FTGuard: A Priority-Aware Strategy Against the Flow Table Overflow Attack in SDN

Menghao Zhang, Jun Bi, Jiasong Bai, Zhao Dong, Yongbin Li, Zhaogeng Li (Tsinghua University)
zhangmenghao0503@gmail.com

❖ *Problem Statement*: Flow Table Overflow Attack

Flow Table:

- Dynamic and fine-grained flow control of SDN requires more and wider flow rules ***VS.*** Manufacturing cost and power consumption constraint the capacity of TCAM
- Flow table is limited and easily overflowed under normal circumstances

Existing Flow Table Overflow Mechanism:

- An eviction mechanism is adopted by most of the popular switch platforms (e.g. Open vSwitch, Pica8, Cisco Nexus)
- Some entries are automatically eliminated to make space for newer flow rules (LRU eviction scheme)

Flow Table Overflow Attack:

- Attacker sends probing packets to sniff *idle-timeout*, *hard-timeout*, and even *flow table capacity*, *flow table usage*, and forges a suitable number of fake packets to trick the controller to issue numerous flow rules
- The entire flow table is used up by malicious users and the benign users may suffer from flow entry starvation

❖ *Countermeasure Analysis*

Strawman Solution:

- ✓ Distinguish suspected traffic from benign traffic and simply drop it at the controller
- ✓ Some benign traffic is inevitably harmed while some attack traffic can easily pass, since the judgment for suspected or not may be unreliable such that false positive or false negative is possible

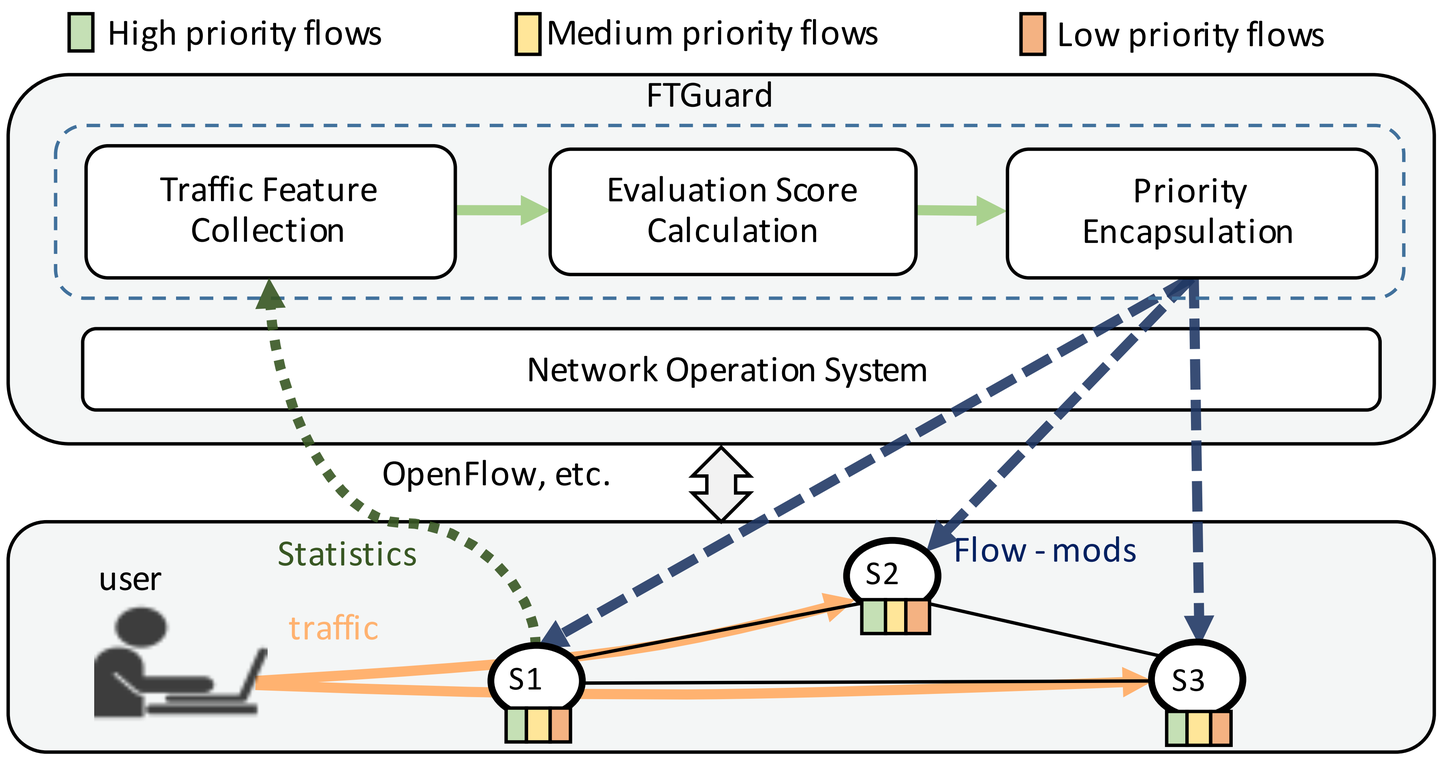
Root Cause:

- ✓ No differentiation between flow entries

FTGuard Basic Idea:

- ✓ Distinguish flows from different source with their traffic features, and achieve soft-isolation for users with priority

❖ *FTGuard Overview*



***Traffic Feature Collection* module:**

- ☐ Frequency of new flows (passive monitoring, classifying, and counting on the controller)
- ☐ Packet number per flow (Issuing statistic messages to the switch periodically (every T seconds) to query the snapshot information)

***Evaluation Score Calculation* module:**

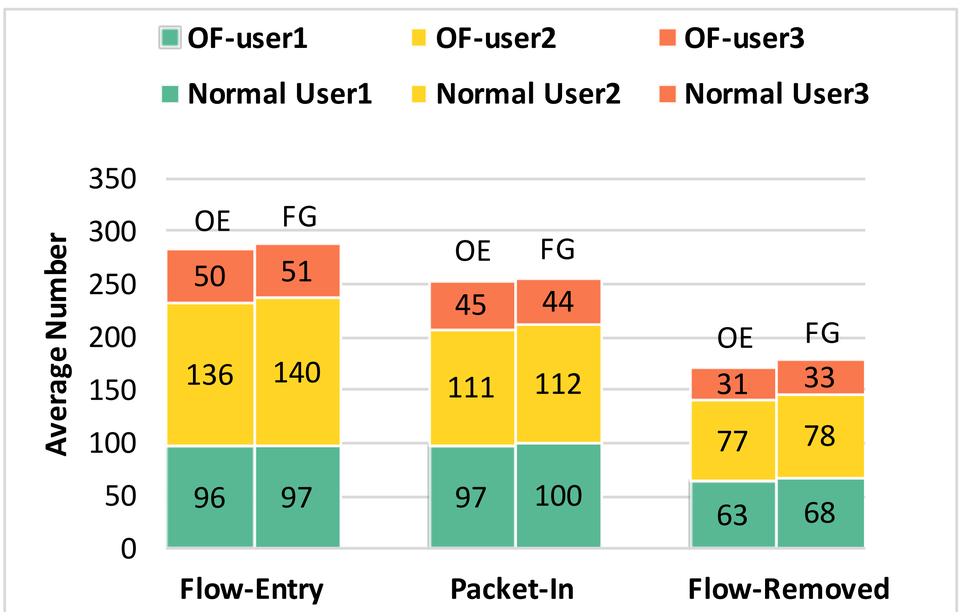
- ☐ Combine the two factors above in two linear correlations as evaluation score (the first is negative correlation while the second is positive correlation)
- ☐ Exponential weighted moving average during the past time

***Priority Encapsulation* module:**

- ☐ map the score to the priority based on probability selection algorithm (two thresholds)
- ☐ Encode priority into the Importance field of flow-mod messages (supported in OpenFlow 1.4+ as optional)

❖ *Evaluation*

OF-Origin Eviction Strategy, FG-FTGuard Strategy
The resource usage of ***three normal users under no-attack scenarios*** (FTGuard works with no extra effect on benign traffic when no attack happens)



The resource usage between ***an attacker and normal users under attack scenarios*** (FTGuard is able to mitigate the overflow attack effectively)