ANCS 2007, 3-4-December 2007

Enhancing interoperability and stateful analysis of cooperative network intrusion detection systems

Michele Colajanni, Daniele Gozzi and
Mirco Marchetti

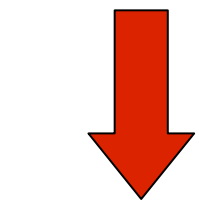
Department of Information Engineering
University of Modena and Reggio Emilia

Network Intrusion Detection System

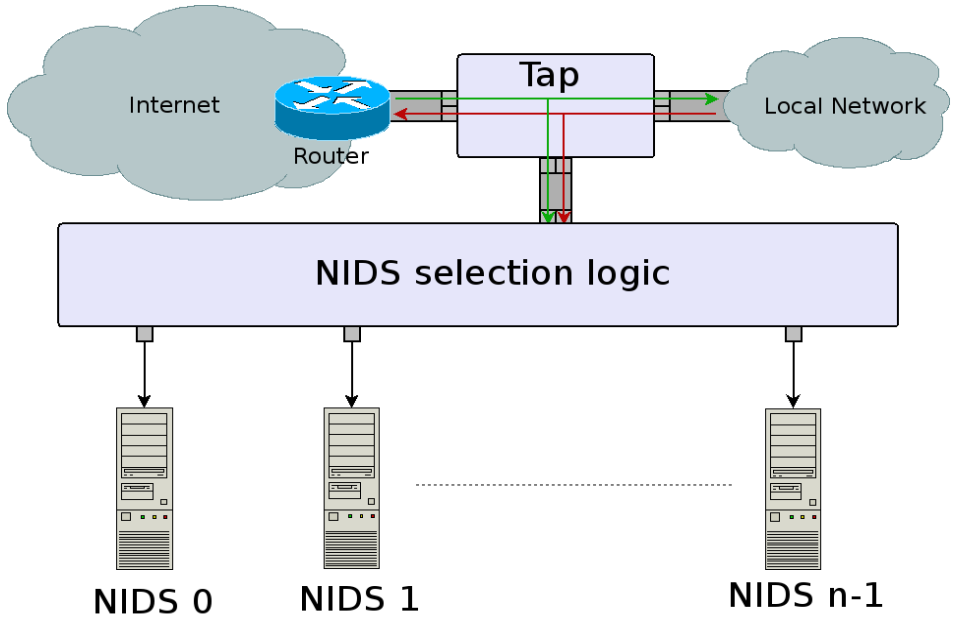
- Analyzes network traffic
  - looks for illicit activities (intrusions)
  - emits alerts
- Stateful signature analysis
  - common approach in many NIDS
  - connection tracking, reordering and reassembling
  - counters insertion and evasion attacks [Ptaceck, Newsham]

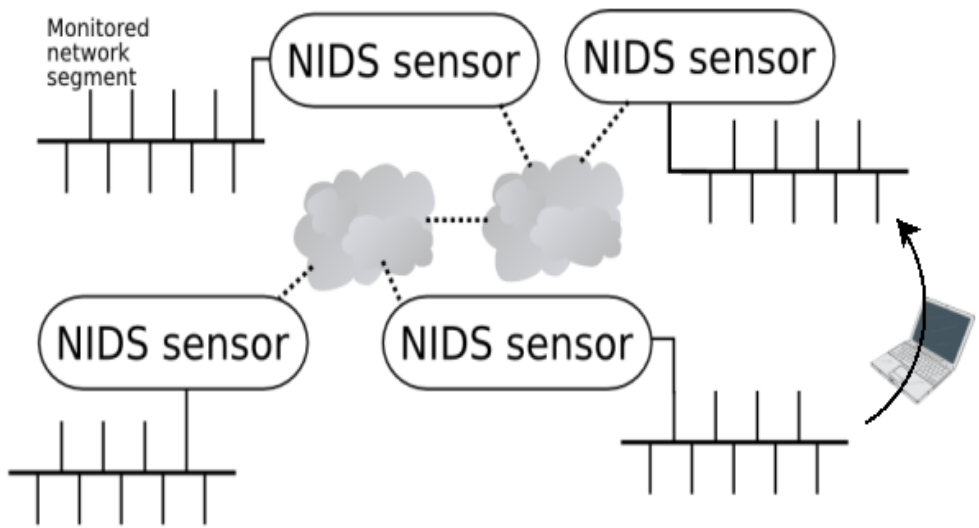
NIDS architectures in modern networks

- Increasing link bandwidth
- Complex/evolving network topologies
- Parallel (redundant) network links
- Mobile nodes



Parallel and distributed NIDS architectures are required...





Evading stateful analysis

- ... but sensors do not distribute their state
  - state is maintained by a single sensor
  - sensor needs all the packets belonging to the same connection
- How to evade stateful analysis:
  - split the connection over links analyzed by different NIDS sensors
  - eg, parallel NIDS cluster with load balancing
  - eg, connection to/from mobile nodes

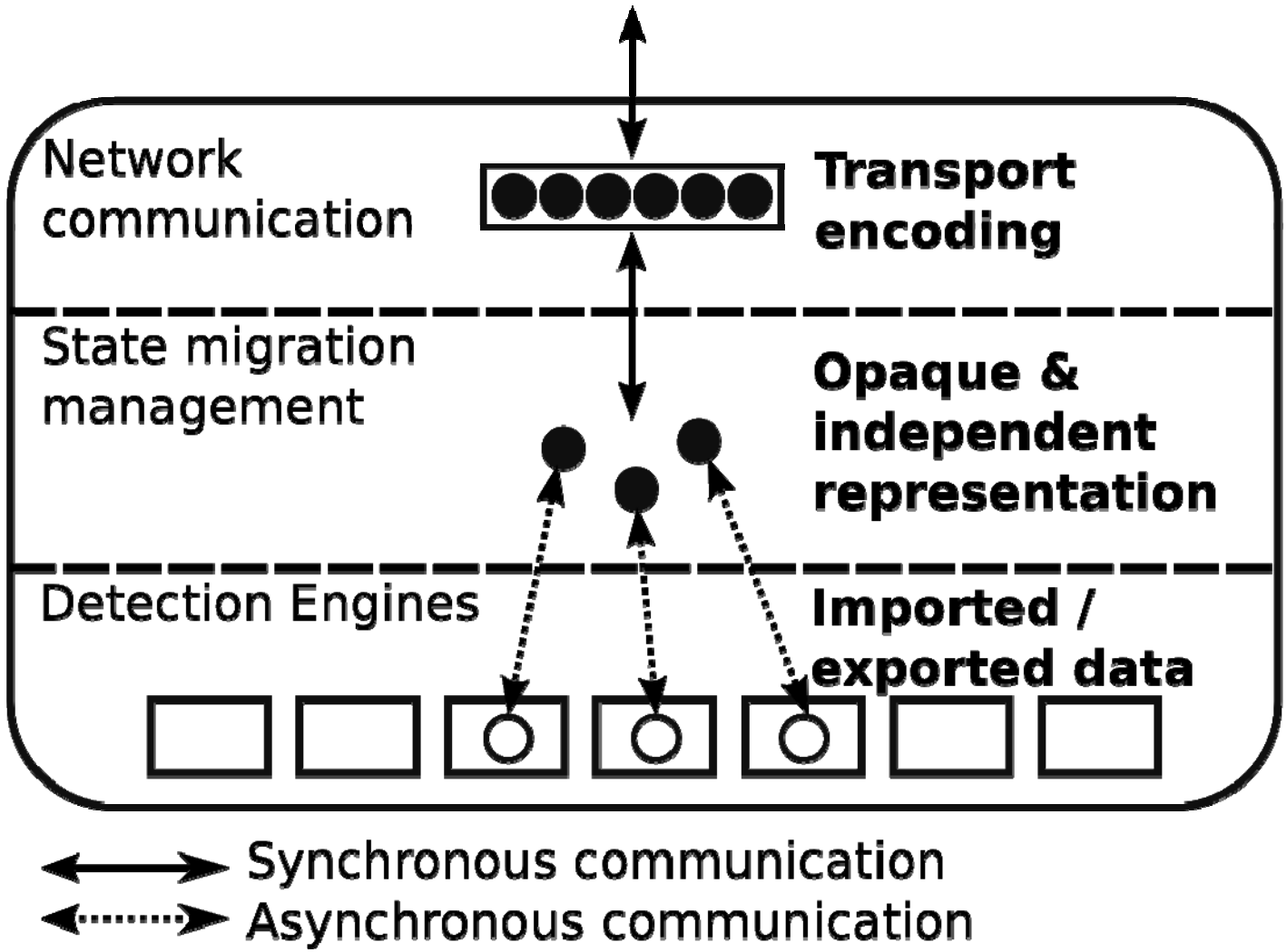
Solution: NIDS cooperation

- Cooperative NIDS state management
  - each NIDS builds its partial state
  - sensors cooperation by partial state exchange
  - partial states merged to obtain the state
- Challenges:
  - sensor communication
  - partial state management
- Requirements:
  - low detection delay
  - unmodified detection rate

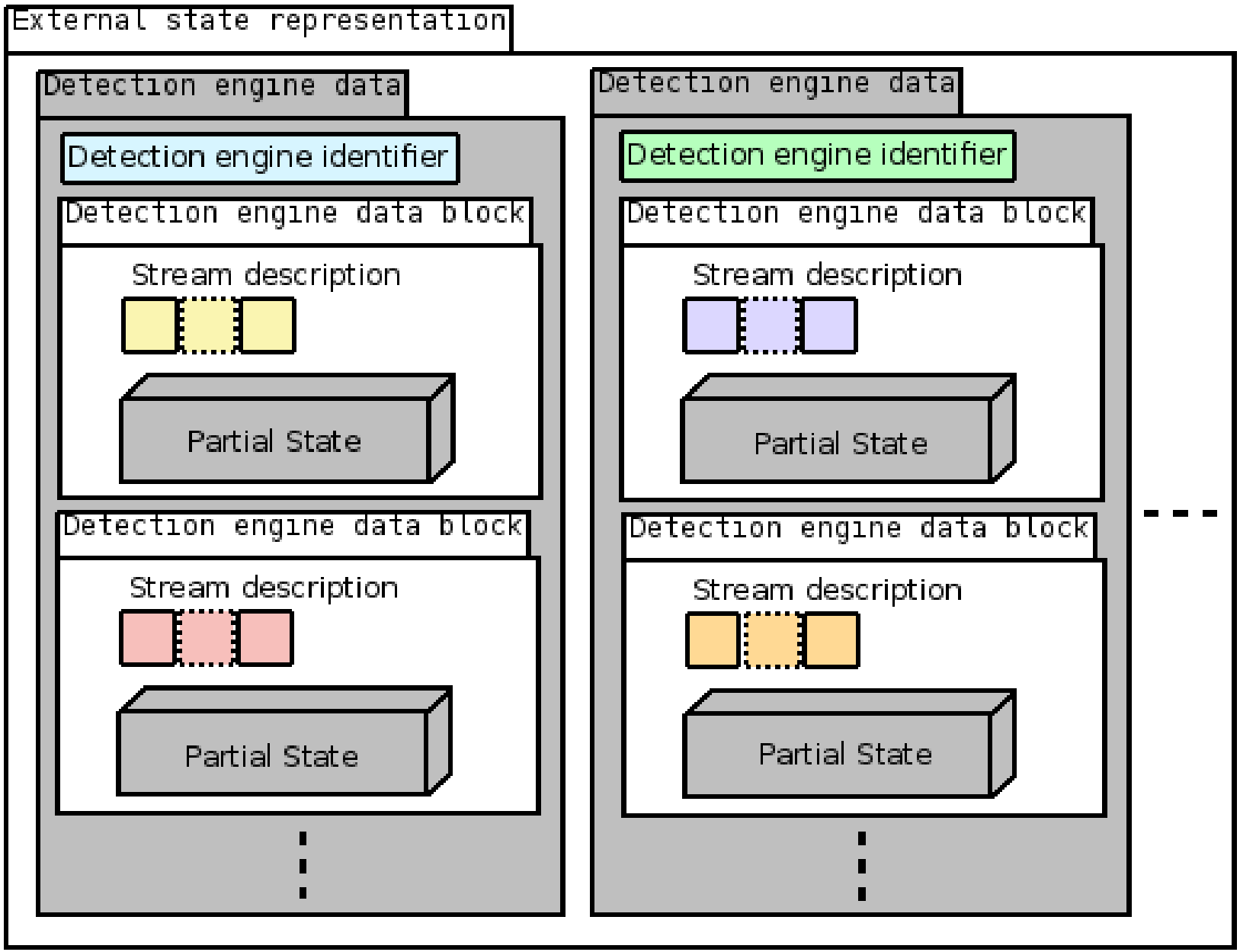
Our contributions

- Definition of a state migration framework
  - generally applicable
- Definition of an external state representation
  - easy to extend (new detection engines)
- Reference implementation
  - demonstrate viability
- Performance evaluation
  - meets delay and detection rate requirements

State migration framework

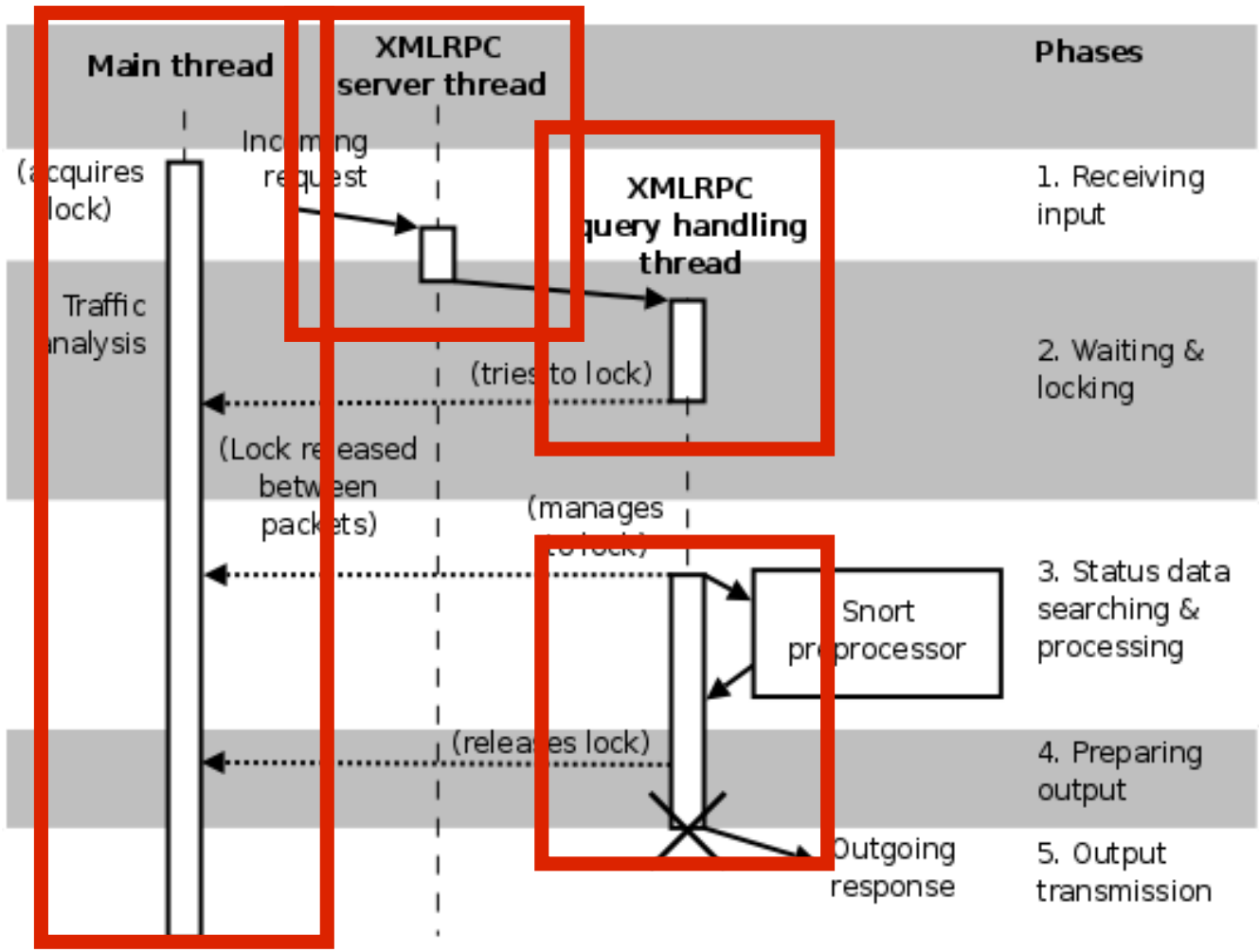


External state representation



Reference implementation

- Patch against Snort 2.6.1.1
- Multithread
- Stream4 preprocessor



Experiment summary

- Prototype validation
  - detection of splitted attacks
- Low performance overhead
  - avoid packet loss
- Low state migration delay
  - compatible with live signature based analysis

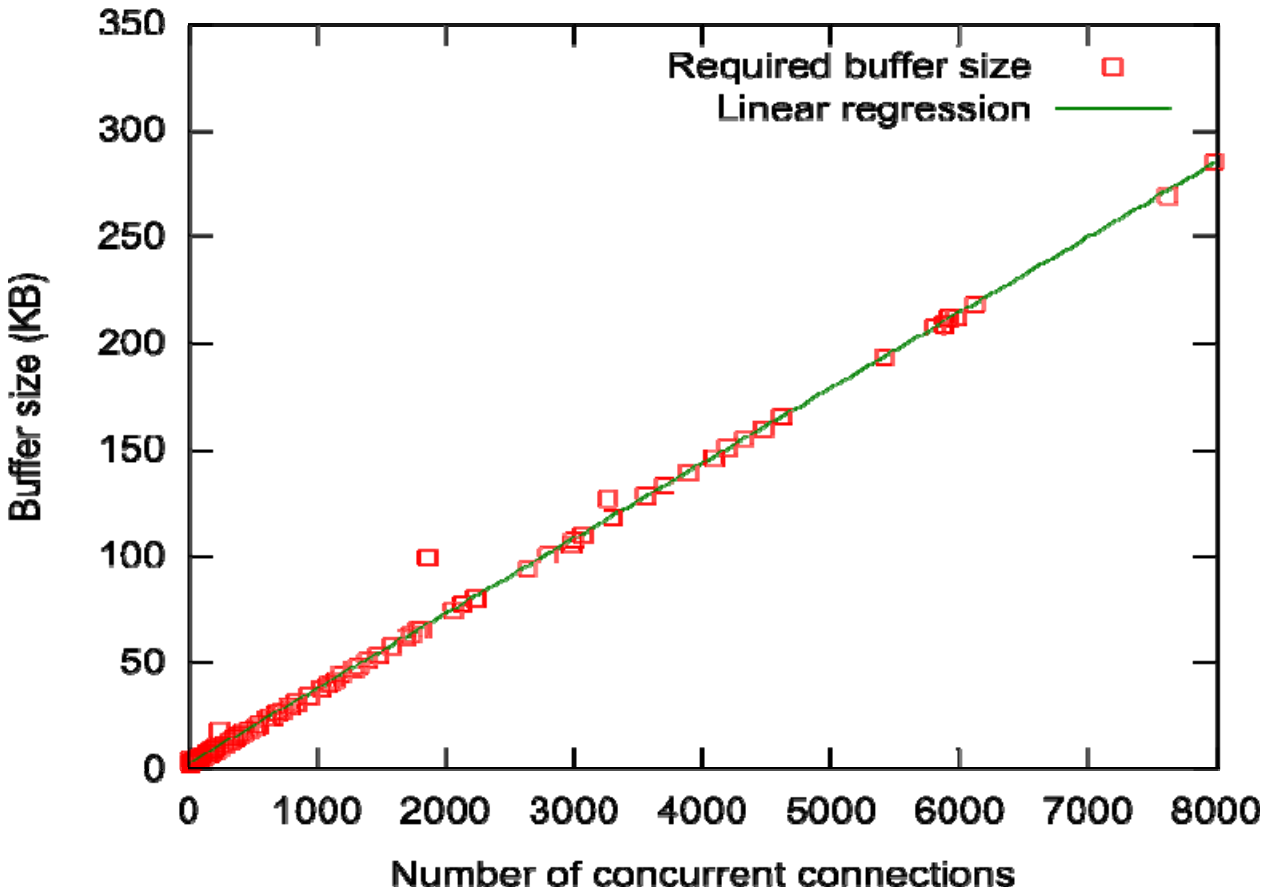
Prototype validation

Known network attack splitted in two parts

1. send the first part of the attack to the first sensor
2. merge the first sensor state with the second sensor state
3. send the second part of the attack to the second sensor

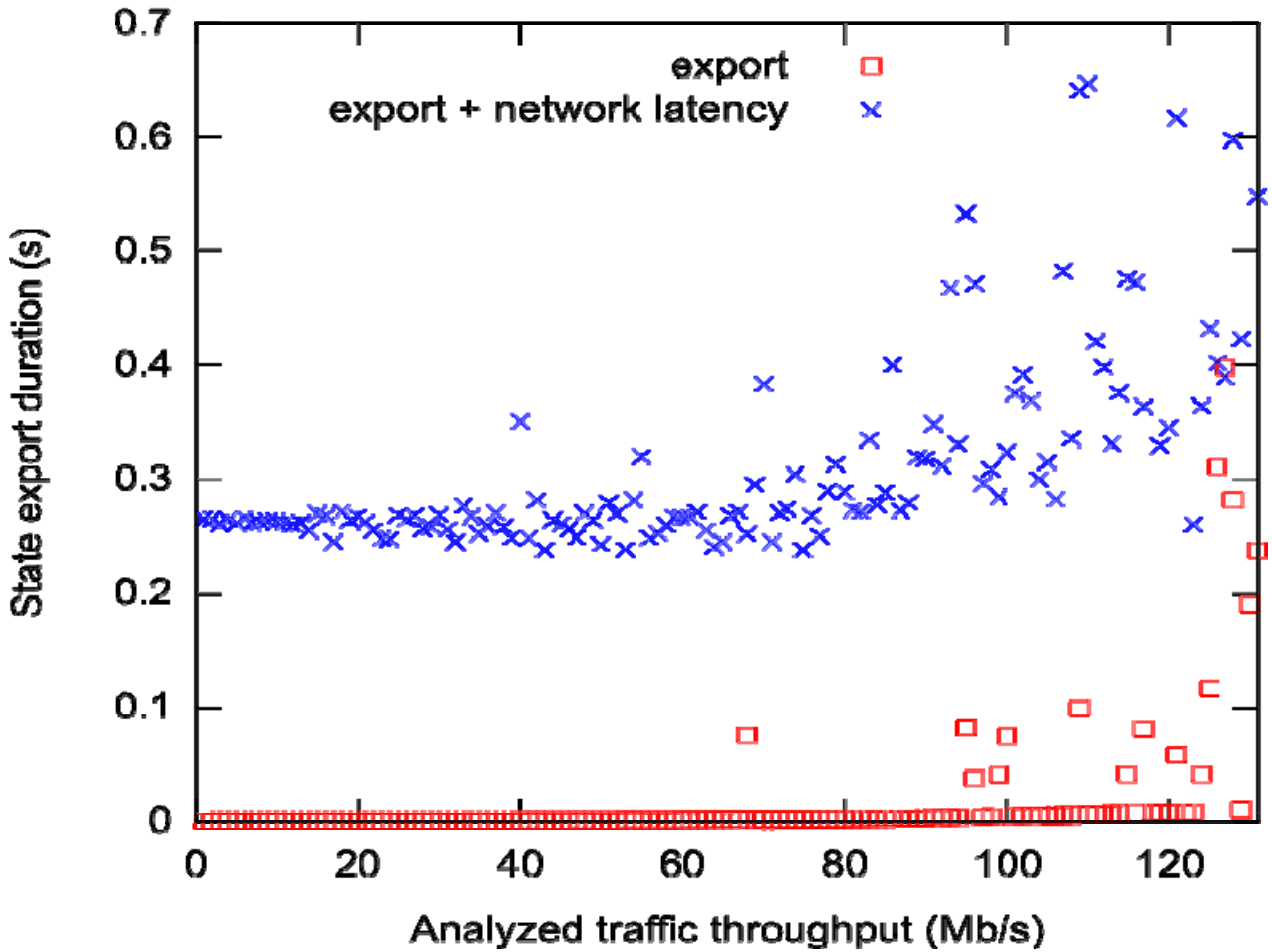
- The second sensor correctly detects the attack
  - order independent (2 and 3 can be swapped and/or overlapped)
  - loose synchronization required

Performance overhead



- 300 KB buffer prevents packet loss (200Mb/s link)
  - internal state locked for less than 0.012 sec
  - compatible with live traffic analysis

State migration delay

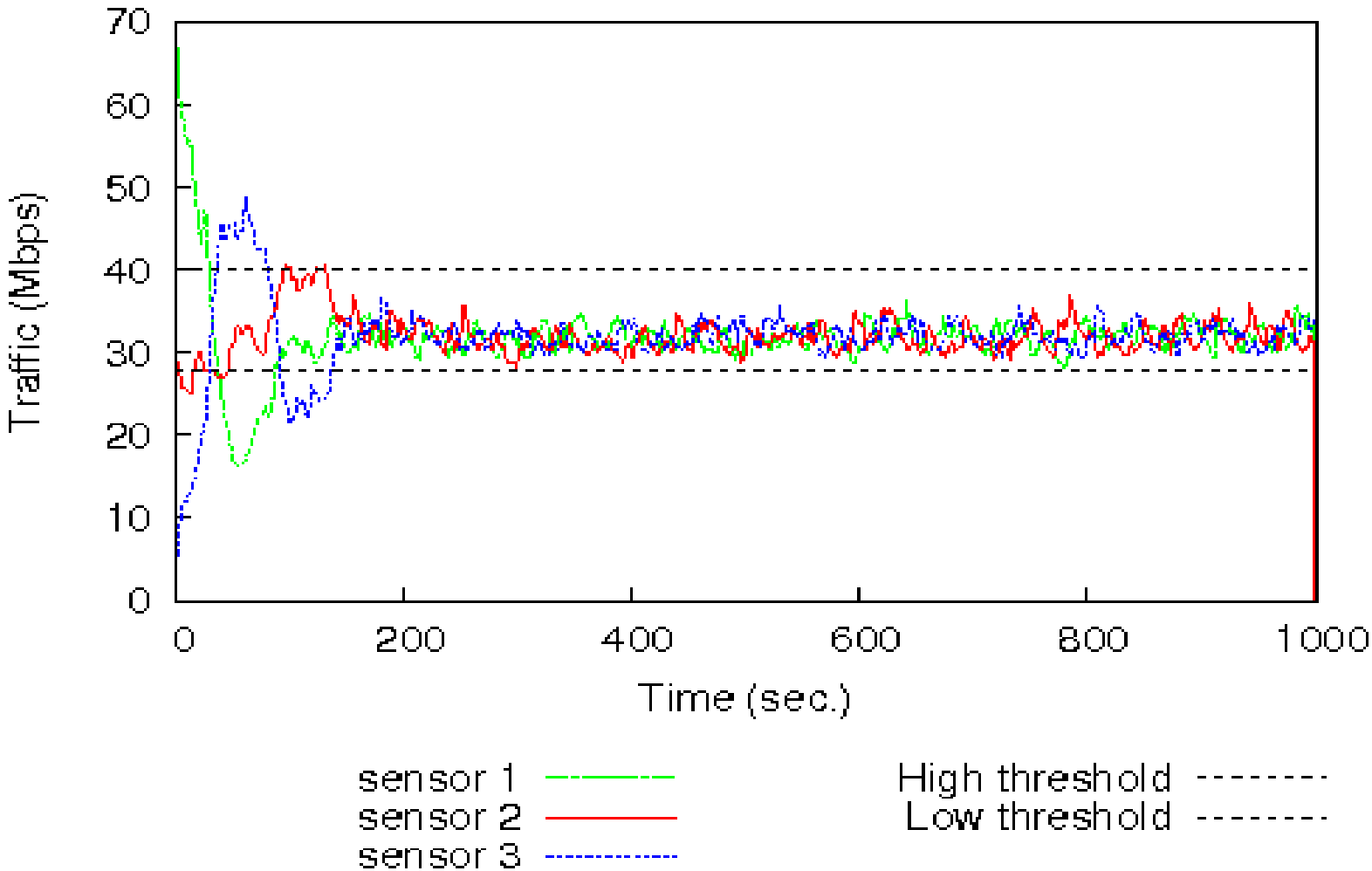


Migration time dominated by network latency

Not an issue for signature based intrusion detection

Application: parallel NIDS architecture

Stateful analysis and load balancing



Conclusions

- Novel NIDS cooperation approach
  - cooperative NIDS state management
  - stateful analysis of traffic flowing in links monitored by different sensors
  - Snort-based reference implementation
  - limited performance overhead
  - suitable for stateful analysis of network traffic generated by mobile nodes

ANCS 2007, 3-4-December 2007

Enhancing interoperability and stateful analysis of cooperative network intrusion detection systems

Michele Colajanni, Daniele Gozzi and
Mirco Marchetti

Department of Information Engineering
University of Modena and Reggio Emilia