2W-04

インターネット定点観測トラヒックにおける 相関係数発生確率行列に基づく異常検知の一検討

間山航平† 角田裕†
†東北工業大学 工学部情報通信工学科

1. はじめに

インターネット定点観測では未使用の IP アドレス空間に配置したトラヒック観測用のセンサに到達する通信を収集する．その通信にはマルウェアによる広域スキャンや DDoS（distributed denial of service）攻撃の被害者からの跳ね返りパケットなどが含まれることが知られており，定点観測トラヒックを分析しトラヒック中から注目すべきイベントを見出すことはマルウェアの拡散やサイバー攻撃の兆候を知るために重要となっている．

本研究では和泉ら[1]による相関係数発生行列に基づく異常検知手法を用いてインターネット定点観測のトラヒックを分析する． 同手法は任意の 2 つの観測量間の相関係数の発生確率を表すヒストグラム（相関係数ヒストグラム）によってネットワークの状態をモデル化し，異常検知を行なう．本研究では異常の原因となった観測量の特定が容易であるというこの手法の特長に着目した．本稿では同手法によってインターネット定点観測トラヒックを分析し，検知した異常について報告する．

2. 相関係数発生行列に基づく異常検知の手順

相関係数発生行列に基づく異常検知の手順を図 1 に示す．同手法では学習用トラヒックデータから相関係数ヒストグラムを作成し，それに基づいて評価対象トラヒックデータを評価する．使用する観測量は，タイムスロット当たりのパケット数をパケット種別ごとに集計したものであり，一定数の連続したタイムスロットの集合であるウインドウ単位で観測量間の相関係数を算出する．そして，ウインドウを一定幅でスライドさせながらすべてのウインドウで相関係数を求め，得られた相関係数の発生確率をヒストグラムで表現する．N個の観測量を使用する場合，学習用トラヒックデータから$\mathrm{N}(\mathrm{N}-1)/2$個の相関係数ヒストグラムが生成される．

相関係数ヒストグラムは，相関係数の取りうる範囲-1.0 から+1.0 外に階級値 1.1, 1.2, 1.3 の階級（算出不可クラス）を持つ．これは，2 つの観測量のうち 1 つ以上の標準偏差が 0 となり，相関係数が算出できない場合を表現するための階級である．1.1 と 1.2 の階級はどちらか一方の観測量の標準偏差が 0 の場合に対応し，1.3 の階級は両方の観測量の標準偏差が 0 の場合に対応する．

評価対象トラヒックデータから観測量の各ペアについて相関係数を求め，図 2 に示すように対応する相関係数ヒストグラムと照合し，求めた相関係数の発生確率を算出する．2 つの観測種別iとjの観測量間の相関係数の発生確率をp_{ij}と表すとき，このp_{ij}を要素とする$N \times N$の対称行列を相関係数発生確率行列M_pと呼ぶ．p_{ij}が小さいとき，観測種別iとjの観測量間の間に異常な相関係数が生じている．

M_pの要素p_{ij}がしきい値Th_p以下の場合を白画素，その他の要素を黒画素で表してM_pを画像化する． 1 つの異常な観測量がある場合には画像中には縦横 2 本の白い直線が生じる[1]ため，ウインドウ内には何がしかの異常が発生している可能性が高い．

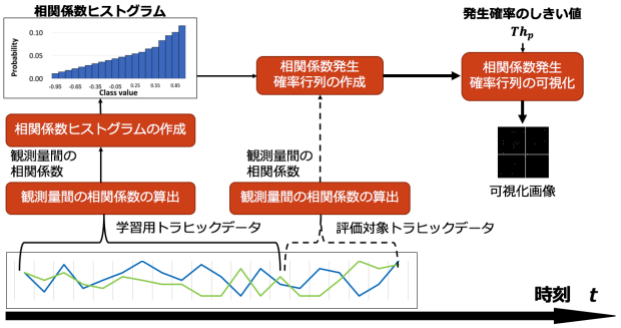


図 1 トラヒック異常検知の手順

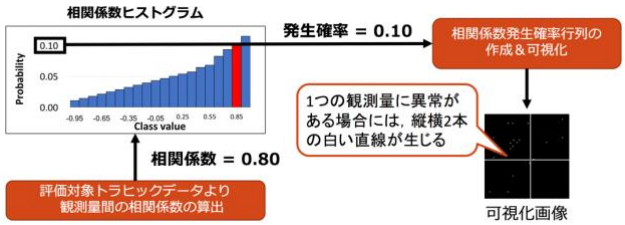


図 2 相関係数ヒストグラムより発生確率の算出

3. 異常検知実験

一般社団法人 JPCERT コーディネーションセンターのインターネット定点観測システム TSUBAME[2]のトラヒックデータを対象とし，異常検知実験を行った．

2015 年のトラヒックを学習用データとして使用し，2016 年のトラヒックを評価対象とした．観測量はプロトコル毎に集計したパケット数や，送信元／宛先ポート番号毎に集計したパケット数など 106 種類を使用した．相関係数はタイムスロットT=1 時間，ウインドウ幅$6T$，スライド幅$2T$という条件で算出した．

A Study on Anomaly Detection Based on Occurrence Probability Matrices of Correlation Coefficients in Internet Threat Monitoring System
Kohei MAYAMA†, Hiroshi TSUNODA†
† Tohoku Institute of Technology

3.1 相関係数発生確率行列M_pの可視化結果

観測期間中の全 4389 個のウインドウのそれぞれについて，しきい値Th_p=0.01 の場合の可視化画像を作成した．異常な観測量を表す縦横 2 本の白い直線を 1 組以上有する画像は 259 個存在した．白い直線に対応する観測量を特定したところ計 13 種類の観測量で異常が確認された．異常な観測量の画像数上位 5 種類を表 1 に示す．

表 1 縦横 2 本の白い線が存在する画像数

異常な観測量		画像数
a	UDP パケット数(宛先ポート 59084～65535)	113
b	UDP パケット数（送信元ポート 615～819）	32
c	UDP パケット数（送信元ポート 410～614）	30
d	UDP パケット数（宛先ポート 7476～13926）	25
e	UDP パケット数（送信元ポート 205～409）	22

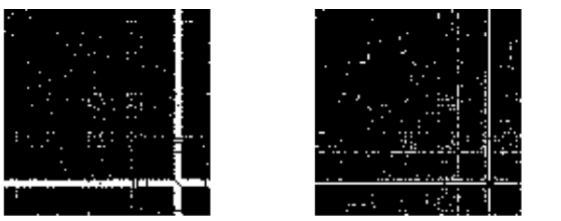
3.2 検知した異常の例

前節で求めた上位 5 種類の縦横 2 本の白い線が存在した画像に対応するウインドウ内のトラヒックを調査した．

表 1 の観測量 a が異常と判断された 113 個の画像については対応するウインドウのいずれにも当該パケットが確認できなかった．すなわち，通常であれば当該パケットが観測されるが，何らかの理由でパケットが到来しなかったことが異常と判断されたと言える．

2016 年 8 月 29 日 20 時から 2016 年 8 月 30 日 2 時までのM_pを可視化した画像を図 3（1）に示す．b，c，e が異常と判断された．該当する観測種別のパケットを調査したところ全てのパケットは送信元が中国であり，宛先ポート番号が 1900/UDP であった．このポート番号は UPnP（Universal Plug and Play）で利用されるプロトコル SSDP（Simple Service Discovery Protocol）である．SSDP を利用する反射型 DDoS 攻撃があることから[3]，このパケットはリフレクタに使用可能な UPnP に対応したネットワーク機器の探索をするものの可能性がある．

2016 年 11 月 9 日 14 時から 2016 年 11 月 9 日 20 時までのM_pを可視化した画像を図 3 (2) に示す．そのウインドウでは特徴量 c が異常と判断された．該当する時間帯のトラヒックには送信元および宛先ポート番号が 520 の UDP パケットが 37 個存在した．パケットの送信元について当該ポート番号は RIP（Routing Information Protocol）で使用されるポートであり，RIP も反射型 DDoS 攻撃に使用されることが指摘されている[4]．Whois 等で調査したところ，全てのパケットがセキュリティソリューションをてがける企業のネットワークから送信されていることがわかった．当該企業ではサービスやプロトコルを対象とした脆弱性を調査し，収集したデータをセキュリティ研究者やユーザなどへ一般公開している．つまり，発見されたパケットは外部からの RIP 通信に応答し，リフレクションとして利用される危険性のある機器を探索するための調査パケットであると判断できる．



（1）08/29 20:00～08/30 02:00　（2）11/09 14:00～11/09 20:00

図 3 異常が発生した観測量

縦横 2 本の白い直線が 1 組以上ある画像から，最高で 4 種類の特徴量が異常となっているものを発見した．対応するウインドウのトラヒックを調査した結果，この異常の原因はゲームサーバへ接続するパケットが誤ってインターネット定点観測システムに到達したものの可能性があることがわかった．また，インターネット調査団体から到来した脆弱性診断のためとみられるパケットも異常の原因となっていることもわかった．

以上のことから，異常を検知したウインドウ内を調査することで何らかのイベントがインターネット定点観測トラヒックで発生していることがわかった．よって，この手法が定点観測トラヒックの分析に有効であると考えられる．

4. おわりに

相関係数を用いたトラヒックの異常検知手法のインターネット定点観測のトラヒックにおける適用可能性を検証するために,相関係数の算出と相関係数ヒストグラムの作成,相関係数発生確率行列の作成と可視化を行った．相関係数発生確率行列を可視化した結果から，脆弱な機器の探索用パケットを検知できた．今後はタイムスロットやウインドウの幅などのパラメータ設定および使用する観測量について検討する．

謝辞

インターネット定点観測システムのデータを提供していただいた一般社団法人 JPCERT コーディネーションセンターに感謝いたします．

参考文献

[1] 和泉ら“相関係数発生確率行列を利用したネットワーク状態評価方式”，信学論(B) Vol J90-B, No.7, pp. 660-669, July, 2007.
[2] TSUBAME（インターネット定点観測システム），JPCERT コーディネーションセンター，http://www.jpcert.or.jp/tsubame/
[3] 警察庁@police, https://www.npa.go.jp/cyberpolice/detect/pdf/20141017.pdf
[4] Akamai, Threat Advisory: RIPv1 Reflection DDoS, https://www.akamai.com/jp/ja/multimedia/documents/state-of-the-internet/ripv1-reflection-ddos-threat-advisory.pdf