L-029

シグネチャ型 IDS とアノマリ型 IDS の組み合わせによる未知の異常検出

Unknwon Anomaly Detection by Combination of Signature based IDS and Anomaly based IDS

谷澤 俊樹 † Toshiki Tanizawa　**青木 茂樹** † Shigeki Aoki　**宮本 貴朗** † Takao Miyamoto

1. まえがき

近年，サイバー攻撃を検出するための侵入検知システム (IDS) に関する研究が盛んに行われている．IDS はシグネチャ型とアノマリ型の 2 種類に大別できる．シグネチャ型では異常を定義したパターンファイルに基づいて攻撃を検出する．そのため，パターンファイルに定義されていない異常は検出できない．一方，アノマリ型の代表的な手法として，文献 [1] が挙げられる．アノマリ型はあらかじめ正常なパターンを学習させ，学習結果からの外れ値を異常として検出する．しかし実運用中のネットワークの正常なトラフィックのみを学習させることが困難であることなどから十分な検出精度を実現することが難しい．

文献 [2] の手法では前述の 2 種類の IDS を組み合わせることで未知の異常を検出する手法を提案している．本稿では文献 [2] の手法に Web やメールの通信に注目した特徴量を追加することによって，文献 [2] の手法では検出が難しい攻撃を検出できる手法を提案する．

2. 提案手法

2.1. パケットからの特徴ベクトル抽出

あるネットワークに対するサイバー攻撃を検出するために, 注目しているネットワークと外部ネットワーク (インターネット) 間の送受信パケットを, 単位時間 w で分割したものを区間 t とし, それを N 個収集する．区間 t で収集したパケットから，単位時間におけるパケットの特徴ベクトル $\boldsymbol{I}_t$ を抽出する．特徴ベクトルとして IP アドレスの種類数やパケットサイズの分散など，表 1 に示す 61 種類の情報を抽出する．その後クラスタリングするために主成分分析法により累積寄与率 80%以上となる最小の次元数 r で次元を圧縮し，圧縮された空間を $\boldsymbol{S}$ 空間と呼ぶ．

2.2. 特徴ベクトルのクラスタリング

表 1 に示す特徴ベクトルを抽出した際，t と $t+1$ の 2 つの区間において同様の異常が含まれるとき，特徴ベクトル $\boldsymbol{I}_t$ と $\boldsymbol{I}_{t+1}$ は類似するために特徴ベクトル間の距離は小さくなる．一方，性質の異なる異常を含む特徴ベクトル間では距離が大きくなると考えられる．そのため，抽出した特徴ベクトルをクラスタリングすると，同一クラスに分類された特徴ベクトル同士では，類似した異常を含むと考えられる．ここでは，$\boldsymbol{S}$ 空間上の座標値を基に Mean-Shift 法を用いてクラスタリングする．この手法はあらかじめ分類するクラス数を定めないため，今回のような異常の種類数が判明していない場合等に適した手法である．

表 1: 特徴量の一覧

パケットサイズ平均	パケットサイズ最大値
パケットサイズ最小値	パケット到着間隔平均
パケット到着間隔最小時間	パケット到着間隔最大時間
パケット到着間隔分散	パケット到着間隔の総時間
パケットサイズの総数	パケット数
パケットサイズの分散	TTL 値平均
TTL 値分散	宛先 IP アドレス種類数
送信元 IP アドレス種類数	送信元ポート番号種類数
宛先ポート番号種類数	SYN パケット数
FIN パケット数	PSH パケット数
RST パケット数	URG パケット数
ACK パケット数	FIN&ACK パケット数
RST&ACK パケット数	SYN&ACK パケット数
PSH&ACK パケット数	TCP 中の RST 割合
TCP 中の SYN 割合	TCP 中の PSH 割合
TCP 中の URG 割合	TCP 中の FIN 割合
TCP 中の ACK 割合	TCP 中の RST&ACK 割合
TCP 中の PSH&ACK 割合	TCP 中の SYN&ACK 割合
TCP 中の FIN&ACK 割合	ICMP パケット数
UDP パケット数	送信元ポート番号 110 番パケット数
送信元ポート番号 22 番パケット数	送信元ポート番号 53 番パケット数
送信元ポート番号 443 番パケット数	送信元ポート番号 80 番パケット数
送信元ポート番号 25 番パケット数	送信元ポート番号 465 番パケット数
送信元ポート番号 587 番パケット数	送信元ポート番号 995 番パケット数
送信元ポート番号 993 番パケット数	送信元ポート番号 143 番パケット数
宛先ポート番号 110 番パケット数	宛先ポート番号 22 番パケット数
宛先ポート番号 53 番パケット数	宛先ポート番号 443 番パケット数
宛先ポート番号 80 番パケット数	宛先ポート番号 25 番パケット数
宛先ポート番号 465 番パケット数	宛先ポート番号 587 番パケット数
宛先ポート番号 995 番パケット数	宛先ポート番号 993 番パケット数
宛先ポート番号 143 番パケット数	

2.3. クラスへのラベル付加

クラスタリングの結果得られた各クラスに対し，シグネチャ型 IDS の異常検出結果を用いてラベル付けを行う．同一クラス内の各区間では，類似した攻撃を受けていると考えられる．そのため，シグネチャ型 IDS を用いて検出される異常と種類や数も類似すると考えられる．各クラスの重心に最も近い特徴ベクトルを選択し，その特徴ベクトルを抽出した区間で，シグネチャ型 IDS を用いて異常検出を行う．選択した区間の特徴ベクトルを $\boldsymbol{I}_t$，シグネチャ型 IDS で定義されたルールを q 個，区間 t で v 番目のルールで検出された異常の個数を $s'_{t,v}$ とすると $\boldsymbol{I}_t$ は $(s'_{t,1}, s'_{t,2}, \cdots, s'_{t,v}, \cdots, s'_{t,q})$ とラベル付けされる．ラベル付けの例を図 1 に示す．図の例では，$q = 3$ であり，$(s'_{t,1}, s'_{t,2}, s'_{t,3}) = (10, 12, 2)$ であるため，このベクトルを $\boldsymbol{I}_t$ のクラスのラベルとして用いる．

† 大阪府立大学　大学院人間社会システム科学研究科

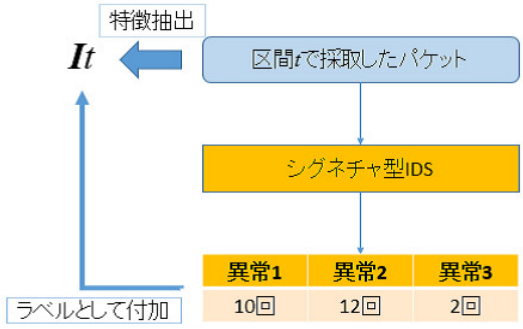

図 1: クラスへのラベル付けの例

2.4. 異常検出

新たな区間で抽出した特徴ベクトルと各クラスの重心との距離を算出し，最も距離が短いクラスを選択する．そして，観測された特徴ベクトルと選択したクラスの重心との距離がしきい値未満の場合には，観測された特徴ベクトルを含む区間において，そのクラスのラベルの異常が含まれると認識する．しきい値以上の場合は，その区間では初めて観測された異常が含まれているとみなし，新たなクラスと認識してシグネチャ型 IDS を用いてラベル付けを行う．

3. 実験及び考察

3.1. 実験条件

本手法の有効性を確認するため実験を行った．実験では，大阪府立大学のキャンパスネットワークと，インターネットとを接続するファイアーウォールの外側でトラフィックを収集し異常検出を行った．まず学習用データとして，2016 年 2 月 2 日 14 時 50 分から 10 分間のトラフィックを収集し，単位時間を 1 秒として 600 個の区間に分割し，特徴ベクトルを抽出した．各クラスへのラベル付けにはシグネチャ型 IDS の一つである Snort[3] と 2016 年 2 月 13 日に取得したルールを使用した．次に異常検出用のデータとして，2016 年 2 月 3 日から 3 日間，同時刻に 10 分間収集した．

3.2. 実験結果と考察

まず，学習用データを学習するため各区間から特徴ベクトルを抽出した．主成分分析法により次元を圧縮したところ累積寄与率 80%以上となる最小の次元数 r は 10 次元となった．クラスタリングした結果，600 個の特徴ベクトルが 18 個のクラスに分類された．

また，文献 [2] で用いられている 44 種類の特徴量で同様の実験を行ったところ，15 個のクラスに分類された．実験結果を表 2 に示す．本手法では，特徴量を 17 種類追加したため，文献 [2] の手法で学習した結果と比較してクラスが新たに 3 つ増加した．また，新たに増加したクラスに分類されたトラフィックデータについて，増加したクラス重心に最も近い特徴ベクトルの区間に含まれる異常を Snort で確認したところ，暗号化通信に関する異常やメール関連のプロトコルに関する異常が含まれていた．

表 2: クラスタリング結果

	従来手法 [2]	本手法
クラス数	15	18
2/3	579 区間→学習クラス (96.5%) 21 区間→新たなクラス (3.5%)	548 区間→学習クラス (91.3%) 52 区間→新たなクラス (8.7%)
2/4	566 区間→学習クラス (94.3%) 34 区間→新たなクラス (5.7%)	526 区間→学習クラス (87.7%) 74 区間→新たなクラス (12.3%)
2/5	570 区間→学習クラス (95.0%) 30 区間→新たなクラス (5.0%)	532 区間→学習クラス (88.7%) 68 区間→新たなクラス (11.3%)

次に，2016 年 2 月 3 日，4 日，5 日のデータを用いて異常検出実験を行った．2016 年 2 月 3 日の検出データでは 91.3%が学習したクラスに分類され，残りの 8.7%が新たなクラスとして認識された．2016 年 2 月 4 日の検出データでは 87.7%が学習したクラスに分類され，残りの 12.3%が新たなクラスとして認識された．2016 年 2 月 5 日の検出データでは 88.7%が学習したクラスに分類され，残りの 11.3%が新たなクラスとして認識された．新たに増加した 3 つのクラスに分類された特徴ベクトルを含む区間を Snort で異常検出すると，それぞれの区間においても学習結果同様，暗号化通信の異常やメール関連の異常が含まれていた．今回追加した特徴量によって，暗号化通信やメール関連の異常の識別能力が向上したと考えられる．

また，文献 [2] で用いられている特徴量を用いて同様の実験をした結果，2016 年 2 月 3 日，4 日，5 日の検出データでは表 2 に示すように，各日共に 95%程度が学習したクラスに分類された．

更に，2 月 3 日のデータに対して，2016 年 5 月 12 日に取得した Snort のルールを適用して異常検出する実験を行った．その結果，学習クラスに分類された 548 区間の内の 17 個の区間に 2016 年 2 月 13 日のルールには存在しない異常が含まれていた．また新たなクラスとして認識された 52 区間の内の 3 個の区間に新たな異常が含まれていた．

4. まとめ

本稿では観測されたパケットの特徴ベクトルをクラスタリングし，得られた各クラスに対して，シグネチャ型 IDS での検出結果の情報を付加することにより，未知の異常を検出する手法を提案した．今後の課題として，リアルタイムでの計測を行えるようにするためのプログラムの改良などが挙げられる．

参考文献

[1] 小島 俊輔, 中嶋 卓雄, 末吉 敏則, “ エントロピーベースのマハラノビス距離による高速な異常検知手法, ”情処学論, vol.52,no.2, pp.656-668, 2011.

[2] 今井 康平, 青木 茂樹, 宮本 貴朗, “ シグネチャ型 IDS を考慮したトラフィック特徴量のクラスタリングに基づく未知の異常検出, ”信学技報, ICSS2014-64, 2015.

[3] Snort https://www.snort.org/