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

2008－MBL－47 (4)
2008－ITS－35 (4)
2008／11／6

プロキシ型 MOBIKE を用いたハンドオフ方式の提案と評価

千葉 恒彦　　横田 英俊
株式会社 KDDI 研究所

近年無線アクセスネットワークを構成する要素として，フェムトセルやピコセルなどの携帯電話の小型基地局が注目されている．通信エリア拡充のためオフィス内にフェムトセルを複数配置した場合，ユーザが移動しながらデータ通信を継続するためには，フェムトセル間のハンドオフ技術が要求される．また，とりわけ VoIP などのリアルタイムアプリケーションでは，フェムトセル間の高速なハンドオフ技術も要求される．本稿では，複数のプロトコル実装にともなうフェムトセルの負荷増大を軽減し，かつフェムトセル間ハンドオフを実現するプロキシ MOBIKE 方式について提案する．

Proposal and evaluation of a handoff mechanism based on Proxy MOBIKE

Tsunehiko Chiba　　Hidetoshi Yokota
KDDI R&D Laboratories, Inc.

Recently, small base station such as femtocell and picocell becomes popular as one of the components in wireless access network. If multiple femtocells are deployed in an office building for expanding the communication area, a handoff mechanism between femtocells is required to support the continuity of data communication. Additionally, real-time applications such as VoIP need a seamless handoff mechanism. In this paper, we propose Proxy MOBIKE mechanism, which realizes efficient handoff between femtocells and mitigates the difficulty of the femtocell implementation due to supporting multiple protocols.

1. はじめに

移動体通信におけるオール IP ネットワークは，3GPP (3rd Generation Partnership Project) 及び 3GPP2 (3rd Generation Partnership Project 2)において IMS (IP Multimedia Subsystem)[1] 及び MMD (Multimedia Domain)[2]が規定され，SIP (Session Initiation Protocol)[3]を用いたマルチメディアアプリケーションの制御基盤が整いつつある．一方，移動体ネットワークの IP 化が進むにつれ，携帯電話の小型基地局であるフェムトセルにて IP レイヤを終端させ，コアネットワークをより簡素化したアーキテクチャが注目されている[4]．フェムトセルは，一般的に高層ビルや地下など広域基地局からの電波が十分に到達しないエリアに配置し，通信エリアを拡充するために用いられる．また，フェムトセルを用いるメリットとして通信エリアの拡充以外にも，小数ユーザで占有的に無線帯域を利用することによる通信容量の増加，一般のブロードバンド回線を介してフェムトセルを移動体通信事業者のコアネットワークと直接通信させることによる，広域の無線ネットワークの負荷軽減などがあげられる[5]．これら背景のもと，標準化団体では汎用の無線 LAN を利用して移動体コアネットワークへ接続する形態は規定されているものの[6]，フェムトセルを利用した移動体コアネットワークへの接続形態は十分な検討がされていない．例えば，基地局を小型化し，その送信電力を小さくすると 1 基地局あたりの収容エリアも狭くなるため，オフィス等の比較的広いエリアに設置して隈なく通信を可能にするにはフェムトセルを複数台設置する必要がある．このような環境下でユーザが移動

しながら通信を行う場合，アプリケーションのデータ通信継続のためにはフェムトセル間のハンドオフを実現する必要がある．とりわけ，音声やテレビ電話などのリアルタイムアプリケーションでは，通信断時間を極力短くした高速ハンドオフ技術も要求される．

本稿では，まずフェムトセル間のハンドオフを実現する関連技術として，汎用の無線LAN のネットワーク間ハンドオフに用いられる MOBIKE (IKEv2 Mobility and Multihoming)[7]，及びネットワーク側でハンドオフを制御するプロキシ・モバイル IP[8][9]について説明する．次に，フェムトセルの実装プロトコル数をより低減したプロキシ MOBIKE を提案し，その評価結果を示す．さらに，プロキシ MOBIKE のハンドオフ高速化について考察する．

2. 関連技術

図 1 に，3GPP2 にて規定されている，無線LAN を経由した移動体コアネットワークへの接続形態を示す[6]．ここで，移動体コアネットワークはセキュアであるが，無線区間，ブロードバンドアクセス回線及びインターネットは非セキュアとする．端末は，これら非セキュアのネットワークを介した通信を暗号化するため，移動体コアネットワークに配置されるセキュリティゲートウェイの PDIF (Packet Data Interworking Function) と IKEv2 (Internet Key Exchange version 2)[10]による IPSec を確立する．また，ネットワーク間ハンドオフの実現には MOBIKE を用いる．MOBIKE では，端末がハンドオフ後に変更された TOA (Tunnel Outer Address)を PDIF へ通知することにより，IPSec のセッションを継続させる．

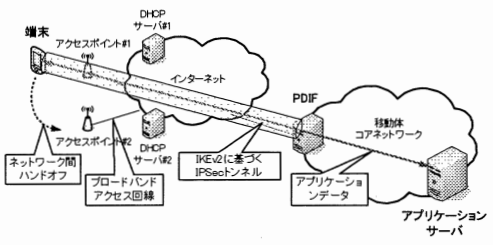

図 1　無線 LAN を利用した移動体ネットワークへの接続

図 2 に無線 LAN を利用した接続形態の処理手順を示す．端末は，アクセスポイント#1 との無線リンク確立に引き続き，DHCP サーバ#1 より IP アドレス（IP#1）を取得する．その後，端末は PDIF との間で IKEv2 手順に基づき IPSec トンネルを確立する．この IKEv2 手順の中で，PDIF は認証サーバと連携してユーザの認証処理を行うとともに，端末に TIA (Tunnel Inner Address)である IP#A を割り当てる．尚，端末と PDIF は，MOBIKE 対応可否の交渉も IKEv2 手順の中で行う．その後，端末は IP#A を用いてアプリケーションデータの送受信を行う．端末がアクセスポイント#2 へ移動した場合，アクセスポイント#1 との無線リンク確立後，DHCP サーバ#2 より IP アドレス（IP#2）を取得する．端末はハンドオフ前後で DHCP サーバより取得した IP アドレスが異なるため，IKEv2 情報通知を用いて MOBIKE に基づく IPSec トンネルの終端変更（IP#1=>IP#2）を PDIF へ通知する．ただし，アプリケーションに用いる IP アドレス（IP#A）は変更されないため，通信は継続される．

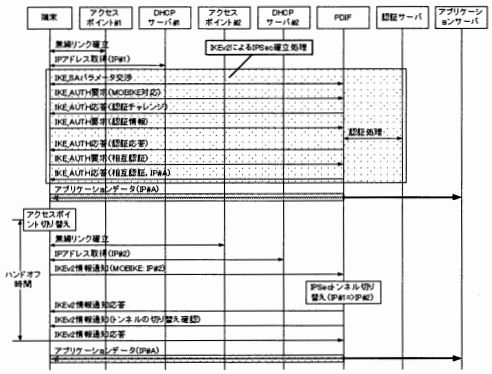

図 2　MOBIKE を用いたハンドオフ手順

一方，携帯電話の小型基地局であるフェムトセルを利用した接続の場合，既存端末は IKEv2 や MOBIKE などのプロトコルをサポートしていない．よって，CDMA (Code Division Multiple Access)方式などにより物理層のセキュリティが十分確保されているとみなされる場合には，端末ではなくフェムトセルで IPSec トンネルを終端する方が望ましい．これにより，無線区間の IP パケットのオ

ーバーヘッド増大を回避することができるとともに，端末における IKEv2 や MOBIKE プロトコルの実装及び処理負荷を軽減できるという利点も得られる．

図 3 に，cdma2000 HRPD (High Rate Packet Data)のフェムトセルを利用した移動体ネットワークへの接続形態を示す[11]．図 3 の構成において，フェムトセルである FAP (Femto Access Point)間のハンドオフを実現するための手法として，ハンドオフ前後で同一の IP アドレスを割り当てるプロキシ・モバイル IP が考えられる．プロキシ・モバイル IP では，モバイル IP [12][13]の登録要求を MAG (Mobile Access Gateway)が端末の代わりに LMA (Local Mobility Anchor)へ送信することにより端末の移動管理を行う．ここでは，FAP が MAG として動作することにより，ハンドオフ前後で同一の IP アドレスを端末へ割り当てる．

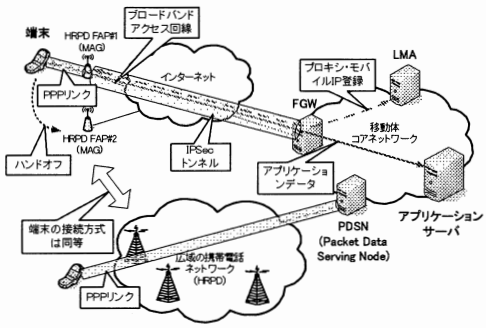

図 3　フェムトセルを利用した移動体ネットワークへの接続

図 4 にプロキシ・モバイル IP によるハンドオフ処理手順を示す．ここで，FAP とセキュリティゲートウェイの FGW (Femto Gateway)間は，IPSec などによりセキュアな通信が可能であるとする．端末は，FAP#1 との無線リンク確立に続き，PPP (Point-to-Point Protocol)[14]リンクの設定を行う．PPP リンクは，LCP (Link Control Protocol)による下位リンクの設定，CHAP (Challenge Handshake Authentication Protocol)などに基づくユーザ認証，NCP (Network Control Protocol)によるネットワークアドレスやヘッダ圧縮の設定の順に交渉が行われた後確立される．代表的な NCP として，IPCP (IP Control Protocol)や IPv6CP (IPv6 Control Protocol)が定義されており，それぞれ IPv4 用の制御と IPv6 用の制御に用いられる．FAP#1 は PPP リンクの認証手順において，端末から受信した認証情報（ユーザ識別子やパスワードなど）を用いて認証サーバと RADIUS (Remote Authentication Dial In User Service)[15]などによる認証処理を行う．FAP#1 は，認証サーバとの認証処理が完了すると，端末へ認証完了応答を返信する．続いて FAP#1 は，端末から IPCP 設定要求を受信すると MAG として端末の位置登録を実行するため，プロキシ・モバイル IP 登録要求を LMA へ送信する．LMA は端末へ割り当てる IP アドレス (IP#A) をプロキシ・モバイル IP 登録応答に含めて返信する．端末は，FAP#1 から送信された IPCP 設定応答に含まれる IP#1 を用いて，アプリケーションデータの送受信を行う．端末が FAP#2 へ移動した場合，FAP#2 が MAG としてプロキシ・モバイル IP 登録要求を LMA へ送信することにより，同一の IP アドレス（IP#A）を端末へ割り当てることができるため，アプリケーションの通信は継続される．

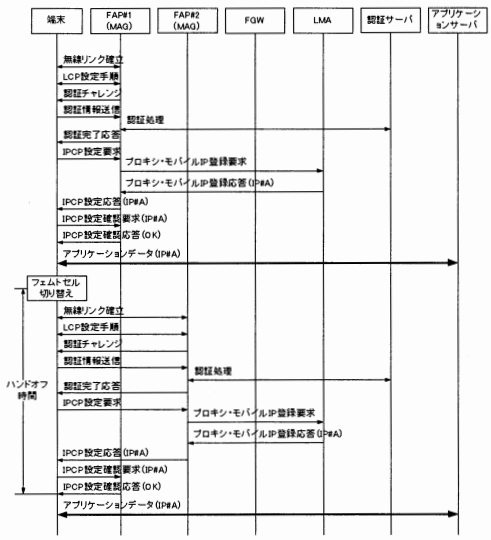

図 4　プロキシ・モバイル IP を用いたハンドオフ手順

しかしながら，プロキシ・モバイル IP を用いた場合，FAP は IKEv2，プロキシ・モバイル IP 及び RADIUS などの認証プロトコルを

実装する必要があり，FAP 上のプロトコル数増大による処理負荷や LMA 配置による設備数増加といった問題が残る．また，厳密なセキュリティ管理のためには，端末毎に IPSec トンネルを確立できる仕組みが要求される．そこで，これらの問題を解決するため，FAP が端末毎に IPSec トンネルを確立し，FGW が IKEv2 手順の中で移動管理を行うプロキシ MOBIKE 方式を提案する．プロキシ MOBIKE の詳細手順を次章に示す．

3. プロキシ MOBIKE の提案と概要

図 5 に，プロキシ MOBIKE による FAP の接続形態を示す．プロキシ MOBIKE では，端末と FAP 間の PPP 手順，及び FAP と FGW 間の IKEv2 手順を連携することにより，ハンドオフ前後で同一の IP アドレスを端末へ割り当てる．よって，本方式では，プロキシ・モバイル IP で用いた LMA は不要となる．

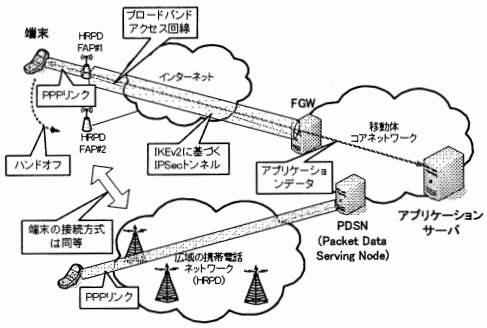

図 5　プロキシ MOBIKE の接続構成

図 6 にプロキシ MOBIKE によるハンドオフ手順を示す．FAP#1 は LCP 設定手順の実行後，IKEv2 手順に基づいて FGW と IKE_SA の算出を行う．その後，FAP#1 は，認証処理に用いるユーザ識別子を取得するため，認証チャレンジを端末へ送出する．FAP#1 は認証情報を端末から取得し，ユーザ識別子を IKEv2 の認証要求に含めて送信する．FGW は当該ユーザ名用の認証チャレンジを生成し，そのチャレンジ値を含めた IKEv2 の認証応答を FAP#1 へ返信する．FAP#1 は FGW から取得した認証チャレンジを再度端末へ送信する．FAP#1 は，端末から受信した認証情報を IKEv2 の認証要求に設定して FGW へ送信する．FGW は，受信した認証情報をもとにユーザの認証処理を行い，認証応答を FAP#1 へ返信する．FAP#1 は認証応答を端末へ返信後，端末からの IPCP 設定要求受信を契機に，FGW に対して端末に割り当てる IP アドレス（IP#A）を要求する．FAP#1 は，FGW から取得した IP#1 を IPCP 設定応答に含めて返信する．端末は指定された IP#A を用いてアプリケーションデータの送受信を行う．端末が FAP#2 へ移動した場合，FGW は IKEv2 の認証手順の中でハンドオフ前と同一の IP アドレス（IP#A）を割り当てるため，アプリケーションの通信は継続される．

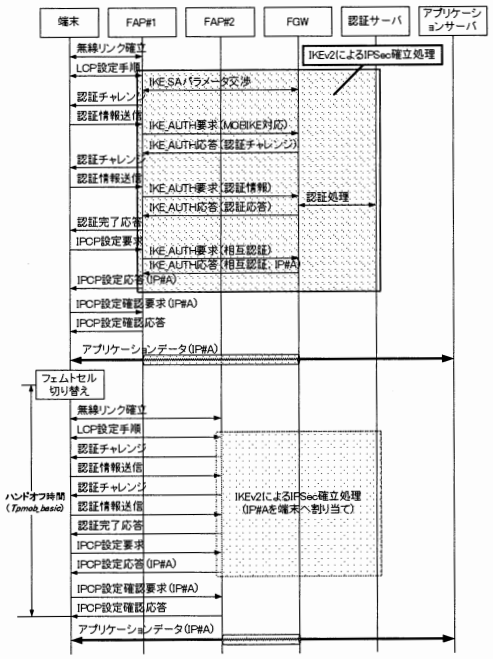

図 6　プロキシ MOBIKE を用いたハンドオフ手順

ここで，無線リンクの確立時間を T_w，端末と FAP 間のメッセージ転送時間を T_1，FAP と FGW 間のメッセージ転送時間を T_2，FGW と認証サーバ間のメッセージ転送時間を T_3 とすると，プロキシ MOBIKE を用いた場合のハンドオフ時間 T_{pmob_basic} は次の式で表される．

$$T_{pmob\_basic} = T_w + 11T_1 + 8T_2 + 2T_3 \quad (1)$$

式(1)のように，T_1が影響するメッセージ数は，LCP の設定交渉が 2 メッセージ，PPP の CHAP 認証処理で 5 メッセージ，IPCP の設定交渉で 4 メッセージの計 11 メッセージとなる．T_2が影響するメッセージ数については，IKEv2 による IPSec 確立処理の 8 メッセージ，T_3に関しては認証処理の 2 メッセージとなる．

4. 提案方式に関する評価実験

4.1. 実験ネットワークの構成と実装機能

図 7 に示した実験ネットワークを構築し，プロキシ MOBIKE のハンドオフ実証実験を行った．実験システムでは FAP を模擬するため，Linux ベースの PC に無線 LAN アクセスポイントを接続したものを仮想 FAP として動作させ，アプリケーションサーバからストリーミングデータを端末へ配信した．また，端末と FAP 間には，PPPoE (Point-to-Point Protocol Over Ethernet)を用いることで，cdma2000 HRPD システムをエミュレーションした．FAP と FGW の IKEv2 プロトコルには，Strongswan[16]をベースに PPPoE との連携及びハンドオフ後の同一 IP アドレス割り当て機能を実装した．尚，ユーザ認証は，外部認証サーバは用いずに FGW に実装した．表 1 に各装置の諸元を示す．

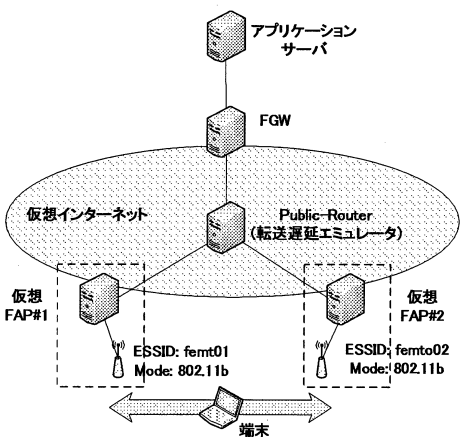

図 7　プロキシ MOBIKE の実験構成

表 1　各装置の諸元

装置 / スペック	端末，ルータ	FAP，FGW，アプリケーションサーバ	アクセスポイント
OS	Fedora Core 4	Fedora Core 6	Corega WLAPGMN
CPU	Pentium M 1.6 GHz	Pentium IV 2.8 GHz	
メモリ	512 MB	512 MB	
ネットワークアダプタ	MELCO WLI-PCM-L11 (Mode: 802.11b)	Intel PRO/1000MT	

4.2. ハンドオフ実験

4.1 節で示した実験ネットワークを用いてプロキシ MOBIKE のプロトコルを実証するとともに，仮想インターネットのパケット転送遅延時間を変動させ，そのハンドオフ時間の測定を行った．転送遅延エミュレータは Public-Router 上に実装し，FAP と FWG 間の送受信パケットの双方向に遅延を加えた．仮想 FAP であるアクセスポイントの切り替えについては，Linux の *iwconfig* コマンドによる手動切り替えとし，PPPoE の開始メッセージである端末からの PADI (PPPoE Active Discovery Initiation)送出時間から IPCP 設定確認応答メッセージ受信時間までをハンドオフ時間とした．測定については，片方向遅延を 0 ミリ秒，50 ミリ秒，100 ミリ秒，200 ミリ秒，500 ミリ秒に設定し，それぞれ 5 回実施した．実測結果の平均値を図 8 に示す．

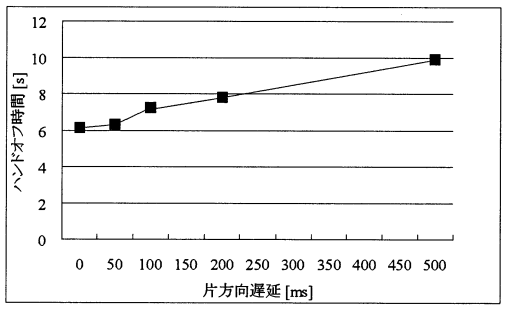

図 8　プロキシ MOBIKE のハンドオフ時間

図 8 に示したとおり，Public-Router 上の片方向遅延が 0 ミリ秒の場合には，ハンドオフ時間が約 6.1 秒 であり，100 ミリ秒の場合には約 7.2 秒，500 ミリ秒の場合には約 9.9 秒であった．この差分は，インターネットを通過する多数の IPSec 確立処理メッセージがハンドオフ時間に大きく影響を及ぼしていることを示している．

5. プロキシ MOBIKE のハンドオフ高速化に関する考察

4.2 節で示した実験結果のとおり，基本的なプロキシ MOBIKE 方式では，ハンドオフ後に再度 IPSec の確立手順を行うため，ハンドオフに 6 秒以上の時間を要する．そこで，プロキシ MOBIKE にコンテキスト転送の概念を適用した手法について提案する．ここでのコンテキスト転送は，IPSec などのリンク設定情報をハンドオフ前のフェムトセルからハンドオフ後のフェムトセルへ転送する機能と定義する．また，そのコンテキスト転送に用いられる，フェムトセル上の IPSec のセッション情報を一意に特定する識別子を IPSec セッション識別子と定義する．図 9 にプロキシ MOBIKE コンテキスト転送方式のハンドオフ手順を示す．端末はハンドオフ後の LCP 設定要求にハンドオフ前のフェムトセルの識別子（FAP#1）及び FAP#1 上に存在する当該端末用の IPSec セッション識別子を含めて送信する．FAP#2 は，この LCP 設定要求を受信すると，FAP#1 に対して IPSec セッション識別子を含めたコンテキスト転送要求を送信する．FAP#1 は IPSec セッション識別子によって特定した当該端末の IPSec セッションの情報（IP#1，IPSec 設定情報，フェムトセル#1 の IP アドレス）を FAP#2 へ転送する．FAP#2 は FAP#1 から取得した当該端末の IPSec セッションの情報に基づいて IPSec セッションを復元し，MOBIKE による IPSec トンネルの終端変更（FAP#1 の IP アドレス =>FAP#2 の IP アドレス）を FGW に通知する．FAP#2 は MOBIKE 処理後，端末に対して認証を不要とした LCP 設定応答を返信する．FAP#2 は端末からの IPCP 設定要求に対し，既に FAP#1 から取得した IP#A を含めて IPCP 設定応答を返信する．よって，基本的なプロキシ MOBIKE 方式と同様，端末に割り当てる IP#A は変更されないため，アプリケーションの通信は継続される．

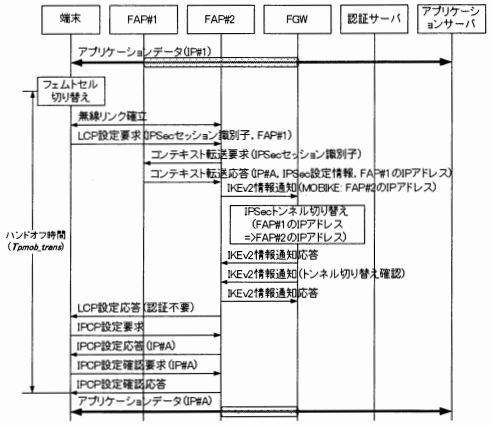

図 9　プロキシ MOBIKE コンテキスト転送方式

ここで，プロキシ MOBIKE にコンテキスト転送方式を適用した場合のハンドオフ時間 T_{pmob_trans} は，FAP 間のメッセージ転送時間を T_4 とすると次の式で表される．

$$T_{pmob\_trans} = T_w + 6T_1 + 4T_2 + 2T_4 \qquad (2)$$

よって，基本的なプロキシ MOBIKE 方式とプロキシ MOBIKE コンテキスト転送方式のハンドオフ時間の差 T_{diff} は，次の値となる．

$$T_{diff} = (1) - (2) = 5T_1 + 4T_2 + 2T_3 - 2T_4 \quad (3)$$

式(3)において，オフィス利用等におけるフェムトセル間の距離は十分短く T_4 の値は小さいと考えられるため，インターネット上の転送遅延（T_1）が大きくなればなるほど，コンテキスト転送方式によるハンドオフ時間の短縮効果も大きくなる．このように，IPSec のセッション情報をハンドオフ前後の FAP 間で引き継ぎ，MOBIKE を FAP 上で実行することにより，認証処理や IPSec の再確立処理が不要となり，基本的なプロキシ MOBIKE に比べ，高速なハンドオフが実現できる．例えば，4.2 節で示した実験結果において，プロキシ MOBIKE コンテキスト転送方式を用いた場合，前述のとおり式(3)の T_4 は十分小さいとすると，片方向遅延（T_1）が 100 ミリ秒の場合には 0.5 秒程度，500 ミリ秒の場合には，2.5 秒程度ハンドオフ時間を短縮できると考えらえられる．

また，[17]のように PPP のリンク設定情報

もハンドオフ前後の FAP 間で引き継ぐことで，PPP リンクの再交渉手順を不要とし，さらに高速なハンドオフを実現することも可能である．

6. 結論

本稿では，フェムトセルを含む移動体ネットワークにおいて，フェムトセルのプロトコル実装数を低減することでその処理負荷低減を図るプロキシ MOBIKE について提案し，フェムトセルとセキュリティゲートウェイ間の遅延とプロキシ MOBIKE のハンドオフ時間の関係について明らかにした．また，高速なハンドオフを実現する方式として，フェムトセル間で IPSec のセッション情報を転送するプロキシ MOBIKE コンテキスト転送方式について考察を行った．

日ごろご指導いただく，KDDI 研究所秋葉所長に深く感謝いたします．

参考文献

[1] 3GPP, "IP Multimedia Subsystem (IMS); stage 2 (Release 8)," TS23.228 v8.5.0, June 2008.
[2] 3GPP2, "All-IP Core Network Multimedia Domain: IP Multimedia (IMS) Session Handling; IP Multimedia (IM) Call Model - Stage 2," X.S0013-003-B v1.0, Dec. 2007.
[3] J. Rosenberg et al., "SIP: Session Initiation Protocol," IETF RFC 3261, June 2002.
[4] FemtoForum, http://www.femtoforum.org/
[5] Vikram Chandrasekhar, Jeffrey G. Andrews and Alan Gatherer, "Femtocell Networks: A Survey," IEEE Communication Magazine, p.59-p.67, Sep. 2008.
[6] 3GPP2, "cdma2000 Packet Data Service: Wireless Local Area Network (WLAN) Interworking - Access to Operator Service and Mobility for WLAN Interworking," X.S0028-200-A v1.0, June 2008.
[7] P. Eronen, "IKEv2 Mobility and Multihoming Protocol (MOBIKE)," IETF RFC 4555, June 2006.
[8] K. Leung, G. Dommety, P. Yegani et al., "WiMAX Forum/3GPP2 Proxy Mobile IPv4," IETF draft-leung-mip4-proxy-mode-09, work in progress, July 2008.
[9] S. Gundavelli, K. Leung, V. Devarapalli et al., "Proxy Mobile IPv6", IETF RFC5213, Aug. 2008.
[10] C. Kaufman, "IKEv2 Internet Key Exchange (IKEv2) Protocol," IETF RFC 4306, Dec. 2005.
[11] 3GPP2, "Femto Network Overview and List of Parts (X.P0059-000-0)," work in progress, X50-20080721-015r2, July 2008.
[12] C. Perkins, "IP Mobility Support for IPv4," RFC 3344, Aug. 2002.
[13] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," IETF RFC 3775, June 2004.
[14] W. Simpson, "The Point-to-Point Protocol (PPP)," IETF RFC 1661, July 1994.
[15] C. Rigney, S. Willens, A. Rubens et al., "Remote Authentication Dial In User Service (RADIUS)," IETF RFC 2865, June 2000.
[16] http://www.strongswan.org/
[17] Anand Kagalkar, Sarit Mukherjee, Sampath Rangarajan et al., "PPP migration: a technique for low-latency handoff in CDMA2000 networks," ACM Mobiquitous, 2005.