モバイルコンピューティングと
ワイヤレス通信
（２００３．３．６）
24－9

IEEE802.1X 認証との連携による IP モビリティ提供手法に関する検討

横田英俊† 久保健† 井戸上彰†

第 3 世代移動通信 (IMT-2000) を利用したデータアクセスや IEEE802.11 無線 LAN の普及により、インターネットの利用環境は家庭やオフィスなどの固定網からより移動度の高い網へ広がり、今後複数の無線 LAN ネットワーク間の連続的な移動や、セルラ網と無線 LAN ネットワーク等異種ネットワーク間の移動といった様々な利用形態が考えられる。移動端末が異なるネットワークに跨って IP アドレスの継続性を提供する方式として Mobile IP が標準化されているが、移動端末において Mobile IP の機能をサポートする必要があり、現状においてこのような環境が必ずしも広く普及している状況ではない。本稿では、無線 LAN ネットワークの利用者が Mobile IP をサポートしていない状況においてもセッションの継続性を維持するための要求条件を精査し、IEEE802.1X にもとづくネットワーク認証を利用することによりネットワーク側が IP モビリティを提供する手法について検討を行う。また、本手法を用いて無線 LAN ネットワーク間のハンドオフを行った場合の性能評価を行い、本手法の実用上の有効性について検証する。

A Study on IP Mobility Service Provisioning in Cooperation with IEEE 802.1X Authentication

Hidetoshi Yokota,† Takeshi Kubo† and Akira Idoue †

As wireless data communications by the third generation mobile telecommunication system (IMT-2000) and IEEE802.11 based wireless LAN are gaining popularity, the environments of Internet users expand from fixed networks such as their homes or offices toward mobile networks such as cellular networks or wireless LAN networks. It will also be seen in the near future that users begin to roam between multiple wireless LAN networks or between heterogeneous networks such as cellular networks and wireless LAN networks. While IP mobility becomes more important in this scenario and Mobile IP has been standardized for this purpose, such a function is not enough supported on the client side at this moment. In this paper, we first investigate requirements for the users on wireless LAN networks to maintain session continuity without supporting Mobile IP. Then, we discuss an IP mobility method leveraging the network authentication by IEEE802.1X, where the network handles IP mobility and maintains session continuity of mobile users. We also evaluate the performance of the proposed method with regard to handoff and validate its effectiveness in practice.

1. はじめに

近年、IEEE802.11 標準にもとづく無線 LAN 技術が急速に普及し、このような無線 LAN のアクセスポイントを屋外に設置することにより、公衆無線 LAN サービスが安価に提供されつつある。これまでは店舗内、駅構内といったスポット的なサービス形態が取られているが、ユーザの利便性を考慮すれば今後はエリア的なサービス展開 (カバレッジエリアの拡大) が重要になると考えられる。一方、多数の無線 LAN アクセスポイントを一つのネットワークで収容することは、ユーザ数およびトラヒックの増大に伴い困難となり、エリアが拡大するにつれて複数のネットワークによる構成が必要となる。このような状況では、異なるネットワークへ移動した際の IP レベル以上での通信の継続性が問題となってくる。また同時に、第 3 世代移動通信 (IMT-2000) と無線 LAN といった異種メディア間の接続に対する関心も高まっている。このように異なる無線ネットワークをシームレスにローミングさせるためには、(1) 通信の継続性と (2) 認証を含めたセキュリティの統一的な提供が重要となる。現在の公衆移動体通信ネットワークと無線 LAN ネットワークは互いに独立しており、上記二つの機能を提供する構成にはなっていない。

移動端末がアクセスポイントを介してネットワークを利用するためには、アクセスポイントが接続されて

† (株)KDDI 研究所
KDDI R&D Laboratories, Inc.

いるネットワークに依存したIPアドレスやゲートウェイアドレス等を取得する必要がある。これらの設定は手動もしくはDHCP (Dynamic Host Configuration Protocol)[1]サーバによる自動設定がしばしば利用される。一方、図1に示すようにセルラー網と無線LANネットワーク間の移動など異種メディア間のハンドオフや異なる無線LANネットワーク間のハンドオフを行う際には、異なるネットワークへ移動することによりアドレスの変更が伴う可能性がある。IPアドレスの継続性が提供されることによって、マルチメディア・ストリーミング、VoIP着信、プッシュ配信など、着信型のサービスが接続ネットワークに依存せず利用することが可能となり、アクセス手段の多様化に対してシームレスにサービスを提供することは、ネットワークの利便性の面から望ましい。移動端末が異なるメディアやネットワークに跨ってIPアドレスの継続性を提供する方式としてMobile IP[2]が標準化されているが、ネットワーク側のみならず移動端末においてもMobile IPの機能をサポートする必要があり、現状においてこのような環境が必ずしも広く普及している状況ではない。

今後、広域な公衆無線LANサービスや、IMT-2000と無線LAN等のシームレスなローミングの普及を考えると、移動端末(ユーザ)側はできるだけ既存の環境で利用できることが望ましい。そこで本稿では、移動端末が無線LANネットワークを利用する際に、移動端末側にローミングのためのソフトウェアの追加や設定をせずに、ネットワーク側でIPモビリティを提供する手法について検討を行う。

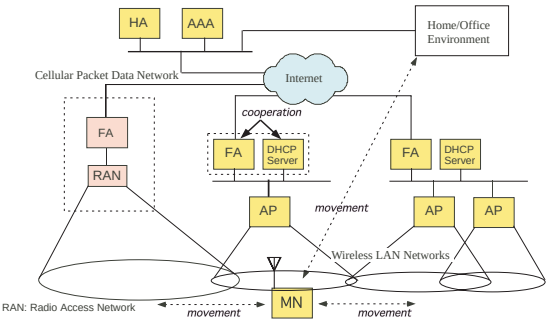

図1 インターネットユーザの移動形態

2. IPモビリティの提供手法

2.1 設計方針

IPモビリティをネットワーク側でサポートするための手法の検討に先だって、まず標準プロトコルとして規定されているMobile IPにおいて、移動検知、端末の識別、位置管理に用いられている手法について検証する。

- 移動検知：
  各ネットワークに配置されたフォーリンエージェント(FA)が定期的にブロードキャストまたはマルチキャストするエージェント広告により移動端末(MN)が検知する。
- 端末の識別：
  位置登録要求メッセージ(RRQ)に格納されるMNのホームアドレスやNAI (Network Address Identifier)[3]で識別し、その認証はRRQに格納されるMN-HA間の認証(Mobile-Home Authentication Extension)により行う。
- 位置管理：
  MNがRRQによりホームエージェント(HA)へ位置登録を行う。位置登録情報は、MNを収容するFAおよびHAの双方で保持する。

ネットワーク側でIPモビリティをサポートするためには、(1) 移動検出のためにMNが移動時に必ず利用するプロトコルをトリガとし、(2) 端末の識別のためにMNを一意に特定でき、かつセキュリティ上安全である必要がある。上記(1)、(2)がサポートされれば、ネットワーク上のノードがMNに代わって位置登録を行うことは容易と考えられる。

2.2 プロトコルの選択

端末がネットワークと接続する際に利用可能なプロトコルとして、下記の2つが考えられる。

PPP[4]**：** IMT-2000では3GPP2[5]において、固定網ではダイアルアップによるモデム接続やADSLにおけるPPPoE (PPP over Ethernet)[6]を用いた常時接続で広く利用されており、多くのOSでサポートされている。PPPにおける認証フェーズを利用することで、設計方針(2)の端末(ユーザ)の識別が可能であるが、PPPリンクの確立とネットワークの接続状態は連携しておらず、設計方針(1)の移動検出のトリガとすることが困難である。また、PPPリンク確立におけるオプションの交換による遅延やPPPフレームのオーバヘッドが問題となる。

IEEE802.1X[7]**：** アクセスポイントに接続する際には必ず起動されるため、設計方針(1)を満たすことが可能である。また、IEEE802.1Xでは、認証時に端末側がユーザ名を送信することにより端末(ユーザ)の識別が可能であり、かつIEEE802.1Xで規定する認証機能を利用することにより、設計方針(2)を満たすことも可能である。さらに、認証以外については通常のIEEE802.11と同様であるため、IEEE802.1Xに起因するフレームのオーバ

ヘッドやコネクション管理等の問題は発生しない。上記の検討結果より、本稿では無線 LAN ネットワークにおいて IEEE802.1X を利用した IP モビリティの提供手法について検討を進める。

3. IEEE802.1X との連携による IP モビリティの提供

IEEE802.1X は LAN 接続の際に認証サーバを利用した認証方式であるが、特に無線 LAN ネットワークにおける認証方式として利用され始めている。IEEE802.1X では、図 2に示すように、移動端末等 LAN に接続して認証を受ける側を Supplicant、MAC ブリッジやアクセスポイント等 LAN 上で認証を行う側を Authenticator、さらに認証サーバのように Authenticator に対して認証サービスを提供する Authentication Server と呼ばれるエンティティが定義されている。また同方式は、EAP (Extensible Authentication Protocol)[8] を利用することにより、MD5-Challenge、TLS (Transport Layer Security) など様々な認証方式への拡張が可能となっている。さらに Supplicant と Authenticator が接続される LAN 区間では EAP を転送するための EAPOL フレームが定義されており、このフレームを用いて鍵情報を交換することにより Supplicant 毎に異なる鍵を割り当てることも可能となる。

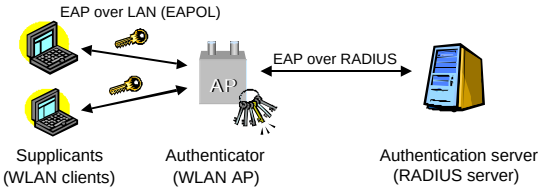

図 2 IEEE802.1X における認証モデル

移動端末 (MN)、アクセスポイント (AP) および認証サーバ (AAA) において EAP-TLS[9] を用いた場合の IEEE802.1X による認証手順の例を図 3に示す。同方式では認証時に MN からユーザ名 (Identity) が提供され、これによりユーザの識別が可能となる。

筆者らは文献 10) において、MN が IEEE802.1X によりネットワーク接続のための認証を行う際に、AP が Mobile IP の手順と連携させることにより、移動先で利用する IP アドレスを MN の Identity に対応付ける手法を提案した。本方式では、MN が異なるネットワーク間を移動しそのネットワークにおいてアドレスを要求した場合でも、一度割り当てられたアドレスを継続的に利用できるよう、移動先の FA、DHCP サーバおよび AAA を連携させる手法を取っている。本稿

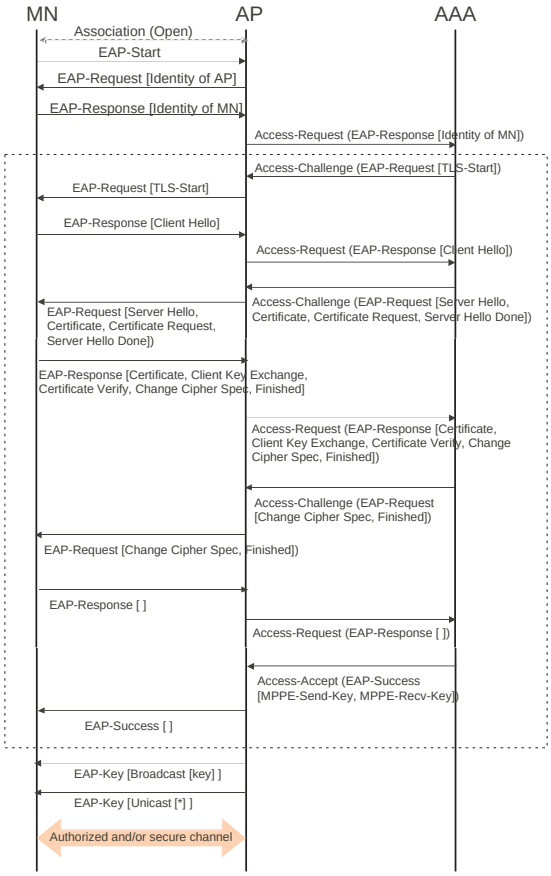

図 3 IEEE802.1X における認証シーケンスの例 (EAP-TLS)

では EAP-TLS を利用した場合を例に、本手法における位置登録手順、ハンドオフ手順、データ転送手順についてその詳細を示す。

3.1 提案方式における認証及び位置登録手順

関連するノードおよび提案手法の手順を図 4に示す。また認証方式として EAP-TLS を用いた場合のシーケンスを図 5に示す。

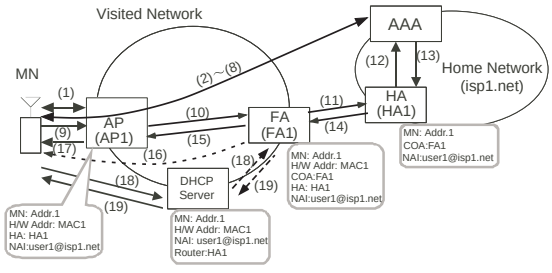

図 4 ネットワーク構成および位置登録手順

手順 (1) において MN-AP 間にアソシエーションが確立すると、AP の要求に対して MN がユーザ名

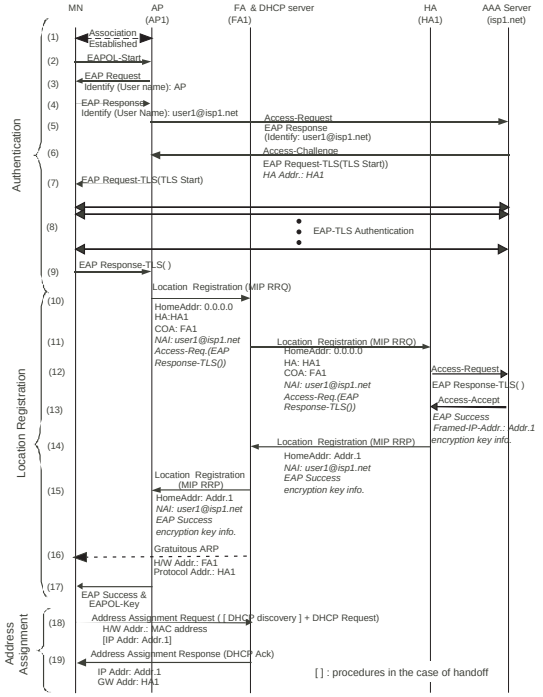

図 5　位置登録手順の詳細 (EAP-TLS)

(Identity) を格納した EAP-Response を応答する。手順 (2)〜(9) では、IEEE802.1X の手順に従って MN が Access-challenge に対する応答を AP に送信するが、手順 (10) において AP は Mobile IP の Registration Request (RRQ) に EAP-Response を格納して FA1 経由で HA に送信する。HA は手順 (12) において EAP-Response を Access-request に格納して AAA サーバに転送し、受信した Access-accept(または Access-reject) にもとづいて Registration Reply (RRP) を転送する。AP はこの RRP の結果により MN のアクセスの許可を決定する。MN が手順 (18) において、DHCP にもとづいて IP アドレスの要求を送信した場合には、DHCP サーバが FA に問い合わせることにより位置登録で割り当てられたホームアドレスおよび HA のアドレスをそれぞれ MN のアドレスおよびルータアドレスとして MN に応答する。

なお、手順 (10) で位置登録を行う際に MN のユーザ名を NAI 拡張フィールド [3] に格納して FA に転送する。また、EAP 応答メッセージは専用の拡張フィールドを定義する。手順 (12)〜(13) において認証が失敗した場合には、位置登録応答メッセージの Code フィールドにその内容を指定してアクセスポイントまで転送する。この場合手順 (17) では EAP-Failure が MN に応答される。AP は MN とのアソシエーションが確立している間は位置登録の更新を行い、アソシエーションが消滅した段階で位置登録を終了（De-registration）する。

3.2　提案方式におけるハンドオフ手順

提案方式における移動端末のハンドオフ手順を図 6 に示す。

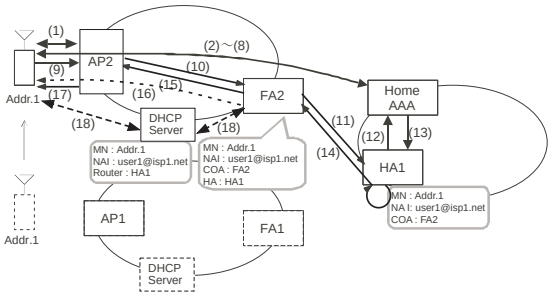

図 6　提案方式におけるハンドオフ手順

手順 (1)〜(13) までは位置登録手順と同様であるが、手順 (14) において HA は Binding List を参照し、MN が登録されている場合には割り当てられているアドレスを RRP のホームアドレスフィールドに格納する。また FA2 が手順 (16) において Gratuitous ARP を送出することにより、MN の ARP キャッシュに HA 宛の MAC アドレスが保持されている場合には、FA2 の MAC アドレスに書き換えられる。MN が DHCP サーバに対してアドレス要求を送出した場合には [手順 (18)]、FA2 に対して位置登録時に割り当てられた MN 用のアドレスを問い合わせ、それを応答する。

3.3　提案方式におけるデータ転送手順

提案方式におけるデータ転送手順を図 7に示す。下り方向のデータ転送 (CN → MN) については Mobile IP の手順に従い、HA 及び FA を経由して MN へ配送される [図中 (a)〜(c)]。上り方向のデータ転送 (MN → CN) の手順を以下に示す。

(1)　MN はアドレス取得時にホームネットワークで有効なアドレスを自ホストのアドレスとし、HA1 のホームネットワーク内におけるアドレスをルータアドレスとして設定する。

(2)　MN が CN 宛にパケットを最初に送信する場合には、ゲートウェイルータである HA1 に対する ARP 要求を出す。

(3)　FA1 は HA1 宛ての ARP 要求に対して代理 ARP 応答を送出する。

(4)　MN は CN 宛のパケットをホームネットワークのゲートウェイルータ (HA1) 向けて送信するが、その宛先 MAC アドレスは FA1 となる。

(5)　FA1 はこのフレームを受信し、宛先 IP アドレスを参照して CN に転送する。

位置登録手順 (図 5) の手順 (16) において、FA が送信

する Gratuitous ARP により MN の ARP キャッシュが変更されている場合には、本手順 (2) は必ずしも実行されなくてよい。

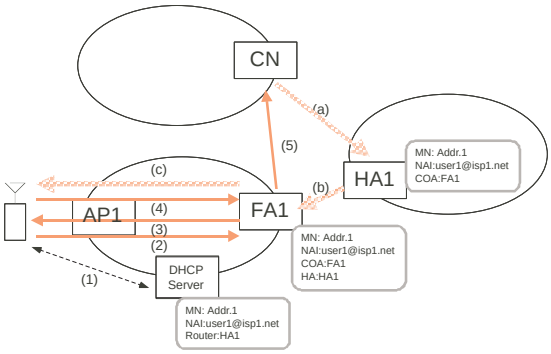

図 7　提案方式におけるデータ転送手順

4. 性能評価

提案手法を用いて異なるネットワーク間をハンドオフした際のセッションの継続性に関する検証を行うために、本手法を LAN 環境上に実装しハンドオフにかかる処理時間に関する評価を行う。使用したネットワークの構成を図 8に、構成要素の諸元を表 1に示す。有線 LAN は全て 100Base-T で接続し、無線 LAN は IEEE802.11b を利用した。本手法の機能実現のために機能追加を行ったノードを表中 (*) で示した。また今回の実験では、簡単のため FA と DHCP サーバは同一マシン上に実装した。

表 1　ネットワークの構成要素

ノード名	ハードウェア (CPU)	OS
HA* FA* (DHCP*)	Pentium III 1.2GHz	FreeBSD2.2.8
AP*	Pentium III 600MHz	Redhat Linux 7.3
AAA*	Pentium III 450MHz	Redhat Linux 7.3
CN	Traffic Generator	N/A
MN	Pentium III 700MHz	Windows XP

(注)*は提案手法のための機能追加を行ったノード

2 つのフォーリンネットワーク間のハンドオフを 10 回試行し、(1) EAP-TLS における認証、(2) Mobile IP による位置登録、および (3)DHCP によるアドレス割り当てに要した処理時間を計測した。その結果を図 9に示す。

この実験結果より、認証および位置登録にかかる処理時間はそれぞれ 400msec と 40msec であったが、IP アドレス割り当て処理が開始されるまでに 200msec 程度を要し、完了するまでの処理時間は 3〜5.4 秒に達

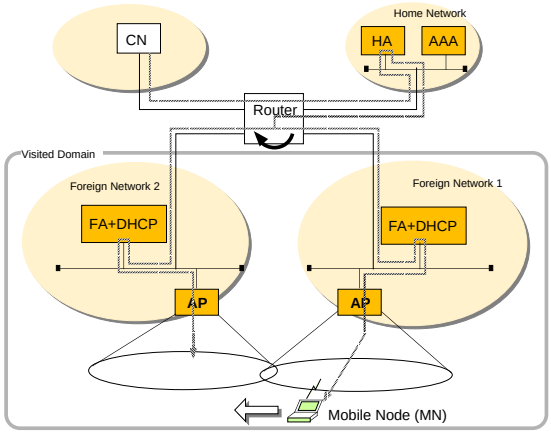

図 8　評価実験に用いたネットワーク構成

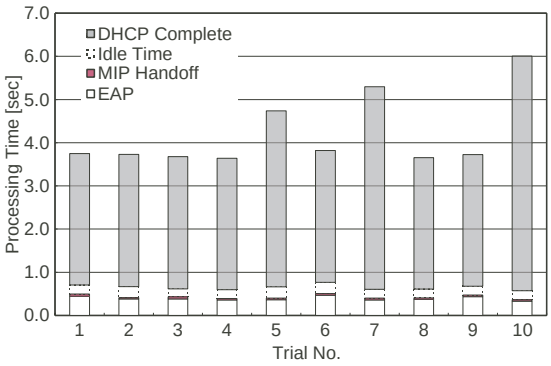

図 9　各処理における処理時間

することが分かった。位置登録と DHCP によるアドレス割り当ての間に空き時間 (Idle Time) が発生する原因として、IEEE802.1X 認証と DHCP による IP アドレス割り当て処理が互いに独立な処理であり、認証処理の完了後ただちにアドレス割り当てが開始することが保証されていないと推測される。

このアドレス割り当て時間がハンドオフにおける転送断の増大の原因となるかを検証するために、クライアントをデータ受信中にハンドオフさせる実験を行った。ストリーミング等のリアルタイムアプリケーションを想定し、CN から 256 バイトの UDP パケットを 50msec 間隔で MN 宛に転送しながら、MN を異なるネットワークに移動させた。このときの実験結果を図 10に示す。この図より、MN は位置登録が完了すると、アドレス割り当てを待たずに CN からのパケットを受信していることがわかる。文献　1) の 3.7 では、ネットワークの接続状態が変わった後でも、有効期限までは取得済のアドレスの使用を許容している。本実験で利用したクライアントにおいても同様に動作しており、MN 宛のパケットが新しいネットワークに転送され次第、受信することが可能となっている。さらに

提案手法を用いることによって、新しいネットワークに移動した場合でも同じアドレスが割り当てられるため、MN は CN からのパケットを受信し続けることが可能となる。

この実験結果より、データ転送断となる時間がアドレス割り当てに要求される処理時間に必ずしも依存しないため、ハンドオフ時にデータの転送が中断される総時間は AP とのアソシエーションを含め 500msec 程度となる。

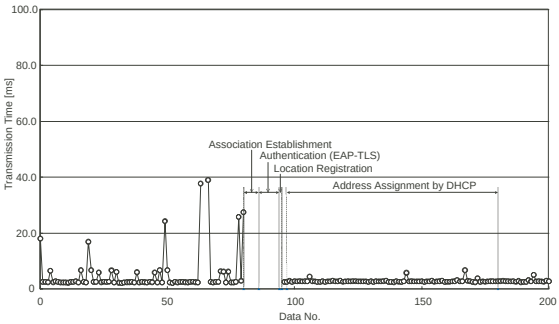

図 10　ハンドオフ時におけるデータ転送

5. 考　　察

MN の位置登録のための RRQ は AP が起点となるため、Mobile IP における MN の認証 (MN-HA 認証拡張[2]) の利用が困難となる。従って、HA が MN の位置登録に関わる認証を行う際には、MN の NAI を利用して AAA サーバ (本実験では RADIUS サーバを用いた) に認証要求を行う等の手法が必要となる。一方、IEEE802.1X に関わる認証と位置登録に関わる認証は独立した処理であり、HA からの位置登録に関する認証に応答するためには、RADIUS サーバにおいて IEEE802.1X における認証成功可否の状態情報を保持する必要があり、両者の同期が煩雑となる。図 5に示す位置登録では手順 (12)〜(13) において認証要求と位置登録要求を合わせて行うことにより、IEEE802.1X における移動端末の認証と位置登録における移動端末の認証を手順として同時に実現させている。

また図 10から、ネットワーク間の移動時におけるデータ転送断は、IEEE802.1X の認証を含めたレイヤ 2 のハンドオフが主な要因となっていることが分かる。Mobile IP を利用する際の移動検出はエージェント広告の受信をもとに行われるが、移動検出にかかる時間はエージェント広告の送出間隔とその有効期間に依存し、文献 11) では移動検出に 2〜3 秒要することが報告されている。これに対して本手法では、AP とのアソシエーションが移動検出のトリガとなることから、EAP-TLS を利用した場合でも 400msec 程度でハンドオフの完了およびデータ転送の再開が行われ、Mobile IP のみを用いた場合よりもハンドオフによる転送断が軽減されることが分かる。

6. おわりに

本稿では、IEEE802.1X によるネットワーク認証と Mobile IP を連携させ、ネットワーク側が IP モビリティを提供する手法についてその詳細を示した。本手法により、移動端末が無線 LAN ネットワーク間を移動した際にも、Mobile IP の手順を使わずに着信型サービス及び移動時のセッションの継続が可能となる。また、提案手法を LAN 環境上に実装し、ハンドオフにかかる処理時間およびデータ転送に関する評価実験を行った。その結果、ネットワークの移動に伴うデータ転送断は 500msec 程度で、クライアントにおいてアドレスの変更なくデータの再受信が可能となることが確認された。日頃御指導頂く KDDI 研究所浅見所長に感謝致します。

参 考 文 献

1) R. Droms “Dynamic Host Configuration Protocol,” RFC2131, IETF, Oct. 1997.
2) C. Perkins “IP Mobility Support for IPv4,” RFC3344, IETF, Aug. 2002.
3) P. Calhoun, *et al.* “Mobile IP Network Access Identifier Extension for IPv4,” RFC2794, IETF, March 2000.
4) W. Simpson “The Point-to-Point Protocol (PPP),” RFC1661, IETF, July 1994.
5) “Wireless IP Network Standard,” P.S0001-B (ver.1.0.0), 3GPP2, Oct. 2002.
6) L. Mamakos, *et al.* “A Method for Transmitting PPP Over Ethernet (PPPoE),” RFC1661, IETF, Feb. 1999.
7) “Standard for Port based Network Access Control,” P802.1X/D10, IEEE, Jan. 2001.
8) L. Blunk and J. Vollbrecht “PPP Extensible Authentication Protocol (EAP),” RFC2284, IETF, March 1998.
9) B. Aboba and D. Simon “PPP EAP TLS Authentication Protocol,” RFC2716, IETF, Oct. 1999.
10) 横田、久保、井戸上、大橋、「IEEE802.1X 認証との連携による IP モビリティ提供手法に関する一考察」、電子情報通信学会ソサイエティ大会、SB-5-6、Sept. 2002.
11) H. Yokota, *et al.* “Link Layer Assisted Mobile IP Fast Handoff Method over Wireless LAN Networks,” ACM MobiCom2002, pp.131-139, Aug. 2002.