プロキシを用いた分散サービス不能攻撃回避方式の提案

萱島 信[†1,†2] 松本 勉[†2]

今日，インターネット技術を用いたネットワークでは，サービス不能（Denial of Service，DoS）攻撃対策が重要になりつつある．DoS 攻撃手法は，ホストの脆弱性を悪用する脆弱性攻撃タイプと，大量の IP パケットでホストやネットワークのリソースを使い尽くす Flood 攻撃タイプがある．特に後者は，分散サービス不能攻撃（Distributed DoS，DDoS）の出現で深刻化している．そこで本論文では，分散 DoS 攻撃の影響を回避する方式を提案する．本提案方式は，アクティブ計測手法である One-Packet 方式とパケットペア/パケットトレイン方式の長所を組み合わせて実現した “パストラフィック推測機構” と，TCP プロキシを用いたオーバレイネットワークで実現した “代替パス構築機構” により構成される．本論文では，Flood 攻撃のシミュレーションにより，パストラフィック推測機構が従来の帯域推定手法より有効に機能することを示した．さらに，代替パスを構成する他の実現方法との比較により，代替パス構築機構の実用性を評価した．

Distributed Denial-of-service Attack Avoidance Method Using Proxy

Makoto Kayashima[†1,†2] and Tsutomu Matsumoto[†2]

On Internet-based networks, defending networks against attacks, particularly denial-of-service (DoS) attacks, is becoming important. DoS attack methods can be classified into two types: the first type uses a security hole in a target host, and the second type exhausts network bandwidth by sending a large number of data packets to a target. The second type is becoming more of a problem because distributed DoS attacks are now taking place. We have developed a method that reduces the severity of distributed DoS attacks. Our method uses two mechanisms: an “path traffic estimation mechanism”, which works by combining one-packet and packet-pair models; and a “substitution path construction mechanism”, which uses a tcp-proxy. We demonstrated that “path traffic estimation mechanisms” effectively reduced the severity of a simulated flood attack. And we demonstrated that “substitution path construction mechanism” is more practical than usual method.

1. まえがき

インターネット技術を用いて構築されたネットワークシステムは，企業などの組織にとって不可欠な情報システムのインフラとなりつつある．その一方で，それらのネットワークシステムに対するさまざまなセキュリティの脅威もまた増大している．

セキュリティの脅威の 1 つに，システムの可用性を損なうことを目的とする，サービス不能（Denial of Service，DoS）攻撃がある．ネットワークシステムに対する DoS 攻撃は，ホストもしくはゲートウェイのセキュリティホールを狙う脆弱性攻撃タイプと，大量の IP パケットを送信する Flood 攻撃タイプに大別することができる．

脆弱性攻撃タイプについては，ホストにパッチを適用する，もしくは，ネットワーク型の侵入防止システム（Intrusion Prevention System，IPS）などを用いて，セキュリティホールを攻撃する IP パケットを識別したうえで遮断するなどの対策が行われている．一方 Flood 攻撃タイプは，多数のホストから攻撃パケットを送信する分散サービス不能（Distributed DoS，DDoS）攻撃の出現により，ますます深刻な問題になりつつある．代表的な Flood 攻撃の手法として，以下のようなものが知られている．

(1) SYN Flood [1)]
TCP のコネクションの成立を行わず，ハーフオープン状態のコネクションを攻撃対象ホストに大量に送信する攻撃手法である．多くの場合，送信元アドレスは偽造される．攻撃を受けたホストは，タイムアウトまで ACK パケットを待ち続けるため，TCP コネクション管理テーブ

†1 日立製作所システム開発研究所
Systems Development Laboratory, Hitachi Ltd.
†2 横浜国立大学大学院環境情報学府/研究院
Graduate School of Environment and Information Sciences, Yokohama National University

ルのメモリが消費されたままになる．

(2) Connection Flood [2)]
攻撃対象ホストに対し，大量の TCP コネクションを成立させ，ソケットを占拠する攻撃手法である．TCP コネクションを確立するため，送信元アドレスは詐称されていない．

(3) UDP Flood [2)]
攻撃対象ホストに大量の UDP パケットを送信する攻撃手法である．ネットワークの帯域を占有するだけでなく，攻撃に短い UDP パケットを使用すると，ゲートウェイに負荷をかけることもできる．多くの場合，送信元アドレスは偽造される．UDP パケットの代わりに ICMP パケットを使用する Ping Flood も同様の攻撃手法である．

(4) Smurf [3)]
送信元アドレスを攻撃対象ホストに偽造した ICMP Echo Request パケットをブロードキャストドメインに送信する攻撃手法である．ドメインに存在するホストに，攻撃対象ホストに向けた ICMP Echo Reply パケットを返信させ，ネットワークの帯域を占有する．

(5) DrDoS [4)]
送信元アドレスを攻撃対象ホストに偽造した SYN パケットを，複数の踏み台ホスト（Reflector と呼ぶ）に送信する攻撃手法である．Reflector は，攻撃対象ホストに SYN/ACK パケットを送信するが，攻撃対象ホストは実際に SYN パケットを送信しておらず，ACK パケットを返送しない．このため，複数の Reflector が SYN/ACK パケットを再送し続けることを利用して，ネットワーク帯域を占有する．

これらの攻撃に対し，現状では次に示す対策方式が提案されている．まず，SYN Flood に対しては，TCP コネクション管理テーブルを使用しない SYN cookie [5)] が利用されるようになりつつある．これは，TCP のスリーウェイ・ハンドシェークで，攻撃対象ホストが SYN パケットを受信したときに，SYN パケットの送信元 IP アドレス，ポート，シーケンスおよび，時間により変化する変数からハッシュ関数を用いて算出したマジックナンバと呼ばれる値をシーケンス番号としてつけ，SYN/ACK パケットを返送する．ACK パケットを受信したときは，SYN パケットと同様のマジックナンバ算出処理を行い，ACK パケットのシーケンス番号が，マジックナンバ +1 になっている場合にハンドシェークが成功したと見なす．

Connection Flood に対しては，攻撃対象ホストの TCP コネクションキューを増やすとともに，途中のゲートウェイなどで送信元アドレスごとに同時接続数を制限する対策方式が行われている．しかし，分散 DoS 攻撃により，攻撃に参加しているホスト数が，攻撃対象ホストの TCP コネクションキュー数を上回る場合には対策不可能であるという問題も残っている．

UDP Flood は，発信元アドレスが偽造されている場合が多く，ゲートウェイでのフィルタリングによる対策が難しい．また UDP Flood は，ネットワーク帯域を占有することによりサービス不能状態を引き起こすことが特徴である．このため，一般的には帯域制御による対策が行われているが，正規の通信も阻害されるという問題も残っている．

Smurf および，DrDoS は，攻撃対象ホストに直接 IP パケットを送信するのではなく，Reflector に偽造パケットを送信し，そのリプライパケットを攻撃パケットとして送信させる “リフレクション攻撃” である．これにより攻撃パケットが増幅され，ネットワーク帯域の占有をコンスタントに引き起こす．対策としては，ゲートウェイにおいて攻撃パケットをフィルタリングする方法が考えられる．しかし，Reflector が送信するリプライパケットは正規の IP パケットであり，Ingress Filtering [6)] などの従来手法では対策できない．

以上のように，各種 Flood 攻撃の中で，UDP Flood，Smurf，および，DrDoS など，ネットワーク帯域を占有する DDoS 攻撃は，既存の方式では対策が困難である．そこで本論文では，冗長化したバックボーンを介してネットワークどうしを接続する環境において，ネットワーク帯域を占有するタイプの Flood 攻撃に対する回避方式を提案する．本方式は，バックボーン上の各パスのトラフィック状況を推測する機構（パストラフィック推測機構）と，デフォルトで使用するパスの状態に応じて使用できる代替パスを実現する機構（代替パス構築機構）を組み合わせることにより，Flood 攻撃の発生時にユーザのコネクティビティを確保することを特徴とする．

以降 2 章では，提案方式を構成する各機構を実現するうえでの課題について述べる．3 章では，提案方式の具体的な実現方法を述べ，4 章でその評価を行うことにより，提案方式の有効性を示す．最後に 5 章で，まとめと今後の課題について述べる．

2. 提案方式実現上の課題

2.1 パスのトラフィック推測に関する課題

Flood 攻撃を回避するには，通信に利用可能な各パ

スで攻撃が発生していることを推測できることが必要である．各ノードは，動的経路制御で得られた経路情報から，あて先ネットワークに到達可能なパス数と，各パスの長さを知ることが可能である．しかし，経路情報からは，あて先ネットワークまで到達可能なパスを構成する，それぞれのリンクのトラフィック量を知ることができない．このため，通信に先立ち，あて先ネットワークまで到達可能な各パスのトラフィック状況を推測する機構が必要である．

2.2 代替パスの実現に関する課題

冗長化されたバックボーンを持つネットワークでは，ゲートウェイが相互に交換した経路情報を用いて最短パスを構成する動的経路制御技術が利用されている．動的経路制御技術を用いることにより，障害発生時に自動的に代替パスに切り替えることが可能になる．しかし，動的経路制御技術による代替パスは，あて先 IP アドレスにより選択されるため，同一のネットワークに対するユーザトラフィックと攻撃トラフィックを分離することができない．そこで，Flood 攻撃の発生時にコネクティビティを確保するには，攻撃トラフィックはそのままで，ユーザトラフィックのみ切り替えることができる代替パスの実現方式が必要である．

3. 提 案 方 式

本章では，2 章で述べた，パスのトラフィック推測に関する課題と，代替パスの実現に関する課題を考慮した，分散サービス不能攻撃回避方式の具体的な実現方法について述べる．

3.1 パストラフィック推測機構

本提案方式では，各送信元ホストがあて先ホストまでの各パスのトラフィックを推測する方法として，プローブと呼ばれる計測用パケットをパスに注入することにより帯域を測定する “アクティブ計測手法” を利用する．アクティブ計測手法には，パケットペア/パケットトレイン方式と，One-Packet 方式がある．パケットペア/パケットトレイン方式は，2 つ以上のプローブを連続注入し，それぞれの到着間隔が帯域の逆数に比例することを利用してボトルネックリンクの帯域を測定する手法で，Cplobe [7] などのツールが提案されている．One-Packet 方式 [8] は，パケットサイズの異なる ICMP パケットの Round Trip Time（以降 *RTT* と略記する）の差異からリンクの帯域を推定する手法である．

パスのトラフィック状況を推測する方法として，パケットペア/パケットトレイン方式を応用し，パケットペアの送信間隔が短いほどクロストラフィックの影響を受けやすくなることを利用して可用帯域を測定する方式が提案されている．SLoPS [9] は，複数のプローブで構成されたトレインを使用するもので，転送レートを増加させながらトレインを複数回注入し，後続プローブの到着が遅延し始めたトレインの転送レートを可用帯域として推定する．IGI/PTR [10] は，ボトルネックリンクの物理帯域に設定されたトレインから，徐々に転送レートを減少させながらトレインを複数回注入し，後続プローブの到着遅延が見られなくなったトレインの転送レートを可用帯域として推定する．pathChirp [11] は，トレイン中のプローブ転送間隔を指数関数的に減少させ，後続プローブの到着遅延が見られるようになったトレインの転送レートを可用帯域として推定する．

パケットペア/パケットトレイン方式を応用したパストラフィックの推測方法には，以下の問題がある．

(1) トレインの転送レートがボトルネックリンクの可用帯域に漸近するまで注入を続ける必要があり，測定に時間がかかる．
(2) バースト的に発生するクロストラフィックの影響を受けやすく，精度を向上させるには，プローブ量を増やす必要がある．

そこで，クロストラフィックの影響を受けにくく，かつ，ユーザトラフィックへの影響を抑えて測定することが可能な One-Packet 方式とパケットペア/パケットトレイン方式を組み合わせてパスのトラフィックを推測する方式を提案する．

One-Packet 方式では，送信元ホスト S から n 番目のゲートウェイに長さの異なるプローブ[⋆1]を送信して帯域を測定する．このとき，各プローブの RTT は，式 (1) の関係になる．

$$RTT = \left(\sum_{i=1}^{n} \left(\frac{Psize}{B_i} + L_i + Q_i \right) \right) \times 2 \quad (1)$$

$Psize$： プローブのパケットサイズ
B_i： i 番目のリンクにおける帯域
L_i： i 番目のリンクで生じる伝播遅延
Q_i： i 番目のゲートウェイで生じるキュー遅延

ここでリンクの帯域に起因する転送遅延は，パケットサイズに比例し，傾きが，

$$\sum_{i=1}^{n} \frac{2}{B_i} \quad (2)$$

⋆1 通常 ICMP Echo Request パケットを使用する．

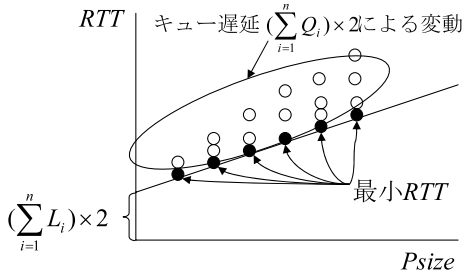

図 1 RTT とパケットサイズの関係
Fig. 1 Relation of RTT and $Psize$.

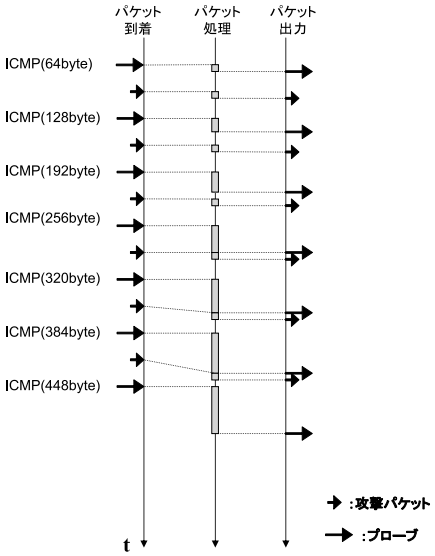

図 2 攻撃パケットが少ない場合
Fig. 2 The case of few attack packets.

となる $Psize$ の 1 次関数で近似できる（**図 1** 参照）．伝播遅延の和 $(\sum_{i=1}^{n} L_i) \times 2$ は，リンクの物理的特性によって決まる定数で，$Psize$ とは独立である．これより，パケットサイズの異なる 2 つのプローブを送信し，それぞれの RTT の測定値とプローブ長の関係から，パスの帯域を推測することができる．

そこで本提案方式では，キュー遅延の和 $(\sum_{i=1}^{n} Q_i)\times 2$ による処理時間の変動に着目し，以下の特徴を持つトレインを用いてパスのトラフィックを推測する．

(1) トレイン内のプローブ送信間隔は一定とする．
(2) トレインを構成するプローブのサイズは同一ではなく，後続プローブほどパケットサイズの大きいものを使用する．

Flood 攻撃によるコンスタントなクロストラフィックが存在する場合，ゲートウェイの処理待ちキューにはプローブと攻撃パケットが混在し，相互にキュー遅延を引き起こす．攻撃パケットの個数が少ない場合（**図 2**），プローブを処理する合間に攻撃パケットの処理を行うことが可能であり，トレイン内のすべてのプローブを最小 RTT で処理することが可能である．

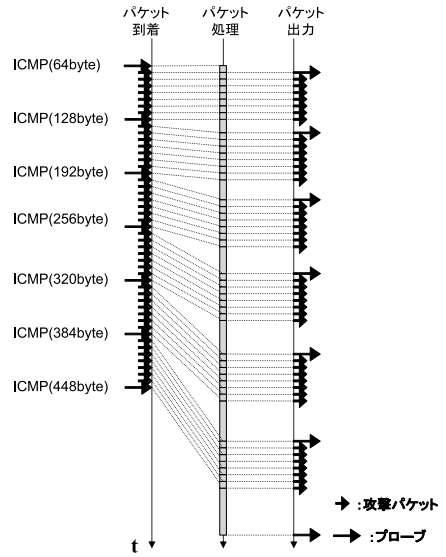

図 3 攻撃パケットが多い場合
Fig. 3 The case of many attack packets.

本提案方式のトレインは，トレインの後半ほどプローブの転送レートが高いという特徴を持つ．このため，攻撃パケットの個数が増加すると，トレイン内で転送レートの高い後半ほどキュー遅延が増大し，帯域が減少していることが推測できる（**図 3**）．そこで，トレインを構成する各プローブの RTT を計測し，トレイン後半のプローブの RTT を Flood 攻撃が発生していない場合と比較することにより，パストラフィックとしてコンスタントな Flood 攻撃が発生しているか否かを推測する．

3.2 代替パス構築機構

本提案方式では，TCP プロキシを用いて構築したオーバレイネットワークで代替パス構築機構を実現する．本構築機構を実装する方法としては，たとえば Socks [12] や，http プロキシを利用することが可能である．

図 4 に，TCP プロキシをサーバエリアスイッチに接続したネットワーク構成例を示す．ユーザ接続エリアに設置された送信元ホストからサーバエリアへの通信には，IP ネットワークの経路制御機構により確立されるパス（以降デフォルトパスと呼ぶことにする）のほかに，次に示すオーバレイネットワークが利用できる．

【パス 1】 プロキシ 1 が中継する 2 本の TCP コネクションにより確立されるパス
【パス 2】 プロキシ 2 が中継する 2 本の TCP コネク

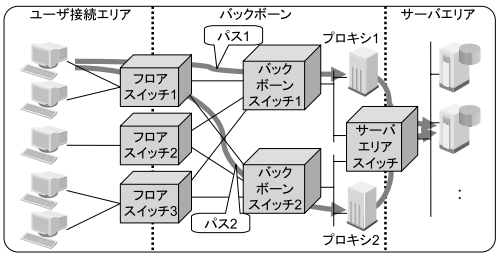

図 4 プロキシによるオーバレイネットワーク
Fig. 4 Overlay network by proxies.

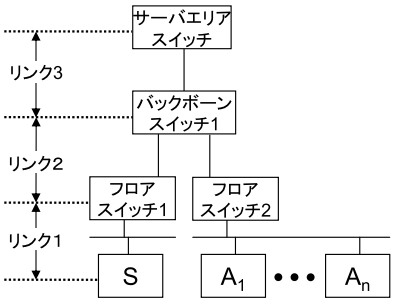

図 5 シミュレーションモデル
Fig. 5 Simulation model.

ションにより確立されるパス

上記の代替パスは，送信元ホストで接続先プロキシを指定することで利用することができる．たとえば，フロアスイッチ 1 に接続された送信元ホストのデフォルトパスが，フロアスイッチ 1–バックボーンスイッチ 1–サーバエリアスイッチを経由するものである場合，フロアスイッチ 1–バックボーンスイッチ 2–サーバエリアスイッチを経由するパス 2 を代替パスとして利用することができる．また，デフォルトパスと代替パスのパストラフィックは，サーバエリアスイッチに接続されたプロキシに対してプローブを送信することにより推定することができる．

4. 評　　価

本章では，2 章で述べた課題を，本提案方式で解決できることを示すため，提案方式を構成する “パストラフィック推測機構” と “代替パス構築機構” のそれぞれに対して評価を行う．

4.1 パストラフィック推測機構の評価

パストラフィック推測機構を評価するため，UC Berkeley，LBL，USC/ISI，および Xerox PARC が開発した離散イベント型ネットワークシミュレータである ns-2[13] を使用してシミュレーションを行った．**図 5** に構成したシミュレーションモデルを示す．

本モデルは，図 4 に示したネットワークで，フロアスイッチ 1 に接続された送信元ホストのパス 1 をシミュレートするもので，以下の 3 つのリンクにより構成される．

【リンク 1】 フロアスイッチに接続された，ユーザ接続エリア内のネットワークをシミュレートする部分である．フロアスイッチ 1 には，パストラフィックを推測する送信元ホスト S が，フロアスイッチ 2 には，攻撃パケットをコンスタントに送信する攻撃ホスト群がそれぞれ接続されている．帯域は 100 Mbps，伝送遅延を 0.5 ms と設定する．

【リンク 2】 バックボーンの中で，各フロアスイッチのトラフィックが分離している区間をシミュレートする部分で，フロアスイッチからバックボーンスイッチ 1 までのリンクに相当する．バックボーンが WAN を用いている場合を想定し，帯域は 1 Mbps，伝送遅延を 50 ms と設定する．

【リンク 3】 バックボーンの中で，各フロアスイッチのトラフィックが集中する区間をシミュレートする部分で，バックボーンスイッチ 1 とサーバエリアスイッチの間のリンクに相当する．バックボーンが WAN を用いている場合を想定し，帯域は 1 Mbps，伝送遅延を 50 ms と設定する．

本モデルにおいて，ユーザ接続エリアの攻撃ホスト群がサーバエリアスイッチに向けて UDP パケットで Flood 攻撃を行うシナリオを作成した．また，モデルの構成を簡単化するため，送信元ホスト S はサーバエリアスイッチに向けてプローブを送信することで，パス 1 のトラフィックを推測する．このプローブは，64 byte を基本として，その倍数の 128 byte，192 byte，256 byte，320 byte，384 byte，448 byte の 7 種類の ICMP Echo Request パケットにより構成されるトレインである．プローブを構成する各プローブの送信間隔は，各フロアスイッチからのトラフィックが合流し，ボトルネックリンクとなるリンク 3 の帯域が 1 Mbps であることを考慮し，トレインの最後尾でも 1 Mbps を超えない 5 ms 間隔に設定した．

4.1.1 パストラフィック推測機構の有効性

まず，帯域を占有するタイプの Flood 攻撃の発生を推測するうえで，本機構が有効に機能することを検証する．Smurf は ICMP Echo Reply パケットで，DrDoS は TCP の SYN/ACK パケットでネットワーク帯域を占有する．これらのパケットはおよそ 64 byte 程度のショートパケットであるため，64 byte の攻撃パケットで Flood 攻撃が行われている状況で，パスのトラフィック状況を推測するシミュレーションを行った．攻撃による転送レートは，同時に稼動するパケッ

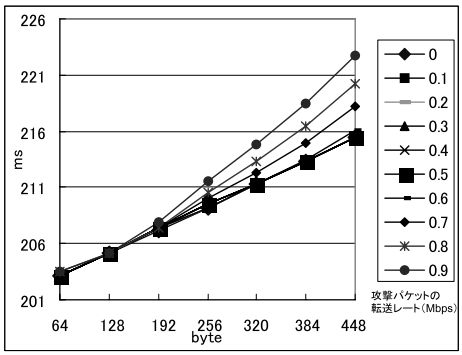

図 6 攻撃パケットサイズが 64 byte の場合のシミュレーション結果
Fig. 6 Simulation result when the length of attack packet is 64 bytes.

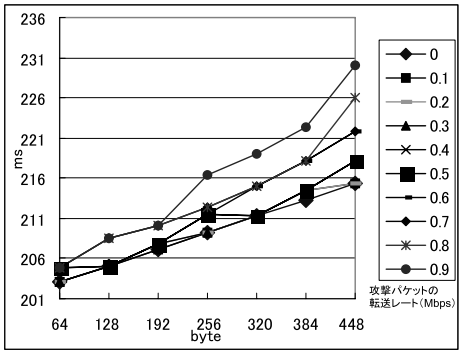

図 7 攻撃パケットサイズが 512 byte の場合のシミュレーション結果
Fig. 7 Simulation result when the length of attack packet is 512 bytes.

トジェネレータの台数を変えることにより，0.1 Mbps から 0.9 Mbps まで 0.1 Mbps 刻みで変更した．シミュレーション結果を**図 6** に示す．

図 6 の横軸はプローブのパケット長，縦軸は送信したプローブが送信元ホスト S に返ってくるまでの *RTT* である．この結果では，攻撃パケットの転送レートが 0.6 Mbps 以下の場合，トレインを構成するすべてのプローブの *RTT* は変化しない．しかし，攻撃パケットの転送レートが 0.7 Mbps を超えると，パケットサイズの大きいプローブほど *RTT* が増大した．

UDP Flood 攻撃では，ロングパケットを用いた攻撃もあるため，ロングパケットを用いた UDP Flood 攻撃を想定し，512 byte の攻撃パケットを用いたシミュレーションも行った．結果を**図 7** に示す．この結果からは，Flood 攻撃の転送レートが 0.5 Mbps（帯域占有率 50%）を超えるとパケットサイズの大きいプローブほど *RTT* が増大した．

以上より，本提案方式の可用帯域推定機構は，送信したトレインの *RTT* を計測することにより，計測対象パスにコンスタントな Flood 攻撃が発生しているか否かを推測できる見通しを得た．

表 1 帯域推定時間およびトラフィック量
Table 1 Bandwidth estimation time and traffic.

	提案方式	pathChirp
帯域推定時間	35 ms	70 ms
トラフィック量	1,802 byte	9,375 byte

4.1.2 パストラフィック推測時間および，プローブの帯域使用量

さらに，従来の可用帯域推定方式の中で最も注入プローブ量が少ない pathChirp を図 5 で示したシミュレーションモデルに適用してプローブ送出時間および，トラフィック量を比較することにより，本提案のパストラフィック推測機構の実用性を評価する．

まず，pathChirp が使用するトレインのプローブ数について考察する．pathChirp ではプローブの転送間隔を指数関数的に減少させて注入する．プローブ転送間隔の初期値を T とし，γ を定数とすると，n 個目のプローブと $n+1$ 個目のプローブの転送間隔 $\Delta(n)$ は，式 (3) で表される．

$$\Delta(n) = \frac{T}{\gamma^{n-1}} \tag{3}$$

定数 γ を 1.4 に設定し，リンク 3 の物理帯域にあわせてプローブ転送レートを 10 Kbps から 1 Mbps まで変化させる場合，トレインは 15 プローブで構成できる．

次に，pathChirp が使用するプローブのパケットサイズについて考察する．プローブ転送レート R は，プローブのパケットサイズ $Psize$ と，n 個目のプローブと $n+1$ 個目のプローブの転送間隔 $\Delta(n)$ により，式 (4) で表される．

$$R = \frac{Psize}{\Delta(n)} \tag{4}$$

プローブ転送間隔は測定精度に影響するため，最小のプローブ転送間隔 $\Delta(14)$ を提案方式と同様に 5 ms に設定して 1 Mbps のプローブ転送レートを実現した場合のプローブ送出時間および，トラフィック量の比較を**表 1** に示す．

本提案方式は，帯域推定時間に関しては 1/2，必要なトラフィック量に関しては 1/5 になる．以上より，ネットワーク帯域を占有するタイプの Flood 攻撃発生時のパストラフィック推測機構として，本提案方式の方が従来方式より有利と考える．

4.2 代替パス構築機構の評価

本節では，本提案方式以外の代替パス構築機構の実

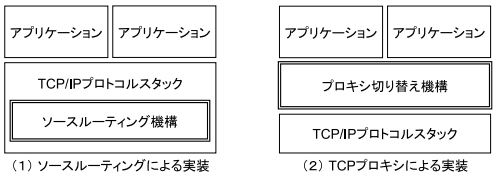

図 8 代替パス構築機構の実装レイヤ比較
Fig. 8 Layer composition of implementation for alternative path.

現方法との比較により，代替パス構築機構を評価する．

代替パス構築機構の実現方法として，IP パケットの通過経路を送信者が明示的に指定する “ソースルーティング” を利用する方法がある．ソースルーティングを使用する場合，代替パスは以下の手順で構築する．

(1) 送信元ホストの IP パケット生成処理で，代替パス上にあるゲートウェイを指定したソースルーティング・オプションを IP ヘッダに付加する．
(2) ゲートウェイの IP パケット転送処理において，ソースルーティング・オプションに従って処理を実行する．

ここで，送信元ホストが行う処理は，TCP/IP プロトコルスタック内で実行される．このため，ソースルーティングで実現した代替パス構築機構は，**図 8** (1) のように TCP/IP プロトコルスタック内に実装する必要がある．

ところで，送信元ホストの TCP/IP プロトコルスタックは，アプリケーションから渡されたデータグラムを IP パケットに変換する処理を行うだけではなく，受信した ICMP Echo Request パケットや，TCP の SYN パケットに対する返送処理も行っている．代替パス構築機構を TCP/IP プロトコルスタック内に実装すると，送信元ホストが Smurf や DrDoS などのリフレクション攻撃の偽造パケットを受信した場合に，攻撃トラフィックも代替パスに流れてしまう．

本提案方式の場合は，以下の手順で代替パスを構築する．

(1) 送信元ホストのアプリケーションが TCP コネクションを生成する際に，あて先ホストの代わりにプロキシとの TCP コネクションを確立する．
(2) プロキシは送信元ホストのリクエストに応じ，あて先ホストに対する TCP コネクションを確立する．

ここで，送信元ホストが行う処理は，図 8 (2) に示すように TCP/IP プロトコルスタックより上位のレイヤで実行される．このため，送信元ホストが Reflector として動作しても，代替パス構築機構が返送パケットの生成処理に関与せず，攻撃トラフィックのパスが切り替わることはない．

表 2 方式比較
Table 2 Comparison of methods.

	提案方式	ソースルーティング
リフレクション攻撃	対策可能	対策不可能
必要機器	プロキシを追加	既存設備のみ
運用ポリシの影響	なし	あり

ソースルーティングを利用する方法は，ソースルーティング・オプションを有効にするようにゲートウェイを設定するだけでよく，プロキシなどの付加機構を必要としない．しかし，ソースルーティング・オプションは，送信元ホストの IP アドレスを詐称してあて先ホストと通信を行う “IP スプーフィング” に悪用される問題が指摘されている．このため，ネットワーク運用ポリシにより，ソースルーティング・オプションの利用を制限する組織も多い．

以上より，提案方式と，代替案であるソースルーティング方式を比較した結果を**表 2** に示す．

本提案方式は，Smurf および DrDoS 攻撃にも対応できる点と，ネットワーク運用ポリシによる制約を受けない点において，ソースルーティング・オプションを用いた実現方法より実用的である．

5. まとめと今後の課題

本論文では，各種 Flood 攻撃の中で，UDP Flood，Smurf，および，DrDos など対策方式が確立されていなかったタイプの Flood 攻撃を対象とし，攻撃を回避する方式を提案した．本提案方式は，One-Packet 方式とパケットペア/パケットトレイン方式を組み合わせて実現した “パストラフィック推測機構” と，TCP プロキシとプロキシ指定機能により実現した “代替パス構築機構” を組み合わせることにより，Flood 攻撃を回避してユーザのコネクティビティを確保する．

本提案方式の有効性を示すため，4 章においてパストラフィック推測機構と，代替パス構築機構を評価した．その結果，本提案方式のパストラフィック推測機構が，64 byte および 512 byte の攻撃パケットによる Flood 攻撃に対して有効に機能することをシミュレーションによって示した．また，トラフィック状況推測時間およびトラフィック量の観点から，従来のパケットペア/パケットトレイン方式を用いてパストラフィックを推測するより効率的であることを示した．

また，TCP プロキシによって構成したオーバレイネットワークで代替パス構築機構を実現することで，Flood 攻撃発生時にユーザトラフィックのみパスの切替えを行えることと，ソースルーティング方式より実

用的であることを示した．

実際の Flood 攻撃では，TCP による攻撃や，長さの異なる攻撃パケットが混合されている攻撃など，さまざまなパターンが考えられる．また，LAN 接続機器の種別により特性が異なるため，特にパストラフィック推測機構に関しては，実ネットワークでの実験など，今後も評価を継続する必要がある．さらに，本方式を具体的なシステムに適用するには，性能を含めたネットワーク設計・実装方式などのさらなる検討を行うことが必要であり，今後の課題である．

参 考 文 献

1) CERT: CERT advisory CA-1996-21 TCP SYN flooding and IP spoofing attacks (1996). available at http://www.cert.org/advisories/CA-1996-21.html
2) 三輪信雄，新井　悠：ネットワーク攻撃詳解攻撃のメカニズムから理解するセキュリティ対策，株式会社ソフト・リサーチ・センター (2002).
3) CERT: CERT advisory CA-1998-01 smurf IP Denial-of-Service attacks (1998). available at http://www.cert.org/advisories/CA-1998-01.html
4) Gibson, S.: The Distributed Reflection DoS Attack (2002). available at http://grc.com/dos/drdos.htm
5) Zuquete, A.: Improving the functionality of SYN cookies, *Proc. 6th IFIP Communications and Multimedia Security Conference*, pp.57–77 (2002).
6) Ferguson, P. and Senie, D.: Network Ingress Filtering: Defeating Denial of Service attacks which employ IP Source Address Spoofing, RFC2827 (2000).
7) Carter, R.L. and Crovella, M.E.: On the Network Impact of Dynamic Server Selection, Computer Networks, *The International Journal of Computer and Telecommunications Networking*, Vol.31, pp.2529–2558 (1999).
8) Bellovin, S.M.: A Best-Case Network performance Model, Technical report, ATT Research (1992).
9) Jain, M. and Dovrolis, C.: End-to-End Available Bandwidth: Measurement methodology, Dynamics, and Relation with TCP Throughput, *SIGCOMM* (2002).
10) Hu, N. and Steenkiste, P.: Evaluation and Characterization of Available Bandwidth Probing Techniques, *IEEE JSAC Special Issue in Internet and WWW Measurement, Mapping, and Modeling*, Vol.21, No.6 (2003).
11) Ribeiro, V.J., Riedi, R.H., Baraniuk, R.G., Navratil, J. and Cottrell, L.: pathChirp: Efficient Available Bandwidth Estimation for Network Paths, *Passive and Active Measurement Workshop* (2003).
12) Leech, M., Ganis, M., Lee, Y., Kuris, R., Koblas, D. and Jones, L.: SOCKS Protocol Version 5, RFC1928 (1996).
13) NS2: The Network Simulator - ns-2. available at http://www.isi.edu/nsnam/ns/

(平成 19 年 5 月 24 日受付)
(平成 19 年 12 月 4 日採録)

萱島　信（正会員）

昭和 62 年横浜国立大学工学部電気工学科卒業．平成元年同大学大学院工学研究科博士課程前期修了．同年（株）日立製作所入社．以来システム開発研究所にて AI 技術，オブジェクト指向技術，ネットワーク技術，セキュリティ技術等の研究に従事．現在，同研究所主任研究員．平成 17 年より横浜国立大学大学院環境情報学府博士課程後期在籍中．IEICE，JSAI 各会員．

松本　勉（正会員）

昭和 56 年横浜国立大学工学部電子情報工学科卒業．昭和 58 年同大学大学院工学研究科修士課程修了．昭和 61 年東京大学大学院博士課程修了．工学博士．同年横浜国立大学講師（工学部電子情報工学科）．平成元年同助教授．平成 6 年カールスルーエ大学客員教授．現在横浜国立大学教授．主として情報セキュリティの基礎理論から応用に至る研究と教育に従事．IACR，IEICE 各会員．