Mitigating Network Resource Abuses and DDoS Attacks with Client Puzzle based Software-Defined Networks

Zhang Liu(student)
zhang.liu@colorado.edu

Eric Keller
eric.keller@colorado.edu

Sangtae Ha
sangtae.ha@colorado.edu

University of Colorado Boulder

1 Motivation

Network resource abuses and distributed denial of service attacks have been troubling network operators and resource owners for a long time since the advent of Internet. The main reason that they are popular among attackers is because they are lucrative activities. Traditional countermeasures are usually deployed in the last mile access network close to the victim and using complex filters and dedicated machines to identify attack traffics from legitimate ones. This type of approaches has two flaws. First, they are not very adaptive to future attacks. Policies are made based on observations of previous attack patterns, as long as there are policies, attackers can always find a way to circle around it. Second, even when the victim is saved during attacks, huge amount of network resources are still wasted by the attacking traffics along the route.

2 Client Puzzle SDN

Our proposed system is a first attempt to integrate Client Puzzles with software defined networks to mitigate network resource abuses and DDoS attacks right at the edge of the network. The main idea is that when the network resources are depleting, the cost of attacking them should increase exponentially to prevent the resources from total depletion. The exponential cost function will also render such attacks not lucrative anymore which will force attackers to drop this kind of attacks.

The system architecture is shown in Figure 1. SDN switches can also act as abnormal load detectors. When they detect higher than normal load, they will inform the situation to the SDN controller together with all flows associated with the load. The SDN controller will identify the source of these flows and push out Client Puzzle requests to corresponding edge switches. The edge switches will carryout actual Client Puzzle challenges with the end hosts associated with the flows. The hosts are required to solve a CPU/memory bound mathematical problem each time they want to send a packet to the scarce resources and include the answer in the IP packet header option field. The edge switch will check whether the answer is legitimate before forwarding the packet to the destination. The difficulty of the Client Puzzle will increase according to the scarcity of the resource affected.

The first benefit of our system is that attackers and legitimate users are treated equally such that there are no policies for attackers to circle around. The second benefit is that attacks and abuses are stopped right at the edge of the network, resources along the original attack paths are all saved. The third benefit is that hosts have to take responsibility of flows generated, botnet computers can be easier to identify due to abnormal CPU/Memory usages involved with Client Puzzle, this will also increase the cost of carrying out such attacks.

The challenge of our system is that SDN switches need to have a small control plane enabled to provision Client Puzzles and verify corresponding answers. This should be the trend of future SDN since switch hardware supports it and enable some degree of control plane will support more applications that can utilize more potentials of software defined networking.

The poster will demonstrate the preliminary simulation results and findings of our system which shows its feasibility and potentials. The future of this project will involve quantifying how much difficulty can be introduced to attackers and how the system performs in large and realistic environments.

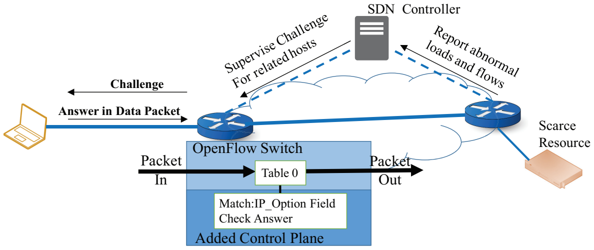

Figure 1: System architecture.