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

2007－ＭＢＬ－41（15）
2007／5／18

アドホックネットワークにおける防御法の分類と耐攻撃性アドホック・ルーティング・プロトコルアーキテクチャの提案

森 拓海† 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 〒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対する攻撃は多種多様なものが存在する．現在では，ある特定の攻撃法に対して，その攻撃パターンを検出し，防御するものがほとんどである．しかし攻撃法は日々進化し，複合攻撃や新たな攻撃法が開発されている．そこで現存する攻撃法を分類し，攻撃法をメタな振る舞いに分解することで総合的な攻撃対処方法を検討する．攻撃の対処には大きく分けて2種類が存在する．1つは攻撃パターンを定義し，攻撃ノードの検出・対処をする「防御機構」である．もう1つは攻撃を行わせない，または無力化する「回避機構」である．本論文では後者の「回避」に着目し，攻撃に対する耐性を持つプロトコルを設計するためのプロトコルアーキテクチャを提案する．

最初に種々の攻撃法を体系的に分類する．分類された各攻撃法に対する防御・回避手法をモジュール化し，必要に応じて取捨選択した組合せが可能であり，さらに新たな攻撃方法が発見されることに備え，それに対応した新たな防御・回避手法を追加する事が可能な汎用的なプロトコルアーキテクチャとする．これらによって，目的に応じた安全なプロトコル設計を可能にする．

キーワード アドホックネットワーク　耐攻撃性アドホック・ルーティング・プロトコルアーキテクチャ　防御機構　回避機構

A Classification of Defense Method in Ad-hoc Networks and Proposal for the Anti Attack Ad-hoc Routing Protocol Architecture

Takumi Mori† Ikumi Mori† Osamu Takahashi‡

† Systems Information Science, 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 various kinds of attack for ad-hoc networks. Now, many defense methods are defense to detect the attack pattern of attacks. However, attack methods are evolved every day and compound attack and new attack methods are developed. Therefore we classify existing attack methods and examine general attack measures method by resolving attack methods to "meta" behavior. We divide the attack measures from two kinds of methods. "Defense mechanism"; defines an attack pattern, and detect / cope attack nodes. Another is "Evasion mechanism"; it is to neutralize or not allowed attacks. We pay attention to "Evasion mechanism" of the latter in this article and propose a architecture to design protocols to have tolerance for many attacks.

We classify attack methods for evading every attack on an ad-hoc networks. We modularize defense or evasion method for each classified attacks. And As for them, it is able to combinate that we chose if necessary. For when a newer attack method is discovered, we define to it with the versatile protocol architecture that we can add new defense or evasion methods. It enable the safe protocol design that accepted security purpose by incorporating defense / evasion mechanism related to each attack among classified defense or evasion methods.

Keyword Ad-hoc Network, Anti Attack Ad-hoc Routing Protocol Architecture, Defense mechanism, Evasion mechanism

1. はじめに

近年，無線通信機器の発達により無線ネットワークを制御する技術の研究は盛んに行われている．特にアクセスポイントを必要としないアドホック通信によるネットワーク形成は，トラフィック分散やメンテナンス不要などの観点から注目されている．無線通信の利便性は有線通信より格段に進歩している．しかし，有線ネットワークと無線ネットワークの普及には背景の違いがある．それは利用人数(ノード数)と利用端末の性能，そして利用用途である．有線ネットワークの普及期は大学機関の論文共有などを主な目的としていた為，通信ノード数は数百程度の規模であった．この状況下で最も重視されたのは接続性と転送速度であった．有線ネットワークの規模は飛躍的に拡大すると，通信ノードの中に悪意を持ったノードが現れはじめた．大規模ネットワークにセキュリティが重要視されたのはこの時期からである．有線ネットワークはトラフィックやルーティング制御器機が多数存在するため，セキュリティはこれらの器機に導入することで比較的に容易に実現することができた．

そして近年，無線技術の普及期が訪れている．ネットワーク上のデータパケットの漏洩や特定のノードを狙ったアタックなどの「攻撃者」が多数存在するネットワークに無線器機を導入することは，攻撃者にとっては攻撃手段を増やす要因となる．そこで，無線通信に認証や暗号化を施すなどのセキュリティ対策がとられてきた．さらに無線通信は，ノード同士が相互にネットワークを形成するアドホックネットワークが近い将来普及するだろう．多くの研究ではアドホックネットワークのための通信プロトコルであるアドホック・ルーティング・プロトコルの接続性や通信速度といった要因は実用化の域に達している．しかしながら実用化がされない最も大きな障害は，多種多様の

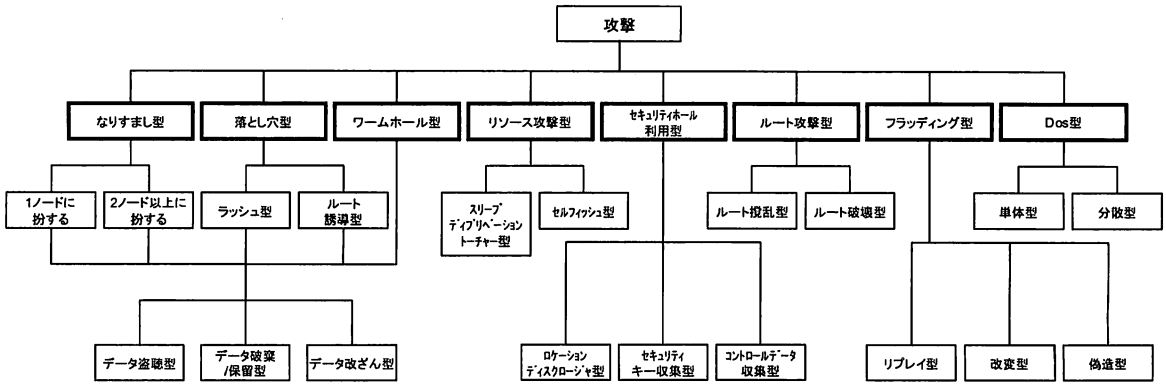

図 1. アドホックネットワークにおける攻撃法の分類

Fig. 1 Categories of Attacks on Ad-hoc Networks

攻撃に対する対処である.

本研究では多様化する攻撃をメタな振る舞いに分解し,その対処法を統合することにより新しい攻撃対処プロトコルアーキテクチャを提案する.本アーキテクチャは従来の攻撃パターンの定義から対処する「防御機構」ではなく攻撃を回避・無力化する「回避機構」に着目したものである.

2. 関連研究

アドホックネットワークにおける攻撃法を総合的に防御・回避する手段の研究としてはHADOF[1]がある. この方式はルーティングプロトコルとしてDSR[2]を対象とした汎用防御機構である.

HADOF ではソースルート上の各ノードに受信パケット数と送信パケット数を報告させることにより,攻撃ノードを検出する.経路制御には確率的マルチパスルーティングを用いており,各経路に関するルートクオリティを信頼度(Honesty Record)と虚偽報告値(Cheating Record)により決定している.

HADOF の研究は,多くの攻撃に対して既存技術による対処を行った上で,攻撃をデータパケットの破棄にのみ収束させている.データパケットの破棄を検出するために各ノードにレポートを記載させ,データパケットの送受信数の変化から攻撃ノードを検出する.また,攻撃者によるフレームアップ(でっち上げ)による誤認を防ぐ手段も用意されている.攻撃ノード候補同士を比較し,信頼値が低い方を攻撃ノードとして確定することでルートクオリティの回復と制裁を行う.

攻撃ノードを検出して対処する方法としては HADOF が最も有効と考えられるが, この方式は DSR のみを対象としたものである.他のルーティングプロトコルの場合,ルーティング特性の違いから実装が困難であると考えられる.また, HADOF の動作特性を利用した攻撃法が開発される可能性がある.本研究ではこのような HADOF 方式の問題点を改善する新しいプロトコルアーキテクチャを提案する.

3. アドホックネットワークに対する攻撃法の分類

アドホック・ルーティング・プロトコルは一般的にプロアクティブ型とリアクティブ型に分けられる.プロアクティブ型はRFCにより標準化されたプロトコルであるOLSR[3]やTBRPF[4]が知られている.しかし,既知の問題として,ノードの増加に対して経路計算量が増大してしまうことがある.一方,リアクティブ型のプロトコルは経路計算を通信要求が発生した時点から行うことで,経路計算負荷を分散している.RFCにより標準化されているプロトコルとしてAODV[5]があるが,実機実験では十分な接続性が保たれていないことや,攻撃に対する脆弱性の多さから実用域には至っていない.しかし,この問題は技術的改良により十分に実用化できる余地がある.本論文では,この2つのアドホック・ルーティング・プロトコルに対する攻撃法をメタな振る舞いに分解し,それぞれに応じた防御・回避法を分類する.

図 1はアドホックネットワークにおける攻撃の分類図である.大きく分け攻撃法は特性別に以下の 8 種類の型(大分類)に分けられる.さらに,各大分類以下にはいくつかの詳細な型(小分類)を定義する.

1) なりすまし型

悪意のあるノードが他のノードになりすますことにより,データの盗聴,破棄,改ざんを行う.

2) 落とし穴型

悪意のあるノードが周囲のノードから経路を集めることで,データの盗聴,破棄,改ざんを行う.

3) ワームホール型

外部パスにより送信元から宛先へのルートを短縮する.距離ベクトルルーティングなどのルーティングメカニズムを混乱させることが目的である.

4) リソース攻撃型

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,限りある資源を奪う攻撃である.

5) セキュリティホール利用型

コマンド管理の不備などのセキュリティホールを利用してルートのホップ数や中継ノード情報を得るものから,セキュリティ・キーを奪うものまで様々な攻撃法がある.一般的にそれ自体が直接被害を与えることは無い.

6) ルート攻撃型

悪意のあるノードが周囲のノードに対し,不正な経路を形成させる攻撃である.不正な経路を利用することで,ドロップパケットが多発したり,ルーティングテーブルを破壊されることで通信不能に陥る.

7) フラッディング型

特定のパケットを周囲に大量送信することで,ネットワークの帯域幅を奪い取る攻撃である.通信速度の低下に始まり,最悪の場合通信が停止する.

8) DoS 型

単体または複数で特定のノードに対し,過剰なサービス要求を行うことで,そのノードの機能を停止させる攻撃である.あらゆるプラットフォームでの攻撃が可能であるため,問題視されることが多い.

4. 防御・回避方法の基本的な考え方

本章では, 3章で分類した各攻撃型に対応する回避法を考察する.3章で分類した各攻撃法と関連する防御法および回避法を図 2に示す.本研究では,攻撃の回避法を優先的に耐攻撃性アドホック・ルーティング・プロトコルアーキテクチャに取り入れる.防御法の分類は攻撃法の大分類に従い,それぞれに応じた防御・回避法を示している.

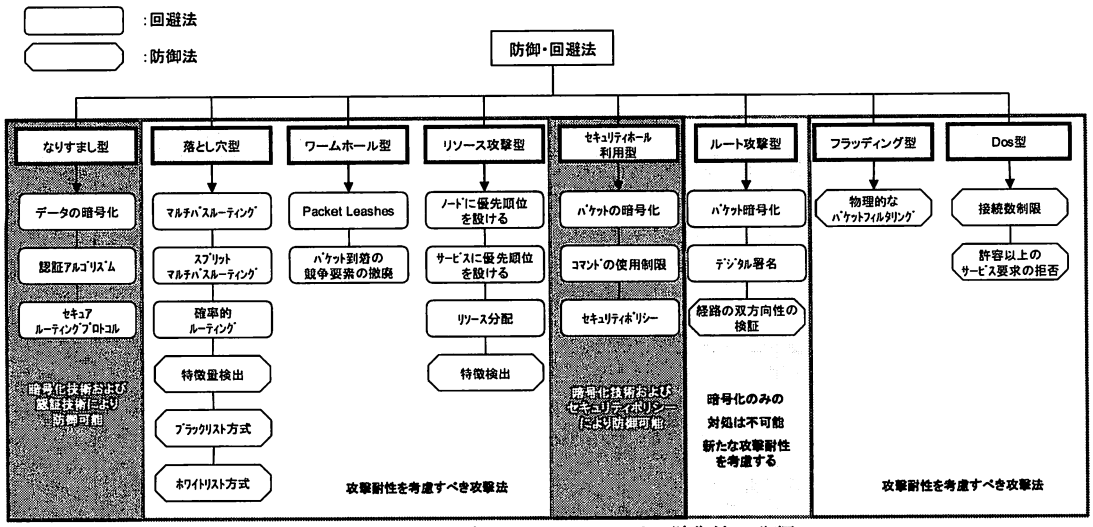

図 2. アドホックネットワークにおける防御法の分類

Fig. 2 Categories of Defense method on Ad-hoc Networks

4.1. なりすまし型攻撃耐性

なりすまし型攻撃にはデータの暗号化や認証といった技術が有効である. 現在のセキュリティの分野ではこの２つの技術は前提条件とされやすい. 暗号化技術は各ノードが送信するすべてのパケットを暗号化することで, 第３者による盗聴を不可能とする. 従って, 攻撃者はなりすましのための情報収集が困難になる. また, 最新の暗号化技術を用いることによりあらゆる改ざんを無効化する. 関連技術としてはディジタル署名, メッセージダイジェストといったものがある.

認証技術はネットワークに参加するすべてのノードを認証する方式である. 一般的にアドホックネットワークでは, 認証は通信範囲を限定することになる. この技術によりネットワーク上のすべてのノードの同一性(唯一性)が保証される. 従って, なりすまし型攻撃を不可能とする. データの暗号化および認証技術はなりすまし型攻撃に加え, ３章の攻撃分類の小分類のデータ盗聴, データ改ざんの攻撃をすべて回避する.

4.2. 落とし穴型攻撃耐性

1) ラッシュ

悪意のあるノードが周囲のノードよりもすばやくROUTE REQUEST(RREQ)をフォワードすることにより, 攻撃者を含む経路を採択されやすくする. この攻撃では, MAC層でフォワーディングを高速化される場合などが考えられる. 最短経路解決法[a]では, RERQまたはRREP（ROUTE REPLY）のホップ数をカウントすることで, ラッシュを行っているノードが最短経路ではない場合は経路形成を回避できる. 従って, RREPホップカウント検査を新たに回避法として追加する. 既存の回避法ではマルチパスルーティング[b]や確率的ルーティング[c]で, 攻撃者を経路上に含む確率を低下させることができる.

2) ルート誘導

攻撃者が周囲のノードに自分が経路形成に適しているかのように情報を装うことで, 自分への経路形成を促す攻撃である. この攻撃に対しては, 攻撃者の出す情報の正誤を確認することが最適だが, 攻撃者以外にその事実を知ることができない情報については真偽を問うことはできない. そこで, 客観的に判断できる材料から, ルーティングに適した条件を判断することが考えられる. 既存の技術では適切な方法が無いが, ルート分散[d]を行うことで攻撃される可能性を低下させる方法がある.

落とし穴型攻撃はマルチパスルーティングを用いることでルート収集を困難にすることができる. また, 複数ある経路が１つのノードに集中しないようなルート分散を行うことで, 攻撃者に経路が集中することを防ぐことができる. それにはAODV-BA[6]のように経路の選択に周辺密度や経路密度を複数のノードが測定し, その平均値から最適な経路を選択することで実現できる.

4.3. ワームホール型攻撃耐性

ネットワーク外部のノードと共謀するため通常よりも早く RREQ が到着する. 実際には, 攻撃されている経路は通信可能なため検出が難しい. タイムスタンプや位置情報をパケットに記載し, その情報からワームホールを検出する Packet Leashes が防御法として一般的であるが, その情報自体が攻撃者によりフレームアップ(でっち上げ)される可能性がある. またワームホールを通るパケットになんらかの細工がされる恐れがあるが, パケットが暗号化されている条件下ではパケットを盗聴・改ざんすることはできないので破棄するのみとなる. パケットを破棄する場合は, 落とし穴型攻撃と同じ対策法をとることができる. よってワームホールにより距離情報が撹乱された場合の対処としても落とし穴型攻撃と同様に, 最短経路解決を行なわず, 確率的マルチパスルーティングによりルート分散を行うことが最善である.

4.4. リソース攻撃型攻撃耐性

スリープ・ディプリイベーション・トーチャー攻撃では断続的な通信要求を行うことで, モバイルノード特有の資源を奪う. この攻撃の対処としては攻撃者の出す不要(不正)な要求を処理しなければよい. 定期的なルート要求に対しては, ルートがあれば処理しないため, なるべく長い時間安定した経路を確保することで, 攻撃をほぼ無力化することができる. 従って, 安定性重視ルーティング[e]か, 複数の経路を保持しているマルチパスルーティングを用いる.

上記の方法とはまったく異なる方法ではサービスやノードに優先順位をつける方法がある. PLBR[7]のようにPL（優先リスト）を用いたノード管理を行うことで実現できる. またノードの優先順位を階層

---

a) 最短経路解決法
通信において, 送信元から宛先までの最短経路を用いる手法である. 一般的に通信スループットが高い経路で通信できるが, リンクが切れやすいなどの欠点がある.

b) マルチパスルーティング
経路を複数本確保するルーティング手法であり, 通信の際には複数ある経路の中から１つを選択する.

c) 確率的ルーティング
マルチパスルーティングにおいて経路を選択するときに, ある条件から経路選択の確率を決定する. 通信に使用する経路は, この確率に従って選択する.

d) ルート分散
特定のノードに経路が集中しないようにする技術である. マルチパスルーティングにおいて実装されることが多い.

e) 安定性重視ルーティング
最短経路解決とは逆に, 最短経路ではなく経路の切断が最も起こりにくい経路で通信を行う. そのために切断危険の通知が重要となる.

表 1. 部品化された攻撃回避技術のまとめ

Table. 1 A Summary of Parted Attack Evasion Method

大分類の攻撃	回避技術	備考
なりすまし	認証技術	前提条件
落とし穴	確率的マルチパス・ルーティング ルート分散	ルート分散は経路のdisjoint性を考慮する
ワームホール	Packet Leashes 記載する情報はメトリクスに関するもの 確率的マルチパスルーティング ルート分散	ルート分散は経路のdisjoint性を考慮する
リソース攻撃	優先リスト(PL)を用いた方法 ex. 隣接ノードへの接続要求→優先度高 遠くのノードへの接続要求→優先度低 ネイバーダウン回数測定(リンク切断危険)による優先度設定	PLの概念はPLBRに基づくもの リンク切断危険の概念はAODV-BAによる
セキュリティホール利用型	セキュリティポリシー	スコープ外
ルート攻撃	ディジタル署名 シーケンス番号 Route Error回数測定(リンク切断危険)による優先度設定	リンク切断危険の概念はAODV-BAによる
フラッディング	ブロードキャスト・ホップ・リミット(固定値) PLによるブロードキャスト管理	主にブロードキャストが行われるパケットはRoute Requestである。従ってRoute Requestを制御することで実現する
DoS攻撃	ファイア・ウォール	スコープ外
小分類の攻撃	回避技術	備考
盗聴・改ざん	ディジタル署名 パケット暗号化	前提条件 (SAODV,SDSRのような機構を想定)

化するで，より詳細な管理を実現できる．優先度の例は以下のようなものがある．

①近くのノード(隣接)への通信要求→優先度が高い
②遠くのノードへの通信要求→優先度が低い

このような方法をとることにより，近くのノードへの連続的な通信要求は経路探索を行うことないので RREQ 連鎖が発生しない．遠くのノードへの通信要求は優先度を低く保つことで，他のノードからの要求(主に隣接から)が処理できなくなる事態を回避することができる．

セルフィッシュ型の攻撃は自分が通信するとき以外のパケットのフォワーディングを行わないので，Hello メッセージを出さない，RREP を返信しないなどの方法がとられる．このとき，明らかに RREP を返信しない率が高い場合などは特徴量検出が行える．また，ノードの優先度を設ける方法ならば RREP を返信しないノードの優先度を低くすることで，制裁を与えることができる．Hello メッセージを出さない場合などはそのノードが Down していると周囲から判断される．電源の節約のために頻繁に Down を繰り返す場合は攻撃者の周囲のノードが単位時間当たりの Neighbor Down の回数を測定することで検出する．実装上は Neighbor Down を繰り返すノードはリンク切断危険があると判断し，そのルートの採択確率を下げる．または Neighbor Down を繰り返すノードを優先リスト上で優先度を低くすることで実現する．

4.5. セキュリティホール利用型攻撃耐性

セキュリティホールの対処として，コマンド使用制限などを設けることがある．この制約は OS からシステム管理者（場合によってはユーザ）が行う．このように，一般的にセキュリティホールはコーディングにおけるバグやコマンド管理の不備など，人為的なミスが関連する．そのため，この攻撃型に対する回避法はルーティングプロトコルレベルで対処することができない．よって 3 章の攻撃法分類のうち「セキュリティホール利用型」攻撃はスコープ外の攻撃と定義する．

4.6. ルート攻撃型攻撃耐性

Ghost Attack[13]のようなルート撹乱型の攻撃では他ノードのビーコンをリプレイする．ディジタル署名が施されている場合は完全なリプレイ攻撃となる．本アーキテクチャではディジタル署名が前提条件となっているので，ビーコンにシーケンス番号[f]を付加することにより攻撃者の送信する偽のビーコンを連続的に処理しないようにする．

積極的に経路を破壊するルート破壊型攻撃に関しては Route Error(RERR)のような Route Broken メッセージを意図的に攻撃者が送信する．このとき，他ノードに成りすまして RERR を送信すると効果的だが，ディジタル署名により無効化できる．この場合，攻撃者は落とし穴型攻撃のように経路を自分に集中してから攻撃を実行する．この攻撃には RERR をあまりにも頻繁に出すノードにはリンク切断危険があるものとし，経路形成をやめるか優先度を下げる方法が有効である．

4.7. フラッディング型攻撃耐性

リプレイパケットを周囲に大量に送信する方法やフラッディングを引き起こすパケットを送信することで帯域幅をフローさせる．例えば存在しないホストへの通信要求を行うことで，周囲のノードからその隣接ノードへと連鎖的に通信要求がブロードキャストされ，フラッディングを引き起こすことができる．現在の帯域幅を考慮すると，意味のないリプレイパケットで帯域をフローさせることは難しく脅威となることは少ないと考えられる．既存の防御法としては物理的なパケットフィルタリングがある．この方法はルーティングプロトコル上で実装することができないので，本アーキテクチャでは扱わない．
回避法として考えられるのは，ブロードキャスト・ホップ・リミットがある．連鎖的に宛先の存在しない通信要求が発生することによるフラッディングは無限に宛先を探索することにより発生する．従って，経路の探索範囲を限定する必要がある．実装には経路探索時に送信する RREQ にブロードキャスト・ホップ・リミットを設ける方法がある．また別のアプローチとして「ブロードキャスト」の概念をなくす手法がある．PLBR のように優先リスト上のノードのみが RREQ をフォワードできるようにすることで，RREQ を受信できるノードを限ることで，帯域幅を消費することを防ぐことができる．

4.8. DoS 型攻撃耐性

大量のサービス要求を特定のノードに行うことで，ターゲット・ノードを機能不全に陥らせる攻撃である．最近のコンピュータでは処理能力が非常に高いので DoS 攻撃を 1 対 1 で実行することは難しい．そこで攻撃者が複数に分かれて特定のノードに DoS 攻撃をする分散

f) シーケンス番号
経路探索において，探索パケットがループしてしまう問題を解決するために，パケットに番号を振ることで番号の古いパケットを破棄する．また，この機構により常に最新のパケットのみを処理することができる．

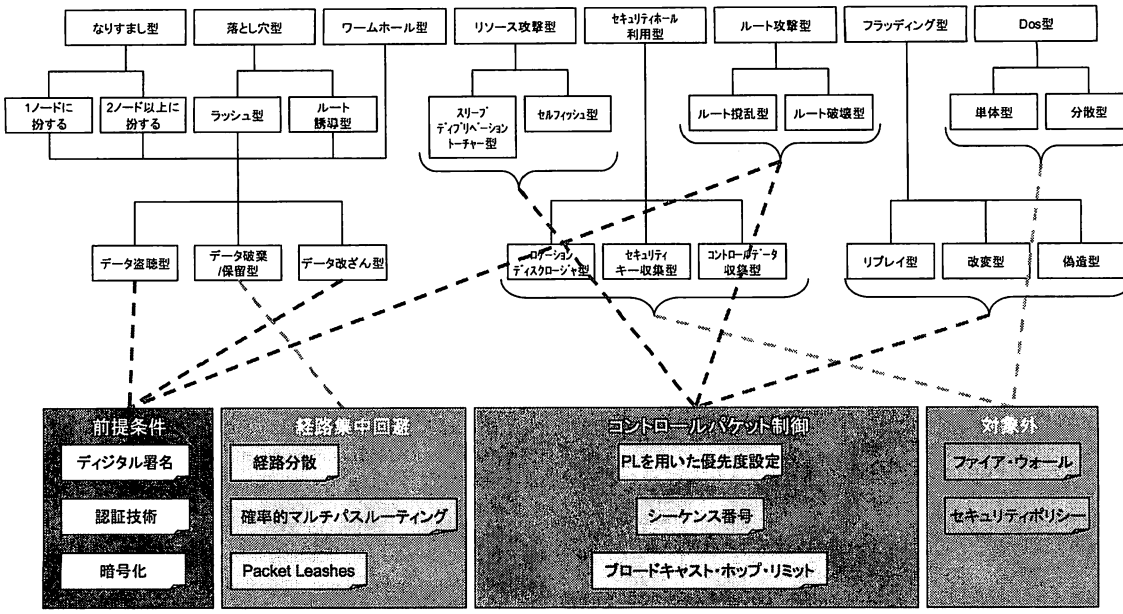

図 3 耐攻撃性プロトコルアーキテクチャ

Fig. 3 Anti Attack Ad-hoc Routing Protocol Architecture

DoS攻撃を行うことが多い．この攻撃に関しては根本的な防御・回避策が無いのが現状である．既存の方法として，有線ネットワークではファイア・ウォール等で一定時間内の接続回数制限やサービス用要求制限により，ある程度抑えることはできる．しかし，フィルタリング基準を動的に変更しなければならない等の問題がある．現在アドホックネットワークで実現の可能性がある防御手法としては，和歌山大学の伊藤大輔らによるSPP[12]と呼ばれる方法がある．この手法はいくつかの実現方法があるが，その中の「特定シーケンス番号方式」が実現の可能性がある．この方法では特定のシーケンス番号からのサービス要求のみを受け付けるものであるが，DoS攻撃を行う場合シーケンス番号に規則性が出ることが多い．その規則性を検出し，ソフトウェアで要求のフィルタリングを行うことで実現できると考えられる．

5. 耐攻撃性アドホック・ルーティング・プロトコルアーキテクチャ

表 1に各攻撃に対する耐性を持つ技術の一覧を示す．4章で考察した際に新たに追加された手法については太字で示す．本章では表 1から攻撃に対する解決技術が同一のものなどを統合し，耐攻撃性アドホック・ルーティング・プロトコルアーキテクチャを作成する．尚，上記解決法を複数導入することによる矛盾が起こる可能性があるものについてはより効果的なものを用いることにする．

はじめに表 1の技術を2種類のグループに分ける．第1グループは複数の攻撃法に対する対処を行うことができる技術で以下の 5 種類である．

① 確率的マルチパスルーティング
② 経路分散
③ ノード優先度(優先度リスト)
④ リンク切断危険検査
⑤ シーケンス番号

この技術と前提条件を用いることでフラッディングと DoS 攻撃を除いた攻撃に対する耐性をルーティングプロトコルに持たせることができる．次に第2グループは特定の攻撃法の対処法として分けられるもので次の8種類である．

① RREQ ホップカウント
② 周辺密度・経路密度検査
③ Packet Leashes
④ 安定性重視マルチパスルーティング
⑤ RREP 特徴量
⑥ ブロードキャスト・ホップ・リミット
⑦ ブロードキャストの概念除去
⑧ 特定シーケンス番号による SPP

RREQ ホップカウントについては，最短経路解決の場合に有効であるがマルチパスルーティングを採用する場合は大きな意味を持たない．周辺密度および経路密度もマルチパスルーティングにより別途に経路分散を行うことで代用できる．RREP 特徴量検査は防御法として提案されたものなので，ルーティングに深くかかわらない．Packet Leashes はフレームアップに対し脆弱性が残る．また Packet Leashes によってパケットに位置情報などが記載されるが，その情報が耐攻撃性プロトコルにおけるメトリクスとして採用される情報に限り行うものとする．安定性重視マルチパスルーティングは第1グループの4リンク切断危険検査と関連が深いので統合できる．RREP 特徴量検査については防御法としての色が強いため，ルーティングにおける必要性が低い．したがってルーティングにおける計算コストの増加が懸念されるため，本アーキテクチャから除外する．ブロードキャストの方式については，ブロードキャストの概念除去かホップリミットのいずれかを導入する．ホップリミットを設けて通信範囲を限定することは前提条件で認証機構を導入していることから考えても合理的といえる．しかし実装に際してはホップリミットの動的な更新が必要となる．その際に多くの制御メッセージがフラッディングされることを防ぐためにもこの機構は用いないことにする．ブロードキャストの概念除去については第1グループでの PL の導入と関連が深いため統合できる．ブロードキャスト・ホップ・リミットに関しては動的な更新ではなく固定値とする．最後に特定シーケンス番号による SPP であるが，シーケンス番号の動的な管理をソフトウェアで行った場合，計算量の増加が懸念される．この方式については実装・評価がなされていないため，今回の耐攻撃性プロトコルアーキテクチャでは用いないこととする．

以上を踏まえ，同一の機能を持つものや，包含する機能を持つ機構を統合し，回避機構をモジュール化する．これらの技術を耐攻撃性アドホック・ルーティング・プロトコルアーキテクチャとして図 1に分類された攻撃と対応させたものを図 3に示す．モジュール化された回避機構は本アーキテクチャでは4種類に分けられる．

1) 前提条件

プロトコル設計上，前提条件として扱われる技術である．ルーティングと無関係に実装できる．

2) 経路集中回避
ある特定のノードに経路が集中しないようにする技術である．経路上に攻撃ノードを含むリスクを低減させる最も重要な技術である．

3) コントロールパケット制御
フラッディング制御やループ回避などを行う技術である．マルチパス化などを行う場合には特に重要となる．

4) 対象外
プロトコル設計には無関係な技術である．ハードウェアまたはユーザに適用される．モラルやポリシーといった抽象的なものを指す場合もあり，セキュリティ要求により対処法が異なる．

上記４つの定義のうち２)，３)に関しては，経路制御とコントロールパケット制御である．この２つの要素はルーティングの根幹部分であり，どのようなアドホック・ルーティング・プロトコルにも共通して対応することができる．新たにモジュールを追加する場合には，経路およびコントロールパケットのいずれかの制御に帰着させることによってプロトコル依存を回避する．

本アーキテクチャの各モジュールは，必要に応じて取捨選択した組合せが可能である．さらに新たな攻撃方法が発見されることに備え，それに対応した新たな回避手法を上記２)または３)に追加する事が可能であり，汎用的なプロトコルアーキテクチャとなっている．

現存するプロトコルに本アーキテクチャを適用させる場合や，新たにプロトコルを設計する場合の技術的な実現手段は多数存在する．本アーキテクチャをプロトコル設計時に考慮することで，プロトコルに応じた適切なセキュリティ基準のプロトコル設計を可能にする．

6. 今後の課題

アドホックネットワークに対する攻撃を 8 つの大分類に分けそれぞれの回避法に着目したことで異なる攻撃に対して共通する回避法が有効であることが明らかとなった．しかし，本アーキテクチャを適用させるプロトコルによっては実装不可能な対処法もある．例えば AODV では Hop by Hop 方式を採用している為マルチパス化が困難である．DSR ではソースルーティングであるため，隣接ノードの切り替え制御が困難である．そこで，本アーキテクチャでは対処法の概念のみを示した．また，それぞれの対処法の衝突やその効果については検証する必要がある．

攻撃の回避に最も重要であるのが，攻撃ノードを含まない経路で通信を行う事である．これはマルチパス化やルート分散が最も重要な役割を果たす．このひとつの解決法として「disjoint 性」の概念がある．マルチパスルーティングにおいて複数のルートを保持した場合に各ルートが互いに依存していないことが望ましい．ルートが disjoint であることの重要性は，現在選択されているルート(プライマリルート)が RouteError となった場合にそのルートのエラーに依存して代替ルートが無効化されてしまう可能性を低くできることである．disjoint 性には 2 種類存在し，1 つは「node-disjoint 性」もうひとつは「link-disjoint 性」である．「node-disjoint 性」はある 2 本のルートが中間ノードを共有していないことであり「link-disjoint 性」は 2 本のルートがリンクを共有していないことである[9]．静岡大学の上野裕介らによって，この概念を数値化したものが NAF(Node Association Factor)値である．NAF 値は Node-disjoint 性を数値化したものであり，それに倣い NAF 値を用いたルート選択を行うことが攻撃の回避に有効である．

そこで NAF 値による経路制御が有効であるといえる．本アーキテクチャを実装する場合は NAF 値による経路制御方式を取り入れることで効率的に実装することができる．

現存するプロトコルに本アーキテクチャを適用するという手段とは別に本アーキテクチャに準拠して設計する新しいルーティングプロトコルを開発することもできる．さらに本アーキテクチャを適用させたプロトコル上にさらに防御機構を組み込むことにより，より強力な攻撃対処を行う事もできる．

7. 終わりに

本論文では特定のプロトコルを想定せず，耐攻撃性アドホック・ルーティング・プロトコルアーキテクチャの提案のみを行った．本アーキテクチャが攻撃耐性を持つことを証明するために，DSR 上に本アーキテクチャを実装した AAAr:Anti Attack Ad-hoc routing protocol の開発と検証を行う予定である．

AAAr は NAF 値を用いた確率的マルチパスルーティングを主体とした，攻撃ノード回避を行うルーティングプロトコルである．従来の攻撃ノード検出と排斥を行わない点で従来の攻撃対処法と大きく異なる．本研究がアドホックネットワークにおけるセキュリティの新しい概念として認知されることを切に願う．

文　献

[1] Wei Yu, Yan Sun and K.J. Ray Liu, "HADOF:Defense Against Routing Disruptions in Mobile Ad Hoc Networks", in INFOCOM 2005, March 2005

[2] DSR : draft-ietf-manet-dsr-10.txt

[3] OLSR : RFC3626 http://www.ietf.org/rfc/rfc3626.txt

[4] TBRPF : RFC3684 http://www.ietf.org/rfc/rfc3684.txt

[5] AODV : RFC3561 http://www.ietf.org/rfc/rfc3561.txt

[6] 田内雅之, 井手口哲夫, 奥田隆史, 田学軍 「経路の切断を回避するアドホックルーティングプロトコルの提案とその性能評価」, 情報処理学会, Oct.2006

[7] PLBR : http://wiki.uni.lu/secan-lab/Preferred+Link-Based+Routing+Protocol.html

[8] WikiPedia Ad-hoc Routing Protocol List http://en.wikipedia.org/wiki/Ad_hoc_routing_protocol_list

[9] 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 2003

[10] 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

[11] 上野裕介, 撫中達司, 小野良司, 渡辺尚 「ルートの独立性を考慮したマルチパスルーチングプロトコルの提案とその評価」, 情報処理学会論文誌 Vol45 No12, Dec. 2004

[12] 伊藤大輔, 泉裕, 齋藤彰一, 上原哲太郎, 國枝義敏 「TCP セッション管理による DoS 耐性の考察」, IC2002, Oct.2002

[13] 森拓海, 横山 信, 高木 剛, 山崎 健一, 高橋 修 「AODV における Ghost Attack とその防御法」, MBL-39, 情報処理学会研究報告 pp.53-58