Science Arena Publications
Specialty Journal of Electronic and Computer Sciences
ISSN: 2412-7485
Available online at www.sciarena.com
2019, Vol, 5 (4): 6-12

Introducing an Intrusion Detection System Based on Combined Fuzzy Inference Method and Hidden Markov Model to Identify DOS and PROBE Attacks

Saeed Teimoori[1]*, Reza Saravani[2]

[1] Department of Computer Science, Faculty of Computer Science and Mathematics, University of Shahid-Bahonar, Kerman, Iran.

[2] Department of Information Technology, Faculty of Electrical Engeering and Computer Engeering, Azad Islamic University of Rafsanjan, Rafsanjan, Iran.

***Corresponding Author**

Abstract: *Denial of Service (DoS) attacks conducted aiming to prevent users from accessing the services provided are among the most serious challenges encountered by the Internet service providers (ISPs). One of the characteristics of this type of attack is the high volume of traffic or service requests by the high number of unauthorized attackers forming a network of robots that decrease the network performance. The increasing expansion of botnets has caused attackers to use distributed approaches to perform DoS attacks. The DoS attacks are carried out in various ways which are divided into two categories of the high-rate and low-rate attacks with respect to the volume of the transmitted traffic. In a high-rate attack, by sending a lot of packets to the network or the victim broker, the attacker tries to get them out of service. In contrast to a high-rate attack, the average traffic rate sent by the attacker is low in a low-rate DoS attack. In a low rate DoS attack against an HTTP packet, the attacker makes an attack by misusing the HTTP request. Therefore, a method has been presented in this study to cope with the HTTP request attacks based on the Hidden Markov Model (HMM) and fuzzy system. In the proposed method, the characteristics of the attack traffic are first examined and the most appropriate ones are chosen. In the next step, these characteristics are pre-processed with data mining methods and trained to the HMM. Then, the fuzzy rules are defined and the membership functions are formed. The experimental findings indicated the more desirable performance of the proposed method in obtaining the accuracy rate compared to the base method.*

Keywords: *Markov model, HTTP request, Data mining, Fuzzy, accuracy rate.*

INTRODUCTION

In order to provide complete security in a computer system, in addition to firewalls and other intrusion prevention systems (IPSs), other systems namely the intrusion detection systems (IDSs) are required so that if the intruder crosses the firewall, the antivirus, and other security equipment and logged into the system, they can detect the attack and devise a way to cope with it. Based on a formal definition, intrusion is an active set of interconnected events aiming to reach an unauthorized access to information, alter the information, or hurt the system in a way to make the system unusable. This definition accounts for both the successful and unsuccessful attempts (Carl et al., 2006). Intrusion detection methods are categorized into two classes, misuse

detection and anomaly detection. Signature-based or misuse-based IDSs store the view of former attacks in their database, and fail to detect attacks that have not been already detected by the system. In the anomaly detection method, the usual behavior of users is in fact considered as the basis of action, and thus any contradicting behavior is identified as an attempt to intrude the system. Detection of anomalies is important in numerous fields and identification of a time series with a specific feature remarkably differs from a large set of other time series. For instance, a company's stock price behavior may exhibit a significant deviation from that of other companies in the same group over time, and the comparisons indicate that the basic problem should lie in the beginning of operations by the stock dealers. The most important objective in such actions is to detect the instantly occurring deviation; otherwise another dealer may suffer losses due to delays in the analysis and decision-making (Axelsson, 2000; Lunt, 1993).

In the present study, an anomaly based IDS has been proposed using a Hidden Markov Model (HMM) with fuzzy inference to detect the denial of service (DoS) attacks. The important task in detecting anomalies is to model or classify patterns, which, if performed well, a better performance can be witnessed in detecting anomalies. Using the HMM is a good strategy to model or classify patterns in an appropriate way (Lunt, 1993). In the previous methods, a threshold was exploited to distinguish between the malware and non-malware transmitted traffic, however the threshold was not responsive well in the case when there was a high deal of similarities between malware and non-malware packets. Thus, the fuzzy inference is employed for this purpose. In this regard, there are N http requests initially, with each request $n \epsilon N$ having an L label; this label can represent either a malware and non-malware request on the basis of the features extracted from several request sets. Each request n includes the IP number, the request time, the code sent to the server, the settling time, the protocol, the service, the flag, the number of bytes of the source data, the number of bytes of the destination data, the number of the failed login attempts, etc. Examining these requests and extracting specific features such as the code sent to the server, request method, IP address, number of bytes of the destination data, number of bytes of the source data, failed system login attempts, and user agent string, one can find out the request type and predict its range of performance in order to correctly group the new requests in accordance with the trained request and then detect the DOS and Probe attacks.

Pervious works

Network security is one of the most important sections of the security domain. Critical services in any infrastructure (wired, wireless, sensor networks) are accessible mainly through web connections. These services are well protected by the firewalls and antivirus software as a defense level. Given the development of the Internet technology, Internet resources and its services are accessible in a distributed environment from a remote area. This feature is beneficial for both the authorized users and attackers.

With the rapid spread of the Internet and the availability of the advanced attack tools as well as the vulnerability of the Transmission Control Protocol (TCP)/Internet Protocol (IP) protocol stack, numerous security attacks including the distributed denial of service (DDoS) attacks have appeared as a serious threat. The DDoS attack is a relatively simple yet strong attack on the Internet resources that initially emerged in June 1998 and expanded quickly. These attacks cause wide damages, attacking the renowned websites such as yahoo, amazon, Data, eBay, Buy, CNN and so on. If the attacker uses multiple systems simultaneously to set up attacks against a remote host, it is regarded as a DDoS attack. In DDoS method, the attacker usually infects several systems and commands them simultaneously (Karig and Lee, 2001).

A DDoS attack is an attempt to make the system and network resources unreachable to the authorized users. Although the goal of the DDoS attack and the motivation behind it may differ, it generally consists of trying to temporarily or permanently interrupt or suspend the services of an Internet-connected host. Financial and economic damages, disruption of the network performance, and inaccessibility of services in vital times are among the factors that motivate the individuals to protect the network resources and applications (Specht and Lee, 2003).

Due to causing malfunction of an information system and depriving users of access to the services provided by the desired server, the DDOS attack is one of the most common types of attacks, hence detection of these attacks is essential; soft computing methods, such as neural networks (NNs), fuzzy inference systems (FISs), and their combination, i.e. the neuro-fuzzy systems, have indicated suitable results in detecting these attacks. In a new method (Koc et al., 2012), a group of adaptive neuro-fuzzy inference systems are exploited to classify network activities and detect intrusions. Then a fuzzy inference module makes the final decision on whether the current activity is a normal or intrusive one. Ultimately, a genetic algorithm (GA) is employed to optimize the structure of the fuzzy decision-making system in order to obtain the best result; this method brings about a high detection rate. In (Sindhu et al., 2012), using the adaptive neuro-fuzzy inference systems and the Bagging algorithm, a group of classifiers have been developed to detect intrusions; this strategy has a high detection accuracy compared to other methods.
A three-step algorithm can be adopted to design a set of the neuro-fuzzy systems. Once the group of the classifiers is formed through the Bagging algorithm, each neuro-fuzzy system updates its own T-norm parameter, consequently improving the accuracy and decreasing the number of the parameters. To improve the accuracy, the neuro-fuzzy systems can be grouped together using the Adaptive Boosting (AdaBoost) algorithm. Fuzzy subsystems are trained by the gradient learning and are initialized by the fuzzy c-means (FCM) clustering algorithm. This change improves the interpretability of knowledge by merging the rule bases of the subsystems into a knowledge base (Garcia-Teodoro et al., 2009).
In (Freiling et al., 2005), a set of neuro-fuzzy classifiers and voting algorithm were applied, with a performance improved in comparison with the existing algorithms. Using a set of neuro-fuzzy classifiers and the AdaBoost algorithm, a novel method has been proposed in which the classification is performed with unknown features and lower number of features.

Proposed Method

The IDSs procedure of action is as the data are initially divided into two parts of training and test data. Thus, the pre-processing is carried out first and the desired features are extracted from the database. In the next step, the IDSs train the first part of the data to their own model and then evaluate their proposed method. Most of the attack detection systems created based on the machine learning algorithms use data training in the first step, and evaluate the previous step in the second step. In the first step, the training model of the system is formed based on the features extracted from the dataset. The schematics of the proposed system is demonstrated in figure (1). In the evaluation step, several HMMs are created for each HTTP packet in this system. Each group of HMMs is trained to model each feature extracted from the HTTP packet. The probabilistic values obtained from the models are combined within a group of HMMs (fused) and the desired final output forms. Then, fuzzifying the output of each HMM group, the inference process specifies the normality or abnormality of the HTTP packets using the fuzzy rules and sets.
The method used to perform the present study was organized as follows:

1. Initially, investigations were conducted regarding the features of the DOS attack detection, and the important features of this attack were specified in the HTTP packet using the data mining methods.
2. Then a large number of data mining algorithms were examined.
3. Studies were carried out on the evaluation criteria associated with the data mining algorithms for DOS attack detection.
4. Using the best data mining algorithms and a new algorithm used for feature creation and selection, a new method was developed to detect the DoS attacks.

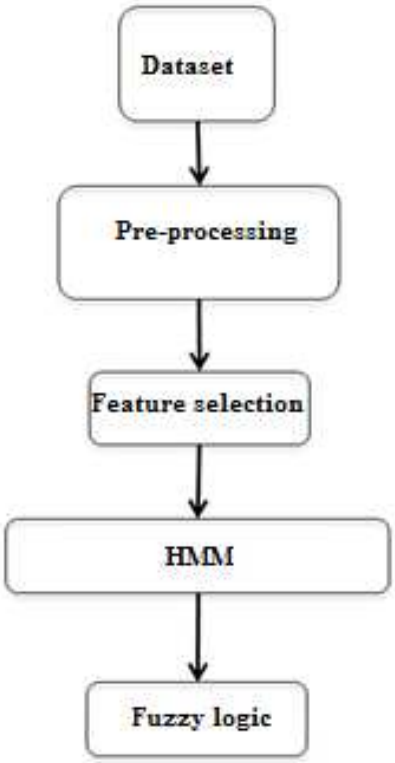

Figure 1. Schematics of the proposed method

Data modeling

The KDDCup99 database was exploited to import input data into the system; this database has been used in most DoS attack detection systems[1]. This database contains 4GB of initial data in 0 and 1 forms recorded over seven weeks. The recorded data include the sum of the packets sent from the origin to the destination. In addition, 2 million records are available in this database for modeling and training, with each record containing 41 features. The attacks used in this database are:

- ✓ DoS attacks
- ✓ Unauthorized access to remote control system
- ✓ Unauthorized access to the system administrator
- ✓ Port attack

A sample neptune attack record and normal record are as follows:

0,tcp,private,S0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,113,10,1.00,1.00,0.00,0.00,0.09,0.07,0.00,255,10,0.04,0.06,0.00,0.00,1.00,1.00,0.00,0.00,neptune.

0,tcp,http,SF,260,1837,0,0,0,0,1,0,0,0,0,0,0,0,0,0,11,11,0.00,0.00,0.00,0.00,1.00,0.00,0.00,24,159,1.00,0.00,0.04,0.04,0.00,0.00,0.00,0.00,normal.

Learning system

After the data preparation, the system learning model, namely HMM, is formed. A HMM uses the Baum-Welch algorithm to learn data. In this way, the observation matrix, hidden layers, transition matrix, and probability matrix must be initialized. Then, each hidden layer is mapped to a feature and the data of this feature are considered as the HMM observations. The trial and error method is used for testing and the best training situation has been achieved.

[1] http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

Fuzzy logic

The fuzzy logic is used at this stage. Thus, the fuzzy rules are defined first, then the membership function is formed and eventually, the inference process is performed. Suppose that the set of the fuzzy rules is as follows:

$$R=\sum_{i=1}^{n} Rule$$

And the selected features are as follows:

$$F=\sum_{i=1}^{5} Feature$$

Accordingly, the membership function formed for these features is as follows based on the rules defined:

$$\mu_R(F_i),\ \mu_R(F_i) \in \{low, medium, high\}$$

Detection

At this stage, the input values from the previous section are initially transformed into the fuzzy values, which are the same as the fuzzy sets. One of the important tasks to perform at this stage is to use the fuzzy functions to calculate the degree of accuracy of each adaptive fuzzy set (AFS) and transform the probabilistic values to fuzzy values in the form of the fuzzy sets. In the next step, the fuzzy values are converted to the real values required, which can be one of the two malware and non-malware values. There are several defuzzification techniques, including the maximum defuzzifier, center of gravity defuzzifier, and the mean of centers defuzzifier.

Experiences and evalution

In order to implement the proposed method, a system with the following configuration is used:

1. Windows operating system
2. 7-core processor
3. RAM memory equal to 6 GB
4. 4 MB of cache memory

Moreover, programming of the proposed method was conducted in the Matlab software environment.

Statistical population

As described in Chapter 3, a special technique is used for feature extraction. These features are trained to each HMM and a set of HMMs are employed for training. For this purpose, 300000 and 150000 records of malware and non-malware data were used for training, respectively. The data were selected using the RAND function included in Matlab software; this function selects the data randomly from the KDDCup database. Given the basic studies, the random selection of the data was performed for the sake of the accurate and fair evaluations.

Evaluation criteria

To evaluate their methods, most IDSs use criteria that indicate the performance of their systems. These criteria will be introduced later. To define these criteria, two types of possible errors in IDSs must be defined first.

1. False alert error: If a normal connection is detected as an attack, a false positive error takes place.
2. False no-alert error: If a connection with the attack label is detected as a normal connection, a false negative error takes place.

The followings are also used as supplementary definitions:

3. Correct alert: The total number of the normal data detected as a normal data during the intrusion detection process.
4. Lack of correct alert: The number of the malware data in the database that are commonly detected to be malware during the intrusion detection process.

In pattern recognition, data retrieval, and binary classification, the accuracy criterion is the proportion of the relevant samples among the retrieved samples. Therefore, accuracy is based on the understanding and measuring of the communication. In other words, in an IDS, this criterion represents the accuracy of the system in detecting the malware packets as malware. Table 2 demonstrates the procedure of calculation of this criterion.

Table 2: procedure of calculation accuracy criterion

accuracy	
positive	negative
$\frac{Tp}{Tp + Fp}$	$\frac{TN}{TN + FN}$

Table 3. Calculation of the accuracy criterion

accuracy	
positive	negative
93.04%	98.4%

Besides, the accuracy rate of the proposed method in comparison to the base method is indicated in figure 2.

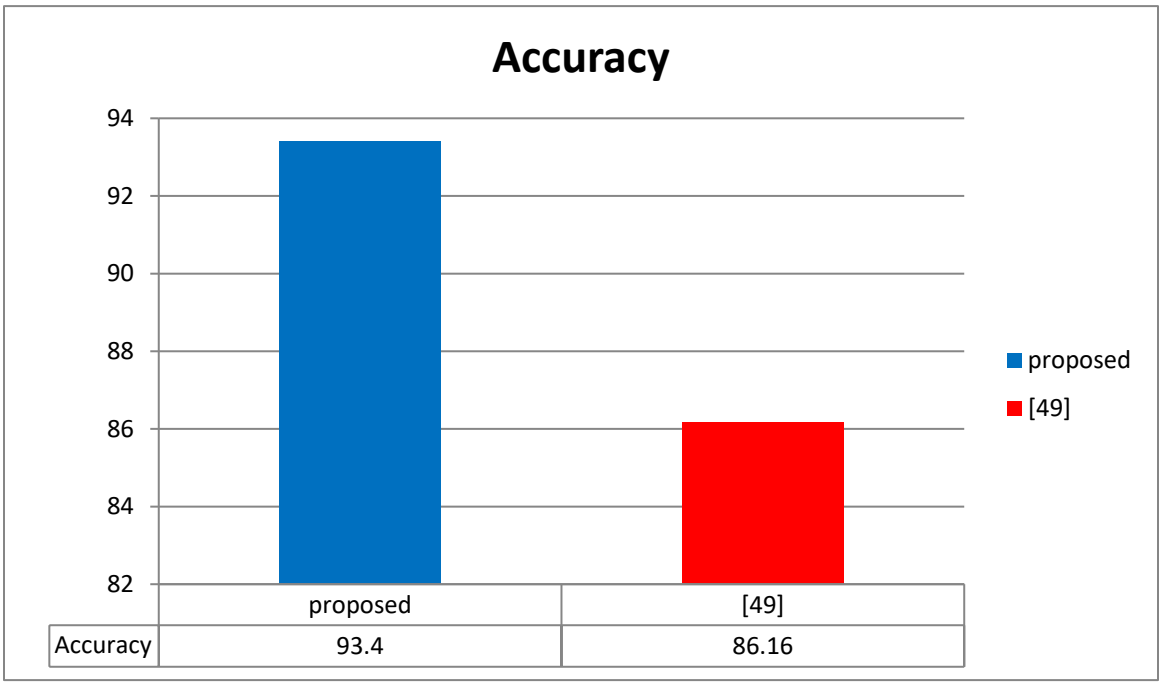

Figure 2. Comparison of the accuracy rate of the proposed system with the latest model proposed (More and Gosavi, 2016)

As it is clear, the performance of the proposed system in detecting the attack was more desirable compared to the base method, and yielded a low error rate, indicating the importance of the HMM in modeling the data as well as the fuzzy logic in decision making, both with a suitable performance.

Conclusion

A DoS attack aims to prevent users from access to machines or network resources. In other words, it is an attempt to deprive the users of accessing their expected services, either by interrupting the server system or disabling the network infrastructure associated with that system. In this study, an IDS was presented based on the HMM and fuzzy logic. The experimental results illustrated the more desirable performance of the proposed method in yielding the accuracy rate in comparison with the base method.

References

1. Axelsson, S. (2000). *Intrusion detection systems: A survey and taxonomy* (Vol. 99). Technical report.
2. Carl, G., Kesidis, G., Brooks, R. R., & Rai, S. (2006). Denial-of-service attack-detection techniques. *IEEE Internet computing*, *10*(1), 82-89.
3. Freiling, F. C., Holz, T., & Wicherski, G. (2005, September). Botnet tracking: Exploring a root-cause methodology to prevent distributed denial-of-service attacks. In *European Symposium on Research in Computer Security* (pp. 319-335). Springer, Berlin, Heidelberg.
4. Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *computers & security*, *28*(1-2), 18-28.
5. Karig, D., & Lee, R. (2001). Remote denial of service attacks and countermeasures. *Princeton University Department of Electrical Engineering Technical Report CE-L2001-002*, *17*.
6. Koc, L., Mazzuchi, T. A., & Sarkani, S. (2012). A network intrusion detection system based on a Hidden Naïve Bayes multiclass classifier. *Expert Systems with Applications*, *39*(18), 13492-13500.
7. Lunt, T. F. (1993). A survey of intrusion detection techniques. *Computers & Security*, *12*(4), 405-418.
8. More, K. K., & Gosavi, P. B. (2016, March). A real time system for denial of service attack detection based on multivariate correlation analysis approach. In *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)* (pp. 1125-1131). IEEE.
9. Sindhu, S. S. S., Geetha, S., & Kannan, A. (2012). Decision tree based light weight intrusion detection using a wrapper approach. *Expert Systems with applications*, *39*(1), 129-141.
10. Specht, S., & Lee, R. (2003). Taxonomies of distributed denial of service networks, attacks, tools and countermeasures. *CEL2003-03, Princeton University, Princeton, NJ, USA*.