



JORNADAS DE SEGUIMIENTO

PROYECTOS EN TECNOLOGÍAS DE LA INFORMACIÓN

DESCRIPCIÓN DE RESULTADOS

Referencia del proyecto: TEL1999-0822

Título: SISTEMA SEGURO DE ACCESO Y DISTRIBUCIÓN EFICIENTE DE SERVICIOS MULTIMEDIA (SSADE)

Investigador principal: Dr. Jorge Mata Díaz

Dirección de contacto:

UNIVERSIDAD POLITÉCNICA DE CATALUÑA
ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA DE TELECOMUNICACIÓN
DEPARTAMENTO DE INGENIERÍA TELEMÁTICA
Sor Eulalia de Anzizu (Módulo C3 Campus Nord)
08034 - Barcelona

Datos sobre el grupo investigador:

Línea de Investigación de Servicios Telemáticos de la Universidad Politécnica de Cataluña. (Código 33259928-00). Personal investigador:

Mónica Aguilar Igartua, Juan José Alins Delgado, Luis Javier de la Cruz Llopis, Jordi Forga Alberich, Juan García Haro, Jorge Mata Díaz, José Luis Melús Moreno, Esteve Pallares Segarra, Josep Pegueroles Valles, Marcos Postigo Boix y Francisco José Rico Novella.

¿Se trata de un proyecto coordinado? No

Referencia del proyecto:

Investigador principal:

Dirección de contacto:

Referencia del proyecto:

Investigador principal:

Dirección de contacto:

1. PROJECT OBJECTIVES

In this project, a system for the access and distribution of multimedia services is proposed. Especial attention is paid to Video on demand and near on demand services, where interactivity and quality of services are a key issue. The main objective is to develop an efficient and accurate transmission method joint to an effective network resource assignment. For that purpose, the entire system will be simulated and intensively evaluated. It is necessary to remark the novel addition of security techniques, ciphering the transmitted traffic and authenticating the user access by using intelligent cards or CD-ROM cards.

The proposed service starts when a client wants to view any multimedia content. The client accesses the server Menu via a web browser. After that, the client can select his own preferences: film or content to retrieve, speed connection, quality requirements, etc. Once the server knows exactly what the client wants, he asks for an electronic payment. When this is done, the server returns to the client the data he will need in order to get the multimedia stream. Usually, he gives to the client the name of the host where the data can be found and a socket port where to connect. Finally, the client is able to connect to the video stream bomb to get the purchased content.

Timetable of task to develop:

Task Description	First year	Second year	Third year
Task 1. Platform instalation and management			
	x x x x x x x x x x x x	x x x x x x x x x x x x	x x x x x x x x x x x x
Task 2. Definition and preliminary implementation of work packages. Simulation of efficient bandwidth management and QoS parameter identification Study of transmission techniques and Internet protocols. Develop of a MPEG-II Video coder-decoder software and ciphering algorithms	x x x x x x x x x x x x	x x x x x x x x x x x x	
Task 3. Testbet implementation an integration. Network QoS configuration. Develop of the efficient and secure MPEG-II transmission sender and receiver, SSADE user interface and secure functionalities on the service access.			
Task 4. QoS evaluation. Efficient network resource analysis. Server and network resources requirements for video on demand services. Subjective image quality degradation on congested networks			

Cost summary in pesetas:

Annual Payment	First year	Second year	Third year	Total
Durable equipment	3.200.000	3.200.000	3.200.000	9.600.000
Consumables	300.000	300.000	300.000	900.000
Travel and Subsistence	1.500.000	1.500.000	1.500.000	4.500.000
Total Costs	5.000.000	5.000.000	5.000.000	15.000.000
Overhead Costs (12%)	6.000.000	600.000	600.000	1.800.000
Contribution from CYCIT	5.600.000	5.600.000	5.600.000	16.800.000

2. LEVEL OF SUCCESS

2.1. Results on efficient video transmission

The high level of QoS needed for VBR video services together with its bursty nature difficult the efficient use of transmission channels. In order to improve this channel utilization efficiency, some services based on dynamic resources allocation have been analyzed. In this project, two new mechanisms to carry out these kinds of services for VBR MPEG video transmission have been proposed. The first method is based on a previous characterization of VBR MPEG video traffic that gives rise to a bidimensional MMFP model. The own nature of this model allows identifying three levels of activity (regular, high and great) in the VBR video sources. Moreover, the threshold values between these levels are also provided. The second method is used on prerecorded video sequences where a pre-processed analysis is performed in order to determine the exact bandwidth requirements on the transmission considering the receiver buffer fullness. These methods take advantage of MPEG-2 SNR scalability possibilities and traffic smoothing methods. The use of smoothing techniques to remove the periodic fluctuations of the bit rate generated by the codification modes of the MPEG algorithm is very suitable in video transmission. In this way, the multiplexing gain is maximized and the resource allocation is reduced on packet networks.

To implement the first method a new element, called Supervisor and Controller (SC), has been developed. Its functionality consists of requesting and releasing network resources as a function of the video source activity level. Moreover, if the requested resources are not available, the SC regulates the source bit rate in order to agree the traffic contract with the network. This functionality can be used also in situations of network congestion. The bit rate is adjusted for real time coded video by means of the increment of the quantification parameter Q. In this case, a new VBR MPEG traffic shaper is used. This shaper use prediction techniques to smooth the traffic. The applied technique is based on the characterization of real traffic as an ARIMA process.

The benefits achieved with the renegotiation system have been quantified in terms of renegotiation gain. In this sense, the classical VBR service has been compared with the proposed renegotiated variable bit rate (RVBR) service. The main observed consequence is the decrement of the renegotiation gain when the number of multiplexed video sources is increased. This is due to the fact that with a large number of multiplexed sources the VBR service achieves the optimal resources allocation. Therefore, the 3 levels RVBR service can not offer a better performance. Thus, the advantages of services with bandwidth renegotiation in front of the classical VBR service appear when the number of multiplexed sources is smaller.

In order to validate the functionality of the proposed SC element some experimental results have been performed. First, a situation where renegotiations are always blocked has been studied and the behavior of the SC has been validated. Later, the SC functionality has been tested when renegotiations are allowed after a processing delay. Finally, some simulations with four real traffic traces have been carried out in order to validate the generality of the threshold values between activity levels. Also, the new shaper scheme has been compared with the classics storing systems. The main disadvantage of these systems is the delay introduced in each frame. Nevertheless, the new scheme has a smaller and bounded delay. This characteristic allows to employ this shaper for interactive services, where small delays are needed.

The second proposed method is based on the renegotiated constant bit rate (RCBR) mechanisms. Among all dynamic resource allocation techniques RCBR is the simplest one. In these, a source can renegotiate its contract rate to the network by sending a signaling message in which increase or decrease of the present rate is asked for. If the network admits the renegotiation, the source can send data to a new constant rate. In other case the video encoder will have to adapt to the available rate or the exceeding information will be lost and a degradation of quality of service will occur. The most important parameters when designing a RCBR service are contract rate levels and instants when renegotiation takes place. Different ways of determining these parameters are taken depending on the type of video service desired. If a stored video-on-demand service is wanted, an optimal renegotiation pattern can be calculated a priori.

The proposed 2-RCBR technique has the aim of balancing high bandwidth efficiency with simple preprocessing algorithms. The simulation results present a suitable adaptation of the 2-RCBR algorithm to deliver MPEG2 scalable sequences into the network. The method not only allows a proper delivery but also provides a simple and fast method of controlling call accepts in a video server.

2.2. Operation and security in video on demand service

Little by little troubles related to bandwidth and QoS have been overcome in current multimedia communications. As these problems are being solved security concerns have been getting increasing significance in data, voice and video transmissions. When cryptographic techniques want to be added to advanced video services such as video-on-demand many aspects have to be considered. First of all multimedia requirements are very time-restrictive, this is why unreliable protocols such as UDP are used, so ciphering techniques cannot rely on transport protocol and they may be fitted to isolated protocol data units (PDU), in any other case, a packet loss will cause forward errors. Secondly, ciphering algorithms may not increase significantly the packet delay. If this occurs, security increase will lead to visual quality decrease or excessive transmission delay, and interactive services will not be possible. Finally, when commercial services are being offered, aspects related to secure payments, server fraud protection and client rights have also to be studied.

The Security Module in SSADE (Secure System for the Access and Efficient Distribution of Multimedia on Demand Services) has centered his investigations in two main items: Secure and Anonymous Payment and Ciphering Techniques for protecting data from eavesdroppers. All this work was developed to join the other modules efforts so a common video server architecture was considered.

The first important point to cover by the Security Module was the prevention of privacy. It should be impossible to anyone but the server to know what the preferences of the client are. This is a well known subject in nowadays open communications. Typically these kind of matters are solved by using SSL (Secure Sockets Layer) protocol. Our prototype has a Secure Web Server to which the client is connected. The client can verify the server identity and be sure to whom he is asking for multimedia content. Identities are guaranteed through digital certificates issued by an own Certificate Authority.

Once the content data based is looked up and the service is chosen, the client will be asked for a payment. The simplest scheme for secure payments consists of three parties: the seller, the buyer and the bank. The buyer, the one who asks for a certain service and must pay for it. The seller, that who offers the service and will receive money for it and the bank (or financial institution), a third party from which the buyer's money is drawn and to which it is returned as seller's income. Likewise, this scheme is divided in three actions: withdrawal, payment and deposit. According to the time when these actions take place the secure payment methods could be classified into pre-payment, instant payment and credit.

When electronic payments are considered, new features arise. In some cases it is desired that the client identity will remain anonymous. This seems a contradiction with identity guarantee, but can be overcome if we assure the client is an authorized purchaser although we do not know his actual identity. When these new features are offered new threads appear: token forgery and double spending. The method must prevent anyone from being capable of issue a valid token (or electronic coin), furthermore a valid token (issued by the authorized entity) must not be used more than once. Usually, when such payment features are desired, tamper-proof devices as smartcards are used.

The Secure Payment method in SSADE project protects client identity (is anonymous) and warrants the seller to be paid for his services. It is also an off-line and pre-payment method. It avoids token forgery by using public key cryptography and hardware devices. It also prevents double-spending by using spent-tokens data bases. Instead of using smartcards, the SSADE payment method uses CD-ROM cards containing valid token and seller data.

As we mentioned before, the data should be protected from unauthorized third parties. This is easily achieved by means of symmetric ciphering. The inclusion of ciphering algorithms in multimedia communications is critical in terms of time. Cryptographic techniques must not add significant delay to data transmission or excessive packet loss due to time constraint violation will occur.

The SSADE project includes symmetric ciphering to the data stream, but it distinguishes between server side and client side due to its different hardware features and time requirements.

- a) Client Side. This is the less time restrictive side cause usually just one multimedia stream will be deciphered by a client. In the other side, it is important to the client to be as much universal as possible. This is why the client side will be developed in JAVA language. This allows the client to be loaded via web by using the applet technology. This chooses greatly simplify the development of the client side since JAVA has a wide variety of cryptographic tools. The study and right election of the cryptographic tools of the client side was another important item in the SSADE Security Module.
- b) Server Side. Typically, a multimedia server can serve of the order of tens of video streams. This reduces at most the computational load that can be offered to the server. An optimized C

programmed DES algorithm has been developed in order to allow the server to cipher many different streams without having an effect over the total delay. This optimized version offers a throughput of 30Mbps over a 500 Mhz P-II.

2.3. Experimental QoS network environment

The client-server system designed for this study will be implemented on LINUX operating system. This implementation allows the study of the system in a controlled scenario to validate the QoS performance of video streams. The system topology consists of three nodes. The client is accessing to one node, while the server is supposed to be connected to a far end node. We use UDP/IP to transfer information between the server and client. In the middle, there is an intermediate Linux routing node that enables the introduction of QoS on the network. We use a traffic source generating best-effort traffic between the routing and the client nodes to simulate the network dynamics.

The resource reservation protocol assumed is RSVP. In this operating system, RSVP daemon acts as a user space process that handles the traffic control done by the LINUX kernel. RSVP will create and handle queue disciplines, classes and filters -in the router device- as needed by the resources reservations requested from the client applications in order to provide the requested QoS.

In this Project, RSVP Version 1 from USC ISI (University of Southern California, Information Sciences Institute) has been used. USC Information Sciences Institute (ISI) has taken a leading role in the development of RSVP and Internet Integrated Services. Much of this work has been done under two successive RSVP projects which were funded by DARPA ITO.

3. RESULTS

3.1. PhD theses

Two PhD theses have been presented for the research staff of this project. Exact references of these works are included on the Appendix A.

3.2. Publications

Several publications have been published as results of the research works developed by research staff of this project. Exact references of these works are included on the Appendix B. The profit of this work is reflected on this summary:

Number of International magazine publications: 1 accepted and 1 submitted

Number of National magazine publications: 1 published

Number of International Communications Conferences: 12 published and 1 submitted

Number of National Communications Conferences: 7 published

Number of Internal Reports: 2

3.3. Patents

"Procedimiento para realizar pagos a través de Internet mediante una tarjeta de pago basada en CDROM no circular". Josep Pegueroles, Francisco Rico. Patent number 200002611.

3.4. Technology transfer. Participation in other national and international projects.

This project is not related on other national or international technology transfer projects.

3.5. Collaboration with other research groups

This project is not related on other national or international technology transfer projects.

Appendix A. PhD theses.

Title: *Contribución a la Evaluación y Dimensionado de Nodos y Enlaces en Redes de Alta Velocidad.*

Author: Esteve Pallarès Segarra

Advisor: Dr. D. Joan García Haro

Date: 6-june-2001

Title: *Contribución al Modelado y Caracterización de Nodos en Redes de Banda Ancha. Aplicación al Multiplexor Inverso ATM.*

Autor: Mónica Aguilar Igartua

Advisor: Dr. D. Joan García Haro

Date: 21-january-2000

Apéndice B. Publications.

International Magazines

- M. Postigo-Boix, J. García-Haro, M. Aguilar-Igartua, "IMA: Technical Foundations, Application and Performance Analysis.", The international journal of computer and telecommunications networking, Computer Networks 35 (2001) pp. 165-183. Elsevier.
- M. Aguilar-Igartua, J. García-Haro, M. Postigo-Boix, "ATM Inverse Multiplexing. Fundamentals and Markovian Single Server Queue Analysis for Performance Evaluation and Validation Purposes", submitted to the Telecommunication Systems.

National Magazines

- Josep Pegueroles, Juan José Alins. Navegar seguro por internet.. Revista Buran, num 16. Diciembre 2000

Internacional Communications Conferences

- L. J. Cruz and J. Mata, Performance of Dynamic Resource Allocation with QoS guarantees for MPEG VBR Video Traffic Transmission over ATM Networks, Proceedings of the IEEE Global Conference on Communication, pp. 1483-1489 , Rio de Janeiro, Diciembre 1999. ISBN 0-7803-5796-5.
- L. J. Cruz and J. Mata, "Asignación Dinámica de Recursos para la transmisión de Vídeo MPEG VBR sobre redes ATM", TELECOM'2000, Cuba, CD, ISBN 84-8138-393-7.
- Josep Pegueroles, Juan José Alins, Luis J. de la Cruz, Jorge Mata. Two-level renegotiated constant bit rate algorithm (2RCBR) for scalable MPEG2 video over QoS networks.. SPIE Information Technologies and Communications Conference (ITCom2001) Denver, August 2001.
- Josep Pegueroles, Juan José Alins, Jorge Mata, Luis J. de la Cruz Two-level renegotiated constant bit rate algorithm (R-CBR) for stored video services over QoS networks.. Submitted to ICC2002.
- M. Postigo-Boix, J. García-Haro, M. Aguilar-Igartua, "Inverse Multiplexing for ATM. Technical Operation, Applications and Performance Evaluation Study", Fifth IEEE Symposium on Computers and Communications, ISCC'2000, Antibes-Juan les Pins, France, 4-6 July, 2000.
- Marcos Postigo-Boix, Joan García-Haro, Mónica Aguilar-Igartua, "Inverse Multiplexing for ATM. Performance Evaluation Under Different Traffic Patterns", SPECTS 2000, Vancouver, British Columbia, 16-20 July 2000.
- Mónica Aguilar Igartua, Joan García Haro, Marcos Postigo Boix, "Multiplexación Inversa ATM. Funcionamiento y Evaluación de Prestaciones". FIE'2000, 12-14 July, 2000.Cuba.

- Marcos Postigo Boix, Joan Garcia-Haro, Mónica Aguilar Igartua, "Cost Minimization Study in the Client-Server Transmission of Semi-Elastic Flows Using Internet". 2001 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, PACRIM'2001, pp. 188-191, 26-28 August 2001, University of Victoria, Victoria, Canada.
- E. Pallarès and J. Garcia-Haro, "Mathematical Approach to Designing Switched LAN's. An Alternative Solution to Compute the Loss Probability in an Heterogeneous Traffic Environment", 10th Mediterranean Electrotechnical Conference (MELECON'2000) , vol. 1, pp. 11-14, Lemesos, Chipre mayo 2000. ISBN 0-7803-6290-X.
- E. Pallares and J. Garcia-Haro, "Fluid-Flow Approximation of the Information Loss Probability for a Switching System with Finite Buffering under Heterogeneous ON/OFF Input Traffic Sources", Fourth International Workshop on Queuing Networks with Finite Capacity (QNETs 2000), pp. 35/1-35/10, Ilkley, Reino Unido, julio 2000. ISBN 0-9540-1512-6.
- E. Pallarès and J. Garcia-Haro "An Efficient Heuristic Methodology to Design Switched LANs". 2001 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, pp. 192-195, Victoria, Canada, august 2001. ISBN 0-7803-7080-5.
- F.J. Rico, "How to strengthen DES", Julio 12-14, 2000, pp.84, Telec' 2000, Cuba, ISBN 84-8138-393-7
- Josep Pegueroles, Francisco Rico. Rekeying System for Large Secure Multicast Groups using Vector Space Secret Sharing Schemes. NGC2001 3rd International Workshop on Networked Group Communications. UCL, London, November 2001.

National Communications Conferences

- Josep Pegueroles, Juan José Alins, Jorge Mata, Luis J. de la Cruz. Algoritmo simple y eficiente de renegociación a dos niveles para redes con calidad de servicio. Jornadas de Ingeniería Telemática. JITEL'01. Septiembre 2001
- M. Postigo-Boix, J. García-Haro, M. Aguilar-Igartua, "Análisis de Minimización de Costes en la Transmisión de Flujos Semi-Elásticos sobre Internet", in the Proceedings of the III Jornadas de Ingeniería Telemática (JITEL 2001), Barcelona, September 2001, pp. 37-44.
- F.J. Rico, E. Sanvicente, 128-EDES, VI Reunión Española sobre Criptología y Seguridad de la Información, pp 73-78, Tenerife, 14-16 septiembre 2000.
- M. Postigo-Boix, J. Garcia-Haro, M. Aguilar-Igartua, "Transmisión Eficiente de Bloques en Tiempo Real sobre Redes IP", Proceedings of URSI 2000, Zaragoza, Spain, September 2000, pp. 405-406.
- E. Pallarès, L. J. De la Cruz y Joan García, "Estudio de la Probabilidad de Pérdida en un nodo de Conmutación Mediante modelos de Fluidos", Actas del XV Simposium Nacional de la Unión Científica Internacional de Radio, pp. 407-408, Zaragoza, 13-15 septiembre 2000. ISBN 84-600-9597-5.
- E. Pallarès y Joan García, "Metodología de Diseño para la Planificación de Redes Conmutadas en Entornos Locales.", III Jornadas de Ingeniería Telemática, Jitel'01, pp. 157-163, Barcelona, 19-21 septiembre 2001. ISBN 84-7653-783-2.
- F.J. Rico, J. Torres Galiano, Secráfono software sobre PC multimedia, VI Reunión Española sobre Criptología y Seguridad de la Información, pp 73-78,. Tenerife, 14-16 septiembre 2000.

Internal Reports

- Josep Pegueroles, Juan José Alins. Servidores web seguros en Linux.. Report Interno. Julio 2000
- Josep Pegueroles, Francisco Rico, Luis J. de la Cruz. Introducción a los esquemas de pagos electrónicos. Report Interno. Julio 2000.