

秘密分散通信のための無線マルチホップ配送手法

金持 徹也^{1,a)} 桧垣 博章^{1,b)}

概要：無線マルチホップネットワークにおいて、配送データを分割した複数のデータメッセージ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、送信元無線ノードを除く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一括して取得しないことを実現するために、経路に含まれる各中継無線ノードの無線信号到達範囲に他の経路の中継無線ノードの隣接無線ノードを共通に含まない隣接独立な経路を検出する。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想定する。シミュレーション実験により、平均隣接無線ノード数が9.6台程度を超えると2つの隣接独立経路が90%以上に検出可能であり、このとき盗聴ノードが存在可能な領域は0.5%程度であることが示された。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。

Wireless Multihop Transmissions for Secret Sharing Communication

TETSUYA KANACHI^{1,a)} HIROAKI HIGAKI^{1,b)}

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. Simulation experiments show that availability of neighbor-disjoint two routes is 90% over in cases that each node has averagely 9.6 neighbor nodes. In addition, the ratio of areas where a node can receive data messages along multiple routes is only about 0.5%.

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が、無線マルチホップ配送経路を構成する中継無線ノードによるデータメッセージの順次転送によって実

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 [1]。有線ネットワークと無線ネットワークとで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、データメッセージ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 (傍受) される。一方、安全なネットワーク通信

¹ 東京電機大学大学院ロボット・メカトロニクス学専攻
Department of Robotics and Mechatronics, Tokyo Denki University

a) kanachi@higlab.net

b) hig@higlab.net

を実現する手法のひとつに秘密分散通信がある。ここでは、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。こうして、盗聴無線ノードが取得可能なデータメッセージを一部に限定することでデータの盗聴を困難にする。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、分割配送される複数のデータメッセージを盗聴無線ノードに一括で受信させない複数の無線マルチホップ配送経路を探索する手法が求められる。本論文では、これを実現するために求められる無線マルチホップ配送経路の隣接独立性を提案し、隣接独立な複数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。

2. 関連研究

データを盗聴によって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複数のデータ片に分割し、各データ片を個別に記憶あるいは通信する [15, 17]。このとき、すべてのデータ片あるいは定められた閾値を越える割合のデータ片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とな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ノード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 個のデータメッセージに分割し、動的に定められた異なる n 個の配送経路に沿ってデータメッセージを配送することによって、盗聴ノードがすべてもしくは閾値以上のデータメッセージ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が提案されている。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 [9] 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て検出され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ことが求められる。そこで、複数の配送経路に共通の無線リンクが含まれないリンク独立 (Link-Disjoint) な複数経路を探索、検出するルーティングプロトコル [4] (図 1) や複数の配送経路に共通の中継無線ノードが含まれないノード独立 (Node-Disjoint) な複数経路を探索、検出する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^{*1}、複数配送経路の探索に要する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の複数配送経路を構成する手法が提案されている。

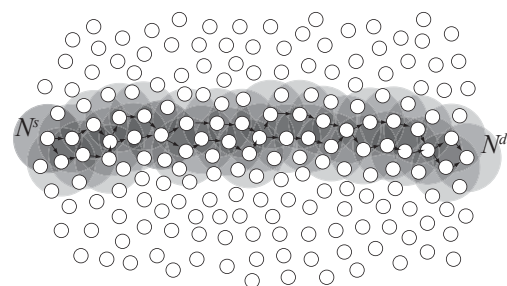


図 1 リンク独立な無線マルチホップ配送経路

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

^{*1} 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、移動と故障による切断頻度は高いことが見込まれる。一方、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。

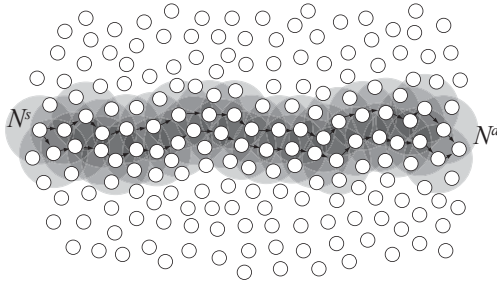


図 2 ノード独立な無線マルチホップ配送経路

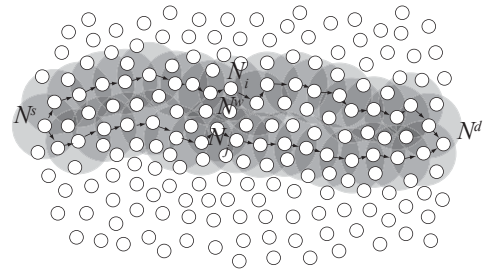


図 3 無線信号独立な無線マルチホップ複数配送経路

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メッセージを配送することでエンドエンドのスループットを向上する手法が提案されている。ここで、無線通信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データメッセージはすべての隣接無線ノードへと到達する。これを原因とする晒し端末問題と隠れ端末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、データメッセージ紛失率の上昇、データメッセージ配送遅延の延長、データメッセージ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メッセージ配送を行なう場合、 $N_i \in \mathcal{R}$ の無線信号到達範囲に $N'_j \in \mathcal{R}'$ が含まれるならば、 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} および N_{i-1} と N'_j が互いに隠れ端末となる。これによってデータメッセージ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含まない無線信号独立 (Radio-Disjoint) な複数配送経路を探索、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]。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ないことによって中継無線ノード間の晒し端末問題と隠れ端末問題の発生を回避し、データメッセージの衝突や衝突回避のための待機時間によるデータメッセージ配送遅延延長による性能低下を低減する (図 3)。

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複数のデータメッセージを盗聴無線ノードが一括して取得することを回避しなければならない。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データメッセージ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メッセージ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メッセージ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隣接無線ノードがこのデータメッセージを受信することができる。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無線ノードのいずれにおいても*2 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を一括して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 $\mathcal{R}_{(i)} = \{N_{0(i)} (= N^s) \dots N_{n_i(i)} (= N^d)\}$ 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、 $\forall N \in R(N_{j(i)})(0 < j < n_i)$ について $N \notin R(N_{j'(i')})(i \neq i', 0 < j < n_{i'})$ となる複数の

*2 送信元無線ノードと送信先無線ノードを除く。

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を隣接独立 (Neighbor-Disjoint) な無線マルチホップ配送経路と呼ぶ。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。

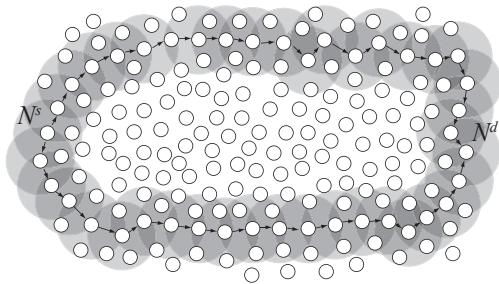


図4 隣接独立な無線マルチホップ複数配送経路

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が困難であることが考えられる。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、図5に示すように、 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安全領域内の無線ノードが共通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 $\mathcal{R}_{(i)}$ は、 $\forall N \in R(N_{i(j)}) \setminus (SZ^s \cup SZ^d) (0 < j < n_i)$ について $N \notin R(N_{j'(i')}) (i \neq i', 0 < j < n_{i'})$ 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

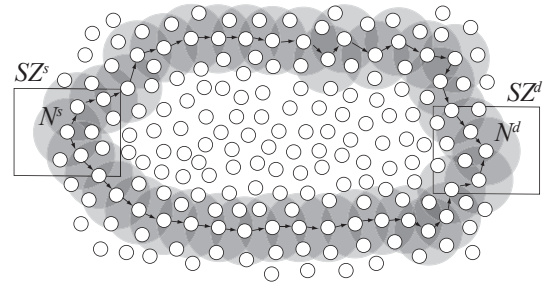


図5 安全領域間を接続する隣接独立な無線マルチホップ複数配送経路

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 [8] 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_i^n が $Rrep$ を傍受 (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_i^n 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_i^{nn} 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。

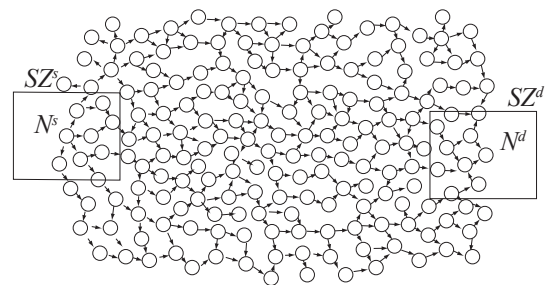


図6 $Rreq$ のフラッディングによる第1経路探索

SZ^s と SZ^d に含まれる無線ノード N については以下

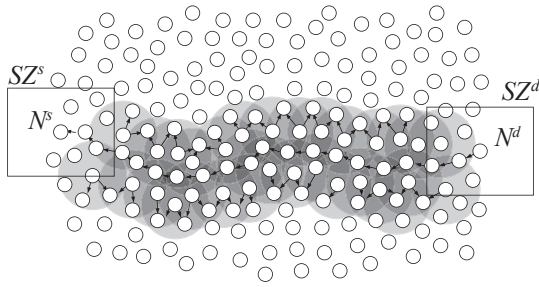


図 7 $Rrep$ と $eRrep$ による第 2 経路探索への制限

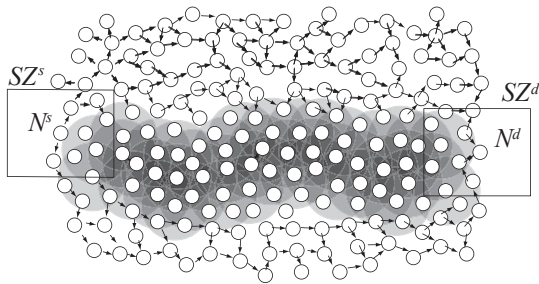


図 8 $Rreq$ のフラッディングによる第 2 経路探索

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るべきである。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。

[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 $N_{n_p-1(p)}$ 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とするとともに、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 $N_{i(p)}^n$]

- (1) 隣接無線ノード $N_{i(p)}$ 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 $N_{i(p)}^{nn}$]

- (1) 隣接無線ノード $N_{i(p)}^n$ 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一括して取得しないことを実現する。ここで、盗聴無線ノード 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。

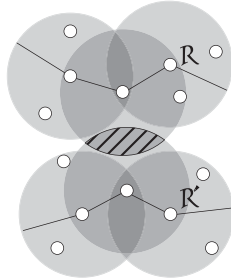


図 9 盗聴無線ノード存在可能領域

ここでは、 $1,000\text{m} \times 1,000\text{m}$ 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 台を一樣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 10 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 $0.217\text{--}1.72\%$ 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。

次に、提案プロトコルにより送信元無線ノードから送信先無線ノードまで隣接独立なふたつの無線マルチホップ配送経路を探索する場合の性能をシミュレーション実験により評価する。ここでは、 $3,000\text{m} \times 3,000\text{m}$ の正方形領域に無線信号到達距離 100m の無線ノードを一樣分布乱数によりラ

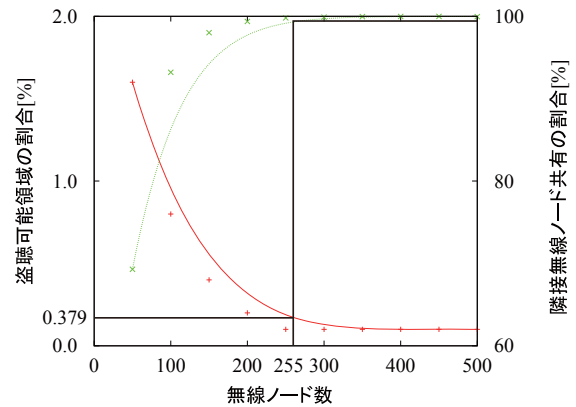


図 10 盗聴可能領域の割合

ンダムに配置する。図 11 に示すように、送信元無線ノードと送信先無線ノードを領域の対角線上、頂点から $750\sqrt{2}\text{m}$ だけ離れた位置に固定配置する。これらは、 $500\text{m} \times 500\text{m}$ の安全領域の中心に位置するものとする。無線ノード数を $1,000\text{--}10,000$ とするときの盗聴可能領域の割合と経路検出率を計測する。経路検出率については、無線信号独立およびノード独立な経路を探索する場合との比較評価を行なう。

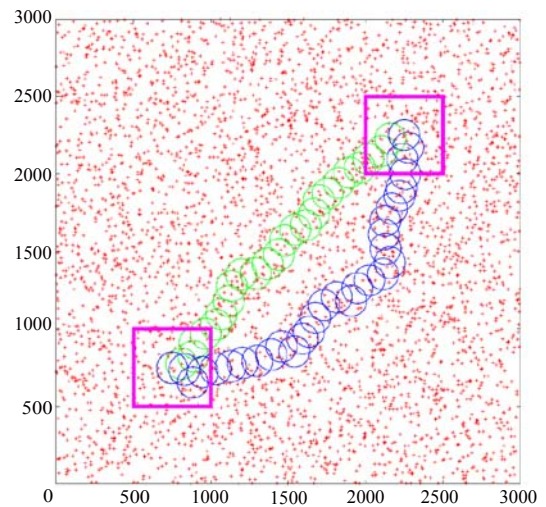


図 11 シミュレーション実験環境

図 12 に盗聴可能領域の割合を示す。シミュレーション実験でランダムに配置した無線ノードはすべて提案プロトコルに従うため、ふたつの異なる経路の中継無線ノードがこれらの無線ノードのいずれかを共通に隣接無線ノードとすることはない。ただし、提案プロトコルに従わず、例えば、制御メッセージを一切送信しないノードのみを共通の隣接無線ノードとする経路が検出されることはあり得る。このような領域の割合は、経路検出に成功する 2,800 以上の無線ノードが配置される場合においては、無線ノード数によらず 0.5% 程度である。図 10 の結果と同一ノード密度と比較するとこの測定結果はやや高めであると考えられるが、

これだけの領域に限定されるならば、盗聴無線ノードを盗聴可能領域に配置することは困難であると考えられる。

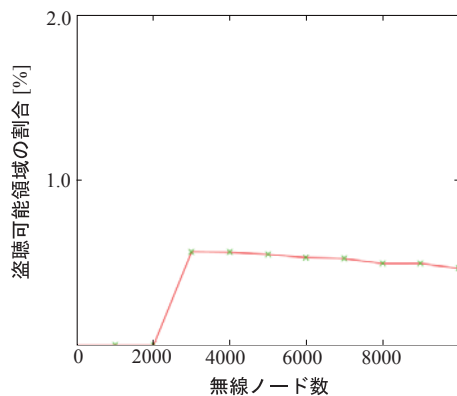


図 12 盗聴可能領域比率

図 13 には経路検出率を示す。隣接独立な複数経路は、無線信号独立およびノード独立な複数経路よりもより厳しい制約条件が課されていることから、経路検出率が低下する。他の手法では、無線ノード数が 1,500 以上で経路検出が可能となり、2,200 以上で 90% を越える経路検出率となる。一方、提案手法では、無線ノード数が 2,800 以上で経路検出が可能となり、3,000 以上で 90% を越える経路検出率となる。このように、他の手法よりも高い無線ノード分布密度となる無線マルチホップネットワークが適用対象となる。この適用対象への制約とデータメッセージ配送の安全性とはトレードオフの関係であり、適用アプリケーションの要求に応じて提案手法の適用性を評価する必要がある。

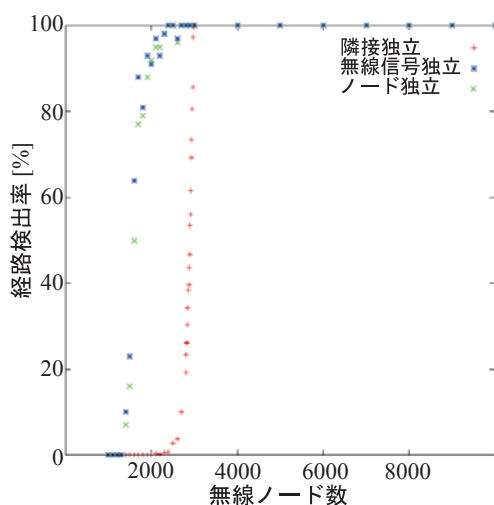


図 13 経路検出率

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、シミュレーション実験により 2 つの配送経路を検出する場合の経路検出率と盗聴可能領域比率を測定した。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。

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, Elsevier, 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] Perkins, C.E., "Ad Hoc On-Demand Distance Vector (AODV) Routing," RFC 3561 (2003).
- [9] Radi, M., Dezfouli, B., Bakar, K.A. and Lee, M., "Multipath Routing in Wireless Sensor Networks: Survey and Research Challenges," Sensors, MDPI, vol. 12, no. 1, pp. 650–685 (2012).
- [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 Sci-

- ence 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).