動的マーキングを用いた効率的なネットワーク攻撃追跡手法の提案

古賀 勝寛[1)] ・ 岡崎 直宣[2)]

A proposal of tracing method for distributed denial of service attacks using dynamic marking scheme

Katsuhiro KOGA[1)], Naonobu OKAZAKI[2)]

Abstract

In recent years, DoS (Denial of Service) attack and more powerful DDoS (Distributed DoS) attack pose security problems on the Internet. As the measure to these attacks, it is important to trace attackers and stop the attacks. However, since information of the attacker is "spoofed", it is difficult to trace. Therefore, the method of specifying attackers is required. Savage et al. proposed a method to trace flooding attacks by "marked" packets. This method, however, has some problems gathering the attack packets through a lot of hops. In this paper, we propose a method to solve this problem by observing the feature of attack traffic and change the "marking probability" of the routers. We implement algorithms both of our proposed method and extending marking method to estimate the efficiency of them. From the results of some experiments, we will show the effectiveness of our proposed scheme.

Key Word :
Distributed Denial of Service, IP traceback, traffic monitoring, IDS

1. はじめに

近年，インターネットの普及が進む一方，ネットワーク上の不正行為が問題となっている．中でも特に問題となっているのが， Distributed DoS (DDoS) である．DDoS攻撃は，複数の攻撃者が標的となるサーバに大量のIPパケットを送りつけることで標的の持つ資源の枯渇や標的の属するネットワークの輻輳を起こし，正常なサービスの運営を妨害する攻撃である[1][2]．この攻撃への対処には，攻撃者に近いルータ上でパケットフィルタリングすることが望ましい．しかし，攻撃パケットの送信元アドレスは改竄されていることが多いため，攻撃者の特定は非常に困難である．そこで，DoS攻撃の追跡手段としてIPトレースバック技術[3]が注目されている．本論文では，その中でも特に有望とされるマーキング手法[4]に着目する．マーキング手法は，ルータが転送するパケットに一定確率でリンク情報を書き込み，この情報を基に攻撃者を追跡する．しかし，マーキング手法は大規模な攻撃の追跡に非常に長い時間がかかる問題がある．そこで，リンク情報を書き込む確率をルータごとに調整する手法が研究されているものの，攻撃者によるリンク情報改竄の影響を受ける問題を改善することはできていない．そこで本論文では，新たなアプローチとしてルータ上での簡易な攻撃検知とマーキング確率の動的な制御による問題の解決を図る手法を提案し，実ネットワークを模したトポロジ上で評価を行う．

2. マーキング手法

本章では，既存のマーキング手法としてFMS(Fragment Marking Scheme)[4]について述べる．

2.1 FMSの概要

FMSは，ルータが攻撃パケットに書き込んだリンク情報を基にして攻撃経路を追跡する手法である．FMSの追跡はルータがパケットにリンク情報を書き込むマーキング手順と被害ノードがリンク情報を基に追跡を行う攻撃経路再構築手順の2つで構成される．

2.2 マーキング手順

FMSでは，各ルータはIPアドレスを基にした固有のリンク情報を所持する．ルータはパケットを転送する際に一定の確率p(例:p=1/25)で自身のリンク情報をパケットに書き込む．

1) 情報システム工学専攻大学院生
2) 情報システム工学科准教授

リンク情報を書き込む領域には，正規通信への影響が小さなIPv4ヘッダ中の通常の通信では用いられない領域が用いられる．FMSでは未使用領域として識別子(Identification)フィールドを用いる．しかし，識別子フィールドはIPアドレスよりも小さいため，IPアドレスをそのまま書き込むことはできない．そこで，ルータはIPアドレスに復元用のチェックサムを付加して分割したものをパケットに書き込む．さらに，マーキング領域を3分割し，距離値やオフセット値といった制御情報を追記することでリンク情報を効率的に復元する．このとき，距離値は被害ノードからリンク情報を書き込んだルータまでのホップ数を示し，オフセット値は書き込んだリンク情報がどの部分のビットであるかを示す．

2.3 攻撃経路ツリーの再構築

被害ノードは収集した情報を基に，攻撃者の追跡を行う．このとき，被害ノードは収集した情報をオフセット値と距離値に基づいて整理し，同じ距離値を持つ情報の組み合わせを作る．この組み合わせが正しいことを確認するため，被害ノードは復元した情報に対して，奇数ビット(IPアドレス)からハッシュ値を生成する．復元した情報が正しいものであれば，生成したハッシュ値は偶数ビット(ハッシュ値)と一致する．

2.4 マーキング手法の問題点

マーキング手法には，攻撃者がマーキング領域を改竄したパケットを用いて攻撃を行った場合に計算量が増大する問題と，上流ルータの情報が下流のルータに上書きされることで消失する問題がある．以下に，各問題について述べる．

2.4.1 リンク情報の改竄問題

被害ノードには，各ルータのリンク情報か，どのルータにもマーキングされなかったパケット中の情報が届く．被害ノードはパケットがマーキングされているか識別できないため，攻撃者がマーキング領域の初期値をランダムな値にすると，リンク情報の組み合わせ数が非常に大きくなり追跡時間が長くなる．本論分では，これを計算量問題と呼び，復元したリンク情報の正しさを確認する回数を計算量と呼ぶ．

2.4.2 リンク情報の上書き問題

リンク情報の改竄問題は，マーキングされていないパケットを減らすことで改善できると考えられる．しかし，単純にマーキング確率を高くすると，リンク情報の上書きが問題になる．ルータは全てのパケットに対して一定確率でマーキングを行う．そのため，攻撃距離が長いとき，一度マーキングされたパケットが下流のいずれかのルータによってさらにマーキングされることがある．このとき，以前に書かれた情報が損失するため，攻撃者に近いルータの情報が届きにくくなり，追跡に要するパケットが非常に多くなると考えられる．

3． 調整確率マーキング手法

マーキング手法の問題を改善する手法として，ルータごとにマーキング確率を調整する手法が研究されている．本手法は，攻撃者に近いルータのマーキング確率を高くし，被害ノードに近づくに従ってマーキング確率を低くすることで，攻撃者に近いルータの情報が届く確率を高めている．本論文ではこの技術を調整確率パケットマーキング手法と呼ぶ．以下に，代表的な調整確率パケットマーキング手法を挙げる．

3.1 APPM:Adjusted Probabilistic Packet Marking Scheme

3.1.1 APPM の概要

本手法は，ルータや攻撃者，被害ノード間の距離を基にマーキング確率を調整し，効率的なトレースバックを試みる手法である[5]．ここではマーキング確率の調整に用いる変数ごとに，各手法をAPPM-1，APPM-2，APPM-3と呼ぶ．APPM-1では，攻撃者からルータまでの距離d_1を，パケットのIPv4ヘッダに含まれるIP option フィールド内に記述する．d_1はルータが転送を行うごとに1つ増加し，マーキングによって上書きされることはない．このとき，各ルータのマーキング確率は $p(d_1)=1/d_1$ となる．APPM-2は，マーキングを行ったルータと，現在パケットを転送しているルータとの距離を基にマーキング確率を変更する手法である．２つのルータ間の距離d_2は，FMSにおける距離値を用いることで実現する．このとき，各ルータのマーキング確率は$p(d_2)=1/2(d_2+1)$となる．APPM-3は，現在パケットの転送をしているルータと，被害ノードの距離を基にマーキング確率を変更する手法である．ルータと被害ノードの距離 d_3 は，RIPやOSPFといったルーティングプロトコルから得ることができる．このとき，各ルータのマーキング確率は$d_3=1/(c+1-d_3)$(c：定数)となる．

3.1.2 APPM の問題点

攻撃者は攻撃パケット中のIPヘッダを容易に改竄できるため，d_1の値を改竄することでAPPM-1のパフォーマンスを下げることができる．さらに，IP optionフィールドを用いた通信は，通常はサーバの設定によって制限されるという問題がある[6]．APPM-2では，攻撃者はd_2の値を改竄することで検出を逃れることができる． APPM-3ではプロトコルから距離を取得するため，攻撃者によるIPヘッダ改竄の影響を受けない．しかし，実際のネットワークでは，攻撃距離は一定ではないためパフォーマンスが低下すると考えられる．

3.2 DPPM:Dynamic Probabilistic Packet Marking Scheme

3.2.1 DPPM の概要

本手法は，パケット中のIPv4ヘッダに含まれるTTL値(Time

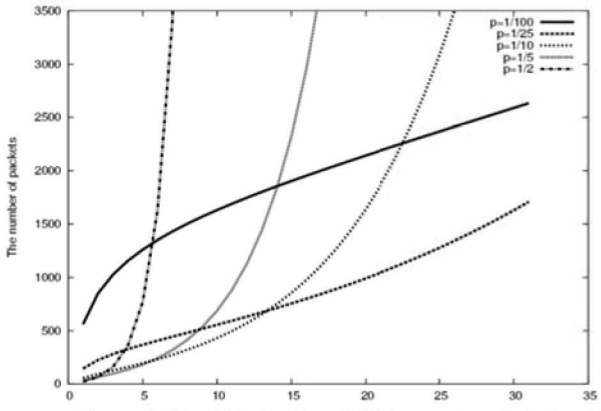


図 1　追跡に要するパケット数とマーキング確率の関係

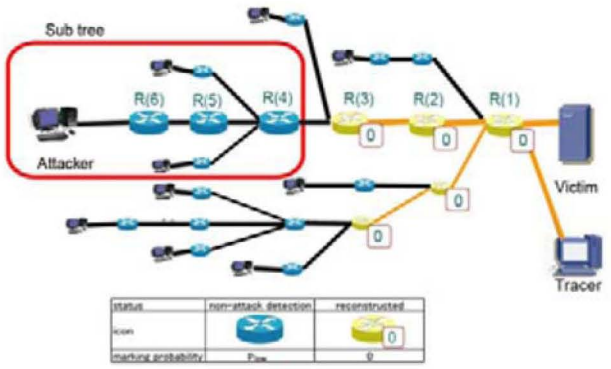


図 2　サブツリー

to live)の値を基にマーキング確率を調整し，効率的なトレースバックを試みる手法である[7]．DPPMでは，TTL値を基にマーキング確率を変更する．このとき，各ルータにおけるマーキング確率は，p=1/(c-TTL) (c：定数) となる．例えば，インターネットを介する通信のほとんどが31ホップ以下であることから[8]，c=32 とする．このとき，ルータはパケット中のTTL値が32以上のとき，TTL値を32に変更する．このとき，全てのパケットはネットワークの入り口でマーキングされるため，非常に効率の良いトレースバックが可能になる．

3.2.2 DPPM の問題点

攻撃者はパケット中のTTL値を容易に改竄することができるため，TTLの初期値を変更することでDPPMのパフォーマンスを下げることができる．例えば，被害ノードまでのホップ数hをPingコマンドを用いて調べ，TTLの初期値をh+1=TTLになるようにする．このとき，p=1になるルータが存在しないため，DPPMの最大の利点である改竄されたリンク情報が存在しないという点を覆すことが可能となる．

4． 提案手法

4.1　目的

本論文では，DDoS攻撃をトレースバック対象として扱う．攻撃者はIPアドレスを改竄しているため，トレースバック技術のみで直接攻撃者を特定することは難しい．そこで，本論文では攻撃者に最も近いルータ(NAR)の特定を目的とする．NARの特定により，攻撃パケットがネットワークに流入することを防ぎ，また可能であれば攻撃者を特定し，攻撃者のアクセスログから真の攻撃者を特定していくことができると考えられる．

4.2　提案手法の概要

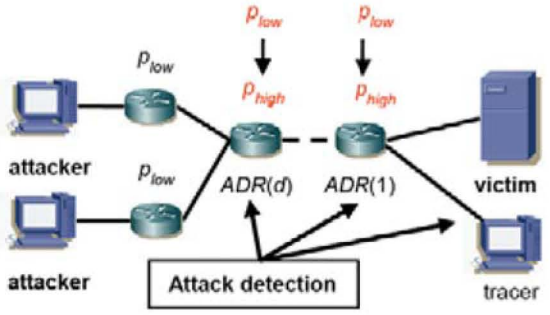
図 1に，リンク情報を8分割する場合に1人の攻撃者を追跡するのに必要なパケット数を示す．このとき，各グラフはマーキング確率 p=1/100，1/25，1/10，1/5，1/2のときのパケット数の期待値を表す．同図より，マーキング確率が高いとき，被害ノードに近い位置からの攻撃を素早くトレースバックすることができる．しかし，攻撃距離が長い場合，マーキング確率の低いほうが効率的に追跡できる．これは，マーキング確率が高いと，リンク情報の上書きが起こりやすいからであると考えられる．従って，攻撃経路を擬似的に短くすることができれば，高いマーキング確率を設定することが可能となり，より効率的なトレースバックを行うことができると考えられる(図 2)．本論文ではこの点に着目し，動的にマーキング確率を変更することで追跡を効率化する手法を提案する．以下では，この手法を ADMS(Attack Detection Marking Scheme)と呼ぶ．提案手法は，従来手法の機能に加えていくつかの機能を必要とする．新たに追加する機能として，ルータ上での簡易な攻撃検知機能，被害ノード側からルータに対してマーキング確率を動的に制御する機能が挙げられる．このとき，提案手法のシステムは，マーキング手法対応ルータと，NIDS（ネットワーク型侵入検知システム[9]）機能やトレースバック機能を持つトレーサ端末，及びルータに対してマーキング中止命令を出す管理端末によって構成される．また，被害ノードへのトラフィックはトレーサによって監視されているものとする．本論文ではFMSのマーキング手順と再構築手順を基にし，提案手法はFMSを発展させたものとする．

4.3　ADMS の処理手順

次に，ADMSの手順を攻撃検知手順，マーキング中止命令手順，マーキング手順，経路再構築手順の4つに分けて述べる．攻撃検知手順では，ルータが攻撃を検知する条件，攻撃検知後の処理について示す．マーキング中止命令手順では，追跡を終えたルータに対してトレーサがマーキングを中止するように命令する際の手順について示す．マーキング手順では，ルータが通過するパケットに対してリンク情報を書き込む際の手順を示す．経路再構築手順では，トレーサが収集したリンク情報を基に攻撃経路ツリーを追跡する手順を示す．

4.3.1 攻撃検知手順

本項では，ルータが攻撃を検知する条件，及び攻撃を検知



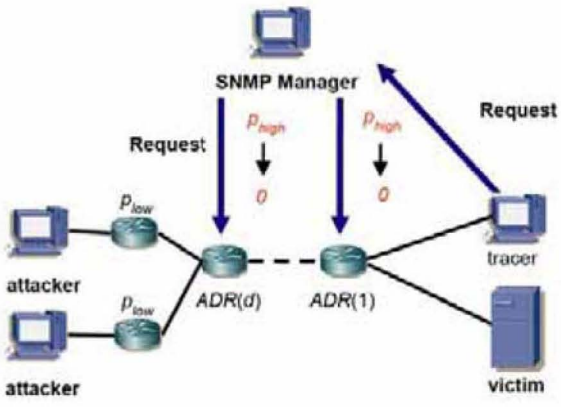
$ADR(d)$: attack detection router
d is distance from victim (d = 1,...,32)
p_x : marking probability ($0 < p_{low} < p_{high} <= 1$)
p_{low} is the probability of a normal router
p_{high} is the probability of an attack detection router

図 3 攻撃検知手順

した後の処理について示す．ルータは攻撃の特徴を持つトラフィックを識別することで簡易な攻撃の検知を行う．以下，攻撃を検知したルータをADR (Attack Detection Router)と呼ぶ．ルータは起動後，一定確率でマーキングを行いながら自身を流れるトラフィックの監視を行う．このとき単位時間あたりのパケット流量を観測するといった簡単な処理にすることでルータへの負荷を減らす．また，攻撃トラフィック量は被害ノードに近い下流のルータほど多いため，あるADRより下流にあるルータはADRになると考えられる．被害ノードはトレーサを用いて攻撃の検知を行う．ここでは，トレーサは攻撃パケットと正規のパケットを識別する機能を持ち，正確に攻撃を検知することができるものとする．このとき，トレーサには全ての攻撃トラフィックが集約するため，いち早く攻撃を検知することができる．被害ノードから dホップの位置にあるルータを R(d) ，ADRを ADR(d) と表す．このとき，被害ノードに最も近いルータはd=1 である．また，通常時のマーキング確率を p_{low} ，攻撃検知時のADRのマーキング確率を p_{high} とする．攻撃を検知したルータは，自身のマーキング確率を通常時よりも高い値 p_{high}に変更する．この変更により，ADRは通常のルータより高い確率でリンク情報と届けることができる．このとき，一時的にリンク情報の上書きが発生しやすい状態になる一方，次に示すマーキング中止命令を早い段階で受けることが可能となる．

4.3.2 マーキング中止命令手順

本項では，トレーサが追跡したルータに以降のマーキングの中止を命令する際の手順について示す．トレーサが距離d_0にあるルータADR(d_0)までの攻撃経路を追跡したとする．このとき，トレーサは管理端末に，ADR(d_0)のマーキング中止を要請する．管理端末は要請を受けると，ADR(d_0)に対して，マーキングの中止を命令する(図)．このとき，R(d_0+1)の情報は上書きされず，R(d)，(d> d_0+1)の情報は，ADR(d_0)のマーキング中止前よりも高い確率でトレーサに届く．命令はSNMP(Simple Network Management Protocol)を用いて実現できる．ルータはSNMPエージェントを備え，ルータのマーキング確率を拡張MIB(Management Information Base)にオブジェクトとして持つことを前提とする．ルータへの命令はトレーサがSNMPマネージャを実装した管理端末を介して行うものとする．以下に，SNMPのコマンドを用いて処理手順を示す．



$ADR(d)$: attack detection router
d is distance from victim (d = 1,...,32)
p_x : marking probability ($0 < p_{low} < p_{high} <= 1$)
p_{low} is the probability of a normal router
p_{high} is the probability of an attack detection router

図 4 マーキング中止命令手順

【STEP1】トレーサは管理端末に，追跡したルータのマーキング中止を要請する．

【STEP2】管理端末はSetRequestコマンドを用いて，再構築したルータに対してマーキングの中止を要求する．

【STEP3】ルータはGetResponseコマンドを用いて，管理端末にマーキングを中止したことを通知する．

【STEP4】管理端末はマーキングの中止が完了したことをトレーサに通知する．

4.3.3 マーキング手順

本項では，ルータが通過するパケットに対してリンク情報を書き込む際の手順を示す．マーキング手順は，パケットに書き込まれた距離値によって処理手順が異なる．以下にマーキング手順を準備段階，初期マーキング，終端マーキング，転送処理の4つに分けて詳説する．準備段階は，ルータ起動時の処理，初期マーキングでは，ルータが一定確率で行う処理について述べる．終端マーキングでは，初期マーキングされたパケットに対して行う処理，転送処理では，マーキングされなかったパケットに対して行う処理について述べる．

【準備段階】ルータが起動時に行う処理である．ルータは自身のIPアドレスを基にリンク情報を生成し，リンク情報を分

割してフラグメント値を得る.

【初期マーキング】ルータがパケットの転送時に行う処理である. 通常時, 及び攻撃検知時に一定確率で, パケットにオフセット値と対応するフラグメント値を書き込み, 距離値を0にする. 通常時と攻撃検知時の相違点を以下に述べる.

[i)**通常時**] ルータは一定の確率p_{low}で初期マーキングを行いながら, 自身を流れるパケットの監視を行う. ルータは監視しているトラフィックから攻撃の特徴を捉えると, 攻撃検知時の動作に移行する.

[ii)**攻撃検知時**] ADRは自身のマーキング確率を一時的に高い値 p_{high}に変更し, 以降は一定確率p_{high}でマーキングを行う.

【終端マーキング】ルータがパケットの転送時に行う処理である. 初期マーキングが行われなかった距離値0のパケットに対して, 自身のフラグメント値とパケットのフラグメント値の排他的論理和を取り, この値(以下, エッジIDと呼ぶ)をパケットに上書きし, 距離値を1つ増やす.

【転送処理】ルータが初期マーキング, 及び終端マーキングされなかったパケットに対して行う処理である. ルータはパケットの距離値を1つ増やす. 距離値は初期値を0とするため, R(d)がマーキングしたパケットの距離値はd-1となる.

4.3.4 経路再構築手順

本項では, トレーサが収集したリンク情報を基に攻撃経路を追跡する手順を示す. トレーサは一定時間パケットを収集した後, 収集したパケット中のフラグメント値とエッジIDを組み合わせる. このとき, 組み合わせが正しければ, リンク情報の奇数ビットのハッシュ値は偶数ビットに一致する.

トレーサは, 全てのNARを復元するまでパケットの収集, 経路再構築, 及びマーキング中止を繰り返し行う.

4.4 追跡スケジュール

ADMSは追跡の進行度によってマーキング確率を変化させるため, トレーサに集まる情報は追跡が進むごとに変化する. 追跡の初期段階では, 攻撃経路上には高いマーキング確率を設定したADRが点在するため, 収集されるリンク情報はADRの物が多い. 追跡が進むに従って, 追跡の終わったADRはマーキングを中止するため, トレーサが新たに得るリンク情報にADRのものは次第に含まれなくなる. 最終的に, トレーサが新たに得るリンク情報はADRを除く攻撃経路上のルータのものか, マーキング領域の初期値のみとなる. また, 復元されるリンク情報の組み合わせ数はトレースバックが進むに従って大きくなるため, 組み合わせの正しさを確認する時間も追跡が進むにつれて長くなる. このとき, 必要以上のパケットを追跡に用いると, それだけ確認する組み合わせも増えるため, 無駄に時間がかかると考えられる. そこで, 追跡の進捗状況によってパケットの収集間隔を変えることで追跡の効率化を図る. 追跡を3段階に分けた場合のスケジュールを図 3に示す. いずれの段階でも, トレーサは追跡とリンク情報の収集を並行して行う. 各段階について次に述べる.

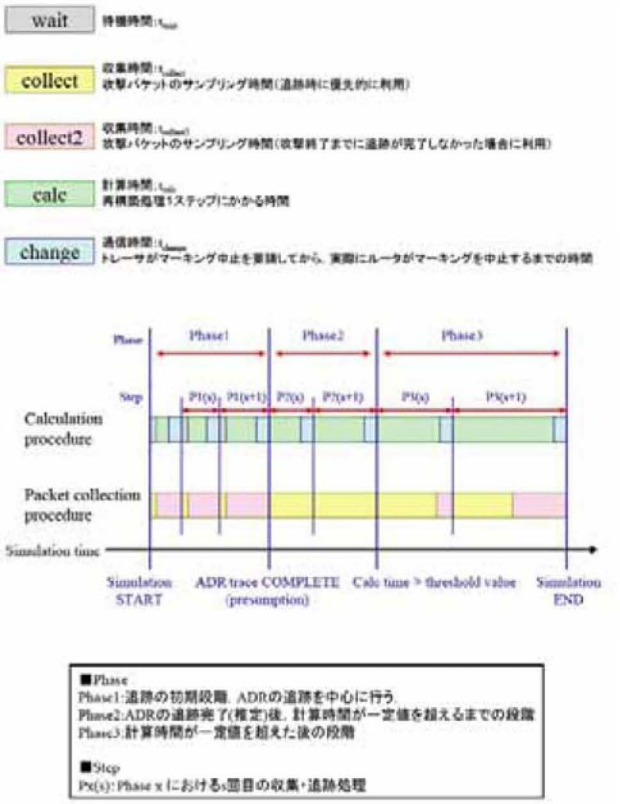


図 3 追跡スケジュール

【Phase1】トレースバックの初期段階では, 主にADRの追跡が行われる. ADRは, マーキング確率が高く, トラフィックが集中し, 追跡が完了するとマーキングを中止する特徴を持つため, Phase1の追跡には以下の特徴があると考えられる.

- 同じリンク情報を含むパケットが多い
- 計算時間が短い
- 1ステップごとに得られるリンク情報の種類が変化する

そこで, Phase1では追跡に利用するパケットを収集する時間$t_{collect}$を極短い時間に設定することで1ステップにかかる時間を短くし, マーキング中止命令をできる限り早く出すことを試みる. また, P1(s)において$t_{collect}$中に集められたパケットは, 同ステップ中の追跡に用いられる. また, P1(s)中に追跡できたルータが存在した場合, 追跡したルータに対してマーキング中止命令を出す. 計算・マーキング中止命令を行っている間に収集されたパケットは, $t_{collect}$中に収集されたパケットと同じリンク情報を所持している可能性が高い. そこで, $t_{collect2}$中に収集されたパケットは, 攻撃終了時に追

1) SNMP はルータ等のネットワークに接続された通信機器をネットワーク経由で監視・制御するためのプロトコルである[10]

跡が完了していなかった場合に追跡を継続する際に用いる予備情報として扱う．このとき，各時間の関係は，$t_{wait}=t_{collect}$，$t_{collect2}=t_{calc}+t_{change}$となる．また，1ステップ中に追跡できたルータが存在しなかった場合，マーキング中止命令を出す必要が無いため，$t_{change}=0$となる．

【Phase2】ADRの追跡が終わると，トレーサが得る情報にマーキング領域の初期値が含まれる割合が増加するため，計算時間が急激に増加する．そこで，計算時間が閾値t_{th1}を超えるとADRの追跡が殆ど終了したものとみなし，Phase2へと移行する．Phase2では，得られるリンク情報は追跡の進捗によって変化しないと考えられる．できる限り少ないステップ数で追跡を終えるために，P2(s+1)での計算にはP2(s)で収集されたパケット全ての情報を用いる．また，Phase2に入っても確実に全ADRの追跡が終わっているとは言い切れないため，トレーサは計算後にマーキング中止命令を発する．

【Phase3】ある程度追跡が進むと，収集した情報のうちマーキング領域の初期値の占める割合が大きくなるため，計算時間が非常に大きくなる．そのため，前ステップの計算中に得られたパケットをすべて利用すると，必要以上のパケットが利用されるために計算時間が大きくなってしまう．そこで，計算時間が閾値t_{th2}を超えると，Phase3に移行する．Phase3では，再構築に利用するパケット数を一定値に制限する．P3(s+1)での追跡には，P3(s)でt_{th2}の間に収集されたパケットを用いる．t_{th2}を超えて収集されたパケットは，攻撃終了時に追跡が完了していなかった場合に，継続して追跡を行う際に用いる予備情報として扱う．このとき，各時間の関係は，$t_{th2}= t_{collect}$，$t_{collect} + t_{collect2} = t_{calc}+ t_{change}$となる．

5． 評価

本章では，提案手法のスケーラビリティについて評価する．評価項目としてインターリーブ値の正当性をチェックする回数(計算量)，収集したパケットの総数(観察量)，追跡時間を図る．観察量を比較することでマーキング手法の上書き問題がどれくらい改善されているのか評価し，計算量を比較することでマーキング手法のリンク情報偽装問題をどれくらい改善されているのか評価する．また，追跡時間を計ることで実用性を評価する．比較対象として従来のマーキング手法，及び調整マーキング手法を評価する．初期のマーキング手法であるFMSと，FMSをマーキング確率の調整による追跡効率化という観点から改良したAPPM，DPPM，及び提案手法であるADMSについてシミュレーションを用いて評価を行う．しかし，FMSは観察量が非常に大きく，大規模な攻撃に対する評価を行うのに適していない．そこで，本論文では，FMSを拡張した Extended FMS (EFMS) を評価対象として用い，APPM，DPPM，

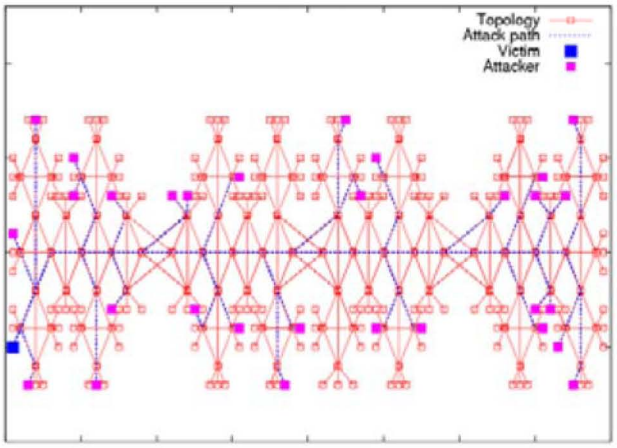


図 4 ネットワークトポロジ

ADMSをEFMSの拡張という位置づけでシミュレーションを行う．はじめに５．１節において，EFMSの有効性について数学的解析により示す．次に，５．２節において，シミュレーションに用いるネットワーク，攻撃モデルについて述べる．また，５．３節において，各手法における固有のパラメータ，および共用のパラメータを示す．５．４節では，以降の実験に用いる観察量，計算量，追跡時間の3つの評価項目について詳説する．そして，５．５節では，提案手法と従来手法を比較することで，提案手法の有効性を示す．

5.1 EFMS:Extended FMS

EFMSでは新たにマーキング領域としてToSフィールド[11]を採用することでリンク情報の分割数を減らす．ToSフィールドは通信の優先度を決めるフィールドであるが，通常の通信では用いられないため，正規通信への影響はごく小さいものであると考えられる．以下に，計算量の観点からFMSとEFMSの評価を行う．

5.1.1 計算量の評価

被害ノードからdホップ離れた位置にr_d個のルータがあり，これらのルータはリンク情報をk個のフラグメントに分割すると仮定する．ここで，簡単化のためマーキングパケットのみを対象とした場合の計算量について考える．このとき，FMSの計算量はr_d^8となる．同様に，EFMSの計算量は，r_d^4となる．従って，EFMSの計算量は，FMSの $r_d^4/r_d^8 = 1/ r_d^4$となる．例えば r_d=10のとき，EFMSはFMSの1/10000の計算量となることから，EFMSは非常に小さな計算量で追跡できることがわかる．

5.2 シミュレーション環境

5.2.1 ネットワークトポロジ

本論文では，トレーサが攻撃パケットと非攻撃パケットの正確な切り分けを可能とし，攻撃発生と同時に攻撃を検知できることを前提とする．また，ネットワークの通信遅延・輻輳・パケットロスは考慮しない．シミュレーションで用いたネットワークトポロジは，実際にインターネット上で構築されているトポロジを参考に構築した[12]．本ネットワークは，

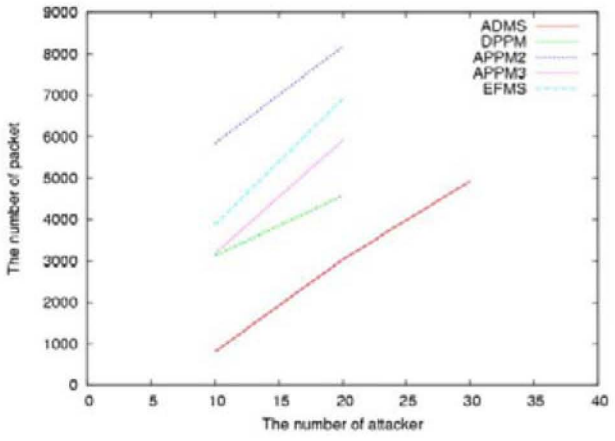


図 5　追跡に要するパケット数（観察量）

複数のリングネットワークが連結した状態を想定している．そして，攻撃経路はダイクストラ法によって導出した最短経路を用いて生成した．図 4は，シミュレーションで用いたネットワークトポロジを破線，及び攻撃経路を実線で表している．同図は，298個のルータを持つネットワーク上で，30人の攻撃者によって行われる攻撃の様子を示している．

5.2.2 攻撃モデル

現在最も頻繁に行われ，今なお頻度の増加が確認されているSYNflood攻撃を想定する[13]．攻撃レートは全攻撃者で等しく 10 packets/second (pps) で連続的に行われるものとする．攻撃者は10人から30人を想定し，DDoS攻撃全体の攻撃量は 100 pps ～ 300 pps で行われる．　また，各攻撃者から送信されたパケットは同時に被害ノードに届くものとする．攻撃パケット中のIPv4ヘッダは容易に変更することができるため，攻撃パケットはIPv4ヘッダ中の送信元アドレスが改竄されているものとする．同様に，提案手法を含む各マーキング手法による検出を逃れるため，識別子フィールド，ToSフィールドの初期値をランダムな値に設定し，さらにTTL値や距離値を調整しているものとする．

5.2.3 シミュレーション

シミュレーションでは，各手法のアルゴリズムをC言語で実装した．表1にシミュレーションに用いた計算機の仕様を示す．シミュレーションはトレーサが全てのNARを追跡完了した時点で終了する．ただし，DDoS攻撃は攻撃開始後3時間ほどでほぼ終了することから[2]，追跡時間が3時間を超えた時点で追跡失敗と見なし，シミュレーションを中断する．

5.3 前提条件

5.3.1 従来手法の前提条件

インターネット上の通信はそのほとんどが31ホップ以下であることから[8]，DPPM，及びAPPM-3においてc=32とする．また，DPPMはAPPM-1と同様のマーキング確率調整を行うこと，及びAPPM-1は通常の通信では利用できないことから，本論文

OS	Fedora Core 5
CPU	Pentium4 1.7GHz
Memory	1GB

表1　スペック表

ではDPPMはAPPM-1を実用的な観点から発展させた手法と考え，APPM-1は評価対象としない．また，APPM-2におけるd_2には，FMSにおける距離値dを用いる．

5.3.2 従来手法の追跡スケジュール

EFMS，DPPM，APPMにおけるトレースバック時のパケット収集プロセスと計算プロセスについて述べる．従来手法では，追跡の進捗状況によって得られるリンク情報の種類が変化することは無いため，提案手法におけるPhase2，及びPhase3を元にしたスケジュールで追跡を行う．ただし，マーキング中止命令を送信する必要がないため，t_{change}=0とする．Phase3に切り替わる閾値としてt_{th1}=3.0(second)を設定した．

5.3.3 提案手法の前提条件

通常のWebサーバの場合，100pps程の攻撃によって通信にタイムアウトが発生する[14]ことから，ルータが攻撃を検知する閾値として100ppsを設定した．また，トレーサがマーキング中止命令を発してからルータが実際にマーキングを中止するまでの時間を，ネットワークが輻輳している状態を想定して500msとする．高すぎるマーキング確率はルータ負荷になることから，p_{low}=0.1とした．また，Phase2に切り替わる閾値としてt_{th1}=1.0(second)を設定し，Phase3に切り替わる閾値としてt_{th2}=3.0(second)を設定した．

5.4 評価項目

5.4.1 観察量

追跡に用いたパケットの総数(観察量)を評価する．観察量は図 3の$t_{collect}$中に収集されたパケットの総数で表す．

5.4.2 計算量

追跡時に復元したリンク情報の正当性を確認した回数(計算量)を評価する．計算量CVは，距離値dを持つリンク情報の数をI(d)，距離値dを持つ正当なリンク情報の数をCI(d)とすると次の式で表すことができる．

$$CV = I(0) + \sum_{d=1}^{31} \mathrm{CI(d-1)I(d)}$$

5.4.3 追跡時間

追跡に要した時間について評価する．追跡時間は，提案手法ではt_{wait}，t_{calc}，t_{change}の総和となり，従来手法ではt_{wait}，t_{calc}の総和になる．

5.5 従来手法と提案手法の比較

ADMS，DPPM，APPM-2，APPM-3，EFMSの観察量，計算量，追跡時間を比較する．図 5，図 6，図 7に各手法の観察量，

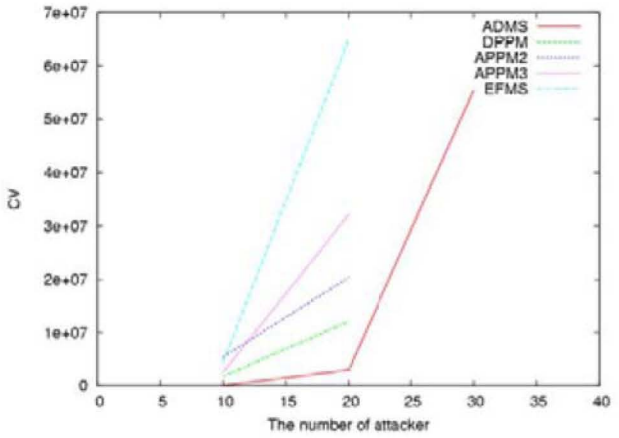


図 6 復元した情報の正しさを確認する回数（計算量）

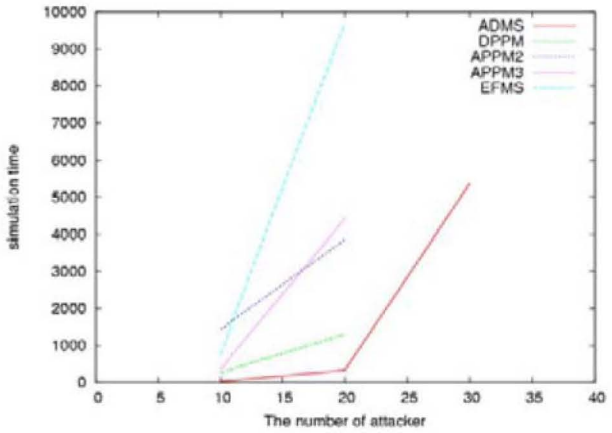


図 7 追跡時間

計算量，追跡時間を示す．ここでは，従来手法では攻撃者10，20の場合について，提案手法では攻撃者10，20，30の場合について示している．従来手法では攻撃者30のとき，いずれの手法も追跡時間が3時間を超えたため，追跡不能と判断した．このとき，提案手法は観察量，計算量，追跡時間のすべての点で従来手法よりも効率的に追跡できていることがわかる．このことから，攻撃経路ツリーを浅くしp_{low}を高い値に設定することは有効であると考えられる．

6．まとめ

本論文ではDDoS攻撃対策として有望なマーキング手法に着目し，そのスケーラビリティを向上する手法を提案した．提案手法では，ルータによる簡易な攻撃検知機能とマーキング確率の動的な制御により攻撃経路ツリーを擬似的に短くし，従来よりも高いマーキング確率の設定を可能にした．また，提案手法をシミュレーションで評価し，従来手法よりも大きな規模の攻撃に対して有効であることを示した．さらに，将来ルータの性能が向上し，高いマーキング確率を設定した場合にオーバーヘッドを殆ど生じない状況を想定し，より高いマーキング確率を用いてシミュレーションを行った．その結果，さらに効率的な追跡を行うことができることを確認した．今後の課題として，PCルータ等を使ってより高い確率でマーキングを行った場合のオーバーヘッドを評価することで，実用的なマーキング確率の高さを検証する予定である．

参考文献

[1] H. Burch, B. Cheswick: “Tracing Anonymous Packets to Their Approximate Source,” Proc. 2000 USENIX LISA Conf., pp. 319-327, (2000-12)

[2] D. Moore, G. Voelker, S. Savage: “Inferring Internet Denial-of-Service Activity”, Proc. of the 2001 USENIX Security Symposium, (2001-5)

[3] 門林雄基，大江将史：“IPトレースバック技術”，IPSJ Magazine, Vol. 42, No. 12, pp. 1175-1180, (2001-12)

[4] S. Savage, D. Wetherall, A. Karlin, T. Anderson: “Practical Network Support for IP Traceback,” Proc. SIGCOMM '00, pp. 295-306, (2000)

[5] T. Peng, C. Leckie, and K. Ramamohanarao: “Adjusted Probabilistic Packet Marking for IP Traceback,” NETWORKING '02: Proceedings of the Second International IFIP-TC6, Vol. 2345, pp. 697-708, (2002)

[6] 松木隆宏，松岡正明，寺田真敏：“IPマーキングによる不正活動ホストの広報機能の開発，” IPSJ-SIG Technical Reports 2008-CSEC-42, pp. 323-328, (2008-7)

[7] J. Liu, Z. Lee, and Y. Chung: “Dynamic probabilistic packet marking for efficient IP traceback,” Computer Networks, Vol. 51, pp. 866-882, (2007-2)

[8] W. theilmann, K. Rothermel: “Dynamic Distance Maps of the Internet,” In Proceeding of the 2000 IEEE INFOCOM Conference, (2000)

[9] 日吉龍：“IDS入門，” 技術評論社, (2004-4)

[10] J. Case, “A Simple Network Management Protocol (SNMP),” RFC1157, (1990)

[11] Philip Miller, 苅田 幸雄，“マスタリングTCP/IP 応用編，” pp. 88-93, (1998)

[12] OCN ネットワーク構成. http://www.ocn.ne.jp/business/info/pdf/ipbackborn¥_080521.pdf

[13] 警察庁技術対策課：“平成２０年上半期におけるインターネット治安情勢について，” (2008)

[14] 警察庁技術対策課：“DoS/DDoS対策について(検証)，” (2004)

[15] 古賀勝寛，岡崎直宣，渡邊晃，朴美娘：“動的マーキングを用いた効率的なネットワーク攻撃追跡手法の提案，” 電気学会論文誌, C08-141, (2009-3)