(3) 4G 移動通信網用 IP アクセスネットワーク技術

インターネットと親和性のあるアクセスネットワークの構築は，4G 移動通信網の実現に向けた重要な課題の 1 つである．ここではUSA研究所におけるIPアクセスネットワーク技術に関連する研究活動および最近の動向について紹介する．

舩渡（ふなと） 大地（だいち） Xiaoning He（シャオニン ハ）
Guangrui Fu（ガングルイ フ） Moo Ryong Jeong（ムー リョン ジョン）

1. まえがき

近年，インターネット技術は，第4世代（4G）移動通信網を構成する基本要素として広く受け入れられてきている．特にIP（Internet Protocol）は，将来において広範に使われるレイヤ3技術と考えられ，モビリティやサービス品質（QoS：Quality of Service），セキュリティといった高度な機能を組み込むことによって進化を遂げてきた．

しかし，4Gに必要な機能の多くをIPレイヤに組み入れることは，ホストやネットワークの運用を複雑なものにする可能性がある．もともとIPレイヤは，エンド・ツー・エンドでのパケット転送を行うシンプルなネットワークレイヤとして設計されており，すべての移動通信処理に対応させるには必ずしも最適なレイヤとは限らない．そこで，USA研究所では，レイヤ間の相互作用を考慮し，高度な機能を適切な場所に配置することで，4Gに向けた移動通信網アーキテクチャの設計を行っている[1].

本稿では，その内のIPアクセスネットワークと無線LAN（Local Area Network）に関連する研究内容を紹介する．ここでは特に，IPレイヤ以下で高度な機能を提供する試みを紹介する．2章では，アクセスネットワークにおけるマイクロモビリティの研究動向を紹介する．3章では，無線アクセスポイントの集中管理方式であるスプリットMAC（Medium Access Control）技術について説明する．4章では，アクセスネットワークの新たなセキュリティ方式としてモバイルファイヤウォールを取り上げる．5章では，無線LANの高速スキャニング方式を紹介する．

2. マイクロモビリティ

2.1 IPモビリティ管理における問題

インターネット技術特別調査委員会（IETF：Internet Engineering Task Force）では，IPプロトコルでエンドホスト（EHOST：End HOST）のモビリティをサポートするために，モバイルIP（MIP：Mobile Internet Protocol）の標準化を行っている[2]．MIPでは，移動局が異なるサブネット間を移動する際に，移動を通知する信号メッセージ，BU（Binding Update）メッセージをホームエージェント（HA：Home Agent）と相手ノード（CN：Correspondent Node）の両方に送信することでその位置を更新する必要がある．

MIPはIPレベルでユーザモビリティをサポートするが，4Gに必要な要求を完全には満たしてはいない．第1に，MIPは一時的なローミングに対応するように設計されているため，シームレスなハンドオーバをサポートしていない．そのため，USA研究所では高速MIP（FMIP：Fast Mobile Internet Protocol）を開発した[1]．第2に，MIPにはスケーラビリティの問題がある．MIPモビリティ管理のユニットサイズがユーザ移動に比べて小さく設計された場合，膨大な量のBUメッセージが生成され，HAとCNの両方に送信される．この時，移動局の数が多いと，これらの信号メッセージによって無線リンクとインターネットバックボーン上の多くの資源（帯域幅など）が消費されることになる．このようなスケーラビリティの問題を解決するために，マイクロモビリティというプロトコルの研究開発が進められている．

2.2 マイクロモビリティプロトコル

ここ数年間に，いくつかのマイクロモビリティプロトコルが提案されている[3]〜[5]．提案されたマイクロモビリティプロトコルを比較すると，その多くが類似した特徴を共有しており，主に以下のような方法により信号メッセージ数とパケットロスを大幅に削減している．

(1) ネットワークを複数のマイクロモビリティドメインに分割する．
(2) 各移動局に2つの気付アドレス（CoA：Care of Addresses）を割り当てる．一方は移動局が位置するドメインの位置（マクロな位置）を，もう一方はドメイン内における移動局の現在位置（マイクロな位置）を示す．
(3) ゲートウェイルータと呼ばれるルータが存在し，移動局がマイクロモビリティドメイン内で移動する場合，BUメッセージをゲートウェイルータのみに送信してその位置情報を更新する．そして移動局がマイクロモビリティドメイン間を移動する場合にのみ，ゲートウェイルータがBUメッセージをHAとCNに送信し，移動局のドメイン情報を更新する．

このようなプロトコルは，それが機能するレイヤに応じて，IPベースのマイクロモビリティプロトコルとMPLS

(MultiProtocol Label Switching) ベースのマイクロモビリティプロトコルの2つの方式に分類できる．IPベースのマイクロモビリティプロトコルは，MIPをベースにしている．いろいろなIPベースのマイクロモビリティプロトコルが提案されており，文献[3]で詳細な比較が行われている．

2.3 MPLSベースのマイクロモビリティプロトコル

MPLSはIETFで標準化された技術である[6]．MPLSはレイヤ2.5のプロトコルで，レイヤ3のトラヒックを非同期転送モード（ATM：Asynchronous Transfer Mode）やフレームリレーなどの接続志向のレイヤ2トランスポートにマッピングできる手段を提供する．MPLSではレイヤ2資源の制御が可能な点から，資源の限られたアクセスネットワークでVoIP（Voice over IP）などの遅延や帯域の変化に影響を受けやすいトラヒックを制御するのに適していると考えられている．

既存のMPLSベースのマイクロモビリティプロトコルは，階層型MIPモデルを基にしている[4][5]．しかし，既存のプロトコルは，モビリティサポートとトンネルヘッダのオーバヘッド削減に重点が置かれ，QoS管理やトラヒック制御機能は十分に考慮されていない．

このような課題を同時に解決するために，USA研究所では新しいMPLSベースのマイクロモビリティプロトコルやドメイン構築法を研究している[7]．例えば，図1に示すようなネットワークで，R1～R2間とR2～R4間の帯域がひっ迫している時に，既存のマイクロモビリティプロトコルを使用する場合，移動局がアクセスルータ（AR：Access Router）1のエリアからAR2のエリアに移動すると，移動用ルーティングアルゴリズムに基づきAR1からAR2を結ぶパスが設定され，AR1とAR2の間にトンネルが設定される．ただし，このパスが移動局のQoS要件を必ずしも満たしているとは限らない．そこで，拡張されたMPLSシグナリングプロトコルを使用することにより，ゲートウェイルータまでの距離は最短ではないにしても移動局に対してQoSを保証するデータパスを任意に設定することができる．

3. スプリットMAC技術

3.1 スプリットMACアーキテクチャ

無線LANは，セルラネットワークを補完し，ブロードバンド無線サービスを提供する，コスト効率の高いソリューションと見なされている．しかし，それを大規模に展開するには，伝送範囲が限られているために，多数の無線アクセスポイント（AP：Access Point）の設置が要求される．また，各種のセキュリティの脅威に対処するため，各APを適切に設定しなければならない．通常，こうした設定は手作業で行われ，そのため多くの時間と労力が必要になる．これは，多数のAPを持つシステムに共通した問題である．したがって，多様な移動通信網にも適用できる一般的なアプローチを編み出す必要がある．

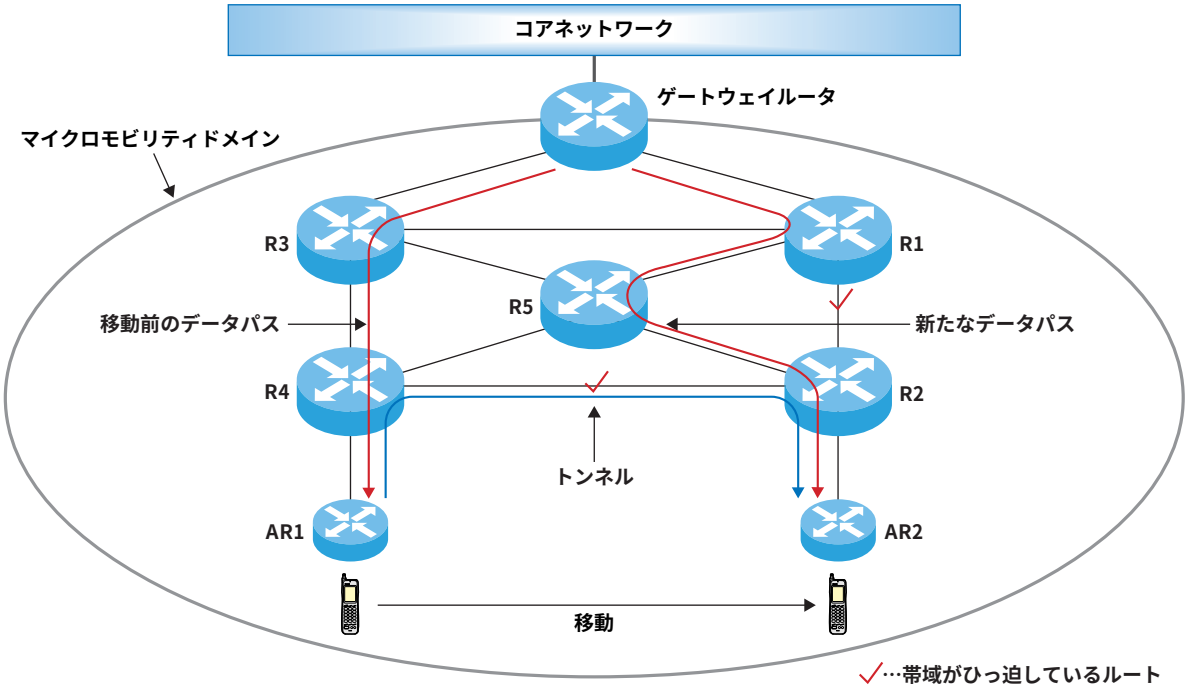


図1　マイクロモビリティルーティングの例

このような問題を解決するために，IPレイヤより下位で動作するスプリットMACと呼ばれる技術を開発している．このアーキテクチャでは，無線部のMACレイヤがAPとARの2つに分離され，主なMACフレーム処理機能はARが受け持ち，移動局との無線制御機能はAPが受け持つことになる．USA研究所を含む数社は，この技術に基づいた軽量アクセスポイントプロトコル（LWAPP：Light Weight Access Point Protocol）[8]をIETFに提案している．

図2はLWAPPのプロトコルスタックを表している．LWAPPでは，まずAPが自動的にARを発見し，ARから適切な設定パラメータを取得する．その後，APは下層のIEEE 802.11無線処理を実行すると，移動局から受信したIEEE 802.11フレームをARにトンネル転送し，ARがこのフレームを処理する．その結果，ARは複数のAPに対する制御センタとして機能する．LWAPPでAPが「軽量」と呼ばれる理由は，暗号化などを含む複雑なMAC処理コードや認証に必要な上位レイヤのプロトコルがAPから取り除かれ，APに要求される処理能力が小さくて済むためである．

このようにスプリットMACアーキテクチャでは，APの軽量化と管理の自動化が図られている．そして，ネットワーク管理者がARのソフトを更新するだけでMACレイヤ以上の新たな機能を追加できるため，サービスの更新やセキュリティ設定の変更に対しても柔軟な対応ができる．

3.2 LWAPPの機能

スプリットMACに基づいたLWAPPが実現する主な機能は以下のとおりである．

(1) AP自動設定と更新機能

APは起動されたときにAR発見プロセスを開始し，接続先ARに設定要求を送信する．ARからの設定応答には，無線チャネル周波数，ビーコン（標識）間隔，無線統計情報報告間隔など，APを設定するのに必要な各種パラメータが含まれている．これらのパラメータは，設定更新要求をARが送信することにより，いつでも更新できる．また，設定更新要求には，ファームウェアをAPがダウンロードし，AP自身の機能を更新する機能も含まれている．

(2) MACフレームカプセル化機能

APは，受信時に得られたRSSI（Receive Signal Strength Indication）および信号対雑音比（SNR：Signal to Noise Ratio）の値を含め，802.3（Ethernet）フレームにより802.11フレームをカプセル化した後，ARへ転送する．また，ARからAPへ送られる802.11フレームもカプセル化される．RSSIおよびSNR値は，ARでのIPモビリティ処理のきっかけを作る，ハンドオフトリガーの判定材料に利用される[9]．

(3) 無線統計情報の収集機能

APは，設定パラメータに基づいて無線インタフェースの統計情報を定期的にARに報告する．複数のAPの統計情報をARが収集することで，APの監視や侵入の検出を集約的に行うことができる．

(4) 移動局制御機能

ARは，一定の条件で特定の移動局とのトラヒックのやり取りを許可することをAPに通知することができる．この機能は，アクセス制御やQoS管理などの高度な機能を実現するために利用される．

4. モバイルファイヤウォール

USA研究所のモバイルファイヤウォール技術は，モバイルユーザがどこに移動しても，パケットフィルタリングによって保護し，エンドユーザとサービスプロバイダの双方に柔軟性の高いセキュリティポリシを提供する．

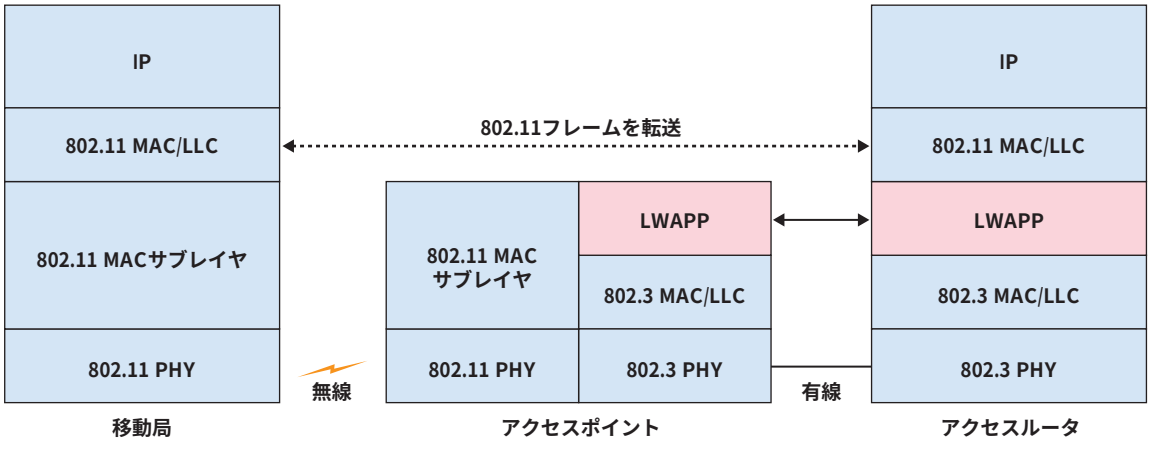


図2　LWAPPプロトコルスタック

4.1 既存のファイヤウォール技術

ファイヤウォールは内部ネットワークを保護するために広く使用されている．一般に，ファイヤウォールはネットワークを内部と外部の2つに分け，この両者間のトラヒックを事前設定されたセキュリティポリシに基づいてフィルタリングする．

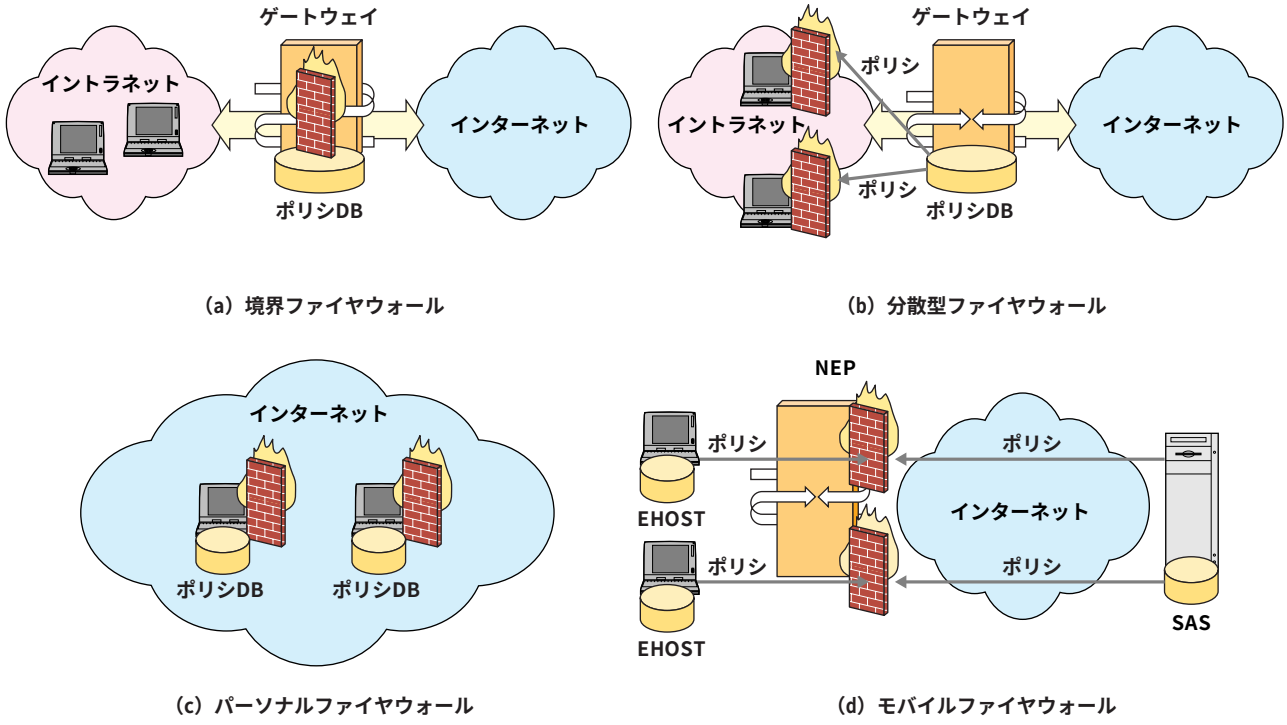
最も一般的なファイヤウォールは境界ファイヤウォール（perimeter firewall）[10]である．境界ファイヤウォールでは，図3(a)に示すように，パケットがネットワークゲートウェイのような出入口ポイントでフィルタリングされる．ネットワーク管理者のみがファイヤウォールにポリシを設定することができる．そのほかにも，既存のファイヤウォールとして，分散型ファイヤウォール（distributed firewall）[11][12]（図3(b)）やパーソナルファイヤウォール（図3(c)）などがある．分散型ファイヤウォールでは，パケットはすべての端末でフィルタリングされるが，ポリシは主としてネットワーク管理者が設定する．また，パーソナルファイヤウォールでは，パケットが各エンドホストでフィルタリングされ，エンドユーザがセキュリティポリシの設定を全面的に制御できる．

こうした既存のファイヤウォール技術は，ホットスポットなどの公衆無線環境で利用するとさまざまな問題を生じる．例えば，境界ファイヤウォールは，悪意のある者と被害者が同一ネットワーク内に存在する場合は，内部からのアタックを防止することができない．パーソナルファイヤウォールと分散型ファイヤウォールは同一ネットワーク内のアタックからエンドユーザを保護できる．しかし，このようなエンドホストベースのフィルタリングは無線アクセスネットワーク資源を浪費する要因となる．これらの方式は，限りあるバッテリ容量やコンピューティング資源をも浪費し，それによって携帯電話や携帯情報端末（PDA：Personal Digital Assistant）など，資源の制約されたEHOSTがDoS（Denial of Service）攻撃を受けやすくさせることになる．さらに，境界ファイヤウォールも分散型ファイヤウォールもユーザの移動を考慮していない．

USA研究所では既存ファイヤウォールが抱えるこのような問題を考慮した上で，モバイルファイヤウォール（図3(d)）を提案している[13]．これは無線アクセスネットワークの帯域幅を浪費せずに，ユーザが移動しても，サブネット内外からのアタックからユーザを保護することができる．移動するユーザに対する従来のパケットフィルタリング機能に加えて，モバイルファイヤウォールでは，エンドユーザやネットワーク事業者，サービスプロバイダがサービスごとにパーソナライズしたさまざまなセキュリティポリシを設定できる．

4.2 モバイルファイヤウォールのアーキテクチャ

モバイルファイヤウォールは，主として移動局を含む



（a）境界ファイヤウォール　（b）分散型ファイヤウォール

（c）パーソナルファイヤウォール　（d）モバイルファイヤウォール

図3　ファイヤウォールのアーキテクチャ

EHOSTネットワークエッジポイント（NEP：Network Edge Point），およびサービス管理サーバ（SAS：multimedia Service Agent for Service control）という3つのネットワーク要素で構成されている．これらの3要素はすべて，個々の優先事項とセキュリティ要件に基づいて，XML（eXtensible Markup Language）で記述したセキュリティポリシを設定することができる．

NEPはポリシ実施ポイントであり，LWAPPにおけるARのように，EHOSTが論理的にポイント・ツー・ポイント接続される最初のネットワーク要素である．各EHOSTについて，NEPはEHOST，SAS，またはNEPに設定したすべてのポリシを総合して階層ポリシ テーブルにマージし，このテーブルに基づいてEHOSTのパケットをフィルタリングする．モバイルファイヤウォールのフィルタ転送プロトコルを使用すると，EHOSTとSASはそのポリシをNEPにアップロードできる．また，モバイルEHOSTが新しいネットワークに移動した場合，NEPはこれらのポリシを以前のNEPから転送することができる．NEPはまた，到着したパケットが事前設定されたトラヒックパターンと一致しているかどうかをEHOSTまたはSASに通知することもできる．

このように，モバイルファイヤウォールは，従来のネットワーク管理目的だけでなく，パーソナルネットワーク管理やサービス固有のニーズに応じてパケットをフィルタリングできる．

5. 無線LANの高速スキャニング

5.1 背景

無線LANにおいて，移動局が接続可能なAPを検索するスキャニングプロセスは，ハンドオフにおいて最も時間を費やすプロセスである[14]．IEEE（Institute of Electrical and Electronics Engineers）のIEEE 802.11無線LANには，このタスクを実行する2つの方法，すなわちパッシブスキャニングとアクティブスキャニングがある．パッシブスキャニングは，受動的にAPからのビーコンフレームを監視するだけである．これに対して，アクティブスキャニングは近傍のAPに対して能動的にプローブ要求を送信する．APからビーコンフレームまたはプローブ応答フレームを受信すると，移動局はAPの到達可能性とプロパティ（性能，サポート速度，タイミング情報など）を学習する．本章では，これらのスキャニング方法を高速化するために，最近IEEE802.11の作業部会（WG：Working Group）のTGk（Task Group k）で検討されている，適応ビーコンと高速アクティブスキャニングについて概説する．

5.2 高速パッシブスキャニングの適応ビーコン

パッシブスキャニングでは，移動局が少なくとも1ビーコン間隔で各チャンネルに留まっていなければならず，しかもビーコン送信に伴うオーバヘッドと節電モードにある移動局の電力消費を抑制するために，その間隔は通常長い時間（100msほど）設定されているのでスキャニングに必要な待ち時間が長くなる．

適応ビーコン[15]では，ネットワーク負荷に応じた頻度で適応ビーコンを送信するため，その負荷が低いときには送信間隔を短くできる．そのため，移動局はビーコンおよび適応ビーコンを受信することで，APの到達可能性とプロパティを短時間で学習できる可能性が高くなる．ただし，適応ビーコンフレームには，節電モードにある特定の移動局宛にバファリングされたトラヒックを示すトラヒック表示マップ（TIM：Traffic Indication Map）が含まれていないため，節電モードにある移動局は，従来どおりビーコン受信時にのみ起動することで電力消費を抑制する．

5.3 高速アクティブスキャニング

アクティブスキャニングでは，できるだけ多くのAPからのプローブ応答を受信するのに十分な時間（最高50ms[16]）だけ各チャネルに留まっている必要があるため，スキャニングに必要な待ち時間は長くなる（図4(a)）．また，従来のプローブ要求はDCF（Distributed Coordination Function）を利用してブロードキャストされるため，APからのプローブ応答フレームと移動局からのデータフレームとの間で競合が生じ，DIFS（Distributed coordination function InterFrame Space）間隔に加えランダムな遅延が生じる．

高速アクティブスキャニング[16][17]では，移動局が受信先指定プローブ要求を特定のAPに送信することができる．受信先指定プローブ要求が送信される対象のAPの決定は，隣接AP情報[18]を持つサイトレポートに基づくものである．受信先指定プローブ要求を受信した対象APはAck（Acknowledge）フレームを送信することで確認応答を行い，後で改めてDIFSあるいはPIFS（Point coordination function InterFrame Space）間隔後にプローブ応答フレームを送信するか（図4(b)，(c)），可能であれば要求フレームに続くSIFS（Short InterFrame Space）間隔内にプローブ応答を送信する（図4(d)）．

このように，対象APを直接指定することで，それ以外のAPからの不要なプローブ応答が排除され，必要なプローブ応答だけがSIFSまたはPIFSを使用して優先的に送信されるため，移動局はプローブ応答をより迅速に取得できる（図4(d)，(c)）．対象APに受信先指定プローブ要求が到達できな

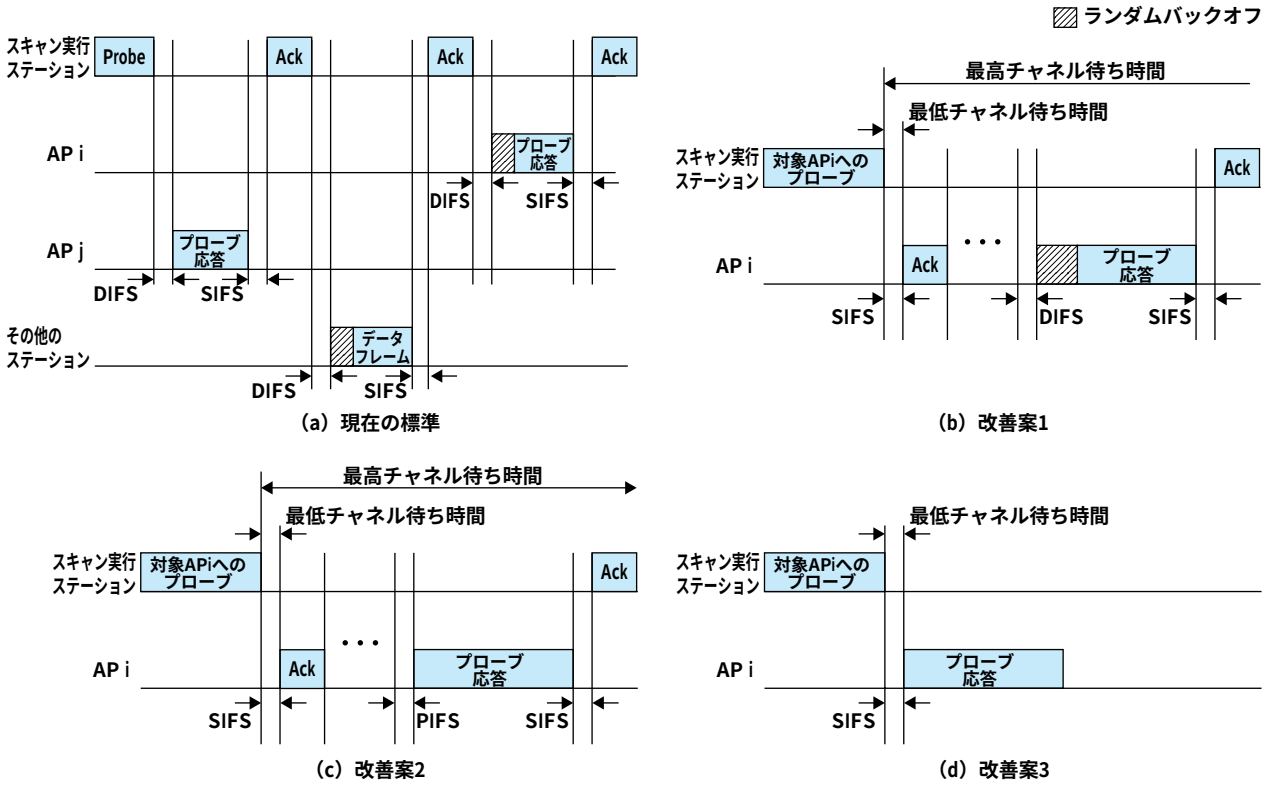


図4　アクティブスキャニングの改善

い場合，移動局は確認応答またはプローブ応答をSIFS内に受信できないことからその事実を迅速に知ることができる．

5.4 高速スキャニングの性能

高速アクティブスキャニングは柔軟性があり，ネットワーク負荷が小さい状態では1ms以内に実行される[17][18]．しかし，ネットワーク負荷が高いと，スキャニングに時間がかかり，帯域幅が消費されるためコストが高くつく．これは，各移動局がプローブ要求とプローブ応答フレームの交換を別々に実行しなければならないからである．一方，適応ビーコンはスキャニングに比較的時間を要するが，ネットワーク負荷に応じてスキャン時間と帯域幅の消費のどちらかを優先することで全般的に帯域幅の消費を抑制することができる．したがって，今後の研究では，適応ビーコンと高速アクティブスキャニングを適切に組み合わせることが要求される．

6. あとがき

本稿では，USA研究所における4G移動通信網に向けたIPアクセスネットワークに関する研究活動を紹介した．モビリティとQoS制御を同時に実現するMPLSベースのマイクロモビリティ方式，さらに複数のAPを1つのARで集中的に自動設定・管理できるスプリットMAC技術を取り上げた．また，モバイルユーザに安全で柔軟なパケットフィルタリングを提供するモバイルファイヤウォールを提案し，最後にシームレスなハンドオフを可能にする無線LANの高速スキャニング方式について概説した．

今後は，提案したさまざまな技術を統合するためのテストベッドを構築し，システム全体として評価していく予定である．

文　献

[1] R. Jain, et al: “(2)4G移動通信網用All-IPネットワークアーキテクチャ，”本誌，Vol. 11，No. 4，pp.13-17，Jan. 2004.
[2] D. Johnson, C. Perkins and J. Arkko: “Mobility Support in IPv6,”IETF work in progress, Jun. 2003.
[3] A. T. Campbell, et.al: “Comparison of IP Micro-Mobility Protocols,” IEEE Wireless Communications Magazine, Vol. 9, No. 1, Feb. 2002.
[4] J. Grimminger and H. P. Huth: “Mobile MPLS-an MPLS-based Micro Mobility Concept,”Wireless World Research Forum, Meeting 3, Stockholm, Sep. 2001.
[5] Recommendation Y.MIPoMPLS: “Mobile IP Services over MPLS,” ITU-T SG13, May 2003.
[6] E. Rosen, et.al: “Multiprotocol Label Switching Architecture,”IETF RFC 3031, Jan. 2001.
[7] X. He, D. Funato and T. Kawahara: “A Dynamic Micro-Mobility Domain Construction Scheme,”The 14th IEEE PIMRC, Sep. 2003.
[8] P. Calhoun, B. O’Hara, S. Kelly, R. Suri, D. Funato and M. Vakulenko: “Light Weight Access Point Protocol,”IETF work in progress, Jun. 2003.
[9] A. Yegin, D. Funato, K. Malki, Y. Gwon, J. Kempf, M. Pettersson, P. Roberts, H. Soliman and A. Takeshita: “Supporting Optimized

Handover for IP Mobility-Requirements for Underlying Systems," IETF work in progress, Jun. 2002.
[10] W. R. Cheswisk and S. M. Bellovin: "Firewall and Internet Security: Repelling the Wily Hacker," Addison-Wesley, 1994.
[11] S. M. Bellovin: "Distributed Firewalls,";login: magazine, special issue on security, Nov. 1999.
[12] S. Ioannidis, A. D. Keromytis, S. M. Bellovin and J. M. Smith: "Implementing a Distributed Firewall,"ACM Conference on Computer and Communications Security, Nov. 2000.
[13] G. Fu, D. Funato, J. Wood and T. Kawahara: "Mobile Firewall," The Fifth IFIP International Conference on Mobile and Wireless Communications Networks, Oct. 2003.
[14] A. Mishra, M. Shin and W. Arbaugh: "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process," ACM Computer Communications Review, 2002.
[15] P. Orava, H. Haverinen and S. Black: "Adaptive Beaconing," IEEE 802.11-03/610, Jul. 2003.
[16] M. Jeong, F. Watanabe and T. Kawahara: "Fast Active Scan for Measurement and Handoff,"IEEE 802.11-03/416, May 2003.
[17] M. Jeong, F. Watanabe, T. Kawahara and Zhun Zhong: "Fast Active Scan Proposals," IEEE 802.11-03/623, Jul. 2003.
[18] IEEE Std 802.11k/D0.6, Specification for Radio Resource Measurement (Draft Supplement to IEEE Std 802.11, 1999 Edition), Mar. 2003.

用 語 一 覧

Ack：Acknowledge
AP：Access Point（アクセスポイント）
AR：Access Router（アクセスルータ）
ATM：Asynchronous Transfer Mode（非同期転送モード）
BU：Binding Update
CN：Correspondent Node（相手ノード）
CoA：Care of Addresses（気付アドレス）
DCF：Distributed Coordination Function
DIFS：Distributed coordination function InterFrame Space
DoS：Denial of Service
EHOST：End HOST（エンドホスト）
FMIP：Fast Mobile Internet Protocol（高速MIP）
HA：Home Agent（ホームエージェント）
IEEE：Institute of Electrical and Electronics Engineers
IETF：Internet Engineering Task Force（インターネット技術特別調査委員会）
IP：Internet Protocol
LAN：Local Area Network
LLC：Logical Link Control
LWAPP：Light Weight Access Point Protocol（軽量アクセスポイントプロトコル）
MAC：Medium Access Control
MIP：Mobile Internet Protocol（モバイルIP）
MPLS：MultiProtocol Label Switching
NEP：Network Edge Point（ネットワークエッジポイント）
PDA：Personal Digital Assistant（携帯情報端末）
PHY：PHYsical layer
PIFS：Point coordination function InterFrame Space
QoS：Quality of Service（サービス品質）
RSSI：Receive Signal Strength Indication
SAS：multimedia Service Agent for Service control（サービス管理サーバ）
SIFS：Short InterFrame Space
SNR：Signal to Noise Ratio（信号対雑音比）
TGk：Task Group k
TIM：Traffic Indication Map（トラヒック表示マップ）
VoIP：Voice over IP
WG：Working Group（作業部会）
XML：eXtensible Markup Language