34TH USENIX SECURITY SYMPOSIUM

Lemon: Network-Wide DDoS Detection with Routing-Oblivious Per-Flow Measurement

Wenhao Wu, Zhenyu Li, Xilai Liu, Zhaohua Wang
Heng Pan, Guangxing Zhang, Gaogang Xie

Network-Wide Measurement

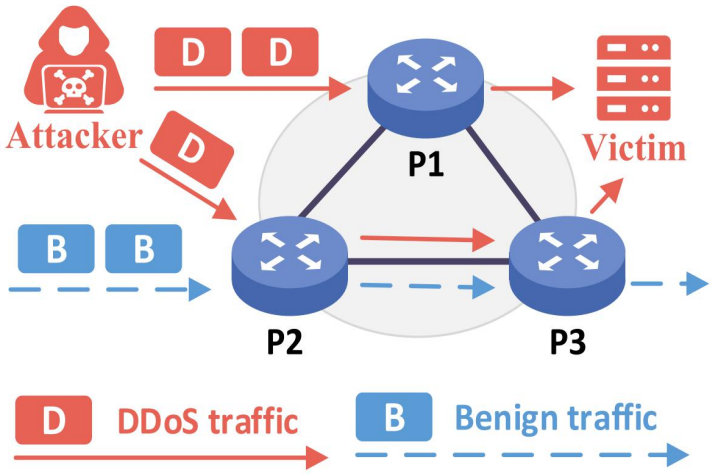
Measurement results from a single measurement point is limited.

Network-wide traffic information is more valuable

Network-wide Measurement

- Aggregating measurement results from multiple nodes to form traffic information across the entire network.

DDoS traffic disperses across multiple paths.



A single-point view cannot detect distributed DDoS traffic

Local View of Measuring Points

View of P1: D D
DDoS Alert: None 1 False Negative

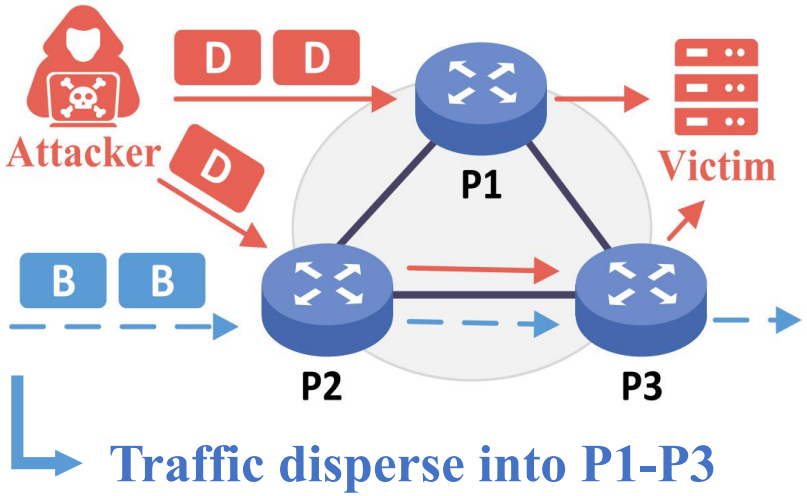
View of P2: D B B
DDoS Alert: None

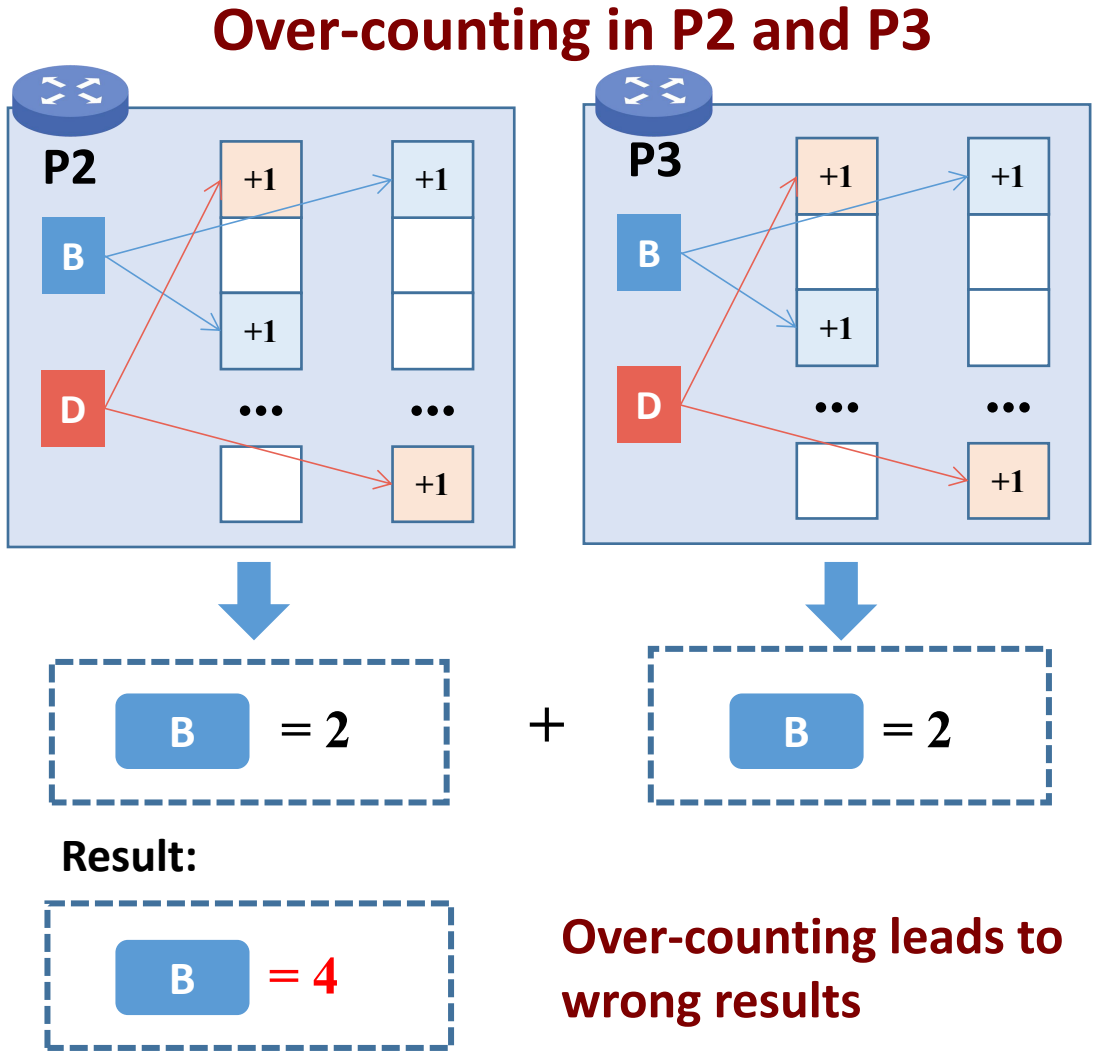
View of P3: D B B
DDoS Alert: None

Issues-1: Over-Counting

For network-wide measurement：

- Aggregation of measurement data must take into account **routing and the topology** of measurement points.
- Improper aggregation can lead to **over-counting** and mis-allocating issues.

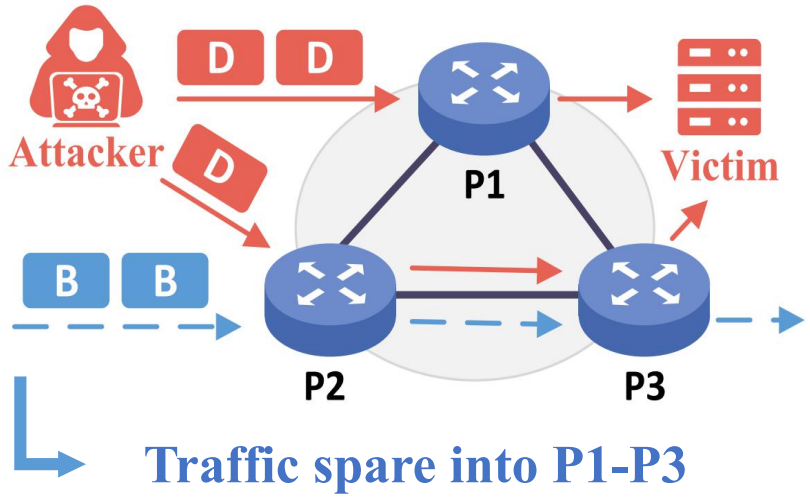




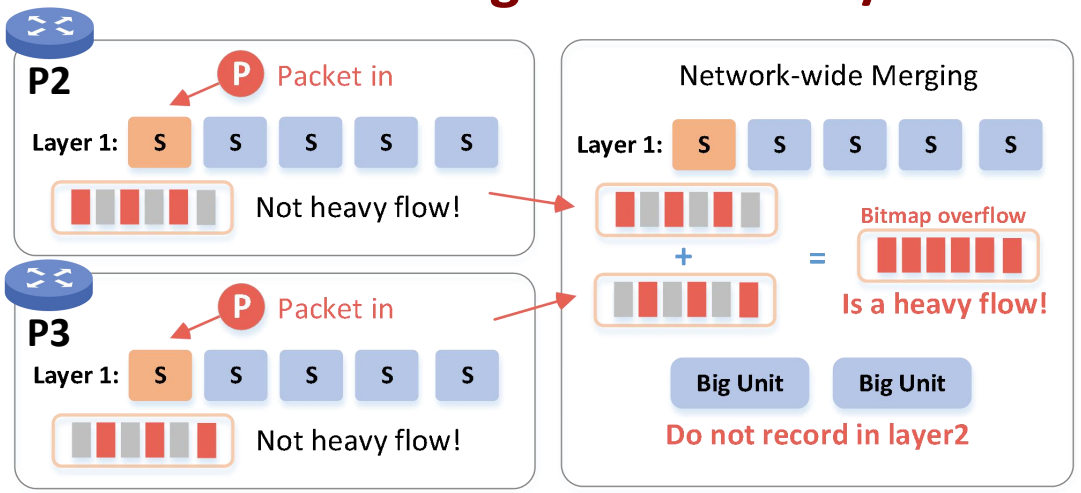
Issues-2: Mis-allocating

For network-wide measurement：

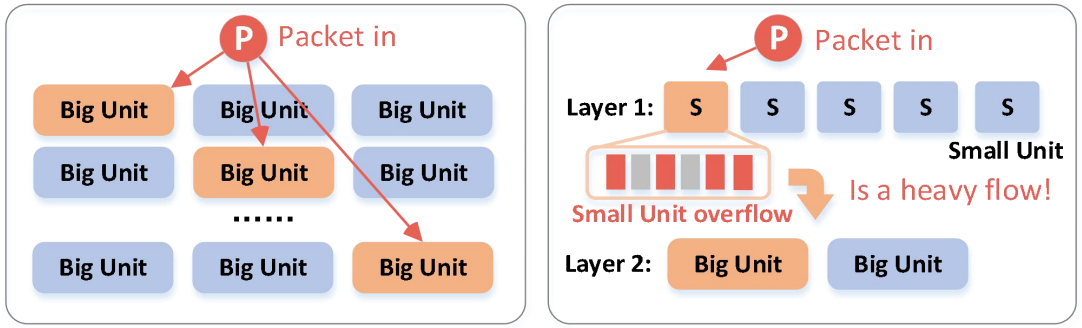
- Aggregation of measurement data must take into account **routing and the topology** of measurement points.
- Improper aggregation can lead to over-counting and **mis-allocating** issues.



Mis-allocating in P1 and P2/P3



Current sketches **save space via multi-stage processing**, assigning flows by size.



Lemon: Design & Performance

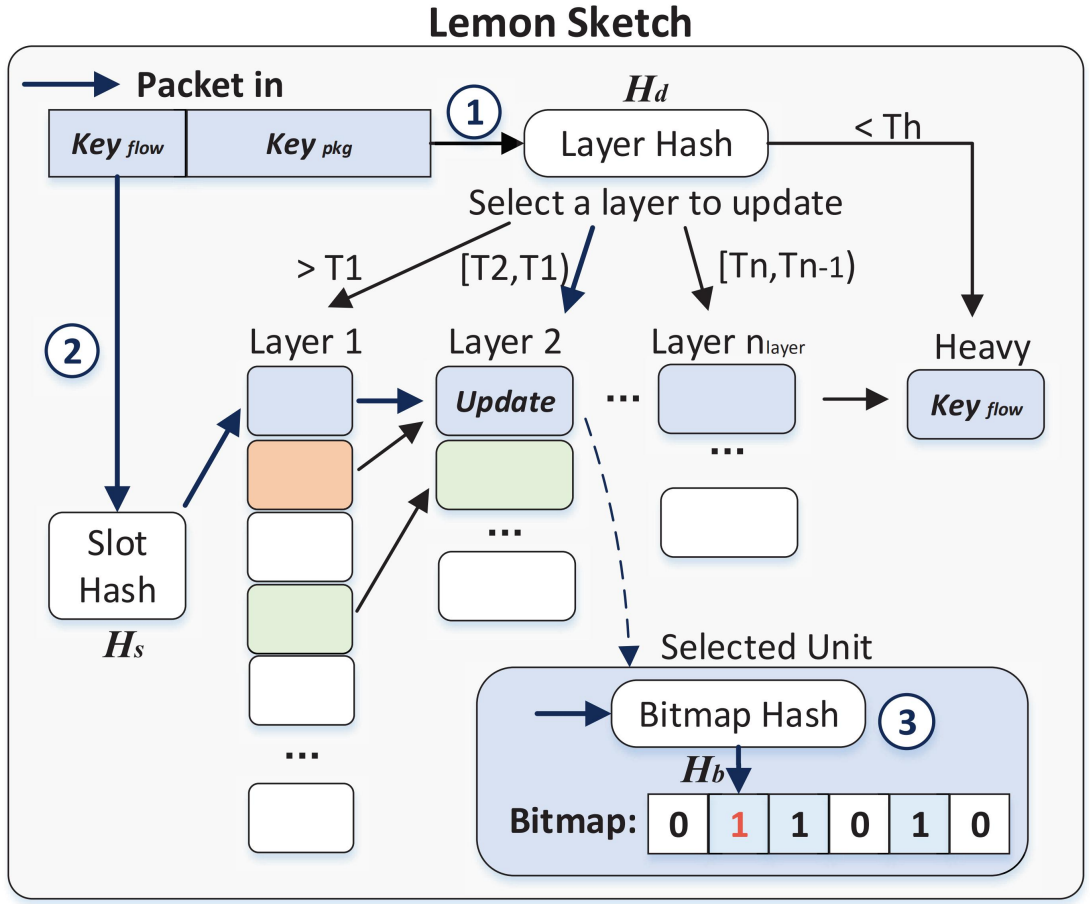
How to addressed issues?

? Carefully merge measurement results using the routing of each packet:

Heavy computational cost | **Dynamic network environment**

Routing-oblivious measurement

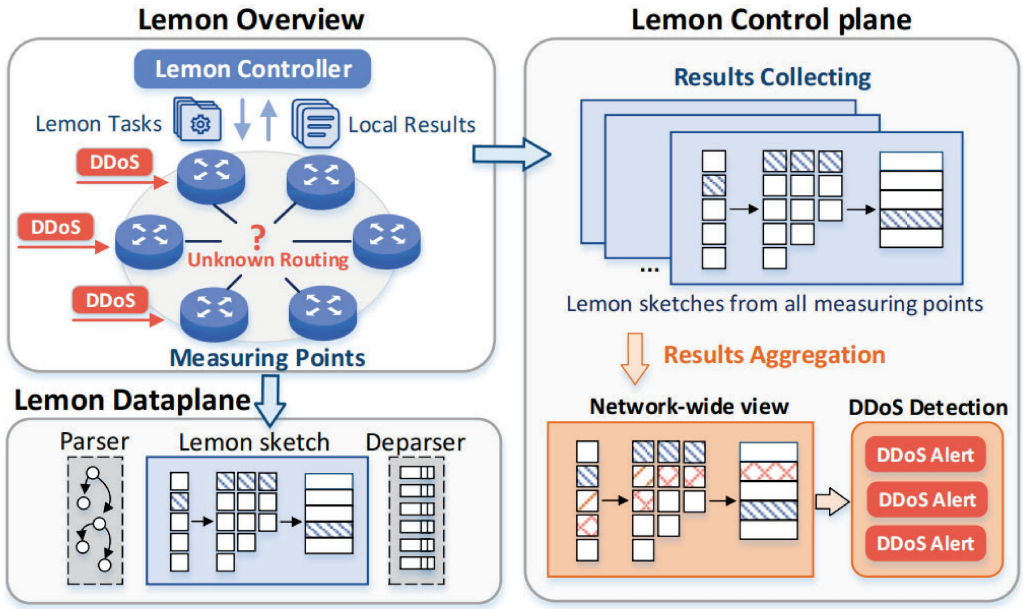
- Obtaining accurate network-wide view with unknown topology and traffic routing
- **Over-counting-free:** each packet is uniquely identified, reframing the packet counting as per-flow cardinality estimation
- **Mis-allocating-free:** assigns flows to units fully via hash results and ensures globally consistent updates



Lemon: Design & Performance

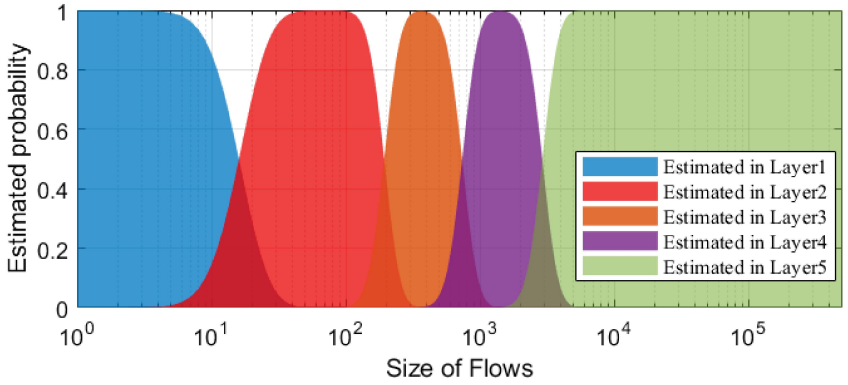
Network-wide measurement with Lemon:

- Accurate network-wide measurement results
- Globally consistent sketch updating

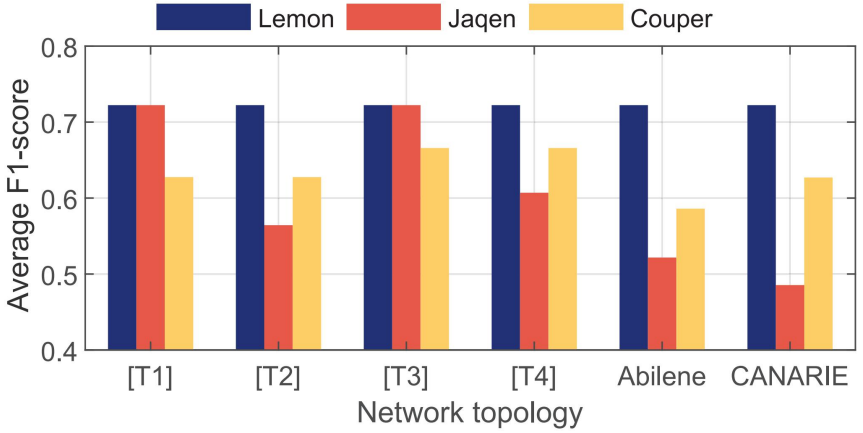


Overview of the Lemon

- **Lemon segregates flows with different sizes into different layers**



- **Accurate network-wide measurement results supports DDoS detection**



Thanks