Limitations of Last Year’s SDN DoS Detection Project

Over blocking

Flaw: The mitigation strategy blocks all traffic on a switch port once a throughput threshold is exceeded. Also it may block it for more switches than needed!

Problem: Legitimate traffic is also dropped.

Possible Solution: Use flow-level granularity, implement blocklisting/whitelisting …

Example: The Piracy Shield Case Italy’s Piracy Shield: Lessons Learned and Mistakes to Avoid

Static Threshold

Flaw: Thresholds are statically defined based on known topology and traffic conditions.

Problem: In real-world scenarios, these values are unknown or change dynamically, making the method unreliable.

Possible Solution: Use adaptive thresholds (e.g., moving average, percentile based …).

Controller-Centric Blocking Decisions

Flaw: Only the controller makes blocking decisions, based on its monitoring logic.

Problem: Prevents external apps or admins from contributing to policies, limiting extensibility.

Possible Solution: Use a shared data structure for blocklists, allowing external modules or admins to contribute policies.

Lack of Modular Detection and Mitigation Design

Flaw: Monitoring, decision-making, and enforcement are not clearly separated.

Problem: Hard to maintain or extend; replacing one part affects the whole system.

Possible Solution: Modularize: separate threads for monitoring, policy computation, and enforcement.

Detection Limited to Classic DoS Patterns

Flaw: Only high-throughput, constant-rate DoS attacks are detected. The detection and mitigation strategy is tailored just for one attacker.

Problem: Fails against stealthy attacks (not constant bitrate) or DDoS with distributed, bursty traffic.

Possible Solution: Simulate diverse attack patterns and detect using features like burst variance and flow intervals.

Topology Sensitivity

Flaw: The system is tuned for a specific topology.

Problem: It may not work with more complex topologies.

Possible Solution: Validate on a different topology with respect to last year.

- Up to 10 switches. The attackers should not be attached to the same switch. They must be distributed across different switches, and their traffic should impact the communication of legitimate hosts. Be careful to cycles in your topology design!

Inflexible Blocking/Unblocking Policy

Flaw: Unblocking is either too early or too late, if it happens at all.

Problem: This can block legitimate users for too long or allow attackers back too soon.

Possible Solution: Up to you.

This year security project work

This year's project builds upon last year's work on detecting and mitigating DoS attacks in a Software Defined Networking (SDN) environment using Mininet and OpenFlow switches.

The goal is **not** to start from scratch, but rather to **take last year's implementation as a starting point** and **significantly improve it** by addressing known issues and limitations.

Specifically, you are required to:

- **Solve at least 5 critical flaws** found in the original design (e.g., static thresholding, indiscriminate traffic blocking, lack of modularity, etc.) with the ones highlighted in yellow mandatory.
- **Enhance the system with additional features of your choice** that could make it more robust, flexible, or intelligent — be creative!