Evaluating Machine Learning Algorithms for Detecting DDoS Attacks*

Manjula Suresh and R. Anitha

Department of Mathematics and Computer Applications,
PSG College of Technology, Coimbatore, India
manjuasmi3@gmail.com, anitha_nadarajan@mca.psgtech.ac.in

Abstract. Recently, as the serious damage caused by DDoS attacks increases, the rapid detection of the attack and the proper response mechanisms are urgent. Signature based DDoS detection systems cannot detect new attacks. Current anomaly based detection systems are also unable to detect all kinds of new attacks, because they are designed to restricted applications on limited environments. However, existing security mechanisms do not provide effective defense against these attacks, or the defense capability of some mechanisms is only limited to specific DDoS attacks. It is necessary to analyze the fundamental features of DDoS attacks because these attacks can easily vary the used port/protocol, or operation method. Also lot of research work has been done in detecting the attacks using machine learning techniques. Still what are the relevant features and which technique will be more suitable one for the attack detection is an open question. In this paper, we use the chi-square and Information gain feature selection mechanisms for selecting the important attributes. With the selected attributes, various machine learning models, like Navies Bayes, C4.5, SVM, KNN, K-means and Fuzzy c-means clustering are developed for efficient detection of DDoS attacks. Then our experimental results show that Fuzzy c-means clustering gives better accuracy in identifying the attacks.

Keywords: Classifier, Navies Bayes, SVM, C4.5, K-NN, K-means, Fuzzy c-means.

1 Introduction

Distributed Denial of Service (DDoS), is a relatively simple, yet very powerful technique to attack Internet resources as well as system resources. Distributed multiple agents consume some critical resources at the target within the short time and deny the service to legitimate clients. As a side effect, they frequently create network congestion on the way from source to target, thus disrupting normal Internet operation and denying the services to many legitimate users.

DDoS is a large-scale, coordinated attack on the availability of services of a victim system or network resources, launched indirectly through many compromised computers called zombies on the internet. Using client/server technology, the

* This work is a part of the Collaborative Directed Basic Research on Smart and Secure Environment project, funded by NTRO and AISRF.

D.C. Wyld et al. (Eds.): CNSA 2011, CCIS 196, pp. 441-452, 2011.

perpetrator is able to multiply the effectiveness of the attack significantly by using the resources of many unwitting accomplished zombies which serve as attack platforms. The zombies carry out the actual attack by increasing the traffic to a victim machine significantly. As a result, the victim machine loses all its computing and communication resources.

Many researchers have analyzed DDoS attacks and contributed some defense mechanisms. The widely used defense techniques are detection, filtering and traceback.

Detection suffers from efficiently differentiating the normal stream and abnormal stream of traffic. Filtering clogs up during heavy traffic whereas traceback can only be effective under subsidized traffic, so performed mostly after the closing of the attack. Most of the existing detection mechanism have limited success because of the following challenges (i) the attack itself often uses legitimate requests to flood the target and this makes it hard to distinguish an attack traffic from legitimate traffic (ii) fast real time detection is difficult because of huge amount of data involved in current computer networks.

Abnormal changes in the resource usage due to DDoS attack could be detected using statistical methods. The problem with statistics based detection is that it is not possible to find out the normal network packet distribution. Rather, it can only be simulated as a uniform distribution [10]. Some methods which apply data mining techniques, can obtain a high correction rate in detecting the attack. However, these methods usually can't be used in real-time computing [14]. Some research papers suggest the usage of clustering methodology to formulate the normal patterns. One of the advantages of clustering methods over statistical methods is that they do not rely on any prior known data distribution. There are many variables that can be used to identify normal network patterns [10]. But extracting the important and relevant attributes from huge network is crucial for modeling network behaviors so that attack behaviors can be differentiated clearly from normal one. In this paper, based on a comprehensive analysis for the current research challenges in DDoS, evaluating machine learning algorithms for detecting DDoS is presented, which includes feature extraction, classification and comparison. Within this evaluation, some recently developed machine learning methods for detecting DDoS are applied and their performances are evaluated based on experiments on public benchmark datasets such as CAIDA [20]. Although various hybrid approaches may be employed, it is illustrated that these evaluation results of research challenges are mainly suitable for machine learning methods. Finally among various machine learning algorithms, fuzzy c-means clustering technique provides better performance over many of the existing methods. A brief report of this work is available in [1].

The rest of the paper is organized as follows. Section 2 summarizes related studies in the area of DDoS attack detection. Next, in section 3, the proposed method for the detection of DDoS attacks is described in detail. Section 4 presents the data collected and the experimental results. Finally, in section 5, we conclude our work with directions of further studies.

2 Related Work

Two important and challenging research problems in detecting DDoS attacks are:

1. extracting a valid and sufficient subset of features that can be used to build efficient models to identify a DDoS attack; and

2. ranking the efficacy of the various machine-learning techniques that have been utilized in the detection process.

For most problem domains, the process of feature reduction which involves extracting the most significant and relevant attributes or features prior to applying modeling techniques (such as machine learning and statistical techniques) can lead to a major improvement in the time required in training and testing the model. However, in comparison with other problem domains, extracting a set of features that characterize Internet traffic to the point of being able to distinguish normal traffic from anomalous traffic is particularly difficult. One problem, for example, is that nodes in the Internet experience widely differing traffic flux densities caused by the large variations in the number of users seen at each node. This makes it difficult to decide as to what constitutes "normal" traffic on the Internet. Another problem, and one that can be seen from the discussion on the detection techniques already presented, is that there are potentially a large number of variables that can be used to characterize network traffic patterns. Nevertheless extracting the important and relevant attributes from network traffic is crucial for modeling network behaviours so that attack behaviours can be differentiated clearly from normal behaviour. This feature-extraction problem has been studied by a number of groups. For example Xu et. al. [4] selected eight relative values as features that are independent from the network flow. Zargar et. al. [24] propose and investigate the identification of effective network features for probing attack detection using the principal component analysis (PCA) method to determine an optimal feature set. Jin et al. [5] discussed the application of multivariate correlation analysis to DDoS detection and proposed a covariance analysis model for detecting flooding attacks. They used all of the flag-bits in the flag field of the TCP header as features in the covariance analysis model. The authors have demonstrated the successful use of the proposed method in detecting SYN flooding attacks which is an important form of DDoS attacks. However, the method has the major limitation that there is no guarantee that the 6 flags are valid or sufficient features to detect all forms of DDoS attack with consistent accuracy.

A widely diverse range of statistical methods and machine learning techniques could be used to detect abnormal changes in the resource usage that are indicative of a DDoS attack. However both approaches have their limitations. For example one identifiable problem with statistics based detection is that it is not possible to find out the normal network packet distribution. Rather, it can only be simulated as a uniform distribution. Some research papers suggested that this problem may be resolved by using clustering methodologies to formulate the normal patterns, since one of the advantages of clustering methods over statistical methods is that they do not rely on any prior known data distribution. While machine learning techniques, typically drawn from the allied field of data mining, have been shown to produce a high degree of accuracy in detecting DDoS attacks, they also have their own limitations. For example these techniques require a lengthy learning period and hence currently these methods can't operate in real-time.

Despite these current limitations, a solution to the problem of reliable DDoS detection will come from either or both these domains and considerable research effort continues to be directed to this end. For example Seo et al. [17] have used a multiclass SVM classification model to detect DDoS attack. In the work of Xu et al. [18],

a group of new features was also introduced including the composition of relative values as part of an expanded set of detection information. They also proposed a new approach of using attack intensity to detect a DDoS event. In [15], Paruchuri et. al. proposed a new probabilistic packet marking (PPM) scheme called TTL-based PPM scheme, where each packet is marked with a probability inversely proportional to the distance traversed by the packet so far, enabling a victim source to traceback the attack source. In [3], Cheng et. al. proposed a novel algorithm to detect DDoS attacks using IP address feature values using support vector machine (SVM) classification. Nguyen et. al. [14] have developed an Anti-DDoS framework for detecting DDoS attack proactively utilising K-NN Classifier. They used the k-nearest neighbour method to classify the network status into each phase of DDoS attack. However, while the K-NN approach is excellent in attack detection, the detector is computationally expensive for real-time implementation when the number of processes simultaneously increases. As has been indicated previously the problem of computational intensity is critical in the DDoS problem as it is in other applications of data mining where large databases are analysed.

One of the key resources used to evaluate the performance of DDoS detection techniques is the KDD dataset. The set contains 14 attacks which is used for testing and model creation. Several methods have been proposed to extract useful features from this dataset and a wide range of classifiers drawn from areas such as statistics, machine learning and pattern recognition have been evaluated against this dataset. For example in Kim et. al. [7], the 1999 KDD data set was pre-processed followed by learning and testing process. In the learning process they used polynomial, kernel functions linear, and radial bias function (RBF). A classification accuracy of 93.56% was achieved. A SVM based one-class classifier is also used to perform anomaly detection in [4]. The training data in the feature space was mapped into a new feature space. Yuan et. al. [23] used the cross-correlation analysis to capture the traffic patterns and then to decide where and when a DDoS attack may possibly arise.

3 Proposed Work

The following study discusses the extraction of a feature set from two different sources of datasets of Internet traffic. These are the public-domain CAIDA Dataset [20] and traffic collected on the smart and secure environment (SSE) Network. Various types of DDoS attacks are studied to select the traffic parameters that change unusually during such attacks. Twenty-three features are collected and ranking the twenty-three features is done with Information Gain and Chi-Square statistic which reduces the number of features to eight. All the features used in this paper are calculated at an interval of 1 second. Since these classes are well divided as attack and normal, it is possible to apply various machine learning algorithms for the detection. The approach considered is to use the feature selection mechanism discussed previously and build the classifier using various machine learning algorithms such as SVM, K-NN, Naive Bayesian, Decision Tree, K-means and Fuzzy c-means clustering. This phase of the study is an evaluation of the performance of the selected set of machine learning algorithms in detecting DDoS attacks. The performance measures are the receiver operating characteristic (ROC) curve and F-measure. An important

conclusion drawn from the experimental results is that, of the various methods used, Fuzzy c-means clustering is very efficient in detecting DDoS attacks.

3.1 Feature Extraction

For the first phase of the study, the following lists of 23 features are extracted.

Table 1. Basic Features

SNo	Feature	Description
1	OnewayRatio	The ratio of one way connection packets to all packets.
2	AverageLengthIPFlow	Number of Ip packets by Number of Ip flows
3	RatioofInOut	Ratio between incoming and outgoing packets
4	Entropyflowlength	Entropy of IP flow length
5	Entropyprotocols	Entropy of the packet ratios of the three protocols TCP, UDP and ICMP
6	Ratiotcp	Ratio of TCP Protocol
7	Ratioudp	Ratio of UDP Protocol
8	Ratioicmp	Ratio of ICMP Protocol
9	Datalength	Number of data bytes from source to destination
10	Dstdatalength	Number of data bytes from destination to source
11	Urg	Number of packets where urg flag is set
12	Service	Destination port mapped to service
13	Prototype	Connection protocol (tcp,udp,icmp)
14	Land	Number of connection is from/to the same host/port
15	Wrongfrag	Number of wrong fragments
16	Segmenterror	Number of connections that have SYN errors
17	Srccnt	Number of connections to the same service
18	Dstcnt	Number of connections having the same destination host
19	Syncnt	Number of packets where syn flag is set
20	Fincnt	Number of packets where fin flag is set
21	Ackcnt	Number of packets where ack flag is set
22	Pshcnt	Number of packets where psh flag is set
23	Rstcnt	Number of packets where rst flag is set

Chi square and Information Gain are applied to measure the importance of each feature. The Information gain of a given attribute X with respect to the class Y is the reduction in uncertainty about the value of Y, after observing values of X. The uncertainty about the value of Y is measured by its entropy defined as

$$\boldsymbol{H(Y) = -\sum_i P(y_i)\log_2(P(y_i))} \tag{1.1}$$

where $P(y_i)$ is the prior probabilities for all values of Y. The uncertainty about the value of Y after observing values of X is given by the conditional entropy of Y given X defined as

$$\boldsymbol{H(Y|X) = -\sum_j P(x_j \sum_i P(y_i|x_j)\log_2(P(y_i|x_j)\log_2(P(y_i|x_j))} \tag{1.2}$$

where $P(y_i|x_j)$ is the posterior probabilities of Y given the values of X. The information gain is thus defined as

$$\boldsymbol{IG(Y|X) = H(Y) - H(Y|X)} \tag{1.3}$$

By calculating information gain, the correlations of each attribute can be ranked to the class. The most important attributes can then be selected based on the ranking.Chi-square [22] measures the lack of independence between a feature X and a cluster Y. It can be compared to the chi-square distribution with one degree of freedom to judge extremeness:

$$\chi^2 = \sum_{i=1}^{r}\sum_{j=1}^{k}\frac{(A_{ij}-E_{ij})^2}{E_{ij}} \tag{1.4}$$

where r is the number of feature and k is number of clusters, A_{ij} is number of instances for which the value of a feature is i and the value of the cluster is j, E_{ij} is the expected number of instances of A_{ij}. The larger the χ^2 value, the more important the feature is to the cluster. Thus ranking the importance of each feature with respect to the clusters based on the value of χ^2 for the proposed work is considered.

Based on the χ^2 value and information gain rank, eight features are considered as the important features. Table 2 gives the ranking of the features based on chi-square and information gain.

Table 2. Feature ranking

Features	Chi-square Rank	Information gain Rank
Ratio ICMP	1	1
Land	2	2
Ratio UDP	3	3
One way Ratio	4	4
Ratio TCP	5	5
Protocol Type	6	6
AverageLengthIPFlow	7	8
Ratio of In/Out Packets	8	7

Based on Chi-square and information gain the following eight features are selected for the detection of DDoS attacks.

a) One Way Connection Density (OWCD):

An IP packet without a corresponding reverting packet composes a One-Way Connection (OWC). In a sampling interval T, the ratio of OWC packets to the all packets is called One-Way Connection Density (OWCD).

$$OWCD = \frac{\sum OWC\ Packets}{\sum IP\ Packets} * 100 \tag{1.5}$$

b) Average Length of IP Flow (L_{ave_flow}):

IP Flow, a concept which is used widely in network analysis area, means that a packets set has a same five-element-group (source IP address, source port, destination IP address, destination port and protocol). Length of IP flow means the number of packets belong to certain IP flow.

$$L_{ave\_flow} = \frac{\sum IP\ Packets}{\sum IP\ flows} \tag{1.6}$$

c) Incoming and Outgoing Ratio of IP packets (R_{io}):

Normally the ratio between incoming and outgoing packets is steady. But in DDoS attack, quickly R_{io} increases.

$$R_{io} = \frac{\sum incoming\ IP\ packets}{\sum outgoing\ IP\ Packets} \tag{1.7}$$

d) Ratio of TCP Protocol (R_t):

$$R_t = \frac{\sum TCP\ packets}{\sum IP\ Packets} \tag{1.8}$$

e) Ratio of UDP Protocol (R_u):

$$R_u = \frac{\sum UDP\ packets}{\sum IP\ Packets} \tag{1.9}$$

f) Ratio of ICMP Protocol (R_i):

$$R_i = \frac{\sum ICMP\ packets}{\sum IP\ packets} \tag{1.10}$$

g) Land:The number of packets having the source ip address same as the destination ip address.

h) Protocol-type: Type of the Protocol, eg: TCP, UDP, ICMP etc.

All the above mentioned features except Land have been selected based on the principles mentioned in Xu et al.[18], are used to classify the network status. Each variable is normalized to eliminate the effect of difference between the scales of the variables, as proposed by Lee et al. [6]. With normalization, variables become

$$z = \frac{x - \overline{x}}{\sigma} \tag{1.11}$$

where x, $\overline{x}$, and $\boldsymbol{\sigma}$, denote the value of each feature, the mean of the sample dataset, and the standard deviation, respectively.

The first step is to extract these eight features from the dataset consisting of both normal and attack data patterns. In the experiments a sampling frequency of one second is used. The next step is to train the machine learning techniques with these datasets. In the detection phase, the same set of eight features are computed for the given network traffic and the traffic is labeled as attack or normal based on the majority of the values computed by the machine learning classifiers.

3.2 Machine Learning Algorithms

In this section, we briefly describe the various machine learning algorithms employed in the proposed framework.

Naive Bayes

The Naïve Bayes is a simple probabilistic classifier [13]. It assumes that the effect of a variable values on a given class is independent of the values of other variables. This assumption is called class conditional independence.

C4.5

C4.5 algorithm which was developed by Quinlan is the most popular tree classifier. This algorithm is based on the $ID3^2$ algorithm that tries to find small decision tree.

K-Mean Clustering

In K-Mean clustering [2], assignment of the data points to clusters depends upon the distance between cluster centroid and data point.

SVM

In classification and regression, Support Vector Machines are the most common and popular method for machine learning tasks [21]. In this method, a set of training examples is given with which each example is marked belonging into one of two categories. Then, by using the Support Vector Machines algorithm, a model that can predict whether a new example falls into one categories or other is built.

k-NN Classifier

The k-NN algorithm [14] is a similarity-based learning algorithm and is known to be highly effective in various problem domains, including classification problems. Given

a test element dt, the k-NN algorithm finds its k nearest neighbors among the training elements, which form the neighbourhood of dt. Majority voting among the elements in the neighborhood is used to decide the class for dt.

FCM Clustering

Fuzzy c-means (FCM) [2] is a method of clustering which allows one piece of data to belong to two or more clusters. This method (developed by Dunn in 1973 and improved by Bezdek in 1981) is frequently used in pattern recognition. It is based on minimization of the following objective function:

$$J_m = \sum_{i=1}^{N}\sum_{j=1}^{C} u_{ij}^{m}\left\|x_i - c_j\right\|^2, \quad 1 \le m < \infty$$

where m is any real number greater than 1, u_{ij} is the degree of membership of x_i in the cluster j, x_i is the ith of d-dimensional measured data, c_j is the d-dimension center of the cluster, and ||*|| is any norm expressing the similarity between any measured data and the center.

4 Experimental Results

The CAIDA Dataset [20] is used in the experiments as the attack component. Data collected on the SSE network provided the normal traffic component. Classification of attack and normal traffic is done using an open-source tool called KNIME (Konstanz Information Miner) version 3 [8]. Table 3 shows details of the CAIDA dataset and the normal traffic collected on the SSE network. Table 4 shows the correct classification and the attack detection time. Table 5 shows the F-measure details and Figure 1 shows the evaluation results using ROC curves for the selected machine learning techniques. Based on the results of these experiments, the Fuzzy C-means based classification gives the best result in detecting DDoS attacks.

Table 3. Samples collected

Network Data	Data Type	Total Number of Packets
Trained	Attack (CAIDA)	945372
	Normal	110535
Untrained Test Data	Attack (CAIDA)	324098
	Normal	36485

Table 4. Classification results

Method Used	Correct Classification %	Detection Time (in seconds)
Fuzzy C Means	98.7	0.15
Naive Bayesian	97.2	0.52
SVM	96.4	0.23
KNN	96.6	0.26
Decision Tree	95.6	0.25
K-Means	96.7	0.20

Table 5. F-Measure details of classifiers

Method	TP	FP	TN	FN	F-Measure
Fuzzy C Means	298	2	270	3	0.987
Naive Bayesian	290	10	256	17	0.972
KNN	280	20	243	30	0.969
SVM	282	18	253	20	0.964
K-Means	285	15	273	0	0.9669
Decision Tree	278	22	218	55	0.956

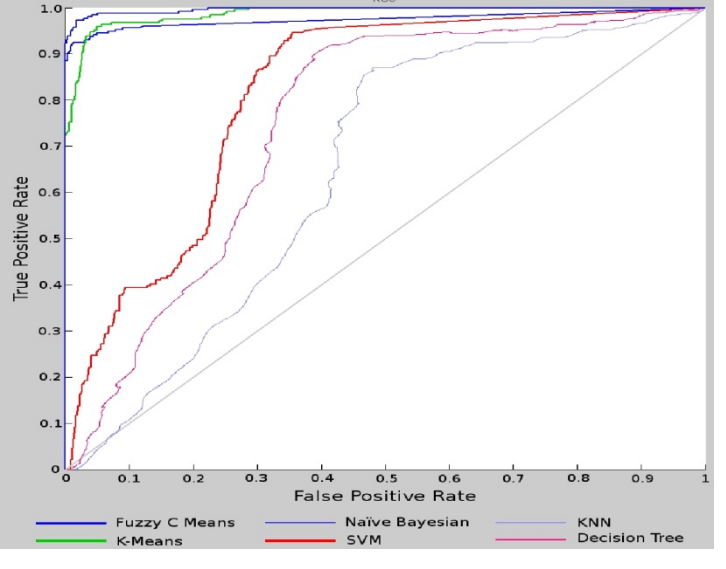

Fig. 1. False vs true positive rate

5 Conclusion

This paper, deals with the evaluation of machine learning algorithms for effectively detecting the DDoS attacks. CAIDA data set is used as the attack data and based on chi-square and information gain ranking, relevant features have been selected. Experimental results show that Fuzzy c-means clustering gives better classification and it is fast compared to the other algorithms.

References

1. Anitha, N.: An Investigation into the detection and Mitigation of Denial of Service (DoS) Attacks, Monograph. Springer, Heidelberg (in press, 2011)
2. A Tutorial on Clustering Algorithms, http://Clustering-FuzzyC-means.htm
3. Cheng, J., Yin, J., Liu, Y., Cai, Z., Li, M.: DDoS Attack Detection Algorithm Using IP Address Features. In: Deng, X., Hopcroft, J., Xue, J. (eds.) FAW 2009. LNCS, vol. 5598, pp. 207–215. Springer, Heidelberg (2009)
4. Erskin, E., Arnold, A., Prerau, M., Portnoy, L.: A Geometric Framework for Unsupervised Anomaly Detection: Detecting Intrusions in Unlabeled Data. In: Barbará, D., Jajodia, S. (eds.) Applications of Data Mining in Computer Security, pp. 77–102. Kluwer, Dordrecht (2002)
5. Jin, S., Yeung, D.S.: A covariance analysis model for ddos attack detection. In: Proceedings of IEEE International Conference on Communications, June 20-24, vol. 4, pp. 1882–1886. IEEE, Los Alamitos (2004)
6. Jang, J.-S.R., Sun, C.-T., Mizutani, E.: Data Clustering Algorithms. In: Neuro-Fuzzy and Soft Computing – A Computational Approach to Learning and Machine Intelligence. ch.15, pp. 423–433. Prentice-Hall, Inc., Englewood Cliffs (1997)
7. Kim, D., Park, J.: Network-Based Intrusion Detection with Support Vector Machines. In: Kahng, H.-K. (ed.) ICOIN 2003. LNCS, vol. 2662, pp. 747–756. Springer, Heidelberg (2003)
8. KNIME, http://www.knime.org (accessed February 7, 2011)
9. Jalil, K.A., Masrek, M.N.: Comparison of Machine Learning Algorithms Performance in Detection Network Intrusion. In: International Conference on Networking and Information Technology, pp. 221–226. IEEE, Los Alamitos (2010)
10. Lee, K., Kim, J., Kwon, K.H., Han, Y., Kim, S.: DDoS Attack Detection Method using Cluster Analysis. Expert Systems with Applications 34, 1659–1665 (2008)
11. Panda, M., Patra, M.R.: Evaluating Machine Learning Algorithms for Detecting Network Intrusions. International Journal of Recent Trends in Engineering 1(1), 472–477 (2009)
12. Kim, M., Na, H., Chae, K., Bang, H., Na, H.: A Combine Datamining Approach for DDoS Attack Detection. In: Kahng, H.-K., Goto, S. (eds.) ICOIN 2004. LNCS, vol. 3090, pp. 943–950. Springer, Heidelberg (2004)
13. Mitchell, T.: Machine Learning. McGraw Hill, New York (1997)
14. Nguyen, H.V., Choi, Y.: Proactive Detection of DDoS Attacks Utilizing K-NN Classifier in an Anti-DDos Framework. International Journal of Electrical and Electronics Engineering 4(4), 247–252 (2009)
15. Paruchuri, V., Durresi, A., Chellappan, S.: TTL based Packet Marking for IP Traceback. In: Proceedings of the IEEE Global Telecommunications Conference, November 30 - Decmber 4, pp. 2552–2556. IEEE, LA (2008)

16. Kabiri, P., Zargar, G.R.: Category-Based Selection of Effective Parameters for Intrusion Detection. IJCSNS International Journal of Computer Science and Network Security 9(9) (September 2009)
17. Seo, J., Lee, C., Shon, T., Cho, K.H., Moon, J.: A New DDoS Detection Model Using Multiple SVMs and TRA. In: Enokido, T., Yan, L., Xiao, B., Kim, D.Y., Dai, Y.-S., Yang, L.T. (eds.) EUC-WS 2005. LNCS, vol. 3823, pp. 976–985. Springer, Heidelberg (2005)
18. Xu, T., He, D., Luo, Y.: DDoS Attack Detection Based on RLT Features. In: Proceedings of the International Conference on Computational Intelligence and Security, China, December 15-19, pp. 697–701 (2007)
19. Xu, T., He, D.K., Zheng, Y.: Detecting DDoS Attack Based on One-Way Connection Density. In: Proceedings of IEEE International Conference on Communications, Singapore, pp. 1–5 (October 2006)
20. UCSD Network Telescope – Code-Red Worms Dataset. The Cooperative As-sociation for Internet Data Analysis (2001), http://www.caida.org/data/passive/codered_worms_dataset.xml: (accessed February 7, 2009)
21. Vapnik, V.: The Nature of Statitical Learning Theory. Springer, Heidelberg (1995)
22. Wang, W., Gombault, S.: Efficient detection of DDoS attacks with important attributes. In: Proceedings of the Third International Conference on Risks and Security of Internet and Systems, pp. 61–67 (October 2008)
23. Yuan, J., Mills, K.: Monitoring the Macroscopic Effect of DDoS Flooding Attacks. IEEE Transactions on Dependable and Secure Computing 2, 324–335 (2005)
24. Zargar, G.R., Kabiri, P.: Identification of effective network features for prob-ing attack detection. In: Proceedings of the First International Conference on Networked Digital Technologies, pp. 392–397 (July 2009)