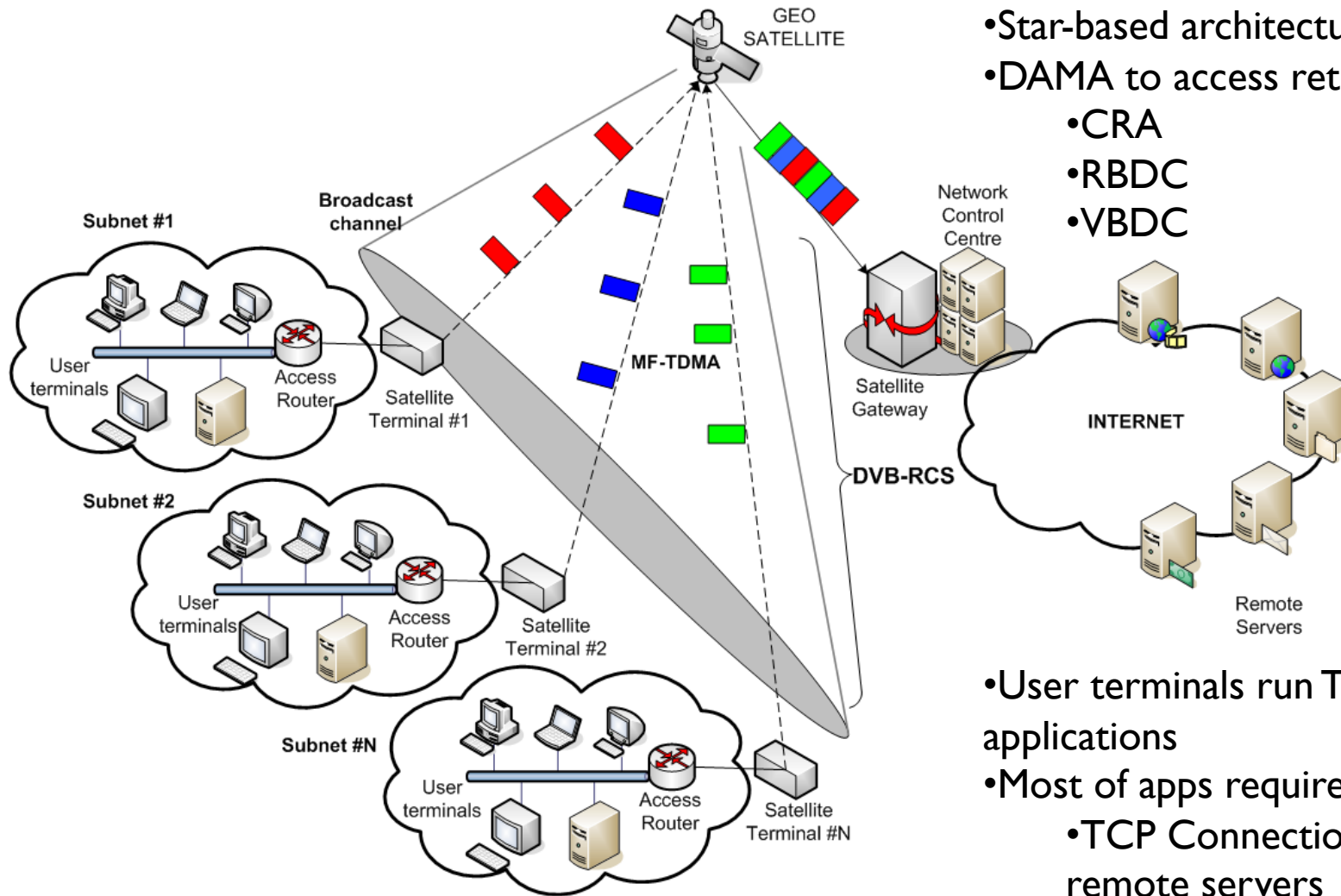


# Attack, Detection and Countermeasures: A demo on Satellite Networks Security

Dr. Cesare Roseti, Ing. F. Belli and Prof. M. Luglio  
CRESM- research unit of University of Rome "Tor Vergata"

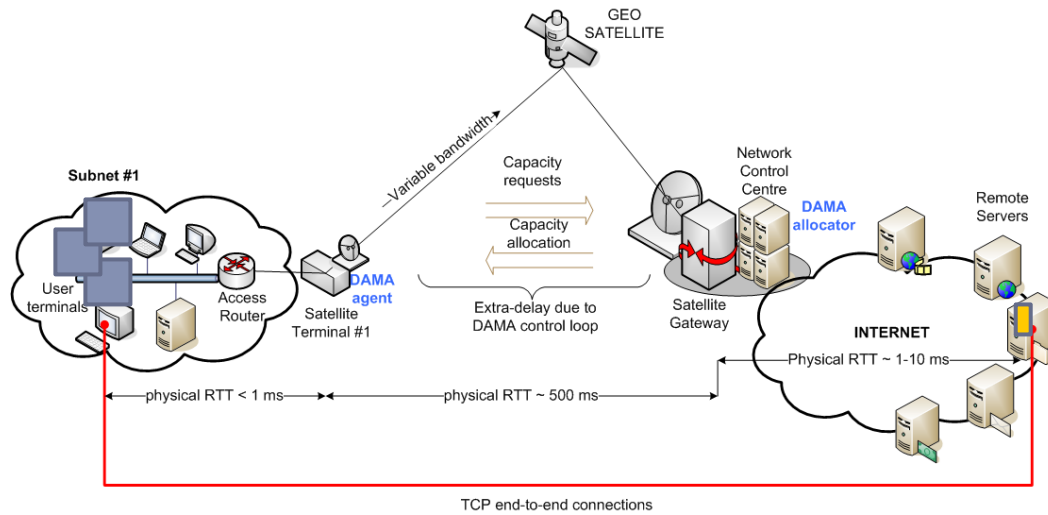
# Reference scenario



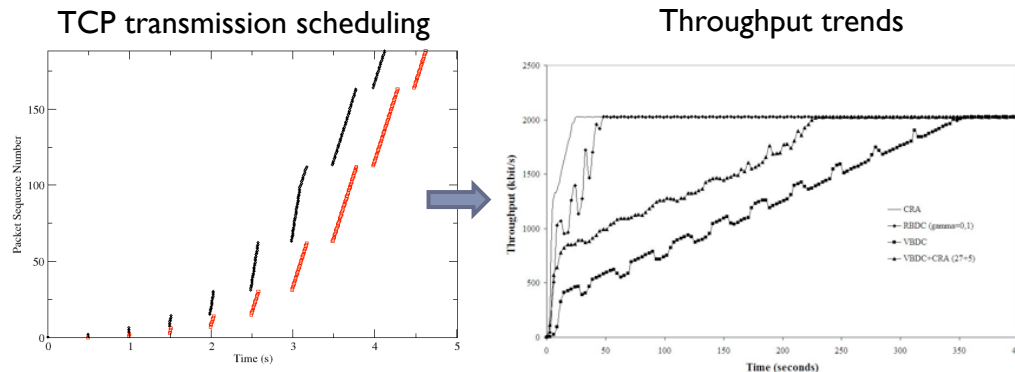
- Star-based architecture
- DAMA to access return link
  - CRA
  - RBDC
  - VBDC

- User terminals run TCP/IP applications
- Most of apps requires reliability
  - TCP Connections towards remote servers

# TCP over DVB-RCS: issues

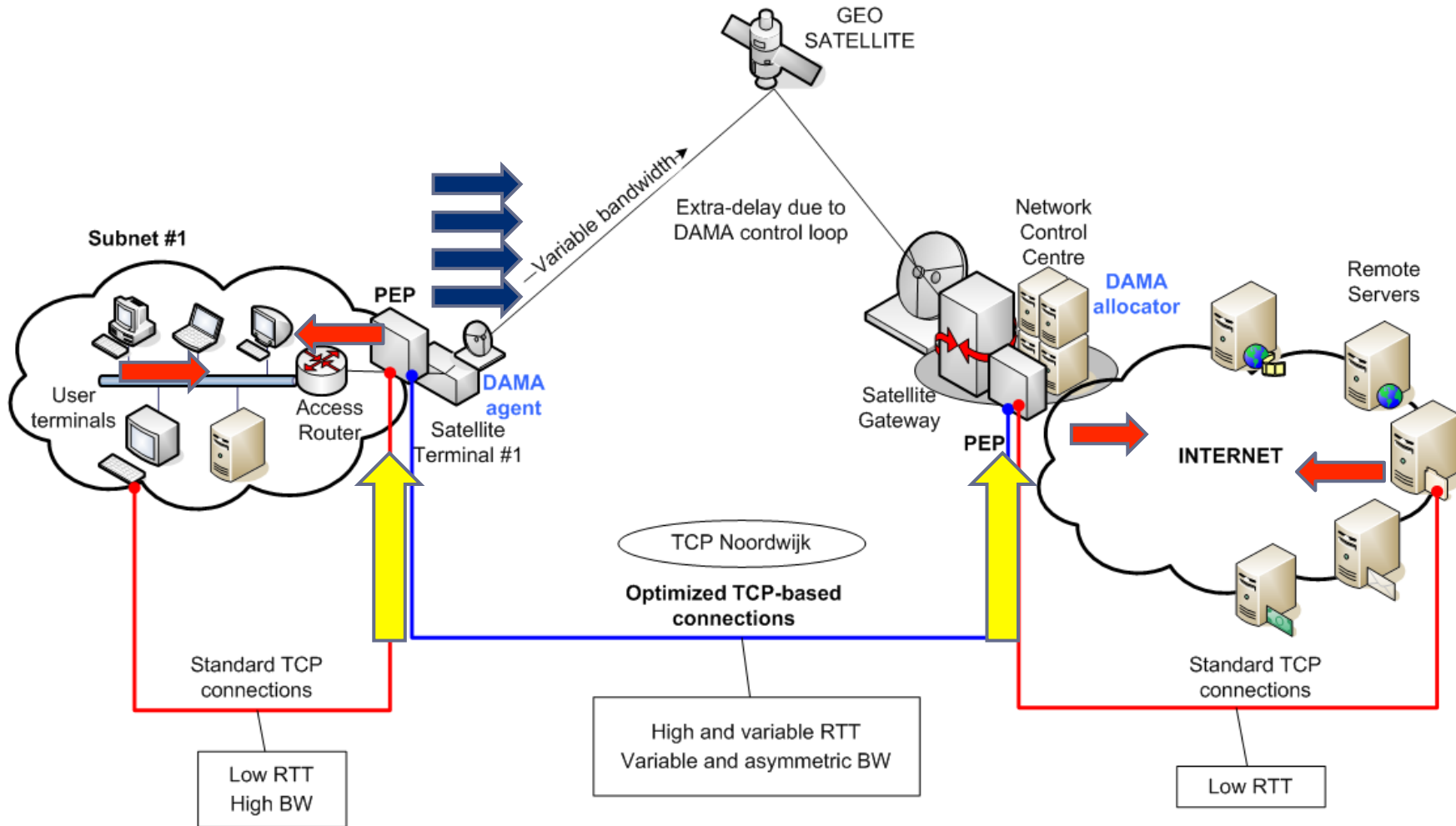


A performance overview

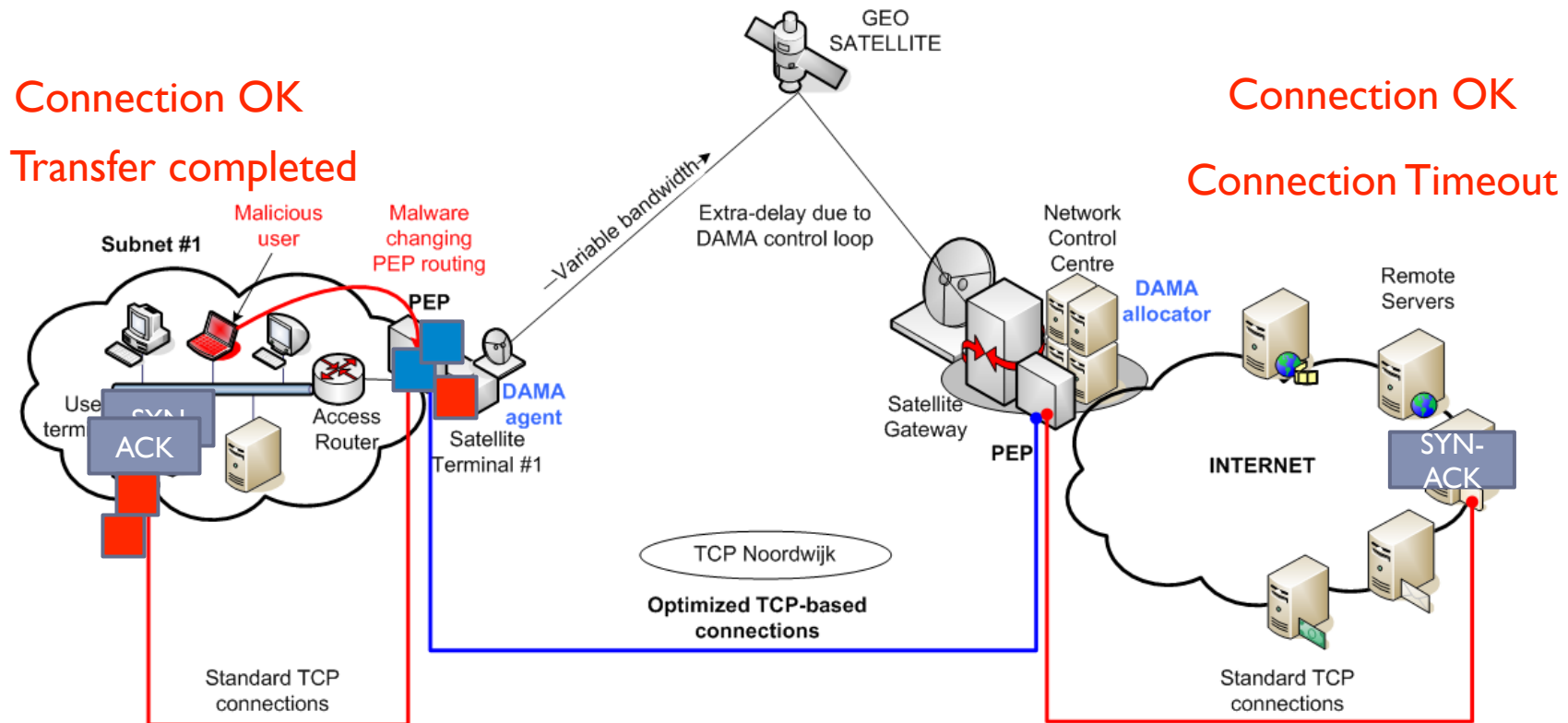


- TCP transmission is ACK-clocked
  - The higher is RTT the slower is throughput increase
  - Start up sending very slow
  - Underutilization of the available resources
- DAMA algorithms may introduce variable contributions to the overall RTT
  - Further slow down of the bw probing
  - Misleading signals of network congestion

# TCP Acceleration



# PEP vulnerability



- PEPs terminate conns, grab all TCP packets (in plain text) and re-route them in new connections
  - TCP PEP are not compatible with IPsec → **Lost of confidentiality** on PEP
  - Maliciously changing routing rules, TCP packet can be dropped after ACK transmission → **Lost of reliability of TCP!**



# IDS goal

---

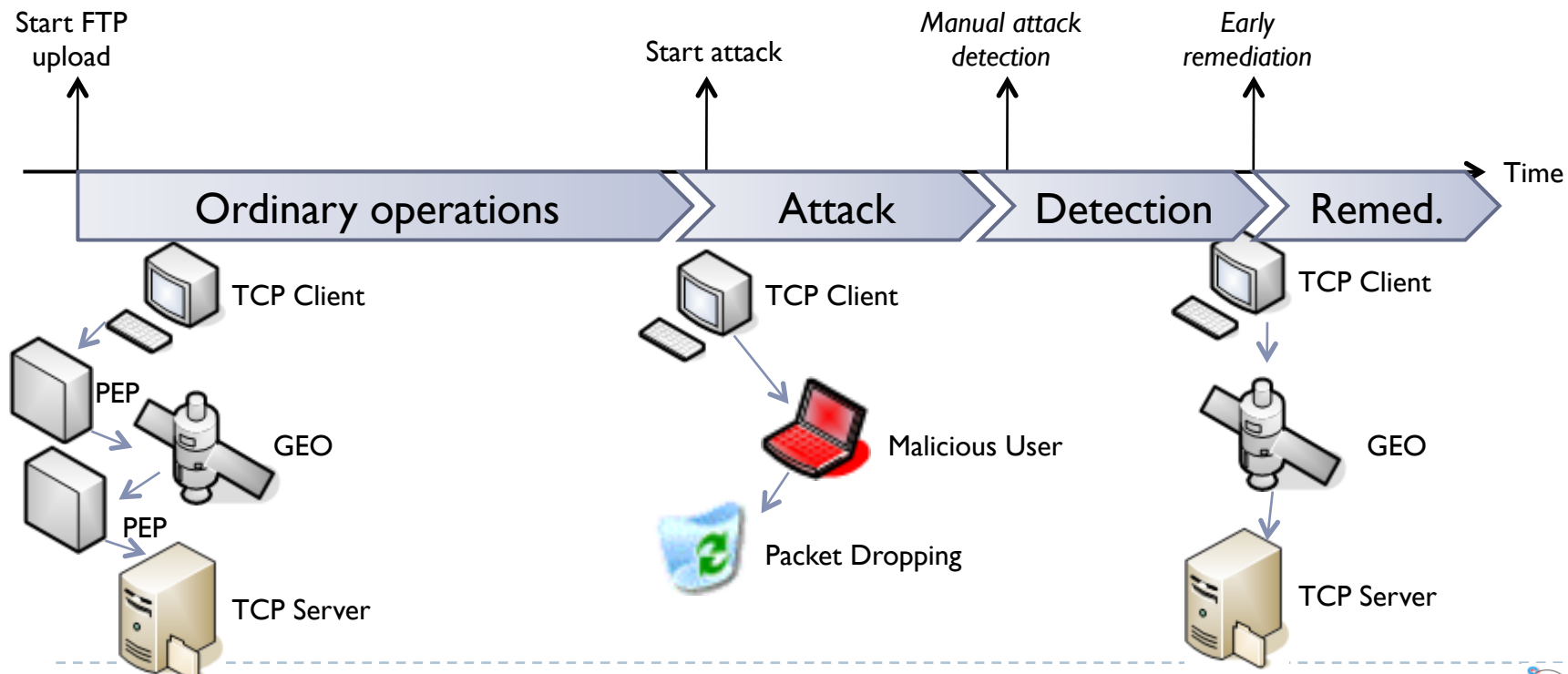
- ▶ Risk reduction!!!!
- ▶ Risk definition ( $R_e$ ): source-unaware traffic dropping
- ▶  $P(e)$ : Likelihood of the event
- ▶  $V(e)$ : PEP adoption
- ▶  $D(e)$ : Lost of data/Denial of Service

$$R_e = \mathbb{P}(e) \cdot V(e) \cdot D(e),$$

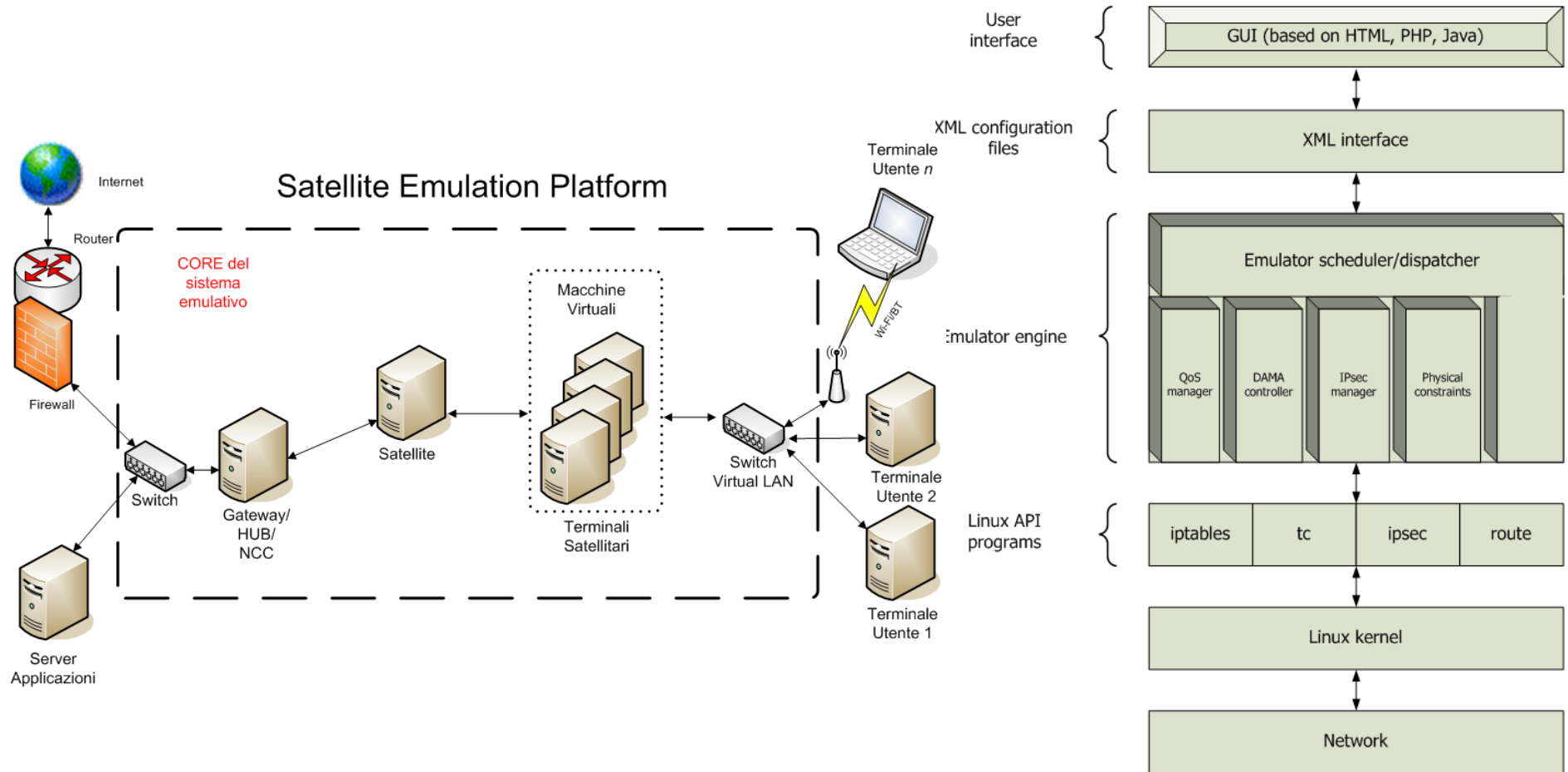
↑ ↑  
Reduction of these factors

# DEMO presentation

- ▶ DEMO through a Satellite Network Emulator Platform
  - ▶ Reproduction of a DVB-RCS-like network
  - ▶ DAMA over return link; NCC functionalities
  - ▶ TCP client connected to Satellite terminal
  - ▶ TCP server beyond Satellite Gateway

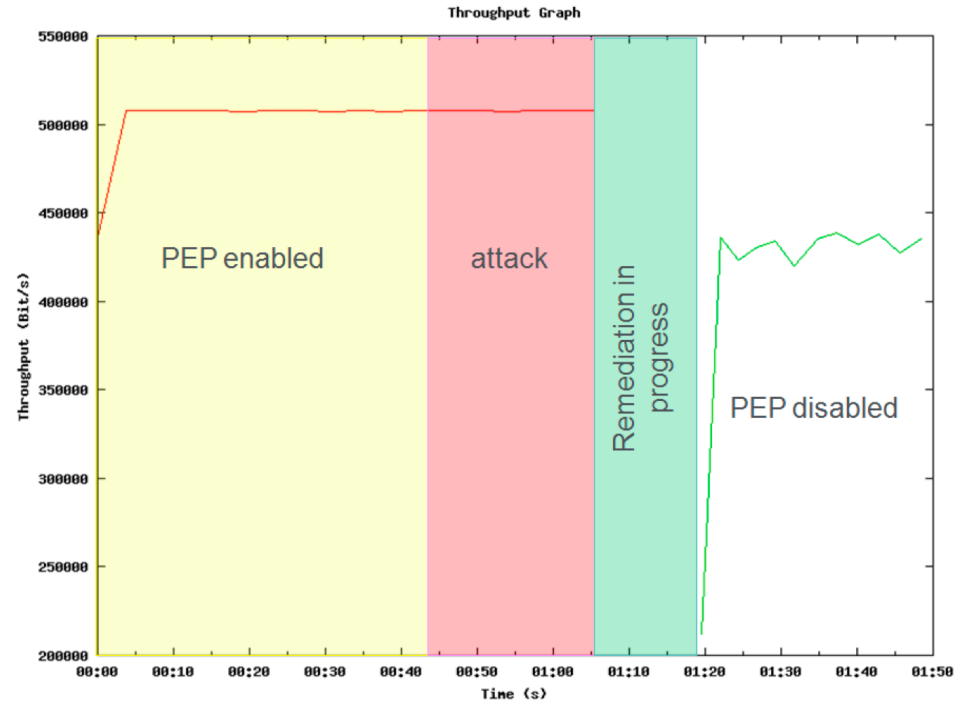


# Move to emulator....



# Result analysis

TCP Sender



TCP Receiver

