4W-05

spectral clustering を用いた不正侵入パケット検知の基礎検討

伊東 道明 † 彌冨 仁 †

法政大学 †

1 概要

現在インターネットを介したサイバー攻撃を検出する方法の一つに侵入検知システムがある．この手法は事前に定義された攻撃パケットのパターンと外部からやってくるパケットの比較により異常を検知するため，未知の攻撃パケットの検出が困難である．このような問題を解決するために，未知の攻撃に対しても効果が期待できる教師なし学習手法を侵入検知に適応する手法が提案されている．本実験では多次元の距離構造をもとに効率的にクラスタリングが可能な spectral clustering をパケットの異常検知に適用し，他の手法と比較する．

2 背景

現在侵入検知システムとして普及しているシグネチャ型検知システムは，事前に定義された攻撃パケットのペイロードのパターンをシグネチャとして記憶し，パターンマッチングにより攻撃を検知をする [1]．また，ペイロード部分を数ビット変更した亜種攻撃を教師あり学習であるサポートベクターマシン (SVM) を用いて攻撃検知をする手法が提案されている [2]．このシステムの主な問題点として，未知の攻撃の検知ができないことが挙げられる．そのため，新たな脆弱性や攻撃手法が出た場合その都度シグネチャを追加していく作業が必要となる．

シグネチャ型検知システムの問題点を解決するために，教師なし学習を用いた侵入検知システムの提案がされている．既存研究では，K-means clustering を用いて攻撃パケットを検知する手法が提案されている [3]．しかし，識別を行う特徴空間において，パケットを記述する特徴量の分布が必ずしも凸ではなく，また K-means clustering では特徴量の重要性も考慮されないことから，実用的な精度を得られていない．そこで本実験では，精度の向上を図るために各パケットデータをグラフ上のノードとして捉え，高次元のデータ上でのデータ間の距離構造を保持する spectral clustering[4] を用いることで，教師なし学習モデルにおける高精度攻撃検知手法の開発の施策を行った．

Improvement of Packet Anomary Detection using spectral clustering

† Michiaki Ito, Hitoshi Iyatomi (Hosei University)

3 実験

3.1 実験データ

学習及び評価に用いるトラフィックデータには，KDDCup1999[5] の中から，正常なパケットデータを 2,000 パケットと，23 種類の攻撃のうち主要な smarf，neptune，back，satan，ipsweep，portsweep，Warezclient，teardrop，Pod，nmap の 10 種類の攻撃データを 200 パケットずつ，計 4,000 パケットを用いた．

各パケットデータは，41 次元の特徴で記述されていたが，本実験では正確な距離指標として扱えない特徴である L4 プロトコルタイプ，上位サービス名，TCP 制御フラグの 3 特徴を学習から取り除いた．また，学習用データセット内で特徴の分散が 0 であった 2 特徴を取り除き，最終的に 36 次元の特徴量に対し平均値 0，標準偏差 10 となる偏差値を求める前処理を行った．本実験では，攻撃パケットと通常パケットの 2 種類を識別することを課題とし，評価には正常パケットを正常と識別する確率 (TP: ture positive)，攻撃パケットを異常と識別する確率 (TN: true negative)，正解率 (accuracy) を用いた．

3.2 パケットデータのクラスタリング

上記データセットに対して，K-means clustering ならびに，spectral clustering を用いた教師なしクラスタリングを行い，攻撃パケットと通常パケットの分類を試みた．spectral clustering では，データ間の距離を表す affinity matrix を作成し，それを元に graph laplacian と呼ばれるデータ間距離に基づいたグラフ構造を作成する．このとき，このグラフが所望のクラスタ内にのみ結合がある理想的な場合，graph laplacian は，データの持つクラスタの数だけ固有値 0 を持ち，それに対応する固有ベクトルは，そのクラスタに含まれるデータ

表 1　K-means clustering，spectral clustering 及び SVM の精度比較

手法	accuracy[%]	TP[%]	TN[%]
K-means	69.5	99.8	39.2
spectral	91.5	83.3	99.8
SVM	-	-	84.1

全てを代表するベクトルとなる．ノイズが含まれる場合でも，類似するデータ群は，対応する同じ固有ベクトルで代表されるため，graph laplacian の固有ベクトルを K-means clustering などでクラスタリングすることで，データ構造に基づく頑健なクラスタリングが実現できる．affinity matrix の各要素になる，任意のデータ $\boldsymbol{x}_i, \boldsymbol{x}_j$ 間の類似度 S_{ij} は，以下の式で求めた．

$$S_{ij} = \exp(-\frac{\|\boldsymbol{x}_i - \boldsymbol{x}_j\|^2}{2\sigma^2}) \tag{1}$$

本実験では予備実験の結果より $\sigma = 0.15$ とした．また比較実験として，9 種類の攻撃パターンと正常パターンを教師あり学習した SVM で，学習していない攻撃パターンを未知の攻撃として識別する実験を攻撃パターン数に応じて 10 種類作成し，それらの平均の識別能を評価した．表 1 にこれらの手法による識別の結果の比較を示す．

K-means clustering と spectral clustering によるクラスタリング結果を比較すると，spectral clustering の方が accuracy が約 22% 高い．

spectral clustering における affinity matrix を図 1 に示す．データセットは，正常パケット，10 種の攻撃パケットの順に並んでおり，この行列はデータの並びに応じた $4,000 \times 4,000$ の行列である．各要素は (1) 式の S_{ij} の値に対応し明るい値ほどデータ間の類似度が高いことを示す．

4　考察とまとめ

TN，TP の値は実際の運用では適切に設定する必要があるが，spectral clustering を用いることにより攻撃パケットの識別能が K-means clustering よりも大幅に優れていることが確認できた．また，本実験において spectral clustering によるパケット識別能は，教師あり学習の SVM が未知の攻撃に対する検出能より高いことも確認できた．これは spectral clustering の過程で得られた affinity matrix が，同様のパケットグループ間でかなり明確に分かれていたことが示すように，今回の問題では識別のために効果的な特徴がすでに得られていたためとも考えられる．

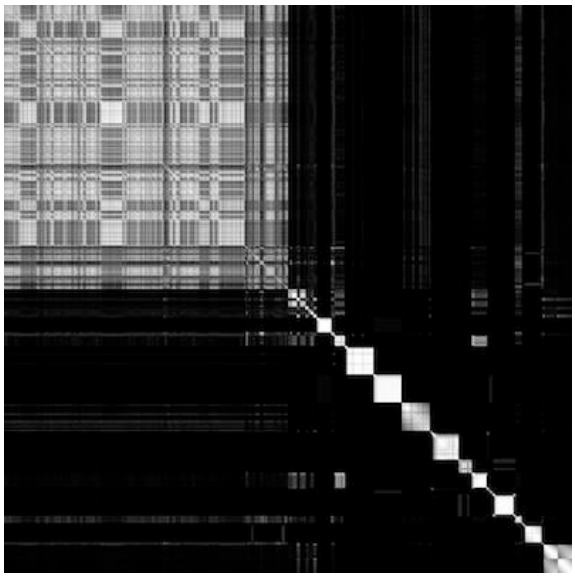

図 1　affinity matrix

参考文献

[1] J. Bispo et al: “Regular expression matching for reconfigurable packet inspection,” in Proc. IEEE Int’l Conference on Field Programmable Technology (FPT’06), Bangkok, (2006), pp. 119–126.

[2] T. Shon, J. Moon: “A hybrid machine learning approach to network anomaly detection,” Information Sciences, 177 (2007), pp. 3799–3821.

[3] G. Munz, S. Li, G. Carle: “Traffic Anomaly Detection Using K-means clustering,” in Proc. of Leistungs, Zuverlassigkeits und Verlasslichkeitsbewertung von Kommunikationsnetzen und Verteilten Systemen, (2007).

[4] U. V Luxburg: “A tutorial on spectral clustering,” Stat. Comput., (2007), vol. 17, no. 4, pp. 395–416.

[5] UCI KDD Data, UCI Archive: (online), KDD Cup 1999 available from https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (accessed 2017-01-13).