特殊な Earth Mover's Distance を用いた通信異常検知

2016SS029 小池めぐみ
指導教員：小市俊悟

1 はじめに

近年，インターネットを使用する人が増加している中で，コンピュータに対するマルウェア攻撃も増加している．インターネット上のマルウェア攻撃を防ぐにはウィルス対策が必要となるが，現在使用されているウィルス対策ソフトでは既存のウィルスを発見することしかできないものが多く，すべてのマルウェア攻撃を防ぐことはできない．

本研究はインターネット上の通信における異常を検知することを目的とする．ただし，インターネットに適用するのは実効性を検証したあととし，既存の通信ログの中から通信異常の検知を行う．通信ログデータの中から異常の検知を行う新たな手法を確立することができれば今まで以上にマルウェア攻撃を見つけ出すことができるようになり，より安全にインターネットを使用することが可能になる．

通信異常の検知には Earth Mover's Distance(以下，EMD) を応用する．そもそも異常検知を行うためには，「異常」とは何かを定義する必要があるが，本研究では，EMD を応用して定める．

EMD の具体的な定義は，あとで説明するが，あわせて EMD が小さいことが意味することについても考察する．本研究では，通信データを具体的な適用例とすることを念頭においているが，提案する手法の適用範囲はそれに限定されるものではなく，より広範な (時系列) データに適用可能であると考える．

2 異常検知の方法

2.1 Earth Mover's Distance

ワッサースタイン計量，もしくは，その離散版と考えられる EMD は分布間の距離を輸送問題を応用して定めるものである．ワッサースタイン計量を定義するときの輸送問題は必ずしも離散最適化問題としての輸送問題とは限らないが，本研究では離散的なヒストグラムを対象にした EMD を 扱うので，ヒッチコック (型) 輸送問題を考える．さらに，本研究では，輸送コストの定め方が特殊な EMD を採用するので，次のような定義が可能である．本研究で扱うヒストグラムの (縦軸の) 値はすべて 0 以上とする．ヒストグラムの横軸は，n 個の離散値からなるとし，$[n] = \{1, 2, \ldots, n\}$ と定める．ヒストグラム a について，各 $i \in [n]$ における値を a_i とし，$a = \{a_i\}_{i=1}^n$ と表す．ヒストグラム b も同様にして，$b = \{b_i\}_{i=1}^n$ と表す．ヒストグラム a, b は，数列とみなすこともできる．ここで，$\sigma : [n] \to [n]$ を $[n]$ の置換とする．このとき，ヒストグラム a, b と置換 σ について，次で定まる $D(a, b, \sigma)$ を考える．

$$D(a, b, \sigma) = |a_1 - b_{\sigma(1)}| + |a_2 - b_{\sigma(2)}| + \cdots + |a_n - b_{\sigma(n)}|$$

これを用いて，ヒストグラム a と b の距離 $d(a, b)$ を次で定める．

$$d(a, b) = \min_{\sigma \in P_n} D(a, b, \sigma)$$

ただし，P_n は $[n]$ の置換すべてである．この $d(a, b)$ を求める問題が，適当な設定のもとに，ヒッチコック輸送問題として記述できることはよく知られた事実である．

実際，下記の問題において，$f_{ij} = |a_i - b_j|$ とすればよい．

$$\begin{aligned} \text{Minimize} & \sum_{i,j \in [n]} f_{ij} x_{ij} \\ \text{subject to} & \sum_{j \in [n]} x_{ij} = 1 \quad (i \in [n]) \\ & \sum_{i \in [n]} x_{ij} = 1 \quad (j \in [n]) \\ & 0 \le x_{ij} \le 1 \quad (i, j \in [n]) \end{aligned}$$

2.2 Earth Mover's Distance による異常の定義

時間軸として離散時刻を考え，対象とするデータは，時間軸上のある時刻において，何かしらの事象が発生し，その事象に関する (特定の一つの) 数値を発生時刻とともに記録したものとする．

このようなデータから時間一定の時間窓を適当に動かしながら，各時間窓でデータを抽出する．その際に，最早時刻と最遅時刻をそれぞれ改めて時刻 1 と n とすれば，前節で考えたようなヒストグラムが各時間窓に応じて得られる．前節に述べたような EMD を採用することで，このようなヒストグラムについて，異常もしくは正常がどのように解釈できるかを考える．

まず，ヒストグラム $a = \{a_i\}_{i=1}^n$ と $b = \{b_i\}_{i=1}^n$ の EMD が $d(a, b) = 0$ となる場合を考えると，上述の EMD の定義より，これは a と b を (数列と見て) 並べ替えたときに等しくなる場合である．数列 a と b をそれぞれ昇順 (または降順) に整列したとき，同じ位置の要素が等しい場合とも言える．実のところ，より一般の場合に対して，次が証明できる．

数列 a と b をそれぞれ昇順に整列したとき，要素の位置から決まる対応関係に相当する置換 σ が一つ決まるが，この σ が $D(a, b, \sigma)$ を最小にし，$d(a, b)$ を与える．この事実は，$d(a, b)$ の計算方法も示している．すなわち，a と b を

昇順に並べ替え，位置が対応する要素で差を取り，その絶対値の和を計算すればよい．

上のような EMD の性質から，本研究で正常であると判定するデータは，一定の時間内において，他と同じような事象が発生しているデータと言える．正常か否かの判定を，個別のデータよりは時間帯に対して行なっていると述べる方が適切かもしれない．個別の事象はランダムに生起していると考えられるが，一方で，一定の時間をとれば，同じような事象が生起しているというのが，本研究における「正常」である．

3 Earth Mover's Distance を用いた異常検知の有効性の検証

3.1 使用データ

使用するデータは 2 種類用意する．

1 つ目のデータとして用意したのは，EMD を用いた異常検知が実際に有効であるかを検証するための人工データである．人工データの作成には，期待値が異なる 4 つの指数分布を用意し，それらに従って発生する 4 種類の乱数を用いて一定の時間帯に異常部を持つデータにした．

2 つ目は VIZSEC[1] によって提供されている京都大学によって計測されたハニーポットのデータである．このデータには通信時の基本情報に加えて，マルウェアによる通信であるかどうかのデータも格納されている．このデータは時系列データであるが，同時刻に発生しているデータが多数あり，そのままでは通常の時系列データとして使うことができない．そのため各時刻を人為的に細分化し，各データが相異なる時刻に割り当てられるようにした．

3.2 人工データに対する異常検知

人工データに対する異常検知は図 1 のようになった．作成した人工データにおいて横軸の 2000 から 2500 の部分 (黄色部) が異常部となるが，青線で示す値が，その部分で大きな値を示したことより異常が的確に検知できているといえる．また，EMD に基づくクラスタリングを用いて判別を行うと図 2 のようになる．このとき異常が含まれているのは 01:36:00-01:39:00 の一部と 01:39:00-01:42:00 であり，クラスタリングにより異常が含まれている 2 ヶ所でクラスタ (青線部) を作っていることが確認できた．

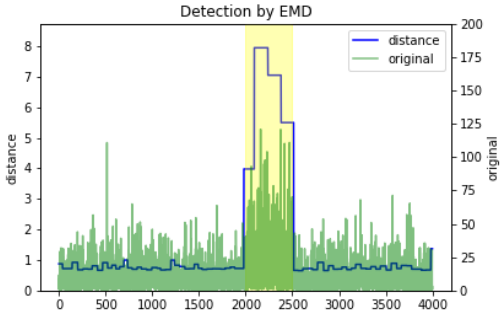

図 1 EMD を用いた異常検知

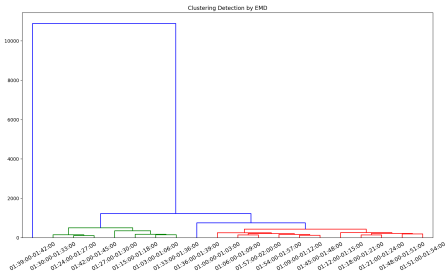

図 2 EMD に基づくクラスタリングによる異常検知

これより人工データに対しては EMD を用いた異常検知は有効であるといえよう．

3.3 実データに対する異常検知

実データに対して EMD を用いて異常検知をおこなうと，図 3 のような結果が得られた．ハニーポットの通信ログデータはそのほとんどが異常であり，正常がむしろ突発的に発生していた．図 3 では青線で示された値が大きいところもあるが，それが正常データを含む部分に一致することはなかった．ハニーポットのデータは，本研究で想定しているような仮定を満たしておらず，このようなデータに対しては検知能力が十分ではないことが判明した．

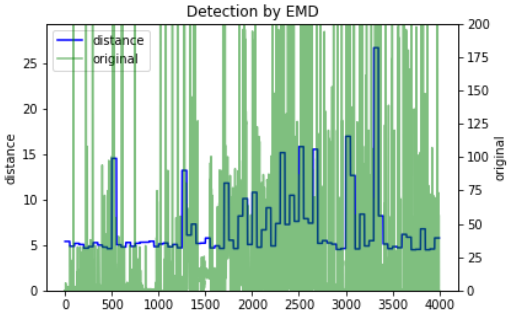

図 3 EMD を用いた実データの異常検知

4 おわりに

検証の結果，EMD を用いた異常検知は人工データのように異常部がまとまって出現しているものに対して有効であることが判明した．既存手法とも比較したが，既存手法ではうまく捉えられない異常を検出できることも確認した．今後の課題として，実データのような正常部に異常が散発的に含まれているデータに対する異常検知の方法の考案が必要である．

参考文献

[1] J. Song, H. Takakura, Y. Okabe:
Traffic Data from Kyoto University's Honeypots, http://www.takakura.com/Kyoto_data/ (アクセス日: 2019/9/23)