THE USE OF CONGESTION PARTICIPATION RATE (CPR) TO DETECT LOW-RATE DDoS ATTACK

Abstract

Low-Rate DDoS (LDDoS) is one of DDoS variation that send less packet than conventional DDoS attack. However, by sending less packet and using unique attack period make LDDoS very effective to lower the quality of a service that rely on network because of overload access on the network. With the unique characteristic, LDDoS is harder to detect because it have no big difference with normal access. It is easy for LDDoS attack to assimilate with normal access because both of it have simmilar access intensity.

The use of congestion participation rate (CPR) to detect LDDoS attack is based on the intensity calculation of the packet flows that going through the router while congestion occured. Each flow being grouped into group flow. Group flow membership is based on the similarity of IP destination, port destination, period, payload, start time, and protocol. The group flow access intesity percentage is become the main parameter to determine whether that group is classified into LDDoS attack or normal access.

The implementation of CPR to detect LDDoS is done by creating a system on router that can conduct packet monitoring.
sniffing, and identification. The identification result is presented by a log that contain the recapitulation result of each group flows.

After conducting some functional and performance testing with the system, it can be concluded that CPR is quiet effective to identify LDDoS attack that based on TCP protocol. But, everyone who want to implement CPR for LDDoS identification must be aware with the router utility and performance, especially with RAM utility.

**Keyword: CPR, LDDoS, Network Congestion**