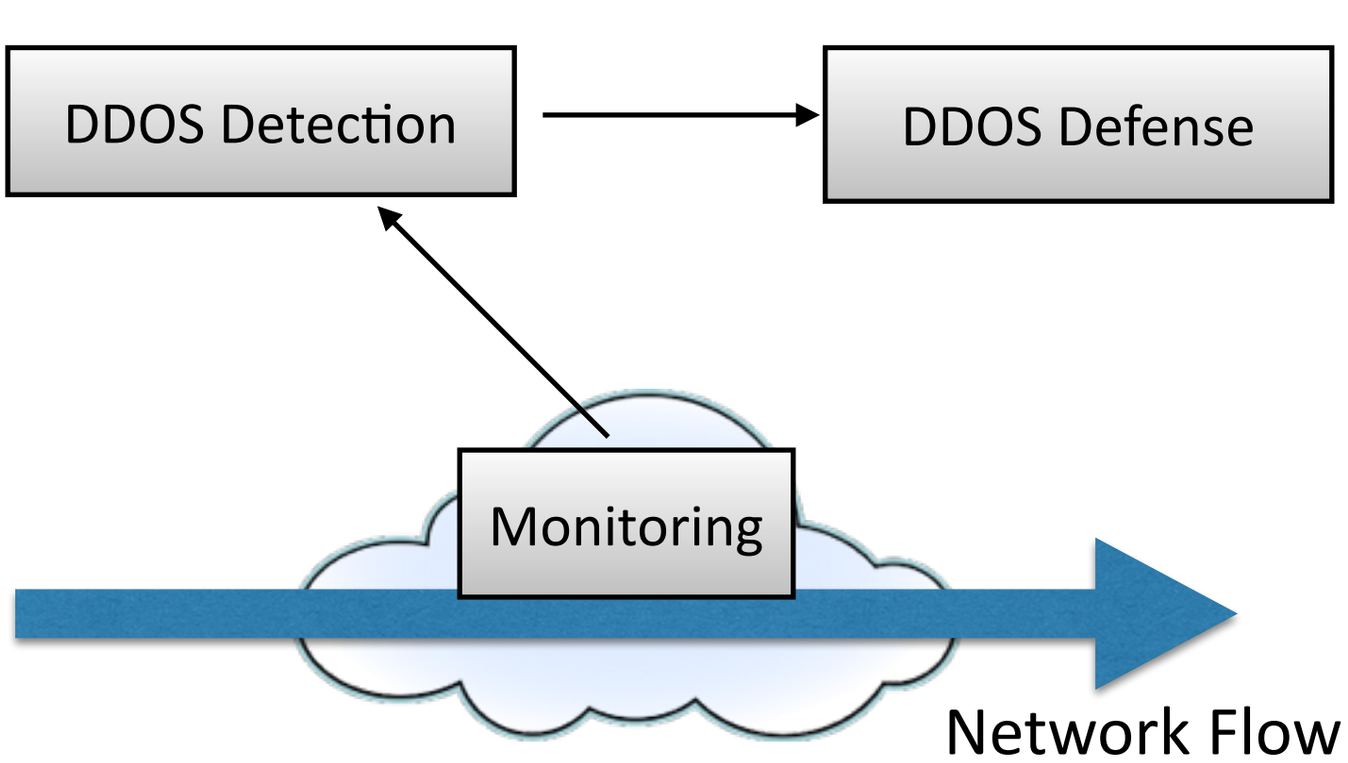
Scalable Attack Detection using Universal Monitoring

Hun Namkung
1st year PhD student @ CMU

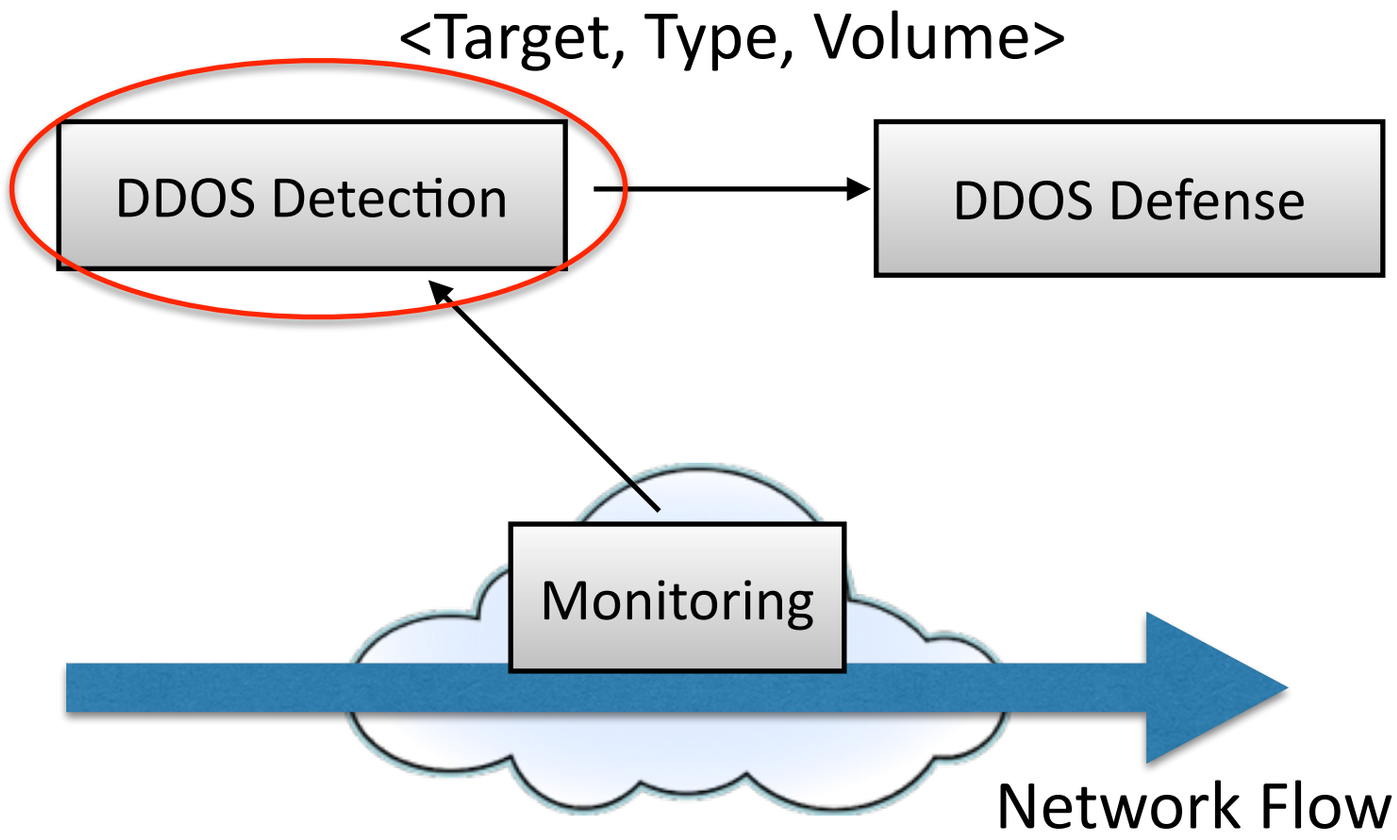
Today's DDOS defense

- DDOS Detection
  - Input - Network Flow
  - Output - <Target, Type, V>
- DDOS Defense
  - Using output of DDOS Detection <Target, Type, V>, mitigate DDOS attack



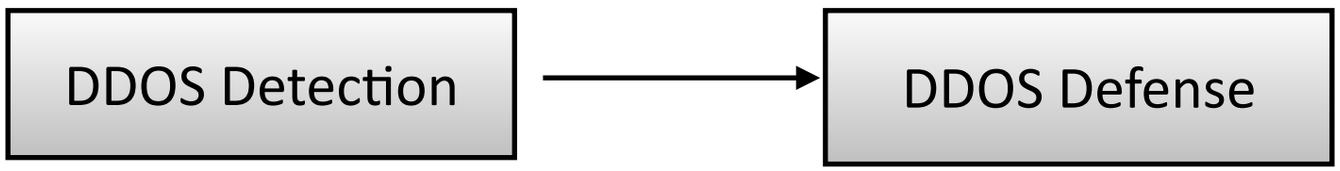
Today's DDOS defense

- DDOS Detection
  - Input - Network Flow
  - Output - <Target, Type, V>
- DDOS Defense
  - Using output of DDOS Detection <Target, Type, V>, mitigate DDOS attack



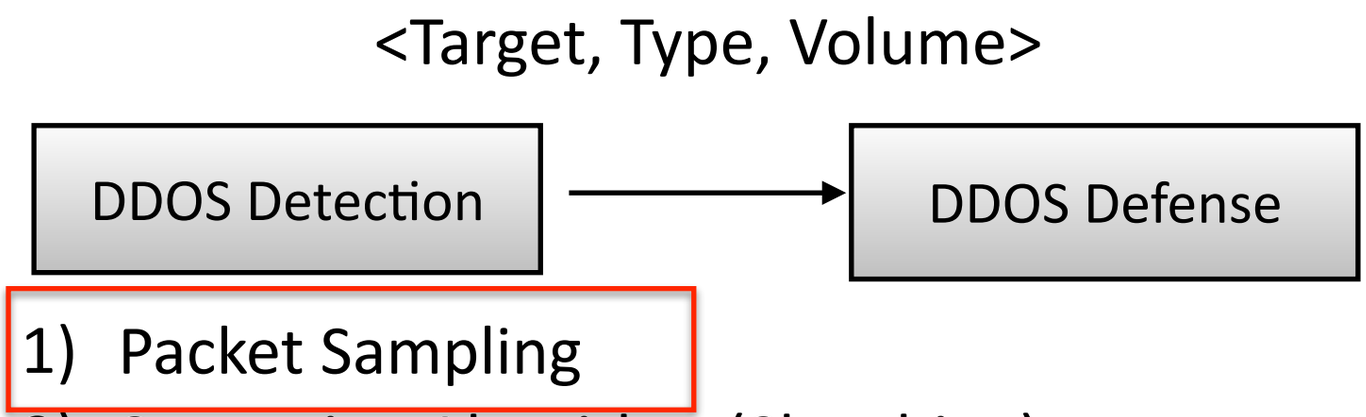
Today's DDOS detection

<Target, Type, Volume>



1) Packet Sampling
2) Streaming Algorithm (Sketching)

Today's DDOS detection

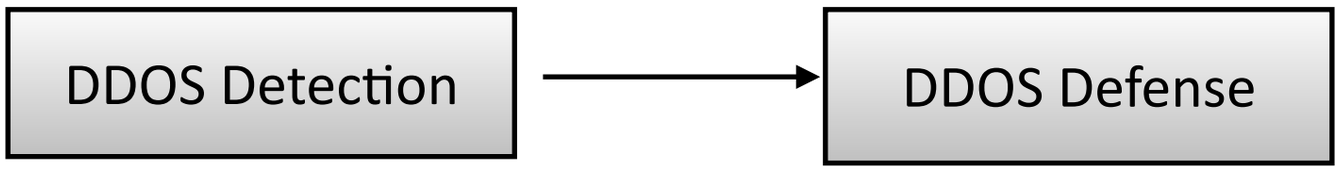


1) Packet Sampling (NetFlow)

- Inspecting every packet -> overhead (memory, compute). Let's skip some packets
- Good - It reduces overhead
- Bad - It misses many packets thus it is less accurate

Today's DDOS detection

<Target, Type, Volume>



1) Packet Sampling
2) Streaming Algorithm (Sketching)

2) Streaming Algorithm (Sketching)

- Specific algorithm for specific needs
- Good - Use less memory space O(LogN). More accurate than sampling
- Bad - Works for only specific detection. Not a general solution.

Opportunity: Universal Monitoring

- Universal Sketching. Use less memory, more accurate than sampling
- Sketching once at the data plane, it can be applied to possibly many sketching algorithms
- Both General and Accurate

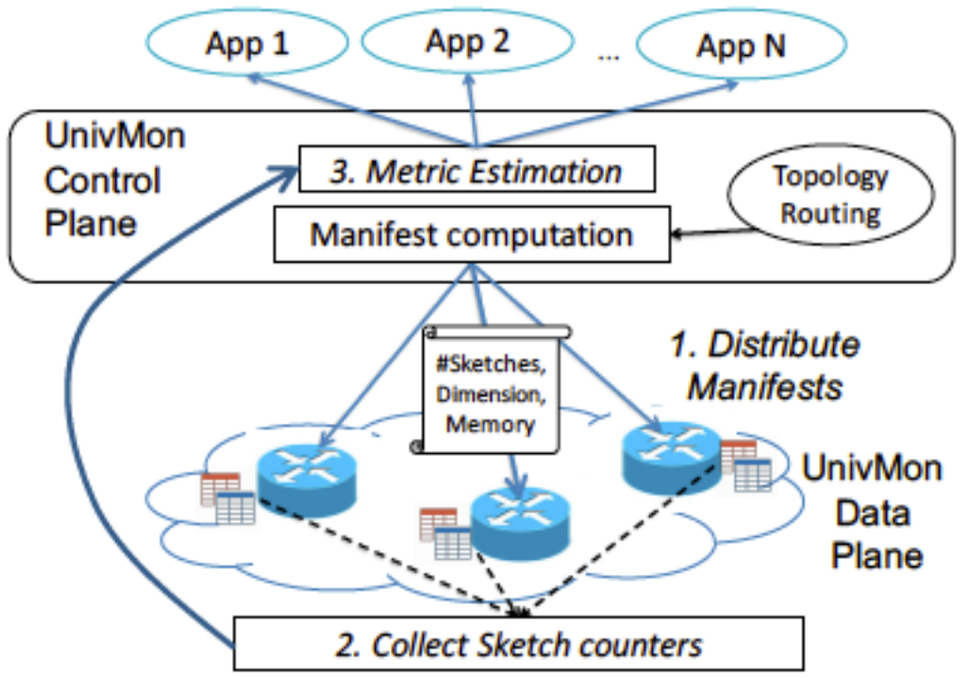
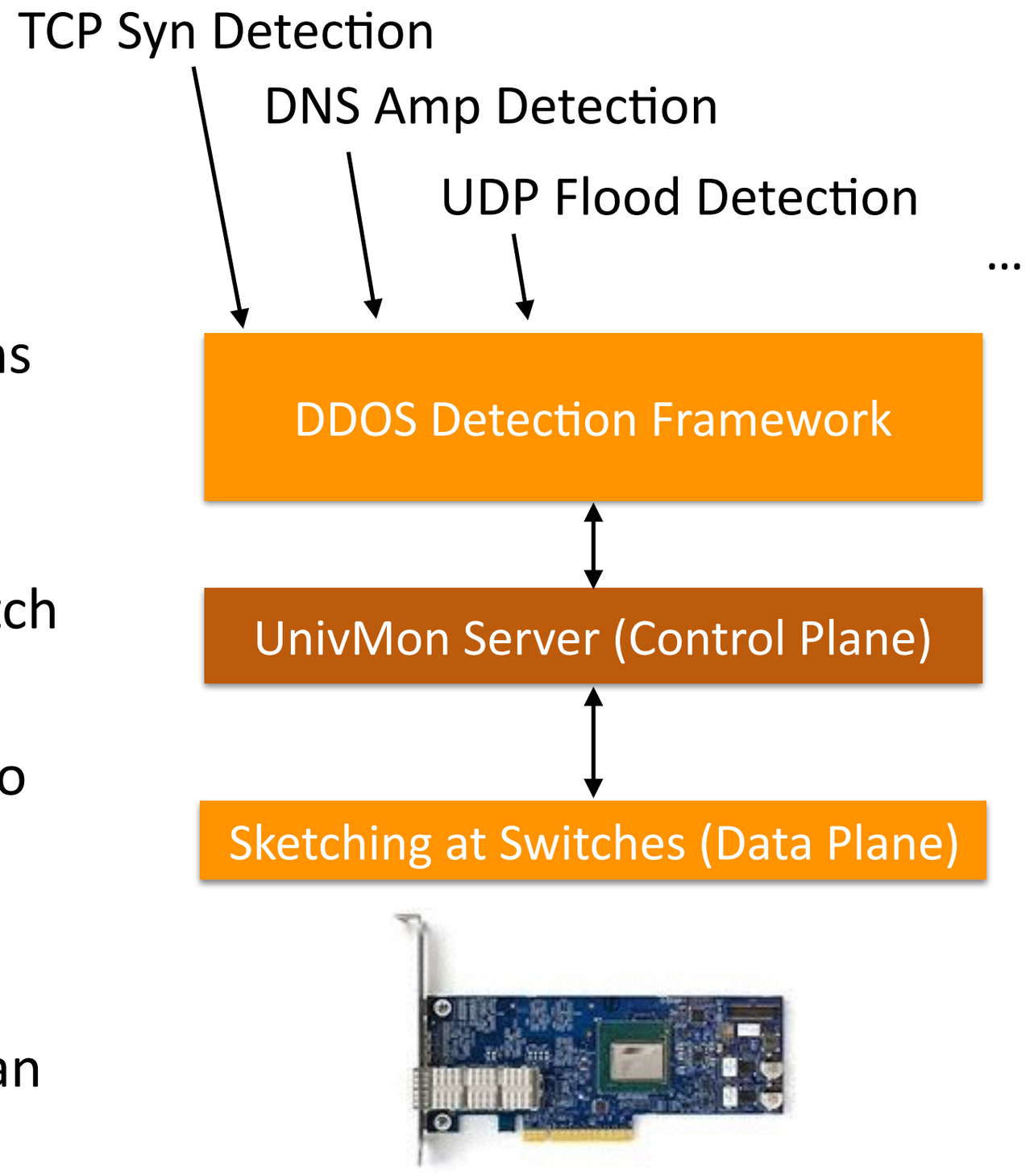


Figure 1: Overview of UnivMon: The data plane nodes perform the monitoring operations and report sketch summaries to the control plane which calculates application-specific metric estimates.

Idea

- Scalable Framework
  - We want to provide library for many DDOS detection algorithms
- UnivMon and Netronome
  - Universal Sketching code at switch level are implemented in P4
  - We envision porting P4 code into Netronome
  - We can show that our idea is deployable in actual HW
  - Real data is more interesting than virtual environment data for evaluation



Thank you