研 究 報 告 書

「時空間解析に基づくインターネットトラフィック異常検出とそのデータベース化」

研究期間: 平成 20 年 10 月～平成 24 年 3 月
研 究 者: 福田 健介

1，研究のねらい

インターネットバックボーン上では，大多数の通常のトラフィックに隠れた異常なトラフィックが存在することが知られており，これらの異常トラフィックをより効率的に発見する手法の確立が求められている．本研究では，上記の目標のために，下記のねらいを定め研究を行った．

(1) 異常トラフィックが持つ特徴量の連続的な変化に着目し，その軌跡を画像処理的アプローチにより検出する異常検出器の実現

(2) 理論的な背景の異なる複数の異常検出器の出力を組み合わせ，その性能の比較を可能とし，また，それらの性能向上を図ることが可能な，ベンチマークアーキテクチャの実現

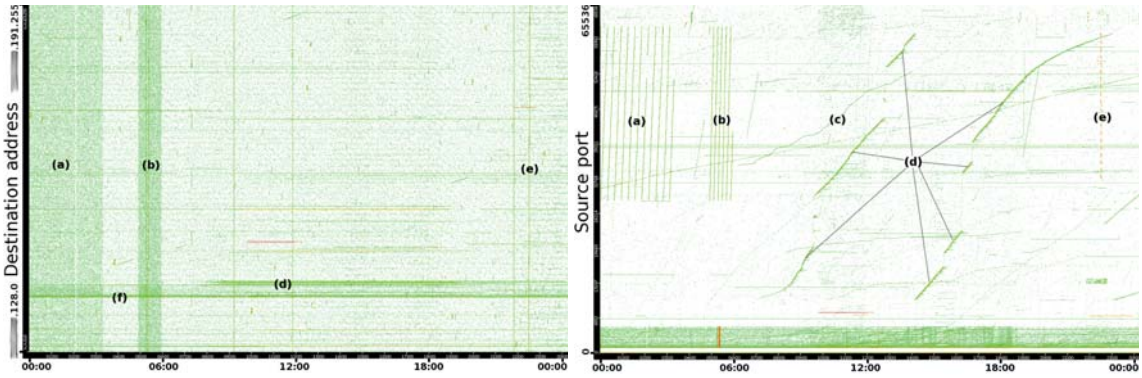
(3) 公開されている 10 年にわたるインターネットトラフィックデータに対して，提案アーキテクチャを適用することで，異常イベントのデータベースを構築し研究コミュニティに公開

2，研究成果

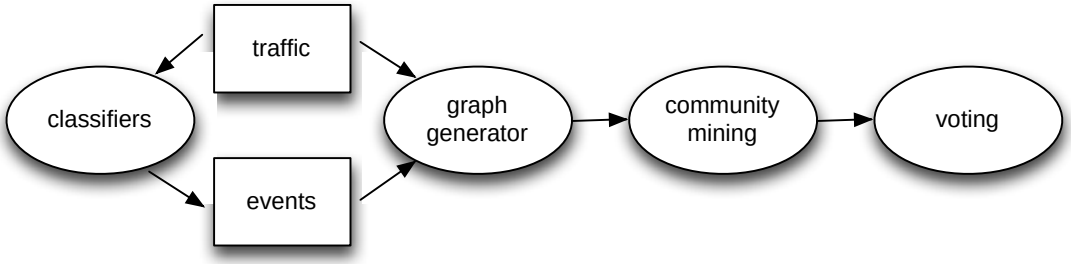
(1) インターネットバックボーントラフィックにおける異常(イベント)は，ウィルス，ワーム，DDos(分散サービス不能攻撃)，機器の故障・設定間違い，フラッシュクラウド(特定コンテンツへのリクエストの集中)等さまざまである．しかしながら，これらの異常イベントは大部分の正常なトラフィックに比べると，トラフィック量としてはそれほどの量とはならない．そのため，トラフィック量を監視しているだけでは，埋もれた異常イベントを検出することが難しい．本研究では，これらの埋もれた異常イベントを構成するパケット群の特徴量の連続する変化を二次元平面上の軌跡と捉え，その軌跡を検出することで異常イベントを検出する，新しいタイプの異常検出器を提案・実装評価した．

下図は，異常トラフィックの時間変化(各点はパケットトラフィックに対応)を示している，左図では特徴量として異常トラフィックの送信元アドレス，右図では送信元ポートを表している．例えば，左図の水平線上の線状の集合は特定ホストへのアクセス，垂直線上の集合は多数のホストへのアクセスに対応している．左図では個々の異常に対応するアクティビティはそれほど明らかではないが，右図のように適切な特徴量を選ぶことで，異常を二次元上の軌跡として捉えることが可能となる．提案アルゴリズムは複数のステップから構成される．(a) トラフィックトレースをランダムハッシュし，複数のサブトレースを生成，(b) サブトレースごとに時間・特徴量(4 種類)空間のデータの切り出し，(c) ハフ変換によるエッジ(軌跡)検出，(d) サブトレースごとに得られた軌跡に属する送信元 IP アドレスをリストアップし，それらのインターセクションを異常イベントに係わる送信元として同定する．提案アルゴリズムを 10 年間にわたるインターネット日米国際リンクトラフィックデータ(MAWIトレース)に適用し，その性能を評価した．提案アルゴリズムは，他のアルゴリズムと比較して，3-5 倍の異常を検出することに成功した．同様に，時間軸と特徴量の変化量に着目し，異常イベントの到達速度を推定する手法を開発した．これ

により，異常イベントの 80–90%は一定の速度をもち，残りの異常イベント(主に特定のオペレーティングシステムによるもの)はランダムな到着であることが明らかとなった．また，提案アルゴリズムを任意の二つの特徴量に拡張し，ユニークなパケットの到着速度に着目することで画像サイズを自動的にチューニングする手法を開発し，オリジナルの手法と比べて，さらに 20%の性能向上が可能となった．α フロー(トラフィック量の多い単一のフロー)に対する検出精度はあまり高くならないものの，他の異常イベントの検出精度が向上したことで，他の検出器では検出困難な異常イベントを検出することが可能となった．



(2) 既存のインターネットトラフィックにおける異常検出器研究に関する問題点として，(a) 共通のトラフィックデータが用いられていない，(b) 異常イベントがラベリングされたデータ(正解データ)が存在しない，(c) 複数検出器の出力の粒度が異なるため単純な比較が困難，(d) これら共通の土俵での検出器の比較検討がなされていないため，どの異常に対してどの異常検出器が優位であるかが不明，などが挙げられる．
以上の問題点を解決するべく，複数異常検出器の出力を比較検討可能とするベンチマークアーキテクチャ(MAWILab)を提案・実装・評価した．提案システムの処理ステップの概略は以下のとおりである(下図参照)



(a) 共通公開トラフィックデータ(MAWI トレース)を入力とした，個々の異常検出器の出力を xml ファイルとして保存．xml ファイルには，異常検出器名，データファイル名，個々の異常イベントの開始，終了時間，トラフィックキー(送信元・送信先アドレスおよびポート，プロトコルの全てもしくはその一部)，イベントのヒューリステックラベル(異常・正常・不明およびその理由)が記録される，個々の異常検出器の出力精度を制御パラメータとするために，個々の検出器ごとに，3 種類の異なるパラメータセット(出力数: 大，最適，小)を用いる．(b) xml ファイル中のイベントからイベント

グラフを生成する．グラフのノードは個々の検出器出力から得られた異常イベント，ノード間のリンクは 2 つのノードに共通するパケットによる重みである．すなわち，複数の異常検出器で共通して得られるイベントはクリークとなり，単一の異常検出器のみから得られるイベントは孤立したノードとなる． イベントに共通するパケットに着目することで，出力粒度の異なる異常検出器を同じように比較検討することが可能となる．（c）得られたグラフから，稠密なサブグラフをコミュニティマイニングアルゴリズムにより検出する．これにより，複数検出器により検出されるイベントを一つのクラスタとして扱うことが可能となる．もし，異常検出器の性能が同じであれば，この結果はクリークとなる．(d) 検出されたクラスタが異常もしくは正常であるかを複数の投票方式(多数決，最大，最小，SVD ベースの教師無し学習（SCANN）)を用いて判定する．SVD を用いる利点は，単一の異常検出器が多くの異常を検出し，その多くが他の検出器で検出されない場合，その結果は最終判定では低い重みがつけられる点である．(e) 得られた異常クラスタに属するパケットデータに，アプリオリアルゴリズムを適用することで，異常クラスタに対応するパケットフィルタルールを生成し，ルータ・スイッチでのフィルタリングを可能とする．
4 種類の理論的なバックグラウンドの異なる異常検出器(画像処理，PCA, Sketch gamman, KL 統計量に基づくもの)を実装し，10 年間わたる公開トラフィックデータ(MAWI トレース)を用いることで，提案ベンチマークシステムの評価を行った．その結果，検出された異常の多くは，少数の検出器によってのみ検出されること，精度の低い検出器の出力は最終出力として採用されず，各々の検出器の寄与が明らかとなった．また，SCANN の結果は必ずしも最適ではないが，平均的に優れた性能を示すことがわかった．すなわち，これらの結果は，単一の精度の高い異常検出器を構築することは困難であり，複数の検出器を組み合わせることによってのみ，精度の向上が可能であることを示すものである．

(3) 上記ベンチマークアーキテクチャを 10 年にわたるトラフィックデータ(MAWI トレース)に適用することで，データ中の異常イベントを抽出・ラベリングし，異常トラフィックデータのデータベースを構築，研究者への公開を 2010 年末より開始した(http://www.fukuda-lab.org/mawilab)．2012 年 2 月現在 15 カ国 2000 を越えるアクセスがあり，本データベースのデータをベンチマークデータとして使用した新たな異常検出器の提案が複数行われている．

上記成果の他に，領域会議中に他研究者より，異常パターンをトラフィックデータから抜いた”準正常データ”を学習データとして用いた異常検出器の改良についての助言があり，追加課題として取り組んだ．しかしながら，異常パターンを単純に抜いたデータでは，トラフィックに不必要なギャップが増えること，不明トラフィックの扱い方による差，輻輳時には正常パターンも異常パターンとなること等，いくつかの問題に直面し，期待した成果を得ることはできなかった．しかしながら，今後，既存異常パターンを抜き出すのではなく，アドレス単位のランダムハッシュを用いて，異常トラフィックを少数のハッシュに分離する方向でさらに研究を進めていく予定である．同様に多次元ハフ変換に基づく異常検出器，非線形次元圧縮に基づく異常検出器に関しても研究を進めたが，主として計算量の問題で，期待した成果を得ることができなかった．

3，今後の展開

本研究では，インターネットトラフィックにおける異常検出を予め収集されたパッシブデータを用いて行った．しかしながら，本研究で行った研究結果を生かすには，リアルタイムにデータを収集し，異常を検出することが望ましい．現在，学術情報ネットワーク(SINET)のバックボーン回線においてデータ収集環境を整えつつあり，今後，開発したシステムを本ネットワークに適用し，リアルタイムでの実証実験を行うことで，開発システムの実ネットワークへの適用を目指す．同様に，機械学習的アプローチを用いた複数異常検出器の出力結果の組み合わせによる精度向上，理論的バックグラウンドの異なる異常検出器の追加，ヒューリスティックラベルの精度向上を行うことでシステムとしての精度向上，他研究者が開発した異常検出器の性能を MAWILab と比較可能な Web インターフェイスの構築，等を行う予定である．

4，自己評価

当初の提案では，画像処理アプローチに基づく異常検出器をメインターゲットとして研究を進める予定であり，実際，精度の高い，自動パラメータ設定可能な検出器を提案できたことから，当初の目的を達成できたと考える．さらに，異常検出器の研究を進めるにつれ，現在のインターネットトラフィック異常検出におけるさまざまな問題点(共通したデータセットの欠如，正解データの欠如，異常検出器間の性能比較方法の欠如)に直面し，これらの問題を解決するよう，研究トピックを追加した．その結果，提案時にはなかった，複数異常検出器の比較ベンチマークアーキテクチャおよび共通データベースの精度向上に関しての研究が進み，トップ国際会議への採択に至った．また，複数検出器出力に基づいた，インターネットトラフィック異常データベースを公開したことで，他研究者からベンチマークに使用される標準データベースとなりつつある点は，当初の目的を達成できたと考える．反面，画像処理ベースの異常検出器の実ネットワーク(リアルタイム)への適用が遅れ，今後の課題となった．

5，研究総括の見解

インターネットトラフィックの時系列を時空間パターンにして解析し、大量のデータに埋もれた少量の検出対象を見つけるという課題である。具体性があり、研究を評価するためのデータの準備も整っており、インターネットに限らず、汎用性のある画像認識によるネットワークダイナミックの異常を検知する技術、また、トラフィック解析のみにとどまらず、幅広い場面での適用が可能な技術となることを期待していた。

当初の提案では、画像処理アプローチに基づく異常検出器をメインターゲットとして研究を進める予定であり、実際、精度の高い、自動パラメータ設定可能な検出器を提案できたことから、当初の目的を達成できていると評価する。さらに、現在のインターネットトラフィック異常検出におけるさまざまな問題点(共通したデータセットの欠如、正解データの欠如、異常検出器間の性能比較方法の欠如)を解決するよう、研究トピックを追加した。その結果、提案時にはなかった、複数異常検出器の比較ベンチマークアーキテクチャおよび共通データベースの精度向上に関しての研究が進み、トップ国際会議への採択に至っている。また、複数検出器出力に基づいた、インターネットトラフィック異常データベースを公開したことで、他研究者からベンチマークに使用される標準データベースとなりつつある。この分野に大きく貢献したと考える。

一方、異常検出器の実ネットワーク(リアルタイム)への適用が遅れており、今後の研究に期待

する。

6，主な研究成果リスト

（1）論文（原著論文）発表

1. R.Fontugne, Y.Himura, K.Fukuda, Evaluation of anomaly detection method based on pattern recognition, IEICE Transactions on Communications, vol.E93-B, no.2, pp.328-335, IEICE, 2010

2. Y.Himura, K.Fukuda, K.Cho, H.Esaki, An evaluation of automatic parameter tuning of a statics-based anomaly detection, International Journal of Network Management, vo.20, no.5, pp.295-316, Wiley, 2010

3. Y.Himura, K.Fukuda, K.Cho, H.Esaki, Characterization of host-based traffic with multi-scale gamma model, IEICE Transactions on Communications, vol.E93-B, no.11, pp.3048-3057, IEICE, 2010

4. R.Fontugne, T.Hirotsu, K.Fukuda, A Visualization tool for exploring multi-scale traffic anomalies, Journal of Networks, vol.4, no.4, pp.577-586, Academy publisher, 2011

5. R.Fontugne, K.Fukuda, Hough-transform-based anomaly detector with an adaptive time interval, ACM Applied Computing Review, vol.11, no.3, pp.41-51, ACM, 2011.

（2）特許出願

研究期間累積件数：0 件

（3）その他の成果（主要な学会発表、受賞、著作物等）

1. R.Fontugne, P.Borgnat, P.Abry, K.Fukuda, Uncovering relations between traffic classifiers and anomaly detectors via graph theory, Proceedings of TMA2010, pp.101-114, Zurich, Apr, 2010

2. K.Fukuda, R.Fontugne, Estimating speed of scanning activities with a Hough transform, Proceedings IEEE ICC2010, p.5, Capetown, Jun., 2010

3. Y.Kanda, K.Fukuda, T.Sugawara, An evaluation of anomaly detection based on sketch and PCA, Proceedings of IEEE GLOBECOM2010, p.5, Miami, Dec., 2010

4. R.Fontugune, P.Borgnat, P.Abry, K.Fukuda, MAWILab: Combining diverse anomaly detectors for automated anomaly labeling and performance benchmarking, Proceedings of ACM CoNEXT2010, p.12, Philadelphia, Dec., 2010

5. K.Fukuda, An analysis of longitudinal TCP passive measurements, Proceedings of TMA2011, pp.29-36, Vienna, Apr., 2011