Detection of Coercive Parsing Attack in XML Requests using Machine Learning Techniques

V. Punitha* and C. Mala
National Institute of Technology, Tiruchirappalli, India
vpunitha21@gmail.com, mala@nitt.edu

Abstract

The enriched cloud technology enables wider usage of web services in commercial applications. The increased bandwidth facilitates the continuous availability of web services. Legitimate access to these services is intentionally blocked by denial of service attacks. The impact of distributed denial of service attacks varies from interrupting the convenience of using the services to primary failure at cloud servers. Besides, the attacks are targeted towards application layer protocols recently. In order to eradicate this type of victim, this paper proposes two classification models based on machine learning techniques. The XML requests are pruned and the features that discriminate the coercive parsing attack are computed. The proposed SVM based classifier and the classification model with unsupervised learning categorize the attacks using constructed features. The simulated results emphasize that the detection rate of the proposed SVM based classifier, is significantly higher than the proposed unsupervised classifier.

Keywords: Distributed Denial of Service attack, Application layer attack, Coercive parsing attack, Machine learning techniques

1 Introduction

The growth of CRM (Customer Relationship Management) software and its applications are exponentially increasing with the cutting-edge technologies. Managing information in a distributed application or between diverse applications is a challenging task, as the applications are implemented in diverse platforms. It further needs application integration and inter-enterprise cooperation. This situation insisted on a common messaging technique for interaction between applications and B2B exchanges. In recent years, XML is widely used for this purpose, as it is interoperable, it works between diverse computing systems [7]. This induces the deployment of XML messaging like SOAP, UDDI, and WSDL, more than before. At the same time, the convenience of applying the technology is very much improved with advanced internetworking. This superiority affects the behaviour of the users and the attackers. Subsequently this misbehavior, creates many threats and malicious traffic in Internet. Among the threats created for many protocols, recently the attackers are targeting application layer protocol [12]. Though many approaches are applied to prevent these threats, perfect classification of user's requests is believed to be an important step to bring out the behaviour of the users and attackers and it further assists to identify various threats and attacks [10].

The machine learning techniques are superior in automatic learning and classification. Many research works are executed in identification and classification of network traffic using machine learning techniques [9]. In most of the research works, external characteristics of the request, like, source IP, arrival time, packet length, etc., are applied for classification, as the usage of payload is restricted due

IT CoNvergence PRActice (INPRA), volume: 6, number: 3 (September 2018), pp. 9-17
*Corresponding author: Research Scholar, Department of Computer Science and Engineering, National Institute of Technology, Tiruchirappalli, India

to privacy [6]. As the implementation machine learning techniques, in identification of applications of network traffic have produced good outcome [9], enforcing these techniques in detection of attacks is expected to give good results. Hence this paper proposes classification techniques to discriminate application layer attack using machine learning techniques.

2 Related Work

Significant existing works in identification of attacks, anomalies and applications in internet traffic are presented in this section.

Authors in [1], examined both flash crowd and DDoS attack traffic in HTTP/2 services. Four different investigations are conducted to analyze the depletion of the resources and HTTP services. Authors proved that beyond protocols, other properties, size and pattern of communication are needed to discriminate the attacks in HTTP/2 services. A two-stage detection technique for mitigating HTTP GET flood attack is presented in [8]. Here, the Confidence Based Filtering (CBF) technique inspects the ability of connected resources and requests. The attacks are discriminated with the calculated confidence value, called CBF score considering the number of requests and server processing speed. Signature and anomaly based attack detection methods are proposed in [5]. Signature based detection method identifies statistical changes in the traffic, like, incoming and outgoing packet rate, number of connections established, etc. It identifies attacks only for defined malicious activities, whereas, anomaly based technique classifies different attacks. It extracts parameters like, IP packet length, packet rate. Here attacks are detected by measuring the distance between normal traffic and testing traffic. But it requires more parameters for accurate classification. Malicious connections are identified using ConnectionScore in [2], based on the behaviour of the established connection. This technique creates a reference profile for normal traffic, describing its characteristics. Every time new score is calculated with the reference profile and the connection which has lower score is declared as malicious connection. This technique eliminates application-layer DDoS attacks effectively. Authors in [7] proposed a security service to detect HTTP and XML attacks using filtering tree. Five filters are applied including double signature and puzzle solver to eliminate the attacks towards cloud servers. In [11], authors presented comprehensive study on zero-day attacks. Using context-behavior of IoT devices, a new consensus framework is proposed which detects the attacks. The proposed approach also ensures reliable communication during the vulnerability of attack with the proposed alert message protocol which distributes the alert notifications and facilitates to form a secure group. The proposed data sharing protocol ensures the data distribution during unfavorable situations. Authors evaluated the approach with the numerical analysis. In [3], authors proposed an intelligent communication ant colony optimization model. A new feature selection methodology is proposed using ant colony technique for unstable varying ultrasound imaging systems. SVM model is developed using the selected features to classify different types of lymph nodes. Authors also proved that the classification performance of the proposed optimization model is better than existing approaches.

The above survey emphasizes that automatic categorization of client request in the view of discrimination of application layer attacks needs further investigation. So this paper proposes two models based on supervised and unsupervised classification techniques, SVM Classifier based on Request structure (SCR) and Unsupervised Classification based on Request structure (UCR) which examine the XML requests and categorize the XML based attack from generic request.

The rest of the paper is organized as follows. Section 3 describes XML based attack and the proposed Classification models. The simulated results are investigated in Section 4 and finally the work is summarized in Section 5.

3 Proposed System

There are two major categories in machine learning algorithms, supervised learning and unsupervised learning. Supervised learning acquires knowledge from the training data to map the input to the respective output label. But unsupervised learning acquires knowledge by discovering the hidden pattern in the unlabeled training data [9]. The SVM, popularly used supervised learning technique defines a hyper plane which classifies the input samples into two categories. It has kernel functions for complex mapping and regularization parameters to produce more generalized model [13]. K-means algorithm, the simplest unsupervised learning algorithm, partitions the data into 'k' groups according to the similarities in data [14]. This paper proposes two models, SCR and UCR using the above described machine learning techniques to detect application layer attacks.

Application layer attacks are more difficult to discriminate than flood attacks, as the flood attacks can be detected with frequency of arrivals, an externally observable parameter; whereas the application layer attacks cannot be predicted with arrival rate. These attacks are pushed, only after the communication is initiated. So communication in application layer is analysed further. Communications between applications can be either through RPC (Remote Procedure Call) or using messages (XML messaging). As HTTP and XML based protocols are mostly applied in recent web architectures, they are more targeted by the attackers. This paper analyses XML messages to discriminate coercive parsing attack, the most vulnerable attack in application layer; in general it is referred as XML based attack. This paper proposes two models to mitigate this attack and the work flow is depicted in Figure 1. As the XML messages cannot be applied directly to machine learning algorithms, they are pruned and pre-processed to get feature vectors. Then, the proposed models are developed with the constructed feature vector; finally the performance of the models are evaluated in different situations.

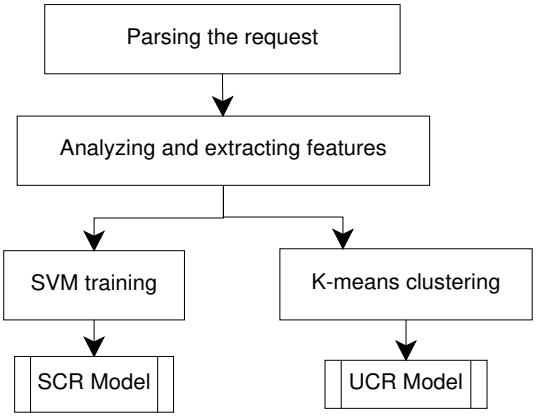

Figure 1: Workflow of the Proposed System

3.1 SVM Classifier based on Request structure (SCR)

Formerly, the superiority of SVM is proved in medical diagnosis and network traffic classification [3],[9]. Hence, SVM is applied in this paper for the detection of application layer attacks.

When a client wants to invoke a procedure, and when he doesn't know about the signature of the procedure, then the client creates a message with the format known to both client and the server (XML message). This message is sent to the server as a request. This request has two parts, header field and body part. The header is processed to verify the presence of requested application and the message encoding scheme. The body includes many tags according to the applications. The proposed models receives messages/requests sent by the client and it is parsed to compute the information about the header

fields and other tags of the requests. The header fields are verified and the requests with unspecific applications or insufficient information about application are eliminated. The XML based attacks are created with malformed messages to exhaust the server time. Normally, the request does not include many namespace declarations, as it is generated for specific application. But attacker generate messages with many namespace declarations which are not needed for the specified application. Moreover, these namespace declarations are verified and errors are notified only during the application processing, this exhausts the server time. So, this paper analyzes the namespace declarations against every applications and if it is found significantly large, then the request is discriminated as attack. Alternatively, attackers create malformed messages with deeper nested structure so that processing of nested XML tags takes more server time. To identify this threat, in this paper, the tags are organised into a tree structure and the height of the tree is computed. When the height is unusually long, it implies that the request has more nested tags which is abnormal in messaging. So the request is declared as an attack. Oversized XML is another attack which deny the service to the legitimate user by exhausting the server time in processing oversized messages. The oversize is due to large names and more attributes, which are uncommon while messaging. Therefore the feature vector is constructed with number of namespace, height of the tag tree and size of the request along with basic features.

SCR model is developed using the feature vectors constructed for all client requests. Before that, the features are transformed into the range [-1,1] for uniformity and the values of kernel parameters are selected using cross validation and grid search [13], as these values influence the performance of the SVM model. The model is tested with the obtained testing requests.

3.2 Unsupervised Classification based on Request structure (UCR)

Labelling of network traffic, while discriminating threats, is not feasible in real time traffic due to its varying characteristics. So this paper proposes a model to discriminate coercive parsing attack using unsupervised classification technique. As depicted in Figure 1, parsing the XML request and the construction of feature vectors are same as in SCR. So, with the constructed feature vectors of training requests the UCR model is developed. K-means clustering technique is applied and the requests are classified into 'k' cluster. The algorithm has two steps, assignment and updating step [14]. During assignment step, distance between the client request and cluster center is calculated and it is repeated for all clusters. Then the request is assigned to the cluster which has closest distance. After each request assignment, the center of the cluster is again redefined in updating step. These steps are iteratively processed to assign all the requests into the clusters. Then requests in each cluster are examined by comparing the request size with the measured normal size. The size of irregular requests are always large. Threshold for normal size is fixed by measuring the average size of the legitimate requests. The cluster with maximum number such threats is detected and the requests are classified as attack. Beyond this, the classification of requests in each cluster requires further investigation. This investigation and application of Dempster-Shaffer theory for this classification are planned to be implemented in the future work.

4 Simulation and Performance Analysis

The performance of the proposed two models are evaluated in a simulated environment which includes a server, clients and a dispatcher. The dispatcher is a global scheduler which is organized before the server to capture the clients' requests and analyzes the requests before forwarding them to the server. In this simulated environment, the clients' requests are captured at the dispatcher in different time intervals using Wireshark, a network protocol analyzer [4] and they are represented as 'Request set 1' and 'Request set 2'. For effortless capturing, in this paper the Wireshark filter is configured to capture the requests with

XML over HTTP. Request set 1 has 600 requests and they are captured for the timespan of 428ms. Request set 2 consists of 575 requests and these requests are captured for the timespan of 390ms. The request set for training the proposed models is captured for the timespan of 325ms and it consists of 520 requests. After capturing, the XML packet details are exported for each request stream using Wireshark. Further they are parsed to formulate the feature vector and the proposed two models are trained using Matlab. The proposed models, SCR and UCR are analyzed and evaluated using classification metrics, precision, recall and accuracy. Precision is defined as the ratio of number of requests correctly classified to total number of predicted requests of the given class. Accuracy is defined as the ratio of number of requests correctly classified for both the classes to total number of requests. Recall is defined as the ratio of number of correctly classified requests to number of labelled requests of a class [9].

4.1 Performance of SCR

In this paper, two sets of requests are captured for analysis in random time. The XML requests are parsed and restructured to compute feature vectors. Feature vectors are computed as described in Section 3. Number of namespace is large only for malformed messages, so the requests with large number of namespaces are identified as XML based attack. SCR discriminates the attacks using the height of tags tree and size of the requests. As the performance of SVM classification relies on kernel functions, SCR is implemented using three kernel functions, Linear, Polynomial and RBF [13]. True positive, true negative, false positive and false negative are computed for all the three kernel functions separately. Then precision and recall values are calculated and plotted in Figure 2. It is observed from Figure 2 that RBF kernel

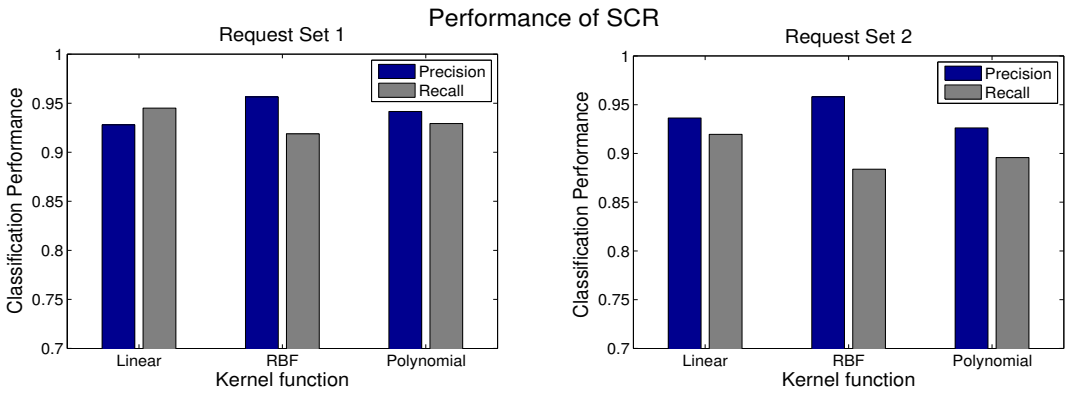

Figure 2: Kernel function Vs Classification performance of SCR

produces high precision and low recall for both request sets; linear kernel function gives low precision and high recall; whereas in polynomial kernel, the recall and precision values are average. Now to overcome the tradeoff, the kernel functions are analyzed against detecting maximum number of attacks. As per the definition of precision, the precision is high, when a kernel function identifies maximum number of attacks. So the RBF kernel function is used to implement SCR to discriminate more coercive parsing attack.

4.2 Performance of UCR

The feature vector constructed for two sets of captured requests are analyzed by the proposed UCR. K-means clustering technique is implemented with the constructed feature set. Initially, the number of

cluster is fixed as 3, i.e., k=3 and the requests are categorized into 3 groups. Then the value of 'k' is increased to 4,5,6 & 7. It is inferred from the results that when k=5, categorization of the requests are more natural; three clusters are almost unchanged and consistent in further clustering with k = 6 and 7. So, UCR analyzes the requests in these three clusters by comparing the size of the request with the normal size, as the size of the irregular request is large due to more number of attributes, elements and

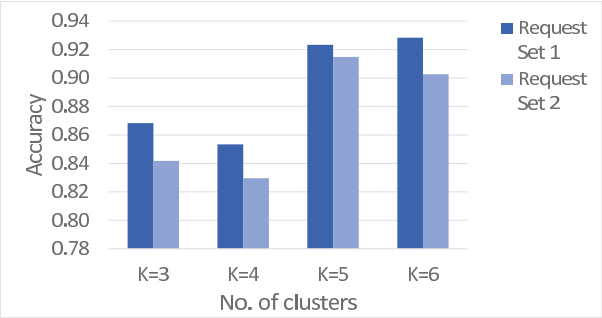

Figure 3: Number of clusters Vs Accuracy

namespaces. Then the cluster which has more number of oversized requests is detected and the requests in that cluster are classified as attacks. Further investigation of labelling in cluster is planned in future work. Now the classification accuracy is computed for both sets of requests and for various 'k' values. It is plotted in Figure 3. It is observed from Figure 3 that the accuracy of UCR is low for both input sets when k=3 and the accuracies are high when k=5 and 6. To evaluate further, the precisions of the clusters for both request sets are computed and plotted in Figure 4. It is inferred from Figure 4 that the precision is low when k=3, however it is high when k=5 for both request sets. But, when k is 6, the precision of request set 2 is lesser than the precision with five clusters, i.e., k=5. This implies that UCR discriminates more attacks when k=5.

Figure 4: Number of clusters Vs Precision

4.3 Classification Analysis

Feature vectors are constructed for both testing request sets and given as test data for both models, SCR and UCR. Accuracy and precision are computed separately for both models and presented in section 4.1 and 4.2. Now the performance of SCR and UCR in terms of precision and accuracy are measured and plotted in Figure 5. It is inferred from Figure 5 that for both request sets the precision of SCR is higher than UCR, but UCR has produced higher accuracy compared to SCR. It implies that the more number of

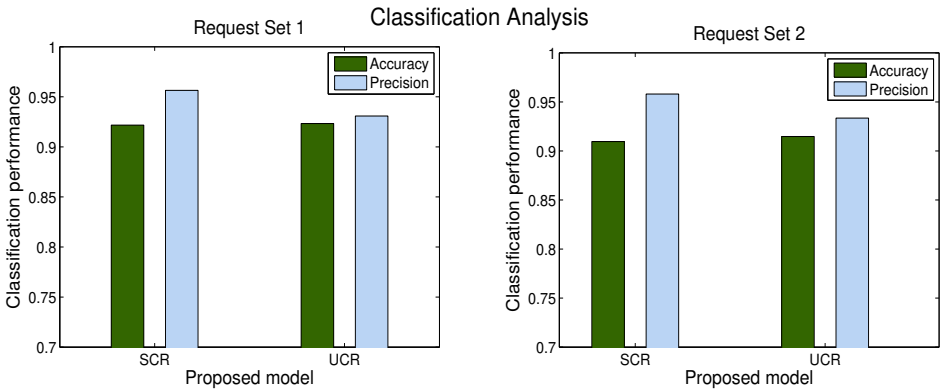

Figure 5: Proposed model Vs Classification performance

attacks are identified correctly by SCR and more number of normal requests are identified by UCR. Additionally, attack detection rates for both models are computed and plotted in Figure 6. It is observed from Figure 6 that detection rate of SCR is higher than UCR for various arrivals for both request sets. Already it is stated that precision of SCR is higher than UCR. Hence the SVM Classifier based on Request structure using RBF kernel proficiently discriminates more number of coercive parsing attacks.

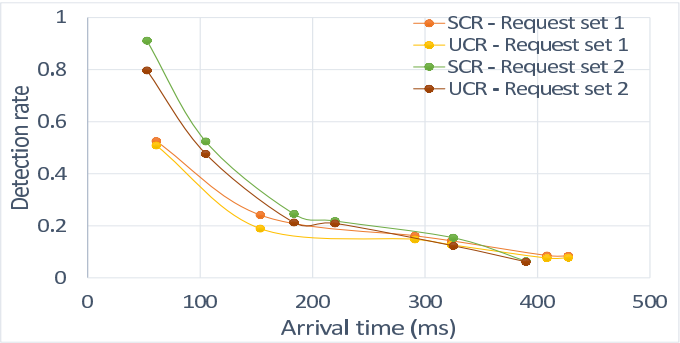

Figure 6: Arrival time Vs Detection rate

5 Conclusion

Classification of requests at cloud server is necessary to prevent the malicious requests and to improve legitimate access to cloud resources. Two machine learning classification models are proposed in this paper to discriminate coercive parsing attack. The captured XML requests are pruned and features are computed. After deep interrogation, the features which discriminates the irregularities are discovered. The proposed SVM based classifier proficiently discriminates the attacks using identified features. Unsupervised classification model categorizes the requests into various clusters according to the similarities in features. The most distinguishable feature to discriminate attacks is further predicted and applied to classify attacks in the cluster. The requests are captured using Wireshark and the classification models are simulated using Matlab. The performance of the proposed classification models are evaluated with respect to precision, recall and accuracy. It is inferred from the simulated results that the SVM based classification model has outperformed unsupervised classification model in discriminating coercive parsing attack.

References

[1] E. Adi, Z. A. Baig, P. Hingston, and C.-P. Lam. Distributed denial-of-service attacks against http/2 services. *Cluster Computing*, 19(1):79–86, March 2016.

[2] H. Beitollahi and G. Deconinck. Tackling application-layer ddos attacks. *Procedia Computer Science*, 10:432–441, 2012.

[3] C.-Y. Chang, K. Srinivasan, S.-J. Chen, M.-S. Chang, and V. Sharma. An efficient svm based lymph node classification approach using intelligent communication ant colony optimization. *Journal of Medical Imaging and Health Informatics*, 8(5):1077–1086, June 2018.

[4] L. Chappell and G. Combs. *Wireshark network analysis: the official Wireshark certified network analyst study guide*. Protocol Analysis Institute, Chappell University, 2010.

[5] V. Durcekova, L. Schwartz, and N. Shahmehri. Sophisticated denial of service attacks aimed at application layer. In *Proc. of the 9th International conference on ELEKTRO (ELEKTRO'12), Rajeck Teplice, Slovakia*, pages 55–60. IEEE, May 2012.

[6] M. Finsterbusch, C. Richter, E. Rocha, J.-A. Muller, and K. Hanssgen. A survey of payload-based traffic classification approaches. *IEEE Communications Surveys & Tutorials*, 16(2):1135–1156, April-June 2014.

[7] T. Karnwal, T. Sivakumar, and G. Aghila. A comber approach to protect cloud computing against xml ddos and http ddos attack. In *Proc. of the IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS'12), Bhopal, India*, pages 1–5. IEEE, March 2012.

[8] V. N. Lakshmi and S. Begum. Ddos defense: Enhanced flooding detection and confidence-based filtering method. *Advances in Computational Sciences and Technology*, 10(8):2257–2272, 2017.

[9] T. T. Nguyen and G. Armitage. A survey of techniques for internet traffic classification using machine learning. *IEEE Communications Surveys & Tutorials*, 10(4):56–76, October-December 2008.

[10] K. M. Prasad, A. R. M. Reddy, and K. V. Rao. Dos and ddos attacks: defense, detection and traceback mechanisms-a survey. *Global Journal of Computer Science and Technology*, 14(7), 2014.

[11] V. Sharma, K. Lee, S. Kwon, J. Kim, H. Park, K. Yim, and S.-Y. Lee. A consensus framework for reliability and mitigation of zero-day attacks in iot. *Security and Communication Networks*, 2017, November 2017.

[12] K. Singh, P. Singh, and K. Kumar. Application layer http-get flood ddos attacks: Research landscape and challenges. *Computers & security*, 65:344–372, March 2017.

[13] R. Yuan, Z. Li, X. Guan, and L. Xu. An svm-based machine learning method for accurate internet traffic classification. *Information Systems Frontiers*, 12(2):149–156, April 2010.

[14] J. Zhang, C. Chen, Y. Xiang, W. Zhou, and A. V. Vasilakos. An effective network traffic classification method with unknown flow detection. *IEEE Transactions on Network and Service Management*, 10(2):133–147, June 2013.

Author Biography

V. Punitha completed a Master of Engineering(ME), Computer Science and Engineering from National Institute of Technology, Tiruchirappalli, India in 2003. Currently she is pursuing Ph.D. degree in the same Institute at Department of Computer Science and Engineering. Her research area of interest includes Parallel and Distributed Systems, Network Security and Soft Computing Techniques.

C. Mala is a Professor in the Department of Computer Science and Engineering, National Institute of Technology, Tiruchirappalli, Tamil Nadu, India – 620 015. Her research area of interest includes Data Structures & Algorithms, Computer Networks, Parallel Algorithms, Computer Architecture, Sensor Networks, Soft Computing Techniques, Image Processing, Intelligent Transportation Systems and Vehicular Adhoc Networks.