■4 群（モバイル・無線）-5 編（モバイル IP，アドホックネットワーク）

2 章 アドホックネットワーク

（執筆者：阪田史郎）［2010 年 5 月 受領］

■概要■

ユビキタスネットワーク社会実現のための一要素となるアドホックネットワークの研究が活発に進められている．アドホックネットワークはその用語の示すとおり，一時的にネットワークを構成しその場だけの利用を目的とし，1970 年代初頭の軍事研究に端を発する．四半世紀にわたる軍事研究を経て，ノードの移動を想定した無線パケット通信技術の発展に伴い 1990 年代半ばから世界的に研究が活発になり，1997 年には IETF（Internet Engineering Task Force）に MANET（Mobile Ad hoc NETwork）WG が発足しルーチングプロトコルを中心とした標準化の議論も開始された．2005 年には四つのユニキャストルーチングプロトコルが標準化され，2010 年現在，リアクティブプロトコルとプロアクティブプロトコルがそれぞれ DYMO，OLSR v2 に集約しつつある．しかし，地震や洪水などの大規模災害を想定した多くの実証実験が報告されているものの，実用化の面では大きな進展に至っていない．

技術課題がまだ多く残されており，本格的な実用は 2015 年以降になると思われる．軍事，災害のような非常時以外にも，ITS，工場や建築の現場，農場，商品倉庫，港湾など想定される利用局面は多岐にわたり，今後の更なる技術開発が期待される．

【本章の構成】

本章では，アドホックネットワークの概要（動作概要とアプリケーション）（2-1 節），アドホックネットワークのプロトコルと IP アドレス自動割当（2-2 節），アドホックネットワークの応用システム（2-3 節），アドホックネットワークの性能（2-4 節），アドホックネットワークのセキュリティ（2-5 節）について述べる．

■4 群 － 5 編 － 2 章

2-1 アドホックネットワークの概要

2-1-1 アドホックネットワークとは [1), 2)]

（執筆者：間瀬憲一）［2008 年 8 月 受領］

モバイルアドホックネットワーク（MANET : Mobile Ad Hoc Network, 以下では単に MANET）は通信機能を有するノード（携帯端末など）の集まりであり，ノードのみによってノード相互の通信を実現する技術である．ノードは新たに追加されたり，退去したり，移動するダイナミックな環境を想定する．原則として，特別な役割をもつノードは存在せず，どのノードも同様の役割をもち対等の関係にある．移動通信における基地局，無線 LAN のアクセスポイント（AP），基地局-AP 間のバックボーンネットワークといったインフラストラクチャを必要としないため, 場所を選ばずノードが集まった時点で即座にネットワークが構築される．MANET は通信インフラを利用できない軍事作戦での通信手段として注目されてきたが，センサネットワーク，無線メッシュネットワーク [3)] やユビキタスネットワーク実現の観点から注目される技術であり，コンピュータの小型・軽量化，無線 LAN の普及などにより，近年，研究開発や標準化が進展している．

MANET では，周囲のどの方向のノードとも通信可能であることが望ましいため，通常，アンテナは無指向性のアンテナ（オムニアンテナ）を使用する．無線送受信機同士が通信相手を探索し，AP などを介さず直接通信する機能が必要である．無線送受信機には互いに干渉しない複数のチャネルを利用できるものが多い．複数のノードの集合である MANET では各ノードの無線送受信機において同一チャネルを選択・設定することが基本となる．これによってノード間に共通チャネルを確保できる．ノードが複数の無線送受信機をもつ場合には MANET 内で複数チャネルの利用が可能になる．

MANET は通常，IP ネットワークとして構成される．IP ネットワークでは IP より下位層の通信システムを一般にリンク，ノードのリンクへの接続点をインタフェースと呼ぶ．インタフェースに対して IP アドレスが与えられる．ノードはリンクにより隣接ノードと接続され，そのリンクを経由して IP パケットの送受を行う．一般にノードは複数の有線／無線インタフェースをもつ場合が考えられる．無線インタフェースの中で，特に MANET を構成するための無線インタフェースを MANET インタフェースと呼ぶことにする．以下では特に断らない限り，インタフェースとは MANET インタフェースを意味する．

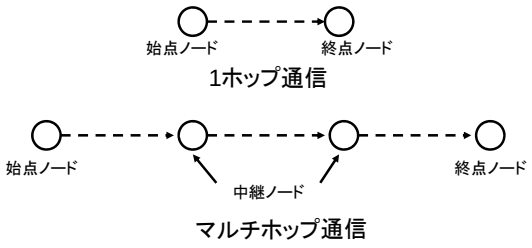


図2・1　1ホップ通信とマルチホップ通信

（出典：小牧省三, 間瀬憲一, 松江英明, 守倉正博「無線 LAN とユビキタスネットワーク」丸善，2004）

送信元のノードと宛先となるノードが近在し，見通しが良い場合にはノード間で直接通信が可能である．このような通信形態を 1 ホップ通信という（**図 2･1**）．また，1 ホップで通信可能なノードを隣接ノードという．ノード X が送信したパケットをノード Y が受信可能であってもノード Y が送信したパケットをノード X が受信可能であるとは限らない．通常，双方向の通信が可能なノードを隣接ノードと呼ぶ．ノードの移動や通信路（チャネル）の状況により，隣接ノードが時々刻々と変化することも考えられる．

宛先との距離が長かったり見通しがなかったりすると，直接通信ができないので，中間に存在する他のノードを中継して通信する．このような通信形態をマルチホップ通信という（図 2･1）．

いま，ノード X がノード Y を介してノード Z にパケットを配送する場合を考える（**図 2･2**）．このとき，ノード Y が一つの無線インタフェースからパケットを受信し，同じ無線インタフェースにパケットを送信することも考えられる（ノード Y が無線送受信機を一つだけもつ場合は必ずそうなる）．ノード X の隣接ノードの集合とノード Y の隣接ノードの集合が異なるため，ノード Y の同一のインタフェースで受信と送信を行うことにより，パケット中継が可能になる．有線通信ではノード X の隣接ノードの集合とノード Y の隣接ノード集合は一致する（例えばイーサネット）ため，ノード Y で同一のインタフェースで受信と送信を行ったとしてもパケットが送信元に送り返されるだけであり，パケット中継にはならない．パケット中継を行うにはノード Y で受信とは異なるインタフェースで送信を行う必要がある．

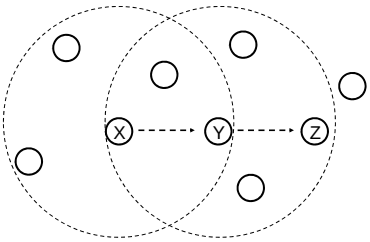


図 2・2　同一インタフェースを利用したパケット中継

このように，有線の場合とインタフェースの利用方法に違いはあるが，MANET ではノードが中継機能も実現することになる．このような機能はルーチングと呼ばれる．ルーチングはネットワークにおいてパケットを生成したノード（始点）からそのパケットの宛先ノード（終点）へパケットを配送する仕組みである．ルーチングは IP ネットワークでいえばルータの機能である．MANET のノードはホスト機能とルータ機能を併せもつといえる．前述のように，各ノードは対等であるので，ノード自身が自律分散的・自動的に中継経路を選択する機能が必要である．**図 2･3** に MANET の例を示す．

インターネットの基本構成単位としは AS（Autonomous System）と概念がある．AS は一つの組織により管理されるネットワークであり，同一のルーチングプロトコルが使用される．AS 内で使用されるルーチングプロトコルもルータによる自律分散制御を前提としている．

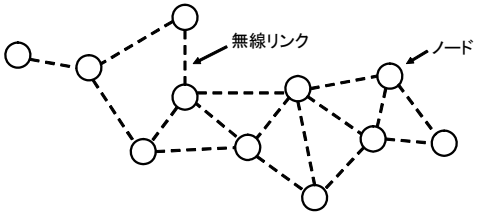


図 2・3　アドホックネットワークの例

（出典：小牧省三, 間瀬憲一, 松江英明, 守倉正博「無線 LAN とユビキタスネットワーク」丸善，2004）

AS 内に適用されるルーチングプロトコルにはベクトル距離型とリンク状態型がある．MANET も原理的には AS と同様にとらえられるが，ノードの高移動性や限られた無線帯域などの特徴を考慮したルーチングプロトコルが必要になる．MANET のルーチングプロトコルはトポロジー情報を利用するルーチングプロトコルと位置情報を利用するルーチングプロトコルに分類される．前者は更にプロアクティブ型ルーチングとリアクティブ型ルーチングプロトコルに分類される（**図 2･4**）．

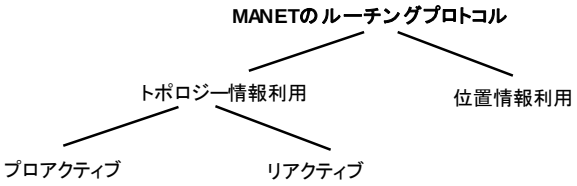


図 2・4　MANET ルーチングプロトコルの分類

ここで MANET の特徴は次のようにまとめられる．

・ノードはユーザ端末（ホスト）であり，移動性を有する．
・一時的に利用されるネットワーク．
・有線ケーブルの配線を必要とせず，ノードだけで構成されるネットワーク．
・ノードはルータの役割を兼ね，無線マルチホップ通信が行われる．
・ノードの移動，無線通信の特性によりネットワークトポロジーが頻繁に変更する可能性がある．
・無線マルチホップに最適化したルーチングプロトコルが利用される．

LAN では同一の LAN に所属する端末同士の通信だけでなく，インターネットなど外部のネットワークと接続する利用形態が一般的である．MANET でも同様にブロードバンドアクセスやユビキタスネットワークの足回りのネットワークなど，インターネットと接続して利用される形態が考えられる．この場合，MANET のノードの一部がインターネットアクセスを提供するルータ(アクセスルータ)への有線または無線インタフェースを介して接続する．MANET 単独で存在する形態をスタンドアローン型 MANET，インターネットと接続する形態を接続型 MANET と呼ぶ．図 2･3 は前者の例である．後者の例を**図 2･5** に示す．

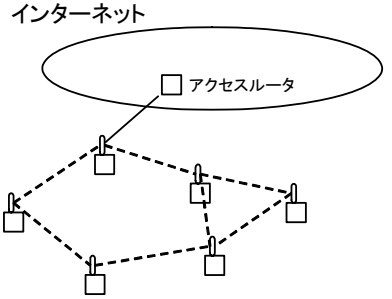


図 2・5　接続型 MANET の例

（出典：間瀬憲一，阪田史郎「アドホック・メッシュネットワーク」コロナ社, 2007）

■参考文献

1) 間瀬憲一，阪田史郎，“アドホック・メッシュネットワーク（ユビキタスネットワーク社会の実現に向けて），” コロナ社, 2007.
2) 小牧省三，間瀬憲一，松江英明，守倉正博，“無線 LAN とユビキタスネットワーク，” 丸善, 2004.
3) I. F. Akyildiz, S. Wang, and W. Wang, “Wireless Mesh Networks: A Survey,” Computer networks, vol.47, no.44, Elsevier Science, pp.445-487, 2005.

2-1-2 アプリケーション例

（執筆者：阪田史郎）［2009 年 1 月 受領］

アドホックネットワークの研究が軍事研究に端を発していることから，戦場での利用がアプリケーションの起源である．現在，最も早期の実現が期待されているのが，戦場での利用と通信環境が類似している災害などの非常時の通信であり，公共サービスの一環として既に国内外で多くの実証実験が実施されている．一部は実験的に運用されているが，公共サービスのため自治体などからの資金援助のもとで実施されているものが多い．民間企業によるビジネスにはまだ至っていない．

表 2・1　アドホックネットワークで想定されている応用

分類	概要
軍事利用	・戦場における兵士，戦車，戦艦，戦闘機の間の通信
災害時の利用	・大規模な地震，火災，津波，洪水，台風などが発生したときの警察や消防による捜索，救出，緊急通報，避難誘導，被害情報の収集・連絡，復旧活動支援，被災者どうしの安否確認
携帯電話網，無線 PAN，無線 LAN をマルチホップ化したサービス	・工場，商品倉庫，建築工事現場，港湾，農場，ゴルフ場，ケーブル敷設困難なエリア（史跡，博物館）などにおける情報伝達・管理 ・ショッピングモール，テーマパーク，イベント会場，スタジアムなどにおける P2P 情報配信（広告配信，ナビゲーションなど） ・広域センサネットワーク（防犯・防災，環境モニタリング） ・情報家電ネットワークにおける各種機器の制御
ITS（テレマティクス）	・車車間通信による事故発生や工事などにおける混雑状況や迂回路情報のリアルタイム通知，カーナビへの反映 ・路車間通信によるサービスエリアのサービス情報配信

アドホックネットワークの全般的なアプリケーションを**表 2･1** に示す [1), 2)]. アドホックネットワークが普及し，一般コンシューマの社会生活に受け入れられ広く普及するには，普段使いの形でビジネスモデルが成り立つ，表に示した携帯電話網，無線 PAN，無線 LAN をマルチホップ化したサービスや ITS（高度道路交通システム，テレマティクス）への応用が必須条件となる.

■参考文献

1) 阪田史郎, 青木秀憲, 間瀬憲一, “アドホックネットワークと無線 LAN メッシュネットワーク,” 信学論, vol.J89-B, no.6, pp.811-823, Jun. 2006.
2) 間瀬憲一, 阪田史郎（電子情報通信学会 編）“アドホック･メッシュネットワーク ーユビキタスネットワーク社会を実現する技術,” コロナ社, Sep. 2007.

■4 群 － 5 編 － 2 章

2-2 アドホックネットワークのプロトコルと IP アドレス自動割当

2-2-1 データリンク層

（執筆者：渡辺　尚）［2009 年 4 月 受領］

データリンクレイヤは，ネットワーク層（第 3 層）と物理層（第 1 層）の間に位置し，ネットワーク層から要求されたパケットを隣接ノードに配送するよう物理層に要求を出す役割を負う．データリンクレイヤは，物理層に近い方から，MAC 副層と LLC 副層の二つに更に細分化される（**図 2･6**）．ここでは，アドホックネットワークで特に重要な役割をもつ MAC について説明する．

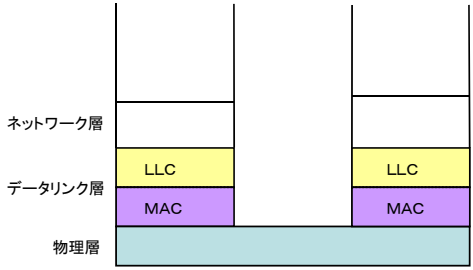


図 2･6　データリンク層の位置づけ

MAC は，一つあるいは複数の物理メディア（物理媒体）を複数のノードが共有して通信する際に必要となる技術である．例えば，PC とプリンタを接続するように，有線によるポイント・ツー・ポイント通信の場合は，送信側インタフェースにビット列を入力すると物理層を介して受信側インタフェースにビット列が現れる．つまり，物理メディアは送信受信ペアによって一意に決定されており，複数のノードが物理媒体を共有することはない．このような場合には，MAC は不要である．反対に，無線の場合や，有線でも一つのノードの信号が複数のノードに届くような物理メディアの場合には，どのノードがどのタイミングで信号を出すのかを MAC で制御する必要がある．すなわち，MAC は交通整理をする役目を負っている．アドホックネットワークでは，移動性を確保するために，無線を利用することが通常であり，MAC の性能がネットワーク全体の性能に大きな影響を与える．

同一のチャネルで同一の時間に複数のノードが信号を発し，それが同一の受信ノードに届いた場合，複数の信号を判別できなくなる．これを衝突という．通常衝突した場合には，再送を行うことになる．一方，他のノードが送信する可能性を考え，信号の送信を保留（あるいは延期）する方法では，保留しすぎると実際には物理媒体は空きであるにもかかわらずどのノードも送信しない無駄な時間が生じる．したがって，MAC の効率化には，物理媒体の空き時間を小さくしつつ衝突を抑える制御が必要になる．いま，**図 2･7** に示すように，時間，空間（ノード），周波数（チャネル），の 3 軸からなる空間を考えると，立方体で表現される送受信データをいかに密に充填するかが問題となる．この考え方に沿って，MAC を最適化問題として捉えることもできる．しかし，一般的には各ノードで発生するトラヒックの予想が立たないこと，ノードの移動によりノード生成･死滅が生じること，衝突や物理層のエラー

によって再送が生じることなどのため，最適なスケジュールを常に維持することは非常に困難である．したがって，多くの MAC では各ノードの第 3 層からパケット送信要求が発生した時点で，物理媒体をアクセスする方式がとられる．

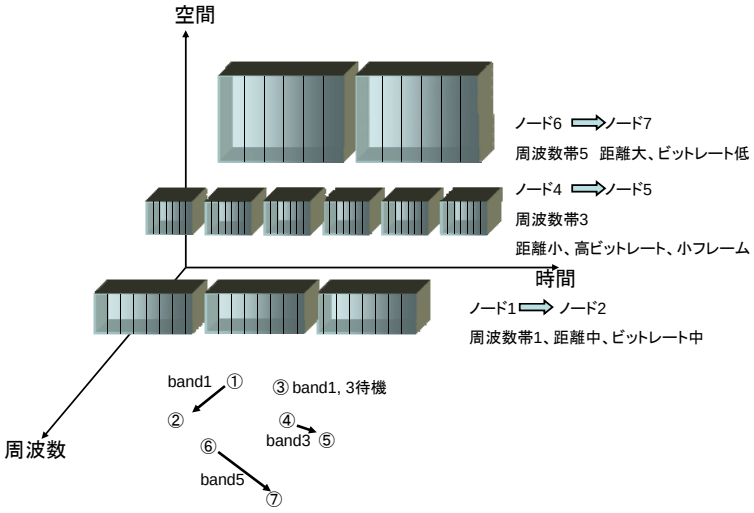
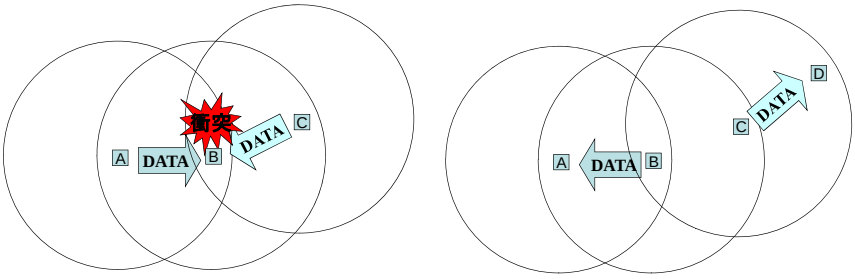


図 2・7　MAC プロトコルの概念

また，無線特有の問題として，隠れ端末問題，さらし端末問題がある．隠れ端末問題とは，**図 2･8**(a) に示すように，AB が通信をしている場合，この通信を知らない C が B に対して信号を送出すると，B には A と C の両方の無線信号が届き衝突が生じる問題である．C を AB に対する隠れ端末という．また，さらし端末問題とは図 2･8(b) のように，AB が通信をしている場合，D へ信号を送出したい C は，AB 間の通信を妨害しないように送信を保留する．しかし，B→A の送信と C→D への送信は同時に行ってもよい．C を AB に対するさらし端末，そしてこの問題をさらし端末問題という．



(a)　隠れ端末問題　　(b)　さらし端末問題

図 2・8　隠れ端末問題とさらし端末問題

具体的な MAC としては，古典的な pure ALOHA，slotted ALOHA，CSMA に加え，CSMA/CA をもとにした IEEE 802.11 などがある．CSMA は，ノードが信号を出す前に他のノードが信号を出していないかチェック（キャリアセンス）し，キャリアを検出しなかった場合に次の送信手順に進む．有線の Ethernet では，信号を送信と同時に受信を行って他のノードと同時に信号を送出したかの衝突検出（Collision Detection）を行う．一方，無線では信号の減衰が激しいため，ノードが信号を送信しているときには他のノードの信号を受信することが不可能である．したがって，キャリアを検出しなかった場合に，すぐに送信するのではなく，ある程度の時間を待ってから（これをバックオフという）信号の送信を行い，衝突回避（Collision Avoidance）を試みる．この方式を CSMA/CA と呼ぶ．

アドホックネットワークのデータリンク層としては，IEEE 802.11 を基本とするものが多い．802.11 は，(1) CSMA/CA による衝突回避（完全には回避されないことに注意），(2) RTS（Request To Send），CTS（Clear To Send）交換による隠れ端末回避，(3) Duration による送信待機時間の通知の特徴をもつ．**図 2･9** に示すように，まずノード B に送信すべきフレームをもつ端末 A は，キャリアをセンスする．キャリアが空きであった場合には，バックオフを行う．その後，RTS フレームを B に向けて送信する．RTS を受信した B は CTS フレームを A に送信する．その後，A は DATA フレームを送信し，B は ACK フレームを返送する．RTS，CTS，DATA には，これからメディアを占有する時間（duration）が含まれている．duration は NAV（Network Allocation Vector）期間とも呼ばれる．したがって，これらのフレームを傍受した端末 C や D は，送信すべきフレームがあったとしても duration の間送信を保留（延期）する．すなわち，C や D はフレーム送信の前のキャリアセンスに先立ち NAV 期間かどうかをチェックする．これを仮想キャリアセンスと呼び，通常のキャリアセンス（物理キャリアセンス）と区別する．

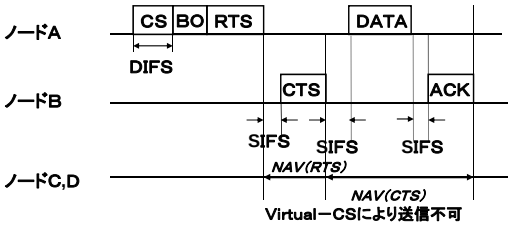


図 2・9　802.11 方式の概念

最近のアドホックネットワークの MAC では，図 2･7 に沿っていえば，(1) 時間利用効率を上げる方法として，複数のレートを適応的に制御する方式（ARF [1]，RBAR [2]），ネットワークコーディングを考慮する方式（coop [3]），(2) 空間利用効率を上げる方法として，スマートアンテナや指向性アンテナを利用する方式（DMAC [4]，SWAMP [5]），送信電力制御を行う方式（COMPOW [6]），(3) 周波数利用効率を上げる方法として，複数のチャネルを利用する方式（DCA [7]，MMAC [8]），などが開発されている．

■参考文献

1) A. Kamerman and L. Monteban, “WaveLAN II; A hight-performance wireless LAN for the unlicensed band,” Bell Labs Tech. J., pp.118-133, 1997.
2) G. Holland, N. Vaidya, and P. Bahl, “A rate-adaptive MAC protocol for multi-hop wireless networks,” in Proc. ACM/IEEE MobiCom’01, Jul. 2001.
3) J. N. Laneman, G. W. Wornell, “Distributed space-time coded protocols for exploiting cooperative diversity in wireless networks, ” IEEE GLOBECOM’02, 2002.
4) R. R. Choudhury, X. Yang, R. Ramanathan, and N. H. Vaidya, “Using directional antennas for medium access control in ad hoc networks,” Proc. ACM MobiCom, pp.59-70, Sep. 2002.
5) Masanori Takata, Katsushiro Nagashima, Takashi Watanabe, “A Dual Access Mode MAC Protocol for Ad Hoc Networks Using Smart Antennas,” IEEE International Conference on Communications (ICC2004), pp.4182-4186, Jun. 2004.
6) http://citeseer.ist.psu.edu/old/narayanaswamy01compow.html
7) Shih-Lin Wu, Chih-Yu Lin, Yu-Chee Tseng, Jang-Laing Sheu, “A new multi-channel MAC protocol with on-demand channel assignment for multi-hop mobile ad hoc networks, Parallel Architectures, Algorithms and Networks, ” I-SPAN 2000, 2000.
8) Jungmin So, Nitin H. Vaidya, “Multi-channel mac for ad hoc networks: handling multi-channel hidden terminals using a single transceiver,” Proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing (Mobihoc), 2004.

2-2-2 プロアクティブ型ユニキャストルーチングプロトコル [1), 2)]

（執筆者：間瀬憲一）［2008 年 8 月 受領］

(1) プロアクティブ型ルーチング [1), 2)]

プロアクティブ型はインターネットのリンク状態型ルーチングプロトコルと同様な原理のもとに MANET への最適化を行う観点から開発されたもので，ノード間で周期的な制御メッセージの交換を行うことにより，各ノードがすべての終点への経路情報を常時保持する．各ノードはハローメッセージを周期的にブロードキャストすることにより，隣接ノードとの接続（リンク）状態を把握する．また，自身のリンク状態を周期的にブロードキャストし，それを初めて受信したノードは再ブロードキャストを行う．これを繰り返し MANET 内のすべてのノードへ情報が伝わる．このような情報伝搬手法はフラッディングと呼ばれる．各ノードはこの情報に基づき，MANET 全体のノードとノード間のリンク状態，いわばネットワークの地図を得ることができ，Dijkstra アルゴリズムを用いて各終点までの最短経路を計算し，自身の経路表を作成する．このように，プロアクティブ型のルーチングプロトコルでは周期的に制御メッセージが生ずることにより制御オーバヘッドが比較的多く，MANET ではそれを削減する工夫が必要になる．以下ではプロアクティブ型ルーチングプロトコルの代表例としてリンク状態ルーチングプロトコルである OLSR [3)] を取り上げ，その基本動作を説明する．

(2) 隣接ノードの発見

一般に，各ノードは複数の無線送受信機と対応する MANET インタフェースをもつことが可能であるが，簡単のため，ここでは各ノードは一つの MANET インタフェースをもち，このインタフェースに与えられた IP アドレスをこのノードのアドレスとする．各ノードは周期的にハローメッセージをブロードキャストする．ハローメッセージ送信間隔の推奨値は 2 秒である [3)]．ハローメッセージには自身のアドレス，シーケンス番号，隣接ノードのアドレス

などの情報が入っている．このため，ハローメッセージを受信したノードは隣接ノードのアドレスのみならず，隣接ノードの隣接ノード，すなわち 2 ホップ先のノード（2 ホップ隣接ノード）のアドレスを得ることができる．また，受信したハローメッセージの隣接ノード・アドレスの中に自身のアドレスが含まれていれば，自身が送出したハローメッセージを隣接ノードが受信したことが確認できる．これは自身と隣接ノード間で双方向にハローメッセージの送受が可能ということであり，このようなリンクを対称リンクと呼ぶ．自身のアドレスが含まれていなければそのリンクは非対称リンクの状態と認識される．このようなリンクの状態もハローメッセージに含めて送られる. **図 2･10** ではノード A のハローメッセージをノード B が受信し, ノード C では受信失敗となっている. その後, ノード B からのハローメッセージがノード A と C によって受信され，その中にノード A のアドレスが含まれていることを検知することにより，ノード A は A-B 間のリンクを対称リンクと認識する．また，ノード C はノード A を 2 ホップ隣接ノードと認識する. 更にその後, C から送信されたハローメッセージがノード A で受信されると，その中にはノード A のアドレスが含まれていないため，ノード A は A-C 間のリンクを非対称リンクと認識する．

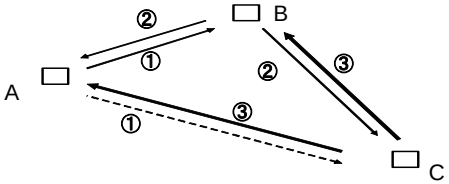


図 2・10　ハローメッセージの送受とリンク状態の認識

（出典：間瀬憲一, 阪田史郎「アドホック・メッシュネットワーク」コロナ社, 2007）

(3)　MPR 選択

OLSR はリンク状態ルーチングプロトコルであり, (1) 項に述べたように各ノードが自身の隣接ノード／リンクの情報を他のノードへ通知するためフラッディングと呼ばれるプロトコルを用いるのが基本となる．フラッディングプロトコルではメッセージの生成元がメッセージをブロードキャストする．それを受信したノードはブロードキャスト（再ブロードキャスト）を繰り返す．これによってすべてのノードにメッセージを届けることを試みる．この過程で同じメッセージを重複して受取った場合には再ブロードキャストを行わず，そのメッセージを廃棄する．フラッディングプロトコルはシンプルであるが，メッセージのブロードキャスト回数が多く，無線帯域利用の点で効率的とはいえない．OLSR では各ノードが周期的にハローメッセージを交換し，MPR（Multi-Point Relay）と呼ばれるノードを選択することにより，制御オーバヘッドの削減を図る．

(2) 項に述べたように，各ノードは受信したハローメッセージに基づき，自身の隣接ノードと 2 ホップ隣接ノードのアドレスを知る．隣接ノードの中で自身と対称リンクをもつものを対称隣接ノード，2 ホップ隣接ノードの中で中間の対称隣接ノードと対称リンクをもつものを対称 2 ホップ隣接ノードと呼ぶ. 各ノードはこれらのノード情報に基づき, 対称隣接ノードの中から必要最小限の MPR を選択する．このとき，MPR を選択する側のノードを MPR セレクタと呼ぶ．あるノードにおける MPR の選択はこのノードがブロードキャストしたパ

ケットをこのノードのすべての MPR が再ブロードキャストすると，すべての対称 2 ホップ隣接ノードにメッセージが届くことを条件として行う．この問題は NP 完全であり，厳密解を求めることは計算量的に困難であるが，発見的は方法が使われている．また，この際，WILLINGNESS（自身が MPR として選択される許容度）というパラメータを導入して，MPR 選択の優先度を考慮できるものとしている．

図 2･11 にはフラッディングプロトコルにおけるパケット転送の様子を示す（図中のすべてのリンクは対称リンクと想定する）．中心のノードがパケットをブロードキャストし，それをすべての隣接ノードが再ブロードキャストする．これによって，すべての 2 ホップ隣接ノードにパケットが到達するが，一つの 2 ホップ隣接ノードが同じパケットを重複して受け取る場合があることがわかる．

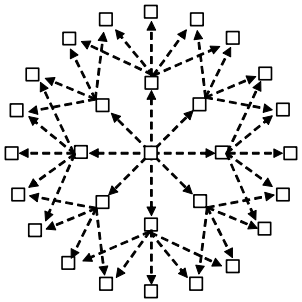


図 2・11　バケットのブラッティング

（出典：間瀬憲一，阪田史郎「アドホック・メッシュネットワーク」コロナ社, 2007）

図 2･12 では中心のノードが 4 個の MPR を選択している．選択された MPR がパケットの再ブロードキャストを行うことにより，すべての 2 ホップ隣接ノードにパケットが到達する．この例の場合，どの 2 ホップ隣接ノードでもパケットの重複受信は発生していない．このように，フラッディングプロトコルとは異なり，隣接ノードのうち MPR として選ばれたノードのみが再ブロードキャストを行うため，ブロードキャストの総数を減少させ，同じパケットの重複受信を減少させることができる．このようなパケット配送の方法を MPR フラッディングと呼ぶ．

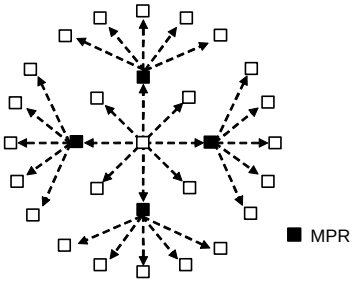


図 2・12　マルチポイントリレー（MPR）の選択と MPR フラッディング

（出典：間瀬憲一，阪田史郎「アドホック・メッシュネットワーク」コロナ社, 2007）

各ノードは自身の MPR を選択すると，その情報をハローメッセージに載せて隣接ノードへ通知する．これを受信した各ノードは自身の MPR セレクタを認識できる．これにより自身の MPR セレクタからブロードキャストされたパケットを受信した場合のみ再ブロードキャストを行うことが可能になる．

(4) リンク情報の配送

OLSR ではリンク情報は TC（Topology Control）メッセージによって運ばれる．TC メッセージを生成するのは MPR のみである．各 MPR は周期的に TC メッセージを生成し，MPR フラッディングにより MANET 全体に配送する．TC メッセージ送信間隔の推奨値は 5 秒である [3]．TC メッセージには自身のアドレス，シーケンス番号，自身の MPR セレクタのアドレスなどの情報が入っている．このように OLSR では次の工夫がなされていることがわかる．

すべてのノードが TC メッセージの生成元になるのではなく，MPR のみが生成元となるため，TC メッセージの生成数が削減される．

TC メッセージにすべての隣接ノードの情報を入れるのではなく，MPR セレクタの情報のみを入れることにより，メッセージサイズが削減される．

TC メッセージは単純なフラッディングではなく MPR フラッディングされるため，TC メッセージの再ブロードキャストの総数が削減される．

図 2･13 では黒塗りの四角で表されたノードが MPR になっており，MPR と MPR セレクタ間のリンクを実線で表している．各 MPR は実線で示される自身の MPR セレクタとの間のリンクの情報のみを TC メッセージに載せて周知する．破線で表されるリンクの情報は周知されない．

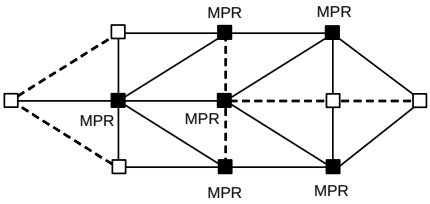


図 2・13　MPR の選択例

（出典：間瀬憲一，阪田史郎「アドホック・メッシュネットワーク」コロナ社, 2007）

(5) 経路計算

各ノードはハローメッセージ，TC メッセージの交換に基づき，ローカルリンク情報ベース（リンクセット），近隣情報ベース（隣接ノードセット，2 ホップ隣接ノードセット，MPR セット，MPR セレクタセット），トポロジー情報ベース（トポロジーセット）を生成・維持する．また，一つのノードが複数のネットワークインタフェースを有する場合に，インタフェースの一つをメインアドレスとし，他のインタフェースのアドレスと関連付けるため，複数インタフェースアソシエーション情報ベースを生成・維持する．

各ノードはローカルリンク情報ベース，近隣情報ベース，トポロジー情報ベース，複数インタフェースアソシエーション情報ベースの情報に基づき，それらの内容が変化したとき各ノードへの経路（ホップ数に基づく最短経路）をダイクストラのアルゴリズムと同種のアル

ゴリズムにより計算し，経路表を更新する．具体的には，経路表の各終点に対し，最短経路を計算し，パケットの次の送り先（次ホップ）を求め，経路表の経路エントリーを生成する．まず，2 ホップ先のノードへの経路はローカルリンク情報ベース，近隣情報ベースの情報を基に計算することができる．次に $n-1$ ホップ先までの経路を計算済みの場合，トポロジー情報ベースの情報に基づき，n ホップ先のノードへの経路を計算可能である．また，複数インタフェースアソシエーション情報ベースの情報に基づき，複数インタフェースをもつノードへの経路計算も可能になる．

■参考文献

1) 間瀬憲一, 阪田史郎, “アドホック・メッシュネットワーク（ユビキタスネットワーク社会の実現に向けて）,” コロナ社, 2007.
2) 小牧省三, 間瀬憲一, 松江英明, 守倉正博, “無線 LAN とユビキタスネットワーク,” 丸善, 2004.
3) T. Clausen and P. Jacquet, “Optimized Link State Routing Protocol (OLSR), ” RFC 3626, Oct. 2003.

2-2-3 リアクティブ型ユニキャストルーチングプロトコル [1), 2)]

（執筆者：間瀬憲一）［2008 年 8 月 受領］

(1) リアクティブ型ルーチング

リアクティブ型では，各ノードは通信要求が生じたときに経路情報を獲得し，その情報を一定時間保持する. このため, 通信要求が生じてから送信可能となるまでの遅延が生ずるが, 通信トラヒックが少ないときには制御メッセージのオーバヘッドが比較的少ない方式である. リアクティブ型は MANET に特有の新たなルーチングの型といえる．以下では，リアクティブ型ルーチングプロトコルの代表例として AODV [3)] を取り上げ，その基本動作を説明する．

(2) 経路発見

AODV における経路エントリーは終点ノード，次ホップ IP アドレス，終点シーケンス番号，終点までのホップ数などの情報で構成される（**図 2･14**）．ノードはアプリケーションからデータパケットを受信し終点への経路エントリーをもたないとき，データパケットをバッファに貯めておき，経路発見の処理を開始する（**図 2･15**）．まず，経路要求（RREQ：Route Request）メッセージ（以下，RREQ）をブロードキャストする（RREQ を格納する IP パケットのヘッダの終点アドレスをブロードキャストアドレスとする）. RREQ メッセージの生成元アドレスには自身の IP アドレス, 終点アドレスには終点の IP アドレスを入れる. RREQ メッセージを初めて受信したノードは生成元への経路エントリー（これを逆方向経路と呼ぶ）を生成すると共に，RREQ の再ブロードキャストを行う．これにより，RREQ は終点ノードへ到達することになる．

終点 ノードアドレス	終点 シーケンス番号	次ホップアドレス	ホップ数	有効期限

図 2・14　経路エントリーの構成例

（出典：小牧省三, 間瀬憲一, 松江英明, 守倉正博「無線 LAN とユビキタスネットワーク」丸善，2004）

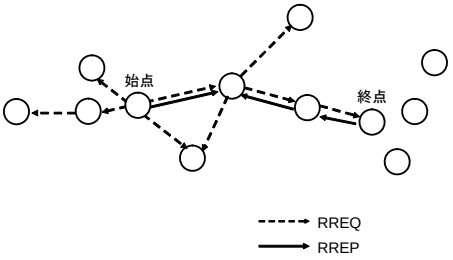


図 2・15　経路発見プロセス

RREQ を受信した終点ノードは逆方向経路の次ホップへ経路応答（RREP：Route Reply）メッセージをユニキャストする（RREP を格納する IP パケットの終点アドレスを逆方向経路の次ホップのアドレスとする）．このとき，RREQ の生成元 IP アドレス，終点 IP アドレスを RREP の対応するフィールドにコピーする．RREP を受信したノードは終点への経路エントリー（これを順方向経路と呼ぶ）を生成すると共に，保持している逆方向経路の次ホップへ RREP をユニキャストする．このとき，RREP の送り先隣接ノードを順方向経路のエントリーに対応するプリコーサリストに入れる（**図 2･16**）．すなわち，プリコーサリストとは，各経路エントリー（終点ノード）に関して，自身を次ホップとする上流隣接ノード（プリコーサ）のリストである．この使い道は(4) 項に述べる．これにより RREP メッセージは RREQ メッセージの配送パスを逆に辿り，RREQ メッセージの生成元に到達し，終点への経路が確立する．その後，バッファ内のパケットの送信を開始する．上記では，終点が RREP を生成する場合を述べたが，終点以外のノードが終点への経路エントリーをもつ場合，そのノードが RREP を返送するモードも用意されている．以上の経路発見プロセスにおいて，各ノードに生成された経路エントリーには有効期限が設定され，経路が利用される都度，有効期限が更新される．有効期限が過ぎたものは無効となるが一定時間保持される．無効化された経路エントリーの情報の利用方法は後述する．

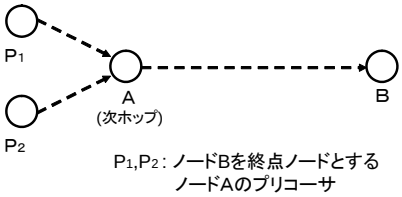


図 2・16　プリコーサの概念

（出典：小牧省三，間瀬憲一，松江英明，守倉正博「無線 LAN とユビキタスネットワーク」丸善，2004）

始点ノードが RREQ を送信する際，RREQ が不必要に MANET 内に拡散するのを防止するため，拡大リング探索と呼ばれる方法がある．RREQ の拡散範囲の制御には RREQ を運ぶ IP ヘッダの TTL（Time-To-Live）が利用される．1 回目の RREQ では始点ノード周辺の限られた範囲に拡散するように TTL の値を選択しておき，一定時間内に RREP が得られない場合には，TTL を一定値増加させ，RREQ を再送する．これを数回繰り返し，TTL が一定値以上に

なっても RREP が得られなければ，最後は MANET 全体に拡散するように TTL のデフォルト最大値を設定する．終点に関する無効化された経路エントリーが残っている場合には，そのホップ数情報に基づいて，1 回目の RREQ の TTL を決めることができる．

(3) シーケンス番号

プロアクティブ型のリンク状態ルーチングプロトコルではネットワーク全体のトポロジー情報に基づいて各終点への経路計算を行うので，原理的には経路ループの可能性は少ないといえる．一方，リアクティブ型のルーチングプロトコルでは，オンデマンドで経路発見が行われるため，各ノードでの生成時点の異なる経路が組み合わさって経路ループが生ずる可能性がある．これを防止するためには古い経路情報を識別・削除し，各ノードにおいて最新の経路情報を維持する仕組みが必要になる．AODV ではこのために各ノードの IP アドレスごとにシーケンス番号を保持しており，必要時に値を増加する．RREQ の終点アドレスと生成元アドレス，RREP の終点アドレスにはそれぞれのシーケンス番号を載せるフィールドがある．また，各ノードの経路エントリーには終点の IP アドレスごとに，そのノードが把握している終点のシーケンス番号をもたせており，これを終点シーケンス番号と呼ぶ．

各ノードは RREQ を送出する直前，自身のシーケンス番号を増加させる．これを受け取ったノードは逆方向経路をすでにもっている場合，その終点シーケンス番号より RREQ に含まれるシーケンス番号の方が大きいため，経路エントリーの更新を行う．これにより逆経路を最新の状態に維持することができる．また，自分宛の RREQ を受け取り，RREP を返す直前，そこに含まれる終点シーケンス番号の値が自身のシーケンス番号より大きいときは RREQ の中のシーケンス番号に一致させる．これは下記に述べるように，MANET 内で自身への経路障害が発生し，より新鮮な経路生成が必要になっているためである．

各ノードは経路の次ホップへのリンク断を検出した場合（(5)項参照），このリンクを使用する終点をリストアップし，これらの終点シーケンス番号を増加すると共に，経路を無効化する．このとき経路エラー（RERR : Route Error）メッセージ（以下，RERR）を生成する（**図 2･17**）．RERR にはこれらの終点 IP アドレスとシーケンス番号が含められるので，RERR を受け取ったノードは終点シーケンス番号を更新し，該当経路エントリーを無効化する．(2) 項に述べたように，経路エントリーは無効となっても一定時間は保持され終点シーケンス番号の参照が可能である．これらのノードに新たに RREQ を生成する場合には，その終点シーケンス番号を RREQ に設定することにより，より新鮮な経路の獲得に役立てる．

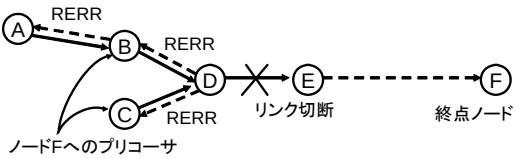


図 2・17　経路エラーメッセージの生成例

（出典：小牧省三，間瀬憲一，松江英明，守倉正博「無線 LAN とユビキタスネットワーク」丸善，2004）

(4) 経路保持

RREQ，RREP にはホップカウントというフィールドがある．それぞれ，RREQ 生成元，終点で 0 に設定され，それらを受け取った中間のノードではホップカウントの値を一つ増やして転送するので，それぞれ，RREQ 生成元，終点からのホップ数を表す．ノードがルーチングメッセージ（RREQ または RREP）を受信し，そこに含まれるノードへの経路エントリーを既にもっている場合，ルーチングメッセージのシーケンス番号が経路エントリーのシーケンス番号より大きければ経路エントリーの更新を行う．シーケンス番号が同じ場合には，メッセージ内のホップカウント ＋ 1（自身から隣接ノードへの 1 ホップ分を加えている）が経路エントリーのシーケンス番号より小さいとき経路更新を行う．

(2) 項に述べたように，各ノードに生成された経路エントリーには有効期限が設定される．経路が使用されると，その経路の始点，終点への経路エントリー，終点へのパス上の次ホップへの経路エントリーの有効期限が更新される．具体的には有効期限を現在時刻＋有効経路タイムアウト時間に設定する．始点-終点間のパスの対称性を想定し，始点への逆方向パス上の次ホップへの経路エントリーの有効期限も更新される．有効期限が過ぎた場合には，その経路エントリーを無効化する．次ホップへのパケット配送ができない場合には，RERR をこの経路を使用する上流ノードへ通知する必要がある．RERR には該当する次ホップを経路とする到達不能になった終点の IP アドレスを含める．RERR はブロードキャストするか，プリコーサリストに含まれるノードへユニキャストする．

RERR を生成するのは以下の場合である．

① 次ホップへのリンク断を検出（(5)項参照）．

② 終点への有効経路がなし．

③ 有効経路に関する RERR を受信．

このとき，到達不能の終点に対する経路エントリーにおいて，①，②の場合にはシーケンス番号を増加し，③の場合は受信した RERR の値をコピーする．その後，これらの経路エントリーを無効化する．

なお，①の場合において終点が経路エントリーにおいて一定ホップ数以内である場合，リンク断を検出したノードが RREQ を生成し，経路の修復を試みるモードがある（**図 2･18**）．これはローカル経路修復と呼ばれる [2]．これが成功した場合には RERR の生成は必要ない．

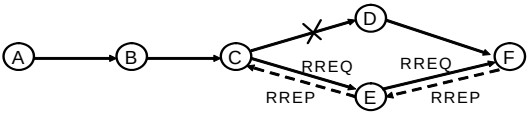


図 2・18 ローカル経路修復

（出典：小牧省三，間瀬憲一，松江英明，守倉正博「無線 LAN とユビキタスネットワーク」丸善，2004）

(5) リンク断の検出

リンク断の検出には次の方法が考えられる．

(1) ハローメッセージ

ノードが有効な経路上にある場合，周期的にハローメッセージを送出する．隣接ノー

ドからのハローメッセージが一定回数届かないとき，そのリンクが切断と判定する．

(2) リンク層通知

リンク層においてリンク切断の検出が可能である場合，その情報をネットワーク層で利用可能とする．例えば IEEE 802.11 では RTS 送信後の CTS タイムアウト，データ送信後の ACK タイムアウトによりリンク断が検出できる．

(3) 受動的確認応答

ノードがデータパケット転送後，相手先のノードがさらのそのパケットを転送するかどうかを監視する．その転送を感知できない場合，または相手ノードが終点（転送は行わない）の場合，次のいずれかの方法でリンク検出ができなければリンク断と判定する．

・次ホップからのパケット受信
・次ホップへの RREQ 送信
・次ホップへの ICMP エコー要求

(6) 片方向リンクへの対応

片方向リンクを含むパスを経由して運ばれた RREQ に対して，終点が RREP を返した場合を考える．この片方向リンクの上流側のノードを a，下流側のノードを b とする．ノード b は RREP を受信するとノード a への転送を試みる．しかし，このリンクは片方向リンクであるため，RREP の転送は失敗する．この結果，RREP は RREQ の生成元まで届かず，経路発見は失敗する．RREQ 生成元のノードはタイムアウトにより経路発見の失敗を認識し RREQ の再送を行うが，再び，同様の失敗を繰り返す可能性がある．MANET 内に片方向リンクを含まないパスがあったとしても，そのパスが発見されない可能性がある．

このような問題に対応するため，ノード b では RREP の転送に失敗すると，ノード a をブラックリストに一定時間登録する. そして, ブラックリストに登録されたノードからの RREQ を受信しても廃棄し，再ブロードキャストを行わないことにする．これによって，片方向リンクを経由して終点に達する RREQ を防止することができる．その結果，双方向リンクのみを経由して終点に到達した RREQ に対して RREP が応答されることにより，双方向リンクのみからなる経路が確立する．

このためには RREP の転送失敗の検出が必要である．IEEE 802.11 のように，リンク層における確認応答が可能である場合，その情報をネットワーク層で利用可能にする方法がある．別の方法としてネットワーク層で RREP に対する確認応答を行う方法がある．これらの確認応答がタイムアウトになると RREP の転送失敗と判定する．

■参考文献

1) 間瀬憲一, 阪田史郎, “アドホック・メッシュネットワーク（ユビキタスネットワーク社会の実現に向けて）,” コロナ社, 2007.
2) 小牧省三, 間瀬憲一, 松江英明, 守倉正博, “無線 LAN とユビキタスネットワーク,” 丸善,2004.
3) C. Perkins, E. Belding-Royer and S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing,” RFC 3561, Jul. 2003.

2-2-4 位置情報利用ルーチングプロトコルとジオキャストルーチングプロトコル

（執筆者：朝香卓也）［2009 年 2 月 受領］

アドホックネットワークでは，ノードの存在する物理的な位置を利用，あるいは考慮したルーチングプロトコルの検討がなされている [1), 2)]．その代表的なものとして，位置情報利用ルーチングプロトコルとジオキャストルーチングプロトコルがある．位置情報利用ルーチングプロトコルでは，ノードの物理的な位置を各ノードが把握・管理しルーチングを行うものであり（**図 2･19**），ルーチングプロトコルのオーバヘッドの削減などの利点がある．また，位置情報利用ルーチングの一形態であるジオキャストルーチングプロトコルでは，ある特定の地域・領域に配置されたノード群のいずれかのノードに対してルーチングを行うものであり（**図 2･20**），始点ノードと終点領域間での通信を行うことで実現されるアプリケーションにおいて有効である．

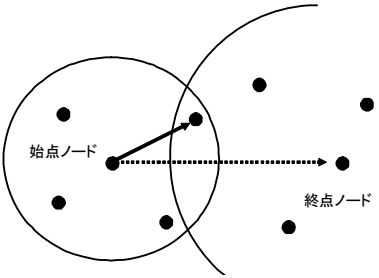


図 2・19　位置情報利用ルーチングプロトコル

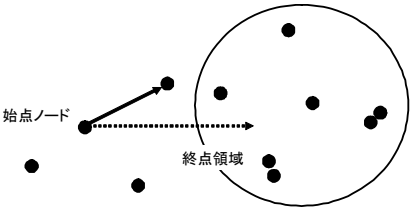


図 2・20　ジオキャストルーチングプロトコル

これらのプロトコルは，インターネットようにトポロジーベースでしかルーチングを行うことができないネットワークと異なり，リンクがアドホック的にしか存在せず，かつノードの物理的位置情報の存在を前提としたルーチングプロトコルとなっていることに特徴がある．一般性は必ずしも確保できないが，ネットワークのおかれた状況やアプリケーションによっては極めて有効なルーチングプロトコルとなることが期待されている．

位置情報利用ルーチングプロトコルでは，前提として GPS などを利用したロケーションサービスに基づき各ノードは自身の物理的な位置情報知ることができるとことを想定している．また，位置情報利用ルーチングプロトコルは，次ホップ転送方式と指向型フラディング方式に分類できる．

次ホップ転送方式では，各ノードは終点ノードへの前進距離が最も大きい，あるいは終点ノードにより近い場所にあるノードを次ホップノードとして選択する方式である．この方式では，始点ノードから終点ノードへの経路が存在したとしても，必ずしも終点ノードに到着するとは限らないものの，転送途中のノードで転送先ノードが見つからない場合における経路の再探索手法として様々なものが提案されている．

指向型フラディング方式は，終点ノードへ向かって中継ノードがブロードキャストを繰り返すことにより，パケットを配信する方式である．ノードの配置場所によってブロードキャストを行うかどうかを決定することにより，不要なブロードキャストを行うことを削減することができる．

ジオキャストルーチングプロトコルでは，終点領域を終点することで実現される．ジオキャストの実現方式としては，終点ノードの代わりに終点領域を用いることにより，前述の位置情報利用ルーチングプロトコルの考え方を直接利用することが可能である．

■参考文献

1) 間瀬憲一，阪田史郎，“アドホック・メッシュネットワーク（ユビキタスネットワーク社会の実現に向けて），” コロナ社，2007.
2) IEEE Computer Society LAN MAN Standards Committee, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Standard 802.11, 1997.

2-2-5 マルチキャストルーチングプロトコル

（執筆者：阪田史郎）［2009 年 1 月 受領］

アドホックネットワークにおけるマルチキャスト通信では，災害現場における被災者への緊急通報（被災状況通知，避難誘導，安否確認など），商品倉庫における管理端末への一斉通報，ショッピングモールなどにおける来場者への広告配信などへの広い応用が考えられる [1), 2)]．アドホックネットワーク用のマルチキャストルーチングプロトコル（以下，マルチキャストプロトコル）については，基本プロトコルの改良版を含めると 2008 年末現在既に 50 以上のプロトコルが論文などにより提案されているが，IETF（Internet Engineering Task Force）における標準化に関しては本格的な議論には至っていない．現在 MANET WG に提案されているのはマルチキャストの一種である MANET 全体へのブロードキャスト型の情報配信を行うプロトコルである．

マルチキャストでは，ユニキャストに比べてプロトコルの良否を決定づける要因の分類軸が多く，様々なトレードオフがあり，用途に応じたより多面的な評価が必要となる．リアクティブ型かプロアクティブ型かのほかにも主な分類軸として下記があげられる [3), 4)]．これら以外にも，表 2･2 の特性の列に示す各種の分類軸，アドホックネットワーク特有の LBM（Location-Based Multicast），GEOCAST などの位置情報補助型のマルチキャストプロトコルも提案されている．

(1) トポロジー：ツリー型／メッシュ型

インターネットにおける ALM（Application Level Multicast）と同様，マルチキャストのトポロジーに関して，ツリー型とメッシュ型がある．伝送効率あるいは伝送遅延については，冗長性を排除するツリー型の方が勝っている．ツリー型は，データの配信がツリー上で一意

に行えるため制御が容易，ループを回避できるなどの利点があるが，経路切断時にツリーを再構成が必要という欠点がある．冗長性をもたせたメッシュ型は，ツリー型とは逆に制御が複雑，ループを生成しやすいという欠点があるが，迂回路の設定が容易なため通信の高信頼化が図れるという利点がある．

また，ツリー型にはインターネットにおける IP マルチキャストと同様，マルチキャストグループの各ノードを送信元とする最短経路木を用いる送信元木による方式と，生成される木は最短経路木にならないが特定の中心的なノード（コアノード, Rendezvous Point などと呼ぶ）をルートノードとする共有木による方式がある．前者は後者に比べて，トラヒックの高負荷時においても高い性能を示すが，全ノードを送信元とする最短経路木を作る処理負荷のために大規模ネットワークには不向きで，スケーラビリティに欠ける．

表 2・2　マルチキャストプロトコルの比較

特性	AMRIS	CAMP	ODMRP	ABAM	DDM	AMRoute	PAST-DM	MAODV
トポロジ	共有木	送信元木	グループベースメッシュ	送信元木	送信元木	メッシュ上の共有木	メッシュ上の送信元木	共有木
ループ	なし	なし	なし	なし	なし	あり	あり	なし
制御パケットオーバヘッド	フラッディング	なし	周期的フラッディング	ツリーの生成と修復	周期的フラッディング	フラッディング	フラッディング	フラッディング
ルーティング制御のタイミング	プロアクティブ（テーブル駆動）	プロアクティブ（テーブル駆動）	リアクティブ（オンデマンド）	リアクティブ（オンデマンド）	リアクティブ（オンデマンド）	プロアクティブ（テーブル駆動）	プロアクティブ（テーブル駆動）	リアクティブ（オンデマンド）
ユニキャストルーティングプロトコルへの依存性	なし	あり	なし	なし	あり	なし	なし	なし
周期的メッセージ	あり	あり	あり	あり	あり	あり	あり	あり
スケーラビリティ	あり	あり	中間	なし	なし	なし	なし	あり
セッションの初期起動	送信側	受信側	送信側	送信側	受信側	送信側／受信側	送信側／受信側	受信側
トポロジのメンテナンス	ハードステート	ハードステート	ソフトステート	ハードステート	ソフトステート	ソフトステート	ソフトステート	ハードステート
実現レイヤ	ネットワーク層	ネットワーク層	ネットワーク層	ネットワーク層	ネットワーク層	アプリケーション層（オーバレイ）	アプリケーション層（オーバレイ）	ネットワーク層
特徴など	・比較的制御が容易で制御パケット数も少ない ・ビーコンを使うので帯域を圧迫しがち ・送信元から宛先までのホップ数が増大する傾向がある ・トラフィックの増大によって衝突が急激に増加	・衝突の増加によって制御パケットロスが増大し，経路再構築の遅延が大きくなる	・比較的制御が容易 ・他のプロトコルに比べ制御オーバヘッドが小さい	・ホップ数ではなくリンクの安定度で送信元木を作成するため配信率が高く，リンク断も少ないため制御パケット数も少ない ・宛先ノード数が多いと特定リンクにトラフィックが集中する	・状態管理が不要 ・10ノード程度までの小規模なネットワークで高い配信率を示す ・宛先ノードが多いと制御パケット数が増大する	・ループの発生で制御パケット数が増大する可能性がある ・メッシュ上に木を生成するため信頼性が高い ・ノードの移動が激しかったりネットワークが大きかったり(ノードが多かったり)すると，ホップ数が増加しやすく，コアノードの変化によるオーバヘッドが大きくなる ・トラフィック増大によりバッファオーバフローが発生しやすい	・他のプロトコルに比べて相対的に配信率が高い	・ユニキャストと共通にできるため制御パケット数が少ない ・ノードが密集したり，移動が激しかったりすると配信率が下がる

AMRIS: Ad hoc Multicast Routing protocol utilizing Increasing id-numberS　　CAMP: Core-Assisted Mesh Protocol
ODMRP: On-Demand Multicast Routing Protocol　　ABAM: Associativity-Based Ad hoc Multicast
DDM: Differential Destination Multicast　　AMRoute: Ad hoc Multicast Routing protocol
PAST-DM: Progressively Adaptive Subtree in Dynamic Mesh
MAODV : Multicast Ad hoc On-Demand Distance Vector routing

(2)　プロトコルの実現レイヤ：ネットワーク層／アプリケーション層（オーバレイマルチキャスト）

MANET WG では，ユニキャスト，マルチキャストいずれもネットワーク層におけるルー

チングを想定している．しかし，マルチキャストについては，インターネットにおけるマルチキャストと同様，通信効率を犠牲にしても，制御の複雑さを抑え，スケーラビリティを高めることを目的として，ネットワーク層ではなくアプリケーション層によるオーバレイマルチキャストの研究も盛んに行われている．

オーバレイマルチキャストについては，共有木における AMRoute，AMRoute における共有木が最短経路でないため低効率という欠点を送信元木にすることによって解決する PAST-DM，更に性能向上を図った ALMA（Application Layer Multicast Algorithm）などが代表的である．

(3) トポロジーのメンテナンス：ハードステート／ソフトステート

ハードステートでは，リンクが切断した場合のみ経路発見のための制御パケットを送出する．ソフトステートでは，最新の経路情報を保持するため，制御オーバヘッドを犠牲にして制御パケットを周期的にフラッディングする．したがって，通常はハードステートよりもソフトステートの方がパケット到達率が高いが，制御パケット数が多い．

表 2･2 に他の方式・パラメータを加えた主なマルチキャストプロトコルの比較を示す．

■参考文献

1) C. K. Toh, “Ad Hoc Mobile Wireless Networks －Protocols and Systems －,” Pearson Education, 2002.
2) C. S. R. Murthy and B. S. Manoj, “Ad hoc Wireless Networks,” Prentice-Hall, 2004.
3) 阪田史郎，青木秀憲，間瀬憲一, “アドホックネットワークと無線 LAN メッシュネットワーク,” 信学論, vol.J89-B, no.6, pp.811-823, Jun. 2006.
4) 間瀬憲一，阪田史郎（電子情報通信学会編），“アドホック･メッシュネットワーク －ユビキタスネットワーク社会を実現する技術,” コロナ社, Sep. 2007.

2-2-6 IP アドレス自動割当 [1), 2)]

（執筆者：間瀬憲一）［2008 年 8 月 受領］

(1) MANET ローカルアドレスの自動割当

2-2-1 項に述べたように，IP ネットワークにおいてはノードのリンクへの接続点（インタフェース）に対して IP アドレスが与えられる．アドレス体系が有効であるためには，アドレスが利用される一定の範囲が定められ, その中でアドレスの一意性が確保される必要がある．この範囲はスコープと呼ばれる．例えば，一つのリンクをスコープとするアドレスはリンクローカルアドレス，一つのサイトをスコープとするアドレスはユニークローカルアドレス，インターネット全体をスコープとするアドレスはグローバルアドレスなどと呼ばれる．一般にアドレスをそれぞれのスコープにおいて手動で重複なく割り当てるには多くの労力を要するため，自動的なアドレス割当手法が望まれる．

MANET のルーチングプロトコルは各ノードの MANET インタフェースに一意の IP アドレスが与えられていることを前提としている．そこで MANET をスコープとするアドレスが必要になる．これを MANET ローカルアドレスと呼ぶことにする．一つのノードが複数の MANET インタフェースをもつ場合にはそれぞれに一意の IP アドレスが必要であるが，以下では記述の簡単化のため，各ノードは一つの MANET インタフェースをもつものとし，ノードのインタフェースのアドレスを単にノードのアドレスという．

与えられたスコープにおいて IP アドレスを自動的に割り当てる仕組みとして，ステートフル型とステートレス型がある（**図 2･21**）．ステートフル型はスコープで利用可能な IP アドレスの全体（アドレス空間）において，使用中のアドレスを管理し，新たな割当要求が生ずると未使用のアドレスを選択し，割り当てるものである．この際，一旦割り当てたアドレスの使用状況を管理し，使用されなくなったアドレスを再利用する仕組みが必要になる．ステートフル型は通常使用中のアドレスを集中管理するサーバなどを必要とし，DHCP（Dynamic Host Configuration Protocol）はその例である．スタンドアローンの MANET では各ノードが対等の関係でネットワークを作るのが基本になる．どのノードも MANET への出入りが自由である．こうした環境で，特定のノードにアドレス集中管理・割当のためのサーバをもたせることは困難である．そこで，ステートフル型の場合にはアドレス管理・割当サーバの機能を各ノードに分散する仕組みが必要になり，そのための制御メッセージに起因するオーバヘッドも大きくなる．

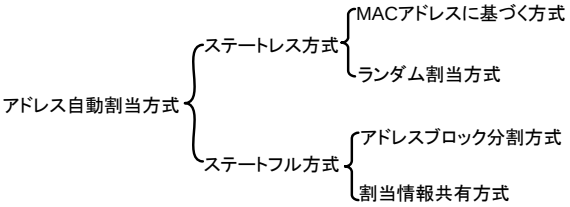


図 2・21　自動アドレス割当方式の分類

（出典：小牧省三，間瀬憲一，松江英明，守倉正博「無線 LAN とユビキタスネットワーク」丸善，2004）

ステートレス型は使用中のアドレスとは独立にアドレス割当を行うものである．MAC アドレスなど下位層が提供するアドレスの一意性を前提として，そのアドレスから IP アドレスを生成する方法，アドレスを対象とするスコープで利用可能なアドレス空間からランダムに選択する方法などがある．ステートレス型は集中管理のためのサーバを必要としないので，MANET 環境で実現しやすいメリットがある．

どのような IP アドレス自動割当方式を採用するにせよ，異なるノードに誤って同じアドレスを割り当てる可能性が考えられる．アドホックネットワークの利用環境では，ノードはその利用期間中に他の多くのノードと出会う可能性があり，LAN のような静的なネットワークに比べて重複アドレスが生ずる可能性は高い [3]．また，アドホックネットワークでは各データパケット，制御パケットの転送オーバヘッドを削減し，無線通信帯域を有効利用するため，IPv6 のような広いアドレス空間の利用が適さず，短いアドレス長が使用される場合もあり，重複アドレスの可能性が増加する [4]．ステートレス型のランダム割当では確率的に重複アドレスが生ずる可能性がある．IPv6 の場合，一般にアドレス空間を広くとることが可能であり，アドレス重複の可能性を十分低くすることができる．しかし，アドレス空間を狭くすることにより制御メッセージ内に含まれるアドレス情報の圧縮効率向上が期待できる [5]．そのような場合には重複アドレスが生ずる可能性が高まることになる．更に，アドホックネットワークでは，ノードの移動により，ネットワークがいくつかの部分に分割されることがあり得る．それぞれの分割（Partition）内ではノードが相互に通信可能であるが，異なる分割のノード間では通信できない．このような状況で，それぞれの分割内で独立に IP アドレス割当が進行す

る. 分割された, あるいは元々独立に発生した MANET が合流（マージ）するとき（**図 2･22**）, 重複アドレスが生ずる可能性がある.

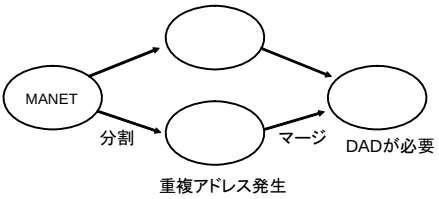


図 2・22　アドホックネットワークの分割・マージと重複アドレス検出（DAD）の必要性

（出典：小牧省三, 間瀬憲一, 松江英明, 守倉正博「無線 LAN とユビキタスネットワーク」丸善, 2004）

重複アドレス検出（DAD：Duplicate Address Detection）の仕組みとして, プリサービス DAD, インサービス DAD の二つのタイプが考えられる. 前者は新たに生成され使用前のアドレスと他の使用中, 使用予定のアドレスとの間の重複, 後者は既に使用中のアドレスと他の使用中のアドレス間の重複を検出するものである.

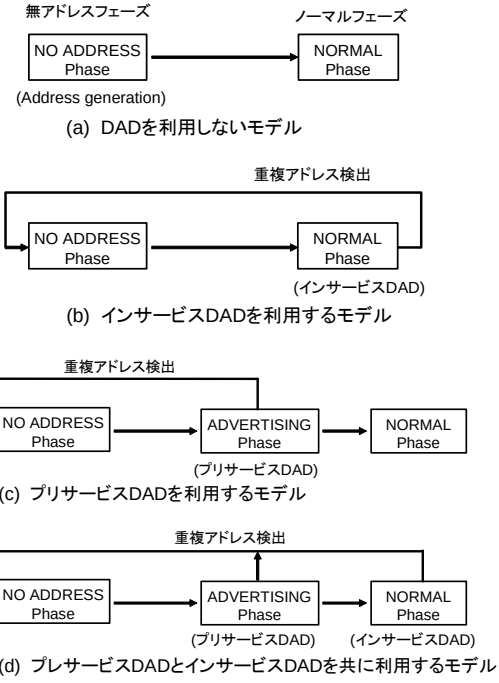


図 2・23　MANET における重複アドレス検出のモデル

（出典：間瀬憲一, 阪田史郎「アドホック・メッシュネットワーク」コロナ社, 2007）

図 2･23 に MANET のアドレス管理に関する四つのモデルを示す．図(a) は DAD を行わない方式であり，アドレスなしの状態においてアドレス生成後，直ちにノーマル状態に移行し，MANET に参加する．図(b) ではノーマル状態においてインサービス DAD を行い，重複アドレスが検出されるとアドレスなしの状態に戻る．図(c) ではアドレスなしの状態で生成されたアドレスは暫定アドレスとされ，広告状態へ移行する．広告状態では暫定アドレスに対してプリサービス DAD が実施される．ここで重複アドレスが検出されるとアドレスなしの状態に戻る．ノーマル状態ではインサービス DAD を行わない．図(d) はプリサービス DAD，インサービス DAD を共に行うフルセットのモデルである．どのモデルを採用するかはアドレス空間の広さ，アドレス生成方式，DAD による制御オーバヘッド，アプリケーションなどを総合的に勘案して決定することになる．プリサービス DAD，インサービス DAD の仕組みが必要である．

(a) プリサービス DAD

プロアクティブ型ルーチングプロトコルではノードは周期的なルーチングメッセージの交換を行うので，これを利用して暫定アドレスの広告が可能である．例えば，OLSR では広告状態のノードは MPR 選択を行うことにより，自身の暫定アドレスが，MPR が生成する TC メッセージにより，MANET 全体に広告される．逆に，受信する TC メッセージから MANET 内のすべてのアドレス情報が得られるので，アドレス重複の検出が可能である．この方法ではプリサービス DAD のための新たな制御メッセージは不要である．

リアクティブルーチングプロトコルではノードが新たに MANET に参加する時点で，アドレス要求（AREQ：Address Request）メッセージを送出する．AREQ は AODV の RREQ と同様のフォーマットとし，生成元アドレスには暫定アドレスとは別に，専用のアドレスブロックから選択した一時アドレスを使用し，終点アドレスには暫定アドレスを載せる．この暫定アドレスを既に利用中のノードは，この AREQ を受信したときアドレス応答（AREP：Address Reply）メッセージを生成元に返すことにより，アドレス重複を通知する．AREQ 生成元のノードは一定回数 AAREQ を行い，AAREP を受信せずタイムアウトとなればアドレス重複はないと判定する．AREP を受信した場合にはそのアドレスを放棄し，新たにアドレス生成を行う [6]．

(b) インサービス DAD

インサービス DAD は使用中のアドレスについて重複の有無を検査する方式であり，受信するルーチングメッセージを観察し，重複アドレスまたはその可能性を検出するものである．以下に二つの方法を紹介する．これらの方式は原理的にはプロアクティブ型，リアクティブ型ルーチングプロトコルのどちらにも適用できる．

(1) アドレス識別子付加方式 [7]

アドレス生成において，本来のアドレスに加えて数オクテットの識別子をランダムに生成し付加する．ルーチングプロトコルはこの識別子が付いたアドレス（拡張アドレス）を用いてルーチング処理を行う．このため，アドレス部が同じであっても識別子が異なることにより，重複アドレスの検出が可能である．見かけ上アドレス空間を拡張した効果が現れるが，データパケットの IP ヘッダに含める始点，終点アドレスはあくまで本来のアドレスである．

(2) パッシブ DAD 方式 [3)]

自身が生成・送出したルーチングメッセージ，過去に受信したルーチングメッセージ，新たに受信したルーチングメッセージの情報内容を照らし合わせ，矛盾，一貫性の欠如などを検出することにより，重複アドレスを検出する方法である．例えば OLSR において，各ノードは自身が生成・送出した TC メッセージのコピーの圧縮情報を保存しておき，自身と同じアドレスを生成元とする TC メッセージを受信した場合，保存しておいた情報と照らし合わせることにより，自身が生成・送出した TC メッセージか，他のノードが生成・送出したメッセージか識別できるので，後者であれば重複アドレスありと判定する．より簡単に，受信した TC メッセージのシーケンス番号が自身のシーケンス番号より大きい，または一定数以上小さい場合には自身が過去に送出した TC メッセージではなく，他のノードが生成・送出した TC メッセージと推定できるので，重複アドレスありと判定することも可能である．シーケンス番号を利用する方法は第 3 者のノードが重複アドレスを検出する場合にも利用可能である．また，各ノードが自身の隣接ノードの履歴，MPR 選択の履歴を記録しておくことも有用である．受信した TC メッセージに含まれる隣接ノードのアドレスの中に，自身のアドレスを検出した場合，自身が過去にこの TC メッセージの生成元と隣接関係にあったか，そのノードを自身の MPR として選択したことがあったか，などを調べ，そのようなことがなければ重複アドレスありと判定できる．

(2) グローバルアドレスの自動割当

接続型 MANET では，MANET のいくつかのノードがインターネットと接続し，インターネットと MANET 間のゲートウェイ（Internet gateway：IGW）として機能することにより，インターネットに直接接続していないノードも IGW を介してインターネットとの通信が可能になる．IGW となるノードは MANET インタフェースに加えて，インターネット内の固定のアクセスルータ（Access Router：AR）への有線／無線インタフェース，及びグローバルアドレスとプレフィックスを有する．IGW として動作するノードも MANET ノードの一つであり移動する場合もあり，インターネットとの永続的な接続が保証されるわけでもない．したがって，IGW に NAT のような処理負荷の高い特別の役割をもたせる方法は適切ではない．

このような環境で MANET 内のノードとインターネット側のノード（以下ではそれぞれ MANET ノード，インターネットノードと呼ぶ）が，IGW の一つを経由して通信可能とするため，MANET ノードにグローバルアドレスをもたせる方法が考えられる．具体的には MANET ノードは選択した IGW のプレフィックスを用いてグローバルアドレス（気付けアドレス）を生成する．これによって，インターネットノードが送信したパケットはこの IGW を経由して MANET ノードに到達する．逆に，MANET ノードが送信したパケットはこの IGW を経由してインターネットノードに到達する．

MANET ノードが気付アドレスを生成するためには，IGW の一つを選択し，選択した IGW に対応するプレフィックスを知る必要がある．このため各 IGW は自身の IGW 情報（IP アドレス，プレフィックスなど）を周期的，あるいはノードからの要求に基づいて MANET 内に送信する．これを IGW 広告と呼ぶ．IGW 広告はフラッディングプロトコルなどを利用して，MANET 全体にブロードキャストされる．各ノードは受信した IGW 広告に含まれる IGW までのホップ数などの情報に基づいて IGW を選択する．**図 2･24** に MANET ノードが IGW を

経由してインターネットノードと通信する概念図を示す.

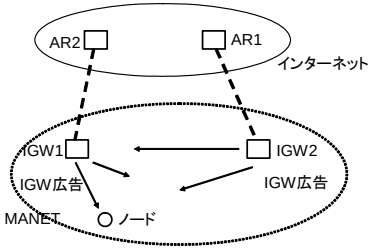


図 2・24　MANET のインターネット接続概念図

（出典：間瀬憲一, 阪田史郎「アドホック・メッシュネットワーク」コロナ社, 2007）

複数の IGW をもつ MANET においては, MANET ノードが送信したパケットは原理的にはどの IGW を経由しても宛先インターネットノードに到達すると考えられる．しかし，パケットの送信元アドレスのプレフィックスが IGW に割り当てられているプレフィックスと異なる場合，そのパケットは中継されない場合がある．MANET ノードがインターネットノードに送信したパケットを選択した IGW に到達させるため，ルーチングヘッダを用いる方式，プレフィックス連続法が提案されている [8]．前者ではインターネットへ向かうパケットの終点アドレスには選択した IGW の IP アドレス，ルーチングヘッダに最終的な終点アドレスを設定する．後者では，各 MANET ノードは複数の IGW から IGW 広告を受取ると，ホップ数などのメトリックに基づき，IGW の一つを選択し，選択した IGW 広告のみ再ブロードキャストを行う．これによりインターネットへ向かうパケットは，同じ IGW を選択した上流ノードのみを経由して IGW に到達する．**図 2･25** にプレフィック連続法の概念図を示す.

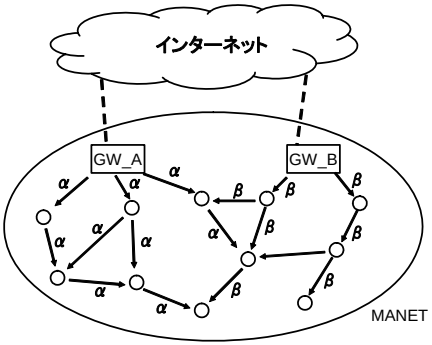


図 2・25　プレフィックス連続法

（出典：間瀬憲一, 阪田史郎「アドホック・メッシュネットワーク」コロナ社, 2007）

MANET ノードがグローバルアドレスを獲得して通信開始後，利用中の IGW から離れた場所に移動することが考えられる．このとき，別の IGW が近くにあったとしても元の IGW の利用を続けると，MANET 内でのホップ数が増し無駄なトラヒックを発生させることになり，

通信品質の劣化も生ずる．もし，ホップ数が少なくて済む近くの IGW へ切替えを行えば，MANET 負荷の軽減，通信品質の向上が期待できる．そこで，インターネットノードと通信を行うノードは，移動中に現行の IGW より条件の良い IGW が見つかれば，その時点でその IGW へ切替えを行うことが考えられる．利用中の既存アドレスの利用を中断し，新たな IGW が広告するプレフィックスを用いて気付けアドレスを新たに生成・設定する．この場合，アドレス変更によりアプリケーションが中断する問題がある．また，このアドレスに関係する経路が MANET 内に再構築されるまで一定の時間を要し，その間，パケット転送の中断が起こることになる．したがって，IGW 切替えの発動は必要最小限とすることが望ましい．

■参考文献

1) 間瀬憲一, 阪田史郎, “アドホック・メッシュネットワーク（ユビキタスネットワーク社会の実現に向けて）,” コロナ社, 2007.
2) 小牧省三, 間瀬憲一, 松江英明, 守倉正博, “無線 LAN とユビキタスネットワーク,” 丸善, 2004.
3) K. Weniger, “PACMAN: Passive Autoconfiguration for Mobile Ad hoc Networks,” IEEE Journal of Selected Areas of Communications (JSAC), vol.23, no.3, Mar. 2005.
4) J. Boleng, “Efficient Network Layer Addressing for Mobile Ad Hoc Networks,” in Proc. of Int. Conf. on Wireless Networks (ICWN ’02), pp.271-277, Las Vegas, Jun. 2002.
5) T. Clausen, C. Dearlove, J. Dean, and C. Adjih, “Generalized MANET Packet/Message Format,” draft-ietf-manet-packetbb-04, Work in Progress, Jan. 2007.
6) C. E. Perkins, J. T. Malinen, R. Wakikawa, E. M. Belding-Royer, and Y. Sun, “IP Address Autoconfiguration for Ad Hoc Networks,” draft-ietf-manet-autoconf-01.txt, Nov. 2001.
7) N. H. Vaidya, “Weak Duplicate Address Detection in Mobile Ad Hoc Networks,” in Proc. of ACM MobiHoc 2002, pp.206-216, Lausanne, Switzerland, Jun. 2002.
8) P. M. Ruiz, F. J. Ros, and A. Gomez-Skarmeta, “Internet Connectivity for Mobile Ad Hoc Networks: Solutions and Challenges,” IEEE Communications Magazine, pp.118-125, 2005.

■4 群 － 5 編 － 2 章

2-3 アドホックネットワークの応用システム

2-3-1 車々間通信（VANET）[1)]

（執筆者：間瀬憲一）［2008 年 8 月 受領］

(1) VANET の概要

交通事故による死傷者増加，環境への悪影響は大きな社会問題になっており，自動車運転の高度安全化，効率化，快適化などを目的として新たなサービスを創出するため，多くの取り組みや共同実験プロジェクトが行われている．サービスには車そのものに関するもの（保守など），運転に関するもの（安全性，効率性など），利用者に関するもの（情報収集，娯楽など）がある．自動車に各種センサ機能を搭載し，自動車内部，自動車相互や外部との通信手段をもたせることで，これらの多彩なサービスの実現が可能になると考えられる．

自動車内部の通信にはLANを装備し，自動車と外部の通信には従来の移動通信や無線LANの技術を適用することが考えられる．一方，自動車相互の通信（車々間通信）には MANET の利用が考えられる．車々間通信に適用されるアドホックネットワークは VANET（Vehicular Ad hoc NETwork）と呼ばれる．自動車には GPS やディジタル道路地図を利用するカーナビゲーションシステムが標準装備化されつつあり，これらを利用することで，VANET に特化した効率的な情報配信実現の可能性もある．車々間通信は，特に車同士の交通事故防止や周辺の交通状況把握のため有望な技術と考えられる．

(2) VANET の特徴

車々間通信を従来型の移動通信を利用して行うことは可能であるが，国全体の道路をすべてセルでカバーするためには膨大な投資が必要になる．VANET はセルの内外にかかわらずサービスが可能であり，また，セルのカバー範囲においてもより効率的で低コストとなる場合もあり得る．利点として次の三つがあげられている [2)]．

(1) 安全に関する情報の許容時間内の低遅延転送
(2) 低通信コスト
(3) 位置情報に基づく近隣車への通信

携帯 PC，PDA などの移動ノードにより構成される通常の MANET と比較し，VANET は以下の特徴を有する．ここで車そのものもノードと呼ぶ．

(1) VANET に参加するノードは常に変化し，広大なエリアに散在する．
(2) ノードの移動範囲は道路，交差点などの物理的構造に従う．
(3) ノード密度と速度は場所と時間により大きく変化し，大きな相関を有する．
(4) 十分な電力供給が可能である．
(5) 各ノードは GPS などを利用し，自身の位置情報を認識可能である．また，ディジタル道路地図も利用可能である．
(6) 各ノードは複数の無線インタフェースをもち，複数チャネルを利用可能である．これによる重量増とコスト増は許容される．
(7) 車々間通信は地理的に近く，匿名のノード間で行われることが多い．
(8) 各ノードは多くのセンサをもち，データを周期的／随時に，また独立／同期して発生

する．情報量は比較的少なく周期的に発生し，許容時間内に転送される必要がある．

(9) メッセージの緊急性により，メッセージ伝送に優先性の考慮が必要である．

(10) 車以外に道路沿いに固定ノードを設置しておき，VANET に参加させることも可能である．これらのノードはセンサや交通信号機の制御機能を有し，インターネットなどの固定網へのゲートウェイとして利用される．また，車々間通信，路車間通信における情報の一時的な保管場所として利用も考えられる．

(3) VANET アプリケーションと技術課題

VANET には多くのアプリケーションが考えられ，以下の三つに分類される．

- **運転支援サービス**：このサービスの目標は交通事故を減らし，運転の安全性と効率を増加させることである．例えば，急ブレーキ情報を即座に後続の車へと伝搬させ，追突事故を防止する．車の位置や速度を近くの車とやり取りすることにより，車線変更，車線合流，交差点通過などを安全に効率的に行うための協調的運転を支援する．
- **道路交通情報サービス**：このサービスの目標は運転者に周辺（例えば半径数 10 km 以内）の道路の交通情報を知らせるものである．例えば，道路を長さ 500 m ごとの区間に分割し，各道路区間の車の平均速度を通知する．このようなサービスは集中管理型のシステムでも実現できるが，車々間通信による自律分散型のシステムにより，より効率的・経済的に実現できる可能性がある．
- **ユーザ通信・情報サービス**：このサービスの目標は，他の車との間で駐車場やガソリンスタンドなどの情報を交換したり，道路沿い設置された固定ノードを利用してインターネット接続を提供することである．

VANET アプリケーションを実現するには，物理層・データリンク層，ネットワーク層，トランスポート層，応用層にわたる各種の技術課題がある．

物理層・データリンク層では，任意の車々間，路車間でのアドホック通信機能が必要であり，無線 LAN/MAN 技術の利用が考えられる．車々間には現状で利用可能なものとして IEEE 802.11a/b/g/n などの無線 LAN 規格がある．また，車々間通信用に IEEE 802.11a をベースとして IEEE 802.11p の標準化が進んでいる．ITS（高度道路交通システム）において路車間，車々間の双方向ブロードバンド通信を用途としては専用狭域通信（DSRC：Dedicated Short Range Communication）の標準化とシステム開発が日本，欧米で進められている．我が国では路車間通信を対象とし，ETC を含めた DSRC システム（ARIB STD T-75）が標準化された．米国では IEEE 802.11p と上位レイヤの IEEE 1609 規格からなる WAVE（Wireless Access in Vehicular Environments）の開発が進められている．これらの技術の VANET への利用が考えられる．また，路車間には MAN に分類される IEEE 802.16e 規格の利用も考えられる．

ネットワーク層では，ルーチングプロトコル，IP アドレスオートコンフィギュレーションなどが課題である．MANET を対象として各種ルーチングプロトコルが提案され，IETF で標準化も進展しているが，これらは(2) 項で述べた VANET の特性には必ずしも適合するものとはいえない．VANET では各ノードが GPS やその他の方法で自身の位置情報を認識していると想定されるため，位置情報利用型のルーチングプロトコルが有望と考えられる．位置情報利用型のルーチングプロトコルの標準化検討には手がつけられていない．

トランスポート層では TCP と UDP があるが，特に TCP についてノード移動に伴うリンク

状態の変化やマルチホップの性能への影響など，MANET，VANET 環境特有の課題がある．

応用層では上述したアプリケーションの実現に有用で共通的な機能要素を確立することが重要である．

更に，性能改善のための層横断的な種々の課題がある．ITS 関連技術の国際標準化は ISO/TC 204 で扱われている．車々間通信についても検討対象であるが，VANET の適用は今後の課題と考えられる．

■参考文献

1) 間瀬憲一，“車々間通信とアドホックネットワーク”，電子情報通信学会論文誌，vol.J89-B，no.6，pp.824-835，2006.
2) H. Hartenstein, B. Bochow, A. Ebner, M. Lott, M. Radimirsch, and D. Vollmer, “Position－Aware Ad Hoc Wireless Networks for Inter－Vehicle Communications: the Fleetnet Project”, Proc. ACM MobiHoc’01, 2001.

2-3-2 無線 LAN メッシュネットワーク

（執筆者：阪田史郎）［2009 年 3 月 受領］

(1) 無線 LAN メッシュネットワークの概要と現状

一般に，モバイルアドホックネットワークが，ネットワークを構成する全ノード，すなわち基地局（無線 LAN ではアクセスポイント，以下 AP）も端末もすべて経路制御，中継を行うのに対し，メッシュネットワークでは，端末は経路制御，中継を行わない．すなわち，無線 LAN メッシュネットワークではメッシュ状に接続された AP のみが経路制御，中継を行い，既存の端末は変更することなくそのまま利用できる．メッシュネットワークの目的としては，面的な広がりのほかに，1 台の AP に集中する負荷の複数 AP への分散による全体性能の向上，メッシュ構成を利用した迂回路の設定により 1 台の AP の障害が引き起こすネットワーク全体の障害（Single Point of Failure：SPF）の回避などがある．**表 2･3** に両者の比較を示す [1)-3)]．

表 2・3　モバイルアドホックネットワークとメッシュネットワーク

	モバイルアドホックネットワーク	メッシュネットワーク（将来の本格的なモバイルアドホックネットワークに向けた前段の現実解）
利　用	当面：戦場，災害時などの一時的な利用 将来：平常時の利用 （実用ネットワークは未だ殆どない）	定常的に利用 （非標準，独自仕様の無線LANメッシュネットワークの製品は多い．主に海外で公共のセキュリティやそのためのビデオ監視等に多く利用されている．）
ネットワークトポロジー	端末の移動を前提とするため動的に変化	基地局／アクセスポイントのみでメッシュを構成するためトポロジーの変化はない
物理ネットワーク	問わない	無線LANを対象として標準化（IEEE 802,11s）、無線MAN（WiMAX）においても中継機能（IEEE 802.16j）を標準化済
標準化機関	IETF MANET WG	IEEE 802
ルーティングの実現レイヤ	レイヤ3（ネットワーク層）	レイヤ2（MAC層）

技術の現状や，端末の負荷とそれに伴う消費電力，他人の携帯端末を中継のために使用することによって起こり得るセキュリティの問題や社会的認知などの問題を考慮すると，モバイルアドホックネットワークの早期普及は難しく，まず無線 LAN メッシュネットワークの利用の進展が期待される．

無線 LAN メッシュネットワークの標準化については，2003 年に IEEE 802.11s タスクグループが発足し，2010 年中に最終仕様が規定される予定である．製品については，MeshNeworks 社（2004 年に Motorola 社が買収）が 2002 年に発売した MEA（Mesh Enabled Architecture）が最初とされ，その後 2005 年頃から米国を中心とする 10 を超える企業から非標準の製品が発表され，実用化が進展しつつある．しかし，これらの製品は独自仕様で異なる製品間での相互接続性がないため，面的な広がりを実現することが困難なだけでなく，標準仕様でないがために量産化に向けた小型化・軽量化も難しく，普及に至っていない．また，利用の大部分が防犯・防災などの公共の安全向けに留まっており，ビジネス面での広がりは 2009 年段階では限定的である [4]．

(2) 無線 LAN メッシュネットワークの標準仕様の概要

IEEE 802.11 ワーキンググループにおいて，2004 年 7 月に IEEE 802.11s タスクグループが発足し，無線 LAN メッシュネットワークの標準化が開始された．2005 年 6 月には合計 15 件の技術提案が行われ，投票・各提案方式の一本化作業の後，2006 年 1 月に Draft 0.01 版が発行された．2009 年 3 月末現在 Draft 2.07 版(4) の修正中で，2010 年 9 月に標準規格が完成する予定である [4), 5)]．IEEE 802.11s は上記のように，MAC 層の仕様であり，物理層の無線 LAN としては，IEEE 802.11b, a, g, n が利用される．

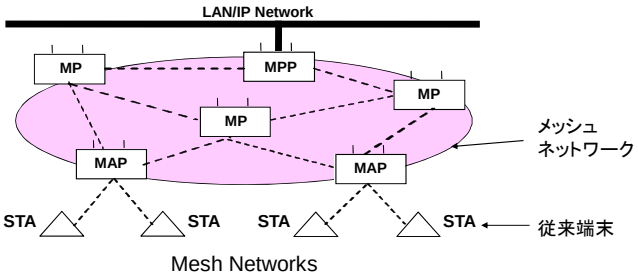
(a) メッシュネットワークの利点と適用領域

メッシュネットワークの利点として，①通信領域の拡大，②設置の容易性，③冗長構成による信頼性の向上，④通信距離短縮による高速化，⑤消費電力の低減，⑥周波数の空間的再利用によるネットワーク容量の増大，があげられる．

メッシュネットワークの用途としては，従来の無線 LAN では困難であった機器間の直接接続や新規に有線通信インフラの設置が困難な屋外通信などに主眼が置かれている．具体的には，①家庭内での AV 機器間の接続，②オフィス内でプリンタ・会議システム・プロジェクタなどの接続，③キャンパス，災害時における屋外での通信手段の確保，などを想定している．

(b) ネットワーク構成とアーキテクチャ

IEEE 802.11s で規定する無線 LAN メッシュネットワークは**図 2･26** に示すように，複数の装置が相互に接続してマルチホップの無線ネットワークを構成する．無線 LAN メッシュネットワークのアーキテクチャに相当する，ネットワークを構成する各ノードの機能構成を**図 2･27** に示す．



総称して： mesh STA

・Mesh Point (MP)： 無線LANメッシュネットワークを構成するためのメッシュ機能を実装.

・Mesh Access Point (MAP)： メッシュ機能とAPの機能を実装. 無線LANメッシュネットワークの構築だけでなく, メッシュ機能を実装していない無線LAN端末のStationも収容.

・Mesh Point collocated with mesh Portal (MPP)： メッシュ機能とメッシュネットワークから他のネットワークとの接続のためのゲートウェイ機能を実装.

図 2・26 IEEE 802.11s におけるノード構成

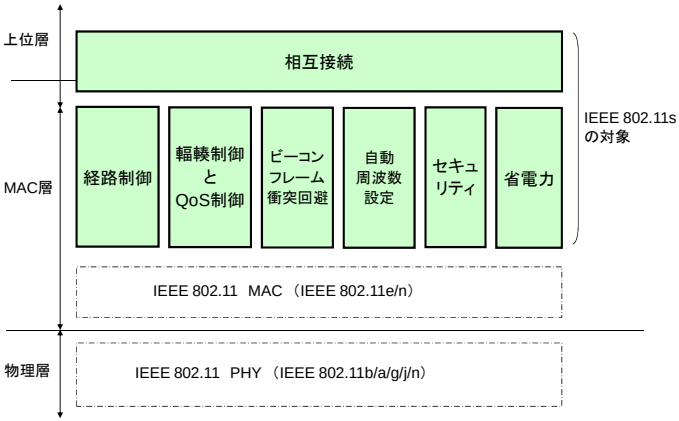


図 2・27 IEEE 802.11s アーキテクチャ

IEEE 802.11s では 32 台（最大 5 ホップ）程度の MP で構成される小中規模の無線 LAN メッシュネットワークを想定している．実際には各 MP に端末（STA）が接続するため，ネットワーク全体の収容端末数は数百台規模となる．また，複数の無線 LAN メッシュネットワークが有線ネットワークを経由，もしくは直接接続することにより，無線 LAN メッシュネットワークの規模を拡大することが可能である．

(c) 経路制御

IEEE 802.11s における経路制御プロトコルは，Hybrid Wireless Mesh Protocol（HWMP）と呼ばれる．HWMP は①通信開始前に事前にツリー状に経路を決定する Proactive tree building

mode と，②トラヒック発生時に経路を決定するリアクティブ型の AODV を踏襲した On demand mode の 2 種類が定義されている．これらは同時に使用することができる．例えば，メッシュネットワークが構築された直後は Proactive tree building mode で経路を構築し即時に通信を開始し，その後で最適経路を構築することが可能である．

経路選択のための指標には，Airtime link metric と呼ばれる無線状況を反映したメトリックの使用が必須である．Airtime link metric は式(1) で定義される．

$$C_a = \left[O + \frac{B_t}{r} \right] \frac{1}{1 - e_f} \tag{1}$$

O はチャネルアクセス時のオーバヘッド時間，B_t はテストフレーム長（8192 bit を推奨），r は各リンクの物理層の速度，e_f はフレーム誤り率である．経路全体のメトリックは，経路構築開始時に送信される Path Request フレームに各無線リンクの Airtime link metric を中継 mesh STA が累積することにより算出される．送信元 mesh STA は累積されたメトリックが最小となる経路を選択し，結果として遅延やエラーの少ない通信が可能となる．また，フレームフォーマットに高い柔軟性をもたせることで，ベンダー独自の経路制御プロトコルやメトリックを使用することが可能となるよう配慮されている．

■参考文献

1) 阪田史郎, 青木秀憲, 間瀬憲一, “アドホックネットワークと無線 LAN メッシュネットワーク,” 信学論, vol.J89-B, no.6, pp.811-823, Jun. 2006.
2) 間瀬憲一, 阪田史郎（電子情報通信学会編）, “アドホック・メッシュネットワーク －ユビキタスネットワーク社会を実現する技術,” コロナ社, Sep. 2007.
3) “Special issue on wireless mesh networks: applications, architectures, and protocols,” IEEE Network Magazine, vol.22, issue 1, Jan.-Feb. 2008.
4) 阪田史郎, 山田 暁, 飯塚宏之, 伊藤哲也, “無線 LAN メッシュネットワーク技術,” 信学誌, vol.92, no.8, Aug. 2009.
5) G. R. Hiertz, Y. Zang, S. Max, T. Junge, W. Weiss, B. Wolz, D. Denteneer, L. Berlemann, and S. Mangold, “IEEE 802.11s: WLAN mesh standardization and high performance extensions,” IEEE Network, vol.22, no.3, pp.12-19, May-Jun. 2008.

2-3-3 センサネットワーク

（執筆者：阪田史郎）［2009 年 1 月 受領］

アドホックネットワークの形態をとるネットワークの一例として，無線によるセンサネットワークがある. センサネットワークでは, ネットワークを構成するシンクノード（Sink Node）と呼ばれる一つのノードに，一般に複数のセンサから計測・認識されたセンシングデータを収集するトラヒックが代表的な情報の流れとなる．当面の利用が，シンクノードもセンサも移動を想定しないため，電池切れによるノードの消滅以外ではトポロジーが変化しないアドホックネットワークとなる [1].

2008 年末現在，センサネットワークとして標準化が進展し製品化も進展している代表例として ZigBee がある [2]. ZigBee は, センサネットワーク用の物理層と MAC（Media Access Control）層として標準化された IEEE 802.15.4 を採用し, ネットワーク層とその上位のプロトコルについては，業界団体の ZigBee Alliance がその標準化を推進している．ネットワーク層における

ルーチング制御として，シンクノードへのルートが常に固定のクラスタツリーと，IETF の MANET WG において標準化された AODV を規定している．比較的小規模なネットワークではクラスタツリー, 中規模以上のネットワークでは AODV を利用することが想定されている．リアクティブ（オンデマンド）型の AODV が選ばれた理由は，センサネットワークにおいて特に要請が強い，極力低い消費電力を実現するためである．

ZigBee は，シンクノードに対応する ZigBee コーディネータ，センサそのものに対応する ZigBee エンドデバイス, ZigBee エンドデバイスの接続とセンシングデータの中継の機能を提供する ZigBee ルータの 3 種類のノードから構成される．物理的には，ZigBee コーディネータと ZigBee ルータがルーチング機能を有する FFD，ZigBee エンドデバイスがルーチング機能をもたない（センシングデータを ZigBee コーディネータか ZigBee ルータに渡すのみ）RFD として，それぞれ実装される．**図 2･28** に ZigBee のネットワークモデルを示す．

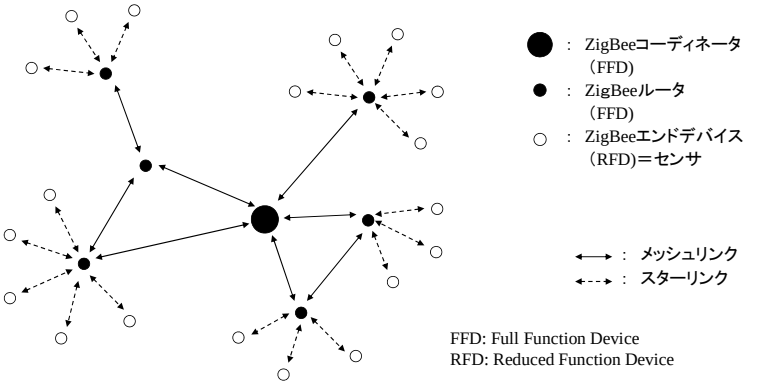


図 2・28　ZigBee のネットワークモデル

将来，防犯・防災，環境モニタリングなどを目的とした広域センサネットワークや，多くのセンサを装着したロボット間の協調作業による工場，商品倉庫，建設現場におけるセンサネットワーク，あるいは情報家電ネットワークと連携したセンサネットワークなどが実用化されると，モバイルを含めたアドホックネットワーク技術のセンサネットワークへの応用が進展する [3].

■参考文献

1) 間瀬憲一, 阪田史郎（電子情報通信学会編）, “アドホック･メッシュネットワーク －ユビキタスネットワーク社会を実現する技術,” コロナ社, Sep. 2007.
2) 阪田史郎編著, “ユビキタス技術　センサネットワーク,” オーム社, May 2006.
3) 阪田史郎, “センサネットワークの最新動向,” ケミカル・エンジニアリング, Nov. 2007.

■4群 － 5編 － 2章

2-4 アドホックネットワークの性能

2-4-1 ネットワークレベルの性能

（執筆者：間瀬憲一）［2008年8月 受領］

(1) 物理層

アドホックネットワークでは一般にノードは移動体であり，人間が歩行時に携帯する場合や乗り物に乗って高速で移動する場合も考えられる．各ノードの動きは予め調整されているわけではなく，独立に動く場合もある．このためフェージングが生じ，ノード間の電波伝播特性，電波の到来方向，妨害波による干渉状態などが急激に変化することも想定される．このような無線チャネル特性の急激な変化がネットワーク性能に大きく影響を与える．

アドホックネットワークではノードが電池駆動である場合が多い．ノードの連続利用時間を延長するには，エネルギー消費を低下させる手段が必要である．このために送信電力を低下させると，電波が届く距離が短くなり，他のノードと通信できなくなることも考えられる．また，受信可能（リッスン）状態を維持することにもエネルギーが消費される．ノードの無線送受信機をスリープ状態にすることにより，電池寿命を延ばすことができるが，スリープ状態の間は通信が不可能になる．したがって，これらの制御は物理層だけで対応するには限界があり，上位層と連携することが不可欠になる．

(2) データリンク層

複数のノードの送信機がチャネルを共有し，データパケットを送信するシステムにおいて，複数の送信機が同時にデータパケットをチャネルに送出すると，データパケットが衝突し，正常な送信ができなくなる．特定のノードがチャネルを占有することなく公平に，かつ効率的に通信路を利用できるメカニズムが必要である．これは複数の利用者が同一のチャネルを共有するシステムに共通する問題であり，メディアアクセス制御と呼ばれる．IEEE 802.11 形の無線 LAN を利用するアドホックネットワークでは，CSMA/CA（Carrier Sense Multiple Access with Collision Detection）と呼ばれるメディアアクセス制御 [1] が使用される．キャリアセンスとは通信機がパケットを送出する前に通信路の状態を調べ，搬送波が検出されればパケット送出を停止し，通信路が空いてからパケットを送出する方式である．

キャリアセンスは衝突を完全に防止することはできない．例えば，**図 2･29** において，ノード A がノード B にパケットの送信を試みる場合を考える．このとき，既にノード C がノード B に通信中であるとする．もし，ノード A がノード C の搬送波を検出できない場合には，ノード A はノード B にパケットを送出し，結果的に衝突が起こることになる．このような現象は隠れ端末問題（Hidden Terminal Problem）と呼ばれる [2]．キャリアセンスはパケットの衝突を防止する有効な手段であるが，不必要にパケットの送信を抑制する場合がある．これは，さらし端末問題（Exposed Terminal Problem）と呼ばれる．例えば**図 2･30** において，ノードＹはノード A からの搬送波が届かない距離（干渉領域外）にあるとする．ノードＸがノードＹに送信中，ノード A はノード B に送信可能であるにもかかわらず，ノード X の搬送波を検出するため，自身はパケットを送信できない．

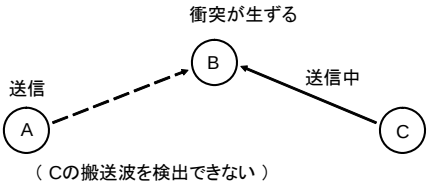


図 2・29　隠れ端末問題

（出典：小牧省三，間瀬憲一，松江英明，守倉正博「無線 LAN とユビキタスネットワーク」丸善，2004）

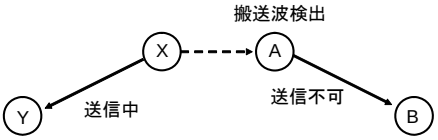


図 2・30　さらし端末問題

（出典：小牧省三，間瀬憲一，松江英明，守倉正博「無線 LAN とユビキタスネットワーク」丸善，2004）

隠れ端末問題を避ける方法として，ノード C がノード B に送信中であることを，ノード B の周囲のノードに予め通知しておくことが考えられる．これは RTS/CTS 方式と呼ばれる [1]．図 2･29 のノード配置を例にとり説明する．ノード C がノード B にパケットを送る場合，まず RTS（Request-To-Send）パケットをブロードキャストする．これを受信したノード B は，応答として CTS（Clear-To-Send）パケットをブロードキャストする．これを受信することにより，ノード C はノード B にパケットの送信を開始する．CTS パケットにはノード C がノード B に通信する時間長が含まれている．これにより，ノード A はノード B へのパケットの送信を控えることになり，ノード B での衝突が防止される．RTS/CTS 方式は IEEE 802.11 標準のオプションであり，アクセスポイントを使用する無線ＬＡＮでの利用を前提に開発されたものであるが，アドホックネットワークにおいても衝突防止に有効である．しかし，RTS/CTS パケットの送信が通信路の帯域を消費するためオーバヘッドが生ずることになる．RTS/CTS 導入が有効かどうかは，衝突減少の効果とのトレードオフの問題になる．

いま，ノードが**図 2･31** のように直線状に並び，両端のノードを始点，終点として n ホップでパケット配送を行う場合を考える．各リンクでは同じチャネルが利用されるものとする．また，パス上の任意の 2 ノード間が相互に m ホップ数以内の場合，それぞれの終点方向へのリンクが干渉範囲にあるものとする．ここで，二つのリンクが干渉範囲にあるとは，各リンクの送信ノードが同時にパケット送信を行うとどちらのパケットも正常に受信されないことをいう．この場合，同時には高々一つのノードしかパケット送信を行うことができない．したがって，ホップ数 n が $m + 1$ 以下の場合，n ホップ通信のスループットは 1 ホップ通信のスループットの高々 $1/n$ となる．n が $m + 1$ より大きい場合には，パス上の $m + 1$ ホップを超える 2 ノードは相互に干渉範囲外となりパケットの同時送信が可能になるため，n ホップ通信のスループットの上限は $1/(m + 1)$ となる．いずれにしろ，マルチホップ通信のスループットは原理的にホップ数の増加により急激に減少する．パス上のリンクで異なるチャネルを使用することによりスループットの低下を抑制することが可能である．

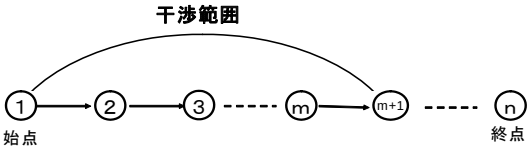


図 2・31　無線マルチホップ通信における干渉範囲の例

(3)　ネットワーク層 [3), 4)]

プロアクティブ型 (テーブル駆動型) ルーチングでは, 経路表が常に維持されているので, パケット送信の必要が生じた時点ですぐにパケット送信を実行可能である．ノードが高速移動を行う場合には，経路表の内容が短時間で古くなり，最新の状態に維持するには内容の更新を頻繁に行う必要がある．このため，制御メッセージのオーバヘッドが増大する問題がある．リアクティブ形ルーチングでは，パケット送信要求が生じてから送出可能となるまで遅延が生ずる. 通信要求が少ない場合には, 制御メッセージオーバヘッドは比較的少ない. ノードの移動速度が大きく, 通信要求の頻度が少ないほど, リアクティブ型が有利になる. 逆に, ノードの移動速度が小さく，通信要求の頻度が多いほど，プロアクティブ型の利点が大きくなるといえる．ノードの移動により，ノード間のリンクが切断されたり，新たなリンクが生ずることが，頻繁にあり得る．経路選択においては，より長時間利用できる安定した経路を選択すると共に，リンク切断が生じても代替経路を迅速に発見できることが必要である．

ルーチングプロトコルの役割は始点から終点までデータパケットを配送するための経路を構築することである．したがって，複数の経路がある場合，その中から最適な経路を選択するための評価尺度（メトリック）が必要になる．最も単純かつ一般的なメトリックはホップ数である．すなわち，始点と終点間の最小ホップ数の経路を最適とし，ルーチングプロトコルは最小ホップ数の経路を選択するように動作する．このメトリックはパケット中継に要するネットワーク資源の使用量を最小化し，パケット配送遅延時間を最小化するねらいをもっている．特にリンクの帯域，性能などが比較的均等なネットワークでは，ホップ数は有効なメトリックと考えられ有線ネットワークでも一般的に利用される．

MANET でもホップ数は測定，実装の容易さなどからよく使用される．しかし，無線マルチホップの通信形態をとることからホップ数は必ずしも適切なメトリックとはいえない．無線リンクは，干渉，フェージングなどの影響で有線ネットワークに比べてパケット損失率が一般に高く，リンクにより大きな差がある．リンク距離が大きい場合や遮蔽物がある場合には受信電力が小さくなり，パケット損失率が高くなる．マルチレートの無線伝送方式では無線リンクの状態により適切な符号化方式を選択することにより，送信データ速度（レート）が大きく変化する．更に，各リンクは独立ではなく，あるリンクが使用されているときにはその周辺のリンクは使用できなくなる．これらの理由により，最短経路が単純に良い経路とはいえない場合が生ずる．そこで様々なメトリックが提案されている．以下に代表的なリンクメトリックを紹介する．

(a)　ETX [5)]

パケット損失が生ずると，それを検出し，再送を行う必要がある．ETX（Expected

Transmission Count）は各リンクで一つのパケットを送信する場合，再送も含めた平均パケット送信回数をリンクのメトリックとするものである．あるリンクにおいてパケットを送信したときのパケットの損失率（順方向損失率）を p_f，このパケットに対する ACK パケットの損失率（逆方向損失率）を p_r とすると，パケット送信に成功する確率 p は次式で表される．

$$p = 1 - (1 - p_f) * (1 - p_r) \tag{1}$$

パケット再送に k 回目に成功する確率 $s(k)$ は次式で表される．

$$s(k) = p^{k-1} * (1 - p) \tag{2}$$

このとき，リンク ETX は次式で表される．

$$ETX = \sum_{k=1}^{\infty} k * s(k) = \frac{1}{1-p} \tag{3}$$

リンク ETX が小さいほどパケット送信に成功するまでのパケット送信回数, 送信時間が少なくなる．すなわち，リンク占有時間が短くなる．単位時間に送信可能なパケット数（スループット）は ETX の逆数に比例するので, ETX はスループットのメトリックにもなっている．

始点，終点間のパスの ETX はパスに含まれる各リンク ETX の総和として表される．パス ETX はパケット配送のために消費するリソースに関するメトリックを意味する．また，パス内のリンクが相互に干渉範囲にある場合には，あるリンクを使用中は他のリンクを使用できないので，パス ETX はパケット配送遅延時間とパスのスループット（パススループット）のメトリックになる．

(b) ETT (Expected Transmission Time) [6)]

ETX ではリンクの送信レートは考慮されていない．ETT はパケット損失率と送信レートの両方を考慮するメトリックである．ETT はあるリンクにおいてサイズ S のパケット送信に成功する平均時間であり，B を送信レートとして，次式で表される．

$$ETT = ETX * S/B \tag{4}$$

この式はフレーム間スペース（SIFS，DIFS）[*1]，バックオフ時間 [*2]，固定レートでのプリアンプル・ヘッダ送信時間 [*3]，ACK などの制御メッセージの送信時間，伝搬遅延時間などの

[*1] IEEE 802.11 規格において定められた送信機が信号を送信する前に必要な最低限の送出信号間隔（IFS：Inter Frame Space）．通常のデータフレームには DIFS（分散制御用フレーム間隔），ACK などの優先フレームにはより短い SIFS（短フレーム間隔）が適用される．

[*2] IEEE 802.11 規格で定められた衝突回避の方法．フレームを送信しようとする送信機は規定の CW（Contention Window）範囲内で乱数を発生させ，バックオフ時間（一定のスロット時間の倍数）を決める．IFS に引き続き，スロット時間ごとにチャネルがアイドルであればバックオフ時間を減算し，バックオフ時間が 0 となった送信機が送信する．フレームの衝突などによる再送ごとに CW の範囲を 2 倍に増加する．

[*3] IEEE 802.11 無線 LAN の物理層は物理層コンバージェンス手順副層（Physical Layer Convergence Procedure sublayer：PLCP 副層）と物理媒体依存副層（Physical Media Dependent sublayer：PMD 副層）からなる．PLCP 副層は MAC フレームにプリアンプル（送信機と受信機を同期させるため，変調方式に依存し，必要な場合に付加）と PLCP ヘッダを付加する．プリアンプルと PLCP ヘッダの部分の送信レートは無線 LAN の方式により固定的に与えられる．MAC フレームの部分は方式により送信レートは可変であり，選択された送信レートが使用される．

オーバヘッドを無視して単純に定式化されている．パケット損失率が大きい場合やパケット衝突が多い場合は 2 進指数バックオフの影響が大きくなるので，その影響を考慮することも考えられる．パスの ETT はパスに含まれる各リンク ETT の総和で表される．パス ETX と同様にパス ETT はパケット配送に消費されるリソース，パケット配送時間，パススループットに関するメトリックになっている．

(c) WCETT (Weighted Cumulative ETT) [6)]

ETX，ETT はすべてのリンクが同一のチャネルを使用することを前提とするメトリックである．IEEE 802.11a/b/g の場合，周波数帯が重ならない複数のチャネル（非オーバラップチャネル）が利用可能である．複数インタフェース，複数チャネルを利用する MANET，メッシュネットワークでは一つのパスにおいて，各リンクに異なるチャネルが割り当てられる場合がある．このような場合のパスメトリックとして WCETT が提案されている．WCETT は次のように定式化される．

$$\mathrm{WCETT} = (1-\beta) * X + \beta * Y \qquad (5)$$

ここで，X はパス ETT，Y はパス上で同じチャネルが割り当てられたリンクの ETT の総和を各チャネルについて求め，その最大値である．β は 0 と 1 の間の値をとる重みである．X はパケット配送に消費するリソース，パケット配送遅延時間の尺度となっており，Y はパススループットの尺度となっている．

■参考文献

1) IEEE Computer Society LAN MAN Standards Committee, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Standard 802.11, 1997.
2) F. A. Tobagi, “Packet Switching in Radio Channels: Part-II- The Hidden Terminal Problem in Carrier Sense Multiple-Access Models and the Busy-Tone Solution,” IEEE Trans. Commun. vol.COM-23, no.12, pp.1417-1433, 1975.
3) 間瀬憲一, 阪田史郎, “アドホック・メッシュネットワーク（ユビキタスネットワーク社会の実現に向けて）,” コロナ社, 2007.
4) 小牧省三, 間瀬憲一, 松江英明, 守倉正博, “無線 LAN とユビキタスネットワーク,” 丸善, 2004.
5) D. De Couto, D. Aguayo, J. Bicket, and R. Morris, “A High-Thoughput Path Metric for Multi-Hop Wireless Routing,” In MOBICOM, 2003.
6) R. Draves, J. Padhye, and B. Zill, “Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks,” In MOBICOM, 2004.

2-4-2 トランスポートレベルの性能

（執筆者：張　兵）[2008 年 8 月 受領]

トランスポート層上のプロトコルはコネクション型の TCP（Transmission Control Protocol）と，コネクションレス型の UDP（User Datagram Protocol）の 2 大トランスポートプロトコルがある [1)]．現在ではインターネット全トラヒックの 90 %以上を占める電子メールやウェブ閲覧，ftp などのサービスは TCP プロトコルによって支えられている．TCP は本来，有線ネットワークを想定して設計されているため，無線ネットワークにおいて頻繁に発生する転送誤り・干渉，リンク切断などに対応できないため，通信性能が著しく劣化する [2)]．特に，アドホックネットワークの特徴であるマルチホップ通信はビット誤り・干渉，リンク切断などといった無線通信の問題を更に助長させてしまう．

TCP は再送制御機構と輻輳制御機構を備えることにより，インターネットにおいて信頼性が高く，かつ効率的なデータ通信を実現している．TCP による輻輳制御はパケットロスをネットワークの輻輳によるものと判断し，輻輳の状態に応じて転送速度の調節を行う．しかし，アドホックネットワークにおいては，輻輳と無関係にリンク切断やビット誤り・干渉によるパケットロスが生じる．TCP は無線環境における高い誤り率・干渉，ならびにモビリティによるリンク切断などに起因するパケットロスを輻輳によるロスと区別できないため，輻輳状態にないにもかかわらず不必要にデータの送信速度を抑制するという問題がある（**図 2･32**）．一方，アドホックネットワーク上で複数のパスを同時に転送に利用するためのマルチパス通信というアプローチが注目されている [3)]．しかし，データ転送パスの切り換えが発生してもパス情報を上位層に通知する仕組みがないために，上位層に TCP のような確認応答を必要とするプロトコルが存在した場合，パフォーマンスの悪化を招く．

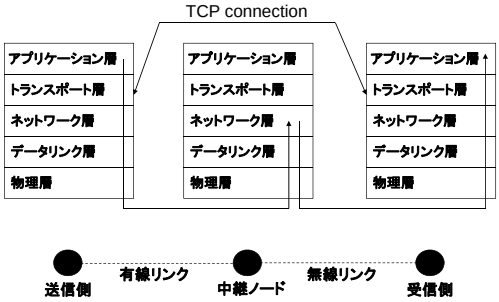


図 2･32　送信側から受信側までアドホックネットワークにおける中継ノードを経由する TCP パケットの経路

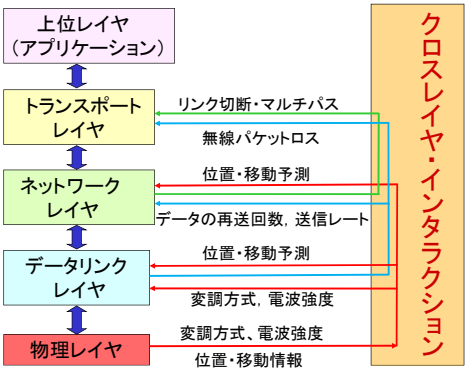


図 2･33　アドホックネットワークにおける MAC 層，ネットワーク層及びトランスポート層間の連携によるクロスレイヤアーキテクチャの設計

上記の問題は，アドホックネットワークにおける MAC レベルの通信状況とネットワークレベルのリンク状態が正確に上位層に通知されないために発生する．これらの問題を解決するために，クロスレイヤ情報交換を実現するクロスレイヤアーキテクチャ（**図 2･33** 参照）を用いることにより，トランスポートレベルの性能の向上が期待できる．ここでは，特に物理層における電波強度（RSSI）[4]，無線リンクロス [5] とリンク切断の明示的な通知などといった，物理・リンク及びネットワーク層の連携に焦点を当てる．

(1) MAC 層との連携によるクロスレイヤアプローチ

物理層における端末の位置，モビリティ，無線チャネルの特性（変調方式，受信信号強度（RSSI））などの情報をレイヤにまたがって利用することにより，高速・安定なリンク確立，最適なルーチング構築が実現でき，それによって，トランスポートレベルの通信性能を向上させることができる．

まず，端末の位置，モビリティ情報をリンク層・ネットワーク層に上げることによって，リンク切断の予測ができるうえ，新しい経路の構築はリンク切断を待たずに開始することができる．特に移動方向・速度の情報をリンク層に知らせることにより，より安定なリンクを予知し，選択することができる．次に，各リンクの送信レートをネットワーク層に通知することにより，送信レートに応じてメトリックを変化させる経路選択方式が可能となる．IEEE 802.11a/b/g は使用する変調方式によって送信レートが異なる．送信レートを固定するモードと自動的に設定するモード（オートレート）があるが，モビリティが高く，不安定なリンクにおいては，オートレートの使用が困難となる．モビリティがそれほどないメッシュネットワークにおいては，各リンクのパケット損失率に基づき最適な送信レートを決定することができるが，データパケットの再送回数，フレームエラーレート，あるいは受信信号強度（RSSI）をネットワーク層に知らせることにより，ネットワーク層で送信レートを決定し，下位層に知らせる方式も考えられる．

一方，無線 LAN MAC プロトコルでは CRC（Cyclic Redundancy Check）によってデータパケットが正しく受け取られたかどうかをチェックする．CRC によりビット誤りが検出される場合，IEEE 802.11 では対象となるパケットを破棄してしまう．このようにリンク層における局所的な再転送が制限回数まで送ったにもかかわらず，最終的に無線のビット誤りによって捨てられたことによって生じたパケットロスと輻輳によるパケットロスと区別するため，送信側のトランスポート層に無線リンクロスを明示的に通知する必要がある．したがって，MAC 層とトランスポート層の連携によって，アドホックネットワークにおいて，TCP における有効な輻輳制御が可能となる．

(2) ネットワーク層との連携によるクロスレイヤアプローチ

前述のように MAC 層とネットワーク層，ならびに MAC 層とトランスポート層の連携により，高速・安定なルーチング構築が可能となったが，ネットワーク層とトランスポート層の連携がなければ，コネクションの切り換え，切断，更にマルチパスに対応できないため，TCP の性能劣化の問題が依然残る．トランスポートプロトコルでは，通信経路の RTT や CWND・パケットロスなどのパラメータを保持しているが，パケット転送で利用している経路情報をトランスポート層に適切に通知しなければ，経路切り換えが発生する場合，異なる

経路状態（RTT など）に基づいて転送制御を行うため通信性能が悪化する．一方，リンク切断の検出はデータパケットの再送回数で判断するケースがあるため，端末の移動がなくても，無線の干渉により通信経路の切り換えが引き起こされる可能性がある．このように端末の移動・干渉により頻繁に発生する通信経路の切り換えに対応するため，リンク切断と経路再構築の情報を何らかの形でトランスポート層に通知する仕組みが必要となる．ネットワーク層におけるルーチング情報を用いることにより，トランスポートプロトコルはリンク切断が発生してから経路再構築ができるまでの間に送信をフリーズする手法などが考えられる．

上記のように，クロスレイヤアーキテクチャ（図 2･33 を参照）を構築することにより，アドホックネットワークにおける無線マルチホップ通信環境と高いモビリティに対応できる，高信頼性・高性能なトランスポート通信技術の確立が可能となる．

■参考文献

1) 村山公保, 西田佳史, 尾家祐二, “トランスポートプロトコル, ” 岩波書店, 1991.
2) 張　兵, “ワイヤレスネットワークにおける TCP の研究”, 電子情報通信学会誌, vol.86, no.4, pp.286-288, Apr. 2003.
3) 内藤壮司, ヌリシラジ マハダド, 美濃導彦, “アドホックネットワークにおける信頼性を保障するプロトコルに向けたマルチレート通信機構”, 電子情報通信学会論文誌, vol.J89-B, no.6, pp.873-887, Jun. 2006.
4) S. Tang, B. Zhang, M. Watanabe and S. Tanaka:“A link heterogeneity-aware on-demand routing (LHAOR) protocol utilizing local update and RSSI information,” IEICE Trans. Commun., Vol.E88-B, No.9, pp.3588-3597, 2005.
5) 張　兵, M. N. シラジ, 田中信介, “無線 TCP における MAC 情報を用いた明示的無線リンクロス通知方式”, 情報処理学会論文誌, vol.45, no.5, pp.1388-1398, May 2004.

■4群 － 5編 － 2章

2-5 アドホックネットワークのセキュリティ

（執筆者：高橋　修）［2009年8月 受領］

2-5-1 はじめに

アドホックネットワークは，本章 2-2 節のルーチングプロトコルに述べたとおり，無線通信を使ったその場限りのネットワークを形成し，通信を行うので，有線ネットワークとは異なる観点からのセキュリティが重要である．すなわち，モバイルアドホックネットワークでは，

(1) 電波を利用しているため，情報は無線到達範囲内で傍受可能であること．

(2) その場限りのネットワークであるので一般に管理者はいないこと．

(3) パケットを中継するのは，第三者であること．

上記のうち，(1) に関する事項は，暗号技術を送受信者相互間で適用すれば，ほとんど解決することは可能と思われるが，(2)，(3) に関しては，ルーチングプロトコルに密接に関連し，やっかいな問題である．本節では，通信路の設定やその維持管理を行うネットワーク層に関する攻撃方法とそれに対する防御方式を中心に，基本方式や研究動向，及び今後の展望について概説する．

2-5-2 特徴的な攻撃と検出・防御方式

(1) 攻　撃 [1)~3)]

アドホックネットワークにおける攻撃を大きく通信の層ごとに分類して**図 2･34** に示す．これらのうち，アプリケーション層やトランスポート層に関連する攻撃は通常の有線ネットワークと同様の攻撃である．アドホックネットワークに特徴的な攻撃は，ネットワーク層とデータリンク層／物理層に関連するものであり，それらの攻撃を中心に概説する．

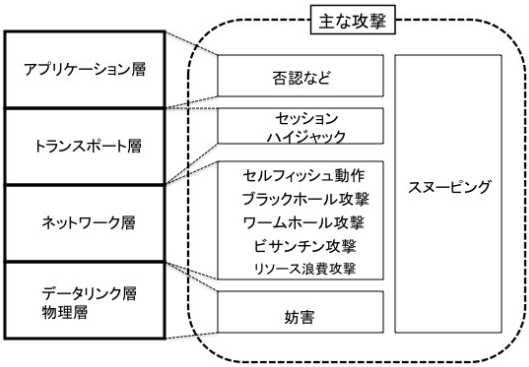


図 2・34　アドホックネットワークにおける主な攻撃の分類

(a) 物理層／データリンク層

妨害（ジャミング）は，攻撃対象ノードの送受信にタイミングと周波数を合わせて信号を

送り，混信させて受信不能にする攻撃である．

(b) ネットワーク層

データパケットの送受信は行うものの，他ノードのデータパケットの中継動作をしないセルフィッシュ動作がある．セルフィッシュ動作を行うノードが存在すると，多ノードのリソースを消費し，結果的に多ノードの通信を妨害することになる．更に，複数の攻撃ノードが共謀し，ある攻撃ノードが受信したパケットをトンネリングによりもう一方の攻撃ノードに転送することなどにより通信ルートを無効にしたりパケットの廃棄を行うワームホール攻撃やビザンチン攻撃がある．その他の攻撃として，悪意のあるノードが通信ルートを構成するノードの一つとなって，受信したパケットを廃棄するブラックホール攻撃や，特定のパケットを複製／改変などして周辺のノードへブロードキャストすることによって，大量のパケットがネットワーク内に発生させるリソース浪費攻撃などがある．

(c) 複数の層に関連

典型的な攻撃法としてスヌーピング（パケットの傍受）がある．ネットワークの動作を混乱させることはないが検出は困難である．データパケットを暗号化することで対応可能である．

(2) 検出・防御方法

(1) 項で述べた各種攻撃に対する汎用的な検出・防御方式はなく，攻撃方法や対象となるプロトコルごとに個別に研究開発されている．本項では，ネットワーク層に関連した攻撃を対象とした代表的な検出・防御方式を概説する．

(a) Watchdog 方式 [4)]

通信ルート上の各ノードが一つ下流の中継ノードの動作（受信パケットを次ノードへ中継転送したか）を監視し，異常動作を検出したノードが，何らかの形ですべてのノードか送信元ノードに報告し，攻撃ノードを避けるように通信ルートの再設定を行う方法である（**図 2・35** 参照）．この方式は，セルフィッシュ動作やブラックホール攻撃を検出・防御するのに有効であるが，無線電波の特性から誤検出が発生することは避けられない．

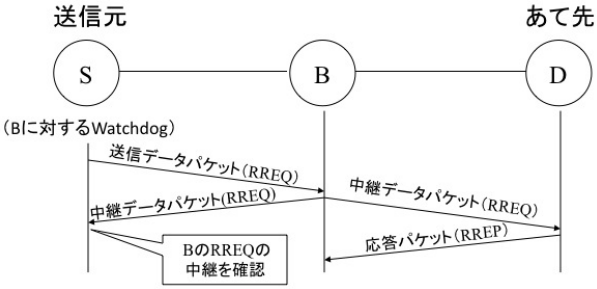


図 2・35 Watchdog 方式の動作概要

(b) 転送レポート方式 [5)]

通信ルート上の各ノードは通信ログ情報(送受信パケット数など)を収集し送信元に送り，送信元でこれらの情報を比較評価することで，攻撃ノードを検出し，攻撃ノードを避けるよ

う通信ルートの再設定を行う方式である（**図 2･36** 参照）．送信元は，あるノードの送信数と一つ下流ノードの受信数が異なる場合には，予めノードごとの信頼度に関する評価関数を定義し各ノードの信頼度によって攻撃ノードを判断する．この方式は，ネットワーク層のあらゆる攻撃に有効ではあるが，送信元で通信ルートを把握している必要があり，ソースルーチングに限定されている．

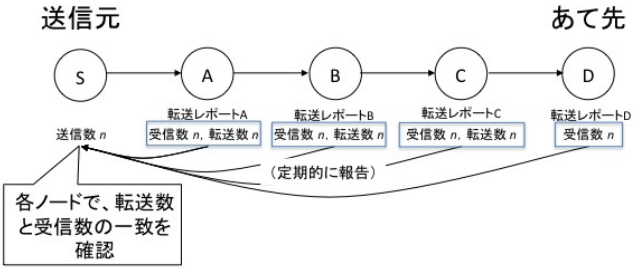


図 2・36　転送レポート方式の概要

2-5-3 今後の展望

アドホックネットワークが広く普及し，一般的に利用されるようになればなるほどセキュリティは重要になる．今後もいろいろな攻撃法が考案される可能性がある．上記で紹介した防御方式は，特定の攻撃方法に個別対応するか，特定のルーチング方式に依存している場合がほとんどであり，汎用的な防御方式の検討が大きな課題となっている．

また，何らかの事件が発生し，後に訴訟問題となった場合に，第三者に証明可能なディジタル証拠を収集する方式としてネットワークフォレンジック技術 [6] がある．アドホックネットワークでは，無線電波の特長を生かし，無線電波を傍受したノードが何らかの形でディジタル証拠を生成し，これらを正しく保管することで，ネットワークフォレンジック技術を適用できる可能性があり，今後の研究開発が期待されている．

アドホックネットワークが健全に発展するためには，セキュリティに関する技術開発がますます重要になってくる．

■参考文献

1) S. V. Kartalopoulos, H-H. Chen, M Freire, L. He, and P. Verma, “Security in mobile ad hoc and sensor networks: Part1,” IEEE Communications Magazine, vol.46, no.2, pp.102-103, 2008.
2) A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J.D. Tygar, “SPINS: Security Protocols for sensor Networks,” The 7th Annual International Conference on Mobile Computing and Networking, pp.189-199, 2001.
3) P. Papadimitratos and Z. J. Haas, “ Secure Routing: Secure Data Transmission in Mobile Ad Hoc Networks,” ACM Workshop on Wirekess Security 2003, pp.41-50, 2003.
4) S.Marti, T.J.Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior inmobile ad hoc networks,” Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, pp.255-265, 2000.
5) W. Yu, Y. Sun, and K. Liu, “HADOF: Defense against routing disruptions in mobile ad hoc networks,” IEEE INFOCOM, vol.2, pp.1252-1261, 2005.
6) RFC 3227, “Guidelines for Evidence Collection and Archiving,” 2002.