# Pi 方式と Pushback 方式を組み合わせた DDoS 攻撃防御方式の評価

金子　陽一　木村　成伴　海老原　義彦
筑波大学大学院　システム情報工学研究科

## 1. はじめに

分散型サービス運用妨害(DDoS: Distributed Denial of Service)による攻撃は，正当なユーザが発するパケットを偽装して行われており，その防御は一般に困難である．著者らは既に DDoS 攻撃対策方式である Pi (Path Identification)[1]方式と，Pushback[2]方式を組み合わせた改良方式を提案している[3]．本論文では，本提案方式を用いたシミュレーション実験を行い，その有効性を確認する．

## 2. Pi 方式と Pushback 方式

Pi 方式は，各ルータで固有値をパケットにマークすることで，攻撃者の真の送信元を推定する方法である．
本方式の動作例を図 1に示す．ここで，Pi 値のフィールド長を N=4 ビット，各ルータがマークするビット長を n=1 ビットとする．まず，ノード N1 があて先 V にパケットを送信したとする．このパケットを最初に受け取るルータ R5 は，Pi 値をそのネットワークインターフェースに対応する番号（ここでは 0000）に初期化する．そして，この Pi 値フィールドの値を 1 ビット左シフトして，これによって空いた下位 1 ビットにマーキング値（例えばルータの IP アドレスのハッシュ値の下位 1 ビット）1 を書き込む．その結果，Pi 値は 0001 となる．同様にして，次のルータ R4 を通過する時，このパケットの Pi 値は 0011 となり，ルータ R1 を通過する時には R5 で書き込まれたマーキング値は失われる．最後に，V の直前のルータ R0 において，その時点での Pi 値ごとにパケットの単位時間当たりの到着量を測定する．この値が閾値を超えていた場合，その Pi 値のパケットを攻撃パケットとみなし，フィルタリングを行う．そうでなければ，これらのパケットをあて先 V へ転送する．なお，R0 ではパケットのフィルタリング制御を行うため，このルータではマーキングは行わない．

The Evaluation for the Combination Method of Pi Method and Pushback Method to Defense against DDoS Attacks
Yoichi Kaneko, Shigetomo Kimura, and, Yoshihiko Ebihara,
Graduate School of Systems and Information Engineering,
University of Tsukuba

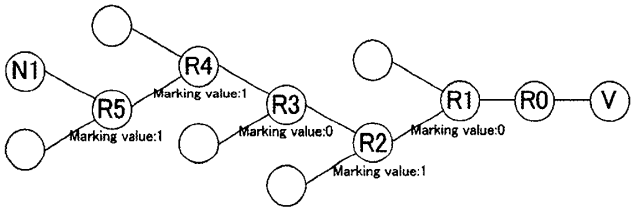


**図 1　Pi 方式の動作概略図**

Pushback 方式は，ルータが特定のあて先に対するトラフィックの総帯域が閾値以上になった時，上流のルータに対して帯域制限の要求（Pushback リクエスト）を出す事によって防御を行う方式である．本方式では，各あて先へのトラフィックの総帯域を一定値以下に抑制することを主な目的としている．そのため，各あて先へのトラフィックそれぞれには，その到着量に応じて閾値で定めた総帯域が分配される．すなわち，攻撃者からの過剰なトラフィックであっても，ある程度の帯域が配分される．

## 3. 提案方式の評価

著者らは，前章で述べた２つの方式を組み合わせた DDoS 防御方式を提案している[3]．この方式において，あるルータがあるホスト V あての Pi 値が p であるパケットの単位時間当たりの到着量が閾値 x を超えており，同パケットが攻撃パケットであると判断したとする．このとき，同ルータは当該パケットを遮断するとともに，Pi 値が p となるパケットを送信しているすべての上流ルータへ Pushback リクエストを送信し，あて先 V に対する閾値 x を通知する．この動作を繰り返し，可能な限り攻撃パケットの送信元ノードまで近づいて，Pi 方式による防御を行う．

本章では，この方式の評価を行うため，図 2に示す完全二分木のネットワークモデルを使用したシミュレーション実験を行う．この図において，パケットを送信するノードは 128 台，ルータは 7 段の構成となっており，全てのパケットはあて先 V が接続するルータ R0.0 に到達するまでに 6 つのルータを経由する事となる．各リンクの帯域は，図に示したもの以外は 1Gbps とした．パケットの Pi 値フィールドは 8 ビット，各ルータがマーキングする値は 2 ビットであり，4 ホップ前までの情報を保有する事ができる．各ルータはシミュレーションの開始時にマークす

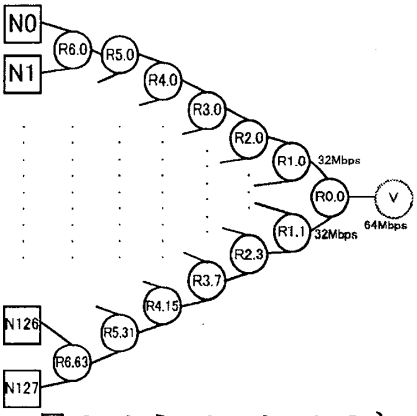


図 2　シミュレーションのネットワーク図

る値をランダムに決定し，以降は変更を加えない．そして，攻撃ノード 16〜64 台をランダムに選択し，攻撃ノードは 10Mbps，それ以外の通常ノードは 0.5Mbps で V に 5000 ビットのパケットを送り続ける．このとき，各ルータで防御しない場合，Pi 方式，Pushback 方式，提案方式をそれぞれ用いる場合についてシミュレーションを２５回ずつ行い，その平均を求める．ここで，Pi 方式と提案方式の場合は，特定の Pi 値のトラフィック量が 5Mbps 以上であればそれを攻撃パケットと判定する．Pushback 方式の場合はあて先 V に到達するトラフィック量の合計が 64Mbps となるように帯域の分配を行う．

シミュレーションの結果を図 3に示す．図において，到着はルータ R0.0 に到達したパケット，ドロップはリンク帯域の飽和によりパケットを破棄したパケット，遮断は防御方式によって破棄したパケットの総到着速度の平均をそれぞれ示している．なお，すべての結果は信頼レベル 90%で精度 10%を満たすことを確認している．

図の結果より，提案方式は通常ノードからのパケットを遮断しておらず，また，Pushback 式と比べても，通常ノードの到着や攻撃ノードの遮断がそれぞれ 74〜130%，53〜195%高い事が分かる．これは，提案方式では，Pushback 方式により攻撃ノードに近づき，Pi 方式で攻撃ノードを推定しながら攻撃パケットを遮断することから，他方式より多くの攻撃パケットを遮断し，その分だけ通常パケットが R0.0 に到着できたためである．

## 4. まとめ

Pi 方式，Pushback 方式，提案方式のそれぞれについて，シミュレーションによる比較評価を行った．その結果，提案方式の方が攻撃パケットをより遮断し，その分，通常パケットがあて

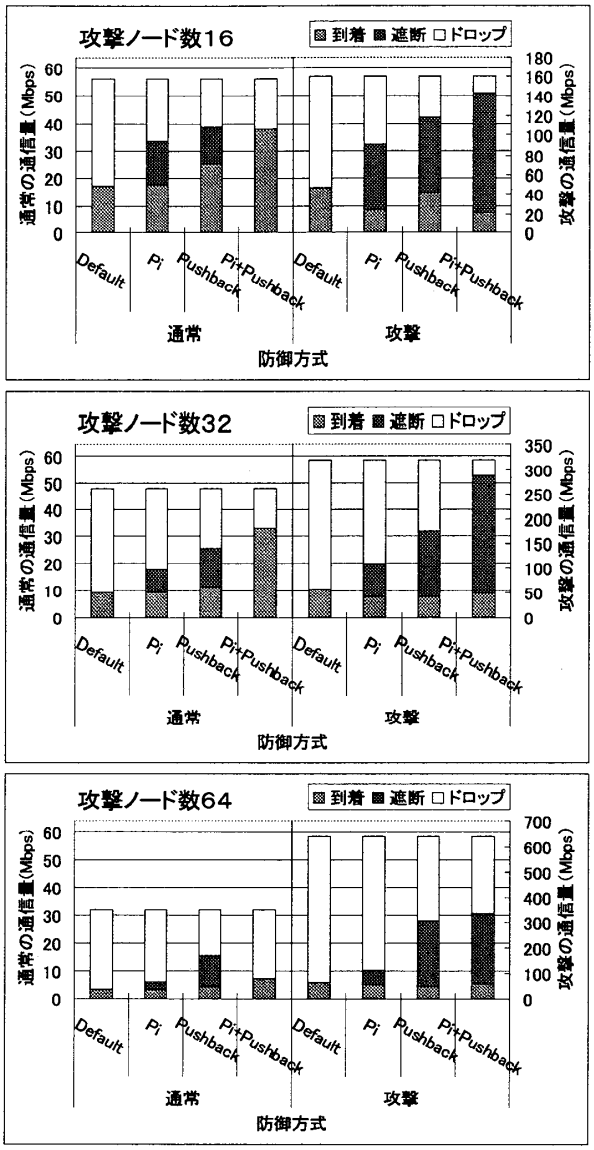


図 3　シミュレーション結果

先により到着することが確認された．しかし攻撃ノードが 64 台の場合，通常パケットが 77%もドロップしており，これを改善することなどが今後の課題である．

参考文献

[1] Abraham Yaar, Adrian Perrig, and Dawn Song, “Pi: A Path Identification Mechanism to Defend against DDoS Attacks,” Proceedings of the 2003 IEEE Symposium on Security and Privacy (SP’03), pp.93–107, 2003.

[2] John Ioannidis and Steven M. Bellovin, “Implementing Pushback: Router-Based Defense Against DDoS Attacks,” Proceedings of Network and Distributed System, pp. 1–12, 2002.

[3] 金子陽一，木村成伴，海老原義彦, “Pushback 方式を導入した Path Identification 方式による DDoS 攻撃防御対策の提案,”信学技報, IN2006-132, 情報ネットワーク, Vol.106, No.420, pp. 109-114, 2006.