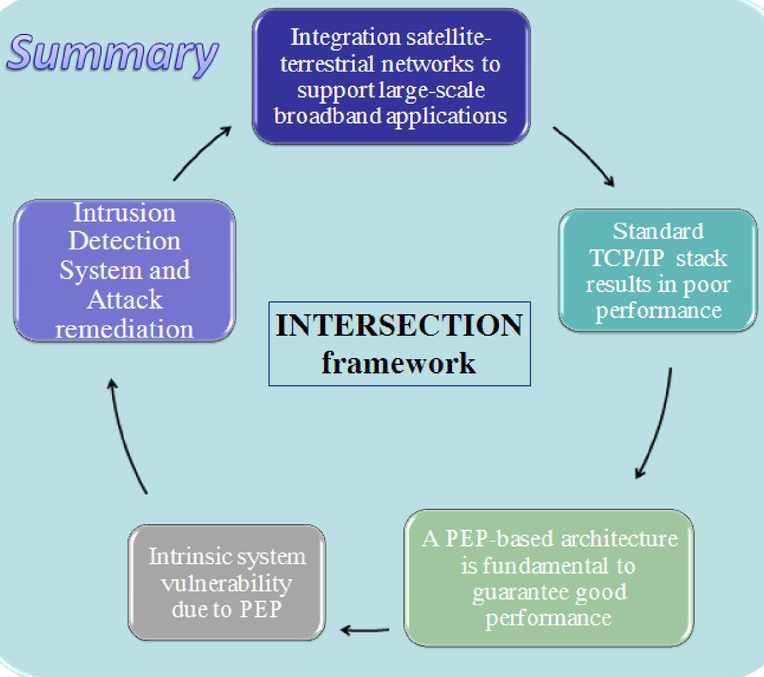
SATELLITE NETWORK PROTECTION AGAINST INTERCONNECTION-RELATED VULNERABILITIES

Prof. Michele Luglio
mailto: luglio@uniroma2.it
Dr. Cesare Roseti
mailto: roseti@ing.uniroma2.it
Mr. Francesco Belli
mailto: belli@ing.uniroma2

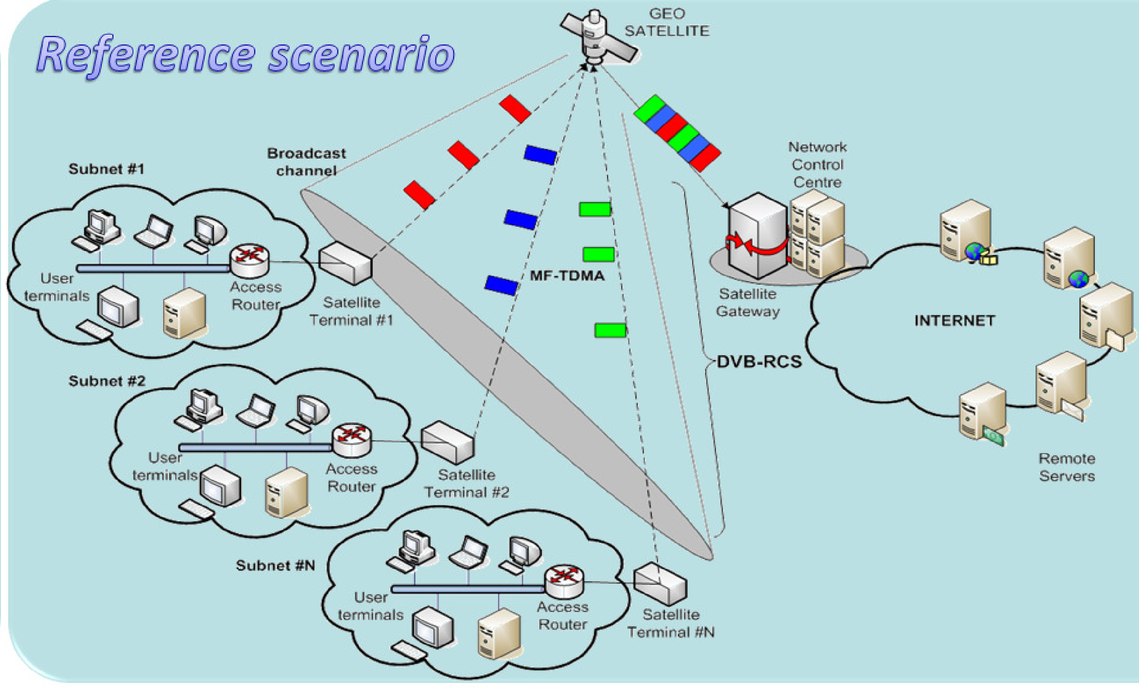
CRESM – Research Unit of University of Rome "Tor Vergata"
Department of Electronics Engineering

Satellite Multimedia Group

Summary

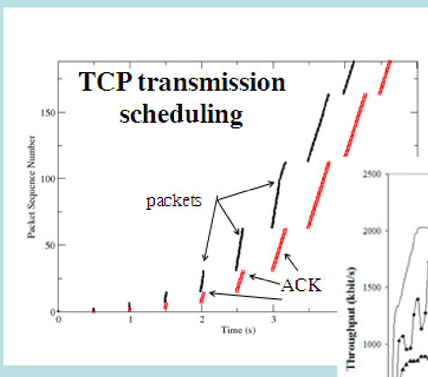


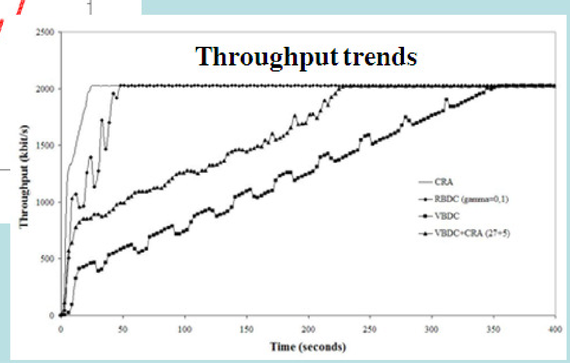
Reference scenario



- Satellite star-based architecture
- DVB-RCS standard
- DAMA algorithms to access return link
  - CRA, RBDC, VBDC
- User Terminals run TCP/IP applications
- Most of the applications require reliability – TCP at the transport layer

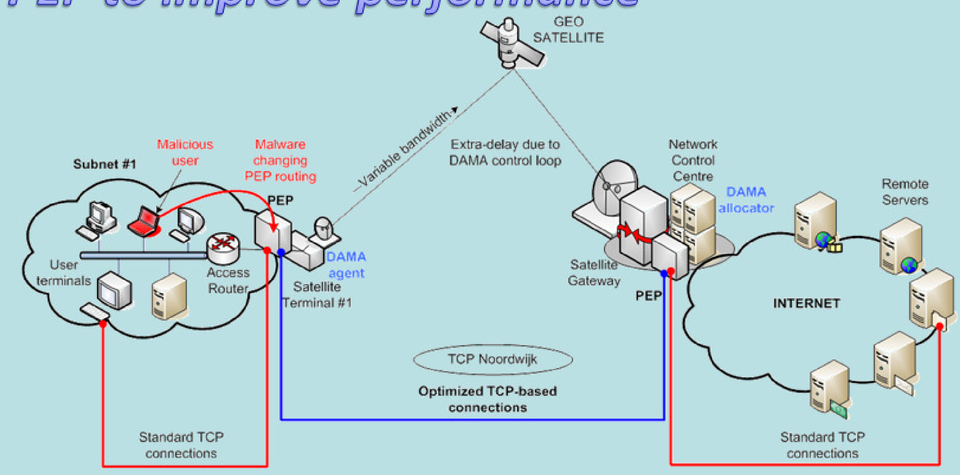
TCP over DVB-RCS: issues





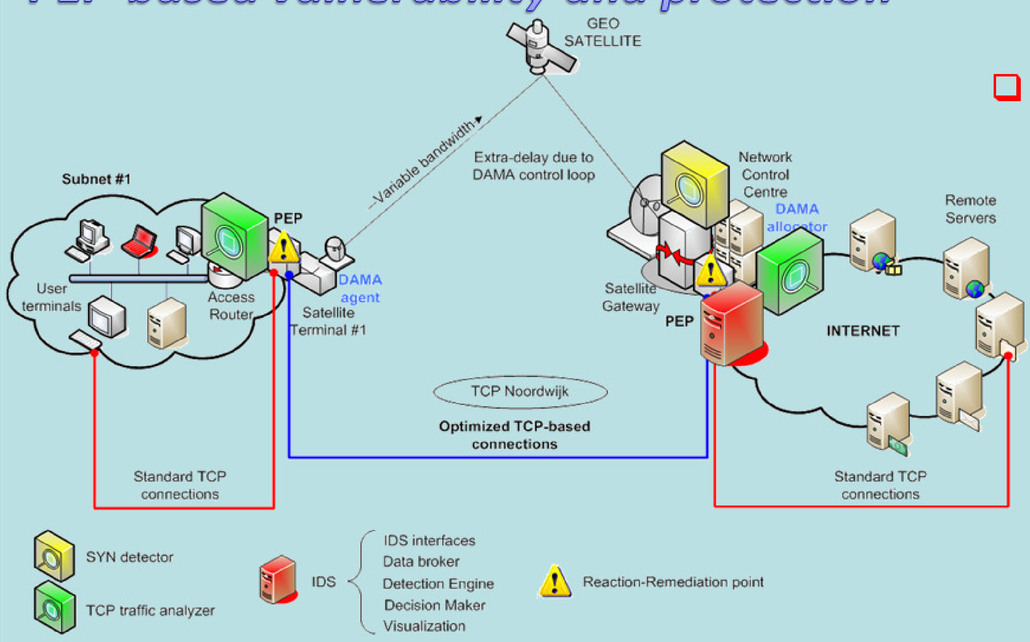
- TCP transmission is ACK-clocked
  - The higher is RTT the slower is throughput increase
  - Start up sending very slow
  - Underutilization of the available resources
- DAMA algorithms may introduce a further variable contribution to the overall RTT
  - Further slow down of BW probing
  - Misleading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

PEP to improve performance



- TCP ACCELERATION - TCP PEP at the edges of the satellite link greatly improve on performance thanks to:
  - TCP splitting architecture → reduce RTT experienced by TCP sender
  - Optimized TCP-based transport protocol over satellite sub-link → i.e. TCP Noordwijk

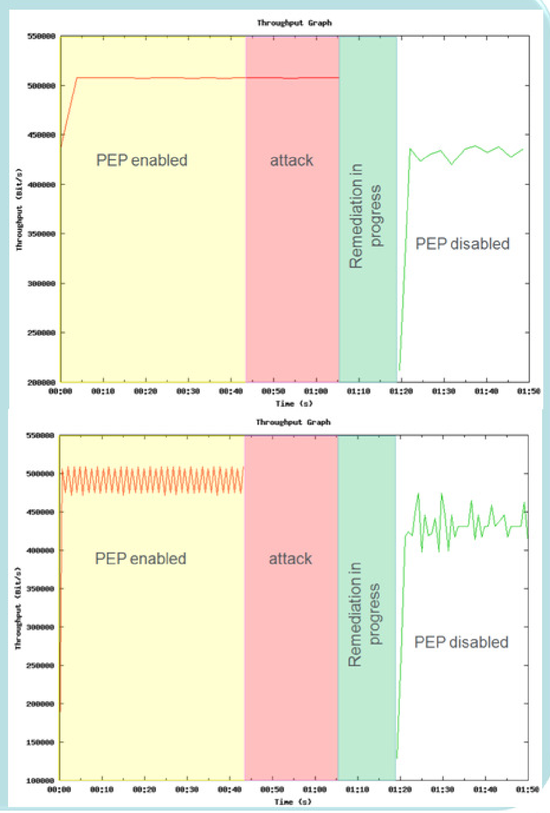
PEP-based vulnerability and protection



- VULNERABILITY - PEPs terminate connections, grab all TCP packets (in plain text) and re-route them in new connections
  - TCP PEP are incompatible with IPsec → lost of confidentiality on PEP
  - Malicious change of PEP rules may lead to drop all the crossing packets with TCP sender not aware about what is happening → lost of reliability of TCP!
- PROTECTION – Intrusion Detection System (IDS)
  - Network Probes for a distributed monitoring of TCP flows (i.e. SYN-FIN exchange, bytes crossing sub-networks)
  - Analysis to detect anomalies (Detection Engine), to decide if an attack is most likely in progress and to send an alarm
  - Reaction/Remediation to the attack: first, disable PEP to guarantee service continuity then restore PEP

Results

- Attack phase:
  - Sender trusts in a successfully transfer
  - Receiver do not receive any packets
- Remediation phase:
  - IDS detects anomaly
  - PEPs are disabled
- After remediation:
  - TCP transfer can be restarted
  - Not-optimal performance waiting for PEP restoring with correct config.



Conclusions

PROPOSED IDS ADDRESSES PEP-RELATED VULNERABILITY MAKING POSSIBLE THE COMBINATION OF OPTIMIZED PERFORMANCE AND SECURITY, AS REQUESTED FOR THE NEXT GENERATION INTERNET