6S-05

線形分類器によるクロスサイトスクリプティング(XSS)の検知に関する考察

梅原 章宏 Umehara Akihiro[I], 松田 健 Matsuda Takeshi[II],
園田 道夫 Sonoda Michio[III], 趙 晋輝 Chao Jinhui[I]
中央大学 理工学部 情報工学科 Chuo University[I]
静岡理工科大学 総合情報学部 コンピュータシステム学科
Shizuoka Institute of Science and Technology[II]
サイバー大学 IT総合学部 Cyber University[III]

1. はじめに

近年インターネットの普及により,日常生活において様々な Web サイトを利用することが増加した.それに伴い,住所氏名やカード番号などの個人情報を盗むサイバー攻撃も増加している.

サイバー攻撃の手法の一つにクロスサイトスクリプティング攻撃(以下 XSS 攻撃)がある.この攻撃は Web アプリケーションの中にある検索ボックスなどの入力部分に対して,不正なスクリプト文を注入することで Web ページの改ざんや個人情報の流出を行うものである.従来の対策として構文解析によるフィルタが提案,実用化されている[1]が,XSS 攻撃の文字列は正常な文字列との区別が容易ではなく,機械的に攻撃か否かを判別することは難しい.

そこで本研究では,XSS 攻撃に含まれる記号に着目して攻撃と正常の文字列がどのように特徴空間上に存在するか調べ,これらのデータが線形分類器である SVM や SCW を用いて分類された場合,攻撃検出にどのような影響を与えるかということについて考察を行った.

2. 事前知識

この章では,本研究で行う考察に必要な知識についてまとめることにする.

2.1 XSS 攻撃

XSS 攻撃は Web アプリケーションの HTML や JavaScript を生成している部分の脆弱性を攻撃するサイバー攻撃の手法である.主な被害として Cookie 値を盗まれることによる成りすましや Web ページの改ざんなどがある.プログラム側の対策としては,'<'や'&'などの特別な記号を別な文字記号に置き換える,HTML の属性値をダブルクオート'"'で囲むといった方法があげられる.

2.2 SVM(Support-Vector Machine)

SVM は線形分類器の一つであり,

$$y(x) = \sum_{n=1}^{N} a_n t_n k(x, x_n) + b$$

で定義される.x は入力ベクトル,a はラグランジュ乗数,t∈{1,-1}は目標値,k(m,n)はカーネル関数,b はバイアスパラメータである(a,b は実数値をとる).

SVM はマージン(分類境界と最も近いデータ点との距離)を最大化することで,汎化誤差を最小化するような解を求める.

SVM にはハードマージン SVM とソフトマージン SVM がある.ハードマージン SVM は分類において誤りを全く許容しない.ソフトマージン SVM は多少の誤りを許容する代わりに,誤った分類に対してペナルティを与える.ペナルティ→∞となる時,ハードマージン SVM と等しくなる.

2.3 SCW(Exact Soft Confidence-Weighted Learning)[2]

SCW はオンライン(逐次学習)線形分類器の一つであり,CW[3]という線形分類器を改良したものである.CW は重みベクトルにガウス分布を導入し,データの過去の出現頻度を考慮した学習を行う.従来の線形分類器に比べて収束が速く精度も高いが,与えられた学習データを確実に分類できるような分類境界を求めようとするため,ノイズがあると性能が劣化する.

SCW はある程度の誤分類を許容し,SVM のようなマージンを考慮して学習を行うことで,汎化性能を向上させノイズに対して強くした分類器である.

3. 線形分類器を用いた検出実験

本研究では XSS 攻撃文と正常文を収集し,学習データとテストデータを生成した.それを線形分類器に入力し,攻撃文と正常文の分類を行う.使

Consideration on the Cross-Site Scripting Detection Using Linear Classifiers
Ⅰ Umehara Akihiro,Chao Jinhui, Chuo University
Ⅱ Matsuda Takeshi, Shizuoka Institute of Science and Technology
Ⅲ Sonoda Michio, Cyber University

Copyright ©2015 Information Processing Society of Japan.
All Rights Reserved.

用する線形分類器はハードマージン SVM, ソフトマージン SVM, SCW の 3 種類である.

3.1 使用するデータの作成

データの作成は攻撃文 915 個, 正常文 1155 個のうちからランダムに 500 個ずつを選択し, 合計 1000 個の攻撃文と正常文の混ざったデータを作成した. そのデータを 200 個ずつ 5 つのデータセットを作り, 1 つのデータセットをテストデータ, 残りを学習データとして交差確認を行った. また文字列をそのまま線形分類器に入力することは不可能なので, 文字列に含まれる記号・文字・数字それぞれの数の総和をとることで 3 次元ベクトルを生成し, それを入力として用いた.

攻撃文・正常文のデータは文献[4]に記載されている攻撃文や Web ページ[5]から収集した URL など, インターネットや文献, ツールの実行結果などから収集したものを利用した.

3.2 実験評価について

今回の実験は次の観点から評価を行った.

1. 正解率(Accuracy, 予測全体と答えが一致している割合)とその平均.

2. 正常文・攻撃文それぞれの精度(Precision, 予測に対して答えが正しいもの)とその平均.

3. 正常文・攻撃文それぞれの再現率(Recall, 答えの中で予測が正しいもの)とその平均.

4. F 値 (F-measure, 精度と再現率の調和平均).

4. 結果・考察

交差確認用のデータを 2 つ作成し, 実験を行った. 結果を表 1 に示す.

		データ 1			データ 2		
		Hard SVM	Soft SVM	SCW	Hard SVM	Soft SVM	SCW
正解率		0.658	0.672	0.491	0.589	0.673	0.550
精度	正常	0.863	0.788	0.934	0.730	0.789	0.229
	攻撃	0.454	0.557	0.038	0.456	0.560	0.873
再現率	正常	0.613	0.639	0.492	0.535	0.643	0.645
	攻撃	0.768	0.725	0.158	0.698	0.726	0.531
F 値	正常	0.715	0.704	0.643	0.608	0.707	0.336
	攻撃	0.566	0.628	0.138	0.532	0.630	0.659

表 1:実験結果

ここで, パラメータはハードマージン SVM は σ=20, ソフトマージン SVM は σ=1.5, C=0.5, SCW は C=2.0, η=0.5 である.

また図 1 は, 表 1 における正解率, 精度, 再現率, F 値について, データ 1 とデータ 2 の相加平均をとったものをグラフ化したものである.

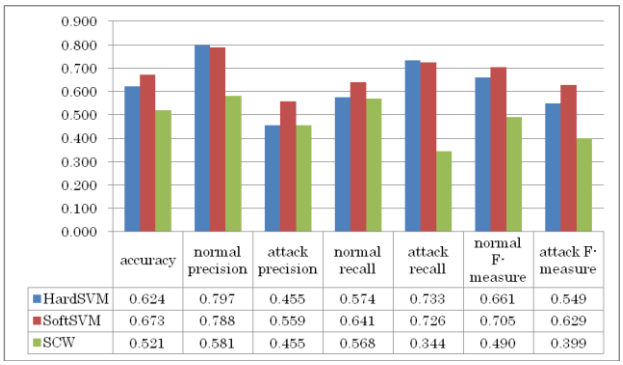

図 1:相加平均の比較グラフ

結果を見ると使用した線形分類器において正解率がおよそ 55%-65%となり, ある程度の分類は可能なもののあまり良いといえる結果にはならなかった. 表 1 を見ると正常と攻撃の精度の値がトレードオフになっていることから, 特徴抽出を行ったデータについて線形分離が難しく, そのためにうまく分類ができなかったものと考えられる. 今回の特徴抽出の手法を考慮すると, 単純に出現記号の頻度を XSS 攻撃の特徴としてとらえるのは, 線形分類器を利用する上では効果的な手法とはいえないと考えられる.

改善案として, 特徴抽出の手法の変更, パラメータの調整, データを増やすことが考えられる. 特徴抽出の手法については, XSS 攻撃において攻撃文と正常文を明確に差別化できるような特徴を発見することで, 線形分類器を用いた検知の精度を大きく向上させることが可能であると考えられる. また特徴抽出の手法を変えることで入力の分布も変化するため, 手法にあったパラメータの調整が必須になると考えられる.

参考文献

[1]http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-iv-the-xss-filter.aspx

[2]Jialei Wang, Peilin Zhao, Steven C.H. Hoi "Exact Soft Confidence-Weighted Learning" ICML 2012

[3]Mark Dredze, Koby Crammer, Fernando Pereira "Confidence-Weighted Linear Classification" ICML 2008 pp.264-271

[4]Jeremiah Grossman, Robert "Rsnake" hansen, Petko "pdp" D.petkov, Anton Rager, Seth Fogie "XSS Attacks" SYNGRESS 2007 ISBN:978-1597491543

[5] http://tshinobu.com/lab/get-page-link/

Copyright ©2015 Information Processing Society of Japan.
All Rights Reserved.