An end-to-end QoS and security joint management for IPTV service delivery

Mohamed Aymen Chalouf, Ismail Djama, Toufik Ahmed, Francine Krief

An End-to-End QoS and Security joint Management for IPTV Service Delivery

M. A. Chalouf, I. Djama, T. Ahmed and F. Krief

CNRS-LaBRI Lab, University of Bordeaux
351 Cours de la Libération, F-33405 – Talence - France
Tel: +33 5 40 00 35 01
Fax: +33 5 40 00 38 95
{chalouf, djama, tad, krief}@labri.fr

Abstract—**Today, the IPTV technology is emerging as a new concept for delivering and accessing audiovisual services over IP networks. The IPTV services promise to change radically the way we consume the video content by introducing content interactivity and adaptation. To allow the transmission of IPTV services on wired and wireless networks, different issues should be overcome regarding scalability, QoS provisioning, security guaranty, and terminals heterogeneity. In the majority of today deployed IPTV architectures, security and QoS mechanisms are managed separately. Although, these two aspects are tightly coupled since they influence the performance of each other. Thus, QoS and security constitute two needs that have to be carefully and tightly managed and not tackled separately. In this context, we have proposed a complete end-to-end architecture for providing IPTV services. This architecture enables managing end-to-end QoS and security, while addressing other issues such as the terminal heterogeneity.**

Thus, in this paper, we describe the proposed IPTV architecture which is composed of two segments: the core network and the access network. Then, we detail the different mechanisms which allow us to manage simultaneously the QoS and the security for the IPTV streams delivered to heterogeneous mobile terminals. Performances evaluation demonstrates the importance of the joint management of security and QoS.

Index Terms— **IPTV, end-to-end QoS, end-to-end security, service level negotiation, MPEG-21 adaptation, cross-layer adaptation.**

I. INTRODUCTION

The increased resources in IP networks during the last years is allowing the emergence of several IP multimedia services such as audio/video streaming, television using IPTV, telephony using Voice over IP (VoIP), etc. The large deployments of these real-time services are very challenging since they require end-to-end Quality of Service (QoS), as well as security. In fact, security could be guaranteed between two communication end-points by employing security mechanisms and protocols. Whereas, QoS could be enabled locally, in each domain, by the use of a QoS model such as IntServ and DiffServ, and extended to the end-to-end level.

On the other hand, the 802.11 technology [1] is considered actually as a serious alternative to the wired Ethernet network in the last mile connection. Several advantages offered by this technology (rapid deployment, cost effectiveness, mobile connection, etc.) have allowed to monopolize the network market in few years. This monopolization is consolidated by the augmentation of bandwidth in the recent standards 802.11g [2], 802.11n [3] and the multiplication of access terminals equipped with 802.11 interfaces (webcam, hard drives, and audio handset).

In the majority of today deployed architecture, security and QoS mechanisms are not managed together but are rather separately implemented and managed. Although, both mechanisms are tightly coupled since they influence the performance of each other. Enabling security has a great impact on the QoS. This impact can be expressed in terms of overheads, as follows:

- *Processor activity*: security mechanisms and features require significant processing power that may alter the performance of the streaming server and/or the player.
- *Memory usage*: security requires maintaining an important context for storing and retrieving security information.
- *Network traffic*: enabling security leads to an increase in network traffic that should be taken into consideration when QoS mechanisms are negotiated between the communication end-points.
- *Delay and latency*: it is the most obvious performance degradation, and its effect on QoS is related to an increase in delay and latency when security is enabled. This impact (delay) has to be taken into consideration for QoS negotiation.

For some cases, it is very difficult to find common tradeoffs between security mechanisms and QoS performances for delay sensitive applications such as IPTV and video streaming. Research activity on this domain considers the security orthogonal to QoS since both of them are separately managed.

Thus, in this paper, we define an end-to-end IPTV architecture that demonstrates the tight management of end-to-end QoS and security. In our proposed architecture, the transmission path for IPTV streams is divided in two management segments: the core network and the wireless access network. To ensure tight management of end-to-end QoS and security for different IPTV stream to mobile users, we consider the service offering for both segments. For the first segment, a service level should be established for IPTV service transport over the core network having both security and QoS constraints. This service should be negotiated through the different implied domains. The QoS and security for the access segment (wireless access network) is ensured according to the user and terminal profiles and capability [4]. In fact, the heterogeneity of user terminal in the wireless access network in terms of hardware and software system capabilities requires service adaptation to ensure QoS and security continuity while maintaining an acceptable level of user perceived quality.

The reminder of this paper is organized as follow: section 2 describes some related works on service level guarantee at the core network as well as at the wireless access network. In section 3, we describe the proposed architecture of the IPTV streaming. Section 4 gives more details on the tight management of QoS and security for the core network. Section 5 details the use of user and terminal profiles to ensure IPTV service adaptation over the wireless access network. The last section concludes the paper and highlights some perspectives of this work.

II. RELATED WORKS

Multimedia service delivery (e.g. IPTV) for mobile heterogeneous users and terminals requires guarantees in terms of end-to-end QoS and security. In this section, we review different mechanisms used to enable both QoS and security. First, we introduce the process of service level negotiation which is used mainly for IP core network, and then we describe recent mechanisms and concepts that emerged recently to allow the transmission of real-time multimedia services on wireless access networks with QoS and security support.

Service offering in the core network is defined through a Service Level Agreement (SLA) which is a contract between the Service Provider (SP) and the Service Consumer or client. The technical parameters of this SLA constitute the Service Level Specification (SLS) and covers different aspects among which QoS, security, and mobility. To guarantee an end-to-end service level, the managers of the different domains implied in a service offer must agree on these parameters. Thus, several protocols were proposed in order to allow dynamic service level negotiation such as QoS-NSLP (QoS NSIS Signaling Layer Protocol) [5], COPS-SLS (Common Open Policy Service) [6], QoS-GSLP (QoS Generic Signaling Layer Protocol) [7] and DSNP (Dynamic Service Negotiation Protocol) [8]. Unlike these protocols which ensure only QoS negotiation, we have proposed recently the SLNP (Service Level Negotiation Protocol) protocol that allows associating both QoS and security parameters in the negotiated service level [9].

During multimedia service delivery, the stream may cross several domains where QoS is locally guaranteed using QoS models. To ensure end-to-end QoS and security, SLNP is used to enable communication end-points to select QoS and security mechanisms and algorithms.

In the core network, the multimedia streams can be secured at different levels: application, transport or network. The application can provide security services by implementing their own security mechanisms. At the transport level, Secure Real-time Transport Protocol (SRTP) [10] and/or Datagram Transport Layer Security (DTLS) [11] can be used. At the network level IP Security (IPSec) [12] is suitable for securing IP communications by authenticating and encrypting each IP packet of a data stream.

In the context of services and networks convergence to the IP technology, the 802.11 access networks have to overcome many challenges to allow a reliable, secure and universal access to IP services.

The reliability is mainly related to QoS which remains an issue in the wireless network, especially for the IP multimedia services. In fact, the intrinsic characteristics of radio wave propagation (reflection, attenuation, interferences, etc.) lead to signal fading that can be fast or slow [13]. The signal fading affects the performance of wireless transmission in terms of bandwidth, loss, delay and jitter. If the QoS in core network was widely investigated by the research community during the last years, the QoS in the access network is still a challenge. The QoS in this last segment should be maintained not only at the IP layer but over all network layers. During the last years, many QoS mechanisms have been defined over all the network layers.

At the Physical layer, different techniques are exploited to enhance the rate and to minimize the signal fading. The adaptive modulation [14] is one of theses techniques, which tries to find a trade-off between the physical rate and the transmission quality. Another technique to increase the transmission reliability is the channel diversity which consists to send many times the same information by using frequential, spatial, or temporal duplication [15].

The 802.11 MAC layer introduces also some mechanisms to minimize the unreliability of the physical layer such as the retransmission, the RTS/CTS messages, and the fragmentation. Moreover, the QoS mechanisms have been introduced in 802.11e standard published in 2005 [16]. The most important mechanism in this new standard is the Access Categories (AC) provided by EDCA (Enhanced Distributed Channel Access). In fact, the EDCA defines 4 categories for background, best effort, video, and voice class of traffic. Each category has its own access priority and channel occupation.

At the Network layer, there are mainly three QoS architectures defined by the IETF: (1) Integrated Service (IntServ) which performs the resource allocation for the network streams (2) Differentiated Service (DiffServ) which defines a classes of service at IP layer with different QoS characteristics (3) and the MPLS architecture that allows a better network management.

At the transport layer, a new congestion control algorithms more adapted for multimedia streams have been proposed. Moreover, to satisfy the characteristics of real-time stream, two new transport protocols have been defined: DCCP (Datagram Congestion Control Protocol) and SCTP (Stream Control Transmission Protocol).

Finally, the application layer has covered all the techniques that allow the multimedia application to face: the bandwidth variations (transcoding, scalable video coding, etc.), the packets losses (error resilience video coding, Interleaving, Forward error correction, Automatic Repeat reQuest), and the delay variations (jitter) by using a reception buffer.

However, to assure QoS continuity, an optimal mapping between application QoS, IP QoS and the link level QoS is needed. The inter-layer communications become crucial. For this purpose, the cross-layer paradigm has emerged recently to surpass the layer isolation and to allow the higher layer to face the wireless channel variation. The ultimate goal of cross-layer is to increase the communications between adjacent and non-adjacent layers in order to enhance the transmission performance [17] [18].

Security issue is another aspect that should be met in the wireless access network. Always in the optic of cross-layer paradigm, the security can be enabled at different levels of the TCP/IP stack. In fact, the application could have its own security mechanisms such WSS (Web Service Secure) [19] for Web Services applications, or can use some existing one. The IPSec

protocol [12] provides security services at the network layer using two mechanisms: Authentication Header (AH) [20] and Encapsulating Security Payload (ESP) [21]. Another example is the TLS (Transport Layer Security) protocol [22] that operates at the transport layer in order to secure TCP based applications, and its adaptation for the UDP based ones: DTLS [11]. At the transport layer, we have also SRTP which enables securing RTP based applications such as IPTV streaming. On the other hand, the communication can be transparently secured at the data link layer using one of the Wi-Fi security mechanisms such as WEP (Wired Equivalent Privacy), WPA (Wifi Protected Access) or WPA2 (802.11i).

Thus, the level of the transmission security should be determined taking into consideration the different security characteristics of the other levels as well as the impact of the security on QoS.

Table 1 illustrates some of the wide-used security protocols that can be applied to real-time traffic such as IPTV. Each security protocol has a particular impact on the QoS of transmitted traffic.

Security protocol	Authentication – Integrity	Confidentiality	Anti-replay
IPSec-AH **(Network level)**	HMAC-SHA1-96, AES-XCBC-MAC-96, HMAC-MD5-96, etc.		Sequence number (Optional)
IPSec-ESP **(Network level)**	HMAC-SHA1-96, AES-XCBC-MAC-96, HMAC-MD5-96, etc.	3DES-CBC, AES-CBC, DES-CBC, etc.	Sequence number (Optional)
DTLS **(Transport level)**	MD5, SHA1	AES, DES, 3DES, RC4-40, RC4-128, IDES, Fortezza, etc.	Sequence number (Auto)
SRTP **(Application / Transport level)**	HMAC-SHA1	AES-CM, AES-f8M	Sequence number (Auto)

Table.1. Security services and used algorithms

The last issue that has to be overcome is the heterogeneity of access terminals in order to provide a universal access for IP services, especially for multimedia services. This issue has introduced a new concept called UMA (Universal Multimedia Access) that aims to provide a universal accessibility for multimedia content any where, any time and using any access terminal. The service adaptation represents the key solution to concretize this concept and to customize the multimedia content according to different parameters (terminal, user and access network). To fulfil the adaptation need, the MPEG-21 standards [23] which aims to define a common framework for multimedia delivery and consumption, dedicates the part-7 [4], called DIA (Digital Item Adaptation), to normalize the adaptation operations. It is important to notice that DIA doesn't define the adaptations techniques, but it defines tools that help to perform adaptation. These tools are defined using XML schemas [24] that allow generating XML descriptions for different entities. The UED (Usage Environment Description) is the most important tool in DIA. It describes the user environment which is very important to perform the adaptation. This environment includes: user characteristics, terminal capabilities, networks characteristics and natural environment characteristics.

In the next section, we present IPTV architecture that takes into consideration all technological aspects presented in this section.

III. PROPOSED ARCHITECTURE

The IPTV services are still an open issue in normalisation bodies: ITU-T with IPTV FG (Focus Group) and ETSI with its recent drafts DVB-IPI. In 2006, the IPTV FG group has proposed a definition for IPTV as multimedia services including television/video/audio/text/graphics/data delivered over managed IP networks to provide the required level of QoS/QoE (Quality of Experience), security, interactivity and reliability [25].

From this definition, we propose in this paper an end-to-end architecture to transmit IPTV for heterogeneous and mobile users connected over 802.11 wireless access networks. The proposed architecture provides a management plane that assures an end-to-

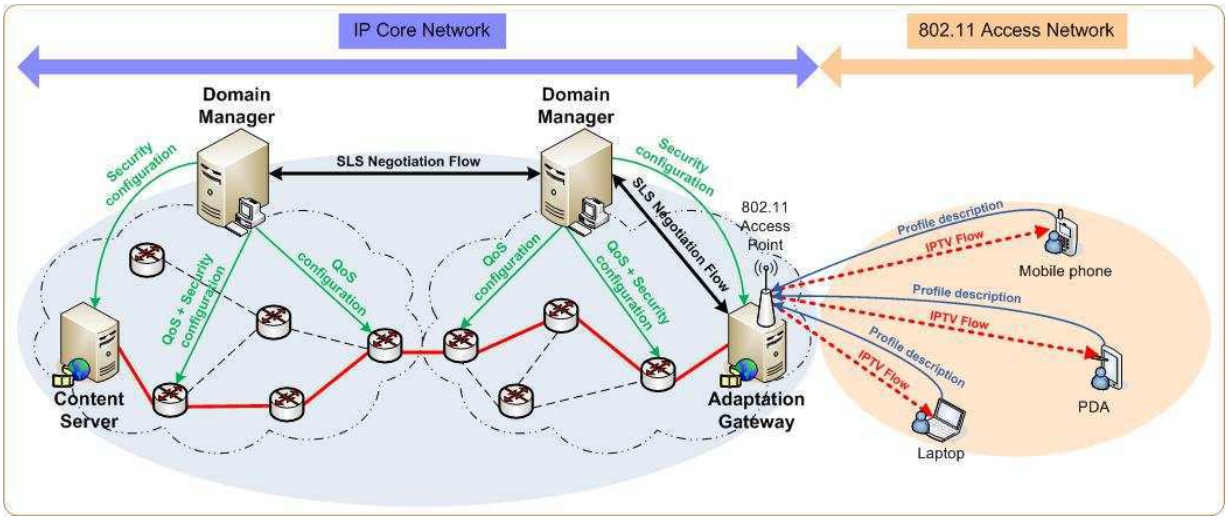

Figure.1. Global architecture of IPTV streaming platform

end QoS and security for the IPTV streams. Figure.1 illustrates the proposed overall architecture which is divided in two segments: the core network and the access network. This separation is motivated by the need to manage efficiently each segment independently since each one has its own characteristics and capabilities.

The core network is a high speed wired IP network composed of many independent domains. Each domain is managed by one entity called DM (Domain Manager). The DM communicates actively with its network entities in order to ensure the QoS and the security in its domain. Moreover, the DM supports an inter-domain service negotiation to assure an end-to-end service level. The core network includes two main entities: the CS (Content Server or TV Head-end) and the AG (Adaptation gateway). The CS is in charge of providing IPTV from digital TV broadcast network to IP network. This latter can be DVB-T for terrestrial network, DVB-S for satellite network or DVB-C for cable network. To avoid the duplication of TV streams in the core network, the CS transmits the IPTV streams using multicast. Each IPTV stream is sent in independent multicast group.

The multicast IPTV streams are received by the AG deployed at the boundary of the wireless access network.

The main functionality of the AG is to adapt the IPTV multicast service to LoD (Live on Demand) service. Thus, a particular end user should request the AG to get a specific IPTV stream that is transmitted in unicast. This would allow customizing QoS and security of the IPTV stream according to the client environment and to avoid useless transmission in wireless network when there is no receiver for IPTV service.

The AG functionalities are decomposed in three phases: negotiation, initialisation, and operational phases.

During the initialisation phase, QoS is negotiated from the AG point to the CS head-end. The QoS negotiation is based on a cascade model in which the local DM of the AG initiates the negotiation process with other DM, by taking into consideration both QoS and security requirements.

Once the negotiated parameters regarding QoS and security are determined (i.e. video traffic mapping into QoS classes and security level), the initialisation phase starts by allowing the AG to retrieve the IPTV multicast streams from the CS head-end. During this phase, the AG is ready to receive user request for IPTV streams. The operational phase starts when the first request arrives to the AG. During this phase, the AG performs two adaptations: before transmitting the IPTV stream and during the transmission. Before the transmission, the IPTV stream is adapted according to the client profile which is transmitted to the AG within the request. The adaptation performed by AG covers both the QoS and security. For instance, to maintain the IPTV QoS for a client connected with phone, the video resolution should be decreased, and security mechanism should not introduce extra overhead that can not be supported by the capability of the terminal. Moreover, if the phone doesn't support the security protocol

at IP level (IPSec), the AG should assure the security for the IPTV stream using others protocols present at others layers (SRTP or DTLS at transport layer, security at application level). During the transmission, the AG performs cross-layer adaptations to preserve the IPTV QoS. Indeed, the network QoS parameters can change during the transmission especially for a wireless network. Therefore, the AG should adapt the IPTV stream according to the network variations by allowing cross-layer communications. For instance, if the available bandwidth in the wireless network decreases at the link layer, the AG should reduce the rate of the IPTV stream using transrating at the application layer.

In the next section, we detail the functioning of the proposed architecture for each segment. In the core network, we present the service level negotiation cross-domains that enables the horizontal tight management of QoS and security. At the access wireless network, we describe protocols and profiles used by the AG to customize the IPTV service according to the terminal capabilities.

IV. Service Level Negotiation In The Core Network

In the core network, the IPTV streaming service needs some guarantees in terms of end-to-end QoS and security. These guarantees would be provided using the service level negotiation which is ensured by a negotiation protocol. In our IPTV architecture, we defined the SLNP (Service Level Negotiation Protocol) protocol which enables the tight management of QoS and security. SLNP allows the simultaneous negotiation of QoS and security while taking into account the problems arising from this association, i.e. security overheads.

A. SLNP Definition

The SLNP protocol was proposed first in [26] in order to enable end-to-end QoS negotiation in a self-aware management environment. Then, security aspects were introduced in the service level negotiation in [9]. In this paper we define how SLNP is used in IPTV service delivery. In fact, using SLNP, a client is able to negotiate a service level with the different domain managers (at least one) implied in the communication chain. The SLNP protocol employs Web Services technology in order to provide interoperability between the different negotiation actors/parts. To satisfy the negotiation requirements, six types of messages are used in the SLNP negotiation process:

- NEGOTIATE message enables requesting the establishment of a service level,
- REVISION message proposes an alternative to the requested service level,
- RESPONSE message allows to accept or reject a request or an offer,
- MODIFY message is used to request changing an already established service level,
- NOTIFY message is used to inform about changes in resources availability or the non respect of a service level,
- RELEASE message allows ending a service level already established.

These messages contain an SLS element which characterizes the negotiated service level. Since SLNP uses Web Services, the structures of the SLS element as well as those of the different messages are described using XML Schema. In the following section, we describe the structure of SLS element by detailing the different contained parameters.

B. SLS Structure

The SLS element transported in SLNP messages refers to the negotiated service level for various communications (e.g. ToIP, VoD, IPTV, etc.) and conforms to the defined XML schema shown in Figure.2.

These parameters can be classified in three types: QoS parameters, security parameters and the parameters that are common to QoS and security. The parameters which are common to security and QoS include: SLS Identifier, Traffic Identification, Negotiation Parameters (Mode, Renegotiation Interval) and Reliability (Mean Down Time, Mean Time To Repair). Then, QoS Parameters contain Scope, Service Schedule, Performance Guarantee (Bandwidth, Jitter, Delay, Loss Rate), Description and Traffic Conformance (Token Bucket, etc.), and finally Excess Treatment. The 'Performance Guarantee' element could be considered as the most important QoS parameter because it actually describes the end-to-end QoS that will be guaranteed by the SLS established after a SLNP negotiation. The QoS level described by this element is independent of the QoS models (DiffServ, IntServ, 802.11e, etc.). End-to-end QoS guarantee is deducted from different local offers proposed by each domain managers participating in the negotiation. Indeed, each QoS attribute is made of a requested part indicating the global value to be guaranteed and an offered part updated by different negotiation participants according to their local offer. For example, the *delayRequested* part of the delay attribute represents the end-to-end delay requested by the client, while the *delayOffred* part corresponds to the sum of the different transit delays ensured by the different domains. The QoS Parameters element is mandatory because the negotiation must at least concerns the QoS. If the service level also includes security, then security impact on QoS must be estimated and considered in the negotiation.

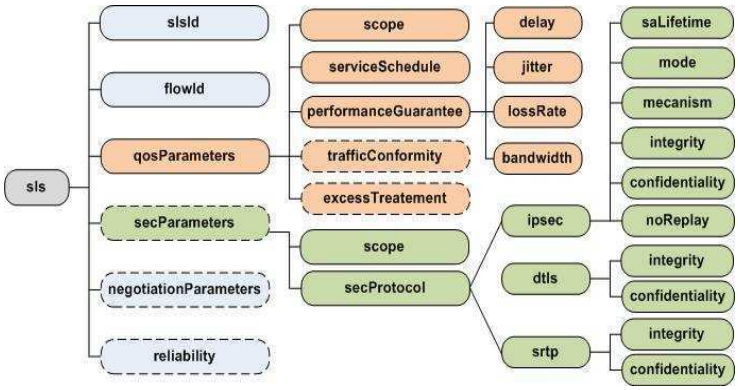

Figure.2. XML Schema for the negotiated SLS

In order to control the security impact on QoS, we propose to tightly manage QoS and security in order to take into account security overheads in the QoS offer. Thus, the SLS negotiated with SLNP contains a Security Parameters element which is composed of: Scope and Security Protocol. We note that this scope can be different from the one specified in QoS parameters. In fact, in a QoS context, the scope made of ingress and egress indicates the two communication end-points (e.g. content server and adaptation gateway). Whereas from a security point of view, they can constitute the peers of an IPsec security association (e.g. CS and AG or security gateways to which these entities are connected to). The second element enables selecting a security protocol (IPSec, TLS/DTLS, SRTP, etc.) for which a set of parameters are negotiated.

C. SLNP PROCESSING

The SLNP protocol could be used for service level negotiation across one or more domains constituting the core network. This negotiation aims to establish an SLS which enables ensuring end-to-end QoS and security for an entire multicast group. In this section, we describe the negotiation process through the example given in Figure.3. In this example, the SLS negotiation involves the managers of the different domains (DM1, DM2 and DM3), the content server (CS), and the various adaptation gateways (AG1, AG2 and AG3).

We note that QoS and security levels depend only on the provided IPTV service. Thus, each AG which wants to join a multicast group should contact the CS to know the parameters of the SLS to negotiate with the different domains involved in the transport of the requested IPTV service. In the provided example (Figure.3), the SLS corresponding to the IPTV service, transported from the CS to the different AGs, is defined through the SLS summarized in Table 2.

QoS level	Security level
Delay = 1000 ms Jitter = 500 ms Loss rate = 5 % Bandwidth = 2500 Kbit/s	Confidentiality = Yes - High Integrity = Yes – High Anti-replay = Yes

Table.2. QoS and Security levels for the considered IPTV service

The SLS negotiation in the core network is performed as shown in Figure.4. First, the AG1 contacts the CS to know the SLS parameters that should characterize the delivered IPTV service. Then, it can initiate the negotiation by sending a Negotiate message to the manager of its domain (DM1). To treat this request (Negotiate), the DM1 must interact with its RMF (Resource Management Function) to obtain information on the QoS (delay, bandwidth, etc.), that can be locally offered to the IPTV streams, as well as the characteristics (supported algorithms and protocols, performances, etc.) of entities that have to perform security treatments. If the SLS requested by the AG1 can not be satisfied in the first domain (D1), then a negative response (Response-Nack) is returned to the AG1. Otherwise, a positive response is returned to this AG1. This involves the creation of a multicast group (MG) and the recording of the corresponding SLS in the SR (SLS Registries) of DM1. Finally security and QoS guarantees can be enabled by configuring the concerned entities.

Now, if the AG2 wants to join the MG, it must also interact with the CS to know the characteristics of the SLS to negotiate. Then, the negotiation is initiated by sending a request (Negotiate) to the manager of its domain (DM2). After asking the RMF, the DM2 may reject the request or forward it to DM1 after updating it according to its local offer (QoS and security). Indeed, the request of the AG2 may be rejected if, for example, the required bandwidth or the needed security services for the IPTV service

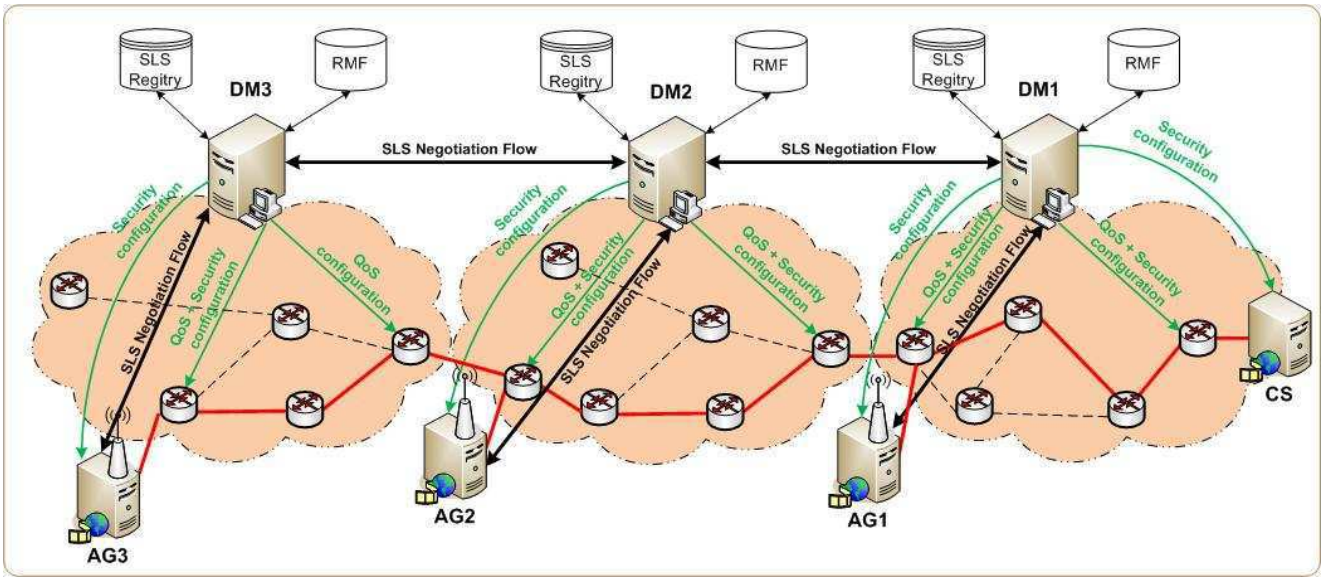

Figure.3. Example of the SLS negotiation for a multicast group

can not be ensured over the second domain D2. Otherwise, the request of the AG2 (Negotiate) is forwarded to DM1. This last can decide to allow or not AG2 to join MG. In fact, DM1 knows the service offer characterizing the IPTV service delivery between the CS and the boundaries of the first domain, as well as the offer proposed on the second domain.

If we consider, for example, the delay parameter, then the negotiation entity DM2 has to calculate the sum of transmission delay on D1 and D2 and that resulting from security operations. After that, if the total delay is greater than the delay characterizing the IPTV service (1000 ms), then DM1 may refuse the request of AG2. When the end-to-end service offer (from CS to AG2) meets the requirements of the IPTV service, the AG2 request is accepted and a positive response (Response-Ack) is returned to AG2 via DM2, which must, therefore, record the SLS on which it is engaged. Thus, the AG2 is added to the multicast group and the SLS already registered at the DM1 must be updated to introduce AG2 among the AGs receiving the IPTV stream. Finally, QoS and security can be configured at the second domain.

When the AG3 (belonging to the third domain) have to join the MG in order to receive the IPTV service, the negotiation will be performed in the same manner as described above. However, the decision is taken, this time, at DM3 or DM2. When the negotiation succeeds, the SLS corresponding to the MG must be registered in the SR of DM3, and updated in those of DM1 and DM2.

When an AG wants to quit the multicast group, it must send a Release request which will be treated by the manager of its domain. In fact, if this domain is involved in the transport of the IPTV service for only this AG, then the corresponding SLS is deleted from the SR of this domain and the reserved resources in this domain can be released. We note that the other DMs implied in the IPTV multicast must be informed of this quit in order to update their records on the SLS of the MG.

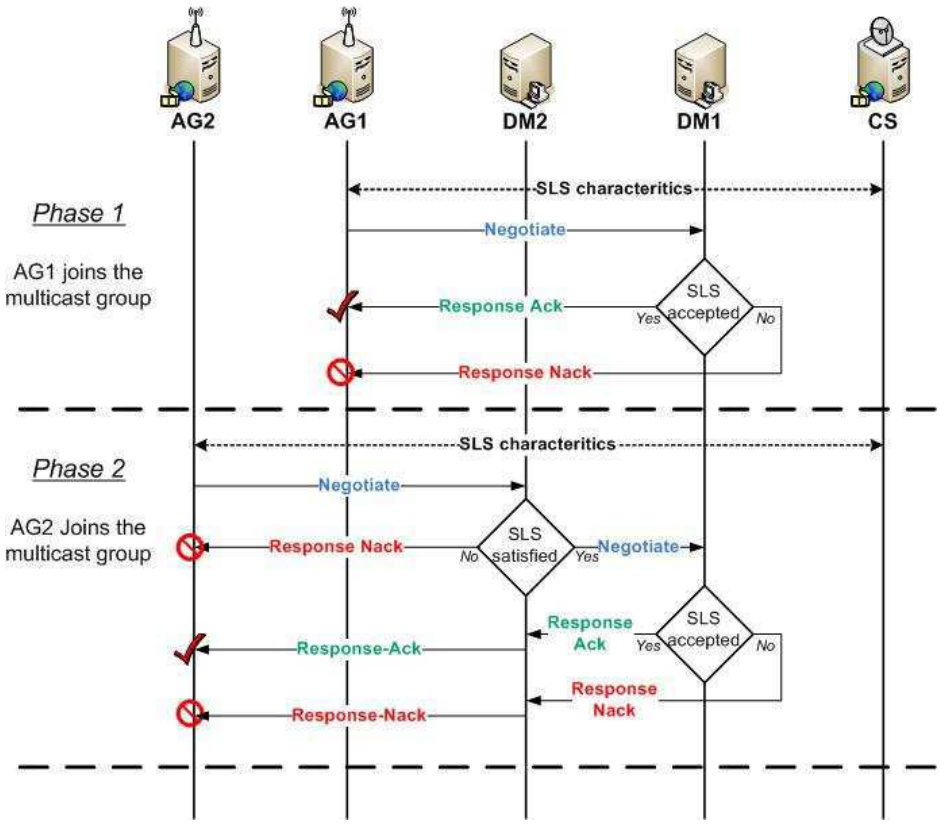

Figure.4. Message Sequence Chart of the SLS negotiation in the core network

From this example, we can see the importance of the use of the SLNP protocol in the core network. SLNP enables ensuring an end-to-end service level covering simultaneously QoS and security for the different AGs belonging to a multicast group. In fact, the sum of the QoS local offers of the different domains involved in the transport of the IPTV service must meet the QoS required by this service. As for security, each domain carrying the IPTV service must provide security services that satisfy the needs of the IPTV service. We note that the layer on which security can be implemented may vary from one domain to another (IPSec, DTLS or SRTP), but the provided security must satisfy the required level; i.e. security services (confidentiality, integrity, non-replay, etc.) and the level of each service (high, mean or low).

Therefore, security impact on QoS parameters such as delay resulting from cryptographic operations at communication ends and extra bandwidth needed for the added headers will be estimated and taken into account when negotiating QoS. To demonstrate the security impact on QoS parameters, we have evaluated the delay and jitter for a UDP transmission using 4 security policies resumed in Table 3. The experimentations were conducted on reel testbed using two systems having the same characteristics (IBM systems, Pentium IV, 2.4 GHZ).

Policy	Characteristics
P1	No security
P2	IPSec, AH, Integrity=HMAC-SHA1-96
P3	IPSec, ESP, Integrity=HMAC-SHA1-96, Confidentiality=AES-CBC.
P4	DTLS, Integrity=SHA1, Confidentiality=AES

Table.3. Security policies used in impact evaluation

The experimental conditions were extremely controlled since the two systems have performed only the application that ensures the transmission and the reception of UDP stream. In addition, the wired network connecting the two systems was over-provisioned (the bandwidth in the network is greater than the UDP throughput) and there is no other streams in the network.

Figure.5 illustrates the security services impact on delay and jitter measurements. We notice clearly that security services (integrity and/or confidentiality), provided through the use of IPSec and DTLS, increase the delay of UDP transmission as well as jitter. For example, we note that the delay introduced by security processing varies between 27% and 45% of the transmission total time. This also depends on used security mechanisms: IPSec-AH, IPSec-ESP or DTLS.

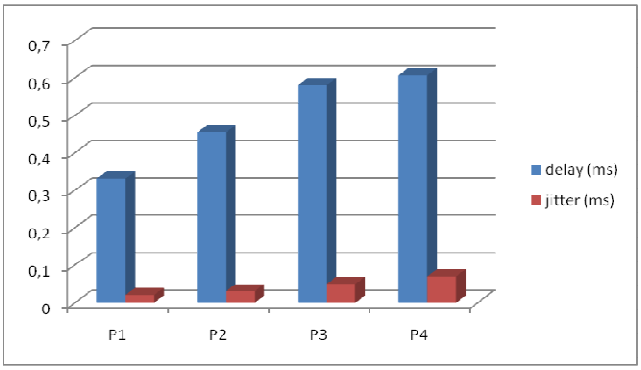

Figure.5. Security impact on QoS parameters (delay and jitter for an UDP traffic

D. SERVICE CUSTOMIZATION IN THE ACCESS NETWORK

As mentioned before, the AG is deployed at the beginning of wireless access network. It transforms the multicast IPTV service on LoD service for heterogeneous mobile clients.

To reach this objective, the AG, shown in Figure.6, includes a new audio/video transmission system based on cross-layer interactions, called XLAVS (Cross Layer Adaptive Video Streaming). This new system interacts with all the network layers (application, transport, network and access link) of the AG as well as the receiving terminal to determine the optimal configuration which improves the transmission performance. The optimal configuration includes audio/video customization at the application level and the QoS setting and mapping over all the layers.

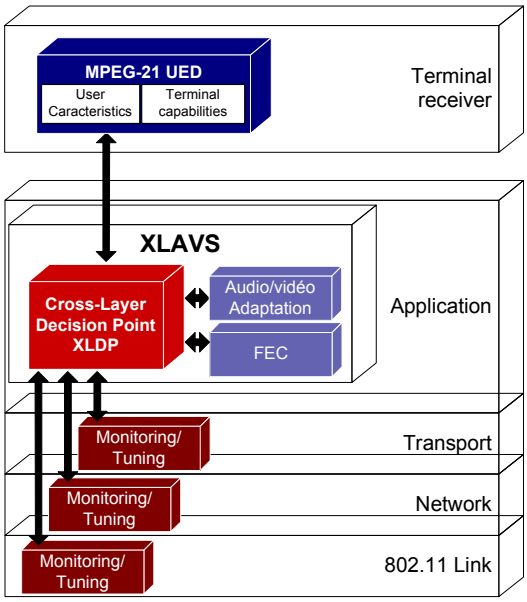

Figure.6. AG Architecture

The XLAVS (Cross-layer Adaptive Video streaming) is based on cross-layer integrated approach that permits a top-down and a bottom-up communications between network layers. This allows, firstly, to translate the QoS requirements of the transmitted stream into network metrics at network and link layer, and secondly, to reflect, at the application level, the dynamic changes of the underlying network.

The added value of our system XLAVS is the centralization in one module, called XLDP (Cross Layer Decision Point), all the information concerning the AG state and all the decisions concerning the adaptations. Figure.6 schematizes this centralization that aims to coordinate all the actions of the system (configurations and adjustments) in order to optimize the transmission of IPTV streams in the network managed by the AG. The XLAVS incorporates two other major modules to ensure the IPTV QoS: The adapter module which allows a real-time transcode for audio/video streams and The FEC (Forward Error Correction) module to add redundancy at the application level to enable the receiver to reconstruct lost packets.

In what follows, we will detail only the adaptation performed before the stream transmission. Indeed, when a client requests a stream, this last is adapted according to the client profile. The performed adaptation is based on the MPEG-21 DIA tools, mainly on Usage Environment Description (UED). The UED description covers all characteristics of the client. In our framework, we focus on user preferences, terminal capabilities and network characteristics. However, all these above-mentioned parameters described by UED are only related to QoS and the security parameters are not considered. The security parameters are important since the AG should know the security technology supported by the client environment according to terminal capability. To overcome this issue, we enhance the UED with security parameters. Figure.7 illustrates the XML schema of an UED with main elements. The QoS parameters are presented with red color and security parameters with green.

The terminal capabilities includes 4 parts: the audio/video decoding capabilities for terminal (codec, bitrate, frame rate), the display capability (display resolution), the audio output capabilities (sampling frequency, number of channels) and finally the security capabilities which enumerate the different security protocols supported by terminal (IPsec, DTLS, etc.) and algorithms which can be used for provided security services by each protocol (Integrity and confidentiality).

The network characteristics include the network capability and network condition. The network capability describes static attributes of network such as maximum rate, average loss ratio. It defines also the security protocols supported by network at link layer such as WEP, WPA or WPA2, since in our architecture we focus on 802.11 wireless networks. Regarding the network condition, the parameters describe the dynamic behaviour of network, for instance, the rate variation, the instantaneous loss ratio, delay and jitter.

The UED should be transmitted to the AG from client when this latter requests a specific IPTV stream. In our architecture, we use RTSP (Real Time Streaming Protocol) [28] which is defined specially to control video streaming session. However, RTSP protocol doesn't provide means for clients to send their profiles i.e. the UED description. In fact, in RTSP architecture, the server provides a static video content described with SDP (Session Description Protocol). The client receives the SDP and if it doesn't support the configuration proposed by the server, the request fails.

In our architecture, we propose to modify the RTSP architecture to allow the UED transmission. The modification is illustrated in Figure.8 that details the RTSP requests/responses exchanged between the client and the AG.

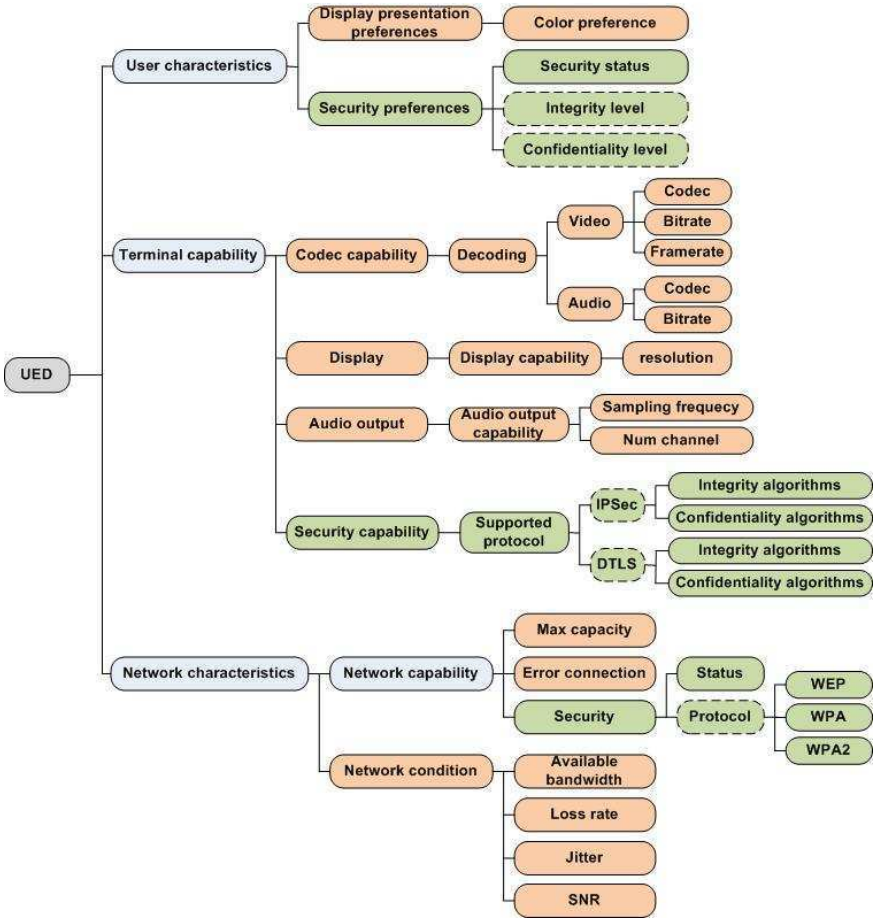

Figure.7. XML Schema for the UED

The UED document is transmitted in the DESCRIBE request body from the client to the AG. First, the AG specifies QoS and security parameters for the session. Then, it generates a new SDP according to the new parameters and transmits the new SDP in the response body of DESCRIBE request. At this point, the security is not configured because the session is not yet created (Figure.8).

Thus, to avoid the useless security configuration in the case where the session is not created, the security parameters are configured after the SETUP request/response. Finally, the client can transmit the PLAY request to receive an adapted and secured IPTV stream.

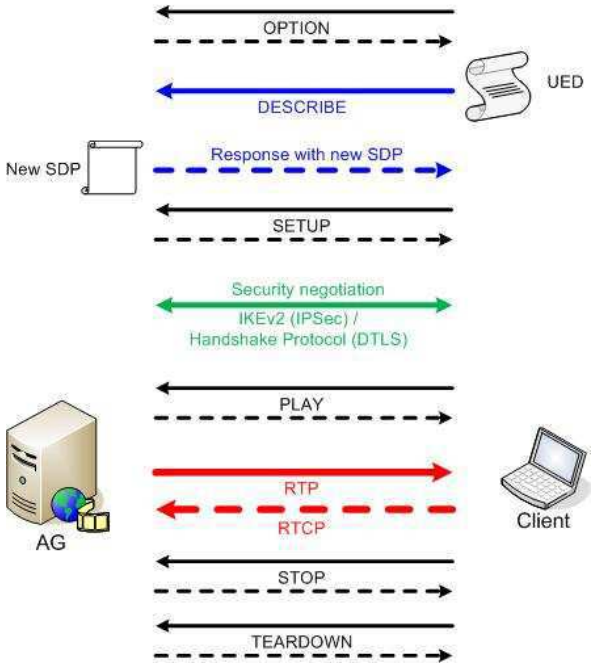

Figure.8. RTSP exchanged messages

V. CONCLUSION

In this paper, we have presented a new IPTV delivery platform that provides mobile users with customized IPTV service via WLAN 802.11 access network. In particular, we have presented mechanisms used by the IPTV architecture to provide the tight management of QoS and security for IPTV services over two different segments of the IPTV transmission path. In fact, we described how the SLNP protocol enables the service level negotiation for end-to-end QoS and security guarantees across heterogeneous domains composing the core network. Then, we detailed the use of the MPEG-21 part-7 standard to guarantee tight management of QoS and security to mobile user for the IPTV delivery. The described results illustrate that security and QoS are mutually related to each other and cannot be implemented orthogonally.

The implementation of the mechanisms allowing the tight management of QoS and security on our IPTV platform is nearly finished. Then, the next objective is to evaluate the real performances of the management process; especially the time needed for the establishment of an end-to-end service level.

Since a domain manager could be implied in several negotiation processes in the same time, we will evaluate the scalability of the SLNP negotiation performed in the core network. It is also planned to study the scalability of the adaptation achieved at an adaptation gateway which have to adapt IPTV streams for a set of heterogeneous terminals.

REFERENCES

[1] IEEE 802.11, IEEE Standards for Information Technology-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Edition (ISO/IEC 8802-11: 1999), 1999.

[2] IEEE 802.11g, IEEE Standard for Information technology-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications-Amendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band, 2003.

[3] IEEE P802.11n-D3.00, Approved Draft Standard for Information Technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 4: Enhancements for Higher Throughput, 2007.

[4] ISO/IEC 21000-7:2007, Information technology-Multimedia framework (MPEG-21)-Part 7: Digital Item Adaptation, 2007

[5] S. V. Den Bosch, G. Karagiannis and A. McDonald, "NSLP for Quality of Service Signaling", IETF Internet draft, draft-ietf-nsis-qos-nslp-06.txt, February 2005.

[6] T. M. T. Nguyen and al., "COPS-SLS: A Service Level Negotiation Protocol for the Internet", IEEE Communication Magazine, May 2002, pp. 158-165.

[7] Ambient Networks Consortium, "Connecting Ambient Networks-Architecture and Protocol Design (Release 1)" Del. D 3.2, March 2005.

[8] J.C. Chen and al., "Dynamic Service Negotiation Protocol (DSNP) and Wireless Diffserv", Proc. ICC, New York, NY, April 2002, pp. 1033-1038.

[9] M. A. Chalouf, X. Delord and F. Krief, "Introduction of security in the service Level Negotiated with SLNP Protocol", Second IFIP International Conference on New Technologies, Mobility and Security NTMS", Tangier, Morocco, November 2008.

[10] M. Baugher, D. McGrew, M. Naslund, E. Carrara, K. Norrman, "RFC 3711: The Secure Real-time Transport Protocol (SRTP)", Request for Comments, IETF, March 2004.

[11] E. Rescola and N. Modadugu, "RFC 4347: Datagram Transport Layer Security (DTLS)", Request for Comments, IETF, April 2006.

[12] S. Kent and K. Seo, "RFC4301: Security Architecture for Internet Protocol (IPSec)," Request for Comments, IETF, December 2005.

[13] D. Tse and P. Viswanath, "Fundamentals of Wireless Communication", ISBN-13: 978-0521845274, Cambridge University Press, May 2005.

[14] I. Haratcherev, J. Taal, K. Langendoen, R. Lagendijk and H. Sips, "Automatic IEEE 802.11 rate control for streaming applications", Wireless Communications and Mobile Computing, Vol 5, pp.412-437, 2005.

[15] J. N. Laneman, et al., "Source-channel diversity approaches for multimedia communication", in IEEE Transactions on Information Theory, vol. 51, no. 10, pp. 3518-3539, October 2005.

[16] IEEE 802.11e, IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, 2005

[17] V. Srivastava and M. Motani, "Cross-layer design : a survey and the road ahead", IEEE Communications Magazine, vol.43, no.12, pp.112-119, December 2005.

[18] M. Van Der Schaar, et al., "Cross-layer wireless multimedia transmission : challenges, principles, and new paradigms", IEEE Wireless Communications Magazine, vol. 12, no. 4, pp. 50-58, August 2005.

[19] A. Nadalin and al., "Web Service Security," OASIS, http://docs.oasis-open.org/wss/v1.1/, 2006.

[20] S. Kent, "RFC 4302: IP Authentication Header (AH)", Request for Comments, IETF, December 2005.

[21] S. Kent, “RFC 4303: IP Encapsulating Security Payload (ESP)”, Request for Comments, IETF, December 2005.

[22] T. Dierks and E. Rescola, “RFC 4346: The Transport Layer Security Protocol (TLS) Version 1.1”, Request for Comments, IETF, April 2006.

[23] ISO/IEC TR 21000-1:2004, “Information technology-Multimedia framework (MPEG-21)-Part 1: Vision, Technologies and Strategy”, 2004.

[24] T. Bray and al., “eXtensible Markup Language (XML) 1.0 (Third Edition,” Recommendation W3C, February 2004.

[25] ITU-T FG IPTV-R-0014, 2nd FG IPTV meeting, Busan, Korea 16- 20 October 2006.

[26] N. Mbarek and F. Krief, “Service Level Negotiation in Autonomous Systems,” The International Conference on Autonomic and Autonomous Systems, USA: Silicon, pp. 35-41, July 2006.

[27] J. Schiller, “RFC 4305: Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload and Authentication Header,” Request for Comments, IETF, December 2005.

[28] H. Schulzrinne, A. Rao, R. Lanphier, “RFC 2326: Real Time Streaming Protocol (RTSP)”, Request for Comments, IETF, April 1998.