Chapter 9

CHALLENGES AND FUTURE WORK

The model is simple and light weight in terms of detection, but while the design has been made keeping in mind flooding attacks (which form most of attacks carried out to the day), input parameters may have to be further fine tuned in order to be detecting convincingly a broader class of DoS attacks. This may involve including payload features as well. Also, at a user level, making the choice of some inputs to the system is very difficult even for an expert user. For example, it may be extremely difficult for even a seasoned network administrator to determine the right choice for the proportion of abnormal traffic in the training input, unless manual checking is done over the entire dataset.

Further more, the scalability of the model to very high volume servers has to be examined. For example, it is quite possible to see a window full of SYN packets with a high volume server, while the signature for SYN flooding attacks still remain the same. Although it may look like increasing the size of the window may solve this problem, this has to be carefully examined before a conclusion could be given. This essentially calls for testing the system with variety of traffic at various volumes.

Outside of the detection problem itself, a few other interesting areas of research surface when the intention is to build a fool proof DDoS protection system. Some of them are the following:

• Extending to other protocols. While we believe that a similar framework will work for other protocols, the research could be extended to include other protocols in the Internet protocol stack. Examples of such protocols include gateway level protocols, or application level protocols.

• Research on sound mitigation techniques. It is also to be noted that these techniques in many cases may have to be applied in-line, which calls for extremely efficient methods to handle attacks. Possible mitigation techniques include graceful degradation, cryptographic methods to stateless monitoring and making launching further attacks tougher.