Vol.2010-DPS-143 No.7
Vol.2010-MBL-54 No.7
2010/5/20

時間応答性を考慮したDDoSの統計的検出手法

小島俊輔[†1,†2] 中嶋卓雄[†3] 末吉敏則[†2]

サーバに対するDDoS攻撃 (Distributed Denial of Services Attack) は，サーバを機能不全に陥らせ，サービスの停止を引き起こす．これまでに，送信元IPアドレスや送信先ポート番号などを確率変数とするエントロピーにより，攻撃が発見可能となることが示されている．一方で，日常的にパケット流量が少ない組織において，攻撃を早期に発見するためには，エントロピーの計算に用いるパケット数，すなわち窓幅を小さくすることが有効である．しかしながら，窓幅が小くなるほど，攻撃を判定するための閾値の範囲は狭くなり，設定が困難となる．そこで，本稿では時間経過とともに変化する動的な閾値の設定方法を提案する．提案する閾値は，窓幅が小さい場合でも効果があるため，時間応答性が良いという性質がある．また，このことから，パケット流量の少ない組織においても，早期の攻撃発見が可能である．さらに，提案する計算式は，特徴量の性質が異なる場合にも有効であることが確認できた．

DDoS Detection Technique using Statistical Analysys considering Response Time

Shunsuke Oshima,[†1,†2] Takuo Nakashima[†3]
and Toshinori Sueyoshi[†2]

DDos attacks to servers cause the disfunction and stop of the server. Previous researches have shown that the entropy for the source IP address or destination port number detect these attacks. In the organization with the small amount of packets calculating the entropy value, the window width could be reduced to detect attacks early. The small window width leads to the difficulty to set the threshold of entropy value to detect these attacks. In this research, we propose the calculation method of entropy threshold value based on the time sequence. This threshold will be effective for the case with the small window width leading the quick responding property. Our proposed method could be able to early detect in the organization with the small amount of packets. The proposed calculation is effective for the different features.

1. はじめに

現在，サイバー攻撃による被害が多数報告されているが，これらの攻撃の中にはサーバの設定ミスやセキュリティホールを狙ったDDoS攻撃 (Distributed Denial of Services Attack) が多数あり，攻撃者は主にHTTP, DNS, SMTPといった，いわゆるwell-knownポートに対する攻撃を行っている[2)3)]．サーバに対するDDoS攻撃は，サーバ自体を機能不全に陥らせ，サービスを停止させる要因となる．また，攻撃対象だけでなく，攻撃者の足場とされる被害も報告されている．これは，ボットと呼ばれるDDoS攻撃用のマルウェアを仕込まれたPCが，攻撃者の指令により所有者に気づかれることなくDDoS攻撃の加害者となる．これらの被害を受けないためには，DDoS攻撃が行われていることをできるだけ早期に発見することが望まれるが，DDoS攻撃は，通常のアクセスとの区別が難しいことが知られている[5)6)]．そこで，これらを検知するためには，サーバやクライアントPCにおいて，DDoS攻撃を自動的に検出するための仕組みが必要であり，これまで多くの手法が検討されてきた．これまでDDoSを自動的に検出するための手法として，送信元のIPアドレスや送信先のポート番号などを確率変数とするエントロピーを用いた手法が提案されている．[1)5)6)7)8)]．

エントロピーを用いたDDoS検出では，まず，連続したパケットの流れを一定の間隔で区切り，その区間内のパケットから特徴量を取り出す．その後，特徴量ごとの出現確率を計算し，個々の区間に対するエントロピーを計算する．以後，本稿では，エントロピーを計算するのに用いた1区間の間隔，すなわちパケットの数を，単に「窓幅」と記す．安定したエントロピー値を計算するためには，数万という窓の大きさが必要であることが知られている[5)8)]．しかし，通常時のパケット流量が少ない組織では，サンプルパケットを収集するまでに時間を要するため，エントロピーの時間応答性はあまりよくない．

大きな窓が必要な理由は，攻撃かどうかを判定する閾値の設定が困難となるからである．閾値が困難な理由は第一に，窓を小さくすると，攻撃を受けていない通常時のエントロピー値が揺らぎはじめる．エントロピー値がばらつくだけでなく，攻撃時のエントロピーの上昇自体も小さくなるため，攻撃と通常時のエントロピーの差は小さくなり，閾値を設定できる

†1 熊本高等専門学校 ICT 活用学習支援センター
Kumamoto National College of Technology, ICT Center for Lerning Support
†2 熊本大学 自然科学研究科
Kumamoto University, Graduate School of Science and Technology
†3 東海大学 産業工学部
Tokai University, School of Industrial Engineering

Vol.2010-DPS-143 No.7
Vol.2010-MBL-54 No.7
2010/5/20

範囲が非常に狭くなる．これにより，閾値が少しずれただけで DDoS 検知がうまくいかなくなる．第二に，攻撃を受けていない通常時のエントロピーが各組織によって異なることが，閾値の設定をさらに困難なものとしている．攻撃部分のエントロピー自体も変化する可能性はある．予見した量の DDoS 攻撃であれば検知可能であるが，実際の攻撃は，ネットワークトポロジやボット数などによって左右される．そのため，窓幅が狭い場合やさまざまな組織における定性的・定量的な閾値の設定が望まれている．

これまでエントロピーを閾値により判定[5] した論文があるが，閾値の設定方法そのものについての細かい議論はなされていない．我々の行った閾値の有効範囲の調査によると，窓幅や特徴量などにより閾値をその都度変更する必要があり，これまでの方法では定性的・定量的な値の設定が困難であることが分かった．

そこで，我々は，時系列で変化する動的な閾値の提案をする．これは，静的な閾値と比べて遜色ない F 尺度 (後述) でありながら，定性的・定量的に閾値を決定できるだけでなく，窓幅が小さい場合でも攻撃判定が可能となることを示す．これにより，パケット流量の多い組織はもちろん，パケット流量の少ない組織でも，エントロピーによる DDoS 攻撃の時間応答性が確保できる．

ところで，閾値の優劣を客観的に評価するには，False-Positive(以後 FP と略), False-Negative(以後 FN と略) を評価基準とすることが多いが，通常，FP を減らすように閾値を設定すると，FN が増える傾向があり，逆に FN を減らすように努力すれば FP が増える．そこで，今回はこれら 2 つの値の代わりに，適合率 (Precision) と再現率 (Recall) という指標を用いることとした．これらの値を計算することで，F 尺度と呼ばれる 1 つの評価値が算出できるため，FP, FN 双方の値を総合的に評価することができる．

本稿は以下のように構成する．まず，第 2 節では，エントロピーや評価に用いた式について解説する．第 3 節では，具体的な実験方法と実験環境について説明し，第 4 節にて，今回得られた結果を示す．最後に，第 5 で結論を述べる．

2. 評 価 式

2.1 エントロピー

本節では攻撃判定の基となるエントロピーの具体的な計算方法について述べる．一般に，情報源が n 個の異なるシンボルを持ち，また，各シンボルの出現確率を P_i とするとき，エントロピー H は次の式で定義される．

$$H = -\sum_{i=1}^{n} P_i \log_2 P_i \tag{1}$$

実際の計算では，まず，到達したパケットを時間軸で並べ，その連続パケット列を窓幅 W[packets] で切り出す．次に，切り出されたパケット列の 1 つ 1 つをヘッダ部とペイロード部に分割し，ヘッダ部が持つ特徴量のみを取り出す．本稿では特徴量として，送信元 IP アドレス (srcip)，送信先 IP アドレス (dstip)，送信元ポート番号 (srcport)，送信先ポート番号 (dstport)，パケット長 (length)，プロトコル (proto)，到達したパケットの TTL 値 (ttl)，フラグメント ID(id)，フラグメント用フラグの状態 (flag) の 9 つについて調査を行った．各値の出現確率は，たとえば，送信元 IP アドレスであれば，各 IP アドレスの出現回数 x_i を集計することで，出現確率 $P_i = x_i/W$ として計算することができる．

2.2 平均と標準偏差

時間の経過とともに計算したエントロピーの系列を，$H_1, H_2, ..., H_i, ...$ とする．t 番目のエントロピーを計算し終えた時点における，平均値 $\bar{H}_t$ と標準偏差 σ_{H_t} を以下のようにして計算することができる．

$$\bar{H}_t = \frac{1}{t}\sum_{i=1}^{t} H_i \tag{2}$$

$$\sigma_{H_t} = \frac{1}{t}\sum_{i=1}^{t}(H_i - \bar{H}_t)^2 = \frac{1}{t}\sum_{i=1}^{t} H_i^2 - \bar{H}_t^2 \tag{3}$$

本稿では，このエントロピーの平均値 $\bar{H}_t$ と標準偏差 σ_{H_t} を，提案する後述の動的な閾値に利用する．

2.3 適合率と再現率

DDoS 検出を行う際，攻撃を受けている時に攻撃と判断しない FN や，攻撃を受けていないのに攻撃と判断する FP を計算し，評価に用いることが多い．しかし，多くの場合，FN を少なくしようとすればするほど，FP は増える傾向があり，その逆もまた正しい．どちらを重要視するかで閾値の最適値が変わることから，客観的な評価が難しい．

そこで，今回は，情報検索の分野でよく用いられる再現率 (Recall) と適合率 (Precision) を評価値として用いることとした．tp, fp, fn を，それぞれ True-Positive，False-Positive，False-Negative となったエントロピーの個数とすると，再現率 R と適合率 P は以下の式で定義される．

Vol.2010-DPS-143 No.7
Vol.2010-MBL-54 No.7
2010/5/20

$$R = \frac{tp}{tp + fn} \tag{4}$$

$$P = \frac{tp}{tp + fp} \tag{5}$$

ここで，再現率 R，および適合率 P とは，本来攻撃を受けていた中で攻撃と判定した割合，攻撃と判定された中で本来攻撃であったものの割合をそれぞれ意味する．これらは，どちらも 0 から 1 の間の値をとり，大きい値ほど良いとされる．以上のことから，前者を FN，後者を FP に代わる指標として利用することができる．

さらに，再現率 R と適合率 P の調和平均となる F 尺度 (F-measure) と呼ばれる値を用いて，FP, FN を総合的に評価することができる．計算式を以下に示す．

$$F = \frac{1}{\frac{1}{2}(\frac{1}{R} + \frac{1}{P})} = \frac{2RP}{R + P} \tag{6}$$

この F 尺度は，R や P がどちらか一方が小さくなると，小さくなる傾向があるため，逆にこの値が大きいということは，R や P の両方が比較的大きな値を取ることを意味する．再現率や適合率と同様に，0 から 1 の間の値をとり，値が大きいほど良い．

2.4 提案する動的な閾値

まず最初に，これまで利用されていた静的な閾値について説明する．これは，過去に受けた DDoS 攻撃のパケット記録を基に，閾値を静的に決定するものである．まず，攻撃を受けている窓と攻撃を受けていない窓の二種類に分け，それぞれにおいて，エントロピーを計算し，さらにその平均値を計算する．それぞれ $\overline{H}_{attack}, \overline{H}_{normal}$ とすると，以下の式 (7) により，閾値 T_1 が決定できる．

$$T_1 = \frac{\overline{H}_{attack} + \overline{H}_{normal}}{2} \tag{7}$$

ただし，この式は DDoS 攻撃が過去に既にあったことを前提としており，これまでにないパターンの新たな攻撃が行われた場合は，対応が難しい．

今回，我々は以下の式 (8) で定義される動的な閾値を提案する．

$$T_2(t) = \overline{H}_{t-1} + Cd \cdot \sigma_{H_{t-1}} \tag{8}$$

ここで，Cd は実験的に求める定数となる．式の定義からも分かるように，エントロピー値の時間変化とともに閾値が変化する．この式により決定する閾値の特徴として，DDoS 攻撃時のエントロピー値が，あらかじめいくつになるのかを知る必要がないことが挙げられる．現在のエントロピー値そのものを用いて閾値を決定するため，窓幅などのパラメータに左右されずに運用することができ，また，これまでにないパターンの攻撃にも対応できる．さらに，閾値自体の値を決定づけるパラメータとして，標準偏差そのものではなく，標準偏差に係る係数 Cd を採用した．これにより，窓幅や特徴量が変更された場合にも，定量的な閾値となることが期待できる．

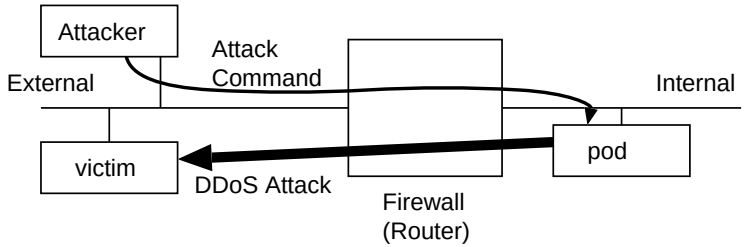

図 1 攻撃者と被害者の関係

3. 実験環境と実験方法

今回，DDoS 攻撃の実験用のパケットとして，DARPA2000[11] を用いた．DARPA2000 では，攻撃のフェーズを以下の 5 段階に分けている．

Phase1 リモートサイトから自組織への IP 掃引
Phase2 sadmind デーモンが動いている SolarisOS の IP アドレス調査
Phase3 sadmind の脆弱性を利用したシステムへの侵入
Phase4 telnet, rcp, rsh を介した DDoS 攻撃ソフトのインストール
Phase5 外部組織に対する DDoS 攻撃の開始

前提として，自組織が DDoS 攻撃を受けているのではなく，何者かが自組織に侵入し，多組織に対して DDoS 攻撃を仕掛けることを想定している．しかし，フェーズ 5 の DDoS 攻撃については，送信元 IP が偽装されており，さらに，攻撃が行われている間も通常の通信で使用されていると思われるパケットデータが流れているため，このフェーズ 5 の部分を，ある組織における DDoS 攻撃のパケットとみなし，今回の実験に利用することとした．

本実験で想定しているモデルを図 1 に示す．まず，攻撃者は Phase1 から Phase4 により，DDoS 攻撃用のマルウェアを組織内のボットとなるコンピュータに仕込む．次に，ファイアウォール内のボットに対して攻撃開始の指示を出す．すると，ボットから大量の DDoS 攻

Vol.2010-DPS-143 No.7
Vol.2010-MBL-54 No.7
2010/5/20

撃パケットが攻撃対象とした外部のサーバに対し大量に送信される．このとき，DARPA では，ファイアウォールを通過する一連のパケットをモニタしており，これを今回の実験データとした．ボットから送出されるパケットに用いられたプログラムは mstream と呼ばれる，実際の DDoS 攻撃などで使用されていたツールである．このツールは，偽 IP アドレスによる攻撃を行うため，モニタされたパケットは，実際の DDoS が仕掛けられているときの送信元 IP などの特徴を持ったパケット分布となる．

また，エントロピーの計算に用いる特徴量の出現確率については，若干の工夫を要する．各パケットの特徴量出現確率 P_i については，出現回数を x_i とすると，$P_i = x_i/W$ にて計算できるが，フラグメント ID とパケット長については，区間内のパケットがすべて異なる値を取ることも十分考えられるため，出現確率がすべて $1/W$ となる可能性もある．このままエントロピーを計算すると常に最大値に近い値になることが想定されるため，フラグメント ID(id) とパケット長 (length) について，それぞれ式 (9), 式 (10) の前処理を行うことでこの影響を少なくした．

$$P_i = \left\lfloor \frac{\mathrm{id}}{(W/c_1)} \right\rfloor /W \tag{9}$$

$$P_i = \left\lfloor \frac{\log_2 \mathrm{length}}{c_2} \right\rfloor /W \tag{10}$$

ここで，c_1, c_2 としては，1 以上の定数を想定しているが，今回は簡単のために，$c_1 = c_2 = 1$ とした．

4. 実験結果

4.1 予備実験

まず，窓幅を 10 から 10,000 まで変化させたときのエントロピー値について調査を行った．結果を図 2 に示す．

ここでは，確率変数として送信元 IP アドレス (srcip) をとり，エントロピーの計算を行った．DDoS 攻撃は図 2 のパケット数 403(×1,000) から 476(×1,000) の間で行われているが，見て分かるとおり，攻撃を受けている部分については，窓幅に関係なくエントロピーは上昇している．また，エントロピーの上昇量については，窓幅が小さいほど，少ない．ポート番号やパケット長といった特徴量を用いた場合の図については割愛するが，この図とほぼ同様の結果が得られた．その一方で，送信先 IP アドレスやパケット長などを確率変数とした場合は，確率変数の取る値が 1 箇所に集中する傾向があるため，エントロピーは逆に小さ

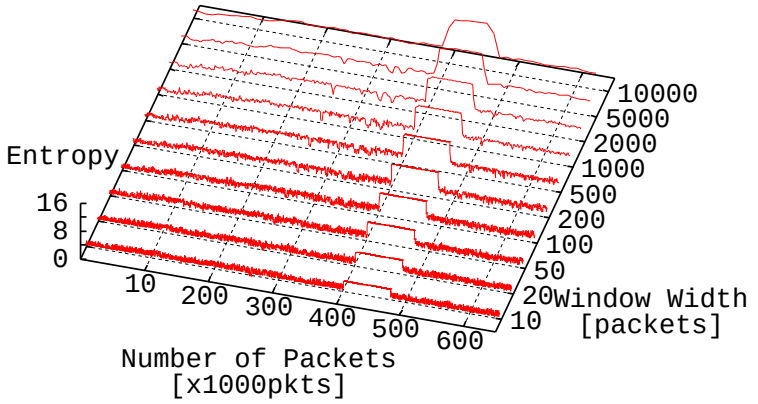

図 2 送信元 IP アドレスより計算したエントロピーと窓幅との関係

くなった．さらに，窓幅が 1000 以上のグラフでは，攻撃を受け始めてからエントロピーが上昇するまで，わずかの時間がある．攻撃の終了時にも同様の時間遅れがあり，窓幅が広いほど顕著に現れている．このことから，窓幅を広くとることで時間応答性が悪くなることがわかる．逆に，窓幅を小さくするほど，この遅れは小さくなり，時間応答性は良い．

ここで，さらに窓幅を変化させた場合の，再現率 R，適合率 P および F 尺度への影響を調べた．この実験では DDoS 攻撃を検出する閾値として式 (7) を用いている．まず最初に DARPA データを用いて閾値を決定し，その後，同じ DARPA データにより DDoS 攻撃の判定を行う．閾値の設定に用いるパケットと攻撃パケットが同じであるため攻撃判定は当然可能であるが，本実験は，あくまで，各特徴量における F 尺度の傾向を知るための予備実験という位置づけとした．まず，DDoS 攻撃部分とそうでない部分に分けて，エントロピーをそれぞれ計算し，式 (7) の閾値を越えたか否かで，tp, fp, fn をカウントする．この tp, fp, fn を基に，式 (4)， 式 (5) および式 (6) により再現率 R，適合率 P および F 尺度を計算した．結果を図 3，図 4 および図 5 に示す．

図 3 では，ほとんどの特徴量において，再現率 R の値はほぼ 1.0 となるが，フラグメント ID(id) を確率変数とした場合，窓幅が大きくなる程，再現率 R が減少している．これは，フラグメント ID の前処理の影響ではないかと考えられる．フラグメント ID が連続値を取ることによる影響を避けるため，式 (9) の前処理を行ったことは既に述べたが，$c_1 = 1$ としたため，ID が連続数の場合，ウィンドウの途中で値が 1 度変化する．変化の場所が窓の

Vol.2010-DPS-143 No.7
Vol.2010-MBL-54 No.7
2010/5/20

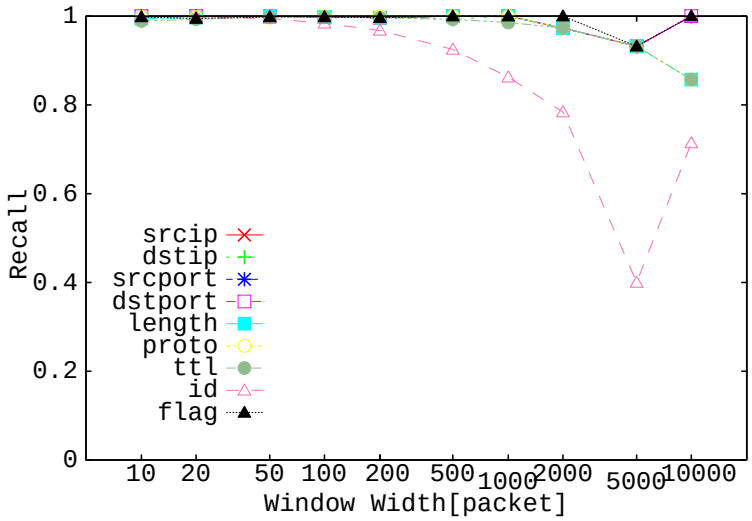

図 3 窓幅をパラメータとする再現率 (Recall) の変化

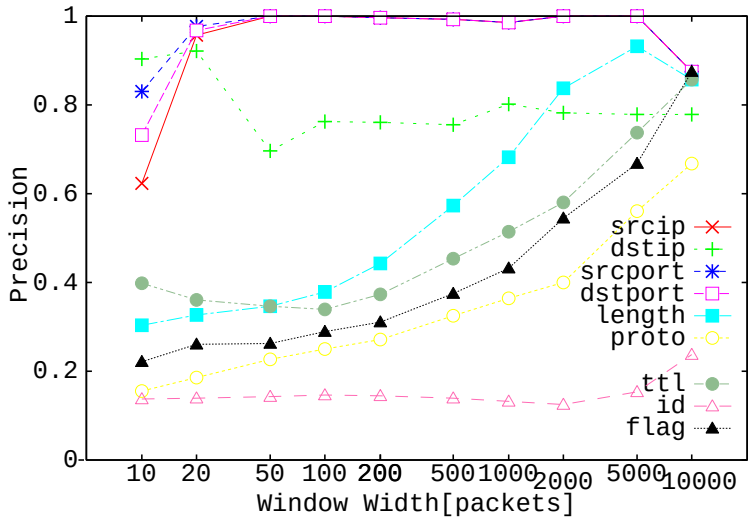

図 4 窓幅をパラメータとする適合率 (Precision) の変化

中央か端かによって，エントロピーの値は大きく変わるため，FN として判定されやすくなる．特に，窓幅が広い場合は，全体のエントロピーの計算数が少ないため，TP の数自体も少なく，その結果，1 つの FN の影響が再現率 R に大きく影響することになる．この影響を避けるためには式 (9) の c_1 を 1 以上に取れば良い．

これらの実験の結果，再現率 R については，いずれの特徴量においても，窓幅が 10 以上あれば良いことがわかった．

次に，適合率 P を調査した図 4 の結果を見ると，送信元 IP(srcip), 送信元ポート番号 (srcport) および送信先ポート番号 (dstport) の 3 つの特徴量については，適合率はほぼ 1.0 に近く，良好な結果が得られている．いずれも窓幅が 50 未満では適合率 P が低下することが確認された．このことから，適合率 P を 1.0 付近に保つためには，窓幅として最低でも 50 以上が必要であることがわかった．また，パケット長 (length)，プロトコル (proto)，TTL(ttl)，フラグメント用フラグ (flag) の 4 つの特徴量については，窓幅を小さくする程，適合率は低くなっていく．最低でも窓幅として 10,000 は必要であり，これは，Feinstein[5] らの結果と一致する．これらの特徴量については，今回の主目的である時間応答性という観点から，適当ではないと判断する．

ところで，フラグメント ID(id) については，常に適合率 P が小さいが，計算値やグラフを確認したところ，DDoS 攻撃時のエントロピーに目立った特徴が現れていないことがわかった．そのため，式 (7) で計算した閾値では，攻撃判定がうまくできず，結果，FN の量は小さいものの FP が大きくなり，適合率 P が低下したものと考えられる．この結果，フラグメント ID(id) は DDoS 検出には向いておらず，関係性も低いと判断する．

次に，送信先 IP アドレス (dstip) では，窓幅によらず，適合率 P が少し低くなっている．これについてもグラフや計算値を確認した結果，攻撃を受けている区間ではエントロピーは極めて小さくなるものの，攻撃を受けていない区間においては，特に窓幅が小さいときにエントロピーが上下に大きく振れることが確認された．この結果，攻撃を受けていない区間でも攻撃とみなす FP が異常に多くなり，適合率 P が低下する原因となった．このことから，送信先 IP(dstip) を確率変数とした場合は，単に窓幅を広くしても，適合率 P を上げることはできず，式 (7) を用いた静的な閾値による DDoS 攻撃判定にはあまり向いていないといえる．

図 3, 図 4 の結果を基に，式 (6) を用いて F 尺度を計算したものを図 5 に示す．この結果から，送信元 IP(srcip)，送信元ポート番号 (srcport)，送信先ポート番号 (dstport) の 3 つ

Vol.2010-DPS-143 No.7
Vol.2010-MBL-54 No.7
2010/5/20

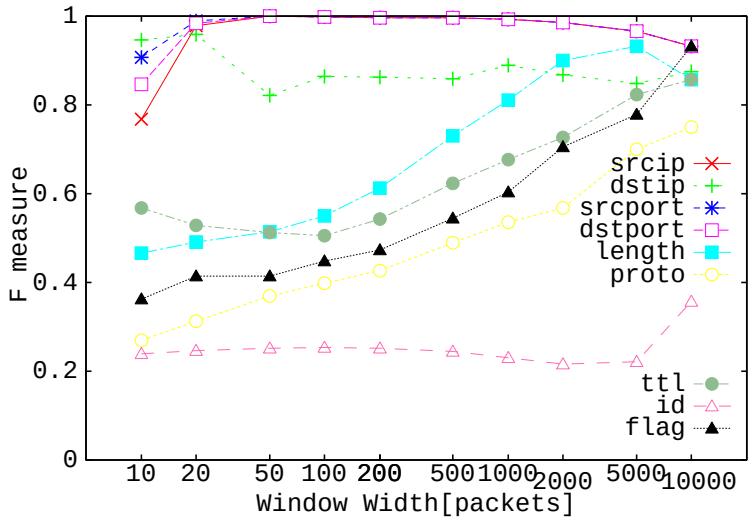

図 5 窓幅をパラメータとする F 尺度の変化

の特徴量が特に優れており，さらに窓幅は 50 以上であれば実用的であることが分かった．他の特徴量については再現率 R は高かったが，適合率 P が低いため，結果として F 尺度は低くなった．

4.2 静的な閾値による実験結果

これまでの実験結果を踏まえ，送信元 IP アドレス (srcip) と送信先 IP アドレス (dstip) を特徴量とするエントロピーで静的な閾値を用いて DDoS 攻撃判定を行った場合，窓幅が異なると F 尺度がどのように変化するのかを調査した．静的な閾値として 0 から 17 まで 0.1 刻みで変化させたときの F 尺度の変化を，図 6，図 7 に示す．これらの図から，窓幅が狭くなる程，F 尺度の大きな範囲が小さくなり，閾値自体の設定が困難になっていく様子が分かる．さらに，窓幅が小さくなると，F 尺度の上昇範囲が左にスライドしており，窓幅に応じて閾値を変化させなければならないことがわかった．

さらに，図 6，図 7 を比較することで，特徴量次第では閾値の適切な範囲がまったく異なる形状を示すこともわかった．このように，窓幅，特徴量次第では，設定する閾値が異なるため，定量的に設定することは困難である．

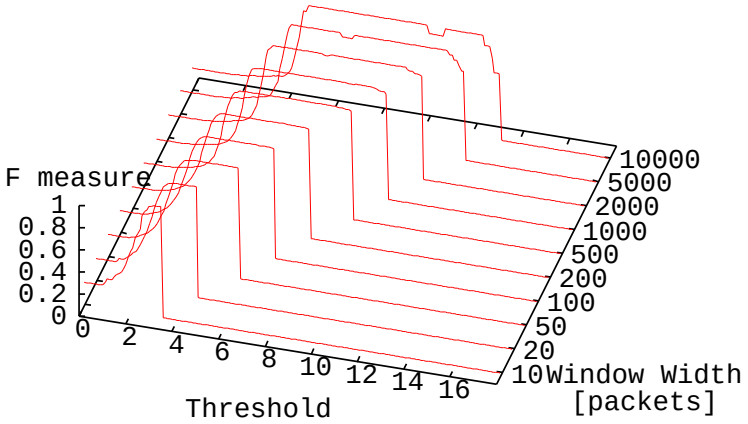

図 6 送信元 IP アドレスを確率変数とした閾値変化に伴う F 尺度

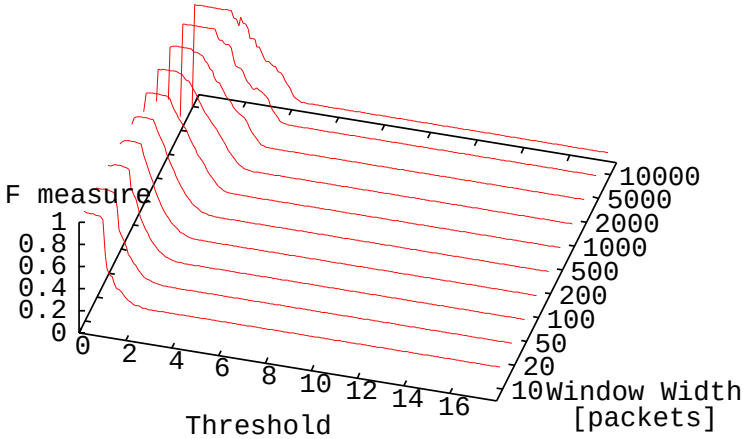

図 7 送信先 IP アドレスを確率変数とした閾値変化に伴う F 尺度

4.3 提案する動的な閾値による実験結果

ここでは，式 (8) に基づいて閾値を動的に設定し，先の図 6，および図 7 の実験と同様に送信元 IP アドレス (srcip) および送信先 IP アドレス (dstip) という 2 つの特徴量を用いてエントロピーを計算し DDoS 攻撃の判定を行った．窓幅などはまったく同一条件で F 尺度

Vol.2010-DPS-143 No.7
Vol.2010-MBL-54 No.7
2010/5/20

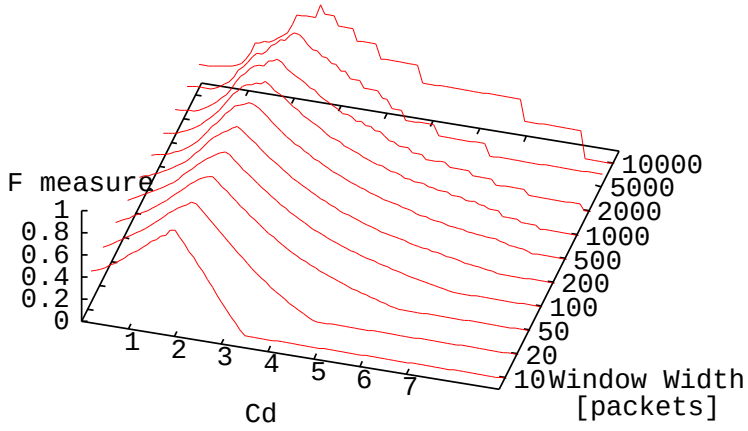

図 8 送信元 IP アドレスを確率変数とした C_d の変化に伴う F 尺度

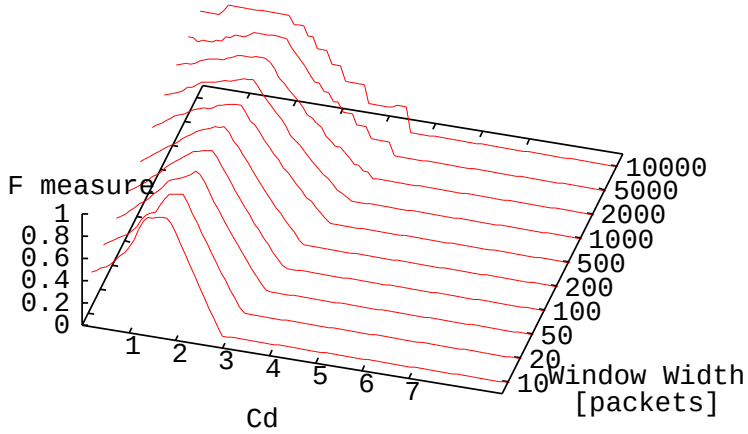

図 9 送信先 IP アドレスを確率変数とした C_d の変化に伴う F 尺度

を計測した．式 (8) の中で必要な定数 C_d については，0.1 から 17 まで 0.1 刻みで変化させている．

結果を図 8，および図 9 に示す．この結果を見ると，どちらも C_d の最適値がほぼ 2 付近に集中していることが分かる．先の図 6 や図 7 では窓幅が狭いときに閾値の範囲が狭くなるのに対し，図 8，および図 9 では窓幅によらず，$C_d = 2$ 前後を最大値とする左右の範囲が最適値となることが確認できた．

表 1 動的閾値を用いた DDoS 判定における F 尺度の最大値

	送信元 IP		送信先 IP	
窓幅	C_d	F 尺度	C_d	F 尺度
10	1.9	0.849	2.1	0.971
20	2.0	0.895	1.8	0.978
50	2.2	0.920	1.8	0.972
100	2.2	0.933	1.9	0.952
200	2.2	0.943	1.9	0.949
500	2.2	0.945	1.9	0.935
1,000	2.3	0.924	1.8	0.942
2,000	2.3	0.914	1.8	0.923
5,000	2.4	0.938	1.8	0.903
10,000	2.7	1.000	1.8	0.875

F 尺度を最大とする C_d が集中していることを確認するために，さらに，F 尺度の最大値となった C_d と，そのときの F 尺度の値をまとめて，表 1 に示す．表から，F 尺度は 1.0 とはならなかったものの，非常に高い値となることが確認できた．また，F 尺度の最大値を取った C_d の範囲が $1.8 \leq C_d \leq 2.7$ となることがわかる．今回は，時間応答性を求めているため，窓幅 5,000 や 10,000 は望ましくない．これらを除外すれば，さらに $1.8 \leq C_d \leq 2.3$ という狭い範囲に集中することになる．この結果から，送信元 IP アドレスと送信先 IP アドレスというまったく性質の違う 2 つの特徴量に対して，C_d にはそれほど大きな違いがないことが確認できた．

これらの実験結果より，窓幅の変化による閾値への影響を式 8 を用いることで抑えることができ，C_d を用いた定量的な閾値の設定が可能となる．

5. 結　　論

今回，様々な特徴量を用いてエントロピーを計算し，これより DDoS 検出を試みた．さらに，FP, FN を総合的に評価する F 尺度を用いて，検出精度の評価を試みた．その結果，送信元 IP アドレス，送信元ポート番号，送信先ポート番号については，窓幅 50 以上という条件で，DDoS 検出に非常に有効であることが確認できた．我々の組織では 1 時間に 5000 パケット程度しか到達しないが，今回の実験結果は，我々のような到達パケットの少ない組

Vol.2010-DPS-143 No.7
Vol.2010-MBL-54 No.7
2010/5/20

織においても，40 秒程度の時間で DDoS 攻撃が検出できることを示唆している．これにより，時間応答性が十分確保できることがわかった．

また，今回，閾値として，これまで提案されていた静的な閾値 (式 (7))，今回提案した動的に変化する閾値 (式 (8))，の 2 つの閾値について，F 尺度の変化を調べた．その結果，後者の我々が提案する閾値が，窓幅や特徴量の影響を受けにくく，さらに C_d として $1.8 \leq C_d \leq 2.3$ という値を取ることで，閾値を定量的に決定できることが確認できた．この実験結果より，窓幅や特徴量によらない閾値の設定が可能となる．

しかしながら，今回用いた DARPA データは，DDoS 攻撃専用ツールを用いてパケット生成しているものの，攻撃自体は人為的に作成されたものであり，非常にわかりやすい特徴を持つデータとなっている．そのため，実際の組織などにおいて DDoS 攻撃検出に応用するためには，実データによる実験や検証が欠かせないと考える．実際の通信パケットを基に多くの実験を重ねる必要があるものの，今回の実験結果は実データを用いた今後の実験の方向性を示唆するものであると考える．

6. 今後の方針

今回，送信元 IP，送信元ポート番号，送信先ポート番号の 2 つの特徴量が良いとの報告を行ったが，この結果は，あくまで 1 つの特徴量のみを単独で用いて判断しただけであり，他の特徴量がまったく不要ということではない．複数の特徴量から多変量解析や主成分分析などの手法を用いて意味のあるデータが得られる可能性がある．今後，これらについて詳細な調査を行っていく予定である．

また，実験で用いた DARPA の DDoS 攻撃データについても，人為的に作成されたものであるため，今後，実データを用いた実験を重ねることで，実際の応用について模索していく予定である．さらに，実際の組織における到達パケットを見ると，朝と夜との違いや曜日による違いがある．そのため，今後はトレンド情報を考慮した閾値について，検討する必要がある．

参 考 文 献

1) K. Lee, J. Kim, K.H.Kwon, Y.Han and S.Kim, “DDoS attack detection method using cluster analysis”, ScienceDirect, Expert Systems with Applications, Vol.34, Issue 3, pp.1659-1665, April 2008.
2) C. L. Schuba, I.V. Krsul, M.G. Kuhn, E.H. Spafford, A. Sundaram, and D. Zamboni, “Analysis of a denial of service attack on TCP”, In Proc. of the 1997 IEEE Symposium on Security and Privacy, pp.208-223, May 1997.
3) A. Magnaghi, T. Hamada,and T. Katsuyama, “A wavelet-based framework for proactive detection of network misconfigurations”, IEEE/ACM Proc. of the ACM SIGCOMM workshop on Network troubleshooting, no.3, pp.253-258, Portland, OR, US, Sept. 2004.
4) Z. Zhang, B. Fang, M. Hu, and H. Zhang, “Security analysis of session initiation protocol”, International Journal of Innovative Computing, Information and Control, vol.3, no.2, pp.457-469, Apr. 2007.
5) L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, “Statistical approaches to DDoS attack detection and response”, Proc. of DARPA Information Survivability Conf. and Exposition, Vol.1, pp.303-314, Apr. 2003.
6) G. Carl, G. Kesidis, R. Brooks, and S. Rai, “Denial-of-service attack detection techniques”, IEEE Internet Computing, vol.10, no.1, pp.82-89, Jan.-Feb. 2006.
7) A. Wagner,and B. Plattner, “Entropy based worm and anomaly detection in fast IP networks”, Proc. of the 14th IEEE International workshops on Enabling Technologies, Infrastructure for Collaborative Enterprise, no.35, pp.172-177, Linköping, Sweden, June 2005.
8) G. Nychis, V. Sekar, D.G. Andersen, H. Kim, H. Zhang, “An empirical evaluation of entropy-based traffic anomaly detection”, Proc. of the 8th ACM SIGCOMM Conf. on Internet measurement, pp.151-156, Vouliagmeni, Greece, Oct. 2008.
9) Y. Gu, A. McCallum,and D. Towsley, “Detecting anomalies in network traffic using maximum entropy estimation”, Proc. of Internet Measurement Conf. 2005, Berkeley,CA, US, pp.345-350, 2005.
10) M. Celenk, T. Conley, J. Willis, and J. Graham, “Anomaly detection and visualization using Fisher discriminant clustering of network entropy”, Third International Conf. on Digital Information Management(ICDIM), no.56, pp.216-220, London, UK, Nov. 2008.
11) Lincoln Laboratory, DARPA Intrusion Detection Evaluation, MIT(オンライン), 入手先 <http://www.ll. mit.edu/mission/communications/ist/index.html>(参照 2009-9-25).
12) K. Xu, Z. Zhang, “Internet traffic behavior profiling for network security monitoring”, IEEE/ACM Transactions on Networking, Vol. 16, No. 6, pp.1241-1252, Dec. 2008.