次世代に向けた無線電話システムの研究

伊藤将志

平成20年度

論文要旨

ここ十数年の間に，遠隔地の相手とのコミュニケーション手段は回線交換方式を利用した電話から，利便性や性能の向上を目的とし，大きく進化を遂げてきた．携帯用の小型無線電話機として携帯電話が登場し，いつでもどこにいても通話をすることができるようになった．通信方式もアナログ方式の第一世代携帯電話から，現在では W-CDMA や CDMA2000 などの第三世代携帯電話が主流となり，通信速度も 2Mbps 程度まで実現している．さらに，第四世代携帯電話の研究も進んでおり，50Mbps〜1Gbps 程度の通信速度が実現できるといわれている．しかし，電波の性質上，通信速度の向上のために周波数を高くすれば，建造物内部などに電波が届きにくくなるなど，高速通信と通信エリアの確保の両立は困難といえる．

一方，インターネット接続はブロードバンドの普及やバックボーンの整備により，膨大な情報を高速に提供できるようになった．近年では FTTH（Fiber To The Home）により 100Mbps〜1Gbps の通信速度を実現している．このインターネット技術を利用して，これまで回線交換方式であった電話を，パケット交換方式にした IP 電話に注目が集まっている．IP 電話は，従来の音声通話だけでなく，アプリケーションと組み合わせることによって，様々な作業の効率化が期待されている．IP 電話を内線として利用することで，通話費の削減も期待できる．また，通信インフラとしては，端末からインターネットへ接続する際のラストワンホップも，無線 LAN の普及により無線が主流になりつつある．無線 LAN は MIMO（Multiple Input Multiple Output）を利用することで 300Mbps 程度の通信速度を実現できる．そして，無線 LAN のエリアを容易に広げる方法として，無線メッシュネットワークの研究に注目が集まっている．無線メッシュネットワークは AP（Access Point）間の接続を無線アドホックネットワークによって無線化し，さらに各 AP に自律的に通信経路を形成する機能を持たせる．これにより，AP を適切に設置するだけで，ネットワークの範囲は拡大されていく．

無線メッシュネットワーク上で IP 電話を利用することを想定するといくつかの課題が発生するが，これらを解決できれば，様々な有用な効果が見込める．IP 電話を有効に利用するにはアプリケーションとの併用も求められ，高速な通信媒体が必要となる．無線メッシュネットワークは，第三世代携帯電話よりも高速な通信を提供することができ，第四世代携帯電話の電波が届きにくくなる屋内でも高速な通信を提供できる．また，これまでケーブル工事などによるコストの回収が難しいといわれた地域や，災害によって通常のインフラが破壊された地域にコミュニケーション手段を提供できる．このように，携帯電話に対し，互いの手の届かないところを補完しあうコミュニケーション手段となる．

本論文では，無線メッシュネットワークの実用化のための課題解決と IP 電話の利便性を向上する方法を提案する．まず，無線メッシュネットワークの一実現方式として WAPL（Wireless Access Point Link）の提案によって，無線メッシュネットワークをパケットロスの発生しないハンドオーバに対応させ，IP 電話などの通信断裂を防ぐ．次に，WAPL 内部

と外部ネットワーク上の端末どうしが通信する際に，複数の GW（Gateway）を利用するゲートウェイ分散方式の提案により，外部ネットワークとの通信を効率的に行う．最後に，WAPL と外部ネットワークの間に NAT（Network Address Translation）や FW（Firewall）が設置されていることを想定し，SoFW（SIP over Firewall）の提案により，IP 電話を含む SIP による通信が WAPL 内部と外部ネットワークで自由に行えるようにする．

第 1 章は序論であり，研究の背景，目的，既存技術，提案方式の概要，論文の構成などについて述べる．

第 2 章では，無線メッシュネットワークの一実現方式である WAPL を提案する．WAPL は，無線メッシュネットワークを実現するための機能を，アドホックルーティングプロトコルから完全に独立させた．その結果，ルーティングプロトコルを自由に選択し，様々な用途に応用できる．また，無線メッシュネットワークに必要なテーブルの生成をオンデマンドで実現するため，制御パケットが通信トラヒックに与える影響が少ない．さらに近隣の AP の通信状況を常時監視しておくことにより，端末が移動したときのハンドオーバ通知をユニキャストで実現できるようにした．これによりシームレスハンドオーバを確実に行うことができる．提案方式の有効性を評価するため，既存方式と WAPL を ns-2 のモジュールに組み込んで比較を行った．その結果，WAPL の特徴を定量的に示すことができた．

第 3 章では，無線メッシュネットワークにおいて効率良くゲートウェイを利用する方式を提案する．無線メッシュネットワークでは，インターネットなどの外部のネットワークと接続するとき，スループットのネックとなる GW 周辺の帯域の消費を解消するため，複数の GW を設置する方法が検討されている．これまで，パケットごとに複数の GW に分配する方式が検討されているが，TCP のふくそう制御の機能により通信のスループットを低下させてしまう．そこで，我々はセッションごとに複数の GW に分配することにより，GW を効率的に利用し，かつ TCP 通信のスループットに影響を与えない方式を提案する．シミュレーションによって提案方式が既存方式に比べて TCP 通信のスループットが向上すること，公平性も十分保たれることを明らかにした．

第 4 章では，ファイアウォールや NAT を通過できる IP 電話を提案する．これまでの類似の研究や解決方法では，専用端末が必要であることや，アドレス空間の統一的管理が必要であることなどの課題があった．SoFW は既存の SIP 端末を利用することができ，アドレス空間の統一的管理が必要なく，導入が容易であるという特長がある．SoFW を Linux 上に実装し，評価実験を行った結果，その有用性を確認することができたので報告する．

第 5 章は結論であり，本論文で得られた成果を統括する．

Abstract

Abstract in English.

目 次

1章　序論

あらまし

いつでもどこでも，音声通信やデータ通信などのサービスを提供できる技術が求められている．これを満たすシステムとして，現在最も広く展開されている携帯電話がある．しかし，第三世代携帯電話の通信速度は高々2Mbps 程度であり，現在研究段階である第四世代携帯電話も通信速度は速いものの，屋内では電波が届きにくいという性質がある．これらの通信手段で保証できないエリアを補う手段として，無線メッシュネットワークと IP 電話を利用する手段が考えられる．本論文では，音声通信を意識して無線メッシュネットワークを構築する際に発生する課題の解決法を提案する．まず，無線メッシュネットワークの一実現方式である WAPL（Wireless Access Point Link）の提案によって，パケットロスの発生しないハンドオーバに対応した無線メッシュネットワークを実現する．次に，WAPL 内部と外部ネットワークに接続した端末どうしが通信を行う際に，複数の GW（Gateway）を利用する GW 分散方式を提案することにより，外部ネットワークとの効率的な通信を実現する．最後に，WAPL と外部ネットワークの間に NAT（Network Address Translation）や FW（Firewall）が設置されていることを想定し，SoFW（SIP over Firewall）の提案により，IP 電話を含む SIP による通信が FW/NAT を越えて自由に行えるシステムを実現する．

1.1　背景，目的

ここ十数年間，遠隔地の相手とのコミュニケーション手段は，音声通信やデータ通信における利便性や性能の向上を目的とし，大きく進化を遂げてきた．現在，いつでもどこでも音声通信やデータ通信を行えるシステムとして，国際電気通信連合（ITU) の定める IMT-2000 規格を利用した第三世代携帯電話がある．第三世代携帯電話では 2Mbps 程度の通信速度を実現しており，通信速度を必要とする Web ブラウジングや E メールなどの電話以外のアプリケーションの快適な利用を可能にした．さらに高速な通信の需要を満たすため，第四世代携帯電話の研究も進んでおり，最大で 1Gbps 程度の通信速度の実現を目指している．このように，現在では音声通信と高速なデータ通信を可能とする無線システムが求められている．

しかしながら，第四世代携帯電話では第三世代携帯電話よりも高い周波数を用いる予定であるため，電波が遮蔽物の影響を受けやすくなり，建造物内部では通信が行えない場合が発生するなど，高速通信と通信エリアの保証の両立は困難といえる．また，僻地などの携帯電話を利用するユーザが少ないようなエリアでは，ケーブル配線の工事にかかる費用などのコストの回収が期待できず，導入が遅れる場合がある．地震や津波などの災害時でも，基地局間を接続するケーブルが切断されたり，安否確認などのために膨大な量の情報トラヒックが発生したりすると，上手く対応できない場合がある．

携帯電話が保証できないエリアを補う方法として，WiMAX や無線 LAN[1]を利用する手段が考えられている．WiMAX は 2〜10km の範囲をカバーし，端末が静止している場合で最大 75Mbps 程度の通信速度を実現する．無線 LAN は特に第四世代携帯電話の課題である屋内のエリアを保証するのに適している．無線 LAN は 100m 程度の範囲をカバーし，MIMO（Multiple Input Multiple Output）の技術を利用することで 300Mbps 程度の通信速度を実現できる．このように，屋内では携帯電話の代わりに無線 LAN によるネットワークを構成して，高速な通信を提供することができる．また，無線 LAN は従来静止した状態でデータ通信を行うことを目的としていたが，携帯電話のように移動しながらの音声通信に対応するために，様々な研究が行われている．しかし，無線 LAN は 1 つの AP（Access Point）でカバーできるエリアが小さいため，屋内でも複数の AP を設置する必要がある．そのため，ネットワークを構成するためには，AP 間を接続する LAN ケーブルの配線が必要であり，一度構築した後にレイアウトを変更する場合など，作業を困難にしてしまう．

そこで，無線 LAN のネットワークを容易に構築し，エリアを広げるシステムとして，無線メッシュネットワークに注目が集まっている．無線メッシュネットワークは AP（Access Point）間の接続を無線アドホックネットワークによって無線化し，各 AP に自律的に通信経路を形成する機能を持たせる．これにより，AP を適切に設置するだけで，ネットワークを拡大することができる．しかし，無線メッシュネットワーク上で音声通信を実現するには，端末が AP 間を移動する際のハンドオーバ手法など未解決の課題がある．

また，これらの無線ネットワークを基盤とする IP ネットワーク上で音声通話を行う技術を IP 電話もしくは VoIP（Voice over IP）と呼ぶ．IP 電話は，ブロードバンドの普及やバックボーンの整備により，安定した品質が保証されるようになり，急速に普及してきた．IP 電話は従来の音声通話だけでなく，アプリケーションと組み合わせることによって，様々な作業の効率化が期待されている．また，無線ネットワーク上に構築した IP 電話システムを内線として利用することで，携帯電話の利用に比べて通話費の削減も期待できる．しかし，ネットワーク上に FW[1] や NAT[2] が存在すると，外部のネットワーク上の端末から内部ネットワーク上の端末への呼び出しができないなどの課題がある．

上記のように，無線メッシュネットワークと IP 電話を組み合わせたシステムは，第四世代携帯電話に対して，互いに補完する関係と位置づけることができる．しかしながら，ハンドオーバや FW/NAT 越えなど様々な課題がある．本論文は，このような背景と要求から，無線メッシュネットワークと IP 電話を組み合わせたシステム VoWiMesh（Voice over Wireless Mesh Network）を想定し，実運用するために起きうる課題の解決方法を提案するものである．本論文で提案する無線メッシュネットワークの一実現方式を WAPL（Wireless Access Point Link）と呼ぶ．また， IP 電話を含む SIP[3] による通信が WAPL 内部と外部ネットワークで自由に行われるようにしたシステムを SoFW（SIP over Firewall）と呼ぶ．

[1]主に IEEE802.11 シリーズのこと指し，相互接続性認定の名称として WiFi と呼ばれることもあるが，本論文では無線 LAN の名称を使用する．

1.2 現在の無線通信技術と IP 電話

音声通信用およびデータ通信用として展開されている無線ネットワークには様々なものがある．現時点で，最も広範囲に展開されているのが W-CDMA や CDMA2000 など第三世代携帯電話のネットワークであり，日本では国内のほぼ全てのエリアを保証している．そして，ホットスポットや公衆 LAN などとして，空港，ホテルやレストランなど，無線 LAN による小さなエリアを保証する無線ネットワークが局所的に展開されている．また，後に第三世代携帯電話として追加されたモバイル WiMAX があり，それまでの第三世代携帯電話とは異なる特色を持っている．第三世代携帯電話よりも高速な通信を実現する第四世代携帯電話による無線ネットワークの研究も進んでいる．そして，これらの保証できないエリアを補完する技術として，無線メッシュネットワークの研究が行われている．

表 1.1 では特に各無線ネットワークに利用される電波や通信速度等の特性を示す．また，これらの無線ネットワークの概要を以下に詳しく説明する．モバイル WiMAX は第三世代携帯電話としても位置付けられるが，W-CDMA や CDMA2000 などの既に展開されている規格とは特徴が異なる．そのため，本論文では第三世代携帯電話とモバイル WiMAX は別に説明する．

(1) **第三世代携帯電話**

既に国内全域にネットワークが構築されており，ユーザ数も他の無線ネットワークに比べて最も多く，現在の日本の携帯電話の主力となっている．ITU の定める IMT-2000 規格に準拠しており，高速移動時で最大 144kbps，低速移動時で最大 384kbps，静止時で最大 2Mbps が規定されている．利用しているアクセス方式は NTT docomo の W-CDMA や，au の CDMA2000 など，通信業者ごとに異なる．基地局のセルは 2〜10km ごとに設置されており，都市部などではセルを小さく，過疎地などではセルを大きくして設置されている．周波数は 800MHz 帯，1.5GHz 帯，1.7GHz 帯，2GHz 帯を利用しており，屋内では電波が届きにくい場所もある．

(2) **第三・五世代携帯電話〜第三・九世代携帯電話**

第三世代携帯電話の通信速度を向上することに特化して W-CDMA や CDMA2000 などの規格を改良・発展させたもので，NTT docomo の利用している HSDPA や HSUPA，au の利用している EV-DO Rev.A などのアクセス方式が第三・五世代携帯電話と呼ばれている．現在では，都市部を中心にサービスエリアを拡大している状態である．

第三・九世代携帯電話は第四世代携帯電話への移行をスムーズにするための技術とされている．通信速度は，LTE と呼ばれる通信規格により，最大 250Mbps を実現する．また，音声通信などのオール IP 化や，無線 LAN や WiMAX などの異なる無線ネットワークとのシームレスな連携方法の検討も行われている．

表 1.1 各無線ネットワークに利用される電波や通信速度等の特性

	セル半径	通信速度	周波数*	特徴
第三世代 携帯電話	2〜10km	最大 2Mbps	800MHz 帯 1.5GHz 帯 1.7GHz 帯 2GHz 帯	広いエリアを カバーできる.
第三・五世代 携帯電話〜 第三・九世代 携帯電話	2〜10km	最大 100Mbps	800MHz 帯 1.5GHz 帯 1.7GHz 帯 2GHz 帯	第三世代携帯 電話と同様の. リソースで高速
第四世代 携帯電話	2〜10km	最大 1Gbps	3.5GHz 帯	非常に高速. 屋内には電波が 届きにくい.
WiMAX	2〜10km モバイル WiMAX では最大 1〜3km	最大 75Mbps モバイル WiMAX では最大 37Mbps	2.5GHz 帯 3.5GHz 帯 5.8GHz 帯	屋内には電波が 届きにくい.
無線 LAN	100m	最大 300Mbps	2.4GHz 帯 5GHz 帯	免許不要.
無線メッシュ ネットワーク	100m （ただし, AP の増設が容易）	ホップ数の増加 により減少. 最大は無線 LAN と同じ.	2.4GHz 帯 5GHz 帯	免許不要. ネットワークの 拡張が容易.

これらでは，周波数や周波数帯域幅などのリソースは第三世代携帯電話と同じものを利用するため，保証できるエリアなどの特徴は第三世代携帯電話と同様である．

(3) **第四世代携帯電話**

より高速なデータ通信を提供するために検討されている方式である．利用周波数はITUの世界無線通信会議（WRC07）において検討された結果，3.5GHz 帯を利用することになった．日本でも既存業務との問題がないとして同周波数帯を利用する．高い周波数帯を利用するため，エリアが狭くなり，屋内への電波も第三世代携帯電話に比べて届き難くなる．

通信速度では，1Gbps を目指しており，NTT docomo では，限定的な実験ではあるが，既に 5Gbps を実現している．無線 LAN，WiMAX，Bluetooth などの無線ネットワークとシームレスに連携することや IPv6 対応を目指している．また，端末の消費電力

も高くなるため，電源容量の確保も課題とされている．

(4) **WiMAX/モバイル WiMAX**

WiMAX は IEEE802.16-2004 と呼ばれる通信規格を利用した無線機器を指す．都市単位のエリアを保証する中距離無線ネットワークとして，携帯電話とは補完の関係に位置づけられている．基地局は 2km〜10km 間隔で設置され，通信速度はユーザが静止しているときで，最大 75Mbps を実現する．

移動通信用の規格はモバイル WiMAX（通信規格は IEEE802.16e）と呼ばれ，第三世代携帯電話の規格の 1 つ IMT-2000 OFDMA TDD WMAN として承認されている．基地局は 1〜3km 間隔で設置され，通信速度は 37Mbps 程度であり，120km/h の移動中でも使用可能である．

また，WiMAX 上で IP 電話を利用するシステムは VoWiMAX と呼ばれている．

(5) **無線 LAN**

IEEE802.11 の通信規格シリーズの総称である．1 つの基地局あたり 100m 程度の小さな範囲を保証し，IEEE802.11a や 11g では最大 54Mbps 程度の通信速度を実現する．MIMO 多重の技術を利用した IEEE802.11n では，最大 300Mbps 程度の通信速度を実現する．

住宅，オフィス，空港，ホテル，レストランなどで無線によるブロードバンドを提供する方法として利用されている．周波数は主に 2.4GHz 帯を利用しており，免許が不要な帯域である故に，他のシステムから発生する電波による干渉などを受けやすい．ラップトップ PC や携帯電話，デジタルカメラなどの家電製品にも搭載され，広く普及している．

無線 LAN 上で IP 電話を利用するシステムは VoWiFi と呼ばれている．

(6) **無線メッシュネットワーク**

無線 LAN の AP を無線アドホックネットワークの技術を用いて無線で接続する．AP どうしは自律的に経路を形成する機能を持っている．通信速度は最大で無線 LAN と同程度であるが，AP をホップするごとに通信速度が落ちる特徴がある．ただし，研究段階ではあるが，複数のチャネルを利用するなどして，ホップ数に関わらず，通信速度を維持する方法もある．

1 つの AP がカバーする範囲は無線 LAN と同様であるが，AP 間のケーブルを必要としないため，ケーブル設置のコストも掛からず，容易に無線ネットワークのエリアを広げることができる．そのため，オフィスなどでは，AP のレイアウトにも縛られることはない．コストが低いため，利用ユーザの少ない僻地などでもコストの回収が望める．災害時には優れた拡張性を利用して，早急な臨時インフラの形成に役立つこと

が期待されている．

無線 LAN だけでなく，別の無線ネットワークにも応用することもできる．例えば，WiMAX で無線メッシュネットワークを組めば，より広い範囲をカバーできる．

これらのネットワークの上では，携帯電話以外でもそれぞれ音声通信，もしくは他のリアルタイム通信を想定してパケットロスの発生しないハンドオーバや別のネットワークとのシームレスな連携などの研究が行われている．ハンドオーバでは，端末が基地局を移動する際に生じる通信断裂時間をできるだけ小さくする方法や，通信断裂時間に受信端末側の基地局に到達してしまうパケットをバッファリングしてパケットロスをなくす方法などが研究されている．異種ネットワーク間のシームレスな連携としては，異なるネットワークで最も品質の期待できるネットワークを選択する方法の研究などが行われている．

また，前述したように，携帯電話でも回線交換方式からオール IP 化へ移る傾向にあり，今後はどのネットワークでもパケット交換方式の IP 電話を利用すると考えられる．オール IP 化により，携帯電話も IP 電話化し，他の無線ネットワークシステムとの親和性が向上する．また，ISP などが提供するネットワークでは SIP と呼ばれるシグナリングプロトコルが使われている．SIP は音声通信以外にも様々なマルチメディア通信に応用できると期待されており，テキスト形式でメッセージをやり取りするため拡張性も優れている．SIP は IETF によって標準化されたプロトコルであるため，業者間で互換性が取れる．そのため，これらの無線ネットワーク上で利用する IP 電話は SIP を使うことを想定して，研究・展開がされており，今後はより一層，各種無線通信どうしの親和性が高まると考えられる．

表 1.2 各条件に対する無線ネットワークの評価

			第三世代携帯電話	第四世代携帯電話	WiMAX	無線 LAN	無線メッシュネットワーク
音声通信	屋外広域		◎	◎	○	△	△
	屋内	内-外	○	△	△	○	◎
		内-内	△	△	△	○	◎
データ通信	屋外広域		○	◎	◎	△	△
	屋内	内-外	△	△	△	◎	◎
		内-内	△	△	△	◎	◎
災害地			○	○	○	△	◎
僻地			○	○	○	△	◎

1.3 VoWiMesh の位置づけ

提案システムである VoWiMesh と他の無線ネットワークとの位置づけを示す．無線ネットワークの適用エリアとして，現在の携帯電話が担う広域，屋内における外線と内線，災害地や僻地などにわけられる．これらの適応エリアごとに各無線ネットワークの適合性を検証していく．

適合性を示すにあたって，音声通信に要求される性質とデータ通信に要求される性質では異なる箇所がある．ファイル転送などのデータ通信では，高速なパケット転送が要求される代わり，ある程度のパケット到達時間の揺らぎやパケットロスなどは，TCP などの端末間の制御によって補われるため許される．音声通信は 64kbps 程度の帯域しか使わないが，インフラ自体にリアルタイム性と品質が要求される．そのため，屋外広域と屋内については音声通信の視点からの位置づけと，データ通信の視点からの位置づけに分けて説明する．

また，これまでの携帯電話では課金制度が従量制であることが多く，インターネットプロバイダを利用した定額低価格な IP 電話が顧客確保の面において，今後有利になるといわれてきた．しかし，現在では，携帯電話事業者もこれらのプロバイダの価格に引けを取らないよう，パケット通信や音声通話の定額低価格化の努力を行っている．そのため，本論文では，携帯電話業者とインターネットプロバイダの通信料金の差については評価から省く．表 1.2 に各条件に対する無線ネットワークの評価を示し，次に詳しく説明する．

1.3.1 音声通信の視点からの各無線ネットワークの適合性

(1) **屋外広域**

広域の無線ネットワークでは携帯電話の利用が適していると考えられる．既に全国でサービスを展開している携帯電話は堅実なシステム構築がなされており，屋外では品

質や接続性において高い信頼性を持つ．そのため，リアルタイム性が要求される音声通信では他の無線ネットワークよりも信頼ができる．また，接続性を保証できる要因として基地局の伝送距離が大きいという理由が挙げられる．1 つの基地局で広いエリアをカバーできるため，見晴らしが良ければ電波の届かない場所が発生する可能性は少ない．これに対して，VoWiFi や VoWiMesh は AP ひとつのセルが 100m 程度と小さく，全てのエリアに電波がいきわたらない場合が生じる．

(2) **屋内**

- **屋内の端末と外部の端末の音声通信**
  屋内に構築されている内部ネットワークに接続している端末と外部ネットワークに接続している端末が音声通信を行う場合，屋内に VoWiMesh や VoWiFi を構築し外部に接続する方法，屋外の第三世代携帯電話の基地局に接続する方法が適している．第四世代携帯電話と VoWiMAX では屋内に電波が届きにくい．また，第三世代携帯電話でも，屋内では電波の届きにくい場所が発生する場合がある（特に地下など）．ただし，携帯電話や WiMAX では中継アンテナを設置する方法もあるが，VoWiMesh や VoWiFi は免許などの問題もなく，手軽に構築できる．さらに構築の自由度で比較すると，屋内の外線用電話では VoWiMesh が適していると考えられる．
- **屋内の端末どうしの音声通信**
  外部から提供されるネットワークを利用すると，コストや電波資源を無駄に消費してしまう．そのため，VoWiMesh や VoWiFi を内部ネットワークとして構築し，利用することが最適といえる．さらに，音声通信では高速な通信速度は要求されないため，屋内で容易に内部ネットワークを構築できる VoWiMesh が適していると考えられる．

1.3.2 データ通信の視点からの各無線ネットワークの適合性

(1) **屋外広域**

第三世代携帯電話，第四世代携帯電話，WiMAX から，そのときの通信速度が最も速いものを選択する方法が適していると考えられる．この場合，通信速度の速さは，第四世代携帯電話，WiMAX，第三世代携帯電話の順になるが，利用しているユーザの数やセルの大きさなどによって通信速度が変わる．最適無線ネットワークの選択方法については現在様々な研究機関などで研究が行われている．複数の無線ネットワークを選択することで電波資源の分散にもなる．

また，前述したように，無線 LAN や無線メッシュネットワークによる接続性を広域で保証することは困難といえる．

(2) **屋内**

- **屋内の端末と外部の端末の通信**
  第四世代携帯電話，WiMAX は電波が屋内に届きにくいため，内部に無線 LAN や無線メッシュネットワークを構築し，インターネットを経由して利用する方法が適しているといえる．第三世代携帯電話は比較的屋内にも届き易いが，他の無線ネットワークと比べると通信速度において劣る．

  無線 LAN と無線メッシュネットワークは通信速度と AP 設置自由度の関係がトレードオフになるため，評価は同等とした．ただし，前述したように，今後，無線メッシュネットワークはホップ数に関わらず通信速度を維持できるよう研究が進んでいる．

- **屋内の端末どうしの通信**
  無線 LAN や無線メッシュネットワークなどの内部に構築したネットワークを利用して通信することが適しているといえる．外部のネットワークを経由する必要がないため，通信速度は十分速く，電波資源も節約できる．

1.3.3 災害地

災害時には基地局を接続するケーブルが断裂することや，基地局自体が破壊される可能性がある．無線メッシュネットワークでは，素早く無線ネットワークの構築ができる．また，レスキュー隊や災害用救助ロボットなどと連携し，AP を適切に配置することで，電波の届きにくい場所にでも，ネットワークを提供できる．

1.3.4 僻地

無線メッシュネットワークが適しているといえる．第三世代携帯電話，第四世代携帯電話，WiMAX でもサービスを提供することは可能であるが，ケーブル設置のコストを回収できないため，ネットワークの提供が難しい場合がある．無線メッシュネットワークはケーブル設置の費用がかからないため，比較的低コストで無線ネットワークを提供できる．また，1 つの AP あたりのセルの大きさを補うため，WiMAX に無線メッシュネットワークの技術を応用する方法も考えられる．

1.3.5 適応エリアのまとめ

それぞれの適合性を検証した結果から，各無線ネットワークの適応エリアを図 1.1 に示す．広域は第四世代携帯電話，第三世代携帯電話，WiMAX によって保証し，データ通信では主に第四世代携帯電話，WiMAX が利用される．屋内では無線メッシュネットワークおよび無

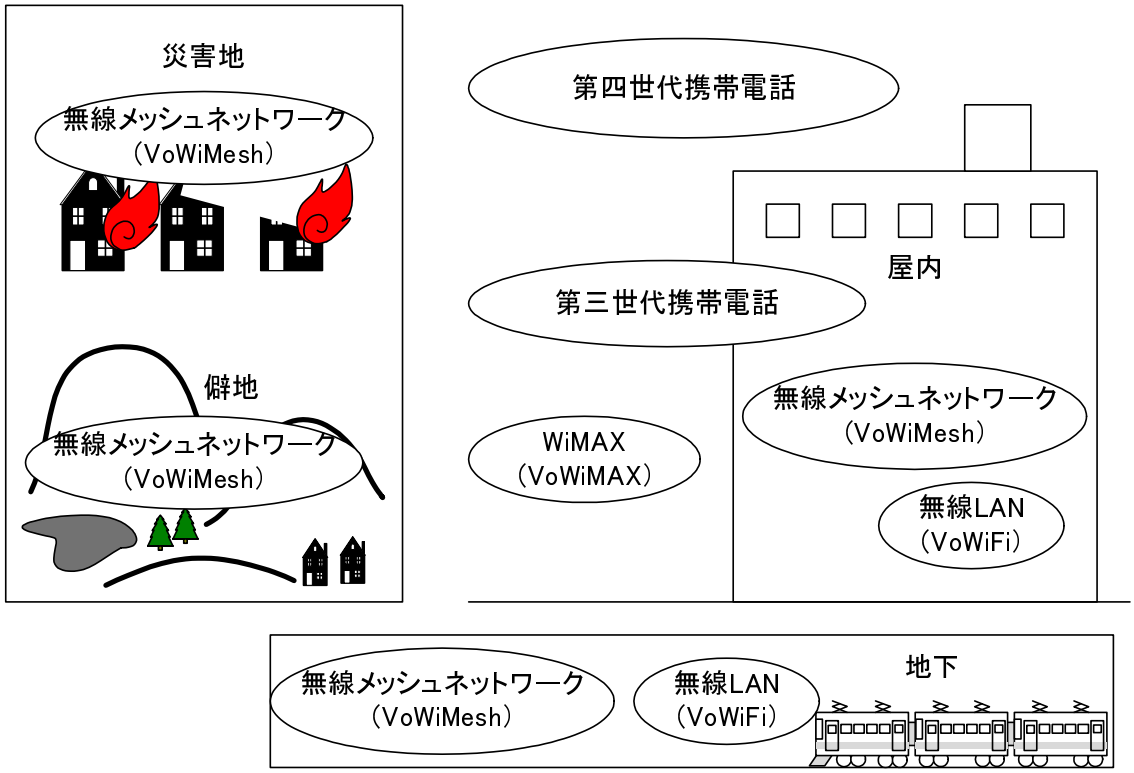

図 1.1 各無線ネットワークの適応エリア

線 LAN によるネットワークを構築する．また，災害地や僻地などでは無線メッシュネットワークを構築する．以上より，無線メッシュネットワークおよび VoWiMesh は携帯電話など他の無線ネットワークに対して，屋内，災害地，僻地などのエリアで効果を発揮できるといえる．

1.4 VoWiMesh に要求される機能と既存技術の課題

本論文では VoWiMesh を運用する上で，発生する課題を解決するための提案を行う．VoWiMesh に要求される技術の 1 つとしてパケットロスのないハンドオーバが挙げられる．無線メッシュネットワークでは，ハンドオーバ時に発生する制御メッセージが消失する可能性が高いため，ハンドオーバに失敗する場合がある．また，既存の無線メッシュネットワークではルーティングプロトコルが固定されているが，自由に変更できると有用である．

次に，通信速度を向上するために，データパケットの経路を最適化し，ネットワークリソースを有効利用する技術も必要となる．また，無線メッシュネットワークと他のネットワークとの間には，NAT や FW が設置されている環境も考えられるため，これらに対応する必要がある．

以下では，これらの要求と既存技術の課題ついて詳しく説明する．

(1) **ハンドオーバ**

端末が通信を行いながら，現在の AP から別の AP へ移動する際に，パケットロスすることなくスムーズに移動することが要求される．パケットロスを防ぐ方法は大きく 2 つに分けられ，1 つは端末が移動する際に発生する，どの AP にも所属していない時間（通信の断裂時間）をできるだけ小さくする方法，もう 1 つは移動によって通信が断裂した間に転送されたパケットをどこかでバッファリングし，端末が新しい AP に移動した際にバッファリングしたパケットを転送する方法である．

通信の断裂時間を小さくする方法は，様々な研究機関で研究されており，基本的に AP と端末間の問題であるため，既存の方式がそのまま無線メッシュネットワークに応用できる．無線メッシュネットワーク特有の問題としては，バッファリング開放時の AP 間メッセージが消失しやすいという問題がある．

無線メッシュネットワークの標準化が行われている IEEE802.11s では，ハンドオーバの方式については未検討の状態であり，別途 IEEE802.11F，IEEE802.11r および IEEE802.21 にて検討されている方式を利用する．しかし，これらの方式は AP 間を有線で接続していることが前提である．無線メッシュネットワークでは，ハンドオーバ時にやり取りされる AP 間メッセージがフラッディングされる．無線アドホックネットワークにおけるフラッディングは信頼性が低く，ハンドオーバに失敗する可能性があるという課題がある．

既存技術である iMesh[4] では，ハンドオーバが発生したときにそのことを検出した移動先の AP がフラッディングにより周辺の AP に情報を通知し，さらに移動前の AP が必要なデータパケットをバッファリングしておくことによりパケットが消失しないように制御する．このように iMesh でもフラッディングを用いるため，ハンドオーバに失敗する可能性がある．

以上から，ハンドオーバ時に発生するメッセージを確実にパケットの送信元 AP と移動前の AP に転送する方法が必要となる．

(2) **ルーティングプロトコルとの独立**

IEEE802.11s，iMesh など既存の無線メッシュネットワークではルーティングプロトコルが 1 つまたは少数に固定されている．将来，IETF のワークグループである MANET（Mobile Ad-hoc Network）[5] において，優秀なルーティングプロトコルが実現された場合やプロトコルがバージョンアップした場合，これらの機能を無線メッシュネットワークに適用するには，再度，システムを作りこむ必要がある．そのため，無線メッシュネットワークの機能をルーティングプロトコルと独立する方法が必要となる．

(3) **ネットワークリソースの有効利用**

無線メッシュネットワークでは，AP を複数ホップすると通信速度が下がってしまうなどの課題がある．そのため，最適化された経路を選択する技術が必要である．

無線メッシュネットワークを実際に運用する場合，インターネットなど外部ネットワークとの通信が頻繁に行われることが想定され，有線との境界に設置される GW 近傍の帯域がボトルネックとなる可能性がある．

[6]〜[8] では，無線メッシュネットワークと外部ネットワークの間に複数の GW を設置し，AP からできるだけホップ数の少ない GW を利用する．しかし，この手法では端末の分布が特定の GW 近傍に集中すると，その GW が帯域を使い切る一方で，他の GW は帯域を余らせてしまう．

また，既存方式である MGA（Multi Gateway Association）[9] では，1 つの AP から複数の GW に接続し，トラヒックを分散する．この方式では，AP は端末からパケットを受けとった際，各 GW に対する適切な転送比率を計算し，それに従って，パケットごとに異なる GW へ転送する．しかし，同一セッションのパケットが複数の GW に分かれるために，各経路の遅延時間の違いによって揺らぎが生じ，TCP 通信のスループットを大きく低下させてしまうという課題がある．

そのため，このような GW 選択手法の課題を解決し，ネットワークリソースを有効利用できる方法が要求される．

(4) **FW/NAT 越え**

VoWiMesh では音声通話の呼制御プロトコルとして SIP を利用する．無線メッシュネットワークと外部ネットワークの間には FW や NAT が設置されている可能性がある．

ここで，SIP は呼設定開始時に相手端末の IP アドレスが特定できるか，相手端末の属する SIP サーバの IP アドレスが特定できることが必須である．そのため，NAT が介在するような環境では呼設定を開始できない．また，企業などの FW は多くの場合，

メールや内部から外部へのWebサーバアクセスなどに通信を限定しており，それ以外の通信を遮断してしまう．このような制限を受けたネットワークにIP電話を導入し，外部との通話に利用しようとすると，企業のセキュリティポリシの変更が必要になり，FWの設定変更の稼動やセキュリティ上のリスクが増加する．

文献[7]では，FWがSIPによる呼設定を監視し，その呼設定によって開始される音声通信のみを許可するようにフィルタ処理を動的に変更する．しかし，音声通信では不特定多数のIPアドレスとポート番号を使ったUDPの通信が利用されるため，企業などによってはセキュリティポリシの変更が必要となる．また，FWへのモジュール追加や新規のVoIP専用GW設置が必要とされるため，導入には手間がかかる．HCAP[11]やSkype[12]では，FWの外側に設置された中継サーバと電話端末間でHTTPトンネルを張ることにより，Webを閲覧できる環境であればIP電話による通話が可能になる．しかし，端末に特殊な機能が必要なため，企業ネットワークに導入するにはIP電話端末の総入替えが必要である．

そのため，FW/NATのルールを変更したり，装置を入れ替えたりすることなく，かつ，既存のIP電話端末を使ってFW/NAT越えを実現する方法が要求される．

1.5 提案システムの概要

以下に提案の概要を述べる．提案の骨子は以下の通りである．

提案 (1) 無線メッシュネットワーク“ WAPL ”の提案

提案 (2) 無線メッシュネットワークにおける GW 分散方式の提案

提案 (3) FW や NAT を通過できる IP 電話システムの提案

提案 (1)(2) は無線メッシュネットワークのアーキテクチャと経路生成に関する提案である．提案 (1) はシームレスハンドオーバとルーティングプロトコルとの独立の課題を解決し，提案 (2) は GW 分散の課題を解決する．提案 (3) は FW/NAT を通過させるために，ネットワーク上に設置する特殊な 2 台の装置に関する提案である．

1.5.1 WAPL の提案

図 1.2 に WAPL の概要を示す．WAPL では無線化した AP を WAP（Wireless Access Point）と呼ぶ．WAP 間の接続は MANET のルーティングプロトコルを使用する．WAPL では端末が通信を開始する際に，オンデマンドで WAP と端末の対応情報を取得する．この取得した対応情報は，LT（Link Table）と呼ぶ独自のテーブルに保持する．WAP は端末からの ARP 要求を受信すると，他の WAP へ LT 生成要求メッセージをフラッディングにより広告する．LT 生成要求メッセージには探索端末の IP アドレス，送信元端末の IP アドレスなどの情報が記載されている．LT 生成要求メッセージを受信した全 WAP は自身の LT にこれらの対応関係を記述する．配下に目的の端末が存在することを検出した WAP は，ユニキャストで送信元 WAP に LT 応答メッセージを返し，送信元 WAP は LT 応答メッセージを受信すると宛先端末と WAP の IP アドレスの関係を LT に記述する．以上の動作により，送信元 WAP には宛先 WAP と宛先端末の情報の対応関係が記録される．これらの処理をルーティングプロトコルの上位レイヤに実装する．これにより，ルーティングプロトコルは既存のどの方式を利用しても WAPL の動作自体には影響を与えない．

WAPL では端末移動時のハンドオーバ通知を確実に行うために，新（移動後）WAP から旧（移動前）WAP と送信元 WAP に対してフラッディングではなく，ユニキャストでハンドオーバを通知する．これを可能とするためには，新 WAP は端末が WAP 間をどのように移動したかを知っている必要がある．そこで，各 WAP では予め近隣で通信中の端末の IP アドレスおよび MAC アドレスと WAP の IP アドレスを関連付けるテーブルを作成しておく．このテーブルを近隣通信テーブルと呼ぶ．近隣通信の把握方法を図 1.3 に示す．WAP はプロミスキャスモードで近隣の WAP が送信する通信パケットを常時モニタする．WAP は自身宛以外のパケットの IP ヘッダから宛先 WAP，送信元 WAP の IP アドレスを，カプセル化された MAC ヘッダと IP ヘッダから宛先端末，送信元端末の MAC アドレスと IP アドレスを取得し，それらを近隣通信テーブルに記録する．

端末が移動し，ハンドオーバが発生した際，端末が移動したことを知った旧 WAP は送信元 AP から転送されてくるパケットのバッファリングを開始する．新 WAP は端末から移動してきたことを知ると，端末の MAC アドレスから近隣通信テーブルを参照し，移動してきた端末の情報が存在すれば通信中であると判断し，ハンドオーバ処理を開始する．このとき，近隣通信テーブルから端末の旧 WAP と送信元 WAP の IP アドレスを参照し，旧 WAP にはパケット解放要求メッセージ，送信元 WAP には経路更新要求メッセージをユニキャストで送信する．旧 WAP と送信元 WAP は受信したメッセージに対して応答メッセージを返す．旧 WAP はパケット解放メッセージを受け取るとバッファリングしていたパケットを新 WAP に転送する．送信元 WAP は経路更新要求メッセージを受け取ると LT を書き換えることによりパケットの経路を更新し，ハンドオーバが完了する．制御メッセージをユニキャストで通知するため，パケット到達の信頼性が高く，通信相手を特定しているため再送制御も可能である．

パケットロスのないシームレスハンドオーバの提案の詳細と評価は第 2 章で述べる．

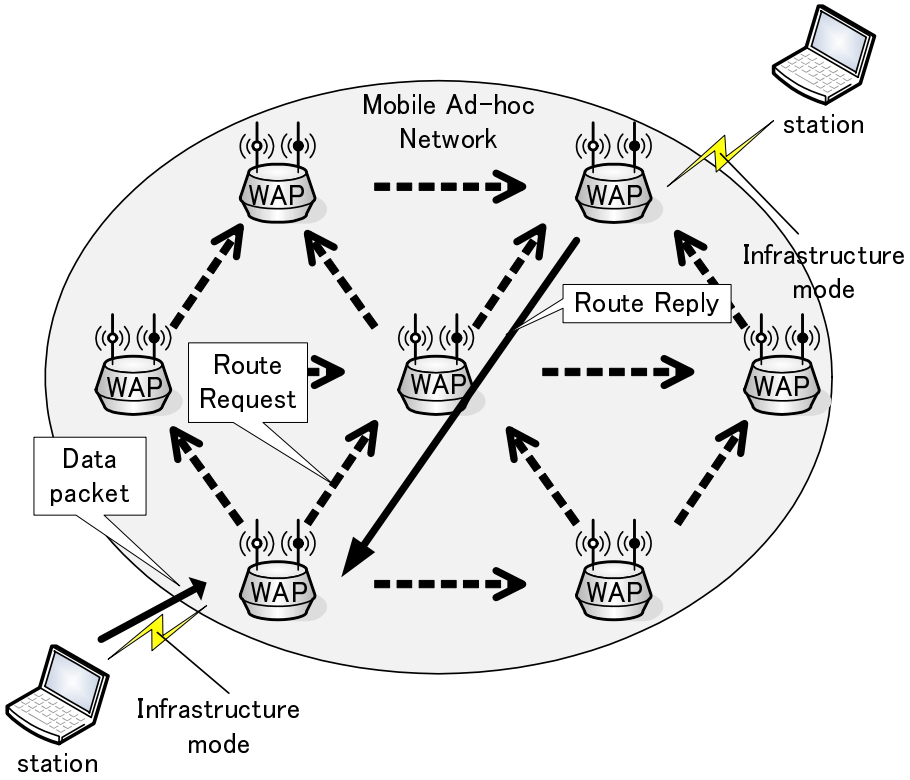

図 1.2 WAPL の概要

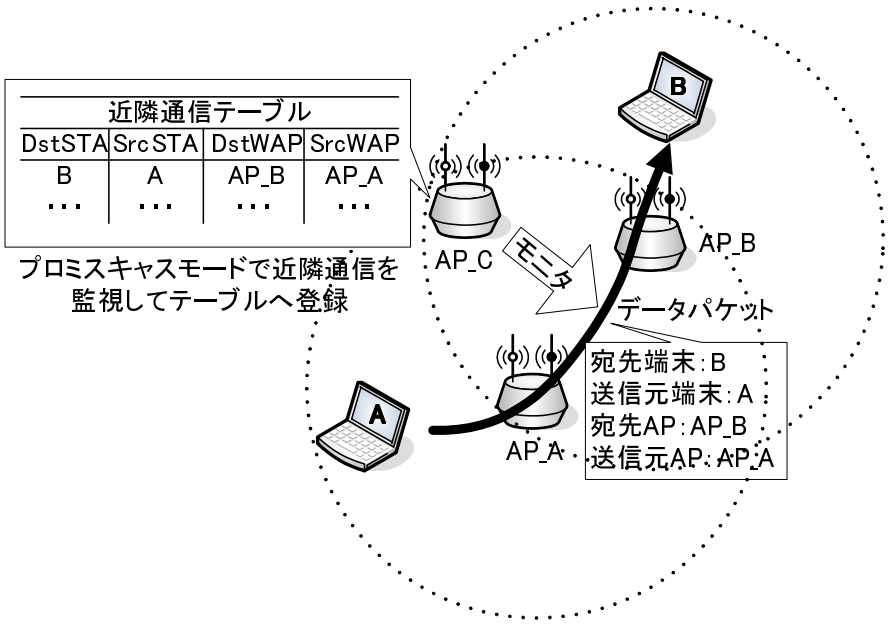

図 1.3 近隣通信の把握方法

1.5.2 GW 選択方式の提案

WAPL ではインターネットなどの外部ネットワークに接続された端末と通信する際は，GW へのトラヒック集中を避けるため，複数 GW 選択方式を利用する．さらに，既存のパケット単位で複数 GW に分配する方式に対して，セッション単位で分配する方式を提案する．パケット単位の分配では各 GW にパケットが到達する際のゆらぎによって，TCP 通信によるスループットを低下させてしまう．そこで，セッション単位で分配することによって，同一セッション内のパケット到達時間のゆらぎを避け，TCP 通信によるスループットを改善する．以後，提案方式をセッション分配方式と呼ぶ．

インターネットと接続した際の WAPL の全体図を図 1.4 に示す．インターネットと接続するため，有線部と接続する WAP を GWAP（GatewayWAP），パケットを集約して外部ネットワークと接続する GWAP を MGWAP（Master GWAP）と呼ぶ．外部との通信は必ず MGWAP を経由する．GWAP と MGWAP 間の通信は有線で接続し，この間の通信はボトルネックになることはないものとする．MGWAP は GWAP の機能を包含する．

GWAP および MGWAP は常に自身の近傍，つまり無線範囲内の一定時間内におけるトラヒックの量を測定する．GWAP および MGWAP はこのようにして得たトラヒック情報を定期的にフラッディングする．このトラヒック情報を送信するメッセージにはホップカウントを記述する項目が含まれており，ホップカウントは各 WAP を中継する毎に値が加算される．このメッセージにより，各 WAP はシステム内に複数存在する GWAP および MGWAP の近傍のトラヒック状況と GWAP および MGWAP までのホップ数を把握する．

セッション分配方式の概要を図 1.5 に示す．WAP は端末からパケットを受け取ると，パケットの宛先 IP アドレスのネットワーク部が外部ネットワークを示す場合，その時点で保持している各 GWAP の近傍トラヒックとホップ数から，スループット期待値を計算し，その値が最も高い GWAP を最適 GWAP として 1 台だけ選択する．同時に，セッションと最適 GWAP の関係を記憶し，以後の同一セッションのパケットは同一の GWAP に転送する．同一セッションとはコネクション ID（送信元 IP アドレス，宛先 IP アドレス，プロトコル番号，送信元ポート番号，宛先ポート番号）が同一のトラヒックを指す．GWAP は受信したパケットを MGWAP へ転送する．MGWAP はセッションと転送元の GWAP の関係を記憶するとともに，パケットを外部ネットワークの端末に転送する．また，外部ネットワークからのパケットは一度，WAPL の代表 GW である MGWAP へ転送される．外部ネットワークからのパケットは MGWAP が記憶された内容に従って転送することにより，適切な GWAP を介して宛先端末の所属する WAP へ転送される．このようにして，同一セッションの往復は同一経路を通ることができる．別のセッションが開始される場合は，その時点での最適 GWAP が新たに選択される．

GW 選択方式の提案の詳細と評価は第 3 章で述べる．

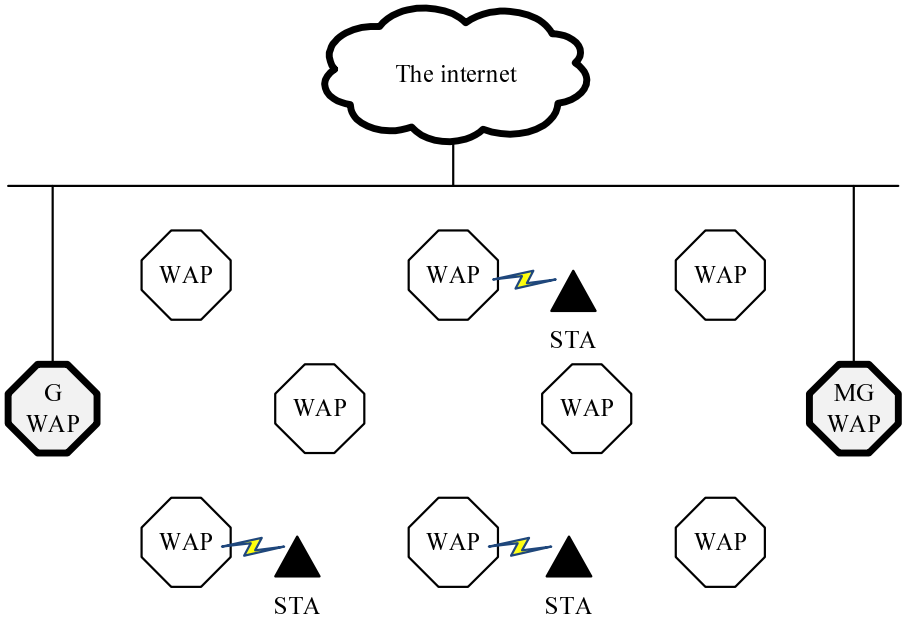

図 1.4 インターネット接続時の WAPL の全体図

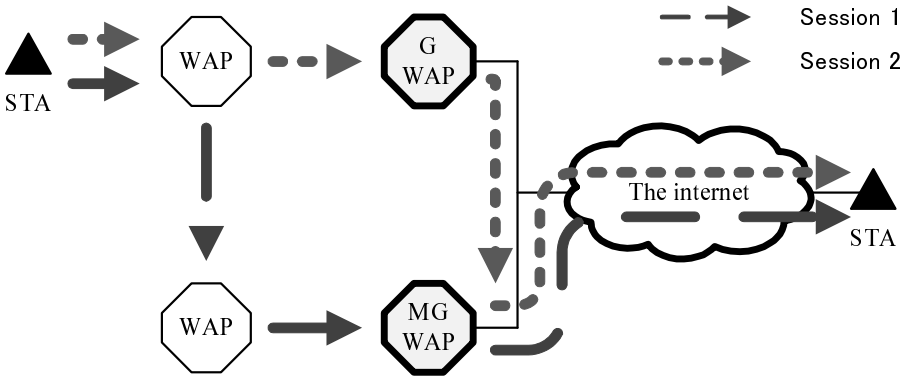

図 1.5 セッション分配方式の概要

1.5.3 FW/NAT を通過できる IP 電話システムの提案

SoFW の構成を図 1.6 に示す．SoFW では SIP サーバの代わりに内部のプライベートアドレス環境上に HRAC（Half Relay Agent Client），外部のグローバルアドレス環境上に SIP サーバ機能を備えた HRAS（Half Relay Agent Server）を設置する．システム立ち上げ時において，HRAS と HRAC は SIP メッセージと音声ストリームを中継するための HTTP トンネルを生成する．呼設定時において HRAS および HRAC は SIP 端末からグローバル IP アドレスとプライベート IP アドレスのインタフェースを持つ仮想的な一つの SIP サーバのように見える．SoFW では，端末とは独立して HTTP トンネルを設置するため，既存の SIP 端末をそのまま利用することができる．

システム起動時から通話終了までのシーケンスを図 1.7 に示す．システムを起動すると HRAS と HRAC は 2 点間でトンネル生成を行う．HRAC は HRAS に対して HTTP に準拠する GET リクエストと POST リクエストメッセージを送信する．HRAS は GET リクエストを受け取ると 200OK レスポンスのヘッダ部を返す．この後，HRAS と HRAC は端末から SIP メッセージが送信されるまで TCP コネクションを維持したまま待機する．以降，SIP メッセージまたは音声ストリームを受信すると HTTP のボディ部としてこれらを中継することができる．内部の SIP 端末は自身の情報を HRAS の SIP サーバに登録するため REGISTER リクエストを HRAC に送信する．HRAC は HTTP トンネルを介してリクエストを HRAS に中継し，HRAS から返信される 200OK レスポンスを内部 SIP 端末に返す．上記処理により外部 SIP 端末からの通話開始ネゴシエーションが可能となる．外部 SIP 端末は INVITE リクエストを HRAS の SIP サーバ宛に送信する．HRAS の SIP サーバは内部 SIP 端末を特定し HTTP トンネルを介して端末に INVITE リクエストを転送し，以降は同様にして SIP メッセージのやり取りを行う．また，INVITE，200OK メッセージを中継する際には，SIP のメッセージボディ（SDP）を HRAS/HRAC が書き換え，以後，エンド端末に対して通信相手が HRAS/HRAC であるように見えるようにする．この理由は，SIP 対応の音声端末では，呼設定後の音声通信は SIP サーバを介さずにエンドツーエンドで実行するためである．すなわち，音声ストリームをエンド端末宛てでなく，HRAS/HRAC に向けて誘導する必要がある．これらの呼設定のネゴシエーションが終わると音声通信が開始される．音声ストリームは，外部端末は HRAS へ，内部端末は HRAC へ送信し続ける．HTTP トンネルはその音声ストリームを対応する端末へ中継する．このとき，HRAS/HRAC は SIP メッセージを中継する際に得た情報から音声ストリームのグローバル IP アドレスとプライベート IP アドレスおよびそれらのポート番号を変換して音声ストリームを中継する．最後に通話終了ネゴシエーションはフックオンを告げる BYE メッセージと確認応答 ACK が HTTP トンネルによって中継され，通話が終了する．

FW/NAT を通過できる IP 電話システムの提案の詳細と評価は第 4 章で述べる．

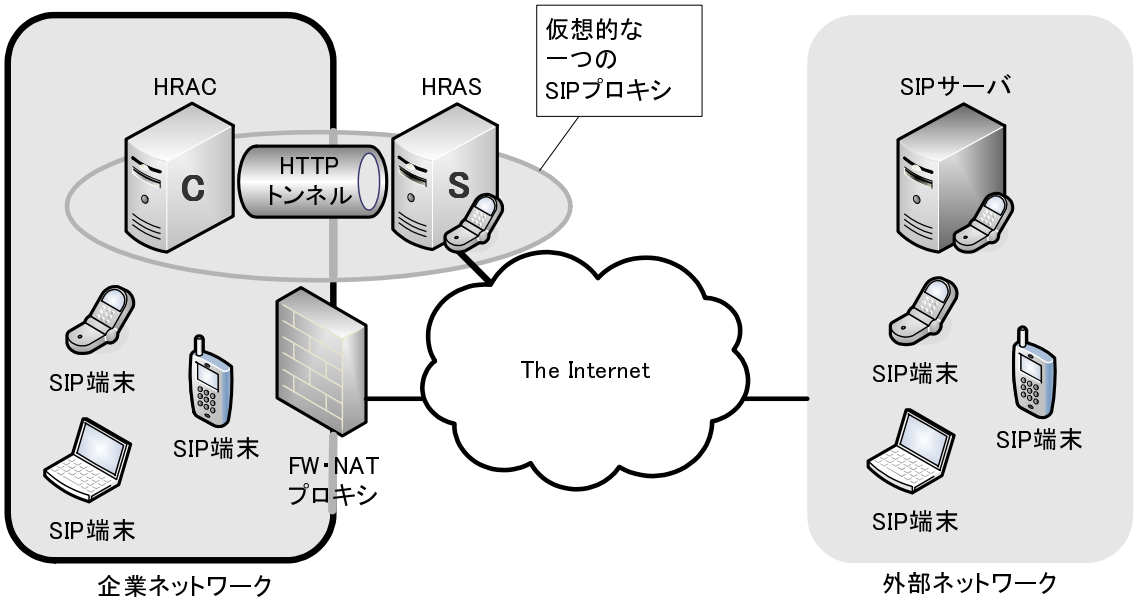

図 1.6 SoFW の構成

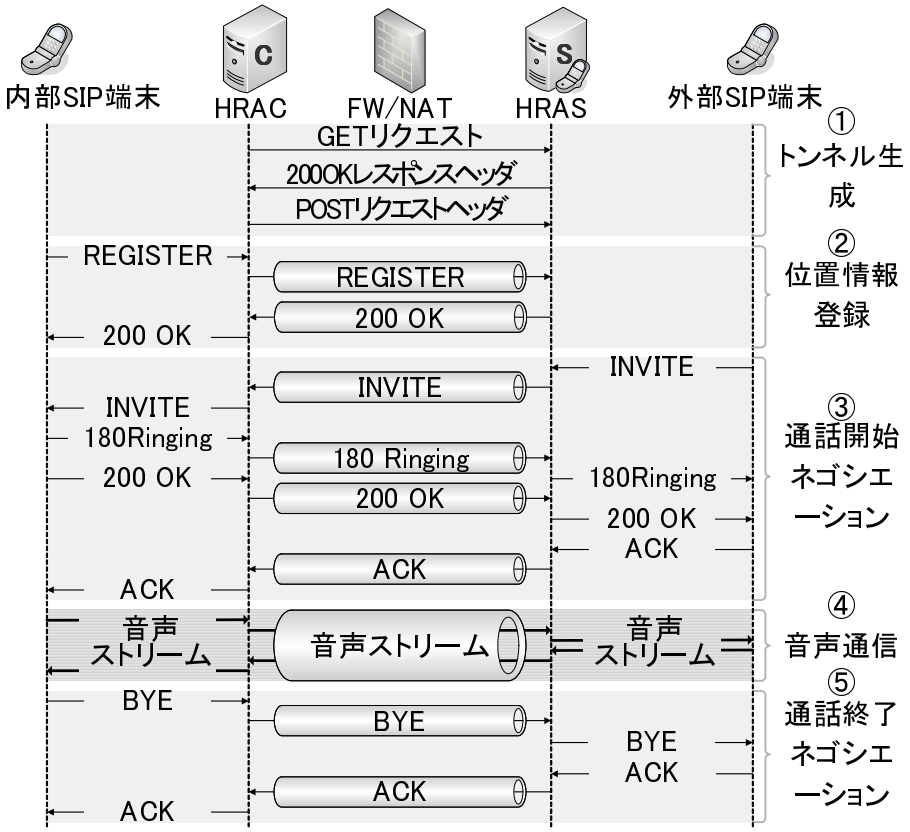

図 1.7 システム起動から通信終了までのシーケンス

1.6　論文の構成と本研究の効果

1.6.1　本論文の構成

本論文は図 1.8 に示すような構成からなる．第 1 章は本論文全体の概要について述べている．第 2 章と第 3 章は，無線メッシュネットワークのアーキテクチャおよび経路生成の視点からの研究であり，パケットロスのないハンドオーバ，ルーティングプロトコルの独立と GW 選択方式を提案する．第 4 章は IP 電話システムの視点からの研究であり，IP 電話が FW/NAT を通過するための特殊な装置を提案する．

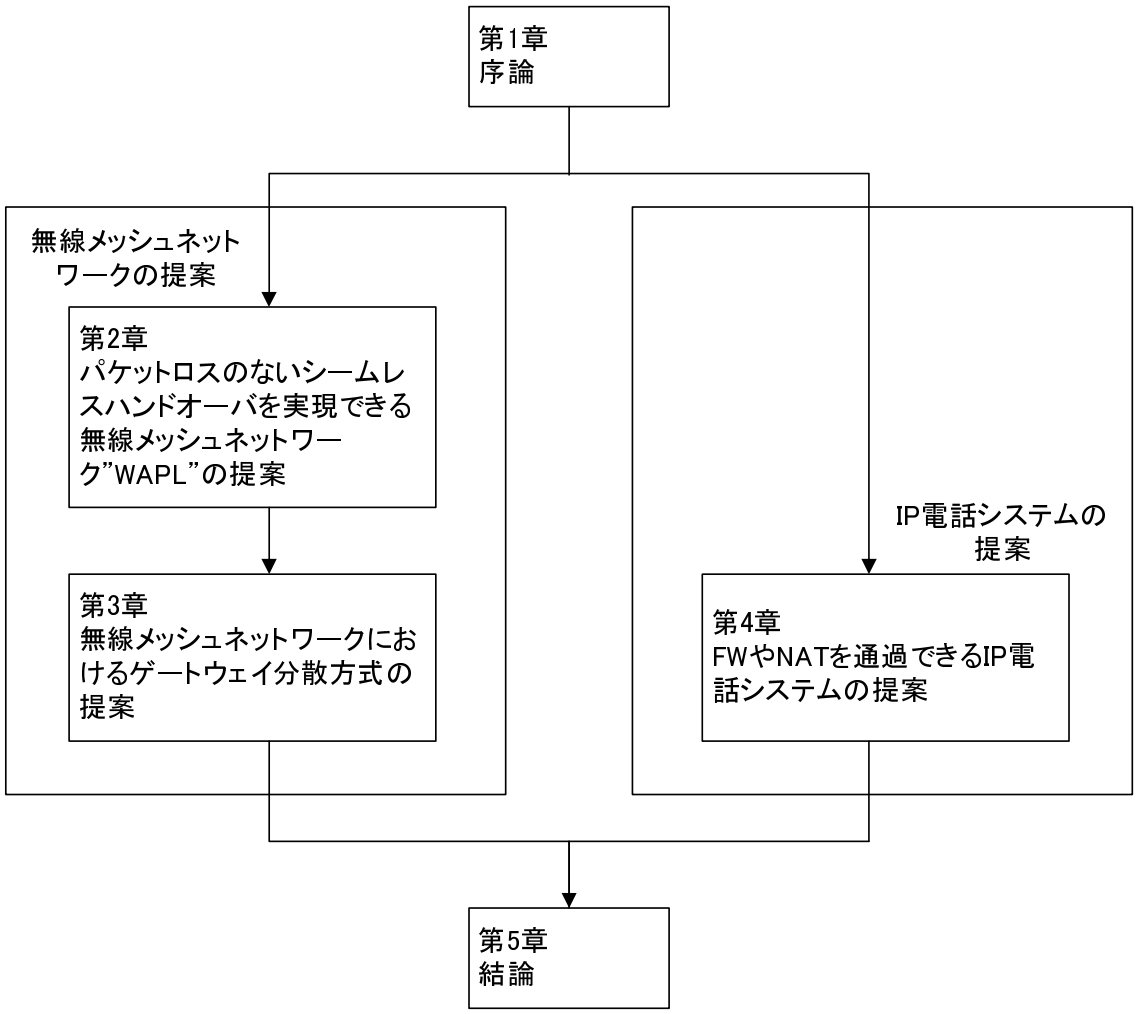

図 1.8　本論文の構成

1.6.2 本論文の効果

第 2 章，第 3 章，第 4 章における目的，従来技術の課題，提案方式の概要，効果について表 1.3 にまとめる．

表 1.3 本研究の効果

2 章	目的	・ 無線メッシュネットワークにおいてパケットロスのないハンドオーバを実現する．
	既存技術の課題	・ ハンドオーバ時のメッセージがフラッディングされる際にロスしやすい． ・ 制御メッセージによるトラヒックが膨大になる． ・ ルーティングプロトコルが固定されている．
	提案方式	・ WAP に近隣のパケットを監視する機能を追加． ・ 監視した情報により，メッセージをユニキャストで送信する． ・ オンデマンドに制御メッセージの交換を行う． ・ MANET の技術と無線メッシュネットワークの技術を分離． ・ ルーティングプロトコルの自由な選択が可能
	効果	・ ハンドオーバの失敗がない． ・ 制御メッセージによるトラヒックが少ない． ・ MANET のプロトコルを何でも容易に無線メッシュネットワークに適応できる．
3 章	目的	・ GW を効率的に利用する．
	既存技術の課題	・ 1 つの GW にトラヒックが集中しやすい． ・ パケット単位で分配すると，TCP スループットの低下を招く．
	提案方式	・ セッション単位で複数の GW にパケットを分配する．
	効果	・ TCP スループットを低下させずに，複数の GW を有効利用することができる．
4 章	目的	・ IP 電話に FW や NAT を通過させる．
	既存技術の課題	・ FW や NAT の装置自体を取り替える必要がある． ・ 特殊な端末を利用するため，従来の SIP 端末を取り替える必要がある．
	提案方式	・ 2 台の特殊な装置（HRAS/HRAC）をグローバルネットワーク側とプライベートネットワーク側に設置し，HTTP トンネルを生成する． ・ 端末からの SIP メッセージの内容を HRAS/HRAC で修正し，音声通信を HRAS/HRAC 経由にする．
	効果	・ HRAS/HRAC の 2 台を接続するだけで，既存の SIP 端末が FW や NAT を越えて外部の端末と通話できる．

1.6.3 システムの要求仕様と提案方式の関係

無線メッシュネットワークとして，既存技術（IEEE802.11s，iMesh，MGA）および提案方式の WAPL と要求仕様の関係を表 1.4 に示す．FW/NAT 越え IP 電話システムとして，既存技術（文献 [6] の方式，HCAP，Skype）と提案方式の SoFW の関係を表 1.5 に示す．

表中の結果の詳細は以下の通りである．

表 1.4 無線メッシュネットワークにおける要求仕様の関係

	IEEE802.11s	iMesh	MGA	WAPL
ハンドオーバ時のパケットロス	×	△	×	○
ルーティングプロトコル切換え	×	×	×	○
制御メッセージのトラヒック	○	○	×	△
GW 選択	×	×	△	○

表 1.5 FW/NAT 越え IP 電話システムにおける要求仕様の関係

	文献 [6] の方式	HCAP	Skype	SoFW
FW/NAT への依存	×	○	○	○
端末への依存	○	×	×	○

(1) **無線メッシュネットワークにおける要求仕様の関係**

- **ハンドオーバ時のパケットロス**

  IEEE802.11s，MGA ではハンドオーバについては考慮されていない．iMesh ではバッファリングによって通信断裂時のパケットロスをなくそうとするが，制御メッセージの損失によってハンドオーバが失敗する可能性がある．WAPL では制御メッセージの到達の確実性を向上させることで確実にパケットロスのないハンドオーバが成功する．

- **ルーティングプロトコルの切換え**

  WAPL 以外のシステムではすべて，ルーティングプロトコルを 1 つまたは少数に固定している．WAPL はルーティングプロトコルと独立しているため，MANET のルーティング技術を自由に適用できる．

- **制御メッセージのトラヒック**

  iMesh では移動時に制御メッセージをフラッディングするため，トラヒックに負荷を与える．WAPL はルーティングプロトコルが独立しているため，通信開始時のシーケンスが多くなるが，オンデマンドで経路を生成するため，制御メッセージを最小限に抑えられる．

- **GW 選択**

  MGA はパケット単位で GW を分散利用するが，TCP スループットの低下を招く．WAPL はセッション単位で GW を分散利用するため，TCP スループットの低下を防ぐ．他の方式は GW の分散利用については考慮していない．

(2) **FW/NAT 越え IP 電話システムにおける要求仕様の関係**

- **FW/NAT への依存**

  文献 [6] は FW/NAT そのものを交換する必要がある．他の方式はすでに設置している FW/NAT をそのまま利用できる．

- **端末への依存**

  HACP，Skype は電話端末に特殊な機能が必要となる．他の方式は既存の SIP 端末を利用できる．

参考文献

[1] Freed, N.: Behavior of and Requirements for Internet Firewalls, *RFC 2979* (2000).

[2] Egevang, K. and Francis, P.: The IP Network Address Translator (NAT), *RFC 1631* (1994).

[3] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and Schooler, E.: SIP: Session Initiation Protocol, *RFC 3261* (2002).

[4] Navda, V., Kashyap, A. and Das, S.R.: Design and evaluation of iMesh: an infrastructure-mode wireless mesh network, World of Wireless Mobile and Multimedia Networks, pp.164-170 (2005).

[5] Mobile Ad-hoc Network(manet):
http://www.ietf.org/html.charters/manet-charter.html

[6] Wakikawa, R., Malinen, J.T., Perkins, C.E., Nilsson, A. and Tuominen, A.J.: Global connectivity for IPv6 Mobile Ad Hoc Networks, draft-wakikawamanet-globalv6-05 (2006).

[7] Jelger, C., Noel, T. and Frey, A.: Gateway and address autoconfiguration for IPv6 adhoc networks, draft-jelger-manet-gateway-autoconf-v6-02 (2004).

[8] Ruffino, S. and Stupar, P.: Automatic configuration of IPv6 addresses for MANET with multiple, draft-ruffino-manet-autoconf-multigw-03 (2006).

[9] Lakshmanan, S., Sundaresan, K. and Sivakumar, R.: On Multi-Gateway Association in Wireless Mesh Networks, WiMesh 2006;Second IEEE Workshop on Wireless Mesh Networks, pp.64-730 (2006).

[10] 大竹八洲考，但馬康宏，寺田松昭: SIP を用いた NAT 通過手法の提案とその実装，情報処理学会論文誌，Vol.45, No.3, pp.813-823 (2004).

[11] 宮内信二: 多様な環境で利用できるインターネットプロトコル，情報処理学会論文誌，Vol.44, No.3, pp.553-560 (2003).

[12] Skype:
http://www.skype.com/home.html

2章　無線メッシュネットワーク ”WAPL ”の提案とシミュレーション評価

あらまし

無線メッシュネットワークは有線LANで接続していたアクセスポイント間をアドホックネットワークで接続することにより無線LANのバックボーンインフラを容易に構築することができる．しかし，従来の無線メッシュネットワークは，アドホックルーティングプロトコルを改造する方式が一般であり，用途が限定されるという課題があった．また，端末が移動したときにパケットロスが発生するという課題があった．本稿で提案するWAPL（Wireless Access Point Link）は，無線メッシュネットワークを実現するための機能を，アドホックルーティングプロトコルから完全に独立させた．その結果，ルーティングプロトコルを自由に選択し，様々な用途に応用できる．また，無線メッシュネットワークに必要なテーブルの生成をオンデマンドで実現するため，制御パケットが通信トラヒックに与える影響が少ない．さらに近隣のAPの通信状況を常時監視しておくことにより，端末が移動したときのハンドオーバ通知をユニキャストで実現できるようにした．これによりシームレスハンドオーバを確実に行うことができる．提案方式の有効性を評価するため，既存方式とWAPLをns-2のモジュールに組み込んで比較を行った．その結果，WAPLの特徴を定量的に示すことができた．

2.1　はじめに

無線LANのAP（Access Point）間をアドホックネットワークで接続し，バックボーンインフラを容易に構築する無線メッシュネットワークの研究に注目が集まっている．無線メッシュネットワークではAPを適切に配置していくだけで無線LANの通信エリアを容易に広げていくことができ，増設や移設が簡単で柔軟性の高いシステムを構築できる．無線メッシュネットワークは様々な機関で研究・開発が進められてきたが[1]〜[4]，いずれも独自の方式であることから互換性がなかった．このことを解決するため，IEEE802.11委員会では2004年6月にタスクグループsを発足させ，無線メッシュネットワークの標準化を進めている[5]．無線メッシュネットワークと呼ぶものの中には通信端末も含めてすべての装置がアドホックモードに設定されていることを前提とする場合がある．しかし，IEEE802.11sでは一般の通信端末が設定を変えることなくネットワークに接続できることを目的とし，APと通信端末はインフラストラクチャモードで接続するものと定義している．本論文でもAP同士はアドホックネットワークを構築し，APと通信端末はインフラストラクチャモードで接続するものを無線メッシュネットワークと定義する．

無線メッシュネットワークを実現するには，APが端末間の通信パケットを，アドホックネットワークを介して適切に中継できる必要がある．このためには，各APは通信相手の端

末がどの AP と接続しているかを示すマッピング情報（以下，AP/端末マッピング情報）を何らかの方法であらかじめ知っている必要がある．AP/端末マッピング情報の生成/保持方法の違いにより様々な方式が存在し，それぞれに特徴や性能の違いがある．

従来の無線メッシュネットワークでは，AP/端末マッピング情報の生成方法として，アドホックルーティングプロトコルを改造する方法をとる．この方法は AP/端末マッピング情報を生成するための情報をルーティングプロトコルの制御パケットに含ませることができ，制御パケットが増加しないという特徴がある．しかし，特定のアドホックルーティングプロトコルに限定する必要があり，おのずと目的を絞ったシステムとなる．これまでの無線メッシュネットワークは，無線 LAN の公衆バックボーンを迅速に構築することが目的とされており，それに適したルーティングプロトコルが選定されていた．しかし，無線メッシュネットワークは，他にも様々な応用を考えることが可能であり，ルーティングプロトコルが限定されるのは好ましくない．ただし，これによって制御パケットが大きく増加しない方式であることが望ましい．

次に通信中に端末が移動した場合においてもパケットのロスがないまま通信の継続ができることが望ましい．本論文ではこのような機能をシームレスハンドオーバと呼ぶ．無線メッシュネットワーク内での移動は，AP が切り替わるだけであるため，端末の IP アドレスが変わることはない．しかし，AP に登録されている AP/端末マッピング情報を迅速に書き換えることができないとパケットロスが発生することになる．

既存技術の代表である IEEE802.11s では，各 AP がデータリンク層においてアドホックルーティングプロトコルと同様の動作を実行して MAC アドレスを用いたルーティングテーブルを生成し，その中で AP/端末マッピング情報も同時に生成する．ルーティングプロトコルにはハイブリッド方式を採用し，リアクティブ型とプロアクティブ型を環境によって切り替えることができるが，選択はその 2 通りに限られ，他のルーティング方式は利用できない．また，シームレスハンドオーバについての議論はなされていないため，移動のタイミングや通信の方向によってはしばらくの間通信が途絶する可能性がある．

シームレスハンドオーバを実現できることを特徴とした無線メッシュネットワークの研究として SMesh[6] と iMesh[7] がある．SMesh ではハンドオーバ時にパケットの経路を二重化することによりパケットロスを回避する．しかし，SMesh は端末もアドホックモードに設定されている必要があり，本論文が定義するメッシュネットワークとは異なる．iMesh ではハンドオーバが発生したときにそのことを検出した AP がフラッディングにより周辺の AP に通知し，さらに AP が必要なパケットをバッファリングしておくことによりパケットが消失しないように制御する．しかし，アドホックネットワークにおけるフラッディングは信頼性が低く，ハンドオーバに失敗する可能性があるという課題がある．

国内における無線メッシュネットワークの研究として M-WLAN[1] がある．M-WLAN ではアドホックルーティングプロトコルとして OLSR を選定し，これを改造することにより AP/端末マッピング情報を生成する．このため，AP/端末マッピング情報は定期的に交換

される．用途としては無線 LAN バックボーン向けである．また，ハンドオーバ時の動作は iMesh と同様な方式をとるが，バッファリングは行わないためパケットロスが発生する．

そこで本論文ではこれらの課題を解決する無線メッシュネットワーク WAPL（Wireless Access Point Link）を提案する．WAPL では AP/端末マッピング情報の生成機能をアドホックネットワークと完全に独立させ，ルーティングプロトコルを自由に選択可能とした．また，AP/端末マッピング情報の生成に係るトラヒックの増加を抑えるため，これらの情報は必要に応じてオンデマンドで生成させることとした．さらにシームレスハンドオーバを実現するため，AP が近隣 1 ホップの通信を常時監視し，通信ペアの端末と各端末が接続する AP との関係を把握する．この情報により端末のハンドオーバ発生時に，ユニキャストにより確実に AP/端末マッピング情報の更新を行い，ハンドオーバの失敗を防止する．

ns-2 によるシミュレーションの結果，従来のフラッディングを用いたハンドオーバ通知では最大 13% が不到達になっていたのに対し，WAPL では同じ条件下で不到達率をほとんど 0% に抑えることができシームレスハンドオーバを実現できることを示した．また，AP/端末マッピング情報の生成方式として，定期交換方式とオンデマンド生成方式がトラヒックに与える影響を調査し，オンデマンド方式が有利であることを示した．さらに，アドホックルーティングプロトコルの違いがシステム性能にどのように影響するかを明らかにした．

以下，2.2 節で既存の無線メッシュネットワークの概要とその課題について，2.3 節で WAPL の概要を説明する．2.4 節ではシミュレーションの結果と考察を述べ，2.5 節でまとめる．

2.2 既存技術

既存技術の代表として，IEEE802.11s をあげる．IEEE802.11s は様々な方式を公募し，日本のグループが提案した SEE-Mesh[8] が方式のベースとなった．しかし，IEEE802.11s はシームレスハンドオーバについては現時点では未検討の状態である．そこで，シームレスハンドオーバを実現する既存技術としては iMesh を取り上げ，その方式を説明する．また，iMesh で利用するフラッディングによる移動通知が信頼性の低い理由を説明する．なお，本論文では AP は移動しないことを前提とする．

2.2.1 IEEE802.11s

IEEE802.11s では無線接続された AP を MAP（Mesh Access Point）と呼ぶ．図 2.1 に IEEE802.11s の構成と経路生成のシーケンスを示す．MAP 間はアドホックネットワーク，MAP/端末間はインフラストラクチャモードの無線 LAN である．IEEE802.11s では MAP 間のルーティングテーブル生成と MAP/端末マッピング情報の生成に HWMP（Hybrid Wireless Mesh Protocol）を利用する．HWMP は，IP アドレスのかわりに MAC アドレスを用いて，アドホックルーティングプロトコルと同様の動作を行う．HWMP は基本的には AODV（Adhoc

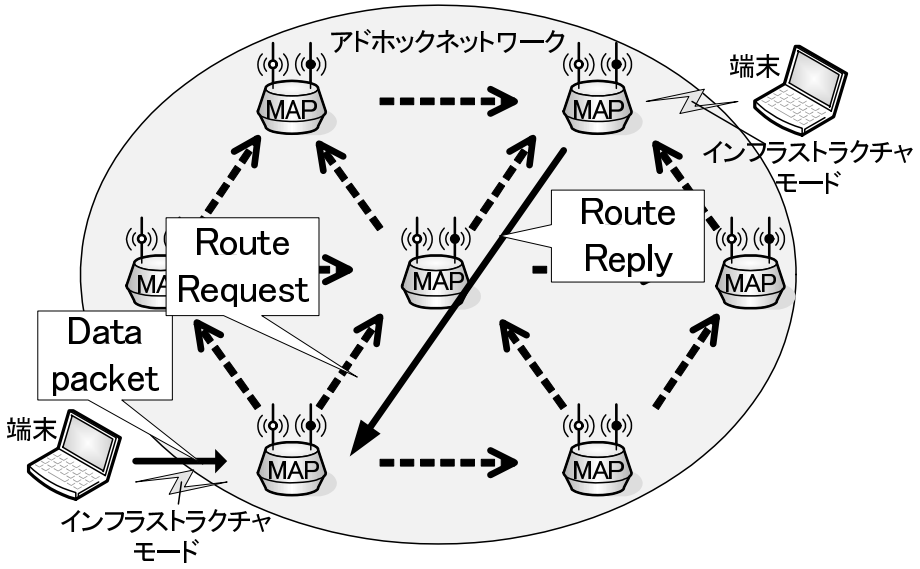

図 2.1 IEEE802.11s の構成と経路生成シーケンス

On-Demand Distance Vector）[9] をベースとした RM-AODV（Radio Metric AODV）によるリアクティブ型のルーティングを行うが，固定的なネットワークを形成する場合は，ツリー型のパスを事前に形成し，プロアクティブ型のルーティングを行うこともできる．IEEE802.11s ではこのように MAC アドレスを用いてルーティングを行うが，これは IEEE802.11 の関与する範囲が MAC 層であるためである．

RM-AODV では，端末が通信を開始すると，図 2.1 に示すように，その端末が接続している MAP が端末の代理で経路要求メッセージを他の MAP に対してフラッディングする．宛先の端末と接続している MAP は送信元 MAP へユニキャストで経路要求応答メッセージを返信する．以上のやり取りでルーティングテーブルと MAP/端末マッピング情報が同時に生成され，端末から端末への経路が確立する．IEEE802.11s で用いられるフレームは WDS（Wireless Distribution System）をベースにしており，MAP/端末間，および MAP 間のすべての通信フレームは，宛先端末，送信元端末，宛先 MAP，送信元 MAP の 4 つの MAC アドレスを持つ．MAP はこの情報から自分がアドホックルーティングの先頭/終点であることを知り，インフラストラクチャモードに設定されている端末同士の通信を実現することができる．

ハンドオーバの方式については IEEE802.11s では未検討の状態である．無線 LAN のハンドオーバについては，別途 IEEE802.11F，IEEE802.11r，および IEEE802.21[10] で検討されており，通信パケットを AP がバッファリングする方法や認証処理の高速化などが検討されている．しかし，これらの方式は AP 間の接続が有線であることを想定しており，無線メッシュネットワークには適していない．例えば，AP の切り替えを通知するために有線 LAN 上にブロードキャストパケットを送信するが，無線メッシュネットワークの場合はこ

れがフラッディングになる．フラッディングは 2.2.3 小節で述べるように，有線のブロードキャストに比べて信頼性が低く，通知に失敗する場合がある．また，これらの機能を実現するには端末側に対応する機能の実装が必要となる．

2.2.2 iMesh

本論文では他の方式と区別するため iMesh における無線接続された AP を iAP（iMesh AP）と呼ぶことにする．iMesh は iAP/端末マッピング情報を生成する方法として OLSR[11] をベースに改造を施す方法をとっている．iMesh は既存のアドホックルーティングと同様に IP 層でルーティングを行う．端末が iAP に参入すると，iAP は HNA メッセージ（OLSR のオプション）を拡張したメッセージをフラッディングする．拡張 HNA メッセージには端末のアドレス情報が含まれており，このメッセージを受け取った iAP は iAP/端末マッピング情報を生成する．ハンドオーバ時にも同様の処理が実行される．図 2.2 に iMesh のハンドオーバシーケンスを示す．図は固定端末から移動端末に向けたパケットが連続して送信されている状態を示している．ここで，移動端末が移動前に所属していた iAP を旧 iAP，移動後に所属する iAP を新 iAP，パケットの送信元の端末が所属している iAP を送信元 iAP と呼ぶ．移動端末は iAP を移動する際，離脱する旧 iAP に対し Deauthentication メッセージ，新 iAP に対し Reassociation Request メッセージを送信する．Reassociation Request メッセージを受信した新 AP は拡張 HNA メッセージをフラッディングする．各 AP に上記拡張 HNA メッセージが届くと移動端末に対する iAP/端末マッピング情報が新 iAP 宛に更新される．この間，固定端末から送信されたパケットは旧 iAP 内にバッファリングされ，拡張 HNA メッセージを受信したときに新 iAP へ転送される．この方式により全てのパケットは移動端末へロスが発生することなく届けることができる．なお，Deauthentication，Reassociation Request メッセージは無線 LAN で定義されているメッセージであり，端末に特殊な機能が必要となるものではない．しかし，フラッディングは次に述べるように信頼性の低い通信方式であり，内容の通知に失敗する場合があるという課題がある．

2.2.3 フラッディングの信頼性

フラッディングとは，メッセージがアドホックネットワーク全体に行き渡るように MAC ブロードキャストの転送を繰り返すものである．MAC ブロードキャストは宛先が特定できないので，RTS/CTS の制御や ACK による再送制御を行うことができない．図 2.3 にユニキャストとブロードキャストのシーケンスの違いを示す．ユニキャストは，AP2 と AP3 間の RTS/CTS 制御により AP4 を待機状態にできる．また ACK により確実に衝突を検出して再送制御が行える．それに対してブロードキャストは，RTS/CTS 制御と ACK の制御は行われないため，AP4 は AP2 が送信中であることを知らずに RTS/CTS を開始してしまう．

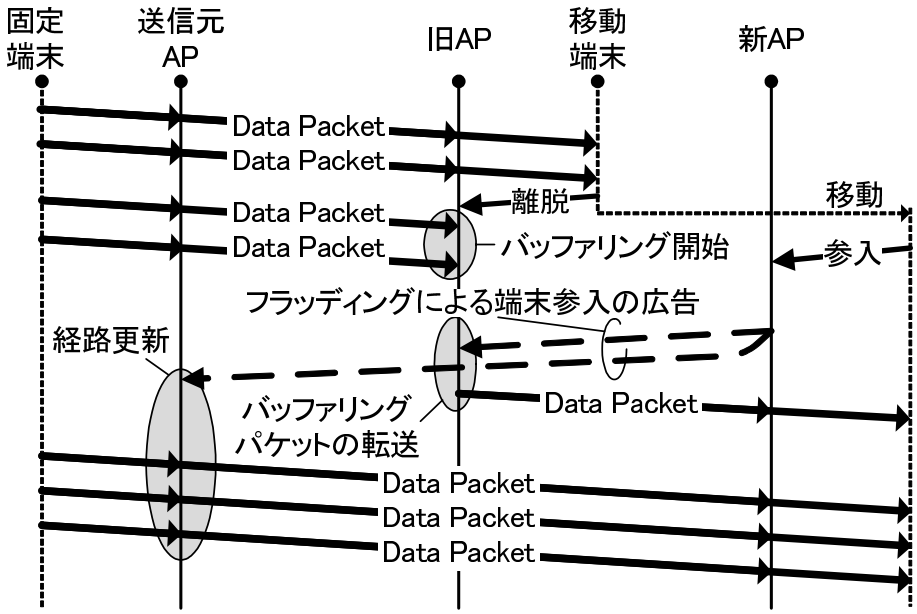

図 2.2 iMesh のハンドオーバシーケンス

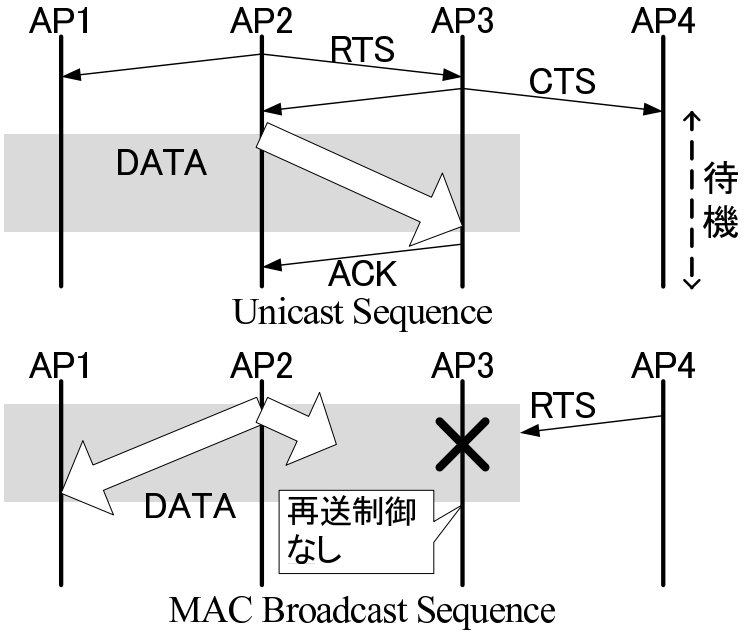

図 2.3 ユニキャストとブロードキャストのシーケンス

このようにブロードキャストパケットは破壊されやすい．また，AP では衝突によりパケットが破壊されたことを知ることができず再送制御が行われない．そのため，背景トラヒックのあるような状態ではブロードキャストの消滅率が高く，ハンドオーバの通知にフラッディングを用いると，その通知に失敗する可能性が高い．このような場合を救済するためには，フラッディングによる通知を一定時間ごとに繰り返す必要があるが，これによりシステム全体のトラヒックを圧迫する可能性がある．トラヒックへの影響を減らすためにはフラッディング間隔を大きくする方法があるが，通知に失敗した場合の回復に時間がかかるという課題がある．

2.3 WAPL の提案

2.3.1 WAPL の基本動作

WAPL では無線化した AP を WAP（Wireless Access Point）と呼ぶ．WAP 間の経路制御はアドホックルーティングプロトコルをそのまま採用し，WAP/端末マッピング情報は，ルーティングテーブルとは独立させ，LT（Link Table）と呼ぶ独自のテーブルとして保持する．また，WAPL では通信開始時に LT を生成するオンデマンドな方式を採用する．具体的には，端末が通信を開始する際の ARP 処理をトリガとして生成または更新する．LT の生成シーケンスを図 2.4 に示す．WAP は端末からの ARP 要求を受信すると，他の WAP へ LT 生成要求メッセージをフラッディングにより広告する．上記フラッディングはアドホックルーティングプロトコルのフラッディングとは独立した WAPL 独自のものであり，これと区別するために以後 LT フラッディングと呼ぶ． LT フラッディングは，WAP を実現するアプリケーションがブロードキャストを繰り返すことで成り立つ．同一の LT フラッディングパケットを 2 度以上受信した WAP はそのパケットを中継せずに廃棄する．

LT 生成要求メッセージには探索端末の IP アドレス，送信元端末の IP アドレスと MAC

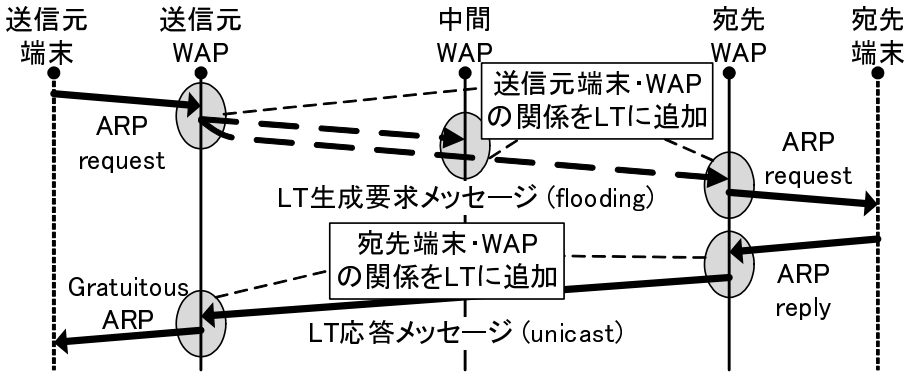

図 2.4 WAPL の LT 生成シーケンス

アドレスが記載されている．LT 生成要求メッセージを受信した全ての WAP は自身の LT に送信元端末の IP アドレスと WAP の IP アドレスの対応関係を記述する．配下に ARP 要求を送信することにより目的の端末が存在することを検出した WAP は，ユニキャストで送信元 WAP に LT 応答メッセージを返す．LT 応答メッセージには探索端末と送信元端末それぞれの IP アドレスと MAC アドレスが記載されており，送信元 WAP は LT 応答メッセージを受信すると宛先端末の IP アドレスと WAP の IP アドレスの関係を LT に記述する．以上の動作により送信元 WAP と宛先 WAP に LT が生成される．送信元 WAP は LT 応答に含まれる宛先端末の MAC アドレスから ARP 応答を生成し，送信元端末へ返す．以後，端末が送信したデータパケットは，送信元 WAP が MAC ヘッダも含めて WAP の IP アドレスにより IP カプセリングし宛先 WAP まで中継する．MAC ヘッダを含めてカプセリングする理由は，2.3.3 小節で述べるシームレスハンドオーバを実現するためにその情報を使用するためである．無通信状態が一定時間以上続くと，通信が終了したものとみなし LT を削除する．もし，端末に ARP キャッシュが残っていると、通信開始時であっても ARP は実行されずにデータパケットが送信されることもある．このとき，もし WAP 側に LT が存在しない場合は，データパケットを一時退避し，ARP の場合と同様に LT 生成要求から始まる LT の生成手順を実行する．

LT フラッディングを定義したことにより通常のアドホックネットワークよりも制御トラヒックが増加する．しかし，WAPL では LT の生成を必要に応じてオンデマンドで生成するため，他のトラヒックのスループットに与える影響は小さい．LT フラッディングは一般のフラッディングと同様の原理であるため，信頼性が高いものではない．そのため，LT の生成に失敗する可能性もあるが，通信開始時においては WAP の再送制御により確実に LT を生成することが可能である．ここで，再送制御とは，LT 応答メッセージが一定時間内に返ってこない場合に再度 LT フラッディングを行う機能である．

2.3.2 WAP の構成とその利点

WAP の構成を図 2.5 に示す．WAP はインフラストラクチャモードとアドホックモードの IEEE802.11 インタフェースを持ち，アドホックモードのインタフェース側ではアドホックルーティングが動作する．WAP は LT を生成し，パケットを中継するための LT 管理，IP カプセリングや近隣通信テーブル管理のモジュールとアドホックルーティングのモジュールを完全に独立させる．これにより，LT の生成方法と WAP 間のルーティングテーブル生成方法を分けて考えることができ，利用環境に応じて効率の良いメッシュネットワークを構築することができる．また，収容する端末数が多いとネットワークに参加していても通信は行わない端末も多く存在する．そのため，AP/端末マッピング情報の生成には常時全端末に係る情報を保持しておく定期交換方式より，WAPL で実現するオンデマンド方式が適している．

一方，AP 間のルーティングテーブルの生成方法は利用環境によって有利となる方式が異

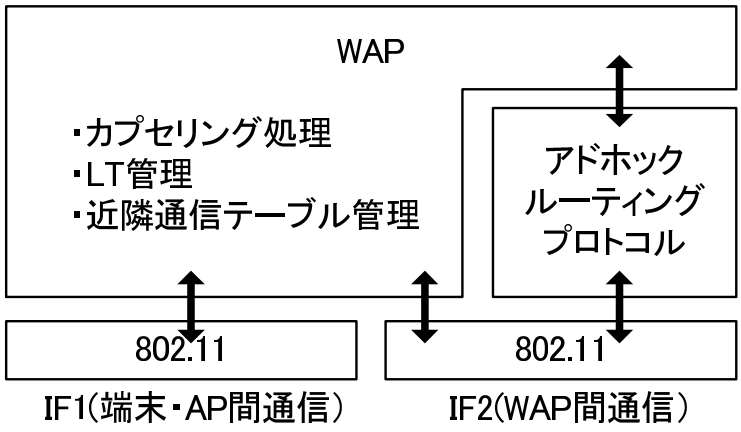

図 2.5 WAP の構成

なる．利用環境としては公共通信網に使用するような無線 LAN バックボーンインフラを構築する場合と，災害発生時や工事現場，イベント会場などに一時的に通信網を構築する場合が考えられる．バックボーンインフラでは AP の移動はなく，電源も供給できる．このような場合は，常時安定したルーティングテーブルを生成しておく OLSR が適していると考えられる．それに対し一時的な通信網では AP が移動する場合が考えられ，電源供給もできるとは限らない．例えば，災害発生時に現地にネットワークインフラを迅速に構築するために利用する応用例が考えられる．この場合は電力を消費しないとされる AODV を採用できる方がよいと考えられる．

また，同一のルーティングプロトコルであってもプロトコル自体が技術的に進化していくことも考えられる．例えば，マルチチャネルや指向性アンテナを用いてアドホックネットワークの帯域幅を広げようとする試みが多岐にわたって行われている [12]〜[15] ．WAPL ではこれらの研究成果をそのまま利用できるという利点がある．さらに，同一プロトコルのバージョンアップが行われた場合にも，他の機能に手を加えることなく容易に追随することができる．

2.3.3 シームレスハンドオーバの実現

次に WAPL ではシームレスハンドオーバが実現できることが重要と考え，以下のような対策をとった．

(1) **近隣通信の把握**

WAPL では端末移動時のハンドオーバ通知を確実に行うために，新 WAP から旧 WAP と送信元 WAP に対してフラッディングではなくユニキャストでハンドオーバを通知する．これを可能とするためには，新 WAP は端末が WAP 間をどのように移動したかを知っている必要がある．そこで，各 WAP では予め近隣で通信中の端末の IP ア

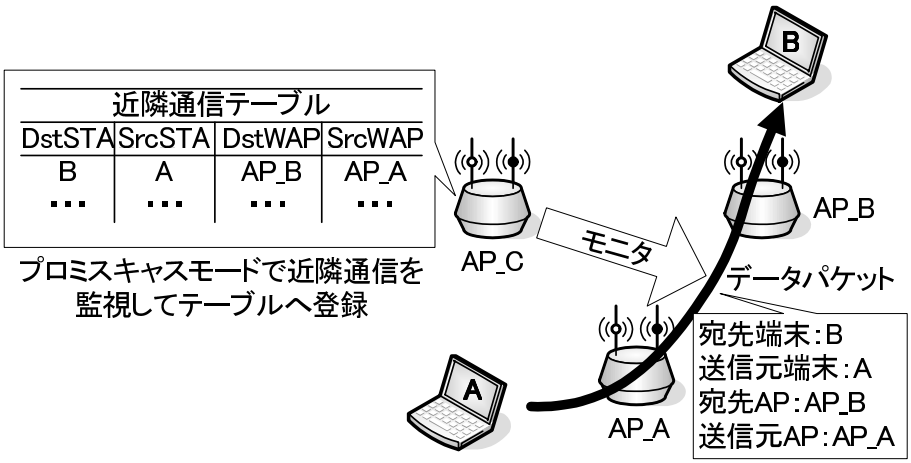

図 2.6 近隣通信の把握方法

ドレスおよびMACアドレスとWAPのIPアドレスを関連付けるテーブルを作成しておく．このテーブルを近隣通信テーブルと呼ぶ．近隣通信の把握方法を図2.6に示す．WAPはプロミスキャスモードで近隣のWAPが送信する通信パケットを常時モニタする．WAPは自身宛以外のパケットのIPヘッダから宛先WAP，送信元WAPのIPアドレスを，カプセル化されたMACヘッダとIPヘッダから宛先端末，送信元端末のMACアドレスとIPアドレスを取得し，それらを図2.6に示す近隣通信テーブルのフィールドであるDstWAP，SrcWAP，DstSTA，SrcSTAに記録する．

また，WAPLでは常時モニタを行うため，暗号化への対応を考慮する必要がある．WAPと端末間の暗号化にはWEP（Wired Equivalent Privacy），WPA（Wi-Fi Protocol Access）等の技術があるが，WAPで一度平文に戻すため，WAPのモニタには影響しない． WAP間の通信はWAPLの管理下であるため，暗号化を行うか否かを選択することができる．暗号化する場合は全WAPがあらかじめ共通の秘密鍵を共有し，WEP，WPAなどを適用する方法が考えられる．また，IPsecのようなIP層以上の暗号化においては，IPアドレス部分は平文であるため，モニタ処理には影響ない．

(2) **ハンドオーバ通知**

端末が移動した際のハンドオーバ通知の動作を図2.7に示す．ハンドオーバ処理のトリガはiMesh同様，Deauthentication/Reassociation Requestメッセージとする．旧WAPは端末からDeauthenticationメッセージを受信するとパケットのバッファリングを開始する．新WAPは端末からReassociation Requestメッセージを受信すると，端末のMACアドレスから近隣通信テーブルを参照し，移動してきた端末のMACアドレスを持つレコードが存在すれば通信中であると判断し，ハンドオーバを開始する．

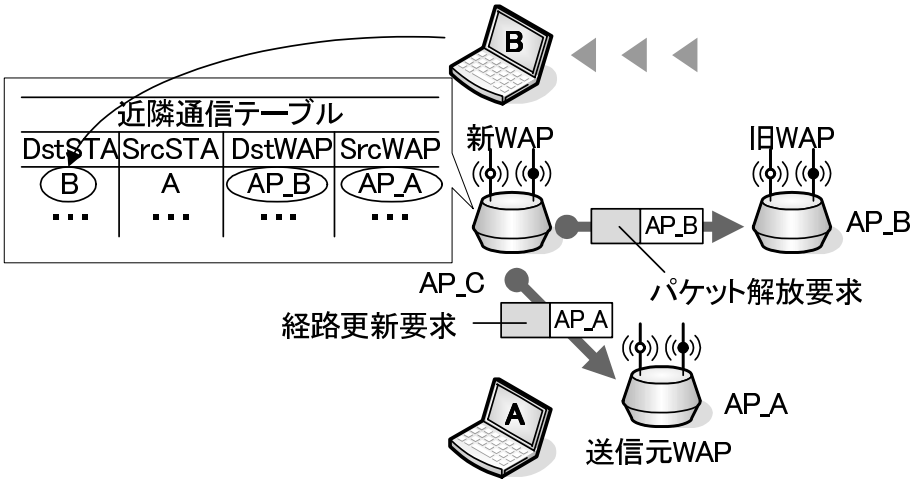

図 2.7 ハンドオーバ通知

すなわち，近隣通信テーブルから端末の旧 WAP と送信元 WAP の IP アドレスを参照し，旧 WAP にはパケット解放要求メッセージ，送信元 WAP には経路更新要求メッセージをユニキャストで送信する．旧 WAP と送信元 WAP は受信したメッセージに対して応答メッセージを返す．新 WAP は一定時間の間に応答メッセージが返ってこない場合は再送処理を行う．旧 WAP はパケット解放メッセージを受け取るとバッファリングしていたパケットを新 WAP に転送する．送信元 WAP は経路更新要求メッセージを受け取ると LT を書き換えることによりパケットの経路を更新し，ハンドオーバが完了する．制御メッセージをユニキャストで通知するため，パケット到達の信頼性が高く，通信相手を特定しているため再送制御も可能である．なお，新 WAP における送信元端末に対する LT は移動端末が新 WAP へ移動した時点で近隣テーブルの内容から直ちに更新することができる．近隣通信テーブルの保持時間は ARP キャッシュと同程度の「2 分」程度が最適と考えられる．また，応答メッセージの待ち時間タイマは今回は 50 ミリ秒とした．

2.4 評価

WAPL の有効性を示すため，ネットワークシミュレータ ns-2（network simulator-2）[16] を利用して WAPL と既存技術の比較評価を行った．iMesh と WAPL において通信中にハンドオーバが発生したとき，ハンドオーバ通知の不到達率を比較して WAPL によるユニキャスト方式がシームレスハンドオーバにいかに有効であるかを 2.4.2 小節に示した．次に，iMesh が iAP/端末マッピング情報を定期的に生成するのに対し，WAPL は WAP/端末マッピング情報をオンデマンドで生成するという違いがある．このことに起因する違いを評価するため，以下のようなシミュレーションを行った．まず，ネットワークに接続する端末の数が増

加したとき，WAPL では制御メッセージによるトラヒックの増加は発生しないが，iMesh では制御メッセージが増加する．そこで 2.4.3 小節では iMesh の制御メッセージがどの程度増加するかをシミュレーションした．次に，端末の通信開始頻度が増加したとき iMesh では制御メッセージによるトラヒックの増加はないが，WAPL では制御メッセージが増加する．そこで 2.4.4 小節では WAPL の制御メッセージがどの程度増加するかをシミュレーションした．さらに，iMesh では通信開始遅延は発生しないが，WAPL では通信開始遅延が発生する．そこで 2.4.5 小節では WAPL の通信開始遅延をシミュレーションにより測定した．

2.4.1 ns-2 の改造

ns-2 は研究機関でよく利用されているフリーソフトである．しかし，ns-2 はアドホックネットワークの機能は充実しているものの，現時点では無線 LAN インフラストラクチャモードの機能が備わっていない．従ってそのままではメッシュネットワークのシミュレーションも不可能である．そこで，ns-2 に以下のような改造を施し，シミュレーション環境を構築した．ns-2 の IEEE802.11 機能実行モジュールにビーコンの発信，電波強度による AP 離脱と次の AP への移動の判断，離脱・参加処理を追加した．無線メッシュネットワークは AP がインフラストラクチャモードとアドホックモードの 2 種類のインタフェースをもつ必要があるが，それぞれのインタフェースを持つノードの内部モジュール間のインタフェース同士をネットワークを介さず直接接続することにより WAP を実現した．今回のシミュレーションでは簡単のためインフラストラクチャモード側はアドホックモード側と干渉しない上で同一チャネルとした．

2.4.2 ハンドオーバ通知の不到達率

端末が移動したとき，新 AP から旧 AP にハンドオーバを通知できなければ旧 AP でバッファリングしていたパケットは損失する．また，送信元 AP と新 AP 間の AP/端末マッピング情報を更新できなければ経路不整合となり，パケットの損失や通信の回復時間が大きくなる原因となる．本シミュレーションではハンドオーバ時に旧 AP と送信元 AP に送信される制御メッセージの不到達率を計算し，同時に制御メッセージが不到達になったときに経路が更新されるまでの回復時間を求めた．制御メッセージは，iMesh 方式はフラッディング，WAPL 方式はユニキャストである点が大きく異なる．シミュレーションのパラメータを表 2.1 に，シミュレーションフィールドの構成を図 2.8 に示す．シミュレーションフィールド上には WAP（iAP）を複数配置し，2 台の端末に VoIP を想定した双方向通信をさせながら，一方の端末は固定し，もう一方の端末は 2 つの WAP（iAP）間を繰り返し移動させる．図 2.8 で示すように，WAP（iAP）同士の距離はすべて等間隔の 80m で近隣の WAP（iAP）が六角形を作るように配置した．WAP（iAP）と端末の電波到達距離は 100m で WAP（iAP）

表 2.1 シミュレーションパラメータ（1）

ハンドオーバを行う端末	
台数	2 台（1 ペア）
通信タイプ	UDP，20ms 間隔，172bytes
ホップ数（AP 間）	1，2，3，4
ハンドオーバ回数	800
背景負荷を発生する端末	
台数	10 台
セッション数	10
送信トラヒック/端末	250, 500, 750, 1000, 1250kbps
設置位置	ランダム
メッシュネットワーク	
AP （WAP）台数	24 台
電波到達距離	100m
WAP(iAP) 間の距離	80m
MAC プロトコル	IEEE802.11g
メッシュネットワークプロトコル	iMesh, WAPL（OLSR）

は近隣の WAP（iAP）の無線セルと重なりあっている．背景負荷をかけるため，端末を複数台設置し，一定期間ごとにランダムにペアを変更しながら双方向の UDP 通信を行わせた．ホップ数ごとの違いを評価するために固定端末の位置をずらし WAP（iAP）間のホップ数を 1，2，3，4 と変化させた．端末側のチャネルはすべて同一とした．なお，ホップ数の値は新旧 WAP（iAP）と送信元 WAP（iAP）間の最短ホップ数であり，経路構築時にルーティングプロトコルによっては冗長経路を生成することもある．

旧 WAP（iAP）へのハンドオーバ通知の不到達率を図 2.9，送信元 WAP（iAP）への不到達率を図 2.10 に示す．横軸の背景トラヒックは背景トラヒック生成用の端末 1 台が送信したトラヒック量を bps に変換して表している．iMesh 方式の旧 iAP への不到達率は背景トラヒックとともに上昇し，背景負荷用端末のトラヒックが 1.25Mbps の時には 10% 程度にまで達することがわかる．送信元 iAP への不到達率はホップ数によって差があり，4 ホップでは背景負荷が 1.25Mbps の時は不到達率が約 13% になる．背景トラヒックが 0 でも iMesh 方式の場合は不到達率が 0% にならない．これは移動端末自身が送受信している双方向の UDP 通信により，ブロードキャストパケットが破壊されるためである．また，ホップ数が多くなれば，送信元 iAP へ拡張 HNA メッセージが届くまでにパケットが衝突する可能性が

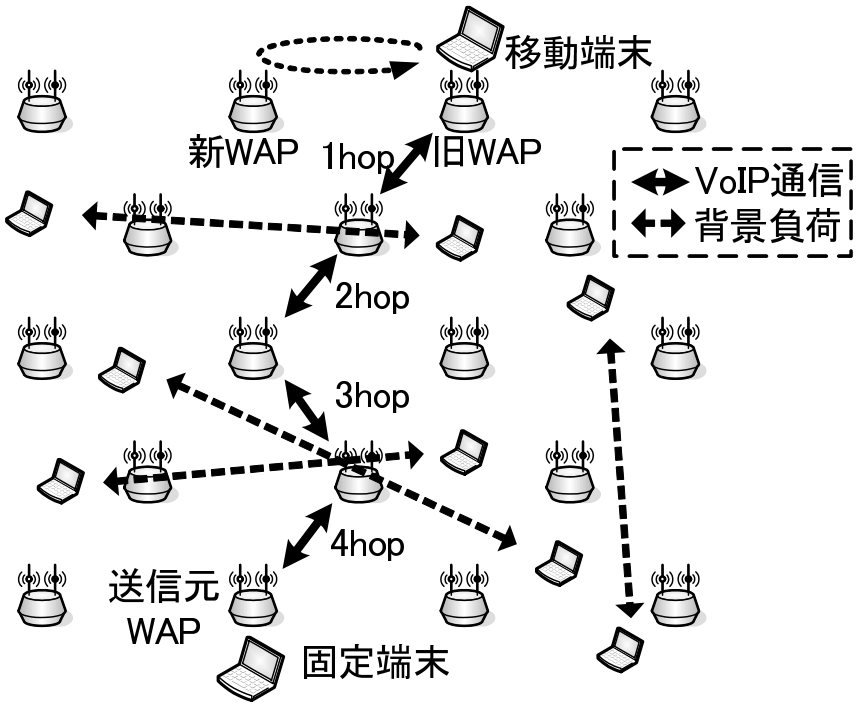

図 2.8 シミュレーションフィールドの構成

高くなり，不到達率が高くなることがわかる．これに対して，WAPL ではユニキャストを用いることによる効果でパケット解放要求，経路更新要求とも不到達率がほぼ 0% になっていることがわかる．ユニキャストは RTS/CTS 制御が働くことと ACK による確認により確実に衝突の検出と再送が行えるためである．

WAPL では送信元 WAP への経路更新要求が不到達となると通信中のパケットは旧 WAP へ送信され続ける．このとき，旧 WAP へのパケット解放要求が正しく到達していればパケットは旧 WAP から新 WAP に中継され，通信の継続は可能である．パケット解放要求も同時に不到達の場合のみハンドオーバは失敗となり，通信が継続できなくなる．

次に，ハンドオーバ開始から経路が更新されるまでの平均回復時間を求めた．ここで言う回復時間とは，端末が新 WAP（iAP）に移動してから送信元 WAP（iAP）の WAP（iAP）/端末マッピング情報の内容が新 WAP（iAP）に更新されるまでの時間である．図 2.11 に背景負荷用端末のトラヒックを 750Kbps に固定した場合の平均回復時間を示す．横軸は新 WAP（iAP）と送信元 WAP（iAP）間のホップ数を示している．iMesh では拡張 HNA メッセージの送信間隔が大きくかつホップ数が増えるにつれて，平均回復時間は大きくなり，拡張 HNA メッセージ間隔が 5 秒，ホップ数が 4 のときは平均回復時間が 0.6 秒となる．WAPL においては 4 ホップの場合でもルーティングプロトコルに OLSR を利用した場合 0.02sec，AODV を利用した場合 0.04sec 程度で iMesh 方式に比べて十分小さい時間で回復していることがわかる． WAPL において AODV の方が OLSR に比べて平均回復時間が大きいのは，

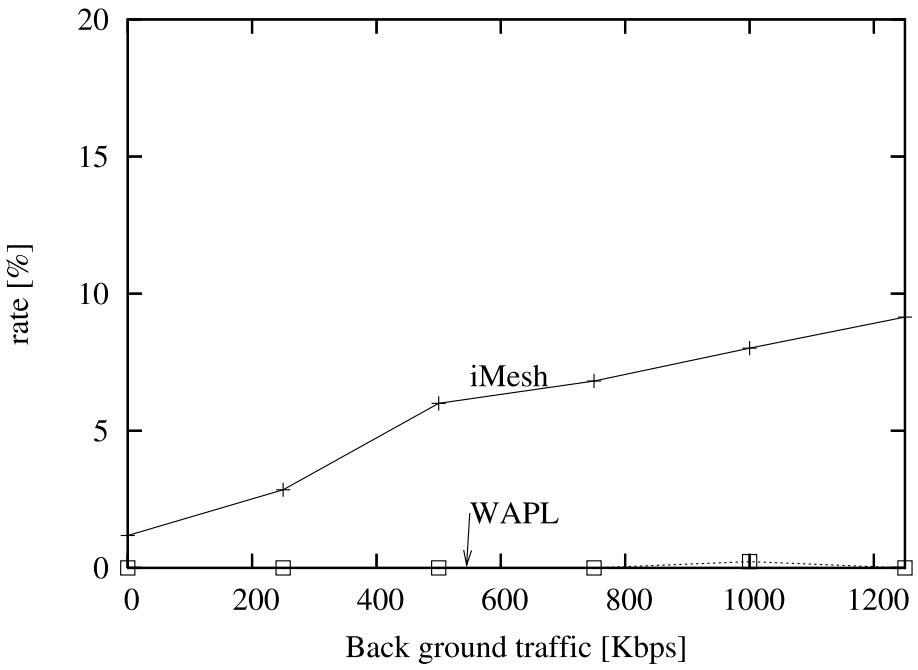

図 2.9 旧 AP への通知不到達率

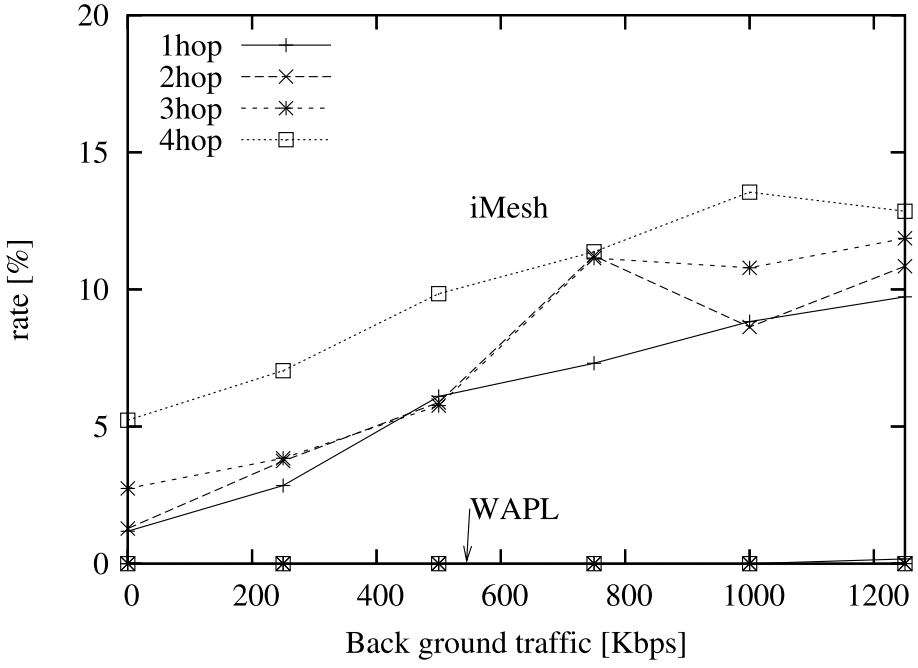

図 2.10 送信元 AP への通知不到達率

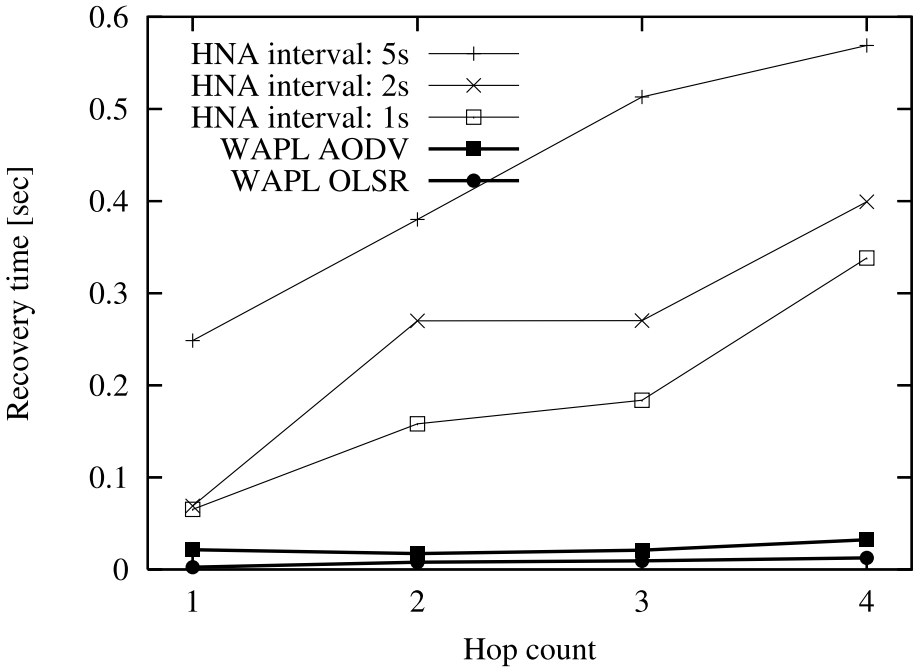

図 2.11 平均回復時間

表 2.2 回復時間の分布

Delay（sec）	0-0.5	0.5-1	1-1.5	1.5-2	2-
WAPL（OLSR）	100	0	0	0	0
WAPL（AODV）	99.1	0.8	0	0.1	0
iMesh（HNA:1s）	85.0	4.0	4.5	4.5	2.0
iMesh（HNA:2s）	80.2	9.8	6.0	2.8	1.2
iMesh（HNA:5s）	65.0	24.6	4.1	1.0	5.3

単位 [%]

OLSR が常に最適な経路を確立維持しているのに対して，AODV ではハンドオーバごとに経路探索を実行するためである．表 2.2 に 4 ホップのときの回復時間の分布を示す．iMesh ではハンドオーバ通知が失敗した際に，次の拡張 HNA メッセージの周期まで通知が遅れるため，大きな回復時間を要する場合がある．それに対し，WAPL では通知が正常に終了するまでその時点で再送処理を行うため，回復時間は極めて少ないことがわかる．また拡張 HNA メッセージは少し待機してから他のメッセージと相乗りして転送される．この待機時間も iMesh の平均回復時間を遅くする要因となっている．

表 2.3 シミュレーションパラメータ（2）

スループット測定用端末	
台数	2 台（1 ペア）
通信タイプ	FTP（50 秒間）
ホップ数（AP 間）	1，2，3，4
背景負荷を発生する端末	
端末密度（台数/AP）	0, 1, 2, 3, 4
通信	なし
拡張 HNA の間隔（秒）	1, 2, 5
設置位置	ランダム
メッシュネットワーク	
AP 台数	38, 52 台
電波到達距離	100m
WAP(iAP) 間の距離	80m
MAC プロトコル	IEEE802.11g
メッシュネットワークプロトコル	iMesh

2.4.3 定期生成方式がトラヒックに与える影響

iAP/端末マッピング情報を定期的なフラッディングにより生成する定期生成方式がトラヒックに与える影響を調べるために，iMesh のシミュレーションを行った．iMesh では拡張 HNA メッセージを定期的にフラッディングする．このフラッディングには全ての端末の情報を必要とするので，通信を行っていない端末の情報も含まれる．表 2.3 にシミュレーションパラメータを示す．シミュレーションフィールド上には iAP を等間隔に配置し，通信を行わない端末をランダムに配置する．その上で，測定用に設置した 2 台の端末に FTP 通信を実行させ，スループットを計測した．拡張 HNA メッセージの間隔は，5 秒,2 秒,1 秒とした．ネットワーク規模による違いを示すため，iAP の台数は IEEE802.11s で想定するネットワーク規模と同程度の 38 台の場合と，さらに規模の大きい 52 台の 2 通りとした．ネットワーク規模が大きくなるとシミュレーション時間が膨大になるため今回は 52 台を最大とした．上記条件のもとで 4 回ずつシミュレーションを行い，平均値を算出した．

図 2.12 に iAP38 台時，図 2.13 に iAP52 台時の端末密度の違いによるスループットの違いを示す．また表 2.4 には HNA 拡張メッセージ送信間隔が 1 秒の場合のスループットの低下率を示す．iAP38 台ではスループットへの影響は少ないものの，拡張 HNA メッセージの間隔が 1 秒のときは端末密度が 0 台と 4 台のときを比較すると，最大約 4.3% の劣化がみられる．iAP52 台のときは拡張 HNA メッセージの間隔が 5 秒であればスループットへの影響は少ないが，1 秒のときは，端末密度が 0 台と 4 台のときを比較すると最大約 9.3% 劣化して

表 2.4 HNA 拡張メッセージ送信間隔が 1 秒の場合のスループット低下率

	1hop	2hop	3hop	4hop
AP38 台	0.3	4.1	3.9	4.3
AP52 台	0.4	9.4	7.9	9.3

単位 [%]

表 2.5 シミュレーションパラメータ（3）

TCP スループット測定用端末	
台数	2 台（1 ペア）
通信タイプ	FTP（50 秒間）
ホップ数（AP 間）	1，2，3，4
背景負荷を発生する端末	
端末密度（台数/WAP）	4
1 端末の通信開始間隔（秒）	60
メッシュネットワーク	
WAP 台数	52 台
電波到達距離	100m
WAP（iAP）間の距離	80m
MAC プロトコル	IEEE802.11g
メッシュネットワークプロトコル	WAPL（OLSR，AODV）

いることがわかる．このように，ネットワーク規模が大きく，拡張 HNA メッセージの間隔が短いと，端末の密度が大きいときにスループットに影響が出ることがわかる．端末密度が高くなれば，拡張 HNA メッセージのデータサイズは長くなり，拡張 HNA メッセージの送信間隔が短くなればパケット数は増加する．また，ネットワークの規模により iAP の数が多くなれば拡張 HNA メッセージの発生源が多くなるため，ネットワーク全体の HNA メッセージ数が多くなる．上記結果から定期生成方式では端末移動時の経路の復旧を迅速に実現するために定期フラッディングの間隔を短くするか，ネットワークの規模，接続する端末の数を制限するかの選択が必要になる．これに対して，WAPL のようなオンデマンド型の方式では定期的メッセージは発生しないため，このようなトラヒックは発生しない．

2.4.4 オンデマンド方式がトラヒックに与える影響

WAP/端末マッピング情報を必要に応じて生成するオンデマンド方式がトラヒックに与える影響を調べるために，WAPL のシミュレーションを実施した．なお，IEEE802.11s もオンデマンド方式の 1 種である．WAPL では端末間の通信開始時に LT 生成のための LT フ

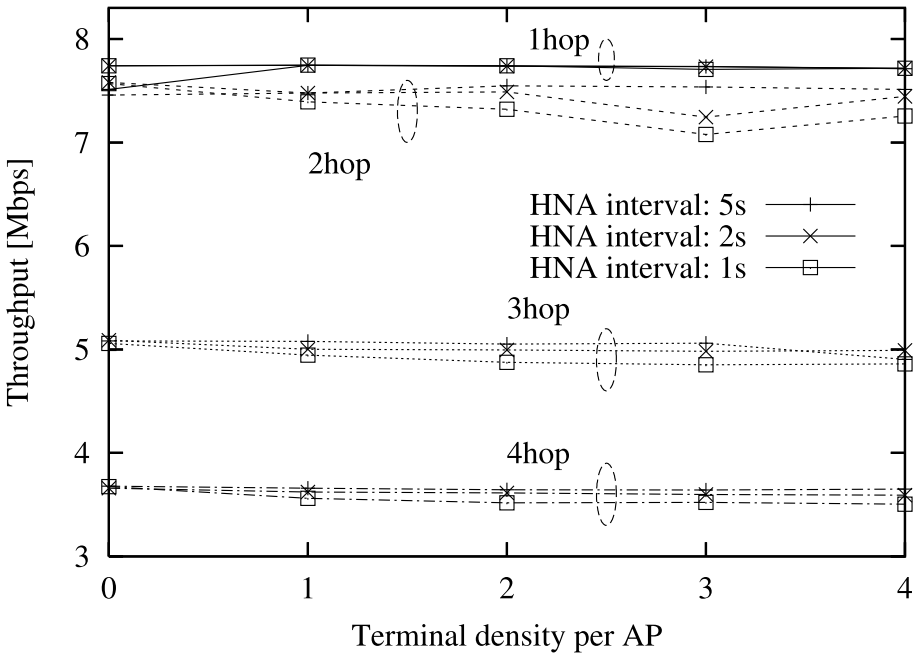

図 2.12 定期生成方式のスループット（AP38 台）

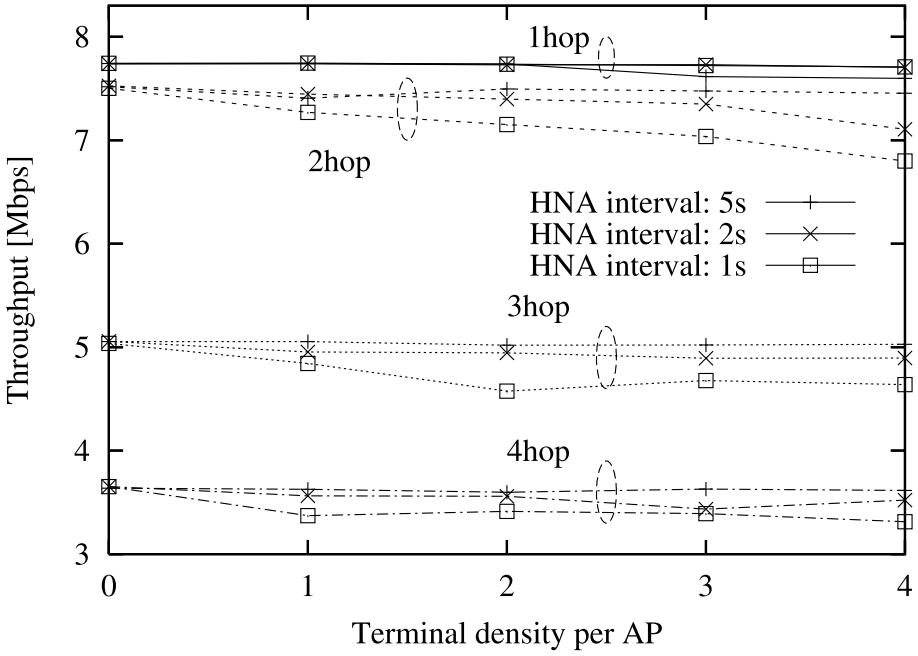

図 2.13 定期生成方式のスループット（AP52 台）

表 2.6 スループットの低下率（OLSR）

WAP 間距離	スループット		低下率
	通信開始なし	全端末が 60 秒に 1 回通信開始	
1hop	7.65Mbps	7.61Mbps	0.54%
2hop	7.48	7.40	1.11
3hop	5.05	5.00	0.97
4hop	3.65	3.62	0.82

ラッディングが実行されるため，通信開始頻度が高いと制御メッセージがネットワークの負荷となる可能性がある．これに対して iMesh のような定期生成方式では通信開始時に制御メッセージは発生しないため，通信開始頻度が変わってもトラヒックの増加はない．そこで，ネットワーク上の通信開始頻度を変化させ，WAPL の方式が一般通信のスループットにどれだけ影響を与えるかを評価した．シミュレーションのパラメータを表 2.5 に示す．シミュレーションフィールド上に WAP を等間隔に設置し，背景負荷用端末に一定時間ごとにランダムにセッションを確立させ，通信開始を繰り返させることにより LT フラッディングによるトラヒックを発生させた．その背景負荷のもとで，1 ペアの端末に FTP による通信を行わせ，スループットの変化を測定した．WAP の台数と端末の密度は 2.4.3 小節における最も厳しい条件と同様の 4 端末/WAP とした．通信開始に係わるトラヒックの影響のみを純粋に測定するため，通信開始後のデータパケットは WAP で遮断し，アドホックネットワーク側に出さないようにした．各端末が 60 秒おきに異なる相手に対して通信を開始する場合と，通信開始が全く発生しない場合を比較した．実際の通信では通信相手が特定のサーバやゲートウェイなど決まった相手に集中することもあるが，この場合は LT が一定時間保持されるため，LT フラッディングは発生しない．上記シミュレーション条件は，より過酷な条件として端末がネットワーク内で IP 電話のような P2P 通信を頻繁に行うというシナリオを想定した．即ち，IP 電話の 1 回の通話時間を 60 秒として，通話終了後にすぐに別の相手に掛け直すという動作をネットワーク上の全ての端末が繰り返し続けるものとする．これは実ネットワークで発生する通信に比べて十分過酷な条件設定であると考えられる．また，WAPL ではルーティングプロトコルを自由に選択できるのでアドホックルーティングプロトコルが OLSR と AODV の 2 通りの場合について比較した．

表 2.6，表 2.7 にルーティングプロトコルがそれぞれ OLSR の場合，AODV の場合のスループット低下率を示す．LT フラッディングが全く発生しない場合に比べて、通信開始による LT フラッディングの背景負荷がある場合は、FTP のスループットは OLSR の場合で約 0.5〜1.2% ，AODV では 0.9〜3.2% の低下となった．このようにオンデマンド生成方式はかなり厳しい条件を与えても一般通信にはほとんど影響を与えることがないことがわかる．

表 2.7 スループットの低下率（AODV）

WAP 間距離	スループット		低下率
	通信開始なし	全端末が 60 秒に 1 回通信開始	
1hop	7.67Mbps	7.56Mbps	1.40%
2hop	7.55	7.39	2.17
3hop	5.12	4.96	3.18
4hop	3.70	3.57	3.28

ルーティングプロトコルが AODV の場合と OLSR の場合を比べると，通信開始なしの場合は若干 AODV の方が平均スループットが高いが，これは OLSR では TC，Hello などの定期メッセージによる背景負荷があるためである．TC，Hello などの定期メッセージは OLSR のルーティングテーブルを生成するための OLSR 独自の制御メッセージである．OLSR の定期メッセージは通信開始がなくても発生するが，AODV は通信開始時にしか制御メッセージが発生しない．そのため通信開始なしの場合には AODV の平均スループットが若干高くなる．また，通信開始頻度によって OLSR の制御メッセージ量が変化しないのに対して，AODV の場合は LT 生成時に LT フラッディングとは別に AODV の経路探索のフラッディングが余分に発生するため，通信開始頻度が上がると AODV の制御メッセージ量は増加する．このため，60 秒に 1 回の通信開始の場合は OLSR のスループットの方が若干高くなる．

2.4.5 オンデマンド方式が通信開始遅延に与える影響

WAPL では通信開始時に LT を生成するために遅延が発生する．これはルーティングプロトコルからの独立性を実現した事に対する見返りの短所と言える．そこで WAPL において，LT を生成するまでにかかる時間を示すシミュレーションを行った．LT の生成に要する時間を純粋に測定するため，アドホックルーティングでは通信開始遅延の発生しない OLSR を利用した．送信元 WAP がインフラストラクチャモード側の端末からパケットを受け取り，LT フラッディングにより LT が生成され，パケットが送信される瞬間までの遅延を異なる背景負荷ごとに測定した．本シミュレーションのパラメータは 2.4.2 小節と同一の条件とした．また，サンプルの分散を示すため，95% 信頼区間を算出した．これはサンプルの母集団の値が 95% の確率でその信頼区間の範囲内にあてはまることを示す．

シミュレーション結果を表 2.8 に示す．1hop であれば背景負荷が最大時平均が 30ms，信頼区間は± 10ms となった．4hop では背景負荷が最大のとき平均が 155ms，信頼区間は± 64ms となった．これに対して，iMesh では定期交換方式であるため通信開始遅延はない．通信開始遅延に関しては iMesh が有利であるが，WAPL の遅延は実用上許容範囲と考えられる．

表 2.8 LT の生成に要する時間

背景負荷端末 1 台あたりの背景負荷 [Kbps]		0	500	1000	1250
1hop	平均	8	4	29	30
	95%信頼区間	± 5	± 2	± 11	± 10
4hop	平均	6	13	92	155
	95%信頼区間	± 4	± 6	± 42	± 64

単位 [ms]

2.5 まとめ

無線メッシュネットワークの一方式として以下のような特徴を持つ WAPL を提案した．まず，アドホックルーティングプロトコルと WAP/端末マッピング生成機能を完全に独立させた．そのため，利用条件に適したルーティングプロトコルの選択ができる上，ルーティングプロトコルのバージョンアップにも容易に追随できる．また，WAP/端末マッピング情報を必要に応じてオンデマンドで生成することにより，一般通信のトラヒックに与える影響をなくした．さらに，各 WAP が近隣通信 WAP の状況を常に把握しておくことにより，ハンドオーバ通知メッセージをユニキャストで実現することとした．これにより，ハンドオーバ通知の信頼性を向上させた．シミュレーションにより，WAPL がシームレスハンドオーバを実現できることを示した．WAPL はアドホックルーティングプロトコルを独立させたことにより，通信開始時のシーケンスが追加される．このため通信開始遅延が発生し，通信開始頻度が高くなると制御メッセージによるトラヒックが増加するという課題がある．ただし，このことによる影響は実用上ほとんどないことをシミュレーションにより示した．今後は WAPL を災害通信への応用など様々な条件下でのシミュレーションを行い，条件に応じたルーティングプロトコルの選定などを行っていく．また，WAP が移動するような応用例についても検討を行う．さらに，実機によるテストベッドを構築・運用し，評価を実施する予定である．

参考文献

[1] 大和田泰伯，照井宏康，間瀬憲一，今井博英：マルチホップ無線 LAN の提案と実装，電子情報通信学会論文誌 B， Vol. J89-B, No. 11, pp. 2092–2102 (2006).

[2] MetroMesh:
http://www.tropos.com/.

[3] MeshCruzer:
http://www.thinktube.com/.

[4] Packethop:
http://www.packethop.com/.

[5] IEEE802.11:
http://grouper.ieee.org/groups/802/11/.

[6] Amir, Y., Danilov, C., Hilsdale, M. et al.: Fast Handoff for Seamless Wireless Mesh Networks, *ACM MobiSys* (2006).

[7] Navda, V., Kashyap, A. and Das, S. R.: Design and evaluation of iMesh: an infrastructure-mode wireless mesh network, *World of Wireless Mobile and Multimedia Networks*, pp. 164–170 (2005).

[8] Aoki, H., Chari, N., Chu, L. et al.: 802.11 TGs Simple Efficient Extensible Mesh (SEE-Mesh) Proposal (2005).

[9] Perkins, C. E., Belding-Royer, E. M. and Das, S. R.: Ad hoc On-Demand Distance Vector (AODV) Routing, *RFC 3561* (2003).

[10] IEEE802.21:
http://grouper.ieee.org/groups/802/21/.

[11] Clausen, T. and Jacquet, P.: Optimized Link State Routing Protocol(OLSR), *RFC 3626* (2003).

[12] 長島勝城，高田昌忠， 渡邊尚：スマートアンテナを用いた 2 種アクセス併用指向性メディアアクセス制御プロトコル，電子情報通信学会論文誌 B， Vol. J87-B, No. 12, pp. 2006–2019 (2004).

[13] Nasipuri, A., Ye, S., You, S. et al.: A MAC protocol for mobile ad hoc networks using directional antennas, *IEEE Wireless Communications and Networking Conference*, pp. 1214–1219 (2000).

[14] Chen, J. and Chen, Y.-D.: AMNP: Ad Hoc Multichannel Negotiation Protocol for Multihop Mobile Wireless Networks, *IEEE International Conference on Communication* (2004).

[15] Jain, N., Das, S. R. and Nasipuri, A.: A Multichannel CSMA MAC Protocol with Receiver-based Channel Selection for Multihop Wireless Networks, *IEEE ICCCN*, pp. 432–439 (2001).

[16] ns2:
http://www.isi.edu/nsnam/ns/.

3章　無線メッシュネットワークにおけるゲートウェイ分散方式の提案と評価

あらまし

無線 LAN の AP（Access Point）間をアドホックネットワークによって接続する無線メッシュネットワークの研究に注目が集まっている．無線メッシュネットワークは AP を自由に設置でき，容易に無線ネットワークの範囲を広げることができる．無線メッシュネットワークでは，インターネットなどの外部のネットワークと接続するとき，スループットのネックとなる GW（Gateway）周辺の帯域の消費を解消するため，複数の GW を設置する方法が検討されている．これまで，パケットごとに複数の GW に分配する方式が検討されているが，TCP のふくそう制御の機能により通信のスループットを低下させてしまう．そこで，我々はセッションごとに複数の GW に分配することにより，GW を効率的に利用し，かつ TCP 通信のスループットに影響を与えない方式を提案する．シミュレーションによって提案方式が既存方式に比べて TCP 通信のスループットが向上すること，公平性も十分保たれることを明らかにした．

3.1　はじめに

無線 LAN は，配線が不要であり，端末が自由に移動できることから，今後も広く普及することが期待されている．無線 LAN の構築方法として，インフラストラクチャモードによる方法とアドホックモードによる方法がある．インフラストラクチャモードは一般に利用されている方式であり，端末は必ず AP（Access Point）を介して通信を行い，AP 間は有線で接続する．一方，アドホックモードは端末どうしで直接通信を行うことができる．アドホックモードの応用としてモバイルアドホックネットワーク（Mobile Ad Hoc Network：MANET）があり，端末のみによるインフラ構築が可能である．しかし，MANET は現在のところ研究レベルの使用にとどまっており，活用の範囲が限られている．その理由として，パケットの中継を行う端末（中継端末）のリソース（CPU，電力など）をユーザの意図に反して使用してしまうこと，中継端末の移動により経路が安定性しないこと，中継端末による攻撃や盗聴など安全性に課題があることなどがあげられる．

そこで，近年では MANET を応用した無線メッシュネットワークの研究に注目が集まっている．無線メッシュネットワークは，AP に MANET を形成する機能を持たせ，AP 間を無線で接続するものである．無線メッシュネットワークは有線ケーブルを必要としないことから，AP の設置の自由度が向上し，容易に無線ネットワークのエリアを拡張することができるという特徴がある．また，端末のリソースを勝手に消費するという問題がなく，中継装置となる AP は基本的に移動しないため，経路も比較的安定している．さらに AP は同一サービスプロバイダが準備すれば良いので安全性の確保が容易である．利用用途としては，

公共無線ネットワーク，災害時の臨時ネットワーク，ローカルな地方へのブロードバンドの提供などが期待されている．無線メッシュネットワークは現在，様々な研究機関により，試験的な運用などが行われており [1]〜[8] ，IEEE でも 802.11 のタスクグループ s により，無線メッシュネットワークの標準化が進められている [8].

ここで，無線メッシュネットワークを実際に運用する場合，インターネットなど外部ネットワークとの通信が頻繁に行われることが想定され，有線との境界に設置されるゲートウェイ（以下 GW）近傍の帯域がボトルネックとなる可能性がある．また，TCP では端末の所属する AP から GW までのホップ数が多いと通信スループットが大きく低下することが知られている．そのため，無線メッシュネットワークと外部ネットワークの間に複数の GW を設置し，AP からできるだけホップ数の少ない GW を利用する手法の研究が行われている [9]〜[12] ．しかし，この手法では端末の分布が特定の GW 近傍に集中すると，その GW が帯域を使い切る一方で，他の GW は帯域を余らせてしまう．そこで，1 つの AP から複数の GW に接続し，トラヒックを分散する方式が研究されている [13]．文献 [13] では，AP は端末からパケットを受けとった際，各 GW に対する適切な転送比率を計算し，それに従って，パケットごとに異なる GW へ転送する．しかし，この方法では，同一セッションのパケットが複数の GW に分かれるために，各経路の遅延時間の違いによって揺らぎが生じ，TCP 通信のスループットを大きく低下させてしまうという課題がある．

本稿では，この課題を解決するため，パケット単位ではなく，セッション単位で複数の GW へトラヒックを分配する方式を提案する．これにより，GW を効率的に利用し，かつ，パケットの転送遅延を最小限に抑え，TCP 通信のスループット低下を防止することができる．シミュレーションにより提案方式のスループットが向上すること，また公平性も十分保たれることを示す.

以下，3.2 節で既存技術とその課題について，3.3 節で提案方式の説明をする．3.4 節ではシミュレーションによる評価を述べ，3.5 節でまとめる．

3.2 既存技術とその課題

本章では無線メッシュネットワークにおける既存の GW 選択方式を単一 GW 選択方式と複数 GW 選択方式に分けて紹介する．前者は複数の GW の中から最も適切な GW を 1 つだけ選択する方式，後者は複数の GW を同時に選択し，トラヒックを分配する方式である．また，MANET における GW 選択方式も技術的には無線メッシュネットワークの GW 選択方式と同様であるため，これらも既存技術に含めて紹介する．

3.2.1 単一 GW 選択方式

単一 GW 選択方式の手法は単純であり，AP は最もホップ数の近い 1 つの GW を介し，外部ネットワークの端末へパケットを転送する．MANET における GW 選択方式では単一の GW を選択することを基本として研究が行われている [9]〜[11] ．MANET ではパケットの中継機能を持つ端末が移動することが前提であり，経路の安定性を確保するためには，単一 GW 選択方式が適していると考えられる．しかし，端末の分布が 1 つの GW 近傍に集中すると，その GW が帯域のボトルネックとなる一方，他の GW は帯域を余らせてしまう．

また，文献 [12] では，無線メッシュネットワークにおいて，端末の分布に対し，効率的な GW の設置場所を選定することにより，通信スループットの向上を計っている．しかし，実環境では GW の設置場所に制限があることが考えられ，利用環境によっては効果を発揮できない場合がある．

3.2.2 複数 GW 選択方式

単一 GW 選択方式の課題を解決するため，文献 [13] では無線メッシュネットワークにおいて，1 つの AP が複数の GW を利用し，トラヒックを分配する方式を提案している．AP は GW までのホップ数，伝送路の帯域の余裕値などのパラメータから，各 GW へのパケットの適切な転送比率を計算する．AP は端末からパケットを受信すると，上記転送比率に従って各 GW にパケットを分配して転送する．GW はパケットをさらに MGW（Master Gateway）へ転送し，MGW がまとめて外部ネットワークへ転送する．しかし，この方法では異なる GW を利用することによって，同一セッション内のパケットの到達時間に揺らぎが発生する．文献 [13] では TCP 通信の場合にこの揺らぎがどのような影響を与えるかが検討されていない．セッションが TCP のときは揺らぎによりパケット到着順序が逆転すると，パケットロスが発生していなくても端末のふくそう制御機能により再送制御が頻繁に発生する可能性がある．そこで，パケット到着時間の揺らぎを防止するため，外部ネットワークへ転送する前にパケットの順序制御を行う方法が考えれれる．しかし，この方法では転送時間の大きい経路から転送されるパケットに対し，転送時間の小さい経路から転送されたパケットに待ちが生じるため，セッション全体の転送時間が大きくなる．そのため，TCP 通信の場合，スループットが低下してしまうという課題がある．

3.3 提案方式

本稿では，GW へのトラヒック集中を避けるため，複数 GW 選択方式を採用する．さらに，3.2.2 小節に示したパケット単位で複数 GW に分配する方式に対して，セッション単位で分配する方式を提案する．セッション単位で分配することによって，同一セッション内の

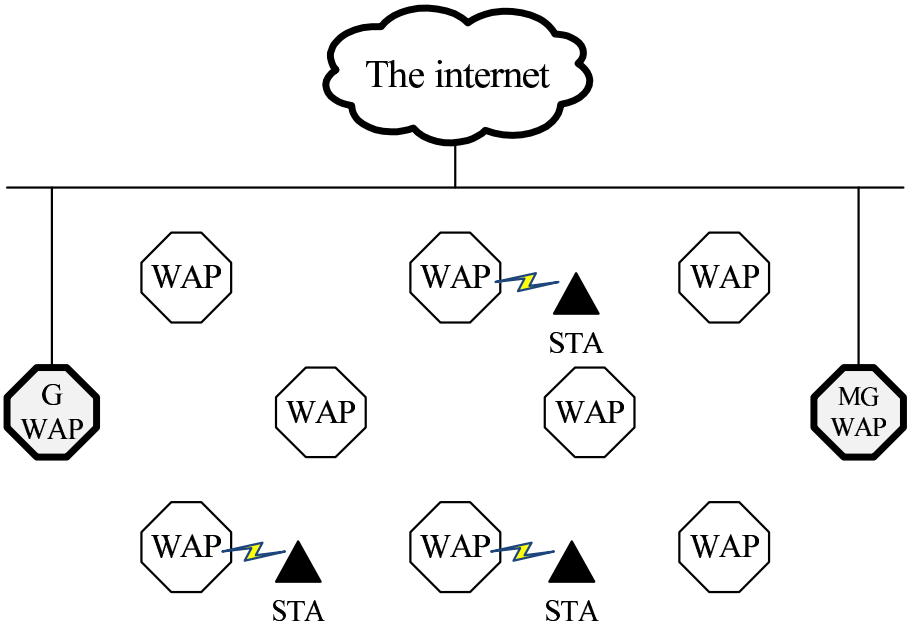

図 3.1　WAPL の全体図

パケット到達時間のゆらぎを避け，TCP 通信によるスループットを改善する．以後，それぞれをパケット分配方式，セッション分配方式と呼ぶ．

パケット分配方式とセッション分配方式を比較評価するため，基盤となる無線メッシュネットワークシステムとして WAPL（Wireless Access Point Link）[1] を用いることとする．WAPL を用いる理由は基本的な無線メッシュネットワークのシミュレーション環境が構築済みであり，提案方式の導入と評価が容易に行えるためである．WAPL の基本的な機能は他の無線メッシュネットワークと同様であり，本研究成果は他の無線メッシュネットワークにも適用可能である．

3.3.1　WAPL

WAPL の全体図を図 3.1 に示す．WAPL では無線化された AP を WAP（Wireless Access Point）と呼ぶ．インターネットと接続するため，有線部と接続する WAP を GWAP（GatewayWAP），パケットを集約して外部ネットワークと接続する GWAP を MGWAP（Master GWAP）と呼ぶ．外部との通信は必ず MGWAP を経由する．GWAP と MGWAP 間の通信は有線で接続し，この間の通信はボトルネックになることはないものとする．MGWAP は GWAP の機能を包含する．

GWAP および MGWAP は常に自身の近傍，つまり無線範囲内のトラヒックの量を測定する．GWAP および MGWAP は近傍のトラヒック量とホップカウントを含むメッセージを定期的にフラッディングする．ホップカウントは各 WAP を中継する毎にその値が加算され

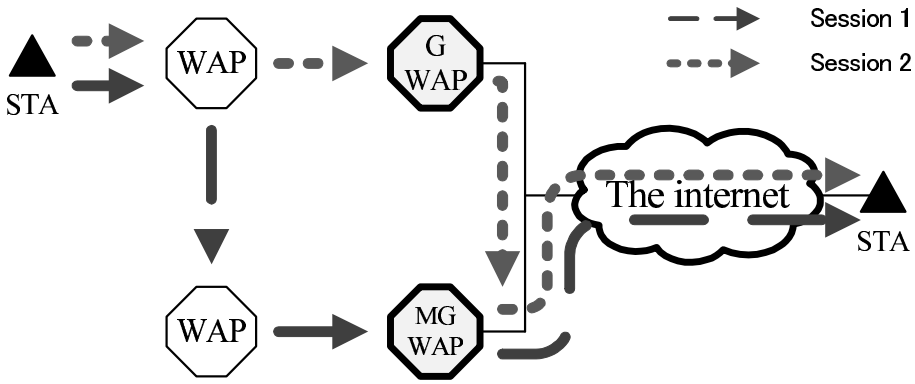

図 3.2 セッション分配方式

る．このメッセージにより，各 WAP はシステム内に複数存在する GWAP および MGWAP の近傍のトラヒック状況と GWAP および MGWAP までのホップ数を把握する．

3.3.2 セッション分配方式

セッション分配方式の概要を図 3.2 に示す．WAP は端末からパケットを受け取ると，パケットの宛先 IP アドレスのネットワーク部が外部ネットワークを示す場合，その時点で保持している各 GWAP の近傍トラヒックとホップ数から，スループット期待値を計算し，その値が最も高い GWAP を最適 GWAP として 1 台だけ選択する．ここで，スループット期待値の計算方法は 3.4.2 小節で説明する．同時に，セッションと最適 GWAP の関係を記憶し，以後の同一セッションのパケットは同一の GWAP に転送する．同一セッションとはコネクション ID（送信元 IP アドレス，宛先 IP アドレス，プロトコル番号，送信元ポート番号，宛先ポート番号）が同一のトラヒックを指す．GWAP は受信したパケットを MGWAP へ転送する．MGWAP はセッションと転送元の GWAP の関係を記憶するとともに，パケットを外部ネットワークの端末に転送する．また，外部ネットワークからのパケットは一度，WAPL の代表 GW である MGWAP へ転送される．外部ネットワークからのパケットは MGWAP が記憶された内容に従って転送することにより，適切な GWAP を介して宛先端末の所属する WAP へ転送される．このようにして，同一セッションの往復は同一経路を通ることができる．別のセッションが開始される場合は，その時点での最適 GWAP が新たに選択される．

外部から通信が開始される場合，MGWAP は外部ネットワークからパケットを受け取ると，システム内の全 WAP に対して現時点での最適 GWAP を問い合わせるメッセージをフラッディングする．目的の端末が所属する WAP は最適 GWAP の IP アドレスを応答する．応答を受けた MGWAP はセッションと GWAP の関係を記憶し，経路が確定する．

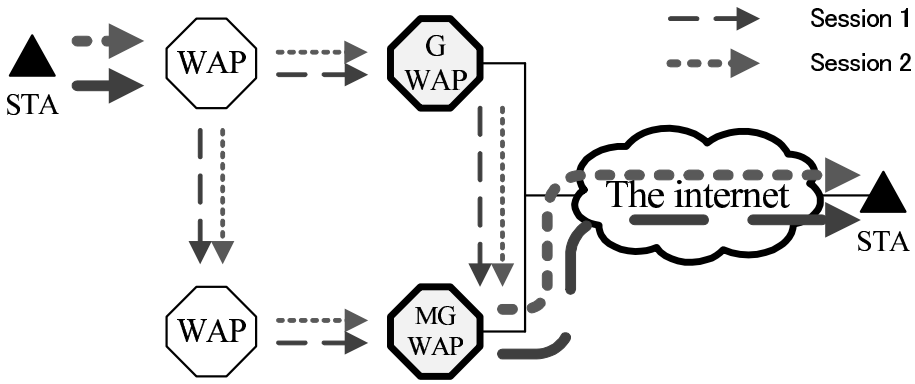

図 3.3 パケット分配方式

3.3.3 パケット分配方式

本小節ではセッション分配方式の効果を明らかにするため，比較対象となるパケット分配方式を WAPL に適用した場合の例を示す．WAPL に適用したパケット分配方式の概要を図 3.3 に示す．WAP は各 GWAP のトラヒックとホップ数から各 GWAP のスループット期待値を計算し，各 GWAP に対する転送比率を決定する．スループット期待値の計算方法はセッション分配方式と同様の方式とする．WAP が端末からパケットを受け取ると，パケットにシーケンス番号を付加し，転送比率に従って，パケットを各 GWAP に分配する．GWAP はこれらのパケットを MGWAP に集約し，MGWAP は外部ネットワークにパケットを転送する．このとき，MGWAP は異なる GWAP から転送されたパケットをバッファリングし，シーケンス番号を元に順序制御を行い，外部ネットワークへ転送する．一定時間シーケンス番号が揃わない場合は，バッファリングのタイムアウトとして，そのまま順序制御されたパケットを外部ネットワークへ転送する．内部から開始された通信に対して，外部から最初のパケットが返ってくる場合，および，外部から通信が開始される場合，MGWAP はパケットを受け取ると，WAP に対して各 GWAP への転送比率を求めるメッセージをフラッディングする．目的の端末が所属する WAP は各 GWAP に対する転送比率を応答する．応答を受けた MGWAP はパケットにシーケンス番号を付加し，転送比率に従って GWAP へパケットを分配する．WAP は異なる GWAP から転送されたパケットをバッファリングし，シーケンス番号を元に順序制御を行い，端末へ転送する．パケット分配方式では分配比率を知る必要があるため，内部から開始された通信であっても外部からのパケットに対して，WAP に転送比率を問い合わせる動作をする．

3.4 シミュレーションによる評価

セッション分配方式の有効性を示すため，ネットワークシミュレータ ns-2（network simulator-2）[14] を用いてシミュレーションを実施した．シミュレーションを可能とするため，ns-2

にいくつかの改造を加えた．また，適切な GWAP を選択するために，予備シミュレーションを用いて，スループット期待値の計算式を求めた．さらに，パケット分配方式の順序制御に利用するバッファのタイムアウト時間が適切となる値を求めた上で，セッション分配方式とパケット分配方式の特性を比較した．比較項目として，スループットとトラヒックの公平性をとりあげた．

3.4.1 シミュレータの実装

ns-2 は研究機関で一般に利用されているフリーソフトである．しかし，ns-2 はアドホックネットワークの機能は充実しているものの，現時点では無線 LAN インフラストラクチャモードの機能が備わっていない．従ってそのままでは無線メッシュネットワークのシミュレーションができない．そこで，ns-2 に以下のような改造を施し，シミュレーション環境を構築した．ns-2 の IEEE802.11 機能実行モジュールにビーコンの発信機能，電波強度により AP を選択する機能，AP 離脱・参入機能を追加した．また，WAPL は WAP がインフラストラクチャモードとアドホックモードの 2 種類のインタフェースをもつ必要があるが，それぞれのインタフェースを持つノードの内部モジュール間のインタフェースどうしを，ネットワークを介さず直接接続することにより，これを実現した．GWAP は同じくアドホックモードと有線の内部モジュール間のインタフェースどうしを直接接続して実現した．さらに，3.3 節で説明したセッション分配方式とパケット分配方式の両方式の機能を実装した．パケット分配方式では，WAPL 内で TCP の順序制御を行う方式と，WAPL では何もせず，エンドエンドの TCP 順序制御に任せる方式を実装した．今回のシミュレーションでは簡単のためインフラストラクチャモード側とアドホックモード側は干渉しないチャネルとした．インフラストラクチャモード側どうしは同一チャネル，アドホックモード側どうしは同一チャネルとした．

3.4.2 スループット期待値

WAP が端末からのパケットを受け取った際に，セッション分配方式であればどの GWAP を最適 GWAP にすべきか，パケット分配方式であれば，GWAP への転送比率をどう決定すべきか判断する方法が必要になる．本研究では，予備シミュレーションによって，WAP と GWAP 間のホップ数，GWAP 近傍トラヒック，および TCP スループットの関係式を求めておき，GWAP のスループット期待値を算出することとした．[15][16] では，TCP スループットの計算式を求める方法として，RTT（Round Trip Time）やパケットロス率などの値を利用する方法が提案されており，これをスループット期待値として利用する方法も考えられる．しかし，RTT やパケットロス率をリアルタイムに取得することは，制御メッセージなどによるトラヒックが大きく影響する無線メッシュネットワークにおいては極めて困難で

表 3.1 シミュレーションパラメータ（1）

背景負荷発生端末	
台数	1〜60 台
通信タイプ	FTP（外部-内部）
	ストリーミング（外部-内部）
	VoIP（外部-内部，内部-内部）
TCP ウィンドウサイズ	128
TCP バージョン	Sack
メッシュネットワーク	
WAP 台数	37 台
電波到達距離	100m
WAP 間の距離	80m
フィールド	860x580（m）
MAC プロトコル	IEEE802.11g

ある．そのため，今回は予備シミュレーションにより，GWAP 近傍のトラヒック量とホップ数の関係からスループット期待値を算出する方法が最適であると考えた．この予備シミュレーションによってスループット期待値の指標を得ることができ，GWAP に重みをつけることができる．ここで求めたスループット期待値を用いて以後の比較を行うこととする．

予備シミュレーションでは，背景負荷となるトラヒックを発生させた上で，1 台の特定端末により，内部と外部の間で TCP セッションを確立し，スループットを測定した．特定端末が所属する WAP と GWAP 間のホップ数，GWAP 近傍トラヒックと特定端末が得た TCP スループットの関係から一次方程式を導いた．この式を導くために使用したシミュレーションパラメータを表 3.1 に，シミュレーションフィールドを図 3.4 に示す．

WAP の台数は 37 台とし，WAP どうしの距離はすべて等間隔の 80m で近隣の WAP が六角形を作るように配置した．GWAP どうしを接続するネットワークは同一ネットワークアドレスを持つことを想定し，帯域を 100Mbps，遅延を 20μs とした．GWAP どうしを接続するネットワークの外側はインターネットを想定し，帯域を 100Mbps，遅延を 20ms とした．背景負荷を発生させるための端末を WAPL 内に複数台設置した．背景負荷用端末の台数を調整し，トラヒック量を変化させた．背景負荷用端末が発生するセッションは外部との FTP 通信，外部から受信するストリーミング通信，内部端末どうしの VoIP 通信，内部と外部の端末間の VoIP 通信を想定した．これらのセッションの比率はシステムにより異なるものであるが，様々なアプリケーションが均等に存在することを仮定し，端末の台数に関わらず，1:1:1:1 のトラヒック量とした．

シミュレーションによって得た GWAP 近傍トラヒックと TCP スループットの関係（GWAP-

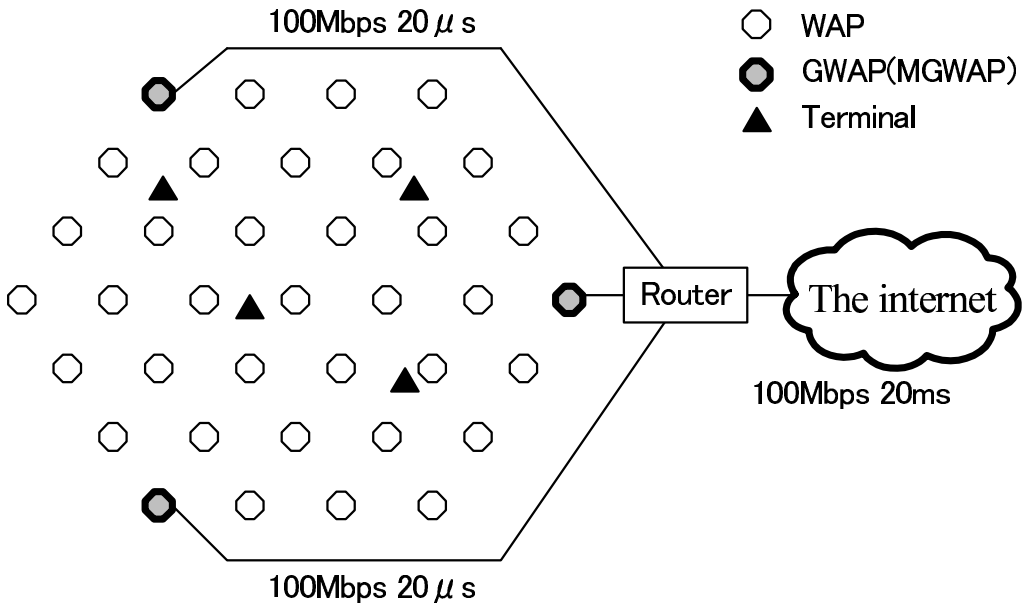

図 3.4 シミュレーションフィールド

表 3.2 スループット期待値計算式

ホップ数	一次方程式
1	$-0.68x + 3.50$
2	$-0.26x + 1.11$
3	$-0.11x + 0.36$
4	$-0.19x + 0.26$
5	$-0.12x + 0.18$

WAP 間が 3 ホップの場合）を図 3.5 に示す．縦軸が TCP スループット，横軸が GWAP 近傍のトラヒックを示している．これらのデータから最小 2 乗法により 1 次関数の近似曲線を計算し，導いた一次方程式は $y = -0.11x + 0.36$ となった．ここで，x は GWAP 近傍トラヒックを示し，y はスループット期待値である．同様にして，ホップ数と GWAP 近傍トラヒックを変化させ，表 3.2 に示すようにホップ数ごとのスループット期待値計算式を求めた．以降のシミュレーションでは，ここで得た一次方程式を使用し，セッション分配方式では GWAP の選択，パケット分配方式では GWAP への転送比率を決定するものとした．

3.4.3 パケット分配方式の最適条件の調査

パケット分配方式では，WAPL 内での順序制御による遅延がスループット低下を引き起こす可能性が考えられる．そのため，パケット分配方式におけるスループットの低下をできるだけ防ぐには，順序制御に利用するバッファのタイムアウト時間を適切に設定する必要が

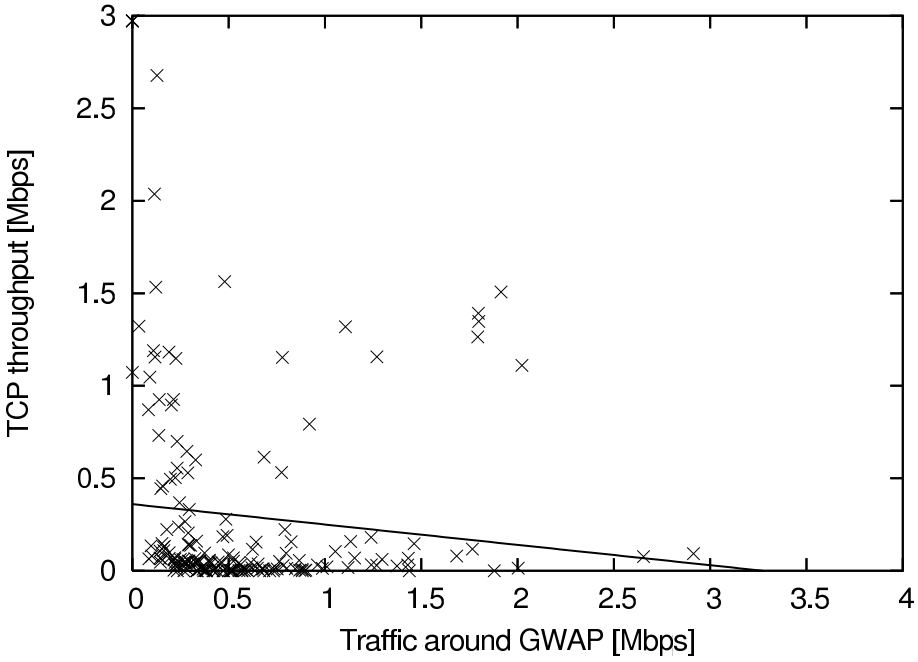

図 3.5 GWAP 近傍トラヒックと TCP スループットの関係（3 ホップ）

ある．バッファのタイムアウト時間が小さいと，遅延は小さくなるものの，順序不整合が多くなるという関係にある．そこで，WAPL 内での順序制御に利用するバッファのタイムアウト時間を調節し，TCP スループットが最も大きくなる条件を調査した．さらに，WAPL 内で順序制御を行わず，エンドエンドの順序制御に任せる場合についても比較した．スループット測定時のシミュレーションフィールドを図 3.6 に，シミュレーションパラメータを表 3.3 に示す．経路を一定に保つため，フィールドには横一列に GWAP と MGWAP を 1 台ずつ，WAP を 5 台設置した．GWAP と MGWAP は列の両端に配置した． GWAP どうしを接続するネットワークは同一ネットワークを想定し，帯域を 100Mbps，遅延を 20μs とした．GWAP どうしを接続するネットワークの外側はインターネットを想定し，帯域を 100Mbps，遅延を 20ms とした．TCP ウィンドウサイズは 128，TCP バージョンは Sack を使用した．

端末 1 台を A の位置に設置し，バッファリングのタイムアウトがそれぞれ 15ms，10ms，5ms，1ms の場合と順序制御なしの場合で 30s 間の TCP スループットを測定した．WAP から GWAP と MGWAP への経路はそれぞれ 3 ホップとなり，パケットは 1:1 の割合で交互に送信される．シミュレーションの結果を表 3.4 に示す．バッファリングのタイムアウト時間が 5ms のときスループットが最も高くなることがわかる．ここで，高速再送制御と TCP タイムアウトの回数に注目すると，5ms においては TCP タイムアウトがなく，かつ高速再送制御の回数が少ないことがわかる．5ms より長いと，順序制御の精度が高いため，高速再送制御は発生しなくなるが，バッファにパケットが滞留する時間が長くなるため，TCP タイムアウトが発生しやすくなる．5ms より短いと，順序制御が完全に行われる前に，転送さ

表 3.3 シミュレーションパラメータ（2）

背景負荷発生端末	
通信タイプ	FTP
TCP ウィンドウサイズ	128
TCP バージョン	Sack
メッシュネットワーク	
WAP 台数	7 台
電波到達距離	100m
WAP 間の距離	80m
フィールド	1000x400（m）
MAC プロトコル	IEEE802.11g

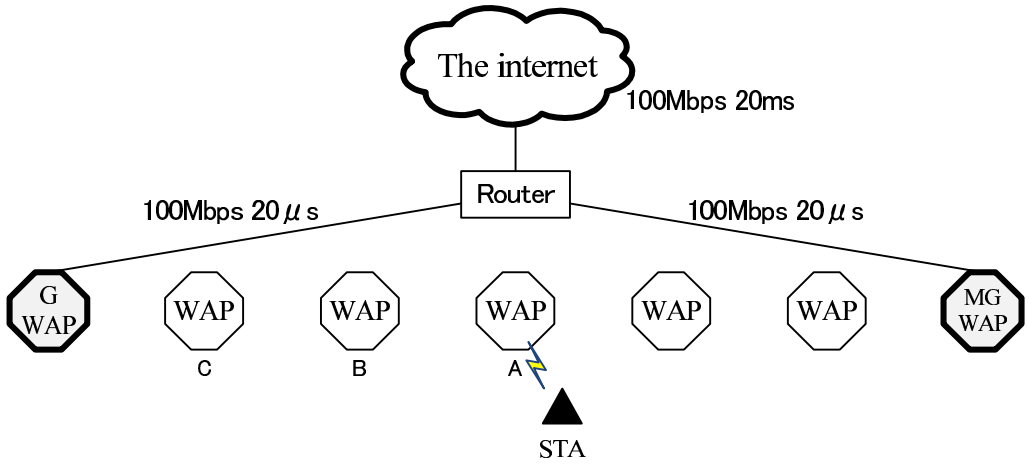

図 3.6 スループット測定時のシミュレーションフィールド

れてしまうため，TCP タイムアウトは発生しないが，順序不整合が多発し，高速再送制御が発生しやすくなる．パケットロスに注目すると，TCP の ACK パケットにロスが発生している．これは ACK パケットが GWAP（MGWAP）から中央の WAP に転送される内側向きの経路をとっており，外側向きの DATA パケットより衝突の発生機会が多いためといえる．また，ロスしているパケットが ACK であるため，今回のケースではパケットロスが TCP タイムアウトの発生回数に与える影響は出ない．以上より，パケット分配方式において高いスループットが期待できるバッファリングのタイムアウト時間の目安を 5ms として今後のシミュレーションを行う．

表 3.4 バッファリング時間による比較

	バッファリングタイムアウト（ms）	スループット（Mbps）	高速再送制御（回）	TCP タイムアウト（回）	パケット損失（%）	
					DATA	ACK
順序制御あり	15	4.19	2	18	0	0.21
	10	4.49	8	11	0	0.29
	5	4.72	32	0	0	0.13
	1	3.71	41	0	0	0.01
順序制御なし	0	3.45	41	0	0	0.02

3.4.4 TCP スループットの評価

セッション分配方式とパケット分配方式が TCP スループットに与える影響をシミュレーションによって詳しく解析した．それぞれの分配方式の動作の特徴を示すため，既に 1 セッション分のトラヒックが発生しているときに，端末が新たに通信を開始するシナリオを作成した．シミュレーションフィールドにおける WAP，GWAP，MGWAP の配置は 3.4.3 小節で示した図 3.6 と同様であり，シミュレーションパラメータは表 3.3 と同様である．図 3.6 のネットワーク上に，端末 1 と端末 2 を設置する．端末 1 は外部に対して TCP 通信によるセッション 1 を開始する．その 10 秒後に，端末 2 は外部に対して TCP 通信によるセッション 2 を開始し，その 30 秒後までのスループットを測定する．最初の端末は，図 3.6 に示す A，B，C の 3 通りの位置に設置された場合を測定する．もう一方の端末は C の位置に固定とする．10 回の試行から TCP スループットの平均を算出した．シミュレーションの結果を表 3.5 に示す．セッション 1 とセッション 2 の合計に注目すると，全てのケースにおいてセッション分配方式の方がパケット分配方式よりも高いスループットを実現していることがわかる．特に端末 1 の位置が C の位置に近いほど，両者の差は大きくなる．パケット分配方式では，3.4.3 小節に示したようにスループットの低下はパケットの順序不整合の度合に影響される．C の位置に近づくほど，セッション 1 ではホップ数の小さい GWAP への転送比率が高くなり，順序不整合の発生率が少なくなるため，スループットは比較的高い．しかし，2 つの両セッションが両 GWAP（MGWAP）への経路を利用するため，互いのトラヒックが負荷となり，順序不整合を発生させ，全体的にセッション分配方式よりもスループットが低くなる．また，C の位置でセッション 2 のスループットが若干向上している理由は，セッション 1 の MGWAP 側への転送比率が低くなり，セッション 2 への影響が小さくなったためである．次に，セッション分配方式では単純にセッション 1 は C の位置へ近いほどスループットが向上し，セッション 2 はほぼ一定である．これはセッション 2 がセッション 1 のトラヒックを避けるように経路を選ぶためである．また，両方式において，両セッションの両 GWAP（MGWAP）までのホップ数が同じ A の位置でも，セッション 2 の方がセッション 1 よりも小さい理由は，セッション 1 の方が早く通信を開始し，背景負荷のかからない時間が長かったためである．以上のように，分配の動作の特徴が顕著に表れる単純な構成で，

表 3.5 スループットの比較

端末 2 の位置		A	B	C
パケット	セッション 1	3.1	4.1	4.5
分配方式	セッション 2	2.5	2.0	3.8
	合計	5.6	6.1	8.3
セッション	セッション 1	3.4	6.4	13.3
分配方式	セッション 2	2.9	2.3	2.5
	合計	6.3	8.7	15.8

単位 [Mbps]

2 方式を比較したところ，セッション分配方式の方が高スループットを実現できることがわかった．

3.4.5 様々なトラヒックが混在したときの総合スループットとラヒック公平性

実際のメッシュネットワークにおいて，様々なトラヒックが混在したときの影響を調べるために，3.4.2 小節と同様の条件でネットワークを構築し，トラヒックを発生させたときのシミュレーションを行った．無線メッシュネットワーク内部と外部の間で流れるパケット転送量と，内部に流れるトラヒックの分布の公平性を評価した．ここでいう公平性とは，各 WAP に流れるトラヒックの量がどれほど公平かを示す．内部と外部の間を流れるパケット量は MGWAP の総スループットを測ることで得られる．また，ネットワークトラヒックの公平性を評価する理由は，セッション分配方式では，パケット分配方式よりも分配の単位が粗いため，ネットワーク全体のトラヒックの公平性を低下させ，各通信のスループットに影響を与える可能性があるためである．シミュレーションパラメータ，およびトラヒックの発生方法は 3.4.2 小節と同様であり，この状態で，WAP にセッション分配方式を適用した場合と，パケット分配方式を適用した場合を比較した．また，GWAP は 2 台，MGWAP は 1 台とした．1〜60 台の各端末数において，3 回ずつシミュレーションを行った．

図 3.7 にセッション分配方式，図 3.8 にパケット分配方式における MGWAP の総合スループットを示す．グラフには，目安として 4 次式による近似曲線を加えた．近似曲線に注目すると，セッション分配方式は，端末数 10 台以降は約 10〜12Mbps の総合スループットを示している．パケット分配方式は端末数 10 台程度のとき，総合スループットが最大となり，約 4Mbps を示し，端末数が多くなるに従い約 1Mbps まで減少した．このようにセッション分配方式が優れた結果となった理由は TCP のトラヒックが大きく影響しており，パケット分配方式ではパケット到着時間の揺らぎが大きく影響したためと考えられる．セッション分配方式において，スループットが 12Mbps 程度に抑えられた理由は，GWAP および MGWAP 周辺の帯域が限界まで使われているためである．

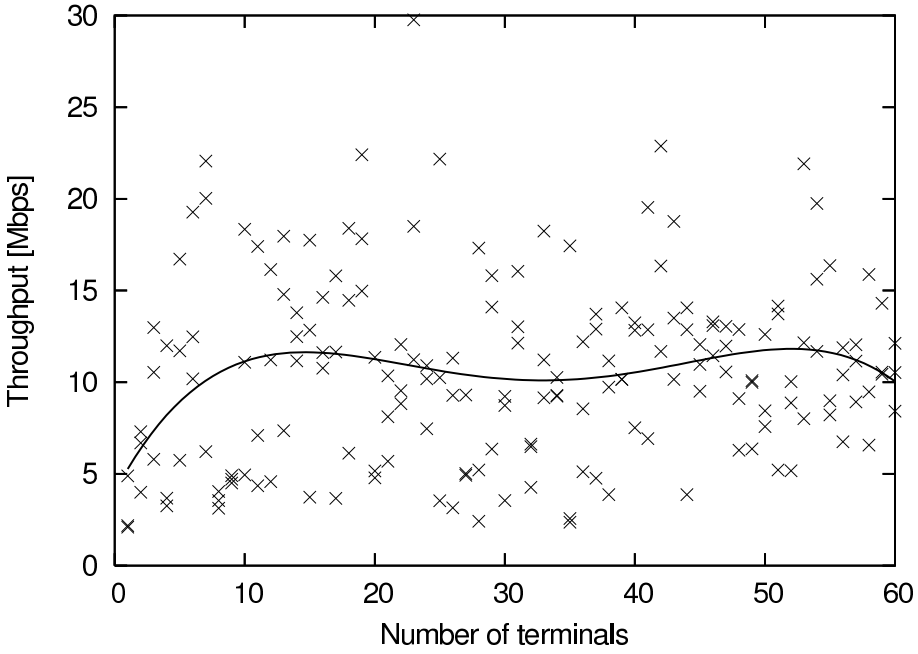

図 3.7 セッション分配方式における MGWAP での総合スループット

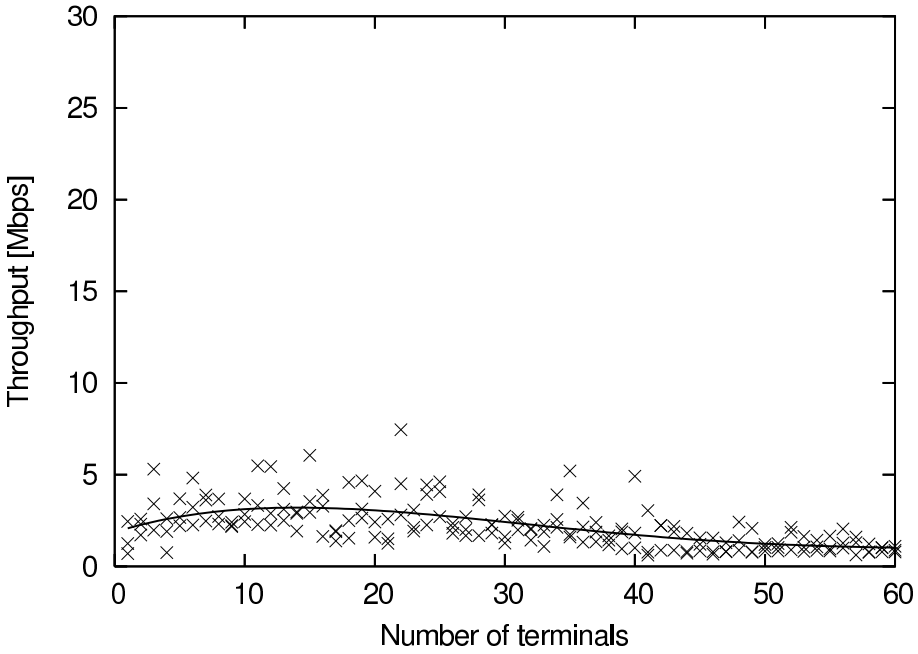

図 3.8 パケット分配方式における MGWAP での総合スループット

次に，各 WAP に流れるトラヒックの公平性の評価した．公平性の評価には文献 [17] による以下の式を利用した．

$$FI = \frac{(\sum_{i=1}^{n} x_i)^2}{n \sum_{i=1}^{n} (x_i)^2} \tag{3.1}$$

FI（FairnessIndex）の値は 1 に近いほど公平性が高い．n は全 WAP の台数，xi は WAPi の転送トラヒックを示す．

図 3.9 にセッション分配方式，図 3.10 にパケット分配方式における FI のグラフを示す．それぞれの横軸はトラヒック発生用の端末の台数，縦軸は FI を示す．グラフには，目安として 4 次式による近似曲線を加えた．線形近似曲線に注目すると，端末数が 30 台程度の場合ではパケット分配方式の FI が約 0.24，セッション分配方式の FI が約 0.17 を示しており，パケット分配方式が優勢といえる．しかし，端末数が 60 台に近づくとパケット分配方式の FI は約 0.2 に収束し，セッション分配方式の FI は約 0.23 となり，ほぼ同じ程度の値となっている．これは，分配の単位の荒いセッション分配方式でもセッション数が多ければ，十分に公平性が高くなるためである．セッション数が少ないときは 1 つのセッションが他のセッションの影響を受ける確率は低く，セッション数が多いときほど，無駄なくネットワーク資源を利用することが重要であるため，セッション分配方式は十分に分配の効果を発揮しているといえる．

以上から，セッション分配方式はパケット分配方式に対して，公平性も問題なく，大幅に MGWAP における総スループットを改善しているといえる．

3.5 まとめ

本稿では，無線メッシュネットワークと外部ネットワークとの通信における TCP スループットの向上と GW の効率的な利用を目的とし，セッション分配方式を提案した．パケット分配方式の順序制御のためのバッファリングのタイムアウト値を適切に設定した上で，パケット分配方式とセッション分配方式の比較評価を行った．その結果，セッション分配方式はパケット分配方式より TCP スループットが改善され，その理由も定性的に説明できることがわかった．外部ネットワークとの総スループット特性においてはセッション分配方式の方が大幅に改善されることがわかった．さらに，ネットワークトラヒックの公平性において，セッション分配方式はパケット分配方式と比較しても大きな差がないことを示した．今回はスループット期待値の計算式を求めるために，予めシミュレーションを行うという方法を採用した．しかしながら，3.4.3，3.4.4 小節の評価よりパケット分配方式における TCP スループット低下の理由はパケットの順序不整合による再送制御の多発であることがわかった．すなわち，TCP スループットを維持するには 1 つのセッションを複数の経路に分配しないことが重要である．そのため，スループット期待値の計算方法に関わらず，セッション分配方

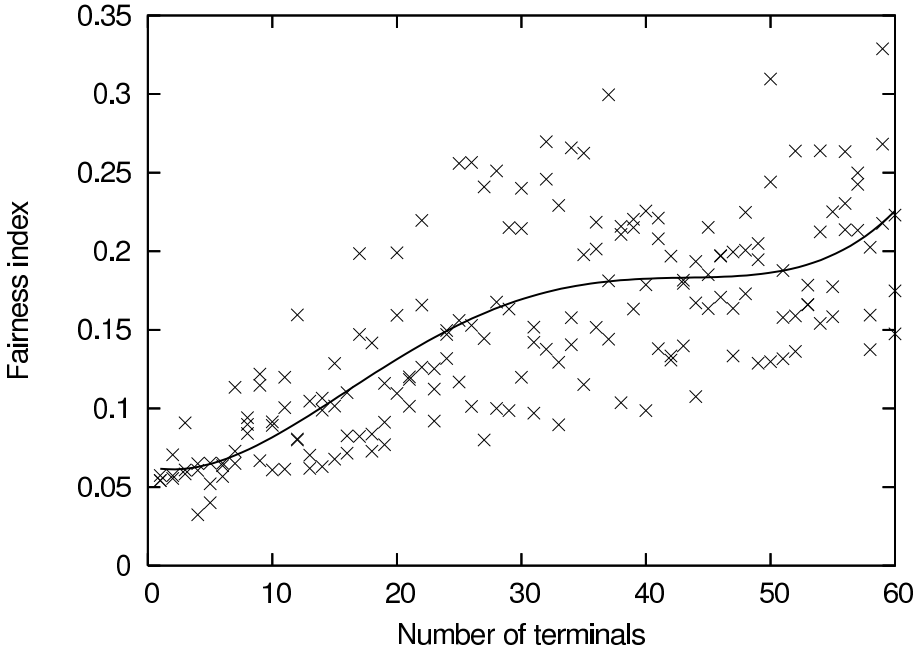

図 3.9 セッション分配方式における Fairness Index

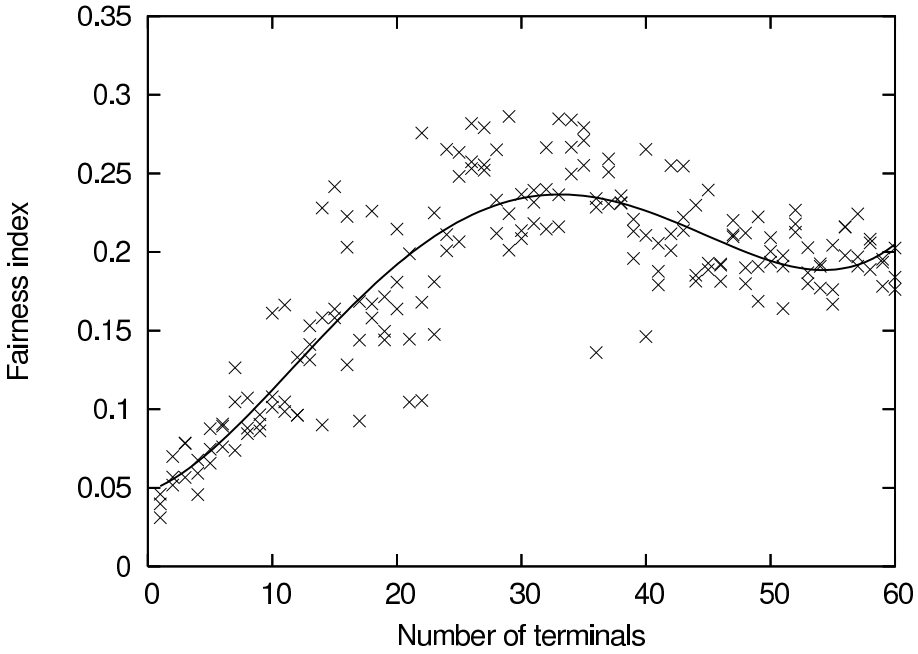

図 3.10 パケット分配方式における Fairness Index

式がパケット分配方式よりも TCP スループットにおいて優れていると考えられる．今回は無線メッシュネットワークの基盤として WAPL を利用したが，セッション分配方式の概念は無線メッシュネットワークの基本動作とは独立しており，他の無線メッシュネットワークにも適用可能である．今後はセッション分配方式を実機に実装し，評価を行う予定である．

参考文献

[1] 伊藤将志，鹿間敏弘，渡邊　晃：無線メッシュネットワーク ”WAPL ”の提案とシミュレーション評価，情報処理学会論文誌， Vol. 49, No. 6 (2008).

[2] 大和田泰伯，照井宏康，間瀬憲一，今井博英：マルチホップ無線 LAN の提案と実装，電子情報通信学会論文誌 B， Vol. J89-B, No. 11, pp. 2092–2102 (2006).

[3] MetroMesh:
http://www.tropos.com/.

[4] MeshCruzer:
http://www.thinktube.com/.

[5] Packethop:
http://www.packethop.com/.

[6] Amir, Y., Danilov, C., Hilsdale, M. et al.: Fast Handoff for Seamless Wireless Mesh Networks, *ACM MobiSys* (2006).

[7] Navda, V., Kashyap, A. and Das, S. R.: Design and evaluation of iMesh: an infrastructure-mode wireless mesh network, *World of Wireless Mobile and Multimedia Networks*, pp. 164–170 (2005).

[8] IEEE802.11:
http://grouper.ieee.org/groups/802/11/.

[9] Wakikawa, R., Malinen, J. T., Perkins, C. E., Nilsson, A. and Tuominen, A. J.: Global connectivity for IPv6 Mobile Ad Hoc Networks, *draft-wakikawa-manet-globalv6-05* (2006).

[10] Jelger, C., Noel, T. and Frey, A.: Gateway and address autoconfiguration for IPv6 adhoc networks, *draft-jelger-manet-gateway-autoconf-v6-02* (2004).

[11] Ruffino, S. and Stupar, P.: Automatic configuration of IPv6 addresses for MANET with multiple, *draft-ruffino-manet-autoconf-multigw-03* (2006).

[12] Tajima, S., Higashino, T. and Funabiki, N.: An Internet Gateway Access-Point Selection Problem for Wireless Infrastructure Mesh Networks, *2006 International Workshop on Future Mobile and Ubiquitous Information Technologies (FMUIT'06)* (2006).

[13] Lakshmanan, S., Sundaresan, K. and Sivakumar, R.: On Multi-Gateway Association in Wireless Mesh Networks, *WiMesh 2006;Second IEEE Workshop on Wireless Mesh Networks*, pp. 64–730 (2006).

[14] ns2:
http://www.isi.edu/nsnam/ns/.

[15] Floyd, S. and Fall, K.: Promoting the use of end-to-end congestion control in the Internet, *IEEE/ACM Transactions on Networking (TON)*, Vol. 7, pp. 458–472 (1999).

[16] Padhye, J., Firoiu, V., Towsley, D. and Kurose, J.: Modeling TCP throughput: a simple model and its empirical validation, *ACM SIGCOMM Computer Communication Review*, Vol. 28, pp. 303–314 (1998).

[17] Jain, R.: The art of computer systems performance analysis, *John Wiley Sons* (1991).

4章　ファイアウォールやNATを通過できるIP電話の提案と評価

あらまし

通信基盤の発達により，IP電話は実用レベルの品質を確保できるようになった．しかし，グローバルネットワークと企業ネットワークの間には，ファイアウォールやNATが存在し，自由かつ安全にIP電話を利用することは困難である．本論文では2台のリレーエージェントをグローバルネットワーク環境と企業ネットワーク環境に設置し，HTTPトンネルを生成することによりVoIP通信のファイアウォールやNATを通過できるIP電話システムSoFW（SIP over FireWall）を提案する．これまでの類似の研究や解決方法では，専用端末が必要であったり，アドレス空間の統一的管理が必要であるなどの課題があった．SoFWは既存のSIP端末を利用することができ，アドレス空間の統一的管理が必要なく，導入が容易であるという特長がある．SoFWをLinux上に実装し，評価実験を行った結果，その有用性を確認することができたので報告する．

4.1　はじめに

ブロードバンドの普及やバックボーンの整備により，ネットワークの伝送容量が大幅に増加し，IP電話は十分な通信品質を確保できるようになった．これに伴い，多くの企業は通話料金の削減や，IP電話特有の機能，アプリケーションとの連携による生産性向上を期待して社内LANへのIP電話導入を進めてきた．

しかし，企業ネットワークには外部ネットワークとの間にファイアウォール[1]やアドレス変換装置（Network Address Translator:以下NAT）[2]が存在するため，企業ネットワークとその外部のネットワークに接続した端末どうしで自由にVoIP（Voice over IP）を利用することができない[3]．企業ネットワークと外部のネットワーク間においてVoIPが自由かつ安全に利用できるようになればIP電話の利便性はさらに向上するものと考えられる．

VoIPのセッション開始プロトコルとしては，電話仕様をベースとして早期にITU-T(International Telecommunication Union - Telecommunication)によって標準化されたH.323[4]がある．しかし，現在はIETF （Internet Engineering Task Force）によって標準化されたSIP （Session Initiation Protocol）[5]が実装も容易で拡張性に優れており，様々なマルチメディア・サービスに利用できるため注目されている．現在，ISPが提供しているIP電話のほとんどがSIPを採用している．SIPは主にユーザエージェントとSIPサーバで構成されており，SIPサーバにユーザエージェントの位置情報を登録し，この位置情報をもとに呼設定のためのメッセージの中継を行う機能を提供する．しかし，SIPは呼設定開始時に相手端末のIPアドレスが特定できるか，相手端末の属するSIPサーバのIPアドレスが特定できることが必須である．そのため，NATが介在するような環境では呼設定を開始できないという課題がある．また，企業などのファイアウォールは多くの場合，メールや内部から外

部へのWebサーバアクセスなどに通信を限定しており，それ以外の通信を遮断してしまう．このような制限を受けたネットワークにIP電話を導入し，外部との通話に利用しようとすると，企業のセキュリティポリシの変更が必要になり，ファイアウォールの設定変更の稼動やセキュリティ上のリスクが増加する．

そこで，ファイアウォールやNATなどによってIP電話としての機能を制限されることのないシステムがいくつか提案されている．これらはファイアウォールの許可する通信を動的に操作する方法と，HTTPなどのあらかじめファイアウォールが通信を許可しているプロトコルを利用して通信する方法の2種類に分けられる．前者はIETFでもいくつかの関連技術が提案されている [6]〜[10] ．この方式はピンホール・ファイアウォールと呼ばれ，例として [11] ではファイアウォールがSIPによる呼設定を監視し，その呼設定によって開始される音声通信のみを許可するようにフィルタ処理を動的に変更する．しかし，音声通信では不特定多数のIPアドレスとポート番号を使ったUDPの通信が利用されるため，ピンホール・ファイアウォールは企業によってはセキュリティポリシの変更が必要となる．また，ファイアウォールへのモジュール追加や新規のVoIP専用ゲートウェイ設置が必要とされるため，導入には手間がかかる．後者の代表的なシステムとしてHCAP[12]，Skype[13] などのIP電話専用システムと，全アプリケーションに適用できるSoftEther（現在ではPacketiX VPNと名称が変更されている）[14] がある．HCAPやSkypeはファイアウォールの外側に設置された中継サーバと電話端末間でHTTPトンネルを張ることにより，Webを閲覧できる環境であればIP電話による通話が可能になる．しかし，端末に特殊な機能が必要なため，企業ネットワークに導入するにはIP電話端末の総入替えが必要である．

SoftEtherはファイアウォール外部の仮想HUBというソフトウェアとファイアウォール内部の仮想LANカードというソフトウェア間でHTTPSなどのトンネルを張り，仮想的なイーサネット環境を構築することができる．しかし，この方法は仮想的なイーサネット内でのIPアドレスとMACアドレスの統一的管理を要すること，内部のネットワークが外部にさらされる危険があるなどの課題があり，企業ネットワークのIP電話として利用するには適していない．

現時点で市場に出ているファイアウォール対応SIP applianceやSIP-NAT対応ファイアウォールとしては下記のようなものがある．

[15] では2台の中継装置によってSIP通信のファイアウォール越えを可能にする．2台の中継装置間ではNATを通過するためにUDPホールパンチング [16] を用いた音声の経路を生成する．このため，ファイアウォールにはUDPを通過させるための設定変更が必要になり，企業のセキュリティポリシに影響を与える．[17] ではルータとして設置された装置がSIPに含まれる情報から，アドレス変換の操作やピンホール・ファイアウォールの設定を動的に変更して音声の通過を可能にする．しかし，UDPホールパンチングの場合と同様にUDPを通過させるため，企業のセキュリティポリシの変更が必要となる．また，ルータの取替えが必要で，導入には手間がかかる．

本論文ではファイアウォールの内部と外部に 1 台ずつリレーエージェントと呼ぶ装置を設置し，その間に呼設定用と音声ストリーム用に HTTP トンネルを張り，すべての端末からの SIP メッセージと音声ストリームをこのトンネルに通す SoFW（SIP over FireWall）を提案する．これを実現するために，呼設定時の SIP のメッセージボディを書き換え，SIP 端末が音声ストリームをトンネルに向けて送信するように誘導する．SoFW は既存のネットワーク機器に影響を与えないため導入が容易であり，既存の SIP 端末をそのまま利用できる．また，IP アドレス管理にもいっさい影響を与えない．将来的には，音声通信に限らず，様々な SIP 端末への応用が可能である．SoFW を実装し性能評価を行った結果，実用に耐え得る性能を発揮できることを確認した．以下，4.2 節で既存技術とその課題について説明し，4.3 節で SoFW の概要と実現方法について述べる．4.4 節では実装方式について説明し，4.5 節で評価，4.6 節でまとめとする．

4.2 既存技術とその課題

ファイアウォール（以下 FW）を通過する既存技術として HCAP と SoftEther をとりあげ，その方式と課題について簡単に説明する．なお SoftEther はすべてのアプリケーションで FW ／ NA(P)T を通過できるシステムであるため，SoftEther により形成された仮想的なイーサネット環境上に IP 電話に必要な装置を設置する場合を想定した．

4.2.1 HCAP

HCAP の概念図を図 4.1 に示す．HCAP では FW の DMZ (DeMilitarized Zone) 上などのグローバルなアドレス空間に中継サーバを設置し，プライベートアドレス空間となる企業ネットワーク内には HCAP 対応機能を内蔵した端末を設置する．HCAP 端末立ち上げ時に端末から中継サーバへ HTTP で接続して，トンネル経路を作る．HTTP の CGI (Common Gateway Interface) の機能を利用して，セッションの開始を行い，Inbound の音声ストリームは HTTP の GET メソッドに対するレスポンスに，Outbound の音声ストリームは POST メッセージに埋め込んで中継する．HCAP は外部の Web サイトを閲覧できる環境であれば，FW ／ NAT を通過できる．また，グローバルアドレス空間上の端末に対しては UDP の利用もできる．HCAP は，個々の端末が HCAP 機能を保持するか，回線交換タイプの既存電話機をアダプタにより収容する方法がある．HCAP は電話端末が FW を越えて通信できるようにすることが目的であり，呼設定および音声通信とも中継サーバを経由した通信となるように独自の手順が定義されている．そのため，SIP 端末との互換性は考慮されていない．SIP 端末対応のアダプタを準備しようとすると，プロトコル変換が必要となるため処理が煩雑になる．

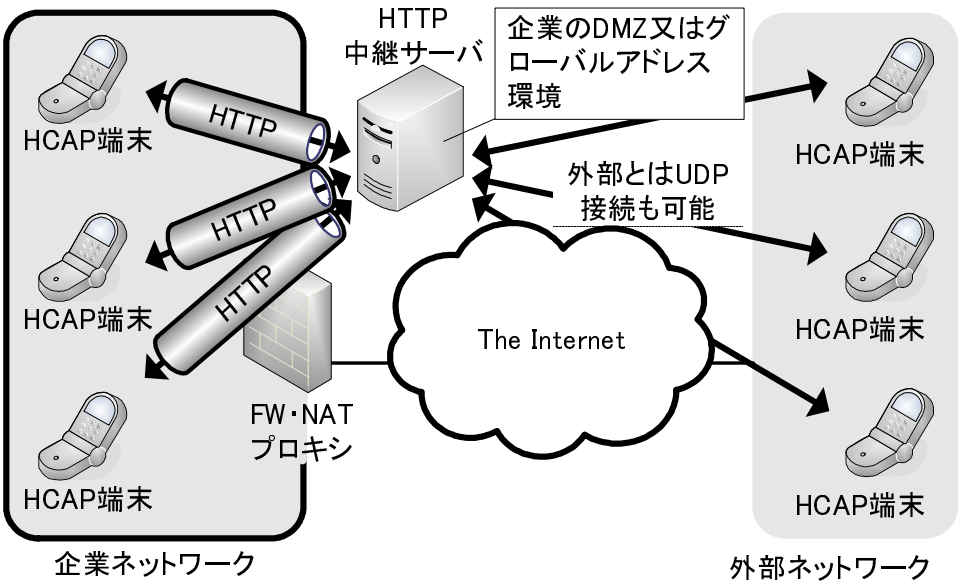

図 4.1 HCAP の概念図

4.2.2 SoftEther

図 4.2 に SoftEther による仮想的なイーサネット上で SIP による IP 電話ネットワークを構築した例を示す．SoftEther は FW 内部の端末に仮想 LAN カードと呼ばれる機能を，外部のサーバ端末に仮想 HUB と呼ばれる機能を組み込む．通信に先立ち仮想 LAN カードは仮想 HUB に対して HTTPS や SSH などの FW を越えられるプロトコルで接続し，トンネルを作る．このとき仮想 LAN カードには仮想 MAC アドレスと仮想 IP アドレスが割当てられる．仮想 LAN カードはトンネルにイーサフレームごと埋め込んで送信し，仮想 HUB がイーサフレームの経路決定を行い，該当する端末に転送することにより仮想的なイーサネット環境を作る．各端末はこの仮想的なイーサネット環境を利用して，FW/NAT の有無に関わらずあらゆる通信を自由に行うことができる．また，仮想 LAN カードを導入した端末と通常のイーサネットをブリッジ接続することにより，ネットワークごと外部に繋ぐことも可能である．仮想的なイーサネット環境上で IP 電話を利用するには仮想的なイーサネット環境上に IP 電話要素を導入すればよい．しかし，この方式では本来 FW に守られているはずのネットワークを危険にさらしてしまうため FW の意味がなくなる．また，仮想的なイーサネット環境上の IP アドレスや MAC アドレスを統一的に管理する必要があり，企業ネットワークの IP 電話として利用するのは難しい．

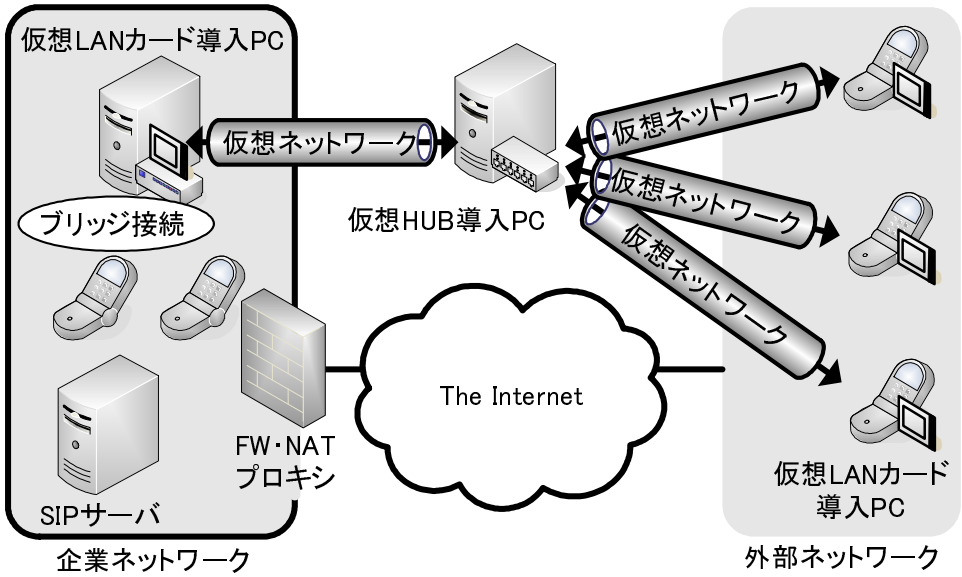

図 4.2 仮想的なイーサネット上での IP 電話ネットワーク構成例

4.3 SoFW

4.3.1 SoFW の概要

SoFW は標準の SIP 対応の音声端末を対象とする．SIP 端末は LAN に直結され，音声端末としてだけでなく様々なアプリケーションを実行できる．SoFW は，このような SIP で構成された既存のネットワーク環境にいっさい手を加えないまま，FW を越えた通信が可能になる．本論文では音声に着目しているが，将来的にはそれ以外の様々な SIP 端末への応用が想定できる．

SoFW の構成を図 4.3 に示す．SoFW では SIP サーバの代わりに内部のプライベートアドレス環境上に HRAC（Half Relay Agent Client），外部 のグローバルアドレス環境上に SIP サーバ機能を備えた HRAS（Half Relay Agent Server）を設置する．システム立ち上げ時において，HRAS と HRAC は SIP メッセージと音声ストリームを中継するためのトンネルを生成する．呼設定時において HRAS および HRAC は SIP 端末からグローバル IP アドレスとプライベート IP アドレスのインタフェースを持つ仮想的な一つの SIP サーバのように見える．音声通信時は SIP メッセージから得た情報から音声ストリームのグローバル IP アドレスとプライベート IP アドレスおよびそれらのポート番号を変換して中継する．SoFW では，端末とは独立して HTTP トンネルを設置するため，既存の SIP 端末をそのまま利用することができる．これは企業がすでに SIP ネットワークを構築していた場合，特に有効である．さらに IP アドレスの管理形態をまったく変える必要がなく，SIP に限定した安全な通話ができる．

SIP 対応の音声端末では，呼設定後の音声通信を SIP サーバを介さずにエンドツーエンド

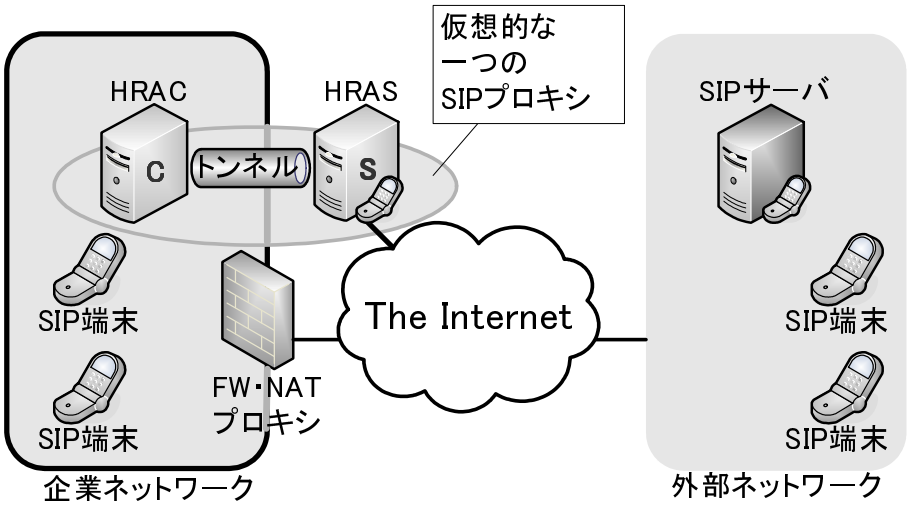

図 4.3 SoFW の構成

で実行する．そのため，FW を越えるためには，音声ストリームをエンド端末宛てでなく，HRAS/HRAC に向けて誘導する必要がある．SoFW ではこれを実現するために，呼設定時に SIP のメッセージボディ（SDP）を HRAS/HRAC が書き換え，エンド端末に対して通信相手が HRAS/HRAC であるかのように見せかける．このようにしてエンド端末は音声データを HRAS/HRAC に送信することになり，音声ストリームが FW を越えられるようになる．以下の記述においては，4.3.2 小節は FW を越える多くのシステムが採用しているトンネル生成に係わる方式の説明であり，4.3.3 小節，4.3.4 小節はこれを前提に音声ストリームを HRAS/HRAC に導く SoFW 独自の技術の説明である．

4.3.2 システム開始から通話までの流れ

外部端末から呼設定を開始し，内部端末が通話を終了する場合を例に取って，システム起動時から通話終了までのシーケンスを図 4.4 に示す．

システムを起動すると HRAS と HRAC は 2 点間でトンネル生成を行う．HRAC は HRAS に対して HTTP（RFC2616）に準拠する GET リクエストと POST リクエストメッセージを送信する．HRAS は GET リクエストを受け取ると 200OK レスポンスのヘッダ部を返す．この後，HRAS と HRAC は端末から SIP メッセージが送信されるまで TCP コネクションを維持したまま待機する．以降，SIP メッセージまたは音声ストリームを受信すると HTTP のボディ部としてこれらを中継することができる．内部の SIP 端末は自身の情報を HRAS の SIP サーバに登録するため REGISTER リクエストを HRAC に送信する．HRAC は HTTP トンネルを介してリクエストを HRAS に中継し，HRAS から返信される 200OK レスポンスを内部 SIP 端末に返す．上記処理により外部 SIP 端末からの通話開始ネゴシエーション

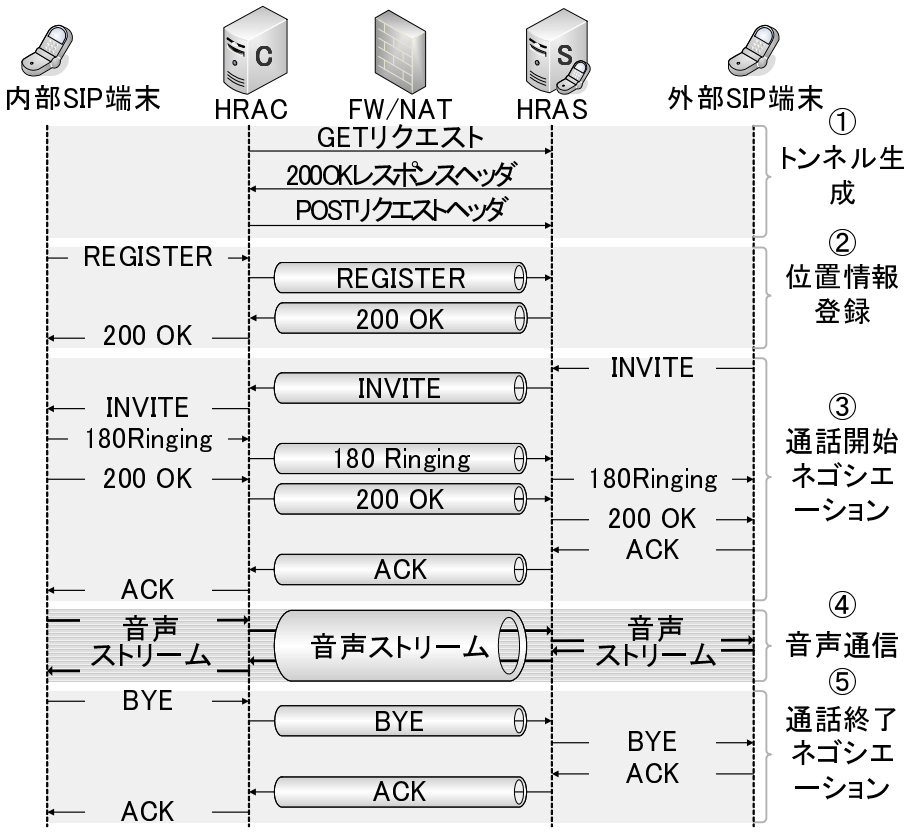

図 4.4 HTTP トンネル生成から通話終了までのシーケンス

が可能となる．外部 SIP 端末は INVITE リクエストを HRAS の SIP サーバ宛に送信する．HRAS の SIP サーバは内部 SIP 端末を特定し HTTP トンネルを介して端末に INVITE リクエストを転送する．INVITE メッセージを受けた内部 SIP 端末は呼出し中を意味する 180 Ringing レスポンスを返し，フックオフすると 200OK レスポンスを返す．呼び出し側はこれを受けて，応答確認の ACK メッセージを返す．通常の SIP ネゴシエーションは初めのリクエストが端末に届いた後は端末間で直接 SIP メッセージを交換しようとする．ネゴシエーションが終わると音声通信が開始される．音声ストリームは以下に述べる方法により，外部端末は HRAS へ，内部端末は HRAC へ送信し続ける．HTTP トンネルはその音声ストリームを対応する端末へ中継する．最後に通話終了ネゴシエーションはフックオンを告げる BYE メッセージと確認応答 ACK が HTTP トンネルによって中継され，通話が終了する．

4.3.3 SDP の修正による音声ストリーム誘導

SoFW では音声ストリームも HRAS/HRAC 間の HTTP トンネルを中継させなければならない．しかし，通常の SIP 端末の仕様では音声ストリームはエンド端末どうしで直接交換される．SoFW では通常の SIP 端末から送信される音声ストリームを HTTP トンネルに

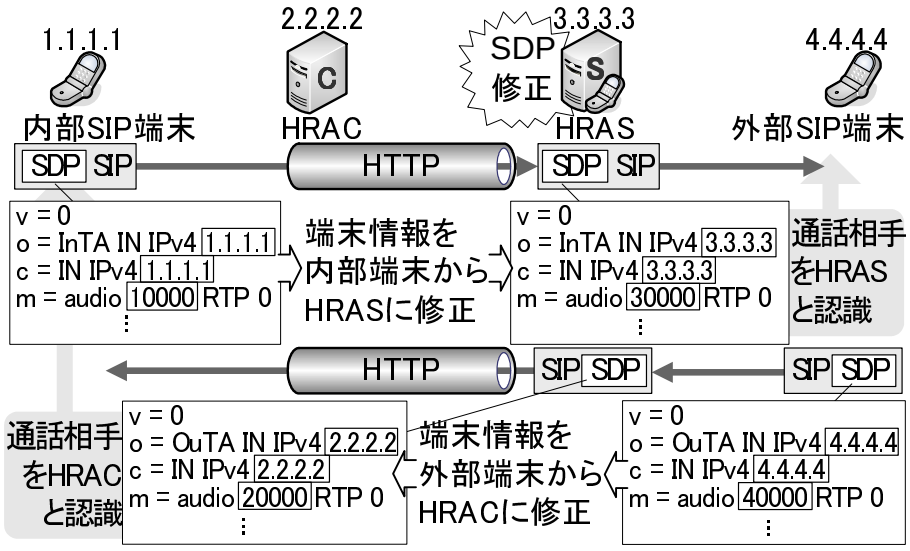

図 4.5 SDP の修正

誘導するために，SIP メッセージの INVITE リクエストとその 200OK レスポンスが HRAS に到達すると，メッセージボディ部の SDP[18] で記述されるタイプ値の修正を行う．この処理により，内部端末は HRAC を，外部端末は HRAS を通信相手とみなすこととなり，端末の機能を変更することなく音声ストリームを HRAS/HRAC に誘導することが可能となる．

SDP 修正の手順を図 4.5 に示す．SDP にはそのセッションの音声通信に必要とされる送信側ユーザエージェントの様々な情報がタイプ値として記述される．タイプ値にはメッセージ送信側の端末が音声通信に使用する IP アドレス・ポート番号やコーデック方式などがあり，端末は SDP を SIP メッセージのボディに記述することにより，音声通信に先立ち互いの音声通信情報を交換する．HRAS は，内部ネットワーク端末から送信された SDP の IP アドレス・ポート番号の値を HRAS の IP アドレス・ポート番号に，また外部ネットワーク端末から送信された SDP の IP アドレス・ポート番号の値を HRAC の IP アドレス・ポート番号に書き換える．修正された SDP を受け取った内部端末は音声ストリームの宛先を HRAC，外部端末は HRAS と認識して音声通信を開始する．

4.3.4 RAT による音声ストリーム経路決定

前節で記述したように，端末は音声ストリームの宛先 IP アドレス・ポート番号を HRAC もしくは HRAS に指定するよう誘導されるため，実際に通信相手となる端末の IP アドレス・ポート番号の情報を持っていない．HRAS/HRAC では宛先端末の IP アドレス情報を持たない音声ストリームに対して適切な通信相手へ送信する経路決定を行う方法が必要になる．

SoFW では呼設定時に両方向の SIP メッセージの SIP ヘッダと SDP の情報から SoFW

表 4.1 RAT の内容

内容	説明
To	受信者情報（ダイアログ ID）
From	送信者情報（ダイアログ ID）
Call-ID	セッション識別子（ダイアログ ID）
IIP	内部ネットワーク端末の IP アドレス
IPort	内部ネットワーク端末のポート番号
OIP	外部ネットワーク端末の IP アドレス
OPort	外部ネットワーク端末のポート番号

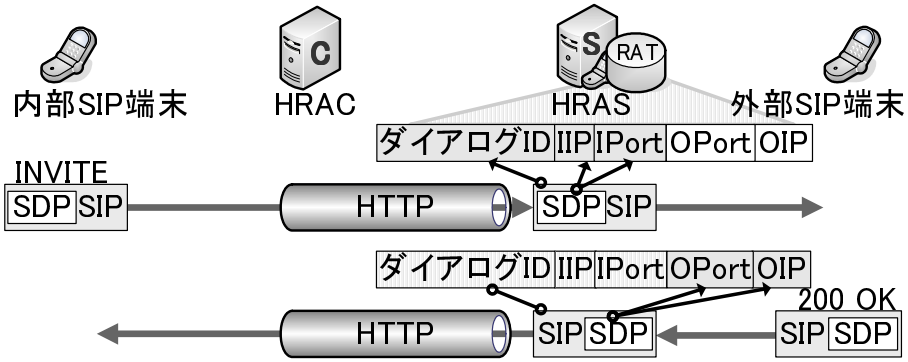

図 4.6 RAT の生成

特有の RAT（Relay Agent Table）と呼ぶテーブルを HRAS で生成し，音声通信時にはこのテーブルを参照して音声ストリームの経路決定を行う．RAT は音声通信を行う両端末を対応させた情報を保持する．RAT の内容を表 4.1 に示す．To，From，Call-ID は SIP メッセージのヘッダ情報であり，この 3 つを合わせて通信を識別するダイアログ ID となる．IIP・IPort は SDP から得られる内部端末の IP アドレス・ポート番号，OIP・OPort は外部端末の IP アドレス・ポート番号の値が書き込まれる．

図 4.6 に内部ネットワーク端末から呼設定を開始する場合の RAT 生成の流れを示す．SDP は SIP の発呼側の開始メッセージである INVITE リクエストと受信側の応答である 200OK レスポンスのボディ部に記述される．HRAS は INVITE リクエストを受信すると，メッセージのヘッダ部からダイアログ ID を RAT レコードに書き込み，SDP からは IP アドレス・ポート番号を IIP・IPort フィールドに書き込む．次に 200OK レスポンスを受信するとメッセージのダイアログ ID が一致する RAT レコードを検索し，SDP に記述されている IP アドレス・ポート番号を OIP・OPort として追記する．このようにして RAT には内部端末と外部端末の IP アドレス・ポート番号を対応させた情報ができる．

呼設定が完了し，音声通信が開始されると HRAS の RAT と RA（Relay Agent）ヘッダと

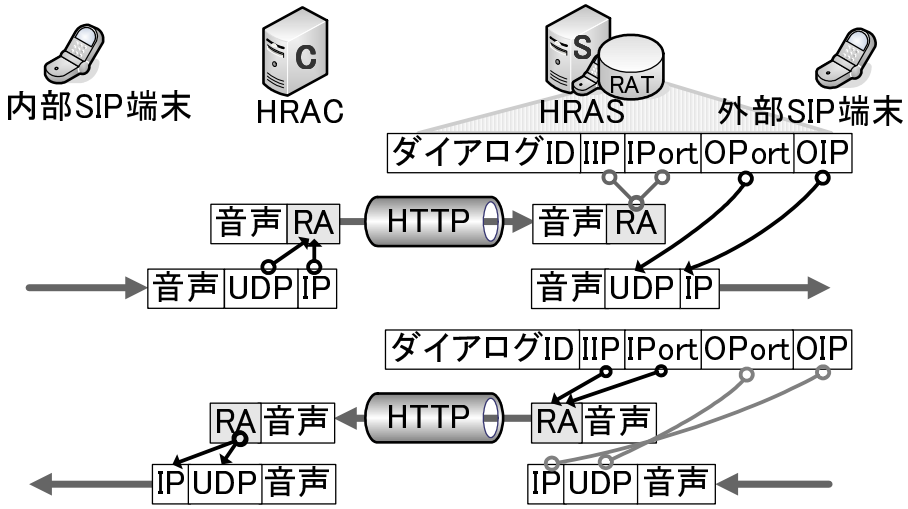

図 4.7 音声ストリーム処理の流れ

呼ぶ独自のヘッダを利用して音声ストリームの経路決定を行う．RA ヘッダは HRAS・HRAC 間のアプリケーションレベルの中継によって失われる IP レベル情報を保持するためのヘッダである．

音声ストリームの処理の流れを図 4.7 に示す．音声ストリームが内部端末から外部端末へ向けられている場合，HRAC はこれを受信すると送信元 IP アドレスとポート番号を RA ヘッダとして音声データに付加し，HRAS へ送信する．HRAS では受け取った RA ヘッダの IP アドレス・ポート番号から RAT で対応する外部端末の IP アドレス・ポート番号を検索し，これを宛先に指定し，音声ストリームを中継する．外部から内部へ向けられた音声ストリームの場合，HRAS がこれを受信すると送信元 IP アドレスとポート番号から RAT によって対応する内部端末の IP アドレス・ポート番号を検索し，RA ヘッダとして音声データに付加し HRAC へ送信する．HRAC は RA ヘッダに含まれる IP アドレス・ポート番号を宛先に指定して音声ストリームを中継する．

最後に，通話を切断する際には RAT からセッションの情報を削除する．HRAS が SIP の切断要求である BYE メッセージを受信すると，そのダイアログ ID から該当する RAT のレコードを検索して該当レコードの内容を削除する．

4.4 実装方式

4.3 節で述べた実現方式を HRAS/HRAC として，それぞれ一台の FedoraCore3.0（linux2.6.9）上のアプリケーションとして実装した．HRAS の SIP サーバ機能の部分はフリーソフトの SIP サーバである SER（SIP Express Router）[19] と連携することによって実現した．

HRAS のモジュール構成と主要な処理を図 4.8 に示す．HRAS の SER 以外の SIP メッセー

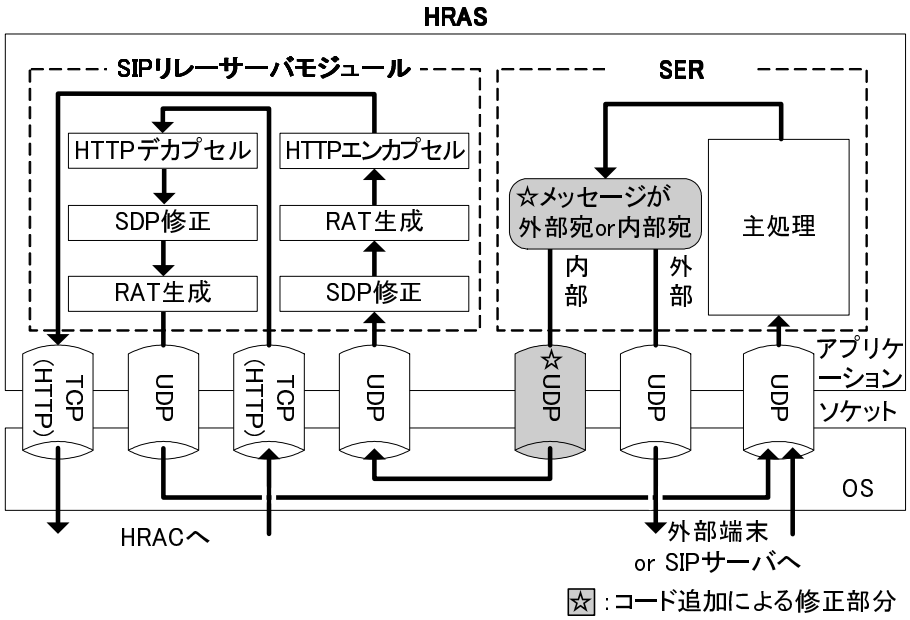

図 4.8 HRAS のモジュール構成と主要な処理

ジ処理に関する処理を SIP リレーサーバモジュールと呼ぶ．SER には SIP メッセージを SIP リレーサーバモジュールとやり取りするために少量のコード修正を加えた．SER で SIP メッセージがソケットに出力される前に，外部ネットワーク端末宛のものか内部ネットワーク端末宛のものかを判別し，外部宛であれば通常通り外部へ送信し，内部宛であれば SIP リレーサーバモジュールの生成したソケットに送信するように修正した．このように，HRAS では SER と SIP リレーモジュールが連携して動作する．

また，SoFW では複数の SIP メッセージおよび音声パケットを同時に扱うため，並行処理を行う必要がある．Linux で並行処理を行うにはマルチプロセス方式とマルチスレッド方式がある．マルチプロセスでは処理単位ごとにメモリ空間が用意されるためプロセス間の独立性が高いという利点があるが，RAT をプロセス間で共有するにはプロセス間通信処理が必要になり効率が悪くなる．そのため，各処理単位が RAT を共有できるマルチスレッド方式を採用した．

4.5 評価

4.5.1 IP 電話の規格と評価システムの構成

総務省発行の IP ネットワーク技術に関する研究会報告書 [20] によると，エンドツーエンド遅延についてはクラスＡ（固定電話並）が 100ms，クラスＢ（携帯電話並）が 150ms，クラスＣ（許容範囲）が 400ms として分類されている．遅延についての数値は 95% の確率

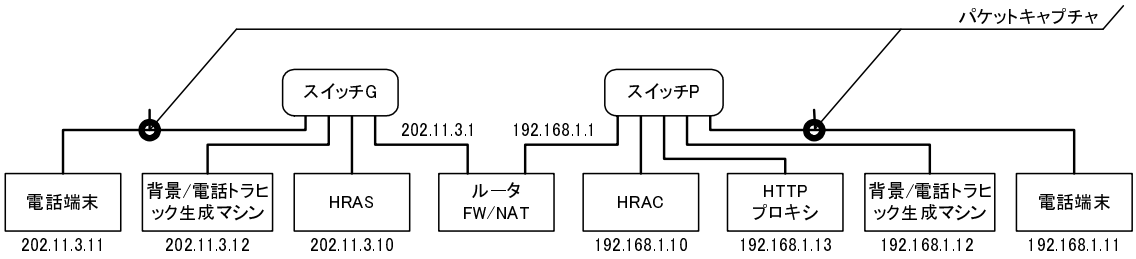

図 4.9 評価システムの構成

で満足させる必要があり，呼損率はすべてのクラスにおいて 0.15 以下とされている．また，ITU-T 勧告 [21] によると IP パケット損失率はすべてのクラスにおいて 1×10^{-3} が目標値とされている．上記規格を参考に，本提案システムの評価においては，クラス C の実現を目指し，HRAS/HRAC と FW 部分の合計遅延が 95% 以上の確率で 70ms 以下（400ms の 5 分の 1 以下）であること，IP パケットの損失が 0.1% 以下であること，SIP による呼損失が 0.15 以下であることを持って実用に耐えうる性能であると判断する．

評価システムの構成を図 4.9 に，SoFW を構成する各装置の性能を表 4.2 に示す．100BASE-TX 対応のスイッチ G，スイッチ P をそれぞれ外部ネットワーク側用とプライベートネットワーク側用に位置づけ，スイッチ G に外部用端末，HRAS，背景/音声トラヒック生成マシン，ルータのグローバルインタフェース側を接続し，スイッチ P に内部用端末，HRAC，HTTP プロキシ，背景/音声トラヒック生成マシン，ルータのプライベートインタフェース側を接続した．スイッチ G に接続するインタフェースにはグローバルアドレスを，スイッチ P に接続するインタフェースにはプライベートアドレスを割当てた．ルータには FW と NAT の機能を実装した．また，背景/音声トラヒック生成マシンは実験ごとに用途を変え，背景トラヒックや音声トラヒックを生成する．背景トラヒックの生成にはトラヒックジェネレータ D-ITG[22] を用いた．FW には内側から外側への HTTP 以外の通信を遮断するルールと TCP レベルのステートフル・インスペクションを設定した．また，SIP 端末は X-Lite，音声コーデックは G.711 を使用した．

4.5.2 実験結果と考察

(1) **パケット処理遅延の測定**

SoFW の純粋な処理速度を評価するため，SoFW を構成する各装置の処理時間が音声パケットに与える遅延を測定する実験を行った．SoFW を利用する環境では必ず FW，NAT および HTTP プロキシを通過させるため，HRAS，HRAC に加え，FW，NAT および HTTP プロキシが音声パケットに対して行う処理時間の合計を測定した．

外部用端末からの呼設定により音声通信を開始した後，モニタマシンによって送信直

表 4.2 評価システムの性能

装置	仕様	
HRAS /HRAC	CPU	Intel Pentium 2.8GHz
	メモリ	512MB
	NIC	Broadcom Tigon3 100BASE-TX
FW/NAT /Proxy	CPU	Intel Pentium 600MHz
	メモリ	256MB
	NIC	Global: Silicon Integrated System crop 100BASE-TX
		Privete: ADMtek FNW-9803-T 10/100BASE-TX
外部用端末	CPU	Intel Pentium 3.4GHz
	メモリ	1GB
	NIC	Broadcom NetXtreme57xx 100BASE-TX
内部用端末	CPU	Intel PentiumM 1.80GHz
	メモリ	512MB
	NIC	Realtek RTL8139/810x 100BASE-TX

表 4.3 遅延時間の測定値

	Outbound	Inbound
average	0.95ms	0.97ms
max	52.0	73.8

後の音声パケット，受信直前の音声パケットをキャプチャし，Outbound（内部端末から外部端末へ）と Inbound（外部端末から内部端末へ）の音声ストリームの平均遅延と分布を計算した．サンプルとなる音声パケットは計 100,000 パケットの平均とした．

遅延時間の測定値を表 4.3 に，遅延時間の分布を表 4.4 に示す．実験結果では Outbound および Inbound ともに平均 1ms 以下であり通話に影響を与えない範囲であると言える．最大値は約 50，70ms であるが，表 4.4 からわかるように，1.9ms 以上の遅延を持つパケットが全体に占める割合は 0.01 %程度であることがわかる．このことより SoFW 構成装置の音声パケットに対する処理時間は音声通話に影響しない範囲であると言える．また，Outbound と Inbound で遅延時間が異なるのは，パケットの処理工程数の多い HRAS において，RA ヘッダに対する処理が生成と参照で異なるためである．

表 4.4 遅延の分布

遅延	～ 0.7ms	0.7～ 1.3ms	1.3～ 1.9ms	1.9ms ～
Outbound	0.4 %	98.3 %	1.3 %	0.01 %
Inbound	1.1	98.0	0.8	0.01

表 4.5 30 セッション時の遅延の分布

遅延 (ms)	～ 10	10～ 30	30～ 50	50～ 70	70 ～
Outbound(%)	74.0	13.7	6.8	1.6	3.8
Inbound(%)	48.8	26.7	17.7	4.3	2.5

(2) **同時通話に対する性能評価**

HRAS/HRAC が対応できるセッション数を測定する実験を行った．複数台の端末装置を接続するのは現実的に困難であるため，あらかじめ HRAS では手動で RAT を生成し，外部と内部に位置する両音声パケット生成マシンから擬似的に複数台分の音声パケットを HRAS および HRAC に送信し，実際に通常の IP 電話端末で SoFW を利用するのと同様の負荷を与えた．音声パケット発生装置は G.711 の音声通信を擬似的に生成する．1 台分の出力音声トラヒックは UDP で 172Byte のデータを 20ms 間隔で送信する．これをランダム間隔で複数台分立ち上げ，1 対の音声通信に加えられる遅延時間とパケットロス率を測定した．

図 4.10 にセッション数に対する遅延時間の増加，図 4.11 にセッション数に対するパケットロスの増加を示す．それぞれ縦軸が遅延時間およびパケットロス率，横軸が端末数を表している．Outbound が Inbound よりも遅延時間，パケットロス率の両方において多数の端末数に耐えられているのは，(1) で述べたように RA ヘッダ処理負荷の違いがより顕著に現れたためであると考えられる．また，遅延時間が一定の値で収束するのは，遅延時間が所定の値以上になるとバッファ量の制限から処理待ちのパケットが溢れて廃棄され，一定以上の処理待ち時間は起こらないためと考えられる．30 セッション程度であればパケットロスは発生せず，平均遅延時間も 20ms 以下を示している．また，表 4.5 の 30 セッション時の遅延の分布から，30 セッションの通話が行われているとき，Outbound，Inbound がともに 95 %以上の確率で 70ms 以下の遅延を維持していることがわかる．この結果から通常使用される PC を用いて構成した HRAS および HRAC は少なくとも 30 セッション程度の負荷まで絶え得ることが分かった．

(3) **呼設定と音声通信が互いに及ぼす影響**

呼設定と音声通信の負荷が混在するときの本システムの有用性を確認するために，呼

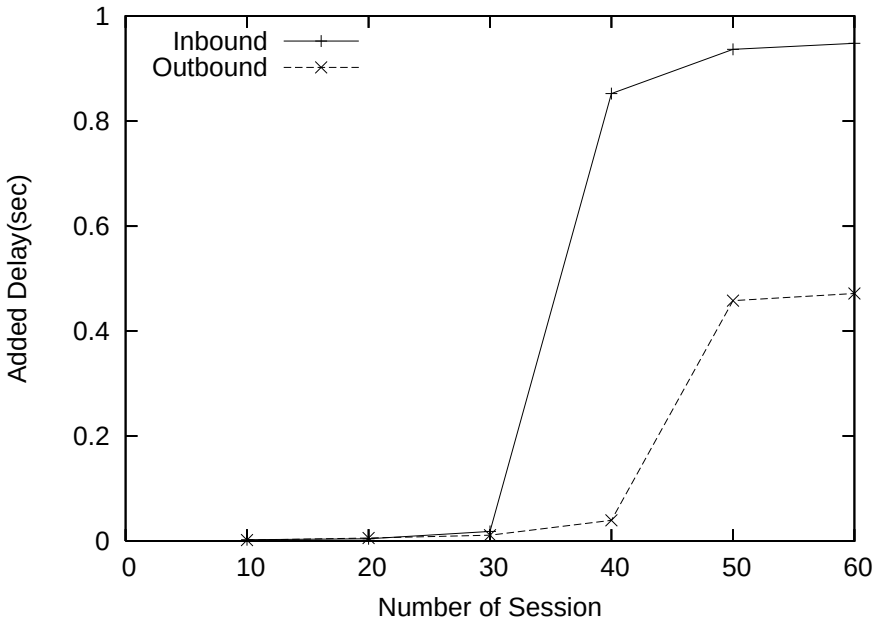

図 4.10 セッション数に対する SoFW による追加遅延

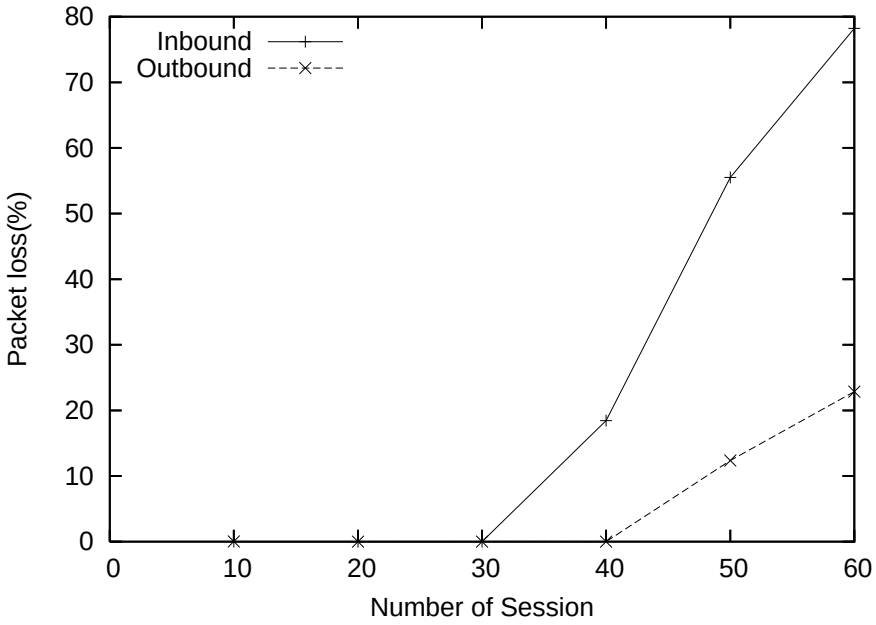

図 4.11 セッション数に対する SoFW によるパケットロス

表 4.6 SIP メッセージの処理時間

	メッセージの種類	Normal 構成	SoFW	SoFW+30 セッション
接続処理	INVITE	0.42ms	2.7ms	5.6ms
	Ringing	0.24	3.1	3.8
	200OK	0.32	2.6	4.8
	ACK	0.25	1.6	2.5
	合計	1.23	10	16.7
切断処理	BYE	0.25	1.7	5.2
	200OK	0.18	1.5	2.1
	合計	0.43	3.2	7.3
登録処理	Register	0.32	3.6	6.3

処理と音声ストリーム処理を同時に実行させ，相互に及ぼす影響を調査した．

呼処理の評価に当っては，呼の接続と切断を，平均間隔 t の指数分布にしたがって連続的に発生させるプログラムを作成した．

SoFW は同時 30 セッションの音声負荷に耐えられるので，ユーザの通話時間を平均 1 分と仮定すると，音声とバランスを取るには，平均毎分 30 以上の呼処理に対応できる必要があると考えられる．以下の評価では，呼の平均間隔 t を 300ms と設定した．これは，同時に受付可能な呼数に換算すると，平均毎分 198 呼に相当するため評価としては十分な余裕を見ていると言える．

システム構成としては，SIP 端末間に SIP サーバのみが存在する場合（Normal 構成）と，SIP 端末間に FW および HRAS/HRAC が存在する場合（SoFW 構成）を想定した．なお，SoFW 構成においては，HRAS が SIP サーバの機能を包含している．

SIP で使用される各パケットが，Normal 構成において SIP サーバを通過する時間，SoFW 構成において FW と HRAS/HRAC を通過する時間をそれぞれ計測した．ただし，Register においては SIP 端末が SIP サーバへ Register メッセージを送信し，200OK メッセージが返ってくるまでの時間とした． SoFW 構成においては，さらに呼処理の情報だけを流した場合と，30 セッションの音声を同時に流した場合を計測した．この結果を表 4.6 に示す．表中の値は 100 回の平均値である．

Normal 構成と SoFW 構成が呼接続時間および呼切断時間に与える遅延は，それぞれ INVITE から ACK までのメッセージの処理時間の合計，BYE から 200OK（BYE）までのメッセージの処理時間の合計となる．また，端末情報の登録時間に与える遅延は Register の処理時間となる．表 4.6 に示すように，SoFW 構成においては Normal 構

表 4.7 呼設定が音声パケットに与える影響

遅延		～10ms	10～30ms	30～50ms	50～70ms	70ms	平均
音声	Inbound	52.3%	43.9%	3.68%	0.05%	0.06%	11.4ms
	Outbound	66.3	16.7	9.1	7.8	0.03	12.5
音声+呼処理	Inbound	44.8	49.3	5.9	0	0	12.3
	Outbound	60.4	20.8	10.1	8.7	0.03	13.8

成に比べ HRAS/HRAC の分だけ接続処理時間と切断処理時間および登録処理時間は増大するものの，音声セッションの処理を同時に実行させた場合においても，ユーザ心理には影響を与えない十分小さな値であるといえる．ここで，SoFW 構成で呼と音声 30 セッションを同時に流した場合において，1000 回の呼処理を連続実行させたが，呼損はまったく発生しなかった．これから SoFW が呼損率を劣化させる要因とはならないことを確認した．以上の結果より，音声データが呼処理に与える影響は十分小さいと判断できる．

次に，呼処理によって音声パケットがどのように影響を受けるかを評価するため，音声 10,000 パケットの遅延時間の変化を測定した．表 4.7 にその結果を示す．本実験では，音声のセッション数が 25 の時点での測定を行った．表 4.7 からわかるように，呼処理を加えることによって Outbound， Inbound とも平均遅延時間と分布の偏りが若干増加するが，いずれの場合においても遅延時間が 95% 以上の確率で 70ms 以下を維持している．以上の結果より，呼設定が音声パケットに与える影響も十分小さいと判断できる．

(4) **TCP 再送制御による影響の評価**

本システムでは UDP 通信を行う 2 台の音声端末の間に，TCP 通信の経路が挟まれるという構造になっている．このような構造では，TCP 経路上でパケットロスが起こった場合に実行される TCP の再送制御によって通話に影響を及ぼすことが懸念される．そこで，HRAS と HRAC 間の TCP の経路が通過するルータに背景負荷となるトラヒックを与えて，故意にパケットロスを発生させ，音声パケットの遅延時間に与える影響を評価する実験を行った．トラヒックジェネレータによりプライベートアドレス側からグローバルアドレス側へ背景トラヒックを発生させ，ルータ部でパケットロスを発生させる．背景トラヒックのデータサイズは 200Byte，送信間隔はランダムとし，単位時間（1 秒）当たりの送信パケット数を調節することによりトラヒック量を変更しながら測定を行った．音声通信を開始した後，モニタマシンによって送信直後のパケット，受信直前のパケットをキャプチャすることにより Outbound と Inbound の音声ストリームの平均遅延時間（50000 パケットの平均）を算出した．また，通常の音声通信と比較するために SoFW を利用せず，ルータの FW と NAT 機能をオフにして

通信する実験も同様の方法で測定した．

図 4.12 に Outbound における背景負荷と遅延時間の関係を，図 4.13 に Inbound における背景負荷と遅延時間の関係を，図 4.14 に Outbound における背景負荷とパケットロス率の関係を，図 4.15 に Inbound における背景負荷とパケットロス率の関係を示す．また表 4.8 に Outbound における遅延時間の分布を，表 4.9 に Inbound における遅延時間の分布を示す．SoFW を利用せず，ルータの FW と NAT 機能をオフにして直接通信した実験を Normal モード，SoFW を利用した実験を SoFW モードとして比較した．図 4.12，図 4.13 の縦軸は音声パケットに加えられた遅延時間を示し，図 4.14，図 4.15 の縦軸はパケットロス率を示す．横軸はいずれも背景トラヒック量で 1 秒間の平均パケット送信回数である．図 4.12，図 4.13 から SoFW モードでは平均パケット送信回数 23000 パケット/秒の背景トラヒック量を与えるまでは十分小さい平均遅延時間を示すが，それ以降は急激に遅延時間が増加する．また，表 4.8，表 4.9 からもわかるように背景負荷が 23000 パケット/秒までは 95% 以上の確率で 70ms 以下の遅延におさまっている．それに対し Normal モードでは背景トラヒックに対して遅延時間の影響はさほど大きくならないことがわかる．次に，図 4.14，図 4.15 から SoFW モードではパケット送信回数 23000 パケット/秒の背景トラヒックまでは実用的なパケットロス率の範囲に収まっているが，それ以降は急激にロス率が増加する．それに対し Normal モードでは 23000 パケット/秒の時点ですでにパケットロス率が 0.1 %を越えている．すなわち，Normal モードでは背景トラヒックの影響は遅延にはさほど現れないかわりにパケットロスに現れる．それに対し SoFW モードでは再送制御がパケットロスを補う代わりに，遅延時間に影響が現れることがわかる．また，23000 パケット/秒以降で SoFW モードの遅延時間が急増しているのは再送制御によりデータ送信が遅れ，TCP の送信待ち行列がオーバーフローして，データが破棄されてしまうためである．このように，SoFW を利用した音声通信では所定の負荷までは十分実用に耐えうる性能を示すが，それを越えると急激に遅延時間が増加して使用できない状態になる．これに対し，UDP を利用した一般の音声通信では，上記と同様の負荷が与えられた段階で，すでにパケットロスが許容範囲を越えた状態になっている．以上の結果より，SoFW はそれを用いない場合に比べ，同等かそれ以上の背景負荷に耐えられるということができる．

ただし，負荷が大きくなっていくと，Normal モードではパケットロスが大きくなって徐々に許容範囲を越えるのに対し，SoFW では HRAS/HRAC 間で TCP の再送制御が働き，あるトラヒックを超えた時点で SoFW がまったく使えない状態になる．これはエンド音声端末に対して TCP の輻輳制御が伝わらないためである．これを防止するには，FW において IP 電話を優先する QoS 制御を行い，かつ IP 電話のセッション数に制限を設けるなどの対策が必要と考えられる．

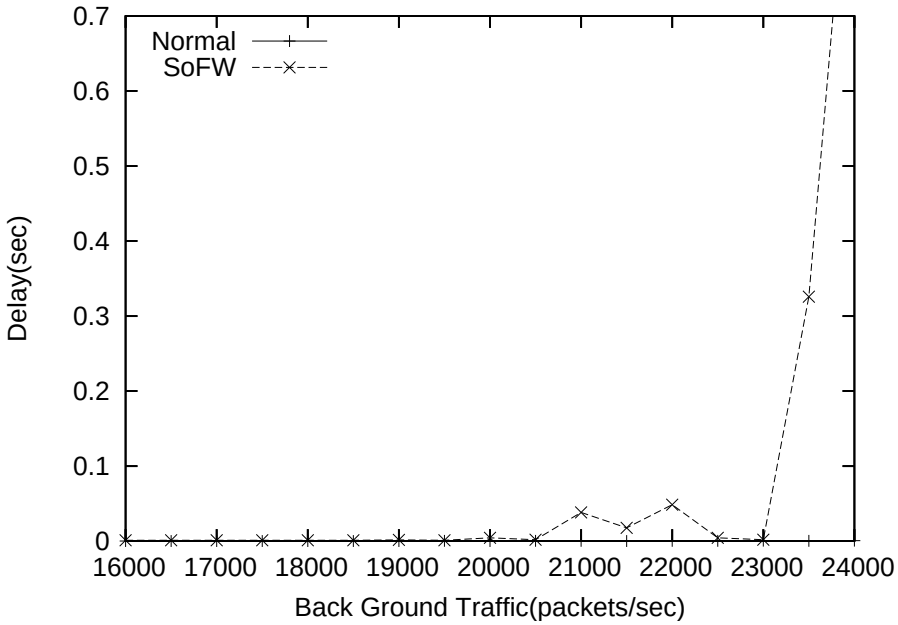

図 4.12 Outbound トラヒックにおける遅延時間の比較

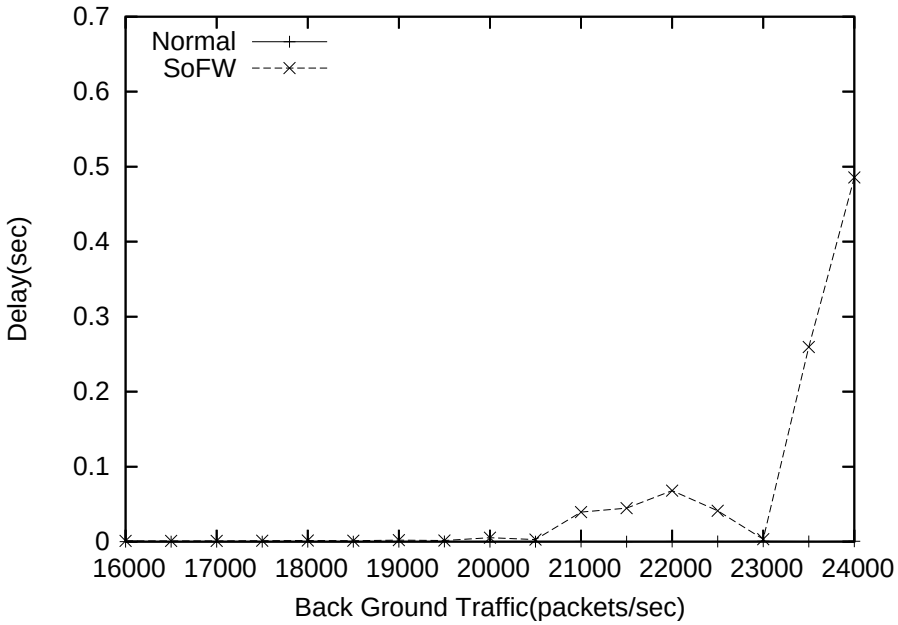

図 4.13 Inbound トラヒックにおける遅延時間の比較

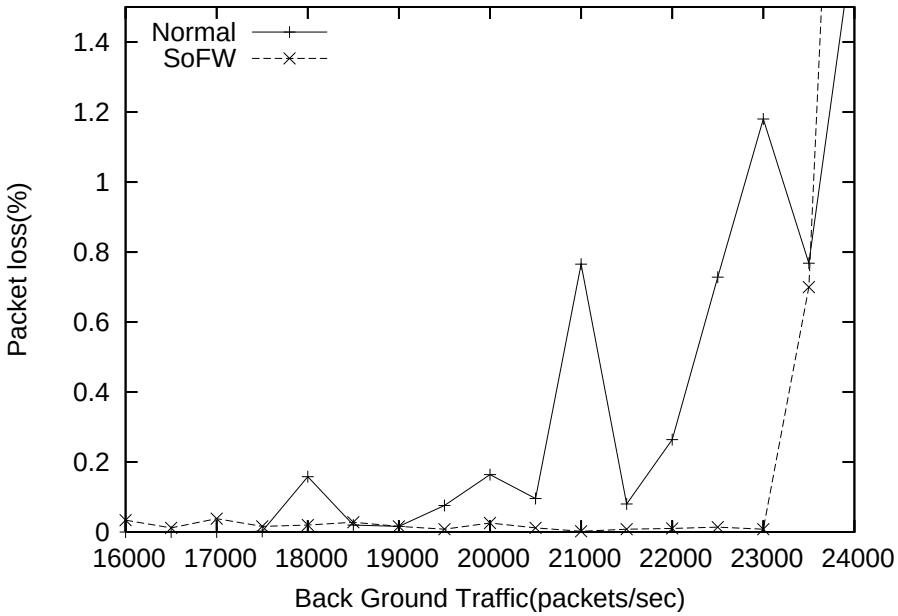

図 4.14 Outbound トラヒックにおけるパケットロス率の比較

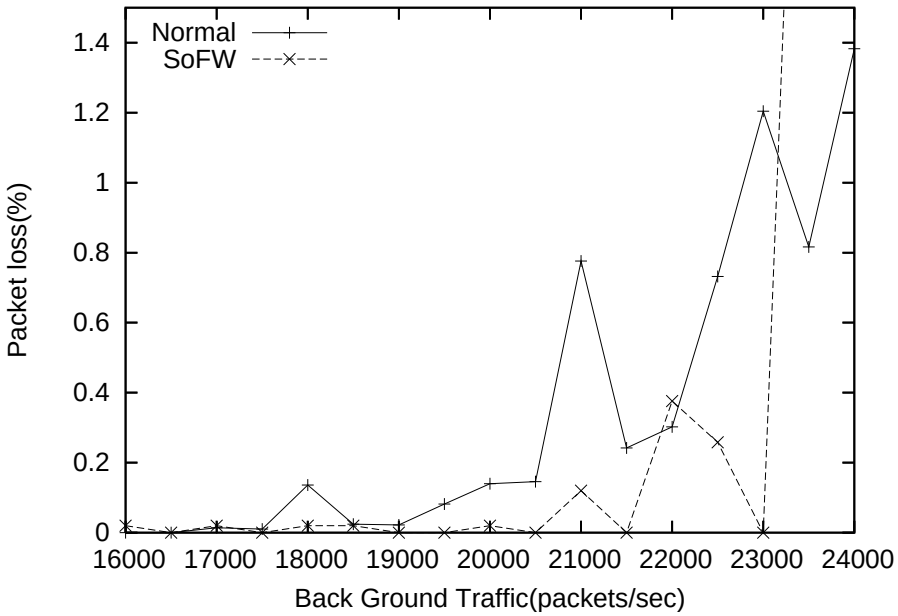

図 4.15 Inbound トラヒックにおけるパケットロス率の比較

表 4.8 Outbound トラヒックにおける遅延時間の分布

背景負荷＼遅延	～ 10ms	10～ 30	30～ 50	50～ 70	70 ～
19000(pkt/s)	99.7 %	0.2	0.0	0.1	0.1
21000	97.4	0.3	0.2	0.1	1.9
22000	96.0	0.4	0.2	0.3	3.2
23000	99.2	0.2	0.2	0.1	0.4
23500	94.8	0.5	0.4	0.5	3.7
24000	92.3	0.4	0.3	0.4	6.6

表 4.9 Inbound トラヒックにおける遅延時間の分布

背景負荷＼遅延	～ 10ms	10～ 30	30～ 50	50～ 70	70 ～
19000(pkt/s)	99.0 %	0.3	0.1	0.1	0.5
21000	95.7	0.5	0.4	0.3	3.0
22000	94.9	0.7	0.3	0.4	3.7
23000	97.7	0.4	0.3	0.2	1.4
23500	91.4	1.3	0.9	0.8	5.6
24000	91.9	0.7	0.5	0.5	7.3

4.6 おわりに

ファイアウォールの外部と内部にそれぞれ 1 台のリレーエージェントを設置し，その間に HTTP トンネルを作ることによってファイアウォールを越えられる IP 電話システム SoFW の実現方法を提案した．SoFW は既存の方式に対して，既存ファイアウォールの取替え，セキュリティポリシの変更が不要なため導入が容易であることや，既存の SIP 端末がそのまま利用できること，アドレス空間の統一的管理の必要がないという利点を持っている．

評価実験では背景トラヒックや同時通信による負荷をかけ性能を測ることにより，SoFW が IP 電話システムとして実用に耐えうる性能を持つことを示した．

本論文では SIP で扱うデータを音声データに限定したが，SIP はさまざまな用途のメディア通信に対して，その将来性が注目されており，今後は SoFW の IP 電話以外への対応も検討していく．

参考文献

[1] Freed, N.: Behavior of and Requirements for Internet Firewalls, *RFC 2979* (2000).

[2] Egevang, K. and Francis, P.: The IP Network Address Translator (NAT), *RFC 1631* (1994).

[3] 大田昌孝：本当のインターネットを目指して：インターネットと電話（2），情報処理学会誌， Vol. 40, No. 9, pp. 922–923 (1999).

[4] ITU-T Recommendation H.323: Visual Telephone Systems and Equipment for Local Area Networks which Provide a Non-guaranteed Quality of Service (1996).

[5] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and Schooler, E.: SIP: Session Initiation Protocol, *RFC 3261* (2002).

[6] Peterson, J.: Application-layer Policy Enforcement at SIP Firewalls, *IETF Internet-Draft* (2000).

[7] Martin, C.: SIP Through NAT Enabled Firewall Call Flows, *IETF Internet-Draft* (2001).

[8] Martin, M.: SIP NSIS Interactions for NAT/Firewall Traversal, *IETF Internet-Draft* (2004).

[9] Rosenberg, J., Schulzrinne, H. and Drew, D.: Getting SIP through Firewalls and NATs, *IETF Internet-Draft* (2000).

[10] Thernelius, F.: SIP Firewall Solution, *IETF Internet-Draft* (2000).

[11] 大竹八洲考，但馬康宏，寺田松昭：SIP を用いた NAT 通過手法の提案とその実装，情報処理学会論文誌， Vol. 45, No. 3, pp. 813–823 (2004).

[12] 宮内信二：多様な環境で利用できるインターネットプロトコル，情報処理学会論文誌，Vol. 44, No. 3, pp. 553–560 (2003).

[13] Skype: .
http://www.skype.com/home.html.

[14] 登大遊：SoftEther の内部構造，情報処理学会誌， Vol. 45, No. 10, pp. 1057–1062 (2004).

[15] Asgent Apostra: .
http://www.asgent.co.jp/Products/
Apostra_Tunnel/tunnel.html.

[16] UDP Hole Punching: .
http://www.brynosaurus.com/
pub/net/p2pnat/.

[17] NEC UNIVERGE IX seriese: .
http://www.sw.nec.co.jp/ix2k3k/index.html.

[18] Handley, M. and Jacobson, V.: SDP:Session Description Protocol, *RFC 2327* (1998).

[19] SER: .
http://www.iptel.org/ser/.

[20] 総務省： (2001). IP ネットワーク技術に関する研究会報告書.

[21] ITU-T Recommendation Y.1541: Network Performance Objectives for IP-Based Services (2003).

[22] D-ITG: .
http://www.grid.unina.it/software/ITG/.

5章　結論

無線メッシュネットワークは携帯電話，WiMAX，無線 LAN など他の無線ネットワークと補完の関係にある．無線メッシュネットワークは第四世代携帯電話，WiMAX の電波の届きにくい屋内や，ケーブルを設置するコストの回収が見込めない僻地，迅速なネットワークの復旧が必要となる災害地などで無線ネットワークを提供できる．さらに，AP を適切に配置するだけで，自律的に経路を形成するため，容易に無線ネットワークを拡大できるという特徴がある．

この無線メッシュネットワーク上で IP 電話を利用することを想定すると，様々な課題が発生する．音声通信を利用するのであればリアルタイム性を保証する必要があり，通信の寸断を避ける必要がある．そのため，端末が AP を移動するときに，パケットロスを発生させず，確実にハンドオーバを成功させる方法が必要となる．無線マルチホップ通信の特性上，ホップを重ねるごとに通信速度が低下してしまう無線メッシュネットワークでは，できるだけ制御メッセージによるトラヒック量を減らす方法や，複数の GW を効率よく利用する方法など，無線ネットワーク上のリソースを有効利用する方法が求められる．また，無線メッシュネットワークを利用する環境には企業などの中程度のプライベートネットワークなども想定され，外部ネットワークとの間には FW/NAT が設置されている場合を考えなければならない．外部のネットワークに接続する端末と自由に音声通信を行うために，FW/NAT を越えて IP 電話を行う方法が必要である．しかし，これらの課題を解決すれば，これまでの無線ネットワークシステムのカバーできなかった領域を補い，音声通信の利用できる有用な無線ネットワークシステムとなる．

第 2 章では，無線メッシュネットワークの一実現方式である WAPL を提案した．WAPL は，無線メッシュネットワークを実現するための機能を，アドホックルーティングプロトコルから完全に独立させた．その結果，ルーティングプロトコルを自由に選択し，様々な用途への応用を可能にした．また，無線メッシュネットワークに必要なテーブルの生成をオンデマンドで実現するため，制御パケットが通信トラヒックに与える影響が少ない．さらに近隣の AP の通信状況を常時監視しておくことにより，端末が移動したときのハンドオーバ通知をユニキャストで実現できるようにした．これによりシームレスハンドオーバを確実に行うことができる．提案方式の有効性を評価するため，既存方式と WAPL を ns-2 のモジュールに組み込んで比較を行った．その結果，WAPL ではハンドオーバの失敗率を 0 に抑えることに成功した．また，既存方式に比べ制御メッセージによるトラヒック量も少ないことを明らかにした．

第 3 章では，無線メッシュネットワークにおいて効率良く GW を利用する方式を提案した．無線メッシュネットワークでは，インターネットなどの外部のネットワークと接続するとき，スループットのネックとなる GW 周辺の帯域の消費を解消するため，複数の GW を設置する方法が検討されている．これまで，パケットごとに複数の GW に分配する方式が

検討されているが，TCP のふくそう制御の機能により通信のスループットを低下させてしまう．そこで，我々はセッションごとに複数の GW に分配することにより，GW を効率的に利用し，かつ TCP 通信のスループットに影響を与えない方式を提案した．提案方式の有用性を評価するため，既存方式と WAPL の GW システムを ns-2 のモジュールに組み込んで比較を行った．その結果，提案方式が既存方式に比べて，TCP 通信のスループットが向上することを明かにした．また，ネットワーク上のトラヒックの公平性においても，既存方式に対して十分な値を示すこと明らかにした．

第 4 章では，FW や NAT を通過できる IP 電話を提案した．これまでの類似の研究や解決方法では，FW/NAT の装置自体を専用のものに取り換える必要があること，専用端末が必要であること，アドレス空間の統一的管理が必要であることなどの課題があった．そこで，2 台の特殊な装置をプライベートネットワークの内側と外側に接続するだけで，FW/NAT を越えて IP 電話を利用できるシステム，SoFW を提案した．SoFW は既存の SIP 端末を利用することができ，アドレス空間の統一的管理が必要なく，導入が容易であるという特長がある．SoFW を Linux 上に実装し，評価実験を行った結果，2 台の装置が通話によるパケットを転送しても，呼制御，音声の遅延などに影響しないこと，システムを利用する台数も 30 台程度まで問題ないことを明らかにした．

謝辞

本論文を完成するにあたり，格別のご指導ご鞭撻を賜りました名城大学理工学部渡邊晃教授に深い感謝の意を表します.

本論文をまとめるにあたり，懇切なるご指導を賜りました名城大学理工学部柳田康幸教授に謹んで感謝の意を表します.

本論文をまとめるにあたり，懇切なるご指導を賜りました名城大学理工学部中野倫明教授に謹んで感謝の意を表します.

本論文をまとめるにあたり，懇切なるご指導を賜りました愛知県立大学井手口哲夫教授に謹んで感謝の意を表します.

本研究を遂行するにあたり，懇切なるご指導を賜りました福井工業大学大学鹿間敏弘教授に謹んで感謝の意を表します.

本研究を遂行するにあたり，日頃より有益なご助言を賜りました名古屋大学小川明名誉教授に謹んで感謝の意を表します.

本研究を遂行するにあたり，日頃より有益なご助言を賜りました名城大学理工学部宇佐見庄五准教授に謹んで感謝の意を表します.

本研究を遂行するにあたり，日頃より有益なご助言を賜りました名城大学理工学部旭健作助教に謹んで感謝の意を表します.

最後に本研究を遂行するにあたり，有益なご助言を賜りました名城大学理工学部渡邊研究室の皆様に心より感謝いたします.