2007 年 5 月 16 日（水）
1031060322 松本　亮介

通信先ホスト数の変化に注目した 異常トラフィック自動検出手法の提案と評価（概略）

0 はじめに

※この資料は，参考文献を元に，参考文献の概略を作成したものです．この研究を私が実際に行ったわけではありませんので注意してください．

1 まえがき

ネットワークがインフラとして広く利用されるようになるにつれ，ワームによる攻撃の監視や，組織内のユーザーが P2P ファイル共有ソフトウェアによって，違法な利用をしているかどうかを確認することも求められている．

しかし，ネットワークにおけるサービスが多様化してきたため，従来のように転送バイト量やパケット量から異常トラフィックを検出する手法や，シグニチャ（異常状態を検出する学習データの最小単位）による異常トラフィックの検出には限界が生じている．

本稿では，既存の異常検出手法とその問題点を挙げ，異常検出手法に重要な要件を検討し，それらの要件に適合する異常検出手法を提案する．また，提案手法がどの程度利用可能であるかを評価する．ここでは，一般的な組織に対して，ワームによる攻撃，及び P2P ファイル交換ソフトウェアによるトラフィックを異常トラフィックと定義する．

2 既存手法とその問題点

異常トラフィックの検出の既存手法として，IDS が挙げられる．IDS とは，狭義ではシステムの侵入を検知するシステムであるが，ワームによる攻撃トラフィックや特定のアプリケーションによるトラフィックの検出にも広く利用される．IDS には，シグニチャ型 IDS とアノマリ検出型 IDS がある．

シグニチャ型 IDS は、事前にワームや特定のアプリケーション固有のペイロード等の知識を，検出シグニチャとして与えることで，該当するトラフィックが観測された際に管理者に通知することができる．この IDS は，シグニチャにマッチするような異常トラフィックであれば，確実に検出できるという利点があるが，シグニチャに対応しない未知の異常や暗号化されたペイロードには効果がない．

アノマリ検出型 IDS は，本稼動前に学習期間が必要である．学習期間中に観測したトラフィックの状態を正常と仮定し，その状態からはずれたトラフィックを観測した際に管理者に通知することができる．しかし，正常状態を仮定する際に閾値を設定する必要があるが，閾値の設定が難しく，特定のトラフィックの高精度な検出には長期の事前データと専門家によるチューニングが必要である．

これらの IDS はミラーリングなどの技術を用い，観測対象トラフィック中のパケットをすべて検査するため，対象となるパケットのレートに比例して IDS 装置の負荷は上昇する．このことから，IDS を用いた手法は，低帯域ネットワークから広帯域ネットワークまで，スケーラブルに対応できないという問題を抱えている．

3 異常検出の機能要件と提案手法

2 で述べたように，シグニチャを用いた手法や広帯域にスケーラブルに対応できない異常トラフィック検出手法には問題がある．また，転送バイト量やパケット数に注目した手法は検出精度が低く優れていない．導入コストや運用コストが高い手法にも問題がある．これらのことから，以下の 6 つの要件が必要であると考えられる．

ⅰ，低コストで利用開始可能
ⅱ，検出シグニチャに非依存
ⅲ，自動で異常トラフィックを検出可能
ⅳ，高い精度で異常トラフィックを検出可能
ⅴ，広帯域環境下で使用可能
ⅵ，リアルタイムで異常トラフィックを検出可能

これらの機能要件を満たす異常検出手法を提案する．提案手法では，企業や学校などの組織内のネットワークを対象として，異常トラフィックの検出を目指す．ここでは，ワームによるトラフィックと，P2P

ファイル交換ソフトウェアによるトラフィックについて考える．

ワームによるトラフィックの特徴を述べる．ワームは，より多くのホストに感染しようとする性質を持っている．攻撃先のホストの選択方法はワームによって異なるが，より多くのホストに感染しようと，多数のホストに攻撃パケットを送信する点は共通である．

P2P ファイル共有ソフトによるトラフィックの特徴を述べる. P2P ネットワークに接続されているホストのアドレス情報や共有ファイル情報などは，各ホストで分散管理している．このため，ユーザーが要求したファイルを検索し，ダウンロードするために分散管理された情報を収集する必要がある．そのため，多数のホストと通信するという性質をもっている．

これらの特徴を利用して，異常トラフィックによって大きく変動し，他のトラフィックによる変動が少ない通信先ホスト数の時間変化を用いて異常トラフィックの検出を試みる．ただし，対象組織内の異常トラフィックを発生させているホストを見つけることを目的とした利用を想定している．

注目指標（通信先ホスト）の時間変化は，ある一定の周期を持つとされている．しかし，周期性があるとはいえ，注目指標にはばらつきがある．また，注目指標はアプリケーションの通信継続時間によっても支配され, 1 時間前の注目指標よりも 5 分前の注目指標に似ている場合もある．こうした特長を持つ注目指標の閾値計算には，Holt-Winters 法を用いる．Holt-Winters 法とは，需要予測分野で実績のある予測手法で，季節変動のある需要予測には最適であるとされている．過去の観測値に対して，各種パラメータと信頼水準を与えることで，次の観測値がある一定の確率異常で収まる範囲（閾値内）を算出することができる．

本稿では，曜日によっては前日と特性が異なる日の精度が悪化するため，周期を 1 週間とした．これにより，予測の信頼水準を高く設定することで，閾値から外れた値を通常のパターンから外れた異常なトラフィックとして取り出すことが可能となる．

閾値計算と異常トラフィック検出の具体的なアルゴリズムは次のようになる．

単位時間を N 秒とした場合，現在時刻から過去 M 秒（トラフィック計測を開始してから提案手法が利用可能になるまでの期間）に対して N 秒ごとの注目指標の変動を取得する．取得した値に Holt-Winters 法を適応し，次の N 秒に対する上限閾値，下限閾値を設定する．次の N 秒間に実際に観測された注目指標が，設定された閾値内に収まらなかった場合，つまり，上限閾値を上回った場合，または下限閾値を下回った場合に，異常トラフィック発生の可能性ありとして管理者に通知する．この作業を，N 秒ごとに実行し，閾値内に収まらなかった実測値を通知することで，リアルタイムな異常トラフィック検出を実現する．

4 評価と考察

3 で述べた機能要件を満たした異常検出が実現しているかどうかを評価する．以下の 3 つの出来事を異常トラフィックのリファレンス（リファレンス異常）として評価に利用する．

ⅰ，ワーム（Sasser）感染の拡大
ⅱ，P2P ファイル共有ソフト（WinMX）の実行
ⅲ，P2P ファイル共有ソフト（e-Donkey）の実行

3 で述べた手法により，ⅰのリファレンス異常は正常に検出されており，提案手法によるワーム感染の検出は妥当であるといえる．しかし，ⅱのリファレンス異常は N=300 の時はすべて検出できているが，N=2400 の時は，検出できるものとそうでないものがあった．また，ⅰのリファレンス異常は，発見され対処されるまでに数日の時間を要し，異常状態の継続状態が長時間にわたった．ⅱのリファレンス異常の継続時間は 20 分と短時間であった. このことから，単位時間を 2400 秒としたときのリファレンス異常が，注目指標へ与える影響も半減し，検出できなかったと考えられる．その一方で，ⅲのリファレンス異常はほとんどの場合で検出が成功していない．これは，P2P ファイル共有ソフトのトラフィックが注目指標に与える変化が小さすぎて，全体量としてみた注目指標を閾値内にとどめたためと考えられる．閾値の自動算出値も Holt-Winters 法のパラメータを変えて実験してみたところ，妥当であるといえる．このことから，事前知識を用いず，管理者の知識や経験に依存することなく，異常検出を実現できているとい

ベクトル同士のカーネル(内積)の計算問題に帰着させ，そのカーネルを注意深い近似手法によって高速化する．

2 高速化計算手法

2.1 特異スペクトル変換

特異スペクトル変換について述べる．等間隔の時刻で観測された時系列データ $\{x_t \in \Re \mid t = 1,2,\ldots\}$ に対して，長さ w の部分系列を，$\Re^w$ の列ベクトルとして

2.2 変化度式の変換

(1)を変更して，

$$z = 1 - \sum_{i=1}^{r} K(i,\mu)^2 \qquad (2)$$

ただし，K は

$$K(i,\mu) \equiv \mu^{\mathrm{T}} u^{(i)} \qquad (3)$$

で定義されるカーネル（内積）である．(2)は μ で張られる空間と履歴空間の距離の 2 乗という意味を持つ．これらの計算を高速化するためには，いかに効

参考文献

[1] 藤井聖 “通信先ホスト数の変化に注目した異常トラヒック自動検出手法の提案と評価”