



(12) 发明专利申请

(10) 申请公布号 CN 102859945 A

(43) 申请公布日 2013.01.02

(21) 申请号 201180020641.8

代理人 杨晓光 于静

(22) 申请日 2011.05.02

(51) Int. Cl.

(30) 优先权数据

H04L 12/28 (2006.01)

61/329,916 2010.04.30 US

13/069,989 2011.03.23 US

(85) PCT申请进入国家阶段日

2012.10.24

(86) PCT申请的申请数据

PCT/US2011/034794 2011.05.02

(87) PCT申请的公布数据

W02011/137439 EN 2011.11.03

(71) 申请人 株式会社东芝

地址 日本东京都

申请人 特勒克利亚科技公司

(72) 发明人 大场义洋 神田充 S·达斯

D·法莫拉里

(74) 专利代理机构 北京市中咨律师事务所

11247

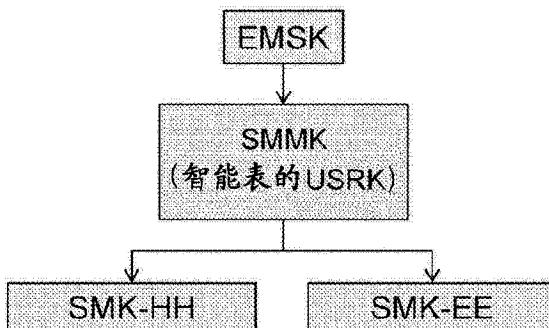
权利要求书 2 页 说明书 14 页 附图 7 页

(54) 发明名称

具有密钥更新机制的密钥管理设备、系统和方法

(57) 摘要

根据一些实施例，用于部署在适于经由网络从与至少一个中继相连的智能表接收计量数据的智能电网系统中的密钥管理装置包括：密钥控制机制，其从一个主密钥导出单独的专用密钥的密钥阵列，以便对于应用中的每个特定使用或者如果应用中仅有一个特定使用则对于每个应用，所述密钥阵列中的专用密钥每个都是独立的加密密钥。



1. 一种用于通信设备的密钥更新方法，包括：

提供密钥控制机制，其从一个主密钥导出单独的专用密钥的密钥阵列，以便对于每个应用或者对于所述应用中的不同使用，所述密钥阵列中的专用密钥每个都是独立的加密密钥。

2. 根据权利要求 1 所述的方法，其中所述密钥控制机制为每个应用从一个主密钥导出应用主密钥，并且从所述应用主密钥导出所述密钥阵列。

3. 根据权利要求 2 所述的方法，其中在同一时间所述密钥阵列中仅有一个专用密钥有效，并且

当有效专用密钥需要密钥更新时，所述密钥控制机制将与所述有效专用密钥对应的阵列索引值存储为已用，并且使用来自所述密钥阵列的未使用的专用密钥之一作为新有效专用密钥。

4. 根据权利要求 3 所述的方法，其中所述密钥控制机制使用具有等于所存储的阵列索引值加一的索引值的专用密钥作为新有效专用密钥。

5. 根据权利要求 1 所述的方法，其中所述密钥控制机制将所述密钥阵列的阵列大小设置为与更新所述专用密钥的频率成比例的值。

6. 根据权利要求 1 所述的方法，其中所述密钥控制机制通过协商对使用所述专用密钥的应用的控制消息的使用来确定所述密钥阵列的阵列大小。

7. 根据权利要求 1 所述的方法，其中每个应用消息包括与加密使用的所述专用密钥对应的阵列索引值。

8. 根据权利要求 7 所述的方法，其中当有效专用密钥需要密钥更新时，所述密钥控制机制通过包括新有效专用密钥的阵列索引值的应用消息来通知对方实体的密钥更新。

9. 根据权利要求 7 所述的方法，其中当有效专用密钥需要密钥更新时，所述密钥控制机制通过包括新有效专用密钥的阵列索引值的控制消息来通知对方实体的密钥更新。

10. 根据权利要求 1 所述的方法，其中：所述通信设备是智能表。

11. 根据权利要求 10 所述的方法，其中所述智能表用于与电动车辆、家用器具、太阳能电池、可充电电池或其他设备的使用相关的计量。

12. 根据权利要求 11 所述的方法，其中所述智能表计量消耗或使用信息，并且经由通信网络将该信息传达回提供商以进行监控和计费。

13. 一种配置成从多个计量设备接收数据的通信设备，其中所述多个计量设备与分布在电网网络中的中继相连，所述通信设备包括：

密钥控制机制，其从一个主密钥导出单独的专用密钥的密钥阵列，以便对于每个应用或者对于所述应用中的不同使用，所述密钥阵列中的专用密钥每个都是独立的加密密钥。

14. 根据权利要求 13 所述的通信设备，其中：所述设备是仪表数据管理服务器。

15. 根据权利要求 13 所述的通信设备，其中所述多个计量设备中的每一个是用于与电动车辆、家用器具、太阳能电池、可充电电池或其他设备的使用相关的计量的智能表。

16. 一种通信网络系统，包括：

配置成将计量数据推送到网络的多个低处理功率设备；以及

具有仪表数据管理服务器的通信设备，所述仪表数据管理服务器被配置成经由至少一个中继节点与所述多个低处理功率设备的每一个相连以接收被所述多个低处理功率设备

的每一个推送到网络的所述计量数据，

其中所述通信设备通过实现统一密钥管理机制与所述多个低处理功率设备的每一个通信，从而以适合多层和多协议环境的方式避免经由简单的统一密钥管理构架的多层次认证，其中所述统一密钥管理机制从单个对等实体认证尝试生成用于多个通信层的多重协议的加密密钥。

17. 根据权利要求 16 所述的系统，其中：密钥管理机制是基于引导多重协议的加密的。
18. 根据权利要求 16 所述的系统，其中：所述系统是智能电网系统。
19. 根据权利要求 16 所述的系统，其中所述多个低处理功率设备中的每一个是用于与电动车辆、家用器具、太阳能电池、可充电电池或其他设备的使用相关的计量的智能表。
20. 根据权利要求 16 所述的系统，其中所述至少一个中继被配置成经由无线网络从所述多个低处理功率设备收集计量数据。

具有密钥更新机制的密钥管理设备、系统和方法

[0001] 相关申请的交叉引用

[0002] 本申请要求于 2011 年 3 月 23 日提交的美国专利申请 No. 13/069989 的权益，该美国专利申请 No. 13/069989 要求于 2010 年 4 月 30 日提交的美国临时申请 No. 61/329,916 的优先权，以引用的方式将其全部内容合并于此。

背景技术

[0003] 1、技术领域

[0004] 此处描述的优选实施例一般涉及智能电网通信以及其它通信。特别地，涉及不依赖使用同一主会话密钥的各个应用的加密密钥的密钥更新的频率的密钥管理机制。

[0005] 2、背景讨论

[0006] 当今世界能源资源的高效使用和管理正变得越来越重要。许多国家正通过使用技术发展水平的通信和信息技术向系统增加性能而给予电力网现代化重视。该转换在智能电网倡议的保护下发生，电力网由此增加高级功能，诸如监控、分析、控制和双向通信性能。目标是节约能源、降低成本和提高可靠性与透明性。虽然现今存在这些特征和性能中的许多，但它们是孤立存在的并且由单独的 ESP 控制。智能电网的目标是创建具有上述高级功能的基础设施，从而通过对能源资源的高效使用来最大限度地提高电网系统的吞吐量。

[0007] 智能电网互操作性项目和电气电子工程师协会标准机构已意识到实现该目标的最好方式是创建由多种不同的技术和层组成的通信网络。该通信网络可从广域网 (WAN) 到用户驻地网，诸如家域网 (HAN) 或商业网 (BAN)。例如，高级计量、家用器具可以连接到 HAN 或者 BAN，然后可以使用 WAN 将信息传送到 ESP。该系统有可能转变成类似于当今的因特网的信息高速公路，其可以潜在地使得团体中的所有风险承担者能够比现今更高效地交互、监控和管理系统。

[0008] 在电力服务提供商 (ESP) 为通信和信息技术的性能振奋时，他们同样关心可能没有电力网的组件通过其进行连接的任何物理界限的事实。例如，不像传统的输电网，高级计量系统可以通过因特网或者通过无线网络连接到 ESP，无线网络容易被攻击并且容易被窃听或欺骗，这可能最终损害输电网的安全性和可靠性。因此，通信和信息安全正变成采用这种技术的主要需求之一。因此，绝对需要保护网络以提供在其上承载的信息是安全的和可靠的保障。

[0009] 尽管现今可有大量的安全技术来处理通信网络安全，但智能电网环境是不同的，因此有不同的需求。例如，高级计量系统中的电表或煤气表或者智能表是具有个人局域无线网络技术(诸如，Zigbee (参见背景技术参考文献 8))的低处理功率设备。这些设备通常被认为是典型地具有 4-12K 的 RAM 和 64-256K 的闪存的低成本无线设备。通常这些设备使用低带宽链路连接到回程。该链路特性还可以根据诸如睡眠或者空闲操作模式的无线射频特征 (wireless radio features) 变化。例如，高级计量系统可以周期性地活跃 (wake up) 以与网络同步，从而节约电力而不是一直保持活跃。设备的附加需求可以包括：i) 支持使用网状拓扑的多跳网络(例如，以延伸追溯的回程)；ii) 支持多链路层技术。这些需求要

求必须优化协议开销和性能。

[0010] 在简单的计量数据之外,高级仪表还可以用于其他目的。如背景技术参考文献 1 中公开的 ANSI C12.12 允许通过中继或者集中器使用高级仪表对等操作。其他应用(诸如,如背景技术参考文献 5 中的 COAP)可能能够在单个仪表上同时地运行。尽管这些是非常有吸引力的特征并且使得高级仪表从经济效益来看更切实可行,但他们为安全性增加了附加需求,诸如,每个应用需要认证并且需要对系统(例如,计费系统)保持数据的完整性。

[0011] 密钥管理是备受关注的领域,尤其是在基于浏览器的 web 应用中。最明显地,已出现诸如(背景技术参考文献 11 中提及的) OAuth、(背景技术参考文献 12 中提及的) OpenID、(背景技术参考文献 13 中提及的) SAML 的倡议和其它以提供单点登录(SSO)能力。 OAuth 是大众化的 SSO 使能器(enabler)。其提供使终端用户在不需要与第三方共享静态证书的情况下授权第三方访问网络资源的机制。 OAuth 通过用户代理重定向和临时发布的与第三方共享的密钥来完成该机制。另一大众化的 SSO 技术是 OpenID,其已通过商业 web 服务获得广泛动力(momentum),并且用于几个著名的 web 服务提供商,诸如 Google、Yahoo!、AOL 和 facebook 等。 OpenID 是开放的、分散接入控制机制,其允许用户使用单个数字身份登录到几个不同的服务。OpenID 需要规律地登录到订户的服务提供商以访问由每个服务提供商提供的服务。也有关于与 OpenID 关联的刚开始显露的脆弱性的安全问题。

[0012] 例如,在背景技术参考文献 14 中,作者处理了认识到的限制,诸如对称加密、认证状态的持续时间存储在中继提供商和 OpenID 提供商处、以及对中间人类型的攻击的脆弱性。安全断言置标语言(SAML)是在诸如企业网络的安全域之间提供认证和授权数据的技术。SAML 定义在 XML 中,并且使用联合身份管理技术来缓和跨越同一联盟下的域的认证和授权任务。在背景技术参考文献 15 中,作者关于可导致 SAML 的易受攻击的实现的机密性、双边认证、完整性和用户跟踪来识别几个安全缺陷。

[0013] 然而,OAuth、OpenID 和 SAML 没有彻底解决需要跨层密钥管理的统一的密钥管理。一些技术已通过尝试如背景技术参考文献 16 和 17 中所描述的与 EAP 结合解决了 Kerberos 内网络接入认证的缺乏。然而,这些技术需要修改的 EAP 方法以与 Kerberos 交互。

[0014] 同样,诸如 EAP(可扩展的认证协议)、PANA(网络接入认证传输协议)和 ANSI C12.22(数据通信网络接口协议规范)的通信协议是已知的。

[0015] 例如,ANSI C12.22 是智能电网通信中的仪表应用协议。ANSI C12.22 使用 EAX'。EAX' 是分组加密算法,其为 EAX 与 128 比特 AES 的组合,并且使用对称加密密钥(cryptographic key)(或者加密密钥(ciphering key))提供数据加密,从而提供应用层加密(ciphering)。ANSI C12.22 允许两个或更多个加密密钥用于同一对等体,并且在会话开始时从这些密钥中选择一个加密密钥。

[0016] 然而,随着使用同一加密密钥加密的数据量增加,密钥被使用的强度被削弱,因为 ANSI C12.22 没有定义对 EAX' 的加密密钥进行动态密钥更新的机制。因此,需要提供针对 ANSI C12.22 加密密钥的密钥更新机制。

[0017] 在由 Oba, Y 于 2010 年 11 月提交的题为“用于传送加密信息的终端(Terminal for transmitting encrypted information)”的 PCT 申请 JP2009_69982 (背景技术参考文献 2) 中示出了使用 EAP 的方法。该方法旨在从由 EAP 认证生成的一个 EMSK (扩展的主密钥) 生成 ANSI C12.22 的加密密钥。当需要 C12.22 的密钥更新时,其执行 EAP 重认证以从新生

成的 EMSK 生成 ANSI C12.22 的新加密密钥。

[0018] 作为上述 PCT 申请 JP2009_69982 中定义的密钥更新方法的加强,考虑从同一 EMSK 生成两个或更多个应用加密密钥的用例。

[0019] 由于当需要 EMSK 的任何派生(descendant)密钥的再生(renewal)时,将需要发生 EAP 重定向以对 EMSK 进行密钥更新,因此将发生使用同一 EMSK 对所有应用的加密密钥的再生。

[0020] 尽管加密密钥的密钥更新频率通常依赖于各个应用的特性,如果发生需要更高的密钥更新频率的应用的加密密钥的密钥更新,则将导致不需要这种高密钥更新频率的其它应用的加密密钥的不必要的密钥更新。

[0021] 为了解决该问题,需要一种密钥管理机制,其中 EAP 重认证的频率不依赖于使用同一 EMSK 的各个应用的加密密钥的密钥更新频率。

[0022] 3、背景技术参考文献

[0023] 以引用的方式将下列背景技术参考文献的全部内容合并于此:

[0024] 1. 美国国家标准。数据通信网络接口协议规范。ANSI C12.22-2008。2008 年(以下称之为【1】)。

[0025] 2. Oba. Y, 用于传送加密信息的终端,JP2009_69982,2010 年 11 月, PCT 申请(以下称之为【2】)。

[0026] 3. Salowey J., 从扩展的主会话密钥(EMSK)派生根密钥的规范。(以下称之为【3】)。

[0027] 4. Aboba B., 可扩展的认证协议(EAP), (以下称之为【4】)。

[0028] 5. Shelby Z., CoAP 需求和特征。(以下称之为【5】)。

[0029] 6. Forsberg D., 网络接入认证传输协议(PANA) (以下称之为【6】)。

[0030] 7. 智能电网互操作性标准项目(以下称之为【7】)。

[0031] 8. ZigBee 联盟。ZigBee 规范。ZigBee 文献 053474r18,2009 年 6 月(以下称之为【8】)。

[0032] 9. A. Patrick, J. Newbury 和 S. Gargan, 电子供应工业中的双向通信系统, IEEE 输电汇刊,13:53-58,1998 年 1 月(以下称之为【9】)。

[0033] 10. Smart Power Directorate (以下称之为【10】)。

[0034] 11. Hammer-Lahav E. OAuth 1.0 协议,2010 年(以下称之为【11】)。

[0035] 12. OpenID 认证 2.0 - 最终技术规范(以下称之为【12】)。

[0036] 13. 动态安全断言置标语言 :简化单点登录。Harding P., Johansson L., Klingenstein N.: IEEE 信息安全与保密杂志,2008 年 8 月(以下称之为【13】)。

[0037] 14. OhHyun-Kyung, JinSeung-Hun, The Security Limitations of SS0 in OpenID. :ICACT,2008 年(以下称之为【14】)。

[0038] 15. Security analysis of the SAML single sign-on browser/artifact profile. Gross T.: 计算机安全应用研讨会 2003 年(以下称之为【15】)。

[0039] 16. Ohba Y., Das S., Dutta A., Kerberized handover keying:a media-independent handover key management architecture. :ACM MobiArch 2007 (以下称之为【16】)。

[0040] 17. A Kerberized Architecture for Fast Re-authentication in Heterogeneous Wireless Networks. Lopez R., Garcia F., Ohba Y.: 移动网络与应用,2010

年(以下称之为【17】)。

[0041] 18. AbobaB., SimonD., EronenP. 可扩展的认证协议(EAP)密钥管理架构。2008年8月(以下称之为【18】)。

[0042] 19. KaufmanC. 因特网密钥交换(IKEv2)协议。2005年5月(以下称之为【19】)。

[0043] 20. Vogt C. 关于第一跳IP源地址确认的解空间分析(A Solution Space Analysis for First-Hop IP Source Address Validation)。2009年1月(以下称之为【20】)。

[0044] 21. OhbaY., YeginA., PANA客户端与实施点之间主密钥的定义(Definition of Master Key between PANA Client and Enforcement Point),2009年(以下称之为【21】)。

[0045] 22. ZigBee 联盟。ZigBee Smart Energy ProfileTM 2.0 技术需求文件,2010年(以下称之为【22】)。

[0046] 23. Narayanan V., Dondeti L. 关于EAP重认证协议(ERP)的EAP扩展,2008年8月(以下称之为【23】)。

附图说明

[0047] 通过参考附图详细描述其示例性实施例,本发明的实施例的上述和其它特征及优势将更加显而易见,其中:

[0048] 图1是示出了实施例的密钥分层结构的示意图;

[0049] 图2是示出了基于实施例的EAP密钥管理构架的密钥管理机制的示意图;

[0050] 图3是示出了实施例的网络配置的示意图;

[0051] 图4是示出了用于建立实施例的MSK和EMSK的顺序的示意图;

[0052] 图5是示出了实施例的ANSI C12.22注册服务的顺序的示意图;

[0053] 图6是示出了实施例的ANSI C12.22解析(resolve)服务的顺序的示意图;

[0054] 图7是示出了实施例的COAP/HTTP的顺序的示意图;

[0055] 图8是示出了实施例的密钥更新的顺序的示意图;

[0056] 图9是示出了实施例的基于EAP的完全统一的模型与部分统一的模型的示意图;

[0057] 图10示出了实施例的高级计量系统架构的基本组件;

[0058] 图11示出了将很多智能表与一个可能的实施例的公用事业管理处进行映射的一个可能的配置。

具体实施方式

[0059] 虽然本发明可以体现在许多不同的形式中,但此处描述的许多说明性实施例应理解为将本公开认为是提供了本发明的原理的示例,并且这些示例不意在将本发明限制为此处描述和/或图示的优选实施例。

[0060] 引言:

[0061] 本发明的优选实施例克服了现有技术中的各种不足。

[0062] 根据一些实施例,通过示例的方式,为智能表提供了一种密钥更新方法,该方法包括:提供从一个主密钥导出单独的专用密钥的密钥阵列的密钥控制机制,以便对于每个应用或者应用中的不同使用,密钥阵列中的专用密钥每个都是独立的加密密钥。在一些示例

中,该方法包括所述密钥控制机制从一个主密钥导出每个应用的应用主密钥,并且从应用主密钥形成密钥阵列。在一些示例中,该方法包括在同一时间密钥阵列中仅一个专用密钥有效,并且当有效专用密钥需要更新密钥时,密钥控制机制将与有效专用密钥对应的阵列索引值存储为已用,并使用来自密钥阵列的未使用的专用密钥之一作为新的有效专用密钥。在一些示例中,密钥控制机制使用具有等于所存储的阵列索引值加一(1)的阵列索引值的专用密钥作为新的有效专用密钥。在一些示例中,所述密钥控制机制将密钥阵列的阵列大小设置为与更新专用密钥的频率成比例的值。在一些示例中,密钥控制机制通过协商使用应用的控制消息来确定密钥阵列的阵列大小,其中该应用使用专用密钥。在一些示例中,密钥控制机制通过协商使用 EAP、EAP 认证方法或者 EAP 传输协议来确定密钥阵列的阵列大小。在一些示例中,密钥控制机制使用 PANA 作为 EAP 传输协议。在一些示例中,主密钥是 EMSK。在一些示例中,密钥导出因子的参数包括与密钥阵列的专用密钥对应的阵列索引值。在一些示例中,每个应用消息包括与加密使用的专用密钥对应的阵列索引值。在一些实施例中,当有效专用密钥需要密钥更新时,密钥控制机制通过包括新的有效专用密钥的阵列索引值的应用消息来通知对方(opposite)实体的密钥更新。在一些实施例中,密钥控制机制使用 ANSIC12.22 作为应用。在一些实施例中,当有效专用密钥需要密钥更新时,密钥控制机制通过包括新的有效专用密钥的阵列索引值的控制消息来通知对方实体的密钥更新。在一些实施例中,密钥控制机制使用 COAP 作为应用。

[0063] 根据本发明的一些其它实施例,提供了一种智能表,包括:密钥控制机制,其从一个主密钥导出单独的专用密钥的密钥阵列,以便对于每个应用或者应用中的不同使用,密钥阵列中的专用密钥每个都是独立的加密密钥。

[0064] 根据本发明的一些其它实施例,提供了一种通信网络系统,包括:统一的密钥管理机制,其从单个对等实体认证尝试生成用于多个通信层的多重协议的加密密钥,以便以适于多层和多协议环境的方式避免经由简单的统一的密钥管理构架的多层次认证。在一些示例中,该系统进一步包括支持引导多重协议的加密的密钥管理构架。在一些实施例中,该系统是智能电网系统。

[0065] 结合附图鉴于下列描述将进一步理解各种实施例的上述和 / 或其它方面、特征和 / 或优势。适用时,各种实施例可以包括和 / 或排除不同的方面、特征和 / 或优势。此外,适用时,各种实施例可以组合其它实施例的一个或多个方面或特征。不应将特定实施例的方面、特征和 / 或优势的描述解释为对其它实施例或权利要求的限制。

[0066] 详细讨论

[0067] 在优选实施例中,从一个 EMSK 导出用于同一目的并且彼此独立地加密的两个或更多个专用密钥作为解决这些问题的途径。这里,专用密钥是应用的加密密钥,并且可以针对应用中的各个具体使用进行定义,如果应用中只有一个具体使用,则可以针对各个应用进行定义。同一使用的两个或更多个专用密钥的阵列被称为专用密钥阵列。同一专用密钥阵列可用于保护在通信的两个方向中具体使用的数据,或者可在每个方向中使用截然不同的专用密钥阵列。如果应用协议自身具有加密机制,则生成的专用密钥可用于对为对应的使用定义的应用协议消息的加密。

[0068] 如果应用协议自身不具有加密机制,但是应用协议的传输协议具有加密机制,则生成的专用密钥可用于加密承载应用协议的消息的传输协议消息。从为每个应用生成的应

用主密钥(APMK)导出专用密钥阵列。

[0069] 使用在【3】中定义的密钥导出算法将APMK 定义为从EMSK 导出的USRK(特定使用的根密钥:Usage Specific Root Key)。APMK=KDF(EMSK, 密钥标签 | "Y0" | 可选数据 | 长度)—这里,例如,application1@ietf.org 是密钥标签通过其指定绑定到APMK 的应用的字符串。

[0070] 可选数据参数是NULL(0x00),并且长度是八位字节的密钥长度,该长度取决于应用。对于KDF(密钥导出函数)的定义,参考【3】。专用密钥阵列PK 的第 i 个阵列元素PK[i]如下所示从APMK 导出。

[0071] PK[i]=KDF(APMK, 密钥标签 | "Y0" | 可选数据 | 长度)—这里,密钥标签是唯一地识别在应用中的使用的字符串,例如,使用Application 1FunctionX@ietf.org;“i”至少包括在可选数据中。此外,可选数据中可包括其它信息。

[0072] 当把专用密钥阵列用于通信的一个特定方向时,也可以包括关于使用密钥的该方向的信息。长度参数是八位字节的密钥长度并且取决于使用。对于KDF(密钥导出函数)的定义,参考【3】。专用密钥阵列的大小可对于每个应用和应用的每个使用而不同。此时,可以与阵列中专用密钥的密钥更新频率成比例地决定专用密钥阵列的大小。

[0073] 此外,可以基于通过使用应用的控制消息在应用的对等实体之间进行协商来动态地确定专用密钥阵列的大小。

[0074] 此外,可以基于在EAP重认证时依靠EAP、EAP认证方法或者诸如PANA【6】的EAP传输协议的协商来动态地确定专用密钥阵列的大小。

[0075] 每个应用通过指定哪个密钥阵列元素需要密钥更新来更新专用密钥。可以有一些方法作为密钥阵列元素的规范的方法。主要方法是在每个消息中包括与用于加密该消息的密钥对应的密钥阵列索引。例如,在ANSI C12.22 中,<key-id> 相当于密钥阵列索引。

[0076] 第二种方法是使用应用的控制消息来交换密钥阵列索引。通过使用该索引的专用密钥加密控制消息,该控制消息可用于安全地执行密钥更新。在同一专用密钥阵列中已在过去使用过的索引不会在密钥更新时使用。此外,当接收到用当前使用中的索引的专用密钥加密的消息和不同的索引时,如果所接收到的索引是已使用过的索引之一,则不执行密钥更新。

[0077] 为了实现该方案,有一种保持每个专用密钥阵列过去使用的索引列表和保持有效索引或当前使用中的索引的方法,其中每次执行密钥阵列的专用密钥的密钥更新时有效索引的值加一。当索引完整性(intact)在专用密钥的密钥更新时不存在时,则执行EAP重认证,其将导致对使用同一EMSK 的所有应用的所有专用密钥进行密钥更新。

说明性实施例:

[0079] 图1中示出了ANSI C12.22 的密钥分层结构的说明性示例。这里,ANSIC12.22 应用描述两个使用;注册服务和解析服务。这里,ANSI C12.22 的APMK 密钥称为SMMK(智能表主密钥)。例如,smmk@ietf.org 用作密钥标签。SMMK(智能表主密钥)=KDF(EMSK, smmk@ietf.org | "Y0" | 可选数据 | 长度):

[0080] - 可选数据=NULL(0x00)

[0081] - 长度=64

[0082] SMK-HH 是解析服务使用的专用密钥阵列,并且SMK-EE 是注册服务使用的专用密

钥阵列。

[0083] 使用专用密钥阵列 SMK-HH 的每个阵列元素以加密 CN12.22 服务器(例如,智能表)和(CN12.22 服务器连接的)C12.22 中继之间的解析请求消息和解析响应消息。用于专用密钥阵列 SMK-HH 的每个阵列元素的密钥标签参数是“SMK-SM-CTR”,可选数据参数是例如,ANSI C12.21 中继 Ap-Title|ANSI C12.21key-id,并且长度参数是 16。SMK-SM-CTR(更智能的表与集中器之间的智能表密钥)=KDF(SMMK, “SMK-SM-CTR”|”￥0”| 可选数据 | 长度):

[0084] - 可选数据 :ANSI C12.21 中继 Ap-Title|ANSI C12.21 key-id

[0085] - 长度 =16

[0086] 使用专用密钥阵列 SMK-HH 的每个阵列元素,以便 C12.22 服务器可以加密 C12.22 服务器与 C12.22 主控中继之间的注册请求消息和注册响应消息。

[0087] 用于专用密钥阵列 SMK-EE 的每个阵列元素的密钥标签参数是“SMK-SM-MDMS”,可选数据参数是例如,ANSI C12.21 客户端 Ap-Title|ANSI C12.21 key-id,并且长度是 16。运算符“|”表示以这里的顺序将前面的数据与其后的数据联系起来的操作。

[0088] SMK-SM-MDMS(更智能的表与 MDMS 之间的智能表密钥)=KDF(SMMK, “SMK-SM-MDMS”|”￥0”| 可选数据 | 长度)

[0089] - 可选数据 :ANSI C12.21 客户端 Ap-Title|ANSI C12.21 key-id

[0090] - 长度 =16

[0091] 在本文献中,单词“加密”包含“加密和完整性保护”。

[0092] 图 2 中示出了使用该实施例的密钥管理系统的示例功能性成分。这里,UKMF 是统一的密钥管理功能(Unified Key Management Function)。应用 1 和应用 2 是应用。功能 X 和功能 Y 是应用 2 的特定功能,其中每个特定功能用作应用内的不同目的。

[0093] EAP 对等体是【4】的 EAP 对等功能。EAP 认证器 / 服务器是包含【4】的 EAP 认证器和 EAP 服务器的功能。EAP 对等体底层和 EAP 认证器底层分别是 EAP 对等体和 EAP 认证器的底层的协议实体。网络中的每个功能元件可以在不同的节点上实现。

[0094] 同样, EAP 认证器 / 服务器功能元件的 EAP 认证器功能和 EAP 服务器功能可以在不同的节点上实现。

[0095] EAP 可以被执行为网络接入认证的一部分或者应用级认证的一部分。在前一情况下,可以使用 PANA、IEEE 802.1X、PKMv2 或者任何其它定义在 IP 层下的 EAP 传输协议。在后一情况下,可以使用 PANA、IKEv2 或者任何其它定义在 IP 层或之上的 EAP 传输协议。

[0096] UKMF 管理 EMSK, 并且对于每个应用,管理应用主密钥和专用密钥阵列。

[0097] 应用 1 仅用作一个目的。

[0098] 应用 2 用作两个目的,一个由功能 X 实现,另一个由功能 Y 实现。

[0099] MSK 和 EMSK 【4】由 EAP 对等体和 EAP 认证器 / 服务器的 EAP 服务器功能产生,并由 UKMF 保持。端主机的 UKMF 从 MSK 生成由 EAP 对等体底层使用的密钥或多个密钥,并且 EAP 对等体底层保持和使用所生成的密钥。类似地,网络的 UKMF 从 MSK 生成由 EAP 认证器底层使用的密钥或多个密钥,并且 EAP 认证器底层保持和使用所生成的密钥。UKMF 从 EMSK 生成用于应用 1 和应用 2 的每一个的 APMK, 并且应用 1、应用 2 的功能 X 和应用 2 的功能 Y 保持所生成的 APMK 并使用上述密钥导出算法从 APMK 生成专用密钥阵列。

[0100] 下面示出用于生成和密钥更新专用密钥的基本顺序。

- [0101] 1. 执行 EAP 对等体和 EAP 认证器 / 服务器之间的 EAP 认证。
- [0102] 2. 如果 EAP 认证成功, EAP 对等体和 EAP 服务器将传递 MSK 和 EMSK 给它们的 UKMF。
- [0103] 3. 端主机 UKMF 和网络 UKMF 生成 MSK 并将 MSK 分别传递给 EAP 对等体底层和 EAP 认证器底层。EAP 对等体底层和 EAP 认证器底层使用 MSK 引导底层加密。
- [0104] 4. 端主机和网络的应用 1、应用 2 的功能 X 和应用 2 的功能 Y 分别发送和接收对等实体之间的应用 1、应用 2 的功能 X 和应用 2 的功能 Y 的消息, 如果需要, 启动应用加密。
- [0105] ●当需要应用加密, 但尚未获得 APMK 时, 它们从其 UKMF 获得 APMK 并生成专用密钥阵列以用于应用的专用目的, 并将密钥阵列的有效索引设置为初始值(例如, 0)。
- [0106] ●当需要专用密钥的密钥更新时, 有效索引被更新, 例如, 通过以一递增该有效索引, 并且专用密钥阵列的新有效索引包括在应用消息中, 该应用消息使用对应于该索引的专用密钥进行加密。
- [0107] ●从对等节点接收的应用消息将被丢弃, 如果包含在该消息中的专用密钥阵列的索引不同于对等节点的有效索引(即, 当前使用的索引) 并且与对等节点之前使用的效果索引之一相同。
- [0108] 接下来, 在图 3 中示出使用应用的具体设置的示例密钥管理操作。图 3 包括智能表、集中器和 MDMS (仪表数据管理系统) 服务器。智能表通过集中器向 MDMS 服务器提供电力使用的量(仪表读数)。
- [0109] 此外, 除了仪表读数外, 智能表充当 Web 应用的客户端, 并通过集中器与 MDMS 服务器上的 web 应用服务器交换应用数据, 其中需求响应可以是 Web 应用。
- [0110] 下面给出每个应用的功能的细节。
- [0111] 应用 1 是 Web 应用, 使用 COAP 【5】和 HTTP 作为协议。智能表具有 COAP 客户端。集中器具有 COAP 代理。MDMS 服务器具有 HTTP 服务器。在 COAP 客户端和 COAP 代理之间交换 COAP 消息。COAP 代理在 COAP 客户端和 HTTP 服务器之间执行 COAP-HTTP 协议转换。在 COAP 客户端和 COAP 代理之间加密 COAP 消息。
- [0112] 应用 2 是仪表读数应用, 并且使用 ANSI C12.22 作为协议。应用 2 具有两个功能, 功能 X 和功能 Y。应用 2 的功能 X 实现 ANSI C12.22 注册服务。
- [0113] 在 ANSI C12.22 注册服务中, 智能表是 ANSI C12.22 服务器, 集中器是 ANSI C12.22 中继, MDMS 服务器是 ANSI C12.22 主控中继和 ANSIC12.22 客户端。ANSI C12.22 中继作为注册消息在 C12.22 服务器和 C12.22 主控中继之间的转发器, 并且注册消息在 C12.22 服务器和 C12.22 主控中继之间加密。
- [0114] 应用 2 的功能 Y 是 ANSI C12.22 解析服务。在 ANSI C12.22 解析服务中, 智能表是 ANSI C12.22 服务器, 集中器是 ANSI C12.22 中继。
- [0115] 在 C12.22 解析服务中, C12.22 服务器向 C12.22 中继询问 C12.22 客户端的传输地址。
- [0116] 在 C12.22 服务器和 C12.22 中继之间对查询消息进行加密。
- [0117] PANA【6】用作 EAP 对等体底层和 EAP 认证器底层。在 PANA 中, 智能表是 PaC(PANA 客户端), MDMS 服务器是 PAA (PANA 认证代理)。
- [0118] 在其它实施例中, PAA 可驻留在其它节点中, 例如, 在图 3 中未图示的集中器或者接入点或者接入路由器中。

[0119] 接下来,在图 4-8 中说明用于密钥管理机制的操作的示例顺序。在图 4-8 中,不同节点之间的箭头表示节点之间的协议消息交换,功能块内部的箭头表示同一节点中的功能元件间的信息 I/O。此外,赋给箭头的编号对应于用于生成和密钥更新专用密钥的前述基本顺序的步骤编号。

[0120] 赋给编号的星号(*)示出了对应的步骤是选项。

[0121] 图 4 中示出了用于建立 MSK 和 EMSK 的示例顺序。

[0122] 下面示出详细的生成过程。

[0123] 1. 在智能表和 MDMS 服务器之间执行 EAP 认证。

[0124] 2. 如果 EAP 认证成功,EAP 对等体和 EAP 服务器将传递 MSK 和 EMSK 给每个 UKMF。

[0125] 3. 智能表和 MDMS 服务器生成 MSK 并将 MSK 分别传递给 EAP 对等体底层和 EAP 认证器底层。EAP 对等体底层和 EAP 认证器底层使用 MSK 引导(bootstrap)底层加密。

[0126] 图 5 中示出了 ANSI C12.22 注册服务的示例顺序。

[0127] 下面示出详细的注册过程。

[0128] 4a- 如果智能表尚未获得 APMK,则从其 UKMF 获取一个 APMK 并初始化有效索引。

[0129] 4b- 智能表将 ANSI C12.22 注册请求消息传送给集中器。

[0130] 4c- 集中器将 ANSI C12.22 注册请求消息转发给 MDMS 服务器。

[0131] 4d- 如果 MDMS 服务器还未获得 APMK,则从其 UKMF 获取,从该 APMK 生成专用密钥阵列,初始化有效索引,并使用由所接收的 ANSI C12.22 注册请求消息中携带的索引指定的专用密钥来解密所接收的 ANSI C12.22 注册请求消息。

[0132] 4e- 如果解密成功,MDMS 服务器将 ANSI C12.22 注册响应消息传送给集中器。

[0133] 4f- 集中器将所接收的 ANSI C12.22 注册响应消息转发给智能表。

[0134] 图 6 中示出了用于 ANSI C12.22 解析服务过程的示例顺序。

[0135] 下面示出详细的解析过程。

[0136] 4a- 如果智能表尚未获得 APMK,则从其 UKMF 获取一个 APMK 并初始化有效索引。

[0137] 4b- 智能表将 ANSI C12.22 解析请求消息传送给集中器。

[0138] 4c- 如果集中器尚未获得 APMK,则将 APMK 获取请求消息传送给 MDMS 服务器以从 MDMS 服务器获取一个 APMK。在 APMK 获取请求消息中包括智能表的识别信息和应用识别信息(APMK 导出算法的密钥标签值)。

[0139] 4d- 如果 MDMS 服务器还未获得 APMK,则从其 UKMF 获取一个 APMK。

[0140] 4e- MDMS 服务器将包含 APMK 的 APMK 获取响应消息传送给集中器。

[0141] 4f- 集中器从 APMK 生成专用密钥阵列并初始化有效索引,如果其使用由所接收的 ANSI C12.22 解析请求消息中携带的索引指定的专用密钥解码 ANSI C12.22 解析请求消息成功,则其将 ANSI C12.22 解析响应消息传送给智能表。

[0142] 此外,APMK 请求消息和 APMK 获取响应消息可被定义为 ANSI C12.22 获取消息,并且可被定义为其它协议的消息。

[0143] 图 7 中示出了用于 COAP/HTTP 服务过程的示例顺序。

[0144] 下面示出详细的 COAP/HTTP 服务过程。

[0145] 4a- 如果智能表还未获得 APMK,则从其 UKMF 获取一个 APMK 并初始化有效索引。

[0146] 4b- 智能表将 COAP 请求消息传送给集中器。

[0147] 4c- 如果集中器尚未获得 APMK，则将 APMK 获取请求消息传送给 MDMS 服务器以从 MDMS 服务器获取一个 APMK。在 APMK 获取请求消息中包括智能表的识别信息和应用识别信息（APMK 导出算法的密钥标签值）。

[0148] 4d- 如果 MDMS 服务器还未获得 APMK，则从其 UKMF 获取一个 APMK。

[0149] 4e-MDMS 服务器将包含 APMK 的 APMK 响应消息传送给集中器。

[0150] 4f- 集中器从 APMK 生成专用密钥阵列并初始化有效索引，如果其使用由所接收的 COAP 请求消息中携带的索引指定的专用密钥解码 COAP 请求消息成功，则其将 HTTP 请求消息传送给 MDMS 服务器。

[0151] 4g-MDMS 服务器将 HTTP 响应消息传送给集中器。

[0152] 4h- 集中器将使用由所接收的 COAP 请求消息中包含的索引指定的专用密钥加密的 COAP 响应消息传送给智能表。

[0153] 此外，APMK 获取请求消息和 APMK 获取响应消息可被定义为 HTTP 消息，并且可被定义为其它协议的消息。在前一情况下，步骤 4c 可与 4f 合并，步骤 4e 可与 4g 合并。

[0154] 图 8 中示出了用于 ANSI C12.22 注册服务的专用密钥的密钥更新的示例顺序。

[0155] 下面示出详细的密钥更新过程。

[0156] 这里，假设智能表和 MDMS 服务器已获得 APMK。

[0157] 4a- 智能表将使用新专用密钥阵列索引加密的 ANSI C12.22 注册请求消息传送给集中器。

[0158] 4b- 集中器将所接收的 ANSI C12.22 注册请求消息转发给 MDMS 服务器。

[0159] 4c- 如果 MDMS 服务器检测到包含在所接收的 ANSI C12.22 注册请求消息中的具体使用的密钥阵列索引不同于有效索引，则检查该索引是否是过去已用于注册器的那些索引之一。如果该索引是已使用的那些索引之一，则所接收的消息将被丢弃并且什么也不做。否则，如果使用由该索引指定的专用密钥成功地解码了 ANSI C12.22 注册请求消息，则 MDMS 服务器使用该索引替换有效索引，并将 ANSI C12.22 注册响应消息传送给集中器。

[0160] 4d- 集中器将 ANSI C12.22 注册响应消息转发给智能表。

[0161] 其它方面和实施例：

[0162] 本发明的其它方面和实施例陈述如下：

[0163] a. 密钥管理机制

[0164] 在一些实施例中，密钥管理机制基于在同一通信层内或者跨不同的通信层定义跨越多重协议的统一的密钥管理功能（UKMF）。图 9 示出了该方案的概念模型。尽管图 9 仅提及了应用层和链路层协议，该概念通常适用于需要在包括网络层和传输层的任何通信层处的加密操作的任何协议。

[0165] 理论上，仅有一个 UKMF 以加密机制跨越所有协议。这称为完全统一的模型并示出在图 9a 中。另一方面，取决于部属需求和其它设计限制，一些协议可使用专用的密钥管理功能（DKMF），而其它协议可使用 UKMF。该模型称为部分统一的模型。图 9b 示出了部分统一的模型的典型实例，其中只有应用层协议使用 UKMF，链路层协议使用 DKMF。通常，在部分统一的模型中，协议与 UKMF 或 DKMF 之间的映射可以是任意的。在完全的和部分统一的模型中，使用 UKMF 的协议还可以具有 DKMF，其中 DKMF 可由 UKMF 管理，并且图 9 中未示出这样的 DKMF。例如，如果一些应用协议基于其自身的特定密钥管理协议可具有 DKMF，则 UKMF 可

生成由特定密钥管理协议使用的对称密钥,以结合(bind) UKMF 与 DKMF。

[0166] 在完全的和部分统一的模型中,建立一对 UKMF 之间的安全关联的初始对等实体认证可基于网络接入认证或应用级认证。例如,如果设备最初所附的接入网络是开放接入网络,则初始对等实体认证可基于应用级认证。

[0167] 尽管通常概念模型足够适用于支持引导多协议的加密的任何密钥管理构架,但 EAP 密钥管理构架的使用被考虑,因为其已经用于诸如以太网、Wi-Fi 和 Wi-MAX 的现有接入技术中。

[0168] 下面描述了基于 EAP 密钥管理构架【18】的密钥管理机制的详细实现作为其基础(图 2)以满足上述所有要求。EAP【4】最初是为用于 PPP(点对点协议)的网络接入认证协议设计的,并已被包括 IEEE 802.3、IEEE802.11 和 IEEE 802.16 的多个数据链路层协议以及诸如 PANA【6】和 IKEv2【19】的 IP 和高层协议采用。PANA 正在被 ZigBee SEP2.0(Smart Energy Profile 2.0)【22】考虑。由 EAP 支持的认证算法称为 EAP 方法。EAP 支持多种方法,包括基于对称和非对称的密钥的方法。

[0169] EAP 使用密钥生成方法向其底层输出两种类型的密钥,MSK(主会话密钥)和 EMSK(可扩展的主会话密钥)。由于 MSK 使用是为了保护 EAP 的底层,并且使用 UKMF 的协议的端点可能与 EAP 的不同,EMSK 的使用被考虑用于生成主要用于诸如 ANSI C12.22【1】和 COAP【1】的 AMI 应用的密钥,而使用 MSK 主要用于保护 EAP 的底层。

[0170] 一些应用具有多个功能,关于同一应用中不同的功能在不同的元件之间执行通信。例如,ANSI C12.22 定义注册功能(其中 C12.22 中继负责注册端主机)和解析功能(其中从端主机的第一跳 C12.22 中继负责解析端主机的通信对等体的传输地址)。对于这样的应用,为每个网络元件生成不同的密钥,并且不同的密钥被分配给每个网络元件,其中网络元件包括在应用的特定功能中并与图 2 中所示的端主机通信。在图 2 中,两个应用被 UKMF 管理,并且应用 2 具有使用不同设置的密钥材料的两个功能。假设端主机中的 UKMF 和其它元件间的通信使用本地 API 实现,而网络中的 UKMF 和其它元件间的通信取决于通信实体是否在同一设备中实现而使用本地 API 或协议实现。

[0171] 基于 EAP 的统一的密钥管理机制中的 UKMF 的主要任务是取决于其是否驻留在端主机或网络中而从 EAP 对等体或认证器 / 服务器接收 EAP 密钥材料,导出密钥材料以分发给其密钥消费者并当需要 MSK 和 EMSK 的密钥更新时触发 EAP 重认证。在图 2 中,应用 1 的元件、应用的功能 X 的元件、应用 2 的功能 Y 的元件、EAP 对等体和认证器底层都是密钥消费者。

[0172] 为了符合阻止 EMSK 输出 EAP 服务器外部的 EAP 密钥管理架构【18】,期待网络中的 UKMF 与 EAP 服务器驻留在同一节点中。EMSK 下的密钥分层基于如下的 USRK(特定使用的根密钥)定义在【3】中:

[0173] $\text{USRK} = \text{KDF}(\text{EMSK}, \text{密钥标签} \mid "\backslash 0" \mid \text{可选数据} \mid \text{长度})$ 。

[0174] 在基于 EAP 的统一的密钥管理机制中,USRK 用于引导应用层加密密钥。从同一 EMSK 导出的不同应用层加密密钥间的密码独立性通过下列方式保证:(i)为每个应用分派唯一的 USRK 标签,(ii)对于具有多个功能的应用,为应用的每个功能定义特定 USRK 的子密钥,其中每个子密钥使用同一 USRK 导出算法但使用其父密钥代替 EMSK 以及应用内的功能的唯一的标签导出。诸如密钥标识符和端主机的标识符的附加参数可包含在 USRK 和其子

密钥的可选数据中。从 EAP 密钥材料(即, MSK 和 EMSK)导出的任何密钥的生命周期由 EAP 密钥材料的生命周期限制。只要生命周期未到期, 导出的密钥可以缓存在其密钥消费者处。

[0175] b. 密钥管理机制替代方案

[0176] 由于存在多种用于将智能表连接到诸如以太网、PLC、ZigBee、Wi-Fi 和 3G 的 AMI 网络的链路层技术, 需要对基于 EAP 的统一的密钥管理方案如何能与可以不同的方式管理链路层特定密钥的不同的链路层技术合作的考虑。有两种不同的方式。

[0177] 在第一架构替代中, EAP 用于网络接入认证和引导应用层加密, 其中可使用链路层特定 EAP 传输在链路层处或者使用 PANA【6】在网络层处执行 EAP。关于使用 PANA 作为 EAP 传输的链路层密钥管理有两种情况。

[0178] ●在第一种情况中, 链路层加密可以独立于 PANA 而启动或无效。

[0179] 在这种情况下, 在 IP 层或以上提供加密或非加密接入控制。示例加密接入控制是 IPsec。示例非加密接入控制是 SAVI (源地址验证改进)【20】。在这种情况下, 可以使用链路层特定认证和可能不支持 EAP 的协定机制(UMTS AKA 是一种这样的机制)来启动链路层加密。这种情况属于部分统一的模型, 因为 UKMF 是用于应用层加密以及可选地用于 IP 层加密的密钥管理的一部分, 但是不是用于链路层加密的密钥管理的一部分。

[0180] ●在第二种情况中, 使用 PANA 引导链路层加密, 其中使用 PANA 安全关联在链路的两个端点之间安全地建立链路层主密钥, 并且安全关联协议使用链路层主密钥来建立链路层加密密钥。链路层主密钥可以是单独的密钥或者组密钥, 取决于链路层的信任模型。当链路层主密钥是单独的密钥时, 该密钥仅在特定链路的端点之间使用。这种单独的密钥的示例是【21】中的 PEMK (PaC-EP 主密钥)。当使用组密钥时, 信任模型提供拥有同一组密钥的所有节点被认为是可信的。使用组密钥的典型的链路层技术是 ZigBee【8】。一旦其成功地认证到网络, 组密钥需要被安全地传递给每个节点。

[0181] PANA 可用于保护组密钥传递。这种情况属于完全统一的模型。

[0182] 在第二架构替代中, EAP 仅用于引导应用层加密。PANA 用作应用级认证的 EAP 传输。注意, IKEv2【19】是 UDP 上的另一 EAP 传输, 然而, 由于 IKEv2 需要对于硬件受限的设备来说可能是负担的 Diffie-Hellman 算法, PANA 是智能表首选的。可以独立于用于引导应用层加密的该 EAP 来执行链路层或网络层处的接入控制。这种架构属于部分统一的模型。该模型的示例用例是用于在 ANSI C12.22 主机和 ANSI 12.22 主控中继之间引导 ANSI C12.22 加密密钥, 其中 ANSI C12.22 主机是 PaC (PANA 客户端), 并且 ANSI C12.22 主控中继是 PAA (PANA 认证代理)。

[0183] 由于 EAP 的当前适用性是关于网络接入认证【4】的, 两种架构替代方案可能需要支持应用级认证的 EAP 适用性的扩展以引导应用层加密。另一方面, EAP 应用性的这种扩展是可能的, 而不一定需要 EAP 自身的修改。下一部分描述扩展 EAP 应用性以适合我们的统一的密钥管理机制需要什么附加考虑。

[0184] c. 引导应用层加密

[0185] 基于 EAP 的统一的密钥管理机制需要一种端主机发现引导应用层加密所需信息的机制。下列信息需要被发现。

[0186] ●支持引导应用层加密的 EAP 认证器的传输标识符。

[0187] ●支持从 EAP 引导应用层加密的应用的一组标识符。

[0188] ●对于支持从 EAP 引导应用层加密的每个应用,网络中的应用端点的标识符。

[0189] d. 对应用层加密密钥进行密钥更新

[0190] 在基于 EAP 的统一的密钥管理机制中,在没有附加密钥更新机制的情况下,通过 EAP 重认证执行对从 EMSK 导出的应用层加密密钥的密钥更新。对 EMSK 的密钥更新将替换从其导出的所有密钥。因此,从优化的角度,期望设计一种系统以便可以尽可能的降低 EMSK 密钥更新的频率。有三种独立的方案可解决密钥更新问题。

[0191] 第一种方案是使用如【23】中的 ERP (用于 EAP 重认证协议的 EAP 扩展) 用于 EAP 重认证。由于 ERP 在不对 EMSK 进行密钥更新的情况下操作,因此这种方案可以避免 EMSK 密钥更新,即使是在使用完全统一的模型并且关于网络接入的 EAP 重认证发生时。

[0192] 第二种方案是使用第二密钥管理替代方案(即,使用由仅用于引导应用层加密的 PANA 携带的 EAP)。该方案在端主机改变其网络附着点时可避免 EMSK 密钥更新,因为 EAP 不用于网络接入并且 PANA 具有其自己的处理端主机的 IP 地址改变的移动性管理机制。

[0193] 第三种方案是为给定应用的每种功能生成应用层加密密钥的多种设置(而不是应用层加密密钥的单一设置)并且当需要密钥更新时改变应用层加密密钥的有效设置。例如,ANSI C12.22 定义加密密钥阵列,其中 key-id 或者阵列索引承载在各个安全激活的消息中,并且改变密钥通过改变 key-id 值来完成。密钥阵列的大小可以基于应用的特性来确定,例如,应用的阵列大小可以设置为使其与应用的平均密钥更新频率成比例。

[0194] e. 示例性高级量测体系(AMI) 系统架构

[0195] 图 10 示出了 AMI 系统的基本组件。安装在消费者家里的智能表将计量数据推送给公用事业管理处中的仪表数据管理系统(MDMS);或者 MDMS 从智能表推送计量数据。并且智能表还可以从 MDMS 或者通过 MDMS 从需求响应管理系统(DRMS) 接收需求响应(DR) 信号。此外,智能表可与家庭显示通信以示出消费者的能源使用,并且可与家庭服务器通信以协调家庭中的能源使用。

[0196] 智能表通过公共广域网(WAN)与 MDMS 通信,公共 WAN 可能是因特网以用于 DR 信号和计量数据的交换。这里考虑将 ANSI C12.22 用作 MDMS 和智能表之间的应用协议。ANSI C12.22 提供安全机制但其缺乏动态密钥管理(密钥更新)机制。此外,在社区网络(NAN)中需要网络接入认证。为了满足这些要求,可以如图 11 所示基于以上讨论的第一架构替代方案应用统一的密钥管理机制。由于很多智能表可以附属于一个 NAN,因此安装数据集中器来收集计量数据。在这种情况下,PANA 用于集中器与智能表之间的 NAN 的网络接入认证。集中器充当 ANSI C12.22 中继和 PANA PAA,智能表充当 ANSI C12.22 主机和 PANA PaC。

[0197] 认证和密钥建立过程的要点示出如下:

[0198] 1. 智能表在自举电路(bootstrapping)处发起与集中器的 PANA 协商。PANA 用于 EAP 传输。

[0199] 2. 集中器在智能表和 MDMS 之间中继 EAP 消息。AAA 协议(例如,半径或直径)用于集中器与 MDMS 之间的 EAP 传输。

[0200] 3. 允许智能表与 ANSI C12.22 网络连接,并且在 EAP 认证成功后,智能表、集中器和 MDMS 共享 ANSI C12.22 加密密钥。从 EAP EMSK 生成该密钥。

[0201] 4. 当需要 ANSI C12.22 加密密钥的密钥更新时,将在 ANSI C12.22 加密密钥期满之前执行 EAP 重认证作为 PANA 重认证的一部分。

[0202] 另一方面,也可以考虑 MDMS 与智能表直接通信而不需要集中器的模型。该模型称为非集中器模型。非集中器模型典型地用于具有少量智能表的 NAN。

[0203] 该模型的认证和密钥建立过程的要点如下:

[0204] 1. 智能表在自举电路处发起与 MDMS 的 PANA 协商。PANA 用于 EAP 传输。

[0205] 2. 在 EAP 认证成功后,智能表与 MDMS 共享 ANSI C12.22 加密密钥。从 EAP EMSK 生成该密钥。

[0206] 3. 当需要 ANSI C12.22 加密密钥的密钥更新时,将在 ANSI C12.22 加密密钥期满之前执行 EAP 重认证作为 PANA 重认证的一部分。

[0207] 统一的密钥管理机制可以实现为具有 Toshiba 微处理器 TLCS-900 的嵌入设备上的 EAP 和 PANA。PANA 和 EAP 实现的占用空间小于 30KB,其表示所提议的统一的密钥管理机制的 EAP 和 EAP 底层部分满足上述要求。

[0208] 统一的密钥管理机制 - 其可从单个对等实体认证尝试生成用于多个通信层的多重协议的加密密钥 - 适用于智能电网用例,尤其是智能表,其中,假设智能表是低成本的无线设备,其为每种协议重复对等实体认证尝试可能是个负担。上述讨论的机制是灵活的,因为对等实体认证可以是网络接入认证或者应用级认证。上述考虑的关于基于 EAP 的统一的密钥管理机制的细节示出了 EAP 广泛地用于现有的链路层技术,并且考虑从 EMSK 引导的加密密钥的密钥更新效率是重要的。

[0209] 此外,统一的密钥管理机制是与基于 ANSI C12.22 的智能表应用和用于网络接入认证的 PANA 以及应用级认证相结合的,具有关于商业微处理器上的 EAP 和 PANA 的初步实现结果。将来,可能会考虑 EV (电动汽车) 作为智能电网的组件。

[0210] 本发明的宽广范围:

[0211] 虽然此处描述了本发明的说明性实施例,但本发明不限于此处描述的各种优选实施例,而是包括本领域的技术人员基于本发明的公开将理解的具有等价元件、修改、省略、组合(例如,跨越各种实施例的方面的组合)、改编和 / 或替代的任何和所有实施例。权利要求中的限制(例如,包括将在以后添加的)应基于权利要求中采用的语言广泛地解释,而不限制为本说明书中或应用的实施期间所述的示例,这些示例应解释为非穷举的。例如,在本公开中,术语“优选地”是非穷举的,且表示“优选地,但不限于”。在本公开中以及在本申请的实施期间,装置功能限定或者步骤功能限定限制仅在所有下列条件在权利要求的限制中的特定权利要求中采用 :a) 明确地陈述了“用于…的装置”或“用于…的步骤”;b) 明确地陈述了对应的功能;以及 c) 没有陈述支持该结构的结构、材料或动作。在本公开中以及在本申请的实施期间,“本发明”或“发明”可用作对本公开中的一个或多个方面的参考。本发明或发明的语言不应被不正确地解释为临界的识别、不应被不正确地解释为跨越所有方面或实施例应用(即,应理解为本发明具有许多方面和实施例)、并且不应被解释为限制申请或权利要求的范围。在本公开中以及在本申请的实施期间,术语“实施例”可用于描述任何方面、特征、方法或步骤、其任何组合和 / 或其任何部分等。在一些示例中,各个实施例可包括重叠的特征。在本公开中,可采用下列缩略术语:“e. g. ”,其表示“例如”。

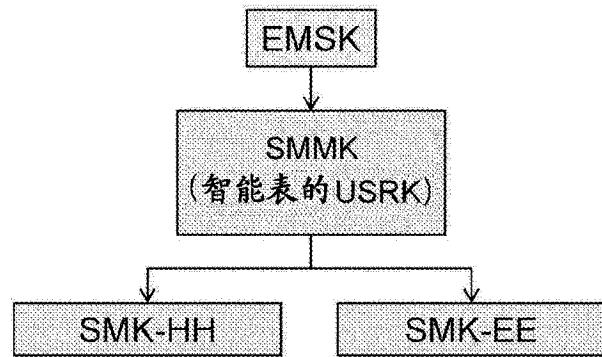


图 1

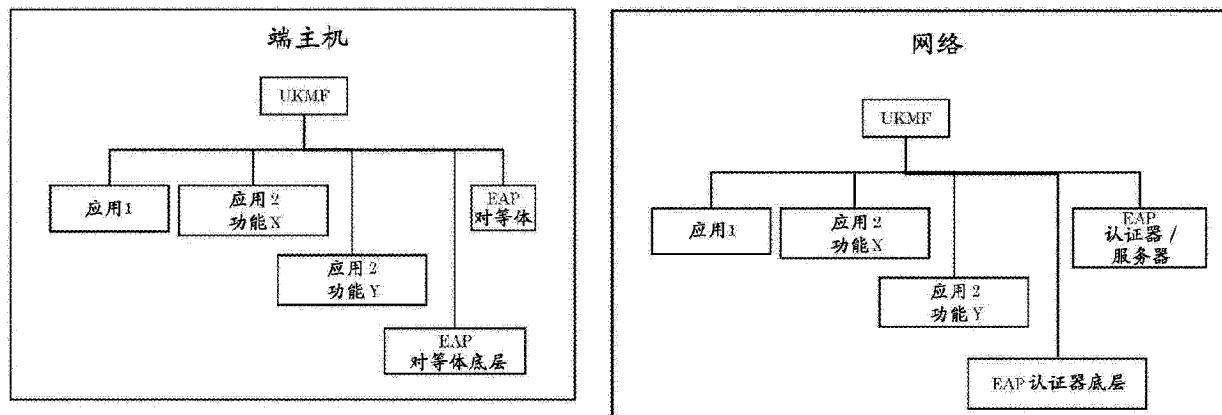


图 2

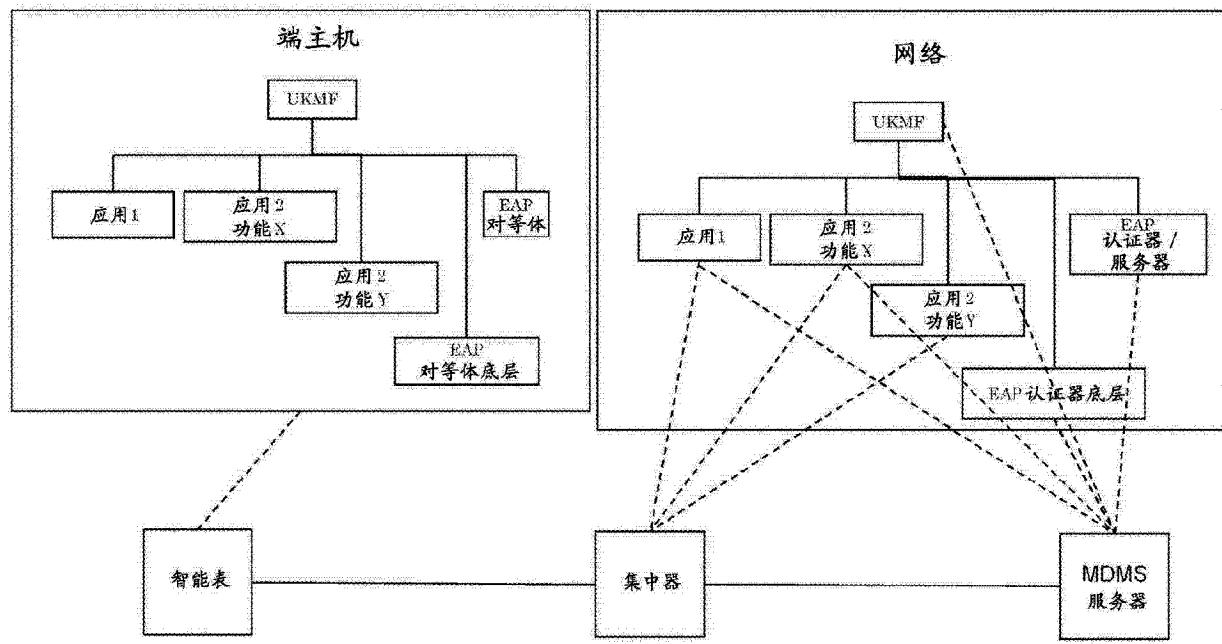


图 3

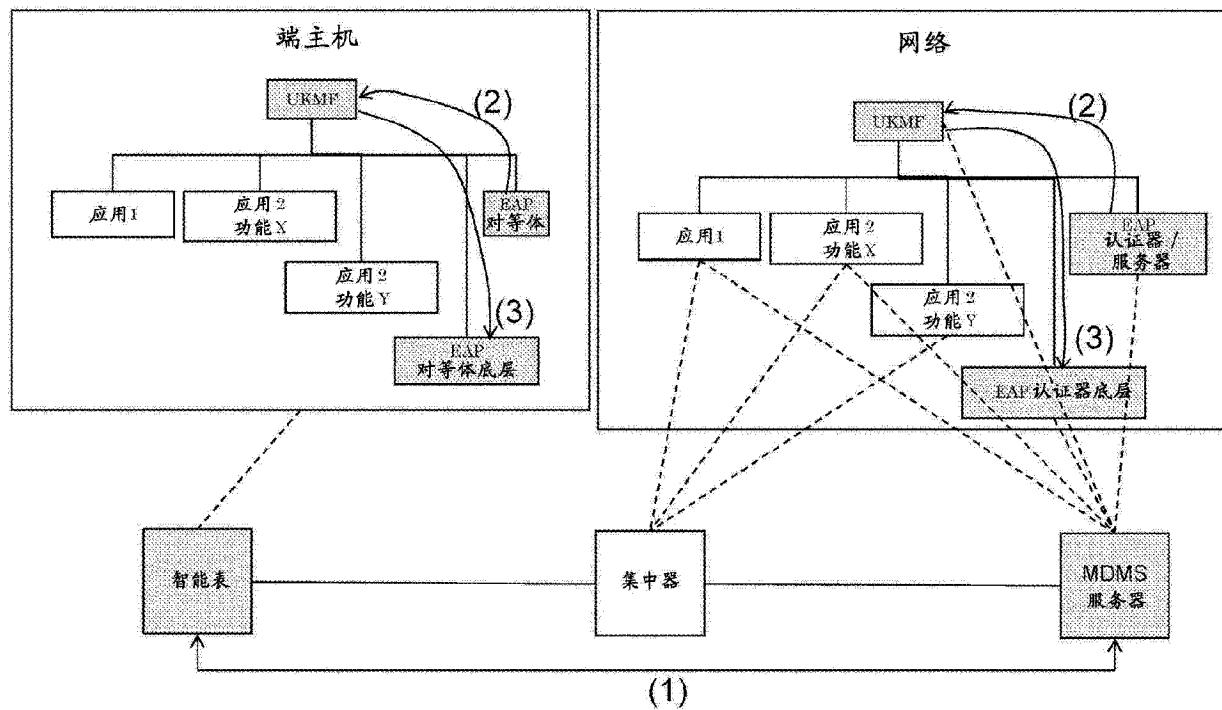


图 4

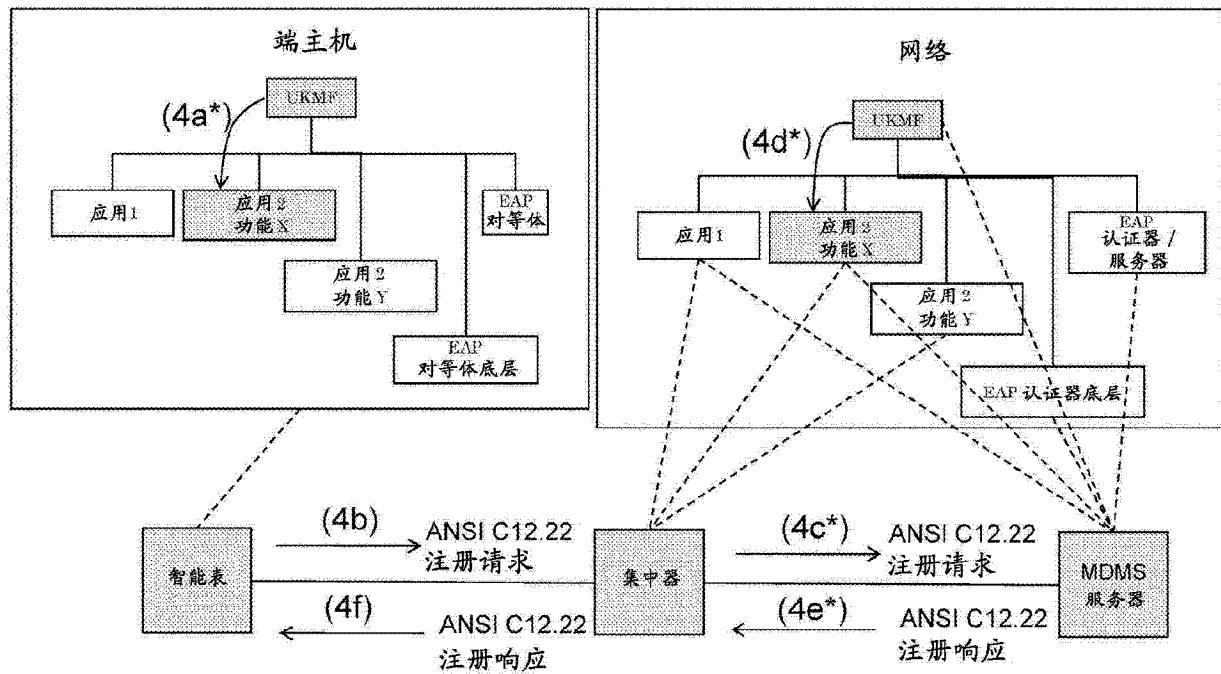


图 5

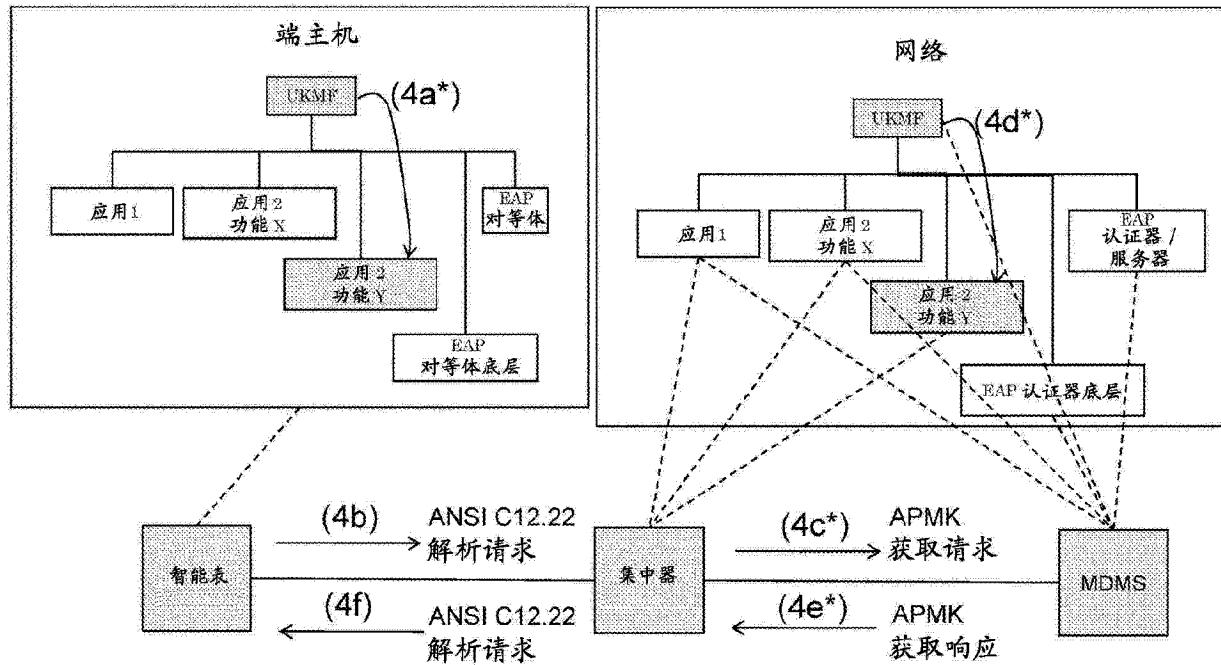


图 6

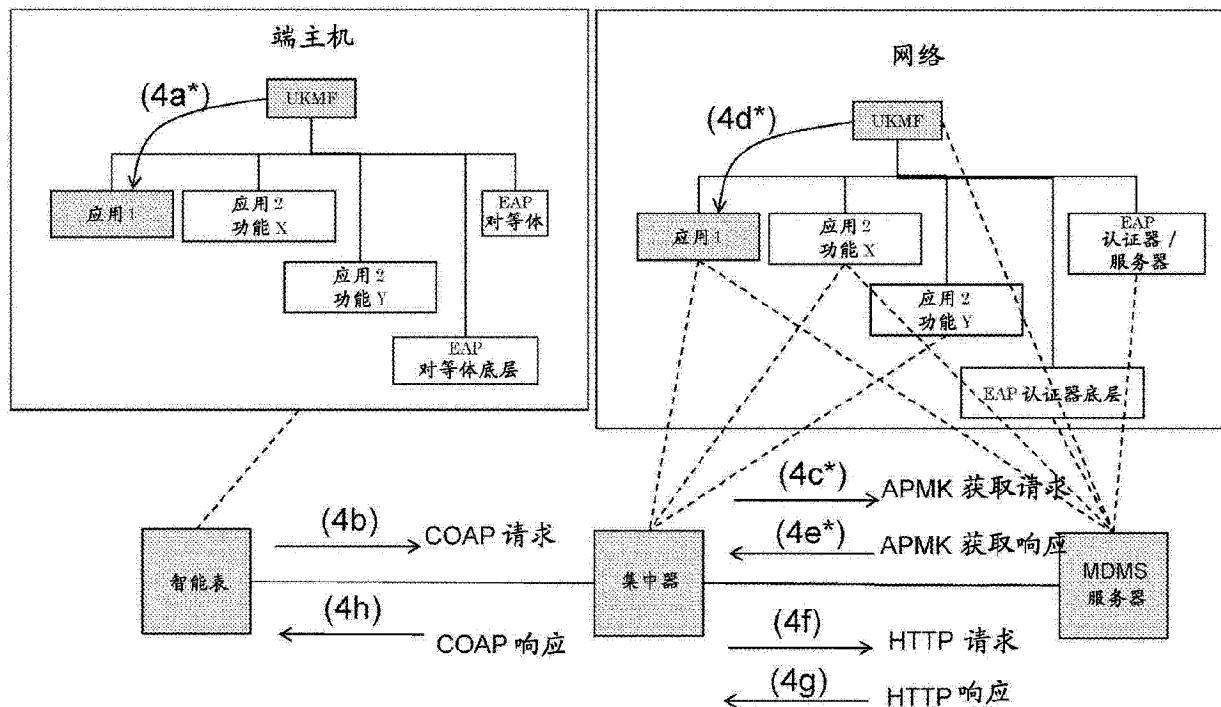


图 7

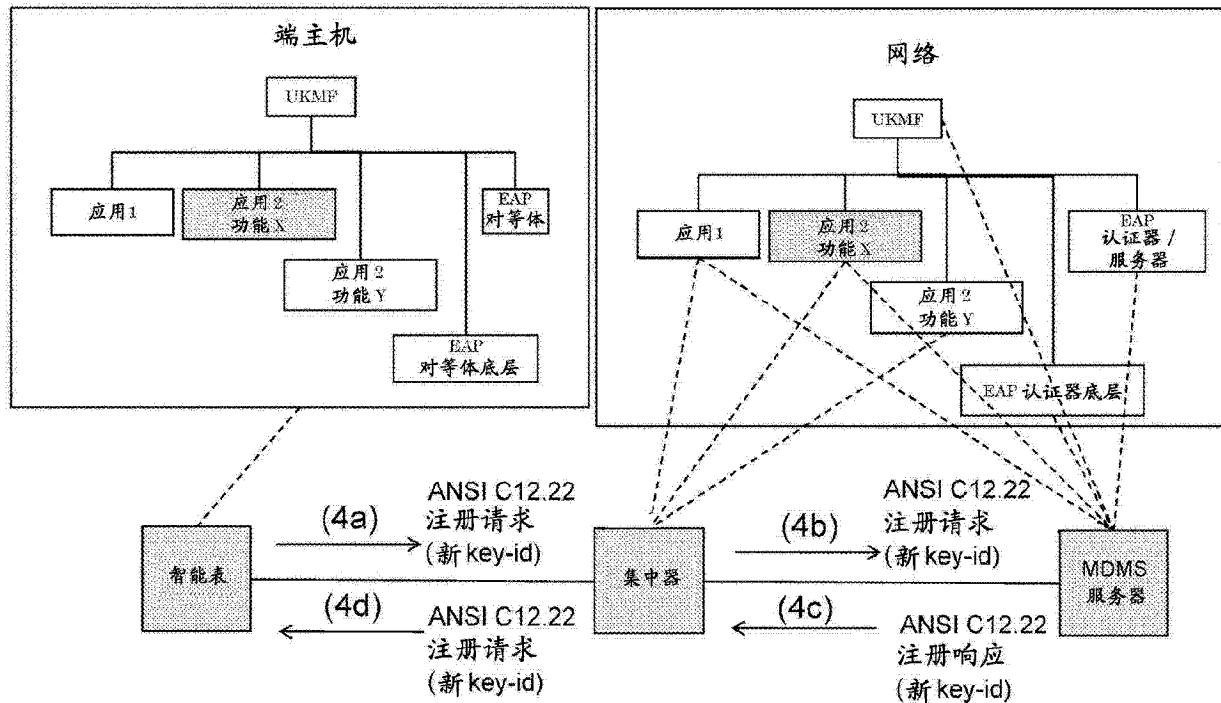
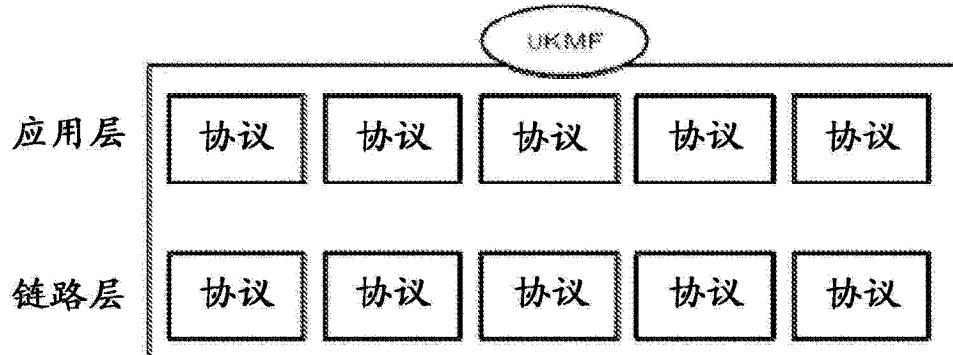
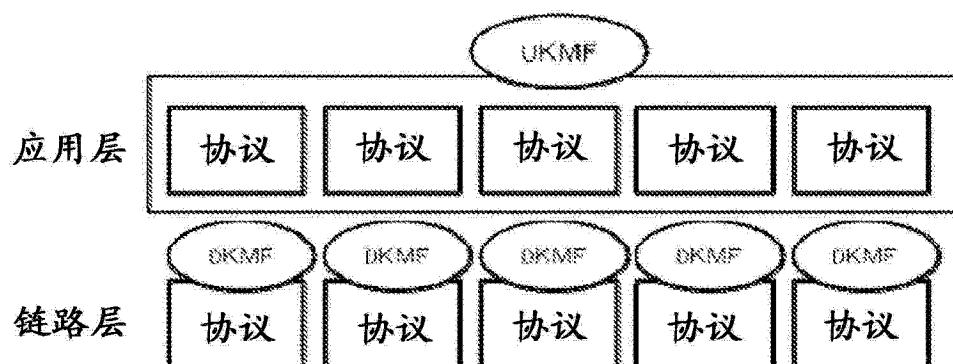


图 8



a): 完全统一的模型



b): 部分统一的模型

图 9

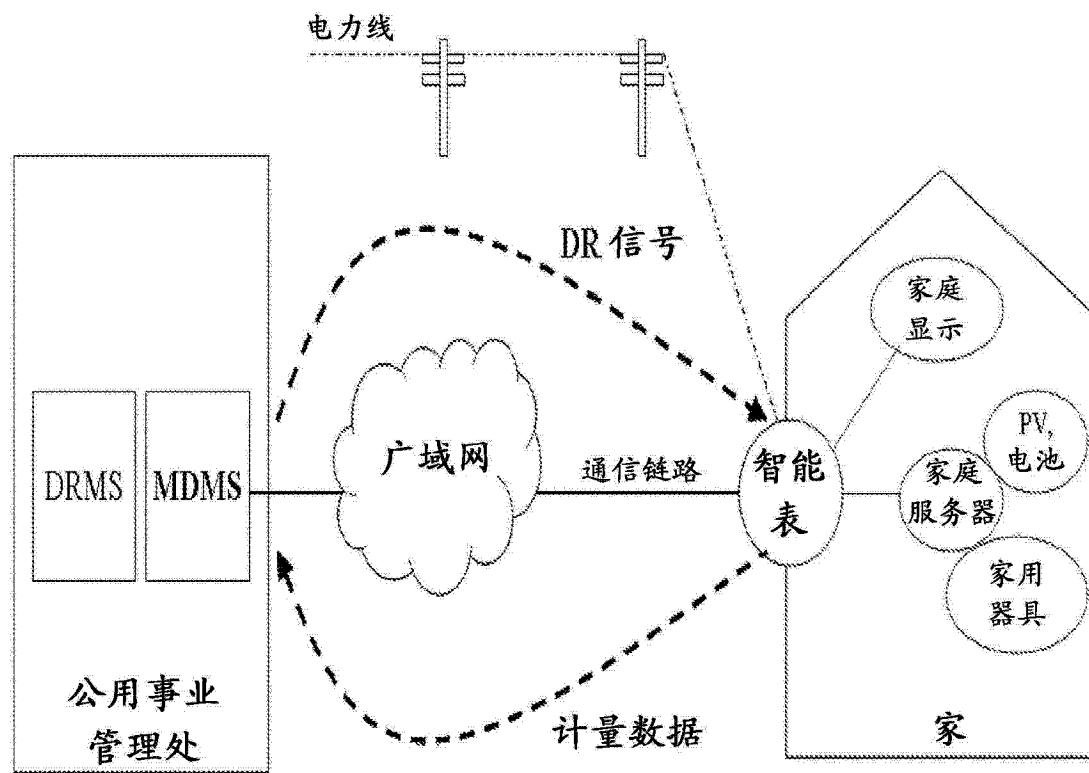


图 10

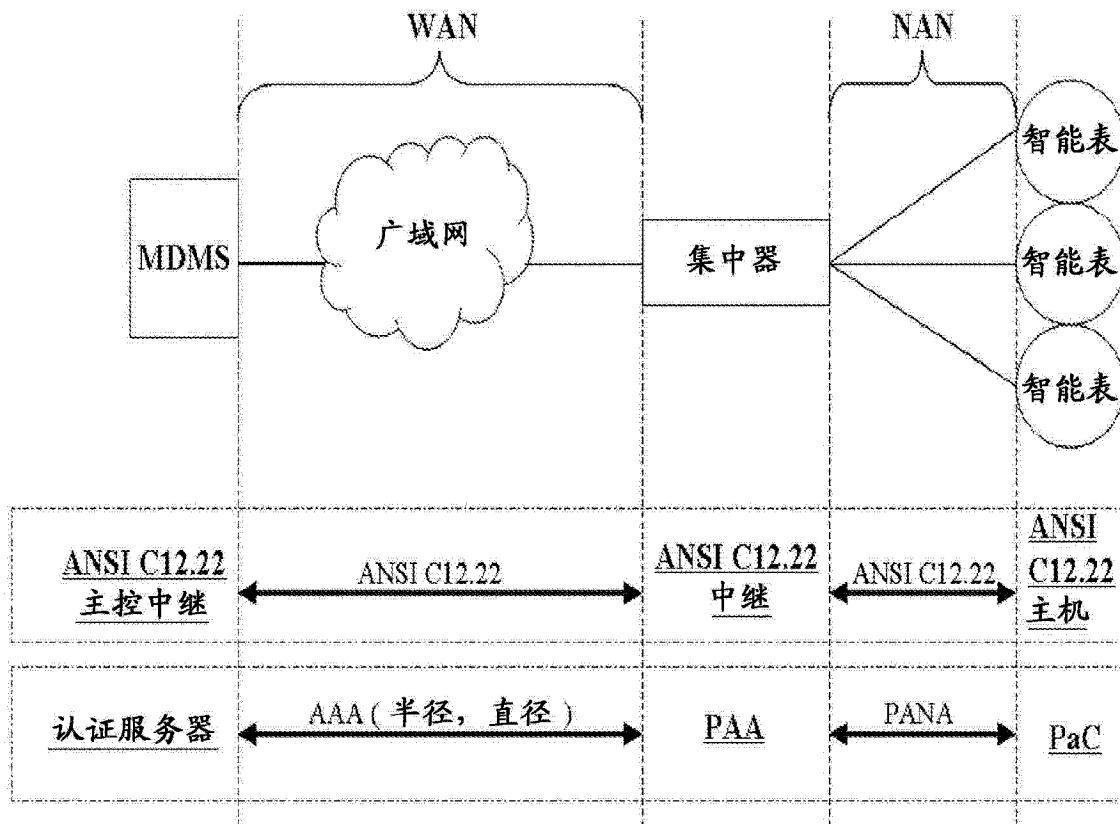


图 11