

# 视频流安全传送系统的设计与实现

时继曦, 沈苏彬

(南京邮电大学 计算机学院, 江苏 南京 210003)

**摘 要:**网络视频流数据具有数据量大、实时性高等特点, 传送中容易遭受窃听、插入、重放等网络攻击。实时传送协议 RTP 对报文身份验证和完整性没有任何定义, SRTP 虽然为视频流传送提供加密、报文身份验证和完整性保护, 但加密范围有限, 提供的身份验证服务较脆弱。在对 SRTP 进行了改进的基础上, 提供密钥推导、加密/解密、报文身份验证的模块化设计, 通过接口调用提高了协议运行的效率和安全性, 并在 linux 环境下进行实现和测试, 对该安全传送方案的实时性、安全性和运行效率进行了分析。

**关键词:**视频流; 流加密; RTP; SRTP/SRTCP

**中图分类号:** TP393

**文献标识码:** A

**文章编号:** 1673-629X(2010)10-0154-05

## Design and Implementation of a Secure Transferring System for Video-Streaming

SHI Ji-xi, SHEN Su-bin

(College of Computer Science, Nanjing University of Posts & Telecommunications, Nanjing 210003, China)

**Abstract:** The network video streaming has characteristics of large volume of data, realtime, etc, so it is vulnerable to be attacked by eavesdropping, insertion and replay. The real-time transport protocol (RTP) does not define the capabilities of message authentication and integrity. SRTP can provide encryption, message authentication, integrity protection for streaming, but it only can provide limited encryption in scope. To improved the SRTP, the key derivation, encryption/decryption, authentication modules are designed which can improve operational efficiency and security through the interface calling. Finally the realtime, security and efficiency of the schemes are analysed and testetd on the linux environment.

**Key words:** video streaming; streaming encryption; RTP; SRTP/SRTCP

### 0 引 言

近年来,以网络视频为主的网络多媒体技术的应用深入各个领域,并正以蓬勃的势头不断发展,逐步走向成熟。视频流在因特网上的传送赶上甚至超越传统的文本数据的传送。同时 IP 视频应用技术作为多媒体流技术的代表也逐步成熟,IP 视频技术已经开始应用于城市安全防范监控、家庭住宅监控等,网络上传送的视频流包含涉及城市安全和家庭隐私的信息,安全传递视频流已经逐步成为一种需求迫切而且实用的技术。

传统的网络环境下的安全传送技术包括 IPsec

(Internet Protocol Security)技术<sup>[1,2]</sup>、SSL(Secure Socket Layer)/TLS(Transport Layer Security Protocol)技术等,在网络层只支持分组传递,SSL/TLS 主要在传送层向上的服务接口上提供的安全控制能力,都不支持流传送。而目前应用比较广泛的实时传送协议 RTP 虽然提供了一定的加密机制,但在具体的实现过程中存在着一些问题,对于完整性和身份验证没有太多的说明,无法满足对安全性要求比较高的视频流的实时传送要求。同时由于 IPsec 在实现过程中隐藏了 TCP 或 UDP 头部数据,取而代之以 ESP<sup>[3]</sup>头部数据,因此,造成 IPsec 在实际网络中跨越防火墙和网络地址转换设备的困难。

IETF 对 RTP 协议进行了扩展,提出一种安全的实时传送协议 SRTP<sup>[4]</sup>。该协议加强了保密性,并定义了报文身份验证、完整性保护和重放攻击保护等安全机制,弥补了 RTP 在安全性能方面的不足。在 SRTP 的基础上对 SRTP 的缺点进行改进,直接进行加密、身份验证的视频流传送安全机制的设计与开发。

收稿日期:2010-01-30;修回日期:2010-04-17

基金项目:国家 863 计划项目(2006AA01Z208);江苏省科技支撑计划项目(BE2009157)

作者简介:时继曦(1982-),男,江苏徐州人,硕士研究生,研究方向为计算机网络与分布计算系统;沈苏彬,研究员,博士生导师,研究方向为计算机网络、网络安全。

目前国内外对视频流安全传送的研究主要有基于流加密算法的研究和基于国际化的研究。针对流加密的研究一般有两个大的研究方向:一是直接加密算法,二是部分加密或叫做选择加密算法。研究热点主要有南开大学基于超混沌的流加密技术<sup>[5]</sup>和基于 Baker 映射的视频流加密算法<sup>[6]</sup>,清华大学主要在选择加密算法上利用扩展压缩视频流的方法<sup>[7]</sup>,中国人民解放军空军工程大学研究利用离散 Hopfield 神经网络对多个线性反馈移位器(LFSR)的非线性选择输出提出了一种强度较高的序列加密系统<sup>[8]</sup>,美国俄亥俄州立大学对 MPEG(Moving Pictures Experts Group)格式的视频进行多层编码加密的研究<sup>[9]</sup>,日本主要对研究流加密引擎进行研究<sup>[10]</sup>。

针对视频流传送的标准化工作国内外主要是对实时传送协议 RTP 的改进和对安全实时传送协议 SRTP 的实现工作,如浙江大学主要研究对安全的实时传送协议 SRTP 的实现<sup>[11]</sup>。

## 1 视频流的特点和安全威胁

### 1.1 视频流数据的特点

目前因特网提供的音频/视频服务大体上可分为三种类型:流式存储音频/视频;流式实况音频/视频;交互式音频/视频。无论哪种类型的视频流数据通信都面临着视频流数据的三个主要特点<sup>[12]</sup>:

(1)数据量大。不同于一般的文本文件,视频图像数据具有数据量大的特点,即使用先进的图像压缩算法进行处理数据量仍然很大。

(2)实时性要求很高,对延迟极为敏感。交互式视频应用端到端延迟应限制在 150ms 之内,这就要求加密算法的时间开销越小越好。

(3)传送是分段进行的。媒体流加密不同于普通文件加密。普通文件加密只要一次性加密全部数据即可,而流媒体加解密需要实时进行。

### 1.2 视频流传送中的安全威胁

视频流在因特网上可能受到的安全威胁主要分为两类:主动攻击和被动攻击。主动攻击如更改报文流、拒绝服务 DoS(Denial of Service)、伪造连接初始化或者恶意程序等<sup>[13]</sup>。被动攻击如截获和窃听他人的通信内容。对被动攻击可采用加密技术,而对主动攻击则需将加密技术与适当的身份验证技术相结合。

#### (1)拒绝服务攻击(DoS)。

由于网络视频要求双方会话的延迟很低,攻击者只需要制造阻塞、RTP 报文或者其他高优先级报文,达到足够数量以后就能使合法的 RTP 流产生延迟,阻碍双方的正常的视频流交互。

#### (2)窃听攻击。

窃听攻击包括拦截、监听、记录通信双方的视频数据信息。由于 RTP 协议没有包括任何机制来防止此类攻击,攻击者在获得视频交互双方的 RTP 报文就可以实现窃听攻击,攻击者只要使用一个监听程序就可以获得传送的视频流信息。

#### (3)插入攻击。

攻击者伪装成其他会话者,然后修改、监听、阻碍、记录双方的正常会话。插入攻击主要是由于 RTP 协议缺少加密和身份验证机制。

## 2 RTP 协议及其安全问题

### 2.1 RTP 协议栈描述

实时传送协议 RTP 是 IETF 制定的一种针对多媒体数据流传送的协议<sup>[14]</sup>,RTP 为实时应用提供端到端的数据传送服务,但不提供任何服务质量的保证。最常用的是 IP/UDP 网络。由于 RTP 向多媒体应用程序提供了服务(如时间戳和序号),因此也可以将 RTP 看成是在 UDP 之上的一个运输层的子层。

### 2.2 RTP 协议的安全问题

RFC1889 中定义的基本的 RTP,提供了对 RTP 报文加密的灵活实现,实现过程中允许对报文进行全部或部分的加密和解密。由于 RTP 与 IPsec 在技术上相互独立,IPsec 并不能解决所有的安全问题,并且 IPsec 不支持多播,当 RTP 采用多播技术传送实时音频和视频数据时,网络的通信安全将得不到保障。

## 3 安全机制的设计

SRTP 虽然能为视频流传送提供加密、报文身份验证和完整性保护,但只是通过增加有效报体的方式,加密范围有限。在 SRTP 的基础上,针对其缺点和不足进行改进和完善,提供加密、身份验证的模块化设计。对 SRTP 所定义的安全机制进行抽象的提取和概括,将不同的功能封装在不同的模块中,主要有密钥推导模块、加密解密模块、报文身份验证模块。如图 1 所示。

### 3.1 密钥推导模块

由于视频流传送需要低延时,所以一般的密钥协商协议都不适用于流传送<sup>[15]</sup>,可以用来解决实时多媒体会话间的密钥管理的密钥管理协议 MIKEY(Multimedia Internet KEYing)。无论是使用加密传输还是身份验证传输,SRTP 必须通过密钥生成器来产生会话密钥(Session Key),以主密钥和会话密钥和报文的索引号为参数,利用密钥推导函数获得三个密钥:加密密钥,身份验证密钥和 salt 密钥<sup>[11]</sup>。

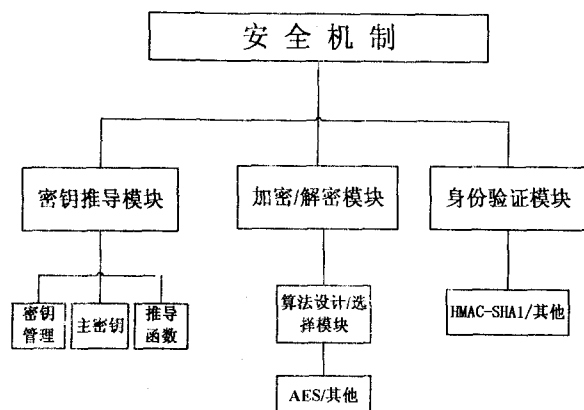


图1 安全机制的设计模块

### 3.2 加密/解密模块

此模块是整个安全机制的核心,由于视频流数据的数据流大、实时性要求高等特点,所以视频流的安全传送不可能完全像 SSL/TLS, IPsec 等协议设计的那样复杂,只能在流加密算法选择和密钥管理上进行有效的的设计。由于流加密对实时性要求特别高所以加密过程不可能设计的很复杂,只需一个密钥流生成器:如 AES-CRT 来产生密钥流,然后与 RTP 报体异或运算即可得到密文流。

### 3.3 身份验证模块

SRTP 里预定义的身份验证算法是 HMAC-SHA1<sup>[16]</sup>。根据对 SRTP 的分析,SRTP 通过增加身份验证标签来提供身份验证机制。SRTP 报文的身份验证部分组成了 RTP 的报头,其后是 SRTP 报文的加密部分。身份验证标签通过身份验证序列号为 RTP 头部和报体提供身份验证,它直接提供防止重放攻击的保护。身份验证模块的流程如图 2 所示。

## 4 验证方法和结果

### 4.1 验证方法

通过在局域网中的两台 linux 2.4.0 版本的 Red-Hat 9.02.4.20-8 上同时安装了程序模块,一端作为服务器端发送视频流数据,一端作为客户端接收视频流数据。文中的实现模型是基于开源库 LibSRTP,将其版本为 srtp-1.4.4.tgz 的压缩包下载并拷贝到 IP 地址为 10.10.136.100 的 linux 目录/home/shiqun/paper/下。

根据上文提出的理论模型分别对 Srtplib 的源文件 Srtplib.c 和 Rtpw.c 进行修改,对其安全策略加密、身份验证、完整性保护机制进行优化处理,最后重新编译执行:

#### ●发送端。

(1)在发送端首先启动密钥生成模块生成一个 30

位的 16 进制数,前 10 位是加密/解密密钥,中间 10 位为身份验证密钥,后 10 位为完整性校验密钥,通过查看命令 echo \$k 可知 k=1c705ac803315a76cc810b94ba59022634a1c308791cca478700147cb296。

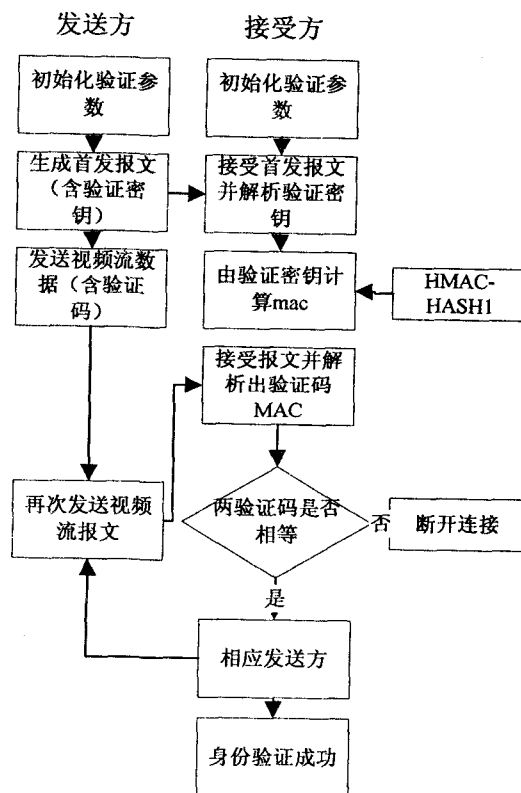


图2 身份验证模块的逻辑流程

(2)执行 Srtplib/test/目录下的可执行文件 rtpw, 其中各个参数的含义为: -s 发送数据流, -k:加密验证密钥, -e 加密保护, -a 身份验证和完整性保护, 10.10.136.100 是本 linux 虚拟机的 IP 地址, 8866 为选择发送的 UDP 的端口号。

(3)发送数据,从视频采集到的视频数据经过应用层处理后传给传送层,视频流数据是以流为语义单元的。发送端的运行结果如图 3 所示。

```

File Edit View Terminal Go Help
[root@localhost srtp]# echo $k
1c705ac803315a76cc810b94ba59022634a1c308791cca478700147cb296
[root@localhost srtp]# test/rtpw -s
security services: confidentiality
set master key/salt to 1c705ac80331
sending word: Aarhus
sending word: Aaron
sending word: Ababa
sending word: aback
sending word: abaft
sending word: abandon
  
```

图3 经 SRTP 安全处理的数据由 UDP 发送

●接收端。

(1)在接收端接收解密、身份验证、完整性校验密钥,和发送端发送的密钥一致。

(2)执行 Srtplib/test/目录下的可执行文件 rtpw 各个参数的含义为: -r 接收数据流, -k 加密验证密钥, -e 加密保护, -a 身份验证和完整性保护。

(3)从运行结果看出接收到的数据和发送的数据是一致的。接收端的运行结果如图 4 所示。

```
root@localhost:/home/shijun/paper/Srtplib
File Edit View Terminal Go Help
[root@localhost srtplib]# echo $k
1c705ac803315a76cc810b94ba59022634a
[root@localhost srtplib]# test/rtpw -r
security services: confidentiality
set master key/salt to 1c705ac80331
received word: Aarhus
received word: Aaron
received word: Ababa
received word: aback
received word: abaft
received word: abandon
```

图 4 从 UDP 接收的数据经 SRTP 安全处理

4.2 结果分析

(1)实时性分析。通过在本机上部署实验,分别在发送方和接收方记录发送时间和接收时间,同时先测试出网络时延,最后比较当每个安全机制加载时对传送时延的影响。

实验主机性能参数: CUP: T2390, 1.86GHz, 内存 0.98GB, 网络带宽: 10MB/s。

发送时间: 发送端在数据流被安全机制处理发送之前调用系统函数获得当前的时间, 时间格式为: 分: 秒: 毫秒, 这里是精确到毫秒级。

接收时间: 接收端在数据流到达经过安全机制处理之后调用系统函数获得当前的时间。

网络时延: 指单纯通过 UDP 传送数据的网络传送时间, 这个时间在本试验中是基本固定的, 大约在 260ms 左右。

处理时间: 指发送视频流数据和接收完视频流数据的时间差减去网络传送时间得到的安全机制处理的时间, 这个最直接衡量使用本安全机制执行时间的参数。

由表 1 可以看出当不使用任何安全机制时, 发送时间和接收时间差为网络传送时延, 处理时间为 0ms, 当使用加密保护时, 处理时间为 11ms, 增加验证保护时处理时间为 29ms, 增加完整性保护时处理时间为 41ms。可以看出加入本安全机制对视频流数据实时

性的影响不大。

表 1 数据流传送的实时性分析

	发送时间	接收时间	网络传送时延	处理时间
无保护	03:05:18	03:05:279	261ms	0ms
加密保护	03:09:103	03:05:377	263ms	11ms
验证保护	03:11:702	03:11:998	267ms	29ms
完整性保护	03:14:94	03:14:403	268ms	41ms

(2)安全性分析。安全性是本课题研究的最直接的目标, 使用的安全机制能满足视频流传送的安全需要, 能防止各类攻击。

防止窃听攻击: 在密钥推导模块和发送模块的保护下, 即使有非法用户截获视频流数据, 但因没有密钥无法还原数据。

防止插入/删除攻击: 在身份验证模块, 通过增加报文的身份验证码和完整性保护序列来提供报文完整性验证和数据源标识验证。

防止重放攻击: 通过两种方法解决重放攻击问题, 一是通过检查 SRTP 报文的序列号是否重复来进行攻击识别; 二是通过完整性保护模块的完整性校验序列来进行校验。

(3)效率分析。主要对安全传送系统的开销进行描述和分析, 这里主要从 CPU 的利用率上来进行分析, 考察的是 CPU 在 0~50s 时间内的利用率, 如图 5 下面的线条为系统没有进行视频流数据传送时 CUP 的利用率, 5% 左右, 中间线条为系统直接利用 SRTP 协议传送流数据时的 CUP 利用率, 20% 左右。上面线条使用改进 SRTP 后的 CPU 的利用率, 7% 左右, 基本上和没有传送视频流数据时的 CPU 的利用率差不多。

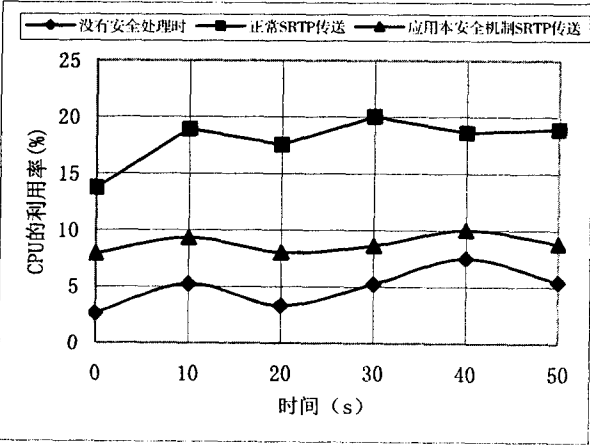


图 5 数据流传送的效率分析

5 结束语

通过对安全实时传送协议 SRTP 的研究, 并查阅

IETF 最新的标准 RFC5506, 对 SRTP 的安全问题做的补充性描述, SRTP 对于首次发送的两个报文没有做明确的处理<sup>[17]</sup>, SRTP 的安全方案有待进一步改进。

文中对 SRTP 协议的密钥推导、加密/解密、身份验证等安全机制进行了抽象的提取和概括, 并进行模块化的设计和实现, 这样彼此之间只要通过接口调用就可以协调工作, 在一定程度上提高了效率, 从而对实时性要求特别高的视频流传输来说减少了延时, 提高了会话效果。

#### 参考文献:

- [1] Doraswamy N, Harkins D. IPSec: The new security standard for the internet, intranets, and virtual private networks[M]. Upper Saddle River, NJ: Prentice Hall, 1999.
- [2] Kent S, Seo K. Security architecture for the internet protocol [S]. Internet Engineering Task Force, RFC 4301, 2005.
- [3] Kent S. IP Encapsulating Security Payload (ESP) [S]. Internet Engineering Task Force, RFC 4303, 2005.
- [4] Baugher M, McGrew D, Naslund M, et al. SRTP: The Secure Real Time Transport Protocol [S]. RFC 3711. IETF, 2004.
- [5] Chen Shuhui, Chen Zengqiang, Yuan Zhuzhi. A Compound Video Encryption Algorithm Based on Hyperchaos [C]// Innovative Computing Information and Control, 2008. ICICIC '08. 3rd International Conference. [s.l.]: [s.n.], 2008.
- [6] 张 萌, 王繁珍, 刘忠信, 等. 基于 Baker 映射的视频流加密算法 [D]. 天津: 南开大学, 2006.
- [7] 袁 春, 钟玉琢, 杨士强, 等. 基于视频对象模板的可扩展压缩视频流加密算法 [D]. 北京: 清华大学, 2005.
- [8] 赵全习, 胡文志, 郑连清, 等. 一种流加密方案的设计与分析 [D]. 西安: 空军工程大学, 2007.
- [9] Tosun Ali Saman, Feng Wu - chi. Efficient Multi - layer Coding and Encryption of MPEG Video Streams [M]. [s.l.]: IEEE, 2000.
- [10] Fukase M, Takeda H, Tenma R, et al. Development of a Multimedia Stream Cipher Engine [M]. [s.l.]: IEEE, 2006.
- [11] 朱孙斌, 陈惠芳, 赵问道, 等. 安全的实时传输协议 SRTP 的研究与实现 [M]. 北京: 中国学术期刊出版社, 2004: 30 - 33.
- [12] Ooi H - S. High - speed stream ciphe [C]// Advanced Information Networking and Applications. 18th International Conference. [s.l.]: [s.n.], 2004: 39 - 42.
- [13] 王 一, 陈 凯, 喻 靓. RTP 流插入攻击及安全机制研究 [D]. 上海: 上海交通大学, 2007.
- [14] Schulzrinne H, Casner S, Frederick R, et al. RTP: A Transport Protocol for Real - time Applications [S]. RFC 3550. IETF, 2003.
- [15] Baugher M, Weis B, Hardjono T, et al. The Group Domain of Interpretation [S]. RFC 3547. IETF, 2003.
- [16] Krawczyk H, Bellare M. HMAC: Keyed Hashing for Message Authentication [S]. RFC 2104. IETF, 1997.
- [17] Johansson I, Westerlund M. Support for Reduced - Size Real - Time Transport Control Protocol (RTCP) [S]. RFC 5506. IETF, 2009.

(上接第 11 页)

- [5] Narayanaswamy S, Kawadia V, Sreenivas R S, et al. Power Control in ad - hoc networks: theory, architecture, algorithm and implementation of the COMPOW protocol [C]// In: Proc of European wireless Conf. Italy: [s.n.], 2002: 156 - 162.
- [6] Kubisch M, Karl H, Wolisz A, et al. Distributed algorithm for transmission power control in wireless sensor networks [C]// In: Proc of IEEE WCNC 2003. New Orleans: IEEE press, 2003.
- [7] Blough D, Leoncini M, Resta G, et al. The k - neighbors protocol for symmetric topology control in ad hoc networks [C]// In: Proc of ACM MobiHoc 03. Annapolis, MD: ACM press, 2003: 141 - 152.
- [8] Xu Y, Heidemann J, Estrin D. Geography - informed energy conservation for ad hoc routing [C]// In: Proc of the 7th annual international conference on Mobile computing and networking. Rome, Italy: ACM press, 2001: 70 - 84.
- [9] Heinzelman W R, Chandrakasan A, Balakrishnan H. An application - specific protocol architecture for wireless microsensor networks [J]. IEEE Transactions on Wireless Communications, 2002, 1(4): 660 - 670.
- [10] Deb B, Bhatnagar S, Nath B. A topology discovery algorithm for sensor networks with applications to network management [EB/OL]. 2001 - 05. <http://athos.rutgers.edu/dataman/papers/TopDisc.pdf>.
- [11] Liu L F, Jin S. A Clustering Control Algorithm of Wireless Sensor Networks in Low Probability Event Scenario [J]. Journal of computer research and development, 2008, 45(10): 1662 - 1668.
- [12] Li N, Hou J C, Sha L. Design and analysis of an MST - based topology control algorithm [C]// In: Proc of Twenty - Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFORCOM 2003). San Francisco, CA: IEEE press, 2003: 1702 - 1712.