

推薦論文

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)}

受付日 2015年7月7日, 採録日 2016年3月4日

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うための隣接独立ルーティング手法を提案する. ここでは, 送信先無線ノードを除くすべての無線ノードがたかだか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, 無線信号到達距離 100m の無線ノードからなる無線マルチホップネットワークで約 2,100m 離れた無線ノードを接続する 2 つの隣接独立無線マルチホップ配送経路を検出した場合の盗聴可能領域は 50m^2 以下であり, 盗聴無線ノードがデータメッセージを一括受信することは困難であることが示された.

キーワード: 無線マルチホップネットワーク, 秘密分散通信, ルーティングプロトコル, 隣接独立

Wireless Multihop Transmissions for Secret Sharing Communication

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

Received: July 7, 2015, Accepted: March 4, 2016

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 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 the area where a wiretapping node receive bulk data messages along two wireless transmission routes between 2,100m apart the source and the destination nodes and the wireless transmission range of all wireless nodes is 100m is less than 50m^2 . That is, the bulk reception of data messages becomes almost impossible by our proposed protocol.

Keywords: wireless multihop network, secret sharing communication, routing protocol, neighbor disjoint

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

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, Adachi, Tokyo 120-8551, Japan

a) kanachi@higlab.net

b) hig@higlab.net

本論文の内容は 2014 年 9 月の第 161 回マルチメディア通信と分散処理研究会にて報告され, 同研究会主査により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である.

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 1 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を実現する手法の 1 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. このように, 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の 1 つに秘密分散法 [2], [14] がある (図 1). 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配送する [20], [22]. このとき, すべてのデータ片あるいは定められた閾値を超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.

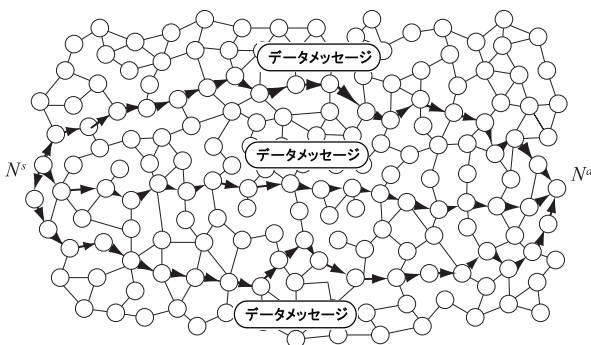


図 1 秘密分散法

Fig. 1 Information sharing.

論文 [9] 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 [19] 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. このため, 後述するように, 盗聴無線ノードの位置によって複数の経路に分割配送されるデータメッセージのすべてあるいは閾値以上のデータメッセージを入手することが考えられる.

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 [11] 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 [12].

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 [6] (図 2) 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 [7] (図 3) 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

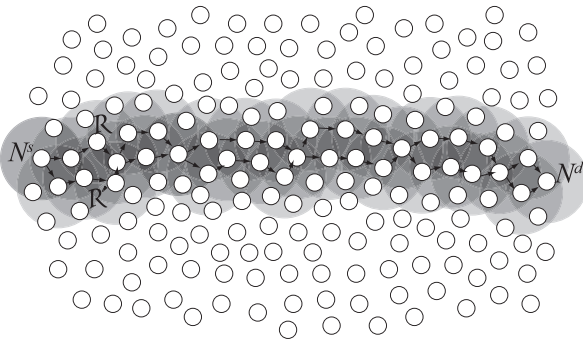


図 2 リンク独立な無線マルチホップ配送経路

Fig. 2 Link-disjoint wireless multihop transmission routes.

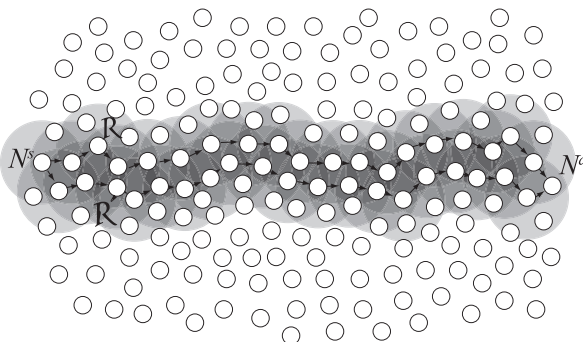


図 3 ノード独立な無線マルチホップ配送経路

Fig. 3 Node-disjoint wireless multihop transmission routes.

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メッセージ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 [4] 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．

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送信無線ノードの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う場合， $N_i \in \mathcal{R}$ の無線信号

^{*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．

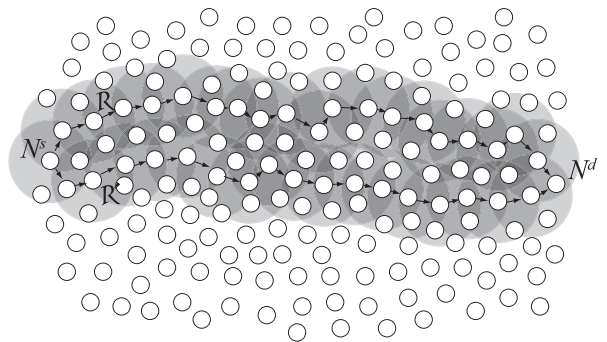


図 4 無線信号独立な無線マルチホップ配送経路

Fig. 4 Radio-disjoint wireless multihop transmission routes.

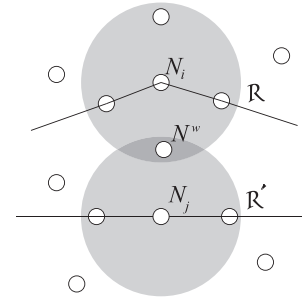


図 5 無線信号独立な複数経路の共通隣接無線ノードによる配送データメッセージの一括受信（傍受）

Fig. 5 Bulk reception of data messages by common neighbor wireless node of intermediate wireless nodes in radio-disjoint wireless multihop transmission routes.

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，エンドエンドのスループット低下を招く．

この問題を解決するために，近接する無線マルチホップ配送経路に含まれる中継無線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 [8], [18], [21]．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 4）．

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受信することを回避しなければならない．しかし，図 5 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

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 隣接独立な複数配送経路

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を用いることで実現することができる。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 $R_{(i)} = \{N_{0(i)} (= N^s) \cdots N_{n_i(i)} (= N^d)\}$ 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、 $NS.R(N)$ を $R(N)$ に含まれる無線ノードの集合とすると、 $\forall N \in NS.R(N_{j(i)}), (0 < j < n_i)$ について $N \notin NS.R(N_{j'(i')}) (i \neq i', 0 < j' < n_{i'})$ となる複数の無線マルチホップ配送経路 $R_{(i)}$ を定めるプロトコルを提案する。図 6 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 (図 7)。隣接独立な 2 つの無線マルチホップ配送経路の間では、それらの任意の中継無線ノードについて、その無線信号到達範囲が重複しないか、重複してもその重複領域に他の無線ノードが存在しないかのいずれかである。各配送経路を互いに隣接独立とすることによって、

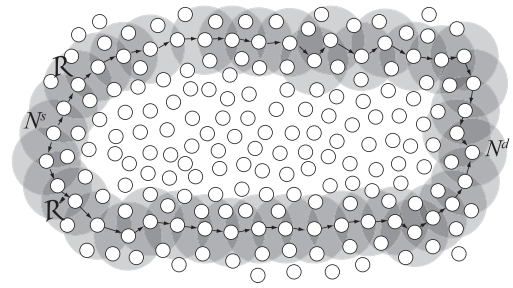


図 6 隣接独立な無線マルチホップ配送経路

Fig. 6 Neighbor-disjoint wireless multihop transmission routes.

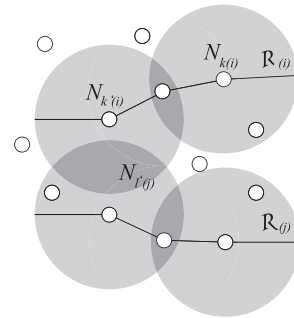


図 7 複数経路の隣接独立性

Fig. 7 Neighbor-disjoint: No common neighbor wireless nodes of intermediate wireless nodes in wireless multihop transmission routes.

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、ただか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、 $NS.R(N_{j(i)}) \cap NS.R(N_{j'(i')})$ に存在する盗聴無線ノードが本論文で提案するルーティングプロトコルに従わず、あらゆるメッセージ送信を行わずにその存在を隣接無線ノードに検出させないことによってデータメッセージを一括受信する可能性がある。このような盗聴無線ノードはメッセージを送信しないことから、他の無線ノードが検出することは不可能である。そこで、 $R(N_{j(i)}) \cap R(N_{j'(i')})$ となる領域の面積が小さいことが求められる。ただし、盗聴無線ノードが本論文で提案するルーティングプロトコルに従わない制御メッセージを送信して経路探索を妨害することや、偽装したデータメッセージを送信する攻撃は対象としない。

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。たとえば、 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 8 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

^{*2} 送信元無線ノードと送信先無線ノードを除く。

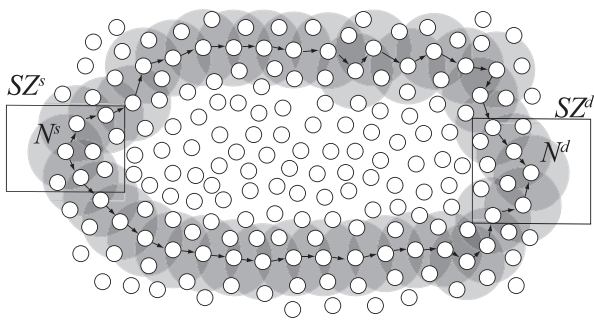


図 8 安全領域間を接続する隣接独立な無線マルチホップ配送経路
Fig. 8 Neighbor-disjoint wireless multihop transmission routes between safe zones including source and destination wireless nodes.

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、 SZ^s , SZ^d に含まれる無線ノードの集合をそれぞれ $NS.SZ^s$, $NS.SZ^d$ とするとき、 $\forall N \in NS.R(N_{i(j)}) \setminus (NS.SZ^s \cup NS.SZ^d) (0 < j < n_i)$ について $N \notin NS.R(N_{j'(i')}) (i \neq i', 0 < j' < n_{i'})$ 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1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 [10] を拡張したプロトコル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。

SZ^s と SZ^d に含まれる無線ノードについては、 N^s と N^d の近隣にあるために近接する複数経路の検出を可能とするために導入した SZ^s と SZ^d の内部には盗聴無線ノードが存在しないという条件に従って、より多くの無線ノードが p 番目の無線マルチホップ配送経路の探索に参加することが望ましい。 q 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については、その前後ホップの中継無線ノードが SZ^s と SZ^d に含まれない場合には、 p 番目に検出される無線マルチホップ配送経路の中継無線ノードとなることはできない。これは、この前後ホップの中継無線ノードがデータメッセージを一括受信可能となることを回避するためである。

また、本節では q 番目に検出した無線マルチホップ配送経路の中継無線ノードの1ホップ隣接無線ノードが $eRrep$ をブロードキャスト送信する手法を導入した。これによって、検出した無線マルチホップ配送経路の中継無線ノードの2ホップ隣接無線ノードを p 番目に検出する無線マルチホップ配送経路の中継無線ノード候補から除外する。その結果、この $eRrep$ を送信する無線ノードがデータメッセージを一括受信することを回避することができる。 SZ^s と SZ^d に含まれる無線ノードは盗聴無線ノードとはならないことから、 $Rreq$ を受信（傍受）した SZ^s または SZ^d に含まれる隣接無線ノードは $eRrep$ を送信しない。また SZ^s または SZ^d に含まれる隣接無線ノードがこれに隣接するすべての中継無線ノードが SZ^s または SZ^d に含まれる場合には、 p 番目に検出する無線マルチホップ配送経路の中継無線ノード候補にもなる。したがって、 $Rreq$ のブロードキャスト送信を行う。ただし、 SZ^s と SZ^d に含まれる無線ノードであっても、 SZ^s と SZ^d に含まれない中継無線ノードが送信した $Rrep$ もしくはそれらの1ホップ隣接無線ノードが送信した $eRrep$ を受信した場合には、この送信無線ノードによるデータメッセージの一括受信を回避するために、 p 番目に検出する無線マルチホップ配送経路の中継無線ノード候補とはならず、 $Rreq$ のブロードキャスト送信を行わない。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とする。

以上をまとめると、 q 番目の経路探索に関わった無線ノードのうち、以下の条件を満足するものは p 番目の経路探索においては $Rreq$ のフラッディングには加わらない。

- SZ^s と SZ^d に含まれない中継無線ノード。

- SZ^s と SZ^d に含まれるが、その前後ホップ中継無線ノードのいずれかが SZ^s と SZ^d に含まれない中継無線ノード.
 - SZ^s と SZ^d に含まれない中継無線ノードが送信した $Rrep$ を受信 (傍受) した 1 ホップ隣接無線ノード.
 - SZ^s と SZ^d に含まれない 1 ホップ隣接無線ノードが送信した $eRrep$ を受信した 2 ホップ隣接無線ノード.
- また, $eRrep$ を送信する 1 ホップ隣接無線ノードは, SZ^s と SZ^d に含まれないものとする.

この条件に従って構成された p 番目の無線マルチホップ配送経路を探索するプロトコルを以下に示す.

[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) 自身もしくは自身の前後ホップ中継無線ノードの少なくとも 1 つが安全領域外にある, あるいは, 隣接無線ノードのいずれかがブロードキャスト送信した $eRrep$ を受信したならば, 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.
- (2) 傍受した $Rrep$ が安全領域外にある中継無線ノードが送信したものであるならば, 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 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 $eRrep$ を受信したならば, 以降に $Rreq$ を受信してもブロードキャスト送信しない.

□

図 9～図 14 に提案プロトコルの適用例を示す. 安全領域 SZ^s に含まれる送信元無線ノード N^s から安全領域 SZ^d

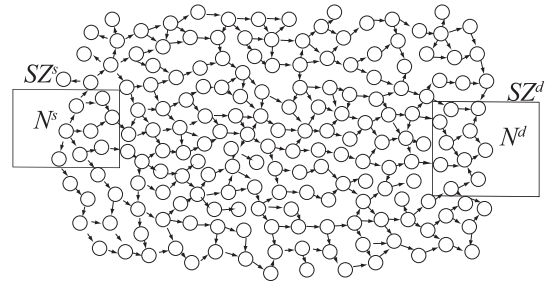


図 9 $Rreq$ のフラッディングによる第 1 経路探索
Fig. 9 Flooding of $Rreq$ for detection of 1st route.

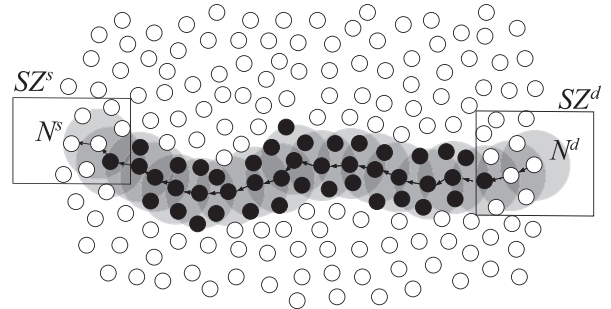


図 10 $Rrep$ のユニキャスト返送による第 2 経路探索への制限
Fig. 10 Unicast transmission of $Rrep$ for restriction on detection of 2nd route.

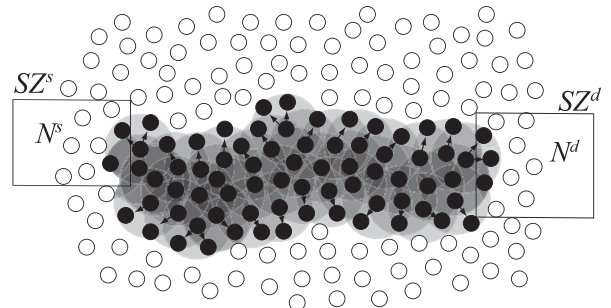


図 11 $eRrep$ のブロードキャスト送信による第 2 経路探索への制限
Fig. 11 Broadcasts of $eRrep$ for restriction on detection of 2nd route.

に含まれる送信先無線ノード N^d までの隣接独立な複数の無線マルチホップ配送経路を検出する. まず, N^s からの $Rreq$ のフラッディングによって N^s から N^d への無線マルチホップ配送経路 $\mathcal{R}_{(1)}$ を検出する (図 9). そして, 図 10 のように, $\mathcal{R}_{(1)}$ に沿って $Rrep$ をユニキャスト配送するとともに $Rrep$ を傍受した $\mathcal{R}_{(1)}$ の中継無線ノードに隣接する安全領域外の無線ノードが $eRrep$ をブロードキャスト送信する (図 11). 自身もしくはその前後ホップが安全領域外にある中継無線ノード, SZ^s と SZ^d に含まれない中継無線ノードが送信した $Rrep$ もしくは $eRrep$ を受信した無線ノードは, 以降の経路探索つまり $Rreq$ のフラッディングには参加しない. すなわち, 隣接無線ノードから $Rreq$ を受信してもこれをブロードキャスト送信しない. したがって, 次の無線マルチホップ配送経路 $\mathcal{R}_{(2)}$ の探索において

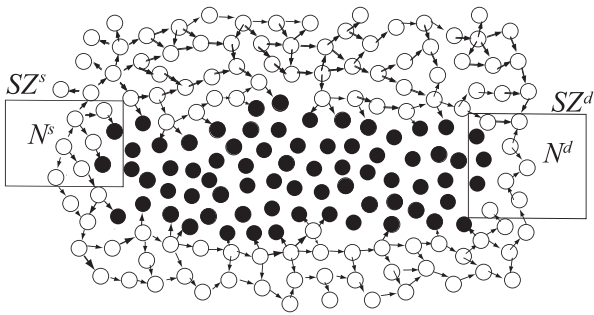


図 12 $Rreq$ のフラッディングによる第 2 経路探索

Fig. 12 Flooding of $Rreq$ for detection of 2nd route.

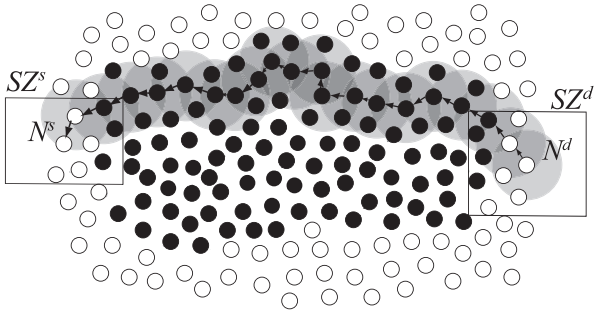


図 13 $Rrep$ のユニキャスト返送による第 3 経路探索への制限

Fig. 13 Unicast transmission of $Rrep$ for restriction on detection of 3rd route.

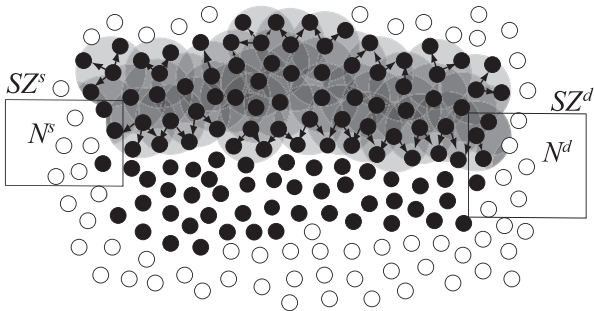


図 14 $eRrep$ のブロードキャスト送信による第 3 経路探索への制限

Fig. 14 Broadcasts of $eRrep$ for restriction on detection of 3rd route.

は、 $Rreq$ のフラッディングは図 12 のように制限される。この結果、 $\mathcal{R}_{(1)}$ とは隣接独立な無線マルチホップ配送経路 $\mathcal{R}_{(2)}$ が検出され、図 13 のように、これに沿って $Rrep$ がユニキャスト配送されるとともに、その中継無線ノードの隣接無線ノードが $eRrep$ をブロードキャスト送信することによって、さらに中継無線ノードの候補が制約される (図 14)。この制約によって隣接独立な複数の無線マルチホップ経路を検出することができる。

4. 評価

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を検出するアドホックルーティングプロトコルは、盗聴無線ノード以外の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

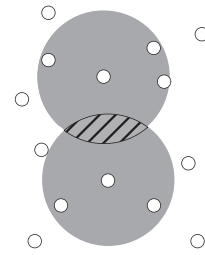


図 15 潜在的盗聴可能領域

Fig. 15 Empty overlap area of wireless transmission ranges of wireless nodes.

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受信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、自身の存在を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データメッセージを一括受信する。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 $N^w \in NS.R(N_i) \cap NS.R(N'_j)$ 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 $N \in NS.R(N_i) \cap NS.R(N'_j)$ を満足するのであれば、 $\mathcal{R}$ と $\mathcal{R}'$ がデータメッセージの同時並行配送に用いられることはない。そこで、2つの任意の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とき、この領域を潜在的盗聴可能領域と呼ぶ (図 15)。潜在的盗聴可能領域に含まれる盗聴無線ノードは N_i と N'_j が異なる無線マルチホップ配送経路の中継無線ノードとなると、データメッセージの一括受信が可能となる。ここでは、潜在的盗聴可能領域の割合を実験評価する。

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 台を一樣乱数を用いてランダムに配置し、潜在的盗聴可能領域の正方形領域に対する割合を計測する。実験結果を図 16 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単独に含まれる可能性がある領域の割合は 0.0598–1.72% 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 250 台以上では 99.0% 以上となる。論文 [13] では、無線マルチホップ配送経路を十

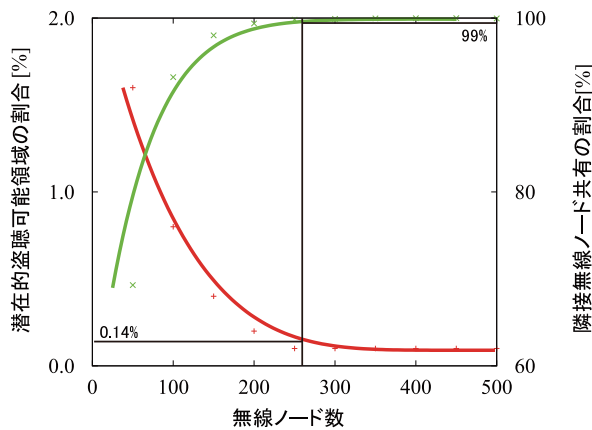


図 16 潜在的盗聴可能領域の割合

Fig. 16 Ratio of empty overlap area of two transmission ranges of wireless nodes.

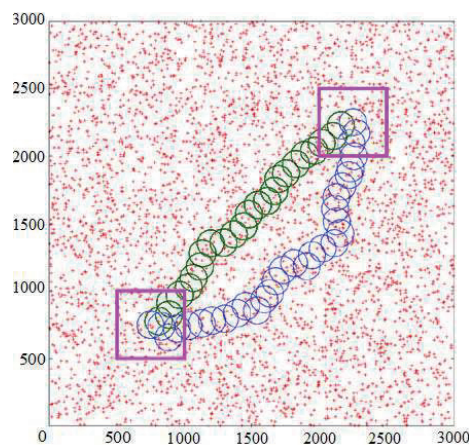


図 17 シミュレーション実験環境

Fig. 17 Setting for simulation experiments.

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、潜在的盗聴可能領域の割合は 0.14% 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、盗聴無線ノードが複数経路を配送されるデータメッセージを一括受信することは困難であると考えられる。

そこで、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 2 つの無線マルチホップ配送経路を探索する場合に異なる経路の中継無線ノードに共通の無線信号到達範囲で他の無線ノードが存在しない領域、すなわち、盗聴無線ノードが存在すればデータメッセージを一括受信できる盗聴可能領域の面積をシミュレーション実験評価する。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 100 m の無線ノードを一様分布乱数によりランダムに配置する。図 17 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

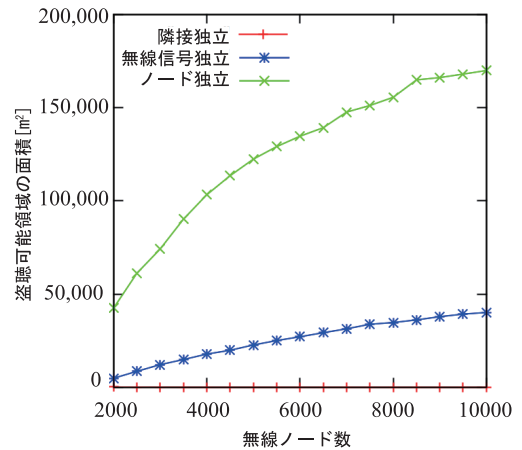


図 18 実際に盗聴可能な領域面積

Fig. 18 Area available for wiretapping wireless nodes.

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 1,000–10,000 とするときの盗聴可能領域の面積と経路検出率を計測する。各ノード数について 3,000 通りの異なる無線ノード配置による実験を行い、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う。シミュレータには NS3 を用い、無線 LAN プロトコルは IEEE802.11 を仮定した。

図 18 に盗聴可能領域の面積を示す。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、2 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、たとえば、制御メッセージをいっさい送信しない盗聴無線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うる。このような領域の面積は、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、他の複数経路探索プロトコルと比較してきわめて小さな面積となった。無線ノード数が 3,000, 4,000, 5,000 のそれぞれの場合における盗聴可能領域の面積は 47.3 m^2 , 8.24 m^2 , 5.84 m^2 であり、5,500 以上では 1 m^2 未満となった、これは無線ノードの無線信号到達範囲の面積 $31,400\text{ m}^2$ と比較しても十分に小さく、送信元無線ノードと送信先無線ノードとの間の距離 $1500\sqrt{2}\text{ m}$ に対してもきわめて狭い領域であるといえる。したがって、安全領域の配置が既知であったとしても、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いえる。

図 19 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% を超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% を超える経路検出

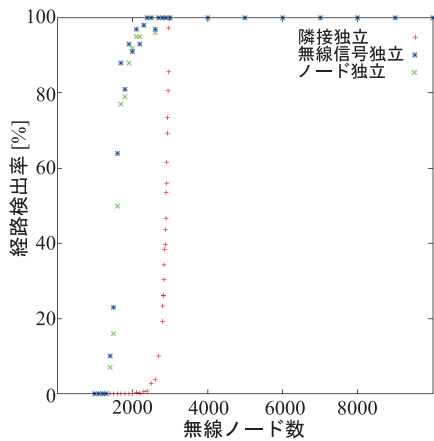


図 19 経路検出率

Fig. 19 Route detection ratio.

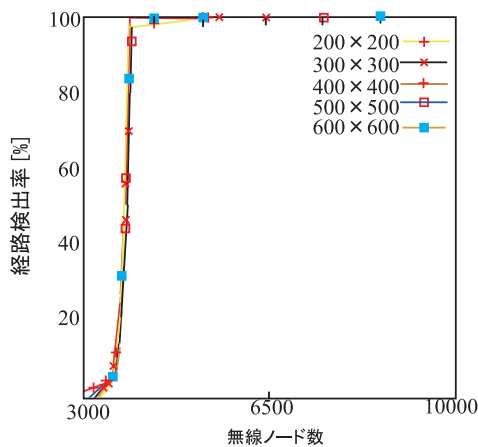


図 20 安全領域サイズの経路検出率への影響

Fig. 20 Route detection ratio with various sizes of safe zones.

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．

最後に，安全領域の大きさによる無線マルチホップ配送経路の検出率への影響を評価する．無線ノード数を2,000–10,000とし，矩形の安全領域の中心位置を前の評価実験と同一としたまま，領域の大きさを200 m×200 mから600 m×600 mまで変化させた場合における提案手法を適用した場合の2つめの経路の検出率を実験評価した結果を図 20 に示す．経路検出率は，無線ノード数に依存して単調増加するものの，安全領域の大きさにはほぼ依存しないことが分かる．複数の隣接独立な無線マルチホップ配送経路を検出する場合，安全領域が小さい場合には，特に安全領域近隣において隣接独立性を維持することが困難であることが考えられる．しかし，2つめの無線マルチホップ配送経路の検出では，図 21 と図 22 に示すように，安全領域が小さい場合には，安全領域から出る最初の中継無線ノード位置が送信先無線ノードの方向とは大きく乖離す

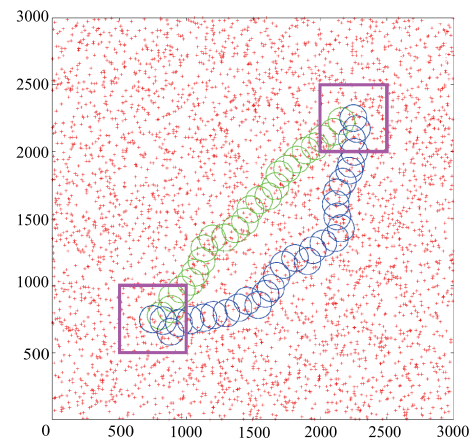


図 21 検出無線マルチホップ配送経路例 (安全領域 600 m×600 m)

Fig. 21 Example of detected wireless multihop transmission routes (600 m×600 m safe zones).

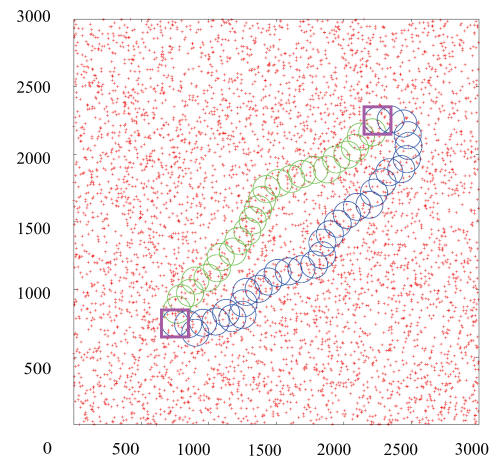


図 22 検出無線マルチホップ配送経路例 (安全領域 200 m×200 m)

Fig. 22 Example of detected wireless multihop transmission routes (200 m×200 m safe zones).

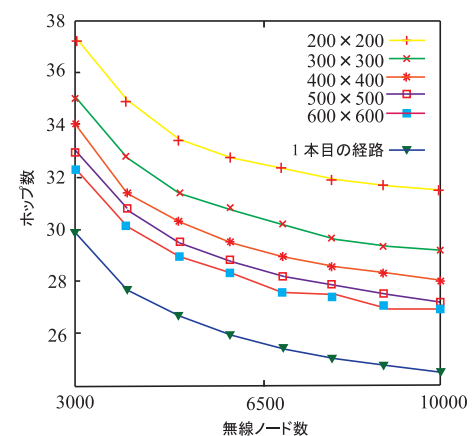


図 23 安全領域サイズの配送経路長への影響

Fig. 23 Numbers of hops of wireless multihop transmission routes with various sizes of safe zone.

るものの，迂回経路を構成することが可能であり，経路検出率の低下を回避している．ただし，迂回による経路長の延長は余儀なくされ，図 23 に示すように，安全領域が大

きいほど2つめの無線マルチホップ配送経路長が短縮している。最初に検出される無線マルチホップ配送経路長と比較すると、安全領域が600m×600mの場合には経路長の拡大率が108.4%となっているのに対して、安全領域が200m×200mの場合には経路長の拡大率が126.1%まで上昇する。結論として、経路検出率の観点からは安全領域の大きさによる影響は受けないと考えられるが、経路長の延長、特に最初に検出された無線マルチホップ配送経路と2つめの無線マルチホップ配送経路の経路長差は安全領域の大きさによる影響が大きいと、提案手法の適用にあたっては、分割データを配送するデータメッセージの配送遅延差がアプリケーションに与える影響を考慮する必要がある。

5. 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たかだか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に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、評価実験により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面積を測定した。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一括受信することは困難である。

本論文では、最初に送信先無線ノードへ到達した *Rrep* の配送経路をデータメッセージ配送経路としているが、盗聴可能領域のさらなる削減、経路ごとのデータメッセージ配送遅延差の縮小の観点から異なる経路を選択することが考えられる。また、*Rreq*, *Rrep*, *eRrep* 制御メッセージを提案プロトコルに従わず送信する攻撃無線ノードへの対応も今後の重要な課題である。

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*, Vol.55, No.13, pp.3032–3080, Elsevier (2011).
- [2] Blakley, G.R.: Safeguarding Cryptographic Keys, *Proc. National Computer Conference*, Vol.48, pp.313–317 (1979).
- [3] Fubao, Y. and Baolin, S.: Ad Hoc On-demand Distance Vector Multipath Routing Protocol with Path Selection Entropy, *Proc. 4th International Conference on Electronics, Communications and Networks*, pp.4715–4718

- (2014).
- [4] Higaki, H. and Umeshima, S.: Multiple-Route Ad Hoc On-Demand Distance Vector (MRAODV) Routing Protocol, *Proc. 18th IEEE Parallel and Distributed Processing Symposium* (2004).
- [5] Hoda, R., Marjan, K. and Hamid, S.: A New Zone Disjoint Multi Path Routing Algorithm to Increase Fault-Tolerant in Mobile Ad Hoc Networks, *Applied Mathematics & Information Sciences*, pp.433–444 (2015).
- [6] 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*, pp.649–661, Springer (2011).
- [7] Lee, S.J. and Gerla, M.: Split Multipath Routing with Maximally Disjoint Path in Ad Hoc Networks, *Proc. IEEE International Conference on Communications*, pp.3201–3205 (2001).
- [8] Maimour, M.: Maximally Radio-Disjoint Multipath Routing for Wireless Multimedia Sensor Networks, *Proc. 4th ACM Workshop on Wireless Multimedia Networking and Performance Modeling*, pp.26–31 (2008).
- [9] Ono, M. and Higaki, H.: Dynamic Multiple-Route IP Transmission for Virtual Private Network, *Proc. 4th International Conference on Communication Systems and Applications*, pp.92–97 (2004).
- [10] Perkins, C.E.: Ad Hoc On-Demand Distance Vector (AODV) Routing, RFC 3561 (2003).
- [11] 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).
- [12] 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).
- [13] Seyama, T. and Higaki, H.: G-AODV+PCMTAG: Routing in MANET with Low Overhead Flooding and Route-Shortening, *Proc. 7th International Conference on Parallel and Distributed Computing and Networks*, pp.103–110 (2008).
- [14] Shamir, A.: How to Generate and Exchange Secret, *Comm. ACM*, Vol.22, No.11, pp.612–613 (1979).
- [15] Shiwam, P. and Mohammad, A.: Efficient Multicasting using Multipath Routing Protocol in Mobile Ad Hoc Network, *Progress in Science and Engineering Research Journal*, Vol.2, pp.172–179 (2014).
- [16] Tanay, J. and Ramachandran, B.: Design and Analysis of Hybrid On-demand Node Disjoint (HOND) Multipath Routing Protocol for Mobile Ad hoc Networks, *International Journal of Engineering Development and Research*, Vol.2, No.1, pp.1171–1178 (2014).
- [17] Vivek, A. and Charu, G.: NDj-AODV: Node Disjoint Multipath Routing in Mobile Ad Hoc Networks based on AODV Protocol, *Contemporary Computing*, pp.601–606 (2014).
- [18] Waharte, S. and Boutaba, R.: Totally Disjoint Multipath Routing in Multihop Wireless Networks, *Proc. IEEE International Conference on Communications*, pp.5576–5581 (2006).
- [19] 今井啓輔, 藤井雅弘, 渡辺 裕: 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, 電子情報通信学会技術報告, Vol.108, No.205, pp.25–30 (2008).
- [20] 栗原正純, 桑門秀典: 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号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).

- [21] 小松辰成, 塩川茂樹: 経路間の干渉を考慮したマルチパスルーティングにおけるスループットの改善, 電子情報通信学会技術報告, Vol.111, No.385, pp.55–83 (2011).
- [22] 山中仁昭, 宮本伸一, 三瓶政一, 森永規彦: 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, 電子情報通信学会技術報告, Vol.110, No.340, pp.221–226 (2010).

推薦文

本論文では, 無線マルチホップネットワークにおいて, 秘密分散通信を行うためのルーティング手法を提案している. 通信範囲が重複しない複数の経路を設定することで, 盗聴の危険性を回避する点が独創的である. また, シミュレーション実験により, 盗聴の危険性がほとんどないことを示しており, 有効性も確認できている. 以上のように, 完成度の高い論文であり推薦に値する.

(マルチメディア通信と分散処理研究会主査 重野 寛)



金持 徹也 (学生会員)

平成 2 年生. 平成 26 年東京電機大学未来科学部ロボット・メカトロニクス学科卒業. 平成 28 年東京電機大学大学院未来科学研究科ロボット・メカトロニクス学専攻修了.



桧垣 博章 (正会員)

昭和 42 年生. 平成 2 年東京大学工学部計数工学科卒業. 同年日本電信電話(株)NTT ソフトウェア研究所入所. 現在, 東京電機大学未来科学部ロボット・メカトロニクス学科教授. 博士(工学). 分散システム, 通信プロトコル, フォールトトレラントネットワーク, モバイルアドホックネットワークの研究に従事. 平成 7 年情報処理学会全国大会奨励賞, 平成 9 年情報処理学会山下記念研究賞, 平成 17 年情報処理学会学会活動貢献賞. ACM, IEEE, 電子情報通信学会各会員.