The Prevention of Network Layer DDoS Attack using Hidden Semi Markov Model

Bhavya K[1] Vidhya S[2] Amrutha Jayaraj K[3] Sangeetha K[4]
[1,2,3,4]B.Tech Student
[1,2,3,4]Department of Computer Science & Engineering
[1,2,3,4]Nehru College of Engineering and Research Centre Thrissur, India

Abstract— Distributed denial of service attack is a type of active attack, which causes serious threats to internet. It blocks the sever system by exploiting the resources, so that the server gets overloaded and legitimate users become unavailable to access the services from server. With the growth in technology, the DDoS attackers have improved their sophistication, by automating the attacks. The attackers create the DDoS attack by exploiting the protocol vulnerabilities. The detection of DDoS attack is little bit difficult since they mix with the legitimate packet traffic. The proposed model makes use of Hidden Semi Markov Model (HSMM), an extended version of Hidden Markov Model (HMM). Arrival rate, Service rate and Retransmission Time Out value are considered as the benchmark for differentiating the normal and attacking packets.

Key words: Hidden Semi Markov Model, Network Layer DDoS Attack

I. Introduction

DDoS attacks are executed against websites and networks of selected victims. It is an attempt to make a machine or network resource unavailable to its intended users. This Work is mainly concentrated on transport layer. TCP SYN attack is one of the main security issue in the transport layer. A SYN flood can be considered as a type of DDoS attack in which an attacking system sends multiple SYN requests to the target system so as to consume a large number of system resources in order to make the system unresponsive to normal traffic. The proposed method checks for the SYN flood attack. The propose system is able to detect both low rate as well as high rate attacks. The traffic is monitored, and based on these observations, system tries to differentiate the normal and attacking systems. Since the calculations are done in milli- seconds, the detection and thereby mitigation become much easier compared to the existing systems. Bayesian update is used to update the update the attack predictions regularly. The abnormality in traffic can be identified by considering the mean deviation of entropy value. Entropy can be defined as the degree of disorder. Based on these values, the attack is distinguished from the normal traffic. The mitigation of low rate attacks can be done with help of setting a RTO value. The RTO value will be normally 1, which is set to any random value so that the attackers couldn’t interpret the variations.

II. Existing System

The DDoS attacks remain very crucial problem in cyber security. The detection of these kinds of attacks are somewhat difficult since the attacker make use of some spoofing techniques, which are complicated to identify. Some methods make use of techniques in which the peer nodes can interact with their neighbor nodes to find the trustworthiness in the network. Existing Methods like PAD, MAD, and HAWK methods suffer from processing and memory overhead.

The detection scheme for SYN flooding is divided into 3 categories.

- Statistical analysis
- Router based
- Artificial intelligence

The detection mechanism is based on the protocol behavior of TCP SYN–FIN (RST) pairs, and is an instance of the Sequential Change Point Detection. To make the detection mechanism insensitive to site and access pattern, a non-parametric Cumulative Sum (CUSUM) method is applied.

III. Proposed System

The proposed system can provide an efficient detection of both high rate as well as low rate attacks, and can also mitigate low rate attacks. The HSMM method detects the occurrence of DDoS attack, and RTO randomization process can be used to mitigate the low rate attacks. The observations are done in milliseconds. The attack predictions are updated regularly by calculating the Bayesian update using the probability value of each observation. The method also mitigates the low rate attack by randomizing the RTO value.

IV. Implementation

The proposed system can be implemented in 3 parts which include techniques to mitigate the low and high rate attacks.

1) Attack Identification
2) Low rate attack mitigation
3) Block attack

A. *Attack Identification*

The attack detection part, consider the packet attributes like IP address, time-to-live, protocol type etc. They help to distinguish attacking packets from normal packets. The service rate, arrival rate and response time rate are compared using HSMM[1]. Hidden Semi Markov Model is used to describe the network behavior implementing a TCP three way handshake. The prediction of attack depends on the previous and current state of the observations. The prediction and update detects the attack packet using the HSMM. Entropy of the node TCP flag sequence fitting to the model is used as a criterion to measure the nodes normality.

HSMM is an extension of the hidden Markov model (HMM) with explicit state duration. It is a stochastic finite state machine, specified by (S, π, A, P) where:

- S is a discrete set of hidden states with cardinality N, i.e. $S = \{1,\dots,N\}$.
- π is the probability distribution for the initial state $\pi_m \equiv P_r\,[s1 = m]$, s_t denotes the state that the system

takes at time and m Є S. The initial state probability distribution satisfies $\sum_{m\pi m} = 1$.

– A is the state transition matrix with probabilities: $a_{mn} \equiv P_r[st = n \mid s_{t-1} = m]$, m, n Є S, and the state transition coefficients satisfy $\sum_n a_{mn} = 1$.
– P is the state duration matrix with probabilities: pm (d) ≡ $\Pr[r_t = d \mid s_t = m]$, r_t denote the remaining (or residual) time of the current state st, m Є S, d Є {1,…,D}, D is the maximum interval between any two consecutive state transitions, and the state duration coefficients satisfy $\sum_d P_m$ (d) = 1

The parameter estimation of HSMM can be done by the forward and backward algorithm. We define the entropy of observations fitting to the HSMM and calculate the average logarithmic entropy (ALE) per observation.

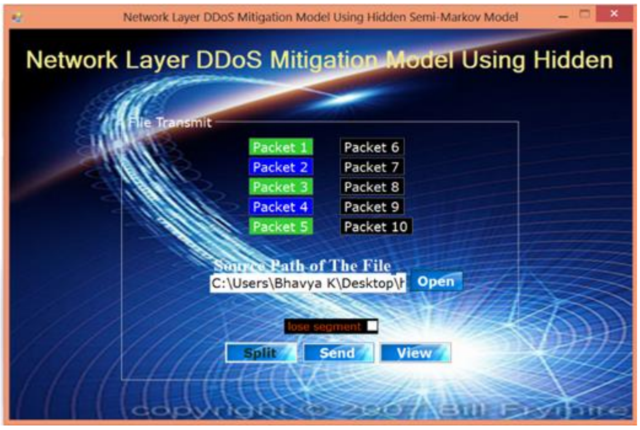
B. Low Rate Attack Mitigation

RTO randomization is used for this task. Normal systems has RTO value set to 1sec. Attackers try to exploit this standard value. Thus if this value is set to some random value it will be difficult for the attacker to find out the next value. This would ultimately help to control the attack rate. Hence using RTO randomization the low rate attacks which solely depend on the RTO value for the attack can be controlled to an extent.

C. Block Attacks

The blocking of attacks is based on the attack identification and RTO randomization outcomes. The high rate attacks are identified at the first stage and RTO randomization detects the low rate attacks. Then the behavior of the nodes can be evaluated. Based on these, the arriving packets can be identified as attacking packets or normal packets. Then the attacking packets are blocked. This technique provides a sophisticated method to mitigate the low rate attack better than the existing methods

V. RESULT AND DISCUSSION

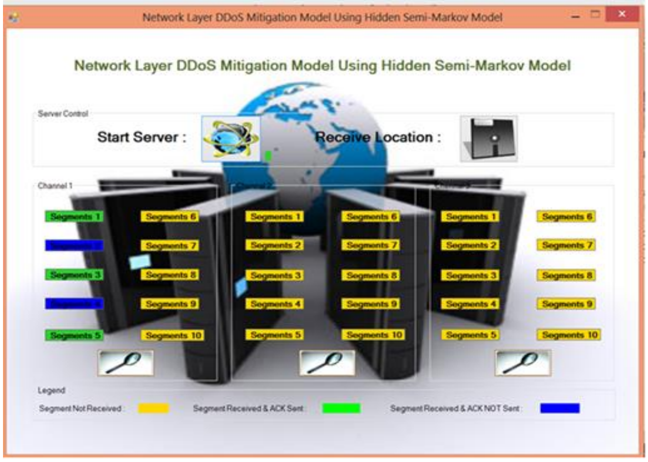


Network Layer DDoS Mitigation Model Using Hidden Semi-Markov Model

Network Layer DDoS Mitigation Model Using Hidden

Fig. 1: Client Form

Fig.1 shows the client side. The client first selects the file for transmission. The data within the file are got split as different packets, normally 10. After clicking the send button, the packets are transferred to the server side. The normal packets are shown in green color, whereas the attacking packets are indicated using blue color. The attack from the packets are then removed, and finally indicated in green color.



Network Layer DDoS Mitigation Model Using Hidden Semi-Markov Model

Network Layer DDoS Mitigation Model Using Hidden Semi-Markov Model

Fig. 2: Server Form

Fig.2 shows the server side. The status of packets which got transferred from different clients can be seen. The time at which the packets received can be obtained by clicking the lens in the picture. The behavior of each node is analyzed using HSMM. The parameters such as arrival rate, service rate, response time rate are calculated and compared with normal nodes using this model. The prediction and update are done constantly to find the unknown state of the node. This gives us the clear indication that there are number of half open connection in the server based on this detection of the attack packets can be found. Then the blocking of attack packets from attacking nodes takes place.

VI. CONCLUSION

Complete implementation of DDoS mitigation using hidden semi-Markov model has done successfully without any complication. C# is used for coding of the project. The most notable characteristic of HSMM is that it can be used to describe most physical signals without many hypotheses. Furthermore, the non-stationary and the non-Markovian properties of HSMM can best describe the self-similarity or long-range dependence of network traffic that has been proved by vast observations on the Internet, which quite benefits the study. The prediction and update detects the attack packet using the HSMM. Entropy of the node TCP flag sequence fitting to the model is used as a criterion to measure the nodes normality.

The HSMM detection is accurate, since it detects the arrival rate of the packets in milliseconds. Parameters like arrival rate, service rate are taken for the detection of DDoS attack. Based on the detection, IP addresses which goes beyond the threshold limit is blocked. The RTO randomization is used to mitigate the low rate attack and detect high rate attack precisely.

VII. FUTURE SCOPE

Future work intends to improve the work on avoidance of attacker packets by using its variation in threshold level using Trust. The detection of even high rate DDoS attack can be done. The prevention of such high rate attacks can be done only up to an extent. In future, the system functions can be extended so that, even high rate attacks can also be detected and prevented and thus completely eradicate DDoS attacks.

REFERENCES

[1] T. V. Duong, H. H. Bui, D. Q. Phung and S. Venkatesh, “Activity recognition and abnormality detection with the switching hidden semi-Markov model,” Computer Vision and Pattern Recognition, CVPR 2005, IEEE Computer Society Conference, June 2005.

[2] P. Efstathopoulos, “Practical study of a defense against low-rate TCP-targeted DoS attack,” Internet Technology and Secured Transactions, ICITST 2009, International Conference, November 2009.

[3] N. A. Noureldien and M. O. Hussein, “Block Spoofed Packets at Source (BSPS): A method for detecting and preventing all types of spoofed source IP packets and SYN flooding packets at source: A theoretical framework,” Applications of Digital Information and Web Technologies, ICADIWT '09, Second International Conference , August 2009.