修 士 論 文

レイヤ2転送を用いたレイヤ3
アドホックネットワークの構成法

Layer 3 Ad-hoc Network using Layer 2
Transmission Capability

平成 19年 2月 2日提出

指導教官　江崎　浩　教授

情報理工学系研究科
電子情報学専攻
56431 中島　亮

梗概

無線技術を用いたアドホックネットワークはモバイルネットワークやセンサネットワークなど，これまでの情報通信にない新しい応用が考えられている．我々が活動を行う空間においては，モバイルノードやセンサーノードの周辺に有線ネットワークに接続された (無線) アクセスポイントが存在する場合が非常に多い．アクセスポイントをアドホックネットワークで利用することによって，アドホックネットワークにおける省電力消費やスループットの向上などを実現することができると考えられる．しかし，既存のアドホックネットワークの研究においては，アクセスポイントを積極的に利用することを考慮したアーキテクチャ設計とはなっていない．そこで，本研究では MAWC(Mobile Adhoc network with Wired Connection) と呼ぶアクセスポイントの利用を考慮にしたアドホックネットワークルーティングプロトコルを提案し, 効率的で実践的なアドホックネットワークの実現を目指した．MAWC では MAC アドレスルーティングを導入することで,IPv4 や IPv6，BlueTooth などの Layer-3 のプロトコル種別に非依存なマルチプロトコルなルーティングを実現している．既存のアドホックネットワークルーティングプロトコルとは異なり，各アドホックネットワークを形成するノードに IP アドレスが割り振られていなくてもレイヤ 3 パケットのルーティングを実現することができるため, IP 以外の任意のプロトコルを用いた通信に対応することを可能にしている．さらに，IPv4 と IPv6 の同一アドホックネットワーク上での共存を容易に実現することも可能とできることも特長となっている．MAWC では, アクセスポイントを介してインターネット上の任意のノードとの IP パケット通信を実現するために、アクセスポイントに接続された有線ネットワーク上に存在する DHCP サーバ から IP アドレスを取得し、これを用いてインターネットへのアクセスを行う．本論文では,MAWC アーキテクチャとその具体的動作、プロトタイプシステムの実装、さらに，実用性に関する初歩的な評価を行っている．

目次

図目次

第 1 章

序論

1.1 研究の背景

メインフレームから始まったコンピュータシステムの進化は中央サーバ型のコンピュータシステムを一台ごとに完結した (エンジニアリングワークステーションとも呼ばれる) コンピュータと変化させ，さらに、各個人が所有可能なコンピュータの出現、すなわち、パソコン (PC; Personal Computer) へと変化してきた．その後もコンピュータの急激な発展と進化は継続され，ノート型 PC や PDA などの可般あるいは携帯が可能なコンピュータ、すなわちモバイルコンピュータが、既に一般化している．．モバイルコンピュータはその高い利便性から世の中に広く普及し，現在では皆携帯電話や PDA，ノート型 PC などを一人複数台持ち歩いている状況が一般化しつつある．

コンピュータのインターネットへの常時接続環境は、エンジニアリングワークステーションが登場した頃から徐々に一般化してきたが、e-Japan 計画などの施策の効用もあり、近年急速に、パーソナルコンピュータや情報家電機器が、インターネットに常時接続される環境が一般化してきている． このような動きは、据え置き方のパーソナルコンピュータや情報家電機器のみならず、モバイルコンピュータや PDA へも普及しようとしている． さらに、商用の無線 LAN ホットスポットサービスや FON のようなコモンズ (Commons) 的な無線 LAN アクセス環境の進展、第 3 世代および第 4 世代の携帯電話システムの展開、さらに、WiMAX の展開などによって、すべてのコンピュータや PDA が、ほぼ、インターネットに常時接続される環境が整備されつつある．

オフィス環境や家庭環境におけるインターネットへの常時接続環境の浸透に伴い、コンピュータの利用法は大きく変化を遂げた． 現在の多くのアプリケーションがインターネットへの接続を前提としたものとなってきている．電子メール、WEB サービス、インターラクティブゲーム、メッセンジャー、IP 電話などは当然のこと、ドキュメントの作成やプレゼンテーションの作成などにおいても、オンライン上での情報検索なしには、効率的な業務や私的活動を行うことが、困難なとなる傾向にある． このような傾向は、モバイルコンピュータ (可搬型および携帯型) に限らず、最近では、ディジタル情報家電機器やセンサーノードのような組み込みかたコンピュータシステムにも急速に波及してきている．可搬型および携帯型、あるいは、センサ

ノードのようなコンピュータ機器は、移動可能な状態で動作することを前提としてシステム設計がされるようになってきており、これらの要求を満足可能な技術として 無線ネットワーキング技術が、広く利用されるようになってきている．無線接続は既存の有線接続とは異なり，各ノードまでの有線を提供する必要がないため，機器の設置場所に拘束される、自由な空間にノードを配置および再配置することができる．IEEE802.11 [1] に代表される周波数の利用に関する免許を必要としない無線ネットワーク技術の仕様が確立され，世界中で広く利用されるようになってきた．

一方、有線によるブロードバンドネットワーク環境を提供することが困難な環境や場所において、ネットワーキングされた環境を提供するための無線技術を用いたアドホックネットワークに関する研究開発が精力的に行われている．従来の無線 LAN システムは図 1.1 に示すように，複数のノードに対して一つの基地局が通信サービスを提供するインフラストラクチャ型と呼ばれるネットワーク形態が一般的であった．それに対し，アドホックネットワーク型のネットワーキングでは図 1.2 に示すように，ノード同士が特定のノードを用いて通信するのではなく、すべてのノードがパケットの中継と送受信を行う．すなわち，アドホックネットワークでは，各ノードが自律的にネットワークを構成する要素となるため，これまでの無線 LAN のようにアクセスポイントを用意して，その背後に有線 LAN をつなげる必要がない．有線技術を用いたブロードバンドインターネット環境が整備されても、すべての情報機器が有線インターネットに接続されたアクセスポイントに直接に接続可能となる環境を想定することは困難であり、無線技術を用いた情報の中継転送を行うような 無線技術を用いたアドホックネットワークが存在しなければならないと考えられる．

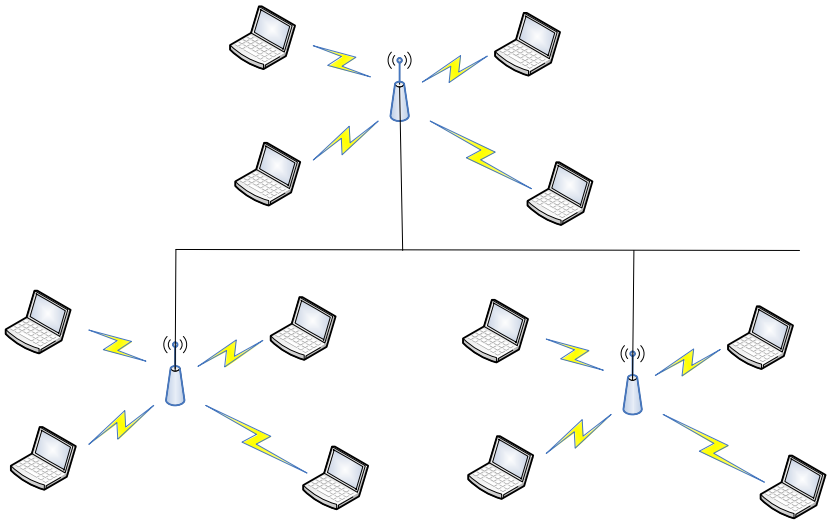


図 1.1　wireless infrastructure mode

無線技術を用いたアドホックネットワークでは，ネットワークを構成するノードのほとんどはバッテリーで駆動する機器であると考えられる．さらに，多くのノードが移動する (あるいは移動可能な) ノードであり，その結果、ネットワークのトポロジが動的に変化すると仮定した

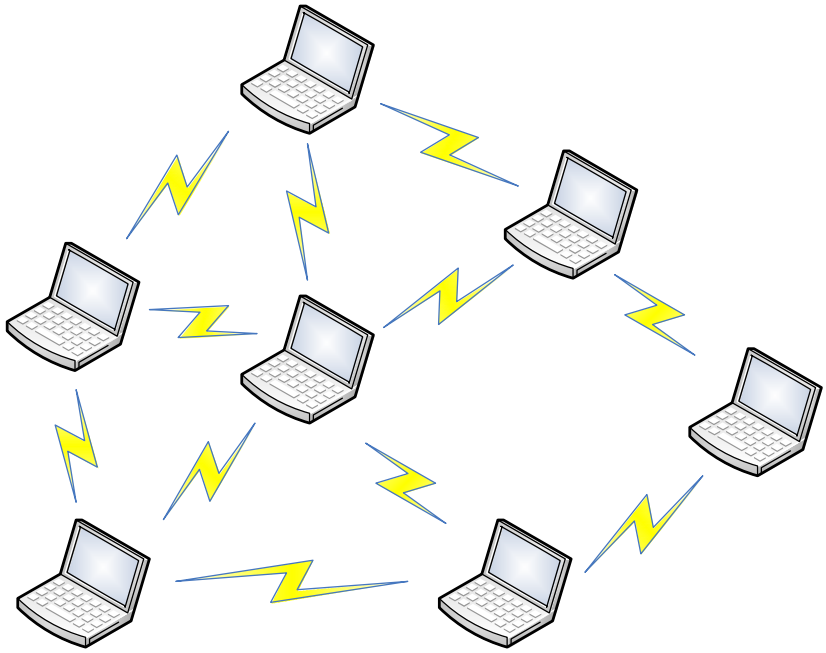


図 1.2　wireless adhoc mode

経路制御技術が適用される必要がある．特に、バッテリー駆動にともなう動作時間の制約は大きく、省電力を実現可能な動的ルーティングプロトコルの適用が必要となる．アドホックネットワークに関するこれまでの研究においては、これら、(1) 省電力 と (2) 動的トポロジーの把握と最適な転送経路の計算 に焦点をあてていた． IETF における MANET(Mobile Adhoc NETworking) 委員会 [6] が定める AODV [4] [8]，DSR [3]，OLSR [5]，TBRPF [7] 等に代表されるような様々なルーティングプロトコルが提案されてきた．このような柔軟なアドホックネットワークにおけるルーティングプロトコルを目指した研究はルーティングの効率性向上やノードの省電力化などに多大な成果をもたらしてきた．

しかし，既存のアドホックネットワークの研究開発は, 基本的にモバイルノードのみで構成されるアドホックネットワークを仮定しており，有線インターネットへの接続性を持つアクセスポイントの存在をほとんど想定していないものとなっていた．アドホックネットワークの有力な利用法として考えられるセンサネットワークやモバイルネットワークにおいては、無線技術で接続されるノードがブロードバンドインターネットに接続された建物の近くで使用されることが多いと想定される．すなわち、このような現実的なネットワーク環境では，各無線ノードの近傍にアクセスポイントが存在する可能性が高いと考えることができる．アクセスポイントはモバイルノードと同じように無線通信を行うことのできるデバイスであるため，アドホックネットワークに属するノードとして、ネットワークアーキテクチャを考えることが可能である．アドホックネットワークはアクセスポイントなどのインフラを設置する必要が無いことを特徴の一つとしているが，既に存在しているアクセスポイントを利用することは否定されるものではない．アクセスポイントは (ほぼ) 無限の電力供給や帯域幅の大きい有線バックボーンと

の接続性を持っており，消費電力の低減やスループット不足への対処を大きな目標としているアドホックネットワークにおいて、むしろ、積極的に利用されるべきものであると考える．そこで本研究では, アクセスポイントの利用を考慮した無線アドホックネットワークプロトコル、MAWC(Mobile Adhoc network with Wired Connection) の提案とプロトタイプシステムの実装を行い、その動作検証を行っている.

1.2　各章の構成

本論文の構成は以下のようである．第四章では関連研究として既存のアドホックネットワークプロトコルによるアクセスポイントの利用法を議論し，その問題点を整理する．第五章では MAWC への要求条件と MAWC のアーキテクチャ設計ならびにアーキテクチャの概要を示す. 第六章では MAWC の実装環境ならびに実装の詳細を解説する．また，MAWC を用いたプロトタイプシステムの評価として、省電力とスループット特性に関する評価を行う．最後に、第七章で本論文のまとめと今後の研究開発の方向性を示す.

第 2 章

無線ネットワーク

本章では，既存の無線ネットワークにおける二つの動作モード (インフラストラクチャモードとアドホックモード) の整理と比較を行い，これら二つの動作モードの統合化に関する議論を行う．さらに，二つのモードを融合し, アクセスポイントをアドホックモードで利用することによる利点に関する議論も行う.

2.1 インフラストラクチャモードとアドホックモード

インフラストラクチャモードでは図 1.1 に示すように，複数のノードが一つのアクセスポイントに接続するスター型のネットワークが構成される．このため，インフラストラクチャモードでは一つのアクセスポイントが周波数や符号化方式あるいは時間スロットによって定義される複数の電波通信チャネルを管理し，それぞれのノードに適宜割り当てるという動作アルゴリズムとなっている．インフラストラクチャモードの特徴は、以下の通りである.

- 既存の有線 LAN と親和性が高い
  アクセスポイントを介在した無線ネットワークは既存の LAN の拡張のように用いることができる．このため，既存の有線ネットワークを変更することなく，アクセスポイントを LAN 内に設置するだけで無線 LAN ネットワークを構築することができる.
  なお，インフラストラクチャモードによるネットワーク環境の構築においては、逆に移動の自由度はアクセスポイントの周辺に限られ，また, 無線クライアントノードが存在するすべての領域にアクセスポイントの設置が行わなけれなければならない.

- 集中管理に適している
  すべてのクライアントノードがアクセスポイントを介して通信を行うために、これらクライアントノードの集中管理が容易となる．また，アクセスポイントを介在したネットワークは DHCP 越しに IP アドレス割り当てを行うことが多いため，IP アドレスによるノードの集中管理も簡易である.

- フレームの衝突が少ない分，電波の利用効率が悪い
  インフラストラクチャモードではノードごとに一つのチャネルを割り当てるため，周波

数効率が悪いとされる．しかし、ノード同士の通信がお互いに干渉する可能性を小さくすることができるとされている．
また，通常アクセスポイントとノードの間の 1 ホップのみで使用されるため，無線を用いながらも帯域はそれほど狭まらない．

インフラストラクチャモードの最大の使用法は LAN 内に設置されたアクセスポイントが無線を通じて LAN への接続性を提供するというものである．この様子を図 2.1 に示す．図 2.1 ではアクセスポイントが接続したノードに LAN への接続性を提供し，アクセスポイントに接続したノードは LAN 内の DHCP サーバから IP アドレスとデフォルトゲートウェイアドレスをもらう．各無線 LAN クライアントノードは、有線 LAN 内に存在するデフォルトゲートウェイを通じてインターネットに接続する．

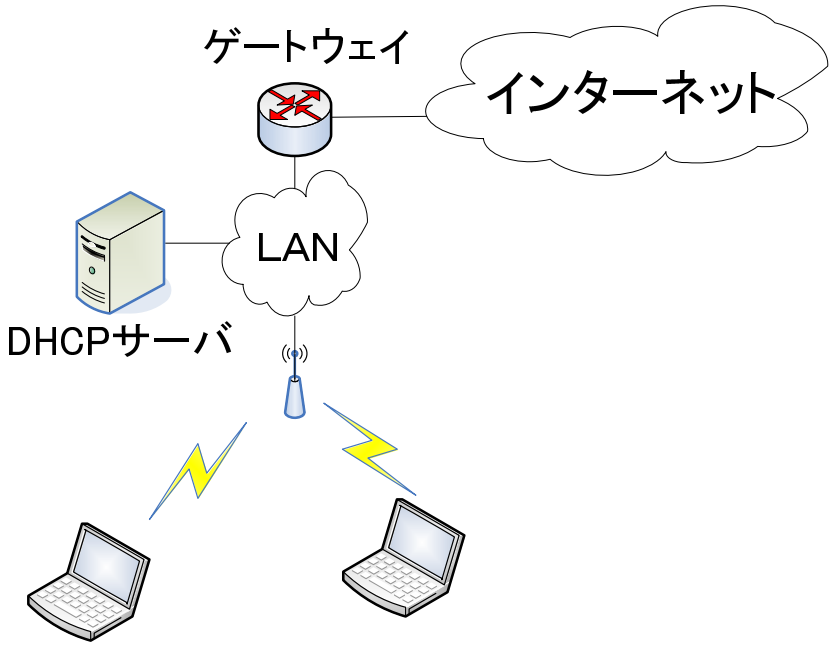


図 2.1　infrastructure mode with LAN

アドホックネットワークでは図 1.2 に示すように，ノードがそれぞれ直接通信を行うピアツーピア型のネットワークが構成される．アドホックモードでは同一アドホックネットワーク内において共通の電波チャネルを使用し，すべてのノードが互いに通信を確立することができるようになっている．既存のアドホックネットワークの特徴は、以下の通りである．

- インフラを必要としない LAN を形成できる
  アドホックネットワークではアクセスポイントのようなインフラの存在を必要条件としていない．何も存在しないところでもモバイルノードが複数台集まればそこにネットワークを構築することが出来る．更にマルチホップを用いることで直接通信できないノード同士が同一ネットワーク上に存在し情報の交換を行うことができる．このような

高いネットワーク構築の自由度のため，アドホックネットワークにおける無線クライアントノードの移動に関する自由度はインフラストラクチャモードよりもはるかに高い．しかしその半面、各ノードも特定の物理的な空間へ固定化が行われないため，各ノード間を相互接続するリンクの通信品質が不安定になりがちである．更に，無線マルチホップを用いるため，一般にインフラストラクチャモードと比べて利用可能な帯域幅が小さい．

- 集中管理が難しい
  アクセスポイントや DHCP サーバのように集中的にノードのアクセスが集まる場所が存在しないため，どのようなノードがアドホックネットワーク内に存在しているのかを把握することは難しい．さらに、ノードがアドホックネットワークに参加したりアドホックネットワークから脱退するような事象の発生頻度が大きくなる傾向にあるり、その結果，IPv4 を用いたアドホックネットワーク内では、一意なアドレスの決定が容易ではなく，アドレス割り当てが大きな技術課題となっている．

- フレームの衝突確率と無線帯域の利用効率
  アドホックネットワークでは同一ネットワーク内で同一周波数チャネルを使用するため，インフラストラクチャモードと比較して同一周波数チャネルを利用するノードの数が多く，周波数効率が良いとされている．しかし、その分互いの通信が干渉を起こしやすく，通信が集中するとスループットの劣化につながってしまう．
  また，無線を用いてマルチホップによってフレームが転送されるため，1 ホップのみのインフラストラクチャモードや有線ネットワークと比較すると帯域が一般的に狭い．

- Single Point of Failure に対する耐性
  アクセスポイントのように通信が一極集中しないため，常に複数の経路が存在する．これにより，ある経路が不通になったとしても他の経路を用いて通信を継続させることができる．

アドホックネットワークのプロトコルでもインフラストラクチャモードのように，インターネットに接続する仕組みは考えられている．この仕組みはアドホックネットワークゲートウェイ (以下，混同しない限りゲートウェイと略す) と呼ばれるルータがインフラストラクチャモードにおけるアクセスポイントのように，インターネット空間とのパケットルーティングを行うことでインターネットと接するという仕組みである．この様子を図 2.2 に示す．ただ，ゲートウェイはブリッジの役割を果たすわけではないため，アクセスポイントと異なり，LAN に備わっている DHCP などのインターネットへのアクセスの仕組みを利用するようには出来ていない．

現在の IEEE802.11 の仕様 [1] ではこの二つのモードには相互通信性がない．このため，アクセスポイントがインフラストラクチャモードで動いている時にアドホックネットネットワークがアクセスポイントを利用しようとしても利用することができない．しかし，アクセスポイントの範囲を広げるためのワイヤレスリピータのように，インフラストラクチャモードにおいてピアツーピア型のネットワークを併用することは技術的には可能である．このため，アクセ

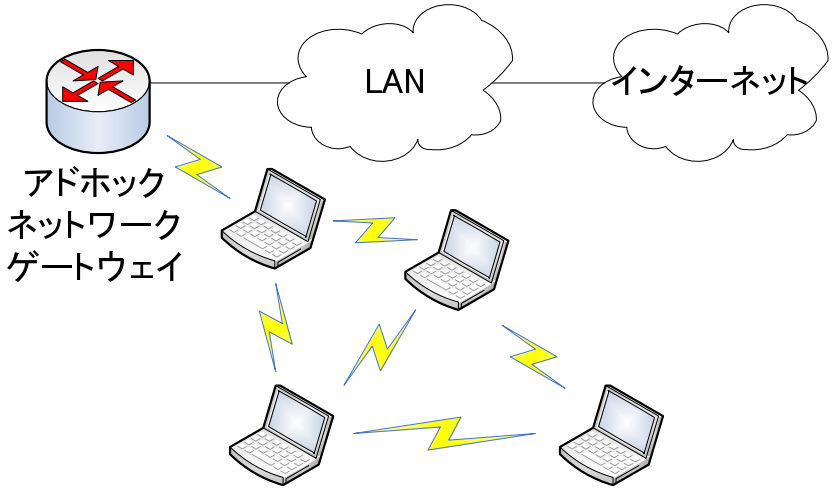


図 2.2　adhoc mode with internet

スポイントをアドホックネットワークに取り入れることは可能であると考えられる．また，最近のアクセスポイントはアンテナや NIC を二つ持っていることは良くあり，片方をアドホックモードにするということも十分考えられる．本稿ではこれ以降，アクセスポイントの無線インターフェースがアドホックネットワークと通信することは可能であるという前提を設ける．

2.2　アドホックネットワークにアクセスポイントを用いる利点

2.2.1　アクセスポイントによるマルチホップ

アドホックネットワークで想定されているノードは主にモバイルノードであり，バッテリ駆動型である．それ故にアドホックネットワークではバッテリの持ち時間が重要な指数の一つとなる．その点，アクセスポイントは一般に電源に接続されており，消費電力を気にする必要がない．アドホックネットワークでは無線マルチホップによってフレームの転送を行うが，無線 NIC において電力を最も消費するのはフレームの送信時である．これはフレームの受信時や受信待機中と比べると消費電力が何倍も大きい．それ故にフレームの転送は転送ノードにかなりの電力負担をしいてしまう．そこで，アドホックネットワークにアクセスポイントを参加させ，マルチホップを一部肩代わりすることでモバイルノードが転送を行う回数を減らし，省電力を実現する．図 2.3 において，左図では中継するモバイルノードが 2 ノード存在しているが，右図では中継するモバイルノードは存在しない．これにより，アドホックネットワーク全体の省電力が実現される．

また，アクセスポイントの参加はアドホックネットワーク内部のノードの数が増えることと同義なため，マルチホップにおけるホップ数も平均的に減少することが考えられる．アドホックネットワークではホップ数が増加するとスループットが反比例して低下することがわかっている．このため，アドホックネットワーク全体のスループットの向上も実現されることになる．

例えば図 2.3 では，アクセスポイントがアドホックネットワークに参加することにより，無線マルチホップのホップ数がモバイルノードのみを経由する 3 ホップからアクセスポイントを経由する 2 ホップへと減少した．ホップ数が 3 ホップから 2 ホップに減少したことにより，周りの影響がなければスループットは 3/2 倍にもなる．

また，アクセスポイントの電力が安定であることから，アクセスポイントの電波は安定かつ強力である．そのため，アクセスポイントの利用はフレームの再送信を減らすという効果があり，その点からもアドホックネットワーク全体の省電力が成立する．さらに，アドホックネットワークではモバイルノードが頻繁に移動する可能性があり，トポロジの頻繁な変更から無線のリンクが不安定であるが，アクセスポイントは移動しないため，アクセスポイントを経由した無線リンクは安定である．しかも，アクセスポイントの加入によって無線リンクの数自体も増えるため，あるリンクが使用不能になったときに迂回路が見つかる可能性が高まる．これらによってアドホックネットワーク全体のリンクの安定性も向上するため，省電力とスループットの更なる向上がおきると考えられる．

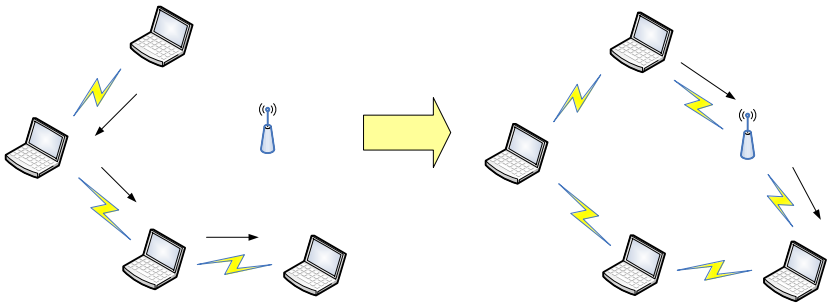


図 2.3　multihop with accesspoint

2.2.2　アクセスポイント間の高速バイパスパス

アクセスポイントとは通常，単独で存在しているものではなく，有線リンクが繋がっているのが普通である．そしてその先にはインターネット空間が広がっている．このため，適切にアクセスポイントを利用することでアクセスポイント間の有線リンクを使用することが可能である．有線リンクは無線マルチホップと異なり，少々ホップ数が増加してもあまりスループットの低下を引き起こさない．しかも，今回考えているケースでは建物のそばなどのアクセスポイント間を想定しているため，あまりネットワーク的な距離も遠くないことが考えられるため，有線リンクにおけるホップ数はあまり増加しないことが多いと考えられる．このため，無線マルチホップのみでアドホックネットワークを構成するよりもはるかに高いスループットを実現できる．

また有線リンクを適切に用いることで，アドホックネットワーク内のモバイルノードが無線マルチホップを行う平均回数そのものが減るため，アドホックネットワーク全体の省電力にも大きく貢献することができる．図 2.4 はアクセスポイント間の高速バイパスパスを利用してい

ない例である．この図では，アクセスポイントはアドホックネットワークに参加しているが，アクセスポイント間の高速バイパスパスが適切に利用されていないため，無駄な無線マルチホップが発生してしまっており，無駄な電力消費とスループットの低下が起きてしまっている．そこで，アクセスポイント間の高速バイパスパスを適切に利用した際のアドホックネットワークを図 2.5 に示す．図 2.5 ではアクセスポイント間の高速バイパスパスを適切に利用することで図 2.4 と比べて無線マルチホップのホップ数が 6 ホップから 2 ホップへと 4 ホップ減っている．また，それに伴ってフレームの転送を行うモバイルノードの数が 5 ノードから 0 ノードへと減っている．これによって大幅なスループットの向上と省電力が見込まれる．

さらに，アクセスポイント間の高速バイパスパスという安定なリンクが増えたことにより，アドホックネットワーク全体のリンク安定度も増加したと考えられる．この例における通信では，関与しているノードがソースノード，デスティネーションノード，アクセスポイントのみであるため，通常であればソースノードかデスティネーションノードが移動したり電源を落としたりしない限り，リンクが途切れることがない．

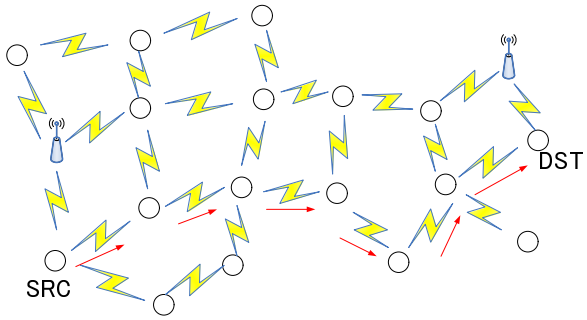


図 2.4　using accesspoint with no bypass

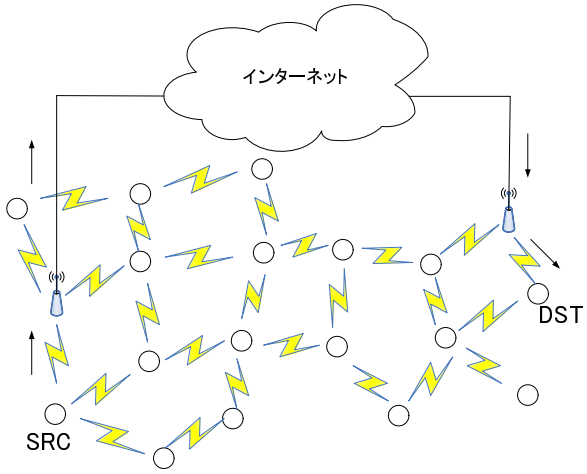


図 2.5　using accesspoint with bypass

第 3 章

2 モード共存における技術課題

本章ではアクセスポイントをアドホックネットワークで利用する際に生ずる主な課題を二点挙げ，それらの詳細を議論する．

3.1 IP アドレスの割り当て

アクセスポイント間の高速バイパスパスを用いるためには，アクセスポイントを通じてインターネットにアクセスできることが必要となる．このためにはアクセスポイントから繋がっている LAN 内部と同じセグメントの IP アドレスを用いて外向きのパケットを送出しなければならない．もし違うセグメントの IP アドレスを勝手に用いてしまうと，その IP アドレスはインターネット内で一意でなくなる可能性があるため，通常 LAN のゲートウェイが外にルーティングしない．仮に LAN から外へのルーティングが行われたとしても，そのパケットに対する返信は違うセグメントへとルーティングされてしまうため，返信が返ってこない．そのため LAN 内部と同じセグメントの IP アドレスを用いて外向きのパケットを送出することが必要となる．

しかし，既存のアドホックネットワークプロトコルでは，事前に IP アドレスが割り当てられていることを前提としているため，LAN 内部と同じセグメントの IP アドレスを取得する仕組みが備わっていない．そのため，新たな仕組みを用意する必要がある．新たな仕組みとしては主に二つの手法が考えられる．

- ノードに LAN と同じセグメントの IP アドレスを割り当てる手法通信を行うノードが DHCP サーバなどからアドレスを取得する (図 3.1)
- 他のノードがパケットの送信元 IP アドレスを書き換える手法通信の中継を行うノードがアドレスを変換する (図 3.2)

3.1.1 プロアクティブ型とリアクティブ型

アドホックネットワークにおけるルーティングプロトコルはプロアクティブ型ルーティングプロトコル，リアクティブ型ルーティングプロトコル，ハイブリッド型ルーティングプロトコ

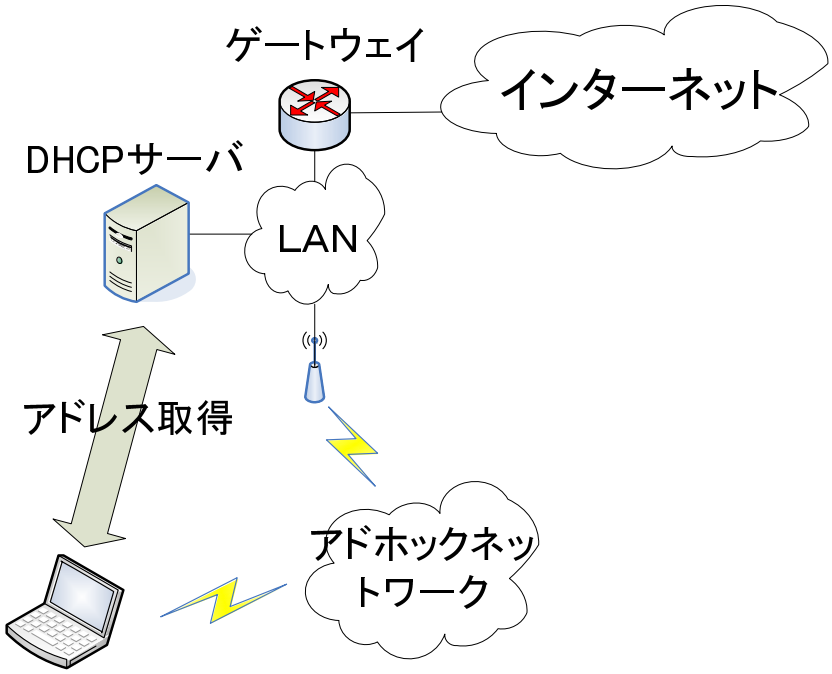


図 3.1　IP assign to each node

ルの三種類に大別される．このうち，ハイブリッド型ルーティングプロトコルは近いノードとはプロアクティブ型ルーティングプロトコルを用い，遠いノードとはリアクティブ型ルーティングプロトコルを用いるというプロトコルである．そのため，ここではプロアクティブ型ルーティングプロトコルとリアクティブ型ルーティングプロトコルについて説明する．

まずはじめにプロアクティブ型ルーティングプロトコルについて説明する．プロアクティブ型ルーティングプロトコルは，アドホックネットワーク内で定期的にルーティング情報を交換し，それぞれのノードがあらかじめネットワーク全体のトポロジに対するルーティングテーブルを持った上で通信を行うプロトコルである．

次にリアクティブ型ルーティングプロトコルについて説明する．リアクティブ型ルーティングプロトコルは，プロアクティブ型ルーティングプロトコルと異なり，定期的なルーティング情報の交換は行わない．そのため，それぞれのノードは全体のトポロジについての情報を知らない．リアクティブ型のルーティングプロトコルでは，ソースノードが通信を開始する際にルートリクエストと呼ばれるコントロールフレームにデスティネーションノードの IP アドレスを入れてアドホックネットワーク全体にフラッディングする．そして，デスティネーションノードはルートリクエストを受け取るとルートレスポンスと呼ばれるコントロールフレームをソースノードに返信する．その一対の通信により，ソースノード，中継ノード，デスティネーションノードの三者は通信経路に関する情報を入手し，通信を行うことができる．

リアクティブ型ルーティングプロトコルは一時的に必要な通信経路のみを入手する手法でありトポロジ全体の情報がないため，アクセスポイントを用いたアドホックネットワークには向いていない．その理由は以下の通りである．

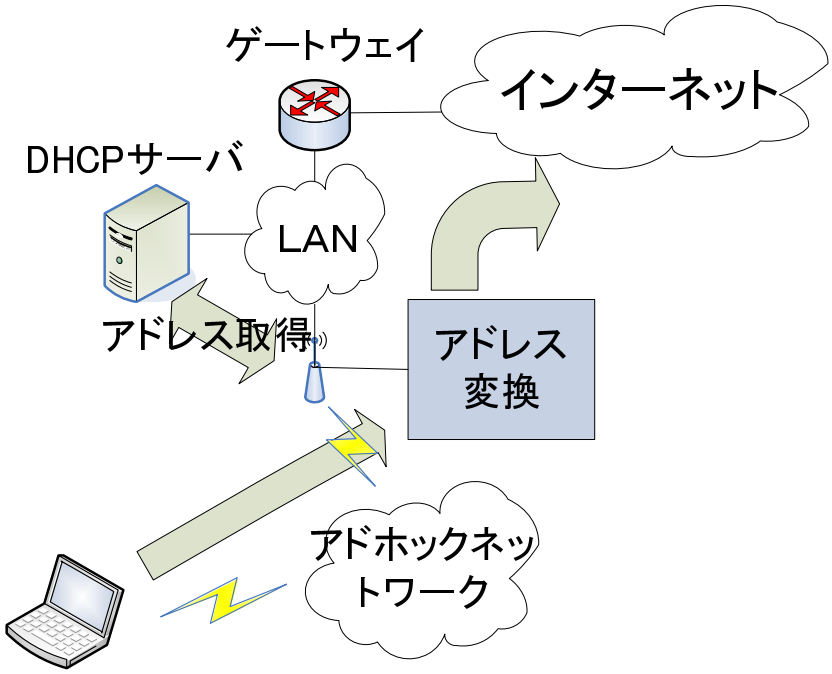


図 3.2　IP translated by relay node

リアクティブ型では，外部ネットワークへのアクセスを確立するためにアクセスポイントがルートリクエストに対してルートレスポンスを返す必要がある．外部ネットワークに存在するノードに対して直接ルートリクエストを行うわけにいかないためである．このため，リアクティブ型でのアクセスポイントの利用は，アドホックネットワークと外部ネットワークをセグメントによって明確に分けて，アドホックネットワーク内に存在しないノードへのアクセスのみアクセスポイントを利用するという方式となっている [21]．これでは，アクセスポイント間高速バイパスパスを利用することができず，アクセスポイントを有効に利用したことにはならない．このため，上記の IP アドレス取得法のうちどちらを用いるとしても，リアクティブ型を用いることはできない．それ故に次章の関連研究の項目でもプロアクティブ型をより詳細に論ずる．

3.2　通信の集中

アドホックネットワークでは一般にホップ数やコントロールメッセージ送受信におけるパケットロス率が主要なメトリックとして経路の選択が行われる．有線は一般に無線と比べて帯域が大きく，パケットロス率が低いため，アクセスポイント間の有線高速バイパスパスは非常に低コストなリンクとして認識されることになる．このため，アクセスポイント周辺に通信が集中してしまうことになる．この通信の集中による問題は二点挙げられる．

- スループットの低下

これまでに記したように，アドホックネットワークはネットワーク内で同一周波数チャネルを用いて通信を行う．このため，アクセスポイントという一点に通信が集中することにより，電波同士の干渉が多数発生してしまうと考えられる．これにより，フレームの再送などが発生してしまい，結果として本来のスループットよりもはるかに低いスループットとなってしまう可能性がある (図 3.3)

- 周辺ノードの疲弊

  アドホックネットワークでは無線マルチホップを用いてフレームの転送を行う．このことはアクセスポイントを利用できるようにしても変わらない．アクセスポイントまでの通信にマルチホップを行うためである．そのため，アクセスポイントに通信が集中してしまうとアクセスポイントの周辺ノードにフレームの送受信を多数強いてしまうことになる．無線で通信を行うノードにおける最大の電力消費はフレームの送信であるため，これは多大に電力消費を促してしまい，周辺ノードのバッテリが尽きるのを早めてしまう．

  当然アクセスポイントにはあらゆる方角からフレームが届く可能性があるが，現実的にアドホックネットワークの特性から考えてアクセスポイントと直接フレームを送受信するノードの数は平均して 10 ノードにも満たないと考えられる．このため，残電力量を用いたルーティング [9] [10] [11] やパケットロス率 [12] を用いたルーティングを行ったとしても，アクセスポイント周辺ノードへの通信の集中は避けられない (図 3.4) これはさらに Single Point of Failure を起こしてしまう可能性を秘めた問題である．アクセスポイントの周辺ノードの数が限られている時に周辺ノードの電力が尽きてしまったら，アクセスポイントへのマルチホップによるアクセスが不可能となってしまい，アクセスポイントの利用ができなくなってしまう可能性がある．このため，アクセスポイント周辺への通信の集中を避ける必要がある．

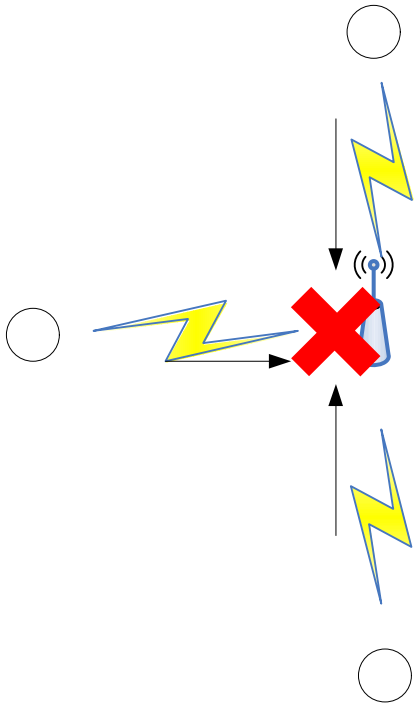


図 3.3　throughput down by traffic congestion around AP

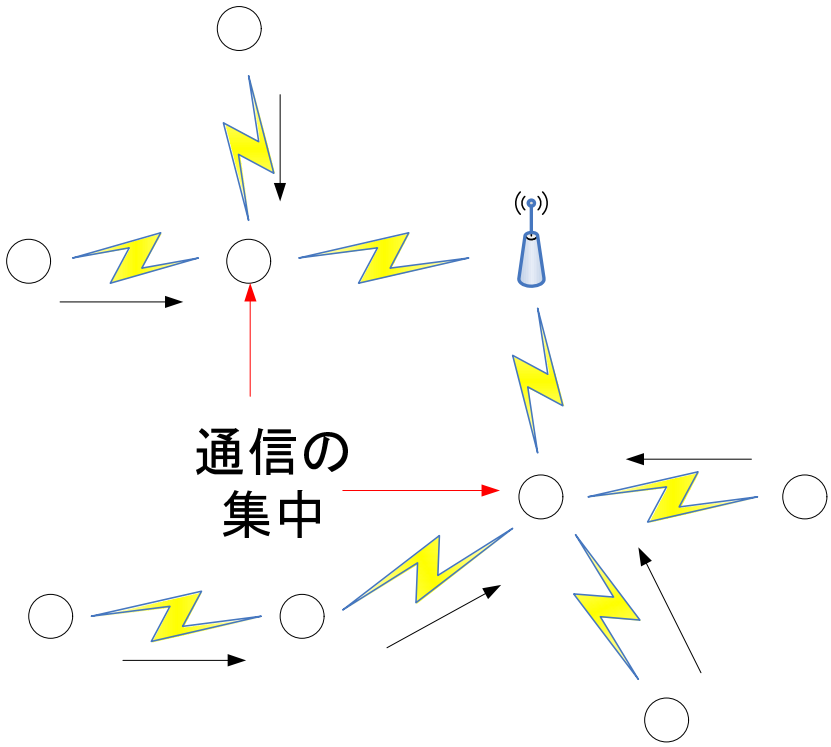


図 3.4　power waste by traffic congestion around AP

第 4 章

関連技術

本章では，関連研究として，既存のアドホックネットワークプロトコルとアドホックネットワークの応用として考えられているワイヤレスメッシュネットワークについて記す．

前章における IP アドレス取得法の項目で示したように，アドホックネットワークには大きくプロアクティブ型，リアクティブ型，ハイブリッド型の三種類が存在する．前章で示したように，プロアクティブ型でなければアクセスポイント間高速バイパスパスを利用することができないため，本稿では比較対象としてリアクティブ型ルーティングプロトコルを考えず，プロアクティブ型ルーティングプロトコルのみを考えることとする．プロアクティブ型ルーティングプロトコルとしては代表的な OLSR について比較を行い，リアクティブ型ルーティングプロトコルに関しては代表的な AODV と呼ばれるルーティングプロトコルについて動作原理のみ紹介する．

4.1 Optimized Link State Routing Protocol(OLSR)

4.1.1 基本システム

OLSR [5] はプロアクティブ型のアドホックネットワークプロトコルである．OLSR では全体のトポロジの把握にリンクステート方式を採用している．リンクステート方式とは，ノード間にリンクが形成されているかどうかというリンクの状態 (リンクステート) をそれぞれのノードがアドホックネットワーク全体にフラッディングして伝える方式である．そしてそれぞれのノードはそのリンクステート情報に自ノードを始点としたダイクストラ法を適用することで各ノードまでのホップ数と次ホップを計算し，routing table に格納する．そして各ノードは通信を行う際に routing table を参照して通信を行う．OLSR は，ルーティング情報を格納する routing table を OS の IP routing table としており，routing table を作成するのみで実際の通信には関与しない．

OLSR では，まずノードは自らの IP アドレスを入れた HELLO メッセージをブロードキャストする．それによって各々のノードは隣接ノードの IP アドレスを知る．なお，HELLO メッセージは転送されないため，1 ホップのみのブロードキャストである．そして次に各々のノー

ドは HELLO メッセージの交換により得た隣接ノードの IP アドレスと自らの IP アドレスを HELLO メッセージに入れてブロードキャストする．これにより，各々のノードは隣接 2 ホップまでのノードの IP アドレス情報を得る．また同時に片方向リンクを排除する．片方向リンクとは，図 4.1 に示すように，ノードの電波送信強度などの違いにより，一方向にしか通信ができないようなリンクのことである．片方向リンクは，隣接ノードから届く HELLO メッセージの中に自らの IP アドレスが入っているかどうかを見ることで判別する．

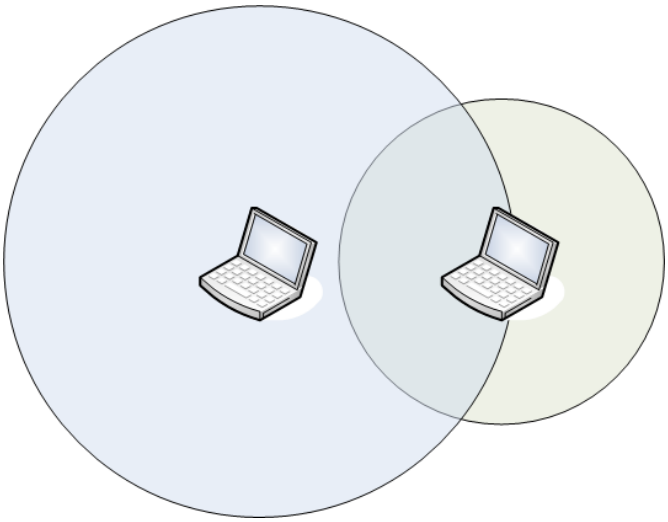


図 4.1　unidirectional wireless link

また，OLSR は HELLO メッセージとは別に TC(Topology Control) メッセージというものを定期的に送信する．このメッセージは MPR 集合というものを利用してアドホックネットワーク全体のトポロジをアドホックネットワーク全体に周知するために送出される．MPR 集合とは，アドホックネットワーク全体へのフラッディングを効率的に行うための仕組みである．MPR 集合の考え方を図 4.2 に示す．図 4.2 は，2 ホップまでの全ノードにソースノードからフレームをフラッディングした場合を表している．上図は MPR 集合を用いなかった場合のフラッディングである．これを見ると 1 ホップ目のノードにおける再ブロードキャストが同一の 2 ホップ目のノードに複数届いてしまっており，効率が悪い．そこで下図のように，再ブロードキャストを行う 1 ホップ目のノードを限定する (赤いノード) ことによって，2 ホップ目のノードに複数ブロードキャストが届くことを防ぐことができる．この赤いノードを MPR と呼ぶ．そしてその場合のソースノードを MPR セレクタと呼ぶ．もちろん，MPR は常にこの図のように厳密に決定できるわけではないので，なるべく重なりが少なくなるように，かつ計算量があまり大きくないように作られたアルゴリズムで決定される．TC メッセージは，MPR がそれぞれ MPR セレクタと自分との間のリンクについて定期的にフラッディングを行うものである．なお，MPR は入れ子関係を築くことができ，自分以外のノードに関する MPR と MPR セレクタを兼ねることは可能である．

また，OLSR には外部ネットワークとの接続を広告するための HNA メッセージと呼ばれる

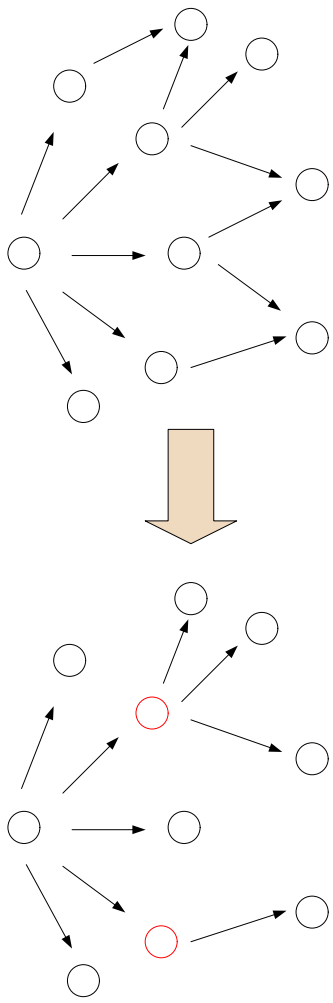


図 4.2　MPR set

コントロールメッセージが存在する．このメッセージには，外部への接続を提供しているノードの IP アドレスと外部ネットワークのプレフィクス情報の対が書き込まれている．OLSR ではこのメッセージを各ノードにフラッディングし，各ノードがそれを routing table に書き込むことで外部ネットワークとの接続を広告する (図 4.3)．OLSR でのアクセスポイントの利用は主にこのメッセージを用いてデフォルトルートをアクセスポイントに指定することで行われる．

4.1.2　アクセスポイントの利用

アクセスポイントを利用するためにはアクセスポイントからつながる有線 LAN 内と同一セグメントの IP アドレス (LAN-IP と呼ぶ) を送出パケットにつける必要がある．そしてそのための方法は上述のようにソースノードが直接 LAN-IP を持つ手法と中継ノードがパケットの送信 IP アドレスを変換する手法の二つがある．このうち，中継ノードがパケットの送信 IP アドレスを変換する手法は主に IPv4 に対して用いられており，

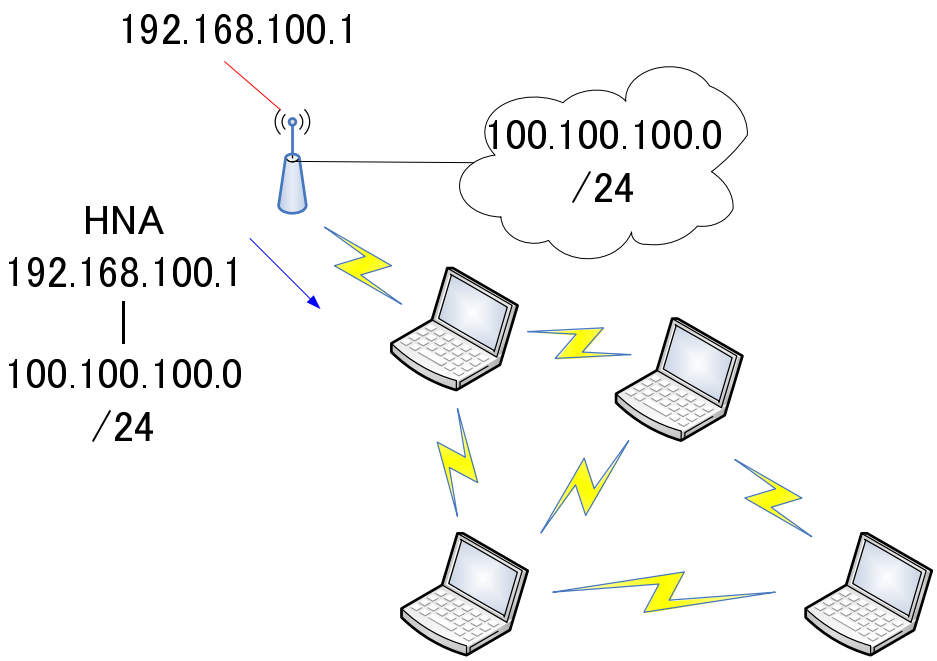


図 4.3　HNA message

- アクセスポイントで NAT [18] を用いる手法
- アクセスポイント間で IP-in-IP トンネリング [22] [23] を行う手法
- Mobile IP [19] を用いる手法

といった手法が挙げられる．しかし，これらの手法には以下に挙げるような問題点がある．

- NAT を用いる手法では，アクセスポイントを通じての外部ネットワークとの通信は可能であるが，アクセスポイント間の高速バイパスパスを利用することはできない．さらに，アドホックネットワーク内に複数のアクセスポイントがあるときにプライベート IP アドレス同士が衝突してしまったりするため，IP アドレスの割り当てが困難となる．
- IP-in-IP トンネリングを行う手法は，アクセスポイント間の高速バイパスパスを利用することは可能であるが，外部ネットワークとの通信が不可能である．さらに，アクセスポイントの増加に伴うトンネル設置作業が大きな手間となる．
- Mobile IP を用いる手法 [20] では，新たに Home agent や Foreign Agent などを設置する手間がかかってしまう．

そこで本稿ではアクセスポイントの利用手法における比較対象として，ソースノードが直接 LAN-IP を持つ手法についてのみ説明する．この手法は，IPv4 か IPv6 かによって手法が異なるため，それぞれに分けて説明する．

IPv4 における IP アドレス割り当て

IPv4 における第一の手法として，ソースノードがアドホックネットワーク内に出現した時に周囲のノードが DHCP relay を動かし，DHCP との通信を成立させるという方法 [13] がある．しかしこの手法では周囲のノードが既に DHCP から IP アドレスを取得しているという前提が必要となる．これは図 4.4 において，アドホックネットワーク内のノードが既に DHCP サーバによってコンフィグされているということである．このため，複数のノードが同時にアドホックネットワークに入ったならば，先にアドホックネットワーク内のコンフィグが行われなければならない．ソースノードはそれによる遅延を待たなければならない．さらに，アドホックネットワーク内に複数のアクセスポイントが存在している場合，先にコンフィグが完了している，より遠いアクセスポイント内の DHCP サーバへと誘導される可能性もある．このため，この方法による IPv4 の IP アドレス割り当てはあまり良い手法とは言えない．

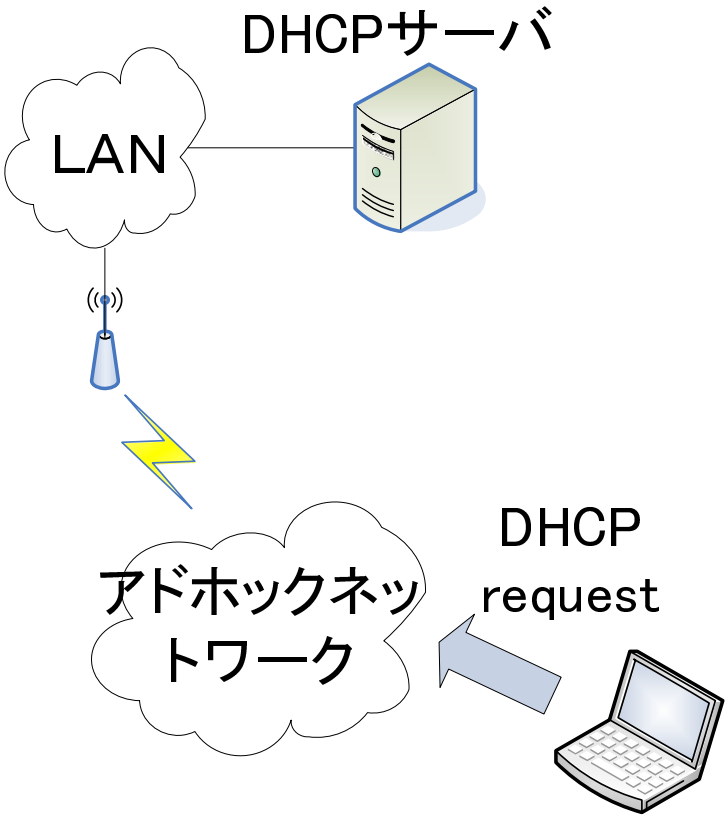


図 4.4　Problem of DHCP relay

第二の手法として，ソースノードに一時的な IP アドレスを割り当て，アドホックネットワークに参加させてからアクセスポイントを通じて DHCP にアクセスさせるという手法 [14] がある．一時的な IP アドレスに利用できる IP アドレスとして，IPv4 にはプライベート IP アドレス (192.168.*.*, 172.16.*.*) と APIPA(automatic private IP addressing) [24] におけるリン

クローカルアドレス (169.254.*.*) がある．APIPA とは，Microsoft の Windows に搭載されている IP アドレスの自動コンフィグレーションの仕組みであり，DHCP request を送った後にしばらく応答がない場合に自動で IP アドレスが割り当てられる仕様である．これらの IP アドレスを用いてアドホックネットワーク内で一意な IP アドレスを割り振る研究は多数行われている [15] [16]．それらの研究に共通する概念として，一意な IP アドレスを割り振るために DAD(Duplication Address Detection) と呼ばれる仕組みが必要となる．DAD とは IP アドレスの重複を調べる仕組みである．DAD では，ノードはネットワークプレフィクスから IP アドレスを任意に選び，同じ IP アドレスを使用しているノードがいないかどうかを，ICMP メッセージをアドホックネットワーク全体にフラッディングすることによって調べたり，ルーティングテーブルから調べたりする．そして重複 IP アドレスがない場合，その IP アドレスを使用する．ただ，そのアドレスが一意なのは DAD を行った時のアドホックネットワーク内のみであり，新たにほかのアドホックネットワークと統合がおきたりすると IP アドレスの一意性を確保することは大変困難となる．更にこれらの手法では，DAD を行いつつ一時的な IP アドレスを割り当ててそれがアドホックネットワークに知れ渡った上で新たに IP アドレスを取得してそれをアドホックネットワーク全体に再度知らしめなければならないため，IP アドレスを取得し，通信を開始するまでに大きな遅延が発生してしまう．

IPv6 における IP アドレス割り当て

IPv6 では，一つの NIC(network interface card) に複数の IP アドレスを割り当てることができる．一般にはリンクローカルアドレスと呼ばれる IP アドレスとグローバルアドレスと呼ばれる IP アドレスの二つが割り当てられることになっている．リンクローカルアドレスとは，IPv4 におけるプライベート IP アドレスに相当するもので，同一セグメント内においてのみ使用されるアドレスである．これは NIC の MAC アドレスを用いて自動生成される．また，グローバルアドレスは IPv4 のグローバル IP アドレスに相当するもので，世界中で一意な IP アドレスである．ただ，IPv6 では DHCP サーバから IP アドレスを得るのではなく，RA(router advertisement) を用いて IP アドレスの自動生成が行われる．RA はネットワークのプレフィクス情報とデフォルトゲートウェイ情報が含まれているメッセージであり，デフォルトゲートウェイによって生成される．また IPv6 にはデフォルトゲートウェイに RA を促すための RS(router solicitation) がある．RS によって生成された RA は通常の RA と異なり，ユニキャストで RS を送信したノードに送られる．このため，IPv6 ではリンクローカルアドレスを用いてアドホックネットワークに参加し，RS によって RA をもらうという手法と，RA をアドホックネットワーク全体に常にフラッディングしておいて，直接グローバルアドレスを生成し，それを用いてアドホックネットワークに参加するという手法の二つがある．

4.2 Ad hoc On-Demand Distance-Vector Protocol(AODV)

4.2.1 基本システム

AODV [4] は，リアクティブ型の代表的なルーティングプロトコルであり，Distance-Vector のアルゴリズムを使いながら，オンデマンドに経路を発見するリアクティブ型のルーティングプロトコルである．DSR との違いは Distance-Vector であること，シーケンス番号を管理し，それをルーティングに積極的に利用すること，各ノードは非常に短い間有効な経路表を持ち，データパケットはそれを用いて転送されること，各経路表のエントリーには precursor リストがあり，リンクに障害があったときに利用されることが挙げられる．

まず通信を開始するにあたって，ソースノードはデスティネーションノードへの経路を発見するために，ソースノードの IP アドレス，デスティネーションノードの IP アドレス，ホップ数 (開始時は 0)，限界ホップ数 (TTL) とシーケンス番号をルートリクエストパケットに入れてアドホックネットワーク全体にフラッディングする．ルートリクエストパケットを受信したノードは，ホップ数を 1 増やし，限界ホップ数を 1 減らす．そして限界ホップ数が 0 でなければイーサネットヘッダの送信元 MAC アドレスを書き換えて再びフラッディングする．また，その際ノードは自身の AODV routing table に

前ホップのノードの IP アドレス-ソースノードの IP アドレス-ホップ数

図 4.5　AODV routing table

図 4.5 に示すような一対のエントリを書き加える．このフラッディングにより，ルートリクエストパケットがデスティネーションノードに到達する．デスティネーションノードは図 4.5 に示す routing table に従い，ルートレスポンスパケットをソースノードに向かってユニキャストで送出する．中継ノードはルートリクエストパケットの時と同様に，ルートレスポンスパケットについても図 4.5 のようなエントリを routing table に書き加える．これにより，ソースノードとデスティネーションノードが双方向に通信可能となる．この様子を図 4.6 に示す．

4.3 メッシュネットワーク

メッシュネットワークはアドホックネットワークと近い概念であるが，アクセスポイント間をアドホックネットワークで結ぼうという発想のもので，全てのノードがアドホックモードで動くという前提を置くアドホックネットワークプロトコルとは考えが異なっている．ただ，現在仕様策定中であり，まだ仕様がほとんど明らかになっていないため，あまりわかっていることは無い．

メッシュネットワークの概念を図 4.7 に示す．

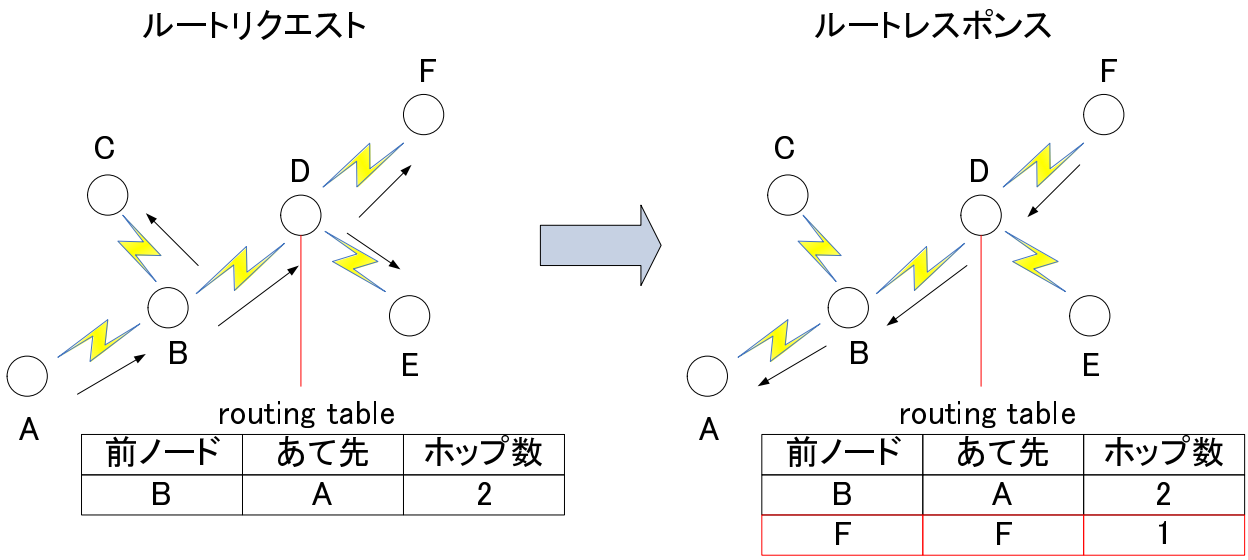


図 4.6　AODV route request/response

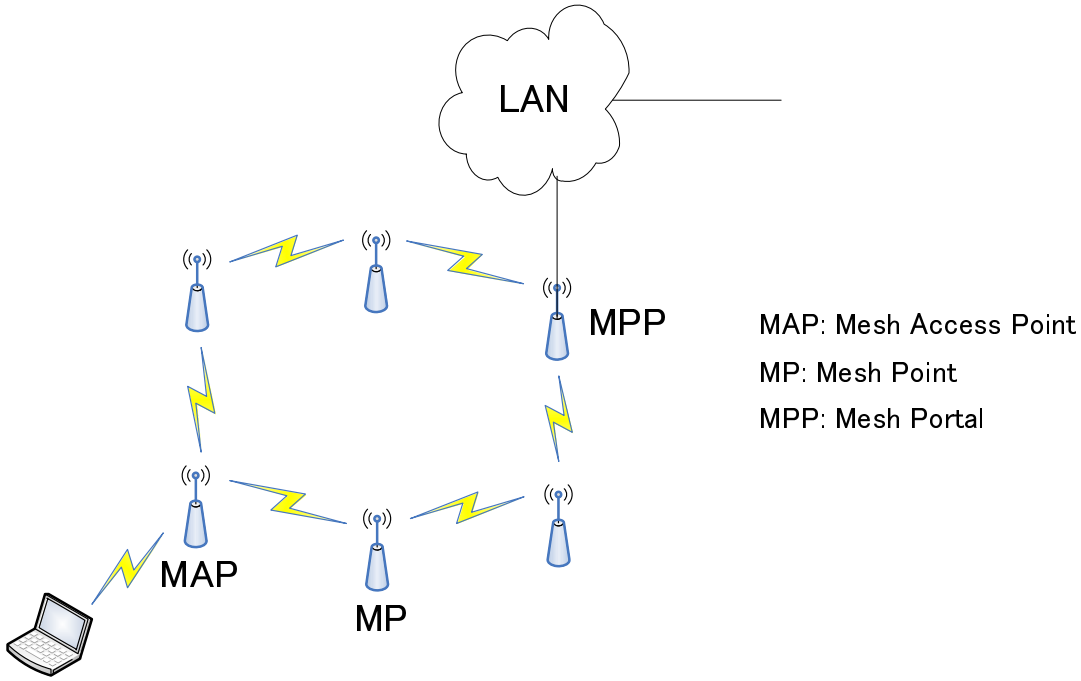


図 4.7　wireless mesh network

メッシュネットワークでは三種類のアクセスポイントが規定されている．アクセスポイントの種類とその役割は

- MAP(Mesh Access Point)
  既存のアクセスポイントに近い役割であり，ノードとメッシュネットワークとのゲート

ウェイとなるアクセスポイントである．

- MP(Mesh Point)
  アドホックネットワークにおける中継ノードに相当するものである．主にメッシュネットワーク内におけるフレームの中継を行う．

- MPP(Mesh Portal)
  アドホックネットワークにおけるゲートウェイに相当するものである．ただ，アドホックネットワークのゲートウェイとは異なり，アクセスポイントのように透過的に既存の LAN との接続性を提供することができる．

今までのところ規定されている仕様としては，OLSR などのプロアクティブ型アドホックネットワークルーティングプロトコルと，リアクティブ型ルーティングプロトコルを合わせたような仕様となっている．基本的にはリアクティブ型のルーティングプロトコルである．ただ，MAP に接続したノードによる通信手法はまだあまりよくわかっていないため，アクセスポイント間での通信を中心に説明する．

アクセスポイントは既存のアクセスポイントと同様に定期的にビーコンを送出する．それを受信した周囲のアクセスポイントはその情報を確保しておく．それにより，それぞれのアクセスポイントは周囲 1 ホップのアクセスポイントの MAC アドレス情報を取得し，Layer-2 routing table として保持する．それ以外の情報は基本的に保持しない．ただし，ルートポータルと呼ばれるアクセスポイントが存在する場合は，ルートポータルが一元的にメッシュネットワーク全体の情報を管理する．ルートポータルは常に自身の情報をメッシュネットワーク全体にフラッディングし続けることで存在を示す．

メッシュネットワークにおける実際の通信は以下のようである．

ルートポータルが存在しない場合

1. Layer-2 routing table を参照し，その中に通信したい相手の MAC アドレスがあるかどうかを検索する．

2. 通信したい相手が存在する場合には直接通信を行う．通信したい相手が存在しない場合には，リアクティブ型アドホックネットワークルーティングプロトコルと同様のルートリクエストパケットをネットワーク全体にフラッディングする．

3. ルートリクエストパケットに対するルートレスポンスパケットが返信されてきたら，その中に含まれている情報を基に，一時的な routing table を構築し，それを用いて通信を行う．
   ルートレスポンスパケットが返信されてこなければ，通信したい相手は外部ネットワークに存在すると考える．そして MPP に向かってパケットを投げ，MPP によって外部ネットワークへとフォワーディングしてもらう．

ルートポータルが存在する場合

1. Layer-2 routing table を参照し，その中に通信したい相手の MAC アドレスがあるかどうかを検索する．
2. 通信したい相手が存在する場合には直接通信を行う．通信したい相手が存在しない場合には，ルートポータルに向かって相手がメッシュネットワーク内にいるかどうかを聞く
3. 相手がメッシュネットワーク内にいる場合，ルートポータルは相手に向かってそのパケットを転送する．そして，相手から送信元ノードに向かってルートリクエストパケットがフラッディングされる．
4. ルートリクエストパケットを受け取った送信元ノードはルートレスポンスパケットを通信相手へと返信する．これにより通信が開始される．
5. 相手がメッシュネットワーク内にいない場合，ルートポータルは送信元ノードにそのことを教える．そしてルートポータルは外部ネットワークにフレームを転送する．

第 5 章

MAWC システムアーキテクチャ

本章では，本稿で提案するシステムについて，要求条件と実際のシステム設計の二点から詳細に議論する．

5.1 提案システムへの要求条件

関連研究の項目で議論したように，アドホックネットワークにアクセスポイントを利用して，アクセスポイントによる無線マルチホップとアクセスポイント間高速バイパスパスを利用するためにはプロアクティブ型のルーティングが必要となる．しかしながら OLSR のように IP アドレスを用いてルーティングを行うモデルでは IP が IPv4 である場合，アクセスポイントから繋がる LAN で配布されている IP(LAN-IP と呼ぶ) を得るために複雑なアルゴリズムと多大な時間の遅延が発生する．このため，IPv4 の初期値である空白 IP アドレスにおいてもルーティングできるようなプロトコルを用いることで，いきなり LAN-IP を取得できるような仕組みが必要である．

また，IPv6 の場合は IP アドレスを用いたルーティングでも LAN-IP を時間遅延なく利用可能である．Layer-3 のプロトコルが IPv6 のみで全てのネットワークが構成されていれば，これでも問題はない．しかしながら IPv4 にのみ対応しているノードや Bluetooth などの IP 以外の Layer-3 プロトコルが実装されているノードなどが大量に世の中にはある上に，IPv4 のみがルーティングされている LAN なども数多く存在する．このため，IPv6 しかルーティングできない IPv6 用プロアクティブ型ルーティングプロトコルでは実際に世の中で運用するには困難が多い．そこで，IPv4 におけるアドレスの空白状態や IPv6，Bluetooth などのさまざまな Layer-3 プロトコルを共存させることのできるプロアクティブ型のルーティングプロトコルが必要となる．更にそのプロトコルでは，アクセスポイントを介した外部ネットワークとの接続と，アクセスポイント間高速バイパスパスを考慮したルーティングが求められる．

また，アクセスポイントをアドホックネットワークに導入することによってアクセスポイント周辺に通信の集中が起きる．これによる問題点は既に記した通りである．アクセスポイントを導入することによってアドホックネットワークに不利な点が生じてしまってはアクセスポイントを導入する意味がないため，通信の集中をできる限り避ける仕組みも必要となる．

5.2　ルーティング基本原理

IPv4 の初期値である IP アドレスの空白状態において既に一意なアドレスとして NIC に割り振られているアドレスとして MAC アドレスがある．MAC アドレスは図 5.1 に示すように，Layer-2 と Layer-3 を分離し，Layer-3 のプロトコルに非依存の状態となるように設計されたものである．このため，MAC アドレスを用いてルーティングを行うことで Layer-3 のプロトコルの種類や状態に非依存でルーティングを行うことが出来る．今回は MAC アドレスルーティングに加えて，特に IPv4 における LAN-IP の取得について実装を行ったため，それらに関する詳細について示す．

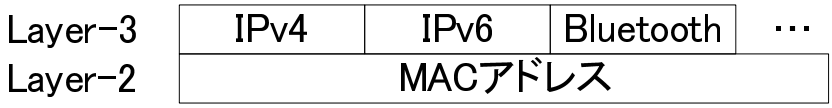


図 5.1　interoperability between Layer-2 and Layer-3

5.2.1　ルーティング情報の収集

MAC ルーティングを行うために，まず MAC アドレスベースでアドホックネットワーク全体のトポロジを把握する必要がある．今回提案するアドホックネットワークルーティングプロトコル (MAWC と呼ぶ) では MAC アドレスベースでトポロジ把握メッセージをやり取りすることによって MAC アドレスによるトポロジを把握する．トポロジ把握メッセージは OLSR と同様の，HELLO メッセージと TC(topology control) メッセージの二つを用いる．トポロジ把握の方式としては，OLSR と同様のリンクステート型を用いることとする．ディスタンスベクター型という手法もあるが，アドホックネットワークのようにノードに動きがあるネットワークではコントロールメッセージによるトポロジ把握がかなり困難となるためである．具体的なコントロールメッセージのフォーマットと通信については 6.2.1 で説明する．

コントロールメッセージによって，アドホックネットワーク全体の MAC アドレスベースのリンクステート情報を得たノードは，その情報にダイクストラアルゴリズムを適用することで MAC アドレスベースの routing table(MAWC routing table) を得る．なお，メトリックには hop 数を用いて計算している．例えば図 5.2 のようになる．複数の経路が同じ値の hop 数を示した場合は先に計算が行われた経路を採用する．

5.2.2　ネットワークの判断

ネットワークの判別手法

アクセスポイントを活用するためには外部ネットワークのノードとアドホックネットワーク内部のノードを Layer-3 で区別する必要がある．通信開始時には通信相手に関しては Layer-3

	Dst MAC	Next MAC	Hop count
1	00:11:22:33:44:55	00:11:22:33:44:55	1hop
2	01:23:45:67:89:ab	00:11:22:33:44:55	2hop
3	aa:bb:cc:dd:ee:ff	12:34:56:78:90:ab	2hop
4	12:34:56:78:90:ab	12:34:56:78:90:ab	1hop

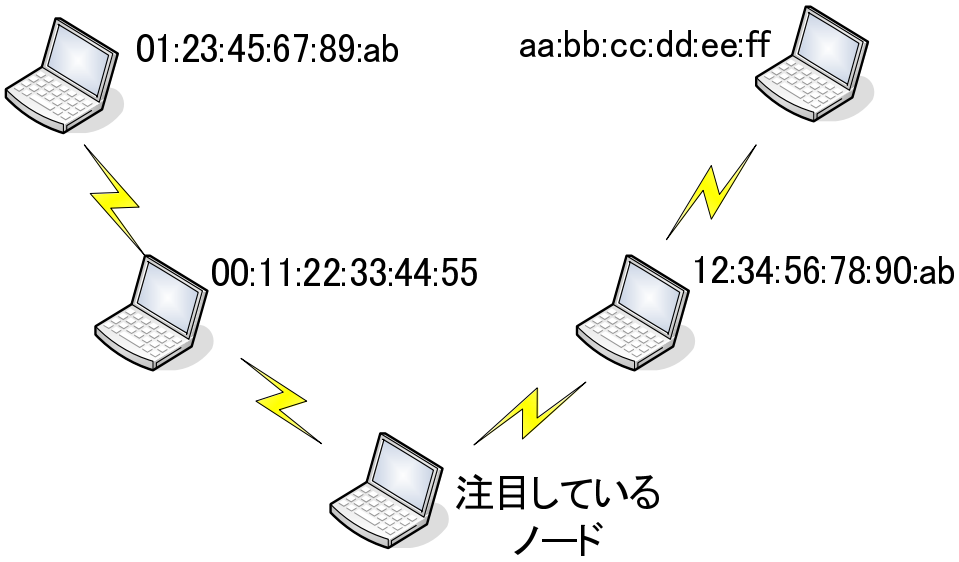


図 5.2　MAC based routing table

の情報しかなく，その情報を基にノードの居場所を外部ネットワークか内部か判断しなければならないためである．通常では IPv4 ではセグメントが同様であれば，ARP メッセージをフラッディングすることにより解決する．しかし MAWC ではこの点に関する情報をプロアクティブ型で収集する．すなわち，アドホックネットワーク内部にいるノードの Layer-3 における識別情報 (IP アドレス) をプロアクティブ型でコントロールメッセージに載せて収集するということである．

この理由は二点ある．

- 外部ネットワークとの明確な区別
  MAWC では，アクセスポイントの利用法としてアクセスポイントによるマルチホップ

とアクセスポイント間の高速バイパスパスを挙げている．
アクセスポイント間の高速バイパスパスを利用するためには，通信相手であるノードはアドホックネットワーク内部に存在しているにもかかわらずアクセスポイントを経由してフレームを送信するということを行わなければならない．もし既存のリアクティブ型のアドホックネットワークプロトコルにおけるルートリクエストパケットのようにアドホックネットワーク全体に ARP をフラッディングして通信相手を探してしまうと，通信相手から直接 ARP レスポンスが返信されてきてしまう．このため，通信相手との間で高速バイパスパスを用いることができるのかどうかわからなくなってしまう．

- 遅延の短縮
  MAWC では MAC アドレスでルーティングを行うために MAC アドレス情報を既に各ノードが保持している．その状況でわざわざ ARP をアドホックネットワーク全体にフラッディングして通信相手の MAC アドレスを取得することは，コントロールメッセージの意味のない増加と通信開始までの遅延の意味のない増加と考えられる．そこで Layer-3 のアドレスを Layer-2 のアドレスに各ノードが変換できるようにすることでコントロールメッセージと遅延の両方の無駄を省くことが出来る．MAWC では OLSR などの IP アドレスによるルーティングを行うプロトコルよりもコントロールメッセージは大きくなるが，その分 ARP を抑制することによる通信遅延の低下が生ずるため，どちらが一方的に有利ということにはならない．

また，IP アドレスをプロアクティブ型で収集することは一見，OLSR のような IP アドレスベースでルーティングを行うプロトコルと同様に見えるかもしれない．しかし，MAWC ではあくまでルーティングには MAC アドレスを用いており，IP アドレスが必要なのは通信相手のみである．中継ノードの IP アドレスは必要としない．この点で MAWC は OLSR などのような IP アドレスベースでルーティングを行うプロトコルと異なっている．

ネットワークの判別

MAWC では前節に挙げた理由により，HELLO メッセージと TC メッセージに IP アドレスを載せることで各ノードに IP アドレス情報を配布する．各ノードはリンクステート情報から MAWC routing table を計算した際に routing table のデスティネーションノードそれぞれに対応した IP アドレスを routing table の一項目として付加する．そしてその routing table のエントリに通信相手の IP アドレスが存在するかどうかで通信相手が外部ネットワークのノードかアドホックネットワーク内部のノードかを判別する．

5.2.3　通信開始までの流れ

通常のネットワークでは図 5.3 に示すようなフローに沿ってあて先のアドレスは決定される．

MAWC では，MAWC routing table にアドホックネットワーク内のノードに関する IP アドレスと MAC アドレスの対が格納されているため，それを ARP Table の代わりとして用いる

通信の処理の流れ

1. パケットデータが作られる．
2. IP ヘッダが作られ，あて先 IP アドレスが代入される
3. OS の IP routing table を見て，次にパケットを渡す相手を決定する
4. パケットに ether ヘッダが作られる
5. 次にパケットを渡す相手に関して ARP Table を参照する
6. もし ARP Table に相手のエントリがあれば，その MAC アドレスをあて先 MAC アドレスに代入する
7. エントリがなければ相手に向けて ARP request を送信し，MAC アドレスの解決を行う．そして解決された MAC アドレスをあて先 MAC アドレスに代入する．

図 5.3　usual communication flow

ことでアドホックネットワーク内部に存在するノードへの ARP request を抑制する．また，外部ネットワークとの通信の場合は ARP request を，最寄のアクセスポイントを通じてアクセスポイントから繋がる有線へと送信する．MAWC における一連の通信開始時の処理の流れは図 5.4 に示すとおりである．

MAWC の通信の処理の流れ

1. パケットデータが作られる．
2. IP ヘッダが作られ，あて先 IP アドレスが代入される．
3. パケットに ether ヘッダが作られる．
4. あて先 IP アドレスに関して MAWC routing table の IP アドレス項目を検索する．
5. もし MAWC routing table にエントリがあれば，その MAC アドレスを取得する．
6. エントリがなければ ARP によってあて先ノードやデフォルトゲートウェイの MAC アドレスを取得する．
7. 得た MAC アドレスをあて先 MAC アドレスに代入する．
8. あて先 MAC アドレスを MAWC routing table から検索する．見つかれば直接ルーティングする．見つからなければ最寄のアクセスポイントを通じて外部ネットワークへとルーティングする．

図 5.4　MAWC’s communication flow

5.2.4　MAC アドレスルーティング

通常，NIC は IP アドレスの前に MAC アドレスによって自分宛のパケットかどうかを判別する．このため，アドホックネットワークでは ether ヘッダ上に置かれる送信元 MAC アドレスとあて先 MAC アドレスはホップバイホップで書き換えられながらルーティングされる．しかし，MAC アドレスでルーティングを行うためには MAC アドレスによって送信元ノードとあて先ノードについても指定しておかなければならない．そこで，MAWC では MAC アドレスによるカプセリングを行うことでこの問題を解決する．カプセリングすることによって保存するべきは送信元ノードの MAC アドレスとあて先ノートの MAC アドレスであるが，MAWC はアクセスポイントを利用することと利用するアクセスポイントを明示するために，更にアクセスポイント指定用の MAC アドレス空間を用意する．ether ヘッダの MAC アドレスに関する変更点を図 5.5 に示す．

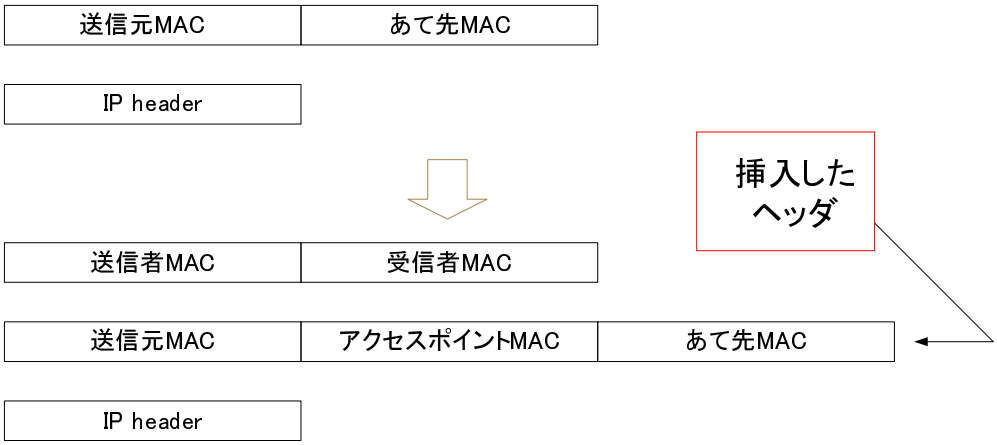


図 5.5　MAWC header

図 5.5 における送信者 MAC アドレスと受信者 MAC アドレスとは，フレームを中継する際の中継ノードを示したものである．これらは ether ヘッダにあたるものであり，NIC ではこれらの MAC アドレスを参照してフレームを破棄するかどうかを決定する．また，アクセスポイント指定用の MAC アドレス空間はアクセスポイントを通過しない通信の場合は空白として，00:00:00:00:00:00 が代入される．各ノードは自分宛のフレームを受け取ると MAWC ヘッダを除去し，送信者 MAC アドレスに送信元 MAC アドレス，受信者 MAC アドレスにあて先 MAC アドレスを代入してから上位レイヤーへと転送する．

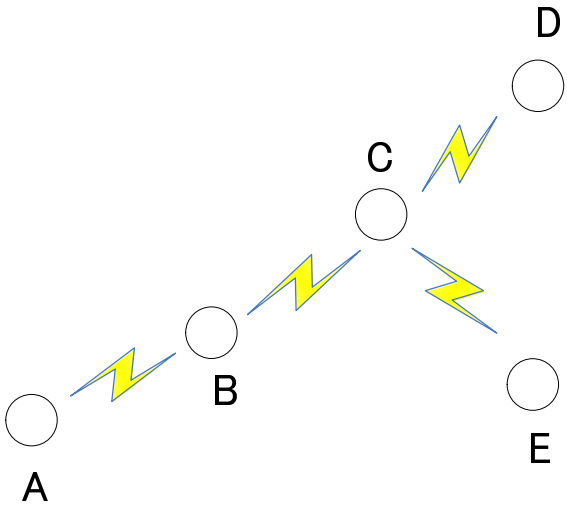
MAWC パケットの判別

MAWC パケットは MAWC ヘッダがついており，通常のパケットとは形が異なる．そのため，MAWC パケットを判別してから処理をしなければならない．そこで ether タイプを拡張し，MAWC パケット専用の ether タイプを作ることで MAWC パケットを判別する．パケッ

ト本来の ether タイプは，MAWC ヘッダに ether タイプの拡張スペースを設けてそこに保存する．そして MAWC ヘッダを除去する際に復元する．

5.2.5　アドホックネットワーク内部のノードとのルーティング例

実際に MAWC ヘッダによってどのようにルーティングが行われるのか，アドホックネットワーク内部のノードとの通信例を示す．トポロジと routing table は図 5.6 で，ノード A がノード D へとフレームを送信する状況を想定する．ヘッダの変遷と処理の流れは図 5.7 に示す．



Aのrouting table

next	あて先	ホップ数	IPアドレス
B	B	1	B-IP
B	C	2	C-IP
B	D	3	D-IP
B	E	3	E-IP

図 5.6　routing example: topology

アドホックネットワーク内部のルーティング

1. Aがパケットを作成し，あて先IPアドレスにD-IPを代入
そのパケットに空のetherヘッダが作成される

etherヘッダ	送信元	送信先
IPヘッダ	A-IP	D-IP

2. あて先IPアドレス(D-IP)をMAWC routing tableから見つける

3. MAWCヘッダを代入し，各値をMAWC routing tableを基に埋める
ヘッダが作成されたら送信

etherヘッダ	A	B	
MAWCヘッダ	A	00:00:···	D
	送信元	アクセスポイント	送信先
IPヘッダ	A-IP	D-IP	

4. 次ホップであるBはMAWCヘッダのアクセスポイントの
空白を見る
次に送信先のDを見て，自身のMAWC routing tableから
Dに対するエントリを探す

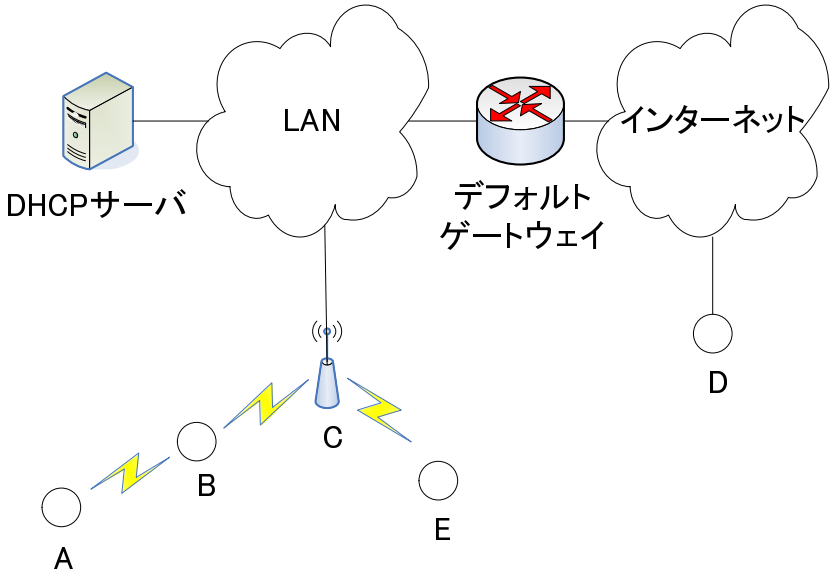
5. 自身のMACアドレスをetherヘッダの送信元に
next hopをetherヘッダの送信先に代入して送信

etherヘッダ	B	C	
MAWCヘッダ	A	00:00:···	D
	送信元	アクセスポイント	送信先
IPヘッダ	A-IP	D-IP	

図 5.7　routing example: routing flow

5.2.6　外部ネットワークのノードへのルーティング例

本節ではアドホックネットワーク外部のノードへのルーティング例を示す．トポロジと routing table は図 5.8 で，ノード A がノード D へとフレームを送信する場合を想定する．また，ノード A はアクセスポイントから繋がる LAN の DHCP サーバから IP アドレスとデフォルトゲートウェイの IP アドレスを得ているものとする．ヘッダの変遷と処理の流れは図 5.9 に示す．



Aのrouting table

next	あて先	ホップ数	IPアドレス
B	B	1	B-IP
B	C	2	C-IP
B	E	3	E-IP

図 5.8　routing example2: topology

外部ネットワークへのルーティング

1. Aがパケットを作成し，あて先IPアドレスにD-IPを代入
そのパケットに空のetherヘッダが作成される

etherヘッダ	送信元	送信先
IPヘッダ	A-IP	D-IP

2. あて先IPアドレス(D-IP)をMAWC routing tableで探す
見つからないため，デフォルトゲートウェイへと送信
することが決定

3. デフォルトゲートウェイへのARP解決を行い，
MACアドレスを把握(DGとする)

4. DGをMAWC routing tableで検索して見つからない
アクセスポイントを通じて外部ネットワークへの送出を決定
MAWCヘッダを代入し，各値を代入して送信

etherヘッダ	A	B	
MAWCヘッダ	A	C	DG
	送信元	アクセスポイント	送信先
IPヘッダ	A-IP	D-IP	

5. BはMAWCヘッダのアクセスポイントの値を見て
MAWC routing tableから探す
そしてアクセスポイントへのnext hopへと転送

etherヘッダ	B	C	
MAWCヘッダ	A	C	DG
IPヘッダ	A-IP	D-IP	

6. アクセスポイントはMAWCヘッダのアクセスポイントと
自身のMACアドレスの一致を見て，フレームを変形
そしてそれを有線へと送信

etherヘッダ	A	DG
IPヘッダ	A-IP	D-IP

図 5.9　routing example2: routing flow

5.3　アクセスポイントを経由するルーティングの詳細

前セクションでは MAWC のルーティング原理について説明した．本セクションではアクセスポイントを経由するルーティングの詳細を示し，アクセスポイントとアクセスポイントから繋がる LAN を利用するための方法について論ずる．

5.3.1　アクセスポイントの存在広告

アクセスポイントの広告は，コントロールメッセージにアクセスポイントであるかどうかのフラグを搭載することで行う．アクセスポイントは HELLO メッセージのアクセスポイントフラグを立てて周囲にブロードキャストする．そのフラグは TC メッセージにもそのまま搭載され，アドホックネットワーク全体に広がる．それによって各ノードはアクセスポイントの存在を知ることができる．なお，アクセスポイントフラグは起動時に手動で設定する．

5.3.2　子ノードテーブル

各アクセスポイントは子ノードテーブルというものを保持する．子ノードテーブルは，アクセスポイントを利用している全ノードを掲載したテーブルであり，アドホックネットワーク上に仮想の LAN を築くために用いられる．子ノードテーブルの作成は，DHCP request などにより，ノード (子ノード) からの通信がアクセスポイントを通過しようとした際にアクセスポイントがそのノードの MAC アドレスを記録することで行われる．

5.3.3　外部ネットワークのノードからのルーティング例

アドホックネットワーク外部のノードから内部のノードへのルーティングの流れを以下に示す．対象とするノードは DHCP サーバから IP アドレスを取得しており，既に子ノードテーブルに登録されているとする．

外部ネットワークからのルーティングの流れ

1. 外部ネットワークのノード (デフォルトゲートウェイの場合も含む) は ARP 解決によってあて先ノードの MAC アドレスを取得
2. 外部ネットワークのノードがあて先ノードに向けてフレームを送信
3. アクセスポイントはフレームを受信すると子ノードテーブルを参照して，あて先ノードがいるかどうかを調べる
4. あて先ノードがいる場合，MAWC routing table を参照してあて先ノードへの経路を調べるそしてフレームに MAWC ヘッダを組み込んであて先ノードに向けてルーティングするこの場合の MAWC ヘッダはアドホックネットワーク内部でのルーティングにおける MAWC ヘッダと同様の形である

5.3.4　ブロードキャスト

MAWC ノードがブロードキャストフレームを送出した場合

MAC アドレスによるトポロジ把握が終わった後の状況を想定する．あて先 MAC アドレスがブロードキャストとなっているフレームは上記に示した外部ネットワークへのルーティングの処理の流れと同様に処理される．アドホックネットワーク内部のノードがブロードキャストフレームを送出した場合の処理の流れは以下に示すとおりである．

アドホックネットワーク内からのブロードキャストフレーム

1. あて先 IP アドレスを MAWC routing table から検索→見つからない
2. IP routing table を基に OS の ARP 関数に処理を任せる
3. ARP 関数があて先 MAC アドレスとしてブロードキャストアドレスを代入
4. MAWC のルーティング処理系にフレームが渡される
5. ブロードキャストアドレスを MAWC routing table から検索して→見つからない
6. 最寄のアクセスポイントへとフレームを送信
7. 最寄のアクセスポイントがアクセスポイントから繋がる LAN へとルーティング
8. アクセスポイントはあて先がブロードキャストアドレスであることを見て，子ノードテーブル上のすべてのノードにもユニキャストで同等のフレームを送信

LAN からブロードキャストフレームが届いた場合

アクセスポイントに LAN からブロードキャストフレームが届いた場合，アクセスポイントはあて先のブロードキャストアドレスを見て子ノードテーブル上のすべてのノードにユニキャストで同等のフレームを送信する．

ブロードキャストフラグ

上記のようにアクセスポイントは子ノードに対してユニキャストでブロードキャストフレームを送信する．ユニキャストの送信では MAWC ヘッダのあて先アドレスに子ノードの MAC アドレスが代入されるため，ブロードキャストフレームという情報が消滅してしまう．そこで元々がブロードキャストフレームであることを示すために，MAWC ヘッダにブロードキャストフラグというものを用意する．そして各々のノードはフレームのあて先がブロードキャストフレームでなくともブロードキャストフラグが立っている場合はあて先をブロードキャストアドレスに直してから上位レイヤへと転送する．

5.3.5　DHCP サーバからの IP アドレス取得

各ノードは IP アドレスを取得するために DHCP request パケットを作成する．DHCP サーバとのやり取りに用いられるパケットは OS 内部で通常の IP のデータパケットとは異なる処理をされるため，MAWC の IP ヘッダ処理系を通過することなく既に ether ヘッダを装着されたフレームの形で MAWC の MAC アドレス処理系に手渡される．このフレームは送信元 MAC アドレスが自身の MAC アドレス，あて先 MAC アドレスがブロードキャストアドレスである．しかし，これの処理は上記のブロードキャストに対する処理と同様である．上記のブロードキャストに対する処理に関して IP ヘッダ処理系を通過した，4 番目以降と同じ処理が行われて送信される．これにより DHCP request は LAN 内の DHCP サーバに到着する．

DHCP サーバの DHCP reply にはブロードキャストとユニキャストの二つのオプションがあるが，どちらで返信が行われても上述の流れに沿ってアクセスポイントに処理され，ノードへと届けられる．これにより DHCP サーバからのダイレクトな IP アドレスの取得が成立する．

5.3.6　ARP

ARP に関するメッセージは DHCP request パケットと同様に，OS 内部で通常の IP のデータパケットとは異なる処理をされる．このため上記の DHCP 関連メッセージと同様にブロードキャストフレームの状態で MAWC の MAC アドレス処理系に手渡される．その結果，まったく同様の処理によってやり取りがなされ，アドレス解決が行われる．

5.4　アクセスポイント間高速バイパスパス

前セクションまでで MAWC におけるルーティングを説明した．しかし，これまでのルーティングではアクセスポイント間高速バイパスパスを利用していない．既出であるが，高速バイパスパスとはアドホックネットワーク内のノード同士の通信にもアクセスポイント間の有線リンクを使うことでスループットの向上と省電力を実現しようというものである．本セクションではアクセスポイント間高速バイパスパスの利用について説明する．

5.4.1　高速バイパスパスの利用可能性の判別

高速バイパスパスを利用できるためにはアクセスポイントから繋がる LAN 内の DHCP サーバから IP アドレスを取得していることが必要である．そこで MAWC ではノードが DHCP サーバから IP アドレスを取得したかどうかについて DHCP フラグというフラグを使用することで判別する．

DHCP フラグは

1. DHCP サーバとのやり取りに使用するメッセージが MAWC が受信したフレームから検出される
2. DHCP メッセージを受信した後に IP アドレスが変更される

の二点を通過した場合に立てられる．なお，DHCP メッセージを受信せずに IP アドレスが変更された場合は直ちに DHCP フラグはたたまれる．

この DHCP フラグはトポロジ把握のためのコントロールメッセージに搭載され，アドホックネットワーク全体に広告される．これにより各ノードは通信相手との間に高速バイパスパスが成立するかどうかを判別する．

5.4.2　高速バイパスパスの利用

高速バイパスパスの利用はアドホックネットワーク内で無線マルチホップのみで伝達するよりもホップ数が少ない時のみ利用すべきである．このためには高速バイパスパスを利用する際のホップ数を見積もることが重要となる．

高速バイパスパスのホップ数

高速バイパスパスのホップ数は

- 送信元ノードから最寄のアクセスポイントまでのホップ数
- アクセスポイント間の有線空間のホップ数
- あて先ノードから最寄のアクセスポイントまでのホップ数

の和で与えられる．このうち，アクセスポイント間の有線は無線と比べて十分に高速だと考えられるため，ホップ数を 0 とする．また，送信元ノードから最寄のアクセスポイントまでのホップ数は，MAWC routing table 上で最寄のアクセスポイントを探せば求められる．つまりあて先ノードから最寄のアクセスポイントまでのホップ数のみが未知数となる．そこで MAWC では link state 情報からあて先ノードを頂点とした MAWC routing table を作成し，あて先ノードから最寄のアクセスポイントまでのホップ数を計算する．

高速バイパスパスの利用

上記の方法で高速バイパスパスのホップ数が求められるため，高速バイパスパスを利用するかどうかは，このホップ数と，MAWC routing table にある，あて先ノードまでの無線マルチホップ数を比較し，よりホップ数の少ない方の経路を選べばよい．しかしこの方法ではアクセスポイントへの通信の集中を避けることができない．

そこで，MAWC では通信を分割することでアクセスポイントへの通信の集中を避ける．具体的には，高速バイパスパスのホップ数と無線マルチホップのホップ数の差が 2 ホップ以内の場合，50% ずつの確率で高速バイパスパスと無線マルチホップ数の双方に経路を振り分ける．これによりアクセスポイントへの通信の集中を緩和する．この処理を MAWC でルーティングを行う前に行う．これにより通信の集中しないアクセスポイント間高速バイパスパスの利用が可能となる．

なお，アクセスポイント間高速バイパスパスを利用することに決定した場合，ノードは外部ネットワークと通信する場合の処理 (図 5.9) の 3 以降の処理を行う．

また，アドホックネットワーク内でルーティングすることに決定した場合，ノードはアドホックネットワーク内部で通信する場合の処理 (図 5.7) の 3 以降の処理を行う．

第 6 章

実装と評価

本章では実装環境や実装に関する擬似コードなどを示し，実際に実装した内容について詳細を示す．また，実装したノードを用いて行った実験について詳細を記し，評価を行う．

6.1 実装環境

実装には PC を用いて擬似的にノードとアクセスポイントを再現した．実装に用いた OS は FreeBSD である．MAWC のソースコードは FreeBSD の Layer-2 プロトコルスタック上に実装した．また実装に用いた PC はそれぞれ Thinkpad X23,X30,X31,X60 である．実験において使用した Wireless カードは X31 と X60 に関しては内蔵の Atheros miniPCI Wireless で，X23 と X30 に関しては BUFFALO WLI-PCM-L11GP Wireless PC カードである．

6.2 実装内容詳細

本セクションでは実装した内容についてメッセージフォーマットや擬似コードなどを示し，実装内容の理解に役立てる．

6.2.1 メッセージ詳細

HELLO メッセージ

HELLO メッセージの構造を示す．各ノードは各値を代入して定期的にブロードキャストする．初期設定では 3 秒ごとに送出している．

HELLO メッセージの構造

コントロールタイプ

送信元ノード MAC アドレス

送信元ノード IP アドレス

アクセスポイントフラグ

DHCP フラグ

コントロールタイプとは，コントロールメッセージを処理のために振り分けるためのものであり，HELLO メッセージコントロールタイプと Topology Control メッセージコントロールタイプの二つが存在する．

Topology Control メッセージ

Topology Control メッセージの構造を示す．このメッセージは二段階構造になっている．一段目がメッセージヘッダであり，二段目がメッセージである．メッセージヘッダは送信元に関する情報とメッセージの処理に関する情報が格納されている．そしてメッセージには各ノードに関する情報が格納されている．link state 情報は送信元ノードとメッセージの各ノードの間の関係として理解される．

Topology Control メッセージは各値を代入されて定期的にブロードキャストされる．初期設定では 5 秒ごとに送出される．

なお，このメッセージはホップリミットの示すホップ数だけブロードキャストによってアドホックネットワーク全体に転送される．

また，このメッセージは各ノードによってシーケンス管理されている．送信元ノードが同一で，かつシーケンス番号が古い TC メッセージはループしているとみなされ，削除される．

Topoogy Control メッセージヘッダの構造

コントロールタイプ

送信元ノード MAC アドレス

送信元ノード IP アドレス

シーケンス番号

ホップリミット

情報数

アクセスポイントフラグ

DHCP フラグ

Topoogy Control メッセージの構造

送信元ノード MAC アドレス

送信元ノード IP アドレス

アクセスポイントフラグ

DHCP フラグ

リンク状態

MAWC ヘッダ

MAWC ヘッダの詳細構造について示す．中身は上述の通りであるが，ここにまとめて構造を示すことにする．

MAWC ヘッダの構造

送信元ノード MAC アドレス

アクセスポイント MAC アドレス

あて先 MAC アドレス

ether タイプ

ブロードキャストフラグ

6.2.2 ルーティング

MAWC のルーティングは二段階に分けて行われる．一段目はあて先 IP アドレスのあて先 MAC アドレスへの解決で，二段目は MAC アドレスから経路を決定し，next hop へと送出するところである．このうち一段目の処理は送信元ノードにおいてのみ行われる処理である．

まず一段目であるが，これは ether ヘッダをパケットに付加し，値を代入して送出を行う ether_output という関数においてパケットヘッダからパケットが IP データパケットだと判別した直後に行う．

処理の流れは以下のようになる．

```
IP データパケットである{
    MAWC がアクティブである{
        分割転送か外部ノードとの通信である場合{
            ARP 関数に処理を渡して MAC アドレスを取得してもらう
        }
        アドホックネットワーク内部のノード間での通信である場合{
            ARP 関数に処理は渡さず，あて先 MAC アドレスを MAWC で代入する
```

```
        }
    }
    MAWC がアクティブでない{
        ARP 関数に処理を渡す
    }
}
```

分割転送か外部ノードとの通信，あるいはアドホックネットワーク内部のみでの通信かどうかを判別するには，MAWC routing table からあて先ノードへのホップ数を調べることで行う．

そして二段目の処理は ether_output_frame という関数と ether_input という関数の二箇所でフレームを MAWC に取り込むことで行う．ether_output_frame は ether_output の後に執行される関数であり，フレームの送信が行われる関数である．また，ether_input は受信したフレームが最初に処理される関数である．

ether_output_frame からフレームを取り込んだ場合は送信元ノードにおいて行う処理を行い，ether_input からフレームを取り込んだ場合は中継ノード，あるいは受信ノードにおいて行う処理を行う．実装では同一の関数でフレームを取り込み，フラグによって内部で処理を分割している．

二段目の処理の実装は以下のようになる．

```
ether_input からフレームを取り込んだ場合{
    アドホックネットワーク用の NIC からフレームを取り込んだ場合{
        MAWC データフレームである場合{
            MAWC ヘッダのアクセスポイント MAC アドレスが
            空白ではない場合{
                自分自身はアクセスポイントモードではない場合
                または自分はアクセスポイントモードだが
                アクセスポイント MAC アドレスが自分と一致しない場合
                {
                    自分の MAWC routing table にアクセスポイントの
                    MAC アドレスに関するエントリがあれば
                    ヘッダを書き換えて next hop に転送
                }
                自分自身がアクセスポイントで，アクセスポイント MAC アドレスが
                自分と一致する場合{
                    あて先 MAC アドレスがブロードキャストアドレスなら，有線と
                    子ノード全てにブロードキャストフレームを送信
                    そうでなければ有線にフレームを送信
                }
```

```
            }
            アクセスポイント MAC アドレスが空白の場合{
                あて先 MAC アドレスが自分の MAC アドレスと一致したら MAWC ヘッダを
                取り外して上位レイヤへとフレーム転送
                あて先 MAC アドレスに関するエントリが MAWC routing table にあれば
                ヘッダを書き換えて next hop に転送
            }
        }
        MAWC コントロールフレームである場合{
            コントロールフレームの処理関数で処理をする
        }
    }
    有線側の NIC からフレームを取り込んだ場合{
        アクセスポイントである場合{
            自分宛のフレームなら取り込む
            あて先 MAC アドレスに関するエントリが子ノードテーブルに存在するなら
            MAWC routing table を参照してフレームに MAWC ヘッダを作成して転送
            あて先 MAC アドレスがブロードキャストアドレスなら子ノード全てに転送
        }
    }
}

ether_output_frame から取り込んだ場合{
    自分がアクセスポイントモードの場合{
        送出しないため，破棄する
    }
    あて先 MAC アドレスがブロードキャストアドレス
    あるいは MAWC routing table に存在しない MAC アドレスである場合{
        MAWC ヘッダを付加し，最寄のアクセスポイントへと送出する
    }
    あて先 MAC アドレスに関するエントリが MAWC routing table に存在する場合{
        MAWC ヘッダを付加し，next hop へと送出する
    }
}
```

6.2.3 IP アドレスの取得

各ノードの IP アドレスについては，IP アドレスが変更された時に実行される in_control という関数に MAWC の変数をリンクすることで IP アドレスが変更される度にリアルタイムに取得する．

また，IP アドレスをどこから取得したかを決定する DHCP フラグについては，in_control と，ether_input の二つの関数に MAWC を連携させることで行う．

具体的にはまず，DHCP フラグと temporary フラグを設ける．そして，ether_input において受信したフレームを監視し，その中に DHCP reply メッセージがあった場合に temporary フラグを立てる．そしてその後 in_control において IP アドレスが変更された場合, DHCP によって IP アドレスが設定されたと判断する．temporary フラグが立っていない状態で in_control において IP アドレスが変更された場合，DHCP フラグをしまう．これにより DHCP サーバからの IP アドレス取得を正確に把握することができる．

6.3 動作検証

ラップトップ PC を用いて実際に作成した MAWC の動作検証について説明する．今回の実験では，IPv4 における IP アドレスの取得と内部ノードおよび外部ノードとの通信を確認した．確認には図 6.1 に示すトポロジを用いた．

まず，IP アドレスの取得について説明する．図 6.1 にはアクセスポイント，ノード A，ノード B の三台の MAWC ノードが配置されている．そしてアクセスポイント，ノード A，ノード B の三台とも初期状態では IP アドレスは振られていない．この状態でノード B が直接アクセスポイントと有線でつながっている DHCP サーバから IP アドレスを取得することができることを確認した．このトポロジの初期状態において各ノードが作成，保持している routing table を図 6.2，6.3，6.4 に示す．図 6.2 がアクセスポイントの routing table，6.3 がノード A の routing table，6.4 がノード B の routing table である．図 6.2 について解説する．上段に LS と書かれた link state 情報が示されており，アクセスポイントとノード A 間のリンク，およびノード A とノード B 間のリンク情報が示されていることがわかる．また，その下には FW としてフォワーディング情報，つまり routing table が示されている．この図から，アクセスポイントからノード A までが 1 ホップ，ノード B までが 2 ホップであり，ノード B にフレームを送信するには next hop がノード A であることがわかる．このトポロジを用いてノード B における IP アドレスの直接取得が実現できた．

また，同じトポロジ (図 6.1) において，今度はノード A にも IP アドレスを取得させた．そしてノード B とノード A 間，およびノード B と DHCP サーバ間で ping, ftp, ssh の三種類の通信を行い，それぞれ通信が成立することを確認した．

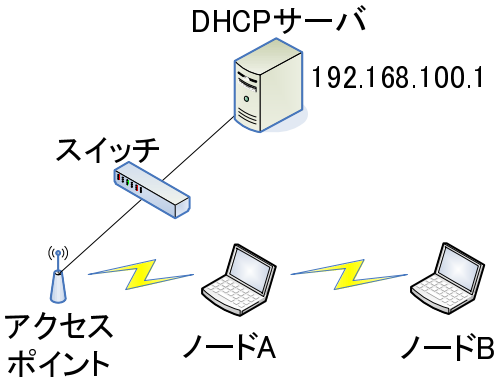


図 6.1　action confirmation:topology

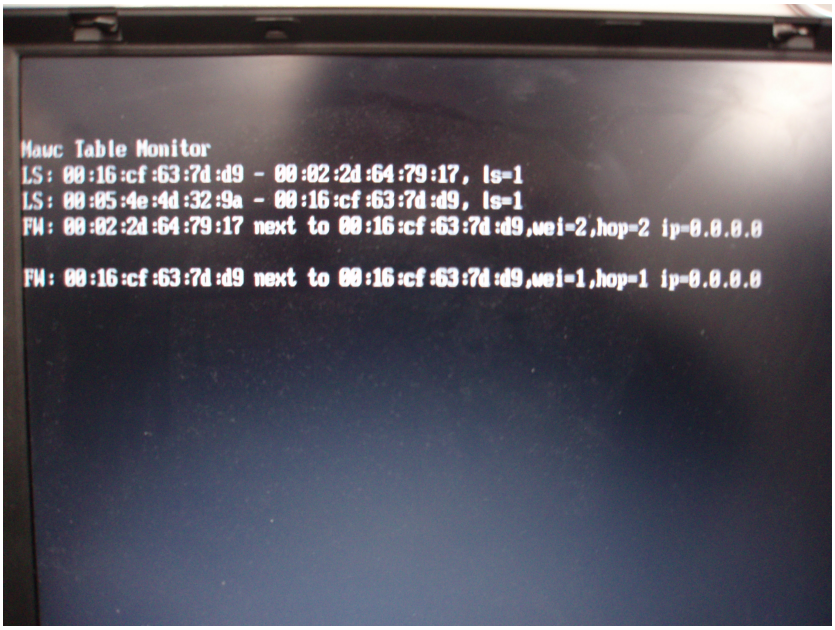


図 6.2　action confirmation:routing table

6.4　省電力に関する評価

MAWC ノードを用いて図 6.5 と図 6.6 に示すトポロジを作成した．そして，送信元ノードとあて先ノードの間で ftp を用いて 30MB のファイルを転送し，無線マルチホップにおいてフレームの中継を行っているノードがどれだけのフレームを転送したかを測定した．なお，図 6.5 では送信元ノードとあて先ノードで 2 ホップの無線マルチホップを用いて通信をしている．また，図 6.6 では送信元ノードとあて先ノードの無線マルチホップ数のホップ数が 2 で，アクセスポイント間高速バイパスパスを用いたホップ数も 2 であるため，無線マルチホップ (2) と高速バイパスパス (1) を用いた経路の二方向の経路に通信が分割される．

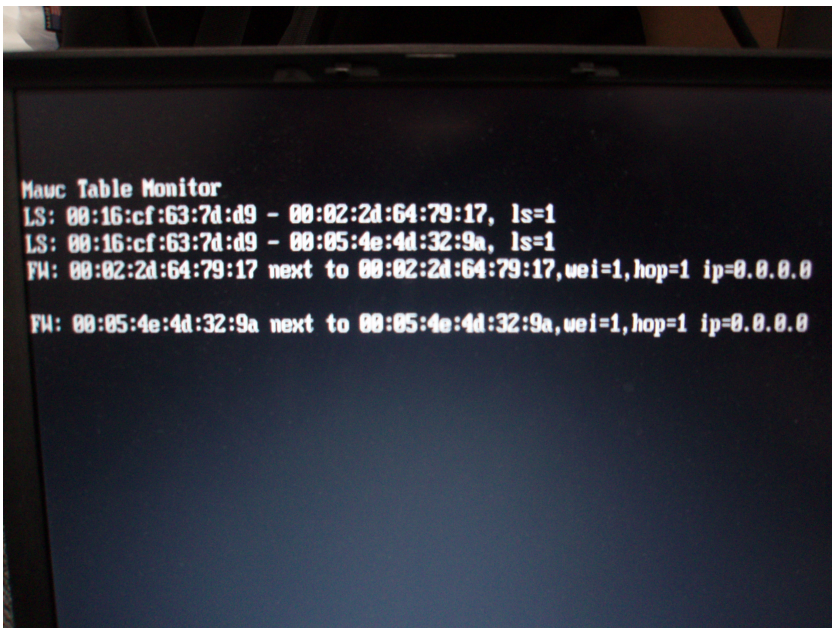


図 6.3　action confirmation:routing table2

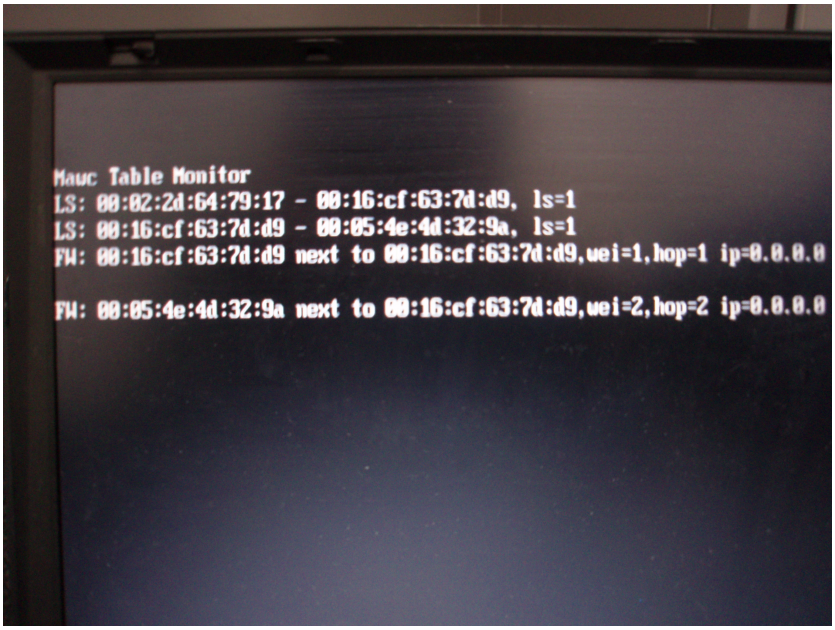


図 6.4　action confirmation:routing table3

実験環境はあまり広くなく，1 ホップで全てのノードに電波が届いてしまう状況であった．そこで MAWC に MAC アドレスフィルタリング機能を設け，指定した MAC アドレスからの HELLO メッセージしか受け取らないようにして実験トポロジを作成した．

結果としてコントロールフレームを除いて，図 6.5 では約 30MB の転送を観測し，図 6.6 では約 15MB の転送を観測した．

無線通信を行うノードにおいて最も電力消費が大きい状態は送信状態である．このため，無

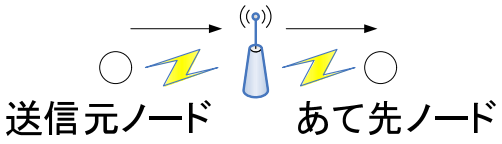


図 6.5　experiment1:wireless hop only topology

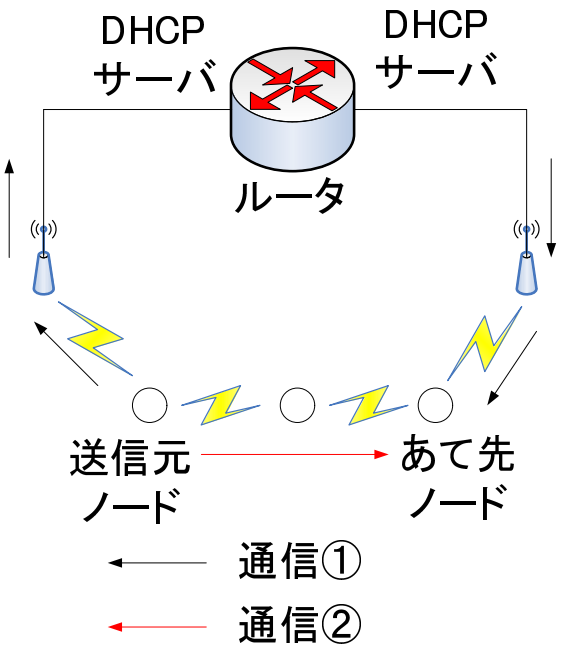


図 6.6　experiment1:divided communication

線ノードは送信回数が少なければ少ないほど電力消費は少なくなる．上記の実験ではアクセスポイント間高速バイパスパスを用いることで送信回数を約半分に抑えることができた．これにより多大な省電力効果が確認された．

6.5　スループットに関する評価

図 6.5 と図 6.6，そして図 6.7 の三種類のトポロジを作成した．そして前セクションの実験と同様に送信元ノードとあて先ノードの間で ftp を用いて 30MB のファイルを転送し，スループットを測定した．スループットの測定は 30 回行い，その平均値を計算した．なお，図 6.7 は全ての通信がアクセスポイント間高速バイパスパスを通過するトポロジである．それぞれのトポロジの作成には 6.4 で記したのと同様の MAC アドレスフィルタリング機能を用いた．またアドホックネットワークは同一チャネルを用いるため，電波到達範囲内に複数の通信リンクが存在すると，それぞれの通信リンクが空間を取得しあう形となり，スループットが抑制されてしまう．そこで今回実験に用いた三種類のトポロジでは通信量を考慮した通信リンクの論理的

な数を同一にし，スループットの抑制が同程度発生するようにした．

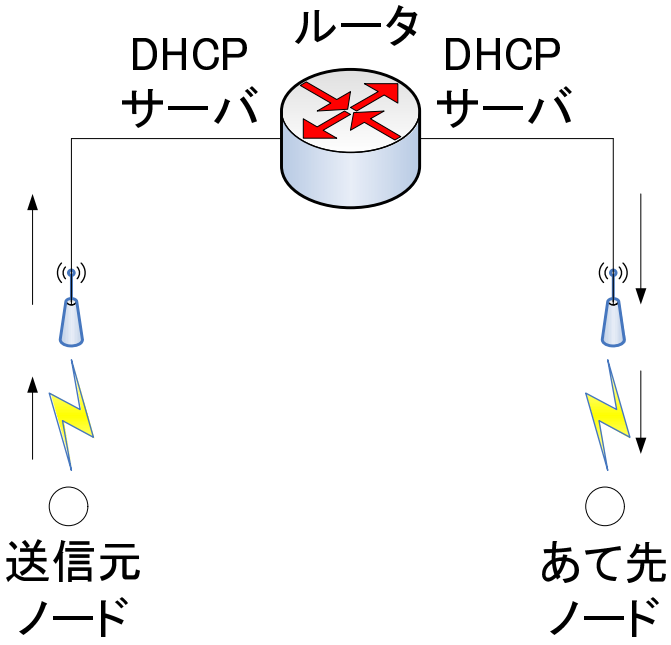


図 6.7　experiment1:bypass path between APs

結果として，図 6.5 と図 6.7 では約 270kB/s となり，ほぼ同じ値となった．図 6.6 のスループットは 240kB/s となり，他の二つのトポロジよりも低下した．

まず，図 6.5 と図 6.7 についてであるが，この二つのトポロジにおける通信経路の違いはアクセスポイント間高速バイパスパスのみである．さらにパケットの処理工程の段数もほぼ変わらないため，パケット処理にかかる時間もほぼ同等である．その上でスループットがほぼ変わらなかったことからアクセスポイント間高速バイパスパスはほぼスループットを低下させていないと考えられる．実際に MAWC を構成した場合はアクセスポイント間の高速バイパスパスに輻輳が発生していたり，高速バイパスパスの距離が非常に遠いものになってしまったりする可能性があるため，この実験とは異なり，スループットを低下させるかもしれない．しかし，アドホックネットワークは 200 ノード，平均 10 ホップ程度で構成されることが多い．このため，アクセスポイント間の物理的距離というものは限られている．そういった状況ではアクセスポイント間のネットワーク的距離もあまり遠くない可能性が高い．それ故にアクセスポイント間の高速バイパスパスが大きくスループットを低下させる可能性は低いと考えられる．

また，図 6.6 のトポロジにおいてスループットが低い原因はパケット処理工程の複雑さが原因だと考えられる．上述のようにアクセスポイント間高速バイパスパスはほぼスループットに影響していない．このため，本来ならばこの場合もほぼ同じ値のスループットが測定されるはずである．

このトポロジではまず MAWC routing table から無線マルチホップでのあて先ノードまでの経路を調べる．そしてその後にあて先ノードを中心とした一時的な MAWC routing table を作

成し，それを用いてアクセスポイント間高速バイパスパスを用いた場合のホップ数を計算している．そしてそれらを比較した上で通信の分割を決定してようやくパケットの送信を行う．これらの処理をパケットごとに行っているため，このトポロジではスループットが低下していると考えられる．その他にもアドホックネットワーク内のノード数が相対的に多いため，コントロールメッセージが増加することによる影響が考えられるが，図 6.5 と図 6.7 の比較においてほぼスループットに変化が見られなかったため，その影響は軽微であると考えられる．

第 7 章

結論

本稿では MAC アドレスルーティングを用いることで，Layer-3 に依存しないルーティングを実現したアドホックネットワーク (MAWC) についてアーキテクチャの提案と動作検証を行った．MAWC はアクセスポイントを積極的に利用することを目的として作られており，IPv4 において LAN 内の DHCP サーバから IP アドレスを直接取得することができる．また，アドホックネットワーク内のノードが自分と異なる Layer-3 プロトコルを用いていてもルーティングに影響を与えない．

現在の MAWC の状態は Layer-3 プロトコルに拠らないルーティングと IPv4 における LAN からの IP アドレス取得が実現できた状態である．ただ，評価の章でも示したように，経路計算の負荷が大きく，経路計算のキャッシュを用いるなど経路計算に一層の工夫が必要である．今後はこの点の改良を施した後に IPv6 や他の Layer-3 プロトコルにも実装を広げ，LAN が提供する Layer-3 プロトコルを自在に受け入れられるプロトコルを構築したい．

参考文献

[1] ANSI/IEEE, “ ANSI/IEEE Std 802.11,1999 Edition ” ,IEEE802.11,1999

[2] C. Perkins and P. Bhagwat, “ Highly Dynamic Destination Sequenced Distance-Vector Routing (DSDV) for Mobile Computers ” ,In Proc. of the ACM SIGCOMM,October 1994.

[3] D. Johnson and D. Maltz,“ Dynamic Source Routing in Ad Hoc Wireless Networks ”,in Mobile Computing (ed. T. Imielinski and H. Korth), Kluwer Academic Publishers, Dordrecht, The Netherlands 1996.

[4] C. E. Perkins, E. M. Royer, and S. R. Das, “ Ad hoc On-Demand Distance Vector (AODV) Routing. ” ,RFC 3561, July 2003.

[5] T. Clausen et al, “ Optimized Link State Routing Protocol (OLSR). ” ,RFC 3626, October 2003.

[6] J. Macker and S. Corson, “ Mobile Ad hoc Networks(MANET). ” , http://www.ietf.org/html.charters/manet-charter.html, 1997. IETF Working Group Charter.

[7] R. Ogier, F. L. Templin, NOKIA, and M. G. Lewis, “ Topology Dissemination Based on Reverse-Path Forwarding (TBRPF). ” ,RFC 3684, Feb 2004.

[8] C. E. Perkins and E. M. Royer, “ Ad Hoc On-Demand Distance Vector Routing. ” ,In Proceedings of IEEE Workshop on Mobile Computing Systems and applications (WMCSA), pages 90-100, 1999.

[9] D. Kim, J.J. Garcia-Luna-Aceves, K. Obraczka, J.-C. Cano, and P.Manzoni, “ Routing mechanisms for mobile ad hoc networks based on the energy drain rate. ” ,IEEE Trans.on Mobile Computing, Vol. 2, No. 2, pp. 161-173 Apr. 2003.

[10] S. Singh, M. Woo, and C.S. Raghavendra, “ Power-aware routing in mobile ad hoc networks. ” ,in Proc. of ACM/IEEE MOBICOM ’ 98, pp. 181-190 Oct. 1998.

[11] C. K. Toh, “ Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks ” ,IEEE Communications Magazine, Vol. 39, No. 6, pp. 138-147 June 2001.

[12] D. S. J. De Couto, Daniel Aguayo, John Bicket and Robert Morris, “ A High-Throughput Path Metric for Multi-Hop Wireless Routing. ” ,in Proc. of ACM/IEEE

MOBICOM ' 03, pp. 14-19 Sep. 2003.

[13] Ancillotti et. al. , " A Layer-2 Architecture for Interconnecting Multi-hop Hybrid Ad Hoc Networks to the Internet " , Proceedings of The Third Annual Conference on Wireless On demand Network Systems and Services (WONS 2006), Les Menuires, France, Jan. 18-20, 2006.

[14] T. Clausen, E. Baccelli, " A Simple Address Autoconfiguration Mechanism for OLSR ", IEEE ISCAS '05, in proceedings.

[15] S. Nesargi and R. Prakash, " MANETconf: Configuration of hosts in a mobile ad hoc network " , in INFOCOM, 2002.

[16] Charles E. Perkins, Jari T. Malinen, Ryuji Wakikawa, Elizabeth M. Belding-Royer, and Yuan Sun., " Ad hoc Address Autoconfiguration " , IETF Internet Draft, draft-ietf-manet-autoconf-01.txt, November 2001

[17] M. Gerla, K. Tang, and R. Bagrodia, " TCP performance in wireless multi-hop networks ", in Proceedings of IEEE WMCSA'99 (to appear), (New Orleans, LA), February 1999.

[18] Srisuresh, P. and Holdrege, M., " IP Network Address Translator (NAT) Terminology and Considerations " , RFC 2663, Internet Engineering Task Force (IETF), August 1999.

[19] Perkins C. (ed.), " IP Mobility Support for IPv4 " , RFC 3344, Internet Engineering Task Force (IETF), August 2002.

[20] Benzaid, M., Minet, P., Al Agha, K., Adjih, C., and Allard, G., " Integration of Mobile-IP and OLSR for a Universal Mobility " , To appear in Wireless Networks journal (Winet), Special Issue on Ad-hoc Networking.

[21] Engelstad, P. and Egeland, G., " NAT-based Internet Connectivity for On Demand MANETs " , Proceedings of 1st Wireless On-Demand Networking Symposium 2004 (WONS 2004),

[22] Perkins, C.E., " IP Encapsulation within IP " , RFC 2003, Internet Engineering Task Force (IETF), October 1996.

[23] Perkins, C.E., " Minimal Encapsulation within IP " , RFC 2004, Internet Engineering Task Force (IETF), October 1996.

[24] http://ja.wikipedia.org/wiki/APIPA

発表文献

[1] 中島 亮, 江崎 浩, “ レイヤ 2 転送を用いたレイヤ 3 アドホックネットワークの構成法 ” , 信学総大 B-6-20,Mar.2007.

謝辞

修士論文研究を進める過程で，常日頃から知識のみならず研究に対する心構えなどについて有益な御指導，御批評，御鞭撻いただいた江崎浩教授に深く感謝致します．また高橋富美秘書、田坂秘書にはすばらしい研究環境を提供していただき感謝しております．特任助手の山本成一さん，博士課程１年の吉田薫さん，藤田祥さんには多大な労力を惜しまず，研究内容の細かい部分に関してまで議論させていただき，研究の方針，位置づけなどに関していろいろ面倒を見ていただきました．ここに深く感謝の意を述べたいと思います．そして同輩の石田真一君，沢村正君，賈洪光君と研究室での苦楽をともに過ごせたことに心より感謝いたします．また，一緒に研究の議論に参加してくれた上に研究室の仕事などを積極的にこなし，研究しやすい体制を整えてくれた修士課程一年の田中陽介君，王智勇君，落合秀也君，安本直史君，山口龍太郎君，学部四年の杉山哲弘君，大口諒君，阪本裕介君に大変感謝いたします．2 年間にわたってありがとうございました．

最後に研究生活のみならず今まで生活すべての面倒を見てくれた両親に心より感謝いたします．24 年間ありがとうございました．