©2010 International Journal of Computer Applications (0975 - 8887)
Volume 1 – No. 19

Resistance against Distributed Denial of Service Attacks (DDoS) Using Bandwidth Based Admission Control

V.Shyamala Devi
Research Scholar
Asst.Prof Dept of IT
K.S.R.C.T, Tiruchengode

R.S.D. Wahidabanu
Research Supervisor
Prof/Head Dept of ECE
Govt.College of Engg.Salem

Dr.K.Duraisway
Dean Ac
K.S.R.C.T
Tiruchengode

ABSTRACT

Internet hosts are threatened by large-scale Distributed Denial of- Service (DDoS) attacks. The Path Identification DDoS defense scheme has recently been proposed as a deterministic packet marking scheme that allows a DDoS victim to filter out attack packets on a per packet basis with high accuracy after only a few attack packets are received. The previous work suggested depicts the Stack Path identification marking, a packet marking scheme based on path identification, and filtering mechanisms. To circumvent detection, attackers are increasingly moving from floods to attacks that mimic the behavior of a large number of clients, and target expensive higher-layer resources such as CPU, database and disk bandwidth. The resulting attacks are hard to defend against using standard techniques, as the malicious requests differ from the legitimate ones in intent but not in content. The proposal in this work improves our previous path identification scheme to protect network servers against DDoS attacks that masquerade the crowds. It provides rate filter authentication using verifiers different from other systems by using an intermediate stage to identify the IP addresses that ignore the verifier, and persistently bombard the server with requests despite repeated failures. Once these machines are identified, it blocks their requests, and allows access to legitimate users. It protects the authentication mechanism from being DDoS attacks and integrates filter authentication with bandwidth admission control. Rate limitation implies that a peer must reject or even drop some incoming requests.

The proposed bandwidth admission control strategy discriminates against the attrition adversary by selectively dropping the requests for attacker legitimacy. Admission control strategies have been used even in circumstances that includes session-based classification (e.g., in web services, preferentially drop requests signifying a new service session, instead of requests that continue longer running sessions with greater potential for a purchase), and reputation-based classification (prefer requesters with a good subjective or global history). Knowing that the admission level is a relative measurement, the component of the control scheme is made adaptive according to the rate limit filter and parameter such as session time, bandwidth level, load demand etc., When the admission level of the bandwidth is used as a DDoS detection indicator for sources, and also achieve similar performance with some expected slight degradation in stability. It is well known that delay is a major concern for any feedback control systems and tested the effect of delays as well. It was found that the control performance remains highly stable when the delay is as high as one second or more.