アドホックネットワークにおける高精度な不正動作ノードの検出と防御方式の提案および実装評価

横山 信[†1,†2] 中根由和[†1]
高橋 修[†2] 宮本衛市[†2]

基地局を必要とせず，近隣の通信端末どうしで構成されるモバイルアドホックネットワークは，情報洪水時代のネットワークサービスを支える情報家電やセンサネットワークに有効な技術であるばかりでなく，P2P 技術との親和性も高く，ユーザ同士のコミュニティにおける新しいアプリケーションを創出する機会を提供している．しかし，アドホックネットワークには，無線インタフェースに起因する様々なセキュリティ上の課題が存在する．たとえば，パケットの盗聴が行われたり，ルーティングを混乱させてネットワークを成り立たせなくしたりする様々な攻撃がありうる．本論文では，パケットを相互に送受信することによって成り立つユーザ同士のコミュニティにおけるアドホックネットワークを想定し，そのようなネットワークに対して行われる攻撃について述べる．また，利己的な動作を行うノード（セルフィッシュノード）は，ネットワークへの攻撃を目的としないが，自己の送受信するパケットの転送を他のノードに要求する一方，自己は極力他のノードのパケットの中継を行わないため，他のノードの帯域幅や電力などの資源を消費する．そのようなノードが増加すると，ネットワークの可用性が低下し，最終的に通信不能となるため，セキュリティ上の重大な問題を引き起こす．そこで，それらのアドホックネットワーク中の不正ノードを，相互監視の方法により検出し，排除する「witness 方式」を提案し，シミュレーションにより提案方式の有効性を実証評価する．

A Proposal of Security System with High-precision Detection of Misbehaving Nodes in Ad Hoc Network and Its Evaluation of Implementation

Shin Yokoyama,[†1,†2] Yoshikazu Nakane,[†1] Osamu Takahashi[†2] and Eiichi Miyamoto[†2]

Mobile ad hoc network relays packets mutually among users' nodes in a network without base stations, which is an essential technology for platform of information sharing space in the near future. It is close to P2P technology that provides chance to enable novel applications for users' communities. However, ad hoc network technology has various issues concerning about security which come from wireless interfaces, for example, tapping of packets and several routing disruption attach which destroy networks. In this paper, we assume ad hoc networks relay packets mutually among users' nodes, which are used in users' community, and we describe attacks for such networks. On the other hand, selfish nodes that have no intention of attacking networks but take advantage of other nodes and do not cooperate with others, make network resources unavailable for legitimate nodes. This problem is categorized as a security issue. Therefore, we propose a security system "witness method" based on mutual watching that detects and excludes such illegal nodes and evaluate the method as well.

1. はじめに

モバイルコンピューティングは急速に発展しており，これにともなって，通信端末の増加が見込まれている．1 人に 1 台の携帯電話が世界的に普及しつつあるというだけでなく，人々が身に着け，持ち歩いている様々な機器や，分散して配置される各種のセンサが通信するようになることを考慮すると，その数は現在の数倍から数十倍になると考えられる．また，小型の通信端末では省電力化のため，電波の出力や到達範囲の制約がある．

そのような状況下では，現状の移動体通信の一般的な形態である基地局と端末が個別に直接のリンクを確立する方法だけでは，帯域幅の確保，基地局の配置お

†1 日本情報通信コンサルティング株式会社
Nippon Information Technology Consulting Co., Ltd.
†2 公立はこだて未来大学
Future University-Hakodate

よび省電力化のうえで困難を生じることが予想される．そこで，近くのノードどうしで構成される，アドホックネットワークの利用が有効となろう．

たとえば，あるユーザが携帯電話と別の電子機器類を持っており，それらがアドホックネットワークを形成することを考えると，電子機器類どうしは近距離で通信して，外部のネットワークへは携帯電話を介して接続する．これにより，帯域幅やバッテリの節約が可能になる．また，複数のユーザがそれぞれ所持する通信端末間で形成されるアドホックネットワークにより，基地局を介さず広範囲の通信が可能となる．

一方，アドホックネットワークは，様々な攻撃の脅威にさらされる可能性があり，それらへの対策を講じる必要がある．また，積極的な攻撃は行わないものの，ネットワーク全体に問題を引き起こしうる，利己的な動作をするノード（セルフィッシュノード）についても検討が必要である．

セルフィッシュノードにも対応可能な，不正動作からの防御方式はいくつか提案されているが，必ずしも正確にセルフィッシュな動作を検出できるとは限らず，正常なノードをセルフィッシュノードとして誤認したり，逆にセルフィッシュノードを発見できず見逃してしまったりする場合があった．本論文では，セルフィッシュノードの高精度な検出に重点を置いた「witness方式」を提案する．本方式は，相互監視を基本としてセルフィッシュノードに起因する問題の軽減を図っており，その効果をシミュレーションで評価して，本方式の有効性を示す．

以下，2章でアドホックネットワークのセキュリティに関する特徴について，3章で提案方式について述べる．4章でシミュレーションに基づく評価を行い，5章で結果を述べ考察する．6章では関連研究について述べ，7章でまとめる．

2. アドホックネットワークのセキュリティに関する特徴

2.1 複数ユーザの各ノード間での相互パケット転送

通常のアドホックネットワークでは，各ノードは単一の所有者の管理下にあり，行われる通信も所有者の目的の下に行われるという想定が多い．しかし，本論文での前提としては，所有者の異なるそれぞれのノードが相互かつ協力的にパケットを中継しあうことを想定している．

これにより，通信可能範囲は大きく広がり，様々なところでネットワークへの常時接続が可能となると期待される．

現状，実用レベルではそのような形態でのアドホックネットワークは見当たらないが，下記の動向の延長線上に実現・普及の可能性が十分にあると考える．

(1) 無線 LAN の展開

限られたエリアではあるが，ホテルや大学などの一部施設で無線 LAN によるインターネット接続を提供していることがある．また，FON[1] など，会員同士が自宅の無線 LAN アクセスポイントを相互に提供しあうサービスが登場してきている．

(2) ゲーム機などの IEEE802.11 無線 LAN 対応

IEEE802.11 無線 LAN を実装している主要な携帯可能なゲーム機は，ゲームに限らない用途やゲームをしない年齢層にも需要が広がっている．マルチホップの中継ではないが，アドホックモードでの通信はすでに可能であり，無線 LAN アクセスポイントから，インターネット接続も可能になっている．

(3) 携帯電話機の Bluetooth 対応

2006 年 11 月初旬，全世界での Bluetooth 搭載機器の累計出荷台数が 10 億台を超え，普及が進んでいる[2]．

Bluetooth は，2 つの端末どうしを直接接続するだけでなく，Piconet と呼ばれる小さなネットワークを構成することができ，さらに Piconet を複数接続した Scatternet と呼ばれるマルチホップのアドホックネットワークを構成することも可能である[3]．

(4) ITS の発展にともなう車載型通信端末の普及

車々間通信を利用して出会い頭の事故や追突を未然に防止するシステムや，交通渋滞や路面状況のリアルタイム情報を収集・配信する，高度化されたカーナビゲーションや，信号機と車が通信して，無停止で交差点を通過できるシステムなどが研究されている．

2.2 不正ノードの存在事由

不正ノードの存在事由としては，下記があげられる．

(1) ウィルス感染

現状のインターネットと同様に，悪意あるユーザによって作成されたウィルスなどが蔓延し，アドホックネットワークを攻撃の目標とする可能性がある．

(2) 妨害したい

インターネットで行われているように，悪意あるユーザによって，アドホックネットワークに対して妨害が行われる可能性がある．悪意あるユーザの割合はごくわずかであっても，影響度の大きい攻撃方法も存在する．

(3) 利得を得たい

自ノードの送受信は行うが他のノードのための中継動作をしないことによって，電力を節約したり，状況によっては，利用できる帯域も増加したりするといっ

表 1 アドホックネットワークでの不正動作
Table 1 Misbehaviors in ad hoc networks.

存在事由	不正動作の分類	影響
ウィルス等に感染	ルーティング	通信不能
妨害したい	混乱攻撃	
利得を得たい	セルフィッシュ動作	可用性の低下, 消費電力の増加, スループットの低下

た利己的な利得がある．ネットワークを利用することが目的であるため，ネットワークが利用不能になるような積極的な妨害を行うものではない．

2.3 アドホックネットワークにおける不正動作

アドホック・ルーティングプロトコルは各種提案されており，IETF で標準化されているものがあるが，セキュリティに関していまだ検討は不十分である．第 3 者が中継ノードとなるため，従来の通信インフラをベースとしたネットワークとは異なり，リスクが大きい．

不正動作は下記のように分類できる．

(1) 攻撃

ウィルスに感染したノードや，妨害を行うノードが，アドホックネットワークに対し攻撃を行う．攻撃は，レイヤごとの分類が可能であり，物理・データリンク層における攻撃であるジャミング，ネットワーク層における攻撃であるルーティング混乱攻撃がある．代表的なものとして blackhole 攻撃が知られている．文献 4) はこれらの攻撃について分類している．

(2) セルフィッシュ動作

自己の送受信するパケットの転送を他のノードに要求する一方，自己は極力他のノードのパケットの中継を行わない動作である．他のノードの電力などの資源を消費するので，協調的なアドホックネットワークにとって有害である．

以上のアドホックネットワークでの不正動作についてまとめると**表 1** のようになる．

少数の悪意あるノードによってネットワークが広範囲にわたり通信不能に陥ったり，セルフィッシュなノードの増加によって，ネットワークの可用性が損なわれたりする恐れがある．

そのため，協調的なアドホックネットワークを実用に供するためには，それらの不正動作をするノードへの対策が不可欠である．

2.4 不正動作の検出と防御

検出の方法に関しては，パケット転送の実施を転送経路上の 1 つ前のノードから観察する watchdog 方式[5] と，経路上の各ノードの転送数の報告の差異を用いる HADOF[6] の方式などがある．

文献 5) に述べられている方式では，パケット転送の経路に沿って，前のノードが次のノードの転送を watchdog で監視し，経路の信頼性を pathrater によって評価する．しかし，その論文自身に述べられているように，watchdog 方式は誤検出をはじめとするいくつかの問題をかかえている．

3. Witness 方式の提案

本論文では，アドホックネットワークの正常な利用の障害となりうる不正動作への対策を目的に，相互監視によるアドホックネットワークのセキュリティ方式である witness 方式を提案する．以下に，その基本的な考え方と動作の説明を行う．

3.1 Witness 方式の基本的な考え方

Witness 方式はアドホックネットワーク中の隣接する各ノードが相互に監視を行って，不正動作を検出し，排除することを基本とする．監視に基づいて検出を行う点で，IDS（Intrusion Detection System）的である．

また，監視の動作は，ルーティングと分離することが可能であるため，汎用性があり，様々な不正動作に対応することができる．同時に，仕組みを比較的単純にでき，分散的に行うことができる．基本的な方針としては，不正な動作を検出し，そのノードを無視することによって排除する．

HADOF[6] では，watchdog を使用せず，各ノードが定期的に受信パケット数と転送パケット数を送信元ノードに報告することによって，送信元が転送数の差異より不正を検出し，不正なノードを避けてルーティングを行う．ただしこの方式は DSR[7] など，ソースルーティングを行うプロトコルに依存している．

Witness 方式では，watchdog 方式を発展させ，通信経路に沿って前ホップのノードからだけでなく，通信経路に隣接するノードにも観察を行わせることによって，疑わしい状況が発生した場合にこれらのノードからも目撃者情報として情報を収集し判断に利用する．これによって，誤検出率を低くすることができる．また，ソースルーティングを行わない AODV[8] などのルーティングプロトコルにも適用可能である．

これらの方式の特徴をまとめて**表 2** に示す．

以下では，witness 方式をセルフィッシュ動作の検出に適用することに絞って説明する．

3.2 検出方式

図 1 において，ノード A がノード C へパケットを転送しようとしており，ノード A は経路がまだない

表 2 不正動作の防御方式とその特徴
Table 2 Defence method against misbehaviors and their features.

方式	特徴	対応可能な不正動作
Watchdog	前ホップのノードから次ホップのノードの動作を監視	セルフィッシュ動作
HADOF	経路上の各ノードが受信・転送パケット数を送信元に報告し，送信元で差異を検出	ルーティング混乱攻撃 セルフィッシュ動作
Witness（提案方式）	watchdog 方式を強化し，転送経路外の第3者ノードによる監視結果を利用して判定	ルーティング混乱攻撃 セルフィッシュ動作

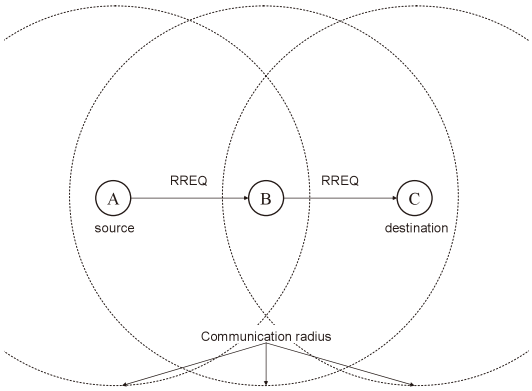


図 1 パケット転送の状況
Fig. 1 Situation of packet transfer.

ため，経路探索要求（RREQ）パケットを送信する．RREQ は隣接の各ノードでブロードキャストされて放射状に中継されていくが，図 1 では 3 つのノードだけを示している．ノード A からノード C へはパケットは直接届かないが，ノード B は，ノード A，ノード C 間を中継可能である．

しかし，ノード B がセルフィッシュノードであり，RREQ を中継しないという動作をとる可能性もある．

ここで，セルフィッシュノードの検出に関して，watchdog 方式とその問題点について述べ，続いて witness 方式について述べる．

(1) watchdog 方式とその問題点

従来の watchdog 方式では，パケットの転送経路に沿って，前のノードから次のノードによるパケットの中継を監視する．図 1 においては，下記の動作となる．

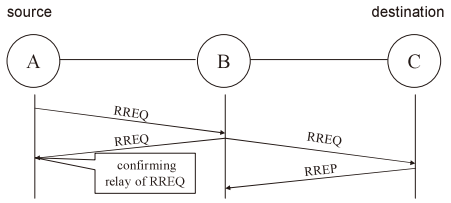


図 2 watchdog 方式における正常動作判定
Fig. 2 Decision of normal behavior in simple watchdog method.

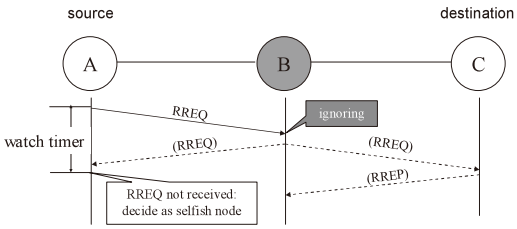


図 3 watchdog 方式におけるセルフィッシュ動作判定
Fig. 3 Decision of selfish behavior in simple watchdog method.

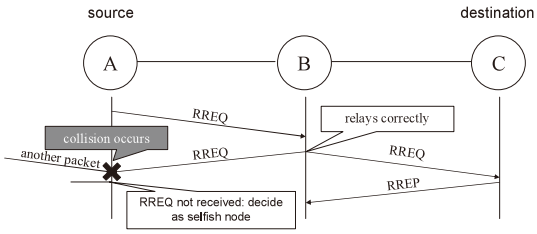


図 4 watchdog 方式で誤検出の起こる例
Fig. 4 A case that false detection occurs in simple watchdog method.

1) ノード A が送信したパケットは，ノード B が受信する．
2) ノード B は，そのパケットを中継し，ノード C が受信する．
3) それと同時に，ノード A もそのパケットを受信する．

3-1) ノード A がノード B の中継したパケットを受信した場合，ノード A はノード B を正常ノードと見なす（**図 2**）．（終了）

3-2) 一定時間内に，ノード A がノード B の中継したパケットを受信しなかった場合，ノード B がセルフィッシュノードであると判断する（**図 3**）．

Watchdog 方式では，ノード A が**図 4** のように別のノードからのパケットを受信している場合や，ノード A が別のパケットを送信している最中にノード B がパケットの中継を行った場合は，ノード A はノード B からのパケットを受信することができないため，

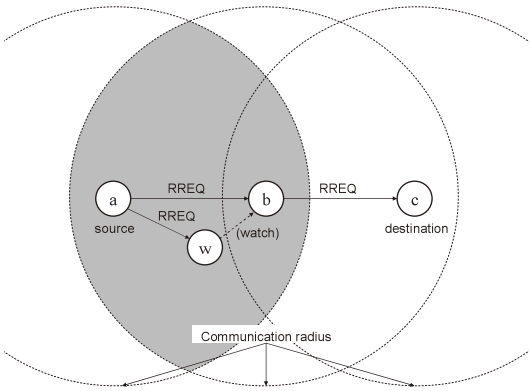


図 5 パケット転送の相互監視の状況
Fig. 5 Situation of mutual watching in packet transfer.

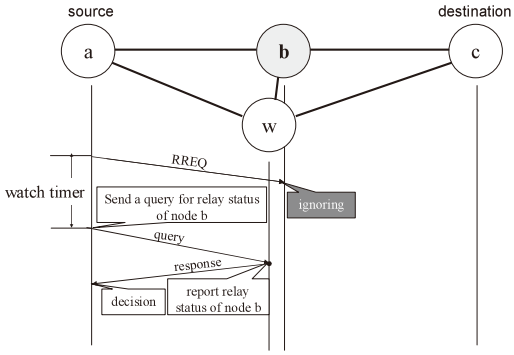


図 6 Witness 方式におけるセルフィッシュノードの判定
Fig. 6 Decision of selfish behavior in the proposal method.

ノード B がパケットを実際に中継したとしてもそれを確認することができない．結果的に，ノード A からは，ノード B が転送を行っていないように見え，ノード A はノード B をセルフィッシュノードと誤判定する．

以上より，ノード A からだけの監視では，ノード B がセルフィッシュノードとして誤判定される可能性がある．

(2) witness 方式

次に，提案の witness 方式がセルフィッシュノードを検出する方法を説明する．Witness 方式では，正常なノードが互いに隣接ノードの送受信状況を監視している．

Watchdog 方式では，本節 (1) の 3-2) において，セルフィッシュノードであることの判断を行うが，witness 方式では，この段階では判断を行わず，隣接ノードへ転送実績の問合せを行い，その応答によって判定を行う．

判定の方式は，転送実績の応答が 1 つもない場合に，正常ノードと見なす性善説型の「タイプ 1」とセルフィッシュノードと見なす性悪説型の「タイプ 2」の両方式を定義する．どちらをとるかによって，検出率と誤検出率が異なることが予想されるため，アプリケーションの要求に応じて選択して利用することを可能とする．

以下では，**図 5** を例に動作を説明する．ノード b は，ノード a とノード c 間のパケット中継が可能であり，ノード w は，ノード b を監視可能，かつ，ノード a と通信可能である．

1) ノード a が送信したパケットは，ノード b が受信する．
2) ノード b は，そのパケットを中継し，ノード c が受信する．
3) それと同時に，ノード a もそのパケットを受信する．

3-1) ノード a がノード b の中継したパケットを受信した場合，ノード a はノード b を正常ノードと見なす．(終了)

3-2) 一定時間内に，ノード a がノード b の中継したパケットを受信しなかった場合，ノード a は隣接ノードに，ノード b の転送実績の問合せのために，問合せパケットを送信する．

4) これを受信したノードのうち，ノード b と隣接していて，ノード a からの中継すべきパケットを受信しているノード（図 5 中，ノード w）は，応答パケットにより，ノード b の転送実績をノード a に応答する．
5) ノード a は，応答に従って次のように判定を行う．

5-1) 「転送実績あり」との応答が 1 つでもあった場合，正常ノードと判断する．(終了)

5-2) 「転送実績あり」との応答がまだ 1 つもなく，「転送実績なし」との応答があった場合，セルフィッシュノードと判断する．

5-3) 転送実績の応答が 1 つもない場合は，判定方式により判定する．判定方式がタイプ 1 の場合，正常ノードと見なし，タイプ 2 の場合，セルフィッシュノードと判断する．

図 6 に上記動作のパケット送受信シーケンスを示す．

なお，ノード a と同様にノード w でも衝突がおきて誤検出となる可能性もあるが，ノード a だけでなく複数のノードでパケットの中継動作を観察することによって，判定をより正確に行うことができる．

以上の判定動作を図示すると**図 7** のようになる．

初期状態では，各ノードは互いに隣接ノードは正常なノードであるとしている．セルフィッシュであると判定した場合，その判定結果は，それぞれのノードで，

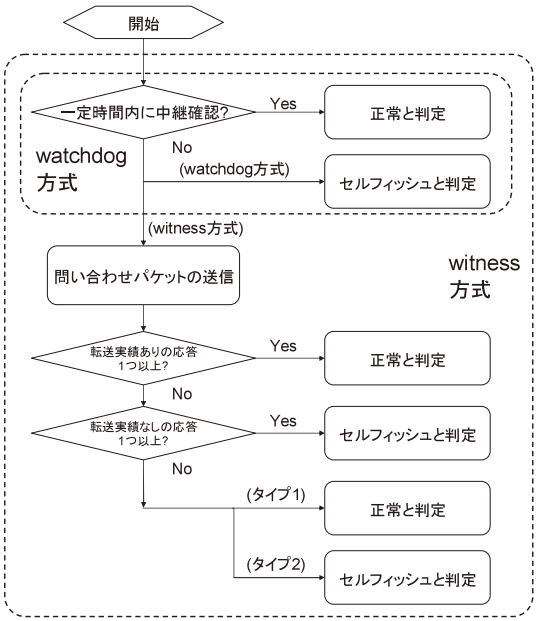


図 7 判定動作のまとめ
Fig. 7 Summary of decision method.

当該ノードのルーティングテーブルのエントリとともに保持され，そのエントリが破棄されるまで保持される．

各ノードとも，セルフィッシュであると判定したノードからのパケットは転送しないということによって，排除を行う．

また，誤検出によっていったんセルフィッシュノードと判定された場合においても，それ以降に転送を行ったことが確認できた場合には，セルフィッシュノードとしての判定を取り消すようにする．

4. シミュレーション評価

本方式の評価のため，ネットワークシミュレータ ns-2[9]，AODV-UU 0.8.1[10] を用い，セルフィッシュノードのネットワークに与える影響の定量的評価と提案する検出・防御方式の評価を行う．

前提としては，文献 6) 同様，暗号鍵による各ノードの認証が行われることを想定する．そのため，セルフィッシュノードが自身の転送実績を他のノードに問合せされたとき，他のノードになりすましを行って，転送実績ありと偽りの応答をすることは不可能である．

また，セルフィッシュノードが，隣接のセルフィッシュノードについて転送実績ありと偽りの応答をすることは，隣接のセルフィッシュノードを有利にするが，偽りの応答をしたセルフィッシュノード自身にとって有利にならない．逆に，隣接の正常ノードについて転送実績があるのに転送実績なしとして応答すると，隣接の正常ノードは誤判定されて除外されるが，結果的にセルフィッシュノード自身もそのノードを通じてパケットを送受信できなくなるため，セルフィッシュノード自身にとって有利にならない．そのため，セルフィッシュノードは偽りの応答はしないものと想定する．また，セルフィッシュノード以外に不正動作を行うノードは存在しないものと想定する．

表 3 シミュレーション条件
Table 3 Simulation parameters.

ノードの配置範囲	1000[m] x 1000[m]
ノードの移動	なし
無線方式	IEEE 802.11 （送信レート 2[Mbps]）（Lucent WaveLAN DSSS 無線インタフェースをシミュレート）
無線到達距離	250[m]

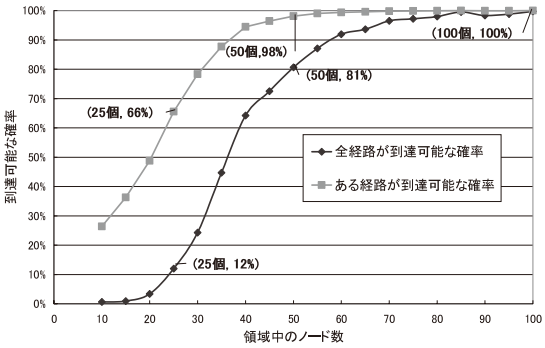


図 8 ノード密度と経路の到達確率の関係
Fig. 8 Node density vs. route reachability.

シミュレーション条件は**表 3** のとおりである．

4.1 ノード密度と到達可能性

シミュレーションを実行するのに妥当なノード密度を決定するために，表 3 の条件でノードをランダムに配置するとき，配置範囲中のノード数に対して，それらノード間の全経路が到達可能になる確率，ならびに，ある経路が到達可能な確率を求めた．結果を**図 8** に示す．

ノード数 50 では，98%の経路が到達可能な状態になり，ノード数 80 以上のとき，98%以上の確率で，すべての経路が到達可能になる．

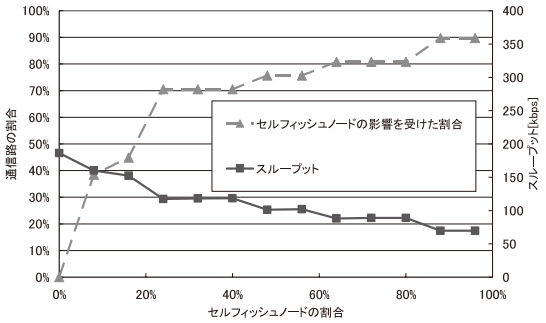
このため，セルフィッシュノードが存在しないときにほとんどのノードが通信できるノード数 50 以上の状況でシミュレーションを行うのが適切である．

4.2 セルフィッシュノードの影響

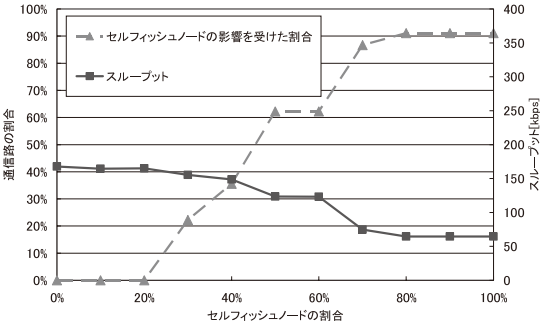
セルフィッシュノードの割合と，影響を受ける通信路の割合の関係を**図 9** に示す．

ノード密度が低いとき，セルフィッシュノードの割合が増加すると，影響が顕著に現れる．これは，セル

a) ノード数 25 の場合



b) ノード数 50 の場合



c) ノード数 100 の場合

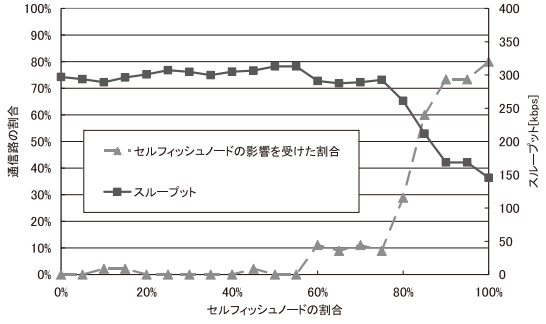


図 9 セルフィッシュノードの増加にともなうネットワークへの影響
Fig. 9 Impact on a network with increasing number of selfish nodes.

フィッシュノードの代わりに中継が可能なノードの数の違いによると考えられる．

なお，セルフィッシュノードの割合が 100%の場合においてもスループットが 0 にならないのは，通信する 2 つのノードが隣接している場合があり，中継ノードによらず直接の通信が可能であるためである．

ノード数 50 の場合，セルフィッシュノードの割合が 50%前後のところで影響が出やすくなっている．そのため，以下のシミュレーションでは，ノード数 50，セルフィッシュノードの割合 50%（25 個）で評価を行う．

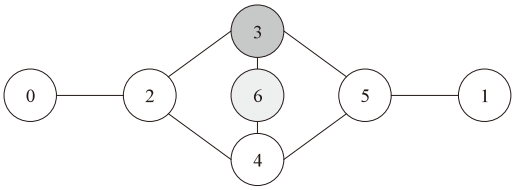


図 10 小規模モデル（その 1）
Fig. 10 Micro model (No.1).

4.3 提案方式の評価

以下の評価では，表 3 のシミュレーション条件のもとに，小規模モデル，大規模モデルを用いて行う．

小規模モデルでは，最も単純化された形で，watchdog 方式と提案の witness 方式の比較を行い，大規模モデルでは，より実用に近い形での性能の比較を行う．評価指標については，以下のとおりである．

(1) 評価指標

以下の検出率と誤検出率を用いる．

- 検出率 R_d（detection Ratio）
  正常ノードが，隣接するセルフィッシュノードをセルフィッシュノードと判定できた割合である．100%に近いほど，性能が良い．
- 誤検出率 R_f（false detection Ratio）
  正常ノードが，隣接している正常ノードを誤ってセルフィッシュノードと判定した割合である．低いほど，性能が良い．

(2) 評価モデル

以下の小規模モデル・大規模モデルを評価に用いる．

1) 小規模モデル

小規模なモデルで，watchdog 方式と witness 方式を比較して効果を確認する．

セルフィッシュノードが存在するときに，どれだけ正確にこれを検出できるかどうかを見る．

まず，検出率を求めるために，**図 10** に示す小規模なモデルを用意した．この図において，ノード 3 だけがセルフィッシュノードである．FTP 的な通信がノード 0 からノード 1 へ行われるとき，ルートの確立のために，RREQ パケットがノード 0 からフラッディングされる．ノード 3 はセルフィッシュノードであり RREQ パケットを中継しない．ノード 4 は，ノード 3 による中継の状況を観察できる位置に配置されている．なお，ノード 6 は，ストリーミングなどのアプリケーションによって混雑したネットワークのトラヒックを模擬し，1.09 [Mbps] のブロードキャスト送信を行っている．

この状況で，100 回のシミュレーション試行を行い，全試行のうち，ノード 2 が，セルフィッシュノードであ

るノード 3 を検出できた割合を検出率 R_d（detection Ratio）とする．

さらに，誤検出率を求めるために，**図 11** のモデルを用意する．図 10 との違いは，ノード 3 も含めすべてが正常ノードであることである．検出率の評価と同様に行い，全試行のうち，ノード 2 が，正常ノードであるノード 3 をセルフィッシュノードとして誤検出する割合を誤検出率 R_f（false detection Ratio）として求める．

2) 大規模モデル

図 12 の大規模モデルを用いて，各方式のセルフィッシュノードの検出性能および対策の効果を評価する．このモデルでは，セルフィッシュノードが 25 個，正常なノードが 25 個存在する．このモデルは，たとえば小規模な大学などで，学生同士が各自のノート PC を利用して，管理されていないアドホックネットワークを展開した場合などに適用可能である．

1 回の試行につき，5 組のノードの対をランダムに選択して，それぞれの組で 1 方向の一定レートのデータ送信（1.09 [Mbps]，ユニキャスト）を行わせた後，正常な各ノードによる判定結果を記録する．

これを，49 通りの組合せで試行し，検出率と誤検出率を算出する．大規模モデルにおける検出率と誤検出率については，以下のように計算する．

- 検出率 R_d（detection Ratio）

$$R_d = \frac{N_d}{N_s} \tag{1}$$

N_s（Number of Selfish nodes）は，すべての正常ノードについて，それぞれが隣接するセルフィッシュノードの数を合計した値である．

N_d（Number of selfish nodes Detected）は，すべての正常ノードについて，それぞれが隣接しているセルフィッシュノードをセルフィッシュノードと判定できた数を合計した値である．

- 誤検出率 R_f（false detection Ratio）

$$R_f = \frac{N_f}{N_n} \tag{2}$$

N_n（Number of normal nodes）は，すべての正常ノードについて，それぞれが隣接する正常ノードの数を合計した値である．

N_f（Number of normal nodes falsely detected）は，すべての正常ノードについて，それぞれが隣接している正常ノードをセルフィッシュノードと誤判定した数を合計した値である．

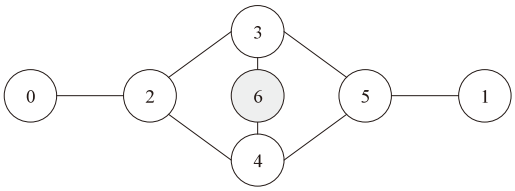


図 11 小規模モデル（その 2）
Fig. 11 Micro model (No.2).

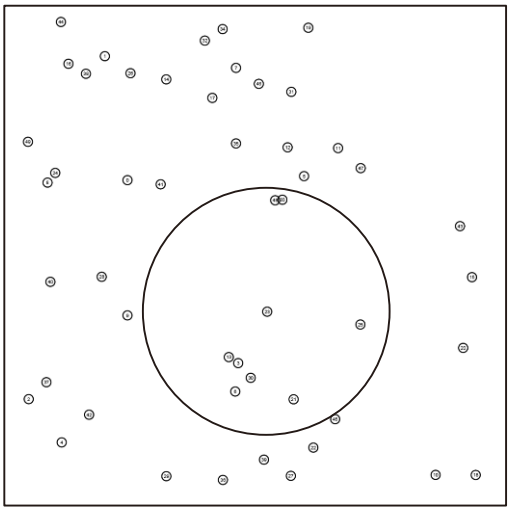


図 12 大規模モデル
Fig. 12 Macro model.

5. 評価の結果と考察

小規模モデルの評価の結果を**表 4** に示す．

小規模モデルにおいて，watchdog 方式の検出率は 100%である．しかし，誤検出率が 20%である．witness 方式（タイプ 1）は検出率が半分程度に下がるものの，誤検出の確率を 2%に低減できている．また，witness 方式（タイプ 2）では，誤検出率は watchdog 方式の半分で，検出率は 100%となっている．

次に，**表 5** に大規模モデルの評価の結果を示す．大規模モデルでは，隣接ノードが多くなるため衝突が発生しやすくなり，セルフィッシュノードの正常な検出

表 4 小規模モデルの結果
Table 4 Result of micro model.

	検出率 R_d	誤検出率 R_f
watchdog 方式	100%	20%
witness 方式（タイプ 1）	57%	2.0%
witness 方式（タイプ 2）	100%	10%

表 5 大規模モデルの結果
Table 5 Result of macro model.

	検出率 R_d	誤検出率 R_f
watchdog 方式	100%	24.8%
witness 方式（タイプ 1）	19.4%	1.75%
witness 方式（タイプ 2）	100%	15.3%

が困難になる．watchdog 方式では，小規模モデルの誤検出率に比べて大規模モデルでの誤検出率がやや増加しているのに対し，witness 方式（タイプ 1）では小規模モデルと同程度の誤検出率を保っている．一方，witness 方式（タイプ 1）での検出率は，小規模モデルと比べて大きく低下している．これは，ノードが比較的まばらなため，監視を行うノードが見当たらず，問合せに対する応答が得られない場合は，誤検出を避けるために，セルフィッシュノードであるとの判定をしないためである．Witness 方式（タイプ 2）は，検出率は 100%を保ったまま，誤検出率を watchdog 方式の 2/3 程度に軽減できている．

5.1 セルフィッシュ動作検出の性能

セルフィッシュノードの検出の際，誤検出されて転送拒否の措置を受けると，そのノードは通信不能になって大きな被害をこうむる可能性が大きい．一方，セルフィッシュノードは，攻撃を行うものではないため少数では影響は小さい．そこで，まず誤検出率は極力低く抑えたうえで検出率を保つのが望ましい．また，まったく対策をしないのでは，本来意図された協調を保つことが難しくなり，アドホックネットワーク全体として本来のパフォーマンスを発揮できなくなると予想される．そのため，転送拒否によって，ユーザが各自のノードにセルフィッシュ動作をさせることの利得と動機を失わせることが望ましい．

Witness 方式（タイプ 1）は watchdog 方式に比べ，検出率が低下するものの誤検出率を抑えることができるので，上記の観点により適合していると考えられる．Witness 方式（タイプ 2）は，検出率を 100%に保ったまま誤検出率を低減させることができている．これらの動作方式（タイプ 1・2）は，アプリケーションの要求などの状況に合わせて選択が可能である．

Witness 方式では，不正動作が疑われたとき，問合せ・応答を行うため，オーバヘッドが生じる．これは 1 つのセルフィッシュノードの存在が疑われた場合につき，隣接ノードとの間の 1 回の問合せ・応答シーケンスで完了するため，複数のホップで送信されうる RREQ よりも小さい負荷となり，無視できると考えられる．

また，一定の割合で転送がなくても転送があったと偽りの報告をするノードがあると，隣接のセルフィッシュノードが検出されなくなる．しかし，4 章で述べたように偽りの報告で利得の増加はない．逆に，転送実績が確認されているのに転送実績なしと偽りの報告をするノードがあると，正常なノードが誤検出されて転送拒否される可能性がある．しかし，図 7 に示した判定アルゴリズムにより，witness 方式が watchdog 方式より誤検出率が高くなることはない．また，他の隣接ノードから転送実績ありとの報告が 1 つ以上あれば，誤検出は避けられる．

5.2 他の不正動作の検出に対する拡張性

本論文では，不正動作のうちセルフィッシュ動作，さらに，RREQ を転送しない動作について評価を行っている．不正動作の判定を行うノードが，自らの監視だけによるのではなく，周囲のノードに問合せを行い，それらからの応答をもとに判定をする方式は，その他のセルフィッシュ動作，またはルーティング混乱攻撃にも対応可能である．

また，本提案方式は，ルーティングプロトコル側の動作に変更を加えるものではない．受動的な監視と，周囲への問合せにより，不正動作を検出し，不正と判定されたノードを無視する動作をするだけなので，利用されるルーティングプロトコルについても制限がない．

ただし，本提案方式では，監視を行うために使用されるルーティングプロトコルに対応すること，および，存在しうる不正動作を検出するための知識が必要となる．また，新たな不正動作が発見された場合には，即座には対応できない．このため，PC のウィルス対策ソフトウェアを更新したり，IDS のエンジンを更新したりする必要があるのと同様に，本提案方式においても，不正動作に対する知識のアップデートが適切に行われなければならないであろう．

6. 関 連 研 究

文献 5) は，セルフィッシュノードという用語を用いている最初の論文である．不正ノードに対して転送拒否などのペナルティを課すような方法はとらず，最も信頼できる経路を選択してスループットを確保するというアプローチである．その他の点における本方式との相違については，主に 2 章に記述した．

文献 11) では，各ノードに他のノードを評価する

カウンタを持たせ，その状態によって相手のパケットを中継する方法を変化させる方法を提案している．文献 12) では，パケットの転送にインセンティブを与えて協調を促進するアプローチがとられている．

文献 13)，14) では，DSR プロトコルにおいてセルフィッシュノードを特定しネットワークから隔離するアプローチをとっている．不正ノードからの RREQ を拒否する点は提案方式も同様であるが，ソースルーティング方式である DSR プロトコルを利用しているため，不正ノードの情報をいったん送信元に戻し，不正ノードを広告する ALARM 情報を付加して別の経路で転送する点が異なる．提案方式は，不正ノードの隣接のノードでのみで問合せと対策を行い，送信元は必ずしも関与しない．

文献 15) では，アドホックネットワークにおけるノードの協調に関する既存の研究をまとめている．現状では，特定のレイヤ・特定のプロトコルに注目したものが多いため，レイヤをまたいだ協調関係のコントロールの必要性を訴え，NeSt（Network Status）アーキテクチャを提唱している．

文献 16) では，転送実績に基づいた参加促進メカニズム PCOM（Proactive Cooperation Mechanism）を提案している．

HADOF [6] では，経路上の各ノードの転送数の報告の差異を用いて検出を行い，blackhole ノードを含む悪意あるノードを検出し，除外する方法を提案している．この方式は，各ノードにおいて，他ノードへの判定結果に基づいて送信元においてソースルーティングを行うことが必要となる．

文献 17) は，提起している問題が類似しているが，端末の電源管理機構自体に，ユーザによる利己的な電源断操作ができないように制限を行うアプローチである点が異なる．

7. おわりに

本論文では，相互監視によるアドホックネットワークのセキュリティ方式を提案した．提案方式は，ノードが単独で不正動作を監視して判断するのではなく，相互監視を行い，問合せと応答により，より確実な判断を可能とする．一例として，セルフィッシュ動作の検出を取り上げ，watchdog 方式と提案の witness 方式の性能を小規模・大規模なモデルでシミュレーション評価した．Watchdog 方式では，正常なノードが攻撃ノードとして誤検出され通信不能となる可能性が問題となっていたが，witness 方式はこれを低減させることができることを確認した．今後の課題としては，誤検出の影響の詳細な分析，偽りの報告による提案方式への攻撃に対する耐性の評価，本論文で取り上げた以外の様々なセルフィッシュ動作や攻撃の検討と対策などがあげられる．

参考文献

1) FON. http://www.fon.com/en
2) http://www.atmarkit.co.jp/news/200612/08/bluetooth.html
3) Toh, C-K.，構造計画研究所（訳）：アドホックモバイルワイヤレスネットワーク—プロトコルとシステム，共立出版 (2003).
4) Wood, A. and Stankovic, J.: Denial of Service in Sensor Networks, *IEEE Computer*, Vol.35, No.10, pp.54–62 (2002).
5) Marti, S., Giuli, T., Lai, K. and Baker, M.: Mitigating routing misbehavior in mobile ad hoc networks, *Proc. Mobicom 2000* (2000).
6) Yu, W., Sun, Y. and Liu, K.J.R.: HADOF: Defense Against Routing Disruptions in Mobile Ad Hoc Networks, *IEEE INFOCOM* (2005).
7) http://www.ietf.org/rfc/rfc4728.txt
8) http://www.ietf.org/rfc/rfc3561.txt
9) UCB/LBNL/VINT, Network Simulator version2 (ns-2).
10) AODV-UU@Uppsala University. http://www.docs.uu.se/docs/research/projects/scanet/aodv/aodvuu.shtml
11) Buttyan, L. and Hubaux, J.P.: Stimulating cooperation in self-organizing mobile ad hoc networks, *MONET* (2003).
12) Zhong, S., Chen, J. and Yang, Y.R.: Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks, *Infocom'03* (2003).
13) Buchegger, S. and Le Boudec, J.-Y.: Performance analysis of the CONFIDANT protocol, *Proc. 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing*, June 09–11, 2002, Lausanne, Switzerland (2002).
14) Buchegger, S. and Le Boudec, J-Y.: Nodes Bearing Grudges: Towards Routing Security, Fairness and Robustness in Mobile Ad Hoc Networks, *Proc. 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing, Canary Islands*, Spain, January 2002, IEEE Computer Society, pp.403–410 (2002).
15) Conti, M., Gregori, E. and Maselli, G.: Cooperation Issues in Mobile Ad Hoc Networks, *ICDCSW'04* (2004).
16) 鈴木俊博，サットルサヤェン・ラタポン，小林基成，森田正範：アドホックネットワークにおける実績に基づいた参加促進メカニズム，IEICE Technical Report, AN2005 (2005).

17) 鈴木俊博，小林基成，カーン・アシック，森田正範：アドホックネットワークにおける Power Off Attack とその対策，情報処理学会研究報告，Vol.37, No.12, pp.61–65 (2006).

(平成 19 年 5 月 18 日受付)
(平成 19 年 11 月 6 日採録)

横山　信（学生会員）

1975 年生．1998 年 3 月横浜国立大学工学部電子情報工学科卒業．同年日本情報通信コンサルティング株式会社入社．移動体通信方式の研究開発・標準化の支援業務に従事．公立はこだて未来大学大学院在学中．電子情報通信学会員．

中根　由和

1954 年生．1976 年 3 月三重大学工学部電気工学科卒業．1976 年日本通信協力株式会社（現，日本情報通信コンサルティング株式会社）入社，主に移動体通信ソフトウェア開発に従事．2001 年より移動体事業本部長．

高橋　修（フェロー）

1975 年 3 月北海道大学大学院工学研究科情報工学修士課程修了．同年 4 月電電公社（現 NTT）入社．電気通信研究所にてコンピュータネットワークアーキテクチャの研究開発，および OSI の標準化に従事．1999 年 1 月 NTT ドコモに異動．モバイルインターネットの研究開発および標準化に従事．2004 年 4 月より公立はこだて未来大学システム情報科学部情報アーキテクチャ学科教授．博士（工学）．電子情報通信学会，IEEE 各会員．当会フェロー．

宮本　衛市（正会員）

1940 年生．1962 年北海道大学工学部電気工学科卒業．1964 年同大学院修士課程修了．同年同大学工学部電気工学科講師，同助教授を経て，1984 年より情報工学科教授．2000 年 4 月より公立はこだて未来大学システム情報科学部教授．工学博士．分散システム，並列オブジェクト指向モデル・設計論，プログラミング環境等の研究に従事．著書に『PASCAL—プログラミングと翻訳技法』，『はじめてのコンパイラ—原理と実践』等．電子情報通信学会，日本ソフトウェア科学会，人工知能学会，IEEE 各会員．