特別研究報告

題目

DDoS 攻撃トラヒックのモデル化および防御アルゴリズムへの適用とその評価

指導教官

宮原 秀夫 教授

報告者

中山 圭

平成 15 年 2 月 19 日

大阪大学 基礎工学部 情報科学科

平成 14 年度 特別研究報告

DDoS 攻撃トラヒックのモデル化および防御アルゴリズムへの適用とその評価

中山 圭

内容梗概

近年頻繁に見られるようになったサービス拒否 (DoS: Denial of Service) 攻撃は、インターネット上に存在する特定のサイトに対して大量のパケットを送りつけることでそのサイトで提供されているサービスを利用できなくする、もしくはそのサービスの品質を著しく低下させるような行為を指す。

DoS 攻撃は近年多様化・分散化し、その威力は増すばかりである。その中でも分散化した攻撃は特に DDoS (Distributed DoS) 攻撃と呼ばれており、その効果的な防御策が確立されていないのが現状である。その大きな理由としてこれらの攻撃が現存するプロトコルの原則に則って行われていることが挙げられる。攻撃を防御する様々なアルゴリズムが検討されているが、その効果を実証するためには様々なネットワーク環境における評価が必要となる。本報告では、TCP SYN Flood という近年最も多く見られる DoS 攻撃を防御するアルゴリズムを検討するために実際のトラヒックをもとに擬似トラヒックを生成し、防御アルゴリズムへの適用とその評価を行う。その結果、防御アルゴリズムにおけるいくつかの最適な設定値を決める上で影響をおよぼすパラメータが判明した。

主な用語

DDoS 攻撃、SYN Flood 、TCP 、トラヒックモニタ，性能評価

目 次

図 目 次

表 目 次

1 はじめに

近年の急速なインターネットの発達により、ネットワークを介した様々なサービスが提供され、その利便性は増すばかりである。その一方で、悪意を持った第 3 者がサービスを提供する計算機に攻撃を行い、一般ユーザの利用を妨げるサービス拒否 (DoS; Denial of Service) が深刻な問題となっている。実際に yahoo や amazon.com といった大手サイトもこういった被害に遭遇しており、多大な損害が出ている [1] 。現在では、サービス拒否の方法は広く公開されており、インターネットに関する多少の技術的知識があれば誰でもサービス拒否を引き起こす攻撃は可能である。

攻撃の技術も近年ますます向上しており、最近は分散された攻撃ホストが同時に同じ計算機を攻撃する DDoS (Distributed DoS) 攻撃と呼ばれるものが主流になりつつある。DDoS 攻撃の手順は、図 1 で示されるように悪意のあるユーザはまずインターネット上に接続されたセキュリティの脆弱な端末 (ハンドラホスト) に侵入し、さらにハンドラホストを踏み台として別の複数の端末 (エージェントホスト) に同様の方法で侵入する。その後、エージェントホストにおいて DDoS 攻撃を行うプログラムを実行できる状態にし、ハンドラホストからの命令を待機させる。これにより、攻撃者がハンドラホストに攻撃命令を発することで、攻撃命令はハンドラホストを通じてエージェントホストに通知され、一斉に攻撃が開始される。

DoS 攻撃にも多種多様なものが確認されており、ターゲットホストに対して許容数を超える接続要求を行い、一般ユーザが新たな接続を確立できなくする TCP SYN Flood 攻撃 [2] や ICMP (Internet Control Message Protocol) などを利用して意図的にターゲットホストにパケットを集中させることで帯域を占有する Smurf 攻撃 [3] などがある。一般的に、パケットのヘッダから攻撃パケットと通常パケットを区別することはできないため、攻撃されたホストで攻撃パケットのみを遮断することは非常に難しい。このため、実際に攻撃が発生した場合、ユーザへのサービス拒否をできる限り最小限にしつつ攻撃トラヒックを検出することが重要である。

攻撃検出メカニズムとしては、これまでにもエッジルータにおいて TCP (Transmission Control Protocol) の SYN パケットと FIN パケットの差から TCP SYN Flood 攻撃を検出

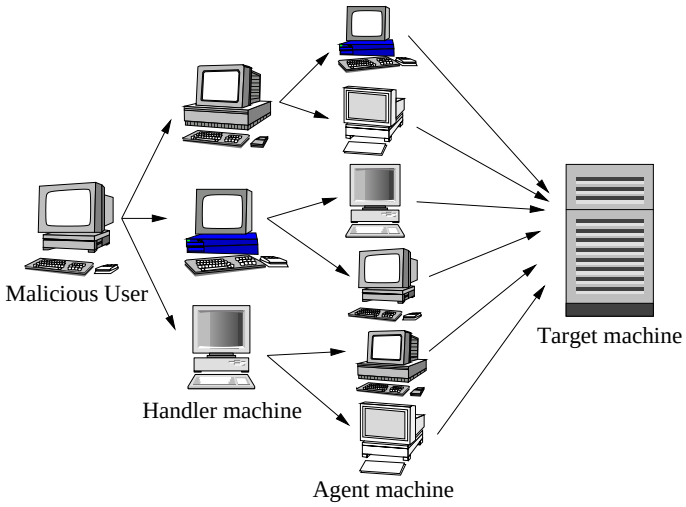


図 1: DDoS 攻撃の構成図

する手法 [4] 、宛先アドレスのプレフィックスごとにパケットレートを測定し、パケットレートが高い宛先アドレスのプレフィックスをさらに細分化して攻撃元を特定する手法 [5] ルーティング情報から入力ポートごとに本来到着しないパケットを観測することで偽装パケットを検出する手法 [6] などの対策が提案されている。

一方、これらの防御アルゴリズムの有効性を確かめる画一的な方法はいまだ決められていない。アルゴリズムの有効性を判断するためには、設計者が想定するトラヒックに対して正しく動作することはもちろんのこと、設計者の意図しないトラヒックが到着した場合でも誤動作することがないかを検証しなければならない。特に、防御アルゴリズムの弱点を見つけるためには、攻撃トラヒックの性質がどのような影響を及ぼすかについて詳細に明らかにしていく必要がある。また、防御アルゴリズムが持つパラメータを最適な値に設定するためには、実トラヒックの性質を勘案した細かい調整が不可欠である。

そこで本報告では、攻撃トラヒックのどのパラメータが防御アルゴリズムの性能に影響を与えるのかを調べるために、様々なパラメータを要素とする攻撃トラヒックを生成し、防御アルゴリズムに適用することで、防御アルゴリズムの問題点を提起し、今後の改善への指針を示すことを目的とする。本報告では現在 DDoS 攻撃の約 90 %に該当する [7] と言われている TCP SYN Flood 攻撃を対象とし、実際にキャプチャしたトラヒックデータをもとに

して作成した擬似攻撃トラヒックを防御アルゴリズムへ適用し、その最適な防御アルゴリズムの設定値を求める上で影響を及ぼすパラメータについて評価を行う。

以下、まず 2 章では、TCP SYN Flood 攻撃の概要を通常の TCP の接続確立のプロセスと対比させて説明し、問題点を述べる。次に 3 章では、実トラヒックの取得手法、およびそこで得られたトラヒックデータをもとにした擬似攻撃トラヒック生成手法を示す。さらに 4 章では、今回評価対象とする DDoS 攻撃防御アルゴリズムの概要説明とシミュレーションによるそのアルゴリズムの評価結果を示す。最後に、5 章でまとめと今後の課題を述べる。

2 TCP SYN Flood 攻撃の概要

本章では、対象とする TCP SYN Flood 攻撃の概要を、通常時の TCP 接続の手順と比較して説明する。

2.1 TCP における接続の確立

通常、TCP における接続の確立は、図 2 で示される 3-way handshake と呼ばれる方法で行われる。その概要を以下に示す。

1. 送信元ホスト (Source) から宛先ホスト (Destination) へ SYN パケットを送信し接続要求を行う。

2. 宛先ホストから送信元ホストへ SYN パケットに対する受信確認である SYN/ACK パケットを送信する。

3. 送信元ホストから宛先ホストへ ACK パケットを送信し、接続が確立する。その後、実際のデータの送受信が行われる。

宛先ホスト側において SYN/ACK パケットを送信してからそれに対する ACK パケットを受け取るまで待機する状態を half-open 状態という。 half-open 状態では、宛先ホスト側において送信元ホストからの通信を受け入れるためにバッファ等が確保されるため、宛先ホストの資源を消費する。このため、宛先ホストでは受け付けられる half-open 状態の接続数には上限があり、これを backlog-queue と呼ばれる待ち行列で管理する。 backlog-queue には上限値が設定されており、この値は通常オペレーションシステムで設定可能なものであり上限を超える数の SYN パケットに対しては受付拒否 (RST パケット) を送信元ホストに返す。したがって、攻撃ユーザが大量に SYN パケットを送信し、half-open 状態のコネクション数を常に上限値にさせることで、サービス提供者とは何ら関係がない第三者が一般ユーザに対してサービスの受付を拒否することができる。次節でこの攻撃手法について詳しく述べる。

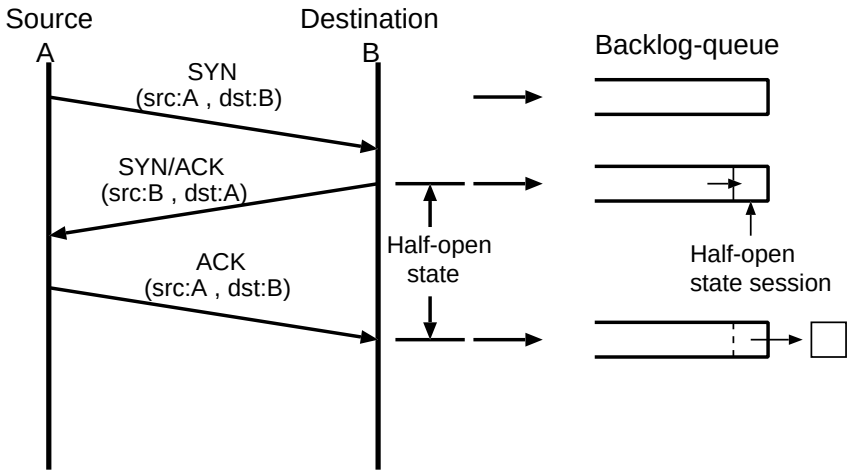


図 2: TCP 3-way handshake

2.2 TCP SYN Flood 攻撃

TCP SYN Flood 攻撃では、攻撃ホストは送信元フィールドを詐称してパケットを送出する。したがって、ターゲットホストは詐称されたアドレスに対して SYN/ACK パケットを送出することになる。実際に詐称されたアドレスを持つホストが存在する場合と存在しない場合ではターゲットホストの動作が異なるため、本節ではそれぞれの場合に分類して動作を説明する。

2.2.1 詐称アドレスがネットワーク上に存在する場合

攻撃ホストが詐称したアドレスを持つホストがネットワーク上に存在する場合のプロセスは図 3 のようになる。

1. 攻撃ホストは自分のアドレスを詐称して、ターゲットとなるホストへ SYN パケットを送信する (詐称アドレスを C とする) 。

2. ターゲットホストはアドレス C に該当するホストから SYN パケットが送信されたと認識するので、アドレス C に対して SYN/ACK パケットを送信する。

3. ネットワーク上に存在するアドレス C に該当するホストは、自身が送信していない

SYN パケットに対する SYN/ACK パケットを受信するため、RST パケットをアドレス B に送信して、接続要求を破棄する。

4. ターゲットホストはホスト C からの接続解除 (RST) パケットを受信した段階で、接続要求を解除する。

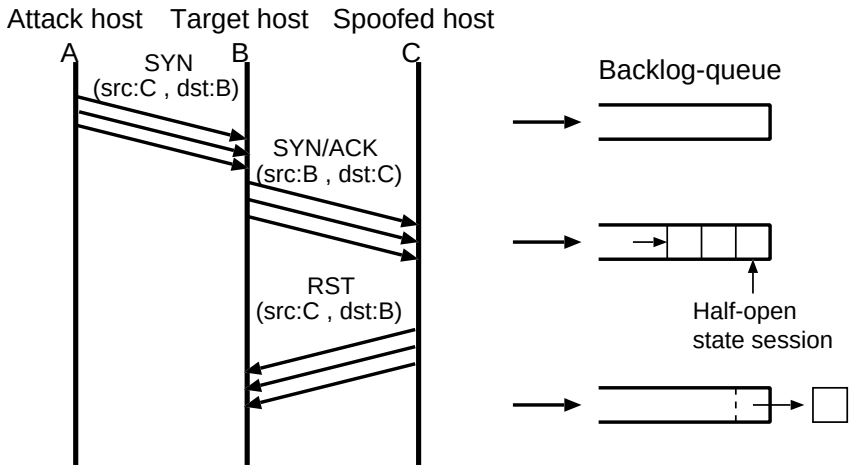


図 3: 詐称アドレスが存在した場合の TCP SYN Flood 攻撃

2.2.2 詐称アドレスがネットワーク上に存在しない場合

攻撃クライアントが詐称したアドレスがネットワーク上に存在しない場合のプロセスは図 4 のようになる。

1. 攻撃ホストは自分のアドレスを詐称して、ターゲットとなるホストへ SYN パケットを送信する (詐称アドレスを C とする) 。

2. ターゲットホストはアドレス C に該当するホストから送信された SYN パケットであると認識するので、アドレス C に対して SYN/ACK パケットを送信する。

3. アドレス C を持つホストは実際に存在しないため、SYN/ACK パケットは棄却される。しかし、ターゲットホストは SYN/ACK パケットが棄却されたことを知ることはできないため、引き続きホスト C からの ACK パケットを待ち続ける。

4. ある一定期間ホスト C からの ACK パケットが到着しなければ、ターゲットホストはホスト C が存在しないと判断して、接続要求を解除する。

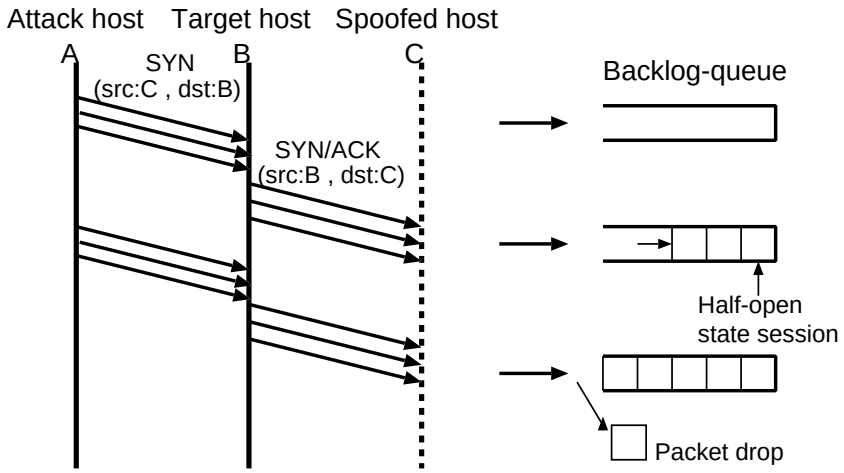


図 4: 詐称アドレスが存在しない場合の TCP SYN Flood 攻撃

前述の詐称アドレスがネットワーク上に存在している場合ではこの half-open 状態は送られてきた RST パケットによって遮断されるが、存在しない場合は、タイムアウトが発生するまで half-open 状態として待ちつづけるので、その間にも次々に攻撃パケットが backlog-queue に蓄積され、結果的に一般ユーザからの接続要求が棄却される。

3　擬似 DDoS 攻撃トラヒックの生成

本章では、本報告で行った実トラヒックの取得手法を示し、それによって得られたトレースデータをもとに擬似攻撃トラヒックの生成を行う。

3.1　実トラヒックの取得手法

本報告では、実トラヒックに基づいて生成した擬似攻撃トラヒックを用いて防御アルゴリズムの評価を行う。このためまず、トラヒックモニタを用いた実トラヒックの収集を行う。観測環境を図 5 に示す。大阪大学と外部をつなぐ 1000Base-SX の光ファイバケーブル上に流れるトラヒックを光スプリッタによって分波させ、それぞれをキャプチャマシンのギガビット NIC のデータ受信側 (RX) へ送り、モニタ側で到着パケットを時系列に従って記録する。パケットの記録には `tcpdump` [8] を用いる。

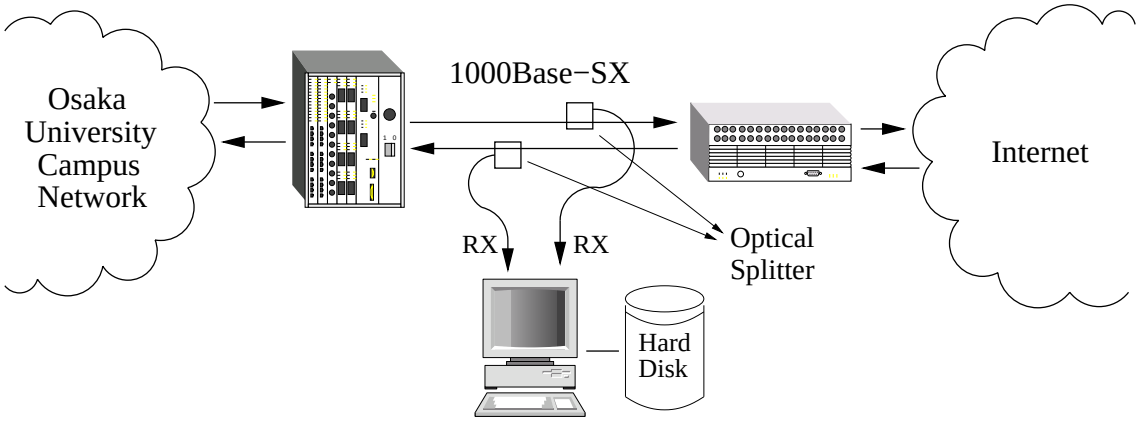


図 5: 実トラヒック取得手法

3.2　擬似攻撃トラヒックの生成

3.2.1　実トラヒックの解析

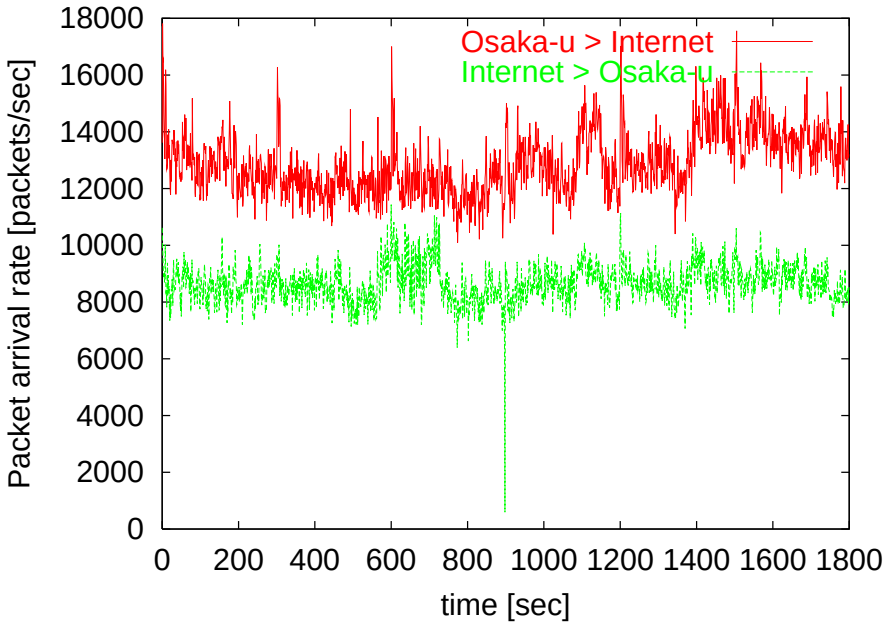
- 取得トラヒックの解析

  本報告では、図 5 のモニタ環境において 2003 年 2 月 11 日 20 時から 30 分間の記録、

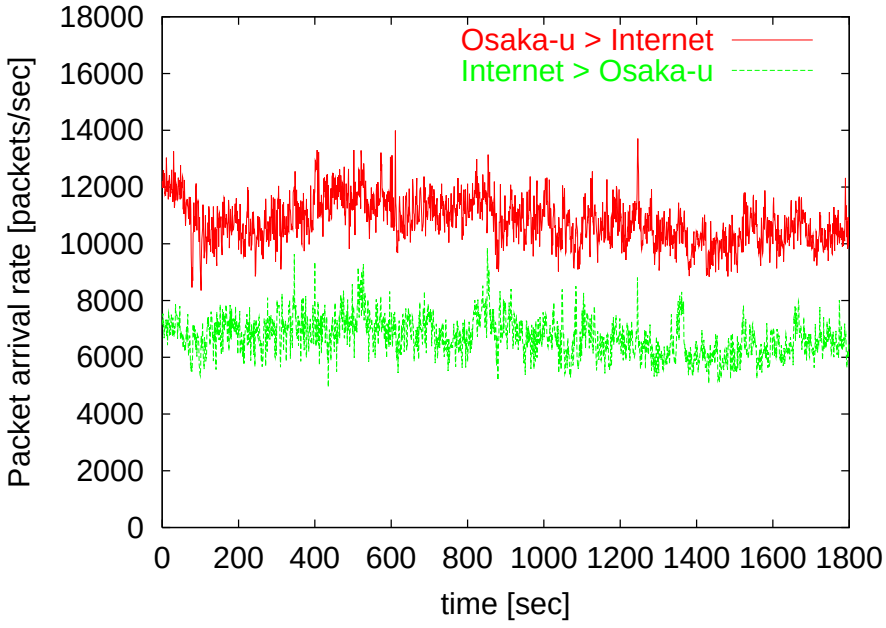
および 2 月 12 日 14 時から 30 分間の記録の 2 種類を分析データとして用いる。記録したトラヒックの概要を表 1 に示す。また、全体のパケットレートの時間変動を図 6 に示す。図の結果より、総パケット数は 14 時よりも 20 時の方が多く、外部から阪大よりも阪大から外部のパケット数の方が多いことがわかる。また、図 6 より、すべてのパケットに対する SYN パケットの割合は非常に少ないことがわかる。

表 1: 取得トラヒックの統計データ

取得時間	11 日 20 時〜20 時 30 分		12 日 14 時〜14 時 30 分	
方向	阪大→外部	外部→阪大	阪大→外部	外部→阪大
総パケット数 [個]	23,203,588	15,596,750	19,467,875	12,101,313
平均パケット到着率 [packets/sec]	12,891	8,665	10,816	6,723
平均ビットレート [Mbps]	98.28	34.86	55.98	40.35

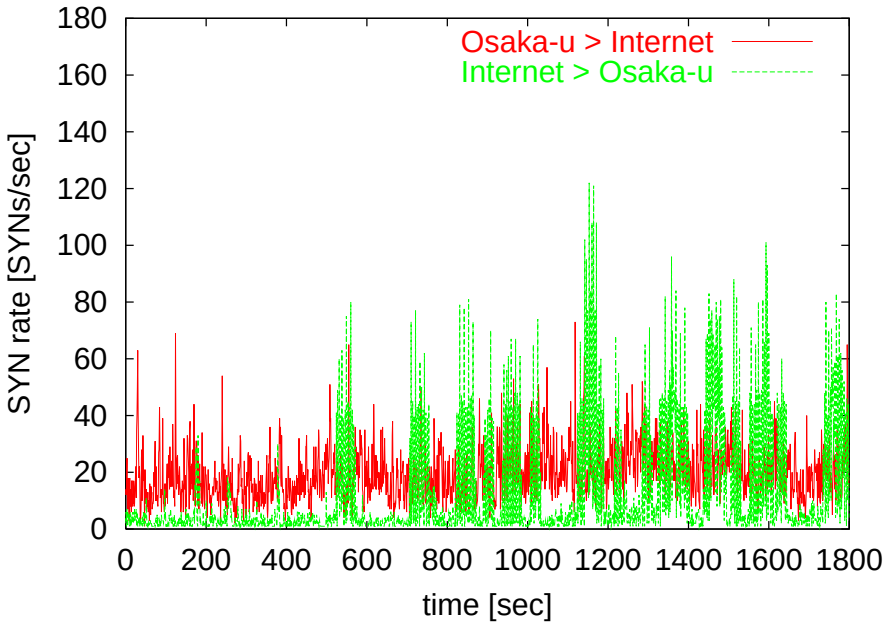


(a) 2 月 11 日 20 時

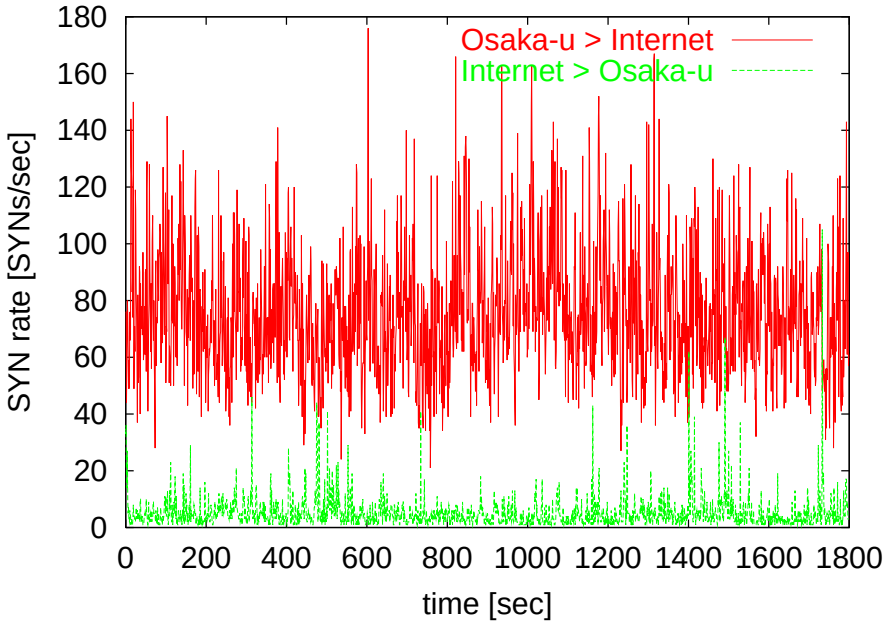


(b) 2 月 12 日 14 時

図 6: 総パケットのレート変動



(a) 2 月 11 日 20 時



(b) 2 月 12 日 14 時

図 7: SYN パケットのレート変動

表 2: SYN パケットの統計データ

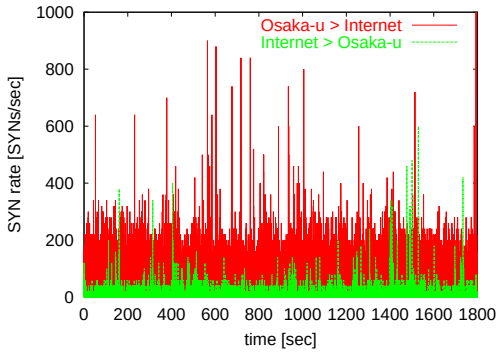
計測時間	11 日 20 時〜20 時 30 分		12 日 14 時〜14 時 30 分	
方向	阪大→外部	外部→阪大	阪大→外部	外部→阪大
総 SYN パケット数 [個]	36,593	23,214	151,094	10,559
平均 SYN 到達率 [SYNs/sec]	20.33	12.90	83.94	5.87

表 3: 各トラヒックデータのサービス分布

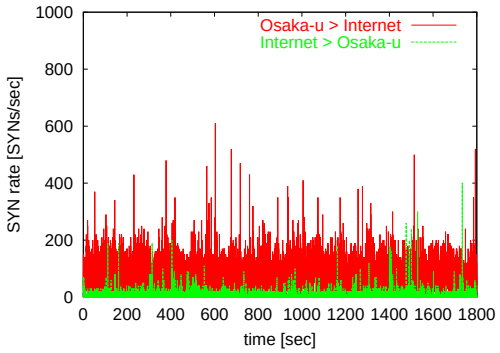
11 日 20 時〜20 時 30 分				12 日 14 時〜14 時 30 分			
阪大→外部		外部→阪大		阪大→外部		外部→阪大	
http(80)	72.2 %	ftp(21)	74.8 %	http(80)	93.4 %	http(80)	65.5 %
smtp(25)	4.0 %	http(80)	11.1 %	smtp(25)	1.6 %	smtp(25)	11.9 %
dns(53)	2.6 %	smtp(25)	2.6 %	https(443)	1.4 %	proxy(3128)	3.6 %

- SYN パケットのレート変動

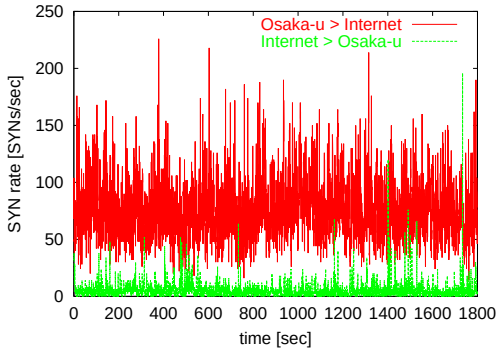
  表 2 に SYN パケットの統計データ、表 3 にサービス分布、図 7 に得られた実トラヒックの SYN レートの変遷を取得時間ごとに示す。図を見ると、2 月 11 日 20 時の外部から阪大へのトラヒックだけ他の 3 つと大きくグラフの形が異なっているのが目立つ。これは ftp ポートスキャン [9] という、今回対象としている TCP SYN Flood とは異なる攻撃によって発生されたトラヒックによるものである。表 3 において、2 月 11 日 20 時の外部から阪大へのデータのみが ftp が最も多く提供されているサービスとなっているのはそのためである。



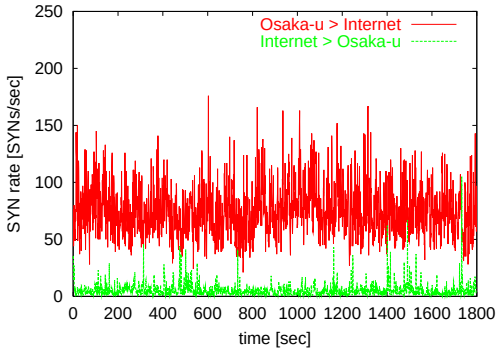
(a) 0.05 秒



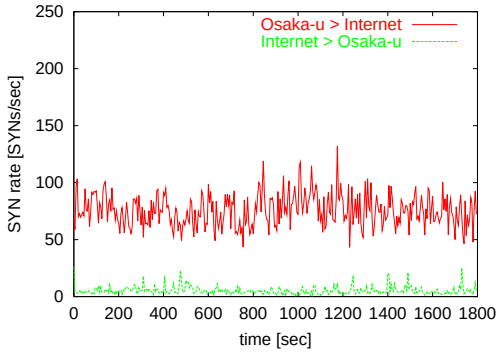
(b) 0.1 秒



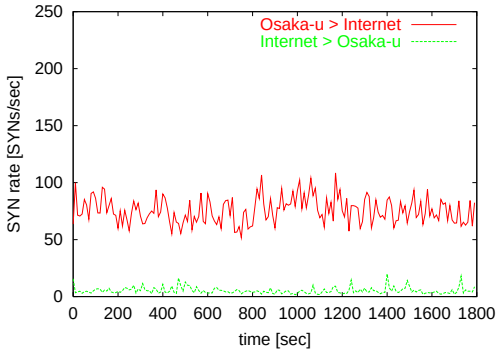
(c) 0.5 秒



(d) 1 秒



(e) 5 秒



(f) 10 秒

図 8: サンプリング周期別で見た SYN パケットのレート変動

また、サンプリング周期による変動のちがいを調べるため、2 月 12 日 14 時からの 30 分間のデータに対して、0.05 秒、0.1 秒、0.5 秒、1 秒、5 秒、10 秒間隔で計測したものを図 8 に示した。サンプリング周期が短くなればなるほど SYN のレートのバースト性は大きくなり、最も短い 0.05 秒間隔のデータとなると最高で 900 SYNs/sec 程度まで観測されている。逆に時間幅が長くなるとバースト性は小さくなり 10 秒間隔のデータにおける最大レートは 110 SYNs/sec にとどまっている。以上の結果よりサンプリング周期が SYN のレートに大きく影響することがわかった。よって、防御アルゴリズムを評価する際にも、サンプリング間隔の影響も考慮する必要がある。

- 宛先ホストの分布状況

  図 9、10 には上で示した計測期間内における宛先アドレス (DA; Destination Address) の分布状況を示している。これらの分布は Zipf の法則 [10] に従っていることが確認された。さらに、多数のアクセスが確認できた宛先アドレスについてその送出元アドレス (SA; Source Address) の分布を調べた。

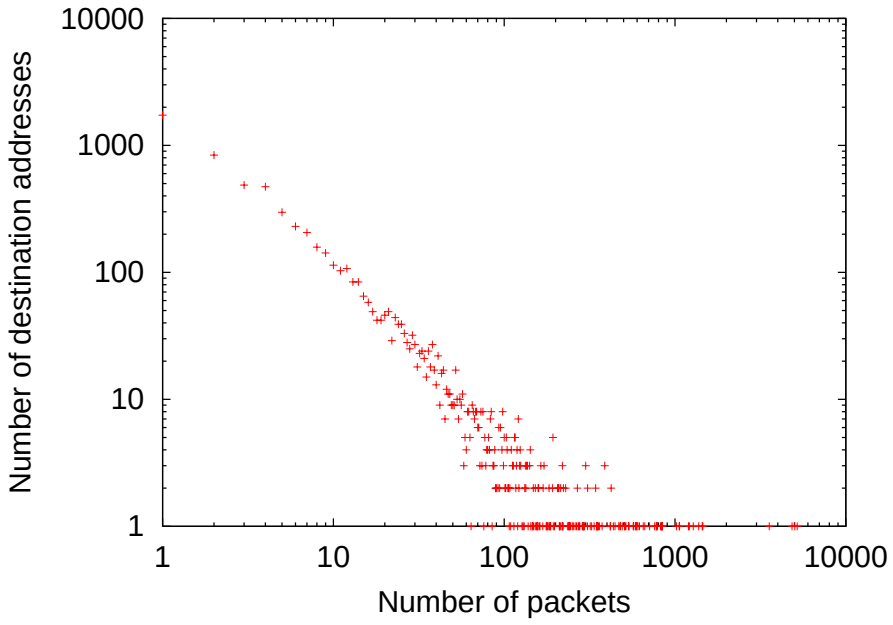


図 9: DA 分布 (阪大→外部)

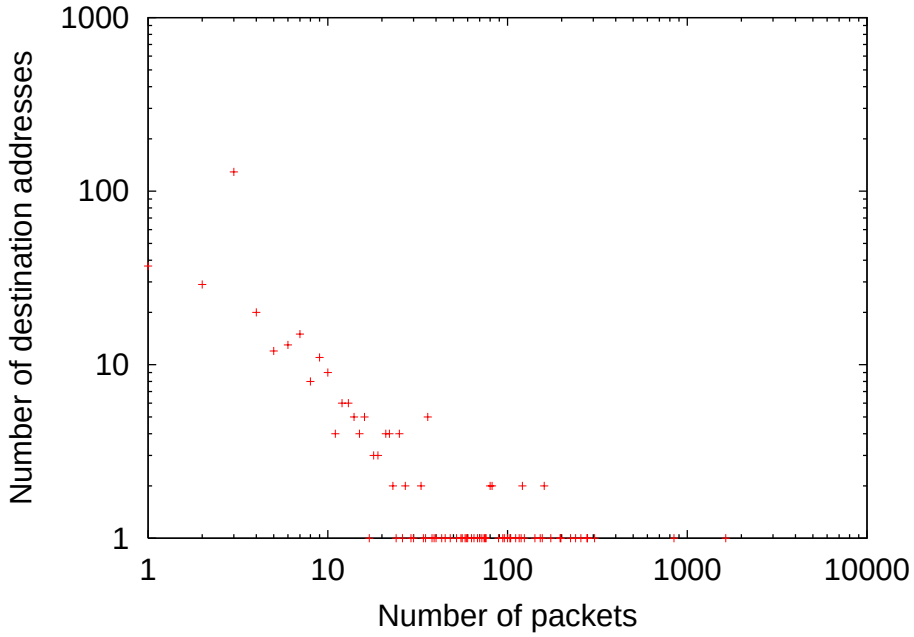


図 10: DA 分布 (外部→阪大)

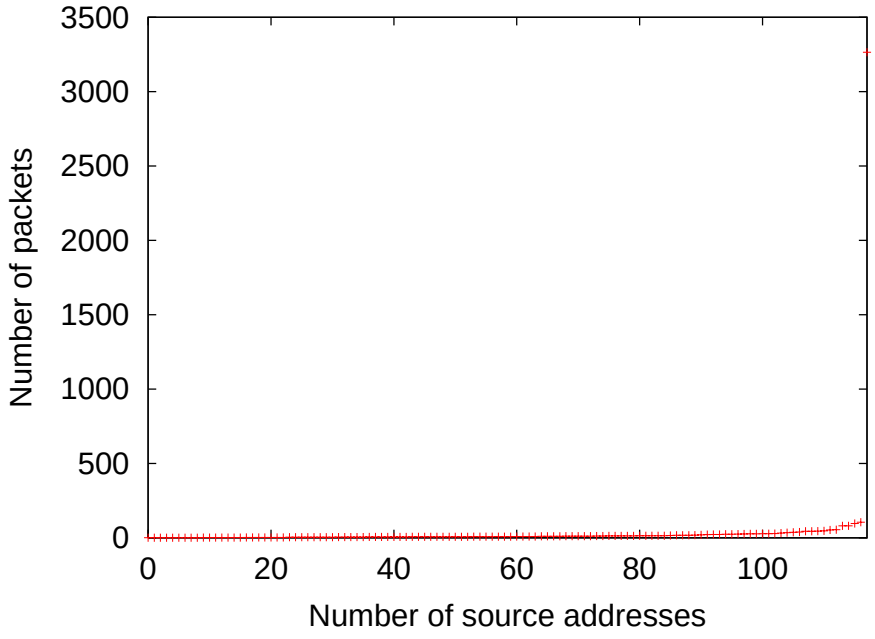


図 11: アクセス数の多い DA に対する SA の分布

図 11 は、図 9 で最もアクセスが多かった阪大から yahoo Japan へのアクセスを示したものである。1 点だけ顕著に多くアクセスしている SA が確認できるがこれはサイバーメディアセンターのプロキシサーバを経由したアクセスで、大阪大学から外部へアクセスする人数を考慮すると考えられる範囲内のアクセス数と言える。実際、トラヒックを解析してみたところ、TCP SYN Flood 攻撃と思われるトラヒックは存在していなかった。

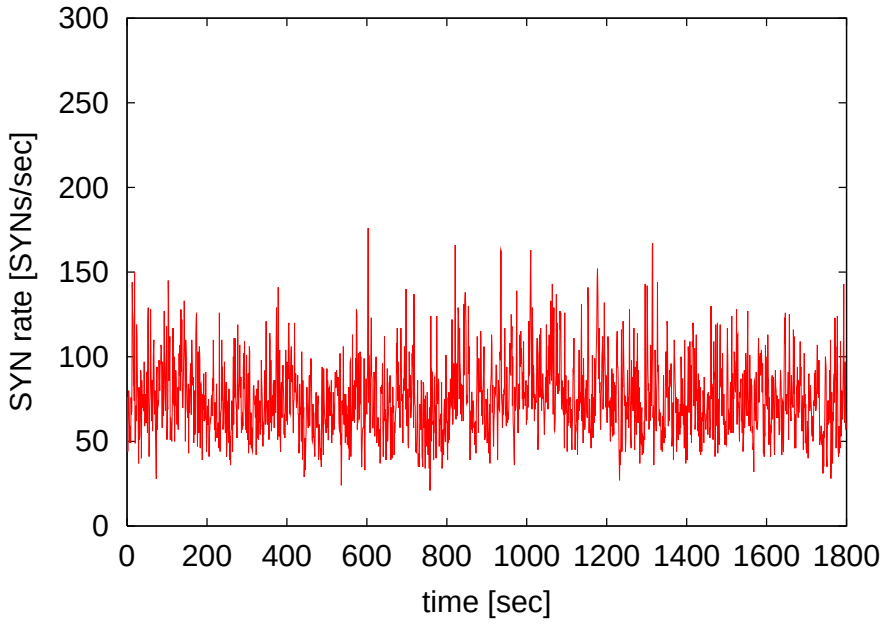
3.2.2 擬似攻撃トラヒックの生成

前節で得られた実トラヒックに定常的な攻撃トラヒックを組み込むことで擬似攻撃トラヒックの生成を行う。擬似攻撃トラヒック生成プログラムにおける入力パラメータとして

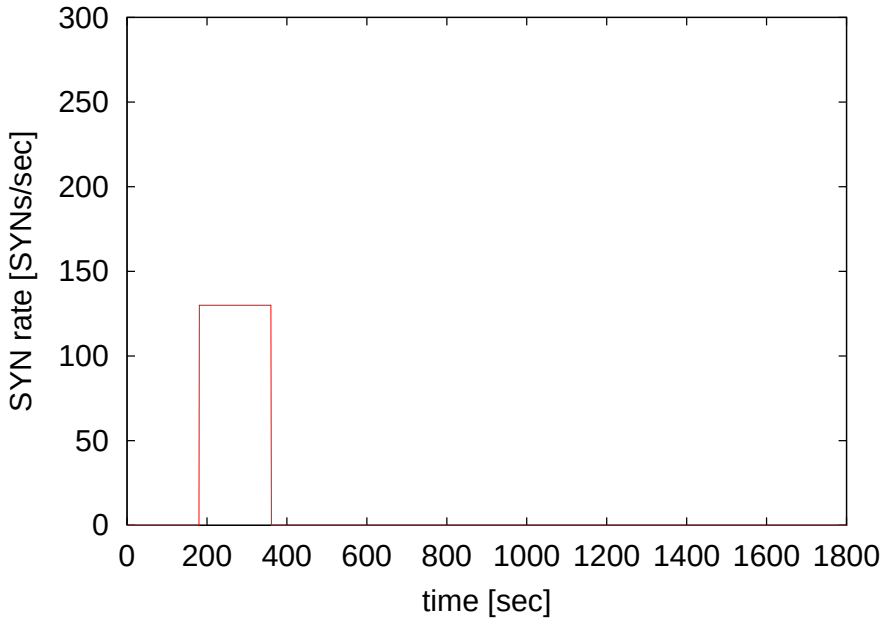
- 攻撃ホスト数 H [hosts]
- 1 攻撃ホストあたりの攻撃レート r [SYNs/sec]
- 攻撃持続時間 D [sec]

を用いる。上記のパラメータの攻撃トラヒックを組み込むと 1 攻撃ホストは攻撃パケットを $1/r$ 秒間隔で送出し、攻撃全体としては Hr [SYNs/sec] の SYN パケット発生が D 秒継続し、総計 HrD 個の攻撃パケットがターゲットホストに送出される。

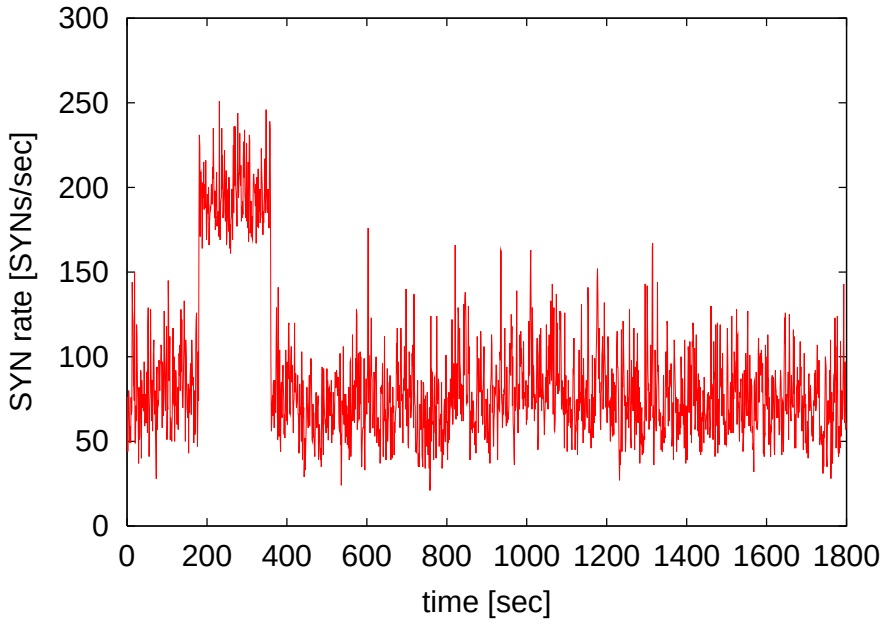
以下の図 (c) は、図 (a) で示す 12 日 14 時から 30 分間キャプチャした阪大から外部への実トラヒックに対して、図 (b) で示す攻撃ホスト数 5 、1 攻撃ホストあたりの攻撃レート 26 SYNs/sec 攻撃持続時間 180 秒 (データ内時間における 3〜6 分) の擬似攻撃トラヒックを組みこんだ擬似攻撃トラヒックの一例である。次章の防御アルゴリズムには以上のようなトラヒックを入力とし、評価を行う。



(a) 取得した実トラヒック



(b) 擬似攻撃トラヒック



(c) 生成された擬似攻撃トラヒック

図 12: 擬似攻撃トラヒックの生成手順

4 DDoS 攻撃防御アルゴリズムの概要及び性能評価

本章では、本報告で評価対象とする DDoS 攻撃防御アルゴリズムの概要を示し、3 章で得られた擬似攻撃トラヒックを適用した性能評価を行う。

4.1 防御アルゴリズムの概要

評価する防御アルゴリズムは、1 つのネットワークに対して 1 つの防御機構を持つ単一 FIFO キューによるアルゴリズムと、1 つの宛先アドレス (DA; Destination Address) に対して 1 つの防御機構を持つ DA ごと FIFO キューによるアルゴリズムの 2 つである。本節ではこれらの防御アルゴリズムの概要と考えられている問題点について述べる。

4.1.1 単一キューによる防御アルゴリズム

このアルゴリズムはネットワークの出入口にファイアウォールを設置し、そこに用意した FIFO キューにおいて送出されてくる SYN パケットを蓄積させ、SYN パケット読み出しレートの制御を行うことでネットワーク内に攻撃の影響が出ないように設計されている。単一キューによるアルゴリズムにおけるパラメータは、

- キュー長 Q [SYNs]
- SYN パケット読みだしレート R [SYNs/sec]
- 攻撃とみなし始めるキュー長 S [SYNs]

の 3 つで、R [SYNs/sec] 以上のレートで SYN パケットが送出されてくるとキューに SYN パケットが蓄積され始め、S 個の SYN パケットが蓄積されたら攻撃とみなし始める。キューに S 個の SYN パケットが蓄積してから キュー長が Q になるまでの間、攻撃検出を行うことができる。

このキューを設置することでネットワーク内のあるホストに対して過剰な SYN パケットが来た場合に直接それらのパケットをターゲットホストに流さずに、いったん蓄積しておくこ

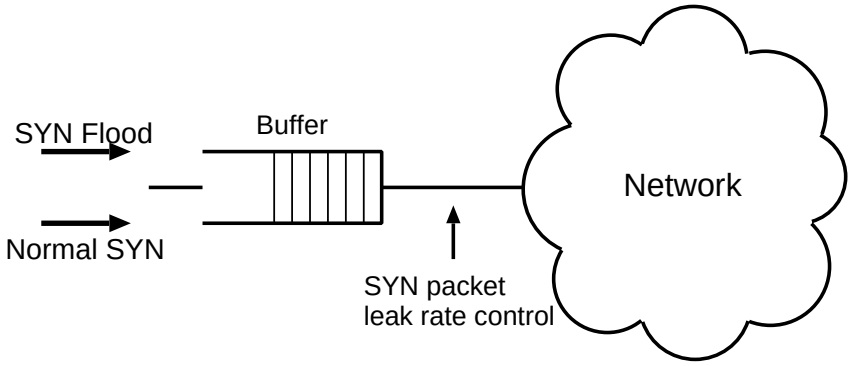


図 13: 単一 FIFO キュー防御構造

とで、攻撃検出を行う時間を稼ぐことができ、ターゲットホストへの影響も抑えることができる。

このアルゴリズムにおいて考えられる問題点として以下が考えられる。

1. 1 つのネットワークに 1 つのバッファしか持っていないので、ネットワーク内のある単一ホストが攻撃されると同一ネットワーク内の他のホストにも影響が及ぶ可能性があること

2. backlog-queue の大きさはホストで決められた値であるので、ネットワーク内の全てのホストにおける backlog-queue をあふれさせないようなレートで読みだすことを実現するのが難しいこと

などが挙げられる。また、この単一キューでは、バッファに SYN パケットが蓄積されない限り、単一ホストにトラヒックが集中している時と多数のホストにアクセスが分散している時の区別がつかないので、このアルゴリズムで検出できない場合でも、エンドホストにおいては攻撃が成立している可能性もある。

4.1.2 DA ごとキューによる防御アルゴリズム

このアルゴリズムは、上で述べたアルゴリズムがネットワークの入口にキューを設置していたのに対し、各ホストの backlog-queue に入る前にキューを設置し、 DA ごとに防御機

構を持つ。DA ごとキューにおけるパラメータは、

- 各ホストの backlog-queue の大きさ q [SYNs]
- SYN パケットのタイムアウト時間 T [sec]
- キュー長 Q [SYNs]

の 3 つである。攻撃検出は q に一定量の SYN パケットが蓄積されたときとし、このキューの攻撃検出時の読みだしレートは q と T によって q/T [SYNs/sec] と決まる。単一キューの場合と同様に Q の値が大きければキューにおけるパケット棄却率は減少し、防御性能はは向上する。各ホストごとにバッファを持っているので、単一ホストが攻撃された場合でも同一ネットワーク内の他のホストに影響を及ぼすことはなく、また q の値に合わせてホストごとに読みだしレートの設定を変えることもできる。よって、通常時はレート制御されること無く SYN パケットを通し、攻撃時のみレート制御を行い q/T [SYNs/sec] で SYN パケットを読みだすことで、backlog-queue を輻輳させないようにしている。ただし、単一キューによるアルゴリズムと比べてバッファの管理機構がより複雑なものになってしまう。

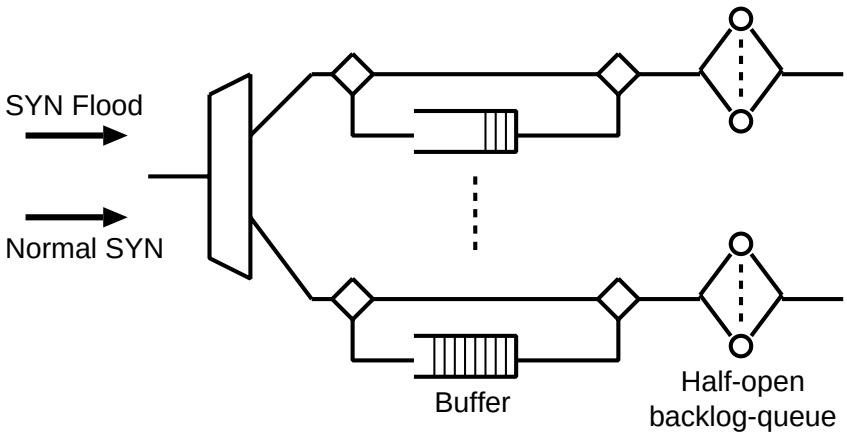


図 14: DA ごと FIFO キュー防御構造

4.2 防御アルゴリズムの評価項目

4.2.1 単一キューによる防御アルゴリズム

本報告では、単一キューによる防御アルゴリズムにおける攻撃レートがキュー長の設定に与える影響、および攻撃検出精度に影響するパラメータを考察するためにそれぞれ以下の相関を調べる。

- 攻撃レートがキュー長の設定に与える影響
  - 攻撃レートによるキュー長の変動

    まずキューの最大長 Q を無限大として、擬似攻撃トラヒックの攻撃レートを変化させ、キュー長の変動を調べる。
  - キュー長制限による影響

    キュー長の長さは実際には上限値 Q [SYNs] があり、Q まで SYN パケットが蓄積されている状態で新たに SYN パケットが来た場合、そのパケットは棄却されてしまう。Q がキュー長の変動に与える影響を調べるため、サービス拒否状態を発生させるような攻撃レートにおけるキュー長の変動をキュー長の最大長を無限大としたものと対比して示す。
  - 攻撃レートとサービス拒否時間の相関

    初期設定で与えたキュー長 Q において、攻撃レートがキューにおけるサービス拒否状態の持続時間に与える影響について調べる。
- 攻撃検出精度に影響するパラメータいち早く攻撃を検知するために必要となる攻撃とみなす閾値 S の最適値を設定する際に影響を与えるパラメータを調べるために以下の相関について調べた。なお、最適な閾値とは攻撃時、通常時を誤りなく判断できるような値をいう。
  - 誤り率と閾値の相関

    誤りとは、攻撃時を通常時、通常時を攻撃時とみなすことをさし、誤り率とは、シミュレーション内の全体時間 T [sec] に対する誤りが発生した時間 M [sec] の

割合 M/T をパーセント表示で表したものである。この値が閾値によってどのように影響を及ぼされるかについて調べる。

– サンプリング間隔と最小誤り率の相関

サンプリング間隔 P [sec] とは、攻撃判別をする最小時間単位のことをさす。この P 秒内に攻撃があったか否かを判断する際の基準は、この P を 10 個の等しいピリオド間隔 $R(= P/10)$ に区切り、それぞれの R におけるキュー長が閾値 S を超えていれば攻撃とみなし、超えていなければ通常時とみなす。10 個の R のうち 5 個以上の R において攻撃とみなされた場合、そのサンプリング間隔 P では攻撃があったとみなされる。このサンプリング間隔が最小誤り率に及ぼす影響について調べる。

– サンプリング間隔と最小閾値の相関

最後にサンプリング間隔が最小閾値に与える影響を示す。

4.2.2 DA ごとキューによる防御アルゴリズム

単一キューの場合とは異なり、 SYN パケットの読みだしレートは、そのホストにおける backlog-queue の大きさに依存することとなるので、単一キューとくらべてパケット流量制限時には急速にキューが伸びる。実際にはキューの長さを無限にすることはできないので、最適なキュー長を考えるために、攻撃レートを変動させながら、キュー長別の性能を以下の 3 つの項目について調べた。なおキューの生存時間とは、攻撃時にキューに SYN パケットが蓄積され始めてからあふれるまでの時間を表す。

- キュー長とパケット棄却率の相関
- キュー長とバッファ内遅延の相関
- キュー長とキュー生存時間の相関

4.3 防御アルゴリズムの性能評価およびその結果

4.3.1 単一キューによる防御アルゴリズム

- 初期設定値

  今回の評価において、単一キューの許容量を 170 [SYNs] 、 SYN パケット読みだしレートを 200 [SYNs/sec] とした。これらの値は、同じアルゴリズムについて検討している NetScreen 社のファイアウォールの初期設定値である [11]。

  擬似攻撃トラヒックとして、2 月 12 日 14 時から 30 分のトラヒックデータに擬似攻撃トラヒック生成プログラムにて攻撃を埋めこんだものを使用する。

- 攻撃レートとキュー長の相関について

  様々な攻撃レートの擬似攻撃トラヒックを入力としてシミュレータを動かした際のキュー長の変動を示したのが図 15 である。図 15 はキューの最大長を無限大として計測を行ったもので、擬似攻撃トラヒックによりサービス拒否状態になるのはおよそ 130 SYNs/sec の攻撃からであることがわかった。今回の計測の初期設定値である 170 [SYNs] の制限をキューに適用した場合のキュー長の変動と対比させたのが図 16 である。許容量 170 [SYNs] を超える SYN パケットは棄却されているのでキューにおいてサービス拒否が発生していると言える。

  さらに攻撃レートを増やすと図 17 で示されるように急激にサービス拒否時間は増加する。この 130 SYNs/sec の攻撃が 26 ホストによる 1 ホストあたり 5 SYNs/sec の攻撃であったとすると、攻撃参加ホストが 2 つ増えることでサービス拒否時間は 70 秒も増えることとなる。さらに攻撃レートが増加するとサービス拒否時間は、攻撃時間である 180 秒に収束していくのかわかる。よって、最適なキュー長を考える際には、想定する攻撃レートを考慮しなければならない。

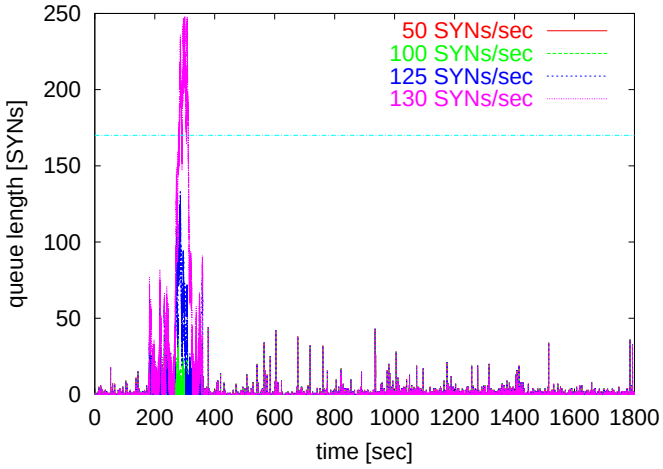


図 15: 攻撃レートによるキュー長の変動

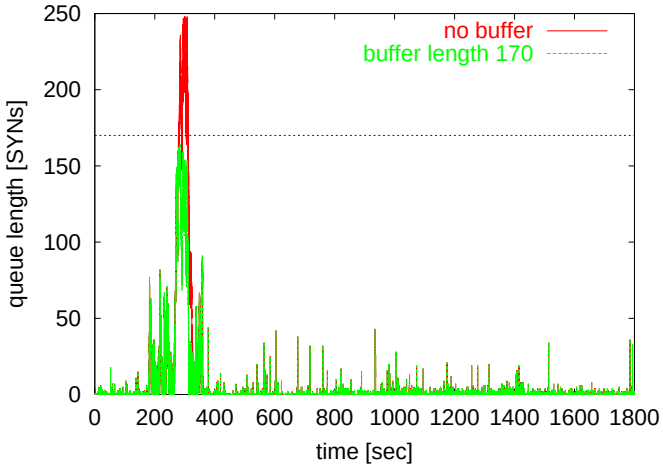


図 16: キュー長制限による影響

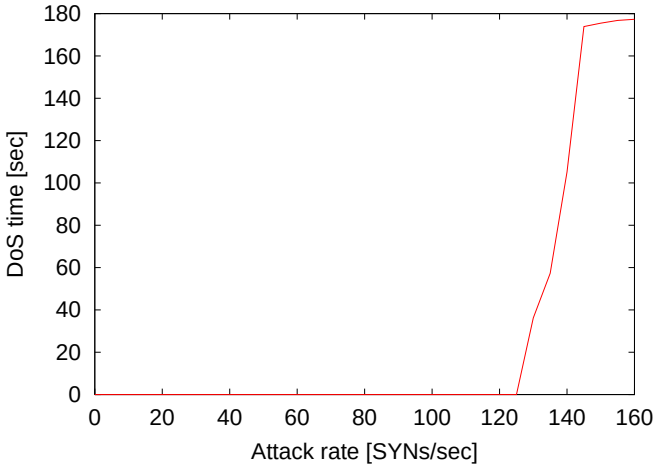


図 17: 攻撃レートとサービス拒否時間の相関

- 攻撃と判断する閾値について

  キュー長を大きくすることで、サービス拒否時間を減少させることができるが、キュー長にも限りがあり、より大規模な攻撃には耐えられないという点から効果的な解決策とは言いがたい。そこでいち早く攻撃を検知するために必要となる攻撃と判断する閾値は、キューにどの程度の SYN パケットが蓄積されたときであるのかについてサンプリング周期も考慮しながら以下に考察した。まず、図 18 で誤り率と閾値の相関をサンプリング周期 1 秒、および 0.1 秒において調べた。ここで、最小誤り率と閾値にサンプリング周期が影響している可能性が見られたので図 19、20 にてさらに関連を調べたところ、サンプリング間隔 2 秒が最も低い誤り率を達成していた。これよりサンプリング間隔が小さくなるとバースト性の影響を受けて、サンプリング間隔が大きくなると計測精度が劣化して、それぞれ誤り率が上昇したと考えられる。また、サンプリング周期が大きくなるにつれ、最小攻撃検出閾値が小さくなることも図 20 よりわかった。以上より、攻撃検出精度の決定においてサンプリング時間が影響を及ぼすことがわかった。

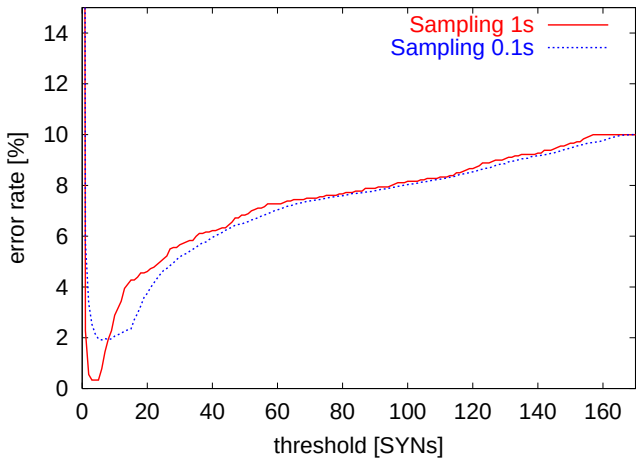


図 18: 誤り率と閾値

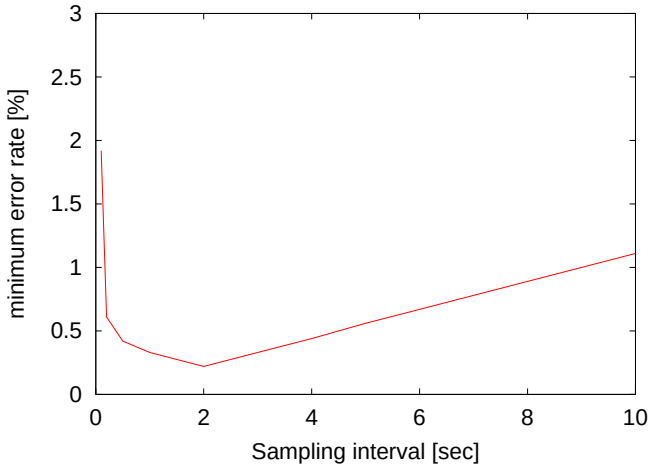


図 19: サンプリング周期と最小誤り率

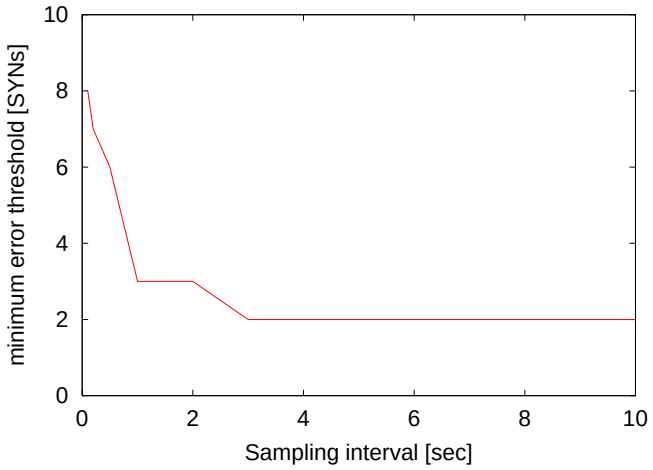


図 20: サンプリング周期と攻撃検出閾値

4.3.2 DA ごとキューによる防御アルゴリズム

- 初期設定値

  今回の評価において、各ホストの backlog-queue の大きさを 256 とし、SYN のタイムアウト時間を 20 秒 (SYN の再送回数 3 回に相当) とする。制限時の読みだしレートは 256/20 (= 12.8) [SYNs/sec] とし、攻撃時においても backlog-queue があふれることのないようにした。また、全ての計測結果は、生成した擬似攻撃トラヒックが意図的に攻撃している宛先アドレス (DA) に相当するホストにおいて計測を行った結果で

ある。

- キュー長に関する評価

  キュー長を大きくすれば、図 22 で示されるようにパケット棄却率を抑えることができ、サービス拒否状態を回避できやすくなるが、図 23 で見られるようなバッファ内遅延が生じてしまう。3000 [SYNs] のキュー長だと、パケット棄却率の観点から見ると、他のキュー長よりも高性能だが、遅延の観点から見ると最大 160 秒近くまで達し、SYN パケットのタイムアウト時間である 20 秒をはるかに上回っている。また、棄却率の上で高性能だと言っても 30 SYNs/sec 以上の攻撃に対してはサービス拒否状態に陥ってしまう。しかし、キュー長が大きければ大きいほど、攻撃を検出する時間が増加させることができる。そのことを示したのが図 21 である。キューの生存時間が大きければ、より攻撃を検出する可能性が高まり、攻撃検出後にフィルタリングを行うことができれば、攻撃下において遅延が大きくても、フィルタリングを行った後は通常時と変わらないトラヒックが流れるので、攻撃に対する耐性は強いものと考えられる。

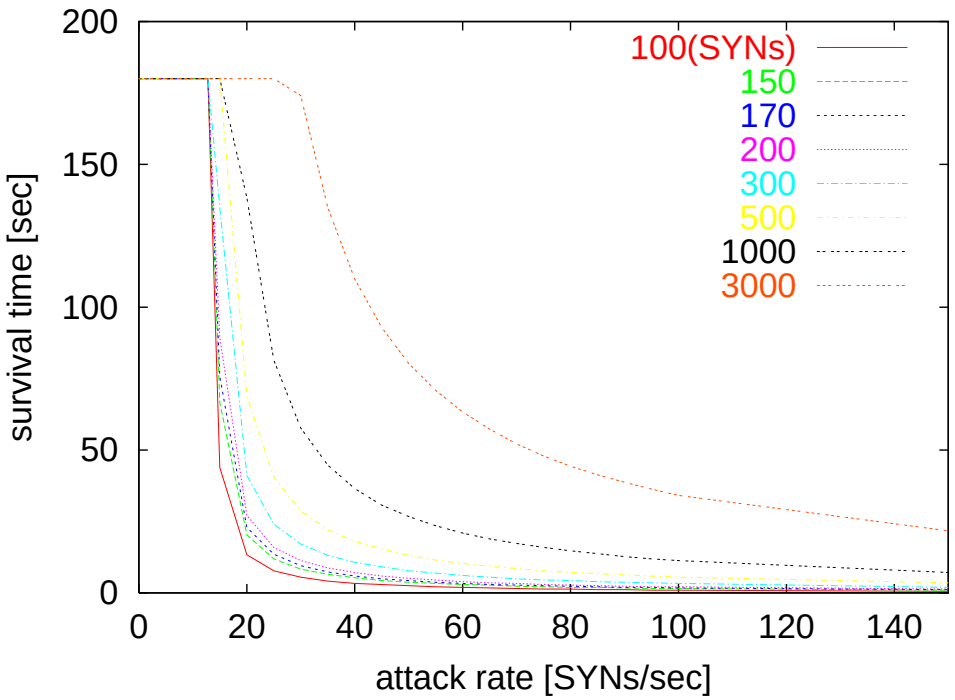


図 21: キュー長とキュー生存時間の相関

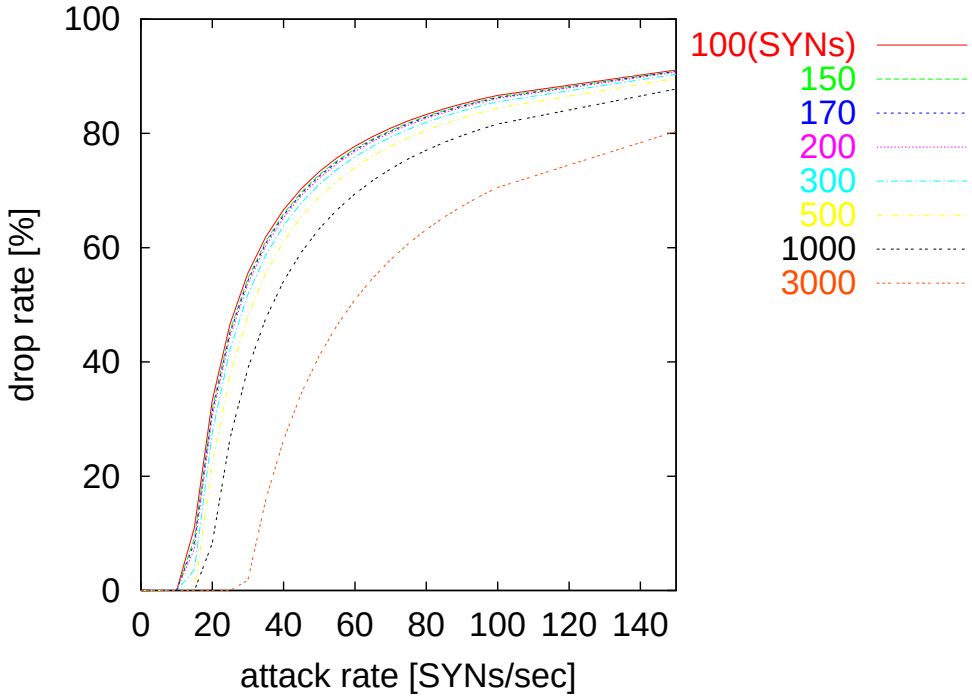


図 22: キュー長とパケット棄却率の相関

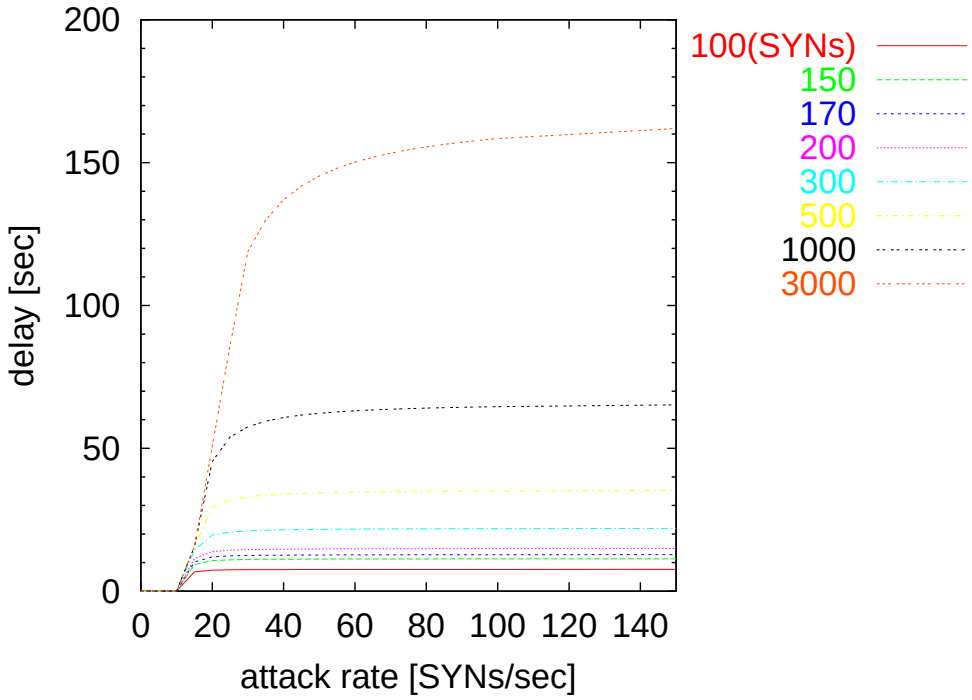


図 23: キュー長とキュー内遅延の相関

5　まとめ及び今後の課題

本報告では、DDoS 攻撃の概要とその問題点について述べ、攻撃の代表例である TCP SYN Flood 攻撃の概要を示した。

次に TCP SYN Flood 攻撃に対する防御アルゴリズムを評価するために、実際のトラヒックを取得し、それに対して擬似攻撃トラヒックを埋めこむことでシミュレーションの入力となる擬似攻撃トラヒックを生成した。また、提案されている DDoS 攻撃防御アルゴリズムの問題点を考察し、先ほど生成した擬似攻撃トラヒックを入力とし、シミュレーションによってその評価を行った。その結果、攻撃レートがキュー長に与える影響、単一キューにおける最適な閾値決定時にサンプリング周期が与える影響、 DA 毎キューにおけるバッファサイズと遅延、パケット棄却率、キューの生存時間の相関がわかった。

今後の課題として、本報告では大阪大学のネットワークのトラヒックを用いて評価を行ったが、様々なネットワーク環境での性能評価が行うことが挙げられる。

また、擬似攻撃トラヒックではなく、実際の攻撃コードを解析した上での攻撃トラヒックの生成をし、シミュレーションを行うことでアルゴリズムの有用性を示す必要がある。そしてこれらの結果から、アルゴリズム最適な設定値を考察することも課題として挙げられる。

謝辞

本報告を終えるにあたって、適切な御指導、御教授を頂いた宮原秀夫教授に心から感謝致します。また、本報告において直接御指導して頂いた村田正幸教授、日頃から適切な御指導、御助言をして頂いた大阪市立大学の阿多信吾助手に深く感謝致します。本報告において多大な御協力、御助言をしていただいた日本電信電話株式会社の山中直明氏、塩本公平氏、片山勝氏に心からお礼申し上げます。

また、本報告を行うにあたり適切な御指導をして頂いた大阪大学サイバーメディアセンターの下條真司教授、大阪府立看護大学の菅野正嗣助教授、大阪大学情報科学研究科の若宮直紀助教授、大崎博之助教授、牧一之進助手、神戸商船大学の鎌原淳三講師、大阪大学サイバーメディアセンターの長谷川剛助教授、大阪大学経済学部の荒川伸一助手、大阪大学国際公共政策研究科の植田和憲助手に心から感謝致します。日頃から多くの御助言をして頂いた後藤嘉宏氏、土居聡氏に感謝致します

最後に本報告を行うにあたり御協力頂いた宮原研究室及び村田研究室の皆様に心からお礼申し上げます。

参考文献

[1] "CNN. Cyber-attarcks batter Web heavyweights." available at `http://www.cnn.com/2000/TECH/computing/02/09/cyber.attacks.01`.

[2] "CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks." available at `http://www.cert.org/advisories/CA-1996-21.html`.

[3] "CERT Advisory CA-98.01 smurf IP Denial-of-Service Attacks." available at `http://www.cert.org/advisories/CA-1998-01.html`.

[4] H. Wang, D. Zhang, and K. G.Shin, "Detecting SYN Flooding Attacks," in *Proceedings of IEEE INFOCOM 2002*, June 2002.

[5] T.M.Gil, "MULTOPS: a data structure for denial-of-service attack detection," Master's thesis, Division of Mathematics and Computer Science, Vrije Universiteit, 2000.

[6] K.Park and H.Lee, "On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets," in *Proceedings of ACM Sigcomm 2001*, pp. 15–26, Aug. 2001.

[7] D.Moore, G.Voelker, and S.Savage, "Inferring Internet Denial of Service Activity," in *Proceedings of USENIX Security Symposium 2001*, Aug. 2001.

[8] "TCPDUMP public repository." available at `http://www.tcpdump.org`.

[9] "Problem with the FTP Port Command." available at `http://www.cert.org/tech_tips/ftp_port_attacks.html`.

[10] S. Glassman, "A Caching Relay for the World Wide Web," *Computer Networks and ISDN Systems*, vol. 27, no. 2, pp. 165–173, 1994.

[11] "NetScreen Technologies." available at `http://www.netscreen.com/dm/land_1/`.

[12] T.Darmohray and R.Oliver, "Hot Spaces for DoS Attacks," in *;login*, July 2000.