Vol.2021-DPS-187 No.32
Vol.2021-MBL-99 No.32
Vol.2021-ITS-85 No.32
2021/5/28

無線マルチホップ配送における盗聴妨害のための ノイズ無線信号送信タイミング通知方法

天野 日菜乃[1,a)]　桧垣 博章[1,b)]

概要：無線マルチホップ通信では, 各中継無線ノードが無線信号到達範囲にデータメッセージをブロードキャスト送信することで次ホップ中継無線ノードへと転送する. このため, 盗聴無線ノードが無線信号到達範囲内で無線信号を傍受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. これを困難とするために, 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の一部がデータメッセージ転送を妨げずにノイズ信号を送信することで, 中継無線ノードの送信する無線信号と意図的に衝突させて盗聴を妨害する. このとき, 各中継無線ノードによるデータメッセージ転送時にノイズ信号を送信する無線ノードを決定し, 各データメッセージごとにノイズ無線信号の送信開始時刻と送信継続時間を通知することが必要となる. 本論文では, 無線マルチホップ配送経路探索時にノイズ信号を送信する無線ノードを決定するプロトコル, データメッセージ配送時に前ホップ中継無線ノードによるデータメッセージ転送のために交換される RTS/CTS 制御メッセージを傍受することで, 次ホップ中継無線ノードによるデータメッセージ転送時のノイズ信号送信タイミングを通知することで, 制御メッセージ同士の衝突を回避しつつデータメッセージの配送遅延を延長しないプロトコルを提案する.

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, 同期手法.

Synchronized Noise Signal Transmission for Secure Wireless Multihop Networks by Intentional Collisions with Data Messages

Abstract: In wireless multihop communication, each intermediate wireless node forwards a data message by broadcasting wireless signal carrying the data message to its wireless signal transmission range. Hence, it is possible for a malicious wireless node in the range to overhear the wireless signal and get the data message illegally. In order to make it difficult or impossible, part of 1hop- or 2hop-neighbor wireless nodes of each intermediate wireless node transmit noise wireless signal synchronously and induce intentional collision with the data message at the malicious wireless node. Here, protocols determining the neighbor wireless nodes transmitting the noise wireless signal for each intermediate wireless node of the wireless multihop transmission route and notifying the beginning and the duration of the noise signal transmission for each data message are mandatory to be introduced. This paper proposes a protocol determining the noise signal transmitting neighbor nodes during route determination by an ad-hoc routing protocol and a protocol notifying the time of noise signal transmission for each data message combined with the RTS/CTS collision avoidance protocol. The timing information notification for synchronized noise signal transmission does not require additional time-overhead and no additional transmission delay of data messages is required though no additional collisions among control signals are induced.

Keywords: Wireless multihop communiation, overhearing avoidance, jamming wireless signals, collisions, synchronization method.

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

[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
[a)] amano@higlab.net
[b)] hig@higlab.net

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, この経路に沿って配送されるデータメッセージを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増大, 配送遅延の延長等の問題をともなうことから, 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, データメッセージの配送と並行してノイズ無線信号を送信することにより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が提案されている. しかし, 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の導入が必要であることから, 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. 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, 本手法を実現するルーティングプロトコルと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, より的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することができる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導入が求められる.

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 [2,5]. 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

Vol.2021-DPS-187 No.32
Vol.2021-MBL-99 No.32
Vol.2021-ITS-85 No.32
2021/5/28

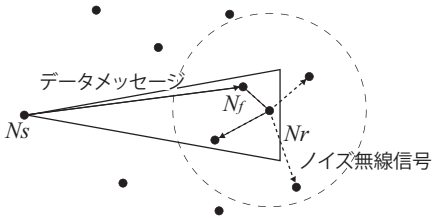

図 1 ノイズ無線とデータメッセージとの衝突および衝突信号の転送による盗聴回避手法.

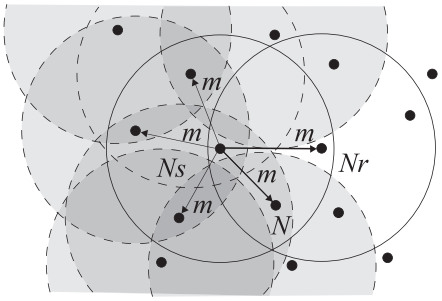

図 2 隣接無線ノードによるノイズ無線信号送信.

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.

3. 提案手法

3.1 ノイズ無線信号との衝突による盗聴妨害

互いに隣接する送信無線ノード 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データメッセージの送信と同時並行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.

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. □

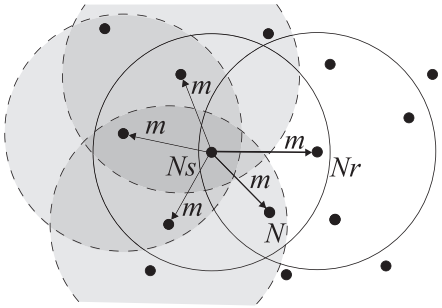

図 3 アドホック通信のためのノイズ無線信号送信.

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_j 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.

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開始タイミングと送信時間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 へと受信確認制御メッセージが送信される時間にはノイズ無線信号の送信を停止することができる. 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制御メッセージとの N_s における衝突を回避するために必要である.

3.2 ノイズ無線信号送信無線ノードの追加

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

Vol.2021-DPS-187 No.32
Vol.2021-MBL-99 No.32
Vol.2021-ITS-85 No.32
2021/5/28

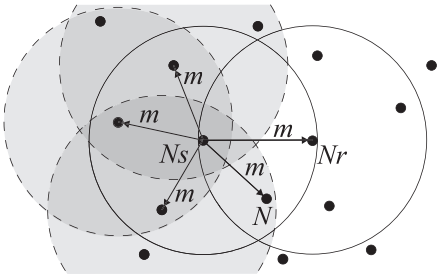

図 4 送受信無線ノード館距離が大きい場合による盗聴妨害.

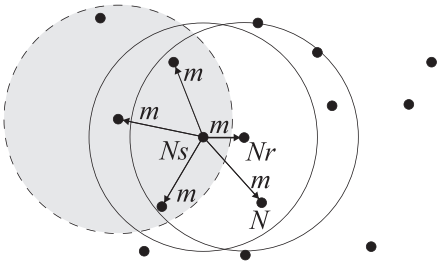

図 5 送受信無線ノード間距離が小さい場合による盗聴妨害.

ズ無線信号の送信時間と送信開始タイミング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, それに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 $|N_sN_r|$ 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 7 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.

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 $||N_0 \dots N_n\rangle\rangle$ 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にあって 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

Vol.2021-DPS-187 No.32
Vol.2021-MBL-99 No.32
Vol.2021-ITS-85 No.32
2021/5/28

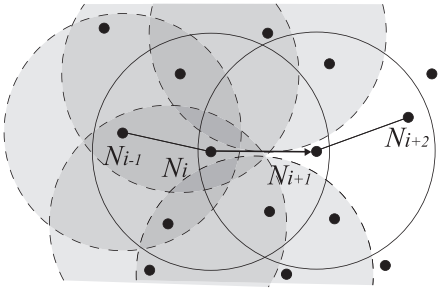

図 6 無線マルチホップ通信のためのノイズ無線信号送信.

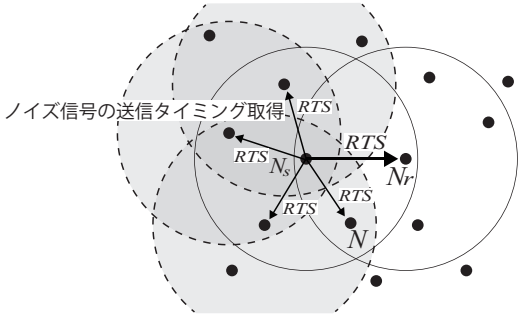

図 7 1 ホップ隣接無線ノードへのノイズ無線信号送信タイミング通知.

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. □

3.3 ノイズ無線信号送信ノード選択プロトコル

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_i' 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でより広く被覆することができる. ただし, N_i' 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 9 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 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, いずれの *Rrep* 制御メッセージをも受信せず, N_i の隣接無線ノード N_i^n と N_{i+1} の隣接無線ノード N_{i+1}^n 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.

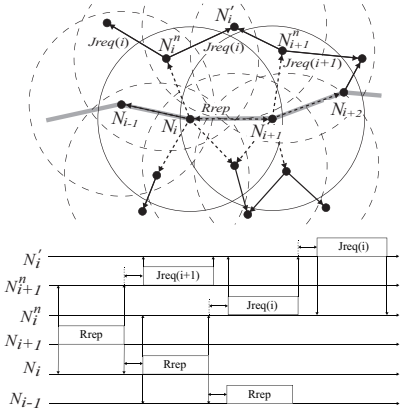

図 8 ノイズ無線信号送信ノード選択プロトコル.

[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_i^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. □

3.4 ノイズ無線信号送信タイミング通知プロトコル

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 N_i の 1 ホップ隣接無線ノードは, 3.2 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 から受信した *RTS* 制御メッセージに含まれる NAV の値を参照することによってノイズ無線

Vol.2021-DPS-187 No.32
Vol.2021-MBL-99 No.32
Vol.2021-ITS-85 No.32
2021/5/28

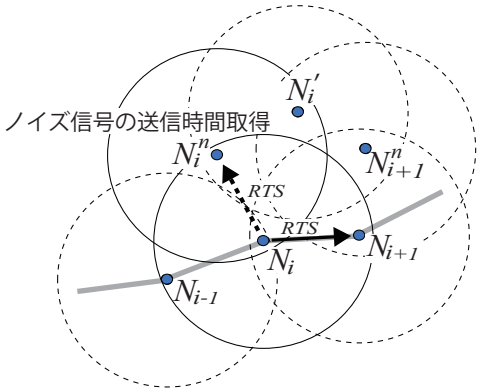

図 9 中継無線ノードの 1 ホップ隣接無線ノードへのノイズ無線信号送信タイミング通知.

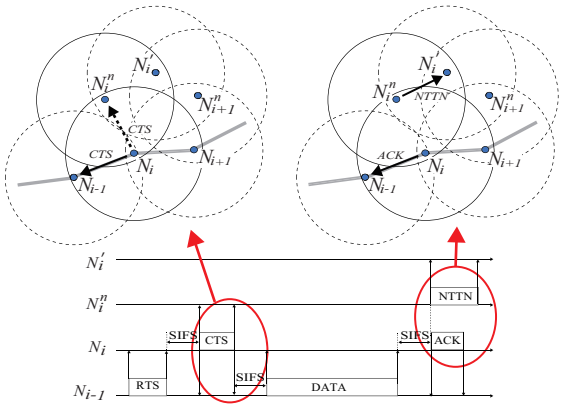

図 10 *NTTN* 制御メッセージによるノイズ無線信号送信時間の通知.

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 N_i と N_{i+1} の共通 2 ホップ隣接無線ノード N_i' 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できない. 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を考えなければならない. 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開始まで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.

この問題を解決するために, 本論文では, N_i が無線マルチホップ配送経路の中継無線ノードであることに注目する. N_i は, N_{i+1} へのデータメッセージ転送に先立って, このデータメッセージを N_{i-1} から受信する. N_{i-1} から N_i へのデータメッセージ転送を行なうための RTS/CTS 制御メッセージの交換によって, N_i' と N_i との共通隣接無線ノードである N_i^n は N_i から送信された *CTS* 制御メッセージを受信する. この *CTS* 制御メッセージに含まれる *NAV* の値から, データメッセージ転送時間を取得することができる. N_i^n がこのデータメッセージ転送時間を含む *NTTN* (ノイズ送信タイミング通知) 制御メッセージを N_i' に送信することで, これを受信した N_i' は, N_i から N_{i+1} へのデータメッセージ転送時におけるノイズ無線信号送信時間を得ることができる. N_i からの *CTS* 制御メッセージを受信した N_i^n は, *NAV* を設定してメッセージ送信を待機するが, これは, 送信するメッセージが N_i でデータメッセージと衝突することを回避するためである. 一方, N_i から N_{i-1} へと *ACK* 制御メッセージが配送されるタイミングでは, N_i^n が同時並行に *NTTN* 制御メッセージを送信しても N_i と N_i^n でこれらの制御メッセージが衝突するものの, N_{i-1} と N_i^n では *ACK* 制御メッセージと *NTTN* 制御メッセージをそれぞれ受信することができる (図 10).

NTTN 制御メッセージを受信した N_i' は N_i から N_{i+1} への データメッセージ転送に要する時間を取得, すなわち, ノイズ無線信号送信時間を取得することが可能となった. しかし, N_i' は N_i から N_{i+1} へのデータメッセージ送信開始時刻を得ることができていないため, ノイズ無線信号の送信開始時刻を定めることができない. 一般に, N_i のデータメッセージ転送時刻は, ランダムに定められる自身のバックオフタイマの値と競合する隣接無線ノードのバックオフタイマの値によって決定されるため, N_i' がデータメッセージ送信開始時刻を推定することが困難である.

ここで, 隣接無線ノードのデータメッセージ送信要求の有無とは無関係にデータメッセージの転送開始時刻を決定することが可能な手法には, MARCH[6] による方法, メッセージバーストによる方法 [7] がある. MARCH は, データメッセージの無線マルチホップ配送において, 各中継無線ノード N_i がその前ホップ中継無線ノード N_{i-1} からのデータメッセージ受信を終えるとただちにそのデータメッセージをその次ホップ中継無線ノード N_{i+1} への転送手続きを開始するものである. ここでは, N_i が送信する N_{i-1} への *ACK* 制御メッセージと N_{i+1} への *RTS* 制御メッセージが重畳される. *RTS* 制御メッセージがランダムバックオフなしに送信されることから, N_i から N_{i+1} へのデータメッセージ転送開始時刻を事前に確定することができる. また, メッセージバーストは, 単一無線ノードがデータメッセージを連続送信する手法であるが, 隣接無線ノード間で連続転送する目的に容易に転用することができる. N_{i-1} からデータメッセージを受信した N_i は, N_{i-1} への *ACK* 制御メッセージの送信を終えるとただちに N_{i+1} への *RTS* 制御メッセージを送信する. このとき, *RTS* 制御

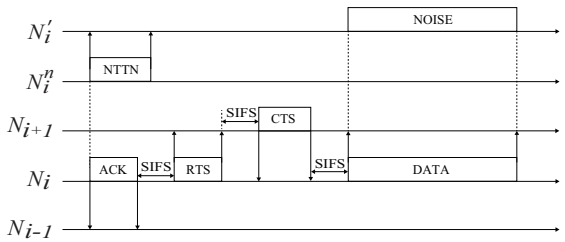

図 11 共通 2 ホップ隣接無線ノード N_i' のノイズ無線信号送信タイミング.

メッセージを *SIFS* インターバル時間経過後に送信する方法と, *RTS* 制御メッセージのバックオフタイマの値を 0 として *DIFS* インターバル時間経過後に送信する方法とがある.

本論文の提案手法では, N_i から N_{i-1} への *ACK* 制御メッセージ配送時間に *NTTN* 制御メッセージを送信しており, これらのメッセージが N_i の隣接無線ノードで衝突することから, *ACK* 制御メッセージに *RTS* 制御メッセージを重畳する手法は適切であるとは言えない. そこで, メッセージバーストによる方法を用いることとする. 図 9 に示すように, N_i' が N_i^n からの *NTTN* 制御メッセージ受信を開始してから N_i が N_{i+1} へのデータメッセージ送信を開始するまでの時間は, *ACK* 制御メッセージの配送時間, *RTS* 制御メッセージの配送時間, *CTS* 制御メッセージの配送時間の和に *SIFS* インターバル時間の 3 倍 (もしくは, *SIFS* インターバル時間の 2 倍と *DIFS* インターバル時間との和) を加えたもので, すべて固定時間である.

以上により, データメッセージ転送時間を含む *NTTN* 制御メッセージの導入によって, N_i から N_{i+1} へのデータメッセージ転送タイミングに合わせて, N_i と N_{i+1} の共通 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が可能となった.

4. 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, 前ホップ中継無線ノードのデータメッセージ転送のための *CTS* 制御メッセージに含まれる *NAV* の値から算出し, これを *ACK* 制御メッセージと同時並行に配送される *NTTN* 制御メッセージに含まることで 2 ホップ隣接無線ノードに通知する. また, データメッセージを隣接中継無線ノードが連続転送することで, 2 ホップ隣接無線ノードがノイズ無線信号送信開始時刻を特定可能とした. ただし, 本提案手法は, 次ホップ中継無線ノードが送信した *RTS* 制御メッセージに対して *CTS* 制御メッセージを返信することを前提としている. 次ホップ中継無線ノードが他の隣接無線ノードからの *RTS* 制御メッセージ, もしくは, *CTS* 制御メッセージを受信しておりメッセージの送信を待機している場合には, データメッセージが転送されないにも関わらずノイズ無線信号が送信されるとともに, データメッセージの送信開始時刻を取得する別の手段を持たなければならない. この問題の解決が今後の課題である.

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: Avhievable Rates and Cooperative Jamming,” IEEE Transactions on Information Theory, Vol. 54, No. 6, pp. 2735–2750 (2008).
[6] Toh, C.K., Vassiliou, V., Guichal, G.and Shih, C.H., “MARCH: A Medium Access Control Protocol for Multihop Wireless Ad Hoc Networks,” Proceedings of IEEE/AFCEA Military Communication Conference, pp. 512–516 (2000).
[7] 重安, 松野, 森永, “IEEE802.11DCF 端末との混在環境下における MAC Level Fairness 向上方式の提案,” 情報処理学会論文誌, vol. 50, no. 3, pp. 1156–1169 (2009).