

無線網における盗聴を困難とするための 自己組織型ノイズ無線信号送信手法の改良

大山 拓海† 谷口 義明†,‡
†近畿大学理工学部 ‡近畿大学情報学研究所

1 序論

無線ネットワークでデータを送信する際、端末はデータをブロードキャストする。そのためデータが盗聴される可能性がある。盗聴の対策としてデータの暗号化があるが、ネットワークに接続するすべての機器が暗号化機能を持っているわけではない。そこで暗号以外の手法でデータの盗聴を防ぐ手法がいくつか存在する。文献 [1] のように送信端末に指向性アンテナを備え付けビームフォーミングを利用することで盗聴可能領域を削減する手法、文献 [2] のように特殊な機器を備え付けずに近くの端末がノイズ信号を送信することで盗聴可能領域を減らす手法がある。

我々の研究グループでは文献 [2] と同じように端末に特殊な機器を付け加えず、周囲の端末が協調してノイズ無線信号を送信することによって物理的な通信可能範囲を狭め、データの盗聴を困難化する手法を検討している (図 1)。先行研究 [3] では、パルス結合振動子モデルに基づく自己組織型タイミング決定手法である DESYNC [4] を、ノイズ無線信号送信に応用する手法を検討している。パルス結合振動子モデルを応用することにより、単純な機構により、端末の移動、追加などの環境変動に適応的に動作する制御が可能となる。

しかしながら、既存手法は初期検討にとどまっており、適切でない端末がノイズ信号を送信することにより受信端末がデータを受信できないほど過剰なノイズが送信される状態に遷移する場合、あるいは、送信端末のデータ送信と同じタイミングでノイズを送信する端末がない状態に遷移する場合があった。本研究では、この問題を回避するため、このような場合に同期状態を再調整する手法を提案、コンピュータシミュレーションにより評価する。

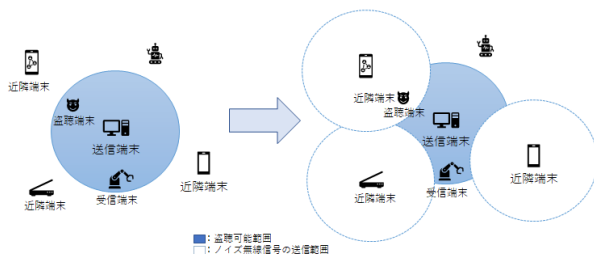


図 1: 盗聴可能領域の削減

A self-organizing method for transmitting noise signals to make eavesdropping difficult in wireless networks
†Takumi Oyama †,‡Yoshiaki Taniguchi
†Faculty of Science and Engineering, Kindai University
‡Cyber Informatics Research Institute, Kindai University

2 ノイズ無線信号送信手法

2.1 基本動作 [3]

本手法では、蛍の発光や心臓の鼓動のタイミングなどの自然界の同期モデルをヒントにしたパルス結合振動モデルに基づいたタイミング決定手法である DESYNC を利用して近隣ノードのノイズ送信タイミングを決定して盗聴可能領域を削減する。DESYNC をシングルホップ環境に適用した場合、全端末が異なるタイミングでパケットを送信するようになるが、マルチホップ環境ではパケット送信タイミングが同じとなる端末の組合せが発生する。本手法では、この性質を利用して、盗聴可能領域を削減する。

本研究では、1 台の送信端末と 1 台の受信端末、およびその周辺に複数台の近隣端末が設置されている環境を想定する。送信端末は一定間隔 T 毎に受信端末に対してデータを送信する。受信端末は正常にデータを受信した場合に ACK パケットを送信するものとする。周辺の近隣端末は、起動時に、送信予定時刻を T_{next} を T 秒後に初期化する。送信予定時刻となった近隣端末は、ノイズ無線信号をブロードキャスト送信し、その時刻 T_{fire} を記録する。また、近隣端末はノイズ無線信号を送信した後、初めて他の端末からのノイズ無線信号を受信した場合、その時刻 $T_{nowfire}$ 、自身の無線信号送信時刻 T_{fire} 、さらにその直前のノイズ無線信号受信時刻 $T_{prefire}$ を用いて自身の送信予定時刻 T_{next} を以下のように調整する。

$$T_{next} = T + (1 - \alpha)T_{fire} + \alpha \frac{T_{prefire} + T_{nowfire}}{2} \quad (1)$$

ここで、 α はパラメータであり、本研究では $\alpha = 0.95$ とする [4]。以上の動作を繰り返す事で 2 ホップ以上離れている近隣端末の一部が送信端末と同じタイミングでノイズ無線信号を送信するようになる。

2.2 同期状態再調整手法

基本動作のみでは、受信端末がデータを受信できないほどの過剰なノイズが送信される状態、あるいは、どの近隣端末も送信端末のデータ送信と同じタイミングでノイズ送信を行わない状態に遷移することがある。そのような場合、送信端末は、次に送信するデータフレームの送信タイミングを一度だけランダムに変更する。このことにより、端末全体の同期状態が再調整される。なお、3 回送信タイミングを変更しても受信端末でデータを受信できない場合は、タイミング調整をあきらめる。

ここで、例えば、送信端末は、ACK パケットが一定回数連続して返ってこない場合、受信端末がデータを

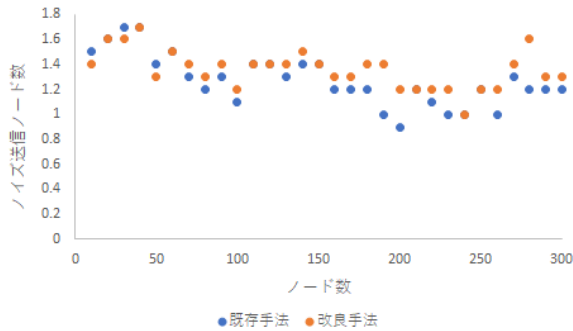


図 2: ノイズ無線信号送信ノード数の比較

受信できないほどの過剰なノイズが送信される状態に遷移していると推定できる。また、受信端末が送信端末からのデータ受信時の信号対干渉ノイズ比 (SINR) を ACK パケットにフィードバックとして含めることにより、送信端末は、送信端末のデータ送信と同じタイミングでどれくらいのノイズ送信が行われているかを推定できると考えられる。

3 シミュレーション評価

先行研究 [3] で提案されている手法を既存手法、既存手法に同期状態再調整手法を導入したものを改良手法とし、先行研究と同じ条件で、近隣端末数を 1 台から 300 台の範囲で 10 台刻みで変化させてシミュレーションを行った。評価指標としてはノイズ無線信号送信端末数、カバレッジ、受信不可率を用いた。ノイズ無線信号送信端末は送信端末のデータ送信タイミングと同じタイミングでノイズ無線信号を送信する端末である。カバレッジは盗聴可能領域をどのくらい削減できたかを表す指標であり、値が大きいくほどより削減できていることを表す。なお、受信端末がデータを受信できない場合のカバレッジは 0 とする。受信不可率は、シミュレーション評価のうち、受信端末が受信できないほど過剰なノイズが送信される場合の割合である。以降の結果は 10 回のシミュレーション結果の平均である。

ノイズ無線信号送信端末数、受信不可率、カバレッジの比較を図 2、図 3、図 4 に示す。まず、図 2 よりノイズ無線信号送信端末数が既存手法より多くなっていることがわかる。これはノイズ無線信号を発信する端末がなかった場合に再調整を行った結果であると考えられる。次に、図 3 より既存手法よりも改良手法の受信不可率が減少していることがわかる。これは、ノイズが過剰に送信された場合に再調整を行うことで、受信端末が送信端末からのデータを受信できるようになったことによると考える。また、その結果、図 4 に示されるように、カバレッジの向上につながったと考えられる。

4 結論

本研究では、DESYNC を利用した自己組織型ノイズ無線信号送信手法の改良を行った。本研究で提案した

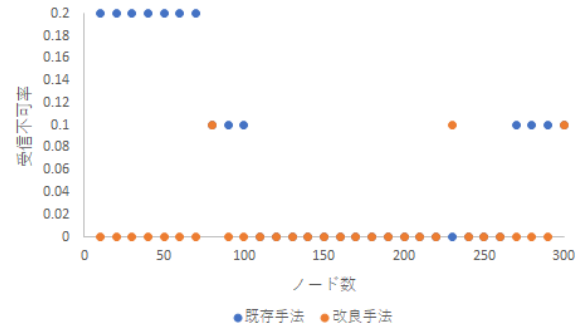


図 3: 受信不可率の比較

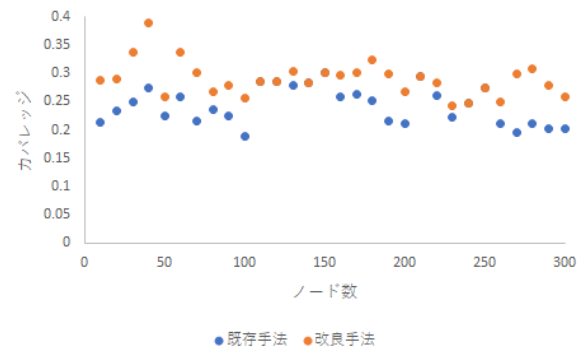


図 4: カバレッジの比較

同期状態再調整手法を用いることにより、受信不可率を削減し、カバレッジを向上できることを確認した。

今後の課題として、マルチホップネットワーク環境における評価がある。

謝辞

本研究の一部は科学研究費 (19K11934) の助成を受けた。ここに記して謝意を表す。

参考文献

- [1] X. He and A. Yener, “Two-Hop Secure Communication Using an Untrusted Relay: A Case for Cooperative Jamming,” in Proceedings of IEEE GLOBECOM 2008, Dec. 2008.
- [2] I. Shimada and H. Higaki, “Interference with over-hearing for secure ad-hoc networks,” in Proceedings of CNSCE 2017, pp. 130–135, Mar. 2017.
- [3] 大山拓海, 大和聖, 谷口義明, “無線ネットワークにおいて盗聴を困難とするための自己組織型ノイズ無線信号送信手法の検討,” 2021 年度情報処理学会関西支部大会講演集, 6 pages, Sep. 2021.
- [4] J. Degeysys, I. Rose, A. Patel, and R. Nagpal, “DESYNC: self-organizing desynchronization and TDMA on wireless sensor networks,” in Proceedings of ACM/IEEE ISPN 2007, Apr. 2007.