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

2006－MBL－39 (8)
2006－ITS－27 (8)
2006／11／16

AODVにおけるGhost Attackとその防御法

森 拓海† 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の構築に欠かすことのできない技術にルーティングプロトコルがある。これは長年研究されてきたにも関わらず、実用化に至っていない。そのひとつの原因としてセキュリティの問題がある。そこで,さまざまな攻撃を考慮してプロトコル設計を行うことが重要な課題となる。

代表的なアドホック・ルーティング・プロトコルの1つにAODV(Ad-hoc On-demand Distance Vector routing protocol)がある。このプロトコルの特徴は周囲のノードがアクティブであるかを確認するために定期的にHelloメッセージを送信することである。Helloメッセージの送受信を行うことで、通信経路の構築や切断判定を迅速に行うことができる。本論文ではHelloメッセージを偽装し、偽の通信経路を構築させて通信を妨害する攻撃「Ghost Attack」を提案する。また、この攻撃に対する有効な防御法を提案する。これらの手法を計算機シミュレーションにより評価し、この攻撃による脅威を事前に解決することができることを示す。

キーワード アドホック・ルーティング・プロトコル AODV Ghost Attack Helloメッセージ

The Ghost Attack and its Defense Method for AODV

Takumi 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, Future University-Hakodate 116-2 Kameda-Nakano-cho, Hakodate Hokkaido, Japan

††† NTT Docomo, Inc. Research Laboratories 3-5 Hikari-no-oka, Yokosuka, Kanagawa, Japan

Abstract A routing protocol is one of the indispensable technology in order to construct mobile ad hoc networks. Though that has been studied for many years, it isn't used practically, because there are security problems. Then, it is important that routing protocol should take account of security attack from malicious nodes.

One of the representative ad-hoc routing protocol is AODV(Ad-hoc On-demand Distance Vector routing protocol). A characteristic of this protocol is that sending a Hello message regularly to confirm whether neighboring nodes are active or not. By transmitting and receiving a Hello message, that can construct and cut connection route quickly. In this paper, we propose that "Ghost Attack" which construct a false connection route, and interfere end-end data transmission by camouflaging a Hello messege. In addition, We propose effective defense algorithm for this attack. We also evaluate proposed methods by computer simulation and show that it can defense from this attack.

Keyword Ad-hoc Routing Protocol, AODV, Ghost Attack, Hello message

1. はじめに

近年、無線技術が普及しノートPCや小型ゲーム機、携帯電話など様々なモバイル機器に無線LANやBluetoothといったアドホック通信が使用されるようになった。しかし、無線通信自体が従来の有線通信のラストホップとしての役割が中心であり、アドホック通信プロトコルがネットワーク通信の主体となることはなかった。その最も大きな理由の1つとして、実用に耐え得るだけのセキュリティや通信速度を確保したアドホック・ルーティング・プロトコルが存在しなかったことにある。

アドホック・ルーティング・プロトコルには、大きく分けて2種類に分類される。1つは「プロアクティブ型」もうひとつは「リアクティブ型」である。前者はOLSR、TBRPFに代表され、通信経路情報を事前に

計算する方式である。後者は DSR、AODV (Ad-hoc On demand Vector routing) [1][2]に代表され、経路は通信要求があってはじめて計算される。AODV はリアクティブ型に分類されているがプロアクティブ型に用いられている隣接ノード識別のための Hello メッセージを扱えるのでハイブリッド方式として分類することもできる。

本論文では AODV の Hello メッセージに着目し、攻撃に応用した。AODV には RREP の一部として Hello メッセージが存在する。通常は送信元に自 IP アドレス、宛先にブロードキャストアドレス (255.255.255.255) を指定する。このパケットを一定間隔発信することで隣接ノードに自分がアクティブであることを知らせることができる。隣接ノードでは、Hello メッセージを一定間隔で受信することにより、隣接ノードの存在を認識する。Hello メッセージを受信できなくなったとき、その隣接ノードが Down(通信範囲外に出たか、電源が切れた)したと判断する。この機構により、隣接のノードの入れ替わりに柔軟に対応することができる。また、Hello メッセージにより隣接ノードを識別すると同時にルーティング・テーブルを作成するので、より高速なルーティングを実現する。しかしながら、RFC3561[1]には必ずしも使用しなければならないわけではなく、オプションの機能として定義されている。また、無線通信はポータブルデバイスに実装されることが多く、バッテリ節約のため、大量にパケットを送信する Hello メッセージを出さないことも多い。AODV-uu[3]では、上記を踏まえ最適化された Hello メッセージの送信方法がある。これは、ROUTE REQUEST(RREQ)を受信したときに一定時間だけ Hello メッセージを送信するというものである。以上のように AODV では Hello メッセージが各ノードの存在と識別をかねた重要なパケットであるといえる。この Hello メッセージを悪意あるノードが偽装・大量送信する攻撃 Ghost Attack を提案する。偽装された Hello メッセージを受信することで隣接ノードを誤って認識することになる。したがって誤って認識されたノードに宛先ノードが含まれると、誤った経路が形成され、大量のロスト・パケットが発生する。Ghost Attack の効果と Ghost Attack に対する効果的な防御法を計算機シミュレーションにより評価する。

2. 関連研究

本攻撃法は偽装 Hello メッセージを送信することから、「なりすまし攻撃」の側面を持つ。代表的ななりすまし攻撃としては Sybil Attack[4]がある。Sybil Attack は悪意のあるノードが権限のあるノードに扮し、サーバなどにアクセスし情報の盗難・改ざん等の攻撃を行うことを目的としている。攻撃者は単に 1 つのノードに扮するのではなく、任意のノード数に扮することも可能である。

この攻撃に対する解決法として Jhon R. Douceur[4]は「ノードの同一性 (唯一性)」を証明することを挙げている。一般的に公開鍵暗号[5]を用いる PGP などの認証方法により実現する。具体的には CFS cooporative system が提唱する方法がある。この方法では VeriSign のような信頼できる認証局を用いて IP アドレスのハッシュを生成し、そのハッシュに基づき認証を行うものである。

Sybil Attack は、センサネットワークにおける攻撃も研究されている。センサネットワークではすべてのノードはサーバにより管理されているため上記の認証局による認証を行うことで、Sybil Attack を容易に防御することが可能である。しかしながら、アドホックルーティングを用いたアドホックネットワーク環境では、すべてのノードを監視するサーバは存在せず、各ノード間の通信に認証を設けることは現実的には不可能である。

Sybil Attack と本攻撃では決定的な違いが存在する。アドホックネットワークへの攻撃はデータの傍受や漏洩を行う Passive Attack と通信やルーティングを阻害する Active Attack が存在する。本攻撃は Active Attack に分類されるが Sybil Attack は Passive Attack と分類される。

3. Ghost Attack

本提案方式の Ghost Attack は、Hello メッセージを偽装する攻撃である。簡略化した攻撃モデルを図 1 に示す。

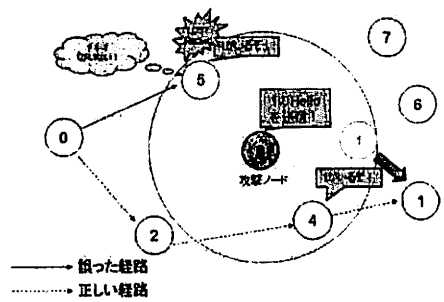

図 1. Ghost Attack モデル

本攻撃では、攻撃ノードが通信可能範囲のノードの Hello メッセージを受信するとそれを模倣し、模倣した Hello メッセージの送信を行う。一度でも攻撃ノードの通信可能範囲に移動すると、以後永続的に Hello メッセージが模倣される。しかし、Hello メッセージの大量送信が攻撃ノードにかける負荷を考慮し、模倣可能な Hello メッセージの数は AODV のルーティング・テーブルのエントリの最大数を上限とした。最大値を超えるノードを認識した場合、最も古くルーティング・テーブルに登録されたノード情報を上書きする。

あるノードが送信する Hello パケットが攻撃ノードに受信された場合、そのノードの Hello メッセージは攻撃ノードにより複製・送信される。攻撃ノードの通信可能範囲にいるノードは攻撃ノードが発信する偽の Hello メッセージにより、ルーティングテーブルに偽の経路情報が登録される。宛先ノードへの最短経路が攻撃ノードまたは攻撃ノードにより通信経路を誤認しているノードより離れている場合、存在しない経路を構築することになり、送信されたデータパケットは必

ず失われる。さらに攻撃ノード同士が相互に通信できる範囲に存在した場合、互いに Hello メッセージの複製を行うため、より多くの Hello メッセージが模倣される。

3.1. 攻撃対象

攻撃ノードが他の隣接するノードの Hello メッセージを受信すると、Hello メッセージの送信元 IP アドレスを攻撃対象リストに登録する。この作業は New Neighbor の場合のみ行われるため、以後同様の Hello メッセージによる 2 重登録が回避される。また一度攻撃ノードの通信可能範囲から外れ Neighbor Down を起こした後、再び通信可能範囲に入った場合は、2 重登録防止機構により、攻撃対象リストへの 2 重登録が回避される。

3.2. Hello メッセージの生成・送信

偽 Hello メッセージの生成は攻撃対象リストに従って行われる。生成される Hello メッセージの送信元情報は攻撃対象リストに記載された IP アドレスとなる。Hello メッセージの生成・送信は 1 秒ごとに攻撃対象リストの全エントリに対し行われる。偽の Hello メッセージを攻撃ノードの隣接ノードが受信し続けることにより、例え経路ノードが通信範囲外に出たとしても Neighbor Down を起こすことなく経路が維持される。

3.3. 存在の隠蔽

攻撃を行うにあたり、攻撃が周囲のノードに感知されないように自分の存在を示す可能性のあるパケットすべてを送信しない。攻撃ノードの存在を示すパケットは自分自身の情報を載せた Hello メッセージ、ROUTE REPLY(RREP)、ROUTE REQUEST(RREQ)である。これらすべてのパケットを送信・処理しないようにする。

4. Ghost Attack に対する防御法

本攻撃に対する防御法の概要を図 2 に示す。

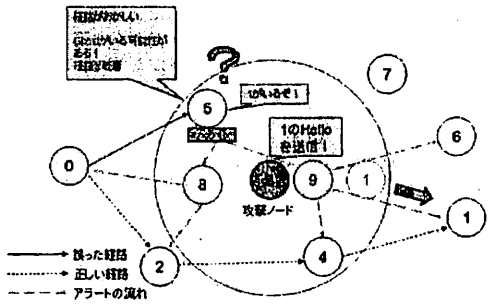

図 2. 防御モデル

本防御法は、Ghost Attack を受けた場合に生じる「通信対象ノードからは Hello メッセージ以外を受信できない」状態を検出する方法である。多くのアプリケーションの通信で用いられる TCP 通信では送信したパケットに対して必ず ACK パケットが返信される。この機能を利用し、ACK が一定時間内に返信されない経路を攻撃経路と判定する。攻撃判定された場合は ACK が返信されなかったノードの Hello メッセージを無視する。また、TCP 通信においてはパケットロストによる再送要求はパケットロストの回数の増加につれて再送間隔が長くなる。そこで、予め周囲のノードに模倣された Hello メッセージの情報を知らせ、攻撃を受けることなく経路を構築する必要がある。この機構は、偽の Hello メッセージの送信元情報を周囲 1 ホップのノードに「アラート」をブロードキャストすることで実現する。

この機構により誤ったルーティングテーブルの構築を完全に防ぐことができるので、Ghost Attack によりデータパケットが失われることを完全に防ぐことができる。しかし最低一度は攻撃を受け、通信経路を再構築するまでの時間がかかる。また ACK の無い UDP 通信には本防御法を適用することはできない。

4.1. 経路リストへの登録

各ノードは自身が送信する TCP パケットに対する ACK パケットが返信されるかを確認するため、TCP パケットの宛先 IP アドレスを経路リストに登録する。経路リストのエントリは、TCP パケットの宛先 IP アドレス、攻撃判定フラグ、TCP・ACK パケット間隔計測タイマー、TTL からなる。TCP パケットの宛先 IP アドレスは TCP パケットの最終宛先 IP アドレスであり、隣接ノードの IP アドレスではない。攻撃判定フラグは攻撃判定された場合に True、安全な経路と判断された場合に False とするフラグである。TCP・ACK パケット間隔計測タイマーは TCP パケットが送信されてから ACK パケットが返信されるまでの間隔を計測するタイマーである。そして TTL がこのエントリの生存時間である。本提案方式では十分に長い時間として 100 秒とする。TCP パケットの送信時に新規に IP アドレスが登録される場合は安全な経路として仮定し、攻撃判定フラグを False とする。また経路リストに登録されたと同時に TCP・ACK パケット間隔計測タイマー、TTL が動作する。

4.2. TCP パケット・ACK パケットの監視

TCP パケットが送信されると、その TCP パケットの宛先 IP アドレスから経路リストのエントリを検索し、TCP・ACK パケット間隔計測タイマーを開始する。送信した TCP パケットに対する ACK パケットを受信すると、TCP・ACK パケット間隔計測タイマーを停止・リセットする。通常 3~5 ホップする経路の場合でも ACK の返信は TCP パケットが送信されてから約 0.1 秒である。したがって、1 秒以内に ACK パケットが返信されなかった時はその経路を不正経路と判断する。不正経路と判断したら攻撃判定フラグを True とし、このエントリの TTL をアップデートする。

4.3. Hello メッセージのフィルタリング

Hello メッセージは 1 秒ごとに受信される。受信するすべての Hello メッセージに対し、経路が安全であるかを確認する。攻撃判定された経路リストの宛先 IP アドレスと一致した Hello メッセージと受信した Hello メッセージの送信元 IP アドレスが一致した場合、その Hello メッセージを処理せずに破棄する。しかし経路リストの宛先 IP アドレスは経路の最終宛先を示しているため、模倣された Hello メッセージが隣接ノード（ネクスト・ホップ）である場合は経路リストから直

接参照した宛先 IP アドレスと一致しない。したがって、ルーティング・テーブルから IP アドレスを検索する必要がある。AODV のルーティング・テーブルには最終宛先 IP アドレスとそれに対応するネクスト・ホップの IP アドレスが記載されている。経路リストの宛先 IP アドレスからネクスト・ホップの IP アドレスを取得し、その IP アドレスと Hello メッセージの送信元 IP アドレスの比較を行う。一致した場合は先ほどと同様に模倣された Hello メッセージと判断し、Hello メッセージを処理せずに破棄する。経路リストの宛先 IP アドレス、またはそのネクスト・ホップ以外の IP アドレスからの Hello メッセージを受信した場合は通常通りの処理を行う。

Hello メッセージを破棄することで、すぐに Neighbor Down が発生し経路の再構築が行われる。このとき、偽の Hello メッセージにより経路が再構築されることが無いので、必ず別の経路が作成される。

4.4. 不正 Hello メッセージの送信元 IP アドレスの周知

攻撃ノードが送信する偽の Hello メッセージは周囲のノードにブロードキャストされているため、個々のノードが随時検出するだけでは次々に他のノードが攻撃を受けてしまうため、経路の再構築が行われない。そこで偽装された経路であると判断された場合、偽装された Hello メッセージの送信元 IP アドレスを「アラート」として周囲 1 ホップ分のノードにブロードキャストする。アラートは ROUTE ERROR(RERR)の一種として実装する。通常の RERR と区別するためのフラグを用意し、そのフラグを True とする。また、不正 Hello メッセージ送信元 IP アドレス、残りホップカウントを記載する。模倣された Hello メッセージの情報を周囲 1 ホップ分のノードにブロードキャストすることにより、確実に攻撃ノードの周囲を迂回する経路を作成する。アラートはなるべく広範囲に周知されるべきだが、1 ホップ以上ブロードキャストさせるとあまりにも多くの Hello メッセージを破棄することになる。本防御機構で破棄される Hello メッセージは本物の Hello メッセージも含まれているため、Hello メッセージを破棄しすぎると本来の Hello メッセージの機能を完全に失うことになる。

4.5. アラート処理

上記の手順で送信されたアラートを受信した場合の処理は 2 つに分けられる。1 つはアラートに記載された IP アドレスが経路リストに登録された場合である。このときは攻撃判定フラグを True とし、そのエントリの TTL をアップデートする。経路リストに存在しない IP アドレスの場合、新規に経路リストに登録後すぐに攻撃判定フラグを True にする。

アラート処理により、攻撃判定フラグが True とされたときは、新たにアラートを生成せず、アラートの残りホップカウントに従い、アラートのフォワードのみを行う。

4.6. 安全な経路

偽装された Hello メッセージにより形成された経路からはいかなるパケットも返信されない。したがって攻撃判定されたノードから RREP、RREQ、TCP パケットのいずれかを受信した場合、実在するノードであると判断する。実在するノードと判断すると、そのノードまたはそのノードがネクスト・ホップである経路の宛先 IP アドレスの経路リストの攻撃判定フラグを False とする。

5. 計算機シミュレーションによる評価

Ghost Attack およびその防御法の評価のために、ns-2[7] によるシミュレーション実験を行った。また攻撃には AODV(AODV-uu0.8.1[8])を使用した。

5.1. シミュレーション環境

表 1 にシミュレーション環境の詳細を示す。

表 1. シミュレーション環境の詳細

環境	
トポロジ	1000m × 1000m
電波到達範囲	半径約200m
ノード数	全100~120 ただし、非攻撃ノードは固定で100ノード、攻撃ノードは0~20の範囲で変化
攻撃ノード数	0~20
防御ノード数	非攻撃ノードの0%か100%
非攻撃ノード数	100（通信が確実に行える密度）
シミュレート時間	100秒
通信	2ノード間の単方向通信。プロトコルはTCP/FTP ノード1とノード（(10-1)×x1 x=1,2,3,4,5,6,7,8,9,10の計10パターンについて行う
通信レート	32Kbps
ノードの動き	ランダム
パラメタ	
全ノード数	100~120の間で刻み幅1
攻撃ノード数	1~20の間で刻み幅1
防御ノードの数	0%・100
正常ノードの数	0%・100
ノードの移動速度	0(停止),3(歩き),7(早歩き),60(車) ただし、これらが混在することはない、またこの速度は最高速度である
定義	
攻撃ノード	攻撃のみを行うノード
防御ノード	防御を行うノード
正常ノード	防御も攻撃もしないノード、AODVのネイティブの機能のみを有する
非攻撃ノード	防御ノードと正常ノード

通信に用いるノード数は十分に通信が行える 100 ノードとし、攻撃ノードはそこに追加する。ノードの移動は ns-2 付属の setdest コマンドにより自動生成されたランダム移動とした。攻撃ノードの数や防御の有無によらず通信に用いるノードは移動速度別に常に同一動作をする。送信元および宛先ノードは通信に用いる 100 ノードから選択する。送信元ノードと宛先ノードの組み合わせには ns-2 上のラベルを用い、(1,9),(1,19),(1,29), (1,39), (1,49), (1,59), (1,69), (1,79), (1,89), (1,99)の計 10 パターンを用いる。これら 10 パターンの通信スループットの平均を用い、通信ノードの位置による通信スループットの偏りを解消する。データ通信には TCP を、パケットの生成には FTP を用いる。シミュレーション時間内に宛先ノードが受信したデータパケットの数を通信スループットとし、攻撃ノード数が 0 のときのスループットを 100%としたときの割合を通信効率とする。

ノードの移動速度は実世界の移動速度を考慮し 0km/h（静止）、2km/h(歩行)、7km/h(早歩き)、60km/h(車)の 4 つを用いる。シミュレーションは各速度別に行う。

シミュレーションは全ノード数 100～120 (21 回) × 移動速度 0~60 (4 種類) × コネクションパターン (10 パターン) × 攻撃 / 防御 (2 回)

の計 1680 回行う。

5.2. シミュレーション結果と考察

シミュレーション結果は、攻撃および防御による通信効率の変化をグラフ化する。また「攻撃ノード数」を横軸、通信効率を縦軸にグラフ化したものを攻撃検証グラフとし、同方法で防御機構適用時のグラフを作成したものを防御検証グラフとする。

図 3 から図 8 に Ghost Attack と防御機構適用時における攻撃ノード数と通信効率の関係、ノード移動速度別の攻撃と防御、そして防御機構適用時の通信スループットの回復率を示す。

図 3 は Ghost Attack における攻撃ノード数による全移動速度の通信効率の平均の変化を示したグラフである。通信効率は攻撃ノード数の増加とともに減少していることから、攻撃ノード数が通信効率の低下を招いていると言える。攻撃ノードの増加に伴い、宛先ノードの Hello メッセージを模倣される確率が高くなる。したがって誤った通信経路の作成が行われ、大量のロストパケットが発生する。一方防御機構適用時も攻撃ノードの増加により経路の再構築に長時間かかるので通信効率が低下する。防御機構非適用時に比べ通信効率の低下が抑えられているため、防御機構が有効に機能していると言える。

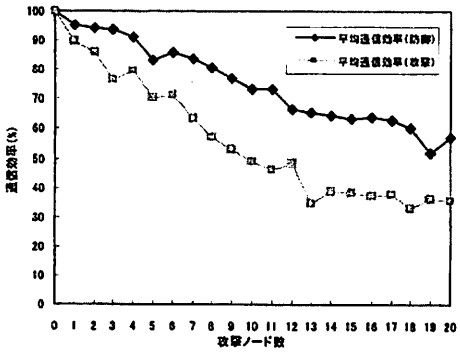

図 3. 攻撃ノード数と全スピードの平均通信効率

図 4 から図 7 は本攻撃に対する防御機構適用時の攻撃ノード数と通信効率の関係をノード移動速度別に示したものである。ノードの移動速度が 2km/h の場合を除き、通信効率の低下は攻撃ノード数の増加に一定の割合で比例している。攻撃の増加に伴い攻撃ノードが通信の宛先及びすでに存在しないノードへの経路が保持された状態に陥りやすくなるため、通信が妨害される可能性が高くなる。防御機構を適用した場合でも、攻撃ノードの増加に伴い経路の再構築回数が増加するため、通信効率は若干低下する。

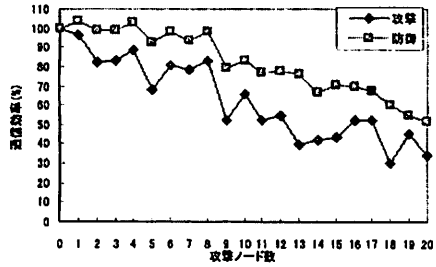

図 4. 0km/h における通信効率の変化

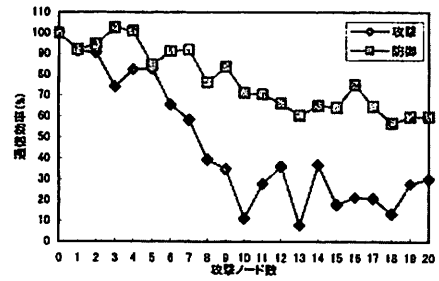

図 5. 2km/h における通信効率の変化

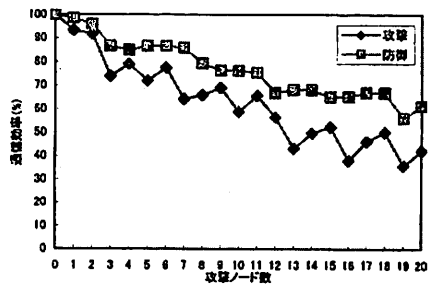

図 6. 7km/h における通信効率の変化

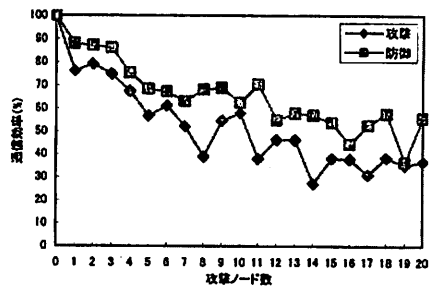

図 7. 60km/h における通信効率の変化

図 8 に防御時における攻撃ノード数と通信効率の回

復率の関係を示す。回復率とは攻撃を受けた場合の通信スループットに比べ、防御機構適用時に回復した通信スループットの割合を表す。通信効率は全ノード移動速度の通信効率の平均値である。攻撃ノード数が 10 前後では回復率が上昇し、それ以降はほぼ 25%前後の回復率を示している。本提案方式では防御機構適用時にも最低 1 度は攻撃を受ける。そのため攻撃ノードの配置がランダムな状況では攻撃ノード数の増加に対し攻撃の回数が必ずしも比例しないため、回復率が上下する。

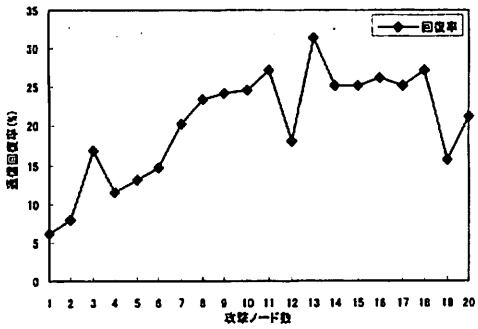

図 8. 防御機構適用時の通信効率の回復率

6. 結論

実験結果より Ghost Attack が通信効率を著しく低下させるが防御機構の適用により、低下した通信スループットが回復する。今回の実験環境では、シミュレーション時間が 100 秒間であるために攻撃された経路を再構築後の通信時間が短い。そのため、複数回攻撃が成功した場合に経路を再構築しても正常通信が行える時間が少ないために、防御時の通信効率の低下が顕著に現れる。長い時間通信を行う場合では、攻撃を受けたとしても問題なく通信できると考えられる。また、Ghost Attack の特性として、一度通信圏内に攻撃対象が侵入してから通信圏外に移動しなければ攻撃が成立しない。したがって、攻撃条件が整うには最適な移動速度がある。結果からノードの移動速度が 2km/h の場合に他の移動速度に比べ顕著に通信効率が低下するため、2km/h が最適な攻撃条件であるといえる。これは攻撃条件が整った後、その状態が長く継続できる速度であると考えられる。

防御機構においては、一度通信不能に陥った経路は記録されるため移動速度に関係なく時間経過により偽の Hello メッセージの検出精度が上がるため、すべての移動速度において一定の通信効率を保障する。本防御機構を適用した場合に最適な経路が得られたことが通信効率の増加につながると考えられる。

実験を通して、Hello メッセージを模倣する Ghost Attack が通信スループットを低下させる攻撃として成立すると言える。またこの攻撃に対する防御機構が模倣された Hello メッセージを検出・破棄することで通信スループットの低下を防ぐことができるといえる。

7. 終わりに

本防御方式は実環境下では、必ずしも攻撃ノードを検出することはできない。なぜなら、実環境では Hello メッセージのような小さなパケットはより遠くまで届く傾向にあり、実際に通信できる距離とのギャップが生じる。このギャップはグレーゾーンと呼ばれ、実環境において AODV のようなアドホック・ルーティング・プロトコルによる通信が不安定になる原因のひとつとなっている。グレーゾーン内のノードの条件と本防御方式における攻撃ノードの検出条件が一致してしまうため誤認する可能性がある。しかしながら、グレーゾーンが発生している状態では通信は行えないので、本防御方式を適用させることにより通信が正常に行われなくなることは無いと考えられる。今後の課題としては、本防御機構が実環境においてもその有効性を示す必要がある。

もう一つの課題としては UDP 通信における防御法の開発である。UDP 通信においては ACK による送信パケットに対する確認がないため本防御機構を適用することができない。現在 VoIP やストリーミング配信など、UDP 通信が使われる場面は多い。アドホックモバイルネットワークにおいてもこれらの技術が使われると考えられ、UDP 通信における防御法の開発が必要である。

文　献

[1] AODV: Ad-hoc On-Demand Distance Vector Routing. RFC3561 http://www.ietf.org/rfc/rfc3561.txt

[2] C-K. Toh,著　構造計画研究所, 訳　「アドホックモバイルワイヤレスネットワーク」, 共立出版株式会社　pp.59-63　2003

[3] AODV-uu: http://core.it.uu.se/adhoc/AodvUUImpl

[4] Jhon R. Douceur,　The Sybil Attack, IPTPS'02, Mar. 2002

[5] アンドリュー・S・タネンバウム, 著　水野忠則, 相田仁, 東野輝夫, 大田賢, 西垣正勝, 訳　「コンピュータネットワーク」, 日経 BP 社　pp.736-748 2003

[6] ns-2: http://www.isi.edu/nsnam/ns/

[7] 岡田伊織,「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」, 第 68 回情報処理学会全国大会, Mar. 2006