利用IPv6提高基于SIP的VoIP的安全性

邓宁波　葛君伟　陈　宁
（重庆邮电学院计算机学院　重庆400065）

摘　要　基于SIP的VoIP作为NGN网络的一项重要业务，正越来越多地得到国际上诸多大型通信公司的支持，极大地推动了NGN的发展。同时网络也变得更为复杂，使得一些重要的安全特性不复存在。因此分析了SIP协议及协议栈结构，列出了基于SIP的VoIP的安全隐患。提出了利用IPv6来提高它的安全性的原理和方法。

关键词　下一代网络，会话初始协议，IPv6，验证报头，封装安全有效载荷

Adopting IPV6 Enhance Security of Voip Base Sip

Deng Ning-bo　Ge Jun-wei　Chen Ning
(Department of computer technology, Chongqing University of Posts and Telecommunications, Chongqing 400065)

Abstract　VoIP base SIP is one service of NGN, which is supported by many communication corporations, accelerate the evolution of NGN. At the same time, network becoming complex make many security characters disappear. So, list these security fault of VoIP base SIP through analyzing SIP and architecture of SIP Stack. And bring forward theory and methods that adopting IPv6 enhance security of VoIP base SIP.

Keywords　NGN, SIP, IPv6, AH, ESP

1　引言

近年来，我国通信事业发展迅速，综合通信能力明显增强。各种网络趋于融合。网络负荷越来越大，业务要求也越来越多样化。在这种背景下，基于软交换技术的NGN网络应运而生。NGN又称下一代网络，是一种综合、开放的网络架构，提供语音、数据、多媒体等业务。实时的IP呼叫和多媒体通信是下一代网络(NGN)提供的重要业务。H.323和SIP(session initiation protocol)都是实现多媒体应用的通信协议。但是基于SIP的VoIP系统相对于H.323的复杂性，SIP采用文本编码，易于解析和调试，实现较容易。另外，SIP在音频、视频编/解码类型的增加和新业务的增加方面较方便，并且效仿了较为成熟的HTTP和SMTP，具有丰富的扩充能力和兼容功能。SIP提供了H.323类似的服务，但更简单，扩

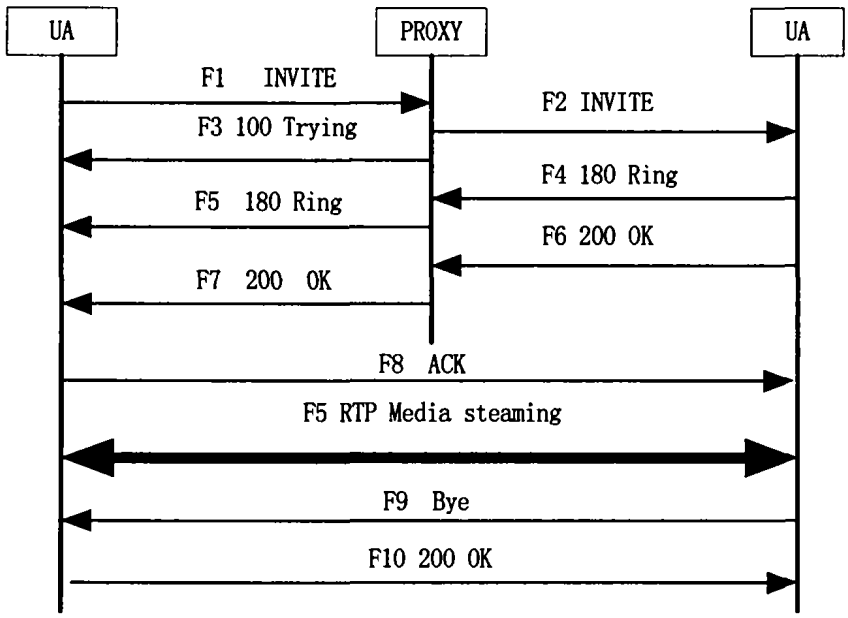

图1　呼叫序列图

邓宁波　研究生，网络安全，网络管理；葛君伟　教授，硕士生导师，重庆中韩GIS研究所所长，网络安全，网络体系结构，GIS信息系统，空间数据库；陈　宁　硕士研究生，网络安全，网络管理。

充性好，适合大规模使用。此外，SIP 提供了良好的 QoS 支持，这对于 NGN 在 IP 网络上实现 VoIP 来说，SIP 在全面满足 NGN 特性要求的应用上具有独特的优势，将成为下一代网络 VoIP 的重要方案。因此如何提高基于 SIP 的 VoIP 的安全性将会是 NGN 网络安全研究的关键技术领域。

2 SIP 协议分析

2.1 SIP 呼叫流程

如图1是一个简单的有 SIP 代理的 SIP 呼叫的建立过程。①F1，主叫呼叫被叫②F2，代理呼叫被叫③F3，代理发送100trying 信息给主叫④F4，被叫发送振铃给代理服务器⑤F5，代理发送振铃给主叫⑥F6，被叫摘机应答⑦F7，代理发送摘机信息给主叫⑧F8主叫应答建立通话⑨双方进行通话⑩F9被叫发送结束通话消息，F10主叫响应，结束通话。

2.2 SIP 电话协议栈

SIP 不是垂直型通信系统，不能独立提供业务，它必须与其它协议共同使用来构建一个完整的多媒体体系结构，所以在构建下一代网络的多媒体体系时，采用以下的协议组合提供多媒体业务。基于 SIP 的电话协议栈如图2所示。

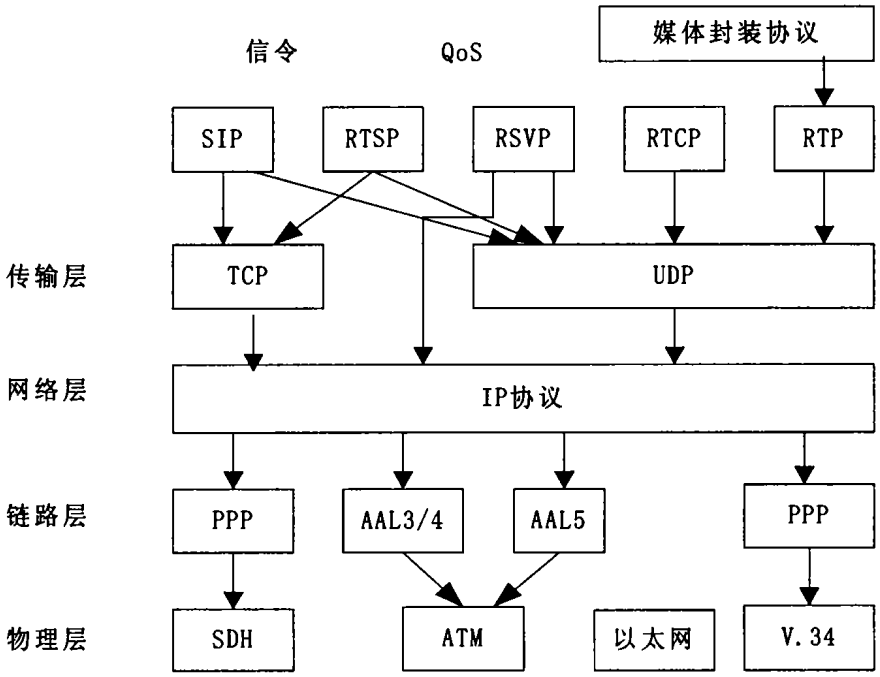

图2 SIP 电话协议栈

·RTSP(realtime streaming protocol)控制发送“一点到多点”文本格式的多媒体数据流。

·RSVP(reservation protocol，资源预留协议)用于主机为特定应用数据流请求特定的 QoS 以及端点应用程序发送 QoS 请求，为数据传送的各个节点保留网络资源(如带宽，缓冲区大小等)，大大增强了现有 Internet 网络的 QoS 控制。

·RTP(real-time transport protocol，实时传送协议)用于 AMR(adaptive multi-rate)和 AMR-WB (adaptive multi-rate wideband)编码的语音信号的实时传送，并提供 QoS 反馈。

·RTCP(real-time transport control protocol，实时控制协议)用于传递实时信号的质量参数，提供 QoS 监视机制，同时还可用于传送用户的信息，建立呼叫控制机制。

媒体封装主要采用 ITU－T 的 G 系列和 H 系列建议，G 系列用于语音压缩，H 系列用于视频压缩，提供视频电话。

3 SIP 的安全隐患以及对策

3.1 安全隐患：

从上面的 SIP 的呼叫流程和协议栈可以看出基于 SIP 的 VoIP 存在以下几个安全问题：

SIP 协议：有些安全漏洞与 SIP 本身有关。默认状态下，SIP 消息采用未加密的明文格式发送，因而容易被截获和篡改。

RTP 协议：SIP 的会话将由可靠传输协议(RTP)来承载。而这种协议容易被截获及篡改，比如起始和目的地址被截获及篡改。如果 RTP 会话未经加密，无法防止身份失窃或者会话内容被篡改。RTP 安全缺乏一种明确的标准。

代码和脚本攻击：传统 IP 电话、软 IP 电话和 PBX 都有可能受到来自可执行代码或脚本的攻击。有人可能会利用可执行代码和脚本控制用户或 NGN 接口，或者传播其他类型的攻击，如 DDoS 攻击。

3.2 安全对策

基于SIP的VoIP有多种安全考虑，可以通过加装防火墙、加密、鉴权、被叫隐藏等一系列的安全措施来保障它的安全性。

加密：SIP请求和响应可能包含关于通信模式以及个人通信内容的敏感信息。SIP消息也可能包含了自己的会话加密密钥。SIP支持两个补充的加密方式以保护秘密：

①对于SIP消息体以及敏感头域的End-to-End加密。

②hop-by-hop加密以防止偷听跟踪主叫和被叫；hop-by-hop是在传输层或者网络层进行加密的方法。

③如果终端系统不能加密，代理服务器需要加密SIP请求以加强安全。

鉴权：必须采用保护方法来防止活跃的攻击者发送修改过的SIP请求和响应。采用用来保证SIP消息真实性的加密方法对初始发送者进行鉴权。鉴权的方式中，可以提供hop-by-hop鉴权，即传输层或者网络层鉴权。

被叫隐藏：用户地址和SIP发起的呼叫可能会侵犯被叫的安全。应该能够针对每一个用户来限制该类被叫用户可以接受的地址以及可能的信息。对被叫信息的隐藏正是基于这种考虑。

在上述的安全考虑中，在进行加密和鉴权时都可以采用hop-by-hop的方式。而IPv6是网络层的协议，它在IPv4的基础上有着许多改进，在安全方面有独特的优点。

4 IPv6如何提高SIP电话的安全

4.1 IPv6协议

IPv4从出现的那天一直用到现在，得到了广泛应用，但是它存在许多不足。其中重要的一点就是安全性的不足。在Internet中传输数据，安全性很重要。而IPv4本身不提供任何验证和加密特性。而IPv6包含了更多的验证和加密选项。这是通过验证报头和封装安全有效载荷报头成为IP报头的一部分来实现的。这些报头作为扩展报头，如果需要的话可以附在IP数据报后。

4.2 IPv6实现了SIP电话在网络层的安全

其具体实现主要通过IP的扩展报头AH(Authentication Header)和ESP(Encapsulating Security Payload)标记来实现。IPv6实现了IP级的安全。

验证报头：

在网络层，IPv6可以通过对SIP会话的IP数据包的包头进行数据完整性和IP分组的鉴权，其标记包含下图3字段。

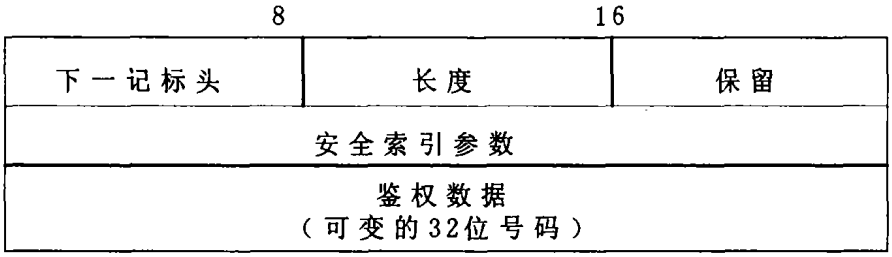

图3 鉴权头标记

下一标记(8bit)表征下一标记的类型；

长度，以32位为单位，鉴权数据字段的长度；

保留字段，留作将来用；

安全参数索引(可变32bit)，32位数字对应一安全协议套；

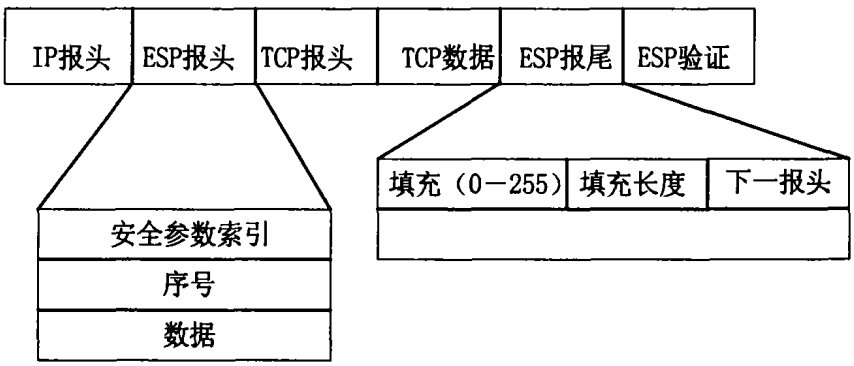

图4 ESP字段信息

鉴权数据，鉴权数据字段的内容由鉴权逻辑来确定，鉴权数据是整个IP分组通过一定的算术逻辑

计算所得(除传输过程中会引起改变的字段外,这些字段在传送过程中被设成0)。

SIP 主叫端的 IP 数据包鉴权计算需在分段前执行,被叫端的鉴权计算则在分段重新合成后进行。只要 SIP 终端和代理服务器共享密钥,鉴权过程就是安全的。通过对数据的验证能够保证报文在传输的过程中没有被更改。

封装安全有效载荷:

ESP 根据 SIP 会话的特殊需求,支持 IP 分组的私密和数据完整性。它既可用于传送层(如 TCP、UDP、ICMP)的加密,称传送层模式 ESP;同时又可用于整个分组的加密,称隧道模式 ESP。ESP 标记以32位的 SPI 开始,余下字段根据不同的解密逻辑算法而有所不同。标记的开始部份,包括 SPI 和其他一些参数,不以加密的方式传送,其余部份则加密传送。如图4所示。

通过 ESP 报头,保证了数据的机密性。它使得 SIP 会话的双方能够将数据报的内容修改成一种中间设备不可理解的格式。从而保证了 SIP 会话的机密。

总之,IPv6的 IP 安全性(IPSec)机制和服务一致。除了必须提供网络层安全这一强制性机制外,IPSec 还提供认证报头(AH)用于保证数据的一致性,而封装有效载荷报头(ESP)两种服务用于保证数据报级别的数据保密性和数据一致性,加强了 IP 数据报的安全。从而使得基于 SIP 的 VoIP 在网络层的安全得到了保证,进而提高了整个应用的安全性。

5 SIP 对 IPv6的支持

SIP 协议支持 IPv6,并且提供了应用的接口。SIP 消息体采用 SDP 定义,而 SDP 的传送和媒体的协商则由 RTSP,HTTP 等来完成。通过在 SDP (Session Description Potocol)对 IPv6地址的引用描述直接支持 IPv6在 SIP 协议中的应用。如图5是一个 SDP 的描述信息:

```
v=0 //协议版本信息
o-nasal 971731711378798081 0 IN IP6 2201:056D::112E:
    144A:1E24
//用户名 会话 ID 版本信息  网络类型  IP 地址类型  IP
    地址
    其它描述信息……略……
```

图5 SDP 对 IP 地址类型的描述

结束语 IPv6作为网络层的协议,它不仅提供了比 IPv4更多的网络空间地址,而且它对安全有着更多的考虑,增加了报头验证和安全报头封装的扩展报头。报头验证确保了报文在传输的过程中没有被更改。安全报头封装使得双方的数据的机密性得到保证,从而提高了基于 SIP 的 VOIP 的安全性能。

参 考 文 献

1 RFC2543,SIP 协议[S]

2 万敏,万晓榆. 基于 SIP 的 VoIP 在下一代网络中的应用[J]. 重庆邮电学院学报. 2003

3 NGN 呼唤安全[EB/OL]. http://www.ctiforum.com/forum/forum.htm/NGN 呼唤安全.htm. 2003-12-12

4 Shanmugam Ramadas, Padmini R, Nivedita S. Special Edition Using TCP/IP, Second Edition[M]. 北京:电子工业出版社, 2003.8

5 IPv6的安全性[EB/OL]. http://www.erp110.com/netschool/ip/ip1.htm

6 RFC3266,Support for IPv6 in Session Description Protocol[S]

7 RFC2327,Session Description Protocol[S]

(上接第212页)

$P(y)=P(k)$

对于任意的明文 $x\in\rho$ 和密文 $y\in e$ 有:

$P(y|x)=P(y)$

而

$P(x,y)=P(y|x)P(x)$

$=P(x|y)P(y)$

故有:

$P(x|y)=P(x)$

即对任意的明文概率分布,这个密码体制仍然是完善保密的。

结束语 近年来密码学的研究有所改变,一方面人类计算能力愈来愈强,另一方面,大量有扰信道的开通,使得信伙伴之间能够共享源源不断的互信息;使用信息处理技术,将这些互信息中敌手已知的部分去掉,保留并协调敌手未知的部分,通信伙伴之间就获得了源源不断的密钥流,因此不需要精心地设计密码函数,只需用群运算来加密和解密即可,使得完善保密性得以实现。但完善保密性的应用还有待进一步的开发。

参 考 文 献

1 [加]Stinson D R,冯登国译. 密码学原理与实践. 北京:电子工业出版社,2002.1~60

2 孟庆生. 信息论. 西安:西安交通大学出版社,1982.446~536

3 胡予濮,等. 对称密码学. 北京:机械工业出版社,2002. 1~14

4 王云光. 关于密码体制的完善保密性. 大连理工大学学报,2003,43(增刊):69~71

5 王云光. SPN 线性密码分析中的线性逼近函数. 电子信息学报,2003,25(增刊)