(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 109714295 B
(45)授权公告日 2021.10.26

(21)申请号 201711008881.1

(22)申请日 2017.10.25

(65)同一申请的已公布的文献号
申请公布号 CN 109714295 A

(43)申请公布日 2019.05.03

(73)专利权人 普天信息技术有限公司
地址 100080 北京市海淀区海淀北二街6号普天大厦

(72)发明人 郄卫军 李瑞林

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
代理人 王莹 李相雨

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 106788959 A,2017.05.31
CN 106788959 A,2017.05.31
WO 2016145558 A1,2016.09.22
CN 103945371 A,2014.07.23
CN 103402198 A,2013.11.20
CN 105743896 A,2016.07.06
CN 102006593 A,2011.04.06
EP 2215795 A2,2010.08.11
EP 1209845 A2,2002.05.29

审查员 刘畅

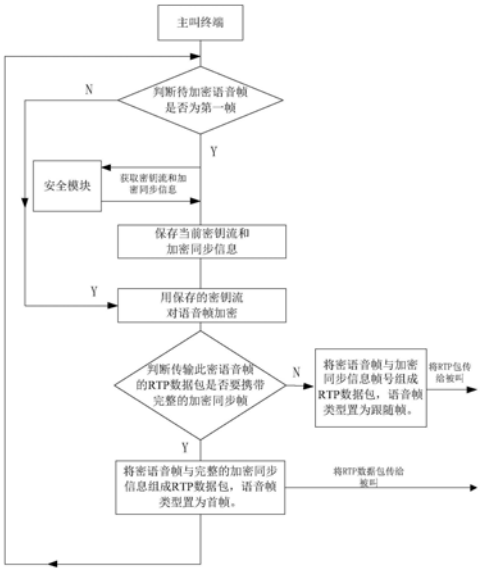
权利要求书2页 说明书6页 附图5页

(54)发明名称

一种语音加解密同步处理方法和装置

(57)摘要

本发明提供一种语音加解密同步处理方法和装置,通过在主叫终端将加密同步信息和加密语音帧在一个数据包中通过用户面发送,多个语音帧共用一个加密同步信息,并分为首帧和跟随帧两类,在携带首帧的RTP数据包中携带完整的加密同步信息,在跟随帧数据包中只携带加密同步信息帧号;共用一个加密同步信息的数个语音包携带的加密同步信息帧号相同;在被叫终端收到数据包后,用首帧中完整的加密同步信息从安全模块获取解密密钥流解密该帧语音,并用该密钥流对后续收到的跟随语音帧解密,如首帧丢失,则放弃后续跟随语音帧的解密。加解密同步处理简单,同步性好,传输效率高,适用于宽带集群速率高的语音帧加解密,对迟后接入处理尤其有效。



CN 109714295 B

1.一种语音加密传输方法,其特征在于,包括:

主叫终端确定发送一组语音帧时,将从安全模块获取的密钥流和加密同步信息更新至本地保存,并根据更新后的密钥流对该组语音帧中每个语音帧进行加密,将加密后的语音帧与加密同步信息组成一个数据包发送;其中,该组语音帧中第一帧语音帧置为首帧,首帧数据包中携带完整的加密同步信息,该组语音帧中后续语音帧置为跟随帧,跟随帧数据包中携带加密同步信息帧号;

同一组语音帧中的跟随帧数据包携带的加密同步信息帧号相同,所述同一组语音帧为使用同一密钥流加密的一组语音帧。

2.根据权利要求1所述的语音加密传输方法,其特征在于,将加密后的语音帧与加密同步信息组成数据包发送具体包括:

主叫终端将加密同步信息和加密后的语音帧在一个实时传输RTP数据包中发送至被叫终端;加密得到自适应多速率AMR语音帧后,将RTP数据包包头中P字段置为1,并在AMR语音帧后扩展RTP包尾,用以携带加密同步信息填充字段。

3.根据权利要求1所述的语音加密传输方法,其特征在于,主叫终端确定发送一组语音帧时,向安全模块获取密钥流和加密同步信息具体包括:

主叫终端发送一帧语音帧前,判断该语音帧是否为待加密的一组语音帧中的第一帧语音帧,若是,则向所述安全模块获取密钥流和加密同步信息,并将所述密钥流和所述加密同步信息更新至本地。

4.根据权利要求3所述的语音加密传输方法,其特征在于,若该语音帧不为待加密的一组语音帧中的第一帧语音帧,则将该语音帧置为跟随帧,根据更新前的密钥流和加密同步信息对该语音帧进行加密传输。

5.一种语音加密传输装置,其特征在于,包括主叫终端,所述主叫终端用于确定发送一组语音帧时,将从安全模块获取的密钥流和加密同步信息更新至本地保存,并根据更新后的密钥流对该组语音帧中每个语音帧进行加密,将加密后的语音帧与加密同步信息组成一个数据包发送;其中,该组语音帧中第一帧语音帧置为首帧,首帧数据包中携带完整的加密同步信息,该组语音帧中后续语音帧置为跟随帧,跟随帧数据包中携带加密同步信息帧号;

同一组语音帧中的跟随帧数据包携带的加密同步信息帧号相同,所述同一组语音帧为使用同一密钥流加密的一组语音帧。

6.一种语音加密传输方法,其特征在于,包括:

被叫终端收到首帧数据包后,保存首帧数据包中完整的加密同步信息并从安全模块获取对应的解密密钥流,根据解密密钥流解密首帧数据包及后续收到的跟随帧数据包;

其中,一组语音帧中第一帧语音帧置为首帧,首帧数据包中携带完整的加密同步信息,该组语音帧中后续语音帧置为跟随帧,跟随帧数据包中携带加密同步信息帧号;同一组语音帧中的跟随帧数据包携带的加密同步信息帧号相同,所述同一组语音帧为使用同一加密密钥流加密的一组语音帧。

7.根据权利要求6所述的语音加密传输方法,其特征在于,还包括:

若首帧数据包丢失,则放弃后续跟随帧数据包的解密。

8.根据权利要求6所述的语音加密传输方法,其特征在于,根据解密密钥流解密跟随帧数据包具体包括:从跟随帧数据包中获取加密同步信息帧号,并判断该帧号与保存的加密

同步信息帧号是否一致，若一致则进行解密，若不一致则放弃解密该跟随帧数据包。

9.一种语音加密传输装置，其特征在于，包括被叫终端，所述被叫终端用于收到首帧数据包后，保存首帧数据包中完整的加密同步信息并从安全模块获取对应的解密密钥流，根据解密密钥流解密首帧数据包及后续收到的跟随帧数据包；

其中，一组语音帧中第一帧语音帧置为首帧，首帧数据包中携带完整的加密同步信息，该组语音帧中后续语音帧置为跟随帧，跟随帧数据包中携带加密同步信息帧号；同一组语音帧中的跟随帧数据包携带的加密同步信息帧号相同，所述同一组语音帧为使用同一加密密钥流加密的一组语音帧。

一种语音加解密同步处理方法和装置

技术领域

[0001] 本发明涉及通信技术领域,更具体地,涉及一种语音加解密同步处理方法和装置。

背景技术

[0002] 随着社会经济的发展和行业需求的变化,以大带宽、高速率、全IP为突出特点的TD-LTE(Time Division Long Term Evolution,分时长期演进)宽带集群正引领集群通信进入全新的时代。TD-LTE宽带集群通信系统以第四代移动通信技术TD-LTE为核心技术,将TD-LTE的高速率、大带宽与数字集群技术中的资源共享、快速呼叫建立、指挥调度等特点进行融合,是集语音、数据、视频为一体的宽带数字集群系统。基于TD-LTE的宽带集群系统分为终端、基站、集群核心网、调度应用平台等组成部分。TD-LTE宽带集群通信系统的手持终端用户具有丰富的业务功能,基本功能包括:语音单呼、语音组呼、视频单呼、视频组呼、短消息、彩信等功能。在这些集群业务中,语音业务是最基础、最常用的业务,而对语音进行端到端加密又是集群系统需求最大的公安行业最基本的要求。

[0003] 端到端加密通信(End to End Encryption ,E2EE)是指加密在发方进行,解密在接收方进行,从发方到接收方可能会经过多个中间设备的转发,而加密的信息在传输通道和这些中间设备上均保持密文状态。端到端加密可根据用户需求,提高与通信系统无关的、用户可控的安全加密。但是端到端加密因同步处理复杂,往往会加大延时。相比于窄带集群的语音传输,TD-LTE宽带集群的语音包采样率更高,传输间隔更短。因此对宽带集群语音包的加解密性能和同步要求更高。

[0004] 现有的集群语音端到端加密实现方案一般分两类:一类是通过控制面信令传递同步加密信息,一般是一话一密(在同一次会话中使用同一个会话密钥),会话密钥通过加密服务器或主叫终端产生,在会话发起时传给需要会话密钥的主被叫双方或被叫一方;通话时,加解密双方要把加密或解密的语音数据及会话密钥传给安全模块,通过加解密算法获得加密或解密后的语音数据,其在不易丢帧的信令面传递会话密钥,在一次通话中只使用一个会话密钥,密钥同步简单高效,不易出错;但为保密性需要,加密算法复杂;且每个语音帧需要送进安全模块加解密;TD-LTE宽带集群语音帧20ms一帧,比窄带60ms一帧更频繁,且采样率高,数据量较窄带大很多,这样频繁且量大的数据进出安全模块及在安全模块中加密算法的耗时均易导致语音的延时,往往需要高性能的加密卡和终端去实现;另一类是通过用户面传递同步加密信息;一般是数帧一密(几个语音帧换一次密钥流),在对语音加密前,从安全模块获得加密密钥流和加密同步数据,使用加密密钥流加密语音数据,然后在用户面数据中把加密同步信息传给被叫;被叫拿到加密同步信息后,结合信令中传递的会话基本信息,从安全模块中获取解密密钥流,然后用解密密钥流对密语音数据解密;其在用户面传递加密同步信息,密钥流数帧一变,因保密性高,相应的数据加密计算简单,且语音数据可以不送入安全模块,减少了频繁访问和数据传送,延时小;但因用户面数据传输易丢帧、乱序,会产生加密同步信息丢帧而使加解密不同步;在窄带语音帧低速率的情况下,往往通过增加传递加密同步信息次数来保证同步;但在TD-LTE宽带集群语音帧20ms 一帧的

速率且通过UDP协议传输下，增加传递加密同步信息次数不仅不能完全保证不丢帧，还会引起时延问题。因此需要有更好的加密信息同步方案。

发明内容

[0005] 本发明提供一种克服上述问题或者至少部分地解决上述问题的一种语音加解密同步处理方法和装置，解决了现有技术中在TD-LTE宽带集群语音帧20ms一帧的速率且通过UDP协议传输下，增加传递加密同步信息次数不能完全保证不丢帧，且还会引起时延的问题。

[0006] 根据本发明的一个方面，提供一种语音加密传输方法，包括：

[0007] 主叫终端确定发送一组语音帧时，将从安全模块获取的密钥流和加密同步信息更新至本地保存，并根据更新后的密钥流对该组语音帧中每个语音帧进行加密，将加密后的语音帧与加密同步信息组成一个数据包发送；其中，该组语音帧中第一帧语音帧置为首帧，首帧数据包中携带完整的加密同步信息，该组语音帧中后续语音帧置为跟随帧，跟随帧数据包中携带加密同步信息帧号。

[0008] 作为优选的，将加密后的语音帧与加密同步信息组成数据包发送具体包括：

[0009] 主叫终端将加密同步信息和加密后的语音帧在一个实时传输RTP数据包中发送至被叫终端；加密得到自适应多速率AMR语音帧后，将RTP数据包包头中P字段置为1，并在AMR语音帧后扩展RTP包尾，用以携带加密信息填充字段。

[0010] 作为优选的，所述同一组语音帧中的跟随数据包携带的加密同步信息帧号相同，所述同一组语音帧为使用同一密钥流加密的一组语音帧。

[0011] 作为优选的，主叫终端确定发送一组语音帧时，向安全模块获取密钥流和加密同步信息具体包括：

[0012] 主叫终端发送一帧语音帧前，判断待该语音帧是否为待加密的一组语音帧中的第一帧语音帧，若是则向所述安全模块获取密钥流和加密同步信息并更新至主叫终端。

[0013] 作为优选的，若该语音帧不为待加密的一组语音帧中的第一帧语音帧，则将该语音帧置为跟随帧，根据更新前的密钥流和加密同步信息对该语音帧进行加密传输。

[0014] 一种语音加密传输装置，包括主叫终端，所述主叫终端用于在确定发送一组语音帧时，将从安全模块获取的密钥流和加密同步信息更新至本地保存，并根据更新后的密钥流对该组语音帧中每个语音帧进行加密，将加密后的语音帧与加密同步信息组成一个数据包发送；其中，该组语音帧中第一帧语音帧置为首帧，首帧数据包中携带完整的加密同步信息，该组语音帧中后续语音帧置为跟随帧，跟随帧数据包中携带加密同步信息帧号。

[0015] 一种语音加密传输方法，包括：

[0016] 被叫终端收到首帧数据包后，保存首帧数据包中完整的加密同步信息并从安全模块获取对应的解密密钥流，根据解密密钥流解密首帧数据包及后续收到的跟随帧数据包。

[0017] 作为优选的，还包括：

[0018] 若首帧数据包丢失，则放弃后续跟随帧数据包的解密。

[0019] 作为优选的，根据解密密钥流解密跟随帧数据包具体括：从跟随帧数据包中获取加密同步信息帧号，并判断该帧号与保存的加密同步信息帧号是否一致，若一致则进行解密，若不一致则放弃解密该跟随帧数据包。

[0020] 一种语音加密传输装置，包括被叫终端，所述被叫终端用于收到首帧数据包后，保存首帧数据包中完整的加密同步信息并从安全模块获取对应的解密密钥流，根据解密密钥流解密首帧数据包及后续收到的跟随帧数据包。

[0021] 本发明提出一种语音加解密同步处理方法和装置，在主叫终端将加密同步信息和加密语音帧在一个数据包中通过用户面发送，多个语音帧共用一个加密同步信息，并分为首帧和跟随帧两类，在携带首帧的RTP数据包中携带完整的加密同步信息，在跟随帧数据包中只携带加密同步信息帧号，共用一个加密同步信息的数个语音包携带的加密同步信息帧号相同；加密同步信息和加密语音帧同包传送，同步性高，对迟后接入处理尤其有效；语音帧数据分首帧和跟随帧，共用一个加解密密钥流，在减少延时的情况下，同步处理简单高效，适用于宽带集群速率高的语音帧加解密；只在首帧数据包携带完整同步信息，跟随帧数据包只携带很少字节的帧号信息，节约了用户面的数据传输，提高了传输效率；被叫终端收到数据包后，用首帧中完整的加密同步信息从安全模块获取解密密钥流解密该帧语音，并用该密钥流对后续收到的跟随语音帧解密，如首帧丢失，则放弃后续跟随语音帧的解密。加解密同步处理简单，同步性好，传输效率高，适用于宽带集群速率高的语音帧加解密，对迟后接入处理尤其有效。

附图说明

[0022] 图1为根据本发明实施例的语音加密传输方法主叫终端加密方法示意图；

[0023] 图2为根据本发明实施例的RTP语音数据包组成结构示意图；

[0024] 图3为根据本发明实施例的RTP语音数据包序列实施示意图；

[0025] 图4为根据本发明实施例的RTP语音数据包序列另一种实施图；

[0026] 图5为根据本发明实施例的语音加密传输装置主叫终端示意图；

[0027] 图6为根据本发明实施例的语音加密传输方法被叫终端解密方法示意图；

[0028] 图7为根据本发明实施例的语音加密传输装置被叫终端示意图。

具体实施方式

[0029] 下面结合附图和实施例，对本发明的具体实施方式作进一步详细描述。以下实施例用于说明本发明，但不用来限制本发明的范围。

[0030] 如图1所示，在本实施例中还提供了一种语音加密传输方法，包括：

[0031] 主叫终端确定发送一组语音帧时，从安全模块获取密钥流和加密同步信息更新至本地，及对主叫终端的密钥流和加密同步信息进行更新；具体的，在本实施例中，可采用每隔若干帧语音帧则从安全模块获取新的密钥流和加密同步信息，进而实现分组，该组的语音帧全都发送出去后，则确定需要新发送一组语音帧，进一步，从安全模块获取密钥流和加密同步信息更新至本地；不同组语音帧采用的密钥流和加密同步信息不同，因此在确定发送的一组语音帧时，需要从安全模块重新获取密钥流和加密同步信息。

[0032] 根据密钥流对该组语音帧中每个语音帧进行加密，将加密后的语音帧与加密同步信息组成数据包发送；其中，该组语音帧中第一帧语音帧置为首帧，加密后得到首帧数据包，首帧数据包中携带完整的加密同步信息，该组语音帧中后续语音帧置为跟随帧，加密后得到跟随帧数据包，跟随帧数据包中携带加密同步信息帧号。

[0033] 在本实施例中,将加密后的语音帧与加密同步信息组成数据包发送具体包括:

[0034] 如图2所示,为一个RTP(Real-time Transport Protocol,实时传输协议)语音数据包组成结构,为了在RTP数据包中携带加密同步信息,需要将RTP包头中P字段置为1,并在AMR(Adaptive Multi-Rate,自适应多速率)语音帧后扩展RTP尾,用以携带加密信息填充字段。

[0035] RTP数据包序列如图3所示,为了防止同步信息帧的丢帧,可以在任意跟随帧数据包中携带重传同步信息帧,此时跟随帧数据包中语音帧类型标志Ftype置为首帧类型。如将头两帧设为首帧,则可有效防止同步信息帧丢弃,如图4所示。

[0036] 在本实施例中,同一组语音帧中的跟随数据包携带的加密同步信息帧号相同。

[0037] 在本实施例中,主叫终端确定发送一组语音帧时,从安全模块获取密钥流和加密同步信息,并将所述密钥流和所述加密同步信息更新至本地具体包括:

[0038] 主叫终端发送一帧语音帧前,判断待该语音帧是否为待加密的一组语音帧中的第一帧语音帧,若是则向所述安全模块获取密钥流和加密同步信息并更新至主叫终端。当主叫终端准备发送一帧语音帧时,首先判断待加密语音帧是否为第一帧;第一帧是指准备使用同一密钥流加密的一组语音帧的第一帧语音;若是则向安全模块获取并更新密钥流和加密同步信息,加密同步信息包括加密同步信息帧和帧号;

[0039] 保存当前密钥流和加密同步信息;

[0040] 用保存的密钥流对语音帧进行加密;若没有保存密钥流,则返回重新判断该语音帧是否为第一帧语音帧。即若待加密语音帧不为使用同一密钥流加密的一组语音帧中的第一帧语音帧,则将该语音帧置为跟随帧,根据当前保存的密钥流和加密同步信息对该语音帧进行加密传输,若当前没有保存的密钥流,则可认为第一帧语音帧判断有误,需要重新进行判断。

[0041] 对语音帧进行加密时,第一帧语音帧置为首帧,后续语音帧置为跟随帧,在携带首帧的RTP数据包中携带完整的加密同步信息,在跟随帧数据包中只携带加密同步信息帧号;具体的,判断传输此密语音帧的RTP数据包是否要携带完整的加密同步帧。判断依据是:该帧是否是第一帧或根据为防止丢帧而增加重传预先确定的帧数(如第二帧);若需要携带完整的加密同步帧,则将密语音帧与完整的加密同步信息组成RTP包,语音帧类型置为首帧;发送给被叫终端,被叫可以是单呼号,也可以组呼号;若不需要携带完整的加密同步帧,则将加密语音帧与加密同步信息帧号组成RTP数据包,语音帧类型置为跟随帧,发送给被叫终端,被叫可以是单呼号,也可以组呼号。

[0042] 当主叫终端发起端到端加密语音呼叫时,每隔数个语音帧便通过会话基本信息从安全模块获得一个新的密钥流和加密同步信息并保存。其中加密同步信息含同步信息帧和对应的帧号。用保存的密钥流对当前AMR语音帧加密后,将密语音帧和加密同步信息通过一个RTP包传给接收方。其中,首帧密语音帧的RTP数据包携带的是完整的加密同步信息,后续跟随语音帧的RTP数据包只携带加密同步信息帧号。首帧和跟随帧用标志区分在RTP包中携带。当完成数帧AMR语音帧加密后,终端再获取新的密钥流和加密同步信息进行加密和打包传输。

[0043] 如图5所示,本实施例中一种语音加密传输装置,包括主叫终端,所述主叫终端用于在确定发送一组语音帧时,向安全模块获取并更新密钥流和加密同步信息,并更新保存

到主叫终端；

[0044] 根据密钥流对该组语音帧中每个语音帧进行加密，将加密后的语音帧与加密同步信息组成数据包发送；其中，该组语音帧中第一帧语音帧置为首帧，首帧数据包中携带完整的加密同步信息，该组语音帧中后续语音帧置为跟随帧，跟随帧数据包中携带加密同步信息帧号。

[0045] 具体的，本实施例中的主叫终端包括密钥流存储模块、加密同步信息存储模块和组RTP包模块；密钥流存储模块用于存储根据第一帧语音帧从安全模块获取更新后的密钥流；所述加密同步信息存储模块用于存储并更新加密同步信息；所述组RTP包用于根据密钥流对该组语音帧中每个语音帧进行加密，将加密后的语音帧与加密同步信息组成RTP数据包发送。

[0046] 如图6所示，图中示出了一种语音加密传输方法，包括：

[0047] 被叫终端收到首帧数据包后，保存首帧数据包中完整的加密同步信息并从安全模块获取对应的解密密钥流，根据解密密钥流解密首帧数据包及后续收到的跟随帧数据包。

[0048] 被叫终端接收到一个RTP数据包时，首先从RTP数据包中获取语音帧类型，判断是否为首帧；

[0049] 若是首帧，则从RTP数据包中获取完整的加密同步信息并保存，并向安全模块发送基本会话信息和加密同步信息获取解密密钥流，保存当前解密密钥流；用保存的解密密钥流对当前AMR语音解密，得到语音帧明文；

[0050] 若不是首帧，则从RTP数据包中获取加密同步信息帧号，若获得的加密同步信息帧号与保存的帧号一致，则用保存的解密密钥流对当前AMR语音解密，得到语音帧明文；若不一致或目前无存储的帧号，则对该语音帧放弃解密。

[0051] 在本实施例中，还包括：

[0052] 若首帧数据包丢失，则放弃后续跟随帧数据包的解密。

[0053] 当被叫终端收到携带加密语音帧的RTP数据包时，首先通过标志判断是否首帧，如果是，则从RTP包中获取加密同步信息并保存。对收到的首帧语音帧，需要通过会话基本信息和加密同步信息从安全模块获得一个解密密钥流并保存，用保存的密钥流对当前AMR语音帧解密，生成语音帧明文。如果收到的是跟随语音帧(通过标志判断)，则从RTP包中获取加密同步信息帧号，如该帧号与存储的帧号一致，则用存储的解密密钥流对当前AMR语音帧解密；否则放弃对该语音帧的解密。此种处理，对于随时可能进入的迟后接入终端可以保持很好的加解密同步。

[0054] 如图7所示，本实施例中还提供了一种语音加密传输装置，包括被叫终端，所述被叫终端用于收到首帧数据包后，保存首帧数据包中完整的加密同步信息并从安全模块获取对应的解密密钥流，根据解密密钥流解密首帧数据包及后续收到的跟随帧数据包。

[0055] 具体的，所述被叫终端包括密钥流存储模块、加密同步信息存储模块和解RTP包模块；密钥流存储模块用于存储根据第一帧语音帧从安全模块获取更新后的解密密钥流；所述加密同步信息存储模块用于存储并更新加密同步信息；所述解RTP包用于根据解密密钥流对该组语音帧中每个语音帧进行解密。

[0056] 本实施例中还示出了一种TD-LTE宽带集群端到端语音加解密同步处理方法，包括：

[0057] 在主叫终端,将加密同步信息和加密语音帧在一个RTP数据包中通过用户面发送,多个语音帧共用一个加密同步信息,并分为首帧和跟随帧两类,在携带首帧的RTP数据包中携带完整的加密同步信息,在跟随帧数据包中只携带加密同步信息帧号,共用一个加密同步信息的数个语音包携带的加密同步信息帧号相同;

[0058] 在被叫终端,收到RTP数据包后,用首帧中完整的加密同步信息从安全模块获取解密密钥流解密该帧语音,并用该密钥流对后续收到的跟随语音帧解密;如首帧丢失,则放弃后续跟随语音帧的解密。

[0059] 当主叫终端发起端到端加密语音呼叫时,每隔数个语音帧便通过会话基本信息从安全模块获得一个新的密钥流和加密同步信息并保存。其中加密同步信息含同步信息帧和对应的帧号。用保存的密钥流对当前AMR语音帧加密后,将密语音帧和加密同步信息通过一个RTP包传给接收方。其中,首帧密语音帧的RTP数据包携带的是完整的加密同步信息,后续跟随语音帧的RTP数据包只携带加密同步信息帧号。首帧和跟随帧用标志区分在RTP包中携带。当完成数帧AMR语音帧加密后,终端再获取新的密钥流和加密同步信息进行加密和打包传输。

[0060] 当被叫终端收到携带加密语音帧的RTP数据包时,首先通过标志判断是否首帧,如果是,则从RTP包中获取加密同步信息并保存。对收到的首帧语音帧,需要通过会话基本信息和加密同步信息从安全模块获得一个解密密钥流并保存,用保存的密钥流对当前AMR语音帧解密,生成语音帧明文。如果收到的是跟随语音帧(通过标志判断),则从RTP包中获取加密同步信息帧号,如该帧号与存储的帧号一致,则用存储的解密密钥流对当前AMR语音帧解密;否则放弃对该语音帧的解密。此种处理,对于随时可能进入的迟后接入终端可以保持很好的加解密同步。

[0061] 本实施例中还提供了一种TD-LTE宽带集群端到端语音加解密同步处理装置,包括上述的主叫终端和被叫终端,所述主叫终端和被叫终端采用上述语音加密传输方法进行语音加密传输。

[0062] 本发明提出一种语音加解密同步处理方法和装置,在主叫终端将加密同步信息和加密语音帧在一个数据包中通过用户面发送,多个语音帧共用一个加密同步信息,并分为首帧和跟随帧两类,在携带首帧的RTP数据包中携带完整的加密同步信息,在跟随帧数据包中只携带加密同步信息帧号,共用一个加密同步信息的数个语音包携带的加密同步信息帧号相同;加密同步信息和加密语音帧同包传送,同步性高,对迟后接入处理尤其有效;语音帧数据分首帧和跟随帧,共用一个加解密密钥流,在减少延时的情况下,同步处理简单高效,适用于宽带集群速率高的语音帧加解密;只在首帧数据包携带完整同步信息,跟随帧数据包只携带很少字节的帧号信息,节约了用户面的数据传输,提高了传输效率;被叫终端收到数据包后,用首帧中完整的加密同步信息从安全模块获取解密密钥流解密该帧语音,并用该密钥流对后续收到的跟随语音帧解密,如首帧丢失,则放弃后续跟随语音帧的解密。此方案加解密同步处理简单,同步性好,传输效率高,适用于宽带集群速率高的语音帧加解密,对迟后接入处理尤其有效。

[0063] 最后,本发明的方法仅为较佳的实施方案,并非用于限定本发明的保护范围。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。

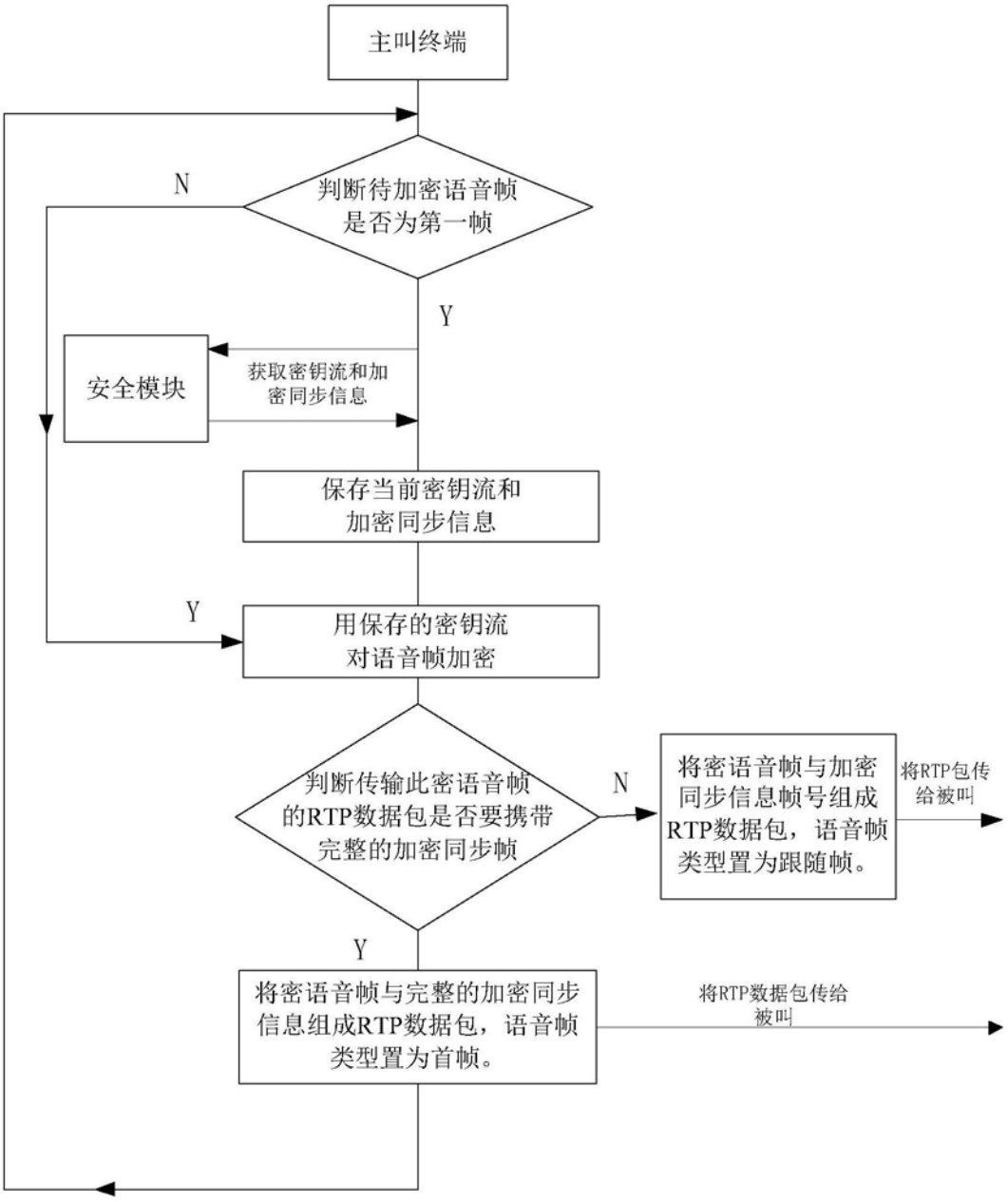
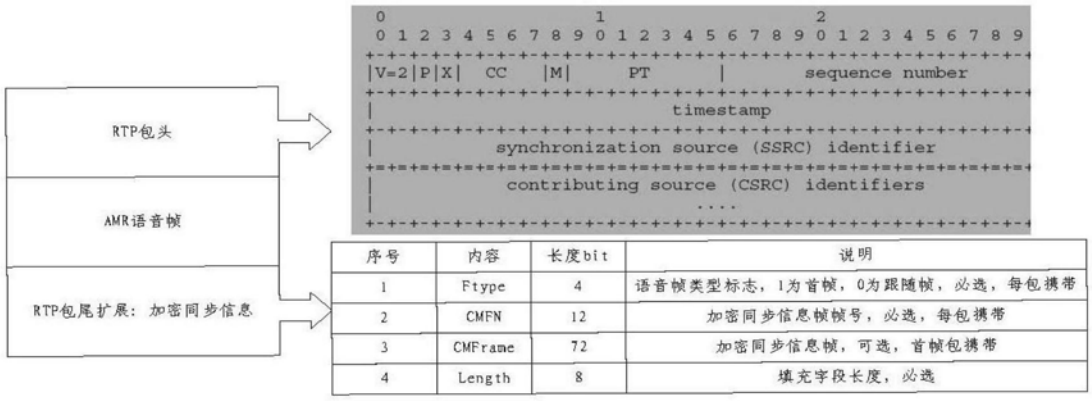

主叫终端
判断待加密语音帧是否为第一帧
N
Y
安全模块
获取密钥流和加密同步信息
保存当前密钥流和加密同步信息
Y
用保存的密钥流对语音帧加密
判断传输此密语音帧的RTP数据包是否要携带完整的加密同步帧
N
将密语音帧与加密同步信息帧号组成RTP数据包，语音帧类型置为跟随帧。
将RTP包传给被叫
Y
将密语音帧与完整的加密同步信息组成RTP数据包，语音帧类型置为首帧。
将RTP数据包传给被叫

图1



序号	内容	长度bit	说明
1	Ftype	4	语音帧类型标志，1为首帧，0为跟随帧，必选，每包携带
2	CMFN	12	加密同步信息帧帧号，必选，每包携带
3	CMFrame	72	加密同步信息帧，可选，首帧包携带
4	Length	8	填充字段长度，必选

图2

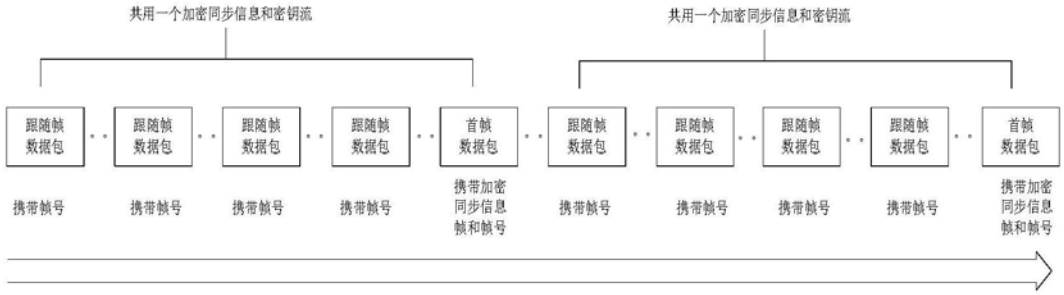


图3

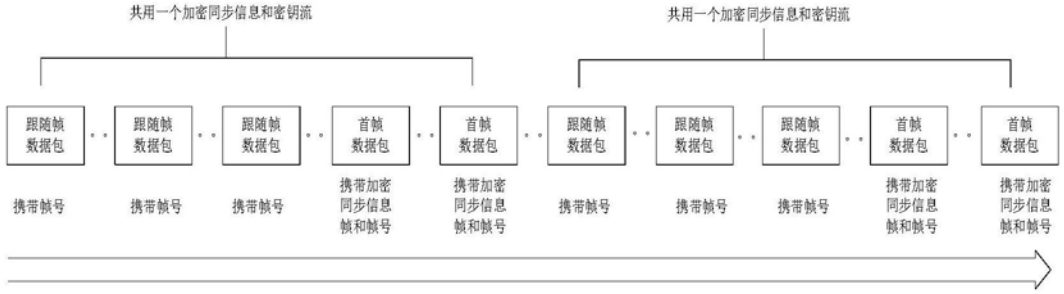


图4

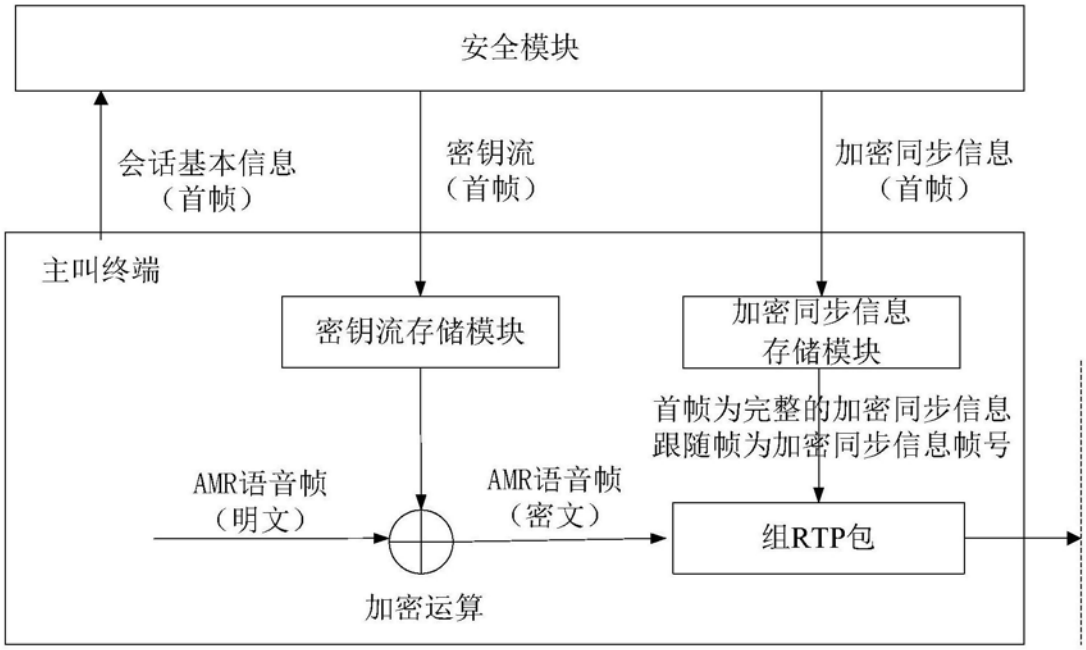

安全模块
会话基本信息
（首帧）
密钥流
（首帧）
加密同步信息
（首帧）
主叫终端
密钥流存储模块
加密同步信息
存储模块
首帧为完整的加密同步信息
跟随帧为加密同步信息帧号
AMR语音帧
（明文）
AMR语音帧
（密文）
组RTP包
加密运算

图5

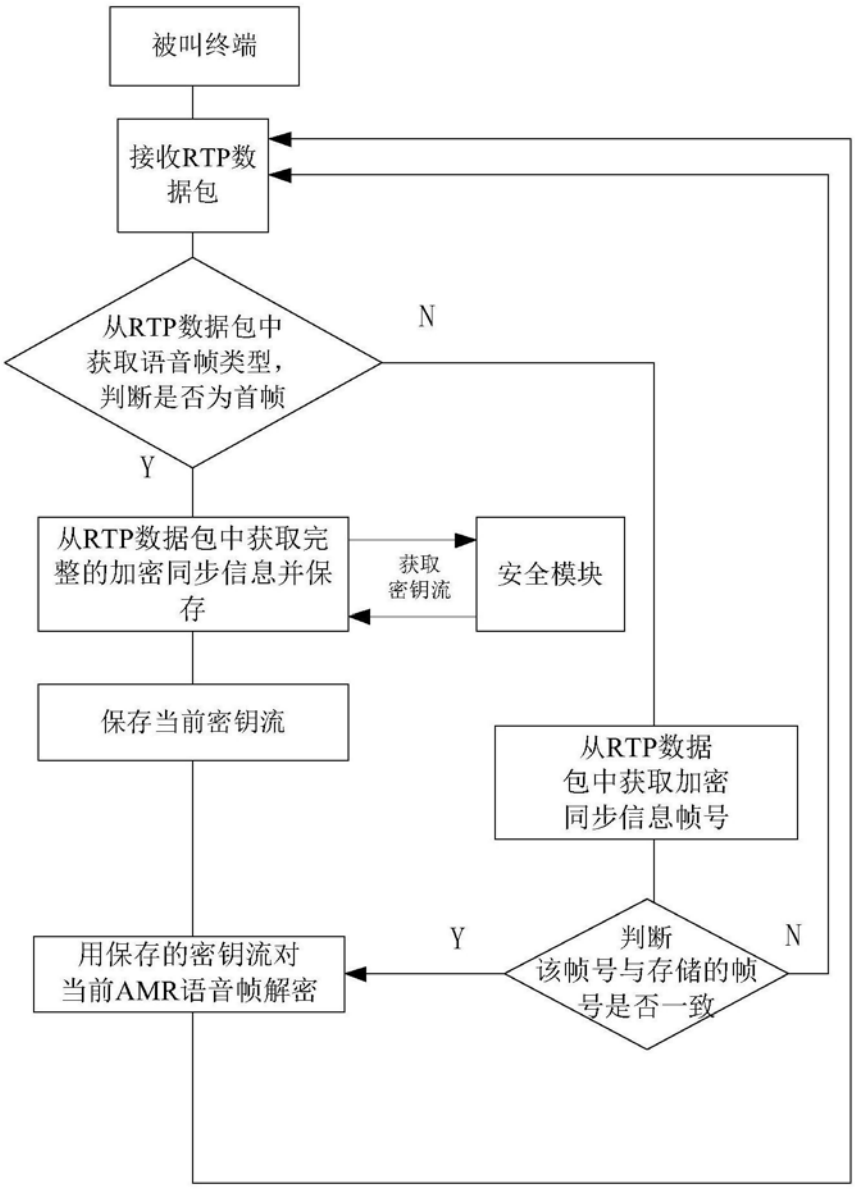

被叫终端
接收RTP数据包
从RTP数据包中获取语音帧类型，判断是否为首帧
N
Y
从RTP数据包中获取完整的加密同步信息并保存
获取密钥流
安全模块
保存当前密钥流
从RTP数据包中获取加密同步信息帧号
判断该帧号与存储的帧号是否一致
Y
N
用保存的密钥流对当前AMR语音帧解密

图6

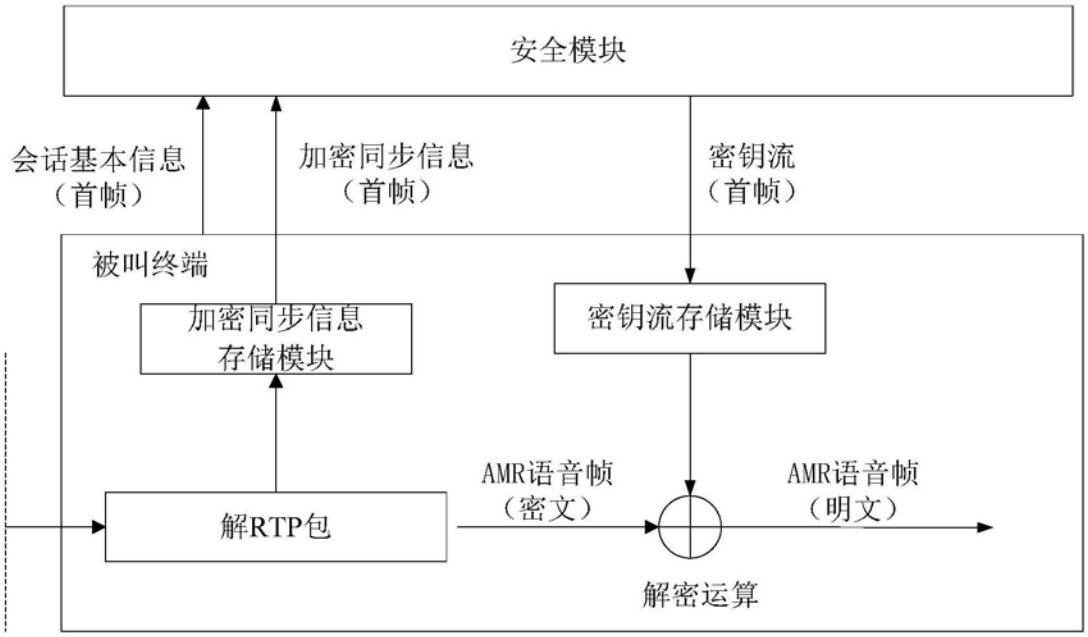

安全模块
会话基本信息
（首帧）
加密同步信息
（首帧）
密钥流
（首帧）
被叫终端
加密同步信息
存储模块
密钥流存储模块
AMR语音帧
（密文）
AMR语音帧
（明文）
解RTP包
解密运算

图7