A Satellite Network Emulation Platform for Implementation and Testing of TCP/IP Applications

Michele Luglio, Cesare Roseti, and Francesco Zampgnaro

Univeristà di Roma Tor Vergata –Electronics Engineering Dpt.
Via del Politecnico, 1 – 00133 Roma, Italy
{luglio,cesare.roseti,francesco.zampognaro}@uniroma2.it

Abstract. In order to assess the performance of TCP/IP based applications and protocols for communication over heterogeneous networks, simulation and emulation activities are of great importance. In particular, real time emulation provides the opportunity to reproduce realistic environment thanks to the implementation in laboratory of real architectures and protocols, avoiding utilizing real networks and in a controlled environment. We developed a broadband satellite real-time emulation platform called SNEP, designed to match the DVB-RCS European standards. The SNEP reproduces with great details the architecture and behavior of a real satellite broadband network, where it is possible to attach end-user PCs and use real protocols and applications. In this way, real network applications can be benchmarked in laboratory as in the real scenario of broadband satellite communications, at the same time proposing alternative solutions and optimizations. Furthermore with the SNEP the integration of satellite platforms with further terrestrial networks is also possible, both real and simulated/emulated, in order to extend the scope for testing.

Keywords: DVB-RCS, Broadband Satellite networks, IP, testbed emulation.

1 Satellite Network Emulation Platform (SNEP)

The SNEP is a cluster of PCs designed to reproduce the characteristics of access to a real Satellite Broadband Network, compliant with the DVB-RCS standards [1]. In particular, one side of the SNEP contains the Network Control Center (NCC)/Gateway-HUB functionalities of the satellite network, and can be connected to the Internet. The other side includes emulated Satellite Terminals (ST, or satellite modems) and user terminals, where applications and real protocols and external hardware are installed. A simplified architecture of the testbed is presented in fig. 1. The whole emulator is built with several virtual machines into a Virtual Environment, and can fully emulate several concurrent Satellite Terminals. Each machine can be connected to resemble the Satellite System real architecture (star/mesh), and performs the same logical operations to recreate the behavior of the real system (e.g., ST is performing login and sync operations, bandwidth on demand and traffic classification/shaping). All lower layers models (e.g., physical delay, interferences, etc.) has been evaluated offline and included in the platform as IP level operations.

T. Korakis, M. Zink, and M. Ott (Eds.): TridentCom 2012, LNICST 44, pp. 1–2, 2012.

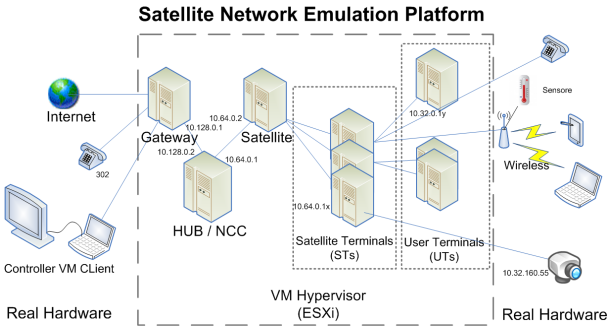

Fig. 1. SNEP logical architecture with real hardware interconnections

The SNEP in particular reproduces all signaling and effects of Bandwidth on Demand used in DVB-RCS to optimize the bandwidth utilization at the cost of introducing additional access delays (which can be much greater than 1 s). The Bandwidth on demand (called DAMA) and all other simulated blocks (error model, QoS, MAC framing and encapsulation, etc.) greatly impact on TCP/IP applications and protocols, than can underperform or misbehave in such challenging environment.

2 TCP/IP Applications Testing on the SNEP Platform

Since the SNEP testbed gives the possibility of controlling and monitoring all the system parameters (not only at network layer, but also below), one of its application can be the execution of real commercial applications (e.g., teleconferencing with Skype), to be assessed and validated before the use on a real system. In addition, the platform has been lately used to verify the impact of cyber-attacks (e.g., malware, eavesdropping, DoS from external STs, etc.) to a satellite network. Using the SNEP makes possible to install ad-hoc malware, which is producing TCP/IP unwanted traffic, or alter the behavior of some nodes. In this way it is possible to better understand possible anomalies in the network propose countermeasures and verify their validity. In particular one of the attacks tested deals with security for heterogeneous and inter-operable networks including a satellite segment. The mandatory presence of Performance Enhancing Proxies (PEPs [2]) at the edges of satellite links, justified to improve TCP performance, opens the way to several proxy-related classic attacks. In this case the focus has been on how to implement an Intrusion Detection System (IDS) and develop software countermeasure in strict relation to the emulated satellite environment.

References

1. ETSI, Digital Video Broadcasting (DVB); Interaction Channel for Satellite Distribution Systems, DVB-RCS standard EN 301 790 (2003), `http://www.etsi.org/deliver/etsi_en`
2. Interoperable Performance Enhancing Proxy, SatLabs Group, ESA, Air Interface Specifications (2005), `http://satlabs.org/pdf/I-PEP_Specification_Issue_1a.pdf`