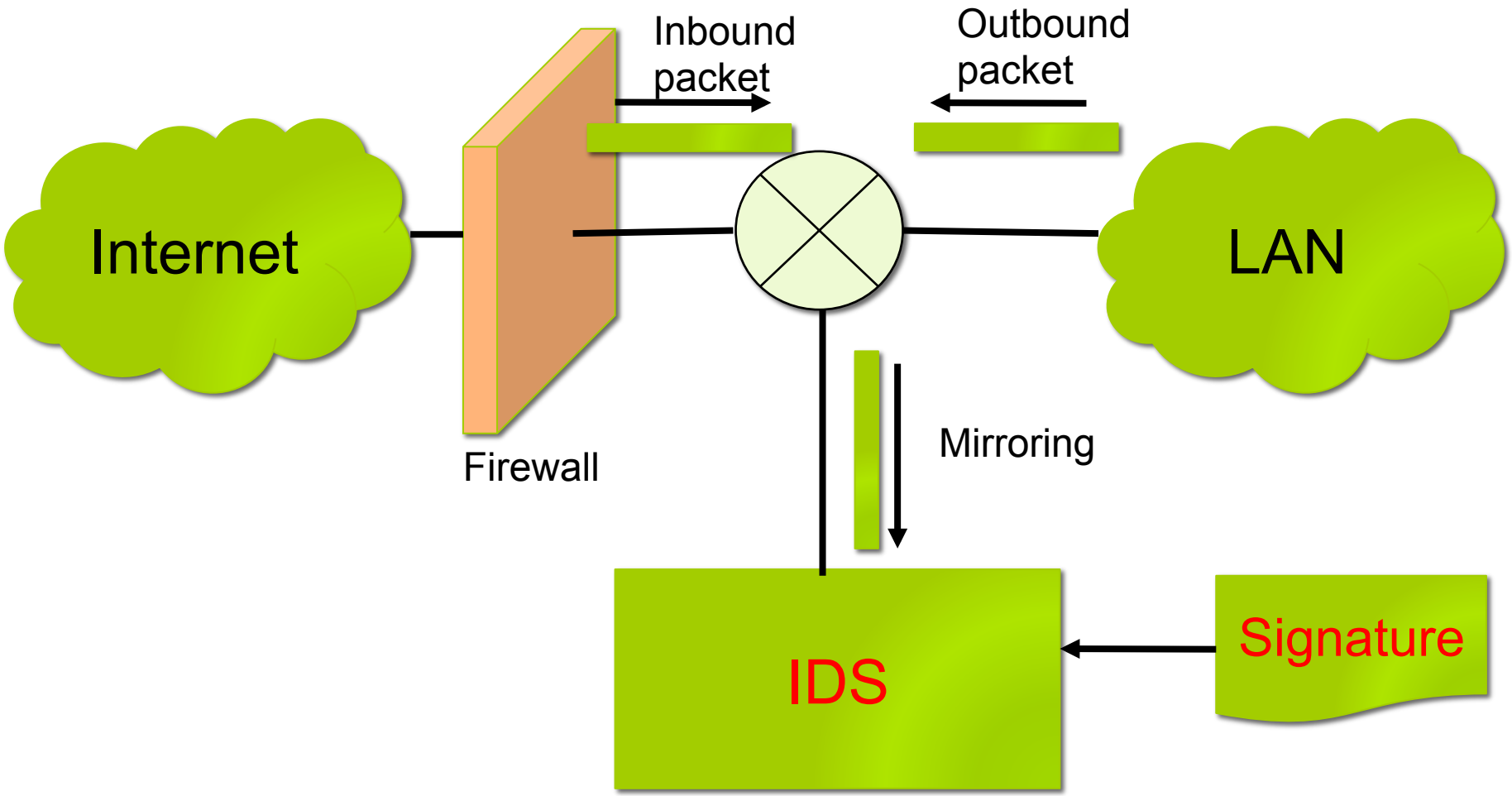
A Latency Reduction Technique for Network Intrusion Detection System on Multicores

Keiji Kimura, Shohei Yamada, Hironori Kasahara
Waseda University

Introduction

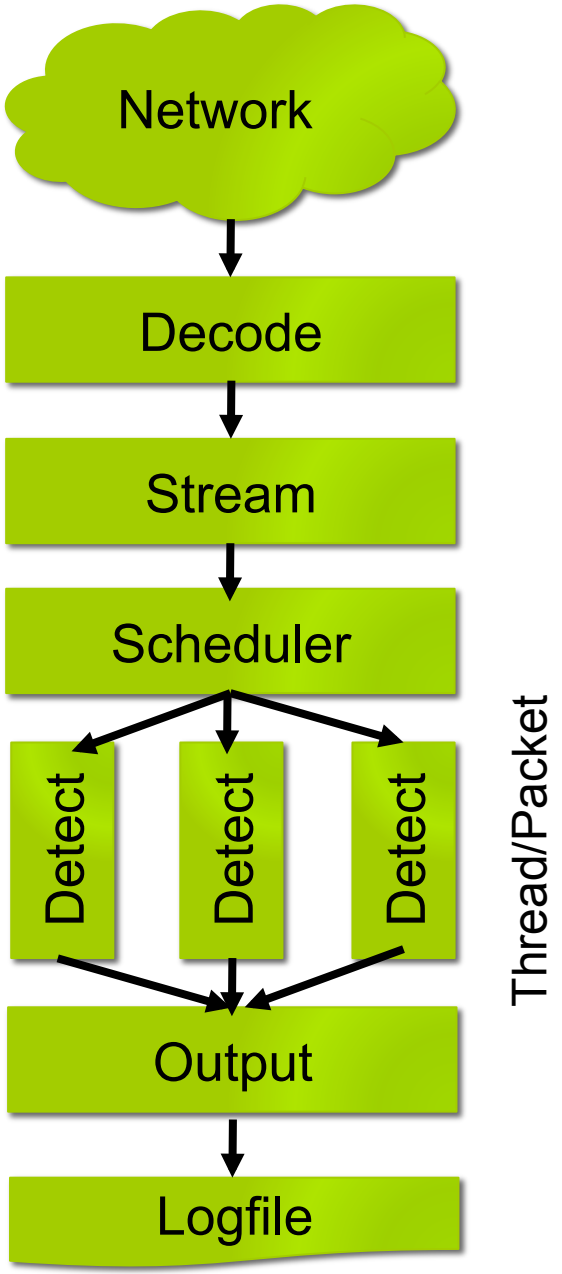
- Network is connecting everything.
  - Servers, Phones, Vehicles, Sensors, …
- Network security threat has been more serious than before.
  - Old days: Only administrator must take care of it.
  - Today: Everyone must take care of it.
- Intrusion Detection System (IDS)
  - Protecting against inbound/outbound attacks
  - **Low-power and High-performance** will be required for future IDSs.
    - Use Multicores more efficiently!
- Multicore for IDS
  - Today: Throughput oriented (Multiple packets at a time)
  - This talk: Latency oriented
    - **Signature (Rule) based parallel processing**

Overview of IDS (NIDS)



Suricata

- Open Source IDS (2010-)
  - Funded by the Department of Homeland Security's Directorate for Science and Technology in USA
- Packet Pipeline
  - Decode: convert packets into intermediate data structure
  - Stream: packets are reassembled as a stream
  - Detect: detect treats by rule matching
  - Output: make alert
- Throughput Oriented Architecture
  - Packet level parallelism



Signature (Rule) Decomposition

- Signature Classification
  - HTTP header inspection
  - Payload inspection
  - Others
    - threshold-check
    - app-layer-event
    - flag-check
    - byte-test
    - decode-event
    - csum-check
    - stream-event
    - other-event

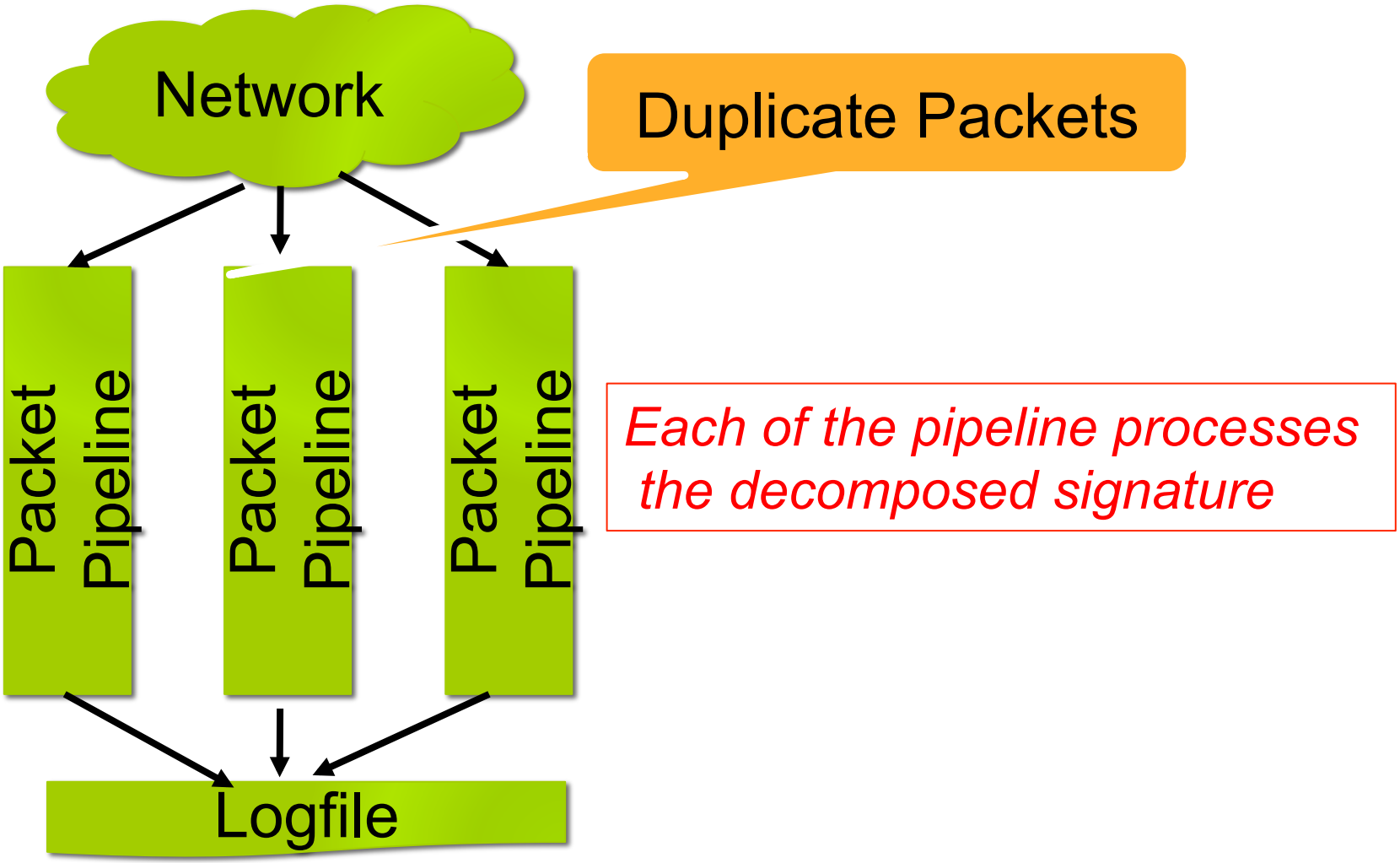
Parallel processing among these signatures is efficient.

Parallel processing among these categories is efficient.

Scheduling these three categories and signatures in "Others" according to the profile data.

cf. – Haiyang Jiang, et al., "Load Balancing by Ruleset Partition for Parallel IDS on Multi-Core Processors", ICCCN 2013
– Zhuojun Zhuang, et al., "A Resource Scheduling Strategy for Intrusion Detection on Multi-Core Platform", IFIP ICNPC 2008

Multi-pipelined Suricata



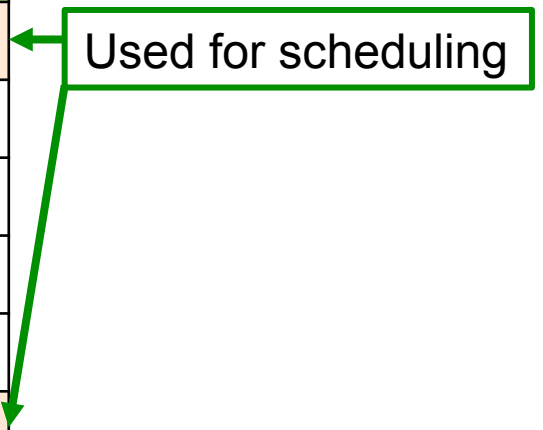
Preliminary Evaluation

- Processing Trace Data on a Local HDD
  - Xeon L5630 (@2.13GHz*4core)
    - Evaluate on 2, 3, 4 cores
      - 1core for control thread
  - Suricata 1.4.5
    - Original vs. Multi-pipelined
    - Compare total execution time
  - Rule-set: emerging-rules (Sep. 1st, 2013)
    - 13,799 signatures

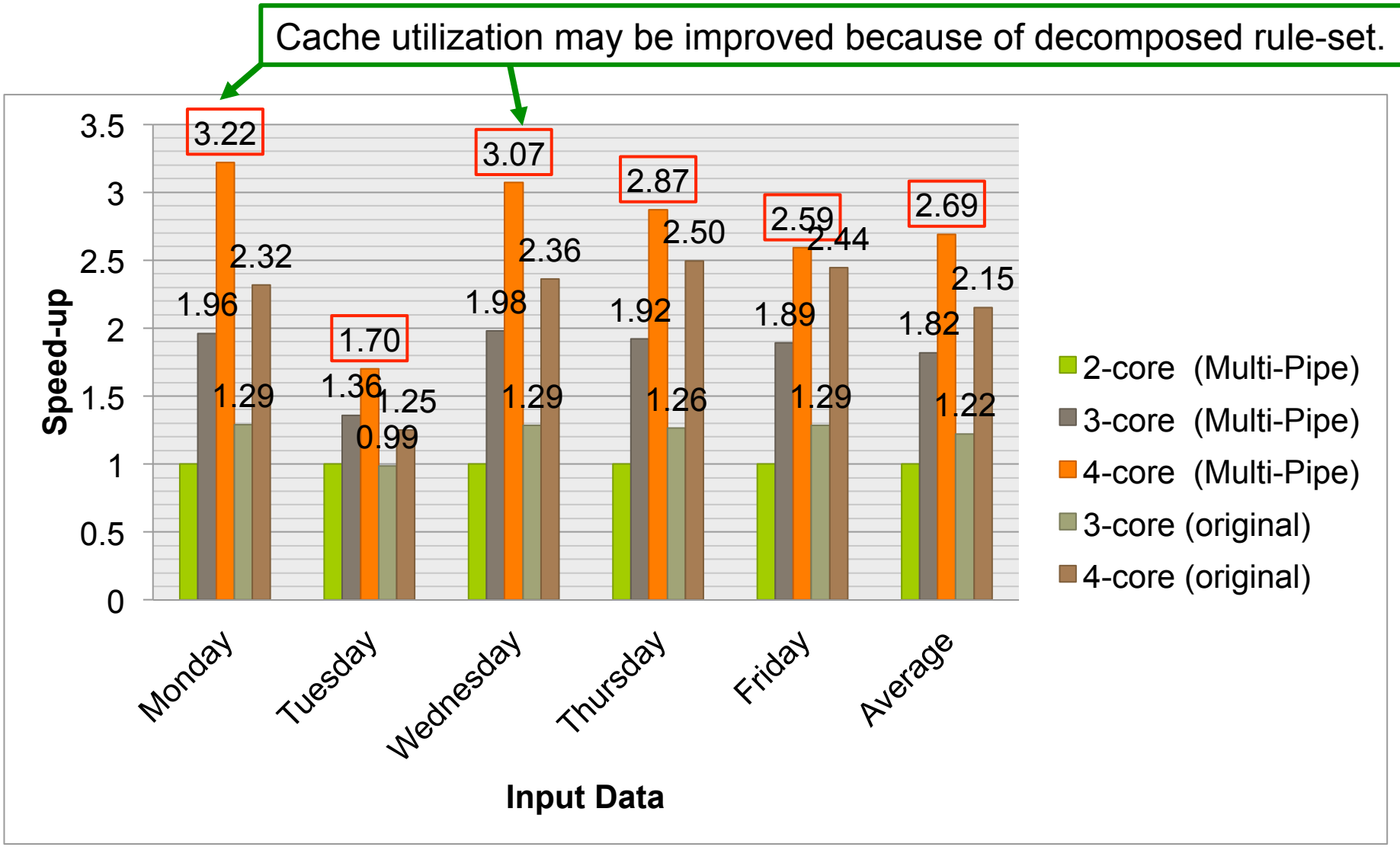
Evaluated Trace Data Set

- DARPA Intrusion Detection Evaluation Data Set (5th week, 1999)
  - Large Processing Cost for HTTP Header Inspection
- Lab. Data (from our lab., Jan, 2014)
  - Large Processing Cost for Other Inspection (than HTTP and Payload)

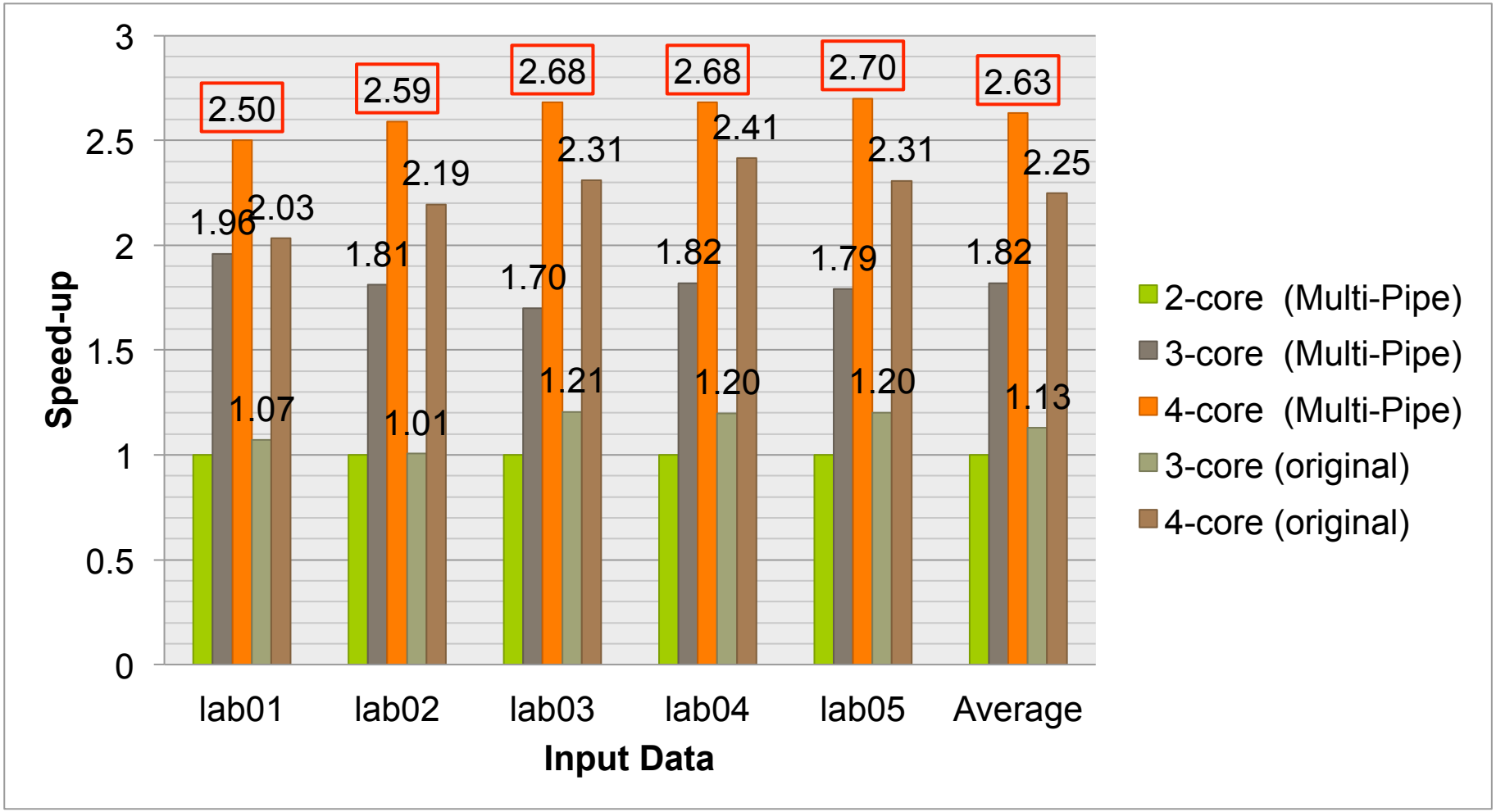
Data Set	Data	# of Packets	Size (MB)
DARPA data set	Monday	3,667,917	783
	Tuesday	5,962,053	899
	Wednesday	3,473,044	800
	Thursday	5,509,639	1,350
	Friday	6,045,505	1,920
Lab. data set	lab01	1,669,404	999
	lab02	5,615,310	2,920
	lab03	3,403,158	1,950
	lab04	5,577,077	2,920
	lab05	5,270,379	2,920



Speed-up on DARPA Data



Speed-up on Lab. Data



Conclusion

- Process Latency Reduction Technique for IDS on Multicores
  - Rule (Signature) based Parallel Processing
  - Decompose rule-set considering characteristics of each rule
- Evaluation of Multi-pipelined Suricata on 4-cores
  - 1-core for control thread, 3-core for detection threads
  - x2.69 speed-up for DARPA dataset against 2-cores
  - x2.63 speed-up for Lab. dataset against 2-cores
- Future topics
  - Evaluation on Network Environment
  - Hierarchical Parallel Processing
    - Latency oriented and Throughput oriented
    - Considering Available Resources and Processing Load
  - Power Optimization