accidental or deliberate overload without also compromising network performance.Techniques include enforcing policies for resource consumption and providing backup resources available on demand.In general, there are four lines of defense against DDoS attacks [PENG07, CHAN02]: o Attack prevention and preemption (before the attack): These mechanisms enable the victim to endure attack attempts without denying service to legitimate clients.RFC 2827, Network Ingress Filtering: Defeating Denial-of-service attacks which employ IP Source Address Spoofing,8 directly makes this recommendation, as do SANS, CERT, and many other organizations concerned with network security.The provision of significant excess network bandwidth and replicated distributed servers is the usual response, particularly when the overload is anticipated.Hence one of the fundamental, and longest standing, recommendations for defense against these attacks is to limit the ability of systems to send packets with spoofed source addresses.This type of filtering can be implemented using explicit access control rules in a router to ensure that the source address on any customer packet is one allocated to the ISPIn addition, prevention mechanisms modify systems and protocols on the Internet to reduce the possibility of DDoS attacks.These either obscure the originating system of direct and distributed DoS attacks or are used to direct reflected or amplified traffic to the target system.This is regularly done for popular sporting sites.