

MANETにおける中継頻度を考慮した セキュアルーティングの検討

大畑 百合^{1,a)} 梅田 沙也華^{1,b)} 神本 崇史^{1,c)} 重野 寛^{1,d)}

概要：モバイルアドホックネットワーク（MANET）では、各ノードがパケットを中継する役割を担うが、各ノードのリソースに制限があるため、パケットの中継を怠る利己的ノードの存在が指摘されている。そこで、ノードの過去の行動を評価したトラスト値を用いて、安全な経路を構築する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、トラスト値が高い一部のノードを集中して中継に利用することや、評価を受ける機会が少ないため検知されない利己的ノードが多数発生するという問題がある。本稿では、この問題に対応するために、中継頻度を考慮したセキュアルーティング手法 RF-AOTDV を提案する。RF-AOTDV は、中継ノードとして選択される頻度の低さを示す未使用度を導入し、過去に中継ノードとして選択されず未使用度が高いノードを用いてパケットを転送する。これにより、各ノードを均等に中継ノードとして選択し、一部のノードにパケットの転送負荷が集中することを防ぐ。また、中継ノードとして選択した際にノードを評価することで、評価の機会を各ノードに分散して与え、利己的ノードを多く検知する。本稿では、コンピュータシミュレーションにより RF-AOTDV と既存手法を比較し、RF-AOTDV ではパケットの転送負荷をノード間で分散させ、より多くの利己的ノードを検知できることを示す。

1. はじめに

近年、モバイルアドホックネットワーク（MANET）と呼ばれるネットワークが注目されている。MANET とは、端末が動的に構築するネットワークであり、既存の基地局などのインフラストラクチャに頼らず、端末間で直接通信を行う。また、直接通信ができない距離にある端末同士も、MANET では第三者の端末がパケットを中継する役割を担うことで、直接通信することが可能である。しかし、全ての端末がパケットの中継に協力的であるとは限らない [1]。特に MANET では、ネットワークを構築する端末がモバイル端末であり、各端末の電力や帯域といったリソースに制限があるため、自身のリソースを確保するためにパケット中継を怠る端末が発生すると考えられる [2]。このような端末は利己的ノードと呼ばれる。MANET では端末が動的にネットワークを構築し、ネットワークを監視する第三者の機構が存在しないため、利己的ノードを検知することは困難である。そこで、利己的ノードによる影響を低減するために、トラストを用いたセキュアルーティングが提案さ

れており [3], [4], [5], AOTDV[6] や TA-AODV[7] などが挙げられる。これらのセキュアルーティングプロトコルでは、トラストを用いてノードやパスの信頼性を評価する。ここで、ノードの信頼性を表す値はリンクトラスト、パスの信頼性を表す値はパストラストと呼ばれる。これらのトラストを考慮することで、セキュアルーティングプロトコルでは、利己的ノードを含まない信頼性の高いパスを用いたパケットの転送を可能にする。

しかし、現在のセキュアルーティングでは、転送負荷集中問題、未検知利己的ノード増加問題の2つの問題がある。転送負荷集中問題とはリンクトラストが高い一部のノードにパケット転送負荷が集中する問題である。リンクトラストはパケットの転送率から算出される値であり、パケットを正しく転送した頻度が高いノードほど高い値を示す。既存のセキュアルーティングでは、このリンクトラストが高く信頼性の高いノードを中継ノードとして採用する。したがって、パケット転送に協力した頻度が高いノードほど、再び中継ノードとして選択される可能性が高く、一部のノードにパケットの転送負荷が集中することが考えられる。一方、未検知利己的ノード増加問題とは、検知されない利己的ノードが多数発生する問題である。セキュアルーティングでは、ノードのパケット転送率によってリンクトラストを算出し、リンクトラストの値でノードを評価する。したがっ

¹ 慶應義塾大学大学院理工学研究科
Graduate School of Science and Technology, Keio University

a) ohata@mos.ics.keio.ac.jp

b) umeda@mos.ics.keio.ac.jp

c) kamimoto@mos.ics.keio.ac.jp

d) shigeno@mos.ics.keio.ac.jp

て、中継ノードとして選択していないノードに対して評価を行うことはできない。しかし、中継ノードとして選択された頻度が低くリンクトラストの値が高くないノードは中継ノードとして選択される確率も低い。これにより、評価を受ける機会が少ないために検知されない利己的ノードが多数発生する。

本稿では、転送負荷集中問題と未検知利己的ノード増加問題を緩和するために、中継頻度を考慮したセキュアルーティング手法 RF-AOTDV を提案する。RF-AOTDV では、ノード未使用度とパス未使用度を導入する。これらの値は、ノードやパスがパケットの転送に利用された頻度を示し、この頻度が高いノードやパスは未使用度が低く、一方で頻度が低いノードやパスは未使用度が高い値をとる。このノード未使用度やパス未使用度を用いることで、RF-AOTDV では中継ノードとして選択されている頻度が低いノードを積極的に中継ノードとして採用し、ノード間でパケットの転送負荷を分散させる。したがって、RF-AOTDV は転送負荷集中問題を緩和する。また、中継ノードを選択した際に、その中継ノードの評価を行うことで評価の機会もノード間で分散させ、未検知利己的ノード増加問題を緩和する。本稿では、コンピュータシミュレーションによって RF-AOTDV が転送負荷集中問題と未検知利己的ノード増加問題を緩和していることを確認する。

2. 関連研究

MANET では、パケット破棄を行う利己的ノードを検知し、これらのノードによる影響を低減するために、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。ここで、トラストとは各ノードやパスに対する信頼度を示す値であり、これらは過去の通信の結果により算出される。トラストを考慮することで、セキュアルーティングプロトコルでは、信頼性の高いパスを用いた通信を可能にする。この章では、トラストを用いた代表的なセキュアルーティングプロトコルについて説明し、そして、既存のセキュアルーティングの問題点について述べる。

2.1 セキュアルーティング

MANET におけるルーティングプロトコルは、プロアクティブ型、リアクティブ型、ハイブリッド型の3つに大きく分けることができる [8]。リアクティブ型のプロトコルは、通信要求が発生したときのみ、経路の構築を行うため、各ノードのリソースの消費を抑えることができる。そのため、各ノードのリソースに制限がある MANET の環境において、リアクティブ型プロトコルは適していると考えられる。よって、本稿では MANET のためのリアクティブ型のルーティングプロトコルである AODV [9] を拡張したセキュアルーティングプロトコルに注目する。

AODV に基づく、トラストを用いたセキュアルーティン

グの例として、AOTDV [6] や TA-AODV [7] などが挙げられる。AOTDV では、リンクトラストとパストラストの2種類のトラストを用いて、パケットの転送に協力的なノードで構成された信頼性の高いパスを選択する。リンクトラストとは、各ノードの信頼度を示し、パストラストとは各パスの信頼度を示す値である。リンクトラストを各ノードのパケット転送率によって算出される。時刻 t において、ノード i が算出するノード j のリンクトラスト $L_{ij}(t)$ は式 (1) により算出される。

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

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常に転送した回数、 N_A は時刻 t までにノード i がノード j に対して転送を要求したパケットの総数を示す。また、 W はウィンドウサイズであり、リンクトラスト $L_{ij}(t)$ は最近 W 時間以内のパケットの転送率である。AOTDV では、各ノードがそれぞれブラックリストを保持し、リンクトラストがブラックリスト閾値 η を下回ると利己的ノードであるとみなし、ブラックリストに追加する。つぎに、最終的なパスの選択を行うため、パス全体の評価を行う。そこで、パス上の中継ノードのリンクトラストを用いてパストラストを算出する。時刻 t における、パス P のパストラスト $T_P(t)$ の値は式 (2) によって算出される。

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

ここで、 n_i と n_j はパス P 上に存在する互いに隣接したノードであり、 N_d はパス P 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。式 (2) より、パストラストはパスを構成する中継ノードのリンクトラストを掛け合わせた値であるため、中継ノードのリンクトラストが高いパスはパストラストの値も高くなる。AOTDV は、パストラストが高いパスを用いてパケットを転送するため、信頼性の高いノードで構成されたパスを選択することが可能である。

TA-AODV [7] は、AOTDV と同様のトラストモデルを用いたセキュアルーティングである。AOTDV と異なる点は、経路探索に使用される Route Reply (RREQ) パケット数を削減し、経路情報を更新するための Route Update (RUPD) パケットを送信する頻度をトラストの値に応じて変化させている点である。ここでは、本稿の提案手法に関わる RREQ パケットの削減方法について述べる。AOTDV では、信頼性の高いパスを構築するために、RREQ パケットなどの制御パケットが AODV と比較して増加する問題点がある [7]。そこで、TA-AODV では、トラストを考慮して RREQ パケットを削減する。具体的には、ノードは全ての RREQ パケットを転送せず、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ノードに対しては、RREQパケットの転送停止命令を出す。こ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に使用されないパスの構築に費やされる余剰な RREQ パケットを削減する。ノード i が隣接ノード j に対して RREQ パケットの転送停止命令を出す確率 P_{ij} は以下の式 (3) によって算出される。

$$P_{ij} = (1 - L_{ij}(t)) \times \alpha \quad (3)$$

ここで、 α は RREQ 削減定数である。式 (3) によって計算される P_{ij} の確率で、RREQ パケットの転送停止命令を出すことで、隣接ノードのリンクトラストが低く、最終的にパケットの転送に使用されないパスを構築する余剰な RREQ パケットを削減することが可能である。

2.2 セキュアルーティングの問題点

既存のトラストを用いたセキュアルーティングには、2つの問題点が考えられる。本稿では、それぞれを転送負荷集中問題と未検知利己的ノード増加問題と定義する。

2.2.1 転送負荷集中問題

転送負荷集中問題とは、リンクトラストが高い一部のノードにパケットの転送負荷が集中することである。セキュアルーティングでは、より信頼性の高いパスを用いて通信を行うために、リンクトラストが高いノードで構成されたパスを選択する。したがって、リンクトラストが高いノードほど、中継ノードとして選択される可能性も高い。リンクトラストとは、パケットの転送率によって算出されるため、中継ノードとして頻りに選択される協力的なノードほどリンクトラストの値は向上し、そして、リンクトラストが向上すると、再び中継ノードとして選択される可能性が増加する。よって、リンクトラストが高い一部のノードにパケットの転送負荷が集中する。

この問題は、ネットワークにさまざまな悪影響を与える。まず、リンクトラストが高くパケット転送に協力的なノードほど、電力といったリソースの消耗が激しい環境になるため、パケット転送に協力的なノードがネットワークから離脱する可能性がある。多くの協力的なノードがネットワークから離脱すれば、ネットワークは機能しなくなる。一方で、中継ノードに選択された頻度が低いノードは、パケット転送に協力的であっても、十分にリンクトラストが高い値ではないため、中継ノードとして選択される可能性は低い。したがって、MANET では各ノードにリソースの制限があるにも関わらず、リソースが有効に活用されていない。また、一部のノードにパケットの転送要求が集中することで、パケット衝突や転送遅延の増加といった影響が生まれることも考えられる。

2.2.2 未検知利己的ノード増加問題

未検知利己的ノード増加問題とは、他のノードに検知されない利己的ノードが多数発生することである。この問題

は、先述の転送負荷集中問題に付随して発生する問題である。セキュアルーティングでは、リンクトラストが向上するにつれて、ノードは中継ノードとしてより頻りに選択される。一方で、リンクトラストが低いほど、中継ノードとして選択される可能性も低下する。しかし、セキュアルーティングでは、パケットの転送率を用いてノードを評価するため、そもそも中継ノードとして選択していないノードに対して評価を行うことは不可能である。つまり、ネットワークに参加して間もないノードなど、まだ中継ノードとして選択されずリンクトラストが高くないノードは、中継ノードとして選択されず、評価を受ける機会も少ない。したがって、利己的ノードがネットワークに参加した場合も、そのノードに対して評価を与えることができず、検知できない。

この問題によって、既存のセキュアルーティングでは、利己的ノードを多く検知することは困難である。したがって、多くの利己的ノードが除外された安全な環境に、ネットワーク全体を変化させることはできない。また、通常ノードは利己的ノードを検知していないために、利己的ノードのパケットの転送要求に応えることが考えられる。各ノードのリソースに制限がある MANET において、利己的ノードのために他のノードのリソースを消費することは避けるべきである。

3. RF-AOTDV

本節では、転送負荷集中問題と未検知利己的ノード増加問題を解決するために、RF-AOTDV (Relay Frequency based Ad hoc On demand Trusted-path Distance Vector) ルーティングプロトコルを提案する。RF-AOTDV では、各ノードのパケットの中継頻度を考慮し、中継頻度が低いノードを中継ノードとして積極的に採用する。このようにすることで、RF-AOTDV では各ノードにパケットの転送負荷を分散させ、そして利己的ノードを効率的に検知する。

RF-AOTDV では、ノード未使用度とパス未使用度を導入する。これらの値は、ノードやパスがパケットの転送に利用された頻度を示し、この頻度が高いノードやパスは未使用度が低く、一方で頻度が低いノードやパスは未使用度が高い値をとる。RF-AOTDV では、パス未使用度が高い、つまり、使用された頻度が低いパスを選択し、パケットを転送する。パス未使用度を算出するために、RF-AOTDV では各ノードが以下の段階を踏む。

- ノード未使用度の算出
- パス未使用度の算出

以下、本節では各段階について説明する。そして、最後にノード未使用度とパス未使用度のルーティングプロトコルへの適用方法について述べる。

3.1 ノード未使用度の算出

RF-AOTDV では、リンクトラストを用いてノード未使用

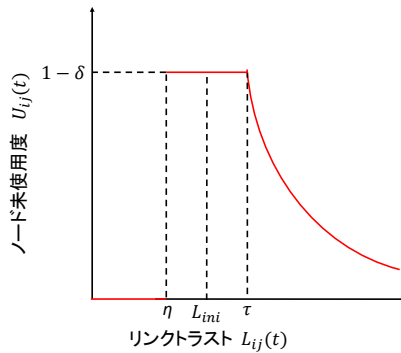


図1 ノード未使用度とリンクトラストの関係

度の算出を行う。リンクトラストの値は、各ノードの packets の中継頻度が高くなるにつれて、一定の値に収束し [7], packets の転送に協力的なノードは中継頻度が高くなるにつれてリンクトラストは高い値に定まる。一方で、packets の破棄を行う利己的ノードは中継頻度が高くなるにつれてリンクトラストは低い値に定まる。したがって、リンクトラストが初期値に近いノードほど中継ノードとして選択された頻度が低く、リンクトラストが初期値から離れるほど、そのノードは中継ノードとして頻繁に選択されていることが分かる。このリンクトラストの特徴から、リンクトラストが初期値に近いノードに対して高いノード未使用度を与え、一方、リンクトラストが初期値から離れるほど低いノード未使用度を与える。

図1はノード未使用度 $U_{ij}(t)$ とリンクトラスト $L_{ij}(t)$ の関係を表す。 $U_{ij}(t)$ は時刻 t においてノード i がノード j に対して算出するノード未使用度を示し、 $L_{ij}(t)$ は時刻 t においてノード i がノード j に対して算出するリンクトラストである。ここで、リンクトラストの値は式 (1) から算出されたものである。また、 L_{ini} とはリンクトラストの初期値、 η はブラックリスト閾値、 τ は未使用度閾値である。リンクトラストがブラックリスト閾値 η を下回ると、そのノードは利己的ノードであるとみなされ、ブラックリスト [6] に格納される。また、未使用度閾値 τ よりリンクトラストが小さいノードは、リンクトラストの初期値と比較してリンクトラストの変化量が小さいため、中継ノードとして選択された頻度が低いノードであるとみなす。

まず、RF-AOTDV では、ノード未使用度を算出するために、リンクトラストによってノードを3種類に分類する。

- 利己的ノード : $L_{ij}(t) < \eta$
- 未使用ノード : $\eta \leq L_{ij}(t) \leq \tau$
- 貢献ノード : $\tau < L_{ij}(t)$

以下、それぞれに分類されたノードの特徴と、ノード未使用度の算出方法について述べる。

利己的ノード

パケット破棄によりリンクトラストの値が低下し、利

己的ノードとみなされたノード。これらのノードはブラックリストに格納され、ブラックリストに格納されているノードからは、いかなるパケットも受け取らず、ブロードキャスト以外によるパケットの送信も行わない。また、これらのノードは既に利己的ノードであると識別されているため、パケット転送率による評価を受けており、過去十分に中継ノードとして選択されたと考えられる。よって、ノード未使用度 $U_{ij}(T)$ は

$$U_{ij}(t) = 0 \quad (4)$$

とする。

未使用ノード

評価を受ける機会が少なく、評価が定まっていないノード。リンクトラストの値が初期値に近い値であるため、過去中継ノードとして選択された頻度が低いノードであると考えられる。よって、ノード未使用度 $U_{ij}(t)$ は

$$U_{ij}(t) = 1 - \delta \quad (5)$$

とする。ここで δ とは調整係数であり、1より極めて小さい値である ($\delta \ll 1$)。RF-AOTDV では、ノード未使用度の最大値を $1 - \delta$ とする。これは、次に計算するパス未使用度で、長いパスと短いパスを区別するためである。パス未使用度とは、パス上の中継ノードのノード未使用度を掛け合わせて算出される。したがって、ノード未使用度の最大値を $1 - \delta$ とすることで、長いパスほどパス未使用度の値が小さくなる。

貢献ノード

パケット転送に協力的であり、中継ノードとして選択された頻度が高い正常ノード。リンクトラストの値が未使用度閾値をこえると、貢献ノードとみなされる。これらのノードは、パケットの転送に協力的であるため、パケットの中継頻度が高くなるにつれて、リンクトラストも向上する。したがって、ノード未使用度 $U_{ij}(t)$ を以下の式で定義する。

$$U_{ij}(t) = \frac{1 - \delta}{r(L_{ij}(t) - \tau) + 1} \quad (6)$$

ここで r は未使用度減少係数であり、 r の値が大きいくほど、リンクトラストの増加による未使用度の減少幅が大きくなる。

上記の方法で計算されたノード未使用度は、過去に中継ノードとして選択された頻度が低いノードほど、値が高くなる性質をもつ。

3.2 パス未使用度の算出

最終的なパスの選択を行うために、パス全体の評価を行う必要がある。そこで、RF-AOTDV ではパス未使用度を導入する。既存のセキュアルーティングにおけるパストラストの算出式 (2) にならい、パス未使用度を式 (7) によって

算出する.

$$U_P(t) = \Pi(U_{ij}(t)|n_i, n_j \in path \quad and \quad n_i \rightarrow n_j \\ and \quad n_j \neq N_d) \quad (7)$$

ここで, n_i と n_j はパス P 上に存在する隣接したノードであり, N_d はパス P 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. 式 (7) が示すように, パス未使用度とは, パス上の中継ノードのノード未使用度を掛け合わせたものである. したがって, ノード未使用度は 1 より小さい値であることを考慮すると, 長さが短く, そして, 構成する中継ノードのノード未使用度が高いパスほどパス未使用度は高い値をとる. そのため, パス未使用度が高いパスを用いてパケットを転送することで, 過去に中継ノードとして選択された頻度が少ないノードで構成された, 短いパスを選択することができる.

3.3 ルーティングプロトコルへの適用

RF-AOTDV は, MANET における代表的なルーティングプロトコルである AODV[9] に, 先述のノード未使用度とパス未使用度を適用したものである. ノード未使用度とパス未使用度を適用することで, RF-AOTDV はパケットの転送負荷をノード間で分散させ, 多くの利己的ノードを検知する.

3.3.1 ルーティング戦略

過去に中継ノードとして選択された頻度が低いノードで構成されたパスを用いてパケットの転送を行うために, RF-AOTDV ではパス未使用度を用いてパスを比較する. そのため, 各ノードがもつルーティングテーブルに, パス未使用度の項目を追加する. また, 既存のセキュアルーティングプロトコルでは, 各ノードがルーティングテーブルの他に, トラスト記録表を保持する. トラスト記録表には, 他のノードに対するリンクトラストの値が記録されているが, RF-AOTDV ではリンクトラストではなく, 各ノードに対するノード未使用度を記録する.

RF-AOTDV では, 経路探索を行う際に, ノード未使用度とパス未使用度を用いる. 新しい経路が構築されると, 構築された経路をパス未使用度と共にルーティングテーブルに追加する. そして, 実際にそのパスを用いてパケットの転送を行うと, 各ノードは自身の隣接ノードが正しくパケットを転送しているかを確認し, 自身のトラスト記録表を更新する. 次節では, 経路探索について詳細に述べる.

3.3.2 経路探索

ノードが経路探索を行うとき, Route Reply (RREQ) パケットと Route Reply (RREP) パケットが用いられる. まず, 経路探索を行うノードは Route Request (RREQ) パケットをブロードキャストする. そして, 目的ノードまでの経路を保持しているノードや, 目的ノード自身が RREQ パケットを受信すると, そのノードは RREP パケットを

送信元ノードに対して送信する. 以下では, あるノードが RREQ パケットや RREP パケットを受信したときの動作をそれぞれ説明する.

RREQ パケット

RF-AOTDV では, 既存の RREQ パケットのフォーマットに, パス未使用度の項を追加する. ノード s が経路探索のために RREQ パケットをブロードキャストするとき, RREQ パケット内のパス未使用度の値は 1 に設定される. ノード i がノード j から RREQ パケットを受信すると, ノード i は以下の手順を踏んで動作する.

Step 1: ノード j がブラックリストに格納されているか確認し, 格納されていれば RREQ パケットを破棄し終了する.

Step 2: ノード j までの経路をパス未使用度 1 としてルーティングテーブルに追加する.

Step 3: ノード i のトラスト記録表に格納されているノード j に対するノード未使用度と, RREQ パケット内に格納されているパス未使用度を掛け合わせることで (式 (7)), RREQ パケットの送信元ノードであるノード s までの経路のパス未使用度を算出し, RREQ パケットに格納されているパス未使用度の値を更新する.

Step 4: 既に同じ RREQ パケットを受信しているか確認する. 既に同じ RREQ パケットを受け取っている場合, 新しい RREQ パケットとパス未使用度を比較し, 新しい RREQ パケットの方がパス未使用度が低いとき RREQ パケットを破棄し終了する.

Step 5: ノード s までの経路をルーティングテーブルに追加または更新する. このとき格納されるパス未使用度の値は Step 3 で算出された値である.

Step 6: ノード i が RREQ パケットの目的ノード d であるか確認する. 目的ノードである場合, RREP パケットを送信し終了する.

Step 7: RREQ パケットの目的ノード d までの使用可能な経路がルーティングテーブルに存在するか確認し, 経路がある場合 RREP パケットを送信し終了する.

Step 8: パス未使用度が低い RREQ パケットを確率的に破棄する.

Step 9: RREQ パケットをブロードキャストする.

ここで, Step 8 について説明する. RF-AOTDV では, AODV と比較して, 多くの RREQ パケットがブロードキャストされることが予想される. これは, AODV では既に受信したものと同一 RREQ パケットを受信した場合, 新たに受信した RREQ パケットは破棄するのに対して, RF-AOTDV では同一 RREQ パケットを受信した場合であっても, 新たな RREQ パケットが高いパス未使用度を保持している場合ブロードキャストする (Step 4) ためである. そこで, RF-AOTDV では, RREQ パケットの数を削減するために, パス未使用度が低く, 最終的には活用されない

可能性が高い RREQ パケットを確率的に破棄する。破棄を行う方法は、既存のセキュアルーティングプロトコルである TA-AODV[7] に倣って行う (式 (3))。RREQ パケットを受信したノード i は、RREQ パケット内のパス未使用度を用いて、式 (8) によって破棄確率を算出する。

$$P = (1 - U_P) \times \alpha \quad (8)$$

ここで、 U_P は RREQ パケットに格納されているパス未使用度、 α は RREQ 削減定数を示す。ノード i は、RREQ パケットをこの確率 P で破棄する。よって、パス未使用度が低い RREQ パケットほど破棄される可能性は高くなる。このように RREQ パケットを確率的に破棄することで、最終的に使用されないパスを構築する可能性が高い RREQ パケットを削減する。

RREP パケット

RREQ パケットと同様に、RF-AOTDV は RREP パケットのフォーマットにパス未使用度の項目を追加する。目的ノードや、目的ノードへのパスを保持するノードが RREQ パケットを受信すると、そのノードは RREP パケットを RREQ パケットの送信元に対して送信する。このとき、RREP パケットの格納されるパス未使用度の値は 1 である。RREP パケットは、RREQ パケットが通過した経路に沿って、送信元ノードに向かって転送される。あるノードが RREP パケットを受信した際の動作は、RREQ パケットを受信した際の動作とほとんど同じである。異なる点は、受信したノードが RREP パケットをブロードキャストではなく、RREQ パケットの送信元ノードに向かってユニキャストする点である。また、RREQ パケットのときのような、確率的な破棄を行わない。

このように RREQ パケットと RREP パケットを用いて経路探索を行うことで、経路上の全てのノードが送信元ノードと目的ノードのそれぞれに対して経路を構築することができる。また、ノード未使用度とパス未使用度を活用することで、構築される経路は、過去に中継ノードとして選択された頻度が低いノードで構成される経路である。

4. シミュレーション評価

提案手法 RF-AOTDV の有用性を示すため、シミュレーションにより評価を行い、既存のセキュアルーティングプロトコルである TA-AODV と比較した。

4.1 シミュレーションモデル

ネットワークシミュレータ Qualnet[10] を用いて、シミュレーションを行った。表 1 は RF-AOTDV と TA-AODV 共通のシミュレーションパラメータを示し、表 2 は、RF-AOTDV に固有のシミュレーションパラメータを示す。TA-AODV に固有のシミュレーションパラメータは、文献 [7] に示されている値に基づく。全ノードは 750m ×

表 1 共通シミュレーション条件

シミュレータ	Qualnet 5.0.2
シミュレーション時間	6000 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
利己的ノードの割合	0~30 %
リンクトラストの初期値: L_{ini}	0.5
ブラックリスト閾値: η	0.4

表 2 RF-AOTDV に関するシミュレーション条件

未使用度閾値: τ	0.4
調整係数: δ	0.1
未使用度減少係数: r	4
RREQ 削減定数: α	0.6

750m の範囲でランダムに配置され、最大速度 2m/s で移動しながら、ランダムに選択されたノードへ経路を構築しデータパケットを送信する。ノードの行動モデルは正常ノードと利己的ノードの 2 種類を定義する。正常ノードは常に全てのパケットを正しく転送する。一方、利己的ノードは受信した全てのデータパケットを破棄する。

RF-AOTDV が、転送負荷集中問題と未検知利己的ノード増加問題に対して有効であることを示すために、以下の 3 つの項目によって性能を評価する。

- パケット中継回数の平均と標準偏差
正常ノードのパケット中継回数の平均と標準偏差について評価する。標準偏差が小さいとき、パケットの中継回数がノード間で分散されていることが分かる。
- 利己的ノードの検知率
各正常ノードが、全ての利己的ノードのうち検知することができた利己的ノードの割合を示す。
- パケット到達率
正常ノードが送信元ノードであるパケットのうち、正しく目的ノードに到達したパケットの割合を示す。

本稿では、利己的ノードの割合を 0% から 30% の間で変化させ、シミュレーションを行った。

4.2 パケット中継回数の平均と標準偏差

図 2 に利己的ノードの割合を変化させた場合の、正常ノードの平均パケット中継回数と標準偏差を示す。棒グラフが平均パケット中継回数、エラーバーが標準偏差を表す。図 2 より、利己的ノードの増加にともない、RF-AOTDV と TA-AODV はともに正常ノードの平均中継回数と標準偏差が増加していることが分かる。しかし、RF-AOTDV は

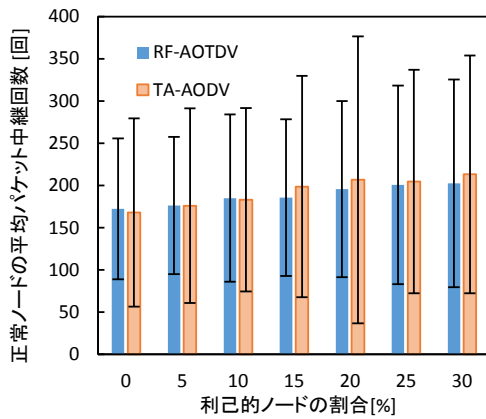


図 2 パケット中継回数の平均と標準偏差

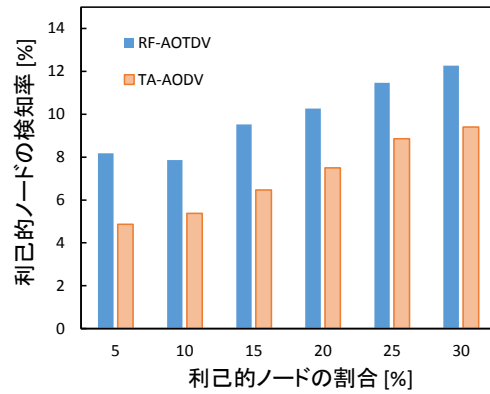


図 3 利己的ノードの検知率

TA-AODV と比較すると常に標準偏差の値が小さく、利己的ノードの割合が 20% のとき、RF-AOTDV は TA-AODV より標準偏差が 38% 小さい値を示している。まず、利己的ノードの増加にともなう標準偏差の増加は、利己的ノードの増加により利己的ノードが密集する地点が発生するためである。周囲を利己的ノードに囲まれた正常ノードは、利己的ノードを避けるために、他のノードによって頻繁に中継ノードとして選択される。したがって、利己的ノードが増加すると、正常ノードのパケット中継回数の標準偏差は増加する。つぎに、RF-AOTDV が TA-AODV と比較して標準偏差が小さい値であるのは、RF-AOTDV では、中継ノードとして過去に選択された頻度が低いノードを選択しているためである。これまでに中継ノードとして頻繁に選択されていないノードを用いてパケットを転送することで、パケットの中継回数をノード間で分散させている。この結果から、RF-AOTDV は転送負荷集中問題に対して有効であることが分かる。

4.3 利己的ノードの検知率

図 3 に、利己的ノードの割合の変化にともなう、正常ノードの利己的ノード平均検知率を示す。図 3 より、RF-AOTDV は常に TA-AODV と比較して、高い検知率を示しており、利己的ノードの割合が 5% のとき、RF-AOTDV の検知率は TA-AODV より 67% 高い値である。これは、TA-AODV では中継ノードとしてリンクトラストが高い特定のノードを選択し続けるのに対し、RF-AOTDV ではより多くの異なるノードを中継ノードとして選択するため、RF-AOTDV は様々なノードに対して評価の機会を与えることができるからである。この結果より、RF-AOTDV は TA-AODV と比較して、より多くの利己的ノードを検知することが可能であり、未検知利己的ノード増加問題を緩和していることが分かる。

4.4 パケット到達率

図 4 に、利己的ノードの割合の変化にともなう、正常

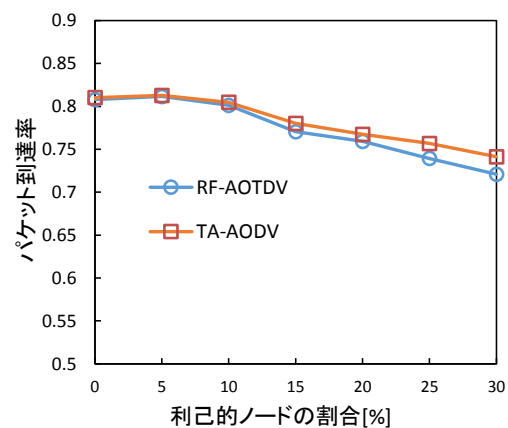


図 4 パケット到達率

ノードのパケット到達率を示す。図 4 より、RF-AOTDV は TA-AODV と比較して、利己的ノードの割合が 10% 以下のとき、同等のパケット到達率を示しているが、利己的ノードの割合が 10% を上回ると、RF-AOTDV のパケット到達率は TA-AODV と比較して、わずかに低いことが分かる。これは、TA-AODV では、リンクトラストが高いノードを中継ノードとして利用し続けることで利己的ノードを避けているのに対し、RF-AOTDV では、過去に利用していないノードを中継ノードとして選択するため、利己的ノードの増加にともない、未検知である利己的ノードによってパケットが破棄される可能性が高まるからである。利己的ノードが増加すると、RF-AOTDV では利己的ノードを検知し終えることができず、TA-AODV と比較してパケット到達率が低下する。しかし、現実的な環境において、利己的ノードが多い環境は想定することは難しい。また、利己的ノードが 10% 以下の環境では、RF-AOTDV は TA-AODV と同等のパケット到達率を示していることから、RF-AOTDV は利己的ノードを早い段階で検知し、正常ノードの間でパケットの中継による負荷を分散させていることが分かる。

5. おわりに

本稿では、転送負荷集中問題と未検知利己的ノード増加

問題を解決するために、中継頻度を考慮したセキュアルーティング手法 RF-AOTDV を提案した。RF-AOTDV では、ノード未使用度とパス未使用度を導入する。これらの値は、ノードやパスがパケットの転送に利用されている頻度を示す値であり、パケットの転送に利用されている頻度が高いほど、ノード未使用度とパス未使用度は低い値を示す。RF-AOTDV ではノード未使用度やパス未使用度が高い、つまり、過去にパケットの転送に利用された頻度が低いノードやパスを用いることでパケットの転送負荷を分散させ、転送負荷集中問題を緩和する。また、中継ノードを選択した際に、その中継ノードに対して評価を行うことで、評価の機会もノード間で分散させ、未検知利己的ノードを緩和する。

RF-AOTDV の有効性を確認するために、本稿ではコンピュータシミュレーションによって RF-AOTDV と TA-AODV を評価した。シミュレーション結果より、RF-AOTDV は TA-AODV と比較して、パケットの中継回数の標準偏差は最大 38% 小さく、一方、利己的ノードの検知率は最大 67% 向上していることが分かる。また、利己的ノードの割合が 10% 以下の環境において、RF-AOTDV は TA-AODV と同等に高いパケット到達率を示している。以上の結果から、RF-AOTDV は、高いパケット到達率を保ちつつ、転送負荷集中問題と未検知利己的ノード問題を緩和していることを確認した。

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] Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N. and Jamalipour, A.: A survey of routing attacks in mobile ad hoc networks, *Wireless Communications, IEEE*, Vol. 14, No. 5, pp. 85–91 (2007).
- [2] Djahel, S., Nait-abdesselam, F. and Zhang, Z.: Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges, *Communications Surveys Tutorials, IEEE*, Vol. 13, No. 4, pp. 658–672 (2011).
- [3] Wang, D., x Mingzeng Hu, M. and Zhi, H.: A Survey of Secure Routing in Ad Hoc Networks, *Web-Age Information Management, 2008. WAIM '08. The Ninth International Conference on*, pp. 482–486 (2008).
- [4] Marchang, N. and Datta, R.: Light-weight trust-based routing protocol for mobile ad hoc networks, *Information Security, IET*, Vol. 6, No. 2, pp. 77–83 (2012).
- [5] 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, *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 42–49 (2013).
- [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 DPS 特集号, Vol. 55, No. 2 (2014).
- [8] Saeed, N., Abbod, M. and Al-Raweshidy, H.: MANET routing protocols taxonomy, *2012 International Conference on Future Communication Networks (ICFCN)*, pp. 123–128 (2012).
- [9] Perkins, C. and Royer, E.: Ad-hoc on-demand distance vector routing, *Second IEEE Workshop on Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99.*, pp. 90–100 (1999).
- [10] Qualnet: Qualnet user manual, <http://web.scalable-networks.com/content/qualnet> (2015).