

無線信号の意図的な衝突による盗聴困難な無線マルチホップ 配送手法とその性能評価

嶋田 勇^{1,a)} 梶垣 博章^{1,b)}

概要：無線マルチホップ通信では、データメッセージが送信元無線ノードから送信先無線ノードまで中継無線ノードの列として構成される無線マルチホップ配送経路に沿って運ばれる。各中継無線ノードによってデータメッセージは、ブロードキャストを基礎とする無指向性無線通信を用いて転送されるため、すべての隣接無線ノードが傍受可能である。そこで、ノイズ無線信号との衝突を利用した盗聴困難な無線通信手法が提案されているが、指向性アンテナや複雑な信号処理を要するなど、安価で多数の無線ノードから構成されることを前提とした無線マルチホップネットワークには不向きなものとなっている。本論文では、中継無線ノードの1ホップおよび2ホップ隣接無線ノードの一部がデータメッセージ転送時にノイズ無線信号を送信することでノイズ無線信号を意図的にデータメッセージと衝突させ、盗聴者によるデータメッセージの取得を困難にする手法を提案する。また、ノイズ無線信号を送信する無線ノードの選択を行なうように拡張したルーティングプロトコルを設計する。さらに、提案手法による盗聴防止効果を1ホップの無線アドホック通信と無線マルチホップ配送について、ノイズ無線信号によるデータメッセージの到達領域に対する被覆率によって評価するシミュレーション実験結果により示す。

キーワード：無線マルチホップ通信, 盗聴回避, ノイズ無線信号, 衝突, ルーティングプロトコル

1. はじめに

無線アドホックネットワーク、無線センサネットワークなどでは、データメッセージが送信元無線ノードから送信先無線ノードまで無線マルチホップ配送される。無線マルチホップ配送経路は、中継無線ノードの列として構成され、各中継無線ノードは、その前ホップ中継無線ノードから転送されたデータメッセージをその次ホップ中継無線ノードへと転送する。ここで、各中継無線ノードがデータメッセージを転送する際には、無指向性アンテナを用いてデータメッセージを含む無線信号をブロードキャスト送信することから、無線信号到達範囲に含まれるすべての無線ノードがこのデータメッセージを傍受することが可能である。つまり、無線マルチホップ配送経路のいずれかの中継無線ノードの無線信号到達範囲に存在する盗聴無線ノードは、データメッセージを容易に傍受することができる。

これらのデータメッセージは暗号化されて配送されるのが一般的である。そのため盗聴無線ノードが暗号化されたデータメッセージを傍受しても復号には復号鍵が必要であ

り、平文のデータメッセージを入手することは必ずしも可能ではない。しかし、高性能で安価なコンピュータの普及により、多数のデータメッセージを傍受、収集することによる盗聴の可能性が指摘されている[1]。このため、無線マルチホップネットワークが社会基盤として機能する将来においては、暗号化されたデータメッセージの傍受をもより困難にすることが必要とされる。また、センサデバイスの取得するセンサデータを集約、活用するセンサネットワークでは、各センサノードに暗号化機構を導入することは、ネットワーク構築コストの拡大、配送遅延の延長等の問題をもなうことから、平文あるいは簡易な暗号方式によって暗号化されたセンサデータメッセージであってもより安全に配送する手法の導入が求められる。

このような要求に対して、次章で述べるように、各中継無線ノードに指向性アンテナを導入してビームフォーミングする手法や複雑な計算を要する信号処理を行なう手法が提案されている。しかし、多数の小型で安価な中継無線ノードから構成される無線マルチホップネットワークでの適用は困難である。そこで、本論文では、各中継無線ノードは無指向性アンテナのみを備え、無線通信はディスクモデルに従うことを前提とし、中継無線ノードの近隣無線ノードが協調してノイズ無線信号を送信することによって盗聴無線

¹ 東京電機大学
Tokyo Denki University, Adachi, Tokyo 120-8551, Japan
a) shimada@higlab.net
b) hig@higlab.net

ノードによるデータメッセージの傍受を困難にする手法を提案する。また、そのためのルーティングプロトコル、データメッセージ転送プロトコルを設計する。

2. 関連研究

無線マルチホップ通信におけるセキュリティに関連して様々な問題が議論され、その解決手法が提案されてきている。無線マルチホップ通信に固有の問題には、セルフフィッシュノード問題やブラックホール攻撃問題等がある。一方、いわゆる盗聴の問題は、有線ネットワーク、無線ネットワークを問わず、その対策が必要とされる問題であるが、特に無線ネットワークにおいてはその通信基盤がブロードキャスト送信される無線信号であることから、よりの確な対策が求められている。ここでの主要な技術は暗号通信であり、モバイル端末の特性から、比較的低い計算コストで受容可能な安全性を提供可能な暗号通信技術が検討されている。しかし、暗号通信技術は、無線ネットワークを配送される暗号化データメッセージを盗聴無線ノードに取得された後に平文データメッセージを取得させない技術である。この点に注目すると、無線ネットワークを配送されるデータメッセージをそもそも盗聴無線ノードに取得されることを困難あるいは不可能にする手法の検討は不可欠である。これらの手法を組み合わせることで、より強力なセキュリティを実現することが期待できる。特に、暗号化と復号に要する計算コストを負担できない膨大な数の無線ノードから構成されるセンサネットワークあるいはIoT(Internet of Things)の実現においては、暗号通信技術にのみ依存しない手法の考案が求められる。

このような手法のひとつに、意図的に送信されたノイズ無線信号とデータメッセージとの衝突によって盗聴無線ノードがデータメッセージを取得することを困難にする手法がある。論文 [2] では、送信無線ノード N_s から受信無線ノード N_r へのデータメッセージ転送において、送信無線ノードが指向性アンテナを備えることによってビームフォーミングを実現することを前提として、 N_r の近隣に位置する盗聴無線ノードがデータメッセージを傍受することを困難にする手法を提案している。ここでは、図 1 に示すように、 N_s からのデータメッセージ送信と並行して N_r がノイズ無線信号をブロードキャスト送信することによって、近隣無線ノードではデータメッセージとノイズ無線信号の衝突によってデータメッセージそのものを受信することが不可能となる。ここで、衝突した信号を受信する無線ノードのひとつである N_f が衝突メッセージを N_r へと転送する。この衝突メッセージを受信した N_r は、ノイズ無線信号は自身が送信したものであることから、信号処理により転送された衝突メッセージからノイズ無線信号を除去することで、データメッセージを取得することが可能である。この方法は、衝突メッセージを転送する N_f を含め、 N_r 以

外のいずれの無線ノードもデータメッセージを取得できない点で優れている。しかし、 N_s に指向性アンテナが備えられていることを前提としている点、 N_r に信号処理を行なうために十分な計算資源が備えられていることを前提としている点が問題である。すなわち、特定の無線ノード間の通信として適用するには有効な手法ではあるものの、必ずしも十分な計算資源を備えることができず、指向性アンテナという特殊な通信デバイスを備えることが容易ではない膨大な数の無線ノードから構成される無線センサネットワーク等においては、適用が困難であると結論せざるを得ない。

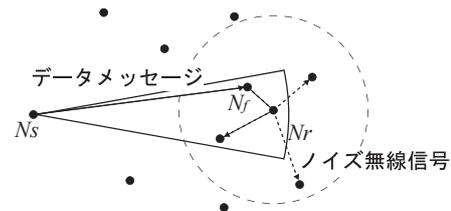


図 1 ノイズ無線とデータメッセージとの衝突および衝突信号の転送による盗聴回避手法

一方、論文 [5] においても、送信無線ノードが指向性アンテナを用いてビームフォーミングを行ない、受信無線ノードのみがデータメッセージを含む無線信号をより強力に受信することを可能にする手法が提案されている。ここでは、その受信レートの差異を拡大するために、他のすべての無線ノードがノイズ無線信号を送信する。盗聴無線ノードの受信レートをノイズ無線信号の送信によって受信無線ノードの受信レートに対して著しく低下させるという手法であるが、論文 [2] と同様に送信無線ノードに特別なハードウェアを備えることを前提としている点、すべての無線ノードにノイズ無線信号の送信を求めていることから電力消費量が著しく増加する点が問題である。

3. 提案手法

本章では、前章で述べた無線マルチホップ通信において盗聴を困難にする手法の問題点、すなわち、無線マルチホップ配送経路の各中継無線ノードから次ホップ中継無線ノードへのデータメッセージの転送がブロードキャストによって行なわれるために、盗聴無線ノードを含むすべての隣接無線ノードによって傍受可能であるという問題点を解決する新しい手法を提案する。ここでは、ビームフォーミングを実現する指向性アンテナなどの特別なハードウェアが各中継無線ノードに備えられていることを前提としない。また、受信無線信号からノイズ無線信号を除去するような特別な信号処理機構を各中継無線ノードが備えていることも前提としない*1。すなわち、各中継無線ノードは無指向性ア

*1 これらを備えることを前提とした手法や暗号通信方式と本論文で提案する手法とを組み合わせることによって、より有効に盗聴を困難にすることは可能である。組み合わせ手法については、今後の検討課題とする。

ンテナのみを備え、隣接無線ノードへの通信はディスクモデル [4] に従うものとする。

3.1 アドホック通信のためのノイズ無線信号送信

本節では、無線マルチホップ通信における盗聴を困難にする手法の検討に先立ち、隣接無線ノード間の無線アドホック通信を対象とした検討を行なう。送信無線ノード N_s から受信無線ノード N_r への無線アドホック通信では、 N_r は N_s の無線信号到達範囲に含まれている。ここで、 N_s から N_r へ送信されるデータメッセージ m は、 N_s の無線信号到達範囲内にブロードキャスト送信されることから、この無線信号到達範囲に含まれるすべての隣接無線ノード N が m を受信することができる。すなわち、いずれかの隣接無線ノード N が盗聴無線ノードであるならば、 N は m を受信することができる。 N による m の受信を困難にするために、前章の関連研究と同様にノイズ無線信号を送信する手法を適用する。ただし、ノイズ無線信号を送信することで盗聴を困難とすることができるのは、図 2 に示すように N_r 以外の N_s の隣接無線ノードにノイズ無線信号を到達させることができる無線ノードである。

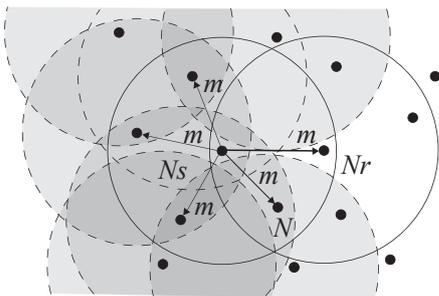


図 2 隣接無線ノードによるノイズ無線信号送信

本節では、無線アドホック通信におけるデータメッセージ m の盗聴を困難にするために、以下の条件を満足する無線ノード N_j がノイズ無線信号を送信することとする (図 3)。

[ノイズ無線信号送信無線ノード N_j]

- (1) N_j は N_s の隣接無線ノードである。
- (2) N_j は N_r の隣接無線ノードではない。

条件 1 は、 N_j から送信されるノイズ無線信号の到達範囲と m の到達範囲とが重複するための十分条件のひとつである。この範囲の重複が発生しない無線ノードがノイズ無線信号を送信しても、盗聴無線ノードによる m の受信を妨げることはできない。また、後述するように、無線 LAN プロトコルの備える RTS/CTS 制御を用いて追加の制御メッセージを導入することなく協調的なノイズ無線信号送信を実現可能とする条件となっている。一方、条件 2 は、 N によって送信されるノイズ無線信号が N_r に到達しないための必要条件である。 N_r は N_s から送信される m を受信す

ることが必要であることから、いかなるノイズ無線信号も N_r に到達してはならない。そこで、 N_r の隣接無線ノードはノイズ無線信号を送信しないこととする。

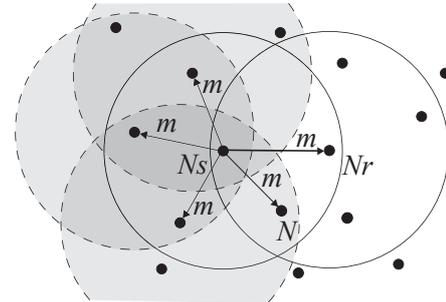


図 3 アドホック通信のためのノイズ無線信号送信

上記のふたつの条件を満足する無線ノードは、無線 LAN プロトコルの備える RTS/CTS 制御における制御メッセージの交換において特定することが可能である。条件 1 を満足する無線ノードは N_s が送信する RTS 制御メッセージを受信し、条件 2 を満足する無線ノードは N_r が送信する CTS 制御メッセージを受信しない。CTS 制御メッセージは N_r による RTS 制御メッセージ受信後 SIFS 待機時間を経て送信されることから、RTS 制御メッセージを受信したが CTS 制御メッセージを受信しない無線ノード N_j がノイズ無線信号を送信すればよい。また、これらの制御メッセージには NAV 情報が格納されていることから、 N_j によるノイズ無線信号の送信タイミングも特定することが可能である。すなわち、 N_j は、 N_s から N_r へとデータメッセージが送信される時間にノイズ無線信号を送信するが、 N_r から N_s へと受信確認メッセージが送信される時にはノイズ無線信号の送信を停止しなければならない。これは、 N_j の無線信号到達範囲に N_s が必ず含まれることから、 N_j が送信するノイズ無線信号と N_r が送信する受信確認メッセージとの N_s における衝突を回避するために必要である。

3.2 無線マルチホップ通信のためのノイズ無線信号送信

前節で述べた無線アドホック通信のためのノイズ無線信号送信手法は、RTS/CTS 制御メッセージの交換のみを用いてノイズ無線信号を送信する無線ノードを決定し、ノイズ無線信号の送信時間を特定することができる。しかし、ノイズ無線信号送信無線ノードの条件を満足する無線ノードの存在確率、および、それともなうノイズ無線信号到達範囲によるデータメッセージ到達範囲の被覆率は、無線ノードの分布密度に加えて送信無線ノード N_s と受信無線ノード N_r との間の距離 $|N_s N_r|$ に依存する。図 4 に示すように N_s と N_r が離れている場合には、ノイズ無線信号送信無線ノードの条件を満足する無線ノードの存在する領域の面積が大きいため、ノイズ無線信号到達範囲によるデータメッセージ到達範囲の被覆率が高いことが期待される。一方、図

5に示すように N_s と N_r が近接している場合には、ノイズ無線信号送信無線ノードの条件を満足する無線ノードの存在する領域の面積が小さいため、ノイズ無線信号到達範囲によるデータメッセージ到達範囲の被覆率が低いことが考えられる。このため、盗聴無線ノードがノイズ無線信号に妨害されることなく、 N_s から N_r へ送信されるデータメッセージ m を傍受することができる可能性が高くなる。

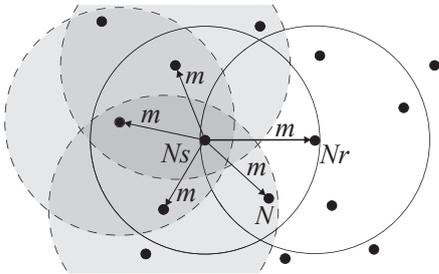


図 4 送受信無線ノード間距離が大きい場合による盗聴妨害

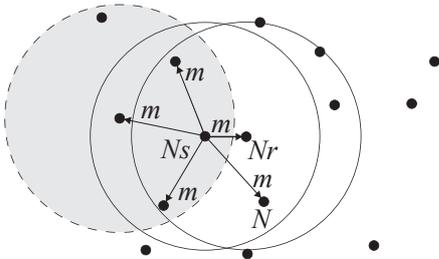


図 5 送受信無線ノード間距離が小さい場合による盗聴妨害

この問題を解決するためには、 N_s の無線信号到達範囲でありながらノイズ無線信号が到達しない領域を縮小することが求められる。前節で述べた手法では、 N_s と N_r の無線信号到達範囲に共通に含まれる領域にある無線ノードはノイズ無線信号を送信できないことから、この領域に含まれない無線ノードが送信するノイズ無線信号によって、できるだけノイズ無線信号到達範囲によって N_s の無線信号到達範囲を被覆し、盗聴無線ノードによる m の受信を妨害することが有効な手法となる。このためには、 N_s と N_r のいずれの無線信号到達範囲にも含まれない無線ノードのうち、 N_s の無線信号到達範囲を無線信号到達範囲に含むものを選択する必要がある。そこで、 N_s の2ホップ隣接無線ノードによるノイズ無線信号送信を導入する。ただし、ノイズ無線信号を送信する無線ノードの選択を前節で述べた無線アドホック通信のためのノイズ無線信号送信手法のように、通信要求発生時に行なうことは困難である。なぜなら、ノイズ無線信号を送信する N_s の2ホップ隣接無線ノードは、 N_s と N_r のいずれの無線信号到達範囲にも含まれないことから、RTS/CTS 制御のための RTS 制御メッセージ、CTS 制御メッセージのいずれも受信しないため、追加の制御メッセージ交換が必要となる。また、 N_s における衝突が

発生するためにこの追加制御メッセージを CTS 制御メッセージと並行して送信することができないことから、データメッセージの配送遅延を延長することとなる。一方、無線マルチホップ配送においては、送信元無線ノード $N^s = N_0$ から送信先無線ノード $N^d = N_n$ までの無線マルチホップ配送経路 $\|N_0 \dots N_n\|$ をデータメッセージ群の配送に先立って探索、検出し、この経路に沿って複数のデータメッセージを順次配送する。そこで、ルーティングプロトコルによる経路探索、経路検出の際に、各中継無線ノード N_i によるデータメッセージ転送に対応するノイズ無線信号送信無線ノードを選択することとする。

前節で述べた無線アドホック通信のためのノイズ無線信号送信手法において、ノイズ無線信号送信無線ノードとなった無線ノードは、本節で提案する無線マルチホップ通信のためのノイズ無線信号送信手法においてもノイズ無線信号送信無線ノードとなる。すなわち、中継無線ノード N_i からその次ホップ中継無線ノード N_{i+1} へのデータメッセージ転送において、 N_i の隣接無線ノードであって N_{i+1} の隣接無線ノードではない無線ノード、すなわち、 N_i の無線信号到達範囲内であって N_{i+1} の無線信号到達範囲外にある無線ノードは、 N_i の無線信号到達範囲に含まれる盗聴無線ノードが転送されるデータメッセージを傍受することを妨げるために、ノイズ無線信号を送信する。

これに加えて、 N_i の無線信号到達範囲には含まれないが、その無線信号到達範囲が N_i の無線信号到達範囲と一部重複する無線ノードから送信されるノイズ無線信号は盗聴無線ノードによる転送データメッセージの傍受を妨害することができる。この無線ノードは N_i の2ホップ隣接無線ノードであることが必要条件となる。ただし、 N_i の2ホップ隣接無線ノードであっても、その無線信号到達範囲が N_{i+1} の無線信号到達範囲と一部重複しないのであれば、盗聴無線ノードによるデータメッセージの傍受を妨害する意味での貢献は小さい。その一方で N_{i+1} の無線信号到達範囲に含まれる無線ノードは、 N_{i+1} による転送データメッセージの受信を妨げてはならないためにノイズ無線信号を送信することはできないことから、 N_{i+1} の2ホップ隣接無線ノードがノイズ無線信号送信無線ノードの候補となる。

以上により、中継無線ノード N_i から N_{i+1} へのデータメッセージ転送において、盗聴無線ノードによるデータメッセージ傍受を困難にするためのノイズ無線信号送信無線ノード N_j は、以下のいずれかの条件を満たすものとする(図6)。

[ノイズ無線信号送信無線ノード N_j]

- (1) N_j は N_i の隣接無線ノードであり、 N_{i+1} の隣接無線ノードではない。
- (2) N_j は N_i と N_{i+1} のいずれの隣接無線ノードでもなく、かつ、 N_i と N_{i+1} の2ホップ隣接無線ノードである。

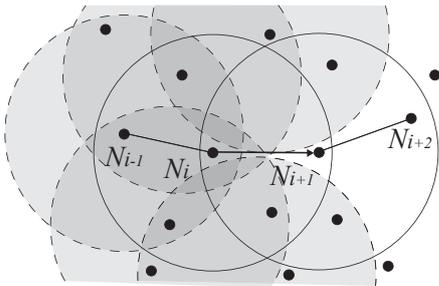


図 6 無線マルチホップ通信のためのノイズ無線信号送信

3.3 提案プロトコル

前節で述べたように、中継無線ノード N_i とその次ホップ中継無線ノード N_{i+1} との共通の 2 ホップ隣接無線ノード N' によるノイズ無線信号送信によって、 N_i の無線信号到達範囲をノイズ無線信号到達範囲によってより広く被覆することができる。ただし、 N' の決定を N_i からのデータメッセージ転送時に決定することは、配送遅延を延長してしまうことから適切ではない。そこで、ノイズ無線信号を送信する無線ノードの決定には、論文 [3] のように AODV を基礎として、経路探索要求メッセージ $Rreq$ のフラッディングと経路探索応答メッセージ $Rrep$ に加えて、 $Rrep$ メッセージのユニキャスト返送の際に追加の制御メッセージを用いることによって実現する方法を適用する。

図 7 に示すように、中継無線ノード N_i がその前ホップ中継無線ノード N_{i-1} へと $Rrep$ 制御メッセージを送信するとき、 N_i の隣接無線ノードは N_i^n はこの $Rrep$ 制御メッセージを傍受することができる。このとき、 N_i^n はノイズ無線信号送信要求制御メッセージ $Jreq(i)$ をブロードキャスト送信する。このプロトコルにより、 N_i が N_{i-1} へユニキャスト送信した $Rrep$ 制御メッセージを受信したが、 N_{i+1} が N_i へユニキャスト送信した $Rrep$ 制御メッセージを受信しなかった無線ノードは、 N_i から N_{i+1} へのデータメッセージ転送時にノイズ無線信号を送信するノードとなる。また、 N_i の隣接無線ノードと N_{i+1} の隣接無線ノードとがそれぞれ送信した $Jreq(i)$ 制御メッセージと $Jreq(i+1)$ 制御メッセージの両方を受信した無線ノードも、 N_i から N_{i+1} へのデータメッセージ転送時にノイズ無線信号を送信するノードとなる。

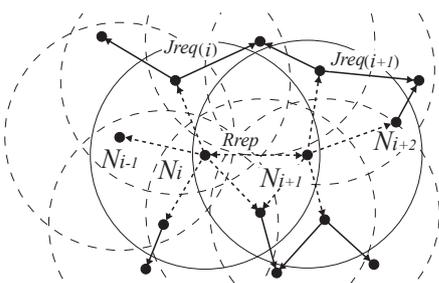


図 7 ノイズ無線信号送信ノード選択プロトコル

[ノイズ無線信号送信無線ノード選択プロトコル]

- (1) 中継無線ノード N_i がブロードキャスト送信した $Rrep$ メッセージを受信した N_i の隣接無線ノード N は、 $Jreq(i)$ メッセージをブロードキャスト送信する。
- (2) N_i がブロードキャスト送信した $Rrep$ メッセージを受信し、 N_{i+1} がブロードキャスト送信した $Rrep$ メッセージを受信していない無線ノード N は、 N_i が N_{i+1} にデータメッセージを転送する際にノイズ無線信号を送信する。
- (3) いずれの $Rrep$ メッセージも受信せず、かつ、 $Jreq(i)$ と $Jreq(i+1)$ の両方を受信した無線ノード N は、 N_i が N_{i+1} にデータメッセージを転送する際にノイズ無線信号を送信する。

N_i からの $Rrep$ 制御メッセージを受信し、 N_{i+1} からの $Rrep$ 制御メッセージを受信しないことでノイズ無線信号送信無線ノードとなった無線ノードは、前節で述べた無線アドホック通信におけるノイズ無線信号送信手法と同様、 N_i からの RTS 制御メッセージを受信することによってノイズ無線信号の送信時間を特定することができる。一方、 N_i と N_{i+1} の隣接無線ノードが送信した $Jreq(i)$ と $Jreq(i+1)$ を受信することでノイズ無線信号送信無線ノードとなった無線ノード N' は、RTS 制御メッセージと CTS 制御メッセージのいずれをも受信することができないため、追加メッセージを用いることなくノイズ無線信号の送信時間を特定することは困難である。そこで、追加制御メッセージを用いてノイズ無線信号の送信時間を検出する方法が考えられる。しかし、RTS 制御メッセージを受信した N_i の隣接無線ノードが N_i から N_{i+1} へのデータメッセージ転送までの時間に追加制御メッセージを送信すると、 N_i において CTS 制御メッセージとの衝突が発生する。一方、CTS 制御メッセージを受信した N_{i+1} の隣接無線ノードは N_i から N_{i+1} へのデータメッセージ転送までの時間に追加制御メッセージを送信することはできない。したがって、データメッセージ配送遅延の延長を回避するために、RTS/CTS 制御手法に追加制御メッセージの転送時間を導入することなしに 2 ホップ隣接無線ノードからノイズ無線信号を送信することは困難である。そこで、本論文では、 N_i の隣接無線ノードが送信するノイズ無線信号を受信した 2 ホップ隣接無線ノードがノイズ無線信号を送信することとする。これによって、ノイズ無線信号を送信する無線ノードは N_i の隣接無線ノードであり N_{i+1} の隣接無線ノードではない無線ノードに隣接する N_i と N_{i+1} の共通の 2 ホップ隣接無線ノードに制限され、 N_i と N_{i+1} の共通の隣接無線ノードのみを隣接無線ノードとする N_i と N_{i+1} の共通の 2 ホップ隣接無線ノードからはノイズ無線信号が送信されないこととなる。また、ノイズ無線信号の送信時間は、最短のデータメッセージ転送時間に制限することで、 N_{i+1} から N_i へ返送される受信確認メッセージとノイズ無線信号との N_i

における衝突を回避する。

4. 評価

ここでは、各無線ノードの無線信号到達距離を 100m とし、中継無線ノードと次ホップ中継無線ノードとの距離を 0–100m の範囲とする。また、各無線ノードの平均隣接無線ノード数を 0–20 として無線ノードを一様分布乱数によってランダムに配置する。各中継無線ノード間距離に対して 1,000 通りの異なる無線ノード配置を行ない、それぞれの配置に対するノイズ無線信号到達範囲による被覆率を、(1) 中継無線ノードの 1 ホップ隣接無線ノードのみからノイズ無線信号を送信した場合、(2) 中継無線ノードの 1 ホップ隣接無線ノードと 2 ホップ隣接無線ノードからノイズ無線信号を送信した場合、(3) 中継無線ノードの 1 ホップ隣接無線ノードとそれに隣接する 2 ホップ隣接無線ノードからノイズ無線信号を送信した場合（本論文の提案手法）、の 3 通りについて評価した。

評価実験結果を図 8 に示す。被覆率は、平均隣接無線ノード数、中継無線ノード間距離に対して単調に増加している。1 ホップ隣接無線ノードのみからノイズ無線信号を送信した場合に注目すると、隣接無線ノード数が増えるほどノイズ無線信号送信ノード数も大きくなり被覆率が高くなる。また、中継無線ノード間距離が短くなるほどデータメッセージ転送と衝突することなくノイズ無線信号を送信できる 1 ホップ隣接無線ノードが少なくなるため、被覆率が低下する。2 つの中継無線ノードに共通の 2 ホップ隣接無線ノードからのノイズ無線信号送信を行なうことによって、中継無線ノード間距離が短い場合の被覆率が大きく改善されることが分かる。2 つの中継無線ノードの共通の無線信号到達範囲における被覆率は、これら 2 つの中継無線ノードの無線信号到達範囲に含まれない 2 ホップ隣接無線ノードからのノイズ無線信号送信によって改善されることが示された。ただし、RTS/CTS 制御のための制御メッセージおよびデータメッセージと衝突することなくノイズ無線信号の送信時間を決定するための追加制御メッセージを送信することが、RTS/CTS 制御メッセージ交換手法を変更することなく実現することが困難であるために、2 ホップ隣接無線ノードによるノイズ無線信号送信を制約した本論文で提案したノイズ無線信号送信手法では、被覆率の改善が大きく制約されることも明らかとなった。このことから、RTS/CTS 制御のための制御メッセージ交換手法にも修正を加えることで、ノイズ無線信号を送信する 2 ホップ隣接無線ノード数を増加させる手法の検討が必要であると考えられる。

なお、送受信無線ノード間距離が長く被覆率が比較的高い場合には、隣接無線ノード数の増加に対して被覆率が改善せず、飽和していることがわかる。すなわち、必要以上にノイズ無線信号送信無線ノードを増やすことは、各無線

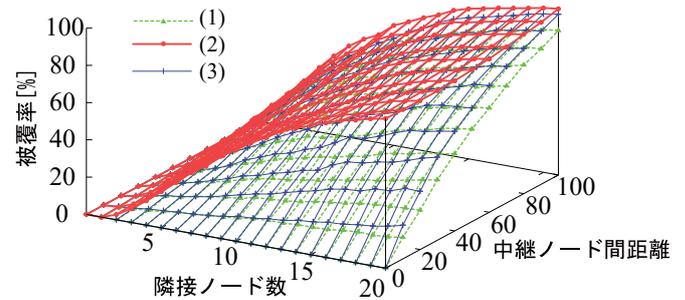


図 8 無線アドホック通信におけるノイズ無線信号到達範囲による被覆率

ノードの消費電力を増加させる、他の無線マルチホップ配送経路に沿ったデータメッセージ転送との衝突を発生させるなどの問題を起こすことこそあれ、被覆率を改善することにはならないことを示している。そこで、ノイズ無線信号送信無線ノードを選択、削減する手法を追加することが必要である。

次に、無線マルチホップ配送に対して提案手法を適用した場合の性能についてシミュレーション実験評価を行なう。ここでは一辺 700m の正方形領域に無線信号到達距離 50m の無線ノード 100–1000 台を一様分布によりランダムに配置する。ただし、送信元無線ノードと送信先無線ノードの座標はそれぞれ (200,200), (500,500) で固定する。1,000 通りの異なる無線ノード配置に対して、それぞれの配送経路における各中継無線ノードの無線信号到達範囲に対するノイズ無線信号到達範囲による被覆率を、(1) 中継無線ノードの 1 ホップ隣接無線ノードのみからノイズ無線信号を送信した場合、(2) 中継無線ノードの 1 ホップ隣接無線ノードとそれに隣接する 2 ホップ隣接無線ノードからノイズ無線信号を送信した場合（本論文の提案手法）、の 2 通りについて評価した。

評価実験結果を図 9 に示す。1 ホップ隣接無線ノードのみからノイズ無線信号を送信した場合に注目すると、隣接無線ノード数が増えるほどノイズ無線信号送信ノード数も大きくなり被覆率が高くなる。また、配送経路の形状によってデータメッセージ転送と衝突することなくノイズ無線信号を送信できる 1 ホップ隣接無線ノードが少ない転送が発生するため、被覆率の分散が大きい。これに対し、2 つの中継無線ノードに共通の 2 ホップ隣接無線ノードからのノイズ無線信号送信を行なう手法では、2 ホップ隣接無線ノードからのノイズ無線信号送信によってそれぞれの平均隣接無線ノード数に対する被覆率が 11% 高くなっている。

さらに、配送経路の形状による被覆率の分散が縮小されていることがわかる。2 つの中継無線ノードの共通の無線信号到達範囲における被覆率の分散は、2 つの中継無線ノードの無線信号到達範囲に含まれない 2 ホップ隣接無線ノードからのノイズ無線信号送信によって改善されており、ノードの配置の変化に対して安定した被覆率の実験が可能と

なっていることがわかる。

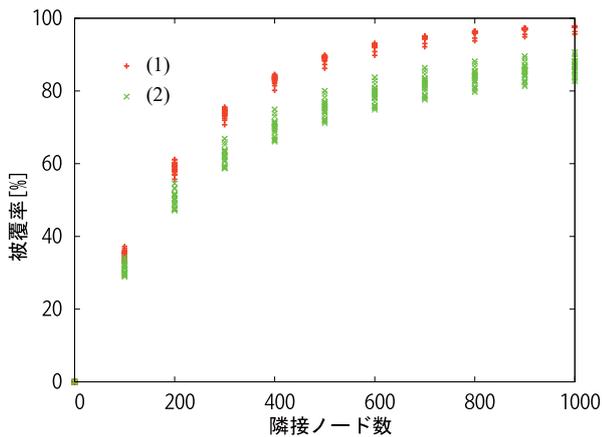


図 9 無線マルチホップ配送におけるノイズ無線信号到達範囲による被覆率

5. まとめと今後の課題

本論文では、無線マルチホップ通信において、中継無線ノードがその次ホップ中継無線ノードにデータメッセージを転送する際に、盗聴無線ノードがこのデータメッセージを傍受することを近隣無線ノードがノイズ無線信号を送信することによって困難にする手法を提案した。ここでは、次ホップ中継無線ノードによる転送データメッセージの受信を妨げることなく、ノイズ無線信号とデータメッセージとの衝突によって盗聴無線ノードによる傍受を妨げる。ノイズ無線信号送信無線ノードの選択はルーティングプロトコルの一部として実現する。また、ノイズ無線信号の送信時間は、RTS/CTS 制御信号の交換とノイズ無線信号の傍受によって特定する。シミュレーション実験により、ノイズ無線信号送信ノードとして選択されたすべての1ホップおよび2ホップ隣接無線ノードからのノイズ無線信号送信が実現すれば、十分に高い被覆率を得ることができることを示した。特に、無線マルチホップ配送においては1ホップ隣接無線ノードによるノイズ無線信号の送信のみでは無線マルチホップ配送経路の形状によって被覆率の高低が影響を受け易いのに対して、2ホップ隣接無線ノードの一部を加えることによってその分散が縮小し、安定的な被覆率を実現することができることが明らかとなった。今後は、被覆率を改善するノイズ無線信号送信タイミングの通知手法を考案する。

参考文献

- [1] Boneh, D., Dunworth, C. and Lipton, R.J., “Breaking DES Using a Molecular Computer,” Proceedings of the 1st International Workshop on DNA Based Computers, pp. 37–66 (1995).
- [2] He, X. and Yener, A., “Two-Hop Secure Communication

Using an Untrusted Relay: A Case for Cooperative Jamming,” Proceedings of the IEEE Global Telecommunications Conference 2008 (2008).

- [3] Kanachi, T. and Higaki, H., “Wireless Multihop Transmissions for Secret Sharing Communication,” Proceedings of the 14th IEEE International Conference on Scalable Computing and Communications, pp. 808–813 (2014).
- [4] Kranakis, E., Singh, H. and Urrutia, J., “Compass Routing on Geometric Networks,” Proceedings of the 11th Canadian Conference on Computational Geometry, pp. 51–54 (1999).
- [5] Tekin, E. and Yener, A., “The General Gaussian Multiple-Access and Two-Way Wiretap Channels: Achievable Rates and Cooperative Jamming,” IEEE Transactions on Information Theory, Vol. 54, No. 6, pp. 2735–2750 (2008).