



(12) 发明专利

(10) 授权公告号 CN 102006294 B

(45) 授权公告日 2014. 08. 20

(21) 申请号 201010559798. 5

(22) 申请日 2010. 11. 25

(73) 专利权人 中兴通讯股份有限公司

地址 518057 广东省深圳市南山区科技南路
55 号

(72) 发明人 梁洁辉 施元庆 康望星

(74) 专利代理机构 北京康信知识产权代理有限
责任公司 11240

代理人 余刚 吴孟秋

(51) Int. Cl.

H04L 29/06 (2006. 01)

审查员 张小倩

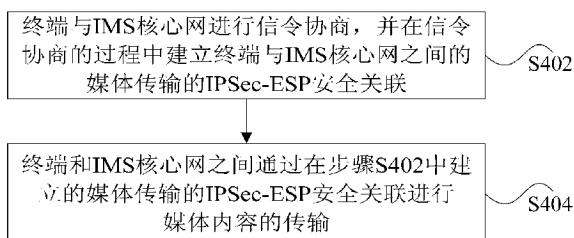
权利要求书4页 说明书7页 附图2页

(54) 发明名称

IMS 多媒体通信方法和系统、终端及 IMS 核心网

(57) 摘要

本发明公开了一种 IMS 多媒体通信方法和系统、终端及 IMS 核心网,其中,IMS 多媒体通信方法包括:终端与 IMS 核心网进行信令协商,并在信令协商的过程中建立终端与 IMS 核心网之间的媒体传输的 IPSec-ESP 安全关联;终端和 IMS 核心网之间通过媒体传输的 IPSec-ESP 安全关联进行媒体内容的传输。本发明确保了终端和 IMS 核心网之间传输的媒体内容的安全性,解决了相关技术中 IMS 下的多媒体通信的安全问题,避免了媒体内容在终端和 IMS 核心网之间进行传输时被他人恶意地盗取和篡改等。



1. 一种 IP 多媒体子系统 IMS 多媒体通信方法,其特征在于,包括:

终端与 IMS 核心网进行信令协商,并在所述信令协商的过程中建立所述终端与所述 IMS 核心网之间的媒体传输的 IP 安全-封装安全负载 IPSec-ESP 安全关联;

所述终端和所述 IMS 核心网之间通过所述媒体传输的 IPSec-ESP 安全关联进行媒体内容的传输;

其中,在终端与 IMS 核心网进行信令协商之前,还包括:所述终端向所述 IMS 核心网进行注册,并在所述注册的过程中建立所述终端与所述 IMS 核心网之间的信令协商的 IPSec-ESP 安全关联;

终端与 IMS 核心网进行信令协商包括:所述终端和所述 IMS 核心网之间通过所述信令协商的 IPSec-ESP 安全关联进行所述信令协商;

其中,所述终端向所述 IMS 核心网进行注册,并在所述注册的过程中建立所述终端与所述 IMS 核心网之间的信令协商的 IPSec-ESP 安全关联包括:

所述终端向所述核心网中的代理型-呼叫会话控制功能 P-CSCF 发送 IMS 注册请求消息,其中,所述 IMS 注册请求消息中包括:所述终端的信息和所述终端的第一安全关联信息;

所述 P-CSCF 保存接收的所述 IMS 注册请求消息中的信息到本地,并向所述终端返回鉴权质询消息,其中,所述鉴权质询消息中包括:第二安全关联信息和所述 P-CSCF 的信息;

所述终端接收所述鉴权质询消息之后,所述终端和所述 P-CSCF 之间通过所述第一安全关联信息和所述 P-CSCF 的第二安全关联信息建立所述信令协商的 IPSec-ESP 安全关联。

2. 根据权利要求 1 所述的方法,其特征在于,所述终端的信息包括:所述终端的 IP 地址、IMS 用户信息和所述终端支持的算法列表;在所述 P-CSCF 保存接收的所述 IMS 注册请求消息中的信息到本地之后以及所述 P-CSCF 向所述终端返回鉴权质询消息之前,还包括:

所述 P-CSCF 获取与所述 IMS 用户信息对应的卡密钥;

所述 P-CSCF 使用所述卡密钥和随机数获得第一认证和密钥协商 AKA 鉴权五元组,其中,所述第一 AKA 鉴权五元组中包括第一完整性密钥 IK、第一加密密钥 CK 和第一响应 RES 字段。

3. 根据权利要求 2 所述的方法,其特征在于,所述鉴权质询消息中还包括:所述第一 RES 字段和所述随机数;在所述终端接收所述鉴权质询消息之后,还包括:

所述终端中的 ISIM 或 USIM 使用本地的卡密钥和所述随机数获得第二 AKA 鉴权五元组,其中,所述第二 AKA 鉴权五元组中包括:第二 IK、第二 CK 和第二 RES 字段;

所述终端判断所述第二 RES 字段与所述第一 RES 字段是否相同;

若判断结果为相同,则所述终端确定所述 P-CSCF 的身份认证成功。

4. 根据权利要求 3 所述的方法,其特征在于,在所述终端和所述 P-CSCF 之间通过所述第一安全关联信息和所述 P-CSCF 的第二安全关联信息建立所述信令协商的 IPSec-ESP 安全关联之后,还包括:

所述终端通过与所述 P-CSCF 的信令协商的 IPSec-ESP 安全关联向所述 P-CSCF 发送 IMS 鉴权验证请求消息,其中,所述 IMS 鉴权验证请求消息中包括:所述终端的信息、所述终端的第一安全关联信息和所述第二 RES 字段;

所述 P-CSCF 接收所述 IMS 鉴权验证请求消息之后,验证所述终端的信息和所述终端的

第一安全关联信息与本地保存的信息是否一致；

若一致，则所述 P-CSCF 继续判断所述第二 RES 字段与所述第一 RES 字段是否相同，并在判断结果为相同的情况下，确定所述终端的身份认证成功以及注册成功；

所述 P-CSCF 向所述终端返回身份认证成功的消息。

5. 根据权利要求 3 所述的方法，其特征在于，所述第一安全关联信息包括：所述终端随机生成的第一安全参数索引 SPI 信息及其对应的端口信息，所述第二安全关联信息包括：所述 P-CSCF 随机生成的第二 SPI 信息及其对应的端口信息，所述 P-CSCF 的信息包括：所述 P-CSCF 的 IP 地址和所述 P-CSCF 支持的算法列表；所述终端和所述 P-CSCF 之间通过所述第一安全关联信息和所述 P-CSCF 的第二安全关联信息建立所述信令协商的 IPSec-ESP 安全关联包括：

所述终端使用所述第一 SPI 信息及其对应的端口信息、所述 P-CSCF 的 IP 地址、所述终端和所述 P-CSCF 均支持的算法、所述第二 IK 和第二 CK 建立与所述 P-CSCF 的信令协商的 IPSec-ESP 安全关联，其中，所述终端和所述 P-CSCF 均支持的算法是从所述终端支持的算法列表以及所述 P-CSCF 支持的算法列表中选择出的；

所述 P-CSCF 使用所述第二 SPI 信息及其对应的端口信息、所述终端的 IP 地址、所述终端和所述 P-CSCF 均支持的算法、所述第一 IK 和第一 CK 建立与所述终端的信令协商的 IPSec-ESP 安全关联。

6. 根据权利要求 5 所述的方法，其特征在于，所述终端和所述 IMS 核心网之间通过所述信令协商的 IPSec-ESP 安全关联进行所述信令协商，并在所述信令协商的过程中建立所述终端与所述 IMS 核心网之间的媒体传输的 IPSec-ESP 安全关联包括：

所述终端向所述 P-CSCF 发送 IMS 会话邀请请求消息，其中，所述 IMS 会话邀请请求消息中包括所述终端的媒体信息和所述终端随机生成的第三 SPI 信息；

所述 P-CSCF 保存接收的所述 IMS 会话邀请请求消息中的信息，将所述 IMS 会话邀请请求消息转发到所述 IMS 会话邀请请求消息所邀请的另一终端；

在所述 P-CSCF 接收到所述另一终端返回的响应消息之后，通知所述核心网中的媒体网控制功能 MGCF 随机生成第四 SPI 信息，并将所述响应消息转发给所述终端，其中，所述响应消息中包括：所述第四 SPI 信息；

所述终端使用所述第三 SPI 信息、所述终端和所述 P-CSCF 均支持的算法、所述第二 IK 和第二 CK 建立与所述 MGCF 的媒体传输的 IPSec-ESP 安全关联；

所述 MGCF 使用所述第四 SPI 信息、所述终端和所述 P-CSCF 均支持的算法、所述第一 IK 和第一 CK 建立与所述终端的媒体传输的 IPSec-ESP 安全关联。

7. 根据权利要求 6 所述的方法，其特征在于，所述终端和所述 IMS 核心网之间通过所述媒体传输的 IPSec-ESP 安全关联进行媒体内容的传输包括：

所述终端使用所述第二 IK、所述第二 CK 以及所述终端和所述 P-CSCF 均支持的算法加密所要发送的媒体内容，并发送加密后的媒体内容到所述 MGCF；以及所述 MGCF 使用所述第一 IK、所述第一 CK 以及所述终端和所述 P-CSCF 均支持的算法解密所述加密后的媒体内容；

或者，所述 MGCF 使用所述第一 IK、所述第一 CK 以及所述终端和所述 P-CSCF 均支持的算法加密要发送到所述终端的媒体内容，并发送加密后的媒体内容到所述终端；以及所述

终端使用所述第二 IK、所述第二 CK、以及所述终端和所述 P-CSCF 均支持的算法解密所述加密后的媒体内容。

8. 一种 IP 多媒体子系统 IMS 多媒体通信系统,其特征在于,包括终端和 IMS 核心网,其中:

所述终端用于与所述 IMS 核心网进行信令协商,并在所述信令协商的过程中建立与所述 IMS 核心网之间的媒体传输的 IP 安全 - 封装安全负载 IPSec-ESP 安全关联,通过所述媒体传输的 IPSec-ESP 安全关联进行所述终端和所述 IMS 核心网之间的媒体内容的传输;

其中,所述终端还用于在与所述 IMS 核心网进行信令协商之前,向所述 IMS 核心网进行注册,并在所述注册的过程中建立与所述 IMS 核心网之间的信令协商的 IPSec-ESP 安全关联,通过所述信令协商的 IPSec-ESP 安全关联与所述 IMS 核心网进行所述信令协商;

其中,所述终端还用于在与所述 IMS 核心网进行信令协商之前,向所述 IMS 核心网进行注册,并在所述注册的过程中建立与所述 IMS 核心网之间的信令协商的 IPSec-ESP 安全关联包括:

所述终端向所述核心网中的代理型 - 呼叫会话控制功能 P-CSCF 发送 IMS 注册请求消息,其中,所述 IMS 注册请求消息中包括:所述终端的信息和所述终端的第一安全关联信息;

所述 P-CSCF 保存接收的所述 IMS 注册请求消息中的信息到本地,并向所述终端返回鉴权质询消息,其中,所述鉴权质询消息中包括:第二安全关联信息和所述 P-CSCF 的信息;

所述终端接收所述鉴权质询消息之后,所述终端和所述 P-CSCF 之间通过所述第一安全关联信息和所述 P-CSCF 的第二安全关联信息建立所述信令协商的 IPSec-ESP 安全关联。

9. 一种 IP 多媒体子系统的终端,其特征在于,包括:

协商与建立模块,用于与 IP 多媒体子系统 IMS 核心网进行信令协商,并在所述信令协商的过程中建立所述终端与所述 IMS 核心网之间的媒体传输的 IP 安全 - 封装安全负载 IPSec-ESP 安全关联;

媒体传输模块,用于通过所述媒体传输的 IPSec-ESP 安全关联将媒体内容发送给所述 IMS 核心网和 / 或接收来自所述 IMS 核心网的媒体内容;

注册与建立模块,其中:

所述注册与建立模块用于在所述协商与建立模块与所述 IMS 核心网进行信令协商之前,向所述 IMS 核心网进行注册,并在所述注册的过程中建立与所述 IMS 核心网之间的信令协商的 IPSec-ESP 安全关联;

所述协商与建立模块用于通过所述信令协商的 IPSec-ESP 安全关联与所述 IMS 核心网进行所述信令协商;

其中,所述注册与建立模块用于在所述协商与建立模块与所述 IMS 核心网进行信令协商之前,向所述 IMS 核心网进行注册,并在所述注册的过程中建立与所述 IMS 核心网之间的信令协商的 IPSec-ESP 安全关联包括:

所述终端向所述核心网中的代理型 - 呼叫会话控制功能 P-CSCF 发送 IMS 注册请求消息,其中,所述 IMS 注册请求消息中包括:所述终端的信息和所述终端的第一安全关联信息;

所述 P-CSCF 保存接收的所述 IMS 注册请求消息中的信息到本地,并向所述终端返回鉴

权质询消息,其中,所述鉴权质询消息中包括:第二安全关联信息和所述 P-CSCF 的信息;

所述终端接收所述鉴权质询消息之后,所述终端和所述 P-CSCF 之间通过所述第一安全关联信息和所述 P-CSCF 的第二安全关联信息建立所述信令协商的 IPSec-ESP 安全关联。

10. 一种 IP 多媒体子系统 IMS 核心网,其特征在于,包括:

协商与建立模块,用于与终端进行信令协商,并在所述信令协商的过程中建立与所述终端之间的媒体传输的 IP 安全-封装安全负载 IPSec-ESP 安全关联;

媒体传输模块,用于通过所述媒体传输的 IPSec-ESP 安全关联将媒体内容发送给所述终端和/或接收来自所述终端的媒体内容;

信令协商安全关联建立模块,其中:

信令协商安全关联建立模块用于在所述协商与建立模块与所述终端进行信令协商之前,接受所述终端的注册,并在所述注册的过程中建立与所述终端之间的信令协商的 IPSec-ESP 安全关联;

所述协商与建立模块用于通过所述信令协商的 IPSec-ESP 安全关联与所述终端进行所述信令协商;

其中,所述信令协商安全关联建立模块用于在所述协商与建立模块与所述终端进行信令协商之前,接受所述终端的注册,并在所述注册的过程中建立与所述终端之间的信令协商的 IPSec-ESP 安全关联包括:

所述终端向所述核心网中的代理型-呼叫会话控制功能 P-CSCF 发送 IMS 注册请求消息,其中,所述 IMS 注册请求消息中包括:所述终端的信息和所述终端的第一安全关联信息;

所述 P-CSCF 保存接收的所述 IMS 注册请求消息中的信息到本地,并向所述终端返回鉴权质询消息,其中,所述鉴权质询消息中包括:第二安全关联信息和所述 P-CSCF 的信息;

所述终端接收所述鉴权质询消息之后,所述终端和所述 P-CSCF 之间通过所述第一安全关联信息和所述 P-CSCF 的第二安全关联信息建立所述信令协商的 IPSec-ESP 安全关联。

IMS 多媒体通信方法和系统、终端及 IMS 核心网

技术领域

[0001] 本发明涉及通信领域,具体而言,涉及一种 IMS 多媒体通信方法和系统、终端及 IMS 核心网。

背景技术

[0002] 随着 3G(the 3rd Generation, 第三代)网络的发展,在 IMS(IP MultiMedia Subsystem, IP 多媒体子系统)核心网下可以部署越来越多的多媒体业务,例如视频共享(VS,VideoSharing)、基于 IP 的语音通信(VoIP,Voice over IP)、基于 IP 的视频与语音通信(V2IP,Videoand Voice over IP)、以及一键通(PoC,Push To Talk over Cellular)等。这些业务都是采用 IP 协议进行传输,而不是采用 2G 网络的 SS7(Signal System 7,7 号信令系统)。

[0003] IP 协议的引入使得在 IMS 核心网部署分组交换业务非常方便,也使得 IMS 核心网完全开放和易于访问。由于接入网络的多样性和复杂性,从而引发了 IMS 下多媒体通信的安全问题。

发明内容

[0004] 本发明的主要目的在于提供一种 IMS 多媒体通信方法和系统、终端及 IMS 核心网,以至少解决上述问题。

[0005] 根据本发明的一个方面,提供了一种 IMS 多媒体通信方法,包括:终端与 IMS 核心网进行信令协商,并在信令协商的过程中建立终端与 IMS 核心网之间的媒体传输的 IPSec-ESP 安全关联;终端和 IMS 核心网之间通过媒体传输的 IPSec-ESP 安全关联进行媒体内容的传输。

[0006] 根据本发明的又一方面,提供了一种 IMS 多媒体通信系统,包括终端和 IMS 核心网,其中:终端用于与 IMS 核心网进行信令协商,并在信令协商的过程中建立与 IMS 核心网之间的媒体传输的 IPSec-ESP 安全关联,通过媒体传输的 IPSec-ESP 安全关联进行终端和 IMS 核心网之间的媒体内容的传输。

[0007] 根据本发明的又一方面,提供了一种终端,包括:协商与建立模块,用于与 IMS 核心网进行信令协商,并在信令协商的过程中建立终端与 IMS 核心网之间的媒体传输的 IPSec-ESP 安全关联;媒体传输模块,用于通过媒体传输的 IPSec-ESP 安全关联将媒体内容发送给 IMS 核心网和/或接收来自 IMS 核心网的媒体内容。

[0008] 根据本发明的又一方面,提供了一种 IMS 核心网,包括:协商与建立模块,用于与终端进行信令协商,并在信令协商的过程中建立与终端之间的媒体传输的 IPSec-ESP 安全关联;媒体传输模块,用于通过媒体传输的 IPSec-ESP 安全关联将媒体内容发送给终端和/或接收来自终端的媒体内容。

[0009] 通过本发明,终端和 IMS 核心网之间通过建立媒体传输的 IPSec-ESP 安全关联,这样,可以在进行媒体内容的传输时通过该媒体传输的 IPSec-ESP 安全关联进行传输,从而

确保了终端和 IMS 核心网之间传输的媒体内容的安全性,解决了相关技术中 IMS 下的多媒体通信的安全问题,避免了媒体内容在终端和 IMS 核心网之间进行传输时被他人恶意地盗取和篡改等。

附图说明

[0010] 此处所说明的附图用来提供对本发明的进一步理解,构成本申请的一部分,本发明的示意性实施例及其说明用于解释本发明,并不构成对本发明的不当限定。在附图中:

[0011] 图 1 是根据本发明实施例的 IMS 多媒体通信系统的架构图;

[0012] 图 2 是根据本发明实施例的 IMS 多媒体通信系统中的终端的结构示意图;

[0013] 图 3 是根据本发明实施例的 IMS 多媒体通信系统中的 IMS 核心网的结构示意图;

[0014] 图 4 是根据本发明实施例的 IMS 多媒体通信方法的流程图;

[0015] 图 5 是根据本发明优选实施例的 IMS 多媒体通信过程的流程示意图。

具体实施方式

[0016] 下文中将参考附图并结合实施例来详细说明本发明。需要说明的是,在不冲突的情况下,本申请中的实施例及实施例中的特征可以相互组合。

[0017] IMS 多媒体通信主要包含两方面的内容:控制面的信令协商和用户面的媒体数据(内容)传输,前者一般采用 SIP(Session Initiation Protocol,会话发起协议)协议,后者一般采用 RTP(Real-time Transport Protocol,实时传送协议)协议。图 1 是根据本发明实施例的 IMS 多媒体通信系统的架构图,如图 1 所示,通常涉及终端 10(UE-A 和 UE-B)和 IMS 核心网 20(UE-A 的归属网络和 UE-B 的归属网络),本发明的以下实施例主要关注终端 10 与 IMS 核心网 20 之间的安全通信,IMS 核心网之间属于专用有线网络,通常不需要考虑安全性问题。

[0018] 为了保护终端与 IMS 核心网之间的媒体内容不会被恶意篡改和盗取,如图 1 所示,根据本发明实施例的 IMS 多媒体通信中的终端(UE)10 可以用于与 IMS 核心网 20 进行信令协商,并在信令协商的过程中建立与 IMS 核心网 20 之间的媒体传输的 IPSec-ESP(IP Security-Encapsulate Secure Payload,IP 安全-封装安全负载)安全关联,通过该媒体传输的 IPSec-ESP 安全关联进行终端 10 和 IMS 核心网 20 之间的媒体内容的传输。例如,通过该媒体传输的 IPSec-ESP 安全关发送媒体内容到 IMS 核心网 20 以及接收 IMS 核心网 20 发来的媒体内容。

[0019] 从而,IMS 核心网 20 也可以用于与 UE 10 进行信令协商,并在信令协商的过程中建立与 IMS 核心网 20 之间的媒体传输的 IPSec-ESP 安全关联,通过该媒体传输的 IPSec-ESP 安全关联进行终端 10 和 IMS 核心网 20 之间的媒体内容的传输。例如,通过该媒体传输的 IPSec-ESP 安全关发送媒体内容到终端 10 以及接收终端 10 发来的媒体内容。

[0020] 进一步,为了保护终端 10 与 IMS 核心网 20 进行信令协商时的信令协商数据的完整性和加密保护,终端 10 还用于在与 IMS 核心网 20 进行信令协商之前,向 IMS 核心网 20 进行注册,并在注册的过程中建立与 IMS 核心网 20 之间的信令协商的 IPSec-ESP 安全关联,从而终端 10 就可以通过该信令协商的 IPSec-ESP 安全关联与 IMS 核心网 20 进行信令协商。

[0021] 在实际应用中,如图 1 所示,终端 10 中包含两部分:ISIM(IP Multimedia

Services IdentityModule, IMS 业务识别模块)/USIM(Universal Subscriber Identity Module, 全球用户识别模块)和 IMS 多媒体通信客户端(即图 1 中的 IMS Client)。其中, ISIM/USIM 主要用于提供终端 10 的身份信息,而 IMS 多媒体通信客户端为用户使用的应用程序。IMS 核心网 20 中包括的网元主要有 HSS(Home Subscriber Server, 归属用户服务器)、P-CSCF(Proxy-Call SessionControl Function, 代理型-呼叫会话控制功能)和 MGCF(Media Gateway Control Function, 媒体网关控制功能),其中, HSS 保存终端的 IMS 用户信息和 ISIM/USIM 的身份信息等, P-CSCF 主要负责多媒体通信的用户注册和会话协商,而 MGCF 负责媒体内容的转发。

[0022] 由上述的系统可知,根据本发明实施例的 IMS 多媒体通信系统中的终端 10 的结构示意图可以如图 2 所示,包括以下模块:协商与建立模块 102,用于与 IMS 核心网 20 进行信令协商,并在信令协商的过程中建立终端 10 与 IMS 核心网 20 之间的媒体传输的 IPSec-ESP 安全关联;媒体传输模块 104,用于通过该媒体传输的 IPSec-ESP 安全关联将媒体内容发送给 IMS 核心网 20 和/或接收来自 IMS 核心网 20 的媒体内容。从而,确保了终端与 IMS 核心网之间的媒体内容不会被恶意篡改和盗取。

[0023] 进一步,为了保护终端 10 与 IMS 核心网 20 的协商与建立模块 102 进行信令协商时的信令协商数据的完整性和加密保护,如图 2 所示,该终端 10 还可以进一步包括:注册与建立模块 106,用于在协商与建立模块 102 与 IMS 核心网 20 进行信令协商之前,向 IMS 核心网 20 进行注册,并在注册的过程中建立与 IMS 核心网 20 之间的信令协商的 IPSec-ESP 安全关联;从而,协商与建立模块 102 就可以通过该信令协商的 IPSec-ESP 安全关联与 IMS 核心网 20 进行信令协商。

[0024] 同样,根据本发明实施例的 IMS 多媒体通信系统中的 IMS 核心网 20 的结构示意图如图 3 所示,包括以下模块:协商与建立模块 202,用于与终端 10 进行信令协商,并在信令协商的过程中建立与终端 10 之间的媒体传输的 IPSec-ESP 安全关联;媒体传输模块 204,用于通过该媒体传输的 IPSec-ESP 安全关联将媒体内容发送给终端 10 和/或接收来自终端 10 的媒体内容。从而,确保了终端与 IMS 核心网之间的媒体内容不会被恶意篡改和盗取。

[0025] 进一步,为了保护终端 10 与 IMS 核心网 20 的协商与建立模块 202 进行信令协商时的信令协商数据的完整性和加密保护,如图 3 所示,IMS 核心网 20 还可以包括信令协商安全关联建立模块 206,用于在协商与建立模块 202 与终端 10 进行信令协商之前,接受终端 10 的注册,并在注册的过程中建立与终端 10 之间的信令协商的 IPSec-ESP 安全关联;则,协商与建立模块 202 就可以通过该信令协商的 IPSec-ESP 安全关联与终端 10 进行信令协商。

[0026] 在实际实施的过程中,上述的协商与建立模块 202 和信令协商安全关联建立模块 206 可以由 P-CSCF 来实现,而媒体传输模块 204 可以由 MGCF 来实现。

[0027] 结合图 1 所示的 IMS 多媒体通信系统,该通信系统进行 IMS 多媒体通信的方法如图 4 所示,包括以下步骤:

[0028] 步骤 S402,终端与 IMS 核心网进行信令协商,并在信令协商的过程中建立终端与 IMS 核心网之间的媒体传输的 IPSec-ESP 安全关联;

[0029] 步骤 S404,终端和 IMS 核心网之间通过在步骤 S402 中建立的媒体传输的 IPSec-ESP 安全关联进行媒体内容的传输。

[0030] 本实施例中,终端和 IMS 核心网之间通过建立媒体传输的 IPSec-ESP 安全关联,这样,可以在进行媒体内容的传输时通过该媒体传输的 IPSec-ESP 安全关联进行传输,从而确保了终端和 IMS 核心网之间传输的媒体内容的安全性,解决了相关技术中 IMS 下的多媒体通信的安全问题,避免了媒体内容在终端和 IMS 核心网之间进行传输时被他人恶意地盗取和篡改等。

[0031] 为了进一步地保护终端与 IMS 核心网进行信令协商时的信令协商数据的完整性,在步骤 S402 之前,终端向 IMS 核心网进行注册,并在注册的过程中建立终端与 IMS 核心网之间的信令协商的 IPSec-ESP 安全关联;则步骤 S402 中终端与 IMS 核心网进行信令协商时,终端和 IMS 核心网之间就可以通过该信令协商的 IPSec-ESP 安全关联进行信令协商。

[0032] 例如,如图 5 所示,终端向 IMS 核心网进行注册的过程包括以下步骤:

[0033] 步骤 1:终端 UE-A 向 IMS 核心网中的 P-CSCF 发送 IMS 注册请求消息,其中,该 IMS 注册请求消息中携带有:终端的信息和第一安全关联信息。

[0034] 其中,终端的信息可以包括:终端的 IP 地址、IMS 用户信息、和终端支持的算法列表(包括完整性算法、加密算法和压缩算法)以便在 UE 与核心网中的 P-CSCF 之间进行算法的协商;第一安全关联信息包括:终端随机生成的 SPI (Secure Parameter Index,安全参数索引) 信息(称为第一 SPI 信息,该 SPI 信息可以为 8 个字节)及其对应的端口信息。如果有多个安全关联,那么需要保证每次生成的 SPI 信息的唯一性,并且,如果上述算法列表中的完整性算法、加密算法或压缩算法均有多种具体算法,则每种算法具有其优先级,终端偏好的算法优先级较高,所有算法可以按照优先级由高到低的顺序排列。

[0035] 在实际应用中,上述第一 SPI 信息及其对应的端口信息可以为两个信令安全关联的 SPI 值和对应的端口号(主叫业务数据处理端口和被叫业务数据处理端口)。

[0036] 步骤 2,P-CSCF 收到终端的 IMS 注册请求消息后,从该 SIP 协议的 IMS 注册请求消息中获取 UE 的 IP 地址、IMS 用户信息、第一 SPI 信息及其对应的端口信息、UE 支持的算法列表、以及 UE 主动和被动发送接收 SIP 消息的一对端口号,并将这些信息保存下来。

[0037] P-CSCF 根据该 IMS 注册请求消息中的 IMS 用户信息获取到 AKA (Authentication and KeyAgreement,认证和密钥协商)鉴权五元组(称为第一 AKA 鉴权五元组),例如,P-CSCF 首先从 HSS 中获取到与该 IMS 用户信息所对应的卡密钥(即终端 UE-A 中的 ISIM/USIM 中的密钥),然后,使用该卡密钥和随机数(可以随机生成或者预先设定该随机数)获得上述第一 AKA 鉴权五元组,其中,该第一 AKA 鉴权五元组中包括第一 IK(完整性密钥)、第一 CK(加密密钥)、和第一 RES(响应)字段。在实际应用中可以采用 AKA 算法来使用该卡密钥和随机数(可以随机生成或者预先设定该随机数)获得上述第一 AKA 鉴权五元组。

[0038] 然后,P-CSCF 向终端返回该 IMS 注册请求消息的鉴权质询消息,其中,该鉴权质询消息中包括:第二安全关联信息和 P-CSCF 的信息。其中,P-CSCF 的信息包括:P-CSCF 的 IP 地址和 P-CSCF 支持的算法列表(包括完整性算法、加密算法和压缩算法);第二安全关联信息包括:P-CSCF 随机生成的 SPI 信息(称为第二 SPI 信息)及其对应的端口信息。如果有多个安全关联,那么需要保证每次生成的 SPI 信息的唯一性,并且,如果上述算法列表中的完整性算法、加密算法或压缩算法均有多种具体算法,则每种算法具有其优先级,终端偏好的算法优先级较高,所有算法可以按照优先级由高到低的顺序排列。

[0039] 同样,在实际应用中,上述第二 SPI 信息及其对应的端口信息可以为两个信令安

全关联的 SPI 值和对应的端口号（主叫业务数据处理端口和被叫业务数据处理端口）。

[0040] 终端 UE-A 收到质询响应消息之后,就可以验证 P-CSCF 的质询响应是否与 UE-A 本地的 ISIM/USIM 的计算结果一致,从而完成对服务器的身份认证,同时还可以得到 UE-A 的 AKA 鉴权五元组（称为第二 AKA 鉴权五元组）,从中得到 IK（称为第二 IK）和 CK（第二 CK）。这样,P-CSCF 和 UE-A 已经共享一对密钥信息,建立信令协商的 IPsec-ESP 安全关联所需的完整性密钥和加密密钥从 IK（包括第一 IK 和第二 IK）和 CK（包括第一 CK 和第二 CK）进行展开,主要考虑完整性算法和加密算法本身的密钥长度问题,例如 3DES 算法需要 192 位密钥,而 IK 和 CK 只有 128 位。此时,例如可以将 IK 和 CK 的 128 位中的前 64 位复制,并放在该 128 位的尾部,从而凑成 192 位。

[0041] 在实际应用中,上述鉴权质询消息中还可以包括:第一 RES 字段和上述随机数。这样,终端 UE-A 验证 P-CSCF 的质询响应是否与 UE-A 本地的 ISIM/USIM 的计算结果一致,从而完成对服务器的身份认证的步骤可以为:终端中的 ISIM 或 USIM 使用本地的卡密钥和上述鉴权质询消息中的随机数获得第二 AKA 鉴权五元组,其中,第二 AKA 鉴权五元组中包括:第二 IK、第二 CK、和第二 RES 字段;终端判断该第二 RES 字段与上述鉴权质询消息中的第一 RES 字段是否相同;若判断结果为相同,则确定 P-CSCF 的身份认证成功。

[0042] 步骤 3:经过前面两次报文交互（即上述步骤 1 和 2）之后,终端 UE-A 与 P-CSCF 已经完成了 SPI 信息、所支持的算法和端口号的协商,建立信令协商的 IPsec-ESP 安全关联的信息已经具备。

[0043] 其中,终端 UE-A 具有建立信令协商的 IPsec-ESP 安全关联的两组安全关联参数如下:

[0044] (1) 主叫业务安全关联参数:终端的 IP 地址、P-CSCF 的 IP 地址、终端的受保护客户端端口号、终端的 SPI 信息、终端与 P-CSCF 均支持的最高优先级的算法（包括完整性算法、加密算法和压缩算法）、IK（即第二 IK）和 CK（即第二 CK）;

[0045] (2) 被叫业务安全关联参数:终端的 IP 地址、P-CSCF 的 IP 地址、终端的受保护服务器端端口号、终端的另一个 SPI 信息、终端与 P-CSCF 均支持的最高优先级算法（包括完整性算法、加密算法和压缩算法）、IK（即第二 IK）和 CK（即第二 CK）。

[0046] 同样,P-CSCF 也具有建立信令协商的 IPsec-ESP 安全关联的两组安全关联参数如下:

[0047] (1) 主叫业务安全关联参数:P-CSCF 的 IP 地址、终端的 IP 地址、P-CSCF 的受保护服务器端端口号、P-CSCF 的 SPI 信息、P-CSCF 与终端均支持的最高优先级算法（包括完整性算法、加密算法和压缩算法）、IK（第一 IK）和 CK（第一 CK）;

[0048] (2) 被叫业务安全关联参数:P-CSCF 的 IP 地址、终端的 IP 地址、P-CSCF 的受保护客户端端口号、P-CSCF 的另一个 SPI 信息、P-CSCF 与终端均支持的最高优先级算法（包括完整性算法、加密算法和压缩算法）、IK（第一 IK）和 CK（第一 CK）。

[0049] 在上述四组安全关联参数中,P-CSCF 与终端均支持的最高优先级算法是从算法列表中选择双方都支持的算法,如果没有交集,则不采用任何相应算法。利用各自的安全关联参数,终端 UE-A 和 P-CSCF 可以建立四组信令协商的 IPsec-ESP 安全关联,之后终端 UE-A 与 P-CSCF 的信令协商消息就可以在这四个信令协商的 IPsec-ESP 安全关联中进行保护。根据不同端口,UE 与 P-CSCF 的一组安全关联用于保护终端主叫业务的信令协商,另一组安全关

联用于保护终端被叫业务的信令协商。这样 UE 与 P-CSCF 的信令协商数据可以实现完整性和加密保护。

[0050] 步骤 4:终端再把 ISIM/USIM 的计算结果,即第二 RES 字段通过 IMS 鉴权验证请求消息发送给 P-CSCF,以便服务器验证终端的身份,其中,该 IMS 鉴权认证请求消息中还包括:终端的信息和终端的第一安全关联信息(终端的信息和终端的第一安全关联信息与上述 IMS 注册请求消息中的相同),以便 P-CSCF 能够对之前的安全参数协商进行确认。

[0051] P-CSCF 在接收到该 IMS 鉴权验证请求消息之后,首先验证其中的终端的信息和终端的第一安全关联信息与本地保存的信息(即在步骤 2 中保存的 IMS 注册请求消息中的第一 SPI 值以及端口号、以及终端支持的算法列表)是否一致,若不一致,则确定终端注册失败;若一致,则继续验证该 IMS 鉴权验证请求消息中携带的第二 RES 字段与之前计算得到的第一 RES 字段是否相同(即一致),若相同,此时确定终端的 AKA 鉴权成功以及注册成功。从而实现了服务器对终端的身份认证。

[0052] 上述的 IMS 鉴权验证请求消息必须在终端和 P-CSCF 的主叫业务的信令协商的 IPsec-ESP 安全关联中进行传输,其它人员无法再恶意地窃听到终端与 P-CSCF 之间的通信信息。

[0053] 步骤 5:P-CSCF 向终端发送鉴权结果消息,其中,鉴权结果可以为鉴权成功或鉴权失败。

[0054] 通过上述的步骤 1-5 即完成了终端向核心网(具体为 P-CSCF)的注册过程,并在注册过程中建立了终端和核心网之间的信令协商的 IPsec-ESP 安全关联,实现了信令协商数据的加密保护和完整性保护。

[0055] 步骤 6:终端 UE-B 也可以按照上述步骤 1-5 完成向核心网(具体为 P-CSCF)的注册过程。

[0056] 如图 5 所示,终端之间(UE-A 和 UE-B)通过核心网进行 IMS 多媒体的媒体数据(内容)传输的过程具体包括以下步骤:

[0057] 步骤 7:UE-A 发起 IMS 会话邀请请求消息给核心网,此消息携带媒体信息以及 UE-A 再次随机生成的用于建立媒体传输的 SPI 信息(称为第三 SPI 信息)以便保护媒体数据的安全传输。如果有多种媒体通信,例如同时包含音频和视频内容的话,那么需要有两个 SPI 信息(即第三 SPI 信息包括两个 SPI 信息)来分别建立两组安全关联。其中,媒体信息可以包括:媒体内容的传输端口信息和媒体描述信息。

[0058] 步骤 8:UE-A 侧的 P-CSCF 收到此 IMS 会话邀请请求消息之后,该 P-CSCF 将此 IMS 会话邀请请求消息中的信息保存下来,并将此 IMS 会话邀请请求消息发送到 UE-B 侧的 P-CSCF,UE-B 的 P-CSCF 通知自己的 MGCF,生成 MGCF 的 SPI 信息,然后发送给 UE-B;UE-B 作为被叫,会使用被叫业务安全关联进行信令协商的安全保护。

[0059] 步骤 9:UE-B 收到 P-CSCF 的 IMS 会话邀请请求消息后,发送振铃响应消息给 UE-B 侧的 P-CSCF 表示 UE-B 已经收到 UE-A 的 IMS 会话邀请请求消息。

[0060] 步骤 10:IMS 核心网将该振铃响应消息转发给 UE-A。终端 UE-A 收到此消息后知道 UE-B 已经收到 IMS 会话邀请请求消息。

[0061] 步骤 11:UE-B 接受会话邀请,向 UE-B 的 IMS 核心网发送 200OK 响应,此 200OK 响应携带 UE-A 和 UE-B 都支持的媒体格式以及音视频传输端口号,此外还有 UE-B 的媒体传输

SPI 信息。

[0062] UE-B 侧的 P-CSCF 收到该 2000K 响应消息后,将 UE-B 的媒体传输安全关联信息通知媒体网关服务器 (MGCF),这样 UE-B 的 MGCF 与 UE-B 共享一组 IPsec-ESP 的安全关联参数信息,IK 和 CK 从之前信令协商的 AKA 鉴权中进行扩展,加密算法和完整性算法使用之前所选择算法。

[0063] 步骤 12 :UE-B 侧的 P-CSCF 将该 2000K 响应消息转发给 UE-A 侧的 P-CSCF,UE-A 侧的 P-CSCF 通知其 MGCF, MGCF 生成 SPI 信息 (称为第四 SPI 信息) 和准备进行媒体传输的端口号,然后将该 2000K 响应消息发送给 UE-A。这样 UE-A 侧的 MGCF 与 UE-A 也共享一组 IPsec-ESP 的安全关联参数信息。

[0064] 步骤 13 :经过步骤 7-12 的消息交互,UE-A 和 UE-B 具有各自媒体传输的安全关联的参数信息,UE-A 采用之前信令协商的 IK 和 CK 以及之前选中的完整性算法和加密算法建立与 UE-A 媒体网关的安全关联,根据传输媒体数目,可能有一组或者多组安全关联,实现了对媒体数据传输的安全保护。

[0065] 步骤 14 :UE-B 根据步骤 7-12 的消息交互信息,建立与 UE-B 所处的媒体网关之间的媒体传输的 IPsec-ESP 安全关联,之后 UE-A 和 UE-B 的媒体数据传输已处于安全保护之中。

[0066] 步骤 15 :UE-A 利用与核心网建立的媒体传输的 IPsec-ESP 安全关联传输媒体内容,实现各种多媒体通信功能,例如音频、视频和图像。

[0067] 步骤 16 :UE-B 的媒体内容通过之前的安全关联进行传输,媒体内容采用之前信令协商的 IK 和 CK 进行加密保护。多媒体通信结束之后,可以结束媒体传输的 IPsec-ESP 安全关联,而信令协商的 IPsec-ESP 安全关联一直保持,直到用户注销为止。

[0068] 从以上的描述中,可以看出,本发明实现了如下技术效果 :终端和 IMS 核心网之间通过建立媒体传输的 IPsec-ESP 安全关联,这样,可以在进行媒体内容的传输时通过该媒体传输的 IPsec-ESP 安全关联进行传输,从而确保了终端和 IMS 核心网之间传输的媒体内容的安全性,解决了相关技术中 IMS 下的多媒体通信的安全问题,避免了媒体内容在终端和 IMS 核心网之间进行传输时被他人恶意地盗取和篡改等。

[0069] 显然,本领域的技术人员应该明白,上述的本发明的各模块或各步骤可以用通用的计算装置来实现,它们可以集中在单个的计算装置上,或者分布在多个计算装置所组成的网络上,可选地,它们可以用计算装置可执行的程序代码来实现,从而,可以将它们存储在存储装置中由计算装置来执行,并且在某些情况下,可以以不同于此处的顺序执行所示出或描述的步骤,或者将它们分别制作成各个集成电路模块,或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样,本发明不限制于任何特定的硬件和软件结合。

[0070] 以上所述仅为本发明的优选实施例而已,并不用于限制本发明,对于本领域的技术人员来说,本发明可以有各种更改和变化。凡在本发明的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

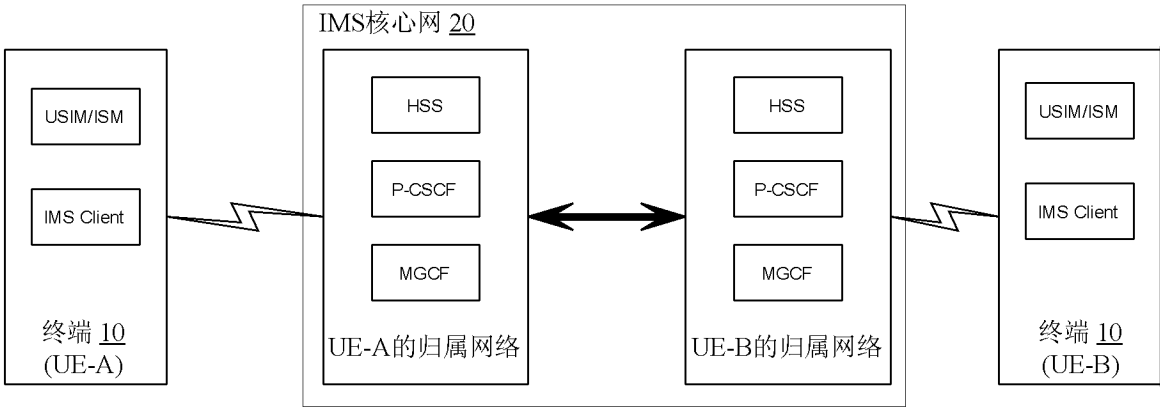


图 1

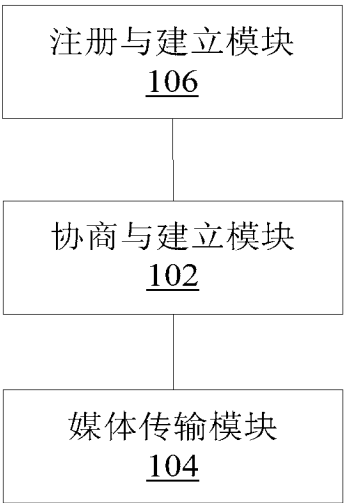


图 2



图 3



图 4

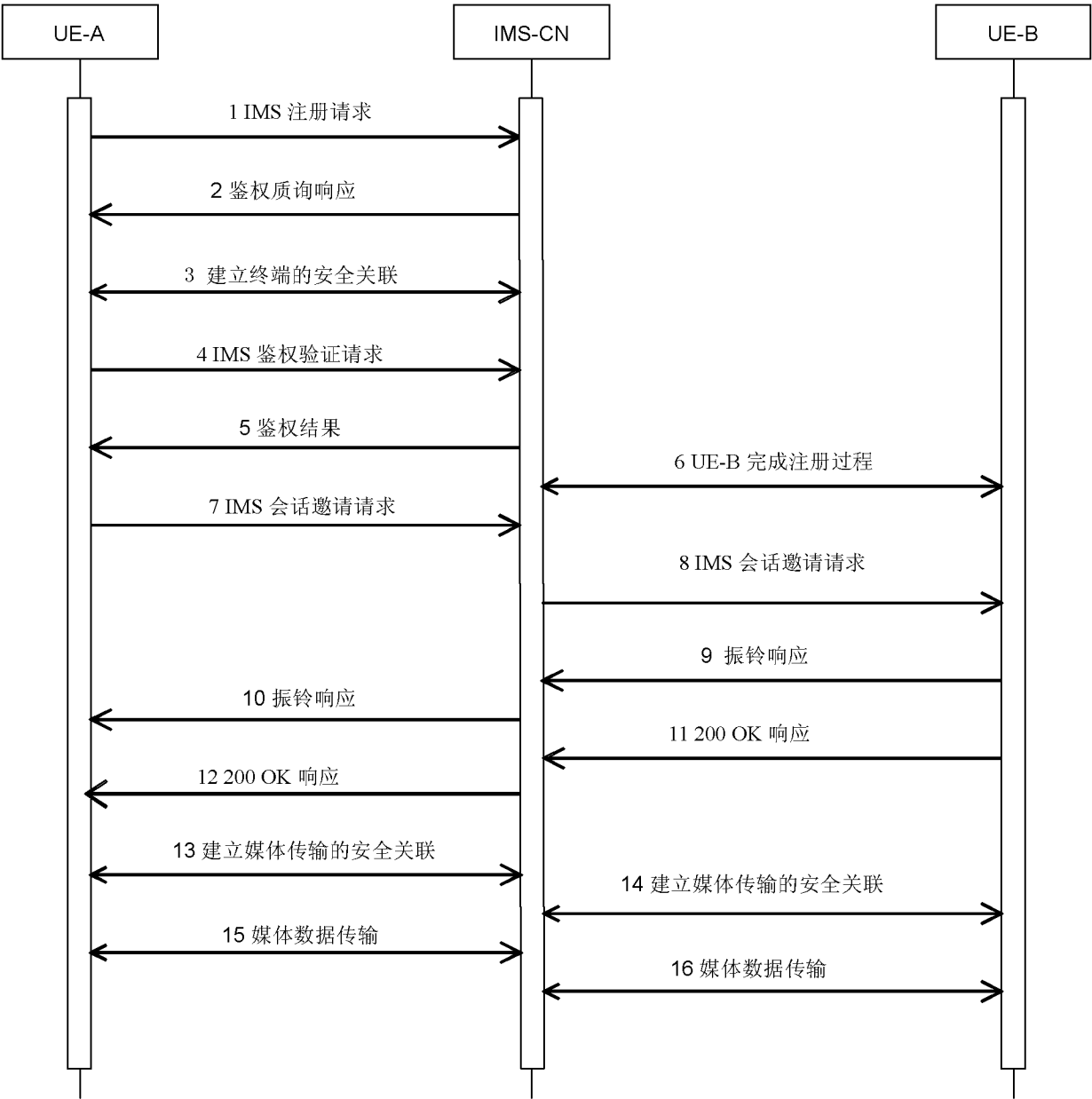


图 5