(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4847322号
(P4847322)
(45)発行日　平成23年12月28日(2011.12.28)　(24)登録日　平成23年10月21日(2011.10.21)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675A

請求項の数 13　(全 15 頁)

(21)出願番号　特願2006-516955(P2006-516955)
(86)(22)出願日　平成16年6月28日(2004.6.28)
(65)公表番号　特表2007-520909(P2007-520909A)
(43)公表日　平成19年7月26日(2007.7.26)
(86)国際出願番号　PCT/KR2004/001569
(87)国際公開番号　WO2005/002131
(87)国際公開日　平成17年1月6日(2005.1.6)
審査請求日　平成19年5月9日(2007.5.9)
(31)優先権主張番号　10-2003-0042611
(32)優先日　平成15年6月27日(2003.6.27)
(33)優先権主張国　韓国(KR)

前置審査

(73)特許権者　503007988
ケーティー・コーポレーション
ＫＴ　Ｃｏｒｐｏｒａｔｉｏｎ
大韓民国京畿道城南市盆唐区亭子洞２０６番地
２０６　Ｊｕｎｇｊａ－ｄｏｎｇ，Ｐｕｎｄａｎｇ－ｇｕ，Ｓｕｎｇｎａｍ－ｓｈｉ，Ｋｙｏｕｎｇｋｉ－ｄｏ，Ｋｏｒｅａ
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠

最終頁に続く

(54)【発明の名称】二重要素認証されたキー交換方法及びこれを利用した認証方法とその方法を含むプログラムが貯蔵された記録媒体

(57)【特許請求の範囲】
【請求項１】
有線、無線の通信を通して、認証サーバーに接続された加入者端末器において相互認証のためのキーを交換する方法において、
ａ）前記加入者端末器が、自身の識別子と前記認証サーバーの公開キーを使用して生成されたキーを前記認証サーバーに送信する段階；
ｂ）前記加入者端末器が前記認証サーバーで生成された乱数を受信する段階；
ｃ）前記受信された乱数と前記加入者端末器に予め設定されているパスワード、及びトークンに貯蔵されたキーを同時に使って、第１特定値を暗号化した値と生成された加入者側認証子を前記加入者端末器を認証するためのキーとして前記認証サーバーに送信する段階；
ｄ）前記加入者端末器が、前記送信された加入者側認証子に対する前記認証サーバーでの認証成功によって、前記認証サーバーで生成された認証サーバー側認証子を前記認証サーバーを認証するためのキーとして前記認証サーバーから受信する段階；並びに
ｅ）前記加入者端末器が、前記トークンに貯蔵されたキーとパスワードを同時に使って前記受信された認証サーバー側認証子に対する認証を行い、前記認証が成功した場合、前記認証サーバー側認証子を受け入れる段階；
を含み、
前記第１特定値は、前記加入者端末器が前記認証サーバーと認証のためのキー交換を行わない場合、即ちａ）段階の前に前記加入者端末器によって生成された乱数を用いて事前

に計算される二重要素認証されたキー交換方法。
【請求項２】
前記トークンに貯蔵されたキーは対称キー（symmetric key）であることを特徴とする、請求項１に記載の二重要素認証されたキー交換方法。
【請求項３】
前記ａ）段階の前に、
前記加入者端末器が、登録過程で対称キーアルゴリズムに使用される前記対称キーと前記パスワードとを決めて、前記認証サーバーと共有する段階をさらに含む、請求項２に記載の二重要素認証されたキー交換方法。
【請求項４】
前記加入者端末器は、前記パスワード、及び前記認証サーバーの公開キーを前記トークンに貯蔵することを特徴とする、請求項１又は３に記載の二重要素認証されたキー交換方法。
【請求項５】
前記ａ）段階で、
前記生成されるキーは、前記加入者端末器の識別子と前記認証サーバーの公開キーに対して一方向ハッシュ関数を使用して生成されることを特徴とする、請求項１又は３に記載の二重要素認証されたキー交換方法。
【請求項６】
前記ｃ）段階は、
前記受信された乱数、前記パスワード、及び前記トークンに貯蔵されたキーに対し、ハッシュ関数を使用して第２特定値を生成する段階；
前記生成された第２特定値を使用して前記第１特定値を暗号化する段階；
前記乱数と前記第１特定値を使用して前記加入者側セッションキーを生成する段階；
前記生成されたセッションキー、前記パスワード、前記トークンに貯蔵されたキー、及び前記加入者端末器の識別子に対し、ハッシュ関数を使用して前記加入者側認証子を生成する段階；並びに
前記第１特定値を暗号化した値と前記加入者側認証子とを前記認証サーバーに送信する段階；
を含む、請求項１又は３に記載の二重要素認証されたキー交換方法。
【請求項７】
前記ｅ）段階は、
前記加入者側セッションキー、前記パスワード、前記トークンに貯蔵されたキー、及び前記認証サーバーの公開キーに対し、ハッシュ関数を使用して第３特定値を生成する段階；
前記生成された第３特定値と前記認証サーバーから受信された認証サーバー側認証子が同じであるか否かを判断する段階；並びに
前記生成された第３特定値と前記認証サーバーから受信された認証サーバー側認証子が同じである場合、前記加入者端末器と前記認証サーバーとの間の認証が成功したものと判断して、前記認証サーバー側認証子を受け入れる段階；
を含む、請求項６に記載の二重要素認証されたキー交換方法。
【請求項８】
前記ａ）段階で、前記加入者端末器の識別子がグローバルローミングと課金を支援するためにＮＡＩ（Network Access ID）形式を使用する場合、前記加入者端末器が、ユーザー名の部分と前記認証サーバーの公開キーをハッシュした値と領域名の部分とを共に前記認証サーバーに送信することを特徴とする、請求項１に記載の二重要素認証されたキー交換方法。
【請求項９】
アクセスポイントを通して加入者端末器と認証サーバーが接続された無線通信システムで、前記加入者端末器と前記認証サーバーとの間に二重要素認証されたキー交換により相

互認証する方法において、
ａ）前記加入者端末器が、前記アクセスポイントから識別子要請を受ける段階；
ｂ）前記加入者端末器が、自身の識別子と前記認証サーバーの公開キーを使用して生成したキーを前記アクセスポイントを通して前記認証サーバーに送信する段階；
ｃ）前記認証サーバーが、前記加入者端末器から受信されたキーを使用して前記加入者関連パスワード及び秘密キーと前記認証サーバーの公開キーを検出し、乱数を生成して、前記アクセスポイントを通して前記加入者端末器に送信する段階；
ｄ）前記加入者端末器が、前記受信された乱数と前記パスワード及びトークンに貯蔵されたキーを同時に使用して、第１特定値を暗号化した値と生成された加入者側認証子とを前記加入者端末器を認証するためのキーとして前記アクセスポイントを通して前記認証サーバーに送信する段階；
ｅ）前記認証サーバーが、前記パスワード、前記トークンに貯蔵されたキー、及び前記乱数を同時に使用して生成した第２特定値を秘密キーにして、前記ｄ）段階で受信された暗号化値を復号し、前記復号された値に基づいて、前記受信された加入者側認証子に対する認証を行い、前記認証が成功した場合、前記パスワード、トークンに貯蔵されたキー、及び公開キーを同時に使用して生成された認証サーバー側認証子を、前記認証サーバーを認証するためのキーとして前記アクセスポイントを通して前記加入者端末器に送信する段階；
ｆ）前記加入者端末器が、前記トークンに貯蔵されたキーとパスワードを同時に使用して、前記受信された認証サーバー側認証子に対する認証を行い、その認証結果を前記アクセスポイントを通して前記認証サーバーに送信する段階；並びに
ｇ）前記認証サーバーが、前記加入者端末器から送信された認証結果が成功と判明した場合、前記加入者に対する接続許可を前記アクセスポイントを通して前記加入者端末器に送信する段階；
を含み、
前記第１特定値は、前記加入者端末器が前記認証サーバーと認証のためのキー交換を行わない場合、即ちａ）段階の前に前記加入者端末器によって生成された乱数を用いて事前に計算される二重要素認証されたキー交換による認証方法。
【請求項１０】
前記トークンに貯蔵されたキーは対称キーであることを特徴とする、請求項９に記載の二重要素認証されたキー交換による認証方法。
【請求項１１】
前記加入者端末器と前記アクセスポイントとの間では拡張可能な認証プロトコル（Extensible Authentication Protocol：ＥＡＰ）が使用され、
前記アクセスポイントと前記認証サーバーとの間ではＲＡＤＩＵＳプロトコルが使用されることを特徴とする、請求項９又は１０に記載の二重要素認証されたキー交換による認証方法。
【請求項１２】
有線、無線の通信を通して認証サーバーに接続された加入者端末器で相互認証のためのキーを交換する方法において、
ａ）前記加入者端末器が、自身の識別子と前記認証サーバーの公開キーを使用して生成されたキーを前記認証サーバーに送信する機能；
ｂ）前記加入者端末器が、前記認証サーバーで生成された乱数を受信する機能；
ｃ）前記受信された乱数と前記加入者端末器に予め設定されているパスワード及びトークンに貯蔵されたキーを同時に使用して第１特定値を暗号化した値と生成された加入者側認証子とを前記加入者端末器を認証するためのキーとして前記認証サーバーに送信する機能；
ｄ）前記加入者端末器が、前記送信された加入者側認証子に対する前記認証サーバーでの認証成功により、前記認証サーバーで生成された認証サーバー側認証子を前記認証サーバーを認証するためのキーとして前記認証サーバーから受信する機能；並びに

ｅ）前記加入者端末器が、前記トークンに貯蔵されたキーとパスワードを同時に使用して前記受信された認証サーバー側認証子に対する認証を行い、前記認証が成功した場合、前記認証サーバー側認証子を受け入れる機能；

を含み、

前記第１特定値は、前記加入者端末器が前記認証サーバーと認証のためのキー交換を行わない場合、即ちａ）段階の前に前記加入者端末器によって生成された乱数を用いて事前に計算されることを実現するプログラムを貯蔵した記録媒体。

【請求項１３】

前記トークンに貯蔵されたキーは対称キーであることを特徴とする、請求項１２に記載のプログラムを貯蔵した記録媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、認証及びキー設定（Authentication and Key Establishment：ＡＫＥ）プロトコルに係り、より具体的には、インターネット、無線ＬＡＮ、公衆無線ＬＡＮなどのサービスでの二重要素認証されたキー交換（Two-factor Authenticated Key Exchange：ＴＡＫＥ）方法と、これを利用して個体認証及びキー設定のための保安を遂行する方法、及びその方法を含むプログラムが貯蔵された記録媒体に関するものである。

【背景技術】

【０００２】

従来の認証及びキー設定方法には、代表的なものとして認証書を利用したＴＬＳ（Transport Layer Security）方式とパスワードを利用したＳＲＰ（Secure Remote Password）方式、ＥＡＰ－ＭＤ５方式、そして認証書及びパスワードの２種類を全て利用したＰＥＡＰ（Protected EAP）、ＥＡＰ－ＴＴＬＳ（Tunneled TLS）などがあるが、各方式は短所を有している。

【０００３】

つまり、ＴＬＳは、複雑で多くの費用を要するＰＫＩ（Public Key Infrastructure）及び認証書管理システムが必要であり、ＳＲＰは、使用者端末側で多くの演算量（2 exponentiation）を要し、2-for-1 guess attack（２件のうち１件は偽者と思われる状態）に脆弱である。またＰＥＡＰとＥＡＰ－ＴＴＬＳはＭｉｔＭ（Man-in-the-Middle：偽者が端末とサーバーの間に介在して、両方の情報を抜き取って利用する状態）の攻撃に弱く、交換メッセージの回数が多い。そして、ＥＡＰ－ＭＤ５は、相互認証とセッション（session）キーを提供しないという短所がある。

【０００４】

特に、（公衆）無線ＬＡＮでＰＤＡｓ（Personal Digital Assistants）を用いる場合に適用できる安全でありかつ効率的である８０２．１ｘのＥＡＰ（Extensible Authentication Protocol）認証方式を探すのが容易でない。なぜかというと、ＰＤＡｓは、累乗（exponentiation）や逆元（inverse element）計算のような複雑な演算量を遂行するのに時間が多くかかり、電力消費が多いからである。

【０００５】

一方、一般的に認証要素には、（１）使用者が記憶するもの（パスワード）と（２）使用者が持っているもの（トークンや無線機器）の２種類の要素がある。

この中で、項目（１）のパスワードを利用した単一要素認証方式は、次のような種々の問題点のために決して安全でないという問題点がある。先ず、使用者がパスワードを入力する時に誰かが使用者の肩越しでパスワードを盗み見ることができ、打鍵状況を見られてパスワードが知られるということである。二番目に、詐欺、脅迫などのような反社会的方法でパスワードを攻撃者に開示させられるということである。三番目には、パスワードは情報量側面から見れば エントロピーが低いので、事典攻撃（網羅的情報攻撃）に脆弱であるということである。四番目には、パスワードを物理的に記録したり、類似パスワードをいくつかの所に更新なしで使うような使用者の悪い習慣によりパスワードを盗み見でき

るということである。特に、ホットスポット（高速通信可能地点）地域でネットワーク接続を試みる公衆無線ＬＡＮサービスは一層攻撃に危険であると言える。たとえ、加入者をパスワードによって認証するＥＡＰ－ＳＲＰ、ＰＥＡＰ、ＥＡＰ－ＴＴＬＳ方式が事前攻撃に安全なプロトコルであっても、攻撃者は、オフライン上で打鍵状況盗み見や反社会的方法でパスワードを獲得することもできるからである。

【０００６】

また、項目（２）のトークンや無線機器を利用した単一要素認証方式は、トークンとトークンを読める入力装置（例:カードリーダー）が必要であるという短所がある。二番目の要素であるトークンは、スマートカード、ＵＳＢキー、そしてＰＤＡｓのような無線機器などが可能である。したがって、無線環境では、トークンをＵＳＢキーや無線機器に用いれば、特にハードウェアを追加しなくてもよいので多くの費用を要しない。但し、トークンは対称秘密キー又は個人の認証関連秘密情報が貯蔵されなければならないので、ある程度の不法変調防止特性を有した保安モジュールに貯蔵されなければならない。

【０００７】

したがって、インターネットや（公衆）無線ＬＡＮなどでは、前記認証要素による認証に比べてより強力な認証体系を要求し、特に、次のような技術的要求事項を解決することのできる認証方法が要求される。

（１）身元保護：盗聴のような受動的攻撃から加入者（client）の身元を保護することは個人の通信秘密のために必要である。特に、ＤＨＣＰ（Dynamic Host Configuration Protocol）にＩＰアドレスの割り当てを受けられる使用者には有用なことである。

【０００８】

（２）強力な相互認証：攻撃者（attacker）は、加入者と認証サーバーとの間に位置してＭｉｔＭ攻撃を遂行できるので、加入者と網に対する相互認証が必要である。

（３）セッションキーの設定：加入者と網との間に交換されるデータを保護するためにセッションキーが設定されなければならない。

【０００９】

（４）Forward Secrecy（ＦＳ）：プロトコルに参加する個体のLong term secret keying material（長期秘密キー資料）が盗み見されても、攻撃者が以前に盗聴したセッションから過去セッションキーを計算できない性質であるＦＳが提供されていなければならない。このようなＦＳは、half FSとfull FSに分けられるが、前者は、加入者と認証サーバーのうちのいずれか一つの個体の秘密キーを見ても攻撃者は過去セッションキーを誘導できないことを意味し、後者は、二つの個体の秘密キーが全て見られた場合にもセッションキーが安全であることを意味する。

【００１０】

（５）オフライン辞典攻撃に対する安全性：攻撃者がオフライン辞典攻撃を行って、加入者とサーバーとの間に共有された秘密情報を盗むことのないように、プロトコルが設計されなければならない。

（６）ＭｉｔＭ（Man-in-the-Middle）攻撃に対する安全性：（公衆）無線ＬＡＮ環境では、rouge AP(化粧で誤魔化した偽Access Point)やrouge無線ＮＩＣを用いたＭｉｔＭ攻撃に脆弱なので、これに対する攻撃に安全であるように設計されなければならない。

【００１１】

（７）Replay(反復)攻撃に対する安全性：攻撃者が既に使用されたメッセージを再伝送して認証及びキー設定に成功することを防止しなければならない。

（８）効率性

－演算負荷の最小化：（公衆）無線ＬＡＮ環境でＰＤＡｓに適用できるほどの少ない演算量を要求しなければならない。そして、事前計算を利用して、オンライン計算の負荷を最小化しなければならない。

－メッセージ交換回数の最小化：網資源の効率性と網上の遅延などを考慮すれば、通信ラウンド（往復通信）数が少ないほど長所がある。したがって、加入者と認証サーバーとの間に交換しなければならないメッセージの回数をできるだけ少なくしなければならない。

－通信帯域幅使用の最小化：プロトコルメッセージの大きさをできるだけ小さくしなければならない。

【００１２】

（９）キーの確認：プロトコルに参加した合法的な使用者が、自分が意図した相手と実際に共通の秘密セッションキーを共有したことを確認しなければならない。

（１０）否認不可（non repudiation）：サービス使用時間と網接続回数などのような課金データに対し、使用者が否めない否認不可機能が提供されなければならない。

【発明の開示】

【発明が解決しようとする課題】

【００１３】

本発明の目的は前記従来の問題点を解決するためのものであって、２個の独立的な認証要素であるパスワードとトークンに貯蔵されたキーとを利用して加入者を認証する二重要素認証されたキー交換（ＴＡＫＥ）方法及びこれを利用した認証方法と、その方法を含むプログラムが貯蔵された記録媒体を提供することにある。

【課題を解決するための手段】

【００１４】

前記目的を達成するための本発明の特徴による二重要素認証されたキー交換方法は、有線、無線の通信を通して認証サーバーに接続された加入者端末器で相互認証のためのキーを交換する方法であって、ａ）前記加入者端末器が、自身の識別子と前記認証サーバーの公開キーを使用して生成されたキーを前記認証サーバーに送信する段階；ｂ）前記加入者端末器が前記認証サーバーで生成された乱数を受信する段階；ｃ）前記受信された乱数と前記加入者端末器に予め設定されているパスワード及びトークンに貯蔵されたキーを使用して、第１特定値を暗号化した値と生成された加入者側認証子を前記認証サーバーに送信する段階；ｄ）前記加入者端末器が、前記送信された加入者側認証子に対する前記認証サーバーでの認証成功によって、前記認証サーバーで生成された認証サーバー側認証子を受信する段階；並びにｅ）前記加入者端末器が、前記秘密キーとパスワードを使用して前記受信された認証サーバー側認証子に対する認証を行い、前記認証が成功した場合、前記認証サーバー側認証子を受け入れる段階；を含む。ここで、トークンに貯蔵されたキーは対称キーを利用するのが好ましい。

【００１５】

前記二重要素認証されたキー交換方法は、前記ａ）段階の前に、前記加入者端末器が、登録過程で対称キーアルゴリズムに使用される前記対称キーと前記パスワードとを決めて前記認証サーバーと共有する段階；及び前記加入者端末器が、前記認証サーバーと認証のためのキー交換を行わない場合に乱数を生成し、前記第１特定値を事前計算する段階；をさらに含む。

【００１６】

そして、前記加入者端末器は、前記前記パスワード及び前記認証サーバーの公開キーをトークンに貯蔵するのが好ましい。

また、前記ａ）段階で、前記生成されるキーは、前記加入者端末器の識別子と前記認証サーバーの公開キーに対して一方向ハッシュ関数を使用して生成されるのが好ましい。

【００１７】

また、前記ｃ）段階は、前記受信された乱数、前記パスワード、及び対称キーに対し、ハッシュ関数を使用して第２特定値を生成する段階；前記生成された第２特定値を使用して前記第１特定値を暗号化する段階；前記乱数と前記第１特定値を使用して前記加入者側セッションキーを生成する段階；前記生成されたセッションキー、前記パスワード、前記対称キー、及び前記加入者端末器の識別子に対し、ハッシュ関数を使用して前記加入者側認証子を生成する段階；並びに前記第１特定値を暗号化した値と前記加入者側認証子を前記認証サーバーに送信する段階；を含む。

【００１８】

また、前記ｅ）段階は、前記加入者側セッションキー、前記パスワード、前記対称キー

、及び前記認証サーバーの公開キーに対し、ハッシュ関数を使用して第３特定値を生成する段階；前記生成された第３特定値と前記認証サーバーから受信された認証サーバー側認証子が同じであるか否かを判断する段階；並びに前記生成された第３特定値と前記認証サーバーから受信された認証サーバー側認証子が同じである場合、前記加入者端末器と前記認証サーバーとの間の認証が成功したと判断して、前記認証サーバー側認証子を受け入れる段階；を含む。

【００１９】

本発明の他の特徴による二重要素認証されたキー交換方法は、有線、無線の通信を通して加入者端末器に接続された認証サーバーで相互認証のためのキーを交換する方法であって、ａ）前記加入者端末器が、自身の識別子と前記認証サーバーの公開キーを使用して生成されたキーを前記認証サーバーに送信する段階；ｂ）前記加入者端末器が、前記認証サーバーで生成された乱数を受信する段階；ｃ）前記受信された乱数と前記加入者端末器に予め設定されているパスワード及びトークンに貯蔵されたキーを使用して、第１特定値を暗号化した値と生成された加入者側認証子とを前記認証サーバーに送信する段階；ｄ）前記加入者端末器が、前記送信された加入者側認証子に対する前記認証サーバーでの認証成功によって、前記認証サーバーで生成された認証サーバー側認証子を受信する段階；並びにｅ）前記加入者端末器が、前記秘密キーとパスワードを使用して前記受信された認証サーバー側認証子に対する認証を行い、前記認証が成功した場合、前記認証サーバー側認証子を受け入れる段階；を含む。ここで、トークンに貯蔵されたキーは対称キーであるのが好ましい。

【００２０】

そして、前記ａ）段階の前に、前記認証サーバーが、登録過程で対称キー暗号アルゴリズムに使用される前記対称キーと前記パスワードとを決めて前記加入者端末器と共有する段階をさらに含む。

ここで、前記認証サーバーは、前記対称キー、前記パスワード、及び前記認証サーバーの秘密キーを保安ファイル関連データベース内に貯蔵するのが好ましい。

【００２１】

また、前記ｄ）段階は、前記パスワード、前記対称キー、及び前記乱数に対し、ハッシュ関数を使用して前記第１特定値を生成する段階；前記生成された第１特定値を秘密キーにして、前記受信された暗号化値を復号して前記第２特定値を生成する段階；前記生成された第２特定値、前記認証サーバーの公開キー、及び前記乱数を使用して前記認証サーバー側セッションキーを生成する段階；前記生成されたセッションキー、前記パスワード、前記対称キー、及び前記加入者端末器の識別子に対し、ハッシュ関数を使用して求められた値と前記受信された加入者側認証子が同じであるか否かを判断する段階；並びに前記求められた値と前記受信された加入者側認証子が同じである場合、前記加入者に対する認証が成功したと判断して、前記加入者側認証子を受け入れる段階；を含む。

【００２２】

また、前記ｅ）段階で、前記認証サーバー側認証子生成に前記生成された認証サーバー側セッションキーが使用されるのが好ましい。

また、前記ａ）段階で、前記加入者端末器の識別子がグローバルローミングと課金を支援するためにＮＡＩ（Network Access ID）形式を使用する場合、前記加入者端末器が、ユーザー名の部分と前記認証サーバーの公開キーをハッシュした値と領域名の部分を共に前記認証サーバーに送信するのが好ましい。

【００２３】

本発明のまた他の特徴による二重要素認証されたキー交換方法を利用した認証方法は、アクセスポイントを通じて加入者端末器と認証サーバーが接続された無線通信システムで、前記加入者端末器と前記認証サーバーとの間に二重要素認証されたキー交換により相互認証する方法であって、ａ）前記加入者端末器が、前記アクセスポイントから識別子要請を受ける段階；ｂ）前記加入者端末器が、自身の識別子と前記認証サーバーの公開キーを使用して生成されたキーを前記アクセスポイントを通して前記認証サーバーに送信する段

階；ｃ）前記認証サーバーが、前記加入者端末器から受信されたキーを使用して前記加入者関連パスワード及び秘密キーと前記認証サーバーの公開キーを検出し、乱数を生成して、前記アクセスポイントを通して前記加入者端末器に送信する段階；ｄ）前記加入者端末器が、前記受信された乱数と前記パスワード及びトークンに貯蔵されたキーを使用して第１特定値を暗号化した値と、生成された加入者側認証子とを前記アクセスポイントを通して前記認証サーバーに送信する段階；ｅ）前記認証サーバーが、前記パスワード、前記トークンに貯蔵されたキー、及び前記乱数を使用して生成した第２特定値を秘密キーにして、前記ｄ）段階で受信された暗号化値を復号し、前記復号された値に基づいて前記受信された加入者側認証子に対する認証を行い、前記認証が成功した場合、前記前記パスワード、トークンに貯蔵されたキー、及び公開キーを使用して生成された認証サーバー側認証子を前記アクセスポイントを通して前記加入者端末器に送信する段階；ｆ）前記加入者端末器が、前記トークンに貯蔵されたキーとパスワードを使用して前記受信された認証サーバー側認証子に対する認証を行い、その認証結果を前記アクセスポイントを通して前記認証サーバーに送信する段階；並びにｇ）前記認証サーバーが、前記加入者端末器から送信された認証結果が成功したと判明された場合、前記加入者に対する接続許可を前記アクセスポイントを通して前記加入者端末器に送信する段階；を含む。

【００２４】

ここで、前記加入者端末器と前記アクセスポイントとの間では拡張可能な認証プロトコル（Extensible Authentication Protocol: EAP）が使用され、前記アクセスポイントと前記認証サーバーとの間ではＲＡＤＩＵＳプロトコルが使用されるのが好ましい。

【発明を実施するための最良の形態】

【００２５】

以下、添付した図面を参照して、本発明の実施例について本発明が属する技術分野で通常の知識を有する者が容易に実施できるように詳しく説明する。しかし、本発明は多様な相違した形態で実現でき、ここで説明する実施例に限定されない。図面においては、本発明を明確に説明するために説明上不要な部分は省略した。明細書全体を通じて類似な部分については同じ図面号を付けた。

【００２６】

まず、本発明の実施例によるＴＡＫＥプロトコルを利用した認証方法について詳細に説明する。

図１は、本発明の実施例によるＴＡＫＥプロトコルのフローチャートである。図１を参照して本発明の実施例によるＴＡＫＥプロトコルについて説明する前に、まず、本発明の実施例で記述される記号について次の通り定義する。

Ａ：加入者

Ｂ：認証サーバー

π：パスワード

ｔ：対称キー暗号で使用される対称キー

$ＩＤ_{A}$：加入者Ａの識別子

$Ｅ_{K}\{\}$、$Ｄ_{K}\{\}$：対称キーＫで、対称キーに暗号化及び復号化

Ｈ（）：一方向ハッシュ関数

$ｓｋ_{A}$：Ａが生成したセッションキー

ｐ：大きな素数

ｑ：（ｐ－１）を分ける大きな素数の数

ｇ：位数がｑである$Ｚ^{*}_{p}$の元素である生成源

ｂ、$ｇ^{b}$（mod　p）：認証サーバーＢの静的秘密キー、公開キー

次に、図１を参照すれば、本発明の実施例によるＴＡＫＥプロトコルの動作は、登録段階、事前計算段階、及び実行段階に分けられる。

【００２７】

まず、登録段階について説明する。

加入者（Client A）、実質的には加入者の無線端末器とサーバー（Server B）は、３Ｄ

ＥＳ（Data Encryption Standard）やラインダール（Rijndael）のような対称キー暗号アルゴリズムに使用される対称キー（ｔ）とパスワード（π）を決めて共有する。そして、サーバーは、特定加入者に対するサーバーの秘密キー［１～ｑ－１］範囲の任意の数＜ｂ＞を選択して安全なデータベース（ＤＢ）に貯蔵し、加入者にサーバーの公開キー（g^b）とドメインパラメーター（ｐ、ｑ、ｇ）を知らせる。加入者は、対称キー（ｔ）をトークンに貯蔵する。サーバーの公開キー（g^b）とドメインパラメーター（ｐ、ｑ、ｇ）は公開できる性質の情報であるから、必ずしも安全な場所に貯蔵せねばならないことはない。

【００２８】

次に、事前計算段階について説明する。

本発明の実施例による事前計算はプロトコル遂行前のオフライン上で行われる段階であり、プロトコル遂行中に要する時間と計算量を減少させる。加入者の無線端末器は、無線ネットワークを使用しない空時間（idle time）や端末器パワーオン時に事前計算を行う。図１に示すように、加入者Ａは、［１～ｑ－１］範囲にある任意の数を選択する。

【００２９】

【数１】

つまり、加入者は、任意の数を$x \in_R Z_q$選択した後、選択した任意の数ｘを使用してg^x、$g^{bx}=c$（以後、mod ｐは省略する）を事前計算する。

次に、実行段階について説明する。

この実行段階は相互個体認証とセッションキー設定を遂行する段階であって、次のような手続からなる。

（１）加入者Ａはインターネットや（公衆）無線ＬＡＮサービス接続のために、自身の識別子ID_Aと認証サーバーＢの公開キー（g^b）をハッシュした値であるＨ（ID_A、g^b）を認証サーバーＢに送る。

【００３０】

もし、加入者ＩＤがグローバルローミングと課金を支援するためにＮＡＩ形式を使用する場合、例えば、加入者ＩＤがｕｓｅｒｉｄ@ｒｅａｌｍ.ｃｏｍである場合、ユーザー名部分とg^bをハッシュした値のＨ（userid、g^b）と領域名の部分を共に送る。

【００３１】

（２）Ｈ（ID_A、g^b）を受けた認証サーバーＢは、加入者保安ファイル関連データベース（ＤＢ）から＜Ｈ（ID_A、g^b）＞、＜ID_A＞、＜π＞、＜ｔ＞、＜ｂ＞を検出し出す。

【００３２】

【数２】

認証サーバーＢは、［１～ｑ－１］範囲にある任意の数$r \in_R Z_q$を選択して、加入者Ａに送る。

【００３３】

【数３】

（３）加入者Ａは、認証サーバーＢが送った任意の数ｒを受信すれば、π及びｔと共に用いてハッシュした値ｆ＝Ｈ（ｒ、π、ｔ）を計算した後、このｆを、g^xを対称キー暗号化する対称キーに使用して$e = E_f\{g^x\}$を計算する。

そして、ｃ、g^x、及びｒをハッシュした値であるセッションキーsk_A＝Ｈ（ｃ、g^x、ｒ）を計算した後、π、ｔ、及びＩＤＡをハッシュした値である認証子M_A＝Ｈ（sk_A、π、ｔ、ID_A）を生成する。加入者Ａは、前記生成されたｅとM_Aを認証サーバーＢに送る。

【００３４】

【数４】

（４）認証サーバーＢは、加入者Ａから送信されたｅとM_Aを受け、ｒ、π、及びｔを使用してハッシュしてｆ＝Ｈ（ｒ、π、ｔ）を計算し、受信されたｅを前記計算された秘密キーｆで復号化して$g^x = D_f\{e\}$を求める。

その後、認証サーバーＢは、前記求められたg^xとｂを使用してｃ＝g^{xb}を計算した後、ｃとｒを共に使ってsk_B＝Ｈ（ｃ、g^x、ｒ）を計算し、次いで、Ｈ（sk_B、π、ｔ、ID_A）を生成して、前記受信されたM_Aと同じであるか否かを検査する。もし、二つの値が同じであれば加入者Ａに対する認証は成功であるから、認証サーバーＢは、加入者Ａから送信されたM_Aを受け入れる。そして、認証サーバーＢは、M_B＝Ｈ（sk_B、π、ｔ、g^b）を計算して加入者Ａに送る。

【００３５】

（５）加入者Ａは、認証サーバーＢから受信したM_Bと自分が計算したＨ（sk_B、π、ｔ、g^b）が同じ値であるか否かを検査する。もし、二つの値が同じであれば認証サーバーＢに対する認証は成功であるから、加入者ＡはM_Bを受け入れる。このように加入者Ａと認証サーバーＢがM_AとM_Bを各々受け入れれば、加入者Ａと認証サーバーＢとの間の相互認証が成功したことを意味する。

【００３６】

図２は、本発明の実施例によるＴＡＫＥプロトコルを用いた（公衆）無線ＬＡＮでの認証及びキー交換フローチャートである。

図２を参照すれば、（公衆）無線ＬＡＮなどのアクセスポイント２００を通して加入者１００と認証サーバー３００とが連結されて、加入者１００に対する認証が認証サーバー３００によって行われる。

【００３７】

ここで、加入者１００とアクセスポイント２００との間では拡張可能な認証プロトコルが使用され、アクセスポイント２００と認証サーバー３００との間ではＲＡＤＩＵＳプロトコルが使用される。

また、加入者１００は、対称キー（ｔ）、パスワード（π）、認証サーバー３００の公開キー（g^b）、及びＤＨ（Diffie-Hellman）ドメインパラメーター（ｐ、ｑ、ｇ）を貯蔵しており、認証サーバー３００は、対称キー（ｔ）、パスワード（π）、認証サーバー３００の公開キー（g^b）、及びＤＨドメインパラメーター（ｐ、ｑ、ｇ）の外にサーバー秘密キー（ｂ）を貯蔵している。

【００３８】

まず、加入者１００が（公衆）無線ＬＡＮなどのサービス接続を要請する場合、アクセ

スポイント２００は、加入者１００にタイプ１（identity）を有するＥＡＰ要請（EAP-Request/Identity）を送る（Ｓ１００）。

加入者１００は、自身の識別子$ＩＤ_A$と認証サーバー３００の公開キー（g^b）をハッシュした値であるＨ（$ＩＤ_A$、g^b）をアイデンティティにするＥＡＰ応答（Ｈ（$ＩＤ_A$、g^b））をアクセスポイント２００に伝達する（Ｓ１１０）。

【００３９】

次に、アクセスポイント２００は、加入者１００から伝達されたアイデンティティを含んで、認証サーバー３００に対する接続要請（Radius-Access-Request、Ｈ（$ＩＤ_A$、g^b））を送る（Ｓ１２０）。

【００４０】

【数５】

認証サーバー３００は、アクセスポイント２００から送信されたにＨ（$ＩＤ_A$、g^b）基づいて、関連データベースから＜ＩＤＡ＞、＜π＞、＜ｔ＞、及び＜ｂ＞を検出し出した後、任意の値$r \in_R Z_q$を選択して、接続チャレンジ値（Radius-Access-Challenge）としてアクセスポイント２００に送れば（Ｓ１３０）、アクセスポイント２００は、このｒ値をＴＡＫＥサブタイプ１（subtype1）にして、ＥＡＰ要請（EAP-Request/TAKE subtype1(r)）を加入者１００に伝達する（Ｓ１４０）。

一方、加入者１００は、認証サーバー３００から送ってきた任意の値ｒを受信すれば、π及びｔと共に使ってハッシュした値ｆ＝Ｈ（ｒ、π、ｔ）を計算した後、このｆを、g^xを対称キー暗号化する秘密キーとして使用してｅ=Ef｛gx｝を計算する。そして、ｃ、g^x、及びｒをハッシュした値であるセッションキーsk_A＝Ｈ（ｃ、g^x、ｒ）を計算した後π、ｔ及び$ＩＤ_A$をハッシュした値である認証子M_A＝Ｈ（sk_A、π、ｔ、$ＩＤ_A$）を生成して、ｅとM_AをＴＡＫＥサブタイプ１に対するＥＡＰ応答（EAP-Response/TAKE Subtype1 (e, M_A)）をアクセスポイント２００に送り（Ｓ１５０）、アクセスポイント２００は、加入者１００から伝達された（ｅ、M_A）を含む接続要請（Radius-Access-Request (e, M_A)）を認証サーバー３００に送る（Ｓ１６０）。

【００４１】

【数６】

次に、認証サーバー３００は、加入者１００から送信されたｅとM_Aを受けてｒ、π、及びｔを使用してハッシュしてｆ＝Ｈ（ｒ、π、ｔ）を計算し、受信されたｅを前記計算された秘密キーｆで復号化して$g^x = D_f\{e\}$を求める。

その後、認証サーバー３００は、前記求められたg^xとｂを使用してｃ＝$g^{x\,b}$を計算した後、ｃとｒを共に使ってsk_B＝Ｈ（ｃ、g^x、ｒ）を計算し、次いで、Ｈ（sk_B、π、ｔ、$ＩＤ_A$）を生成して、前記受信されたM_Aと同じであるか否かを検査する。もし、二つの値が同じであれば加入者１００に対する認証は成功であるので、認証サーバー３００は、加入者１００から送信されたM_Aを受け入れる。そして、認証サーバー３００は、M_B＝Ｈ（sk_B、π、ｔ、g^b）を計算して、接続チャレンジメッセージ（Radius-Access-Challenge (M_B)）としてアクセスポイント２００に送る（Ｓ１７０）。

【００４２】
アクセスポイント２００は、認証サーバー３００から送ってきたM_BをＴＡＫＥサブタイプ２にして、ＥＡＰ要請（EAP-Request/TAKE subtype2 (M_B)）を加入者１００に伝達する（Ｓ１８０）。
次に、加入者１００は、認証サーバー３００から送ってきたM_Bを受信して、自分が計算したＨ（sk_B、π、ｔ、g^b）と同じ値であるか否かを検査する。もし、二つの値が同じであれば、認証サーバー２００に対する認証は成功なので、加入者１００はM_Bを受け入れる。このように加入者１００と認証サーバー３００がM_AとM_Bを各々受け入れれば、加入者１００と認証サーバー３００との間の相互認証が成功に行われたことである。
【００４３】
次に、加入者１００は確認を意味するＴＡＫＥサブタイプ２に対するＥＡＰ応答（EAP-Response/TAKE Subtype2）をアクセスポイント２００に送り（Ｓ１９０）、アクセスポイント２００は、加入者１００から伝達されたメッセージを含む接続要請を認証サーバー３００に送る（Ｓ２００）。
【００４４】
認証サーバー３００は、アクセスポイント２００を通して加入者１００から送ってきた認証結果が成功であれば、接続許容メッセージ（Radius-Access-Accept）をアクセスポイント２００に送り（Ｓ２１０）、アクセスポイント２００は、この結果によりＥＡＰ成功メッセージ（EAP-Success）を加入者１００に送った後（Ｓ２２０）、認証サーバー３００から接続が許容されたことを知らせるためにＥＡＰＯＬ－Ｋｅｙメッセージを加入者１００に送る（Ｓ２３０）。
【００４５】
ここで、加入者１００とアクセスポイント２００との間に伝えられるメッセージ又はパケットには、ＬＡＮプロトコルを通したＥＡＰカプセル化（EAP encapsulation over LAN protocol:EAPOL）が使用される。
前記のように、本発明の実施例によるＴＡＫＥプロトコルを利用した認証方法が、強力な認証のために要求される技術的事項を満足するかについて説明する。つまり、本発明の実施例によるＴＡＫＥプロトコルを利用した認証方法に対する安全性の分析は次の通りである。
【００４６】
（１）身元保護：加入者は、ＩＤ要請を受けると自身のID_Aの代わりにＨ（ID_A、g^b）を伝送して、盗聴者のような受動的攻撃者が加入者の身元を分からないようにする。但し、認証サーバーは加入者の匿名と実際の身元をマッチングできなければならない。
【００４７】
（２）強力な相互認証：加入者は、パスワード（π）と秘密キー（ｔ）、そして認証サーバーの公開キー（g^b）を知ることによって、初めて認証子M_Aを誘導することができて、加入者認証を受けることができる。一方、認証サーバーは、パスワード（π）と秘密キー（ｔ）、加入者識別子（ＩＤＡ）、そしてサーバーの秘密キー（ｂ）を知ることによって、初めてM_Bを誘導することができて、ネットワーク認証を受けることができる。したがって、強力な相互認証を提供するようになる。
【００４８】
（３）セッションキー設定：加入者と認証サーバーとの間で、データ保護のためにセッションキー（sk_A、sk_B）が生成される。生成されたセッションキーは乱数性と新規性を提供するが、これは各個体の動的な任意数ｘとｒの選択に起因する。
（４）Forward Secrecy(FS)：加入者が所持している秘密情報＜ID_A＞、＜π＞、＜ｔ＞、＜g^b＞を、攻撃者が全て盗み見できる場合、攻撃者はｅ暗号文を復号してg^xを知り得るだろうが、$c = g^{xb}$値はＤＬＰ（離散対数問題）だから計算が難しい。また、サーバーの秘密キー＜ｂ＞を盗み見できる場合には、$c = g^{xb}$値を計算するためにg^xを知らなければならず、g^xを知るためには＜π＞及び＜ｔ＞を知らなければならない。つまり、攻撃者は、＜ｂ＞、＜π＞、＜ｔ＞を全て知ることによって、初めてセッション

キーを計算することができる。しかし、実際に（公衆）無線ＬＡＮ環境では、サービスを提供する企業が大企業であって自身の強力な保安体制を持っているはずなので、保安関連の重要な秘密情報が攻撃者に漏れる可能性は非常に低いと考えられる。したがって、ＴＡＫＥプロトコルは、（公衆）無線ＬＡＮでは一般的なhalf FSというよりは、実用的なhalf FSと言える。

【００４９】

（５）オフライン辞典（offline dictionary）攻撃：攻撃者達は、認証成功に必要な秘密情報を得るためにオフライン辞典攻撃を試みる可能性がある。エントロピーの少ないパスワードは、このような攻撃に脆弱であるが、ＴＡＫＥでは、トークンに貯蔵されたエントロピーの高い秘密キーとパスワードとが任意の値g^xを暗号化するキーに共に使用されるので、このような攻撃は事実上不可能である。つまり、攻撃者は、パスワードと秘密キーそして任意の値g^xまで推測しなければならない。

【００５０】

（６）Man-in-The-Middle(MitM)攻撃に対する安全性：攻撃者は、加入者とサーバーとの間に位置してＭｉｔＭ攻撃を行うことができる。しかし、ＴＡＫＥでは強力な二重要素認証を使っているので、このような攻撃が成功するのは非常に難しい。

【００５１】

（７）Replay攻撃に対する安全性：Replay攻撃は、攻撃者が既に使用されたメッセージを再伝送して以前のセッションキーを再び設定しようとする攻撃方法である。ＴＡＫＥでは、加入者とサーバーが毎セッションごとに任意の数ｘとｒを各々生成してセッションキーを生成するので、Replay攻撃に安全である。

【００５２】

（８）効率性(efficiency)

－演算負荷の最小化：DH(Diffie-Hellman)プロトコルは、ＦＳを提供できるので認証及びキー設定（ＡＫＥ）プロトコルで多く使用されているが、累乗計算を要求するために演算量が多くなる。ハッシュ関数及び対称キー暗号化/復号化にかかる時間は非常に短いので、演算に要する時間の大部分は累乗と逆元計算、そして掛け算で占められている。特に、ＰＤＡｓでは、演算量が多くなると実時間認証にかかる時間が多くなる。したがって、ＴＡＫＥでは、オンライン上で加入者側が対称キー暗号１番とハッシュ５番を使用するようにし、オフラインでは、事前計算で２番の累乗計算をするように設計された。一方、サーバー側では、累乗１番、対称キー復号１番、そしてハッシュ４番の演算量が必要である。

－メッセージ交換回数の最小化：ＴＡＫＥでは４回のパス（pass）があるため、加入者と認証サーバーとの間で交換しなければならないメッセージの回数が少ない。

－通信帯域幅使用の最小化：５個のメッセージのうちで３個はハッシュの出力ビット数であり、一つは乱数のビット数であり、他の一つはg^x暗号文の出力ビット数である。

【００５３】

（９）キー確認：ＴＡＫＥでは、認証子M_AとM_Bにセッションキーを含ませてキー確認を行うことにより、プロトコルに参加した合法的な加入者が自身の意図した認証サーバーと実際に共通の秘密セッションキーを共有したことを確認することができる。

（１０）否認不可：ＴＡＫＥではデジタル署名方式を使用しないが、強力な二重要素認証を使うので、欺瞞的な使用者がサービスを利用してこれを否認することを防止することができる。

【００５４】

以上のような本発明の方法は、プログラムに実現されてコンピュータで読むことのできる形態に、記録媒体（ＣＤ－ＲＯＭ、ＲＡＭ、ＲＯＭ、フロッピー（登録商標）ディスク、ハードディスク、光磁気ディスクなど）に貯蔵することができる。

以上、本発明の好ましい実施例について詳細に説明したが、本発明はこれに限定されるものではなく、その他の多様な変更や変形が可能である。

【図面の簡単な説明】

【００５５】

【図１】本発明の実施例によるＴＡＫＥプロトコルのフローチャートである。
【図２】本発明の実施例によるＴＡＫＥプロトコルを用いた（公衆）無線ＬＡＮでの認証及びキー交換フローチャートである。

【図１】

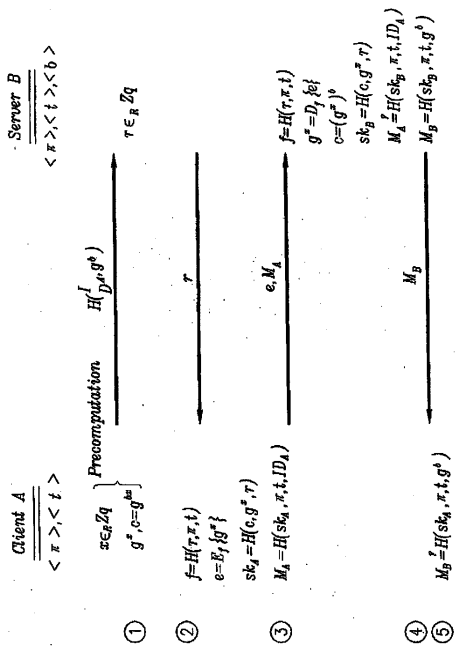

図１

【図２】

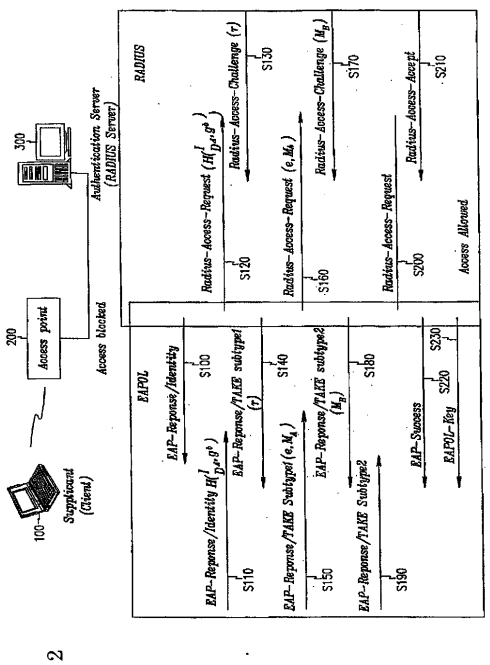

図２

フロントページの続き

(74)代理人 100109830
弁理士 福原 淑弘
(74)代理人 100095441
弁理士 白根 俊郎
(74)代理人 100084618
弁理士 村松 貞男
(72)発明者 パーク、ユンーマン
大韓民国、ソウル １３９－９０４、ノウォンーグ、サングイェ ６－ドン、ミド・アパートメント １０２－２１０
(72)発明者 リ、ソンーチョン
大韓民国、ソウル １３５－７７５、カンナムーグ、デチードン、ミド・アパートメント １０６－２０４
(72)発明者 チャ、ヨンージョ
大韓民国、キュンキード ４６３－７２０、ソンナムーシティー、ブンダンーク、グムゴクードン、チョンソルーメウル・ファイン・アパートメント ２０４－３０３

審査官 中里 裕正

(56)参考文献 米国特許出願公開第２００３／００９３６８０（ＵＳ，Ａ１）
特表２００２－５２１９６２（ＪＰ，Ａ）
特開２００１－０６０９４７（ＪＰ，Ａ）
特開２００１－３１３６３４（ＪＰ，Ａ）
Samfat, D. , Molva, R., A Method Providing Identity Privacy to Mobile Users during Authentication, First Workshop on Mobile Computing Systems and Applications, １９９４年１２月 ９日, p.196-199

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 9/32