

博 士 論 文

透過的モバイルネットワークシステムの
アーキテクチャに関する研究

ATMOS: Architecture for
Transparent Mobile Networking Systems

指導教官 江崎 浩 教授

東京大学大学院

情報理工学系研究科 電子情報学専攻

藤田 祥

内容梗概

本研究の目的は、モバイルホストから構成される分散システムの構築と運用に関する課題を解決することである。モバイルホストは安定したネットワークに留まらないインターネットホストである。本論文では以下のような状況を考慮する。第一に、到達性が完全ではないネットワーク中を移動するモバイルホストが分散システムを構成している状況である。これをオーバーレイアドホックネットワーク上の分散システムと呼ぶ。この状況では、ネットワーク間の到達性は、ファイアウォールや NAT などの機器により通信の開始できる方向が制限されていたり、運用障害やフィルタリングにより完全に遮断されていたりしうる。第二に、IEEE802.11 の IBSS のような無線リンクを利用するモバイルホストが分散システムを構成している状況である。これを無線アドホックネットワーク上の分散システムと呼ぶ。この場合、モバイルホスト間のリンクには双方向性、推移性、安定性があるとは限らない。我々は、以上の 2 つのネットワーク、つまり、ホスト間に安定した到達性があるとは限らないネットワーク上の分散システムについて議論する。

これまでの分散システムが基にするネットワークアーキテクチャでは、有線ネットワークとそこから移動しない固定ホスト、そしてインターネットの透過性を前提として設計されている。したがって、その前提が成り立たないオーバーレイアドホックネットワークや無線アドホックネットワーク上で発生する、IP アドレスの変更、ホスト間の到達性の変更、リンクブロードキャストの配送範囲の変更などは、系統的に対応されておらず、個々のシステムによって場当たり的に対応されているのが現状である。また、Mobile IP など、これらの問題を部分的に解決するプロトコルが提案されているが、これらのプロトコルでは特定のホストへの安定した到達性を前提としているため我々が対称とするネットワークには適用できない。今後モバイルホストがインターネットの主要ホストになっていくことを考慮すると、我々は上述したネットワークの変更について系統的に対応する新しいアーキテクチャがインターネットには必要だと考える。

本論文では現在のインターネットアーキテクチャを拡張し、リンク層とネットワーク層の間に新たにリンク補完層を導入する。リンク補完層は、ネットワーク以上の層に対し、分散システム内のホストを含む、ブロードキャスト可能な仮想リンクを提供する。この仮想リンクの上では、アプリケーションはあるホストに対する一貫した IP アドレスによるユニキャスト送信と一貫したリンクローカルマルチキャスト IP によるマルチキャスト送信が利用できる。これにより、現在のインターネットアーキテクチャのために作られた既存のプロトコルを再利用して分散システムがモバイルホスト上に構築できる。またリンク補完層は、ネットワーク以下の層

に対し、他のホストへの到達性と品質の変化に適応する経路制御と中継機構を実装する。リンク補完層が分散システム内のモバイルホスト全体の到達性の維持に必要な処理を集約して実装しているので、複数のアプリケーションが独自に実装しなくても同じ機能を共有できる。また、無線アドホックネットワークのリンク品質を評価するために、各モバイルホストが観測したフレームの時刻を同期するための手法を提案する。この手法によりリンク間の干渉や競合を検出に十分な精度の分散観測が可能になる。

本論文の貢献は以下の通りである。第一に、オーバレイアドホックネットワークの問題と無線アドホックネットワークの問題から、時間変化する有向グラフ上の経路制御という本質的な問題を抽出して解決した。これにより両者とその混合ネットワーク上の到達性の問題を統一的に解決した。第二に、移動透過性を扱った既存研究がモバイルホストや中継ノードに安定した到達性があることを仮定していたのに対し、本論文では到達性に制限があるネットワーク間をモバイルホストが移動した場合の問題を扱って応用範囲を広げた。また、モバイルホストが協調して経路制御と中継を行った場合にモバイルホスト内の到達性を回復できる条件を明らかにした。第三に、モバイルホストによって通信リンクの設計の自由度が上がっても従来通りの一貫したインターフェースを提供できることを示した。第四に、我々は提案アーキテクチャに基づくネットワークを実装し、被災地向けの情報収集システム内における実際の運用に基づく考察を行った。その過程で無線アドホックネットワークの運用上の問題解決に役立つ分散観測手法を提案し、その動作を実証した。モバイルホストが主要なホストになる将来のインターネットにおいて重要なこれらの貢献によって、我々は将来のインターネットアーキテクチャが取るべき設計指針を示した。

Abstract

The goal of this research is to solve problems in constructing and operating distributed systems among mobile hosts. A mobile host is an Internet host that does not connect to a network persistently. In this thesis, we assume the following situations. First, the mobile hosts form an *overlay ad-hoc network*, in which they move among restricted networks such as the networks with firewalls or network address translations(NATs) that prohibit incoming connections and networks with failures or filters that prohibit connections in both directions. Second, the mobile hosts form a *wireless ad-hoc network* using wireless links that do not restrict connectivity such as IEEE 802.11 IBSS mode. In this situation, the links among the mobile hosts might not be bidirectional, transitive and stable. In summary, distributed systems without stable reachabilities among hosts will be discussed.

The current Internet architecture was designed under the assumptions that links were wired and hosts were fixed. Therefore, Internet architecture cannot handle issues as change of IP address, change of reachability among mobile hosts, change of a link broadcast distribution range and so on. Instead, these issues are worked out by each applications in ad-hoc manner. And some protocols such as mobile IP solved some problems, but mobile IP assumes the stable reachabilities among mobile nodes. So it cannot be used for distributed systems without stable reachabilities. Since we assume the number of mobile hosts will grow, it is necessary to design a new architecture to solve issues systematically.

In this thesis, we propose the extended Internet architecture that has the link complement layer between the link and network layers. The link complement layer provides broadcast, virtual links to which all hosts under the distributed system are connecting. This virtual links allow applications to transmit unicast and multicast packets with consistent unicast IP addresses and link-local multicast IP addresses. Therefore, distributed systems can be constructed reusing unmodified applications that are designed for the current Internet architecture. The link complement layer also implements routing and forwarding mechanisms to adjust to changes in reachabilities and communication qualities among the mobiles hosts. Then, all applications can have routing and forwarding mechanisms without its own implementation. In addition, we propose a method that synchronizes and merges event traces that are captured by the mobile hosts. We show that this method can be used

to diagnose operational problems in wireless ad-hoc networks. Finally, we implemented a network based on the proposed architecture and applied it as a information collecting system for disaster stricken buildings. Through this experience, we proved that our architecture is suitable to constructing a distributed system among mobile hosts without stable reachabilities.

The contributions of this thesis are the following. First, we extracted a fundamental property of reachabilities among mobile hosts from both overlay ad-hoc networks and wireless ad-hoc networks; that is a time-varying directed graph. A combination of overlay and wireless ad-hoc networks also has this property and we can handle it in the same way as overlay and mobile ad-hoc networks. Second, our architecture has broader applicability because it can be applied to the situation some nodes have unstable reachabilities from the other nodes. Moreover, we show the condition in which mobile hosts can recover the end-to-end reachability after their mobility. Third, we show that the consistent interfaces that are conforming to the existing application can be provided over both overlay and mobile ad-hoc networks. This makes it possible to have larger flexibility on design of the link layer. Lastly, we implemented and operated a system based on the proposed architecture and consider the pros and cons based on the operational experience. These contributions are valuable in the future Internet where most hosts will move. We show the directions that the future Internet architecture should follow.

目次

第 1 章	序論	1
第 2 章	従来ネットワークのモデル化	3
2.1	前提	3
2.1.1	古典的 IP リンクモデル	4
2.1.2	インターネットの透過性	7
2.1.3	固定ホスト	8
2.2	従来のネットワークモデルとその特性	9
第 3 章	モバイルネットワークのモデル化	12
3.1	前提の変化	12
3.1.1	非古典的 IP リンク	12
3.1.2	インターネットの非透過性	14
3.1.3	モバイルホスト	15
3.2	モバイルホストのネットワークモデルとその特性	16
第 4 章	モバイルシステムの課題と関連研究	22
4.1	問題	22
4.1.1	ユニキャストインターフェースの一貫性	23
4.1.2	マルチキャストインターフェースの一貫性	23
4.2	既存研究	23
4.2.1	無線アドホックネットワーク	23
4.2.2	オーバーレイネットワーク	27
第 5 章	透過的モバイルネットワークシステムのアーキテクチャ	31
5.1	有向グラフ上のプロトコル	32
5.2	統一インターフェース	33
5.3	物理リンクの性能計測	36
第 6 章	共通インターフェースの実装	38
6.1	ソフトウェアアーキテクチャ	38

6.1.1	ユニキャストサービス	39
6.1.2	マルチキャストサービス	40
6.2	実証実験	40
第 7 章	無線リンクの品質評価の実装	45
7.1	無線リンクの特性	45
7.1.1	物理副層	46
7.1.2	MAC 副層	48
7.2	無線リンクの性能特性の観測	50
7.2.1	既存研究	50
7.3	無線ネットワーク分散観測	51
7.3.1	分散観測時系列データベースの作成	52
7.3.2	実証実験	56
第 8 章	議論	59
第 9 章	結び	61
	謝辞	62
	参考文献	63
	本研究に関する発表論文	68

目次

2.1	インターネット構成例	3
2.2	バス型の有線リンク技術を用いたサブネット	5
2.3	スター型の有線リンク技術を用いたサブネット	5
2.4	片方向リンク	6
2.5	非推移的なリンク	7
2.6	IEEE 802.11 プロトコルの BSS モードによるネットワーク	8
2.7	従来のネットワークモデル	9
2.8	識別子の配布状況の変化	10
3.1	IEEE 802.11 プロトコルの IBSS モードによるネットワーク	13
3.2	NAPT による通信を開始する方向の制限	14
3.3	NAPT による通信の開始制限とその回避	14
3.4	両方の条件を満たしている構成	17
3.5	両方の条件を満たしている構成	17
3.6	両方の条件を満たしている構成	18
3.7	無線アドホックネットワークモデル	19
3.8	オーバレイアドホックネットワークモデル	19
3.9	双方向の到達性)	20
3.10	IP アドレス変更による到達性の喪失	20
3.11	IP アドレス通知による到達性の回復)	21
4.1	初期状態	25
4.2	RREQ メッセージの散布 (a)	25
4.3	RREQ メッセージの散布 (b)	26
4.4	RREP メッセージの返信	27
4.5	モバイル IP	28
4.6	モバイルノードの移動	29
4.7	CoA 通知による接続性の復帰	30
5.1	提案アーキテクチャ	31
5.2	推移性の補完	32

5.3	双方向性の補完	33
5.4	A multicast message delivery in a wireless ad-hoc network	34
5.5	A multicast message delivery in an overlay ad-hoc network	35
5.6	signaling process in overlay ad-hoc networks	36
6.1	ミドルウェア	38
6.2	フレームフォーマット	39
6.3	robohoc ノード内部表側	41
6.4	robohoc ノード内部裏側	41
6.5	robohoc ノード外観	42
6.6	robohoc ロボット外観	43
6.7	マルチチャネルメッシュネットワーク	43
6.8	robohoc 実験結果	44
7.1	無線伝送	46
7.2	電波の減衰	46
7.3	電波のフェージング	47
7.4	変調方式と通信可能距離	48
7.5	隠れ端末問題	48
7.6	RTS 送信	49
7.7	CTS 送信	49
7.8	分散観測の概要	52
7.9	送信フレームと ACK フレームのペアリング	53
7.10	フレーム間間隔	54
7.11	実験環境	57
7.12	計測結果	57
7.13	送信時刻推定と結合適用後の結果	58

表目次

6.1	無線ネットワークノードの構成	41
7.1	Radiotap ヘッダ内の情報	53
7.2	ペアリングアルゴリズム	55

第 1 章

序論

我々は、近い将来のインターネットにおいて、接続ネットワークを変えるモバイルノードが主流になっていくと考える。先進国では携帯情報端末を使ったインターネットアクセスが既に増加し始めている。その背景にあるのは、どこにいても、どんな時もインターネットを利用したいという要請である。ウェブ、メール、その他のアプリケーションは、個人、企業を問わず、活動に必要なツールとして定着してきた。ウェブ上には、膨大な知識が蓄積され、検索エンジンによって高速なアクセスが提供されている。この知識のデータベースは、我々が学び方や問題解決のやり方に大きな影響を与えている。また、ウェブ上のコミュニケーションサービスやメールによってリアルタイムに思考を交換できるようになり、さらに新しい知識が生み出されている。これらのツールの重要性が高まると同時に依存度も高まってくる。いつでもどこでもこれらのツールを使いたいという要請も高まっている。実際、日本の平成 19 年時点における個人のインターネット利用者のうち、携帯電話、PHS その他の携帯端末の利用者は 82.7 パーセントに達している [1]。また発展途上国では、高価な配線コストを避けるため、広域無線通信網が有線通信網に先立って展開されている。この広域無線通信をインターネットへの接続に応用できるようになれば、固定端末を介さずに、直接、携帯端末が普及する進んでいくと考える。現在の世界のインターネット利用者は、世界人口の 67 億人超に対して、17 億人を超えたばかりである。今後発展途上国への展開が進めばインターネットホストの構成が大きく塗り替えられることは間違いない。

3 章で詳しく述べるように、携帯端末は他の端末との接続時間を最大化するために、接続するネットワークを切り替えたり、同時に複数のネットワークに接続したり、無線アドホックネットワークを構成したりする。このようなモバイルホストの振る舞いは、利用者の時間や場所の自由を保ちながらホストがお互いに接続している時間を長くするが、同時に IP アドレスやホスト間の到達性の変更による問題をも導入する。現在のインターネットアーキテクチャは、有線のリンクとそこに固定されたホストを前提に設計されたためこの問題へ対応を定義していない。個々のアプリケーションが場当たり的に対応しているというのが現状である。アプリケーションが個々にこの仕組みを実装するのは負荷が大きく、また対応が不十分になりうるという問題がある。したがって、我々は、このままのインターネットアーキテクチャでモバイルホストが主流になると、今後インターネット上の分散システムを構築と運用を難しくするのではないか

という危惧を持っている。モバイルホストをこれまでの固定ホストと同じように透過的に扱えるネットワークアーキテクチャが必要だと考える。

そこで本論文では、モバイルホストが集まって分散システムを構築するためのネットワークアーキテクチャを提案する。このアーキテクチャは、現在のインターネットアーキテクチャを基に、新たにリンク層とネットワーク層の間にリンク補完層を挿入したものである。リンク補完層は、モバイルホストが導入した、IP アドレスの変更、ホスト間の到達性の変更、その他の変更により発生する問題を解決し、上位層に一貫したネットワークの眺めを提供する。つまり、アプリケーション層からこの問題への対応という責務を取り除く。

本論文の構成

本論文を以下のように構成する。

2 章では、モバイルホストを考慮しないこれまでのインターネットアーキテクチャに対応する、従来のネットワークモデルについて考察する。3 章では、モバイルホストを考慮した新しいネットワークモデルを考案し、その特性について考察する。4 章では、3 章で提案したネットワークモデルの上で、分散システムを構成する場合の課題について述べ、その課題が既存研究の中でどのように取り組まれてきたかまとめる。5 章ではリンク補完層を提案する。6 章では、提案アーキテクチャに基づいて作られたシステムの実装について述べ、そのシステムを利用した実証実験を紹介する。7 章ではリンク補完層が扱う各リンクの品質評価をどのように行うべきか議論する。また、その中でモバイルホストの分散システムのデバッグに必要な分散監視機構について述べ、その実装と実証実験の結果を紹介する。8 章では本論文の提案手法について議論し、最後に 9 章で本研究をまとめる。

第2章

従来ネットワークのモデル化

これまでの分散システムが前提としてきたネットワークのモデル化について考察する。まず、これまでのインターネットでは一般的な3つの性質を示す。次にその3つの性質を前提とするネットワークをモデル化する。最後に、そのネットワークモデルがアプリケーション層サービスにとって望ましい特性を保持していることを示す。

2.1 前提

インターネットは、**ノード**と呼ばれる、IPを実装する機器から構成される。各ノードは1つまたは複数の**サブネット**に属している。サブネットは1つのリンクによって所属ノードをつな

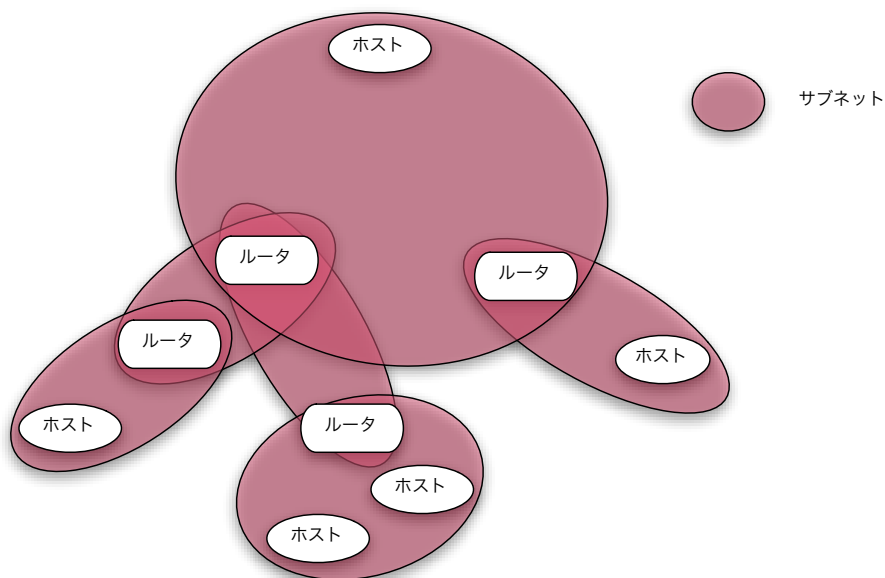


図 2.1 インターネット構成例

げている。複数のサブネットに属してそれらを繋げるノードは特に**ルータ**と呼ばれ、ルータ以外のノードは特に**ホスト**と呼ばれる。インターネットの具体的な構成例を図 2.1 に示す。

これまでのインターネットでは以下のような構成が一般的だった。

1. 各サブネットのリンクは IP に適したリンクモデルを持つ。
2. インターネットはデータパケットを取り除いたり変更したりしない。
3. 各ノードは特定の単位ネットワークへの接続を維持している。

以下にそれぞれの構成について詳しく述べる。

2.1.1 古典的 IP リンクモデル

IETF の IAB が中心になって、IPv4 と IPv6 を含む IP に適したリンクのモデルが議論されてきた [2]。この中で IP に適したリンクは以下の 3 つだとされている。

マルチアクセスリンクモデル このモデルでは、0 個以上のルータを含む複数のノードが同じリンクに接続している。リンクローカルブロードキャストアドレス (255.255.255.255) やリンクローカルマルチキャストアドレスに送信されたデータパケットは、他の全ての対象ノードによって受信される。同じリンクに接続する 2 ノードは IPv4 の TTL や IPv6 の Hop Limit を減らさずに通信できる。リンク内には任意の数のレイヤ 2 の機器 (ブリッジ、スイッチ、アクセスポイント、その他) が存在する。

ポイント・ツー・ポイントリンクモデル このモデルでは、リンク上には 2 ノードが接続している。リンクローカルブロードキャストアドレスやリンクローカルマルチキャストアドレスに送信されたデータパケットは、他方のノードによって受信される。2 ノードは IPv4 の TTL や IPv6 の Hop Limit を減らさずに通信できる。リンク内には任意の数のレイヤ 2 の機器 (ブリッジ、スイッチ、アクセスポイント、その他) が存在する。

非ブロードキャストマルチアクセス (NBMA) モデル マルチアクセスリンクモデルの派生であり、2 ノード間でもブロードキャストやマルチキャストパケットが送信できないことを除けば、マルチアクセスリンクモデルと同様である。結果として、ブロードキャストやマルチキャストを利用するプロトコルやアプリケーションは NBMA の上では役に立たない。

3 章で述べる別のリンクモデルと対比して、これらのリンクモデルを特に**古典的 IP リンクモデル**、古典的 IP リンクモデルに即したリンクを古典的 IP リンクと呼ぶ。これまでのインターネットでは主に古典的 IP リンクである。

古典的 IP リンクモデルに共通するのは、そのリンクに接続するノードはお互いに直接に通信できることである。つまり、ルータを介さずに、レイヤ 2 の機器のみを介して各ノードが繋がれている。また別の言い方をすれば、あるリンクはあるノード集合という明示的な通信範囲

を提供している。その通信範囲の中にある全てのノードは、通信範囲内の他の全てのノードと通信できる。

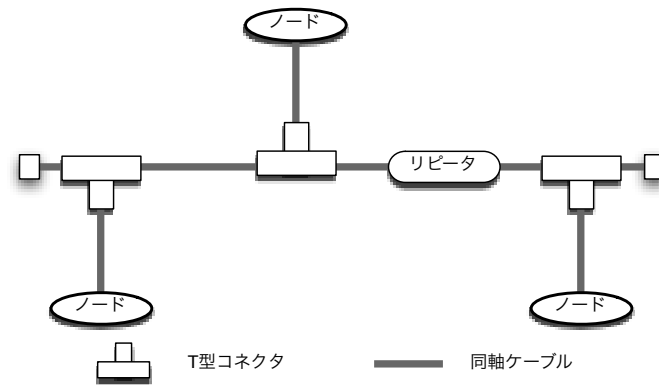


図 2.2 バス型の有線リンク技術を用いたサブネット

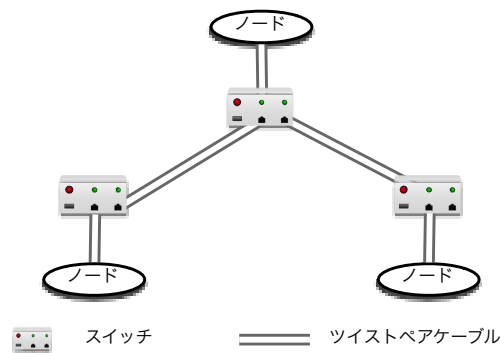


図 2.3 スター型の有線リンク技術を用いたサブネット

古典的 IP リンクモデルが受け入れられてきたのは、これまでの主要なリンクだった有線リンクが、自然に、このリンクモデルを実現できるからである。有線リンクでは、配線とレイヤ 2 の機器が信号が伝搬する範囲を決めている。つまり、この範囲に含まれる全てのノードは、お互いにデータパケットを交換して通信できる。有線リンク技術を用いたサブネットの例として、図 2.2 に 10Base-2 などのバス型有線リンクのサブネットを示す。10Base-2 では、規格を満たす同軸ケーブル、T 型コネクタ、リピータによって通信範囲が決められる。図 2.3 に 10Base-T などのスター型有線リンクのサブネットを示す。10Base-T では、規格を満たすツイストペアケーブル、スイッチによって通信範囲が決められる。実際、この通信範囲に含まれる全てのノードはお互いに通信できている。

リンク内の全てのノードがお互いに直接に通信できる時は、リンクに**双方向性**と**推移性**が成り立っている。サブネット内の要素を特定して、ノードを $node_i$ で表し、 $node_1$ から $node_2$ へ送信可能なことを以下の式のように表すものとする。

$$node_1 \Rightarrow node_2 \quad (2.1)$$

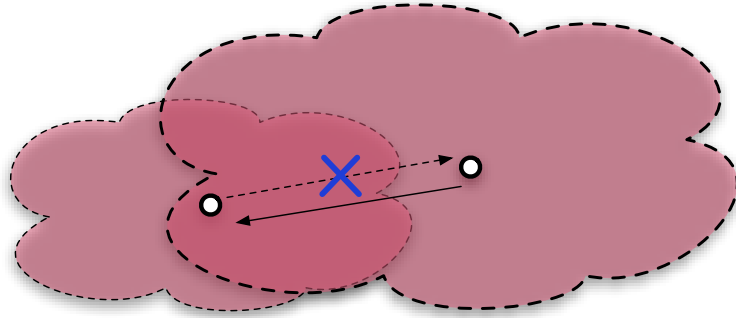


図 2.4 片方向リンク

双方向性とは、ノード 1 とノード 2 について、ノード 1 からノード 2 へデータパケットを直接に送信できるなら、ノード 2 からノード 1 へもできるという特性である。假定より、ノード 1 からノード 2 へデータパケットが直接に送信できるなら、ノード 1 とノード 2 は同じリンクによって決められる通信範囲に含まれているということである。したがって、ノード 2 からノード 1 へも直接に送信できる。式では以下のように表わせる。

$$node_1 \Rightarrow node_2 \text{ ならば } node_2 \Rightarrow node_1 \quad (2.2)$$

また推移性とは、ノード 1, ノード 2, ノード 3 について、ノード 1 からノード 2 へ、かつ、ノード 2 からノード 3 へデータパケットを直接に送信できるなら、ノード 1 からノード 3 へもできるという特性である。双方向性の議論と同様に、假定より、ノード 1 とノード 2 は同じリンクによって決められる通信範囲に、ノード 2 とノード 3 も同じリンクによって決められる通信範囲に含まれている。したがってノード 1 とノード 3 も同じリンクによって決められる通信範囲に含まれており、ノード 1 からノード 3 へもデータパケットを直接に送信できる。式では以下のように表す。

$$node_1 \Rightarrow node_2 \text{ かつ } node_2 \Rightarrow node_3 \text{ ならば } node_1 \Rightarrow node_3 \quad (2.3)$$

以上の議論により、

$$\text{古典的 IP リンクならば双方向性と推移性が成り立っている。} \quad (2.4)$$

ことが証明された。

しかし双方向性と推移性は、無線伝送を用いる無線リンクにとっては、自然ではない。配線とレイヤ 2 の機器によってリンク内のノードの通信範囲が一意に決められていた有線リンクと異なり、無線伝送では、各ノードが信号を送信できる範囲はそれぞれ異なっているためである。図 2.4 に示すように、例えば無線ネットワークインターフェースの送信パワーが異なるノード 1 とノード 2 については、ノード 1 からノード 2 へは直接に送信できるが逆にノード 2 からノード 1 へはできない状況、つまり、双方向性が成り立たない状況がある。また同様に、図 2.5 に示すように、ノード 1 からノード 2 へ、ノード 2 からノード 3 へ直接に送信できるが、ノード

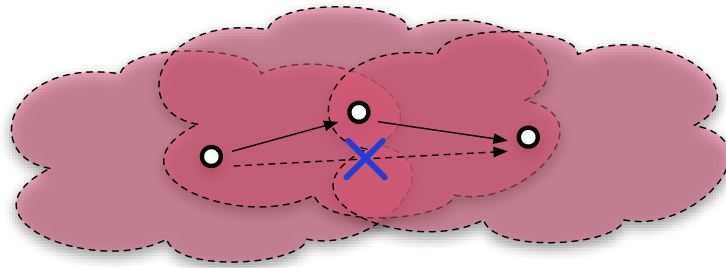


図 2.5 非推移的なリンク

ド1からノード3へはできない状況、つまり、推移性が成り立たない状況がある。式2.4の対偶を考えれば、双方向性を持たない、または、推移性を持たない、無線リンクは、古典的IPリンクではない。このようなリンクによってつながれたホストの集合は、現在のインターネットアーキテクチャではそのまま利用できない。

とはいえ、IEEE802.11 プロトコルの BSS モード、Bluetooth など、実際に広く利用されている無線リンクの多くは古典 IP リンクである。これらのは無線伝送の応用範囲に制約を課すことで、双方向性や推移性が成り立たないリンクを排除して古典的 IP リンクモデルに適合しているためである。例として IEEE802.11 プロトコルの BSS モードについて説明する。IEEE802.11 プロトコルの BSS モードは、リンク内のノードをステーションとアクセスポイントに仕分け、ステーション間の直接通信を禁止している。ステーションから送信されたフレームはアクセスポイントのみに受信されるため、あるステーションから別のステーションへフレームを配送するためには、アクセスポイントがそのフレームを再送する必要がある。したがって、IEEE802.11 プロトコルの BSS モード内では、ある2つのステーションが通信するためには、両方のステーションがアクセスポイントと双方向の接続性を持たなければならない。図2.6に IEEE802.11 プロトコルの BSS モードをリンクに用いるサブネットの構成例を示す。この中で、ステーション1、ステーション2、ステーション3、ステーション4はアクセスポイントと双方向の接続性を持つ。したがってこの中の全てのステーションはアクセスポイントを経由してお互いに通信できる。つまり、無線伝送を用いていながらも古典的 IP リンクモデルを持つ。

したがって、少なくともこれまでのインターネットで利用されてきた有線リンクと無線リンクは古典的 IP リンクである。そこで本章では分散システム内のホストが接続するサブネットは古典的 IP リンクだと仮定する。

2.1.2 インターネットの透過性

これまでのインターネットが成功した要因の一つとしてエンドツーエンド原理が挙げられる。エンドツーエンド原理は、エンドポイント間のプロトコルはネットワークが管理する状態に頼るべきではなく、状態が破壊されるのはエンドポイント自身が破壊されたときだけになるように、通信に必要な状態はできるだけエンド上で管理されるべきというものだ [3]。この原理を満

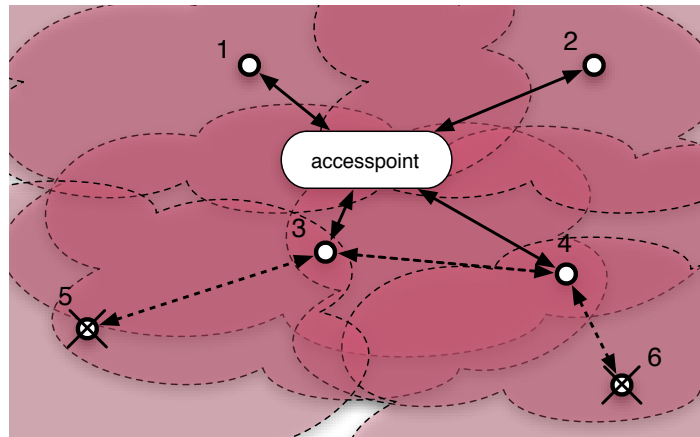


図 2.6 IEEE 802.11 プロトコルの BSS モードによるネットワーク

たすインターネットは、通信パスの中間にあるルータはデータパケットを出来るだけ効率的に早く送信する処理を行い、通信パスの端にあるホストが複雑な処理を行うように設計されている。この設計により、アプリケーション特有の処理は更新がしやすいホスト上のみに実装されているため、さまざまなアプリケーションサービスが展開できたし、比較的少数しかないルータの負荷を下げ、インターネットが経験したホスト数の爆発的な増加にも対応できた。エンドツーエンド原則を満たしたインターネットは、内部でデータパケットを取り除いたり変更したりせずにそのまま通過させるので、**透過性**を持つとも表現される。インターネットの透過性はインターネットコミュニティが今後も保護すべきものとされている [4]。

以上の議論により、少なくともこれまでのインターネットの大部分は透過性を持っていたと考える。そこで本章では分散システム内のホストをつなぐインターネットは透過性を持っていると仮定する。

2.1.3 固定ホスト

これまでのインターネットでは一般的なホストは特定のサブネットにつながり続けている**固定ホスト**だった。コンピュータそのものにさまざまな物理的な制約があり同じ位置に備え付けて利用することが多かったためである。特にインターネット黎明期のコンピュータはサイズも重量も大きく移動は困難だった。またコンピュータに必要な電力を確保するために電源ケーブルを、他のコンピュータと通信するために通信ケーブルを配線する必要があるため、これらの配線によってもやはり移動が制限された。

また、同じサブネットに接続し続けるホストは同じ IP アドレスを利用し続ける。固定 IP アドレスを設定されている場合はもちろん、Dynamic Host Configuration Protocol(DHCP)[5] や Point-to-Point Protocol(PPP)[6] によって動的に IP アドレスを割り当てられる場合も IP アドレスの利用期間を更新すればほとんどの場合特定の IP アドレスを利用し続けられる。

以上の議論により、少なくともこれまでのインターネット上の大部分ホストは固定ホストだったと考える。そこで本章では分散システム内のホストは固定ホストだと仮定する。

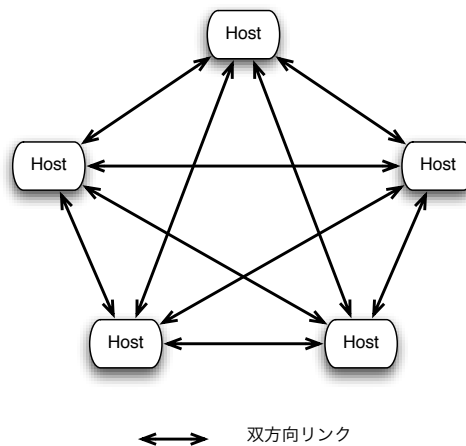


図 2.7 従来のネットワークモデル

2.2 従来のネットワークモデルとその特性

本節では、分散システム内のホストとその間のネットワークに上述した仮定が成り立っていた、これまでのインターネットのネットワークモデル、つまり従来のネットワークモデルについて考察する。

まず、ホストが古典的 IP リンクに接続しているという仮定より、同じサブネットの内部の全てのホストはお互いに通信できる。次に、インターネットに透過性があるという仮定より、サブネット間をつなぐルータはデータパケットを破棄したり変更したりしない。よって異なるサブネットにつながる全てのホストはお互いに通信できる。最後に、ホストが固定ホストであるという仮定により、ホストに割り当てられた IP アドレスは変わらないのでホストの識別子として IP アドレスが利用できる。したがって、これまでのインターネットは、図 2.7 に示すように、全てホストが割り当てられた一意な IP アドレスを利用してお互いに通信できるとモデル化できる。

アプリケーション設計という観点からみると、従来のネットワークモデルは2つの望ましい性質を持っている。

第一に、このモデルは分散システムが作るホスト間の接続を全く制限しない。図 2.7 に示すように、各ホストをつなぐネットワークは全てのホスト間に接続性を提供している。したがって、任意の2つのホストは、少なくとも一方がもう一方の識別子さえ知っていれば通信を開始できる。

第二に、このモデルが利用する識別子は絶対的な値であり、あるホストに対する識別子はどのホストからみても同じである。つまり、識別子をデータとしてデータパケットに含めて他のホストへ送信しても識別子の利用価値は失われない。これを利用すれば、ホスト間で識別子を交換して新しい通信の可能性を広げていくことができる。例を用いて説明する。図 2.8(a) は、従来のネットワークモデルにおいて、ホスト 1、ホスト 2、ホスト 3、ホスト 4 がホスト 0 の識

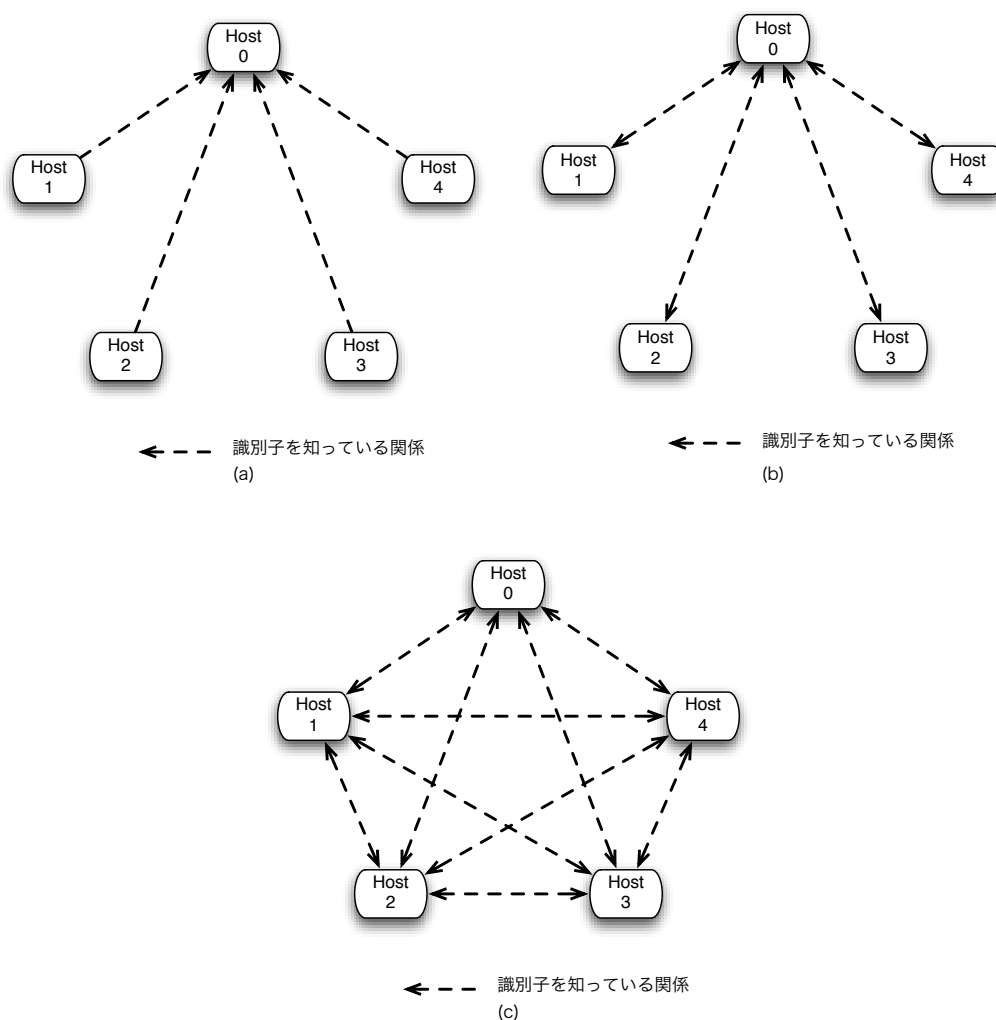


図 2.8 識別子の配布状況の変化

別子を知っている状態を表している。この状態では、ホスト間のネットワーク自体は通信を制限しないが、お互いに識別子を知らないホスト間では通信をそもそも開始できない。図 2.8(b) は、ホスト 1, ホスト 2, ホスト 3, ホスト 4 が唯一知っていたホスト 0 へ通信を開始した後の状態である。ホスト 0 はデータパケットの送信元アドレスフィールドからホスト 1, ホスト 2, ホスト 3, ホスト 4 の識別子を知る。そして図 2.8(c) は、ホスト 0 が一手順前で知った全てのホスト識別子を、それぞれのホストへ配布した後の状態である。各ホストは他の全てのホストの識別子を知り自由に通信を開始できるようになっている。

従来のネットワークモデルは、アプリケーション設計の観点から考えると柔軟な設計を行えるネットワークモデルだと考える。各ホストは IP アドレスを知る全てのホストを通信相手して選べるからである。逆に、あるホスト間の通信が制限されれば、そのホスト間の通信を諦めてアプリケーションの設計空間を狭めたり、本来取り組むべき処理に加えて別のホストを迂回するための処理を実装したりしなければならない。革新的なアプリケーションの開発を阻害す

る恐れがある。

また既に多くのアプリケーションが従来のネットワークモデルを基に開発されてきたことにも留意すべきである。これらのアプリケーションは理想的なネットワークに依存した設計を持ちうる。もし従来のネットワークモデルの仮定が崩れてホスト間の通信に制限が発生すれば、アプリケーションの一部の機能が利用できなくなったり、最悪の場合にはアプリケーションが完全に利用できなくなったりしうる。

第 3 章

モバイルネットワークのモデル化

本章では、モバイルホストが実状に即したインターネットにつながれている場合を扱うための新しいネットワークモデルについて考察する。まずモバイルホストと実状に即したインターネットが、2章の仮定に即していないことを確認する。次に、モバイルホストが実状に即したインターネットにつながれている場合は扱う新しいネットワークモデルを提案しその特性について述べる。

3.1 前提の変化

インターネットは絶えず変化し続けている。インターネットが社会に欠かせないインフラストラクチャになるにしたがって、スケーラビリティ、堅牢性、セキュリティへの要求が高まってきた。また、インターネットの応用範囲が広がるにしたがって、その構成技術も多様化してきた。このような背景の中で、2章で述べた3つの前提は以下のように変わりつつある。

1. 古典的 IP リンクを用いないサブネットが現れ始めている。
2. インターネットの透過性が失われつつある。
3. ネットワーク間を移動するホストが現れ始めている。

それぞれの仮定について議論する。

3.1.1 非古典的 IP リンク

IEEE802.11 プロトコルの BSS モードは貴重な電波資源を効率的に利用していない。これまでのインターネットが古典的 IP リンクモデルを前提としていたのは、インターネット黎明期に広く利用されていたリンクが有線リンクだったためである。確かに、IEEE802.11 プロトコルの BSS モードが広く普及した理由は、無線伝送の応用範囲を制約することで古典的 IP リンクモデルに適合し、有線リンクの代替としてそのまま利用できたからである。しかし、この制約によって無線伝送の特性を活用する機会が失われてきたことは留意すべきであり、古典的 IP リンクに適合しない無線リンクについて再考する必要があると考える。

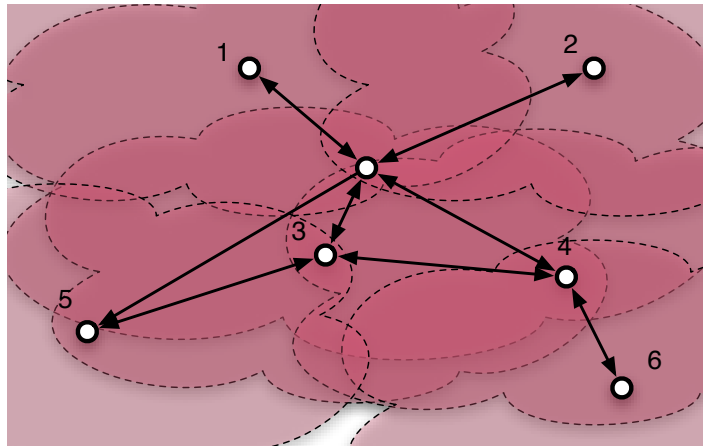


図 3.1 IEEE 802.11 プロトコルの IBSS モードによるネットワーク

IEEE802.11 プロトコルの BSS モードは無線伝送のブロードキャスト特性を活用していない。2つの機器を結ぶ配線の上には伝搬路を持たない有線伝送と異なり、無線伝送は複数の伝搬路を持ちうるため、無線リンクは複数ノードに同時にデータパケットを配送を配送できるという特性である。しかし図 2.6 に示したように、各ステーションが送信したフレームはアクセスポイント以外のノードは受信しない IEEE802.11 プロトコルの BSS モードは、無線伝送のブロードキャスト特性を生かさず、ステーションとアクセスポイントという 2つの機器間の伝搬路のみを利用している。これはステーションとアクセスポイントの二点間のみを結ぶ有線リンクをエミュレートしていることに他ならない。

本来利用可能なはずの複数ノードへの伝搬路を 1つに絞る制約はさまざまな損失を生む。図 2.6 に示す構成例では、ステーション 3 とステーション 4 はお互いに伝送可能範囲に含まれているが、制約によって、アクセスポイントを経由して通信する。このとき、ステーション 3 からステーション 4 へ直接に送信する場合と比較して、アクセスポイントが送信する分の電波資源が余計に消費されている。また、全てのデータパケットがアクセスポイントを通るのでアクセスポイントが性能上のボトルネックになりやすい。さらに、ステーション 5 とステーション 3、ステーション 6 とステーション 4 は互いに無線伝送できるにもかかわらず、制約によって、アクセスポイントとの双方向接続がないステーション 5 とステーション 6 は、この無線リンクを利用できない。アクセスポイントと直接通信できるトポロジに無線伝送が応用範囲が狭められている。

我々は、貴重な電波資源をこれまで以上に有効活用するために、今後は無線伝送のブロードキャスト特性を生かした無線リンクが採用されていくと考える。このような無線リンクの例として IEEE802.11 プロトコルの IBSS モードについて議論する。IEEE802.11 プロトコルの IBSS モードでは、ステーションとアクセスポイントという区別はなく、全てのノードはお互いに直接通信できるステーションである。図 3.1 は、IEEE802.11 プロトコルの IBSS モードを用い、図 2.6 のアクセスポイントをステーションに置き換えたのネットワークである。同じ配置でも IEEE802.11 プロトコルの BSS モードでは、全く通信できなかったステーション 5 とス

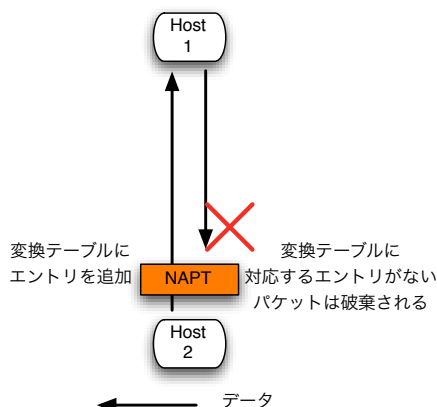


図 3.2 NATP による通信を開始する方向の制限

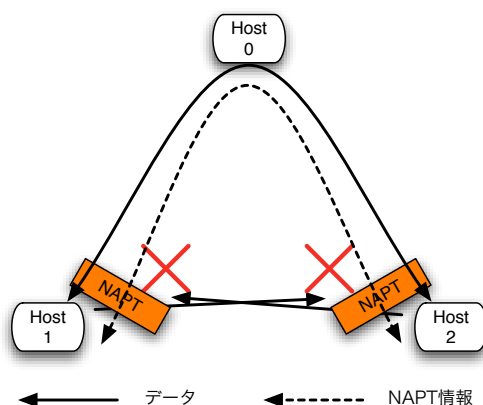


図 3.3 NATP による通信の開始制限とその回避

テーション 6 が通信できている。また、ステーション 3 とステーション 4 は直接に通信できしており、一度の送信によってデータパケットを配送できている。一方で、IEEE802.11 プロトコルの IBSS モードを利用する場合はリンクに双方向性や推移性は成り立たず、

つまり、同じリンクに接続していても直接には通信できないつまり、ノード間の接続性は時間変化する有向グラフによって表現される。各ノードはこのグラフの上の経路制御という問題を解く必要がある。

3.1.2 インターネットの非透過性

さまざまな要因によってインターネットの透過性が失われてきている。

第一の要因は、IPv4 アドレスの消費を抑えるために IPv4 アドレスを複数ノードによって共有する Network Address and Port Translation(以下、NAPT とする) 機器の普及が進んだことである。NAPT は内側と外側の 2 つのネットワークをつないでデータパケットを中継するルータの一種である。ルータとしての基本的な機能に加えて、パケット内のヘッダを書き換え

て、外側のネットワークインタフェースの IP アドレスを、内側のネットワークのホストが共有できるようにする [7]。通信パス上の NAPT は、図 3.2 に示すように通信を開始する方向を制限したり個々のホストのセッション数を制限したりするため、インターネットの透過性を阻害する。図 3.2 のように片方のホストのみが NAPT の内側にある場合は通信の開始方向を制限されるだけだが、図 3.3 のように両方のホストが NAPT の内側にある場合は通信を開始できない。このようなホストがデータを交換するには、他のホスト上を迂回してデータを交換するか、STUN[8] サーバを利用して NAPT を通過するか、いずれの対応をするにせよ NAPT の内側にはない第三者ホストの協力が必要になる。さらに、IPv4 アドレスの枯渇が近づき、ISP の内部に設置される NAPT、つまり Large Scale NAT(LSN) の導入も検討されている [9]。ISP 加入者が既に利用している NAPT と合わせて通信パス上に複数の NAT が存在するようになれば、問題のさらなる悪化が懸念される。

第二の要因は、ホストを悪意があるアクセスから守るために、ファイアウォールはパケットの内容に基づいてデータパケットを遮断するファイアウォールのネットワーク内への導入が進んだことである。エンドツーエンドの原則により全てのホストが直接に通信できる状況では、ホストは世界中のホストからのアクセスを受けうる。もちろん、個別のホスト上にファイアウォール機能を実装するなどのセキュリティ対策を施すことも可能だが、ホストの数が大きい場合や個別のセキュリティ対策の強制が難しい場合には、ネットワーク内へのファイアウォール機器の設置は依然として有効なセキュリティ対策である。通信パス上のファイアウォールを完全に通信を遮断したり通信を開始する方向を制限したりするため、インターネットの透過性を阻害する。開始方向が制限される場合は NAPT と同様の対応が必要になる。

第三の要因は、ルータのハードウェアやソフトウェアの問題やリンクの切断によりリンク故障が起きた場合や DDoS 攻撃やバースト的な通信が起こした輻輳によりパス障害が起きた場合にホスト間の特定の通信パスが利用できなくなることである。そもそもその通信パスしか利用できない場合はリンクやパスが故障から復旧するまで待つしかないが、複数の通信パスが利用できる場合にはインターネット中の経路制御が代替パスを構築するまで待てばよい。しかし、Anderson らによれば、Autonomous System(以下、AS とする)間の経路制御に使われている Border Gateway Protocol(以下、BGP-4 とする)は、ホスト間の通信の耐障害への適応性が低いという問題がある [10]。BGP-4 は、スケーラビリティを最優先に設計されているため、スケーラビリティの実現や AS の経路制御ポリシーを強制のために多くの経路情報を隠し、トラフィック量に関する情報を持たず、スケーラビリティのために経路情報の更新を控えている。このため AS 内部で利用される他の経路制御プロトコルと比較して代替パスの構築が遅れ、ホスト間の通信が数分から数時間にわたって利用できないことがある。

3.1.3 モバイルホスト

ウェブ、メール、チャットなどのインターネット上のサービスは社会インフラストラクチャとして我々の生活に欠かせなくなった。またコンピュータの小型化、バッテリーの高性能化が進み、ラップトップコンピュータ、スマートフォンなどの携帯可能なコンピュータが手に入るように

なった。結果として、利用したいときに我々がインターネットホストの前に移動するパラダイムから常に利用できるようにインターネットホストが移動するパラダイムへの転換が起こった。

しかし、コンピュータは生活に合わせて移動できるようになっても、一定のネットワークへそのコンピュータが接続しつづけられるとは限らない。一般にネットワークに接続できる領域は制限されているためである。有線リンクを用いたネットワークには通信ケーブルが届く領域しか接続できないし、無線リンクの IEEE802.11 を用いたネットワークには一般にアクセスポイントから百メートル程度の領域内しか接続できない。日本の人口カバー率が 100% を達成している docomo の 3G を用いたネットワークですら、電波が届かない建物の地下では利用できない。移動するコンピュータがインターネットへの接続性を維持するためには、複数のネットワークを使い分ける必要がある。

またネットワークはそれぞれ接続できるかどうかだけではなくさまざまな性質を持つ。3G 無線を用いたネットワークが利用可能な場合にも、他に IEEE802.11 などのカバーエリアは狭いがより広帯域な無線リンクを用いたネットワークや配線が必要だが安定して広帯域な有線リンクを用いたネットワークを選択すれば、

また同種のネットワークでも、リンク状態やネットワークの内部の輻輳状況によってサービスの品質は左右される。同じ IEEE802.11 の BSS モードを用いたネットワークでも、より近いアクセスポイントや接続するステーション数が少ないアクセスポイントがあるなら、そちらを利用した方がやはり高品質なサービスを受けられる。つまり、人間と共に移動するインターネットホストが、インターネットへのそもそもの接続性や接続の品質を維持するためには、複数のネットワークの使い分けが必要不可欠である。

ホストが接続するネットワークを切り替えると、IP アドレスを含むネットワーク層以下の状態は大きく変わることになる。また IP アドレスなどの状態変更の影響を受けて、トランスポート層、アプリケーション層も影響を受ける。固定ホストが仮定できる環境では IP アドレスは、一意で変更されないの、ホスト識別子として利用できていた。しかし、モバイルホストは IP アドレスを変更するので、IP アドレスをホスト識別子として利用できない。

3.2 モバイルホストのネットワークモデルとその特性

これまで述べたように、我々は今後のインターネットでは 2 章の前提が必ずしも成り立たないと思う。これら前提が成り立たないホストとネットワーク上の分散システムのためには、従来のネットワークモデルではない新しいネットワークモデルが必要である。この新しいネットワークモデルを特にモバイルホストのネットワークモデルと呼ぶ。

モバイルホストは、一定のネットワークへの接続を維持するとは限らず、ネットワークの間を移動する。つまり、新しいネットワークへ接続したり現在の接続ネットワークから離脱したりする。このときホストが利用する IP アドレスも同時に変更される。そこで、このように接続するネットワークに変更される IP アドレスとは別に各ホストに識別子が割り当てられているものとする。あるホストにデータパケットを送信できるのは以下の条件を満たすときである。

1. そのホストの IP アドレスを知っている.
2. その IP アドレス到達するパスをインターネットが提供している.

あるホストが移動すると、移動によって変更された IP アドレスが他のホストに通知されるまで、他のホストからそのホストへデータパケットを送信することはできない。

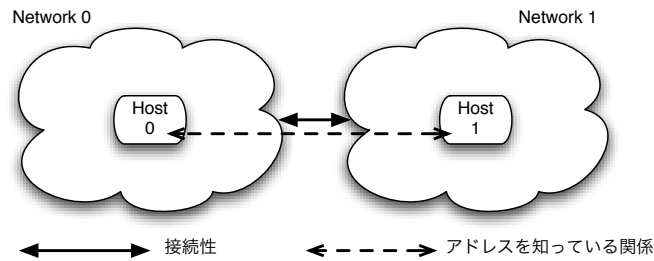


図 3.4 両方の条件を満たしている構成

図 3.4 はホスト 0 がネットワーク 0 に、ホスト 1 がネットワーク 1 に接続している状態である。ホスト 0 とホスト 1 はお互いの IP アドレスを知っており (条件 1)、ネットワーク 0 とネットワーク 1 の間にもパスが存在している (条件 2)。このときはホスト 0 からホスト 1 からも通信を開始できる。

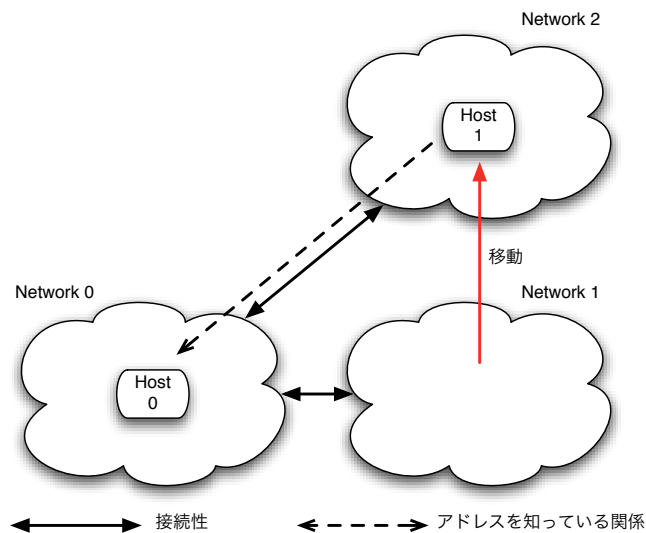


図 3.5 両方の条件を満たしている構成

図 3.5 は、図 3.4 の状態から、ホスト 1 がネットワーク 2 へ移動した状態である。ホスト 1 は、ネットワーク 1 で利用していた IP アドレスは無効にし、ネットワーク 2 から新しい IP アドレスを取得する。ネットワーク 0 とネットワーク 1 の間にパスは存在するが、ホスト 0 は、ホスト 1 の有効な IP アドレスを知らないため、ホスト 1 へ通信を開始することはできない。一方、ホスト 1 は、ホスト 0 の IP アドレスを覚えているので、ホスト 0 への通信を開始できる。

ホスト 0 は、1 度ホスト 1 からのパケットを受信すれば、ホスト 1 の新しい IP アドレスを取得できる。これにより最終的に、図 3.4 と同様の、ホスト 0 からホスト 1 からも通信を開始できる状態に復帰する。

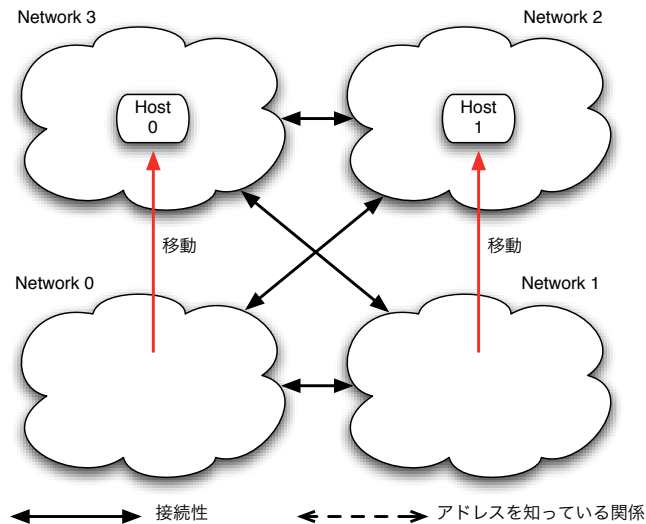


図 3.6 両方の条件を満たしている構成

図 3.6 は、図 3.4 の状態から、ホスト 0 がネットワーク 3 へ、ホスト 1 がネットワーク 2 へ同時に移動した状態である。ホスト 0 とホスト 1 は、元々のネットワークで利用していた IP アドレスを無効にし、移動先のネットワークから新しい IP アドレスを取得する。移動先のネットワークでもインターネットはホスト 0 とホスト 1 間のパスを提供している（条件 2）が、ホスト 0 もホスト 1 も相手の新しい IP アドレスを知らないので通信を開始できない。この状態に陥ると、両方のホストの新しい IP アドレスを知る第三のホストの協力を得てどちらかのホストがもう一方の IP アドレスを取得しない限り、図 3.4 と同様の、通信ができる状態には復帰できない。

上述した状況では、ネットワーク間の通信パスは常にあることを仮定していた。実際には NATP、ファイアウォール、障害などによりモバイルホスト間のネットワークに透過性がなく、通信の開始方向が制限されていたりそもそも通信の開始が制限されていたりすることもある。例えば、図 3.5 の状況でネットワーク 0 に NATP が設置された状況を考えると、ホスト 1 はホスト 0 の有効な IP アドレスを知っているが、NAPT の外側のホスト 1 からホスト 0 には通信を開始できないためホスト 1 は新しい IP アドレスをホスト 0 に通知できない。したがってホスト 0 とホスト 1 はどちらからも通信を開始できない。

それではどのような状況のときに通信を開始できる状態に復帰するのだろうか。図 3.7 は無線アドホックネットワーク内のホスト間の接続関係を示している。ホストは物理的に移動し、無線フレームが受信できる範囲は限られているので、ホスト間の接続関係は時間変化する。また前述したようにこの接続性には双方向性、推移性も成り立たない。このホストを集めたネットワークの全体の接続性は、ホストをノード、接続関係をエッジとした時間変化する有向グラフになる。

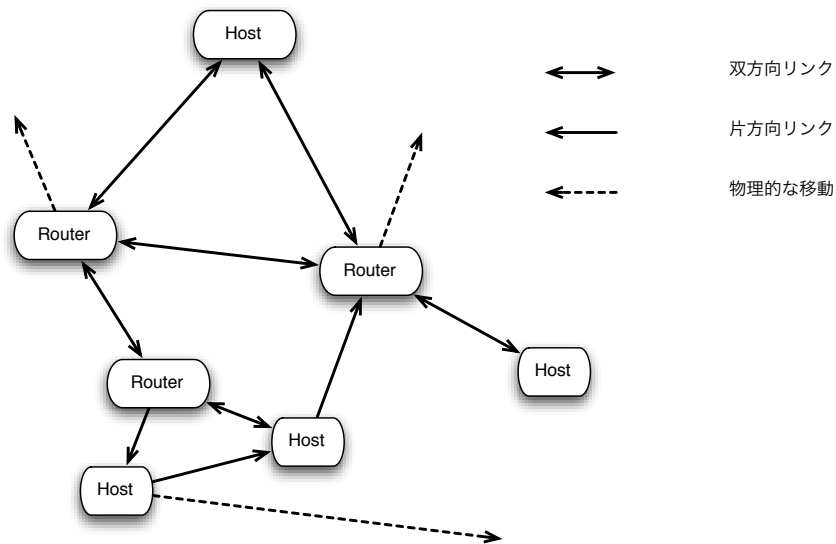


図 3.7 無線アドホックネットワークモデル

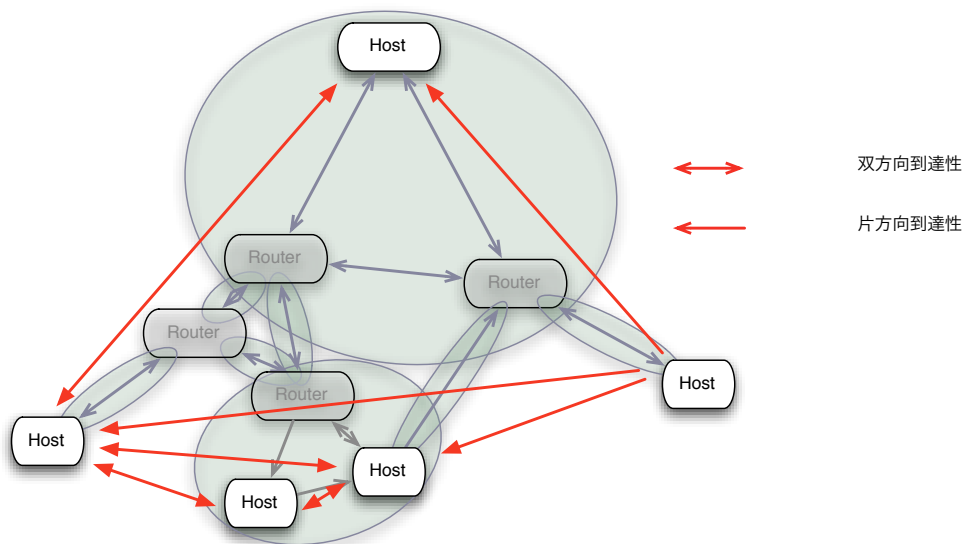


図 3.8 オーバレイアドホックネットワークモデル

図 3.8 はお互いの IP アドレスの知識が限られているホスト集合の到達関係を示している。モバイルホストがあるネットワークから別のネットワークに移動すると IP アドレスが変わるのでこの到達関係は変化する。この到達関係には双方向性、推移性も成り立たない。やはり、ホストをノード、到達関係をエッジとした時間変化する有向グラフになる。

制約がない無線リンクの問題と、非対称な到達性を持つネットワーク間のホスト移動の問題は、ホスト間の関係が時間変化する有向グラフとして扱える点で一致している。もちろん、こ

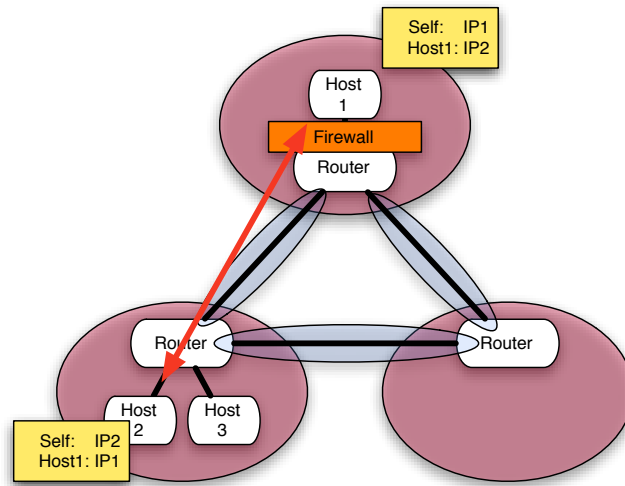


図 3.9 双方向の到達性)

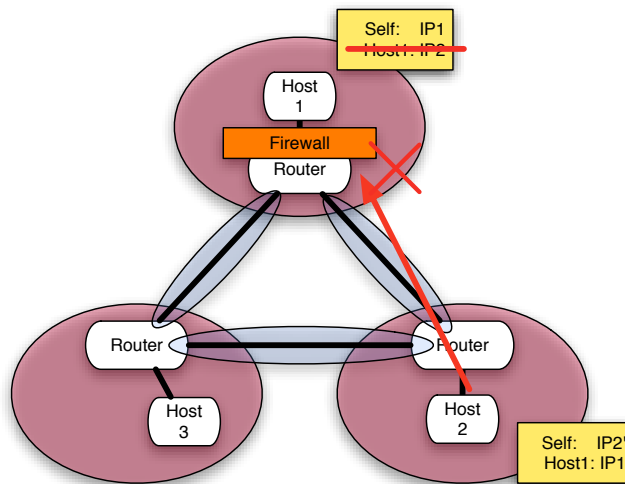


図 3.10 IP アドレス変更による到達性の喪失

のグラフの実装方法は両者で全く異なるため、同じ操作を両者にそのまま適用できる訳ではない。後の5章では両者を同じように扱うための統一インターフェースについて議論する。

図 3.9 に、ホスト 1 とホスト 2 が通信している状況を示す。ホスト 1 が接続しているネットワークにはファイアウォールが設置されている^{*1}。図 3.10 に示すように、ホスト 2 が別のネットワークに移るとホスト 2 は、移動先で、ホスト 1 が知らない新しい IP アドレスを割り当てられる。また、通信を再開するために、ホスト 2 からホスト 1 にパケットを送信してもファイアウォールのためにホスト 1 には配送されない。またホスト 1 から通信を再開しようとしても、ホスト 1 はホスト 2 の古い IP アドレスしか知らないのでできない。このような状況で通信を

^{*1} ホスト 2 からホスト 1 へはセッションを開始することはできないのでホスト 1 から開始されたはずである。

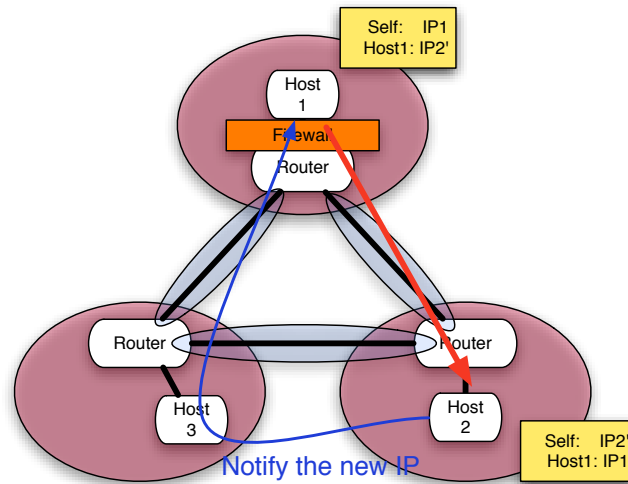


図 3.11 IP アドレス通知による到達性の回復)

再開するためには、ホスト 2 の IP アドレスを何らかの手段でホスト 1 に通知する必要がある。例えば、図 3.11 に示すように、ホスト 2 から到達できてかつホスト 1 へ到達できるような第三者ノードがあれば、そのノードを経由してホスト 1 へ新しい IP アドレスを通知し通信を再開できる。通信しているホストがどちらもファイアウォールや NAT の下に移動した場合は、第一の原因で述べた問題以外にどちらからもセッションを開始できないという問題がある。この場合は、後述する第三の原因の場合と同じように対応するか、STUN[8] サーバなどの第三者ホストの協力を必要とする。移動先のネットワークから他のホストへの、あるいは、他のホストから移動先ネットワークへの到達性がそもそもないことである。移動先のネットワークのポリシー、インターネット上の経路制御における障害などさまざまな理由により、移動先のネットワークから他のホストへ到達できないことがあり得る。この場合、モバイルホストが通信を再開するためには、モバイルホストと通信相手ホストの、どちらのホストとも通信できる第三者のホストを経由する必要がある。特に第二の原因と異なり、IP アドレスだけでなくデータパケットについても経路する必要がある。

ここで通信を再開できる条件を考える。まず、IP アドレスを知ればパケットを配送できるという潜在的な到達性をリンクとして、そのリンクを繋げたパスが双方向であることが必要である。次に、それぞれのリンクに対して宛先ホストの IP アドレスを知る必要がある。

第 4 章

モバイルシステムの課題と関連研究

2 章で既存のアプリケーションが仮定してきた従来のネットワークモデルについて述べ、3 章でモバイルホストとその間にある現実のインターネットに即した新しいネットワークモデルについて述べた。アプリケーション層のサービスの設計を妨げないという観点からは従来のネットワークモデルが望ましいが、必要な前提が厳しくモバイルホストが主要なホストになる今後のインターネットでは利用できない。一方、インターネットに対する前提を緩和したモバイルホストのネットワークモデルでは、既存のアプリケーション層のサービスが正しく動作できず、また革新的なサービスの登場を阻害する恐れもある。

本章では、本論文の取り組む課題である、モバイルホスト上に分散システムについて、理想的な従来のネットワークと実際のモバイルホストのネットワークモデルの差異という観点から議論する。また、この差異は依然として大きく、これまでの既存研究では埋められていないことを述べる。

4.1 問題

モバイルホストのネットワークモデルは時間変化する有向グラフとしてモデル化される。

このモデル上で解決しなくてはならない課題の 1 つは経路制御である。このモデル上のあるノードから別のノードへ経路が存在するか、複数の経路が存在するならどれを使うべきか、また経路をどのように探索すればいいのかという課題である。

もう一つの問題はこのモデルに基づく下位層のネットワークを上位層にどのように見せるかである。前章で述べたように既存のネットワークモデルは静的な構造を持ち、多くのアプリケーションがそのモデルを仮定している。新しいネットワークモデルの動的な面をアプリケーションに見せるとアプリケーションを変更しなければいけなくなる。分散システム上のアプリケーションにとって基本的なネットワーク操作はユニキャスト送信とマルチキャスト送信である。既存のアプリケーションをサポートするにはこの 2 つへのインターフェースの一貫性を保持する必要があると考える。

4.1.1 ユニキャストインターフェースの一貫性

前章で見たようにアプリケーションが利用する下位のインターフェースであるソケットは IP アドレスを直接指定して通信相手を決定している。また他のホストからの通信を受理した場合に取得するのも IP アドレスである。通信相手がモバイルホストであり、IP アドレスを変更したり、そのホストへの到達性が失われた場合には、このソケットを無効になる。通信を再開するためには新しい IP アドレスを取得するか、あるいは移動先のアドレスを知っている第三者ホストに中継を依頼する必要がある。このような既存のアプリケーションをモバイルホスト上でそのまま使うためには、頻繁に変化する IP アドレスの代わりにアプリケーション実行中に一貫して変わらない IP アドレスを与える必要がある。

4.1.2 マルチキャストインターフェースの一貫性

マルチキャストを利用するアプリケーションはそれほど多くないが、通信相手が一つに決まっていない場合、例えば複数のホストの中からある特性を満たすものを探索する場合や、こちらの IP アドレスを知らない未設定のホストと通信する場合には必要だである。モバイルホストの性質上、サービス発見やアドレス割当などの処理は重要度が高いため、マルチキャスト送信についても議論をすべきだと考える。データを複数のホストに同時に送るマルチキャストのためのインターフェースも影響を受ける。全てのホストが同じリンクセグメントに配置されていた場合は、リンクブロードキャストを使ってパケットをすべてのホストに配送できる。そうでない場合は、よりスコープの広いサイトスコープマルチキャストやグローバルスコープマルチキャストか、アプリケーション独自の機構を採用する必要がある。つまり、状況に関わらず一貫して使えるマルチキャストインターフェースがない。特に自動アドレス割り当てを行う Dynamic Host Configuration Protocol (DHCP) [5] などのプロトコルやサービス発見を行う Multicast Domain Name System (mDNS) [11] などのプロトコルはリンクブロードキャストやリンクローカルマルチキャストに頼っており、全てのノードが同じリンクセグメントに属していない場合は利用できない。状況に関わらずシステム内のホストの部分または全体集合に対してデータを配送するための一貫したインターフェースが必要だと考える。

4.2 既存研究

4.2.1 無線アドホックネットワーク

本研究では、??章で述べたモバイルホストのネットワークモデルのうち、接続性の特性に対応したネットワークを無線アドホックネットワークと呼ぶ。IETF の autoconf-wg で進められていた議論では、双方向性、推移性、安定性が成り立たない無線リンクへのネットワークインターフェースをセミブロードキャストインターフェースと呼び、このインターフェースを含むネットワークを Mobile Ad-hoc Network(モバイルアドホックネットワーク)と呼んでいた

[12].

無線アドホックネットワーク上の経路制御に関しては多くの研究が行われ、実際に経路制御を行うルーティングプロトコルについても開発が進められている。これらは無線通信によってできた時間変化する有向グラフ上から経路を探索する。

ここでは無線アドホックネットワーク上の経路制御を簡単にまとめる。ルーティングプロトコルはプロアクティブ型、リアクティブ型、そして両者を混合したハイブリッド型が提案されている。プロアクティブ型のルーティングプロトコルは、各ノードは常に近隣ノードとメッセージを交換し、経路表を最新の状態に保とうとする。IETF で標準化が進められている Optimized Link State Routing(OLSR) プロトコル [13]、同じく標準化が進められている Packet Building Block(PacketBB) パケットフォーマット [14] を利用して OLSR を再設計した、NeighborHood Discovery Protocol(NHDP)[15] と OLSR version 2(OLSRv2) プロトコル [16] の組み合わせが代表的ある。他にも Topology Dissemination Based on Reverse-Path Forwarding(TBRPF) プロトコル [17] や Fisheye State Routing(FSR) プロトコルなどが提案されている。ここでは詳しい説明は割愛する。

リアクティブ型のルーティングプロトコルは、その経路が必要になった時に初めてメッセージを交換して経路を構築する。IETF で標準化が進められている Dynamic Source Routing(DSR) プロトコル [18] や Ad-hoc On-demand Distant Vector(AODV) プロトコル [19]、上述した PacketBB パケットフォーマットを利用して AODV プロトコルを再設計した DYnamic MANET On-demand(DYMO) プロトコルが代表的である [20]。

ここでは DYMO プロトコルについて述べる。DYMO プロトコルの経路構築プロセスは、経路リクエスト (RREQ) メッセージの散布とそれに対する経路レスポンス (RREP) メッセージの返信という 2 つのサブプロセスからなる。

経路リクエストメッセージの散布では、送信元ノードは、送信元ノードの IP アドレスと宛先ノードの IP アドレス、ホップ数、送信元ノードが管理するシーケンス番号を含んだ RREQ メッセージをリンクローカルアドレスを使ってマルチキャストする。そのメッセージを受信したノードは送信元 IP アドレスとシーケンス番号を学習し、その送信元 IP アドレスへ経路に対する次ホップノードの IP アドレスとして、そのメッセージ送信に使われたリンクローカルユニキャストアドレス、ホップカウント、シーケンス番号を登録する。ただし、既に登録された経路のシーケンス番号と比較して RREQ メッセージのシーケンス番号が小さかった場合や既に登録された経路のホップカウントと比較して RREQ メッセージに含まれるホップカウントが大きかった場合は通知された経路が劣っているとみなし破棄する。メッセージの宛先 IP アドレスが受信ノードの IP アドレスと異なる場合は、そのメッセージのホップカウントを 1 つ増やし、再度リンクローカルマルチキャストする。メッセージの宛先 IP アドレスが受信ノードの IP アドレスと同じだった場合は経路レスポンスメッセージを送信元 IP アドレスへ向かってユニキャストする。ここまでで送信元 IP アドレスへの経路が完成していることに注意されたい。

例として、図 4.1 の接続性を持つ無線アドホックネットワークにおける、ルータ 1 からルータ 5 までの RREQ メッセージの散布を説明する。ルータ 1 が RREQ メッセージをリンクロー

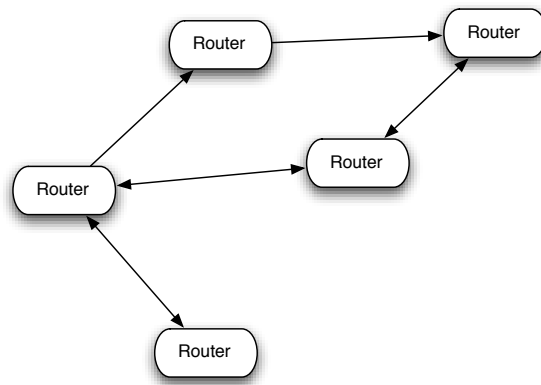


図 4.1 初期状態

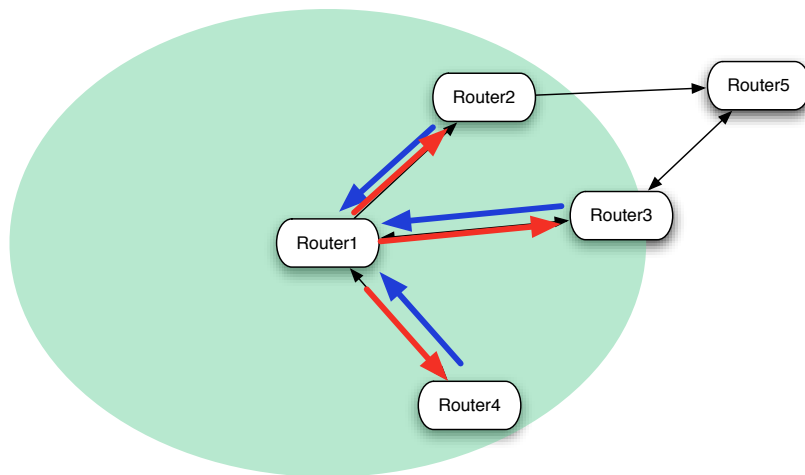


図 4.2 RREQ メッセージの散布 (a)

カルマルチキャストすると、図 4.2 の赤矢印に示すように、そのメッセージはルータ 1 の近隣のルータ 2、ルータ 3、ルータ 4 に受信される。青矢印で示すように、それぞれのルータはルータ 2 の IP アドレスへの経路を学習する。

ルータ 2、ルータ 3、ルータ 4 はそれぞれ RREQ メッセージのホップカウントを増やし、再度リンクローカルマルチキャストする。ここではルータ 3 が最初に送信したものとすると、メッセージはそれぞれ、図 4.3 の赤矢印に示すように受信される。紫の矢印もメッセージの受信を表すが、特に、シーケンス番号やホップカウントの条件によりメッセージが破棄されたことを表す。ルータ 5 は宛先ノードなので RREQ メッセージを再送せず、RREP の返信を開始する。

RREP メッセージの返信では、宛先ノードの IP アドレス、送信元ノードの IP アドレス、ホップカウント、宛先ノードが管理するシーケンス番号を含んだ RREP メッセージを宛先ノードの IP アドレスに対する経路の次ホップノードに向かってユニキャストする。ホップカウントを増やしなが RREP メッセージは RREQ メッセージと逆向きに流れていき、RREP メッ

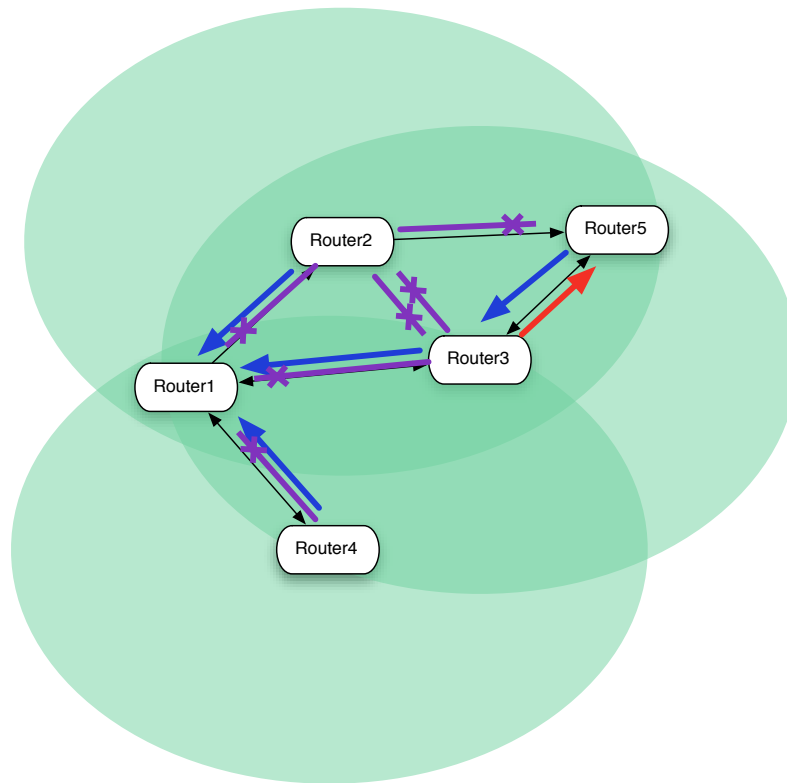


図 4.3 RREQ メッセージの散布 (b)

セージを受信したノードは宛先ノードへの経路を、RREQ メッセージの受信時と同じように登録していく。送信元ノードが RREP メッセージを受信すると送信元ノードと宛先ノード、そしてその間にある全ての中継ノードの上に、送信元ノードと宛先ノードへの経路が登録される。図 4.4 に示すように、図 4.3 の後 RREP メッセージが RREQ と逆向きに伝搬していく。RREP メッセージがルータ 1 に届くと、ルータ 1、ルータ 5、そしてルータ 3 に、ルータ 1 とルータ 5 までの経路が設定され双方向の到達性が確立されている。

最後に、ハイブリッド型のルーティングプロトコルは 2 つのアプローチを使い分けるプロトコルである。ホップ数の近いノードの経路のみプロアクティブに管理し、遠いノードについてはリアクティブに構築する Zone Routing Protocol(ZRP) はその代表である。ここでは詳しい説明は割愛する。

ネットワーク層の無線アドホックネットワークの経路制御を行った場合には、一般に各ホストには一貫したユニキャストアドレスが割り当てられる。したがって我々が問題として挙げたユニキャストインターフェースは、無線アドホックネットワーク内では問題にならない。しかし、マルチキャストのインターフェースに関しては問題が残る。従来のネットワークモデルでリンク内のホストへのマルチキャストインターフェースとして広く使われているのはリンクローカルマルチキャストである。このリンクローカルマルチキャストは無線アドホックネットワーク内では、そのモバイルホストから 1 ホップで到達できるモバイルホストへのマルチキャスト

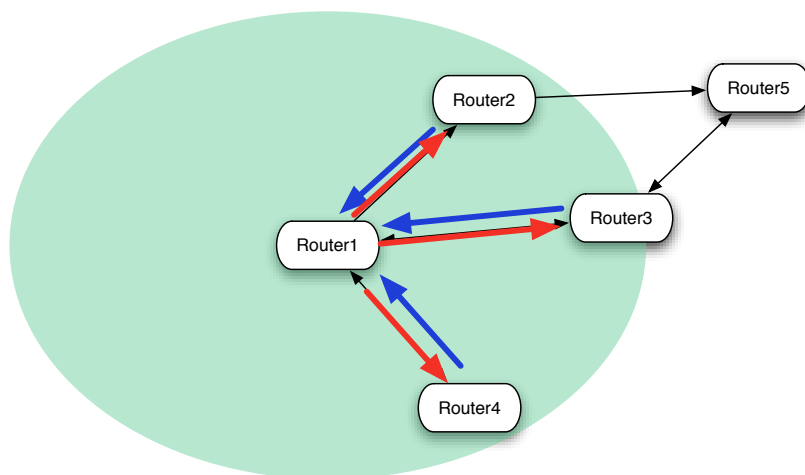


図 4.4 RREP メッセージの返信

ストという意味で使われている。このマルチキャストの通信可能範囲は、モバイルホストが移動したり、通信環境が変わったりすると変更されてしまう。またこの通信範囲はモバイルホスト上のアプリケーションからは制御できない。サイトローカルマルチキャストを利用することで SMF などが提供する無線アドホックネットワーク内のマルチキャストサービスを利用することはできるが、従来のアプリケーションの書き換えが必要なのと、ネットワークに応じてマルチキャストアドレスの変更が必要なのは望ましくない。

IEEE 802.11s プロトコルは IEEE802.11 プロトコルを拡張したプロトコルであり、マルチホップ無線ネットワークの上にフラットなイーサネットセグメントを構築するものである。現在、標準化が進められている。また IETF の autoconf-wg では MANET 上に仮想リンクを構築する提案がなされていた [21]。これらは下位層のネットワークの構成を限定している。IEEE802.11s は IEEE802.11 プロトコルに限定しているし、MANET 上の仮想リンクは MANET に限定していて、モバイルホストがネットワーク間を移動する状況については考慮していない。我々は、モバイルホストが導入した問題は IEEE802.11 や MANET に限られたものではなく、より広範囲な枠組みで解くべき問題だと考えている。

4.2.2 オーバレイネットワーク

本研究では、??章で述べたモバイルホストのネットワークモデルのうち、到達性の特性に対応したネットワークをオーバレイアドホックネットワークと呼ぶ。

モバイル IP は、条件付きのオーバレイアドホックネットワークにおける、到達性の回復を実装している。その条件とはインターネット上の全てのホストから到達可能な Home Agent(HA)と呼ばれるノードが存在することである。最初は図 4.5 に示すように、モバイルホストは HA と同じネットワークに接続しており、別のネットワークにいる Corresponding Node(CN) と通信している。CN は Mobile IP を、実装していない普通のノードであり、モバイルホストの IP

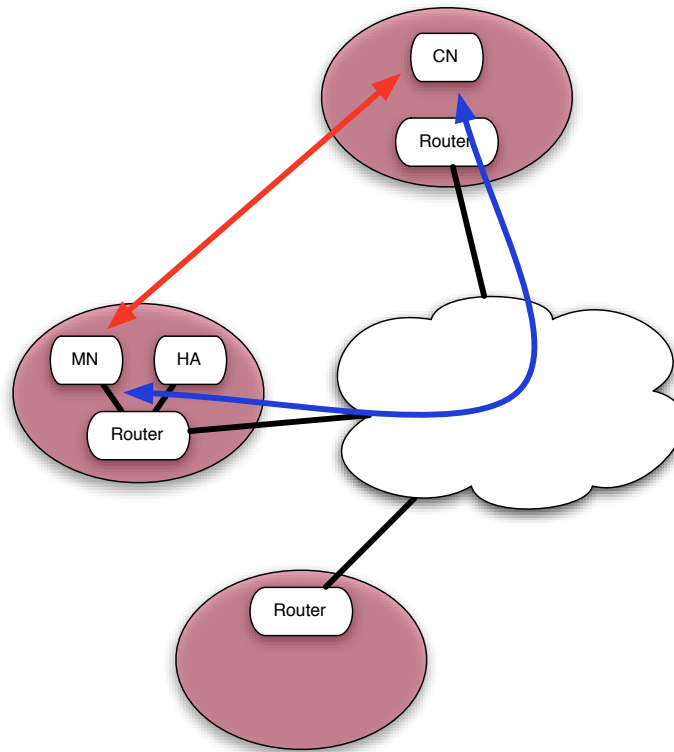


図 4.5 モバイル IP

アドレスを使ってソケットを使って通信している。赤実線はその矢印の向きに到達性があることを、青実線はその矢印の向きはモバイルホストと CN の間のデータが流れていることを示す。ある時図 4.6 に示すように、モバイルホストが HA と同じネットワークを切断して別のネットワークへ移動する。この瞬間、CN が通信を行っていた IP アドレスに対応する場所からモバイルホストがいなくなるので CN とモバイルホストの間の到達性は失われる。モバイルホストは移動先のネットワークから新しい IP アドレスを得る。モバイルホストは HA の IP アドレスを覚えているので、移動先のネットワークから HA までの下位層の到達性があると仮定すると、モバイルホストは HA への到達性を持っている。普通の IP では、モバイルホストは新しい IP アドレスを使って CN に接続し直して新しいセッションを開始しなければならないが、Mobile IP では、以下に示す手順でモバイルホストと CN の間のセッションを保存できる。図 4.7 に示すように、モバイルホストは、HA までの到達性を使って、HA に新しい IP アドレスを含む通知を行う。これにより HA はモバイルホストの新しい IP アドレスを学習するとともに、モバイルホストがそのネットワークを離れていることを知る。HA はモバイルホストの元々の IP アドレスへ送られていたパケットをモバイルホストの代わりに受信し、そのパケットをカプセル化してモバイル IP の新しい IP アドレスに向けて送信する。またモバイルホストは CN 向けのパケットをやはりカプセル化して HA に向けて送信する。このように HA というモバイルホストが元々いたネットワークにあるホストを経由して通信することで移動前と移動後で同じセッ

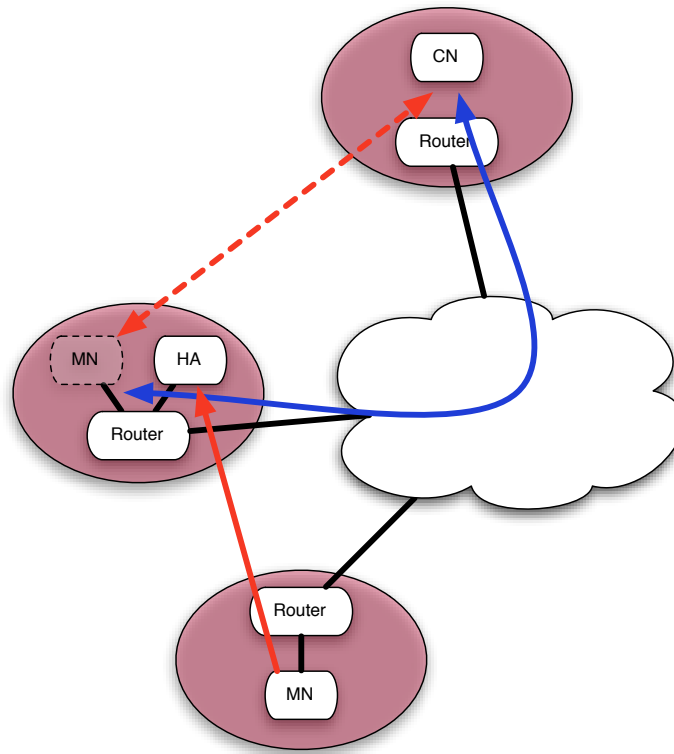


図 4.6 モバイルノードの移動

ションを維持している。

モバイルホストをサポートするために、下位層のネットワークアドレスとホストの識別子を分離するというアイデアは上述した Mobile IP(MIP)[22, 23], ROAM [24, 25], Host Identity Protocol (HIP) [26], そして Location Independent Networking for IPv6 (LIN6) [27] などでも広く利用されている。これらの手法はユニキャスト送信インターフェースの一貫性を保持しているものの、分散システム内のモバイルホスト間のブロードキャスト、マルチキャスト送信をサポートせず、したがってその一貫性に寄与しない。またこれらの手法は、MIP の HA のように、インターネットのどこからも到達できるという全体到達性を持つホストの存在を仮定している。したがって、分散システムが分断された状況などを考慮していない。

コアネットワークとエッジネットワークで利用する IP Prefix を分離するアーキテクチャ [28] も提案されている。このアーキテクチャの目的はコアネットワークで管理しなければならない IP Prefix の数を減らし、コアネットワークの管理可能性を向上させることが目的であり、エッジネットワークに接続しているモバイルホスト間の接続性をモバイルホスト自身が維持しようとする本研究の目的とは異なっている。

Virtual Private Network(VPN)[29, 30, 31, 32] は L2 フレームや L3 データグラムを他のプロトコルによってカプセル化して転送することにより遠隔のリンクやネットワークへホストを接続させる手法である。VPN によって作られた仮想リンクやポイントツーポイントリンクは、

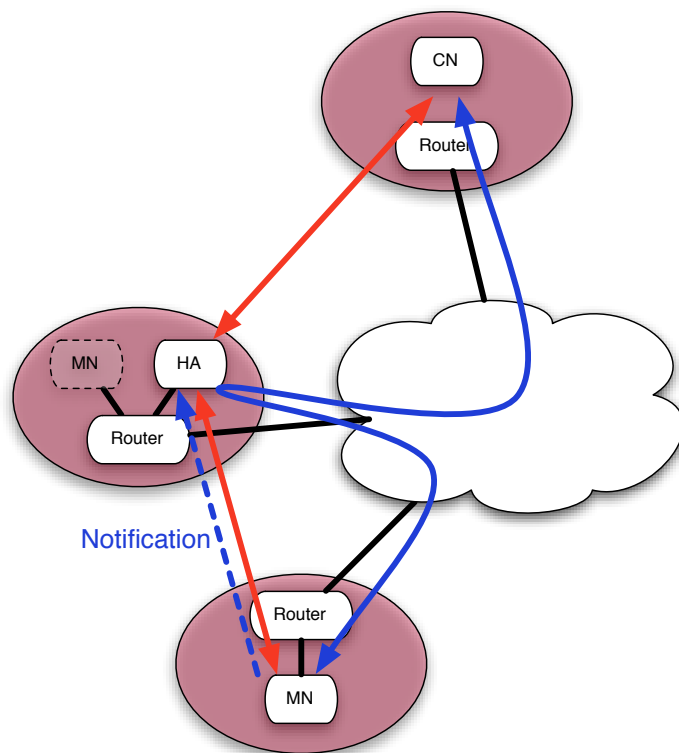


図 4.7 CoA 通知による接続性の復帰

下位層のネットワークの構成を隠蔽し、そのリンクに接続したホストは同じネットワークに見えるように見え、実際に同じリンクを共有していた場合と同じアプリケーションが利用できる。しかし、我々はそれが構築される前提、プロセスについて議論を深めている。従来の VPN は VPN サービスを提供するサービスが、MIP の HA のように、全体到達性を持つことを仮定している。我々はモバイルホストが接続しているネットワークの間に一様の到達性がない場合や、制約がない無線リンクの上のネットワークが構築されている場合について議論を行い、分散システムが分断された場合にもその上のアプリケーションの実行が続けられるようなアーキテクチャを提案する。

第5章

透過的モバイルネットワークシステムのアーキテクチャ

前章までに見てきたように、モバイルホストは現在のインターネットアーキテクチャに基づいた分散システムにさまざまな問題を与える。これまでこの問題は個々のアプリケーションが場当たり的に対応してきたが、我々は新たにこの問題に対応するコンポーネントを、図 5.1 に示すように、インターネットアーキテクチャのリンク層とネットワーク層の間に導入する。このコンポーネントをリンク補完層と呼ぶ。

リンク補完層は、従来のネットワークモデルを求めるネットワーク以上の層にブロードキャスト可能な仮想リンクを提供する。分散システム上のホストはこの仮想リンクの上に直接接続しているように見える。この仮想リンクの上ではユニキャストによって他のホストと通信できることはもちろん、マルチキャストやブロードキャストを使って、分散システム内のホスト全体へパケットを配送できる。また、一方でリンク補完層は、モバイルホストが導入した下位層の問題を解決する。前章までに述べたようにモバイルホスト間のネットワークは時間変化する

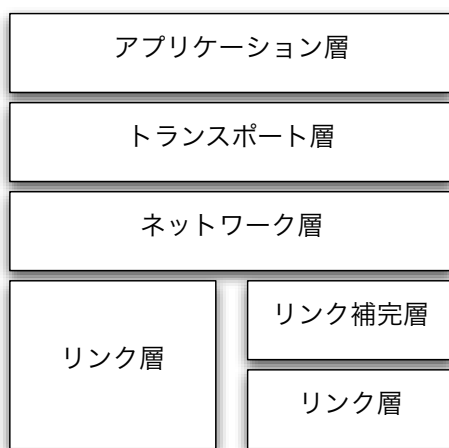


図 5.1 提案アーキテクチャ

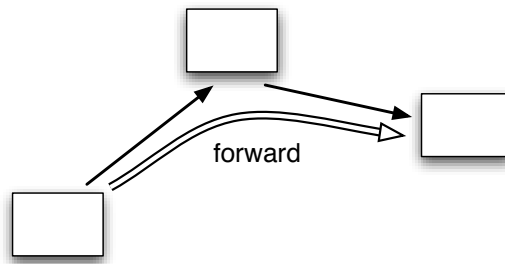


図 5.2 推移性の補完

有向グラフによってモデル化できる。リンク補完層はこのグラフの上の経路制御やパケット転送を実装する。

5.1 有向グラフ上のプロトコル

リンク補完層の役割の一つは、時間変化する有向グラフにモデル化されるモバイルホストの集合の上に、従来のネットワークモデルに合致するリンクを構築することである。従来のネットワークモデルにおけるリンクは、双方向性、推移性、安定性という特性を持っていた。本節では、リンク補完層がどのように双方向性、推移性、安定性を実現するか述べる。

推移性の補完

推移性が成り立つネットワークでは、あるホストが全てのホストへ1ホップで直接フレームを配送できる。リンク補完層では、時間変化する有向グラフの上で、フレームをホストからホストへ中継する通信パスを探索する。リンク補完層は、仮想リンクから渡された L2 フレームをカプセル化する。カプセル化された L2 フレームを探索によって発見された通信パスに沿って中継し、本来1ホップの通信では到達できないホストに配送する。カプセル化によって、L2 フレームの L2 ヘッダ、ネットワーク以上の層の情報、例えば IP ヘッダ上の TTL や Hop Count フィールドなど、は変更されないまま、L2 フレームは送信先ホストに配送される。以上の処理により、リンク補完層は推移性が成り立たない下位層のネットワークの上に推移性を実現する。

双方向性の補完

上述したように、リンク補完層が提供する経路制御機構によって L2 フレームはマルチホップ配送される。実行される経路制御はホスト対の経路を非対称な探索も可能である。つまり、あるホストから他方への経路と、他方からあるホストの経路を別々に探索できる。この場合、図 5.3 に示すように、個々のリンクが片方向の接続性しか持たない場合にも、全体として2つのホストの間に双方向の到達性を実現することは可能である。リンク補完層は双方向性を持たない下位層のネットワークの上に双方向性を実現する。上述した例は、もし下位層で片方向の到達

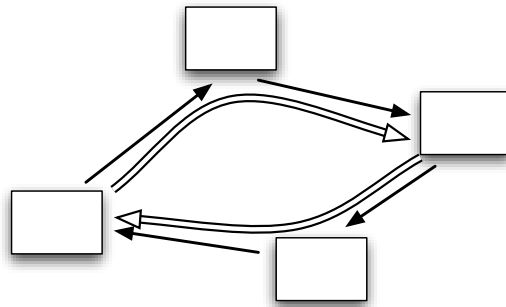


図 5.3 双方向性の補完

性しか持たないリンクを認めていなければこの2つのホストはそもそもネットワークへ参加できず通信する機会を奪われていたことに注意されたい。つまり、双方向性を前提とせずにリンク補完層が実現すべき特性にすることで、通信機会を増加しつつネットワーク以上の層に提供される特性を保持している。

安定性の補完

リンク補完層は上位層に対して仮想リンクを、仮想ネットワークインターフェースを通して、提供する。仮想ネットワークインターフェースは物理ネットワークインターフェースと独立しているため、物理ネットワークの状態に関わらず、仮に物理ネットワークインターフェースが筐体から取り外されたとしても、上位層には稼働した状態を示し続ける。もちろん物理的なネットワークインターフェースが内状態では接続性の実現はできないが、モバイルホストによるネットワークの接続や切断といった挙動をネットワーク以上の層から隠すことができる。以上の処理により、リンク補完層は実際には接続と切断を繰り返す下位層のネットワーク上に安定性を実現する。

5.2 統一インターフェース

リンク補完層の役割の一つは、ネットワーク以下の層のトポロジ特性とそれが同実装方法を分離することである。前章までに見たように、分散システムの中で、制約がない無線リンクを用いた場合とさまざまな到達性のネットワーク間をホストが移動した場合の特性は時間変化する有向グラフとしてモデル化できる。しかし、この時間変化する有向グラフは特性こそ似ているものの実際の実装は大きく異なっている。我々は、モバイルホスト上の分散システムの本質的な特性は時間変化する有向グラフであって、リンク補完層内に実装する経路制御機構やフレームの転送機構は2つ実装を差異を意識することなく同様に扱えることが望ましいと考える。

そこで2つの実装に共通するプリミティブ操作を定義する。リンク補完層はこの実装を隠蔽し抽象化された操作を介して実際のネットワークにアクセスすることで、ネットワークの実装と本質的な特性に対する処理を分離できる。ここで定義する共通するプリミティブ操作は、ユ

ユニキャスト送信操作, マルチキャスト送信操作, 受信操作である。ユニキャスト送信操作は, ホストからその近隣ホストを指定してメッセージを配送する操作である。マルチキャスト送信操作は, ホストからその全ての近隣ノードにメッセージを配送する操作である。受信操作は, ユニキャスト送信操作とマルチキャスト送信操作を問わず, 送信されたメッセージを受信し, そのメッセージの中身と送信元ホストのアドレスを返す操作である。後の第6で示すように, これら操作を使って実際の経路制御プロトコルを実装するのに十分である。

ユニキャスト送信操作の実装は, 無線アドホックネットワークとオーバレイアドホックネットワークで同じである。つまり, 指定した下位層のIPアドレスを使用してソケットでメッセージを送信する。ユニキャスト送信に関しては, ソケットは送信先のホストが無線アドホックネットワーク上なのか, オーバレイアドホックネットワークなのかを適切に隠蔽する。

一方, マルチキャスト送信操作は無線アドホックネットワークと, オーバレイアドホックネットワークで大きく異なる実装方式を持つ。無線アドホックネットワークでは, 下位層のリンク

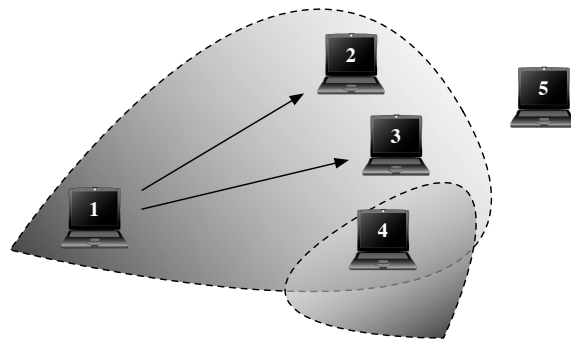


図 5.4 A multicast message delivery in a wireless ad-hoc network

ローカルマルチキャスト IP アドレスを使用してソケットでメッセージを送信する。実際にそのメッセージがどのホストに配送されるかは下位層の伝送特性に依存する。また, ホストが複数の物理ネットワークインターフェースを持っている場合には, それぞれについてマルチキャスト送信を実行する。図 5.4 に, 制限がない無線リンクを通じたマルチキャスト送信操作を示す。ホスト 1 によって送信されたメッセージは減衰しながら伝搬し, 受信ホスト周辺の電波環境に応じて受信できるかどうかが決まる。この例ではホスト 2 とホスト 3 は正しく復調され受信されたが, ホスト 4 とホスト 5 はそれぞれ干渉と減衰により正しくフレーム復調できなかった。このマルチキャスト送信操作は, 無線伝送環境が定義する伝送範囲をリンク補完層から直接アクセスさせる操作である。

オーバレイアドホックネットワークにおいて, 各ホストは分散システム内の他のホスト含んだテーブルを管理する。マルチキャスト送信操作は, このテーブルに含まれる全てのホストへ, ユニキャスト送信操作を使ってメッセージを送信する操作である。マルチキャストメッセージ配送は以下のように実装される。到達可能なホストのテーブルは後述するシグナリングプロセスによって維持管理される。

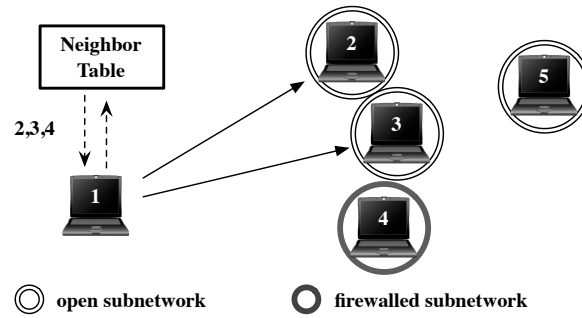


図 5.5 A multicast message delivery in an overlay ad-hoc network

図 5.5 に、オーバレイアドホックネットワークにおけるマルチキャスト送信操作を示す。ホスト 1 はテーブル内に保持していた 3 つのホストの IP アドレスに対してユニキャスト送信操作を試みた。この例の場合、ホスト 2 とホスト 3 に対して送信されたメッセージは配送されたが、属しているネットワークの入り口に設置されたファイアウォールのためホスト 4 へは配送できなかった。このマルチキャスト送信操作は、テーブルに含まれるホストのうち到達可能性を保持しているホストへアクセスさせる操作である。

オーバレイアドホックネットワークにおけるマルチキャスト送信操作のためには分散システム内の他のホストの IP アドレスを知る必要がある。この IP アドレスは手動で設定する必要はない。??章で説明したように、下位層が持つ潜在的な到達性とその時点の IP アドレスの知識が一定の条件を満たした時、その IP アドレスの知識を配布し続けることによって全体の到達性は回復する。この IP アドレスの知識を配布するプロセスを本研究ではシグナリングプロセスと呼ぶ。シグナリングプロセスでは、ユニキャスト送信操作とマルチキャスト送信操作の際に分散システム内の自分が知っている他のホストの IP アドレスをメッセージに添付する。メッセージを受信したホストはこの IP アドレスをテーブルに追加し学習する。モバイルホストは IP アドレスを変更することがあるので、定期的に各 IP アドレスの到達性を確認し到達性がないものは、無効になったものとしてテーブル内から削除する。

図 5.6 に 3 つのホストのシグナリングプロセスの例を示す。3 つのホストは元々同じネットワークに属しており、お互いの IP アドレスを共有していたものとする。図 5.6(a) に示すように、ホスト 1 とホスト 3 は、それぞれそのネットワークから新しいネットワークへ移動し、その IP アドレスを変更している。図 5.6(b) に示すように、ホスト 1 とホスト 3 が新しい通信パスを探索するためにマルチキャスト送信操作を実行すると、それらのメッセージはホスト 2 に配送され、そのメッセージからホスト 2 はホスト 1 とホスト 3 の IP アドレスを学習する。一方、ホスト 1 からホスト 3、ホスト 3 からホスト 1 へのメッセージは、お互い IP アドレスを変更したため配送されない。これにより図 5.6(c) に示すように、ホスト 1 とホスト 2、ホスト 3 とホスト 2 の間に双方向の接続性が回復している。さらに図 5.6(d) に示すように、ホスト 2 がマルチキャスト送信操作を実装すると、今学習したホスト 1 とホスト 3 の IP アドレスを添付したメッセージを、ホスト 1 とホスト 2 の両方にユニキャスト送信する。これにより、最終的にホスト 1 とホスト 3 はお互いの新しいネットワークアドレスを知り、全てのホストの間双方

向の接続性を回復する。

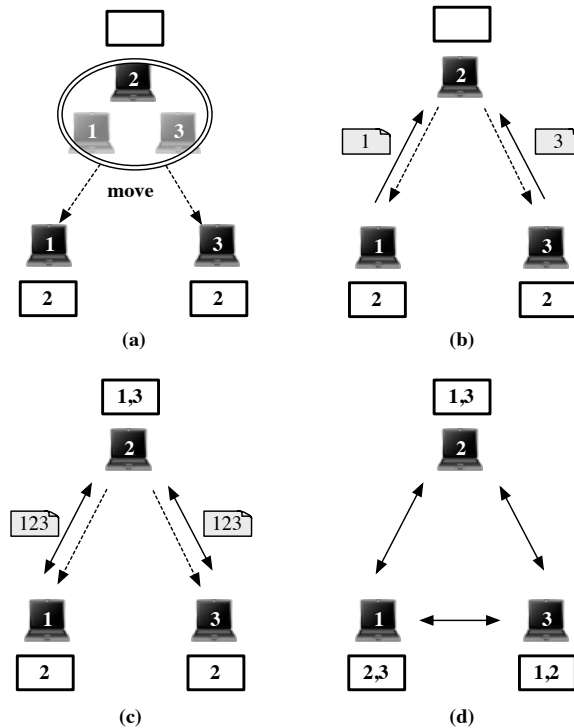


図 5.6 signaling process in overlay ad-hoc networks

オーバーレイアドホックネットワークにおけるマルチキャスト配送を行うためには近隣ホストのネットワークアドレスが必要である。ネットワークアドレスを事前に知り、そのネットワークアドレスへの到達性が提供されていない場合には、マルチキャストメッセージ配送は利用できない。一方、無線アドホックネットワークにおけるマルチキャストメッセージ配送は、事前にネットワークアドレスを知る必要がない。図 5.6(a) では、ホスト 1 とホスト 3 がホスト 2 と同じネットワークに属している間にネットワークアドレスを取得していたため、シグナリングプロセスによって到達性が復活できた。モバイル IP と異なり、ホスト 2 のような固定のホストが必須ではないということに注意されたい。つまり、ホスト 1 とホスト 3 が移動してから、各ホストがネットワークアドレスを通知して到達性を復帰させる前までに、ホスト 2 が元のネットワークに留まっていたことは必要だったが、かと言ってホスト 2 の移動を提案アーキテクチャが禁止している訳ではない。

5.3 物理リンクの性能計測

時間変化する有向グラフの上で、送信元から送信先まで複数の通信パスを発見できることがある。このような場合、通信品質を考慮して、より良い通信パスを選択できることが望ましい。しかし、時間変化する有向グラフという実際のネットワークの状態は仮想リンクによって隠蔽されているので、仮想リンクの上で実行されるアプリケーションからは通信パスの品質を計測

することはできない。

経路制御プロトコルがより良い通信パスを選択できるように、時間変化する有向グラフの上で各リンクの性能を計測するのは、リンク補完層の役割である。リンク補完層は、そのリンクの型に応じた適切なリンクの性能計測手法を実行し、その性能をメトリックとしてリンク補完層内で実行される経路制御プロトコルに渡す。経路制御プロトコルは各リンクのメトリックを積算して通信パスの評価として計算し、通算のメトリックが小さいものを最適の通信パスとして設定する。

第 6 章

共通インターフェースの実装

我々は、提案したアーキテクチャを検証するために 2 つの実装とそれらの運用を重ねてきた。前者はプロトタイプとして python 言語で実装し、特にリンクローカルマルチキャストを利用する mDNS や DHCP といった既存のアプリケーションが無線アドホックネットワーク上で利用できることを実証した [33]。後者では Click Modular Router ライブラリ [34] を利用して実装し、複数のネットワークから構成されるマルチ無線マルチチャネルメッシュネットワーク上でシームレスな接続性が提供できることを実証した [35]。

本章は特に後者の実装の詳細について述べた後、実証実験の構成やその結果について考察する。

6.1 ソフトウェアアーキテクチャ

図 6.1 に示すように、提案した透過的モバイルネットワークシステムのアーキテクチャに基づくシステムを構築した。リンク補完層はユーザ空間のミドルウェアとして実装している。このミドルウェアは、TUN/TAP デバイス [36] を使って、アプリケーションとオペレーティング

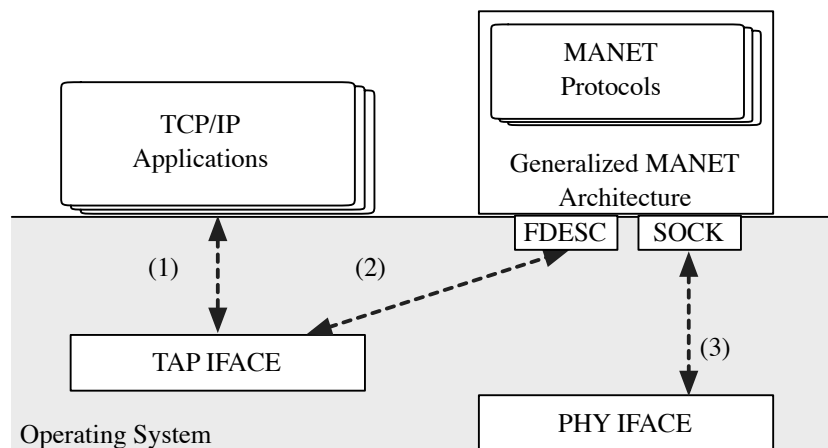


図 6.1 ミドルウェア

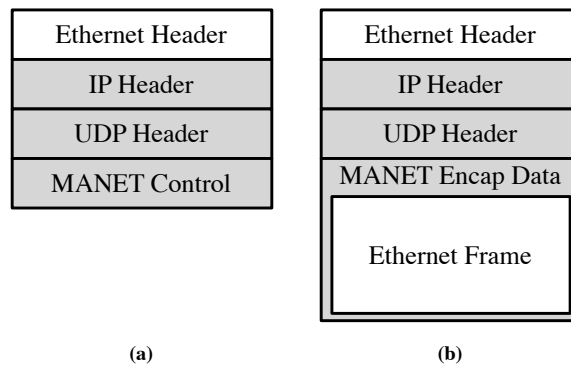


図 6.2 フレームフォーマット

システムのネットワーク処理に割り込んでいる。TUN/TAP デバイスは仮想的なネットワークデバイスの実装で、オペレーティングシステムに仮想ネットワークインターフェース、ユーザ空間のミドルウェアに対応するファイル記述子を提供する。仮想ネットワークインターフェースは、物理的なネットワークインターフェースと同様に、IP アドレスを割り振ったり、Maximum Transmission Unit(MTU) などのリンク層のパラメータを設定したり、L2 フレームの送受信をしたりできる。ただし、仮想ネットワークインターフェースから送信された L2 フレームは、実際にホストから送信される代わりにミドルウェアが開いているファイル記述子からバイト列として読み出せる。一方、ミドルウェアのファイル記述子にバイト列を書き込むと、それが L2 フレームとして仮想ネットワークインターフェースに受信される。つまり、ミドルウェアは仮想ネットワークインターフェースを介した透過型プロキシとしてアプリケーションの送受信した L2 フレーム一度全て取得する。

ミドルウェアは、図 6.2 に示すフレームフォーマットは利用して、他のホストのミドルウェアとメッセージを交換する。このフレームフォーマットは IETF で標準化が進められている PacketBB パケットフォーマット [14] を基に設計しており、図 6.2(a) に示す、経路情報の交換などに利用するコントロールフレームと、図 6.2(b) に示す、L2 フレームをカプセル化するデータフレームがある。コントロールフレームを使って近隣探索や経路探索を行い、データフレームを使ってアプリケーションから受け取った L2 フレームをカプセル化して転送する。以下ではこのフレームフォーマットを利用したユニキャスト用の経路探索の実装と、マルチキャスト用のフラッドイングの実装について述べる。

6.1.1 ユニキャストサービス

ユニキャストサービスを提供する必要がある。ミドルウェアの設計は汎用的であり特定のルーティングアルゴリズムに縛られている訳ではないが、実用的なルーティングアルゴリズムが実装可能であることを実証するために 4 章に述べた DYMO プロトコルを実装した。RREQ メッセージなど周辺の全てのノードに対する必要があるものには提案アーキテクチャのマルチキャスト送信操作を利用し、RREP メッセージなど特定のノードが受信すればよいものには

ユニキャスト送信操作を利用した、それぞれ受信操作によって各ノードが受信した時に同時に近隣ノードがメッセージを送信したノードの IP アドレスを学習し、経路表にエントリを追加する。

一般に、DYMO のようなルーティングプロトコルをオペレーティングシステム非依存な形で実装するのは難しい。DYMO はリアクティブ型のルーティングプロトコルなので、ある宛先 IP アドレスへのエントリが経路表になかった場合のみに経路探索を行う。しかし、この経路表をオペレーティングシステム内部に実装されており、経路の検索が失敗したというイベントの取得が難しく、あってもオペレーティングシステム依存の方法だからである。今回の実装は、TAP デバイスを利用してユーザ空間に実装したリンク補完層内部の経路表を参照しているためオペレーティングシステム非依存に実装されている。

6.1.2 マルチキャストサービス

ユニキャストサービスと同様に、マルチキャストサービスまたはブロードキャストサービスを提供する必要がある。Simplified Multicast Forwarding(SMF) プロトコルのフラッディングサービスを実装した^{*1}。SMF は、経路の管理を行わないプロトコルである。SMF は重複して受信したパケットの検知アルゴリズムを実装し、初めて受信したマルチキャストパケットは転送するが二度目以降の重複したパケットは転送しない。

我々の実装したミドルウェアは、L2 フレームの宛先 MAC アドレスのグループビットが立っているかどうかを調べ、立っていた場合にはマルチキャストと見なし SMF の処理へ、立っていない場合にはユニキャストと見なし DYMO の処理へ送る。

6.2 実証実験

被災建造物内の情報インフラ構築と情報収集システムの研究プロジェクトために本論文で提案するアーキテクチャを基づく無線ネットワークを実装、運用した。このプロジェクトは、被災地環境という通常のネットワークが破壊された環境において、無線アドホックネットワークの技術を応用して代替ネットワークを構築し、その上で情報収集を行うことを目的としていた。プロジェクトには、我々のようなネットワークの研究者だけでなくロボティクスの研究者も参加していた。ロボティクスの研究者は、我々が提供するネットワークを利用してその上で車輪走行するロボットを制御し、ロボットに付属するカメラや各種センサからの情報を収集する。システムそのものの構成が複雑であることはもちろん、ロボティクスの研究者というネットワークに関しては深い知識を持っていない人々に無線アドホックネットワークを利用させるという課題があった。

このプロジェクトのために我々は無線メッシュネットワークノードを設計、実装した。表 6.1 に無線メッシュネットワークノードの仕様をまとめる。i386 系の CPU を搭載した組み込み

^{*1} SMF は NeighborHood Discovery プロトコル (NHDP) の情報を利用したフラッディングの最適化も仕様には含まれているが、今回は NHDP を用いていないためその部分の実装は割愛した。

表 6.1 無線ネットワークノードの構成

CPU	AMD Geode 500[MHz]
Memory	256 [Mbyte]
Storage	Flash Memory 4[Gbyte]
NIC	Atheros Communications Inc. AR5413 802.11abg ×2
OS	Ubuntu Linux 8.04 (2.6.24-19-generic)

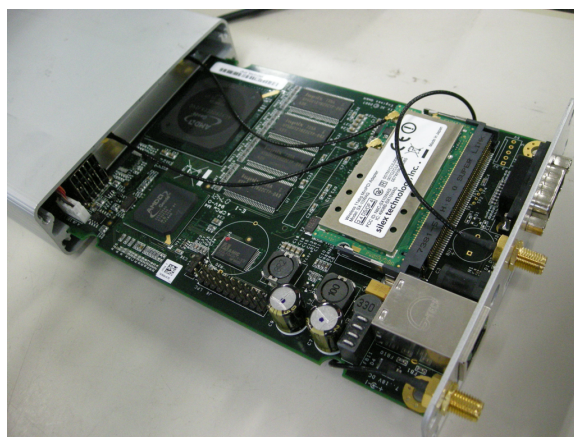


図 6.3 robohoc ノード内部表側



図 6.4 robohoc ノード内部裏側

ボード ALIX PC Engine に 4G バイトの Flash メモリを挿入し Ubuntu Linux 8.04 をインストールした。図 6.3 と図 6.4 に、メッシュネットワークノードの内部を示す。また 2 つの mini PCI スロットそれぞれに Atheros Communications Inc. AR5413 802.11abg を挿入し、それぞれに 2 つずつのアンテナを装着した。アンテナダイバーシティを利用することでフェージングに対応するためである。また USB や GPIO などの拡張ポートを利用して、ウェブカムとノードの状態を通知する LED を装着した。図 6.5 にノードの外観を示す。同様のノードを図

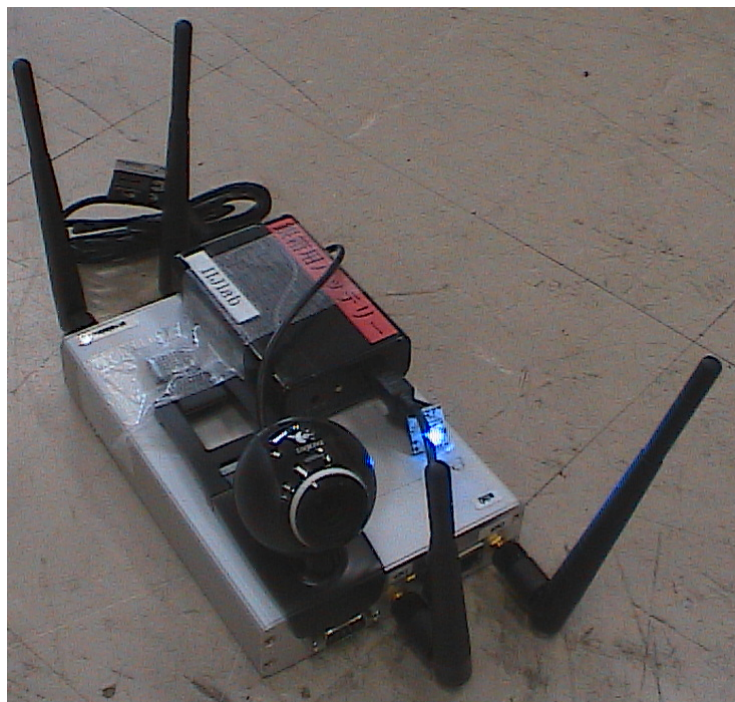


図 6.5 robohoc ノード外観

6.6 に示すロボットにも組み込んだ。

図 6.7 に示すように 1 ホップ毎に周波数帯を切り替えた。つまり、各ホストが内蔵している 2 つの無線 NIC にそれぞれ 2.4GHz 帯のチャンネルと 5GHz 帯のチャンネルを設定している。これは同じ周波数帯の最も遠いチャンネル、例えば 5GHz 帯の 32 チャンネルと 64 チャンネルに無線 NIC を設定しても、無線 NIC の間に強い干渉が見られスループットが伸びなかったためである。周波数帯を分割することで図 6.8 に示すように、オペレータが接続するメッシュネットワークルータからメッシュネットワーク上のロボット上のホストへのスループットは高い値を実現できた。これはロボット上のカメラやセンサの情報を収集し、ロボットをストレスなく制御するのに十分な性能だった。

しかし一方で、無線メッシュネットワーク中をロボットが移動する際に、ウェブカムの映像やロボットの制御を滞らせることなくチャンネルが異なる複数のネットワークの間を乗り継ぐという課題が新しく発生した。つまり、ロボットは IEEE802.11 IBSS モードと利用したネットワークの間を移動する。これはオーバレイアドホックネットワークと無線アドホックネットワークが混在したネットワークである。我々は [35] の中で、この混在ネットワークの中でシームレスな接続性を保つためのシステムを紹介した。



図 6.6 robohoc ロボット外観

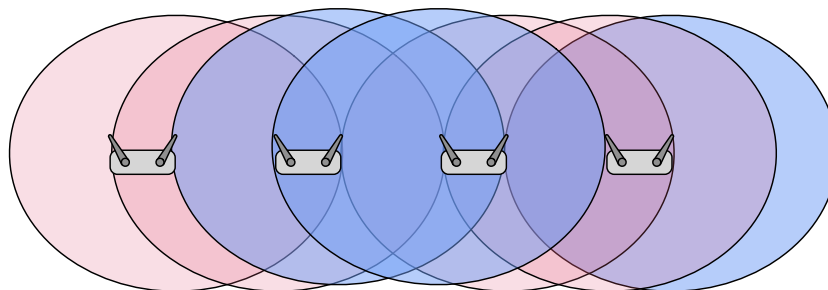


図 6.7 マルチチャネルメッシュネットワーク

第 7 章

無線リンクの品質評価の実装

第 5 章で提案したアーキテクチャでは、時間変化する有向グラフの中から最もコストの低い通信パスを選択すると述べた。適切に通信パスを選択するためには、通信パスを構成する各リンクについてあるメトリックとそのメトリックに基づく品質を得る必要がある。有線ネットワークに関しては遅延やパケットロスなどさまざまなメトリックに基づいてホスト間の通信品質を計測する手法が提案されている [37, 38, 39, 40, 41, 42, 43, 44, 45]。我々は無線ネットワーク内のリンクの品質評価に注目する。モバイルホストの 1 ホップ目のリンクは無線リンクであることが多く、また一般に、無線リンクは帯域と遅延について有線リンクより劣っているため無線リンクが分散システムの性能を制限するボトルネックリンクになりやすいためである。本論文では、無線ネットワーク中でも特に制約がない無線リンクを利用する無線アドホックネットワークについて議論する。

7.1 無線リンクの特性

まず有線リンクと比較した無線リンクの性能特性について述べる。無線リンクの、有線リンクに対する根本的な違いは伝送が開空間で行われることである。伝送路を 1 つのノードが占有できることは稀であり、一般には 2 つ以上のノードが伝送路を共有する。特に IEEE802.11bg プロトコルなどが利用する 2.4GHz の周波数帯は、Industry Science Medical(ISM) バンドと呼ばれ、多くの国で免許なく使用できるため、電子レンジなどの通信以外の機器も利用する。これらの機器は、一般に通信ノードと周波数利用について協調する術を持たないため、その周波数帯の電波を一方的に利用して無線リンクの性能に破壊的な影響を及ぼすことも少なくない。本節ではまず物理副層について述べ、無線伝送技術の原理、特に無線リンクの性能を決める電波やその上で利用される変調方式の性質についてまとめる。次に無線伝送技術に使われる開空間を複数のノードが協調しながら利用するための Media Access Control(MAC) 副層について述べ、物理副層の問題をどのように解決するか、またどのような新しい問題を導入するかまとめる。以降、本論文では具体的なプロトコルとして IEEE802.11 プロトコルを取り上げて説明する。

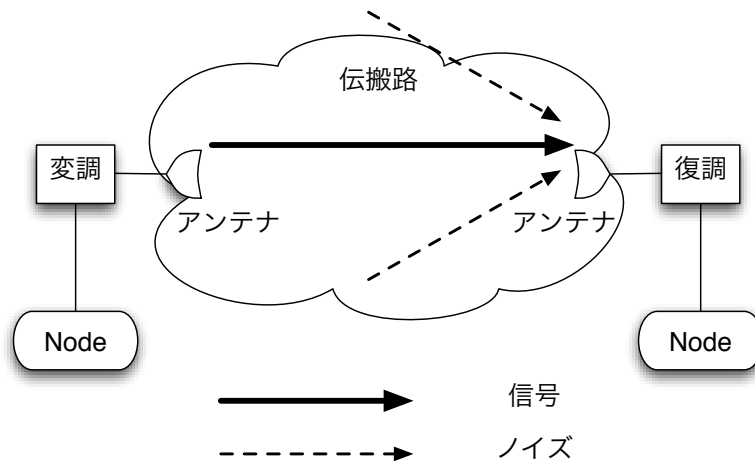


図 7.1 無線伝送

7.1.1 物理副層

物理副層では、図 7.1 に示すようにデジタル信号の伝送が行われる。伝送の手順は以下の通りである。

1. 送るべき原信号は、そのままでは電波として放出できないため、変調して搬送波に乗せる。
2. 搬送波は、アンテナによって効率良く電波のエネルギーに変換され、空間に放射される。
3. 電波のエネルギーは劣化しながら受信ノードまで伝搬する。
4. 電波のエネルギーは、受信ノードのアンテナで効率良く、搬送波に変換される。
5. 搬送波は、復調され、原信号を取り出される。

手順 1 と手順 2 は、送信ノード上で行われる処理で、主に送信ノードの設定に関連する。手順 3 は、送信ノードと受信ノードの間の伝送路に関連する。手順 4 と手順 5 は、受信ノード上で行われる処理で、受信ノードの設定と受信ノード周辺の電波環境に関連する。それぞれが複雑に関係しあって伝送が成功するかしないかを決定する。

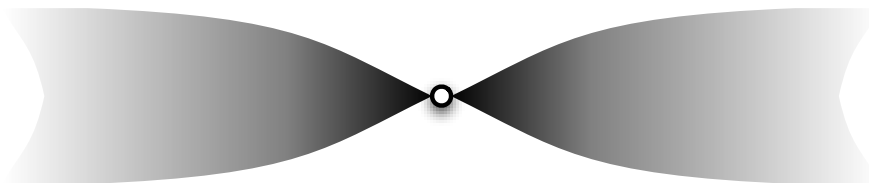


図 7.2 電波の減衰

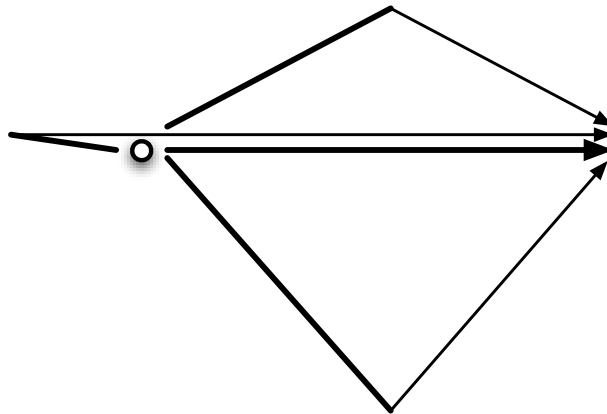


図 7.3 電波のフェージング

まず、手順 3 について述べる。電波エネルギーは減衰やフェージングという現象によって劣化する。減衰は、図 7.2 に示すように、電波の送信元から離れれば離れるほど電波エネルギーが拡散し小さくなることである。フェージングは、図 7.3 に示すように、ある電波がさまざまな伝送路を通して時間差を持って到着し干渉し合う現象である。一般に、フェージングによる効果の大きさは送信ノードと受信ノードの位置と、その間の伝送路を決める周辺環境に大きく依存する。我々は屋内であれば壁の形状や素材に応じて僅か数センチの違いで無線電波の強度、そして通信の性能が全く異なるという現象が実際に起こることを観測した。数センチの違いにより発生するフェージングを正確に理解、あるいはシミュレーション上に再現することは難しい。現在の無線ネットワークのシミュレーションには、現実のネットワークとの差異が多く残っているが、フェージングは現実ネットワークとの乖離が大きい部分だと考える。

次に手順 4 と手順 5 について述べる。受信ノードは送信ノードが放射した電波エネルギーをアンテナから受信するが、同時に他の送信ノードが放射した電波や周辺の電波雑音も受信する。受信ノードが得る搬送電波はこれらを全て重ね合わせたものになる。これにより波形が劣化しすぎると復調により原信号を取り出すことができなくなる。本論文では、減衰やフェージングによって劣化した電波が熱雑音と干渉して復調できなくなることを伝送路障害、他の送信ノードが放射した電波との干渉が原因で復調できなくなることを衝突と呼ぶ。

次に手順 1 と手順 2 について述べる。送信ノードは搬送の送信電力や変調方式を設定できる。送信電力を大きくすると搬送波の振幅が大きくなり受信側で他の電波と重ね合わせられたときに復調できることが多くなる。一方で、他のノードが送信した搬送波の波形を壊し復調できなくさせることも多い。また後述する MAC 副層では、送信パワーを大きくするとより広範囲のノードが搬送波検知するようになり、ネットワーク全体のスループットを下げることもあり得る。一般に伝送速度が高い変調方式を用いるほど、図 7.4 に示すように、変調に必要な信号強度などの条件が厳しくなり遠方のノードが復調しにくくなる。

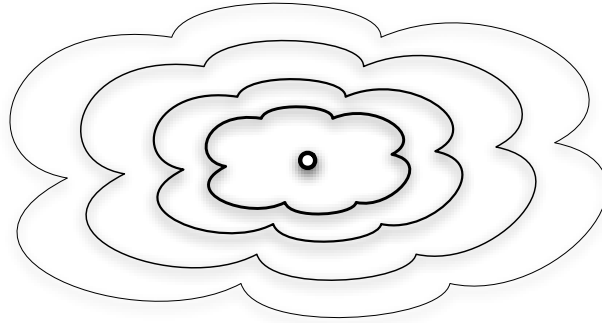


図 7.4 変調方式と通信可能距離

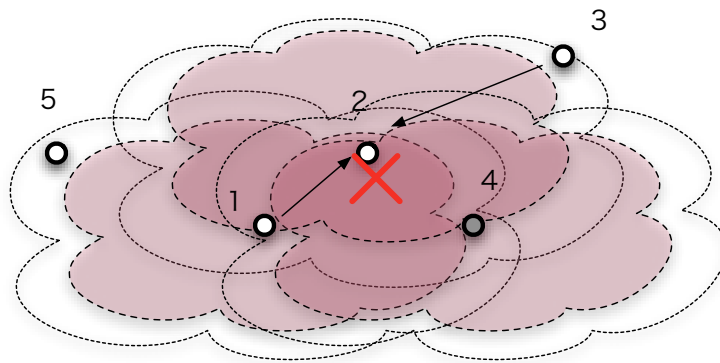


図 7.5 隠れ端末問題

7.1.2 MAC 副層

802.11 の MAC プロトコルは CSMA/CA の一種で、搬送波の検知に、物理的な搬送波の検知と仮想的な搬送波の検知の両方を用いる。各ノードは送信の前に物理的にネットワークを監視する。Distributed Interframe Space(DIFS) 時間の間に他ノードが送出した搬送波が検知されなければ、すぐフレームを送信する。検知された場合はその搬送波が終わるのを待って $(0, N]$ から乱数を生成しバックオフ数とする。Short Interframe Space(SIFS) 時間経った後は slot 時間に 1 つずつバックオフ数を減算していき 0 になったらフレームを送信する。また 802.11 では、ノードがユニキャストフレームを送信したとき、その受信ノードはすぐ Acknowledgement(ACK) フレームを返さなければいけない。に対して Acknowledgement(ACK) フレームを使って確認応答する。ACK フレームが返ってこなかった場合、送信ノードは N を 2 倍して再度バックオフ数を初期化し、もう 1 度同じフレームの送信を試みる。

802.11 プロトコルはノード間のフレームが衝突を起こさないように協調させるが、図 7.5 に示すように、実際には衝突が起こりうる。図 7.5 で色付きの枠はその中心にあるノードが伝送可能な範囲、より大きな色がない枠は搬送波が検知される範囲を図示している。初めにノード

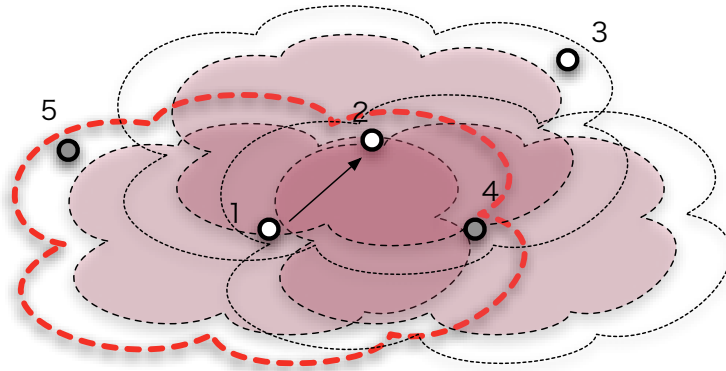


図 7.6 RTS 送信

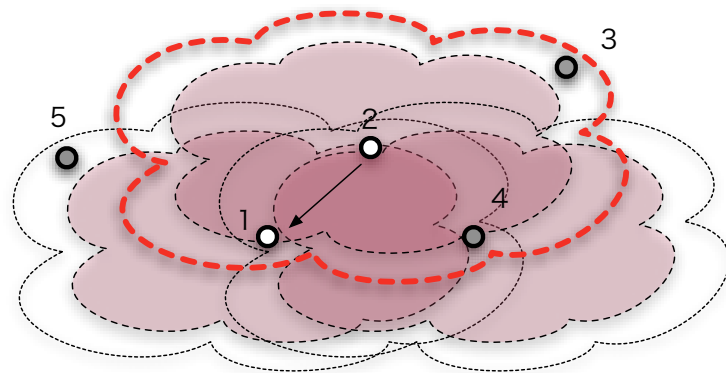


図 7.7 CTS 送信

1 がノード 2 へフレームを伝送しているものとする。ノード 3 はノード 1 から離れていてノード 1 の搬送波を検知できないため、ノード 1 が伝送を終える前に伝送を開始する。これによりノード 2 の上でノード 1 とノード 3 の搬送波が衝突してフレームの受信に失敗する。つまり、衝突という現象を回避するためには、受信ノードが他の搬送波を受けているかどうか重要であり、送信ノードからはその搬送波が検知できないことがある。この現象は隠れ端末問題と呼ばれる。

802.11 プロトコルはヘッダ内に duration というそのフレーム交換トランザクションが終わるまでの時間をマイクロ秒単位で格納している。フレームを受信したノードは、その後 duration マイクロ秒トランザクションが続くことを知りその間通信を遅らせる。この処理を実際に物理的な搬送波を検知して通信を遅らせる処理と対比して仮想的な搬送波の検知と呼ぶ。802.11 は Request To Send(RTS)/Clear To Send(CTS) という仮想的な搬送波の検知を利用した隠れ端末問題への解消する機構がある。図 7.6, 図 7.7 に示すように、RTS, CTS は送信される。赤い点線は RTS, CTS が届く範囲を、色が灰色になったノードは RTS, CTS に含まれた duration の値を読み込んで送信を送らせたノードを図示する。一般に RTS/CTS を含むブロードキャスト

トフレームは、ユニキャストフレームより低い伝送レートで送信されるため、他のフレームより遠くに届く。図 7.6 によってノード 4 とノード 5、図 7.7 によってノード 3 が duration フィールドを使った仮想的な搬送波の検知によって送信を送らせている。

しかし、RTS/CTS にも問題はある。まず RTS と CTS を送信するコストがそもそも高いといことがある。RTS と CTS は一般にデータフレームより低い伝送レートで送信されるため、フレームサイズが小さいにも関わらず送信に時間が掛かる。また RTS/CTS によって送信を遅らせる必要がないノードまで送信を遅らせてしまう。この問題はさらされ端末問題と呼ばれており、RTS と CTS に特有の問題ではないが悪化させられる問題である。以上を考慮した上で、我々のネットワークでは RTS/CTS を無効化して運用していた。

7.2 無線リンクの性能特性の観測

前節で述べた物理副層や MAC 副層内の問題は、フレームの再送やバックオフ時間の増大につながり、結果として無線リンク上の性能を低下させる。しかし、逆に無線リンクの性能低下を測定するだけではどの問題が根本原因になってそれが引き起こされたのか診断することは難しい。例えばホスト 1 からホスト 2 へユニキャストフレームを送信したが、ホスト 2 からの ACK フレームが一定時間以内に返ってこなかった場合を考える。まず、ホスト 1 からホスト 2 へのデータフレームの送信とそれともホスト 2 からホスト 1 への ACK フレームの送信のどちらが失敗したのかという問題がある。無線リンクでは 2 つの方向の伝送は非対称な性質を持つ。もしデータフレームが届いていて ACK フレームが落ちているのであれば、ホスト 1 が送信パワーを上げたり、変調方式の通信レートを下げたりしても効果はない。次に、ホスト 1 からホスト 2 へのデータフレームが落ちたとして、それがチャネル障害で落ちたのか、衝突によって落ちたのかという問題がある。チャネル障害で落ちた場合は、送信パワーを上げたり通信レートを下げたりすると波形がノイズによって壊されにくくなり、パケットの配送率が上がる可能性は高い。しかし、衝突によって落ちていた場合は効果は薄い。特に通信レートを下げた場合にはそれによりフレームの伝送時間が伸びるので、衝突する可能性を高め、配送率をより下げる可能性がある。このようにノードの設定変更によって性能低下を解消する場合、性能低下を引き起こしている根本原因の問題を特定していないと設定変更によってさらに性能が悪化することある。

したがって無線ネットワークでは単純なスループットや遅延によってリンクの評価を付けるのではなく、そのリンクと他のリンクの関係、周りにノイズ源がある可能性、その上を流れるトラフィックの量などを総合的に考慮してリンクの評価を下す必要がある。

7.2.1 既存研究

品質をどのメトリックで測るかについてもさまざまな議論がされている。有線ネットワークでも利用される、ホップカウント [46], Round Trip Time(RTT)[47] や、再送処理に注目した, Expected Transmission Count(ETX)[48], Expected Transmission Time(ETT)[49], Weighted

Cumulative ETT(WCETT)[49], さらにリンク間の干渉や負荷を考慮した, Metric of Interference and Channel-switching(MIC)[50, 51], Interference Aware Routing Metric(iAware)[52], Interference-Load Aware routing metric(ILA)[53] などが提案されている。

これまでの計測手法の課題

無線リンク品質の計測手法は大きく分けて能動的な手法と受動的な手法がある。能動的な手法は計測を行うノードがパケットを送出し、そのパケットがどのように配送されるかを評価することにより無線リンクの品質を計測する。ブロードキャストパケットを定期的に送り続ける Broadcast-based Active Probing(BAP) や Efficient and Accurate link-quality monitor(EAR)[54] などの手法が知られている。また、我々は実時間内にリンク品質を測定する手法についても議論してきた [55]。しかし、能動的な計測には計測のためにパケット送出を伴うため計測する場合としない場合でネットワークの状態が変わってしまうという根本的な問題がある。受動的な手法は計測を行うノードがパケットを送出せず、実際にネットワーク中に流れているトラフィックを観測することにより無線リンクの品質を計測する。しかし、上述したように無線アドホックネットワーク中のリンクの品質を計測するには、ネットワーク中の1点から観測してもその品質を与えている根本原因の診断ができない。したがって、無線リンク上で受動的に観測した結果をそのノード中に蓄えているだけではやはり根本原因が特定できない。これまでの受動的計測の手法は、各ノードに無線リンク以外に有線のバックボーンセグメントが接続されているテストベッド環境などを想定していた。したがって、受動的計測に留まりながらも、有線のセグメントを使って観測結果を集約し解析することが可能だった。しかし、無線アドホックネットワークは、一般に無線ネットワークなどの安定したネットワークがない状況で、代替手段として利用されるネットワークであるため、有線セグメントを仮定することは現実的ではない。

7.3 無線ネットワーク分散観測

1つのノードの視点からネットワーク中の無線リンクの品質にどの現象が作用しているのか診断することは難しい。複数のノードが連携してネットワーク中の現象を観測する手法が提案されている [56][57][58]。

上述した手法は無線ネットワークテストベッドでの利用を前提としている。つまり、ネットワークシステムに含まれるノード以外に、有線リンクで中央サーバに接続された観測専用のノードを配置し、ネットワークシステム内の状態を観測している。そもそもマルチホップ無線ネットワークを利用している理由の1つは、有線ネットワークの配線に必要なコストを排除し安価なネットワークを作ることである。この場合、ネットワークを維持管理するために新しく有線ネットワークと観測専用のノードを運用しなくてはならないとすると、元々の目的を達成できない。そこで我々は、ネットワークに参加しているノードが、ネットワークの状態を観測するために上述した手法を拡張する。

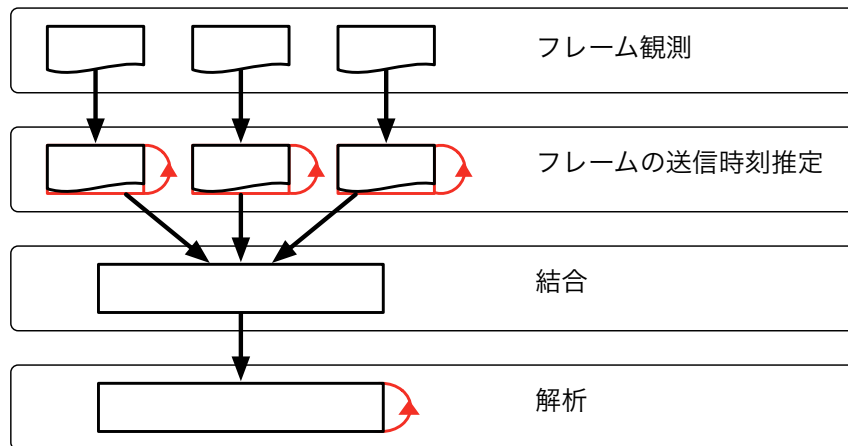


図 7.8 分散観測の概要

7.3.1 分散観測時系列データベースの作成

図 7.8 に分散観測の概要を示す。第一に、各ノードはそれぞれ無線 NIC をモニタモードに設定し、他のノードから送られた無線フレーム、自分が送った無線フレームの情報を蓄える。この蓄えられた無線フレームの中で送信フレームに関する情報は、後で述べるように、不正確な時刻が含まれているという問題がある。第二に、各ノードの収拾した無線フレームの関係に注目し、情報に推定アルゴリズムを適用し送信フレームの不正確な時刻情報を修正する。第三に、各ノードが収拾した無線フレームの集合を、一カ所に集めて結合する。各ノードが集めた無線フレームに対応付けられた時刻は、それぞれのノードの NIC 内の MAC timestamp が基になっている。したがって結合する前にこの時刻を同期する。第四に、集約された時系列データベースに対して、既存の解析アルゴリズムを適用し、無線リンクの関係性などの情報を抽出する。

分散フレームキャプチャ

一般に、無線 NIC はその MAC アドレス宛かブロードキャストアドレス宛のフレームしか受信しないが、モニタモードに設定することにより他の MAC アドレス宛のフレームとその IEEE802.11 ヘッダと radiotap ヘッダを受信できる。radiotap ヘッダに含まれるフィールドのうち Madwifi が取得するフレームに含まれるものを表 7.1 に示す。

送信フレーム時刻の推定

複数のノードで分散したフレームは、後に結合されて一つの時系列データベースにまとめる。各ノードが観測したフレームに含まれる受信時刻として MAC timestamp を使う。オペレーティングシステムが管理している時刻を利用することも考えられるが、フレームが受信されてから実際にオペレーティングシステムに通知が行われるまでに割り込み処理などのタイムラグがあるため NIC 内で管理されているクロックに基づく MAC timestamp の値の方が正確であ

MAC timestamp	NIC 内で管理される 64bit のタイムスタンプ
Flags	short preamble に対応しているか, FCS は合っていたかなどのフラグ
Rate	どのデータレートが使われているか
Channel Frequency	どの周波数が使われているか
Channel Type	どの周波数帯や変調方式が使われているか
Antenna Signal	受信信号の電波強度
Antenna Noise	ノイズの電波強度
Antenna	どのアンテナを受信に使ったか
dB antenna signal	Antenna Signal と Antenna Noise の差分
Tx Flags	送信が成功したかどうか
Data Retries	再送回数

表 7.1 Radiotap ヘッダ内の情報

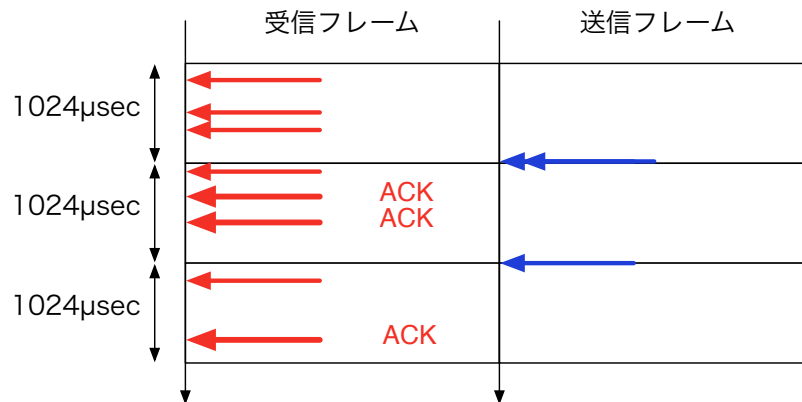


図 7.9 送信フレームと ACK フレームのペアリング

ると考えられるためである。

Atheros の IEEE802.11 のデバイスドライバである Madwifi では、ノードが送信したフレームの Radiotap ヘッダに含まれる送信時刻が正確ではない。64bit の MAC timestamp の値の下 10bit が常にクリアされた状態になっている。図 7.9 に示すように、受信フレームは時刻が正確に分かるにも関わらず、送信フレームは時刻が 1024 マイクロ秒に揃えられている。1024 マイクロ秒以内に複数の送信が行われた場合は全く同じ時刻に複数の送信フレームがあるように見える。また、この問題は Madwifi 特有の問題ではなく、他のデバイスドライバについてはそもそも MAC timestamp の値が送信フレームの Radiotap に含まれていないという状況が発生している。IEEE802.11 の送信処理は、CCA によって他のノードがチャネルを使っていないことを確認した後に、フレームを送信することになっている。この処理は数マイクロ秒の精度のリアルタイム処理が求められているため、一般にオペレーティングシステム上のスケジューリングではなく、NIC 上のリアルタイム OS 上で行われる。オペレーティングシステムがフレー

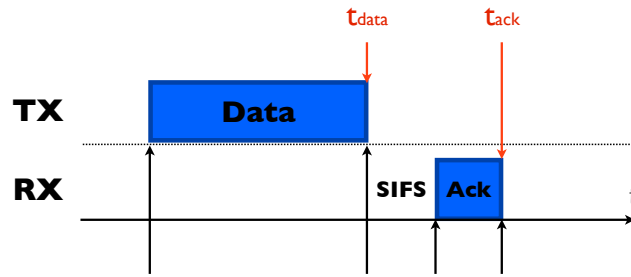


図 7.10 フレーム間間隔

ムを生成しそれを NIC に転送した後の処理は、オペレーティングシステムから検知できないため、送信フレームの MAC timestamp が不正確になる、または取得できないという状況が生じていると推定される。

本研究では、送信フレームに含まれる Radiotap ヘッダの MAC timestamp の正しい値を推定するために正しく配送されたユニキャストのデータフレームには Acknowledgement(ACK) フレームが返信されるという IEEE802.11 プロトコルの処理を利用する。IEEE802.11 では、図 7.10 に示すように、データフレームが正しく配送されると Short InterFrame Space(SIFS) の間隔を開けて ACK フレームの配送が始まる。この SIFS は周波数帯や変調方式により一意に決まる。また、データフレームや ACK フレームの配送に掛かる時間は、そのフレームの配送に使われた周波数や変調方式から導き出すことができる。したがって、あるデータフレームを送信したノードは、その送信フレームの時刻は正確ではないが、後に受信した ACK フレームの時刻は正確でありかつ ACK フレームの配送時刻からデータフレームの配送時刻が推定できる。次に式を示す。

$$T_{data} = T_{ack} - ACK \text{ の伝送時間} - SIFS \quad (7.1)$$

そのためにはデータフレームと ACK フレームを対応付けることが必要だが、ACK フレームにはデータフレームとの対応付けに十分な情報が含まれていない。1024 マイクロ秒の間隔をウィンドウと呼ぶと、1 つウィンドウ内にモニタ失敗した送信フレームや ACK フレームがある場合に対応付けができなくなる。そこで、表 7.2 に示すアルゴリズムを使い、曖昧さが残るケースを除外して送信フレームと ACK フレームを対応付けする。

アルゴリズムを解説する。あらかじめウィンドウ毎に送信フレームと受信フレーム分けており、2 行目と 3 行目でそれぞれ txs と rxs のリストに格納する。7 行目で checkdrop() 関数を使って txs 内に観測漏れが含まれていないかチェックする。IEEE802.11 のデータフレームにはインクリメントされていく sequence 番号が含まれており、sequence 番号の抜けを調べることで観測漏れがあるかないか調べられる。8 行目と 10 行目の処理で、観測抜けがあった場合には、このウィンドウについての送信フレームの送信時刻の推定を諦め、次のウィンドウに処理を移す。観測漏れがなかった場合にはさらに推定を進める。12 行目で、ACK フレームのうち


```
1: foreach window in windows:
2:   rx = getRx(window)
3:   tx = getTx(window)
4:
5:   results = []
6:
7:   dropped = checkdrop(tx)
8:   if dropped:
9:     # this tx are not used for further process
10:    continue
11:
12:   a = filter(isAck and sentTo(txmitter), rx)
13:   if len(t) == len(a):
14:     accurate.extend(zip(t, a))
15:   else:
16:     # this t are not used for further process
17:     continue
```

表 7.2 ペアリングアルゴリズム

受信 MAC アドレスが自分の MAC アドレスのものだけを抜き出す。13 行目で、観測されたデータフレームと ACK フレームの数を比べ、同じ場合は、それぞれ初めから 1 対 1 に対応させる。異なる場合は、対応を諦め、次のウィンドウに処理を進める。

このアルゴリズムにより ACK フレームとの対応付けが曖昧性を残さず決定できた送信フレームは式 7.1 を使って ACK フレームの受信時刻から正確に送信時刻が導出される。一方、曖昧性が残った送信フレームは破棄されて以降の処理には使われない。

時系列データベースの作成

送信フレーム時刻の推定を終えると、各ノードは送信時刻が正確に再設定された送信フレームと受信したフレームを合わせた送受信記録を得る。この送受信記録は単体では、性能低下を引き起こした根本原因の診断には不十分である。そこでこの送受信記録を集約、結合して、複数ノードの視点を統合した時系列データベースを作成する。

時系列データベースの結合にはいくつか問題がある。

第一に、各ノードが格納した大きな送受信記録のファイルをどのように集約するかという問題である。現在の設定では 1 フレームあたりに先頭から TCP ヘッダまでを含む 100 バイト程度を取り記録している。これまでの実験では一日パケットの送受信を収集し続けると、その記録ファイルのサイズは数 G バイトを超える。この記録ファイルを無線リンクを介して収集すると、無線ネットワーク中を伝送されるべきデータフレームの帯域を圧迫し、無線ネットワーク

の本来の目的を達成できない恐れがある。本論文では、時間をネットワーク利用者が多い運用時間帯と少ない休止時間帯に分けて、運用時間帯に収集した送受信データを、休止時間帯に集約するアプローチを取る。現在のストレージ技術であれば一日数 G の送受信記録ファイルの保存は十分許容できる範囲だと考える。このアプローチでは収集したデータをすぐにネットワーク設定に生かすことはできないが、運用時間帯の無線ネットワークの帯域圧迫を避けることができる。

第二に、各ノードがフレームの送受信時刻に使った NIC のクロックは同期されていないという問題がある。本研究では Reference Broadcast を使った時刻同期手法をベースに複数の送受信ファイルの時刻同期を行う。Reference Broadcast とは無線伝送のブロードキャスト特性によって2つ以上のノードが受信したフレームを基準に時刻同期する方法である [59]。MAC などにより制御できない遅延が発生する送信処理を時刻同期のクリティカルパスから排除し、受信時刻だけを使って時刻制御を行うことで無線ネットワーク上でも数マイクロ秒精度の正確な時刻同期を可能にする。Reference broadcast の限界は、本質的に送信ノードと2つ以上の受信ノードが必要であり、合計3つ以上のノードがないと適用できない点である。6章で説明したマルチ無線マルチチャネルメッシュネットワークでは、スループットを向上させるために1ホップ毎に異なるチャネルを異なる周波数帯から設定した。各チャネルは干渉と競合をさけるためにできるだけ少ないノードが共有するようになっており、ほとんどの場合各チャネルに2つしかノードがなく Reference Broadcast を使った時刻同期は適用できない。

我々は送信時刻推定によって、送信フレームの送信時刻を正確に推定している。また、電波は光速で伝搬するため IEEE802.11 が一般的に使われる通信範囲では伝搬遅延は無視できる。したがって我々はあるフレームの送信と受信はほぼ同時に発生すると仮定し、実際にフレームの交換を行ったノード間の送受信フレームから基準となる時刻を抽出した。この基準時刻を基に送受信記録ファイルを同期することにより、2つのノードしかなく、また不安定な無線リンクを介して無線ノード上に格納された送受信記録ファイルの時刻同期が正確に行える。

7.3.2 実証実験

図 7.11 に示すように、4つの無線ノードを用いて実証実験を行った。赤い丸は実際に無線フレームを送受信する送受信ノード、白い丸は送受信するノードを監視するだけで自らはフレームの送信を行わないモニタノードである。本章で提案した手法は送受信ノードに適用され、有線のバックボーン回線や専用のモニタがなくても十分な観測ができることを示す。モニタノードは比較のために設定している。

図 7.13 に計測結果の概要を示す。枠内の3つの数字は右から送信フレーム数、受信フレーム数、pcapによって返される保存しきれなかったフレーム数である。全ての結果で保存しきれなかったフレーム数は0である。左側の送受信ノードは送信フレーム 546、受信フレーム 2195、右側の送受信ノードは送信フレーム 417、受信フレーム 788 を記録している。左側のモニタノードは受信フレーム 5431、右側のモニタノードは受信フレーム 3651 を記録している。

推定アルゴリズムを適用した結果、左の送受信ノードは 546 個のフレーム中 474 個について

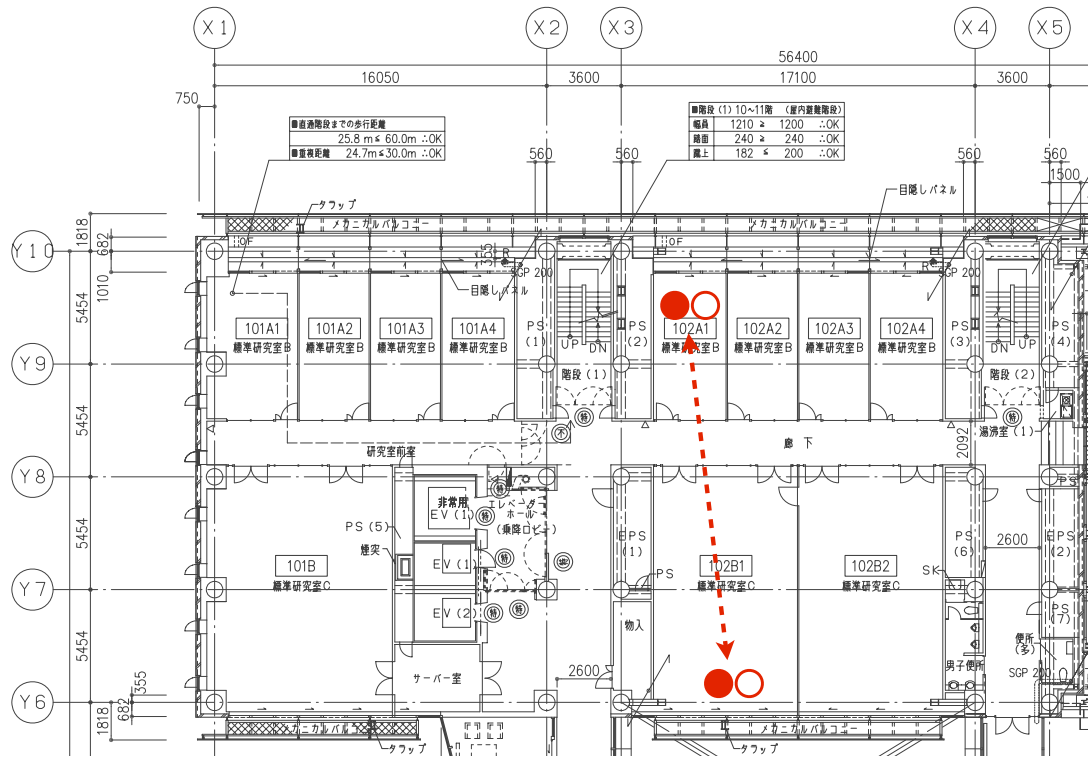


図 7.11 実験環境

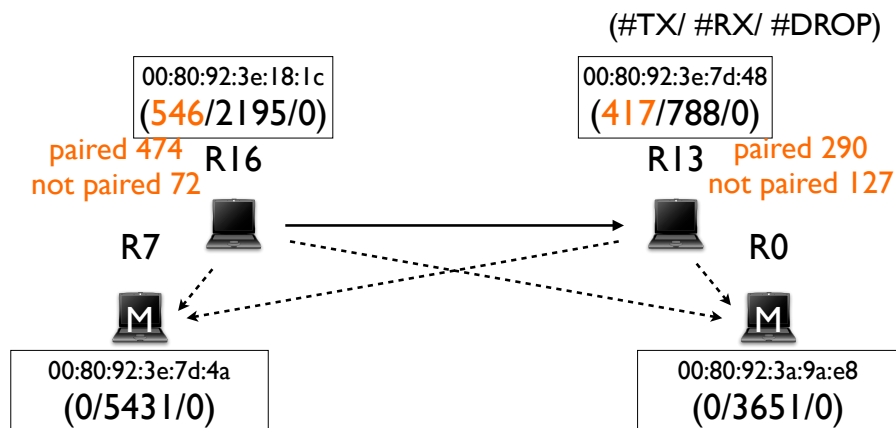


図 7.12 計測結果

曖昧性なく ACK フレームと対応付け、送信時刻を推定している。右の送受信ノードは 417 個中 290 個である。送信時刻が正確になった送信フレームを基準として記録ファイルの時刻同期、結合を行うと、送受信ノードの組は 3273 個のフレームを得た。一方モニタノードは 5904 個である。

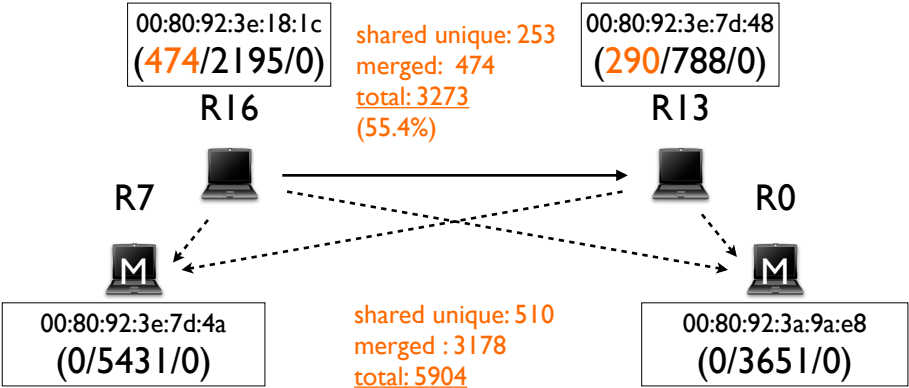


図 7.13 送信時刻推定と結合適用後の結果

第 8 章

議論

本研究では、透過的モバイルネットワークシステムのアーキテクチャを提案した。モバイルホストの上の分散システムを構築するためのアーキテクチャ設計の選択肢は広く、これまではその中の一部についてしか議論をしてこなかった。ここでは、我々が選択した選択肢とそれ以外の選択肢について比較を行う。

本節では、アプリケーション層に提供されるインターフェースに関する設計についての選択肢について議論する。本論文では、我々はブロードキャスト可能な仮想リンクをネットワーク以上の層に提供するアプローチを取った。分散システム内のホストは、同一のネットワークブリフィックスが割り当てられ、全て仮想リンク上にオンリンクに見える。これには 2 つのメリットがある。第一に、リンクローカルマルチキャストアドレスを使ったマルチキャスト通信が可能である。これにより mDNS や DHCP のような有用なアプリケーションをそのままモバイルホスト上で利用できる。第二に、下位層の到達性の変化に適応する機能の適用範囲を指定しやすいことである。到達性の変化に対応するためには、リンク品質の評価、経路探索、その他の処理が必要であり、これらの処理を実行するためには、計算資源、メモリ資源、ネットワーク帯域資源などのコストを支払うことになる。したがって、これらの処理はそれを必要とするアプリケーションに範囲を絞って適用できることが望ましい。

例えば、最近のインターネット上のアプリケーションは、HTTP を用いた WEB アプリケーションが主流になっている。サーバ側に情報を集約している WEB アプリケーションは、アプリケーションレベルでセッション管理や認証管理を行うことが一般的である。この場合、モバイルホストの IP アドレスが切り替わることはもちろん、クライアントの端末自体が切り替わることも問題にならない。このようにアプリケーション層で認証やセッション管理の問題が既に扱われている場合は、問題をネットワーク以下の層で解決しても新たにコストだけが導入されることになる。

モバイル IP を用いた場合、モバイルノードには MA と CoA の両方の IP アドレスが割り当てられることになる。MA をソースアドレスとして用いた場合には、同じ IP アドレスをどこにいても利用できるという移動透過性の効果を得られ、同時に移動透過性を実現するためのコストを支払うことになる。一方、CoA をソースアドレスとして用いた場合には、IP アドレスは変化するがコストを支払う必要はない。したがって、利用するアプリケーションの性質に応じて

2 種類のソース IP アドレスを変更できることが望ましい。これまで提案されている手法では、アプリケーション内部でソースアドレスを指定するか、宛先 IP アドレスのプリフィックス毎にオペレーティングシステムのポリシーテーブルを編集しソース IP アドレスを指定する必要がある。一方、我々の手法では、仮想リンク上に割り当てられた IP アドレスに対してのみ、仮想ネットワークインターフェースとミドルウェアを介した通信が行われるので、適用範囲は分散システム内部に絞られている。

ネットワーク以下の層で接続性と到達性の課題を解決した場合、変更したリンクとパスの品質は変化する。現状では、トランスポート層に対して品質の変化を通知する方法がないため、トランスポート層内に実装された輻輳制御に問題が生じる可能性がある。この問題は既に Mobile IP のコンテキストで議論されている。しかし、本研究のアプローチでは、経路の変化がトランスポート層プロトコルを実行するエンドのホストを含まない形で起こりうるため、ホストが経路の変化を直接検知してトランスポート層に働きかけるアプローチの適用できない。

仮想リンクと別のアプローチとして名前志向ソケットがある [60]。本研究のように下位層とアプリケーション層が使う識別子を分けるために新しい階層を追加する代わりに、既にある名前と IP アドレスという 2 つの識別子を利用して問題を解決する手法である。本研究のアプローチと異なり、現在、一般的な IP 志向のソケットを使って記述されているアプリケーションを書き換える必要がある。確かにアプリケーションの書き換えコストは高く付くが、アプリケーションの書き換えを嫌うあまり現実には即していない従来のインターフェースを使い続けることもコストを払い続けていることになる。名前志向ソケットの様にどこかで互換性を諦める必要もあると考える。

第9章

結び

本論文では透過的モバイルネットワークシステムのアーキテクチャを提案した。このアーキテクチャの目的は、今後増えるだろうモバイルホストの上に分散システムを構築、運用における課題を解決することだった。我々は、オーバレイアドホックネットワークと無線アドホックネットワークという、実装が異なる2種類のネットワークから共通する特性を抜き出した。ホスト間の到達性が時間変化する有向グラフとして扱えるという特性である。次にこのグラフの上に統一インターフェースとして、ユニキャスト送信操作とマルチキャスト送信操作と受信操作を定義し、実装の異なる2つのネットワークに同じ操作が適用できるようにした。そして、この統一インターフェースの上に、ブロードキャスト送信可能な仮想リンクを作成し、分散システム内のホストがオンリンクに見えるようにすることで、一貫したユニキャストIPアドレスと、リンクローカルマルチキャストIPアドレスを使った既存のアプリケーションをそのまま実行できるようにした。

以下に本論文の貢献をまとめる。本論文の貢献は以下の通りである。第一に、モバイルホストが到達性に制限があるネットワーク間を移動した場合の問題と無線アドホックネットワークの問題から、時間変化する有向グラフ上の経路制御という本質的な問題を抽出して解決した。これにより、両者とその混合ネットワーク上の到達性の問題を統一的に解決した。第二に、移動透過性を扱った既存研究がモバイルホスト、あるいは Mobile IP の Home Agent のような中継ノードに安定した到達性があることを仮定していたのに対し、本論文では到達性に制限があるネットワーク間をモバイルホストが移動した場合の問題を扱って応用範囲を広げた。また、モバイルホストが協調して経路制御と中継を行った場合にモバイルホスト内の到達性を回復できる条件を明らかにした。第三に、モバイルホストによって通信リンクの設計の自由度が上がっても従来通りの一貫したインターフェースを提供できることを示した。最後に提案したアーキテクチャに基づくシステムの実装し、実際のシステム内での運用に基づく考察を行った。その過程で無線アドホックネットワークの運用上の問題解決に役立つ分散観測手法を提案し、その動作を実証した。モバイルホストが主要なホストになる将来のインターネットにおいて重要なこれらの貢献によって、我々は将来のインターネットアーキテクチャが取るべき設計指針を示した。

謝辞

修士課程の2年間と博士課程の4年間、計6年間に渡ってご指導頂いた東京大学大学院 情報理工学研究科の江崎 浩教授に深く感謝致します。

江崎研究室の皆様へ感謝致します。研究補助員として働かせて頂いていた IIJ 技術研究所の皆様へ感謝致します。WIDE プロジェクトの皆様へ感謝致します。

最後に、満利子と結へ、いつも支えてくれて有り難う。

参考文献

- [1] 情報通信政策局. 平成 19 年 通信利用動向調査報告書. Technical report, 総務省, 2007.
- [2] D. Thaler. Multi-Link Subnet Issues. *Network Working Group RFC 4903*, May 2007.
- [3] B. Carpenter. Architectural Principles of the Internet. *Network Working Group RFC 1958*, June 1996.
- [4] B. Aboba and E. Davies. Reflections on Internet Transparency. *Network Working Group RFC 4924*, July 2007.
- [5] R. Droms. Dynamic Host Configuration Protocol. *Network Working Group RFC 2131*, March 1997.
- [6] W. Simpson. The Point-to-Point Protocol (PPP). *Network Working Group*, July 1994.
- [7] F. Audet and C. Jennings. Network Address Translation (NAT) Behavioral Requirements for Unicast UDP. *Network Working Group RFC 4787*, January 2007.
- [8] J. Rosenberg and R. Mahy and P. Matthews and D. Wing. Session Traversal Utilities for NAT (STUN). *Network Working Group RFC 5389*, October 2008.
- [9] T. Nishitani and I. Yamagata and S. Miyakawa and A. Nakagawa and H. Ashida. Common Functions of Large Scale NAT (LSN). *Work in Progress*, November 2009.
- [10] D Andersen, H Balakrishnan, and F Kaashoek. Resilient overlay networks. *Proceedings of the ...*, Jan 2001. 内容が濃い.
- [11] Stuart Cheshire and Marc Krochmal. Multicast DNS. *Working in Progress*, September 2008. draft-cheshire-dnsext-multicastdns-07.txt.
- [12] I. Chakeres, J. Macker, and T. Clausen. Mobile Ad hoc Network Architecture. *Work in Progress*, November 2007. draft-ietf-autoconf-manetarch-07.
- [13] T. Clausen and P. Jacquet. Optimized Link State Routing Protocol (OLSR). *Network Working Group RFC 3626*, October 2003.
- [14] T. Clausen and C. Dearlove and J. Dean and C. Adjih. Generalized Mobile Ad Hoc Network (MANET) Packet/Message Format. *Network Working Group RFC 5444*, February 2009.
- [15] T. Clausen and C. Dearlove and J. Dean and The OLSRv2 Design Team. Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP). *Work in Progress*, October 2009. draft-ietf-manet-nhdp-11.

- [16] T. Clausen and C. Dearlove and P. Jacque and The OLSRv2 Design Team. The Optimized Link State Routing Protocol version 2. *Work in Progress*, September 2009. draft-ietf-manet-olsrv2-10.
- [17] R. Ogier and F. Templin and M. Lewis. Topology Dissemination Based on Reverse-Path Forwarding (TBRPF). *Network Working Group RFC 3684*, February 2004.
- [18] D. Johnson and Y. Hu and D. Maltz. The dynamic source routing protocol (dsr) for mobile ad hoc networks for ipv4. *Network Working Group RFC 4728*, February 2007.
- [19] C. Perkins and E. Belding-Royer and S. Das. Ad hoc On-Demand Distance Vector (AODV) Routing. *Network Working Group RFC 3561*, July 2003.
- [20] I. Chakeres and C. Perkins. Dynamic MANET On-demand (DYMO) Routing. *Work in Progress*, February 2008. draft-ietf-manet-dymo-12.
- [21] F. Templin. MANET Autoconfiguration over Virtual Ethernets. *Work in Progress*, February 2007. draft-templin-autoconf-virtual-00.
- [22] C. Perkins. IP Mobility Support for IPv4. *Network Working Group RFC 3344*, August 2002.
- [23] D. Johnson and C. Perkins and J. Arkko. Mobility Support in IPv6. *Network Working Group RFC 3775*, June 2004.
- [24] Ion Stoica, Daniel Adkins, Shelley Zhuang, Scott Shenker, and Sonesh Surana. Internet Indirection Infrastructure. In *ACM SIGCOMM*, 2002.
- [25] Shelley Zhuang, Kevin Lai, Ion Stoica, Randy Katz, and Scott Shenker. Host Mobility Using an Internet Indirection Infrastructure. In *ACM/USENIX Mobisys*, 2003.
- [26] R. Moskowitz and P. Nikander and P. Jokela and T. Henderson. Host Identity Protocol. *Network Working Group RFC 5201*, April 2008.
- [27] Mitsunobu Kunishi, Masahiro Ishiyama, Keisuke Uehara, Hiroshi Esaki, and Fumio Teraoka. LIN6: A New Approach to Mobility Support in IPv6. In *International Symposium on Wireless Personal Multimedia Communications*, September 2001.
- [28] Dan Jen, Michael Meisel, Land Wang, Beichuan Zhang, and Lixia Zhang. Towards A New Internet Routing Architecture: Arguments for Separating Edges from Transit Core. In *ACM Workshop on Hot Topics in Networks*, October 2008.
- [29] K. Hamzeh and G. Pall and W. Verthein and J. Taarud and W. Little and G. Zorn. Point-to-Point Tunneling Protocol (PPTP). *Network Working Group RFC 2637*, July 1999.
- [30] W. Townsley and A. Valencia and A. Rubens and G. Pall and G. Zorn and B. Palter. Layer Two Tunneling Protocol "L2TP". *Network Working Group RFC 2661*, August 1999.
- [31] Yoshiaki Tobioka, Nodoka Mimura, Hiroyuki Morikawa, and Tomonori Aoyama. Mynetspace:a user controlled virtual closed network for flexible access control. In

- IEICE Tech. Rep.*, pp. 139–144, March 2005.
- [32] Shin Miyakawa, Satoshi Ono, Takuro Kubo, Kazuyuki Terao, and Katsuyuki Hasebe. Yet Another Mobility Support for the Internet. *IEIEC Transactions on Information and Systems*, Vol. E82-D, No. 4, pp. 778–783, April 1999.
- [33] Sho Fujita and Hiroshi Esaki. ATMOS: A middleware for Transparent MOBILE ad-hoc networking Systems. In *International Conference on Ubiquitous Information Management and Communication*, January 2009.
- [34] E Kohler, R Morris, B Chen, and J Jannotti. The click modular router. *ACM Transactions on ...*, Jan 2000.
- [35] Sho Fujita, Tadashi Yasumoto, Hiroshi Esaki. On Seamless Connectivity over Multi-Radio and Multi-Channel Wireless Mesh Networks. In *ACM CoNEXT Student Workshop*, December 2008.
- [36] VTun Project. <http://vtun.sourceforge.net/>.
- [37] A. Tachibana, S. Ano, T. Hasegawa, M. Tsuru, and Y. Oie. Locating Congested Segments over the Internet Based on Multiple End-to-End Path Measurements. *IEICE Trans. Commun.*, Vol. E89-B, pp. 1099–1109, April 2006.
- [38] John W. Byers. Inference and labeling of metric-induced network topologies. *IEEE Trans. Parallel Distrib. Syst.*, Vol. 16, No. 11, pp. 1053–1065, 2005. Member-Azer Bestavros and Member-Khaled A. Harfoush.
- [39] 藤井資子, 山本正晃, 永見健一, 菊池豊, 中川郁夫. インターネットにおける通信品質の地域間格差調査—インターネットの一極集中構造がもたらす通信品質デバイド—. *情報社会学会誌*, Vol. 3, No. 1, pp. 13–22, June 2008.
- [40] K. Papagiannaki, S. Moon, C. Fraleigh, P. Thiran, and C. Diot. Measurement and analysis of single-hop delay on an IP backbone network. In *IEEE Journal on Selected Areas in Communications*, Vol. 21, pp. 908–921, 2003.
- [41] Neil Spring, Ratul Mahajan, David Wetherall, and Thomas Anderson. Measuring ISP topologies with rocketfuel. *IEEE/ACM Trans. Netw.*, Vol. 12, No. 1, pp. 2–16, 2004.
- [42] Mark Coates, Rui Castro, Robert Nowak, Manik Gadhiok, Ryan King, and Yolanda Tsang. Maximum likelihood network topology identification from edge-based unicast measurements. *SIGMETRICS Perform. Eval. Rev.*, Vol. 30, No. 1, pp. 11–20, 2002.
- [43] Michael Rabbat, Mark Coates, and Robert D. Nowak. Multiple-Source Internet Tomography. *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 12, pp. 2221–2234, 2006.
- [44] A. Coates, Hero, R. Nowak, and Bin Yu. Internet tomography. *Signal Processing Magazine, IEEE*, Vol. 19, No. 3, pp. 47–65, 2002.
- [45] 吉田薫. 品質計測・分析に基づいた
選択的ルーティングアーキテクチャに関する研究. PhD thesis, 東京大学大学院情報理工

- 学系研究科, 2008.
- [46] DB Johnson and DA Maltz. Dynamic source routing in ad hoc wireless networks. *KLUWER INTERNATIONAL SERIES IN ENGINEERING AND COMPUTER SCIENCE*, pp. 153–179, 1996.
 - [47] A Adya, P Bahl, J Padhye, A Wolman, and L Zhou. A multi-radio unification protocol for ieee 802.11 wireless networks. *IEEE Broadnets*, pp. 344–354, 2004.
 - [48] DSJD Couto, D Aguayo, J Bicket, and R Morris. A high-throughput path metric for multi-hop wireless routing. *Wireless Netw*, Vol. 11, No. 4, pp. 419–434, 2005.
 - [49] R Draves, J Padhye, and B Zill. Routing in multi-radio, multi-hop wireless mesh networks. *Proceedings of the 10th annual international conference on Mobile computing and networking*, p. 128, 2004.
 - [50] Y Yang, J Wang, and R Kravets. Interference-aware load balancing for multihop wireless networks. *University of Illinois at Urbana-Champaign*, Jan 2005.
 - [51] Y Yang, J Wang, and R Kravets. Designing routing metrics for mesh networks. *IEEE Workshop on Wireless Mesh Networks* (... , Jan 2005.
 - [52] A Subramanian, M Buddhikot, and S Miller. Interference aware routing in multi-radio wireless mesh networks. ... *on Wireless Mesh Networks* (... , Jan 2006.
 - [53] D Manikantan Shila and T Anjali. Load aware traffic engineering for mesh networks. *Computer Communications*, Jan 2008.
 - [54] KH Kim and KG Shin. On accurate measurement of link quality in multi-hop wireless mesh networks. *Proceedings of the 12th annual international conference on Mobile computing and networking*, p. 49, 2006.
 - [55] 安本直史. マルチホップ無線メッシュネットワークにおけるリアルタイム性を考慮した品質評価手法の提案と実装. Master's thesis, 東京大学大学院情報理工学系研究科, 2008.
 - [56] A Sheth, C Doerr, D Grunwald, R Han, and D Sicker. Mojo: A distributed physical layer anomaly detection system for 802.11 wlans. *Proceedings of the 4th international conference on Mobile systems, applications and services*, pp. 191–204, 2006.
 - [57] YC Cheng, J Bellardo, P Benkö, AC Snoeren, GM Voelker, and S Savage. Jigsaw: Solving the puzzle of enterprise 802.11 analysis. *Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications*, Vol. 36, No. 4, pp. 39–50, 2006.
 - [58] YC Cheng, P Verkaik, P Benkö, J Chiang, AC Snoeren, S Savage, and GM Voelker. Automating cross-layer diagnosis of enterprise wireless networks. 2007.
 - [59] J Elson, L Girod, and D Estrin. Fine-grained network time synchronization using reference broadcasts. *ACM SIGOPS Operating Systems Review*, Vol. 36, pp. 147–163, 2002.
 - [60] C Vogt. Simplifying internet applications development with a name-oriented sockets

.... *christianvogt.mailup.net*.

本研究に関する発表論文

査読付き論文は以下である。

- Sho Fujita, Keiichi Shima, Yojiro Uo, Hiroshi Esaki, "A Decentralized VPN Service over Generalized Mobile Ad-Hoc Networks", IEICE, Vol. J92-D, No. 10, pp. 1897-1904, October, 2009

その他の査読付き論文は以下である。

- Sho Fujita, Hiroshi Esaki, "ATMOS: A middleware for Transparent MOBILE ad-hoc networking Systems", the 3rd International Conference on Ubiquitous Information Management and Communication (ICUIMC 2009), January, 2009
- Sho Fujita, Tadashi Yasumoto, Hiroshi Esaki, "On Seamless Connectivity over Multi-Radio and Multi-Channel Wireless Mesh Networks", ACM CoNEXT 2008 Student Workshop, December, 2008
- 藤田 祥, 江崎 浩, "透過型アドホックネットワーク構築ミドルウェア ATMOS", マルチメディア, 分散, 協調とモバイル (DICOMO2008) シンポジウム, July, 2008 (優秀論文賞, ヤングリサーチ賞受賞)
- Sho Fujita, Hiroshi Esaki, "OMNI: an Overlay Mobile Ad-Hoc Network at the Edge of the Internet", 3rd International Conference on Future Internet Technologies (CFI08), June, 2008

査読無し発表は以下である。

- 藤田 祥, "被災地情報収集ネットワーク", シンポジウム「ロボット群による被災建造物内の情報インフラ構築と情報収集システム」, August, 2009
- Sho Fujita, "Analyzing the MAC-level Behavior of Multi-Radio Wireless Networks", 7th CNRS-WIDE Workshop, March, 2009
- Sho Fujita, "On Seamless Connectivity on Multi-Radio, Multi-Channel Wireless Mesh Network", The Second Asia Future Internet (AsiaFI) School on Mobile and Wireless Networks, January, 2009
- Sho Fujita, "the current status of the robohoc network", 6th CNRS-WIDE Workshop, October, 2008

-
- 安本 直史, 藤田 祥, 江崎 浩, ”無線パケットモニタリングに基づくメッシュアクセスポイント配置手法”, 第 46 回モバイルコンピューティングとユビキタス通信研究会, September, 2008
 - Sho Fujita, ”ATMOS: A middleware for Transparent MOBILE ad-hoc networking Systems”, The First Asia Future Internet (AsiaFI) School on Architecture and Building Blocks, August, 2008
 - 亀川 哲志, 佐藤 徳孝, 松野 文俊, 藤田 祥, 島 慶一, 宇夫 陽次朗, ”被災建物内探索用兄弟型レスキューロボットの開発 —アドホックネットワーク環境下における複数台遠隔操縦のためのソフトウェアデザイナー—”, 中国四国支部・九州支部合同企画 岡山講演会, October, 2008
 - Keiichi Shima, Yojiro Uo, Sho Fujita, ”Auto configuration and management mechanism for the robotics self extensible WIFI network”, International Conference on Instrumentation, Control and Information Technology(SICE Annual Conference 2008), August, 2008
 - Sho Fujita, ”An Extensible and Portable Programming Framework for Ad-Hoc Networks”, 東京大学精華大学共同ワークショップ, May, 2008
 - Sho Fujita, ”An Extensible Programming Framework for Ad-Hoc Networking”, 5th CNRS-WIDE Workshop, March, 2008
 - 島 慶一, 宇夫 陽次朗, 藤田 祥, 安本 直史, 田中 陽介, 河村 悠生, 飯塚 拓郎, 堀川 大輔, ”無線マルチホップ通信を用いた 合宿バックボーンネットワーク構築実験”, WIDE Technical-Report, 2008
 - 藤田 祥, 安本 直史, 江崎 浩, ”リアクティブ型近隣探索によるブロードキャストストームの抑制”, 第 43 回モバイルコンピューティングとユビキタス通信研究会, November, 2007
 - 藤田 祥, 落合秀也, ”RFID と Web2.0 を用いた協調的ログ作成補助システム”, 第 14 回インタラクティブシステムとソフトウェアに関するワークショップ (WISS 2006), December, 2006