



(12) 发明专利

(10) 授权公告号 CN 1643839 B

(45) 授权公告日 2012. 09. 05

(21) 申请号 03806687. 4

(22) 申请日 2003. 03. 20

(30) 优先权数据

60/367, 082 2002. 03. 22 US

10/140, 148 2002. 05. 06 US

(85) PCT申请进入国家阶段日

2004. 09. 22

(86) PCT申请的申请数据

PCT/US2003/009078 2003. 03. 20

(87) PCT申请的公布数据

W02003/084123 EN 2003. 10. 09

(73) 专利权人 通用仪器公司

地址 美国宾夕法尼亚州

(72) 发明人 亚历山大·梅德温斯基

(74) 专利代理机构 中国国际贸易促进委员会专

利商标事务所 11038

代理人 李德山

(51) Int. Cl.

H04L 9/00 (2006. 01)

(56) 对比文件

CN 1312991 A, 2001. 09. 12, 全文.

US 4803725 A, 1989. 02. 07, 全文.

US 5535276 A, 1996. 07. 09, 全文.

A. Menezes, P. van Oorschot, S.

Vanstone. Handbook of Applied Cryptography.

CRC Press, 1997, 501-502.

审查员 廖佳佳

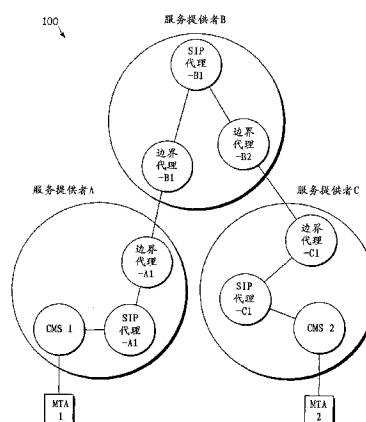
权利要求书 1 页 说明书 4 页 附图 3 页

(54) 发明名称

IP 语音通信系统的媒体流密钥的端对端保护

(57) 摘要

本发明减少了密钥材料对在第一和第二服务器之间的通信信道的中间设备的暴露。在一个实施方式中,第二服务器从第一服务器接收媒体流密钥的第一半。第二服务器使用基于 Kerberos 的应用请求和票证以发送媒体流密钥的第二半给第一服务器。使用此方法,媒体流密钥的暴露被减少到只暴露给服务器。



1. 一种用于在第一和第二服务器之间交换密钥的方法,其中,第一和第二服务器之间的通信路径包括一个或多个中间传输设备,该方法包括:

在第二服务器接收要用于随后的数据传输的部分媒体流密钥,其中该部分媒体流密钥在从第一服务器传输到第二服务器期间未受到保护;

使用一个安全机制以保护要用于随后传输的媒体流密钥的附加部分;以及
通过一个或多个中间传输设备将被保护的媒体流密钥的附加部分传输到第一服务器。

2. 如权利要求1所述的方法,其中该安全机制包括使用 Kerberos 票证。

3. 如权利要求1所述的方法,其中该安全机制包括使用证书。

4. 如权利要求1所述的方法,其中该安全机制包括使用认证符。

5. 如权利要求1所述的方法,其中该安全机制包括使用数字签名。

6. 如权利要求1所述的方法,其中媒体流会话信息被加密、认证并与所述媒体流密钥的附加部分一起被传输到第一服务器。

7. 如权利要求1所述的方法,其中媒体流会话信息未被加密。

8. 如权利要求1所述的方法,其中第一和第二服务器是 IP 语音通信系统中的呼叫管理服务器。

9. 如权利要求1所述的方法,进一步包括从第二服务器发送包括 Kerberos 票证的应用请求到第一服务器以认证第二服务器自身。

10. 如权利要求9所述的方法,其中使用对称服务密钥对该 Kerberos 票证加密。

11. 如权利要求9所述的方法,其中该 Kerberos 票证包括一个对称会话密钥。

12. 一种用于在第一和第二服务器之间交换密钥的装置,其中第一和第二服务器之间的通信路径包括一个或多个中间传输设备,该装置包括

在第二服务器接收要用于随后的数据传输的部分媒体流密钥的装置,其中该部分媒体流密钥在从第一服务器传输到第二服务器期间未受到保护;

使用一个安全机制以保护要用于随后传输的媒体流密钥的附加部分的装置;以及

通过一个或多个中间传输设备将被保护的媒体流密钥的附加部分传输到第一服务器的装置。

IP 语音通信系统的媒体流密钥的端对端保护

[0001] 相关申请的交叉引用

[0002] 本申请从共同未决的美国临时专利申请 No. 60/367, 082 要求优先权, 其于 2002 年 3 月 22 日申请, 名称为 IP 语音通信系统的媒体流密钥的端对端保护, 在此引入作为参考, 对于所有目的, 如同在本文中全文提出一样。

技术领域

[0003] 本发明一般涉及安全数据传输, 尤其涉及安全数据在端对端通信系统中的传输, 该系统使用呼叫信令通过中间传输交换密钥。

背景技术

[0004] 在当今很多系统中, 数字信息的安全通信是非常重要的。例如, 在一个典型的 IP 语音通信 (“voice-over-IP”或“VoIP”) 系统中, 呼叫管理服务器 (CMS) 由 VoIP 服务提供者操作。CMS 与一个数字电话用户连接, 并与另一个位于远程位置的 CMS 连接, 该远程 CMS 又与另一个数字电话用户 (或多媒体终端适配器 (MTA)) 连接。此系统允许用户在诸如因特网的大型网络上互相通话。

[0005] 当然, 用户希望他们的谈话 (和其他数据交换) 是安全的。但是, 要在一个大型, 无定形的网络, 如因特网, 上保持高级别的安全性是很困难的, 在网络中, 信息到达期望的目的地之前, 可能经过多个服务器, 交换机, 路由器, 集线器和其他中间设备。一种维护安全的方法是使两个 CMS 交换通话中所使用的 “媒体流密钥”。现有技术中也存在几种交换此类密钥的方法。例如, 可使用 PacketCable 呼叫信令协议。但是, 这些方法还要求从第一个 CMS 到第二个 CMS 的密钥材料传输, 以及, 随后的从第二个 CMS 到第一个 CMS 的密钥材料交换。当密钥 (或其他数据) 以这种方式交换时, 密钥必须两次经过中间设备。由于每一个中间设备都对数据存在潜在的安全危险, 因此希望最小化密钥对中间设备的暴露。

[0006] 在使用 PacketCable 方法的系统中, 两个电话机, 或 VoIP 终端或 MTA 之间的呼叫信令协议被称为基于网络的呼叫信令 (NCS)。MTA 和 CMS 之间的每一个呼叫信令接口在网络层受到保护。在每一个参与 VoIP 连接的 MTA 由一个单独的 CMS 控制的情况下, CMS 到 CMS 的信令协议是基于会话发起协议 (SIP)。SIP 和其他标准用于确定密钥的交换和管理, 例如, 会话密钥和媒体流密钥。而且, 可以传输认证信息和其他相关数据以初始化会话。这些材料总称为密钥材料。

发明内容

[0007] 本发明减少了密钥材料对在第一和第二服务器之间的通信信道上的中间设备的暴露。在一个实施例中, 第二服务器接收来自第一服务器的媒体流密钥的第一半。第二服务器使用基于 Kerberos 的应用请求和票证 (ticket) 以传输媒体流密钥的第二半到第一服务器。使用这种方法, 媒体流密钥的暴露减少到只暴露给第一和第二服务器。

[0008] 在一个实施例中, 本发明提供了用于在第一和第二服务器之间交换密钥的方法,

其中第一和第二服务器之间的通信路径包括一个或多个中间传输设备。该方法包括,在第二服务器接收用于随后的数据传输的部分媒体流密钥,其中该部分媒体流密钥在从第一服务器传输到第二服务器期间未受到保护;使用一个安全机制保护用于随后的传输的媒体流密钥的附加部分;以及通过上述一个或多个中间传输设备传输受保护的媒体流密钥的附加部分到第一服务器。

[0009] 附图说明

[0010] 图 1 说明服务提供者之间的信令路径;

[0011] 图 2 说明建立安全关联的概述;以及

[0012] 图 3 说明 Kerberos 结构内的被加密和认证的媒体流密钥管理信息。

具体实施方式

[0013] 图 1 中,系统 100 包括第一和第二多媒体终端适配器 (MTA),分别是 MTA1 和 MTA2。呼叫管理服务器 (CMS) 由不同的服务提供者提供。CMS1 接收来自 MTA1 的数据并执行处理和发出信令,从而与期望目标建立安全通信。在本例中,MTA2 是期望目标。

[0014] 通常,一个 VoIP 呼叫可能发生在两个独立的 VoIP 服务提供者之间,这两者都有自己的 CMS。呼叫信令消息在 CMS 之间的中间信令代理 (称为 SIP 代理) 之间被路由,而且,甚至能通过中间服务提供者被路由。

[0015] MTA1 发起的呼叫由 CMS1 控制。CMS1 使用路由信息将 SIP 消息转发到 SIP 代理 -A1。SIP 代理 -A1 路由该消息到边界代理 -A1。边界代理 -A1 路由该消息到中间服务提供者 B。而后,信令消息被路由通过服务提供者 B 内的几个 SIP 代理,而且通过服务提供者 C 内的 SIP 代理。该消息最终到达 CMS2 和其在 MTA2 的目的地。

[0016] 注意,可使用任意数量的中间代理。通常,中间代理可以是接收和转发信令消息或其他信息的设备或进程。使用中间信令代理的说明被描述,例如,在“SIP:会话发起协议”,IETF 请求注释 2543,1999 年 3 月。借此引入这个参考文献作为参考,对于所有目的,如同在本文中全文提出一样。

[0017] 在一个优选实施例中,使用 PacketCable 信令体系。该 PacketCable 体系假定每一个 CMS 和 SIP 代理执行一个目的电话号码的查找,并因此获得 SIP 信令消息应被转发到的下一个主机的地址。该下一个主机可以是目的 CMS 或某一个中间 SIP 代理。与不同信令域的另一个 SIP 代理连接的 SIP 代理称为边界代理。单个 VoIP 服务提供者通常可包括一个或多个信令域。

[0018] 典型地,当呼叫发起 MTA 初始化一条信令消息时,该初始消息包括用于会话的一半密钥材料。呼叫应答 MTA,即图 1 实例中的 MAT2,用第二半密钥材料响应。当任意一个 MTA 都在消息中包含密钥材料时,该密钥材料不仅在这两个 CMS,而且在每一个中间代理处暴露。虽然每一个 SIP 代理可能被一个可信任的服务提供者拥有或操作,但该信令体系在潜在的大量的节点暴露媒体流密钥。危及任何一个节点的安全都将危及媒体流的隐私。

[0019] 当 MTA1 产生其部分 (例如,一半) 密钥材料并将其发送给 CMS1 时,由于 CMS1 不知道 CMS2 的身份,CMS1 无从选择只能通过中间 SIP 代理发送密钥材料。但是,在第一个呼叫信令消息被 CMS2 接收后,仅在中间 SIP 代理暴露一半媒体流密钥。

[0020] 在这点上,无一 SIP 代理拥有完整的媒体流密钥。而且,CMS2 知道 CMS1 的身份。

现在, CMS2 可以在剩下的一半密钥被返回到 CMS1 之前将其加密。即使返回信令消息将通过 SIP 传回,但相关的媒体流密钥管理材料可被加密,因此,它仅能被 CMS1 解密(而后转发到 MTA1)。这种实现可以使应用层安全,因为在 PacketCable 体系内,从 CMS2 返回到 CMS1 的第一信令消息通过中间 SIP 代理路由。

[0021] 保护 CMS2 上的一半媒体流密钥的一种方法是,为 CMS2 查询 CMS1 的数字证书,然后用其加密密钥材料。可以使用在一个或多个 CMS 的密码加速器以提高此种方法的速度。

[0022] 或者, CMS1 和 CMS2 可提前协商某一对称密钥,而后 CMS2 可用其加密一半媒体流密钥。这就要求除了必须维护的 IPsec 密钥之外, CMS 还应为应用层安全维护一个独立的加密密钥表。这种方法的一个缺点是其要求更多由于获取和维护密钥的处理“开销”。

[0023] 本发明的一个优选实施方式使用一个名为 Kerberos 的流行的认证服务。对于 IPsec 和密钥创建, PacketCable 体系已经利用了 Kerberos 密钥管理,因此可预计,标准系统中的每一个 MTA 和 CMS 都将支持 Kerberos。注意,虽然优选实施方式使用 Kerberos 机制,但其他认证服务或安全数据传输技术也可与本发明一起使用。可以找到关于 Kerberos 密钥管理协议的细节,例如,在“Kerberos 网络认证服务 (V5)”IETF 请求注释 1510,1993 年 9 月。

[0024] 图 2 所示是概述如何用 Kerberos 在一对 CMS 或 SIP 代理之间建立 IPsec SAs(安全关联),其中 IPsec SA 包含一组用于加密和认证 IP 分组的对称密钥。图 2 所示是第一 CMS 向密钥分发中心(KDC)认证自身,KDC 是与其每一个客户共享对称密钥的可信任的权威。其通过发送认证(AS)请求或票证授予服务(TGS)请求消息来完成。同样,KDC 在给 CMS1 的返回消息(AS 应答或 TGS 应答)中认证自身,并在应答中包含一个 Kerberos 票证。

[0025] Kerberos 票证与数字证书类似,因为票证持有者可用其向另一方认证自身。或者,可使用任意类型的数字证书。但是,不像一般的数字证书,Kerberos 票证仅用于认证一个特定的服务器——票证中所指定的服务器。也可使用较快的对称密钥密码算法加密票证并带来比数字证书少的开销。

[0026] 虽然本发明的优选实施方式使用 Kerberos 票证,其他实施方式也可使用不同的安全机制。例如,可以使用其他(即,非 Kerberos)票证格式。票证,证书,认证符,数字签名,或其他安全机制可用于取代或补充本发明的优选实施方式所用的安全机制。

[0027] CMS1 收到票证之后,能够向 CMS2 认证自身,同样, CMS2 也将向 CMS1 认证自身,两者将能建立一组共享的 IPsec 密钥。详细说明 Kerberos 化的 IPsec 在,例如,“PacketCable™安全规范”,PKT-SP-SEC-I02-001229,有线电视实验室公司,2000 年 12 月。

[0028] 一种优选实施方式允许 CMS2 获取 CMS1 的 Kerberos 票证,然后使用该票证加密和认证一半媒体流密钥以及所选的加密算法和数据(即,“密钥套件”)。产生的 Kerberos 认证符,媒体流密钥和所选的密钥套件如前一样,在 SDP 选项中返回。注意,在此情况下,是 CMS2 获取 CMS1 的票证,与图 2 所示的情况相反。

[0029] 图 3 所示是 KRB-PRIV Kerberos 结构中被加密和认证的媒体流密钥管理信息。该 KRB-PRIV 结构前面是一个 Kerberos 应用(AP)请求对象,其包括一个 Kerberos 票证。为了说明方便,在此仅讨论相关的 Kerberos 对象。Kerberos 服务的细节可在所引用的参考文献和其他合适的参考文献中找到。用对称服务密钥加密票证,该密钥仅为 CMS1 和 KDC 所共享,而对于 CMS2 或网络中的任何其他节点是不可用的。因此,此特殊票证可由 CMS1(此 SDP

内容的预定目标)解密并验证,而不能被 CMS2 更改,CMS2 不拥有解密该票证所必需的服务密钥。这意味着,票证持有者 CMS2,若篡改票证中所包含的信息必将被发现。如上所述,替代的实施方式可以使用数字证书,或其他形式的安全保护机制。

[0030] 票证包括一个对称会话密钥。虽然 CMS2 不能解密该票证和读取其内容,但它有其自己的与 KDC 安全发送(例如,在 AS 应答或 TGS 应答消息中)的会话密钥完全一样的拷贝。CMS2 已经拥有该会话密钥,并且 CMS1 能解密该票证并从中抽取会话密钥。一旦 CMS1 接收该票证,它将与 CMS2 共享该会话密钥。

[0031] 本发明的一个优选实施方式使用会话密钥以加密和认证媒体流密钥管理信息,包括一半媒体流密钥和所选的密钥套件。票证与被保护信息一起发送,因此,CMS1 将能够提取解密和确认密钥管理数据所需的会话密钥。但是,对于完整的 Kerberos 认证,仅仅发送票证是不够的。为了能使 CMS2 向 CMS1 认证其自身,它必须发送一个 AP 请求(其中包括票证)。

[0032] 此解决方案将引入的唯一的附加消息是 CMS2 和 KDC 之间为获取 CMS1 票证的交换。但是,Kerberos 票证通常被缓存并重用直到某一过期时间——PacketCable 中票证可持续至多一个星期。因此,此开销仅会影响较小比例的呼叫。而且,由于 CMS2 和 CMS1 也直接交换一些信令消息,最后它们将请求 IPsec 安全关联,所以,同样的 Kerberos 票证可为此目的而重用。

[0033] 在优选实施方式中,票证是由 KDC 分发给客户的认证标记。在其他信息中,票证包含客户名,特定服务器名和会话密钥(对称加密密钥)。客户名和会话密钥需要保密并用另一密钥加密,该密钥被称为服务密钥。服务密钥仅为 KDC 和票证中指定的服务器所知。由于客户并不拥有此服务密钥,因此,他不能解密票证和改变其内容。通常,客户也需知道会话密钥,由于他不能从票证中获取该密钥,所以 KDC 给客户发送同一会话密钥的单独的拷贝。

[0034] 为了用票证认证一条消息,客户应在该消息中包含票证和认证符,该认证符包括一个使用票证中存在的会话密钥计算的加密的校验和。注意,该票证中的会话密钥使用服务器的服务密钥加密。当票证中指定的服务器收到来自客户的消息时,它能用其服务密钥解密该票证,验证客户名并获取会话密钥。而后,该会话密钥将被用于验证加密的校验和并因此认证该消息。

[0035] 因此,本发明减少了密钥材料的暴露。虽然,关于 Kerberos 讨论了本发明,其他实施方式也可使用其他方法。但是,Kerberos 是 PacketCable 安全体系的不可缺部分,因此其使用无须引入一个新的协议或新的密钥管理基础设施。而且,Kerberos 提供了一个密钥管理解决方案,从而避免了与 PKI(公钥基础设施)相关的开销。对于媒体流密钥暴露在中间网络单元的问题,其提供了一个有效的解决方案。

[0036] 注意,本发明的其他实施方式不必是基于 PacketCable 体系的系统。本发明的范围仅由所附权利要求书确定。

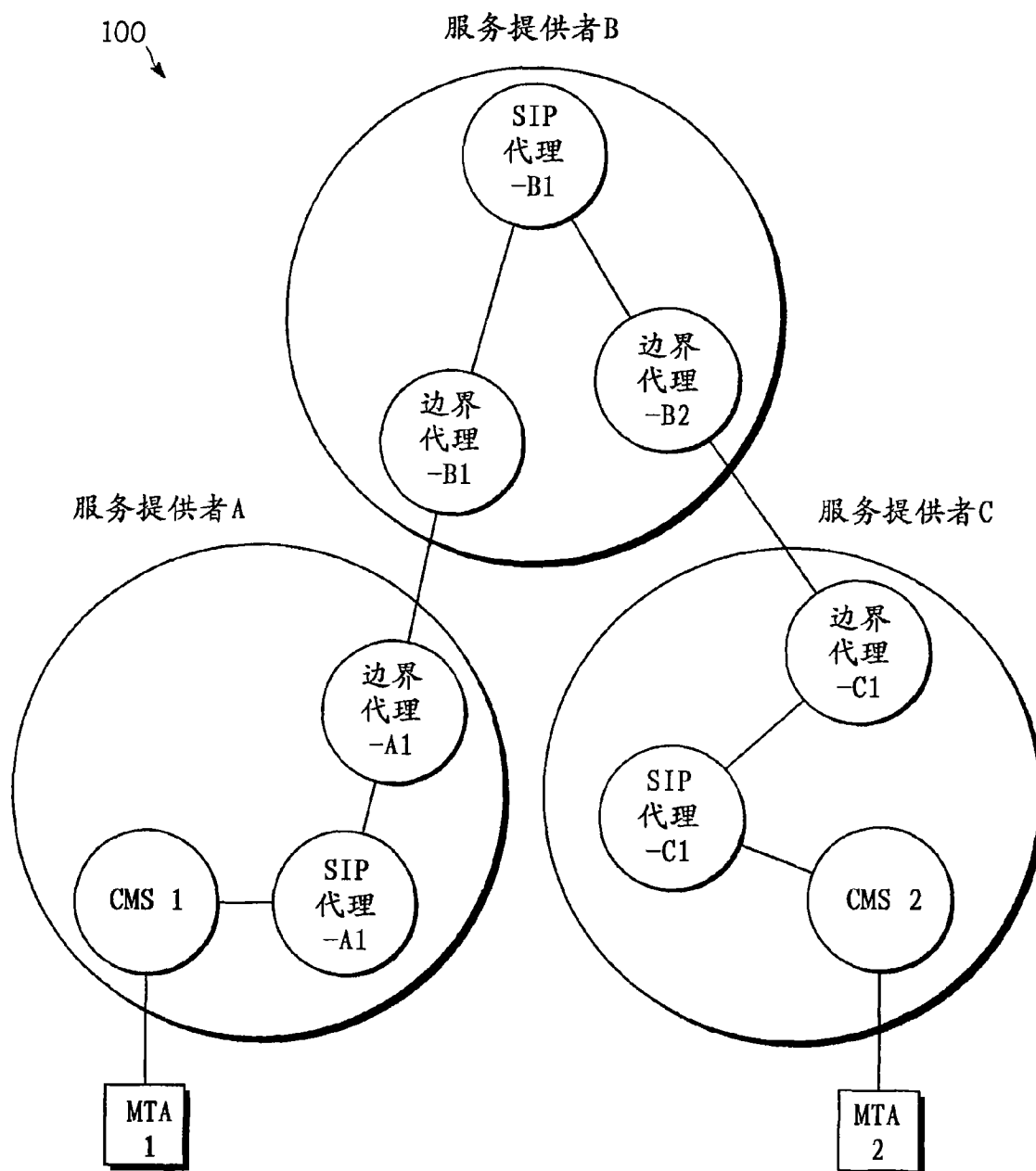


图 1

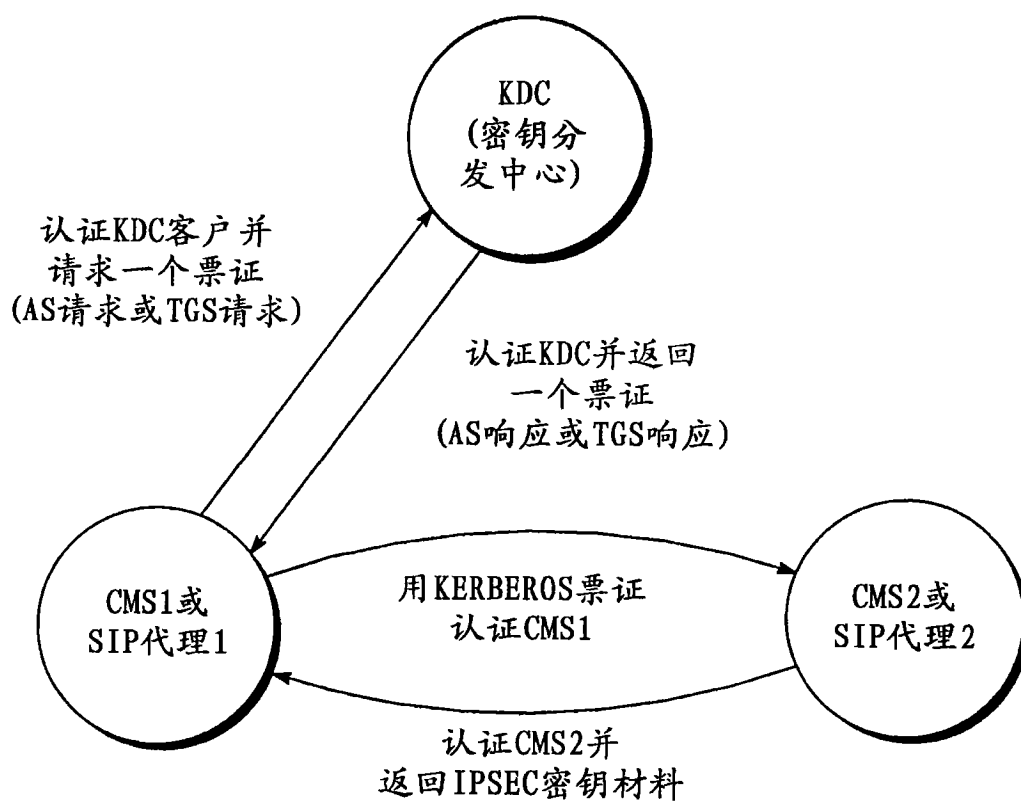


图 2

图 3

