0. 論文

DETECTION AND LOCALIZATION OF CHANGE-POINTS IN HIGH-DIMENSIONAL NETWORK TRAFFIC DATA

BY CÉLINE LÉVY-LEDUC AND FRANÇOIS ROUEFF

CNRS, LTCI and Télécom ParisTech

タイトル：Detection and localization of change-points in high-dimensional network traffic data
著者：Celine Levy-Leduc, Francois Roueff

arXiv投稿日：
学会/ジャーナル： The Annals of Applied Statistics(2009)

1. どんなもの？

- Dos攻撃のようなネットワーク異常を検出することを目的
- レコードフィルタリングに基づくデータ量の削減
- U統計学に基づいた変化点検出テスト(検定？)によって検出を行う

2. 先行研究

- Dos攻撃を検知する手段
    - 既知の攻撃パターンとの比較を行う手法
        - 異常パターンをあらかじめ知っていないと無理
    - ネットワーク特性に急激な変化をもたらすと仮定して異常を検出することを目標にする
        - 未知時間に発生するので，できるだけ早く検知する必要がある
        - これは変化点検出問題として記述できる
- 一番普及しているのはCUSUMアルゴリズム
    - Wang, Zhang and Shin (2002)
    - Siris and Papagalou (2004)
    - メモリのコストが無視できない
    - 集約された系列に変化が発生した場合に検知できるが，悪意のあるフローを特定することは不可能
- 各IPアドレスごとに分析して変化点検出を行う
    - スプーフィングと呼ばれる問題がある(この分野に詳しい訳でないのでどの様な問題かは分からない)
- Gombay and Liu(2000)でノンパラメトリック統計的変化点検出手法の提案
    - Wilcoxonの順位検定を一般化したもの

3. コアアイディア

- $N_i(t)というデータが観測される
    - 例:アドレスiに送られる時間tのパケットの数

$$W_P = \max_{1 \le t \le P} |S_t|$$

-
- 上記の量を最大にするtについて注目する
- $S_t = (\sum_{s=1}^{t}U_s)/(\sum_{s=1}^{P}U_s)^{1/2}$
- P: 系列長
- $U_s = \sum_{t=1}^{P}A_{s,t}$
- $A_{s,t} = {1}\hspace{-0.19em}\mathrm{I}(X(s) > X(t)) - {1}\hspace{-0.19em}\mathrm{I}(X(s)<X(t))$
- $X(\cdot)$: ある時点での全ての系列

$$Pval(b) = \mathbb{P}(B^\star > b) = 2\sum_{j=1}^{\infty}(-1)^{j-1}e^{-2j^2b^2},$$

-
- 上記のようにp値を計算し，棄却された場合以下で変化点とする $$\hat{t}P = *argmin*{1\leq t \leq P}|S_t|$$

4. どうやって有効だと検証した？

- 実際のインターネットトラフィックデータ
  - TCPの総数が多すぎて攻撃先の特定が困難になっている
  - 実際のアルゴリズムは以下の3ステップでおkなわれる
    - １．レコードフィルタリングステップ
    - ２．時系列の打ち切り決定
    - ３．変化点検出テスト
  - 2ステップ目まではデータ量を削減して，リアルタイム応答に対応するために行われる
    - あまり読んでもしょうがないかも
    - 現実的な時間で反応できるように一度に見る系列長を60に設定
    - 系列数は10を設定
  - ハイパーパラメータとして$M^{\prime}$がある
    - トップ$M^{\prime}$までの系列を探索することになる
  - CUSUMのアルゴリズムと比べて誤報の数が極端に小さくなっている

TABLE 1

Statistical performance for detecting the 4 successive SYN flooding attacks displayed on the right-hand side of Figure 1. The attacks consist in sending SYN packets to a given destination IP address. In the top row the intensity (number of SYN packets per second) of each attack is given. In the TopRank *part of the table, the displayed p-values are the smallest ones that ensure the detection of the attack by the* TopRank *algorithm and below that the corresponding number of false alarms in the whole traffic trace is given. In the SP part of the table [SP is the method devised by Siris and Papagalou (2004)], the h row gives the smallest threshold values that ensure the detection of each attack. In the last row the corresponding number of false alarms is displayed*

	Number of SYN packets	**1000**	**500**	**200**	**50**
TopRank	*p*-values	10^{-8}	10^{-10}	2×10^{-6}	10^{-12}
	Number of false alarms	3	1	9	0
SP	*h*	5	6.5	9.7	16.34
	Number of false alarms	69	65	62	22

  -

- 上記はSYN floodの攻撃例で他にもDos攻撃の種類はあり，それに対しても適用しているが似たような結果なので割愛

5. データセット

- ANRRNRT OSCARプロジェクト内のFranceによって提供されたインターネットトラフィック

6. 疑問点

- 複数の系列が共通する変化点を持つようにはできていないっぽい
    - あくまで変化がありそうな系列をトップ～まで個別に探索するようになっているのではないか？

7. 次に読むべき論文は？

キーワード