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

2003－DPS－114　(25)
2003－EIP－ 20　(25)
2003／8／29

DDoS 攻撃に対するアクティブシェーピング手法の評価

松 本 真 弥[†]　森 川 裕 介[††]　重 野　寛[†]
岡 田 謙 一[†]　松 下　温[†††,†]

帯域消費型 DDoS(Distributed Denial of Service) 攻撃の対策手法として, アクティブシェーピング手法が提案されている. アクティブシェーピング手法では, ネットワークノードが輻輳の原因となっているトラヒックを帯域制限することで, 防御側ホストに大量のトラヒックが流れ込む一次時被害を抑止する. それと同時に, 攻撃情報を攻撃経路上のネットワークノードに伝達し上流ノードでも対策することで, 正規トラヒックが低下してしまう二次被害を段階的に改善するものである. 本研究では, 広域ネットワーク上でのアクティブシェーピング手法の有効性を示すためにシミュレーション評価を行った.

Evaluation of Active Shaping Method against DDoS Attacks

Shin-ya Matsumoto,[†] Yusuke Morikawa,[††] Hiroshi Shigeno,[†]
Ken-ichi Okada[†] and Yutaka Matsushita[†††,†]

An Active Shaping Method is proposed as a countermeasure of flooding Distributed Denial of Service Attacks. In this method, routers near the victim effectively shapes the traffic of attacks. In addition, this method improves "secondary" damages to legitimate users by notifing the infomation of attacks to the upstream routers and upstream router's countermeasure. In this paper, we describe evaluation of this method on the wide area network and effectiveness of this method.

1. はじめに

2002 年 2 月に生じたアメリカの主要 Web サイトへの DDoS 攻撃 (Distributed Denial of Service Attack)[4], 以降, 各種 Web サイト, 電子商取引サイトにおいて DDoS 攻撃対策の需要が高まっている. DDoS 攻撃とは, 攻撃者が攻撃用のプログラムをセキュリティ対策のされていない多数のホストに侵入させ, 標的とするサーバやネットワークに対し各ホストから一斉に大量のトラヒックを送信する攻撃である.

DDoS 攻撃への対策手法として, アクティブシェーピング手法が提案されている. この手法では, サーバに大量にトラヒックが流れ十分なサービスが出来なくなってしまう一次被害を防ぎつつ, 正規ユーザのトラヒックまで廃棄してしまう二次被害を改善する. また, 文献[6],[13] ではアクティブネットワーク技術[10],[12] を用いてアクティブシェーピング手法を搭載したネットワークノードの設計, 実装を行っている. 本稿ではこのようなノードをアクティブノードと呼ぶ. アクティブノードを用いて DDoS 攻撃対策をするためには, 既存のネットワークノードとアクティブノードを交換する必要があり, すべてのネットワークノードを同時に交換するのは現実的には非常に難しい. しかしこれらの論文では, DDoS 攻撃への対策効果を得るために必要なアクティブノードの割合や実ネットワークへの導入順序などの議論が不十分である.

本稿では, 段階的なネットワークノードの交換を考慮したシナリオに基づいてシミュレーションすることで, アクティブシェーピング手法を実装したノードをどのような順序で, どの程度導入すれば DDoS 攻撃に対して有効であるか考察する. また, 一次被害, 二次被害の両方を考慮して適切な帯域制限値についても考察する. 以下, 2 章で DDoS 攻撃と既存の対策手法について, 3 章でアクティブシェーピング手法について説明し, 4 章で広域ネットワーク上での有効性を示すためのシミュレーション評価を述べ, 5 章でまとめと

† 慶應義塾大学理工学部
Faculty of Science and Technology, Keio University
†† NTT コムウェア株式会社
NTT COMWARE CORPORATION
††† 東京工科大学
Tokyo University of Technology

する.

2. DDoS 攻撃と既存の対策

DDoS 攻撃とは, 多数のホストから同時に大量のトラヒックを攻撃対象ホストへ送信することで, 攻撃対象ホストのネットワーク帯域やコンピュータリソースを消費し, 正規ユーザへのサービス提供を停止させてしまう攻撃である. この攻撃として代表的なものに TCP SYN Flood や UDP Flood などがあり [8], また送信元アドレスを偽装する Spoofing が行われることもある [5]. 攻撃者はウィルスなどを用いてセキュリティレベルの低い多数のホストにプログラムを埋め込み, これらのホスト (以下, 攻撃ホスト) が同時に攻撃トラヒックを送信することでこれを実現する. 広帯域かつ常時接続が一般的となった現在のインターネット利用状況下では, 一般ユーザの端末が攻撃ホストとなってしまうことが多く, DDoS 攻撃の脅威はさらに増大するだろう.

DDoS 攻撃の対策に関する研究としては,[3],[7],[9] などが挙げられる. これらの研究では, ISP バックボーンなどのネットワーク全体で攻撃パケットの帯域を制限をすることで, 標的のホストを守るモデルを提案している. しかし, これらの研究では一次被害を抑止することは可能であるが, 攻撃トラヒックの識別方法についての検討が十分に行われておらず, 対策によって正規トラヒックまで誤って帯域制限されてしまい, 二次被害が発生してしまう点が問題となっている. この二次被害の改善に着目した研究として次節に挙げるアクティブシェーピング手法がある.

3. アクティブシェーピング手法

アクティブシェーピング手法は ISP が管理するネットワークノードに付加価値のある機能として導入され, DDoS 攻撃対策を行ないたいホストに対して ISP がサービスを提供するためのものである. 本章では, この手法の基本コンセプトと帯域制御手法, バックトラックシェーピングについて説明する.

3.1 基本コンセプト

図 1 にアクティブシェーピング手法の概要を示す. 広域ネットワークのエッジにアクティブシェーピング手法を搭載したアクティブ化されたノードが存在し, 管理サーバが DDoS 攻撃の検出情報やアクティブノードを管理している. アクティブノードをネットワークのエッジにのみ配置したのは, 近年の Smart Edge, Fast Core の概念からなるもので, 攻撃トラヒックの検出やその情報の通知のような複雑な処理機能はエッジルータにのみ持たせるべきであるという考えに基づいている.

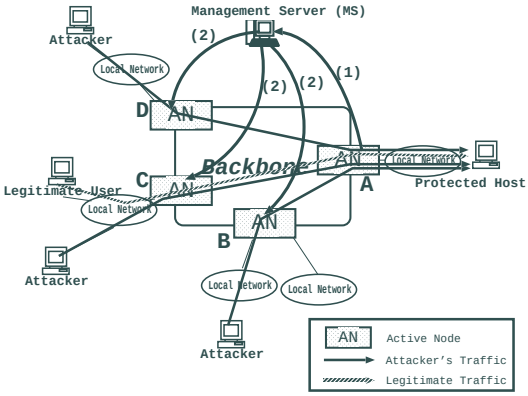

図 1 アクティブシェーピング手法の概念図

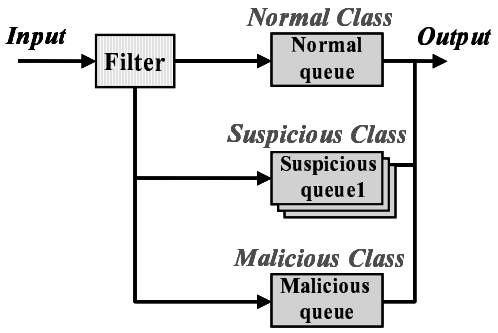

図 2 帯域制御モデル

図中のネットワークノード A はトラヒック監視機能を備えており, 対象サイトへ流れるトラヒックを監視している. アクティブシェーピング手法ではこのノードはアクティブノードであることを前提とし, このノードをルートノードと呼ぶ. 典型的な DDoS 攻撃手法である TCP SYN Flood, UDP Flood などによる攻撃を受け, ルートノードが異常なトラヒックパターンを検出すると, その原因となっているトラヒックの帯域制限をするとともに, 宛先アドレス, プロトコル番号, ポート番号などのトラヒックの属性を管理サーバ (MS) へ通知する (1). そして, 管理サーバは上流ノード B, C, D へこのトラヒック属性を通知する (2). これをバックトラックと呼ぶ. バックトラックの後, 上流ノードでも同様の帯域制限を行うことで, 攻撃を上流で阻止することが可能となり, 広域ネットワーク全体の帯域消費を抑えることが出来る.

3.2 適応型帯域制御手法

アクティブシェーピング手法では, 攻撃トラヒックを防ぎつつ二次被害を回復するために, 攻撃を検出す

るごとに帯域制御の変更を行う．これを適応型帯域制御と呼ぶ．適応型帯域制御を行うアクティブノードは**図 2** に示すように，出力インターフェースに 3 つのクラスが用意されている．また，各クラス毎に帯域制限値が設けられ，帯域制限値を越える速度で入力されるパケットを廃棄することで帯域制限値以上のトラヒックが流れない仕組みになっている．この操作をシェーピングと呼ぶ．

ルートノードが攻撃を検出すると，その原因となっているトラヒックの宛先アドレス，プロトコル番号，ポート番号などの属性値から暫定的な攻撃トラヒック識別子である Suspicious シグネチャを作成する．DDoS 攻撃には，大量のトラヒックが長期間流れるという特徴があるため，防御側ホストによって設定される帯域と時間に関する閾値を用いて攻撃を検出する．この Suspicious シグネチャには攻撃トラヒックの属性値が含まれており，上流でもこのシグネチャを用いて帯域制限を行う．このように異常トラヒック毎の識別子を用いることで，異常トラヒックのみを帯域制限し，正規トラヒックの二次被害を防ぐことが可能となる．しかし，この時点では識別確度に限界があり，攻撃トラヒックと同じ属性値をもつ正規トラヒックは Suspicious シグネチャによって攻撃トラヒックと同様に帯域制限されてしまう．

適応型帯域制御手法では攻撃トラヒックの識別確度を上げるために，Suspicious シグネチャにより分類されたトラヒックを送信元アドレスやパケット長などの属性値に関して統計的に解析し，攻撃と断定できたトラヒックに関してはその属性値を用いて Malicious シグネチャを作成する．

ここで作成された 2 種類のシグネチャを用いて，アクティブノードではトラヒックを分類し，Suspicious シグネチャにマッチするトラヒックは Suspicious クラスに，Malicious シグネチャにマッチするトラヒックは Malicious クラスに分類される．Suspicious クラスには攻撃とは断定できない異常トラヒックが分類され，帯域制限値は 3.3 節で述べる手法によって決定される．一方，Malicious クラスには攻撃トラヒックと断定されたトラヒックが分類されるため，帯域制限値は 0 か 0 に近い値に設定されている．

各クラスへの適合性の判断は Malicious, Suspicious の順に行ない，いずれにも分類されなかったトラヒックは Normal クラスに分類される．このモデルを用いることで攻撃と断定できるトラヒックは Malicious クラスによって大幅に削減できる．また，疑わしいトラヒックは Suspicious クラスによって抑えつつ，誤って識別された正規トラヒックもある程度流すことが可能となる．

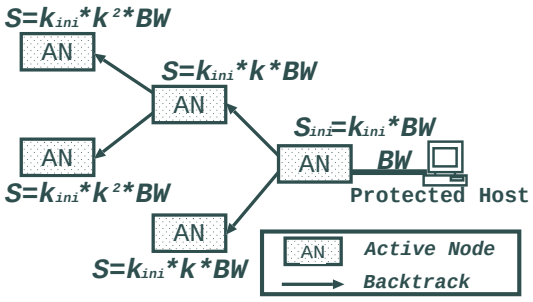

図 3 バックトラックシェーピング

3.3 バックトラックシェーピング

バックトラック機能により管理サーバから Suspicious シグネチャを受け取ったアクティブノードは，そのシグネチャにマッチするトラヒックが大量に流れシェーピングが行われた場合さらにバックトラックを行い，より上流でシェーピングを行う．

図 3 にバックトラック時の帯域制限値を示す．各アクティブノードでの Suspicious クラスの帯域制限値は，2 つの係数 k_{ini}, k を用いて計算される．攻撃を検出したノードでの帯域制限値 S_{ini} は以下のように定義される．

$$S_{ini} = k_{ini} * BW (0 < k_{ini} < 1) \quad (1)$$

k_{ini} の値は，防御側ホストが ISP と契約する時に，防御側ホストのセキュリティポリシーによって設定される．BW は防御側ホストのアクセス回線の帯域である．

一方，あるノードでのシェーピング値を S とした時，バックトラック後の上流ノードでの帯域制限値 S' は以下のように定義される．

$$S' = k * S (1/n < k < 1, n : \text{上流ノード数}) \quad (2)$$

Suspicious クラスは暫定的に識別された攻撃トラヒックであるため，正規トラヒックもシェーピングされてしまう可能性がある．そのため，この k の値は ISP 管理者が適切な値に設定する必要がある．

4. シミュレーション評価

アクティブシェーピング手法の十分な対策効果を得るために必要な，アクティブノードの導入割合や，アクティブノードの導入順序，Suspicious シェーピングの係数の検討を目的として，以下のようなコンピュータシミュレーションを行なう．

シミュレーション 1: 単一ドメイン内でアクティブノードの割合を変化させた時の攻撃トラヒック

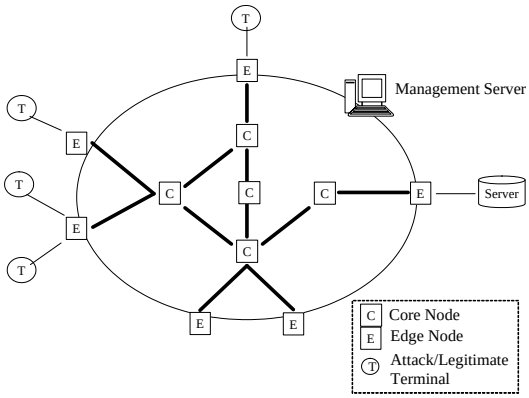

図 4 単一ドメイン内でのネットワークトポロジー

表 1 シミュレーション 1 おけるシミュレーションパラメータ

ドメイン内のエッジノード数	100
ドメイン内のコアノード数	100
攻撃元ホスト	**図 4** の T からランダムに 10 個
防御側ホストへの攻撃トラヒック	1〜5Mbps の乱数値
防御側アクティブノードでの攻撃トラヒック検出閾値	6Mbps, 60sec

の識別誤差を測定し, DDoS 攻撃への対策効果を得るために必要なアクティブノードの割合を検討する.

シミュレーション 2: 複数のドメインにおいて, アクティブノードの導入過程を想定して作成したシナリオ上で, 攻撃トラヒックに対する正規トラヒックの割合を測定し, アクティブノードの導入順序を検討する.

シミュレーション 3: Suspicious シェーピングの帯域制限値を変動させた時の攻撃トラヒックと正規トラヒックのスループットを測定し, Suspicious シェーピング時の適切な係数を検討する.

本シミュレーションでは, シミュレータとして, Network Simulator version 2(ns-2) を使用し, アクティブシェーピング手法を実装した. OS には RedHat Linux 7.1, 個々の機能の実装には C++を利用し, またシミュレーション全体の動作を記述するために Tcl を使用した.

4.1 シミュレーション 1

図 4 に単一ドメイン内を対象としたシミュレーションにおけるネットワークトポロジーを示す. 本トポロジーでは, Core Node 間は半メッシュ状, Edge Node と Core Node は n 対 1 で接続されている. 図中において, コアネットワークのリンクは 100Mbps, アクセスリンクは 10Mbps とした.

アクティブノードの導入割合によるアクティブノードでの攻撃トラヒックの識別確度を調べるため, 図 4 のトポロジーにおいて**表 1** に示すパラメータでシミュレーションを行なった. ルートノードでは, 大量のトラヒックが長期間流れるという DDoS 攻撃の特徴から, 同じ宛先アドレス, プロトコル番号, ポート番号を属性値として持つトラヒックが 6Mbps 以上, 60 秒間以上流れたときに攻撃として検出するものとした.

アクティブノードで確実に攻撃トラヒックを識別できると仮定した場合, 攻撃元ホストに最も近いエッジノードで攻撃トラヒックを識別し, バックボーンネットワークへ流れる攻撃トラヒックのシェーピングが可能となる割合の期待値は, バックボーンに導入されたアクティブノード数 N_A, 全エッジノード数を N_E としたとき以下のようになる.

$$E_d = \frac{N_A}{N_E} \tag{3}$$

この時の E_d はアクティブノードを通過する攻撃トラヒックは 100% 識別できるときの割合であるため, これ以上の期待値で攻撃トラヒックの対策をすることは理論的に不可能である. そこでこの E_d を理想対策割合と呼ぶ. 単一ドメイン内を対象としたシミュレーションでは, 理想対策割合に対する実際の対策割合の期待値の誤差率 Err をアクティブシェーピング手法の対策効果の指標として定義し, 実測した対策可能割合の期待値を E_f とすると以下のようになる.

$$Err = \frac{E_d - E_f}{E_d} \times 100[\%] \tag{4}$$

この Err は理想対策割合との誤差であるため, アクティブノードでの攻撃トラヒックの識別誤差を意味することになる. **図 5** に単一ドメイン内において攻撃元ノード数を変えたときの全エッジノードに対するアクティブノード導入割合と攻撃トラヒックの識別誤差の関係を示す.

アクティブノードの導入割合が増えると識別誤差が減少しているのがわかる. これは多くのアクティブノードを導入することでバックトラックの回数が増え, より上流での対策が可能となったためである. 逆にアクティブノードが少ないとバックトラックの回数が少なくなり, 攻撃元ホスト近くにあるアクティブノードまで攻撃情報が伝達されず, 識別誤差が増大してしまう. 特にアクティブノードの導入割合が 30% 以下の場合はグラフの傾きが大きいことから, アクティブノードの導入割合を増やすことで大きな対策効果を得ることが出来ている. 一方, アクティブノードの導入割合が 30% 以上になるとグラブの傾きが小さくなり, アク

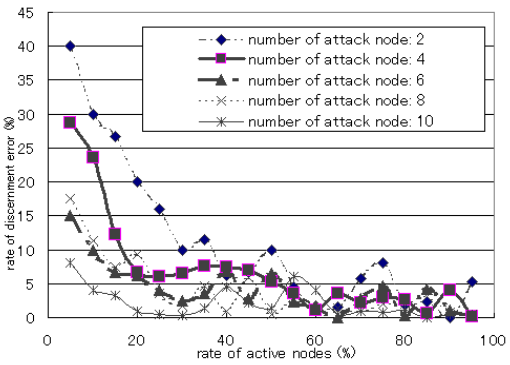

図 5 攻撃トラヒックの識別誤差

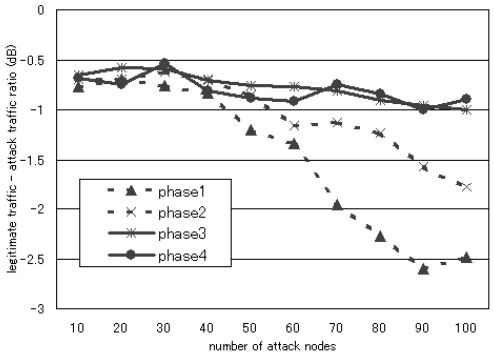

図 7 シミュレーション 2 における正規トラヒック割合

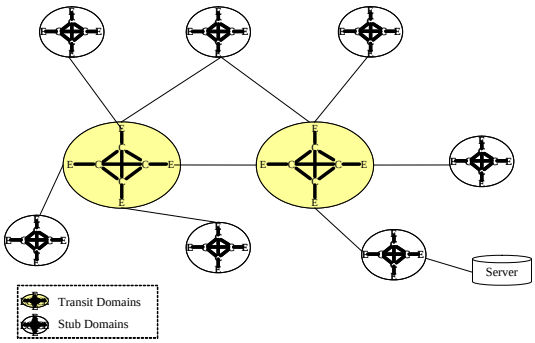

図 6 複数ドメインでのネットワークトポロジー

表 2 シミュレーション 2 におけるシミュレーションパラメータ

ドメイン内のエッジノード数	10
ドメイン内のコアノード数	100
総ドメイン数	10
サーバへ正規トラヒックを流すノード	10

ティブノードの導入割合を上げてもさらなる改善効果は見込まれない．したがって，アクティブノードの導入割合は 30% が十分な値と考えられる．

4.2 シミュレーション 2

図 6 に，複数のドメインを接続した場合のトポロジーを示す．本シミュレーションにおいてドメイン間は Stub-Transit モデル [11)2)] で接続し，Stub ドメインとはユーザ端末などと直接接続する可能性があるドメインである．一方，Transit ドメインとはユーザ端末と直接接続することは無く Stub ドメイン同士あるいは Stub ドメインと Transit ドメインを接続する機能を持つドメインである．実際のバックボーンネットワークにおいてドメイン間は 1〜5Gbps 程度の帯域で接続されている [1)]．これを参考に，ドメイン間を 1Gbps とした．

模擬した広域ネットワークのシミュレーションパラメータを**表 2** に示す．そして以下のシナリオに従ってシミュレーションを行い，正規トラヒック及び攻撃トラヒックのスループットをそれぞれ測定した．なお，このシナリオは ISP 内でアクティブノードが導入されていく過程を想定して作成した．

フェーズ 1: 防御側ホストを収容するエッジノードと防御側ホストを収容するドメインの BN をアクティブノードにする (BN: Border Node, 他のドメインと接続するノード)．

フェーズ 2: 防御側ホスト収容するドメイン内の全エッジノードをアクティブノードにする．

フェーズ 3: 全 BN をアクティブノードにする．

フェーズ 4: 全エッジノードをアクティブノードにする．

対策効果を表す指標として，防御側ホストに流れる正規トラヒックの比率を表す R を以下のように定義する．

$$R[dB] = 20 \times \log \frac{\text{正規トラヒックのスループット}}{\text{攻撃トラヒックのスループット}}$$

サービス提供側にとってサーバの存在意義はサービス提供にリソースを使うことであり，攻撃トラヒック量や正規トラヒック量の絶対的な値よりも，正規トラヒックの処理にリソースが使用された割合が重要である．処理しきれない正規トラヒックは，CDN 技術などを用いて他のプロキシサーバに処理させればよく，サーバを無駄なく使用することが重要である．R はこの無駄を表す指標として新たに定義した値であり，ネットワーク帯域利用の SN 比を表すものである．

図 7 に攻撃ホスト数を変化させたときの R を示す．フェーズ 1 とフェーズ 2 を比較するとアクティブノード数が 50 を超えたあたりから変化があり，フェーズ 1 に比べてフェーズ 2 は R の値が大きい．したがって，防御側ホストを収容するドメインの BN だけでな

表 3 シミュレーション 3 におけるシミュレーションパラメータ

攻撃トラヒック	UDP(1Mbps/Node)
攻撃トラヒックのノード数	100
正規トラヒック	TCP(150kbps/Node)
正規トラヒックのノード数	20

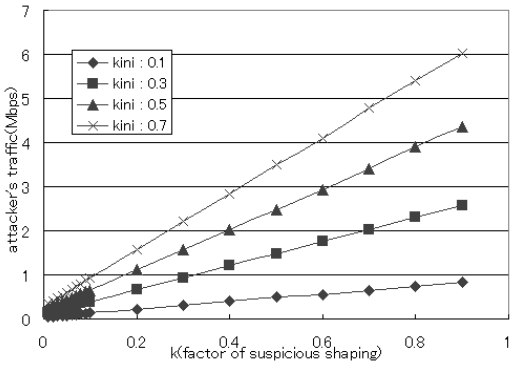

図 8 シェーピング値による攻撃トラヒックの変化

く, 防御側ホストを収容するドメインの全てのエッジノードをアクティブノードにすることで DDoS 攻撃に対する対策効果が得られることがわかる. アクティブノードの導入を全ての BN にまで増やしたフェーズ 3 では, 攻撃ノード数を増やしても R の値が減少せず, 高度に分散化された DDoS 攻撃に対してはフェーズ 2 よりも対策効果が上がったと考えられる. また, フェーズ 4 と比較しても対策効果が下がっていないことから, フェーズ 3 までアクティブノードを導入することで十分な対策効果を得ることができる.

4.3 シミュレーション 3

3.3 節で定義した Suspicious シェーピングにおける係数 k, k_{ini} と攻撃トラヒックおよび正規トラヒックのスループットの関係を調べるために, 前節のフェーズ 3 に基いてシミュレーションを行なう. **表 3** にシミュレーションパラメータを示す.

図 8 にシェーピング係数 k を変化させたときのバックボーンネットワークへ流れる攻撃トラヒックのスループットを示す. この図から係数 k_{ini} によらず, 係数 k を小さくすることで Suspicious クラスの帯域制限値が小さくなり, 攻撃トラヒックを削減できていることがわかる. しかし Suspicious クラスには暫定的な攻撃トラヒックが流れるため, 正規トラヒックも同時に削減している可能性が考えられる. そこで, 防御側ホストへ流れる正規トラヒックのスループットを測定し, **図 9** に示す. k を大きくし上流ノードでのシェーピングを緩和すると正規トラヒックのスループットが大きくなっている. これは, Suspicious クラスの帯域制限

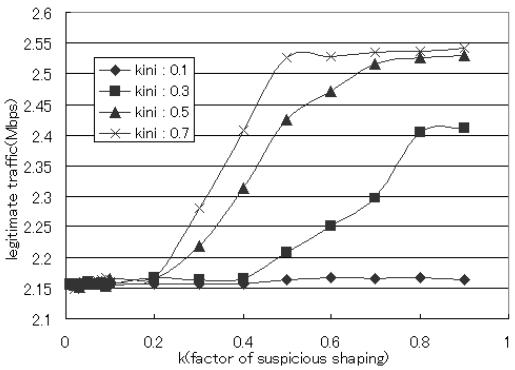

図 9 シェーピング値による正規トラヒックの変化

値を大きくすることで, 誤って攻撃と識別された正規トラヒックのスループットも上がったためと考えられる. 逆に k を小さくすると, 攻撃トラヒックと同様に Suspicious クラスによってスループットが小さくなってしまっている. このように攻撃トラヒックの阻止と正規トラヒックの回復はトレードオフの関係にあるが, $k < 0.2$, $k > 0.8$ では正規トラヒックのスループットに変化がないことから, 防御側ホストが $0.2 < k < 0.8$ で決定する必要があると考えられる.

5. ま と め

本稿では, DDoS 攻撃対策における二次被害対策を実現するアクティブシェーピング手法の有用性を示すためにシミュレーション評価を行なった. アクティブシェーピング手法では, バックトラックによって攻撃の検出時に攻撃トラヒック情報を共有し, 攻撃先ノードだけでなく攻撃元ホストに近い上流ノードにおいても帯域制御を行う手法である.

しかし, アクティブシェーピング手法を実際に広域ネットワークへ展開するためには, 既存のネットワークノードの一部を交換し, アクティブノードを導入する必要がある. 本稿では, アクティブノードの導入割合や導入順序, 帯域制限値の適切な設定をシミュレーションを通して検討した. シミュレーション 1 よりアクティブノードは全エッジノードに対して 30% 程度導入することで十分な対策効果が得られることを示した. また, シミュレーション 2 より全てのエッジノードをアクティブノードと交換しなくても, ドメイン間に存在するボーダーノードへ重点的に導入することで効果を得られることを示した. そしてフェーズ 3 より, Suspicious シェーピングの係数の適切な値は $0.2 < k < 0.8$ であることを示した.

参 考 文 献

1) インターネット白書 2002. 株式会社インプレス, 2002. 財団法人インターネット協会 監修.
2) K.I. Calvert, M.B. Doar, and E.W. Zegura. Modeling Internet Topology. *IEEE Communications Magazine*, pp. 160–163, June 1997.
3) E.Y. Chen. AEGIS:An Active-Network-Powered Defense Mechanism against DDoS Attacks. In *Proceedings of IWAN2001*, pp. 12–17, April 2000.
4) L. Garber. Denial-of-service attacks rip the internet. In *IEEE Computer*, pp. 12–17, April 2000.
5) L.M. Gil and M. Poletto. MULTOPS: A Data-Structure for Bandwidth Attack Detection, booktitle = The 10th USENIX Security Symposium, pages = 23-38, year = 2001, month = .
6) D. Kashiwa, E.Y. Chen, H. Fuji, S. Machida, H. Shigeno, K. Okada, and Y. Matsushita. Active Countermeasure Platform against DDoS Attacks. *IEICE Transactions on Infomation and Systems*, Vol. E85-D, No. 12, pp. 1918–1928, December 2002.
7) R. Mahajan, S.S. Dellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker. Controlling high bandwidth aggregates in the network - extended version. 2001.
8) D. Moore, G.M. Voelker, and S. Savaeg. Inferring Internet Denial-of-Service Activeity. In *Proc. 10th USENIX Security Symposium*, 2001.
9) D.Schnackenberg, K.Djahandari, and D.Sterne. Infrastructure for intrusion detection and response. In *Proceedings of the DARPA Information Survivability Conference and Exposition(DISCEX*, 2000.
10) D.L. Tennenhouse, J.M. Smith, W.D. Sincoskie, D.J. Wetherall, and G.J. Minden. A Survey of Active Network Research. *IEEE Communications Magazine*, pp. 80–86, 1997.
11) E.W. Zegura, K.L. Calvert, and S.Bhattacharjee. How to model an internetwork. In *Proceedings of IEEE Infocom 1996*, pp. 594–602, 1996.
12) 山本幹. アクティブネットワークの技術動向. 電子情報通信学会論文誌, pp. 1401–1412, 2001.
13) 柏大, E.Y. Chen Chen, 冨士仁, 重野寛, 岡田謙一, 松下温. 広域ネットワークへの適用を考慮したアクティブフロー制御プラットフォーム. 情報処理学会論文誌, Vol. 44, No. 3, pp. 647–659, March 2003.