情報処理学会論文誌 Vol.57 No.2 471–479 (Feb. 2016)

モバイルアドホックネットワークにおけるノードの行動に適応したトラストモデル

梅田 沙也華[1,a)] 大畑 百合[1] 神本 崇史[1] 重野 寛[1]

受付日 2015年5月14日, 採録日 2015年11月5日

概要：モバイルアドホックネットワーク（MANET）では，他ノードのパケット転送に協力的でない利己的ノードへの対策として，パケットが正常に転送される度合いを表した値であるトラストを用いたセキュアルーティングが研究されている．しかし，既存のセキュアルーティングではリソースの変化によって突然パケット転送をやめたノードに対して利己的ノードとしての検知が遅れ，このようなノードを含んだ経路を選択するという問題がある．そこで，本論文では，行動変化を検知してノードの行動に適応したトラストを算出する手法（TEAB）を提案する．TEAB ではトラストの変化量に注目してノードの行動変化を検知し，行動変化直後のノードに対しては現在の行動を反映させることで，行動変化に対応しながらも安定したトラストをセキュアルーティングで実現する．提案手法の評価はシミュレーションにより行い，利己的ノードを早く検知することで破棄されるデータパケットが減るという結果から TEAB の有用性を示す．

キーワード：モバイルアドホックネットワーク，セキュアルーティング，トラスト，行動変化

Trust Model Considering Node Behavior in Mobile Ad hoc Networks

Sayaka Umeda[1,a)] Yuri Ohata[1] Takashi Kamimoto[1] Hiroshi Shigeno[1]

Received: May 14, 2015, Accepted: November 5, 2015

Abstract: In mobile ad hoc network (MANET), secure routing protocols based on trust, which is a value representing the degree packets are forwarded correctly, are developed as countermeasures against selfish nodes not cooperating with packet forwarding. However, in the existing secure routing protocols, as it takes many times to detect nodes that drop packets due to their resources, each node may select the route including such selfish nodes. In this paper, we propose a trust evaluation method adapted to node behavior by detecting changing behavior (TEAB). After each node detects changing behavior according to the variation of trusts, the node changing behavior is evaluated from the current behavior. Therefore, it calculates stable trusts considering nodes changing behavior in secure routing. We evaluate TEAB through the computer simulation. The results show the number of dropped data packets decreases by detecting selfish nodes quickly.

Keywords: mobile ad hoc network, secure routing, trust, changing behavior

1. はじめに

近年，移動中や外出先で利用されるモバイル端末の普及により，基地局を介さずにノード間で協調して構築されるモバイルアドホックネットワーク（MANET）が注目されている．MANET では，直接通信できないノード間においても，他ノードがパケットの中継をすることで通信が可能になる．しかし，MANET において想定されているモバイルノードは電力や帯域幅といったリソースに制限があるため，他ノードのパケット中継に協力的でない利己的ノードの存在が指摘されている [1]．ここで，利己的ノードとは自身のリソース保持を目的として，転送要求されたパケットを意図的に破棄するノードを示す．このように，管理者

[1] 慶應義塾大学大学院理工学研究科
Graduate School of Science and Technology, Keio University, Yokohama, Kanagawa 223–8522, Japan
[a)] umeda@mos.ics.keio.ac.jp

が存在せず，すべてのノードが自由に参加することで構築されるネットワークの特徴に対して，参加ノードはリソースにおいてパケット転送に制限がある．そのため，パケット中継に協力的でない利己的ノードが MANET に存在し，通信が成立しないことが問題とされている [2], [3].

そこで，MANET におけるセキュリティ対策の 1 つとして，セキュアルーティングプロトコルが研究されている [4], [5], [6]．セキュアルーティングでは，トラストと呼ばれる評価値を利用することで，パケットを意図的に破棄する利己的ノードを検知し，パケットを転送するノードのみを中継する安全な経路を選択することを目的とする．ここで，トラストとはノードや経路における信頼度を数値化した値であり，一般にパケットが正常に転送される度合いを表す．各ノードがトラストを算出し，この値に基づいて通信経路を決定することで，MANET で確実な通信を可能にする．

しかし，既存のセキュアルーティングでは協力的なノードが自身の電力や帯域幅の減少にともなって突然利己的ノードに変化した場合，行動変化によって新たに生まれた利己的ノードを含んだ経路を選択するという問題がある．原因として，行動変化した直後の利己的ノードを検知できないこと，経路情報の更新頻度が低いことの 2 つがあげられる．まず，トラストは過去のパケット転送の記録によって決まるため，長期的に収集した多くの転送記録から算出することで安定した値になる．このような特徴から，ノードがリソースの変化にあわせて利己的ノードに変化した場合であっても，すぐにトラストは大きく変化せずに利己的ノードとして検知されない．次に，セキュアルーティングではトラストの変化に合わせて経路更新の頻度を決定する．そのため，過去の評価が高く，トラストがあまり変化しないノードの行動変化では経路の更新が行われず，利己的ノードを含んだ経路が通信に使われる．

そこで，本論文では行動変化を検知して，ノードの行動に適応したトラストを算出する手法 TEAB（Trust Evaluation Method Adapted to Node Behavior in MANET）[7] を提案する．提案手法は，各ノードがトラストの変化量に基づき隣接ノードの行動変化を検知する．そして，ノードの行動に合わせてトラスト算出時に用いる過去の転送記録の範囲を変化させることで，新たな行動を評価しながら安定したトラストを維持できるトラストモデルである．この手法によって，ノードが行動を変化させる環境においても利己的ノードを回避した通信を実現する．

以下本論文では，2 章において関連研究について述べ，3 章で TEAB を提案し，4 章でシミュレーション評価により提案手法の有用性を示す．最後に 5 章で結論を述べる．

2. 関連研究

本章では MANET におけるノードの行動モデルやセキュアルーティングにおける関連研究をあげ，そこで用いられるトラストモデルについて述べる．

2.1 MANET におけるノードの行動モデル

MANET に参加するノードは，他ノードのパケットを転送する役割を担っている．しかし，一般にモバイルノードはバッテリで動作すると想定されており，自身のリソースを保持するために他ノードから転送要求されたパケットを破棄するような利己的ノードが存在する [1]．利己的ノードの行動モデルとして，すべてのパケットを破棄するモデル，選択的に一部のパケットを破棄するモデル，一時的にパケットを破棄するモデルが想定されている．すべてのパケットを破棄するノードは，パケットの転送をいっさい行わないため，このノードを含む経路ではデータパケットが目的ノードまで到達しない．そのため，パケット到達率が低下し，ネットワーク全体の性能が低下する．選択的に一部のパケットを破棄するノードは，制御パケットのみ転送することで自身を経由する経路を構築するノードや，一定以上の転送協力をしないノードがあげられる．また，一時的にパケットを破棄するノードは，バッテリの残量といったリソースの減少にともなって，パケットを転送していた行動から突然パケットを破棄する行動へと変化する．これらのノードは，一見パケット転送を行っているようにも見えるため，ネットワークを混乱させる原因となる．

2.2 セキュアルーティングプロトコル

セキュアルーティングとして，利己的ノードを回避して安定した経路を構築するための手法が検討されてきた [4]．各ノードがトラストと呼ばれる評価値を用いて，より確実に目的ノードにデータを転送できる経路を見つける．

セキュアルーティングプロトコルの代表例として，AOTDV [8]，LWT-AOMDV [9]，TA-AODV [10] がある．AOTDV はトラストとホップ数に基づくルーティングを実現している．さらに，LWT-AOMDV と TA-AODV ではセキュアルーティングにおける経路構築のオーバヘッド増加を軽減させる．

2.3 トラストモデル

セキュアルーティングで用いられるトラストモデルは，リンクトラストとパストラストという大きく 2 種類のトラストから構成される [8].

2.3.1 リンクトラスト

リンクトラストとは，隣接ノードが正常にパケットを転送するかの信頼度を数値化した値である．各ノードは隣接ノードにパケット転送を要求した後，その要求が正常に満たされるかオーバヒアによって確認する．時刻 t にノード i が j に対して持つリンクトラスト $L_{ij}(t)$ は以下の式で算出される．

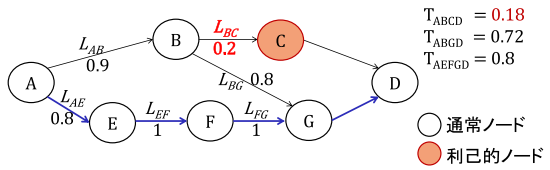

図 1 パストラストの例
Fig. 1 Example of path trust.

$$L_{ij}(t) = \begin{cases} \dfrac{N_C(t) - N_C(t-W)}{N_A(t) - N_A(t-W)} & (t > W) \\ \dfrac{N_C(t)}{N_A(t)} & (t \leq W) \end{cases} \quad (1)$$

ここで，$N_C(t)$ は時刻 t までにノード j が i からの要求に対して正常に転送した累積パケット数，$N_A(t)$ は時刻 t までにノード i が j に転送を要求した累積パケット数を表す．W は評価期間を示すタイムウィンドウであり，リンクトラストは W 時間前から現在までに転送されたパケットから算出されることを意味する．$L_{ij}(t)$ が 0 に近いほど，ノード j は多くのパケットを破棄したことを示し，ノード i は j を今後も破棄する可能性が高いノードだと判断できる．そして，ブラックリスト閾値 $T_{blacklist}$ 以下であるノードを利己的ノードと判別し，一定期間そのノードへのパケット転送を行わない．

2.3.2 パストラスト

パストラストとは，その経路を通ってパケットが目的ノードに到達するかの信頼度を数値化した値である．経路 P におけるパストラスト T_P は以下の式で表される．

$$T_P = \Pi(L_{ij}(t) | n_i, n_j \in P \quad \text{and} \quad n_i \to n_j \quad \text{and} \quad n_j \neq N_d) \quad (2)$$

$n_i \to n_j$ は経路 P 上で n_j が n_i の次ホップのノード，N_d は経路の目的ノードであることを示すため，パストラストは中継ノードのリンクトラストの積によって算出される．

図 1 にノード A から D へ 3 通りの経路におけるパストラストの例を示す．ここで，ノード C は利己的ノードであり，パケットを転送しないため L_{BC} は 0 に近い値をとる．ノード A はそれぞれのパストラストを比較することで，ノード C を回避した経路 P（$AEFGD$）を選択して通信できる．セキュアルーティングにおいて，このパストラストは経路探索時に制御パケットを転送していく中で算出され，各ノードの経路表に保持される．そして，今後たとえば L_{EF} が 0 に近い値へと下がった場合には経路更新（RUPD）パケットが送信されて，更新された経路表によってノード F を回避した経路 P（$ABGD$）が選択される．

2.4 セキュアルーティングにおける問題点

MANET では，パケット転送に協力的なノードがリソースの変化にともない利己的ノードに変化する可能性がある [11]．特に既存のトラストモデルを用いた場合，ある程度パケット転送に協力して周囲からの評価を得た後に行動を変化させることで，パケットを転送せずにネットワークに参加できる期間が生まれる．そのため，多くのノードが利己的ノードに変化する可能性が考えられる．このような行動変化が発生したとき，セキュアルーティングでは行動変化によって新たに生まれた利己的ノードを含んだ経路を選択するという問題がある．この問題によって，データ転送の効率が低下することやデータが目的ノードまで到達しないといった影響がでる．以下では，この根本的な原因としてあげられる，行動変化した直後の未検知利己的ノードの存在と経路情報の更新頻度の低下についてそれぞれ説明する．

まず，今まで転送に協力していたノードが突然行動を変化させてパケット破棄を開始した場合，すぐに利己的ノードとして検知できない．既存のセキュアルーティングで用いられるトラストは，長期的に収集した多くのパケット転送記録から算出されることで安定した値を維持している．ここでの安定した値とは，通信途中でパケットロスが発生した可能性を考慮して，1 回の転送結果によってトラストが急激に変化しない値となっていることを意味する．そのため，パケット転送を繰り返して一度トラストが収束したノードであれば，ノードがリソースの変化にともなって行動を変えてもトラストが一定の閾値以下となって隣接ノードから検知されるまで時間がかかる．よって，一定の行動を続けるノードに対しては安定したトラストを維持しながら，行動を変化させたノードに対しては新しい行動を反映したトラストを算出できるトラストモデルが必要となる．

また，トラストの変化が小さい場合に経路更新の頻度は低くなり，経路に関するトラスト情報の更新や新たな経路構築の機会が減る．つまり，セキュアルーティングでは，各ノードの算出するリンクトラストの変化にともなって経路表が更新される．そのため，ノードの行動が変化してもトラストが大きく変化しない場合，利己的ノードとして検知できないだけでなく，パケット破棄を行うノードを中継ノードとして含んだ経路が各ノードの経路表内に存在し続けることになる．したがって，パケット破棄を開始したノードを含む経路における経路更新の頻度が高くなることで安全な経路選択を可能にするために，ノードの行動に合わせて大きく変化できるようなトラストモデルを利用したセキュアルーティングが必要となる．

3. TEAB の提案

本章では行動変化を検知して，ノードの行動に適応したトラストを算出する手法 TEAB（Trust Evaluation Method Adapted to Node Behavior in MANET）を提案する．

3.1 TEAB の概要

提案手法の目的は，ノードの行動変化が発生する環境で

あっても，利己的ノードを中継に含まない経路を選択して無駄のない確実なデータの送信を実現することである．提案手法ではトラスト算出時に用いる評価期間であるタイムウィンドウに着目し，一定の行動を続けるノードと行動を変化させたノードのそれぞれに合わせたトラストを算出することで利己的ノードをより正確に検知する．まず，各ノードはリンクトラストの変化量の符号と大きさに基づいて，パケットの転送または破棄という観点から行動を変化させたノードを検知する．そして，行動変化が検知されたノードは今後利己的ノードに変化する疑いがあると考え，以降の新しい行動に注目したリンクトラストを算出する．具体的には，可変タイムウィンドウによってノードの行動に合わせてトラスト算出時に用いる過去の転送記録の範囲を変化させることで，変化後の行動をリンクトラストに早く反映させながら，一定の行動を続けるノードに対しては安定したリンクトラストを算出できる．さらに，提案手法をセキュアルーティングに利用すると，現在の行動を表して変化したリンクトラストから経路更新の頻度が高くなる．以下では，行動変化検知の手順とトラストモデル，セキュアルーティングへの応用について詳細を述べる．

3.2 行動変化の検知

一般的なセキュアルーティングでは，収集した多くのパケット転送記録の平均として算出されるトラストの値のみに注目していたため，ノードの平均的な行動しか評価できずに現在の行動を知ることができない．そこで，提案手法ではノードの過去の行動を評価しながらも，リンクトラストの変化量によって現在の行動も把握してノードの行動変化を検知する．ここでの行動変化の検知とは，今までパケットを転送していたノードの直近のパケット破棄を見逃さないことであり，長期的にノードの行動を判断して利己的ノードを分類することではない．ここでは，一定の行動を続けるノードと行動を変化させたノードのそれぞれに合わせてトラストを算出するために，ノードを行動によって分類することを目的とする．

時刻 t にノード i がノード j に対する行動変化の検知に用いる変化量 $\Delta L_{ij}(t)$ を式 (3) によって定義する．

$$\Delta L_{ij}(t) = L_{ij}(t) - L_{ij}(t_{prev}) \tag{3}$$

$L_{ij}(t)$ は時刻 t にノード i がノード j に対して持つリンクトラストであり，式 (1) に従って算出される．また t_{prev} は直前にリンクトラストを算出した時刻を表すため，変化量 $\Delta L_{ij}(t)$ の大きさはリンクトラストがどの程度変化したかを表す．さらに，この変化量の符号に注目すると，正の値はノード j がノード i の要求したパケットを転送していることを示し，一方で負の値はノード j が転送要求を破棄していることを意味する．このような特徴を表す変数として，符号判別変数 $D_{ij}(t)$ を式 (4) によって定義する．

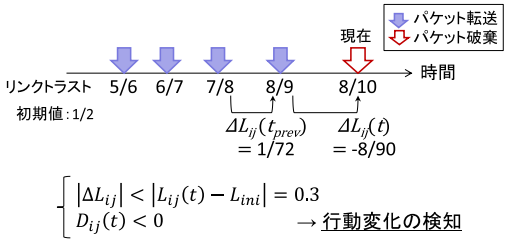

図 2 行動変化検知の例

Fig. 2 Example of detection of changing behavior.

$$D_{ij}(t) = \Delta L_{ij}(t) \times \Delta L_{ij}(t_{prev}) \tag{4}$$

これらの値を用いて，提案手法では変化量 $\Delta L_{ij}(t)$ の符号と大きさの 2 点に基づき，以下の式 (5) の条件を満たしたノードに対して行動変化を検知する．

$$\begin{cases} D_{ij}(t) < 0 \\ |\Delta L_{ij}(t)| < |L_{ij}(t) - L_{ini}| \end{cases} \tag{5}$$

ここで，L_{ini} はリンクトラストの初期値である．第 1 式は，変化量の符号に関する条件であり，式 (4) より $\Delta L_{ij}(t)$ と $\Delta L_{ij}(t_{prev})$ が異符号であることを意味する．つまり，変化量の符号がノードの行動を表すことを考慮すると，新たな行動に変化があったノードだと判断できる．さらに第 2 式は，変化量の大きさに関する条件である．ここで，リンクトラストの変化量は初期値に近いほど大きく，時間経過とともに値が収束して小さくなることが知られている [10]．つまり，この条件式はリンクトラストが初期値付近では右辺が小さいため満たされにくく，リンクトラストが収束したノードにおいては満たされやすい．提案手法では，トラストの変化が小さいノードにおいて行動変化をトラストに反映させることを目的とするため，第 2 式を行動変化検知の条件に加えることで，トラストが安定していないノードにおけるパケットロスに過剰に反応しない検知手法となる．

図 2 にリンクトラストの推移と行動変化の検知例を示す．これは，評価ノード i の転送要求に対する評価対象ノード j の行動と各時間での転送結果の例を表す．ノード j がパケット転送を続けているときはリンクトラストが増加を続けるため，符号判別変数 $D_{ij}(t)$ は正の値を維持する．しかし，転送を続けるノード j がパケットを破棄したとき，条件から行動変化として検知できる．このように，リンクトラストの変化量に基づく判別することで，トラストの変化が小さなノードの行動変化に対する新たな対応を可能にする．

3.3 行動に適応したトラストモデル

既存のトラストモデルでは，すべてのノードに対して同様に安定したトラストを目指しているため，一度トラストが収束したノードに対しては，行動変化が発生しても新しい行動がトラストに反映されるまでに時間がかかる．そこで，提案手法では一定の行動を続けるノードに対しては従

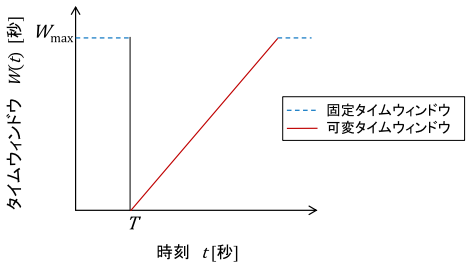

図 3 タイムウィンドウの変化例
Fig. 3 Example of changing time window.

来の安定したトラストを維持しながら，行動を変化させたノードに対しては新しい行動を反映したトラストを算出できるトラストモデルを確立する．つまり，3.2 節の手順によって行動変化したと判断されたノードは，今まで転送に協力的であっても今後利己的な行動をとる可能性があると考え，評価期間であるタイムウィンドウを意図的に短くすることで，評価に含める過去の転送結果を制限する．

既存のトラストモデルでは式 (1) に従ってリンクトラストを算出している．ここで，固定のタイムウィンドウ W を利用しているため，すべてのノードに対してトラストは過去の一定期間での転送結果を評価した値となる．そこで，提案手法では可変タイムウィンドウを導入する．時刻 t にノード i がノード j に対する評価に用いるタイムウィンドウ $W_{ij}(t)$ を以下の式で定義する．

$$W_{ij}(t) = \min\{W_{\max}, t - T_{ij}\} \tag{6}$$

$W_{\max}$ は固定の最大ウィンドウ定数を表し，T_{ij} はノード i が j に対して行動変化を検知した時刻である．そのため，行動変化が検知されないノードに対しては既存のトラストと同様に固定のタイムウィンドウが採用され，行動変化が検知されたノードに対しては変化後から現在までの行動を評価に含むように可変タイムウィンドウで調整する．ここで，行動変化が検知されたノードに対して，可変タイムウィンドウを利用せずに固定の短いタイムウィンドウを用いることで過去の転送結果を評価から排除するという手法も考えられる．しかし，短いタイムウィンドウを使い続ける場合，少ない結果から評価しなければならないため十分に収束したトラストが算出されない．そこで，提案手法では過去の転送結果を制限しながらも，その中で長期間を評価できるような可変タイムウィンドウを導入する．これによって，新しい行動を単にトラストに反映させるだけでなく，ノードの行動に合わせて大きく変化できるようなトラストを実現する．

図 3 に行動変化を検知した場合の時間経過に対するタイムウィンドウの変化例を示す．タイムウィンドウは行動変化を検知した時刻に最短になり，そこから時間経過とともに伸ばす．そして行動変化時刻から最大タイムウィンドウと同じ時間が経過した時点から，また固定タイムウィンドウを利用する．以上により，行動変化ノードを考慮して可変タイムウィンドウを既存のトラストモデルに加えることで，行動変化したノードと一定の行動を続けるノードにおいてそれぞれの特徴にあわせた対応が可能になる．

表 1 トラストレコードの構成
Table 1 Structure of a trust record.

ノード ID
L：リンクトラスト
N_C：正常に転送されたパケット数
N_A：転送を要求したパケット数
ΔL：リンクトラストの変化量
W：タイムウィンドウ
T：行動検知時刻
パケットバッファ

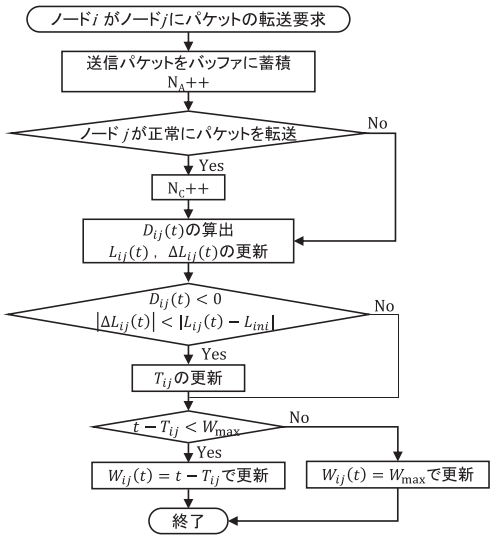

図 4 トラストレコード更新アルゴリズム
Fig. 4 Algorithm of updating trust records.

3.4 セキュアルーティングへの応用

トラストを用いたセキュアルーティングでは，各ノードがトラストに関する情報を把握するためにトラストレコードを保持し，経路表にパストラストのフィールドを追加する [8]．そして，リンクトラストが一定以上変化した場合，経路更新（RUPD）パケットによって各ノードの持つ経路表に含まれるパストラストが更新される．

提案手法のトラストモデルをセキュアルーティングへ応用する場合，基本的なルーティングプロトコルは既存手法 TA-AODV [10] に従うものとし，ここでは提案手法による変更点のみを述べる．各ノードの保持するトラストレコードを**表 1** に示す．そして，**図 4** に提案手法を用いたセキュアルーティングにおけるトラストレコード更新のアルゴリズムを示す．まず，隣接ノードにパケットの転送要求をしたノードは，転送したパケット情報の更新とプロミスキャスモードによる監視を行う．監視結果に基づいて $L_{ij}(t)$，$\Delta L_{ij}(t)$ を更新し，これらの値に従って経路更新パケットを送信するか判断する．また，トラストレコードの情報から $D_{ij}(t)$ を算出し，式 (5) に従って行動変化の検知を行う．

ここで，行動変化が検知された場合は検知時刻 T_{ij} の更新を行い，その結果に基づいて $W_{ij}(t)$ を算出する．

このように，既存の経路更新の特徴に合わせて，提案手法ではノードの行動に合わせて大きく変化できるようなトラスト算出を行う．つまり，行動変化ノードに対してリンクトラストが変化することで経路更新の頻度を上げ，経路表から利己的ノードを含んだ経路を排除して協力的なノードのみによる経路を用いた通信を可能にする．

4. シミュレーション評価

提案手法 TEAB が利己的ノードを早く検知して利己的ノードを回避した経路選択を行うことを示すために，シミュレーションにより評価を行った．

4.1 シミュレーションモデル

シミュレーションのパラメータを**表 2** に示す．これらの値は文献 [10] に従って設定した．シミュレーションエリア内にはすべてのパケットを転送する通常ノードとデータパケットのみをすべて破棄する利己的ノードが存在する．また，シミュレーションのシナリオは，はじめ全 N ノードが通常ノードとしてパケットを転送し，その後最終的に N_s 個のノードが利己的ノードに変化する．このとき，行動変化のタイミングは，一定以上のパケット転送または 2,000 秒以降で初めて転送要求を受けたときとした．シミュレーション後に調査した結果，2,000 秒の前後 200 秒程度に集中して利己的ノードが増加するシナリオとなった．ここで，N_s は各シミュレーションで固定であり，シミュレーションで条件を段階的に設定した．なお，特に断りがない場合，N_s は 10 個とした．提案手法で用いる最大ウィンドウ定数 $W_{\max}$ は，既存手法 AOTDV [8] での固定のタイムウィンドウと同じ値を用いた．提案手法がノードの行動変化が発生するような環境において，利己的ノードを中継ノードに含まない経路を選択して確実なデータの送信を実現することを示すため，以下の 4 つの項目により提案手法の性能を評価する．

- 利己的ノードの被検知数
  あるノードを利己的ノードとして検知したノード数の平均を表す．
- 経路更新パケット数
  行動変化後に経路情報が更新されることを確認する．
- データパケット到達率
  利己的ノードの影響が関係する 2,000 秒以降のデータパケットが目的ノードに届く割合を表す．
- 利己的ノードへの転送要求数
  利己的ノードがデータ転送の中継に含まれた回数から，利己的ノードを回避した経路選択ができることを確認する．

比較対象は TA-AODV [10]，AOTDV [8] とする．また，パケット到達率に関しては一般的なルーティングプロトコルである AODV とも比較を行う．

表 2 シミュレーションパラメータ
Table 2 Basic simulation parameters.

ネットワークシミュレータ	Qualnet5.0.2
評価時間	8,000 秒
無線通信方式	IEEE 802.11b
シミュレーションエリア	750 m × 750 m
無線通信範囲	250 m
トラフィックタイプ	CBR (UDP)
ペイロードサイズ	512 byte
パケットレート	4 pkts/s
モビリティモデル	ランダム
最大移動速度	2 m/s
全ノード数：N	100
最大利己的ノード数：N_s	0, 10, 20, 30, 40
リンクトラストの初期値：L_{ini}	0.5
ブラックリストスレッショルド：$T_{blacklist}$	0.5
最大ウィンドウ定数：$W_{\max}$	300 秒

4.2 TEAB の動作確認

提案手法において導入した可変タイムウィンドウの動作を確認する．**図 5** に，2,000 秒に行動変化した特定の利己的ノードに対する代表的な 3 個のノードのタイムウィンドウの時間変化を示す．ノード 33 は利己的ノードの行動変化直後にタイムウィンドウを変化させていることが確認できた．このように，利己的ノードの行動変化直後にその利己的ノードのパケット破棄の影響を受けたノードは，早くタイムウィンドウを変化させることで，行動変化を検知したノードに対して新しい行動を評価できる．また，ノード 37 は行動変化からある程度時間が経過した後にタイムウィンドウを変化させていることが確認できた．このように，ノードのモビリティの変化にともなって，利己的ノードの影響を受けた段階でタイムウィンドウを変化させることができる．さらに，ノード 40 ではタイムウィンドウの変化が見られず，利己的ノードの隣接でないために影響を受けないノードでは，タイムウィンドウは変化していないこと

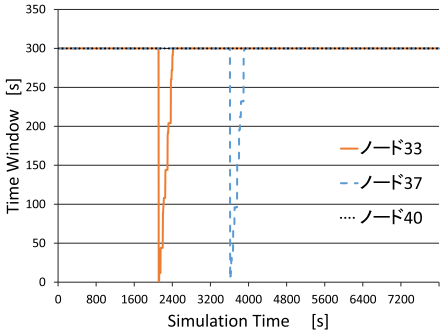

図 5 タイムウィンドウの時間変化（$N_s = 10$）
Fig. 5 Variation of time window.

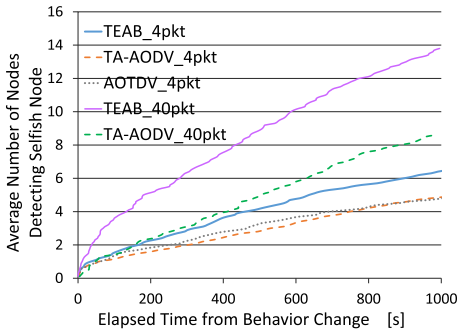

図 6 利己的ノードの平均被検知数（$N_s = 10$）
Fig. 6 Number of nodes detecting the selfish node.

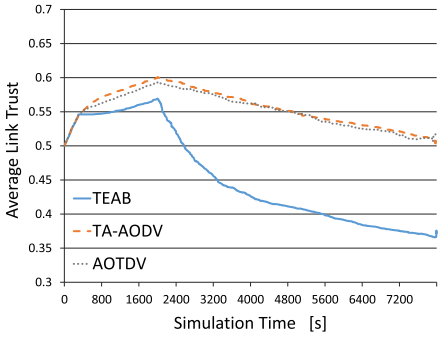

図 7 利己的ノードのリンクトラスト平均値の推移（$N_s = 10$）
Fig. 7 Variation of average linktrust of selfish nodes.

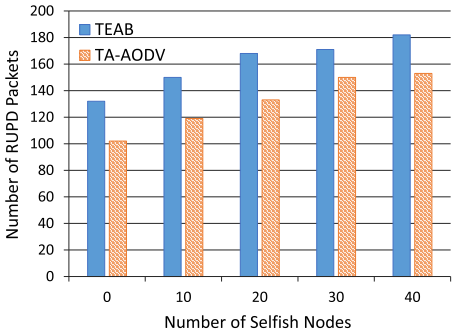

図 8 経路更新パケット数
Fig. 8 Number of RUPD packets.

も確認できた．

以上により，ノードがそれぞれの状況に合わせてタイムウィンドウを変化させるという提案手法 TEAB の動作を確認できた．

4.3 利己的ノードの被検知数

行動変化後の利己的ノードの検知の早さを比較する．ここで，利己的ノードの検知とはリンクトラストが閾値 $T_{blacklist}$ 以下になることであり，この検知は各ノードが独立して行う．行動変化時刻からの経過時間に対する利己的ノードを検知した平均ノード数（利己的ノードの被検知数）を**図 6** に示す．ここで，1 回のシミュレーションで利己的ノードは 10 個存在し，行動変化時刻はノードごとに異なる．そのため，各利己的ノードが行動を変化させたときを 0 秒とした場合の経過時間を横軸として，利己的ノードとして検知したノード数の増加について求め，10 個の利己的ノードで平均した推移を表す．図より，同じ時間で比較すると提案手法は最も多くノードによって利己的ノードが検知されており，4 pkt/s のときに既存手法を基準として平均検知数を 35%向上させることが確認できる．また，パケットレートが 40 pkt/s のときには平均検知数を最大で 110%向上させ，4 pkt/s のとき以上に提案手法の効果が確認できる．これは，可変タイムウィンドウを用いて新しい行動を評価できる提案手法は，大きいパケットレートを活用して短時間で評価を安定させることができるからだと考えられる．このことから，トラストモデルは，極端に小さいパケットレートでは評価が安定せずに効果がないが，ある程度大きいパケットレートでは提案手法は有効であると考えられる．

さらに，シミュレーション時間にともなう利己的ノードのリンクトラスト平均値の推移を**図 7** に示す．図において行動変化の影響が強くなる 2,000 秒以降に注目すると，既存手法では緩やかに行動変化に対応してトラストが低下するのに対して，提案手法では早く利己的ノードであると検知されるような低いトラストに変化する．また，行動変化の影響が少ない後半に注目すると，提案手法では利己的ノードに対して低いトラストに収束していることから，一定の行動を続けるノードに対しては従来同様の安定したトラストを維持することも確認できる．このことから，一定行動を続ける通常ノードに対しては従来の安定したトラストを維持できると考えられる．

図 6 と図 7 より，提案手法ではノードの行動に合わせたトラストを用いることで，行動変化直後に利己的ノードがより早く多くの隣接ノードに検知されたと考えられる．

4.4 経路更新パケット数

セキュアルーティングでは，リンクトラストの変化に応じて経路更新パケットが転送される．最大利己的ノード数 N_s を変化させたときの経路更新パケット数を**図 8** に示す．ここで，既存手法の AOTDV と TA-AODV では経路更新を行う条件が異なるので，提案手法の性能を確認するために更新の条件が等しい TA-AODV を比較対象とする．図 8 より，提案手法では経路更新パケットが既存手法を基準として約 23%増加することが確認できる．提案手法では行動変化直後にリンクトラストが大きく変化することで経路更新が増えたと考えられる．つまり，この結果は行動変化直後に集中して経路更新を行うことで，提案手法では各ノードが検知した利己的ノードに関する情報を経路表の更新によってデータ送信前に共有できることを意味する．一方で，制御パケットが増えることはルーティングオーバヘッドの観点から望ましくないと考えられるが，提案手法では

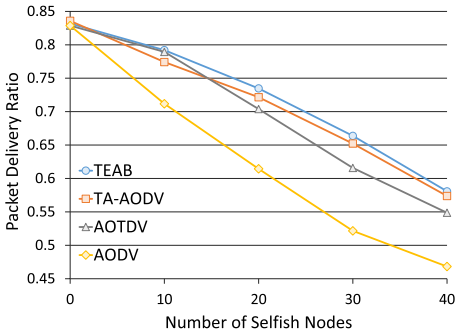

図 9 パケット到達率
Fig. 9 Packet delivery ratio.

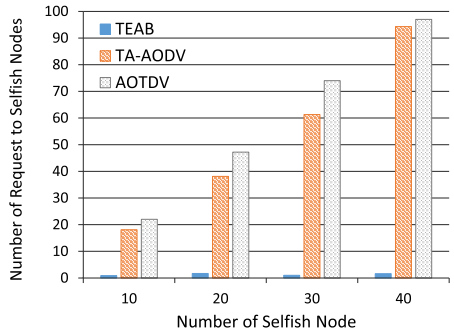

図 10 利己的ノードへの転送要求数
Fig. 10 Number of requests to selfish nodes for forwarding.

わずかな経路更新パケットの増加によってより安全な経路を選択した通信が可能になったといえる．

4.5 データパケット到達率

図 9 に最大利己的ノード数 N_s を変化させたときのシミュレーション時間 2,000 秒以降のパケット到達率を示す．図より，提案手法は高い到達率を維持しており，利己的ノードの数が 30 のとき TA-AODV より 2%，AOTDV より 5%，AODV より 15%改善される．これは，提案手法では利己的ノードを回避した経路選択によってより多くのデータが目的ノードに到達したことを示す．また，利己的ノード数の変化に注目すると，ノード数 30 において提案手法による改善が最も強く見られる．利己的ノードが少ない場合，目的ノードへの経路は多く存在するため利己的ノードの影響は小さく，一方で利己的ノードが増えすぎる場合，利己的ノードを回避した経路が存在しない可能性が高くなり，どちらにおいてもトラストモデルの違いが大きく反映されない．つまり，提案手法では目的ノードへの経路の中から利己的ノードを回避した経路を選択し，より確実なデータ転送を実現することが分かる．

4.6 利己的ノードへの転送要求数

4.5 節では提案手法による改善が見られたが，絶対的な改善量は大きくない．それは，そもそも経路が存在しないことや意図的でないパケットロスの影響を受けるからである．そこで，最大利己的ノード数 N_s を変化させたときの利己的ノードへのデータ転送要求の数を図 10 に示す．図より，提案手法では利己的ノードを含んだ経路の選択回数が少なく，既存手法を基準として 5%以下に抑制されることが確認できる．この結果は，提案手法は行動変化後の新しい行動を反映したトラストによって経路更新の頻度が上がり，経路表から利己的ノードを含む経路を早く削除することで利己的ノードを中継として使わないことを意味する．以上により，提案手法は利己的ノードを中継することで破棄されるデータパケットを削減して，より確実なデータ転送が可能であるといえる．

5. おわりに

本論文では，行動変化が発生する環境において，行動変化を検知してノードの行動に適応したトラストを算出することで，利己的ノードを含まない安全な経路を用いたデータ転送を実現する手法 TEAB を提案した．提案手法では，リンクトラストの変化量の符号と大きさに基づいて，行動を変化させたノードを検知する．そして，可変タイムウィンドウを用いることで，変化後の行動をリンクトラストに早く反映させながら，一定の行動を続けるノードに対しては安定したリンクトラストを算出できる．この提案手法をセキュアルーティングに利用すると，各ノードの経路表に利己的ノードを排除した経路が構築される．提案手法をシミュレーションにより比較評価し，ノードの行動に合わせたトラストによって行動変化直後の利己的ノードを早く検知して経路更新を行うことで，利己的ノードを回避した経路を用いたより無駄の少ない確実なデータ転送ができることを確認した．以上より，提案手法の有用性を示した．

謝辞 本研究は JSPS 科研費 25280032 の助成を受けたものです．

参考文献

[1] Cho, J.-H., Swami, A. and Chen, I.-R.: A Survey on Trust Management for Mobile Ad Hoc Networks, *Communications Surveys Tutorials*, Vol.13, No.4, pp.562–583, IEEE (2011).
[2] Abdelshafy, M. and King, P.: Analysis of security attacks on AODV routing, *8th International Conference for Internet Technology and Secured Transactions* (*ICITST*), pp.290–295 (2013).
[3] Chadha, K. and Jain, S.: Impact of black hole and gray hole attack in AODV protocol, *Recent Advances and Innovations in Engineering* (*ICRAIE*), pp.1–7 (2014).
[4] Abusalah, L., Khokhar, A. and Guizani, M.: A survey of secure mobile Ad Hoc routing protocols, *Communications Surveys Tutorials*, Vol.10, No.4, pp.78–93, IEEE (2008).
[5] Marchang, N. and Datta, R.: Light-weight trust-based routing protocol for mobile ad hoc networks, *Information Security*, Vol.6, No.2, pp.77–83, IET (2012).
[6] Poonam, Garg, K. and Misra, M.: Trust Based Multi Path DSR Protocol, *International Conference on Availability, Reliability, and Security* (*ARES*), pp.204–209

(2010).
[7] Umeda, S., Takeda, S. and Shigeno, H.: Trust Evaluation Method Adapted to Node Behavior for Secure Routing in Mobile Ad hoc Networks, *8th International Conference on Mobile Computing and Ubiquitous Networking* (*ICMU*), pp.143–148 (2015).
[8] Li, X., Jia, Z., Zhang, P., Zhang, R. and Wang, H.: Trust-based on-demand multipath routing in mobile ad hoc networks, *Information Security*, Vol.4, No.4, pp.212–232, IET (2010).
[9] Qu, C., Ju, L., Jia, Z., Xu, H. and Zheng, L.: Light-Weight Trust-Based On-Demand Multipath Routing Protocol for Mobile Ad Hoc Networks, *IEEE International Conference on Trust, Security and Privacy in Computing and Communications* (*TrustCom*), pp.42–49 (2013).
[10] 牛窪洋貴，武田苑子，重野　寛：モバイルアドホックネットワークにおけるトラストを利用した効率的セキュアルーティング，情報処理学会論文誌，Vol.55, No.2, pp.649–658 (2014).
[11] Wang, D., Muller, T., Liu, Y. and Zhang, J.: Towards Robust and Effective Trust Management for Security: A Survey, *IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications* (*TrustCom*), pp.511–518 (2014).

梅田 沙也華　（学生会員）

2014 年慶應義塾大学理工学部情報工学科卒業．現在，同大学大学院理工学研究科修士課程在学中．

大畑 百合　（学生会員）

2015 年慶應義塾大学理工学部情報工学科卒業．現在，同大学大学院理工学研究科修士課程在学中．

神本 崇史　（学生会員）

2015 年慶應義塾大学理工学部情報工学科卒業．現在，同大学大学院理工学研究科修士課程在学中．

重野 寛　（正会員）

1990 年慶應義塾大学理工学部計測工学科卒業．1997 年同大学大学院理工学研究科博士課程修了．現在，同大学理工学部教授．博士（工学）．情報処理学会学論文誌編集委員，同高度交通システム研究会幹事等を歴任．現在，情報処理学会マルチメディア通信と分散処理研究会主査．Vice Chair of IEEE ComSoc APB TAC．ネットワーク・プロトコル，ITS 等の研究に従事．著書「情報学基礎第 2 版」（共立出版）等．電子情報通信学会，IEEE，ACM 各会員．