L-031

アドホックネットワークにおける動的閾値を用いたブラックホール攻撃防御法

A Black-hole Attack Prevention Method using Dynamic Threshold in Adhoc Networks

野口拓 †
Taku Noguchi
山本貴也 †
Takaya Yamamoto

1. まえがき

固定インフラを必要とせず，各ノードが相互に無線接続される事でネットワークを形成するアドホックネットワークは，場所や設備の制約を受けずに柔軟にネットワークを構築できるため，その特徴を活かした様々なアプリケーションが考えられている．例えば，大規模災害発生時の安否情報・非難情報の通知や，車両間アドホックネットワークを利用した安全運転支援，緊急車両・事故情報通知などが検討されている．このようなアプリケーションにおいて人命の安全に関わる情報を扱う場合，通信そのものに高いセキュリティが求められる．しかし，インフラレスであるアドホックネットワークでは送信元ノードと宛先ノード以外のノードがルータとしてデータ転送に寄与するため，なりすましやデータの改ざん・盗聴など従来の固定有線／無線ネットワーク上でも存在していたセキュリティ脅威に加え，データの不正受信や意図的廃棄などアドホックネットワーク特有のセキュリティ脅威が存在する．

アドホックネットワークのセキュリティ脅威として特に問題視されているものの 1 つがブラックホール攻撃 [1, 2] である．ブラックホール攻撃は通信経路に対する攻撃の一種であり，攻撃ノードが宛先ノードあるいは有力な中継候補ノードになりすまし，送信元ノードが送信したデータを不正に受信し廃棄する攻撃である．ブラックホール攻撃によって送信データの大部分が不正に廃棄されると，パケット到達率やスループットが低下するだけでなく，経路再構築などの制御トラヒックが急増し，ネットワーク全体に甚大な影響を及ぼす．アドホックネットワークにおける代表的ルーチングプロトコルである AODV[3] は，シーケンス番号とホップ数を用いて経路選択を行っているため，この 2 つの情報を偽造することで簡単にブラックホール攻撃が可能である．

本論文では，AODV 型ルーチングプロトコルに対するブラックホール攻撃の防御法を提案する．提案手法では，ノード数や経過時間などのネットワークから取得可能な情報に基づいて，ノードを正常ノードとブラックホールノードに分類する．提案手法では，ブラックホールノードリスト（ブラックリスト）を用いてブラックホールノードを排除した経路を設定することでブラックホール攻撃を防ぐ．さらに，ブラックリスト内のブラックホールノードに対しダミーの経路要求（RREQ:Route REQuest）を用いて再判定を行い，ブラックホールノードの誤判定を防ぐ．提案手法の有効性を検証するため，ネットワークシミュレータを用いた性能評価を行う．

†立命館大学情報理工学部, College of Information Science and Engineering, Ritsumeikan University

2. 関連研究

AODV に対するブラックホール攻撃に関する既往研究は，1) オピニオンベース，2) シーケンス番号ベースに分類できる．オピニオンベース方式は，正常ノードとブラックホールノードの振る舞いの違いに着目する．AODV では，経路応答（RREP:Route REPly）の返送経路上にあるノードがルータの役割を果たし他ノード宛のパケットを転送する．一方，ブラックホールノードはパケットの転送をほとんど行わない．さらに，ブラックホールノードは自身への経路を設定させるため，RREQ には必ず応答する．このような振る舞いの違いに関して，他ノードから報告されるオピニオンをもとにブラックホールノードを識別する．シーケンス番号方式は，ブラックホール攻撃時に AODV で用いられる経路の新しさを示すシーケンス番号が偽造される点に着目し，不自然なシーケンス番号を持つ RREP 送信元をブラックホールノードと判定する．本論文の提案手法は，オピニオンベースとシーケンス番号ベース両者のハイブリッド方式にとなる．

オピニオンベース方式の SADOV[4] は，受信した RREP に含まれる次ホップ情報（オピニオン）を蓄積し，この情報を元に正常ノードとブラックホールノードを識別する．RREQ 送信ノードが一定期間内に受信した同一宛先ノードに関する複数の RREP を分析し，複数の RREP が共通する次ホップノードを持つ場合に，その次ホップノードを正常ノードと判断する．

文献 [5, 6] で提案されている手法もオピニオンベース方式に分類される．[5] は，各ノードが隣接ノードの転送パケットをモニタリングし，RREP 送信元ノードの転送パケット数が閾値を下回った場合にブラックホールノードと判定する手法を提案している．ブラックホールノード情報は，ブロードキャストで全ノードに周知され，ブラックホールノードは通信経路から排除される．[6] では，信頼されたノード (Base Node) が定期的にダミー RREQ を送信し，この RREQ に対し RREP で応答したノードをブラックホールノードと判定する．ブラックホールノードを伝えるブロックメッセージはブロードキャストによって全ノードに転送され，ブラックホールノードは通信経路から排除される．

シーケンス番号ベース方式としては，文献 [7, 8, 9] や SRD-AODV[10] がある．[7] は，RREQ 送信数，RREP 受信数および，一定時間内に受信した RREP のシーケンス番号から計算される特徴量を利用して，ブラックホール攻撃を検知する手法を提案している．[8, 9] は，ネットワークの通信状況に応じた閾値を用い，RREP

内の宛先シーケンス番号が閾値を超える場合は，RREP 送信元をブラックホールノードと判定する．しかし，閾値の算出方法は検討課題となっており，明らかにされていない．SRD-AODV[10] は，ネットワーク内のノード数に応じてシーケンス番号閾値を定めており，ノード数が多い場合にはシーケンス番号の増加率が大きくなる点を考慮し，閾値も大きな値に設定している．

3.Ad Hoc On Demand Distance Vector Routing（AODV）

リアクティブ型の代表的なルーチングプロトコルである AODV は，データ送信前に経路を確立する．各ノードは自身のシーケンス番号を持ち，RREQ 生成時および RREQ に対する RREP 送信時にシーケンス番号を更新する．各ノードは，シーケンス番号を用いて経路の新しさを判断する．AODV における経路構築手順は以下の通りである．

1. 送信元ノードは，RREQ をブロードキャストする．
2. RREQ を受信したノードは，自身のルーチングテーブルに宛先ノードの経路エントリがあるかどうか確認する．経路エントリが存在しない，あるいは古い経路エントリしかない場合 RREQ を最ブロードキャストする．
3. RREQ を受信したノードが宛先ノード，あるいは宛先ノードへの新しい経路エントリをもつノードである場合，経路応答メッセージ RREP を生成し，送信元ノードへユニキャストで送信する．
4. RREP は，RREQ 転送時に生成された RREQ 転送元ノード情報を用いて，送信元ノードまで返送される．
5. 手順 1〜4 により，送信元ノードと宛先ノード間に双方向通信経路が構築される．送信元ノードが複数の RREP を受信した場合は，宛先シーケンス番号の最も大きい RREP を経路として採用する．宛先シーケンス番号が同一の場合は，ホップ数が最小の RREP を採用する．

図 1 に AODV のパケットフォーマットを示す．図 1 において，Pkt Type はパケット種別を示し，RREQ の場合は 1，RREP の場合は 2 となる．Hop Count は送信元ノードからホップ数を示す．RREQ の Destination IP Address，Destination Sequence，Source IP Address，Source Sequence Number は，それぞれ宛先 IP アドレス，宛先シーケンス番号，送信元 IP アドレス，送信元シーケンス番号を表す．RREQ ID は，送信元 IP アドレスと組み合わせることで RREQ を特定する識別子としても用いられる．RREP の Destination IP Address，Destination Sequence，Source IP Address は，それぞれ宛先 IP アドレス（RREQ で指定されていたものと同一），宛先シーケンス番号（RREP 生成ノードによって適宜更新される），送信元 IP アドレス（RREQ で指定されていたものと同一）を表す．Life time は，RREP によって構築される経路の生存時間を表す．

Pkt Type	Reseved	Hop Count
RREQ ID		
Destination IP Address		
Destination Sequence Number		
Source IP Address		
Source Sequence Number		

(a) RREQ

Pkt Type	Reseved	Hop Count
Destination IP Address		
Destination Sequence Number		
Source IP Address		
Life time		

(a) RREP

図 1: AODV パケットフォーマット

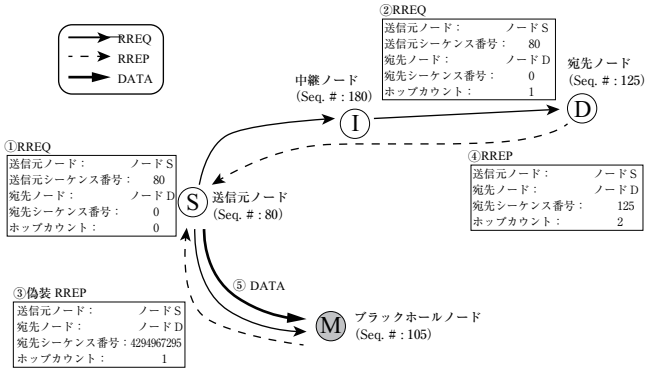

図 2: ブラックホール攻撃

4. ブラックホール攻撃

ブラックホール攻撃とは，ブラックホールノードが宛先ノードあるいは中継ノードになりすまし，送信元ノードが送信したデータを不正に受信し廃棄する攻撃である．ブラックホールノードが，RREQ を受信すると，巨大な値の宛先シーケンス番号と小さな値のホップカウントを持つ偽造 RREP を生成し，それを送信元ノードへ返送する．送信元ノードは，宛先シーケンス番号で経路の新しさを判断するため，ブラックホールノードへ至る経路を最新経路と誤認し，その経路を用いてデータパケットを送信してしまう．図 2 にブラックホール攻撃の例を示す．図 2 において，ノード S を送信元ノード，ノード D を宛先ノード，ノード M がブラックホールノードとする．送信元ノードが送信した RREQ（①，②）は，宛先ノードとブラックホールノード双方が受信する．宛先ノードは自身のシーケンス番号を記載した RREP を生成し送信元ノードへ返送する（④）．一方，ブラックホールノードは，大きな値の宛先シーケンス番号を記載した偽造 RREP を送信元ノードへ返送する（③）．送信元ノードは，宛先ノードが送信した正常な RREP とブラックホールノードが送信し

た偽造 RREP を受信するが，宛先シーケンス番号の大きい偽造 RREP を最新経路だと判断し，ブラックホールノードへ向けてデータパケットを送信する（⑤）．ブラックホールノードは受信したデータパケットの転送は行わないため，パケット到達率やスループットが低下し，さらに宛先ノードの上位層で再送制御が行われると制御パケットが発生しネットワーク全体の性能に悪影響を与える．

5. 提案手法

AODV 型ルーチングプロトコルに対するブラックホール攻撃では，ブラックホールノードは，宛先シーケンス番号を大きな値に設定した偽造 RREP を送信する．このため，閾値を用いて宛先シーケンス番号が不自然な値かどうかを判定し，ブラックホールノードを検出する手法が提案されている [10, 8, 9]．閾値を用いる手法では，高いブラックホールノード検出率と低い誤認率を実現する適切な閾値を算出することが重要な技術課題となる．そこで本研究では，ネットワーク内で通信を頻繁に行っているアクティブなノード数および経過時間を元に動的に閾値を計算し，ブラックホールノードを判定する手法を提案する．また，ブラックホールノードと誤判定された正常ノードをブラックリストから削除するため，一定期間ごとにブラックホールノードに対してダミー RREQ を用いた再判定を行う．提案手法は，閾値判定とダミー RREQ による判定の両者を併用することで，ブラックホールノード検出率の向上と誤認率の低減を目指している．

5.1. ブラックリストの作成

各ノードは，隣接端末から RREQ および RREP を受信した場合に，その送信元をグレーリストへ登録する．グレーリストのエントリは，1) ノードアドレス，2)RREQ フラグ，3)RREP フラグ，4) 生存時間で構成される．ノードアドレスは，RREP/RREQ の送信元アドレスを示し，RREQ フラグ，RREP フラグは，エントリ生成時に受信した制御パケットを示しており，例えば，RREQ 受信時にエントリを生成した場合は RREQ フラグに 1 をセットする．生存時間は，エントリの寿命を表しており，エントリ追加後に生存時間が満了すると，グレーリストから削除される．

RREP を受信した場合には，続けて，RREP 送信元ノードがブラックリストに登録されているかどうかを確認する．ブラックリストのエントリは，1) ノードアドレス，2) 生存時間で構成される．ブラックリストに登録されている場合は，RREQ は廃棄する．登録されていない場合，RREP の宛先シーケンス番号 DS を確認し，判定閾値 TH より大きい場合はブラックホールノードと認定しブラックリストに登録する．判定閾値 TH より小さい場合は，正常ノードとみなしブラックホール判定手順を終了し，通常の処理を行う．図 3 にブラックホールノード検出手順のフローチャートを示す．

5.2. 判定閾値

提案手法では，アクティブなノード数および経過時間を用いてブラックホールノード判定閾値 TH を動的に計算する．TH は，以下の式によって求める．

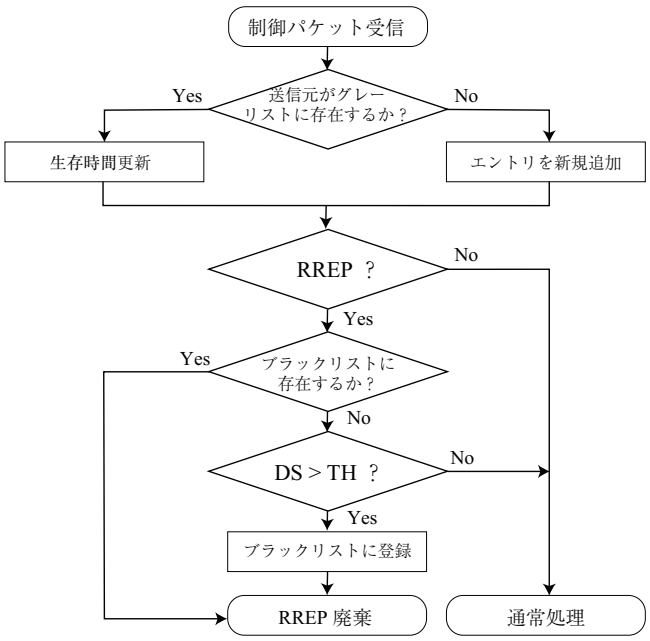

図 3: ブラックホールノード検出手順フローチャート

$$TH = (\alpha N + \beta)t + DS_{known} \quad (1)$$

ここで，α, β は調整用の係数で正の定数とする．また，N はネットワーク内のアクティブなノード数を表し，本手法ではグレーリストのエントリ数を用いる ‡．DS_{known} は，本判定を行うノードが保持している宛先ノード（RREP の Destination IP address）のシーケンス番号（$\neq DS$）を表している．宛先ノードのシーケンス番号を保持していない場合は，$DS_{known} = 0$ とする．t は，DS_{known} を取得した時刻（前回，宛先ノードに関する RREP/RREQ を処理した時刻）からの経過時間を表し，$DS_{known} = 0$ の場合は，本判定ノードの経路制御プトロコル起動時刻からの経過時間を用いる．

5.3. ダミー RREQ を用いた再判定

提案手法では，誤ってブラックホールノードに判定されたノードが永続的にブラックホールノードとして排除されることを防ぐため，ブラックリストの各エントリは生存時間を持つ．生存時間が満了すると，ブラックホールノードの再判定処理を行い，再判定によってブラックリストから削除するか，生存時間を再設定するかを決定する．各ノードは，自身が保持するブラックリストのなかで生存時間満了エントリが発生するとダミー RREQ を生成し送信する．ダミー RREQ の宛先として，ネットワークに存在しないアドレスからランダムに選ばれたものを設定する．ネットワークに存在しないアドレス宛のダミー RREQ に対して RREP で応答するノードはブラックホールノードだと考えられる．したがって，RREP を受信した場合は RREP 送信

‡別プロトコル/サービスによって，より正確なネットワーク内のアクティブなノード数を取得可能な場合は，それを利用できる．

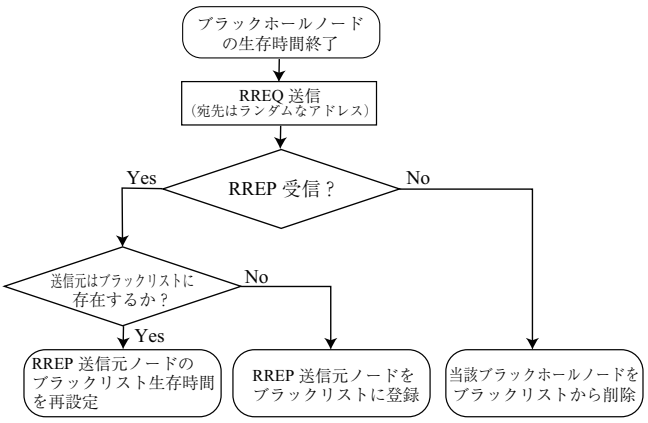

図 4: ブラックホールノード再判定手順フローチャート

元ノードがブラックリストに登録されているかどうかを確認し，登録されていれば生存時間を再設定し，登録されていなければ新たにブラックホールノードとして登録する．図 4 にブラックホールノード再判定手順のフローチャートを示す．

6. シミュレーションによる性能評価

提案方式の有効性を検証するため，ネットワークシミュレータ ns2[11] を用いて性能評価を行う．

6.1. シミュレーションモデル

シミュレーション時間は 200 秒とし，試行回数は 20 回である．ブラックホールノードは，受信したすべての RREQ に対して偽造 RREP で応答するものとし，偽造 RREP の宛先シーケンス番号には正しい宛先シーケンス番号を 1.5 倍した値を使用する．その他シミュレーション諸元を表 1 に示す．比較対象として，AODV(攻撃無/有)，SRD-AODV[10] を用いた．評価指標は以下のものを用いた．

1) ブラックホールノード検出率 R_d

ブラックホール攻撃発生時に，攻撃を検知しブラックホールノードをブラックリストに登録できた割合であり，以下の式で表される．

$$R_d = \frac{N_{black}}{N_{fakeRREP}} * 100 \tag{2}$$

ここで，$N_{fakeRREP}$ は，正常ノードが受信したブラックホールノードから送信された RREP の総数を表し，N_{black} は，ブラックリストの総エントリ数から正常ノードの誤認エントリを除いた値である．

2) ブラックホールノード誤認率 R_f

正常ノードが送信した RREP をブラックホールノードからのものと誤認して廃棄した割合であり，以下の式で表される．

$$R_f = \frac{N_{discard}}{N_{RREP}} * 100 \tag{3}$$

ここで，N_{RREP} は，正常ノードが受信した RREP（ダミー RREP を除く）の総数を表し，$N_{discard}$ は，誤って廃棄された正常ノードからの RREP の総数である．

3) スループット Throughput

宛先ノードのが 1 秒間に受信したデータ量 (bit) であり，以下の式で表される．

$$\text{Throughput} = \frac{PktSize * 8 * N_{recv}}{T} \tag{4}$$

ここで，$PktSize$ はデータパケットサイズ (byte)，N_{recv} は宛先ノードが受信したデータパケット数，T は送信元ノードが最初の RREP を受信してからシミュレーション終了までの時間を表す．

4) パケット到達率 PDR

送信元ノードが送信したデータパケット数に対する宛先ノードで受信されたデータパケット数の割合であり，以下の式で表される．

$$PDR = \frac{N_{recv}}{N_{sent}} * 100 \tag{5}$$

ここで，N_{sent} は，送信元ノードが送信したデータパケット数を表す．

表 1: シミュレーション主要諸元

シミュレータ	NS-2（NS-2.35）
シミュレーション時間	200 秒
ノード数	10, 20, 30, 40, 50, 60, 70, 80, 90, 100
ノードの移動速度	1 〜 5 m/s
フィールドサイズ	800 × 800 m
移動モデル	Random Waypoint
トランスポートプロトコル	UDP
通信タイプ	CBR
ブラックホールノード数	5
閾値調整係数 α, β	$\alpha = 0.002, \beta = 0.1$
ブラックリスト生存時間	30 秒

6.2. シミュレーション結果

図 5 は，ノード数に対するブラックホールノード検出率の変化を示している．提案手法は，すべてのノード数において検出率 100 %を実現している．一方，SRD-AODV は，ノード数の増加にともなって検出率が低下している．提案手法では，動的な判定閾値による偽造 RREP の判別と，ダミー RREQ を用いたブラックホールノード判定が十分に機能したためである．SRD-AODV では，閾値はノード数から決定される固定値であるため，宛先シーケンス番号が小さい状況下（シミュレーション開始後一定期間）では，偽造 RREP の宛先シーケンス番号も小さい値となりブラックホール攻撃を検出できない．しかし，ノード数が増加すると宛先シーケンス番号の増加ペースも高まるため，ノード数の増加に伴って検出率は向上している．

図 6 は，ノード数に対するブラックホールノード誤認率の変化を示している．SRD-AODV の誤認率は非常に小さく，5 %以下であった．一方，提案手法では，

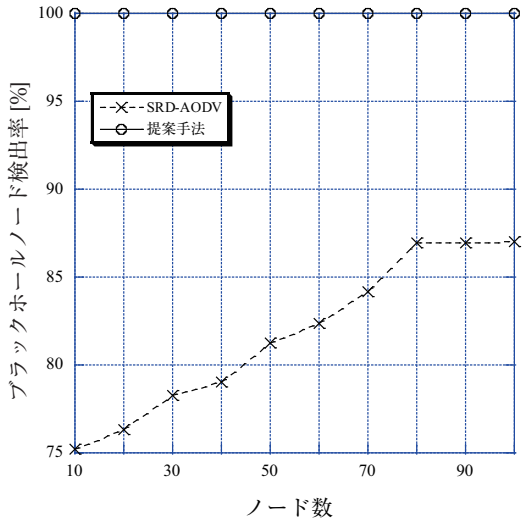

図 5: ノード数に対するブラックホールノード検出率の変化

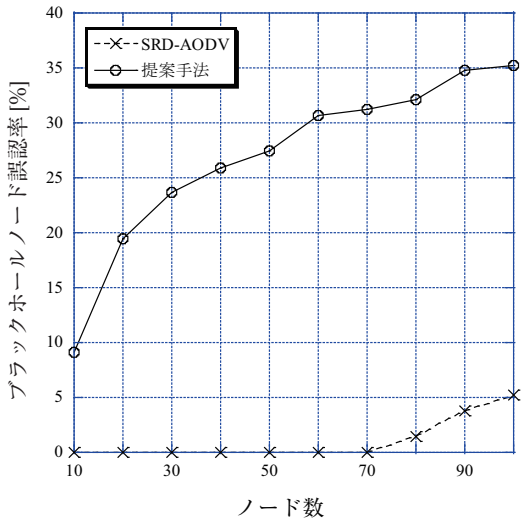

図 6: ノード数に対するブラックホールノード誤認率の変化

ノード数の増加にともなって誤認率が悪化している．提案手法では式 (1) を用いて動的に判定閾値を設定しているが，ノード数が多くシーケンス番号が増加しやすい環境では，正しい宛先シーケンス番号が判定閾値より大きくなるケースが生じ，正常ノードをブラックホールノードと誤認してしまう．しかし，提案手法はダミー RREQ を用いた再判定を行うことで，誤認した正常ノードをブラックリストから削除しており，シミュレーション終了時にはすべての誤認ノードをブラックリストから削除できていた．

図 7 は，ノード数に対するスループットの変化を示している．図中の AODV(攻撃無) は，ブラックホールノードが 0 の場合の結果であり性能目標値である．図 7 より，AODV(攻撃無)，提案手法，SRD-AODV，AODV(攻撃有) の順に性能が低下している．AODV(攻撃有) は，ブラックホール攻撃によって，ほとんどのデータパケットが宛先ノードに届かない．一方，提案方式と SRD-AODV は，ブラックホールノードを検知しブラックホールノードを排除した経路を用いることで一定のスループットは達成できている．提案手法は，ブラックホールノード再判定時に送信するダミー RREQ の負荷によって，データパケットとの衝突やロスを招き，スループットが AODV(攻撃無) よりも低下している．SRD-AODV は，シミュレーション開始後の一定期間は，ブラックホールノードを検出できないため，この期間中の悪影響がスループットを下げる要因となっている．AODV(攻撃無)，提案手法および SRD-AODV は共通して，ノード数が少ない場合にスループットが低い．この理由は，ノード数が少ない場合には移動による経路切断が生じやすく，経路再構築遅延が増加しているためである．

図 8 は，ノード数に対するパケット到達率の変化を示している．スループットの場合と同様に，AODV(攻撃無)，提案手法，SRD-AODV，AODV(攻撃有) の順に性能が低下している．AODV(攻撃無)，提案手法および SRD-AODV いずれも，ノード数の増加に伴ってパケット到達率が増加している．この理由は，ノード数が少ない場合には移動による経路切断が生じやすく，切断によるパケットロスが生じているためである．

7. むすび

本論文では，アドホックネットワークにおけるブラックホール攻撃に対し，ノード数や経過時間などのネットワークから取得可能な情報に基づいて動的に閾値を設定しブラックホールノードを検出する手法を提案した．提案手法は，ダミー RREQ を用いたブラックホールノード再判定を行うことで，ブラックホールノードと誤認した正常ノードをアドホックネットワークへ復帰させることができる．提案手法の有効性を確認するためシミュレーション評価を行い，提案手法が既存手法と比較して，ブラックホール検出率，スループット，パケット到達率の点で性能が向上することを明らかにした．今後の課題としては，提案手法の誤認率の改善が挙げられる．誤認率の改善は適切な閾値設定により実現できるため，判定閾値算出式で用いた調整係数を様々なネットワーク環境において最適化する手法を検討必要がある．

謝辞

本研究は JSPS 科研費 26289122, 15K00141 の助成を受けたものである．

参考文献

[1] F. -H. Tseng, L. -D. Chou, and H. -C. Chao, “A survey of black hole attacks in wireless mobile ad hoc networks,” *Human-centric Computing and Information Science*, vol.1, no. 1, pp.1-16, Dec. 2011.

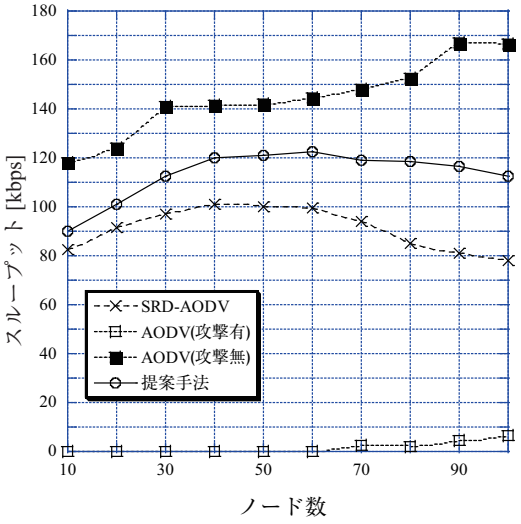

図 7: ノード数に対するスループットの変化

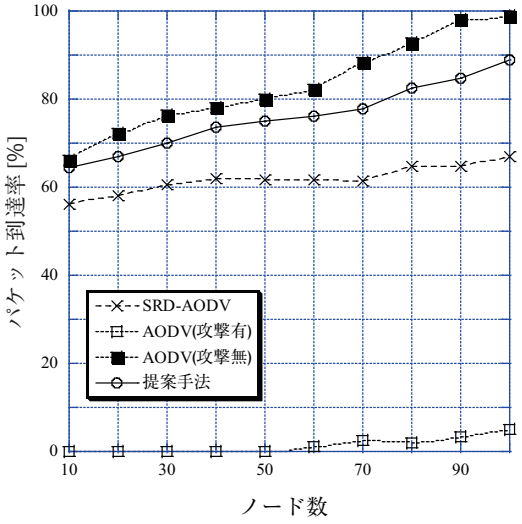

図 8: ノード数に対するパケット到達率の変化

[2] A. Sherif, M. Elsabrouty, and A. Shoukry, “A Novel Taxonomy of Black-Hole Attack Detection Techniques in Mobile Ad-hoc Network (MANET),” In proc. of *IEEE International Conference on Computational Science and Engineering*, pp. 346-352, Dec. 2013.

[3] C. Perkins, E. Belding-Royer, and S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing,” RFC3561, https://www.ietf.org/rfc/rfc3561.txt.

[4] L. Tamilselvan, and V. Sankaranarayanan, “Prevention of blackhole attack in MANET,”In proc. of *IEEE International Conference on Wireless Broadband and Ultra Wideband Communications*, p.21, Aug. 2007.

[5] D. Kshirsagar, and A. Patil, “Detecting and Overcoming Blackhole Attack in Aodv Protocol,” In proc. of *IEEE International Conference on Computing, Communications and Networking Technologies*, pp.1-5, July 2013.

[6] S. Jain, and A. Khunteta, “Detecting and overcoming blackhole attack in mobile Adhoc Network ,” In proc. of *IEEE International Conference on Green Computing and Internet of Things*, pp.225-229, Oct. 2015.

[7] S. Kurosawa, H. Nakayama, N. Kato, and A. Jamalipour, “Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method,” *International Journal of Network Security*, vol.5, no.3, pp.338-346, Nov. 2007.

[8] 佐條 研, 三好 匠, “アドホックネットワークにおけるブラックホール攻撃防御法,” 電子情報通信学会技術研究報告, CQ, コミュニケーションクオリティ 107(312), pp.21-24, 2007-11-08.

[9] 佐條 研, 三好 匠, “適応型ブラックリストを用いたブラックホール攻撃の防御法,” 電子情報通信学会技術研究報告, NS, ネットワークシステム 107(524), pp.365-368, 2008-02-28.

[10] S. Tan, and K. Kim,“Secure Route Discovery for Preventing Black Hole Attacks on AODV-Based MANETs,” In proc. of *IEEE International Conference on on High Performance Computing and Communications and IEEE International Conference on Embedded and Ubiquitous Computing*, pp.1159-1164, Nov. 2013.

[11] DARPA, The Network Simulator - ns-2 (online), available from (http://www.isi.edu/nsnam/ns/) (accessed 2016-04-10).