Department of Information Engineering
University of Modena and Reggio Emilia, Italy

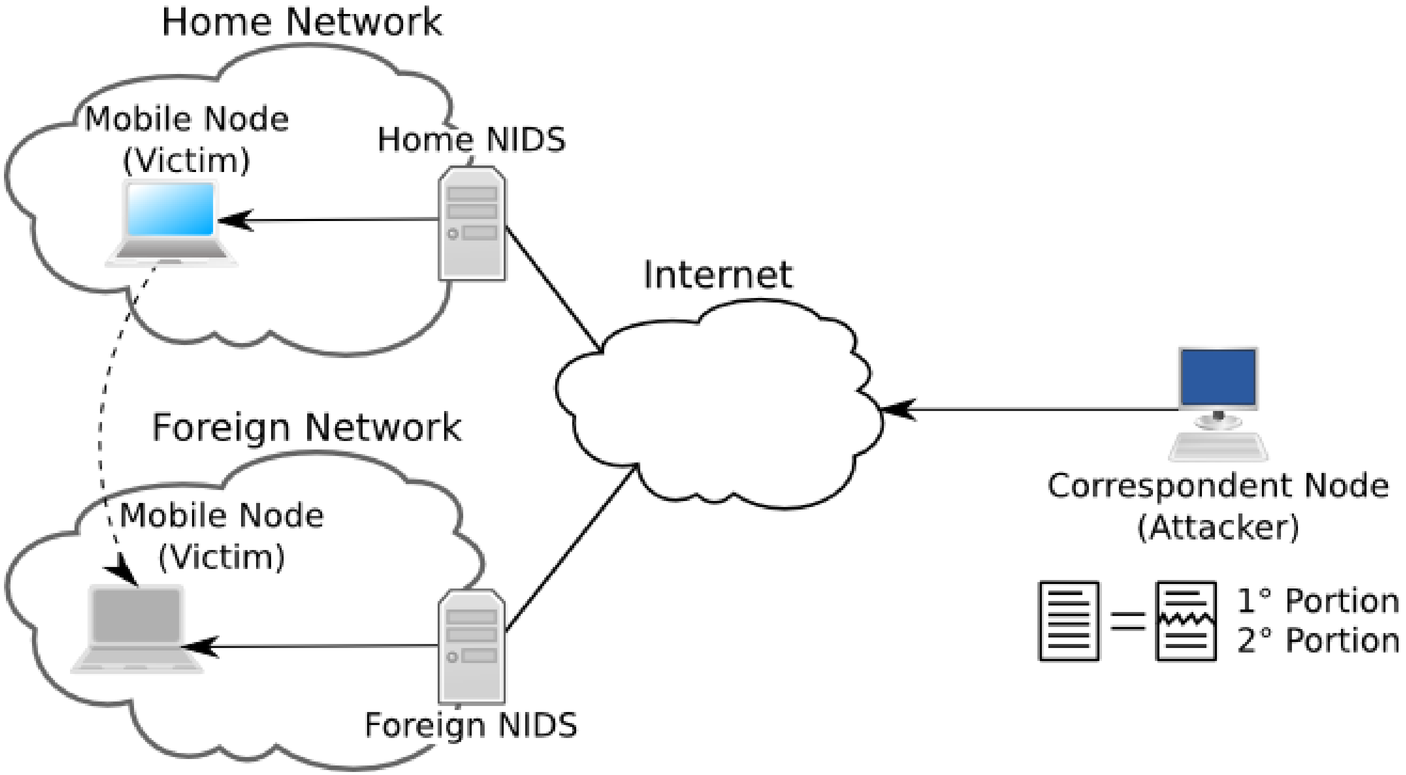
Defeating NIDS evasion in Mobile IPv6 networks

Michele Colajanni, Luca dal Zotto,
Mirco Marchetti and Michele Messori

Lucca, 22 June 2011
12th IEEE International Symposium on a
World of Wireless, Mobile and Multimedia Networks

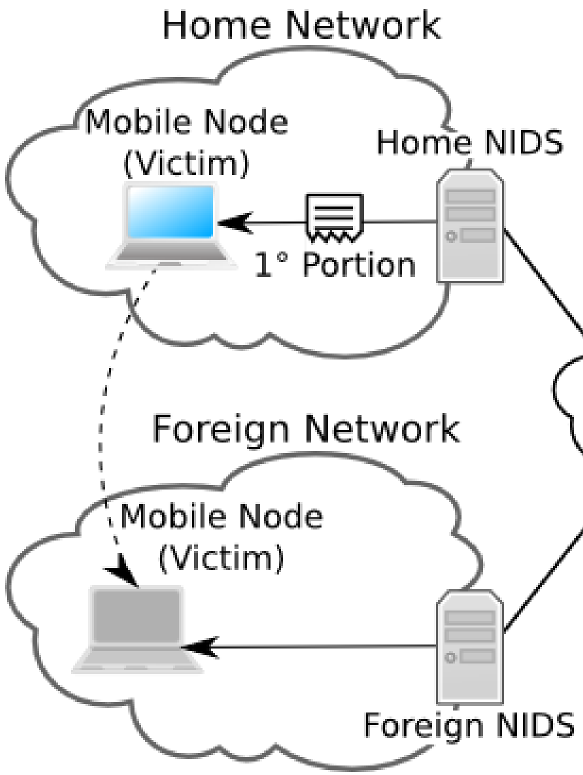
Attack example

Mobile Victim and Fixed Attacker using Route Optimization



Attack example

Mobile Victim and Fixed Attacker using Route Optimization



Attacker sends the 1° portion

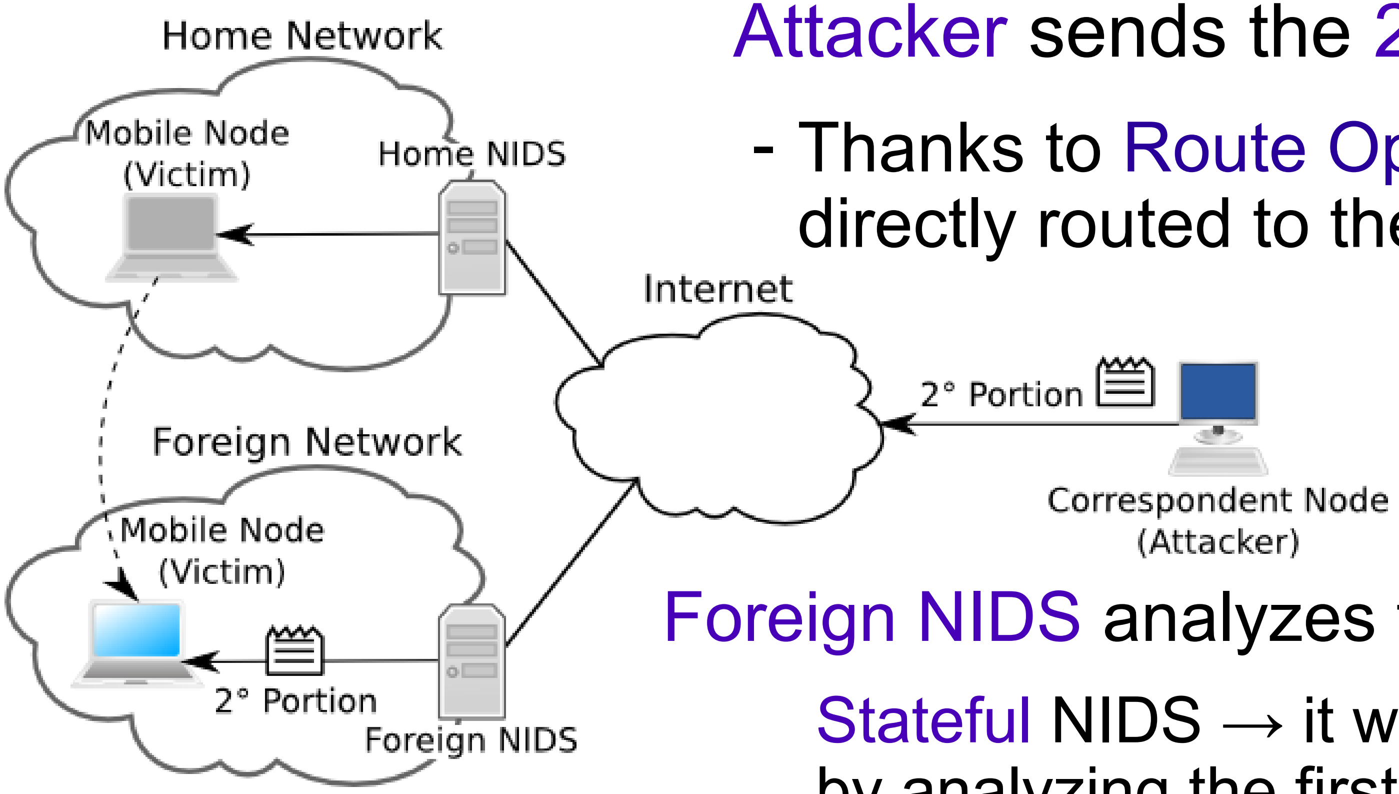
Home NIDS analyzes the 1° portion

Stateful NIDS → it would detect the attack by analyzing the second portion...

... but it never receives it

Attack example

Mobile Victim and Fixed Attacker using Route Optimization



Attacker sends the 2° portion

- Thanks to Route Optimization it is directly routed to the Victim

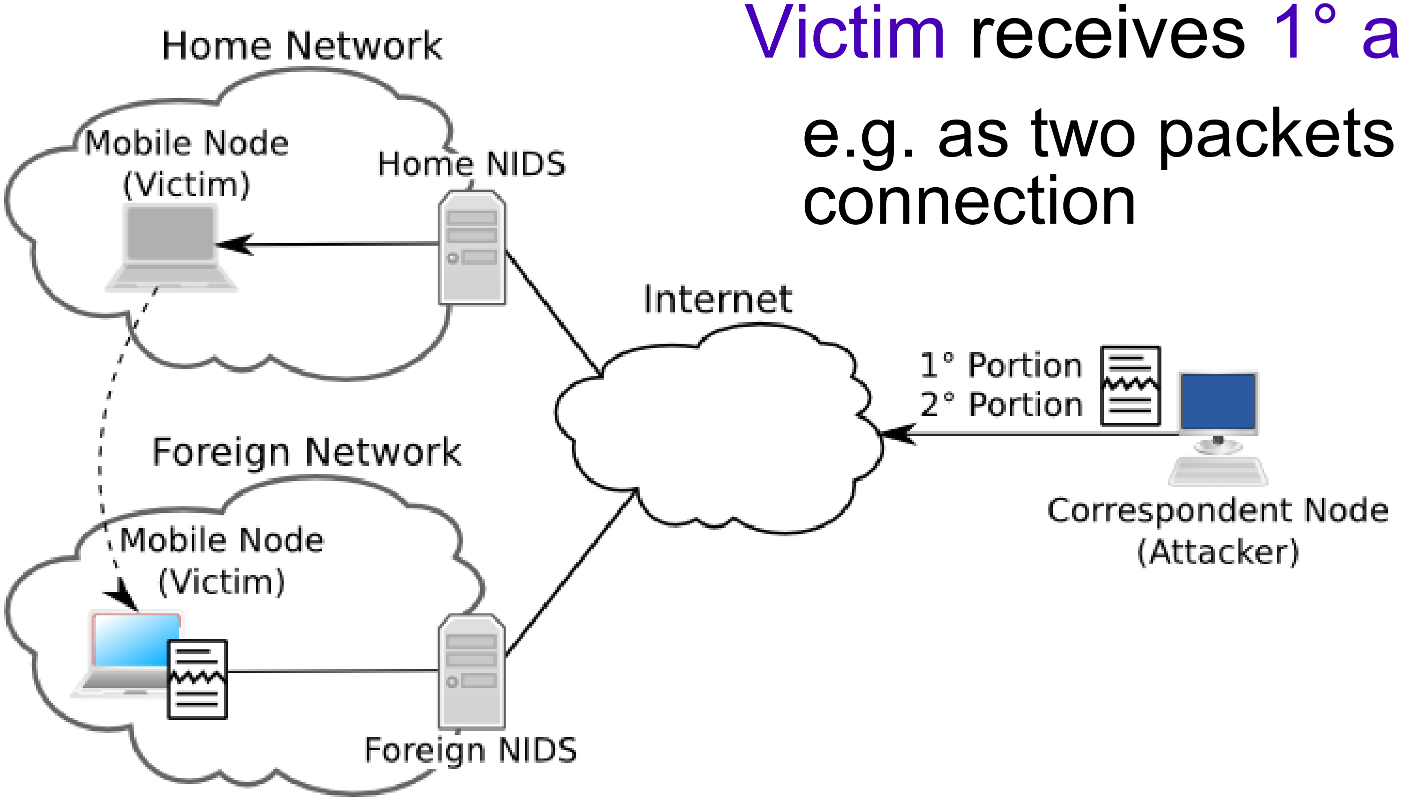
Foreign NIDS analyzes the 2° portion

Stateful NIDS → it would detect the attack by analyzing the first portion (even if out of order)...

... but it never receives it

Attack example

Mobile Victim and Fixed Attacker using Route Optimization

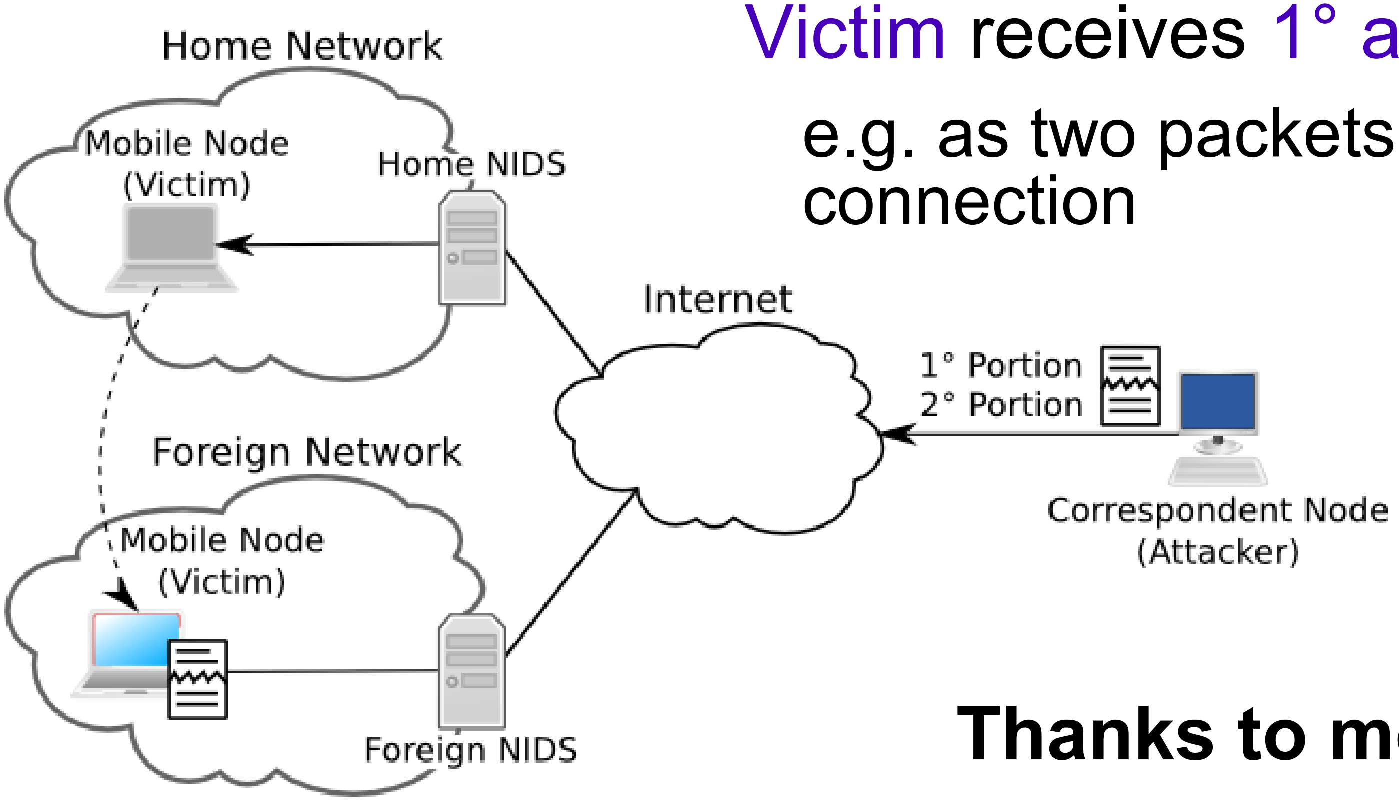


Victim receives 1° and 2° portion

- e.g. as two packets of the same TCP connection

Attack example

Mobile Victim and Fixed Attacker using Route Optimization



Victim receives 1° and 2° portion

e.g. as two packets of the same TCP connection

Thanks to mobility:

NIDSs fail, attacker wins

... how many examples?

- Three possible nodes positioning:
  - Mobile Victim and Fixed Attacker
  - Fixed Victim and Mobile Attacker
  - Mobile Victim and Mobile Attacker
- Two different communication channels
  - With Route Optimization
  - Without Route Optimization
- Possibly more than one migration per node
  - Home Network → Foreign Network → Home Network
  - Home Network → Foreign Network 1 → Foreign Network 2 → … → Foreign Network N
- A lot of possible combinations...

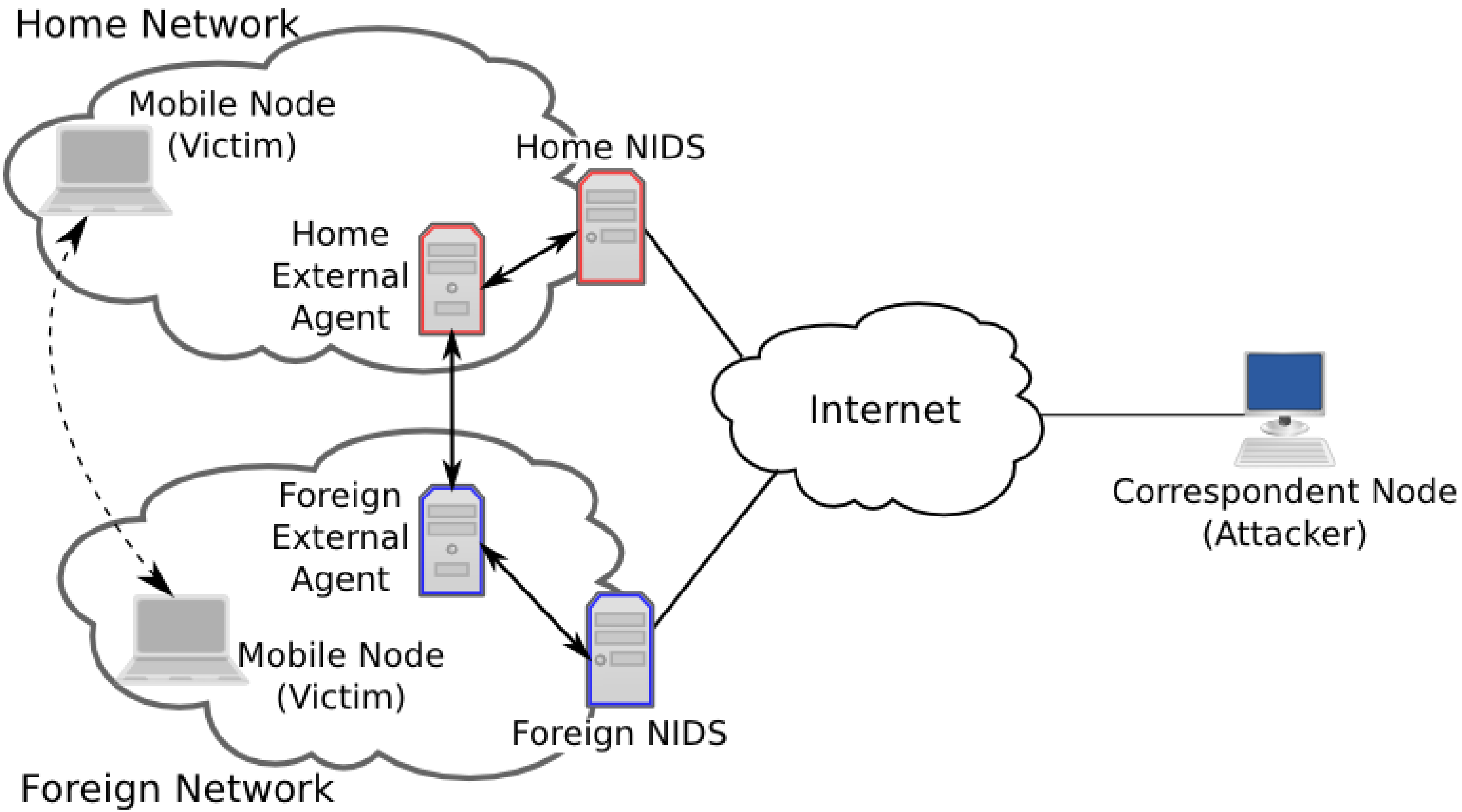
... how many examples?

- Three possible nodes positioning:
  - ✔ Mobile Victim and Fixed Attacker
  - ✔ Fixed Victim and Mobile Attacker
  - ✔ Mobile Victim and Mobile Attacker
- Two different communication channels
  - ✔ With Route Optimization
  - ✔ Without Route Optimization
- Possibly more than one migration per node
  - ✔ Home Network → Foreign Network → Home Network
  - ✗ Home Network → Foreign Network 1 → Foreign Network 2 → … → Foreign Network N
- A lot of possible combinations...
  - ✔ → we already manage
  - ✗ → we don't manage yet

NIDS Cooperation

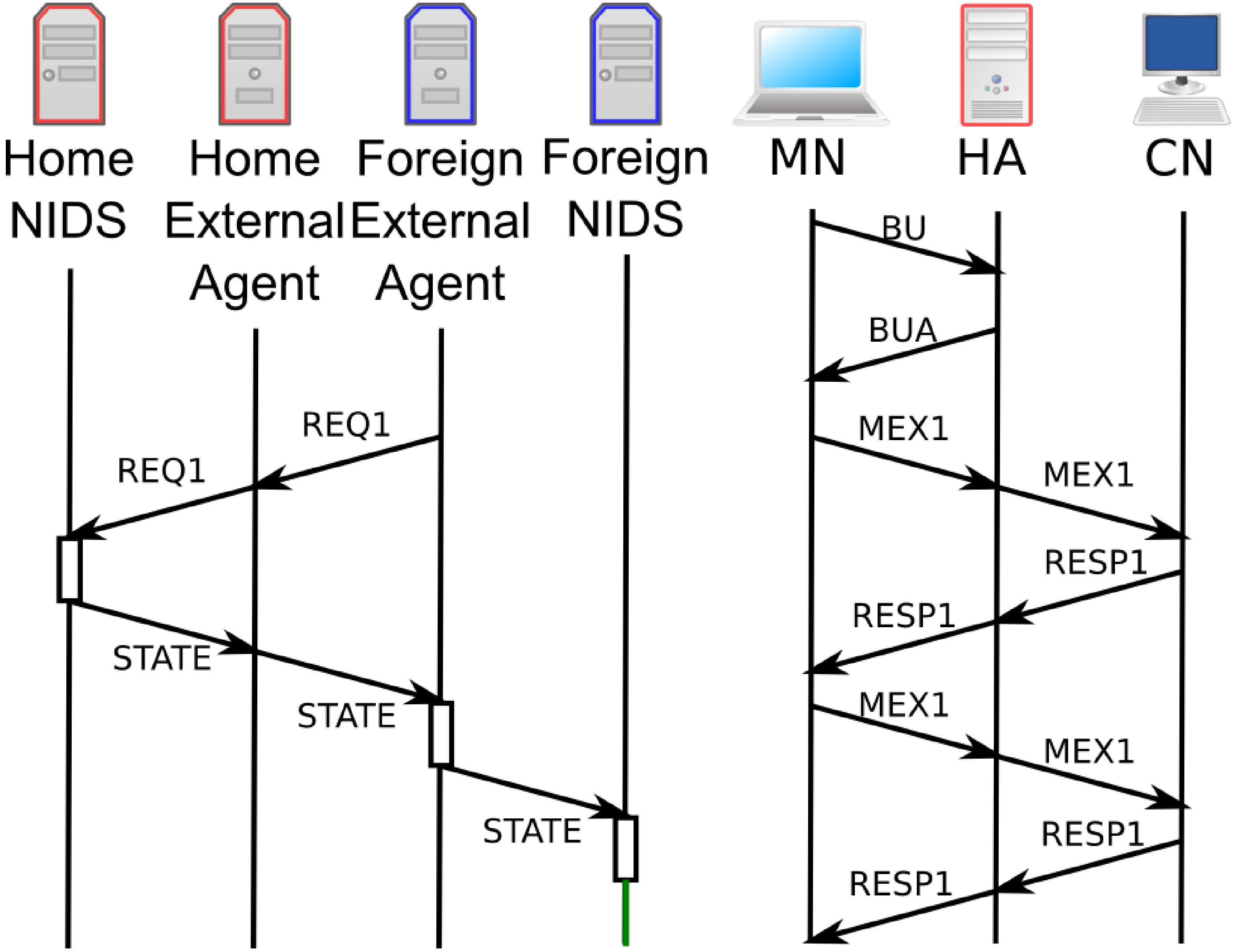
- Modified version of **Snort**
  - Added state.import and state.export methods
  - Added a XML-RPC server
- Developed the **External Agent**
  - It detects Mobile Nodes roaming thanks to the Binding Updates
  - It implements a XML-RPC client to contact the Local NIDS or remote External Agents
  - It implements a XML-RPC server to replay to remote External Agents's requests
  - It preprocesses state information before importing it into the local NIDS

Proposed Architecture



State exchange protocol

Migration from Home to Foreign Network

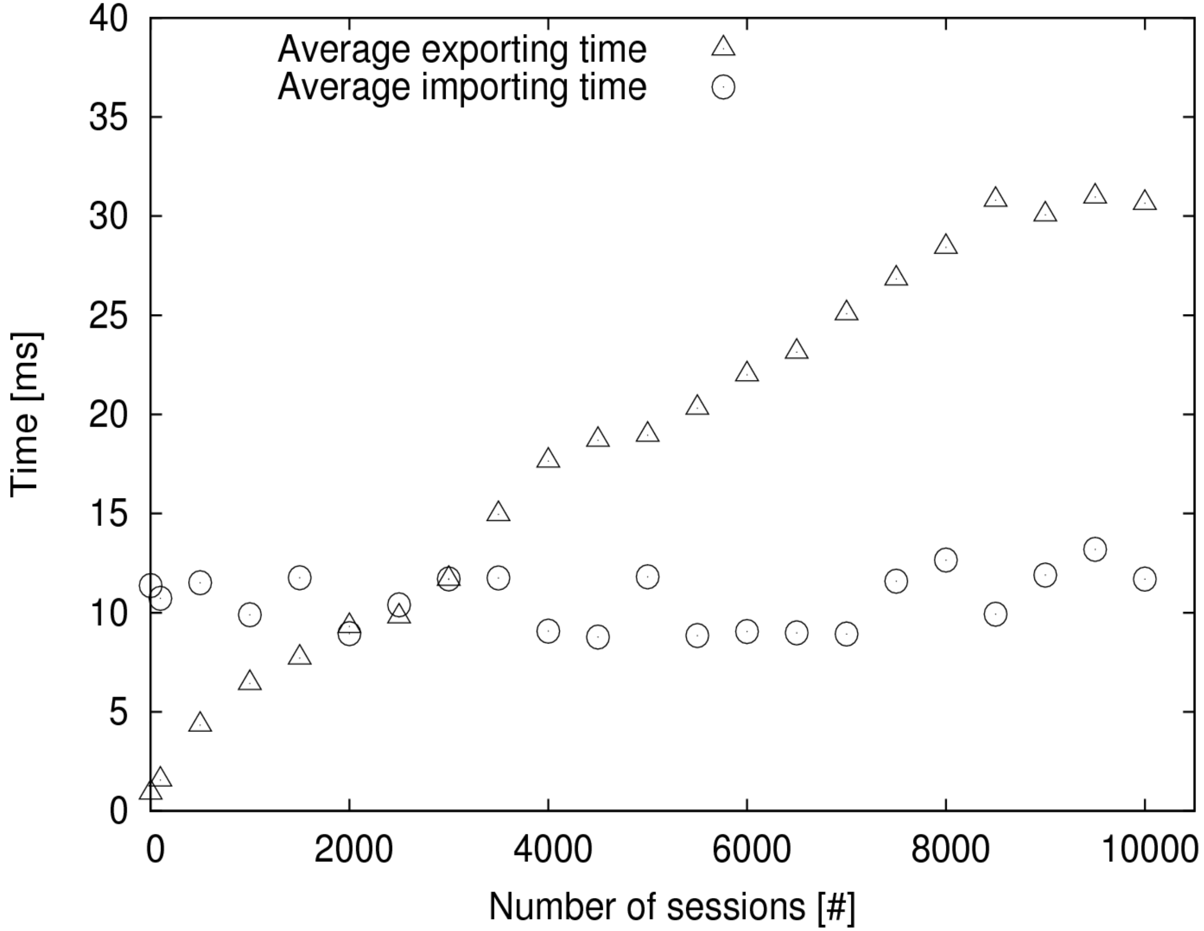


Prototype implementation

- Viability demonstrated through prototype implementation
  - Modified Snort (version 2.8.6.1) to import/export state information
  - Designed a new software agent to coordinate state import, export and transmission
  - Designed new protocol for state management
- Experimental results:
  - It works! Thwarts mobility-based evasion in all the scenarios (NIDSs do not fail anymore)
  - Delays compatible with live traffic analysis
  - Traffic traces available for scrutiny (http://cris.unimore.it/cris/DefeatingMIPv6Evasion)

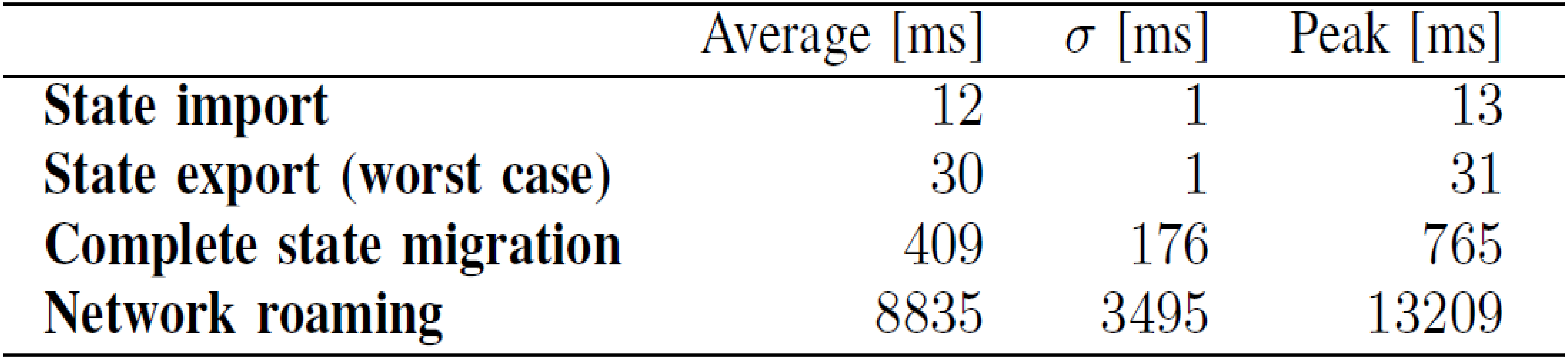
Scalability of state migration activities

- State export time scales linearly with the number of concurrent TCP sessions
- State import time is constant



State migration performance

- Compatible with real-time traffic analysis and MIPv6 node mobility
  - One order of magnitude lower than migration



	Average [ms]	σ [ms]	Peak [ms]
State import	12	1	13
State export (worst case)	30	1	31
Complete state migration	409	176	765
Network roaming	8835	3495	13209

Conclusions & open issues

- Mobility-based NIDS evasion
  - New NIDS evasion technique
  - Effective against all state-of-the-art NIDS
  - Exploits protocols for transparent node mobility
  - Immediately applicable to existing mobile networks!
  - Can only be solved through NIDS cooperation

    (One NIDS alone cannot defeat it, independently on the reassembly algorithm)

- Our solution works

- Open research issues:
  - Interoperability among heterogeneous NIDSs
  - Securing state migration protocol