情報処理学会論文誌 Vol.53 No.2 836–846 (Feb. 2012)

複合攻撃への検知精度を向上させるχ^2手法の提案と評価

小島 俊輔[1,2,a)] 中嶋 卓雄[3] 末吉 敏則[2]

受付日 2011年5月30日, 採録日 2011年11月7日

概要：パケットの異常を検知する統計的手法として，エントロピーやχ^2値を用いた数多くの手法が提案されている．これらの研究の中でも，エントロピー手法には，IP アドレスやポート番号など多数の特徴量を同時に確率変数とする手法が提案され，異常検知の判定精度が向上するなどの成果をあげている．しかし，χ^2手法には，異常検知の精度向上を目指した多数の特徴量を同時に扱う手法がない．また，従来の異常検知用データセットは，同一時刻においては単一の攻撃であることが多く，複合的な攻撃が加わった際の評価がされていない．そこで，本稿ではχ^2値を基にした，多変数の確率変数から異常の有無を判定するCSDM（Chi-square-based Space Division Method）手法を提案する．送信元 IP アドレスとパケットの到達時間差分の 2 つの確率変数に着目して評価した結果，提案手法は，2 つの確率変数を単独で使用するより，同時に使用した場合にF尺度が上昇することを確認した．また，DoS/DDoS の複合的な攻撃を加えた評価の結果，エントロピー手法および従来のχ^2手法と比較して，高いF尺度となった．

キーワード：DoS/DDoS 検知，異常検知，カイ二乗値，統計的手法

Proposal and Evaluation of Chi-square Method with Improvement of Detection Accuracy for Multiple Attacks

Shunsuke Oshima[1,2,a)] Takuo Nakashima[3] Toshinori Sueyoshi[2]

Received: May 30, 2011, Accepted: November 7, 2011

Abstract: As the statistical method to detect anomaly packets, a lot of methods based on entropy or chi-square method have been proposed. An entropy-based method in these researches has been proposed to treat simultaneously multiple features such as IP address and port number as the probabilistic variable. This entropy-based method achieved the improvement of the detection accuracy. On the other hand, there is no chi-square method to treat simultaneously multiple features to improve the accuracy. In addition, datasets conducted to detect anomaly attacks merely include single attack at the same time meaning that multiple attacks have not be evaluated. In this paper, we propose the CSDM (Chi-square based Space Division Method) to detect anomaly packets based on chi-square values using multi probabilistic variable. As the results of evaluations focusing on the two probabilistic variables; source IP address and packet arrival interval time, the proposed method can improve the F-measure using two features simultaneously compared to use independently. In addition, our method can achieve the high F-measure compared to the entropy method and conventional chi-square method.

Keywords: DoS/DDoS detection, anomaly detection, chi-square value, statistical approach

[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, Yatsushiro, Kumamoto 866–8501, Japan
[2] 熊本大学大学院自然科学研究科
Graduate School of Science and Technology, Kumamoto University, Kumamoto 860–8555, Japan
[3] 東海大学産業工学部
School of Industrial Engineering, Tokai University, Kumamoto 862–8652, Japan
[a)] oshima@kumamoto-nct.ac.jp

1. はじめに

ネットワークに接続されたコンピュータは，サーバの機能を停止させる DoS（Denial of Service）攻撃や DDoS（Distributed DoS）攻撃の脅威に，つねにさらされている．DDoS では，悪意あるユーザは，DDoS 攻撃の第 1 段階として，ネットワーク接続された脆弱な PC を乗っ取り，BOT

と呼ばれるコンピュータを多数作成する．この脆弱なPCを探し出すために利用されるのが，ポートスキャンやIPスキャンと呼ばれる手法である．スキャンにともない，組織などのネットワークには大量のパケットが流れる．第2段階として，悪意あるユーザは，多数のBOTに対してDoS/DDoS攻撃対象となったサーバへの攻撃指令を出し，サーバの機能を麻痺させる．ここでも，サーバとBOTの間で大量のパケットが送受信される．いずれも，大量のパケットがネットワークを流れており，本稿ではこれ以降，サーバやPCが接続されたネットワークで大量に観測される悪意あるパケットを**攻撃**と呼ぶことにする．DoS/DDoS攻撃の被害を最小限に抑えるためには，攻撃を早期に発見するための手法が必要である．このような攻撃の早期検知手法では，新たに生み出されるさまざまな攻撃に対応するため，何の知識も必要としない攻撃の発見手法が望まれる．

我々は，統計的な手法により通常トラヒックと攻撃トラヒックの違いを見分ける研究を行っており，本稿はその中のχ^2手法について着目している．エントロピー手法とまったく同一の条件下において，提案するχ^2手法を評価することで，χ^2手法の有用性を検証する．具体的には，送信元IPアドレスと差分時間とを同時に確率変数としてχ^2値を計算し，エントロピー手法との検知精度の比較検討を行った．さらに従来のχ^2手法において別々に処理されてきた通常パケットの学習とχ^2値の計算パラメータの決定という2つの機能を1つに集約した．これにより，トラヒック量が動的に変化した場合における追従を可能とした．

本稿は以下のように構成する．まず，2章では，統計的な攻撃検知手法に関する，これまでの研究と問題点について紹介する．次に，提案手法を3章で述べる．実験方法や実験結果を4章に示し，5章で結論と今後の方針を述べる．

2. 定義および関連研究

統計的な攻撃検知は，送信元IPアドレスや送信先ポート番号などの特徴量を独立変数と見なして，パケットのフィールドをシンボルとして取り出し，その度数からエントロピーやχ^2値を計算することで攻撃を検知する．本章では，これまでの統計的手法の研究についてまとめる．

2.1 エントロピー

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．

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

攻撃検知における実際の計算では，まず，到達した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のヘッダ部が持つ送信元IPアドレスや送信先ポート番号などの特徴量を取り出す．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．

エントロピーは，各シンボルの出現度数が一様に分布すると増大し，逆に1つのシンボルが集中して出現すると小さくなるという特徴がある．この特徴を用いて，これまでに多くの攻撃検知に関する論文が発表されている [1], [3], [7], [9], [12], [13], [17]．文献 [1] では，11個の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攻撃検知を試みている．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シンボルごとに評価する．文献 [7] は，パケットから取り出した9つのシンボルを確率変数としてエントロピーを計算した後，主成分分析を行い，文献 [13] は，3種類の情報源から計算したエントロピーを，振舞いの似た27のクラスタに分割して攻撃を検知している．また文献 [17] では9つのシンボルから計算したエントロピーよりマハラノビス距離を求め，攻撃検知を行っている．

2.2 χ^2 値

χ^2値は，以下の式で計算する．

$$\chi^2 = \sum_{i=1}^{B} \frac{(O_i - E_i)^2}{E_i} \tag{2}$$

ここで，Bは観測されるシンボルの数，E_iはシンボルの期待度数，O_iは観測度数である．以後，シンボルの観測に用いる区間を窓，区切る基準長を窓幅W [packets]と表記する．式 (2) は自由度$B-1$のχ^2分布に従い，期待度数と観測度数の間に差異があるほど大きくなる．文献 [3] は，到達パケットの送信元IPアドレスから求めたχ^2値が，DDoS攻撃の検知に有効であることを示している．また，文献 [4] や文献 [16] では，プリンタの使用頻度やページ数，ホームページのURLアクセス頻度などの情報から，通常と異なるユーザの使用を検知する方法が提案されている．さらに，文献 [14], [15] では，Solaris監査機能（BMS）のauditログのイベント発生度数から移動平均を計算し，それを期待値としてχ^2値を計算することで，攻撃が検知できることを示している．

2.3 既存手法の問題点

本稿で提案する手法の特長を明確にするため，本節では，既存の手法における問題点を整理する．

2.3.1 複合攻撃への耐性

世界中に多数のBOTが存在している今日では，DoSやDDoSなど，攻撃の種類数や個数自体も多く，DoSやDDoSの攻撃が重なることも多い．しかし，これまでの研究では，ほぼ同時にDoSやDDoS攻撃が発生した場合など，複合

表 1 さまざまな条件におけるエントロピー H と χ^2 値の比較
Table 1 Comparison between entropy and χ^2 values under different conditions.

Condition	Number of Packets				H	χ^2
	x_1	x_2	x_3	x_4		
Normal	64	24	9	3	1.371	0.000
DoS	100	0	0	0	0.000	56.25
DDoS	25	25	25	25	2.000	213.6
DoS+DoS	46	46	6	2	1.387	26.56
DDoS+DoS	70	10	10	10	1.357	25.17

的な攻撃を受けた際の評価はされていない．そこで，本稿では複合攻撃に対するエントロピー手法と χ^2 手法の特性を調査した．

送信元 IP アドレスやポート番号，時間などの特徴量からシンボルを取り出し，頻度 x_i で降順にソートすると，x_i は指数関数的に減少するべき乗則（power-law）に従う [2]．**表 1** は，4 種類のシンボルを持ったパケットについて，べき乗則に準じた正常値（Normal と表記）の場合，DoS/DDoS 攻撃，2 つの攻撃が重なった場合のそれぞれにおいてパケット数を想定し，エントロピー H と χ^2 値の計算結果を比較したものである．エントロピー手法では，正常時のエントロピーを基準とし，その差から攻撃かどうかを判定する．一方，χ^2 手法では，正常時の BIN のパケット数を期待度数 E_i とし，得られた χ^2 値が大きいか否かで攻撃の有無を判定する．表からも分かるとおり，DoS，DDoS の単独攻撃については，エントロピー，χ^2 値とも Normal とは異なる値となり，攻撃を検出可能である．しかし，2 つの DoS 攻撃が重なった攻撃（DoS+DoS と表記）や，DDoS 攻撃と DoS 攻撃が重なった攻撃（DDoS+DoS と表記）は，エントロピー H は正常時とほぼ同じ値となり，攻撃が検知できない．一方の χ^2 値は少し減少するものの，攻撃と認識できる値にとどまる．このように，エントロピー手法では，複合的な攻撃の検知は難しい．

2.3.2 BIN 境界の決定問題

χ^2 手法では通常時のパケットの期待度数 E_i は統計量として 5 以上となるように設定しなければならない．しかし，特徴ごとに集計したパケットの数 x_i はべき乗則 [2] に従っており，この値をそのまま E_i として用いると，べき乗則のロングテール部分において，5 より小さい期待度数 E_i が多数発生する．この問題を解消するためには，隣り合った x_i をあらかじめ決めておいた区間で複数まとめて処理する．本稿では，この複数のパケットをまとめた単位を BIN，その境界を BIN の境界と表記する．x_i が多い場合は BIN の境界を狭く，x_i が少なくなるに従って境界を広くとるようにすれば，BIN の期待度数 E_i が 5 未満となることはない．しかし，BIN のパケット数は，送信元 IP アドレスやポート番号といった特徴量の数 N，特徴量の中の総シンボル数，窓幅 W，BIN 数 B，などの多くのパラメータが影響するため，BIN の境界を決定するのは難しい．

2.3.3 複数の特徴量への対応

パケットから特徴量を 2 つ以上抽出して，そのつながりを保ったまま，攻撃の有無の判定に使用すれば，判定の精度が向上するだろうことは容易に想像できる．エントロピー手法においては，これまでに，文献 [1], [7], [13] により，独立変数を複数使用した攻撃検知手法が示されている．また，我々は，複数の特徴量から計算したエントロピーにより異常を判定する多次元マハラノビス距離法（Entropy-based Multi-dimensional Mahalanobis distance Method: EMMM）[17] を提案している．提案手法では，ある時間 $t+1$ 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，2 つのエントロピーベクトル間のマハラノビス距離を求めることで攻撃を検知する．マハラノビス距離は以下の式で求まり，$d_m > \theta$ によって異常を判定する．

$$d_m = \sqrt{(\boldsymbol{H}_{t+1} - \bar{\boldsymbol{H}}_t)^T (\boldsymbol{\Sigma}_t)^{-1} (\boldsymbol{H}_{t+1} - \bar{\boldsymbol{H}}_t)} \qquad (3)$$

一般に，n 次元のマハラノビス平方距離 d_m^2 は自由度 n の χ^2 分布に従うことが知られている．ここで，自由度 n の χ^2 分布の上側確率が α となる値を $\chi^2(\alpha, n)$ と表記し，標準正規分布の標準偏差が p 以上となる確率を $P\,(Z > p)$ と表記すれば，正規分布における 2σ の距離に相当する n 次元マハラノビス距離のしきい値 θ_n は $\theta_n = \sqrt{\chi^2(P(|Z| > 2), n)}$ で定義できる．したがって，この場合の EMMM のしきい値は，$\theta_1 = 2.000$，$\theta_2 = 2.486$ となる．本稿では，この EMMM を，今回の提案手法と比較実験する．

一方，χ^2 手法で多数の独立変数を扱う際は，まず $n \times m$ 分割表を作成し，各セルの値を観測値 O_i と見なす．この場合，求めた χ^2 値は $(n-1)\cdot(m-1)$ の自由度を持つ χ^2 分布に従う．しかし，次にあげる 2 つの理由から，ネットワークを流れるパケットに対して χ^2 手法をそのまま適用することは難しい．第 1 の問題は，送信元 IP アドレスやパケット長など，パケットが持つ特徴量の各シンボルの出現頻度はべき乗則に従っており [2]，単純に分割表を適用すると，パケットが集中するセルと，ほぼ 0 となるセルが生じ，分割表の意味が薄れることである．たとえば，どちらの特徴量から見ても，50%ずつに配分される分割表を**図 1** (a) と図 1 (b) に示した．特徴が図 1 (a) であれば，分割表を χ^2 手法に適用できるが，一般的なパケットには図 1 (b) のような傾向があり，χ^2 手法への適用は難しい．第 2 に，BIN の境界の決定問題がある．BIN の境界は，次元数や分割数が増えるほど設定が困難となり，すべての BIN で期待度数 E_i を 5 以上とするのは難しい．

本稿では，複合攻撃への耐性を備え，かつ上記の問題を改善した CSDM 手法を提案し，実験によりその有効性を示す．

		Feature A	
		50%	50%
Feature B	50%	25%	25%
	25%	25%	25%

(a) 一様分布の分割表

(a) Division table of uniform distribution

		Feature A	
		50%	50%
Feature B	50%	49%	1%
	50%	1%	49%

(b) 一様分布ではない分布の分割表

(b) Division table of un-uniform distribution

図 1 2 つの特徴量を用いた分割表の例

Fig. 1 An example of the division table for two features.

2.4 評価式

攻撃検知では，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．どのような攻撃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 [5] や文献 [17] 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 尺度の計算式を以下に示す．

$$F = \frac{1}{\frac{1}{2}(\frac{1}{R} + \frac{1}{P})} = \frac{2RP}{R+P} \tag{4}$$

ここで，R は再現率（Recall），P は適合率（Precision）と呼ばれる数である．攻撃を攻撃と検知した True-Positive（TP）の回数を tp，誤検知となった FP と FN の回数をそれぞれ fp，fn とすれば，$R = tp/(tp+fn)$，$P = tp/(tp+fp)$ として求めることができる．どちらも 0 から 1 の間の値をとり，1 に近いほど良い．誤検知の指標となる F 尺度もまた，0 から 1 の間の値をとり，1 に近いほど攻撃の有無の判定が正確であることを意味する．

3. 提案手法

これまでに提案された χ^2 手法 [3], [4], [14], [15], [16] において，計算に用いる確率変数は 1 種類である．しかし，パケットヘッダには IP アドレスやポート番号，パケット長，TTL，フラグなど，攻撃検知に有用と考えられるさまざまなフィールドが含まれる．χ^2 手法において，攻撃の有無を判定する精度を向上させるためには，これら複数の特徴を同時に分析することが必要となる．そこで，本稿では，2 つ以上の確率変数を同時に扱うことができる，新たな **χ^2 ベースの空間分割法**（Chi-square-based Space Division Method（**CSDM**））を提案する．

3.1 χ^2 値の計算

CSDM における χ^2 値の計算手順を以下に示す．

(a) 特徴量の数を N として，各特徴量ごとのシンボルをインデックスとする N 次元の配列を作成する．次に窓幅 W に入ったパケットについて順にシンボルを取り出し，該当する配列のセルの度数を 1 だけ増加し，同時に各特徴量ごとの総数も増加する．

(b) 窓内のすべてのパケットの集計が完了したら，ソート対象の特徴量以外の場所を保ったまま，特徴量ごとに総数でソートする．攻撃時のパケットは，送信元 IP アドレスなどのシンボルが集中か分散，どちらかの傾向がある．頻度順にソートすることで総数の多い DoS，あるいは総数が極端に少ない DDoS 攻撃などの異常なシンボルの位置が近づく．

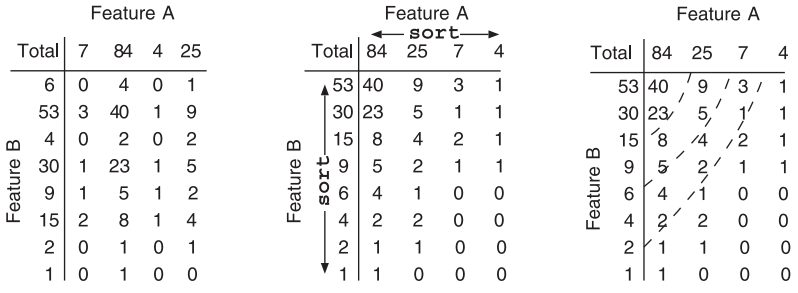
(c) 各特徴量ごとの順位から，総合的な評価値 s を決める．求めた s を基に，用意した BIN に分割する．最後に，BIN 中のパケット総数をカウントし，この値を観測度数 O_i として χ^2 値を求める．

次に，具体的な BIN への分割手順を示す．まず，パケット j の評価値 s_j を以下のように定める．

$$s_j = \sum_{k=1}^{N} \frac{r_{j,k}}{m_k} \tag{5}$$

ここで，N は使用している特徴量の数，$r_{j,k}$ は特徴量 k におけるパケット j の順位，m_k は特徴量 k のシンボル数である．$0 \le r_{j,k}/m_k \le 1$ であるため，評価値 s は $0 \le s \le N$ の範囲となる．たとえば，特徴量 A のシンボル数を 4，特徴量 B のシンボル数を 8 とし，特徴量 A におけるパケット j の順位を 2，特徴量 B の順位を 3 とすれば，評価値 $s_j = 2/4 + 3/8 = 0.875$ を得る．次に，あらかじめ定めておいた境界値 d_i を用いて，パケットを BIN へ分割する．d_i の範囲は $0 < d_i < N$ であり，$d_{i-1} < d_i$ とする．すべての評価値 s_j について，$d_{i-1} < s_j \le d_i$ となる i を求め，パケットの個数を i 番目の BIN である BIN_i へ加える．たとえば，$d_1 = 0.5$，$d_2 = 0.75$，$d_3 = 1$ であれば，s_j が 0.5 以下なら BIN_1，0.75 以下なら BIN_2，1 より大きい場合は BIN_4 が該当する BIN となる．例示した $s_j = 0.875$ は，BIN_3 となる．

これらの手順を分かりやすく図示したものが**図 2** である．図の左から順に，それぞれ計算手順の (a)，(b)，(c) を示している．図は特徴量が 2 つの場合を説明しているが，特徴量が N 個ある場合は，N 次元へと容易に拡張できる．提案手法の計算において，最も負荷が大きいのは，(b) のソートである．たとえば，N 個の特徴量を扱う場合，図 2 (b) で解説したソートを用いると，N 次元の配列の入



(a) 分割表 (b) 各特徴量でソート (c) BIN 分割

(a) Division table (b) Sort by each feature (c) BIN Division

図 2 2 つの特徴量による CSDM の計算

Fig. 2 Calculation of CSDM for two features.

れ換え作業が必要となる．そこで，パケットの持つ送信元 IP アドレスや送信先ポート番号などの特徴から，パケットを BIN へ直接配置する方法を考える．その基準となる式 (5) の s_j は，パケット j の各特徴量 k ごとの $r_{j,k}$ が分かれば計算可能である．1) まず，窓内のパケットを順に取り出しながら，各特徴量ごとのシンボルの度数を調べる．このときに必要な配列のサイズは，最大でも NW である．2) 次に，1) で得られた結果を度数順にソートして各シンボルごとに順位を決定し，シンボルをキーとした最大 W 個のデータからなる順位検索用のハッシュテーブルを N 個作成する．この段階で頻度情報の入った配列は不要となる．3) 最後に，再び窓内の W のパケットを先頭から順に取り出しながら，先ほど作成した順位検索用のハッシュテーブルを用いてシンボルの順位を $O(1)$ で調べ，式 (5) に従って N 個の $r_{j,k}$ から評価値 s_j を計算し，該当する BIN を決定する．

以上の手順によって，N 次元の配列だけでなく，配列内の膨大なデータの入換え作業がすべて不要となる．この手順に従ったときの 1 窓あたりの時間計算量は，まず 1) ではシンボルの検索にハッシュを用いており，該当シンボルを検索する時間は $O(1)$ となるので，1 窓あたりの時間計算量はパケットの数 W と特徴量の数 N の積に比例しており，$O(NW)$ となる．また 2) は，窓 W の中のシンボルの種類数の最大値を単に m（$\leq W$）とすれば，$O(N \cdot m \log m)$ 以下となる．m が W と等しくなるのは，DDoS 攻撃などのように窓内のすべてのシンボルが異なるときである．3) は W パケットから順位検索テーブルを用いて N シンボルの順位を取り出す時間と，s_j を計算する時間の合計である $O(NW+N)$ となる．これらのことから，1 窓あたりの処理に必要な時間計算量は，$O(NW+N \cdot m \log m)$ と表せる．

本稿では，第 1 の特徴量として，論文 [3] などにおいて有効とされた送信元 IP アドレス（以降 `srcip` と表記）を，また，第 2 の特徴量として，あるパケットが到達してから次のパケットが到達するまでの到達時間の差 Δt（以降 `dt-srcip` と表記）を用いる．`dt-srcip` を用いた理由は，Web アクセスや ssh，telnet などのパケットの `dt-srcip` は，人のキー操作などの場合と，攻撃の場合で特徴が異なると考えられるためである．エントロピーや χ^2 値を利用した攻撃検知手法は，通常時の `srcip` の分布がべき乗則に従っており，DoS や DDoS の `srcip` がべき乗則から外れることを利用して，攻撃を判定する．しかし，Web や telnet などのパケットがたまたま集中すると，`srcip` の観測結果は DoS 攻撃に見える．提案手法は，`dt-srcip` を加えた 2 次元平面上の分布を見ることで，単なるパケットの集中と DoS 攻撃とを区別する．

3.2 動的 BIN の提案

これまでの BIN の境界の決定方法として，通常時のパケットについて，シンボルの種類数や度数を事前に調査し，その調査した数を基に，BIN の境界値を決めておく手法（以後**固定 BIN** と表記）が用いられていた．前節で解説した CSDM でも，パケットを BIN に分割する際に必要な境界値 d_i を決めておく必要がある．しかし，χ^2 値の統計学における制約を考慮すれば，各 BIN のパケットの期待度数が 5 以上となる d_i を注意深く設定しなければならない．d_i はまた，窓幅や BIN 数，確率変数に使用した特徴量などの影響を受けるため，設定がさらに難しい．そこで，本稿ではある時刻 t における BIN_i の境界値 $d_i(t)$ を次式によって定義する（以後，この動的にする BIN 領域を**動的 BIN** と表記）．

$$d_i(t) = d_i(t-1) \cdot \left(1 - \eta \frac{\overline{p_i}(t-1) - E_i}{E_i}\right) \tag{6}$$

この式は，それぞれの BIN の中の平均パケット度数 $\overline{p_i}(t)$ を，期待度数 E_i に近づけるように，境界値 $d_i(t)$（$0 < d_i(t) < N$）をつねに変化させる．時刻 t は，窓幅の W [packet] を処理するごとに 1 つ増える値であり，1 つの窓を処理するたびに 1 度計算すればよい．したがって，動的 BIN の更新である式 (6) および後述する式 (7) の処理に必要な時間は，攻撃パケットを受信してから攻撃を検知するまでの処理遅延と比較して非常に小さい．ここで，η は $d_i(t)$ の変更係数であり，$d_i(t)$ が振動しないように 0.1 以下の小さな数に設定し，期待度数 E_i は，すべての BIN にパ

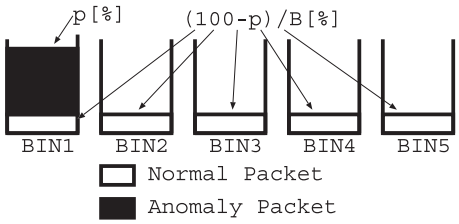


図 3 p[%] の攻撃パケット（DoS）がある場合の BIN の様子
Fig. 3 Condition of BIN within the p[%] anomaly packets (DoS).

ケットを等しく配分する定数 W/B に設定する．$\overline{p_i}(t)$ はある BIN_i のパケットの平均数であり，時刻 t における窓内のパケット数 $p_i(t)$ より以下の指数移動平均の式で求める．

$$\overline{p_i}(t) = \lambda p_i(t) + (1-\lambda)\overline{p_i}(t-1) \tag{7}$$

λ（$0 < \lambda < 1$）は指数移動平均の平滑化係数である．DoS 攻撃を受けると，多くのパケットの特徴が酷似するため，$d_i(t)$ は 0 に近づき，逆に，パケットの特徴がすべて異なる DDoS 攻撃では，$d_i(t)$ は N に近づく．

文献 [3], [14], [15] では，1 日や 1 週間といった期間で変化するトラヒック変化に対応するため，観測した過去のパケットを基に，指数移動平均により期待度数 E_i を計算する．この方法は，BIN の境界は固定であり，異なる観測データでは特徴量の数 N やシンボル数，窓幅 W，BIN 数 B などのパラメータが異なるため，BIN の境界を再計算しなければならない．一方，提案する式 (6) は，期待度数 E_i を W/B などに固定し，動的に BIN 境界 $d_i(t)$ を変化させるため，期待度数 E_i の持つべき条件を満足するだけでなく，パラメータの変更による影響を式として表している．

3.3 提案手法（CSDM）におけるしきい値

χ^2 値が最大となるのは，窓幅 W のパケットの特徴が DoS 攻撃などによってすべて同じとなり，1 つの BIN に集中して入る場合である．提案する CSDM では，$E_i = W/B = E$ と仮定しており，このとき χ^2 値の最大値 $\chi^2_{\max}$ は以下の式で表せる．

$$\chi^2_{\max} = \frac{(W-E)^2}{E} + \frac{(0-E)^2}{E} \cdot (B-1) \tag{8}$$

$\chi^2_{\max}$ は，窓幅 W や BIN 数 B，期待度数 E によって大きく変化するが，最大値が変動すれば，しきい値を一意に決定することが困難となる．そこで本稿では，χ^2 値を $\chi^2_{\max}$ で除算し区間 [0:1] に正規化した値を攻撃の判定に用いる．この正規化によって，窓幅や BIN 数によらないしきい値を設定できる．まず，窓幅 W パケットのうち p[%] が DoS 攻撃によって生じたパケットであったと仮定し，そのときの BIN の様子を**図 3** に示す．χ^2_p は，次の式となる．

$$\chi^2_p = \frac{(pW + \frac{1-p}{B} \cdot W - E)^2}{E} + \frac{\left(\frac{1-p}{B}W - E\right)^2}{E} \cdot (B-1) \tag{9}$$

この式を正規化した $\chi^2_p/\chi^2_{\max}$ は，以下の式で求めることができる．

$$\begin{aligned}
&\frac{\chi^2_p}{\chi^2_{\max}} \\
&= \frac{\left(pW + \frac{1-p}{B} \cdot W - \frac{W}{B}\right)^2 + \left(\frac{1-p}{B} \cdot W - \frac{W}{B}\right)^2 \cdot (B-1)}{\left(W - \frac{W}{B}\right)^2 + \left(\frac{W}{B}\right)^2 \cdot (B-1)} \\
&= \frac{(pB + (1-p) - 1)^2 + ((1-p) - 1)^2 \cdot (B-1)}{(B-1)^2 + (B-1)} \\
&= \frac{p^2(B-1) + p^2}{(B-1) + 1} = p^2
\end{aligned} \tag{10}$$

結果，窓幅 W や BIN 数 B によらない式が得られる．したがって，CSDM では，次の式により攻撃を判定する．

$$\chi^2_p/\chi^2_{\max} > \theta = p^2 \tag{11}$$

ここで p[%] は，発見され得る攻撃率の最小値である．つまり，異常を発見したいパケット列に p[%] の異常パケットが混入していると仮定すれば，しきい値 θ は $\theta = p^2$ に設定すればよい．

4. 実験方法と実験結果

4.1 データセット

攻撃検知に用いることができるデータセットとして，DARPA [8]，MWS [18]，CDX [11]，LBNL [6] などのデータが公開されている．MWS では，多くの種類のマルウェア攻撃パケットを含んでおり，これらの攻撃パケットを DoS や DDoS 攻撃と見なすことができるが，通常時のパケットが提供されておらず，通常パケットの中から攻撃を検知する実験目的にはそぐわない．CDX では，DoS/DDoS だけでなく，侵入やスキャン攻撃など多岐に及ぶ最新の攻撃パケットが提供されているが，攻撃を含まない学習用データセットの提供がなく，今回の BIN の境界 $d_i(t)$ を事前の学習データで決定するアルゴリズムの評価ができない．LBNL では，アプリケーションレベルでのスキャンパケットを含めて攻撃として分類している．我々は DoS/DDoS 攻撃のような IP，TCP/UDP ヘッダに攻撃の特徴が表れる攻撃を攻撃と定義しており，LBNL とは攻撃の定義が異なるため，F 尺度が計算できない．また，我々は，今後多くの特徴量を基にした実験を予定しており，パケットが匿名化された LBNL データセットは，特徴量ごとに計算した結果を比較するうえで，大きな支障となる．

そこで，本実験では DARPA1999（以降 DARPA と表記）を使用することとした．このデータは MIT によって 1999 年に作成されたものであり，データセットとしては古いが，多くの種類の攻撃を含んでいるだけでなく，攻撃パケットや通常パケットにいっさいの加工をしていない pcap ファイルとして提供される．そのため，本データセットはパケットの多くの情報を確率変数とする実験には都合が良

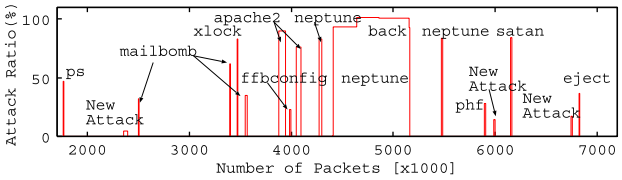


図 4 攻撃パケットの分布
Fig. 4 Distribution of attacking packets.

い．また，攻撃パケットにはすべてラベルが付与されているため，F 尺度を用いて攻撃の検知結果を客観的に評価することができる．以上の理由から，DARPA が我々の目的に最も適しており，実験で使用することとした．

4.2 実験方法

DARPA では，全部で 5 週間のデータが提供されている．今回は，この中から多くの攻撃パケットを含んでいる outside パケットを利用した．まず，第 1 週に相当する 1999 年 3 月 1 日～3 月 5 日のパケットには攻撃パケットが含まれておらず，この間のパケットを学習用として使用した．次に，3 月 29 日～4 月 2 日の第 4 週，および 4 月 5 日～4 月 9 日の第 5 週のデータについてはラベル付けされた攻撃パケットが多数含まれてる．そこで，この 2 週分のデータを攻撃検知の精度を測定する実験に使用した．

これまでの研究 [3], [10] において，窓幅を $W = 10{,}000$ とすることで，攻撃発見に効果があったとの結果が得られている．そこで，窓幅のパラメータをこの窓幅に統一して EMMM と CSDM を比較する．さらに，CSDM においては，$B = 5$，$\eta = 0.05$，$\lambda = 0.2$ とした．確率変数の種類や窓幅によって EMMM や CSDM の最大値が大きく変動することから，本稿では EMMM と CSDM の結果は，すべて最大値を 1 とする区間 [0:1] に正規化して表示する．

4.3 実験結果

DARPA の攻撃パケットのラベルに基づき，データセット中の攻撃パケットをグラフにしたものを**図 4** に示す．縦軸は通常パケットの中に含まれていた攻撃パケットの割合を窓ごとに計算したものである．DARPA の攻撃パケット数は数十から数万と幅広く，また 200 もの攻撃が含まれている．本稿では攻撃パケットの総数が 2,000 以上となった 19 個のラベルの攻撃を検出対象とした．EMMM や CSDM の窓幅を $W = 10{,}000$ としており，パケット数が 2,000 以下の攻撃は窓内の攻撃パケットの割合が 20%以下となるため，今回の攻撃検知の対象から外した．

4.3.1 単一の攻撃による実験結果

図 5 および**図 6** に，`srcip` を基に計算した EMMM と CSDM の計算結果を示した．各図において，1) `srcip` のみ，2) `dt-srcip` のみ，3) `srcip` と `dt-srcip` の両方，の計 3 通りの実験結果を示している．EMMM，CSDM いずれにおいても apache2 や neptune といった攻撃パケットを検知している．その一方で，mailbomb のようなアプリケーションレベルの攻撃は検知されなかった．これは，mailbomb が通常の SMTP パケットシーケンスと似ており，統計的な攻撃検知では発見困難なことを示している．また，異常パケットがまったくない場所において，EMMM や CSDM が増加している箇所は，ユーザの行動によって ssh や telnet，さらには ftp のファイルコピーパケットが集中したところであった．

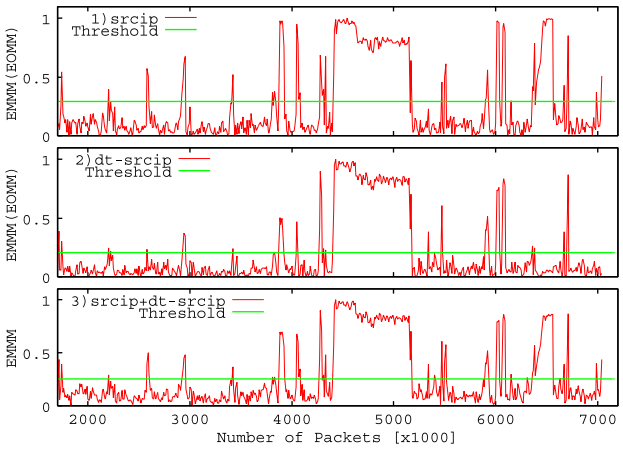


図 5 送信元 IP アドレスを対象にした EMMM
Fig. 5 EMMM for the source IP address.

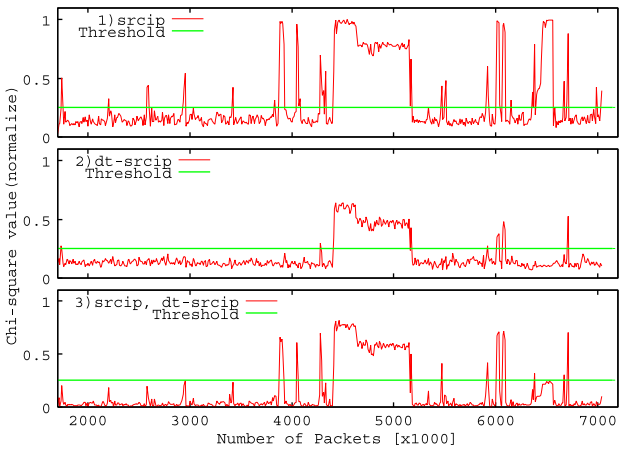


図 6 送信元 IP アドレスを対象にした CSDM
Fig. 6 CSDM for the source IP address.

表 2 に，EMMM と CSDM の検出精度を測定した結果を示す．それぞれの実験では，F 尺度が最大となるようなしきい値を設定した．表より，EMMM においては，`dt-srcip` の値が最も良く，`srcip+dt-srcip` では F 尺度は低下する．この低下の原因は，確率変数を差分時間としたことでシンボルの種類が多くなり，エントロピーの変動が大きくなりすぎたためである．エントロピーがたまたま大きくなった箇所は FP としてカウントされるため，その結果，F 尺度は低下する．近隣のシンボルをまとめてカウントするなどの工夫が必要である．一方，CSDM において

表 2 送信元 IP アドレスを対象とした EMMM と CSDM による判定結果
Table 2 Metric values of EMMM and CSDM for the source IP address.

Random variable	EMMM					CSDM				
	fp	fn	R	P	F	fp	fn	R	P	F
1) srcip	52	9	0.904	0.620	0.736	56	8	0.915	0.606	0.729
2) dt-srcip	31	12	0.872	0.726	0.792	10	19	0.798	0.882	0.838
3) both	58	7	0.926	0.600	0.728	13	12	0.872	0.863	0.868

は，srcip と dt-srcip それぞれを独立変数とした場合より，srcip+dt-srcip の F 尺度が改善されていることが分かる．この要因は FP が大きく減少したことによる．時間差分の情報を同時に用いることで，srcip のみの分析では集中していた telnet や ssh パケットが分散し，攻撃か否かの正しい判定が可能となった．

EMMM や CSDM では，確率変数が持つ関連性の扱いにも違いがある．たとえば，srcip と dt-srcip におけるエントロピーから EMMM を求める際，1 パケットあたりの srcip と dt-srcip の関連はいったん断ち切られてエントロピーの計算に利用されるのに対し，CSDM では，1 パケットの関連性を保ったまま 2 次元空間にパケットを配置し異常を判定する．パケットの関連性を利用する CSDM は，EMMM に比べて攻撃の判定に有利である．

4.3.2 複合攻撃による実験結果

複合攻撃は，DARPA にはほとんど含まれていない．そこで，DARPA を基に，攻撃が加わっている時間帯において，パケットの一部を，人為的に別の攻撃パケットの特徴に変更することで 2 重攻撃を生成する．具体的には，DARPA の攻撃データに対して，ある一定の割合で DoS 攻撃の特徴となる IP アドレスおよび時間間隔を同一のものに書き換えた（以降ではこの書き換えたパケットを **2nd 攻撃**と表記）．この 2nd 攻撃により，DARPA に含まれるオリジナルの攻撃に，さらに DoS 攻撃が複合的に加わったと見なすことができる．2nd 攻撃の割合を 0%から 30%まで変化させ，F 尺度を測定した．EMMM や従来の χ^2 手法の F 尺度と提案手法を比較した結果を**図 7** に示す．1) は EMMM，2)，3) は CSDM による F 尺度である．1)，2)，3) はいずれも，srcip と dt-srcip の 2 つの統計量を用いた．また，2) は動的 BIN を用いて，つねに式 (6) により BIN の境界を調整した場合の実験結果であり，3) は通常時のパケットで式 (6) の学習をした後，動的 BIN の学習を停止して攻撃検知を試みた．4)，5) は，固定 BIN を用いた従来の χ^2 手法に基づいて，srcip および dt-srcip より χ^2 値を計算した．

まず，確率変数を 2 つ用いた EMMM と CSDM について比較する．図 7 の 1) と 2)，3) のグラフを比較すると，CSDM の F 尺度が EMMM より高いことが分かる．特に，25%以上の 2nd 攻撃を加えた場合，EMMM の F 尺度は急激に低下するのに対し，CSDM ではそれほど F 尺度は低下しなかった．さらに 1) と 2) を見ると，2nd 攻撃の率が 0%では F 尺度の開きは少ないが，2nd 攻撃の率が上昇するに従って，差が開いていくことが確認できた．この実験結果より，CSDM は EMMM と比較して 2 重攻撃に対する攻撃の有無の判定精度が高い．これは χ^2 値の複合攻撃を発見する特徴を CSDM が有するためである．次に，従来の χ^2 手法と CSDM を比較する．図 7 の 2)，3) は CSDM であり，4)，5) は独立変数を単独で用いた従来手法である．結果，2) の CSDM 手法は 4) と比較して F 尺度が改善されており，また 3) の CSDM の手法は，4)，5) と比較して F 尺度が改善されている．

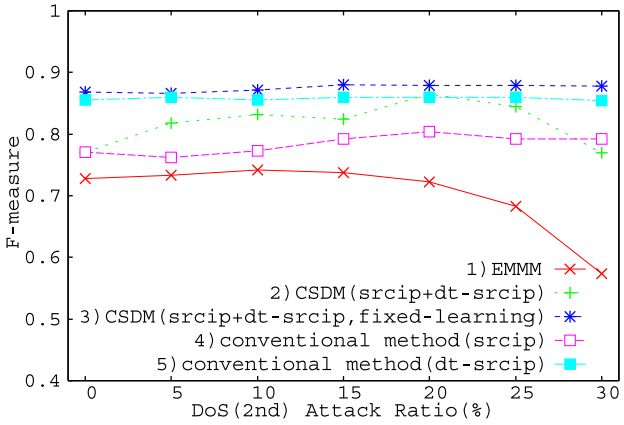


図 7 2 重攻撃を加えたときの F 尺度
Fig. 7 F-measure for duplex attacks.

また，図 7 の 2)，3) より，学習データと攻撃検知データを分離させた 3) の F 尺度が高くなる．これは，学習機能を有効にしたまま攻撃を判定した 2) において，攻撃そのものを学習したことで，TN が減少し，FP が増加したためである．攻撃を学習したことで，攻撃直後の異常判定において，本来は攻撃でないものを攻撃と判定していた．この実験から，学習データを分離し，学習データで決定した動的 BIN をそのまま利用した手法が有効であることが分かった．しかし，昼夜のトラヒックに対応させるためには，学習をつねに有効にしておかなければならず，その場合は η などの学習パラメータを小さく設定するなどして対応することが可能である．この学習に関する実験や検証は，別の論文として報告したい．

次に，3 重の攻撃を加えたデータを用いて，CSDM における F 尺度を評価した．具体的には，図 7 と同様に，DARPA の DoS や DDoS 攻撃が加わっている部分のパケッ

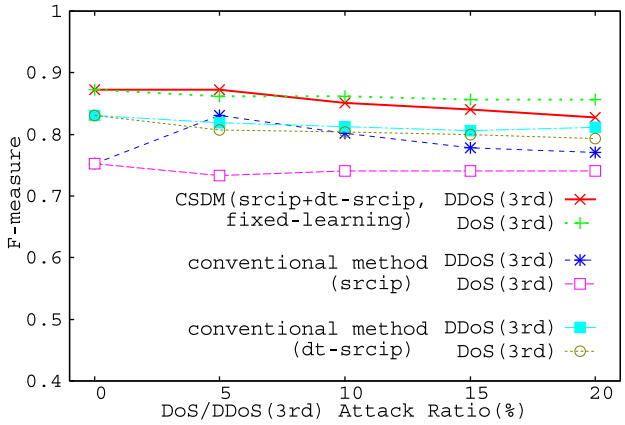


図 8 3 重攻撃を加えたときの F 尺度
Fig. 8 F-measure for triple attacks.

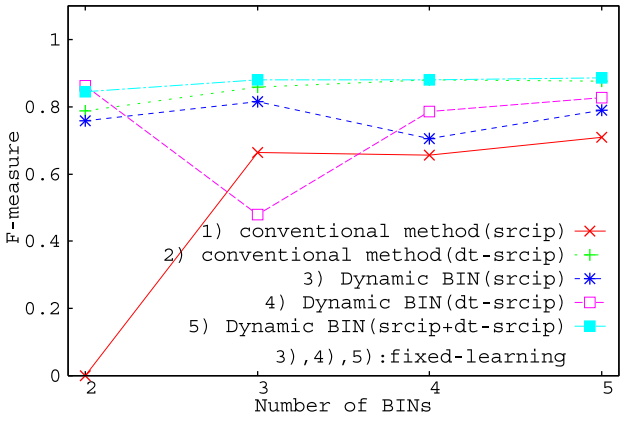


図 9 動的 BIN と静的 BIN の F 尺度の変化
Fig. 9 Variation of F-measure between dynamic BIN and static BIN.

トを，20%の割合で DoS 攻撃に変更し，2 つ目の DoS 攻撃と見なし（2nd 攻撃），さらに，残った 80%のパケットに対して，0%から最大 20%の割合で 3 つ目の攻撃と見なした DoS もしくは DDoS 攻撃に書き換えた（以降では **3rd 攻撃**と表記）．攻撃サイズは，図 7 と比較できるように，2nd 攻撃 20%に 3rd 攻撃を 20%加えた合計 40%とした．また，DDoS を 3rd 攻撃でのみ付加した理由は，本来，DDoS 攻撃自体が多重攻撃の特性を持っており，DDoS を 2 つ以上加えたパケットの `srcip` の特徴は DDoS を 1 つ加えた場合とほぼ同等となるためである．CSDM の計算値も DDoS の個数によらずほぼ同じ値となるため，本実験は 3 重 DoS，もしくは 2 重 DoS に DDoS を 2 つまたはそれ以上加えたパターンに対応していると考えることができる．

DARPA に存在する攻撃に，新たに 2 つの攻撃を加えた 3 重の攻撃データについて CSDM を用いて攻撃検知の評価をし，F 尺度を求めた結果を**図 8** に示す．実験の結果，3 重の攻撃を加えた場合の F 尺度は，3rd 攻撃の率を増加させたすべての場合において，2 重の攻撃を加えたときと同様に，高い値をほぼ維持した．このことから，χ^2 値が持つ複合攻撃への耐性を CSDM が引き継いでおり，さらに，手案手法は BIN への適切な分配によりつねに高い χ^2 値を示した．

4.3.3 BIN 境界アルゴリズムの評価

本節では，動的 BIN の有用性を確認する．**図 9** に，固定 BIN を用いた場合と動的 BIN を用いた場合のそれぞれについて，BIN 数を 2 から 5 まで変化させたときの F 尺度を示す．図の 1) と 2) のグラフは固定 BIN であり，あらかじめ調べたシンボル数を基に，各 BIN のパケットがほぼ等しくなるよう，べき乗則に沿って BIN の領域を決定している．また，3)，4)，5) は，学習データで動的 BIN の領域を決定し，そのまま BIN を変化させずに攻撃検知を行った．1)–4) は単一の確率変数を使用したものであり，5) は 2 つの確率変数を用いた CSDM に，動的 BIN を適用している．1) と 3) の結果より，`srcip` の場合は，固定 BIN の F 尺度より動的 BIN の F 尺度が全体的に F 尺度が大きいことが確認された．固定 BIN は，特に BIN 数を 2 としたときの F 尺度が小さい．`srcip` のシンボル数を調査したところ，通常パケットには 29 種類のシンボルが含まれており，この値を基に $\mathrm{BIN}_1 = 9$，$\mathrm{BIN}_2 = 20$ とした．しかし，局所的な窓 $W = 10{,}000$ に入るパケットの実際のシンボルは平均して 11 種類と少なく，BIN_1 にほとんどのパケットが入ってしまった．DoS 攻撃時にも χ^2 の値が異常を検知できず，TP がゼロとなったことで F 尺度は低下した．この BIN のパケットの偏りは BIN 数が少ないほど影響が大きい．一方，`dt-srcip` の 2) と 4) を比較すると，固定 BIN の方は，若干 F 尺度が大きい．これは，事前調査によって `dt-srcip` のシンボル数が 92 種類と BIN に分割するのに十分な数が確保できており，かつ，窓に入ったパケットのシンボルが，事前調査と同じ 92 種類とほぼ等しくなったためである．本来予定した数のパケットが固定 BIN に割り当てられた結果，F 尺度が上昇した．時間に関した確率変数では，その値のバラツキが大きく，種類も多くなるため固定 BIN においても有効に機能する．しかし，パケットヘッダの値については，バラツキは限定しており，さらに総数も組織によっては少ない可能性があるため，時間を考慮した総合的な評価が必要である．それを示したのが，図 9 の 5) であり，最も高い F 尺度を示した．このことから 2 つの確率変数を使用した場合でも，動的 BIN の式 (6) から適切に計算されており，動的 BIN の有用性が示された．

4.3.4 異常検知までの待機遅延と処理遅延の評価

パケットを受信してから異常を検知するまでの待機遅延や処理遅延は提案手法の実用性を左右する．そこで，本項ではこれらについて述べておく．

ここでは DARPA を使用して異常パケットを受信してから計算を開始するまでの時間を評価する．まず，DARPA では，攻撃の区間は明確に決まっており，この間のパケット数の合計を攻撃時間の合計で割った攻撃時のパケット

表 3 提案手法（CSDM）の処理遅延
Table 3 Processing delay of the proposed method (CSDM).

	時間 [sec]					
	$N=1$		$N=2$		$N=4$	
窓幅 W	Total	Delay	Total	Delay	Total	Delay
1,000	266.07	0.038	520.44	0.074	1034.36	0.147
2,000	263.15	0.075	514.88	0.146	1011.62	0.287
5,000	262.42	0.186	508.72	0.360	1011.39	0.287
10,000	262.71	0.372	504.00	0.714	1017.47	1.442

Total：全パケットの処理時間
Delay：1 窓あたりの処理遅延

平均流量は 615 [packets/sec] であった．CSDM では，窓に W 個のパケットが溜まってから計算を開始するため，計算開始までの待機遅延は，窓幅 $W = 2{,}000$ で 3.25 [sec]，$W = 10{,}000$ で 16.3 [sec] となる．DARPA が作成された 1999 年当時と現在の回線速度を比較すると，2–3 桁以上のオーダで高速化されており，したがって現在の回線速度を最大限に利用した攻撃はデータ量も増えているため，窓にパケットがすぐ溜まることが予想される．これにより待機遅延は 2–3 桁少ないオーダであり，たかだか 1 秒程度と考えられる．このように攻撃が強くデータ量が多くなれば，待機遅延は短くなる．

次に，DARPA データを用いて，実際の処理時間を調査した．計算に使用した PC スペックは，AMD Sempron(TM) 2800+, Main Memory 1 GB であり，OS として Vine Linux 4.2 を使用している．処理プログラムはすべて perl 5.8.6 でフィルタとして記述しており，tcpdump の出力するテキストデータから CSDM の χ^2 値を求めるまでをシェルのパイプにより処理した．DARPA では，学習用の第 1 週のデータと攻撃検知用の第 4 週・第 5 週の計 3 週間で，計 7,057,960 個のパケットが観測されている．ここで動的 BIN の更新まで含めた CSDM における全パケットの処理時間，および 1 窓あたりの処理遅延を調査した結果を**表 3** に示す．

結果から，同一の N について，全体の処理時間は窓幅 W に依存せずほぼ一定であり，1 窓あたりの処理遅延は W にほぼ比例しており，また，全体の処理時間は N にほぼ比例したことから，時間計算量の正統性を確認することができた．さらに，たとえば，1 窓あたりの処理遅延は $N = 2$，$W = 2{,}000$ では 0.146 [sec]，$N = 2$，$W = 10{,}000$ では 0.714 [sec] であった．これらのことから，perl スクリプトとパイプで記述したプログラムは，処理遅延がたかだか数秒程度であり，また，$N = 2$，$W = 10{,}000$ において，1 秒あたり $1/0.714 = 1.40$ 回の計算が可能であることから，1 秒あたり 1.4 万 [packets] を計算する能力を有している．Perl で費した時間の大部分は，tcpdump の出力するテキストデータから IP アドレスやポート番号などのフィールドを取り出す処理であり，C 言語を用いてパケットのバイナリデータを直接取得するように実装すれば，おそらく 1 桁以上の処理の高速化が望める．

5. おわりに

本稿では，従来の χ^2 手法を拡張し，多数の確率変数から総合的に攻撃を検知する CSDM 手法を提案した．次に，送信元 IP アドレスと差分時間を確率変数とする攻撃検知において，従来の χ^2 手法および EMMM と提案手法とを比較し，F 尺度により精度を評価した．

実験結果から，CSDM では，EMMM と同様に neptune や satan といった攻撃の判定が可能であった．しかし，mailbomb のようなアプリケーションレベルでの攻撃パケットの検知は困難であった．EMMM は，`srcip` や `dstport` が集中する傾向がある ftp や telnet，ssh といった通常のパケット列において，攻撃と判定する傾向があるが，CSDM では各パケットから取り出した確率変数の関連性を保ったことで，telnet など一部の FP が減少し，F 尺度が改善された．これらのことから，CSDM は，EMMM と比較して多数の確率変数から統計値を求める際に有効であり，差分時間に対しても有効である．また，各種条件を同じとする EMMM と CSDM の攻撃判定において，2 つの確率変数を用いた実験の結果，CSDM が F 尺度が大きく，性能が良いことが分かった．さらに，攻撃が 3 重となった場合においても，CSDM の性能がほぼ維持されることを確認した．今回，2 重 DoS 攻撃，3 重 DoS 攻撃，2 重 DoS 攻撃+DDoS 攻撃を加えた場合について提案手法を評価したことで，EMMM および従来の χ^2 手法と比較して，多くの攻撃パターンにおいて提案手法が有用であることを確認した．しかしながら，複合攻撃の組合せはこれ以外にも多数あり，また，実際の環境では 4 重以上の攻撃もありうるため，4 重以上の攻撃を受けた場合の評価については，今後の検討課題としたい．

次に，動的 BIN と固定 BIN を比較する実験の結果，動的 BIN による 2 つの確率変数を用いた CSDM において，あらゆる BIN 数で最大の F 値となった．このことから，CSDM のように複数の確率変数を使用し，多くの種類のシンボルが観測される場合において，動的 BIN が有効に機能していることが確認された．

また，処理時間を測定する実験の結果，1 窓あたりの処理遅延は窓幅 W にほぼ比例しており，1 窓あたりの処理遅延と全パケットの処理時間は，特徴量の数 N にほぼ比例していることが確認された．結論として，最初の攻撃パケットが観測されてから攻撃を検知するまでの待機遅延と処理遅延はいずれもたかだか数秒程度であり，実用的な時間で終了する．

最後に，本手法は，多くの特徴量，たとえばパケット長や TTL，フラグといった情報を確率変数として利用することが可能である．今後の課題として，これらを確率変数とする CSDM の有効性の検証を考えている．特に，我々は

差分時間を用いた際の χ^2 値の挙動に着目しており，今後検証していきたい．

参考文献

[1] 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).

[2] Falutsos, M., Faloutsos, P. and Faloutsos, C.: On Power-Law Relationships of the Internet Topology, *Proc. ACM SIGCOMM*, pp.251–262 (1999).

[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] Goonatilake, R., Herath, A., Herath, S., Herath, S. and Herath, J.: Intrusion Detection using the Chi-Square Goodness-of-Fit Test for Information Assurance, Network, Forensics and Software Security, *Papers of the 14th Annual CCSC Midwestern Conference and Papers of the 16th Annual CCSC Rocky Mountain Conference*, Vol.23, No.1, pp.255–263 (2007).

[5] 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).

[6] LBNL: LBNL/ICSI Dataset, available from ⟨http://www.icir.org/enterprise-tracing/download.html⟩.

[7] 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).

[8] MIT: DARPA Intrusion Detection Evaluation Data Set, available from ⟨http://www.ll.mit.edu/mission/communications/ist/index.html⟩.

[9] 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).

[10] Oshima, S., Nakashima, T. and Sueyoshi, T.: Anomaly Detection using Chi-Square Values based on the Typical Features and the Time Deviation, *25th International Conference on Advanced Information Networking and Applications* (*AINA2011*), pp.97–104 (2011).

[11] 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 (2009).

[12] 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).

[13] 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).

[14] Ye, N. and Chen, Q.: An Anomaly Detection Technique Based on a Chi-Square Statistic for Detecting Intrusions into Information Systems, *Quality and Reliability Engineering International*, Vol.17, pp.105–112 (2001).

[15] Ye, N., Emran, S.M., Chen, Q. and Vilbert, S.: Multivariate Statistical Analysis of Audit Trails for Host-Based Intrusion Detection, *IEEE Trans. Computers*, Vol.51, No.7, pp.810–820 (2002).

[16] Zhou, B., Shi, Q. and Merabti, M.: Intrusion Detection in Pervasive Networks Based on a Chi-Square Statistic Test, *Proc. 30th Annual International Computer Software and Applications Conference* (*COMPSAC'06*), Chicago, Illinois, pp.203–208 (2006).

[17] 小島俊輔，中嶋卓雄，末吉敏則：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，情報処理学会論文誌，Vol.52, No.2, pp.656–668 (2011).

[18] 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).

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 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．