社団法人　情報処理学会　研究報告
IPSJ SIG Technical Reports

2007－ＱＡＩ－25（11）
2007／10／26

LIN6とMISP/PDMAの連携による高速認証とシームレスハンドオーバを実現する無線インターネット環境の実現

藤川　賢治†　森岡　仁志†　真野　浩†

†ルート(株)　〒141-0031 東京都品川区西五反田 7-21-11 第2TOCビル8F
E-mail: †{fujikawa,hmorioka,hmano}@root-hq.com

あらまし　本研究の目的は、家庭で一般的に利用可能なIPv4インターネット環境下で、利用者にグローバルIPアドレスと高速認証、シームレスハンドオーバを提供することである。この際、無線端末にはFQDNとパスワード情報を予め無線端末に設定するだけでよい。このため、我々はモビリティプロトコルとしてLIN6を、認証プロトコルとしてMISP/PDMAを採用し、そのサーバ機能を、IPv6/6to4機能を持つ無線ブロードバンドルータに導入した。提案する無線ブロードバンドルータをIPv4インターネット上に分散配置することで、利用者は固定FQDNとIPv6アドレス、高速認証、シームレスハンドオーバを利用することが出来る。我々はこれらの機能が協調して動作する手法を提案し、評価する。

キーワード　IPv6, LIN6, MISP, PDMA, 高速認証, シームレスハンドオーバ

Construction of Wireless Internet Environments Implementing Fast Authentication and Seemless Handover by Cooperation of LIN6 and MISP/PDMA

Kenji FUJIKAWA†, Hitoshi MORIOKA†, and Hiroshi MANO†

† ROOT Inc., 8F TOC2 Bldg. 7-21-11 Nishi-Gotanda, Shinagawa-ku, Tokyo 141-0031, JAPAN
E-mail: †{fujikawa,hmorioka,hmano}@root-hq.com

Abstract　The purpose of this paper is to provide a user with global IP addresses, and fast authentication and seamless handover mechanisms, under an IPv4 Internet environment commonly provided to our homes. All the information what should be pre-set in a wireless terminal is just a pair of a specific FQDN and a password for authentication. For this, we introduce the server functions in LIN6 for mobility and the server functions in MISP/PDMA for fast authentication and seamless handover, into a wireless broadband router equiped with IPv6/6to4. By distributing broadband routers with these functions under the IPv4 Internet environment, a user is able to utilize fixed FQDN's and global IPv6 addresses, and fast authentication and seamless handover functions under wireless Internet environments. We propose a method of these functions' cooperating with each other, and evaluate it.

Key words　IPv6, LIN6, MISP, PDMA, seamless handover, fast authentication

1. はじめに

現在、IPv4インターネットを手軽に利用できる環境は整っているが、IPv6インターネットに関してはそうとはいい難い。一方、IPv4インターネットでは個人が手軽に複数の固定グローバルIPアドレスを入手し利用することは難しいが、IPv6を利用すれば固定グローバルIPアドレスを複数利用することは容易である。

本研究では、無線配下でグローバルIPアドレスを付与し、利用者が何時でも何処でもインターネット接続できる環境を提供することを目的とする。その際、現在個人が手軽に用意できるIPv4インターネット環境を利用することを考え、グローバルアドレスとしてはIPv6アドレスを利用する。この際、無線端末にはFQDNとパスワード情報を予め無線端末に設定するだけでよい。このため、我々はモビリティプロトコルとしてLIN6を、認証プロトコルとしてMISP/PDMAを採用し、そのサーバ機能を、IPv6/6to4機能を持つ無線ブロードバンドルータに導入した。提案する無線ブロードバンドルータをIPv4インターネッ

ト上に分散配置することで、利用者は固定 FQDN と IPv6 アドレス、高速認証、シームレスハンドオーバを利用することが出来る。我々はこれらの機能が協調して動作する手法を提案し、評価する。VPN 機能、高速認証、ハンドオーバー機能、LIN6 の各種サーバ機能、高速認証プロトコル MISP のサーバ機能である。

2 章で導入すべき技術の考察を行い、3 章でそれらの技術の改良手法を提案し Home Residential Gateways (HomeRG's) に組込み、4 章で HomeRG と無線端末の通信の動作シーケンスを示し、5 章は実装と評価について述べる。

2. 導入技術の検討

本論文の目的は、無線配下でグローバル IP アドレスを無線端末へ付与し、利用者が何時でも何処でもインターネット接続できる環境を提供することである。そのため、次の機能を提供することを考える

（1） グローバル IP アドレスの提供

（2） VPN 機能

（3） 高速認証

本システムに基く無線環境化では、利用者が特定できる仕組みを提供する。これにより、無線環境化からインターネットに対する各種攻撃が行われたときに、誰の責任であるかを特定することができる。また認証を高速で行うことにより、高速ハンドオーバを可能にする。

（4） 移動透過性

接続先の無線アクセスポイントを変更しても、現在使用している TCP 等のセッションが切れない仕組を提供する。

以下、それぞれの機能を実現するために導入する技術を検討する。各導入技術の動作の詳細は、3 章において説明する。

2.1 グローバル IP アドレスの提供

グローバル IP アドレスを無線端末に提供することで、端末をインターネット電話やリアルタイム動画カメラなどに利用することが出来る。しかし現状、IPv4 アドレスを個人で複数入手し、無線端末ごとに提供することは困難である。

そこで無線端末には IPv6 アドレスを付与し、それが固定となるような仕組も同時に提供することとする。もちろん、IPv4 インターネットへの接続性も実用上重要であるので、IPv4 インターネットへ接続する方法も同時に提供する。

現在、個人が家庭や SOHO に IPv4 インターネット回線を引いて IPv4 アドレスを最低一つ入手することは比較的用意である。そこで、6to4 技術を導入し、IPv4 アドレスを元に無線端末に IPv6 アドレスを付与することとする。

2.2 VPN 機能の検討

他人が用意した無線環境化からインターネット接続することを考える。

無線環境では盗聴が容易であるため、家庭や SOHO まで VPN 接続することが一般的に行われる。本稿では IPsec6 を利用することを考える。

後述する移動透過技術により、IPsec6 による VPN 接続も移動透過性を持つことになる。

2.3 高速認証技術の検討

無線環境化の認証プロトコルとして一般に IEEE802.1x [3] が利用されている。しかし、無線技術である IEEE802.11 [4] との組合せでは次のような問題が生じる。

- 無線端末の無線モジュールが一つしかない場合、一つ複数の基地局に同時接続できない。
- IP アドレス取得後認証が高速に行えない。
- 認証のためのプロトコルシーケンスが多いため、高速な認証が行えない。
- 認証の後、DHCP(IPv4) や DAD(IPv6) を行うため、高速な IP アドレス取得が行えない。

これらの問題を解決するため、我々が既に開発済みの MISP/PDMA 技術を用いる。MIPS/PDMA 技術は、

- 複数の基地局への同時接続、
- 認証と IP アドレスの取得を高速に行う

ことが出来る。

2.4 移動透過性技術の検討

IPv6 用の標準の移動透過性プロトコルとして Mobile IPv6 がある。しかし、Mobile IPv6 にはパケットにオプションヘッダが必要となり、MTU サイズが変更されてしまうという問題がある。

本稿での方式は、VPN などのトンネル技術を採用するため、できるだけ、ヘッダが増えることを抑制したい。

そこでオプションヘッダを必要としない LIN6 プロトコルを採用することとする。LIN6 は標準的な技術では無いが、LIN6 を用いる場合でも IPv6 インターネットや IPv4 インターネットへの接続性は確保されるので通常の使用に問題は無い。加えて本稿では、LIN6 を用いて通常の IPv6 インターネットや IPv4 インターネットへの接続も移動透過になる手法を提案する。

3. 関連技術の改良と HomeRG への組込み

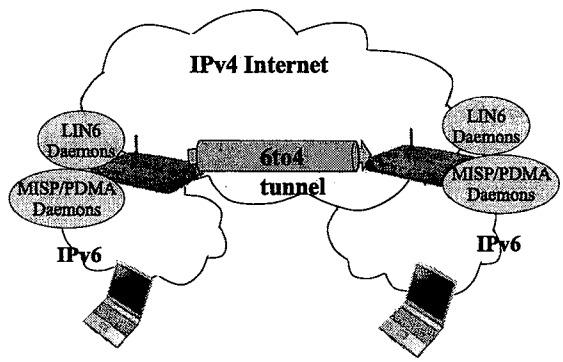


図 1 HomeRG embedded LIN6/MISP/PDMA within

本稿では、IPv4 インターネット配下に設置し、無線により IPv6 インターネットを提供する無線ブロードバンドルータを、Home Residential Gateway (HomeRG) と呼ぶ。

2 章での検討を基に、HomeRG に導入した機能、技術、改良点等を説明する。(図 1)

3.1 6to4

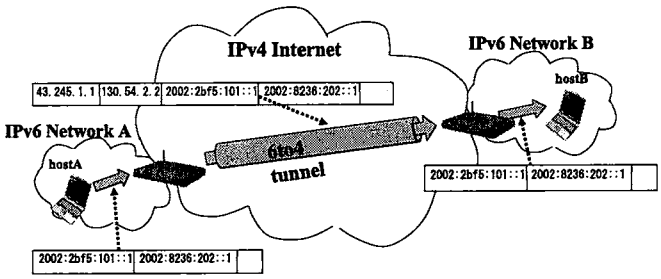


図 2 Inter-IPv6-site communication via the IPv4 Internet

6to4 は IPv4 ネットワークを介して、IPv6 サイトが相互に通信したり、IPv6 サイトがリレールータによってグローバル IPv6 インターネットと通信したりする方法を提供する。

HomeRG に 6to4 の機能を組込み、配下の無線端末に IPv6 インターネット環境を提供する。HomeRG 利用者が用意するものは、一般の IPv4 インターネット接続環境で良く、固定 IPv4 アドレス接続や、DHCP, PPPoE など一般的な各種接続方法が選択できる。

本稿では特に HomeRG 配下での IPv6 サイト相互の通信を重視する。(図 2) これは HomeRG 配下の無線端末同志での通信を意識しているからである。

3.2 LIN6

Location Independent Network for IPv6 (LIN6) [8] は IPv6 アドレスの下位 64bit を ID として、移動透過性ととマルチホーム機能を提供するプロトコルである。

LIN6 では DNS の reverese look up 機能と、Mapping Agent (MA) と呼ばれる位置情報サーバによって移動端末の位置情報を通信相手に提供する。しかし LIN6 では DNS サーバと Mapping Agent を誰が管理するのかという問題が生じる。

本稿では、この DNS サーバと MA を HomeRG に組込むことで、サーバの管理問題に組込む方法を提案する。これにより HomeRG を設置するだけで、LIN6 利用に必要な各種デーモンを使用することが出来る。

図 3.2 は、各種サーバ/デーモンなどの相関図である。動作の詳細は [9] 参照のこと。

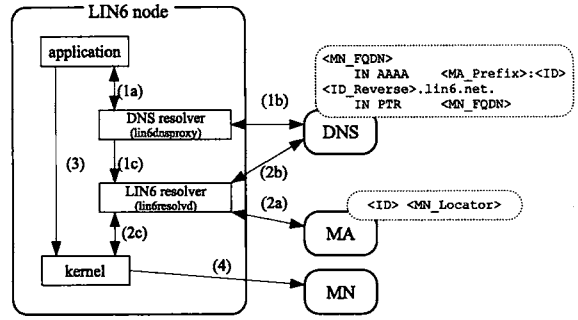
3.3 MISP/PDMA

Mobile Internet Service Protocol (MISP) は移動端末と基地局の接続時間を短縮できる高速認証システムである。

MISP は 802.1x と RADIUS、DHCP/DAD の機能を併せ持ち、高速認証とアドレス取得を同時に行う。

図 3.3 に MISP と IEEE802.11/IEEE802.1x/DHCP のプロトコルシーケンスの比較を示す。

Packet Division Multiple Access (PDMA) [6] は、各無線基地局の利用帯域を敢て分けないことで、電波の利用高率を上げようという試みである。また無線端末は複数の帯域をスキャンする必要が無いため、複数基地局からの電波を同時に受ける際に受信機を複数用意する必要が無い。



Example of the values

<MN_FQDN>:	mn.miako.net
<ID>:	8302:2bf5:1:1
<ID_Reverse>:	1.0.0.0.1.0.0.0.5.f.b.2.2.0.3.8
<MA_Prefix>:	2002:2bf5:1:0 (means <MA_Address> is 2002:2bf5:1:0:100::)
<MN_Locator>:	2002:2bf5:2:2

（1） アプリケーションが DNS の AAAA レコードを lin6dnsproxy 経由で引くと O+ID が返ってくる。(a, b) その際 lin6dnsproxy は Locator を取得し、lin6resolvd にも ID と MA のアドレス情報を通知する。(c)

（2） LIN6 resolver は MA に問い合わせ CN の Locator を取得する。(a) それと同時に ID からの DNS の逆引き及び正引きをを行う。(b) ((b) の結果、異る MA が見つかった場合は MA への query をやり直すが、DNS が正常に設定されている限り、このやり直しは起きない) カーネルに、ID に対応する取得した locator を登録する。(c)

（3） アプリケーションが connect システムコールを発行する。(2) とは並列実行である。

（4） (2) の処理が終了するまでパケットが遅延され Locator で示されるアドレスに送信される。

図 3 Relation between LIN6 servers/clients

MISP と PDMA とを組合わせることにより、make-before-break 型ハンドオーバを行い、ハンドオーバ時のパケットロスを無くすことが出来る。[5]

HomeRG に MISP/PDMA 機能を実装することで、無線端末からの複数基地局への同時接続と高速ハンドオーバを実現する。

4. HomeRG の動作

HomeRG と無線端末のシーケンスは大まかに以下のように分けられる。

（1） HomeRG の設置及びアドレス取得
（2） 家庭内無線端末のアドレス取得
（3） ForeignRG 配下での無線端末のアドレス取得
（4） IPsec による HomeRG との VPN 接続
（5） gif トンネルによる IPv4 接続

それぞれの動作について説明する。

4.1 HomeRG の設置及びアドレス取得

（1） HomeRG は通常のブロードバンドルータと同じく、DHCP もしくは PPPoE によって上流回線に接続され IPv4 アドレスを取得する。むろん固定 IP アドレスでもよい。IPv4 アドレスはグローバルである必要がある。

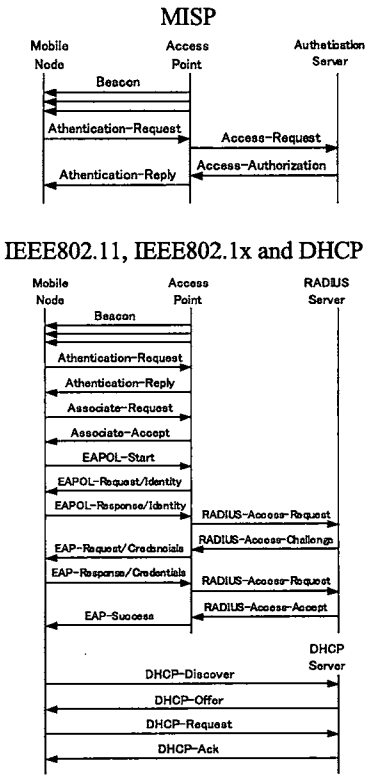


図 4　Comparison of MISP and 802.11/802.1x/DHCP

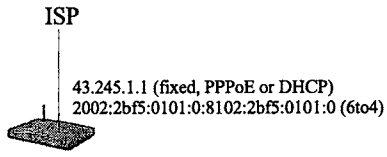


図 5　HomeRG obtains an IP address from ISP

（2） 6to4 によって HomeRG 自身にグローバル IPv6 を持たせ、IPv6 インターネットに接続できるようにする。

（3） IPv4 アドレスを Dynamic DNS (DDNS) サーバに登録し、FQDN 名でルータにアクセスできるようにする。例えば HomeRG は r0001.ddns0.miako.net のような FQDN 名を持つ。また IPv6 アドレス解決のため、r0001.ddns0.miako.net のドメインの委譲も受ける。すなわち ddns0.miako.net サーバには以下の情報が登録される。(DHCPv4 で 43.245.1.1 を取得した場合)

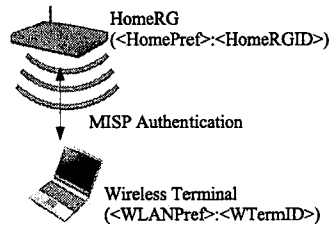
```
r0001.ddns0.miako.net.
  IN NS r0001.ddns0.miako.net.
  IN A 43.245.1.1
  IN AAAA 2002:2bf5:0101:0:8102:2bf5:0101:0
```

（4） HomeRG で LIN6 端末のための DNS サーバを起動する。次のようなデータベースを持つ。

```
r0001.ddns0.miako.net.
  IN SOA r0001.ddns0.miako.net. (snip)
  IN NS r0001.ddns0.miako.net.
  IN A 43.245.1.1
  IN AAAA 2002:2bf5:0101:0:8102:2bf5:0101:0

h01.r0001.ddns0.miako.net.
  IN AAAA 2002:2bf5:0101:0:8302:2bf5:0101:0001
h02.r0001.ddns0.miako.net.
  IN AAAA 2002:2bf5:0101:0:8302:2bf5:0101:0002
...

1.0.1.0.5.f.b.2.2.0.1.8.lin6.net.
  IN SOA 1.0.1.0.5.f.b.2.2.0.1.8.lin6.net.
  IN NS 1.0.1.0.5.f.b.2.2.0.1.8.lin6.net.
  IN A 43.245.1.1
  IN AAAA 2002:2bf5:0101:0:8302:2bf5:0101:0002

0.0.0.0.1.0.1.0.5.f.b.2.2.0.1.8.lin6.net.
  IN PTR r0001.ddns0.miako.net.
1.0.0.0.1.0.1.0.5.f.b.2.2.0.3.8.lin6.net.
  IN PTR h01.r0001.ddns0.miako.net.
2.0.0.0.1.0.1.0.5.f.b.2.2.0.3.8.lin6.net.
  IN PTR h02.r0001.ddns0.miako.net.
  ...
```

この手法により、配下の無線端末は FQDN 名を持つことが出来るようになる。

4.2　家庭内無線端末のアドレス取得




```
<HomePref> := 2002:2bf5:0101::/48
              (6to4 address of 43.245.1.1)
<WLANPref> := 2002:2bf5:0101:2::/64
<HomeRGID> := 8102:2bf5:0101:0000
<WTermID> := 8302:2bf5:0101:0001
```

図 6　MISP association under HomeRG

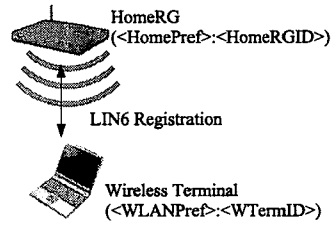


図 7　LIN6 registration under HomeRG

（1） 無線端末にはあらかじめ

- 固有の FQDN (例: h01.r0001.ddns0.miako.net) と
- パスワード

のみを設定する。これらの情報から以下のものが自動生成される。

- LIN6 ID (DNS を利用、例: 8302:2bf5:0101:0001)
- LIN6 Mapping Agent の FQDN (例: r0001.ddns0.miako.net)
- LIN6 Mapping Agent の IPv6 アドレス

(DNS を利用、例: 2002:2bf5:0101:0:8102:2bf5:0101:0000)

- MISP のアカウント (例: h01@r0001.ddns0.miako.net)
- MISP のパスワード
- IPsec の鍵

（2） HomeRG は MISP のビーコンメッセージを無線 LAN 内でブロードキャストする。LIN6 及び MISP 認証用のアカウント情報は HomeRG 内で管理する。

（3） 無線端末は MISP による認証を行い、HomeRG を介して IPv6 インターネットとの通信ができるようになる。

（4） 無線端末は HomeRG 内の LIN6 Agentd に対して、LIN6 プロトコルを用いてプレフィックスを登録する。

4.3 ForeignRG 配下での無線端末のアドレス取得

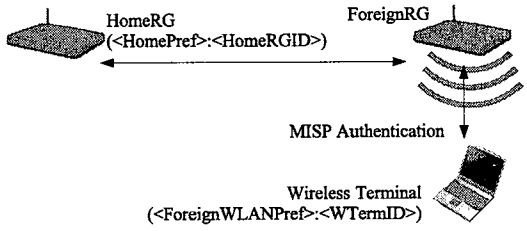


図 8 MISP authentication under ForeigRG

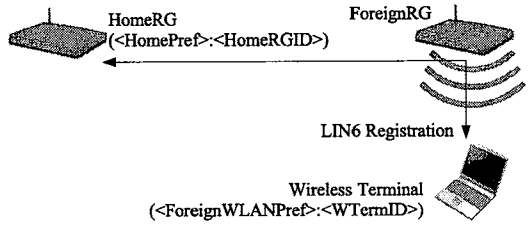


図 9 LIN6 registration under ForeignRG

以下、別の利用者が設置した HomeRG を ForeinRG と呼ぶ。

（1） ForeginRG は MISP のビーコンメッセージを無線 LAN 内でブロードキャストする。

（2） 無線端末は MISP による認証を ForeginRG を介して HomeRG に行う。認証が通れば HomeRG への通信のみ可能となる。なお ForeginRG と HomeRG との間では RADIUS による認証が行われる。

（3） 無線端末は HomeRG 内の MA (lin6agentd) に対して、LIN6 プロトコルを用いて Prefix を登録する。(図 9)

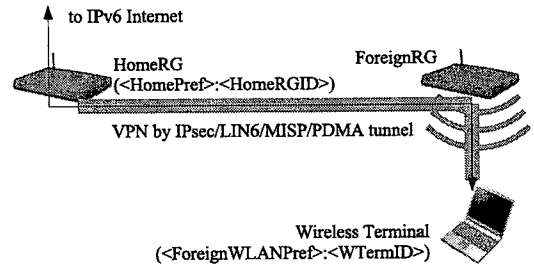


図 10 VPN Connection with a HomeRG by IPsec

4.4 IPsec による HomeRG との VPN 接続

無線端末は、HomeRG との通信を IPsec 化することにより HomeRG を VPN サーバとして利用する。LIN6/MISP/PDMA 上での IPsec のため、接続基地局を移動しても VPN 接続を継続可能となる。また DNS には次のアドレスが登録されているため、LIN6 ホストだけでなく、通常の IPv6 ホストとの通信も転送可能となる。

```
h01.r0001.ddns0.miako.net.
        IN AAAA 2002:2bf5:0101:0:8302:2bf5:0101:0001
```

4.5 GIF トンネルによる IPv4 接続

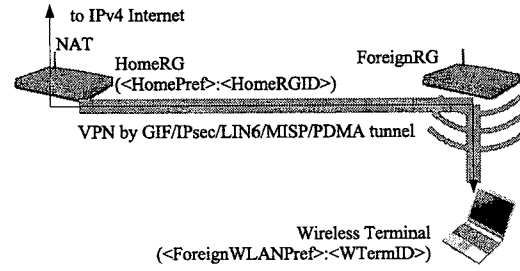


図 11 Access to the IPv4 using a Gif Tunnel

無線端末は HomeRG との間に GIF トンネルにより IPv4 over LIN6 の経路を確立する。(図 11) これにより IPv4 インターネットの接続においても

- LIN6/MISP/PDMA によるモビリティ機能
- IPsec6 による VPN 機能

を利用できる。

5. 実装と評価

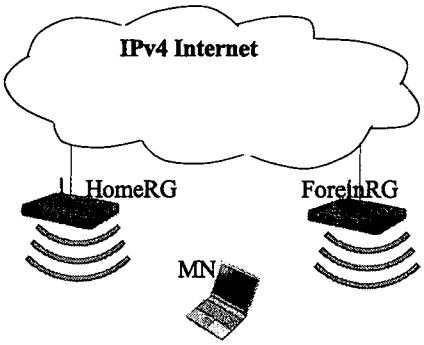
提案したシステムを i386 アーキテクチャ上の NetBSD 3.1 上に実装した。

図 12 のような環境化において、無線端末が、

- HomeRG と ForeignRG との MISP とのアソシエーションにかかる時間
- ForeignRG を介した LIN6 registration にかかる時間

を実測した、そのタイムシーケンスを示す。

基地局から最初のビーコンを受け、二つの基地局との無線認証、IP アドレス割当て、LIN6 registration を完了するまで、23.5 msec である。音声通話のアプリケーションを考慮しても十分高



DNS records

```
h01.r0001.miako.net
    IN AAAA 2002:2bf5:1:1:8102:2bf5:1:10
    IN AAAA 2002:2bf5:2:1:8102:2bf5:2:10
r0001.miako.net (HomeRG)
    IN AAAA 2002:2bf5:1:0:8102:2bf5:1:0 (uplink)
    IN AAAA 2002:2bf5:1:2:8102:2bf5:1:0 (wireless)
r0002.miako.net (ForeignRG)
    IN AAAA 2002:2bf5:2:0:8102:2bf5:2:0 (uplink)
    IN AAAA 2002:2bf5:2:2:8102:2bf5:2:0 (wireless)
h01.r0001.miako.net (MN)
    IN AAAA 2002:2bf5:1:0:8302:2bf5:1:1
```

The addresses of MN

```
2002:2bf5:1:2:8302:2bf5:1:1 (HomeRG)
2002:2bf5:2:2:8302:2bf5:1:1 (ForeignRG)
```

図 12　An experimental wireless environment

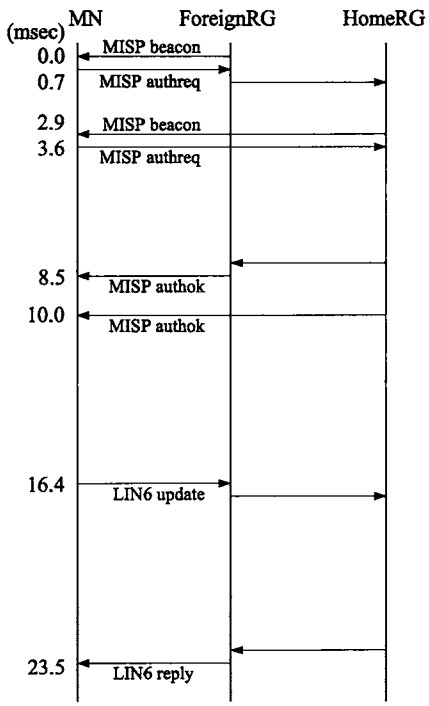


図 13　Time sequence of MISP and LIN6

速であるといえる。

また本方式は同時に複数の基地局と接続可能であるので、make-before-break 型ハンドオーバも実現可能である。

6. おわりに

本稿では、6to4 に対応した無線ブロードバンドルータに、モビリティのための LIN6 の各種サーバ機能と、高速認証プロトコル MISP/PDMA のサーバ機能とを組込むことを提案した。この際、無線端末には FQDN とパスワード情報を予め無線端末に設定するだけでよい。本方式ではサーバ機能は完全に分散配置され、これにより無線環境化でのグローバル IP アドレスと高速認証・ハンドオーバー機能を個人でも容易に利用できるようになる。

今後の課題としては、無線端末において、接続した複数のアクセスポイントの内、どのアクセスポイントを優先してパケットを送信するか決定する方法を検討することなどが挙げられる。

文　献

[1] B. Carpenter and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds," RFC3056, February 2001.

[2] S. Kent, and K. Seo, "Security Architecture for the Internet Protocol," RFC4301, December 2005.

[3] "IEEE Std 802.1X-2001 Port-Based Network Access Control," IEEE, 2001.

[4] "ANSI/IEEE std 802.11 Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer(PHY) Specifications," IEEE, 1999.

[5] H. Morioka, H. Mano, M. Ohmori, and M. Ohta, "MIS Protocol for Secure Connection and Fast Handover on Wireless LAN," , No. 454, The IEEE 20th International Conference on Advanced Information Networking and Applications, Austria, Apr. 18-20, 2006.

[6] H. Morioka, H. Mano, M. Ohmori, M. Ohta, M. Inoue, M. Hasegawa, M. Hirabaru, "Seamless Handover with Wireless LAN, Mobile IP, MISP and PDMA," WPMC2006, USA, 2006.

[7] D. Johnson, C. Perkins, and 1 . Arkko, "Mobility Support in IPv6," RFC3775, June 2004.

[8] M. Ishiyama, M. Kunishi, and F. Teraoka, "An Analysis of Mobility Handling in LIN6," International Symposium on Wireless Personal Multimedia Communication, 2001.

[9] K. Fujikawa, H. Nakano, M. Kunishi, K. Takaaki, "LIN6 Extensions for Simultaneous Utilization of Multiple Wireless Base Stations, Proc. of APSIT 2006, November 2005.