

本資料について

- 本資料は下記の文献を基に作成されたものです。文章の内容の正確さは保障できないため、正確な知識を求める方は原文を参照してください。
 - 著者 : P.McCann
 - 文献名 : Mobile IPv6 Fast Handovers for 802.11 Networks
 - 種類 : Internet Draft
 - 発表日 : August 2004

Mobile IPv6 Fast Handover for 802.11 Networks

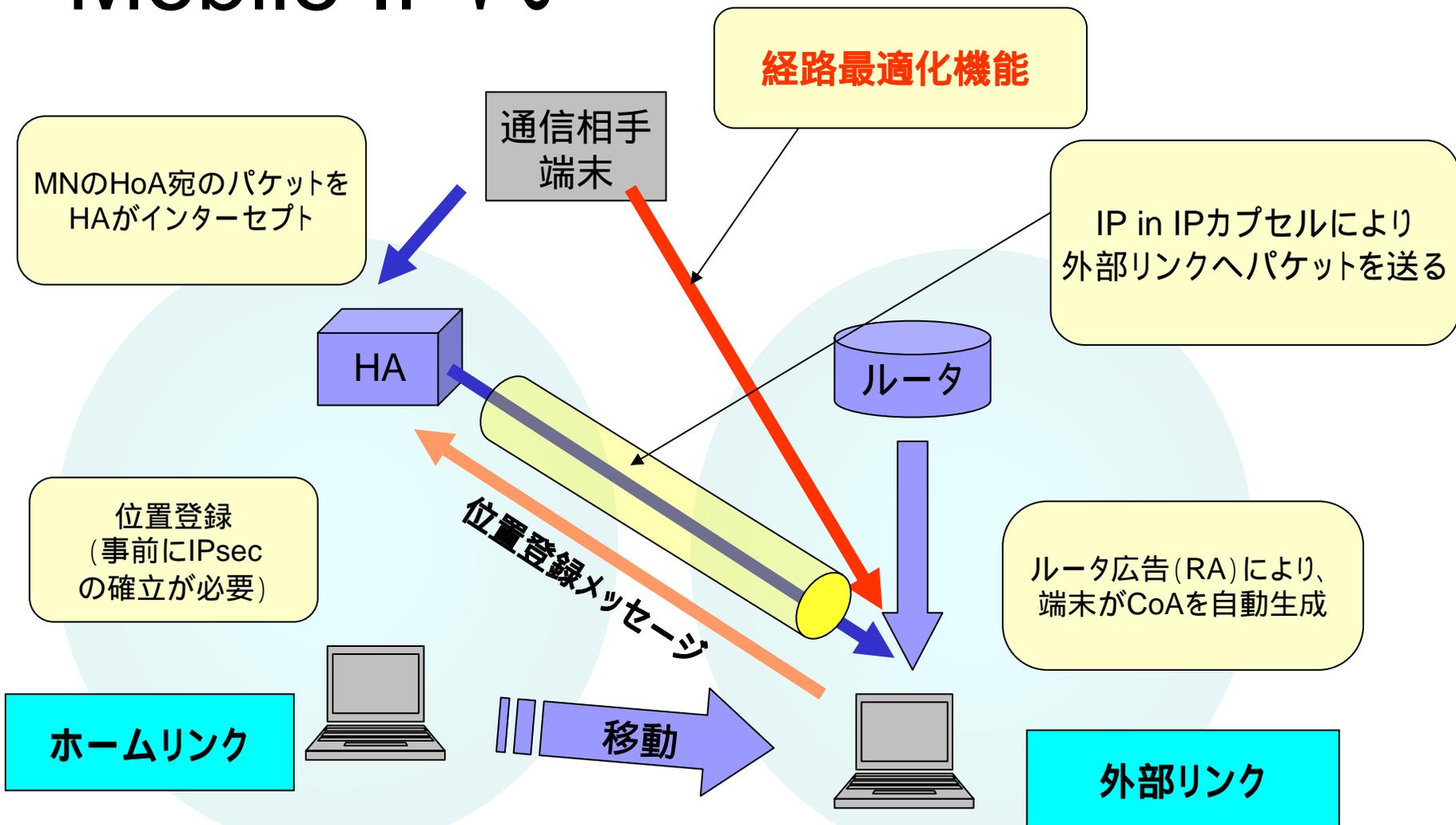
渡邊研究室

01j042 小島崇広

はじめに

- ハンドオーバーとは、
接続するAP (AccessPoint) を切り替えること
- Mobile IP
IPレベルでモビリティを実現する技術
MobileIPv4, MobileIPv6など

Mobile IPv6



Mobile IPv6の問題

■ Mobile IPv6

…移動時においてもIPサービスの継続性が確保可能
しかし、

ハンドオーバーのときアドレス生成処理と位置登録処理に時間がかかる

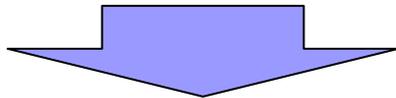
パケットロスが発生

リアルタイムアプリケーションなどの品質が著しく劣化

移動中でも途切れることなく高速通信を実現する高速ハンドオーバー技術が**必要**

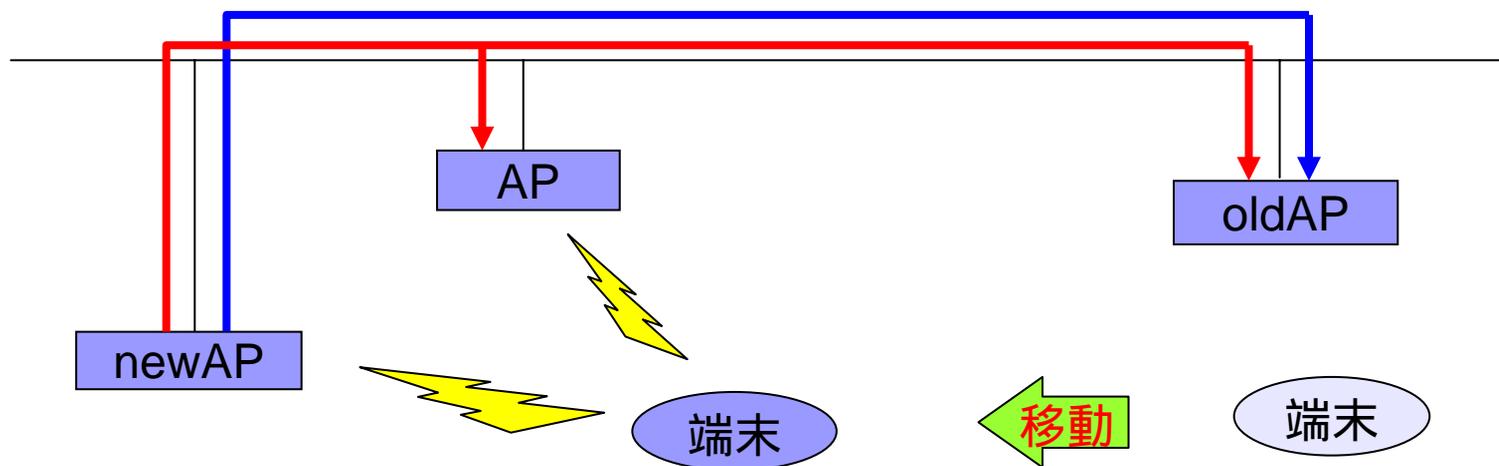
FMIPv6 (Fast handovers for MIPv6) とは

- IETFで標準化作業中の高速ハンドオーバーの実現技術
- 移動元サブネットで通信中に移動後サブネットの検出や移動後サブネットでのIPレイヤ設定値の生成実施
 - モバイルIPv6では旧サブネットでの通信不可が確定後に実施
- 通信ができない期間は網内でパケットをバッファ



パケット廃棄や遅延時間の短縮を実現

802.11ハンドオーバー



使用可能なAPをスキャン

物理層の情報と共にAPのリストを作成

リストからひとつのAP(以後newAP)を選び時刻同期を取る

端末はnewAPとの認証を行う

端末とAPの間でリアソシエーション要求/応答フレームの交換が行われる

newAPはリアソシエーション要求に含まれるoldAPのMACアドレスからoldAPのIPアドレスを検索。
oldAPから端末の情報を消去

テーブルの更新を行う

802.11ハンドオーバー についての補足

- 802.11ハンドオーバーは同一管理ドメイン内での移動を想定したものである
- 無線電波状態は一瞬で変化することがあるので、スキャンしたAPが次の同期を取る時点で使用できる保証はない
- スキャンは所有者の走査アルゴリズムを利用してNICの中のファームウェアによって実行される

CN: Correspondent node 通信相手

HA: Home Agent

PAP: Previous Access Point

PAR: Previous Access Router

NAP: New Access Point

NAR: New Access Router

MN: Mobile Node

RtSolPr : Router Solicitation Proxyルータ要請代理

PrRtAdv : Proxy Router Advertisement

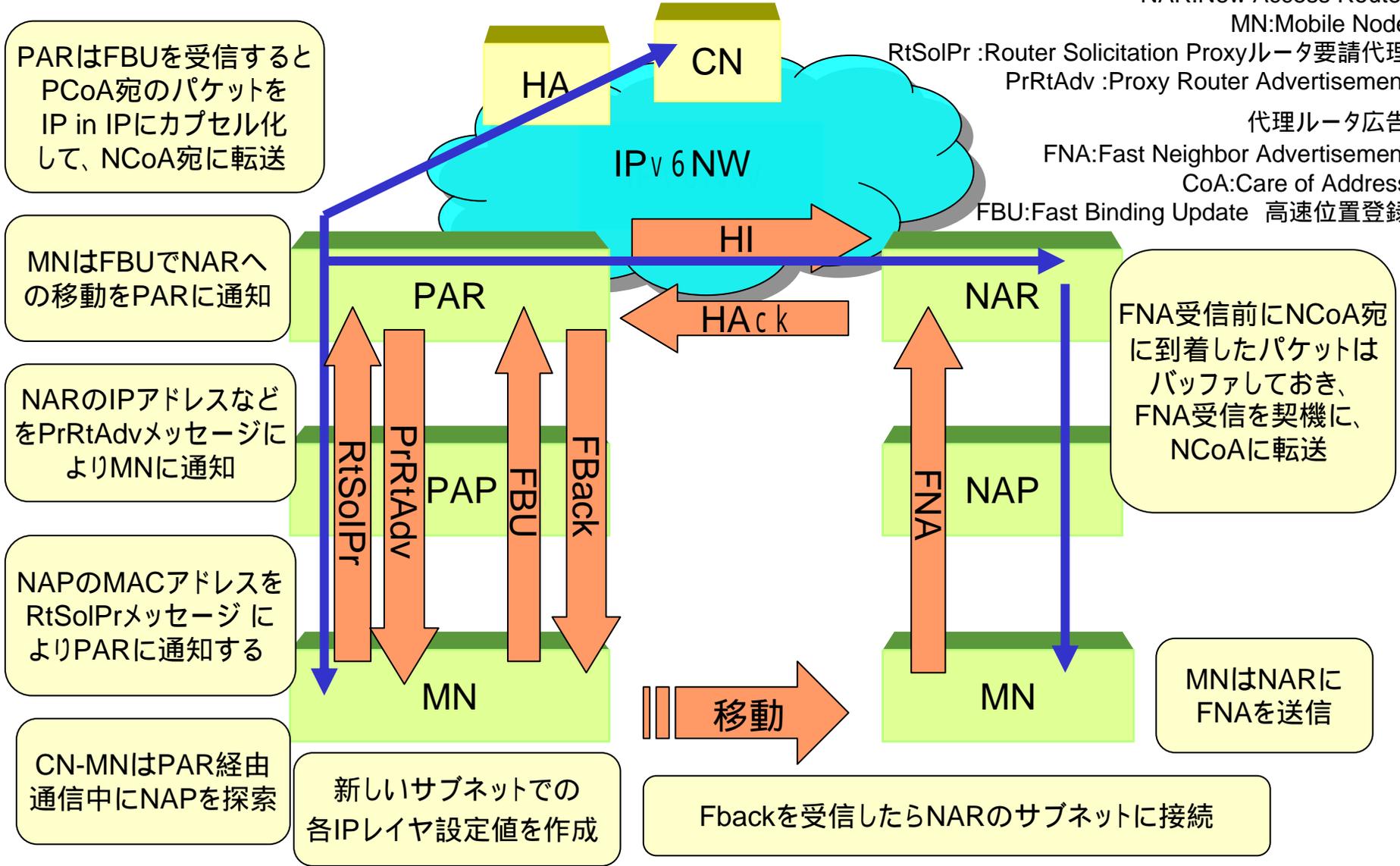
代理ルータ広告

FNA: Fast Neighbor Advertisement

CoA: Care of Address

FBU: Fast Binding Update 高速位置登録

FMIPv6 (802.11と組み合わせたときの動作図)



信号走査

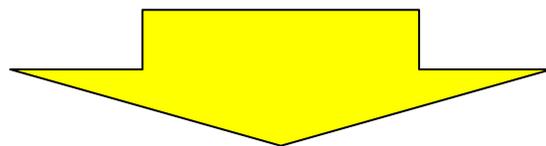
- 信号走査は、信号の強さ情報により利用可能なAPのリストを作る。このリストは、RtSolPrメッセージで必要なMACアドレスが供給される。
- ルータ要請代理メッセージ(RtSolPr)はAPに接続されたARに関する情報を要求するために使用される。APはRtSolPrの中ではMACアドレスによって指定されている。APのIP層情報は代理ルータ広告(PrRtAdv)の中で返される

セキュリティ

■ FBUメッセージ

- FMIPv6メッセージにおいて唯一フォワーディング状態を設立できる

既存のセキュリティ・メカニズムによって保護されているので、PARはFBUがMNで生成されたと保証



移動先のAPからのアソシエーションが相互の認証を使用して保護されていないと、悪意のあるAPはPARにFBUを送ることでMNをだますことができる

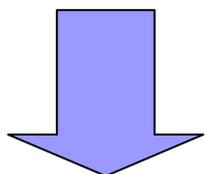
セキュリティ

- 根本的な802.11ハンドオフのセキュリティ問題
 - 悪意のあるノードにより802.11ハンドオーバーで説明した、 が実行された場合、レイヤ2をフォワーディング状態にできサービスの混乱を引き起こすことができる。
 - 802.11ハンドオーバーでは標準化された安全な認証アルゴリズムがない

セキュリティ

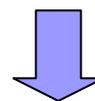
■ 802.1Xについての問題

- 802.1X認証はアソシエーションの後に行われる

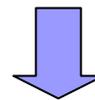


- 悪意のあるノードが同じサブネット上の異なるAPへの通信を転送することが可能

オープンシステム認証



アソシエーション要求・応答



802.1X認証

より速いサブネット認証の可能性

■ より速いクロス・サブネット認証

- セキュリティ資格を移動するためにIAPPの転送機能の背景に影響を与える
- サブネット境界を渡るPANA (Protocol for Carrying Authentication for Network Access ネットワーク・アクセスのための認証を運ぶためのプロトコル) のようなIP層メカニズムを使用する前認証