科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　１６　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：　２３５０００７６

研究課題名（和文）Ｒ／Ｓポックスダイアグラムの散布形状によるトラフィックの異常検知

研究課題名（英文）Network Traffic Anomaly Detection Utilizing the Dispersion of R/S Poxdiagram

研究代表者
五十嵐　隆治（Igarashi, Ryuji）

秋田大学・工学（系）研究科（大学院）・教授

研究者番号：０００９１７８６

交付決定額（研究期間全体）：（直接経費）　　3,400,000円、（間接経費）　　1,020,000円

研究成果の概要（和文）：　現在重要なインフラとなっているインターネット上で悪意あるトラフィックが疎通した場合、これは異常トラフィックとして検知できる。インターネットトラフィックはランダム時系列であり、異常トラフィックが混在していないときには2次の自己相似過程に従っている。Ｒ／Ｓポックスダイアグラムはこの自己相似パラメータ推定に用いられるものであるが、異常トラフィック混在時には独特な散布形状を呈する。　本研究ではこの散布形状を異常トラフィック検知に援用し、異常トラフィックを検知し得ることを見出した。

研究成果の概要（英文）：Over the Internet many kinds of malicious traffic are superimposed on the normal flow. In those cases, pieces of malicious traffic are detected as an anomaly in the traffic flow. It is well known that the Internet traffic obeys a selfsimilarity and the degree of the selfsimilraity is estimated by an R/S pox diagram. In case anomaly is superimposed in the traffic, the shape of the R/S pox diagram provides characteristic dispersions. In this study the author could successfully apply the characteristic dispersion of the pox diagram to detect the traffic anomaly.

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：　ポートスキャン　異常トラフィック検知　R/S解析　ポックスダイアグラム　パワースペクトル　ペリオドグラム

１．研究開始当初の背景

(1)インターネット上で疎通しているトラフィックは自己相似性を呈する場合があることはよく知られている。さらに，ネットワークが輻輳と非輻輳との臨界状態にあるときに自己相似性を呈するという指摘もなされている。

(2)インターネット上では悪意あるトラフィックも疎通し，このようなときの疎通トラフィックフローは異常状態を呈する。悪意あるトラフィック検知の手法はシグネチャ方式と統計的方式に大別されるが，日々新種のウィスルやワームが播種されている状況では，トラフィック異常を検知する手法はシグネチャ方式より検知率が劣る統計的方式も有力な検知法である。

(3)異常トラフィックが重畳されていない場合のトラフィックフローは自己相似パラメータHにより特徴付けられる。自己相似パラメータは統計量であり，この推定法として従来複数の方法が提案されている。実トラフィックが理論的な 2 次の自己相似過程，すなわち長期依存過程に従っているときには統計量としてのHの信頼帯の把握は重要であり，Whittle Estimator による推定は有用である。しかし実トラフィックは常に 2 次の自己相似過程に従っているとは限らず，自己相似過程からの推移の把握も容易なグラフ的推定法を用いる方が有為な場合が多い。

(4)自己相似パラメータのグラフ的推定法の一つとして R/S ポックスダイアグラムを用いる方法がある。R/S ポックスダイアグラムは古くはナイル川流域の流量推定のために H. E. Hurst が採用した方法で，その後 B. B. Mandelbrot らにより数学的な基礎付けがなされた方法である。長期依存性を有する時系列に，調和関数による周期性を重畳させた場合の R/S ポックスダイアグラム形状の変化に関しては既に Mandelbrot らがシミュレーション的な検討を実施していたが，系統的な検討は未だ実施されてはいなかった。

２．研究の目的

(1)上述の背景より，統計的手法による異常トラフィック検知法の提案は有用であることがわかる。本研究では，悪意あるトラフィックが流入した場合にはトラフィックフローに急激なレベル変化，すなわちレベルシフトが重畳されることに注目し，レベルシフト検知により異常トラフィックを検知する手法を探ろうとするものである。

(2)悪意あるトラフィックのうちサーバー等への侵入を意図するものは事前にポートスキャンを行うので，この場合のトラフィック異常は周期的なレベルシフト重畳として観測される。このような周期的レベルシフト検知も本研究の目的とした。

３．研究の方法

(1)異常トラフィックとして，単純なレベルシフト重畳が存在する場合の R/S ポックスダイアグラムが特徴的な散布形状，特にその分布が上方に大きく開くことを著者らは既に見出していた。本研究では異常検知の感度も勘案しつつ，R/S ポックスダイアグラムの散布程度を解析，実験およびシミュレーションにより評価する。

(2)異常トラフィックとしてのレベルシフトは，統計的には変化点検知の問題として取り扱える。研究においては，変化点検知の観点から CUSUM 法との対比も実施してみる。ここでもシミュレーショントラフィックを用いるが，定常トラフィックが 2 次の自己相似過程に従っている場合を考慮し，シミュレーション時系列には FGN（Fractional Gaussian Noise）を採用する。

(3)ポートスキャントラフィックは周期的レベルシフトの重畳として把握できる。研究ではシミュレーションならびに実トラフィックを用いた R/S ポックスダイアグラムの散布特徴の同定を試みてみる。

４．研究成果

(1)R/S ポックスダイアグラムの計算式は決定論的な時系列に対しても適用可能で，このときの計算法を単純レベルシフトに適用した結果が図１である。図 1(a)に示したのが決定論的な単純レベルシフト重畳に対する R/S ポックスダイアグラムの拡がり，図 1(b)がシミュレーションランダム時系列にレベルシフトを重畳させた場合で，このときのダイアグラムの拡がりは(a)に示した理論解析との一致が得られている。

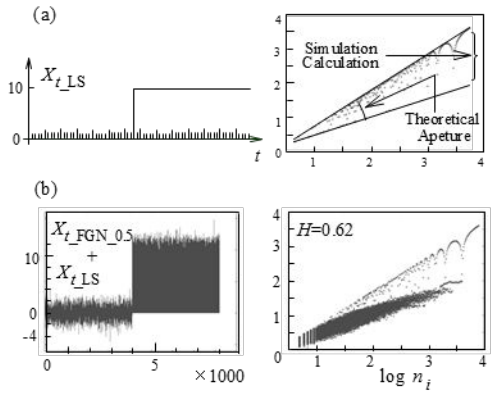

図１　レベルシフト重畳時の R/S ポックスダイアグラム散布形状．(a) 決定論的レベルシフト重畳時，(b) ランダム時系列にレベルシフトを重畳させた場合．

(2)上述(1)を踏まえ，シミュレーショントラフィックによるレベルシフト重畳が時系列内でどのように観測されるのかを確認したシミュレーション結果が図 2 に示されたもの

である。図 2 に例示した単一レベルシフト重畳は DoS，DDoS などのフラッド攻撃に対応するシミュレーションで，一般的にはレベルシフトフローの流入，継続，終了となり，フロー流入時と終了時にレベルシフトが観測される。統計的にはこれは変化点の介在ということになる。図 2 に示した結果は，トラフィック時系列にレベルシフトが重畳された場合，R/S ポックスダイアグラムの拡がりにより，その変化点を明確に検知できることを示したものである。

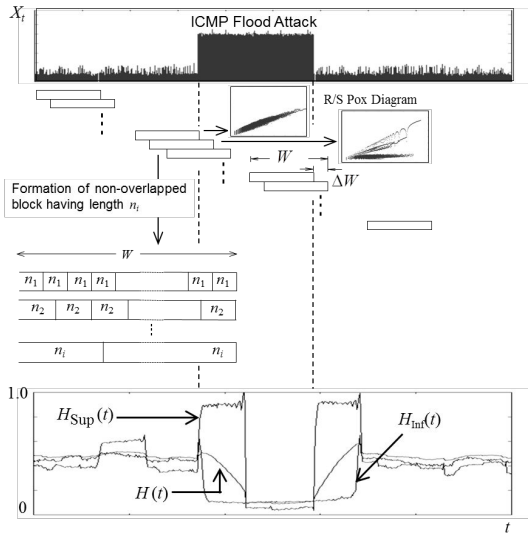

図 2　レベルシフト重畳により変化点が存在する場合の R/S ポックスダイアグラム散布形状の変化.

図 2 より，変化点を R/S 統計量の計算区間に含むときの R/S ポックスダイアグラムの拡がりは明確にレベルシフトを検知していることが確認できる。さらに図 2 のような単純レベルシフト重畳の場合，上述(1)の解析により，ランダムトラフィックの平均レベルをわずかに超えただけでもダイアグラムの拡がりが得られることを著者らは確認していて，この場合の変化点検知感度は高くなることも確かめている。

(3) R/S ポックスダイアグラムの拡がりによる変化点検知感度の優位性は図 3 より明らかである。図 3 の下部は変化点検知の統計的方法である CUSUM 法適用時の決定関数 g_t の変化を示したもので，ポックスダイアグラムの拡がりを示す指標 H_{S_sup} が CUSUM 法適用時の決定関数 g_t より小なるレベルシフトに対し急峻な変化を示していることがわかる。図 3 に認められる特質は，ランダム時系列に重畳されるレベルシフトの振幅 A がランダム過程の分散 V に比して小なる場合でも十分な応答を示していることである。図 3 の例によると CUSUM 法での決定関数 g_t は，ポックスダイアグラムの拡がりが十分に応答する V=1 に対し殆ど応答を示していないことがわかり，本研究での R/S ポックスダイアグラムの援用法の有効性をうかがえる。

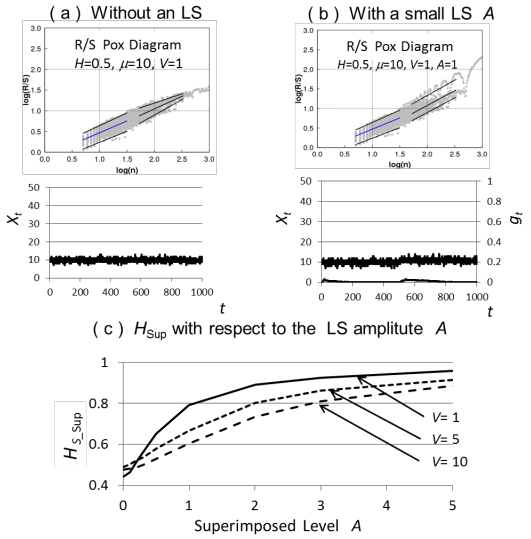

図 3　R/S ポックスダイアグラムの拡がりによる変化点検知感度が CUSUM 法によるそれよりも優位であることを確認した結果．(a)はレベルシルトがないときのポックスダイアグラム，(b)は振幅 A が A=1 のときのポックスダイアグラムの拡がりを示す指標 H_{S_sup} と CUSUM 法における決定関数 g_t の変化．(c)がランダム過程の分散 V を V=1，5，10 と変化させた場合の H_{S_sup} の変化の様子。レベルシフト A が A=0.1 でも H_{sup} は明確な変化を呈している．

(4) R/S ポックスダイアグラムは単純なレベルシフトのみならず，周期的なレベルシフト重畳時にも特徴的な変化を呈する。これは重畳された周期に相当する時間のところで膝を曲げたような形で折れ曲がることに因み，著者らはポックスレッグライン特性と命名した。この特徴は図 4 に示すように，折れ曲り点（KP）に対応する時間が流入する周期的トラフィックの周期に対応することである。

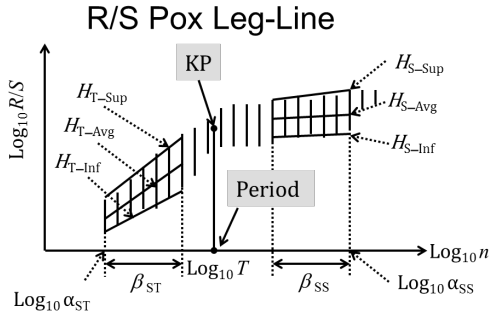

図 4　周期的なレベルシフト重畳に対する R/S ポックスダイアグラムの変化．脚部の折れ曲がりに似た形状に因み，ポックスレッグライン特性と命名.

(5) 各種の周期的異常トラフィック重畳に対するシミュレーション結果を図 5 に示す。サイン波的な重畳に対しても，また方形波的な重畳に対しても同様に応答し，且つ対応する周期は両波形に対して一致している。この性質は，サーバーへの侵入への前段階でポートスキャンを試みるようなトラフィックを異常検知として検出するような応用へは有為な方法となる。このように自己相似パラメータ推定の方法を援用できるというのは新たな知見である。

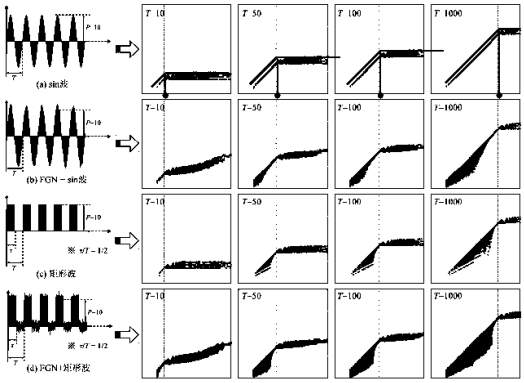

図 5　サイン波ならびに方形波的な周期的レベルシフト重畳に対する R/S ポックスダイアグラムの変化．レッグライン特性の膝部（KP）が，サイン，方形の両流入レベルシフト波形の周期に一致していることが読み取れる．

通常の信号解析における周波数解析ではフーリエパワースペクトルが広く用いられていて，著者らもこの方法を適用してみた。その結果，フーリエ解析では重畳された周期的レベルシフト以外にも複数の周期を検知し，レッグライン特性の援用に対する特段の優位性は示さなかった。この様子を図 6 に示す。

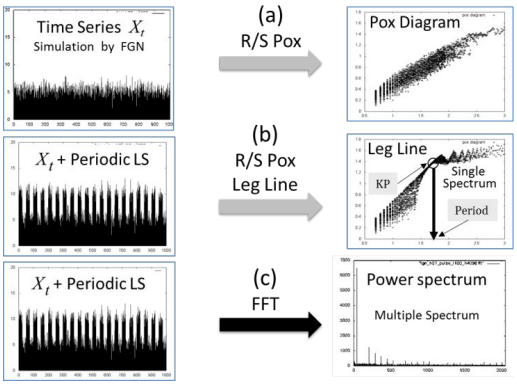

図 6　R/S ポックスレッグラインおよびフーリエパワースペクトルによるポートスキャン周期検知のシミュレーション結果．FFT では重畳された周期以外の複数周期を検出してしまうのに対し，R/S ポックスレッグライン特性では重畳させた周期のみ検知できていることが明確に読み取れる．

(6)以上(1)～(5)の成果は以下のように総括できる。すなわち，
①単純レベルシフトとなる異常トラフィックに対する R/S ポックスダイアグラムの拡がりは，異常検知に対する十分な検知感度を有していて，統計的な変化点検知法として広く用いられている CUSUM 法より優位となる場合がある。
②R/S ポックスダイアグラムの特徴的変化は，周期的なレベルシフトを有するポートスキャンのような異常トラフィック検知に対しても有効で，ダイアグラムの折れ曲がり点検知により流入する異常トラフィックの周期の同定が可能であることを見出した。
③周期同定であれば従来のフーリエ解析による結果も検討してみる必要がある。シミュレーショントラフィックにより両法の比較を実施してみた結果，同一入力に対し R/S ポックスレッグライン特性では単一の周期同定が可能だったのに反し，FFT パワースペクトル図では複数スペクトルを検知してしまい，本研究での提案法である R/S ポックスレッグライン特性の優位性を確認できた。

(7)今後は本研究で得られた R/S ポックスレッグライン特性と併用する形で CUSUM 法や FFT パワースペクトルを用いたトラフィック同定，特に異常検知の観点からの研究を進めて行く。ただし，レベルシフトなどのフロー異常以外にもインターネットの特異な使用に基づく輻輳崩壊前駆現象などの検知には，自己相似パラメータ推定法のひとつであるペリオドグラム法の観点から，FFT パワースペクトルによる同定は有為である。同様に輻輳状態の把握には物理学での相転移現象解析に用いられる方法も有効と考えられ，これら複数の方法を援用しつつトラフィック特性の同定を試みて行くことが今後の課題である。

５．主な発表論文等

〔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，査読有，Vol.54，No.6 pp.1761-1770，2013．

〔学会発表〕（計 23 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，査読無，10，2014．
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，査読無，11，2014．
③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 年度日本知能情報ファジィ学会東北支部研究会，査読無，12，2014．
④グェン・スァン・ルーン，五十嵐隆治，高橋秋典，相転移モデルの閾値超過持続時間分布を援用した異常トラフィック検知法の提案に関する研究，平成 25 年度日本知能情報ファジィ学会東北支部研究会，査読無，09，2014．
⑤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講演論文集，査読無，1F03，2013．
⑥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講演論文集, 査読無, 1F09, 2013.
⑦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講演論文集, 査読無, 1F04, 2013.
⑧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, 査読無, No.6, 2013.
⑨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, 情報処理学会第 75 回全国大会講演論文集, 査読無, 3Z-2, pp.3-537－3-538, 2013.
⑩高橋秋典, 五十嵐隆治, 上田浩, 岩谷幸雄, 木下哲男, R/SPox レッグライン特性, 第 11 回情報科学技術フォーラム(FIT2012)講演論文集, 第 4 分冊, 査読有, pp.9-16, Sep.2012.
⑪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 合同研究発表会研究報告, 査読無, Vol.2012-IOT-17, No.1, pp.1-6, 2012.
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講演論文集, 査読無, 2F-16, 2012.
⑬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講演論文集, 査読無, 2F-17, 2012.
⑭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講演論文集, 査読無, 2F-18, 2012.
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研究, 平成 24 年度情報処理学会東北支部研究会, 査読無, 2012.
⑯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 年度情報処理学会東北支部研究会, 査読無, 2012.
⑰近藤大智, 阿部正弥, 奈須野裕, 高橋秋典, 五十嵐隆治, ＬＡＮの対外トラヒックの解析と考察, 平成 23 年度電気・情報関係学会北海道支部連合大会講演論文集, 査読無, 2011.
⑱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講演論文集, 査読無, 1C07, p83, 2011.
⑲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講演論文集, 査読無, 1C08, p84, 2011.
⑳高橋宏幸, 高橋秋典, 五十嵐隆治, 上田浩, 岩谷幸雄, 木下哲男, 奈須野裕, ON/OFF モデルに基づくバックグラウンドトラフィック生成法に関する研究, 平成 23 年度電気関係学会東北支部連合大会講演論文集, 査読無, 1C09, p85, 2011.
㉑鬼沢彩人, 五十嵐隆治, 高橋秋典, 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講演論文集, 査読無, 1C10, p86, 2011.
㉒鬼沢彩人, 五十嵐隆治, 高橋秋典, 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, 査読無, 資料番号 18, 2011.
㉓高橋宏幸, 高橋秋典, 五十嵐隆治, 上田浩, 岩谷幸雄, 木下哲男, 奈須野裕, ON/OFF モデルに基づくバックグラウンドトラフィック生成法に関する研究, 平成 23 年度第 2 回情報処理学会東北支部研究会, 査読無, 資料番号 19, 2011.

６．研究組織

(1)研究代表者

五十嵐　隆治（IGARASHI, Ryuji）
秋田大学・大学院工学資源学研究科・教授
研究者番号：00091786