Towards a Unified In-Network DDoS Detection and Mitigation Strategy

Kurt Friday, Elie Kfoury, Elias Bou-Harb, Jorge Crichigno
The Cyber Center For Security and Analytics, University of Texas at San Antonio, USA
Integrated Information Technology Department, University of South Carolina, Columbia, South Carolina

Abstract

- Distributed Denial of Service (DDoS) attacks have terrorized our networks for decades.
- With attacks now reaching 1.7Tbps, the slightest latency in detection and subsequent remediation is enough to bring an entire network down.
- P4 recently emerged as a platform agnostic language for programming the data plane and thus allowing for customized and sophisticated switch pipelines.
- In this project we propose a P4-based detection and mitigation scheme that functions regardless of the size of the attack.
- It successfully defends against the broad spectrum of currently relevant attacks while concurrently emphasizing the Quality of Service (QoS) of legitimate clients.
- We demonstrate its effectiveness using a software programmable P4-switch, namely, the Behavorial Model version 2 (BMv2).
- Results substantiate that the mechanism herein is orders of magnitude faster than traditional approaches such as NetFlow or sFlow.
- We concur that the approach's design particularities facilitate seamless and scalable deployments in high-speed networks requiring line-rate functionality.

Contributions

- Designing and developing a DDoS detection and mitigation engine that tackles a broad spectrum of attacks in real-time solely by analyzing one-way ingress traffic on the switch.
- Placing emphasis on practicality and QoS via its lightweight, switch-based methodology.
- Nullifying all flow table and control channel saturation vulnerabilities by way of fixing both the amount of storage utilized on the switch.
- Completely negating all TCP flooding attacks that strive to impersonate authentic sessions with the server solely in-network.
- Providing a blueprint for harnessing the abilities of programmable switches to provide enhanced network security measures.

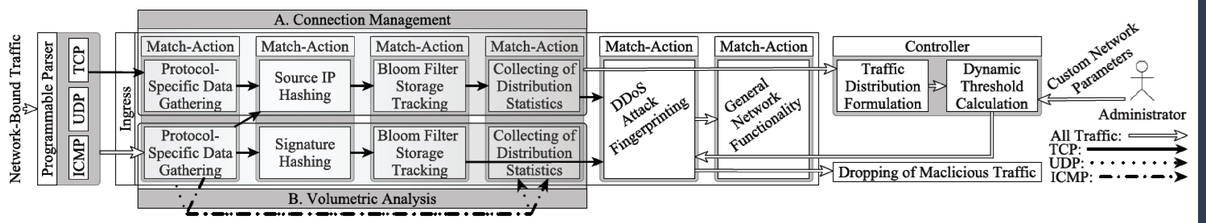
SDN research gaps pertaining to DDoS

- Lack of a unified detection paradigm.
- Source attribution.
- Innate SDN shortcomings.
- Arbitrary threshold and detection techniques.
- Explicit QoS considerations.

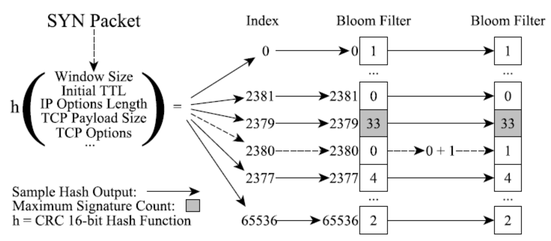
Methodological considerations

- Efficient network integration.
- Quality of service (QoS).
- Administrator input.
- High-speed performance.
- SDN attack-resistance.

Proposed system architecture



SYN request signature tracking



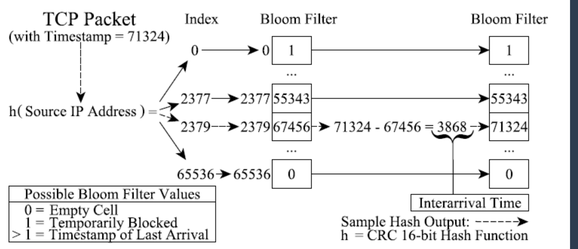
Slow DDoS threshold calculation

Algorithm 1: Slow DDoS threshold calculation

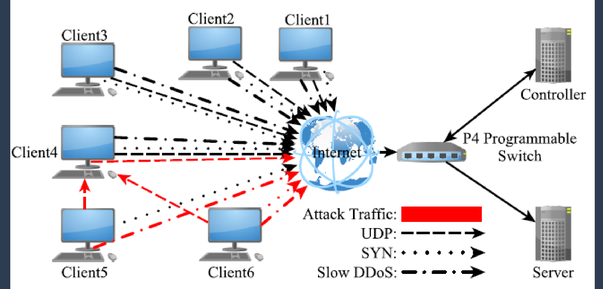
Input: A, c_{est}, c_{tot}
Output: a

$i = 0$;
$dist_{sum} = 0$;
$pdf\_est = 0$;
for $x \in A$ **do**
  $dist_{sum} = dist_{sum} + x$;
end
while $i < |A|$ **do**
  $pdf\_est = pdf\_est + (A[i]/dist_{sum})$;
  if $(1 - pdf\_est) \leq (c_{est}/c_{tot})$ **then**
    return $i * 0.01$;
  end
  $i = i + 1$;
end

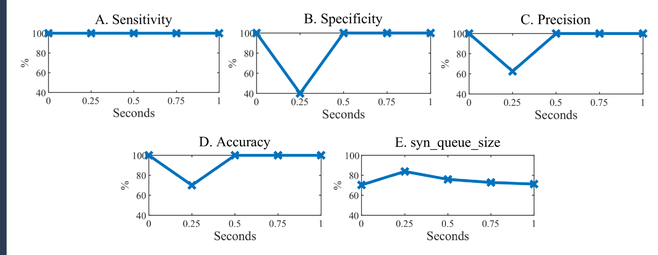
In-network management of TCP sessions



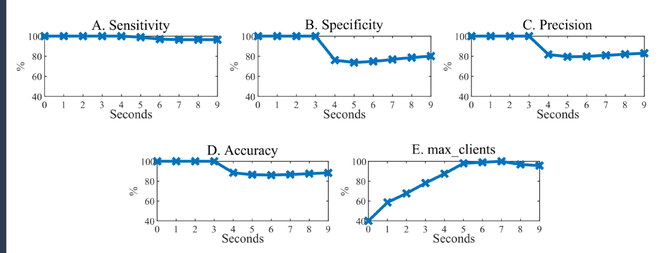
Evaluation topology



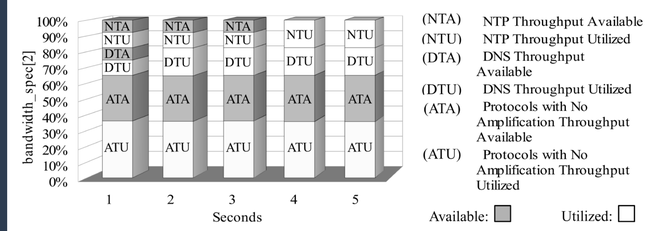
SYN flood attack results



Slow DDoS attack results



UDP amplification attack results



Acknowledgement

- This work was supported by the National Science Foundation (NSF), Grants 1829698 and 1907821.

Concluding remarks and future direction

- The proposed approach rooted in P4 targets the extensive assortment of DDoS attacks while simultaneously circumventing the vulnerabilities of SDN.
- By way of three use cases, the effectiveness of the proposed approach was demonstrated amid both volumetric and slow DDoS attack vectors, as well as validating its explicit emphasis on QoS and ease of deployment.
- For future work, we aim to deploy the methodology on real hardware amid an actual network to put the aforesaid findings to a more comprehensive test.