Vol.2018-DPS-175 No.18
Vol.2018-MBL-87 No.18
Vol.2018-ITS-73 No.18
2018/5/24

モバイルアドホックネットワークにおける ノード使用度に注目したトラストモデルの検討

浅井 菜々香[1,a)]　五箇 奏乃子[1,b)]　重野 寛[1,c)]

概要：ノード間で協調して通信を行う 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攻撃ノードが存在する．この攻撃ノード対策として，トラストと呼ばれる評価値を用いて，攻撃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 1 つに，トラストを一定以上に保ちつつ，時間ごとにパケットの転送と破棄を繰り返すオンオフ攻撃がある．本稿では，ノード使用度に注目したトラストモデル UMO（Trust Model Focused on Node Usage against MANET On-Off Attack）を提案する．UMO ではオンオフ攻撃の特徴を考慮して，オンオフ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，オンオフ攻撃を行うノードの検知率が向上しネットワーク全体のパケット到達率が向上するという結果から，UMO の有用性を示す．

1. はじめに

モバイルアドホックネットワーク（MANET）[1] が，さまざま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 では端末間で直接通信を行っており，端末が動的にネットワークを構築しているため，大規模災害時などインフラが使用できない場合に通信を行う有効な手段として運用が期待されている．MANET では，モバイル端末でネットワークを構築しており，リソース確保のためにパケットを破棄する非協力ノードの存在が想定される．そこで，対策としてセキュアルーティングが提案されており， AOTDV[2], [3] や TA-AODV[4] などが挙げられる．セキュアルーティングでは，各ノードが自身の 1 ホップノードをトラストを用いて評価する評価値システムを用いて非協力ノードを避けたルーティングを実現する．トラストとは，ノードのパケット転送率で算出され，パケットの中継に協力的なノードほど高い値をもつ．トラストが閾値よりも低い場合，ブラックリストに格納し，ネットワークから除外する．このようにセキュアルーティングでは，非協力ノードの影響を低減し，パケット到達率を向上させている [2], [4].

しかし，MANET では非協力ノードとして検知されないように振舞う攻撃 [5] が存在する．たとえば悪口攻撃では，他ノードのトラストを実際よりも低く，近隣ノードに知らせることで，自身の評価を上げる．行動攻撃では，パケットの破棄を行う場所と自身のパケットを転送する場所を変えることで，パケット転送を可能とする．非協力ノードとして検知されないように振舞う攻撃の 1 つとして，オンオフ攻撃がある．オンオフ攻撃とは，時間ごとにパケットの転送と破棄を繰り返すことで，トラストを一定以上に保つ攻撃である．また，パケット中継依頼数が多い場合，意図的なパケット破棄を行っても，トラストが低下しにくいため，非協力ノードとして検知することが困難である．したがって，通信数に対して評価値システムが変わらないことにより，攻撃検知が困難であるという問題が発生する．

本稿では，オンオフ攻撃に対応したトラストモデル UMO（Trust Model Focused on Node Usage against MANET On-Off Attack）を提案する．本提案では通信数から算出するノード使用度に応じて，ブラックリストの閾値を動的に変化させる．通信数が多い場合，閾値を高く設定することで，オンオフ攻撃を行う非協力ノードを検知する．また，通信数が多いために，意図的なパケット破棄を行ってもトラストがあまり下がらず，非協力ノードとして検知することが困難であったノードも検知する．そして，非協力ノードをネットワークから除外することで，オンオフ攻撃による影響や非協力ノードの影響を低減する．

本稿では，2 章で関連研究について述べ，問題点を抽出する．3 章で，提案手法を説明し，4 章でコンピュータシ

[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)] asai@mos.ics.keio.ac.jp
[b)] goka@mos.ics.keio.ac.jp
[c)] shigeno@mos.ics.keio.ac.jp

ミュレーションを用いた評価によって提案手法の有用性を示す．最後に 5 章で本稿の結論を述べる．

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

送信元ノードから目的地ノードにパケット転送を行うとき，経路に非協力ノードを選択した場合，パケットは破棄され，目的地ノードに届かない．セキュアルーティングプロトコルとは，そのような非協力ノードが存在するような現実的な環境において，より信頼できる経路を選択することで，安全な通信を実現することを目標とするルーティングプロトコルである [6], [7].

MANET におけるセキュアルーティングプロトコルとして，評価値システムを用いたセキュアルーティングプロトコルを挙げることができる．評価値システムではトラストと呼ばれるノードに対する信頼度を表す指標を用いることで非協力ノードを検知し，より信頼性の高い安全な経路を選択する [8], [9].

2.1.1 トラストモデル

トラストとは，各ノードが隣接ノードに対して算出する値のことで信頼度を表す．このトラストが高いノードを中継ノードとして選択することで，各ノードは信頼できる経路を用いた通信が可能となる．

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で自身が送信したパケットを隣接ノードが正常に中継したかを確認し，トラストの算出や更新を行う．ここで、正常に中継するとは，データが改ざんされたり破棄されたりせずに転送されたことを意味する．トラストとはパケット転送率を表しており，中継依頼を受けた全パケット数に対する正常に中継したパケット数の割合で定義される [10]．よってトラストの値は 0 以上 1 以下の値であり，中継に協力的なノードはトラストが高く，一方で，中継に協力的ではない非協力ノードではトラストが低くなる．

2.1.2 ブラックリスト

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検知するために使用される閾値がブラックリスト閾値である．各ノードにおいて，トラストがブラックリスト閾値以下である隣接ノードは非協力ノードであると考えることができるため，ブラックリストに格納される．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ない．また，ブロードキャスト以外において，そのノードにパケットの転送を行わない．つまり，全隣接ノードのブラックリストに格納された場合，そのノードはそのネットワーク上から完全に除外されることを表す．

このように，ブラックリストを使用することで，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り，信頼できる協力ノードによって構成されたネットワークにおいて安全な通信を行うことが可能となる．

2.2 既存研究の問題点

MANET ではさまざまな攻撃が想定される．本稿において，通信数とは中継ノードとして選択された回数とする．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，一定時間でパケットの転送と破棄を繰り返すことで，一定以上のトラストを保ちつつ，パケット破棄を行うオンオフ攻撃などについては考慮されていない [11]．また，通信数が多い場合，意図的なパケット破棄を行なってもトラストが下がりにくいため，非協力ノードとして検知されにくいという問題が挙げられる．本稿では，この 2 つの問題点をオンオフ攻撃問題，検知問題と定義し，以下それぞれの問題の原因，そしてネットワークに与える影響について述べる．

2.2.1 オンオフ攻撃問題

オンオフ攻撃 [5] とは，時間ごとにパケットの転送と破棄を繰り返すことで，一定以上のトラストを保ちつつパケット破棄を行う攻撃である．ブラックリスト閾値に定数を用いる既存のトラストモデルではオンオフ攻撃を検知することができない．オンオフ攻撃を行うノードを協力ノードと判定することで，非協力ノードによるパケット破棄が発生する．また，協力ノードがオンオフ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，オンオフ攻撃を行うノードに対してパケットを送信することも想定される．つまり，ノードのリソースに限りがある MANET において，協力ノードが余分なリソースを使用することとなり，ネットワーク全体の性能が低下することが考えられる．したがって，オンオフ攻撃を行うノードを非協力ノードとして検知できないというオンオフ攻撃問題は解決すべき課題である．

2.2.2 検知問題

トラストの算出において，転送率を用いるが，これはあるノードが隣接ノードに対して算出するもので，通信数に対する正常に中継したパケット数の割合を表している．つまり，通信数が少ないほど，トラストは大幅に変動し，通信数が多いほど，トラストは正常に中継したパケット数に対しての変動が小さくなる．よって，通信数が少ない場合において，通信エラーによるパケット損失が起きたとき，トラストが大幅に減少してしまい，非協力ノードとして検知されてしまう可能性がある．また，通信数が多い場合において，意図的にパケット破棄を行っても，トラストはあまり減少しないため，非協力ノードとして検知することが困難である．既存のセキュアルーティングにおけるトラストモデルにおいては，ブラックリスト閾値は通信数に依存

しない定数を用いている．このブラックリスト閾値が低い値だった場合，前者の問題については対応できるが，全体としての非協力ノードの検知率は低下する．またブラックリスト閾値が高い値だった場合，後者の問題については対応でき，また全体の非協力ノードの検知率は上がるが，前者の問題への対応ができないため，協力ノードを非協力ノードであると誤検知してしまうことが想定される．以上より，ブラックリスト閾値に通信数に依存しない定数を用いることで，ネットワーク全体の性能が低下することが考えられる．したがって，通信数を考慮しないことにより発生する検知問題は解決すべき課題である．

3. 提案

本章では，ノード使用度に注目した，オンオフ攻撃問題と検知問題に対応したトラストモデルとして UMO（Trust Model Focused on Node Usage against MANET On-OffAttack）を提案する．

3.1 提案の概要

UMO では，オンオフ攻撃問題と検知問題を解決するために，ノード使用度 U_{ij} を導入する．ノード使用度 U_{ij} とは，ノード j がノード i によって過去に中継ノードとして選択された回数を 0 以上 1 未満で表した値であり，値が大きいほど，ノード j がノード i によって中継ノードとして選択された回数が多いことを表す．

図 1 のようにノード i とノード j は 1 ホップの近接ノードとする．まず，ノード i が隣接ノード j にパケットの中継を依頼した後，オーバヒアによってパケットが正常に中継されたか確認し，トラスト T_{ij} を算出する．次に，過去の通信数からノード使用度 U_{ij} を算出し，ブラックリスト閾値 B_{ij} の決定を行なう．最後に，ブラックリスト閾値とトラストを比較し，閾値以下の場合は非協力ノードと判定し，ブラックリストに格納する．

提案手法 UMO では，以下の手順を通してオンオフ攻撃問題と検知問題に対応するトラストモデルを実現する．

トラスト T_{ij} の算出

トラスト T_{ij} は，ノード i がノード j に対して算出する．中継に協力的なノードほど値は高く，一方，中継に協力的ではない非協力ノードは値が低くなる．

ノード使用度 U_{ij} の算出

ノード使用度 U_{ij} は，ノード i がノード j に対して算出する．ノード j がノード i によって過去に中継ノードとして選択された回数を 0 以上 1 未満で表した値であり，値が高いほどノード j がノード i から中継ノードとして選択された回数が多いことを表す．

ブラックリスト閾値 B_{ij} の決定

ノード j に対するノード使用度 U_{ij} を用いたブラックリスト閾値 B_{ij} の決定を行う．ブラックリスト閾値 B_{ij} とは，ノード i がノード j を協力ノードであるか判定するためのトラストの閾値である．ノード i がノード j に対して算出するトラストが，ブラックリスト閾値 B_{ij} 以下であるとき，ノード j は非協力ノードとして検知される．

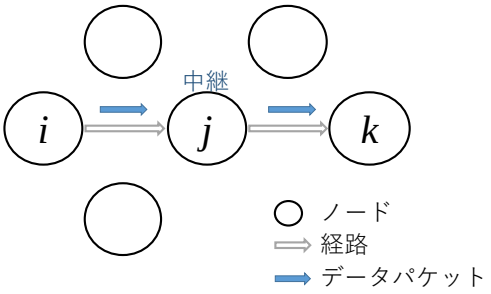

図 1 ノード i とノード j の関係

3.2 提案の動作

3.2.1 トラスト T_{ij} の算出

トラスト T_{ij} とは，ノード i がノード j に対して，パケット転送率に基づいて算出する値である．ノード i 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 j が正常に転送したかを確認し，トラストの算出と更新を行う．トラストはパケット転送率を表し，ノード j がノード i から中継依頼を受けた全パケット数に対して，ノード j が正常に中継したパケット数の割合で定義する．以上より，ノード i が隣接ノード j に対して算出するトラスト T_{ij} は式 1 によって定義する．

$$T_{ij} = \frac{\alpha_{ij} + \eta}{(\alpha_{ij} + \eta) + (\beta_{ij} + \sigma)} \tag{1}$$

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，η はパケット転送数の初期値，σ はパケット破棄数の初期値である．ただし，$\eta \geq 1 \cap \sigma \geq 1$ 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トラストの算出が可能となる．トラストは 0 以上 1 以下の値であり，転送に協力的なノードほど値は高く，転送に協力的ではない非協力ノードは値が低くなる．

3.2.2 ノード使用度 U_{ij} の算出

ノード使用度 U_{ij} とは，ノード j がノード i によって過去に中継ノードとして選択された回数を 0 以上 1 未満で表した値であり，値が大きいほど，ノード j が中継ノードとして選択された回数が多いことを表す．

ノード使用度 U_{ij} は式 2 によって定義する．

Vol.2018-DPS-175 No.18
Vol.2018-MBL-87 No.18
Vol.2018-ITS-73 No.18
2018/5/24

$$U_{ij} = 1 - \frac{\gamma}{\alpha_{ij} + \beta_{ij} + \gamma} \quad (2)$$

ここで，α_{ij} はノード j がノード i から中継依頼を受けたパケットを正常に中継した回数，β_{ij} はノード j がノード i から中継依頼を受けたパケットを破棄した回数，γ は定数である．ただし，$\gamma > 0$ とする．ノード使用度 U_{ij} は 1 未満の値であり，値が高いほど，ノード i によって過去に中継ノードとして選択された回数が多いことを表す．

図 2 は通信数とノード使用度 U_{ij} の関係を表す．通信数とは，ノード j がノード i から過去に中継ノードとして選択された回数のことである．

式 2 の通信数 $\alpha_{ij} + \beta_{ij}$ は通信数を表す．また，ノード使用度 U_{ij} は，ノード i が隣接ノード j に対して持つノード使用度を示し，式 2 で算出される．式 2 の定数 γ を 5，10，20，30 と変化させ，それぞれのノード使用度を算出した．図 2 より，通信数が 0 のとき，ノードの使用度は 0 である．そして通信数が増えるにつれて，ノード使用度が上昇することがわかる．さらに，式 2 の γ を変化させたとき，γ の値が小さいほど急激にノード使用度が上昇し，γ の値が大きいほど，緩やかにノード使用度が上昇することがわかる．

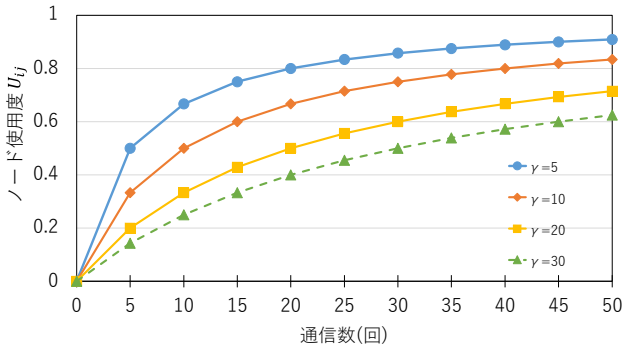

図 2 通信数とノード使用度 U_{ij} の関係

3.2.3 ブラックリスト閾値 B_{ij} の決定

ブラックリスト閾値 B_{ij} とは，協力ノードかどうかを判定するためのトラストの閾値を表す．ノード i がノード j に対して算出するトラストがブラックリスト閾値 B_{ij} 以下であるとき，ノード i はノード j を非協力ノードとして検知する．式 2 より算出したノード使用度 U_{ij} を用いて，ブラックリスト閾値 B_{ij} の決定を行う．

ブラックリスト閾値 B_{ij} は式 3 によって定義する．

$$B_{ij} = U_{ij} \times \rho \quad (3)$$

ここで，式 3 の ρ は定数であり，$0 < \rho \leq 1$ である．式 3 より，ノード使用度 U_{ij} に比例して，ブラックリスト閾値 B_{ij} も上昇する．

ノード使用度が低いノードに対してはブラックリスト閾値を低くすることで，トラストが低くても非協力ノードとして検知しない．一方で，ノード使用度の高いノードに対してはブラックリスト閾値を高くすることで，トラストが閾値未満の場合には非協力ノードとして検知する．また，ρ が大きいとき，ノード使用度の増加に伴い，ブラックリスト閾値は大きく変化するが，ρ が小さいとき，ノード使用度の増加に伴うブラックリスト閾値の変化は小さくなる．さらにノード使用度 U_{ij} が 0 以上 1 未満の値であることから，ブラックリスト閾値は $0 \leq B_{ij} < \rho$ の値をとることがわかる．

3.3 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 UMO は，さまざま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．既存研究では解決できないオンオフ攻撃問題そして検知問題を解決するために，UMO を既存のルーティングプロトコル AODV に適用する仕組みを説明する．

UMO 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を協力ノードか，または非協力ノードであるかを判定する手順を述べる．ノード i がノード j にパケットの中継を依頼した場合，以下の手順がとられる．

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 の中継をオーバヒアして，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 よりトラスト T_{ij} を算出する．

Step 3: 式 2 よりノード使用度 U_{ij} を算出する．

Step 4: Step 3 で求めたノード使用度 U_{ij} を用いて，式 3 よりブラックリスト閾値 B_{ij} を決定する．

Step 5: トラスト T_{ij} をブラックリスト閾値 B_{ij} と比較して，ブラックリスト閾値 B_{ij} より高ければノード j を協力ノードと判定し，終了する．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．

4. シミュレーション評価

提案手法 UMO の有用性を示すために，オンオフ攻撃またはランダムパケット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なった．

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 [12] を用いてシミュレーションを行った．提案手法を評価するにあたり，既存のトラストモデルを使用したセキュアルーティング AOTDV[2] と比較して，提案手法 UMO ではどのような違いが生じるか確認した．

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．ネットワークには，IEEE 802.11n を利用するものとした．シミュレーションでは，全てのノードを 1000m×1000m の範囲でランダムに配置し，ランダムに選択したノードへのデータパケット送信を繰り返す．また，送信電力は 20dBm とした．その他のシミュレーションのパラメータは表 1 に示す．また, AOTDV と UMO における個別のパラメータはそれぞれ表 2, 表 3 で表す. 表 1, 表 2 の値は，既存研究 AOTDV[2] のパラメータを基に決定した．

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
全ノード数	50
無線規格	IEEE 802.11n
マップサイズ	1000m × 1000m
転送範囲	250m
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 pkts/s
モビリティモデル	Random waypoint

表 2 AOTDV に関するシミュレーション条件

トラストの初期値 T_{ini}	0.75
ブラックリスト閾値 β_α	0.4
パケット転送数の初期値	3
パケット転送要求数の初期値	4

表 3 UMO に関するシミュレーション条件

トラストの初期値 T_{ini}	0.5
式 1 中のパケット転送数の初期値 η	1
式 1 中のパケット破棄数の初期値 σ	1
式 2 中の定数 γ	10
式 3 中の定数 ρ	0.9

4.2 ノードの行動モデル

ノードの行動において，今回のシミュレーションでは 2 種類のノードが存在する．

協力ノード

常にすべてのパケット転送を正常に行うノードを表す．意図的なパケット破棄や，パケットの中身の改ざんを行わず，ネットワークに協力的な振る舞いをする．

非協力ノード

自身が送信元, もしくは目的ノードであるデータパケットのみ送受信を行うが, 他のデータパケットの転送は設定したパケット破棄率に応じてパケット破棄を行うノードを表す．ただし, 制御パケットの転送は行うとする．

- **オンオフ攻撃**

  時間ごとにパケットの転送と破棄を繰り返し，一定以上のトラストを保つ攻撃を表す．

- **ランダムパケット破棄攻撃**

  パケット破棄率にあわせてランダムにパケットの破棄を行う攻撃を表す．

4.3 評価項目

本シミュレーションでは以下の項目について評価を行った．

攻撃ノードの平均検知率（AD） ：

各協力ノードが，全体の非協力ノード数のうち検知できた割合を表す．平均検知率 AD は式 4 によって定義する．

$$AD = \frac{N_d}{N_c} \times 100 \tag{4}$$

ここで，N_d は協力ノードが検知した非協力ノードの平均個数，N_c は協力ノードが通信をしたことのある非協力ノード数とする．

パケット到達率 (PDR) ：

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常に目的ノードに到達したデータパケット数の割合を表す．本稿では, 非協力ノードを除く協力ノードが送信したデータパケットの到達率を算出する．パケット到達率 PDR は式 5 によって定義する．

$$PDR = \frac{N_a}{N_s} \times 100 \tag{5}$$

ここで，N_a は目的ノードに到達したデータパケット数，N_s は送信元ノードで送られたデータパケット数とする．

4.4 攻撃ノードのパケット破棄率による影響

ここでは, ノードの最大速度を 0〜5m/s とし, 攻撃ノードの個数を 20 個，オンオフ攻撃のオンオフの 1 サイクルを 10 秒に固定した．また，攻撃ノードのパケット破棄率を 0〜100% で変化させる．

4.4.1 攻撃ノードの平均検知率（AD)

(a). オンオフ攻撃

図 3 は，オンオフ攻撃ノードのパケット破棄率の変化に伴う，協力ノードによる攻撃ノードの平均検知率を示す．図 3 より，既存手法 AOTDV においては，攻撃ノードのパケット破棄率の増加に伴い，検知率は増加している．これは，パケット破棄率が高いとき，トラストは低くなるため，AOTDV のブラックリスト閾値 0.4 以下になると検知することができるからである．

一方，提案手法 UMO では AOTDV と比較して，常に高い検知率を示している．特に攻撃ノードのパケット破棄率

Vol.2018-DPS-175 No.18
Vol.2018-MBL-87 No.18
Vol.2018-ITS-73 No.18
2018/5/24

が 40% のとき，UMO は AOTDV に対して，約 19*pt* 平均検知率を向上させた．攻撃ノードのパケット破棄率が 20% から 40% について，UMO が AOTDV に対して大きく差をつけている理由として，AOTDV のブラックリスト閾値が 0.4 であるため，0% ～ 60% のパケット破棄率のノードを検知することが困難であることが挙げられる．それに対して，UMO ではノード使用度の高いノードに対して，ブラックリスト閾値を高く設定しているため，一定以上のトラストを保つオンオフ攻撃を行う攻撃ノードを検知した．以上の結果から，提案手法 UMO は既存手法 AOTDV と比較して，オンオフ攻撃ノードの平均検知率を最大約 19*pt* 向上させたことを確認した．

(b)． ランダムパケット破棄攻撃

図 4 は，ランダムパケット破棄攻撃ノードのパケット破棄率の変化に伴う，協力ノードによる攻撃ノードの平均検知率を示す．図 4 より，既存手法 AOTDV においては，攻撃ノードのパケット破棄率の増加に伴い，検知率は増加している．これは，パケットの破棄率が高いとき，トラストは低くなるため，AOTDV のブラックリスト閾値 0.4 以下になると検知することができるからである．

一方，提案手法 UMO では AOTDV と比較して，常に高い検知率を示している．特に攻撃ノードのパケット破棄率が 40% のとき，UMO は AOTDV に対して，約 30*pt* 平均検知率を向上させた．AOTDV ではブラックリスト閾値に定数を用いているため，20% のランダムパケット破棄を行う攻撃ノードをほとんど検知できていないが，UMO ではノード使用度が高くなればブラックリスト閾値が上昇するため，ノード使用度の高いノードに対して攻撃ノードであるか否かを厳しく判定することで，20% のランダムパケット破棄でも約 14% の検知率を達成した．以上の結果から，提案手法 UMO は既存手法 AOTDV と比較して，ランダムパケット破棄攻撃ノードの平均検知率を最大約 30*pt* 向上させたことを確認した．

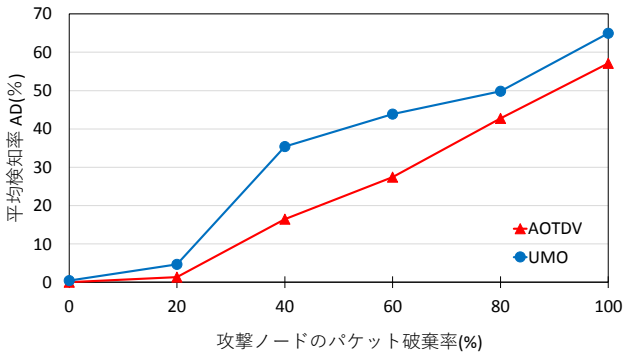

図 3 オンオフ攻撃ノードのパケット破棄率の変化に伴う攻撃ノードの平均検知率の変化

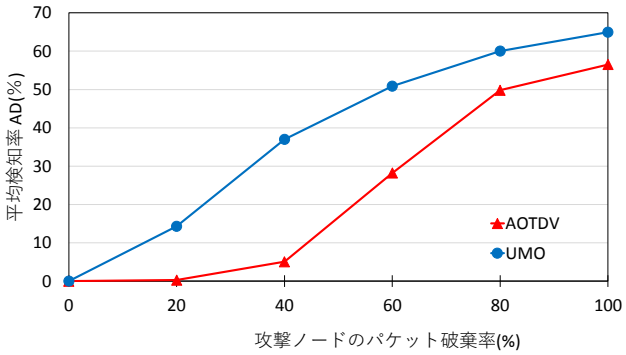

図 4 ランダムパケット破棄攻撃ノードのパケット破棄率の変化に伴う攻撃ノードの平均検知率の変化

4.4.2 パケット到達率（*PDR*）

(a)． オンオフ攻撃

図 5 は，オンオフ攻撃ノードのパケット破棄率の変化に伴うパケット到達率を示す．図 5 より，どちらの手法においても，攻撃ノードのパケット破棄率が増えると，パケット到達率は低下している．また，提案手法 UMO と既存手法 AOTDV を比較すると，同等かそれ以上のパケット到達率を達成していることがわかる．まず，攻撃ノードのパケット破棄率が増加すると，攻撃ノードによりパケットが破棄される可能性が高くなるため，到達率は低下する．AOTDV では，ブラックリスト閾値が 0.4 であるため，パケット破棄率が 60% 以下のオンオフ攻撃を行う攻撃ノードを検知するのは困難であり，攻撃ノードをネットワークから除外することができず，パケット到達率が低下する．また，パケット破棄率が 60% 以上の場合に関しては，攻撃ノードの検知率は上昇するが，検知できない攻撃ノードの破棄率も上昇しているため，全体のパケット到達率としては低下する．次に，提案手法 UMO では，ノード使用度の高いノードに対してブラックリスト閾値を高く設定しているため，ノード使用度が高い場合オンオフ攻撃を行うノードを検知できる．よって，攻撃ノードをネットワークから除外することができるため，AOTDV より高い到達率を示す．特に，攻撃ノードのパケット破棄数が 80% のとき，UMO は AOTDV に対して，最大約 3*pt* パケット到達率を向上させた．

(b)． ランダムパケット破棄攻撃

図 6 は，ランダムパケット破棄攻撃ノードのパケット破棄率の変化に伴うパケット到達率を示す．図 6 より，どちらの手法においても，攻撃ノードのパケット破棄率が増えると，パケット到達率は低下している．また，提案手法 UMO と既存手法 AOTDV を比較すると，同等かそれ以上のパケット到達率を達成していることがわかる．まず，攻撃ノードのパケット破棄率が増加すると，攻撃ノードによりパケットが破棄される可能性が高くなるため，到達率は低下する．AOTDV では，ブラックリスト閾値が 0.4 であり，パケット破棄率が 60% 以下のランダムパケット破棄攻

撃を行う攻撃ノードを検知するのは困難であるため，攻撃ノードをネットワークから除外することができず，パケット到達率が低下する．また，パケット破棄率が 60% 以上の場合に関しては，攻撃ノードの検知率は上昇するが，検知できない攻撃ノードのパケット破棄率も上昇しているため，全体のパケット到達率としては低下する．次に，提案手法 UMO では，ノード使用度の高いノードに対してブラックリスト閾値を高く設定しているため，ノード使用度が高い場合ランダムパケット破棄攻撃を行うノードを検知できる．よって，攻撃ノードをネットワークから除外することができるため，AOTDV より高い到達率を示す．特に，攻撃ノードのパケット破棄率が 80% のとき，UMO は AOTDV に対して，最大約 5*pt* パケット到達率を向上させた．

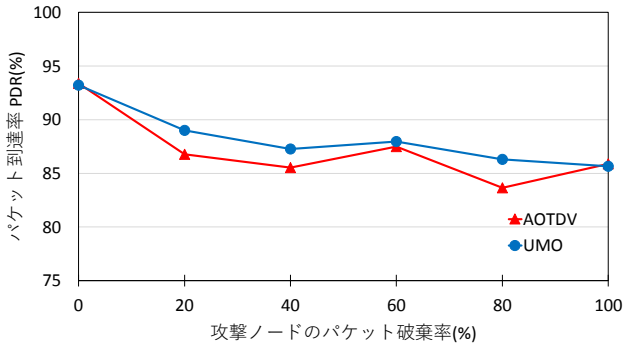

図 5 オンオフ攻撃ノードのパケット破棄率の変化に伴うパケット到達率の変化

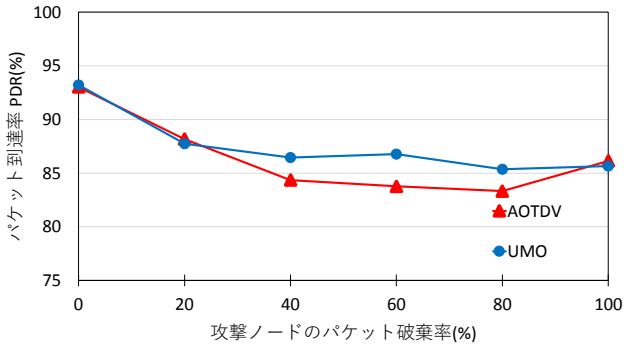

図 6 ランダム破棄攻撃ノードのパケット破棄率の変化に伴うパケット到達率の変化

5. おわりに

本稿では，ノード使用度に注目した動的なブラックリスト閾値を用いたトラストモデル UMO を提案した．提案手法 UMO では，過去に中継ノードとして選択された回数を 0 以上 1 未満で表した値としてノード使用度を導入した．ノード使用度は，中継ノードとして選択された回数の増加に伴い増加する．また，ブラックリスト閾値をノード使用度によって動的に変化させることで，ノード使用度の低いノードに対しては低いブラックリスト閾値を用い，ノード使用度の高いノードに対しては高いブラックリスト閾値を用いた．よって，通信数が多く，意図的なパケット破棄を行う非協力ノードを効果的に検知し，さらに，時間ごとにパケットの転送と破棄を繰り返すことで，一定以上のトラストを保つオンオフ攻撃を行うノードを検知することが可能となった．

シミュレーションを用いて評価を行い，提案手法 UMO は既存手法 AOTDV と比べて，攻撃ノードの平均検知率をオンオフ攻撃で最大約 19*pt*，ランダムパケット破棄攻撃で最大約 30*pt* 向上させたことを確認した．この結果，パケット到達率をオンオフ攻撃で最大約 3*pt*，ランダムパケット破棄攻撃で最大約 5*pt* 向上させたことを確認した．

以上より，提案手法 UMO は既存のトラストモデルと比較して，非協力ノードを効果的に検知することで，オンオフ攻撃問題と検知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 17KT0082 の助成を受けたものです．

参考文献

[1] S. Corson and J. Macker, *Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations*, RFC 2501 (Informational), (1999).
[2] X. Li, Z. Jia, P. Zhang, R. Zhang, and H. Wang, Trust-based on-demand multipath routing in mobile ad hoc networks, 技術評論社 nformation Security, IET, Vol. 4, No. 4, pp.212-232(2010).
[3] H. R. Karande and S. A. Thorat, Performance analysis of ftdsr and aotdv trust based routing protocols, Eleventh International Conference on Wireless and Optical Communications Networks(2014).
[4] 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).
[5] A.A. Pirzada, C. McDonald, and A. Datta, Trust-distortion resistant trust man-agement frameworks on mobile ad hoc networks: A survey, IEEE Communications Surveys and Tutorials,(2016).
[6] S.A. Thorat and P.J. Kulkarni, Design issues in trust based routing for manet, In Computing, Communication and Networking Technologies(2014).
[7] Yuri Ohata, Takashi Kamimoto, Ryoki Shinohara, and Hiroshi Shigeno, Cooperation incentive system balancing virtual credit in mobile ad hoc networks, In Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, pp. 218-226,(2016).
[8] Huaizhi Li and M. Singhal, Trust management in distributed systems, Computer, Vol. 40, No. 2, pp. 45-53(2007).
[9] P. Mitra and S. Mukherjee, A review of trust based secure routing protocols in manets, In 2015 International Conference and Workshop on Computing and Com- munication, pp.1-7(2015).

[10] Chi Zhang, Xiaoyan Zhu, Yang Song, and Yuguang Fang, A formal study of trust-based routing in wireless ad hoc networks, In INFOCOM, 2010 Proceedings IEEE, pp. 1-9(2010).
[11] S. D. Khatawkar and N. Trivedi, Detection of gray hole in manet through cluster analysis, In 2015 2nd International Conference on Computing for Sustainable Global Development, pp.1752-1757(2015).
[12] Qualnet, Qualnet user manual, 入手先 ⟨http://web.scalable-networks.com/content/qualnet⟩ ([Online; accessed 9-Apr-2018]).