4U-07

ノイズ無線信号との意図的衝突による盗聴妨害をともなう無線マルチホップ配送手法

天野 日菜乃 † 桧垣 博章 †
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 †

1 はじめに

無線アドホックネットワークでは, データメッセージが送信元無線ノードから送信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. 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, 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可能である.

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によるデータメッセージの取得を困難にする手法が提案されている [1] . 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ことや複雑な信号処理を行なうことが必要であるため, 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アドホックネットワークへの適用は困難である. 論文 [2] 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している. 本論文では, 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 提案手法

無線マルチホップ配送経路の中継無線ノード N_i からその次ホップ中継無線ノード N_{i+1} へ送信されるデータメッセージ m は, N_i 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. そのため, いずれかの N が盗聴無線ノードであるならば, N は m を受信する. これを困難にするために, m の送信と同時並行に以下の 2 条件を満たす近隣無線ノード N_i^n がノイズ無線信号を送信する手法を適用する.

(1) N_i^n の無線信号到達範囲が N_i の無線信号到達範囲と重複する.
(2) N_i^n は N_{i+1} の隣接無線ノードではない.

論文 [2] では, 以下の 2 種の近隣無線ノードがノイズ無線信号を送信する.

(1) N_{i+1} の 1 ホップ隣接無線ノードでない N_i の 1 ホップ隣接無線ノード N_i^{1n}.
(2) N_i , N_{i+1} のいずれの 1 ホップ隣接無線ノードでもない, N_i , N_{i+1} の共通 2 ホップ隣接無線ノード N_i^{2n}.

2.1 ノイズ無線信号送信ノード選択プロトコル

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無線ノードの決定には, 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* のユニキャスト追加の制御メッセージを用いることで実現する.

図 1 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* を送信するとき, N_i の隣接無線ノードは N_i^c はこの *Rrep* を傍受できる. このとき, N_i^c 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. N_i が N_{i-1} へ送信した *Rrep* を傍受したが, N_{i+1} が N_i へ送信した *Rrep* を傍受しなかった無線ノードが N_i^{1n} である. また, N_i^c と N_{i+1}^c とが送信した *Jreq*(i) と *Jreq*$(i+1)$ の両方を受信した無線ノードが N_i^{2n} である. N_i^{2n} はノイズ無線信号送信応答制御メッセージ *Jrep*(i) を N_i^c へ送信する.

2.2 ノイズ無線信号送信タイミング通知プロトコル

N_i^{1n} は N_i が送信する *RTS* を受信するため, ノイズ無線信号の送信時刻と送信時間を取得可能である. これらを N_i^{2n} が取得する手法を図 2 に示す. N_{i-1} から N_i へのデータメッセージ転送のために送信された

Wireless Multihop Transmissions with Intentional Collisions for Eavesdropping Prevension
†Hinano Amano and †Hiroaki Higaki
†Department of Robotics and Mechatronics, Tokyo Denki University

Copyright ©2021 Information Processing Society of Japan.
All Rights Reserved.

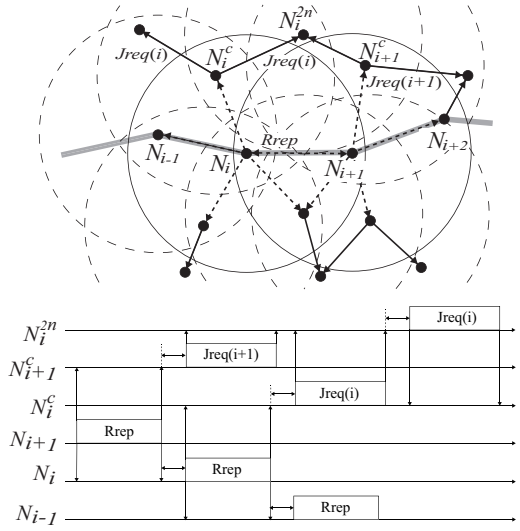

図 1: ノイズ無線信号送信ノード選択プロトコル.

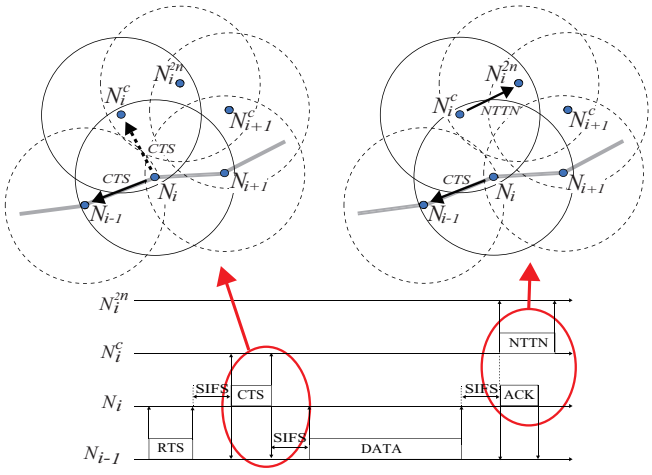

図 2: ノイズ無線信号送信時間の通知.

CTS を N_i^c が受信する. この CTS に含まれる NAV 値から, データメッセージ転送時間を取得できる. N_i^c は, CTS 受信後, データメッセージ転送時間に $SIFS$ インターバル時間の 2 倍を加えた時間待機することで, N_i から N_{i+1} への ACK 返送と並行してデータメッセージ送信時間を含むノイズ送信タイミング通知制御メッセージ $NTTN$ を N_i^{2n} にユニキャスト送信する. これが CTS と N_{i-1} で衝突しないために, N_i^c は N_{i-1} の隣接無線ノードではないことが求められる.

$NTTN$ を受信した N_i^{2n} は N_i から N_{i+1} へのデータメッセージ転送時間, すなわち, ノイズ無線信号送信時間を取得する. しかし, N_i^{2n} は N_i から N_{i+1} へのデータメッセージ送信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送信時刻は, ランダムに定められる自身と競合する隣接無線ノードのバックオフタイマ値によって決定されるため, N_i^{2n} がデータメッセージ送信時刻を推定することは困難である.

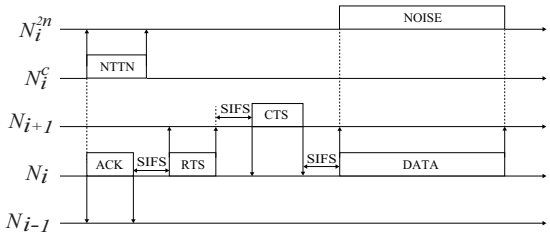

図 3: 共通 2 ホップ隣接無線ノード N_i^{2n} のノイズ無線信号送信タイミング.

そこで, 提案手法ではデータメッセージの配送にメッセージバースト [3] を適用する. 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. これによって, 図 3 に示すように, N_i^{2n} が $NTTN$ 受信終了後, ACK の配送時間, RTS の配送時間, CTS 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, $NTTN$ の配送時間を減じた時間だけ待機し, ノイズ無線信号を送信する.

3 まとめ

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した. ここでは, ノイズ無線信号を送信する近隣無線ノードの選択と, これらに対するノイズ無線信号送信時刻, 送信時間の通知を追加の時間オーバーヘッドなしに実現している.

参考文献

[1] 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).
[2] Shimada, I. and Higaki, H., “Intentional Collisions for Secure Ad-Hoc Networks,” Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems, pp. 183–188 (2016).
[3] 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).

Copyright ©2021 Information Processing Society of Japan.
All Rights Reserved.