様式 C-19

科学研究費補助金研究成果報告書

平成２３年６月１日現在

機関番号：17104
研究種目：若手研究(B)
研究期間：2009～2010
課題番号：21700079
研究課題名（和文） 正常トラヒック情報の効率的な抽出と統合モデルによるロバスト異常トラヒック検出技術
研究課題名（英文） Robust Anomaly Detection based on Ensemble Model through Efficient Extraction of Normal Traffic Information
研究代表者
内田 真人（UCHIDA MASATO）
九州工業大学・ネットワークデザイン研究センター・准教授
研究者番号：20419617

研究成果の概要（和文）：
正常なトラヒックパターンを表す確率モデル（基準モデル）を用いた非正常パターン検出型の異常トラヒック検出技術について検討した．本研究では，時間周期的パケットサンプリングにより効率的に抽出された正常トラヒック情報を用いて基準モデルを学習する手法を提案した．また，複数の確率モデルの統合により，検出性能の改善と検出感度の調整を可能とする手法を提案した．提案手法の有効性は，理論解析と実トラヒックデータを用いた実証実験により評価した．

研究成果の概要（英文）：
I proposed an anomaly detection method that trains a baseline model describing the normal behavior of network traffic using normal traffic information which is efficiently extracted through time-periodical packet sampling. In addition, in order to improve detection performance and adjust alarm sensitivity, I proposed an ensemble anomaly detection that collectively exploits multiple baseline models in parallel. Theoretical analysis and testing using actual traffic traces showed that the proposed anomaly detection methods perform well.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	2,200,000	660,000	2,860,000
2010 年度	900,000	270,000	1,170,000
年度			
年度			
年度			
総　計	3,100,000	930,000	4,030,000

研究分野：情報ネットワーク，情報理論，学習理論
科研費の分科・細目：情報学，計算機システム・ネットワーク
キーワード：ネットワーク計測，異常トラヒック検知

１．研究開始当初の背景

インターネットトラヒックの増加，インターネットの利用形態やアプリケーションの多様化に伴い，ネットワークを適切に管理運用するためのトラヒック計測分析技術の重要性が高まっている．特に，ネットワークの品質劣化の要因となるネットワーク資源の浪費や，セキュリティ上の問題を引き起こす異常トラヒックを検出するためのトラヒック計測分析技術の重要性は増すばかりである．我が国においても，第 3 期科学技術基本計画(総合科学技術会議，2006 年 3 月)や u-Japan 推進計画 2006(総務省，2006 年 9 月)の中で，社会インフラとしての信頼性や安全

性のあるユビキタスネットの実現は，情報通信分野における重要な研究開発課題として位置付けられている．

異常トラヒックの検出技術は，異常パターン検出型と非正常パターン検出型という互いに相補的な方式に分類される．異常パターン検出型は，「異常な」トラヒックのパターンを検出した際に警告を発する方式である．Snort や Bro はこの方式に分類される．この方式では，異常トラヒックのパターンが記録されたデータベースとの照合を行うため，既知の異常トラヒックの検出には非常に有効である．しかし，未知の異常トラヒックの検出には無力であり，データベースの定期更新が必要となる．一方，非正常パターン検出型は，「正常な」トラヒックとされないパターンを検出した際に警告を発する方式である．この方式は，上記の異常パターン検出型のようなデータベースの管理が不要であり，未知の異常トラヒックをも検出できる可能性があるという大きな利点を持つため，研究開始当初においても活発に研究されていた．

２．研究の目的

本研究では，後者の非正常パターン検出型の異常トラヒック検出技術について検討する．この方式は，通常，正常時のトラヒックパターンを表現する基準モデルを予め学習した上で，その基準モデルで表現されたトラヒックパターンと計測したトラヒックパターンが異なるかどうかを判定することによって実現される．基準モデルの学習においては，所与のトラヒックデータにおける個々のパケットを正常/異常パケットに分類し，そこから選別された正常パケットのみからなるトラヒックデータが学習データとして用いられる．しかし，このような分類作業は専門家による手作業によって行われることが多く，正常トラヒックデータの取得には多大な手間と時間がかかるという問題がある．本研究の目的は，異常トラヒックの検出精度を犠牲にすることなく，この問題を解決することにある．

３．研究の方法

上記の問題を解決するために，本研究では，監視対象ネットワークにおいて計測されたトラヒックデータとの比較のために用いられる正常時のトラヒックパターンを表す確率モデル（基準モデル）を，正常／異常パケットが分類されてないトラヒックデータ（教師無しトラヒックデータ）を用いて学習することのできる教師無し異常トラヒック検出手法を提案した．提案手法の基本アイデアは，本来とは異なる目的でパケットサンプリングを用いることにある．一般に，パケットサンプリングはトラヒック計測の軽量化を目的として用いられるが，多くのパケットがサンプルされずに破棄されることからサンプル結果に偏りが生じ，元来のトラヒック特性に関する情報が失われるという欠点がある．これに対し本研究では，この欠点を，異常パケットが混在する所与の教師無しトラヒックデータから，正常パケットに偏ったトラヒックデータをサンプルするために利用する．すなわち，提案手法では，教師無しトラヒックデータに含まれる正常トラヒックに関する情報（つまり，正常パケット）を効率良く抽出するために，パケットサンプリングの欠点である情報損失特性を逆手に利用する．特に本研究では，TCP の SYN パケットを大量送信するようなバースト性を持つ異常トラヒックをサンプルしにくくするために，適当な確率分布により決定されたサンプリング時間間隔に従う時間周期的サンプリングを適用し，その統計的偏りや散らばりを活用した手法を提案する．提案手法の有効性は，実トラヒックデータを用いた理論解析と検証実験によって評価する．

４．研究成果

(1)時間周期サンプリングの有効性に関する理論解析：

提案手法では，所与の教師無しトラヒックデータから正常パケットを抜き出すために時間周期的パケットサンプリングを用いる．時間周期的パケットサンプリングとは，時刻 $T_n = t_1 + t_2 + \cdots + t_n$ [sec]をトリガーとし，その直後に到着したパケットのみをサンプルし，その他のパケットはサンプルしないという計測手法である．ここで，t_i はサンプリング時間間隔を表す．以下では，サンプリング時間間隔 t_i が期待値 t を持つ独立同一の指数分布に従うものとする．すなわち，トリガーは，レート $\tau = 1/t$ のポアソン過程に従い生起するものとする．提案手法では，基準モデルを学習するために時間周期的にサンプルされたパケットデータを用いるため，事前準備としての手作業の分類が不要となる．本研究では，異常トラヒックがバースト的に発生している場合，時間周期的にサンプルされたトラヒックデータは，サンプリング前のオリジナルトラヒックよりも高い割合で正常パケットを含むものと期待できることを理論的に検証した．このことを以下に示す．

まず，2 本のフローが多重されているとする．また，フロー1 を構成するパケットはレート λ_1 のポアソン過程に従い生成され，フロー2 を構成するパケットはレート Λ_2 のポアソン過程に従い生成されるとする．ただし，Λ_2 は $(0, 2\lambda_2)$ 上の一様分布に従う確率変数であり，その期待値は λ_2 である．フロー1 は正常トラヒックを表し，フロー2 は異常トラヒック（バーストトラヒック）を表している．

また，フローiのj番目のパケットを$A_j^{(i)}$とし，時刻$T_0 = 0$の後に最初に到着したパケットがフローiのものである確率を$p_1^{(i)}$とする．このとき，本研究では，$p_1^{(2)} / p_1^{(1)} < \lambda_2 / \lambda_1$が成り立つことを理論的に証明した．この不等式は，正常トラヒックフロー（フロー1）のパケットに対する異常トラヒックフロー（フロー2）のパケットの割合は，サンプルされる前のオリジナルのトラヒックデータよりも時間周期的にサンプルされたトラヒックデータの方が低いことを意味している．

(2) 複数の基準モデルを用いたアンサンブル異常検出の提案：

提案手法では，基準モデルの学習に最大エントロピー原理に基づいた手法を用いた．基準モデルはパケットクラスの集合Ω上の一般化ギブス分布$P(\omega;\Xi), (\forall\omega \in \Omega)$を用いて定義した．ただし，$\Xi$は一般化ギブス分布のパラメータ集合を表し，その推定には共役勾配法を用いた．

本研究では，スライディングウィンドウ方式に基づいた異常トラヒック検出手法を用いた．この手法では，固定長δ[sec]で分割されたタイムスロット毎に異常トラヒック検出を行う．あるタイムスロット内で計測されたパケットの集合をΠとし，このタイムスロット内のパケットクラスの経験分布を$P(\omega,\Pi), (\forall\omega \in \Omega)$と書き，$P(\omega,\Pi)$と$P(\omega;\Xi)$間のパケットクラス$\omega$に関する部分相対エントロピーを

$$D(\omega;\Pi,\Xi) = P(\omega,\Pi)\log\frac{P(\omega,\Pi)}{P(\omega,\Xi)}$$

と定義する．そして，あるパケットクラスωに対し，連続するW個のタイムスロットのうちh個以上のタイムスロットにおいて

$$D(\omega;\Pi,\Xi) > d \qquad (1)$$

を満たす場合に警告を上げる．

しかし，以下で示すように，基準モデル$P(\omega;\Xi)$の異常トラヒック検出性能はサンプル結果に依存して変動する．そこで本研究では，この変動を軽減するために，時間周期的パケットサンプリングを独立に実行して得られた複数のサンプルデータを用いて複数の基準モデルを個別に学習し，それらを統合した新たな基準モデルを用いたスライディングウィンドウ手法により異常検出を実行する，という異常トラヒック検出手法を提案する．この手法では，式(1)の代わりに以下を用いる．

$$\frac{1}{M}\sum_{i=1}^{M} D(\omega;\Pi,\Xi_i) > d \qquad (2)$$

ここで，Ξ_iはi番目の時間周期的サンプリングで得られたトラヒックデータを用いて学習された基準モデルのパラメータを表し，Mは統合する基準モデルの個数を表す．

さらに本研究では，複数の基準モデルの変動を異常検出の感度調整に利用する手法として，異常トラヒックの見逃しを緩和するための高感度な判定規則

$$\max_{i=1,2,\ldots,M} D(\omega;\Pi,\Xi_i) > d \qquad (3)$$

と，異常トラヒックの誤検出を緩和するため低感度な判定規則

$$\min_{i=1,2,\ldots,M} D(\omega;\Pi,\Xi_i) > d \qquad (4)$$

を提案した．

(3)実トラヒックデータを用いた実験による提案手法の有効性の検証：

①利用するトラヒックデータ：

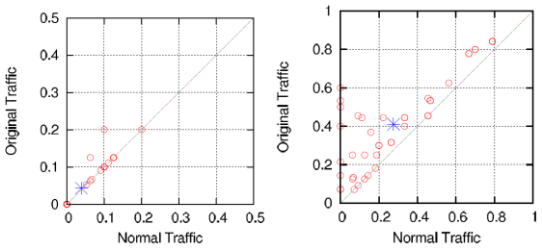
本研究では，Umass Trace Repository で提供される実トラヒックデータを利用した．この実トラヒックデータは，米国マサチューセッツ大学（Umass）が Verio と Internet2 を介してインターネット接続するギガビットイーサネットリンクにおいて計測されたものである．本研究では，2004 年 7 月 16 日から 7 月 22 日の午前 9 時 30 分から 10 時 30 分に計測された「Gateway Link 3 Trace」を利用した．この実トラヒックデータに含まれるパケットの属性（正常／異常）は手作業で分類されているが，提案手法においてはこの分類結果を参照しない．

②時間周期的パケットサンプリングの有効性に関する評価：

以下の手順で，時間周期的パケットサンプリングの有効性を評価した．まず，ある計測日のトラヒックデータについて，正常トラヒックデータ，サンプリング前のオリジナルトラヒックデータ，時間周期的にサンプルした 10 通りのトラヒックデータ，ランダムにサンプルした 10 通りのトラヒックデータを用いて基準モデルを学習した．そして，これとは異なる計測日のトラヒックデータを用いて，正常パケットを異常とみなす誤検出数(FP: False Positives) と異常パケットを正常とみなす検出漏れ数(FN: False Negatives) を評価した．例えば，7 月 16 日のトラヒックデータを用いて基準モデルを学習した場合は，7 月 17 日から 22 日のトラヒックデータを評価に用いた．学習と評価に用いるトラヒックデータの計測日については全ての組み合わせを網羅した．また，異常トラヒック検出の際は連続した FP を 1 つの FP とみなし，フロー単位での異常検出を行った．ただし，FP と FN の値は，評価に用いるトラヒックデータ中に含まれる異常トラヒックの総数で正規化した．なお，特に断らない限り，サンプルした 10 通りのトラヒックデータを用いて基準

モデルを学習した場合の FP と FN の値は，その平均値を用いて評価を行った．以下では，$t = 0.1$，$d = 0.01$，$W = 60$，$h = 30$とした．

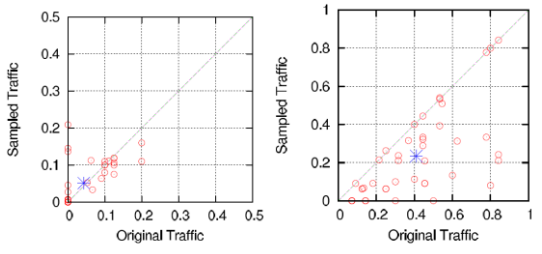
図 1 に示す散布図は，正常トラヒックデータとオリジナルトラヒックデータを用いて基準モデルを学習した場合の FP と FN を表している．図中の 1 つの丸印は，学習と評価に用いるトラヒックデータの計測日の 1 つの組み合わせに対応し，星印は図中の全ての丸印の平均位置を表わす．なお，以降の図も同様の記法を用いている．図 1 より，FP と FN のどちらについても，正常トラヒックデータよりもオリジナルトラヒックデータを用いた方が劣ることが分かる．



(a) FP　　(b) FN

図 1　オリジナルトラヒック vs. 正常トラヒック

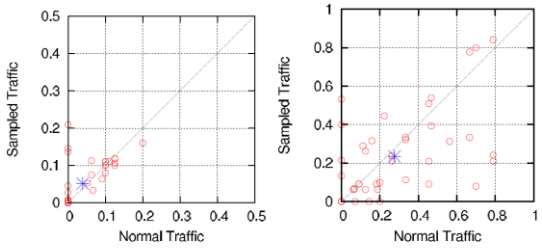
図 2 に示す散布図は，時間周期的にサンプリングしたトラヒックデータとオリジナルトラヒックデータを用いて基準モデルを学習した場合の FP と FN を表している．図 2(a) より，個別の FP の性能（丸印）は変動しているものの，平均的な FP の性能（星印）は，どちらのトラヒックデータを用いた場合もほぼ同等であることが分かる．一方，図 2(b) より，時間周期的にサンプルしたトラヒックデータを用いた場合の FN の性能は，オリジナルのトラヒックデータを用いた場合よりも優れることが分かる．なお，この結果は平均サンプル時間間隔 t の値に強く依存しないことを確認済みである．



(a) FP ($t = 0.1$)　　(b) FN ($t = 0.1$)

図 2　時間周期的にサンプルされたトラヒック vs. オリジナルトラヒック

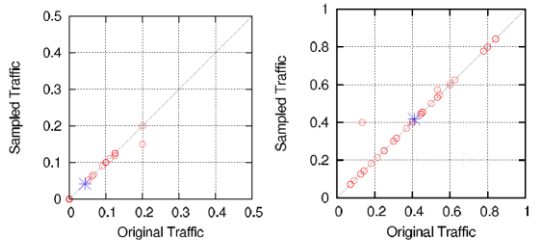
図 3 は時間周期的にサンプリングしたトラヒックデータと正常トラヒックデータを用いて基準モデルを学習した場合の比較評価である．図 3 より FP と FN の個々の性能は変動しているものの，その平均はどちらのトラヒックデータを用いた場合もほぼ同等であることが分かる．



(a) FP ($t = 0.1$)　　(b) FN ($t = 0.1$)

図 3　時間周期的にサンプルされたトラヒック vs. 正常トラヒック

図 2，3 の結果より，時間周期的サンプリングしたトラヒックデータを用いることは，FP の性能を犠牲にすることなく，FN の性能を改善することに有効であることが分かる．一方，図 4 に示すように，サンプリングレート $r = 0.001$でランダムにサンプリングしたトラヒックデータを用いた場合の FP と FN の性能は，オリジナルトラヒックデータを用いた場合とほぼ同等であることが分かる．このことは，ランダムにサンプリングしたトラヒックデータを用いることは有効ではないことを意味している．



(a) FP ($r = 0.001$)　　(b) FN ($r = 0.001$)

図 4　ランダムにサンプルされたトラヒック vs. オリジナルトラヒック

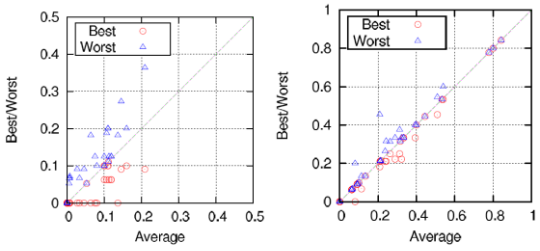
③アンサンブル異常検出の有効性に関する評価：

図 2，3 では，時間周期的サンプリングを 10 回実行し，それらを用いて学習した基準モデルにおける FP と FN の平均を示したが，図 5 では，平均を取る前の個別の基準モデルにおける FP と FN の平均性能と最良/最悪性能を比較した結果を示す．この図より，個別の基準モデルの性能は時間周期的サンプリングの確率的な特性によって変動していることが分かる．

図 6 は，式(1)に示した手法の性能（図 2，3 に示した個別の基準モデルの平均性能）と，複数のサンプルトラヒックデータを用いて学習した複数の基準モデルを統合するという式(2)に示した手法（$M = 10$）の性能を比較したものである．図 5 と比較すると，図 6 に示す FP と FN の性能の変動幅は小さくなっ

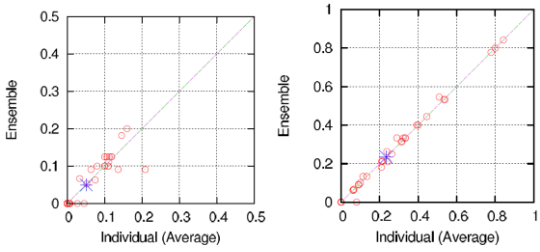
ていることが分かる．したがって，式(2)の手法は，個別の基準モデルの性能の変動を抑制するのに有効であるといえる．

図 7 は，異常検出の変動抑制を目的とした式(2)に示した手法の性能と，異常検出の感度調整を目的とした式(3)，(4)に示した手法の性能を比較したものである．この図より，式(3)を用いた場合は FP を犠牲にすることで FN の改善が可能であり，式(4)を用いた場合は FN を犠牲にすることで FP の改善が可能であることが分かる．この結果は，基準モデルの変動を利用することで，異常検出の感度調節が可能であることを意味している．



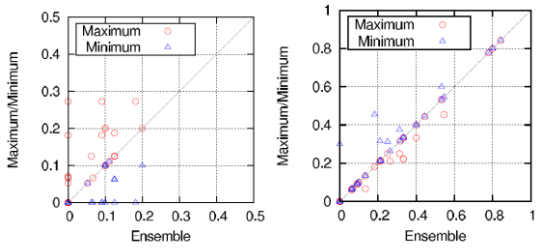
(a) FP ($t = 0.1$)　(b) FN ($t = 0.1$)

図 5　平均性能と最良/最悪性能の比較



(a) FP ($t = 0.1$)　(b) FN ($t = 0.1$)

図 6　式 (1) と式 (2) の比較



(a) FP ($t = 0.1$)　(b) FN ($t = 0.1$)

図 7　式 (2) と式 (3)，式 (4) の比較

④まとめ：

本研究では，基準モデルを学習する際に，手作業で分類されたトラヒックデータを必要としない異常トラヒック検出手法を提案した．この手法の特徴は以下の三点である．(i) 本来とは異なる目的でパケットサンプリングを利用すること．(ii)複数の基準モデルを統合して使用することによりパケットサンプリングにおける変動を軽減し，全体的な異常検出性能を改善すること．(iii)あるいは，この変動を利用して，異常検出の感度を調整可能であること．

本研究では，理論解析と実データを用いた実験結果より，以下のことを確認した．(a) ランダムパケットサンプリングと比較して，時間周期的パケットサンプリングはバースト的な異常トラヒックを含む可能性がある未分類のオリジナルトラヒックから効率良く正常パケットを抽出することが可能である．(b) 未分類のオリジナルトラヒックデータやランダムサンプリングされたトラヒックデータと比較して，時間周期的サンプリングされたトラヒックデータを用いて学習した基準モデルは FP や FN の観点から異常検出に有効である．(c) 複数の基準モデルを統合して用いることで検出性能を改善すること，もしくは，検出感度を調整することが可能である．以上の結果より，提案手法を用いることで，異常トラヒックの検出精度を犠牲にすることなく分類コストを削減できることが明らかとなった．この研究成果は，異常トラヒック検知技術の実用性の向上に寄与するものであると言える．

なお，本研究の成果は，情報ネットワーク分野において最も権威のある国際会議である IEEE Infocom 2010 の併催ワークショップへの採択を果たしており，高いプレゼンスを実現できた．さらに，本研究で利用した実トラヒックデータや分析プログラムの一部は，研究代表者が以前滞在した米国マサチューセッツ大学より提供を受けたものであり，当該大学出身の研究者との共著論文を執筆する等，海外との連携も達成できた．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔学会発表〕（計３件）

① 内田 真人，縄田 秀一，Yu Gu，鶴 正人，尾家 祐二，″時間周期的パケットサンプリングの統計的性質とその異常トラヒック検知への応用，″ 電子情報通信学会 ネットワークシステム研究会，信学技法 Vol. 110，No. 448，pp. 651-656 (NS2010-278)，2011 年 3 月 3-4 日(沖縄コンベンションセンター，沖縄県宜野湾市)．

② Shuichi Nawata, Masato Uchida, Yu Gu, Masato Tsuru, and Yuji Oie, Unsupervised Ensemble Anomaly Detection through Time-Periodical Packet Sampling, 13th IEEE Global Internet Symposium 2010, 6 pages, San

Diego, CA, USA, March 19, 2010.
③ 縄田 秀一, 内田 真人, Yu Gu, 鶴 正人, 尾家 祐二, ″時間周期的パケットサンプリングによる教師無しアンサンブル異常検出手法,″ 電子情報通信学会 情報ネットワーク研究会, 信学技法 Vol.109, No.449, pp.325-330(IN2009-198), 2010年3月4-5日(フェニックス・シーガイア・リゾート, 宮崎県宮崎市).

〔その他〕
http://www.ndrc.kyutech.ac.jp/~m.uchida

６．研究組織
研究代表者
内田 真人 (UCHIDA MASATO)
九州工業大学・ネットワークデザイン研究センター・准教授
研究者番号：20419617