マルチメディア通信と分散処理 107－2
（２００２．３．２８）

無線インターネットサービスに必要なセキュリティを提供する高速認証システム

藤川 賢治[†]　中野 博樹[††]　太田 昌孝[†††]　平原 正樹[‡]
真野 浩[‡‡]　池田 克夫[‡‡‡]
[†]京都大学　[††](株)トランス・ニュー・テクノロジー
[†††]東京工業大学　[‡](財)九州システム情報技術研究所
[‡‡]モバイルインターネットサービス(株)　[‡‡‡]大阪工業大学

無線インターネットサービスを提供することを前提に、無線アクセス区間で強固なセキュリティ機能を持つ高速認証システムを設計し、実装、評価した。まず無線インターネットサービスのセキュリティ確保の重要性について述べ、無線端末の認証、パケットの認証と暗号化のためのセッションキーの交換、基地局の認証が必要であることを明らかにする。そして、無線端末と認証サーバとの間で１往復のメッセージを交換するだけで、無線端末の認証、セッションキーの交換、基地局の認証、ネットワーク情報の取得のすべてを行う高速認証システムを提案する。また無線アクセス技術としてIEEE802.11b を用いて、提案する高速認証システムを実装した。システムで用いられる認証サーバの性能測定の結果、実際にサービスを行うのに十分な性能を得られた。

A Fast Authentication System for Secure Wireless Internet Services

FUJIKAWA Kenji[†]　NAKANO Hiroki[††]
OHTA Masataka[†††]　HIRABARU Masaki[‡]
MANO Hiroshi[‡‡]　IKEDA Katsuo[‡‡‡]
[†]Kyoto University　[††]Trans New Technology, Inc.
[†††]Tokyo Institute of Technology
[‡]Institute of Systems & Information Technologies/KYUSHU
[‡‡]Mobile Internet Services, Inc.　[‡‡‡]Osaka Insitute of Technology

We design and implement a fast authentication system with robust security on wireless accesses, for the purpose of providing wireless Internet services. First, we address the importance of providing security for wireless Internet services, and clarify that authentication of wireless terminals, session-key exchange for authentication and encryption of packets, and authentication of base stations are necessary. Then, we propose a fast authentication system that realizes authentication of wireless terminals, session-key exchange, authentication of base stations and retrieval of network information, just by exchanging one round-trip message. We implemented our proposed system using IEEE802.11b as a wireless access technology. As a result of performance measurement of an authentication server, which is used in our system, it is shown that the authentication server has sufficient ability for providing actual services.

1. はじめに

IEEE802.11b[1] などの無線 LAN を利用し、人の集る場所、いわゆるホットスポットや、街角でインターネット接続サービスをする動きが活性化している。これらを商用サービスとして提供する場合、無線アクセスのセキュリティ確保が重要な要素となる。ところがこの重要性が十分に認識されず、サービスが提供されようとしているのが現状である。

本稿ではまず無線インターネットサービスのセキュリティ確保の重要性について述べ、無線アクセス上で強固なセキュリティを提供する認証システムを提案する。この際、無線端末が基地局を次々と切り替えることがあること、及びインターネット電話の使用を考慮に入れて、高速な認証が行えるシステムを提案する。そして提案する高速認証システムを実装し評価を行う。

以下、2 章でセキュリティの必要性について論じ、3 章で想定するネットワークインフラについて述べる。4 章で高速認証システムを設計する。5 章で本システムと既存システムを比較する。6 章で実装について述べ、7 章で実験を行い評価する。

2. セキュリティの必要性

まず三つの観点から無線インターネットサービスのセ

キュリティの必要性について論じ、そして要件を明かにする。

2.1 社会的観点からのセキュリティの必要性

無線インターネット接続は、公園の水飲み場と同じく公共物であり、無料で不特定多数に提供すればよい、という考え方もある。事実シンガポールのチャンギ国際空港は無料で不特定多数に無線インターネット接続が提供されており、世界各地でこのような動きが見られる。しかし我々はこれらは非常に危険な方向だと考える。

これまでの有線インターネットも非常に匿名性の高いメディアであった。しかしそれでも、あるIPアドレスが犯罪に利用されたときに、利用者を特定することができた。例えばあるIPアドレスがSPAMやウィルスメールを送信するのに使われた場合、通信事業者に当局が問い合わせることで、利用者を特定できる。

無線インターネットの不特定多数への提供は、本人特定を全く不可能にする。日本では身代金目的の誘拐事件の連絡にプリペイド携帯電話が使われて、その匿名性が問題となったが、全く同じことが起こると予想される。すなわちウィルスメールの送付、犯罪の連絡などに利用されるであろう。

よって誰がいつどのIPアドレスを利用し通信したかという記録が残るサービスを提供するのが電気通信事業者の責務である。これは電気通信事業法[2]第四十八条の二やプロバイダ責任法[3]第四条に照らしても妥当である。これにより無線インターネット利用者からインターネットを保護することができる。

2.2 サービス提供者の観点からのセキュリティの必要性

次に無線アクセスサービス提供者、すなわち通信事業者の観点から考える。

サービスであるため、ユーザから利用料金を徴収し、それを設備投資やアカウント管理に充てることになる。

このとき利用料金を払わないユーザが利用できるシステムではサービスが成り立たなくなってしまう。よって不正使用を防止する仕組み、すなわちユーザ認証を行い、成りすましを防ぐことが必要不可欠である。

2.3 ユーザの観点からのセキュリティの必要性

有線と違い、無線は盗聴が容易である。よって有線と同レベルの安全性を保証するには、無線アクセス区間での暗号化、しかもユーザごとの個別の暗号化が必要となる☆。

もう一つ忘れてならないのは、偽の基地局に繋がされないようにする仕組みが必要であることである。これは非常に重要なセキュリティ要素なのであるが、既存システムではほとんど考慮されていないのが現状である。

有線のアクセス網なら特に工夫せずとも、接続先は正当なサービス提供者であると信頼できるが、無線の場合は何らかの仕組みを導入しないと、接続先が正当なサービス提供者であると信頼できない。ユーザが偽の基地局に接続させられると、さらに偽のインターネットへ接続させられる可能性が出てくる。

例えば、正当なサービス事業者のそばで偽の基地局を立ち上げ、ユーザを偽のインターネットに接続させたとする。そのとき実在する銀行や証券会社に類似のWWWページを用意しておき、ユーザがそれらのページへのユーザアカウントとパスワードを入力することで、それらの情報を容易に盗むことができる。これらの本物のページではSSL[6]を使うことが一般的であるが、接続のたびにSSLで接続していることを確認する(URLがhttps:で始まることや、証明書を確認する)ユーザは現実には皆無であるため、このようなことが容易に可能である。

また無線区間の暗号化はインターネット接続のさい、偽のサイトへの接続を防止するという意味でも重要である。もし無線区間の暗号化がなければ、偽の基地局に接続させなくても、偽のWWWページなど、偽のサイトへ無線端末を接続させることができる。例えば次のような方法である。

ユーザが接続するサイトのホスト名を指定すると、無線端末はそれをIPアドレスに変換すべく、DNSのqueryメッセージを送信する。このとき、無線アクセス網を盗聴することでqueryメッセージの内容を知り、正しいDNSのreplyメッセージが返ってくる前に偽のreplyメッセージを送信することで、無線端末を任意のサイトに接続させてしまえる。現在の有線のインターネットのDNSが信頼できるのは、あくまで有線のアクセス網は盗聴されないという前提があるからである。

この他にもアクセス網を盗聴することで偽のサイトに接続させる様々な手法が存在するが、無線アクセス網での暗号化によりこれらを回避できる。

2.4 セキュリティ機能の要件

以上まとめると、提供されるべきセキュリティ機能は、

(1) 無線端末の認証(利用者の同定及び不正利用の排除)
(2) 無線区間暗号化
(3) 基地局の認証(偽の基地局への接続抑止)

となる。

また認証や暗号化に際しては、

- 無線端末ごとに異なる鍵を用いて、
- パケット単位で行う

ことが重要である。無線端末ごとに異なる鍵を用いなければ、鍵を共有する端末からの不正利用や盗聴が防げず、パケット単位で認証を行わなければ、無線端末の認証が成功したあと、成りすましによる不正利用が可能となってしまう。

以降、上記要件の提供を考え、無線アクセス区間の認証手順を設計する。

3. 想定するネットワークインフラ

無線インターネットを提供することを念頭に単純なネッ

☆ ただし端末が、必ず接続先とあらかじめ交換した鍵によって暗号化する場合はこの限りではない。IPSec[4]によるVPNやSSH[5]のポートフォワーディングを常に行っている場合などである。

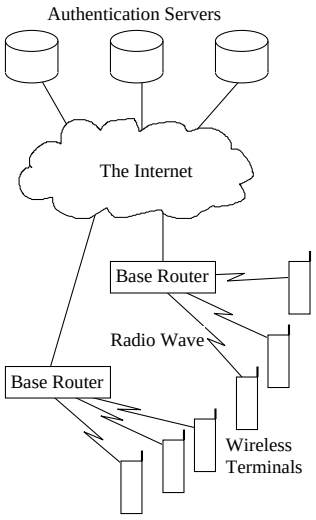


図 1　想定するネットワークインフラ

トワークインフラを考える。IP プロトコルによりインターネットさえ使用できればいいため、無線基地局はそれ自体がルータ (レイヤ 3 スイッチ) となるものを考える (図 1)。これは基地局で認証などの複雑な処理をしないといけないため、基地局をレイヤ 2 スイッチにすることによる一般的な利点、例えば機器コストの削減や運営コストの削減という効果がないためである。逆に基地局をルータとすることで、余分なブロードキャストパケットを配信せずに済むという利点も生まれる☆。無線端末と基地局ルータは point-to-point 接続で結ばれ、無線端末間の通信は必ず基地局経由で行われる。

またインターネット上には、無線端末を認証する認証サーバも置かれる。認証サーバの必要性やその動作については 4 章で述べる。

現在のシステムの実装は無線アクセス技術として現在最もコストパフォーマンスのよい IEEE802.11b を使っている。ただし本稿で提案するシステムはこれに特化したものではなく、その他の無線アクセス技術に適用可能である。

4. 高速認証システムの設計

2.4 節で述べたセキュリティ機能を提供し、かつ同時に DHCP や PPP で得られるネットワーク情報、すなわち IP アドレスやデフォルトゲートウェイ等の情報も取得する高速な認証手順を提案する。ここで高速性は必須の項目である。なぜならユーザが移動しながら無線インターネットを利用する場合、移動により、次々と基地局を変更することが考えられるためである。特にインターネット電話の利用において高速性は重要である。

認証手順中には行われる 5 項目について述べ、2.4 節のセキュリティとの関連を述べる。

(1) 基地局の存在の通知と発見

(2) 無線端末の認証
これにより 2.4 節 (1) の 無線端末の認証 (利用者の同定) が行われる。

(3) セッションキー (詳細は後述) の交換
これにより 2.4 節 (1) の認証 (不正利用の排除) 及び (2) の暗号化が行えるようになる。

(4) 基地局の認証
これにより 2.4 節 (3) の基地局の認証が行われる。

(5) ネットワーク情報の取得

以下、各項目の動作について説明し、最後にそれらを統合したプロトコルを提案する。

4.1 基地局の存在の通知と発見

基地局の存在の通知は基地局が定期的にビーコンとなるメッセージをブロードキャストすることによって行う (図 2)。これは IEEE802.11[7] のインフラストラクチャモードなど一般的な無線システムで行われている手法である。無線端末はビーコンメッセージを受け取ることで基地局を発見する。

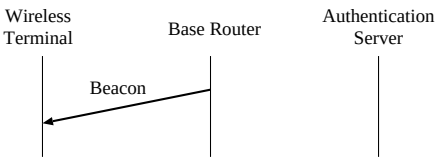


図 2　ビーコンの送出

4.2 無線端末の認証

無線端末の認証は、原理的には、各無線端末が利用できる全ての基地局との間とで鍵を交換しておけば実現できる。しかしこれでは無線端末数と基地局数の積の数の鍵が必要になってしまい、現実的ではない。

そこでダイヤルアップインターネット接続で一般的に行われている RADIUS[8] などの認証サーバによる認証、特に PAP よりも安全な CHAP を参考にする。

認証サーバと無線端末とはあらかじめ秘密の鍵を交換しておくこととする。必要な鍵の数は無線端末の数となる。

各基地局と認証サーバはあらかじめ秘密の鍵を交換しておくことで、安全な通信路を確保しておくものとする。(この安全な通信路の確保は RADIUS で一般に行われていることなので、本稿では以降言及しない。)

提案する認証の手順は以下のようになる (図 3)。なおメッセージ中には無線端末の識別子も含まれるが説明の簡略化のため省略した。

(1) 基地局は現在時刻 t を含めたパケットをブロードキャストする。

(2) 無線端末は、認証サーバとの間であらかじめ交換してある秘密鍵 k を用いて t を一方向性ハッシュ関数でハッシュした値 $H_k(t)$ を計算し、t と共に認証要求メッセージとして基地局に送信する。具体的なハッシュ関数としては HMAC-MD5[9] など

☆ 実際にレイヤ 2 スイッチの複数の無線基地局でネットワークを構成すると、そのブリッジ機能により、ネットワーク上を多数のブロードキャスフレームがブロードキャストされ、帯域が浪費されてしまう。また Windows 系の OS の問題ではあるが、共有フォルダが他人に見えてしまうことや、それによるウィルスの感染も、実用上は大きな問題である。

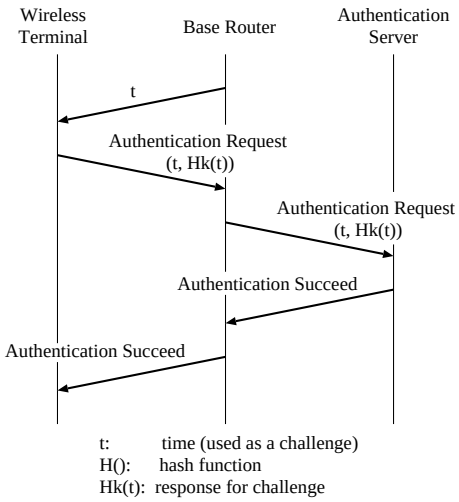


図 3　無線端末の認証

が考えられる。

(3) 基地局は t が最近のものであった場合のみ $H_k(t)$ と t との組を認証サーバに転送する。

(4) 認証サーバは受け取った t から独自に $H_k(t)$ を計算し、受け取ったものと同じである場合にのみ、基地局に認証成功メッセージを送る。(失敗の場合の挙動は省略する)

(5) 基地局は認証成功メッセージを受け取った場合、無線端末に認証成功メッセージを転送する。

以上の手順により無線端末の認証が完了し、以降、無線端末は基地局ルータを介してインターネットへの通信が可能になる。

t と $H_k(t)$ はそれぞれ、CHAP における challenge と response にあたり、無線区間が盗聴されていたとしても秘密鍵が知られることはない。また基地局は秘密鍵が何であるか知ることなく無線端末の認証が行える。

単調増加する値である現在時刻 t を用いることで、replay attack にも対処する。一定の時間が過ぎれば、既に認証に成功した t と $H_k(t)$ とを利用して再度認証を成功させることはできない。

4.3　セッションキーの交換

不正利用の排除には、利用者が各パケットに利用者ごとに異なるデジタル署名、すなわち認証ヘッダを付けることで行える。具体的なデジタル署名の方法としては HMAC-MD5 などが利用できる。

無線端末から送出されるパケットには全て認証ヘッダを付ければよい。このとき、この鍵として認証サーバとの間の秘密鍵を用いるのは、鍵が知られたときの影響が大きい。そこで秘密鍵を用いてセッションキーと呼ぶ一時的な鍵を作り、これを用いて認証ヘッダを生成することを考える。

セッションキーは無線区間上に流れるパケットの暗号化にも利用できる。具体的な暗号化として AES[10] などが利用できる。

セッションキーを作る方法として Diffie-Hellman (DH) の鍵交換アルゴリズム[11] を使うことも検討した。しかし DH は公開暗号鍵の一種であり、計算時間がかかるという欠点がある。そこで認証サーバと無線端末が共通の秘密鍵を持っていることを利用した、DH を利用しないセッションキー生成方法を提案する。

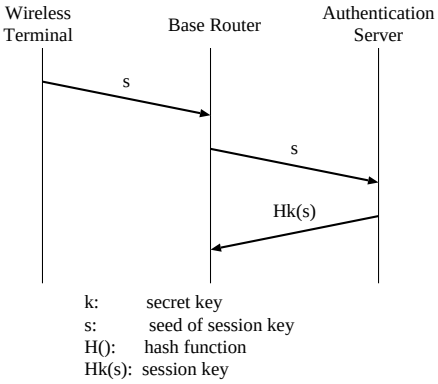


図 4　セッションキーの交換

手順は次のようになる (図 4)。

(1) セッションキーの種 (seed) となるランダムな値 s を無線端末が基地局に送る。

(2) 基地局は s を認証サーバに転送する。

(3) 認証サーバは s を秘密鍵 k でハッシュした値 $H_k(s)$ を基地局に返信する。(認証サーバと基地局との間は 4.2 節で述べたように安全な通信路が確保されていることに注意)

無線端末も $H_k(s)$ が計算できるので、以上の手順により $H_k(s)$ を一時的な秘密鍵であるセッションキーとすることができる。ここでも 4.3 節と同じく、基地局は無線端末と認証サーバとの間の秘密鍵を知ることがない。仮に無線区間が盗聴されていても、秘密鍵を知られない限り、セッションキーが計算されるとこはない。また鍵の生成のために必要なのはハッシュ値の計算だけであるため、非常に高速にセッションキーを生成することができる。

各パケットはこのセッションキーにより認証ヘッダが付けられる。基地局は、認証ヘッダが正しくないものは不正利用であると判断することができる。またこのセッションキーを用いて各パケットを暗号化することもできる。

なお、無線端末と基地局との間とパケットの交換に伴ないこのセッションキーが頻繁に使用されることになるので、実際の運用では利用する基地局が変わらない場合でもセッションキーを適宜変更する方がよい。

4.4　偽の基地局への接続の抑制

基地局も必ず 4.3 節 で生成したセッションキーで認証ヘッダを付けることとする。正しい基地局しか無線端末と共通のセッションキーを持てないため、基地局からのパケットの認証ヘッダを調べることで、パケットを送出した基地局が正しい基地局かが確認できる。

また 4.2 節 (5) の認証成功メッセージにセッションキーによる認証ヘッダを付けることで、認証成功メッセージ

が正しい基地局からのものかどうかを確認することもできる。

このように、無線端末が偽の基地局へ接続させられなくする仕組みが提供される。

なお実際の運用では、認証成功メッセージを一定時間以内に受け取れない場合には、接続しようとしている基地局が偽のものである可能性もあるので、即座に別の基地局への接続を試みるべきである。

4.5 ネットワーク情報の取得

無線端末は基地局発見の後、基地局に対してネットワーク情報の取得要求メッセージを送信し、基地局がネットワーク情報を返信することで、ネットワーク情報の取得を行う (図 5)。

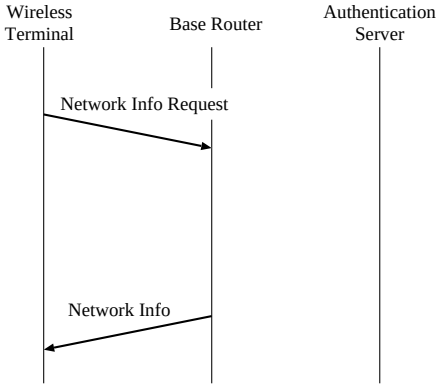
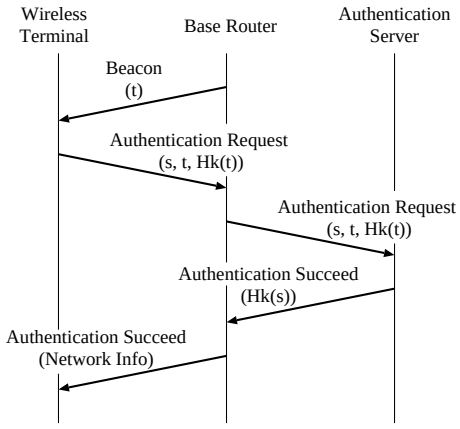


図 5 ネットワーク情報の取得

4.6 認証プロトコルの統合

以上 4.1 節から 4.5 節で説明した、基地局の通知と発見、無線端末の認証、セッションキーの交換、基地局の認証、ネットワーク情報の取得の全てを統合して行う認証プロトコルを提案する (図 6)。



t: time (used as a challenge)
k: secret key
s: seed of session key
H(): hash function
Hk(t): response for challenge
Hk(s): session key

図 6 統合された認証プロトコル

(1) 基地局は現在時刻 t を含めたパケットをビーコンメッセージとしてブロードキャストする。無線端末はこのメッセージを受けとることにより基地局を発見する。

(2) 無線端末はセッションキーの種 (seed) となるランダムな値 s と、秘密鍵 k を用いて t を一方向性ハッシュ関数でハッシュした値 $H_k(t)$、及び t を含む認証要求メッセージを基地局に送信する。このメッセージはネットワーク情報取得要求も兼る。

(3) 基地局は t が最近のものであった場合のみ s, $H_k(t)$, t を含む認証要求メッセージを認証サーバに転送する。

(4) 認証サーバは受け取った t から独自に $H_k(t)$ を計算し、受け取ったものと同じである場合にのみ、基地局に $H_k(s)$ を含む認証成功メッセージを送る。

(5) 基地局は認証成功メッセージを受け取った場合、無線端末にネットワーク情報を含む認証成功メッセージを送る。

既に説明した通り $H_k(s)$ がセッションキーとなり、各パケットの認証ヘッダの作成と、暗号化に使用される。

無線端末の成りすましや、盗聴、偽基地局の立ち上げにはこのセッションキーが必要になる。しかし秘密鍵が知られない限りセッションキーが知られることはなく、秘密鍵は、認証手順中、無線区間はもとより有線区間も流れることがない。よって本認証方式は非常に強固なセキュリティを提供することが可能である。

また高速な動作という点でも本方式は優れている。無線アクセス網には必須である (1) の手順を除くと、無線端末と認証サーバの間がわずか 1 往復、四つのメッセージにより、無線端末の認証、セッションキーの交換、基地局の認証、ネットワーク情報の取得のすべてを行うことができる。また無線端末の認証やセッションキーの生成もハッシュ値を求めるだけでよいので、高速に計算できる。

本方式は単純であるがゆえに提供するセキュリティがさらに強固なものとなっている。一般にプロトコルは複雑になればなるほどセキュリティが脆弱になっていく。複雑であればあるほど、仕様策定、実装、運用、それぞれの段階で、セキュリティホールが生じる余地が増えるためである。本方式は最小限のメッセージのやり取りので必要な情報の交換が全て終わるので、セキュリティホールが生じる余地が非常に小さい。

5. 本システムと既存システムとの比較

無線 LAN (IEEE802.11 シリーズ) の標準の暗号化方式である WEP を用いたり、最初に特定の WWW ページに強制的にアクセスさせて、ユーザ ID やパスワードを入力させるシステムが既に存在する。しかしこれらの方法では各パケットが端末ごとの個別の鍵で暗号化されていないため、認証が終わった後、無線端末の IP アドレスや MAC アドレスを偽ることで容易に成りすましが

でき不正利用が可能である。また盗聴は防げず、偽の基地局や偽のインターネットへの接続抑止は全く考えられていない。

この他 LAN 上でユーザ認証を行う仕組みとして IEEE802.1x[12] が提案されており、無線 LAN への適用も考えられている。IEEE802.1x も成りすましが可能であることが指摘されている[13]が、その点は除いて、認証の高速性に関してのみ比較する。

IEEE802.1x は LAN への接続のための認証システムであるため、認証終了後にできるのは、インターネットへの接続ではなく、あくまで LAN への接続である。その後 DHCP などで IP アドレスを取得して初めてインターネットに接続できるようになる。IEEE802.1x の認証だけに無線端末と認証サーバとの間で複数回のメッセージの往復が必要な上、DHCP も無線端末と DHCP サーバとの間のメッセージ交換が 1〜2 往復ある。

IEEE802.1x を利用してインターネットに接続することに比べ、無線インターネットに特化した本方式は、認証とネットワーク情報の取得が 1 往復で済むので高速であり、優れている。

6. 実　　装

本方式に基く認証システムを既に実装した。認証サーバは NetBSD 1.5 上の PC に実装し、またルート (株) 製の基地局ルータ RGW を本システムに対応させた。無線端末としては、NetBSD 1.4/1.5、 FreeBSD 4.3/4.4、Windows 98/Me/2000 が利用できる。無線アクセスの通信方式は IEEE802.11b である。

具体的な認証方式 (デジタル署名方式) としては HMAC-MD5 を利用し、暗号化方式としては AES が利用できる。秘密鍵、セッションキー共 128bit 長とした。

より詳しいプロトコル仕様やフレーム・パケットフォーマットは、モバイルブロードバンド協会で策定されており、その WWW ページ (http://www.mbassoc.org/) から入手可能となる予定である。

7. 実験と評価

評価として、システム上で一番処理の負荷がかかる認証サーバの性能を測定する。

PC (PentiumIII 500MHz、メモリ 128Mbytes、NetBSD 1.5.2) 上で認証サーバを起動し、単位時間あたりの認証要求メッセージの処理時間を測定した。認証サーバには 10 万の無線端末のアカウントと 4000 の基地局が登録されている。

実測の結果、秒間 2400 のメッセージが処理できることを確認した。各端末が 10 秒ごとに基地局を切り替えると仮定しても、認証サーバ 1 台で同時に 24000 台の無線端末を処理できることになる。これは実際にサービスを行うのに十分な性能である。

8. おわりに

本稿では無線インターネットサービスのセキュリティ確保の必要性について述べ、その要件を明らかにした。そして、無線端末と認証サーバとの間で 1 往復のメッセージを交換するだけで、無線端末の認証、セッションキーの交換、基地局の認証、ネットワーク情報の取得のすべてを行う、高速認証システムを提案した。本システムでは成りすましによる不正使用や、無線区間の盗聴も防ぐことができ、強固なセキュリティを提供する。認証プロトコルが単純であるため、セキュリティホールが生じる余地も小さい。また本システムを実装し、認証サーバの性能測定を行った。その結果実際にサービスを行うのに十分な性能が得られた。

本稿では、基地局を変更しても通信が途切れない、ハンドオーバー機能については言及しなかったが、これもモーバイル IP を利用することで実現する。

本高速認証システムとモーバイル IP を利用して、福岡や東京で無線インターネットサービスの実証実験を行っており、本サービスを 2002 年 4 月より開始する予定である。

参 考 文 献

1) IEEE, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer Extention in the 2.4 GHz Band,", IEEE802.11b, September 1999.
2) http://www.soumu.go.jp/joho_tsusin/policyreports/japanese/laws/telecom/index-re9908.html
3) http://www.soumu.go.jp/joho_tsusin/top/denki_h.html
4) Kent, S., and Atkinson, R., "Security Architecture for the Internet Protocol," RFC2401, November 1998.
5) http://www.ssh.com/
6) Dierks, T., and Allen, C., "The TLS Protocol Version 1.0," RFC2246, January 1999.
7) IEEE, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE802.11, August 1999.
8) Rigney, C., Rubens, A., Simpson, W., and Willens, S., "Remote Authentication Dial In User Service (RADIUS)," RFC2138, April 1997.
9) Krawczyk, H., Bellare, M., and Canetti, R., "HMAC: Keyed-Hashing for Message Authentication," RFC2104, February 1997.
10) Daemen, J., and Rijmen, V., "Rijndael, the advanced encryption standard," Dr. Dobb's Journal, Vol. 26, No. 3, pp.137–139. March 2001.
11) Diffie, W., and Hellman, M.E., "New directions in cryptography," IEEE Transactions on Information Theory 22, pp.644–654, 1976.
12) IEEE, "Port-Based Network Access Control," IEEE802.1x, July 2001.
13) Mishra, A., and Arbaugh, W. A., "An Initial Security Analysis of the IEEE 802.1X Standard," http://www.cs.umd.edu/~waa/1x.pdf, February 2002.