Vol.2017-DPS-169 No.2
2017/1/19

盗聴データメッセージの無線マルチホップ配送を困難にすることによるアドホックネットワークの安全性向上

原嶋 勇介[1,a)]　桧垣 博章[1,b)]

概要：無線マルチホップネットワークでは, データメッセージが中継無線ノードの列である無線マルチホップ配送経路に沿って各中継無線ノードが順次転送することによって配送される. 安全な無線マルチホップ配送を実現するために暗号通信の適用は必須であるが, 小型軽量で省電力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は, 計算性能を要する高度な暗号手法を必ずしも適用できるとは限らない. そこで, データメッセージの盗聴を困難にする手法, 盗聴したデータメッセージの暗号解読用サーバコンピュータへの配送を困難にする手法とを組み合わせることによる総合的な安全性の実現が求められる. 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によるデータメッセージ送信を一定時間禁止することによって, 盗聴無線ノードが傍受したデータメッセージを配送することを困難にする手法を提案する. また, この手法によっては防ぐことのできない配送を検出し, 動的に配送を妨害する手法を組み合わせることによって, 無線マルチホップネットワークの配送性能と安全性とのトレードオフを実現することを提案する.

Interference Method for Eavesdropped Data Transmission in Wireless Multihop Networks

Yusuke HARASHIMA[1,a)]　Hiroaki HIGAKI[1,b)]

Abstract: In wireless multihop networks, data messages are transmitted along a wireless multihop transmission route consisting of a sequence of intermediate wireless nodes which contain their previous- and next-hop intermediate wireless nodes within their wireless transmission ranges. Data messages are forwarded by the intermediate wireless nodes based on broadcast transmissions of wireless signals. Hence, for secure wireless multihop transmissions of data messages cryptography is mandatory. However, for small and lightweight wireless nodes in wireless multihop networks, it is not always possible to apply highly developed encryption algorithms which require high performance calculation. Thus, combination of an appropriate encryption algorithm, a method for interfering eavesdrop and a method for interfering transmissions of data messages from a eavesdropper wireless node to a server computer for illegal decryption. This paper proposes a method for interfering transmissions of eavesdropped data messages by suspension of data messages in 1-hop and 2-hop neighbor wireless nodes of intermediate wireless nodes. Though it does not completely avoid the transmission of data messages from a eavesdropper wireless node to the server computer, an additional method to interfere a detected transmissions of data messages realizes a tradeoff between performance of the wireless multihop network and the provided security.

1. はじめに

無線マルチホップ配送は, 小型軽量でときには移動性能を備えた多数の無線ノードから構成される無線ネットワークにおいて, 各無線ノードの電力消費を抑制しつつ, 高い接続性と通信の並行性による高い性能を提供することが可能となる技術であり, 無線センサネットワーク, M2M ネットワーク, V2V ネットワークの重要な基礎技術となるものである. 送信元無線ノードから送信先無線ノードまで互いに前ホップ中継無線ノードと次ホップ中継無線ノードを無線

[1] 東京電機大学ロボット・メカトロニクス学科
Department of Robotics and Mechatronics, Tokyo Denki University, Adachi Tokyo 120–8551, Japan
[a)] harashima@higlab.net
[b)] hig@higlab.net

信号到達範囲に含む中継無線ノードの列として無線マルチホップ配送経路を構成し, 前ホップ中継無線ノードから受信したデータメッセージを次ホップ無線ノードへと送信するデータメッセージの転送を各中継無線ノードが行うことによって, データメッセージの配送が実現される. ここでは, 無線マルチホップ配送経路がルーティングプロトコルによって動的に探索, 検出されること, 各無線ノードは, 送信元無線ノード, 送信先無線ノード, 中継無線ノードのいずれにもなり得ること, 各中継無線ノードによるデータメッセージの転送が無線信号のブロードキャスト送信によってなされることから, データメッセージ配送の安全性には特別な配慮が必要である. 安全なデータメッセージ配送を実現する主要技術は暗号通信であるが, 暗号解読技術の高度化に対してより複雑で計算性能を要求するアルゴリズムの適用は, 小型軽量な多数の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は常に容易に可能であるとは限らない. 暗号通信は暗号文データを含むデータメッセージを盗聴され, 暗号解読用サーバコンピュータに配送, 収集された後に平文データや暗号化キー, 復号キーを入手されることを困難にする手法であることから, データメッセージの盗聴やその配送, 収集を困難にする手法と組み合わせることによって, 総合的な安全性を提供することを検討するべきである.

2. 関連研究

現在, ネットワークを配送されるデータを不正に取得, 使用されることを防ぐことを目的とする主要な技術はデータの暗号化である. これは, 送信元ノードで暗号化鍵データ (暗号化キー) を用いて定められたアルゴリズムによって平文データを暗号文データに変換 (暗号化) し, 送信先ノードで復号鍵データ (復号キー) を用いて定められたアルゴリズムによって暗号文データを変換 (復号) して平文データを得るものである. ここで, 暗号文データから平文データを取得することや, 暗号文データの集合から暗号化キーあるいは復号キーを取得することは, 計算量的に困難, すなわち, 計算時間的に現実的ではないように設計されたアルゴリズムが用いられている. しかし, 高い計算性能を備えたコンピュータが安価に入手可能であり, それらを協調動作させる並列処理技術の高度化とその普及により, 盗聴により取得した暗号文データ (の集合) から平文データ (の集合) あるいは暗号化キー, 復号キーを取得することが現実的となり [14], よりデータの不正取得を困難とする暗号化/復号アルゴリズムの開発が必要となっている.

一方, CPU やメモリ等の小型軽量化, 省電力化と無線通信モジュールの小型軽量化, 省電力化, 高性能化により, あらゆる「モノ」にコンピュータが備えられ, それらがネットワーク接続されるユビキタスコンピューティング/ネットワーキングが指向され, 「モノ」が取得, 計算したデータを相互に交換する IoT (Internet of Things) 技術の高度化が目指されている. 環境情報を取得する種々のセンサを備えたセンサノードが取得したデータを無線ネットワークを介して交換, 収集し, 計算結果をユーザに情報提供したり, 種々のアクチュエータ (各種ロボット等を含む) の動作に反映させたりする. センサネットワーク [10] や M2M (Machine-to-Machine) [2], V2V (Vehicle-to-Vehicle) [6] 等の通信形態を基礎としたネットワークの構成技術が活発に研究されている. このようなシステムの構成要素には移動性を備えたものも考えられ, 小型軽量かつ省電力であることが求められる. また, 多種多様な「モノ」に計算, 通信機能を備えさせるためには, 個々の無線ノードは必ずしも十分に高い計算性能と通信性能とを備えていないことを前提にすることが必要である. そのため, より多くの計算量を要するデータメッセージの暗号化手法をすべての無線ノードにおいて適用することは困難である.

送信元無線ノードで平文データを暗号化キーによって変換して作られた暗号文データを無線ネットワークによって配送し, 送信先無線ノードで対応する復号キーで平文データに戻す暗号無線通信手法は, たとえ中継無線ノードや隣接無線ノードなどの他の無線ノードによって暗号文データが取得されたとしても, そこから容易には平文データが取得できないという暗号アルゴリズムの頑強性を根拠としているが, 暗号解読に用いられるコンピュータの計算能力の向上とユビキタスネットワークを構成する無線ノードの小型軽量化と省電力化への要求との間で適用性に問題を生じつつある. これは, 暗号化データを含むデータメッセージが盗聴無線ノードによって取得され, 解読に用いられるコンピュータへと収集されることを前提としていることによると考えられる. そこで, 盗聴無線ノードによって配送されるデータメッセージが取得されることそのものを困難にする手法との組み合わせによって安全性を高める方法が検討され始めている. 特に, 無線アドホックネットワークでは, 各無線ノードは自身の無線信号到達範囲に含まれる隣接無線ノードとデータメッセージの交換を行うが, このデータメッセージを運ぶ無線信号は無線信号到達範囲にブロードキャスト送信されるため, この範囲に含まれるすべての無線ノードは盗聴無線ノードも含めてこの無線信号を受信 (傍受) し, データメッセージを取得することが可能である. また, 送信元無線ノードから送信先無線ノードまでを接続する無線マルチホップ配送経路は, 互いに物理的に隣接する前ホップ中継無線ノードと次ホップ中継無線ノードとの間でデータメッセージの転送を行う中継無線ノードの列によって構成され, これらは AODV [7] などのアドホックルーティングプロトコルによって動的に構成される. そのため, 盗聴無線ノードが中継無線ノードやその隣接無線ノードになると, 配送されるデータメッセージをその中継や転送の傍受によって容易に取得することが可能である.

データメッセージのルーティングに介入し, 盗聴無線ノードが送信先無線ノードや中継無線ノードを偽ってデータメッセージを収集する攻撃手法はブラックホールノード手法と呼ばれ, 様々な対応手法が提案されてきている [11].

これに対し, 盗聴無線ノードの物理的な位置あるいは隣接関係によって定まる論理的な位置を取得した上で, 盗聴無線ノードによるデータメッセージの傍受を防ぐアドホックルーティングを行う手法として avoidance routing が提案されており, さらに, 複数の無線マルチホップ配送経路を用いてデータメッセージ群を分割配送する multipath avoidance routing 手法 [8] も考案されている. ここでは, 盗聴無線ノードの位置情報を用いて盗聴困難な無線マルチホップ配送経路を構成しているが, 一般的に盗聴無線ノードは無線信号を可能な限り送信しないことで自身の位置を明らかにしないのみならず, その存在をも明らかにしないことが考えられる. 論文 [13] では, 盗聴無線ノード位置が不明であることを前提に, 複数の無線マルチホップ配送経路を用いてデータメッセージ群を分割して配送する際に, 単独の盗聴無線ノードが取得可能なデータメッセージを限定するルーティング手法を提案している. また, 論文 [4] では, 指向性アンテナと受信無線信号から既知のノイズ無線信号を除去する信号処理を用いて, 送信無線ノードがデータメッセージを運ぶ無線信号を送信するのと並行して受信無線ノードがノイズ無線信号を送信することによって隣接する盗聴無線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している. ただし, ネットワークを構成するすべての無線ノードが送信元無線ノード, 送信先無線ノード, 中継無線ノードのいずれにもなり得る無線マルチホップネットワークでは, すべての無線ノードが特別なハードウェアを備えることを前提とする方法は適用性が高くはないという問題があると考えられる. 論文 [9] では, 無線マルチホップ配送経路の中継無線ノードの無線信号到達範囲内にあ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困難にするために, データメッセージを転送する中継無線ノードの 1 ホップおよび 2 ホップ隣接無線ノードのうち次ホップ中継無線ノードの無線信号到達範囲に含まれない無線ノードがノイズ無線信号を送信する手法を提案している. このように, 取得されたデータメッセージ群に含まれる暗号文メッセージの解読を困難にする暗号通信技術に加えて, 配送されるデータメッセージの盗聴無線ノードによる取得を組み合わせることによって, 小型軽量化が求められる無線ノードによる無線マルチホップ配送を基盤とする無線マルチホップネットワークにおける安全性の改善が試みられている.

3. 提案手法

3.1 問題点

前章で述べたように, これまで無線マルチホップネットワークにおける配送データの不正な取得, 使用を防ぐ手法として検討, 適用されてきたのは, データの暗号通信技術であった. しかし, 暗号通信技術は, データの不正取得, 使用を試みる者が取得済みの暗号文データから平文データの不正取得を困難にする手法であり, 平文データの不正取得, 使用をより困難とするためのより計算量を要求する高度なアルゴリズムの開発, 適用は, 多数の必ずしも高い計算性能を備えないデバイス (ノード) で構成されるユビキタスネットワーク環境とは整合するものではない. そこで, 無線マルチホップネットワークを配送される暗号文データの取得を困難にする手法がいくつか提案されていることを前章で述べたが, 平文データの不正な取得と使用のプロセスを改めて検討すると以下の 3 つのステップで構成されることがわかる.

(1) 無線マルチホップ配送経路を配送される暗号文データの取得 (盗聴)
(2) 取得した暗号文データの配送/収集
(3) 暗号文データから平文データ, 暗号化キー, 復号キーの取得 (解読)

すなわち, これらのそれぞれのステップにおいて, 平文データの不正な取得と使用を困難にするための諸手法を考案し, 総合的に安全性を高めることが必要である. そこで, 本論文では, 無線マルチホップ配送される暗号文データを盗聴ノードによって取得された後にこれを配送, 収集することを困難にする手法を検討する. 無線マルチホップ配送における各中継無線ノードは, 前ホップ中継無線ノードから受信したデータメッセージを次ホップ中継無線ノードに転送する. このデータメッセージの転送は, データメッセージを運ぶ無線信号を中継無線ノードの無線信号到達範囲にブロードキャスト送信することによって行われる. したがって, 中継無線ノードの次ホップ中継無線ノードは必ず中継無線ノードの無線信号到達範囲に含まれていなければならない. 同時に, 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受信 (傍受) することができる. このため, 盗聴無線ノードが中継無線ノードの無線信号到達範囲内に位置するならば, この中継無線ノードによって転送されるすべてのデータメッセージを傍受することが可能である. このとき, 論文 [9, 13] において著者らが論じているように, 盗聴無線ノードが一切の無線信号を送信することがなければ, 他のいかなる無線ノードも転送されたデータメッセージを傍受されたことのみならず, この盗聴無線ノードが存在することをも検出することができない. したがって, もしこの盗聴無線ノードが移動性能を備えているならば, 送受信される無線信号のみではこの盗聴無線ノードが取得したデータメッセージを配送 (運搬) することを妨害することは不可能であり, 移動盗聴無線ノードを検出する別のデバイスを要することから, 本論文ではこの問題は対象とはしない.

移動性能を備えない盗聴無線ノードは, 傍受したデータメッセージ群を暗号解読用サーバコンピュータへと配送する必要があり, この暗号解読用サーバコンピュータは対象の無線マルチホップネットワークの外部に存在するのが一般的である. したがって, 盗聴無線ノードの目標は, 傍受したデータメッセージ群を無線マルチホップ配送によっていずれかの無線基地局へと配送することとなる. そこで, 無線基地局において傍受したデータメッセージ群を通過させない手法の適用が考えられるが, 転送を要求されたメッセージに盗聴無線ノードによって傍受されたデータメッセージが含まれていることを無線基地局で特定することは難しい. 一方, 傍受されたデータメッセージ群が無線基地局を通して外部ネットワークへと配送されることを阻止するために, すべての無線基地局におけるデータメッセージの転送を一時的に停止することも考えられるが, 他のデータメッセージの正当な配送をも一時停止させることとなり, 適切な解決策であるとはいえない. つまり, 傍受されたデータメッセージの配送を妨害あるいは阻止する手法においては, 一時的な通信の停止が必要になる場合であっても他の無線ノード対間あるいは無線ノードと無線基地局との間のデータメッセージの無線マルチホップ配送への影響, すなわち, 性能低下を極力小さくすることが必要である.

3.2 無線信号送信規制による盗聴無線ノードの検出

無線マルチホップ配送経路に沿って配送されるデータメッセージが盗聴無線ノードに傍受されるのは, 盗聴無線ノードがいずれかの中継無線ノードの無線信号到達範囲に含まれる場合, すなわち, 中継無線ノードの 1 ホップ隣接無線ノードである場合に限られる. 盗聴無線ノードを含むすべての無線ノードが送信する無線信号がユニットディスクモデル [12] にしたがって送信無線ノードを中心とした同一半径の円周とその内部に伝播するならば, 傍受されたデータメッセージを転送した中継無線ノードは盗聴無線ノードの無線信号到達範囲に必ず含まれることから, 盗聴無線ノードによる傍受データメッセージの転送を検出することができる (図 1). また, 中継無線ノードが次ホップ中継無線ノード以外の隣接無線ノードにデータメッセージを送信することも, この中継無線ノードの次ホップ中継無線ノードおよび前ホップ中継無線ノードが無線信号到達範囲に含まれることにより検出が可能である. すなわち, データメッセージ群の無線マルチホップ配送を行う時間およびその後の一定時間において, 中継無線ノードには次ホップ中継無線ノードへのデータメッセージ転送のみを可とし, 中継無線ノードが他の隣接無線ノードにデータメッセージを転送すること, 中継無線ノードの 1 ホップ隣接無線ノードがその隣接無線ノードにデータメッセージを転送することを禁止することにより, このような転送が発生した場合にはいずれかの中継無線ノードが検出することができる.

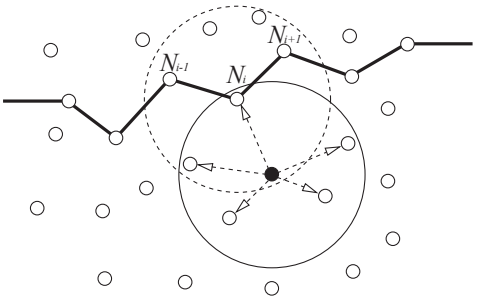

図 1 中継無線ノードによる盗聴無線ノードの検出.

しかし, 論文 [1, 15] 等で述べられているように, 盗聴無線ノードがいずれの中継無線ノードをも無線信号到達範囲に含まないように無線信号到達範囲を縮小して, すなわち, 適切に低下させた送信電力によって傍受したデータメッセージを送信することによって, 中継無線ノードに検出されることなくデータメッセージを中継無線ノードに隣接しない無線ノードへ転送することができる (図 2). これによって, 以降は通常の無線マルチホップ配送を用いることにより, 盗聴無線ノードが傍受したデータメッセージ群をいずれかの無線基地局へと配送することが可能となる. このようなデータメッセージの転送は, 禁止されたデータメッセージの送信を中継無線ノードのみではなく中継無線ノードの 1 ホップ隣接無線ノードも行うことにより, より困難にすることができる. ただし, 中継無線ノードおよびその 1 ホップ隣接無線ノードを無線信号到達範囲に含まないように縮小した電力でいずれかの他の無線ノードを無線信号到達範囲に含むことができれば, 盗聴無線ノードは結託することなく単独で傍受したデータメッセージ群を無線基地局へ無線マルチホップ配送することが可能である. また, この手法では, 盗聴無線ノードによる傍受データメッセージ群の不正な転送を検出することが可能な場合でも, それを妨害あるいは阻止することはできない.

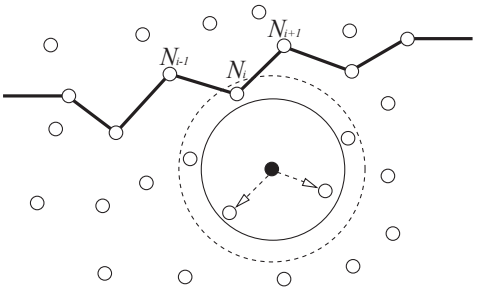

図 2 盗聴無線ノードの無線信号到達範囲縮小による傍受データメッセージの無線マルチホップ配送.

この問題を解決する手法として, 中継無線ノードの 2 ホップ隣接無線ノードによるデータメッセージ転送も一定時間禁止する手法を提案する. 盗聴無線ノードはデータメッ

セージ群を傍受可能な中継無線ノードの無線信号到達範囲に含まれることから中継無線ノードの 1 ホップ隣接無線ノードであり, かつその隣接無線ノードは中継無線ノードの 2 ホップ隣接無線ノードであることから, 中継無線ノード, 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データメッセージ転送を一定時間禁止することによって, 盗聴無線ノードを検出するとともに, 傍受されたデータメッセージ群がいずれかの無線基地局に無線マルチホップ配送されることを防ぐことができる (図 3). この盗聴無線ノードによる不正なデータメッセージ転送はそのすべての隣接無線ノードが検出することから, 盗聴無線ノードが移動性能を備えていない場合には, 盗聴無線ノードから送信されるあらゆるデータメッセージを転送しないことによって傍受されたデータメッセージがいずれかの無線基地局へ無線マルチホップ配送されることもないし, 盗聴無線ノードから送信されるあらゆる制御メッセージをも処理しないことによって, 盗聴無線ノードを中継無線ノードとする無線マルチホップ配送経路を構成することもない.

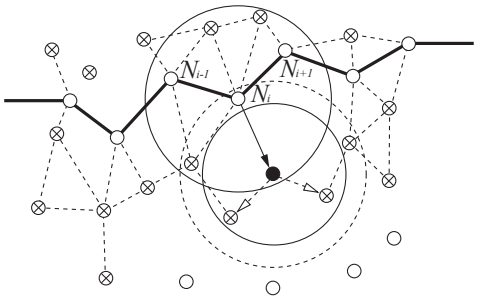

図 3 2 ホップ隣接無線ノードのデータメッセージ転送禁止による傍受データメッセージ配送の阻止.

この中継無線ノードの 1 ホップおよび 2 ホップ隣接無線ノードのデータメッセージ転送を一定期間禁止するためのプロトコルは, AODV[7] 等のフラッディングに基づくアドホックルーティングプロトコルを拡張することによって実現できる. フラッディングによって経路探索要求メッセージ *Rreq* のひとつが送信元無線ノード N^s から送信先無線ノード N^d へ到達すると, その配送経路 $R = ||N_0(= N^s) \ldots N_n(= N_d))\rangle\rangle$ が検出されたことになる. このとき, 各中継無線ノード N_i のルーティングテーブルには, N_s への次ホップ隣接無線ノードとして N_{i-1} が記録されていることから, N_s を宛先とする経路探索応答メッセージ *Rrep* を N_d から N_s へ R に沿って逆方向に無線マルチホップ配送できる. 各中継無線ノード N_i は N_{i+1} から *Rrep* メッセージを受信することによって N_d への次ホップ隣接無線ノードが N_{i+1} であることを検出し, これをルーティングテーブルに記録するとともに, *Rrep* をルーティングテーブルにしたがって N_{i-1} へ転送する. この *Rrep* メッセージは, N_i の無線信号到達範囲にブロードキャスト送信されるため, N_i のすべての 1 ホップ隣接無線ノードが傍受する.

中継無線ノードの 2 ホップ隣接無線ノードにデータメッセージ転送の一定時間の禁止を通知するためには, *Rrep* メッセージを傍受した 1 ホップ隣接無線ノードからの制御メッセージ送信が必要である. そこで, 中継無線ノードの 1 ホップ隣接無線ノードは, 最初の *Rrep* メッセージ受信に対応して[*1]データ送信一時停止要求メッセージ *TSreq* をブロードキャスト送信する. *Rrep* メッセージを傍受せずに *TSreq* を受信する無線ノードは R の中継無線ノードの 2 ホップ隣接無線ノードである (図 4).

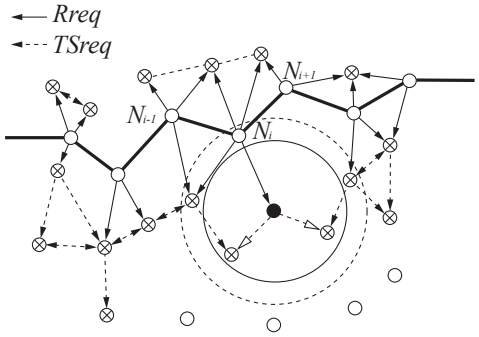

図 4 2 ホップ隣接無線ノードのデータメッセージ転送を禁止するプロトコル.

3.3 動的な無線信号送信規制の拡大

前節では, 無線マルチホップ配送経路の中継無線ノードの 1 ホップおよび 2 ホップ隣接無線ノードがデータメッセージを転送することを禁止することによって, 盗聴無線ノードが傍受したデータメッセージ群をいずれかの無線基地局まで無線マルチホップ配送することを防ぐことができることを述べた. ただし, ここでは中継無線ノードのすべての 1 ホップ隣接無線ノードが *TSreq* メッセージをブロードキャスト送信することが前提となっている. 盗聴無線ノードは, 自身の存在を隣接無線ノードに検出されないようにするためにデータメッセージも制御メッセージも送信しないことが一般的であり, また, 傍受したデータメッセージ群の無線基地局への無線マルチホップ配送経路を構成することを困難にする *TSreq* メッセージの送信も行わないことが考えられる. 次章のシミュレーション実験評価結果に示すように, 中継無線ノードの 2 ホップ隣接無線ノードは複数の 1 ホップ隣接無線ノードに隣接することが多いため, 盗聴無線ノードが *TSreq* メッセージを送信しない場合でも, この盗聴無線ノードの隣接無線ノードである中継無線ノードの 2 ホップ隣接無線ノードの多くが他の 1 ホップ隣接無線ノードがブロードキャスト送信する *TSreq* メッセージ

[*1] 中継無線ノードの 1 ホップ隣接無線ノードは複数の中継無線ノードに隣接する場合が多い. このとき, 複数の *Rrep* メッセージを傍受する.

を受信する (図 5). しかし, 盗聴無線ノードが隣接する唯一の中継無線ノードの 1 ホップ隣接無線ノードである中継無線ノードの 2 ホップ隣接無線ノードでは, この 2 ホップ隣接無線ノードにはデータメッセージ送信の一定時間の禁止を通知することができない. そのため, 盗聴無線ノードからこの 2 ホップ隣接無線ノードを中継無線ノードとしていずれかの無線基地局への無線マルチホップ配送経路が構成され, 傍受したデータメッセージ群が無線マルチホップ配送されてしまう問題がある (図 6).

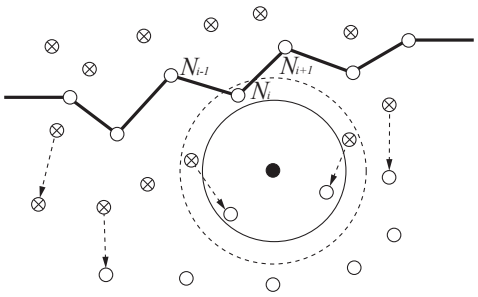

図 5 周囲の 1 ホップ隣接無線ノードからの *TSreq* メッセージの受信.

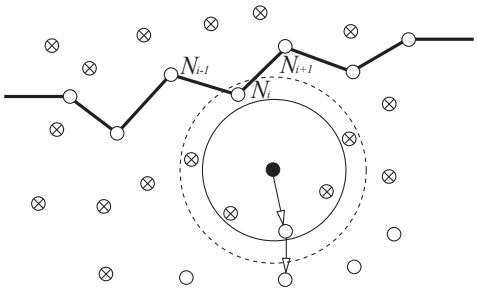

図 6 盗聴無線ノードから無線基地局への傍受データメッセージの無線マルチホップ配送.

このような盗聴無線ノードから無線基地局への無線マルチホップ配送経路を用いた傍受データメッセージ群の配送は, 以下の事象によって検出される可能性がある.

- 盗聴無線ノードが送信する *Rreq* メッセージの中継無線ノードによる受信.
- 盗聴無線ノードからフラッディングが開始された *Rreq* メッセージの中継無線ノードの 2 ホップ隣接無線ノードによる受信 (図 7).
- 盗聴無線ノードに隣接する中継無線ノードの 2 ホップ隣接無線ノード[*2]が送信する *Rreq* メッセージの隣接無線ノードによる受信.
- 盗聴無線ノードに隣接する中継無線ノードの 2 ホップ隣接無線ノードが送信する *Rrep* メッセージの隣接無線ノードによる受信.
- 盗聴無線ノードが送信するデータメッセージの中継無線ノードによる受信.
- 盗聴無線ノードに隣接する中継無線ノードの 2 ホップ隣接無線ノード[*3]が転送するデータメッセージの隣接無線ノードによる受信.
- 盗聴無線ノードに隣接する中継無線ノードの 2 ホップ隣接無線ノードが返送する受信確認メッセージ *Ack* の隣接無線ノードによる受信.

このようなメッセージの受信により傍受データメッセージ群の無線マルチホップ配送を検出した場合には, この配送を行なう中継無線ノードによるデータメッセージ転送を一定時間禁止することが必要である. 盗聴無線ノードの次ホップ中継無線ノードが送信するメッセージを受信することによって検出した場合には, その検出無線ノードが *TSreq* メッセージをこの無線ノードに転送することによってデータメッセージ送信の一定時間の禁止を通知することができる. その他のメッセージ受信によって検出した場合には, データメッセージ送信の一定時間の禁止が通知されている中継無線ノードの 1 ホップおよび 2 ホップ隣接無線ノードと盗聴無線ノードの次ホップ中継無線ノードとが隣接しておらず, *TSreq* メッセージをこの無線ノードに配送することができるとは限らない. そこで, 図に示すように, 盗聴無線ノードからいずれかの無線基地局への無線マルチホップ配送経路と交差する無線マルチホップ配送経路を構成し, この 1 ホップおよび 2 ホップ隣接無線ノードのデータメッセージ配送をも一定時間禁止することとする. この追加経路は, 盗聴無線ノードの隣接無線ノードの k ホップ前後の中継無線ノードの 2 ホップ隣接無線ノードを互いに接続する無線マルチホップ配送経路とする. このとき, データメッセージ送信が一定時間禁止される無線ノードを少なくするためには k を小さくすることが求められるが, 盗聴無線ノードが複数の中継無線ノードに隣接することが考えられることから, 追加経路が確実に盗聴無線ノードから無線基地局への無線マルチホップ配送経路と交差するためには, k はある程度大きくしなければならない.

4. 評価

本章では, 3.3 節で述べたように, 盗聴無線ノードが *TSreq* メッセージのブロードキャスト送信を行わないことによって, 本来 *TSreq* を受信することでデータメッセージの転送を行わない中継無線ノードの 2 ホップ隣接無線ノードであるにもかかわらず, 盗聴無線ノードが送信する経路探索要求メッセージ *Rreq*, 経路探索応答メッセージ *Rrep*, 盗聴無線ノードが傍受したデータメッセージを含むデータメッセージを送受信する無線ノードがどの程度存在するかをシ

[*2] この無線ノードは *TSreq* メッセージを受信していない.

[*3] この無線ノードは無線基地局への無線マルチホップ配送経路における盗聴無線ノードの次ホップ中継無線ノードである.

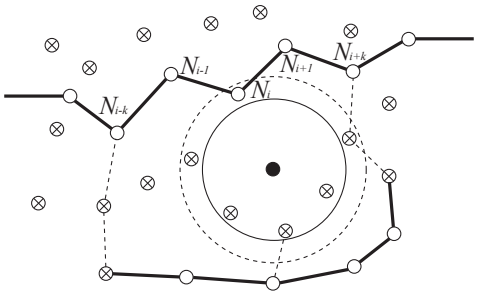

図 7 追加無線マルチホップ配送経路の構成による傍受データメッセージ配送経路の切断.

ミュレーション実験評価する. ここでは, 一様分布乱数によりランダムに配置した無線ノード群に対して, 送信元無線ノードから送信先無線ノードまでの無線マルチホップ配送経路を構成し, その中継無線ノードから 3 ホップ以上離れている無線ノードの無線信号到達範囲と中継無線ノードの無線信号到達範囲とが重複する領域の大きさを評価する. 提案するプロトコルでは, 中継無線ノードから 3 ホップ以上離れている無線ノードは, 中継無線ノードが送信する *Rrep* メッセージを傍受することもなく, 中継無線ノードの 1 ホップ隣接無線ノードがブロードキャスト送信するデータメッセージ送信の一定時間禁止を通知する *TSreq* メッセージを受信することもないが, この重複領域に盗聴無線ノードが存在するならば, この盗聴無線ノードは中継無線ノードの無線信号到達範囲に含まれることから無線マルチホップ配送経路を配送されるデータメッセージを傍受することが可能であると同時に, 中継無線ノードから 3 ホップ以上離れている無線ノードの無線信号到達範囲に含まれることから, この無線ノードを次ホップ隣接無線ノードとする無線マルチホップ配送経路を構成して傍受したデータメッセージをいずれかの無線基地局へ無線マルチホップ配送することが可能である.

ここでは, シミュレーション実験領域を 1,000×1,000m の正方形領域とし, ひとつの頂点を原点, 原点を通る 2 つの領域境界線をそれぞれ x 軸, y 軸とするとき, 送信元無線ノード, 送信先無線ノードの座標をそれぞれ (200m, 200m), (800m, 800m) で固定とする. これらを含むすべての無線ノードの無線信号到達距離を 100m で固定とし, 200–1,000 台の無線ノードを一様分布乱数を用いてランダムに配置する. 図に示すような提案手法によって無線マルチホップ配送経路の探索とデータメッセージ送信一定時間禁止の通知を行った後の中継無線ノードの無線信号到達範囲とすべての中継無線ノードから 3 ホップ以上離れた無線ノードの無線信号到達範囲との重複領域の面積を評価した結果を図に示す. 盗聴無線ノードによる傍受データメッセージの転送可能領域は, 無線ノード数の増加とともに単調に減少している. これは, 無線ノードの分布密度が高い状況では中継無線ノードとその 1 ホップおよび 2 ホップ隣接無線ノードの無線信号到達領域による被覆領域が大きくなることから, 対象領域の面積が縮小することによるものである. ただし, 本シミュレーション実験で対象とした無線ノード数では, 無線マルチホップ配送経路が 90%以上の確率で検出されることから, 盗聴無線ノードによる傍受データメッセージの無線マルチホップ配送をより困難とすることが必要である. 図に示す例でも分かるように, 無線ノードが比較的密に分布する領域では 3.2 節で述べた 2 ホップ隣接無線ノードまでの一定時間のデータメッセージ送信禁止によって傍受データメッセージの配送を阻止することができるものの, 局所的に無線ノードの分布密度が低い領域においては 3.3 節で述べた動的にデータメッセージの無線マルチホップ配送を遮断する方法を適用することが必要であると考えられる.

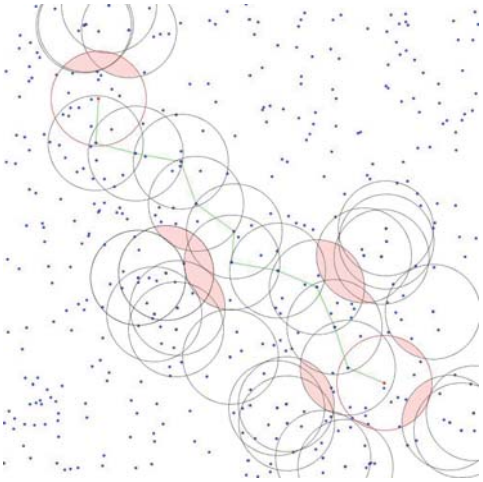

図 8 盗聴無線ノードによる傍受データメッセージの転送可能領域 .

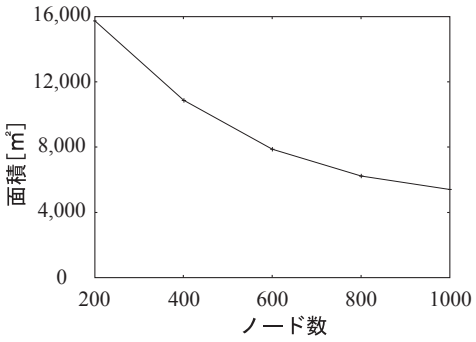

図 9 盗聴無線ノードによる傍受データメッセージの転送可能領域面積.

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, 盗聴無線ノードが中継無線ノードから傍受したデータメッセージ群を暗号解読用サーバコンピュータへ配送するためにいずれかの無線基地局まで無線マルチホップ配送することを困難にする手法を提案した. 無線マルチホップ配送経

路の 1 ホップおよび 2 ホップ隣接無線ノードに対して一定時間データメッセージの送信を禁止することにより, 多くの場合, 盗聴無線ノードによる傍受したデータメッセージを無線マルチホップ配送を試みてもデータメッセージを無線基地局に到達させることはできず, この盗聴無線ノードを隣接無線ノードが検出することができる. ただし, 局所的に無線ノード分布密度が低い領域では, 盗聴無線ノードが提案するルーティングプロトコルの制御メッセージ送信を行わないことによって, 傍受データメッセージを無線マルチホップ配送する無線基地局までの経路を構成することが可能である. 無線マルチホップネットワーク全体の性能とのトレードオフから, この問題に対しては動的に経路を遮断する手法を提案した. これを実現する具体的な手順を構成することが今後の課題である.

参考文献

[1] Balakrishnan, K., Deng, D. and Varshney, P., “TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks,” Proceedings of the Wireless Communication and Networking Conference, vol. 4, pp. 2137–2142 (2005).
[2] Barki, A., Bouabdallah, A. and Gharout, S., “M2M Security, Challenges and Solutions,” IEEE Communications Surveys and Tutorials, Vol. 18, No. 2, pp. 1241–1254 (2016).
[3] Fei, Y., Matthew, A. and Sumit R.,“V2V Wireless Communication Protocol for Rear-End Collision Avoidance on Highways,” Proceedings of the IEEE International Conference on Communications Workshops, pp. 52–59 (2008).
[4] He, X. and Yener, A., “Hop Secure Communication Using an Untrusted Relay: A Case for Cooperative Jamming,” Proceedings of the IEEE Global Telecommunications Conference (2008).
[5] Jennifer, Y. , Biswanath, M. and Dipak, G.“Wireless Sensor Network Survey,” Computer Networks, pp. 2292–2330 (2008).
[6] Papadimitratos, P., Buttyan, L. and Holczer, T., “Secure Vehicular Communication Systems: Design and Architecture,” IEEE Communications Magazine, Vol. 46, No. 11, pp. 100–109 (2008).
[7] Perkins, C.E. and Royer, E.M., “Ad hoc OnDemand Distance Vector Routing,” RFC 3561 (2003).
[8] Sakai, K., Sun, M.T. and Ku, W.S., “Multi-Path Based Avoidance Routing in Wireless Networks,” Proceedings of the 35th IEEE International Conference on Distributed Computing Systems, pp. 706–715 (2015).
[9] Shimada, M. and Higaki, H., “Intentional Collisions for Secure Wireless Ad-Hoc Networks,” Proceedings of the International Workshop on Mobile Ubiquitous Systems, Communications and Applications (2016).
[10] Tellez, M., El-Tawab, S. and Heyday, H.M., “Improving the Security of Wireless Sensor Networks in an IoT Environmental Monitoring System,” Proceedings of the IEEE Systems and Information Engineering Design Symposium (2016).
[11] Tsung, F.H., Chou, L.D. and Chao, H.C., “A Survey of Black Hole Attacks in Wireless Mobile Ad Hoc Networks,” Human-Centric Computing and Information Science, Springer (2011).
[12] Urrutia, J., “Two Problems on Discrete and Computational Geometry,” Proceedings of Japan Conference on Discrete and Computational Geometry, pp. 42–52 (1999).
[13] 金持, 桧垣, “秘密分散通信のための無線マルチホップ配送手法,” 情報処理学会論文誌, Vol. 57, No. 6, pp. 1554–1564 (2016).
[14] 情報通信研究機構, 情報処理推進機構, “暗号技術評価委員会報告,” (2016).
[15] 武井, 桧垣, “無線アドホックネットワークにおける送信電力低下をともなう故障中継無線ノード検出手法,” 電子情報通信学会技術報告, Vol. 116, No. 361 pp. 69–74 (2016).