CHAPTER 7

CONCLUSION

In this work, Application Service Network Request Identification (ASNRI) technique has been implemented. It first identifies the service requests made by the users. After receiving the request, the ASNRI technique classifies the IP and MAC streams separately. Then it has the interaction with the IHBCM, to evaluate the request which is raised by legitimate or malicious user. If the request is malicious, then it is filtered by the respective filters for identifying and restricting App-DDoS attacks to be convinced further in the internet application servers.

App-DDoS attack mitigation is done by the Trust and AM based HMM with traffic flow filters. It allows service providers to protect the legal broadband subscribers and enterprises against App-DDoS attacks.

The measurement of resisting App-DDoS attacks requires monitoring dynamic and static objects of the network activities, and to obtain significant information in a timely manner. The proposed IHBCM with Gaussian distribution factor is introduced in the detection architecture to monitor web traffic in order to reveal dynamic shifts in normal burst traffic. It indicates the onset of App-DDoS attacks during the flash crowd event. Bayesian factor reveals early attacks merely depending on the document popularity obtained from the server log.

The simulation experiment is conducted with different App-DDoS attack nodes like constant rate attacks, increasing rate attacks and stochastic pulsing attack. For the simulation purpose, the flash crowd network traffic data are traced from an ISP. The simulation results show that the system captured the shift of web traffic caused by attacks under the flash crowd. In entropy, the abnormality of observed data is measured by Bayesian distribution factor.

The performance evaluation of ASNRI technique is simulated in wired and wireless topology with true positive, and true negative rates of request identification.
ASNRI technique captures the App-DDoS attack characteristics of the internet traffic stream, and filters it with IHBCM and makes the application render valid, authenticates the legitimate users and provides uninterrupted services to them. The true positive rate is comparatively higher for ASNRI technique compared to the conventional wired and wireless DDoS attacks resistance methods. The true negative rate is found to be minimized in ASNRI when compared with the earlier techniques.

In experiments, when the detection threshold of entropy is set to 4.82, the detection rate is 93% and the false positive rate is 0.78%. The proposed architecture monitors the App-DDoS attacks, and performs more dedicated detection on victim network.

The load variance of application servers are maintained at bay, and throughput of the rendered services are at higher levels of 43%, which is better than the existing DDoS attack resistance schemes. In addition, the response time of the ASNRI technique shows incredible improvement of nearly 94% compared to other resistance schemes.

7.1 Limitations of Proposed Work

HMMs are well described only for the function of a distinct independent variable. In this model, after filtering the data traffic, it needs to be stored as a vector or file. Each data stream is in need of large vector size for storage. Even though HMM is found to perform better, further improvement is needed to store the gradually increasing rate attacks in the traffic. HMM has been organized with state transition probabilities, which are dependent only on the preceding states. Due to this reason, the HMM seems to be unrealistic for many real world applications. Hence, higher-order dependencies in the transition behavior can direct to further improvements in the recommendation. The number of states in the HMM desires to be preset for a particular application.

ASNRI technique omits the time that the user stays on a page, and it does not consider the hyperlinks provided by the current page. The other issue of this technique is, it does not have the capability to identify the proxies’ replies for legitimate users’ HTTP
requests. In addition, when the total number of pages in the website is very big, the algorithm would be too difficult to be implemented in online detection of App-DDoS attacks.

**7.2 Scope for Future Enhancement**

Due to the limitations of the HMM model, the enhancement of the work is needed for ASNRI technique. So instead of HMM, the ASNRI technique can be designed to have communication with artificial neural networks using genetic algorithms. With this integration, higher discriminative and training performance can be achieved. It also allows different numbers of states to evolve.