(1) What is the primary difference between “flash crowds” and “flooding DoS attacks”?

intention

(2) What is the most popular solution to cope with flash crowds?

load-balancing over CDNs (or clouds)

(3) Mention one example for the known flooding attacks that target:

(destination hosts) x (software) x (application processes)

Example: “F5 attacks” (other examples are possible)
(4) Why are “DNS-amplification DoS attacks” a popular attack now?

DNS-amplification attacks have recently become popular: personal wireless routers (or access points) are popularly used, but many of them are owned by non-technical users, who do not properly set up their personal wireless routers, letting a DNS server in such wireless routers wide open to attackers.

As soon as attackers tap into “DNS hierarchy”, attackers can abuse other, properly protected DNS servers. Thus attackers easily abuse the existing DNS servers, as long as they can find unprotected wireless routers.

(5) “Cloud Computing” has become a double-edge sword for security administrators to cope with DoS attackers. Explain how (why) is “cloud computing” a good defending tool to security administrators (i.e., defenders). Explain how(why) is “cloud computing” a good offending tool for DoS attackers.

Security administrators can load-balance incoming traffic to clouds especially when flash crowds hit their servers, at the same time DoS attackers also can use clouds to amplify their attacking traffic to specific targets using clouds.