Vol.2018-IOT-43 No.12
Vol.2018-SPT-30 No.12
2018/9/28

MANETにおける複数経路を活用するワームホール攻撃対策手法
Prevention of Wormhole Attacks using multipath routing in MANETs

高橋　万里 †
Banri Takahashi

今泉　貴史 ‡†
Takashi Imaizumi

1. はじめに

近年、スマートフォン等のモバイル機器の急激な普及により、モバイルアドホックネットワーク (MANET)[1] の研究が盛んに進められている。MANET は各端末がマルチホップ通信を用いることで、自身の通信範囲外の端末と通信するが、マルチホップ通信を用いるがゆえに、MANET に対して攻撃が行われやすい。その中で特に脅威とされているものがワームホール攻撃である。

ワームホール攻撃では、攻撃ノード間で遅延やホップ数などのコストが低いリンクを構築することで、攻撃ノードを通る経路を優先的に選択させるようにし、中継するデータの盗聴などを図る。ルーティングプロトコルの一つである Ad hoc On demand Vector Routing(AODV) は、経路選択の際、このコストを利用するため、特にこの攻撃の被害を受けやすい。

本研究では、この問題を解決するため、WAODV を提案する。WAODV では、攻撃経路のホップ間の平均遅延が通常経路と比較して大きくなることを利用し、ワームホール攻撃を検出する。さらに、各ノードに信頼度を設けることで、攻撃ノードの検出も行う。平均遅延が大きい攻撃経路内に存在する信頼度が低いノードを攻撃者と特定することで、以降の通信要求時に一度特定した攻撃者を含む経路を構築することがなくなる。

また、シミュレーション実験から、WAODV での検知は、攻撃ノード間のリンクが長く、かつ片方の攻撃ノードが宛先ノードの近隣に存在する環境では、安全な経路を構築できない場合があることが判明した。この問題点について、WAODV における中継ノードの振る舞いを変更することでの解決方法を考察する。中継ノードは単一の RREQ しか受け付けないが、これを複数受け付けられるようにする。これにより、経路の候補を増やすことで、安全な経路を選択しやすくする。

2.MANET

2.1.AODV

AODV は、データ送信要求があって初めて、宛先ノードまでの経路を探索するリアクティブ型のルーティングプロトコルである。

送信元ノードは、経路探索のため Route Request(RREQ) をブロードキャストする。RREQ を受信したノードは、自身が宛先でない場合、RREQ に記載された情報から自身のルーティングテーブルに送信元ノードへのエントリを作成し、近隣ノードに再ブロードキャストする。以後、中継ノードは、同じ宛先ノードへの RREQ を受け取ると単に破棄する。これは、ネットワークの帯域を圧迫を制限し、ループを生じさせないためである。

RREQ を受信した宛先ノードは、Route Reply(RREP) を、RREQ を送信したノードに対してユニキャストする。RREP を受信したノードは、先ほど作成したルーティングテーブルのエントリに基づいて、RREP を送信すると共に、宛先ノード D への経路表のエントリを作成する。送信元ノード S に RREP が到着すると、データ送信が可能となる。

AODV は、他のルーティングプロトコルと比べ、トポロジー変化が大きい環境でも経路構築率が高いことから、MANET の事実上の標準となっている。

2.2. ワームホール攻撃

マルチホップ通信の特性を利用した MANET に対する攻撃が存在しており、その手法は多岐にわたる。その中で、特に脅威とされているのがワームホール攻撃である。ワームホール攻撃では、複数の攻撃ノードが共謀し、その間で遅延やホップ数などのコストが低いリンクを構築し、送信元から宛先までの経路の短縮を図る。これにより、攻撃ノードに経路を集中させることが可能となる。

ワームホール攻撃を行う攻撃ノードが含まれる際の経路構築の手順を以下に示す。

1. 通信開始時、送信元ノードは RREQ を宛先ノードに向けてブロードキャストする。
2. RREQ を受信した攻撃ノードは、攻撃リンクを通じて共謀ノードへ RREQ をユニキャストする。
3. RREQ を受信した共謀ノードは、宛先ノードに向けてさらにブロードキャストする。
4. RREQ を宛先ノードが受信すると、送信元ノードへ RREP をユニキャストする。
5. RREP を受信した攻撃ノードは、攻撃リンクを通じて RREP を送信元ノードへユニキャストする。
6. 送信元ノードは、RREP を受信し、攻撃経路を構築することとなる。

AODV は、経路選択にホップ数などのコストを用いるため、攻撃経路を構築する可能性が高くなっている。

†千葉大学融合理工学府
‡千葉大学統合情報センター

Vol.2018-IOT-43 No.12
Vol.2018-SPT-30 No.12
2018/9/28

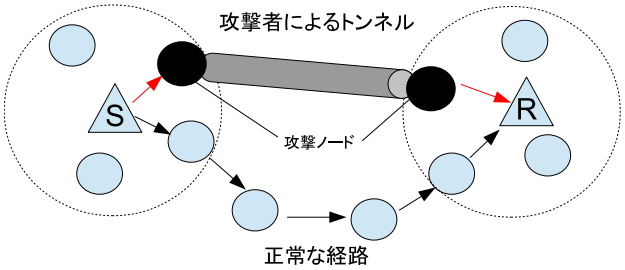

図 1: ワームホール攻撃

2.3. 関連研究

2.3.1.MAODV

MAODV [2] では、送信元から宛先までの複数経路上のホップ数と遅延情報を収集することでワームホール攻撃を検出する手法である。AODV をベースにしているため、ネットワークのリソースを必要以上に消費せず、追加するハードウェアもない。しかし、攻撃者の特定ができない問題点が挙げられる。また、攻撃ノード間のリンクが短い場合、検出率が低下してしまう。本手法は、提案手法の WAODV の性能評価と比較するために利用する。

2.3.2.IDSAODV

IDSAODV [3] では、ネットワーク内に侵入検知ノードを設置する。侵入検知ノードは近隣ノードが正しくパケット中継しているか確認する。パケット中継回数が閾値以上失敗したノードを攻撃ノードだと判断し、侵入検知ノードは通常ノードに攻撃ノードの情報をブロードキャストする。本手法は、侵入検知ノードに対して攻撃されないことを前提としている。また、ネットワーク内のすべてのノードに侵入検知ノードの見張りが行き届くように配置しなければいけないため、ハードウェア用意のコストが必要となる。

2.3.3.MLAMAN

MLAMAN [4] は、RREQ の認証を 2 段階行い、さらに GPS 情報を利用することで攻撃者の検出を行う。本手法は、認証を行う必要があるため、ネットワークのリソースが消費が激しく、経路探索に時間がかかる。また、GPS 情報を利用するため、追加ハードウェアの用意が必要となる。

3.WAODV(Watchdog powered AODV)

MANET におけるワームホール攻撃の対策手法として、WAODV [5] を提案する。WAODV は、送信元から宛先までの複数経路上のホップ数と遅延情報を利用してワームホール攻撃を検出する。ワームホール攻撃は、攻撃ノード間でコストの低いリンクを構築する。このリンクが、通常ノードを複数跨る長いものであることから、通常経路に比べて攻撃経路の方が平均遅延が大きくなる。

また、WAODV ではネットワーク内の各ノードに信頼度を設定する。信頼度は、中継ノードが、不正な動作を検出した場合に信頼度を下げ、正常にパケット中継が確認されれば信頼度を上げる。攻撃経路内に信頼度が低いノードが含まれている場合、そのノードを攻撃者と認定し、ブラックリストに加える。

3.1. 対象とする攻撃

本研究では、共謀した 2 台の攻撃ノードによるワームホール攻撃を対象とする。攻撃ノード間では、有線ネットワーク、または大出力の無線電波を使用してリンクを構築する。また、通常ノードによる長距離リンクの存在は排除する。つまり、ノードの通信半径以上のリンクはワームホール攻撃のリンクとする。

攻撃ノードは、送信元ノードからの RREQ を共謀ノードにユニキャストする。その後、共謀ノードは転送された RREQ を宛先ノードに向けてブロードキャストする。

3.2. 信頼度

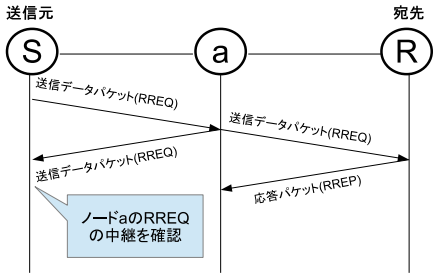

図 2: パケット中継の確認

あるノード宛に送信された RREQ の中継を確認することで、その近隣ノードの信頼度を計算する。

無線通信は、電波に指向性がないため、送信元ノードの送信半径内に存在するノードすべてにデータを受信する。通常ノードは、RREQ を受信すると、自身が宛先でない場合、RREQ を送信してきた上流の近隣ノード含めて全ノードにブロードキャストする。しかし、はじめに RREQ を受信する攻撃ノードは、攻撃経路を選択する確率を少しでも高めるため、RREQ を共謀ノードに向けてユニキャストする。

ここでは、RREQ を受信したノードはパケットの宛先と送信元から近隣ノードが正しく RREQ を中継しているか判断する。一定時間内に近隣ノードからの RREQ の中継を確認できない場合、中継失敗とみなし、信頼度を下げる。

図 2 において、ノード S はノード a から送信された RREQ の宛先と送信元および攻撃ノードフィールドを確認することで自身が送信した RREQ を中継したと判断する。

3.3. 動作

WAODV の動作は経路情報収集と攻撃検出の 2 ステップに分けられる。

経路情報収集ステップ

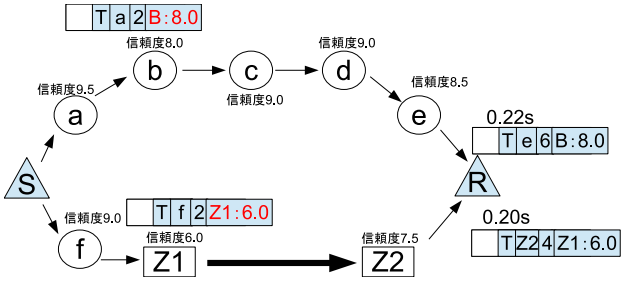

図 3: 経路情報収集ステップ

通信開始時に送信元ノード S は RREQ をブロードキャストする。RREQ には通常のタイムスタンプ、前ホップおよびホップカウントフィールドに加え、攻撃ノードフィールドとノード信頼度フィールドを持つ。前者には、経路上の最も信頼度が低いノード ID が記載しており、後者には通信範囲内の全ノード ID と信頼度のリストを保持する。図 3 における RREQ のフィールドは右から攻撃ノード、ホップカウント、前ホップおよびタイムスタンプである。RREQ を受信した中継ノードは、ノード信頼度フィールドと自身の信頼度を比較し、書き換えるかを判断する。その後、前ホップノード、ホップ数を書き換え、周囲にブロードキャストする。

攻撃検出ステップ

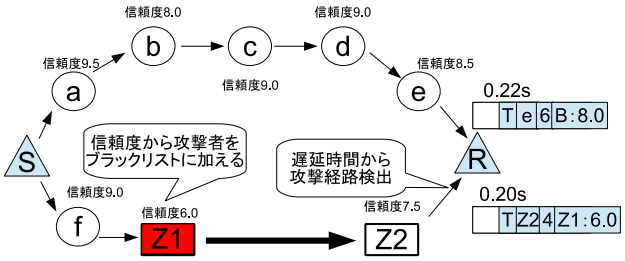

図 4: トンネルが長い場合の攻撃検出

宛先ノードに RREQ が届くと、RREQ から平均遅延を計算する。平均遅延 (DPH) は RREQ 内のホップカウント値 H、タイムスタンプ値 T_a および RREQ の受信時間 T_b を用いて次式で計算できる。

$$DHP = \frac{T_b - T_a}{H} \quad (1)$$

複数経路の平均遅延を比較して、閾値より大きい経路を攻撃経路と判断する。さらに、攻撃ノードフィールドに記載している信頼度が閾値以下であれば、そのノードをブラックリストに追加する。平均遅延が小さい経路で、攻撃ノードフィールドが閾値以下であれば、その経路は優先経路から除外されるが、そのノードはブラックリストには加えられない。これは、通常ノードがパケット中継を正常に行えなかったことを考慮している。

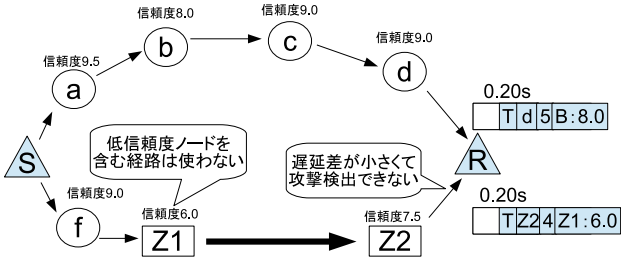

図 5: トンネルが短い場合の攻撃検出

図 5 において、ノード Z1 は RREQ をノード Z2 にユニキャストしていることから、上流のノード f がノード Z1 を正しくパケット中継していないと判断し、信頼度が閾値以下となり、攻撃ノードと判断されている。

信頼度の改ざん

WAODV において、中継ノードは自身の信頼度と攻撃ノードフィールドの信頼度を比較し、RREQ を書き換える。しかし、ワームホール攻撃において、攻撃ノードが自身の信頼度を偽る可能性がある。

中継ノードは、ノード信頼度フィールドに自身の通信範囲に存在する全ノードの信頼度情報を記載する。そのため、RREQ を受信したノードは、自身の信頼度だけでなく、前ホップノードの近隣に存在するノードの信頼度も把握できる。攻撃ノードの近隣に存在するノードは、受信した複数の RREQ に記載されている信頼度を比較し、信頼度の改ざんを検知できる。

4. シミュレーション評価

本章では、シミュレーション評価を用いて WAODV の有効性を示す。シミュレーションでは、AODV、MAODV および WAODV の 3 つの方式についてシミュレーションを行い、結果を比較する。

4.1. 諸元

シミュレーション評価には、2 つシナリオを用いた。

1. シナリオ 1 では、攻撃者によるトンネルを含む経路を必ず構築してしまう場合を想定する。図 6 のように，エリアを 3 つに分割する。分割したそれぞれのエリアに中継ノードをランダムに配置し、いずれかのエリアにワームホール攻撃ノードを 1 組配置する。その際、攻撃ノードの組は同じエリアの 3 ホップ以上離れた位置に配置する。
2. シナリオ 2 では、攻撃者が必ずしも送信元ノードと宛先ノードの近隣に存在しない場合を想定する。図 7 のように、送信元ノードと宛先ノードを 200m × 200m の範囲に、ワームホール攻撃ノードは 1 ホップ以上離れた位置にランダムに配置する。

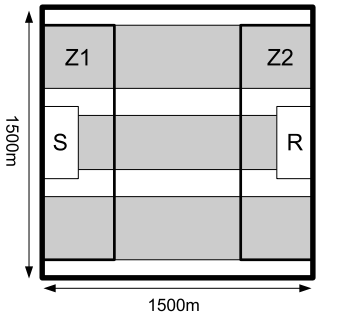

図 6: シナリオ 1

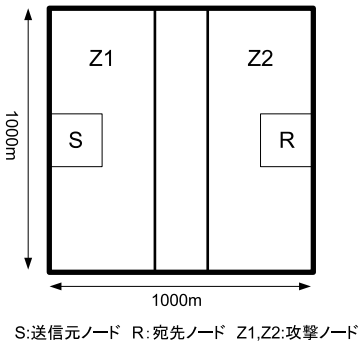

図 7: シナリオ 2

主なシミュレーション諸元は表 1 のとおりである。MAODV と WAODV で収集する経路を 3 経路とし、3 経路が収集できない場合でも最初の経路を発見してから 3 秒後に攻撃検出ステップに移行する。WAODV における信頼度について、初期値は 1.0 とし、閾値は 0.6 に設定した。次ホップ先ノードの RREQ の中継を確認できた場合、そのノードの信頼度を 0.5 上げ、確認できなかった場合、0.5 下げる。

4.2. 評価指標

WAODV の有効性の評価指標を、配信率および RREQ 受信数から評価する。

表 1: シミュレーション諸元

	シナリオ1	シナリオ2
シミュレーター	QualNet netw ork Simulator 5.02	
シミュレーション範囲	1500[m]×1500[m]	1000[m]×1000[m]
シミュレーション時間	25[s]	
ノード数	100[ノード]	
ワームホールノード	2[ノード]	
MAC Protocol	IEEE802.11b	
Routing Protocol	AODV	
送信半径	200[m]	
ホップ間遅延閾値	0.005[s]	
ノード信頼度閾値	0.6	

配信率

ワームホール攻撃のリンクを経由しない安全な経路が構築できた割合を配信率と定義する。通常の AODV による経路構築では，ホップ数の少ない経路を構築するため，攻撃経路を優先経路として選択する可能性が高い。したがって、配信率によって、どれだけ攻撃者を排除した経路を構築できたかが評価できる。

RREQ 受信数

MAODV と WAODV では複数の経路を収集するため，ネットワーク内に流れる RREQ 数が増加する。したがって，どの程度 RREQ 数が増加するかを評価する必要がある。送信元ノードが宛先ノードからの RREP を受信するまでにネットワーク内の全ノードが受信した総 RREQ 数を RREQ 受信数と定義する。

4.3. シミュレーション結果

4.3.1. シナリオ 1

シナリオ 1 の配信率を図 8、RREQ 受信数を図 9 に示す。

配信率について、各方式で大きく異なっている。AODV では、ホップ数が最小の経路を構築するため、攻撃ノードのリンクを含む経路を必ず構築している。ホップ間の平均遅延を用いる MAODV の配信率は 33%であり、ノードの信頼度を加えた WAODV では、81% という高い配信率を実現している。

RREQ 受信数について、AODV が約 400 個に対して、MAODV と WAODV が共に約 1000 個と多くなっている。宛先ノードからの RREP を受信するまで、ネットワーク内には RREQ が流れ続ける。複数経路を収集する MAODV と WAODV は、待機時間があるため、ネットワーク内に流れる RREQ が増加している。

4.3.2. シナリオ 2

シナリオ 2 の配信率を図 10、RREQ 受信数を図 11 に示す。

Vol.2018-IOT-43 No.12
Vol.2018-SPT-30 No.12
2018/9/28

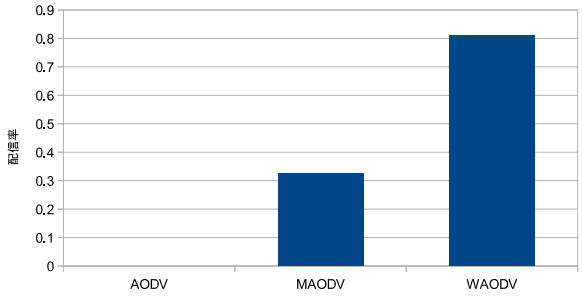

図 8: 配信率

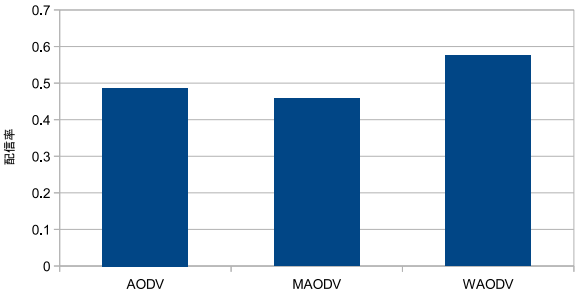

図 10: 配信率

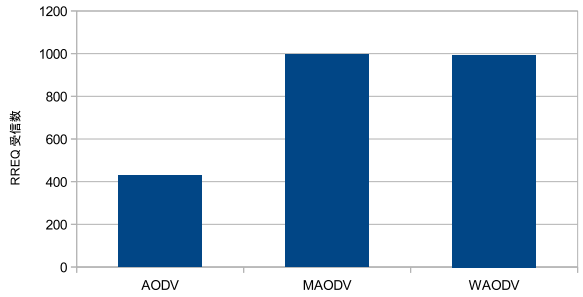

図 9: RREQ 受信数

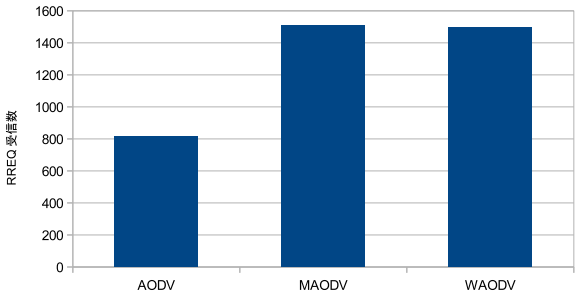

図 11: RREQ 受信数

配信率について、シナリオ 1 ほど各方式で配信率に大きな違いがみられなかった。攻撃者を送信元ノードと宛先ノードの近隣に固定しないことで、攻撃経路が最小ホップ数になるわけではない。そのため、AODV でも配信率は 49% であった。MAODV では 46% と AODV を下回り、WAODV では他の 2 方式より高い 58%であった。

RREQ 受信数について、シナリオ 1 と同様に AODV と比較して、MAODV と WAODV が多くなっている。また、シナリオ 2 ではシナリオ 1 より各方式で 400 個ほど RREQ 受信数が増えている。これは、シナリオ 1 では、シミュレーション範囲を 3 つのエリアに分割したため、RREQ を中継する範囲が限られていた。一方で、シナリオ 2 では、シミュレーション範囲全体にノードを配置したため、複数の近隣ノードから RREQ を受信する機会が増え、ネットワーク内の RREQ 受信数が増えたと考えられる。

5. 考察

5.1. シナリオ 2 における MAODV の配信率

図 10 において、セキュリティ機構のない AODV よりワームホール攻撃対策をした MAODV の配信率が低下した。これは、複数の経路を収集することで、AODV では届かなかった攻撃ノードの RREQ が宛先ノードに届いてしまうことが考えられる。AODV では、宛先ノードに最初に受信した RREQ に対してのみ RREP を返すため、二度目以降に攻撃者を経由した RREQ が宛先ノードに届いても、攻撃経路を構築しない。しかし、MAODV では、複数経路を収集するため、本来であれば破棄していた攻撃者経由の RREQ も受信する。宛先ノードは、複数経路間のホップ間の平均遅延を比較し、閾値以上の差異があれば攻撃経路の検出を行うが、差異がない場合、複数経路の中で最小ホップ数の経路を優先的に選択する。図 12 のように攻撃経路に閾値以上の差異がない場合、ホップ数の小さい攻撃経路を選択してしまうため、MAODV の配信率が低下したと考えられる。

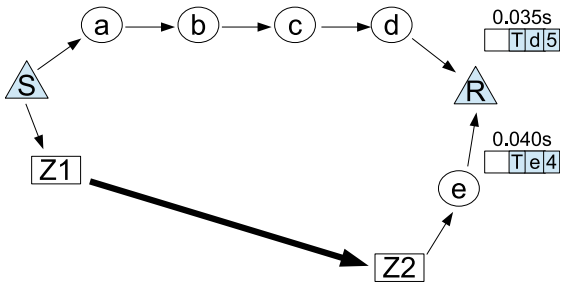

図 12: 収集した複数経路の例

5.2. シナリオ 1 とシナリオ 2 の配信率の比較

シナリオ 1 と比較し、シナリオ 2 の配信率が 20% ほど低下した。これは攻撃ノードから中継された RREQ により周囲のノードが正常なノードからの RREQ を破棄してしまったためだと考えられる。図 13 を用いて説明する。送信元ノードからの RREQ を受信した攻撃ノード Z1 は、共謀している攻撃ノード Z2 に RREQ をユニキャストする。その後、RREQ を受信した攻撃ノード Z2 は宛先ノードに向けて RREQ をブロードキャストする。この時、宛先ノードの他に周囲のノードも攻撃ノード Z2 からの RREQ を受信することになる。周囲の中継ノードは、攻撃ノード Z2 からの RREQ を受信した時点で、以降の RREQ を中継せずに破棄してしまう。このため、通常の中継ノードを経由してきた経路を構築することができず、宛先ノードが収集する経路は、攻撃者を含む経路のみとなる。この問題は、攻撃ノードからの RREQ を受信する中継ノードが増えるほど顕著に現れるため、攻撃者間のリンクが長く、攻撃ノードが宛先ノードの近隣に存在するほど被害が甚大となる。本問題は、AODV のルーティングプロセスに起因しているものであるため、WAODV に限らず、AODV をベースにワームホール攻撃対策を行っている手法の多くに潜在している。

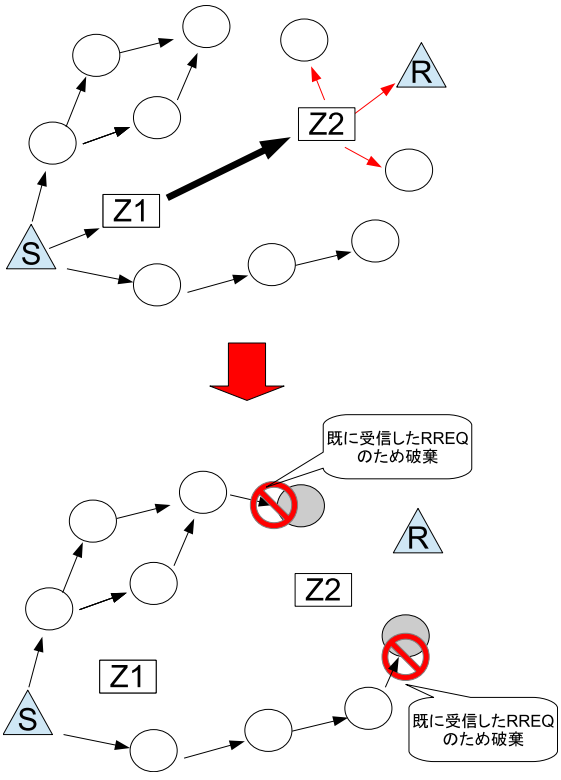

図 13: 攻撃ノードによる RREQ

5.3. 配信率低下の改良

前節で述べた問題点を解決するために、WAODV における中継ノードの振る舞いを変更することを考慮する。本来、AODV において中継ノードが初めの RREQ しか受け取らないのはループが生じる可能性を低くするためであった。WAODV において、宛先ノードのみが RREQ を複数する受け付けるため、ループの可能性は AODV と変わらなかった。

WAODV の中継ノードが宛先ノードと同じように一定時間内の RREQ をすべて受け付けるとすると、2 つのノード間で RREQ を一定時間内に送りあうこと事象が発生し、RREQ のループが生じると考える。また、ループが生じやすい環境のため、WAODV よりも RREQ 受信数が増え、ネットワークのリソース消費が激しくなると考える。よって、このように単調に中継ノードの振る舞いを変更するのは不適である。

次に、攻撃ノードフィールドの信頼度を利用した方法を考慮する。WAODV における RREQ には、その経路上の一番信頼度が低いノードの ID が含まれる攻撃ノードフィールドがあり、ルーティングテーブルにもこの情報が記載されている。図 13 において、ノード A は初めに攻撃ノード Z2 から RREQ を送信され、ルーティングテーブルに Z1〜Z2 の経路を記載する。この時、攻撃ノードフィールドに Z1 の ID を記載したとする。その後、左上の通常ノードから RREQ がノードへ送信されたとき、宛先に加え、攻撃ノードフィールドも参照する。宛先が同じでも、RREQ の攻撃ノードフィールドには Z1 以外の ID が記載されているため、ノード A は、同じ宛先に関する複数経路だと判断し、後に送られた RREQ でもブロードキャストする。

本手法では、同一経路上の 2 つのノード間では攻撃ノードフィールドが同じため、前述のような 2 つのノード間で同じ RREQ を送信しあうことはない。異なる経路が合流するようなノードは、初め、ルーティングテーブルの攻撃ノードフィールドと異なるため、1 度 RREQ を送信しあうことになるが、2 回目以降は同様な攻撃ノードフィールドをもつ RREQ が送信されたことを判断できるため、それ以上 RREQ がネットワークに広がることはない。また、RREQ 受信数について、宛先ノードに届ける RREQ を多くしたいため、WAODV と比較して、各ノードの RREQ 受信数は多くなる。しかし、ループが起こるように RREQ を送信しあうこと可能性が小さいとされるため、大きくなりすぎることはないと考えられる。

6. おわりに

6.1. まとめ

本論文では、MANET におけるワームホール攻撃を防ぐために、WAODV を提案した。WAODV は、ワームホール攻撃の攻撃経路が通常経路と比較して、ホップ間の平均遅延が大きくなることを利用し、複数経路の平均遅延情報を収集する。これに加え、近隣ノード

の監視情報を用いて、攻撃経路を排除した。また、ネットワークシミュレータを用いて WAODV の性能評価を行った。その結果、どのようなトポロジでもほかの 2 方式より高い配信率を実現した。

しかし、シナリオ 2 の配信率から、攻撃ノードからの RREQ を受信したノードが別の中継ノードからの RREQ を破棄してしまう問題が判明した。この問題に対し、信頼度を利用することで中継ノードの振る舞いを変更する手法を考察した。

6.2. 今後の課題

今後の課題として、攻撃検出に用いる閾値の最適化が挙げられる。ネットワークの規模やトラフィック量に応じて遅延時間は変化するため、これらを考慮した最適な閾値を設定することで、さらに検出率が向上する。また、ノード信頼度を線形に変化させたが、信頼度を上下させる値や上限について再度考える余地がある。

最後に、攻撃ノードフィールドの信頼度を利用し、中継ノードの振る舞いを変更し、複数の RREQ を受け付ける手法について今後詳細を考慮していく。これにより、シナリオ 2 のようなトポロジーでも配信率の向上が見込まれる。この手法を WAODV に取り込み、ネットワークシミュレータを用いて性能評価を行うことで、有効性を示していきたい。

参考文献

[1] 阪田史郎, 青木秀憲, 間瀬憲一. アドホックネットワークと無線 lan メッシュネットワーク (無線アドホックネットワーク技術論文) 電子情報通信学会論文誌. B, 通信, pp.811-823, June 2006.

[2] Umesh Kumar Chaurasia, Varsha Singh. Maodv:Modified wormhole detection aodv protocol. 2013.

[3] Farrukh Aslam Khan, Muhammad Imran, Haider Abbas, Muhammad Hanid Durad. A detection and prevention system against collaborative attacks in Mobile Ad hoc Networks. 2017.

[4] Tu T.Vo, Ngoc T.Luong, Doan Hoang. MLA-MAN:a novel multi-level authentication model and protocol for preventing wormhole attack in mobile ad hoc network. 2018.

[5] 鈴木貴之. MANET における Watchdog 方式を用いたワームホール攻撃対策手法. Master's thesis, 千葉大学大学院融合科学研究科情報科学専攻知能情報コース, 2014.

[6] C. Perkins, E. Belding-Royer, and S. Das. Ad hoc on-demand distance vector (AODV) routing, July 2003.

[7] Mahesh K.Marina and Samir R.Das. Ad hoc on-demand multipath distance vector routing, 2002.

[8] Sergio Marti, T.J.Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. pp.255-265, 2000.

[9] Parvinder Kaur, Dalveer Kaur, Rajiv Mahajan. Wormhole Attack Detection Technique in Mobile Ad Hoc Networks. 2017.