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

2006－ＭＢＬ－37 (15)
2006／5／19

VPNによる複数経路統合方式の提案と実装

藤野 信次† 原 政博† 塩内 正利† 石原 進‡ 水野 忠則‡

†富士通研究所 〒211-8588 神奈川県川崎市中原区上小田中 4-1-1
‡静岡大学 〒432-8561 静岡県浜松市城北 3-5-1

E-mail: †{fujino, hara.masahiro, shiouchi.masato}@jp.fujitsu.com,
‡{ishihara@sys.eng, mizuno@inf}.shizuoka.ac.jp

あらまし 複数経路統合方式はモバイル環境で他の端末の通信リソースを使用して帯域拡大や通信の信頼性を向上する手段として有用である。特に Mobile IP による複数経路統合方式はアプリケーションに依存せず、エンドサーバに修正が不要で実用的である。しかし、企業等のファイヤ・ウォールのある環境では Mobile IP プロトコルを通す必要があり、セキュリティ上設置が困難であった。そこで本論文ではこのような環境でも適用し易い VPN を利用した複数経路統合方式を提案している。更に本提案の実用性を検証するために行った試作について述べる。評価実験により、VPN によるセキュリティを確保しつつ複数経路統合が可能なことを確認した。

キーワード VPN, 複数経路統合, 実装

Proposal and Implementation of Multiple Paths Aggregation Using VPN

Nobutsugu FUJINO† Masahiro HARA† Masatoshi SHIOUCHI† Susumu ISHIHARA‡
and Tadanori MIZUNO‡

†Fujitsu Laboratories Ltd. 4-1-1 Kamikodanaka, Nakahara-ku, Kawasaki, 211-8588 Japan
‡Shizuoka University 3-5-1 Johoku, Hamamatsu-shi, Shizuoka, 432-8561 Japan

E-mail: †{fujino, hara.masahiro, shiouchi.masato}@jp.fujitsu.com,
‡{ishihara@sys.eng, mizuno@inf}.shizuoka.ac.jp

Abstract Multiple paths aggregation is useful in the mobile environment, which allows bandwidth or reliability of communication to be increased. Especially, multiple paths aggregation using Mobile IP is efficient because it is not dependent on applications nor needs any modifications. However, it is difficult to apply it in the intranet with firewall because of security problem on Mobile IP protocol not to pass through over the firewall. Therefore, we propose multiple paths aggregation using VPN, which can apply such an environment. We also show the implementation of the developed prototype system and evaluation.

Keyword VPN, Multiple paths aggregation, Implementation

1. はじめに

近年、移動通信網の急激な発展とともに、モバイル端末からインターネットにアクセスするモバイルインターネット環境が整いつつある。特に無線 LAN の普及により広帯域でのモバイルインターネットアクセスが可能になってきた。最近では 3G 携帯と無線 LAN の両方が使える端末も登場している。無線 LAN を使用すれば、アクセヒポイント経由でインターネットにアクセスするだけでなく、近くにいる端末同士でアドホックにネットワークを形成することが可能である。これを利用して他の端末のリモートアクセス経路と自己のアクセス経路を同時に使用する複数経路統合[1][2]が注目されている。複数経路統合はリモートアクセス帯域の拡大、信頼性の向上が可能で、モバイル環境では有用である。

複数経路統合は SHAKE[2]として研究されている。その実現方式は様々なものが提案されている。Web proxy を利用しアプリケーションレベルで実現する Web SHAKE[3]、Mobile IP[4]を利用し IP レベルで実現する Mobile IP SHAKE[5]などがある。特に Mobile IP SHAKE は IP レベルで実現するため、アプリケーションに依存しないという利点がある。また Mobile IPv4 を利用する場合はエンドサーバに修正を加える必要がなく実用的である。しかし、ファイヤ・ウォールに Mobile IP プロトコルを通すのはセキュリティ上問題があるため、Mobile IP の Home Agent を企業等のファイヤ・ウォール内に設置するのは困難であった。

一方、Mobile IP を使用する異種網シームレスローミ

ングでも同様の問題があった。これに対し、我々はMobile IPの代わりにVPNを使用してセキュリティを確保しつつローミングを行う手法を提案している[6]。今回、同様の手法を複数経路統合に適用し、企業等のファイヤ・ウォールのある環境でも適用しやすい、VPNによる複数経路統合方式を提案する。また、その実用性を検証するための試作を行ったので報告する。

本論文では第2章でMobile IPによる複数経路統合の概略と企業等に適用する場合の問題を示す。第3章で提案方式について述べ、第4章で試作システムとその評価を示す。最後に第5章でまとめる。

2. Mobile IPによる複数経路統合方式

2.1. 複数経路統合

図1に複数経路統合の概念を示す。複数のモバイル端末(MN)が各々インターネットに接続するためのネットワークと、端末同士のアドホックな接続を行うためのネットワークを持ち、同時に2つのネットワーク接続ができるものとする。ここでアドホック接続の通信帯域はインターネット接続の通信帯域に対して充分高速とする。この時ある端末が一つのサーバ(CN)と通信する場合、ある端末は自己のインターネット接続ネットワークを経由してサーバに接続する経路の他に、アドホック接続ネットワークを経由し、更に他の端末のインターネット接続ネットワークを経由してサーバに接続する経路も存在する。これらの経路を同時に使用することで、端末は自己のインターネット接続の帯域を仮想的に増大することが可能となる。また、複数の経路を同時に利用することでネットワーク接続性を高め、信頼性を向上させることができる。

このような複数経路統合を行うためにはネットワーク側と端末側にトラフィックを分配・集約する仕組みが必要になる。分配・集約機構としてMobile IPのHome Agent(HA)を利用するものにMobile IP SHAKEがある。

2.2. Mobile IP SHAKEの概要

Mobile IP SHAKEはIPレベルでトラフィックの分配・集約を行うため、アプリケーションに依存しないという利点を持つ。特にMobile IPv4 SHAKEではCNとは独立のHAでデータの分配・集約を行うため、CNに影響を与えないという特徴がある。図2にMobile IPv4 SHAKEの概要を示す。

他の端末のネットワークリソースを使用する端末（アライアンス・リーダーAL）はネットワークリソースを提供する端末（アライアンス・メンバーAM）を発見するとアドホックなネットワーク（クラスタ）を構成し、HAにAMの気付アドレス（CoA）を登録する。HAはAMのCoAの登録が完了するとALに対して登録応答メッセージを返す。これらのメッセージはMobile IPの登録メッセージを拡張して実現している。

HAではMobile IPのトンネリングプロトコルによってAL、AMへのデータ配送を行う。すなわちALに対しては送信元：CN、宛先：ALのHoAのパケットを送信元：HA、宛先：ALのCoAのパケットでカプセル化して送る。AMに対しては送信元：CN、宛先：ALのHoAのパケットを送信元：HA、宛先：AMのCoAのパケットでカプセル化して送る。

2.3. 企業適用時の課題

他の端末の通信リソースを有効活用する複数経路統合は外出先から企業内のサーバにアクセスする場合にも有効である。しかし、通常、企業等のイントラネットとインターネットの間にはファイヤ・ウォールが存在するため、セキュリティ上の問題が発生する。Mobile IPを使用する方式ではHAを企業内に置く必要がある。この時、以下のような課題がある。

(1) Mobile IPの登録メッセージのファイヤ・ウォールを越え：Mobile IPの登録要求メッセージは社外から社内に送られるため、ファイヤ・ウォールを通過できない。通過させるためにはファイヤ・ウォールに穴を空ける必要があるが、登録メッセージが使用するUDPポート434番はセキュリティ・ポリシーによっては許可されない場合がある。

(2) Mobile IPの通信トラフィックのファイヤ・ウォール越え：Mobile IP自体がIPトンネリングであるため、セキュリティ・ポリシーにより通常、ファイヤ・ウォールを通過できない。Mobile IPの登録時に認証プロセスが実行されるが、その後はMobile IPでカプセル化された全てのプロトコルを通す事になり、ファイヤ・ウォールを設けている意味がほとんど無くなってしまう。

(1)はセキュリティ・ポリシーによっては許可される場合もあるが、(2)は深刻である。(2)の対策として通信内容を暗号化する方法が考えられるが、Mobile IPのヘッダは平文であるので何時、何処から何処への通信かは観測可能でセキュリティ上、問題が残る。また、Mobile IPをIPsecでカプセル化する方法も考えられるが、その場合は二重にカプセル化することになり、伝送効率が悪化する。そもそも、それが可能なら次章の提案方式が適用できる。

3. 提案方式

VPNを利用した経路統合方式を提案する。一般に社外のインターネット上の端末（MN）から社内のイントラネット上のサーバ（CN）に安全にアクセスする手段としてVPNが使用される。VPNではインターネットとイントラネットの間（DMZ）に設置されたVPNサーバによりイントラネットで使用されるプライベートアドレスによるIPパケットをカプセル化し、ペイロードを暗号化して端末との通信を行う。従ってインターネット上の端末からの全てのパケットはVPNサーバを経由する。そこで提案方式ではこの特徴を利用して、VPNサーバをトラフィックの分配・集約機構として利用する。これにより、通信の安全性を確保しつつ複数経路統合を可能となる。

本方式はMobile IPによる方式と同様、IPレベルで実現するので全てのアプリケーションに適用できる。また独立したVPNサーバを利用するので既存のコンテンツサーバに影響を与えない。

3.1. プロトコル概要

図3に提案方式のプロトコル概要を示す。ALとなるモバイル端末MN1は予めVPNサーバを経由してイントラネットに接続されているものとする。MN1はAMとなる端末MN2を発見すると、MN2に中継機能の使用を要求する（中継要求①）。MN2がそれを許可する応答を返す（中継許可応答②）と、MN1はVPNサーバにMN2を中継ノードとして追加することを依頼する（中継ノード追加依頼③）。一方、MN2はVPNサーバに接続する（VPN接続④）。

この時VPNサーバは通常のVPNと同様にMN2にイントラネット内のプライベートアドレスを仮想VPNアドレスとして付与する。ALがネットワーク上を移動した場合にも[6]で提案したように移動前と同一の仮想VPNアドレスを付与することにより、移動透過性も確保できる。

3.2. VPNサーバによるトラフィック分配

VPNサーバは各MNの帯域や遅延量に応じてトラフィックを分配して各MNに配送する。帯域や遅延に関係なく配分する方法もある。具体的なトラフィックの分配手法については[8]で詳しく述べられているのでここでは言及しない。

AL(MN1)に対しては送信元：CN、宛先：ALの仮想VPNアドレスのパケットを、送信元：VPNサーバ、宛先：ALのCoAのパケットでカプセル化して送る。AM(MN2)に対しては送信元：CN、宛先：ALの仮想VPNアドレスのパケットを、送信元：VPNサーバ、宛先：AMのCoAのパケットでカプセル化して送る。パケットを受信したAM(MN2)はデカプセル化したパケットの宛先がAL(MN1)であるため、パケットをALに転送する。図4にVPNサーバによるデータ配送を示す。

3.3. イントラネット方向へのトラフィック分配

次に端末からイントラネットに対するトラフィック分配について述べる。前節同様、MN1がALの場合について記す。AL(MN1)は帯域、遅延量に応じて送信元：AL、宛先：CNのパケットを自己のリモートインタフェースとローカルの他の端末（AM）のインタフェースに向けてルーティングする。AMではローカルのインタフェースから流入したパケットの宛先がCNであるため、自己のリモートインタフェースに向けてルーティングすることにより、CNに転送される。

4. 試作

提案方式の実用性を検証するために試作を行った。以下、システムの設計と実装、評価を示す。

4.1. システム設計

図5に試作システムの構成を示す。システムは主に分配、集約、中継モジュールからなり、各々ネットワーク側のVPNサーバ、ALとなるモバイル端末、AMとなるモバイル端末上に実装される機能モジュールである。これらを管理・制御するサービス・コーディネータ(SC)を各ノードに配備する。SCはアライアンスの構築・制御も行う。このように極力、独立した機能モジュールで構成する設計とした。

各機能モジュールはUPnP[9]サービスとして実現し、モジュール間の通信にはUPnPプロトコルを使用する[10]。各SCはシナリオに従って連携動作する。これについては別途報告することとし、ここでは詳細な記述を割愛する。

図6に各モジュール間の動作シーケンス例を示す。図は動作中に中継ノード（AM）を追加する場合のシーケンスである。

4.2. 実装

本試作では、モバイル端末としてネットツーコム社製WiPCom1000[10]を使用し、集約、中継モジュールはWindows CE上で独自に開発したルータを使用して実現した。VPNサーバにはLinuxで動作するPPTPサーバ[12]を使用し、VPNによるシームレスローミング[7]の実装を参考に独自修正を加えた。トラフィック分配は単純なラウンド・ロビンとした。表1に試作・評価環境を示す。

4.3. 評価

基本的な機能・性能を検証するために評価実験を行った。図 7 に実験系を示す。1 経路の場合と 2 経路の場合のスループットを実環境で測定した。Web サーバに 1 つの 1MB のコンテンツを用意し、端末上の Web プラウザでの取得時間を測定してスループットを求めた。

図 8 に測定結果を示す。1 経路時のスループット 25.7kbps に対し、2 経路時のスループットは 47.2kbps であった。スループットは 10 回実測した結果の平均値である。2 経路時のスループットは 1 経路時のものより約 1.8 倍と増加しており、経路統合が動作していることが分かる。

中継機能による遅延のため、経路間の遅延差が発生し、性能に悪影響を及ぼすと予想したが、その影響は小さいことが分かった。

表 1 試作・評価環境

	サーバ	クライアント
使用機器	FMV-Biblo NE8/1000H	WiPCom1000
OS	Linux(Fedora core2)	Windows CE 4.2
VPN	Poptop Ver 1.3.0	WindowsCE 標準
リモート通信	—	PHS 32kbps 回線交換
ローカル通信	—	IEEE 802.11b

5. まとめ

セキュリティを確保しつつ帯域拡大や信頼性の向上が可能な VPN による複数経路統合方式を提案した。提案方式は IP レイヤで分配・集約を行っており、独立した VPN サーバを使用するため、アプリケーションに無依存で既存のサーバに影響を与えない。本方式は VPN による通信の安全性を確保しており、企業等のファイヤ・ウォールのある環境にも適用し易いという特徴を持つ。

本方式の実用性を検証するためにシステムを試作し、基本的な動作を確認した。実環境での性能評価を行い、帯域拡大効果を確認した。2 経路時の伝送速度は 1 経路時の約 1.8 倍であった。

今後、VPN による経路統合方式のより詳細な機能、性能評価を行う予定である。今回は PPTP[13]による実装を行ったが、今後は IPsec[14]による本格的な実装を行い、実用性の検証を行いたい。また、UPnP によるアライアンス構築の自動化を進め、その実用性も検証したい。

文　献

[1] 林孝典, 山崎真一郎, 森田直人, 相田仁, 武市正人, 土居範久, “インターネットを用いた複数経路データ伝送方式の性能評価,” 信学論(B), Vol.J84-B, No.3, pp.523-533(2001)

[2] H.Mineno, S.Ishihara, K.Ohta, M.Aono, T.Ideguchi and T.Mizuno, "Multiple paths protocol for a cluster type network," International Journal of Communication System, vol.12, pp.391-403, 1999.

[3] Y.Konishi, S.Ishihara and T.Mizuno, "Web SHAKE: A fast WWW access method for mobile terminals on temporary cluster networks," Proceedings of 2002 IEEE International Conference on Communications, 2004.

[4] C. Perkins, "IP Mobility Support," RFC 2002, October 1996.

[5] 伊藤陽介, 小山健二, 太田賢, 石原進, "Mobile IP を用いた通信回線共有方式の実装", マルチメディア・分散・協調とモバイル(DICOMO2003),No.9, pp.97-100,2003.

[6] 武仲正彦, 藤本 真吾,"IPsec/IKE によるセキュアな P2P シームレスローミング方式," SICS2004 2C2-1, 2004 年 1 月

[7] 武仲正彦, 藤本真吾, 藤野信次, “IPsec/IKE によるセキュアなシームレスローミング方式の試作,” ISEC 2004-46, 2004 年 7 月

[8] 小山健二, 伊藤陽介, 石原進, 倉掛正治, 水野忠則, "Mobile IP SHAKE におけるトラフィック分配機構の検討", 情報処理学会第 65 回全国大会(3), p.473-474, 2003.

[9] UPnP, . http://www.upnp.org/

[10] 藤野信次, 福田茂紀, 石原進, 水野忠則, “モバイル・ユビキタス統合アーキテクチャの提案,” 情報処理学会研究報告, 2006-MBL-36, pp.403-408, Feb. 2006.

[11] 藤野信次, 原政博, 福田茂紀, 森信一郎, 城ヶ崎寛, ”ユビキタス環境に適した無線 IP 携帯端末の設計と実装,” 情報処理学会研究報告 2005-UBI-9, pp.69-72, Nov. 2005

[12] PPTP Server, http://www.poptop.org/

[13] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, G. Zorn, "Pont-to-Point Tunneling Protocol(PPTP)," RFC 2637, July 1999.

[14] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406, November 1998

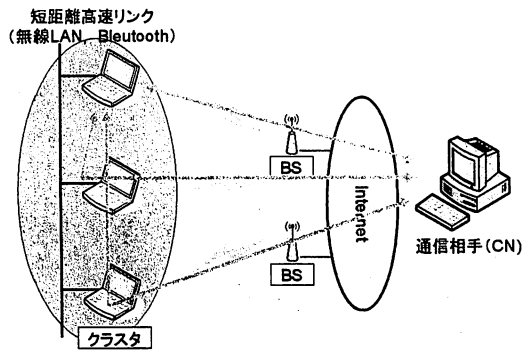

図 1　複数経路統合

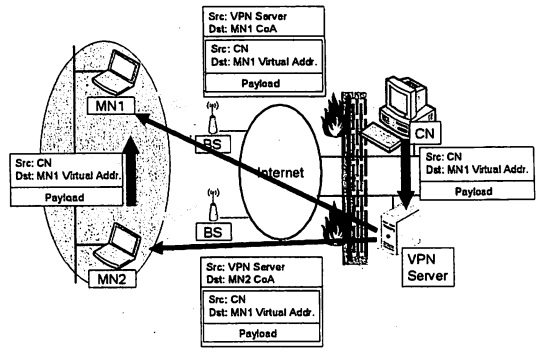

図 4 提案方式のデータ配送

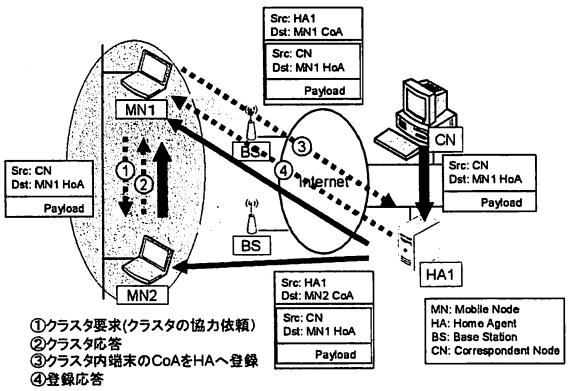

図 2　Mobile IP SHAKE の概要

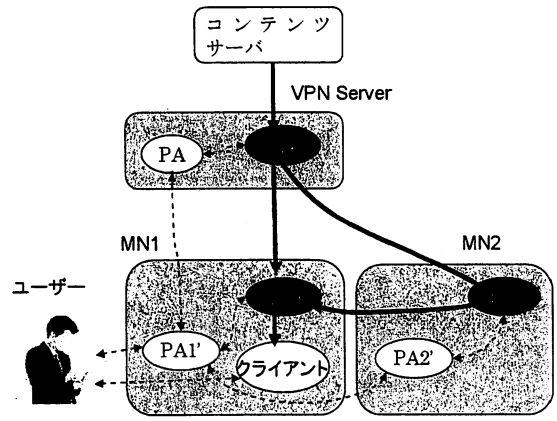

図 5 試作システムの構成

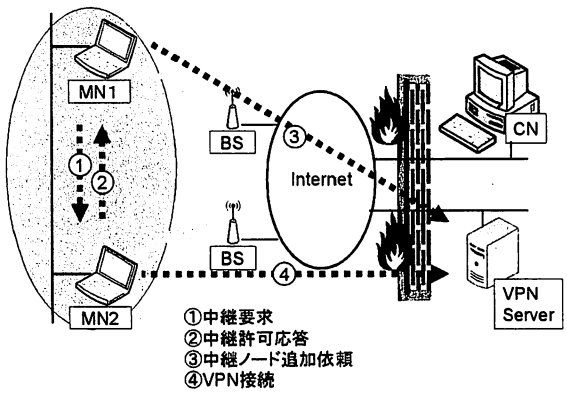

図 3 提案方式のプロトコル概要

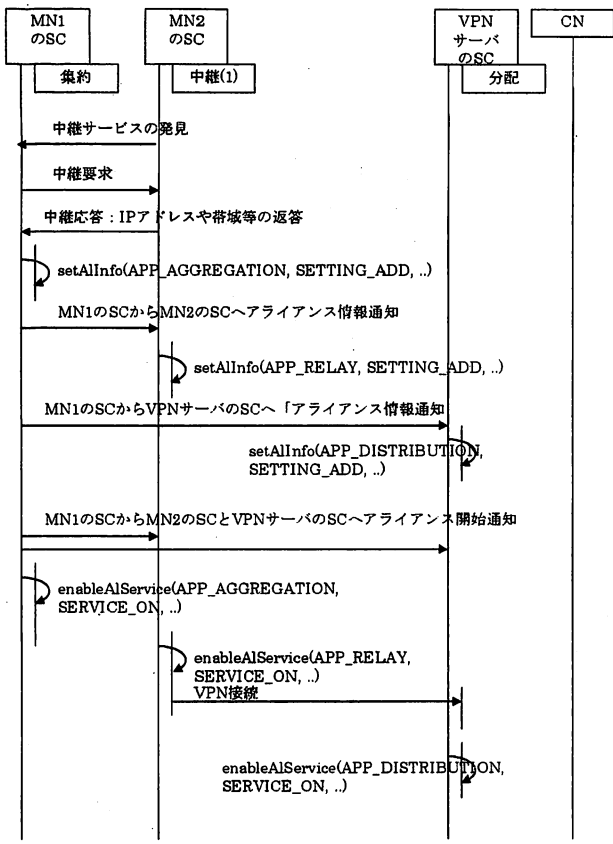

図 6 試作システムの動作シーケンス例

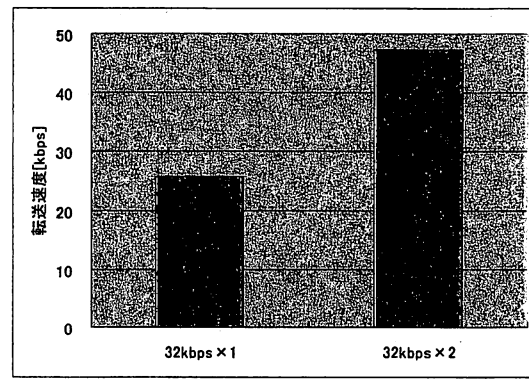

図 8 測定結果

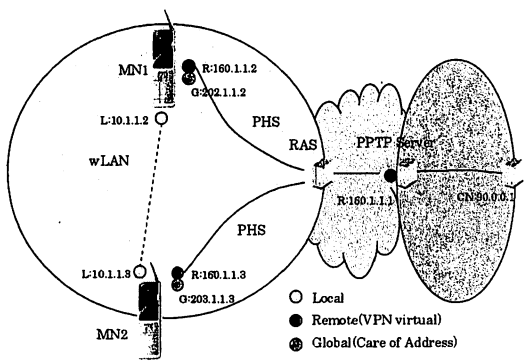

図 7 評価実験系