

センサネットワークにおける協調した意図的衝突による 盗聴妨害手法

大栗 正宏 梶垣 博章

東京電機大学 未来科学部 ロボット・メカトロニクス学科

1 はじめに

無線センサネットワークでは、各センサネットワークがセンサデバイスによって取得した観測データを含むデータメッセージを無線シンクノードまで無線マルチホップ通信で配送する。このとき、各無線センサノードが次ホップ隣接無線センサノードに転送したデータメッセージは、この無線センサノードの無線信号到達範囲内で傍受可能である。しかし、この傍受を試みる盗聴無線ノードが他の無線センサノードの無線信号到達範囲にも含まれ、この無線センサノードが同時並行してデータメッセージを転送するならば、盗聴無線ノードにおいて意図的に衝突を発生させることによって傍受を妨害することができる。本論文では、これを実現するために、各無線センサノードに転送スロットを割り当てる方法を提案する。

2 関連研究

無線アドホックネットワークにおいて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の盗聴無線ノードによる傍受を妨害する方法として、中継無線ノードやその近隣無線ノードがノイズ無線信号をデータメッセージの転送と同時並行に送信する方法が提案されている。論文 [1] では、中継無線ノードは指向性アンテナを備え、無線信号を次ホップ中継無線ノードに向けて送信し、次ホップ中継無線ノードはノイズ無線信号を同時並行に送信する方法を提案している。ここでは、指向性アンテナと信号処理のための計算性能が各無線ノードに求められることに加えて、配送遅延が延長する問題がある。論文 [3] では、無指向性アンテナを備えた中継無線ノードの近隣無線ノードがノイズ無線信号をデータメッセージ転送と同時並行に送信することによって意図的に衝突を発生させ、盗聴無線ノードによる傍受を妨害する手法を提案している。ただし、ノイズ無線信号は意図的衝突のみを目的として送信しており、無線アドホックネットワーク全体の性能への影響を考慮する必要がある。

無線センサネットワークでは、TDMA 方式に基づいてデータメッセージの衝突を回避し、無線アドホックネットワーク全体の性能向上を目指す手法が提案され

ている [2]。ここでは、データメッセージの転送先無線センサノードでの衝突が発生しないように、各無線センサノードにデータメッセージ転送のための時間スロットを割り当てる。

3 提案手法

論文 [3] では、無線アドホックネットワークにおける無線マルチホップ配送において、中継無線ノード N_i から N_{i+1} へ転送されるデータメッセージを盗聴無線ノードに傍受されることを困難にするために、 N_i の 1 ホップ隣接無線ノードであり N_{i+1} の 1 ホップ隣接無線ノードではない無線ノード、および、 N_i と N_{i+1} に共通の 2 ホップ隣接無線ノードがノイズ無線信号をデータメッセージ転送と並行して送信する方法が提案されている。本論文では、無線センサネットワークを対象として、近隣無線センサノードが並行してデータメッセージを転送することによって互いの送信する無線信号が互いの無線信号到達範囲に含まれる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協調的手法を提案する。ここでは、データメッセージの配送経路はシンクノードからの制御メッセージのフラッディングを用いて定められていることを前提として、TDMA を基礎として各無線センサノードにデータメッセージを転送するスロットを適切に割り当てることによって、高い盗聴防止効果を得ることを目的とする。

まず、ノイズ無線信号の送信が盗聴無線ノードによるデータメッセージ傍受を妨害する効果を定式化するために以下を定義する。

[ノイズ支援可能無線センサノード] 無線センサノード N_i の次ホップ隣接無線センサノードが N_j であるとき、無線センサノード N の無線信号到達範囲と N_i の無線信号到達範囲に共通部分があり、 N の無線信号到達範囲に N_j が含まれないとき、 N は N_i のノイズ支援可能無線センサノードであるといい、 $N \Rightarrow N_i$ と表す。□ $N \Rightarrow N_i$ のとき、 N_i から N_j へのデータメッセージ転送と並行して N がノイズ無線信号を送信することによって、 N と N_i の無線信号到達範囲の共通部分に存在する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ことができる。

この妨害の効果は、共通部分が大きいほど大きい。これは、以下の単純盗聴妨害貢献度によって評価できる。[単純盗聴妨害貢献度] $N \Rightarrow N_i$ であるとき、 N の無線信号到達範囲と N_i の無線信号到達範囲とが重複する領域の面積の N_i の無線信号到達範囲の面積に対する比

Cooperative Intentional Collisions for Reduction of Eavesdropping in Sensor Networks
Masahiro OKURI and Hiroaki HIGAKI
Department of Robotics and Mechatronics, Tokyo Denki University

を単純盗聴妨害貢献度といい $SC(N \Rightarrow N_i)$ と表す。□
 すべての無線センサノードの無線信号到達距離が等しい場合には、単純盗聴妨害貢献度は無線センサノード間の距離のみによって定まる。 $N \Rightarrow N_i$ で、無線信号到達距離が r 、 $|NN_i| = d$ であるとき、 $SC(N \Rightarrow N_i) = \frac{1}{\pi} \cos^{-1} \left(\frac{d^2}{2r^2} - 1 \right) - \frac{d}{2\pi r^2} \sqrt{(2r+d)(2r-d)}$ であり、 d の変域 $0 \leq d \leq 2r$ に対する $SC(N \Rightarrow N_i)$ の値を図1に示す。近隣無線センサノードの無線信号到達範囲は相互に重複することから、単純盗聴妨害貢献度が高い無線センサノードに同一のスロットを割り当てることが直接的に盗聴無線ノードによる傍受をより妨害することができるとは限らないが、結果的に得られる貢献度に対して一定の正の相関を持つことは期待できる。

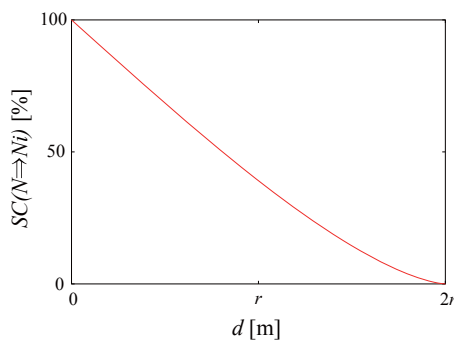


図 1: 単純盗聴妨害貢献度。

本論文で提案する同時並行に行われるデータメッセージ転送が互いに盗聴無線ノードによる傍受を妨害する無線センサノードの関係は、以下により定められる。
 [相互ノイズ支援可能無線センサノード対] 無線センサノード N_i と $N_{i'}$ が互いにノイズ支援可能無線センサノードであるとき、すなわち、 $N_i \Rightarrow N_{i'}$ かつ $N_{i'} \Rightarrow N_i$ であるとき、 N_i と $N_{i'}$ は相互ノイズ支援可能無線センサノード対であるといい、 $N_i \leftrightarrow N_{i'}$ と表す。□
 このとき、図2に示すように、 N_i と $N_{i'}$ の無線信号到達範囲に共通部分があり、 $N_j, N_{j'}$ がそれぞれ $N_{i'}, N_i$ の無線信号到達範囲に含まれないことから、 $N_i, N_{i'}$ が同時並行にデータメッセージを転送しても $N_j, N_{j'}$ において衝突せず、無線信号到達範囲の共通部分に含まれる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ことができる。ここで、単純盗聴妨害貢献度については以下が成り立つ。

[定理] $N_i \leftrightarrow N_{i'}$ のとき、 $SC(N_i \Rightarrow N_{i'}) = SC(N_{i'} \Rightarrow N_i)$ である。□

より多くの相互ノイズ支援可能無線センサノード対に同じスロットを割り当てることによって、盗聴無線ノードによるデータメッセージの傍受を妨害し、より困難にすることができる。そこで、以下の貪欲アルゴリズムを提案する。ここで、スロット割り当てのために推移的相互ノイズ支援可能無線センサノード集合を定義する。

[推移的相互ノイズ支援可能無線センサノード集合] 無線センサノード N について、 $N \leftrightarrow N'$ かつ $N' \leftrightarrow N''$

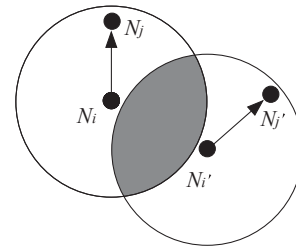


図 2: 相互ノイズ支援可能無線センサノード対。

であるとき、 N と N'' は推移的相互ノイズ支援可能無線センサノードといい $N \leftrightarrow N''$ で表す。また、無線ノード集合 $RMNS(N) := \{N' | N \leftrightarrow N'\}$ を推移的相互ノイズ支援可能無線センサノード集合という。□

[定理] $N \in RMNS(N)$ である。□

[スロット割り当てアルゴリズム]

1. スロットが割り当てられていない無線センサノード N をランダムに選択する。すべての無線センサノードにスロットを割り当て済みであれば終了する。
2. すでにいずれかの無線センサノードに割り当て済みのスロットのうち $N' \Rightarrow N$ である N' に割り当てられていないスロットのひとつを選択し N に割り当てる。そのようなスロットがない場合には、新しいスロットを N に割り当てる。
3. N と同じスロットが割り当て済みであり $N' \in RMNS(N)$ である無線センサノード N' について、 $N' \leftrightarrow N''$ である無線センサノード N'' のうち $SC(N' \Rightarrow N'')$ が最大である N'' に N と同じスロットを割り当てる。このような N'' が存在するならば 3 へ、存在しないならば 1 へ。□

4 まとめ

本論文では、無線センサネットワークにおいて、各無線センサノードが衝突を発生させることなくデータメッセージを転送し、かつ、相互の送信する無線信号が隣接無線ノードに対してノイズ無線信号となるように同一のスロットを割り当てることによって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スロット割り当て手法を提案した。本手法では、単純盗聴妨害貢献度を指標とする貪欲アルゴリズムによりスロットを割り当てており、その効果を実験評価することが今後の課題である。

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] Ozlem, I., Amitabha, G., Bhaskar, K. and Krishnakant, C., "Fast Data Collection in Tree-Based Wireless Sensor Networks," IEEE Transactions on Mobile Computing, vol. 11, no. 1, pp. 86-99 (2012).
- [3] 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).