**Summary of “DDoS Attack Detection under SDN Context”**

**Name:** Avineet Kumar Singh

**ID#:** M12135865

**Abstract.** Software Deﬁned Networking (SDN) is a new network management platform. Its centralized control architecture presents many new opportunities among them utilization of SDN for network measurement is considered the most important one. As most of the applications are running online frequency of DDoS attacks has become higher. So, detection of Distributed Denial-of-Services (DDoS) attack quickly and precisely is a very challenging problem. In this paper author proposes methods to detect DDoS attacks leveraging on SDN’s ﬂow monitoring capability which are Sequential and Concurrent. It utilizes measurement resources available in the whole SDN network to adaptively balance the coverage and granularity of attack detection. The methods capture the asymmetry feature of DDoS attacks to achieve higher detection accuracy. These methods can quickly locate potential DDoS victims and attackers by using a constrained number of ﬂow monitoring rules. Two proposed methods are compared based on performance and applicability under different TCAM (Ternary Content Address Memory) size limits. If the TCAM capacities are pretty large, Concurrent Method is more preferable, as it can quickly find the victims along with the attackers. On the other hand, if the TCAM capacities are very constrained, it is likely that the Concurrent Method will exit at a very coarse observation granularity, while at least the Sequential Method can pinpoint the victims precisely. Self-Organizing Mapping (SOM) is used as DDoS attack detection classiﬁer.

**Contributions.** In this paper author tries to capture traffic rate deviation/asymmetry to achieve higher detection accuracy as previous papers only discussed inflow and outflow of the network.

Also, the authors coordinate monitor rule placement on all switches to efficiently utilize all TCAM entries available in the whole network to maximize the coverage and minimize the granularity of detection.

**Weaknesses.** The weakness of the paper is that the proposed methods require a large amount of data storage which is difficult to manage in case of memory limited devices and the OpenFlow creates vulnerabilities for network attacks especially Distributed Denial of Service (DDoS).