ABSTRACT

Today’s world is highly dependent on the internet. And like any other information and communication system the users of the internet, while enjoying it’s services, also suffer from it’s vulnerabilities. This defenselessness of the internet is because of it’s open architecture and protocol stack. One of the most damaging and ever changing amongst it’s vulnerabilities is degradation in it’s quality-of-services due to Distributed-Denial-of-Service (DDoS) attacks. DDoS attacks are easy to launch because of the weaknesses of the TCP-IP protocol stack. The attackers make use of automatic programs, bots, to launch distributed attacks from compromised machines and harm the services of legitimate users. Consequently, it is critical to study DDoS attacks and develop techniques for fast, accurate and reliable detection of these attacks. One particular challenge faced by the researchers in detecting anomalies like illegitimate DDoS attacks is that they have close resemblance to legitimate anomalies like flash crowds.

Recently, anomaly-based signal processing techniques like wavelet transforms, entropy measurements and spectral analysis, due to their abilities in point change detection and data transformation, have been used to study network traffic behaviour. Scale-invariance is one such feature of the network traffic that has been worked upon by the researchers to model the network traffic behaviours. We, in this thesis, have used scale-invariance of the network traffic to address the challenge of detection of old and new breeds of rate based anomalies. The work presented in this thesis therefore makes few contributions.

The first contribution is to provide a collaborative solution for detection and classification of DDoS attacks. The second contribution is to detect and differentiate DDoS attacks from flash crowds. The third contribution is to explore self-similarity as a property of scale-invariance for detection of DDoS attacks. Fourth and last contribution is development of a visualizer for locating anomalies.