Traffic Characterization, Routing and Security Issues in High Speed Networks Interconnected Through LEO Constellations

F.-N. Pavlidou*, M. Annoni, J.Aracil, H. Cruickshank, L. Franck, T.Ors, E. Papapetrou
***Aristotle University of Thessaloniki, School of Engineering,**
Department of Electrical & Computer Engineering, Telecommunications Division
54006 Thessaloniki, P.O.Box: 1641, Greece
Tel/Fax: +30 31 996285,
Email:niovi@eng.auth.gr

1 INTRODUCTION

The COST Action 253 is aiming to study high speed terrestrial (based on ATM technology) networks interconnected by non-GEO satellite constellations. The performance of these networks depends very much on the successful characterization and estimation of offered services and traffic loading, as well as on efficient management techniques for the integrated, terrestrial and space system.
In the context of COST253, WG1 (Traffic Characterization), WG5 (Network Security Issues) and part of WG4 (Networking) cover mainly these issues as it is seen in ANNEX I, where is also given the man-power involved in these topics.
In the following sections we shall cover in brief the research carried out and the results obtained so far in the Action during the last two years of operation.

2 TRAFFIC MODELING

A) Service Categories and Requirements

The applications foreseen for LEO constellations interconnecting ATM networks can be different as: private voice-data lines, public voice-data lines, environment monitoring, broadcasting, messaging, remote control, Internet services, videoconferencing, file transfer, tele-education etc. These services can be classified in two broad categories depending on the time constraints they can sustain [1]

a) Real time applications which can be modeled as CBR, VBR
b) Non-real time applications which can be modeled as UBR, VBR, ABR

1: The Constant Bit Rate (CBR) Service Category is used for connections that request a static amount of bandwidth continuously available during the connection. It is adequate for voice, video, and audio and is characterized by the Peak Cell Rate (PCR).
2: The Variable Bit Rate (VBR) Service is used for connecting sources alternating between active and silent periods or varying in bit rate continuously. Various parameters must be defined for the success of this service, like Peak Cell Rate (PCR), Sustainable Cell Rate (SCR), and Intrinsic Burst Tolerance (IBT). The service can be used for voice, video, data, audio etc..
3: The Available Bit Rate (ABR) Service is used for connecting sources that can modify their bandwidth according to the network availability. They are mainly data sources and two parameters must be defined for the success of the service; The Peak Cell Rate (PCR) and the Minimum Cell Rate (MCR). The service is associated with a rate-based flow control technique.
4: The Unspecified Bit Rate (UBR) Service Category is used for non-real-time applications like email, file transfer. So far, the technique does not specify traffic related service guarantees.

The QoS parameters associated with every service category are given in Table.1:(5) as they are recommended by ITU-T. 356 (U means unbounded).

	CTD	CDV	CLR
default	no	no	no
Class1	400 msec	3 msec	3.10^{-7}
Class2	U	U	10^{-5}
	CER	CMR	SECBR
default	$4\ 10^{-7}$	1/day	10^{-4}
Class1	default	default	default
Class2	default	default	default

B) Source Modeling

The activity of a source is a stochastic process, that is a family of random variables which are functions of time. The classic way to characterize a source activity is by using a closed form probability distribution. The most used ones are [2]-[4]:

1: Markovian models:
Even for special cases the analytic solution is computationally intensive thus improving the computational complexity in such systems is a topic of active research. The well known models are:
MMPP model: It is a multi-state process and has been widely used to characterize different types of traffic

such as voice, video, and images. A Markov-modulated source is governed by an underlying continuous Markov chain, with state space S, which determines the current state of the source. In each state i the source transmits information at a rate λ_i according to a stochastic process which we will call the *modulated process.* The sojourn times for each state are exponentially distributed thus the cells arrive according to a Poisson process whose intensity depends on the state of a Markov process.
When each sojourn time is over, the Markov chain moves to a state j with probability p_{ij} , which is called the transition rate from state i to state j.
ON-OFF model: It is the most popular two-state model for voice. Packets are generated during talk spurs (ON) with fixed inter-arrival time.
IPP model: It is also a two-state process differing from ON-OFF model in that the arrivals occur according to a Poisson distribution thus inter-arrival times are exponential. The discrete version of IPP is called Interrupted Bernoulli Process (IBP).
GMDP model: It is a generalization of the ON-OFF model, a multi-state process where cells are generated with constant inter-arrival time following an arbitrary distribution.
MMF model: (Markov modulated fluid) Information is general and processed as a continuous flow (fluid) at a rate which depends on the state of the underlying Markov process. The numerical complexity is independent of the buffer size. It can be viewed as an approximation to the MMPP for large buffer sizes.
PSMP model(Periodic sequense modulated Poisson): In this process the modulating process is a random periodic sequence with period N while arrivals follow a Poisson distribution with variable arrival rate.
Birth-Death Process: It is a Marcov process where only transitions to adjacent states are permitted. The arrival rate depends on the current state.
Poisson Process: A special case of the birth-death process for constant arrival rate.

2:Regression Models:
Regression models define explicitly the next random variable in a sequence via a function of previous ones within a specified time window and a moving average of a white noise. It has to be noted that these models are not convenient for queuing analysis, but mostly used in simulation studies. They can be:
Autoregressive Models (continuous or discrete with stationary or moving averages):
An autoregressive model of order p is a polynomial of correlated random variables(arbitrary probability distribution) where the factors are real numbers and the constant factor is a white noise parameter. Its autocorrelation function consists in general of damped exponentials
Regression models with constant average can model sources with fast decaying correlations while regression models with moving average can be used for sources with slow decaying correlation.
Tes models: The transform expand sample models are non-linear regression models. They aim to capture both auto-correlation and marginal distribution of empirical data.

C) Aggregate Network Traffic Modeling

1: Self Similar models:

Recent analysis of real traffic traces [5,6] clearly show that Internet traffic exhibits self-similarity features. Precisely, let X_n be the number of packets arriving in interval n and form the aggregated process $X_n(m)$ consisting of the sample mean of m non-overlapping intervals. The measured process X_n is self-similar since $X_n(m)$ is equal to X_n in distributional sense. Therefore, the process looks like a fractal: no matter the time scale that we consider the distribution remains invariant. On the other hand, we note that the burstiness of the packet arrival process also remains invariant with increasing time scale, thus severely affecting network performance.

Self-similar traffic exhibits long-range dependence in the packet counting process in contrast to Poissonian models, which show independent increments. A stationary stochastic process is long-range dependent if the autocorrelation function is non-summable. Regarding the process X_n it turns out that the autocorrelation function decays slowly as a power law ($r(k) = k^{-(2-2H)}$). The parameter H ($0.5 < H < 1$) is called the Hurst parameter and serves to the purpose of measuring the long range dependence of X_n. The effect of such slowly-decaying correlations in the queueing performance is rather striking, if we compare to the performance figures obtained with Poissonian input.

Self-similar models can be grouped in the following categories: Fluids such as the Fractional Brownian Motion, Point Processes such as Fractal Renewal Processes and Deterministic Transformations such as chaotic maps. Point processes are used to model Internet services such as the virtual terminal (Telnet), in which no bulk traffic is generated and thus differ from fluid-flow behavior. Deterministic transformations serve to the purpose of modeling the effect of some deterministic features such as the TCP timers, that explain part of the self-similarity phenomena.

However, it has been shown [6,8] that Internet traffic is dominated by TCP transactions (mostly from the FTP and WWW), for which a fluid-flow approach applies. Such transactions are generated by a large number of independent users, so that the arrival process is Poisson. However, Poisson arriving heavy-tailed bursts tend to a Fractional Brownian Motion in the limit, which is a

well-known self-similar process. A heavy-tailed distribution shows finite mean but infinite variance. Recent measurements show that the size distribution of WWW pages in the Internet is heavy-tailed (Pareto distribution) [7], thus providing a phenomenological explanation of self-similarity in terms of file sizes and transmission duration.

2: Gateway and on-board traffic modeling.

All the well known queueing models can be used for an approximated study of the on-board switch. The MMF model is considered to be very adequate for modeling the traffic of an on-board switch.
The Gateway is essentially a multiplexer. Some models have been proposed in the literature to determine the loss probability at an ATM multiplexer. [9] Models are based on the assumption of MM arrival processes but the loss probability is computationally intensive and impractical, especially when the state space of the aggregate arrival process is large. This is the case of ATM networks where we expect to have a large number of sources.

D) Geographic Traffic Models

They characterize the spatial and temporal distribution of the traffic intensity. Since satellite network planning concerns cells of very big coverage it is impossible to model subscribers separately. Also, the movement of subscribers for LEO systems can be neglected in comparison to the speed of satellite beams. Thus, to analyze the network load in global mobile satellite systems, a global geographic traffic model is needed.
These models [10], [11], [12] estimate the traffic as a function of various demographic and cultural data (population, income, mobiles penetration etc). Object oriented programming has been recently used to simulate such models.
An appropriate geographic traffic model for LEO loading is currently studied in COST253 Action.

3 ROUTING IN LEO CONSTELLATIONS

A) Routing Principles.

Designing routing algorithms for a network architecture is a delicate process. This is mainly due to the two sided aspect of routing. On the one hand, routing is a key factor in order to guarantee efficient use of resources and therefore to minimize the operating costs. On the other hand, routing is a process having a direct influence on the quality of service the user is provided with. As a result, the goal of a routing algorithm is to achieve a balance between operating costs and quality of service, the difficulty lying in the fact that these two aspects are dual.

Routing algorithms have been studied since a long time, however the characteristics of the LEO constellations environment call for revisiting this classical research domain. Indeed, as far as legacy terrestrial routing is concerned, the topology can be considered quasi-static. This assumption does not hold anymore with LEO constellations and terrestrial ad-hoc networks. Considering LEO constellations with inter satellite links, the satellite movement leads to a dynamic, although deterministic, topology. Furthermore, taking into account pointing, acquirement and tracking requirements of antennas, some ISLs are not permanent as well are the links between stations and satellites (this type of link is referred to as up/down link). Considering a connection oriented environment, the dynamics of the constellation causes handover (or handoff) of a connection where the connection is interrupted and must be rerouted in a seamless way from a user stand point. Taking into account all these aspects, routing algorithms for LEO constellations must face two challenges: handling numerous topology changes as well as numerous route computations caused by handovers. Unfortunately, these two aspects raise several routing design issues referred to as scalability and convergence rate. These are two crucial topics often considered in the routing litterature.

Finally, given the broadband services currently proposed, it is mandatory for the routing algorithm to support Quality of Service. It consists in having a communication channel which characteristics are defined as a contract between the user and the network. Although, QoS routing is not a characteristic of LEO environments, unresolved issues still exist that have to be sorted out for both terrestrial and spatial networks.

Referring to previous studies on routing algorithms, it is possible to define a set of criteria helping in the classification of routing algorithms. These criteria are the following:

- Adaptivity to traffic variation, or more generally to topology changes.
- Pre-computed route or on-demand route computation or a mixed approach.
- Centralised or decentralised or distributed route computation.
- Legacy or Type of Service or Quality of Service routing.
- Unicast or multicast routing.
- Connection less or connection oriented mode.

In [18], a survey of all these considerations and their impact on LEO routing is conducted. Considering the complexity of routing algorithms as well as the complexity of LEO constellations, studies on routing

algorithm performance are often realised using simulations. For these reasons, in the Cost 253 action, two research efforts are currently undertaken on that topic. The first one [17] implements a terrestrial routing algorithm, known as Flow Deviation, and studies its performance in a LEO environment using metrics such as end-to-end delay and network load distribution. The second one [15] aims at providing a simulation framework for studying link state routing algorithms for QoS and connection oriented environments.

Future work will consist in the follow up of these two research efforts in order to quantify the influence of the different factors taking part in the overall performance of routing algorithms.

B) Reliability Issues

The classical definition of reliability is the following (19):
Reliability is the probability that a device will operate successfully for a specified period of time and under specified conditions when used in a manner and for the purpose intended.
Reliability values are usually expressed as probabilities.

The definition of a general reliability model for a satellite network could be faced by first identifying the catastrophic and the partial failures of the system and then by defining different independent sub-models which jointly concur to the overall satellite reliability.

The modeling methodology consists of the following steps:

1. Reliability modeling and off-line analysis
   Development of the reliability model of each independent satellite subsystem.
   Collection of typical elementary or aggregated failure rates for the elements included in the reliability model.
   Calculation of the reliability as a function of time for each satellite subsystem.
2. Constellation cycle of life modeling and off-line simulation
   Hypothesis about the constellation deployment plan.
   Hypothesis about the constellation O&M policy.
   Simulation of one constellation cycle of life.

A preliminary list of failure modes relevant for the design and the performance evaluation of routing schemes is provided as an example. As additional failure modes will be identified, they will be added to this list and modeled accordingly.

1. Catastrophic satellite failure-The satellite has no more routing capability
2. Single in-plane ISL failure
3. Single cross-plane ISL failure
4. Double in-plane ISL failure-The satellite can receive packets only from satellites on adjacent planes (under the hypothesis that the satellite has just one front and one back ISL)
5. Double cross-plane ISL failure- The satellite can receive packets only from adjacent satellites on the same orbital plane (under the hypothesis that the satellite has just one left and one right ISL)
6. In-plane island-Composite failure of two opposite (front and back) ISL's on two adjacent satellites on the same orbital plane (under the hypothesis that the satellite has just one front and one back ISL)
7. Cross-plane island-Composite failure of two opposite (right and left) ISL's on two satellites on the adjacent orbital planes (under the hypothesis that the satellite has just one left and one right ISL).

4 SECURITY ISSUES

The security systems in second generation mobile systems (such as GSM) have been very successful until now. However, the increasing demand for security by users, network operators and regularity bodies calls for more advanced security features in the third generation systems such as Universal Mobile Telecommunications Systems (UMTS). UMTS security [20] can be used as a template to address the satellite network security.

The satellite access to communication networks produces special security problems for the following reasons:

- Eavesdropping and active intrusion is much easier than in terrestrial fixed or mobile networks because of the broadcast nature of satellites.

- Satellite channels experience high bit error rates which may cause the loss of security synchronization. This demands a careful evaluation of encryption systems to prevent Quality of Service (QoS) degradation because of security processing.

- Satellite networks, inherently, experience long delays, therefore satellite security systems must be efficient and should only add a minimum delay.

The biggest obstacle preventing the progress of security deployment in communication networks (in general) is political rather than technical, because different countries have different rules and regulations about security issues. Therefore, any security system proposed for satellite ATM networks must be flexible to allow rapid implementation of various encryption systems and key lengths to comply with different countries national rules and regulations [21], [22].

A) Security Aspects of Satellite ATM Networks

1:Transmission Rate and Encryption Key Updating

The encryption block size in a typical cipher (such as DES) is 64 bits and no more than 10^9 blocks should use the same key to prevent intruders analysing the data [23]. ATM has been designed for high data rates, therefore, there is a need for a mechanism to change the encryption key frequently. For ATM traffic, the lifetime of the encryption key can be calculated (ignoring the ATM and other headers overhead) as follows:

- For data rates of 155 Mbps: The key lifetime is about 6.9 minutes.
- For data rates of 2 Mbps: The key lifetime is about 8.9 hours.

Therefore at lower rates a single encryption key can be used for the whole duration of connection. While at higher rates the key has to be changed frequently. The ATM Forum [23] uses the master-key concept which can be used to derive several session-keys. The master-key concept is implemented in this paper for the U-S authentication and key exchange protocol.

2: Encryption Synchronization in High Bit Error Rates

Satellite channels, normally, experience high bit error rates and errors are of bursty nature. Therefore it is important to examine the impact of such errors on ATM cell payload encryption performance.

Two types of errors can occur, one is the complete loss information bits (slips) but this does not affect the encryption unit, because the Transmission Convergence (TC) sub-layer will detect that through the cell delineation function, before it reaches the ATM layer (and the encryption unit). The second type of digital errors is the information bit changing its value (0-to-1 or 1-to-0 This type of error will affect the decryption outcome on the receiver.

Secret-key systems can be used for bulk data ciphering (encryption) because they are much faster than public-key systems. Therefore, let us analyze a typical encryption system namely the Digital Encryption Standard (DES). DES can be used in Cipher Block Chaining (CBC) mode where the previous cipher block affects the encryption of the present cipher block. CBC mode is considered to have good security and is widely implemented [24]. An ATM payload (48 bytes) can be divided into 6 DES cipher blocks of 64 bits (8 bytes) each. In case of bit/bits errors in a DES cipher block, generally one ATM cell will be affected except when the error occurs in the 6^{th} DES block (last block in the ATM cell). This will affect the first block of the next cell. Therefore, in the worst case, bit errors in a single DES block (64 bit) will affect up to 1.1666 ATM cells. Therefore DES in CBC mode is considered suitable for satellite networks. A detailed description of the hardware realisation of such a DES/TripleDES encryption board including CBC is shown in another paper presented university of Surrey to this cost253 meeting.

3: Reducing the Cost of Satellite Network Infrastructure

User authentication is an important issue for satellite Network operators in order to prevent fraud and protect revenue. However, information privacy and integrity is an end-to-end service and only concerns the user and the Service provider. Therefore, the role of satellite network operator should be confined to user-network mutual authentication only. In order to reduce the cost of network infrastructure, data privacy and integrity can be taken out of the satellite network.

End-to-end data encryption can be performed between the user and the server provider. To conform with ATM Forum specifications, the encryption can be performed in the ATM cell payload only. The clear ATM header allows easy cell routing and switching by the satellite ATM network.

Digital signatures can be used to authenticate any other signalling and management messages exchanged between the user-network such as satellite handover and call termination messages.

CONCLUSIONS

Some important topics for the overall performance study of an integrated terrestrial and space satellite network were investigated and adequate techniques for their study were proposed. Traffic characterization remains a basic issue and a quite big part of activities in COST253 were devoted to the topic, aiming to produce very soon an effective simulation tool. Routing, in conjunction with its reliability aspect, constitutes another fundamental point for study, so big efforts were put on a detail research on this subject. The main selection criteria were clearly defined and the first simulation results offered a very helpful insight in the performance of several routing algorithms in non-GEO satellite networks.

Finally, for a successful implementation of the new satellite networks, it is essential to address the security requirements of users, satellite network operators and multimedia service providers which can either be part of the satellite network or be located outside the satellite network boundaries. The impact of satellite environment constraints such as long delays and high bit error rates on security processing must be examined. In order to minimize the cost of implementing security systems for satellite ATM networks, the network

operator role in security service can be limited to mutual authentication with the satellite user during the call set-up period.

REFERENCES

[1] T.Ors et al." An Overview of Source Modeling" COST253 TD (98) 001

[2] L.Kleinrock "Queueing Systems " Vol. 1, John Wiley, 1975

[3] G.Babic et al "Analysis and Modeling of Traffic in Modern Data Communications Networks", http://www.cis.ohio-state.edu/~jain/

[4] J.Daigle and J.Langford " Models for analysis of packet voice communications systems" IEEE JSAC. Vol 4, pp. 847-855, Sept. 1986

[5] W.E.Leland et al " "On the self similar nature of Ethernet traffic", IEEE/ACM Trans. on Net. Vol.2, no 1, pp. 1-15,1994

[6] V.Paxson and S.Floyd, "Wide-area traffic: The failure of Poisson modeling" IEEE/ACM Trans. on Net. vol. 3, no, pp. 226-244, 1995

[7] M.Crovella and A.Bestavros, "Self-Similarity in World Wide Web Traffic: Evidence and Possible Causes", IEEE/ACM Trans. On. Net. Vol.5, No 6, pp 835-845, 1997

[8] J.Aracil "On Internet Traffic Self-Similarity", COST253 TD (98) 002

[9] N.Shroff and M.Schwartz, "Improved Loss Calculations at an ATM Multiplexer", IEEE/ACM Trans. on Net. Vol.6, No 4, August 1998.

[10] G.Schorcht, et al "A Global Traffic Model for Simulation of the Network Load in Mobile Satellite Communication Networks" Proceedings of ICT98, Greece

[11] M.Werner et al: "Analysis of System Parameters for LEO/ICO –Satellite Communication Networks" IEEE JSAC Feb. 1995

[12] A.Jamalipour et al : "Traffic Characteristics of LEOS-Based Global Personal Communications Networks" Comm Magazine, Feb 1997

[13] L.Franck "Routing in LEO Satellites" COST253 TD(98) 006

[14] E.Papapetrou et al "Traffic and Routing simulator for LEO Constellations" COST253 TD(98)012

[15] L.Franck "LeoSim: a routing simulator for LEO's" COST253 TD(98)015

[16] E.Papapetrou et al "Performance evaluation of LEO…." COST253 TD(99)002

[17] E.Papapetrou et al "Performance study of adaptive routing algorithms foe LEO satellite constellations under self-similar and Poisson traffic" COST253 TD(99)003

[18] L.Franck COST253 TD(99)004 "Routing in Leo constellations with Intersatellite Links" COST253 TD(99)004

[19] M.Annoni "Reliability modeling for sat constellation.systems." COST253 TD (99) 006

[20] : ASPeCT project: Advanced Security for Personal Communication Technologies.
Migration/Evolution Towards UMTS- Security Issues

[21] H. Cruickshank "Authentication Protocols to Secure Satellite ATM Networks", COST253 TD (98) 016

[22] H. Cruickshank "Security systems design and implementation examples in ATM networks " COST TD (98) 017

[23] ATM Forum. ATM Security Specification Version 1.0 draft. 1998.chneier, B. Applied Cryptography. J. Wiley & Sons, 1996.

[24] Schneier, B. Applied Cryptography. J. Wiley & Sons, 1996.

ANNEX I

WG1: Traffic characterization

1.1:Types of services for different network architectures.
1.2:Source modeling for any service type.
1.3:Traffic modeling at the LAN gateway for fixed or mobile terminals.
1.4:Traffic in/out the satellite node for passive or regenerative satellites (switching) for various channel access techniques.
1.5:An end-to end traffic model justified by simulation work.

Participating Institutions
University of Bradford
University of Cantabria
Universite Libre de Brussels
University of Navarra
University of Surrey
Aristotle University of Thessaloniki

WG5: Network Security issues

Task 5.1: Study of threats and security requirements for interconnecting LANs through non-geostationary satellites. Also, identification of suitable encryption and digital signatures systems.
Task 5.2: Propose authentication and encryption key exchange protocols.
Task 5.3: Examine satellite-ATM security implementation details.
Task5.4: Assess other issues such as Trusted Third Parties, network management security and billing.

Participating Institutions
University of Surrey

WG4: Networking

Task 4.1 Identification of functional and network architecture
Task 4.2 LAN-Gateway Interconnection
Task 4.3 Network Operation
Task 4.4 Transport Layer Function
Task 4.5 Link Layer Functions

Participating Institutions
CSELT
CNUCE/CNR
ENST
JSI
University of Bradford
University of Brussels
University of Navarra
University of Surrey
Aristotle University of Thessaloniki