Systematic literature review and taxonomy for DDoS attack detection and prediction

ABSTRACT

Distributed denial of service (DDoS) attack has been significantly discussed in the computer security domain, particularly due to the damaging effects it causes to organisations' assets. However, it confronts the challenge under massive growth of internet user traffic and lightning speed of computer access. In this paper, we present a comprehensive systematic literature review and measurement analysis of the DDoS impact, including: a) DDoS definition; b) types of DDoS attack; c) various types of existing DDoS detecting techniques; d) different kinds of DDoS attack prediction techniques.Furthermore, this paper provides an in-depth analysis the advantages and the drawbacks of existing DDoS detection and prediction technique to assist for both academia and industry researchers towards produce better DDoS detection and prediction mechanism.

Keyword: Metadata; Distributed denial of services attack; DDoS; Intrusion detection system; DDoS attack prediction