

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-208073

(P2004-208073A)

(43) 公開日 平成16年7月22日(2004.7.22)

(51) Int.Cl.⁷

H04L 9/32

H04L 9/08

H04Q 7/38

F I

H04L 9/00

675A

H04B 7/26

109R

H04L 9/00

601C

テーマコード (参考)

5J104

5K067

審査請求 未請求 請求項の数 4 O L (全 20 頁)

(21) 出願番号 特願2002-375281 (P2002-375281)

(22) 出願日 平成14年12月25日 (2002.12.25)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(74) 代理人 100082740

弁理士 田辺 恵基

(72) 発明者 日高 伊佐夫

東京都品川区北品川6丁目7番35号ソニー株式会社内

Fターム(参考) 5J104 AA07 KA02 KA04 PA01 PA07

5K067 AA30 BB04 BB21 DD17 EE02

EE10 EE16 EE24 HH36 JJ39

(54) 【発明の名称】 無線通信システム

(57) 【要約】

【課題】簡易な手順で高速にアクセスポイント間のハンドオフを実行し得る無線通信システムを実現する。

【解決手段】初回認証時、無線通信端末の識別番号に対応付けて第1の乱数を認証サーバの認証情報記憶手段に記憶しておく。そして無線通信端末のハンドオフ時、当該無線通信端末から送信された識別番号に基づいて認証情報記憶手段からパスワード及び第1の乱数を取得して認証サーバ側で新たな暗号鍵を生成するとともに、無線通信端末でも新たな暗号鍵を生成し、ハンドオフ先のアクセスポイントが、この2つの暗号鍵に基づいて無線通信端末の認証を行うようにしたことにより、応答値の算出処理を省いて認証手順を簡略化し、これにより簡易な手順で高速にアクセスポイント間のハンドオフを実行することができる。

【選択図】 図7

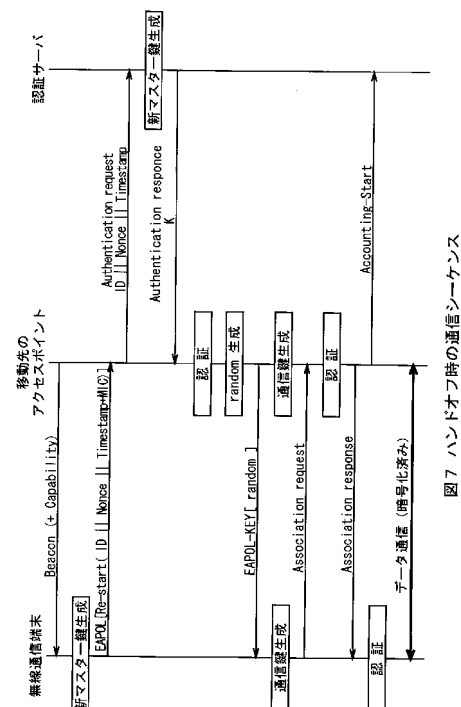


図7 ハンドオフ時の通信シーケンス

【特許請求の範囲】

【請求項 1】

無線通信端末と、当該無線通信端末に対する認証を行う認証サーバと、上記無線通信端末との間で無線を介した通信を行い、当該無線通信端末と外部ネットワークとの間、及び当該無線通信端末と上記認証サーバとの間の通信を中継する複数のアクセスポイントとからなる無線通信システムにおいて、
上記無線通信端末は、
上記アクセスポイントから送信される第 1 の乱数、当該無線通信端末固有の識別番号及びパスワードから応答値を生成する端末側応答値生成手段と、
生成した第 2 の乱数、上記識別番号及び上記応答値を認証要求に格納して上記認証サーバ 10
に送信する認証要求手段と、
上記パスワード、上記第 1 の乱数及び上記第 2 の乱数から暗号鍵を生成する端末側暗号鍵生成手段と、
当該生成した暗号鍵を用いて暗号化通信を行う端末側暗号通信手段と
を具え、
上記認証サーバは、
上記無線通信システムに所属する全ての上記無線通信端末それぞれの上記識別番号及び上記パスワードを対応付けて記憶する認証情報記憶手段と、
上記無線通信端末から送信された上記識別番号に対応するパスワードを上記識別情報記憶手段から取得し、当該取得したパスワード、上記無線通信端末から送信された上記識別番号 20
及び上記アクセスポイントから送信された上記第 1 の乱数から上記応答値を生成するサーバ側応答値生成手段と、
上記サーバ側応答値生成手段で生成した上記応答値と上記無線通信端末から送信された上記応答値とを比較し、これらが一致したとき、当該無線通信端末が当該無線通信システムの正当なユーザであるとして認証するとともに、上記第 1 の乱数を当該無線通信端末の識別番号に対応付けて上記認証情報記憶手段に記憶する認証手段と
を具え、
上記無線通信端末が第 1 の上記アクセスポイントから第 2 の上記アクセスポイントにハンドオフする際、
上記認証要求手段は、上記識別番号、新たに生成した上記第 2 の乱数及び上記第 2 のアクセスポイントから送信される時間情報を含むハンドオフ要求を生成するとともに、上記パスワード、上記第 1 の乱数、新たな上記第 2 の乱数及び上記時間情報から新たな暗号鍵を生成し、当該新たな暗号鍵と上記ハンドオフ要求とから当該ハンドオフ要求の改ざんを防止する改ざん防止情報を生成し、当該改ざん防止情報を当該ハンドオフ要求に付加し上記第 2 のアクセスポイントを介して上記認証サーバに送信し、
上記認証手段は、上記ハンドオフ要求に含まれる上記識別番号に対応する上記パスワード及び上記第 1 の乱数を上記認証情報記憶手段から取得し、当該取得したパスワード及び第 1 の乱数、上記ハンドオフ要求に含まれる上記第 2 の乱数及び上記時間情報から新たな暗号鍵を生成して上記第 2 のアクセスポイントに送信し、
上記第 2 のアクセスポイントは、上記認証サーバから送信された上記新たな暗号鍵と上記 40
ハンドオフ要求とから上記改ざん防止情報を生成し、当該生成した上記改ざん防止情報と、上記ハンドオフ要求に付加された上記改ざん防止情報とが一致したとき、上記無線通信端末が上記無線通信システムの正当なユーザであるとして認証してハンドオフを許可することを特徴とする無線通信システム。

【請求項 2】

無線通信端末と、当該無線通信端末に対する認証を行う認証サーバと、上記無線通信端末との間で無線を介した通信を行い、当該無線通信端末と外部ネットワークとの間、及び当該無線通信端末と上記認証サーバとの間の通信を中継する複数のアクセスポイントとからなる無線通信システムのハンドオフ方法において、
上記アクセスポイントから上記無線通信端末に対して送信される第 1 の乱数、当該無線通 50

信端末固有の識別番号及びパスワードから応答値を生成し、生成した第2の乱数、上記識別番号及び上記応答値を認証要求に格納して上記無線通信端末から上記認証サーバに送信する認証要求ステップと、

上記パスワード、上記第1の乱数及び上記第2の乱数から暗号鍵を生成する端末側暗号鍵生成ステップと、

上記無線通信端末から送信された上記識別番号に対応するパスワードを識別情報記憶手段から取得し、当該取得したパスワード、上記無線通信端末から送信された上記識別番号及び上記アクセスポイントから送信された上記第1の乱数から上記応答値を生成し、当該生成した応答値と上記無線通信端末から送信された上記応答値とを比較し、これらが一致したとき、当該無線通信端末が当該無線通信システムの正当なユーザであるとして認証するとともに、上記第1の乱数を当該無線通信端末の識別番号に対応付けて上記認証情報記憶手段に記憶する認証ステップと、

10

上記無線通信端末が第1の上記アクセスポイントから第2の上記アクセスポイントにハンドオフする際、上記識別番号、新たに生成した上記第2の乱数及び上記第2のアクセスポイントから送信される時間情報を含むハンドオフ要求を生成するとともに、上記パスワード、上記第1の乱数、新たな上記第2の乱数及び上記時間情報から新たな暗号鍵を生成し、当該新たな暗号鍵と上記ハンドオフ要求とから当該ハンドオフ要求の改ざんを防止する改ざん防止情報を生成し、当該改ざん防止情報を当該ハンドオフ要求に付加し上記第2のアクセスポイントを介して上記認証サーバに送信するハンドオフ要求送信ステップと、

上記ハンドオフ要求に含まれる上記識別番号に対応する上記パスワード及び上記第1の乱数を上記認証情報記憶手段から取得し、当該取得したパスワード及び第1の乱数、上記ハンドオフ要求に含まれる上記第2の乱数及び上記時間情報から新たな暗号鍵を生成して上記認証サーバから上記第2のアクセスポイントに送信する暗号鍵送信ステップと、

20

上記認証サーバから送信された上記新たな暗号鍵と上記ハンドオフ要求とから上記改ざん防止情報を生成し、当該生成した上記改ざん防止情報と、上記ハンドオフ要求に付加された上記改ざん防止情報とが一致したとき、上記無線通信端末が上記無線通信システムの正当なユーザであるとして認証してハンドオフを許可するハンドオフ許可ステップとを具えることを特徴とする無線通信システムのハンドオフ方法。

【請求項3】

無線通信端末及び複数のアクセスポイントとを有する無線通信システムにおける上記無線通信端末に対する認証を行う認証サーバにおいて、

30

上記無線通信システムに所属する全ての上記無線通信端末それぞれの識別番号及びパスワードを対応付けて記憶する認証情報記憶手段と、

上記無線通信端末から送信された上記識別番号に対応するパスワードを上記識別情報記憶手段から取得し、当該取得したパスワード、上記無線通信端末から送信された上記識別番号及び上記アクセスポイントから送信された第1の乱数から応答値を生成するサーバ側応答値生成手段と、

上記サーバ側応答値生成手段で生成した上記応答値と上記無線通信端末から送信された上記応答値とを比較し、これらが一致したとき、当該無線通信端末が当該無線通信システムの正当なユーザであるとして認証するとともに、上記第1の乱数を当該無線通信端末の識別番号に対応付けて上記認証情報記憶手段に記憶する認証手段と

40

を具え、

上記認証手段は、上記無線通信端末が第1の上記アクセスポイントから第2の上記アクセスポイントにハンドオフする際、当該無線通信端末から送信されたハンドオフ要求に含まれる上記識別番号に対応する上記パスワード及び上記第1の乱数を上記認証情報記憶手段から取得し、当該取得したパスワード及び第1の乱数、上記ハンドオフ要求に含まれる上記第2の乱数及び上記時間情報から新たな暗号鍵を生成して上記第2のアクセスポイントに送信することにより、当該新たな暗号鍵を用いて上記無線通信端末の認証及びハンドオフの許可を上記第2のアクセスポイントに実行させる

ことを特徴とする認証サーバ。

50

【請求項 4】

複数のアクセスポイント及び認証サーバを有する無線通信システムの無線通信端末において、

上記アクセスポイントから送信される第 1 の乱数、当該無線通信端末固有の識別番号及びパスワードから応答値を生成する端末側応答値生成手段と、

生成した第 2 の乱数、上記識別番号及び上記応答値を認証要求に格納して上記認証サーバに送信する認証要求手段と、

上記パスワード、上記第 1 の乱数及び上記第 2 の乱数から暗号鍵を生成する端末側暗号鍵生成手段と、

当該生成した暗号鍵を用いて暗号化通信を行う端末側暗号通信手段と

10

を具え、

第 1 の上記アクセスポイントから第 2 の上記アクセスポイントにハンドオフする際、上記認証要求手段は、上記識別番号、新たに生成した上記第 2 の乱数及び上記第 2 のアクセスポイントから送信される時間情報を含むハンドオフ要求を生成するとともに、上記パスワード、上記第 1 の乱数、新たな上記第 2 の乱数及び上記時間情報から新たな暗号鍵を生成し、当該新たな暗号鍵と上記ハンドオフ要求とから当該ハンドオフ要求の改ざんを防止する改ざん防止情報を生成し、当該改ざん防止情報を当該ハンドオフ要求に付加し上記第 2 のアクセスポイントを介して上記認証サーバに送信することにより、上記時間情報、上記識別番号に対応する上記パスワード及び上記第 1 の乱数から上記認証サーバが生成した新たな暗号鍵と上記ハンドオフ要求とを用いた当該無線通信端末の認証及びハンドオフの許可を上記第 2 のアクセスポイントに実行させる

20

ことを特徴とする無線通信端末。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は無線通信システムに関し、例えば複数のアクセスポイントの間でハンドオフを行い得るようになされた無線 LAN システムに適用して好適なものである。

【0002】

【従来の技術】

従来、無線 LAN システム等の各種通信システムにおいて、端末の正当性を確認するための認証が一般的に行われている。

30

【0003】

例えば、ある端末がアクセスポイントを経由して通信を行おうとする場合、当該アクセスポイントは、正当なユーザのみに対して利用を許可するため端末に対して認証を行う。また端末は、正当なアクセスポイントのみを利用するためアクセスポイントに対して認証を行うこともある。この場合、端末とアクセスポイントの相互で認証を行うことになる。

【0004】

この認証方式には様々なものがある。例えば、端末にパスワードを用意しておき、これをアクセスポイントに送付することにより正当な端末であることを伝える P A P (Password Authentication Protocol) や、パスワードを利用してデータを暗号化して認証する C H A P (Challenge Handshake Authentication Protocol)、R S A (Rivest Shamir Adleman) や E C C (Elliptic Curve Cryptography) を用いた公開暗号鍵方式を利用する T L S (Transport Layer Security) プロトコル等の認証方式が広く用いられている。

40

【0005】

ここで、P A P はパスワードが通信路に平文で流される（無暗号化）ため、安全性を考慮すると、電話回線のような秘匿性が保証された通信路でしか利用できない。これに対して C H A P や T L S プロトコルはパスワードが暗号化されるため、インターネットや無線 LAN のような通信内容の秘匿性が保証されない通信路での利用が可能である。

【0006】

しかしながら C H A P や T L S プロトコルは、端末とアクセスポイントの間のデータのや

50

りとりが多く、また処理に要する計算量が多いため処理時間が長くなるという欠点がある。特に、T L S プロトコルは C H A P に比べて強固であるが、その分計算量も多く長い処理時間を要する。しかし、パーソナルコンピュータ等の情報処理装置の処理能力向上もあり、今後は主として T L S プロトコルが利用されることが考えられている。

【0007】

無線通信システムにおいては、これらの認証方式を利用して端末（及びアクセスポイント）を認証するとともに、鍵を第三者に知られないようにして生成する。この鍵は、以降の通信においてデータを暗号化したり、データが改ざんされていないことを保証するために利用される。

【0008】

ここで、無線 L A N システムのアクセスポイントはその通信可能範囲が比較的狭いため、アクセスポイントを複数設置して、無線 L A N システム全体の通信可能範囲を拡大することが行われている。

【0009】

このような複数のアクセスポイントを有する無線 L A N システムにおいて、端末が第 1 のアクセスポイントの通信可能範囲から第 2 のアクセスポイントの通信可能範囲に移動した場合、当該端末は第 1 のアクセスポイントとの通信接続を終了して移動先の第 2 のアクセスポイントとの通信接続を開始することにより、異なるアクセスポイント間に渡って継続して通信を行う。かかるアクセスポイント間に渡る通信接続の切替えをハンドオフと呼ぶ（例えば、特許文献 1 参照）。

【0010】

【特許文献 1】

特開 2 0 0 1 - 2 5 8 0 5 9 公報

【0011】

【発明が解決しようとする課題】

上述したようにハンドオフに際しては、当該ハンドオフ毎に再度認証を繰り返す。ところが上述したように認証処理に複雑な手順が必要であり、ハンドオフに時間がかかる。このため、ハンドオフを行うことによって実質的な伝送速度が落ちてしまうとともに、多数の端末が同時にハンドオフを行った場合、認証サーバの負荷が増大してしまうという問題があった。

【0012】

本発明は以上の点を考慮してなされたもので、簡易な手順で高速にアクセスポイント間のハンドオフを実行し得る無線通信システムを提案しようとするものである。

【0013】

【課題を解決するための手段】

かかる課題を解決するため本発明においては、無線通信端末と、当該無線通信端末に対する認証を行う認証サーバと、無線通信端末との間で無線を介した通信を行い、当該無線通信端末と外部ネットワークとの間及び認証サーバとの間の通信を中継する複数のアクセスポイントとからなる無線通信システムにおいて、無線通信端末に、アクセスポイントから送信される第 1 の乱数、当該無線通信端末固有の識別番号及びパスワードから応答値を生成する端末側応答値生成手段と、生成した第 2 の乱数、識別番号及び応答値を認証要求に格納して認証サーバに送信する認証要求手段と、パスワード、第 1 の乱数及び第 2 の乱数から暗号鍵を生成する端末側暗号鍵生成手段と、当該生成した暗号鍵を用いて暗号化通信を行う端末側暗号通信手段とを設けた。

【0014】

また認証サーバに、無線通信システムに所属する全ての無線通信端末それぞれの識別番号及びパスワードを対応付けて記憶する認証情報記憶手段と、無線通信端末から送信された識別番号に対応するパスワードを識別情報記憶手段から取得し、当該取得したパスワード、無線通信端末から送信された識別番号及びアクセスポイントから送信された第 1 の乱数から応答値を生成するサーバ側応答値生成手段と、サーバ側応答値生成手段で生成した上

10

20

30

40

50

記応答値と上記無線通信端末から送信された上記記応答値とを比較し、これらが一致したとき、当該無線通信端末が当該無線通信システムの正当なユーザであるとして認証するとともに、上記第1の乱数を当該無線通信端末の識別番号に対応付けて上記認証情報記憶手段に記憶する認証手段を設けた。

【0015】

そして、無線通信端末が第1のアクセスポイントから第2のアクセスポイントにハンドオフする際、無線通信端末の認証要求手段は、識別番号、新たに生成した第2の乱数及び第2のアクセスポイントから送信される時間情報を含むハンドオフ要求を生成するとともに、パスワード、第1の乱数、新たな第2の乱数及び時間情報から新たな暗号鍵を生成し、当該新たな暗号鍵とハンドオフ要求とから当該ハンドオフ要求の改ざんを防止する改ざん防止情報を生成し、当該改ざん防止情報を当該ハンドオフ要求に付加し第2のアクセスポイントを介して認証サーバに送信するようにした。また認証サーバの認証手段は、ハンドオフ要求に含まれる識別番号に対応するパスワード及び第1の乱数を認証情報記憶手段から取得し、当該取得したパスワード及び第1の乱数、ハンドオフ要求に含まれる第2の乱数及び時間情報から新たな暗号鍵を生成して第2のアクセスポイントに送信するようにした。

【0016】

そして、第2のアクセスポイントは、認証サーバから送信された新たな暗号鍵とハンドオフ要求とから改ざん防止情報を生成し、当該生成した改ざん防止情報とハンドオフ要求に付加された改ざん防止情報とが一致したとき、無線通信端末が無線通信システムの正当なユーザであるとして認証してハンドオフを許可するようにした。

【0017】

初回認証時、無線通信端末の識別番号に対応付けて第1の乱数を認証情報記憶手段に記憶しておく。そして無線通信端末のハンドオフ時、当該無線通信端末から送信された識別番号に基づいて認証情報記憶手段からパスワード及び第1の乱数を取得して新たな暗号鍵を生成するとともに、無線通信端末でも新たな暗号鍵を生成し、この2つの暗号鍵に基づいてハンドオフ先のアクセスポイントが無線通信端末の認証を行うようにしたことにより、応答値の算出処理を省いて認証手順を簡略化し、これにより簡易な手順で高速にアクセスポイント間のハンドオフを実行することができる。

【0018】

【発明の実施の形態】

以下図面について、本発明の一実施の形態を詳述する。

【0019】

(1) 無線LANシステムの全体構成

図1において、1は全体として本発明による無線LAN通信システムとしての無線LANシステムを示し、無線通信基地局としての2つのアクセスポイント2(2A、2B)、無線通信端末3、及び認証装置としての認証サーバ4で構成される。

【0020】

實際上、無線通信端末3はPCカード型の無線LANカードであり、ノートブック型パーソナルコンピュータ(以下、これをノートパソコンと呼ぶ)5のPCカードスロットに挿着されている。第1のアクセスポイント2A及び第2のアクセスポイント2Bと無線通信端末3は、例えば2.4[GHz]帯で相互にCSMA/CA方式による無線通信を行う。また、アクセスポイント2A及び2Bと認証サーバ4との間は、有線ネットワーク6を介して接続されている。

【0021】

認証サーバ4は無線通信端末5のユーザID及びパスワードを記憶しており、アクセスポイント2A又は2Bを介して、当該無線通信端末5に対する認証を行う。無線通信端末3は、認証サーバ4によって正当なユーザとして認証された場合にのみ、有線ネットワーク6に接続された外部ネットワーク7に対するアクセスが可能になる。そして無線LANシステム1においては、無線通信端末3及びアクセスポイント2A又は2Bを介して、ノー

10

20

30

40

50

トパソコン 5 と外部ネットワーク 7 に接続されたパーソナルコンピュータ等の情報処理装置の間でデータ通信を行い得るようになされている。

【0022】

アクセスポイント 2 A 及び 2 B は、それぞれ固有の通信可能範囲 a 及び b を有している。そして無線通信端末 3 が一方の通信可能範囲から他方へと移動した場合、後述するハンドオフ認証処理に従って、簡易かつ高速にアクセスポイント間のハンドオフを行い得るようになされている。

【0023】

図 2 は、無線 LAN システム 1 のプロトコルスタックを示し、アクセスポイント 2 と無線通信端末 3 の間の低位プロトコルとしては IEEE 802.11 (無線 LAN) を用いている。その上位プロトコルとしては IEEE 802.1x で定義される EAPOL (Extensible Authentication Protocol Over LAN) と EAP プロトコルを用い、これを用いて認証を行う。 10

【0024】

また、アクセスポイント 2 と認証サーバ 4 の間の低位プロトコルとしては IEEE 802.3 (Ethernet (登録商標)) を用い、その上位では TCP/IP (Transmission Control Protocol/Internet Protocol) を用いたネットワーク/トランスポートレイヤでの通信が行われ、RADIUS (Remote Authentication Dial In User) を用いて認証を行う。

【0025】

(2) アクセスポイント、無線通信端末及び認証サーバの構成 20

次に、アクセスポイント 2、無線通信端末 3 及び認証サーバの構成 4 の構成を、それぞれ図 3、図 4 及び図 5 を用いて説明する。

【0026】

図 3 に示すようにアクセスポイント 2 においては、CPU 11 に対してネットワークインターフェース 12、データ処理部 13、送受信部 14 が接続されている。また CPU 11 には、後述するマスター鍵や通信鍵等の認証に伴う設定値や、各種プログラムを記憶するためのメモリ 15 と、リアルタイムクロック 16 が接続されている。CPU 11 はアクセスポイント通信制御プログラムに従い、アクセスポイント 2 の各部を統括的に制御する。

【0027】

送受信部 14 は、無線通信端末 3 から送信された上りの送信信号をアンテナ 17 を介して受信して復調し、受信データとしてデータ処理部 13 に供給する。データ処理部 13 は受信データの無線フレームを分解し、ネットワークインターフェース 12 を介して有線ネットワーク 6 に供給する。 30

【0028】

またデータ処理部 13 は、有線ネットワーク 5 からネットワークインターフェース 12 を介して供給された無線通信端末 3 への送信データを、無線フレームに構成して送受信部 14 に供給する。送受信部 14 は送信データを変調して下りの送信信号を生成し、アンテナ 17 を介して送信する。

【0029】

一方、図 4 に示すように無線通信端末 3 においては、CPU 21 に対してホストインターフェース 22、端末側暗号通信手段としてのデータ処理部 23 及び送受信部 24 が接続されている。また CPU 21 には、認証に伴う設定値や各種プログラムを記憶するためのメモリ 25 と、リアルタイムクロック 26 とが接続されている。CPU 21 は端末通信制御プログラムに従い、無線通信端末 3 の各部を統括的に制御する。 40

【0030】

送受信部 24 は、アクセスポイント 2 から送信された下りの送信信号をアンテナ 27 を介して受信して復調し、受信データとしてデータ処理部 23 に供給する。データ処理部 23 は受信データの無線フレームを分解し、ホストインターフェース 22 を介してノートパソコン 5 に供給する。 50

【0031】

またデータ処理部23は、ノートパソコン5からホストインターフェース22を介して供給されたアクセスポイント2あての送信データを、無線フレームに構成して送受信部24に供給する。送受信部24は送信データを変調して上りの送信信号を生成し、アンテナ27を介して送信する。

【0032】

また、図5に示すように認証サーバ4においては、CPU31に対し、バス35を介してネットワークインターフェース32、認証に伴う設定値や各種プログラムを記憶するための認証情報記憶手段としてのメモリ33、及びリアルタイムクロック34が接続されている。CPU31は認証制御プログラムに従い、無線LANシステム1における認証処理を実行する。

10

【0033】

(3) 無線LANシステムの認証処理

次に、この無線LANシステム1における認証時の通信シーケンスを、図6に示すシーケンスチャートを用いて詳細に説明する。この通信シーケンスは、IEEE802.11の標準的なものである。

【0034】

アクセスポイント2は、ビーコン(Beacon)と呼ばれるIEEE802.11で規定された制御信号を一定間隔で送信している。このビーコンを受信した無線通信端末3は、アクセスポイント2との通信を開始する。

20

【0035】

上述したようにこの無線LANシステム1においては、認証プロトコルとしてEAPOLを利用する。このEAPOLはEAPパケットと鍵情報とをLAN上で伝送するためのプロトコルであり、実際の認証にはEAP-MD5方式を利用する。

【0036】

まず無線通信端末3は、認証の開始を意味するStartメッセージを、EAPOLパケットに格納し、認証要求としてアクセスポイント2に送信する(すなわち、図6に示すEAPOL[Start])。アクセスポイント2はEAPOLパケットを受信すると、当該パケットに格納されたStartメッセージに従い、EAPプロトコルで規定された16バイトのデータである第1の乱数としてのChallengeをランダムに生成し、これをEAPOLパケットに格納して無線通信端末3に送信する(EAPOL[EAP[Challenge)])。

30

【0037】

無線通信端末3はEAPOLパケットを受信すると、当該パケットに格納されたChallengeと、識別番号としてのユーザID及びパスワードを用いてアクセスポイント2に対する応答を作成する。

【0038】

すなわち無線通信端末3は、ユーザID、パスワード及びChallengeを結合したものを、rfc(request for comments)1321で定義されるMD5関数に入力して16バイトのHash値を生成する。そして無線通信端末3は、ユーザID、第2の乱数としての16バイトの乱数(Nonce)及び生成した応答値としてのHash値(MD5-hash)を、EAPOLパケットに格納してアクセスポイント2に送信する(EAPOL[EAP[ID||Nonce||MD5-hash)])。

40

【0039】

アクセスポイント2はEAPOLパケットを受信すると、先に生成して無線通信端末3に送信したChallengeと、当該EAPOLパケットに含まれるデータ群(ユーザID、16バイトの乱数及びHash値)とをまとめ、RADIUSのAuthentication requestパケットに格納して認証サーバ4に送信する(Challenge||ID||Nonce||MD5-hash)。

【0040】

認証サーバ4はAuthentication requestパケットを受信すると、無線通信端末3に対する認証を開始する。

50

【0041】

認証サーバ4のメモリ33には、各ユーザのユーザID及びパスワードを記憶したユーザ管理テーブルが格納されている。認証サーバ4は、ユーザ管理テーブルからAuthentication requestパケットに含まれていたユーザIDのエントリを検索し、当該ユーザIDに対応するパスワードを抽出する。

【0042】

さらに認証サーバ4は、ユーザID、ユーザ管理テーブルから抽出したパスワード、及びChallengeを結合してMD5関数に入力してHash値を生成し、当該生成したHash値と、Authentication requestパケットに含まれていたHash値とを比較する。この2つのHash値が一致した場合、無線通信端末3は無線LANシステム1の正当なユーザであり、一致しない場合は正当なユーザではないと識別できる。 10

【0043】

このようにして認証サーバ4は無線通信端末3に対する認証を行う。そして無線通信端末3が正当なユーザであると認証した場合、認証サーバ4はPRF (Pseudo Random Function: 疑似乱数生成関数) を用いてマスター鍵を生成する。このマスター鍵は通信路を安全に保つためのセッション鍵であり、PRFにはrfc2104で定義されるHMAC (Keyed-Hashing for Message Authentication) 関数を使用する。マスター鍵Kは次式によって算出される。

【0044】

$K = \text{HMAC}(\text{password}, "key\ expansion" \parallel \text{Challenge} \parallel \text{Nonce}) \dots\dots (1)$ 20

【0045】

そして認証サーバ4は、認証結果(認証OK又はNG)及び生成したマスター鍵を、RADIOUSのAuthentication responseパケットに格納してアクセスポイント2に送信する(OK or NG $\parallel$ K)。ここで、認証サーバ4とアクセスポイント2との間は別途認証されているものとする。またこのとき認証サーバ4は、アクセスポイント2から受信したChallengeを、無線通信端末3のユーザIDに対応付けてユーザ管理テーブルに記憶する。

【0046】

アクセスポイント2はAuthentication responseパケットを受信すると、当該パケット内の認証結果をEAPOLパケットに格納して無線通信端末3に送信する。このときアクセスポイント2は、このEAPOLパケットが改ざんされていないことを証明するためのMIC (Message Integrity Code) をマスター鍵を用いて生成し、当該EAPOLパケットに付加する(EAPOL[EAP[Success or Failure + MIC]])。 30

【0047】

MICは、認証サーバ4から送付されたマスター鍵とEAPOLパケット全体とをHMAC関数に入力したものであり、次式によって算出される。EAPOLパケット内にはMICが含まれるが、当該MICの算出時には、EAPOLパケット内のMICを「0x00」で置き換えて計算する。

【0048】

$\text{MIC} = \text{HMAC}(K, \text{EAPOLパケット全体}) \dots\dots (2)$

【0049】

一方、無線通信端末3も(1)式を用いてマスター鍵を生成する。そして無線通信端末3はEAPOLパケットを受信すると、(2)式を用いてマスター鍵とEAPOLパケットからMICを算出する。このときも、EAPOLパケット内のMICを「0x00」で置き換えて計算する。そして無線通信端末3は、算出したMICと、受信したEAPOLパケットのMICとを比較することにより、当該EAPOLパケットが正しいものか否かを判定してアクセスポイント2を認証する。 40

【0050】

かくして、無線通信端末3とアクセスポイント2の双方についての認証が完了する。この後無線通信端末3及びアクセスポイント2は、暗号化通信を行うための通信鍵を双方で生成する。 50

【0051】

まずアクセスポイント2は、通信鍵を生成するための乱数(random)を生成し、当該 random を EAPOL-KEYメッセージに格納して無線通信端末3に送信する(EAPOL-key[random])。このEAPOL-KEYメッセージは、マスター鍵を用いて暗号化されている。そして無線通信端末3及びアクセスポイント2の双方は、当該random、マスター鍵及びマスター鍵生成時に使用したNonceを用い、次式を用いて通信鍵を生成する。

【0052】

通信鍵 = HMAC (マスター鍵, "Key expansion" || Nonce || random) …… (3)

【0053】

そしてこれ以降、無線通信端末3及びアクセスポイント2は、この通信鍵を使ってデータの暗号化やMICの生成(プロトコルデータの場合)を行う。 10

【0054】

更に無線通信端末3は、アクセスポイント2に帰属するための処理(アソシエーション)を実行する。すなわち無線通信端末3はアクセスポイント2に対してAssociation requestを送信する。このとき無線通信端末3は、通信鍵を使って当該Association requestを暗号化するとともに認証のためMICを付加する。

【0055】

アクセスポイント2はAssociation requestを受信すると、これに付加されたMICを用いて当該Association requestを認証し、Association responseを無線通信端末3に返信するとともに、無線通信端末3のネットワーク利用開始を伝えるAccounting Startを認証サーバ4に送信する。以上でアソシエーションが完了し、以降、外部ネットワーク7との通信の際、アクセスポイント2と無線通信端末3の間は通信鍵によって暗号化される。 20

【0056】

(4) 無線LANシステムのハンドオフ処理

次に、本発明の特徴である無線LANシステム1におけるハンドオフ時の通信シーケンスを、図7に示すシーケンスチャートを用いて詳細に説明する。

【0057】

上述したように従来の無線LANシステムにおいては、図6に示した認証処理をハンドオフ毎に全て繰り返すため、ハンドオフに時間がかかっていた。これに対して本発明の無線LANシステム1においては、ハンドオフ時にマスター鍵を生成する際、Hash値の代わりに初回認証時に用いた認証情報を用いることにより、処理負荷の大きいHash値の算出を回避してハンドオフ時の処理量を減らし、高速にハンドオフを実行し得るようになっている。 30

【0058】

すなわち、本発明を適用したアクセスポイント2から送信されるビーコンには、本発明による高速ハンドオフ機能が有効であるか否かを示すCapability情報が付加されている。無線通信端末3が移動して新たなアクセスポイント2の通信可能範囲に入った場合、当該無線通信端末3は受信したビーコンのCapability情報を参照し、高速ハンドオフが可能であるかを判断する。

【0059】

Capability情報が「無効」である場合、無線通信端末3は図6に示す認証シーケンスを再度実行する。これに対してCapability情報が「有効」である場合、無線通信端末3は次式を用いて新たなマスター鍵Kを生成する。ここで、Challengeは前回の認証時に使用したものであり、Nonceは今回新たに生成した16バイトの乱数、Timestampはビーコンに含まれている8バイトの時間情報である。 40

【0060】

$$K = \text{HMAC}(\text{password}, \text{"key expansion"} || \text{Challenge} || \text{Nonce} || \text{Timestamp}) \dots\dots (4)$$

【0061】

そして無線通信端末3は、高速ハンドオフを要求するRe-startメッセージをEAPOLパケットに格納してアクセスポイント2に送信する。このとき無線通信端末3は、ユーザI 50

D、Nonce 及びTimestamp を当該EAPOLパケットに格納するとともに、新たなマスター鍵を用いてMICを生成し、これを当該EAPOLパケットに付加する（EAPOL[Re-start[ID || Nonce || Timestamp + MIC]]）。

【0062】

EAPOLパケットを受信したアクセスポイント2は、当該パケットに含まれるユーザID、Nonce 及びTimestamp を抽出してRADIUSのAuthenticationrequestパケットに格納し、認証サーバ4に転送する（ID || Nonce || Timestamp）。

【0063】

上述したように認証サーバ4のユーザ管理テーブルには、無線通信端末3のユーザIDと、当該ユーザIDに対応するパスワード及びChallenge が対応付けられて記憶されている。認証サーバ4はAuthentication requestパケットを受信すると、当該パケットに格納されたユーザIDのエントリをユーザ管理テーブルから検索し、当該ユーザIDに対応するパスワード及びChallenge を抽出する。 10

【0064】

そして認証サーバ4は（4）式を用い、当該ユーザ管理テーブルから抽出したパスワード及びChallenge と、Authentication requestパケットに格納されたNonce 及びTimestamp から新たなマスター鍵を生成し、これをRADIUSのAuthentication response パケットに格納してアクセスポイント2に送信する。

【0065】

アクセスポイント2はAuthentication response パケットを受信すると、当該パケットに格納されているマスター鍵を用いて、先に無線通信端末3から受信していたEAPOLパケット（Re-startメッセージ）のMICを算出する。そしてアクセスポイント2は、算出したMICと、EAPOLパケットのMICとを比較することにより、当該EAPOLパケットが正しいものか否かを判定して無線通信端末3を認証する。 20

【0066】

この後、無線通信端末3及びアクセスポイント2は、図6に示した認証時の通信シーケンスと同様に、通信鍵の生成及びアソシエーションを行う。

【0067】

まずアクセスポイント2は、通信鍵を生成するための乱数（random）を生成し、当該randomをEAPOL-KEYメッセージに格納して無線通信端末3に送信する（EAPOL-key[random]）。このEAPOL-KEYメッセージは、新たなマスター鍵を用いて暗号化されている。そして無線通信端末3及びアクセスポイント2の双方は、当該random、新たなマスター鍵及び当該新たなマスター鍵生成時に使用したNonceを用い、（3）式を用いて新たな通信鍵を生成する。 30

【0068】

そしてこれ以降、無線通信端末3及びアクセスポイント2は、この新たな通信鍵を使ってデータの暗号化やMICの生成を行う。

【0069】

このように本発明の無線LANシステム1においては、初回認証時のChallenge を認証サーバ4に記憶しておき、ハンドオフ時、当該Challenge を用いて無線通信端末3に対する認証を行うことにより、処理負荷の大きいHash計算を回避してハンドオフに要する時間を短縮している。 40

【0070】

（5）アクセスポイント、無線通信端末及び認証サーバの制御処理

次に、アクセスポイント2、無線通信端末3及び認証サーバ4それぞれの制御処理を、図7～図11に示すフローチャートを用いて詳細に説明する。

【0071】

まず、アクセスポイント2の通信制御処理について説明する。アクセスポイント2のCPU11は、図7に示すアクセスポイント通信制御処理RT1の開始ステップから入ってステップSP1に移る。ステップSP1においてCPU11は、所定の送信間隔に従ってビ 50

ーコンを送信した後、次のステップ S P 2 に移って無線通信端末 3 からの認証を要求する Start メッセージが格納された E A P O L パケットを待ち受ける。

【0072】

ステップ S P 2 において Start メッセージが格納された E A P O L パケットを受信すると、C P U 1 1 は図 9 に示すサブルーチン S R T 1 の通常認証処理を実行する。

【0073】

すなわち C P U 1 1 は、サブルーチン S R T 1 の開始ステップから入ってステップ S P 1 1 に移り、Challenge を生成した後これを E A P O L パケットに格納して無線通信端末 3 に送信し、次のステップ S P 1 2 に移る。

【0074】

ステップ S P 1 2 において C P U 1 1 は、無線通信端末 3 から送信された応答パケットに含まれるユーザ I D、Nonce 及び H a s h 値を、Authentication request パケットに格納して認証サーバ 4 に転送し、次のステップ S P 1 3 に移る。

【0075】

ステップ S P 1 3 において C P U 1 1 は、送信した Authentication request パケットに対する Authentication response パケットを受信すると、当該パケットから無線通信端末 3 についての認証結果及びマスター鍵を取得し、次のステップ S P 1 4 に移る。

【0076】

ステップ S P 1 4 において C P U 1 1 は、Authentication response パケットから取得した認証結果に基づき、無線通信端末 3 に対する認証が成功したか否かを判断する。ステップ S P 1 4 において無線通信端末 3 に対する認証が成功したと判断した場合、C P U 1 1 はステップ S P 1 5 に移り、認証成功を示す応答の E A P O L パケットを生成するとともに、当該 E A P O L パケットに対してマスター鍵を用いた M I C を付加し、次のステップ S P 1 7 に移る。

【0077】

これに対してステップ S P 1 4 において無線通信端末 3 に対する認証が失敗したと判断した場合、C P U 1 1 はステップ S P 1 6 に移り、認証失敗を示す応答の E A P O L パケットを生成するとともに、当該 E A P O L パケットに対してマスター鍵を用いた M I C を付加し、ステップ S P 1 7 に移る。

【0078】

そして、ステップ S P 1 7 において C P U 1 1 は、生成した E A P O L パケットを無線通信端末 3 に送信し、次のステップ S P 2 8 で処理を終了して図 8 に示すアクセスポイント通信制御処理手順 R T 1 のステップ S P 4 に移る。

【0079】

一方、アクセスポイント通信制御処理手順 R T 1 のステップ S P 2 において、認証を要求する EAPOL[Start] パケットを受信しなかった場合、C P U 1 1 はステップ S P 3 に移り、無線通信端末 3 からのハンドオフを要求する ReStart メッセージを格納した E A P O L パケットを待ち受ける。ステップ S P 3 において E A P O L パケットを受信しなかった場合、C P U 1 1 はステップ S P 1 に戻って再度ビーコンを送信する。

【0080】

これに対して、ステップ S P 3 において E A P O L パケットを受信すると、C P U 1 1 は図 10 に示すサブルーチン S R T 2 のハンドオフ認証処理を実行する。

【0081】

すなわち C P U 1 1 は、サブルーチン S R T 2 の開始ステップから入ってステップ S P 2 1 に移り、無線通信端末 3 からの ReStart メッセージを格納した E A P O L パケットに含まれるユーザ I D、Nonce 及び Timestamp を Authentication request パケットに格納して認証サーバ 4 に転送し、次のステップ S P 2 2 に移る。

【0082】

ステップ S P 2 2 において C P U 1 1 は、送信した Authentication request パケットに対する Authentication response パケットを受信すると、当該パケットから新たなマスター

10

20

30

40

50

鍵を取得し、次のステップ S P 2 3 に移る。

【0083】

ステップ S P 2 3 において C P U 1 1 は、取得したマスター鍵を用いて、ReStart メッセージが格納された E A P O L パケットの M I C を算出し、次のステップ S P 2 4 に移る。そして、ステップ S P 2 4 において C P U 1 1 は、算出した M I C と Authentication response に付加された M I C とを比較することにより無線通信端末 3 に対する認証を行う。

【0084】

ステップ S P 2 4 において、算出した M I C と Authentication response パケットに付加された M I C とが一致し、無線通信端末 3 に対する認証が成功した場合、C P U 1 1 はステップ S P 2 5 に移り、認証成功を示す応答の E A P O L パケットを生成するとともに、当該 E A P O L パケットに対してマスター鍵を用いた M I C を付加して次のステップ S P 2 7 に移る。

10

【0085】

これに対してステップ S P 2 4 において、算出した M I C と Authentication response パケットに付加された M I C とが一致せず、無線通信端末 3 に対する認証が失敗した場合、C P U 1 1 はステップ S P 2 6 に移り、認証失敗を示す応答の E A P O L パケットを生成するとともに、当該 E A P O L パケットに対してマスター鍵を用いた M I C を付加してステップ S P 2 7 に移る。

【0086】

そして、ステップ S P 2 7 において C P U 1 1 は、生成した応答の E A P O L を無線通信端末 3 に送信し、次のステップ S P 2 8 で処理を終了して図 8 に示すアクセスポイント通信制御処理手順 R T 1 のステップ S P 4 に移る。

20

【0087】

ステップ S P 4 において C P U 1 1 は、無線通信端末 3 に対する認証の成否を判断する。ステップ S P 4 において、無線通信端末 3 に対する認証が失敗した場合、C P U 1 1 はステップ S P 1 に戻って再度ビーコンを送信する。これに対してステップ S P 4 において、無線通信端末 3 に対する認証が成功した場合、C P U 1 1 は次のステップ S P 5 に移る。

【0088】

C P U 1 1 は、ステップ S P 5 において random を生成した後ステップ S P 6 に移り、マスター鍵を用いて当該生成した random を暗号化するとともに M I C を付加し、次のステップ S P 7 に移る。

30

【0089】

C P U 1 1 は、ステップ S P 7 において暗号化した random を E A P O L パケットに格納して無線通信端末 3 に送信した後、ステップ S P 8 に移り、random、マスター鍵、及び当該マスター鍵に使用した Nonce を用いて通信鍵を生成し、次のステップ S P 9 に移る。

【0090】

そして、ステップ S P 9 において C P U 1 1 はアソシエーション処理を実行し、当該アソシエーションの完了後、データ通信を開始する。

【0091】

次に、無線通信端末 3 の端末通信制御処理について説明する。無線通信端末 3 の C P U 2 1 は、図 10 に示す端末通信制御処理 R T 2 の開始ステップから入ってステップ S P 3 1 に移る。ステップ S P 3 1 において C P U 2 1 は、アクセスポイント 2 から送信されるビーコンを待ち受け、当該ビーコンを受信すると次のステップ S P 3 2 に移る。

40

【0092】

ステップ S P 3 2 において、C P U 2 1 はハンドオフの実行／非実行を判断する。ステップ S P 3 2 において、無線通信端末 3 がまだ認証サーバによる認証を受けていないか、あるいはハンドオフを行わないと C P U 2 1 が判断した場合、当該 C P U 2 1 はステップ S P 3 3 に移る。

【0093】

ステップ S P 3 3 において C P U 2 1 は、認証を要求する Start メッセージを E A P O L

50

パケットに格納してアクセスポイント2に対して送信し、次のステップSP34に移る。ステップSP34においてCPU21は、アクセスポイント2から送信されるChallengeが格納されたEAPOLパケットを待ち受け、受信した当該EAPOLパケットからChallengeを取得して次のステップSP35に移る。

【0094】

ステップSP35において、端末側応答値生成手段及び端末側暗号鍵生成手段としてのCPU21は、ユーザID、パスワード及び取得したChallengeを結合してMD5関数に入力することにより応答値としてのHash値を計算するとともに、16バイトの乱数Nonceを生成し、更にパスワード、Challenge及びNonceを用いてマスター鍵を生成して次のステップSP36に移る。

10

【0095】

ステップSP36において、認証要求手段としてのCPU21は、ユーザID、Nonce及びHash値をEAPOLパケットに格納してアクセスポイント2に送信し、次のステップSP37に移る。ステップSP37においてCPU21は、アクセスポイント2から送信される認証結果が格納されたEAPOLパケットを待ち受け、これを受信するとステップSP38に移る。

【0096】

ステップSP38においてCPU21は、受信したEAPOLパケットのMICに基づいて当該パケットの正偽を判断し、当該パケットが不正なものであると判断した場合、ステップSP31に戻って再度ビーコンを待ち受けるのに対し、当該パケットが正当なものであると判断した場合、次のステップSP39に移る。

20

【0097】

ステップSP39においてCPU21は、当該パケットの認証結果の内容を判断する。そしてCPU21は、当該パケットの認証結果が「認証失敗」である場合、ステップSP31に戻って再度ビーコンを待ち受けるのに対し、当該パケットの認証結果が「認証成功」である場合、次のステップSP40に移る。

【0098】

一方、ステップSP32においてハンドオフを行うとCPU21が判断した場合、当該CPU21はステップSP44に移る。

【0099】

ステップSP44において、端末側暗号鍵生成手段としてのCPU21は、乱数Nonceを新たに生成し、当該Nonce、前回の認証時に用いたChallenge及びビーコンに含まれるTimestampを用いて新たなマスター鍵を生成し、次のステップSP45に移る。

30

【0100】

ステップSP45においてCPU21は、ハンドオフを要求するRe-StartメッセージをEAPOLパケットに格納するとともに、新たなマスター鍵を用いて当該EAPOLパケットにMICを付加し、次のステップSP46に移る。

【0101】

そしてCPU21は、ステップSP46においてEAPOLパケットを送信した後ステップSP40に移る。

40

【0102】

ステップSP40においてCPU21は、アクセスポイント2から送信されるrandomが格納されたEAPOLパケットを待ち受け、これを受信すると次のステップSP41に移る。

【0103】

ステップSP41においてCPU21は、受信したEAPOLパケットのMICに基づいて当該パケットの正偽を判断し、当該パケットが不正なものであると判断した場合、ステップSP31に戻って再度ビーコンを待ち受けるのに対し、当該パケットが正当なものであると判断した場合、次のステップSP42に移る。

【0104】

50

ステップ S P 4 2 において C P U 2 1 は、受信した E A P O L パケットに格納された random、ステップ S P 3 5 で生成したマスター鍵、及び当該マスター鍵に使用した Nonce を用いて通信鍵を生成し、次のステップ S P 4 3 に移る。

【0105】

そして、ステップ S P 4 3 において C P U 2 1 は生成した通信鍵を用いてアソシエーション処理を実行し、当該アソシエーションの完了後、データ通信を開始する。

【0106】

次に、認証サーバ 4 の認証制御処理について説明する。認証サーバ 4 の C P U 3 1 は、図 1 2 に示す認証制御処理 R T 3 の開始ステップから入ってステップ S P 5 1 に移る。ステップ S P 5 1 において C P U 3 1 は、アクセスポイント 2 からのパケットを待ち受け、当該パケットを受信すると次のステップ S P 5 2 に移り、受信したパケットの種類を判別する。 10

【0107】

ステップ S P 5 2 において、受信したパケットが Authentication Request パケットであり、かつ challenge を含んでいる場合、当該パケットは無線通信端末 3 に対する認証要求であり、このとき C P U 3 1 はステップ S P 5 3 に移る。

【0108】

ステップ S P 5 3 において、サーバ側応答値生成手段としての C P U 3 1 は、受信した Authentication Request パケットに含まれているユーザ I D に対応するパスワードをユーザ管理テーブルから抽出し、ユーザ I D、パスワード及び受信した Authentication Request パケットに格納されている challenge を用いて応答値としての H a s h 値を生成するとともに、パスワード、challenge 及び Authentication Request パケットに格納されている Nonce を用いてマスター鍵を生成し、次のステップ S P 5 4 に移る。 20

【0109】

ステップ S P 5 4 において、認証手段としての C P U 3 1 は、算出した H a s h 値と、Authentication Request パケットに格納されている H a s h 値とを比較することにより無線通信端末 3 に対する認証を行う。

【0110】

ステップ S P 5 4 において 2 つの H a s h 値が等しい場合、このことは無線通信端末 3 が無線 LAN システム 1 の正当なユーザであることを表しており、この時 C P U 3 1 はステップ S P 5 5 に移り、認証 O K を示す認証結果及びマスター鍵を Authentication Response パケットに格納し、ステップ S P 3 1 に戻る。 30

【0111】

これに対して S P 5 4 において 2 つの H a s h 値が異なる場合、このことは無線通信端末 3 が無線 LAN システム 1 の正当なユーザではないことを表しており、この時 C P U 3 1 はステップ S P 5 6 に移り、認証 N G を示す認証結果及びマスター鍵を Authentication Response パケットに格納し、ステップ S P 3 1 に戻る。

【0112】

一方ステップ S P 5 2 において、受信したパケットが Authentication Request パケットであり、かつ Timestamp を含んでいる場合、当該パケットは無線通信端末 3 によるハンドオフ要求であり、このとき C P U 3 1 はステップ S P 5 7 に移る。 40

【0113】

ステップ S P 5 7 において C P U 3 1 は、受信した Authentication Request パケットに含まれているユーザ I D に対応する Challenge をユーザ管理テーブルから抽出し、パスワード、challenge 及び Authentication Request パケットに格納されている Nonce を用いて新たなマスター鍵を生成して次のステップ S P 5 8 に移る。

【0114】

そして、ステップ S P 5 6 において C P U 3 1 は生成した新たなマスター鍵を Authentication Response パケットに格納し、ステップ S P 3 1 に戻る。

【0115】

またステップ S P 5 2 において、受信したパケットが Accounting-start パケットである場合、当該パケットは無線通信端末 3 によるアカウントリング要求であり、このとき C P U 3 1 はステップ S P 5 9 に移り、アカウントリング処理を実行した後ステップ S P 3 1 に戻る。

【0116】

(6) 動作及び効果

以上の構成において認証サーバ 4 は、無線通信端末 3 に対する認証時、当該無線通信端末 3 から送信された Challenge を、パスワードとともにユーザ I D に対応付けてメモリ 3 3 内のユーザ管理テーブルに記憶しておく。

【0117】

そして無線通信端末 3 がハンドオフする際、当該無線通信端末 3 は、パスワード、前回の認証時に使用した Challenge、新たに生成した Nonce 及びビーコンに含まれる Timestamp を用いて新たなマスター鍵を生成する。

【0118】

そして無線通信端末 3 は、ハンドオフを要求する Re-start メッセージを含む E A P O L パケットにユーザ I D、Nonce 及び Timestamp を格納するとともに、新たなマスター鍵を用いて M I C を生成し、これを当該 E A P O L パケットに付加し、ハンドオフ先のアクセスポイント 2 を介して認証サーバ 4 に送信する。

【0119】

認証サーバ 4 は、無線通信端末 3 から送信されたユーザ I D に対応するパスワード及び Challenge をユーザ管理テーブルから検索して取得し、当該取得したパスワード及び Challenge と無線通信端末 3 から送信された Nonce 及び Timestamp から新たなマスター鍵を生成し、これをアクセスポイント 2 に送信する。

【0120】

アクセスポイント 2 は認証サーバ 4 から送信された新たなマスター鍵を用いて、先に無線通信端末 3 から受信していた E A P O L パケット (Re-start メッセージ) の M I C を算出し、当該算出した M I C と、E A P O L パケットに付加されていた M I C とを比較することにより、当該 E A P O L パケットが正しいものか否かを判定して無線通信端末 3 を認証し、これらが一致した場合、無線通信端末 3 が無線 L A N システム 1 の正当なユーザであると認証してハンドオフを許可する。

【0121】

以上の構成によれば、無線通信端末 3 に対する初回認証時に、当該無線通信端末 3 から送信された Challenge をパスワードとともにユーザ I D に対応付けてユーザ管理テーブルに記憶しておき、無線通信端末 3 がハンドオフする際、当該無線通信端末 3 のユーザ I D に対応するパスワード及び Challenge をユーザ管理テーブルから取得してこれを用いて新たなマスター鍵を生成し、当該新たなマスター鍵を用いてアクセスポイントで認証を行うようにしたことにより、処理負荷の大きい H a s h 計算を省くとともに認証に伴うやりとりを削減し、これによりハンドオフに要する時間を短縮することができる。

【0122】

またハンドオフ時、アクセスポイント 2 から送信されるビーコンの Timestamp を用いてマスター鍵を生成することにより、悪意ある第 3 者がパケットを傍受して再送することによるハッキングを防止することができる。

【0123】

(7) 他の実施の形態

なお、上述の実施の形態においては、無線通信端末として P C カード型の無線 L A N カードに本発明を適用した場合について述べたが、本発明はこれに限らず、例えば U S B (Universal Serial Bus) 接続等の外付け型無線 L A N 端末や、あるいはノートパソコン等の情報処理装置に一体で内蔵された無線 L A N 端末に本発明を適用してもよい。

【0124】

また上述の実施の形態においては、アクセスポイント 2、無線通信端末 3 及び認証サーバ

10

20

30

40

50

4が、それぞれのメモリに記憶されている制御プログラムに従ってそれぞれの制御処理を実行するようにしたが、本発明はこれに限らず、上述したプログラムが格納されているプログラム格納媒体をインストールすることにより、上述の各制御処理を実行するようにしてもよい。

【0125】

この場合、上述したプログラムをインストールするためのプログラム格納媒体としては、例えばC D - R O M (Compact Disk-Read Only Memory) やD V D (Digital Versatile Disk) 等のパッケージメディアのみならず、プログラムが一時的又は永続的に格納される半導体メモリや磁気ディスク等で実現しても良い。また、これらプログラム格納媒体にプログラムを格納する手段としては、ローカルエリアネットワークやインターネット、デジタル衛星放送等の有線及び無線通信媒体を用いても良い。 10

【0126】

【発明の効果】

上述のように本発明によれば、無線通信端末に対する初回認証時に、当該無線通信端末から送信された乱数をパスワードとともに識別番号に対応付けて認証情報記憶手段に記憶しておき、無線通信端末がハンドオフする際、当該無線通信端末の識別番号に対応するパスワード及び乱数を取得して新たな暗号鍵を生成するとともに、無線通信端末でも新たな暗号鍵を生成し、この2つの暗号鍵に基づいてアクセスポイントで認証を行うようにしたことにより、認証に伴う処理及びやりとりを削減し、これにより簡易な手順で高速にアクセスポイント間のハンドオフを実行することができる。 20

【図面の簡単な説明】

【図1】本発明の一実施の形態による無線LANシステムの全体構成を示す略線図である。

【図2】無線LANシステムのプロトコルスタックを示す図である。

【図3】アクセスポイントの回路構成を示すブロック図である。

【図4】無線通信端末の回路構成を示すブロック図である。

【図5】認証サーバの回路構成を示すブロック図である。

【図6】認証時の通信シーケンスを示すシーケンスチャートである。

【図7】ハンドオフ時の通信シーケンスを示すシーケンスチャートである。

【図8】アクセスポイント通信制御処理手順を示すフローチャートである。 30

【図9】通常認証処理手順を示すフローチャートである。

【図10】ハンドオフ認証処理手順を示すフローチャートである。

【図11】端末通信制御処理手順を示すフローチャートである。

【図12】認証制御処理手順を示すフローチャートである。

【符号の説明】

1 ……無線LANシステム、2 ……アクセスポイント、3 ……無線通信端末、4 ……認証サーバ、5 ……ノートパソコン、6 ……有線ネットワーク、7 ……外部ネットワーク、11、21、31 ……CPU、12、32 ……ネットワークインターフェース、13、23 ……データ処理部、14、24 ……送受信部、15、26、33 ……メモリ、16、26、34 ……リアルタイムクロック、17、27 ……アンテナ、35 ……バス。 40

【図 1】

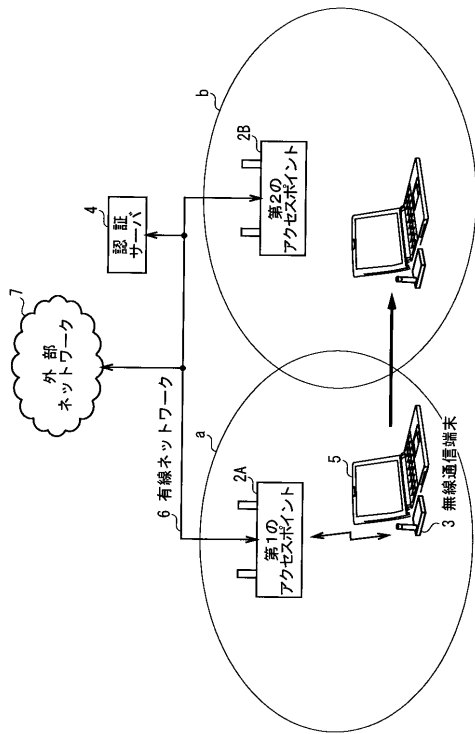


図 1 本発明による無線LANシステム

【図 2】

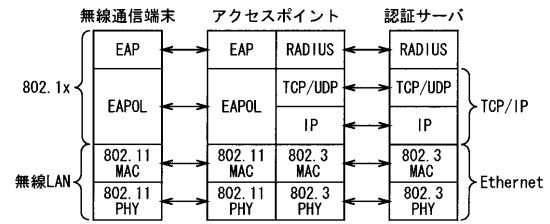


図 2 無線LANシステムのプロトコルスタック

【図 3】

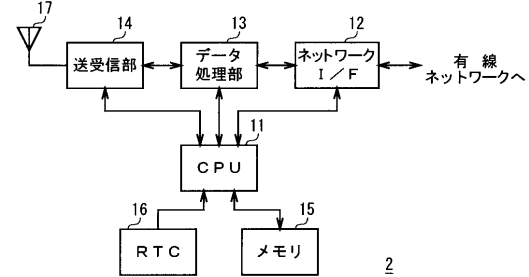


図 3 アクセスポイントの構成

【図 4】

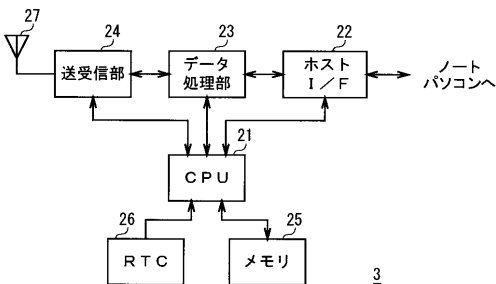


図 4 無線通信端末の構成

【図 5】

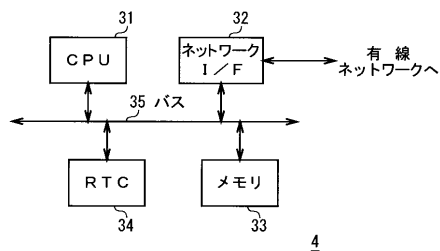


図 5 認証サーバの構成

【図 6】

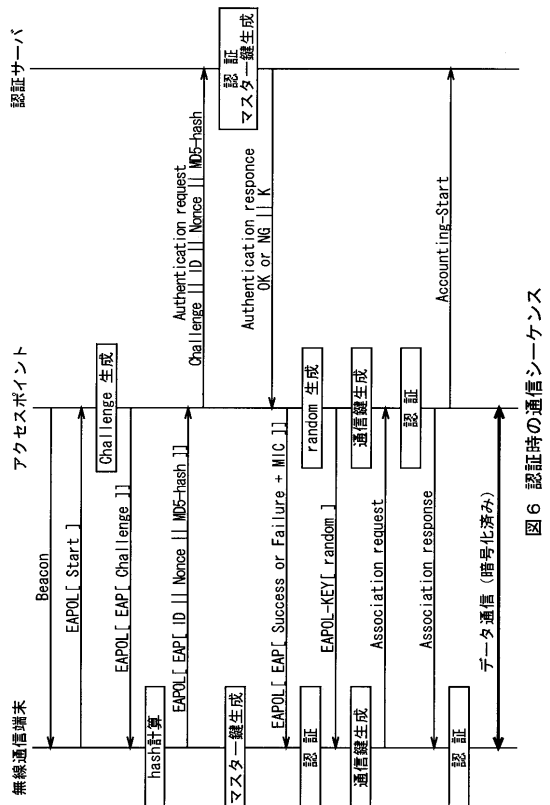


図 6 認証時の通信シーケンス

【図 7】

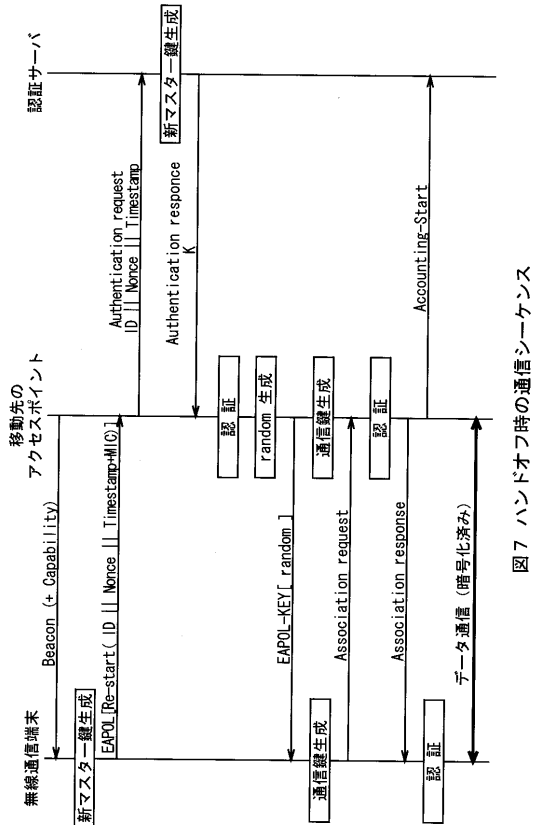


図 7 ハンドオフ時の通信シーケンス

【図 8】

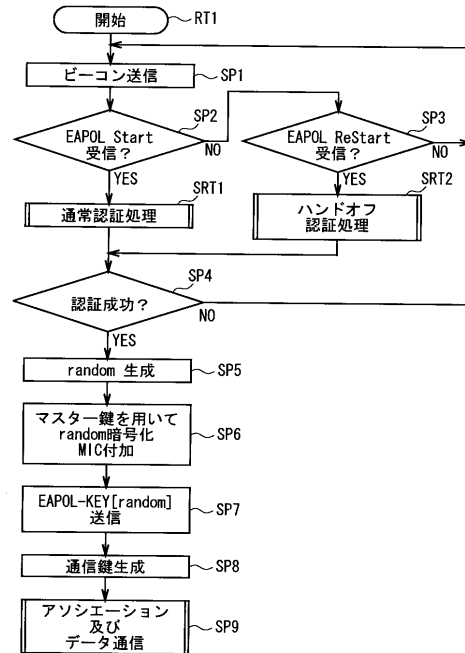


図 8 アクセスポイント通信制御処理手順

【図 9】

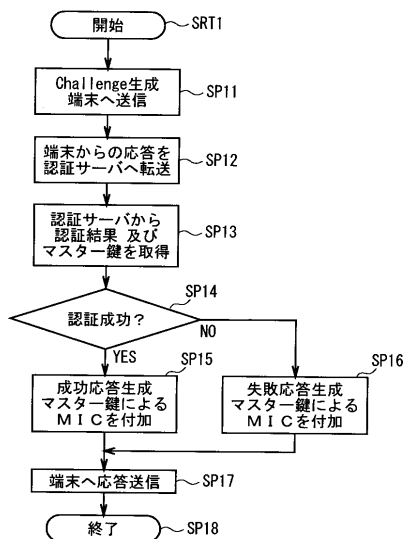


図 9 通常認証処理手順

【図 10】

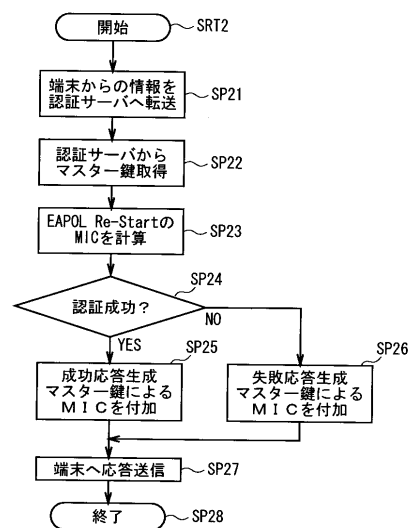


図 10 ハンドオフ認証処理手順

【図 1 1】

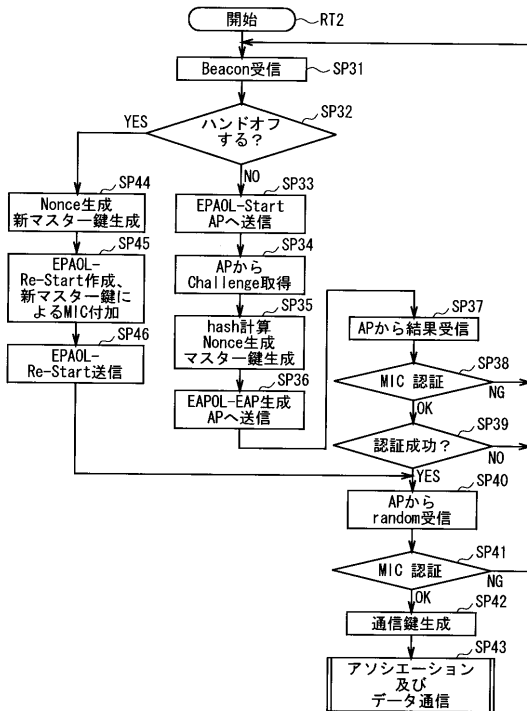


図 1 1 端末通信制御処理手順

【図 1 2】

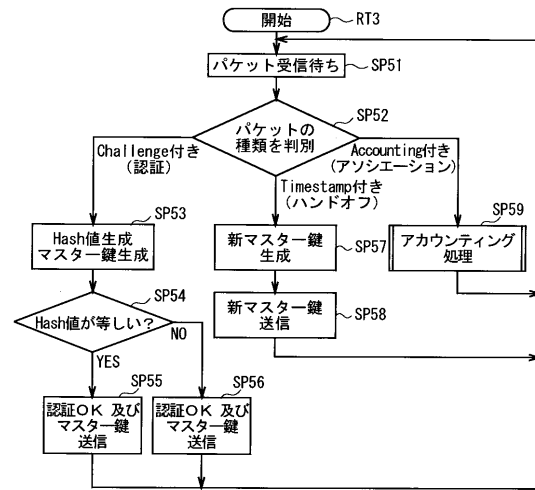


図 1 2 認証制御処理手順