

無線アドホックネットワークにおける偽検出通知送出する 攻撃ノード検出手法

曾田雄大 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中継無線ノードによって転送されることによって配送される無線マルチホップ通信が用いられる。ここでは、無線アドホックネットワークの正常な動作を困難あるいは不可能とすることを目的とした攻撃ノードが混在することが考えられる。本論文では、攻撃ノードによるデータメッセージの転送あるいは攻撃ノードの検出を通知する制御メッセージの送信を偽る攻撃に対して、この攻撃ノードを検出する手法を提案する。

2 関連研究

無線マルチホップ配送経路を検出した後のデータメッセージ配送において、データメッセージが正しく送信元無線ノードから送信先無線ノードへと配送されることを困難にする攻撃とそれへの対処方法が検討されている。中継無線ノードが前ホップ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転送しないという攻撃や前ホップ無線ノードから受信したものと異なるデータメッセージを次ホップ無線ノードへと転送する攻撃、前ホップ無線ノードからデータメッセージを受信していないにもかかわらず次ホップ無線ノードへとデータメッセージを送信する攻撃などに対して有効な方策として watchdog 手法 [2] と two-ack 手法 [1] がある。watchdog 手法では、中継無線ノードがデータメッセージを正しく転送しているかどうかをその隣接無線ノードが監視する。一方、two-ack 手法では中継無線ノードのデータ転送に対して通常は次ホップ中継無線ノードからの受信確認 (ack) メッセージを受信するのに加えて、次々ホップ中継無線ノードからも受信確認 (ack) メッセージを受信する。

従来の watchdog 手法では、データメッセージの転送に関わる攻撃を行なう中継無線ノードを検出している。攻撃ノードの検出は制御メッセージの配送によって通知され、送信元無線ノードに攻撃ノードの検出を通知して経路を再検出させる。これに対して、中継無線ノード間で交換される制御メッセージを偽装する攻撃が考えられる。攻撃ノードは、攻撃ノードではない中継無線ノードを攻撃ノードと偽って通知することによって、データメッセージ配送を中断させるとともに、攻撃

ノードとして通知された無線ノードが経路探索から排除されることによって、経路検出率を低下させることができる。

3 提案手法

攻撃ノードである中継無線ノードがデータメッセージ転送を偽る攻撃については、中継無線ノード N_i の転送するデータメッセージを前ホップ中継無線ノード N_{i-1} が傍受することによって検出可能である。 N_i が攻撃ノードであることを検出した N_{i-1} から送信元無線ノード $N^s = N_0$ まで攻撃ノード検出メッセージ $Mdet$ を R に沿って逆方向に配送することによって N^s に N_i が攻撃ノードであることを通知する。一方、 N_{i-1} が攻撃ノードであり、 N_i が攻撃ノードではないにも関わらず N_i を攻撃ノードとして検出したとする $Mdet$ メッセージを N_{i-1} が前ホップ中継無線ノード N_{i-2} へと送信することが考えられる。この場合、 N_{i-2} はこの $Mdet$ メッセージが N_{i-1} によって送信された偽の攻撃ノード検出メッセージと判定することはできず、 $Mdet$ メッセージは N^s へと配送される。この問題を解決するために、本論文では、 N_{i-1} と N_i から送信されるすべてのメッセージを傍受可能な隣接監視無線ノード O_i が存在する場合にのみ無線通信リンク $[N_i N_{i+1}]$ を無線マルチホップ配送経路に含むことができるという制約を導入する (図 1)。ここで、 O_i は N_{i-1} と N_i の無線信号到達範囲に共通に含まれる無線ノードのひとつ、すなわち、 N_{i-1} と N_i に共通の隣接無線ノードのひとつである。したがって、 O_i は N_{i-1} が N_i へ送信するデータメッセージと N_i が N_{i+1} へ送信するデータメッセージとをいずれも傍受することができる。このため、 O_i は N_{i-1} と同様に N_i が偽のデータメッセージを N_{i+1} へ送信することを検出することが可能である。これに加え、 O_i は N_{i-1} がその前ホップ中継無線ノード N_{i-2} へ送信する $Mdet$ メッセージを傍受することができる。したがって、 N_i が攻撃ノードではないにも関わらず N_{i-1} が N_i を攻撃ノードとして検出したとする偽の $Mdet$ メッセージを N_{i-2} へと送信したならば、これを傍受することによって N_i ではなく N_{i-1} が攻撃ノードであることを O_i は検出することができる。

このように、 N_{i-1} が偽の $Mdet$ メッセージを用いた攻撃を行なったことを O_i が検出した場合、 N_{i-1} が N_{i-2} へ送信した $Mdet$ メッセージが N_0 に配送されないようにすることに加え、 N_{i-1} を攻撃ノードとして検出したとする $Mdet$ メッセージを N_0 へと配送することが求められる。ここで、この $Mdet$ メッセージを攻撃ノードである N_{i-1} を経由して配送することはできないことから、本論文では、 O_i がこの $Mdet$ メッセージ

Cooperative Watchdog for Detection of Malicious Nodes Transmitting False Detection in Wireless Ad Hoc Networks

Norihiro SOTA and Hiroaki HIGAKI

Department of Robotics and Mechatronics, Tokyo Denki University

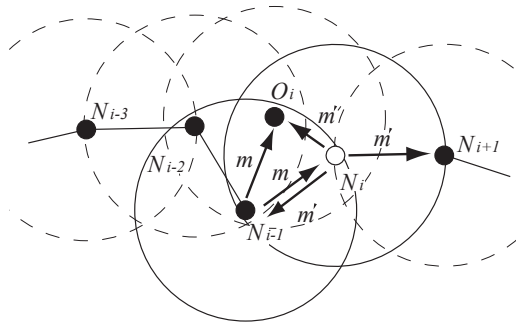


図1: 隣接監視無線ノード。

を N_{i-2} を経由して N_0 へと配送することとする。したがって、 O_i は N_{i-2} の隣接無線ノードでもあるとする。しかし、この O_i がすべての無線リンク $|N_i N_{i+1}|$ に対して存在しなければならないという制約は厳しく、経路検出率が著しく低下することが考えられる。そこで、本論文では、 O_i が N_{i-1} へと送信する攻撃ノード検出メッセージ $Mdet$ を中継する監視中継無線ノード I_i を導入する(図2)。 O_i は N_i のデータメッセージ転送を監視するために、 N_{i-1} と N_i の無線信号到達範囲に含まれなければならないが、 N_{i-2} に直接 $Mdet$ メッセージを送信することができる必要性は必ずしもない。また、 I_i は $Mdet$ メッセージを O_i から N_{i-2} へと転送することだけが求められることから、 N_{i-1} を無線信号到達範囲に含む必要はない。このように、 N_{i-2} , N_{i-1} , N_i , O_i の隣接関係に関わる制約を緩和し、 I_i に対しても厳しい制約条件を課していないことから、無線マルチホップ配送経路の検出率が改善されることが期待できる。

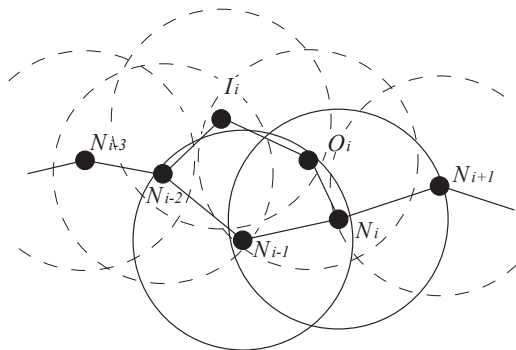


図2: 監視中継無線ノードによる経路検出率の改善。

4 評価

本章では、シミュレーション実験により、監視可能無線リンク条件による制約が経路検出率にどれだけの影響を与えるか評価する。250m×250mの正方形領域に無線信号到達距離10mの無線ノード0-3,000台を一様分布乱数に基づいてランダムに配置して、経路検出率を測定する。

実験結果を図3に示す。提案手法における経路検出率は、AODVによる経路検出率と比較すると、無線ノード数が2,000台以上(平均隣接無線ノード数10.05

台)の場合には、経路検出率に大きな差異はないものの、1,500-1,900台ではその差が次第に顕著になる。送信元無線ノードから送信先無線ノードまでの距離に対する経路検出率の低下の度合も、無線ノード数2,000台以上においてはほぼ同等の変化であるものの、1,900台以下では距離の増加に対する経路検出率の低下の度合がAODVと比べて顕著に大きくなることが分かる。また、監視中継無線ノードの導入によって経路検出率は、配送経路長の延長に対して経路検出率が向上し、配送経路長が150mのときに最大で17.5%改善することができている。なお、経路検出率は隣接無線ノード間の経路探索要求メッセージの送信順序と近隣無線ノードの同時送信による経路探索要求メッセージ間の衝突の発生率の影響を受ける。そこで、このような影響が除去できた場合の経路検出率の上限を評価した結果も図3に示している。この結果から、無線ノード数1,000台から2000台については経路探索要求メッセージの送信タイミングの制御、送信順序への優先度の導入などにより経路検出率を改善できる可能性があることがわかる。

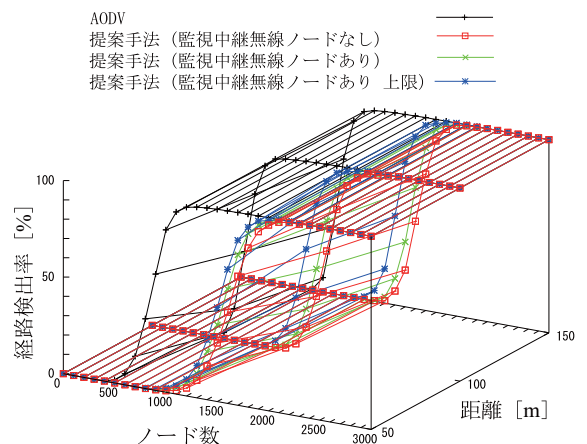


図3: 無線マルチホップ配送経路検出率。

5 まとめ

本論文では、無線ノードの偽攻撃ノード検出通知による攻撃を検出可能な無線マルチホップ通信手法を提案した。無線マルチホップ配送経路の中継無線ノードによる攻撃をその前ホップ無線ノードとこれらに隣接する監視無線ノードとによる協調監視する方法を示した。さらに、監視無線ノードの導入によって低下した経路検出率を改善するために、監視中継無線ノードを導入することを提案した。

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] Martl, S., Giulini, T.J., Lai, K. and Baker, M., "Mitigating routing misbehavior in mobile ad hoc networks," Proceedings of the International Conference on Mobile Computing and Networking, pp. 255-265 (2000).