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

2007－ＭＢＬ－41（16）
2007／5／18

# 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

森 郁海† 森 拓海† 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 〒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 システム情報科学部 〒041-8655 北海道函館市亀田中野町116-2

**概要** アドホックネットワークには様々な攻撃が存在し，その対処法も多岐にわたっている．アドホックネットワークにおける攻撃法の分類は，攻撃体系をモデル化するとともに，汎用的な防御法を考える上でも重要である．本稿では，現存する主な攻撃を9形態・各々1～2段階の樹形図に分類しその攻撃特性を判断し，有効とされる防御法をピックアップする．さらに，汎用的な防御法の考察に当たり，カバーしなければならない攻撃形態を選択し，要求条件を明確化する．検討に当たっては，ネットワークレイヤ以外の各レイヤに依存する防御法については前提条件として定めるほか，暗号化及び認証技術は存在するものとして考える．そして，汎用的な防御法としてHADOFの技術を基に，パケット監視・レポートの交換・信頼度の設定などに注目したAODVベース(hop by hop)のルーティングプロトコルで動作する汎用防御法を提案する．本提案防御法は，①バックアップルートの作成②データパケットの監視③レポートを1ホップさせること(1ホップレポート法)により frame-up 攻撃を防ぎかつパケットの監視が可能となることが特徴であり，HADOFの核となる技術を踏襲した攻撃ノード検出技術を実現する．

**キーワード** HADOF, report, AODV, hop by hop, バックアップルート, 1ホップレポート法

# Classification of Attacks and Defense method and Proposal of AODV-based Secure Routing Protocol in Mobile Ad Hoc Networks

Ikumi Mori† Takumi Mori† Osamu Takahashi‡

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

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

**Abstract** There are many Attacks and its Defense method in Mobile Ad-hoc Networks (MANET). Classification of Attacks in MANET is useful for Attack modeling and it is important to learn a versatile Defense method against various Attacks. In this Paper, we make a treelike diagram constructed 9 patterns and 1 or 2 levels for each pattern, and get characteristic features of Attacks at this treelike diagram. We also make a similar tree diagram for Defense method against 9 patterns of Attacks. After definition of 9 patterns and classification of Attacks, we consider picking up patterns of Attacks that must be covered for create a proposal versatile Defense method. We set up an encryption and authentication technology as a prerequisite for proposal Defense method, and out of consideration except for Network layer. Our proposal Defense method based on data packet monitoring, exchanging report and compute honesty score in HADOF operate with hop-by-hop routing protocols, and has mainly 3 processes; ①create Backup route, ②monitoring data packet, ③create a report included monitoring data packet and send it to 1 hop ahead. Each node can detect frame-up attack and monitoring relation among itself to neighbor node to next node of neighbor node because of these processes.

**Keyword** HADOF, report, AODV, hop-by-hop, Backup route, Source route list, 1 hop report method

## 1. はじめに

近年，ネットワークの形態は多様化しているが次世代ネットワークとして注目されている技術として，アドホックネットワークが挙げられる．アドホックネットワークの普及につれ，そのセキュリティ対策が重要視されることは明白である．アドホックネットワークにおける攻撃及び防御法は，多岐にわたり多くの研究はひとつの攻撃法に対する防御法の提案を対象としている．一方，汎用的な防御法として知られているHADOF[1]は，ソースルーティングベースのアドホックルーティングプロトコルでなければ動作しない．ソースルーティングでは，送信元が経路を完全に指定するため中間ノードでリンクの切断が生じると送信元までその報告を行わなければならず，高移動性環境に弱いとされている．しかしながらHADOFで用いているRoute Traffic Observerの原理やレポートの交換，マルチパス化，ルート採択メトリックなどは非常によく，watchdog[2]やpathrater[2]よりもルーティングオーバヘッドやパケットのドロップ率を低下させている．

本稿では高移動性環境に強いAODV[1]を用いて，HADOFで提案されているレポートの交換を主体とした汎用的な防御法を提案する．提案手法が汎用的であるかを検証するため，まず既存のアドホックネットワーク上での攻撃法を9形態に分け，各々1～2段階の樹形図を作成する．そして，この9形態の特性に着目し現在有効だとされている防御法の中から適切なものをピックアップし，9形態にそれぞれ対応するように防御法を分類する．このようにして作成した分類図を元に，前提条件を定め提案手法がどの攻撃部分に対応すればよいかを定める．

3章では，アドホックネットワークにおける攻撃法の分類を行い4章では防御法についても同様に述べる．5章では，詳細な攻撃分類の定義を述べ，6章でAODVベースルーティングプロトコルにおける汎用的な防御法のモデルを提案する．

## 2. 関連研究

既存の攻撃法を分類した主な研究は，以下のようなものがある．

### 2.1 Ad-hoc Network Specific Attack [3]

A.Burg[3]は，アドホックネットワーク上の攻撃を4つのクラス分けによって分類している:①攻撃ノードが存在する位置によってネットワーク外部/内部のように分類，②受動的/能動的な攻撃に分類，③攻撃がどのネットワークレイヤに対するものかで分類，④セキュリティ課題(アプリケーション/プライバシ要件)によって分類．また，攻撃タイプを7つに分類しその攻撃をモデル化した形で定義している．大枠として本論文は継承しているが，攻撃形態にまだもれがある．

### 2.2 Vulnerability of Wireless Routing Protocols [4]

Qifeng Lu [4]は，ワイヤレスルーティングプロトコルの脆弱性を述べている．中でもモバイルアドホックネットワークを脆弱性の最も高いネットワークと位置づけ，弱点をピックアップしている．攻撃を能動的/受動的攻撃に分類し，具体的な攻撃方法も多数紹介している．またAODV,DSRで攻撃可能な攻撃方法を検証している．最後に，セキュリティ評価基準と可能なセキュリティ要件を作成している．非常に攻撃方法や防御方法が充実しているが，防御法の実装方法やframe-up攻撃については触れられていない．

### 2.3 Secure Ad hoc On-Demand Distance Vector Routing [5]

AODV に公開鍵暗号によるセキュリティ向上を述べたインターネットドラフトである．主に，公開鍵の配布方法ヘッダ情報の定義や認証の仕方が述べられており，AODV におけるパケット認証を可能にしている．認証は，攻撃者の特定・ヘッダ情報の改ざんを困難にする

重要な防御法の一つである.

## 3. アドホックネットワークにおける攻撃法の分類[3][4]

アドホックネットワーク上での攻撃法を分類するが, ここではノードの移動をほとんど考慮しないプロアクティブ型のルーティングプロトコルは対象としないことにする. 攻撃法の分類を図 1に示す. 攻撃を単純にモデル化した場合に類似した振る舞いを行うものを同一形態として分類し, 細かな攻撃動作を数段階のパターンに分けたものである. 注意したいのは, ある攻撃法があったときこの分類図の一つのリーフに帰着するのではなく複数のリーフの特性を持つ場合があるということである. 例えば一般的なブラックホール攻撃を行う場合には, 攻撃者は自身の存在を隠し攻撃を行うので「なりすまし型」+「落とし穴型」というような特性を持つ.

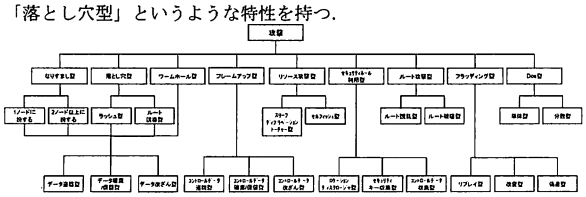

図 1 アドホックネットワークでの攻撃法の分類図

## 4. アドホックネットワークにおける防御法の分類[3][4]

攻撃法の分類を基に, 防御法を分類する. 図 1の 9 形態の攻撃分類に対応した防御法の分類を図 2に示す.

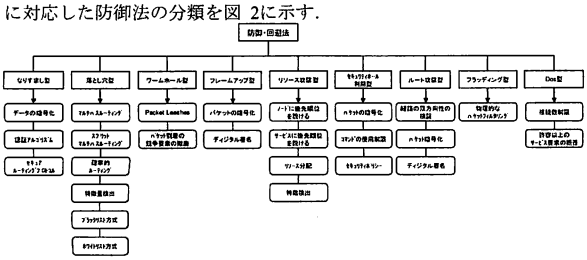

図 2 アドホックネットワークでの防御法の分類図

## 5. 攻撃法及び防御法の詳細な定義

既存の攻撃法の分類及び防御法[3][4]は, 攻撃がどのネットワークレイヤに位置するか, 攻撃者のポジション(ネットワーク内/外)はどこか, 攻撃者が積極的に攻撃をするか/受動的なものか, セキュリティ用件がどこに依存するか(アプリケーション/セキュリティポリシー)などに分類されていた. しかし, アドホックネットワーク上(特にリアクティブ型)での攻撃の場合, ネットワークトポロジが頻繁に変化する環境を利用した攻撃が脅威となる場合が多い. そこで本稿では, 既に攻撃者が経路上にいた前提での攻撃にネットワーク形成段階での攻撃をプラスすることでアドホックネットワーク特有の攻撃に特化した分類を提案する. この章では攻撃法の 9 形態を詳細に定義する. 以下は「攻撃形態名」「攻撃形態図」「攻撃例」「防御例」の順に 9 形態の定義を説明する.

### 5.1 なりすまし型

#### 5.1.1 定義

**単体データ-破棄/保留型**

アタッカーは 1 つのノードになりすます. 送信者または宛先からその存在を知られてはならない. 受信したデータは破棄または保留し, 送信者との通信を行う.

**単体データ-盗聴/改ざん型**

アタッカーは 1 つのノードになりすます. 送信者または宛先からその存在を知られてはならない. 受信したデータは盗聴または改ざんされ, 送信者と宛先の中継を行う. アタッカーは送信者からは宛先のように見え, 宛先からは送信者のように見えるようなりすましている.

**複数体データ-破棄/保留型**

アタッカーは複数のノードになりすます. 送信者または宛先からその存在を知られてはならない. 受信したデータは破棄または保留し, 送信者との通信を行う.

**複数体データ-盗聴/改ざん型**

アタッカーは複数のノードになりすます. 送信者または宛先からその存在を知られてはならない. 受信したデータは盗聴または改ざんされ, 送信者と宛先の中継を行う. アタッカーは送信者からは宛先のように見え, 宛先からは送信者のように見えるようなりすましている.

#### 5.1.2 形態

なりすまし型の攻撃形態を図 3に示す. 単体-データ破棄/保留型, 単体-データ盗聴/改ざん型, 複数体-データ破棄/保留型, 複数体-データ盗聴/改ざん型の 4 態が存在する.

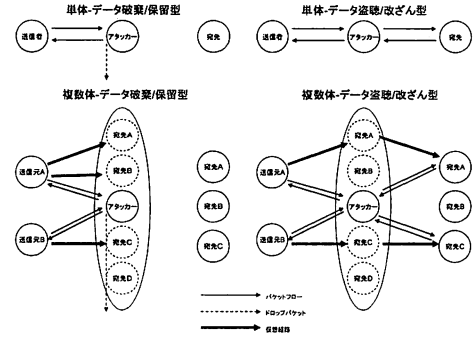


図 3 なりすまし型の攻撃形態図

#### 5.1.3 攻撃例

具体的な攻撃例として Man-in-the-middle 攻撃, スプーフィング, Sybil 攻撃などが存在する.

#### 5.1.4 防御法

既存の防御法として有効とされるものは, データの暗号化, 認証アルゴリズムの利用, セキュア・ルーティング・プロトコルの利用などである.

### 5.2 落とし穴型

#### 5.2.1 定義

**ルート誘導[a]-データ破棄/保留型**

アタッカーが隣接ノードからの経路またはトラフィックを引き寄せる. アタッカーが受信したデータは破棄または保留される. 他の攻撃の前段階である.

**ルート誘導-データ盗聴/改ざん型**

アタッカーが隣接ノードからの経路またはトラフィックを引き寄せる. アタッカーが受信したデータは改ざんまたは盗聴され, 宛先ノードへ中継される.

**ラッシュ[b]-データ破棄/保留型**

アタッカーはラッシュにより自分が中継するようになったパケットを破棄, または保留する. 他の攻撃の前段階である.

**ラッシュ-データ盗聴/改ざん型**

アタッカーはラッシュにより自分が中継するようになったパケットを盗聴, または改ざんする. アタッカーが受信したデータは改ざんまたは盗聴され, 宛先ノードへ中継される.

#### 5.2.2 形態

落とし穴型の攻撃形態を図 4に示す. ルート誘導-データ破棄/保留型, ルート誘導-データ盗聴/改ざん型, ラッシュ-データ破棄/保留型, ラッシュ-データ盗聴/改ざん型の 4 態が存在する.

#### 5.2.3 攻撃例

具体的な攻撃例として, ブラックホール攻撃, ラッシング攻撃, 協力的ブラックホール攻撃, グレイホール攻撃[6] などが存在する.

#### 5.2.4 防御法

既存の防御法として有効とされるものは, マルチパス・ルーティング, スプリット・マルチパス・ルーティング(SMR)[7], 確率的ルーティング, 特徴量検出, ブラックリスト方式, ホワイトリスト方式などである.

---

a) ルートの誘導とは, アタッカーが周囲のノードに対し, 自分を中継するようなルートの構築または再構築を促すことを言う. 例えば, 距離ベクトル改ざん[4](距離ベクトルを実際の距離より長くまたは短くすることで自分へのルート作成を優先させる)やシーケンス番号の改ざん[4](シーケンス番号を高くすることで, 自身のルート作成要求を採択されやすくする)がある.

b) ラッシュは, オンデマンド・ルーティングにおけるループ回避の機能を利用する. ネットワーク内のノード密度が高い場合に正常なノードは同じパケットを処理しないための検査を行う. その際にネットワーク内のノード密度が低い場合に比べ, データホップに遅延(通常の 3 ノード 2 ホップ分ほどの時間)が生じる. アタッカーはこの遅延が生じないように最速でフォワーディングを行う. 従って宛先までの経路にアタッカーが含まれる確率を上げる. この経路が採択された場合, 真の経路要求は処理されない.

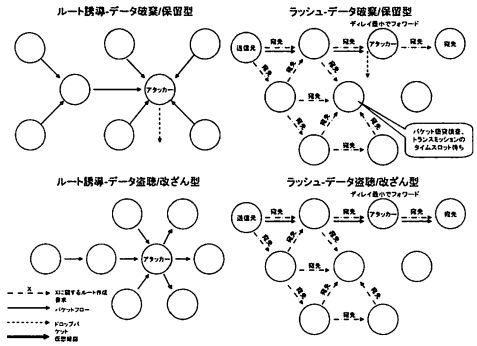


図 4 落とし穴型の攻撃形態図

## 5.3 ワームホール型

### 5.3.1 定義

**データ破棄/保留/盗聴/改ざん型**

外部パスにより送信元から宛先へのルートを短縮する．アタッカーは外部リンクへデータをフォワードする役目と外部リンクからデータを受信する役目の少なくとも 2 ノードが必要となる．ワームホール自体に有害ではない．一般的にはデータが到着するのが早くなる．またプロトコルや使用しているサービスに依存せずに攻撃が可能である．ルーティングメカニズムの混乱を狙う．距離ベクトルルーティングへの影響が強い．

### 5.3.2 形態

ワームホール型の攻撃形態を図 5に示す．データ破棄/保留/盗聴/改ざん型の 1 態が存在する．

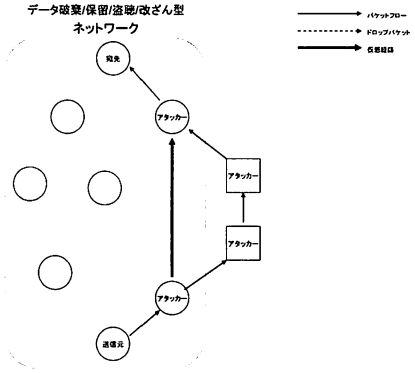


図 5 ワームホール型の攻撃形態図

### 5.3.3 攻撃例

具体的な攻撃例として，ワームホール攻撃が存在する．

### 5.3.4 防御法

既存の防御法として有効とされるものは，Packet Leashes，パケットの到着に関する競争要素をなくすなどである．

## 5.4 フレームアップ型

### 5.4.1 定義

**コントロールデータ破棄/保留型**

コントロールデータのやり取りによってノード間が情報を共有する場合，アタッカーはそのコントロールデータを破棄あるいは保留することで情報の共有を阻害することが出来る．

**コントロールデータ盗聴/改ざん型**

コントロールデータのやり取りによってノード間が情報を共有する場合，そのコントロールデータの内容が正しいかどうかを検証することが出来ない．アタッカーは，自身のコントロールデータをフレームアップ(でっち上げ)することによって誤った情報を周辺ノードに通知することによりルート採択などのメトリックに影響を与えることが出来る．

### 5.4.2 形態

フレームアップ型の攻撃形態を図 6に示す．コントロールデータ破棄/保留型，コントロールデータ盗聴/改ざん型の 2 態が存在する．

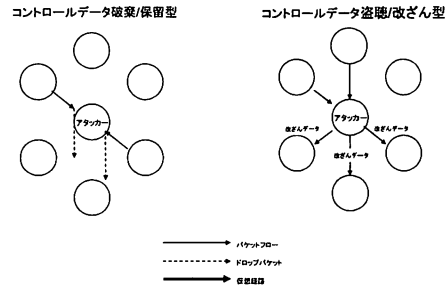


図 6 フレームアップ型の攻撃形態図

### 5.4.3 攻撃例

具体的な攻撃例として，frame-up 攻撃が存在する．

### 5.4.4 防御法

既存の防御法として有効とされるものは，パケットの暗号化，ディジタル署名などであるが，アタッカー自身のコントロールパケットが偽装された場合は防ぐことは出来ない．

## 5.5 リソース攻撃型

### 5.5.1 定義

**スリープ・ディプリベーション・トーチャー型**

アドホックネットワーク内のモバイルノードに特徴的な限りある資源を乗っ取る．アタッカーはターゲットに対し次々にサービス要求をかけ，アイドル状態やバッテリ休止状態にさせないようにする．制限のある資源を奪うためにネットワークにダメージが与えられ，本当に接続したいノードが隠されてしまう．

**セルフィッシュ型**

モバイルアドホックネットワークにおいて，自身に関連するパケットのみを処理しフォワーディングなどの中継およびルート検索行為を行わないことによりアタッカーはバッテリや計算資源を節約する．

### 5.5.2 形態

リソース攻撃型の攻撃形態を図 7に示す．スリープ・ディプリベーション・トーチャー型，セルフィッシュ型の 2 態が存在する．

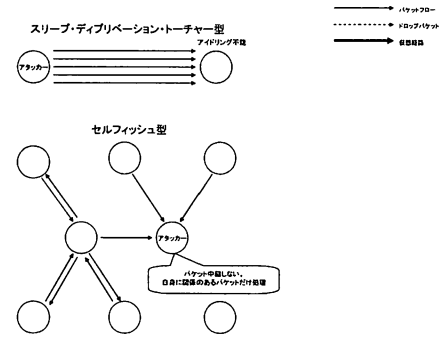


図 7 リソース攻撃型の攻撃形態図

### 5.5.3 攻撃例

具体的な攻撃例として，スリープ・ディプリベーション・トーチャー，セルフィッシュ・ノードなどが存在する．

### 5.5.4 防御法

既存の防御法として有効とされるものは，ノードに優先順位を設ける[c]，サービスに優先順位を設ける[d]，リソース分配[e]，特徴検出[f]などである．

---

c) 優先順位の低いノードからの接続要求またはサービス要求によって妨害されることはない．優先順位の高いノードにはより多くの資源が割り当てられ，資源の追加要求が優先される．

d) 優先順位の低いサービスからの要求によって妨害されることはない．優先順位の高いサービスにはより多くの資源が割り当てられ，資源の追加要求が優先される．

e) 固定割合または動的に資源利用の上限を決め，各ノードに資源を割り当てる．

f) 悪意のあるノードに対し，周囲のノードがその特徴（パケットの流れなど）を検出する．セルフィッシュ・ノードの場合，RREQ などを中継しているかを見ることで，ノードの特性を得ることができる．

## 5.6 セキュリティホール利用型

### 5.6.1 定義

**ロケーション・ディスクロージャ型**

アタッカーは traceroute コマンドなどを用い，自分までのルートのホップ数や中継ノードの情報を得る．アタッカーはこの情報を元にさまざまな攻撃を行う．

**セキュリティキー収集型**

セキュアネットワーク内で攻撃する際に必要なセキュリティキーやパスワード（パスフレーズ）などを収集する．アタッカーは収集したキーを用いてセキュアネットワークに侵入し，さまざま攻撃を行う．

**コントロールデータ収集型**

アタッカーはルーティング指標となるデータを収集する．収集したデータはさまざまな攻撃に利用される．例えば距離ベクトルルーティングならば周囲のノードのホップカウントを知ることにより，ROUTE REQUEST に対し周囲のノードよりもより小さいホップカウントに偽造した ROUTE REPLY を返信することで，自分へのルートを形成させることができる．

### 5.6.2 形態

セキュリティホール利用型の攻撃形態を図 8に示す．ロケーション・ディスクロージャ型，セキュリティキー収集型，コントロールデータ収集型の 3 態が存在する．

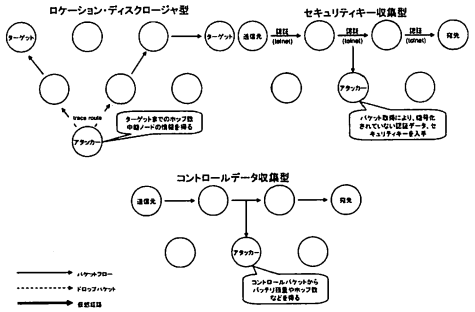


図 8 セキュリティホール利用型の攻撃形態図

### 5.6.3 攻撃例

具体的な攻撃例として，ロケーション・ディスクロージャ[4]，パケットスニッフィングなどが存在する．

### 5.6.4 防御法

既存の防御法として有効とされるものは，パケットの暗号化，コマンド使用制限[g]，セキュリティポリシーを設ける[h]などである．

## 5.7 ルート攻撃型

### 5.7.1 定義

**ルート撹乱型**

アタッカーは隣接ノードに不正なルートを形成させる．不正なルートに送信されたデータパケットはドロップしてしまう．アタッカーはデータパケットに直接触れることはない．

**ルート破壊型**

アタッカーは隣接ノードが保持しているルーティングテーブルのエントリ（ノードリスト）を破壊または使用不能することによりそのルートを使用不能にする．破壊されたルートは修復されるか再構築されるが再び攻撃を受けることにより通信不能に陥る．アタッカーはデータパケットに直接触れることはない．

### 5.7.2 形態

ルート攻撃型の攻撃形態を図 9に示す．ルート撹乱型，ルート破壊型の 2 態が存在する．

### 5.7.3 攻撃例

具体的な攻撃例として，Ghost Attack[8]，False route error[9]などが存在する．

### 5.7.4 防御法

既存の防御法として有効とされるものは，経路の双方向性を検証する[i]，パケット暗号化，ディジタル署名[j]などである．

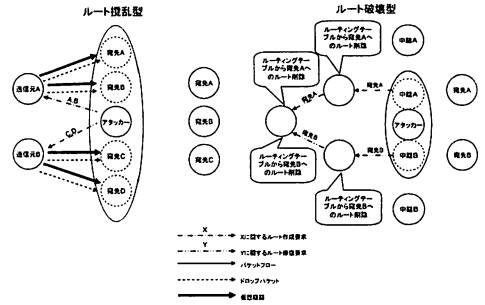


図 9 ルート攻撃型の攻撃形態図

## 5.8 フラッディング型

### 5.8.1 定義

**リプレイ/改変/偽造型**

他の攻撃の後段階に行われる．

**(1) ブロードキャスト**

アタッカーは特定のパケットを複製/改変または架空のパケットを生成し周辺のノードへブロードキャストする．それがルート検索要求の場合はクエリが次々にフォワードされネットワーク上にパケットが大量に発生する．これらのパケットが帯域幅以上に達すると通信不能に陥る．被害はネットワークの広範囲に及ぶ．

**(2) 宛先指定**

アタッカーは特定のパケットを複製/改変または架空のパケットを生成し特定のノードへ連続的に送信する．たくさんのパケットをターゲットに送る．アタッカーの周囲にパケットが溢れ返ることによりその一帯は通信不能に陥る．ただし，パケットはフォワードされないためアタッカーの周囲のノードのみが被害を受ける．

**(3) ピンポイント**

ネットワーク上のボトルネック（経路が集中しているノード）に対し，大量のパケットを送信することによりネットワークの一部を通信不能状態にする．負荷分散が適切になされていないルーティングプロトコルで発生する．

**(4) 連鎖型**

アタッカーは経路検索要求など，周囲のノードに対し連鎖的にパケットが発生するパケットを送信する．例えば存在しないノードへの ROUTE REQUEST(RREQ)パケットをアタッカーが送信した場合，アタッカーからの RREQ パケットを受け取った周囲のノードはさらに経路を検索するために RREQ パケットを周囲のノードに送信する．その繰り返しによりネットワーク上に RREQ パケットが溢れかえってしまい通信不能に陥る．

### 5.8.2 形態

フラッディング型の攻撃形態を図 10に示す．リプレイ/改変/偽造型の 1 態であるが，4 つのフラッディング方法が存在する．

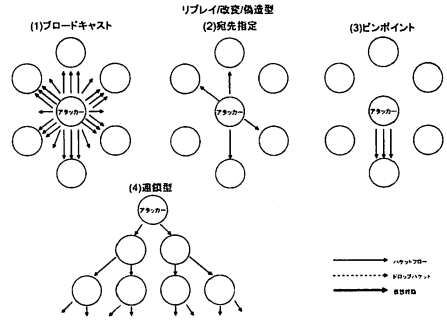


図 10 フラッディング型の攻撃形態図

g) 意図的に情報が引き出せるコマンドを制限する．ルーティングプロトコル内での制限はできないため，OS やサービスで制限をかける必要がある．

h) セキュリティキー管理のガイドラインの作成，情報の漏れにくいシステムの構築，個人（ノード）情報の公開/非公開の定義などを設ける．

i) TCP ならばデータパケットに対する ACK を監視することにより，経路が双方向に形成されていることを確認する．

j) パケットの改ざんの予防をする

#### 5.8.3 攻撃例

具体的な攻撃例として，選択的フォワーディング，頂点カット，パケットリプレイ，帯域幅消費，パケットクローニング，Malicious route request[4]などが存在する．

#### 5.8.4 防御法

既存の防御法として有効とされるものは，物理的なパケットフィルタリング，一定時間内に特定のノードからのパケットを制限するなどである．

### 5.9 Dos 型

#### 5.9.1 定義

**単体型**

**(1) 宛先指定**

アタッカーは特定のノード(１つ)に大量のサービス要求をかけ，ターゲットをリソースフロー状態に陥らせる．攻撃されたノードはサービスが利用できなくなる．主に接続要求パケットが用いられる．

**(2) ブロードキャスト**

アタッカーは周囲のノードに大量のサービス要求をかけ，ターゲットをリソースフロー状態に陥らせる．宛先指定型とは使用するパケットが異なる．主にルート作成要求や Hello パケットが用いられる．

**分散型**

１つのターゲットに対し，複数のアタッカーが同時に（正常な）サービス要求をかける．それによりターゲットに許容以上の負荷をかけ，サービスを停止させる．

#### 5.9.2 形態

Dos型の攻撃形態を図 11に示す．単体型，分散型の 2 態が存在する．特に単体型は 2 つのサービス要求の仕方がある．

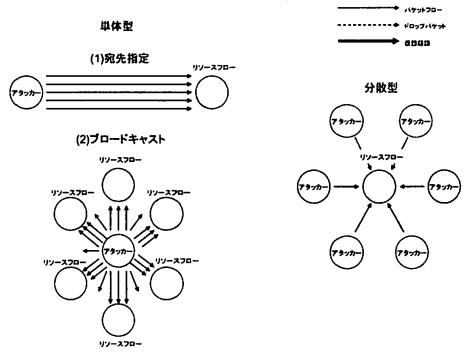


図 11 Dos 型の攻撃形態図

#### 5.9.3 攻撃例

具体的な攻撃例として，DoS攻撃（サービス拒否攻撃），DDoS攻撃（分散サービス拒否攻撃），ルーティングテーブル・オーバーフロー[k]などが存在する．

#### 5.9.4 防御法

既存の防御法として有効とされるものは，接続数に制限を設ける，許容以上のサービス要求を拒否するなどである．

## 6. 汎用的な防御法の検討

### 6.1 基本方針

耐攻撃性を検討するに当たり，2 つのアプローチが考えられる．一つは攻撃の回避を目的とした耐攻撃性ルーティングプロトコルを作成するもの，他方は既存のルーティングプロトコル上で動作する防御機構の開発である．本稿では，既にRFCにより標準化されたAODV[10]があることから後者に着目し，既存のルーティングプロトコル上で動作する汎用防御法を提案する．汎用的な防御法として有名なHADOFは，各ノードのパケットのドロップ状態を監視している．後述の前提条件から除外された攻撃を簡単化した場合，最終的にはパケットを破棄するしかないという結論を得ることが出来る．従ってHADOFの手法は，前提条件下では汎用防御法として有効である．しかし，HADOFのようなソースルーティングベースで動作する防御法の場合，hop by hopのルーティングプロトコルで動作しない．一方hop by hopのルーティングプロトコル上で動作する防御法の場合は，ソースルーティングベースのルーティングプロトコルでも動作可能でありより汎用性が高いといえる．本稿では，このHADOFに着目しその核となる技術をAODVに適用する事により汎用的な防御法を提案する．

### 6.2 前提条件

HADOF とほぼ同等な防御を実現するために前提条件も HADOF の動作環境と同様とする．

**(1) 物理・MAC 層の条件**

ノードはネットワーク領域内を自由に移動できるものとする．また，互いのノードは無線通信によりリンクすることができる．このリンクは双方向でなければならないが，互いの帯域幅が同等である必要はない．特別な用件として，互いの無線通信範囲内にいる隣接ノードとは直接通信が行えるものとする．そして無線通信のアクセス制御方式はCSMA/CA を用いることとし，MAC 層でのデータ送信確認(ACK)が存在するものとする．但し，物理・MAC 層においては改竄不可能なものとする．従って物理・MAC 層に対する攻撃は対象とせず，ネットワーク層のみの攻撃に限定する．「DOS」「フラッディング」は基本的に不可能とする．

**(2) 公開鍵・秘密鍵によるパケットの暗号化及び署名**

全てのノードは一つの Authority に属す．これは，ネットワークを一定の範囲に限定することを意味する．この Authority 内では，各ノードが公開鍵を所持しているか，またその鍵が正しいかの認証を行う．これによって公開鍵-秘密鍵の一意性が保たれる．そして各ノードは，自身に関する公開鍵・秘密鍵を所有する．ノードの公開鍵は IP アドレスなどのノードを識別できる ID から生成される．つまり署名認証時には署名したノードが判明するようになっている．各ノードは，他のノードの公開鍵を知っているものとし，それを使って認証できるものとする．また秘密鍵は漏洩しないものとする．送信元は，全てのデータパケットに対し暗号化をし，ヘッダを含むパケット全体に対して署名を行い宛先へ送信する．送信元と宛先は，信頼関係が成り立っているものとしなりすましは不可能とする．

以上よりネットワーク攻撃の中の「なりすまし」「パケットの盗聴」「パケットの改ざん」は不可能である．また一定のセキュリティポリシーが設けられ人的ミス，OS や通信環境のセキュリティホールはないものとする．よって「セキュリティホール利用型」の攻撃も不可能とする．「フレームアップ」に関しては HADOF 同様に，本提案防御法で対応する．

### 6.3 対象とする攻撃

対象とする攻撃は上記の前提条件から除外された以外の攻撃方法である．ジャミングなどの物理層や MAC 層に影響を及ぼす攻撃に関しては，防御法も物理的なものとなるので考慮しないこととする．従って，ネットワーク層での攻撃のみに限定する．対象とする攻撃方法の具体的なものは以下の通りである．

- ラッシングによるルート誘導(落とし穴型前段階)
- ブラックホール攻撃(落とし穴型)
- グレイホール攻撃(落とし穴型)
- ワームホール攻撃(ワームホール型)
- セルフィッシュ・ノード(リソース攻撃型)
- frame-up 攻撃(フレームアップ型)

「落とし穴型」「ワームホール型」は最終的にはパケットを破棄することしか出来ないためパケットの監視を行うことで検出可能となる．「リソース攻撃型」は，積極的な検出は出来ないが既に攻撃者への経路が出来ており，攻撃者がパケットを受信しないなどの行動をとった場合は検出が可能となる．

### 6.4 提案防御法の位置づけ

本提案防御法は，リアクティブ型ルーティングプロトコルでノード間の通信が双方向リンクを持つものであれば適用可能である．そして前述の対象とする攻撃の全てに対応する．その位置付けは図 12のようになる．

### 6.5 提案防御法のアルゴリズム

本提案方式は，HADOF の特徴的な検出技術であるレポートの交換と信頼度の設定に着目する．HADOF と異なり送信元が一括してレポートを管理・チェックし検出するのではなく，経路上の攻撃ノードの隣接ノードが検出することとなる．従って，レポートの管理・チェックは常に経路上のノードが行わなくてはならない．また，hop by hop のルーティングプロトコルではマルチパス化が困難であるため再検索による経路の再構築が主となる．従って，経路クオリティは無く信頼度のみで検出する方法をとる．

k) ルーティングテーブルのライフタイムを長くすることでルーティングテーブルのエントリから削除されないようにして，ルーティングテーブルをオーバーフローさせる．

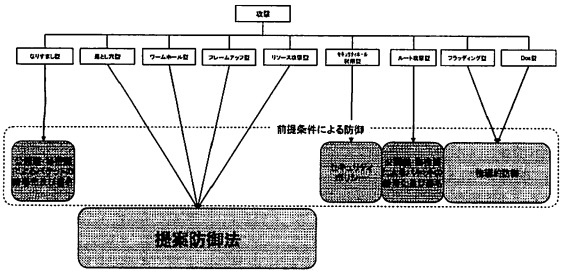


図 12 提案防御法の位置づけ

**(1)バックアップルートの作成**

前述のようにマルチパス化をすることは困難だが，予備の経路(バックアップルート)を作成することは可能である[11][12]．これにより攻撃ノード検出の際にバックアップルートに切り替えることで，再検索によるオーバヘッドが抑えられる．

**(2) レポートの作成及び配布**

通信経路上の各ノードは，通信開始直後から自身のデータパケットの流れを監視する．監視するノードを $A$ とすると，$T$ 時間内にノード $X$ から受信したデータパケット数を $RN_{cur}(A,X)$ と表す．同様に，ノード $Y$ に送信したデータパケット数を $FN_{cur}(A,Y)$ と表す．また $A$ が何らかの理由でデータパケットをドロップする場合があるのでその数を $DN_{cur}(A)$ と表す．$A$ はこれらの情報をレポートとして $T$ 時間内にデータパケットを受信及び送信したノードへ送信する．そして，そのレポートを受信したノードはレポートが送信されたフローとは逆方向の使用経路にフォワードする．これによりレポートは 1 ホップ先のノードまで届くことになる(1 ホップレポート法)(図 13)．

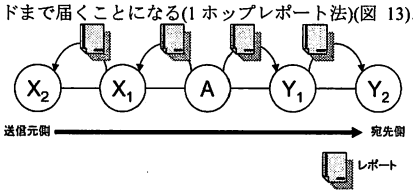


図 13 1 ホップレポート法

**(3)パケットの監視による信頼度の計算**

各ノードは，レポートにより隣接間の $RN$，$FN$ の関係をチェックすることが出来る．具体的には $A$ が $X$ にデータパケットを送信した場合は，まず $X$ のレポートの内容が正しいかどうかを $X$ のレポート中の $FN+DN=RN$ の関係を調べることによって検証する．この関係は，$X$ が処理したパケットに不明なものが無いかを調べている(受信したパケットはドロップするか，フォワードするかのどちらかであるため)．次に $FN_{cur}(A,X)+DN_{cur}(A)=RN_{cur}(X,A)+DN_{cur}(X)$ が常に成立するので，まずこの式が成立しない場合はノード $A$ から見た $X$ の信頼度 $H(A,X)$ に制裁を与えることが出来る．同様に $A$ の隣接(図 13 $X_1$・$Y_1$)とさらにその隣接($X_2$・$Y_2$)の関係もチェックすることが出来る．例えば $X_1$ - $X_2$ 間では，それぞれレポートの内容のチェックを行った後，$FN_{cur}(X_1,X_2)+DN_{cur}(X_1)=RN_{cur}(X_2,X_1)+DN_{cur}(X_2)$ を調べることにより，同様に制裁を与えることが出来る．詳細なフローチャートを図 14に示す．

**6.5.4 信頼度による経路再構築**

各ノードが持つ他ノードの信頼度が閾値以下になるとそのノードからの管理パケットを全て破棄するようになり，同時に ROUTE ERROR を送信することで経路を破棄するようにする．これにより中継ノードは，バックアップルートに切り替えるか経路の再検索を行う．

## 7. 今後の課題

今後は，提案防御法の実装と評価を行い検証する．その際レポートの Frame-up についての検証も合わせて行う．

## 8. まとめ

本稿では，アドホックネットワークにおける攻撃法と防御法の分類を行いそこから汎用的な防御法のモデルを作成した．提案防御法は HADOF の核となる技術であるレポートの交換と信頼度の計算を継承して，hop by hop のルーティングプロトコルにも適用できるようにモデル化した．

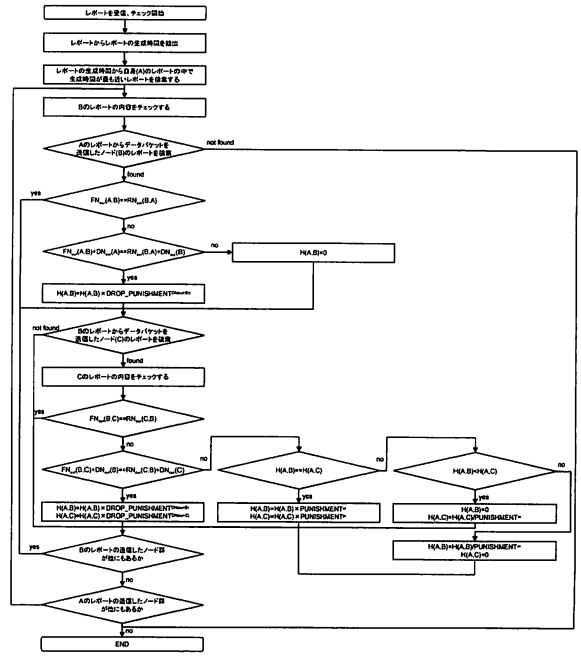


図 14 レポートチェックのフローチャート

## 文　献


[1] Yu, W. Sun, Y. Liu, K.J.R., "HADOF: defense against routing disruptions in mobile ad hoc networks", INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, 1252- 1261 vol. 2, 13-17 March 2005

[2] Sergio Marti, T.J Giuli, Kevin Lai, Mary Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", 6th MobiCom, BA Massachusetts, Aug. 2000.

[3] A.Burg, "Ad-hoc Network Specific Attacks", Seminar Ad-hoc network, Technische Universitaet Muenchen, 2003.

[4] Qifeng Lu, "Vulnerability of Wireless Routing Protocols", University of Massachusetts Amherst, 2002.

[5] Secure Ad hoc On-Demand Distance Vector (SAODV) Routing, http:/ /www. ietf.org/internet-drafts/draft-guerrero-manetsaodv-05.txt.

[6] Pankaj Goyal, Kunar Kapil, "Prevention from Gray Hole Attack in MANETS", Mobile Conputing (CS634) Student working on : group 7, September 3, 2004.

[7] 谷山　健太, "アドホックネットワークにおけるディスジョイントのマルチパスルーティングプロトコル", 早稲田大学学士論文, pp18, 2004.

[8] 森　拓海, 横山　信, 高橋　修, 高木　剛, 山崎　憲一, "AODV における Ghost Attack とその防御法", 情報処理学会 MBL39 研究会 2006.

[9] Abu Raihan Mostofa Kaman, "Adaptive Secure Routing in Ad-hoc Mobile Network", Master of Science Thesis, pp35, 2004.

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

[11] 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.

[12] 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ジョイント・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.