

# 秘密分散通信のためのアドホックルーティング手法

金持 徹也<sup>1,a)</sup> 桧垣 博章<sup>1,b)</sup>

**概要：**無線マルチホップネットワークにおいて、データメッセージ群を複数の異なる経路を用いて配送する秘密分散通信を行なうための隣接独立ルーティング手法を提案する。ここで、盗聴無線ノードを含むすべての無線ノードが高々単一経路を配送されるデータメッセージ群のみを取得し、複数経路を配送されるデータメッセージを取得しないことを実現するために、異なる経路に含まれる中継無線ノードの無線信号到達範囲の共通領域に無線ノードが含まれることを回避する。ただし、送信元無線ノードと送信先無線ノードの近隣では複数配送経路が近接することから、これらの無線ノードの近隣は盗聴無線ノードが存在しない安全領域であることを適用条件とする。また、簡易実験結果により、提案するルーティングプロトコルに従った制御メッセージ送信を行わない盗聴無線ノードが複数経路を配送されるデータメッセージ群を取得できる領域は1%未満であり、これを可能とする経路が検出される可能性を考慮すれば、実際にデータメッセージ群を取得できることはほとんど考えられないことを示す。

## Ad-hoc Routing Method for Secret Sharing Communication

TETSUYA KANACHI<sup>1,a)</sup> HIROAKI HIGAKI<sup>1,b)</sup>

**Abstract:** This paper proposes a novel routing protocol called neighbor-disjoint routing protocol in wireless multihop networks for secret sharing communication where data messages are transmitted along multiple wireless multihop transmission routes. Here, all wireless nodes including wiretapping wireless nodes receive data messages transmitted along at most one transmission route, i.e., they never receive data messages transmitted along multiple transmission routes. This is realized by the proposed protocol which ensures that there are no or less wireless nodes whose locations are included in wireless transmission ranges of intermediate wireless nodes included in different wireless multihop transmission routes. In order to assure this security property, it is assumed that there are no wiretapping wireless nodes around the source and the destination wireless nodes since multiple wireless transmission routes are neighboring. A result of naive experiments show that an area where wiretapping wireless nodes are included in wireless signal transmission ranges of intermediate wireless nodes in different wireless transmission routes is less than 1% under our neighbor-disjoint routing environments.

### 1. はじめに

アドホックネットワークやセンサネットワークのようなデータメッセージの無線マルチホップ配送によって無線ノード間の相互接続を実現するネットワークの研究開発が活性化しつつある。ここでは、送信元無線ノードから送信先無線ノードまでのデータメッセージ配送は、無線マルチ

ホップ配送経路を構成する中継無線ノードがデータメッセージを順次転送することによって実現される。ここでは、無線ノードの移動性、無線リンクの低信頼性等を考慮した経路制御が必要であり、有線ネットワークとは異なる無線ネットワークの特性に基づいた独自のルーティングプロトコルが検討、提案されている。有線ネットワークと無線ネットワークが典型的に異なる特性のひとつとして、無線通信のブロードキャスト性がある。隣接無線ノード間のユニキャスト通信においても、無線信号は送信無線ノードのすべての隣接無線ノードに到達し受信される。一方、安全なネットワーク通信を実現する手法のひとつに秘密分散通

<sup>1</sup> 東京電機大学未来科学部ロボット・メカトロニクス学科  
Department of Robotics and Mechatronics, Tokyo Denki University

<sup>a)</sup> kanachi@higlab.net

<sup>b)</sup> hig@higlab.net

信がある。配送対象のデータを複数のデータメッセージに分割し、異なる複数の経路を用いて配送することによって盗聴者が取得可能なデータメッセージの一部に限定することによってデータの盗聴を困難にする手法である。無線マルチホップネットワークにおいて秘密分散通信を実現するためには、分割配送するための複数の無線マルチホップ配送経路を従来の複数経路探索アドホックルーティングプロトコルで検出することはできない。本論文では、これを実現するために求められる複数経路の隣接独立性を示し、隣接独立な複数経路を検出するアドホックルーティングプロトコルを構成する。

## 2. 関連研究

データを盗聴等により不正に取得されることを防止する手法に秘密分散法 [2, 12] がある。ここでは、データもしくはデータの暗号鍵をデータ片に分割し、各データ片を個別の記憶、通信する [15, 17]。このとき、データ片の全体あるいは定められた閾値を越える割合を取得しない限りデータの全体あるいは一部の取得が不可能であるように分割を施すことによって秘密を保持する。単一の送信元ノードから単一の送信先ノードへのデータ配送に対して秘密分散法を適用する場合、それぞれのデータ片を異なる複数の配送経路を用いて配送することによって盗聴者がデータを不正に取得することが困難になる。すなわち、データを  $m$  個のパケット群に分割し、動的に定められた異なる  $n$  個の配送経路に沿ってパケットを配送することによって、盗聴者がすべてもしくは閾値以上のパケットを入手することを困難にすることができる。論文 [7] では、有線ネットワークを対象として動的に定められた複数の中継点（ルータ）を経由する配送経路を用いる秘密分散通信手法を提案している。ここでは、送信元ノードから送信先ノードまでのホップ数に基づいて定めた TTL とランダムに選んだ IP アドレスを用いて複数の中継点を探索し、この中継点を経由した IP データグラム配送を ICMP エコーによるカプセル化を用いて実現している。一方、論文 [14] では、アドホックネットワーク等の無線マルチホップネットワークにおいて複数の配送経路による秘密分散通信を用いることによって盗聴等を困難とする手法が提案されている。ここでは、秘密分散通信における符号化手法の提案とその効果の評価がなされており、秘密分散通信の有効性が示されている。しかし、配送経路の探索には従来の複数経路アドホックルーティングプロトコルを適用することとしている。

ネットワークを構成する各無線ノードがデータ配送の中継ノードとして機能する無線マルチホップネットワークでは、無線信号のブロードキャスト性、無線通信の低信頼性、無線ノードの移動性等を考慮し、多様なルーティングプロトコルが提案されている [1]。ここでは、送信元無線ノードから送信先無線ノードまでの単一配送経路を探索、検出す

る多くのルーティングプロトコルに加えて、複数経路を探索、検出するルーティングプロトコル [8] が提案されている。無線マルチホップネットワークでは、送信元無線ノード、中継無線ノード、送信先無線ノードの移動や電源容量枯渇によるネットワークからの離脱、障害物の移動、無線ノイズの発生等によって、ルーティングプロトコルを用いた唯一の無線マルチホップ配送経路が切断されることが考えられる。この場合の経路再探索や経路修復による無線マルチホップ配送の一時停止時間の短縮を目的として、複数経路を同時に探索、検出するルーティングプロトコルと経路切替手法の導入が提案されている [10]。このとき、現用配送経路の切断原因となる無線リンクの切断（無線ノードの移動や障害物の移動、無線ノイズの発生等による）や無線ノードの離脱（無線ノードの電源容量枯渇や故障による）によって切替配送経路も同時に切断されることを回避するために、リンク独立 (Link-Disjoint) な複数経路探索、検出を行なうルーティングプロトコル [4] (図 1) やノード独立 (Node-Disjoint) な複数経路探索、検出を行なうルーティングプロトコル [5] (図 2) が提案されている。ただし、すべての無線ノードが同様に移動、電力消費、故障する環境においては、切替経路が現用配送経路よりも特別に切断し難いことはなく<sup>\*1</sup>、ルーティングオーバーヘッドとデータ配送の一時停止によるアプリケーションへの悪影響のトレードオフが重要となる。なお、論文 [3] では、再経路探索頻度の低減を目的としてメッシュ状により多数の配送経路を検出する手法を提案している。

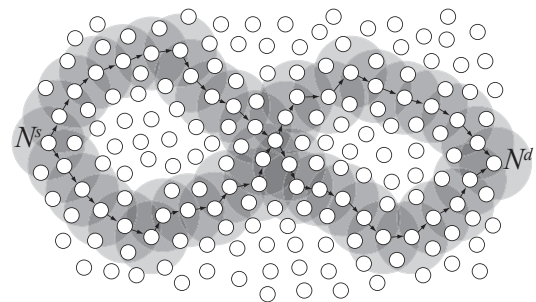


図 1 リンク独立な無線マルチホップ配送経路

ルーティングプロトコルで検出した複数の配送経路を切断時に切替えて用いるばかりでなく、これらの複数配送経路を同時並行に用いてデータを配送することによってエンドエンドのスループットを向上することが検討されている。ここで、無線信号はブロードキャスト性を持ち、隣接無線ノードを宛先として送信されたメッセージを含む無線信号はすべての隣接無線ノードへと到達する。この無線信号の干渉を原因とする晒し端末問題と隠れ端末

<sup>\*1</sup> もしくはデータの暗号鍵一般的に切替経路は現用経路よりも経路長が大きいために移動と故障による切断頻度は高いことが見込まれる。データ配送による電力消費の観点では現用経路の方が切替経路よりも切断の可能性が高い。

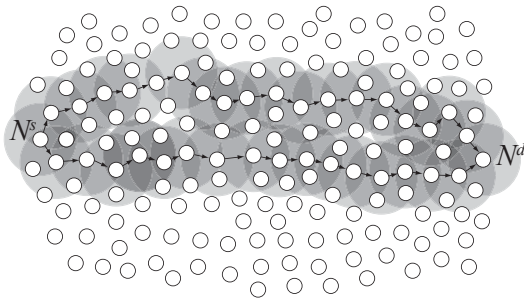


図2 ノード独立な無線マルチホップ配送経路

問題によって無線マルチホップ配送の性能低下, すなわち, データ紛失率の上昇, データ配送遅延の延長, データ配送スループットの低下を招く問題がある. 送信元無線ノード  $N^s$  から送信先無線ノード  $N^d$  への異なる無線マルチホップ配送経路  $\mathcal{R} := \{N_0(= N^s) \dots N_n(= N^d)\}$  および  $\mathcal{R}' := \{N'_0(= N^s) \dots N'_{n'}(= N^d)\}$  を同時並行に用いてデータ配送を行なう場合,  $N_i \in \mathcal{R}$  の無線信号到達範囲に  $N'_j \in \mathcal{R}'$  が含まれることによって,  $N_i$  と  $N'_j$  が互いに晒し端末となるとともに  $N_i$  と  $N'_{j-1}$  が互いに隠れ端末となることによってデータ転送の並行性が低下し, エンドエンドスループットの低下を招く.

この問題を解決するために, 経路に含まれる中継ノードを互いに無線信号到達範囲にできるだけ含まない (Radio-Disjoint) 経路を探索, 検出するルーティングプロトコルが提案されている [6, 13, 16](図3). ここでは, 配送経路  $\mathcal{R}$  の中継無線ノード  $N_i \in \mathcal{R}$  と配送経路  $\mathcal{R}'$  の中継無線ノード  $N'_j \in \mathcal{R}'$  とが互いに無線信号到達範囲に含まれないことによって晒し端末問題と隠れ端末問題の発生を回避し, 干渉による無線信号の衝突や衝突回避のための待機時間による配送遅延延長による性能低下を低減する. ただし, 送信元無線ノードと送信先無線ノードの近隣の無線中継無線ノードにおいては, 複数配送経路の近接は回避できない問題がある.

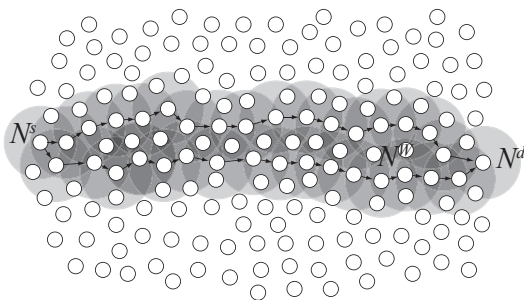


図3 無線信号独立な無線マルチホップ複数配送経路

無線マルチホップネットワークにおける秘密分散通信を実現するためには, 異なる複数の配送経路を用いて同時並行に配送されるデータ片を含むパケット群を盗聴者が取得することを回避することが求められる. しかし, 図3に示すように, 配送経路  $\mathcal{R}$  の中継無線ノード  $N_i \in \mathcal{R}$  と配送経路  $\mathcal{R}'$  の中継無線ノード  $N'_j \in \mathcal{R}'$  の双方の無線信号到達範

囲に含まれる無線ノード  $N^w$  は,  $\mathcal{R}$  と  $\mathcal{R}'$  に沿って配送されるすべてのパケット群を取得することが可能であるという問題があり, これまでに提案されている複数経路探索, 検出を行なうアドホックルーティングプロトコルの適用では解決することができない.

### 3. 提案手法

#### 3.1 隣接独立配送経路

送信元無線ノードから複数の中継無線ノードを経由して送信先無線ノードへとデータを配送する無線マルチホップ通信では, 各無線ノードがデータを含む無線信号をブロードキャストすることから, 無線信号到達範囲に含まれるすべての無線ノードが無線信号を受信し, 配送データを取得することができる. 複数配送経路を用いた秘密分散通信を無線マルチホップネットワークで実現するためには, いずれかの配送経路に含まれる無線ノード, いずれの配送経路にも含まれないノードのいずれにおいても, 複数の異なる経路に沿って配送されるデータメッセージ群を受信することができないようにすることが, データの盗聴をより困難とするために求められる. いずれかの配送経路に含まれる中継無線ノードが他の配送経路の中継無線ノードの無線信号到達範囲に含まれないことは, 無線信号独立 (Radio-Disjoint) な複数経路探索ルーティングプロトコルによって検出することができる. 一方, いずれの配送経路にも含まれない無線ノードが異なる複数の配送経路に含まれる中継無線ノードの無線信号到達範囲に共通に含まれないようにすることは, 従来の複数経路探索ルーティングプロトコルでは実現することができない.

そこで, 本論文では, 送信元無線ノード  $N^s$  から送信先無線ノード  $N^d$  への複数の無線マルチホップ配送経路  $\mathcal{R}^i := \{N_0^i \dots N_{N_i}^i\}$  を用いて秘密分散通信を実現するために, 複数の異なる中継無線ノードの無線信号到達範囲に含まれる無線ノードの発生を回避するルーティング手法を提案する. すなわち,  $R(N)$  を無線ノード  $N$  の無線信号到達範囲とすると,  $\forall N \in R(N_j^i)$  について  $N \notin R(N_{j'}^i | i \neq i')$  となる複数の無線マルチホップ配送経路  $\mathcal{R}^i$  を定めるプロトコルを提案する. 図4に示すように, これは異なる複数の無線マルチホップ配送経路間で隣接無線ノードを共有しないことを意味していることから, 本論文ではこのような配送経路は隣接独立 (Neighbor-Disjoint) な無線マルチホップ配送経路であると呼ぶ. 各配送経路を互いに隣接独立とすることによって, 送信元無線ノードと送信先無線ノードを除いた他のすべての無線ノードは, 高々単一経路に沿って配送されるデータメッセージしか受信することができない.

しかし, 送信元無線ノードと送信先無線ノードの近隣においては複数の配送経路が互いに近接するため, 隣接独立な複数経路を検出することは困難である. これは, 無線信号独立な複数配送経路の探索においても同様に生じる問



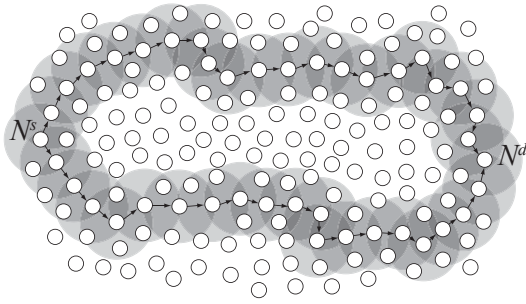


図 4 隣接独立な無線マルチホップ複数配送経路

題である．ここで，秘密分散通信の適用シーンとして，送信元無線ノード  $N^s$  と送信先無線ノード  $N^d$  の近隣には盗聴無線ノード  $N^w$  が存在しない状況が考えられる．例えば， $N^s$  と  $N^d$  がそれぞれ異なるオフィスの内部にあり，これらのビル内には  $N^w$  が侵入することができない等が考えられる．そこで， $N^s$  と  $N^d$  はそれぞれ安全領域  $SZ^s$ ， $SZ^d$  に含まれており，これらの領域内部には  $N^w$  が存在しないこととする．このため， $SZ^s$  と  $SZ^d$  のいずれかに含まれる無線ノードは，互いに隣接独立である必要はなく，複数の配送経路に含まれる中継無線ノードの無線信号到達範囲に含まれることを可とする．したがって，本論文で構成する隣接独立な複数無線マルチホップ配送経路  $R^i$  は， $\forall N \in R(N_j^i) \setminus (SZ^s \cup SZ^d)$  について  $N \notin R(N_j^{i'} | i \neq i')$  となるものである．

### 3.2 ルーティングプロトコル

3.1 節で述べた隣接独立な複数無線マルチホップ配送経路を検出するアドホックルーティングプロトコルを構成する．ここでは，配送経路をひとつずつインクリメンタルに検出するプロトコルとする．送信元無線ノード  $N^s$  と送信先無線ノード  $N^d$  はそれぞれ安全領域  $SZ^s$  と  $SZ^d$  に含まれているとする．提案プロトコルに従って機能するすべての無線ノードの無線信号到達範囲に被覆される無線マルチホップネットワーク領域には，少数の盗聴無線ノードが存在し得るが  $SZ^s$  と  $SZ^d$  には侵入しないものとする．

各  $p$  番目の無線マルチホップ配送経路探索には AODV [9] を用いるものとする．ただし， $1 \leq q < p$  番目に検出された無線マルチホップ配送経路の中継無線ノードとその隣接無線ノードおよびその隣接無線ノード (すなわち 中継無線ノードの 2 ホップ隣接無線ノード) は  $p$  番目の無線マルチホップ配送経路の中継無線ノードとはなり得ないことから経路探索要求制御メッセージ  $Rreq$  のフラッディングには参加しない．これを実現するために， $q$  番目の経路探索における経路探索応答制御メッセージ  $Rrep$  の  $N^d$  から  $N^s$  への検出経路に沿ったユニキャスト配送においては，この経路の中継無線ノード  $N^i$  の隣接無線ノード  $N^{ni}$  が  $Rrep$  を傍聴 (overhear) することによってこの経路の隣接無線ノードであることを検出し， $p$  番目の経路探索における  $Rreq$  を

受信してもこれをブロードキャストしないこととする．さらに， $N^{ni}$  が拡張経路探索応答制御メッセージ  $eRrep$  をブロードキャスト送信し，これを受信した無線ノード  $N^{nni}$  も  $p$  番目の経路探索における  $Rreq$  を受信してもこれをブロードキャストしない．

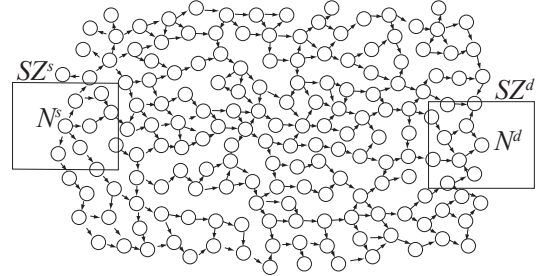


図 5  $Rreq$  のフラッディングによる第 1 経路検出

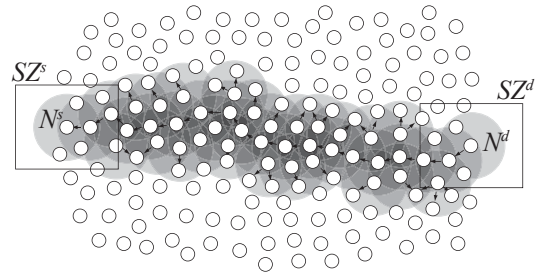


図 6  $Rrep$  と  $eRrep$  による第 2 経路検出への制限

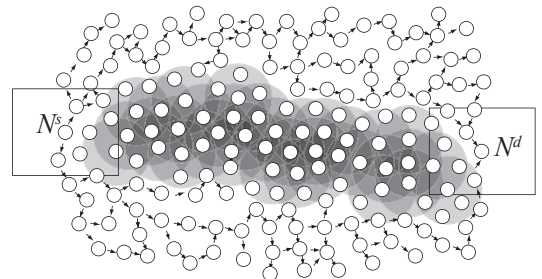


図 7  $Rreq$  のフラッディングによる第 2 経路検出

$SZ^s$  と  $SZ^d$  に含まれる無線ノード  $N$  については以下のようにする．上記のプロトコルにおいて，検出された配送経路の中継無線ノードおよびその隣接無線ノードが新たに検出される配送経路の中継ノードとならないようにするのは，安全領域外に形成される盗聴可能領域を削減するためである．この観点で考えると，無線信号到達範囲が安全領域に含まれる中継無線ノードのみと隣接する場合には，盗聴可能領域を拡大し得ないことから以降の経路検出においても中継無線ノードの候補とすべきである．一方，無線信号到達範囲に安全領域外を含む中継無線ノードと隣接する無線ノードは，自身およびその隣接無線ノードが以降に検出される無線マルチホップ配送経路に含まれることによって盗聴可能領域を拡大することになる．そこで，これ

らの無線ノードは  $eRrep$  メッセージをブロードキャスト送信するとともに以降の経路探索では  $Rreq$  のフラッディングに参加しない。なお、各無線ノード自身が安全領域に含まれるか否かは何らかの管理機構によって与えられる情報で検知可能であり、隣接無線ノードが安全領域に含まれるか否かは管理機構によって提供されるデジタル署名等の機構によって把握可能であるものと仮定する。

[送信元無線ノード  $N^s$ ]

- (1)  $p$  番目の配送経路を探索する  $Rreq$  をブロードキャスト送信する。
- (2) 隣接無線ノード  $N_1^p$  から  $Rrep$  を受信したならば、 $N_1^p$  を  $p$  番目の配送経路の次ホップ無線ノードとする。

[送信先無線ノード  $N^d$ ]

- (1) 最初に受信した  $p$  番目の配送経路を探索する  $Rreq$  を送信した隣接無線ノード  $N_{np-1}^p$  へ  $Rrep$  をユニキャスト送信する。

[中継無線ノード  $N_i^{(p)}$ ]

- (1) 最初に受信した  $p$  番目の配送経路を探索する  $Rreq$  を隣接無線ノード  $N_{i-1}^{(p)}$  から受信したならば、この  $Rreq$  をブロードキャスト送信する。
- (2) 隣接無線ノード  $N_{i+1}^{(p)}$  から  $Rrep$  を受信したならば、 $N_{i+1}^{(p)}$  を  $p$  番目の配送経路の次ホップ無線ノードするとともに、この  $Rrep$  を  $N_{i-1}^{(p)}$  へユニキャスト送信する。
- (3) 自身もしくは隣接無線ノードの少なくとも1つが安全領域外にあるならば、以降に  $Rreq$  を受信してもブロードキャスト送信しない。

[中継無線ノードの隣接無線ノード  $N_i^{ni(p)}$ ]

- (1) 隣接無線ノード  $N_{i-1}^{(p)}$  から  $N_{i-1}^{(p)}$  へユニキャスト送信された  $Rrep$  を傍受し、自身もしくは隣接無線ノードの少なくとも1つが安全領域外にあるならば、 $eRrep$  をブロードキャスト送信する。以降に  $Rreq$  を受信してもブロードキャスト送信しない。

[中継無線ノードの2ホップ隣接無線ノード  $N_i^{nni(p)}$ ]

- (1) 隣接無線ノード  $N_i^{ni(p)}$  からブロードキャスト送信された  $eRrep$  を受信し、自身もしくは隣接無線ノードの少なくとも1つが安全領域外にあるならば、以降に  $Rreq$  を受信してもブロードキャスト送信しない。

□

### 3.3 実験

3.2 節で提案した秘密分散通信のための隣接独立配送経路検出のためのアドホックルーティングプロトコルは、すべての無線ノードが提案プロトコルに従って機能するときに複数の異なる経路に沿って配送されるデータメッセージ群を安全領域外の無線ノードが取得しないことを実現する。ここで、盗聴無線端末  $N^w$  はプロトコルに従った制御メッセージの送信を行わず、自信の存在の他の無線ノードに

知らせないことによって、複数の異なる配送経路に含まれる中継無線ノードの無線信号到達範囲に含まれる位置でこれらの経路を配送されるすべてのデータメッセージ群を受信することが可能となる。すなわち、

配送経路  $\mathcal{R} := ||N_0(= N^s) \dots N_n(= N^d)||$  の中継無線ノード  $N_i$  と配送経路  $\mathcal{R}' := ||N'_0(= N^s) \dots N'_n(= N^d)||$  の中継無線ノード  $N'_j$  の無線信号到達範囲  $R(N_i)$  と  $R(N'_j)$  の共通領域に盗聴無線ノード  $N^w$  が含まれ  $N^w \in R(N_i) \cap R(N'_j)$  を満足することが考えられる。ただし、提案プロトコルに従って機能する別の無線ノード  $N$  がこの共通領域にあり  $N \in R(N_i) \cap R(N'_j)$  を満足するのであれば、 $\mathcal{R}$  と  $\mathcal{R}'$  がデータメッセージ群の同時並行配送に用いられることはない。そこで、2つの異なる配送経路のそれぞれの中継無線ノードの無線信号到達範囲に共通する領域に提案プロトコルに従って機能する無線ノードが存在しないことがどの程度発生するかをシミュレーション実験によって評価する。

ここでは、1,000m × 1,000m の正方形領域に無線信号到達距離が 100m の無線ノード 50–500 台を一様乱数を用いてランダムに配置し、いずれかの無線ノード対について、その無線信号到達範囲に無線ノードが1台も含まれない領域の全体正方形領域に対する割合を計測する。この領域に含まれる盗聴無線ノードは、この領域を無線信号到達範囲に共通に含む無線ノード対がそれぞれ異なる配送経路に含まれる場合、これらの経路に沿って配送されるすべてのデータメッセージ群を受信することになる。実験結果を図8に示す。ここでは、いずれか1対の無線ノードの無線信号到達範囲に含まれる領域の全体正方形領域に対する割合を合わせて計測している。この割合が小さい場合には、無線マルチホップ配送経路の探索成功率が低く、そもそもデータメッセージ配送を行なうことができない。実験結果から、 $N^w$  が複数経路の中継無線ノードの無線信号到達範囲に含まれる可能性がある領域の割合は 0.217–1.72% の範囲であり、無線ノード分布密度の上昇とともに低下する。また、隣接無線ノードに共通に無線信号到達範囲に含まれる領域は無線ノード分布密度の上昇とともに上昇し、無線ノード 200 台以上では 99.0% 以上となる。論文 [11] では、無線マルチホップ配送経路を十分高い確率で検出するためには無線ノードの平均隣接ノード数が 8 台程度必要としており、本実験では 255 台以上となる。このとき、盗聴可能領域の割合は 0.379% 以下となる。実際には、この領域を形成した無線ノード対が必ずしも異なる配送経路の中継無線ノードとなるとは限らないことから、盗聴無線端末が複数経路を配送されるデータメッセージ群をすべて入手することは困難であると考えられる。

### 4. まとめ

本論文では、無線マルチホップネットワークにおいて秘

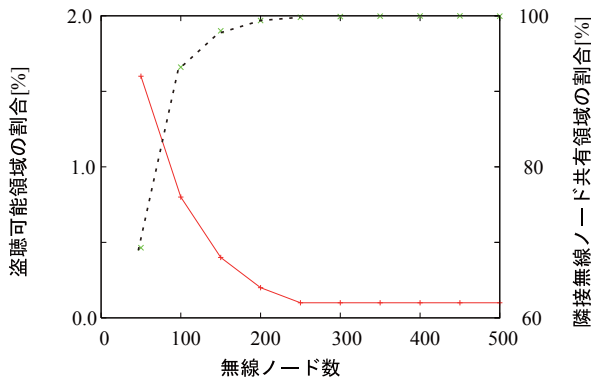


図 8 盗聴可能領域の割合

密分散通信を実現するために無線ノードが高々単一経路を配送されるデータメッセージのみを取得可能な隣接独立複数経路探索アドホックルーティングプロトコルを提案した。送信元無線ノードと送信先無線ノードは盗聴無線ノードが存在しない安全領域であることを適用条件として、各配送経路の中継無線ノードおよび中継無線ノードの隣接無線ノードが他の配送経路の中継ノードとならないことで上記の性質を保証している。また、AODVを拡張することで配送経路をインクリメンタルに検出するルーティングプロトコルを構成した。簡易なシミュレーション実験結果から、複数経路が構成可能な無線ノード分布密度においては、提案プロトコルが検出した複数経路を配送されるデータメッセージを単一盗聴無線ノードが取得することは困難であることを示した。提案したルーティングプロトコルは、複数配送経路をひとつずつ順次検出する手法である。このため、(1) 探索時間が長いことデータメッセージ配送開始までの待機時間が長い、(2) 制御メッセージのフラッディングを複数要し通信オーバーヘッドが大きい、(3) 複数経路の経路長差が大きい、という問題がある。そこで、複数経路を単一のフラッディングで探索、検出するプロトコルへの改良が望まれることから、今後検討する。

## 参考文献

- [1] Boukerche, A., Turgut, B., Aydin, N., Ahmad, M.Z., Boloni, L. and Tugut, D., "Routing Protocols in Ad Hoc Networks: A Survey," *Computer Networks*, vol. 55, no. 13, pp. 3032–3080 (2011).
- [2] Blakley, G.R., "Safeguarding Cryptographic Keys," *Proceedings of the National Computer Conference*, vol. 48, pp. 313–317 (1979).
- [3] Higaki, H. and Umeshima, S., "Multiple-Route Ad Hoc On-Demand Distance Vector (MRAODV) Routing Protocol," *Proceedings of the 18th IEEE Parallel and Distributed Processing Symposium* (2004).
- [4] Le, P.H. and Pujolle, G., "A Link-Disjoint Interference-Aware Multi-Path Routing Protocol for Mobile Ad Hoc Network," *Digital Information and Communication Technology and Its Applications*, Springer, pp. 649–661 (2011).
- [5] Lee, S.J. and Gerla, M., "Split Multipath Routing with

- Maximally Disjoint Path in Ad Hoc Networks," *Proceedings of the IEEE International Conference on Communications*, pp. 3201–3205 (2001).
- [6] Maimour, M., "Maximally Radio-Disjoint Multipath Routing for Wireless Multimedia Sensor Networks," *Proceedings of the 4th ACM Workshop on Wireless Multimedia Networking and Performance Modeling*, pp. 26–31 (2008).
- [7] Ono, M. and Higaki, H., "Dynamic Multiple-Route IP Transmission for Virtual Private Network," *Proceedings of the 4th International Conference on Communication Systems and Applications*, pp. 92–97 (2004).
- [8] Park, V.D. and Corson, M.S., "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," *Proceedings of the 16th Annual Joint Conference of the IEEE Computer and Communications Societies*, pp. 1405–1413 (1997).
- [9] Perkins, C.E., "Ad Hoc On-Demand Distance Vector (AODV) Routing," RFC 3561 (2003).
- [10] Ravindra, E., Kohir, V.D. and Mytri, V.D., "A Local Route Repair Algorithm based on Link Failure Prediction in Mobile Ad Hoc Network," *World Journal of Science and Technology*, vol. 1, no. 8, pp. 64–67 (2011).
- [11] Seyama, T. and Higaki, H., "G-AODV+PCMTAG: Routing in MANET with Low Overhead Flooding and Route-Shortening," *Proceedings of the 7th International Conference on Parallel and Distributed Computing and Networks*, pp. 103–110 (2008).
- [12] Shamir, A., "How to Generate and Exchange Secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613 (1979).
- [13] Waharte, S. and Boutaba, R., "Totally Disjoint Multipath Routing in Multihop Wireless Networks," *Proceedings of the IEEE International Conference on Communications*, pp. 5576–5581 (2006).
- [14] 今井, 藤井, 渡辺, "多経路を用いたセキュア無線ネットワークに関する一検討," *信学技報*, vol. 108, no. 205, pp. 25–30 (2008).
- [15] 栗原, 桑門, "修復可能な分散ストレージシステムにおける最小ストレージ再生成符合に基づく秘密分散法," *電子情報通信学会論文誌*, vol. J96-A, no. 4, pp. 166–174 (2013).
- [16] 小松, 塩川, "MANETにおける経路間の干渉を考慮したマルチパスルーティングプロトコル," *電子情報通信学会通信ソサイエティ大会講演論文集*, p. 477 (2011).
- [17] 山中, 宮本, 三瓶, 森永, "秘密分散法に基づくセキュアな無線通信リンク形成のための送信指向性制御パラメータに関する検討," *信学技報*, vol. 110, no. 340, pp. 221–226 (2010).