REVIEW 1

OWASP ATTACKS (DOS)

ARAVIND V RAJEEV
18BIT0387

LITERATURE REVIEW

Defense against distributed DoS attack detection by using intelligent evolutionary algorithm[1]

Shubhra Dwivedi, Manu Vardhan

1) In order to mitigate denial of service attacks, in this paper, they use grasshopper optimization algorithm (GOA) with machine learning algorithm called GOIDS. This approach is based on creating an intrusion detection system (IDS) to fulfill the requirements of the monitored environment and able to distinguish between normal and attack traffics. Furthermore, GOIDS selects the most relevant features from the original IDS dataset that can help to distinguish typical low-speed DDoS attacks and then, selected features are passed to the classifiers.

   The study of DDoS attacks is a significant area of research; there are a number of techniques that have been proposed such as evolutionary algorithm and artificial intelligence in the literature for detecting DDoS attacks.
   Unfortunately, the modern well-known DDoS detection schemes are deteriorating to validate the objective and prior recognition of DDoS attacks.

2) Traditional denial of service (DoS) attacks primarily abuse network bandwidth around internet subsystems and degrade service quality by generating congestion on the network. The main concern of the DoS attack is to fully interrupt or reduce the available resources or services for legitimate users by malicious users. The distributed denial of service (DDoS) attack is a kind of DoS attack that slows the response of servers to the client or rejects the request of clients. The most commonly initiate DDoS attacks are SYN flood, ICMP flood, DNS amplification, and Smurf attacks in the wire and wireless networks [8]. It can be identified by examining network behavior to discover an infrequent increase in packet transfer speed before services are interrupted.

3) Grasshopper optimization algorithm (GOA) withmachine learning algorithm (GOIDS) is introduced to deal with stagnation issue that is found in the traditional optimization techniques. GOIDS is utilized to provide an efficient and effective global search space for finding the relevant features and afterward apply multilayer perceptron (MLP), naïve Bayes (NB), support vectormachine (SVM), and decision tree (C4.5) as classification algorithms for evaluating the performance of IDS on KDD Cup 99 and CIC-IDS 2017 datasets.

   Begin
   Set the swarm size, *cz*max, *cz*min and
   maximum number of iterations *t*max;
   Randomly generate the population *Y*;
   Estimate the fitness value of each agent;
   T = best search agents;
   While (t < *t*max)
   Update *cz* according to Equation (9);
   For *i* = 1:*n*
   Normalize the distances between Grasshoppers *Y*;
   Modify the current agent *yi* position according to Equation (8);
   end For
   t = *t*+1
   end while
   return *T*
   end

Statistics-Enhanced Direct Batch Growth Self-Organizing Mapping for Efficient Dos Attack Detection[2]

XIAOFEI QU, LIN YANG

1) A new model of the ``statistic-enhanced directed batch growth self-organizing mapping'', renew the definition of the growth threshold used to evaluate/control neuron expansion, and first introduce the inner distribution factor for fine-grained data distinguishing.

There remains a challenge to accurately depict the topology of network traffic data with unbalanced distribution, which deteriorates the performance of *e.g.* DoS attack detection.

2) The denial of service (DoS) attack is arguably the most common network intrusion, which can greatly occupy the resources of legitimate requests and long-term paralyze the network. With the explosive increase of Internet bandwidth and the rapid development of various DoS hacking tools, the frequent DoS attack becomes emerged. In the past decade, various methods of Dos attack detection have been developed, yet suffer from the challenge of data classification for large-scale datasets.

3) SE-DBGSOM Training

1: Initialization: Set the training epochs at 100; Calculate the growing threshold using the training dataset; Optimize the regulation coefficient using the training dataset.
2: **for** *i* D 1 to 100 **do**
3: The growth threshold follows Eq. (5) while other parameters value from Ref. [25]
4: **end for**
5: Return weight vectors and labels for winning neurons

Fine-Grained Classification

1: Initialization: Input testing and training dataset; Calculate IDF for normal and DoS attack data vectors, respectively.
2: **for** *j* D 1 to length(testing dataset) **do**
3: Calculate mean value of all items in each data vector in testing dataset.
4: **end for**
5: **if** the mean value is in-between IDF (DoS attack) **then**
6: This data is DoS attack
7: **end if**
8: Return normal data in testing dataset.

The proposed SE-DBGSOM model is using entire KDD99 and CICIDS2017 datasets.

A Low-rate DoS Attack Detection Method Based on Hilbert Spectrum and Correlation[3]

Dan Tang, Xiaoxue Wu, Liu Tang

1) Correlation-based approach that instead of calculating the correlation coefficient of network traffic sequence directly, it calculates the correlation coefficient of the Hilbert Spectrum of the network traffic. The Hilbert Spectrum, obtained by applying Hilbert-Huang Transform to the network traffic, is an energy-frequency-time distribution which presents more information about the network traffic than raw network traffic sequences. They conduct NS-2 simulations, public dataset experiments to evaluate the performance of the proposed approach.

The periodic mechanism applied by LDoS makes its average attack traffic speed very low compared to DoS attack, which means existing DoS detection methods based on high attack traffic speed are incapable of detecting LDoS attack.
2) Denial of Service (DoS) attack still causes great damage to the Internet in spite of many years' research on its detection and defense. Low-rate Denial of Service (LDoS) attack, a new type of DoS attack, exploits the congestion control mechanism of Transmission Control Protocol (TCP) to degrade the throughput of network by sending periodic pulse attack traffic. In this way, targeted victims constantly go from congestion to recovery or the other way around and thus cannot operate properly and satisfactorily.

3)
```
Start
One Detection Window
Calculate all Hilbert Spectrums
Calculate all Pearson coefficients
Calculate mean value of Pearson coefficients
If mean value < threshold then
The current window is normal
Else
The current window is under LDoS attack
End
```

Machine Learning Based DDoS Attack Detection From Source Side in Cloud[4]

Zecheng He, Tianwei Zhang, Ruby B. Lee

1) DOS attack detection system on the source side in the cloud, based on machine learning techniques. This system leverages statistical information from both the cloud server's hypervisor and the virtual machines, to prevent network packages from being sent out to the outside network. They evaluate nine machine learning algorithms and carefully compare their performance.

These attacks are often sourced from virtual machines in the cloud, rather than from the attacker's own machine, to achieve anonymity and higher network bandwidth. Past research focused on analyzing traffic on the destination (victim's) side with predefined thresholds. These approaches have significant disadvantages. They are only passive defenses after the attack, they cannot use the outbound statistical features of attacks, and it is hard to trace back to the attacker with these approaches.

2) Distributed Denial of Service (DDoS) attacks are attacks targeting the availability of networks, hosts and services from multiple attack source machines. These are some of the most dangerous attacks, especially as they are very easily launched, can cause catastrophic loss of service and are difficult to trace back to the true attackers. Application level DOS attacks disable service by exhausting server resources. These attacks can disable accesses to a single webpage, or to very large servers, e.g. email, DNS or http servers.

3) The cloud has six servers ($S0...S5$) and each server runs multiple virtual machines. In the first experiment, we launch four different kinds of DDoS attacks (SSH brute-force, DNS reflection, ICMP flooding and TCP SYN attacks) on virtual machines from $S0$. The victim is a virtual machine on another server $S1$ running web service. Virtual machines on the other servers (except $S0$ and $S1$) request web service, simulating the legitimate users. In the second experiment, the attacks source from three

virtual machines on *S*0, *S*2 and *S*3 to simulate distributed DoS attacks. The victim is the same virtual machine on *S*1. The defense systems are deployed on *S*0, *S*2 and *S*3. Our experiments are safe since they run behind a VPN router, so the attack packages never escape to the outside Internet.

Low-Rate DoS Attack Detection Using PSD based Entropy and Machine Learning[5]

Naiji Zhang, Fehmi Jaafar, Yasir Malik

1) The algorithm is designed to balance the detection rate and its efficiency. The detection algorithm combines the Power Spectral Density (PSD) entropy function and Support Vector Machine to detect LDoS traffic from normal traffic. In our solution, the detection rate and efficiency are adjustable based on the parameter in the decision algorithm. To have high efficiency, the detection method will always detect the attacks by calculating PSD-entropy first and compare it with the two adaptive thresholds. The thresholds can efficiently filter nearly 19% of the samples with a high detection rate.

The LDoS exploits the vulnerability of TCP congestion-control mechanism by sending malicious traffic at the low constant rate and influence the victim machine. Recently, machine learning approaches are applied to detect the complex DDoS attacks and improve the efficiency and robustness of the intrusion detection system.

2) Distributed Denial of Service (DDoS) attack is a comparatively straightforward yet powerful method to consume network resources and disrupt normal traffic. The attacker performs a DDoS attack by loading the target with a constant flood of traffic, which can consume computing resources and the bandwidth of the network. LDoS exploits the vulnerability of TCP's congestion-control mechanism by sending malicious traffic at the low constant rate and exploits retransmission time out mechanism to reduces the throughput.

3)

```
if entropy >threshold0 then
    Delete() from TestSet
    output normal                    ▷ The threshold0 is for normal
end if
if entropy <threshold1 then
    Delete() from TestSet
    output attack                    ▷ The threshold1 is for LDoS
end if
Scaling(TestSet)
TestSet=PCA(TestSet)                 ▷ lower the dimensions
Setting the classifier               ▷ SVM
Kernel=RBF
predict= SVM.predict(TestSet)        ▷ Prediction with SVM model
count=0
while count<predict.length do        ▷ Output the result
    if predict[count]=0 then
        output normal
    end if
    if predict[count]=1 then
        output attack
    end if
    count++
end while
end procedure
```

TECHNIQUE	ACCURACY	DETECTION RATE	PRECISION
Intelligent evolutionary algorithm	99.96	98.81	98.52
Statistics-Enhanced Direct Batch Growth Self-Organizing Mapping	99.70	99.89	99.85
Method Based on Hilbert Spectrum and Correlation	98.84	99.10	98.8
Machine Learning Based DDoS Attack Detection	94.36	98.3	100
Detection Using PSD based Entropy	98.56	99.19	99

References

[1] Shubhra Dwivedi, Manu Vardhan & Sarsij Tripathi (2020): Defense against distributed DoS attack detection by using intelligent evolutionary algorithm, International Journal of Computers and Applications

[2] XIAOFEI QU 1,2, LIN YANG2, KAI GUO2, LINRU MA2, TAO FENG2, SHUANGYIN REN2, AND MENG SUN (2019): Statistics-Enhanced Direct Batch Growth Self-Organizing Mapping for Efficient Dos Attack Detection, IEEE

[3] Dan Tang, Xiaoxue Wu (2018) : A Low-rate DoS Attack Detection Method Based on Hilbert Spectrum and Correlation, IEEE

[4] Zecheng He, Tianwei Zhang (2017): Machine Learning Based DDoS Attack Detection From Source Side in Cloud, IEEE

[5] Naiji Zhang, Fehmi Jaafar (2019): Low-Rate DoS Attack Detection Using PSD based Entropy and Machine Learning, IEEE