



(12) 发明专利

(10) 授权公告号 CN 102868665 B

(45) 授权公告日 2016. 07. 27

(21) 申请号 201110187072. 8

CN 102035718 A, 2011. 04. 27,

(22) 申请日 2011. 07. 05

CN 102111404 A, 2011. 06. 29,

(73) 专利权人 华为软件技术有限公司

CN 101090314 A, 2007. 12. 19,

地址 210012 江苏省南京市宁南大道 11 号
花神国际大酒店

CN 101197674 A, 2008. 06. 11,

CN 101090314 A, 2007. 12. 19,

CN 101197674 A, 2008. 06. 11,

(72) 发明人 周学艺 杨俊 张凯 曹鸿涛

审查员 徐苏宁

(74) 专利代理机构 北京中博世达专利商标代理
有限公司 11274

代理人 申健

(51) Int. Cl.

H04L 29/06(2006. 01)

H04L 9/32(2006. 01)

(56) 对比文件

CN 101771535 A, 2010. 07. 07,

CN 1889562 A, 2007. 01. 03,

CN 1682505 A, 2005. 10. 12,

US 7243370 B2, 2007. 07. 10,

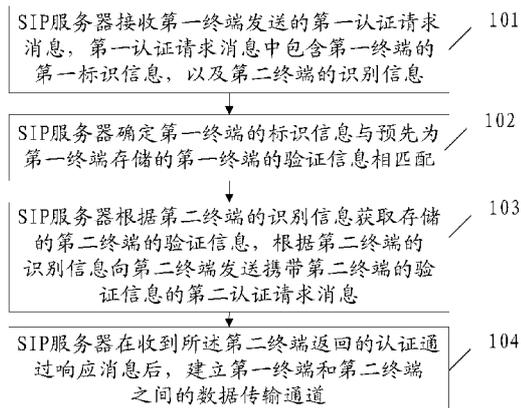
权利要求书1页 说明书15页 附图5页

(54) 发明名称

数据传输的方法及装置

(57) 摘要

本发明实施例公开了一种建立数据传输通道的方法、系统、SIP 服务器、会话边界控制器, 涉及通信技术, 能够提高数据传输的安全性。该方法包括: 接收第一终端发送的第一认证请求消息, 第一认证请求消息中包含第一终端的标识信息, 以及第二终端的识别信息; 确定第一终端的标识信息与预先存储的第一终端的验证信息相匹配; 根据第二终端的识别信息向第二终端发送携带第二终端的验证信息的第二认证请求消息; 在收到第二终端的认证通过响应消息后, 建立第一终端和第二终端之间的数据传输通道。主要用于数据传输。



1. 一种数据传输的方法,其特征在于,包括:

接收通信请求端发送的数据传输请求消息,所述数据传输请求消息中包括第一载荷、以及通信对端的识别信息;

判断所述数据传输请求消息中是否包含第一校验字段,所述第一校验字段是利用所述通信请求端根据所述第一载荷和通信请求端的校验码并通过预设校验算法计算得到的;

若所述数据传输请求消息还包括第一校验字段,确定所述第一校验字段是利用所述第一载荷和通信请求端的校验码并通过预设校验算法计算得到的;

将所述第一载荷转发给所述通信对端。

2. 根据权利要求1所述的数据传输的方法,其特征在于,所述方法还包括:

若所述数据传输请求消息不包括第一校验字段,或者,所述第一校验字段不是利用所述第一载荷和通信请求端的校验码并通过预设校验算法计算得到的,则拒绝所述通信请求端的数据传输请求。

3. 一种会话边界控制器,其特征在于,包括:

接收单元,用于接收通信请求端发送的数据传输请求消息,所述数据传输请求消息中包括第一载荷、以及通信对端的标识信息;

判断单元,用于判断所述数据传输请求消息中是否包含第一校验字段,所述第一校验字段是利用所述通信请求端根据所述第一载荷和通信请求端的校验码并通过预设校验算法计算得到的;

确定单元,用于若所述数据传输请求消息包括第一校验字段,确定所述第一校验字段是利用所述第一载荷和通信请求端的校验码并通过预设校验算法计算得到的;

转发单元,用于将所述第一载荷转发给所述通信对端。

4. 根据权利要求3所述的会话边界控制器,其特征在于,还包括:

拒绝单元,用于若所述数据传输请求消息不包括第一校验字段则拒绝所述通信请求端的数据传输请求,或者若所述第一校验字段不是利用所述第一载荷和通信请求端的校验码并通过预设校验算法计算得到的,则拒绝所述通信请求端的数据传输请求。

数据传输的方法及装置

技术领域

[0001] 本发明涉及通信技术领域,尤其涉及数据传输的方法及装置。

背景技术

[0002] 随着网络技术的不断发展,运用网络技术实现各种数据的传输已经成为人们生活、工作中不可或缺的一部分。

[0003] 随着VoIP(Voice over Internet Product,将模拟声讯号数字化)技术的不断发展,RTP(实时传输协议,Real-time Transport Protocol)在宽带网络媒体数据传输过程中得到广泛运用。同时,数据传输时数据通道的安全问题也逐渐被人们所重视。然而,现有VoIP组网存在些安全漏洞,企业存在机密信息外泄的可能。

[0004] 在终端A和终端B之间的数据传输过程中,终端A与终端B发起的信令协商过程都是标准流程,在该标准流程中,终端与会话初始协议(SIP,Session Initiation Protocol)服务器之间传输的每条信令的格式及内容,都是本领域里人们所熟知的,所以,利用现有软件技术很容易实现构造上述信令协商过程,包括注册协商、呼叫协商等过程比如利用非法软件同样在SIP服务器下信令协商成功,从而创建非法的数据通道,利用SIP服务器传输非法数据。

发明内容

[0005] 本发明的实施例提供一种数据传输的方法及装置,以提高数据传输的安全性。

[0006] 为达到上述目的,

[0007] 本发明一方面提供了一种建立数据传输通道的方法,包括:接收第一终端发送的第一认证请求消息,所述第一认证请求消息中包含所述第一终端的标识信息,以及第二终端的识别信息;确定所述第一终端的标识信息与预先存储的第一终端的验证信息相匹配;根据所述第二终端的识别信息获取存储的第二终端的验证信息;根据所述第二终端的识别信息向所述第二终端发送携带第二终端的验证信息的第二认证请求消息;以便于第二终端确认所述第二认证请求消息中的第二终端的验证信息与第二终端的标识信息相匹配,并返回认证通过响应消息;在收到所述第二终端返回的认证通过响应消息后,建立第一终端和第二终端之间的数据传输通道。

[0008] 本发明另一方面提供了一种数据传输的方法,包括:接收通信请求端发送的数据传输请求消息,所述数据传输请求消息中包含加密载荷、以及通信对端的识别信息;根据存储的通信请求端的校验码和预设的解密算法从所述加密载荷中解密出第一载荷;根据所述通信对端的识别信息将所述第一载荷转发给所述通信对端。

[0009] 本发明再一方面提供了一种数据传输的方法,包括:

[0010] 接收通信请求端发送的数据传输请求消息,所述数据传输请求消息中包括第一载荷、以及通信对端的识别信息;判断所述数据传输请求消息中是否包含第一校验字段,所述第一校验字段是利用所述通信请求端根据所述第一载荷和通信请求端的校验码并通过预

设校验算法计算得到的;若所述数据传输请求消息还包括第一校验字段,确定所述第一校验字段是利用所述第一载荷和通信请求端的校验码并通过预设校验算法计算得到的;将所述第一载荷转发给所述通信对端。

[0011] 本发明又一方面提供了一种SIP服务器,包括:第一接收单元,用于接收第一终端发送的第一认证请求消息,所述第一认证请求消息中包含所述第一终端的标识信息,以及第二终端的识别信息;第一确定单元,用于确定所述第一终端的标识信息与预先存储的第一终端的验证信息相匹配;第一发送单元,用于根据所述第二终端的识别信息获取存储的第二终端的验证信息;根据所述第二终端的识别信息向所述第二终端发送携带第二终端的验证信息的第二认证请求消息;以便于第二终端确认所述第二认证请求消息中的第二终端的验证信息与第二终端的标识信息相匹配,并返回认证通过响应消息;建立单元,用于在收到所述第二终端返回的认证通过响应消息后,建立第一终端和第二终端之间的数据传输通道。

[0012] 本发明又一方面提供了一种会话边界控制器,包括:

[0013] 接收单元,用于接收通信请求端发送的数据传输请求消息,所述数据传输请求消息中包含加密载荷、以及通信对端的识别信息;解密单元,用于根据存储的通信请求端的校验码和预设的解密算法从所述加密载荷中解密出第一载荷;转发单元,用于根据所述通信对端的识别信息将所述第一载荷转发给所述通信对端。

[0014] 本发明又一方面提供了一种会话边界控制器,包括:接收单元,用于接收通信请求端发送的数据传输请求消息,所述数据传输请求消息中包括第一载荷、以及通信对端的标识信息;判断单元,用于判断所述数据传输请求消息中是否包含第一校验字段,所述第一校验字段是利用所述通信请求端根据所述第一载荷和通信请求端的校验码并通过预设校验算法计算得到的;确定单元,用于若所述数据传输请求消息包括第一校验字段,确定所述第一校验字段是利用所述第一载荷和通信请求端的校验码并通过预设校验算法计算得到的;第二转发单元,用于将所述第一载荷转发给所述通信对端。

[0015] 本发明又一方面提供了一种数据传输的系统,包括:如上所述的SIP服务器以及如上所述的会话边界控制器。

[0016] 本发明又一方面提供了一种数据传输的系统,包括:如上所述的建立数据传输通道的方法及如上所述的数据传输方法。

[0017] 本发明实施例提供的建立数据传输通道的方法、SIP服务器、会话边界控制器,以及数据传输的方法和系统,由于,SIP服务器中预先存储有用于验证终端的验证信息,SIP服务器在终端之间建立数据传输通道之前,对进行数据传输的终端的合法性进行验证,只有在确定通信请求端是合法的终端时,才在通信请求端和通信对端之间建立数据传输通道,降低了非法终端与SIP服务器非法协商建立数据传输通道的风险。

[0018] 对于包含种会话边界控制器SBC的数据传输系统,SBC根据预设的解密算法对加密载荷进行解密,解密出第一载荷,将解密出的第一载荷转发给通信对端,只有合法的通信请求端发送的载荷才能够被正确的转发给通信对端,对于非法的通信请求端的数据传输请求,由于通信请求端预先无法知道预设的加密算法,因此非法的通信请求端不能够对载荷进行正确的加密,非法通信请求端的载荷在经过SBC的解密后,解密出的载荷一定不是通信请求端所希望传输给通信对端的载荷,而通常会是一些乱码,因此,能够有效的减小非法通

信请求端模拟数据通道进行非法数据传输的风险。

[0019] 或者,SBC在将通信请求端的第一载荷转发给通信对端之前,需要判断通信请求端的数据传输请求中是否包含用于对通信请求端进行验证的第一校验字段,在通信请求端的数据传输请求中包含第一校验字段,并且第一校验字段正确的情况下,SBC才将通信请求端的第一载荷转发给通信对端,因此,能够有效的减小非法通信请求端模拟数据通道进行非法数据传输的风险。

附图说明

[0020] 为了更清楚地说明本发明实施例中的技术方案,下面将对实施例描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0021] 图1为本发明实施例提供的建立数据传输通道的方法的流程图;

[0022] 图2为本发明实施例提供的另一建立数据传输通道的方法的流程图;

[0023] 图3为本发明实施例提供的又一建立数据传输通道的方法的流程图;

[0024] 图4为本发明实施例提供的再一建立数据传输通道的方法的流程图;

[0025] 图5为本发明实施例提供的SIP服务器的结构图;

[0026] 图6为本发明实施例提供的另一SIP服务器的结构图;

[0027] 图7为本发明实施例提供的会话边界控制器的结构图;

[0028] 图8为本发明实施例提供的另一会话边界控制器的结构图;

[0029] 图9为本发明实施例提供的数据传输的系统的结构图。

具体实施方式

[0030] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0031] 本发明实施例提供了一种建立数据传输通道的方法,如图1所示,包括以下步骤:

[0032] 101、SIP服务器接收第一终端发送的第一认证请求消息,第一认证请求消息中包含第一终端的标识信息,以及第二终端的识别信息。

[0033] 第一终端在与第二终端进行数据传输之前,首先,第一终端向SIP服务器发送第一认证请求消息,请求SIP服务器对该第一终端的合法性进行认证。为了给SIP服务器提供认证依据,第一认证请求消息中包含第一终端的标识信息。

[0034] 所述第一终端的标识信息可以是终端的国际移动用户识别码(International Mobile Subscriber Identity,简称IMSI),也可以仅仅是终端的序列号(SNR),还可以是终端的其它标识。此外,所述第一终端的标识信息采用第一终端与服务器约定的函数封装,还可以是现有的其它函数,本发明在些不做明确限制。所述第二终端的识别信息通常可以为第二终端的路由信息,如第二终端的号码等。

[0035] 关于第一终端和第二终端,本发明实施例中的第一终端和第二终端可以是手机、

PC机(个人计算机)、便携式计算机等。

[0036] 102、SIP服务器确定第一终端的标识信息与预先存储的第一终端的验证信息相匹配。

[0037] 在接收到第一终端的认证请求消息后,SIP服务器从第一认证请求消息中获取第一终端的标识信息,通过该第一终端的标识信息对该第一终端进行认证。

[0038] 关于第一终端的验证信息,在SIP服务器中预先存储所有该SIP服务器提供服务的终端的标识信息的验证信息,该验证信息与终端的标识信息满足预设的对应关系,本实施例中第一终端的验证信息即为第一终端的验证信息。第一终端的标识信息即为第一终端的标识信息。

[0039] 验证信息与终端的标识信息之间预设的对应关系,可以根据需要而设置,例如,可以将验证信息和标识信息设置为相同,即,本实施例中将第一终端的第一终端的验证信息与第一终端的标识信息设置成相同。为了进一步提供数据传输通道的安全性,可以使验证信息与标识信息满足一个预设的函数关系,验证信息可以是标识信息加1,也可以是标识信息的乘方,本实施例中将第一终端的验证信息设置为标识信息加1,也可以设置为标识信息的乘方。对于终端的验证信息与标识信息的预设关系可以是本领域技术人员所熟知的其它任何对应关系,在此不再赘述。

[0040] 103、SIP服务器根据第二终端的识别信息获取存储的第二终端的验证信息;根据第二终端的识别信息向第二终端发送携带第二终端的验证信息的第二认证请求消息;以便于第二终端确认第二认证请求消息中的第二终端的验证信息与第二终端的标识信息相匹配,并返回认证通过响应消息。

[0041] 若第一终端的标识信息与预先存储的第一终端的验证信息相匹配,则表明第一终端的是合法的,可以通过SIP服务器进行数据通信。于是,SIP服务器向第二终端发送第二认证请求消息,第二终端就是第一终端请求建立数据传输通道的通信对端。

[0042] 104、SIP服务器在收到第二终端返回的认证通过响应消息后,建立第一终端和第二终端之间的数据传输通道。

[0043] 第二终端在接收到SIP服务器发送的第二认证请求消息后,会从该第二认证请求消息中获取第二终端的验证信息,并将获取的第二终端的验证信息与该第二终端的第二终端的标识信息进行匹配,若匹配成功,则向SIP服务器发送认证通过响应消息,若匹配失败,则第二终端拒绝与第一终端建立数据传输通道。

[0044] 本发明实施例提供的建立数据传输通道的方法,SIP服务器接收第一终端发送的第一认证请求消息,第一认证请求消息中包含第一终端的标识信息,SIP服务器对第一终端的合法性进行验证,即:SIP服务器根确定预先存储的第一终端的验证信息与第一终端的标识信息匹配,若第一终端的验证信息与第一终端的标识信息匹配,则SIP服务器可以确认第一终端是合法用户,在第一终端和第二终端之间建立数据传输通道。

[0045] 由于,SIP服务器中预先存储有用于验证终端的验证信息,SIP服务器在终端之间建立数据传输通道之前,对进行数据传输的终端的合法性进行验证,只有在确定通信请求端是合法的终端时,才在通信请求端和通信对端之间建立数据传输通道,降低了非法终端与SIP服务器非法协商建立数据传输通道的风险。

[0046] 作为本实施例的一种改进,本发明实施例提供另一种建立数据传输通道的方法,

如图2所示,包括以下步骤:

[0047] 201、SIP服务器接收第一终端发送的第一认证请求消息,第一认证请求消息中包含第一终端的标识信息、第一校验码、以及第一终端和第二终端的识别信息。

[0048] 所述第一校验码为第一终端随机生成的,与第一终端的标识信息共同采用第一终端与服务器约定的第一算法封装,如MD5算法,还可以是现有的其它算法,本发明在些不做明确限制。

[0049] 为了进一步验证终端的合法性,还要对终端进行鉴权。如第一校验码M就是用于在对终端的鉴权过程中,在终端向SIP服务器发起数据传输通道建立时,由发起请求的第一终端随机生成。

[0050] 本实施例中,第一终端在第一认证请求消息中携带的第一终端的标识信息和第一校验码采用现有的且与SIP服务器协商好函数封装,如 $Z1(SN1, M1)$,其中,SN1为第一终端的序列号,M1为第一校验码。SIP服务器接收到该第一认证请求消息后,将第一终端的识别信息如第一终端的号码,第一终端的校验码,第二终端的识别信息如第二终端的号码对应存储。

[0051] 进一步可选地,本发明实施例中的第一终端和第二终端可以在同一个网络区域内,也可以分别在不同的网络区域内。

[0052] 202、SIP服务器从第一认证请求消息中获取第一终端的标识信息。

[0053] 为了对第一终端进行认证,在接收到第一终端的认证请求消息后,SIP服务器从第一认证请求消息中获取第一终端的标识信息。

[0054] 本实施例中,SIP服务器对第一认证请求消息进行解析,从中解析出第一认证请求消息携带的 $Z1(SN1, M1)$,进一步从 $Z1(SN1, M1)$,中解析出第一终端的标识信息SN1。

[0055] 203、SIP服务器确定第一终端的标识信息与预先为第一终端存储的第一终端的验证信息是否相匹配。

[0056] 在SIP服务器中预先存储所有该SIP服务器提供服务的终端的标识信息的验证信息以及与所有终端的识别信息如终端的号码的对应关系,该验证信息与终端的标识信息满足预设的对应关系,验证信息与终端的标识信息之间预设的对应关系,可以根据需要而设置,例如,可以将验证信息和标识信息设置为相同,即,本实施例中将第一终端的验证信息与第一终端的标识信息设置成相同。为了进一步提供数据传输通道的安全性,可以使验证信息与标识信息满足一个预设的函数关系,验证信息可以是标识信息加1,也可以是标识信息的乘方,本实施例中将第一终端的验证信息设置为第一终端的标识信息加1,也可以设置为第一终端的标识信息的乘方。对于终端的验证信息与标识信息的预设关系可以是本领域技术人员所熟知的其它任何对应关系,在此不再赘述。

[0057] 本实施例中,以SIP服务器内预存的每个终端的验证信息与该终端的标识信息相同为例,第一终端的验证信息即为第一终端的验证信息。SIP服务器将第一终端的标识信息SN1同第一终端的验证信息进行比较,SIP服务器根据第一终端的识别信息获取第一终端的验证信息,进而判断第一终端的标识信息与第一终端的验证信息是否相同,若相同,则执行步骤204;若不同,则执行步骤218。

[0058] 204、SIP服务器向第一终端发送认证确认消息。

[0059] 第一终端通过SIP服务器的认证后,SIP服务器向第一终端发送认证确认消息。

[0060] 205、第一终端向SIP服务器发起会话请求消息invite-sdp。

[0061] 206、SIP服务器向第一终端发送第一认证字段,第一认证字段是利用第一校验码及SIP服务器产生的第一随机数并通过预设的第一算法计算得到的,为了便于第一终端利用存储的第一校验码及预设的第一算法获取第一认证字段中的第一随机数,并在发给SIP服务器的鉴权请求消息中携带获取到的第一随机数。

[0062] 为了进一步确认第一终端的合法性,SIP服务器通知第一终端发起鉴权流程,SIP服务器同时向第一终端发送第一认证字段。

[0063] 所述第一认证字段,是利用第一校验码、及SIP服务器产生的第一随机数并通过预设的第一算法计算得到的。例如,可以是第一校验码、SIP服务器产生的第一随机数经MD5算法计算生成一个nonce值,对于本领域技术人员所熟知的其它用于计算nonce值的算法,同样适用本发明实施例,在此不再赘述。

[0064] 本实施例中,SIP服务器在鉴权请求消息中携带第一认证字段,由头域proxy-Authenticate携带nonce值,该nonce值利用MD5算法并对服务器产生的随机数计算得到,并使用M1加密生成。

[0065] 第一校验码是在认证过程中由第一终端发送给SIP服务器的,因此,只有第一终端和SIP服务器能够获知该第一校验码,非法客户端无法获取该第一校验码。

[0066] 207、SIP服务器接收第一终端发送的鉴权请求消息,鉴权请求消息中携带第一终端从第一认证字段中获取的第一随机数。

[0067] 第一终端在接收到SIP服务器的第一认证字段后,利用存储于本地的M1以及与预设的第一算法MD5算法获得服务器生成的第一随机数作为第一认证信息responsew值,并将第一认证信息携带在鉴权请求消息中发送给SIP服务器。

[0068] 第一终端重新发起会话Invite请求,附带Proxy-Authorization鉴权请求消息,并在该鉴权请求消息中携带response值,用于作为SIP服务器判断该第一终端合法性的依据,关于response值的其它计算方式和方法,可以是本领域技术人员来说是熟知的其它算法,在此不再赘述。

[0069] 208、SIP服务器确定鉴权请求消息中携带的第一终端从第一认证字段中获取的第一随机数与SIP服务器产生的第一随机数相同。

[0070] 对于SIP服务器所服务的终端,若SIP服务器确定鉴权请求消息中携带的第一终端从第一认证字段中获取的第一随机数与SIP服务器产生的第一随机数相同,则执行步骤209。否则,则执行步骤218。

[0071] 209、SIP服务器根据识别信息向第二终端发送第二认证请求消息,第二认证请求消息中包含SIP服务器随机生成的第二校验码、以及为第二终端预设的第二终端的验证信息。

[0072] 若第一终端的标识信息与预先存储的第一终端的验证信息相匹配,则表明第一终端的是合法的,第一终端可以通过SIP服务器与第二终端进行数据通信。于是,SIP服务器根据识别信息确认第二终端的地址,并根据该地址向第二终端发送第二认证请求消息,第二终端就是第一终端请求建立数据传输通道的通信对端。

[0073] 所述第二认证请求消息,该第二认证请求消息中可以包含预先存储的第二终端的

验证信息,第二终端的验证信息与第二终端的第二终端的标识信息满足预设的对应关系。终端验证信息与终端的标识信息之间预设的对应关系,可以根据需要而设置,例如,可以将验证信息和标识信息设置为相同,即,本实施例中第二终端的验证信息与第二终端的标识信息设置成相同。为了进一步提供数据传输通道的安全性,可以使验证信息与标识信息满足一个预设的函数关系,验证信息可以是标识信息加1,也可以是标识信息的乘方,本实施例中第二终端的第二验证信息设置为第二标识信息加1,也可以设置为第二标识信息的乘方。对于终端的验证信息与标识信息的预设关系可以是本领域技术人员所熟知的其它任何对应关系,在此不再赘述。

[0074] 所述第二终端的标识信息可以是终端的国际移动用户识别码(IMSI),也可以仅仅是终端的序列号(SNR),还可以是终端的其它标识。此外,所述第二终端的标识信息采用第二终端与服务器约定的函数封装,还可以是现有的其它函数,本发明在些不做明确限制。

[0075] 所述第二校验码为SIP服务器随机生成的,与第二终端的标识信息共同采用第二终端与服务器约定的第一算法封装,如MD5算法,还可以是现有的其它算法,本发明在些不做明确限制。

[0076] 210、第二终端从接收的第二认证请求消息中解析出第二终端的验证信息,对SIP服务器进行认证。

[0077] 第二终端在接收到SIP服务器发送的第二认证请求消息后,会从该第二认证请求消息中获取第二终端的验证信息,并将获取的第二终端的验证信息与该第二终端的标识信息进行匹配,确认第二认证请求消息中的第二终端的验证信息与第二终端的标识信息相匹配,若匹配成功,则第二终端向SIP服务器发送携带第二终端的标识信息的认证通过响应消息,若匹配失败,则第二终端拒绝与第一终端建立数据传输通道。

[0078] 211、SIP服务器接收第二终端发送的认证通过响应消息。

[0079] 212、SIP服务器判断第二终端发送的认证通过响应消息中是否携带第二终端的标识信息。

[0080] 若第二终端发送的认证通过响应消息中携带第二终端的标识信息,则执行步骤213;否则,执行步骤218。

[0081] 213、SIP服务器从第二终端发送的认证通过响应消息中获取该第二终端的标识信息,确定第二终端的标识信息与预先存储的第二终端的验证信息是否相匹配。

[0082] 若匹配,执行步骤214;若不匹配,执行步骤218。

[0083] 214、SIP服务器向第二终端发送第二认证字段,第二认证字段是利用第二校验码及SIP服务器产生的第二随机数并通过预设的第二算法计算得到的,以便于第二终端利用存储的第二校验码及预设的第二算法获取第二认证字段中的第二随机数,并在发给SIP服务器的鉴权请求消息中携带获取到的第二随机数。

[0084] 为了进一步确定第二终端的合法性,SIP服务器向第二终端发起鉴权流程,向第二终端发送第二认证字段。SIP服务器将第二终端的识别信息如第二终端的号码,第二终端的校验码,第一终端的识别信息如第一终端的号码对应存储。

[0085] 关于第二认证字段,是利用第二校验码及SIP服务器产生的第二随机数并通过预设的MD5算法,或SIP服务器与第二终端协商好的现有的其它算法计算得到。例如,可以是第二校验码及SIP服务器产生的第二随机数经MD5算法计算生成一个nonce值,对于本领域技

术人员所熟知的其它用于计算nonce值的算法,同样适用本发明实施例,在此不再赘述。

[0086] 本实施例中,SIP服务器在鉴权请求消息中携带第二认证字段,由头域proxy-Authenticate携带nonce值,该nonce值利用服务器产生的随机数并通过MD5算法计算得到,并使用M1加密生成。

[0087] 第二校验码是在认证过程中由SIP服务器发送给第二终端的,因此,只有第二终端和SIP服务器能够获知该第二校验码,非法终端无法获取该第二校验码,所以非法终端无法通过认证,不能伪造非法数据通道。即使非法客户端获取了第二校验码,但是,由于每次认证过程的校验码都是随机产生的,而不是沿用上次使用的校验码,因此,能够进一步的降低非法用户模拟建立非法数据通道的风险。

[0088] 215、SIP服务器接收第二终端发送的鉴权请求消息,鉴权请求消息中携带第二终端从第二认证字段中获取的第二随机数。

[0089] 第二终端在接收到SIP服务器的第二认证字段后,第二终端利用存储的第二校验码及预设的第二算法获取第二认证字段中的第二随机数,response值,并在发给SIP服务器的鉴权请求消息中携带获取到的第二随机数。

[0090] 第二终端重新发起会话Invite请求,附带Proxy-Authorization鉴权请求消息,并在该响应消息中携带response值,用于作为SIP服务器判断该第二终端合法性的依据,关于response值的其它计算方式和方法,可以是本领域技术人员来说是熟知的其它算法,在此不再赘述。

[0091] 216、SIP服务器确定鉴权请求消息中携带第二终端从第二认证字段中获取的第二随机数与SIP服务器产生的第二随机数相同。

[0092] 若相同,则执行步骤217;若不同,则执行步骤218。

[0093] 217、SIP服务器在第一终端和第二终端之间建立数据传输通道。

[0094] 若鉴权请求消息中携带第二终端从第二认证字段中获取的第二随机数与所述SIP服务器产生的第二随机数相同,可以说明第二终端为合法终端,SIP服务器在第一终端和第二终端之间建立数据传输通道,供第一终端和第二终端进行数据传输使用。

[0095] 218、SIP服务器拒绝在第一终端和第二终端之间建立数据传输通道。

[0096] 若第一终端的标识信息与预先存储的第一终端的验证信息不匹配;或者认证通过响应消息中包含第二终端的第二终端的标识信息,但第二终端的标识信息与预先存储的第二终端的验证信息不匹配;或者鉴权请求消息中携带的第一终端从第一认证字段中获取的第一随机数与SIP服务器产生的第一随机数不同;或者,鉴权请求消息中携带第二终端从第二认证字段中获取的第二随机数与SIP服务器产生的第二随机数不同,则第一终端、第二终端中至少有一方为非法终端,SIP服务器不能为第一终端和第二终端服务,所以,拒绝在第一终端和第二终端之间建立数据传输通道。

[0097] 本实施例中的第一算法、第二算法可以采用同一算法。

[0098] 本实施例提供的建立数据传输通道的方法,SIP服务器接收第一终端发送的第一认证请求消息,第一认证请求消息中包含第一终端的标识信息,SIP服务器对第一终端的合法性进行验证,即:SIP服务器确定预先存储的第一终端的验证信息与第一终端的标识信息匹配,若第一终端的验证信息与第一终端的标识信息匹配,则SIP服务器可以确认第一终端是合法用户,在确认了第一终端为合法用户后,进一步对第一终端进行鉴权认证。

[0099] 在第一终端通过鉴权认证后,根据第二终端的识别信息获取存储的第二终端的验证信息;在收到第二终端返回的认证通过响应消息后,利用第二终端的验证信息对第二终端进行验证,在确认了第二终端为合法一用户后,进一步对第二终端进行鉴权认证,在对第二终端的鉴权认证通过后,在第一终端和第二终端之间建立数据传输通道。

[0100] 在对第一终端和第二终端进行鉴权的流程中,用于鉴权的第一认证字段和第二认证字段都是分别第一校验码或第二校验码,以及SIP服务器产生的随机数经一定的算法计算得到的,由于每次鉴权过程中,SIP产生的随机数均不同,非法终端无法事先获取这个随机数,有效的避免了非法用户获取用于鉴权的数据的风险。

[0101] 由于,SIP服务器中预先存储有用于验证终端的验证信息,SIP服务器在终端之间建立数据传输通道之前,对进行数据传输的终端的合法性进行验证,只有在确定通信请求端是合法的终端时,才在通信请求端和通信对端之间建立数据传输通道,降低了非法终端与SIP服务器非法协商建立数据传输通道的风险。

[0102] 在有些情况下,为了信息的安全考虑,在第一终端和第二终端之间只能进行RTP流导通,而对于其它网络数据信息进行隔离,则需要在SIP服务器与第一终端或第二终端之间需要设置会话边界控制器(Session Boundary Controller,SBC)。

[0103] 为了提高终端之间所传输的数据的安全性,本发明实施例提供了一种数据传输方法,如图3所示,包括以下步骤:

[0104] 301、SBC接收通信请求终端发送的数据传输请求消息,数据传输消息中包含加密载荷、以及通信对端的识别信息。

[0105] 在包含SBC的网络系统中,终端可以通过SBC进行数据传输的。

[0106] 为了进一步提高终端传输数据的安全性,终端向SBC发送的携带载荷的数据传输请求消息,终端可以对该载荷进行加密操作,将加密后的载荷携带在数据传输请求中,为SBC判断通信请求终端所传输的数据的合法性提供依据。

[0107] 关于加密载荷,加密载荷是终端根据需要传输的第一载荷、以及之前在认证过程中终端与SIP服务器协商的第一校验码经过加密算法计算得到的。

[0108] 本实施例中,若第一终端是通信请求终端,采用现有的且与SIP服务器协商好函数封装,在第一终端携带的加密载荷可以是 $Ls(1, M1)$,其中, Ls 为加密载荷, 1 为第一终端希望传输给通信对端的第一载荷, $M1$ 为在认证协商过程中终端与SIP服务器协商的第一校验码。

[0109] 关于加密算法,终端与SBC之间,为了对终端的合法性进行确认,在终端预先存储预设加密算法,在SBC上预先存储有该加密算法的解密算法。

[0110] 302、SBC根据存储的通信请求端的校验码和预设的解密算法从加密载荷中解密出第一载荷。

[0111] SBC接收的通信请求终端发送的数据传输请求后,通过预先存储的解密算法,从数据传输请求消息中解析出第一载荷。

[0112] 关于通信请求端的校验码,可以在数据通道建立阶段,在认证过程中,由SIP服务器随机生成,或者由通信请求端在发起数据通道建立流程时,由通信请求端随机生成。

[0113] 303、SBC根据存储的通信对端的校验码和预设的加密算法对第一载荷进行加密。

[0114] 为了进一步提高输出传输的合法性,SBC根据存储的通信对端的校验码和预设的加密算法对第一载荷进行加密。只有接收到加密后的第一载荷的第二终端为合法用户时,

第二终端才能够正确的活动第一载荷,若第二终端为非法用户,则第二终端无法正确的解密出第一载荷,进一步,提高了数据传输的安全性。

[0115] 304、SBC根据所述通信对端的识别信息将所述第一载荷转发给所述通信对端。

[0116] 在采用上述方案进行终端的数据传输时,如果非法终端通过伪造的方式构造数据传输消息进行传输,当数据传输消息到达SBC后,SBC将无法对其解密成功,从而丢弃该数据传输消息,避免非法终端盗用合法终端建立的数据传输通道。

[0117] 即使有部分非法数据传输消息能够被SBC解密成功,但是,由于经过解密操作后的数据已经被破坏,非法终端的通信对端也无法还原出非法通信请求终端所发送的数据。所以,通过在数据传输过程中,对载荷进行加密和解密操作可以保证数据传输的安全性,降低终端之间的数据通道被盗用的风险。

[0118] 对于包含SBC的数据传输系统,SBC根据预设的解密算法对加密载荷进行解密,解密出第一载荷,将解密出的第一载荷转发给通信对端,只有合法的通信请求端的载荷才能够被正确的转发给通信对端,对于非法的通信请求端的数据传输请求,由于通信请求端预先无法知道预设的加密算法,因此非法的通信请求端不能够对载荷进行正确的加密,非法通信请求端的载荷在经过SBC的解密后,解密出的载荷一定不是通信请求端所希望传输给通信对端的载荷,而通常会是一些乱码,因此,能够有效的减小非法通信请求端模拟数据通道进行非法数据传输的风险。

[0119] 为了提高数据传输过程中,被传输数据的安全性,本实施例提供了另一种数据传输方法,包括以下步骤:

[0120] 401、SBC接收通信请求终端发送的携带载荷的数据传输请求消息,数据传输请求消息中包含第一载荷、以及通信对端的识别信息。

[0121] 为了进一步提高终端传输数据的安全性,终端向SBC发送的携带第一载荷的数据传输请求消息,终端可以在数据传输请求消息中携带第一校验字段和通信请求终端的标识信息。该第一校验字段可以做为SBC判断通信请求终端所传输的数据的合法性提供依据。

[0122] 402、SBC判断数据传输请求消息中是否包含第一校验字段,第一校验字段是利用通信请求端根据第一载荷和通信请求端的校验码并通过预设校验算法计算得到的。

[0123] SBC接收的通信请求终端发送的数据传输请求后,从数据传输请求消息中解析出第一载荷、和通信请求终端的标识信息。若所述数据传输请求消息还包括第一校验字段,执行步骤403,否则执行步骤406。

[0124] 关于通信请求端的校验码,可以在数据通道建立阶段,在认证过程中,由SIP服务器随机生成,或者由通信请求端在发起数据通道建立流程时,由通信请求端随机生成。

[0125] 403、SBC根据第一载荷和通信请求终端的校验码通过预设校验算法计算一个校验字段。

[0126] 404、SBC确定第一校验字段是利用第一载荷和通信请求端的校验码并通过预设校验算法计算得到的。

[0127] SBC将第一校验字段和计算出的校验字段相比较,判断第一校验字段和计算出的校验字段是否相同。

[0128] 若第一校验字段和计算出的校验字段相同,则执行步骤405;若第一校验字段和计算出的校验字段不同,则执行步骤406。

[0129] 405、SBC根据通信对端的识别信息将第一载荷转发给通信对端。

[0130] 406、SBC拒绝为通信请求终端传送该第一载荷。

[0131] 采用在数据传输消息中增加校验字段的方案进行终端的数据传输时,如果非法终端通过伪造的方式构造数据传输消息进行传输,当数据传输消息到达SBC后,SBC将无法对校验字段验证成功,从而拒绝为该非法终端传输数据,丢弃该数据传输消息,避免非法终端盗用合法终端建立的数据传输通道。

[0132] 即使有部分非法数据传输消息恰巧能够被SBC校验成功,但是,由于经过校验字段的解析将通信请求终端发送的数据已经被破坏,非法终端的通信对端也无法还原出非法通信请求终端所发送的数据。所以,通过在数据传输过程中,在数据传输消息中携带校验字段可以保证数据传输的安全性,降低终端之间的数据通道被盗用的风险。

[0133] SBC在将通信请求端的第一载荷转发给通信对端之前,需要判断通信请求端的数据传输请求中是否包含用于对通信请求端进行验证的第一校验字段,在通信请求端的数据传输请求中包含第一校验字段,并且第一校验字段正确的情况下,SBC才将通信请求端的第一载荷转发给通信对端,因此,能够有效的减小非法通信请求端模拟数据通道进行非法数据传输的风险。

[0134] 本发明实施例提供了一种SIP服务器,如图5所示,包括:第一接收单元51、第一确定单元52、第一发送单元53、建立单元54。

[0135] 其中,第一接收单元51,用于接收第一终端发送的第一认证请求消息,第一认证请求消息中包含第一终端的标识信息,以及第二终端的识别信息;

[0136] 第一确定单元52,用于确定第一终端的标识信息与预先存储的第一终端的验证信息相匹配;

[0137] 第一发送单元53,用于根据第二终端的识别信息获取存储的第二终端的验证信息;根据第二终端的识别信息向第二终端发送携带第二终端的验证信息的第二认证请求消息;以便于第二终端确认第二认证请求消息中的第二终端的验证信息与第二终端的标识信息相匹配,并返回认证通过响应消息;

[0138] 建立单元54,用于在收到第二终端返回的认证通过响应消息后,建立第一终端和第二终端之间的数据传输通道。

[0139] 本实施例提供的SIP服务器,SIP服务器接收第一终端发送的第一认证请求消息,第一认证请求消息中包含第一终端的标识信息,SIP服务器对第一终端的合法性进行验证,即:SIP服务器根据预先存储的第一终端的验证信息与第一终端的标识信息匹配,若第一终端的验证信息与第一终端的标识信息匹配,则SIP服务器可以确认第一终端是合法用户,根据第二终端的识别信息获取存储的第二终端的验证信息;根据第二终端的识别信息向第二终端发送携带第二终端的验证信息的第二认证请求消息;在收到第二终端返回的认证通过响应消息后,在第一终端和第二终端之间建立数据传输通道。

[0140] 由于,SIP服务器中预先存储有用于验证终端的验证信息,SIP服务器在终端之间建立数据传输通道之前,对进行数据传输的终端的合法性进行验证,只有在确定通信请求终端是合法的终端时,才在通信请求终端和通信对端之间建立数据传输通道,降低了非法终端与SIP服务器非法协商建立数据传输通道的风险。

[0141] 作为本实施例的一种改进,本发明实施例提供另一种SIP服务器,如图6所示,包

括：第一接收单元51、第一确定单元52、第二发送单元61、第二接收单元62、第二确定单元63、第三确定单元64、第一发送单元53、第三发送单元65、第三接收单元66、第四确定单元67、建立单元54、拒绝单元68。

[0142] 其中，第一接收单元51，用于接收第一终端发送的第一认证请求消息，第一认证请求消息中包含第一终端的标识信息，以及第二终端的识别信息。

[0143] 第一终端在与第二终端进行数据通信，需要向SIP服务器发送第一认证请求消息，请求SIP服务器对该第一终端的合法性进行认证。为了给SIP服务器提供认证依据，第一认证请求消息中包含第一终端的标识信息。为了使SIP服务器能够确定通信对端，同时携带了作为通信对端的第二终端的识别信息。

[0144] 关于第一终端的标识信息，用于标识第一终端。为了实现终端识别，为每个终端设置一个唯一的标识信息，该标识信息可以在终端出厂时设置，由于不是明码，因此，可以减少被非法终端盗用的风险。

[0145] 为了进一步合适终端的合法性，还要对终端进行鉴权，随机生成的第一校验码M用于终端的鉴权过程，该校验码在终端向SIP服务器发起数据传输通道建立时，由发起请求的终端随机生成，或者在SIP服务器向通信对端发起认证时，由SIP服务器产生。

[0146] 第一确定单元52，用于确定第一终端的标识信息与预先存储的第一终端的验证信息相匹配。

[0147] 第二发送单元61，用于向第一终端发送第一认证字段，第一认证字段是利用第一校验码及SIP服务器产生的第一随机数并通过预设的第一算法计算得到；以便于第一终端利用存储的第一校验码及预设的第一算法获取第一认证字段中的第一随机数，并在发给SIP服务器的鉴权请求消息中携带获取到的第一随机数。

[0148] 在SIP服务器中预先存储所有该SIP服务器提供服务的终端的标识信息的验证信息，该验证信息与终端的标识信息满足预设的对应关系。

[0149] SIP服务器获取第一终端的验证信息。SIP判断第一终端的标识信息与第一终端的验证信息是否相匹配。

[0150] 为了进一步确认第一终端的合法性，SIP服务器向第一终端发起鉴权流程，SIP服务器向第一终端发送第一认证字段。

[0151] 第二接收单元62，用于接收所述第一终端发送的鉴权请求消息，所述鉴权请求消息中携带第一终端从第一认证字段中获取的第一随机数。

[0152] 进一步可选地，第一认证信息是由第一认证字段和第一终端的标识信息由第一终端和SIP服务器约定的函数封装。

[0153] 第二确定单元63，用于确定认证通过响应消息中包含第二终端的标识信息，且第二终端的标识信息与预先存储的第二终端的验证信息相匹配。

[0154] 第三确定单元64，用于确定鉴权请求消息中携带的第一终端从第一认证字段中获取的第一随机数与SIP服务器产生的第一随机数相同。

[0155] 第一发送单元53，用于根据第二识别信息向第二终端发送第二认证请求消息。

[0156] 进一步可选地，第二认证请求消息中包含随机生成的第二校验码、以及为第二终端预设的第二终端的验证信息。

[0157] 若第一终端的标识信息与预先存储的第一终端的验证信息相匹配，则表明第一终

端的是合法的,第一终端可以通过SIP服务器进行数据通信,于是,SIP服务器根据识别信息确认第二终端的地址,并根据该地址向第二终端发送第二认证请求消息,第二终端就是第一终端请求建立数据传输通道的通信对端。

[0158] 关于第二认证请求消息,该第二认证请求消息中可以包含预先存储的第二终端的验证信息,第二终端的验证信息与第二终端的第二终端的标识信息相匹配。

[0159] 第三发送单元65,用于向第二终端发送第二认证字段,第二认证字段是利用第二校验码及SIP服务器产生的第二随机数并通过预设的第二算法计算得到的;以便于第二终端利用存储的第二校验码及预设的第二算法获取第二认证字段中的第二随机数,并在发给SIP服务器的鉴权请求消息中携带获取到的第二随机数。

[0160] 在接收到第二终端发送的携带第二认证信息的认证通过响应消息后,SIP服务器需要判断认证通过响应消息中携带的第二随机数是否正确,进而判断第二终端是否为合法的终端。

[0161] 第三接收单元66,用于接收第二终端发送的鉴权请求消息,鉴权请求消息中携带第二终端从第二认证字段中获取的第二随机数。

[0162] 进一步可选地,第二认证信息是利用第二认证字段和第二终端的标识信息并通过第一算法计算得到的。

[0163] 第四确定单元67,用于确定鉴权请求消息中携带第二终端从第二认证字段中获取的第二随机数与所述SIP服务器产生的第二随机数相同。

[0164] 所述建立单元54,用于在收到第二终端返回的认证通过响应消息后,建立第一终端和第二终端之间的数据传输通道。

[0165] 对于SIP服务器所服务的终端,在SIP服务器和其服务的终端之间,预先约定第一算法,所以,SIP服务器可以判断第二认证信息是否是利用第二认证字段通过第一算法计算得到的。

[0166] 进一步可选地,建立单元若所述认证通过响应消息中包含第二终端的标识信息,且第二终端的标识信息与预先存储的第二终端的验证信息相匹配,则建立第一终端和第二终端之间的数据传输通道。

[0167] 拒绝单元68,用于若第一终端的标识信息与预先存储的第一终端的验证信息不匹配;或者认证通过响应消息中包含第二终端的第二终端的标识信息,但第二终端的标识信息与预先存储的第二终端的验证信息不匹配;或者鉴权请求消息中携带的第一终端从第一认证字段中获取的第一随机数与SIP服务器产生的第一随机数不同;或者,鉴权请求消息中携带第二终端从第二认证字段中获取的第二随机数与SIP服务器产生的第二随机数不同,则拒绝建立第一终端和第二终端之间的数据传输通道。

[0168] 本实施例提供的SIP服务器,SIP服务器接收第一终端发送的第一认证请求消息,第一认证请求消息中包含第一终端的第一终端的标识信息,SIP服务器对第一终端的合法性进行验证,即:SIP服务器根确定预先存储的第一终端的验证信息与第一终端的标识信息匹配,若第一终端的验证信息与第一终端的标识信息匹配,则SIP服务器可以确认第一终端是合法用户,根据第二终端的识别信息获取存储的第二终端的验证信息;根据第二终端的识别信息向第二终端发送携带第二终端的验证信息的第二认证请求消息;在收到第二终端返回的认证通过响应消息后,在第一终端和第二终端之间建立数据传输通道。

[0169] 此外,图5以及图6所示的SIP服务器可执行图1和图2所示的对应方法实施例的的具体步骤,本实施例在此不在详述。此外,该SIP服务器可以是计算机等实体设备,各单元执行的相关功能可由计算机的处理器执行。

[0170] 由于,SIP服务器中预先存储有用于验证终端的验证信息,SIP服务器在终端之间建立数据传输通道之前,对进行数据传输的终端的合法性进行验证,只有在确定通信请求终端是合法的终端时,才在通信请求终端和通信对端之间建立数据传输通道,降低了非法终端与SIP服务器非法协商建立数据传输通道的风险。

[0171] 本发明实施例提供了一种会话边界控制器,如图7所示,包括:接收单元71、解密单元72、转发单元73、加密单元74。

[0172] 其中,接收单元71,用于接收通信请求终端发送的携带载荷的数据传输请求消息,数据传输请求消息中包含加密载荷、以及通信对端的识别信息;

[0173] 解密单元72,用于根据存储的通信请求端的校验码和预设的解密算法从加密载荷中解密出第一载荷;

[0174] 转发单元73,用于根据通信对端的识别信息将第一载荷转发给通信对端。

[0175] 进一步可选地,本发明实施例还可以包括:加密单元74,用于根据存储的通信对端的校验码和预设的加密算法对所述第一载荷进行加密。

[0176] 本实施例提供的会话边界控制器,在采用上述方案进行终端的数据传输时,如果非法终端通过伪造的方式构造数据传输消息进行传输,当数据传输消息到达SBC后,SBC将无法对其解密成功,从而丢弃该数据传输消息,避免非法终端盗用合法终端建立的数据传输通道。此外,图7所示的会话边界控制器可执行图3所示的对应方法实施例的的具体步骤,本实施例在此不在详述。此外,该会话边界控制器可以是计算机等实体设备,各单元执行的相关功能可由计算机的处理器执行。

[0177] 即使有部分非法数据传输消息能够被SBC解密成功,但是,由于经过解密操作后的数据已经被破坏,非法终端的通信对端也无法还原出非法通信请求终端所发送的数据。所以,通过在数据传输过程中,对载荷进行加密和解密操作可以保证数据传输的安全性,降低终端之间的数据通道被盗用的风险。

[0178] 本发明实施例提供了另一种会话边界控制器,如图8所示,包括:接收单元81、判断单元82、确定单元83、转发单元84、拒绝单元85。

[0179] 其中,接收单元81,用于接收通信请求终端发送的携带载荷的数据传输请求消息,数据传输请求消息中包含第一载荷、以及通信对端的标识信息;

[0180] 判断单元82,用于判断数据传输请求消息中是否包含第一校验字段,所述第一校验字段是由通信请求端利用第一载荷和通信请求端的校验码并通过预设校验算法计算得到的。

[0181] 确定单元83,用于若数据传输请求消息包括第一校验字段,确定所述第一校验字段是利用所述第一载荷和所述通信请求端的校验码并通过预设校验算法计算得到的。

[0182] 转发单元84,用于将第一载荷转发给所述通信对端。

[0183] 拒绝单元85,用于若所述数据传输请求消息不包括第一校验字段则拒绝所述通信请求端的数据传输请求,或者若所述第一校验字段不是利用所述第一载荷和通信请求端的校验码并通过预设校验算法计算得到的,则拒绝所述通信请求端的数据传输请求。

[0184] 本实施例提供的会话边界控制器,采用在数据传输消息中增加校验字段的方案进行终端的数据传输时,如果非法终端通过伪造的方式构造数据传输消息进行传输,当数据传输消息到达SBC后,SBC将无法对校验字段验证成功,从而拒绝为该非法终端传输数据,丢弃该数据传输消息,避免非法终端盗用合法终端建立的数据传输通道。

[0185] 此外,图8所示的会话边界控制器可执行图4所示的对应方法实施例的具体步骤,本实施例在此不在详述。此外,该会话边界控制器可以是计算机等实体设备,各单元执行的相关功能可由计算机的处理器执行。

[0186] 即使有部分非法数据传输消息恰巧能够被SBC校验成功,但是,由于经过校验字段的解析将通信请求终端发送的数据已经被破坏,非法终端的通信对端也无法还原出非法通信请求终端所发送的数据。所以,通过在数据传输过程中,在数据传输消息中携带校验字段可以保证数据传输的安全性,降低终端之间的数据通道被盗用的风险。

[0187] 本发明实施例提供了一种数据传输的系统,如图9所示,包括:SIP服务器91、会话边界控制器92。

[0188] 其中,SIP服务器91可以是图5或图6提供的任一SIP服务器,其各单元的具体功能可参见上述实施例的介绍;

[0189] 会话边界控制器92可以是图7或图8提供的任一会话边界控制器,其各单元的具体功能可参见上述实施例的介绍。

[0190] 本实施例提供的数据传输的系统,SIP服务器接收第一终端发送的第一认证请求消息,第一认证请求消息中包含第一终端的第一终端的标识信息,SIP服务器对第一终端的合法性进行验证,即:SIP服务器根确定预先存储的第一终端的验证信息与第一终端的标识信息匹配,若第一终端的验证信息与第一终端的标识信息匹配,则SIP服务器可以确认第一终端是合法用户,在第一终端和第二终端之间建立数据传输通道。

[0191] 由于,SIP服务器中预先存储有用于验证终端的验证信息,SIP服务器在终端之间建立数据传输通道之前,对进行数据传输的终端的合法性进行验证,只有在确定通信请求终端是合法的终端时,才在通信请求终端和通信对端之间建立数据传输通道,降低了非法终端与SIP服务器非法协商建立数据传输通道的风险。

[0192] 通过以上的实施方式的描述,所属领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件的方式来实现,当然也可以通过硬件,但很多情况下前者是更佳的实施方式。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品存储在可读取的存储介质中,如计算机的软盘,硬盘或光盘等,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备)执行本发明各个实施例所述的方法。

[0193] 以上所述,仅为本发明的具体实施方式,但本发明的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本发明揭露的技术范围内,可轻易想到变化或替换,都应涵盖在本发明的保护范围之内。因此,本发明的保护范围应所述以权利要求的保护范围为准。

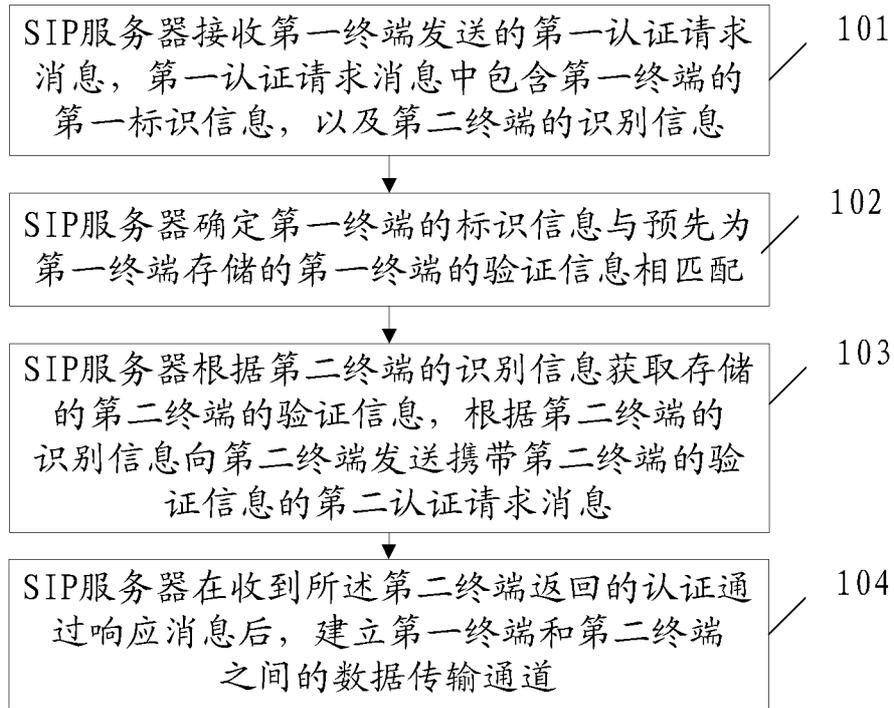


图1

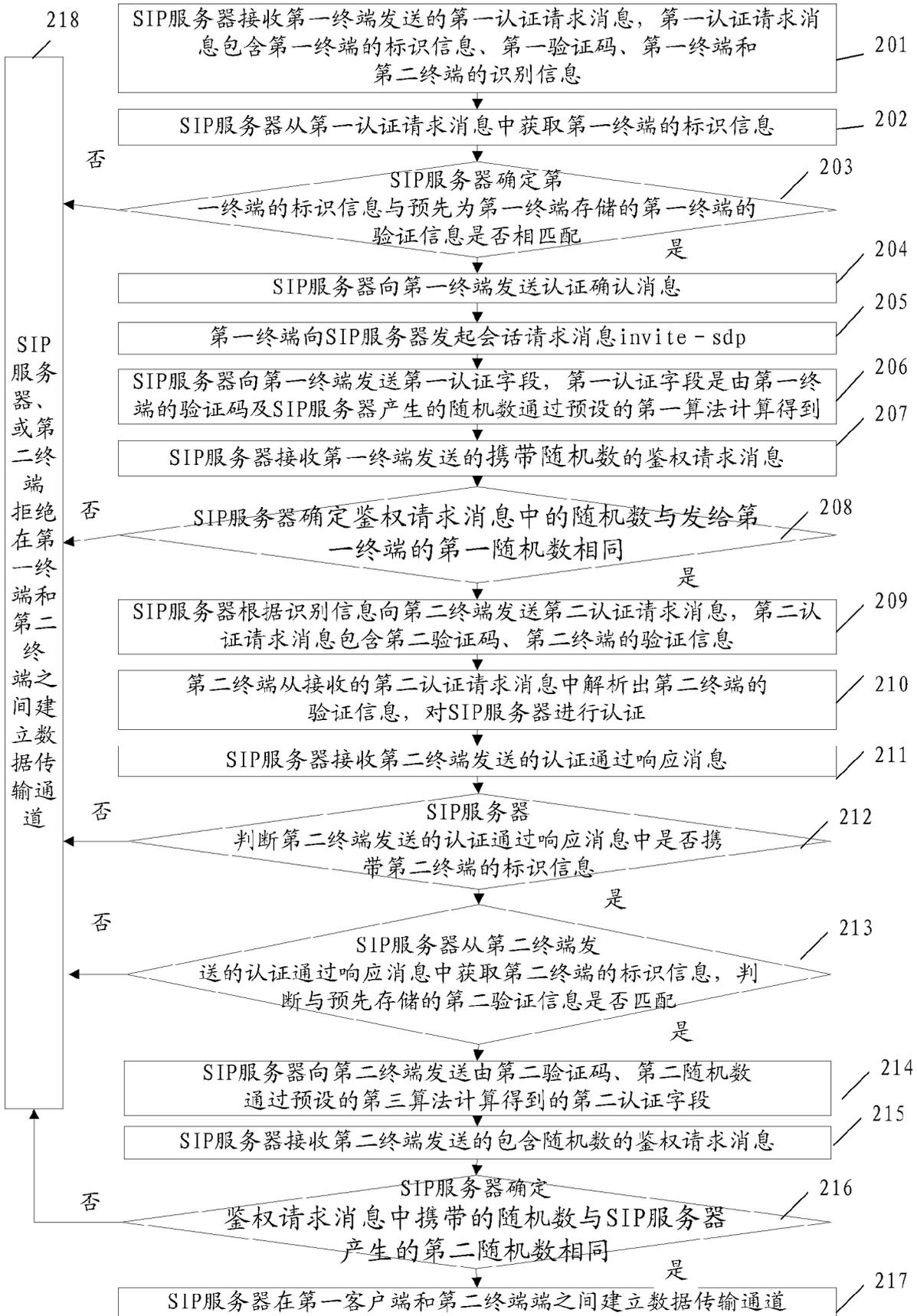


图2

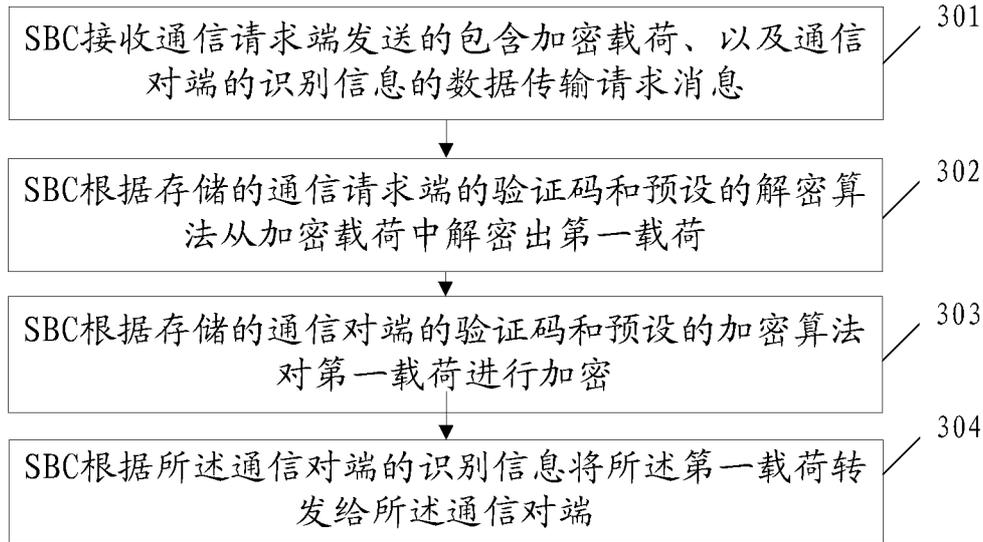


图3

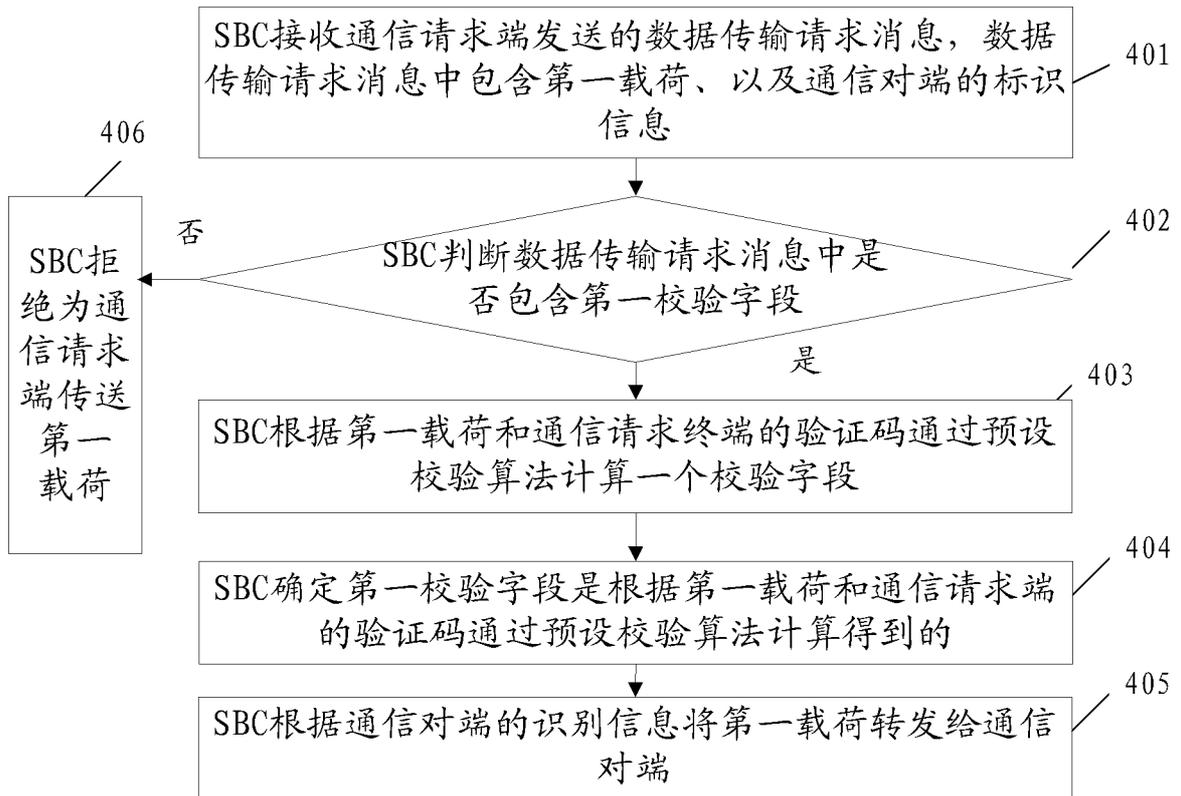


图4

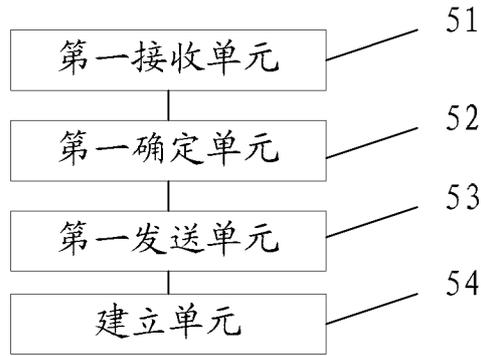


图5

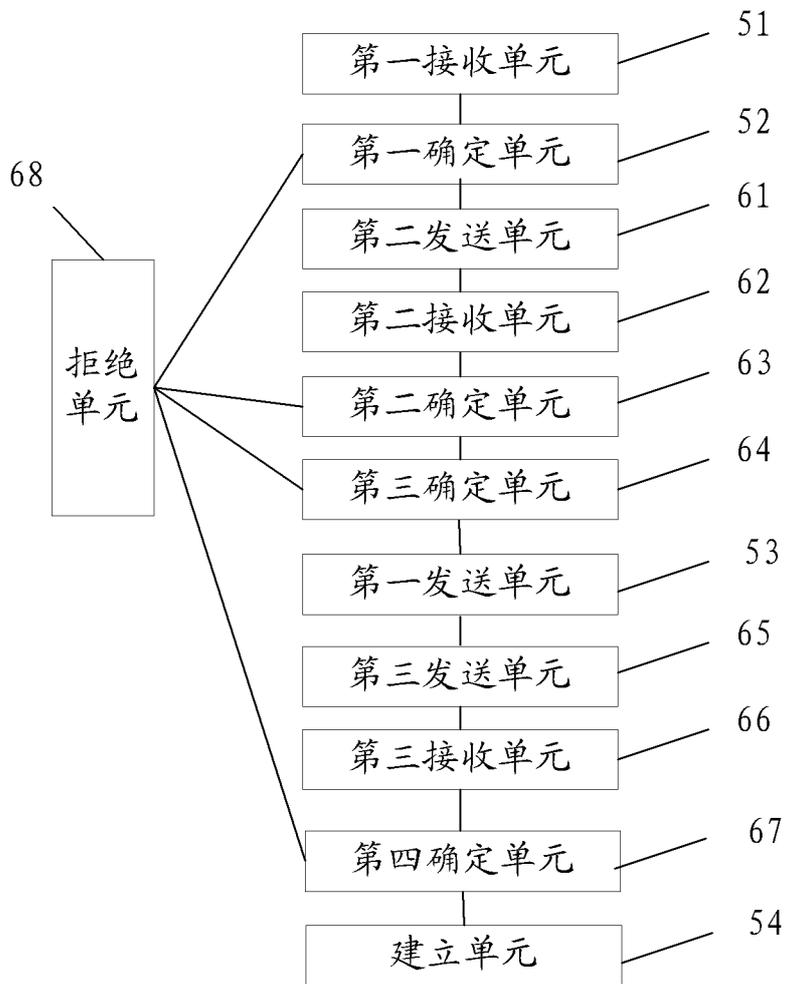


图6

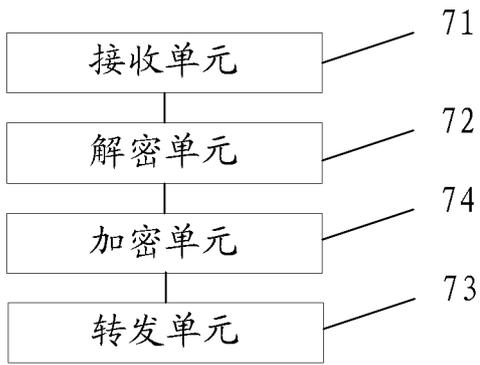


图7

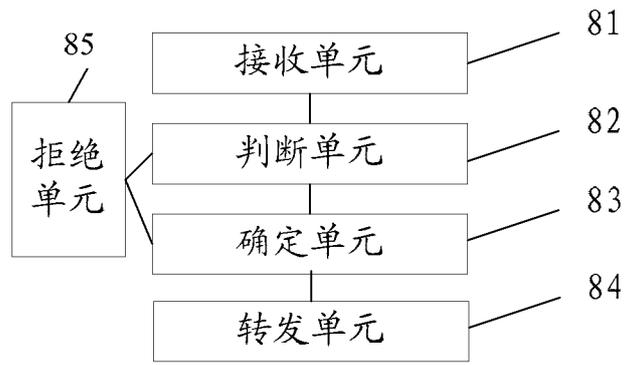


图8

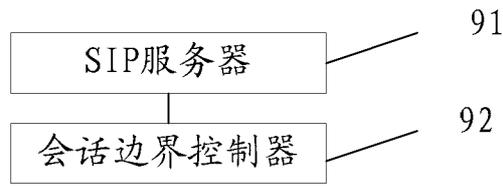


图9