Vol.2016-DPS-168 No.1
Vol.2016-SPT-21 No.1
Vol.2016-EIP-74 No.1
2016/11/17

無線アドホックネットワークにおける偽検出通知を用いる攻撃ノードの検出手法

曽田 雄大[1,a)]　桧垣 博章[1,b)]

概要：無線アドホックネットワークでは, 各無線ノードが隣接無線ノードのいずれかを前後ホップとする無線マルチホップ配送経路を構成し, これに沿ってデータメッセージを配送する. このとき, 攻撃ノードがこの配送経路の中継無線ノードとして含まれることが考えられ, この攻撃ノードを配送経路から除外するために, これを検出する手法が求められる. 本論文では, 中継無線ノードが偽のデータメッセージを転送する攻撃を検出可能な watchdog 手法を拡張し, 他の攻撃ノードではない中継無線ノードを攻撃ノードとして検出したとする偽の攻撃ノード検出通知を送信する攻撃に対しても攻撃ノードを検出可能な協調 watchdog 手法を提案する. 提案手法では, 中継無線ノードによる攻撃のみでなく, 協調 watchdog 手法を実現するために導入された監視無線ノードによる攻撃も検出可能である. 提案手法は, 攻撃を検出した場合にのみ制御メッセージ交換や隣接無線ノード間の同期を要し, 攻撃がなされない場合にはこれらを必要としない点で優れている. さらに, 経路検出率を改善するための監視中継ノードを導入し, その効果を実験評価する.

Detection of Malicious Nodes with False Detection Notification in Wireless Ad-Hoc Networks

Norihiro Sota[1,a)]　Hiroaki Higaki[1,b)]

Abstract: In wireless ad-hoc networks, each wireless node whose two neighbor nodes serve roles of its previous- and next-hop nodes contribute to configure a wireless multihop transmission route for a sequence of data messages. Here, a malicious wireless node is included in the route as an intermediate wireless node. In order to remove it from the route, it is required to be detected. Conventional watchdog methods can detect a malicious node transmitting different messages from receiving ones. This paper proposes an extended method called cooperative watchdog methods with an additional observing node for each wireless link in a route. It detects not only false data message transmissions but also false notifications of a malicious node detection. Here, a malicious node is detected even if it is the additional observing node. The proposed method requires no additional control message transmissions while no malicious data and control messages are transmitted. For improving the connectivity degraded by the proposed method, additional intermediate node is introduced to help the observing node. The improvement is evaluated in simulation experiments.

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. 電源容量の限られた無線ノードによって構成されながらもより高い接続性を得ることが求められることから, 比較的高密度で無線ノードが配置され, 電源の枯渇による無線ノード離脱や新規無線ノードの追加, また, 移動機能を備えた無線ノードの動的な参加と離脱のある環境において, 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. 攻撃ノードの行なう攻撃には様々なものが考えられ, すべてに対応する手法を考案することは不可能である. 本論文では, 攻撃ノードは無線マルチホップ配送に関与する無線ノード, すなわち,

[1] 東京電機大学大学院ロボット・メカトロニクス学専攻
Department of Robotics and Mechatronics, Tokyo Denki University, Adachi Tokyo 120–8551, Japan
[a)] sota@higlab.net
[b)] hig@higlab.net

中継無線ノードあるいは提案手法で導入する監視無線ノード, 監視転送無線ノードであり, 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

無線アドホックネットワークにおいて, 攻撃ノードによってデータメッセージの配送を困難にするような攻撃には様々なものがあり, 多様な対策が提案されている. 送信元無線ノードから送信先無線ノードまでデータメッセージを配送するためには, 複数の中継無線ノードによるデータメッセージの転送が不可欠であり, これを困難にする攻撃の方法として経路の検出, すなわち, ルーティングを困難にする手法がある. セルフィッシュノードは, 自身が送信元無線ノードあるいは送信先無線ノードとなる無線マルチホップ配送は行なうものの, 他の無線ノード間の無線マルチホップ配送に対して中継無線ノードとして貢献することを拒む無線ノードである. このようなセルフィッシュノードの存在によって無線マルチホップ配送経路の検出率が低下する. ここでは, 存在するセルフィッシュノードを検出する手法が提案されており, 検出されたセルフィッシュノードを送信元無線ノードあるいは送信先無線ノードとする無線マルチホップ配送経路の構築を行なわない, セルフィッシュノードの発生を防ぐために中継無線ノードの役割を担うことに対して妥当なインセンティブを与えるなどの方策が考えられている [1], [3], [5], [9]. 一方, 積極的に無線マルチホップ配送経路に含まれることによってデータメッセージの無線マルチホップ配送を困難にする手法のひとつがブラックホールノードである. ブラックホールノードは, 経路探索において送信先無線ノードを偽る, あるいは, 送信先無線ノードへの経路をキャッシュに保持しているかのように偽ることによって, 誤って検出された無線マルチホップ配送経路上の無線ノード (送信先無線ノード, あるいは, 中継無線ノード) を偽装する. そして, ブラックホールノードは, この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を受信するが転送しないことによって送信先無線ノードへと到達することを妨害する. このようなブラックホールノードの検出手法についても様々なものが考案されている. また, このような無線ノードを検出される無線マルチホップ配送経路に含めないようにするためにレピュテーション, すなわち, 無線ノード間の相互評価を用いる方法が提案されている. 長期に運用される無線アドホックネットワークにおいては, 各無線ノードに対する評価が蓄積される有効な方法である [4], [6].

一方, 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関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 [7] と two–ack 手法 [2] 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手法である. 最も簡易な手法は, 監視対象の中継無線ノードの前ホップ中継無線ノードが監視する方法である. これに対し, two–ack 手法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方法である. これによって, 前記の中継無線ノードによる攻撃を検出することが可能であるが, 多数の受信確認 (ack) メッセージが送信されるため, これらとデータメッセージ転送との競合により無線マルチホップ配送の性能が低下する問題がある. この他に, データメッセージ転送時の送信電力を攻撃ノードが調節することによって, 前記の攻撃を実施する方法とその対策について提案する研究もある.

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, 例えば, 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. そこで, 本論文では, 偽の攻撃無線ノード検出通知メッセージを送信する攻撃への対処として, この攻撃ノードを検出し, これを送信元無線ノードへと通知する手法を提案する. なお, 複数の攻撃ノードが相互に協調して攻撃することはなく, ひとつの無線マルチホップ配送経路の中継無線ノード, および, 本論文で導入する監視無線ノード, 監視中継無線ノードには高々 1 つの攻撃ノードのみが存在すると仮定する.

3. 提案手法

3.1 偽攻撃ノード検出通知による攻撃

攻撃ノードである中継無線ノードは, 前ホップ中継無線ノードから受信したデータメッセージを次ホップ中継無線ノードに転送しない, 前ホップ中継無線ノードから受信し

Vol.2016-DPS-168 No.1
Vol.2016-SPT-21 No.1
Vol.2016-EIP-74 No.1
2016/11/17

たデータメッセージとは異なるデータメッセージを次ホップ中継無線ノードへと転送する, 前ホップ中継無線ノードから受信していないデータメッセージを次ホップ中継無線ノードへと送信するといった攻撃をする. このような攻撃については, 各中継無線ノードのメッセージ送信がディスクモデル [10] に従って受信されることから, 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} が受信 (傍受) することによって検出可能である. 図 1 に示すように, データメッセージ m を転送した N_{i-1} は, N_i が次ホップ中継無線ノード N_{i+1} へと転送するデータメッセージ m' を受信する. m と m' とが同一である場合には N_i はデータメッセージの転送を正しく行なっているが, m と m' が異なるならば N_i は攻撃ノードであり, これを N_{i-1} が検出することができる.

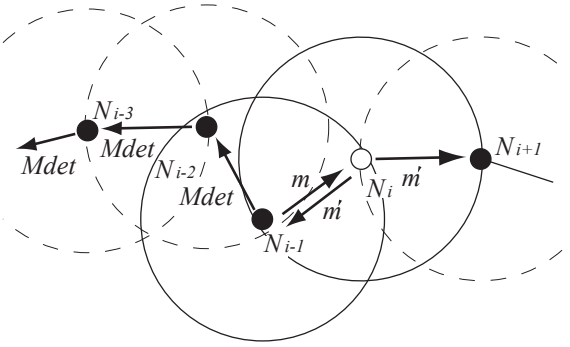

図 1 攻撃ノードによるデータメッセージ偽装の検出.

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 $\mathcal{R}$ 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. N^s は N_i を除去した新たな無線マルチホップ配送経路 $\mathcal{R}'$ を探索, 検出することで N^d へのデータメッセージ配送を再開する. 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 (図 2). 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, 前ホップ中継無線ノード N_{i-3} へと転送する. 以下, 同様のことが繰返されることで攻撃ノードではない N_i を攻撃ノードとして検出したとする $Mdet$ メッセージが N^s へと配送され, N^s は攻撃ノードではない N_i を除いた無線マルチホップ配送経路の再探索を行なうこととなる. このとき, 新たに検出された無線マルチホップ配送経路には攻撃無線ノードである N_{i-1} を中継無線ノードとして含む可能性がある.

なお, この $Mdet$ メッセージが N_i によって送信された偽の攻撃ノード検出メッセージであり, その送信元中継無線ノードである N_{i-1} が攻撃無線ノードであることを N_i は検出可能である. ただし, これを N_0 に通知する, すなわち 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 へと無線マルチホップ配送するためには, N_{i-1} を含まない N_0 までの無線マルチホップ配送経路が必要となる. この方法を用いる場合, このような前ホップ中継無線ノードを含まない送信元無線ノードまでの無線マルチホップ配送経路がすべての中継無線ノードについて必要となる点, N_0 には N_i を攻撃ノードとして検出したとする N_{i-1} からの $Mdet$ メッセージと N_{i-1} を攻撃ノードとして検出したとする N_i からの $Mdet$ メッセージとの両方が配送され, N_0 はいずれが攻撃ノードであるかを決定できない点が問題となる.

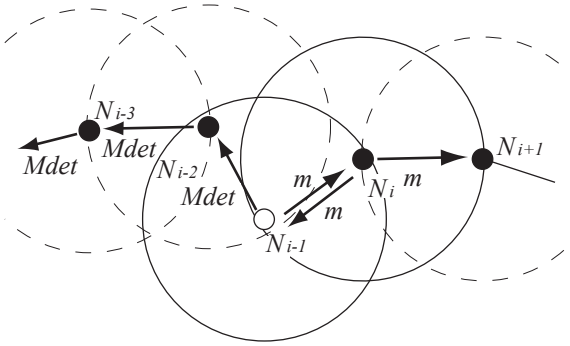

図 2 偽の攻撃ノード検出メッセージを用いる攻撃.

3.2 隣接監視無線ノード

前節で示した問題, すなわち, 中継無線ノード N_i を攻撃ノードとして検出したとする偽の攻撃ノード検出メッセージ $Mdet$ を前ホップ中継無線ノード N_{i-1} が送信する攻撃に対して正しく N_{i-1} を攻撃ノードと検出するという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 $|N_iN_{i+1}\rangle$ 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 3). 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受信 (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 $Mdet$ メッセージを受信 (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

Vol.2016-DPS-168 No.1
Vol.2016-SPT-21 No.1
Vol.2016-EIP-74 No.1
2016/11/17

信したならば, これを受信 (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.

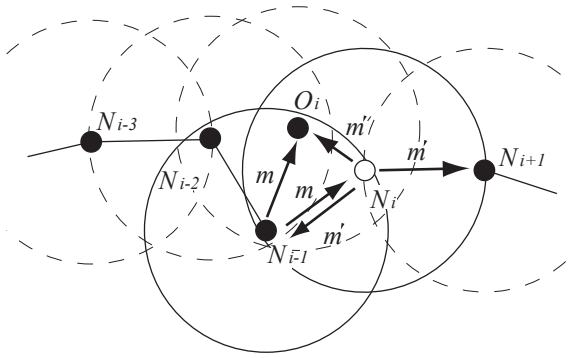

図 3 隣接監視無線ノード.

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[*1].

以下では, N_{i-2}, N_{i-1}, N_i, O_i の処理手順について検証し, N_i が偽のデータメッセージを N_{i-1} へと送信する攻撃ノードであること, N_{i-1} が N_i を攻撃ノードとして検出したと偽の攻撃ノード検出メッセージを N_{i-2} へと送信する攻撃ノードであることを N_{i-2} が検出できることを示す. さらに, N_{i-1} が O_i を攻撃ノードとして検出したとする偽の攻撃ノード検出メッセージを N_{i-2} へと送信する攻撃ノードであること, O_i が N_{i-1} を攻撃ノードとして検出したとする偽の攻撃ノード検出メッセージを N_{i-2} へと送信する攻撃ノードであることをも N_{i-2} が検出できることを示す.

まず, これらのノードのすべてが攻撃ノードでない場合[*2], データメッセージ m は中継無線ノード N_i による転送が繰返されることで無線マルチホップ配送経路 $\mathcal{R}$ に沿って配送される. このとき, 追加の制御メッセージが送受信されることはない (図 4).

N_i が正しくデータメッセージを N_{i+1} へと転送しない攻撃を行なった場合には, N_{i-1} から N_i へ転送されたデータメッセージ m が N_i によって N_{i+1} へと転送されない,

[*1] この条件の緩和については後述する.
[*2] あるいは攻撃ノードではあるが実際には攻撃を行なっていない場合.

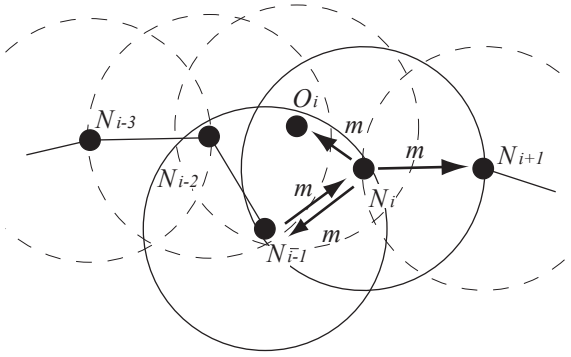

図 4 攻撃無線ノードのないデータメッセージ配送.

N_i によって m と異なるデータメッセージ m' が N_{i+1} へと転送される, N_{i-1} がデータメッセージを N_i へ転送していないにも関わらず N_i が N_{i+1} へデータメッセージを送信する, のいずれかが N_{i-1} と O_i によって検出される (図 5). このとき、N_i を攻撃ノードとして検出したとする *Mdet* メッセージが N_{i-1} から N_{i-2} へ送信されるとともに, O_i から も同じ *Mdet* メッセージが N_{i-2} へ送信される. したがって, N_{i-2} は N_i を攻撃ノードとして検出したとする 2 つの *Mdet* メッセージを受信する.

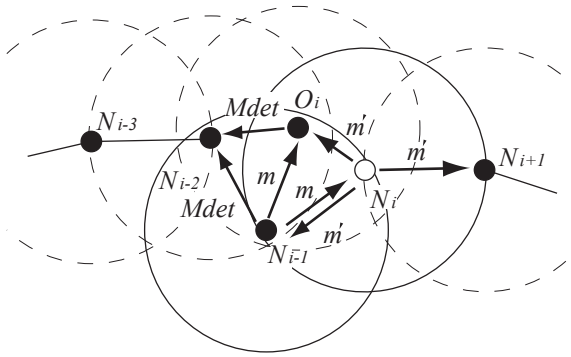

図 5 N_i による攻撃の検出と通知.

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} が N_{i-1} から受信することが考えられる (図 6). このとき, N_{i-1} が N_i へと転送したメッセージと N_i が N_{i+1} へと転送したメッセージの両方を受信する O_i は N_i が攻撃ノードではないと判断できる. そのため, N_i が攻撃ノードではないにも関わらず N_{i-1} が 偽の *Mdet* メッセージを送信していることを, これを受信 (傍受) する O_i は検出可能である. そこで, O_i は 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_{i-2} へ送信する. したがって, N_{i-2} は N_i を攻撃ノードとして検出したとする *Mdet* メッセージと N_{i-1} を攻撃ノードとして検出したとする *Mdet* メッセージとを受信する.

Vol.2016-DPS-168 No.1
Vol.2016-SPT-21 No.1
Vol.2016-EIP-74 No.1
2016/11/17

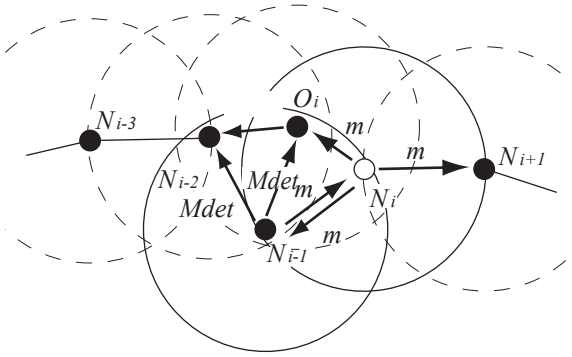

図 6 N_{i-1} による攻撃の検出と通知.

同様に, O_i が攻撃ノードであり, N_i が攻撃ノードではなににも関わらず O_i 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} が O_i から受信することが考えられる (図 7). このとき, N_{i-1} が N_i へと転送したメッセージと N_i が N_{i+1} へと転送したメッセージの両方を受信する N_{i-1} は N_i が攻撃ノードではないと判断できる. そのため, N_i が攻撃ノードではないにも関わらず O_i が 偽の *Mdet* メッセージを送信していることを, これを受信 (傍受) する N_{i-1} は検出可能である. そこで, N_{i-1} は O_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-2} へ送信する. したがって, N_{i-2} は N_i を攻撃ノードとして検出したとする *Mdet* メッセージと O_i を攻撃ノードとして検出したとする *Mdet* メッセージとを受信する.

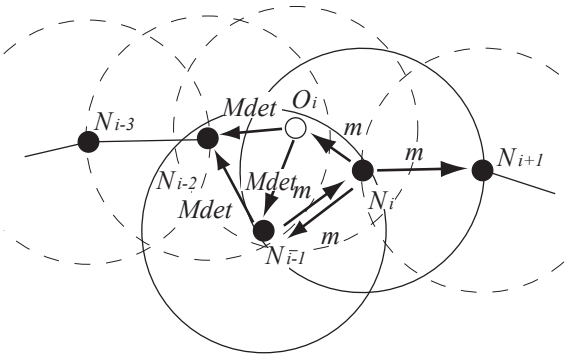

図 7 O_i による攻撃の検出と通知.

最後に, N_i が攻撃ノードではないにも関わらず O_i もしくは N_{i-1} のいずれかが攻撃ノードであり, 他方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-2} へと送信することが考えられる (図 8). この場合, O_i と N_{i-1} は互いが送信した 偽の *Mdet* メッセージを受信 (傍受) することができることから, この攻撃ノード検出に対応する *Mdet* メッセージを N_{i-2} へと送信することとなる. 結果として, N_{i-2} は N_{i-1} と O_i をそれぞれ攻撃ノードとして検出したとする 2 つの *Mdet* メッセージを受信する.

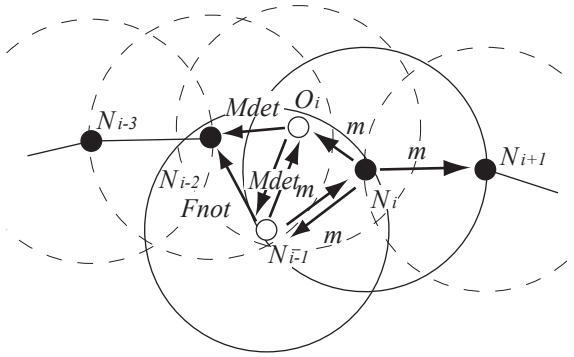

図 8 O_i もしくは N_{i-1} による攻撃の検出と通知.

表 1 に示すように, N_{i-2} が N_i を攻撃ノードとして検出したとする *Mdet* メッセージを含む 2 つの *Mdet* メッセージを O_i と N_{i_1} から受信した場合には, N_i, N_{i-1}, O_i のいずれが攻撃ノードであるかを N_{i-2} が検出することができる. 一方, O_i と N_{i-1} が互い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-2} に送信した場合はいずれかを攻撃ノードであると特定できるかを考察する. 前三者については必ず N_i を攻撃ノードとして検出したとする *Mdet* メッセージが N_{i-1} または O_i から N_{i-2} へと送信される. これは, 送信されるメッセージによってのみ攻撃ノードを検出することができるためである. これに対し, 最後のケースについてはデータメッセージの転送のタイミングあるいは転送されるデータメッセージとは独立に *Mdet* が送信されるが, このような送信は攻撃ノードの検出と無関係になされたものであると判断できる. したがって, O_i と N_{i-1} から互いに他を攻撃ノードとして検出したとする *Mdet* メッセージを受信した場合, N_{i-1} は先に *Mdet* メッセージを送信したノードが攻撃ノードであると判断できる.

表 1 N_{i-2} が受信する攻撃検出メッセージ.

N_{i-1} からの *Mdet* が示す攻撃ノード	O_i からの *Mdet* が示す攻撃ノード	攻撃ノード
N_i	N_i	N_i
N_i	N_{i-1}	N_{i-1}
O_i	N_i	O_i
O_i	N_{i-1}	N_{i-1} または O_i

ここで, 攻撃ノードである中継無線無線ノード N_i が N_j $(j > i+1)$ を攻撃ノードとして検出したとする *Mdet* メッセージの N_0 への配送を開始する場合が考えられる (図 9). 本来, N_{j-1} および O_j が送信した N_j を攻撃ノードとして検出したとする *Mdet* メッセージは N_{j-2} から N_0 へと配送される. ただし, 上に示したように N_j を攻撃ノードとして検出したとする *Mdet* メッセージが N_i から N_{i-1} へと

Vol.2016-DPS-168 No.1
Vol.2016-SPT-21 No.1
Vol.2016-EIP-74 No.1
2016/11/17

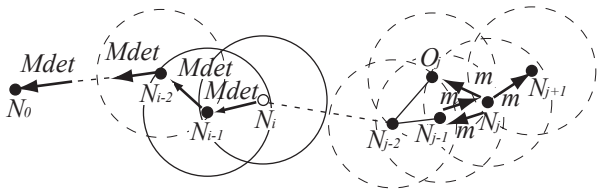

図 9 攻撃ノード検出通知の誤配送.

転送されるのは N_j が攻撃ノードであることが N_{j-2} において確認された場合であることから, 攻撃ノードは 1 台のみとする本論文の仮定により N_{i-1} は受信した $Mdet$ メッセージを無条件に N_{i-2} へと転送して問題がないはずである. ただし, ここで問題とした N_i が攻撃ノードであって, このような偽の $Mdet$ メッセージの配送を開始する場合には, これを転送する N_k $(0 < k < i)$ は N_i が攻撃ノードであることを検出することができないため, N_j を攻撃ノードとして検出したとする $Mdet$ メッセージが N_0 へと誤配送されることとなる. この誤りは, N_i と N_{i+1} の隣接無線ノードである O_i によって検出可能である. N_i は, N_{i+1} から転送された N_j に関わる $Mdet$ メッセージを転送しなければならないにも関わらず, N_{i+1} から送信されていないまま N_i が N_{i-1} へと送信することを検出できるからである. これを検出した O_i は N_{i-2} へその $Mdet$ メッセージが誤りであることを通知可能である. しかし, これを通知する手法を導入すると $Mdet$ メッセージの配送を 1 ホップずつ正当であることを確認しながら行なうこととなり, その配送遅延が拡大する. 本論文では, $Mdet$ メッセージにはその送信元無線ノードの識別子を含み, さらにそのデジタル署名を付与することにより, 中継無線ノードは無条件に $Mdet$ メッセージを転送し, N_0 によって $Mdet$ メッセージの正当性を確認することとする.

3.3 監視可能経路

前節で述べたように, 偽のデータメッセージを送信する攻撃ノードに加えて, 偽の攻撃ノード検出メッセージを送信する攻撃ノードを検出することが可能な無線マルチホップ配送を実現するためには, 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 $\mathcal{R} := ||N_0 \dots N_n\rangle\rangle$ を構成するすべての無線リンク $|N_iN_{i+1}\rangle$ が監視可能でなければならない. ここで, $|N_iN_{i+1}\rangle$ が監視可能であるのは, 以下の条件を満たす場合である.

[監視可能無線リンク]

$|N_iN_{i+1}\rangle$ が監視可能無線リンクであるのは, N_{i-2} , N_{i-1} , N_i すべてと隣接する監視無線ノード O_i が存在する場合である (図 10). □

このように, $|N_iN_{i+1}\rangle$ が監視可能リンクであるか否かの判定には N_{i-2}, N_{i-1} との隣接関係が影響する. このため, N_i のすべての隣接ノードの隣接ノード集合, すなわち N_i

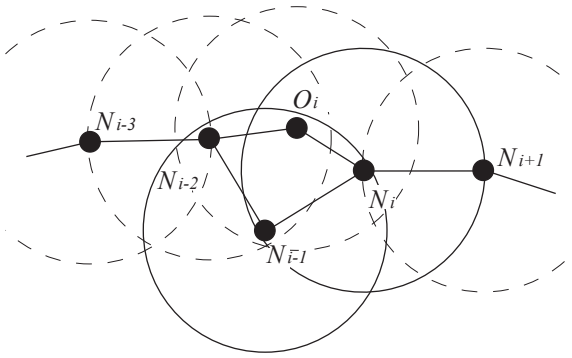

図 10 監視可能無線リンク.

がその 2-hop 隣接無線ノード関係を取得することが求められている. これには一般的に以下のふたつの方法が考えられる.

[無線ノードの位置情報を用いる手法]

各無線ノードが自身の位置情報を GPS レシーバ等により取得可能であるならば, 各無線ノードが取得した位置情報を含む制御メッセージを隣接無線ノードへブロードキャスト送信する. これによって, N_i は自身の隣接無線ノードとそれらの隣接関係を得ることが可能となり, 前ホップ中継無線ノード N_i に対して, 監視可能リンクで接続された次ホップ無線ノード候補を決定することができる. □

[無線ノードの位置情報を用いない手法]

各無線ノードは, 自身と隣接無線ノードの識別子を含む制御メッセージを隣接無線ノードへブロードキャスト送信する. これによって, N_i は自身の隣接無線ノードとそれらの隣接関係を得ることが可能となり, 前ホップ中継無線ノード N_i に対して, 監視可能リンクで接続された次ホップ無線ノード候補を決定することができる. □

これによって, AODV を拡散することで制御メッセージのフラッティングを用いた経路探索プロトコルを構築することができる.

3.4 監視中継無線ノードによる経路検出率の改善

前節の要件に従って監視可能無線リンクのみによって構成される無線マルチホップ配送経路では, 本論文が対象としているデータメッセージと攻撃ノード検出通知メッセージの偽装に対して, その送信無線ノードを攻撃ノードとして検出することができる. しかし, 監視無線ノード O_i は無線マルチホップ配送経路の連続する 3 つの中継無線ノードに共通の隣接無線ノードでなければならず, この O_i がすべての無線リンク $|N_iN_{i+1}\rangle$ 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 11). O_i は N_i のデータ

Vol.2016-DPS-168 No.1
Vol.2016-SPT-21 No.1
Vol.2016-EIP-74 No.1
2016/11/17

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.

なお, このとき, 新たに I_i を導入することによって, I_i が攻撃ノードである可能性を考えなければならなくなる. そこで, I_i が攻撃ノードである場合にこれを検出する方法について示す. I_i が送信するメッセージは O_i が送信する攻撃ノード検出メッセージ *Mdet* のみである. すなわち, N_i または N_{i-1} を攻撃ノードとして検出したとする *Mdet* のみである. これらの *Mdet* メッセージは本来 O_i から送信されたものであるが, これらを O_i が送信していない, あるいは, O_i が送信したものとは異なる *Mdet* メッセージを N_{i-2} に送信している場合には, I_i が送信した *Mdet* メッセージを O_i が受信 (傍受) することによって検出できる. このとき, O_i は I_i を攻撃ノードであるとして検出したとする *Mdet* メッセージを $Ni-1$ を経由して N_{i-2} へと配送する. これによって, N_{i-2} は他の場合と同様に 2 つの *Mdet* メッセージを受信する. 一方, N_{i-1} あるいは O_i が I_i を攻撃ノードであるとして検出したとする *Mdet* メッセージを送信する (O_i からは N_{i-1} を経由して N_{i-2} へと配送される) ことが考えられる. この場合にも N_{i-1} が攻撃ノードである場合には O_i が, O_i が攻撃ノードである場合には I_i がそれぞれ検出し, *Mdet* メッセージを直接あるいは I_i を経由して N_{i-2} へと配送される. したがって, N_{i-2} は他の場合と同様に 2 つの *Mdet* メッセージを受信する. これらの *Mdet* メッセージの配送状況は, 3.2 節における O_i と N_{i-1} とがともに *Mdet* メッセージを N_{i-2} へと送信する場合と同じである. つまり, 2 つの *Mdet* メッセージのうち, あとから受信される *Mdet* メッセージが正しく, この *Mdet* によって通知される攻撃ノードが正しい攻撃ノードである.

4. 評価

3 章で提案したプロトコルにより, データメッセージの無線マルチホップ配送時に発生する中継無線ノードによる二種類の攻撃, すなわち, 偽のデータメッセージ送信と偽の攻撃ノード検出メッセージ送信を検出し, 正しい攻撃検出メッセージを送信元無線ノードへ配送することができる. ここで, 監視可能無線リンクのみから構成される無線マルチホップ配送経路の探索には, 通常の AODV における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* の検出配送経路 $\mathcal{R}$ に沿ったユニキャスト配送のみが用いられており, 追加の制御メッセージ交換や同期による時間オーバヘッドは要さない. ただし, 隣接無線ノードが監視可能無線リンクで接続された次ホップ無線ノード候補であるか否かを定めるためには 2 ホップ隣接関係を得ることが必要であるため, 3.3 節で述べたように, 各無線ノードが自身の位置情報もしくは隣接無線ノード識別子を含む制御メッセージを経路探索要求とは独立にブロードキャスト送信することが求められる. 一方, 提案プロトコルでは, 中継無線ノードによる攻撃が行なわれない場合には, データメッセージが $\mathcal{R}$ に沿って配送されるのみであり, 追加の制御メッセージを要さない. すなわち, 中継無線ノードによる攻撃が検出されるまでは, 提案手法では追加制御メッセージの交換や同期による遅延などのオーバヘッドは要さない.

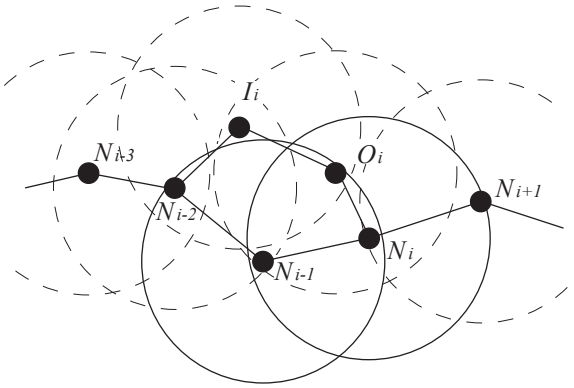

図 11 監視中継無線ノードによる経路検出率の改善.

制御メッセージの配送が必要となるのは, 中継無線ノード N_{i-1} および監視無線ノード O_i から N_{i-2} までの攻撃ノード検出通知メッセージ *Mdet* の配送と送信元無線ノード N_0 までのこのメッセージの転送のみである. ふたつの *Mdet* メッセージ配送は N_{i-2} で同期されるため, その時間オーバヘッドが追加となる.

提案手法では, データメッセージ配送に用いられる無線マルチホップ配送経路が監視可能無線リンクのみで構成されることが必要である. 無線マルチホップネットワークのすべての無線リンクを経路の一部として含むことができないことから, 経路検出率が低下することが考えられる. そこで, 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 0–2,000 台を一様分布乱数に基づいてランダムに配置する. 図 12 に示す固定位置に送信先無線ノードと送信元無線ノードを配置する. 無線ノードの 1,000 通りの異なる配置について, 無線マルチホップ配送経路検出の可否を調べ経路検出率を測定する.

実験結果を図 13 に示す. ここでは, X 軸を無線ノード数, Y 軸を送信元無線ノードから送信先無線ノードまでの距離, Z 軸を経路検出率としている. 提案手法における経路検出

Vol.2016-DPS-168 No.1
Vol.2016-SPT-21 No.1
Vol.2016-EIP-74 No.1
2016/11/17

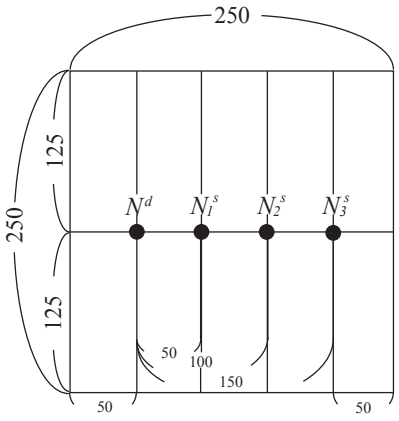

図 12 シミュレーション実験領域.

率は, 比較のために測定した AODV による経路検出率と同様, ノード密度が高く, 送信元無線ノードから送信先無線ノードまでの距離が短いほど高くなっている. 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. 1,100 台以下では, 無線ノード密度そのものが低すぎるため AODV でも経路検出が困難である. 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の向上し, 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. このように, 無線ノードが低密度に分布する環境では監視無線ノードの配置が困難な場合が増加し, 十分な経路検出率が得られないという問題はあるものの, 中高密度分布においては, 追加制御メッセージの交換等の通信オーバヘッドを要することなく攻撃ノードを検出できる提案手法の有効性の高さが認められると考えられる.

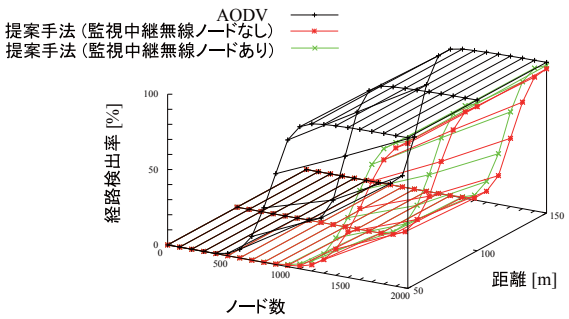

図 13 無線マルチホップ配送経路検出率.

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. また, 監視無線ノードによる攻撃もこれらが相互監視することによって実現している. 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. 提案手法は, 経路探索とデータメッセージ配送において追加の制御メッセージ交換を要することなく実現される. シミュレーション実験の結果, 低下した経路検出率に改善が認められたものの, AODV に対する経路検出率の低下は依然として大きいことが明らかになった. この経路検出率の改善が今後の課題である.

参考文献

[1] Asghari-Pari, S.M., Salehi, M.J., Noormohammadpour, M., “An Incentive-Based Leader Selection Mechanism for Mobile Ad-hoc Networks (MANETs),” Wireless Days (WD)2013 IFIP, (2013).

[2] Balakrishnan, K., Deng, D. and Varshney, P., “TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks,” Proceedings of the Wireless Communication and Networking Conference (WCNC), vol. 4, pp. 2137–2142 (2005).

[3] Hernandez-Oralio, E., Olmos, MD.S., Cano, J.C., Calafate, C.T. and Manzoni. P., “CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes,” IEEE Transactions on Mobile Computing, vol. 14, no. 46 pp. 1162–1175 (2015).

[4] Imran, M., Khan, F.A., Abbas, H. and Iftikhar, M., “Detection and Prevention of Black Hole Attacks in Mobile Ad hoc Networks,” Ad-hoc Networks and Wireless, vol. 8629, pp. 111–122 (2015).

[5] Kurkure, A.M., Chaudhari, B., “Analysing credit based ARAN to detect selfish nodes in MANET,” Proceedings of the International Conference on Advances in Engineering & Technology Research (ICAETR), (2014).

[6] Luo, J., Fan, M., Ye, D., “Black Hole Attack Prevention Based on Authentication Mechanism,” Proceedings of the International Conference on Communication Systems (ICCS), pp. 173–177 (2008).

[7] Martl, S., Giuli,T.J., Lai, K. and Baker, M., “Mitigating routing misbehavior in mobile ad hoc networks,” International Conference on Mobile Computing and Networking (MobiCom), pp. 255-265 (2000).

[8] Perkins, C., Belding-Royer, E. and Das, S., “Ad Hoc On-Demand Distance Vector (AODV) Routing,” RFC 3561 (2003).

[9] Rodriguez-Mayol, A. and Gozalvez, J., “Reputation based selfishness prevention techniques for mobile ad-hoc networks,” Telecommunication Systems, vol. 57, no. 2, pp. 181–195 (2014).

[10] Urrutia, J., “Two Problems on Discrete and Computational Geometry,” Proceedings of Japan Conference on Discrete and Computational Geometry, pp. 42–52 (1999).