様式 C-19

科学研究費補助金研究成果報告書

平成 21 年　4 月　1 日現在

研究種目： 基盤研究（C）
研究期間：2006～2008
課題番号：１８５０００６５
研究課題名（和文）
アドホック・パーソナルエリアネットワークにおける安全な通信方式の研究
研究課題名（英文）
Secure Communication Protocol for Ad Hoc Personal Area Networks
研究代表者
佐藤　文明（SATO FUMIAKI）
東邦大学・理学部・教授
研究者番号：４０２７３１６４

研究成果の概要：アドホックネットワークにおける問題の一つに、利己的な端末のネットワークへのアクセス制御がある。利己的なノードは、アドホックネットワークにおけるルーティングを阻害し、ネットワークを不安定にする要因となる。この研究では、P2P での評判情報技術を応用して、アドホックネットワークにおいて利己的なノードを従来方式より正しく検出する方法、及び利己的なノードの動作を改善するための方法を提案し、シミュレーションによって有効性を示した。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2006 年度	1,900,000	0	1,900,000
2007 年度	800,000	240,000	1,040,000
2008 年度	800,000	240,000	1,040,000
年度			
年度			
総　計	3,500,000	480,000	3,980,000

研究分野：総合領域
科研費の分科・細目：計算機システム・ネットワーク
キーワード：アドホックネットワーク、セキュリティ、ルーティング、P2P、評判システム

１．研究開始当初の背景

ユビキタスネットワークのデバイス間通信方式として、アドホックネットワークが注目されている。アドホックネットワークは、無線をベースにした通信技術であるため、安全性について有線ネットワークよりも課題が多い。一つは、無線傍受による情報の漏洩が問題であり、無線 LAN においては基地局と端末とに共通鍵を使った暗号化が行われるのが普通である。しかし、アドホックネットワークにおいては、参加するノード全員に対して共通の鍵を前提とすることはできない。そのため、公開鍵基盤（PKI）を前提としたアルゴリズムも多く提案されている。しかし、ユビキタスネットワークにおける多数の端末に公開鍵を登録させるのはやはり困難である。

我々は、PGP などに利用されている「信頼の輪」（信頼する友人が信頼している人は信頼できる）をベースにしたセキュアルーティングを設計してきた。しかし、この方式のみでは信頼度の低いノードを使った経路が選択できないため、経路ができない可能性が高くなる。我々は、更に匿名通信方式の一つであ

るオニオン方式を取り入れた経路選択方式を設計している。
一方、情報漏洩と異なる問題に、アドホックネットワークにおける利己的なノードの存在である。従来の研究では、アドホックネットワークは利他的なノードがボランティア的に経路を構築することが前提になっている。しかし、アドホックネットワークが一般化するにつれて、全ノードが利他的なノードであるということが前提にできないことは明らかである。その問題に対して、近隣ノードの無線を傍受することで利己的なノードを検出する方法が提案されている。しかし、この方法はノードの検出に誤差があること、検出したノードを除外すると、ネットワークが縮小し、経路が構築しにくくなってしまう問題がある。

２．研究の目的

この研究では、従来の利己的なノードの検出誤差を改善するために、ノードの評判情報に基づく判定方法を提案する。評判情報とは、対象となるノードが普段どのような振る舞いをしているかの履歴情報を管理し、それを周囲のノードと交換することで計算される。我々は、P2P ネットワークにおける評判情報についての研究を実施しており、多人数が結託して虚偽の評判をフィードバックしても、精度良く評判情報を算出するためのアルゴリズムを確立した。その値を使うことによって、従来研究で起こりがちであった誤判定を減少させることができる。また、利己的と判定されたノードにペナルティを与えるだけでなく、利他的な行動をすることによるインセンティブを与えることにする。このことで、利己的なノードも積極的に中継サービスに参加することを促す方法を提案する。

ノードに協調的な動作を強制する方法に、評判情報による方法や、データ送信に対価を支払う方法などが提案されてきた。しかし、これらの方式は方法が複雑であり、なりすましや結託攻撃などのセキュリティ上の問題も多い。本方式は、信頼のおける隣接ノードの情報のみを使うことで、構成をシンプルにしている。その結果、情報の信頼度についてあまり大きな影響を受けにくくすることをねらっている。

このようなアクセス管理方式を評価するために、利用者の行動モデルを提案している。利己的なノードであっても、ある条件を満たせば、中継を行う行動モデルである。このモデルを使って評価したところ、評判情報を使ったアクセス管理方式は、評判情報を使わない場合にくらべてルート発見率が向上し、ネットワークの機能が低下しないことが分かった。

３．研究の方法

従来方式では、近隣のノードの通信状況を傍受することにより、近隣ノードが利己的な動作をしていないかどうかを検出するものであり、無線によるパケットロスと利己的な動作の違いを判別できない問題があった。我々は、この問題を近隣のノードの評判情報を計算することによって改善するものである。

研究の方法は、まず P2P ネットワークでの評判情報を収集する方式を研究し、その研究成果をアドホックネットワークに適用して、近隣ノードの利己的動作の判別精度を向上させる手順を踏む。

2006 年、2007 では主に P2P ネットワークでの評判情報の高精度化に関する研究を実施し、2007 年、2008 年ではその成果をアドホックネットワークに適用する研究を実施した。

４．研究成果

以下に、従来方式の概要と問題点、提案方式とシミュレーションによる有効性の評価を述べる。

（１）従来の利己的なノードの検出

ここでは、利己的なノードを検出する方法を紹介する。

①RREQ(RREP)を転送しないノードの検出

基本は、RREQ（RREP）メッセージを送信しているか否かを確認して判定する。例えば、図 4.1 において、ノード C への RREQ をノード A が送信した場合、ノード B がその RREQ を送信したか否かは、電波の無指向性より、A にも傍受により分かるようになっているはずである。

従って、ノード A は RREQ 送信後、自身の周囲のノード（この場合ノード B）が RREQ を一定時間内に転送しない場合、利己的なノードとして検出する。

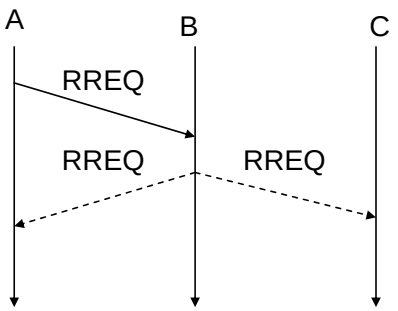

図 4.1 RREQ メッセージを転送しないノード

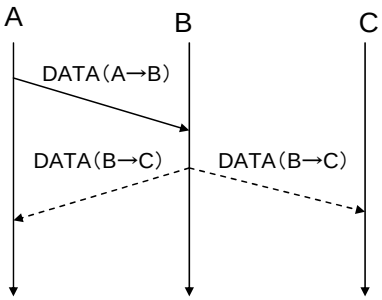

図 4.2 DATA メッセージを転送しないノード

なお、ノード A は自身の周囲のノードのリストを HELLO パケットの送受信により作成し、保持しているものとする。
また、この方法は、データパケットの転送を行わない利己的なノードの検出も同様に行うことができる。

②HELLO パケットを送信しないノードの検出
次に、自ノードがそこに存在することを隠しているノードへの対処法である。このノードは、本来、自身の存在を隣接ノードに知らせる為の HELLO パケットを送らないことで、自身がルートに選ばれないようにする。こういったノードへは、リアクティブな対策しか取れないのが現状で、突如パケットを送信してきたノードをその際にリストへと登録し、以降は①の方法で検出する。

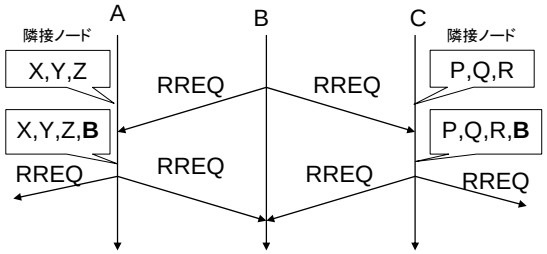

図 4.3 存在を隠すノード

③故意に遅延を大きくするノードの検出
最後に、リクエストを中継してはいるが、中継を故意に大きく遅延させるノードへの対策である。ルートをリクエストする際、早くこれを確立したほうが優先的に選択されるので、故意に遅延を大きくすることによってルートにならない、つまり、それ以降のデータを中継せずに済むということである。こういったノードへも、リアクティブな対策しかないのが現状だが、基本の方法にて、リクエストを中継したときに、常に遅れているノードというのも毎回中継時間のデータを記録することで検出できる。図 4.4 では C が故意に遅延を大きくするノードである。ノード A にはこういった利己的なノードを検出するための中継時間を記録するテーブルを作成する。これにより、C が常に遅れて応答を返していることが分かり、利己的なノードとして検出できる。

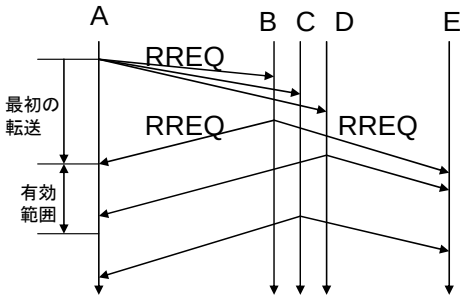

図 4.4 故意に遅延を大きくするノード

（2）従来方式の問題点
従来方式で、利己的なノードの検出はできる。しかし、これには二つの問題がある。
ひとつは、パケットロスのことを考慮していないことである。上記の方法で利己的なノードを検出する際に、通常の動きをしているノードが、中継をしたのに、そのパケットが何らかの理由でロスしてしまったとき、そのノードは利己的なノードとして扱われてしまう。以下、この現象を誤検出と表記する。パケットロスは、モバイルアドホックネットワークの性質上、どうしても起こり易いものであるので、誤検出が起こる可能性もそれに応じて大きい。誤検出によって、通常ノードが利己的なノードとして不当に扱われることのみでなく、経路が発見されにくくなるなど、ネットワークが更に機能しなくなる原因となる。
もうひとつが、利己的なノードを検出した際、その処理をどうするかという問題である。利己的なノードというのは、悪意ある行為を行っているので、そのネットワークから排除するという選択肢もある。確かに、排除を行うことによって、通常ノードが担う負担は、利己的なノードが利用する分だけ減少する。しかし、ネットワークの縮小という問題を解決できない。そこで、利己的なノードを排除するのではなく、そういったノードに利己的な行為を止めさせ、通常の動きをさせることが重要となる。

（3）提案方式
先に述べた問題点を考慮し、本研究では、信頼性についての評判情報を用いて利己的なノードを判別する方法を提案する。

①利己的なノードの検出方法の改良

評価値の割り当て

評価値とは、相手を信頼するための判断材料のひとつである。本研究の場合、評価値は利己的なノードかどうかの判断材料である。各ノードに評価値を設定し、低ければ利己的なノードで、高ければそうでないノードと考える。また、この評価値は近隣のノード間で評判情報として共有される。

評価値は、評価者が送信したパケットを対象ノードがどの程度中継したかを表す値としている。評価は一定回数のパケットを送信した後で更新されていく。今、ノードｐにおけるｉ回目の更新後の評価値を$E_i(p)$とすると、次のような式で計算される。

$$E_i(p) = \alpha E_{i-1}(p) + \beta \ (n_t(p) / n) \quad \cdots \text{式１}$$

ここで、$E_{i-1}(p)$は更新直前の評価値であり、$n_t(p)$は一定の送信パケット数ｎの中で正常に中継されたパケット数を示す。α、βは重みであり、今回はそれぞれ 0.7，0.3 を用いている。また、初期値E_0は 0.5 としている。

この提案方式では、ノードがパケットを中継した際にそのノードに対する評価値が増加、中継を行わなかった場合は減少していく。また、Helloパケットなしで突如パケットを送信してきた際には、$n_t = 0$として計算をすることで、評価値を減少させる。

この評価値は、近隣のノード間でHelloパケットに付けて送受信される。そして隣接ノードによって評価された値を平均して新しい値とする。

評価値に基づく高精度な検出アルゴリズム

従来方式の検出方法を用いれば、少なくとも、中継要請先のノードが利己的なノードである場合は確実に利己的な振る舞いを検出することができる。しかし、パケットロスによる誤検出が問題である。誤検出かどうかを判定するのに、式１で算出した評価値を利用する。

正常に中継するノードはパケットロスが発生しない際には正常に中継するため、式１で述べた評価値が上昇していく。利己的なノードに関してはその逆である。その結果、利他的なノードは評価値が高く、利己的なノードは評価値が低くなる。この結果を利用して、誤検出の防止を行う。利己的なノードと思われる振舞いを検出した際に、その対象のノードの評価値を参照する。その評価値が閾値以上ならば誤検出、また、それ以下ならば通常に利己的なノードとして検出する。

②利己的なノードへの対処方法

前述した通り、利己的なノードを検出したとしても、その後の処理の工夫をしなければネットワークの縮小は避けられない。ここでは、先に提案した各ノードへの評価値を用いて利己的なノードの処理、また、利他的なノードの処理を行うことで、利己的な行動への抑止力を働かせる方法を提案する。これにより、利己的なノードの総数が減少し、ネットワークの縮小が防止できる。

ペナルティー

評価値の低いノードに対して、ペナルティーを与えることを考える。利己的なノードに利己的な行動を止めさせるには、それに対する抑止力が必要となる。つまり、そういった行為を重ねて行い、結果、評価値が一定以下にまで減少したノードには何らかのペナルティーを与える。このペナルティーには様々な方法が考えられるが、代表的なものとしては、帯域制御や、接続の優先度の変更が挙げられる。こういったペナルティーを設けることによって他ノードの目的の為のパケットを中継することに対するデメリットよりも大きなデメリットを利己的なノードに課す。そうすることで利己的なノードは利己的な行為をするメリットが相対的に減少し、正常に利他的な行動を取らざるを得なくなる。

インセンティブ

他ノードの目的の為のパケットを中継することに対してメリットを生み出す為に、中継を続けて評価値が一定以上にまで増加したノードには何らかのインセンティブを与える。インセンティブの具体的な内容もペナルティーと同じく、様々な方式が考えられるが、代表的なものはやはり帯域制限と接続優先度の変更である。そうすることで、他ノードの目的の為のパケットを中継することによるデメリットと中継することによるメリットとを相対的に考えさせる。このメリットが利己的な行動に対する抑止力となる。

（4）シミュレーション

提案方式を評価するために、シミュレーションを実施した。シミュレーションモデルは以下の通りである。基本となるルーティングプロトコルは AODV である。シミュレーション時間は 20 秒間を１０回行って平均した。ただし、自己の存在を隠すノードは既に発見してリストに加えられた後とし、また、故意にリクエスト中継を遅延させるノードに関しては、今回は考慮しない。

表 4.1 シミュレーションモデル

全ノード数	50,100
送信要求発生頻度	0.5sec
電波の届く範囲	200 (m)
遅延（1ホップ）	0.5msec
範囲	1000 (m) ×1000 (m)
利己的なノードの数	6～36
パケットロス率	5～30 (%)

ノードの配置される位置、ノードがルートリクエストを送信する際、その目的ノードはランダムとし、ノードの移動はないものとした。シミュレーションでは、利己的なノードがペナルティーを受けたときにどのように振る舞うかを仮定する必要がある。以下に代表的な4つの行動モデルを定義した。これらの行動モデルに基づいて振る舞うノードが存在した場合、どのように提案方式が機能するかを評価した。

表 4.2 ノードの行動モデル

グループ1	ペナルティーを受けても利己的な行動続ける。
グループ2	パケットの転送拒否を受けると、利他的な行動を取る。
グループ3	ペナルティーを受けると、利他的な行動を取る。
グループ4	ペナルティーを受けないように利己的な行為を適度に行う型。

なお、比較の為に評価値を導入していないタイプのシミュレーターも作製した。初期値は評価値導入版と同値で起動する。ただし、利己的なノードの数はグループ1のみとし、評価値がないため、誤検出である可能性を考えない。また、利己的なノードと判断したら、即刻ネットワークから排除するようにした。ただし、排除後も RREQ の送信は続け、正常に中継をしたならばネットワークに復帰するようになっている。
図 4.5、4.6 にシミュレーションによって評価したルート発見率、誤検出率を示す。ルート発見率はデータ送信要求によってルート検出が行われるときの全体のルート検出回数に対するルートが発見された回数のパーセンテージである。ルートが発見できなければデータ送信ができないため、ネットワークの可用性を示す指標となる。誤検出率はシミュレーション時間が経過した時点で、通常なノードの数に対して、通常なノードが利己的なノードと判断されている数のパーセンテージである。

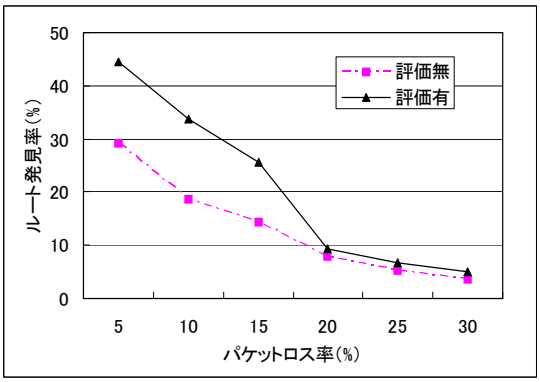

図 4.5 パケットロス率変化時のルート発見率

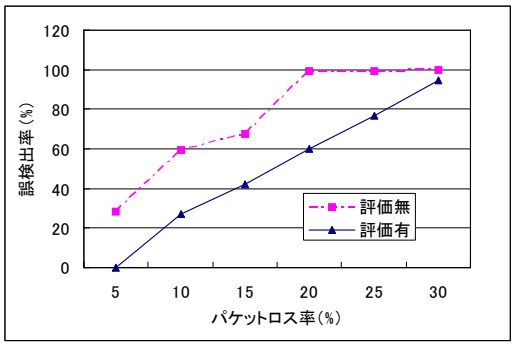

図 4.6 パケットロス率変化時の誤検出率

まず、利己的なノードの数を 12 とし、そのときパケットロスの確率を変化させながらシミュレーションした。なお、評価値を導入したシミュレーションでの利己的なノード数はグループ 2 が 4、グループ 3 が 4、グループ 4 が 4 とした。

評価値を導入したシミュレーションではルート発見率、誤検出率共に評価値を導入していないシミュレーションの値を上回っている。しかし、パケットロス率がある程度高くなってしまうとその効果は薄れてしまい、パケットロス率が 20%程度からは評価値を導入していないシミュレーションの値とほぼ差がないようになってしまっている。
パケットロス率が高くなると、評価値を増加させるための正常な通信ができなくなる。特にパケットロス率が 30%を超えると RREQ の正しい傍受確率が 50%を割ってしまい、評価値増加に繋がらなくなる。そのため、評価値が機能しなくなったと考えられる。

（5）成果のまとめ

本研究では、アドホックネットワークにおいて、各ノードに対する評価値を設定し、それをシミュレーターによってシミュレーシ

ョンした。その結果、これを利用することで、利己的なノードを検出する際の誤検出を減少させることができた。また、評価値に応じたペナルティーとインセンティブを設け、これらが利己的な行為に対する抑止力となるという前提の上でだが、利己的なノードを減少させることができた。そして、利己的なノードが減少することによってアドホックネットワークの縮小を防止できることを確認した。

５．主な発表論文等

〔雑誌論文〕（計３件）

① Fumiaki Sato and Shigetoshi Wakabayashi: “Bloom Filters Based on the B-Tree”, IEEE Third Workshop on Engineering Complex Distributed Systems (ECDS 2009), pp.500-505,(2009.3)

② Fumiaki Sato and Sumito Iijima: “Battery and Power Aware Routing in Mobile Ad Hoc Networks”, Network-Based Information Systems (NBiS 2007), LNCS 4658, Springer-Verlag Berlin Heidelberg, pp.30-39, (2007,9)

③ Fumiaki Sato: “Estimation of Trustworthiness for P2P Systems in Collusive Attack”, DEXA The First International Conference on Complex, Intelligent and Software Intensive Systems (CISIS2007),pp.171-176, (2007,4)

〔学会発表〕（計６件）

① 荻野隆史, 佐藤文明,“移動ノードを含むワイヤレスセンサネットワークにおける通信経路の維持方式の提案”,情報処理学会マルチメディア通信と分散処理シンポジウム論文集, IPSJ Symposium Series, Vol.2008, (2008,12)

② 佐藤文明, 永田欣久,“MANETにおけるノードの信頼度を用いた利己的ノードの検出方法”,情報処理学会マルチメディア通信と分散処理研究会研究報告No.137, (2008,11)

③ 若林繁寿, 佐藤文明,“B木構造に基づくBloomフィルタの提案”, 情報処理学会マルチメディア通信と分散処理研究会研究報告No.137, (2008,11)

④ 鴨居栄次郎, 佐藤文明,“階層型P2Pシステムの耐故障性向上のための動的な構成変更方式”,情報処理学会マルチメディア通信と分散処理シンポジウム論文集, IPSJ Symposium Series, Vol.2007, No.9, pp.85-86(2007.10)

⑤ 飯島澄人, 佐藤文明,“電力残量と省電力を考慮したアドホックネットワーク”,情報処理学会第６９回全国大会論文集, (2007.3)

⑥ 齊藤匡圭, 佐藤文明,“弛緩法を用いた無線通信による屋内向け測位方式の提案”, 情報処理学会第６９回全国大会論文集, (2007.3)

〔図書〕（計１件）

① 水野忠則、佐藤文明、鈴木健二、竹中友哉、西山智、峰野博史、宮西洋太郎 共訳, A.S.タネンバウム、M.F.スティーン著、“分散システム 原理とパラダイム第２版”、ピアソンエデュケーション (2009,1)

６．研究組織

(1)研究代表者

佐藤 文明（SATO FUMIAKI）
東邦大学・理学部・教授
研究者番号：４０２７３１６４

(2)研究分担者

なし

(3)連携研究者

なし