

密集端末を活用するアドホックネットワーク
のための経路制御プロトコルに関する研究

平成 18 年 度

三重大学大学院工学研究科
博士前期課程 電気電子工学専攻

渡 邊 貴 則

修 士 論 文

密集端末を活用するアドホックネットワーク
のための経路制御プロトコルに関する研究

A Study on Routing Protocols of Using
Dense Condition for Ad Hoc Network

平成18年度修了

三重大学大学院工学研究科

博士前期課程 電気電子工学専攻

通信工学研究室

渡邊 貴則



目次

第 1 章 序論	1
第 2 章 アドホックネットワーク	6
2.1 アドホックネットワークの基本動作	7
2.2 ルーティングプロトコル	8
2.3 AODV(Ad hoc On-demand Distance Vector)	14
2.3.1 経路発見	14
2.3.2 経路保全	23
2.3.3 経路修復	26
第 3 章 信号電力に基づく経路制御情報の削減手法の提案	28
3.1 密集端末が経路探索に与える影響	29
3.2 信号電力に基づくルーティング手法	30
3.3 計算機シミュレーションによる特性評価	32
3.3.1 総端末数に対する RREQ パケットのブロードキャスト数	33
3.3.2 総端末数に対するスループット特性	34
3.3.3 総端末数に対する遅延時間	35
第 4 章 局所代替経路を用いたアドホックルーティング手法の提案	37
4.1 アドホックネットワークにおいてパケット配送時に生じる問題	38
4.1.1 隠れ端末問題がアドホックネットワークに与える影響	38
4.1.2 アドホックネットワークに対するさらされ端末問題	40
4.2 代替経路構築方式	42

4.2.1	近隣端末による代替経路の構築	42
4.2.2	代替経路の利用条件	44
4.3	計算機シミュレーションによる特性評価	45
4.3.1	総端末数とデータパケット到着率との関係	45
4.3.2	総端末数に対する 1 通信当たりのリンク損失数との関係 . . .	46
4.3.3	総端末数に対する 1 通信当たりの制御パケット数との関係 . .	48
第 5 章 結論		50
参考文献		52
謝 辞		55
研究業績		56

図 目 次

2.1	アドホックネットワークの例	7
2.2	マルチホップ通信	8
2.3	ルーティングプロトコルの分類	9
2.4	プリコーサの概念	15
2.5	送信元端末における経路発見処理のフローチャート	16
2.6	中継端末における経路発見処理のフローチャート	17
2.7	送信先端末における経路発見処理のフローチャート	17
2.8	RREQ の構成	19
2.9	RREP パケットの構成	19
2.10	経路発見プロセス	22
2.11	RERR の構成	25
2.12	RERR 作成の例	26
2.13	ローカル経路修復	27
3.1	中継端末の探索エリアの比較	29
3.2	信号電力に基づくルーティング手法を用いた時の中継端末における フローチャート	30
3.3	優先度に応じて経路制御を行う際の動作例	31
3.4	優先度に応じて経路制御を行う際のパケットの配送過程	32
3.5	総端末数に対する RREQ パケットのブロードキャスト数	33
3.6	総端末数に対するスループット特性	34
3.7	総端末数に対する遅延時間	35

4.1	隠れ端末問題	39
4.2	RTS/CTS 方式	40
4.3	さらされ端末問題	41
4.4	さらされ端末問題が発生した時のパケットの流れ	42
4.5	代替経路が利用可能な端末配置例	43
4.6	代替経路の構築過程	44
4.7	主経路から代替経路への切替過程	44
4.8	総端末数に対する平均データパケット到着率	46
4.9	総端末数に対する 1 通信当たりのリンク損失数	47
4.10	総端末数に対する 1 通信当たりの制御パケット数	48

表 目 次

3.1 シミュレーションパラメータ	36
4.1 シミュレーションパラメータ	49

第1章

序論

近年, 移動通信の技術開発が急速に進むことにより, 無線通信機器が身近なものとなり, 多数の移動通信サービスが提供されつつある [1-3]. 総務省の調べによると平成 18 年 9 月末時点で, 携帯電話・PHS の利用者数は 9800 万人を超えた [4]. これは, 国民の約 8 割が無線通信サービスを利用していることになり, 今後の更なるサービスが期待されている. 移動通信サービスの代表例としては, 携帯電話・PHS やラップトップ型 PC などを用いたサービスが挙げられる. 携帯電話サービスでは第 3 世代の移動通信サービスがすでに提供されており, 2010 年には第 4 世代の移動体通信サービスの開始が予定されている. 一方, 小型・軽量化したラップトップ型 PC は無線 LAN に接続することで, 容易にネットワークに接続することが可能である. そのため, 街中などに無線 LAN を設置することで, 無線通信を用いたインターネット接続サービスを利用可能にしたアクセスポイントの需要が年々増加している. アクセスポイントの利用形態は, その場で一時的にネットワークの利用を開放している場合とサービスを提供する業者の会員になる場合の 2 種類が主流である. 前者はその場にいる全ての人がアクセスポイントを利用することが可能である. 一方, 後者は様々な提供業者によるアクセスポイントサービスが存在するため, 利用者はより良いサービスを選択することが可能である. しかし, 利用する業者により, ある場所ではアクセスポイントの利用が可能であるが, 別の場所では利用できない状況が発生する. さらに, 面としてのサービスを提供するためには, アクセスポイントのような基盤設備を多数設置する必要がある.

そこで, 近年, いつでもどこでもネットワーク接続への需要が増加することで, セ

ルラ方式やアクセスポイントのような基盤設備を必要とはしないアドホックネットワークの研究が注目されている [5,6]. アドホックネットワークは各々の所持している無線通信端末のみで自律分散型のネットワークである. そのため, 基盤設備が存在しない場所でも, 無線通信端末のみでその場限りのネットワークを構築することが可能であるため, アドホックネットワークの基は軍事目的で研究が行われた. 一方, 民需的な利用としては, 災害やイベント時の通信手段, 監視システムへの適用などが想定されており, 利用範囲や対象は比較的限定されていた. つまり, その場限りのネットワークまたは特定の利用目的のための閉鎖的なネットワークである. しかし, 無線通信機器が小型・軽量化されることでさまざまな利用が考えられる. アドホックネットワークの利用方法としては, ラップトップ型 PC や携帯電話などの無線通信端末同士が直接通信を行うことにより, ネットワークを構成する. これにより, 端末間で容易にデータ通信を行うことが可能である. しかし, 無線通信端末が直接通信できる範囲には限りがあり, これだけでは容易にネットワークを構築することは不可能である. そこで, アドホックネットワークを実現するためには, 直接通信を行うことが出来ない場合でも近隣端末が中継処理をするマルチホップ通信を行うことが必須となる. しかし, マルチホップ通信を行うだけでは送信先の端末にデータを送ることはできない. なぜなら, 無線 LAN などのアクセスポイントを用いて通信を行う場合, アクセスポイントを中心にネットワークを構築する. これにより, 端末情報はアクセスポイントで集中管理される. それに対し, アドホックネットワークを構築する端末がマルチホップをする場合, アクセスポイントのような基地局を持たない. そこで, 各端末は端末情報を周辺端末に通知する必要がある. アドホックネットワークでは, 各無線通信端末は自身の存在および周辺端末の存在を知らせるために, 各々の通信半径内の端末に情報を報知するフラッドイングを行う. フラッドイングを行うことで, 同一パケットを1つの端末から全ての端末へ配信することが可能である. 結果として, 離れた端末との間で経路を確立することが可能となる. しかし, フラッドイングは最も単純な通知手法であるため問題も生じる. 例えば, フラッドイングを行うことである端末間の経路は確立されるが, 確立した経路が最適な経路が確立されるとは限らない. そこで, 各無線通信端末間で端末情報を記録した経路情報を管理する経路制御が必要となる. これまで, アドホックネットワークにおける経路制御手法に関する研究が多数行われ

てきた。例えば、データパケットの送信要求が発生する前から経路構築を行っておき、データパケットの送信要求が発生すると共にデータパケットを送信先端末へ送信するプロアクティブ型の経路制御手法がある。一方で、データパケットの送信要求が発生して初めて経路構築を開始し、経路構築後にデータパケットを送信するリアクティブ型の経路制御手法がある。これらの経路制御手法を用いる事で、アドホックネットワークを容易に構築することが可能となる。しかし、実環境を想定した場合、さまざまな問題が発生する。例えば、多数の端末が存在する状況下で送信元端末が送信先端末に向けてデータパケットを送信する場合、送信元端末は経路構築パケットをフラッディングすることで、送信先端末の探索を行う。この時、経路構築パケットを受信した中継端末は、送信先端末を探索するために、更に経路構築パケットのフラッディングを行う。しかし、端末数に比例した数だけフラッディングが行われるため、ネットワーク上で経路構築パケットが多量に発生し、正常な通信を行うことが困難になる。この問題はアドホックネットワークにおいて、ブロードキャストストーム問題と呼ばれている [7]。ブロードキャストストーム問題を回避するためには最小のブロードキャスト数でネットワーク全体にパケットを送信する必要がある。そのため、有効な中継端末のみが中継処理を行う手法が提案されている [7]。この手法では、ブロードキャストを行った端末とそれを受信した端末との距離により、再ブロードキャストを決定する方法である。そのため、各端末間の距離を決定するために GPS(Global Positioning System) を用いている。GPS を用いることで、どの端末が有効な中継を行うことが可能か知ることができる。しかし、GPS を利用することでブロードキャストストームを回避することは可能であるが、アドホックネットワークを構築する端末は GPS の利用は想定していない。そのため、ブロードキャストストームの解決には至らない。一方、ブロードキャストすることで、ネットワークに存在する経路構築パケットが同一のパケットであるという点に着目している手法が提案されている [8]。この手法では、ある移動端末においてホップ数が N 回である経路構築パケットを受信した場合、送信先端末でなければ、ホップ数を $N+1$ 回にした経路構築パケットのブロードキャストを行う。そして、この経路構築パケットを再ブロードキャストする前に、ホップ数が M 回である経路構築パケットを受信した時に、 $M > N$ が 2 回成立すると、経路構築パケットの中継を中止する。しかし、この手法では中継を中止することでブロードキャストを削減可能であるが、

$M > N$ を満たす状況が多数発生するため、経路構築が困難な状況になる。これらの関連研究に対し、本論文では、経路構築を行う際に用いられる経路構築パケットの受信電力に基づいて、経路構築パケットの配送の有無を判断する手法を提案する。また、近隣端末で一定時間の間、配送が行われない場合は、パケット配送の有無に限らず中継処理を行う。この処理により、ネットワーク全体に経路制御パケットを送信することが可能となる。提案手法を用いることで、各端末は経路構築時に発生する冗長な経路構築パケットを送信抑制することが可能である。中継端末の送信抑制を行うことで、ネットワーク内に多量に発生する経路構築パケットを抑制可能となる。これにより、データパケットの配送を円滑に行うと共に伝送効率の改善を明らかにする。

更に、経路構築後、送信元端末と送信先端末間のデータパケット配送に着目する。経路制御手法により各端末は経路が構築され、送信元端末は送信先端末にデータパケットを送信する。しかし、アドホックネットワークでは、各端末の近隣で複数の経路が同時に構築され、同時に通信が行われる。そのため、各端末は各々のタイミングでパケットの送信を行うとパケット衝突が発生する。そこで、各端末は同時にパケット送信を避けるために、パケット送信前に近隣端末からの搬送波の有無を確認する。搬送波を確認することで、パケットの送信可能か判断することが可能である。もし、近隣端末からの搬送波を感知した場合は、パケット衝突を回避するために一定時間待機した後、再び搬送波の有無を確認する。この制御を CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) と呼ぶ。しかし、電波を通さない障害物などの影響により、近隣端末の搬送波を確認できない場合が発生する。そのため、CSMA/CA を行うことで各端末は全てのパケット衝突を回避することは不可能であり、この問題は隠れ端末問題と呼ばれる [11]。そこで、隠れ端末問題を解決するために、パケットの送信前に周辺端末にチャンネルを使用することを通知する RTS/CTS (Request To Send / Clear To Send) 方式が提案された [12, 13]。CSMA/CA と RTS/CTS を用いることで、各端末はデータパケットの送信前に無線チャンネルの使用状況を確認し、周辺端末にチャンネルを使用することを通知することが可能となる。しかし、マルチホップ通信で RTS/CTS 方式を用いた場合、送信側または受信側の近隣端末は RTS パケットや CTS パケットを受信することで、近隣でのデータ通信が終了するまで送信を一時的に抑制される。この問題をさらされ端末問題と呼

ばれる [14]. もし, 送信を抑制された端末が他の端末のデータパケットを中継する中継端末である場合でも, 送信できない状況にあることを送信側に知らせることができない. 結果として, データパケットの送信が不可能になり, 構築した経路が存在しないものとして経路損失が発生する. しかし, 実際は一時的に送信が抑制されているだけなので, 経路としては有効であるにも関わらず経路の再構築が行われる. さらに端末問題を回避するためには, 周辺端末の位置関係や送信状況を考慮してパケット送信を行う必要がある. そこで, 各端末間の存在する方向情報を観測することで, さらに端末問題を回避する手法が提案されている [15]. この手法では, 干渉となり得る端末に限り送信抑制をかけることで, さらに端末問題を減少させた. しかし, 定期的に近隣トポロジを学習するために端末数の増加と共に制御パケットのオーバーヘッドが増加し, スケーラビリティに影響を与える. 関連研究に対し, 本論文では, さらに端末問題に対応した経路制御手法を提案する. 提案手法では, これまでに提案された多数のプロトコルに使用することが可能である. 本論文では, リアクティブ型の代表的な AODV を基として, 構築した経路の近隣に代替経路を構築する. 更に, さらに端末問題が発生した場合に, 代替経路を利用する. 代替経路を利用することで, 一時的に送信抑制を強いられた端末を用いずにデータパケットの配送を継続することが可能である. これにより, 冗長な経路再構築処理を削減すると共に, さらに端末問題による経路損失の削減を行う. 本論文の構成としては, 第2章でアドホックネットワークの基本的な動作原理, および既存のルーティングプロトコルについて述べ, 第3章では信号電力に基づく経路制御情報の削減手法の提案と計算機シミュレーションによる検討結果を述べる. 第4章では局所代替経路を用いたアドホックルーティング手法の提案と計算機シミュレーションによる検討結果を述べる. 第5章で結論を述べる.

第2章

アドホックネットワーク

本章では、本論文において検討するアドホックネットワークの概要について述べる。アドホックネットワークの基は軍事研究にある。1960年代の終わりから1970年代に、ALOHAプロジェクトにおいて、中央コンピュータと分散する端末を結ぶUHF帯域を用いたパケット交換網の研究が進められ、1970年代に運用を開始した。これにより、無線のブロードキャストの特性を利用してデータパケットを送受信するパケット無線の可能性が実証された。そして、多くの端末が共有の無線通信路にアクセスするランダムアクセスの原理が確立した。1972年には、パケット通信網 (PRNET: Packet Radio Network) の研究が開始した。PRNETは中央制御局を前提とするプロトコルを用いていたが、その後自律分散型の構造へと変革した。更に、PRNETは無線の接続性が不十分な環境の中で、無線端末に十分な接続性を提供するためのマルチホップのパケット交換経路制御技術を含むものであり、アドホックネットワークの起源となった。1980年の初期にPRNETの実現性は実証されたが、パケット無線装置は大きく、大きな電力を必要とした。そのため、当時は実用化の段階にはいたらなかった。その後、1990年代後半には小型・軽量化・低コストの無線装置が開発されたことにより、無線LANの導入が急速に普及した。無線LANを用いる事で、一部のエリアにインターネット接続を提供するアクセスポイントも普及した。このような環境の変化により、1990年代後半にアドホックネットワークの軍事目的の研究が再び加速し、1980年代には実現できなかった商用利用の可能性が再び注目されることになる。2000年代に入り、アドホックネットワークを利用した新たなコンピュータネットワークサービスやインターネット接続サービスの商

用サービスの提供も検討されている。そのため、現在ではアドホックネットワークの研究は世界中で盛んに行われている。

2.1 アドホックネットワークの基本動作

アドホックネットワークは基地局などの基盤設備に依存せず、無線通信端末のみで構成されている自律分散ネットワークのことである。アドホックネットワークを構築する端末は無線通信端末同士で直接通信を行うことができる場合、端末間で直接通信を行う。図 2.1 で、アドホックネットワークにおいて直接通信の可能な端末間で無線リンクの接続が可能な場合の一例を示す。図 2.1 では、端末 A は近隣端末 B、C と通信を行い、端末 D は端末 E と通信を行う場合を示す。

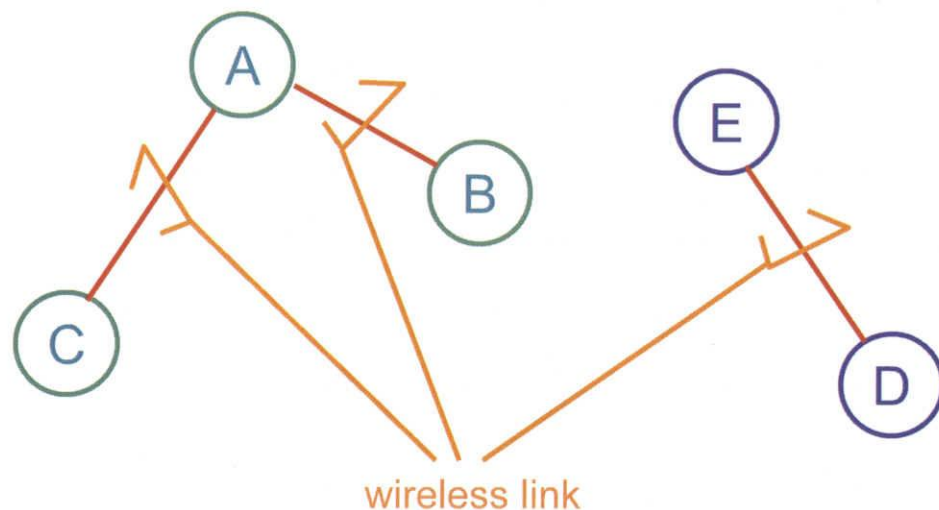


図 2.1 アドホックネットワークの例

しかし、特定の端末がある程度広い範囲に分散配置している場合や端末間に遮蔽物が存在する場合は、任意の送信元端末から送信先端末へ直接通信することが可能とは限らない。この場合、基盤設備を用いずに通信を行うには、近隣の端末(中継端末)を経由して、情報を中継する形態のマルチホップ通信を行う。図 2.2 で、マルチホップ通信に関する例として、送信元端末 S1 が送信先端末 D1 と直接通信で

きない状況を示す。S1 は D1 と通信を行うために、S1 は近隣の中継端末 R1, R2 の順に中継端末を経由して D1 へ情報を転送する。マルチホップ通信を行うことで、S1 は D1 と通信を行うことが可能となる。

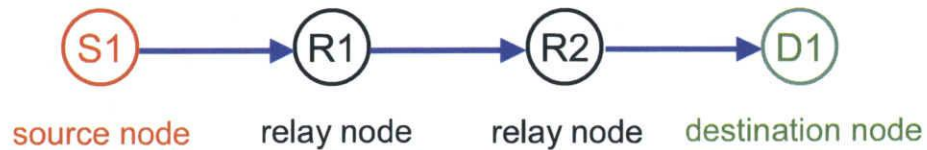


図 2.2 マルチホップ通信

しかし、基地局のように集中制御を行う基盤設備が存在しないアドホックネットワークでは、各端末がどこに存在しているか把握することは困難である。そのため、送信元端末は送信先端末と通信を行うために、ネットワーク全体に経路情報を報知するフラッディングを行うことで経路探索を行う。経路探索により、送信元端末と送信先端末との間で経路構築が完了して初めて通信を行うことが可能となる。しかし、フラッディングによる経路探索は最も単純な経路探索であるため、ネットワーク内に存在する端末数や端末の移動状況により有効に機能しない場合が発生する。更に、フラッディングを行うことで端末間の経路は確立されるが、送信元端末と送信先端末との間の経路が最適な経路が確立されるとは限らない。そこで、各端末で経路制御が必要となる。次節では、これまでに多数提案されているアドホックネットワークにおける経路制御プロトコルについて説明を述べる。

2.2 ルーティングプロトコル

本節では、アドホックネットワークにおいて送信元端末と送信先端末の間で経路構築処理がどのように行われているか既存のルーティングプロトコルを基に述べる。まずアドホックネットワークを用いて通信を行うためには、送信元端末は送信先端末への通信経路を構築する必要がある。無線ネットワークにおける通信経路とは、有線ネットワークのように実際に端末同士がケーブルを通して繋がるものではない。そこで、送信先端末までの経路をどのように決定するかが重要な課題となる。経路選択においては、長時間利用でき、安定した経路を選択すると共に、無線リ

リンクの切断が生じてても代替経路を迅速に発見することが必要となる。そこで、送信元端末と送信先端末との間で効果的な経路構築を行うために、多数の経路制御プロトコルが提案されている。これまでに提案されてきた経路制御プロトコルは、Proactive 型, Reactive 型, Hybrid 型に分類することができる。更にそれぞれの型は図 2.3 のように分類される。以下にそれぞれのプロトコルについて詳細を述べる。

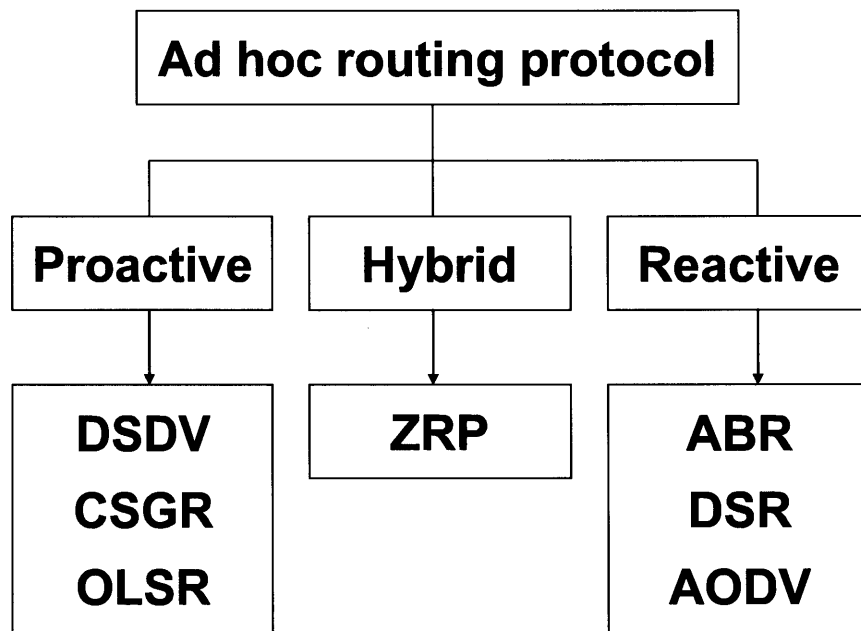


図 2.3 ルーティングプロトコルの分類

• Proactive

Proactive 型は、ネットワーク上の全ての端末が最新の経路制御情報を維持を行うように動作する。そのため、各端末はネットワークトポロジの変化に反応して、ネットワーク全体に経路の更新情報を転送する。常に最新の経路表を保持するため、通信要求があるとすぐにデータパケットを送信することが可能である。また、端末の移動頻度が少ない場合は、経路表の更新の機会が減るため、安定した通信を行うことが出来る。しかし、端末が高速移動する場合は、経路表を頻繁に更新する必要が生じる。このため、経路表を更新するための経路制御パケットの送信が増加し、トラヒック負荷が増大する問題があ

る. そのため, 経路表の更新周期を状況に応じて適切に設定する必要がある. 以下で, Proactive 型の例として, DSDV [16], CSGR [17], OLSR [18] についての詳細を述べる.

DSDV(Destination Sequenced Distance Vector)

DSDV プロトコルは, 古典的な Bellman-Ford ルーティングアルゴリズムを基にしたテーブル駆動型ルーティングプロトコルである. ネットワーク中の各端末は, 同一ネットワーク内の到達可能な全ての端末とその送信先端末までのホップ数を記録することで経路表を管理する. これにより, 送信元端末は経路を必要とするかしないかに関わらず, 常に利用可能なルーティング情報が準備されている. また, DSDV は経路を維持するために経路情報更新用のパケットとして, フルダンプパケットとフルダンプより小さい差分パケットを用いる. フルダンプパケットは利用可能な全ての経路情報を格納しており, 経路情報が大きく更新される場合に用いられる. 一方, 差分パケットは最後に送信したフルダンプパケット以降の更新情報のみを送信する場合に用いる. これらのパケットを用いる事で経路維持を行う.

CSGE(Cluster Swtich Gateway Routing)

端末はクラスタ (集団) に分類され, 各クラスタにはクラスタヘッド (クラスタの代表) が存在する. このクラスタ化により階層化構造が形成される. クラスタヘッドは分散クラスタヘッド選択アルゴリズムを用いる事で選定され, クラスタヘッドになるとクラスタ内の端末を制御することが可能である. もしクラスタヘッドが移動することでクラスタヘッドとして機能しなくなると, 新しいクラスタヘッドをクラスタ内の端末より選択する. また, クラスタのメンバーを変更するたびにクラスタヘッドの再選択が発生することを避けるために, LCC(Least Cluster Change) アルゴリズムが採用されている. CSGE プロトコルでは, 送信元端末から送信先端末にパケットを送信する場合, 送信元端末はクラスタ内のクラスタヘッドにパケットを送信する. パケットを受信したク

ラスタヘッドは、隣接するクラスタヘッドへパケットを転送する。もし、隣接するクラスタ内に送信先端末が存在しなければ、更にクラスタヘッドから隣接するクラスタヘッドへ転送する。この操作を繰り返すことで、送信先端末にパケットが到達する。しかし、CSGE プロトコルは、必ず隣接するクラスタヘッドを中継するように制約しており、形成された経路が最適なものではない。

OLSR(Optimized Link State Routing)

OLSR の特徴はフラッディングをより効率よく行うことが可能な点である。フラッディングを行うことで、同一パケットが1つの端末から全ての端末に配信される。結果として、多数の制御パケットが送信が起こるため、ネットワークへの負荷が高くなる。そこで、OLSR では制御パケットのフラッディングにおいて、マルチポイントリレー (MPR(MultiPoint Relay)) [19] の概念を導入している。ある端末がブロードキャストしたパケットをその端末の選択した MPR と呼ばれる端末のみが再ブロードキャストすることで経路制御パケットのオーバーヘッドを削減を行う。経路維持を行うため場合は、経路情報の生成は MPR のみが行うことでフラッディングされる経路情報を削減することが可能である。更に、MPR として選択した MPR 端末と間で経路情報を交換することで、経路制御パケットのオーバーヘッドを削減することが可能である。

• Reactive

Reactive 型は、送信元端末が通信要求した時にのみ経路構築を行う。そして、送信先端末への経路を構築するために、ネットワーク内に経路構築パケットをブロードキャストすることで送信先端末を探索し、経路表を作成する。経路構築処理は、送信元端末が送信先端末への経路を構築すると完了する。経路構築後は、各端末は経路表を基に送信先端末の方へデータパケットを送信する。もし、送信元端末と送信先端末の間の経路が無効となる場合が発生しても、経路修復処理を行い、データパケットの送信を再開する。また、アドホックネットワークでは、各端末はバッテリー駆動型の端末を想定するため、経路構築およびパケットの転送にバッテリーは不可欠である。Reactive 型のプロトコルは、

通信要求後に経路の構築を行い、通信要求がない時は、不要な制御パケットを送信する必要はない。そのため、不要なバッテリーの消費を抑えることが可能である。しかし、通信要求後に経路構築を行うので、データパケット送信までの遅延時間が発生する。以下では、Reactive 型の例として、ABR [20], DSR [21], AODV [22] についての詳細を述べる。

ABR(Associativity-Based Routing for Ad-Hoc Mobile Networks)

ABR プロトコルは経路の寿命がより長くなるように、安定したリンクを利用して経路を作成することを狙いとしている。安定したリンクを検出するため、周期的にビーコンを送信する。また、隣接端末からのビーコンを受信し、その連続受信回数(リンク結合度)を求める。このリンクの結合度が既定の閾値を超えるとリンクが安定しているとみなされる。

DSR(Dynamic Source Routing)

DSR プロトコルでは、送信元端末が送信先端末までの経路を指定する始点経路制御方式を採用している。これは、送信するデータパケットには送信先端末から送信先端末へ向かう経路上の中継端末が順番に指定する方法で、始点経路と呼ばれる。始点経路制御を行うことで、中継端末における経路情報の維持や更新などは不要となる。DSR では、経路発見と経路保持の2つのメカニズムにより成り立つ。経路発見では、送信元端末が送信先端末へのパケットを保持し、送信先端末への経路を保持していない場合に行う。経路保持は利用中の経路が利用できない場合に代替経路の利用や経路発見を行うメカニズムである。

AODV(Ad hoc On-demand Distance Vector)

AODV はリアクティブ型の経路制御プロトコルである。DSR が送信元端末が送信先端末への経路を保持する始点経路制御方式であるのに対し、AODV は

送信元端末と送信先端末の間の各中継端末が送信先端末のアドレスに基づき、次の中継端末を決定する経路制御方式である。また、各端末はシーケンス番号を保持し、端末間のリンクに変化があるとシーケンス番号を1つ増加する。もし、複数の経路が存在する場合、シーケンス番号を利用することで、最新の経路の選択が可能である。AODVは経路発見と経路保全を行うことで、アドホックネットワークを実現する。AODVについては、本論文の基となるプロトコルとして、次節で詳しく説明を行う。

• Hybrid

Hybrid型はReactive型とProactive型を組み合わせたプロトコルである。送信元端末の近隣の端末に対してはProactive型で経路表を作成する。以下で、Hybrid型の例としてZRP [23]を述べる。

ZRP (Zone Routing Protocol)

ZRPプロトコルはリアクティブ型のルーティングプロトコルとプロアクティブ型のルーティングを組み合わせたハイブリッド型の経路制御プロトコルである。ZRPでは、各端末は近隣の1, 2ホップ程度の範囲内の端末情報を保持する経路制御ゾーンを定める。経路制御ゾーンは、データの送信要求が発生時に利用する。そこで、データの送信要求が発生すると、送信元端末は経路制御ゾーン内の最大ホップ数の端末へ経路構築パケットを送信する。ゾーン内の最大ホップ数の端末は経路構築パケットを受信すると、自身のゾーン内に送信先の端末が存在するか確認すると共に、経路キャッシュを確認する。もし、経路キャッシュ内に有効な経路が存在する場合は、中継端末は経路確立パケットを送信元端末に向けて転送する。有効な経路が存在しない場合は、さらに経路構築パケットを転送する。しかし、経路構築パケットの転送を繰り返すと、転送の範囲が重なる場合が発生する。この時、ZRPでは、経路構築パケットを受信した中継端末は転送する必要があるか判断し、不要な場合は、中継を中止する処理が行われる。

以上のようにルーティングプロトコルは Proactive 型, Reactive 型, Hybrid 型に分類することが可能である. 本論文では, これらの中でも代表的な Reactive 型の AODV(Ad hoc On-demand Distance Vector) について詳細を次節で述べる.

2.3 AODV(Ad hoc On-demand Distance Vector)

AODV プロトコルは, Reactive 型の代表的なプロトコルの一つで, これまでに AODV を基にして複数経路構築手法など多数提案されている [24-26].

AODV プロトコルは, 経路発見と経路保全により経路制御が行われる. 経路発見は送信元端末が送信先端末へのデータパケットを保持し, 送信先端末への経路を保持しない場合, 経路構築を開始する. 経路構築を開始すると, 送信元端末は送信先端末を発見するために, 経路構築パケットを送信する. 経路構築パケットを受信した中継端末はルータとして, 送信先端末のアドレスに基づき次ホップを決定し, ホップごとに経路制御を行う. 各端末はシーケンス番号を持っており, 経路に変化が生じるとシーケンス番号を1つ増加する. 複数の経路が存在する場合は, 送信先端末のシーケンス番号が大きい方の経路を選ぶことにより最新の経路の選択が可能となる. また, 経路保全は構築した経路が利用できないことを検出し, 代替りの経路を発見する仕組みである. 経路発見, 経路保全における詳しい説明は次項以降で述べる. また, 端末間の情報を表す経路表は送信先端末, 次ホップの IP アドレス, 送信先のシーケンス番号, 送信先までのホップ数, TTL(Time To Live) を保持している. 図 2.4 では, 端末 P1, P2 が端末 B を送信先端末とし, 端末 A の隣接上流端末(プリコーサ)である関係を示す. 経路表の各経路は TTL を持ち, 経路が利用される度に更新され, TTL までに利用されないと経路は無効となる. 各端末は送信先端末ごとに, 自身を送信先への次ホップとするプリコーサリストを保持する. このプリコーサリストは経路損失時の経路修復のために使用される.

2.3.1 経路発見

本項では, AODV プロトコルの経路発見について述べる. 図 2.5 に, 送信元端末における経路発見処理のフローチャートを示す. 図 2.6 に, 中継端末における経路発

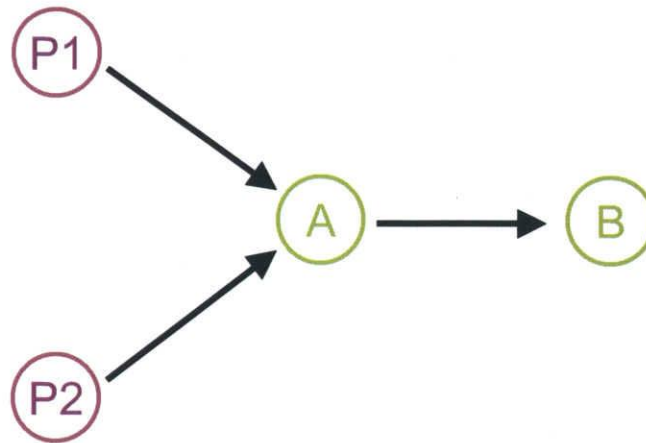


図 2.4 プリコーサの概念

見処理のフローチャートを示す. 図 2.7 に, 送信先端末における経路発見処理のフローチャートを示す.

送信元端末はデータパケット送信要求が発生すると, 送信先端末への経路を保持しているか経路表を確認する. 送信先端末への経路を保持する場合, 次ホップ端末へデータパケットを送信する. 経路表に経路がない場合は, すぐにデータパケットを送信せず, 経路発見のための処理を行う. まず, 送信元端末は経路要求 (Route Request(以下 RREQ)) メッセージを作成し, ネットワーク内の不特定多数の端末に向けてデータを送信するブロードキャストを行う. 図 2.8 に RREQ パケットの構成を示す. RREQ パケット内の各フィールドに格納される情報は以下のものである.

- type
パケットが RREQ パケットであることを識別するためのフィールドで, 1 を格納する.
- J,R,G,D,U flag
J, R フラグはマルチキャスト通信を行う場合に用いる. 本論文では使用しない. G フラグは, 不必要な RREP パケットを送信するべきか判断するときに使用する. D フラグは, 送信先端末以外が RREP パケットを返信できないように

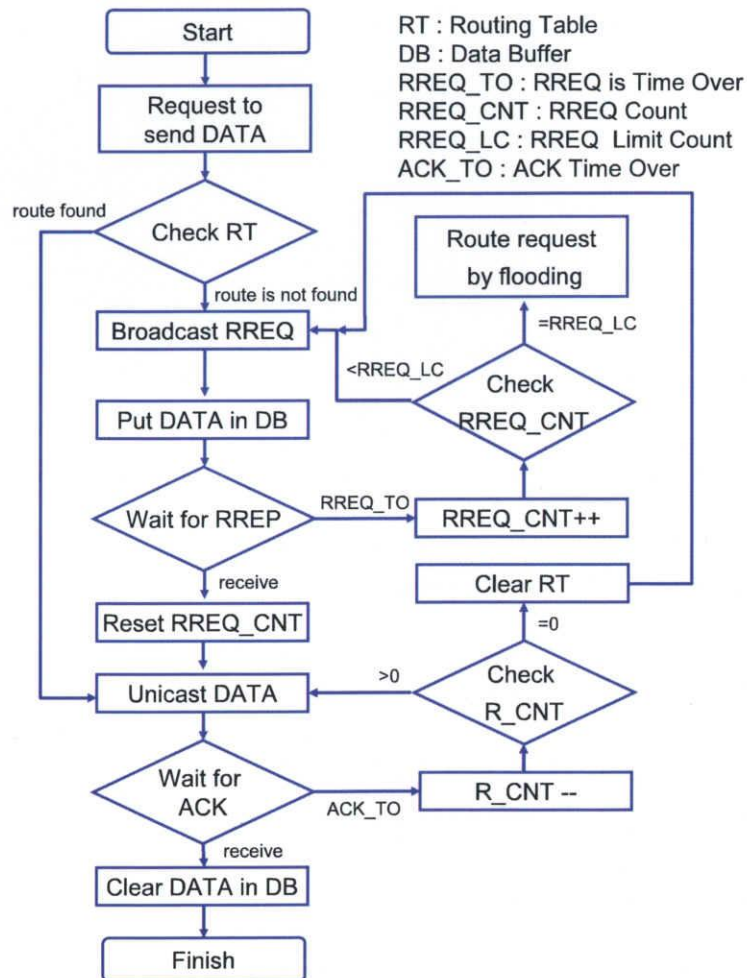


図 2.5 送信元端末における経路発見処理のフローチャート

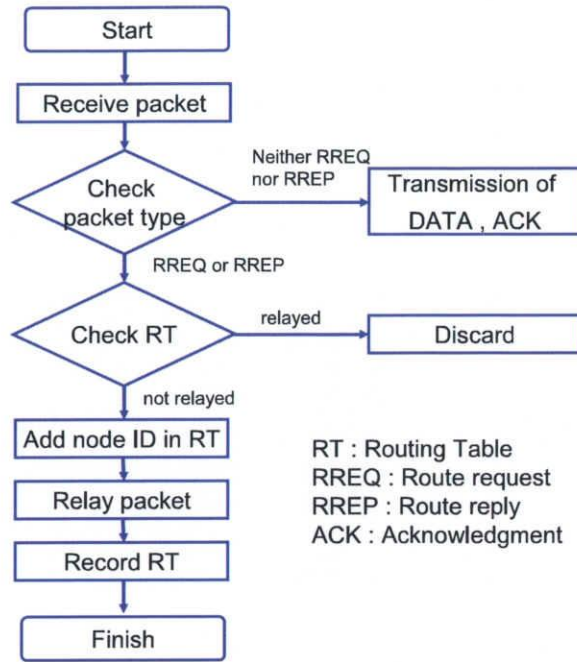


図 2.6 中継端末における経路発見処理のフローチャート

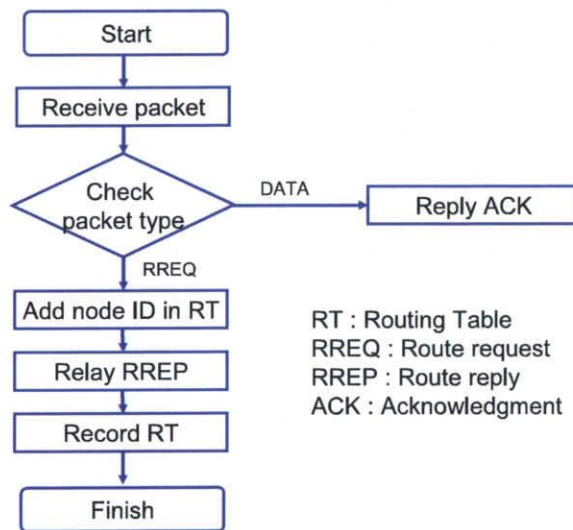


図 2.7 送信先端末における経路発見処理のフローチャート

する時に使用する。Uフラグは、経路表の中にエントリーが存在せず、シーケンス番号が分からない場合に使用する。

- reserved
送信予約する際、フィールドに0を格納する。
- hop count
送信元端末から何回転送されたかを表すフィールドであり、経路要求直後は0を設定する。
- RREQ ID
最後に送信した RREQ パケットで利用した RREQ ID に一つ加えた値を設定する。
- destination IP address
送信先端末の IP アドレスを示す。
- destination sequence number
送信先端末について最後に得たシーケンス番号を示し、経路表の中から検索する際に使用する。
- source IP address
送信元端末の IP アドレスを示す。
- source sequence number
送信先端末のシーケンス番号を複製するために、端末は RREQ パケットを作成する直前に送信元端末のシーケンス番号を増加させる。

RREQ パケットを受信した近隣の中継端末は、RREQ パケットのシーケンス番号を確認し、初めて受信した RREQ パケットの場合は、再ブロードキャストを行う。しかし、アドホックネットワーク全体に RREQ パケットの転送を可能にすると、ネットワーク上で多数の RREQ パケットが発生する。そこで、AODV では送信先端末の探索範囲を徐々に広げる方法を採用する。探索範囲の制御には RREQ パケットの IP ヘッダに用いられる TTL(Time To Live) を利用する。送信元端末は一回目の探索で TTL を決められた値に設定する。もし一定時間内に経路応答 (Route Reply(以下 RREP)) メッセージが得られない場合は、TTL を一定値増加させて、RREQ パケットを再送する。これらの処理を繰り返すことで、TTL が一定値以上になっても RREP が得られないければ、アドホックネットワーク全体に探索するように TTL を設定する。さらに、送信元端末は送信先端末に対して無効になった経路を保持していた

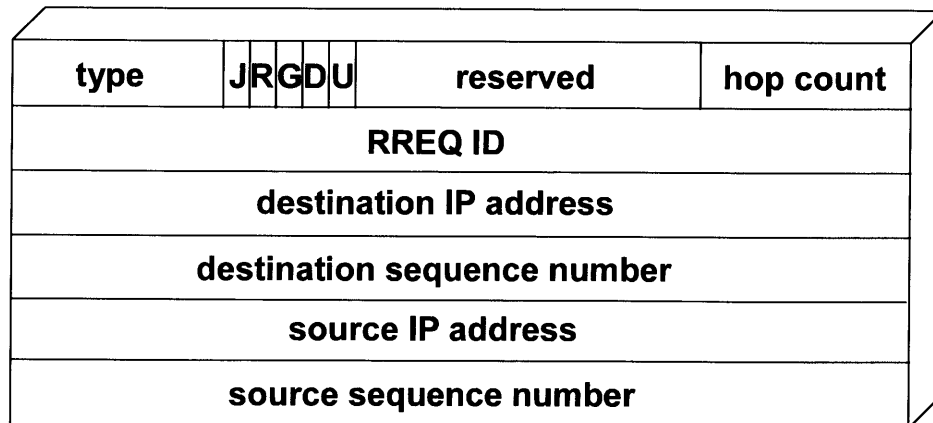


図 2.8 RREQ の構成

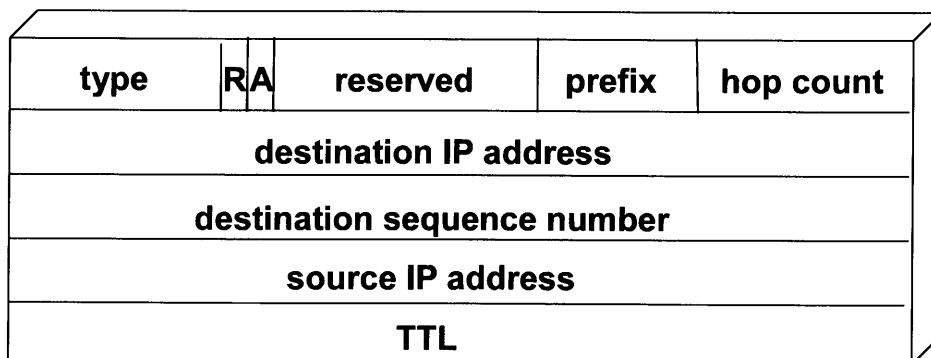


図 2.9 RREP パケットの構成

場合には、その経路の TTL の値に基づいて、TTL の初期値として決定する。このように無効な経路もすぐには破棄せず、一定時間保持することで、過去の情報を経路発見に活用する。

次に RREQ パケットを受信した端末が経路確立のための RREP パケットの作成の処理について述べる。図 2.9 に RREP パケットの構成を示す。RREP パケット内の各フィールドに格納される情報は以下になる。

- type
このパケットが RREP パケットであることを識別するためのフィールドで、2 を格納する。
- R,A flag
R フラグは、マルチキャスト通信を行う場合に用いる。A フラグは、ACK を必要としている場合に使用する。
- reserved
送信予約する際、フィールドに 0 を格納する。
- prefix
アドホックネットワークをいくつかのサブネットワークを分割して行う際に使用する。本論文では、使用しない。
- hop count
送信元端末から送信先端末までのホップ数を示す。
- destination IP address
送信先端末のアドレスを示す。
- destination sequence number
送信先端末について最後に得たシーケンス番号を示し、経路表の中から検索する際に使用する。
- source IP address
送信元端末のアドレスを示す。
- TTL
経路の有効時間を示す。

RREP パケットを作成する時、RREQ パケットの送信先端末のアドレスと送信元端末のアドレスを RREP パケットの対応するフィールドに複製する。AODV では、RREQ パケットを受信した端末が送信先端末である場合と送信先への経路を持つ

中継端末である場合で RREP パケットの作成処理が異なる。そのため、以下ではそれぞれの場合について説明を行う。

1. 送信先端末が RREP を返す場合：

送信先端末は RREP パケットを作成する直前に、送信先シーケンス番号を次のように更新する。RREQ パケットの送信先シーケンス番号に 1 加えた番号と送信先端末のシーケンス番号を比較し、大きい方の値を新しいシーケンス番号とする。送信先端末はこのシーケンス番号の値を RREP パケットの送信先シーケンス番号のフィールドに格納し、ホップカウントは 0、TTL は既定値を格納する。

2. 送信先端末以外の中継端末が RREP を返す場合：

RREP パケットの送信先シーケンス番号フィールドとホップカウントのフィールドについては、その端末が保持する順経路エントリに基づき設定する。RREP パケットの生存時間フィールドにはその経路エントリの残り有効時間（有効期限－現在時刻）を格納する。次に送信先端末への順経路と始点端末への逆経路のエントリをそれぞれ更新する。すなわち、RREQ パケットが通過してきた直前ホップの端末の IP アドレス（IP ヘッダの送信元アドレスから得られる）を送信先端末のプリコーサリストに入れる。同様に送信先端末へ向かう次ホップの端末を送信元端末のプリコーサリストに入れる。送信元端末は RREP パケット受信時に得られた送信先端末のシーケンス番号を保持する。もし経路が無効となる場合に、この同じ送信先端末への RREQ パケットを送る際に、RREQ パケットに含めることになる。

以上により RREQ パケットを受信した端末が送信先端末または送信先端末への経路を保持している中継端末の場合、その端末は RREP メッセージを作成する。RREP パケットには送信先端末の情報と送信元端末へ転送するために必要な情報を付加して送信を行う。そして、RREP パケットは RREQ パケットが送られてきた経路とは逆の経路を通ることで送信元端末に返信される。これにより、送信元端末と送信先端末との間で最短経路が選択される。もし送信元端末が複数の RREP パケットを受信した場合は、最初に RREP パケットが転送された経路を選択する。し

かし、後から届いた RREP パケットの情報でも、先に届いた RREP パケットのホップ数に比べて少ない場合や送信先シーケンス番号が大きい場合は、経路を更新することが可能である。これらの処理により、送信元端末は送信先端末への経路を確立する。経路確立後、送信元端末はバッファに格納しておいたデータパケットの送信を開始する。

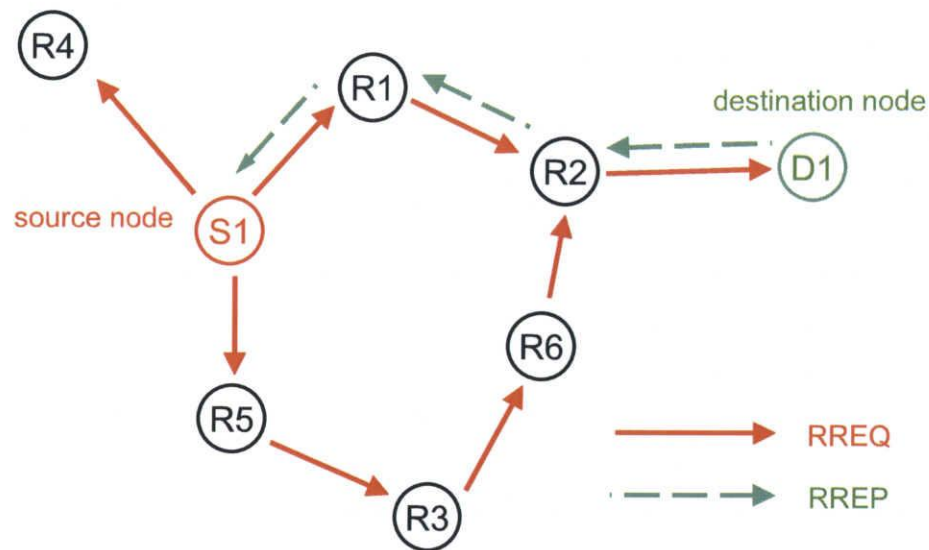


図 2.10 経路発見プロセス

図 2.10 は、送信元端末 S1 が送信先端末 D1 への経路発見プロセスを示す。図中では実線矢印が RREQ パケットの流れを示し、破線矢印が RREP パケットの流れを示す。S1 は D1 への経路探索を行うために、近隣の端末へ向けて RREQ パケットをブロードキャストする。RREQ パケットを受信した R1, R4, R5 は D1 への経路を保持していないため、再ブロードキャストを行う。R1 の近隣には R2 が存在し、R5 の近隣には R3 が存在するが、D1 ではないためそれぞれ再ブロードキャストを繰り返す。結果、R2 がブロードキャスト行くと D1 へ RREQ パケットを転送することが可能となる。RREQ パケットを受信した D1 は、RREQ パケットが転送されてきた $S1 \rightarrow R1 \rightarrow R2 \rightarrow D1$ の逆経路の $D1 \rightarrow R2 \rightarrow R1 \rightarrow S1$ の順に RREP パケットの転送を行う。D1 から送信された RREP パケットを S1 が受信することで、S1 と D1 の間で経路発見が完了する。

2.3.2 経路保全

経路発見により送信元端末と送信先端末の間で, RREQ・RREP パケットの配送により経路が確立する. 経路が確立しても, 各端末は端末情報を近隣端末と共有したのみで, 近隣端末のパケット送信などの影響により, 常に構築した経路が有効であるとは限らない. しかし, 端末間の有効なリンクが切断されたと判断できるのは, 実際にパケットを送信しなければ確認することができない. そこで, 有効なリンクの切断が発生した場合の処理について述べる.

リンク切断が発生した場合の処理

ある端末で発生した経路の切断はネットワーク全体に影響を与えるため, その経路を利用する送信元端末へ通知することが望ましいと考えられる. そのため, 近隣端末へのパケット送信失敗を MAC(Media Access Control) 層からの通知に基づいて, 検出することが考えられる. 例えば, IEEE802.11 ではパケット送信後, 確認応答メッセージ (ACK) が受信されない場合, または, RTS(Request To Send) 送信後, CTS(Clear To Send) が受信されない場合に, パケット送信が失敗したことを検出する. もし, 一定回数の再送を行ってもパケットを送信できなければリンク切断と判断する. MAC 層からの通知方法が利用できない場合には以下の方法が考えられている.

1. Hello メッセージを採用する方法:

端末は有効経路に含まれる隣接端末とのリンク維持を確認するため, 定期的に Hello メッセージを近隣端末のみに送信するローカルブロードキャストを行う. メッセージフォーマットとして RREP を利用して, IP ヘッダの TTL を 1 に設定する. 一定時間以上, Hello メッセージあるいはその他のパケットが受信されない場合, その隣接端末とのリンクが切断されたと判断する.

2. 受動確認方式を採用する方法:

この受信確認方式とは, 対称リンクの端末 A と端末 B が存在する時, 端末 A から端末 B へのパケット転送に対する確認応答を端末 B から端末 A へ直接送信する. 非対称リンクの時は, 複数ホップを経由して確認応答を返送する.

送信したパケットに対して、確認応答が得られるまで、確認応答要求を繰り返し行う。確認応答要求は独立のパケットとして、あるいは再送パケットや後続パケットへ相乗りさせることで、再送を行う。確認応答要求が一定回数に達しても確認応答が得られなかったら、次ホップへのリンクが切断されたと判断し、確認応答が得られなかったパケットを破棄する。また、このリンクを経路キャッシュから削除し、このリンクで最後に確認応答が得られた後にこのリンクを含む送信先経路を利用してパケットを送信したすべての送信先端末へ、経路エラー (Route Error(以下 (RERR))) メッセージを作成し、送信する。RERR パケットの作成については次項で説明を行う。RERR パケットを送るための送信先経路の発見は通常のデータパケットの場合と同様である。RERR パケットを受信した送信先端末は経路キャッシュからそのリンクを含む送信先経路を削除する。

3. 上記 1, 2 以外の方法：

受動確認が得られない時や次ホップが送信先端末の場合には、次ホップからのパケット受信 (Hello メッセージを含む)、次ホップへの RREQ 送信、次ホップへの ICMP(Internet Control Message Protocol) エコー要求などで次ホップへのリンクを確認する。これにより、リンクを検出できない場合、リンク切断と判定する。

RERR 作成

図 2.11 に RERR パケットの構成を示す。RERR パケット内の各フィールドに格納される情報は以下のようなになる。

- type
パケットが RERR パケットであることを識別するためのフィールドで、3 を格納する。
- N flag
ローカル経路修復を行ったときに、N フラグを用いる。N フラグを用いることで、上流端末に経路を破棄行わないようにすることを知らせる。
- reserved

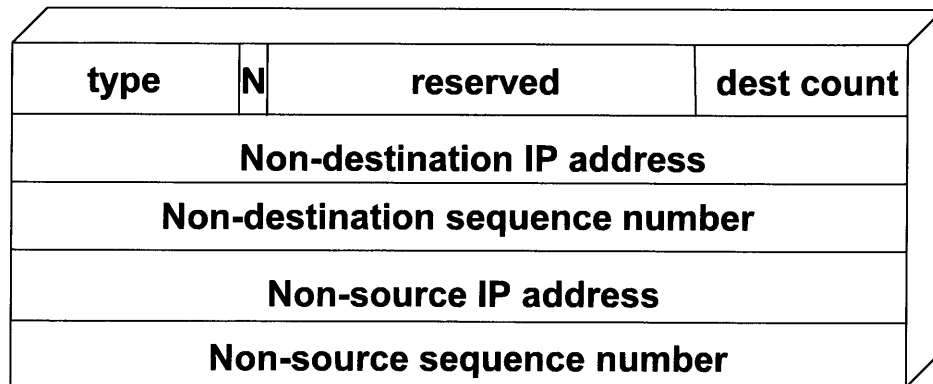


図 2.11 RERR の構成

送信する際, フィールドに 0 を格納する.

- Dest Count
Non-destination IP address と Non-destination sequence number を一つの組とし, この組の個数を示す.
- Non-destination IP address
リンク切断により, 到着不可の送信先端末の IP アドレスを示す.
- Non-destination sequence number
リンク切断により, 到着不可の送信先端末のシーケンス番号を示す.
- Non-source sequence number
リンク切断により, 到着不可の送信元端末の IP アドレスを示す.

リンク切断を検出した端末は, そのリンクを使用していた経路のエントリを抽出し, それらが無効化する. 同時に RERR パケットを作成し, 無効化された経路の送信先端末の IP アドレスのリストを格納し, これらの端末の上流端末へ送信する. 又, 受信したパケットの送信先端末への有効な経路が存在しない場合にも RERR パケットを作成する. このとき, 送信先端末シーケンス番号を 1 つ増やし, その値を RERR パケットに格納する. 上流端末が 1 つあれば RERR パケットをユニキャストで送り, 複数ある場合はユニキャストを繰り返すか, TTL を 1 としてブロードキャストする. RERR パケットを受信した端末は RERR パケットの送信先端末のリストを参照する. そして, 自身の経路表の中に含まれる送信先端末への経路エントリがあり, その経路エントリの次ホップが RERR パケットを送信してきた隣接端末に

末から送信された後続のデータパケットを一時バッファリングする。一定時間内に RREP パケットが得られなければ、通常のリンク切断と同様に RERR パケットを送信元端末へ向けて通知する。中継端末は送信先端末から RREP パケットが返信された場合、まず新たな経路と以前の経路の送信先端末へのホップ数を比較する。このとき、新たな経路が以前の経路よりホップ数が多い場合には、それを送信元端末へ通知し、N フラグを立てた RERR パケットを上流端末へ転送する。その後は、通常の RREP パケットを受信した場合と同様に経路表のエントリを更新し、RREP パケットを上流端末へ転送する。この処理は上流端末の経路情報を更新する必要があるからである。このようにして RREP パケットが送信元端末へ到着した時点で経路修復を完了する。図 2.13 では、端末 B と端末 C でリンク切断が発生し、リンクの修復を端末 B が行う場合の動作例を示す。端末 S1 が端末 D1 への経路として、 $S1 \rightarrow A \rightarrow B \rightarrow C \rightarrow D1$ の経路を確立し、 $B \rightarrow C$ へのリンク切断が発生した場合を考える。このままでは、端末 S1 から端末 D1 へデータパケットを送信することが不可能なため、端末 B は後続から送信されたデータパケットを一時バッファリングする。更に、端末 D1 との経路を再構築するために近隣端末に RRRQ パケットをブロードキャストする。ブロードキャストにより、 $B \rightarrow D \rightarrow D1$ の順で RREQ パケットを転送する。端末 D1 は端末 B へ RREP パケットを返信することで、新たに、 $S1 \rightarrow A \rightarrow B \rightarrow D \rightarrow D1$ の経路が確立する。結果、端末 S1 と端末 D1 との間の経路は修復されたため、データの送信を再開する。

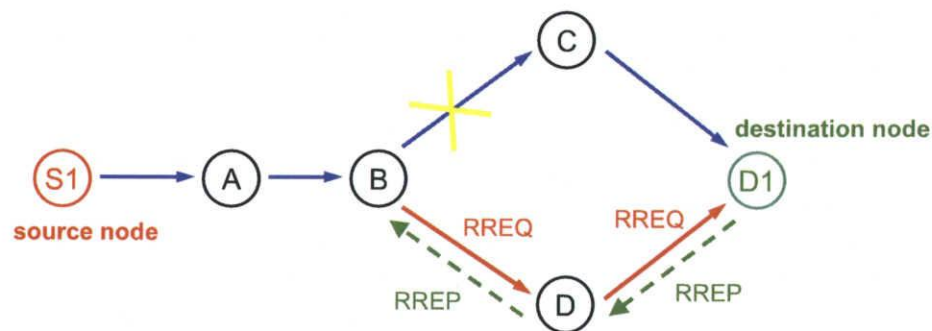


図 2.13 ローカル経路修復

第3章

信号電力に基づく経路制御情報の削減手法の提案

本章では、既存のルーティングプロトコルを用いて行う経路探索処理に着目する。アドホックネットワークでは、各端末は情報を転送するために近隣端末と通信を行う。直接通信を行うことが不可能な場合は、通信相手を探索する必要がある。既存のルーティングプロトコルでは、各端末が経路情報をネットワーク全体に報知することにより、直接通信が不可能な端末間の経路探索を行う。このような動作をフラッディングと呼び、実装が容易なことから多くのプロトコルで採用されている。しかし、フラッディングを行うだけでは、経路探索に効率の悪い端末も不要な送信を行う状況が発生する。そのため、既存のルーティングプロトコルはネットワーク内に存在する端末数により、転送する端末が大きく変化するため有効に機能しない場合が発生する。もし、ネットワーク内に端末が多数存在する場合は、過剰な経路探索情報がフラッディングされる。結果として、冗長な経路情報がネットワークの帯域を過剰に消費することで、ネットワークの性能が劣化する。そこで、提案方式では端末が多数存在する場合に、ネットワークの性能を劣化させることなく、経路探索を行うことが可能なプロトコルを提案する。1節で端末が多数存在する状況下で既存のルーティングプロトコルを用いた時に生じる問題について説明を述べる。2節で提案手法である信号電力に基づく経路制御手法について述べ、3節では提案方式の有効性を計算機シミュレーションを行うことで明らかにする。

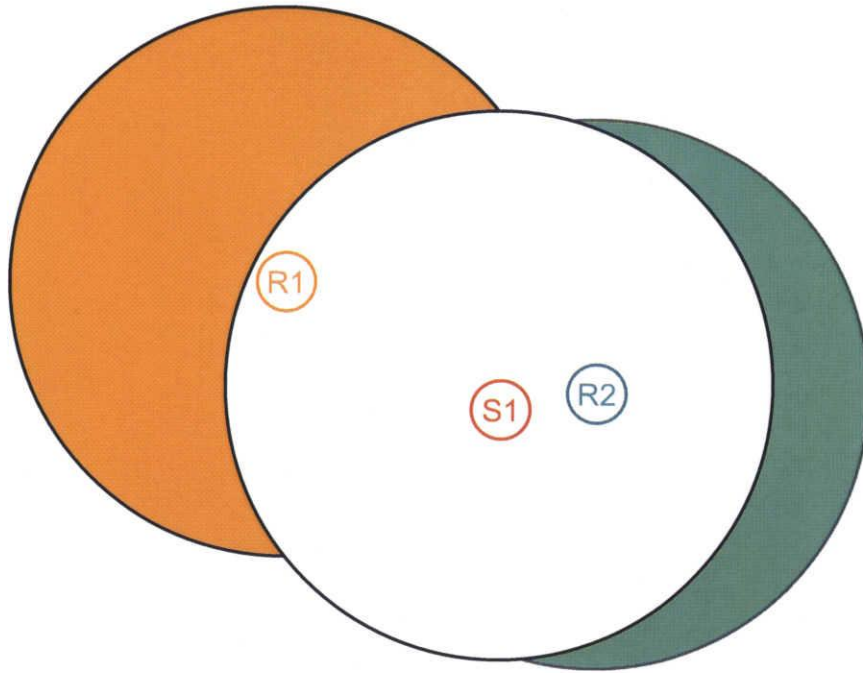


図 3.1 中継端末の探索エリアの比較

3.1 密集端末が経路探索に与える影響

各端末は経路探索する場合、経路情報を転送することで探索を行う。経路探索を行う際、端末が多数存在すると端末数に比例して経路構築パケットが増大する。結果として、ネットワーク上に経路構築パケットが多数発生するため、正常な通信を行うことが困難になる。そこで、経路情報を中継する端末が送信端末との間の距離に対する探索エリアに着目する。図 3.1 では、端末 R1 と端末 R2 が再転送を行う場合の探索エリアを示す。また、端末 R1 と端末 S1 との間の距離は端末 R2 と端末 S1 との間の距離より長いものとする。図 3.1 より、端末 S1 との距離が遠いほど新たに探索可能なエリアが広いことが確認できる。これにより、端末間距離の遠い中継端末が再転送を行うことで、効率的な経路探索が可能となる。特に端末が多数存在する状況下では通信半径内に多数の端末が存在する。そのため、可能な限り探索エリアの広い端末が経路情報を中継することが有効である。

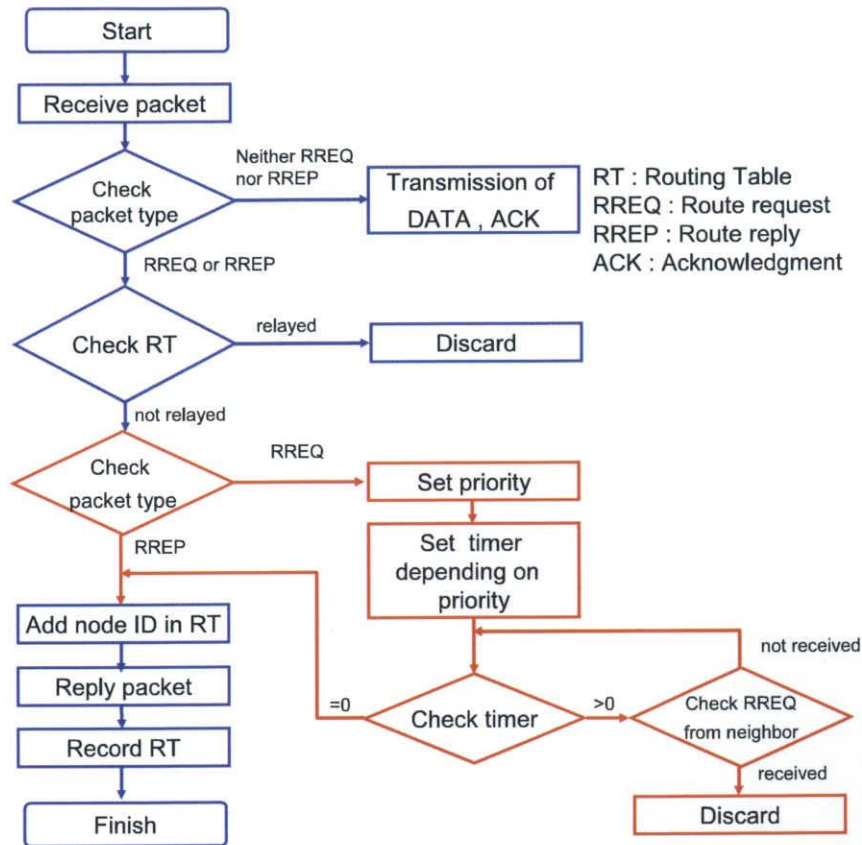


図 3.2 信号電力に基づくルーティング手法を用いた時の中継端末におけるフローチャート

3.2 信号電力に基づくルーティング手法

本論文では、経路構築時に発生する多量の制御パケットを抑制するために、既存のルーティングプロトコルに適応することが可能である手法を提案する。本項では、リアクティブ型の代表的な AODV を例として用いることで、経路構築時に発生する多量の制御パケットの抑制を行う。図 3.2 では、信号電力に基づくルーティング手法を用いた時の中継端末におけるフローチャートを示す。AODV の処理に従い、データパケットの送信要求が発生した時、経路構築を行うために RREQ パケットのブロードキャストを行う。RREQ パケットを受信した端末は、受信した RREQ により受信電力を推定することで、端末間距離を推定することが可能である。この

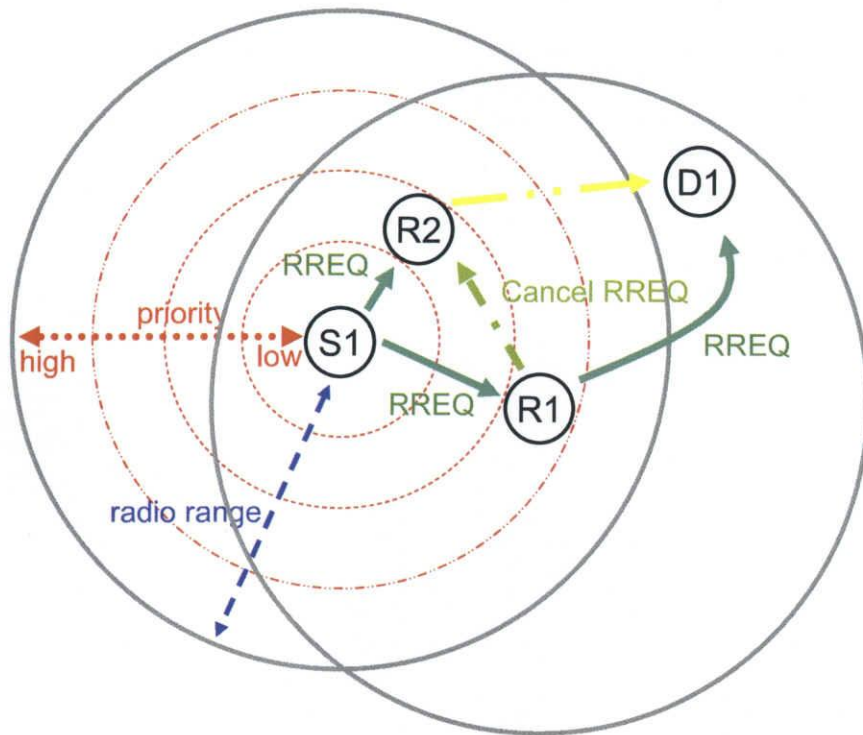


図 3.3 優先度に応じて経路制御を行う際の動作例

時, AODV では RREQ パケットを受信した端末が送信先端末でない場合, RREQ パケットを受信した全ての端末が転送を行う. そこで, 提案手法では推定した受信電力に応じて RREQ パケットの転送するためのタイマを設置する. このタイマは, タイムアウトすると端末は RREQ パケットをブロードキャストを行う. タイマ時間の設定については, 次のように設定する. 受信電力が小さい場合, タイマ時間を短く設定し, 受信電力が大きい場合, タイマ時間を長く設定する. 異なるタイマ時間を設けた理由は, 推定した受信電力が小さい時, RREQ パケットを受信した端末は遠方に存在する. 一方, 推定した受信電力が大きい場合は, RREQ パケットを受信した端末は近隣に存在することが考えられる. 次にタイムアウト後, ブロードキャストされた RREQ パケットについて説明する. ブロードキャストされた RREQ パケットは, 新たに RREQ パケットを受信した端末とすでに同一の RREQ パケットを受信した端末に分けることができる. 新たに RREQ パケットを受信した端末は, 送信先端末でない場合を除き, 再度 RREQ パケットをブロードキャストするためにタ

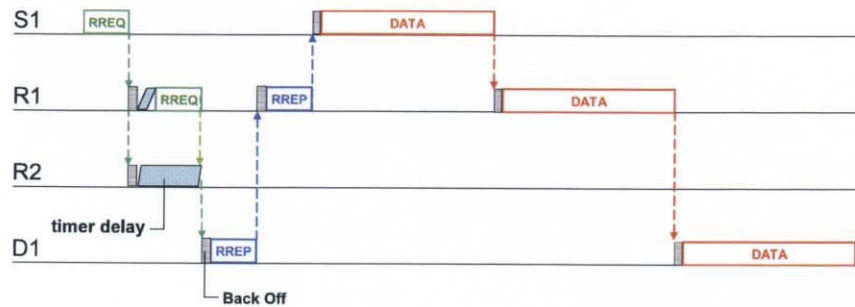


図 3.4 優先度に応じて経路制御を行う際のパケットの配送過程

イマを設置する. 同一の RREQ パケットを受信した端末は, 近隣端末がすでに同一の RREQ パケットのブロードキャストを行ったと判断し, タイマを停止し, RREQ パケットを破棄する.

図 3.3 に, 提案方式を用いて送信元端末 S1 と送信先端末 D1 とが通信する場合の動作例を示す. 図 3.4 に, 優先度に応じて経路制御を行う際のパケットの配送過程を示す. 送信元端末 S1 が送信先端末 D1 にデータパケットを送るとき, 送信元端末 S1 は RREQ パケットをブロードキャストする. この場合, 通信範囲内に存在する中継端末 R1, R2 が RREQ を受信する. この時, 送信元端末 S1 より距離の遠い中継端末 R1 の端末に中継端末 R2 よりも高い優先度が与えられ, 中継端末 R1 が先に RREQ のブロードキャストを行う. 中継端末 R1 によるブロードキャストにより, R2 はタイマ終了後に送信しようとしていた RREQ の送信を中止する. また, 中継端末 R1 がブロードキャストした RREQ パケットは送信先端末 D1 に受信されるため, S1-R1-D1 という経路が確立される.

3.3 計算機シミュレーションによる特性評価

提案方式の特性を検討するために, 計算機シミュレーションを行った. シミュレーションでは, ブロードキャストストームが起こりうるように端末が多数存在する状況下で行う. また, 表 3.1 にシミュレーションパラメータを示す.

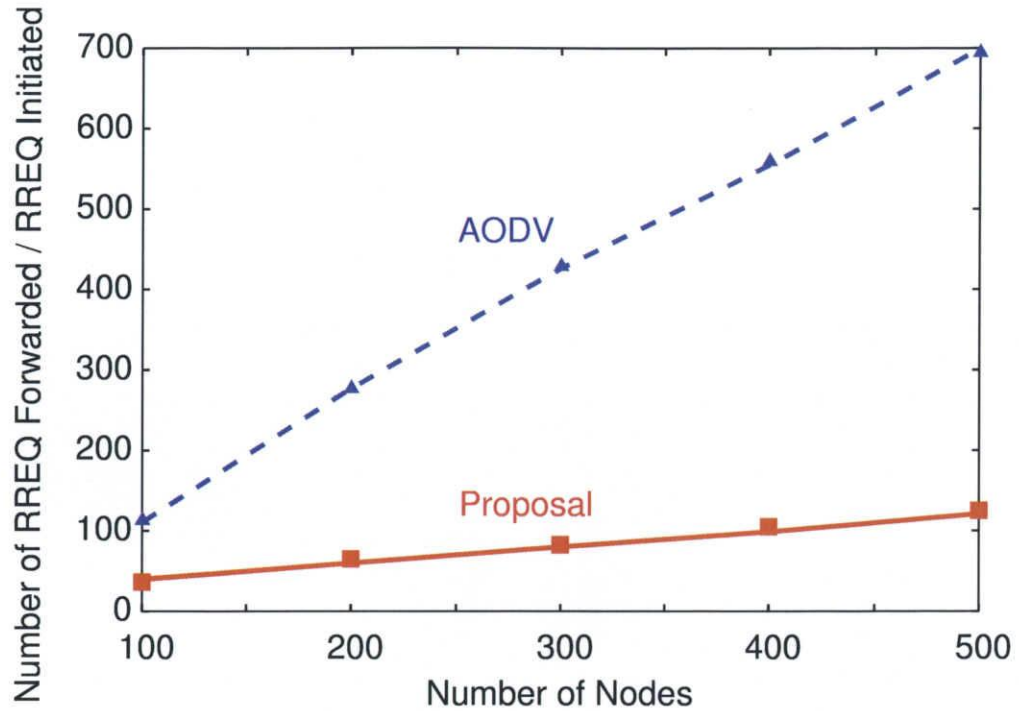


図 3.5 総端末数に対する RREQ パケットのブロードキャスト数

3.3.1 総端末数に対する RREQ パケットのブロードキャスト数

図 3.5 に、総端末数に対する RREQ パケットのブロードキャスト数を示す。ここでの RREQ パケットのブロードキャスト数は、1 回の経路構築の際にネットワーク上に送信される RREQ パケットの数を示す。結果より、総端末数が増加するに伴い、制御パケット数は増加する傾向がある。既存の AODV では、端末数が増加するに従って、1 回のブロードキャストで RREQ を受信する端末が多数存在するため再ブロードキャストする端末数も増えることが分かる。それに対して、提案方式では、RREQ を受信した後にブロードキャストを行わず、優先度の高い端末から順にブロードキャストを行う制御を行った。そのため、優先度の高い端末のみが再ブロードキャストを行うことで、冗長な RREQ の削減を行うことが可能であることを示した。

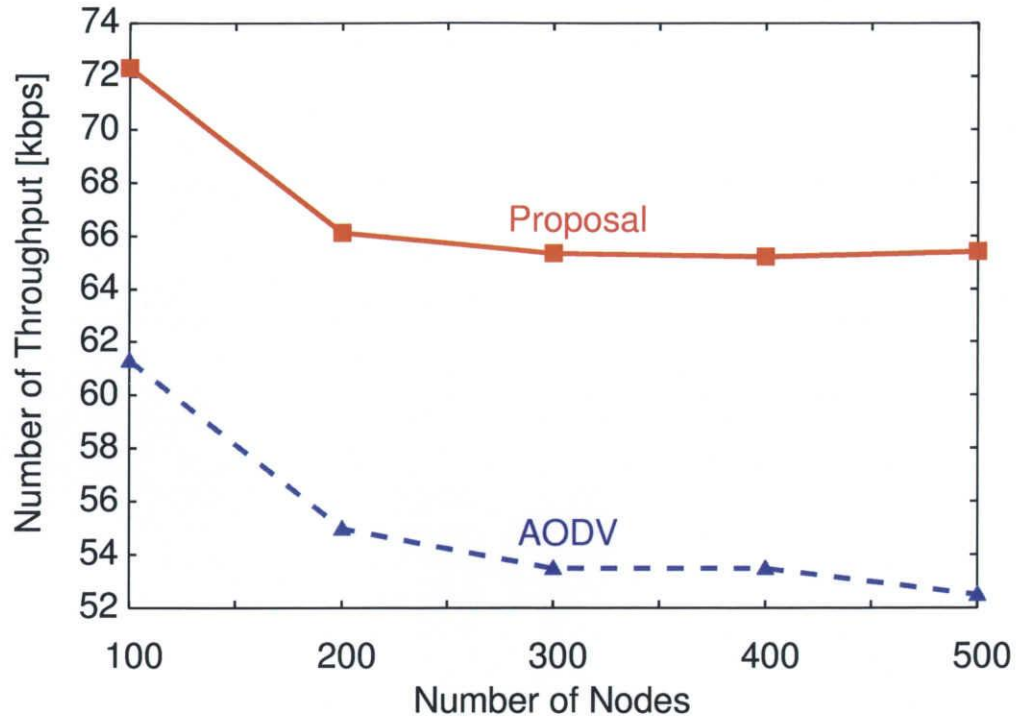


図 3.6 総端末数に対するスループット特性

3.3.2 総端末数に対するスループット特性

図 3.6 に、総端末数に対するスループット特性を示す。図 3.6 より、既存の AODV に比べ提案方式の方がスループット特性が改善していることがわかる。これは、タイマ機能及びブロードキャストの中止を行うことで、冗長な RREQ のブロードキャストを中止し、ネットワーク上に RREQ パケットが溢れている状況が緩和されたと考えられる。また、端末数が増加するに従い、既存の AODV はスループット特性の劣化が確認できる。一方、提案方式では高いスループットを維持することが出来ている。これは、端末増加により AODV では、多数の RREQ パケットが送信されたことによりネットワークにかかる負荷が増加したため特性が劣化したと考えられる。それに対し、提案方式では端末が増加した場合でも、ネットワークにかかる負荷がタイマ及びブロードキャストの中止により、トラヒックが一定に保たれていることが考えられる。そのため、端末増加に対しても AODV に比べ、スループット特性の

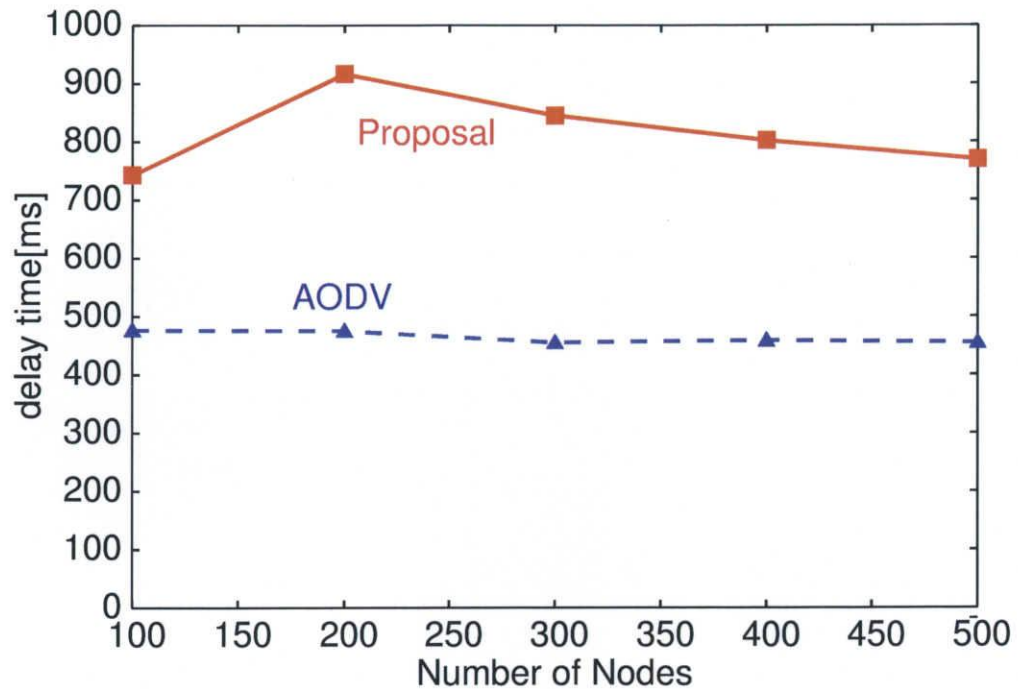


図 3.7 総端末数に対する遅延時間

改善することが可能である。

3.3.3 総端末数に対する遅延時間

図 3.7 に、総端末数に対する遅延時間を示す。ここでの遅延時間は、送信元端末より経路要求が発生し、経路構築に要した時間を示す。結果より、タイマ機能を用いた提案方式は既存の AODV に比べ遅延時間が増加していることが確認できる。提案方式では、通信半径内の遠方に存在する端末の優先度を高く設定する。今回のシミュレーションでは、5 種類のタイマ時間を設けたことにより、最短のタイマ時間になる場所に端末が存在しているとは限らない。そのため、既存の AODV に比べ遅延時間が増加したといえる。

表 3.1 シミュレーションパラメータ

シミュレータ	Qualnet
シミュレーション時間	600[s]
シミュレータエリア	750[m] × 750[m]
ノード数	10~500
ノード配置	ランダム配置
移動度	なし
呼の発生	ポワソン分布 平均 0.2 個発生
データパケット長	512[byte]
通信時間	10[s]
送信間隔	50[ms]
無線アクセスプロトコル	IEEE802.11
受信モデル	SNR threshold BASED
伝送速度	2[Mbps]
通信半径	100[m]
無線伝播環境	自由伝播モデル
アプリケーション	CBR
ルーティングプロトコル	AODV
タイマ時間の設定	通信半径内で5種類設定
試行回数	100 回

第4章

局所代替経路を用いたアドホックルーティング手法の提案

本章では、既存のルーティングプロトコルにおける経路構築後の処理に着目する。アドホックネットワークでは、各端末の近隣で複数の経路が同時に構築され、同時に通信が行われる。もし近隣の端末同士が同時に送信を行った場合、ある端末においてパケット衝突が発生し、正常にパケットを受信することが不可能になる。そこで、各端末は同時にパケット送信を避けるために、パケット送信前に近隣端末からの搬送波の有無を確認する。搬送波を確認することで、パケットの送信可能か判断することが可能である。もし、近隣端末からの搬送波を感知した場合は、パケット衝突を回避するために一定時間待機した後、再び搬送波の有無を確認する。この制御を CSMA/CA と呼ぶ。しかし、電波を通さない障害物などの影響により、近隣端末の搬送波を確認できない場合が発生する。そのため、CSMA/CA を行うことで各端末は全てのパケット衝突を回避することは不可能であり、このような状況を隠れ端末問題と呼ぶ。そこで、隠れ端末問題を解決するために、パケット送信前に送信要求と受信準備完了の確認を近隣端末に報知する手法として RTS/CTS 方式が提案されている。RTS/CTS 方式を用いることで、隠れ端末問題は解決する。しかし、アドホックネットワークでは複数の端末との間で経路が構築されるため、RTS/CTS 方式により構築した経路が一時的に利用困難な状況が発生する。このような状況をさらされ端末問題と呼ぶ。さらされ端末問題が発生することで、一時的に通信を行うことが出来なくなり、経路上の端末が存在しないと誤判定する端末が発生す

る。そのため、この端末はデータパケットを次の中継端末に送信できないため、一時的に通信を行うことができない端末との経路を切断し、再構築処理を行う。そこで、提案方式では一時的に経路が利用できなくなった場合に備え、主経路の構築とは別に代替経路の構築を行う。代替経路を利用することで、誤判定により経路の切断を防止する。以下、1節で隠れ端末問題とさらされ端末がアドホックネットワーク与える影響を示し、2節で提案方式である代替経路構築方式について述べる。3節では、提案方式を計算機シミュレーションを行うことで明らかにする。

4.1 アドホックネットワークにおいてパケット配送時に生じる問題

本節では、アドホックネットワークにおいてパケット配送時に発生する隠れ端末問題とさらされ端末問題について述べる。

4.1.1 隠れ端末問題がアドホックネットワークに与える影響

アドホックネットワークでは、端末間で通信を行うことにより、各端末が近隣で同時に通信を行う状況が頻繁に発生する。そのため、各端末は各々のタイミングでパケットの送信を行うとパケット衝突が発生する。各端末は近隣で通信が行われていないか確認し、無線チャネルの使用状況を確認してから送信する CSMA/CA アクセス制御を行う。CSMA/CA を用いることで、もし近隣の端末が通信を行っている間は、送信を見合わせることで、パケット衝突の回避を行うことが可能である。しかし、端末間の距離が遠く離れていたり、電波を通さない障害物などの影響により、近隣端末の無線信号を確認できない場合が発生する。このような状況下で、端末が近隣で通信が行われていないと誤判定をした場合、通信相手の端末でパケット衝突が発生する。これを隠れ端末問題と呼ぶ。図 4.1 では、端末 A と端末 B が端末 D へ向けてパケットを送信する際に発生した隠れ端末問題の例を示す。また、端末 A, B 間には電波を通さない障害物があるため、互いの信号を受信することはできないものとする。端末 A, B は互いに端末 D と通信を行う際、CSMA/CA により近隣で通信が行われていないか無線チャネルの状況を確認する。この時、端末 A と端

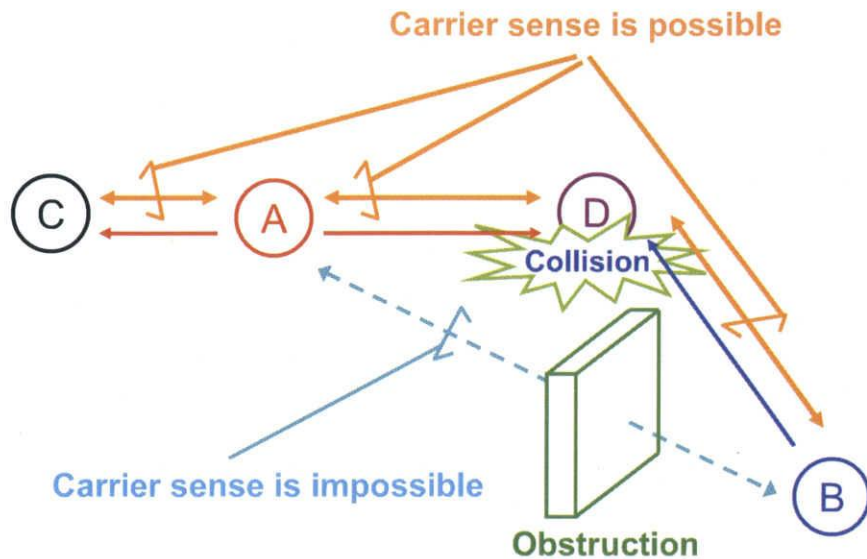


図 4.1 隠れ端末問題

末 B は互いの信号を受信できないため、送信可能と判断し、端末 A と端末 B は端末 D へ向けて送信を開始する。結果として、端末 D でパケット衝突が発生する。そこで、隠れ端末問題を解決するために、近隣端末にチャネルが使用中であることを知らせる RTS/CTS 方式が提案されている。RTS/CTS 方式は、RTS パケットと CTS パケットからなり、これらのパケットを送信側と受信側で送受信を行うことで周辺端末にチャネルを使用する事を知らせることが可能となる。

図 4.2 では、RTS/CTS 方式を用いて、端末 A が端末 D にデータパケットを送信する場合の動作例を示す。端末 A が端末 D にデータパケットの送信要求が発生した場合、同時間に近隣端末が送信を行わないように、端末 A は RTS パケットを送信する①。RTS パケットを受信した隣接端末 C は、RTS パケットを送信した端末の通信が終わるまでの時間として NAV(Network Allocation Vector) 時間を設ける。また、RTS パケットを受信した端末 B は、受信することが可能な状態を示す CTS パケットを端末 A に送信する②。CTS パケットを送信する事で、端末 A に送信許可を出すだけでなく、近隣端末に端末 A と端末 D がこれから通信を行うことを知らせることが可能である。これによって、端末 A は端末 D との間で、近隣端末から邪魔されることなく、データパケットを送信を行うことができる③。データパケットを受信した端末

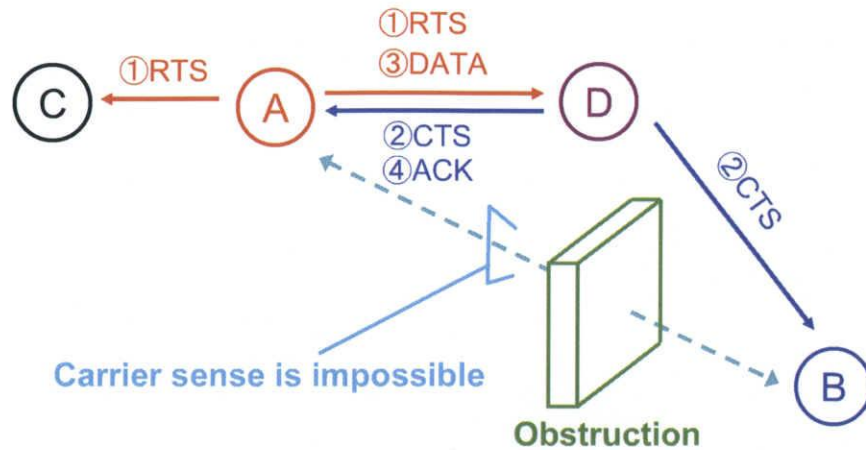


図 4.2 RTS/CTS 方式

B は正常に受信完了したことを端末 A に知らせるために, ACK(Acknowledgment) パケットを返信する④. しかし, RTS/CTS 方式を用いることで, さらされ端末問題が発生する.

4.1.2 アドホックネットワークに対するさらされ端末問題

さらされ端末問題とは, 隣接する端末が送信した RTS/CTS パケットを受信することで, 他の端末への送信を抑制する問題が発生する.

図 4.3 では, さらされ端末問題の動作例を示し, 図 4.4 では, さらされ端末問題が発生した時のパケットの流れを示す. 図 4.3 において, 送信元端末 S1 と送信先端末 D1, 送信元端末 S2 と送信先端末 D2 との間でデータパケットを送信する場合を考える. このとき, S1 は $S1 \rightarrow R1 \rightarrow R2 \rightarrow D1$ の経路が構築されており, S2 は $S2 \rightarrow D2$ の経路が構築されているとする. もし, S2 が D2 に向けてデータパケットを送信するために RTS パケットを周辺端末に向けて送信した時, D2 は S2 に CTS パケットを返信し, R2 は S2 の通信が終わるまで送信を抑制する NAV 時間を設定する. NAV 時間が終わるまで, R2 はあらゆるパケットを受信しても返信することは出来ない. しかし, NAV 時間中であることは R2 の周辺端末は知ることができないため, $S1 \rightarrow D1$ の経路上の端末 R1 から RTS パケットを受信しても, CTS

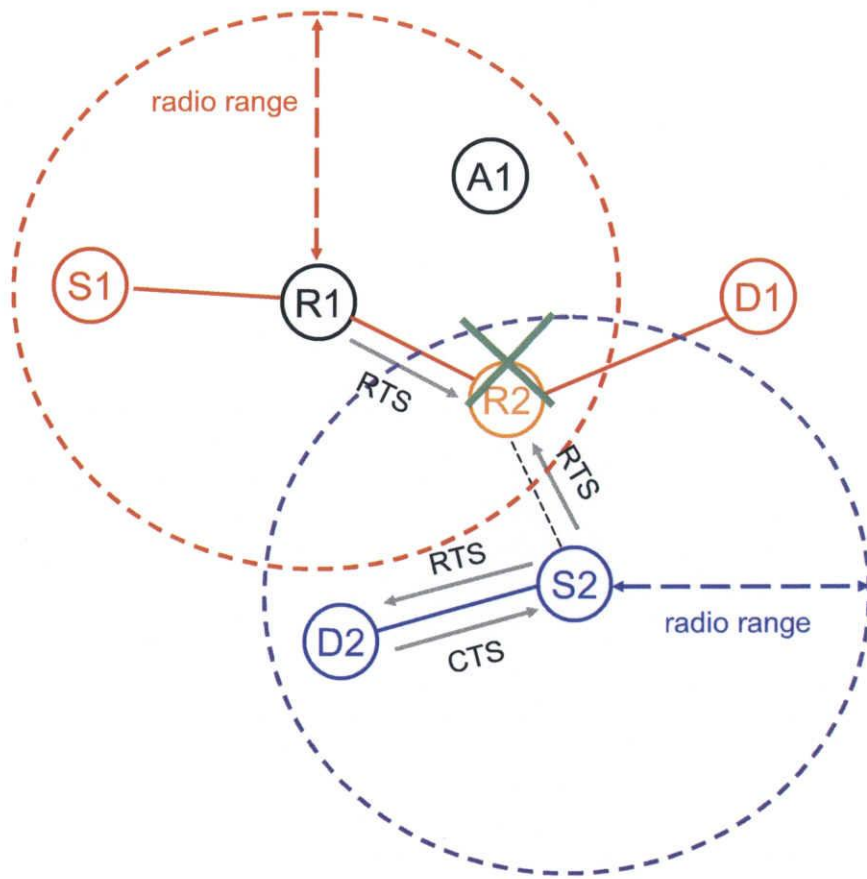


図 4.3 さらにされ端末問題

パケットを返信できない. これにより, R1 と R2 との間で一時的に通信不可能な状態が発生する. 図 4.4 のように, R1 は R2 に対して, CTS パケットを返信してもらうために, RTS パケットの再送を行う. RTS パケットを複数回再送したにも関わらず R2 から CTS パケットを受信できなければ, R1 は R2 が存在しないものとして経路損失を送信元端末に知らせる処理を行う. 結果, 送信元端末は経路再構築処理を行うことになる.

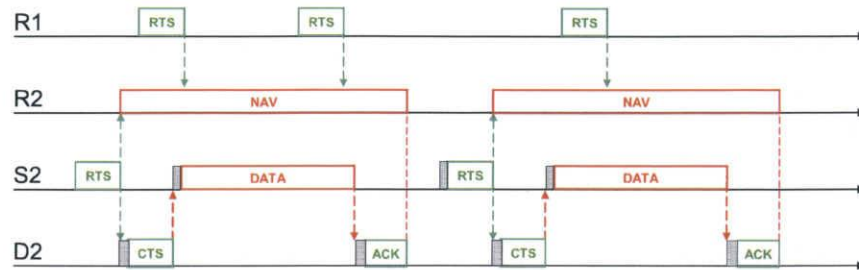


図 4.4 さらに端末問題が発生した時のパケットの流れ

4.2 代替経路構築方式

本論文では、端末の移動によるリンク損失ではなく、RTS/CTS方式による一時的な通信抑制に注目する。図 4.5 に、代替経路が作成可能な端末の配置状態を示す。図 4.5 では、送信端末 S1、中継端末 R1、R2、受信端末 D1 の通信と、送信端末 S2 と受信端末 D2 の通信が存在する状況を示している。そして、近隣端末 A1 は中継端末 R1 と受信端末 D1 と通信可能な状況を示している。

図 4.5 では、送信端末 S2 と受信端末 D2 が通信を行う場合、受信端末 D2 が送信した CTS パケットにより、中継端末 R2 は一時的に通信が行えなくなる。結果として、中継端末 R1 から送信された RTS パケットに対する CTS パケットの送信が行えなくなる。RTS/CTS 方式では複数回の再送が行われるが、長期にわたって中継端末 R2 の通信が抑制された場合、中継端末 R1 はリンク損失が発生したと判断し、送信端末 S1 に向けて RERR パケットの送信を行う。また、RERR パケットを受信した送信端末 S1 は再度経路構築を行うため、一時的に通信が不可能となる。提案方式では、AODV により経路構築が行われた後、経路上の端末がさらされ端末問題による影響を受けた場合に備え、近隣端末が代替経路の作成を行う。代替経路は構築された経路の近隣端末が構築することにより、一時的な通信抑制に対処する。

4.2.1 近隣端末による代替経路の構築

AODV では、経路構築を行う際に、RREQ パケットが送信元端末から送信先端末に向けてフラッドされる。また、RREQ パケットを受信した送信先端末は送信元端末に向けて RREP パケットを返信する。これらの制御パケットは近隣端末

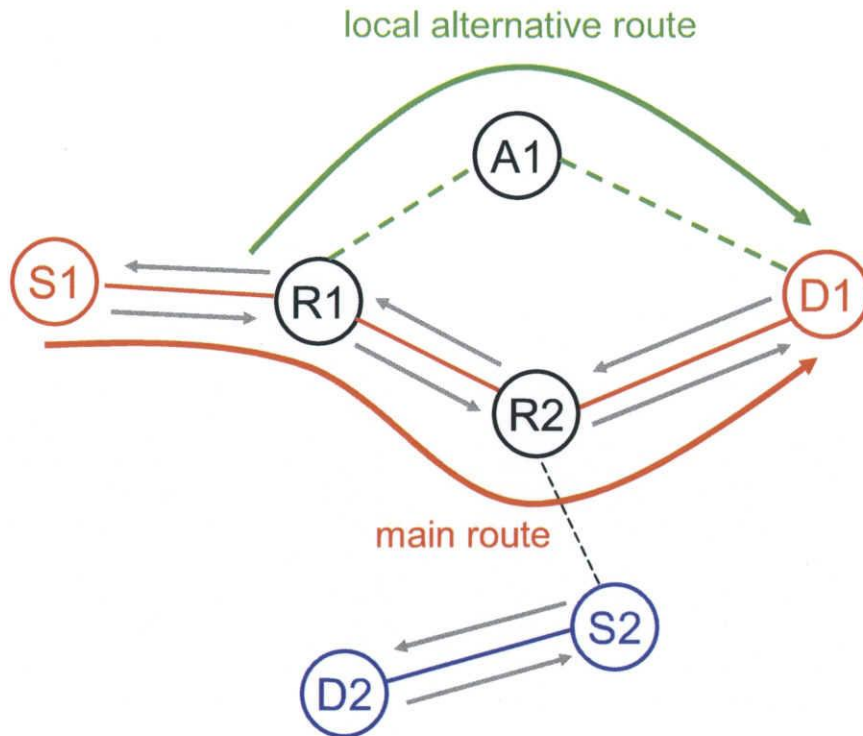


図 4.5 代替経路が利用可能な端末配置例

も受信可能であるため、構築される経路周辺の端末も経路の存在を確認することが可能となる。また、近隣端末が異なる経路上の端末から RREP パケットを複数受信した場合、この近隣端末は経路上の複数の端末と通信可能なことを示している。つまり、この近隣端末は代替経路を作成可能な位置に存在していることを示している。そこで、本論文では、近隣端末が主経路上の端末から複数回 RREP パケットを受信した時、代替経路構築手続きを開始するものとする。

図 4.6 に AODV の主経路の構築過程と代替経路の構築過程を示す。例では、近隣端末 A1 が受信端末 D1、中継端末 R2、R1 からの送信される RREP パケットを受信していることが確認できる。この結果、近隣端末 A1 は中継端末 R1 と受信端末 D1 に対して代替経路構築パケット (AREQ: Alternative Route Request) の送信を行う。また、中継端末 R1 と受信端末 D1 は代替経路となる近隣端末 A1 との間で経路確立を行うための代替経路確認パケット (AREP: Alternative Route Reply) を返信する。こ

D2からのさらされ端末問題による影響を受けた場合の、代替経路の利用過程を示す。図では、送信端末 S2 と受信端末 D2 間の通信により、中継端末 R2 が一時的に通信不可能となっている状況である。そのため、中継端末 R1 が中継端末 R2 に向けて送信を行うために RTS パケットを送信したとしても、中継端末 R2 は CTS パケットを返信することができない。中継端末 R1 は複数回の RTS 再送にも関わらず、CTS パケットを受信できなかった場合、代替経路の利用を決定する。代替経路の利用を決定した場合、中継端末 R1 は代替経路となる端末 A1 に向けて RTS パケットの送信を行う。端末 A1 は中継端末 R1 からの RTS パケットに対して CTS パケットの返信を行うことで、代替経路を利用するデータパケットの受信を行う。そして、端末 A1 は経路テーブルに記載されている正規の経路上の端末に向けてデータの転送を試みる。このような動作を行うことで、さらされ端末問題により一時的に通信が行えない経路端末の代理を近隣端末が行う。

4.3 計算機シミュレーションによる特性評価

提案方式の特性を検討するために、シミュレーションを行った。シミュレーションでは、さらされ端末問題によるリンク損失の影響を明らかにするために、総端末数を変化させた場合のパケット到着率とリンク損失回数に着目した。また、表 4.1 にシミュレーションパラメータを示す。

4.3.1 総端末数とデータパケット到着率との関係

図 4.8 に総端末数に対するデータパケットの到着率を示す。ここで、到着率とはシミュレーション時間中に送信されるデータパケット数に対して送信先端末に到着したデータパケット数の割合である。結果より、総端末数が少ない場合の到着率は低く、AODV と提案手法による差も小さいことが確認できる。これは、シミュレーションエリアを固定した上で総端末数が少ない条件を検討しているため、端末の存在密度が極めて低い状態になっているためである。このような状況では代替経路の作成が困難だけでなく、主経路の構築も困難な状況が多々発生する。結果として、経路構築を完了できなかったため、到着率は非常に低くなる。

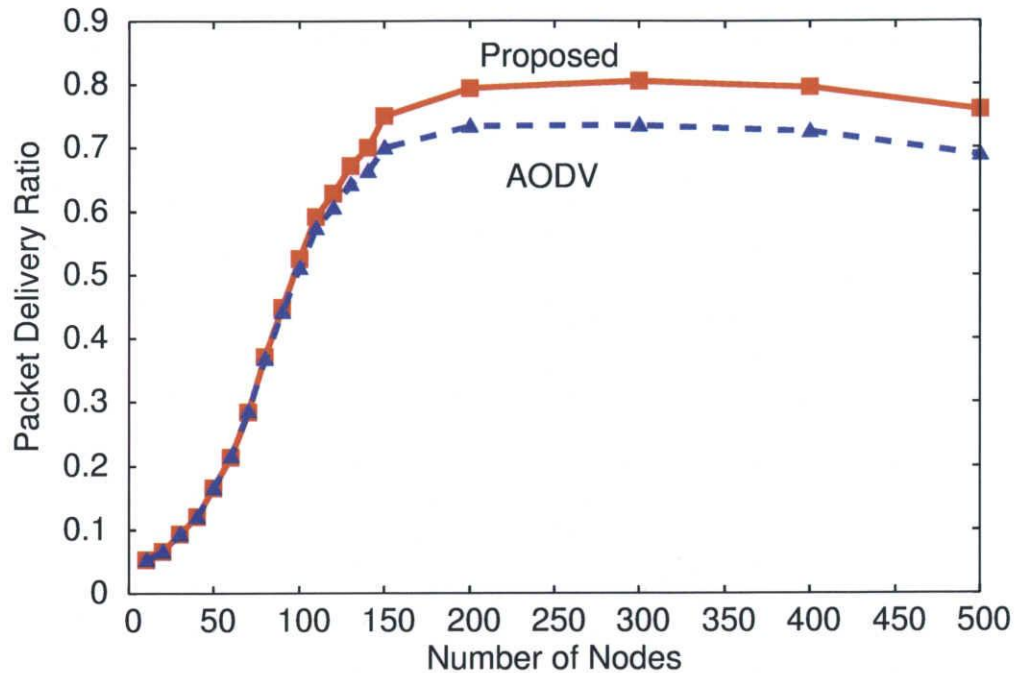


図 4.8 総端末数に対する平均データパケット到着率

一方、総端末数が 100 を越えた状態では AODV に比べて提案方式の到着率が 1 割ほど高くなっている。これは、総端末数が増加したことにより、主経路の構築だけではなく、代替経路の作成も可能になったためと思われる。なお、総端末数の増加に対して、AODV と提案方式の到着率の差が大きく変化しない。これは、シミュレーションで総端末数に対するトラヒックが常に一定となっているためである。その結果、さらされ端末問題が発生する頻度は総端末数には大きく依存していないためと思われる。

4.3.2 総端末数に対する 1 通信当たりのリンク損失数との関係

図 4.9 に総端末数に対する経路構築後に生じるリンク損失回数を示す。結果より、AODV 及び提案方式ともに、総端末数が少ない場合には、リンク損失が起こる頻度も少ないことが確認できる。これは、一部の端末間の経路しか確立できなかった結果、さらされ端末問題の影響を大きく受けなかったためと思われる。

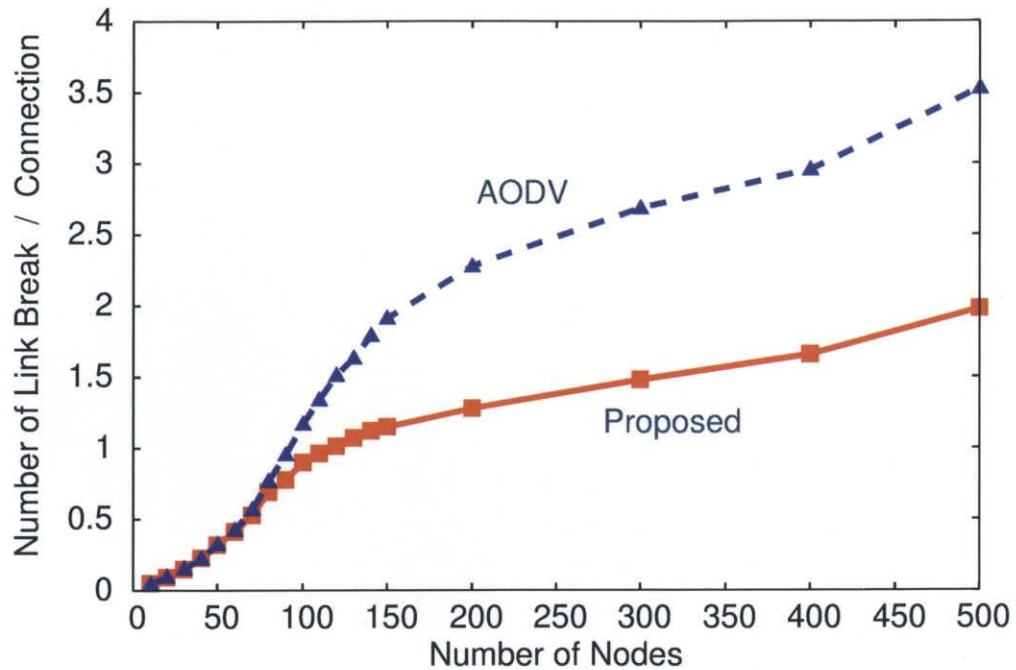


図 4.9 総端末数に対する 1 通信当たりのリンク損失数

一方、総端末数が 100 を超えた条件では、AODV のリンク損失回数は総端末数の増加に伴い大幅に増加していることが確認できる。総端末数が増加した場合、端末間の経路確立の多くが完了し、結果としてさらされ端末問題の発生頻度が高くなることが予測される。そして、さらされ端末問題が発生した場合には、経路上の中継端末の送信が抑制され、誤ったリンク損失の判定がなされたものと思われる。

さらに、提案方式の特性に着目すると、リンク損失回数は AODV の約半分に軽減されていることが確認できる。提案方式では、さらされ端末問題による一時的な通信抑制が発生した場合においても、代替経路となりうる端末が存在すれば、異なる経路を利用することで継続的な通信を実現可能である。結果として、誤ったリンク損失が検出されないだけでなく、継続的に通信が行われるため、AODV が誤って経路を削除することも防いでいると思われる。

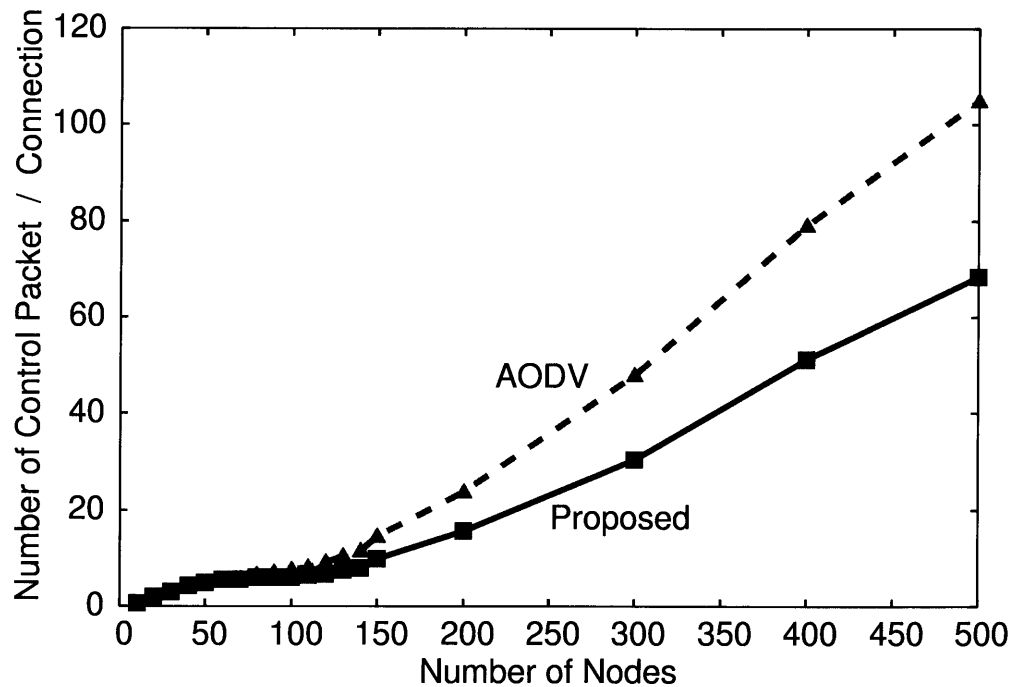


図 4.10 総端末数に対する 1 通信当たりの制御パケット数

4.3.3 総端末数に対する 1 通信当たりの制御パケット数との関係

図 4.10 に, 総端末数に対する 1 通信当たりの経路制御パケット数を示す. ここで, 経路制御パケットとは, 1 回の通信を行う際に各端末が送信した制御パケットの合計数を示す. 結果より, 総端末数が増加するに伴い, 制御パケット数は増加する傾向がある. これは, AODV の RREQ はフラッディングにより転送されるため, 総端末数が増加した場合, RREQ の送信数も大幅に増加するためと思われる. また, 提案方式の制御パケット数は AODV で必要とした制御パケット数より約 3 割少ないことが確認できる. これは, 提案方式では代替経路を利用することにより, 経路再構築の発生を抑えたためと思われる.

表 4.1 シミュレーションパラメータ

シミュレータ	Qualnet
シミュレーション時間	600[s]
シミュレータエリア	750[m] × 750[m]
ノード数	10～500
ノード配置	ランダム配置
移動度	なし
呼の発生	ポワソン分布 平均 0.2 個発生
データパケット長	512[byte]
通信時間	10[s]
送信間隔	50[ms]
無線アクセスプロトコル	IEEE802.11
受信モデル	SNR threshold BASED
伝送速度	2[Mbps]
通信半径	100[m]
無線伝播環境	自由伝播モデル
アプリケーション	CBR
ルーティングプロトコル	AODV
代替経路に切替	2 回目の再送時に切替
試行回数	100 回

第5章

結論

本論文では, アドホックネットワークの利用が想定される状況での経路制御に関する検討を行った. 特に, 経路を構築する時に生じる問題点と経路が完成した後に発生する問題点に着目した.

信号電力に基づく経路制御情報の削減手法では, 端末が多数存在する中で既存の経路制御手法を用いると制御パケットが多数発生し, 正常に通信を行うことが不可能な状況に対応した. 提案方式で, 経路構築時に受信した経路構築パケットの信号電力により, 異なるタイミングで再ブロードキャストの制御を行った. また, 再ブロードキャストを行う際に, 同一の経路構築パケットの送信を予定していた端末が受信した場合は予定していたブロードキャストの中止を行った. これにより, 経路構築時に発生する冗長なパケットの発生を回避した. 提案方式の有効性を評価するために, 計算機シミュレーションを行い, スループット特性の改善および冗長な経路構築パケットの発生を削減することが可能なことを示した. しかし, 有効な経路構築パケットだけの送信を識別するために, タイマを利用して送信タイミングを利用したため, 遅延が増加する結果となった. アドホックネットワークにおいて, 重要視しなければならない点は, 集中管理を行えないネットワークなため, 各端末が正常に通信を行える状況を作ることである. 既存の経路制御プロトコルで生じるブロードキャストストームに対応することで, 提案方式は正常な通信が行える状況を実現した.

局所代替経路を用いたアドホックルーティング手法では, 経路構築後のデータパケットの配送について, 従来から問題となっているさらされ端末問題がネットワー

クに与える影響を明らかにした. さらに端末問題が起こることで, 一時的に通信不可能な状態となり, 結果としてリンク損失を引き起こす. 提案方式では, 経路構築時にさらに端末問題が発生しても, すぐに対処できるように既存の経路制御プロトコルによって構築された経路の近隣に代替経路を構築する. 代替経路を利用することで, さらに端末問題が発生しても, リンク損失が起きることなく, 次の中継端末にパケットの送信を行った. 提案方式の有効性を評価するために計算機シミュレーションを行い, リンク損失の削減および経路再構築の削減を示した.

上記2つの提案手法では, 端末は移動していない状況で行ったため, 端末が多数存在する状況が経路制御プロトコルの影響を明らかにすることができた. しかし, アドホックネットワークを構築する端末は移動することが可能なため, 今後の課題としては, 多数の端末が存在し, 移動環境下での評価が必要である.

参考文献

- [1] E.M.Royer and C.-K.Toh, "A review of current routing protocols for ad hoc mobile wireless networks," IEEE Pers. Commun, vol.6, no.2, pp.46-55, April 1999.
- [2] 小牧省三, 松江英明, 間瀬 憲一, 守倉正博 "無線 LAN とユビキタスネットワーク 無線技術とその応用," 丸善, Feb 2004.
- [3] C. - K. Toh, "アドホックモバイルワイヤレスネットワーク—プロトコルとシステム," 共立出版, June 2003.
- [4] 総務省, "平成 18 年版 情報通信白書," 2006.
- [5] S.Corson and J.Macker, "Mobile ad hoc networking(MANET) : Routing protocol performance issues and evaluation considerations," IETF, RFC 2501, Jan 1999.
- [6] H.Y.Hsieh and R. Sivakumar, " Performance comparison of cellular and multi-hop wireless networks: A quantitative study," Proc. ACM SIGMETRICS, pp.113-122, Boston, MA, USA, June 2001.
- [7] S.Y.Ni,Y.C.Tseng,Y.S.Chen and J.P.Sheu, "The broadcast storm problem in a mobile ad hoc network," Proc.ACM / IEEE MOBICOM'99, pp.151-162, Seattle, WA, Aug 1999.
- [8] 小川 将克, 服部武, 加山英俊, 梅田成視, "アドホックネットワークにおける動的な移動端末の状態を用いた MAC プロトコル," 信学論 (B), Vol.J88-B No.3 pp643-655 2005
- [9] IEEE Computer Society LAN MAN Standards Committee, "Wireless LAN Medium

- Access Control(MAC)and Physical Layer (PHY) Specifications,” IEEE Standard 802.11 1997.
- [10] L.Kleinrock and F.A.Tobagi, “Packet Switching in Radio Channel :Part I - Carrier Sense Multiple - Access Models and their Throughput-Delay Characteristics,” IEEE Trans.Commun, Vol.COM-23, no.12, pp.1400-1416, Dec 1975. ”IEEE Trans. Commun. Vol.COM -23,No.12 ,pp1417-1433,1975.
 - [11] F.A.Tobagi, “Packet Switching in Radio Channel :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, pp1417-1433, 1975.
 - [12] V.Bharghavan et al, “MACAW : A Media Access Protocol for Wireless LANs,” Proc.ACM SIGCOMM’94, pp.215-225, Aug 1994.
 - [13] Jing Deng, Zygmunt J Hass, “Dual Busy Tone Multiple Access(DBTMA) : A New Medium Access Control for Packet Radio Networks,” IEEE ICUPC’98, Oct 1998.
 - [14] S.Xu and T. Saadawi, “Does the IEEE802.11 MAC protocol work well in multihop wireless ad hoc networks,” IEEE Commun.Mag, vol39, no.6, pp.130-137, June 2001.
 - [15] 橋口正哉, 平田明史, タユフェールエディ, 大平考, “アダプティブエスパアンテナを用いた無線アドホックネットワークの MAC に関する基礎検討,” IEEE Commun.Surveys Tutorials, vol.2, no.4, Fourth Quarter 1999.
 - [16] C.P.P.Bhagwat, “Highly Dynamic Destination-Sequenced Distance Vector Routing (DSDV) for Mobile Computers,” in Proceedings ofACM SIGCOMM’94, pp.234-244, September 1994.
 - [17] C.C.Chiang, H.-K.Wu.W.Liu and M.Gerla, “Routing in Clustered Multihop Mobile Wireless Networks with Fading Channel,” in proceedings of IEEE Singapore International Conference on Networks, 1997.
 - [18] T.Clausen and P.jacquet, “ Optimized Link State Routing Protocol,” IRFC3626, Oct 2003

- [19] A.Qayyum, et al., "Multipoint Relaying :A Efficient Technique for Flooding in Mobile Wireless Networks," 35th Annual Hawaii Int.Conf.on System Sciences(HICSS'2001) 2001.
- [20] C.-K.Toh, "Associativity - Based Routing for Ad-Hoc Mobile Ad Hoc Networks," in Proceedings of Communications, Vol.4, No.2, pp.103-139, 1997.
- [21] David B.Johnson and David A.Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," Internet Draft, draft-ietf-manet-dsr-09.txt, Apr, 2003.
- [22] C. Perkins, E. Royer, S.R. Das, " Ad Hoc On-demand Distance Vector (AODV) routing, Internet Draft, MANET Working Group, draft-ietf-manet-aodv-06.txt," July 2000.
- [23] Z.J.Haas ,et al., "The Zone Routing Protocol (ZRP)for Ad Hoc Networks," IETF Internet Draft, Jul 2002.
- [24] Josh Broch, David A.Maltz, David B. Johnson, Yih-Chun Hu, Joreta Jetcheva, " A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols," Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking October 25-30, 1998.
- [25] Shinji MOTEGI, Hiroki HORIUCHI, " AODV-Based Multipath Routing Protocols for Mobile Ad Hoc Networks," IEICE TRANS.COMMUN., Vol.E87-B, NO.9, SEPTEMBER 2004.
- [26] Ki-Hyung KIM, Hyun-Gon SEO, " The Effects of Local Repair Schemes in AODV-Based Ad Hoc Networks," IEICE TRANS.COMMUN ., Vol.E87-B, NO.9, SEPTEMBER 2004.
- [27] Network Simulator QualNet is <http://www.scalable-networks.com/>

謝 辞

本論文を進めるにあたり、小林英雄教授、森香津夫助教授、内藤克浩助手には適切な御助言を賜りならびに御指導をしていただき、感謝の意を表します。そして、貴重なお時間をさいて本修士論文の査読をしていただきました三重大学大学院工学研究科電気電子工専攻の篠木剛助教授に深く感謝いたします。最後に常に完璧な研究設備の環境を整えてくださった山本好弘技官、ならびに通信工学研究室の院生、学部生に深く感謝致します。

研究業績

- 渡邊貴則, 内藤克浩, 森香津夫, 小林英雄, “信号電力に基づく経路制御情報の削減手法に関する検討” 電気関係学会東海支部連合大会, O-235, 2005 年 9 月 15-16 日
- 渡邊貴則, 内藤克浩, 森香津夫, 小林英雄, “局所代替経路を用いたアドホックルーティングプロトコルに関する一検討” 電子情報通信学会 NS 研究会, Vol.106, No.167 p.49-52 , 19-21 July. 2006
- 渡邊貴則, 内藤克浩, 森香津夫, 小林英雄, “露出局問題に対応したアドホック経路制御手法に関する一検討” 電気関係学会東海支部連合大会, O-142, 2006 年 9 月 28-29 日
- Takanori Watanabe, Katsuhiro Naito, Kazuo Mori and Hideo Kobayashi , “Study of local alternative ad hoc routing protocol for the exposed terminal problem” IEEE ISPACS Dec. 2006