Journal of Theoretical and Applied Information Technology
20th April 2014. Vol. 62 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN APPROACH FOR DESIGN AND IMPLEMENTATION OF SECURE VIDEO STREAMING USING SRTP

[1]P. IYYANAR, [2]DR. M. CHITRA
[1]Research Scholar, Anna University, Chennai, India.
[1]Assistant Professor, Information Technology, Sona College of Technology, Salem, India.
[2]Professor, Information Technology, Sona College of Technology, Salem, India.
Email: [1]inr.info@gmail.com , [2]chitra_slm@yahoo.co.in

ABSTRACT

Video streaming is one of the most important and growing application in multimedia communication due to reduction of storage and increase in high speed network access for any environment. Real-time live video or stored video is the predominant part of the real-time multimedia networking. In the streaming technology, the video file need not be downloaded in full, but is being played out while the content of the video file are being received and decoded. This paper proposes secure video streaming using SRTP protocol. The video formats of the RTP transmission are .MPG, .AVI video container. The value of the prototype system is to provide an effective transmission across the Internet with quality-guaranteed manner while using RTP and RTCP protocol on un-trusted Client–Server networks.

Keyword- *Video Streaming, RTP, RTCP, SRTP*

1. INTRODUCTION

The video streaming [1] [2] [3] has been extensively used for information broadcasting. The availability of improved and enhanced transmission facilities like high speed LAN, wireless Ethernet, make it further possible to use video streaming in fast real time applications. Real time video streaming is useful in surveillance, conferencing, media broadcasting and applications that include remote assistance. In real time nature, video streaming has bandwidth, delay and loss of packet requirements. In video streaming, raw video and audio data are compressed by video compression and audio compression algorithms and saved in storage devices. If the client gives the request, a streaming server retrieves compressed audio and sends the video data from storage devices to that particular client. When starting to send the audio and video streams across the network, a transport protocol uses two packets the compressed byte of streams and send the audio- video packets to the Internet. For packets that are successfully delivered to the receiver, they first pass through the transport layers and then are processed by the application layer being decoded at the audio- video decoder. The system deals with the issues of real-time protocol implementation on live or stored video.

2. AN OVERVIEW OF VIDEO FORMATS

Video formats are classified into two distinct and different technologies such as containers or wrappers and codecs [4]. Codec video format will be confusing so that it will be used inside of a container. The container illustrates the structure of the file, where the various pieces are stored and how they are interleaved, and which codecs are used by which pieces. It may denote an audio codec as well as video.

It is used to package the video and its components (audio/metadata). The container is identified by a file extension such as .AVI, .MP4 or .MOV. Coder and decoder are called codec in the video formats. It is a technique of encoding audio or video into a stream of bytes.
Codec is the way used to encode the video and is the ruler determiner of quality. The codec is identified by a file extension such as MPEG, MPEG-2, MPEG-4, H.264, mp3, MJPEG, DV, WMV, RM, and DivX.

Table 1 List of Most Common Containers

Container	Description
AVI (Audio Video Interleave)	A Windows' standard multimedia container

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

. MP4 (MPEG-4 Part 14)	Is the standardized container for MPEG-4
FLV (Flash Video)	The format used to deliver MPEG video through Flash Player
. MOV (MPEG-4 Part 12)	Apple's QuickTime container format
MKV (Mastroska)	Open-specification container
VOB (DVD Video Object)	It's DVD's standard container
ASF (Advanced Streaming Format)	Microsoft's proprietary digital audio/digital video container format designed for WMV, WMA files can end in .Wm or .asf

Table 2 List of Most Common codec

Codec	Description
MPEG, MPEG-2, MPEG-4	Moving Pictures Expert Group video formats for video compression
H.264	Most commonly used codecs for videos uploaded to the web
MP3	Used for music and VideoCD
MJPEG (Motion JPEG)	A codec consisting of a stream of JPEG images
DV (Digital Video)	Used for video grabbed via firewire off a video camera
WMV (Windows Media Video)	A collection of Microsoft proprietary video codecs
RM (Real Media)	A closed codec developed by Real Networks for streaming video and audio.

3. RELATED WORKS OF VIDEO STREAMING

Video streaming is the process of playing the video file while it is completely received. Streaming technology is categorized into two methods [5] [6] [7]. One is progressive streaming and another one is called an adaptive streaming method. Progressive or download method is the process of transfer digital media files from web server rather than streaming server to a client by using HTTP protocol. Now-a-days most of the video file is delivered via progressive download seem, in which the end-user begins to play once, click the button and continue smoothly until the end. YouTube, ESPN and CNN websites are delivering without a streaming server via progressive download. True streaming is known as an adaptive streaming method, in which it uses a streaming protocol to control the transfer of video data. The rate of transfer can automatically change in response to the transfer conditions. The client is not able to keep up a higher data rate, then the server will drop to the lower data rate and quality. The client receives a high quality and high data-rate-stream when the connection is good. Adobe's Dynamic Streaming, Apple's HTTP Live Streaming and Microsoft's Smooth Streaming is the further streaming alternatives to an adaptive streaming. Video streaming is divided into video on-demand and real-time streaming. In video on-demand streaming, the receiver requests a recording or movie and receive it. In this streaming no one client will receive the same recording at the same time.
But the real-time streaming, the server determines what to send, the client plays it back as it's sent with slight, consistent delay.

In real-time streaming, the service is usually managing a known number of clients and it may be point-to-point (one sender-one receiver) or broadcast (one sender-many receivers).

3.1 Streaming Protocols

- The application layer HTTP protocol was used to stream the video in the beginning of the video streaming system.
- Adobe Flash is released a specification for Real Time Message Protocol (RTMP proprietary protocol). It is operated in the application through session layer, in which the data transmission is done by the TCP. RTMP is tunnelled through HTTP.
- HLS or HTTP Live Streaming Protocol has been developed by Apple for iOS and it is not used outside of Apple products. The HTTP is used to stream with adaptive bit rates. HTTP with TCP/IP is designed for reliable delivery.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- Microsoft Media Service (MMS) protocol is used to transfer real-time multimedia data. MMS uses a TCP connection to control the streaming media session and to send messages by both client and server. The server sends multimedia data over TCP/UDP.
- The best protocol for real-time transmission of video streaming system is RTSP (Real-time Streaming Protocol) [8] [9]. The protocol stacks of RTP, RTCP, RTSP is called "RTSP". An RTSP session may consist of multiple streams to be combined at the receiver end and audio and video may be on separate channels.

4. REAL TIME TRANSPORT PROTOCOL

Real-time Transport Protocol is the usual protocol for the transport of real-time data, including audio and video [10]. RTP is useful in media-on-demand and interactive services such as Internet telephony. RTP consists of a data and a control part. RTP has its companion RTP control Protocol (RTCP). The data part of RTP is a thin protocol given that support for applications with real-time properties such as continuous media (e.g., Audio and video), timing reconstruction, loss detection, security and content identification. RTCP provides support for real-time conferencing of groups of any size within an internet. This support includes: Source identification and support for gateways like audio and video bridges, Multicast-to-unicast translators and Quality-of-Service feedback from receivers to the multicast group and Support for the synchronization of different media streams.

RTP was implemented using the concept of Application Level Framing (ALF), first described by Clark and Tennenhouse. The ALF may be able to manage disordered or lost packets in any kind of applications such as ignoring the loss, re-sending the lost data and sending new data which take over from the lost data. The application has been working as per the above choice, if the transport protocol is dealing with data in Application Data Unit (ADUs). The data in the Application Data Unit can be processed out-of-order with respect to the other Application Data Unit. The real-time transport protocol has the property of ADUs, in which it contains the information to be processed by the receiver immediately. In video streaming system the compressed video data in an ADU must be capable of being decompressed regardless of whether previous ADUs have been received. The ADU must contain header information detailing its position in the video image and the frame from which it came. In a specific application, the information is not present in the generic RTP header and which will be specified in RTP Profiles and Payload formats. RTP describes a profile and one or more associated payload formats for specific applications like audio and video.

5. SECURE REAL TIME TRANSPORT PROTOCOL

The Secure Real-time Protocol [11] is a profile of the Real-time Transport Protocol (RTP) offering not only confident, but also message authentication, and replay protection for the RTP traffic as well as RTCP (Real-time Transport Control Protocol). SRTP offers a structure for encryption and message authentication of RTP and RTCP streams. SRTP can achieve high throughput and low packet expansion.

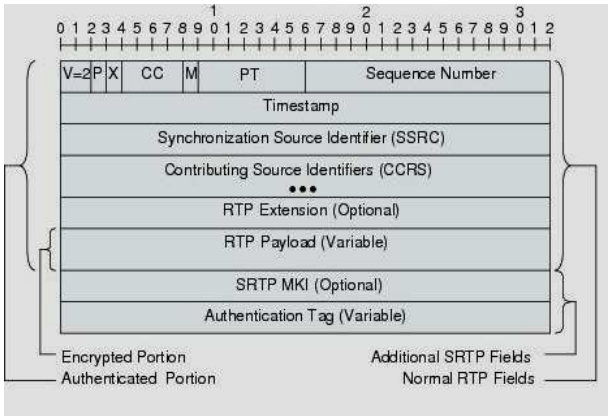

Figure 1. Secure RTP Packet Format

SRTP is independent of a specific RTP stack implementation and of a specific key management standard, but Multimedia Internet Keying (MIKEY) has been designed to work with SRTP. In comparison to the security options for RTP there are some advantages to using SRTP. The advantages over the RTP standard security and also over the H.264 security for media stream data are listed below.

SRTP provides increased security, achieved by

Journal of Theoretical and Applied Information Technology
20th April 2014. Vol. 62 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- Confidentiality for RTP as well as for RTCP by encryption of the respective payloads.
- Integrity for the entire RTP and RTCP packets, together with replay protection.
- The possibility to refresh the session keys periodically, which limits the amount of cipher text produced by a fixed key, variable for an adversary to cryptanalysis.
- An extensible framework that permits upgrading with new cryptographic algorithms.
- A secure session key derivation with a pseudo-random function at both ends.
- The usage of salting keys to protect against precipitation attacks. Security for unicast and multicast RTP applications

6. REAL TIME AUDIO/VIDEO STREAMING

The separate session has been used when the audio and video file is being transmitted through RTP [12], in which two separate UDP port pairs and/or multicast addresses are used in RTCP transmission Even though there is no direct coupling at the RTP level between audio and video sessions, but the session will be associated due to the user will use and participate both sessions with distinguished name in the RTCP packets. The separation of the audio and video, playback of a source's is synchronized using timing information accepted in the RTP packets for both sessions.

6.1 Mixer

RTP is used to transmit the video files where the clients in one are connected through a low-speed link instead of who enjoy high-speed network access. The mixer is the RTP-level relay, it may be placed near the low-bandwidth area for clients to use a lower-bandwidth and reduced quality video encoding. The mixer is used to resynchronize the incoming packets for constructing the constant 20ms spacing generated by the server. It mixes these reconstructed streams into a single stream. RTP translates the video encoding to lower-bandwidth one and forward the lower-bandwidth packet stream across the low-speed-link. The packet stream is received either single recipient in unicast or multiple recipients in multicast systems. The RTP header maintains the information about the mixers to identify the source that consists to a mixed packet.

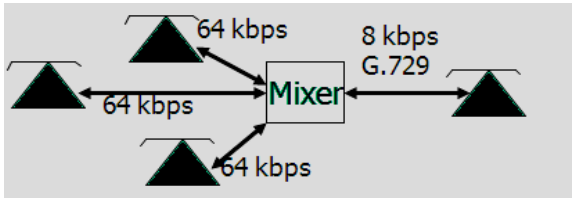

Figure 2. Mixer in RTP transmission

6.2 Translator in RTP

In the video streaming, some of the planned participants may be connected with high bandwidth links but might not be directly reachable via IP multicast; due to it may be in front an application-level firewall that will not allow any IP packets pass. In this situation, the mixer may not be required, in which case other types of RTP-level relay called a translator may be used. There are two translators are installed in both outside and inside of the firewall, the translators are responsible for tunnelling all multicast packets received through a secure connection inside the firewall and transmit them again as multicast packets to a multicast group. G. 729 and PCM are the digital video codecs.

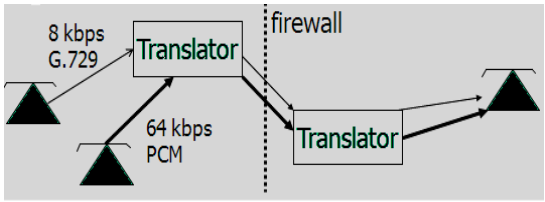

Figure 3. Translator in RTP transmission

7. DESIGN AND IMPLEMENTATION OF AUDIO/VIDEO STREAMING

The stored or live video file is captured and processed on server side. The server is ready to broadcast the video file to the client who is already known to the server. On the server side, first the video file is compressed and converted into RTP packets. After the packetization is over , the AES encryption is done on the RTP payload portion using the encryption key issued by key management. The authentication process is started after the encryption in RTP packet by using authentication key. HMAC-SHA1 hash algorithm is used for authentication. The authentication SRTP packet is ready to send via RTP protocol across the network. If the client- server connection is established and the client is started to receive the video files, the

Journal of Theoretical and Applied Information Technology
20th April 2014. Vol. 62 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

first SRTP packet is sent to the client's buffer. After receiving the SRTP packet, the authentication verification will be done and then decryption will be done on SRTP packet. Now the RTP packet is ready for decompression process. The media player is being received the video file and play out at the end of the file. In our proposed system, MPG and AVI video containers are implemented as video formats while streaming the video files in real-time.

In the secured video streaming implementation, the compressed audio-video data is retrieved and packetized at the SRTP layer for the Data plane at the sending side. The SRTP packetized streams provide timing and synchronization information and as well as sequence number. The SRTP packetized streams are then passed to the UDP layer and the IP layer. The resulting IP packets are transported across the Internet.

At the receiver side the media streams are processed in the reversed manner before their presentation. For the control plane, SRTCP packets and RTSP packets are multiplexed at the UDP layer and are moved to the IP layer for transmission across the Internet.

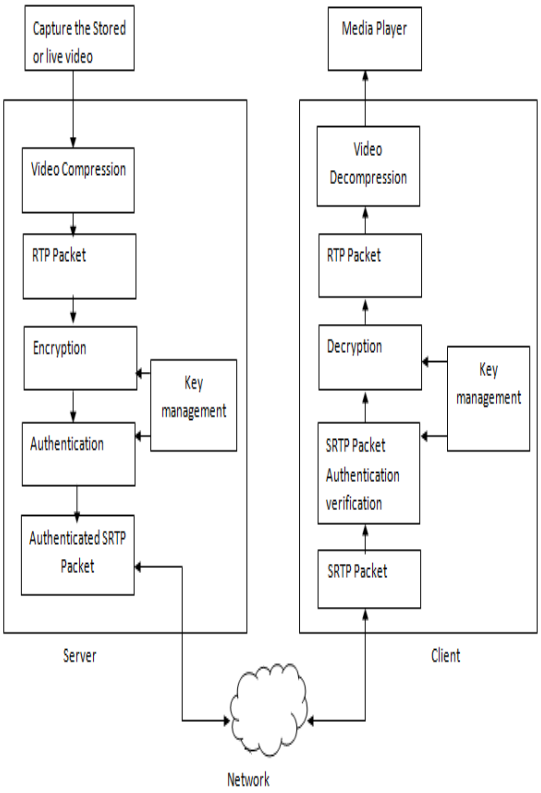

Figure 4. Design and implementation of secure video streaming

7.1 Implementation of Secure RTP Transmission

The video data is acquired from a database and to be streamed under the control of Session Manager, who initialize and control a session so that the server can stream data across the network. The stored or live capture video source to be transmitted across the network by using the RTP protocol. The algorithm of the secure RTP transmission is in Figure 5.

Figure 5. Session Algorithm for RTP transmission

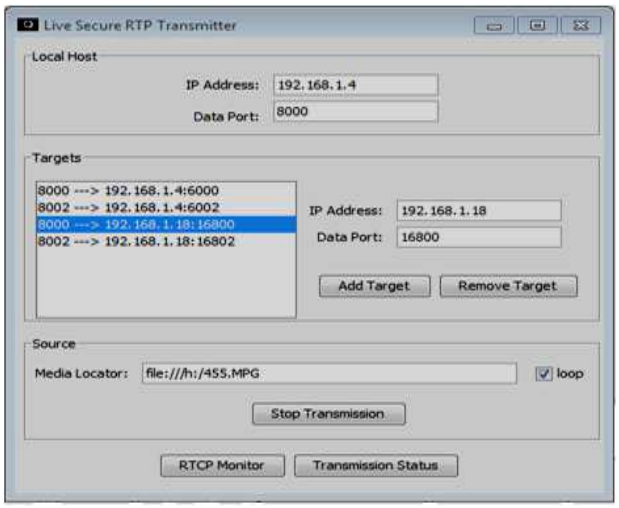

Figure 6. RTP Transmission from Server

The transmission is controlled through the SendStream start and stop methods. The Session Manager is acting as a receiver when it is first started. After SendStream is created, the Session Manager begins to send out RTCP Sender reports and behave as a Sender. It will be a sender host as one as more send stream exist. The sessionManager is act as passive receiver when all SendStream are closed.

Journal of Theoretical and Applied Information Technology
20th April 2014. Vol. 62 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

7.2 Implementation of Secure RTP Reception

The client is registered their IP address and its port address to the server, who is broadcasting the video files. The receiver is constructed a player, which is handled the presentation of an incoming RTP stream. The media locator is used to receive and present a stream from an RTP session that describes the session to construct a player. The format of the media locator is rep : //address: port [: ssrc] /content-type/[++1].

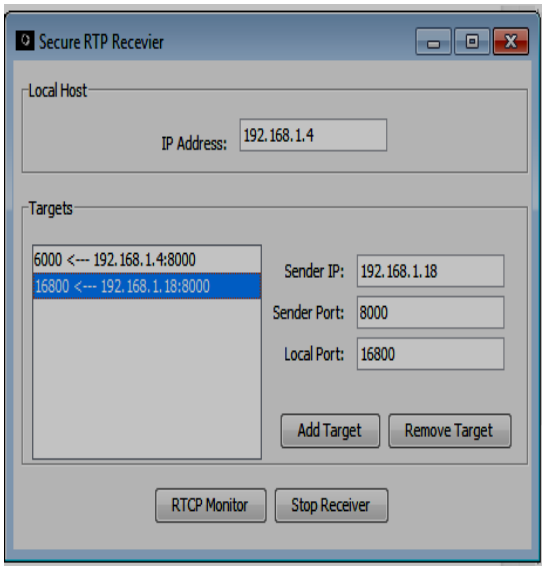

Figure 7. Client –RTP Reception

Figure 8. Receiving the Video streams from Server through Secure RTP

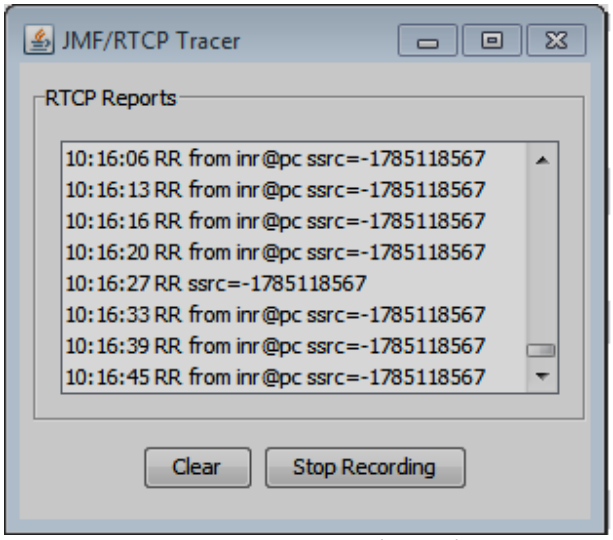

Figure 9. RTCP Tracer in Client side

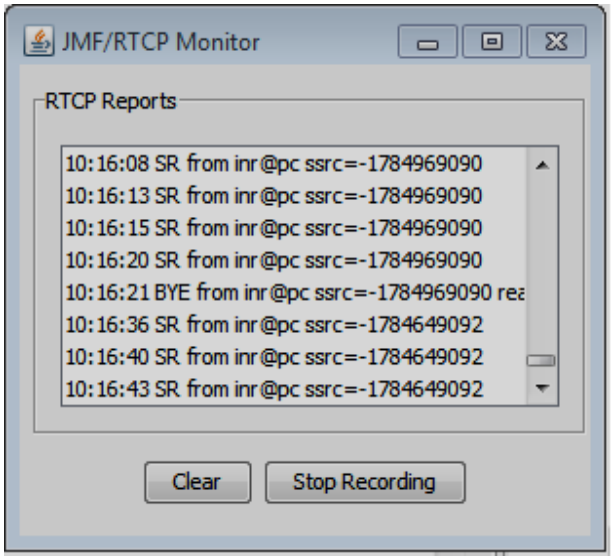

Figure 10. RTCP in Server side

The player is constructed using the first stream in the session when connected with server from client. The sessionManager is used while multiple stream in the session. The sessionManger will send the notification to the receiver whenever a stream is added to the session. The sessionManager is responsible to monitor and control the session directly. On the receiver side, the player is being played out the video files decoded and received at the client end. The JMF player is constructed in client side and it is used to receive the first stream and continue to play at the end of the file. Figure.8 shows the video streaming is received from a streaming server using a secure RTP protocol. RTCP protocol is designed in the server side to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

trace the transmission and the client side for monitor the streams have been received. Figure.9 and Figure 10 show the RTCP Tracer and RTCP monitor and generated RTCP reports on both sides of the server and the client.

8. APPLICATION LAYER QOS

The purpose of application layer QoS control is to avoid congestion and maximize video quality in the presence of packet loss. The application layer QoS control techniques include congestion control and error control. These technique are employed by the end systems and do not require any QoS support from the network. For streaming video, congestion control obtains the form of rate control. There are three kind of rate control: source-based, receiver-based and hybrid rate control. The source-based rate control is suitable for unicast video and other two rate control for multicast video.

9. CONCLUSION

In video streaming system, both progressive download streaming and adaptive streaming have their own benefits and its limitation. The clients have a slower connection and to need high quality then the progressive download would be the best option. If the clients have a fast enough connection to view the stream from the server, the client might save on bandwidth by streaming the video. In our proposed system RTSP server applications transmit captured or stored media streams across the network. The main challenge in designing a video streaming application across the multimedia networks is how to deliver video streams to users with different video codec as secure RTP payload type and provide the data security, efficient video data transmission. The media streams might be encoded in multiple media formats and sent out on several RTP sessions for conferencing with heterogeneous receivers.

REFERENCE:

[1] P. Iyyanar , Dr. M. Chitra *"Effective and Secure Scheme for Video Streaming using SRTP"* International Journal of machine Learning and Computing , volume 2, No.6, December 2012.

[2] Mamma Asghar, Saima *Sadaf "SVS - A Secure Scheme for Video Streaming Using SRTP AES and DH"* European Journal of Scientific Research, Vol.40 No.2 (2010), pp. 177-188.

[3] Tarun Maheswari, Neetu Gupta *Proposal for robust and adaptive forward error correction for real-time audio-video streaming solutions"* IOSR Journal of electronic and communication engineering, volume 3, issue 2, 2012.

[4] http://library.rice.edu/services/dmc/guides/video/VideoFormatsGuide.pdf

[5] http://www.garymcgath.com/streamingprotocols.html

[6] Saurabh Goel *"Cloud-based Mobile Video Streaming technique"* Global Journal of Computer Science and Technology, volume 12, issue 17, 2012.

[7] Howdy Pierce *" The many ways to stream video using RTP and RTSP"* Cardinalpeak , 2011

[8] H. Schulzrinne, A. Rao, and R. Lanphier, *"Real Time Streaming Protocol (RTSP)"*,IETF RFC 2326 (proposed standard), http://www.ietf.org/rfc/rfc2326.txt

[9] http://www.javvin.com/ProtocolRTSP.html

[10] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacob-son, *"RTP: A Transport Protocol for Real-Time Applications"* , IETF RFC 3550, 2003.

[11] M. Baugher, D. McGrew, M. Naslund, E. Carrara, and K. Norrman, *"The Secure Real-time Transport Protocol (SRTP)"*, RFC 3711, 2004

[12] C. Perkins, RTP: Audio and Video for the Internet, Ad-Dison Wesley, 2003.