# A Review of Classification Approaches Using Support Vector Machine in Intrusion Detection

Noreen Kausar[1], Brahim Belhaouari Samir[2], Azween Abdullah[1], Iftikhar Ahmad[3], and Mohammad Hussain[4]

[1] Department of Computer and Information Sciences, Universiti Teknologi PETRONAS, Bandar Seri Iskandar, 31750 Tronoh, Perak, Malaysia
[2] Department of Fundamental and Applied Sciences, Universiti Teknologi PETRONAS, Bandar Seri Iskandar, 31750 Tronoh, Perak, Malaysia
[3] Department of Software Engineering, College of Computer and Information Sciences, P.O. Box 51178, Riyadh 11543, King Saud University, Riyadh, KSA
[4] Department of Computer Science, King Saud University, Riyadh, KSA
noreenkausar88@yahoo.com, brahim_belhaouari@petronas.com.my, azweenabdullah@petronas.com, wattoohu@gmail.com, mhussain@ksu.edu.sa

**Abstract.** Presently, Network security is the most concerned subject matter because with the rapid use of internet technology and further dependence on network for keeping our data secure, it's becoming impossible to protect from vulnerable attacks. Intrusion detection systems (IDS) are the key solution for detecting these attacks so that the network remains reliable. There are different classification approaches used to implement IDS in order to increase their efficiency in terms of detection rate. Support vector machine (SVM) is used for classification in IDS due to its good generalization ability and non linear classification using different kernel functions and performs well as compared to other classifiers. Different Kernels of SVM are used for different problems to enhance performance rate. In this paper, we provide a review of the SVM and its kernel approaches in IDS for future research and implementation towards the development of optimal approach in intrusion detection system with maximum detection rate and minimized false alarms.

**Keywords:** Intrusion Detection System (IDS), SVM, Kernel, RBF, Knowledge Discovery and Data Mining (KDD), Defense Advanced Research Projects Agency (DARPA).

## 1 Introduction

With the continuous advancement in the computer technology and specially the internet, the exposure of malicious attacks and illegal accesses to computer systems is also increasing at a high rate [1-3]. In order to protect network security, intrusion detection systems are the key to detect intrusions so that the network remains stable and functioning. Performance of the intrusion detection system depends on the technologies and the techniques used [4]. Intrusion detection system has become the research focus for security implementers in order to enhance the detection rate and

A. Abd Manaf et al. (Eds.): ICIEIS 2011, Part III, CCIS 253, pp. 24–34, 2011.

reduce false alarms by applying different approaches of feature selection and classifiers. The subject matter also includes decreasing training time and increasing the accuracy rate of detecting normal and intrusive activities. To overcome these issues SVM is the better choice to be used as classifier in intrusion detection systems [5]. Different approaches applied on intrusion detection using SVM is the focus of this paper.

In this paper, Section 2 gives an overview of intrusion detection system. Section 3 describes support vector machines. Section 4 discusses the approaches applied to intrusion detection using SVM with detail of their proposed model, experimental dataset used, IDS structure and result obtained. Section 5 provides discussion on the SVM approaches applied in IDS and finally Section 6 concludes with ideas for future research in the field of IDS.

## 2 Intrusion Detection System

An unauthorized access to a network for certain purpose is known as intrusion and the user who accesses the network illegally is known as intruder. Anderson introduced the theory of intrusion detection in 1980 [6]. The purpose of the intrusion detection system is to detect such attacks and respond in a suitable way [7]. The model for intrusion detection was proposed by Dr. Dorothy Denning in 1987. Her proposed model is the basic core of the methodologies of intrusion detection in use today [5]. The intrusion detection is either anomaly detection or misuse detection. Anomaly detection is the identification of the normal activities and misuse detection is the detection of attacks on the basis of attack signatures through pattern matching approach. There are many flaws in an intrusion detection system like false positive and false negative. In such cases the IDS needs more training data to be trained and more time to gain better performance rate [8]. Classifiers are used to separate normal and intrusive data accurately and to attain maximum detection rate and minimum false alarms.

## 3 Support Vector Machines

Support vector machine (SVM) is a machine learning method proposed by Vapnik which is based on statistical learning theory [9]. SVM solve problems related to classification, learning and prediction [10]. As compared to other classifiers, SVM adopts the principle of structural risk minimization, it avoids local minimum and solves the issues like over learning and provides good generalization ability [11]. It performs the classification of the data vectors by a hyperplane or set of hyperplanes in a high dimensional space [12]. For classification there can be several hyperplanes for separation but the best hyerplane produces maximum margin between the data points of two classes. In many cases the data points are not linearly separable in the input space so they need nonlinear transformation into a high dimensional space and then the linear maximum margin classifier can be applied [13].Kernel functions are used for this purpose [14]. They are used at the training time of the classifiers to select the support vectors along the surface of the function. Then SVM classify the data by using these support vectors which outline the hyperplane in the feature space [15].

Selection of an appropriate kernel for a certain classification problem influence the performance of the SVM because different kernel function constructs different SVMs and affects the generalization ability and learning ability of SVM [16]. There is no theoretical method for selecting kernel function and its parameters. Presently Gaussian kernel is the kernel function which is mostly used because of its good features [17,18]. But there are many other kernel functions which are not yet applied in intrusion detection. For intrusion detection, SVM provide high classification accuracy even there is less prior knowledge available and the IDS will have better performance in terms of detection [19].

## 4 SVM Approaches to Intrusion Detection

There are different approaches applied for intrusion detection using SVM kernels for classification and regression. Several techniques in IDS are used for features transformation and selection along with SVM kernel functions for classification are implemented and then evaluated for determination of detection accuracy in terms of true positives and true negatives. Improving existing techniques for reducing errors in intrusion detection like false positives and false negatives are also in focus for researchers in order to contribute their applied technique towards the designing of robust IDS with maximum detection rate and minimized false alarms. A review of applying SVM approach for intrusion detection systems is as below:

### 4.1 SVM Approach-1

One of the SVM based approach for IDS was performed by Xiao et al. [10] in which they suggested a technique for intrusion detection based on Ad hoc technology and Support vector machine. IDS performance was improved in two ways: feature subset selection and optimization of SVM parameters. They provided ad hoc based feature subset selection and then 10-fold cross validation was used for optimizing SVM parameters. The extracted features were classified with the help of Gaussian Kernel of SVM. For this experiment, they used DARPA 1998 containing all the 41 features with four different attack classes such as DOS, R2L, U2R and probe. The experiment showed that it was not only better than other data mining techniques but also intelligent paradigms as well. A review of their results is given in Table 1.

**Table 1.** SVM Approach-1

| Author | Year | Data Source | Structure | Results |
|---|---|---|---|---|
| Xiao et al. | 2007 | DARPA 1998 randomly generated 11,982 records having 41 features. | Ad hoc based feature selection, SVM with Gaussian Kernel | Improving IDS performance (feature subset selection, optimization of SVM parameters). |

### 4.2 SVM Approach-2

Another approach of SVMs was applied by Yendrapalli et al. [20] in 2007. They used SVM, BSVM (Biased support vector machine), Looms (leave–one-out model selection) based on BSVM on the DARPA dataset containing four attacks and the normal data. The experiment concluded that SVM performs well for Normal and U2R, BSVM for DOS and Looms (BSVM) for Probe and R2L. SVM achieved above 95% detection accuracy for all five classes of DARPA dataset. They also demonstrated that the ability of SVMs to classify intrusions highly depends on both kernel type and the parameter settings. The results of their approach are shown in Table 2.

**Table 2.** SVM Approach-2

| Author | Year | Data Source | Structure | Results |
|---|---|---|---|---|
| Yendrapalli et al. | 2007 | DARPA | SVM with RBF kernel, BSVM, Looms based on BSVM | Classification accuracies: SVM for Normal: 98.42 SVM for U2R: 99.87 BSVM for DOS: 99.33 Looms for Probe: 99.65 Looms for R2L: 100.00 |

### 4.3 SVM Approach-3

Yuancheng et al. [21] proposed an IDS approach based on feature extraction using KICA (Kernel Independent Component Analysis) and then using KICA extracted features as input data to SVM for classification. The SVM kernel used in this approach is Radial basis function (RBF). They used KDDCUP99 for experiment with some rules like test data set and training data set from different probability distribution and test data set also included other attacks which do not exist in training data set. Due to the good generalization ability of SVM, the experimental results showed that it can also detect new attacks apart from existed attacks. The accuracy of this IDS was also increased remarkably by doing feature extraction. Even thought the detection rate decreased to some extent but the results were acceptable as false alarm rate also decreased considerably and these reduced false alarms had positive impact on the performance of the system. They also stated that different kernel functions for this method gives different performance results so still more work to be done to find optimal kernel for maximum accuracy. The results of their IDS are given in Table 3.

**Table 3.** SVM Approach-3

| Author | Year | Data Source | Structure | Results |
|---|---|---|---|---|
| Yuancheng et al. | 2008 | KDDCUP 99 | KCIA,SVM with RBF kernel | Accuracy : 98.9% Detection rate: 97.4%. False alarm: 1.1% |

### 4.4 SVM Approach-4

Another work was done by Yuan et al. [22] in which they proposed machine learning method for accurate internet traffic classification. Their method classified internet traffic according to the network flow parameters taken from the packet headers. They represented a method based on SVM technique for a set of traffic data collected on Gbps Ethernet link. The application signatures were used for identification for collected traffic data via precise signatures matching. They adopted cross validation to evaluate the experiment accuracies. This SVM based classification was more computationally efficient as compared to previous methods having similar accuracies. It also lends well for real time traffic identification as all the features parameters were computable without storing of multiple packets. This internet traffic classification technique is also applicable to encrypted network traffic as it does not rely on application payload. The identification of the traffic was too late as it was done after collecting the network flow, so it is necessary to be done in the early stage of the traffic flow. The results for the biased and unbiased training and testing samples are shown below in Table 4.

**Table 4.** SVM Approach-4

| Author | Year | Data Source | Structure | Results |
|---|---|---|---|---|
| Yuan et al. | 2008 | Traffic data collected from Gbps Ethernet link | SVM, RBF Kernel | Accuracy:<br>Biased: 99.42%<br>Unbiased: 97.17% |

### 4.5 SVM Approach-5

Another attempt in the field of intrusion detection with SVM was done by Zaman et al. [23] in which they proposed a new method for selecting features using Enhanced Support Vector Decision Function (ESVDF) SVM technique. The features were selected on two factors, the features rank which was calculated using Support Vector Decision Function (SVDF) and the second was the correlation between the features based on Forward Selection Ranking (FSR) or Backward Elimination Ranking (BER). They used KDD cup that consist of 4 types of attacks (DOS, R2L, U2R and Probing). The experiment was done in two steps. In first the features were selected and secondly the results were validated using SVM and Neural Network (NN) classifier. The experiment showed high accuracy for both SVM and NN with decreasing the training and testing time. This proposed model performed very well by selecting best features regardless of the classifier's type and with minimum overhead and maximum performance. A review of their results is given in the Table 5.

**Table 5.** SVM Approach-5

| Author | Year | Data Source | Structure | Results |
|---|---|---|---|---|
| Zaman et al. | 2009 | Subset of KDD cup 1999 | SVM with FSR and BER | Improvement in false positive rate, training time and testing time. |

### 4.6 SVM Approach-6

Gao et al. [11] presented a method based on classify SVM and used genetic algorithm (GA) to optimize SVM parameters in order to increase the detection rate. This new method detected intrusion behaviours quickly and efficiently with strong learning and generalization ability of SVM. They also used radial basis function neural network (RBFNN) to detect the anomaly intrusion behaviour to compare with the performance of SVM. They found that the classify SVM is stronger than RBFNN in generalization ability. SVM is less dependent of sample data and has smaller fluctuation range of generalize error than RBFNN. So this new approach is more stable and has high detection rate. Review of their work is mentioned below in Table 6.

**Table 6.** SVM Approach-6

| Author | Year | Data Source | Structure | Results |
|---|---|---|---|---|
| Gao et al. | 2009 | Training and testing data based on MIT 1999 | SVM, GA, RBFNN | SVM having higher stability and obtain higher recognition and detection accuracy. |

### 4.7 SVM Approach-7

In 2009, Rung-Ching et al. [24] used rough set theory (RST) and SVM for the detection of the intrusion in network. The purpose of using RST was to do pre-processing of the data by reducing dimensions. Then the selected features were sent to SVM for training and testing respectively. The dataset used for experiment was KDD cup 99 having 41 features and containing four different types of attacks. The features were reduced to 29 by using RST. The performance evaluation of the system was done on three formulas [25]; attack detection rate (ADR), false positive rate (FPR) and system accuracy. The performance of this approach was compared with 41 features and with entropy. This system had higher accuracy with reduced features as compared to full features and entropy but its attack detection rate and false positive were worse than entropy. The results of this IDS is given below in Table 7.

**Table 7.** SVM Approach-7

| Author | Year | Data Source | Structure | Results |
|---|---|---|---|---|
| Rung-Ching et al. | 2009 | KDD cup 99 | Rough set, SVM with RBF Kernel | ADR: 86.72%<br>FPR: 13.27%<br>Accuracy: 89.13% |

### 4.8 SVM Approach-8

Another work for intrusion detection was done by Yuan et al. [19]. They applied hypothesis test theory to SVM classifier (HTSVM) in order to get increased accuracy and decreased the impact of penalty factor. They selected RBF kernel of SVM in comparison with sigmoid and polynomial kernels. Experiment data was taken from KDD cup 99. In comparison with CSVM, the false positive rate (FPR) and false negative rate (FNR) of HTSVM were lower but the training and testing time was slightly increased. The results showed that HTSVM classifier had better generalization and learning ability and the performance of the IDS can be improved. The result of their work is given in Table 8.

**Table 8.** SVM Approach-8

| Author | Year | Data Source | Structure | Results |
|---|---|---|---|---|
| Yuan et al. | 2010 | Experiment data KDD 99 | SVM, HTSVM, CSVM, Gaussian Kernel | HTSVM:<br>Detection Precision (%) : 93.97<br>FPR (%) : 0.11<br>FNR (%) : 0.68<br>Training time : 26.53<br>Testing Time : 18.98 |

### 4.9 SVM Approach-9

Another contribution in the field of intrusion detection using SVM and Agent was done by Guan et al. [26] in 2010. The experimental data selected for this IDS model was KDD CUP 99 containing four attacks including Probe, DOS, R2L and U2R to test their proposed SVM model. They explained IDS in which Agent was used for the detection of abnormal intrusion and four SVM classifiers were used to recognize the intrusion types. The results proved to have better detection accuracy than artificial neural network. The review of this work is given below in Table 9.

**Table 9.** SVM Approach-9

| Author | Year | Data Source | Structure | Results |
|---|---|---|---|---|
| Guan et al. | 2010 | KDD CUP 99 | Agent, SVM | Detection precision:<br>SVM: 0.9457<br>BP neural network (BPNN): 0.8771 |

### 4.10 SVM Approach-10

Xiaomei et al. [27] combined adaptive genetic algorithm (AGA) and SVM for audit analysis by using KDD CUP 99 for experiment. SVM could work successfully as a classifier for security audit system but the problem was learning two parameters

penalty factor and kernel function which were key factors that could affect the performance of SVM. So, in this approach AGA optimized the penalty factor and also kernel function parameters of SVM. The results showed that this technique is more efficient and has higher accuracy than SVM. The best security audit should obtained higher accuracy rate in shorter training time but AGA-SVM had longer training time than that of SVM as it used heuristic method which took a lot of time for the exhaustive search. The systematic review of this approach is given below in Table 10.

**Table 10.** SVM Approach-10

| Author | Year | Data Source | Structure | Results |
|---|---|---|---|---|
| Xiaomei et al. | 2010 | KDD CUP 99 | AGA, SVM | For Pure data:<br>Average attack detection rate of AGA-SVM is 2.44% higher than SVM.<br>For Noise data:<br>Average attack detection rate of AGA-SVM is 8.04% higher than SVM. |

### 4.11 SVM Approach-11

Another attempt was done by Ahmad et al. [28] in IDS by applying SVM and back propagation neural network were used to be applied on distributed denial of service (DDOS). The experiment data used was cooperative association for internet data analysis (CAIDA) which is a standard for evaluating security detection mechanisms. The proposed model performed well in experiments and was better than other approaches used in IDS like K-NN, PCA and LOF in terms of detection rate and false alarms. A review of their work approach is given below in Table 11.

**Table 11.** SVM Approach-11

| Author | Year | Data Source | Structure | Results |
|---|---|---|---|---|
| Ahmad et al. | 2010 | CAIDA | SVM | SVM neural network<br>True Positive (%) : 100<br>True Negative (%) : 90.32<br>False Positive (%) : 0<br>False Negative (%) : 9.67 |

## 5 Discussion

The above review about the approaches applied for intrusion detection using support vector machines provides a lot of details regarding the techniques combined together with SVM to enhance the performance of the IDS and to focus different issues that

need to be solved or improved. The data for the training and testing is a very critical issue. They can be obtained from any of the three ways; real traffic, sanitized traffic or simulated traffic. The real traffic is very costly and sanitized is risky. Even creating simulated traffic is also a hard job [28].

In the beginning, DARPA was used as dataset for training and testing which has different attacks classes but then afterwards mostly approaches used KDD CUP and CIADA which are the standard datasets for evaluation of security mechanisms. The reason for choosing KDD CUP standard dataset is that it is easy to compare the result with other approaches to find optimal technique in IDS and also it is very hard to get any other dataset which contains rich types of attacks for training and testing purpose of IDS.

The performances of the approaches were observed on the basis of their detection rate, accuracy, false alarms, training time and testing time. In many cases mentioned above, some focused on the minimization of the false alarms which results either in decreasing the detection rate or increasing the training and testing time. Choosing different feature selection techniques apart from the classifier and its parameters selection also contributed in minimizing overhead and maximizing the performance. Good generalization ability and the less dependency on the dataset make SVM better in classification as compared to other classifiers. Also in case of CIADA dataset, experiment showed that SVM performed better than other approaches like K-NN, PCA and LOF in detection rate and false alarms [28].

The ability of the SVM classification depends mainly on the kernel type and the setting of the parameters. There are many kernel functions of SVM but the one which had mainly used in existing approaches is RBF. Other kernels should also be used in comparison to find optimal results for applying SVM based approach depending upon the nature of classification problem. The selection of different techniques for feature preprocessing and selection also affects directly to the result of the SVM classifier.

## 6 Conclusion and Future Suggestion

In this paper we presented a review of current researches of intrusion detection by using support vector machines as classifier. We discussed most recent approaches with a systematic review of their applied techniques, datasets used and results obtained from their proposed IDS model. Research in intrusion detection using SVM approach is still an ongoing area due to good performance and many hybrid techniques are also applied in order to maximize the performance rate and minimize the false alarms. Different kernel functions of SVM apart from RBF should also be applied for IDS classification purpose which may provide better accuracy and detection rate depending on different nonlinear separations. Different feature selection techniques can also be applied to dataset in combination with SVM classifier and its kernel functions so that the training time can be minimized instead of processing redundant data and to get enhanced accuracy rate from extracted features of dataset rather than processing large number of features which does not even affect the accuracy factor.

## References


1. Ahmad, I., Abdullah, A.B., Alghamdi, A.S.: Artificial neural network approaches to intrusion detection: a review. In: Proceedings of the 8th Wseas International Conference on Telecommunications and Informatics, Istanbul, Turkey (2009)
2. Kabiri, P., Ghorbani, A.A.: Research on intrusion detection and response: A survey. International Journal of Network Security 1(2), 84–102 (2005)
3. Mitrokotsa, A., Douligeris, C.: Detecting denial of service attacks using emergent self-organizing maps. In: Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology 2005, pp. 375–380 (2005)
4. Yuxin, W., Muqing, W.: Intrusion detection technology based on CEGA-SVM. In: Third International Conference on Security and Privacy in Communications Networks and the Workshops, SecureComm 2007, pp. 244–249 (2007)
5. Denning, D.E.: An Intrusion-Detection Model. IEEE Trans. Softw. Eng. 13(2), 222–232 (1987)
6. Anderson, J.P.: Computer security threat monitoring and surveillance. Technical Report. pp. 1–56. Ford Washington PA (1980)
7. Ahmad, I., Abdullah, A.B., Alghamdi, A.S.: Application of artificial neural network in detection of DOS attacks. In: Proceedings of the 2nd International Conference on Security of Information and Networks, Famagusta, North Cyprus (2009)
8. Zhu, G., Liao, J.: Research of Intrusion Detection Based on Support Vector Machine. In: International Conference on Advanced Computer Theory and Engineering, pp. 434–438 (2008)
9. Vladimir, V.N.: The Nature of Statistical Learning Theory. Springer, Heidelberg (1995)
10. Xiao, H., Peng, F., Wang, L., Li, H.: Ad hoc-based feature selection and support vector machine classifier for intrusion detection. In: IEEE International Conference on Grey Systems and Intelligent Services (GSIS 2007), pp. 1117–1121 (2007)
11. Gao, M., Tian, J., Xia, M.: Intrusion Detection Method Based on Classify Support Vector Machine. In: Proceedings of the 2009 Second International Conference on Intelligent Computation Technology and Automation, pp. 391–394 (2009)
12. Ahmad, I., Abdulah, A., Alghamdi, A.: Towards the Designing of a Robust Intrusion Detection System through an Optimized Advancement of Neural Networks. In: Kim, T.-h., Adeli, H. (eds.) AST/UCMA/ISA/ACN 2010. LNCS, vol. 6059, pp. 597–602. Springer, Heidelberg (2010)
13. Yang, M.-h., Wang, R.-c.: DDoS detection based on wavelet kernel support vector machine. The Journal of China Universities of Posts and Telecommunications 15(3), 59–63, 94 (2008)
14. Kumar, G., Kumar, K., Sachdeva, M.: The use of artificial intelligence based techniques for intrusion detection: a review. Artificial Intelligence Review 34(4), 369–387 (2010)
15. Mulay, S.A., Devale, P.R., Garje, G.V.: Intrusion Detection System Using Support Vector Machine and Decision Tree. International Journal of Computer Applications 3(3), 40–43 (2010)
16. Li, C.-C., Guo, A.-l., Li, D.: Combined Kernel SVM and Its Application on Network Security Risk Evaluation. In: International Symposium on Intelligent Information Technology Application Workshops (IITAW 2008), pp. 36–39 (2008)
17. Jiancheng, S.: Fast tuning of SVM kernel parameter using distance between two classes. In: 3rd International Conference on Intelligent System and Knowledge Engineering (ISKE 2008), pp. 108–113 (2008)

18. Broomhead, D.S., Lowe, D.: Multivariable Functional Interpolation and Adaptive Networks. Complex Systems 2, 321–355 (1988)
19. Yuan, J., Li, H., Ding, S., Cao, L.: Intrusion Detection Model Based on Improved Support Vector Machine. In: Proceedings of the 2010 Third International Symposium on Intelligent Information Technology and Security Informatics, pp. 465–469 (2010)
20. Yendrapalli, K., Mukkamala, S., Sung, A.H., Ribeiro, B.: Biased Support Vector Machines and Kernel Methods for Intrusion Detection. In: Proceedings of the World Congress on Engineering (WCE 2007), London, U.K (2007)
21. Yuancheng, L., Zhongqiang, W., Yinglong, M.: An intrusion detection method based on KICA and SVM. In: 7th World Congress on Intelligent Control and Automation (WCICA 2008), pp. 2141–2144 (2008)
22. Yuan, R., Li, Z., Guan, X., Xu, L.: An SVM-based machine learning method for accurate internet traffic classification. Information Systems Frontiers 12(2), 149–156 (2010)
23. Zaman, S., Karray, F.: Features Selection for Intrusion Detection Systems Based on Support Vector Machines. In: 6th IEEE Consumer Communications and Networking Conference (CCNC 2009), pp. 1–8 (2009)
24. Rung-Ching, C., Kai-Fan, C., Ying-Hao, C., Chia-Fen, H.: Using Rough Set and Support Vector Machine for Network Intrusion Detection System. In: First Asian Conference on Intelligent Information and Database Systems (ACIIDS 2009), pp. 465–470 (2009)
25. Chen, R.C., Chen, S.P.: Intrusion Detection Using a Hybrid Support Vector Machine Based on Entropy and TF-IDF. International Journal of Innovative Computing, Information and Control (IJICIC) 4(2), 413–424 (2008)
26. Guan, X., Guo, H., Chen, L.: Network intrusion detection method based on Agent and SVM. In: The 2nd IEEE International Conference on Information Management and Engineering (ICIME), pp. 399–402 (2010)
27. Xiaomei, Y., Peng, W.: Security audit system using Adaptive Genetic Algorithm and Support Vector Machine. In: 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), pp. 265–268 (2010)
28. Ahmad, I., Abdullah, A.B., Alghamdi, A.S., Hussain, M.: Distributed Denial of Service attack detection using Support Vector Machine. Journal of Formation-Tokyo, 127–134 (2010)