入れるような方法で、セキュリティキー更新を容易にすることが可能である。とくに、更新方式におけるメッセージの受信あるいは非受信に応じて、１個あるいはそれ以上のメッセージの再伝送を行わせるためにステートマシンが実現可能である。このようにして、本技術はセキュリティキー更新のための強力な方式を与えることが可能であり、そしてネットワークセキュリティを改善することが可能である。

【００１１】

一つの実施例においては、本開示はネットワークへのアクセスのために第１の登録要求を受信することを含む方法を与える。なお、第１の登録要求はキーを用いて形成される。方法はさらに、第１の登録要求に応じた、ネットワークにアクセスするためにはキー更新が必要であることを示す第１の回答を送出すること、そして新しいキーを含む第２の登録要求を受信することを含む。方法はさらに、第２の登録要求に応じて新しいキーが受信されたことを示す第２の回答を送出し、そしてネットワークへのアクセスを許可するに先立って他の第２の登録要求を受信するときは、新しいキーが受信されたことを示す他の第２

の回答を再送出することを含む。方法はさらに、第３の登録要求を受信すること、なお第３の登録要求は新しいキーを用いて形成されており、そして第３の登録要求に対応してネットワークへのアクセスを許可することを含む。

【００１２】

他の実施例においては、本開示は、ネットワークへのアクセスを要求するためにキーを用いて形成された第１の登録要求を送出し、そしてネットワークへのアクセスのためにはキー更新が必要であることを示す、第１の回答を受信することを含む方法を与える。方法はさらに、第１の回答に対応して新しいキーを含む第２の登録要求を送出し、そしてネットワークにアクセスするためにはキー更新が必要であることを示す他の第１の回答を受信することを含む。方法はさらに、他の第１の回答の受信に対応して新しいキーを含む他の第２の登録要求を送出し、そして第２の登録要求に応じて、新しいキーが受信されたことを示す第２の回答を受信することを含む。方法はさらに、新しいキーを用いて形成された第３の登録要求を送出し、そして第３の登録要求に続いてネットワークにアクセスすることを含む。

【００１３】

この中に記述されたこれらのそして他の技術は、それぞれ移動デバイスあるいは移動デバイスに対してネットワークアクセスを与えるサーバによって実行することが可能である。いずれの場合においても、技術はハードウエア、ソフトウエア、ファームウエア、あるいはこれらの任意の組み合わせ内で実行することが可能である。種々の実施例が、移動デバイス、サーバ、あるいはこの中に記述された技術の一つを実行するための、デバイスあるいはサーバ等の部分を形成する回路に対して示されるかも知れない。若干のソフトウエア実施例に対しては技術は、実行される場合に１個あるいはそれ以上の技術を実行するプログラムコードを含む、計算機により読み出し可能な媒体上に具体化されるかも知れない。

【００１４】

種々の具体例に関するさらなる詳細は、付属されている図面および以下の記述の中に示されている。他の特徴、目的および利点は、記述および図面から、また請求項から明白となろう。

【発明を実施するための最良の形態】

【００１５】

一般的に、本開示は、移動ＩＰネットワークにおける使用のためのセキュリティキー更新方式を記述する。更新方式は、移動デバイスおよび、移動デバイスを認証するサーバ計算機間のセキュリティキー更新を容易にするために実行することが可能である。セキュリティキーは、パスワードに類似しているかも知れず、そしてパケットに基づいたネットワークにアクセスするための移動デバイスによる試行の期間中に、認証のために移動デバイスによって用いられることが可能である。しかしながら、種々のシナリオ(scenario)においては、知られているキーの乱用の脅威に対応して、あるいは可能性のある脅威に先んじそして妨害するために周期的な基準等によって、セキュリティキーを変更することは望ましいかも知れない。いずれの場合においても、この中に記述された技術は、更新ルーチン期間中の可能性のあるメッセージ損失、更新ルーチン期間中の移動デバイス故障、あるいは移動ネットワークセッティングにおいて典型的に遭遇する他の問題を考慮に入れた方法で、セキュリティキー更新を容易にすることが可能である。このようにして技術はセキュリティキー更新のための強力な方式を与えることが可能であり、そしてネットワークセキュリティを改善することが可能である。

【００１６】

図１は、移動ＩＰ等の、あるいは同様の移動ネットワーキングプロトコルをサポートするように配置された方式２を示すブロック線図である。とくに、方式２は、移動ネットワークプロトコルによってパケットに基づいたネットワーク１４にアクセスを得ることが可能な移動デバイス１０を含む。移動デバイス１０は、異なった地理的位置に移動されることのできる任意のデバイスであることが可能である。たとえば、移動デバイス１０は、ウ

インドウズ（Windows）（登録商標）、マッキントッシュ(Macintosh)、ユニックス(Unix)（登録商標）、あるいはリナックス(Linux)環境で動作する、デスクトップ、ラップトップ、あるいは可搬型計算機、パーム(Palm)、ウインドウズＣＥ、あるいは小型可搬デバイスのための同様なオペレーティングシステム環境に基づいたパーソナルディジタルアシスタント（ＰＤＡ）、あるいは移動電話、双方向(interactive television)テレビジョン、無線データ端末、無線データ収集デバイス、および同様の他の無線デバイスを含むことが可能である。

【００１７】

例として本開示に関する多くの詳細が、移動電話の形態において移動デバイス１０の環境に対して概説される。この場合、移動デバイス１０は、音声通信信号および、パケットに基づいたネットワーク１４を経由して伝達することが可能なデータパケットの両者を、通信するよう配置されるかも知れない。移動デバイス１０は、基地局４と無線信号１２を交換する。無線信号１２は、たとえば、符号分割多元接続（ＣＤＭＡ：code division multiple access）変調された信号、時間分割多元接続（ＴＤＭＡ：time division multiple access）変調された信号、周波数分割多元接続（ＦＤＭＡ：frequency division multiple access)変調された信号、あるいは２個あるいはそれ以上の変調技術の種々の組み合わせを含む、種々の変調技術の任意のものに従って変調された信号を含むことが可能である。

【００１８】

移動デバイス１０は、たとえば、（１）“デュアルモード広帯域スペクトル拡散セルラシステムのための、ＴＩＡ／ＥＩＡ－９５－Ｂ　移動局－基地局両立性標準”（ＩＳ－９５標準）、（２）“デュアルモード広帯域スペクトル拡散セルラ移動局のための、ＴＩＡ／ＥＩＡ－９８－Ｃ　推奨最小標準(Recommended Minimum Standard)”（ＩＳ－９８標準）、（３）“第３世代パートナーシッププロジェクト”（３ＧＰＰ）と命名されたコンソーシアムによって提案され、そして、文書番号３Ｇ　ＴＳ　２５．２１１、３Ｇ　ＴＳ　２５．２１２、３Ｇ　ＴＳ　２５．２１３、および３Ｇ　ＴＳ　２５．２１４を含む１式の文書に具体化された標準（Ｗ－ＣＤＭＡ標準）、（４）“第３世代パートナーシッププロジェクト２”（３ＧＰＰ２）と命名されたコンソーシアムによって提案され、そして、“ｃｄｍａ２０００スペクトル拡散システムのための、ＴＲ－４５．５　物理レイヤ標準、”“ｃｄｍａ２０００スペクトル拡散システムのための、Ｃ．Ｓ０００５－Ａ　上部レイヤ（レイヤ３）信号標準、”および“Ｃ．Ｓ００２４　ＣＤＭＡ２０００　高レートパケットデータエアインタフェース規格”（ＣＤＭＡ２０００標準）、（５）ＴＩＡ／ＥＩＡ－ＩＳ－８５６、“ＣＤＭＡ２０００　高レートパケットデータエアインタフェース規格”内に文書化された(documented)ＨＤＲシステム、および（６）若干の他の標準、等の１個あるいはそれ以上のＣＤＭＡ標準をサポートするように設計されるかも知れない。代わりに、あるいはさらに、移動１０デバイスはＧＳＭ規格あるいは関係規格、たとえばＤＣＳ１８００およびＰＣＳ１９００標準等の他の規格をサポートするように設計されるかも知れない。ＧＳＭシステムは、ＦＤＭＡおよびＴＤＭＡ変調技術の組み合わせを使用する。移動１０はまた他のＦＤＭＡおよびＴＤＭＡ標準をサポートするかも知れない。

【００１９】

あるいは信号１２は、ＩＥＥＥ　８０２．１１ｂ無線ネットワーキング標準に従ったデバイスによって典型的に実行されるバイナリ位相シフトキーイング（ＢＰＳＫ：binary phase shift keying）あるいは直交位相シフトキーイング（ＱＰＳＫ：quadrature phase shift keying）変調方式、あるいは、ＩＥＥＥ　８０２．１１ｇあるいはＩＥＥＥ　８０２．１１ａ無線ネットワーキング標準に従ったデバイスによって典型的に実行されるＯＦＤＭ変調方式等の、無線ネットワーキングに対して用いられる変調方式に従って変調されるかも知れない。また、信号１２は、ブルートゥーススペシャルインタレストグループ(Bluetooth Special Interest Group)によって定義された変調方式に従って変調されるかも知れない。しかしながら、これらの場合は（基地局４よりはむしろ）アクセスポイントが、移動デバイス１０からの信号を受信しそして進めるために用いられるであろう。

【００２０】
図１に示された例において、基地局４は移動デバイス１０から無線信号１２を受信しそして、時には基地トランシーバシステム（ＢＴＳ：base transceiver system）として参照される基地局制御器１８は信号を復調する。基地局制御器１８は、基地局４および公衆交換電話ネットワーク（ＰＳＴＮ：public switched telephone network）１３間に、電話呼が移動デバイス１０に向けておよび（これ）から発送されることができるように、インタフェースを与えることが可能である。さらに、基地局制御器１８は基地局４およびパケットに基づいたネットワーク１４に接続されたエージェント１８間に、パケットが移動デバイス１０に向けておよび（これ）から発送されることができるようにインタフェースを与えることが可能である。基地局制御器１８は、何れの復調された信号が音声データに対応し、そして何れの復調された信号がパケットに対応するかを識別することが可能であり、そしてデータをそれに応じて進めることが可能である。たとえば、もしも無線信号がデータ呼に対応する場合は、基地局制御器１８はデータをパケットに基づいたネットワーク１４のエージェントに進めることが可能である。

【００２１】
移動デバイス１０が移動電話ではない他の実施例においては、移動デバイス１０はパケットに基づいたネットワーク１４のエージェントに接続されたアクセスポイントと通信することが可能である。しかしながらこの場合、典型的には移動デバイス１０はＰＳＴＮ１３にアクセスしていないであろう。移動ＩＰネットワークに関するこれらのそして他の配置はまた、以下に記述される技術を実行することが可能である。若干の実施例においては、移動デバイス１０は、物理的伝送ラインたとえば臨時に結ばれた接続を経由してエージェントに丁度接続されるかも知れない。この場合、以下に記述される強力な更新方式が、伝送ライン上のデータ衝突に起因するであろう問題を避けるために用いられることが可能である。なおその他の実施例においては移動デバイス１０は、外部エージェントを用いることなしにネットワークに直接に接続されるかも知れない。

【００２２】
いずれの場合においてもパケットに基づいたネットワーク１４にアクセスを得るために、移動デバイス１０はＡＡＡサーバ２０からの許可を要求することが可能である。たとえば、インターネットサービスプロバイダ（ＩＳＰ）は、認証、許可、および課金処理機能を実行するために、ＡＡＡサーバ２０を維持することが可能である。換言すれば、移動ＩＰ環境においてはＡＡＡサーバ２０は、移動デバイス１０がネットワーク１４にアクセスすることを認証しそして許可することが可能であり、そして移動デバイス１０のユーザが、それに応じてＩＳＰによって請求されることが可能であるように、移動デバイス１０のエアタイムの利用(air time usage)に関する課金処理を与えることが可能である。

【００２３】
移動ＩＰプロトコルをサポートするシステム２において、移動デバイス１０はホームサブネットワーク上にＩＰアドレスを有することが可能である。このホームＩＰアドレスは、ＩＰアドレスが固定ホストに割り当てられるのと同様な方法で処理されることが可能である。ホームＩＰアドレスはパケットをホームエージェント（ＨＡ）２２に送るために用いられる。そしてそれは、典型的には移動デバイス１０に関するホームサブネットワーク上のルータである。さらに、ホームエージェント２２は、それ（移動デバイス）がホームから離れている場合は、移動デバイス１０への配送のためにパケットをトンネルすることが可能であり、そして移動デバイス１０に対する現在の位置情報を維持することが可能である。

【００２４】
そのホームサブネットワークから離れている場合は、移動デバイス１０は外部エージェント（ＦＡ）１８を割り当てられるかも知れない。ＩＳ‐８３５‐Ａネットワークにおいては、外部エージェント１８はパケットデータサービスノード（ＰＤＳＮ）として参照され、そして典型的には移動デバイス１０に発送サービスを与える訪問時サブネットワーク(visited sub-network)上のルータである。ＩＳ‐８３５‐ＡネットワークにおいてはＰ

ＤＳＮはまた、外部エージェントとして動作することに加えてさらなる機能を有することが可能である。いずれの場合においても、外部エージェント１８は、ホームエージェント２２によってネットワーク１４の向こうにトンネルされた、移動デバイス１０に対するパケットを配送することが可能である。移動デバイス１０によって送出されたパケットに対して外部エージェント１８は、ネットワーク１４に付属された(attached)他のデバイスに対してパケットを送出するための、省略時ルータとして動作することが可能である。

【００２５】

上に言及したように、パケットに基づいたネットワーク１４にアクセスを得るために、移動デバイス１０はサービスプロバイダからの許可を要求することが可能である。たとえば、許可はセキュリティキー（以後キーという）を用いて達成されることが可能である。たとえば移動デバイス１０は、パスワード認証プロトコル（ＰＡＰ：password authentication protocol）に従って登録要求と共にキーを送信するかも知れず、あるいは、不確実なシステムにおいては、キーを用いて形成されたオーセンティケータ値を発生するかも知れない。たとえば、移動デバイスはセキュリティキーを用いて、チャレンジハンドシェーク認証プロトコル（ＣＨＡＰ）に対する応答を発生するかも知れない。応答はそこで移動デバイス１０のユーザを確認するために、ＡＡＡサーバ２０によって確認されることが可能である。これらのあるいは他の方法において、移動デバイス１０はそのセキュリティキーを用いて認証を要求することが可能である。キーは移動デバイス１０のユーザが、ＡＡＡサーバ２０と組み合わせられたサービスプロバイダの、許可された加入者であることを認証するパスワードに類似している。

【００２６】

許可されたキーを用いて形成された登録要求を移動デバイス１０から受信する場合、ＡＡＡサーバ２０は、移動デバイス１０がパケットに基づいたネットワーク１４の中の種々の計算機に蓄えられた資源および情報にアクセスすることを可能とする。課金処理の目的のために、ＡＡＡサーバ２０はまた、その期間中に移動デバイス１０がパケットに基づいたネットワーク１４にアクセスしているエアタイム利用を記録するかも知れない。たとえば、パケットに基づいたネットワーク１４は、インターネット等の世界に亙るネットワークを含むかも知れず、あるいはより小さい公的あるいは私的ネットワークを含むかも知れない。

【００２７】

ある例においては、移動デバイス１０のためのセキュリティキーを変更することが望ましいかも知れない。たとえば、もしも異端のデバイスがキーに対してアクセスを得る場合、異端のデバイスは許可されていないユーザとしてパケットに基づいたネットワーク１４にアクセスすることが可能であるかも知れない。再び、用語“異端のデバイス”は他のデバイスのキーを用いてネットワーク１４にアクセスしあるいはアクセスを試みるデバイスとして参照される。もしも成功する場合は、異端のデバイスは移動デバイス１０からエアタイムを盗み、あるいはサービスプロバイダからエアタイムを盗むことが可能となるかも知れない。さらに、異端のデバイスは、他のユーザを装ってネットワーク１４にアクセスするためにキーを用いるかも知れず、そしてサイバー犯罪あるいはサイバーテロリズムを実行するかも知れない。これらの、そして他の理由のために、知られている異端の脅威に対応して、あるいは可能性のある異端の脅威に先んじそして妨害するために周期的な基準で、移動デバイス１０のキーを変更することが望まれるかも知れない。

【００２８】

図２は、外部エージェント（ＦＡ）１８を経由しての、移動１０およびＡＡＡサーバ２０間の通信を示すメッセージフロー線図である。通信は実際には基地局１８（図１）あるいは無線ネットワークアクセスポイント等の種々の他のデバイスを経由して送出されるかも知れない。いずれの場合においても図２はセキュリティキーの更新に対して改善された方式を示している。

【００２９】

キー更新処理は一連の事象を含むことが可能であり、そしてそこで移動デバイス１０お

よびＡＡＡサーバ２０は、事象に対応して種々の状態を経由移行する。もしも一つの事象すなわち送信された要求あるいは送信された回答が伝送期間中に見逃されあるいは失われる場合は、移動デバイス１０あるいはＡＡＡサーバ２０は、事象のすべてが発生することを保証するためにそれに対応して応答することが可能である。このようにして移動デバイス１０およびＡＡＡサーバ２０は互いに同期外れとならないことを保証することが可能である。換言すれば、移動デバイス１０およびＡＡＡサーバ２０は、保管されたセキュリティキーが整合しないシナリオを避けることが可能である。

【００３０】

一つの実施例においては、移動デバイス１０はキー更新処理の期間中２個の可能な状態の間を移行することが可能であり、そしてＡＡＡサーバ２０は３個の可能な状態の間を移行することが可能である。このようにして、キーの更新は更新の承認と同様に、移動デバイス１０およびＡＡＡサーバ２０がともに新しいキーをメモリに引き渡し、そして、ネットワーク１４にアクセスするために移動デバイス１０による使用のための新しいキーを承認する以前に必要とされるかも知れない。図２に示された技術は、更新処理の期間中に１個あるいはそれ以上の通信が失われる場合の問題の回避を含むいくつかの利点を得ることが可能である。さらに、この技術は移動デバイス１０、ＡＡＡサーバ２０、およびＦＡ１８を修正することによって実行することが可能である。換言すれば、この技術はシステム２の他のデバイスに対して影響が少ない(transparent)かも知れない。移動デバイス１０およびＡＡＡサーバ２０はそれぞれのステートマシンを含むように修正することが可能であり、そしてＦＡ１８はキー更新ルーチン期間中にアクセス拒否（ＡＲ）を受信する場合に、呼を終了しないことを保証するように修正することが可能である。

【００３１】

図２に示すように移動デバイス１０は最初は“キー有効(key valid)”状態（２５に示したように）にあることが可能である。キー有効状態においては、移動デバイス１０はネットワーク１４にアクセスする場合に用いられるべきセキュリティキーをメモリ内に保管して有している。移動デバイス１０は、登録要求（Ａ）を送出することによって移動ＩＰセションを確立することを試みる。登録要求はこの中では“ＲＲＱ”として略記される。外部エージェント１８はＲＲＱ（Ａ）を受信し、そして、当業界において既知のＲＡＤＩＵＳ（remote authentication dial-in user service）クライアント／サーバプロトコルに従う等により、アクセス要求（１）を送出する。アクセス要求はこの中では“ＡＲＱ”として略記される。ＡＲＱ（１）は、移動デバイス１０を確認するためにＡＡＡサーバ２０によって受信される。

【００３２】

通常の場合ＡＡＡサーバは、もしも正しい場合は認証情報を受領することが可能であり、そしてアクセス受け入れ（ＡＡ：access accept）メッセージで応答することが可能である。しかしながら図２の線図においてＡＡＡサーバ２０は最初は“キー更新(update key)”の状態にある（２６に示されるように）。この場合、ＡＲＱを確認するよりはむしろＡＡＡサーバ２０は、移動デバイス１０はそのキーを更新すべきであることを示すアクセス拒否（２）形式の回答をもって応答する。アクセス拒否はこの中では“ＡＲ”として略記される。外部エージェント１８はＡＲ（２）を受信し、そして移動１０にそのキーを更新することを命令するために登録回答（Ｂ）を送出する。登録回答はこの中では“ＲＲＰ”として略記される。

【００３３】

ＡＡＡサーバ２０は種々の刺激あるいは事象の何れかによってキー更新状態の中に置かれることが可能である。たとえば、サービスプロバイダはＡＡＡサーバ２０を移動ユーザの要求に対応して、あるいは既知のセキュリティの違反に対応してキー更新状態の中に置くかも知れない。あるいはＡＡＡサーバ２０は、何らかの可能性のあるセキュリティ違反を妨害するために周期的にキー更新状態に入るかも知れない。いずれの場合においても一度ＡＡＡサーバ２０がキー更新状態に置かれれば、それ（サーバ）が移動１０からのＲＲＱに対応するＡＲＱを受信する場合は、それはキー更新ルーチンを開始するであろう。

【００３４】
一度移動デバイス１０がそのキーを更新すべきであることを示すＲＲＰ（Ｂ）を受信するときは、移動デバイス１０は（２７に示されるように）キー更新状態に入る。キー更新状態においては、移動デバイス１０は新しいキーおよびトークン(token)を発生する。たとえば、移動デバイス１０は、与えられた瞬間における受信された電磁的エネルギーの総量を計算し、そして与えられた瞬間における受信された電磁的エネルギーのランダムな総量に基づいて乱数を発生するハードウエアをもととしたエネルギー計算器等の乱数発生器を含むことが可能である。トークンは同様な方法で発生することが可能であり、そしてＡＡＡサーバ２０による新しいキーのその後の受領を確認するために使用されるであろう別々の数に対応する。しかしながら、トークンの発生および交換はこのような確認を達成するただ一つの典型的な方法である。若干の実施例においては、移動デバイス１０は、移動‐ＡＡＡキー、移動‐ＨＡキー、ＣＨＡＰキー、あるいは他の認証キーを含むいくつかのキーを発生しそして／あるいは送信することが可能である。

【００３５】
移動デバイス１０はそこで新しいキー（あるいは複数の新しいキー）およびトークンを含むＲＲＱ（Ｃ）を送出する。外部エージェント１８はＲＲＱ（Ｃ）を受信し、そして新しいキーおよびトークンを含むＡＲＱ（３）をＡＡＡサーバ２０に送出する。新しいキーおよびトークンは外部のホスト、あるいは若干の他の外部の手段により可能性のある盗聴に対して、保護されることが可能である。たとえば、新しく発生されたキーは、移動デバイス１０およびＡＡＡサーバ２０に対してのみ知られた別々の暗号化キーを用いて暗号化されるかも知れない。

【００３６】
たとえば、外部エージェント１８は、移動デバイス１０によって用いられるＲＲＱフォーマットの到来要求を、ＡＡＡサーバによって用いられるＡＲＱフォーマットの発出要求(outgoing request)に変換し、あるいはＡＲフォーマットの到来回答を、ＲＲＰフォーマットの発出回答に変換するための、ルックアップテーブルを含むことが可能である。しかしながら、要求および回答内に含まれる情報は、一般的に外部エージェント１８が要求あるいは回答を一つのフォーマットから他に変換する場合は変更されない。従って、もしもＲＲＱ（Ｃ）が新しいキーおよびトークンを含む場合はＡＲＱ（３）は同様に新しいキーおよびトークンを含む。

【００３７】
ＡＲＱ（３）を受信するときは、ＡＡＡサーバ２０は新しいキーをメモリ内に保管し、そして（２８に示されるように）更新承認(update acknowledge)状態に移行する。ＡＡＡサーバ２０はそこでメッセージを復号し、そしてＡＲ（４）を用いて、ＡＡＡサーバ２０が移動デバイス１０に対して認証するトークンを移動１０に返送する応答を行う。これは移動デバイス１０に対して、それ（デバイス）が正しいＡＡＡサーバと通信していることを立証しそして、移動デバイス１０に対して、ＡＡＡサーバ２０に対して送信された新しいキーが受信（受領）されたことを示している。外部エージェント１８は、ＡＲ（４）を受信しそして、トークンを移動デバイス１０に戻すために ＲＲＰ（Ｄ）を送出する。しかしながら他の実施例においては、トークンの発生および交換は、ＡＡＡサーバ２０に対して送信された新しいキーが受信されたことを移動デバイス１０に示すための、他の技術によって削除することが可能である。

【００３８】
トークンとともにＲＲＰ（Ｄ）を受信するときは、もしもさきにＲＲＱ（Ｃ）内に送出されたものとトークンが整合する場合は、移動デバイス１０は（２９に示されたように）キー有効状態に戻ることが可能である。移動デバイス１０はそこでその新しいキーを用いて形成された通常の登録要求ＲＲＱ（Ｅ）を作成する。さらに、新しいキーを用いて形成された通常の登録要求は、キーを送信すること、キーを用いて発生された許可値を送信すること、ＣＨＡＰチャレンジに応答すること、あるいは同様なことを含むかも知れない。

【００３９】

いずれの場合においても、外部エージェント１８はＲＲＱ（Ｅ）を受信し、そしてＡＡＡサーバ２０にＡＲ（５）を送出する。一度ＡＡＡサーバ２０が新しいキーを用いて発生された要求に対応するＡＲ（５）を受信するときは、ＡＡＡサーバ２０は（３０に示されるように）キーＯＫ状態に移行し、保管された新しいキーを永久メモリに引き渡し、そしてアクセス受け入れ（ＡＡ）を用いて外部エージェント１８に回答する。外部エージェント１８はそこでホームエージェント２２と通信することを許可されることが可能である。

【００４０】

移動ＩＰプロトコルの一部として外部エージェント１８は、ＲＲＱをホームエージェント２２に進める。移動‐ＨＡ認証の一部としてＨＡ２２はＡＲＱをＡＡＡサーバ２０に送出する。ＡＡＡサーバ２０はＡＡをＨＡ２２に移動‐ＨＡキーとともに送出する。そしてそれはまた移動デバイス１０によって発生され、 上に概説したように、新しいキーおよびトークンの伝送とともにＡＡＡサーバ２０に送信される。ＨＡ２２は移動‐ＨＡキーを用いて、移動‐ホーム認証延長を確認する。ホームエージェントはそこでＲＲＰを外部エージェントに送出することが可能となり、そしてそれは順にＲＲＰを移動デバイス１０に送出することを可能とする。このようにして、一度移動デバイス１０のキーが更新され、そしてそこでＡＡＡサーバ２０によって確認されれば、データはホームエージェント２２および外部エージェント１８間のトンネリングによって移動デバイス１０に送られることが可能である。

【００４１】

図２の線図内に示されたキー更新ルーチンは、もしも更新処理期間中に１個あるいはそれ以上の通信が失われる場合に、問題の回避を含むいくつかの利点を得ることが可能である。とくに、ＡＡＡサーバ２０内における少なくとも３個の別々な状態、および移動デバイス１０内における少なくとも２個の別々な状態の使用は、システムが更新ルーチン期間中に可能性のあるメッセージ損失を処理しうることを保証することが可能である。その場合、もしもＡＡＡサーバが、更新ルーチンに関する一連の定義されたＡＲＱ内の次のＡＲＱを予期しており、しかし異なったＡＲＱを受信する場合は、ＡＡＡサーバ２０は移動１０およびＡＡＡサーバ２０が同じキーを有することを保証するために、先に送信されたＡＲを再送出することによって応答することが可能である。したがって、移動デバイス１０上のキーは、ＡＡＡサーバ２０上に保管されたキーと同期外れになることはないであろう。キー同期の喪失は、移動デバイス１０を、確認の失敗によって局部ネットワークにアクセス不能とすることが可能である。

【００４２】

さらに、図２の線図内に示された技術はキー更新ルーチン期間中における、移動デバイス１０の電力事故と組み合わせられた問題を回避することが可能である。また、エアリンクの損失、リセット、通話事故(call failure)、あるいは更新ルーチン期間中に発生する他の中断等の事象の場合に、問題を回避することが可能である。これらの場合に、移動デバイス１０およびＡＡＡサーバ２０は同期外れになることを避けることが可能であり、そしてＡＡＡサーバ２０は遷移的な状態に固定されることを避けることが可能である。代わりに、キー更新ルーチンは、先に送出され、しかし受信されあるいは確認されなかった１個あるいはそれ以上の通信を再送出することによって、継続することが可能である。重要なことは、一度ＡＡＡサーバ２０が新しいキーを受信するときは、それ（サーバ）は新しいキーが受信されたことを移動デバイス１０に通信するのに十分なトークン回答あるいは他の回答をもって回答する。そこで、ＡＡＡサーバ２０は、それが新しいキーを用いて送出されたＲＲＱに対応するＡＲＱを受信するまではキーＯＫ状態への移行はしない。したがって、キー更新ルーチンは更新方式の各事象が発生するまでは終了しないことが可能である。

【００４３】

図２に示された技術はまた、そうでない場合は、一度その通信はすでに受信された１個あるいはそれ以上の通信の再伝送、あるいはＡＡＡサーバ２０から移動デバイス１０へのサービス通信の否定等の更新ルーチン期間中の他の通信の伝送の原因となるであろう、問

題の取り扱いを容易にすることが可能である。これらの場合キー更新ルーチンは、ある事象が発生していないであろうことから終了されないであろう。さらに、この技術の他の利点は、移動デバイス１０およびＡＡＡサーバ２０をそれぞれのステートマシンで修正することによって、そしてＦＡ１８を、キー更新ルーチンの期間中ＦＡ１８がＡＲを受信する場合は、呼が終了されないことを保証するように修正することによって、それらが実行されうることである。換言すれば、この技術を実現するために必要とされる修正は、システム２の他のデバイスに対して影響が少ないことである。

【００４４】

図３は、この中に記述されたようにキー更新ルーチンの実行のために配置された移動デバイス１０に関する典型的なブロック線図である。この例においては、移動デバイス１０はアンテナ３２、ＲＦ受信機／送信機３３、モデム（変調‐復調ユニット）３４、移動ＩＰ制御ユニット３５、メモリ３６、キー更新論理３８、および新しいキーの発生器(new key generator)３９を含む種々のコンポーネントを含む。

【００４５】

ＲＦ受信機／送信機３３は、使用された変調方式に従って変調された電磁的信号を、アンテナ３２を経由して送信しそして受信する。ＲＦ受信機／送信機３３はまた、到来信号に関するアナログ‐ディジタル変換、および発出信号に関するディジタル‐アナログ変換を実行するかも知れない。 ＲＦ受信機／送信機３３は別々の受信機および送信機コンポーネントを含むかも知れずあるいは、一体化されたユニットすなわちトランシーバを含むかも知れない。モデム３４は発出信号の変調および到来信号の復調を実行するディジタル処理装置を含むかも知れない。

【００４６】

移動ＩＰ制御ユニット３５は移動ＩＰプロトコルにおける通信の伝送および受信を制御する。たとえば、登録ルーチンの期間中移動ＩＰ制御ユニット３５は発出ＲＲＱを発生するかも知れず、そして到来ＲＲＰを解釈するかも知れない。さらに、移動ＩＰ制御ユニット３５は、移動デバイス１０の同一性を確認するためのオーセンティケータを発生するために、セキュリティキーを用いるかも知れない。移動ＩＰ制御ユニット３５は、登録処理の期間中用いるためのセキュリティキーを得るためにメモリ３６にアクセスするかも知れない。さらに、移動ＩＰ制御ユニット３５は、移動デバイス１０がキー更新状態に入っているか否かを識別するためにキー更新論理３８にアクセスするかも知れない。

【００４７】

キー更新論理３８は、セキュリティキー更新ルーチンの期間中に移動デバイス１０の状態を移行させるための状態論理を含むかも知れない。特に、もしも移動ＩＰ制御ユニット３５が到来ＲＲＰをＡＡＡサーバからのキー更新メッセージとして理解する場合は、キー更新論理３８は移動デバイス１０をキー更新状態に移行させる。キー更新状態においては、移動ＩＰ制御ユニット３５は、ＡＡＡサーバ２０に送信すべき新しいキーを発生するために新しいキーの発生器３９を呼び出すかも知れない。一つの例においては、新しいキーの発生器３９は、少なくとも２個の新しい数：１）新しいキーおよび、２）トークンを発生することが可能である。移動デバイス１０はそこで、新しいキーおよびトークンとともにＲＲＱを通過させることが可能となり、トークンを含むＲＲＰの形態で承認を受信するまでは、キー更新状態にとどまることが可能である。若干の実施例においては、移動デバイスは移動‐ＡＡＡキー、移動‐ＨＡキー、ＣＨＡＰ‐キー等のいくつかのキーを発生しそして／あるいは送信するかも知れない。キーの若干あるいはすべては新しく発生されたキーであるかも知れず、あるいは若干のキーは前に保管されたものであるかも知れず、そして他のキーは新しく発生されるものであるかも知れない。他の場合においては、トークンの発生および交換は若干の他の承認技術によって回避することが可能である。

【００４８】

新しいキーの発生器３９は、ランダムなあるいは擬似ランダムな数値を発生することが可能な何らかの回路を含むことが可能である。一つの例においては、前に言及したように、新しいキーの発生器３９は、与えられた瞬間におけるアンテナ３２によって受信された

電磁的エネルギー総量を計算し、そして与えられた瞬間における受信された電磁的エネルギーのランダムな総量に基づいて乱数を発生する、ハードウエアに基づいたエネルギー計算器を含む。トークンは同様な方法で発生することが可能である。もしも必要とされる場合は、移動ＩＰ制御ユニット３５はまた、移動デバイス１０およびＡＡＡサーバ２０に対してのみ知られた暗号化キーを用いることによって等で、伝送に先立ってセキュリティキーおよびトークンを暗号化することが可能である。いずれの場合も新しく発生されたキーおよびトークンは後の使用のためにメモリ３６内に保管することが可能である。

【００４９】

キー更新状態に入るときは、移動デバイス１０はそれがトークン回答を受信するまでキー更新状態にとどまることが可能である。したがって、キー更新状態に移行した後に、もしも移動デバイス１０が割り当てられた量の時間内にトークン回答を受信しない場合は、それはトークンとともに同じキーを再送信し、そしてもしも移動デバイス１０がキー更新要求を受信する場合は、それは新しく発生されたキーおよびトークンを再送信し、そして他の通信を無視する。いずれの場合も、図３の配置は移動デバイス１０が、通信が失われあるいはそうでなければ受信されないというシナリオで処理することを可能とする。これらの場合に、移動デバイス１０がネットワーク１４（図１）にアクセスを得るために新しいキーの使用を試みる前に、移動デバイス１０およびＡＡＡサーバ２０が同期状態を維持するための通常の事象が起きていることを保証するために、移動デバイス１０は単にキー更新ルーチンの１個あるいはそれ以上のステップを繰り返すことが可能である。

【００５０】

図４は、この中に記述されたようなキー更新ルーチンの実行のために配置されたＡＡＡサーバ２０に関する典型的なブロック線図である。この例においては、ＡＡＡサーバ２０は受信機／送信機４２、ＡＡＡ制御ユニット４４、メモリ４６、およびキー更新論理４８を含む種々のコンポーネントを含む。

【００５１】

受信機／送信機４２は、インターネットプロトコル（ＩＰ）および移動インターネットプロトコル（移動ＩＰ）に従って信号４５を送信しそして受信する。とくに、受信機／送信機４２は、アクセス要求（ＡＲＱ）の形態の信号を受信し、そしてアクセス拒否（ＡＲ）あるいはアクセス受け入れ（ＡＡ）の形態の信号を送信する。受信機／送信機４２は、別々の受信機および送信機コンポーネントを含むかも知れず、あるいは一体化されたユニットすなわちトランシーバを含むかも知れない。本開示はこの点で限定される必要はないけれども、受信機／送信機４２は、ディジタル領域内で動作するかも知れない。

【００５２】

ＡＡＡ制御ユニット４４は、ハードウエアあるいは処理装置によって実行されるソフトウエアモジュールを含むかも知れない。いずれの場合においても、ＡＡＡ制御ユニット４４は、認証、許可、および課金処理サービスを実行するように配置されることが可能である。メモリ４６は、これによってＡＡＡサーバ２０がネットワークアクセスを認めることが可能となっている、セキュリティキーおよび組み合わせられたユーザあるいはデバイスのリストを保管することが可能である。ＡＡＡサーバ２０によってサポートされるネットワークデバイスが、それぞれのセキュリティキーを用いて形成された登録要求を送信することによって等で、ネットワークアクセスを要求する場合、ＡＡＡサーバ２０は、メモリ４６に保管された対応する加入者キーに基づいて、要求しているデバイスに対してアクセスを認証しあるいは拒否する。さらに、認証処理は、登録要求とともにキーを伝送すること、あるいは登録要求とともにキーを用いて発生された認証値を伝送することを含むかも知れない。たとえば、ＡＡＡサーバ２０は、いずれの移動デバイス１０が認証されるためにキーを用いて応答しなければならないかのために、チャレンジハンドシェーク認証プロトコル（ＣＨＡＰ）を呼び出すかも知れない。いずれの場合も、もしも要求しているデバイスが固有のキーを用いて形成された登録要求を送信する場合は、ＡＡＡサーバ２０は要求しているデバイスに対してネットワークアクセスを許可することが可能である。

【００５３】

キー更新論理４８は、ＡＡＡサーバ２０がこの中に記述されたキー更新ルーチンを実行することを開始するように配置された、ステートマシンを含むことが可能である。。キー更新論理４８は、ＡＡＡサーバ２０に対して、キー更新に関して少なくとも３個の可能な状態：１）キーＯＫ、２）キー更新、および３）更新承認、を定義することが可能である。通常の動作の期間中キー更新論理は、キーＯＫ状態を識別することが可能であり、そしてこの場合ＡＡＡサーバ２０はネットワークへのアクセスを要求しているデバイスからの要求を受信し、そして要求しているデバイスのユーザを立証するために認証を実行する。

【００５４】

ある例においては、キー更新論理４８は、外部入力に応じてあるいは周期的な基準（時刻を見計らって）等で、キー更新状態に置かれることが可能である。キー更新状態は、ＡＡＡサーバ２０によって認証されるべき１個のそれぞれのデバイスに対して特定であるかも知れず、あるいはＡＡＡサーバ２０によって認証されるべきデバイスの、若干あるいはすべてはそれらのキーを更新しなければならないというように、より一般的であるかも知れない。いずれの場合においても、ネットワークアクセスを要求するかも知れない任意の与えられたデバイスに関して、ＡＡＡサーバがキー更新状態に置かれる場合、この中に記述されるようにそのデバイスに対してキー更新ルーチンを開始するであろう。

【００５５】

とくに、ＡＡＡサーバ２０がキー更新状態に置かれる場合、それは与えられたデバイスからの登録要求に対応してＡＲ（キー更新）回答を送出するであろう。たとえば、もしもＡＡＡサーバ２０が移動デバイス１０に対するネットワークアクセスを要求するＡＲＱとして受信する場合は、ＡＡＡサーバは、移動デバイス１０はそのキーを更新しなければならないことを示すＡＲ（キー更新）回答を返信する。そこでＡＡＡサーバ２０は移動デバイス１０からの、新しいキーおよびトークンを含むＡＲＱを受信することを予期する。もしもＡＡＡサーバ２０がＡＲＱ（新しいキー、トークン）要求を受信する場合は、ＡＡＡ制御ユニット４４は、新しいキーをメモリ４６に保管し、そしてキー更新論理はＡＡＡサーバ２０を更新承認状態に移行させる。　ＡＡＡサーバ２０はそこで移動デバイス１０にトークンを返送しそしてそれによって移動デバイス１０に、ＡＡＡサーバ２０は新しいキーを受信したことを示すために、ＡＲ（トークン）回答を送出する。しかしながら、さらにこの開示の原理に従って、移動デバイス１０にＡＡＡサーバ２０は新しいキーを受信したことを示すために、他の技術（トークンの交換以外の）が使用されるかも知れない。

【００５６】

ＡＡＡサーバ２０は、それが移動デバイス１０によって送出され、そして新しいキーを用いて形成されたＲＲＱに対応する他のＡＲＱを受信するまでは、キーＯＫ状態には復帰しない。この点で、ＡＡＡサーバ２０および移動デバイス１０は新しいキーに関して同期状態にあり、そしてキー更新ルーチン内の通信は失われなかったことが知られる。このように、ＡＡＡサーバ２０は、新しいキーを用いて移動デバイス１０によって送出されたＲＲＱに対応するその後のＡＲＱを、移動デバイス１０からの、それがＡＡＡサーバのトークン回答を受信したとの受領通知として、そしてまたネットワークへのアクセスに対する要求の両者として処理する。したがって、ＡＡＡサーバ２０が、新しいキーを用いて移動デバイス１０によって送出されたＲＲＱに対応するＡＲＱを受信する場合は、キー更新論理４８は、キーＯＫ状態に移行し、そしてＡＡＡ制御ユニットは移動デバイス１０の認証を実行する。

【００５７】

図５は、移動デバイス１０の視点からのセキュリティキー更新ルーチンの実施例を示すフロー線図である。図５に示されるように、送信機／受信機３３は、登録要求（ＲＲＱ）を送信する（５１）。たとえば、移動ＩＰ制御ユニット３５はその現在のキーを用いてＲＲＱを発生することが可能であり、そしてモデム３４は、ＲＲＱを変調しそして変調されたディジタル信号を、アンテナ３２を経由して送信機／受信機３３によって送出されるべきアナログＲＦ信号に変換することが可能である。通常の動作の期間中移動デバイス１０はキー更新回答を受信しないであろう（５２の“いいえ”ブランチ）。代わりに、通常の

動作の期間中移動デバイス１０は、要求を受け入れることあるいは要求を拒否することの何れかの回答を受信するであろう。もしも移動デバイス１０がＡＡＡサーバ２０から許可を受信する場合は（５３の“はい”ブランチ）、そこで移動デバイス１０は、移動デバイス１０がパケットに基づいたネットワーク１４上に通信することを可能とする、パケットに基づいたネットワーク１４（図１）にアクセスを得ることが可能である（５４）。他方、もしも移動デバイス１０がＡＡＡサーバ２０から拒否を受信する場合は（５３の“いいえ”ブランチ）、そこで移動デバイス１０は他の登録要求を送信することによって登録を試みることが可能である（５１）。

【００５８】

しかしながら、もしもＡＡＡサーバ２０がキー更新状態にある場合は、そこで移動デバイス１０はその登録要求に対応してキー更新回答を受信することが可能である（５２の“はい”ブランチ）。この場合には、キー更新論理３８は移動デバイス１０をキー更新状態に移行させ、そして新しいキーの発生器３９は、新しいキーおよびトークンを発生する（５５）。移動デバイスはそこで新しいキーおよびトークンとともに登録要求を送出する（５６）。たとえば、移動ＩＰ制御ユニット３５は新しく発生されたキー、および新しく発生されたトークンを用いてＲＲＱ（新しいキー、トークン）を発生することが可能であり、そしてモデム３４は、ＲＲＱ（新しいキー、トークン）を変調し、そして変調されたディジタル信号を、アンテナ３２を経由して送信機／受信機３３によって送出されるべき、アナログＲＦ信号に変換することが可能である。もしも移動デバイス１０がキー更新状態５５に移行した後にリセットされる場合は、それはまた、このようなリセットに続いてＲＲＱ（新しいキー、トークン）を送信することが可能である（５６）。

【００５９】

ＲＲＱ（新しいキー、トークン）に対応して、もしも移動デバイス１０がトークン回答ＲＲＰ（トークン）を受信する場合は（５７の“はい”ブランチ）、そこで移動デバイス１０は、ＡＡＡサーバ２０が新しいキーを受信したことを知る。この場合は、キー更新論理３８は、移動デバイス１０をキー有効状態に戻し（５８）、そして移動デバイス１０は、新しいキーに対応する現在のキーを用いて形成された通常の登録要求を送信する（５１）。もしも移動デバイス１０がＡＡＡサーバ２０から許可を受信する場合は（５３の“はい”ブランチ）、そこで移動デバイス１０は、移動デバイス１０がパケットに基づいたネットワーク１４上に通信することを可能とする、パケットに基づいたネットワーク１４（図１）にアクセスを得ることが可能である（５４）。もしも必要とされれば、移動デバイス１０はまた、もしも予期された応答がタイミング間隔内で受信されない場合は、何等かの与えられた登録要求の再伝送をもたらすタイマーを実行することが可能である。

【００６０】

図６は、ＡＡＡサーバ２０の視点からセキュリティキー更新ルーチンに関する実施例を示すフロー線図である。示されるように、受信機／送信機４２が古いキーを用いて形成されたアクセス要求を受信する場合は（６１）、ＡＡＡ制御ユニット４４は、ＡＡＡサーバ２０の状態を決定するためにキー更新論理４８を呼び出す。もしもＡＡＡサーバがキー更新状態になく（６２の“いいえ”ブランチ）あるいは更新承認状態にない場合は（６３の“いいえ”ブランチ）、そこでＡＡＡサーバ２０はキーＯＫ状態にある（６４）。この場合、ＡＡＡ制御ユニット４４は、アクセス要求を認証し、そして従って移動デバイス１０に応答する（６５）。とくに、ＡＡＡ制御ユニット４４は送信されたセキュリティキーを調査し、そしてそれをメモリ４６内に保管されたセキュリティキーと比較することが可能である。あるいは、ＡＡＡ制御ユニットはそのセキュリティキーを用いて発生された、送信された許可値を調査し、そしてメモリ内に保管されたセキュリティキーとの比較のために許可値からセキュリティキーを抽出することが可能である。他の例においては、ＡＡＡ制御ユニット４４は、登録要求によって呼び出されたＣＨＡＰチャレンジに対する移動デバイスの応答を調査することが可能である。

【００６１】

いずれの場合においても、もしも移動デバイス１０が、固有のキーを用いて形成された

登録要求を送出する場合は、ＡＡＡサーバ２０は、移動デバイス１０がネットワーク１４（図１）にアクセスすることを許可するために、アクセス受け入れ回答を送出することによって応答することが可能である。もしもそうでない場合は、ＡＡＡサーバ２０は、移動デバイス１０がネットワーク１４にアクセスすることを拒否するためにアクセス拒否を送出することによって応答することが可能である。

【００６２】

しかしながら、もしもＡＡＡサーバ２０がキー更新状態にある場合は（６２の“はい”ブランチ）、そこでＡＡＡサーバ２０は移動デバイス１０とともにキー更新ルーチンを開始することが可能である。また、もしも若干の理由のためにＡＡＡサーバ２０が最初に更新承認状態にある場合は（６３の“はい”ブランチ）、ＡＡＡサーバ２０はキー更新状態に移行することが可能である（６６）。いずれの場合においても、一度ＡＡＡサーバ２０がキー更新状態になるときは、ＡＡＡ制御ユニット４４は、受信機／送信機４２による伝送のためにキー更新回答を発生することが可能である（６７）。そこで、キー更新回答を送出する後に、もしもＡＡＡサーバ２０が新しいキーおよびトークンを含むアクセス要求を受信した場合は（６８）（６９の“はい”ブランチ）、キー更新論理４８は、ＡＡＡサーバ２０を更新承認状態に移行させ（７１）、そしてＡＡＡサーバ２０は、トークンを含むアクセス回答を送信する（７２）。とくに、ＡＡＡ制御ユニット４４はトークン回答を発生することが可能であり、そして受信機／送信機４２は、それが正しいＡＡＡサーバと通信していることを移動デバイス１０に示すためにトークン回答を送出することが可能である。さらに、移動デバイス１０によるトークン回答の受信は新しいキーがＡＡＡサーバ２０によって受信されたことの表示を与えることが可能である。

【００６３】

そこで、トークン回答を送信する後に（７２）、もしもＡＡＡサーバ２０が移動デバイス１０によって送出されそして新しいキーを用いて形成されたＲＲＱに対応するアクセス要求を受信する場合は（７３）（７４の“はい”ブランチ）、キー更新論理４８は、ＡＡＡサーバ２０をキーＯＫ状態に移行させる（７５）。その点においてＡＡＡサーバ２０は、新しいキーを永久メモリに引き渡すことが可能であり、そしてＡＡＡ制御ユニット４４はアクセス要求を認証し、そして従って移動デバイス１０に応答することが可能である（６５）。とくに、ＡＡＡ制御ユニット４４は、移動デバイス１０が、キー更新ルーチンの一部としてＡＡＡサーバ２０によって先に受信された新しいキーに対応する、新しいキーを用いたか否かを決定することによって、移動デバイス１０を認証することが可能である。

【００６４】

この中に記述されたキー更新技術は、もしも更新処理期間中に１個あるいはそれ以上の通信が失われる場合、問題の回避を含むいくつかの利点を得ることが可能である。たとえば、もしもＡＡＡサーバ２０がトークン回答を送信する後に（７２）新しいキーおよびトークンを含む他のアクセス要求を受信する場合（７３、７４の“いいえ”ブランチ、および６９の“はい”ブランチ）、ＡＡＡサーバ２０は、更新承認状態にとどまり（７１）、そしてトークン回答を再送信することが可能である（７２）。この場合、ＡＡＡサーバ２０はさきのトークン回答は失われ、あるいはそうでなければ移動デバイス１０によって受信されなかったと仮定することが可能である。

【００６５】

また、もしもＡＡＡサーバ２０が新しいキーおよびトークンとともにアクセス要求を予期し、しかしこのような要求を受信しない場合（６９の“いいえ”ブランチ）は、ＡＡＡサーバ２０はキー更新ルーチンを再スタートすることが可能である。従って、このような場合、ＡＡＡサーバはキー更新状態に移行し（７０）、他のキー更新回答を再送信することが可能である（６７）。このようにして、更新ルーチンの個別の実行すなわち、キー更新ルーチンの事象のすべてに関する個別の実行を保証することが可能である。とくに一度ＡＡＡサーバ２０がキー更新状態に置かれるときは（６２、６６、あるいは７０）、それが最初に新しいキーおよびトークンとともにアクセス回答を受信し（６９の“はい”ブラ

ンチ）、そしてそこで移動デバイス１０によって送出され、そして新しいキーを用いて形成されたＲＲＱに対応するアクセス要求を受信する（７７の“はい”ブランチ）まではキーＯＫ状態に移行しないであろう。

【００６６】

この中に記述された技術は、そうでない場合は、一度通信がすでに受信されたときの、一度あるいはそれ以上の通信の再伝送、あるいはＡＡＡサーバ２０から移動デバイス１０へのサービス通信の否定等の、更新ルーチン期間中の他の通信の伝送によって引き起こされるかも知れない問題の、取り扱いを容易にすることが可能である。これらの場合、キー更新ルーチンに関するすべての事象が発生していないであろうことからキー更新ルーチンは終了しないであろう。さらにこの技術の他の利点は、移動デバイス１０およびＡＡＡサーバ２０のみをそれぞれのステートマシンとともに修正しそして、それがキー更新ルーチン期間中アクセス拒否（ＡＲ）を受信する場合は呼が終了されないことを保証するようにＦＡ１８を修正することによって、それらが実行されうることである。換言すれば、技術を実現するために必要とされる修正は、システム２の他のデバイスにとって影響の少ないことが可能なことである。また、この中に記述された更新ルーチンは、ＡＡＡサーバ２０がキーＯＫ状態に移行する以前に更新ルーチンのすべての事象が実行されるべきことを要求することによって、異端の攻撃から改善されたセキュリティを与えることが可能である。

【００６７】

この中に記述された技術は、移動デバイスおよび移動デバイスのユーザを認証するサーバによってそれぞれ実行することが可能である。いずれの場合も、技術はハードウエア、ソフトウエア、ファームウエア、あるいはそれらの任意の組み合わせ内で実行されることが可能である。もしもソフトウエア内で実行される場合は、この技術は、実行される場合はここに記述された技術の１個あるいはそれ以上を実行する、プログラムコードを含む計算機が読み出し可能な媒体で命令されることが可能である。たとえば、計算機が読み出し可能な媒体は、ディジタル信号処理装置（ＤＳＰ）等の処理装置内で実行される場合に、それぞれの移動デバイスあるいはサーバ等がこの中に記述された技術の１個あるいはそれ以上を実行することのもととなる、計算機が読み出し可能な命令を保管することが可能である。ＩＳ‐８３５‐Ａネットワークの環境においては、多くの詳細が与えられている。同様な技術が種々の他の無線ネットワークに適用されることが可能である。これらおよび他の実施例は請求項の範囲内にある。

【図面の簡単な説明】

【００６８】

【図１】図１は、その中でセキュリティキー更新ルーチンが移動デバイスおよびＡＡＡサーバによって実行されることが可能な、移動ネットワーキングプロトコルをサポートするよう配置されたシステムを示すブロック線図である。

【図２】図２は、一つの実施例に従ってセキュリティキー更新を実行するために、外部エージェントを経由しての移動デバイスおよびＡＡＡサーバ間の通信を示しているメッセージフロー線図である。

【図３】図３は、この中に記述されたようなセキュリティキー更新ルーチンの実行のために配置された、移動デバイスに関する典型的なブロック線図である。

【図４】図４は、この中に記述されたようなセキュリティキー更新ルーチンの実行のために配置された、ＡＡＡサーバに関する典型的なブロック線図である。

【図５】図５は、移動デバイスの観点からセキュリティキー更新ルーチンを示している、フロー線図である。

【図６】図６は、ＡＡＡサーバの観点からセキュリティキー更新ルーチンを示している、フロー線図である。

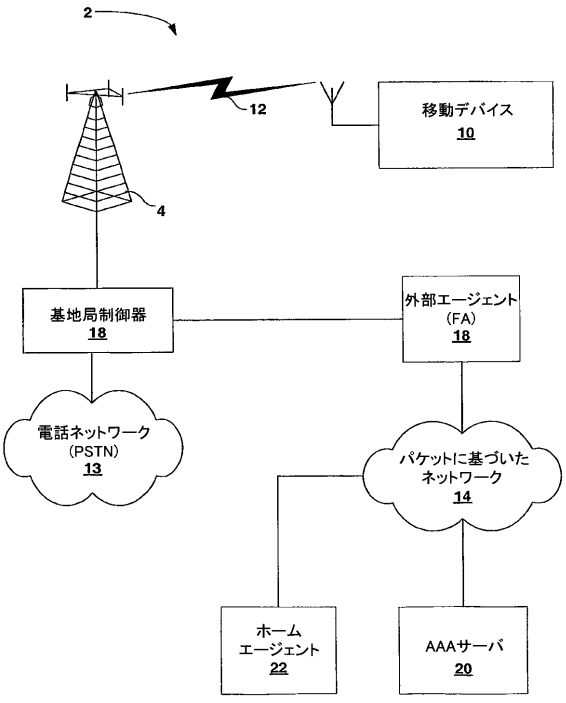
【符号の説明】

【００６９】

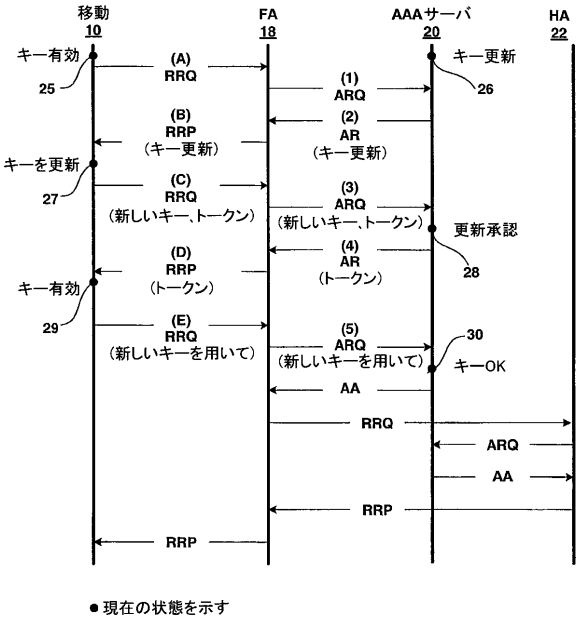
２…システム、　４…基地局、　１０…移動デバイス、　１３…公衆交換電話ネットワ

ーク、　１４…ネットワーク、　１８…ＦＡ、　２０…ＡＡＡサーバ、　２２…ホームエージェント、　３２…アンテナ、　３３…送信機、　３３…受信機、　３４…モデム、　３５…ＩＰ制御ユニット、　３６…メモリ、　３８…キー更新論理、　３９…発生器、　４２…送信機、　４４…ＡＡＡ制御ユニット、　４６…メモリ、　４８…キー更新論理、

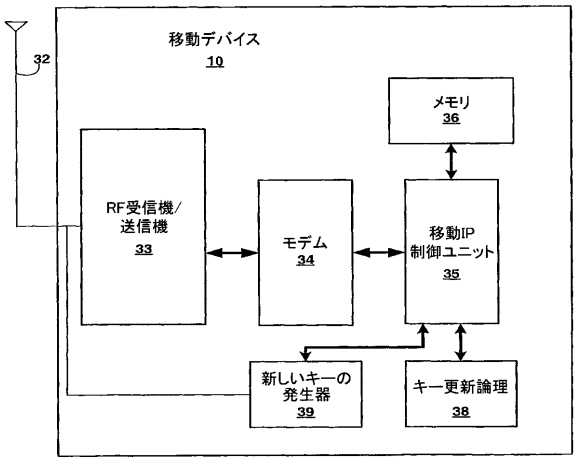
【図１】



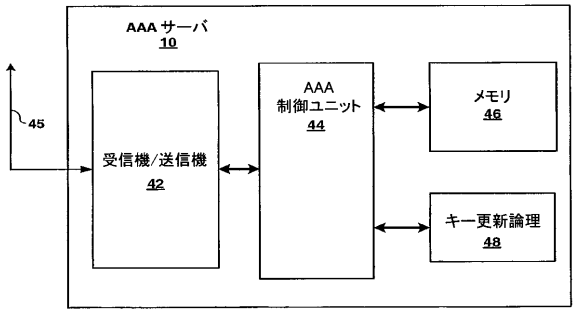
【図２】



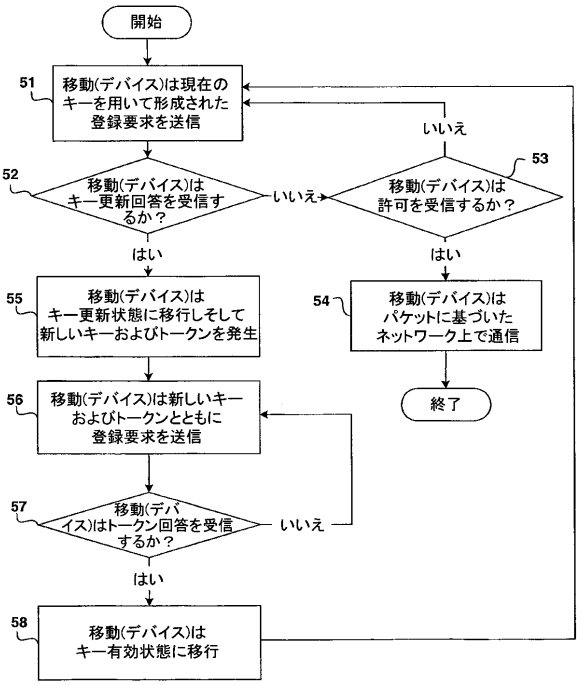
【図３】


移動デバイス
10
32
メモリ
36
RF受信機/
送信機
33
モデム
34
移動IP
制御ユニット
35
新しいキーの
発生器
39
キー更新論理
38

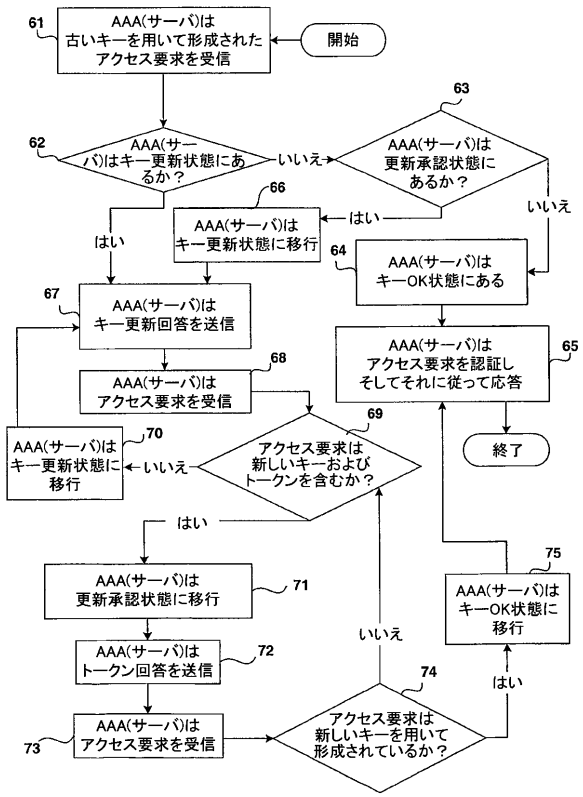
【図４】


AAA サーバ
10
45
受信機/送信機
42
AAA
制御ユニット
44
メモリ
46
キー更新論理
48

【図５】


開始
51
移動(デバイス)は現在の
キーを用いて形成された
登録要求を送信
52
移動(デバイス)は
キー更新回答を受信す
るか？
いいえ
はい
53
移動(デバイス)は
許可を受信するか？
いいえ
はい
55
移動(デバイス)は
キー更新状態に移行しそして
新しいキーおよびトークンを発生
54
移動(デバイス)は
パケットに基づいた
ネットワーク上で通信
終了
56
移動(デバイス)は新しいキー
およびトークンとともに
登録要求を送信
57
移動(デバ
イス)はトークン回答を受信
するか？
いいえ
はい
58
移動(デバイス)は
キー有効状態に移行

【図６】


61
AAA(サーバ)は
古いキーを用いて形成された
アクセス要求を受信
開始
62
AAA(サー
バ)はキー更新状態にあ
るか？
いいえ
はい
63
AAA(サーバ)は
更新承認状態に
あるか？
いいえ
はい
66
AAA(サーバ)は
キー更新状態に移行
64
AAA(サーバ)は
キーOK状態にある
67
AAA(サーバ)は
キー更新回答を送信
65
AAA(サーバ)は
アクセス要求を認証し
そしてそれに従って応答
68
AAA(サーバ)は
アクセス要求を受信
69
アクセス要求は
新しいキーおよび
トークンを含むか？
終了
70
AAA(サーバ)は
キー更新状態に
移行
いいえ
はい
71
AAA(サーバ)は
更新承認状態に移行
72
AAA(サーバ)は
トークン回答を送信
73
AAA(サーバ)は
アクセス要求を受信
74
アクセス要求は
新しいキーを用いて
形成されているか？
いいえ
はい
75
AAA(サーバ)は
キーOK状態に
移行

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 03/10512

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 073 233 A (LUCENT TECHNOLOGIES INC) 31 January 2001 (2001-01-31) paragraph '0006!	1-30
A	WO 01 76125 A (SIMOCO INT LTD ;RAYNE MARK WENTWORTH (GB)) 11 October 2001 (2001-10-11) column 2, line 34 -column 3, line 11; claim 1	1-30

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 June 2003	04/07/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Veen, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Informa on patent family members

International A[redacted]cation No
PCT/US 03/10512

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1073233 A	31-01-2001	AU 4882600 A	01-02-2001
		BR 0002975 A	13-03-2001
		CA 2314303 A1	29-01-2001
		CN 1283906 A	14-02-2001
		EP 1073233 A2	31-01-2001
		JP 2001077804 A	23-03-2001
WO 0176125 A	11-10-2001	AU 4434601 A	15-10-2001
		EP 1269680 A2	02-01-2003
		WO 0176125 A2	11-10-2001
		GB 2365702 A ,B	20-02-2002

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NI,NO,NZ,OM,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,UZ,VC,VN,YU,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
マッキントッシュ
リナックス
Ｂｌｕｅｔｏｏｔｈ
Ｍａｃｉｎｔｏｓｈ
Ｌｉｎｕｘ

(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100092196
弁理士 橋本 良郎
(72)発明者 クイック、ロイ・フランクリン・ジュニア
アメリカ合衆国、カリフォルニア州 ９２１０７、サン・ディエゴ、バルセロナ・ドライブ １１５０
(72)発明者 ダイク、ジェフレイ
アメリカ合衆国、カリフォルニア州 ９２１１７、サン・ディエゴ、マウント・ハリス・ドライブ ４８１６
(72)発明者 リオイ、マルセロ
アメリカ合衆国、カリフォルニア州 ９２１２２、サン・ディエゴ、ナンバー１９２４、チャーマント・ドライブ ７５８８
(72)発明者 マンダヤム、ジャヤンス
アメリカ合衆国、カリフォルニア州 ９２１２２、サン・ディエゴ、ナンバー５２８、レボン・ドライブ ３４２５

Ｆターム(参考) 5J104 EA16 PA02 PA07
5K030 GA15 HA08 HC09 JT09 KA06 LD19 MC07
5K067 AA33 BB21 CC08 DD17 DD23 DD24 EE02 EE10 HH21 HH24