Scalable NetFlow Analysis with Hadoop

Yeonhee Lee and Youngseok Lee

{yhlee06, lee}@cnu.ac.kr

http://networks.cnu.ac.kr/~yhlee

Chungnam National University, Korea

January 8, 2013

FloCon 2013

Contents

- Introduction
- Overview
- Hadoop-based traffic processing tool
- Evaluation
- Summary

INTRODUCTION

Internet Measurement

- Challenges
  - Scalability
  - Fault-tolerant system
  - Extensibility
- CAIDA data
  - Capture, Curation, Storage, Search, Sharing, Analysis, and Visualization
    - Ark topology: 1.8 TB
    - Telescope: 102 TB
    - Packet headers: 18.8 TB

Josh Polterock, "CAIDA: A Data Sharing Case Study," Security at the Cyber Border: Exploring Cybersecurity for International Research Network Connections workshop, 2012

Harness Distributed Computing and Storage ?

Google MapReduce, 2004

- 1 PB sorting by Google
  - 2008: 6 hours and 2 minutes on 4,000 computers
  - 2011: 33 minutes on 8000 computers
  - 2011: 10PB, 8000 computers, 6 hours and 27 minutes

Google

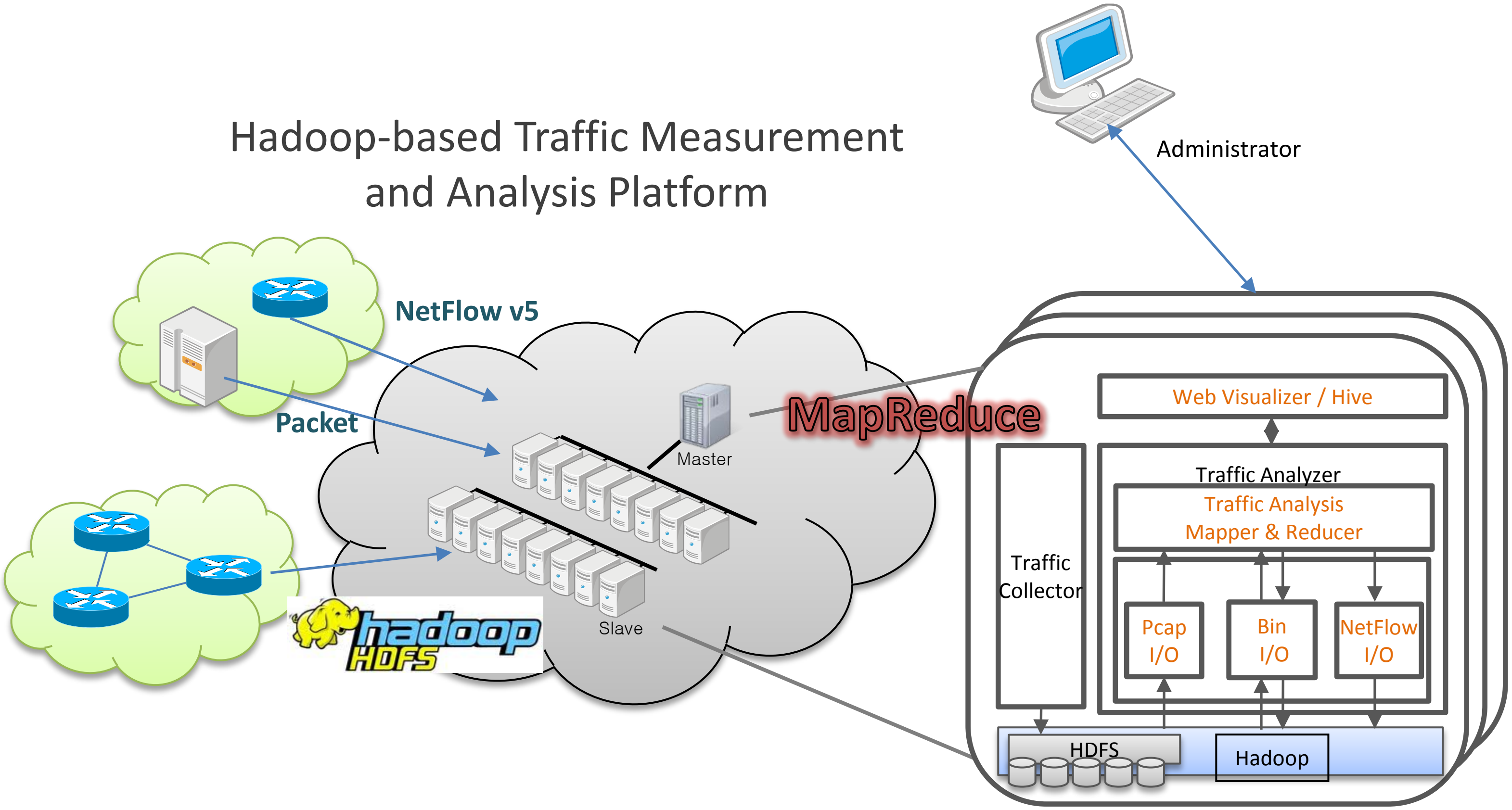
Apache Hadoop project

hadoop

IBM
LinkedIn
NETFLIX
facebook
YAHOO!
EMC²
twitter
ebay
Microsoft
NTT Communications
YAHOO!
cloudera
hortonworks

CBS Interactive
ORBITZ

Our Proposal



1. *Yeonhee Lee and Youngseok Lee, "Toward Scalable Internet Traffic Measurement and Analysis with Hadoop," ACM SIGCOMM Computer Communication Review (CCR), Jan. 2013*
2. *Yeonhee Lee and Youngseok Lee "A Hadoop-based Packet Trace Processing Tool" , TMA, April 2011*
3. *Yeonhee Lee and Youngseok Lee, "Detecting DDoS Attacks with Hadoop", ACM CoNEXT Student Workshop, Dec, 2011*

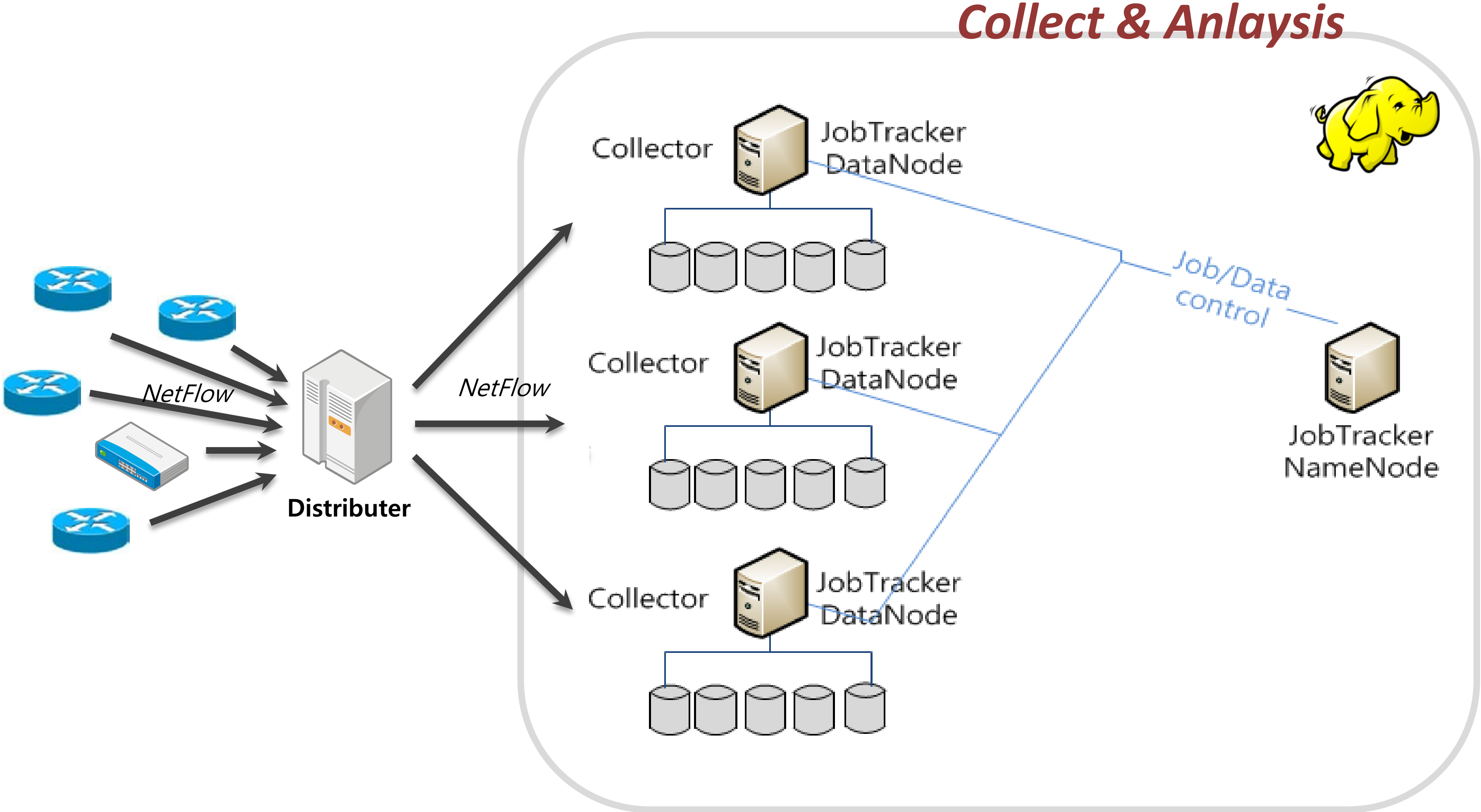
Related Work

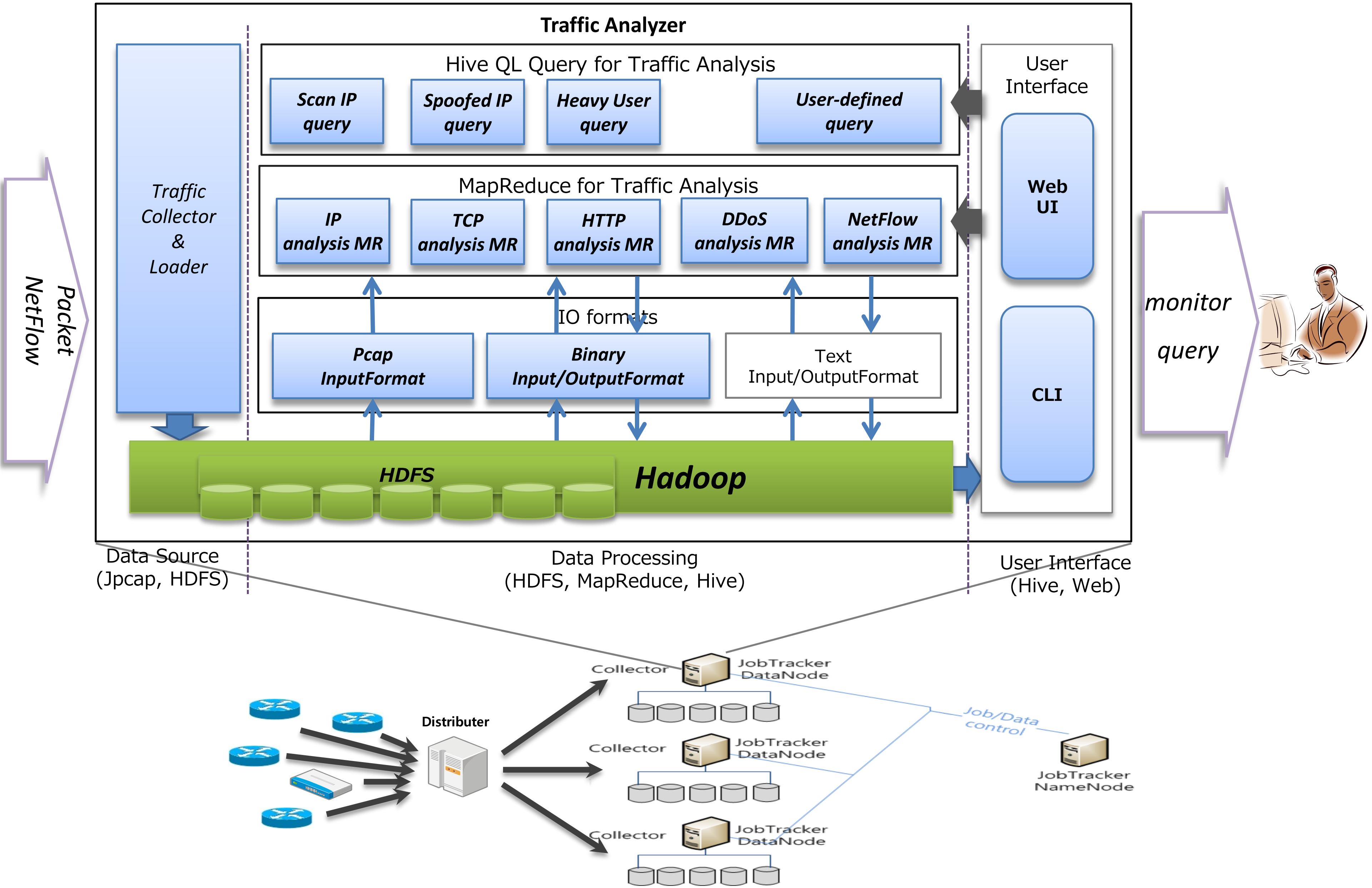
- Traffic analysis of DNS root server (RIPE, 2011.11)
- PacketPig (2012.03) - Big Data Security Analytics platform
- Sherpasurfing – Open Source Cyber Security Solution, Hadoop World 2011
  - Firewall/IDS logs, netflow/packet
- Performing Network and Security Analytics with Hadoop, (Travis Dawson, Narus), Hadoop Summit 2012
- Distributed Bro (IDS)

Viewing: Site Name

OVERVIEW

Hadoop-based NetFlow Analysis

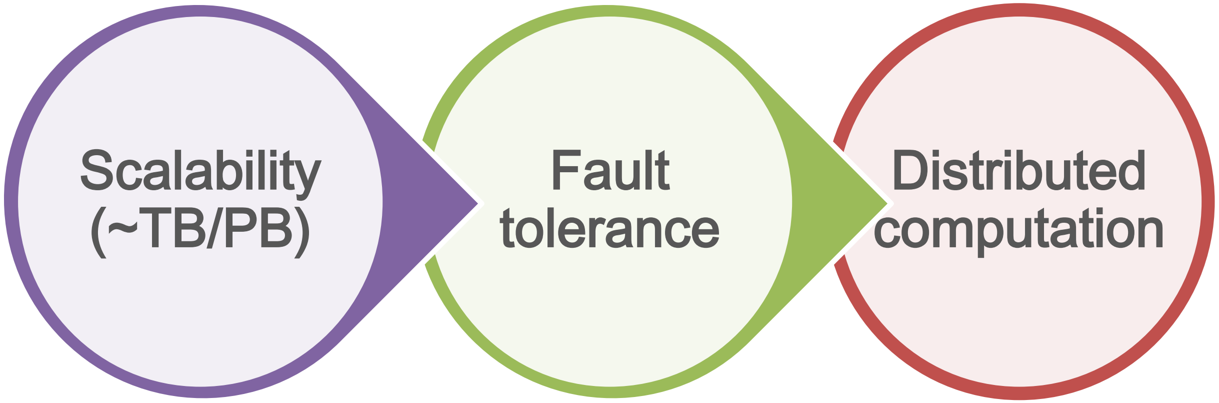



Traffic Analyzer
Packet
NetFlow
Traffic Collector & Loader
Hive QL Query for Traffic Analysis
Scan IP query
Spoofed IP query
Heavy User query
User-defined query
MapReduce for Traffic Analysis
IP analysis MR
TCP analysis MR
HTTP analysis MR
DDoS analysis MR
NetFlow analysis MR
IO formats
Pcap InputFormat
Binary Input/OutputFormat
Text Input/OutputFormat
HDFS
Hadoop
User Interface
Web UI
CLI
monitor
query
Data Source (Jpcap, HDFS)
Data Processing (HDFS, MapReduce, Hive)
User Interface (Hive, Web)
Distributer
Collector
JobTracker DataNode
Collector
JobTracker DataNode
Collector
JobTracker DataNode
Job/Data control
JobTracker NameNode

HADOOP-BASED TRAFFIC ANALYSIS

Challenges

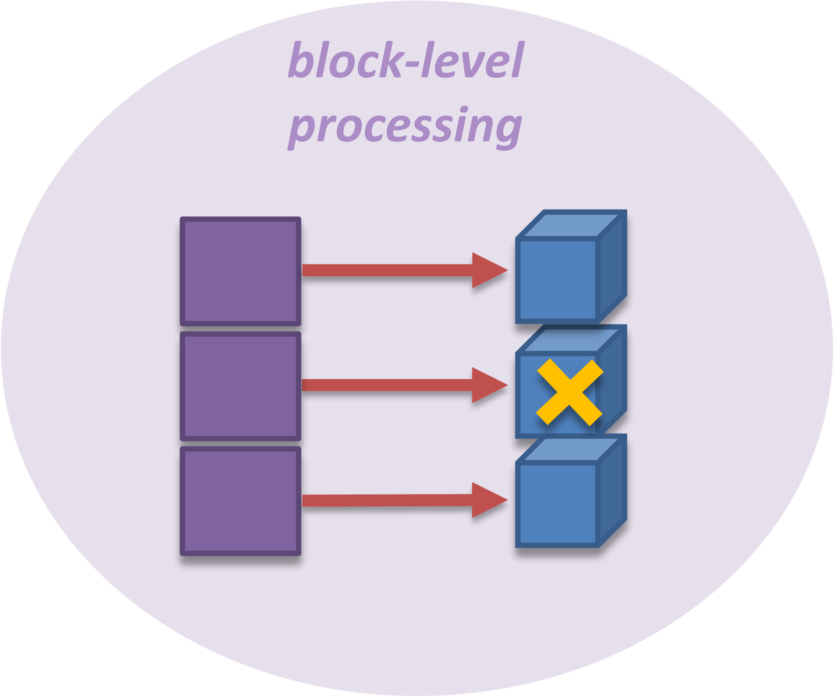
1. Data handing issue in HDFS
2. Distributed traffic analysis MapReduce algorithms
3. Performance tuning in a large-scale Hadoop



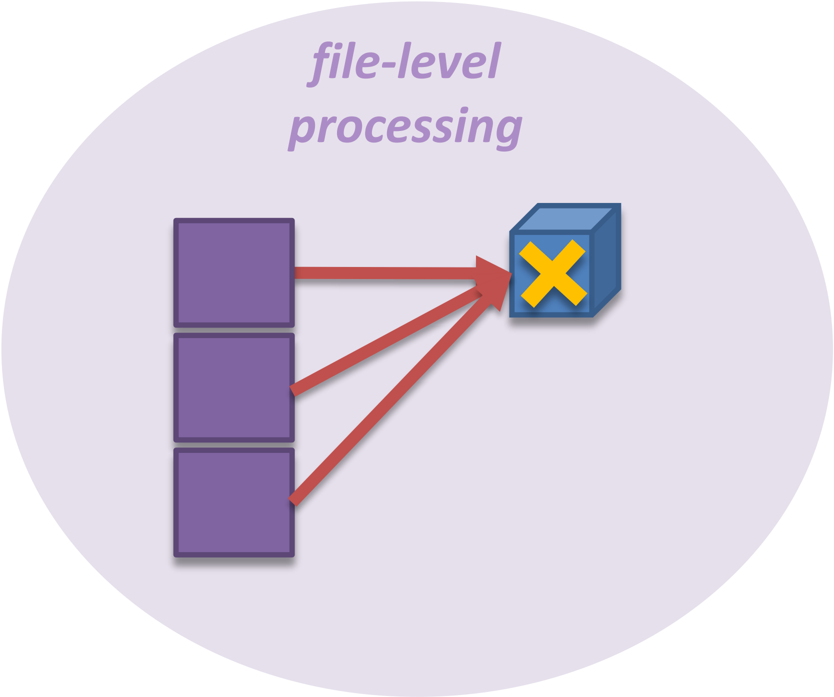
Challenges

1. Data handing issue in Hadoop
2. Distributed traffic analysis MapReduce algorithms
3. Performance tuning in a large-scale Hadoop testbed

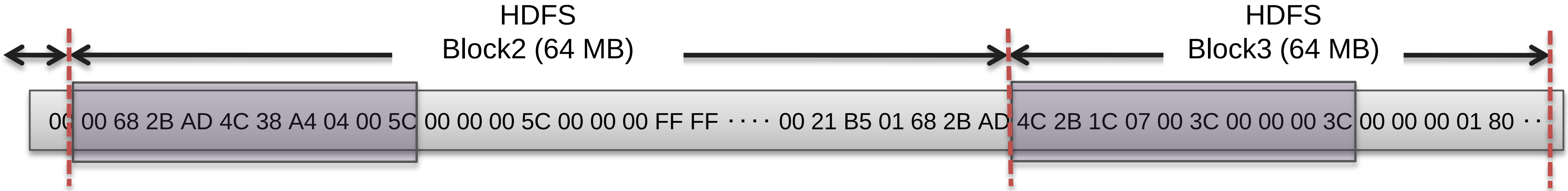
Block-level Parallelism



block-level processing



file-level processing

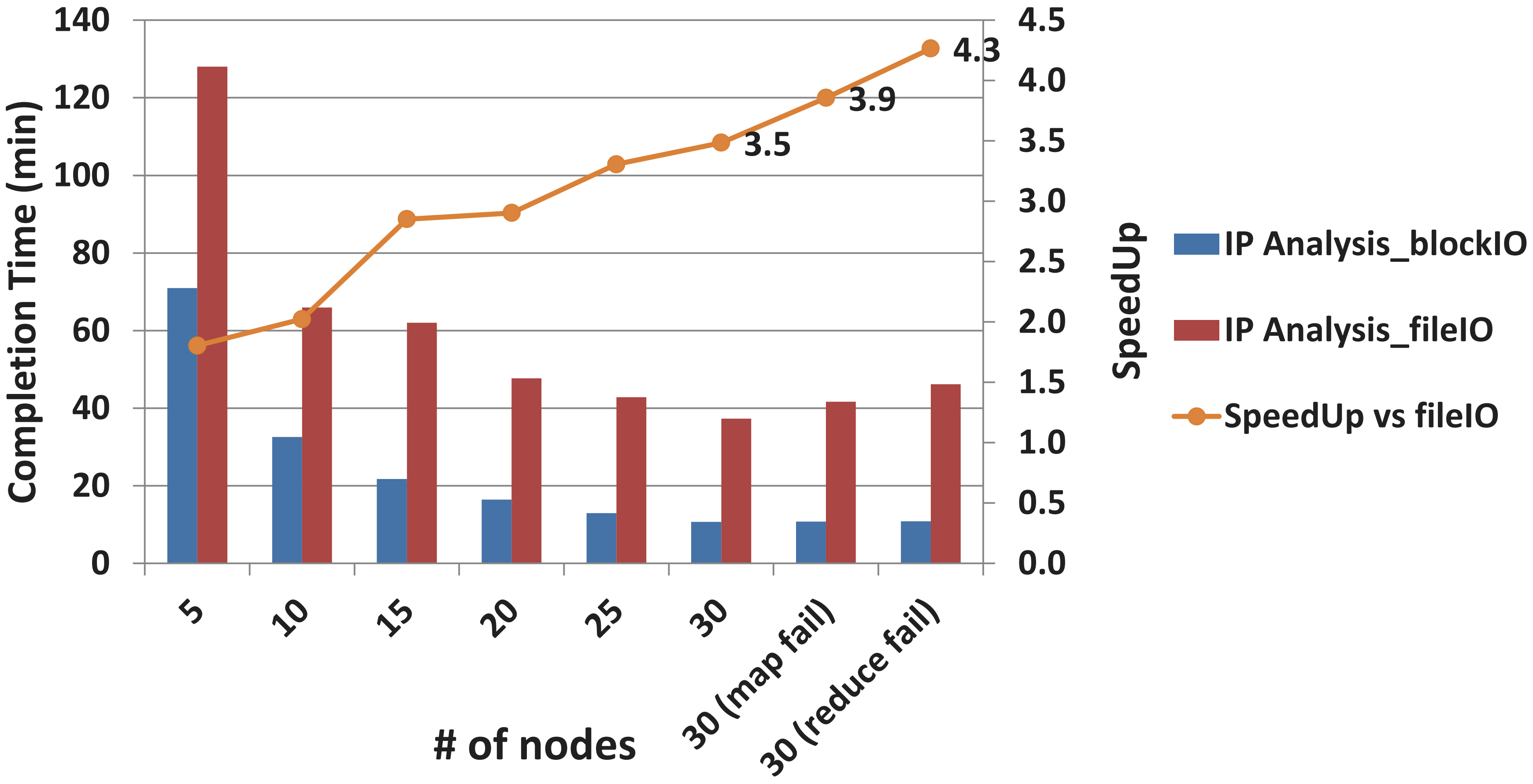


HDFS Block2 (64 MB)

HDFS Block3 (64 MB)

00 00 68 2B AD 4C 38 A4 04 00 5C 00 00 00 5C 00 00 00 FF FF · · · · 00 21 B5 01 68 2B AD 4C 2B 1C 07 00 3C 00 00 00 3C 00 00 00 01 80 · ·

Block-level IO vs. File-level IO



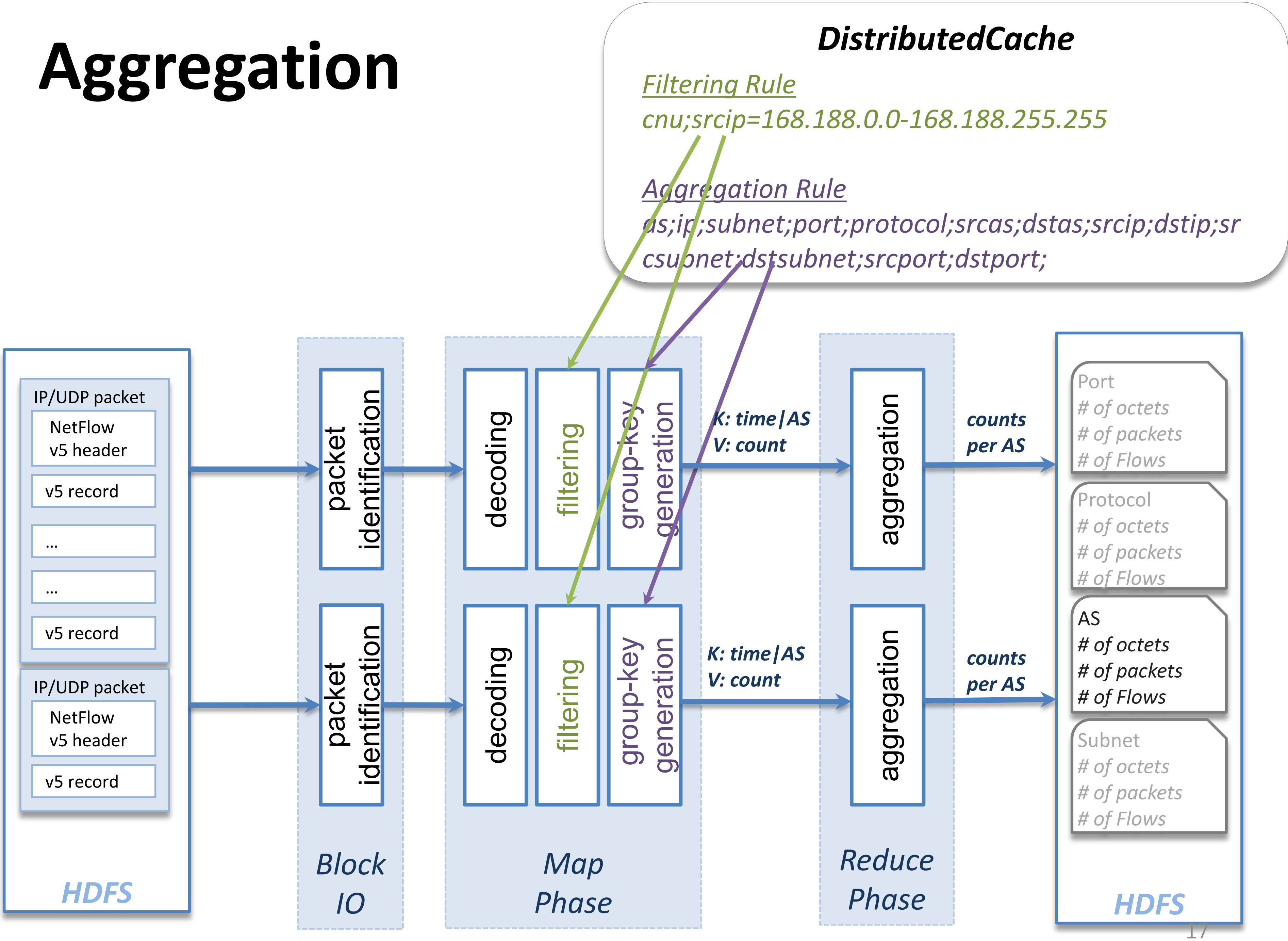
Challenges

1. Data handing issue in Hadoop

2. Distributed traffic analysis MapReduce algorithms

3. Performance tuning in a large-scale Hadoop testbed

Aggregation



DistributedCache

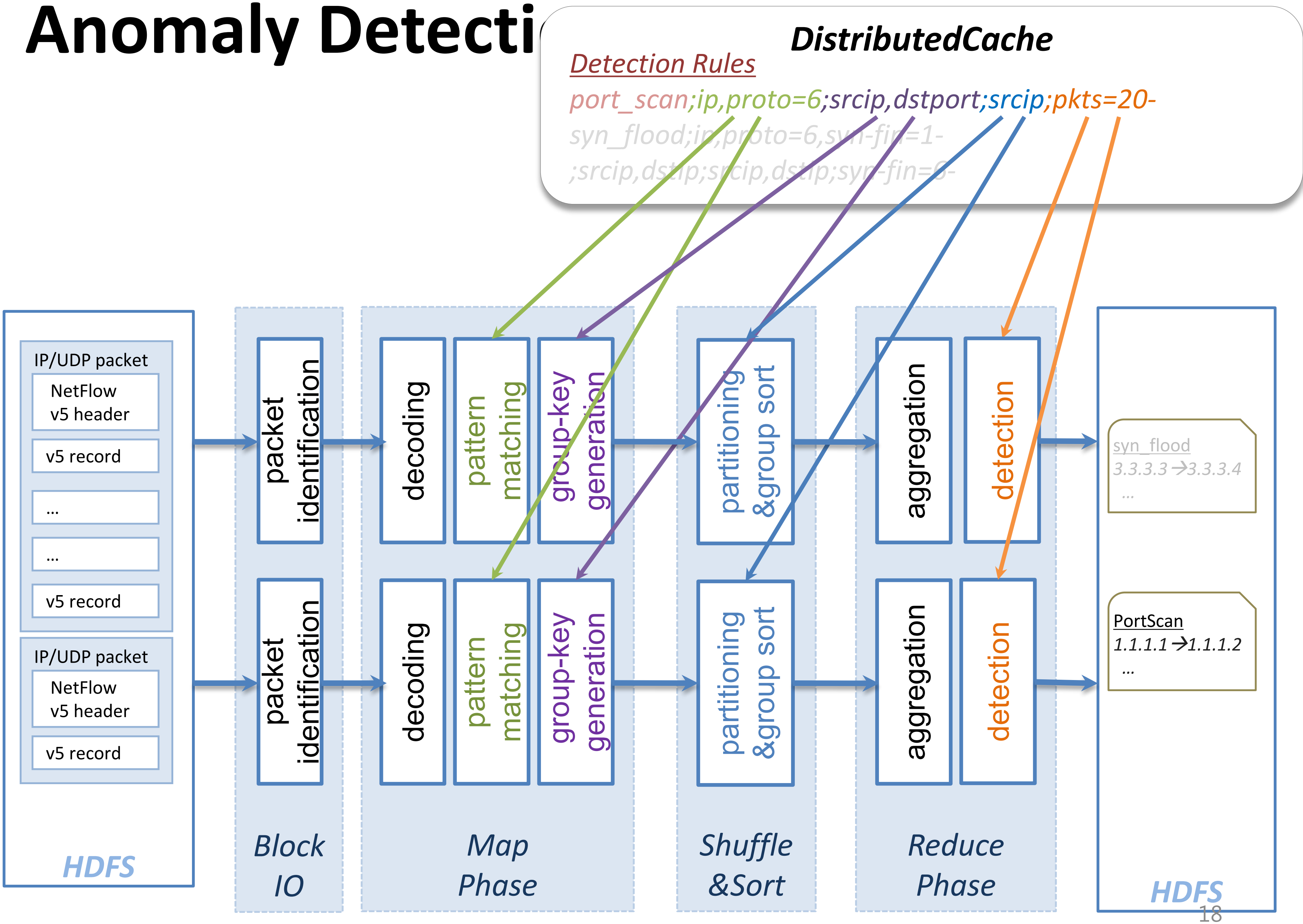
Filtering Rule

cnu;srcip=168.188.0.0-168.188.255.255

Aggregation Rule

as;ip;subnet;port;protocol;srcas;dstas;srcip;dstip;srcsubnet;dstsubnet;srcport;dstport;

Anomaly Detecti



DistributedCache

Detection Rules

port_scan;ip,proto=6;srcip,dstport;srcip;pkts=20-

syn_flood;ip,proto=6,syn-fin=1-

;srcip,dstip;srcip,dstip;syn-fin=0-

Challenges

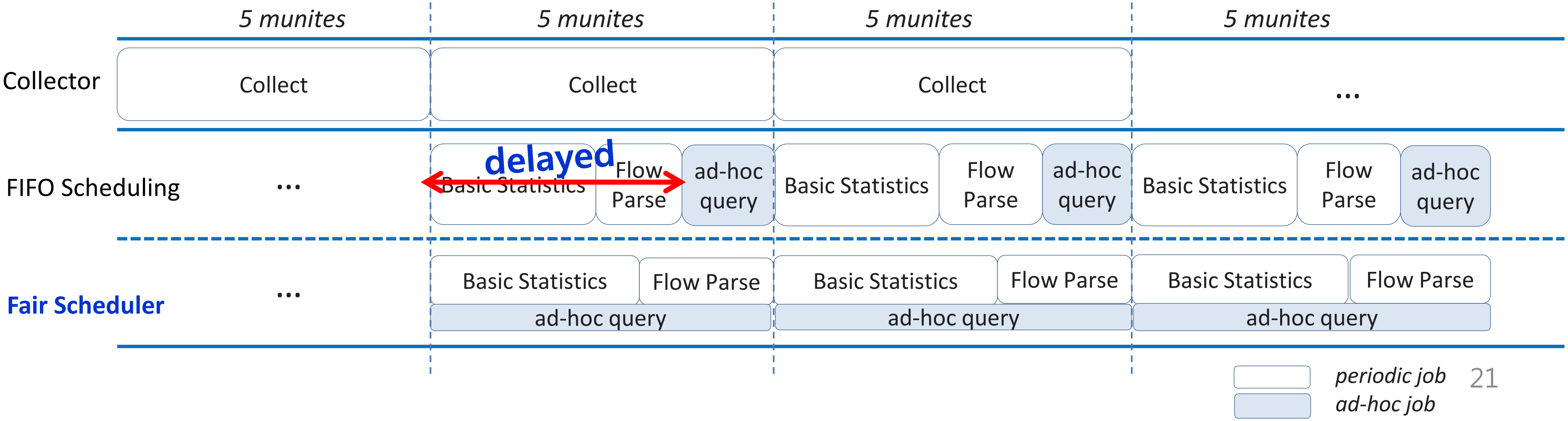
1. Data handing issue in Hadoop
2. Distributed traffic analysis MapReduce algorithms
3. Performance tuning in a large-scale Hadoop

Performance Tuning

- Configuration
  - Hadoop IO Buffer (128K → 1 MB)
  - Java heap space (300 MB →1 024 MB)
  - # of MapReduce Slots (→# of cores)
- MapReduce Algorithm
  - normal combiner vs inMapper combiner
- Job scheduling

Job Scheduling

- Different job types
  - Periodic jobs (for monitoring)
    - guaranteed service within time
    - e.g Aggregated Statistics for monitoring, Flow Parse job for analytics
  - Small ad-hoc query job (for analytics)
    - fast response time



PERFORMANCE EVALUATION

Experiments

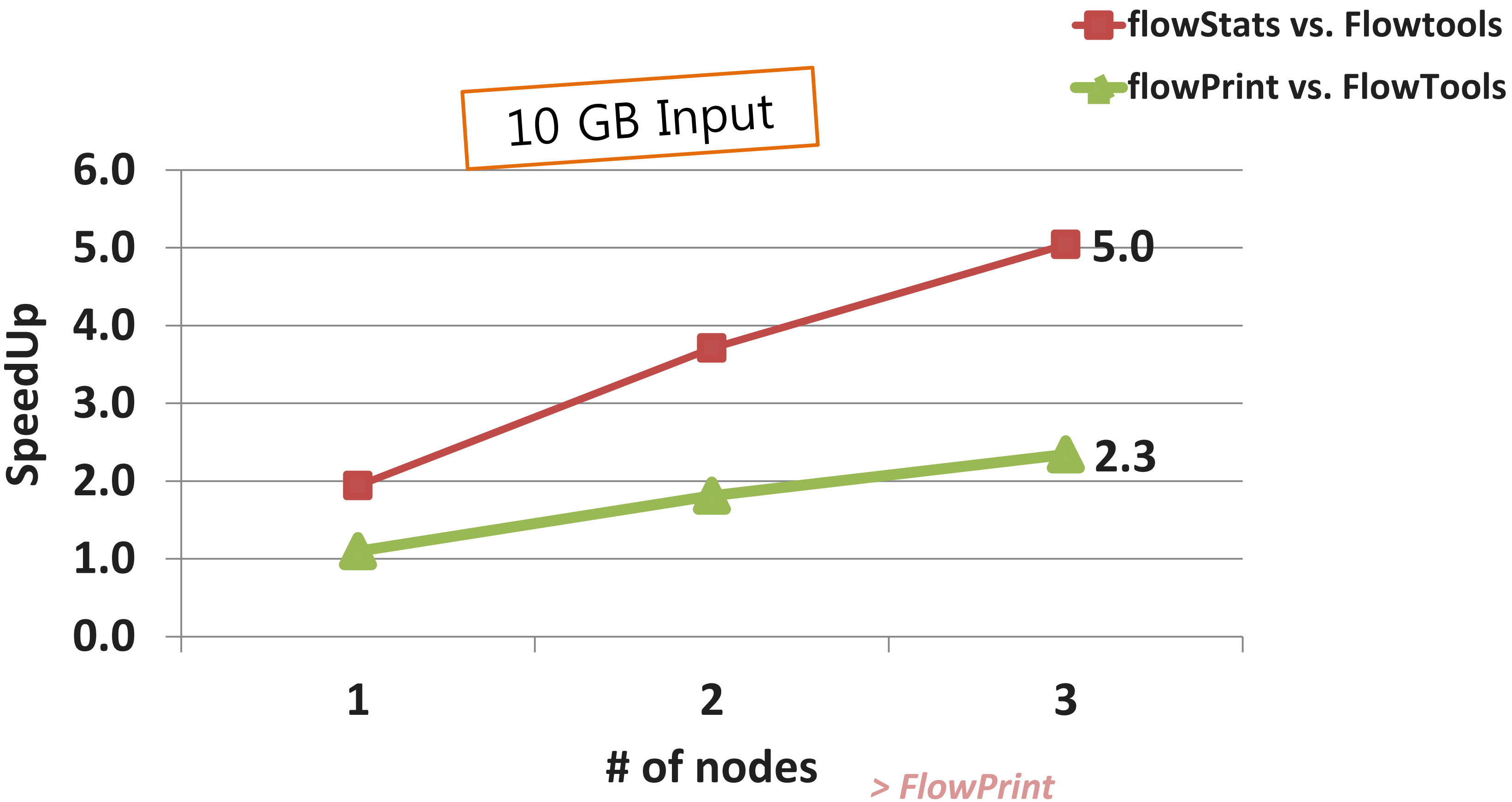
- Testbed

Type	Nodes	Cores	CPU	Memory	HardDisk	Rack
Small	3	24	3.4 GHz 8 core	16 GB	2 TB	1 Rack
Medium	30	240	2.93 GHz 8 core	16 GB	4 TB	1 Rack
Large	200	400	2.66 GHz 2 core	2 GB	500 GB	4 Racks

- Data and MapReduce jobs

Type	Dataset	MapReduce Job	Testbed
NetFlow	1 TB from KOREN	flowStats, flowDetect, flowPrint	Small
Packet	1 ~ 5 TB from CNU campus N/W	IP, TCP, Web (webpop, User Behavior, DDoS)	Medium, Large

NetFlow: SpeedUp (vs. Flowtools)



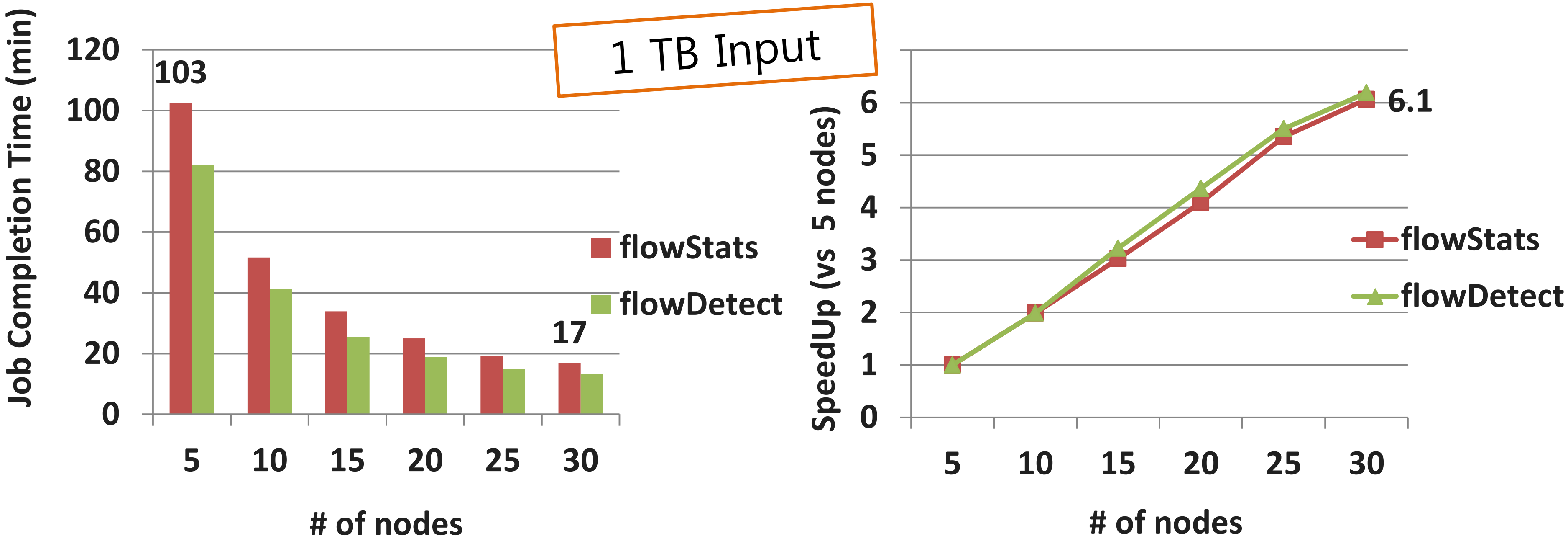
> FlowPrint

```
flow-cat -p flowfile |flow-print –f14
```

> FlowStats

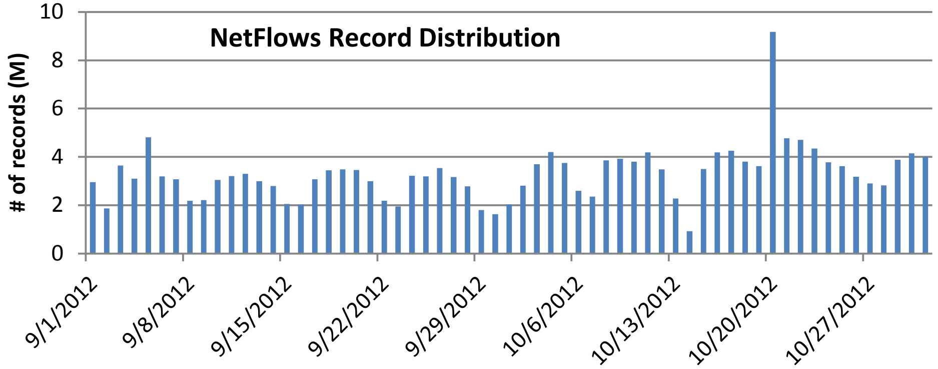
```
flow-cat -p flowfile|flow-stat -f12
flow-cat -p flowfile|flow-stat –f5
```

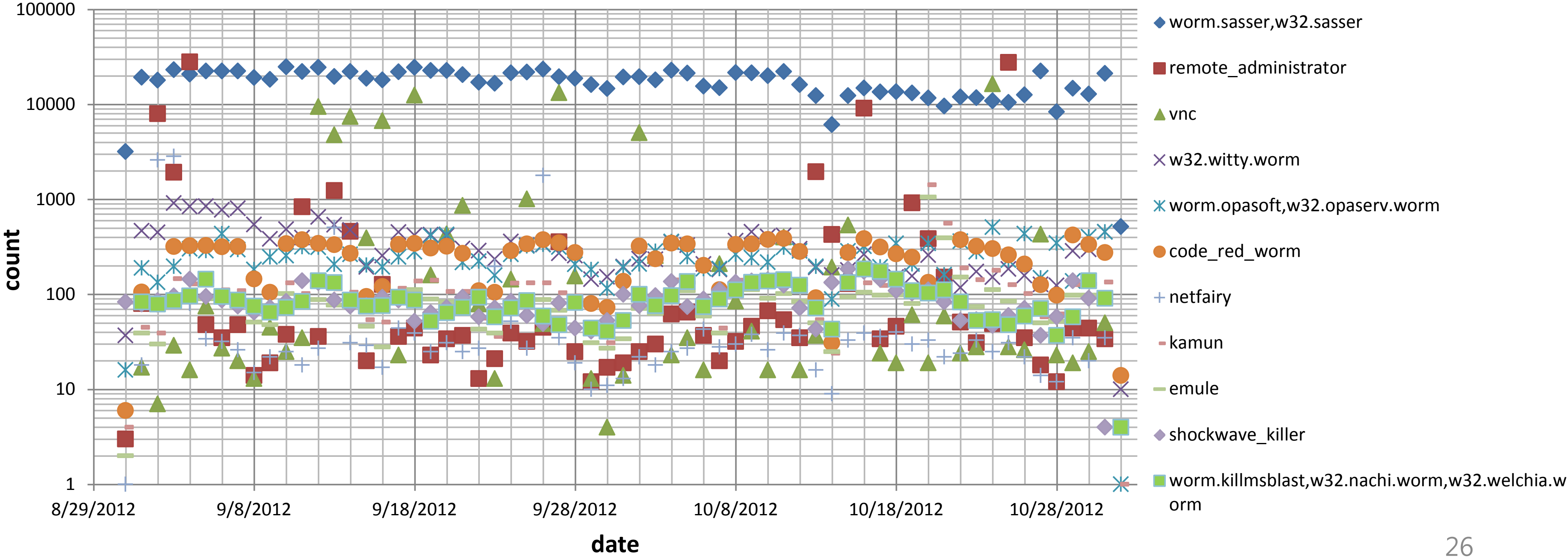
NetFlow: Scalability



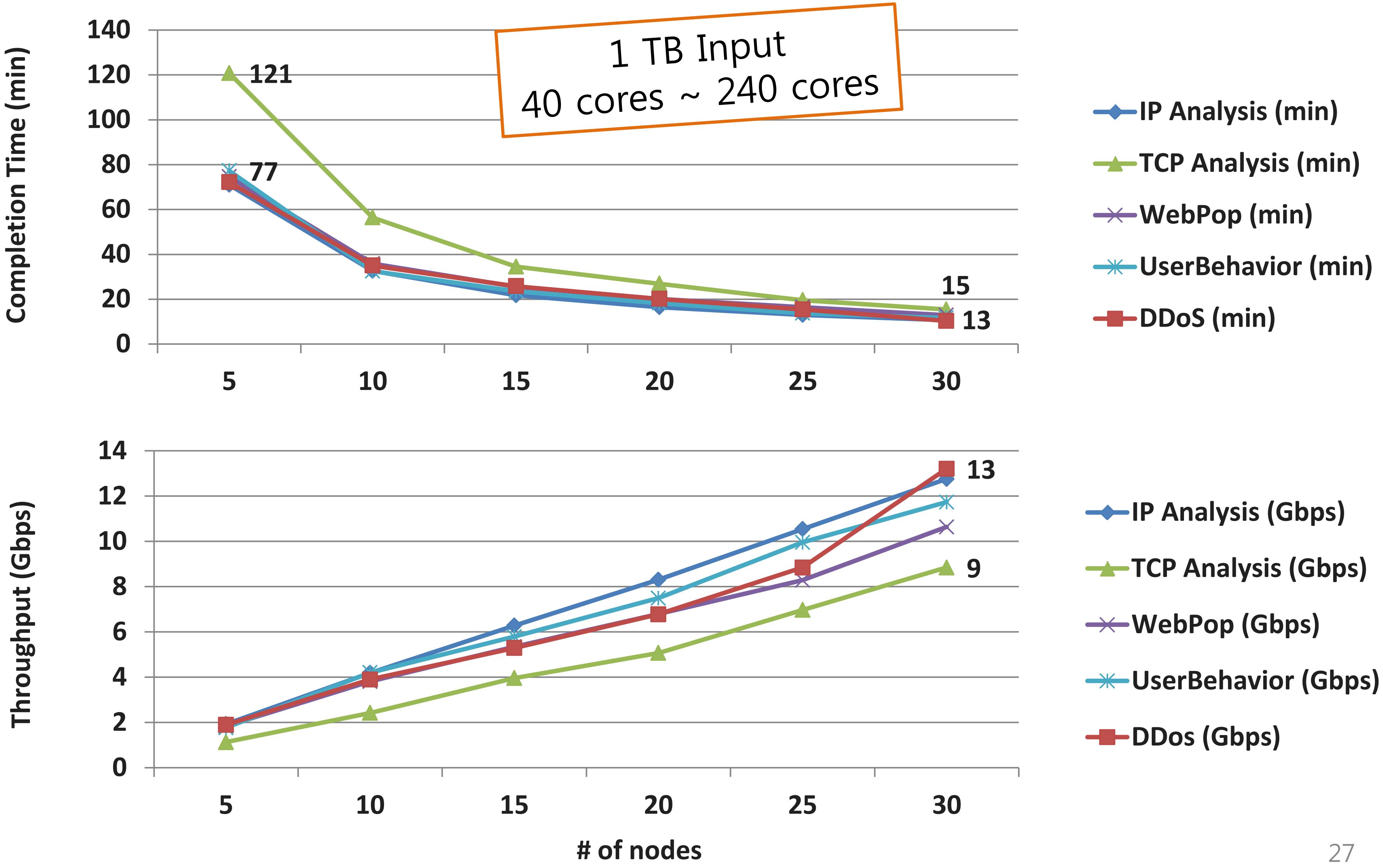
1 TB Input

NetFlow: Pattern Matching Result

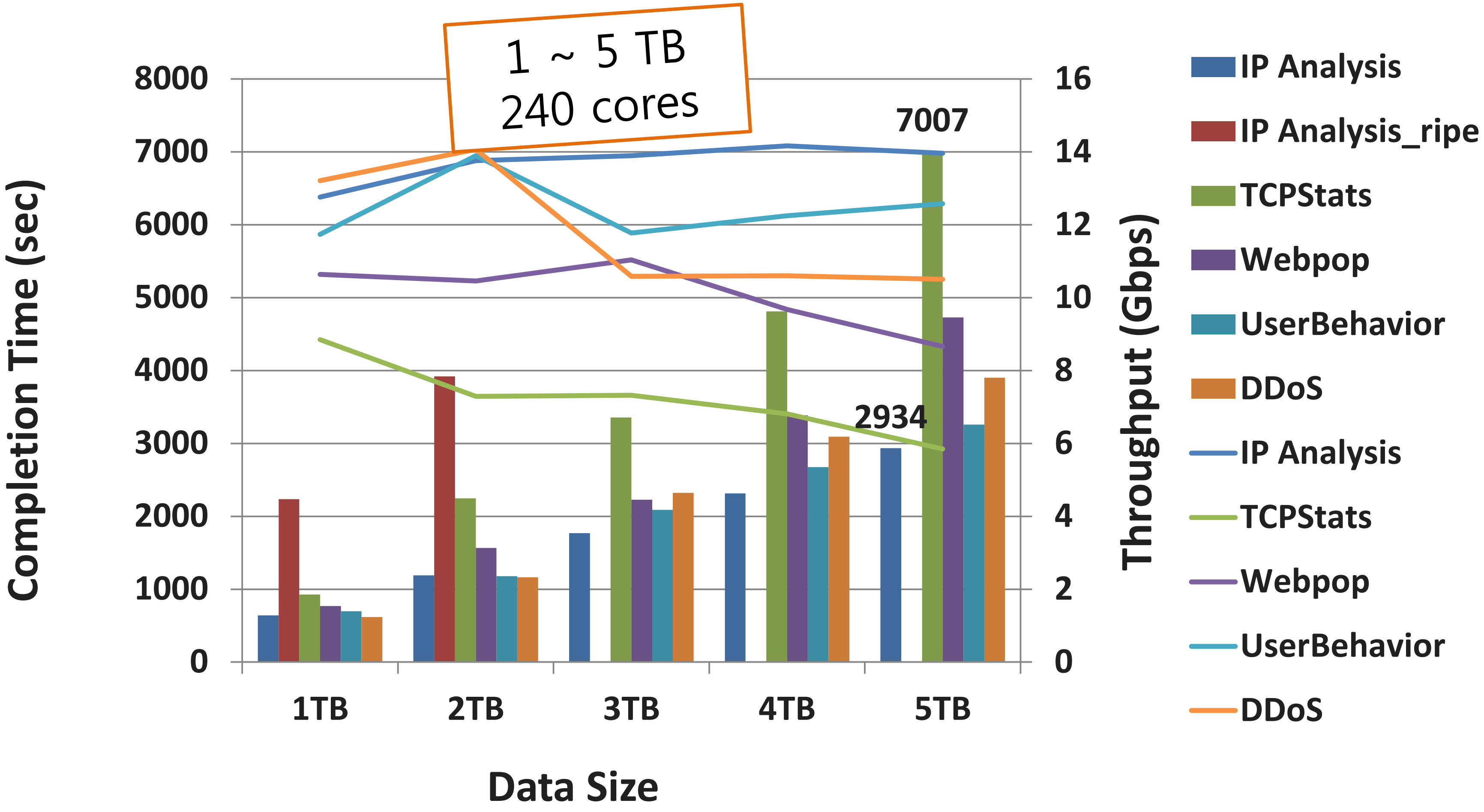




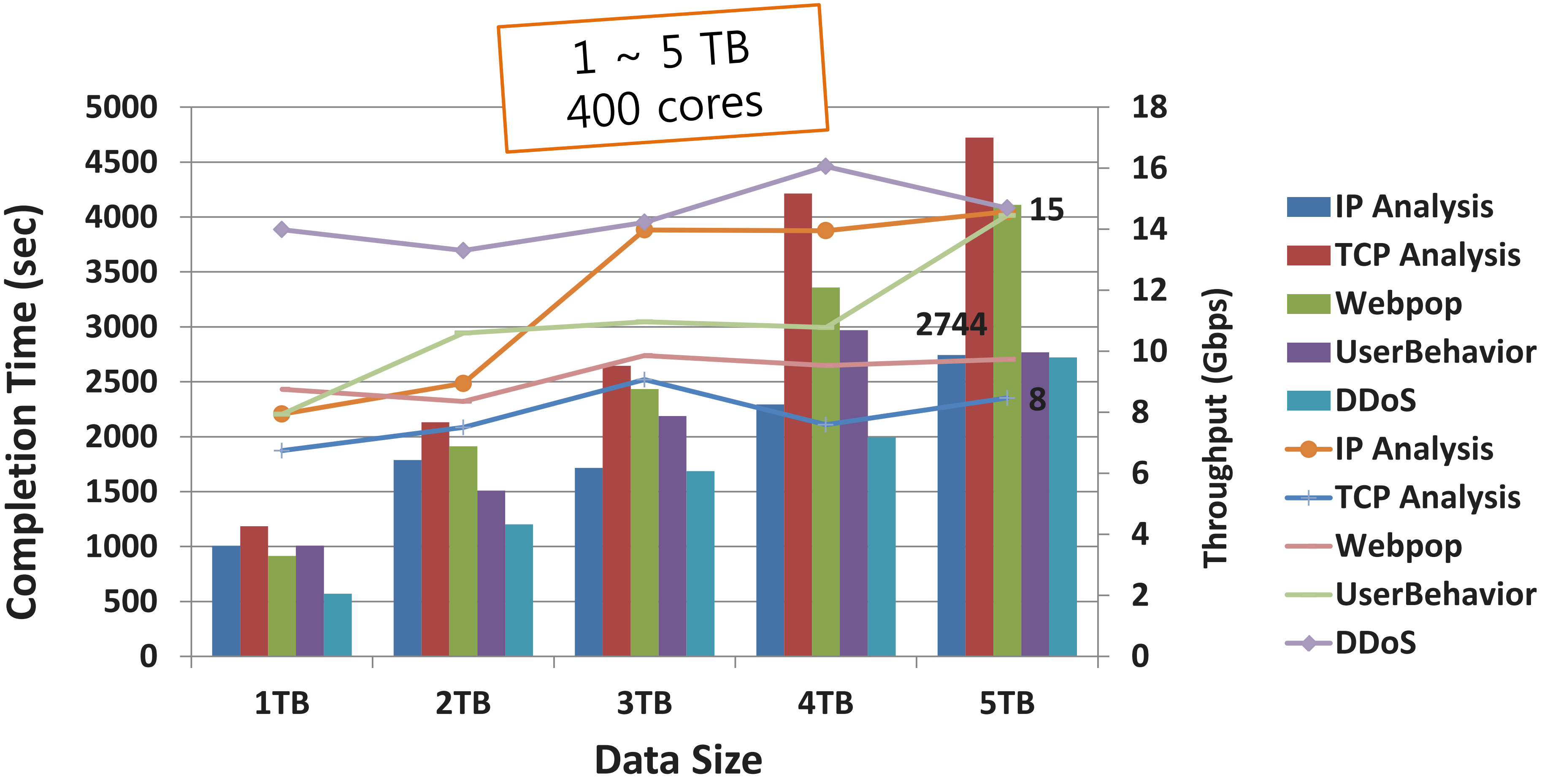
Packet: ScaleOut


1 TB Input
40 cores ~ 240 cores

Packet: SizeUp (30 nodes)



Packet: SizeUp (200 nodes)



SUMMARY

Summary

- NetFlow analysis with Hadoop
  - NetFlow v5 processing module
  - MapReduce algorithms: statistics

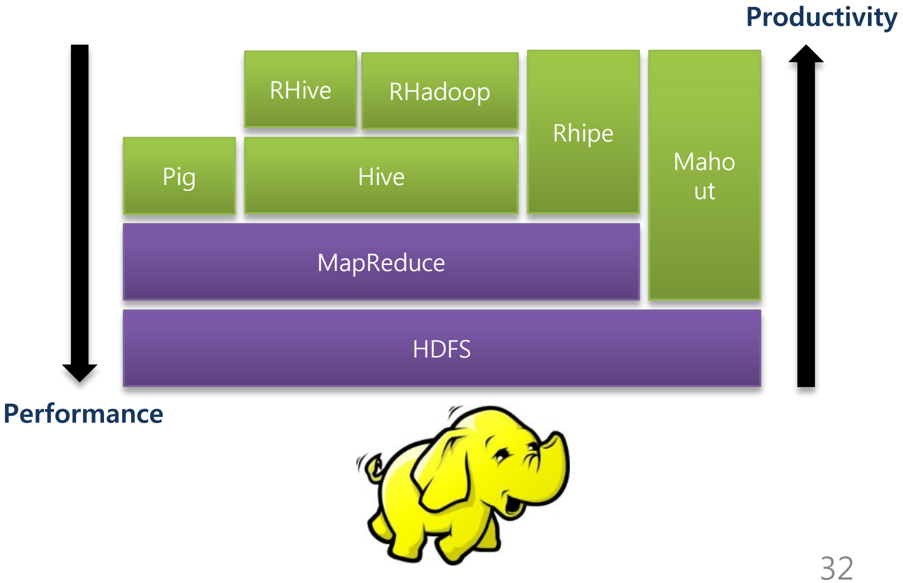
- Distributed computing and storage with Hadoop
  - Fits Internet measurement application
  - Scalability

- Source codes are available at
  - Packet, NetFlow
  - https://sites.google.com/a/networks.cnu.ac.kr/dnlab/research/hadoop
  - https://github.com/ssallys/pcap-on-Hadoop

Ongoing Work

- Distributed real-time monitoring
  - Rule matching for Streamed NetFlow
  - Developing rule for MapReduce
  - Rule classification for dedicated rule matching
- Integration
  - Streaming packages
  - Enhanced analytics
    - Data mining: Mahout
    - Machine learning

- Scalable collection
  - E.g.) 10GE → 10 X 1 GE HDFS



Reference

- Papers

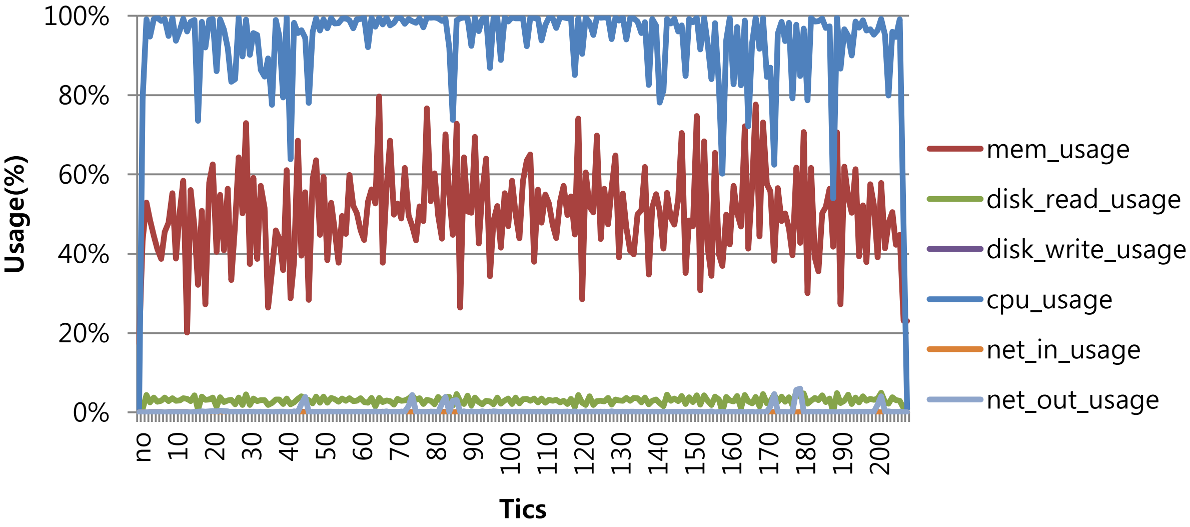
1. *Y. Lee and Y. Lee, "Toward Scalable Internet Traffic Measurement and Analysis with Hadoop," ACM SIGCOMM Computer Communication Review (CCR), Jan. 2013*
2. *Y. Lee, W. Kang, and Y. Lee, "A Hadoop-based Packet Trace Processing Tool," The Third TMA, April 2011*
3. *Y. Lee and Y. Lee, "Detecting DDoS Attacks with Hadoop", ACM CoNEXT Student Workshop, Dec, 2011*

- Software

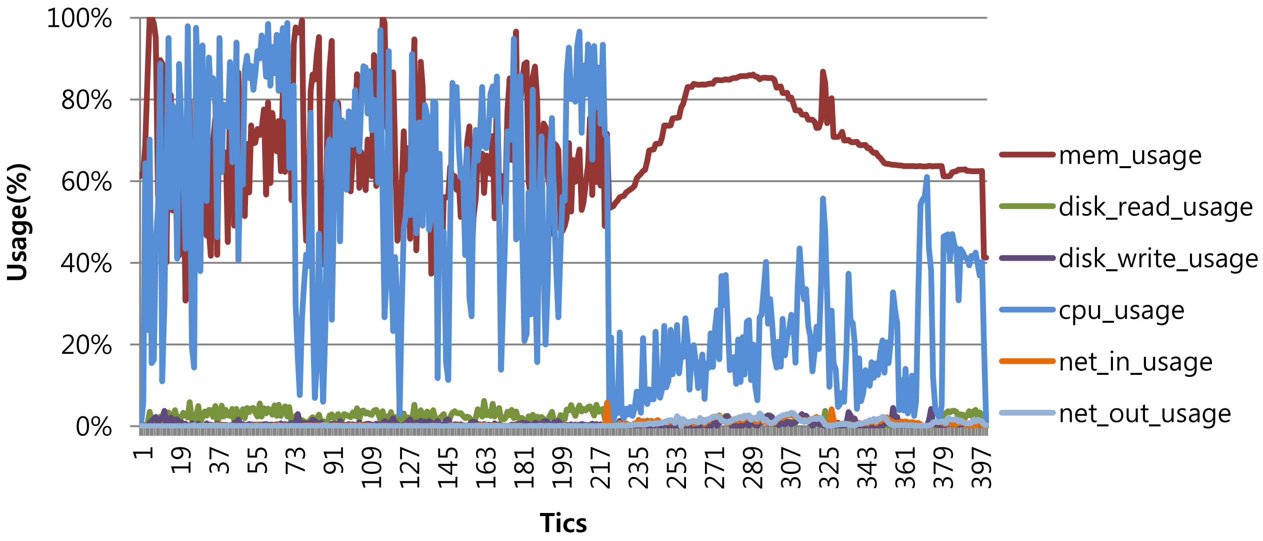
1. *http://networks.cnu.ac.kr/~yhlee*
2. *https://sites.google.com/a/networks.cnu.ac.kr/dnlab/research/hadoop*
3. *https://github.com/ssallys/pcap-on-Hadoop*

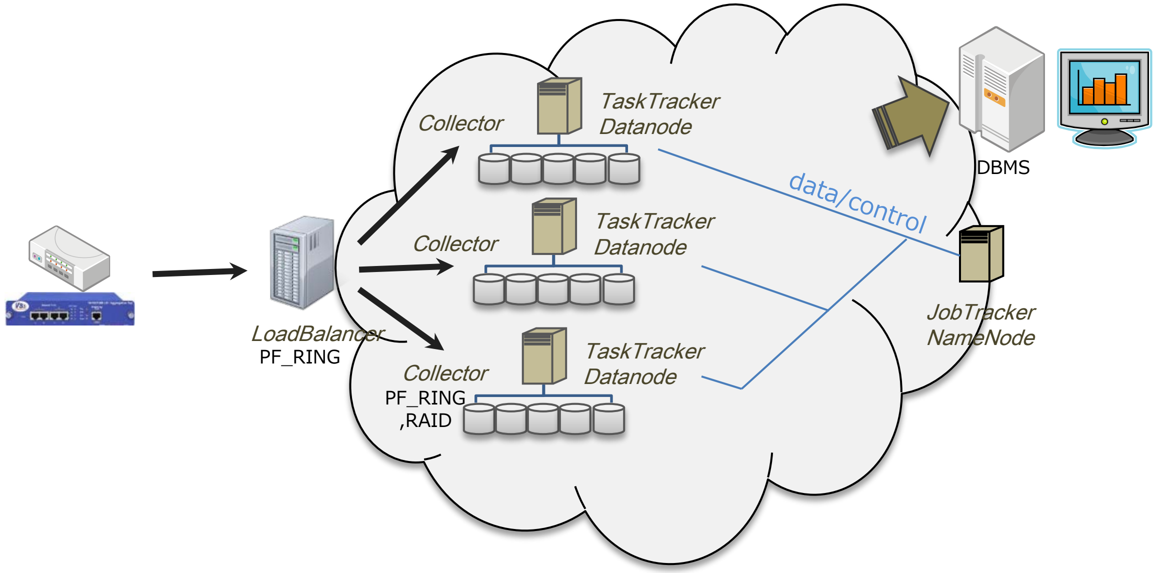
THANK YOU !

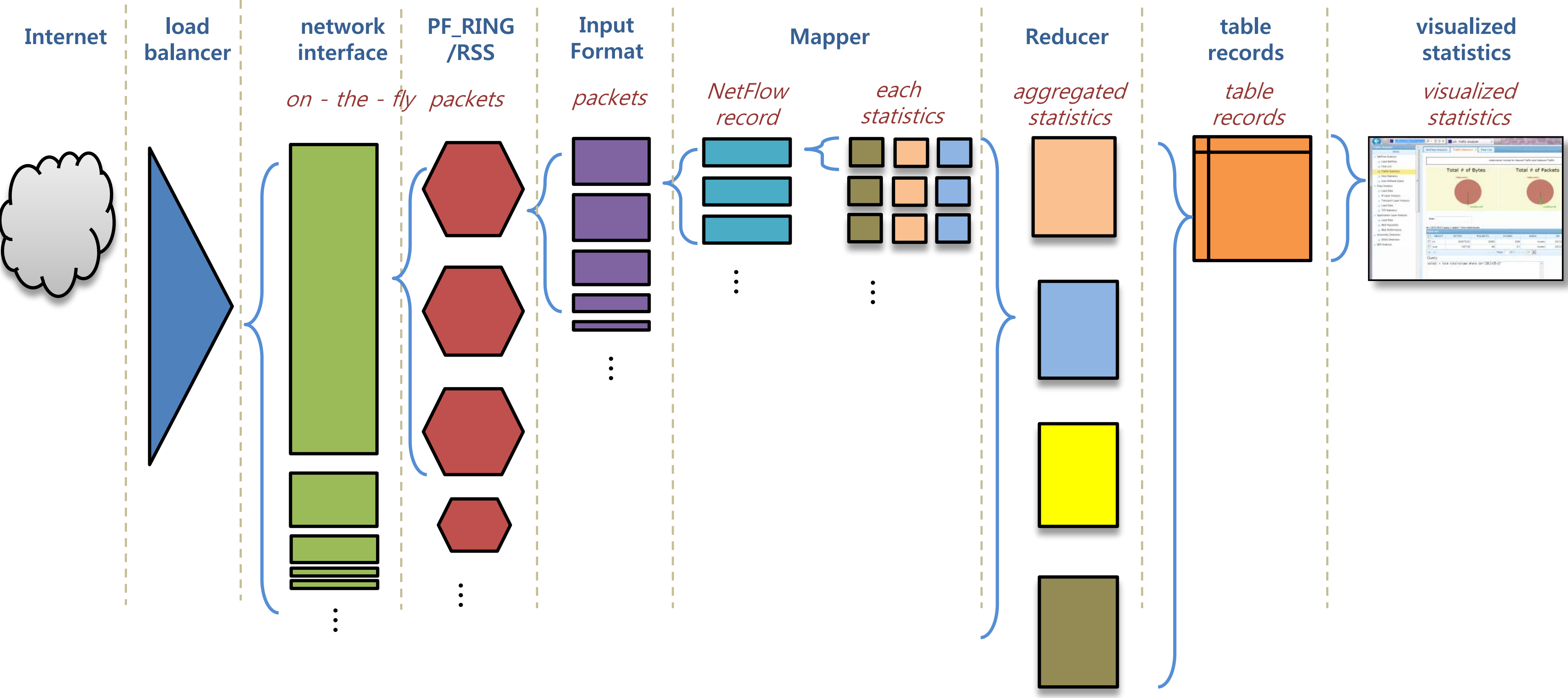
IP Analysis



TCP Analysis




Collector
TaskTracker
Datanode
Collector
TaskTracker
Datanode
LoadBalancer
PF_RING
Collector
PF_RING
,RAID
TaskTracker
Datanode
data/control
DBMS
JobTracker
NameNode



rule name; filter pattern; mapout key; patition&groupsort key;detection condition; action

ex)
port_scan;ip,proto=6;srcip,dstport;srcip;pkts=20-
syn_flood;ip,proto=6,syn-fin=1-;srcip,dstip;srcip,dstip;syn-fin=6-