

ビザンチン攻撃の検出と回避を考慮した Hop By Hop ベースルーティングプロトコルの提案と実装・評価

森 郁海[†] 高橋 修[‡]

[†] 公立はこだて未来大学大学院 システム情報科学研究科

[‡] 公立はこだて未来大学

概要 Mobile Ad-hoc NETwork(MANET)は、無線技術を用いたマルチホップ通信により固定インフラが存在しない状況でもネットワークを構築することが可能である。一方で、第三者ノードを中継する可能性を持つためエンド間、リンク間のセキュリティを確保することが重要である。MANET ではアドホックルーティングプロトコルを用いることでネットワークを構築するが、悪意のあるノードはルーティングメカニズムに干渉し、攻撃を行うことができる。この種の攻撃で最も強力であるとされるビザンチン攻撃は、攻撃者自身が経路に入り込み特定のパケットやデータパケットの全てあるいは大部分を破棄するものである。この攻撃の検出する場合、MANET が持つ本来の輻輳や無線リンクの使用によって自然発生するパケットドロップ、プロトコル自体のバグ、ハードウェアの構成ミスなどによって誤認が発生する。本稿ではこの誤認を軽減するために、単位時間内のリンク間のデータパケットの送受信数の整合性を確かめる過程で厳密に一致させるのではなく許容を持たせる手法を提案し、AODV 上の実装し評価する。

AODV-BDA: AODV with Byzantine attacks Detection and Avoidance

Ikumi MORI[†] Osamu TAKAHASHI[‡]

[†] Graduate School of Future University-Hakodate, Systems Information Science

[‡] Future University-Hakodate

Abstract Mobile Ad-hoc NETwork(MANET) that is multi-hop communication using radio link can build a network in the situation that there is not fixed infrastructure. However, in order to relay packets by intermediate node, a secure communication of end to end and between the nodes is needed. MANET builds a network using Ad-hoc Routing Protocol, but malicious node can attack it interfering routing mechanism. The Byzantine attack that is the strongest attack against routing get into a route that is used in order to relay data packets, and drop a specific packet or all/almost of the data packet. When detecting this malicious node, misconception occurs by naturally occurring packet drop is caused by a congestion of MANET, the use of radio link, the bug of the protocol and a hardware configuration mistake. In this paper, in order to reduce this misconception, we suggest a technique that allows the consistency of the number of send and receive data packet of link until predetermined threshold. And then we implement it on AODV and evaluate it.

1. はじめに

現在の MANET におけるビザンチン攻撃の対処法では、悪意のあるノードを特定(検出)せずに、そのノードが含まれない経路を検索し回避している^[1]。悪意のあるノードを検出しようとする誤認が発生し、正常なノードがルーティングに参加できなくなる可能性があるためである。

一般に、ネットワークに参加する悪意のあるノードは単独あるいは共謀している。また、悪意のある単独/共謀ノードは以下に示す行動ができる^{[2][3]}。

- パケットの傍受、改ざん、偽造
- ルーティングループの作成
- 選択的なパケットの破棄(Black hole, Gray hole)
- パケットを遅らせる
- 非最適経路でパケットをルーティングさせる
- 経路を実際より短く/長くみせる

上記の全ての攻撃は、ルーティングサービスの混乱や低下を目的としている。[1]ではビザンチンなふるまいをソフトウェアやハードウェアの誤り(構成ミス)や悪意のあるノードによる行動に起因するとしており、ビザンチン攻撃をルーティングで最も検出が難しい問題と位置づけている。

本稿では、共謀していないビザンチン攻撃を行っているノードを迅速に検出し回避することを目的とする。提案する手法(以下 AODV-BDA)は、以下の 3 フェーズからなる。

- 最短・準最短遅延経路の作成 最短遅延経路と準最短遅延経路を検索する。

● ビザンチン攻撃の検出 送信元と宛先と中継ノードは、自身から 1hop 以内の保持経路上のノード間のデータパケットの送受信数の一貫性を監視することで攻撃ノードを検出する。

● ビザンチン攻撃の回避 攻撃ノードとして検出したノードおよび上流(送信元側)ノードは、攻撃ノードが含まれる経路を削除する。経路の削除が発生した上流ノードおよび検出したノードは準最短遅延経路を保持している場合は切り替え、保持していない時は送信元のみ経路再検索を行う。

この時、攻撃ノードが再び含まれないように検出したノードは攻撃ノードが出す全ての制御パケットを無視する。

加えて、送信元と宛先は信頼されており中継ノードは認証されていることとする。すなわち、中継ノードは IP アドレスなどを改ざんして他のノードになりますことはできず、宛先や送信元が偽装されていることがない。

次章以降の本稿の構成は、次のようになる。2 章で関連研究について述べる。3 章で提案手法の説明を行い、4 章でそのシミュレーション評価を示す。5 章でまとめと今後の課題を述べる。

2. 関連研究

アドホックネットワークに対する既存のセキュアルーティングプロトコルを示す(表 1)。ALAN^[4]は、公開鍵暗号を用いて否認防止・制御メッセージの完全性・認証を提供する。しかし、信頼された認証局の存在が条件である。ARIADNE^[5]は、DSR を拡張したもので共通鍵暗号を用いて制御メッセージの完全性・認証を提供する。CONFIDANT^[6]は、ルートディスカバリ時に不正を行うノードの周りの経路を除外し、レピュテーション(評判)システムによって攻撃ノードを孤立させる。DCMD^[7]は、対象となるネットワークをモデル化し、ノードが受信したデータをそのモデルと比較する。一致しない場合は、さらに攻撃者モデル(攻撃パターンを定義したもの)と比較し、その結果に基づいて対処を行う。SAODV^[8]は、AODV のセキュア拡張でありルーティングメッセージの完全性・認証・否認防止を提供する。SEAD^[9]は、帯域幅や計算資源に対する DoS 攻撃を防ぐもので、一方ハッシュ関数の実を使用するため動作が高速である。SLSP^[10]は、公開鍵暗号と一方ハッシュ関数を用いてセキュアなブロードキャストルーティングを提供する。また、隣接のフラッディング頻度を監視し、不正なフラッディングが行なえないようにしている。SPAAR^[11]は位置情報と公開鍵暗号を用いて認証・否認防止・秘匿性・完全性を提供するが、ネットワーク上の各ノードは、公開鍵と秘密鍵のペア、公開鍵とノード ID

表 1 セキュアルーティングプロトコル一覧

	Design Considerations				
	Reactive		Proactive	Hybrid	Geographic
	Hop By Hop	Source Routing			
Authentication	•ALAN •SAODV •SEAD •SRP •SAR •TIARA •(AODV-BDA)	•(ALAN) •ARIADNE •SEAD •SRP •SAR •TIARA •(HADOF)	•SOLSR	•SLSP	•SPAAR
Integrity	•ALAN •SAODV •SEAD •SRP •SAR •TIARA •(AODV-BDA)	•(ALAN) •ARIADNE •SEAD •SRP •SAR •TIARA •(HADOF)	•SOLSR	•SLSP	•SPAAR
Confidentiality	•SAR •TIARA •(AODV-BDA)	•SAR •TIARA •(HADOF)			•SPAAR
nonrepudiation	•ALAN •SAR	•(ALAN) •SAR		•SLSP	•SPAAR
Exclude misbehaving nodes (Route Discovery)		•CONFIDANT •WATCHDOG- PATHRATER •OSRP			
Exclude misbehaving nodes (Dynamic)	•(DCMD) •AODV-BDA	•(DCMD) •HADOF •AODV-BDA	•(DCMD)	•(DCMD)	

を結びつけている信頼された証明書サーバ、証明書サーバの公開鍵を必要とする。SOLSR^[12]は、OLSR プロトコルのセキュリティ拡張であり、メッセージ認証コードとタイムスタンプの交換によって OLSR のシグナルパケットに対する認証の提供とリプレイ攻撃の防止を提供する。WATCHDOG-PATHRATER^[13]は、DSR の拡張として設計されており、WATCHDOG で不正なふるまいをするノードを検出し、PATHRATER で検出した攻撃ノードを通らないようにルーティングパケットを送信する。SRP^[14]は、既存のルーティングプロトコルのパケットヘッダに SRP ヘッダを追加し、メッセージ認証コードによって完全性と認証を提供するが共通鍵暗号を使用するためにエンド間のセキュリティアソシエーションを必要とする。OSRP^[15]は、ルーティングプロセスでビザンチン攻撃を実行するノードの存在下で機能ができるオンデマンドセキュアルーティングプロトコルである。logn 回誤り(パケットドロップ)が生じた後に誤りリンクとして検出することに基づき、リンクウェイト収集による誤りを回避したルートディスカバリを行う。SAR^[16]は、ルーティングの決定に距離・位置情報・電力などを利用せずに、セキュリティアトリビュート(信頼関係や信頼値)を用いる。そして、セキュリティアトリビュートによってセキュリティレベルを定義できる。TIARA^[17]は、MANET における DoS 攻撃に対する解決法(設計原理、技術)を既存のアドホックルーティングプロトコルに提供するものである。Packet Leashes^[18]は、wormhole 攻撃に対する防御法である。HADOF^[19]は、ソースルーティング上でデータパケットの流れの一貫性をレポートを用いて定期的に監視し、誠実度によって使用経路を確率的に決定するマルチパスルーティングにより回避を行う。MANET での IPsec の利用^[20]なども検討されている。

従来の方式では、主にメッセージの保護と攻撃の検出に主に DSR のようなソースルーティングを使用するプロトコルを求めている。しかし、ソースルーティングは制御メッセージ長の増加や経路切り替えを送信元のみが行うので攻撃検出から回避行動に移行するまでに時間がかかることが予想される。AODV のような Hop By Hop のルーティング上での方式でも、主にセキュアな経路構築を目的としており、回避行動は経路再検索によってのみ実行される。従って、検出から回避までの時間が増加する。

AODV-BDA では、経路上の各ノードが自身から 1hop 以内の経路の監視に限定することで、より高速に攻撃の検出を行い、回避行動を送信元まで戻すことなく攻撃を検出し

たノードが経路の切り替えを行うことで回避行動までの時間を短縮できる。

3. 提案手法

3.1. 基本原理

AODV-BDA では、送信元と宛先を含む全てのの中継ノードが監視ノードとなり、監視ノードごとに独立に**最短・準最短遅延経路の作成**、**ビザンチン攻撃の検出**、**ビザンチン攻撃の回避**の3フェーズによる監視・回避処理を行う(図 1)。

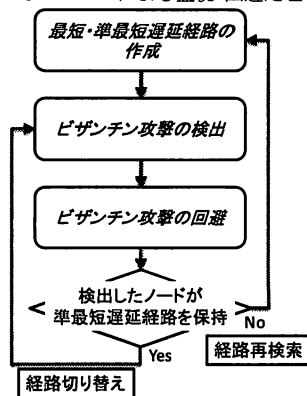


図 1 AODV-BDA の各フェーズ

● **最短・準最短遅延経路の作成** 最短遅延経路と準最短遅延経路を検索する。各中継ノードは予め定めた条件に一致した場合、Route Request (RREQ)を複数受信でき、複数の経路を保持できる。また、宛先ノードは複数の Route Reply (RREP)を送信でき、送信元ノードはそのうち最短遅延のものを主経路(最短遅延経路)、主経路より短いホップ数を持つ場合その経路をバックアップ経路(準最短遅延経路)として短い順に保持していく[21][22]。

● **ビザンチン攻撃の検出** 送信元・宛先を含むすべての経路上のノードは、RREP 受信時から期間 t 内に自身が処理した受信/送信/ドロップパケット数を記載したレポート(RPRT)を、経路上の隣接ノードとその隣接(1hop)のノードに送信する。RPRT を受信したノードは、自身・隣接・1hop 先のノード間のパケット数の一貫性を調べ、矛盾が発生した場合該当するノードの誠実度 H (初期値は $1, 0 \leq H \leq 1$)を下げる(図 2 パラメータ P)^[19]。矛盾が生じなくてもパケットドロップ報告があった場合も H を下げる(図 2 パラメータ P_d)。しかし、モビリティ変化やコリジョンなどの正当な理由でのドロップによる誤認が発生する。AODV-BDA ではこの誤認を低減するために許容値 d を設ける(図 2)。 H が閾値 $H_{threshold}$ 以下に達したとき、ビザンチン行動を行ったとして該当したノードを攻撃ノードとして検出する。

● **ビザンチン攻撃の回避** 攻撃ノードとして検出したノードは、攻撃ノードが含まれる経路を削除し、全ての逆経路に Route Error (RERR)を送信元へ送信する。RERR を受信したノードは、検出したノードと攻撃ノードのリンクを含む経路を破棄し、同様にすべての逆経路に送信する。検出したノードはバックアップ経路が存在するとき、自身が持つバックアップ経路のうちホップ数の短い経路に切り替える。また、攻撃ノードとして検出したノードは以降 H が $H_{threshold}$ 以下の間は、検出されたノードからの RREQ, RREP, RERR, RPRT を無視し、経路再検索時に攻撃ノードが含まれないようにする。

ビザンチン攻撃時の耐性は以下ようになる。

● **パケットの傍受、改ざん、偽造** AODV-BDA はベースプロトコル上に実装されるものである。ベースプロトコルの制御パケットが、ハッシュチェーン、デジタル署名、

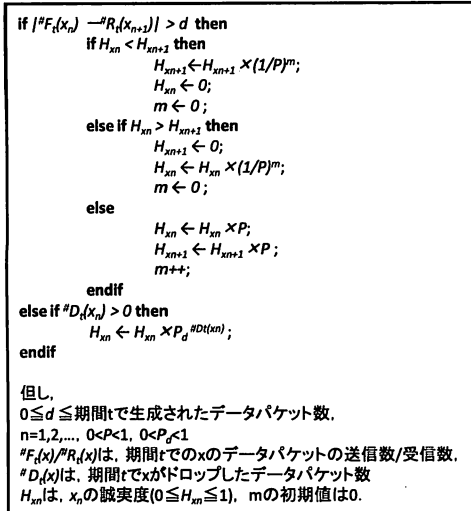


図 2 誠実度 H の下げ幅

メッセージ認証コード(MAC)、暗号化などによって否認防止・認証・完全性・秘匿性が保護されている場合は安全である。AODV-BDA が必要とする拡張領域と追加パケットは、多くのセキュアルーティングプロトコルと同様にデジタル署名やハッシュチェーン、MAC によって傍受、改ざん、偽造から守られていることとする。データは、IPsec などでは認証・完全性・秘匿性を保護する。

● **ルーティングループの作成** ルーティングループの作成には、最低二つの攻撃ノードが必要である。本稿では、共謀している攻撃ノードの存在を想定していないが、エンド間の ACK を使用することで回避可能である。ベースプロトコルでエンド間 ACK の使用することで対応可能である。

● **選択的なパケットの破棄(Black hole, Gray hole)** データパケットの流れの一貫性のチェックにより非共謀攻撃によるパケットドロップを検出できる。

● **パケットを遅らせる** 期間 t 毎にデータパケットの一貫性チェックを行っているため、パケットフォワーディングの時間が長い(t 以上)と一貫性に矛盾が生じ、パケットをドロップしていかなくても検出できる。

● **非最適経路でパケットをルーティングさせる** 攻撃ノードが意図的に主バックアップ経路以外の経路を使用した場合、転送されたノードが経路を保持していない場合はドロップし検出される。保持している場合は、その経路でルーティングするが攻撃ノードが共謀していないと大幅な遅延は発生しにくい。

● **経路を実際に短く/長くみせる** この行動の最終的な目的は攻撃者に経路を集める/攻撃者が経路に含まれないようにする(Selfish ノード)ことである。前者の場合、経路集中後パケットを破棄することが多い。この場合は、選択的なパケットの破棄と同様に検出できる。後者の場合は、ホップカウントにハッシュチェーンを用いることで、距離ベクトルベースのルーティングの場合は防ぐことができる。

3.2. 経路の作成

最短・準最短遅延経路の作成 フェーズで送信元と宛先間にマルチパスを作成する。この方法によるマルチパスの構築は AODV よりエンド間平均パケット到着遅延時間が短く、RERR 数が減少する^[22]。そのため、リアルタイム性を必要とするアプリケーションの QoS が向上する。

3.3. 攻撃の検出

ビザンチン攻撃の検出 フェーズではデータパケット数の

送受信に関する一貫性の監視を行う。今、ノード x_1 がデータパケットを期間 t で 4 つ受信したとすると x_1 は x_2 へフォワーディング($F_i(x_1 \rightarrow x_2, Data1)$)する(図 3a)。

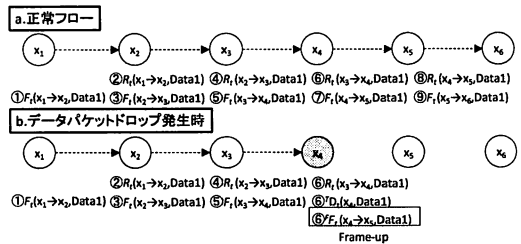


図 3 データパケットの流れ

x_2 はパケットを受信($R_i(x_1 \rightarrow x_2, Data1)$)し、 x_3 へフォワーディング($F_i(x_2 \rightarrow x_3, Data1)$)する。同様の処理を x_3 以降も行い最終的に宛先までデータを届ける。各ノードは、期間 t の間に処理したデータパケットについて、どのノードに対してどのような処理(F, R, D)を何度行ったか(F_i, R_i, D_i)を自身の RPRT に記録する。この RPRT を経路上の隣接、1hop 先のノードに報告する^{[25][26]}。既存方式では、ソースルーティングのため、経路上のノードは RPRT を送信元へフィードバックする必要があった^[19]。AODV-BDA では、攻撃ノードの周辺ノードが自身から 1hop 以内を監視対象とするので RPRT を素早く収集できる^{[25][26]}(図 4)。

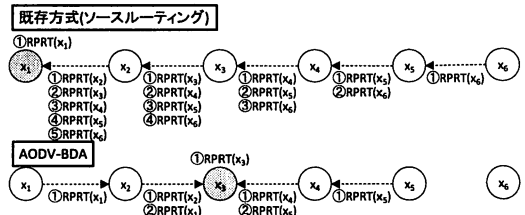


図 4 RPRT の流れ(x_3 への報告)

フォワーディング処理は極めて短い時間で行われるので、正常ならば期間 t での x_n の送信数と x_{n+1} の受信数は 4 となる($n=1, \dots, 5$)。しかし、モビリティ変化や攻撃が原因で x_4 がデータパケットをドロップした場合、 x_4 の受信数と送信数に差が生じ、その差はドロップ数($D_i(x_4, Data1)$)として x_4 はレポートで報告しなければならない(図 3b)。攻撃の場合、攻撃者は正直にドロップ数を報告する(自然にドロップしたことによる($D_i(x_4, Data1)$))か、以下のように自身がドロップしたこと隠蔽すること隠蔽すること^[19]。

● x_3 からパケットを受信していないことにする
● x_5 へパケットを送信したことによる($F_i(x_4 \rightarrow x_5, Data1)$)
後者は検出が困難^[19]とされているため、本稿は Frame-up を後者の行為とする。問題は、モビリティ変化やコリジョンによるドロップであり、この場合も攻撃とみなされるためこのままでは誤認率が増加する^{[25][26]}。AODV-BDA では、この問題を解決するために期間 t で送受信数の差 d は期間 t で生成されたデータパケット数を越えない(受け、差が d 以下の場合は H を下げないようにする(図 2)。

攻撃の検出をより早く回避に反映し、期間 t の間にあらゆる監視ノードで経路の切り替えが発生しても矛盾が生じないように、RPRT 中のデータパケットの送信元、送信先ノードを複数保持する^{[25][26]}(図 5a)。既存方式では、各ノードが期間 t で監視した結果を送信元までフィードバックしなければ経路切り替えができない^[19]。また、リンク間のパケットロス率が高いと送信元から離れるほど RPRT の到達率が低下し、最悪の場合検出に必要な監視情報が収集で

きなくなる(図 4)。AODV-BDA では、各ノードが独立に監視を行うため期間 t 内でも切り替えができ(図 5a)、さらに RPRT は最大でも 1hop しかないので、リンク間のロス率が高い場合でも高い確率で検出に必要な監視情報を収集できる(図 5b)。

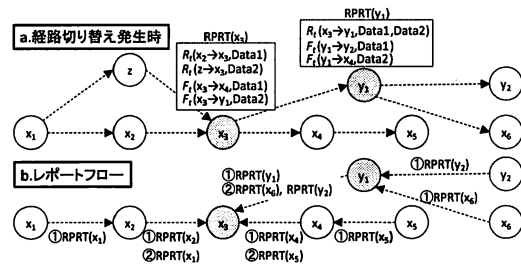


図 5 AODV-BDA での(RPRT)の構成と流れ

3.4. 攻撃の回避

ビザンチン攻撃の回避フェーズでは、検出されたノードへの経路を切断と経路の切り替えまたは経路の再構築を担っている。今、 x_3 がレポートを収集し送受信の一貫性の監視により x_4 を検出したとする(図 4)。既存方式では、送信元(x_1)は自身が保持する経路のうち攻撃者 x_4 が含まれていない経路に切り替える。この時、経路の切断は行わず x_4 が含まれる経路の採択確率を下げることで攻撃を回避する[19] (図 6)。AODV-BDA では、攻撃者 x_4 の隣接ノード x_3 が、自身が持つバックアップ経路のうち隣接が x_4 でない経路に切り替え回避する[25][26] (図 6)。AODV-BDA は、局所的に回避行動を取ることでハイモビリティへの適応性が高い。

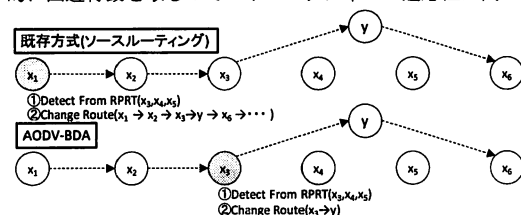


図 6 経路切り替え

4. シミュレーション

ネットワークシミュレータ ns2[24]と AODV-UU[23]を用いて、ビザンチン攻撃の一種である Grayhole がネットワークに存在する場合の AODV-BDA と AODV の性能を比較評価する。本稿では Grayhole ノードを、共謀せず経路上に自身が組み込まれるまではプロトコル準拠の動作を行い、データパケットを受信したときに破棄するという行動をとるものと定義する。また、不正リンクを長く保持させるため RERR の転送を行わない。シミュレーションパラメータを表 2 に示す。 t , $H_{threshold}$, P , P_d , d の条件は、図 2 に従う。それぞれ、監視サイクル(t)、データパケットの流れの一貫性チェック時の H の下げ幅に関するパラメータ(P)、データパケットドロップ時の下げ幅に関するパラメータ(P_d)、一貫性チェック時の許容値 d である。

4.1. 評価メトリック

性能を評価するため下記について計測を行った。計測は、トラフィックペアを変えた 20 回の平均値を用いた。

● **End to end packet delay (sec)** 送信元がデータパケットを生成してから宛先に届くまでの時間である。これは、攻撃ノードの検出と経路切り替えまたは経路再検索による回避行動にかかる時間を含んでおり、短いほど AODV-BDA の検出と回避行動が高速であることを示している。

表 2 シミュレーションパラメータ

トポロジ範囲	1000m × 1000m
シミュレーション時間	300sec
正常ノード数	100
Grayholeノード数	0-20 (1刻み)
トラフィックペア	1
ノード移動モデル	Random Way Point
最大移動速度	60km/h (ポーズタイム:0sec)
通信プロトコル	UDP(CBR,500byte,4 packets/sec)
帯域幅	2Mbps
無線伝達半径	約200m
保持経路数	3(主経路1,バックアップ経路2)
レポート生成間隔(t)	1sec
$H_{threshold}$	0.1
P	0.2
P_d	0.2
d	0-3

● **RPRT Transmissions** レポートパケット(RPRT)のトランスミッションである。トランスミッションとはリンクに流れたパケット数である。例えば、図 3 で x_1 から x_3 へパケットが流れるとトランスミッション数は 2 となる。これは、検出に必要な情報収集のためのオーバーヘッドである。

● **Precision & Recall of the Detection, fallout, F-measure** 検出性能を評価する為 Precision は、($True\ Detection$)/($True\ Detection + False\ Detection$)であり検出されたノードが真に攻撃ノードであった割合である(図 7)。Recall は($True\ Detection$)/($True\ Detection + Missed\ Detection$)でありどれだけ攻撃ノードを検出できたか(どれだけ見逃さなかったか)を示す(図 7)。fallout=($False\ Detection$)/($False\ Detection + True\ Detection$)であり、検出結果のうち正常なノードを検出してしまった割合である(誤認率に相当する)(図 7)。F-measure=($2 \times Precision \times Recall$)/($Precision + Recall$)の値が高ければ、検出性能が良いことを意味する。

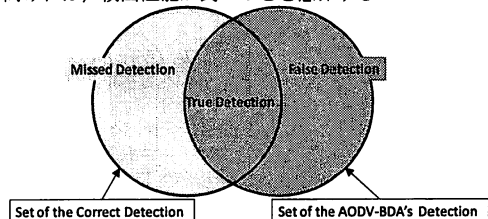


図 7 各検出の関係

● **Number of Drop packet (Data)** 攻撃によるデータパケットのドロップ数を明示したものである。

4.2. 結果と考察

4.1 での評価メトリックに基づいたシミュレーション結果とその考察を示す。

● **End to end packet delay (sec)** 図 8 より $d=0$ の時、 $d=1-3$ に比べ若干の増加が見られるが、その差は 0.01 秒以下であり AODV と比較しても約 0.02-0.04 秒高速である。また、Frame-up 時でも Frame-up しない場合とほぼ傾向は変わらなかった。攻撃ノード数が増加しても遅延が増加しないことから、AODV-BDA の攻撃の検出から回避行動までの時間が高速であることがわかる。結果、攻撃ノードが存在する状況でもリアルタイム性を必要とするアプリケーションの QoS が低下しない。

● **RPRT Transmissions** 図 9 より RPRT 数は 1hop 周辺のみで監視であるため、経路長や攻撃ノードの増加によらず約 2000 で大幅に増減することはない。また、Frame-up 時でも Frame-up しない場合とほぼ傾向は変わらなかった。従って、AODV-BDA の RPRT によるオーバーヘッドはノード数のスケ

ラビリティへの対応性が高いと言える。

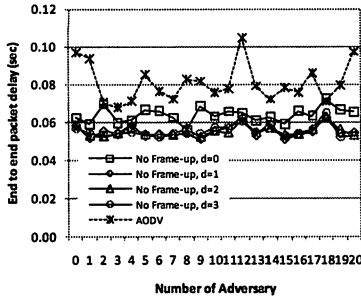


図 8 End to end packet delay (Frame-up なし)

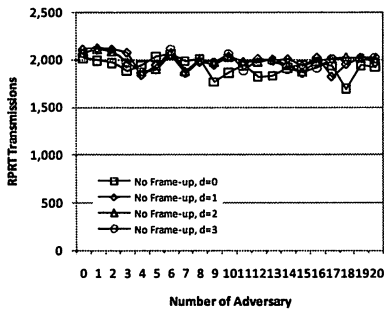


図 9 RPRT Transmissions (Frame-up なし)

● Precision & Recall of the Detection, fallout, F-measure 図 10 より Frame-up の有無に関わらず $d=0$ の時、攻撃ノードが少数の時ほど Precision が低下しており誤検出が多い。

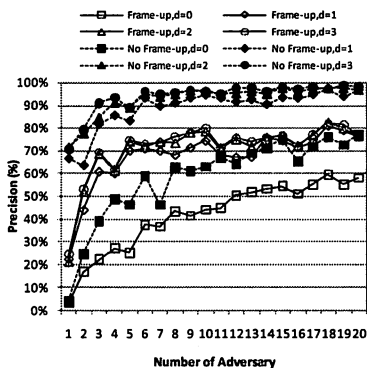


図 10 Precision

$d=1-3$ の場合は、Frame-up なし時で最悪でも 60%以上、Frame-up 時でも約 20-80%で大幅に改善されている。本稿のシミュレーション環境では、許容値 d が小さくても誤検出が大幅に抑えることができる。図 11 より Frame-up なし時の Recall は、70%以上であるが Frame-up 時は 40-60%で攻撃ノードを見逃すことが多い。これは、Frame-up によって攻撃ノードが特定しにくいためである。Frame-up 時で $d=0$ の場合に $d \geq 1$ に比べ若干高いのは、厳密に一貫性チェックを行うので過検出になる為である。但し図 10 からわかるように $d=0$ では誤検出が多い。よって、 $d=0$ での Recall の向上によるメリットよりも $d \geq 1$ での Precision の向上(誤検出の低減)のメリットの方が大きいと言える。図 12 より fallout は Frame-up なしで $d=0$ の時、 $d=1-3$ と比較して 20-60%

高く誤認率が高かった。 $d=1-3$ の間では大きな変化はなく、攻撃ノード数が少ないとき若干高いが、概ね 10%以下で良好である。Frame-up 時でも傾向は変わらないが、総じて 20%程の増加がみられる。 $d=0$ では、Frame-up の有無で 10-20%の差はあるが非常に高い(30-40%以上)。これは、一貫性チェックを厳密化することによって自然発生するドロップも攻撃とみなしてしまう割合が増加しているということである。許容値 d によって誤認を低下させることができるが、許容値 d は、モビリティや電波状況などを考慮に入れその時点で最適な値を選択する必要がある。

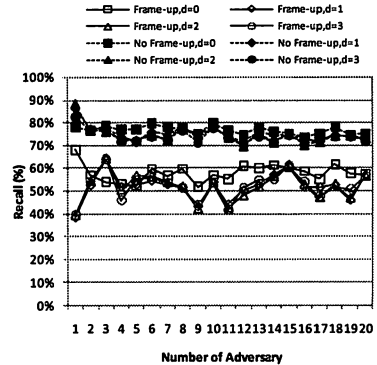


図 11 Recall

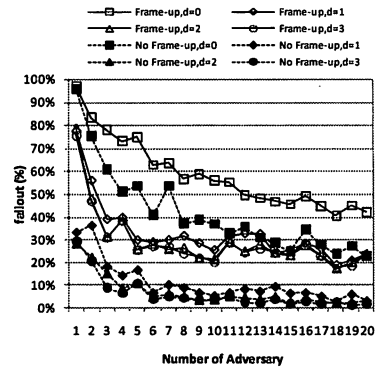


図 12 fallout

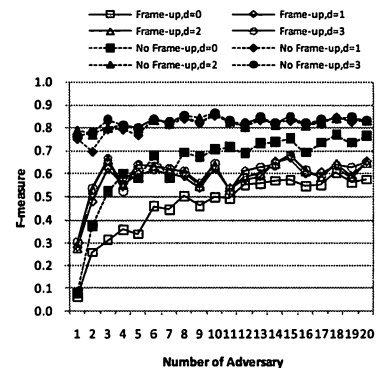


図 13 F-measure

図 13 より Frame-up なし時の F -measure は、 $d=1-3$ で約 0.8 を示し検出性能が高いことがわかる。Frame-up 時は 0.6 程度で誤検出が多いため低下する。 $d=0$ は、攻撃ノードが少数の場合に性能が極端に低下する。AODV-BDA は、 $d \geq 1$ で検出の正確さが約 70-90%以上であり、 $d=0$ と比較して $d \geq 1$ でも攻撃ノードを大幅に見逃すことがない。誤検出も $d \geq 1$ で概ね 10-39%以下に抑えられている。検出性能は $d \geq 1$ で 0.6-0.8 以上と良好である。本稿の環境では、 $d \geq 1$ で d による性能差は見られなかった。しかし、モビリティやパケット生成間隔などの環境を変更した場合はこの限りではないため許容値 d の動的な変更が必要であると考えられる。

● **Number of Drop packet (Data)** 図 14 より AODV と比較し AODV-BDA は攻撃によるドロップパケット数が約半分である。AODV-BDA でも攻撃ノードの増加に比例してドロップパケット数が増加するのは、各監視ノードが独立に攻撃ノードを見つけるため、経路(経路候補)に攻撃ノードが含まれる割合が高いほど検出回数が増加し、検出に伴うパケットドロップが発生する為である。

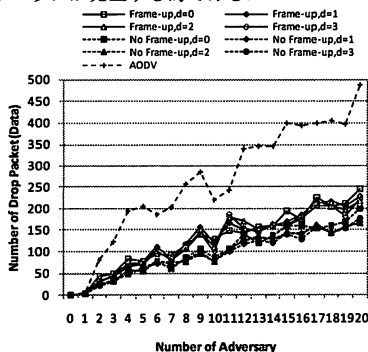


図 14 Number of Drop packet (Data)

上記の結果より、AODV-BDA は攻撃者がレポートの Frame-up をしない状況で特に良い性能であると言える。Frame-up をすると誤検出が多くなるが、実験結果より $d \geq 1$ で誤検出が大幅に改善される。パケット到着遅延は Frame-up の有無に関わらず AODV より短縮される。従って AODV-BDA の検出と回避行動が高速に行われていると言える。しかし、モビリティやパケット生成間隔などの環境を変更した場合はこの限りではないため許容値 d の動的な変更が必要であると考えられる。

5. まとめ

本稿では、非共謀ビザンチン攻撃ノードを検出し回避することを目的とする AODV-BDA を提案した。さらに許容値 d を設け、 d の値により誤検出が低下することをシミュレーションにより確認した。AODV-BDA では経路切り替えを経路上の中継ノードが独立に行うことにより、従来方式で問題であった検出から回避までの移行時間を短縮した。

今後は共謀している攻撃ノードの検出を考慮し、宛先がデータパケットに対する ACK を送信元へ送信する Secure Data Transmission(SDT)^[27]との連携やメッセージの完全性・認証方式の導入などが求められる。また、環境ごとに最適な許容値 d や誠実度 H に対する下げ幅のパラメータ P, P_d による性能変化を調査する必要がある。

参考文献

- [1] Argyrouridis, P.G. and O'Mahony, D., "Secure routing for mobile ad hoc networks." IEEE Communications Surveys & Tutorials. v7.
- [2] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures," WISE'02, Atlanta, Georgia, September 2002.

- [3] E. Fonseca, and A. Festag, "A Survey of Existing Approaches for Secure Ad Hoc Routing and Their Applicability to VANETS", Technical Report NLE-PR-2006-19, NEC Network Laboratories, March 2006.
- [4] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields and E.M. Royer, "A Secure Routing Protocol for Ad hoc Networks", Proc. 10th IEEE Int'l. Conf. Network Protocols (ICNP'02), IEEE Press, pp. 78-87, 2002.
- [5] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks," Proc. 8th ACM Int'l. Conf. Mobile Computing and Networking (Mobicom'02), Atlanta, Georgia, pp. 12-23, September 2002.
- [6] S. Buchegger, and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Ad hoc NeTworks)," Proc. 3rd Symp. Mobile Ad hoc Networking and Computing (MobiHoc 2002), ACM Press, pp. 226-236, 2002.
- [7] P. Golle, D. Greene, and J. Staddon, "Detecting and Correcting Malicious Data in VANETs", In Proceedings of the 1st ACM Workshop on Vehicular Ad Hoc Networks (VANET 2004), Philadelphia, PA, USA, pp. 29-37, October 2004.
- [8] M.G. Zapata, and N. Asokan, "Secure Ad hoc On-Demand Distance Vector Routing," ACM Mobile Computing and Communications Review, vol. 3, no. 6, pp. 106-107, July 2002.
- [9] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks," Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications, Calicoon, NY, pp. 3-13, June 2002.
- [10] P. Papadimitratos, and Z.J. Haas, "Secure Link State Routing for Mobile Ad hoc Networks," Proc. IEEE Workshop on Security and Assurance in Ad hoc Networks, IEEE Press, pp. 27-31, 2003.
- [11] S. Carter and A. Yasinac, "Secure Position Aided Ad hoc Routing Protocol", In Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN02), November 2002.
- [12] T. Clausen, C. Adjih, P. Jacquet, A. Laouti, A. Muhlethaler, and D. Raffo, "Securing the OLSR Protocol", In Proceeding of IFIP Med-Hoc-Net, June 2003.
- [13] S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad hoc Networks," Proc. 6th Annual ACM/IEEE Int'l. Conf. Mobile Computing and Networking (Mobicom'00), Boston, Massachusetts, pp. 255-265, August 2000.
- [14] P. Papadimitratos, and Z.J. Haas, "Secure Routing for Mobile Ad hoc Networks," Proc. Communication Networks and Distributed Systems, Modeling and Simulation Conf. (CNSD'02), San Antonio, Texas, pp. 27-31, January 2002.
- [15] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures," WISE'02, Atlanta, Georgia, pp. 21-30, September 2002.
- [16] S. Yi, P. Naldurg, and R. Kravets, "Security-Aware Ad hoc Routing for Wireless Networks," Proc. 2nd ACM Symp. Mobile Ad hoc Networking and Computing (MobiHoc'01), Long Beach, CA, pp. 299-302, October 2001.
- [17] R. Ramanujan, A. Ahamed, and K. Thurber, "Techniques for Intrusion Resistant Ad hoc Routing Algorithms (TIARA)," Proc. Military Communications Conf. (MILCOM 2000), Los Angeles, CA, pp. 660-664, October 2000.
- [18] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad hoc Networks," Proc. 22nd Ann. Joint Conf. IEEE Computer and Communications Societies (INFOCOM 2003), IEEE Press, pp. 1976-1986, 2003.
- [19] W. Yu, Y. Sun, and K. J. R. Liu, "HADOF: Defense against routing. disruptions in mobile ad hoc networks," in IEEE INFOCOM, Miami, FL, March 2005.
- [20] 鎌田 美緒, 小口 正人, "マルチホップ無線ネットワークにおけるセキュアコネクション管理モデルの提案と実装", 第 17 回電子情報通信学会データ工学ワークショップ (DEWS 2006) 論文集, 2006 年 3 月.
- [21] 森井 健之, 谷山 健太, 甲藤 二郎, "アドホックネットワークにおけるオンデマンド型マルチパスルーティングプロトコル実装", 電子情報通信学会通信ソサエティ大会 2004.
- [22] 谷山 健太, 櫻井 祐介, 甲藤 二郎, "アドホックネットワークにおけるディスタント・マルチパスルーティング", 電子情報通信学会通信ソサエティ大会 2005.
- [23] AODV-UU, <http://core.it.uu.se/adhoc/AodvUUIImpl>.
- [24] Network Simulator version 2(ns-2), <http://www.isi.edu/nsnam/ns>.
- [25] 森 郁海, 森 拓海, 高橋 修, "アドホックネットワークにおける攻撃法・防御法の分類と AODV ベースセキュアルーティングプロトコルの提案", MBL41 2007.
- [26] 森 郁海, 森 拓海, 高橋 修, "AODV ベースセキュアルーティングプロトコルの提案とその実装・評価", DICOMO2007 2007.
- [27] P. Papadimitratos and Z. Haas, "Secure data transmission in mobile ad hoc networks," in 2nd ACM Workshop on Wireless Security (WiSe), 2003.