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).

## What is TCAM

A commodity workstation using Random Access Memory (RAM) and requires the application to provide an *address* to retrieve the *content*. Networking equipment has the opposite requirement as the packet contains the destination’s virtual IP (content) and needs to be mapped to a virtual switch port (address).

Ternary Content-Addressable Memory (TCAM) addresses this requirement by allowing each bit in the content to represent states (a) on; (b) off; or (c) doesn’t care about ‘x’. Due to the wildcard nature, lookup tables can be queried in parallel and network masks applied in a single clock cycle (Ullah, Ullah, Afzaal, & Lee, 2019).

The amount of TCAM on a device is limited due to (1) the chips are expensive to produce; (2) requires significant power for complex circuits; (3) required power consumption emits large amounts of heat; and (4) the complex circuitry reduces amount of memory that can be placed per square centimeter.

According to Ullah et al, a typical chip contains on the order of 1000 x 144-bit words. This is enough for traditional static networks but will limit innovation as competing consumers fight for these finite resources. The number of words does not directly map to the number of consumers, as filter policies can be implemented by vendors as multiple ‘allow’ and ‘drop’ actions requiring additional entries.

To partially mitigate the scenario vendor’s have introduced the notion of ‘Flow Groups’ as a mechanism to group multiple flows into the same policy entry. However, many business-critical scenarios such as DDoS mitigation and ensuring QoS will require more fine-grained policies.

# Influence of Legitimate Traffic

It is well publicized that the rise of Industrial Internet of Things (IIoT) 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.

For many scenarios of the Industry 4.0 movement having mechanisms to ensure Quality of Service are required for safety reasons. Frodigh used a contrived example with a balancing robot that relied on external network services for calibration information. As he talked, the network signal was increasingly delayed causing the robot to drunkenly wobble. Eventually the robot tipped over representing cataphoric failure.

These scenarios can be mitigated by either undersubscribing the networking gear or using more granular priority policies. As the size of the network increases it becomes prohibitively expensive to undersubscribe networking equipment (Jain et.al, 2013). These policies will need to correctly handle network attack scenarios and maintain continuity of core business services.

# Influence of Malicious Traffic

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.

## Understanding DDoS Scenarios

A Denial of Service (DoS) attack occurs when a malicious actor performs some action on a resource with the goal of preventing another user from accessing it. A Distributed Denial of Service (DDoS) occurs when a malicious actor uses multiple intermediaries to perform the action against the resource.

There are two broad categories of DDoS attacks (a) Network Level and (b) Application Level. Attacking the networking level is often easy to detect because of the sheer volume and statistically anomalous packet headers. Application level is harder to distinguish as its mixed with legitimate traffic and flows into every corner of the network. Typically, when an application is attacked the goal is to (1) flood a request queue; as (2) a mechanism to consume all processing threads which (3) delays other requests to that same queue.

## Challenges from Limited Data Sets

It is well publicized that server providers are unwilling to share their network traces of DDoS attacks with researchers, as they are concerned about the privacy of their users. This has resulted in most researcher operating on limited data sets or simulated traffic across small Local Area Networks (LAN) (Prasetiawan, Abdurohman, & Yulianto, 2017).

Without the availability of high-quality data sets researchers have focused on statistical models for detecting networking level DDoS scenarios. Many of these models are tweaks to Feinstien’s 2003 solution that relies on simple Chi-Squared Tests. Li et al demonstrated that using a Long-Term Short-Term (LTSM) neural network could boost the detection confidence to nearly 99%.

After the network level attack is detected, resiliency strategies, such as deploying virtual network functions (VNF) (e.g. firewalls), can mitigate the issue at the edge and largely solves the problem (Shood, Yu, & Xiang, 2006).

## Challenges in Managing Application Level Attacks

In contrast, application level attacks have been ignored or addressed with impractical solutions. Singh et al.’s survey identified multiple publications that relied on headers inspection of HTTP GET Requests to confirm that the user-agent was a human. Others have proposed that the requiring the client supports JavaScript. Ultimately any solution the relies on data provided by the client (or through obscurity) will never secure.

Others have proposed very naïve solutions such as if an attacker requests a single page at maximum bandwidth until the end of time. In the limited amount of data available there is already significant evidence this is not how Advanced Persisted Threats (APTs) attack enterprise environments.

Unlike Network Level attacks, Application Level occur after the edge while interacting with internal systems. Modern microservice designs can further hide these traffic patterns as services cascade calls to other services. Detecting these situations require a holistic view of the entire network, like the vantage point available to the SDN controller.

When an attack is detected the controller needs to remediate all flows that under control of that specific individual user. Presently, the OpenFlow policies are too coarse and would target a group, such as throttling all users of the web application. Effectively such a remediation policy is performing the denial of service *for* the attacker!

Authoring policy to be more granular level does not work scale as the attack is distributed in nature. Eventually the OpenFlow tables will become saturated as it is a finite resource, Quality of Service will not be guaranteed, and then the robot tips over.

# Alternative Solutions

## Systems based on Traditional Networking

Businesses today address these challenges through (1) provisioning excess network capacity; (2) deploying Web Application Firewalls; and (3) assuming it will not happen to them (Singh, Singh, & Kumar, 2017).

Provisioning additional capacity can be in the form of segmented networks that are air-gapped from attackers. However, anyone that has worked in distributed systems can attest that bad patches can result in similar levels of chaos. If the system is unable to detect and quarantine the misconfigured devices, they will degrade the overall health of the topology.

Web Application Firewalls can detect a subset of malicious attacks, such as SQL Injections and certain HTTP flooding attacks. These technologies do not protect against an army of bots requesting public endpoints and exploiting an asymmetry of compute requirements.

Another common solution is to do nothing and assume that it will not impact their business. This appear is choosing to ignore the risks and will eventually be forced to handle the scenario during a mild crisis. Like the bad patch scenario, the root cause might not be a malicious actor, but some event such as a positive viral video.

## Systems based on OpenFlow

The current state-of-the-art solutions for enforcing Quality of Service leverage the OpenFlow 1.3 specification’s addition of networking queues (Mirchev, 2015). An example implementation might create N priority queues, then use a fair sharing algorithm to drain them accordingly. If a flow is detected to be violating a resource quota, then it is associated with a lower level priority queue.

One of the challenges with this approach is that OpenFlow supports a finite number of queues, and this can lead to the scenario that high priority (e.g. interactive traffic) is remediated at in exchange for lower priority traffic (e.g. background copy jobs) being delayed. While this is a preferred state it is not sustainable long term. Eventually the applications will timeout and need to compensate the operations.

Another new solution was published last month, that replaces the TCAM design with Static Random-Access Memory (SRAM) Field Programmable Gate Arrays (FPGA) devices. Their approach improved read operations by 2.5x using a 2/3rds less power. This was achieved by reprogramming the logic gates into multiple filter masks, then taking a union of the masks to reconstruct the same answer as TCAM.

However, there is a performance penalty each time the route table needs to be updated. This is caused by the logic gates needing to perform blocking I/O while the configuration is rearranged. In the worst case this can result in all gates being touched and require over 500 clock cycles to complete. The authors propose that partitioning and sorting algorithms could be used to reduce the probability that large numbers of gates need to be modified. Additional research is required in this area as it might not be performant for certain highly dynamic environments (e.g. wireless IIoT and 5G services).

# Conclusions

Ensuring Quality of Service with software defined networks is an easier problem than traditional networks, as the system can be dynamic and responsive to a holistic view. However, many of the same challenges continue to exist in the new paradigm. These systems need to express granular policy so that expected increases in legitimate (e.g. IIoT) and malicious (e.g. DDoS) traffic can co-exist without disrupting the continuity of core business services.

While research into preventing DDoS has existed for some time it has been lacking in scope and focusing on half the problem space. Application Level attacks are growing in ‘popularity’ at an alarming rate of 60% annually. This will require innovations from software defined network controllers to isolate the malicious flows and apply policies to throttle or block them. This will require solving two problems (1) build more efficient classifiers to determine if a user is malicious or not; and (2) expand the size of the OpenFlow Tables so more granular policies can be authored.