情報処理学会論文誌 Vol.55 No.2 649–658 (Feb. 2014)

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

牛窪 洋貴[1,a)] 武田 苑子[1] 重野 寛[2]

受付日 2013年5月13日, 採録日 2013年10月9日

概要：モバイルアドホックネットワークでは，リソース温存のためパケットを意図的に破棄する利己的ノードが存在する．利己的ノードへの対策として，評価値を用いて安定した通信経路を構築するセキュアルーティングプロトコル（SRP）が研究されている．評価値とは正常にパケットを転送できるかの信頼度を表す値である．しかし，従来の SRP はルーティングにかかるオーバヘッドが増大するという問題がある．そこで，本論文ではルートリクエスト（RREQ）パケットと経路更新（RUPD）パケットを効率的に削減した SRP である TA-AODV を提案する．まず，TA-AODV では評価値をパケットの転送基準としても利用し，経路構築にかかる不要な RREQ パケットの削減を行う．また，経路情報の変化量に応じて RUPD パケットを転送することで効率的に経路の維持を行う．提案手法の評価はシミュレーションにより行い，制御パケット数を削減しつつ，高いデータパケット到着率を維持しているという結果から TA-AODV の有用性を示す．

キーワード：アドホックネットワーク，セキュアルーティングプロトコル，トラスト

An Effective Secure Routing Protocol Considering Trust in Mobile Ad hoc Networks

Hiroki Ushikubo[1,a)] Sonoko Takeda[1] Hiroshi Shigeno[2]

Received: May 13, 2013, Accepted: October 9, 2013

Abstract: In a mobile ad-hoc network (MANET), selfish nodes arbitrarily drop data packets delivered from other nodes to save their own resources. Secure routing protocols (SRP), which use trust in the routing process, have been developed in order to protect MANET. Trust can be defined as the accuracy and sincerity of the immediate neighboring nodes. The secure routing protocols, however, have larger routing over head. This paper proposes TA-AODV which suppress routing overhead, namely number of route request (RREQ) packets and route update (RUPD) packets, effectively by considering characteristic of trusts. First, we suppress the the number of redundant RREQ packets by each relay node selectively forwarding the packets based on trust. Second, we maintain routes effectively by flooding RUPD packets according to the variation of route information. We evaluate TA-AODV through the computer simulation. The results show that packet delivery ratio keeps up a high level, while the total number of control packets are reasonably cut down.

Keywords: ad hoc networks, secure routing protocol, trust

1. はじめに

近年，モバイルアドホックネットワーク（MANET）が様々な場面で注目されている．MANET は特定の基地局などを介さずノード間で協調して構築されるネットワークである．ノードが自由にネットワークに参加し，ノード自

[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
[2] 慶應義塾大学理工学部
Faculty of Science and Technology, Keio University, Yokohama, Kanagawa 223–8522, Japan
[a)] ushikubo@mos.ics.keio.ac.jp

体がパケット中継の機能を果たすことでネットワークの柔軟性や拡張性を高めている．しかし，このような環境下ではプロトコルに従わない利己的なノードも介入しやすいといった問題がある [1]．具体的には，利己的ノードとは自身のリソース保持を目的として意図的にパケットを破棄するノードのことを示す．そのため，宛先やルーティング情報を改ざんすることにより，ネットワークを破壊することが目的である “悪意あるノード” とは区別される．一般に，MANET に参加する無線端末はバッテリで動作することが想定され，送受信帯域などの性能にも限りがあることから，自身のリソースの温存のためパケットを破棄する利己的ノードが発生し，このような利己的な行動により正常な通信が阻害されるため問題となる [2], [3].

MANET におけるセキュリティの 1 つに，セキュアルーティングプロトコル（SRP）がある [4], [5], [6]．SRP ではトラストの手法を取り入れ，パケットを意図的に破棄する利己的ノードを回避した経路を構築することを目的としている．トラストとはノードの信頼度を数値化した値である評価値を算出し合い，評価値を用いてノード間で協調してセキュリティを構築するセキュリティ手法の 1 つである [7]．SRP における評価値は各ノードが正常にパケットを中継するか否かの信頼度を表す．MANET では特定のインフラの利用を想定していないため，ノード間で分散的にセキュリティを構築する仕組みが必要となる．

しかし，SRP では安全な経路を捜索するにあたりより多くの RREQ パケットを転送する必要があるため，最短経路を構築する既存のルーティングと比べオーバヘッドが増加する．さらに，SRP では評価値の変化を通知するため，定期的に更新メッセージである経路更新（RUPD）パケットをフラッディングする．評価値の変化は一定周期で起こるとは限らず，評価値更新の通知が必要ない際に不要な RUPD パケットをフラッディングしてしまうことがある．MANET では各ノードの保持電力や帯域には限りがあるため，このオーバヘッドをいかに抑えるかが重要となる．

そこで，本論文では評価値を用いて RREQ パケットと RUPD パケットを効率的に削減することにより，経路構築にかかるオーバヘッドを抑制する手法 TA-AODV を提案する．提案手法では各中継ノードは隣接ノードに対して持つ評価値を参照し，評価値の低いノードへ RREQ パケットの転送停止命令を出すことで選択的にパケットを削減する．また，隣接ノードの評価値の変化量に応じて RUPD パケットの転送頻度を変動させることにより，更新メッセージ数の削減を行いつつ高信頼経路の構築を維持する．

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 TA-AODV 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効性を示す．最後に 5 章で結論を述べる．

2. 関連研究

本章では SRP における既存研究をあげ，評価値の算出方法や評価値を用いたルーティングについて述べる．

2.1 MANET における SRP

SRP は既存のルーティングプロトコルに評価値を導入し，安定した経路を構築することを目的としている．SRP における評価値は大きくリンクトラストとパストラストに分けられる．リンクトラスト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表す．また，パストラストはリンクトラストから算出され，目的ノードまでパケットを正常に転送できるかの信頼度を表す．SRP では経路表と制御パケットにパストラストを保持するフィールドを追加し，中継ノードは RREQ パケット，RREP パケットを転送する中で各ノードのリンクトラストを集約し，パストラストを算出する．そしてパストラストの高い経路を選択しデータパケットを流すことでより安定した通信を実現する．

基本とするプロトコルにより，SRP も大きくリアクティブ型とプロアクティブ型に分けられる [8]．リアクティブ型のプロトコルは通信要求があったときのみ経路構築を行うためリソースを温存することができる．そのため MANET などリソースの限られた環境により適していると考えられ，以後我々はリアクティブ型プロトコルに焦点を絞る．リアクティブ型 SRP の代表的なものとして ATDSR [9] と AOTDV [10] がある．ATDSR は DSR [11] をベースとし，AOTDV は AODV [12] をベースとした SRP を確立している．

2.2 MANET における評価値の算出

2.2.1 リンクトラストの算出

パケットをフラッディングしたノードはプロミスキャスモードにより隣接ノードが自身の転送したパケットを正常に中継するか確認する．そして，時刻 t においてノード i が隣接ノード j に対して持つリンクトラスト $L_{ij}(t)$ を式 (1) から算出する．

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

ここで，$N_C(t)$ はノード j が i からのパケットを正常に転送した回数，$N_A(t)$ はノード i が j へパケットを転送した総数を示す．

利己的ノードのように意図的にパケットを破棄する場合に加え，モビリティや外部環境によりパケットが正常に転送できなかった場合も転送失敗と見なし，リンクトラストが下がる要因となる．W は一定の評価期間を示すタイムウインドウであり，W 時間ごとにリンクトラストが算出される．$L_{ij}(t)$ は 0 から 1 の値で表され，1 に近いほどノード

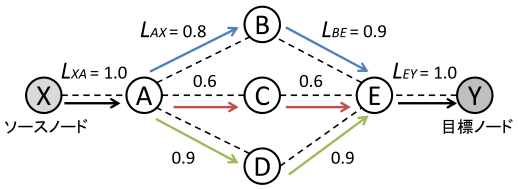

図 1 パストラスト算出例
Fig. 1 Example of calculating path trusts.

j は正常にパケットを中継する可能性が高いと判断できる．一方，$L_{ij}(t)$ がある閾値以下の場合，各ノードが固有に持つブラックリストにアドレスが追加される．ブラックリストに追加された場合，ある一定期間ノード j へのパケットの転送や j からのパケットの中継も行わない．

2.2.2 パストラストの算出

パストラスト T_P とは経路の安定性を数値化したものである．パストラストは経路上に存在するノード間のリンクトラストから算出される．SRP では制御パケットにパストラストを計算するフィールドを保持し，パストラストは制御パケットを転送していく中で算出される．

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

ここで，n_i，n_j はパス P 上に存在するノードであり，N_d は経路 P の目標ノード，$n_i \to n_j$ は n_j が n_i の隣接ノードであることを示す．

図 1 を用いてパストラストの算出例を示す．矢印は評価の向きを表す．まず，ソースノード X が RREQ パケットのフラッディングを開始し，3 つの経路をたどり目標ノード Y まで到達したとする．ここで，RREP パケットがノード E，B，A，X の順で返信された場合を例にとる．このとき，まず目標ノード Y から RREP パケットを受信したノード E は，RREP パケットのパストラストのフィールド $T_{(path)}$ に L_{EY}=1.0 を書き込み，ノード B へユニキャストで RREP パケットを返す．さらにノード B はパストラストのフィールドを $T_{(path)}$=L_{BE} × L_{EY}=0.9 ×1.0=0.9 に更新してノード A へ RREP パケットを返す．これを繰り返すことでソースノード X が目標ノード Y へのパスに対して持つパストラスト $T_P(X, A, B, E, Y)$ は 0.72 と計算される．同様にして $T_P(X, A, C, E, Y)$=0.36，$T_P(X, A, D, E, Y)$=0.81 となり，パストラストを比較することで経路 $P(X, A, D, E, Y)$ が最も安定した通信経路であると相対的に判断できる．

2.3 評価値を利用したルーティングプロトコル

SRP の最大の目的は目標ノードまで最短かつ最もパストラストの高い経路を構築することである．これを達成するため各ノードは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．トラストレコードとはリンクトラスト算出に関わるデータを格納したものであり，各ノードが隣接ノードに対し固有に保持する．SRP における経路表は**表 1** に示すような 6 つのフィールドからなる．表 1 の例では，宛先ノード E までパケットを届けるためには次にノード A または B へパケットを転送すればよいことが分かる．さらに SRP では，パストラストがより大きいノード A を経由する経路を採用する．このようにして目標ノードまで最短経路かつパストラストの高い経路を構築する．その後，ソースノードの要求に従いデータパケットを転送すると，SRP ではプロミスキャスモードにより隣接ノードのパケット転送状況を監視する．もしパケットが正常に中継されなければ利己的ノードが存在する低信頼な経路であるため，経路情報を更新する必要がある．そこで SRP では構築経路のパストラストを更新するため，新たに RUPD パケットを導入している．RUPD パケットは更新ホップ数と更新パストラストのフィールドを持ち，各ノードは RUPD パケットを周期的にフラッディングすることで経路情報の変化を各ノードに通知する．

表 1 SRP のルーティングテーブルの例
Table 1 Example of routing table in SRP.

宛先ノード	宛先シーケンス #	Route List			
		次ノード	ホップ数	パストラスト	有効期間
A	1	C	1	1	5
E	2	A	4	0.8	4
		B	4	0.6	4

2.4 SRP の問題点

SRP ではルーティングに要するオーバヘッドが増加し，結果的にノードのリソースが大きく消耗するといった問題がある．この根本的原因として，

(1) 高信頼経路構築にともなう不要な RREQ パケット転送
(2) 経路情報更新のための RUPD パケット転送

が考えられる．まず，原因 1 について図 1 の例を用いて解説する．図 1 において，ノード E へ順にノード B，C，D から RREQ パケットが転送されてきたとする．一般的なルーティングプロトコルでは最短経路のみを構築するため，後から転送されてきたパケットは経路のホップ数が同等以上であれば破棄する．図 1 の例ではノード E はノード B からの RREQ のみを転送する．一方，SRP では記載されたパストラストがより高い RREQ パケットを転送する．図 1 の例では，ノード E はまずノード B からの RREQ パケットをノード Y へ転送する．次にノード C から受信した RREQ パケットのパストラストは 0.36 と，先に受信したノード B からの RREQ パケットのパストラスト 0.72 より低いため，破棄する．最後にノード D から受信した RREQ パケットのパストラストは 0.81 と最も高いためノード Y へ転送する．よって，最もパストラストが

高い経路 $P(X, A, D, E, Y)$ がデータ転送経路として用いられることになる．そのため，パストラストが低いために破棄されてしまった経路 $P(X, A, C, E, Y)$ 上に存在するノード A，C は，この信頼性の低い経路の構築のために不要な RREQ パケットを転送してしまっていることになる．よって，パストラストの低い経路の構築を抑制する必要がある．また，SRP では経路表に保持する各経路に対し一定のタイムアウト時間を設け，この時間ごとに RUPD パケットをフラッディングすることで経路情報の変化を通知する．しかし，リンクトラストやパストラストの変化は一定周期とは限らず，変化の少ないような更新通知の必要のない場合には不要な RUPD パケットをフラッディングしてしまう可能性がある．そのため，RREQ パケットと RREP パケットを効率的に削減し，ルーティングに要するオーバヘッドを抑制する手法が必要となる．

3. TA-AODV の提案

本章では評価値を用いて SRP における経路構築に要するオーバヘッドを抑制する手法 TA-AODV（Trust Aware Ad hoc On-demand Distance Vector）を提案する．

3.1 TA-AODV の概要

提案手法の目的は，経路構築に要するパケット数の削減を行いつつ，パケットを破棄する利己的ノードを回避した経路を構築し，高いデータパケット到着率を実現することである．提案手法では既存の SRP において不要な RREQ パケット，RUPD パケットがフラッディングされていることに着目し，これらを効率的に削減することで経路構築にかかるオーバヘッドを抑制する．まず，提案手法ではリンクトラストの低い隣接ノードに対し RREQ パケットの転送停止命令を出す．これにより，パストラストが低く結果的に破棄される可能性の高い経路の構築を抑制し，データ転送経路構築に要する総 RREQ パケット数を削減する．さらに，RUPD パケットの更新をリンクトラストの変化量に応じて行う．具体的には，リンクトラストやそれにともなうパストラストの変化量が大きいと考えられる場合には更新頻度を上げ，変化量が少ない場合には更新頻度を落とすことで，効率的に RUPD パケットをフラッディングする．そのため，リンクトラストの変化量に応じた更新スレッショルドを新たに定義し，スレッショルドに応じて RUPD パケットをフラッディングする手法を導入する．以下では，RREQ パケット転送停止アルゴリズムや，RUPD パケットの転送方法について述べる．

3.2 RREQ パケット転送停止アルゴリズム

一般的な SRP ではデータ転送経路の探索は自身の経路表に信頼できる経路情報がないときに行われ，各ノードは RREQ パケットをフラッディングし，RREP パケットの返信を待つ．ここで，提案手法においてはすべての RREQ パケットを中継するわけではない．提案手法では，リンクトラストが低くパケットを破棄する可能性の高い 1 ホップ圏内にいる隣接ノードに対しては，RREQ パケットの転送を停止するよう RREQ パケットのフラッディングにより通知する．そして，その RREQ パケットを受信した隣接ノード自身が転送停止を求められているかを個別に判断し，RREQ パケットの転送停止を実行する．このように，隣接ノードに対し転送禁止命令先ノードであることをフラッディングにより通知し，隣接ノード自身が転送を停止する一連の流れを本論文では “転送禁止命令を出す” と表す．また，利己的ノードはリソース保持が目的であるため，自身の電力を消費してまで RREQ パケットをフラッディングし，転送禁止命令に背くことはない．以上のようにすることで，パストラストが低く結果的にデータ転送経路として用いられないような経路の構築にかかる不要な RREQ パケットを削減する．RREQ パケットの転送停止を通知するため，提案手法では RREQ パケットのフィールドに「破棄フィールド」を追加する．破棄フィールドには転送停止命令を出す隣接ノードの宛先アドレスが入る．また，どのノードを破棄フィールドに加えるかは新たに設けた転送停止命令を出す確率 P_{ij} に従い決定する．ある中継ノード i が隣接ノード j に対して算出する転送停止確率 P_{ij} は以下の式 (3) により算出される．

$$P_{ij} = (1 - L_{ij}(t)) * \alpha, \tag{3}$$

ここで，$L_{ij}(t)$ は時刻 t においてノード i が j に対して持つリンクトラストであり，式 (1) に従い算出される．また α は削減定数であり，α の値を大きくするほどより多くの RREQ パケットを削減することになるため，提案手法の削減効果に影響を与える．しかしながら，RREQ パケットを過剰に削減してしまうと経路構築に失敗しやすくなるため，α の値はこれらのトレードオフを考慮して決定していく必要がある．

次に，転送停止確率 P_{ij} を用いた RREQ パケットの転送停止アルゴリズムを**図 2** に示す．まず，RREQ パケットを受け取った中継ノードは自身の隣接ノードに対し P_{ij} を算出し，転送停止命令を出す隣接ノードの候補を決定する．その際，隣接ノードのうち実際にいくつのノードを破棄フィールドに加えるかは，新たに設けた削減上限数 D に従う．もし，転送停止命令を出す隣接ノードの候補数が削減上限数 D 以下であれば，それらのアドレスをすべて破棄フィールドに追加する．一方，候補数が D を超えていた場合はリンクトラストの低いノードから順に削減上限数 D だけ破棄フィールドに追加する．その後，破棄フィールドを更新した RREQ パケットを隣接ノードへフラッディングする．RREQ パケットを受け取った隣接ノードは破棄フィールドに自身のアドレスがないか確認し，もしあれば

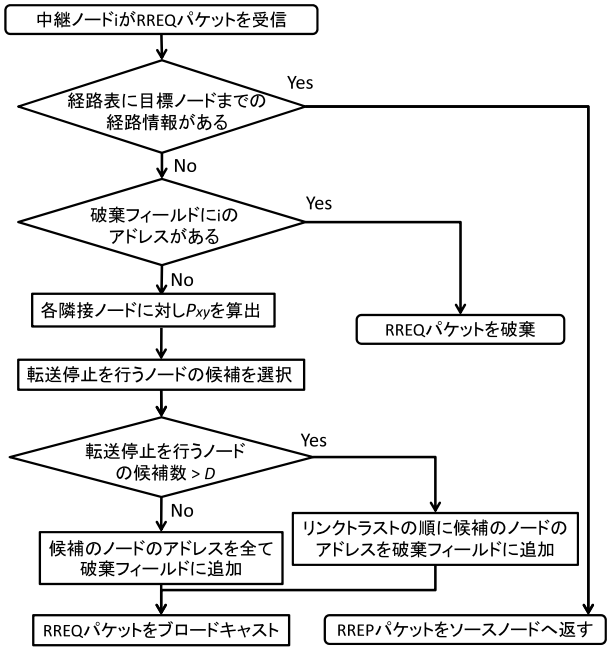

図 2 RREQ パケット転送停止決定アルゴリズム

Fig. 2 The algorithm of selecting nodes to discard RREQ packets.

その RREQ パケットを破棄し転送を停止する．また，パラメータ D は破棄フィールドに記載可能な最大隣接ノード数であるため，D の値が小さい場合，転送禁止命令を出せる隣接ノード数が制限され，RREQ パケットの削減効果が減少してしまう．そのため，D の値はネットワーク全体のノードの平均密度により決定し，RREQ パケットの削減効果に影響がないよう十分な値に設定する．以上のようにして，信頼度の低い経路構築のためにフラッディングされる RREQ パケットのみを削減することで，パケット数は削減しながらも高信頼経路の構築は維持し，高いデータパケット到着率を達成する．また，ルーティング情報の改ざんなどによりネットワークを破壊することが目的である悪意あるノードは転送禁止命令に背くことが考えられるが，暗号化や鍵認証を用いた悪意あるノードに対する手法 [13], [14] と組み合わせていくことで対応可能だと考えられる．

3.3 RUPD パケットの転送頻度調整

既存の SRP では RUPD パケットは，リンクトラストの変化による経路の信頼度の変化を通知し，パストラストを更新するために定期的にフラッディングされる．しかし，リンクトラストはノードの行動やノードのモビリティで変わるトポロジに依存するため，その変化は一定周期ではないと考えられる．そのため，RUPD パケットの転送頻度はリンクトラストの変化量に応じている方が望ましい．すなわち，変化量が大きく経路の変更が必要だと考えられる場合には RUPD パケットの転送頻度を上げ，パストラストがより早く信頼性の高い値に収束するようにする．一方，リンクトラストの変化が小さく，パストラスト更新通知の必要がない場合は RUPD 転送頻度を下げることで不要なパケットのフラッディングを抑制する．

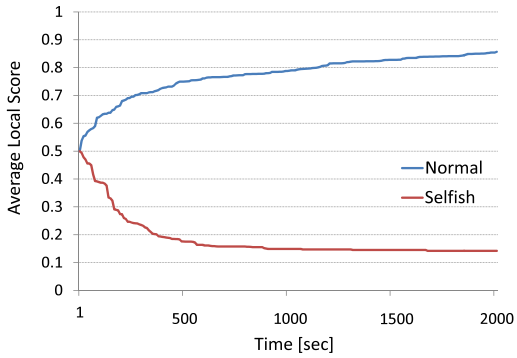

図 3 初期値 0.5 のときのリンクトラストの平均値の推移

Fig. 3 Variation of link trusts when initial local value is 0.5 in AOTDV.

そこで，リンクトラストの変化の様子を探るためシミュレーションにより予備実験を行った．**図 3** は，AODV をベースにした代表的な SRP である AOTDV において，リンクトラストの初期値を 0.5 に設定した際の正常ノード，利己的ノードの各リンクトラストの平均値の推移を表したものである．本シミュレーションは，全 100 ノードのうち 30%がデータパケットをすべて破棄する利己的ノードである環境で行った．図 3 より，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変化量が小さくなっていることが見て取れる．これより，初期値との差が小さいとき，すなわちリンクトラストが収束していないときほど RUPD パケットの転送頻度を上げることで，精度の高いパストラストをより早く算出することができると考えられる．また，初期値との差が大きく，リンクトラストの値が収束していると考えられるときには RUPD パケットの転送頻度を下げ，不要な RUPD パケットのフラッディングを抑制する．これをふまえ，提案手法では RUPD パケットの転送を式 (4) で表される更新スレッショルド $T_{ij}(t)$ に従い操作する．

$$T_{ij}(t) = \beta * |L_{ij}(t) - L_{ini}|, \tag{4}$$

ここで，β は更新定数，L_{ini} はリンクトラストの初期値である．

更新スレッショルド $T_{ij}(t)$ を用いた RUPD パケット転送アルゴリズムを**図 4** に示す．まず，パケットを転送したノードはプロミスキャスモードにより隣接ノードが正常にパケットを中継するかを監視し，リンクトラスト $L_{ij}(t)$ を更新する．更新スレッショルド $T_{ij}(t)$ はリンクトラストを更新するたびに式 (4) により算出される．そして，リンクトラストの変化量 ΔL_{ij} が更新スレッショルド $T_{ij}(t)$ 以上であれば RUPD パケットを隣接ノードにフラッディングする．変化量 ΔL_{ij} は式 (5) で算出される．

$$\Delta L_{ij} = |L_{ij}(t) - L_{ij}(t_{prev})|, \tag{5}$$

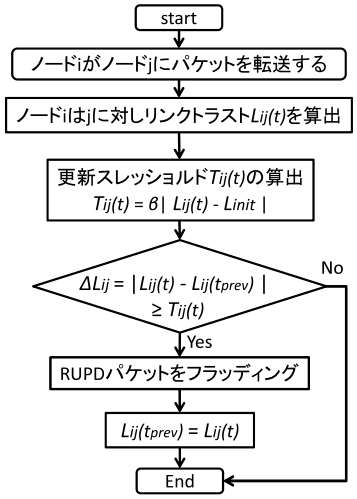

図 4 RUPD パケット転送アルゴリズム
Fig. 4 The algorithm of broadcasting of RUPD packets.

ここで，$L_{ij}(t_{prev})$ は前回の RUPD パケットをフラッディングした際に通知したリンクトラストの値である．リンクトラスト L_{ij} とその初期値 L_{ini} との差の絶対値が大きくなることで更新スレッショルド $T_{ij}(t)$ の値が大きくなるため，ΔL_{ij} は $T_{ij}(t)$ を超えにくくなり，RUPD パケットのフラッディングが抑えられる．

このようにして，リンクトラストが初期値と離れているとき，すなわちリンクトラストの変化量が小さいと考えられる場合には，更新スレッショルドの値を上げ，不要な RUPD パケットのフラッディングを抑制する．一方，リンクトラストが初期値に近い値のとき，すなわちリンクトラストの変化量が大きいと考えられる場合には，更新スレッショルドの値を下げることで RUPD パケットの転送頻度を上げ，より早くパストラストが経路の信頼性を表した値に収束するようにする．以上により，評価値算出の精度を維持しつつ，RUPD パケットを効率的に削減することができる．

4. シミュレーション評価

提案手法 TA-AODV の有用性を示すため，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．750 m × 750 m のエリアに 100 ノードが存在し，各ノードはエリア内において，一定周期ごとに無作為に選択したノードへ経路構築を行い，データ通信を開始するものとする．また，エリア内には正常ノードと利己的ノードが混在し，利己的ノードはデータパケットのみをすべて破棄するものとする．これは，データパケットは制御パケットに比べデータ量が大きく転送コストがかかるのに加え，制御パケットを含めすべてのパケットを破棄した場合ブラックリストに追加され，自身のデータ通信が行えなくなってしまうためである．また，シミュレーションエリア，無線通信範囲，ノード数，利己的ノードの割合の関係から，1 ホップ圏内にいる平均の利己的ノード数は 14 と計算されるため，削減上限数 D の値は余裕を持たせ 20 と設定した．既存手法の各経路に対するタイムアウト時間は AOTDV に倣い 8 秒とする．提案手法が制御パケットを削減しつつも安定した経路の構築を維持できていることを示すため，以下の 3 つの項目により提案手法の性能を評価する．

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：t	2,000 秒
シミュレーションエリア	750 m × 750 m
全ノード数：N	100
無線通信方式	IEEE 802.11b
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
利己的ノードの割合：γ	10%～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
削減定数：α	1.25
削減上限数：D	20
更新定数：β	1.0

- 制御パケット数
  提案手法の制御パケット削減効果について確認する．特に RREQ パケット数，RUPD パケット数について評価を行う．
- ルーティングオーバヘッド ROR
  ルーティングオーバヘッドはデータパケット転送経路の構築のために，どれだけの制御パケットが必要であるかを示す値であり，次式で表される．

$$\mathrm{ROR} = \frac{\text{全制御パケット数}}{\text{全データパケット数}}. \tag{6}$$

- データパケット到着率 PDR
  データパケット到着率はソースノードから目標ノードへデータパケットが届く割合であり，信頼性の高い経路を構築できたかを表す指標である．

比較対象は AODV と，AODV をベースとした SRP である AOTDV である．

4.2 削減定数 α の設定

RREQ パケットの削減数と経路構築の安定性のトレードオフの関係を考慮し，提案手法における削減定数 α の値を決定する．そのため，利己的ノードが 30%存在する環境下

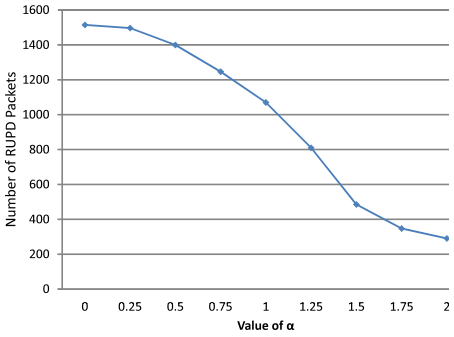

図 5 削減定数 α と RREQ パケット数の関係
Fig. 5 The number of RREQ packets with varying α.

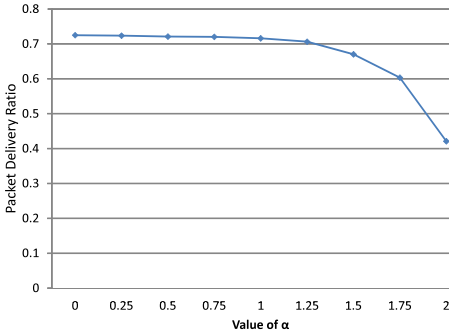

図 6 削減定数 α とデータパケット到着率の関係
Fig. 6 Packet delivery ratio with varying α.

において，パラメータ α の値を変動させたときの RREQ パケット数の変化，およびデータパケット到着率の変化を検証した．それぞれの結果を**図 5**，**図 6** に示す．

図 5 の結果より，α の値を大きくするほど隣接ノードに対し RREQ パケットの転送停止命令を出す確率が上がるため，RREQ パケットの転送数が減少していくことが見て取れる．一方図 6 の結果より，α の値が増加するに従いより多くの RREQ パケットが削減されるため，経路構築に失敗しやすくなり，到着率が大きく低下してしまっていることが見て取れる．α の値が 1.25 より大きくなると到着率が低下していくため，RREQ パケットの削減数と到着率のトレードオフを考慮し，α を 1.25 に設定する．

4.3 制御パケット数

利己的ノードが 30%存在する環境下において，シミュレーション終了時の全ノードが転送した制御パケット数の合計の比較とその内訳を**図 7** に示す．また，利己的ノード数の割合を変化させたときの総 RREQ パケット数，総 RUPD パケット数の変化をそれぞれ**図 8**，**図 9** に示す．ここで，AODV では RUPD パケットは用いられないため，図 9 において AODV の RUPD パケット数は記載していない．

図 7 より，提案手法の制御パケット数が最も少ないことが見て取れ，AOTDV に対し 48%，AODV に対し 33%削減された．また，RREQ パケット数に関しては図 8 より，

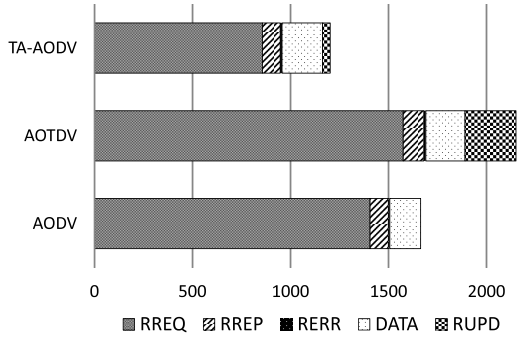

図 7 γ=30%の場合の全転送パケット数とその内訳
Fig. 7 The number of packets and the breakdown.

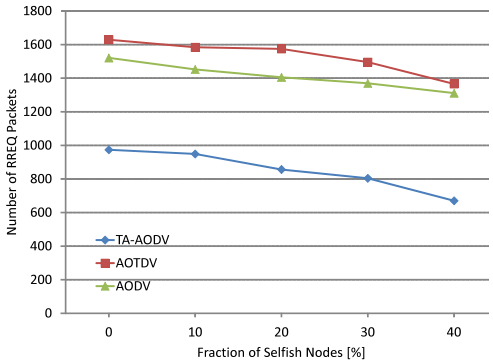

図 8 利己的ノードの割合と RREQ パケット数
Fig. 8 The number of RREQ packets with varying fraction of selfish nodes.

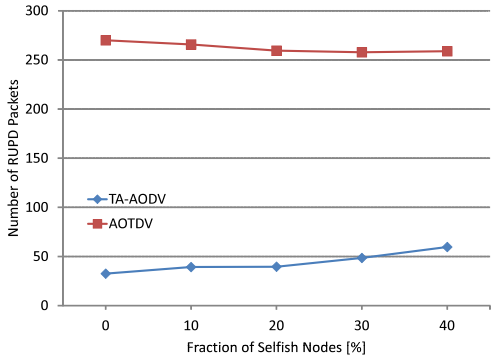

図 9 利己的ノードの割合と RUPD パケット数
Fig. 9 The number of RUPD packets with varying fraction of selfish nodes.

AOTDV に対し 43%削減され，RUPD パケット数に関しては図 9 より，AOTDV に対し 78%削減されたことを確認した．すべての手法で利己的ノードの増加により RREQ パケット数が減少しているのは，パケットの転送を拒むノードをブラックリストに登録し，登録されたノードに対しては RREQ パケットを転送しないようにしているためである．

RREQ パケット数，RUPD パケット数の削減結果について以下で考察する．まず，既存の AODV，AOTDV では各中継ノードは転送されてきた RREQ パケットをすべ

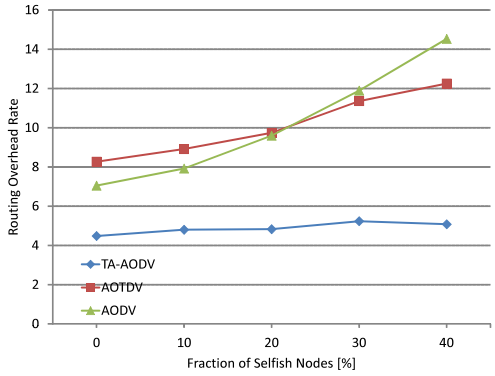

図 10 ルーティングオーバヘッドついて
Fig. 10 Routing overhead.

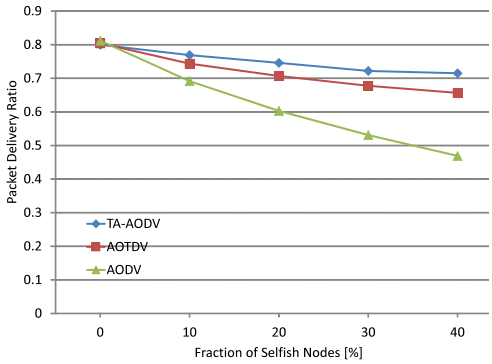

図 11 利己的ノードとパケット到着率
Fig. 11 Packet delivery ratio.

てフラッディングしていた．しかし，SRP では経路を構築したとしても，パストラストが低い経路の場合は破棄される可能性が高いため，最終的にデータ転送に用いられない無駄な経路を構築してしまっている．これに対し，提案手法ではリンクトラストの低い低信頼なノードの RREQ パケット転送を停止させる．これにより，ネットワーク全体での RREQ パケット数を削減しつつ，信頼性の高い経路のみを効率的に構築することができる．また RUPD パケットに関しては，AOTDV では定期的にフラッディングしていたのに対し，提案手法ではリンクトラストの変化に応じて RUPD パケットの転送頻度を変動させる．これにより，リンクトラストの変化が小さい場合には更新頻度が下がり，経路情報の更新通知の必要ない場合にもフラッディングされていた不要な RUPD パケット転送が抑制されたため，結果的にネットワーク全体での RUPD パケットの削減を達成することができたと考えられる．一方，提案手法は各隣接ノードに対し新たに「転送停止命令を出す確率 P_{ij}」，「更新スレッショルド $T_{ij}(t)$」を算出することで制御パケット数を削減しているため，既存手法に対し計算量は増加することが考えられる．しかしながら，これらの変数算出にかかる計算量のオーバヘッドは隣接ノード数に比例し，一般に MANET に参加するノード数はたかだか 1,000 ノード程度のため，加えられた数式処理は各ノードの計算能力を超過するような処理ではなく，提案手法を導入することでルーティングに致命的な遅延が発生するなどの問題はない．

4.4 ルーティングオーバヘッド

ルーティングオーバヘッド ROR は 1 つのデータパケットを転送するのにどれだけの制御パケットが必要か，すなわちデータパケット転送経路構築の効率性を表す．利己的ノードの割合を変化させた場合の ROR を**図 10** に示す．

図 10 より，提案手法では利己的ノードの割合によらず最も低い ROR を維持している．一方，利己的ノードの割合が低いときには，AOTDV は AODV と比べ高い値となっており，利己的ノードに対処するためにルーティングにかかるオーバヘッドが増加してしまっていることが確認できる．AOTDV では新規経路の構築の際に全 RREQ パケットを転送するため，利己的ノードが存在する経路であっても，その経路上に存在する他の正常ノードのリンクトラストが高い場合，結果としてパストラストが高くなる．その結果，データ転送経路として選択されるが，利己的ノードによりデータパケットは破棄されるため RREQ パケットの再送が起こる．一方，提案手法では各中継ノードがリンクトラストから利己的ノードか判断し，パケットの転送を停止させる．これにより，利己的ノードを含んだ経路を選択しにくくなり，RREQ パケットの再送が抑えられたため，ROR が低い値となったと考えられる．

4.5 データパケット到着率

図 11 に利己的ノードの割合とデータパケット到着率の変化を示す．

図 11 より，提案手法は他のルーティングと比較し高い到着率を維持していることが確認でき，利己的ノードの割合が 40%のとき AOTDV と比較し 5%，AODV と比較し 24%改善されている．この結果は，提案手法ではリンクトラストを用いることによって信頼度の低い経路構築に要する RREQ パケットのみを削減しつつ，高信頼経路の構築を維持できたことを示す．さらに，AOTDV では経路のパストラストの更新は一定周期であったが，提案手法ではリンクトラストの変化の大きい初期値付近で頻繁に行うようにしているため，AOTDV と比べより早くリンクトラストが信頼性の高い値に収束し，正常なノードを選択しやすくなるため，到着率が向上したと考えられる．

次に，**図 12** に RREQ パケット数とデータパケット到着率の関係を示す．

図 12 より，提案手法は同じ RREQ パケット数で比較した際，最も高いデータパケット到着率を維持しており，高信頼経路の構築において最も効率的に RREQ パケットを転送していることが分かる．

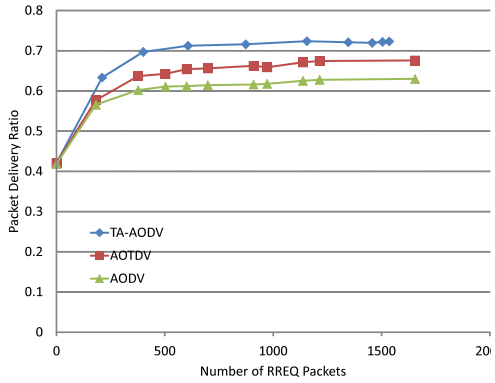

図 12 RREQ パケット数とデータパケット到着率の関係

Fig. 12 Packet delivery ratio with varying number of RREQ Packets.

以上より，提案手法 TA-AODV は評価値を用いて効率的に制御パケットを削減しつつ，高いデータパケット到着率を達成する手法であることが示された．

5. おわりに

本論文では，評価値を用いて不要な RREQ パケット，RUPD パケットのフラッディングを削減することで，高信頼経路構築にかかるオーバヘッドの増加を抑制するセキュアルーティング手法 TA-AODV を提案した．

提案手法ではパケットを正常に転送しない信頼度の低いノードに対して，RREQ パケットの転送停止命令を出すことで，低信頼経路構築に要する RREQ パケットのみを削減する．また，経路情報更新メッセージである RUPD パケットの転送を評価値の変化に応じて行う．このようにすることで，評価値をより早く信頼度の高い値に収束させることができ，評価値の更新の通知が必要ない際には不要な RUPD パケットのフラッディングを削減することができる．提案手法をシミュレーションにより比較評価し，RREQ パケット数，RUPD パケット数を削減しながらも，高いデータパケット到着率を達成していることを確認した．

以上より，提案手法は効率的に高信頼な経路を構築できるという有用性を示した．

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] Santhanam, L., Xie, B. and Agrawal, D.P.: Selfishness in Mesh Networks: Wired Multihop MANETs, *Wireless Communications*, Vol.15, No.4, pp.16–23, IEEE (2008).
[2] Jin-Hee, C., Swami, A. and Ing-Ray, C.: A Survey on Trust Management for Mobile Ad hoc Networks, *Communications Surveys & Tutorials*, Vol.13, No.4, pp.562–583, IEEE (2011).
[3] Bala, A., Kumari, R. and Singh, J.: Investigation of blackhole attack on AODV in MANET, *Journal of Emerging Technologies in Web Intelligence*, Vol.2, No.2, pp.96–100 (2010).
[4] Poonam, G.K. and Misra, M.: Trust Based Multi Path DSR Protocol, *ARES 2010*, pp.204–209 (2010).
[5] Marchang, N. and Datta, R.: Light-weight Trust-based Routing Protocol for Mobile Ad hoc Networks, *Information Security, IET 2012*, Vol.6, No.2, pp.77–83 (2012).
[6] Velloso, P.B., Laufer, R.P., Duarte, O.C.M.B. and Pujolle, G.: Trust Management in Mobile Ad hoc Networks Using a Scalable Maturity Based Model, *IEEE Trans. Network and Service Management*, Vol.7, No.3, pp.172–185 (2010).
[7] Huaizhi, L. and Mukesh, K.: Trust Management in Distributed Systems, *Computer*, Vol.40, No.2, pp.45–53, IEEE (2007).
[8] Pirzada, A.A., Mcdonald, C. and Datta, A.: Performance Comparison of Trust-based Reactive Routing Protocols, *IEEE Trans. Mobile Computing*, Vol.5, No.6, pp.695–710 (2006).
[9] Halim, I.T.A., Fahmy, H.M.A., Bahaa El-Din, A.M. and El-Shafey, M.H.: Agent-Based Trusted On-Demand Routing Protocol for Mobile Ad Hoc Networks, *NSS 2010*, pp.255–262 (2010).
[10] 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).
[11] Johnson, D.B. and Maltz, D.A.: Dynamic Source Routing in Ad hoc Wireless Networks, *Mobile Computing*, pp.153–181 (1996).
[12] Perkins, C.E. and Royer, E.M.: Ad-hoc On-demand Distance Vector Routing, *WMCSA*, pp.90–100, IEEE (1999).
[13] Dahshan, H. and Irvine, J.: Key Management in Web of Trust for Mobile Ad Hoc Networks, *AINA 2009*, pp.363–370 (2009).
[14] Guo, Y., Ma, J. and Wang, L.: Mechanism Design Based Nodes Selection Model for Threshold Key Management in MANETs, *TrustCom*, pp.303–309, IEEE (2012).

牛窪 洋貴 （学生会員）

2012 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．

武田 苑子 （学生会員）

2013 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 （フェロー）

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）．情報処理学会学会誌編集委員，同論文誌編集委員，同マルチメディア通信と分散処理研究会幹事等を歴任．現在，情報処理学会高度交通システム研究会幹事，電子情報通信学会英文論文誌 B 編集委員．Vice Chair of IEEE ComSoc APB TAC．ネットワーク・プロトコル，モバイルコンピューティング，ITS 等の研究に従事．著書『コンピュータネットワーク』（オーム社），『ユビキタスコンピューティング』（オーム社）等．電子情報通信学会，IEEE，ACM 各会員．