Section 1: Week 2: SDN Problem Statement

Nate Bachmeier

TIM-7010: Computer Networking and Mobile Computing

July 7th, 2019

North Central University

# QoS in Software Defined Networks

Software Defined Networking (SDN) represents the next evolutionary step in network design. This is accomplished by a clear separation of application, control, and data planes; such that (1) hardware switches are reduced simple packet forwarding devices; (2) viewing and modifying the network configuration is standardized across vendors; and (3) general purpose programming languages can register for networking events across the pipeline. Having these capabilities enables networks to be highly dynamic and reactive to issues impacting the Service Level Agreements (SLA).

An open research area within software defined networks is mechanisms for increasing the supportable size of Policy Based Routing (PBR) on the Open Flow Tables. This is caused by the finite availability of Ternary Content-Addressable Memory (TCAM) on the physical networking devices (Shood, Yu, & Xiang, 2006). If these tables are unable to continue growing at a sustainable rate this will lead to challenges managing large scale dynamic networks, due to an expected explosion in both legitimate (e.g. IIoT and 5G) and malicious traffic (e.g. DDoS).

It is well publicized that the rise of Industrial Internet of Things and 5G wireless are expected to cause a 1000-fold increase in the number of connected devices (Petel, Ali, & Sheth, 2018) (Frodigh, 2018). Each of these devices will need to be registered within the OpenFlow switches as a requirement to correctly route the last hop. In high traffic areas, such as convention centers or autonomous factories, these wireless devices will roam about the premise. This adds further load across multiple physical switches as they must cache the policy for devices that are likely to return soon.

It is also well publicized that Distributed Denial of Service attacks are continuing to grow in frequency against enterprises. Akamai Technologies is responsible for the management of Global Content Delivery Networks (CDN); they have reported an annualized increase in attacks at 60% (Singh, Singh, & Kumar, 2017). A literature review suggests that many businesses expect to leverage software defined networking solutions as their mitigation strategy. However, these studies are (1) based on small simulated data sets; (2) addressed only half the scenario; and; (3) ignored the scalability concerns of granular policy requirements.