Disturbed playing: Another kind of educational security games

Sebastian Koch
Jörg Schneider
Jan Nordholz

Technische Universitaet Berlin

Motivation

- Risk assessment and policy design
  - Important
  - No one wants to learn it
- CTF Games etc.
  - Hands-on experience
  - Ad-hoc solutions, no policy
  - Privacy and Integrity, but no availability

Disturbed Playing

- 1. Computer Game
  - Easy to learn
  - Unrelated to security
  - Success depends on IT infrastructure
  - No automation
- 2. Threat model
  - Well defined
  - Real life problems in shorter time
  - Automated, synchronized attacks

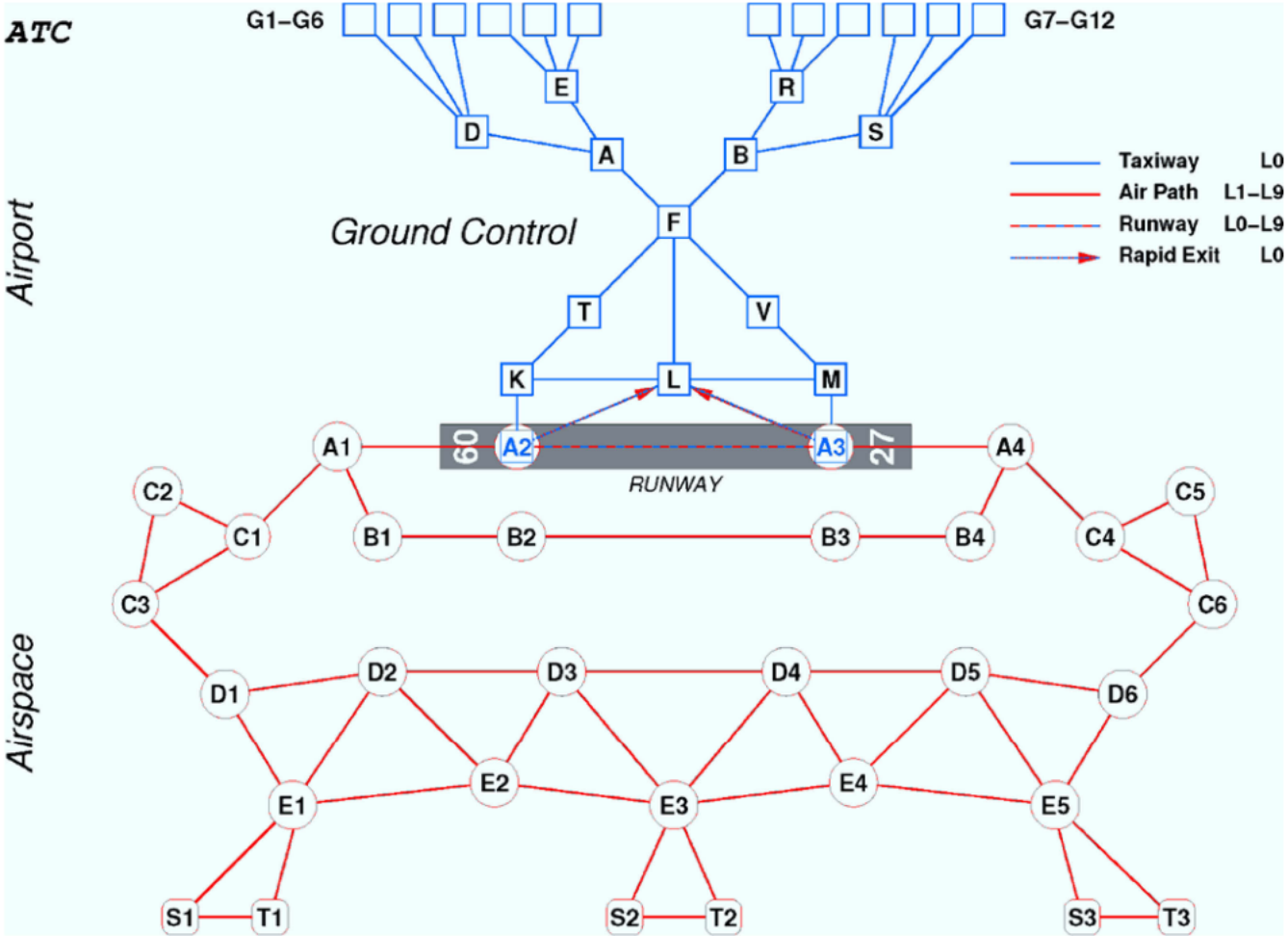
Playing the game

- Students have all roles:
  - Policy designer
  - Implementer
  - User affected by policy
- Multiple game sessions

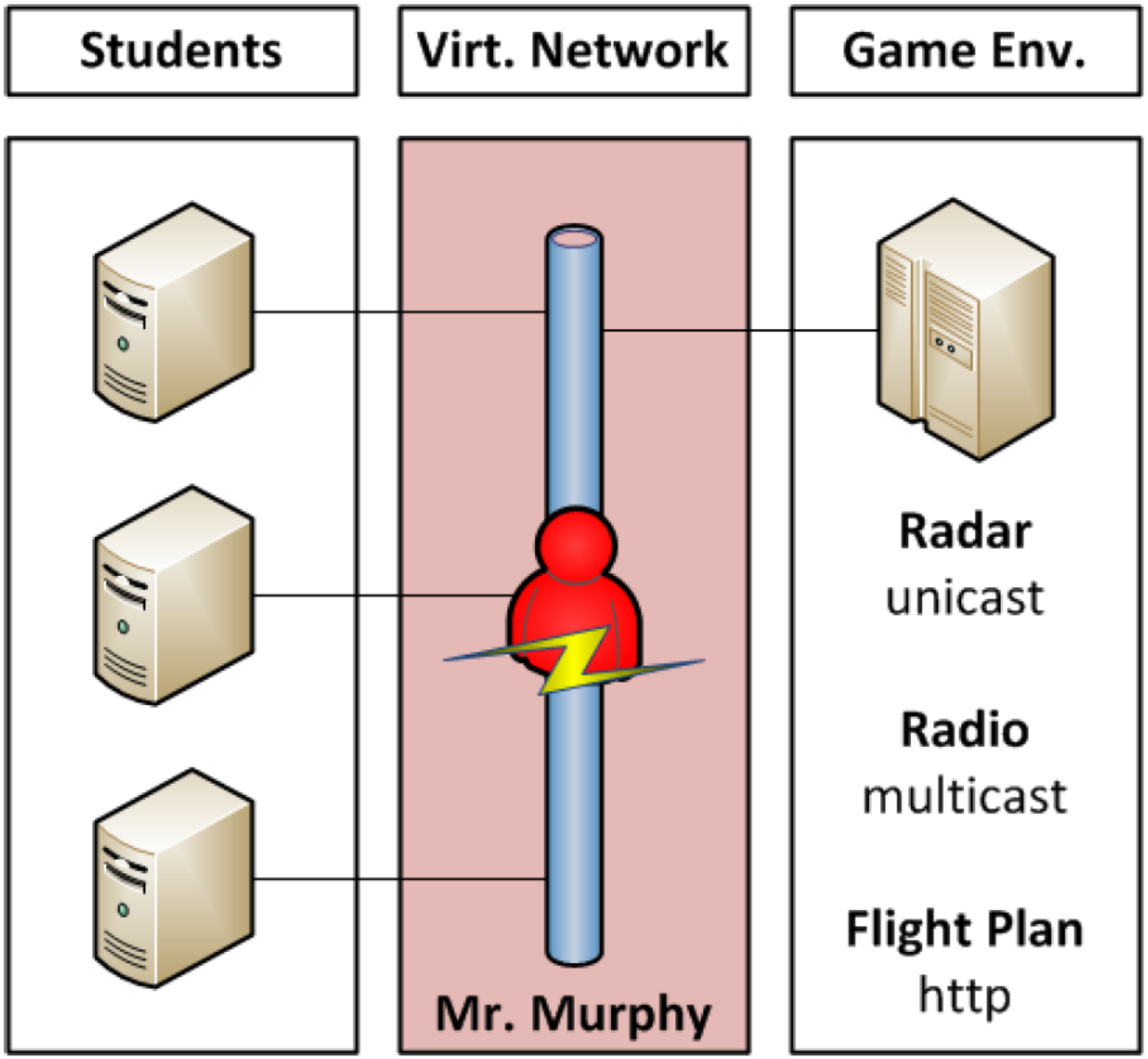


Example: ATC Game

- Simulate Air traffic control with 3 controller



Threat model



Experiences

- Plan the rules.
  Restrict the threat model well in advance.
- It is a lot of work. You need a good team.
- Students will try to automate the game play.
- Fun factor is hard to calculate.
- The students‘ motivation is
  at least constant or even rising.
- It works!

Disturbed playing: Another kind of educational security games

Sebastian Koch, *Jörg Schneider*, Jan Nordholz
Technische Universitaet Berlin

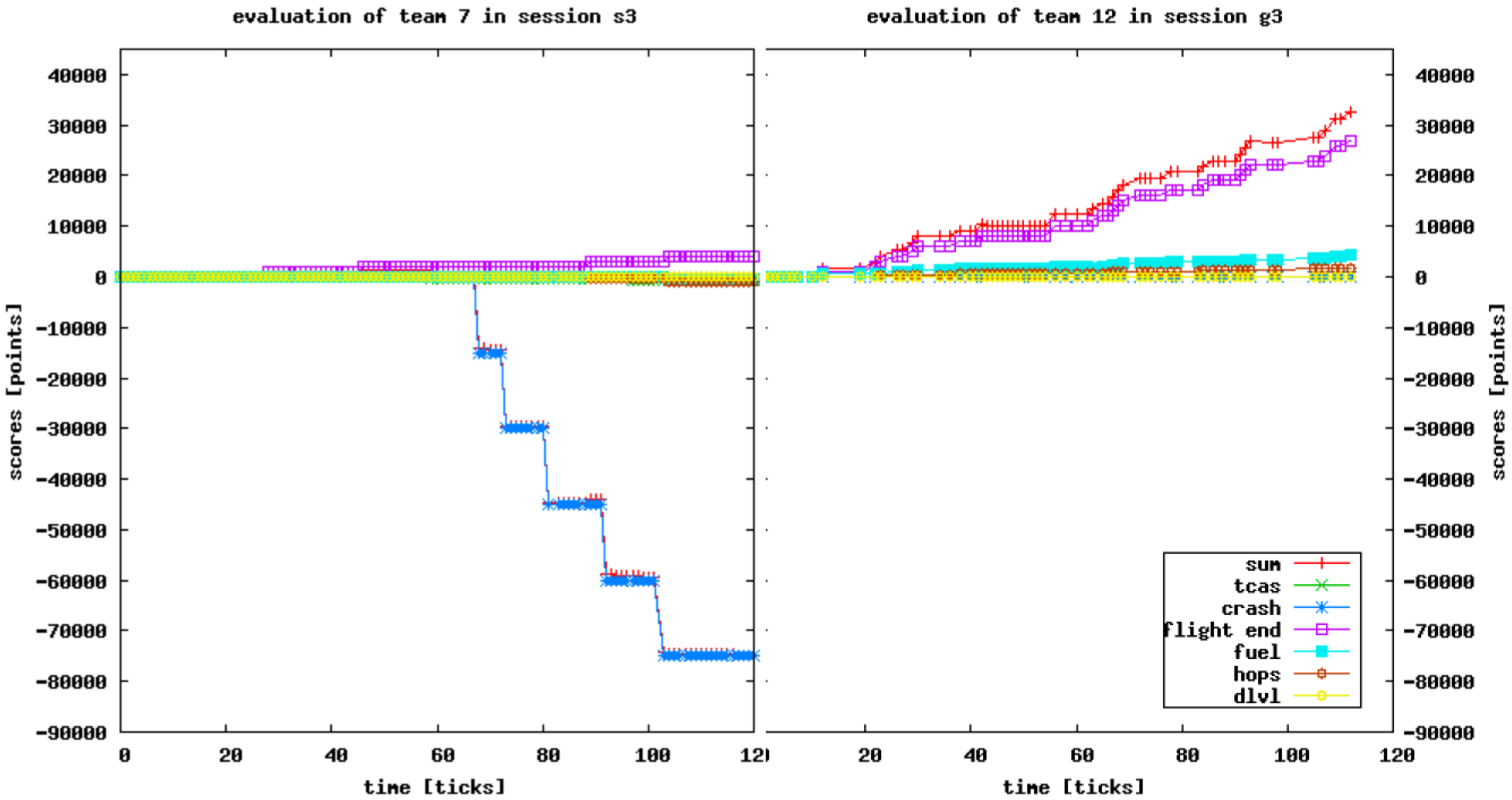
komm@cs.tu-berlin.de
www.kbs.tu-berlin.de

metafly.info

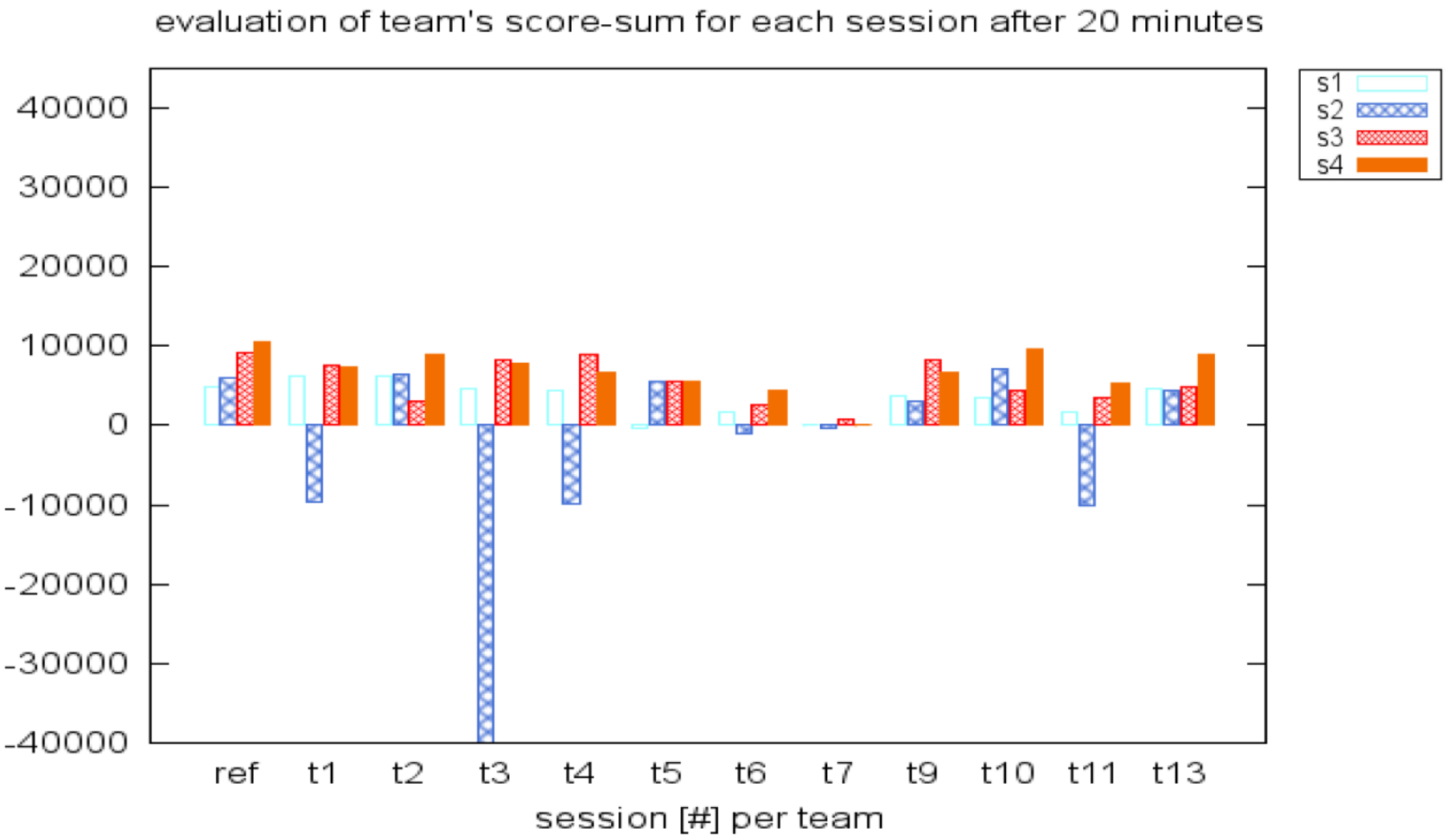
Appendix

- Results
  - Point vs. preparation example
  - Learning progress: Phase 1, 2, 3
- ATC game model
  - Risk map
  - Vertical model
- Implementation
  - Integration in iptables

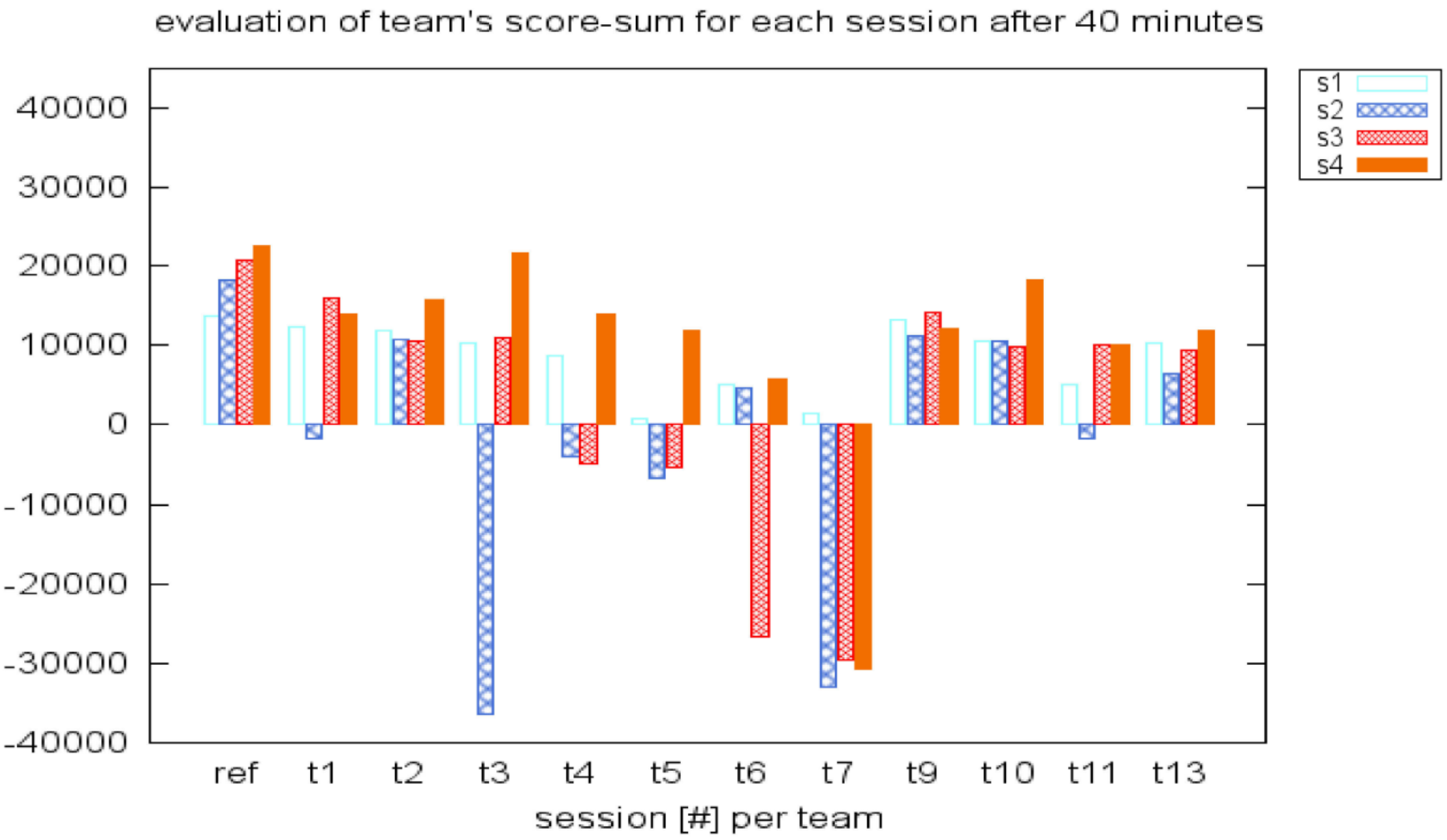
Points vs. preparation



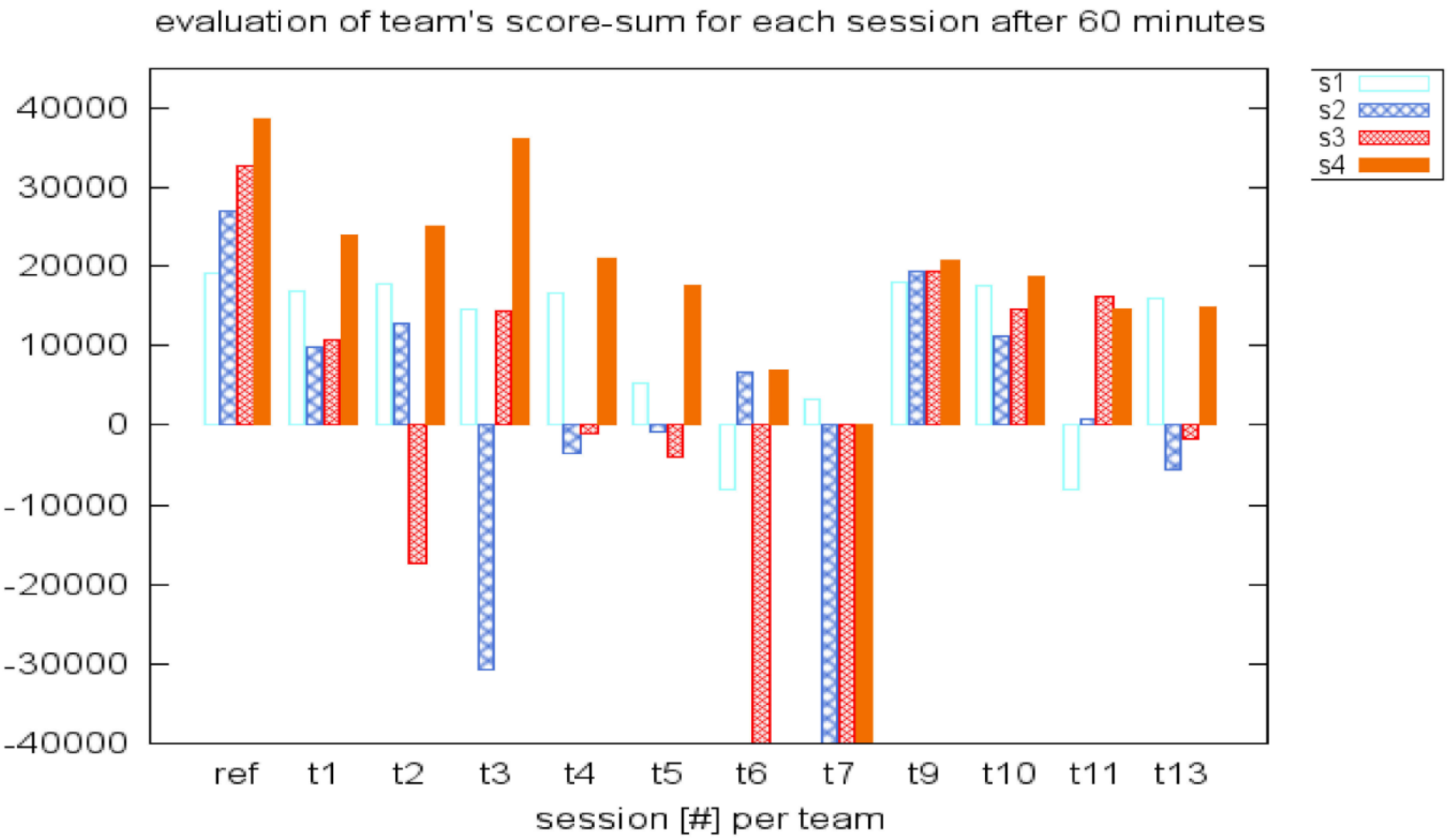
Learning: Progress 1. Phase



Learning: Progress 2. Phase

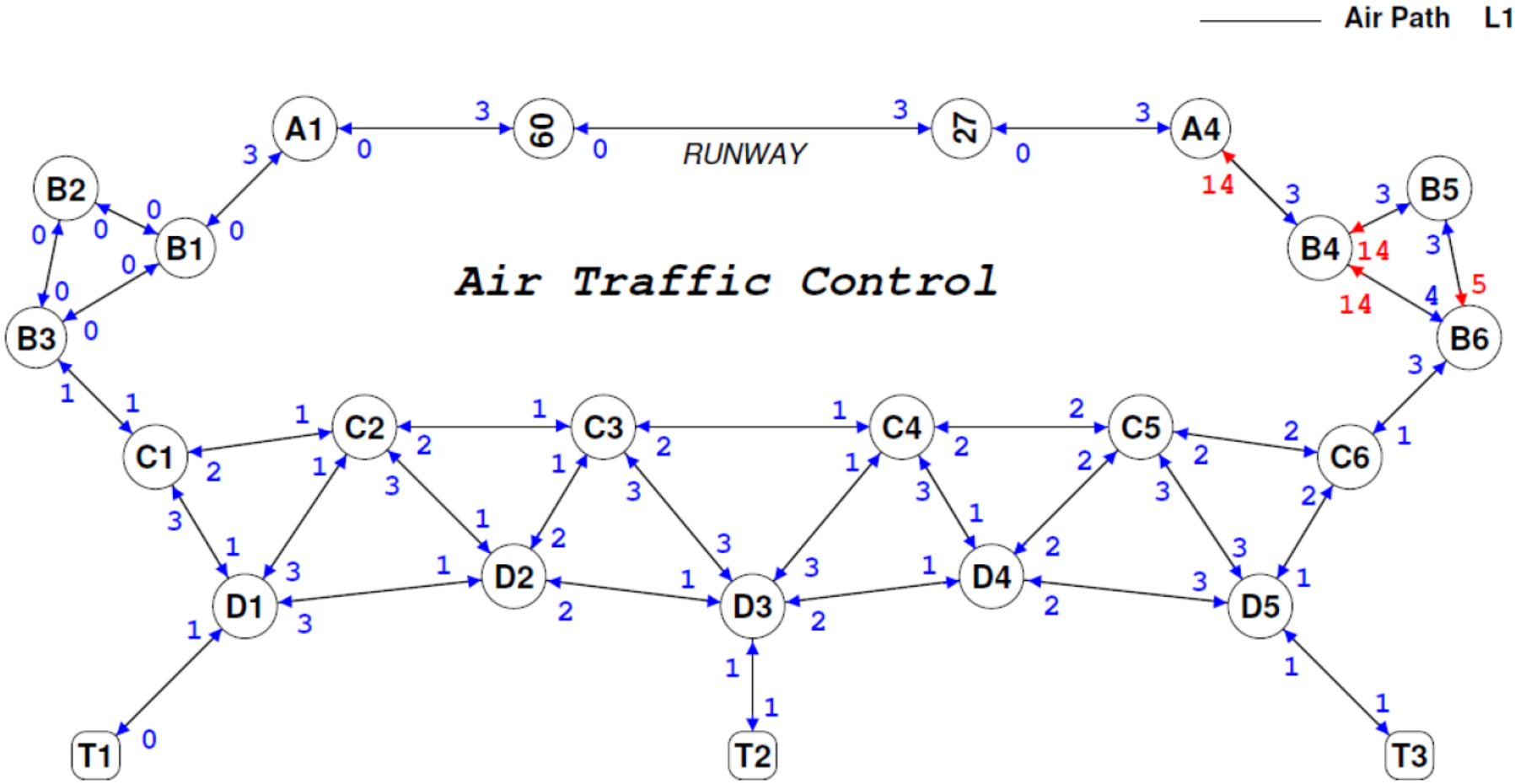


Learning: Progress 3. Phase

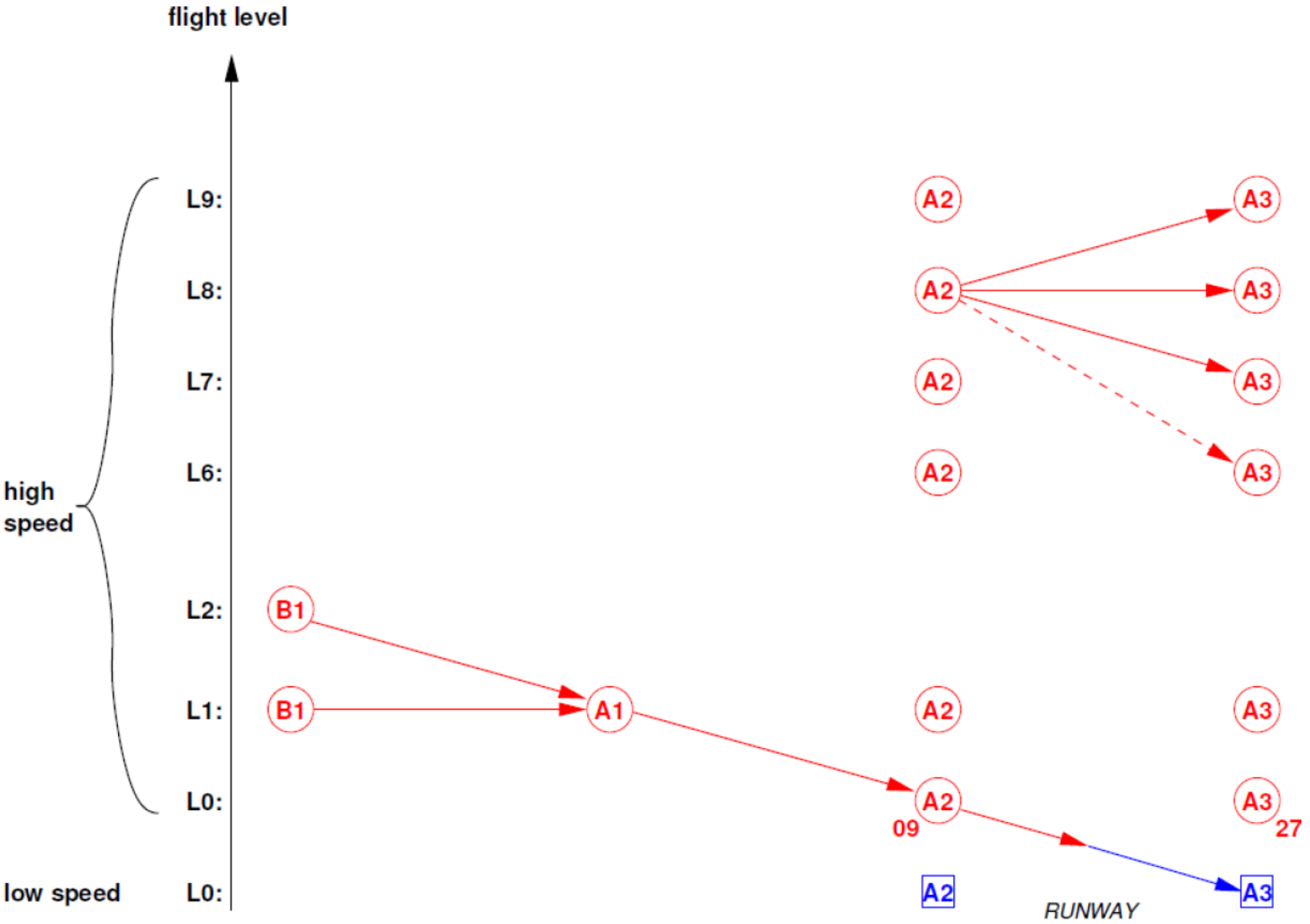


Risk Map

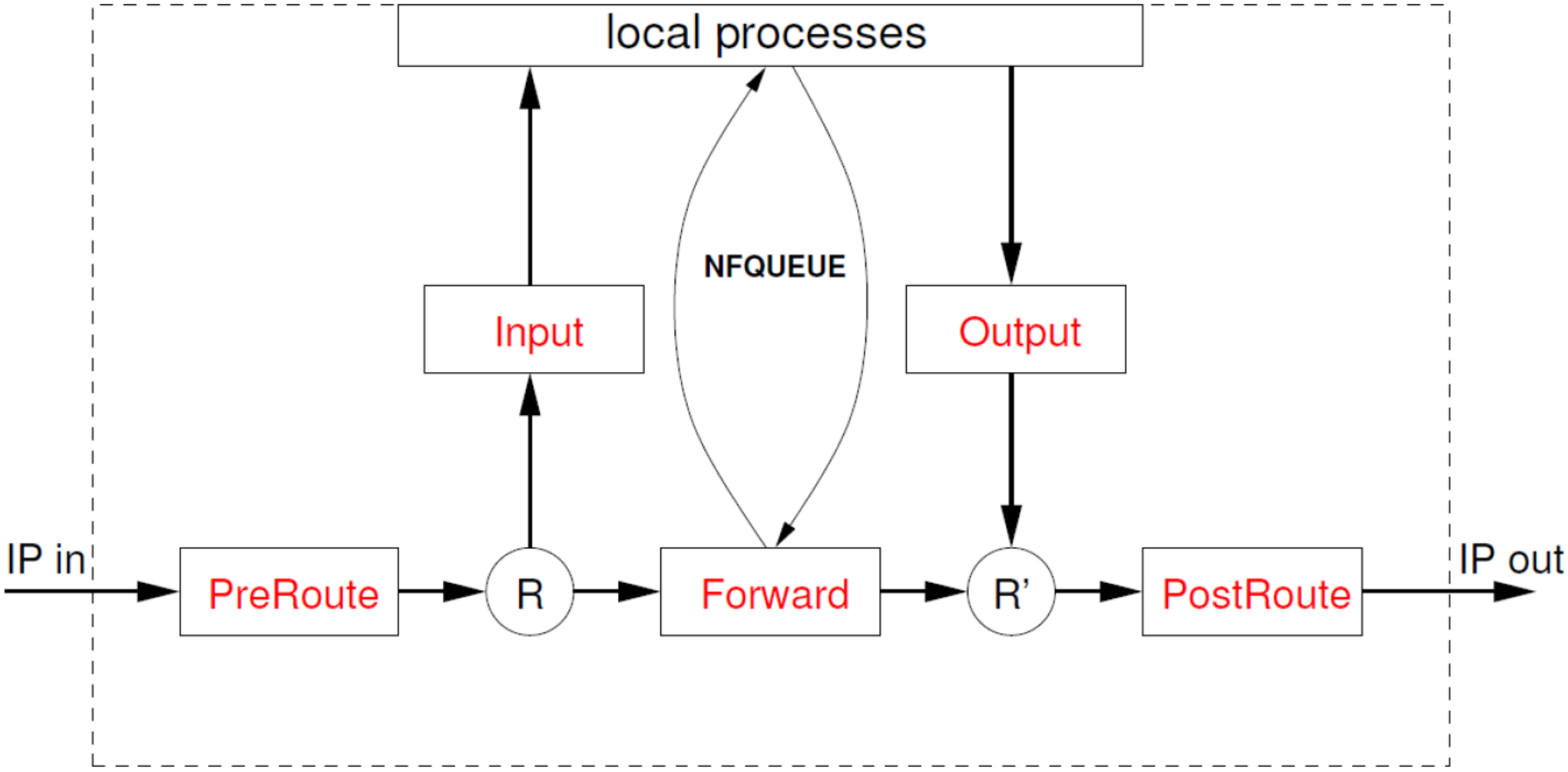
Extra hops needed after mistake at this point



Vertical airspace model



Integration in iptables



packet filter data flow (iptables)