ヒューマンインタフェース 86－2
モーバイルコンピューティング 11－2
（1999．11．25）

境界ルータを用いたMobile IPの経路最適化に関する研究

村上慎吾† 木村成伴†† 海老原義彦††

インターネットプロトコル(IP)を拡張し移動透過な通信を実現するためプロトコルとしてMobile IPが提案されているが，これは経路冗長性の問題があることが知られている．これに対しMobile IPの経路最適化方式が提案されているが，これはモバイルホスト(MH)の全ての通信相手(CH)にも変更を要するため，多大なコストを要する．そこで本稿では上述の経路最適化方式を基に，CHに一切変更を加えず，境界ルータ(BR)のみを変更することで実現可能な，経路最適化方式を提案する．また，BRを設置したサブネット内にBRを置いた場合，互いに負荷分散する機能も提供する．最後に，ネットワークシミュレーションによりこれらの提案方式を評価する．

Route Optimization in Mobile IP with Boundary Routers

SHINGO MURAKAMI,† SHIGETOMO KIMURA†† and YOSHIHIKO EBIHARA††

Mobile IP allows transparent interoperation for mobile hosts by extending Internet Protocol (IP), but has the problem of wasteful longer routing. Although route optimization extension of Mobile IP is proposed to solve this problem, it needs very large costs to modify any correspondent hosts (CHs) of mobile hosts. This paper realizes route optimization which modifies only boundary routers (BRs) but not any CHs, based on the above optimization. It also provides load distribution facility when a BR is set within the subnet with a BR. In final, our proposal of route optimization has been evaluated by network simulations.

1. はじめに

近年，携帯型コンピュータの小型化，高性能化が進み，モバイルコンピューティング環境が整いつつある．しかし，インターネットでの現在の標準プロトコルであるインターネットプロトコル(IP)はコンピュータがネットワーク上の位置を動的に移動することは全く考慮されていなかった．このため，移動ホスト(MH：Mobile Host)はドメインを移動する度に，DHCPなどを利用して，そのIPアドレスを変更する必要があった．この方法ではIPアドレスとMHとの一対一の対応関係が崩れてしまい，MHの通信相手(CH：Correspondent Host)はIPアドレスからMHを識別できなくなるという問題があった．これを解決するためにIPを拡張したMobile IP[1)]が開発された．

Mobile IPでは移動ホストがオリジナルのIPアドレスのみで通信を行うための手段を提供するが，MHからCHへの通信経路が冗長になるという問題を有する．このため，Mobile IPを拡張して経路を最適化する方式がドラフト2)で提案されているが，この方式ではすべてのCHを変更する必要があった．そこで本稿では，CHに対しては変更を行わず，境界ルータ(BR：Boundary Router)のみを変更するだけで実現可能な経路最適化方式を提案する．本方式では，更に，BRを複数配置し互いに負荷分散する機能も提供する．最後に，ネットワークシミュレーションにより，これらの方式の性能評価を行う．

2. Mobile IP

2.1 Mobile IPによる通信

Mobile IPによる通信の概要を図1に示す．MHが通常接続しているネットワークはホームリンクと呼ばれる．このMHが，図1のようにホームリンクから外部リンクへ移動したとする．このとき，MHの通信相手CHはMHが移動したことは知らないため，CHがMHに送信したIPパケットはMHのホームリンクに向けて送信される．ホームリンク上でMHの移動を管理するHA(Home Agent)はこれを代理受理し，MHが現在いる外部リンク上のFA(Foreign Agent)へトンネリングにより転送する．ここで，トンネリングとはMH宛のIPパケットに，宛先をFAのアドレス(気付アドレス)，送信元をHAのアドレスとしたIPヘッダを更に付加して転送する方式である．このパケットを受け取ったFAはトンネリングによるヘッダを外し，MHへ配送する．このようにCHからMH宛のパケットは常にHAを経由するため，経路に冗長性があるという問題が発生する．但し，MHからCH宛のパケットは直接CHへ送信される．こ

† 筑波大学大学院工学研究科
Doctoral Program in Engineering ,University of Tsukuba
†† 筑波大学電子・情報工学系
Institute of Information Sciences and Electronics, University of Tsukuba

の経路冗長問題を解決するために Mobile IP の拡張として MIP 経路最適化[2] が提案されている．

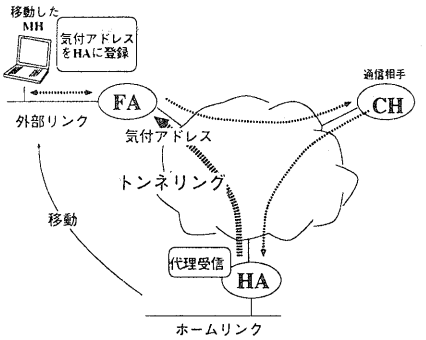

図1 Mobile IP による通信

2.2 MIP 経路最適化

MIP 経路最適化では，各 CH に結合エントリを導入し，ここに MH の移動先を示す気付アドレスを保持させる．これにより，CH が MH と通信する場合でも，CH が MH の結合エントリを持てば，その気付アドレスへトンネリングを使って直接送信できる (図 2参照)．

CH が MH の結合エントリを持たない場合，従来の Mobile IP と同様に，HA によるトンネリングが行われる．これと同時に，HA は BUM (Binding Update Message) を CH へ送信し，MH の気付アドレスを通知する．CH はこれを基に MH の結合エントリを作成し，次のパケットから直接 MH へ送信する (図 3参照)．

この方法は CH が MH と最適経路で通信する手段を提供するが，すべての CH に変更を要求するため，多大なコストを要する．

3. 境界ルータを用いた経路最適化

本節では，前節で述べた MIP 経路最適化を基に，CH の変更を回避し，境界ルータ (BR) のみを変更するだけで実現可能な経路最適化方式を提案する．ここで，本方式で用いる BR とは，外部ネットワーク側からサブネット内のすべての CH へ向かうパケット，及びサブネット内のすべての CH から外部ネットワーク側へ向かうパケットがすべて通過するという条件を満たすルータである．

本方式では，BR にサブネット内に所属する CH のための結合エントリを持たせる．そして，BR は HA から CH 宛に BUM が送信されると，これを捕捉し，自分自身に MH の結合エントリを登録する (図 4(1)(2) 参照)．但し，結合エントリが溢れ，新規のエントリが登録できない場合は，本稿では最も古くから利用されていないエントリを削除し，新規登録を行うものとする．BR は常に自分の内側からのパケットの宛先を監視し，結合エントリ中にある MH のホームアドレスだった場合は，トンネリングによりその気付アドレスに転送する (図 4(3) 参照)．

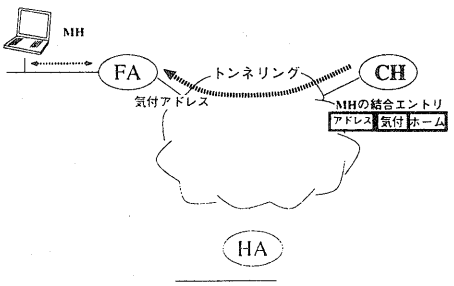

図2 CH が結合エントリを持っている場合

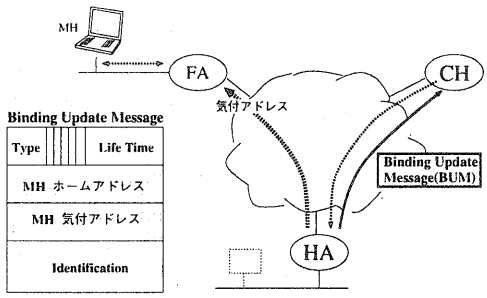

図3 CH が結合エントリを持っていない場合

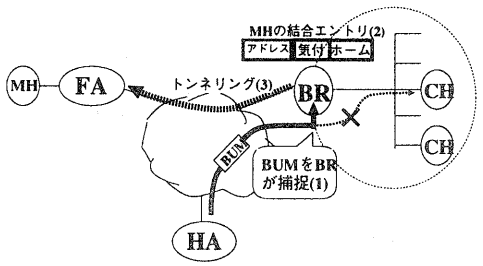

図4 BR による BUM の捕捉

ところで，HA から送られる BUM の宛先は MH に対してデータグラムを送信した CH の IP アドレスであるため，通常の IP ルーティングでは BR はこれを捕捉することはできない．このため，本方式では UDP のポート番号を監視する方法により BUM を捕捉する方法を提案する．

3.1 BUM の捕捉方法

ドラフト 2) の規定では BUM は UDP の 434 番ポートを用いて送付される．従って，BUM を捕捉するためには，このポートを監視し，かつ，そのタイプ番号が 18 であることを確認すれば良い．しかし，より高速に BUM を捕捉するため，本方式では，BUM を未使用 UDP ポート番号に割り当てることを提案する．従って，BR はこの UDP ポート番号を監視し，かつ受信先アドレスが自分のサブネット内のアドレスであった場合に限り，そのパケットを捕捉する．その後，BR は HA を認証し (後述)，これに成功した場合は MH のための結合エントリを作る．

4. 複数の BR による結合エントリ分散機能

比較的大きな規模のサブネットになると，サブネット

の中にサブネットが存在すると考えられる．このとき，内側のサブネットとこれを包含する外側のサブネットに前節で提案した BR を設置したとしても，外側にある BR が BUM をすべて捕捉することになり，内側の BR は全く機能しない．

そこで本節では，BR が同一サブネット内に複数存在したときにもお互いが協調して BUM の処理を行う協調動作機能を提案する．これにより結合エントリの総数が増加すると共に BR の負荷分散につながると期待される．

ここで，相対的に外側にある BR を上位 BR，それより内側にある BR を下位 BR と呼ぶことにする．例えば，図5において，BRn $(n = 1, 2, 3)$ は，以下で提案する協調機能を持った境界ルータ，R は経路最適化機能を持たない従来のルータであるとすると，BR2 に対して，BR1 は上位 BR，BR3 は下位 BR である．本提案方式では，CH に近い下位 BR に結合エントリを持たせる方針を採る．但し，輻輳などによりその BR の負荷が過負荷になった場合のために，新たな結合エントリの作成を拒否できる仕組みを設ける．

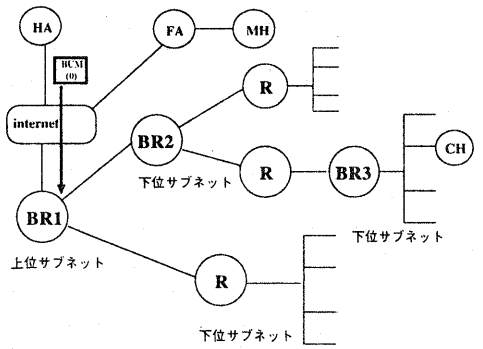

図5　上位と下位サブネット

4.1　協調動作のための拡張

まず，各 BR に同サブネット内の直接下位 BR の存在を示す PET (Partner Entry Table) を動的に持たせる．図5の例では，BR1 の PET は BR2 のエントリを，また，BR2 のそれは BR3 のエントリを持つ．PET の各エントリには以下のフィールドが存在する．

- 下位 BR の IP アドレス
- このエントリの保持期限：このフィールドの値は一定時間ごとに減算され，0 になると更新要求メッセージが下位 BR に送信される．
- Ack タイマ：下位 BR に応答を要求した場合に，その応答が返信されるまでの許容待ち時間．この時間までに応答を受信できないと，その BR のエントリは PET から削除される．
- 下位 BR の受け持つネットワークアドレスとそのサブネットマスク，及び，これらの組の個数を有する．

次に，PET に基づいた協調動作を行うため，以下に示す新たなメッセージを5つ定義する．まず，最初の3つを図6～8に示す．これらは 1) の BUM を拡張したものであり，それぞれ，BUM(0), BUM(1), BUM(2) と呼ぶ．また，これらの図に BUM 認証拡張フィールドがあるが，これについては次節で述べる．

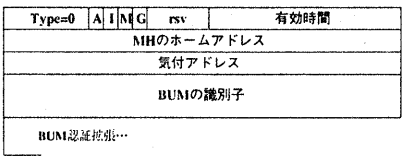

図6　BUM(0) の構成

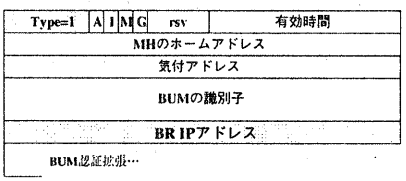

図7　BUM(1) の構成

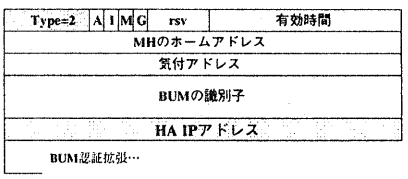

図8　BUM(2) の構成

まず，BUM(0) は従来の BUM と同等であり，主に HA から CH に対して MH のホームアドレスと気付アドレスを通知するために用いられる．BUM(1) は BUM(0) を捕捉した上位 BR が下位 BR に対して送付するものであり，これにより，上位 BR は下位 BR が結合エントリを作成し，その後，上位 BR への返答 (BUM(2) または後述の PAM) を期待する．この BUM(1) に対して下位 BR が結合エントリが作成できなかった場合は，上位 BR に対して BUM(2) を通知し，上位 BR で結合エントリを作成するよう依頼する．ところで，BR が負荷過重や結合エントリのあふれなどのため所定の処理が行えない状態で BUM(0) または BUM(1) を捕捉した時は，何の処理を行わずにこれを CH 側へ転送する．また，BUM(2) を捕捉した場合は，結合エントリを作成せずにこれを破棄する．これらにより結合エントリが生成できなかった場合でも，CH から送られたメッセージは HA が MH に転送するため，CH と MH 間の通信は維持される．

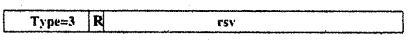

図9　PURM (PET Update-Registration Message) の構成

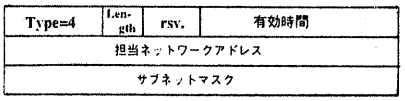

図10　PAM (PET Ack Message) の構成

残り2つのメッセージを図9と図10に示す．前者を

PURM (PET Update-Registration Message), 後者をPAM (PET Ack Message) と呼ぶ. PURM は R ビット (Registration ビット) によりその働きが異なる. R ビットがオン (1) の場合は, 上位 BR が未知の下位 BR を探索する時に送出される. これを捕捉した下位 BR は, 自分の担当するネットワークアドレスとそのサブネットマスクを PAM によって知らせる. 担当するネットワークアドレスが複数ある場合はこれを列挙し, その数を PAM の長さ (length) フィールドに記す. 但し, BR が負荷過重や PET エントリのあふれなどのため所定の処理が行えない状態で PAM を受けとった場合は, これを破棄する. R ビットがオフ (0) の PURM は, PET にある下位 BR のエントリの保持期限が 0 になると上位 BR が下位 BR に対して送付するものである. これに対して, 下位 BR は PAM で応答するが, ここでは長さフィールドを 0 として, 有効時間のみを通知する. 但し, 担当ネットワークに変更があった場合については, R ビットがオンの PURM に対する応答に準じる.

4.2 BR 協調動作の概要

以下では, 図 5において, HA から BUM(0) が CH に対して送付された時に行われる BR の協調動作について概説する.

BR1 が BUM(0) を捕捉すると, PET エントリにある担当ネットワークアドレスとサブネットマスクの内, CH を対象とするものがあるかどうかを検索する. 図 5の場合では, BR2 がこれに該当する. これが存在する場合は, BUM(1) の BR IP アドレスフィールドに BR1 のアドレスを入れて, これを CH に対して送る. このとき, BUM(1) の送信元アドレスも BUM(0) と同じ HA のままにする. また, PET エントリの Ack タイマを起動し, タイムアウトまでに下位 BR からの応答 (BUM(2) または PAM) がなければ, そのエントリを削除する. ところで, BUM(0) が直接 BR 宛に送付される時がある. これは, MH が移動して FA を変更した場合であり, このとき, 例えば, BR2 が移動前の FA にデータを送付するとこの FA は移動後の FA にデータを転送すると共に, BWM (Binding Warning Message) を HA に送付する. その後, HA がデータを転送した BR2 宛に BUM(0) を直接送付し, FA が変更されたことを BR2 に通知しようとする[2]. しかし, BR2 の担当ネットワークアドレスに BR2 のアドレスが含まれている必要はないため, 上述の検索方法だけでは BR2 に BUM(1) が送付されない可能性がある. このため, PET エントリを検索する際は, BR1 自身のアドレスと PET エントリに登録されている BR2 のアドレスも対象とする必要がある. 前者の場合は, 同時に BR1 内の結合エントリを更新する.

一方, 該当する PET エントリが存在しない場合は, BR1 は MH の結合エントリを作成する. 同時に R ビットをオンにした PURM を CH に対して送出し, 下位 BR を探索する. 但し, BR1 が BUM(0) の処理をできない時は上述の処理は行わず, BUM(0) をそのまま CH に送る.

BR2 が BR1 からの BUM(1) を捕捉したとする. BUM(0) の場合と同様に, BUM(1) の宛先が BR2 自身であれば, HA より直接送られたメッセージなので BR2 の結合エントリを更新する. そうでなければ, PET エントリ内を検索し, 下位 BR 自身のアドレス (図 5では BR3) もしくはこれが対象とするネットワーク (図 5では CH) であれば, BUM(1) の BR IP アドレスフィールドを BR2 のアドレスに書き換え, これを転送する. 但し, 送信元, 及び, 送信先アドレスは捕捉時のままで変更はしない. PET エントリに該当するものがない場合は, 結合エントリを作成し, 同時に R ビットをオンにした PURM を CH に対して送信する. 最後に, エントリの有無に関わらず, BR1 に対して PAM を送信し, BR1 の PET エントリを更新する. 但し, BR2 が BUM(1) の処理をできない時は上述の処理は行わず, BR3 のエントリが PET にあれば受信した BUM(1) をそのまま中継する. エントリがない場合は, BUM(2) を BR1 へ送信し, BR1 に結合エントリを作成するよう依頼する.

BR2 からの BUM(2) を BR1 が受信した場合は, そのメッセージで示される MH の結合エントリを作成する. 但し, BR1 がこの処理を行えない場合は, BUM(2) を破棄する.

BR2 が R ビットがオンの PURM を BR1 から受信した場合は, BR2 は自分の担当するネットワークアドレスとサブネットマスクを PAM で応答する. R ビットがオフならば, 担当ネットワークに変更がない限り, PAM で有効時間のみを応答する.

BR1 が BR2 より PAM を受信した場合, BR1 は PET エントリに BR2 が存在するかどうかを確認する. もしあれば, その有効時間を更新し, かつ, PAM の長さフィールドが 0 でなければ, 同エントリの担当ネットワークアドレスとサブネットマスクを更新する. BR2 の PET エントリがない場合はこれを作成するが, PAM の長さフィールドが 0 のときは, PET エントリを作成せずにこれを破棄する. また, 上述の更新・作成の処理ができない場合は, BR2 の PET エントリを (もしあれば) 削除し, PAM も破棄する.

5. 認証方法

前節の MIP 経路最適化では, MH の現在の居場所を教えるために BUM(0) が HA から CH に対して送付される. これに応じて, BR は MH に対する結合エントリを更新し, 通信経路が変更する. しかし, この操作を無条件に行うと, 悪意をもつ者に偽の BUM(0) を送信された場合, CH から MH への通信が正しく送られなくなるという問題がある. この問題はサービス拒絶攻撃と呼ばれ, これを防ぐために BR は BUM(0) が HA から送られたことを認証する必要がある.

従来の MIP 経路最適化における認証方法は, HA と

Type	Length	Auth Type	SPI	Cert-cnt
Home Agent (HA) Digital Signature				
Sender-Certificate-Length		Sender-Certificate		
Sender-Certificate, continued...				
CA-Certificate-Length		CA-Certificate		
CA-Certificate, continued...				
additional <CA-Cert>s as necessary				

図11 BUM 認証拡張

CH が手動により互いの共通鍵を保持 (MSA の確立) することで実現されている．しかし，手動による鍵交換はスケーラビリティの面から現実性に欠けるため，現在 IETF では様々な認証方法が提案されている[3),4)]．これらの方式の中から，本提案方式では 4) に基づき，公開鍵を用いた認証方式を採用する．

まず，認証のため BUM 認証拡張を図 11のように定義し，HA はすべての BUM(0) にこれを付加する (図 6)．同様に，BUM(1) と BUM(2) にもこれを付加するが，この内容は BUM(0) に付加されたものをそのまま転送するものとする．図 11で，Type ビットがオフ (0) の場合は従来の共通鍵による認証を，オン (1) の場合は公開鍵による認証を行う．Length フィールドは Type ビットから HA Digital Signature フィールドまでのバイト数を表す．Auth Type と SPI は，認証に用いる公開鍵及び共通鍵暗号方式をそれぞれ表す．HA Digital Signature フィールドは BUM(0) の内容に HA が電子署名を行ったものである．この電子署名の対象は，BUM(0) 中のタイプ番号フィールドを除いた UDP ペイロード (図 6 の A フラグから BUM の識別子フィールドまで) と，BUM 認証拡張内部の Type 及び Length フィールドである．

公開鍵による認証には HA の公開鍵が必要となるが，この公開鍵の配布には，信頼できる第三者機関である認証局 (CA) により電子署名された電子証明書が用いられ，この長さと内容が HA-Certificate-Length と HA-Certificate に格納される．BR は認証局の公開鍵を予め取得していることが仮定されており，これにより，HA から配布される公開鍵の認証が行われる．なお，認証局が多数ある場合は各々が階層構造を取り，上位認証局が下位認証局の電子証明書 (CA-Certificate) を発行する．Cert-cnt フィールドは，これらの電子証明書の総数を格納する．

6. シミュレーションモデルと評価

これまで提案した経路最適化方式の性能を評価するため，本節では，シミュレーション実験により各 BR での平均処理時間と，各パケットが冗長経路を通る確率を求める．

6.1 シミュレーションモデル

実験に用いるネットワークモデルとして，BR 1 台で 2 つのサブネットの処理を行う集中方式 (図 12) と，一方のサブネットに下位 BR を置いた分散方式 (図 13) を用いた．また，従来方式との比較を行うため，図 12の BR1 を R に置き換えた場合についても測定を行った．

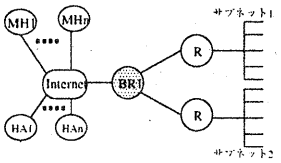

図12 集中方式のシミュレーションモデル

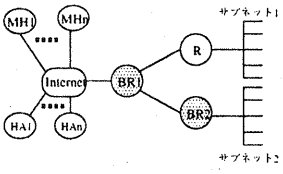

図13 分散方式のシミュレーションモデル

シミュレーション条件は以下の通りである．各リンクスピードはいずれも 100Mbps，LAN (BR1 と各サブネット間) の伝搬遅延は 2ms，WAN (BR1 と MH 及び HA 間) の伝搬遅延は 4ms とする．各サブネットからは同数の互いに異なる MH 宛にパケットを送信し，MH 一台当たり 384Kbps のトラヒックを送るものとする．同時に，同数の非移動ホスト宛にもパケットを送出し，MH 宛のものとあわせて合計 10Mbps のトラヒックをそれぞれ送出するものとする．

集中方式及び分散方式の BR1 のパケット処理時間は以下に示す各平均処理時間の指数分布に従う．すなわち，BUM 以外のパケットは 30μs，ただし，トンネリングを行う場合はその 2 倍の 60μs とする．また，BUM を処理する場合は共通鍵暗号による認証処理を行うとし，そのオーバーヘッドを 500μs とするが，分散方式のみ BUM(0) を BUM(1) に直す場合は平均 100μs のオーバーヘッドがかかるとする．分散方式の BR2 のパケット処理時間も BR1 と同様に各平均処理時間の指数分布に従うが，BR2 の処理時間は BR1 の場合の 2 倍を要するとする．但し，BUM(2) に直し BR1 へ返信する場合は平均 150μs のオーバーヘッドとする．

その他のルータ (図中の R) はすべてのパケットに関し平均 50μs の指数分布に従うこととする．また，BR1 で保持できる結合エントリ数は 20 エントリ，BR2 の結合エントリ数は BR1 の 1/2 倍の 10 エントリとする．最後に，各 MH は継続的に FA を変更するものとし，その移動間隔は平均 100s の指数分布に従う．

上記の条件のもと，各サブネットがパケットを送出する MH の数を変化させながら実験を行った．

6.2 評　価

各方式において MH 宛へ送信されたパケットが冗長経路を通る確率を図 14に示す．図より，集中方式は MH の総数が 20 台まで，分散方式では 30 台までならば冗長経路を通る確率はほぼ 0%，すなわち，約 100% 最適経路で送付することができる．しかし，それよりも台数が増える

と冗長経路を通る確率は急激に増加する．これは，MHの総数が各BRの結合エントリ数の総和を超えたため，結合エントリに登録されないMHが多数生じたことに起因する．

次に，各方式におけるBR (又はR)の平均パケット処理時間を図15に示す．MHの総数が各ルータの結合エントリ数の総和以内に収まっている場合，集中方式のBR1では，従来方式と比べて最大10μsのオーバーヘッドで済むことがわかる．また，分散方式のBR1は，オーバーヘッドが5μs以下に低下するが，BR2では集中方式のBR1よりも最大40μsのオーバーヘッドが生じてしまう．これはBR1の負荷がBR2に移ったことを示すが，BR2の処理能力はBR1の1/2倍であるために，このようなオーバーヘッドが生じている．さて，MHの総数が各ルータの結合エントリ数の総和を超えた場合，急激に各BRでの平均処理時間が上昇する．図14で示したように，結合エントリが不足する状況では冗長経路を通過する確率は非常に高い．MHが冗長経路からパケットを受け取ると，そのHAは最適経路を通過させるためBRに対してBUM(0)の発行するが，この発行数が急増したことによりBRでのBUMの処理に要する時間が非常に大きくなったことが原因である．

図16に，各方式において各サブネットからWAN側に送出されたパケットを各BR (又はR)が処理するために要した平均時間の合計を示す．MHの総数が各ルータの結合エントリ数の総和を超えた場合，急激に平均処理時間が増加するのは図15と同様である．そうでない場合，分散方式におけるサブネット2からの平均パケット処理時間は，集中方式のそれに比べ最大50μsも多いが，サブネット1の場合は最大5μsの減少となり，後者はBR2の処理時間の影響を受けていないことが分かる．

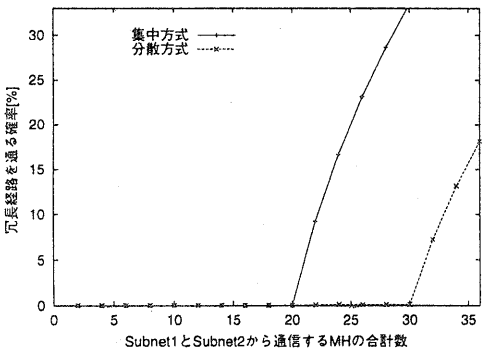

図14 集中方式，分散方式においてパケットが冗長経路を通る確率

以上の結果より，MHからのアクセスは十分少なく，常に結合エントリの総数以下である場合は，処理速度の速い上位のBRで一括処理する集中方式の方が有効であると言える．一方，MHからのアクセスが非常に多く，結合エントリ数を一台の上位BRで格納し切れない場合には，集中方式よりもより多くの結合エントリが持てる分散方式の方が有効である．

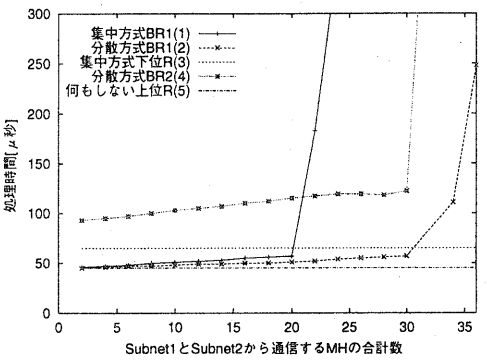

図15 各BRでの平均パケット処理時間

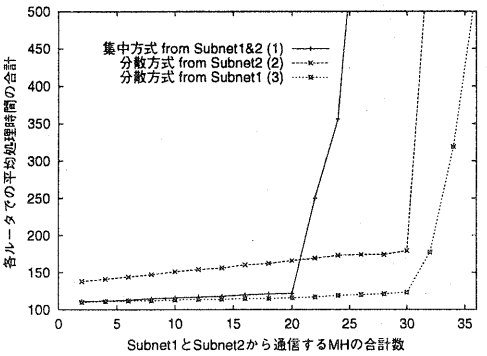

図16 サブネット1・2より送付したパケットの平均処理時間の合計

7. まとめと今後の課題

本稿ではドラフト2)に変更を加え，BRを変更するだけでCHを一切変更せずに実現する経路最適化法を提案した．更に，複数のBRで処理を行う負荷分散方式についてもあわせて示し，シミュレーション実験により，従来方式や集中方式の場合の平均処理時間を比較し，MHからのアクセスが多い場合には，分散方式の方が有効であることを示した．

しかし，MHが十分少ない時は分散方式は集中方式よりも処理時間がかかることから，これを改良する必要がある．また，公開鍵を用いたBUMの認証方法は非常に計算時間がかかることから効率の良い認証方法を導入することなどを今後の課題としたい．

参考文献

1) C.Perkins, "IP Mobility Support," RFC2002, 1996
2) D.Johnson and C.Perkins, "Route Optimization in Mobile IP." Internet Draft, 1997
3) http://www.ietf.org/ids.by.wg/mobileip.html
4) S. Jacobs, "Mobile IP Public Key Based Authentication," Internet Draft, 1999