INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 3 (2016) PAGES 1030-1036
RECEIVED : 29/05/2016. PUBLISHED : 08/06/2016
June 8, 2016

A SYSTEM FOR DETECTION AND PRVENTION OF PATH BASED DENIAL OF SERVICE ATTACK

P.Priya[1] , S.Tamilvanan[2]
[1]M.E-Computer Science and Engineering Student, Bharathidasan Engineering College, Nattrampalli.
[2]Assistant Professor in Computer Science and Engineering, Bharathidasan Engineering College, Nattrampalli,

Abstract:
Interconnected systems, such as Web servers, database servers, cloud computing servers etc, are now under threads from network attackers. As one of most common and aggressive means, Denial-of-Service (DoS) attacks cause serious impact on these computing systems. In this paper, we present DoS attack detection and prevention system that uses Multivariate Correlation Analysis (MCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. Our MCA-based DoS attack detection system employs the principle of anomaly-based detection in attack recognition. This makes our solution capable of detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only.

Keywords-Denial-of-service attack, network traffic characterization multivariate correlations, etc.,

1. INTRODUCTION

The main features of an Internet network are its open environment and scalability. On one hand, these characteristics have led the growth of the Internet. On the other hand, vulnerabilities in the network have occurred simultaneously. The threat of Distributed Denial of Service (DDoS) attacks now has become a major issue in network security. Launching a DDoS attack becomes easier for DDoS attackers while the defenders have a more difficult detecting malicious network flow since the DDoS attacker now uses normal packets flow with spoofed packet information. A burden for the defenders is to process all packet information within a limited time because a DDoS attacker sends a lot of normal packets to a victim. Although there is a good monitoring scheme against DDoS attacks, it still needs relatively high computational time to identify an attack from a normal packet flow. The few current studies have focused mainly on reducing computation resources to detect a DDoS attack.This paper concentrates on designing an efficient DDoS attack detection method that can both significantly reduce computational time and increase detection accuracy. For the DDOS attack detection compare the packet number distribution of packet flows, which are out of the control of attackers once the attack is launched, and found the similarity of attack flows is much higher than the similarity among legitimate flows e.g. : flash crowds. Entropy growth rate as the length of a stochastic sequence increases.

A DoS attack might embrace execution of malware supposed to exhaust the CPU's usage, preventing any work from occurring, trigger errors within the firmware of the machine, trigger errors within the sequencing of directions, therefore on force the computer into associate unstable state or lock up or exploits the errors within the software system to cause resource starvation. DDoS attacks attempt to exhaust the victim's resources. These resources may be network information measure, computing power, or software package knowledge structures. To launch a DDoS attack, malicious user's initial build a network of computers that they'll use to supply the amount of traffic required to

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 3 (2016) PAGES 1030-1036
RECEIVED : 29/05/2016. PUBLISHED : 08/06/2016
June 8, 2016

deny services to computer users. To form this attack network, attackers discover vulnerable sites or hosts on the network.

Vulnerable hosts are typically those who are either running no antivirus code or out of date antivirus code, or those who haven't been properly patched. Vulnerable hosts square measure then exploited by attackers who use their vulnerability to achieve access to those hosts. Ensuing step for the trespasser is to put in new programs referred to as attack tools on the compromised hosts of the attack network. The hosts that are running these attack tools are referred to as zombies and that they will perform any attack underneath the management of the aggressor. Several zombies along kind a military, though this preparation stage of the attack is incredibly crucial, discovering vulnerable hosts and putting in attack tools on them became a Vulnerable hosts are typically those who are either running no antivirus code or out of date antivirus code, or those who haven't been properly patched. Vulnerable hosts square measure then exploited by attackers who use their vulnerability to achieve access to those hosts. Ensuing step for the trespasser is to put in new programs referred to as attack tools on the compromised hosts of the attack network. The hosts that are running these attack tools are referred to as zombies and that they will perform any attack underneath the management of the aggressor. Several zombies along kind a military, though this preparation stage of the attack is incredibly crucial, discovering vulnerable hosts and putting in attack tools on them became a really simple method. there's no would like for the trespasser to pay time in making the attack tools as a result of there are already prepared programs that mechanically realize vulnerable systems, break into these systems, and so install the required programs for the attack. After that, the systems that are infected by the malicious code search for alternative vulnerable computers and install on them constant malicious code.

2. SYSTEM ARCHITECTURE

The overview of our proposed DoS attack detection system architecture is given in this section, where the system framework and the Hidden Markov model mechanism are discussed.

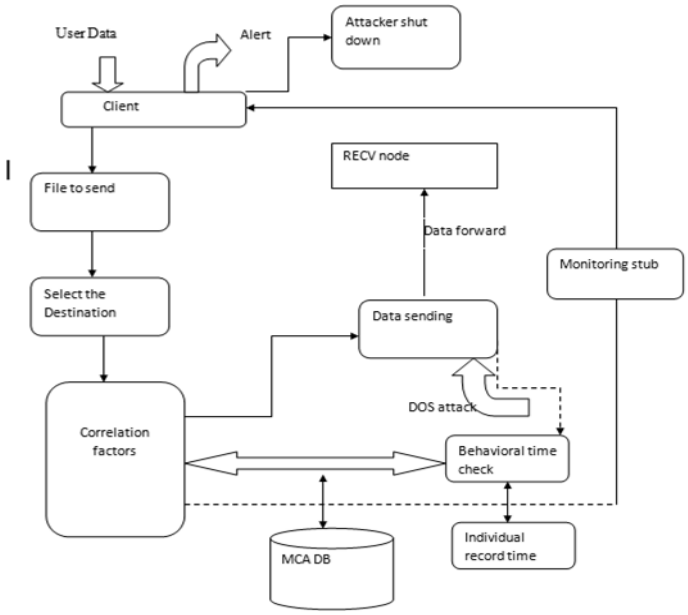


Fig.1.System architecture

2.1. SYSTEM FRAMWORK

Basic features are generated from ingress Network traffic to the internal network where protected servers reside in and are used to form traffic records for a well-defined time interval. Monitoring and analyzing at the destination network reduce the overhead of detecting malicious activities by concentrating only on relevant inbound traffic. This also enables our detector to provide protection which is the best fit for the targeted internal network because legitimate traffic profiles used by the detectors are developed for a smaller number of network services.

Multivariate Correlation Analysis, in which the "Triangle Area Map Generation" module is applied to extract the correlations between two distinct features within each traffic record coming from the first step or the traffic record normalized by the "Feature Normalization". The occurrence of network intrusions cause changes to these correlations so that the changes can be used as indicators to identify the intrusive activities. All the extracted correlations, namely triangle areas stored in Triangle Area Maps (TAMs), are then used to replace the original basic features or the normalized features to represent the traffic records. This provides higher discriminative information to differentiate between legitimate and illegitimate traffic records.The anomaly-based detection mechanism is adopted in Decision Making. It facilitates the detection of any DoS attacks without requiring any attack relevant knowledge. Furthermore, the labor-intensive attack analysis and the frequent update of the attack signature database in the case of misuse-based detection are avoided. Meanwhile, the mechanism enhances the robustness of the proposed detectors and makes them harder to be evaded because attackers need to generate attacks that match the normal traffic profiles built by a specific detection algorithm.

2.2 HIDDEN MARKOV MODEL

In this project, we present an alternative approach based on a novel Hidden Markov Model (HMM) for computing behavioral distance, and present the design, implementation, and evaluation of a novel architecture using HMM-based behavioral distance to detect attacks. An HMM models a doubly stochastic process; there is an underlying stochastic process that is not observable (it is "hidden") but that influences another that produces a sequence of observable symbols. When applied to our problem of computing behavioral distance, the observed symbols are process behaviors, and the hidden states correspond to aggregate tasks performed by the processes (e.g., read from a file).

An interesting and important observation is that since these hidden tasks should be the same, it should be possible to reliably correlate the simultaneous observable behaviors of the two processes when no attack is occurring, and to notice an increased behavioral distance when an attack succeeds on one of them. Perhaps surprisingly, our technique uses a single HMM to model both processes simultaneously, in contrast to traditional uses of HMMs for anomaly detection, where an HMM models a single process.

3. MULTIVARIATE CORRELATION ANALYSIS

DoS attack traffic behaves differently from the legitimate network traffic, and the behavior of network traffic is reflected by its statistical properties. To well describe these statistical properties, we present a novel Multivariate Correlation Analysis (MCA) approach in this section. This MCA approach employs triangle area for extracting the correlative information between the features within an observed data object (i.e., a traffic record).

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 3 (2016) PAGES 1030-1036
RECEIVED : 29/05/2016. PUBLISHED : 08/06/2016
June 8, 2016

Our MCA approach supplies with the following benefits to data analysis. First, it does not require the knowledge of historic traffic in performing analysis. Second, unlike the Covariance matrix approaches proposed. Which is vulnerable to linear change of all features, our proposed triangle-area-based MCA withstands the problem. Third, it provides characterization for individual network traffic records rather than model network traffic behavior of a group of network traffic records. This result in lower latency in decision making and enable sample-by-sample detection. Fourth, the correlations between distinct pairs of features are revealed through the geometrical structure analysis. Changes of these structures may occur when anomaly behaviors appear in the network. This provides an important signal to trigger an alert.

4. DETECTION MECHANISM

In this section, we present a threshold-based anomaly detector, whose normal profiles are generated using purely legitimate network traffic records and utilized for future comparisons with new incoming investigated traffic records. The dissimilarity between a new incoming traffic record and the respective normal profile is examined by the proposed detector. If the dissimilarity is greater than a pre-determined threshold, the traffic record is flagged as an attack. Otherwise, it is labeled as a legitimate traffic record. Clearly, normal In this section, we present a threshold-based anomaly detector, whose normal profiles are generated using purely legitimate network traffic records and utilized for future comparisons with new incoming investigated traffic records. The dissimilarity between a new incoming traffic record and the respective normal profile is examined by the proposed detector. If the dissimilarity is greater than a pre-determined threshold, the traffic record is flagged as an attack. Otherwise, it is labeled as a legitimate traffic record. Clearly, normal profiles and thresholds have direct influence on the performance of a threshold-based detector. A low quality normal profile causes an inaccurate characterization to legitimate network traffic. Thus, we first apply the proposed triangle area-based MCA approach to analyze legitimate network traffic, and the generated TAMs are then used to supply quality features for normal profile generation.

Require: $X_{TAM_{lower}}^{normal}$ with g elements
1: $\overline{TAM_{lower}^{normal}} \leftarrow \frac{1}{g}\sum_{i=1}^{g} TAM_{lower}^{normal,i}$
2: Generate covariance matrix Cov for $X_{TAM_{lower}}^{normal}$ using (12)
3: **for** $i = 1$ to g **do**
4: $MD^{normal,i} \leftarrow MD(TAM_{lower}^{normal,i}, \overline{TAM_{lower}^{normal}})$ {Mahalanobis distance between $TAM_{lower}^{normal,i}$ and $\overline{TAM_{lower}^{normal}}$ computed using (14)}
5: **end for**
6: $\mu \leftarrow \frac{1}{g}\sum_{i=1}^{g} MD^{normal,i}$
7: $\sigma \leftarrow \sqrt{\frac{1}{g-1}\sum_{i=1}^{g}(MD^{normal,i} - \mu)^2}$
8: $Pro \leftarrow (N(\mu, \sigma^2), \overline{TAM_{lower}^{normal}}, Cov)$
9: **return** Pro

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

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 3 (2016) PAGES 1030-1036
RECEIVED : 29/05/2016. PUBLISHED : 08/06/2016
June 8, 2016

4.1.ATTACK DETECTION

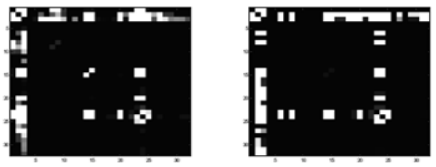
To detect DoS attacks, the lower triangle (TAMobservedlower) of the TAM of an observed record needs to be generated using the proposed triangle-area-based MCA approach. Then, theMD between the TAMobservedlower and the TAMnormal lower stored in the respective pre-generatednormal profile Pro is computed .The detailed detection algorithm is shown in Figure.3

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

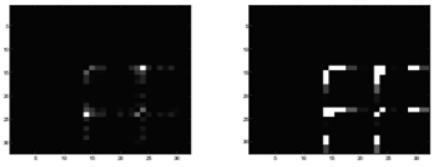
Fig.3.Algorithm

5. RESULTS AND ANALYSIS

In the evaluation, the TAMs of the different types of traffic records are generated using 32 continuous features. The images for the TAMs of Normal TCP record, Back attack record, Land attack record and Neptune attack record are presented in Fig. 4. The images demonstrate that TAM is a symmetric matrix, whose upper triangle and lower triangle are identical. The brightness of an element in an image represents its value in the corresponding TAM. The greater the value is, the brighter the element is. The images in Fig. 4 also demonstrate that our proposed MCA approach fulfils the anticipation of generating features for accurate network traffic characterization.



(a) Normal TCP record (b) Back attack record



(c) Land attack record (d) Neptune attack record

Fig. 4. Images of TAMs of Normal TCP traffic, Back, Land and Neptune attacks generated using original data

To evaluate the performance of our detection system along with the change of the threshold, the average TNRs for legitimate traffic and the average DRs for the individual types of DoS attacks are shown in Table.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 3 (2016) PAGES 1030-1036
RECEIVED : 29/05/2016. PUBLISHED : 08/06/2016
June 8, 2016

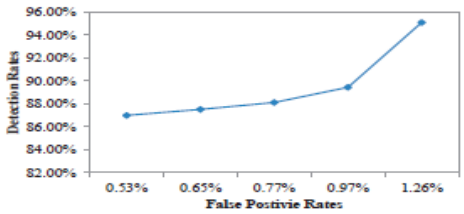
TABLE 1
Average Detection Performance of the Proposed System on Original Data Against Different Thresholds

Type of records	Threshold				
	1σ	1.5σ	2σ	2.5σ	3σ
Normal	98.74%	99.03%	99.23%	99.35%	99.47%
Teardrop	71.50%	63.92%	57.93%	52.81%	48.45%
Smurf	100.00%	100.00%	100.00%	100.00%	100.00%
Pod	100.00%	100.00%	100.00%	100.00%	100.00%
Neptune	82.44%	61.79%	57.00%	54.84%	52.96%
Land	0.00%	0.00%	0.00%	0.00%	0.00%
Back	99.96%	99.82%	99.58%	99.44%	99.31%

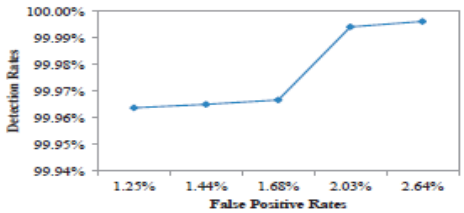
To have a better overview of the performance of our MCA-based detection system, the overall FPR and DR are highlighted in Table 2. The overall FPR and DR are computed over all traffic records regardless the types of attacks.

TABLE 2
Detection Rate and Fals 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%



(a) ROC curve for analysing original data



(b) ROC curve for analysing normalized data

Fig. 5. ROC curves for the detection of DoS attacks

CONCLUSION

This paper has presented a MCA-based DoS attack detection system which is powered by the triangle-area based MCA technique and the anomaly-based detection technique. The former technique extracts the geometrical correlations hidden in individual pairs of two distinct features within each network traffic record, and offers more accurate characterization for network traffic behaviors. The latter technique facilitates our system to be able to distinguish both known and unknown DoS attacks from legitimate network traffic.

FUTURE ENHANCEMENT

We will further test our DoS attack detection system using real world data and employ more sophisticated classification techniques to further alleviate the false positive rate.

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] W. Hu, W. Hu, and S. Maybank, "AdaBoost-Based Algorithm for Network Intrusion Detection," Trans. Sys. Man Cyber. Part B, vol. 38, no. 2, pp. 577-583, 2008.

[8] C. Yu, H. Kai, and K. Wei-Shinn, "Collaborative Detection of DDoS Attacks over Multiple Network Domains," Parallel and Distributed Systems, IEEE Transactions on, vol. 18, pp. 1649-1662, 2007.