Vol.2014-DPS-159 No.8
Vol.2014-MBL-71 No.8
2014/5/15

行動変化を伴う利己的ノードに素早く対応するトラスト算出手法

梅田 沙也華[†1]　武田 苑子[†1]　重野 寛[†1]

概要：近年注目されるモバイルアドホックネットワーク（MANET）は，ノード間で転送協力することで成立する．そのため，パケットを転送しない利己的ノードを経由するパケットは目的の端末に届かない．そこで，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．既存手法では全ノードが一定行動だと仮定し，トラストをノード間で共有するためのパケットを削減するが，実際の環境ではリソースによってパケットを転送していたノードが別の時には転送しないといった行動変化が考えられるため，このような行動変化ノードを再評価してトラストを更新する必要がある．本稿では，行動変化を検知して変化後の行動を素早く評価に反映させるトラスト算出手法 TCMBC を提案する．行動変化に対応したトラスト算出を行うため，各ノードは隣接ノードに対して，トラスト変化量からトラストの増減が変化した時を検知して，行動変化が起きたと判断する．行動変化がある場合，過去の行動の評価が直接現在の行動に繋がらないため，トラスト算出時に用いる評価時間を変化させ，最近の行動を重視した評価を行う．この手順によって，現在の行動を素早くトラストに反映させる．シミュレーションを用いて評価した結果，TCMBC を用いることで既存のセキュアルーティングと比べて早く新しい利己的ノードを検知できていることが確認された．

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

Trust Calculation Method Responding to Selfish Nodes Changing Behabior

Abstract: A mobile ad-hoc network (MANET) is built by forwarding packets cooperatively. So, the packet relayed by selfish nodes which don't forward packets can not arrive at the destination node. Secure routing protocols using trust have been developed. In the existent method, all nodes are supposed that they behave invariably and packets which is used to share trust between nodes are suppressed. But in the real environment, there are many nodes which change their behavior because of their resource, so these nodes must be revaluated and update trust. In this paper, we propose TCMBC, the trust calculated method for reflecting the new behavior in trust. When each node finds the fluctuation of the neighbor's trust, it decides the neighbor changes behavior. In case of changing behavior, the past evaluation doesn't represent the current behavior, so we evaluate the trust making a point of the current behavior. Simulation results show the secure routing using TCMBC finds new selfish nodes sooner than the existent routing.

Keywords: mobile ad hoc network, secure routing, trust

1. はじめに

近年，モバイルアドホックネットワーク（MANET）[1] は様々な場面において注目されている．MANET とは，特定の基地局を介さずにモバイル端末間で直接協調して構築されるネットワークのことである．このようなネットワークを通して，直接通信できない端末間においても，複数の端末を仲介して通信が可能になる．しかし，MANET で想定しているモバイル端末では電力や帯域幅に制限があるため，自分のリソース確保を目的として別の端末の転送に協力的でないものが存在する．このような端末は利己的ノードと呼ばれている．利己的ノードの振る舞いの 1 つとして，blackhole attack [2] と呼ばれる転送を要求されたパケット

[†1] 現在，慶應義塾大学大学院理工学研究科
Presently with Graduate School of Science and Technology, Keio University

を全て破棄する攻撃がある．また，これに類似した攻撃として，選択的にパケットを破棄する攻撃 [3] や一時的にパケットを破棄する攻撃 [4] も考えられている．MANET の特徴から見ると，このような利己的な振る舞いによって，パケット転送が目的の端末まで続かずに正常な通信ができないことがある．

そこで，MANET におけるセキュリティ対策の 1 つに，セキュアルーティングプロトコルがある [5]，[6]．セキュアルーティングプロトコルとは，トラストを用いることで利己的ノードを判別し，協力的なノードだけで転送の経路を作ることを意図した仕組みである．ここでトラストとは，ノードや経路において正しくパケットを転送できるかを表す値のことであり，このトラストによって周囲のノードが信頼できるノードか否か判断できる．セキュアルーティングプロトコルでは，パケットを用いてノード間で共有されたトラストから信頼できる経路を決定できる．しかし，このトラスト共有に使われるパケットによってルーティングのオーバヘッドが増加してしまう．そこで，MANET はリソースに限りがあるノードを対象とすることを考慮し，トラストの変化に合わせてオーバヘッドを削減したセキュアルーティングプロトコルも研究されている [7]．

現在のセキュアルーティングプロトコルでは，主にパケットを常に破棄する攻撃を考慮している．具体的には，トラスト算出の際に過去のパケット転送全てを平均的に評価することで，長期的に安定したトラストを利用している．そのため，協力的なノードが突然利己的ノードに変化した場合，変化以前の振る舞いがトラストに大きく影響することで新しい行動を正しくトラストに反映できず，信頼できる経路を選択できないという問題が生じる．このように，ノードが一定の行動をとることが前提とされている現在の手法では，途中で利己的ノードに変化するような行動変化ノードの問題が考慮されていなかった．

本稿では，行動変化が発生した場合，あるノードに対するトラストを算出する際に用いる評価時間を行動変化の有無に応じて可変にすることで，行動変化以降の行動に注目した評価を行い，現在の利己的ノードを素早く検知できるトラスト算出手法を提案する．ここでの評価時間とは，トラストを求める時に考慮される時間のことであり，評価時間前から現在までのパケット転送率によってトラストは算出される．この提案により，行動変化によって突然利己的ノードが発生した場合でも，変化後の行動から算出されるトラストにより早く利己的ノードとして検知できるようになる．その結果，通常ノードからパケット転送の要求があった場合，協力的なノードだけによる経路が選択されてパケット到達率が向上される．

2. 関連研究

本章では，はじめに一般的なセキュアルーティングで用いられるトラストモデルについて述べる．そして，このようなセキュアルーティングの 1 つとして，本稿の評価にも利用した TA-AODV について少し詳しく説明する．

2.1 トラストモデル

信頼度を表すトラストとして，リンクトラストとパストラストの 2 種類が用いられている [6]．以下では，それぞれの算出方法と特徴を述べる．

2.1.1 リンクトラスト

各ノードは隣接ノードにパケットの中継を要求した直後，プロミスキャスモードにより中継が正しく行われるかどうか確認する．この結果から，隣接ノードのパケット転送における振る舞いを評価した値がリンクトラストである [8]．時刻 t におけるノード i が隣接ノード j に対して持つリンクトラスト $L_{ij}(t)$ は式 (1) から算出される．

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

ここで，$N_C(t)$ は時刻 t までにノード j がノード i からのパケットを正しく転送した回数，N_A は時刻 t までにノード i がノード j に対して転送要求したパケットの総数を表す．また，W はウィンドウサイズと呼ばれて評価時間の幅を示す．このリンクトラストは W 時間におけるパケット転送率を意味するため，リンクトラストが 1 に近い値であることは転送に協力的で信頼できるノードであることを表し，一方で 0 に近いリンクトラストはほとんどパケット転送に協力しないノードを表していると判断できる．ここから，既存のセキュアルーティングでは各ノードの保持するリンクトラストがブラックリスト定数 $T_{blacklist}$ 以下であるノードを利己的ノードであると判断する．そして，各ノードは利己的ノードと判断したノードを一定時間自身のブラックリストに入れて，隣接ノードとしてパケット転送を行うことをしない．この仕組みによって，利己的ノードを含まないネットワークを構築することを目指す．

2.1.2 パストラスト

リンクトラストを利用して，経路全体の信頼度を表したのがパストラストである．このパストラストは，中継ノードのリンクトラストの連続積によって定義されているため，その経路に沿って送信されたパケットが送信元ノードから目的ノードまで到達する確率を表す [9]．時刻 t における経路 $path$ のパストラスト T_{path} は式 (2) から算出される．

$$T_{path} = \Pi(L_{ij}(t) | n_i, n_j \in path \quad and \quad n_i \rightarrow n_j \quad and \quad n_j \neq N_d) \quad (2)$$

ここで，n_i と n_j は経路 $path$ 上に存在する隣接したノードであり，N_d は経路 $path$ における目的ノードである．そして，$n_i \rightarrow n_j$ は n_j が n_i の次のホップであることを示す．

セキュアルーティングでは，このパストラストは制御パケット内で転送の度に算出される．そして，各ノードが保持する経路表の中にパストラストの項目を加える．この情報を比較することで，各ノードはある目的ノードに対してより安定した通信経路を選択することが可能になる．

2.2 セキュアルーティングプロトコル

トラストを用いたセキュアルーティングプロトコルとして，AODV[10] を基にした TA-AODV[7] がある．トラストを導入することにより，セキュアルーティングでは制御パケットが増えすぎるという問題から，TA-AODV では制御パケットの削減を目指している．そこで，経路更新に利用される RUPD パケットの転送頻度を制御する．

一般的なセキュアルーティングプロトコルでは，リンクトラストの変化に合わせて，その値から算出されるパストラストを更新するために RUPD パケットが定期的にブロードキャストされる．しかし，MANET では移動があるノードを含んでいることを考慮して，リンクトラストの変化量に応じて RUPD パケットの転送頻度を決定することが有効であると言える．つまり，変化量が多く経路全体にも大きく影響する場合には転送頻度を上げてパストラストが早く収束することを目指し，それ以外の場合では余剰なパケットを削減する．

TA-AODV では一定行動をとるノードに対するリンクトラストは初期値に近いほど大きく変化し，時間の経過とともに一定値に収束する性質を利用した．そこで更新頻度の決定のために使われる閾値である更新スレッショルド T_{ij} は式 (3) から算出される．

$$T_{ij}(t) = \beta \times |L_{ij}(t) - L_{ini}| \tag{3}$$

ここで，β は更新定数，L_{ini} はリンクトラストの初期値を表す．この更新スレッショルド以上にリンクトラストが変化した場合にのみ経路更新を行うことで，更新パケットの数を効率的に削減可能にする．

2.3 既存手法の問題点

MANET には様々な攻撃が考えられている [11]．既存のセキュアルーティングでは，安定した長期的な評価によってトラストを算出しているため，リソースの変化に合わせて利己的ノードに変化するような行動変化は考慮されていない．そのため，1 回の転送結果はリンクトラストに対して大きな影響を持たず，リンクトラストの変化が緩やかになることが考えられる．ここで，リンクトラストが大きく変化しないことにより，以下の 2 つの問題があげられる．

- リンクトラストから利己的ノードを正しく判断できない
- 経路更新の頻度が低くなるため信頼できる経路が選択できない

既存手法において，リンクトラストが一定以下になったノードに対して利己的ノードと判断しているため，リンクトラストの変化が緩やかになると正しい判断ができなくなる．また，リンクトラストの変化量に応じて経路更新の頻度が決定するため，経路の情報を書き換えるためにも現在の行動に合わせてリンクトラストを大きく変化させなければならない．そのため，行動変化を伴う利己的ノードに対して新しい行動を素早くトラストに反映させる必要があるといえる．

3. 提案

本稿では，利己的ノードにおける行動変化を検知して新しい行動を素早く評価に反映させるトラスト手法として，TCMBC (Trust Calculation Method for Evaluating Behavior Change Nodes) を提案する．以下では，TCMBC について説明する．

3.1 提案の概要

提案手法 TCMBC は，セキュアルーティングプロトコルにおけるトラスト算出手法である．行動変化が発生した場合，あるノードに対するトラストを算出する際に用いる評価時間を行動変化の有無に応じて可変にすることで，行動変化以降の行動に注目した評価を行い，現在の利己的ノードを素早く検知できるトラスト算出手法である．本手法は，以下にあげる 2 つの段階を通して利己的ノードの行動変化に対応する．

- リンクトラストの変化量による行動変化の検知
- 可変評価時間を用いた新しい行動に対する評価

はじめに行動変化があるかどうかに注目し，行動変化が検知された場合にのみ新しい行動を重視した評価を行う．この 2 段階の提案手法によって行動変化を伴う利己的ノードに対応した評価を実現する．

以下では，TCMBC の具体的な仕組みを述べる．

3.2 リンクトラストの変化量による行動変化の検知

行動変化を検知するために，リンクトラストの変化量を利用する．本提案では時刻 t におけるノード i のノード j に対する変化量 $\Delta L_{ij}(t)$ は式 (4) によって定義する．

$$\Delta L_{ij}(t) = L_{ij}(t) - L_{ij}(t - \Delta t) \tag{4}$$

ここで，$L_{ij}(t)$ は時刻 t におけるノード i のノード j に対するリンクトラストであり，式 (1) から算出される．また $t - \Delta t$ は前回算出されたリンクトラストを表すので，変化量は直前のリンクトラストから現在のリンクトラストにどの程度変化があったのかを示す．そのため，変化量とノードの行動には以下の関係があるといえる．

- $\Delta L_{ij}(t) > 0$： ノード j はノード i から要求されたパケット転送に協力

- $\Delta L_{ij}(t) < 0$： ノード j はノード i から転送要求されたパケットを破棄

このような特徴から，本稿では各ノードが保持しているリンクトラストにおいて変化量の正負が逆転した場合，行動変化が検知されたと定義する．ただし，この時点で変化量が正から負に変わったノードを利己的ノードであるとは考えない．パケットエラーや誤検知なども考慮し，この段階では隣接ノードに行動変化があったことだけを検知し，このノードが通常の協力的なノードであるか利己的ノードに変化したのかは判断しない．行動変化が検知された時，そのノードが現在利己的ノードであるかを決定するため，新しい行動に注目した評価を行う．

3.3 可変評価時間を用いた新しい行動に対する評価

行動変化を検知した場合，その隣接ノードが利己的ノードに変化した疑いがあると考え，古い行動に大きな影響を受けずに評価を行いたい．そこで，本提案では新しい行動に注目した評価を行うために可変評価時間を導入する．

既存のセキュアルーティングプロトコルにおいて，リンクトラストは式 (1) によって算出される．ここで，W は全てのノードにおいて常に一定であった．さらに AODV を基にした TA-AODV ではこの W を長い値で固定することで，過去の多くの行動を評価して安定したリンクラストを算出している．しかし，行動変化がある場合には過去の行動の評価が現在の行動を表していないので，固定の W は有効でない．

そこで行動変化に合わせてこの評価時間 W を変えることで，リンクトラスト算出の時に考慮する過去の行動を制御する．時刻 t においてノード i がノード j のリンクトラストを算出する際に用いる評価時間 $W_{ij}(t)$ は式 (5) によって定義する．

$$W_{ij}(t) = \min\{W_{\max}, t - T\} \tag{5}$$

ここで，T とは行動変化が検知された時刻を表す．さらに $W_{\max}$ は最大評価時間定数として，既存手法に基づいて大きな値で固定する．つまり，行動変化の直後は変化時から現在までの行動を評価できるように評価時間を長くしていき，最近の行動変化から $W_{\max}$ 時間経過した以降は常に評価時間 $W_{\max}$ を用いる．これによって，一定行動をとっているノードに対しては，長い評価時間により多くの行動から安定したリンクトラストを算出できる．一方で行動変化が検知されたノードに対しては，過去の評価によらず新しい行動を直接表したリンクトラストを算出できる．図 1 はパケット転送の結果の例と，その場合に行動変化を検知する前後での評価時間の変化を表す．

このように，行動変化を検知して評価するという 2 段階の仕組みを利用することで，行動変化を伴う利己的ノードが存在するネットワークにおいても，現在の行動を素早くトラストに反映することが可能になる．

表 1 トラスト記録表の項目

ノード ID
リンクトラスト (L)
N_C：正しく転送されたパケットの総数
N_A：転送要求したパケットの総数
リンクトラストの変化量 (ΔL)
評価時間 (W)
行動変化時刻 (T)
パケットバッファ

3.4 TCMBC を用いたセキュアルーティング

以下では，このトラスト算出手法を既存のルーティングに用いた場合の仕組みを述べる．セキュアルーティングにおいて，各ノードは全隣接ノードに対してトラストに関する記録表を保持する．TCMBC を利用する場合，既存のセキュアルーティングのものに評価時間 (W)，行動変化時刻 (T)，リンクトラストの変化量 (ΔL) の 3 つの項目を追加する．そして，トラスト記録表全体は表 1 のような 8 つの項目で構成される．

ノード i から j にパケット転送の要求があった場合，ノード i は j に送信したパケットをパケットバッファに加え，ノード j の行動を監視して N_A と N_C を更新する．さらに，N_A と N_C から新たに算出されるリンクトラストと現在保持しているリンクトラストを用いて式 (4) から変化量 ΔL_{ij} を求める．ここでトラスト記録内の変化量と新しい変化量を比較してノード j に行動変化が検知された時には，式 (5) を用いて評価時間 $W_{ij}(t)$ も更新する．この時に行動変化時刻 T も現在の時刻に書き換える．このように，パケット転送が行われる度にトラスト記録表の内容を書き換えることで，TCMBC を利用したリンクトラストの算出を行う．

4. シミュレーション評価

提案手法 TCMBC を評価するために，シミュレーションによる評価を行った．評価にあたり，TCMBC を既存の TA-AODV に適応し，AODV，TA-AODV と比較した．

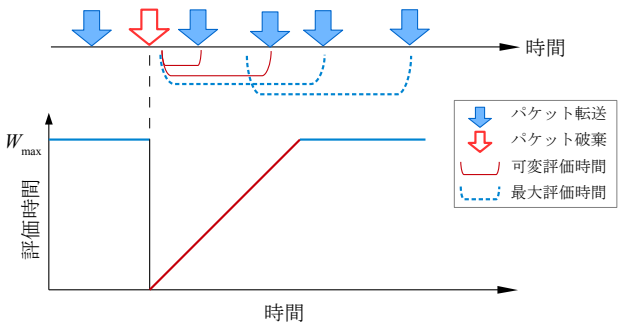

図 1 評価時間の移り変わり

表 2　シミュレーション条件

パラメータ	値
シミュレータ	Qualnet 5.0.2
シミュレーション時間	8000 sec
全ノード数	100
無線規格	IEEE 802.11b
マップサイズ	750m × 750m
転送範囲	250m
トラフィックの種類	CBR (UDP)
パケットサイズ	512 byte
パケットレート	4 pkts/s
モビリティモデル	Random waypoint
ノードの最大速度	2 m/s
接続数	20
利己的ノードの割合	0〜40 %
リンクトラストの初期値 L_{ini}	0.5
ブラックリスト定数 $T_{blacklist}$	0.5
RUPD 更新定数　β	0.3
最大評価時間　$W_{\max}$	1000 sec

4.1　シミュレーションモデル

表 2 はシミュレーションのパラメータを示す．全てのノードは初め 750m×750m の範囲でランダムに配置され，最大速度 2 m/s で移動しながらランダムに選択されたノードへデータパケットを送信するという手順を繰り返し行う．また，各ノードは 1 ホップにおける転送範囲 250m の中で通信が可能とする．ノードの行動モデルとしては，通常ノードと行動変化を伴う利己的ノードが存在する．通常ノードは常に全てのパケット転送を行う．一方，行動変化を伴う利己的ノードは，シミュレーション開始時には通常ノードと同様に振る舞うが，一定以上のパケット転送を行った以降は全パケットを破棄して転送に協力しない．つまり，今回のシミュレーションでは初めは全てのノードがパケット転送を行うが，時間の経過とともにパケット破棄を行うノードが増えていく環境を想定している．

また，評価項目としては以下の 3 項目を用いた．

- 行動変化の検知時間：
  利己的ノードが行動変化を起こした時刻から，そのノードが別のノードによって利己的ノードとして検知されるまでの時間．
- 破棄されたデータパケット数：
  未検知の利己的ノードに転送要求を行うことによって破棄されたデータパケットの数．
- パケット到達率：
  送信元において送信されたデータパケット数に対する正しく目的ノードに到達したデータパケット数の割合．信頼度の高い経路が選択できたかを表す．

4.2　行動変化の検知時間

図 2 は様々な利己的ノードの割合において，それぞれのノードが自身の算出するリンクトラストから利己的ノードを検知できるまでにかかる時間の平均値を表す．ここで，リンクトラストがブラックリスト定数 $T_{blacklist}$ 以下になった時，1 つのノードが 1 つの利己的ノードを検知できたと判断する．図 2 を見ると，TA-AODV と提案手法の両方の結果で利己的ノードが少ない時には検知時間が長いが，利己的ノードの割合が増えた時に検知時間が最小になり，さらに増えると検知時間も長くなることがわかる．利己的ノードが極度に少ない場合，1 つの目的ノードに対して多くの経路候補をあげることができる．そのため，利己的ノードが転送に利用される確率も低くなるので，利己的ノードの検知に時間がかかる．一定以上の利己的ノードが存在すると，利用できる経路も限られてくるため利己的ノードは早く検知される．しかし，さらに利己的ノードの割合が増えてしまうと，パケット転送が続きにくくなることでパケットの流れがなくなり，リンクトラストも更新されなくなる．

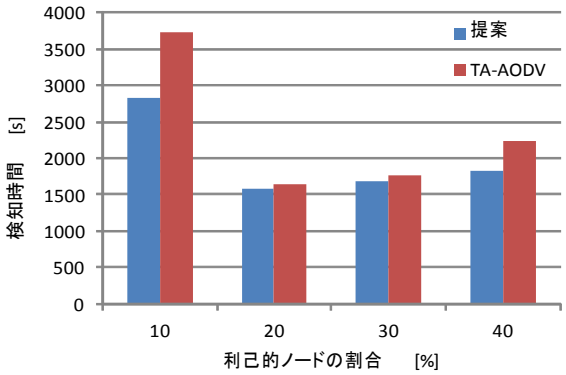

図 2　平均検知時間

さらに，図 2 から提案手法と TA-AODV と比較すると，提案手法において検知時間を短縮できていることが確認できる．特に，利己的ノードの割合が少ない場合に提案手法が有効であることがわかる．利己的ノードが少ない場合，信頼できる経路の候補が多く存在するため，提案手法によって検知時間を短縮できれば利己的ノードを含む経路を利用している場合に早く信頼できる経路に変更できる．そして，別の利己的ノードが発生した時に検知するまでの時間も削減できることから，より提案手法による改善がみられたと考えられる．この結果から，提案のトラスト算出手法を用いることで，特に利己的ノードの割合が少ない場合に行動変化を伴う利己的ノードをより早く検知できることが示せた．

4.3　破棄されたデータパケット数

通常ノードのように行動していたノードが，行動変化を起こして利己的ノードになった場合，行動変化以前にこのノードと通信した経験を持つノードは，通常ノードと同様

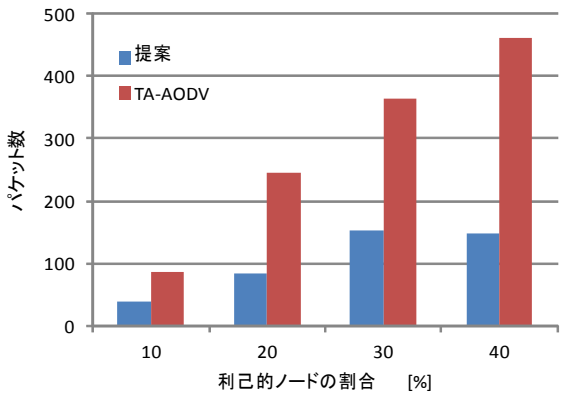

図 3 破棄されたデータパケット数

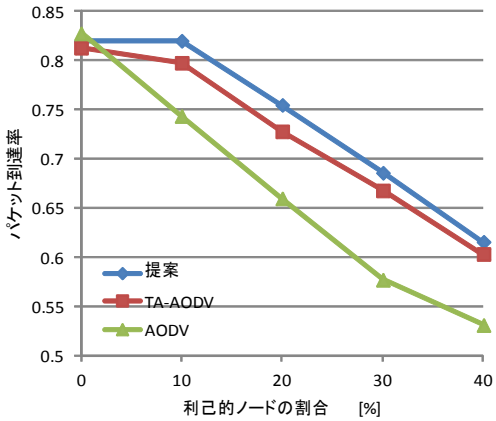

図 4 パケット到達率

の良い評価をすると考えられる．このように，未検知の利己的ノードにパケット要求を行うことで，データパケットが破棄されることがある．

図 3 は，利己的ノードの割合を変化させた時，未検知の利己的ノードによって破棄されるデータパケット数を提案手法と TA-AODV において示した結果である．この結果から，利己的ノードの割合によらず TCMBC を用いることで TA-AODV に対してパケット数を 50% 以上削減できることがわかる．これは，利己的ノードを検知するまでの時間も影響するが，TCMBC ではリンクトラストの変化に合わせて各ノードが保持する経路表も早く更新される．経路表の更新によって，早く利己的ノードを転送経路から除くことができるため，利己的ノードによって破棄されるデータパケット数も削減できると考えられる．

4.4 パケット到達率

図 4 は，利己的ノードの割合を変化させた時の提案手法と TA-AODV，AODV におけるパケット到達率の比較を表す．この結果から，TCMBC を利用することで TA-AODV より約 3% ，AODV より約 11% パケット到達率を向上できていることが示せる．特に，利己的ノードの割合が少ない場合，提案手法では利己的ノードが存在しない時に等しいパケット到達率が実現できている．これは，提案では利己的ノードを早く検知して，転送率が高く安全な経路を選択できることで，ネットワーク全体においてもデータパケットの高い到達率につながるからだと考えられる．さらに，経路選択において利己的ノードを回避した通信ができる可能性が高いと考えられる利己的ノードの割合が少ない環境では，転送経路を決定する時に利己的ノードを早く判断できる TCMBC を用いることで，より高い効果が見られることがわかる．

5. おわりに

本稿では，行動変化が発生した場合，あるノードに対するトラストを算出する際に用いる評価時間を行動変化の有無に応じて可変にすることで，行動変化以降の行動に注目した評価を行い，現在の利己的ノードを素早く検知できるトラスト算出手法 TCMBC を提案した．TCMBC では，行動変化を検知して，行動変化ノードに対してリンクトラスト算出時に用いる評価時間を変化させるという 2 段階の手順によって，行動変化があった場合現在の行動を素早くトラストに反映することができる．さらに，TCMBC を既存のセキュアルーティングに取り入れることで，行動変化に合わせて早く変動したトラストから，信頼できる経路を選択した通信が可能になる．

コンピュータシミュレーションを用いて評価を行った結果，TCMBC を用いると，TA-AODV と比べてより早く多くのノードが新しく発生した利己的ノードを検知できていることが確認された．さらに，提案手法によって経路情報も早く更新され，利己的ノードを中継として選択することによって破棄されるパケット数やパケット到達率においても，既存手法に比べて向上が見られた．また，利己的ノードの検知時間とパケット到達率において，利己的ノードの割合が 10% の時に提案手法における改善が大きく見られたことから，提案手法は利己的ノードの割合が少ない時に特に有効だといえる．以上より，既存の TA-AODV と比較して TCMBC を用いることでより早く安全な経路によって通信が実行できることが示せた．

謝辞 本研究の一部は，JSPS 科研費（B）課題番号 25280032（2013 年）の助成により行われました．

参考文献

[1] Corson, S. and Macker, J.: Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, RFC 2501 (Informational) (1999).

[2] S. Kurosawa, H. Nakayama, N. K. A. J. and Nemoto, Y.: Detecting blackhole attack on aodv-based mobile ad hoc networks by dynamic learning method, *International Journal of Network Security*, Vol. 5, No. 3, pp. 338–345

(2007).
[3] Sen, J., Chandra, M., Harihara, S., Reddy, H. and Balamuralidhar, P.: A mechanism for detection of gray hole attack in mobile Ad Hoc networks, *Information, Communications Signal Processing, 2007 6th International Conference on*, pp. 1–5 (2007).
[4] Perrone, L. and Nelson, S.: A Study of On-Off Attack Models for Wireless Ad Hoc Networks, *Operator-Assisted (Wireless Mesh) Community Networks, 2006 1st Workshop on*, pp. 1–10 (2006).
[5] Abusalah, L., Khokhar, A. and Guizani, M.: A survey of secure mobile Ad Hoc routing protocols, *Communications Surveys Tutorials, IEEE*, Vol. 10, No. 4, pp. 78–93 (2008).
[6] Li, X., Jia, Z., Zhang, P., Zhang, R. and Wang, H.: Trust-based on-demand multipath routing in mobile ad hoc networks, *Information Security, IET*, Vol. 4, No. 4, pp. 212–232 (2010).
[7] 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).
[8] Zhang, C., Zhu, X., Song, Y. and Fang, Y.: A Formal Study of Trust-Based Routing in Wireless Ad Hoc Networks, *INFOCOM, 2010 Proceedings IEEE*, pp. 1–9 (2010).
[9] Sun, Y., Yu, W., Han, Z. and Liu, K.: Information theoretic framework of trust modeling and evaluation for ad hoc networks, *Selected Areas in Communications, IEEE Journal on*, Vol. 24, No. 2, pp. 305–317 (2006).
[10] Perkins, C. and Royer, E.: Ad-hoc on-demand distance vector routing, *Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on*, pp. 90–100 (1999).
[11] Cho, J.-H., Swami, A. and Chen, I.-R.: A Survey on Trust Management for Mobile Ad Hoc Networks, *Communications Surveys Tutorials, IEEE*, Vol. 13, No. 4, pp. 562–583 (2011).