DETECTION OF DDoS ATTACKS USING SOURCE IP BASED ENTROPY

JASWINDER SINGH[1], MONIKA SACHDEVA[2]& KRISHAN KUMAR[3]

[1]Assistant Professor at GTBKIET, Chhapianwali District, Mukatsar, Punjab, India

[2]Associate Professor at SBSSTC, Ferozepur District, Ferozepur, Punjab, India

[3]Associate Professor at PTU Main Campus, APIT, Kapurthla District, Jalandhar, Punjab, India

ABSTRACT

There are about nine hundred million people, who use internet now-a-days. They use the internet to communicate with each other and all over the world, business-men can do their work over the internet, and there is much more to it. In a nutshell, the world is highly dependent on the Internet. Therefore, the availability of internet is very critical for the socio economic growth of the society. One of the major security problems in the current Internet, is the denial-of-service (DoS) attack always attempts to stop the victim from serving legitimate users. Denial-of-service (DoS) and distributed-denial-of-service (DDoS) attacks cause a serious danger to Internet operation.

An important method for stopping DDoS attacks is to detect attackers and handlers. Detection of DDoS attacks is a challenging problem for network security. In this paper, the proposed work aims at detecting DDoS attacks in the network using Entropy Based Anomaly Detection Algorithm. The value of entropy is calculated with respect to time and packet windows. The results indicate that during normal activity i.e. only legitimate traffic is flowing, value of entropy lies in a narrow range but in case of attack, it increases or decreases considerably. So, attack can easily be detected.

KEYWORDS: DoS, DDoS, Availability, Entropy, Detection