A Two-Tier System for Web Attack Detection Using Linear Discriminant Method

Zhiyuan Tan[1], Aruna Jamdagni[1,2], Xiangjian He[1], Priyadarsi Nanda[1], Ren Ping Liu[2], Wenjing Jia[1], and Wei-chang Yeh[3]

[1] Centre for Innovation in IT Services and Applications (iNEXT)
University of Technology, Sydney, Australia
{Zhiyuan.Tan,Aruna.Jamdagni}@student.uts.edu.au,
{xiangjian.he,Priyadarsi.Nanda,Wenjing.Jia-1}@uts.edu.au
[2] CSIRO, ICT Centre, Australia
ren.liu@csiro.au
[3] Department of Industrial Engineering and Engineering Management
National Tsing Hua University, Hsinchu, Taiwan 300, R.O.C
yeh@ieee.org

Abstract. Computational cost is one of the major concerns of the commercial Intrusion Detection Systems (IDSs). Although these systems are proven to be promising in detecting network attacks, they need to check all the signatures to identify a suspicious attack in the worst case. This is time consuming. This paper proposes an efficient two-tier IDS, which applies a statistical signature approach and a Linear Discriminant Method (LDM) for the detection of various Web-based attacks. The two-tier system converts high-dimensional feature space into a low-dimensional feature space. It is able to reduce the computational cost and integrates groups of signatures into an identical signature. The integration of signatures reduces the cost of attack identification. The final decision is made on the integrated low-dimensional feature space. Finally, the proposed two-tier system is evaluated using DARPA 1999 IDS dataset for web-based attack detection.

Keywords: Web-based attack, Intrusion detection, Packet payload, Feature selection, Linear discriminant method.

1 Introduction

Since an increasing number of transactions are relocated to network environment, the attacking targets of cyber-criminalities have been shifted from Telnet ports to web-based applications. Web servers and web-based applications are popular attack targets because tools used for creating web applications are easy to use, and many people writing and deploying them need only little background in security. Web servers and web-based applications are vulnerable to attack because of improper and poor security policy and methodology. According to the Common Vulnerabilities and Exposures (CVE) list [1], web-based attacks accounted for 20%–30% of the total number of attacks from 1999 to 2005, and there was at least one new attack found every hour

M. Soriano, S. Qing, and J. López (Eds.): ICICS 2010, LNCS 6476, pp. 459–471, 2010.

[2]. The rapid growth of cyber attacks and criminalities has raised the attentions of both industry and research sectors to network security. There are high demands of various security tools that can effectively protect a system from being compromised.

As one of the important solutions, Intrusion Detection System (IDS) [3] has been applied in many contemporary computer infrastructures. They are either developed using known attack signatures [4][5] or based on normal network traffic behaviors [6][7][8]. However, the former (misuse-based IDS) is easy to be evaded by novel attacks, and the latter (anomaly IDS) has relatively higher rates of false positives and computational costs.

Feature reduction techniques are essential to create an efficient IDS when taking into account the computational complexity and the classification performance. The approaches as shown in [9][10][11] were discussed and proposed to reduce the header features of packets. However, there are very few papers that have considered feature selection according to application-layer payload. The early feature reduction approach [12] on payload, developed by Krugel et al., grouped the byte frequency distributions of 256 ASCII characters into six bins, namely 0, 1-3, 4-6, 7-11, 12-15 and 16-255. Wang et al. [13] proposed an Anagram detector, in which Bloom Filter (BF) was used to reduce memory overhead. Nwanze and Summerville proposed a lightweight payload inspection approach [14], where bit-pattern hash functions were employed to map the bytes at the packet payload onto a set of counters which were the selected features used for intrusion detection. All of these approaches for payload feature reduction fail to consider one of the important payload characteristics, i.e., the correlations among the payload features (ASCII characters).

Thus, a novel Linear Discriminant Method (LDM) was proposed for feature selection in [15]. It attempts to select the discriminating features from the *difference distance map* between a normal Mahalanobis Distance Map (MDM) and the MDM of a particular type of attack by using Linear Discriminant Analysis (LDA). The MDMs are generated by the Geometrical Structure Model (GSM) [16], a key component of the Geometrical Structure Anomaly Detection (GSAD), for each single network packet to explore the correlations among features (ASCII characters) in the packet payload. All of the selected features are integrated into a new significant feature set as an integrated identical signature. The LDM-based feature selection approach [15] is proven efficient in reducing the computational complexity while retaining the high detection rates. However, in [15], we considered only three types of attacks, namely Apache2, Back, Phf, in the experiments. We excluded the CrashIIS attack due to the small packet payload size, which bias the overall detection performance and increases the false positive and the negative alarm rates.

To overcome this problem, we propose an efficient two-tier IDS in this paper. The two-tier system separates the small size payloads from the normal size payloads based on the length of payload. Tier one is a statistical based detector responsible for the detection of the small size payload attacks, and tier two is LDM-based detector applied to identify the other attacks. Finally selected low-dimensional significant features are used for intrusion detection under HTTP environment.

The rest of this paper is structured as follows. Section 2 gives a brief explanation of the LDM-based feature selection approach. Section 3 proposes a two-tier IDS. In Section 4, we discuss the experimental results and analysis. Section 5 draws conclusions and future work.

2 LDM Based Feature Selection

GSAD model [16] employs a 256-by-256 Mahalanobis distance map to analyze the hidden patterns of a network packet payload. This raises heavy computation costs in model training as well as in attack detection. This also makes the model far away from being applied for on-line intrusive behavior detection. As discussed in [15], LDM-based feature selection approach was proposed to address the computational issue of the newly proposed GSAD model. The model is a single tier payload-based IDS, which shows promising results in the detection of Web-based attacks. However, the LDM-based approach is not able to detect small payload attacks. The brief discussion of LDM-based feature selection approach is given in the following subsections.

2.1 Methodology

To extract significant features, difference distance maps need to be generated to measure the difference between normal traffic and particular types of attack traffic, such as the difference between each pair of {*Normal*, *Phf attack*}, {*Normal*, *Back attack*} and {*Normal*, *Apache2 attack*}. The difference for each element (*i, j*), where 0 ≤ *i, j* ≤ 255, is calculated using Equations (1) as discussed in [15].

$$diff_{(i,j)} = \frac{(\bar{d}_{(i,j)}^{normal} - \bar{d}_{(i,j)}^{attack})^2}{\sigma_{normal(i,j)}^2 + \sigma_{attack(i,j)}^2}. \tag{1}$$

Here, $\bar{d}_{(i,j)}^{normal}$ and $\sigma_{normal(i,j)}^2$ denote the mean and the variance of the (*i, j*) elements of the normal sample MDMs, and $\bar{d}_{(i,j)}^{attack}$ and $\sigma_{attack(i,j)}^2$ denote the mean and the variance of the (*i, j*) elements of the attack sample MDMs. The difference distance map between the normal samples and the attack samples is defined by $Diff = \left[\, diff_{(i,j)}\right]_{256\times256}$.

Then, LDM is employed to select the most signification features for each normal and attack pair based on the pre-generated difference distance maps. For the selection of the most significant features, we randomly choose normal training samples and various attack training samples from the labeled samples set. A generated difference distance map is used for the significant feature selection. We first select the most significant *r* features from the difference distance map. Then, the optimal value of projection vector A_r is computed as discussed in [15]. Once the projection vector is finalized, the corresponding final set of features is considered as the most significant features.

3 Two-Tier Intrusion Detection System

In this section, a two-tier intrusion detection system is proposed to detect various payload size attacks. The detailed discussion of the system is given in the following subsections.

3.1 System Framework

The framework of this two-tier intrusion detection system is given in Fig. 1. The system consists of four key components, namely *Filter*, *Statistical Signature Based Detector*, *LDM Based Detector* and *Alert Generator*. The solid arrow indicates the incoming network traffic, and the dotted arrow stands for the analysis decisions made by the detectors.

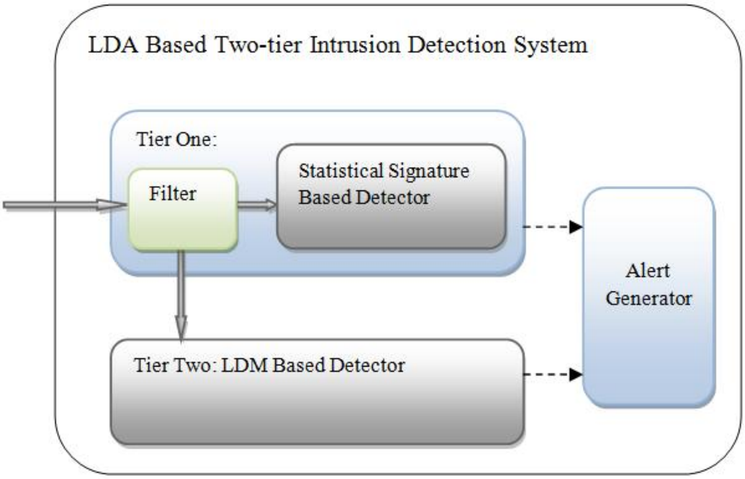

LDA Based Two-tier Intrusion Detection System
Tier One:
Filter
Statistical Signature Based Detector
Alert Generator
Tier Two: LDM Based Detector

Fig. 1. Framework of LDM based two-tier intrusion detection system

Under the HTTP environment, we make use of the length of packet payload as the filtering criterion because the normal HTTP packet has a very low probability to carry a very short payload. Therefore, the *Filter* component preprocesses the non-zero incoming HTTP Get request packet. Then, preprocessed request packets are grouped together based on the length criterion. If the length of any payload is less than the criterion, the packet will be forwarded to the *Statistical Signature Based Detector* on the first tier. Otherwise, the packet will be passed to the second tier detector, i.e. the *LDM Based Detector.*

The detectors analyze the received packet and make the final decision. Then, the *Alert Generator* will decide to raise an alarm or not based on the detection result given by the detectors.

3.2 Tier-One: Statistical Signature Based Detector

As the first tier detector, *Statistical Signature Based Detector* only processes the small packet payloads. In this case, the observed HTTP Get request packets are highly suspicious, and the anomaly patterns carried by the attacks are easy to be learnt from the character relative frequencies. This is because these attacks have very high frequencies on some particular ASCII characters in the payloads, which is unusual and is not going to happen in the normal cases. Thus, we can develop the statistical signatures for these types of attacks.

To develop the attack signatures, the techniques in [16] are used to parse and to extract the character relative frequencies from the labeled training attack packet payloads. The patterns of the character relative frequencies are stored as the signatures and are applied to identify the corresponding attacks in the future.

In the attack recognition phase, any new incoming packet is processed using the same techniques mentioned above to generate character relative frequency profile. The profile is compared with each known statistical signature, and the attack is identified as long as the profile is matched with one of the known statistical signatures.

3.3 Tier-Two: LDM Based Detector

If the length of HTTP Get request packet payload is larger than the pre-set criterion, the packet will be forwarded to the *LDM Based Detector*. The proposed LDM-based feature selection approach is used to extract a low-dimensional feature space for profile development and attack detection. The processes of normal profile development and attack recognition are discussed in detail in the following subsections.

Normal Profile Development. To measure the similarity between any new incoming packet and normal packets, the characteristics of the normal packets need to be extracted to develop a normal profile, which has been discussed in [15]. In this section, we briefly explain the generation of the normal profile.

Mean values of the significant *r* features of all normal training samples and a detection threshold are the basic components of the normal profile. The Mean values $\overline{F}$ of the significant *r* features of all normal training samples is calculated by Equation (2), where $F_k = [f_{k(U1\,,V1)}, f_{k(U2\,,V2)}, \ldots, f_{k(Ur\,,Vr)}]^T$ is the significant feature set for the k^{th} sample. (U_1, V_1), (U_2, V_2), …, (U_r, V_r) indicate the locations of the significant *r* features.

$$\overline{F} = \frac{1}{m}\sum_{k=1}^{m} F_k \tag{2}$$

To achieve a satisfactory detection performance, a threshold is selected through a distribution analysis of the Euclidean distance between each normal training sample and the mean value of the significant features. The Euclidean distance from the k^{th} normal training sample to the mean value $\overline{F}$ is obtained by Equation (3).

$$ED_k = \sqrt{\sum_{i=1}^{r}\left(f_{k(U_i,V_i)} - \overline{f_{(U_\iota,V_\iota)}}\right)^2} \tag{3}$$

$\overline{f_{(U_\iota,V_\iota)}}$ is the (U_i, V_i) element of $\overline{F}$. The standard deviation of the Euclidean distances from the k^{th} normal training sample to the mean value $\overline{F}$ of the normal training samples is

$$\delta = \sqrt{\frac{1}{m-1}\sum_{k=1}^{m}(ED_k - \overline{ED})^2}, \tag{4}$$

where $\overline{ED} = \frac{1}{m}\sum_{k=1}^{m} ED_k$ .We assume that the distance ED_k is of normal distribution, so three standard deviations account for 99% of the sample population.

Attack Recognition. In the attack recognition process, the values of the most significant r features are generated and used to form a feature vector F. An incoming packet is considered as an attack or a threat if and only if the Euclidean distance from F to $\overline{F}$ is greater than $+3\delta$ or smaller than -3δ, where δ is the standard deviation computed by Equation (4).

Computational Complexity. This approach not only reduces the feature space from 256^2 to a small size but also decreases the heavy computational complexity. The computational complexity of the GSAD model is $O(n^2)$, while the computational complexity of the LDM-based IDS is $O(m)$, where n and m represent the number of features used in the detection process. Here, n^2 is much greater than m.

4 Experimental Results and Analysis

To evaluate the effectiveness of the proposed two-tier system, a series of experimentation are conducted on the DARPA 1999 IDS dataset [17] and compared with the outcomes of LDM-based IDS. In the following subsections, we present the experimental results and the analysis.

4.1 Experimental Results

DARPA 1999 IDS dataset is a five-week network traffic tcpdump record which consists of two weeks' attack-free data (Week 1 and week 3) and three weeks' attack-containing data.

Due to the importance of web servers and web-based applications to modern business and human daily life, and their popularities to the cyber-criminals, we focus on the detection performance of the proposed IDS on HTTP traffic in the experimentation. Moreover, because the HTTP-based attacks are mostly carried by the HTTP Get request at the server side, only the inbound HTTP Get requests are considered in this practice.

In the experiments, we use the same conditions discussed in [16] to filter the interested HTTP Get request traffic from the week 4 (5 days) and the week 5 (5 days) data of the DARPA 1999 dataset, and the extracted packets are grouped into normal and attack sample sets respectively. We randomly choose a certain number of extracted normal packets and attack packets from the sample sets for the training of the model, and the rest of sets are used for testing. The attack packets contain CrashIIS attack, Apache2 attack, Back attack and Phf attack. The LDM-based IDS and the proposed two-tier system are trained and tested with the selected inbound HTTP Get request traffic carrying non-zero payload as discussed in [15] and Section 3 respectively.

The experiments we conduct in this research for the LDM-based IDS using all four types of attacks to obtain the significant feature set. The proposed two-tier system, however, uses Apache2 attack, Back attack and Phf attack only, and we exclude the CrashIIS attack. This is because CrashIIS attack is the only attack carrying a small packet payload with respect to the length criterion using in our experiments. Thus, in the proposed two-tier system, the pattern of the character relative frequencies of CrashIIS is used as the statistical signature for the tier-one detector. Fig. 2 shows the character relative frequencies of CrashIIS attack.

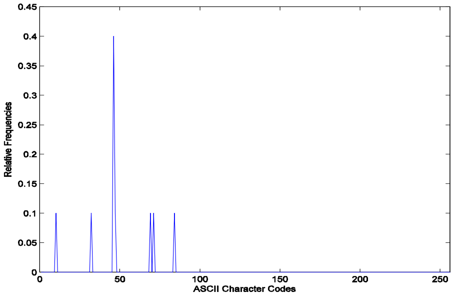


Fig. 2. Character relative frequencies of CrashIIS attack

To obtain the optimal feature sets for Phf attack and Apache2 attack, we use Fig. 3 and Figs. 4(a) and 5(a) to generate the difference distance maps as shown in Figs. 4(b) and 5(b). The same method is applied to the other types of attacks.

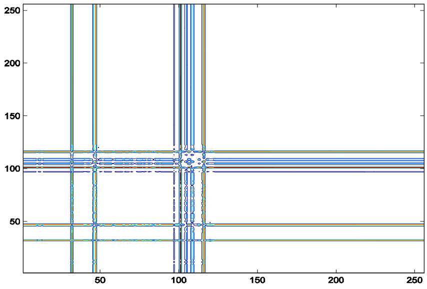
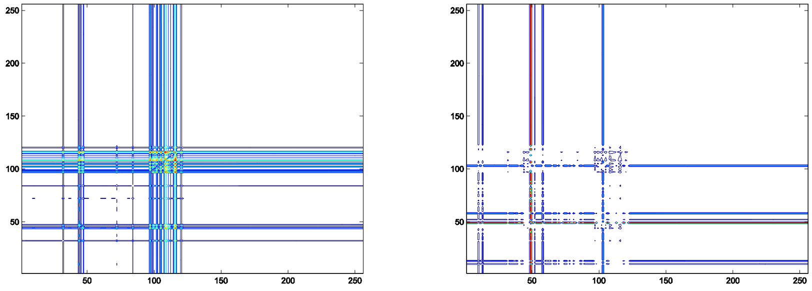


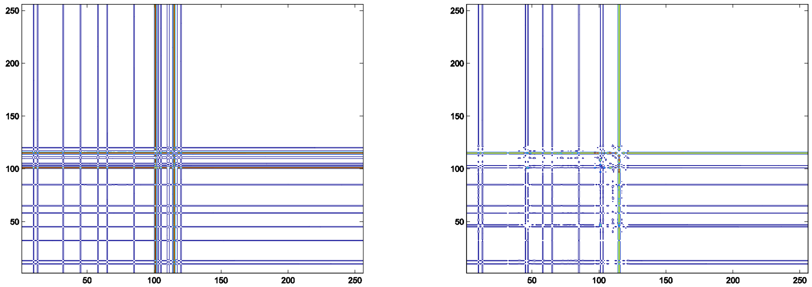
Fig. 3. Average Mahalanobis distance map of normal HTTP Get request packets



(a) Average Mahalanobis distance map

(b) Difference distance map

Fig. 4. Average Mahalanobis distance map of Phf attack packets, and difference distance map between normal HTTP and Phf attack packets



(a) Average Mahalanobis distance map

(b) Difference distance map

Fig. 5. Average Mahalanobis distance map of Apache2 attack packets, and difference distance map between normal HTTP and Apache2 attack packets

Experiments are conducted to extract the optimal number of significant features to best separate normal packets from attack packets. The optimal result is found to be 100 features selected by LDM for each of four types of attacks. Then, the normal profiles of the LDM-based IDS and the proposed two-tier system are developed based on the integrated 381 and 300 significant features respectively.

In the test stage, the trained LDM-based IDS and the trained proposed two-tier system are evaluated on the testing sample sets containing both the normal packets and the attack packets. All the test samples are used for the testing of LDM-based IDS. However, in the proposed two-tier system, the test samples are assigned to the detectors on different tiers according to the length criterion as discussed in Section 3. In tier-one, the detector uses the character relative frequencies of any assigned new incoming packet payload to compare with the pre-generated signatures in order to identify the suspicious intrusive activity. In tier-two, the detector evaluates the similarity between any new incoming packet and the normal profile using Euclidean distance as given by Equation (3), and the decision is made by comparing the distance with the pre-set threshold (i.e. ±3δ).

The experimental results of the LDM-based IDS and the proposed two-tier system are shown in Table 1 and 2 respectively.

Table 1. Performance of LDM-based IDS using features extracted from four types of attacks

Test samples	300 training samples		700 training samples		4000 training samples	
	Classify correctly	Mis-classify	Classify correctly	Mis-classify	Classify correctly	Mis-classify
Normal	96.83%	3.17%	97.1%	2.9%	99.07%	0.93%
Apache2 attack	100%	0%	86.94%	13.06%	0%	100%
Back attack	100%	0%	100%	0%	100%	0%
Phf attack	100%	0%	100%	0%	100%	0%
CrashIIS attack	**6.67%**	**93.33%**	**5.64%**	**94.36%**	**4.1%**	**95.9%**

Table 1 presents the performance of LDM-based IDS using features extracted from four types of attacks. The table gives a comparison between the results obtained for the normal profiles developed using different numbers of training samples, i.e. 300, 700 and 4000 samples. As can be seen from the table, the percentage of correct classification of normal samples is improved as the number of training samples increases. Back attack and Phf attack remain constant in all cases and have 100% correct classification rates. In contrast, the trend of correct classification of Apache2 attack and CrashIIS attack is reverse. In the case of 4000 training samples, the classification of Apache2 attack drops down to 0%.

The results in Table 1 show the LDM-based IDS is unable to classify CrashIIS attack correctly, and has misclassification rates higher than 93% consistently.

Table 2. Performance of two-tier system using features extracted from three types of attacks

Test samples		300 training samples		700 training samples		4000 training samples	
		Classify correctly	Mis-classify	Classify correctly	Mis-classify	Classify correctly	Mis-classify
Tier-two (LDM-based detector)	Normal	96.62%	3.38%	96.81%	3.19%	98.5%	1.5%
	Apache2 Attack	100%	0%	100%	0%	86.94%	13.06%
	Back Attack	100%	0%	100%	0%	100%	0%
	Phf Attack	100%	0%	100%	0%	100%	0%
Tier-one (Statistical signatured etector)	CrashIIS Attack	100%	0%	100%	0%	100%	0%

In Table 2, the performance of two-tier system using features extracted from three types of attacks is given. It compares the results obtained for the normal profiles developed using the same numbers of training samples as Table 1. The difference is that the normal profiles for tier-two detector are built up on three types of attacks (Apache2 attack, Back attack and Phf attack) instead of all the four types.

As can be seen from Table 2, the proposed two-tier system achieves encouraging performances in all the cases except the detection of Apache2 attack using the normal profile developed by 4000 training samples. In this case, the two-tier system can only correctly identify 86.94% of the total number of attack samples. However, compared with the LDM-based IDS, the proposed two-tier system is proven more promising. It outperforms the LDM-based IDS in detecting CrashIIS attack. Benefiting from two-tier architecture, we are able to classify all the CrashIIS attack samples. The detailed analysis is given in the next subsection.

4.2 Result Analysis

The results in Table 1 and 2 reveal that the 300 training samples can provide sufficient knowledge for both the LDM-based IDS and the proposed two-tier system to achieve good overall detection performance. In this section, the information contained in these two tables is further analyzed using Detection Rate (DR) and False Positive Rate (FPR) [15].

Table 3 shows the comparison of the number of features, the detection rates and the false positive rates for LDM-based IDS, two-tier system and GSAD model [16].

Table 3. Comparison of IDSs

Systems	Number of features	Detection rate (%)	False positive rate (%)
Two-tier system	300	100	3.38
LDM-based IDS	381	99.8	3.17
GSAD model	65536	100	0.087

The results show that the proposed two-tier system outperforms the LDM-based IDS. It has 100% detection rate and can successfully classify CrashIIS attack, and it uses less number of features in comparison to LDM-based IDS for the attack classification.

Compared with the GSAD model, the two-tier system achieves 100% detection rate. Although it has a higher false positive rate, the system successfully transforms the original 65536 dimensional feature space in GSAD model to a relatively very low dimensional feature space. It integrates various attack signatures while preserving the most significant information for the final detection. It not only significantly reduces the computational complexity of the detection process (attack signature comparison operation) but also reduces computational time.

In the following, we give two Receiver Operating Characteristic (ROC) curves for the LDM-based IDS and the proposed two-tier system in Figs 6 and 7, which show the relationships between detection rates and false positive rates to the corresponding systems. As shown in Fig. 6, the detection rate of LDM-based IDS increases significantly from 13.7% to 99.82% when the false positive rate is set to be around 3.38%. Then, the detection rate keeps going up slowly to 99.8%. Contrastively, the ROC curve of the two-tier system in Fig. 7 is more stable, and it always stays at 100%.

Despite the ROC curve of LDM-based IDS finally reach to nearly 100% detection rate, the detection performance of the LDM-based IDS in fact is significantly influenced by the number of small payload (i.e. CrashIIS attack) appearing in our test sample set. The test sample set used in this paper is heavily dominated by the Apache2 attack (97576 test samples), and the small payload attack (i.e. CrashIIS attack) only contributes a very small portion (195 test samples) to the test sample set. Therefore, even around 93.33% of the CrashIIS attack packets are classified incorrectly by the LDM-based IDS shown in Table 1, its overall detection rate did not drop dramatically. Hence, the ratio of the attacks in a test sample set bias the detection performance of LDM-based IDS. However, our two-tier system does not have this issue. The proposed two-tier IDS shows a more promising future in network intrusion detection.

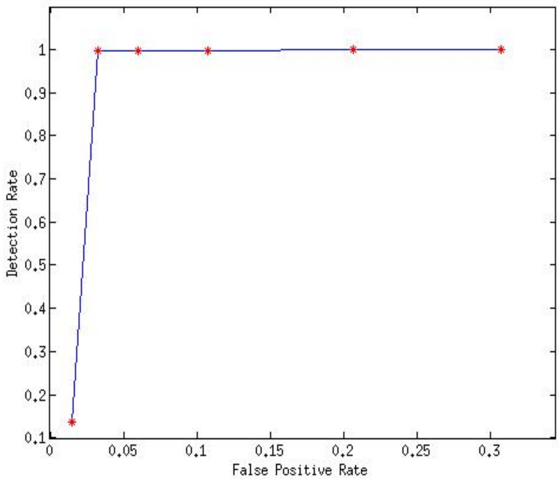


Fig. 6. ROC Curve of LDM-based IDS

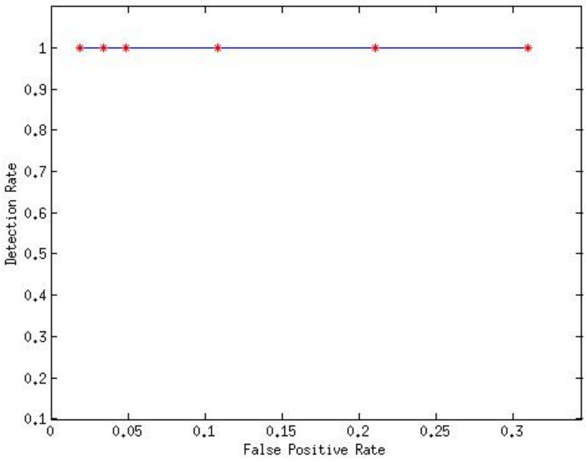


Fig. 7. ROC Curve of Two-tier IDS

5 Conclusions and Future Work

This paper proposed a two-tier system for network intrusion detection. The system process the incoming packets based on the payload length of the packet. The tier-one uses the statistical signature approach for the classification of small payload attack packets, and the tier-two uses LDM-based approach for the classification of the other attack packets.

The proposed two-tier system has been evaluated using DARPA 1999 IDS dataset for the HTTP traffic. It has achieved encouraging results with 100% detection rate and 3.38% false positive rate, and it can classify the CrashIIS attack successfully, which is not able to be identified by the LDM-based IDS. Compared to GSAD model, it transforms a high dimensional feature space to a very low dimensional feature space, which efficiently reduce the computational complexity and the detection time.

However, the amount of selected significant features may grow to a large number when more types of attacks are considered. This is because more sets of significant features will be selected with respect to the increasing number of types of attacks, but the optimal feature set can be used to generate the single signature for a group of attacks. This will reduce the signature comparison for those selected attacks. To reduce the false positive rates, we are conducting experiments using different experimental settings, and the work is in progress. Also, we will extend this research work to integrate the attack signatures for other types of attacks.

References

1. Corporation, M.: Common vulnerabilities and exposures, `http://cve.mitre.org/` (accessed June 16, 2006)
2. Kay, J.: Low Volume Viruses: New Tools for Criminals. Network Security, 16–18 (2005)
3. Denning, D.E.: An Intrusion-detection Model. IEEE Transactions on Software Engineering, 222–232 (2006)
4. TippingPoint, `http://www.tippingpoint.com/`
5. Paxson, V.: Bro: A System for Detecting Network Intruders in Real-time. Computer Networks 31, 2435–2463 (1999)
6. Patcha, A., Park, J.M.: An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends. Computer Networks 51, 3448–3470 (2007)
7. Wang, K., Stolfo, S.J.: Anomalous Payload-based Network Intrusion Detection. In: Jonsson, E., Valdes, A., Almgren, M. (eds.) RAID 2004. LNCS, vol. 3224, pp. 203–222. Springer, Heidelberg (2004)
8. Mahoney, M.V.: Network Traffic Anomaly Detection Based on Packet Bytes. In: The 2003 ACM Symposium on Applied Computing, pp. 346–350. ACM, New York (2003)
9. Shih, H.C., Ho, J.H., Chang, C.P., Pan, J.S., Liao, B.Y., Kuo, T.H.: Detection of Network Attack and Intrusion Using PCA-ICA. In: 3rd International Conference on Innovative Computing Information and Control, p. 564(2008)
10. Singh, S., Silakari, S.: Generalized Discriminant Analysis Algorithm for Feature Reduction in Cyber Attack Detection System. International Journal of Computer Science and Information Security 6, 173–180 (2009)
11. Chen, Y., Li, Y., Cheng, X.Q., Guo, L.: Survey and Taxonomy of Feature Selection Algorithms in Intrusion Detection System. In: Lipmaa, H., Yung, M., Lin, D. (eds.) Inscrypt 2006. LNCS, vol. 4318, pp. 153–167. Springer, Heidelberg (2006)
12. Krugel, C., Toth, T., Kirda, E.: Service Specific Anomaly detection for Network Intrusion Detection. In: The 2002 ACM Symposium on Applied Computing, pp. 201–208. ACM, New York (2002)
13. Wang, K., Parekh, J., Stolfo, S.: Anagram: A Content Anomaly Detector Resistant to Mimicry Attack. In: Zamboni, D., Krügel, C. (eds.) RAID 2006. LNCS, vol. 4219, pp. 226–248. Springer, Heidelberg (2006)

14. Nwanze, N., Summerville, D.: Detection of Anomalous Network Packets Using Lightweight Stateless Payload Inspection. In: The 33rd IEEE Conference on Local Computer Networks, pp. 911–918 (2008)
15. Tan, Z., Jamdagni, A., Nanda, P., He, X.: Network Intrusion Detection Based on LDA for Payload Feature Selection. In: IEEE Globecom 2010 Workshop on Web and Pervasive Security, pp. 1–5. IEEE Press, Los Alamitos (2010) (to appear)
16. Jamdagni, A., Tan, Z., Nanda, P., He, X., Liu, R.: Intrusion Detection Using GSAD Model for HTTP Traffic on Web Services. In: The 6th International Wireless Communications and Mobile Computing Conference, pp. 1193–1197. ACM, New York (2010)
17. 1999 DARPA Intrusion Detection Evaluation Data Set, http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/1999data.html