# DDoS Detection in SDN Switches using Support Vector Machine Classifier

Xue Li[1, a *], Dongming Yuan[2,b], Hefei Hu[3,c], Jing Ran[4,d] and Shulan Li[5,e]

[12345]Beijing University of Posts and Telecommunications, Beijing, 100876

[a]lx_laura@163.com

**Keywords:** SDN Switches, Distributed Denial-of-Service (DDoS), Support Vector Machine (SVM), Genetic Algorithm (GA)

**Abstract.** Compared with traditional network, Software Defined network (SDN) technology contains data plane, control plane and application plane. The control plane centralized controls multiple switches instead of only one switch. Therefore, SDN has more security requirements. The existing network security equipment already can no longer adapt to the environment of SDN. Distributed Denial-of-Service Attacks (DDoS) is one of the most major threats. DDoS detection is necessary for SDN switches. Support vector machine (SVM) classification technology is widely used in various fields. In this article, we will detect DDoS attacks using SVM optimized parameter c and g with cross validation-genetic algorithm (CV-GA). The experiments show that CV-GA-SVM classification performs better than others.

## Introduction

In recent years, Software defined network (SDN) as a new research highlight appears in the development of computer network [1]. SDN was originated from the Clean Slate project at Stanford University in the United States. With further researches, SDN which gradually obtained the wide recognition of academia and industry, has become the mainstream direction of the Internet's development in the future. The network control plane is separated from the underlying network in SDN technologies. Instead of the traditional closed control plane, the open plane controls the entire network by the centralized controller, and allows a programmable network. SDN has good openness and flexibility to bring the huge change of network. According to the SDN's architecture which defined by Open Networking Foundation (ONF) [2], SDN is divided into the infrastructure layer, the control layer, the application layer, the north interface and the south interface which connect the layers of data exchange.

Distributed Denial-of-Service (DDoS) is a destruction of the effectiveness of network service. It leads that a suffered host or network can't receive and deal with the request from outside world. So the host or network cannot provide normal service for a legitimate user. Thus the attack forms a denial of service. Compared with the traditional network, SDN has more flexibility and controllability so that the SDN is more vulnerable to DDoS attacks [3]. Therefore, the detection of DDoS attacks is one important research direction of SDN security.

In this paper, compared with other existing methods, we first prove the superiority of SVM based on traffic flow for DDoS detection in SDN switches. Secondly, this paper proposes a parameter optimization for SVM classification based on traffic flow to improve the quality of detection. We come up with CV-GA (cross validation - genetic algorithm) with adjusting factor to optimize parameter. At last, we compare results with un-optimized SVM.

## Related Work

Some methods for detecting DDoS attacks in SDN switches have already been proposed. In [4], R. Braga and E. Mota proposed a lightweight method to DDoS attack detection based on traffic flow. The authors extracte six characteristic values from 41 flow characteristic values and use the un-optimized SOM mode to detect DDoS attacks. The less characteristic values to reduce the

© 2015. The authors - Published by Atlantis Press 

computational complexity is the advantage. One disadvantage is that the accuracy of test results is low, and the miscarriage rate is higher.

In [5], the authors put forward a kind of traffic detection model based on particle swarm the BP neural network, combined with the global searching of particle swarm optimization (PSO) algorithm and the fast convergence of the genetic algorithm to detect DDoS attacks. In [6], the authors proposed a kind method based on clustering algorithm to detect DDoS attacks.

Our approach differs from the above methods. We propose the optimized SVM detection based on traffic flow with CV-GA (cross validation - genetic algorithm) with adjusting the factor to optimize parameters.

## Background

**The data source.** Test data from DARPA Intrusion Detection Data Sets of CYBER SYSTEMS AND TECHNOLOGYGROUP in MIT Lincoln Laboratory. With the support of the Defense Advanced Research Projects Agency (DARPA ITO) and the Air Force Research Laboratory (AFRL/SNHS), the research team collected a lot of materials about network intrusion data. MIT Lincoln laboratory sampled 9 weeks. Each traffic is a data, which contains 41 characteristic values and a label of category (normal or abnormal).

**Support vector machine.** SVM [7] is to solve the problem how to classify the input variable sample. Through constructing the optimal hyperplane segmentation, SVM makes a class on one side of the hyperplane and another class on other side of the hyperplane, so as to realize the classification problem of the sample.

Samples for training set:

$$(x_1, y_1),\ (x_2, y_2),\ \cdots,\ (x_N, y_N)$$

Among above, $x_i \in \boldsymbol{R}^d$ (the dimension of sample data is $d$), category label $y_i \in \{-1, 1\},\ i \in [1, N]$.

The optimal separating hyperplane for quadratic programming problem is

$$\min_{w,b,\xi} \frac{1}{2}\boldsymbol{w}^T\boldsymbol{w} + C\sum_{i=1}^{N}\xi_i$$

$$\text{s.t.} \quad y_i(\boldsymbol{w}^T\boldsymbol{x}_i + b) \geq 1 - \xi_i, \xi_i \geq 0, i = 1,\ \cdots,\ N \tag{1}$$

Among above, $C$ is the punish coefficient (or regularization coefficient). Combining the Lagrange method and the principle of duality, the objective function can be converted into

$$\min_{\alpha} \frac{1}{2}\sum_{i,j=1}^{N}\alpha_i\alpha_j y_i y_j K(x_i, x_j) - \sum_{i=1}^{N}\alpha_i$$

$$\text{s.t.} \quad \sum_{i=1}^{N} y_i\alpha_i = 0,\ C \geq \alpha_i \geq 0,\ i = 1,\ \cdots,\ N \tag{2}$$

Among above, $K(x_i, x_j)$ is the kernel function. Mainly Types are

1. The linear kernel function: $K(x_i, x_j) = {x_i}^T x_j$; (3)
2. The polynomial kernel function: $K(x_i, x_j) = (\gamma {x_i}^T x_j + r)^p,\ \gamma > 0$; (4)
3. The radial basis kernel function: $K(x_i, x_j) = exp\left(-\gamma\|x_i - x_j\|^2\right),\ \gamma > 0$; (5)
4. The two layer perceptron kernel function: $K(x_i, x_j) = \tanh(\gamma {x_i}^T x_j + r)$. (6)

## CV-GA-SVM Detection of DDoS Attack

When using SVM to detect DDoS attacks, two parameters affecting the effects of classification is the punish parameters $C$ and the kernel function parameters $\gamma$. In order to make the DDoS detection effect better, we use the GA looking for the punish parameters $C$ and the kernel function parameters $\gamma$ of the global optimal solution. Algorithm flow chart shows in Fig.1.

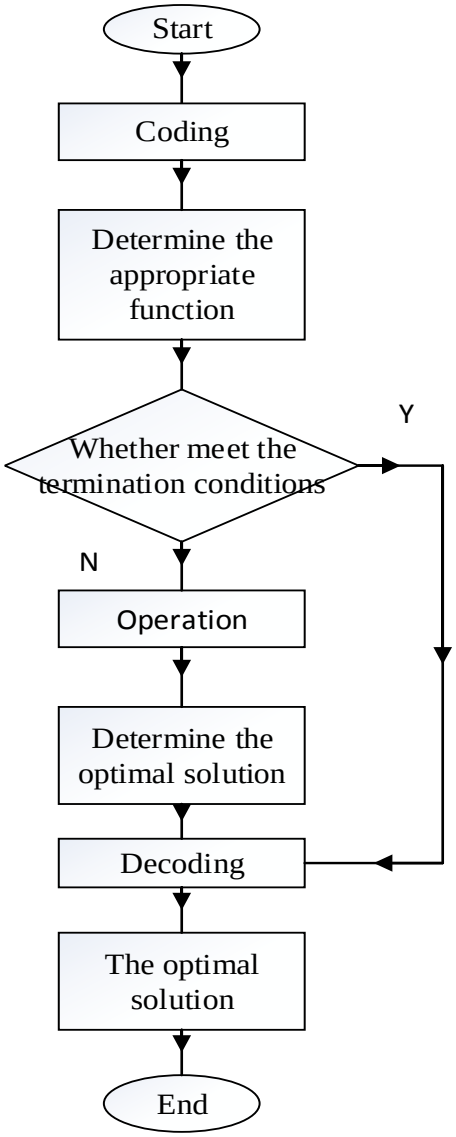


Fig. 1

The selection of the appropriate function is important for GA optimization model. In this article, in order to better adapt to the characteristic of SDN switches, we put forward the appropriate function based CV with adjustment factors. The expression of appropriate function as follow.

$$F = \lambda_1 TN + \lambda_2 FN \quad (7)$$

Among above, $\lambda_1 + \lambda_2 = 1, 0 \leq \lambda_1 \leq 1, 0 \leq \lambda_2 \leq 1, TN$ shows the ratio of normal packets to be as attack packets, $FN$ shows the ratio of attack packets to be as normal packets. $\lambda_1$ and $\lambda_2$ can be adjusted according to different requirements.

CV is a statistical analysis method used to verify the performance of classifier. Its basic idea is to group the original data, one part as the training set, the other part as a validation set. Firstly, it use training set to train a classifier. Validation set is used to test the training set to get the optimal performance.

Firstly, we use CV to cross validation the SVM classification model, in order to choose the best punish parameters $C$ and kernel function parameters $\gamma$. Then we use the SVM model with the above result which as the initial parameter values. Preliminary classification results are obtained. The preliminary classification result is the initial value of the appropriate function in the GA model, further to find the optimal punishment parameters $C$ and kernel function parameters $\gamma$. The final SVM parameters are obtained by GA model. Finally, we use the SVM to detect DDoS attack packets with the final punish parameters $C$ and kernel function parameters $\gamma$.

## Results

We randomly select 6000 items from more than 400000 items, as the experimental sample data. 5000 items are selected randomly as the training set, 1000 items are selected randomly as the test set.

In Table 1, we compare the CV-GA-SVM model which uses the best punish parameters $C$ and kernel function parameters $\gamma$ with the un-optimized SVM mode. This can prove that the mentioned optimization method improves the detection result of SVM.

Table 1 Results of CV-GA-SVM model and SVM

| | TN | FN |
|---|---|---|
| the un-optimized SVM mode | 0.53% | 0.45% |
| the CV-GA-SVM model | 0.35% | 0.00% |

In Table 2, respectively using the CV-GA-SVM model, the SOM model, the BP neural network model and the clustering model to classify test samples, we get results. The results prove that the CV-GA-SVM model is superior to other methods. Fig 3 shows the classification results.

Table 2 Results of CV-GA-SVM model and other models

| | TN | FN |
|---|---|---|
| the CV-GA-SVM model | 0.35% | 0.00% |
| the SOM model | 1.24% | 1.15% |
| the BP neural network model | 0.53% | 1.38% |
| the clustering model | 2.84% | 0.45% |

## Conclusion

Compared with other methods, the SVM model using the CV-GA to optimize parameters can improve the effect of the classification and the detection of DDoS attacks. At the same time, we put forward the appropriate function with adjustment factors, which can be used not only in the SDN switches. According to different scenarios, the appropriate function also can be adjusted to use. It has general applicability.

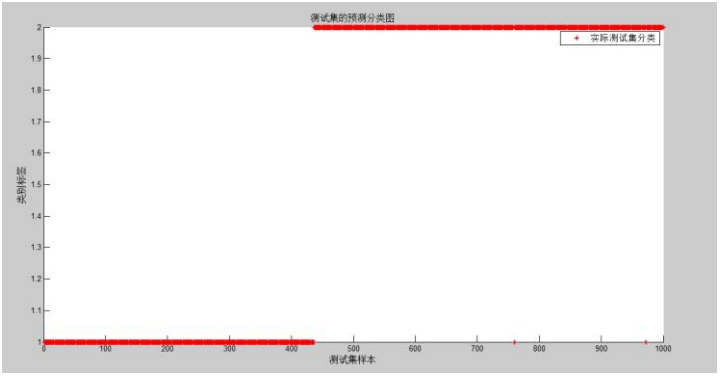


Fig. 3 The result of CV-GA-SVM model


## Acknowledgements

This work was supported by the National Natural Science Foundation of China (No. 61272518) and 2013RC0208 research of the information access technology for complex information system.


## Reference


[1] McKeown N, Anderson T, Balakrishnan H, et al. OpenFlow: enabling innovation in campus networks [C]. SIGCOMM Comput Commun Rev, 2008, 38 (2): 69-74.

[2] ONF (Open Networking Foundation). Software-Defined Networking: The New Norm for Networks [M]. ONF Whitepaper, 2012.7-11.

[3] Shin S, Porras P, Yegneswaran V, et al. FRESCO: Modular composable security services for software-defined networks [C]. Proceedings of Network and Distributed Security Symposium, San Diego: Internet Society, 2013:135-139.

[4] R. Braga, E. Mota, A. Passito. Lightweight DDoS flooding attack detection using NOX/OpenFlow [C]. In 2010 IEEE 35th Conference on Local Computer Networks (LCN), Denver: LCN, (Oct 2010): 233-236.

[5] Li Feng. Application of particle swarm BP neural network in DDoS attack detection [C]. Network and Communication, 2014:49-51.

[6] Li Lijuan, Li Shandong. Application of adaptive clustering algorihm on DDoS attacks detection. Computer Engineering and Applications, 2012, 48(2): 86-89.

[7] Corinna Cortes, Vladimir Vapnik, Support-Vector Networks, Machine Learning [C], 1995: 20:273-297.