モバイルアドホックネットワークにおける 選択的破棄攻撃に適応したトラストモデルの検討

五箇 奏乃子[1]　大畑 百合[1]　重野 寛[1]

概要：ノード間で協調して通信を行うシステムである Mobile Ad hoc Network（MANET）では，各端末のリソースに制限があるため，パケットを破棄することで，自身のリソースを確保する非協力ノードが存在する．この非協力ノード対策として，リンクトラストと呼ばれる評価値を用いて非協力ノードを検知するトラストモデルが提案されている．MANET において指摘されている攻撃の一つに，リンクトラストをある一定以上に保ちながらパケットを破棄する選択的破棄攻撃がある．本稿では，選択的破棄攻撃を行うノードを検知するトラストモデル TMSPD（Trust Model against Selective Packet Dropping attack）を提案する．TMSPD では選択的破棄攻撃の特徴を考慮した選択的破棄攻撃を行うノードの検知を行う．シミュレーションを用いて提案手法を評価し，選択的破棄攻撃を行うノードの検知率が向上するという結果から TMSPD の有用性を示す．

A study of Trust Model against Selective Packet Dropping Attack for Mobile Ad Hoc Networks

SONOKO GOKA[1]　YURI OHATA[1]　HIROSHI SHIGENO[1]

1. はじめに

近年，モバイルアドホックネットワーク（MANET）[1]が，様々な場面において柔軟性を持つネットワークとして注目されている．MANET とは，携帯電話やノート PC，タブレット PC といったモバイル端末同士が直接通信することによって，動的に構築するネットワークである．特定の基地局を介さないノード間での通信が可能であり，大規模災害時といった基地局が使用できない場合において，高い対災害性を持つネットワークとしても運用が期待されている．MANET では，ノードが自由にネットワークに参加し，各ノードがパケット転送の役割を担うが，パケットを破棄することで，自身のリソースを確保し他ノードの通信を妨害するノードが存在することが考えられる [2] [3]．このようなノードのことを，非協力ノードと呼ぶ．

そこで，この非協力ノードに対する対策として提案されているセキュアルーティング [4] [5] では，トラストモデルを導入することで，非協力ノードを避けたルーティングを行う．トラストモデルでは，一般的にリンクトラストを用いて各ノードが自身の隣接ノードを評価する．リンクトラストとはノードのパケット転送率で算出され，パケットの転送に協力的なノードほど値は高くなる．既存のトラストモデルでは，ある一定の閾値より高いリンクトラストをもつノードを協力ノードと判断する．

MANET においては，選択的にパケットを破棄することで，ある一定以上にリンクトラストを保つノードが存在することが考えられる．このようなノードは，既存のトラストモデルでは非協力ノードとして検知されない．本稿では，この攻撃を選択的破棄攻撃と呼ぶ．

本稿では，選択的破棄攻撃に対応したトラストモデル TMSPD（Trust Model against Selective Packet Dropping attack）を提案する．TMSPD では，選択的破棄攻撃を行うノードであるという予想値を表す不信度を導入する．選択的破棄攻撃の特徴をとらえて，選択的破棄攻撃を行う可能性の高いノードに対して，不信度に高い値を与える．これにより，選択的破棄攻撃を行うノードの検知を実現する．

以下本稿では，2 章において関連研究について述べ，3 章

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

で TMSPD 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．

2.1 セキュアルーティングプロトコル

MANET では，全体を管理する中央機構が存在しないため，非協力ノードを検知することは困難である．そこで，この非協力ノードに対して様々な対策が研究されている [6] [7] [8]．セキュアルーティングとは，非協力ノードが存在する現実的な環境のなかで，信頼できる経路を選択することによって安全な通信を目標とするルーティングプロトコルであり，対象とするルーティングや攻撃によって様々な種類が存在する [9] [10]．以下では，セキュアルーティングプロトコルにおけるトラストモデルの具体的な仕組みについて説明する．

トラストモデル

トラストにはリンクトラストとパストラストの 2 種類が存在する．リンクトラストはパケット転送率を基に各ノードが隣接ノードに対して算出する値である [11]．ノードはデータパケットを送信した直後に，オーバヒアを行うことによって自身が送信したパケットを隣接ノードが正常に転送したかを確認し，リンクトラストの算出と更新を行う．リンクトラストはパケット転送率を表し，転送要求があった全パケット数に対する正常に転送されたパケット数の割合で定義される [12]．ここで，正常に転送されるとはデータが改ざんされずに転送されるということを意味する．リンクトラストは 0 から 1 の間の値であり，転送に協力的なノードほど値は高く，一方，転送に協力的ではない非協力ノードは値が低くなる．

パストラストは中継ノードのリンクトラストの累積によって求めることができる．経路全体を評価した値であり，このパストラストが高い経路を選択することによって，各ノードは信頼できる経路を用いた通信を行うことができる．

ブラックリスト

リンクトラストが更新された際に，その隣接ノードが非協力ノードであるかを判断するために使用される閾値がブラックリスト定数 τ_α である．各ノードにおいて，リンクトラストがブラックリスト定数 τ_α 以下である隣接ノードは非協力ノードであると考えられ，一定時間ブラックリストに追加される．各ノードは，自身の保持するブラックリスト内のノードから受信したパケットは次のノードへの転送を行わず，ブロードキャスト以外ではそのノードに対してパケットを送信しない．つまり，全隣接ノードのブラックリストに加えられたノードは完全にネットワークから除外される．

ブラックリストに一定時間入れられたノードは，リンクトラストにブラックリスト定数と同じ値を与えられ，ブラックリストから除外される．ここで，このノードが転送に協力的であればリンクトラストは向上し，ネットワークに再び参加することが可能となる．一方，パケットを破棄すると，非協力ノードであると判断され再びブラックリストに格納される．ブラックリストを使用することによって，非協力ノードをネットワークから除外することが可能となる．

2.2 既存手法の問題点

既存のセキュアルーティングにおけるトラストモデルでは，特に選択的にパケットを破棄することで，ある一定以上にリンクトラストを保つ選択的破棄攻撃を行うノードついては考慮されていない．したがって，隣接ノードが協力ノードであるかを正しく判断できないという問題点があげられる [13]．既存のトラストモデルにおいては，リンクトラストがブラックリスト定数 τ_α より高ければ協力ノードと判断される [4]．

選択的破棄攻撃を行うノードを協力ノードと判断することにより，攻撃ノードによるパケット破棄が発生する．また，非協力ノードではない正常ノードが，選択的破棄攻撃を行うノードから受信したパケットを他のノードに転送したり，選択的破棄攻撃を行うノードに対してパケットを送信することも考えられる．これにより，各ノードの電力や送受信帯域といったリソースに限りがある MANET において，非協力ノードではない正常ノードのリソースをより多く使用することとなる．以上より，選択的破棄攻撃を行うノードを協力ノードと判断することにより，ネットワーク全体の性能が低下するという問題が発生する．したがって，選択的破棄攻撃を行うノードを攻撃ノードとして検知できないという点は，解決すべき課題である．

3. TMSPD の提案

本章では，選択的破棄攻撃に対応したトラストモデル TMSPD（Trust Model against Selective Packet Dropping attack）を提案する．

3.1 TMSPD の概要

提案する TMSPD では，選択的破棄攻撃を行うノードであるという予想値を表す不信度を導入する．選択的破棄攻撃の特徴をとらえて，選択的破棄攻撃を行う可能性の高いノードに対して，不信度に高い値を与える．

選択的破棄攻撃を行うノードは，パケット転送数と破棄数の偏りが小さく，また通信数が多くなってもリンクトラストが高い値に収束しないという特徴をもつ．そこで，パケット転送数と破棄数の偏りが小さいノードに対して，不信度に高い値を与える．また，通信数が多いにも関わらず

リンクトラストが高い値に収束しないノードを検知するために，通信数が多いノードに対して不信度に高い値を与える．

そして，不信度 S_{ij} を，トラスト閾値 $T_{threshold}$ に反映する．不信度の高いノードに対してリンクトラストの閾値を高くすることにより，選択的破棄攻撃を行うノードを検知する．そして，ネットワークから除外することで，選択的破棄攻撃を行うノードによる影響を低減する．

提案手法 TMSPD では，以下の手順を通して選択的破棄攻撃に対応するトラストモデルを実現する．

- リンクトラスト L_{ij} の算出
  リンクトラスト L_{ij} は，ノード i がノード j に対して算出する．転送に協力的なノードほど値は高く，一方，転送に協力的ではない非協力ノードは値が低くなる．
- 不信度 S_{ij} の算出
  不信度 S_{ij} は，ノード i がノード j に対して算出する選択的破棄攻撃を行うノードであるという予想値を数値化した値である．
- トラスト閾値 $T_{threshold}$ の決定
  ノード j に対する不信度 S_{ij} を用いたトラスト閾値 $T_{threshold}$ の決定を行う．トラスト閾値 $T_{threshold}$ とは，協力ノードと判断するためのリンクトラストの閾値である．ノード i がノード j に対して算出するリンクトラストが，トラスト閾値 $T_{threshold}$ 以下であるときは，ノード j は攻撃ノードとして検知される．

3.2 リンクトラスト L_{ij} の算出

リンクトラストとは，パケット転送率を基に各ノードが隣接ノードに対して算出する値である．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} は式 1 から算出される．

$$L_{ij} = \frac{\alpha_{ij} + \eta}{(\alpha_{ij} + \eta) + (\beta_{ij} + \rho)} \tag{1}$$

ここで，α_{ij} はノード j がノード i からのパケットを正常に転送した回数，β_{ij} はノード j がノード i からのパケットを破棄した回数．$\eta(\eta \geq 1)$ はパケット転送数の初期値，$\rho(\rho \geq 1)$ はパケット破棄数の初期値である．初期値を定義することにより，通信を行ったことのないノードに対してもリンクトラストの算出が可能となる．リンクトラストは 0 から 1 の間の値であり，転送に協力的なノードほど値は高く，一方，転送に協力的ではない非協力ノードは値が低くなる．

3.3 不信度 S_{ij} の算出

選択的破棄攻撃の特徴

選択的破棄攻撃とは，選択的にパケットを破棄することで，ある一定以上にリンクトラストを保つ攻撃である．選択的破棄攻撃に対応したトラストモデルを提案するために，選択的破棄攻撃を行うノードの特徴について考える．まず 1 つ目の特徴として，パケット転送数と破棄数の偏りが小さいことがあげられる．これは，ある一定以上にリンクトラストを保つために，パケット破棄を行うだけではなくパケット転送も行うことが原因である．もう 1 つの特徴として，選択的破棄攻撃を行うノードは選択的にパケットを破棄することで，ある一定以上にリンクトラストを保つため，通信数が多いにも関わらずリンクトラストが高い値に収束しないということがあげられる．

図 1 はパケット転送数・破棄数とリンクトラストの関係を表す．ここで図中，パケット転送数 α_{ij} は，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，パケット破棄数 β_{ij} は，ノード j がノード i からのパケットを破棄した回数．リンクトラスト L_{ij} は，ノード i が隣接ノード j に対して持つリンクトラストを表し，式 1 から算出される．式 1 中の定数 η は 1，定数 ρ は 1 とする．図 1 中の赤い丸で示した部分にあるノードは，パケット転送数と破棄数の偏りが小さく，また，通信数が多いのにリンクトラストが高い値に収束しないノードであると考えられる．したがって，選択的破棄攻撃を行っている可能性が高い．既存のトラストモデルにおいては，通信数が多くてもリンクトラストがブラックリスト定数 τ_α より高ければ協力ノードと判断される．図 1 中の赤い丸で示した部分は，リンクトラスト L_{ij} が 0.4 以上となっていることが分かる．したがって，たとえばブラックリスト定数 τ_α が 0.3 の場合，図 1 中の赤い丸で示した部分にあるノードは，非協力ノードとして検知されない．このように，選択的にパケットを破棄することで，ある一定以上にリンクトラストを保つ，つまり選択的破棄攻撃を行うノードは既存のトラストモデルでは検知できないことが分かる．

選択的破棄攻撃の特徴を考慮した不信度 S_{ij} の算出

不信度 S_{ij} とはノード i がノード j について算出する選択的破棄攻撃を行うノードであるという予想値を表した値である．不信度 S_{ij} を以下の式 2 で定義する．

$$S_{ij} = 1 - \frac{|\alpha_{ij} - \beta_{ij}| + 1}{\alpha_{ij} + \beta_{ij} + 1} \times \frac{1}{\alpha_{ij} + \beta_{ij} + 1} \times \mu \tag{2}$$

ここで，α_{ij} はノード j がノード i からのパケットを正常に転送した回数，β_{ij} はノード j がノード i からのパケットを破棄した回数．$\mu(\mu > 0)$ は定数である．不信度 S_{ij} は 1 以下の値であり，ノード j が選択的破棄攻撃を行うノードであるという予想値を定義する．

図 2 はパケット転送数・破棄数と不信度 S_{ij} の関係を表す．ここで図中，パケット転送数 α_{ij} は，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，パケット破棄数 β_{ij} は，ノード j がノード i からのパケットを破棄した回数．不信度 S_{ij} は，ノード i が隣接ノード j に対して持つ不信度を表し，式 2 から算出される．式 2 中の定数 μ は 20 とする．図 2 より，パケット転送数と破棄数の偏りが

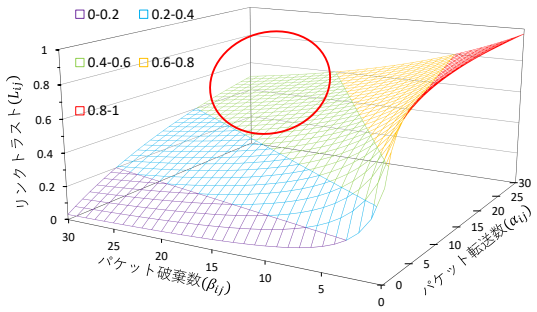

図 1　パケット転送数・破棄数とリンクトラスト L_{ij} の関係

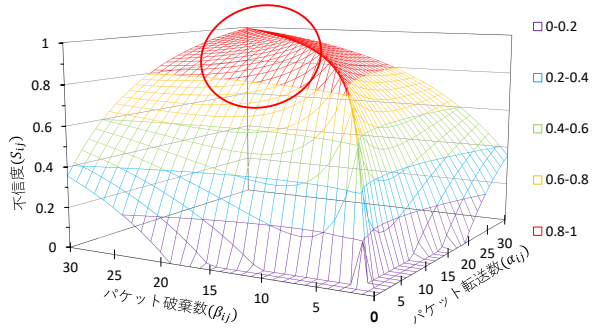

図 2　パケット転送数・破棄数と不信度 S_{ij} の関係

小さいときに不信度 S_{ij} は高く，また通信数が多いときも不信度 S_{ij} は高くなっていることが分かる．図 1 中の赤い丸で示した部分は，選択的破棄攻撃を行うノードである可能性が高い．図 1 と図 2 を比較すると，図 2 中では，赤い丸で示した部分の不信度 S_{ij} は高くなっていることが分かる．したがって，選択的破棄攻撃を行うノードである可能性が高いノードに対して，不信度 S_{ij} は高くなっていることが分かる．

3.4　トラスト閾値 $T_{threshold}$ の決定

トラスト閾値 $T_{threshold}$ とは，協力ノードと判断するためのリンクトラストの閾値である．ノード i がノード j に対して算出するリンクトラストがトラスト閾値 $T_{threshold}$ 以下であるときは，ノード j は攻撃ノードとして検知される．式 2 から算出した不信度 S_{ij} を用いてトラスト閾値 $T_{threshold}$ を決定する．トラスト閾値 $T_{threshold}$ を以下の式 3 で定義する．

$$T_{threshold} = S_{ij} \times \gamma \tag{3}$$

ここで不信度 S_{ij} はノード j が選択的破棄攻撃を行うノードであるという予想値を表した値であり，式 2 から算出される．$\gamma (0 < \gamma \leq 1)$ は定数である．不信度 S_{ij} が高いほど，トラスト閾値 $T_{threshold}$ も高くなる．

3.5　セキュアルーティングプロトコルへの適用

トラストモデル TMSPD は，様々なセキュアルーティングプロトコルへの適用が可能である．既存のトラストモデルで検知できない選択的破棄攻撃を行うノードを検知するために，本稿では，TMSPD を既存のセキュアルーティングプロトコル AOTDV [4] に適用する仕組みを説明する．

TMSPD の手順

ここでは，ルーティングにおけるパケットの転送を通して，各ノードが隣接ノードが協力ノードであるかを判断する手順を述べる．ノード i がノード j にパケットを転送した場合は以下の手順がとられる．なお，Step 5 は既存のセキュアルーティングプロトコル AOTDV におけるトラストモデルである．

Step 1: 送信元ノード i はノード j にパケットを送信．ノード i はノード j の転送を監視して，自身のトラスト記録表を更新する．

Step 2: 更新されたトラスト記録表に従って，式 1 よりリンクトラスト L_{ij} を算出する．

Step 3: 式 2 より不信度 S_{ij} を算出する．

Step 4: Step 3 で求めた不信度 S_{ij} を用いて，式 3 よりトラスト閾値 $T_{threshold}$ を決定する．

Step 5: リンクトラスト L_{ij} をブラックリスト定数 τ_{α} と比較して，ブラックリスト定数 τ_{α} より高ければ Step 6 に進み，そうでなければノード j をブラックリストに格納し，終了する．

Step 6: リンクトラスト L_{ij} をトラスト閾値 $T_{threshold}$ と比較して，トラスト閾値 $T_{threshold}$ より高ければ Step 7 に進み，そうでなければノード j をブラックリストに格納し，終了する．

Step 7: ノード j を協力ノードと判断し，終了する．

4.　シミュレーション評価

提案手法 TMSPD の有用性を示すため，選択的破棄攻撃が発生する環境を再現した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

提案手法を評価するにあたり，既存のトラストモデルを用いたセキュアルーティング AOTDV [4] と比較して，TMSPD ではどのような違いが生じるか確認した．今回の評価では，ネットワークシミュレータとして Qualnet [14] を用いてシミュレーションを行った．マップサイズ内にはすべてのパケットを転送する正常ノードと，設定したパケット転送率に基づいてデータパケットを転送する非協力ノードが存在する．シミュレーション時間を 3600 秒として，10 回の結果の平均値を用いて評価する．MAC 層のプロトコルとして，無線 LAN の規格 IEEE 802.11n を利用する．シミュレーションでは，すべてのノードは初め 1000m×1000m の範囲でランダムに配置され，そして，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

表 1　共通シミュレーション条件

シミュレータ	Qualnet 6.1
シミュレーション時間	3600 sec
ノード数	50
無線規格	IEEE 802.11n
マップサイズ	1000m × 1000m
送信電力	20dBm
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	1 pkt/s
モビリティモデル	Random waypoint
ノードの最大速度	1〜10 m/s
攻撃ノードのパケット転送率	0〜100 %
攻撃ノードの割合	20 %

表 2　トラストモデルに関するシミュレーション条件

リンクトラストの初期値 L_{ini}	0.5
ブラックリスト閾値 τ_α	0.4
式 1 中のパケット転送数の初期値 η	3
式 1 中のパケット破棄数の初期値 ρ	3
式 2 中の定数 μ	5, 10, 15, 20, 25
式 3 中の定数 γ	1

いう手順を繰り返し行う．また，各ノードは 1 ホップにおける送信電力 20dBm の中で通信が可能とする．その他のシミュレーションのパラメータは表 1 に示す．そして，トラストモデルに関するパラメータは表 2 に示す．

4.2　評価項目

本シミュレーションでは以下の 2 項目について評価を行った．

攻撃ノードによるパケット破棄数 (N_r) ：
全シミュレーション時間における，攻撃ノードがパケット転送要求を受けたにも関わらず，パケットを破棄した回数．

攻撃ノードの平均検知率 (N_d) ：
全シミュレーション時間における，各正常ノードが通信をしたことのある攻撃ノード数のうち，各正常ノードが攻撃ノードとして検知した攻撃ノード数の割合．平均検知率 (N_d) は式 4 によって定義される．

$$N_d = \frac{x_1}{x_2} \times 100 \qquad (4)$$

ここで，x_1 は正常ノードが攻撃ノードとして検知した攻撃ノード数，x_2 は正常ノードが通信をしたことのある攻撃ノード数である．

4.3　攻撃ノードのパケット転送率による影響

ここでは，ノードの最大速度を 2 m/s，式 2 中の定数 μ を 20 に固定し，攻撃ノードのパケット転送率を 0〜100% で変化させる．

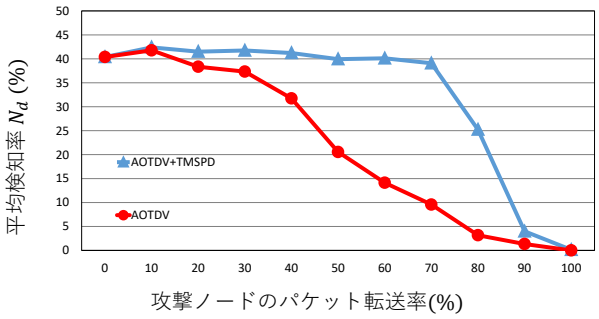

図 3　攻撃ノードのパケット転送率の変化に伴う攻撃ノードの平均検知率 (N_d) の変化

攻撃ノードの平均検知率 (N_d)

図 3 に攻撃ノードのパケット転送率の変化に伴う，正常ノードによる攻撃ノードの平均検知率を示す．図より，既存手法 AOTDV においては，攻撃ノードのパケット転送率の増加に伴い平均検知率は低下している．これは，攻撃ノードのパケット転送率が低ければ，リンクトラストも低くなり，攻撃ノードとして検知しやすいためである．そして，パケット転送率が 100% のとき，攻撃ノードはパケットを破棄しないため，攻撃ノードとして検知しない．一方，提案手法 TMSPD においては，パケット転送率 0% から 70% の間，平均検知率を 39% より高い値で保っている．提案手法 TMSPD は AOTDV と比較して常に同等またはそれ以上の高い平均検知率を得ており，さらに，攻撃ノードのパケット転送率が 0% から 70% の間，平均検知率の差は大きくなっている．特に，攻撃ノードのパケット転送率が 70% のとき AOTDV と比較して約 29 pt 平均検知率が向上している．これは，提案手法 TMSPD では選択的破棄攻撃を行っている可能性の高いノードに対して，高いリンクトラストの閾値を用いることによって，選択的破棄攻撃を行うノードを検知することができたためである．

以上の結果より，提案手法 TMSPD は既存手法 AOTDV と比較して，攻撃ノードの検知率を最大約 29 pt 向上させたことを確認した．

攻撃ノードによるパケット破棄数 (N_r)

図 4 に攻撃ノードのパケット転送率の変化に伴う攻撃ノードによるパケット破棄数を示す．図より，提案手法 TMSPD は既存手法 AOTDV と比較して，常に同等またはそれ以上の攻撃ノードによるパケット破棄数の削減をしていることが分かる，特に，攻撃ノードのパケット転送率が 60% のとき，攻撃ノードによるパケット破棄数を約 42% 削減している．これは，提案手法 TMSPD では選択的破棄攻撃を行うノードを攻撃ノードとして検知してブラックリストに格納し，ネットワークから除外したためである．

また，AOTDV は攻撃ノードのパケット転送率が 0% から 70% の間，パケット転送率の増加に伴い，攻撃ノードによるパケット破棄数が増加している．これは，図 3 より，

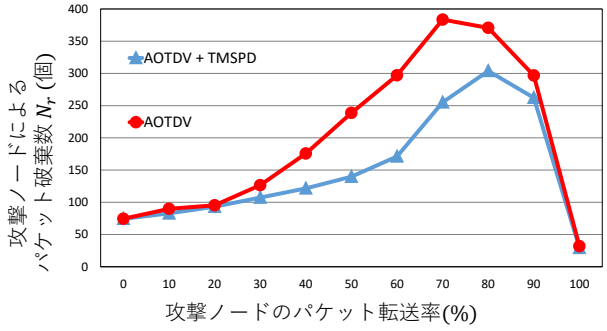

図 4　攻撃ノードのパケット転送率の変化に伴う攻撃ノードによるパケット破棄数 (N_r) の変化

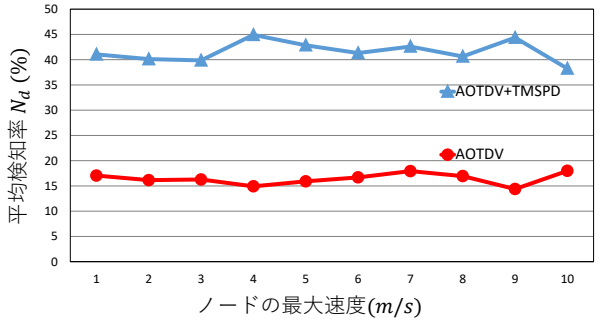

図 5　ノードの最大速度の変化による攻撃ノードの平均検知率 (N_d) の変化

既存手法 AOTDV において，攻撃ノードのパケット転送率の増加に伴い平均検知率が低下しているためである．

また，図 3 より，提案手法 TMSPD においては，パケット転送率 0% から 70% の間，検知率を 39% より高い値で保っている．しかし，提案手法 TMSPD では，攻撃ノードのパケット転送率が 0% から 80% の間，パケット転送率の増加に伴い，攻撃ノードによるパケット破棄数が増加している．これは，パケット転送率が高いほどリンクトラストも高くなるため，攻撃ノードとして検知するのに時間がかかり，検知するまでの間に攻撃ノードによってパケットを破棄されたためである．

また，提案手法 TMSPD と AOTDV 共に，パケット転送率が 100% のとき，攻撃ノードはパケット破棄を行わない．したがって，このときの攻撃ノードによるパケット破棄数は，ノードのモビリティといった環境により，目的ノードへの経路がなくなり，転送を行うことが不可能となったパケットの総数である．

以上の結果より，提案手法 TMSPD は既存手法 AOTDV と比較して選択的破棄攻撃を行うノードを検知することによって，攻撃ノードによるパケット破棄数を最大約 42% 削減したことを確認した．

4.4　ノードの速度による影響

ここでは，攻撃ノードのパケット転送率を 60%，式 2 中の定数 μ を 20 に固定し，ノードの最大速度を 1〜10 m/s で変化させる．

攻撃ノードの平均検知率 (N_d)

図 5 にノードの最大速度の変化に伴う，正常ノードによる攻撃ノードの平均検知率を示す．図より，今回のシミュレーションにおいて，提案手法 TMSPD はノードの最大速度に関わらず，平均検知率は約 42% で一定である．一方，AOTDV は常に約 16% の検知率を示す．したがって，提案手法 TMSPD は AOTDV と比較して常に高い平均検知率を得ていることが分かる．特にノードの最大速度が，4 m/s のとき約 29 pt 平均検知率が向上している．これは，提案手法が選択的破棄攻撃を行うノードを検知しているためである．

また本来は，ノードの最大速度が大きくなるほど，非協力ノードであると検知する前に通信範囲外に移動してしまうノードが存在するため，平均検知率が下がることが考えられる．しかし今回のシミュレーションでは，提案手法 TMSPD と AOTDV は共に，攻撃ノードの最大速度と平均検知率の間に関係がみられない．これは，すべてのノードがマップサイズ内を動くため，通信範囲外に移動しても，再び通信範囲内に移動することが可能なためである．

以上の結果より，提案手法 TMSPD は既存手法 AOTDV と比較して，今回のシミュレーションでは，ノードの最大速度に関わらず，攻撃ノードの平均検知率を最大約 29 pt 向上させたことを確認した．

攻撃ノードによるパケット破棄数 (N_r)

図 6 にノードの最大速度の変化に伴う，攻撃ノードによるパケット破棄数を示す．図より，提案手法 TMSPD は AOTDV と比較して，常に攻撃ノードによるパケット破棄数を削減していることが分かる．特にノードの最大速度が $2m/s$ のとき，攻撃ノードによるパケット破棄数を約 45% 削減していることが分かる．これは，図 5 より，提案手法 TMSPD では AOTDV と比較して選択的破棄攻撃を行うノードを攻撃ノードとして検知してブラックリストに格納し，ネットワークから除外したためである．また，提案手法 TMSPD と AOTDV は共に，攻撃ノードの最大速度と攻撃ノードによるパケット破棄数の間に関係がみられない．これは，図 5 より，提案手法 TMSPD と AOTDV は共に，攻撃ノードの最大速度に関わらず，平均検知率が一定のためである．

以上の結果より，提案手法 TMSPD は既存手法 AOTDV と比較して，今回のシミュレーションでは，ノードの最大速度に関わらず，選択的破棄攻撃を行うノードを検知をすることによって，攻撃ノードによるパケット破棄数を最大約 45% 削減したことを確認した．

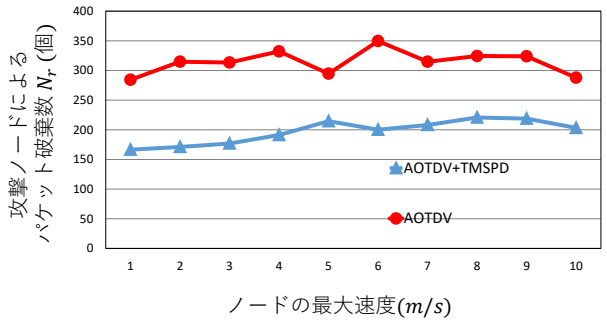

図 6　ノードの最大速度の変化による攻撃ノードによるパケット破棄数 (N_r) の変化

5. おわりに

本稿では，選択的破棄攻撃に対応するトラストモデル TMSPD を提案した．TMSPD では，選択的破棄攻撃による影響を緩和するために，選択的破棄攻撃を行うノードであるという予想値を表す不信度を導入した．選択的破棄攻撃の特徴をとらえて，選択的破棄攻撃を行う可能性の高いノードに対して，不信度に高い値を与えた．

選択的破棄攻撃を行うノードは，パケット転送数と破棄数の偏りが小さく，また通信数が多くなってもリンクトラストが高い値に収束しないという特徴をもつ．そこで，パケット転送数と破棄数の偏りが小さいノードに対して，不信度に高い値を与えた．また，通信数が多いにも関わらずリンクトラストが高い値に収束しないノードを検知するために，通信数が多いノードに対して不信度に高い値を与えた．

そして，不信度を，トラスト閾値に反映した．不信度の高いノードに対してリンクトラストの閾値を高くすることにより，選択的破棄攻撃を行うノードを検知し，ネットワークから除外することで，選択的破棄攻撃を行うノードによる影響を低減した．

シミュレーションによる評価を行い，提案手法を適用したときの攻撃ノードの平均検知率と攻撃ノードによるパケット破棄数を調査した．その結果，提案手法では攻撃ノードの平均検知率を最大約 29 pt 向上させたことを確認した．また，選択的破棄攻撃を行うノードを検知することによって，攻撃ノードによるパケット破棄数を最大約 42% 削減したことを確認した．また，今回のシミュレーションでは，ノードの最大速度に関わらず，攻撃ノードの平均検知率を最大約 29 pt 向上させ，それによって，攻撃ノードによるパケット破棄数を最大約 45% 削減したことを確認した．

以上より，提案手法 TMSPD は既存のトラストモデルと比較して，選択的破棄攻撃を行うノードを検知することで，選択的破棄攻撃による影響を緩和していることを確認した．

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] Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N. and Jamalipour, A.: A survey of routing attacks in mobile ad hoc networks, *IEEE Wireless Communications*, Vol. 14, No. 5, pp. 85–91 (2007).

[3] Movahedi, Z., Hosseini, Z., Bayan, F. and Pujolle, G.: Trust-Distortion Resistant Trust Management Frameworks on Mobile Ad Hoc Networks: A Survey, *IEEE Communications Surveys Tutorials*, Vol. 18, No. 2, pp. 1287–1309 (2016).

[4] 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).

[5] Karande, H. R. and Thorat, S. A.: Performance analysis of FTDSR and AOTDV trust based routing protocols, *2014 Eleventh International Conference on Wireless and Optical Communications Networks (WOCN)*, pp. 1–5 (2014).

[6] Thorat, S. and Kulkarni, P.: Design issues in trust based routing for MANET, *2014 Computing, Communication and Networking Technologies (ICCCNT)* (2014).

[7] Ohata, Y., Kamimoto, T., Shinohara, R. and Shigeno, H.: Cooperation Incentive System Balancing Virtual Credit in Mobile Ad Hoc Networks, *Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pp. 218–226 (2016).

[8] 沙也華梅田，百合大畑，崇史神本，寛　重野：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，情報処理学会論文誌，Vol. 57, No. 2, pp. 471–479 (2016).

[9] Abusalah, L., Khokhar, A. and Guizani, M.: A survey of secure mobile Ad Hoc routing protocols, *IEEE Communications Surveys Tutorials*, Vol. 10, No. 4, pp. 78–93 (2008).

[10] Mitra, P. and Mukherjee, S.: A review of trust based secure routing protocols in MANETs, *2015 International Conference and Workshop on Computing and Communication (IEMCON)*, pp. 1–7 (2015).

[11] Pirzada, A., McDonald, C. and Datta, A.: Performance comparison of trust-based reactive routing protocols, *IEEE Mobile Computing on Transactions*, Vol. 5, No. 6, pp. 695–710 (2006).

[12] Zhang, C., Zhu, X., Song, Y. and Fang, Y.: A Formal Study of Trust-Based Routing in Wireless Ad Hoc Networks, *2010, INFOCOM, IEEE*, pp. 1–9 (2010).

[13] Khatawkar, S. D. and Trivedi, N.: Detection of gray hole in MANET through cluster analysis, *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 1752–1757 (2015).

[14] Qualnet: Qualnet user manual, http://web.scalable-networks.com/content/qualnet ([Online; accessed 1-May-2017]).