

**CHENNAI – PONDICHERRY**

**A COLLABORATIVE DDOS DEFENCE FRAMEWORK USING NETWORK FUNCTION VIRTUALIZATION**

**Abstract:**

High-profile and often destructive distributed denial of service (DDoS) attacks continue to be one of the top security concerns as the DDoS attacks volumes are increasing constantly. Among them, the SYN Flood attack is the most common type. Conventional DDoS defense solutions may not be preferable, since they demand highly capable hardware resources, which induce high cost and long deployment cycle. The emerging of network function virtualization (NFV) technology introduces new opportunities to decrease the amount of proprietary hardware that is needed to launch and operate network services. In this paper, we propose a DDoS defense mechanism named CoFence, which facilitates a “domain-helps-domain” collaboration network among NFV-based domain networks. CoFence allows domain networks to help each other in handling large volume of DDoS attacks through resource sharing. Specifically, we design a dynamic resource allocation mechanism for domains so that the resource allocation is fair, efficient, and incentive-compatible. The resource sharing mechanism is modeled as a multi-leader-follower Stackelberg game. In this game, all domains have a degree of control to maximize their own utility. The resource supplier domains determine the amount of resource to each requesting peer based on optimizing a reciprocal-based utility function. On the other hand, the resource requesting domains decide the level of demand to send to the resource supplier domains in order to reach sufficient support. Our simulation results demonstrate that the designed resource allocation game is effective, incentive compatible, fair, and reciprocal under its Nash equilibrium.