A System for Denial-of-Service Attack Detection using MCA and IDS-based on Fuzzy Logic

Lalita Saini
ME-II Student
SSBT'S College of Engineering
and technology,Jalgaon

N.Y. Suryawanshi
Professor
SSBT'S College of Engineering
and technology, Jalgaon

ABSTRACT

In the networking world, a denial of service (DoS) attack is an incident in which a user is deprived of the services of a resource they would normally expect to have. Intrusion Detection System (IDS) is the tool that is able to detect occurrences of intrusion at host, the network and application in the system. One of the most common network attacks is Denial of Service (DoS) attack. In DoS attack of the computer system an individual host will send huge number of packets to one machine so it make the operating of the network and host slow. In this paper, signature of selected attacks such as Smurf, Ping-of-Death which are based on network flow is considered and Mail-Bomb. The system uses MCA based system for detection of the DoS attack. The proposed system monitors the network path to detect attacks and the results show less false negative error during monitoring of the system. Specially, signature based IDS which use fuzzy decision tree for monitoring network path observes that there are great improvements on speed of detection as well as performance of system in the organization.

General terms

We are using two main terms MCA based system and IDS based fuzzy logic system.

Keywords

Denial-of-Service attack, IDS, Multivariate correlations, fuzzy logic.

1. INTRODUCTION

Deniel of service (DoS) attacks are one type of most commanding and more intrusive behavior to on-line servers in the network systems. DoS attacks severely break down the availability of a victim which can be a host or router or an entire network in the system. They impose intensive computation tasks to the victim by exploiting its system vulnerability or flooding it with large amount of useless packets in the network. The Detection systems based on these mechanisms monitor traffic transmitting over the protected networks in the system. These mechanisms release the protected online servers from monitoring attacks with ensure that the servers can dedicate themselves to provide quality services with minimum delay in response in networking. Additionally, network-based detection systems are loosely coupled with operating systems running on the host machines which they are protecting. Finally the configurations of network-based detection systems are simpler than that of host-based detection systems.

Therefore experts started to explore a way to gain novelty-tolerant detection systems and developed a most advanced concepts namely

anomaly- based detection of the network area. The principle of detection of attacks which monitors and flags any network activities presenting significant deviation from valid traffic profiles as suspicious objects. anomaly-based detection techniques show more promising in detecting zero-day intrusions that exploit previous unknown system vulnerabilities[3]. It is not constrained by the expertise in network security because of the fact that the profiles of valid behaviors are developed based on techniques like data mining [4],[5]machine learning [6] and statistical analysis method. These proposed systems commonly face the high false positive rates because the correlations between features/attributes are neglected or the techniques do not manage to fully exploit these correlationsin the network system. Here, Intrusion detection has emerged as a significant field of research and because it is not theoretically possible to set up a system. One main confrontation in intrusion detection is that we have to find out the concealed attacks from a huge quantity of routine communication activities in the system . Most of the machine learning (ML) algorithm setection method, Fuzzy Logic [7], and Data Mining and more have been extensively employed to detect intrusion activities both known and unknown from large amount of difficult and run time datasets in the system. In the Generating rules is vital for IDSs to distribute standard behaviors from strange behavior by examining the dataset which is a list of tasks created by the operating system that are registered into a file in historical sorted order in the database. Different researches with data mining as the chief constituent has been carried to find out newly encountered intrusions in the system. Overall analysis of data to determine relationships and find concealed patterns of data which otherwise would go unobserved is known as data mining techniques. So, Many researchers have used data mining to concentrate into the subject of database intrusion detection in databases regarding network systems.

2. SYSTEM ARCHITECTURE

The overview of our denial of service (DoS) attack detection system architecture and framework is given below:

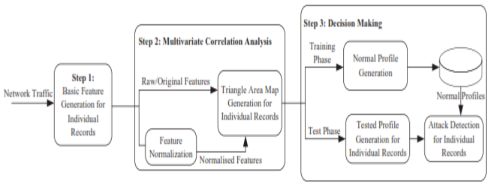

Network Traffic
Step 1:
Basic Feature Generation for Individual Records
Step 2: Multivariate Correlation Analysis
Raw/Original Features
Triangle Area Map Generation for Individual Records
Feature Normalization
Normalised Features
Step 3: Decision Making
Training Phase
Normal Profile Generation
Normal Profiles
Test Phase
Tested Profile Generation for Individual Records
Attack Detection for Individual Records

Fig 1 :Framework of the proposed denial-of-service attack detection system

2.1 Framework

The complete detection process consists of three major steps as shown in Fig.1. Initially,In Step 1 basic features are generated from admission network traffic to the internal network where protected servers reside in and are used to form traffic records for a well-defined time interval. Step 2 is Multivariate Correlation Analysis(MCA) in which the Triangle Area Map Generation module is applied to enhance the correlations between two distinct features. In Step 3 the anomaly-based detection mechanism [3] is adopted in Decision Making of the data. It facilitates the detection of any DoS attacks without getting any attack related knowledge of the system. Furthermore, the labor-intensive attack analysis and the frequent update signature of the attack database in the case of misuse-based detection are avoidedby the system. So, the mechanism enhances the special property robustness of the proposed detectors and makes them harder to be evaded due to attackers need to create attacks that match the normal traffic profiles built by a specific detection algorithm of dos detection.

3. IMPLEMENTATION

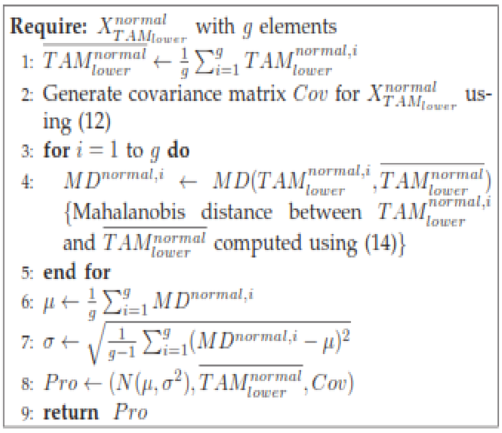
3.1 Multivariate Correlation Analysis

DoS attack traffic behaves varily from the valid network traffic and the behavior of network traffic is responded by its statistical properties of detection system. So to describe these statistical properties we present a Multivariate Correlation Analysis (MCA) approach in this module of DoS attack detection. Here, this MCA motto employs triangle area for enhancing the correlative information between the features within an observed data object in the system.

3.2 Detection Mechanism

In this module we present a threshold-based anomaly detector whose normal profiles are generated using purely valid network traffic records and use it for future comparisons with new incoming investigated traffic records of data. Initially we apply the proposed triangle area-based MCA approach to analyze valid network traffic and the generated TAMs are then used to gain the most unique attributes for normal profile generation of the system.

A. Normal Profile Generation



```
Require: $X^{normal}_{TAM_{lower}}$ with $g$ elements
$\overline{TAM^{normal}_{lower}} \leftarrow \frac{1}{g}\sum_{i=1}^{g} TAM^{normal,i}_{lower}$
Generate covariance matrix $Cov$ for $X^{normal}_{TAM_{lower}}$ using (12)
for $i = 1$ to $g$ do
    $MD^{normal,i} \leftarrow MD(TAM^{normal,i}_{lower}, \overline{TAM^{normal}_{lower}})$
    {Mahalanobis distance between $TAM^{normal,i}_{lower}$ and $\overline{TAM^{normal}_{lower}}$ computed using (14)}
end for
$\mu \leftarrow \frac{1}{g}\sum_{i=1}^{g} MD^{normal,i}$
$\sigma \leftarrow \sqrt{\frac{1}{g-1}\sum_{i=1}^{g}(MD^{normal,i} - \mu)^2}$
$Pro \leftarrow (N(\mu, \sigma^2), \overline{TAM^{normal}_{lower}}, Cov)$
return $Pro$
```

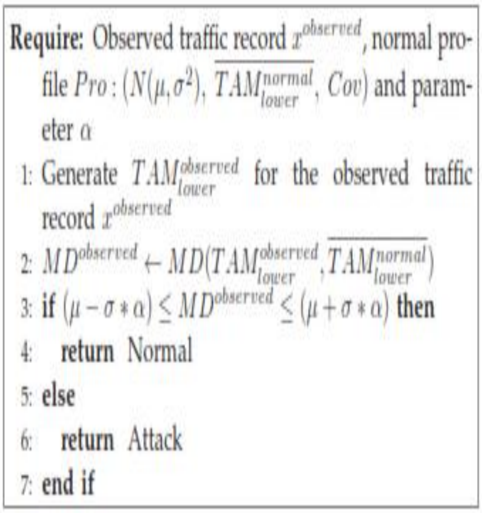
Fig 2: Algorithm for normal profile generation based on triangle-area-based MCA.

Here Fig. 2 shows the algorithm for normal profile generation in which the normal profile P ro is built through the density estimation of the MDs between individual network traffic records (T AM normal,i) and the expectation (T AM normal) of the g valid training traffic recordsin the flow.

B. Attack Detection

3.3 Network intrusion Detection System using fuzzy logic

Recently, different researchers focused on fuzzy rule learning for effective intrusion detection using data mining techniques in the computer systems. Here, the fuzzy rules developed from the latest strategy can be able to provide best distribution rate in detecting the intrusion behavior in the network. Mainely the advantage of anomaly-based detection techniques is their ability to detect unknown intrusion occurrences from the network. The different steps involved in the proposed system for anomaly-based intrusion detection are described below:(1) Classification of training data(2) Different Strategy for generation of fuzzy rules(3) Fuzzy decision module (4) searching an appropriate classification for a test Input



```
Require: Observed traffic record $x^{observed}$, normal profile $Pro : (N(\mu, \sigma^2), \overline{TAM^{normal}_{lower}}, Cov)$ and parameter $\alpha$
Generate $TAM^{observed}_{lower}$ for the observed traffic record $x^{observed}$
$MD^{observed} \leftarrow MD(TAM^{observed}_{lower}, \overline{TAM^{normal}_{lower}})$
if $(\mu - \sigma * \alpha) \leq MD^{observed} \leq (\mu + \sigma * \alpha)$ then
    return Normal
else
    return Attack
end if
```

Fig 3: Algorithm for attack detection based on Mahalanobis distance

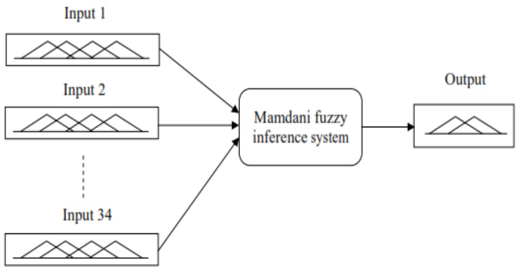


Fig 4: The designed of fuzzy logic

3.3.1 Strategy for Generation of Fuzzy rule

This module describes the designed strategy for automatic creation of fuzzy rules to provide effective learning in the system. Generally, the fuzzy rules given to the fuzzy system is done manually who are given the rules by analyzing intrusion behavior in the system. It is very hard to generate fuzzy rules manually because of the fact that the input data is huge also more attributes of the system. few of researches are available in the literature for automatically introducing of fuzzy rules in latest times of the network system. Using above reference we make use of mining methods to identify a better set of rules in the networking. Here, definite rules obtained from the single length frequent items are used to provide the proper learning of fuzzy system in the given area. So, The process of fuzzy generation is given in the following sub-section.(a) Mining of single length frequent items (b) Identification of suitable attributes for rule generation(c) Rule generation (d) Rule filtering(e) Generating fuzzy rules

3.3.2 Fuzzy Decesion Module

This module describes the designing of fuzzy logic system for searching the suitable class label of the test dataset of the system. Here, the designed fuzzy system shown in fig. 2 includes total 34 inputs and single output where inputs are relevant to the 34 attributes and output is related to the class label in the system. Actually here 34 input and single-output of Mamdani fuzzy inference system with defuzzification strategy was used for this purpose in the network area. These rules obtained to the fuzzy rule base for learning the actual system in the networking system.

4. RESULT ANALYSIS

A.MCA based detection:

In the MCA-based detection system the overall DR and FPR are described in Table 1. The overall FPR and DR are computed overall traffic records regardless the types of attacks in the networking. Here,when the threshold grows from 1σ to 3σ the FPR decreases quickly from 1.26% to 0.53% and DR also decreases from 95.11% to 86.98% at the time of threshold increases. So,It shows clearly in the table that a bigger number of valid traffic records are covered by a greater threshold, and more DoS attack records are not correctly accepted as valid traffic in the meantime of system.

Table 1: Detection Rate and False Positive Rates Achieving by the Proposed System on Original Data

	Threshold				
	1σ	1.5σ	2σ	2.5σ	3σ
FPR	1.26%	0.97%	0.77%	0.65%	0.53%
DR	95.11%	89.44%	88.11%	87.51%	86.98%
Accuracy	95.20%	89.67%	88.38%	87.79%	87.28%

Table 2:Detection Rate and False Positive Rate Achieving by the Proposed System

	Threshold				
	1σ	1.5σ	2σ	2.5σ	3σ
FPR	2.64%	2.03%	1.68%	1.44%	1.25%
DR	100.00%	99.99%	99.97%	99.97%	99.96%
Accuracy	99.93%	99.95%	99.93%	99.93%	99.93%

4.1 For IDS-Based on Fuzzy Logic

In the IDS based fuzzy logic method, the training dataset includes normal data as well as four types of attacks which are given to the proposed system for identifying the suitable attributes for the system. Here, the selected attribute for the process of rule generation is given in table 3. Using the fuzzy rule learning strategy the system creates two types of rule definite and indefinite rules and finally, fuzzy rules are generated from the definite rules. In the testing phase the testing dataset is given to the proposed system which classifies the input as a normal or attack to the system. So, the obtained result is then used to compute overall accuracy of the proposed system in the network. Hence, the overall accuracy of the proposed system is computed based on the precision and recall also F-measure which are normally used to estimate the rare class prediction of the data.

These are computed using the confusion matrix in Table 4, and defined as follows

Table 3: Selected attributes for rule generation

Attribute index	Selected
1	duration
5	src_bytes
6	dst_bytes
8	wrong_fragment
9	urgent
10	hot
11	num_failed_logins
13	num_compromised
16	-
17	num_file_creations
18	num_shells
19	num_access_files
23	count
24	srv_count

Table 4: Confusion matrix

Predicted class			
		Positive class	Negative class
Actual	Positive class	True Positive	False Negative
Class	Negative class	False Positive	True Negative

Finally, the evaluation metrics are calculated for both training and testing dataset in the testing phase and get the result. So,by analyzing the result the overall performance of the proposed system is improved significantly and it gains more than 90% accuracy for all types of attacks in the networking system.

5. CONCLUSION

We have developed an anomaly based intrusion detection system for detecting the intrusion within a network. In this fuzzy decision-making module was constructed to generate the system more accurate for attack detection using the fuzzy inference approach. The proposed method is very much useful in detecting various intrusions in computer networks system. Here, the proposed system achieves equal or better performance as compared to the two state of the art approaches. Inthe future work we will further implement our DoS attack detection system with the help of real world data and find more impressive classification techniques to further less severe false positive rate.

6. ACKNOWLEDGMENTS

I would like to thanks my guide of project Mr. N.Y. Suryawanshi for moral support . I m also thankful to my college for giving me an apportunity.

7. REFERENCES

[1] V. Paxson, “Bro: A System for Detecting Network Intruders in Realtime,”Computer Networks, vol. 31, pp. 2435-2463, 1999

[2] P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E.Vzquez, “Anomaly-based Network Intrusion Detection: Techniques,Systems and Challenges,” Computers & Security, vol. 28,pp. 18-28, 2009.

[3] D. E. Denning, “An Intrusion-detection Model,” IEEE Transactions on Software Engineering, pp. 222-232, 1987.

[4] K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, “DDoS attack detection method using cluster analysis,” Expert Systems with Applications, vol. 34, no. 3, pp. 1659-1665, 2008.

[5] A. Tajbakhsh, M. Rahmati, and A. Mirzaei, “Intrusion detection using fuzzy association rules,” Applied Soft Computing, vol. 9,no. 2, pp. 462-469, 2009.

[6] J. Yu, H. Lee, M.-S. Kim, and D. Park, “Traffic flooding attack detection with SNMP MIB using SVM,” Computer Communications, vol. 31, no. 17, pp. 4212-4219, 2008.

[7] J. Luo, and S. M. Bridges, “Mining fuzzy association rules and fuzzy frequency episodes for intrusion detection”, International Journal of Intelligent Systems, Vol. 15, No. 8, pp. 687-704, 2000.