# 科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　１２　日現在

機関番号：　１１４０１
研究種目：　基盤研究(C)
研究期間：　2011～2013
課題番号：　２３５０００７７

研究課題名（和文）ハースト空間を用いた異常トラフィック検知方法に関する研究

研究課題名（英文）Study of Anomaly Detection Method using Hurst Space.

研究代表者
高橋　秋典（Takahashi, Akinori）

秋田大学・工学（系）研究科（研究院）・助教

研究者番号：９０２３６２５８

交付決定額（研究期間全体）：（直接経費）　　1,900,000円、（間接経費）　　570,000円

研究成果の概要（和文）：本研究では，トラフィック時系列に現れる非定常的特徴を定量化するトラフィック特性，ならびにこの特性を用いた周期的時系列に対する異常検知法を提案した．提案手法は，周期的特徴を持つ長期的ポートスキャン攻撃などの低レート攻撃の検知に有効であることを示した．さらに，ネットワーク管理者を支援するという観点から，特性変化の視認性を高めるためハースト空間を用いた可視化手法を提案した．

研究成果の概要（英文）：This study proposes a newly defined expression of traffic characteristic to quantify a non-stationarity of the Internet traffic time series, and an anomaly detection method for periodic time series using that characteristic as well. The proposed method showed that it was effective for the detection of low-rate attacks having such a cycle as long-term port scan.Furthermore, from the viewpoint of supporting a network manager, we proposed helpful visualization methods to the manager by using the Hurst space to step up the visibility of the characteristic changes.

研究分野：　総合領域

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：　ネットワークトラフィック　異常検知　自己相似性　ハーストパラメータ　R/S Pox レッグライン特性
トラフィック可視化手法

１．研究開始当初の背景

近年，インターネットには多様で利便性の高いトラフィックに加え，悪意あるトラフィックも疎通し，輻輳崩壊やサービス品質劣化と言った諸問題が発生することから，その対策が重要課題となっている．このとき現実的な方法として，異常なトラフィックが発生したときのトラフィック量変化を検知する方法があるが，インターネットトラフィックは自己相似性に起因するバーストトラフィックが発生するため，正常範囲のトラフィック変化を誤って異常と判断してしまう不都合が予想される．

この自己相似性の程度を表すハースト数は，トラフィック事象変化に対して影響を受けることが確認されているが，積極的に異常検知に対する指標として適用する試みは見受けられない．特に，周期性を含んだトラフィックに対して特徴的変化が生じることから，この特性を用いた異常検知手法を提案した．さらに特性変化の特徴を容易に認識することが可能となる可視化表現を検討することにより，管理者支援システムの構築を目指す．

２．研究の目的

本研究では，ハースト数推定法の一つである R/S 解析法に着目し，トラフィック事象変化に対する R/S Pox Diagram の特徴的プロット形状の関係を明らかにして，そこから得られる特徴量を用いた異常検知手法を新たに確立する．さらに，特徴量を 3 次元空間にマッピングすることで異常トラフィックを認識可能とするハースト空間による可視化手法について検討を行うことを目的とする．

３．研究の方法

（1）トラフィック時系列に対する R/S Pox Diagram の特徴調査

非定常的に発生する異常トラフィックと R/S Pox Diagram の関係を検討するため，実ネットワーク環境より計測されたパケットトラフィックデータを測定単位時間毎に到着したパケット数に変換したトラフィック時系列データを用いて R/S Pox Diagram を導出したときのプロット形状を調査する．さらに，どんな非定常性に影響があるかを調査するため，定常時系列として FGN(Fractional Gaussian Noise)を利用して非定常性を重畳させたシミュレーション時系列を作成する．非定常性には，突発的トラフィック量の増減を表すレベルシフト，また時間間隔をおいて到着するときに現れる周期性を検討する．

（2）特徴的プロット形状の定量化および性能評価

（1）で検討した特徴的プロット形状を定量化し，非定常性を表現できる特徴量を新たに提案する．R/S Pox Diagram より推定されるハースト数は，最少二乗誤差より求められるプロット点群の回帰直線の傾きで表されるが，特徴的プロット形状では複数の傾きが顕現する．そこで，プロット点群を上限点群，平均点群，下限点群に分け，それぞれを用いて傾きを推定する手法を検討する．また，プロット点群の前・後半で傾きが変化する場合もあるため，推定範囲をそれぞれ設けて特徴量を推定する．

これらの特徴量の性能評価として，非定常性のパラメータを変化させたときの各特徴量の変化を調査する．この特徴量を用いることで，非定常性を有する異常トラフィックの検知が可能と考えられる．

（3）異常トラフィック検知法の提案と評価

実ネットワークトラフィックデータを計測しながら特徴量を演算し，かつ異常検知を行う手法を検討する．パケットキャプチャーライブラリおよびリングバッファを用いたマルチスレッド処理によってトラフィック時系列データを生成しながら，高速に演算するアルゴリズムの開発を行う．さらに，外部に影響を与えない仮想ネットワーク環境を用いて疑似攻撃トラフィックを実施したときの検知性能を評価する．

（4）トラフィック可視化手法の検討

（1）～（3）で検討した異常検知手法をより視覚的に認知しやすい表現方法を検討する．具体的に，上限点群，平均点群，下限点群から得られる特徴量を 3 次元空間の一点に対応させたハースト空間による可視化手法について検討する．

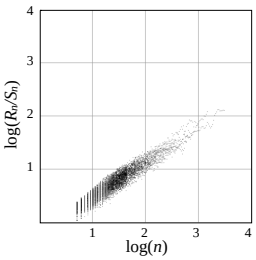
４．研究成果

突発的にパケット量が増加するレベルシフトトラフィック，および間欠的にパケットが到着することで周期性を示すトラフィックを想定した非定常的変化を重畳させたシミュレーション時系列を生成し，R/S Pox Diagram の特徴的プロット形状の解析を行った．その結果を例を図 1 に示す．図 1(b)に示すように，レベルシフト時系列に対しては R/S Pox Diagram の上限点群の傾きが大きくなる傾向を示した．また，図 1(c)に示すように，周期的時系列に対してはプロット点群の傾きが一方向ではなく，途中から折れ曲がり二方向の傾きを呈した．さらに，この折れ曲がるポイントは，R/S 解析法における任意長区間と重畳させた非定常時系列の周期とほぼ一致していることが観測された．つまり，このポイントを定量化することにより，時系列の周期推定が可能となると推測される．

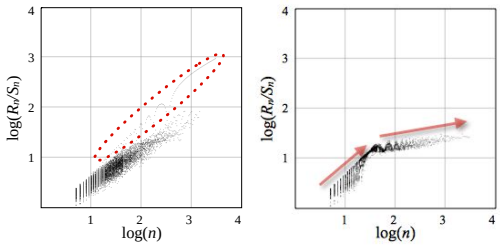
この特徴を定量化するため，計画にあった提案特徴量 $H_{\mathrm{Sup}}$，$H_{\mathrm{Inf}}$ を拡張し，R/S Pox Diagram プロット点群の前半部分と後半部分における上限点群，下限点群，平均点群から最少二乗法を用いて導出される傾きを新たな特徴量として検討した．そのときの特徴量を図 2 に示す．このプロット形状は人体の脚

部と形状が似ていることからR/S Pox レッグライン特性と名付けた．

シミュレーション時系列に対する評価を行ったところ，明確な変化傾向を示すことが観測された．特に周期的時系列に対する特徴は，攻撃者が行うポートスキャンにおいて，検知しにくくするために少量の調査パケットを間欠的に送信する長期的ポートスキャン攻撃の検知に有効であると推測される．




(a)定常状態




(b)レベルシフト時系列　(c)周期的時系列

図 1. R/S Pox Diagram のプロット形状

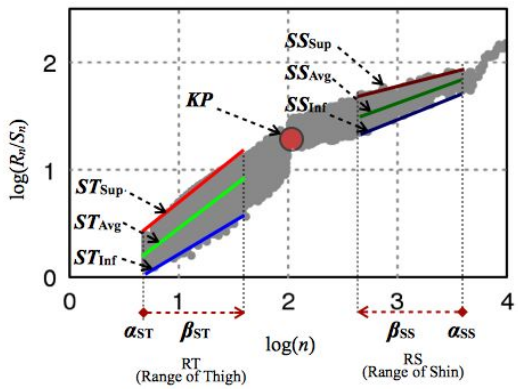



図 2. R/S Pox レッグライン特性

実際のキャンパスネットワークから取得したパケットトラフィックデータに対してR/S Pox レッグライン特性の解析を実施して，非定常的に発生する異常トラフィックに対する提案特性を用いた検知手法の可能性を検討した．

まず，pcap ライブラリおよびリングバッファを用いたマルチスッド処理によって実時間でパケットデータから時系列データを生成するモジュールを開発し，それを用いた実時間によるR/S Pox レッグライン特性解析プログラムを作成した．キャンパスネットワークに適用した結果，パケットロスなく解析が行えることを確認できた．

次に，トラフィック事象変化点検出アルゴリズムの検討として，R/S Pox レッグライン特性を用いて，周期的時系列の周期と同等の値を呈するプロット点群の折れ曲がるポイントを推定する周期推定手法を考案した．これを用いて，実トラフィックデータに混在する長期的ポートスキャン攻撃トラフィックの周期性を検知できることを明らかにした．

さらに，R/S Pox レッグライン特性の傾きの変移を捉えることで，観測時系列における攻撃トラフィックの状態（攻撃開始，攻撃中，攻撃終了）を推測する手法の検討も行った．具体的には傾きの特徴量に対してニューラルネットワークを用いたパターン認識を行うことで，状態判別を実現した．

R/S Pox レッグライン特性の実用性を考慮したトラフィック可視化システムの検討を行った．具体的には，特徴量の 3 値を用いたハースト空間を定義し，現在のトラフィック特性を空間内の 1 点にマッピングする可視化手法を提案した．ハースト空間を用いた可視化手法の概要を図 3 に示す．このように，R/S Pox レッグライン特性の 2 つの導出範囲をハースト空間にマッピングすると，定常時には 2 点間の距離が近いのだが，周期性を含む異常トラフィックが混入すると，特徴量 SS の 1 点が原点に近づき，2 点間の距離が離れることが確認でき，異常性の存在が認識可能となった．

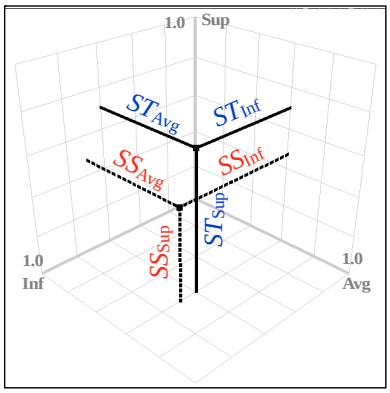



図 3. ハースト空間を用いた可視化手法

本研究の成果により，目的である R/S 解析法に基づいたトラフィック事象変化を検知するトラフィック特性，および異常状態を認識可能とする可視化手法の提案が実現できたと考える．

## 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）

〔雑誌論文〕（計 1 件）

(1) 高橋秋典，五十嵐隆治，上田浩，岩谷幸雄，木下哲男，"R/S Pox レッグライン特

性", 情報処理学会論文誌, Vol.54, No.6, pp.1761-1770, 2013, 査読有.

〔学会発表〕(計 19 件)

(1) 加賀谷享諒, 高橋秋典, 五十嵐隆治, 上田浩, 岩谷幸雄, 木下哲男：R/S Pox レッグライン特性を用いた異常検知に関する研究, 平成 25 年度日本知能情報ファジィ学会東北支部研究会, 秋田市, 2014 年 3 月 7 日, 査読無.

(2) 竹原里紗, 高橋秋典, 五十嵐隆治, 上田浩, 岩谷幸雄, 木下哲男：フロー単位のパケット比率に着目したポートスキャン検知に関する研究, 平成 25 年度日本知能情報ファジィ学会東北支部研究会, 秋田市, 2014 年 3 月 7 日, 査読無.

(3) 杉澤知, 高橋秋典, 五十嵐隆治, 上田浩, 岩谷幸雄, 木下哲男, 奈須野裕：フロー量閾値設定のトラフィック特性の同定に関する研究, 平成 25 年度情報処理学会東北支部研究会, 秋田市, 2013 年 12 月 2 日, 査読無.

(4) 杉澤知, 高橋秋典, 五十嵐隆治, 上田浩, 岩谷幸雄, 木下哲男, 奈須野裕：フロー量閾値設定のトラフィック特性の同定に関する研究, 平成 25 年度電気関係学会東北支部連合大会, 福島市, 2013 年 8 月 22 日, 査読無.

(5) 藤井俊, 五十嵐隆治, 高橋秋典：区分的周辺分布によるトラフィック特性の同定, 平成 25 年度電気関係学会東北支部連合大会, 福島市, 2013 年 8 月 22 日, 査読無.

(6) 高橋秋典, 五十嵐隆治：情報セキュリティーポリシーを考慮したトラフィックデータ統計情報提供システムの試作, 平成 25 年度電気関係学会東北支部連合大会, 福島市, 2013 年 8 月 22 日, 査読無.

(7) 加賀谷享諒, 高橋秋典, 五十嵐隆治, 上田浩, 岩谷幸雄, 木下哲男：R/S Pox レッグライン特性を用いたトラフィック状態推定法に関する研究 , 平成 25 年度電気関係学会東北支部連合大会, 福島市, 2013 年 8 月 22 日, 査読無.

(8) 加賀谷享諒, 高橋秋典, 五十嵐隆治, 上田浩, 岩谷幸雄, 木下哲男, "R/S Pox レッグライン特性を用いたトラフィック状態判別法に関する研究", 第 75 回情報処理学会全国大会, 仙台市, 2013 年 3 月 7 日, 査読無.

(9) 小西航, 高橋秋典, 五十嵐隆治, 上田浩, 岩谷幸雄, 木下哲男, "ネットワークトラフィック変化検知のための視覚的表現法に関する研究", 平成 24 年度 第 1 回情報処理学会東北支部研究会, 秋田市, 2012 年 12 月 3 日, 査読無.

(10) 中尾拓也, 高橋秋典, 五十嵐隆治, 上田浩, 岩谷幸雄, 木下哲男, "長期的ポートスキャントラフィックのパターン解析に関する研究",平成 24 年度 第 1 回情報処理学会東北支部研究会, 秋田市, 2012 年 12 月 3 日, 査読無.

(11) 高橋秋典, 五十嵐隆治, 上田浩, 岩谷幸雄, 木下哲男, "R/S Pox レッグライン特性", 第 11 回情報科学技術フォーラム, 小金井市, 2012 年 9 月 5 日, 査読有.

(12) 中尾拓也, 高橋秋典, 五十嵐隆治, 上田浩, 岩谷幸雄, 木下哲男, "長期的ポートスキャントラフィックのパターン解析に関する研究", 平成 24 年度電気関係学会東北支部連合大会, 秋田市, 2012 年 8 月 30 日, 査読無.

(13) 小西航, 高橋秋典, 五十嵐隆治, 上田浩, 岩谷幸雄, 木下哲男, "Pox Diagram 特徴量空間を用いたトラフィック変化検知", 平成 24 年度電気関係学会東北支部連合大会, 秋田市, 2012 年 8 月 30 日, 査読無.

(14) 杉澤知, 五十嵐隆治, 高橋秋典, 上田浩, 岩谷幸雄, 木下哲男, 奈須野裕, "フロー量閾値設定のトラフィック特性の同定に関する研究", 平成 24 年度電気関係学会東北支部連合大会, 秋田市, 2012 年 8 月 30 日, 査読無.

(15 )小西航, 高橋秋典, 五十嵐隆治, 上田浩, 岩谷幸雄, 木下哲男, "ネットワークトラフィック変化検知のための視覚的表現法に関する検討", 情報処理学会第 57 回 CSEC･第 17 回 IOT 合同研究発表会, 秋田市, 2012 年 5 月 10 日, 査読無.

(16) 鬼沢彩人, 高橋秋典, 五十嵐隆治, 上田浩, 岩谷幸雄, 木下哲男, 奈須野裕, "統計的な変化点検出法によるトラフィック異常検知", 平成 23 年度 第 2 回情報処理学会東北支部研究会, 秋田市, 2011 年 12 月 5 日, 査読無.

(17) 鬼沢彩人, 高橋秋典, 五十嵐隆治, 上田浩, 岩谷幸雄, 木下哲男, 奈須野裕, "統計的な変化点検出法によるトラフィック異常検知", 平成 23 年度電気関係学会東北支部連合大会, 多賀城市, 2011 年 8 月 25 日, 査読無.

(18) 中尾拓也, 高橋秋典, 五十嵐隆治, 上田浩, 岩谷幸雄, 奈須野裕, 木下哲男, "仮想マシンを用いたシミュレーショントラフィック生成に関する研究", 平成 23 年度電気関係学会東北支部連合大会, 多賀城市, 2011 年 8 月 25 日, 査読無.

(19) 小西航, 高橋秋典, 五十嵐隆治, 上田浩, 岩谷幸雄, 木下哲男, 奈須野裕, "長期的スキャン攻撃の周期性に着目した異常検知法に関する研究", 平成 23 年度電気関係学会東北支部連合大会, 多賀城市, 2011 年 8 月 25 日, 査読無.

６．研究組織

(1)研究代表者

高橋　秋典（TAKAHASHI, Akinori）
秋田大学・大学院工学資源学研究科・助教
研究者番号：90236258