The Implementation of An Secure RTP Transmission Method Based on DTLS

Zhuang Linlin, Lei Weimin, Zhang Wei, Liu Shaowei
College of Information Science and Engineering
Northeastern University
Shenyang, China
13889151369@139.com, leiweimin@ise.neu.edu.cn,
zhangwei1@ise.neu.edu.cn, liu_nongfu@163.com

Zhuang Linlin, Lei Weimin, Zhang Wei, Liu Shaowei
College of Information Science and Engineering
Northeastern University
Shenyang, China
13889151369@139.com, leiweimin@ise.neu.edu.cn,
zhangwei1@ise.neu.edu.cn, liu_nongfu@163.com

Abstract—**Neither the Real-time Transport Protocol security (RTP) nor the Secure Real-time Transport Protocol (SRTP) key management mechanisms is adequate, the complexity of SRTP based on Datagram Transport Layer Security (DTLS) is too high to reduce the scope of use, so this paper designs a real-time encrypted transport mechanism, using DTLS to achieve key management and negotiating encryption algorithms. Extend the DTLS, and then achieve encryption of RTP based on the DTLS and packaging transmission. To be compared in the particular case, the method, under certain safety requirements, is better suited for the high efficiency transmission network. The mechanism provides a good foundation for real-time multipath transmission. (Abstract)**

Keywords- real-time transport; key management; DTLS-RTP ; complexity (key words)

I. INTRODUCTION

The Real-time Transport Protocol (RTP) was developed by the Audio-Video Transport Working Group of the Internet Engineering Task Force (IETF) [1], using extensively in communication and entertainment systems that involve streaming media. RTP is designed for end-to-end, real-time, transfer of stream data. The protocol provides facility for jitter compensation and detection of out of sequence arrival in data, which is based on the UDP. So, the RTP based on UDP(UDP-RTP) can only guarantee the real-time data transmission, but can do nothing to provide a reliable transport mechanism, flow control or congestion control. The Secure Real-time Transport Protocol (or SRTP) defines a profile of RTP (Real-time Transport Protocol), intended to provide encryption, message authentication and integrity and replay protection to the RTP data [2], however, it does not provide key management. The SRTP based on DTLS(DTLS-SRTP) makes up for the lack of the SRTP key management [3], but it brings a great deal of complexity, and for the moment the use of RTP is far greater than the SRTP, its applicability is inadequate

This paper designed a RTP secure transmission method, which is based on DTLS [4], presented a wide range of applications, low complexity. Using DTLS key management, encryption algorithm negotiation and other functions, achieve RTP encryption and secure transmission based on DTLS. To be compared in the particular case, the method, under certain safety requirements, is better suited for the high efficiency transmission network. The analysis of the principle, DTLS expansion is difficult to design, this method provides a good foundation for real-time multipath transmission.

II. RELATED PRINCIPLES

A. DTLS

In 1999, Transport Layer Security (TLS) was standardized based on Security Socket Layer Protocol (SSL) 3.0 by IETF working group [5]. TLS provides the upper layer a transparent connection-oriented secure channel [6], which can easily be added to the application layer and the transport layer to ensure the security of application protocols, but it is based on reliable transmission channel, the data needs to be reliable and sequentially sent to the receiver, it does not have the internal mechanism to deal with datagram protocol packet loss and disorder issues, so it is not suited to be directly used to ensure that the data reported communication (such as UDP) security.

In recent years, due to its own characteristics, a growing number of applications choose to use packets to transmit data, for example, real-time video conferencing, online gaming, Quack and Startcraft, these applications are delay-sensitive, and the use of unreliable datagram transmission. The Datagram Transport Layer Security (DTLS) protocol provides communications privacy for datagram protocols. DTLS allows datagram-based applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. The DTLS protocol is based on the stream-oriented Transport Layer Security (TLS) protocol and is intended to provide similar security guarantees.

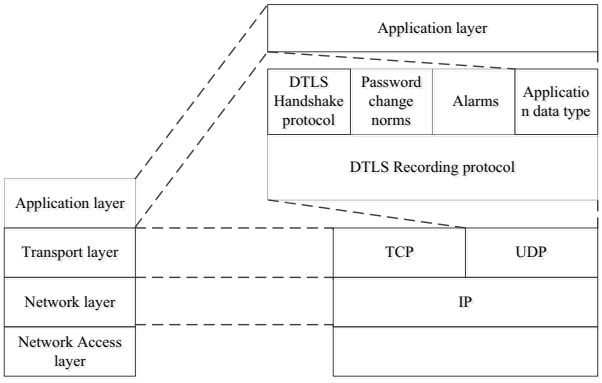

Figure 1 DTLS architecture

978-0-7695-5122-7/13 $26.00 © 2013 IEEE
DOI 10.1109/IMCCC.2013.87

In TCP / IP protocol stack, DTLS is between the transport layer and application layer, it is a layered protocol, which consists of a set of protocols, the architecture is shown in Figure 1.

B. RTP

RTP is used in conjunction with the RTP Control Protocol (RTCP). While RTP carries the media streams, RTCP is used to monitor transmission statistics and quality of service (QoS) and aids synchronization of multiple streams .

RTP packet includes a 12-byte fixed RTP header, and a variable continuous media data. After the header, optional header extensions may be present. This is followed by the RTP payload, the format of which is determined by the particular class of application. The format is shown in Figure 2.

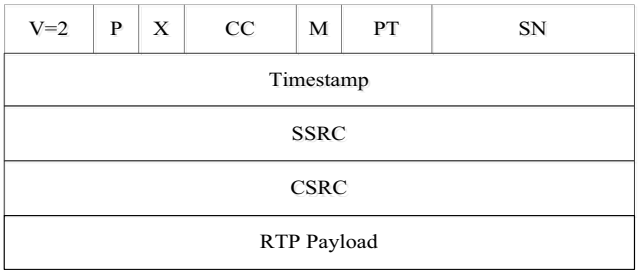

Figure 2 The format of RTP packet header.

RTP is originated and received on even port numbers and the associated RTCP communication uses the next higher odd port number.

During RTP encryption, the sender and receiver is required to maintain status information for each encrypted SRTP stream, the information is defined as encrypted environment. Encrypted environment has two set of parameters, ones related to the encryption and the authentication methods are known as transformation related parameters, and the other parameters are called transformation unrelated parameters, including rollover counter(ROC), the serial number, the encryption algorithm identifier, Master Key Identifier(MKI), the master key, key derivation rate and so on . RTP encryption is as follows.

a)According to formula (1) to determine encryption environment, the ID number of the encryption environment is SSRC, the destination network address and the destination transport port number are uniquely determined ,parameters of encryption communication are determined by the key management.

$$context\ ID =< SSRC,\ destination\ network\ address,\ destination\ transportport\ \ number > \quad (1)$$

b) SRTP packet index number which corresponds to a 48bit value is calculated as follows:

$$i = 2^{16} * ROC + SEQ \quad (2)$$

Determine the master key and master salt: an encryption environment can have multiple master key, the MKI field of data package specified directly or by a <From, To> value and SRTP packet index number determine which SRTP master key to handle the package.

c) Through a key derivation function, derive the session key and session salt.

d) Use encryption algorithm specified by the key management and the session key, the session salt from the previous step to encrypt RTP Payload, then obtain SRTP Payload.

e) If the MKI indicator is 1, then add the MKI field to the packet.

f) Integrity protection: use the message authentication method specified by the handshake negotiation process and the generated session certification key to generate message authentication label, and then the label is attached to the packet.

Encryption process is encryption first, and decryption process was encryption first, if authentication fails then discards, the steps are broadly consistent with these steps, so will not repeat them.

C. DTLS-SRTP

DTLS-SRTP is a SRTP extension for DTLS that combines the performance and encryption benefits of SRTP with the flexibility and convenience of DTLS-integrated key and association management. DTLS-SRTP can be viewed in two equivalent ways: one as a new key management method for SRTP, and the other one as a new RTP-specific data format for DTLS. DTLS-SRTP is defined for point-to-point media sessions, in which there are exactly two participants. Each DTLS-SRTP session contains a single DTLS association, and either two SRTP contexts or one SRTP context. For each RTP or RTCP flow the peers do a DTLS handshake on the same source and destination port pair to establish a DTLS association. Which side is the DTLS client and which side is the DTLS server must be established via some out-of-band mechanism such as SDP. The keying material from that handshake is fed into the SRTP stack. Once that association is established, RTP packets are protected using that keying material.

A DTLS-SRTP session may be indicated by an external signaling protocol like SIP. In [7], it introduces in the SIP protocol, how to represent DTLS-SRTP session. In [8], it introduces a method, which uses SDP extensions to implement SRTP encryption environment parameter negotiation.

The media is transported over a mutually authenticated DTLS session where both sides have certificates. It is very important to note that certificates are being used purely as a carrier for the public keys of the peers. This is required because DTLS does not have a mode for carrying bare keys, but it is purely an issue of formatting. The certificates can be self-signed and completely self-generated. The certificate fingerprints are sent in SDP over SIP as part of the offer/answer exchange.

Endpoints wishing to set up an RTP media session do so by exchanging offers and answers in SDP messages over SIP. In a typical use case, two endpoints would negotiate to transmit audio data over RTP using the UDP protocol. Figure 3 shows a typical message exchange in the SIP trapezoid. DTLS-SRTP brings a great deal of complexity, and for the moment the use

Identify applicable sponsor/s here. If no sponsors, delete this text box. (sponsors)

of RTP is far greater than the SRTP, its applicability is inadequate.

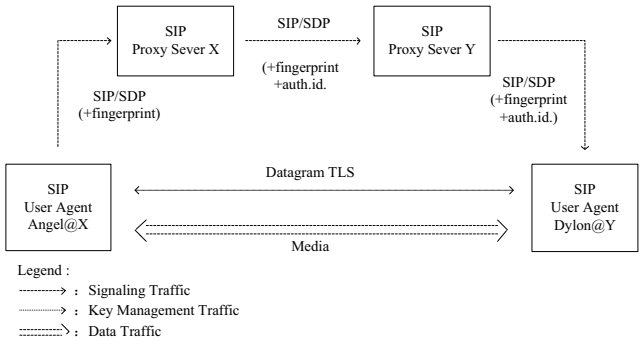

Figure 3 A typical message exchange in the SIP trapezoid.

III. DTLS-RTP

DTLS is generic, for the transmission network, whose safety requirements are not high, but requires a relatively high efficiency, the RTP based on DTLS (DTLS-RTP) is better meet.

A. Design Ideas

By extending DTLS, communicating parties can know RTP data will be encrypted transmission. Use DTLS perfect key management and encryption mechanism, and then the receiving side takes the first byte identification mechanism to distinguish the received data.

B. DTLS Expansion

DTLS recording layer encrypts each application data packet fragments, and then DTLS recording header information need to be attached to each slice. Recording header and encrypted payload are the actual transfer content. DTLS recording header includes the content type, the used protocol version, epoch value, serial number, and the length of the data. The content type is the upper layer protocol type carried by recording layer protocol, including 4 types, handshake, alarms, the password change norms and application data type. Extend the content type field so that DTLS can support RTP transmission.

In order to transmit RTP data and negotiate the use of DTLS data protection, clients include an extension of type "use_dtls_rtp" in the DTLS extended client hello. This extension must only be used when the data being transported is RTP or RTCP. The "extension_data" field of this extension contains the list of RTP parameters, as indicated below.

```
unit8  DTLSRTPProfiles [2];
struct{
DTLSRTPProfiles DTLSRTPProfiles;
}UseDTLSRTPData;
DTLSRTPProfiles DTLSRTPProfiles <2..2^16-1>;
```

Servers that receive an extended hello containing a "use_dtls_rtp" extension can agree to transmit RTP by including an extension of type "use_dtls_rtp", with the DTLS protection in the extended server hello.

C. DTLS-RTP Implementation

DTLS-RTP handshake negotiation process is divided into three logical stages, including exchange the hello information, authentication and key exchange and completes the handshake. Figure 4 shows the process.

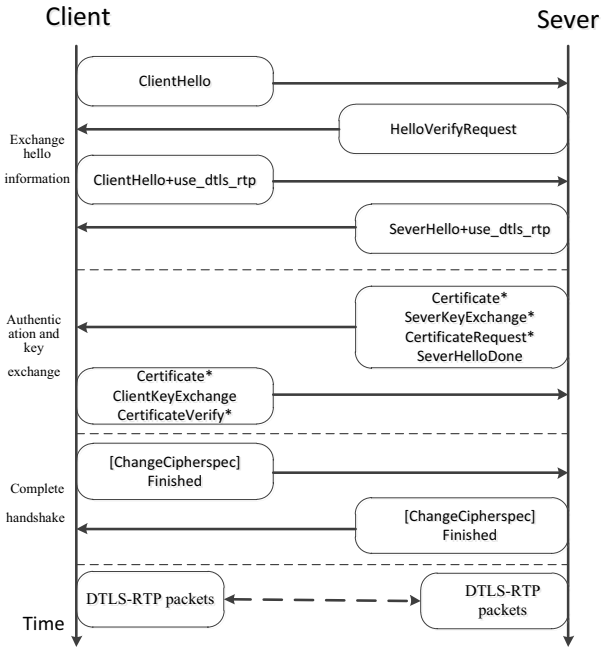

Figure 4 DTLS-RTP handshake negotiation process.

Note that '*' indicates messages that are not always sent in DTLS. The CertificateRequest, client and server Certificates, and CertificateVerify will be sent in DTLS-RTP.

DTLS-RTP data protection: Once the DTLS-RTP handshake has completed, the peers can send RTP or RTCP over the newly created channel. Within each DTLS-RTP session, DTLS-RTP processing must not take place before the DTLS-RTP handshake completes.

First, recording layer protocol divides the RTP data into fragmentations, second, do packet encapsulation. In packet encapsulation process, after MAC value of RTP data being calculated, attach the MAC value to the RTP data fragment, and then encrypt the entire message, the procedure is shown in Figure 5.

DTLS-RTP transmission: DTLS define a number of record content types. In ordinary DTLS, all data is protected using the same record encoding and mechanisms. When in the DTLS-RTP mechanism, this is modified so that data written by upper-level protocol clients of DTLS is assumed to be RTP/RTP and is encrypted using DTLS rather than the standard TLS record encoding. When a user of DTLS wishes to send an RTP packet in DTLS-RTP mode, it delivers it to the DTLS implementation as an ordinary application data write, and then The DTLS implementation then invokes the processing described in Figure 5. The resulting DTLS-RTP packet is then sent directly on the wire as a single datagram with no DTLS framing. This

provides an encapsulation of the data that conforms to and interoperates with RTP.

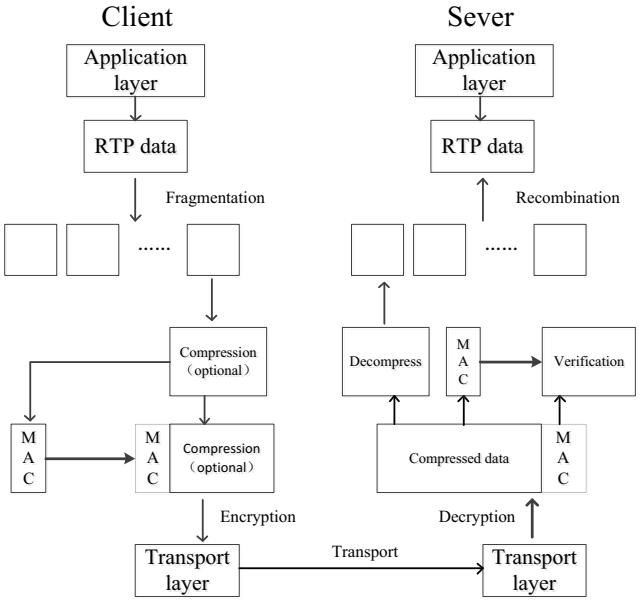

Figure 5 DTLS-RTP data protection

DTLS-RTP reception: When DTLS-RTP is used to protect an RTP session, the RTP receiver needs to demultiplex packets that are arriving on the RTP port. Arriving packets may be of types RTP, DTLS, or STUN [9]. If these are the only types of packets present, the type of a packet can be determined by looking at its first byte. This process is summarized in Figure 6.

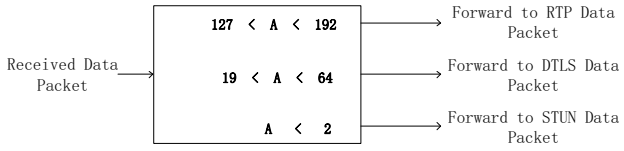

Figure 6: The DTLS-RTP receiver's packet demultiplexing algorithm. Here the field A denotes the leading byte of the packet.

IV. TEST AND VALIDATE MPLATE

In network simulation software omnet++, the Inet framework provides a UDP-RTP implementation. Based on the research, DTLS-RTP implementation is the next job, here we will evaluate the proposed method qualitatively.

A. Security enhancements for RTP

DTLS is a communication protocol, which ensures data transmission in an unreliable channel. DTLS can be applied to all applications based on UDP. DTLS is generic, DTLS extension apply to encryption and transmission of RTP to achieve an improved safety. Here, DTLS was extended only for RTP, if need to support a variety of upper layer protocols, we can also make similar extensions.

a) Recording layer for data encapsulations.

DTLS itself is a layered protocol, in which the recording protocol is an encapsulated protocol for encapsulating and encrypting upper layer protocol data (including application data). DTLS can be used to protect the transmission of any UDP-based applications, so it is easy to implement RTP data package using DTLS record protocol.

b) The certificate authentication mechanism.

In DTLS-RTP handshake negotiation process, the two sides will be authenticated. DTLS-RTP implementation uses certificate authentication mechanism, and the method is based on the Public Key Infrastructure (PKI) architecture.

c) Profect key management.

DTLS-RTP is a RTP extension for DTLS that combines the performance benefits of RTP with the flexibility and convenience of DTLS-integrated key, association management and encryption flexibility benefits of DTLS.

B. Reduce DTLS-SRTP complexity.

DTLS-SRTP takes advantage of encryption benefits of SRTP. For encrypting and decrypting of the data flow and providing confidentiality of the data flow, SRTP (together with SRTCP) utilizes AES as the default cipher. Though technically SRTP can easily accommodate new encryption algorithms, the SRTP standard states that new encryption algorithms besides those described cannot simply be added in some implementation of SRTP protocol. For the moment the use of RTP is far greater than the SRTP, so its applicability and flexibility is inadequate.

The method of implementation of DTLS-RTP applies to RTP directly, which can bring increased RTP security, wide range of applications, low complexity.

V. CONCLUSIONS AND OUTLOOK

DTLS-RTP presented a wider range of applications, lower complexity than DTLS-SRTP, meanwhile more safety than RTP, which uses convenience of DTLS-integrated key, association management and encryption flexibility benefits of DTLS. Under certain safety requirements, DTLS-RTP is better suited for the high efficiency transmission network.

Based on this research, the next target is the completion of network simulation of a DTLS-RTP secures transmission, and trying to extend DTLS-RTP to multi-path transmission.

REFERENCES

[1] Schulzrinne H, Casner S, Frederick R, et al. "A transport Protocol for Real-Time applications", RFC 3550. 2003.

[2] McGrew D, Carrara E, Baugher M, et al. "The Secure Real-time Transport Protocol (SRTP)", RFC 3711. 2004.

[3] McGrew D, Rescorla E, et al. "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)", RFC5763. 2010.

[4] Rescorla E, Modadugu N, et al. "Datagram transport layer security", RFC4347. 2006.

[5] Dierks T, Allen C, et al. "The TLS protocol version", RFC 2246. 1999.

[6] Scott C, Wolfe P, Erwin M, et al. Virtual private networks[M]. O'Reilly Media, Inc. 1999.

[7] Fischl J, Rescorla E, Tschofenig H. “Framework for establishing a secure real-time transport protocol (SRTP) security context using datagram transport layer security (DTLS)”,RFC5764. 2010.

[8] Andreasen F, Baugher M, Wing D. “Session description protocol (SDP) security descriptions for media streams”,RFC4568. July, 2006.

[9] Rosenberg J, Weinberger J, Huitema C, et al. “STUN-simple traversal of user datagram protocol (UDP) through network address translators (NATs)”,RFC 3489. Internet Engineering Task Force (IETF). Mar, 2003.