

DDoS Detection in Software Defined Networking

The project is divided into three phases:

1. Collection Phase :

This phase is concerned with the collection of data whenever any PACKET_IN message arrives at the controller. The action related to this phase is implemented in the CDM class. The CDM class implements **IFloodlightModule**, **IOFMessageListener**. The receive() function listens to the PACKET_IN message.

2. Detection Phase:

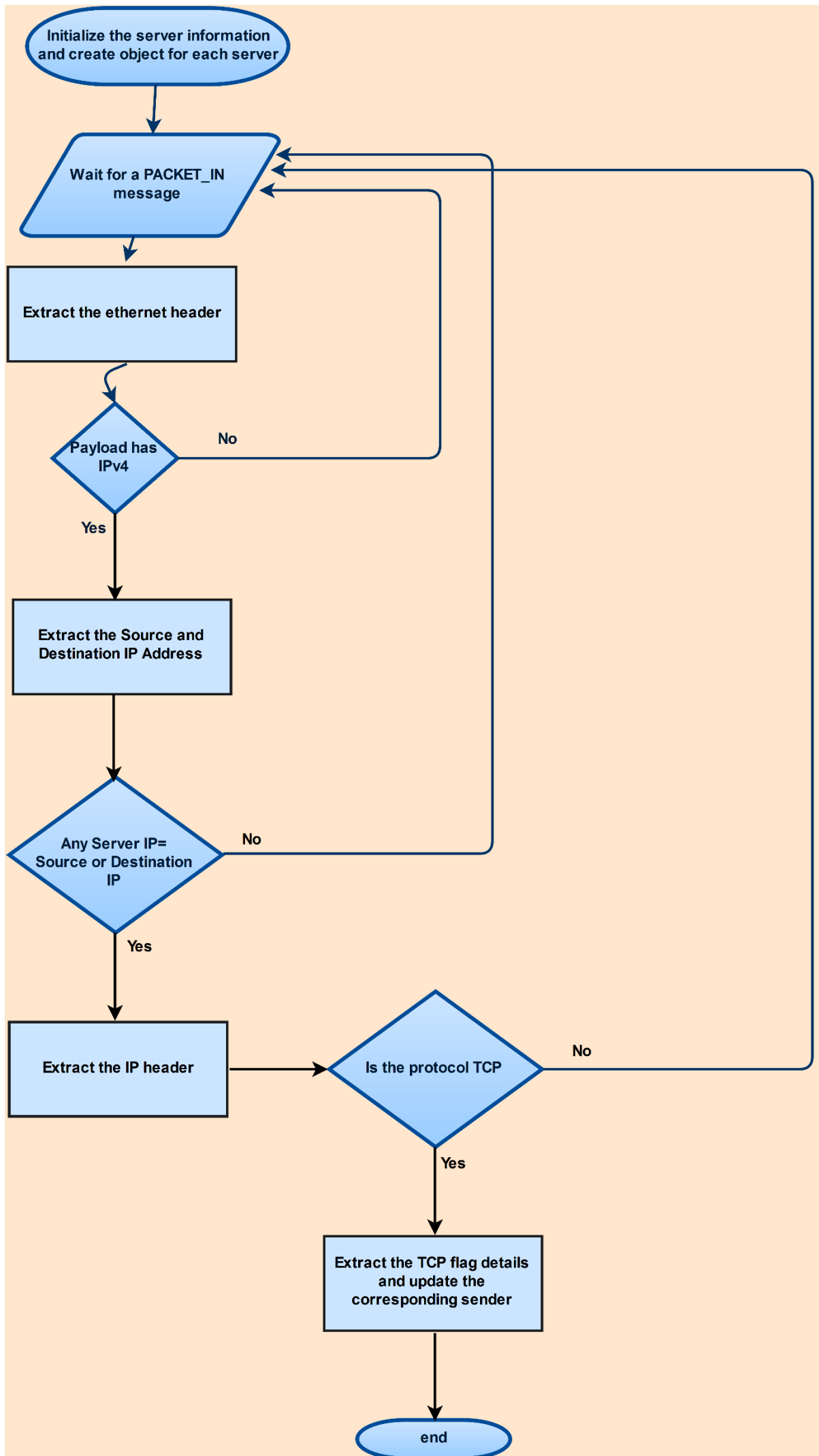
In the detection phase, the detection algorithm is run over the data collected during the collection phase for a period of 15 seconds. After every 15 seconds this cycle repeats. For creating thread the CDM class also implements **runnable** interface.

3. Mitigation Phase:

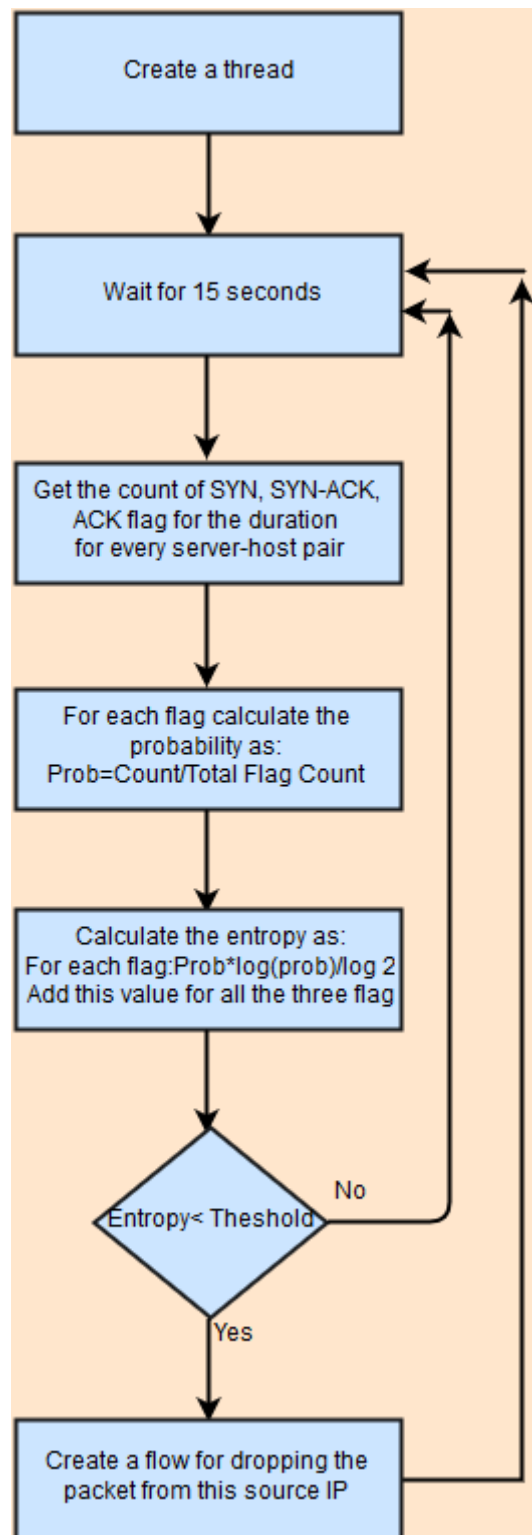
If any attack is detected in detection phase, then the mitigation phase works. The mitigation phase uses **FlowEntryPusher** Service for blocking any traffic at the switch.

The detailed flowcharts for working of all the phases are given below.

The first one is for collection phase.



This flowchart is for the detection and mitigation phase.



The network used for the demonstration purpose:

In the network server IP is 10.0.0.1.

Host h2, h3 are the attacker node and the host h4,h5 are normal user.

