社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2006－MBL－39 (7)
2006－ITS－27 (7)
2006／11／16

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する防御法の提案と実装・評価

森 郁海† 横山 信†† 高木 剛† 山崎 憲一††† 高橋 修†

†公立はこだて未来大学 システム情報科学部 〒041-8655 北海道函館市亀田中野町 116-2

††公立はこだて未来大学大学院 システム情報科学研究科 〒041-8655 北海道函館市亀田中野町 116-2

†††NTT ドコモ 総合研究所 〒239-8536 神奈川県横須賀市光の丘 3-5

あらまし モバイルアドホックネットワークにおける脅威としてブラックホール攻撃が注目されている。ブラックホール攻撃ノード(以下ブラックホールノード)は、始点ノードの ROUTE REQUEST(RREQ)に対して自身のネクストホップに目的ノードが存在するかのように振る舞い偽装した ROUTE REPLY(RREP)を始点ノードにユニキャストする。これによってブラックホールノードは、始点ノードとの双方向経路を作成し、始点ノードから送信されるパケットを得てしまうというものである。このブラックホール攻撃を防ぐために、ブラックホールノードの検出と防御が必要となる。従来手法では、始点ノードが偽装された RREP を判別するため経路上のノードは経路表に誤ったエントリを登録することによる 2 次的な被害を及ぼしかねない。本稿ではブラックリスト方式を用いブラックホールノードの隣接ノードが偽装 RREP を検出、破棄することで被害を最小限にとどめる検出および防御方式を提案する。シミュレーションによる評価を行い提案手法が有効であることを示す。

キーワード モバイルアドホックネットワーク,ブラックホール攻撃,AODV,ブラックリスト

Proposal of Defense Method, its implementation and Evaluation against Black hole Attack in AODV-based Mobile Ad Hoc Network

Ikumi Mori† Shin Yokoyama†† Tsuyoshi Takagi† Kenichi Yamazaki††† Osamu Takahashi†

† Systems Information Science, Future University–Hakodate 116-2 Kamedanakano-cho Hakodate Hokkaido, Japan

†† Systems Information Science Graduate course, The graduate school of Future University–Hakodate 116-2 Kamedanakano-cho Hakodate Hokkaido, Japan

††† NTT DoCoMo, Inc. Research Laboratories 3-5 Hikarinooka Yokosuka Kanagawa, Japan

Abstract Attention is currently focused on Black hole Attack in Mobile Ad Hoc Network. Black hole attack node acts as if it has the route of destination node, and sends a fake ROUTE REPLY (RREP) to source node against its ROUTE REQUEST (RREQ). This will be made a routing table to include a black hole node, and lose TCP packet at the black hole node. It is necessary that detecting black hole nodes and its defense method. Current defense method may cause an unfavorable effect on relay node because source node determines right RREPs or not. In this paper, we propose new defense method using Black List and neighbor nodes of black hole node determine right RREPs. The simulation results show the effectiveness of proposed defense method.

Keyword Mobile Ad Hoc Network, Black hole Attack, AODV, Black List

1. はじめに

近年、インターネットを始めとするネットワークの利用は急速に拡大し、ビジネス・政治・娯楽などあらゆるものがネットワークに依存している。ネットワークの普及につれ、企業サイドはコスト・接続性に優れる無線ネットワークを積極的に導入し始めている。この背景には、ノート PC や携帯電話、PDA に代表される接続場所を固定しないモバイルノードの増加がある。また、一方ではアクセスポイントを用いない(アドホック)通信方式の研究が積極的に行われ、近い将来実用的に使用される事が予想される。それ故に、無線ネットワーク特有の問題は不可避であると考えられる。例えば、電波を利用することによって電波範囲内のノード全体が情報を受信できてしまう問題、それに起因する盗聴の助長、情報漏えいなどが挙げられる。これらの問題を踏まえ、近い未来におけるネットワーク攻撃の

脅威を回避する目的で、移動ノードに強いオンデマンド型アドホックルーティングプロトコルであるAODV[1]に着目しその攻撃法、防御法の評価を行う。攻撃法としてブラックホール攻撃を取り上げる。ブラックホール攻撃は、始点(送信元)ノードからのROUTE REQUEST(RREQ)に対して攻撃ノードはネクストホップに目的(宛先)ノードが存在するかのように偽装したROUTE REPLY(RREP)を始点ノードへユニキャストすることにより、双方向経路を形成させデータトラヒックを攻撃ノードへ集中させ、それらを破棄することによって正常な通信を行わせないものである。

ブラックホールノードを検出する方法は、いくつか提案されている[2][3][4]。しかし、いずれも検出法および防御法の理論のみで実装・評価はなされていない[2][3]か、検出のみで防御法の提案はなされておらず[4]、検出と防御法式とその実装・評価を行ったものはない。

本稿では、AODV ルーティングの機能が実装されている AODV-UU[5]を用いブラックホール攻撃及び提案防御法の実装を行う。そしてネットワークシミュレータ NS-2[6]を使用し、攻撃法及び防御法の評価を行う。

2. 関連研究

ブラックホール攻撃を検出する方法として以下の方法が提案されている。

2.1 ブラックホール攻撃の評価と対策[2]

岡田[2]らは、ブラックホール攻撃を実装しその影響をシミュレーションによって評価している。結果としては、ブラックホールノードが少数でも十分な効果があるとされている。検出方法としては、1)被攻撃者がRREP の数を監視する 2)頻繁にリンクブレイクを起こすノードを監視する 3)目的ノードではないノードがRREQ を転送しているかを監視する の三つからなり、これら条件を全て満たすものをブラックホールノードとしている。検出後、ブラックリストにノード情報を登録し、配布する方式による防御法を提案している。但し、実際に評価は行われておらず提案のみである。

2.2 ブラックホールノードを取り囲む対策法の提案[3]

山内ら[3]は、ブラックホールノードを検出後そのノードを取り囲むようにグループを形成し、以後そのノードにRREQ が届かないようにする防御法を提案している。しかし、対策法の提案のみで評価はなされていない。

2.3 自動学習を用いたブラックホールノードの検出[4]

黒澤ら[4]は、ブラックホールノードの宛先シーケンス番号の増加量などを利用した 3 次元特徴量ベクトルの閾値を用いた自動学習により異常検出する防御法を提案している。この方式では、学習データが 600 秒毎に更新されるため適応性が高く、従来の静的な検出方法と比較して検出率がよく誤認率が低い。しかし、攻撃ノードまでの経路形成を防御するものではなく始点ノードが RREP を破棄するという方法を用いているため経路上のノードが誤った経路表を作成してしまう可能性がある。

3. ブラックホール攻撃の定義

3.1 前提条件

AODV ルーティングプロトコルは RFC3561 に準拠した AODV-UU を用いるが、その中でも使用が任意とされているものについて、以下のように定めるものとする。

1) hello メッセージを使用しない

2) その他 AODV-UU の NS-2 上のデフォルト動作に準拠する

1)は、モバイルノードを対象とするためバッテリ消費の観点から使用しないのが望ましいとしたからである。また hello メッセージはテーブル駆動型の要素を含んでおり、純粋なオンデマンド型としての AODV を評価する上では必要ないと判断したためである。その他、AODV ヘッダへのエクステンションなども全て用いないことにする。

3.2 ブラックホールノードの動作

ブラックホール攻撃の実現方法はいくつか存在する[2][4]。代表的なものは、ブラックホールノードがネクストホップに目的ノードが存在するかのように装う方法[2]とブラックホールノード自身が目的ノードに偽装する方法[4]である。前者は、「目的ノードへの十分新しい経路を持つノードは、RREP を作成始点ノードへユニキャストできる」という AODV の機能の一つを悪用したものである。後者は、いわゆる「なりすまし」でアドホックネットワークでの「ノードの唯一性」の検証が困難な点を利用したものである。本稿では、セキュリティホールに成り得る AODV の機能の脆弱性を利用した攻撃が行われたと想定し、前者の方法を用いてブラックホール攻撃の実装を行う。

ブラックホールノードは、目的ノードまでの経路を自身のネクストホップにあると詐称し受信した RREQ に対し偽装した RREP を始点ノードへユニキャストすることにより双方向経路を作成させデータパケットを不正に取得する攻撃を行う。ブラックホールノードは、RREQ に対し即時 RREP を作成するがこのとき宛先シーケンス番号を改変しない。通常の RREP と同じように処理を行うものとする。具体的には RREQ のシーケンス番号+1 と自身のシーケンス番号を比較し大きい方を RREP の宛先シーケンス番号に載せる。また、送信元ノードは受信した RREP に対し即時経路作成を行うものとする。つまりより早く到着した RREP に対し

て通信を行う。複数の RREP が同時に到着した場合は宛先シーケンス番号の大きい方と通信を行う。この前提を元に以下にブラックホールノードの定義を示す(図 1)。

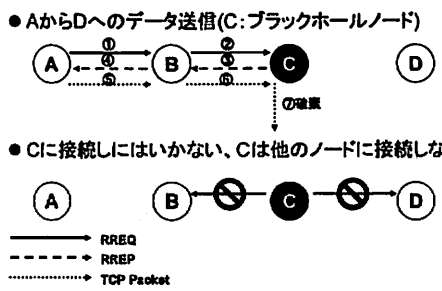

図1 ブラックホール攻撃の定義

ブラックホールノードは、自らを送信元とする通常の通信要求を出さない。つまり、RREQ の送信元、RREP の宛先がブラックホールノードのアドレスと指定されることはないものとする。その理由は、ブラックホールノードは積極的に自身の身元を明らかになることは極力避ける行動をとるためである。ブラックホールノードを宛先とする通常通信はないものとする。つまりどんな RREQ も宛先アドレスにブラックホールノードのアドレスが入ることはない。これは通常ユーザは身元不明な IP を持つノードに対しては不用意に通信を行ってはならないことを意味する。全ての RREQ に対して即時に RREP を作成し送信する。RREP を偽装し、送信元が目的ノードであるかのようにする。このパケットは目的ノードまでの十分新しい経路を持つノードが返す RREP と同様なものである。経路確立後、TCP パケットが届くとそのパケットを破棄する。その際通常 ROUTE ERROR(RERR) を作成し送信するが、この処理を行わない。経路表内に宛先までの正規の経路が存在したとしても、TCP パケットをフォワードしない。通信が 0 ホップで完了する(始点ノードの隣接に目的ノードが存在する)場合は攻撃できないことに注意する。

4. 検出及び防御方式の提案

4.1 基本方針

ブラックホールノードの特性を利用し、各ノードは受信するパケットを監視して条件によるフィルタリングを行うことで検出及び防御を実行する。その条件の達成状況を保存するためにブラックリスト方式を用いる。防御法のコンセプトは、「ブラックホールノードの隣接ノードがブラックホールノードからの RREP を破棄し、双方向経路を作成させない」である。

始点ノードのみが RREP をフィルタリングする方式だと、始点ノードとブラックホールノードまでの双方向経路が作成されてしまい、経路上にいるノードが宛先に偽装された RREP の送信元宛を指定してしまうと誤った経路が使用される可能性が生じる。これを防ぐ為に、双方向経路を完全に形成させない手法が必要となる。そのための手段として、各中継ノードに防御機構を取り入れることで早期に攻撃の検出及び偽装パケットの破棄を行うという方法を用いることとした。

4.2 ブラックリストの構成

ブラックリストのエントリの詳細を以下に示す(表 1)。ブラックリストに TTL が設けられているが、これは正常ノードを誤ってブラックホールノードと判断してしまった場合そのエントリを削除しなければならないためである。加えて、ブラックリストはそのエントリがブラックホールノードでなくても隣接ノードの状態を常に記録している。そのため、定期的に無通信状態のノードに関してはエントリを削除しブラックリストのエントリが無尽蔵に増加することを防がなくてはならない。エントリされているノードが RREQ あるいは RREP を送信するたびに TTL をデフォルト値に戻すことによって、無通信状態のノードを判断する。つまり、TTL 時間内に何も RREQ,RREP を送信しなかったノードは無通信状態と判断されエントリから削除される。この TTL はブラックホールノードの検出率に影響があると考えられるためシミュレーション時にはパラメータの一つとして与える。しかし、誤認されたノードが通信を試みる場合 RREQ をブロードキャストすれば自動的にブラックホールノードの条件を満たさなくなるため通信に影響はない。

表1 ブラックリストのエントリ

エントリ	説明
ブラックホールノード候補の IP アドレス	隣接ノードからの RREQ,RREP 受信時に登録する。
isRREQBroadcast フラグ	候補ノードが RREQ をブロードキャストしたらフラグを立てる。
isRREP フラグ	候補ノード宛に RREP がユニキャストされた場合にフラグを立てる。
TTL	このエントリの生存時間である。

4.3 検出及び防御手順

このブラックリストを用い、以下の手順で検出、防御を行う。

1) 隣接ノードからの受信パケットから IP レベルの送信元アドレスを抽出、ブラックリストに登録する。
2) 隣接ノードからの受信パケットを監視し、ブラックリストの各フラグの成立条件と一致した時対応したフラグを立てる。
3) RREP を受信した時、IP レベルの送信元 IP アドレス

と AODV パケットヘッダの送信元を比較する。

4a) 一致しなかった場合は、目的ノードまでの経路を持っており、RREP を短縮してユニキャストしたか攻撃を受けているかのどちらかであるのでブラックリストを見る。

4b) 一致した時、その IP アドレスを持つノードはブラックホールノードではない。検出手順を終了し、通常の処理を行う。

5) ブラックリストから対象の IP アドレスを持つエントリを検索する。

6a) ブラックリストにエントリが存在した場合、そのエントリの中のフラグを見る。

6b) ブラックリストにエントリが存在しない場合、初めて送信したパケットが RREP ということになる。RREQ などを送信せず経路表に目的ノードまでの経路が作成される可能性は低い。よって、ブラックホールノードとみなしブラックリストにこのノードを追加する。そして手順 8)へ移る。

7a) ブラックリストのエントリ内の各フラグが全て立っていない時、その IP アドレスを持つノードはブラックホールノードである。

7b) ブラックリストのエントリ内の各フラグが一つでも立っている時、ブラックホールノードではない。検出手順を終了し、通常の処理を行う。

8) RREP を破棄する。

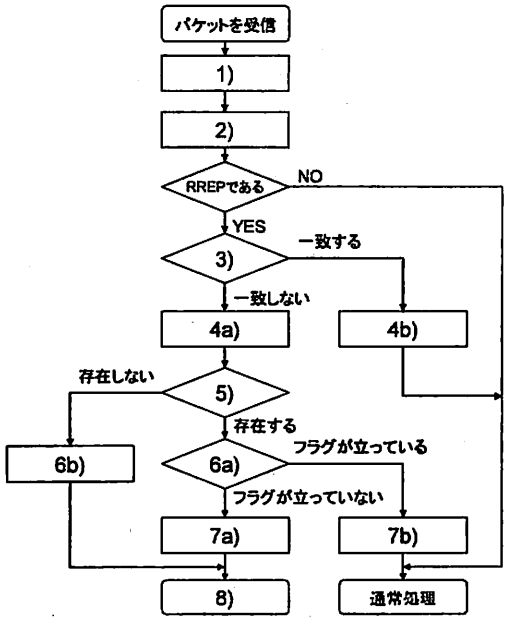

図2 検出及び防御手順のフローチャート

図 2 に検出及び防御手順のフローチャートを示す。図 3 に防御方式の動作例を示す。

但し、ブラックホールノードと誤認された場合、そのノードからの正しい RREP が破棄されてしまい異なる経路を検索するが、そのノードが通信を行おうと RREQ をブロードキャストするか何もしないでブラックリストのエントリの TTL が切れエントリから削除されることで再び上記の処理が行われる。

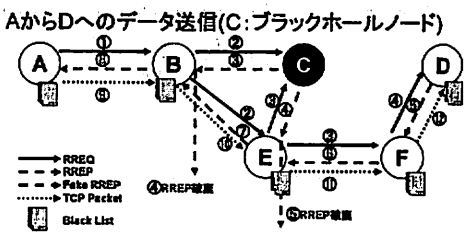

図3 防御方式の動作例

5. 検出及び防御方式の評価

ブラックホールノードの増加によって攻撃効率が大きく変化すると考えられる。そこで、正常時と比較しスループット、接続率がどのように変化するかをシミュレーションによって評価する。

5.1 シミュレーション条件

トポロジは 1000m×1000m とし、シミュレーション時間は 100 秒とし、無線電波到達範囲は半径約 200m とする。ノード数は正常ノード 100 個とブラックホールノード 0-50(5 刻み)個で変化させるものとする。正常ノードは防御方式を適用/不適用の 2 パターンとする。各ノードにはノード番号を付与する。ノード番号 0～99 が正常ノード、100～149 ブラックホールノードとする。通信環境は、正常ノード 1 つと正常ノード 1 つとの 1 対 1 単方向 TCP 通信とする。データパケットは FTP によりジェネレートする。通信はシミュレーション開始から 0.1 秒後に開始する。通信速度は 2Mbps とする。より自然な通信をシミュレーションするためにコネクションパターンを設ける。コネクションパターンは始点ノード番号-目的ノード番号の対で識別し、0-x(x=4,9,14,19,...,99)と表記する。コネクションパターンを数回分繰り返し、評価にはこの平均を用いる。ブラックホールノードは、ブラックホール攻撃に準拠した動作を行い、防御方式は適用しない。その他、ブラックリストの TTL を 10 秒、50 秒、100 秒と分け、それぞれノードの最大移動速度を移動無し(0km/h)、人間の歩き(2km/h)、早足(7km/h)、車での移動(60km/h)に変化させシミュレートする。ノード配置や速度はノードの移動シナリオのファイルを生成するツールである

setdest を使用する。ノードの移動動作は setdest によるランダムモーションとする。表 2 にシミュレーションパラメータの一覧を示す。

表2 シミュレーションパラメーター覧

トポロジ	1000(m) × 1000(m)
無線電波到達範囲	約 200m(半径)
ノード数	• 正常ノード 100 + ブラックホールノード 0,5,10,15,20,25,30,35,40,45,50 • ノード番号 0～99 正常ノード • 100～149 ブラックホールノード
通信	• 正常ノード 1 つと正常ノード 1 つとの 1 対 1 単方向 TCP 通信 • パケットは FTP によりジェネレート • 通信速度は 2Mbps
コネクションパターン (送信元-宛先)	0-4,0-9,0-14,0-19,0-24,0-29,0-34,0-39,0-44,0-49, 0-54,0-59,0-64,0-69,0-74,0-79,0-84,0-89,0-94,0-99
シミュレーション時間	100 秒
ブラックホールノード	• ブラックホールノードの定義に準じる ブラックリスト機構を用いない
ブラックリストの TTL	0 秒(切れやすい)、50 秒(一般的)、100 秒(長い、切れない)
ノードの動作	• 移動無し(0km/h)、人間の歩き(2km/h)、早足(7km/h)、車での移動(60km/h) • 全てのノードはランダムモーション

5.2 シミュレーション結果

シミュレーション結果からスループット、接続率、検出率、誤認率を算出する。100 秒間に目的(宛先)ノードがどれだけ TCP パケットを受信したかをスループットとし、コネクションパターンで平均を取る。接続率は、100 秒間に一つも TCP パケットを受信できなかった場合のコネクションを接続不可とし、各コネクションパターンで割合を算出する。検出率は、ブラックホール攻撃の成功、失敗に関わらず攻撃を行った回数のうち防御方式を適用したノードがどれだけ検出できたかを割合で算出する。誤認率は、100 秒間処理した RREP のうち正常ノードからの RREP を誤って破棄した割合を算出する。ブラックホールノード数別の平均スループットを図 4 に示す。接続率を図 5 に示す。縦軸は接続可能ノードの割合(%)である。検出率を図 6 に示す。縦軸は接続可能ノードの割合(%)である。誤認率を図 7 に示す。縦軸は誤認率(%)である。

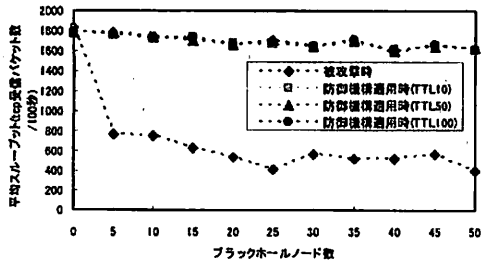

図4 ノード数別スループットの変化

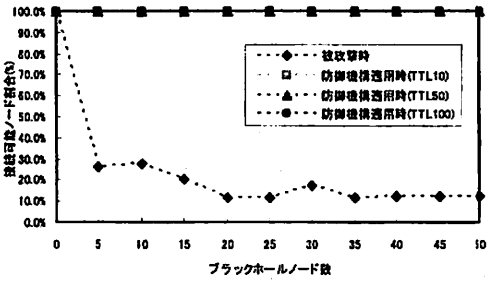

図5 ノード数別接続可能ノードの割合の変化

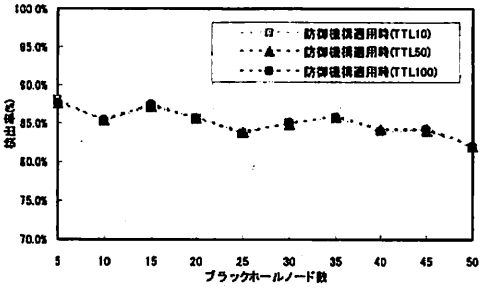

図6 ノード数別検出率の変化

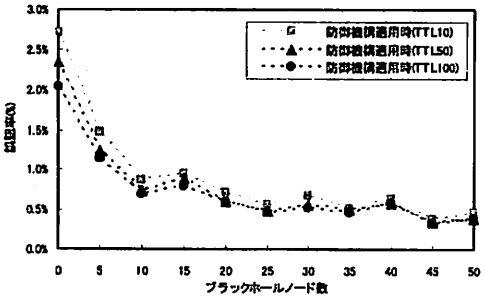

図7 ノード数別誤認率の変化

5.3 考察

図 4 より、被攻撃時ではスループットはブラックホールノード数が少数でもスループットが著しく低下するが、防御方式を適用することによりブラックホールノード数に関わらずほとんどスループットが低下しないことが分かる。被攻撃時にスループットが 0 にならないのは、隣接ノードとの通信には攻撃が成立しないためである。スループットに関しては防御方式のパラメータ TTL を変化に関わらず一定の効果を発揮することが出来る。非常に緩やかに下降しているがこれはプ

ラックホールノード増加によるRREP処理計算コストの増加によるものと考えられる。

図5より、接続率は被攻撃時ではブラックホールノード数が少数でも著しく低下し最終的には約10%になるが、防御方式を適用することによりブラックホールノード数に関わらず100%を維持することが分かる。TTLが10秒でかつブラックホールノード数が50の場合に100%を少しだけ下回るがTTLを十分長く取ることで問題なく効果を発揮できる。

図6より、検出率はブラックホールノード数の増加に伴い緩やかに下降するが80～85%を維持している。実際の通信にはほとんど影響がないレベルと考えられる。この内攻撃が成功しなかった場合も含まれるためスループットや接続率の値とは必ずしも関係があるとは限らない。

図7より、誤認率はブラックホールノード数が少なくTTLが短いほど高いことが分かる。これは、攻撃回数を分母にとっているため攻撃回数が増加するほど誤認したノードの割合が目立たなくなるためであると考えられる。そのことを考慮に入れても0.5%～3%の低確率で起こるので通信にはほとんど影響がない範囲である。誤認が起こる場合でも、誤認されたノードが通信を行おうとすればRREQをブロードキャストするのでブラックリストから除外される。従って、誤認されたノードが通信不能になるという事態は回避できる。

6. 今後の課題

ブラックホールノードの動作を拡張した際にも対応できるような防御機構を提案する必要がある。具体的には、helloメッセージを用いた場合、ブラックホールノードが通信を行う場合である。まず、helloメッセージを用いる場合は隣接ノードを常に把握できるため隣接ノードが目的ノードである場合には攻撃を受けないという利点はあるが、高い確率でRREPが目的ノードの隣接ノードが返すため検出率が低下すると考えられる。加えて、ブラックホールノードが通信を行う場合にはRREQをブロードキャストするため現在の防御機構では防御できない可能性がある。

これらの問題の解決案として現在検討している防御方式を簡単に説明する。TCP通信でのみ有効であるがTCP ACK監視によるブラックホールノードの検出である。TCP通信を行う場合、通常3way-hand-shakeを行う。その最初のパケットであるSYNパケット及びそれに対して応答するSYN ACKパケットに着目しブラックホールノードの検出を行うものである(図8)。

この方式では、必ず最初の一回は攻撃を受けてしまうが、ブラックホールノードが通信を行う場合やhelloメッセージを用いて隣接ノードがRREPをユニキャストしても問題なく検出できるため検討の余地がある。

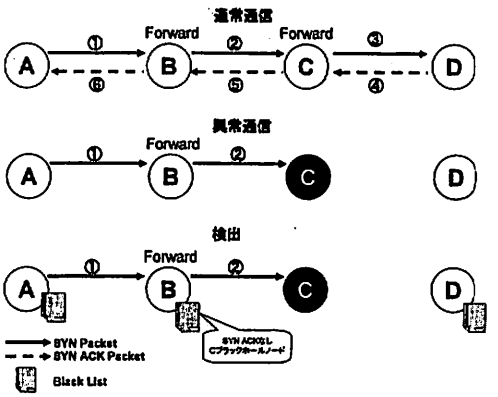

図8 TCP ACK監視による検出方式案

7. まとめ

本稿では、アドホックネットワークにおけるブラックホールノードの動作特性を利用して検出を行いブラックリストを用いることで攻撃を回避するという方式である。この方式の特徴は、始点ノードがブラックホールノードを判断するもしくは攻撃を防ぐのではなく攻撃ノードの隣接ノードが検出し防御する点である。これにより、中継ノードが誤った経路表を作成することを防ぐことができ、二次被害を最小限に止められる。

シミュレーション結果を解析することにより、提案防御法が有効であること示した。

文　献

[1] Ad hoc On-Demand Distance Vector (AODV) Routing, http://www.ietf.org/rfc/rfc3561.txt.

[2] 岡田伊織,横山信,高橋修, "アドホックネットワークにおけるブラックホール攻撃と対策", 情報処理学会全国大会, March 2006.

[3] 内山彰,梅津高朗,安本慶一,東野輝夫, "無線ネットワークにおいて問題が発生している位置範囲を特定するネットワークモニタ方式の提案", 情報処理学会 DICOMO 2005 シンポジウム論文集, pp.329-332, July 2005.

[4] 黒澤怜志,中山英久,加藤寧,Abbas Jamalipour,"自動学習を用いたモバイルアドホックネットワークにおける BLACKHALE ATTACK の検出", 電子情報通信学会技術研究報告 NS2005-174, pp.65-68, March 2006.

[5] AODV-UU, http://core.it.uu.se/adhoc/AodvUUImpl.

[6] Network Simulator version 2(ns-2),http://www.isi.edu/nsnam/ns.