

# アドホックネットワークの packets 衝突を減少させる方式の検討

後藤秀暢

アドホックネットワークの隠れ端末問題を解決するために、IEEE802.11 では RTS/CTS 方式を採用している。しかし、RTS/CTS は一種の packets であり、これ自体の衝突が発生しやすいという課題がある。そこで、本稿では単一の周波数による制御信号(CS ; Control Signal)を用いてキャリアの状態を遠隔のノードに伝えることにより、RTS/CTS 方式の課題を解決する方法を提案する。

## Proposal of decreasing packet collision for Ad-hoc Networks

Hidenobu Goto

IEEE802.11 adopts a RTS/CTS method to solve " Hidden Terminal Problem " of the ad hoc network. However, RTS/CTS is a kind of packet, and there is the problem that the collision of RTS/CTS in itself is easy to occur. By this report, I suggest a method to solve the problem of the RTS/CTS method by introducing the state of the carrier into the remote node with a control signal by the single frequency.

### 1 章. はじめに

ユビキタス社会に向けて無線 LAN の技術が注目されている。無線 LAN の利点は配線工事が不要、ノードの移動や設置が簡単、迅速な LAN の構築が可能、屋外通信が可能、などが挙げられる。

無線 LAN のネットワーク形態にはアドホックモードとインフラストラクチャモードがある。アドホックモードは無線 LAN ノード同士が直接通信をする形態で、お互いの出す電波を受信できる近隣の範囲に設置して閉じたネットワークを構築する。アドホックモードのノードをマルチホップして遠隔のノードと通信できるようにしたネットワークはアドホックネットワークと呼ばれる。マルチホップ通信は、アクセスポイントがなくても、他のノードを中継しながら通信エリアを拡大できるというメリットを持つ。一方、インフラストラクチャモードはアクセスポイントを介して通信する形態で外部ネットワークとの接続が可能である。

これら無線 LAN には本質的に避けられない問題として「隠れ端末問題」がある。「隠れ端末問題」とは、2 つのノードが互いに電波の到達範囲外にいるとお互いにキャリアを検出できずに packets を送信し、衝突を引き起こす問題である。IEEE802.11 では RTS (request to send) /CTS (clear to send) による送信予約によりこの課題を解決している。

しかし、RTS/CTS 方式では課題が完全には解決されていない。その理由として、RTS/CTS が一種の packets であり、それ自体の衝突が発生しやすい。このことに起因してデータの衝突が発生したり、無駄に送信を待たされる状況が発生する可能性がある。この問題はアドホックネットワークにおいて特にスループットを低下させる要因となっている。

そこで、本稿では単一の周波数からなる CS(Control Signal)と呼ぶ制御信号を用いて RTS/CTS のキャリアの状況を遠隔のノードまで伝えることにより、RTS/CTS の衝突を回避する方法を提案する。

以下，2章では RTS/CTS の課題を明確にし，3章では提案方式について説明を行う．4章では ns-2(Network Simulator 2)改造方法の検討結果を述べる．最後に5章でまとめを行う．

## 2章. 既存技術とその課題

### 2.1 RTS/CTS 方式

隠れ端末問題を解決するには，送信ノードと受信ノードに隣接する全てのノードにチャンネルが使用中であることを知らせる必要がある．RTS/CTS方式の動作を図1に示す．ノードAはデータフレーム送信前にDIFS(Distributed Coordination Function Interframe Space)とバックオフ時間を加えた時間だけキャリアがないことを検出すると送信を予約するためRTSをノードB宛に送信する．ノードBはSIFS(Short Interframe Space)時間後にノードA宛に予約を許可するCTSを返信する．ノードBが送信したCTSは遠隔にあるノードCも受信することができる．RTSには無線を使用する予定期間が記載されており，これがCTSに転記されてノードCに届く，周辺ノードはRTS/CTSを監視しており，これらを検出すると一連のシーケンスが終了するまでの所定の期間だけ送信を禁止する．この期間のことをNAV(Network Allocation Vector)と呼ぶ．このようにノードCに仮想的なキャリア・センス状態を作ることにより送信が禁止され，衝突を回避することができる．CTSを受信したノードAはSIFS時間後にデータフレームを送信する．データフレーム受信完了後，ノードBはSIFS時間後にACKフレームを返信して通信を終了する．

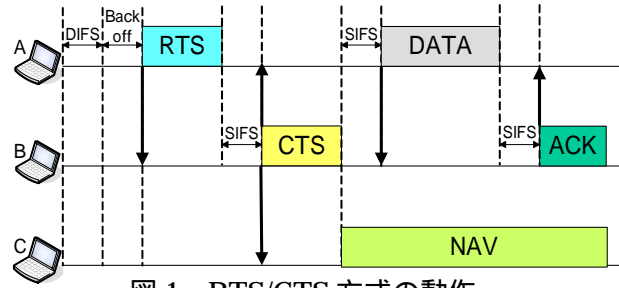


図1 RTS/CTS方式の動作

### 2.2 RTS/CTS方式の課題

RTS/CTS方式の課題の例を図2，および図3に示す．図2はノードAとノードBがRTS/CTSのやりとりをしている間に3ホップ先にあるノードDがRTSを送信した状態を示している．ノードDのRTSとノードBのCTSがノードCの地点で衝突する．ノードDはノードCがCTSを応答しないためRTSを再送信する．一方，ノードAはノードBからのCTSを受信するので，ノードCで衝突が発生していることに気がつかずにノードBに対してデータ送信を始める．ノードCはノードDからのRTSに回答してCTSを送信するため，ノードAのデータと衝突が発生する．

図3はノードAがノードBにRTSを送信したときにノードCがRTSを送信した状態を示す．ノードBではRTS同士の衝突が発生し，正しく受信できない．ノードAとノードCはCTSの返信が来ないのでRTSの再送処理に入る．図3ではノードAが先にRTSの再送時間となったため，RTS/CTSのやり取りが行われ，更にデータフレームの送信が成功している．ノードDはノードCのRTSを受信し，RTSに記載されているNAV期間だけ送信を禁止する．しかし，ノードCが送信したRTSはすでに破壊されているので，ノードDは無駄な時間待機することになる．

これらの課題はRTS/CTSがパケットの交換であるためにある程度の時間を必要とし，衝突が発生しやすいことに起因している．

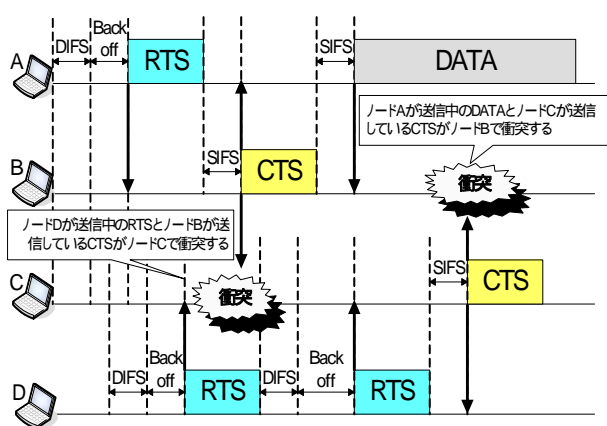


図2 RTS/CTS方式の課題(1)

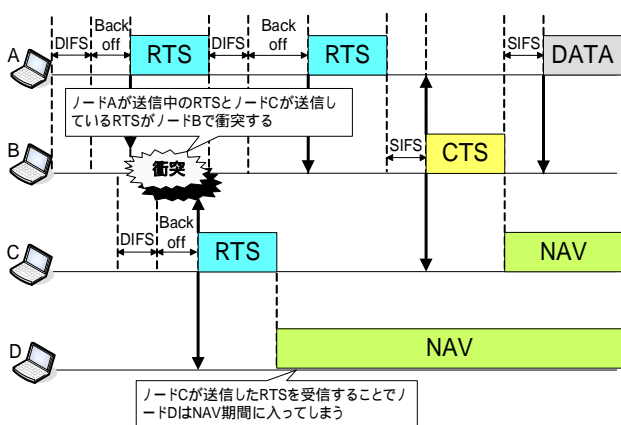


図3 RTS/CTS方式の課題(2)

### 3章. 提案方式

RTS/CTS方式の課題を解決するために、本稿では RTS 又は CTS を送信するノードが、あらかじめ決められた特定の周波数( $S_1, S_2, S_3$ )を持つ制御信号 CS を発生させる。CS は RTS 又は CTS の送信中のみ発生させる。周囲のノードは CS 受信中には送信ができないものとする。CS は RTS の場合は 2 ホップ、CTS の場合は 1 ホップ先まで送る必要がある。なぜなら、図 2, 3 で示したように送信端末から 3 ホップ先にある端末の影響でデータの衝突が発生するためである。RTS や CTS は制御フレームであるため受信してからフレーム内容の処理を実行するための処理時間を必要とする。一方 CS はデータを持たない信号であるため処理時間を必要としない。

即ち、あるノードが RTS 又は CTS を送信開始した瞬間から CS はノード間を中継し、周囲のノードの送信を制御する。RTS 送信時の CS の動作を図 4 に、CTS 送信時の CS の動作を図 5 に示す。

RTS 送信の際、ノード A が RTS を送信すると同時に周波数  $S_1$  の CS を発生させる。ノード B は周波数  $S_1$  の CS を受けたので即座に周波数  $S_2$  の CS を発生させる。周波数  $S_2$  の CS を受けたノード C はさらに周波数  $S_3$  の CS を発生させる。周波数  $S_3$  の CS を受けたノード D はこれ以上 CS を中継させない。

CTS 送信の際、ノード B は CTS を送信すると同時に周波数  $S_2$  の CS を発生させる。ノード C は周波数  $S_2$  の CS を受けたので周波数  $S_3$  の CS を発生させる。ノード D はこれ以上 CS を中継させない。図 6, 7 に RTS, CTS 送信の際に CS による送信抑制効果の影響が 3 ホップ先のノードに表れる様子を示す。

このように、提案方式では RTS/CTS の送信状況を、CS を用いて遠方のノードにいち早く伝えることができるため、RTS/CTS 自体の衝突の可能性を大幅に軽減させることができる。

CS を導入した場合の動作を図 8 に示す。まず、ノード A からノード B に RTS を送信すると同時に周波数  $S_1$  を発生させる。これにより、ノード A の通信可能範囲にあるノード B は周波数  $S_1$  を受信する。ノード B は周波数  $S_1$  受信と同時に周波数  $S_2$  を送信する。同様にしてノード C は周波数  $S_2$  受信と同時に周波数  $S_3$  を送信する。このようにして、CS がノード D まで中継される。これによりノード A が RTS を送信している間はノード B, C, D はフレーム送信ができなくなる。次に、ノード B がノード A に CTS を送信する。このときも CTS と同時に CS を発生させる。RTS の場合と同様にして、CS がノード A, C, D に中継され、ノード A, C, D はフレーム送信ができなくなる。

ノード C はノード B からの CTS を検出するとその内容により NAV 期間に入る．以後の動作は RTS/CTS で規定された内容に従う．ノード D が RTS をノード C に送信しても RTS は破棄され，ノード D は RTS の再送を試みる．

このように CS を取り入れることにより RTS/CTS 方式に残されていた課題を解決できる．

#### 4 章. ns 2 の改造の検討

ns-2 は多くの研究機関で利用されているフリーのネットワークシミュレータである．

ns-2 のネットワークモデルと TCP/IP モデルの対応を図 9 に示す．ns-2 はノード・リンク層，エージェント層，アプリケーション層の 3 層構造からなる．アプリケーション層では，FTP，CBR(constant bit rate)，Telenet，HTTP などのフロータイプを定義している．

CS の機能を ns-2 に追加するために，エージェント層，ノード・リンク層の改造を行う．ns-2 の改造内容を図 10 に示す．

CS の機能を持つ CS モジュールをノード内に追加する．CS モジュールには CS の中継機能や CS の有効範囲，発生期間などの情報を持たせる．3 つの NIC(Network Interface Card)を追加し CS の発生，検出を行う．シミュレーション上では 1 つの周波数ごとに 1 つ NIC を割り当てる．実機に CS を導入する場合は，CS の発生検出用の特殊な装置を用意するため，NIC を 3 つ追加する必要はない．ns-2 では RTS，CTS やデータフレームなどは MAC モジュールで作られるので，NIC-1 の MAC モジュールと NIC-S<sub>1</sub>，S<sub>2</sub>，S<sub>3</sub>の CS モジュールを結ぶ．そうすることで，RTS を送信する前に NIC-S<sub>1</sub>の CS モジュールが呼び出され，CS(S<sub>1</sub>)を発生させる．CTS を送信する場合は NIC-S<sub>2</sub>の CS モジュールが呼び出され，CS(S<sub>2</sub>)を発生させる．

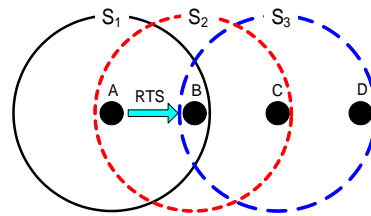


図 4 RTS 送信時の CS の動作

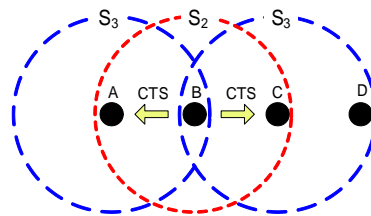


図 5 CTS 送信時の CS の動作

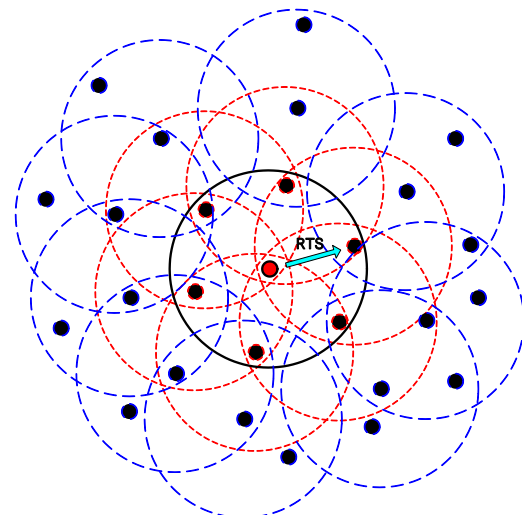


図 6 RTS 送信時の CS の広がる様子

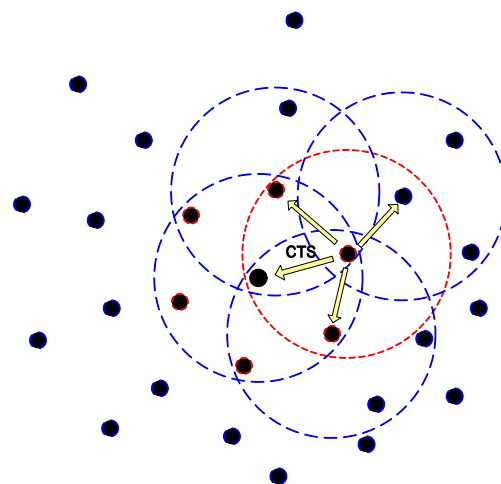


図 7 CTS 送信時の CS の広がる様子

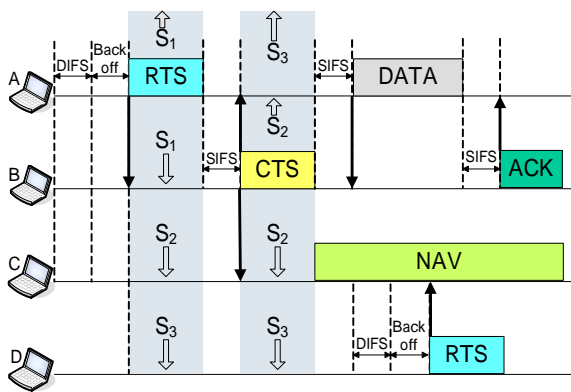


図 8 CSを導入した場合の動作

CS モジュールと繋がる NIC- $S_1, S_2, S_3$  内部のインタフェースキュー (IFq : Interface queue) と MAC モジュールには変更すべき点がある。インタフェースキューは、届いたパケットの中から目的地のアドレスが判明しているパケットを順次キューから出すというフィルターをサポートしている。CS モジュールから発生するフレームの処理を優先させることにより、インタフェースキューによるキュー待ちを発生しないようにする。実際のネットワーク環境では RTS, CTS を受信するまでに遅延が生じる。しかし、シミュレーション上では遅延は生じない。そこで、ns-2 ではイベントスケジューラでパケットの処理遅延を擬似的にシミュレートしている。その処理遅延は MAC モジュールで処理されている。3章で述べたように、CS はデータを持たない信号なので処理時間を必要としない。つまり、CS モジュールと繋がっている NIC- $S_1, S_2, S_3$  内部の MAC モジュールの遅延時間を変更し、CS を瞬時に各ノードに中継する。

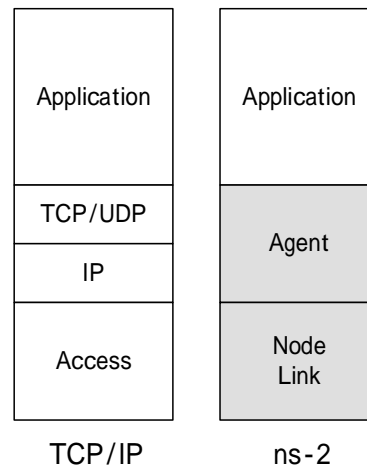
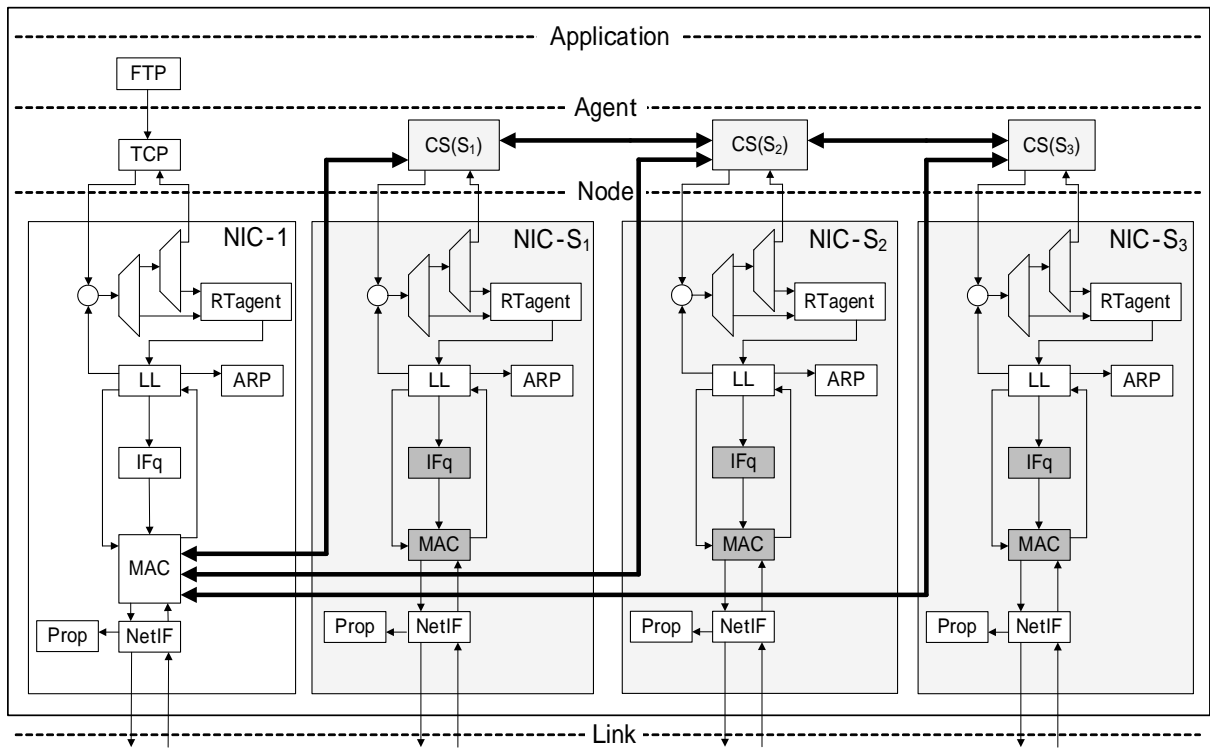


図 9 ns-2 のネットワークモデルと TCP/IP モデルの比較

## 5 章. むすび

RTS/CTS 方式の課題を解決するために、制御信号 CS を用いて他のノードからの送信を抑制する方法を提案した。それによりフレーム同士の衝突によるデータ破壊を未然に防ぐことが可能となる。更に、CS の機能を ns-2 に導入するための検討を行った。今後は、ns-2 の改造を行い、提案方式をシミュレーションにて評価する。



追加部分

変更部分

図 10 ns-2 の改造内容

## 参考文献

- [1] 守倉正博, 久保田周治, "802.11 高速 LAN 教科書", 2006
- [2] C-K.Toh, "アドホックモバイルワイヤレスネットワーク", 2003
- [3] 大水祐一, "802.11 セキュア無線 LAN 設計ガイドブック", 2004
- [4] 銭飛, "NS2 によるネットワークシミュレーション", 2006
- [5] YAGYU Kengo, FUJIWARA Atsushi, TAKEDA Shinji, OMAE Koji, AOKI Hidenori, MATSUMOTO Yoichi, "Topology and Traffic Aware Channel Assignment for Layer-2 Mesh Networks", 電子情報通信学会技術研究報告. RCS, 無線通信システム Technical report of IEICE. RCS Vol.105, No.196 ( 20050714 ) pp. 127-132 RCS2005 - 61
- [6] Ashish Raniwala, Kartik Gopalan, Tzi-cker Chiueh, " Centralized Channel Assignment and Routing Algorithms for Multi-Channel Wireless Mesh Networks", ACM SIGMOBILE Mobile Computing and Communications Review, 2004
- [7] Jenhui Chen, Yen-Da Chen, " AMNP: Ad Hoc Multichannel Negotiation Protocol for Multihop Mobile Wireless Networks", IEEE international conference on communications, 2004
- [8] 野崎正典, " IEEE802.11s における無線メッシュネットワークの標準化動向", 沖電気工業株式会社, 2006
- [9] Nitin Jain, Samir R.Das, Asis Nasipuri "A Multichannel CSMA MAC Protocol with Receiver-Based Channel Selection for MultihopWireless Networks", IC3N2001

## 付録

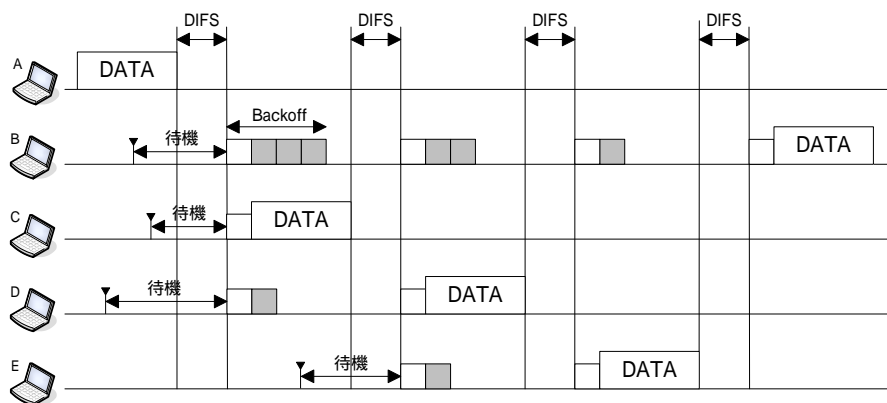


図 11 CSMA/CA 方式の概要

### CSMA/CA 方式

CSMA/CA 方式の原理について説明する。まず、ノード A がデータを送信する。その間にノード B, C, D が待機している。無線ではキャリアがなくなったとたんに送信するのではなく DIFS(Distributed Coordination Function Interframe Space)とバックオフ時間をとってからデータを送信する。DIFS とはキャリア・センスを行う際に、ビジー状態のチャンネルから未使用状態に変化したと判断されるまでに必要なチャンネルの連続未使用期間である。待ち時間はランダムな数値で設定され、単位時間ごとにキャリア・センスを行い、誰も送信していなければ待ち時間を 1 減らし 0 になったら送信する。もし、バックオフ中にほかの端末が送信したときは、バックオフ時間が次の送信時に持ち越される。図 11 ではノード B が待ち 4、ノード C が待ち 1、ノード D が待ち 2 となっている。つまり、ノード A の送信が終わり、次に待ち時間が 0 となったノード C が送信し、その次にノード D が送信する。ノード E は途中から加わっているがノード B よりも待ち時間が短いのでノード E が優先的にデータを送信できる。そして、最後にノード B がデータを送信して完了となる。CSMA/CA は衝突を検知できないので、このようなしくみで衝突を回避する。

### 隠れ端末問題

前章で述べたように CSMA/CA 方式を採用するアドホックネットワークにおいて気をつけなければならないのが「隠れ端末問題」である。「隠れ端末問題」とは、2 つのノードが互いに隠れた位置におり(電波の到達範囲外)、両者が同じ受信ノードに情報を送信しようとする、受信ノードにおいてデータの衝突を引き起こす問題である。隠れ端末が存在する無線通信を図 12 に、隠れ端末のデータの衝突を図 13 に示す。

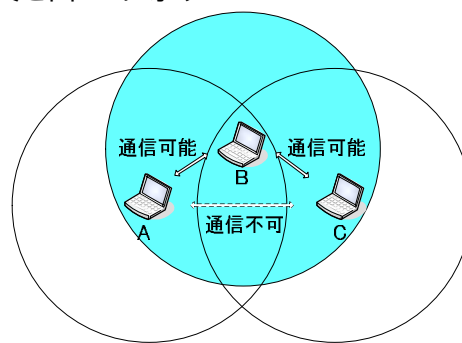


図 12 隠れ端末が存在する無線通信

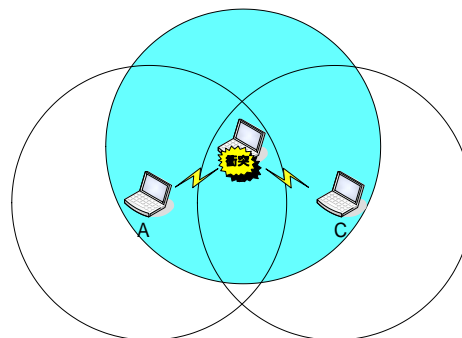


図 13 隠れ端末のデータの衝突