2008－MBL－45（3）
2008/5/22

異種無線ネットワーク環境におけるサービス移動透過性のためのハンドオーバ認証方式の検討

藤澤俊之† 稲村勝樹‡ 田中俊昭‡

† 日本放送協会 放送技術研究所 〒158-8510 東京都世田谷区砧 1-10-11
‡ 株式会社 KDDI 研究所 〒356-8502 埼玉県ふじみ野市大原 2-1-15
E-mail: † fujisawa.t-dg@nhk.or.jp

あらまし 異種無線ネットワーク間におけるハンドオーバ制御技術がいくつか提案されている．その多くは Mobile IP をベースとしたハンドオーバやネットワーク認証などの処理時間の短縮化に関する技術を背景としている．しかし，コンテンツ配信サービスなどリアルタイム性を要求するサービスにおいて，端末側およびネットワーク側の独立した処理の時間の短縮だけでは冗長な処理の存在によりサービスの連続性を保障することが困難であると考えられる．そのため端末側とネットワーク側の協調によるハンドオーバおよびネットワーク認証とサービス認証の効率的な処理が要求される．筆者らは，ハンドオーバの制御およびネットワーク認証とサービス認証を効率化する方式を提案し，コンテンツ配信サービスにおけるサービス移動透過性（モビリティ）について考察する．

キーワード ハンドオーバ，サービス移動透過性，認証連携，異種ネットワーク

A Handover Authentication Scheme for Service Mobility in Heterogeneous Wireless Networks

Toshiyuki FUJISAWA† Masaki INAMURA‡ and Toshiaki TANAKA‡

† JAPAN BROADCASTING CORPORATION, Science & Technical Research Laboratories
1-10-11 Kinuta, Setagaya-Ku, Tokyo, 157-8510 Japan
‡ KDDI R&D Laboratories Inc. 2-1-15 Ohara, Fujimino-Shi, Saitama, 356-8502 Japan
E-mail: † fujisawa.t-dg@nhk.or.jp

Abstract There are some proposed handover technologies in heterogeneous wireless networks. Most of the proposed technologies are based on the Mobile IP technology that is to reduce a processing time for handover, network authentication and service authentication. However it is difficult to guarantee continuity of a real-time service and/or video on demand service, even if it reduces a processing time of a terminal side or a network side independently without cooperation. Therefore it is required a cooperative processing between a terminal side and a network side, network authentication and service authentication. Hence we propose an efficient handover control and authentication scheme that combines networks and services, and discuss service mobility for contents distribution services.

Keyword Handover, Service Mobility, Authentication, Heterogeneous Networks

1. はじめに

無線ネットワークはさまざまな規格が存在している．例えば，IEEE802.11[1]，WiMAX フォーラム[2]や 3GPP[3]/3GPP2[4]などである．これらのネットワークは独立に機能している．最近，これらのネットワークを相互に接続できる異種ネットワーク間におけるハンドオーバの研究[5]-[8]がなされている．これらの多くの事例は，Mobile IPv6(MIPv6)[9]などをベースにハンドオーバを制御し相互接続を実現する．ハンドオーバは携帯端末の移動に伴うネットワークの切替制御技術である．そのため，携帯端末の移動透過性（モビリティ）が重要な要求条件となる．ハンドオーバの主な処理は，ネットワークの発見および選択，アクセスポイントの切替，ネットワーク設定，IP レイヤのハンドオーバである．しかし MIPv6 のみでハンドオーバを実行するとその処理に多くの時間を必要とし，結果としてシームレスな相互接続はできない．そこで，ハンドオーバを支援する技術として IEEE802.21[10]や LIES[11]などが検討されている．これらの技術はリンクレイヤ

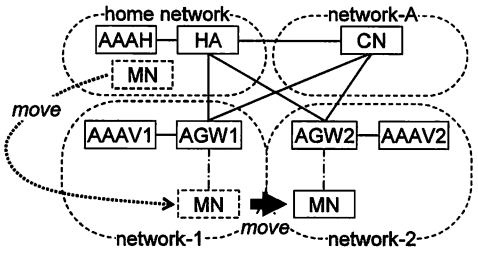

図1 全体の構成図

とネットワークレイヤ間で情報を協調して伝達し，高速かつ効率的なハンドオーバを支援する．

本研究は，コンテンツ配信サービスにおいて携帯端末が異種ネットワーク間を移動してもシームレスにサービスを提供できるように高速かつ効率的なハンドオーバ制御の実現を目標とする．コンテンツ配信サービスでは携帯端末が移動しても携帯端末のモビリティを確保しかつ携帯端末上でサービスを中断させることなく実時間でコンテンツを提供しなければならない．上記のようにサービスの連続性を確保するモビリティを「サービスモビリティ」と定義する．サービスモビリティを実現するためには，ネットワーク認証とサービス認証などの処理を効率化し，ハンドオーバとサービスの提供に関わる処理の簡素化を図る必要がある．本研究ではハンドオーバにおけるネットワークの事前設定方法およびネットワーク認証とサービス認証を連携させた認証方法に着目し基本的なネットワーク制御プロトコルを検討する．

第２章では想定するコンテンツ配信サービスモデルの概要と要求条件を述べる．第３章ではシームレスなコンテンツ配信を行うためのネットワーク制御について述べ，第４章では提案方法の考察を行う．第５章は関連研究を紹介し，第６章でまとめる．

2. 想定するサービスモデル

2.1. サービスの概要

本研究で想定するコンテンツ配信サービスは携帯端末で配信されたコンテンツの受信中に，ユーザーの移動によるネットワークの切替えが行われても途切れることなくシームレスにコンテンツを視聴できる．ユーザーは異なる規格，例えば，セルラー網と WiMAX など，に対応する複数のネットワークインターフェース(IF: interface)を搭載する携帯端末(MN: mobile node)を所有し，通信事業者(A)と契約している．通信事業者(A)はネットワーク接続に関して複数の通信事業者(X)と提携の関係にある．本サービスモデルはユーザーの移動に伴い，異なるネットワークへ接続が必要となった場合，通信事業者(A)と通信事業者(X)がネットワーク接続で提携関係にあればハンドオーバにより相互接続することができる．したがってユーザーは MN でコンテンツを受信しながら移動し，現在接続中のアクセスゲートウェイ(AGW: access gateway)のサービスエリアを越えた場合であっても他の通信事業者(X)のネットワークに自動的に接続し，コンテンツが途切れることなく連続して MN で視聴できる．コンテンツは H.264[12]などの構造化された符号化方式で符号化されている．

また，ユーザーは MN で専用アプリケーションを起動することで本サービスを利用できる．そしてコンテンツを選択して MN でそれを視聴する．この時点から本サービスのためのサービスモビリティ制御を開始する．なお，サービスモビリティ制御の開始前はノードモビリティ[13]を実現する Proxy Mobile IPv6 (PMIPv6) [14]などで制御されているものと仮定する．

2.2. 品質制御

異種ネットワーク間でのハンドオーバではそれぞれのネットワークで提供できる品質が異なると予想される．つまり，現在接続中のネットワークと同一の品質をハンドオーバ候補先のネットワークでは維持できないことを考慮しなければならない．その解決のため，本サービスモデルはユーザーにコンテンツの提供品質に関する受信ポリシーの設定手段を提供する．その受信ポリシーの例を以下に示す．

(1) 最高品質受信：ネットワークで提供できる最高品質でコンテンツを受信する．ハンドオーバごとに提供される品質は異なるが，そのネットワークが提供できる最高品質でコンテンツが提供される

(2) 平均品質受信：提携されたネットワーク間でハンドオーバを行ってもできる限り同一の品質でコンテンツを受信する．一定の品質でコンテンツを提供できるようにネットワーク側で調整する

(3) 最低品質受信：ネットワークで提供できる最低品質でコンテンツを受信する．最低品質はユーザーがコンテンツを認識可能な程度の品質とする

上記受信ポリシーをネットワーク側に通知することでユーザーは希望する品質でコンテンツを受信できる．

2.3. 構成

本サービスモデルの構成は図１に示すように携帯端末(MN)，MN が直接接続するアクセスゲートウェイ(AGW)，AGW が所属するネットワークへの接続許可および課金処理を行う AAA サーバー(AAAV: visited authentication authorization and accounting)，MN が所属するホームネットワーク上のホームエージェント

(HA: home agent), ホームエージェントが所属するネットワークの AAA サーバー(AAAH: homed AAA)および MN の通信相手(CN: correspondent node)で構成される. MN は PKI(public key infrastructure)を搭載する. CN はサービス提供者のコンテンツ配信サーバーなどである. また, ホームネットワークは HA,AAAH,MN などで構成されるネットワークである.

各構成要素の前提条件を以下に述べる. AGW, AAAV, HA, AAAH はネットワーク基盤として安全である. また, MN は攻撃者の悪意により他の構成要素に対してネットワーク面およびサービス面で一般的なネットワーク攻撃が可能である. ただし, MN 内の TRM(tamper resistant module)は安全であり攻撃者は攻撃または攻撃のための利用ができない. AGW はパケット転送および AAAV と連携して AAA 処理に関わるがコンテンツ配信サービスに直接関与しない. AAAV は管理下にある AGW に接続する MN の AAA 処理およびモビリティ管理を行う. これらの情報は AAAH に安全に送信される. HA はコンテンツ配信サービスに直接関与しない. AAAH は HA の管理下にある MN の AAA 処理およびモビリティ管理など MN のすべてを管理する. CN は MN に対する匿名性を確保するため MN を直接把握せずに, コンテンツ配信サービスに関する処理を安全に行う. また, AAAH はユーザー管理とネットワーク管理を行うための DB(data base)を有する. ユーザー管理 DB は契約ユーザーに関するデータや課金のための MN の移動およびサービス受信履歴を管理する. ネットワーク管理 DB はハンドオーバ可能な通信事業者のリスト, そのネットワークプレフィックスおよび提供可能な転送レートなどを管理する. これらの DB は随時更新される.

2.4. 要求条件

本サービスモデルを実現するための要求条件を以下に示す.

(1) コンテンツ配信：ハンドオーバが行われても MN でシームレスにコンテンツを視聴できること
(2) MN の管理：HA は MN のモビリティおよび利用したサービスを管理できること. ただし HA はコンテンツ配信サービスに直接関与しないこと
(3) 匿名性：CN に MN の行動を把握されないこと
(4) なりすましの防止：各構成要素のなりすましが防止できること
(5) 課金正当性：MN のネットワーク接続を把握し正しく課金およびその一元管理ができること
(6) 通信の安全性：構成要素間の通信において安全な通信が確保できること
(7) ハンドオーバの安全性：ハンドオーバに関する攻撃を防止できること
(8) CN の構成：CN はコンテンツ配信サーバーであることを想定し, ネットワークごとに配置されることを考慮すること

3. 提案方式の基本設計

MN の移動に伴うハンドオーバ手順は, 主に(a)ハンドオーバの必要性を判断する処理, (b)ハンドオーバ候補先を決定するためのネットワーク選択処理および(c)認証処理を含むハンドオーバ実行処理である. 提案方式は上記(a)から(c)の処理を高速かつ効率的に処理するためのメカニズムである. 本章では図２の動作手順に従って提案方式を説明する.

3.1. 携帯端末の匿名性

提案するハンドオーバ制御方式では要求条件(3)により CN は通信相手である MN を直接把握することができない. そのため, HA は CN がコンテンツ配信サービスを提供する際に MN の匿名性を確保しなければならない. まず, HA は MN-CN 間で用いる制御信号用の暗号鍵(Ks)を生成する. Ks は MN がハンドオーバするごとに HA で生成される. MN は気付アドレス(CoA: care of address)と Ks でハッシュ値 h(CoA||Ks)を計算し, 関係[CoA,h(CoA||Ks)]を含むバインディング更新(BU: binding update)を行う. そして HA は MN が接続中の AGW の IP アドレス(IPA_AGW)と関連付けて関係[h(CoA||Ks), IPA_AGW]を CN に送信する.

CN は MN にパケットを送信する場合, h(CoA||Ks)を属性として IPA_AGW 宛にパケットを送信し, AGW は関係[CoA,h(CoA||Ks)]を参照し MN にそのパケットを送信する. Ks は課金の単位としても用いられる.

3.2. コンテンツ配信サービスの開始

ユーザーは専用アプリケーションを起動してコンテンツ配信サービスを受信する. 専用アプリケーションはコンテンツを提供する CN に接続しコンテンツの提供を受けるための設定を行う. ネットワーク認証は既に MN がネットワークに接続しているので行わない. 専用アプリケーション起動前のネットワークの状態は, MN の気付アドレスは CoA1 とし, MN-AGW 間, AGW-HA 間, HA-AAAH 間はそれぞれ暗号鍵 Kma1, Kha1, Kta による IPsec({Kma1, Kha1, Kta})が構成されている. 実際には, それぞれ複数の IPsec が構成されるが簡単のため IPsec(暗号鍵)と表記する.

まず, アプリケーションの起動後, HA と MN は PKI を用いて暗号鍵(Km)を共有する. また, HA は HA-CN 間通信で用いる暗号鍵(Ksa)および MN-CN 間の制御信号用の暗号鍵(Ks1)を生成し, それぞれの鍵を共有する. また, HA は MN の識別子 h(CoA1||Ks1)を計算し, CN に MN の BU を行い, 関係[h(CoA1||Ks1), IPA_AGW1]を送信する. AGW1 もこの情報を共有する. CN はこ

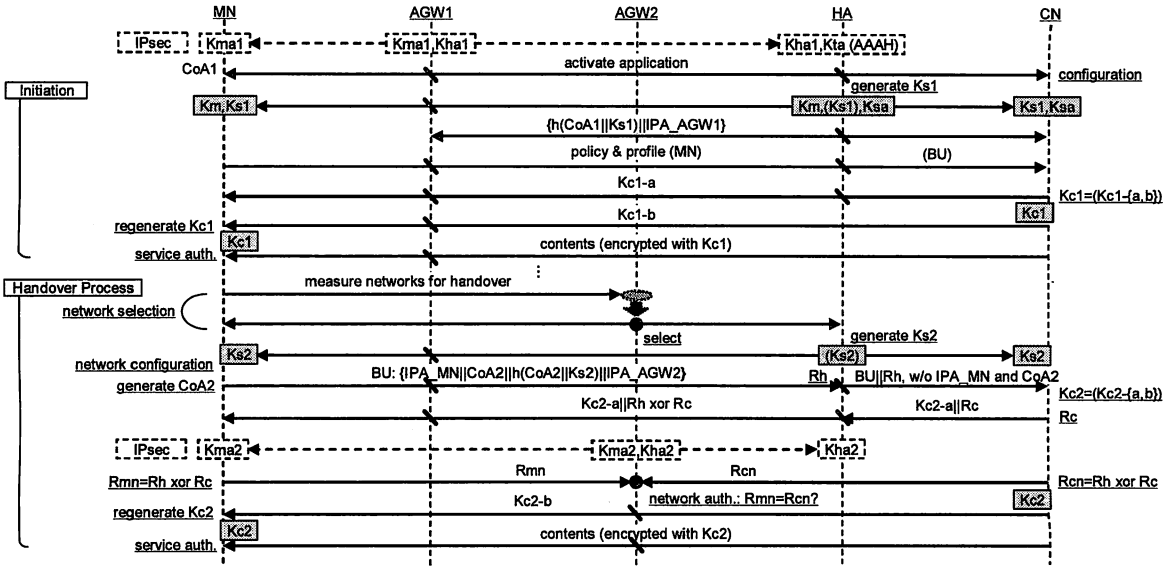

図2 ネットワーク制御の動作手順

の関係情報を用いてAGW1を経由してMNと通信する．また，MNは自身の性能に関するプロファイルと受信ポリシーをCNに送信する．

一方，CNはコンテンツ鍵(Kc1)を所定のアルゴリズムを用いて2分割(Kc1-{a,b})する．Kc1-aは経路CN-HA-AGW1-MNで，Kc1-bは経路CN-AGW1-NMでそれぞれMNに送信される．そしてMNはKc1-aとKc1-bを所定のアルゴリズムで合成しコンテンツ鍵(Kc1)を復元する．MNは配信されたコンテンツを正しく復号できればサービス認証とみなしてCNに通知し，CNは連続的にコンテンツを配信する．

3.3. ハンドオーバの事前処理

受信中の電界強度や受信安定度が劣化した場合，MNはハンドオーバが必要であると判断し，自身が搭載する他のネットワークIFを起動する．そしてそのネットワークのビーコンを捕捉して一定期間内にその安定度を測定する．ビーコンは図3のように，規格上の基本部分に加え，拡張部分（非暗号化部分と暗号化部分）およびメッセージ認証子(MAC: message authentication code)で構成される．非暗号化拡張部分はAGWのMN接続率と提供可能な転送レートが含まれる．MNはこれらの情報を用いて受信ポリシーを満たす場合，ハンドオーバ候補先としてその暗号化拡張部分を復号し，ネットワークプレフィックスなどを抽出し接続に必要な設定を行う．必要に応じて，ネットワーク側のハンドオーバ候補先の決定の支援を受けることもできる．提携ネットワークのビーコン鍵およびMAC鍵はユーザー契約時に通信事業者から提供される．またはこれらの鍵はネットワーク経由でも入手でき，それぞれ更新が可能である．

Basic Part (on Standard)	Extended Part (non encrypted)	Extended Part (encrypted)	MAC

図3 ビーコンの構成

3.4. ハンドオーバ制御

MNはビーコンから抽出したネットワークプレフィックスをもとにHAにハンドオーバ候補先の接続許可を要求する．そしてMNはハンドオーバ候補先のネットワークプレフィックスとインタフェースIDを用いてCoA2を生成してAGW2への接続設定を行う．

HAはMN-CN間の制御信号用の暗号鍵(Ks2)を生成し，MNとCNにKs2を送信する．またMNは識別子h(CoA2||Ks2)を計算し，HAとHAを経由してCNにBU処理を行い，関係[h(CoA2||Ks2), IPA_AGW2]を送信する．同時にAGW2もこの情報を共有する．このとき，HAはネットワーク認証のため乱数(Rh)を生成しCNに送信する．そしてCNは乱数(Rc)とコンテンツ鍵(Kc2)を生成し，Kc2を所定のアルゴリズムを用いて2分割(Kc2-{a,b})し，RcとKc2-aをHAに送信する．HAとCNはRhとRcを用いて排他的論理和(Rh⊕Rc=Rmn=Rcn)を求める．HAはKc2-a||Rmn (=Rh⊕Rc)を経路CN-HA-AGW1-MNを通してMNに送信する．

一方，ハンドオーバ候補先の通信を確立するため，HA-AGW2間およびAGW2-MN間でそれぞれIPsec({Kha2,Kma2})を構成する．また，ネットワーク認証のため，MNのRmnとCNのRcnをそれぞれAGW2に送信し，一致するかを検証する．その後，CNはKc2-bを経路CN-AGW2-MNを通してMNに送信する．MNは受信したKc2-aとKc2-bを所定のアルゴリズムで合成しコンテンツ鍵(Kc2)を復元する．MNは配信された

コンテンツを正しく復号できれば，MN，経路および Kc2-{a,b}の正当性の検証が確認でき，ネットワーク認証およびサービス認証とみなして CN に通知する．その後 CN は連続的にコンテンツを配信する．

4. 考察

提案したネットワーク制御および認証方式は，MN でハンドオーバの必要性の判断やネットワーク接続の設定を行い，AGW がプロキシとしてハンドオーバを実行する．したがって提案方式は，MIPv6 と PMIPv6 を組み合わせたアーキテクチャと考えられる．本章では提案方式での高速性，効率化および 2 章で述べた要求条件をもとに議論する．

4.1. 高速処理と効率化

要求条件(1)により，提案方式は高速かつ効率的な処理が要求される．3.4 章によるハンドオーバ手順(a)，(b)，(c)で要求される処理速度について考察する．(a)は接続中のネットワークの安定度や電界強度の劣化などを判断する処理であり高速処理が要求される．しかし安定度を判定するため，一定時間の測定が必要である．(b)はハンドオーバ候補先の選択に関する処理である．具体的には，MN に搭載されたネットワーク IF を起動し，受信したビーコンから必要な情報を抽出する．このとき提案方式では暗号処理が含まれているため高速処理が要求される．しかし MN に 3 以上のネットワーク IF が存在する場合，それらを順じ起動し，測定後にハンドオーバ候補先を判断する必要がある．この部分の処理が遅くなればなるほど実際のハンドオーバが遅れ，コンテンツのシームレスな提供が不可能となる恐れがある．そのため不必要なネットワーク IF の起動を抑制する必要があるため，ネットワーク側のハンドオーバ候補先の決定に関する支援は有効である．(c)はハンドオーバを実行するための処理であり，ハンドオーバ候補先への接続処理が行われる．特に CoA 生成，BU 処理，ネットワーク認証およびサービス認証などで高速処理が要求される．

一方，コンテンツ配信サービスを開始する場合の処理，つまり，専用アプリケーションの起動からコンテンツ配信までの処理は上記(a)から(c)に比べて高速処理を要求しない．したがって MN と HA において計算コストの高い PKI による暗号鍵交換は許容される．

上記考察から要求される高速処理，効率的な認証処理およびその他の要求条件を考慮し，提案方式は下記の特徴を具備している．

(1) アドレス生成とバインディング更新

MN の CoA 生成はビーコンのネットワークプレフィックスと MN のインタフェース ID を用いる．バインディング更新処理は HA と CN に対して行う必要がある．要求条件(3)により CN に対する MN の匿名性を確保するため，MN は識別子 h(CoA||Ks) を計算し，関係 [h(CoA||Ks), IPA_AGW]を HA 経由で CN へ BU 処理を行う．AGW でもこの関係情報を共有する．また，AGW は関係[CoA,h(CoA||Ks)]も管理する．

MN が同一 AGW に接続すると同一の CoA を生成するが，提案方式を用いることで，関係 [h(CoA||Ks),IPA_AGW]による MN のモビリティを実現することで，CN に対する MN の匿名性が確保される．これにより要求条件(2),(3)を満たすことができる．

(2) MN-CN 間通信

MN-CN 間での通信はハンドオーバ制御信号とコンテンツが混在する．要求条件(2),(5)により HA は MN のモビリティを管理するため，その管理単位および課金単位として用いる暗号鍵(Ks)をハンドオーバごとに生成し，MN,HA,CN で共有する．

また，MN,CN で共有するコンテンツ鍵(Kc)は CN が 1 台構成であればハンドオーバごとの生成を必要としない．また，複数の CN で構成してもコンテンツ提供位置などのコンテクストの共有が必要なため，コンテクストに Kc を含めることができる．しかし，要求条件(8)を考慮し，CN は Kc を独立に管理が可能なように，コンテンツ鍵(Kc)をハンドオーバごとに生成する方式とした．

(3) 認証処理

ネットワーク認証とサービス認証はハンドオーバの処理の短縮化のため連携が不可欠である．

まず，MN と経路検証のため，CN はコンテンツ鍵(Kc)を(Kc-{a,b})に 2 分割する．そして一方は現在接続中の経路 CN-HA-AGW1-MN を，他方はハンドオーバ候補先の経路 CN-AGW2-MN を通して MN に送信する．そして MN は受信した Kc-a と Kc-b を用いて Kc を復元する．コンテンツは構造化された符号化方式で符号化されているため，暗号化されたコンテンツを復元した Kc で復号し，正しく復号されれば Kc が正しく復元されたと判断し，ネットワーク認証とサービス認証の正当性が検証できたと判断できる．これにより高速かつ効率的な処理が可能であり要求条件(1),(6)を満たす．

その他，ビーコンの拡張部分で接続に必要な情報を暗号化することで，攻撃者が意図するネットワークへの誘導攻撃などを防止できるため要求条件(7)を満たす．また，適切な IPsec の構成により要求条件(4),(6)を満たす．

5. 関連研究

Mobile IP に関連した研究は数多くなされている[7]. モビリティを実現する IP を用いたアーキテクチャは，端末の移動に伴うハンドオーバ制御などを端末自身が行う Host Based Mobility と，端末はリンクレイヤ（L2）のみを認識しハンドオーバ制御などはネットワーク側で行う Network Based Mobility が検討されている．MIPv6[9]は前者をベースとし，PMIPv6[14]は後者をベースとしている．現在，IETF で PMIPv6 の標準化が策定中であり，3GPP/3GPP2 や WiMAX フォーラムでの利用が想定されている．また，MIPv6 と PMIPv6 を同時利用するアーキテクチャも検討されている[15][16].

6. むすび

本稿は，コンテンツ配信サービスのサービスモビリティを実現するためのハンドオーバ制御の高速化およびその認証方式の効率化に関するネットワーク制御方式の検討を行った．結果として MIPv6 と PMIPv6 の特徴を併用した方式となった．しかし，本稿の検討範囲は基礎段階であり，筆者らが把握していない課題を含むと考えている．

今後はこれらの課題を抽出し，さらなる高速化や効率化が可能なネットワーク制御とその認証方式を検討する．また，今回は CN が複数台で構成されることを考慮したが，より実用性の高い CN 構成法を考慮したサービスモビリティの実現法の検討を進める．

謝辞

本研究を進めるにあたり，本研究に関して日ごろご指導いただいた株式会社 KDDI 研究所・秋葉重幸所長ならびに長谷川亨執行役員に深く感謝する．

文　献

[1] http://www.ieee802.org/11/

[2] http://wimaxforum.org/

[3] http://www.3gpp.org/

[4] http://www.3gpp2.org/

[5] 泉川晴紀，福原忠行，宇野新太郎，松中隆志，蕨野貴之，杉山敬三，“異種通信システム環境におけるリアルタイムサービスのシームレス通信，” 信学技報，IN2006-20，pp.19-24，Jun.2006.

[6] 小川猛志，伊東匡，“DHCP をベースとしたシームレスハンドオーバ方法の研究，”信学論(B)，Vol.J88-B，No.11，pp.2228-2238，Nov.2005.

[7] Ian F. Akyildiz, J. Xie and S. Mohanty,"A Survey of Mobility Management in Next-Generation All-IP-Based Wireless Systems," IEEE Wireless Communications, Vol.11, Issue.4, pp.16-28, Aug.2004.

[8] S. Leggio, J. Manner and K.Raatikainen,"Achieving Seamless Mobility in IP-Based Radio Access Networks," IEEE Wireless Communications, Vol.12, Issue.1, pp.54-59, Feb.2005.

[9] D.Johnson, C.Perkins and J.Arkko, “Mobility Support in IPv6,”IETF RFC3775, Jun.2004.

[10] http://www.ieee802.org/21/

[11] 渋井理恵，神谷弘樹，寺岡文男，“レイヤ間情報伝達機構 LIES，” 日本ソフトウェア科学会，インターネットテクノロジ研究会第 6 回インターネットテクノロジワークショップ（WIT2004），pp.65-72，Oct.2004.

[12] T.Wiegand, G J.Sullivan, G Bjontegaard and A Luthra, “Overview of the H.264/AVC Video Coding Standard,” IEEE Trans. on Circuits and Systems for Video Tech., Vol.13, No.7, Jul 2003.

[13] 寺岡文男,”インターネットにおけるノード移動透過性プロトコル，”信学論(D)，Vol.J87-D-1，No.3，pp.308-328，Mar.2004.

[14] S.Gundavelli, K.Leung, V.Devarapalli, K.Chowdhury and B.Patil,"Proxy Mobile IPv6," draft-ietf-netlmm-proxymip6-11.txt, Internet-Draft, Internet Engineering Task Force, Feb. 2008.

[15] 湧川隆次，村井純，”Proxy Mobile IPv6 及び周辺技術の概要，及びその IETF 標準化動向について，”情処学 MBL 研報，Vol.2007，No.43，pp.83-89，Nov.2007.

[16] 田辺哲通，輿水敬，藪崎正実，”Mobile IP, Proxy Mobile IP 選択方式の提案,”信学会総合大会，B-7-203，pp.293，Mar.2007.

付録（記号）

- ||: 連接
- AAA*X*: authentication, authorization and accounting. *X*={H(home network), V(visited network)}
- AGW: access gateway
- BU: binding update
- CN: correspondent node
- CoA: care of address
- HA: home agent
- IPA_*XX*: 構成要素 *XX* の IP アドレス
- IPsec(*K*): 暗号鍵(*K*)により構成された IPsec
- Kc: CN がハンドオーバごとに生成するコンテンツ鍵
- Kc-{a,b}: 所定のアルゴリズムにより 2 分割されたコンテンツ鍵(Kc)のデータ
- Kha: AGW-HA 間における IPsec の暗号鍵
- Km: MN と HA の共通暗号鍵
- Kma: MN-AGW 間における IPsec の暗号鍵
- Ksa: HA-CN 間における暗号鍵
- Kta: HA-AAAH 間における暗号鍵
- MN: mobile node
- R{h,c}: 乱数（それぞれ HA,CN で生成される）
- R{mn,cn}: MN,または CN が所有する以下の演算による値．R{mn,cn}= Rh ⊕ Rc

なお，各記号の数字はネットワークの識別子である