様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　５　月　１７　日現在

機関番号：　３２５０３
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６３３０１１２

研究課題名（和文）人為的過誤と監視コストを低減するマン・マシン協調による異常トラヒック検出システム

研究課題名（英文）Anomaly Detection System Reducing Human Error and Measurement Cost Based on Man-Machine Collaboration

研究代表者

内田　真人（Uchida, Masato）

千葉工業大学・工学部・教授

研究者番号：２０４１９６１７

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：本研究では，監視対象ネットワークの状態を正常時のネットワーク状態を記述した基準モデルと比較するという非正常パターン検知型の異常トラヒック検知手法について検討する．基準モデルの学習においては，通常，所与のトラヒックデータにおける個々のパケットを専門家の手作業によって正常/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を用いる．本研究では，パケットサンプリングにおける情報損失特性を活用することで，この分類作業におけるヒューマンエラーに対して頑健な異常トラヒック検知について提案した．実トラヒックデータを用いた実験の結果，提案手法の有効性が示された．

研究成果の概要（英文）：This research focuses on an anomaly detection method that uses a baseline model describing the normal behavior of network traffic as the basis for comparison with the audit network traffic. In the anomaly detection method, an alarm is raised if a pattern in the current network traffic deviates from the baseline model. The baseline model is often trained using normal traffic data extracted from traffic data for which all instances (i.e., packets) are manually labeled by human experts in advance as either normal or anomalous. However, since humans are fallible, some errors are inevitable in labeling traffic data. Therefore, this research proposes a human error tolerant anomaly detection. The proposed method takes advantage of the lossy nature of packet sampling for the purpose of correcting/preventing human errors in labeling traffic data. By using real traffic traces, we show that the proposed method can better detect anomalies than the existing method.

研究分野：　情報ネットワーク，数理モデリング

キーワード：　異常トラヒック検出

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・複雑化に伴い，ネットワークを適切に制御・管理するためのトラヒック計測・分析技術の重要性が増している．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，平成 23～27 年度の第 4 期科学技術基本計画（総合科学技術会議）や平成 25 年版情報通信白書（総務省）の中で，安心・安全に情報通信技術を利用するための信頼性の高い情報セキュリティ技術の研究開発は重要な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（図１参照）．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．この方式では，異常トラヒックのパターンを登録し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高い効果を発揮する．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，ある程度の誤検出は避けられないものの，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優れた特徴を持つ．そこで本研究では，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した．

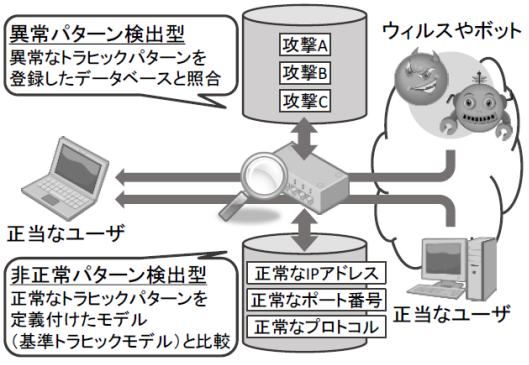


図１：異常トラヒック検出技術の分類

２．研究の目的

非正常パターン検出型の異常トラヒック検出技術を実現するためには，正常なトラヒックパターンを定義付けた基準トラヒックモデルの構築に用いる正常トラヒックデータの抽出と，監視対象のネットワークの状態を実時間で把握するために用いる実態トラヒックデータの計測が必要となる．しかしながら，正常トラヒックデータの抽出は通常，専門家の手作業により行われることが多く，膨大な手間と時間がかかるという問題がある．また，抽出作業における人為的過誤が避けられないという問題もある．そこで本研究では，マン・マシン協調という新たなコンセプトに基づく異常トラヒック検出システムについて検討し，これらの問題を解決することを目指した．

３．研究の方法

文献[1] では，専門家の手作業により正常トラヒックデータが抽出されている．すなわち，個々のパケットを専門家の手作業によって正常/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．そのため，このような手作業により個々のパケットにラベル付けする手法においては，専門家の知見が反映された基準モデルを用いた異常トラヒック検知が可能となる．しかしこの手法においては，専門家による手動抽出に伴うコストが発生し，手動抽出におけるヒューマンエラーに対処できない．一方，文献[2] では，時間周期的パケットサンプリングと呼ばれる計測手法を用いて正常トラヒックを機械的に自動抽出する手法が提案されている．この手法では，手動抽出に伴うコストやヒューマンエラーは原理的に発生しないが，専門家の知見を反映した基準モデルを構築できない．

そこで本研究では，文献[1, 2] の手法を併用することで，互いの利点を活かしながら欠点を補完する二つの手法を提案した．第一の手法は，時間周期的パケットサンプリングにより自動抽出された正常トラヒックデータに対して専門家のラベリングによる手動抽出を施す手法である．また，第二の手法は，専門家のラベリングにより手動抽出された正常トラヒックデータに対して時間周期的パケットサンプリングによる自動抽出を施す手法である．本研究においては，前者の手法を sl（sampling-and-labeling）法，後者の手法を ls（labeling-and-sampling）法と呼ぶことにする（図 2 参照）．

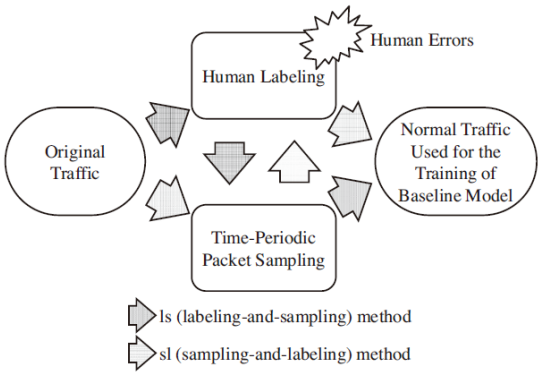


図 2：提案手法の概要

一方，sl 法や ls 法において実行される時間周期的サンプリングのサンプリング周期が確率的に決定されることから，これらの手法により抽出さ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検知性能は変

動することとなる．そこで本研究では，複数の基準モデルにおける検知結果を一つに集約することで検知性能の変動を抑制/活用することのできる，「平均（Ensemble)」，「敏感（Maximum)」，「慎重（Minimum)」の 3 つ手法を提案した．平均とは，複数の基準モデル間での検知結果を平均化して集約する方法である．敏感とは，各基準モデル間の検知結果のうち，一つでも異常と判断すれば，集約した検知結果としても異常と判断する方法である．慎重とは，各基準モデル間の検知結果のうち，一つでも正常と判断すれば，集約した検知結果としても正常と判断する方法である．

参考文献：
[1] Y. Gu, A. McCallum, and D. Towsley. Detecting anomalies in network traffic using entropy estimation. In Proc. of IMC 2005, pp.345-350, 2005.
[2] M. Uchida, S. Nawata, Y. Gu, M. Tsuru, and Y. Oie. Unsupervised ensemble anomaly detection using time-periodic packet sampling. IEICE Trans. Commun., E95-B(7), pp.2358-2367, 2012.

４．研究成果

〔異常トラヒック検知に関する研究〕

(1) 理論解析による性能評価

sl 法と ls 法において用いられている時間周期的パケットサンプリングとは，時刻 $T_n = t_1 + t_2 + \ldots + t_n$ [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トラヒック計測手法である（図 3 参照）．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．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状況においては，ls 法により抽出されたトラヒックデータよりも sl 法により抽出されたトラヒックデータの方が，高い割合で正常パケットを含むことを理論的に明らかにした．この概要を以下に示す．

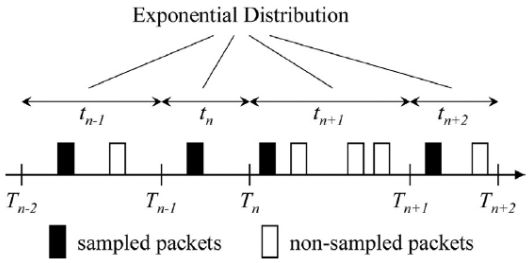


図 3：時間周期的パケットサンプリング

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，専門家による手動抽出においてパケットの分類を誤る確率（Flip Rate）を ε とする．このとき，本研究では，sl 法を用いたときにフロー i のパケットが抽出される確率を $p_i^{(sl)}$，ls 法を用いたときにフロー i のパケットが抽出される確率を $p_i^{(ls)}$ とすると，

$$\frac{p_2^{(sl)}}{p_1^{(sl)}} < \frac{p_2^{(ls)}}{p_1^{(ls)}} < \varepsilon \frac{\lambda_2}{\lambda_1}$$

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，ls 法よりも sl 法の方が低いこと，及び，いずれの手法を用いたとしても，オリジナルのトラヒックデータにおける割合よりも低くなることを意味している．

(2) 実データを用いた性能評価

本研究ではまず，専門家による手動抽出に誤りがある場合を想定し，sl 法と ls 法の有効性について評価した．手動抽出の誤りの形態としては，パケット単位での抽出誤りを想定した．

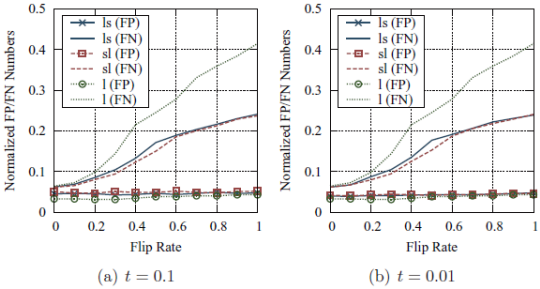
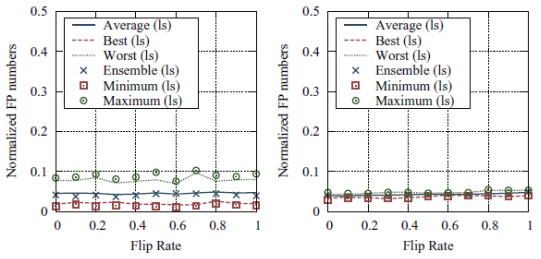


図 4：ls 法と sl 法における FPR と FNR

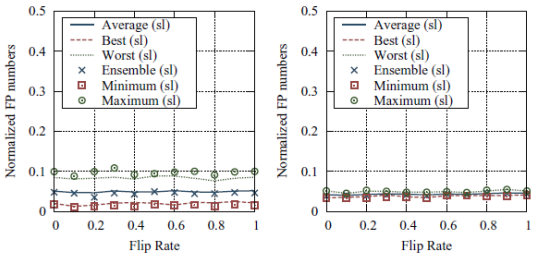
図 4 に，マサチューセッツ大学の対外接続回線で計測された実トラヒックデータを用いた評価結果を示す．図の横軸はパケット単位での抽出誤りが起こる確率 ε（Flip Rate）を表し，縦軸は異常トラヒックの見逃し率（FNR: Fales Negative Rate）と，異常トラヒックの誤検知率（FPR: Fales Positeve Rate）を表す．また図中の 1 は，専門家による手動抽出のみを行う手法を表す．これらの図より，提案手法を用いることで，抽出誤り確率の増加に伴う FNR の増加が抑制され，特に抽出誤り確率が 2〜3 割程度以下である場合は，抽出誤りが発生していない場合と同等の性能を達成可能であることが分かる．なお，本研究においては，異常トラヒックを正常トラヒックとして抽出するという抽出誤りを想定したため，抽出誤り確率の変化に FPR が大きく依存することはなかった．

次に，複数の基準モデルを用いた非正常パターン検知型異常トラヒック検知手法である，「平均（Ensemble)」，「敏感（Maximum)」，「慎重（Minimum)」の 3 つ手法の評価結果を図 5〜8 に示す．凡例の Average/Best/Worst は，複数の基準モデルの平均/最良/最悪性能を表している．これらの図より，Average/Best/Worst の性能が異なることから，サンプリングに伴う検知性能が確かに変動することを確認できる．また，「平均」を用いた場合はこの検知性能の変動が安定化することがわかる．さらに，「敏感/慎重」を用いた場合は，この検知性能の変動を活用することで，FPR/FNR を犠牲にした上で FNR/FPR を改善することが可能であることがわかる．このことは，異常トラヒック検知における検知感度をネットワーク管理者の運用ポリシーによって調整可能であることを意味する．



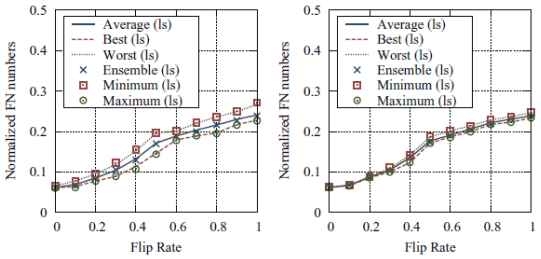
(a) $t = 0.1$　(b) $t = 0.01$

図 5： ls 法における FPR の比較



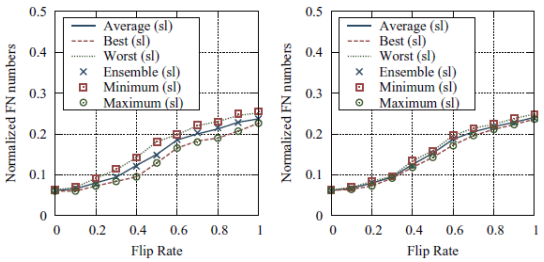
(a) $t = 0.1$　(b) $t = 0.01$

図 6： sl 法における FPR の比較



(a) $t = 0.1$　(b) $t = 0.01$

図 7： ls 法における FNR の比較



(a) $t = 0.1$　(b) $t = 0.01$

図 8： sl 法における FNR の比較

〔その他の研究〕

本研究課題においては，異常トラヒック検知に関する研究から派生した研究についても取り組んだ．

○教師なしアンサンブル学習に関する研究

複数の基準モデルを用いた異常トラヒック検知の理論的基礎を与えるために，複数の予測機構の統合によって予測能力の向上を図る機械学習の手法として知られるアンサンブル学習について検討した．具体的には，対称化カルバック情報量を背景とした教師なしアンサンブル学習を提案し，そのアルゴリズム構造を明らかにした．

○サンプルされた Wikipedia ネットワークの特性分析に関する研究

サンプリングが与える影響に関する理解を深めるために，ネットワークトラヒックではなくネットワークトポロジに対するサンプリングを施した場合における影響について検討した．具体的には，Wikipedia ネットワークを対象とし，それをサンプリングすることで得られる部分ネットワークの特徴について実データに基づいて分析した．

○電気通信事故の発生状況に関する統計分析に関する研究

ネットワークの安全性・信頼性の現状を把握するために，日本国内で発生した法令上の重大な電気通信事故の発生傾向や経年変化に関する統計分析を行った．この結果，通信事故の発生傾向は，サービス別，事業者別，要因別などにおいてそれぞれ異なる特性を示すことが明らかとなった．

○OD トラヒック行列推定に関する研究

ルータでの計測が容易である複数のネットワークフローを集約した流量から，個別のネットワークフロー流量の統計的特性を推定するための技術である OD トラヒック行列推定について検討した．特に，観測データのリサンプリングによる推定精度の向上を図る手法について初期検討を行った．

５．主な発表論文等

〔雑誌論文〕（計 2 件）

① Masato Uchida, "Human Error Tolerant Anomaly Detection Based on Time-Periodic Packet Sampling," Knowledge-Based Systems, Volume 106, pp. 242-250, August 2016. （査読有）

② Masato Uchida, "Unsupervised Weight Parameter Estimation for Exponential Mixture Distribution based on Symmetric Kullback-Leibler Divergence," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E98-A, No. 11, pp. 2349-2353, November 2015. （査読有）

〔学会発表〕(計 20 件)

① 加瀬 史門, 内田 真人, ″観測フローデータのリサンプリングによる OD トラヒック行列推定の精度向上,″ 電子情報通信学会 コミュニケーションクオリティ研究会, 信学技報 Vol.116, No.497, pp.37-42(CQ2016-117), 2017 年 3 月 6-7 日(九州大学, 福岡県福岡市).

② 大山 拓海, 内田 真人, ″Wikipedia ネットワークの成長過程と BA モデルの類似性について,″ 電子情報通信学会 コミュニケーションクオリティ研究会, 信学技報 Vol.116, No.497, pp.31-36(CQ2016-116), 2017 年 3 月 6-7 日(九州大学, 福岡県福岡市).

③ 加瀬 史門, 内田 真人, ″MDL 基準を用いたネットワークフロー流量分布の推定,″ 2016 年電子情報通信学会総合大会, B-11-6, 2016 年 3 月 15-18 日(九州大学, 福岡県福岡市).

④ Masato Uchida, ″Categorical Characteristics of Recent Serious Network Failures in Japan,″ INFORMS International Conference, Waikoloa, USA, June 12-15, 2016.

⑤ 石川 優樹, 内田 真人, ″電気通信事故の発生状況に関する事業者別・発生要因別の統計分析,″ 2016 年電子情報通信学会総合大会, B-11-5, 2016 年 3 月 15-18 日(九州大学, 福岡県福岡市).

⑥ 大石 悟史, 会川 諒太, 内田 真人, ″非正常パターン検知型異常トラヒック検知における基準モデルの高精度化,″ 2016 年電子情報通信学会総合大会, B-11-4, 2016 年 3 月 15-18 日(九州大学, 福岡県福岡市).

⑦ 会川 諒太, 大石 悟史, 内田 真人, ″複数の基準モデルを用いた非正常パターン検知型異常トラヒック検知,″ 2016 年電子情報通信学会総合大会, B-11-3, 2016 年 3 月 15-18 日(九州大学, 福岡県福岡市).

⑧ 野口 雄輝, 内田 真人, ″一般化平均を用いた記事類似度による適応的な Wikipedia 検索,″ 2016 年電子情報通信学会総合大会, B-11-2, 2016 年 3 月 15-18 日(九州大学, 福岡県福岡市).

⑨ 榎波 早敏, 内田 真人, ″Wikipedia ネットワークのリンク関係推定に関する一考察,″ 2016 年電子情報通信学会総合大会, B-11-1, 2016 年 3 月 15-18 日(九州大学, 福岡県福岡市).

⑩ 高知尾 遼, 岩井 智宏, 内田 真人, ″重大な電気通信事故の深刻度レベルに関する分析,″ 2015 年電子情報通信学会総合大会, B-11-13, 2015 年 3 月 10-13 日(立命館大学, 滋賀県草津市).

⑪ 岩井 智宏, 高知尾 遼, 内田 真人, ″重大な電気通信事故の発生状況に関する経年変化の分析,″ 2015 年電子情報通信学会総合大会, B-11-12, 2015 年 3 月 10-13 日(立命館大学, 滋賀県草津市).

⑫ 近藤 美紗希, 内田 真人, ″Wikipedia における記事情報量分布に関する分析,″ 2015 年電子情報通信学会総合大会, B-11-11, 2015 年 3 月 10-13 日(立命館大学, 滋賀県草津市).

⑬ 榎波 早敏, 内田 真人, ″サンプルされた Wikipedia ネットワークにおける記事引用関係,″ 2015 年電子情報通信学会総合大会, B-11-10, 2015 年 3 月 10-13 日(立命館大学, 滋賀県草津市).

⑭ Masato Uchida, ″Tight Lower Bound of Generalization Error in Ensemble Learning,″ SCIS & ISIS 2014, pp.1130-1133, Kitakyushu, Japan, December 3-6, 2014.

⑮ Masato Uchida, ″Unsupervised Weight Parameter Estimation for Exponential Mixture Distribution based on Symmetric Kullback-Leibler Divergence,″ SCIS & ISIS 2014, pp.1126-1129, Kitakyushu, Japan, December 3-6, 2014. (Best Poster Award)

⑯ 榎波 早敏, 内田 真人, ″非正常パターン検知型異常トラヒック検知におけるヒューマンエラーへの対処に関する研究,″ 2014 年電子情報通信学会ソサイエティ大会, B-11-41, 2014 年 9 月 23-26 日(徳島大学, 徳島県徳島市).

⑰ 石川 優樹, 内田 真人, ″非正常パターン検知型異常トラヒック検知における人的作業コスト抑制に関する研究,″ 2014 年電子情報通信学会ソサイエティ大会, B-11-40, 2014 年 9 月 23-26 日(徳島大学, 徳島県徳島市).

⑱ 野口 雄輝, 内田 真人, ″非正常パターン検知型異常トラヒック検知におけるネットワーク監視コストの軽減に関する研究,″ 2014 年電子情報通信学会ソサイエティ大会, B-11-39, 2014 年 9 月 23-26 日(徳島大学, 徳島県徳島市).

⑲ Masato Uchida, ″Human Error Tolerant Anomaly Detection using Time-Periodic Packet Sampling,″ WIND 2014, 6 pages, Salerno, Italy, September 10-12, 2014.

⑳ 内田 真人, ″時間周期的パケットサンプリングを用いたヒューマンエラーに頑健な異常トラヒック検知,″ 電子情報通信学会 コミュニケーションクオリティ研究会, 信学技報 Vol.114, No.131, pp.7-12(CQ2014-16), 2014 年 7 月 10-11 日(大阪大学, 大阪府豊中市).

〔その他〕

ホームページ等

http://www.uchida-lab.jp

６．研究組織

(1)研究代表者

内田　真人（UCHIDA, Masato）
千葉工業大学・工学部・教授
研究者番号：20419617