スケッチおよびガンマ関数モデルを用いたインターネットトラフィック異常検出アルゴリズムの性能評価と最適化

肥村洋輔 [1]　福田健介 [2]　長健二朗 [3]　江崎浩 [1]

東京大学 [1]　国立情報学研究所 [2]　IIJ 研究所 [3]

概 要

本研究では，異常検出手法の統一的な評価を行うためのフレームワークを提供するための第一歩として，異常トラフィック検出手法のひとつである“スケッチおよびガンマ関数を用いた異常検出アルゴリズム”のパラメータ最適化および性能評価を行う．このアルゴリズムの基本的な考え方は，次の通りである：(1) トラヒックをスケッチ（ハッシュ関数の組み合わせ）によってフローに分解する，(2) 各フローの単位時間あたりのパケット到着数をガンマ分布で近似する，(3) ガンマ分布が要求する 2 つのパラメータ α，β について，他のフローと著しく異なるパラメータ値を持つフローを異常フロー源とみなす．評価用データセットには，WIDE プロジェクトが提供する国際線のパケットトレースのうち，2006 年 03 月分および 2007 年 09 月分を用いた．データセットに含まれる攻撃パターンを調べたところ，2006 年 03 月は SYN フラッディングが多く，2007 年 09 月は PING スキャンが多いことがわかった．パラメータ最適化にあたっては，検出率が最大となるパラメータを最適値として採用し，性能評価には ROC 曲線を用いた．その結果，要求するパラメータのうち，タイムウィンドウ T_{win}（データ処理を行うトラフィック時間長），α についての閾値 λ_α および β についての閾値 λ_β については，データセットによる依存性が確認された．

1　はじめに

1.1　背景と目的

インターネットが必要不可欠な社会インフラへと成長するに伴い，インターネットを介した脅威も増加し，充実したセキュリティ機能が求められるようになった．セキュリティ機能の一例として，インターネットにおける異常トラフィック検出がある．この機能は，DDoS 攻撃に代表される悪意のあるトラフィックを検出し，エンドホストの保護を行う．本研究ではこの異常検出に注目し，統計処理によって異常検出を行うアノマリ型異常検出手法に焦点をあてる．この手法は，広帯域トラフィックにおける異常検出に適している．

現在，広帯域トラフィック異常検出は，短時間に大量のパケットを処理する必要があるため，難しい技術課題とされている．こうした技術課題を解決するために，高効率・高精度で異常検出を行う手法の研究開発が行われている．しかし，多くの研究においては手法の提案に主眼が置かれており，統一的な性能評価が行われていない．さらに，信頼性の高い性能評価は難しいトピックである．なぜならば，(1) 異常をいかに定義するかという問題，(2) 評価用データセットに含まれている異常が全てわかるわけではないという問題 などがあるためである．

本研究では，統一的な性能評価を行うフレームワークを提供することを目標とする．この目標を達成するためには，異なる検出手法を同一のデータセットを用いて公平に評価する必要がある．公平な評価ためには，それぞれの手法のパラメータの最適化を行った上で，同一の評価基準を用いて評価を行うことが求められる．

本論文では目標達成の第一歩として，特定の異常検出手法を用いてパラメータの最適化方法と評価基準の設定方法について検討を行う．用いた異常検出手法は，Dewaele らが提案する“スケッチおよびガンマ関数モデルを用いた異常検出アルゴリズム”[4] である．評価用のデータセットとして，WIDE プロジェクトが運用する国際線のパケットトレースを用いた．その結果，

統一的な評価のための一定の指標を得ることができた．

2 関連研究

異常検出手法として，シグニチャ型とアノマリ型がよく知られている．

- シグニチャ型: 異常トラフィックを構成するパケットの特徴をルール化・データベース化し，パターンマッチによって異常検出を行う方法である．その代表例として snort[7] がある．
- アノマリ型: 数理的なモデルを用いて正常なトラフィックの特徴をルール化し，ルールを満たさないトラフィックを異常とみなす方法である．

本研究で対象とするアルゴリズムは，アノマリ型異常検出手法である．関連研究の代表例として以下のものが挙げられる．

(a) ホルトウィンタース法: ホルトウィンタース法とは，時系列データの予測方法のひとつで，観測データを定常成分・直線成分・周期成分に分解し，各々の成分について予測を行う手法である．周期性のあるデータに対して，効率的に予測を行うことができる．Brutlag は，この手法による予測値から外れたトラフィックを異常であると定義し，異常検出を行っている [2].

(b) ウェーブレット変換法: ウェーブレット変換とは，時間スケールの情報を保持しつつ周波数解析を行う手法である．Barford らは，この手法を用いて，トラフィックの時系列データを，高周波・中周波・低周波に分解し，持続時間の異なる異常を分離して検出している [1].

(c) 主成分分析法: 主成分分析とは，データマイニング手法のひとつで，多変数のデータを少数の合成変数 (主成分) で表す手法である．Lakhina らはこの手法を用いて，トラフィックを主成分と残差成分に分解し，残差成分に注目し異常検出を行っている [6].

現在，これらの手法は実用には至っていない．その理由として，以下の事項が挙げられる．

- 高性能検出の難しさ: 広帯域トラフィック異常検出のためには，高速な処理を必要とするため，パケット数や IP アドレスといった限られた情報から異常検出を行う必要がある．一般的に，検出精度と処理速度はトレードオフの関係があり，両者を兼ねそろえた手法を考案することは難しい．
- 手法の評価の難しさ: 厳密な評価を行うための評価用データセットには，含まれている異常が全て分かっている必要があるが，内在する異常を全て把握することは難しく，また，異常の定義によってその情報が変化してしまう．現在，多くの研究者が行っている評価は各自が用意したデータで行われており，それらのデータは各自が定めた基準を用いてラベル付けがされている．従って，評価に厳密な一貫性がなく，普遍的な性能比較が行われない．

本論文で焦点をあてる手法は，“スケッチおよびガンマ関数モデルを用いた異常検出アルゴリズム”である．この手法に焦点をあてた理由は，以下のふたつである．

- 技術的優位性がある: (a) および (b) の手法では異常をもたらしているフロー源を特定することができず，(c) の手法ではマルチスケールにおける異常検出を行うことができない．本手法は，このふたつの課題を達成できている．
- プログラムの利用が可能である: 本手法は，本研究における共同研究者によって提案され，既に実装されている．そのため，プログラムの実行・修正が容易に行え，また，プログラムの詳細情報を手に入れることができる．

3 アルゴリズム解説

この章では，アルゴリズムの流れについて説明し，設定が必要となるパラメータをまとめる．なお，本論文におけるフローの定義を，“同一の送信元 IP アドレスを持つパケット群”と定義する．これは，あるホストから送信されるパケット全体を意味する．

3.1 アルゴリズム概要

本アルゴリズムは，以下に示す 7 ステップに分けられる．図 1 は，ステップ 1 からステップ 5 までをまとめたものである．

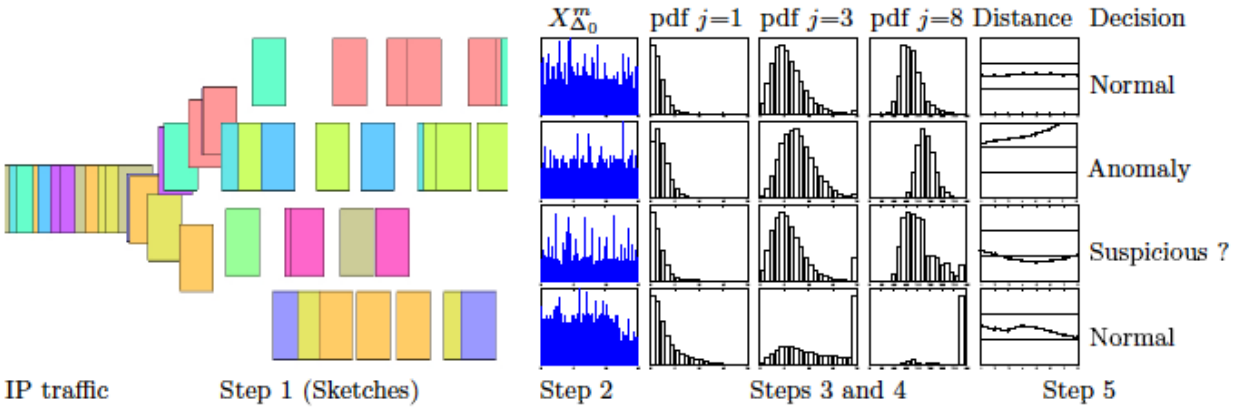

図 1: アルゴリズム概要

0. 処理データの切り出し: 前処理として，トラフィックのデータを処理しやすいデータに分割する．本論文では，全体で T 秒のデータを，T_{win} 秒ずつのデータに分割する．この T_{win} を，ウィンドウサイズやタイムウィンドウなどと呼ぶ．
1. スケッチによるトラフィック分割: スケッチを用いて，トラフィックをフローに擬似的に分割する．スケッチとは，小さなサイズのハッシュテーブルを持つハッシュ関数を複数個組み合わせ，非常に大きなサイズのハッシュテーブルを持つハッシュ関数を擬似的に作り出す手法である [4]．ハッシュ関数を $h_n(n \in 1, 2, \ldots, N)$，出力の値を $m(1 \leq m \leq M)$ とする．各々のハッシュ関数について，処理対象のトラフィックデータを送信元 IP アドレスをキーにしたハッシュ関数を用いてサブ集合に分割する．
2. 多重分解能集約: スケッチによって分割されたデータを，$\Delta_j(j = 0, 1, \ldots, J)$ を単位時間にして集約する．集約されたデータを，$X^{n,m}_{\Delta_j}(t)$ と表す．
3. ガンマ関数モデリング: $X^{n,m}_{\Delta_j}(t)$ のヒストグラムを作成し，ガンマ分布 $\Gamma_{\alpha,\beta}(x) = \frac{1}{\beta\Gamma(\alpha)}(\frac{x}{\beta})^{\alpha-1}\exp(-\frac{x}{\beta})$ に近似する．ガンマ分布は，α と β の 2 つのパラメータによって決定される．$X^{n,m}_{\Delta_j}(t)$ のヒストグラムを最もよく近似するパラメータの組を，$(\alpha^{n,m}_{\Delta_j}, \beta^{n,m}_{\Delta_j})$ とする．
4. リファレンス: 各々のハッシュ関数について，$\alpha^{n,m}_{\Delta_j}$ の平均値 $\alpha^{n,R}_{\Delta_j} = \langle\alpha^{n,m}_{\Delta_j}\rangle_m$ および分散 $\sigma^2_{m,\alpha,\Delta_j} = \langle\langle\alpha^{n,m}_{\Delta_j}\rangle\rangle_m$ を計算する．β についても同様である．
5. マハラノビス距離の計算: Δ_j について，マハラノビス距離を計算する．α についてのマハラノビス距離は，$(D_{\alpha^{n,m}})^2 = \frac{1}{J}\Sigma_{j=1}^{J}\frac{(\alpha^{n,m}_{\Delta_j} - \alpha^{m,R}_{\Delta_j})^2}{\sigma^2_{m,\alpha,\Delta_j}}$ という式で与えられる．ここで，閾値 λ_α を導入する．$D_{\alpha^{n,m}} \leq \lambda_\alpha$ であれば，$X^{n,m}_{\Delta_j}(t)$ は正常であるとみなし，$D_{\alpha^{n,m}} \geq \lambda_\alpha$ であれば，$X^{n,m}_{\Delta_j}(t)$ は異常であるとみなす．β についても同様である．
6. スケッチによる異常要素判定: 異常トラフィックをもたらしているフロー源を特定する．ある送信元 IP アドレスについて，全てのハッシュ関数による射影先が，異常とみなされたサブ集合であれば，そのフローは異常フロー源である．これを，全ての IP アドレスについて行うことで，異常トラフィックを構成するフロー源が全て特定される．なお，一定値以上のパケット数 (以降，最低パケット数と呼ぶ) を持つフローのみを特定対象とする．

3.2 必要パラメータ

本アルゴリズムに要求されるパラメータを以下に示す．なお，括弧の中に示す数値は，初期設定値である．

- T_{win}: タイムウィンドウ (60 秒)
- N: ハッシュ関数の個数 (8 個)
- M: ハッシュテーブルの大きさ (32)
- Δ_0: 基本集約時間 (5 ミリ秒)
- Δ_j の取り方 $(\Delta_0 \times 2^j (j = 1, 2, \ldots, 5))$
- λ_α: α についての閾値 (1.7)

- λ_β: β についての閾値 (初期設定では β による検出は行わない)
- 最低パケット数 (10000 個)

4 性能評価方法

4.1 MAWI データベース

本研究では，WIDE プロジェクトが運用する国際線のトラフィックデータ [3] を用いる．このデータは，日本・アメリカ間の学際的なネットワークのトラフィックを，2001 年から毎日 14 時から 15 分間，tcpdump によってキャプチャした pcap トレースである．プライバシー保護のため，パケットのペイロード部分を除去し，IP アドレスをスクランブルしている．

本研究で用いたデータは，2006 年 03 月（帯域 18Mbps），2007 年 09 月（帯域 180Mbps）の 4 週間分のデータである．サイズはそれぞれ 15.4Gbyte, 44.6GByte である．表 1 に，データの基本的な統計情報を示す．なお，2006 年 03 月の時点ではリンクはほぼ輻輳状態にあり，2006 年 07 月にリンク帯域の増強が行われた．

4.2 フロー分別

検出されたフローが害のあるフローであるかを調べることは，異常検出手法の性能評価を行うにあたって必要である．本研究では，パケットヘッダによる経験的なフロー分別手法を用いた．この手法は，フローに関して様々な経験的なルールを定義することにより，フローを以下の 6 カテゴリに分別する．

- Attack: 対象のホストから攻撃が行われていると判断されたフローである．例えば，SYN フラグの立っているパケットが 20%以上含まれていた時，このフローを“SYN フラッディング攻撃”のフローであるとみなす．
- Victim: 対象のホストが攻撃を受けていると判断されたフローである．例えば，SYN/ACK フラグの立っているパケットが 20%以上含まれていた時，このフローを“SYN フラッディング被害”のフローであるとみなす．
- OK: 害がないと判断されたフローである．HTTP サーバからの WEB トラフィックなどが該当する．
- Warning: 異常とも正常とも言い切れないフローである．HTTP サーバへの大量のリクエストなどが該当する．
- Special: 特定のアプリケーションによる通信であると判断されたフローである．例えば，53 番ポートを多く使うフローは“DNS”であり，6881 番ポートから 6889 番ポートまでを多く使うフローは“BitTorrent”であると分別する．
- Unknown: 上記 5 カテゴリのいずれにも該当しなかったフローを Unknown フローとする．

以降，攻撃カテゴリおよび被害カテゴリを合わせて，異常カテゴリと呼ぶ．

4.3 最適パラメータ設定と性能評価

本研究で評価したパラメータは，以下に示す 5 つである．

- 最低パケット数
- タイムウィンドウ T_{win}
- 基本集約時間 Δ_0
- α についての閾値 λ_α
- β についての閾値 λ_β

最適化にあたっては，パラメータが独立であると仮定し，ひとつのパラメータを変化させ（他のパラメータは初期設定値を用いる），異常カテゴリの検出率を調べる．検出率が最も高くなる時のパラメータを，最適パラメータであるとする．最後に，最適パラメータを組み合わせ，性能評価を行う．性能とは検出率および処理時間 を指す．

5 性能評価

5.1 最低パケット数の評価

図 2 は，最低パケット数を変化させた時の検出フローの依存性を調べたものである．(a)，(c) は 2006 年 03 月のデータ，(b)，(d) は 2007 年 09 月のデータである．(a)，(b) は検出フロー数を表し，(c)，(d) は各カテゴリの割合を表す．

表 1: MAWI データベースの基本統計情報（15 分の pcap トレース）

	方向	リンク帯域	パケットレート	ビットレート	ユニークなアドレスの数	
					送信元アドレス	宛先アドレス
2006 年 03 月	日本→アメリカ	18 MBps	3.89 Kpps	12.7 Mbps	1.46×10^5	1.87×10^5
	アメリカ→日本	18 Mbps	4.98 Kpps	15.2 Mbps	2.47×10^4	2.47×10^4
2007 年 10 月	日本→アメリカ	150 Mbps	10.2 Kpps	55.3 Mbps	2.39×10^4	1.02×10^5
	アメリカ→日本	150 Mbps	15.0 Kpps	78.7 Mbps	6.24×10^4	6.24×10^4

両者のデータにおいて，異常カテゴリの割合は，最低パケット数に対して依存性が小さい．従って，検出したいフローの絶対数に応じて決定できると考えられる．ここでは，10000 を最適値として採用する．

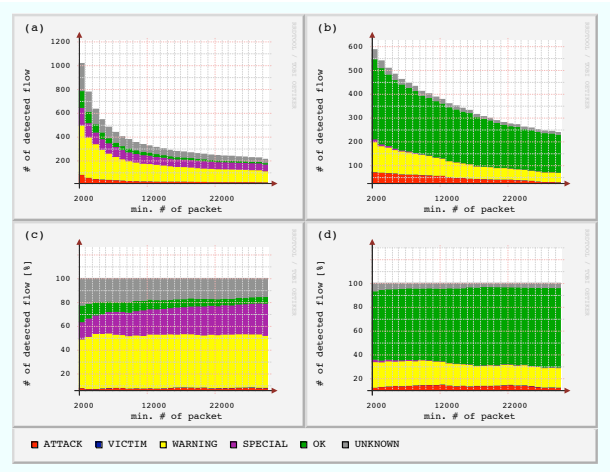

図 2: 最低パケット数の評価

5.2 タイムウィンドウ T_{win} の評価

図 3 は，T_{win} を変化させた時の検出フローの依存性を調べたものである．(a)，(c) は 2006 年 03 月のデータ，(b)，(d) は 2007 年 09 月のデータである．(a)，(b) は検出フロー数を表し，(c)，(d) は各カテゴリの割合を表す．

両者のデータにおいて，T_{win} に関して検出フロー数は減少傾向にある．異常カテゴリの割合は，

- 2006 年 03 月では，増加傾向にあるため，T_{win} は大きい方がよく，900 秒を最適値とする．
- 2007 年 09 月では，60 秒から 400 秒あたりに増減がみられ，180 秒の時に最大値をとっている．このデータに対しては，180 秒を最適値にできる．

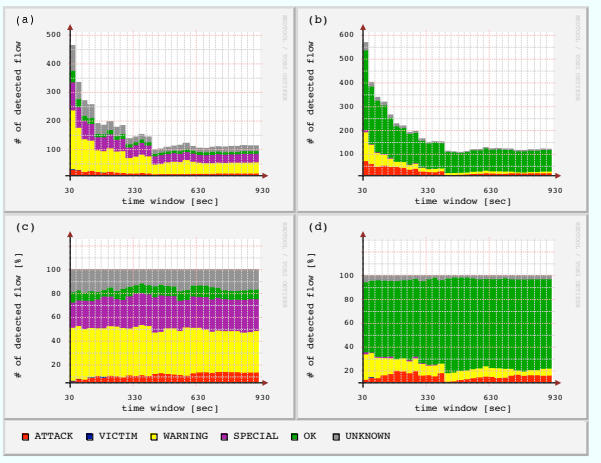

図 3: タイムウィンドウの評価

5.3 基本集約時間 Δ_0 の評価

図 4 は，Δ_0 を変化させた時の検出フローの依存性を調べたものである．(a)，(c) は 2006 年 03 月のデータ，(b)，(d) は 2007 年 09 月のデータである．(a)，(b) は検出フロー数を表し，(c)，(d) は各カテゴリの割合を表す．

両者のデータにおいて，異常カテゴリの割合は Δ_0 に対して依存性が小さい．従って，検出したいフロー数に応じて決定できると考えられる．ここでは，以下の考えに基づき，$\Delta_0 = 5$ ミリ秒を最適値とする．

- マルチスケール検出達成のため，Δ_0 を小さくとる．
- パケットのタイムスタンプにおいて，信頼できる精度が 1 ミリ秒程度である．

5.4 α についての閾値 λ_α の評価

図 5 は，λ_α を変化させた時の検出フローの依存性を調べたものである．(a)，(c) は 2006 年 03 月のデータ，(b)，(d) は 2007 年 09 月のデータである．(a)，(b) は

図 4: Δ_0 の評価

検出フロー数を表し，(c)，(d) は各カテゴリの割合を表す．

- 2006 年 03 月について: 異常カテゴリの割合は，2.1 付近から増減を繰り返し，3.0 付近から減少し始め，検出率 10%程度を維持する．したがって，2.1 から 3.0 までの値を最適値として採用できると考えられる．ここでは，2.5 を最適値とする．
- 2007 年 09 月について: 異常カテゴリの割合は，2.1 付近で最大値をとる．したがって，この値を最適値として採用できる．

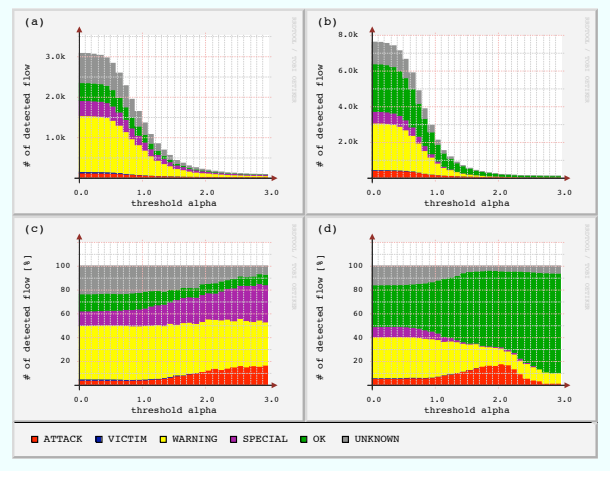

図 5: λ_α の評価

5.5 β についての閾値 λ_β の評価

図 6 は，λ_β を変化させた時の検出フローの依存性を調べたものである．(a)，(c) は 2006 年 03 月のデータ，(b)，(d) は 2007 年 09 月のデータである．(a)，(b) は検出フロー数を表し，(c)，(d) は各カテゴリの割合を表す．なお，α による検出は行っていない．

両者のデータにおいて，λ_β に関して異常カテゴリの割合は増加傾向にある．2.5 から 3.0 の間は，異常カテゴリの検出数には変化がないため，この間を最適値に採用する．ここでは，2.5 を最適値とする．

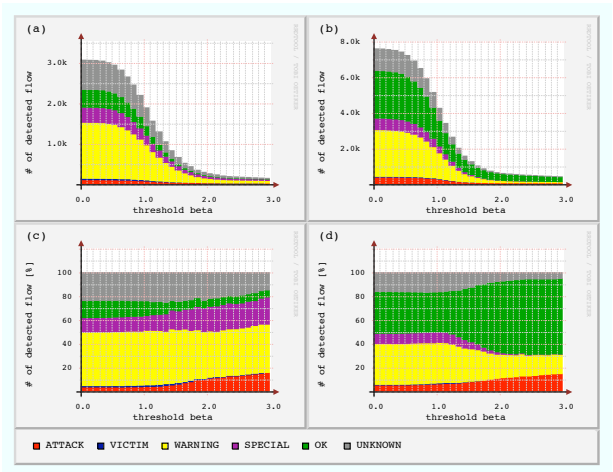

図 6: λ_β の評価

5.6 α と β の併用性の評価

α による検出と β による検出を併用したことにより，検出フローがどのように変化するかを調べる．表 5.6 は検出フロー数を，(1)α のみによる検出，(2)β のみによる検出，(3) 両者を用いた検出の 3 つの場合に分けて調べたものである．λ_α および λ_β のパラメータ値には，前述した最適値を用いた．

α と β の両方を用いた場合は，どちらか一方だけを用いた場合に比べて異常フローの割合が低下している．つまり，どちらか一方だけで検出されるフローは正常なフローが多い．また，両者のデータセットにおいて，β のみによる検出が最も精度が高い．したがって，β のみによる検出を最適な検出方法とする．

表 2: α と β の併用性の評価

	2006 年 03 月		
	正常フロー数	異常フロー数	異常フローの割合
α のみ	43	9	17.3%
β のみ	37	17	31.5%
α と β	86	17	16.5%
	2007 年 09 月		
	正常フロー数	異常フロー数	異常フローの割合
α のみ	101	18	15.1%
β のみ	166	37	18.2%
α と β	242	39	13.9%

5.7 精度評価

それぞれのパラメータに初期設定値および最適値を設定し，検出率・誤検出率を調べた．その結果を表 3 に示す．特に 2006 年 03 月のデータに対して，最適値設定による性能向上がみられる．

表 3: 最適パラメータにおける性能評価

	2006 年 03 月		
	正常フロー数	異常フロー数	異常フローの割合
初期設定値	326	31	8.7%
最適値	37	17	31.5%
	2007 年 09 月		
	正常フロー数	異常フロー数	異常フローの割合
初期設定値	141	19	11.9%
最適値	166	37	18.2%

図 7 は，λ_β に関する ROC 曲線を示したものである．この図により，以下のことがわかる．

- λ_β が小さな時: λ_β を増加させた時，正常フローの検出数も異常フローの検出数も同様の割合で減少している．
- λ_β が大きな時: λ_β を増加させた時，正常フローの検出数の減少率が大きく，異常フローは検出数の減少率は小さい．

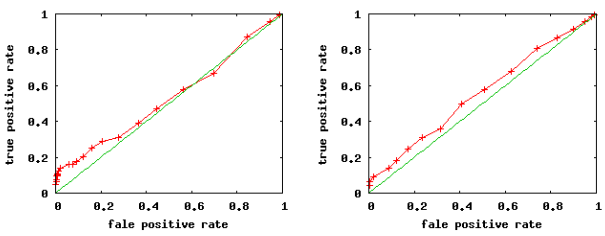

図 7: ROC 曲線（左：2006 年 03 月，右：2007 年 09 月）

計算時間は，2006 年 03 月のデータに対して 26 秒程度，2007 年 09 月のデータに対して 50 秒程度であった（プロセッサ: Interl Core 2 Duo 2.4 GHz，メモリ: 4 GB）．このデータセットに対しては，リアルタイム検出を行うことができる．

6 議論

6.1 データセットによる依存性について

ふたつのデータセットについて差異を検討する．

- リンク帯域: 2006 年 03 月時点におけるリンク帯域は小さく，多くのフローが輻輳状態にある．その結果，図 8 に示すような持続的な形をしたフローが多くみられる．2007 年 09 月時点においてはリンク帯域の増大により，データ転送時間が短くなった．その結果，図 8 に示すような突発的な形をしたフローが多くみられる．また，各データセットにおいて攻撃フローを調べた結果，突発的なフローが多いことがわかった．
- フローの種類: 図 9 は，パケット数 10000 以上のフローについて，フロー分別を行った結果である．図 10 は，その中の Attack カテゴリに対して，さらに詳細なフロー分別を行った結果である．2006 年 03 月は SYN フラッディング攻撃が多くみられ，2007 年 09 月は PING スキャンが多く見られる．この差異がパラメータの依存性に影響を与えるように思われるが，λ_α においては両者のデータとも，ピークの原因となっているフローは SYN フラッディング攻撃のフローであった．

リンク帯域の差異の影響が，主に以下の 3 つのパラメータに表れている．

- T_{win}: T_{win} を大きくとると，持続的なフローは平均化され，検出されにくくなる．実際，T_{win} が大きい時に検出されるフローを調べたところ，突発的なフローが多くみられた．そのため，2006 年 03 月のデータに対しては，T_{win} を大きくとることにより，正常フローと異常フローの分離がしやすくなる．
- λ_α: 持続的なフローは，極端な α 値をとる傾向にあることが分かっている．2006 年 03 月のデータは，持続的なフローが多いため，α 値の分布は大きくなる．そのため，正常と異常をうまく分離するための λ_α の値が大きくなる．

- λ_β: 突発的なフローは，極端な β 値をとる傾向にあることが分かっている．2006 年 03 月においては，λ_β を大きくするにつれて，異常カテゴリのフローは検出率が大きく増加する．この理由として，2006 年 03 月のデータは正常フローと攻撃フローの特性の違いが表れやすいためだと考えられる．一方，2007 年 09 月のデータは，正常フローと攻撃フローの特性の違いが小さくなり，β による検出が難しくなっている．

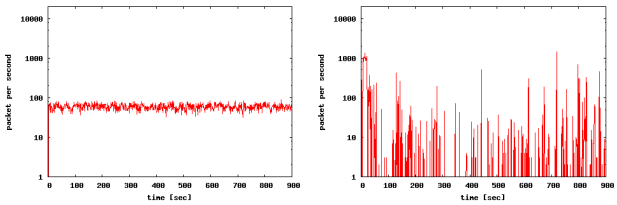

図 8: フローの代表例（左：2006 年 03 月，右：2007 年 09 月）

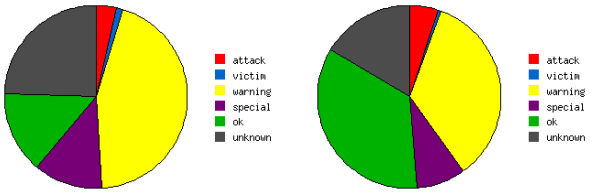

図 9: 各カテゴリの割合（左：2006 年 03 月，右：2007 年 09 月）

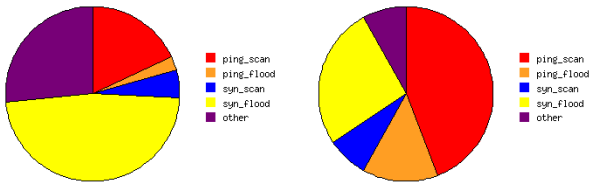

図 10: 攻撃フローの詳細な分別と割合（左：2006 年 03 月，右：2007 年 09 月）

6.2 性能評価および分別方法について

パラメータの最適値および性能評価は，フローの分別に大きく依存する．本論文では，異常カテゴリに分別されたフローのみを，異常フローとみなした．しかし，現在使用している分別手法では，その他のカテゴリにも少なからず異常フローが含まれているはずである．例として，以下のものがある．

- Warning カテゴリ: 現状では，正常な HTTP リクエストのフローと HTTP フラッディング攻撃フローが分別できず，それらは全て Warning カテゴリに分別される．
- Special カテゴリ: 現状では，DNS のフラッディング攻撃などは分別できない．
- Unknown カテゴリ: Unknown カテゴリも同様に，異常フローが含まれているであろう．

今後は，さらに信頼できる性能評価を行うために，分別手法の向上を図る必要があるといえる．

7 結論

7.1 まとめ

本研究では，統一的な異常検出手法の評価を行うための第一歩として，アノマリ型異常検出手法である“スケッチおよびガンマ関数モデルを用いた異常検出手法”について，最適化および評価を行った．その結果，統一的な性能評価を行うための指標を得ることができた．今後はフロー分別手法の高精度化を行い，さらに信頼性のある評価手法を確立する．

7.2 今後の課題

さらに信頼性の高い性能評価を行うためには，以下の事項が必要となる．

- 分別手法の精度向上: 既に述べたように，信頼性の高い評価を行うためには，可能な限り精度の高い分別手法が必要である．今後は，Karagiannis らが提案する手法 [5] などを取り入れ，精度向上を図る．
- 他のパラメータの評価: いまだ評価されていないパラメータの評価を行う．スケッチに関するパラメータは，性能に大きく関与しうるであろう．
- サンプリングデータに対する性能評価: さらに広帯域なデータに対しては，パケットサンプリングが必要になる．サンプリングレートは性能評価に影響を与えることが予想される．

- 他の異常検出手法との性能比較: 性能評価のためのフレームワークが整った後，他の手法との性能比較を行う．性能比較を行うことで，各手法の得手不得手などをデータベース化する．
- 異常データベースの構築: 性能評価を行う際に，さまざまな異常が発見される．それらの異常をデータベース化し，異常検出に携わる研究者に広く提供する．

謝辞

本研究において貴重な助言を与えていただいた，Patrice Abry 氏，Pierre Borgnat 氏，ならびに Guillaume Dewaele 氏に深く感謝します．また，本研究の一部は，科学技術振興機構 戦略的国際科学技術協力推進事業の一環として行った．

参考文献

[1] P. Barford, J. Kline, D. Plonka, and A. Ron. A signal analysis of network traffic anomalies. *ACM IMW'02*, pages 71–82, November 2002.

[2] J. Brutlag. Aberrant Behavior Detection in Time Series for Network Monitoring. *USENIX LISA 2000*, pages 139–146, December 2000.

[3] K. Cho, K.Mitsuya, and A. Kato. Traffic Data Repository at the WIDE Project. *USENIX 2000 FREENIX Track*, June 2000.

[4] G. Dewaele, K. Fukuda, P. Borgnat, P. Abry, and K. Cho. Extracting Hidden Anomalies using Sketch and Non Gaussian Multiresolution Statistical Detection Procedure. *ACM SIGCOMM LSAD'07*, pages 145–152, August 2007.

[5] T. Karagiannis, K. Papagiannaki, and M. Faloutsos. BLINC: Multilevel Traffic Classification in the Dark. *ACM SIGCOMM'05*, pages 229–240, 2005.

[6] A. Lakhina, M. Crovella, and C. Diot. Diagnosing Network-Wide Traffic Anomalies. *ACM SIGCOMM'04*, pages 219–230, August 2004.

[7] M. Roesch. Snort - Lightweight Intrusion Detection for Networks. *LISA'99: Proceedings of the 13th USENIX conference on System administration*, pages 229–238, November 1999.