階層型ネットワークアドレス変換を用いたIP移動透過性の検討

岡崎　直宣[1)]・末吉　寿光[2)]

A study of a method to support the mobility of IP addresses using hierarchical IP address translations

Naonobu OKAZAKI, Toshiaki Sueyoshi

Abstract

Recently, various mobile networks have been provided for mobile Internet services. Mobile IP has a key protocol for location management for mobile nodes and is basically intended to support the mobility of global IP addresses. However, it requires each mobile node to extend the functions of its protocol stack and this lead us hard to introduce it.

In this paper, we will propose a new method to realize the mobility of IP addresses using a technique of hierarchical IP address translations.

Key Words:

mobile networks, mobility of IP addresses, network address translator

1. はじめに

近年，第3世代携帯電話に代表される広域セルラー網やホットスポット型の無線 LAN など，さまざまなモバイルネットワークが構築され，IP 通信サービスが提供されつつある。これらのモバイルネットワークにおいて，移動ノード(MN:Mobile Node)の位置管理と移動時のシームレスな通信をサポートする様々なプロトコルが研究されている。MN の移動透過性には，(1) MN が移動しても MN が確立しているコネクションを維持できること，(2) MN の位置によらず MN との通信を開始できること，の二つの要素がある。一般に MN が移動すると，インターネット上の識別子である IP アドレスが変わる。このため MN は通信相手ノード（CN：Correspondent Node）から移動前後で別の MN と判断される。

移動透過性を実現するプロトコルとして策定された Mobile IP では，常に同じ IP アドレス（ホームアドレス）を使うことにより移動透過性を実現できる。Mobile IP は IP 層で実現するため，IP を利用する全てのアプリケーションが移動透過性を持つことができる。しかしながら，Mobile IP を利用する全ての端末に拡張が必要となる。そのため現状では導入が難しい。

ホームアドレスの代わりに DNS の Dynamic Update（いわゆる DDNS ）とネットワークアドレス変換(NAT:Network Address Translator) を組み合わせ，移動透過性を実現する IPMN(IP Mobility with NAT)方式[1]は，モバイルネットワークとインターネットの接続地点にある GFA (Gateway Foreign Agent)によって，配下の複数の FA (Foreign Agent)に接続された全ノードの MAC アドレスを基に管理し，NAT を行うことで移動透過性を実現する。使用者は MN の指定に FQDN を用いるので利便性が高い。また，トンネルを用い

1) 情報システム工学科助教授
2) 情報システム工学科学部生

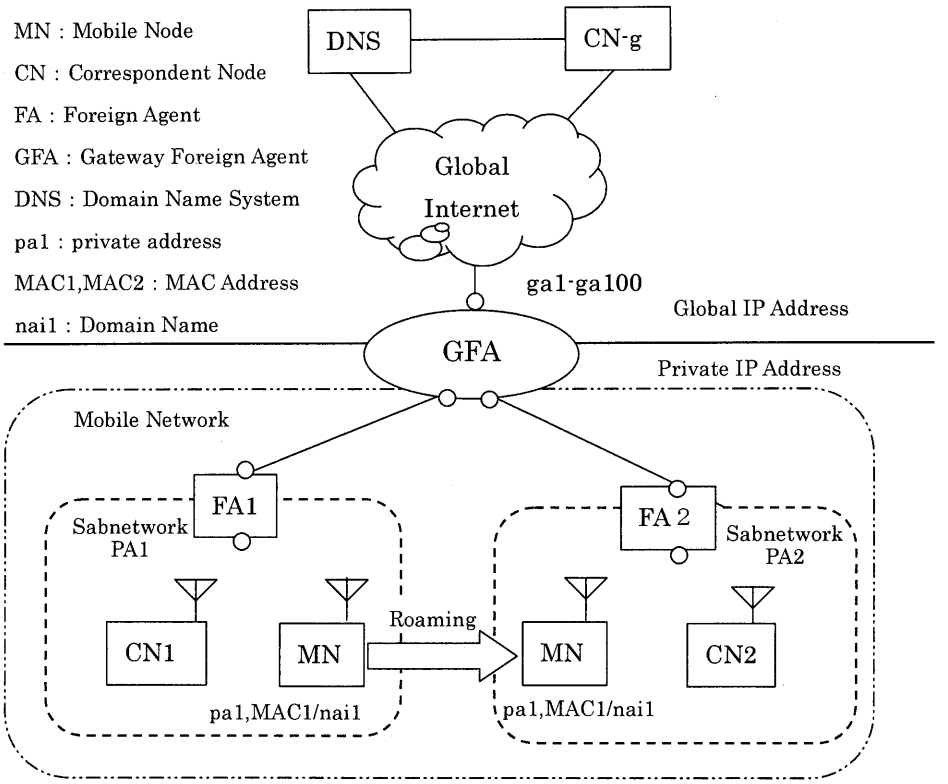

図1　IPMN 方式のネットワーク構成

る MobileIP と比較し，NAT を用いることでパケットオーバーヘッドが少ない。さらに GFA と FA の機能拡張で実現できるため，Mobile IP に比べより容易に実現可能である。しかしながら IPMN 方式では，グローバルアドレスを多く消費する，GFA に負荷が集中する，FA 配下での IP アドレスを柔軟に設定できない，などの課題があった。

そこで本論文では，IPMN 方式に階層構造を取り入れて拡張し，これらの課題を解決した移動透過性の実現方式を提案する。

以下，本論文では，2 章で既存方式である IPMN 方式について述べる。3 章では，提案方式について述べ，4 章で，プロトタイプシステムの構築について述べる。最後に 5 章でまとめと今後の課題について示す。

2. 既存の IP 移動透過性の実現方式

既存の IPMN 方式は，ホームアドレスの代わりに FQDN を用い，MN のローミング時に NAT を用いてコネクションが維持できる移動透過性の実現方式である。

以下，2．1 で IPMN 方式のネットワーク構成，2．2 で IPMN 方式における GFA，FA の機能，2．3 で通信シーケンス，2．4 で IPMN 方式の問題点を述べる。

2．1 ネットワーク構成

IPMN 方式のネットワーク構成を図 1 に示す。モバイルネットワークに GFA（Gateway Foreign Agent）及び FA を導入したものである。GFA と FA の詳細については 2．2 にて後述する。モバイルネットワークは 1 つの管理主体にて管理される。ここでは GFA が，モバイルネットワークの管理を行う。モバイルネットワーク内の各サブネットに存在するプライベート IP アドレスは重なっていないものとする。FA はこのサブネットを管理する。モバイルネットワーク内では，内部の FA により MN の位置管理が行われている。通信相手ノードはグローバルネットワーク上に存在する CN-g，同じサブネット内の CN1，別のサブネット内の CN2 と表す。この図 1 で MN が初期接続時に FA1 で割り当てられたプライベート IP アドレ

スを pa1 とし，MN の MAC アドレスを MAC1，ドメインネームを”nai1”とする。また MN がグローバルネットワークと通信を行う際，GFA の NAT により割り当てられるグローバル IP アドレスを ga1 とする。

2．2 GFA/FA の機能

ここでは IPMN 方式における GFA と FA の機能を述べる。

2．2．1 GFA

GFA は，モバイルネットワークとインターネットの接続地点にある NAT 機能を持ったルータである。IPMN 方式では，MN のドメインネーム登録の際に MN の IP アドレスではなく，GFA のグローバル IP アドレスの 1 つである ga を登録するメッセージ（RegReq メッセージ）を送信する。GFA は，NAT によるグローバル IP アドレスとプライベート IP アドレスの対応を NAT テーブルに記録する。このとき，MAC アドレスをプライベート IP アドレスに付加する。NAT テーブルに登録した MAC アドレスと，同一の MAC アドレスが NAT テーブルに存在すると，GFA は NodeRes メッセージに NAT テーブルにある MAC アドレスとプライベート IP アドレスをパラメータ値として送信する。GFA は，ドメイン登録メッセージを送信すると，登録完了メッセージ（RegAck メッセージ）を FA に送信する。

2．2．2 FA

MN が FA の管理するサブネットに接続し，プライベート IP アドレスを MN に割り当てる。IPMN 方式では，FA は MN 接続時に得る MAC アドレスを NodeReq メッセージとして GFA に送り，GFA からの NodeRes メッセージのパラメータ値で MN が初期接続か FA 間ローミングかを判断する。このときのパラメータ値に new_node が含まれていると，MN は初期接続と判断し，new_node 以外のパラメータ値であるとローミング時の接続と判断する。MN が初期接続時は DHCP によって IP アドレスを割り当てる。ローミング時は DHCP で割り当てるプライベート IP アドレス pa2 と GFA に登録されている NAT テーブルのプライベート IP アドレス pa1 を対応付けし，NAT テーブルを作成する。

2．3 IPMN 方式の通信シーケンス

インターネット上の CN-g(Correspondent Node) が MN に通信を始めようとするとき，CN-g は MN のドメインネーム”nai1”を DNS に問い合わせる。DNS は”nai1” と対応する ga1 を返信する。CN-g は ga1 宛てにパケットを送信し，パケットを受信した GFA は NAT を行う（ga1>pa1）。宛先 IP アドレスが pa1 となり，MN へと転送される。

MN が FA2 にローミングした場合，FA2 は pa2 と GFA に登録されている pa1 を対応付けし，GFA は pa2 と ga1 を対応付ける。以降 ga1 宛てのパケットは，FA2 を経由し MN に転送される。
これにより移動透過性を実現し，通信中に MN が新たなサブネットに移動した場合にも，MN は移動前 IP アドレス(pa1)を変えずに，通信が途切れることなく通信の継続ができる。

2．4 IPMN 方式の課題点

IPMN 方式では，FQDN を用いることでユーザーの利便性を高め，また NAT を行うことで通信の継続性，移動透過性を実現した。しかしながら IPMN 方式では，次の三つ課題が生じてしまう。一つは，モバイルネットワークの外部に位置する DNS を利用するため，モバイルネットワーク内の MN 数と同数のグローバルアドレスを消費してしまうという課題である。もう一つは，モバイルネットワーク内にある全ての MN の MAC アドレスを GFA が管理するため，負荷が GFA に集中してしまうという課題である。さらに，GFA が MN に IP アドレスを割り当てるため，FA 配下で使用する IP アドレスを柔軟に設定できないという課題がある。

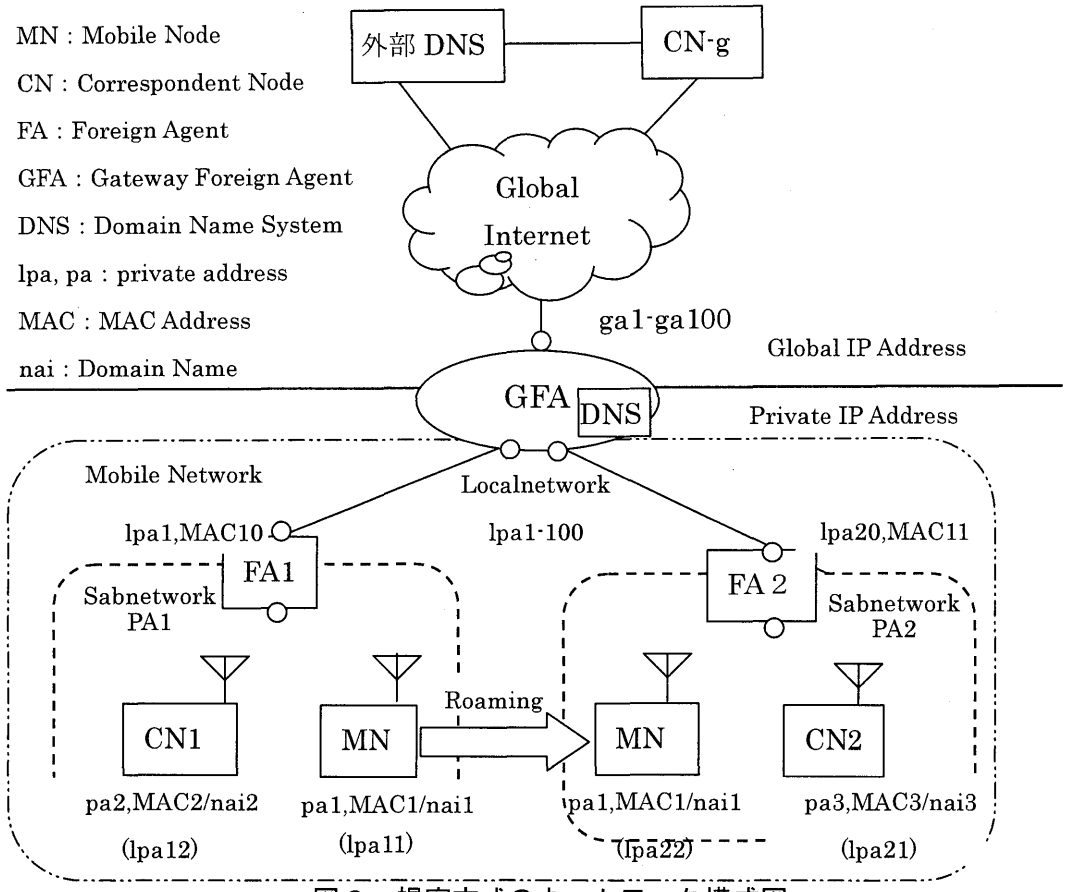

図２　提案方式のネットワーク構成図

3. 提案方式

本論文では 2. 4 節で述べた課題点を解決するためにGFA に DNS 機能を付加し，GFA は FQDN を基に，FA は MAC アドレスを基に管理する階層構造を取り入れた，階層型 IPMN 方式を提案する。

本提案方式の特徴は，GFA 配下のノード同士の通信において，互いに常に相手が一つ上流のネットワークに属しているように FA は配下の MN に対して見せることである。通信中に相手が別の FA に移動しても，FA により適切に NAT が行われることで通信を維持することができる。

内部に接続する MN は原則として GFA と同一のドメイン部を持つ FQDN を使用するが，サービスの相互ローミングも考慮し外部ドメインを利用することも可能である。

3. 1 ネットワーク構成

提案方式のネットワーク構成を図 2 に示す。モバイルネットワークは GFA が各端末の FQDN を基に管理を行う。FA はこのサブネットを各端末の MAC アドレスを基に管理する。モバイルネットワーク内では，内部の FA により MN の位置管理が行われている。通信相手ノードはグローバルネットワーク上に存在する CN-g，同じサブネット内の CN1，別のサブネット内の CN2 と表す。この図 2 で MN が初期接続時に FA1 で割り当てられたプライベート IP アドレスを pa1 とし，MN の MAC アドレスを MAC1，ドメインネームを”nai1”とする。また MN がグローバルネットワークと通信を行う際，GFA の NAT により割り当てられるグローバル IP アドレスを ga1 とし，モバイルネットワーク内で通信する際に FA により割り当てられるプライベートアドレスを lpa2 とする。

CN1 が FA1 で割り当てられたプライベート IP アドレスを pa2 とし，CN1 の MAC アドレスを MAC2，ドメインネームを”nai2”とする。また

CN1 がグローバルネットワークと通信を行う際，GFA の NAT により割り当てられるグローバル IP アドレスを ga2 とし，モバイルネットワーク内で通信する際に FA により割り当てられるプライベートアドレスを lpa3 とする。CN2 が FA2 で割り当てられたプライベート IP アドレスを pa3 とし，CN2 の MAC アドレスを MAC3，ドメインネームを”nai2”とする。また MN がグローバルネットワークと通信を行う際，GFA の NAT により割り当てられるグローバル IP アドレスを ga3 とし，モバイルネットワーク内で通信する際に FA により割り当てられるプライベートアドレスを lpa21 とする。

3．2 拡張機能

ここでは本提案方式における GFA と FA の機能を述べる。

3．2．1 FA

MN が FA の管理するサブネットに接続したのを検知すると，その FA はプライベート IP アドレスを MN に割り当てる。提案方式では，FA は MN 接続時に DHCP 要求で得る nai を NodeReq メッセージとして GFA に送り，GFA からの NodeRes メッセージのパラメータ値で MN が初期接続か FA 間ローミングかを判断する。このときのパラメータ値に new_node が含まれていると，MN は初期接続と判断し，new_node 以外のパラメータ値であるとローミング時の接続と判断する。MN が初期接続時は DHCP によって IP アドレス pa を割り当てる。ローミング時は移動前 FA に MN について NodeReq し，NodeRes メッセージに含まれる pa を MN に割り当てる。また pa と対になる lpa を割り当て NAT に登録し，GFA に nai と lpa の対応を DDNS 登録申請する。

3．2．2 GFA

GFA は，モバイルネットワークとインターネットの接続地点にある DNS 機能と NAT 機能を持ったルータである。提案方式では，MN の nai1 が GFA と同一ドメインであれば，lpa と nai の対応を DNS に付加する。DNS 登録後登録完了メッセージ(RegAck メッセージ)を送信する。MN のドメイン名が GFA と異なる場合，外部の DNS に GFA のグローバル IP アドレスの 1 つである ga を登録するメッセージ(RegReq メッセージ)を送信する。送信後登録完了メッセージ(RegAck メッセージ)を FA に送信する。FA からの NodeReg メッセージに含まれる nai と，同一の nai が DNS に存在すると，GFA は NodeRes メッセージに nai とプライベート IP アドレス lpa をパラメータ値として送信する。

GFA は，外部へのアクセス及び外部からのアクセスがあると，NAT テーブルを参照しグローバル IP アドレス ga を割り当て，ga とプライベート IP アドレス lpa の対応を NAT テーブルに記録する。また ga と nai の対応を DNS に登録する。

3．3 通信シーケンス

提案方式を実現するためには，MN の登録手順と通信を行うための手順(通信プロトコル)が必要である。提案方式の通信プロトコルは，case1 MN の初期登録，case2 MN の移動登録がある。さらに，(a)CN から MN への着信，(b) モバイルネットワーク内のノード間の通信，(c)MN のローミング時の通信，の 3 通りについて考える必要がある。

以下では，基本動作を case1，case2 にて示し，さらに(a)，(b)，(c)の場合の動作を述べる。

3．3．1 移動端末の管理

MN が FA に接続すると，FA は MN の MAC アドレスを検出する（MAC1 detect)。FA は nai1 を GFA に送信する（NodeReq [nai1])。GFA は NAT テーブルに nai1 と一致するエントリを検索する。GFA の DNS に nai1 のエントリが存在するかどうかによって，以下の 2 つの場合に分けられる。

case1　初期登録

GFA の NAT テーブルに MAC1 のエントリが存在しない場合，MN の初期登録時とみなす。このとき以下のような動作を行う（図 3 a)。

(i)FA は nai1 を GFA に送信する(NodeReq [nai1])。

(ii)GFA は DNS に nai1 と一致するエントリを検索

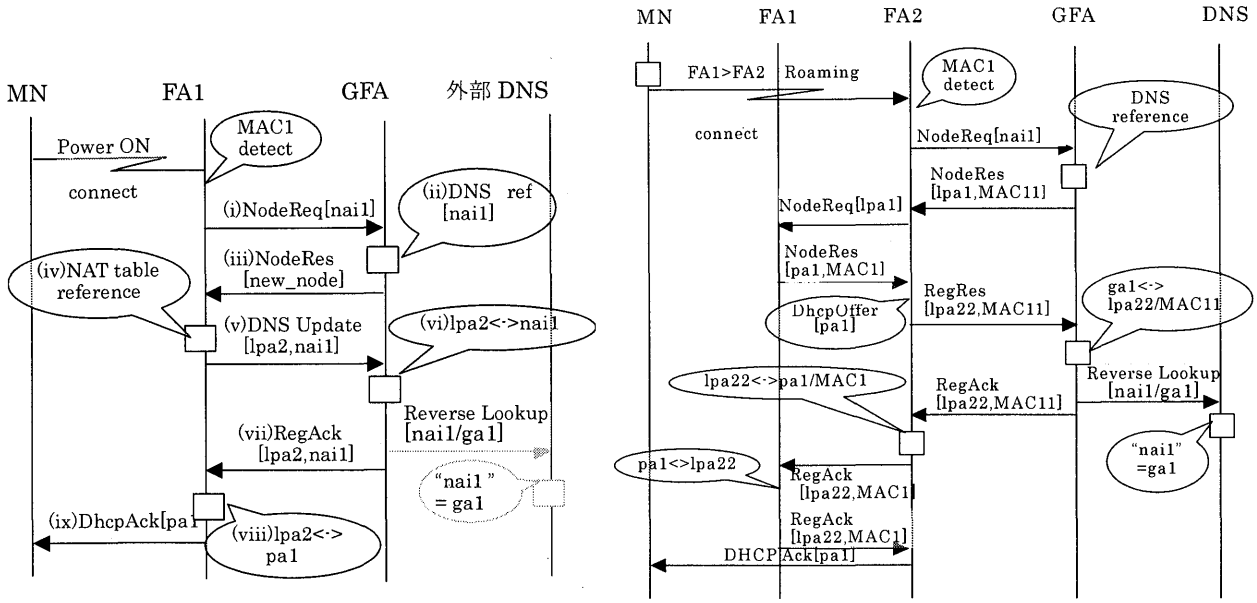

図３　移動端末の管理

する(DNS reference)。

(iii)GFA はFA にパラメータ値[new_node]を含んだ NodeRes メッセージを送信する(NodeRes [new_node])。

(iv)FA は NAT テーブルを参照し，利用可能なアドレス範囲のうち使用されてないものをMN用IP アドレスとして lpa2 を割り当てる(NAT table reference)。

(v)FA は MN 用の IP アドレス lpa2 と nai1 を GFA 送信する(DNS Update[lpa2，nai1])。

(vi)nai1 が GFA1 と同じドメインであれば (viii)に，異なればGFA はNAT テーブルを参照し，グローバル IP アドレス ga1 を割り当て ReverseLookup メッセージを送信し，外部 DNS は MN のドメインネームに新たな IP アドレスを登録する(“nai1” =ga1)。

(vii)GFA はDNS 更新を行うと，FA1 に DNS Update 完了メッセージを送信する(RegAck[lpa2，nai1])。

(viii)FA1 は NAT テーブルに新たな条件を登録する(lpa2<->pa1)。

(ix)FA1 はMN に pa1 を割り当てる(DhcpAck[pa1])。

case2　移動登録

GFA の DNS に nai1 のエントリが存在する場合，MN はローミングによる FA2 への接続と判断する。このとき以下のような動作を行う（図 3 b)。

(i)FA は nai1 を GFA に送信する(NodeReq[nai1])。

(ii)GFA はDNS に nai1 と一致するエントリを検索する。

(iii)GFA は FA2 にパラメータ値[lpa2]を含んだ NodeRes メッセージを送信する(NodeRes[lpa2])。

(iv)移動元の FA1 に対して，lpa2 に関連した pa を問い合わせる(NodeReq[lpa2])。

(v)FA1 はNAT テーブルを参照する(NAT table ref [lpa2])。

(vi)FA1 は FA2 にパラメータ値[pa1，MAC1]を含んだ NodeRes メッセージを送信する(NodeRes[pa1，MAC1])。

(vii)FA は NAT テーブルを参照し，利用可能なアドレス範囲のうち使用されてないものをMN用IP アドレスとして lpa22 を割り当てる(NAT table reference)。

(viii)FA はMN用のIP アドレス lpa22 と nai1 をGFA 送信する(DNS Update[lpa2，nai1])。

(ix)nai1 が GFA1 と同じドメインであれば (v)に。異なればGFA はDNS を参照し，nai1 に対応するグローバル IP アドレス ga1 と共に ReverseLookup メッセージを送信し，外部 DNS は MN のドメインネームに新たな IP アドレスを登録する(“nai1”

=ga1)。
(x)GFA は DNS 更新を行うと，FA1 に DNS Update 完了メッセージを送信する(RegAck[lpa2，nai1])。
(xi)FA2 は NAT テーブルに新たな条件を登録する(lpa22<->pa1)。
(xii)FA2 は MN が lpa22 に移動したことを FA1 に送信する(RegReq [pa1，lpa22，MAC1])。
(xiii)FA1 は pa1 を開放し，NAT テーブルに新たな条件を登録する(lpa2>lpa22)。
(xvi)FA1 は FA2 に完了メッセージを送信する。
(xv)FA2 は MN に pa1 を割り当てる(DhcpAck[pa1])。

3．3．2 通信シーケンス

ここでは，グローバルネットワークからの着信，同一サブネット内同士の通信，MN のローミング時について述べる。

(a) グローバルネットワークからの着信

CN-g が MN に通信を行うときの手順を図 4 に示す。

(i)MN のドメインネーム”nai1”を DNS に問い合わせる。

(ii)DNS は”nai1”に登録してある ga1 を返信する。

(iii)CN-g は ga1 宛てのパケットを送信する。

(iv)GFA は受け取ったパケットを NAT し FA1 に転送する。(ga1>lpa11)

(v)FA1 は受け取ったパケットを NAT し MN へ転送する。(lpa11>pa1)

(b) モバイルネットワーク内のノード間の通信

CN1 が MN へ通信を行うときの手順を図 5 に示す。

(i)MN のドメインネーム”nai1”を DNS に問い合わせる。

(ii)DNS は”nai1”に登録してある lpa11 を返信する。

(iii)CN1 は lpa11 宛てのパケットを送信する。

(iv)FA1 は受け取ったパケットを NAT し MN に転送する。(lpa11>pa1，　pa2>lpa12)

(c) MN のローミング時

MN のローミング時登録動作は，3．3．1 の case2 の登録動作を行う。(b)の通信中に MN が FA2 にローミングした場合の手順を図 5 に示す。図 5 中の太矢印は MN のローミングを表す。

(i) CN1 からのパケットは FA1 が NAT を行い FA2 に転送する(lpa11>lpa22，　pa2>lpa12)。

(ii) FA2 は NAT を行い MN に転送する(lpa22>pa1)。

このことより，新たなサブネットに移動した場合にも，MN は移動前 IP アドレス(pa1)と変わらず，また通信が途切れることなく通信の継続ができる。

4. プロトタイプシステム

ここでは提案方式の実現性を示すために必要である図 3 b におけるステップ(xii)とステップ(xiii)の機能について，実装の設計を行った。

プロトタイプシステムにおいて，GFA 及び FA は FreeBSD 5．3 で稼動するパソコンを使用する。DDNS サーバ，DHCP サーバについては既存の BIND，ISC－DHCP サーバを利用する。また NAT については PF を利用する。また MAC アドレスと対になる割当 IP アドレスは固定し，ノードの移動は CN1 と MN の通信中に，MN が FA1 配下から FA2 配下への移動に限定する。割当 IP アドレスと対になる仮想 IP アドレスは初期値を与え，ローミング時にプログラムにより一部変更する。

図 3 b におけるステップ(xii)からステップ(xvi)の機能は以下のようになる。

(i) FA1 側のプログラムは特定のポートを常時監視し，FA2 側のプログラムは，ISC-DHCP サーバに対し OMPI 関数にて MN の存在を常時監視する。

(ii) FA2 側のプログラムは，MN を検知すると，FA1 の特定のポート宛てにパラメータ値[pa1，lpa22，MAC1]を含むパケットを送信する。

(iii) FA1 側のプログラムは，パケットを受信するとパラメータ値に従い NAT テーブルを更新する (pa1>lpa22) 。

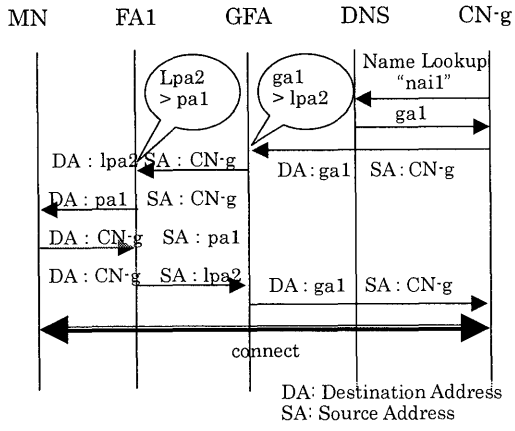

図4 CN-g から MN への通信開始時の動作

以上のプロトタイプシステムにより提案手法の特徴である，仮想 IP アドレスを用いて通信すること，そして通信中に相手が別の FA に移動しても，FA により適切に NAT が行われることで通信を維持できることが確認できる。

5．まとめ

本論文では，IP 移動透過性を実現する方式として，既存の IPMN 方式に階層型構造を取り入れた，階層型 IPMN 方式を提案した。

提案方式では，GFA に DNS 機能を付加することで，モバイルネットワークと同一ドメインに属する MN には，外部との通信時に動的にグローバル IP アドレスを確保することが可能になり，IPMN 方式でのグローバルアドレスが多く消費されるという課題を解決した。また，GFA は FQDN を基に，FA は MAC アドレスを基に管理する階層型構造を取り入れたことにより，負荷の分散が可能になり，GFA に負荷が集中するという課題を解決した。さらに，ネットワークを階層構造にすることより，GFA，FA 間と FA 配下とで独立した IP アドレス空間が使用可能になり，FA 配下で使用する IP アドレスを柔軟に設定できないという課題を解決した。

今後の課題として，プロトタイプシステムを実装し，MN のローミング時に通信の継続が可能であることを確認する必要がある。また MN のローミング時における通信の中断時間が TCP のコネクションや上位アプリケーションに与える影響を詳細に調べる必要がある。

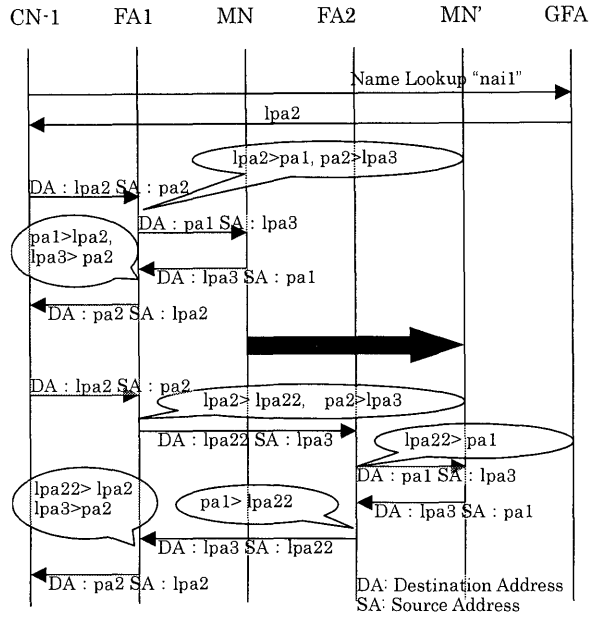

図5 CN-1・MN 間通信時に移動した場合

参考文献

[1] 岡崎 直宣,板山 俊一, “NAT を用いた IP 移動透過性の検討,” 宮崎大学工学部紀要, Vol.33, pp.391-398,2004.

[2] 井戸上 影,久保 健,横田 英俊,“プライベートアドレスを使用するモバイルネットワーク間のローミング手順とその実装,” 情報処理学会, Vol.42,No.12, pp.2958-2967,2003.

[3] 岡川 隆俊,澤田 政宏,西田 克利,趙 晩熙, “IP2 におけるパケットルーチングメカニズム,” 電子情報通信学会 信学技報 IN2002-123,151(2002-11,12).

[4] R. Droms, “ Dynamic Host Configuration Protocol,” RFC2131,1997.

[5] P. Vixie,S. Thomson,Y. Rekhter,J. Bound, “Dynamic Updates in the Domain Name System (DNS UPDATE) ,” RFC2136,1997.

[6]ASH Multimedia Lab., “ UNIX Network BIND-DNS サーバの構築と管理,” ソフトバンクパブリッシング株式会社,2002