2007 年 5 月 01 日(水)
1031060322 松本　亮介

One-Class SVM による ネットワークトラフィックからの不正アクセス検出（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 概略

ネットワークの不正アクセスが普及してきている中，未知の攻撃を検出するために，異常検出の手法に注目する．既知のデータを基に学習を行い，識別超平面を決定し分類を行う SVM（サポートベクターマシン）に対して，ネットワークトラフィックデータ内に含まれる攻撃の割合は少ないという特徴を利用し，割合で識別超平面を決定し分類を行う One-class SVM という手法を用いて異常を検出する.

ポートスキャンの一種である TCP SYN スキャンは，ACK Flag を受け取った後，コネクションを確立する直前で RST Flag を送り強制中断するために，ログに痕跡が残らない．そのため，コネクション確立以前の TCP Flag のやり取りから，ポートスキャンの傾向を読み取ることができると考えられる．このため，TCP Flag を 9 次元のベクトルデータとして作成し，それを利用して One-class SVM の手法で異常検出を行う.

通常の SVM では，学習を行った後，識別超平面を決定する際に非常に多くの計算量を必要とし，低スペックの計算機では時間がかかりすぎてしまう．そのため，プロファイルデータベースの更新に時間がかかり，更新する前に不正アクセスなどの攻撃を受けてしまう可能性がある. 一方 One-class SVM では，任意の割合を与えてその割合で識別超平面を決定するため，処理時間が少なくてすむ．また，割合で分類するため，知られていない未知の攻撃を検出する可能性もある.

SVM では，学習を行うために正常を異常として検出することは少ないが，未知の攻撃に対しては学習データに未知の攻撃データが含まれていないために異常を正常と検出してしまうことがある．そのため、学習する処理時間も考えると有効であるとはいえない．それに対して，One-class SVM は正常を異常と検出する割合は高くなってしまうが，異常を正常と検出する割合は SVM と比べて低くなっている. 不正アクセス検出としては，正しく攻撃を見つけ出すことが重要なため，正常を異常と検出することより、異常を正常とすることの方が問題になる．このことから，One-class SVM が有効であることがわかる.

参考文献

[1] 宮本雅人, “One-Class SVMによるネットワークトラフィックからの不正アクセス検出”