THESIS ABSTRACT

DDOS DETECTION AND MITIGATION USING MACHINE LEARNING

By

ARPIT RAMESH GAWANDE

Thesis Director:

Dr. Jean-Camille Birget

Distributed Denial of Service (DDoS) attacks are very common these days. It is evident that the current industry solutions, such as completely relying on Internet Service Provider (ISP) or setting up DDoS defense infrastructure, are not sufficient in detecting and mitigating DDoS attacks, hence consistent research is needed. Most of the current industry solutions involve setting up a centralized expensive hardware system which can analyze the data packets for probable DDoS attacks, but those solutions use different protocols to transfer the attack information between the detection system and the router, limiting the scope of DDoS attack detection systems. In this paper we have discussed a way to detect DDoS attacks using machine learning tools at the routers, instead of setting a centralized analysis system. We have also proposed a standard communication architecture which can be used across all the networking devices for mitigating DDoS attacks.