情報処理学会論文誌 Vol. 52 No. 2 656–668 (Feb. 2011)

エントロピーベースのマハラノビス距離による高速な異常検知手法

小島俊輔[†1,†2] 中嶋卓雄[†3] 末吉敏則[†2]

サイバー攻撃の被害を最小限に抑えるためには，できるだけ早期に，かつ多様の異常トラヒックを検知する必要がある．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異常検知が可能であることが示されている．しかし，従来の手法は，安定したエントロピーを得るために数万個の標本パケットが必要であり，早期の異常検知は困難であった．また，多くの種類の異常を検知しようとする場合，IP アドレスやポート番号などの情報源を異常の種類に応じて個別に選択する必要があり，多様な異常を同時に検出するのは困難であった．本稿ではエントロピー手法に多次元マハラノビス距離を適用した EMMM を提案する．EMMM は，複数の確率変数から求めたエントロピーだけでなく，エントロピーの相関を同時に考慮しており，多様な異常を同時に検知できる手法となる．F 尺度を用いた評価実験により，EMMM は DDoS 攻撃や IP アドレススキャンを高い精度で検出できた．また，窓幅を狭めた EMMM において，高い精度で異常を発見することができ，異常検知までの時間を大幅に短縮することができた．

Fast Anomaly Detection Method Using Entropy-based Mahalanobis Distance

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

Deterrence for minimum damage from cyber attacks requires early detection of a variety of anomaly traffic as much as possible. Possible detection of anomalies from entropy using the source IP address and destination port number as random variables has been reported. However, conventional methods require tens of thousands of sample packets to have stabilization of entropy fluctuations, making early anomaly detection difficult. In addition, detection of different sorts of anomalies requires individual selection of information sources such as IP addresses or port numbers according to the type of anomaly attacks, making concurrent detection of diverse anomaly attacks difficult. This paper proposes EMMM as an application of multidimensional Mahalanobis distance for an entropy method. The EMMM is a method to detect various anomalies concurrently, considering correlativity between each entropy as well as that acquired from multiple random variables. An evaluation experiment with F-measure proved that EMMM can detect DDoS attacks and IP address scanning with a high degree of accuracy. In anomaly detection, considerable accuracy was seen in EMMM with narrower window width meaning a substantial reduction in the detection time.

1. はじめに

近年，コンピュータウィルスによる感染被害や各種サーバに対する妨害，サービスの停止を狙った DoS/DDoS 攻撃などのサイバー攻撃が後を絶たない．DoS/DDoS 攻撃，コンピュータウィルスやワーム，ボット化された PC などを瞬時に，かつ自動的に発見できれば，サイバー攻撃の被害を最小限に抑えることができる．そのためには，コンピュータネットワークにおいてパケットをリアルタイムに監視し，通常とは異なるトラヒックの変化をとらえることが重要であり，トラヒック変化を検知する手法やシステムに関する研究が行われている．

本稿では，ウィルスや DoS/DDoS などのサイバー攻撃を**異常**，その検知を異常検知（Anomary Detection）と記す．異常検知において重要となるのは，過去に観測された異常と異なる新たな異常を検知することである．たとえば，文献 1) では，異常検知システムに対して，異常に関する統計情報やトレーニングデータを事前に与えない，という点が強調されている．そこで，異常検知システムの性能を評価する指標について特徴をまとめると次のようになる．まず第 1 に，DoS/DDoS 攻撃やワーム，Smurf，Ping of Death など様々な種類の攻撃や，新たな異常が検知可能か否か（攻撃多様性），第 2 に，異なる組織，ネットワーク，ホストであっても，同一の手法や計算アルゴリズムにより異常検知が可能か否か（組織多様性），第 3 に，1 日，1 週間あるいは 1 カ月単位で変化するようなネットワークトラヒックのパターンや周期が変化した場合でも検知が可能か否か（追従性），の 3 つの指標に大別できる．さらに，本稿では，第 4 に，異常検知アルゴリズムに必要な計算量は十分

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

小さいか（高速計算性），第 5 に，攻撃が開始されたことを短時間に検知可能か否か（即応性），という 2 つの指標を加えた計 5 つの指標により異常検知の性能を評価する．

異常検知は，パケットを観測する場所により，ホスト型とネットワーク型に分類できる．ホスト型の異常検知とは，監視の対象となるホスト自体に検知の仕組みを導入し，ホストのログ情報などを基に異常を検知する手法である．ネットワーク型の異常検知とは，検知アルゴリズムをルータやファイアウォールなどで実装し，通過するパケットを観測することで，セグメントあるいは組織全体の異常を検知する手法である．ネットワーク型は，ホスト型に比べて装置の設置数が少なくなるため設置や管理のコストは抑えられるが，高速ネットワークでの運用や組織全体におけるパケットの一括処理のため，高速計算性が必要であり，また，守るべきサーバの種類が多岐に及ぶため，攻撃多様性が必要となる．

異常検知はまた，検知するアルゴリズムにより，署名（シグネチャ）型と統計型に分類できる．署名型の異常検知は，攻撃のパターンを登録した署名と呼ばれるデータベースをあらかじめ持つことで，署名とのパターンマッチングにより異常を検知する．署名型は，組織やホストごとに署名を定めなければならず，組織多様性は低い．また，署名の数が増加するとパターンマッチングの計算量が増加するため，高速計算性は低下し，攻撃多様性への対応が困難となる．

これに対し，統計型の異常検知は，通常時のパケット列の統計情報と，異常の有無を判定したいパケット列の統計情報を比較し，異常の有無を判定する．統計型の異常検知では，連続したパケット列を，窓と呼ばれる一定の区間ごとに，窓幅と呼ばれる基準長によって区切る．窓幅は，時間もしくはパケット数を単位とする．窓に入ったパケットの持つ情報を情報源として，送信元 IP アドレスや送信先ポート番号などをシンボルとして取り出し，それらを確率変数と見なして各種の統計処理を行う．

統計型の異常検知としては，時間を窓とするパケットの総量を Z 検定や t 検定などの手法で検知する方法が提案されている．この統計型手法は，比較的簡単な計算で異常が検知できるというメリットがある．統計型手法のデメリットとして，第 1 に，検知に用いる統計量が 1 つの確率変数である場合，攻撃者は 1 つの統計情報をうまくコントロールした攻撃を仕掛けることで，異常パケットを通常パケットに見せかけた攻撃が可能となること，第 2 に，統計型の異常検知は昼夜で変化するトラヒックに対応することが困難で，追従性の確保が難しいこと，第 3 に標本パケットを収集するまでの時間が必要となるため即応性がないこと，があげられる．

我々は統計的検知手法の中で，エントロピーを用いた手法に着目した．理由として，第 1 に，攻撃者がある組織の通常時のエントロピーを知ることは難しく，通常時と異常時のエントロピーの差を観測する手法は組織多様性に優れていること，第 2 に，エントロピーを求める際は，統計処理の対象とする窓を利用するため，昼夜や週ごとのトラヒック量の変化に対応することが可能であり，少しの工夫で追従性が期待できること，第 3 に，エントロピーの計算の多くを占めるパケット数のカウントは計算量が少なく，パターンマッチング手法と比較して高速計算性があること，などのメリットがあるためである．一方，エントロピー手法のデメリットとして，第 1 に，攻撃の種類に応じて反応を示す情報源が異なるため，1 種類の情報源によるエントロピーでは攻撃多様性が低く，第 2 に，従来のエントロピー手法は，数万から数十万パケットの大きな窓幅を必要とするため，他の統計的手法と同様に即応性がない，といったことがあげられる．

そこで，本研究では，従来のエントロピー手法にマハラノビス距離を組み合せた異常検知を提案する．本手法は，エントロピー手法のメリットである組織多様性，追従性および高速計算性のメリットを損なうことなく，デメリットであった攻撃多様性と即応性を改善する．本手法は，これまでのエントロピー手法では困難であった，狭い窓による異常検知が可能なこと，および，種類の違う攻撃を検知可能なことを示す．異常が検知された場合，異常パケットの候補は窓の中にあり，窓が狭い場合は異常パケットの絞り込みが可能となる．

異常検知の精度の評価では，これまで多くの場合，異常ではないものを異常と判定してしまう False-Positive（FP）や，異常であるのに異常ではないと判定する False-Negative（FN）を使用することが多かった．しかし，FP と FN はトレードオフの関係にある．サイトポリシとの関連もあるため，FP，FN のどちらを優先するかということを含めて考えなければならず，評価基準の設定が難しかった．そこで本稿では，異常検知の精度を評価する指標として，F 尺度を使用した．これにより FP，FN の両方を可能な限り大きくとることを保証した評価が可能となる．

本稿は以下のように構成する．2 章では，これまでの関連研究と問題点を明らかにする．3 章では，エントロピーやマハラノビス距離の計算方法，F 尺度を用いた評価式について解説する．4 章では，具体的な実験方法と実験環境について説明する．5 章で実験より得られた結果を示す．最後に，6 章で結論と今後の研究方針を述べる．

2. 関 連 研 究

DoS，DDoS，ポートスキャンなどの異常を検知するため，これまでに，送信元の IP アドレスや送信先のポート番号などを情報源とするエントロピー H を用いた手法が数多く提

案されている[2)–6)]．このような異常検知の研究において，エントロピー自体が持つ特性により，攻撃多様性と即応性という 2 つの問題が生じていた．本章ではこれらについて説明する．

2.1　即応性に関する問題

一般に，DoS や DDoS，ワームなどの検知を目的とした文献では，エントロピーを計算するパケットの標本を多くとる傾向がある．たとえば，文献 2)，3) では，評価試験において数万パケットからなる窓幅を推奨している．また，文献 7) では，パケットを 2,348 種類に細かく分類してエントロピーを計算することで，スローなトラヒック変化にも柔軟に対応できることを示している．これらの手法において，窓幅を広くし，サンプルパケットを多く収集する目的は，一時的に生じた突発的な正常パケットを平均化するためである．窓が狭いと，たとえば，ある 1 つの送信元 IP アドレスを持つ通常パケットが，偶然連続して入ることは十分考えられ，エントロピーはそれに対して DoS 攻撃と同様の反応を示す．そこで，窓を広くとることにより，安定したエントロピーが計算でき，しきい値のような 1 つの指標で異常の検知が可能となる．

一方，即応性の確保には，逆に窓幅を狭くすることが有効である．しかし，エントロピーの即応性についてはこれまで十分議論されていない．理由として，狭い窓を用いた通常時のエントロピーは，異常と通常の区別ができないほど振幅の大きな値となることがあり，しきい値による異常検知が困難になるというデメリットあるからである．即応性を確保しながら，同時に FP を減らすような手法が望まれている．

2.2　攻撃多様性と異常の検知に関する問題

文献 2)，4)，6)，8) では，複数の情報源より求めたエントロピーから，多くの異常を検知する方法を示している．文献 4) では，送信元 IP アドレス，送信先 IP アドレス，送信元ポート番号，送信先ポート番号といった複数の情報源シンボルを取り出し，個別にユニバーサル符号でデータ圧縮する．データの圧縮率から間接的にエントロピーを使用し，異常検知が可能であることを示している．また，文献 6) では，さらにプロトコルを加えた 5 つの情報源シンボルについてエントロピーを求め，それぞれのエントロピーでクラスタ分析を行い，その振舞いを見ることで異常を検知している．文献 8) では，11 個の情報源シンボルからエントロピーを計算し，Fisher の線形判別法による異常検知を試みている．いずれの手法においても，送信元 IP アドレスや送信先ポート番号などの情報からエントロピーを計算し個別に評価する．

また，文献 2) は，パケットから取り出した 9 つの情報源シンボルを確率変数としてエントロピーを計算した後，主成分分析を行っている．その結果，第 3 主成分までの抽出で，異常の種類をクラス分け可能であることを示しているが，異常か否かの明確な判定基準は示されていない．

本節で紹介した手法は，複数の情報源から求めたエントロピーを利用しているため，攻撃多様性はあるものの，異常を検知する全体的なシステムが明確でない．複数のエントロピーの振舞いから異常を検知する仕組みが必要である．

3. 評　価　式

3.1　エントロピー

情報源が m 個の異なるシンボルを持ち，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．

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

具体的なエントロピー計算手順は次のとおりである．

(i)　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] ごとに切り取る．

(ii)　窓の中に入ったパケットから，パケットの持つ IP アドレスやポート番号などをシンボルとして取り出し，各シンボルごとの出現回数をカウントする．

(iii)　シンボルの出現回数 x_i から出現確率 $P_i = x_i/W$ を計算し，式 (1) によりエントロピー H を求める．

(iv)　窓を W ずつ移動しながら，上記 (i)–(iii) を繰り返すことで，時系列エントロピー $H_1, H_2, H_3, ...$ を得る．

本稿では，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），パケットバイト数（length），プロトコル（proto），TTL 値（ttl），フラグメント ID（id），フラグメント用フラグの状態（fflag）の 9 つの情報源について，それぞれ上記の計算を行い，エントロピー系列を求めた．

3.2　平均値を用いた異常検知

一般的なしきい値は，過去に観測された異常パケットにおけるエントロピーの値を基に決定する．文献 3) では，異常な部分のエントロピーと異常ではない部分のエントロピーの値が 2 つのグループに分類できることを示しており，その中間にしきい値を設定する方法を提案している．本稿では，このように平均や分散を用いた方法でしきい値を設定する方法を，

一次統計手法（First-order Statistic Method: FSM）と呼ぶことにする．

しきい値 θ は，2 グループのエントロピーの平均値の単純平均ではなく，判別分析などで用いられている判別値とするのがよい．異常時と通常時のエントロピー系列において，それぞれの平均および分散を $\bar{H}_{\rm anom}$，$\bar{H}_{\rm nom}$，$S^2_{\rm anom}$，$S^2_{\rm nom}$ とするとき，しきい値 θ から各平均値までの距離を分散により標準化すると，$(\theta-\bar{H}_{\rm anom})^2/S^2_{\rm anom}$，$(\theta-\bar{H}_{\rm nom})^2/S^2_{\rm nom}$ となる．この標準化した 2 つの距離がちょうど等しくなる位置が 2 グループを分割する場所である．2 つの距離がちょうど等しくなる θ は次の式から求まる．

$$\theta=\frac{S_{\rm anom}\bar{H}_{\rm nom}+S_{\rm nom}\bar{H}_{\rm anom}}{S_{\rm anom}+S_{\rm nom}} \tag{2}$$

この式は $S_{\rm anom}=S_{\rm nom}$ のとき，$\bar{H}_{\rm anom}$ と $\bar{H}_{\rm nom}$ の単純平均の式と一致する．異常か否かを判定したいエントロピーを H_{t+1} とすると，$H_{t+1}>\theta$ が成り立つとき異常と判定する．

この FSM のメリットは $\bar{H}_{\rm anom}$ や $\bar{H}_{\rm nom}$ が既知の場合に，しきい値を簡単に設定できることである．一方，デメリットとして，第 1 に，$\bar{H}_{\rm anom}$ と $\bar{H}_{\rm nom}$ の差が小さい場合や，分散 $S_{\rm anom}$，$S_{\rm nom}$ が大きい場合は，異常時と通常時のエントロピーの分布が重なり合い，FP や FN などの誤検知が多くなることがあげられる．窓幅を広くとることで $S_{\rm anom}$ や $S_{\rm nom}$ は小さくなるが，標本パケットの収集に時間がかかり，即応性は悪くなる．第 2 に，$\bar{H}_{\rm anom}$ を基にしきい値を決定するため，これまでにないタイプの異常の検知が難しく，攻撃多様性に乏しくなる．また，固定されたしきい値は昼夜のトラヒック変化に対応することが困難であり，追従性も低下する．そこで，本稿では攻撃多様性と追従性を実現するため，次で説明するマハラノビス距離を導入した．

3.3　マハラノビス距離

3.3.1　定　　義

マハラノビス距離は，データの持つ分散や相関を考慮した，2 つのベクトルの類似度を測る統計学的な距離として定義される．各要素の間に相関がある n 次元のベクトルデータ $\boldsymbol{H}=(H_1,H_2,...,H_n)$ とその平均 $\bar{\boldsymbol{H}}=(\bar{H}_1,\bar{H}_2,...,\bar{H}_n)$ を考える．$\bar{\boldsymbol{H}}$ から見た $\boldsymbol{H}$ のマハラノビス距離 d_m は，以下の式で定義される．

$$d_m=\sqrt{(\boldsymbol{H}-\bar{\boldsymbol{H}})^T\boldsymbol{\Sigma}^{-1}(\boldsymbol{H}-\bar{\boldsymbol{H}})} \tag{3}$$

ここで，$\boldsymbol{H}^T$ はベクトルの転置，$\boldsymbol{\Sigma}^{-1}$ は分散共分散行列の逆行列である．

1 次元と 2 次元のマハラノビス距離を用いた異常検出の概要を**図 1** に示した．図中の○や×はエントロピーの標本であり，標本の重心は組織ごとに持っている固有のエントロピー平均値となる．たとえば，H1 の平均と分散を調べれば，H1 の分布の左右に，統計的に求められるしきい値を設定することができる．1 次元マハラノビス距離は，H1 の重心からみた水平方向の距離として求まる．H1 の重心と分布は，標本をとる組織や時間帯によって変化する．したがって，平均や分散を H1 の標本値から動的に求めることで，異常判定に組織多様性や追従性を持たせることが可能となる．

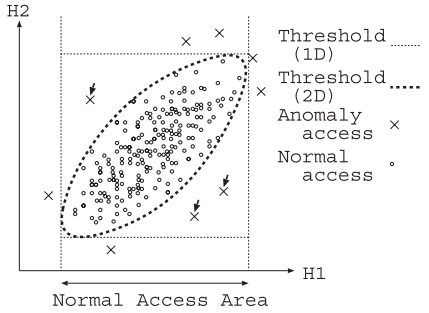


図 1　マハラノビス距離を用いた異常検知
Fig. 1　Anomaly detection using Mahalanobis distance.

さらに，2 次元マハラノビス距離は，H1 と H2 の間の相関を考慮する．図中に示した楕円は，重心からの 2 次元マハラノビス距離が等しい場所を線で結んだものである．異常の判定は，マハラノビス距離がある一定値，この図では，楕円の外に出たものを異常と判定する．1 次元マハラノビスにおいて，H1 と H2 の双方のしきい値を考慮しても発見できなかった図中の矢印のエントロピーを異常として検知することができる．

n 次元のマハラノビス距離では，各エントロピー間に $n(n-1)/2$ 個の相関が存在する．そのため，多次元マハラノビス距離は，2 次元マハラノビス距離と比較して，多くの種類の異常を検知する効果が期待できる．さらに，多次元マハラノビス距離を異常検知に用いることで，攻撃者は相関をすべて考慮した検知されにくい攻撃パケットを生成することが困難となる．

3.3.2　1 次元マハラノビス距離法（EOMM）による異常検知

エントロピーの追従性を強化するため，エントロピーベース 1 次元マハラノビス距離手法（Entropy based One dimensional Mahalanobis distance Method: EOMM）を提案する．異常の有無を判定したいエントロピーを H_{t+1}，時刻 t までのエントロピー系列の平均と分散を $\bar{H}_t$，S^2_t とし，先の式 (3) にあてはめると，マハラノビス距離は以下のスカラー量

の式 (4) となる．

$$d_m = \sqrt{\frac{(H_{t+1} - \bar{H}_t)^2}{S_t^2}} \tag{4}$$

次の式 (5) が成り立つ場合，異常と判定する．

$$d_m > \theta \tag{5}$$

たとえば，データの分布が分散 σ を持つ正規分布に従うとき，しきい値として，統計的に 2σ や 3σ が 95.4% および 99.7% というデータの存在範囲を表す．それに準じると，しきい値は $\theta = 2$ または $\theta = 3$ となる．

式 (4) では，時刻 $t+1$ の異常の判定に時刻 t までのエントロピーの統計情報を利用している．つまり，EOMM のしきい値の決定には FSM のような異常時のエントロピー値は不要で，さらにエントロピーのトレンドや組織におけるエントロピー値を考慮した値となる．これらの特徴から，EOMM は FSM と比較して追従性に優れているといえる．

3.3.3　多次元マハラノビス距離法（EMMM）

EOMM では，1 つの確率変数より求めたエントロピーを利用しており，攻撃多様性がない．そこで，複数の確率変数から求めたエントロピーベース多次元マハラノビス距離法（Entropy based Multi dimensional Mahalanobis distance Method: EMMM）を提案する．時間 $t+1$ におけるエントロピーベクトルを $\boldsymbol{H}_{t+1}$，時刻 t までのエントロピー平均ベクトルと分散共分散行列をそれぞれ $\bar{\boldsymbol{H}}_{\boldsymbol{t}}$，$\boldsymbol{\Sigma}_t$ とし，式 (3) にあてはめると，EMMM におけるマハラノビス距離は以下の式 (6) で求めることができる．

$$d_m = \sqrt{(\boldsymbol{H}_{t+1} - \bar{\boldsymbol{H}}_t)^T (\boldsymbol{\Sigma}_t)^{-1} (\boldsymbol{H}_{t+1} - \bar{\boldsymbol{H}}_t)} \tag{6}$$

EOMM と同様に式 (5) により異常を判定する．

本稿では，3 章で述べた 9 つの確率変数による 9 次元マハラノビス距離を用いた．次元数を多くした理由は，第 1 に，異常が発生した場合に計算に含めたエントロピー系列の中に異常な動きを示すエントロピーがあれば異常を検知できるため，攻撃多様性の向上が見込めること，第 2 に，窓幅が狭い EMMM でも，次元数を多くすることで見かけ上の標本数が多くなり，窓幅が広い場合と同様に平均化の効果によるエントロピーの振幅を抑即する効果と，それによる即応性の向上が見込めること，の 2 点があげられる．

EMMM の主な計算は，窓幅 W パケットごとに生じる分散共分散行列の逆行列 $\boldsymbol{\Sigma}^{-1}$ の計算である．全パケット数を N，窓幅を W として，逆行列の計算に吐き出し法を用いた場合，n 次元マハラノビス距離を用いた EMMM の時間計算量を求めると，$O(n^3 N/W)$ となる．一般に $n \ll W \ll N$ の関係があるので，$W \simeq n^2$ とした場合は，時間計算量は $O(nN)$ となる．n は一般に小さな値をとることから，十分高速に計算することが可能である．さらに，$W \simeq n^3$ であれば $O(N)$ となり，通常のエントロピー手法と比較しても，十分な高速計算性がある．また，$\boldsymbol{\Sigma}$ は対称行列であることから，n が大きい場合は特に，逆行列の計算に LDL 法などを用いることで，逆行列の計算を高速化できる．

3.4　誤検知の評価

異常検知では，誤検知となる False-Negative（FN）や False-Positive（FP）を検知の評価に用いることが多い．どのような異常検知方法を用いた場合でも，一般に FP を少なくするような穏やかな検知方法は，FN を増加させる傾向があり，その逆もまた正しい．そこで，本稿では情報検索の分野でよく用いられ，また文献 7) でも採用された F 尺度を用いて，FP，FN を総合的に評価することとした．F 尺度の計算式を式 (7) に示す．

$$F = \frac{1}{\frac{1}{2}(\frac{1}{R} + \frac{1}{P})} = \frac{2RP}{R+P} \tag{7}$$

ここで，R は再現率（Recall），P は適合率（Precision）と呼ばれる数であり，以下の式 (8)，(9) で定義される．

$$R = \frac{tp}{tp + fn} \tag{8}$$

$$P = \frac{tp}{tp + fp} \tag{9}$$

異常判定の結果，tp は異常を異常と検知した True-Positive（TP）の回数，また fp，fn は誤検知となった FP や FN の回数である．どちらも 0 から 1 の間の値をとり，1 に近いほど良い．さらに，F 尺度は，R と P の両方が同時に大きい場合に大きな値をとるため，F 尺度を，FP，FN の双方をあわせた誤検知の指標として利用することができる．再現率や適合率と同様に，0 から 1 の間の値をとり，1 に近いほど良い．

4.　実験環境と実験方法

DDoS 攻撃の実験用のパケットとして，DARPA [9] を用いた．これは，MIT Lincoln Laboratory によって作成された様々な攻撃を含んだパケットデータのサンプルであり，文献 2)，10) の評価でも利用されている．DARPA2000 のシナリオは，何者かが組織に侵入し，組織内のホストのボット化を行った後，他の組織にあるサーバに対して DDoS 攻撃を仕掛けると

いうものである．IP スキャンや DDoS 攻撃のデータ以外に，侵入の過程におけるデータがすべて保存してある．DARPA2000 は，DDoS 攻撃開始までの流れを次の 5 段階の Phase に分けている．

Phase1　リモートサイトからターゲット組織に対し，IP アドレススキャンにより使用 IP アドレスを調査．

Phase2　Phase1 で調査した IP に対して，sadmind デーモンの有無を調査．

Phase3　sadmind の脆弱性を利用したシステムへの侵入を telnet により試みる．

Phase4　telnet，rcp，rsh を利用して DDoS 攻撃ソフト mstream を 3 台のホストにインストールしボット化．

Phase5　攻撃者はボットに対して DDoS 攻撃の開始を指示．

DARPA2000 では，FW となるルータが組織の内側と外側を接続しており，このルータの内側で観測されたパケット（以下，inside データと略）と外側で観測されたパケット（以下，dmz データと略）の 2 つのパケットダンプを提供している．Phase1 の異常は，icmp echo を利用した外側から内側に対して実行された計 767 個の IP アドレススキャンからなる．ルータでは，内側の特定のサーバに対するパケットのみが通過する設定となっており，そのため Phase1 の IP スキャンパケットは内側ではわずか 20 個しか観測されない．内側から見ると，サーバ監視パケットと同じであるため，異常とは見なせず，inside データを用いた異常検知では異常の対象から外した．

一方，Phase5 の異常は，mstream と呼ばれる実際の DDoS 攻撃などで使用するツールによって生成された合計 33,754 個の DDoS 攻撃パケットからなる．内側にあるボットから，送信元 IP アドレス，送信元ポート番号，送信先ポート番号を偽装したパケットが，外側にある攻撃対象のサーバへ送信される．Phase5 のパケットは，inside データ，dmz データの両方においてほぼ同数のパケットが観測されており，異常検知の対象となる．

Phase2-4 は，Phase1 や Phase5 のようにネットワークの脆弱性を狙った攻撃ではなく，それぞれ 13 個，35 個，9 個という非常に少量の telnet や rpc を用いたアプリケーションレベルのパケットである．これらのパケットはルータを通過する設定になっており，接続されたアプリケーション側，あるいは audit などサーバのログで異常か否かを判断する．

したがって，本稿の実験において，inside データを用いた異常検知では Phase5 を，dmz データを用いた異常検知では Phase1 と Phase5 を，それぞれ異常検知の対象とした．

4.1　シンボルの前処理

シンボルとして選んだフラグメント ID（id），およびパケットバイト数（length）の 2 つの確率変数については，その性質上，そのままエントロピーの計算をしても効果が得にくいため，文献 3) や文献 7) で使用されたシンボルを複数個まとめる手法を採用した．具体的には，$[\mathrm{id}/(W/c)]$，および $[\log_r(\mathrm{length}/a)]$ の計算を施した数値を新しいシンボルと見なして出現回数をカウントすればよい．ここで，[] はガウス記号であり，c，a，r は経験的に求める定数である．ここでは，$c = 5$，$a = 1$，$r = 2$ として実験した．

表 1　実験用計算機システムの仕様
Table 1　Specification of experimental computer system.

CPU	Athlon64 X2 Dual Core Processor 5200+
Mem&Cache	メイン: 2 GB，L1: 16 KB，L2: 1,024 KB
OS	ホスト OS: Microsoft Windows XP SP3 ゲスト OS: Vine Linux 4.2 （1 コア，メモリ 1 GB に設定）
処理系	Perl v5.8.6

4.2　統計情報の更新

他の観測値から大きく外れた値を外れ値という．一般に，平均や分散の値は，外れ値に大きく引っ張られる傾向がある．EOMM や EMMM の計算においても，エントロピー H_t が外れ値となれば，平均や分散共分散行列は引っ張られてしまい，$t+1$ 以降の異常検知に与える影響が無視できなくなる．そこで，エントロピー H_t から求めたマハラノビス距離が，たとえば正規分布における 3σ と同等の概念を持つ値[⋆1]を超えた場合，H_t を外れ値と見なし，外れ値を平均や分散共分散行列の更新に使用しないこととした．以後，平均や分散共分散行列の更新を，単に**学習**と表記する．つまり，外れ値は妥当と思われるデータ以外を学習から外すためのパラメータである．一方，異常値は，異常と判定するためのしきい値であり，外れ値と同様に 3σ 付近の値を設定する．計算で求めたマハラノビス距離は，外れ値か否かに関係なく，異常値を超えた時点で異常と判定される．

4.3　使用した計算機環境と実行時間

エントロピーやマハラノビス距離の計算に使用した実験環境を**表 1** に示す．実験環境では，Windows XP のインストールされた PC 上に Linux の仮想環境を構築した．FSM や EOMM，EMMM を求める処理プログラムは非常に軽いため，実験に用いたプログラムはすべて，仮想マシン上において Perl スクリプトと UNIX のパイプ処理により記述した．こ

⋆1 n 次元のマハラノビス平方距離 d_m^2 は自由度 n の χ 二乗分布に従うことが知られており，これを利用して正規分布における 3σ に相当する値を求めることができる．

れにより，各種計算に用いるパラメータやオプションを簡単に変更したり，計算の途中経過を確認できる．

DARPA2000 では，流量の多い inside データにおいて，3 時間 15 分の間に計 649,787 個のパケットが観測されており，1 秒あたりのパケット流量を求めると，平均 55.2 [packets/sec] となる．作成したプログラムにおいて，この 55.2 [packets/sec] の処理に相当する EMMM（$n = 9$）の計算時間を計測したところ，窓幅 10 ではマハラノビス距離 5.52 個分に相当し，平均 5.18 [msec]，窓幅 100 ではマハラノビス距離 0.552 個に相当し，平均 0.527 [msec] であった．したがって，パケット流量に対するマハラノビス距離の計算時間のスケール差は 2 桁以上となる．Perl の処理時間の大部分は，tcpdump の出力するテキストから IP アドレスやポート番号などのフィールドを切り出す処理であるため，C 言語により，パケットのバイナリを直接取得するように実装しなおすことで，おそらく 1 桁程度の処理の高速化が望める．これにより，おそらく 3 桁以上のスケール差が確保でき，異常の発見までのタイムラグはない．参考まで，DARPA2000 の全パケットを Perl スクリプトで処理するのに要した時間は，窓幅 10 の場合に 61 秒であり，1 秒あたり 1 万パケット以上の処理能力がある．

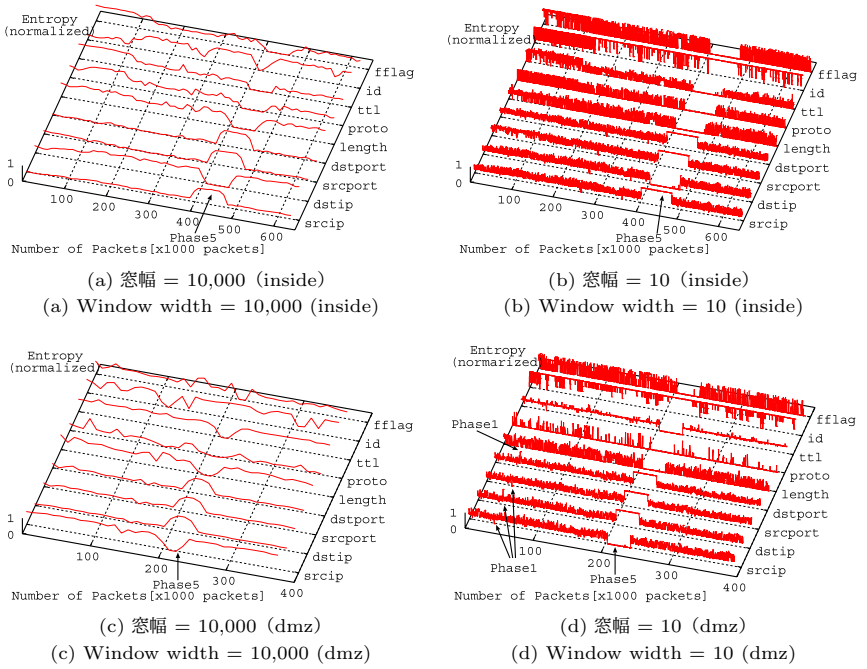
5. 実験結果

この実験で評価の対象としたデータは，DARPA2000 の IP スキャン（Phase1）および DDoS 攻撃（Phase5）である．DARPA の資料[9] によると，IP スキャンパケットは，dmz データにおいて，36,995–37,281，37,361–37,610，37,783–38,086 [packets] の 3 つの区間で断続的に観測されている．また，DDoS 攻撃パケットは，inside データでは 403,161–476,716 [packets] の区間で，dmz データでは 203,435–237,399 [packets] の区間で観測されている．

5.1 エントロピーの特性と窓幅による影響

図 2 に，inside データおよび dmz データにおいて，それぞれ窓幅 $W = 10{,}000$ および $W = 10$ を用いた，9 種類の確率変数から求めたエントロピーの結果を示す．確率変数や窓幅によってエントロピーの最大値は大きく異なるため，[0 : 1] で正規化している．

一般に，DDoS 攻撃では送信元 IP アドレス（srcip）は広い範囲に分布するためエントロピーは増加し，また，送信先 IP アドレス（dstip）は 1 つに絞られるためエントロピーは減少することが予想されるが，図 2 (a) および図 2 (c) において，その特徴が確認できた．また，id を除く他の確率変数において，異常な区間におけるエントロピーの値に増加または減少する傾向があり，特に，srcip，dstip，srcport，dstport の 4 つのエントロピーについては変化量が大きい．一方，id を確率変数とするエントロピーは，異常の有無とは関係なく変化した．



(a) 窓幅 = 10,000（inside）
(a) Window width = 10,000 (inside)

(b) 窓幅 = 10（inside）
(b) Window width = 10 (inside)

(c) 窓幅 = 10,000（dmz）
(c) Window width = 10,000 (dmz)

(d) 窓幅 = 10（dmz）
(d) Window width = 10 (dmz)

図 2　9 つの確率変数におけるエントロピーの変動
Fig. 2　Fluctuation of Entropy values in terms of 9 random variables.

窓幅によるエントロピーの違いを見ると，まず，窓幅が広い図 2 (a) や図 2 (c) の場合は，振幅の少ない安定したエントロピーが得られた．これは，窓幅 W を広くとることでパケットの分布が平均化されたためである．一方，窓を狭くした図 2 (b) や図 2 (d) は，図 2 (a) や図 2 (c) と同様にエントロピーの増加や減少の傾向は現れているものの，異常のない部分における振幅が大きい．振幅が大きい原因は，標本の数が少ないため各パケットがエントロピーに与える影響が大きくなるからである．窓幅 $W = 10$ と小さいため，たとえば，同じ送信先ポート番号（dstport）がたまたま数個程度連続して観測されると DoS/DDoS 攻撃と同じようにエントロピーは減少し，振幅が大きくなる．単に窓幅を狭くする手法は，FP,

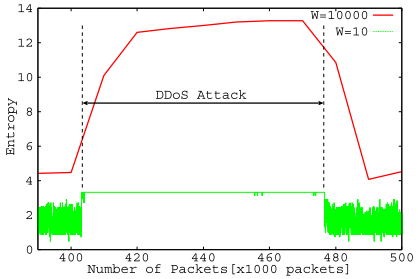
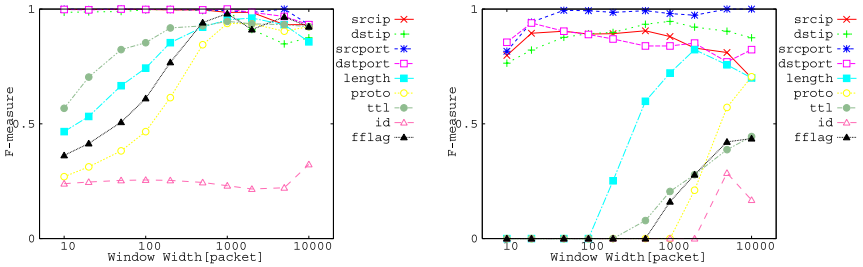


図 3　srcip の応答性に関した拡大図（inside）
Fig. 3　Zoomed up for quick response for srcip (inside).

FN が増加する傾向があり，異常検知に使用することは難しい．

確率変数の違いによるエントロピーの動きもすべて異なる．まず，図 2 (a) や図 2 (c) では srcip，dstip，srcport，dstport から求めたエントロピーに，異常と分かる大きな動きがある．mstream によって生成された DDoS 攻撃データは，このように大きな特徴が 4 つの確率変数に現れており，このことから，各種の攻撃の要素を含んだ攻撃データであるということができる．また，図 2 (c) では，Phase1 の異常がまったく検知されていない．窓幅を $W = 10{,}000$ と広くとったことにより，わずか 767 パケットからなる異常は均衡化された．このことから，少数の異常に対しては，適切な窓幅の設定が必要である．一方の図 2 (d) は，srcip，dstip，srcport，dstport の 4 つのエントロピーに IP スキャンと思われる攻撃の形跡が少し見られるが，従来の単一パラメータによる手法では，判定は難しい．一般に，DoS や Smurf，Ping-of-Death などの異常では，Phase1 の IP スキャンや Phase5 の mstream の実験結果と同一の動きとなり，攻撃多様性を確保するためには，複数の確率変数により異常を検知するマハラノビス距離のような仕組みが必要となる．

図 2 (a) および図 2 (b) の srcip において，390–500 [×1,000 packets] の区間を拡大したものを**図 3** に示す．$W = 10{,}000$ の窓を用いたエントロピーは，DDoS 攻撃の開始や終了の直後に少し遅れて反応しており，一方の窓幅 $W = 10$ のエントロピーでは，即座に反応している．エントロピーは標本パケットの収集後に計算するため，窓幅に比例した遅れが生じることになる．実際に，窓幅 $W = 10{,}000$ のグラフでは，エントロピーの変化が始まって収束するまで，ほぼ 10,000 パケットの時間を要している．したがって，エントロピーに即応性を持たせるには，窓幅の狭いエントロピーを用いることが条件となる．



(a) FSM　(b) EOMM ($\theta = 2.0$)
(a) FSM　(b) EOMM ($\theta = 2.0$)

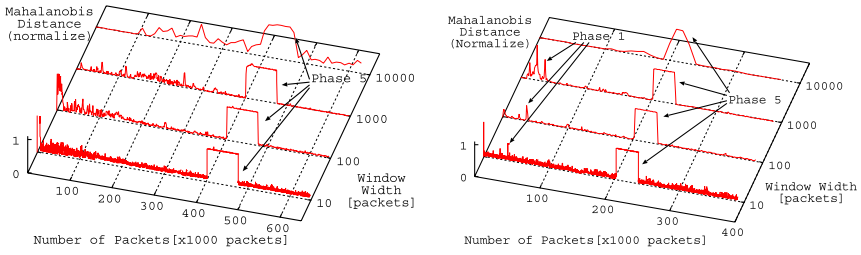
図 4　確率変数ごとの F 尺度（inside）
Fig. 4　F-measure of each random variable (inside).

5.2　EOMM における即応性の評価

FSM と EOMM による異常検知において，inside データを用いて窓幅 W をパラメータとする F 尺度の変化を調べたものを**図 4** に示す．FSM では異常検知に先立って式 (2) よりしきい値を求めた．一方の EOMM では，しきい値は実験の開始前に計算せず，式 (4) および式 (5) から動的に求めている．

図 4 (a) において，srcip，dstip，srcport，dstport の 4 つの確率変数における F 尺度は，窓幅が狭い $W \leq 1{,}000$ の区間では，F 尺度が 0.986 以上となり，特に，srcport や dstport では 1.000 となることが分かった．これは，FP と FN の個数がどちらもほぼ 0 であることを意味する．しかし，図 3 によると，$W = 10$ における異常時と通常時のエントロピーの差はごくわずかである．このような場合はしきい値の設定が難しく，上下に少しずらすだけで，F 尺度は急激に小さくなる．次に，窓幅が広い $W > 1{,}000$ において F 尺度は低下している．特に窓幅 10,000 では F 尺度は 0.923 に低下する．これはエントロピーの即応性が悪いためである．窓幅が広い場合は，異常なパケットの受信開始直後，あるいは受信終了直後はエントロピーはすぐには反応せず，F 尺度は低下する．

図 4 (b) の EOMM の結果は，srcip，dstip，srcport，dstport の 4 つの確率変数における F 尺度が高くなった．FSM には及ばないものの，特に srcport において，窓幅が広い $W \geq 100$ で，F 尺度が 0.974 以上となった．EOMM ではエントロピーの値にあわせてしきい値をリアルタイムに変化させており，エントロピーの値に順応した異常検知ができた．しかし，窓幅が狭い場合，特に $W < 100$ の区間では，F 尺度は 0.816 まで下降しており，



(a) inside データ
(a) inside data

(b) dmz データ
(b) dmz data

図 5　多次元マハラノビス距離による異常検知
Fig. 5　Anomaly detection using multi dimensional Mahalanobis distance.

即応性の問題は残る．他の length，proto，ttl，id，fflag は，F 尺度が全体的に小さく，誤検知が多すぎるため単独で利用することはできない．

5.3　EMMM の学習と検知精度に関する考察

式 (6) を基に，窓幅を 10,000，1,000，100，10 と変化させて，マハラノビス距離を求めたものを**図 5** (a) および図 5 (b) に示す．ここでは 9 つのエントロピーをすべて利用したエントロピーベクトルにより 9 次元マハラノビス距離を計算している．さらに，窓幅 W によってマハラノビス距離の絶対値が大きく異なるため，異常な区間のマハラノビス距離の大きさを 1 に正規化しプロットした．まず，Phase5 の異常については，inside，dmz どちらのデータを用いた場合でも，窓幅によらず異常を正確に検知している．1 つの確率変数から計算したエントロピーの図 2 と比較しても，明らかに図 5 の多次元マハラノビス距離は大きな反応を示している．さらに，窓幅が狭い $W = 10$ の場合は，マハラノビス距離は異常の開始と同時に急激に上昇し，異常の終了と同時に急激に下降することも確認できた．次に，Phase1 の異常は，図 5 (b) の窓幅 10，100，1,000 において正常に検知されている．しかし，窓幅 $W = 10{,}000$ とした場合，エントロピーの図 2 (c) と同様に，767 個の異常パケットは均衡化された．このことから，EMMM は，異常パケットが少ない場合でも，窓幅を適切に選ぶことにより有効な手法となる．

マハラノビス距離の初期の動きに着目すると，測定の開始直後は，平均や分散共分散行列が安定せず，10,000–20,000 [packets] 付近まで値が乱れている．特に inside データの窓幅 $W = 100$ 以下，あるいは dmz データの窓幅 $W = 1{,}000$ 以下のマハラノビス距離において，学習過程でマハラノビス距離が大きな値をとることが多い．これは，学習用に使用されるパケットの絶対数が少ないためである．式 (3) から，$\boldsymbol{\Sigma}$ の各要素の絶対値が小さい場合，もしくはエントロピーベクトル $\boldsymbol{H_t}$ の各要素の絶対値が大きい場合は，マハラノビス距離は大きくなるが，一般に，窓幅が狭い場合はエントロピーベクトル $\boldsymbol{H_t}$ の各要素のバラツキが大きく，マハラノビス距離も大きくなる傾向がある．したがって，窓幅が狭いと，学習過程において多くのマハラノビス距離が外れ値と見なされ，分散共分散行列 $\boldsymbol{\Sigma}$ の更新が遅くなるため，その間はマハラノビス距離が大きな値となる．本稿では検知精度を向上させることを目的としてパラメータを設定しており，学習過程ではエントロピーの多くが外れ値となる．しかし，この乱れは inside データにおいて 8,000 [packets] 以降，dmz データにおいて 20,000 [packets] 以降は収束する．窓幅が狭い場合は数万パケット程度の学習サンプルが必要であるが，本稿では一定の学習後の検知精度向上を目的としており，そのため，学習そのものはここでは議論の対象とはせず，今後の課題として提示するにとどめた．

図 2 の結果から，srcip，dstip，srcport，dstport の 4 つの確率変数から求めたエントロピーが DDoS 攻撃に対して反応を示すことが確認されている．一方，length，proto，ttl，fflag といった確率変数はそれほど大きな変化はなく，特に id に至っては DDoS 攻撃とは直接関係していない．つまり，異常とは関係のないエントロピーの要素がマハラノビス距離のパラメータに入っており，それにもかかわらず異常を検知できた．このことから，無関係なエントロピーがマハラノビス距離に入っていてもよく，逆に，これまでに知られていない新たな異常を検知するためには，できるだけ多くのエントロピーを含めた方が良い．現在，想定している他のエントロピーは，パケット到達時間の間隔，syn，ack，fin などの TCP ヘッダフラグ，SEQ，ACK などのシーケンシャル番号である．パケット到達時間の間隔については，同一送信元 IP アドレスや，同一送信先ポート番号を持つパケットに限定して求めることもできる．

EMMM の異常検知の精度を評価するため，**図 6** に，FSM や EOMM と同様に F 尺度を求めた結果を示す．ここでは，Phase5 の異常のみを含む inside データを用いており，異常の有無を判定するしきい値 θ を 5，10，15，20 とし，学習期間も異常検知の対象とする 4 通りの実験をした．この結果から，$\theta \geq 15$ では，窓幅 $W < 100$ において F 尺度が 0.993 以上となった．EMMM は異常か否かの判定精度が FSM や EOMM と比べて非常に高い．一方，窓幅が $W \geq 2{,}000$ と広い場合は F 尺度は低くなったが，これは，分散共分散行列 $\boldsymbol{\Sigma}$ の値が安定しなかったことが原因である．実験に用いるパケット数は同じでも，窓幅 W が広い場合は求められるエントロピー系列 H_i の数は少なくなる．ここで用いた DARPA2000 のデータ量では，$\boldsymbol{\Sigma}$ が安定するまで十分な量のエントロピー H_i が得られず，その前に攻撃

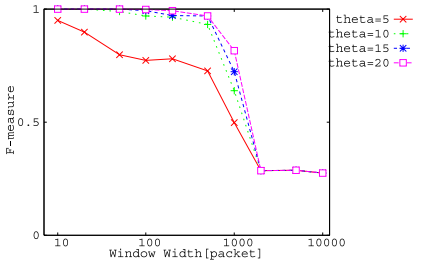


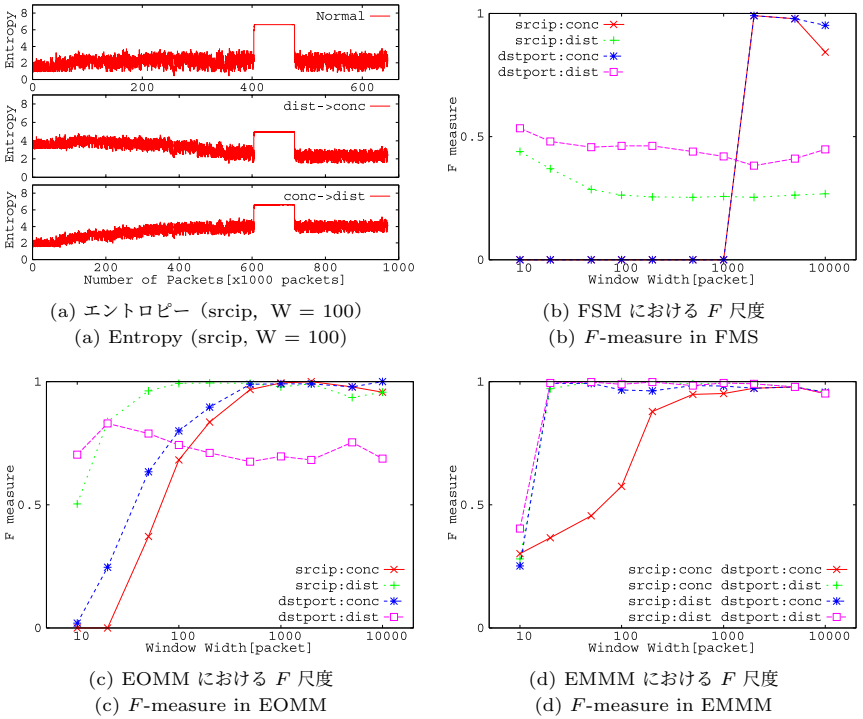
図 6　EMMM における F 尺度の向上（inside）
Fig. 6　Improvement of F-measure based on the EMMM (inside).

パケットが到達してしまい，間違った判定となった．もし $\mathbf{\Sigma}$ が安定するだけの十分な数の学習用エントロピーを攻撃前に得ることができれば，この問題は解決できる．

5.4　提案する手法における追従性の評価

FSM や EOMM の実験において F 尺度が比較的高い値を示した srcip と dstport を用いて，EOMM および EMMM の追従性の評価実験を行った．この srcip や dstport は，エントロピーを用いた異常検知において頻繁に利用される特徴量でもある．一般に，正常時のエントロピーは組織固有の値をとり，それほど大きな変化はないが，ここでは条件を少し厳しくして，通常時のエントロピーの平均値が 2 倍も変化するような場合でも，追従性があることを確認する．実験では，srcip と dstport の分布が時間とともに分散傾向から集中傾向へ変化する場合と，集中傾向から分散傾向へ移行する場合について，計 4 つのパケット列を生成し（以降ではこれを追加トラヒックと記述），DARPA2000 の inside データに対して，パケット数の 50%に相当する量を DARPA2000 全域に加えた．エントロピーの特徴から，srcip や dstport 以外の他の特徴量が集中，あるいは分散する傾向となる場合も，EOMM や EMMM の反応は srcip や dstport の反応と類似したものとなる．つまり，srcip と dstport の特徴量の分散・集中傾向およびその組合せについて調査することは，一般的なすべてのトラヒックをシミュレーションしたものと見なすことができる．

この追加トラヒックを加えたデータについて，エントロピーを求めたものを，**図 7** (a) に示す．上の図は追加トラヒックを加えていないもので，中央の図はトラヒックが分散傾向（distribution の `dist` と記載）から集中傾向（concentration の `conc` と記載）へ変化（`dist->conc`）したもの，下の図は集中傾向から分散傾向へ変化（`conc->dist`）したものである．srcip のみを示したが，dstport のエントロピーもほぼ同じ傾向となった．求めたエントロピーに対して FSM，EOMM および EMMM の各手法を適用し，F 尺度を求めたものが図 7 (b)，図 7 (c)，図 7 (d) である．外れ値や異常値といったパラメータは，各手法が有効に働くように窓ごとに微調整した．図中の `srcip:conc` とは送信元 IP アドレス（srcip）が分散傾向から集中傾向（conc）へ推移したことを意味し，`dstport:dist` とは，送信先ポート番号（dstport）が集中傾向から分散傾向（dist）へ推移したことを意味する．



(a) エントロピー（srcip，W = 100）
(a) Entropy (srcip, W = 100)

(b) FSM における F 尺度
(b) F-measure in FMS

(c) EOMM における F 尺度
(c) F-measure in EOMM

(d) EMMM における F 尺度
(d) F-measure in EMMM

図 7　追加トラヒックを付加したエントロピーと F 尺度（inside）
Fig. 7　Entropy and F-measure with the additional traffics (inside).

図 7 (b) の FSM では，srcip や dstport が集中傾向にある追加トラヒックについては，窓幅が広い $W \geq 2{,}000$ において，図 4 と同様に高い F 尺度となるが，他の部分についてはトラヒックの変化に追従できず，総じて F 尺度は低い．一方，図 7 (c) の EOMM では，F 尺度が FSM より全体的に大きくなっており，窓幅やパラメータによらず，追従性は改善さ

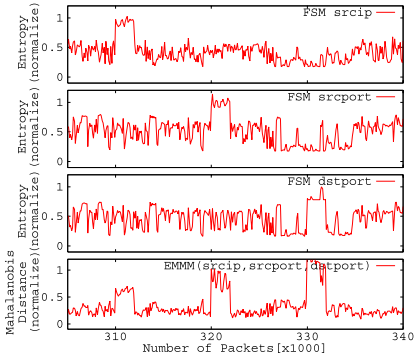
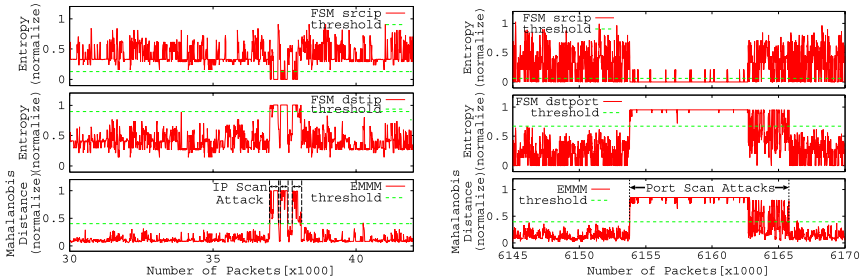


図 8　FSM と EMMM の攻撃多様性の比較（inside）
Fig. 8　Comparison of various attack detection between FSM and EMMM (inside).

れている．しかし，EOMM は，窓幅が狭い $W < 200$ の範囲において F 尺度は低くなる傾向があり，即応性に問題が残る．図 7 (d) の EMMM は，srcip，dstport が同時に集中傾向となる追加トラヒックを加えたグラフ以外の窓幅 $W \geq 20$ において，F 尺度は 0.952 以上となり，非常に高い追従性を有する．一方で，srcip と dstport の両方が集中する場合は，窓幅 $W \leq 200$ において F 尺度は低くなっているが，この原因は，追加トラヒックとして与えたパケット列の特徴が DoS 攻撃のものと似ており，特に窓幅が狭い場合に正常トラヒックを異常と見なす FP が増加したためである．

5.5　EMMM における攻撃多様性の評価

ここでは，提案する EMMM の攻撃多様性を実験により確認する．具体的には，srcip，srcport，dstport のいずれか 1 つの確率変数のみを，50%の割合で攻撃パケットの特徴であるランダム値に変更する．さらに，残りの確率変数は，ランダムな値とせず，組織の持つパケットの分布が真似されたという厳しい条件を持たせた．310 [×1,000 packets]，320 [×1,000 packets]，330 [×1,000 packets] のタイミングにおいて，それぞれ srcip，srcport，dstport のみをランダム値に書き換えており，これを基に，従来手法である FSM からエントロピーを計算したもの，およびそれから求めたマハラノビス距離を**図 8** に示した．310 [×1,000 packets] の異常については，srcip のエントロピーでは検知できるが，偽装された srcpot や dstport では検知できない．srcport や dstport をランダムに書き換えた 320 [×1,000 packets]，330 [×1,000 packets] の異常についても同様である．一方，提案する EMMM では，すべての異常を検知できる．この特徴は srcip や srcport，dstport だけでなく，マハラノビス距離の計算に使用したすべての確率変数に該当する．したがって，EMMM は，従来のエントロピー手法と比べて攻撃多様性に優れた方法となる．



(a) Phase1 における FSM と EMMM による IP スキャン検知（dmz）
(a) IP scan detection using FSM and EMMM in Phase1 (dmz).

(b) FSM と EMMM によるポートスキャン検知（DARPA1999）
(b) Port scan detection using FSM and EMMM (DARPA1999).

図 9　FSM および EMMM によるスキャニング攻撃に対する異常検知（W = 10）
Fig. 9　Anomaly detection for scanning attacks using FSM and EMMM (W = 10).

実データにおける EMMM の攻撃多様性を確認するため，DARPA2000 の Phase1 の IP アドレススキャン，および DARPA1999 [9] のポートスキャンという 2 つのデータを用いた結果を，それぞれ**図 9** (a)，および図 9 (b) に示す．前者は，図 2 (d) と図 5 (b) の Phase1 の部分を拡大したものである．この結果から，srcip や dstip, dstport のエントロピーは，いずれの場合も振動が大きく，異常とのマージンが小さいため，しきい値が設定しにくいのに対して，EMMM は振動が小さく，異常とのマージンが大きいため，容易に判定可能である．このように，EMMM は，DDoS 以外の IP アドレススキャンやポートスキャンが検知できたため，FSM と比較して攻撃多様性を備えた手法となる．さらに，EMMM は窓幅が 10 や 20 という非常に短い窓でもうまく機能するため，異常パケットが短期間に分かれて到達する場合でも，図 9 (a) のように，異常の有無に対して素早く反応している．EMMM は，従来の窓幅の広いエントロピーにはなかった高い即応性がある．

6. おわりに

従来のエントロピーを用いた異常検知は，数万個の標本パケットを用いることで安定したエントロピー値を得ることができるが，窓幅に比例した検知の遅れが生じる．逆に窓幅を狭くして即応性を優先させれば，エントロピーの振幅が大きくなり，しきい値による異常検

知が困難となる．また，異常の種類によって反応する確率変数やエントロピーの大きさが異なるため，従来の手法は，異常検知のシステムが明確でなく，攻撃多様性に対処するためには，異常の種類に応じて確率変数を適宜選択しなければならないという問題があった．

本稿で提案したEMMMは，複数の確率変数から求めたエントロピー，およびエントロピーの相関を同時に考慮したマハラノビス距離による異常検知手法である．F尺度を用いたEMMMの評価実験の結果，DDoS攻撃やIPアドレススキャンを高い精度で検出することができた．また，エントロピー間の相関を考慮したことで，窓幅が狭いEMMMにおいて異常に対応した大きな反応が得られた．これらから，EMMMは，即応性と攻撃多様性を備えた異常検出手法として有用である．しかしながら，EMMMでは，DoS/DDoSやIPアドレススキャンなど，すべての異常で値が大きくなるため，異常の種類を判定することができない．EMMMにおいて異常の種類を判定するためには，EMMMの計算過程で得られたエントロピーの増減を利用するなどの方法が考えられる．さらに，窓幅の狭いEMMMにおいては，異常なパケットがこの狭い窓の中に含まれており，窓内のパケットが10や20と少ない場合は，異常を観測した際の窓内のパケットの情報から，攻撃タイプを直接判定することは可能であると思われる．

今後の課題として，第1に実際のトラヒックによる検証を考えている．本稿で用いたDARPAデータは，DDoS攻撃専用ツールを用いてパケットを生成しており，DDoSの性質を持つものの，攻撃自体は人為的に作成されており，実際の攻撃と比較して，単純な構造を持つ．また，DARPAは1998年から2000年に作成されており，近年の攻撃の兆候を反映しているとはいい難い．そこでマルウェア対策人材育成ワークショップ（MWS）によって提供されているMWS Datasets[11]やNSAによって提供されているCDX Datasets[12]など，近年に収集されたデータを用いた実験を検討したい．第2に，過去の統計情報を効果的に忘れるような忘却モデルを確立し，このモデルをEMMMに組み込んだ，実際のトラヒックデータによる異常検知の検証を考えている．これまでに時間関数によって忘却するモデルがいくつか提案されているが，必ずしも，時間軸に沿った忘却が好ましいとは限らない．たとえば，学習過程において異常が観測される場合，あるいは正常パケットより異常パケットが長く大量に含まれる場合などにおいて，時間的な忘却モデルでは検知精度が落ちることが確認されている．異常検知をリアルタイムに動作させつつ，検知精度を上げるためには，異常部分を学習データから効率的に忘却させるための何らかの対策が必要となる．第3に，学習時間の短縮があげられる．複数の確率変数から求めるEMMMは，EOMMと比較して学習時間は長くなる．これは，外れ値を学習しないようにしたことが大きく影響している．外れ値を学習しないとは，すなわち，正常なエントロピーのエリアを慎重に，かつ少しずつ広げていくような動作となることを意味しており，学習時間を短縮するためには，正常な空間の範囲をいかに早く広げるかが鍵となる．これには，異常を含まないパケットを学習データとして与え，その間は外れ値であっても学習する，あるいは，外れ値も含めていったんすべて学習し，ある程度の学習が完了した後に，大きく外れた値のみを統計データから外す，などの工夫が必要となる．これは，先の忘却モデルとも深く関連しており，別テーマとして研究を進めている．

参 考 文 献

1) Chandora, V., Banerjee, A. and Kumar, V.: Anomaly Detection: A Survey, *ACM Computing Surveys* (*CSUR*), Vol.41, pp.1–72 (2009).
2) Lee, K., Kim, J., Kwon, K.H., Han, Y. and Kim, S.: DDoS Attack detection method using cluster analysis, *Expert Systems with Applications*, Vol.34, pp.1659–1665 (2008).
3) Feinstein, L., Schnackenberg, D., Balupari, R. and Kindred, D.: Statistical Approaches to DDoS Attack Detection and Response, *Proc. DARPA Information Survivability Conference and Exposition*, Vol.1, pp.303–314 (2003).
4) Wagner, A. and Plattner, B.: Entropy Based Worm and Anomaly Detection in Fast IP Networks, *Proc. 14th IEEE International Workshops on Enabling Technologies, Infrastructure for Collaborative Enterprise*, Linköping, Sweden, pp.172–177 (2005).
5) Nychis, G., Sekar, V., Andersen, D.G., Kim, H. and Zhang, H.: An empirical Evaluation of Entropy-based Traffic Anomaly Detection, *Proc. 8th ACM SIGCOMM Conference on Internet Measurement*, Vouliagmeni, Greece, pp.151–156 (2008).
6) Xu, K. and Zhang, Z.L.: Internet traffic behavior profiling for network security monitoring, *IEEE/ACM Trans. Networking*, Vol.16, No.6, pp.1241–1252 (2008).
7) Gu, Y., McCallum, A. and Towsley, D.: Detecting Anomalies in Network Traffic using Maximum Entropy Estimation, *Proc. Internet Measurement Conference*, Berkeley, CA, US, pp.345–350 (2005).
8) Celenk, M., Conley, T., Willis, J. and Graham, J.: Anomaly Detection and Visualization using Fisher Discriminant Clustering of Network Entropy, *3rd International Conference on Digital Information Management* (*ICDIM*), London, UK, pp.216–220 (2008).
9) MIT: DARPA Intrusion Detection Evaluation Data Set. http://www.ll.mit.edu/mission/communications/ist/index.html
10) Lee, W. and Xiang, D.: Information-Theoretic Measures for Anomaly Detection, *Proc. 2001 IEEE Symposium on Security and Privacy*, pp.130–143 (2001).

11) 畑田充弘ほか：マルウェア対策のための研究用データセット—MWS 2010 Datasets, MWS2010 (2010).
12) Sangster, B., O'connor, T.J., Cook, T., Fanelli, R., Dean, E., Adams, W.J., Morrell, C. and Conti, G.: Toward Instrumenting Network Warfare Competitions to Generate Labeled Datasets, *CSET '09 2nd Workshop on Cyber Security Experimentation and Test* (2009).

(平成 22 年 5 月 31 日受付)
(平成 22 年 11 月 5 日採録)

小島　俊輔（正会員）

1991 年熊本大学工学部電気情報工学科卒業．1993 年同大学院修士課程修了．同年八代高専情報電子工学科助手．2003 年同校助教授．現在，熊本高専 ICT 活用学習支援センター准教授．主としてネットワークセキュリティに関する研究に従事．電子情報通信学会，ACM 各会員．

中嶋　卓雄（正会員）

1986 年熊本大学大学院工学研究科修了．富士通を経て，1991 年熊本大学大学院自然科学研究科単位修得後退学．熊本大学工学部助手を経て，2001 年九州東海大学応用情報学部講師．大学統合後，現在，東海大学産業工学部電子知能システム工学科教授．博士（工学）．ネットワークパフォーマンスの評価，AdHoc ネットワークのルーティング，セキュリティ等の研究に従事．2006 年情報処理学会山下記念研究賞受賞．ACM，IEEE-CS 各会員．

末吉　敏則（正会員）

1976 年九州大学工学部情報工学科卒業．1978 年同大学院修士課程修了．同年九州大学工学部助手．同大学院助教授，九州工業大学助教授を経て，1997 年熊本大学工学部教授．現在，同大学院自然科学研究科教授．工学博士．コンピュータアーキテクチャ，コンピュータネットワーク，システムソフトウェア，リコンフィギャラブルシステム等の研究に従事．著書『並列処理マシン』，『リコンフィギャラブルシステム』（各共著）等．IEEE，電子情報通信学会，電気学会各会員．