



(12) 发明专利申请

(10) 申请公布号 CN 103765165 A

(43) 申请公布日 2014. 04. 30

(21) 申请号 201280042141. 9

(22) 申请日 2012. 08. 30

(30) 优先权数据

11179338. 6 2011. 08. 30 EP

61/528, 826 2011. 08. 30 US

(85) PCT国际申请进入国家阶段日

2014. 02. 28

(86) PCT国际申请的申请数据

PCT/EP2012/066809 2012. 08. 30

(87) PCT国际申请的公布数据

W02013/030250 EN 2013. 03. 07

(71) 申请人 纳格拉影像股份有限公司

地址 瑞士舍索苏尔洛桑

(72) 发明人 C·勒布汗

(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 张荣海

(51) Int. Cl.

G01D 4/00(2006. 01)

H04L 9/32(2006. 01)

H02J 13/00(2006. 01)

权利要求书3页 说明书9页 附图1页

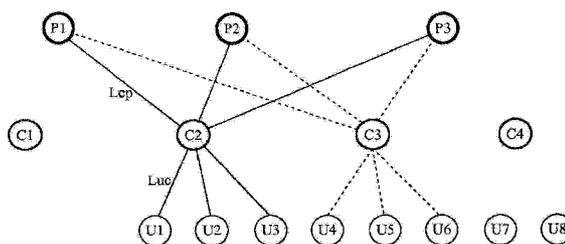
(54) 发明名称

智能网内的公用事业消费的计价系统和方法

(57) 摘要

一种包括多个公用事业计量表 (U1-U8) 智能网内的公用事业消费的计价方法, 公用事业计量表 (U1-U8) 分别通过中间数据集中器 (C1-C4), 连接到至少一个公用事业管理中心 (P1-P3), 所述方法包括以下步骤: 安全地从每个公用事业管理中心 (P1-P3), 接收至少一个资费表, 所述资费表包含每 24 小时的至少一个时间间隔 [DT1, DT2], 和与所述时间间隔相关的费率, 利用所述数据集中器, 在所有资费表的所有时间间隔的费率之中, 为每个时间间隔 [DT1, DT2] 选择最低的费率, 从所述公用事业计量表接收受保护的公用事业计量表消息 DTup_{u,c}, 公用事业计量表消息 DTup_{u,c} 都包括: 由发送该消息 DTup_{u,c} 的公用事业计量表报告的计量数据测量结果 DTup, 其公用事业计量表标识符 Uid, 数据集中器标识符 DCid 和管理中心标识符 Pid, 根据几个计量数据测量结果 DTup, 确定利用所述公用事业计量表在时间间隔 ΔT 内, 测量的 2 个计量计数器消费指数 CPT 之差计算的计量计数器差分消费值 ΔCPT, 把对于时间间隔 ΔT, 提出最低费率的公用事业管理中心分配给所述消费值 ΔCPT, 为每个管理中心建立受保护的报告, 所述报告至少包含该计量计数器差分消费值 ΔCPT, 以及所述值 ΔCPT 涉及的公用事业计量表标识符 Uid, 把所述受保护的报告从所述数据

集中器发送给该公用事业管理中心。



1. 一种包括多个公用事业计量表 (U1-U8) 的智能网内的公用事业消费的计价方法, 每个公用事业计量表 (U1-U8) 与至少一个公用事业管理中心 (P1-P3) 相关, 并通过利用数据集中器标识符 DCid 识别的中间数据集中器 (C1-C4) 连接到所述至少一个公用事业管理中心 (P1-P3), 每个公用事业计量表 (U1-U8) 是利用公用事业计量表标识符 Uid 识别的, 并且适合于产生并向所述数据集中器发送受保护的公用事业计量表消息 DTup_{u,c}, 每个数据集中器适合于产生并向所述管理中心 (P1-P3) 发送受保护的报告, 每个管理中心 (P1-P3) 是利用管理中心标识符 Pid 识别的, 所述方法包括以下步骤:

- 利用所述数据集中器 (C1-C4), 从每个所述公用事业管理中心 (P1-P3) 接收包含至少一个资费表的受保护的数据集中器消息, 所述资费表包含每 24 小时的时段的至少一个时间间隔 [DT1, DT2] 和与所述时间间隔 [DT1, DT2] 相关的费率,

- 解密和 / 或核实所述数据集中器消息的真实性和完整性; 在失败或不成功结果的情况下: 中断对所述数据集中器消息的处理,

- 利用所述数据集中器 (C1-C4), 在所有资费表中的所有时间间隔的费率之中为每个时间间隔 [DT1, DT2] 选择最低的费率, 以便得出有利的资费表,

- 利用所述数据集中器 (C1-C4), 从所述公用事业计量表 (U1-U8) 接收所述公用事业计量表消息 DTup_{u,c}, 这些公用事业计量表消息 DTup_{u,c} 中的每一个包括: 由发送该消息 DTup_{u,c} 的公用事业计量表报告的计量数据测量结果 DTup、其公用事业计量表标识符 Uid、所述数据集中器标识符 DCid 以及所述管理中心标识符 Pid,

- 解密和 / 或核实所述公用事业计量表消息的真实性和完整性, 在失败或不成功的情况下: 中断对所述公用事业计量表消息的处理,

- 基于几个计量数据测量结果 DTup, 确定利用由所述公用事业计量表在由第一时间 T1 和第二时间 T2 限定的时间间隔 ΔT 内测量的 2 个计量计数器消费指数 CPT 之差计算的计量计数器差分消费值 ΔCPT ,

- 把对于包含在所述第一时间 T1 和所述第二时间 T2 之间的时间间隔 ΔT 提出最低费率的公用事业管理中心 (P1-P3) 分配给所述计量计数器差分消费值 ΔCPT ,

- 为每个管理中心 (P1-P3) 建立报告, 所述报告至少包含分配给该管理中心 (P1-P3) 的计量计数器差分消费值 ΔCPT 以及所述值 ΔCPT 涉及的公用事业计量表标识符 Uid,

- 加密并且

- 保护所述报告, 之后把所述报告从所述数据集中器 (C1-C4) 发送给所述公用事业管理中心 (P1-P3), 只有在解密所述报告和 / 或检查所述报告的真实性和完整性之后, 所述公用事业管理中心 (P1-P3) 才处理所述报告。

2. 按照权利要求 1 所述的方法, 其中通过加密和 / 或通过签名所述消息或报告, 保护每个所述公用事业消息和 / 或所述数据集中器消息和 / 或所述报告。

3. 按照任意前述权利要求所述的方法, 其中所述方法还包括响应收到所述公用事业计量表 (U1-U8) 发送的所述公用事业计量表消息 DTup_{u,c}, 从所述数据集中器 (C1-C4) 向所述公用事业计量表 (U1-U8) 发送确认的步骤。

4. 按照权利要求 1 所述的方法, 其中在报告时期 ΔRT 内收集多个计算的消费值 ΔCPT , 并保存在数据集中器 (C1-C4) 的存储器中, 之后在所述报告时期 ΔRT 结束时在所述报告内将所述多个计算的消费值 ΔCPT 从所述数据集中器发送给与所述公用事业计量表

相关联的公用事业管理中心 (P1-P3)。

5. 按照权利要求 4 所述的方法,其中每个所述消费值 ΔCPT 和该值 ΔCPT 涉及的公用事业计量表标识符 U_{id} 一起被保存在所述存储器中,并且所述消费值 ΔCPT 与和单个公用事业管理中心 (P1-P3) 关联并由所述数据集中器处理的全部公用事业计量表 (U1-U8) 有关。

6. 按照任意前述权利要求所述的方法,其中所述数据集中器 (C1-C4) 还连同所述资费表一起接收与可从每个所述公用事业管理中心 (P1-P3) 交付的可用公用事业的数量有关的信息。

7. 按照任意前述权利要求所述的方法,其中在收到来自数据集中器的传输询问之后,公用事业计量表响应数据集中器的请求而执行对所述公用事业计量表消息 $DTup_{u,c}$ 的发送。

8. 按照任意前述权利要求所述的方法,其中所述数据集中器向所述公用事业计量表发送配置消息,以便更新公用事业计量表消息 $DTup_{u,c}$ 的报告频度。

9. 一种包含多个公用事业计量表 (U1-U8) 的智能网内的公用事业消费的计价系统,每个公用事业计量表 (U1-U8) 与至少一个公用事业管理中心 (P1-P3) 相关,并通过利用数据集中器标识符 $DCid$ 识别的中间数据集中器 (C1-C4) 连接到所述至少一个公用事业管理中心 (P1-P3),每个公用事业计量表 (U1-U8) 是利用公用事业计量表标识符 U_{id} 识别的,并且适合于产生并向所述数据集中器发送受保护的公用事业计量表消息 $DTup_{u,c}$,每个数据集中器适合于产生并向所述管理中心 (P1-P3) 发送受保护的报告,每个管理中心 (P1-P3) 是利用管理中心标识符 P_{id} 识别的,所述系统包括:

- 连接装置,用于通过把数据集中器 (C1-C4) 分别连接到所述公用事业计量表和所述公用事业管理中心的通信网络链路 Luc 、 Lcp 来建立所述通信,

- 接收装置,用于由所述数据集中器 (C1-C4) 从每个所述公用事业管理中心 (P1-P3) 接收包含至少一个资费表的受保护的数据集中器消息,所述资费表包含每 24 小时的时段的至少一个时间间隔 $[DT1, DT2]$ 和与所述时间间隔 $[DT1, DT2]$ 相关的费率,

- 加密 / 解密装置,和 / 或用于签名和核实在所述公用事业管理中心 (P1-P3)、所述数据集中器 (C1-C4) 以及所述公用事业计量表 (U1, U8) 之间交换的所有消息的真实性和完整性的装置,

- 选择装置,用于利用所述数据集中器 (C1-C4) 比较所有资费表的所有时间间隔 $[DT1, DT2]$ 的费率,并确定每个时间间隔 $[DT1, DT2]$ 的最低费率,以便得到和保存有利的资费表,

- 测量装置,用于通过读取在每个公用事业计量表处的计数器消费指数 CPT 来确定计量数据测量结果 $DTup$,

- 在每个公用事业计量表 (U1-U8) 内产生受保护的公用事业计量表消息 $DTup_{u,c}$ 的装置,每个所述公用事业计量表消息包括:所述计量数据测量结果 $DTup$ 、所述公用事业计量表标识符 U_{id} 、所述数据集中器标识符 $DCid$ 以及所述管理中心标识符 P_{id} ,

- 公用事业计量表发送装置,用于把所述受保护的公用事业计量表消息 $DTup_{u,c}$ 传送给所述数据集中器,

- 计算装置,用于基于几个计量数据测量结果 $DTup$,确定利用由所述公用事业计量表在由第一时间 $T1$ 和第二时间 $T2$ 限定的时间间隔 ΔT 内测量的 2 个计量计数器消费指数

CPT 之差计算的计量计数器差分消费值 ΔCPT ,

- 分配装置,用于把对于包含在所述第一时间 T1 和所述第二时间 T2 之间的时间间隔 ΔT 提出最低费率的公用事业管理中心 (P1-P3) 分配给所述计量计数器差分消费值 ΔCPT ,

- 数据集中器发送装置,用于从数据集中器向所述公用事业计量表 (U1-U8) 关联的公用事业管理中心 (P1-P3) 传送受保护的报告,所述受保护的报告至少包含被分配给所述管理中心 (P1-P3) 的计量计数器差分消费值 ΔCPT 以及所述值 ΔCPT 涉及的公用事业计量表标识符 Uid,

- 管理所有所述装置的中央处理单元。

10. 按照权利要求 9 所述的系统,其中所述数据集中器包括用于在报告时期 ΔRT 内收集多个计算的消费值 ΔCPT 的存储器,之后在所述报告时期 ΔRT 结束时所述多个计算的消费值 ΔCPT 由所述数据集中器发送装置在所述受保护的报告内发送。

智能网内的公用事业消费的计价系统和方法

技术领域

[0001] 本发明涉及通过通信网络中的至少一个中间数据集中器,从至少一个公用事业管理中心监视和管理的公用事业计量表的领域。

背景技术

[0002] 进行中的全球能源分配市场中的管制解除驱动对智能公用事业分配网和智能计量表的需求,从而使公用事业提供商和消费者都能够通过开放的通信网络,在任何时候监视最终用户的详细消费量。如今特别关注能源市场,不过相关问题也与其它公用事业市场,比如水或气有关。

[0003] 尽管许多传统计量表已利用例如标准光接口或调制解调器接口,实现一些点对点自动抄表 (AMR) 协议,不过它们不能利用无线或电力线通信网络,与最终用户家庭区域网络或者远程公用事业监视设施交互作用。于是在下一个 10 年中,该行业对这种管理要求的响应在于以传统计量表换所谓的智能计量表。

[0004] 智能计量表使公用事业提供商能够通过开放的通信网络,在任何时候监视最终用户的详细消费量。消费量测量采样粒度从而可以远远小于每年约一次地人工控制计量表的传统系统中的相应采样粒度。还可以支持不同提供商的多个资费表,和按照更小的测量周期更频繁地修改它们。

[0005] 从公用事业提供商的角度看,由于不再存在依靠授权人员的就地测量和计量表功能的物理控制,智能计量体系结构需要仔细的设计,以确保从智能计量表到提供商公用事业服务设施的安全、防篡改和可信的数据收集和传输。根据现有加密协议和受公用事业提供商控制的密钥管理系统,可以定义各种解决方案。这些解决方案一般要求智能计量表专门为特定的公用事业提供商生成其测量报告消息。在智能计量表能够与多个提供商协商其资费表的解除管制的市场中,这导致带宽和处理需求增大,以及公用事业计量表的防篡改设计复杂性、制造成本和维护成本增大。

[0006] 文献 W001/06432 公开一种计算机辅助分析,用于找出一个或多个能源供应商提供的最佳替代购买物,以便实时地自动获得可能的最佳能源供应。为此,该文献提出一种分析模块,所述分析模块必须安装在最终用户侧,以便实时地跟踪多个燃料计价模型,所述模型允许根据价格和使用时间能源模式,即时切换备选能源。费率分析模块允许用户比较多种费率,确定哪个能源销售商提供的费率计划最适合于他们的需要。

[0007] 文献 US2004/0225625 公开一种费率引擎,所述费率引擎接收诸如公用事业数据和费率数据之类的输入,并基于每个记录时间间隔,生成费用数据。测量设备(公用事业计量表)收集的数据,比如用量/消费量测量结果通过网络被传送给费率引擎。另外,管理公用事业的供应的一个或多个公用事业管理实体(比如电、水或气供应商)与公用事业耦接,并可通过网络,借助费率数据服务器公布费率数据。费率引擎接收各种输入,包括公用事业数据、费率数据、时间数据和可选的元数据(例如,计费周期 id、费用中心 id、地理位置等)。输出可以是一个或多个时间间隔,费用与每个时间间隔关联。

[0008] 然而,尽管报告数据同时涉及上百万的公用事业计量表,不过这些文献都没有提出尽可能地优化交换的数据的管理,以便节约带宽和计算资源的手段。此外,这些文献仅仅提出通过已知网络交换通信,而没有注意防止某些恶意之人造成的黑客攻击和篡改。

[0009] 于是,需要更灵活的智能计量网络拓扑,以优化智能计量操作、通信和安全。

发明内容

[0010] 本发明提出一种用于由通信网络内的公用事业计量表计量的公用事业消费的计量的安全计量报告通信方法,所述通信网络包含作为中间设备,位于公用事业计量表和至少一个公用事业提供商之间的至少一个数据集中器代理。更特别地并且按照优选实施例,本发明涉及智能网内的公用事业消费的计价方法,所述智能网包括分别与至少一个公用事业管理中心关联,并且通过利用数据集中器标识符 DCid 识别的中间数据集中器,连接到所述至少一个公用事业管理中心的多个公用事业计量表,每个公用事业计量表是利用公用事业计量表标识符 Uid 识别的,并且由于安全装置,适合于产生和把受保护的公用事业计量表消息 DTup_{u,c} 发送给数据集中器,每个数据集中器适合于产生并把受保护的报告发送给管理中心,每个管理中心是利用管理中心标识符 Pid 识别的,所述方法包括以下步骤:

[0011] - 利用数据集中器,从每个所述公用事业管理中心,接收包含至少一个资费表的受保护的数据集中器消息;所述资费表包含每 24 小时的至少一个时间间隔 [DT1, DT2],和与该时间间隔相关的费率,

[0012] - 解密和 / 或核实所述数据集中器消息的真实性和完整性;在失败或不成功的情况下:中断所述数据集中器消息的处理,

[0013] - 利用数据集中器,在所有这些资费表中的所有时间间隔的费率之中,为每个时间间隔 [DT1, DT2] 选择最低的费率,以便得出有利的资费表,

[0014] - 利用数据集中器,从公用事业计量表接收公用事业计量表消息 DTup_{u,c},这些公用事业计量表消息 DTup_{u,c} 分别包括:由发送该消息 DTup_{u,c} 的公用事业计量表报告的计量数据测量结果 DTup,其公用事业计量表标识符 Uid,数据集中器标识符 DCid 和管理中心标识符 Pid,

[0015] - 解密和 / 或核实所述公用事业计量表消息的真实性和完整性,在失败或不成功的情况下:中断所述公用事业计量表消息的处理,

[0016] - 根据几个计量数据测量结果 DTup,确定利用在由第一时间 T1 和第二时间 T2 定义的时间间隔 ΔT 内,公用事业计量表测量的 2 个计量计数器消费指数 CPT 之差计算的计量计数器差分消费值 ΔCPT ,

[0017] - 把对于包含在所述第一时间 T1 和所述第二时间 T2 之间的时间间隔 ΔT ,提出最低费率的公用事业管理中心分配给该计量计数器差分消费值 ΔCPT ,

[0018] - 为每个管理中心,建立报告,所述报告至少包含分配给该管理中心的计量计数器差分消费值 ΔCPT ,以及所述值 ΔCPT 涉及的公用事业计量表标识符 Uid,

[0019] - 保护所述报告,之后把所述报告从数据集中器发送给上述公用事业管理中心,只有在解密所述报告和 / 或检查所述报告的真实性和完整性之后,所述公用事业管理中心才处理所述报告。

[0020] 本发明还涉及一种实现上述方法的系统。

附图说明

[0021] 参考附图,将更好地理解本发明,附图中:

[0022] 图 1 表示包括最终用户公用事业计量表、数据集中器和公用事业提供商管理中心的星形网络的示意图。

[0023] 图 2 表示由两个不同的公用事业提供商提供的两种资费表,和由数据集中器根据所述两种资费表计算得到的有利的资费表。

具体实施方式

[0024] 提出的解决方案包括既连接到智能计量表,又连接到许多公用事业提供商的数据集中器。

[0025] 图 1 根据连接到中间数据集中器 C2 的最终用户公用事业计量表的子集 U1、U2、U3 的星形网络,图解说明一种可能的智能网网络拓扑。该数据集中器又连接到多个公用事业提供商管理中心。集中器一般与附近地区的低压配电系统共处一地,监视多达数千个公用事业计量表。在解除管制的公用事业市场中,数据集中器 C2 还可连接到向最终用户提供竞争的公用事业交付报价的多个公用事业提供商 P1、P2、P3(图 1)。

[0026] 每个公用事业管理中心 P1、P2、P3 实现各种公用事业管理处理,比如数据管理计费、负荷管理和储运损耗控制,并通过智能网全球通信网络链路 Lpc,相应地查询和控制数据集中器 C1、C2、C3、C4。

[0027] 每个数据集中器 C1、C2、C3、C4 包括借助一方面通过本地通信网络链路 Luc,与各个计量表的安全通信,另一方面通过全球智能网网络链路 Lcp,与公用事业提供商管理中心的安全通信,负责实施计量表使用监视,和向公用事业管理中心报告的功能组件。

[0028] 图 1 的各个通信网络链路 Lcp、Luc 建立在公用事业计量通信物理网络,比如(但不限于)电缆网、电力线、无线网络或者它们的组合上,并且采用通信网络协议,比如(但不限于)网际协议(IP)v4 或 v6。在这些网络之上,关于智能网和智能计量表的通信消息接发主要由电信业产生,并且服从新出现的诸如 ANSI 或 IEC 之类的国际委员会的标准。

[0029] 在解除管制的市场中,每个最终用户可选择其优选的公用事业提供商。例如,为公用事业计量表 U1 和 U3,选择公用事业提供商 P2,而为公用事业计量表 U2,选择公用事业提供商 P1。随着公用事业报价逐渐朝着资费粒度更细,并且更新更频繁发展,公用事业计量表必须相应地处理所述资费,并与以前相比更高的频度,例如每 15 分钟报告其公用事业消费量。这既使有限的计量表处理能力过载,又使公用事业提供商和公用事业计量表之间的通信网络过载。

[0030] 借助分布式计算系统,可避免该问题,在分布式计算系统中,数据集中器 C 与每个公用事业提供商建立安全通信,从每个公用事业提供商接收可传送到单独的计量表的资费表和相关信息,比如可用公用事业的数量,并根据该信息选择最佳报价。有利的是,通过获得与每个提供商能够交付的可用公用事业的数量相关的信息,数据集中器能够在早期有效地管理与每个提供商的供给可能性有关的最终用户的需求。公用事业提供商可以是商业提供商,国家控制的提供商,或者甚至产生被重新注入公用事业输送网络的一定数量的公用事业的最终用户设施。

[0031] 数据集中器 C 还与每个公用事业计量表 U 建立安全通信,从每个公用事业计量表 U 接收定期的公用事业消费量报告 $DTup_{u,c}$, 并且按照先前的报价选择,单独地计算预定给每个公用事业提供商 P 的合并报告 $RTup_{u,p}$ 。这种解决方案的优点在于公用事业计量表只需要在任何时刻,为数据集中器 C 建立、加密和签名于一个 $DTup_{u,c}$ 消息,而不管哪个公用事业提供商实际向其进行供给,报告其消费量,而不必负责随着时间变化的详细资费的选择,以及相应的消费量计价报告的计算。公用事业计量表消息 $DTup_{u,c}$ 一般包含至少一个时间和日期 DT,和公用事业计量表 U 在该时间和日期 DT 测量的计量计数器消费指数 CPT,或者在第一时间 T1,例如以前传送的时间和日期 DT_{prev} ,和第二时间 T2,例如,当前时间和日期 DT_{curr} 之间测量的计量计数器差分消费值 ΔCPT 。在一种其中公用事业计量表和数据集中器同步通信,即,基于同步时钟通信(其中一个时钟位于公用事业计量表内,另一个时钟位于数据集中器内)的更简单的实现模式中,只有公用事业计量表消费指数被传送给负责测量对应日期和时间的数据集中器。不过,应注意这两个时钟不必具有相同的时基,例如,位于数据集中器内的时钟可以是公共时钟,而公用事业计量表的时钟可以仅仅是倒计时时钟或者能够产生脉冲的装置。在另一种备选方案中,公用事业计量表可以只应数据集中器的请求,将其消费指数传送给数据集中器。为了清楚起见,应注意用语“指数”指的是公用事业计量表计数的数字。例如,该数字可以涉及用 KW/h,或者用 m^3 ,或者用随公用事业计量表所用于的用途(即,该公用事业计量表是用于计量电、水还是气等)而定的任何其它单位表述的消费量。

[0032] 为了识别其在开放的通信网络中的来源和目的地, $DTup_{u,c}$ 消息还包括源公用事业计量表标识符和目的地数据集中器标识符。目的地数据集中器标识符可以是在制造时唯一地与设备关联的整数值,网络地址标识符,或者它们的任意组合。

[0033] 为了确保公用事业计量表消息的完整性,可进一步对所述消息签名,以致数据集中器证实计量报告来自真实的公用事业计量表源。为了按需确保公用事业计量表消息的保密性(例如,确保最终用户消费数据隐私),所述消息也可被加密,以致只有经授权的数据集中器目的地才可访问公用事业计量表数据。

[0034] 就安全设计来说,多数智能网标准要求建立公钥基础设施(PKI),其中网络中的每个节点与一对公共和私有不对称密钥(例如RSA密钥对),和由可信的中心机构签署的一系列的公钥证书(例如X.509证书)关联。在对应于图1的网络拓扑的简单实现中,为了报告其计量数据测量结果 $DTup$,公用事业计量表U1产生随机的有效负载密钥 Kp ,用数据集中器C2的公钥 $KpubC2$ 加密有效负载密钥 Kp ,并借助 Kp 加密和签名于数据测量结果 $DTup$ 。公用事业计量表U1用一个或几个消息把 $(Kp)KpubC2$ 和 $(DTup)Kp$ 传送给数据集中器C2,数据集中器C2借助其唯一的保密私钥 $KprivC2$,解密 Kp 值,随后借助先前解密的 Kp 密钥解密有效负载数据 $DTup$ 。在一种更优化的实现中,公共事业计量表和数据集中器可协商安全认证通道(SAC),以建立更长期共享的会话密钥 Ks 。所述会话密钥 Ks 可类似于先前的有效负载密钥 Kp 被使用,不过持续一段时间地被反复使用,以在公用事业计量表和数据集中器之间的点对点传输中,实现通信消息完整性和保密性。源于公用事业提供商的可用报价可由公用事业提供商P1-P3发送给连接到这些提供商的每个数据集中器C1-C4的资费表表示。为了保密地公开这些资费表,这些资费表是在受保护的公用事业提供商消息内发送的。可以利用几种方式保护所述消息。第一种方式是按照对称或私有/公共方案,加密所述消息。

保护所述消息的第二种方式是看得见地对该消息签名,以保护其内容免于任何修改。这可由发送者借助单向函数(例如,散列函数)完成,所述单向函数被应用于待发送的消息,以便获得随后利用发送者的私钥加密的散列值。加密的散列值(对应于签名)可由接收者利用发送者的公钥解密。此外,也可利用来自认证机构的证书,验证该公钥。保护消息的另一种方式是发送签名的加密消息。这种消息提供双重保护,假定一方面它受其加密层保护,以免任何容易的读取,另一方面,由于签名和证书的保护而避免其内容的任何篡改。从而,消息的真实性和完整性可有利地与其加密结合。可以对任何消息,例如对公用事业消息或者数据集中器消息,应用加密和/或签名操作。

[0035] 如图2中所示,资费表提供消费单位计价值,例如0.15分每kw/h,该消费单位计价值被映射到日期和时间间隔[DT1, DT2],例如每天从DT1=22:00到DT2=22:30:00。资费表必须包含每24小时的至少一个时间间隔[DT1, DT2],和与该时间间隔相关的费率。通过比较各个提供商的报价,例如提供商P1的资费表1和提供商P2的资费表2,数据集中器C2识别由开始时间和日期DT1及终止时间和日期DT2定义的最佳报价实际计价期,例如从DT122:00~DT222:30,费率为0.15的P1,如图2中的表3所示。从而,数据集中器可根据几个资费表(资费表1和资费表2),得到和计算出有利的资费表(资费表3)。最好,有利的资费表将被保存在数据集中器的存储器内。

[0036] 数据集中器每隔一定时间,例如每15分钟,从每个连接的公用事业计量表,接收包含从每个连接的公用事业计量表发送的计量数据测量结果DTup的公用事业报告消息DTup_{u,c},解密相关的公用事业报告消息DTup_{u,c},并核实其签名。如果该消息被验证,那么数据集中器从定义为计量数据测量结果DTup的传送的一系列的计数器值CPT或者差分值 ΔCPT ,得到在计价时间间隔[DT1, DT2]中,来自公用事业计量表的消费值。如果公用事业计量表本身还未确定差分值 ΔCPT ,那么数据集中器得出在特定时间和日期DT2的计量计数器值CPT2与在特定时间和日期DT1的计量计数器值CPT1之间的差分 $\Delta CPT_{1,2}$ 。从而,取决于公用事业计量表的技术性质和其预定任务,目的地数据集中器必须根据几个计量数据测量结果,确定差分概念值 ΔCPT 。更一般地,计量数据测量结果DTup可包含不同的数据,即:

[0037] - 至少一个计量计数器消费指数CPT;或者

[0038] - 至少一个计量计数器消费指数CPT,以及由所述公用事业计量表可读的时钟产生的,并且与测量该计数器消费指数的时刻对应的时间和日期DT信息;或者

[0039] - 直接包含计量计数器差分消费值 ΔCPT ,例如,如果公用事业计量表能够进行这种计算任务的话。

[0040] 在一个实施例中,数据集中器C随后把计算的差分 $\Delta CPT_{1,2}$ 传送给在资费期[DT1, DT2]内,与公用事业计量表U相关的公用事业提供商P。于是,数据集中器把计算的差分消费值 ΔCPT 分配给在测量所述值 ΔCPT 的时间间隔 ΔT 内,报出最低费率的公用事业管理中心P1-P3。从而,所述值 ΔCPT 最好连同所述公用事业计量表的公用事业计量表标识符U_{id}一起,从目的地数据集中器被发送给适当的公用事业管理中心,即,与被分配给差分消费值 ΔCPT 的费率相关的公用事业管理中心。

[0041] 在另一个实施例中,数据集中器C持续特定的报告时期 ΔRT ([RTa, RTb]),例如1天、1周或1月,为公用事业计量表收集和计算一系列(即,多个)值 $\Delta CPT_{1,2}$ 、 $\Delta CPT_{2,3}$ 、

$\Delta CPT_{3,4}$, 并记录在数据集中器的存储器中, 例如记录在公用事业计量表消费计价报告 $MRup_{u,c,p}$ 中。在报告时期 RTb 结束之后, 提出的分布式计算系统中的数据集中器 C 与和每个公用事业计量表 U 相关的 $P1$ 、 $P2$ 、 $P3$ 之中的每个公用事业提供商 P 建立安全通信, 并且例如通过发送公用事业计量表消费计价报告 $MRup_{u,c,p}$, 把收集的消耗值 ΔCPT 传送给该公用事业提供商 P 。这种解决方案的优点在于每个报告时期, 公用事业提供商只需要处理一个公用事业计量表消费计价报告消息 $MRup_{u,c,p}$, 而不管公用事业计量表消费报告的实际细微增益粒度, 也不管这期间的实际资费更新。通过提供合并的报告消息, 可有利地减少报告消息的数目, 于是, 能够节约带宽和计算资源。

[0042] 为了识别其在开放的通信网络中的来源和目的地, 公用事业计量表消费计价报告消息 $MRup_{u,c,p}$ 还包括源公用事业计量表标识符 Uid 。最好, 它还包括目的地数据集中器标识符 $DCid$ 和公用事业提供商标识符 Pid 。这些标识符可以是在制造时唯一地与设备相关的整数值, 网络地址标识符或者它们的任何组合。

[0043] 为了确保公用事业计量表消费计价报告消息 $MRup_{u,c,p}$ 的完整性, 该消息可被签名, 以致公用事业提供商证实计量报告来自于真实的数据集中器源。为了根据需要, 确保公用事业计量表消费量的保密性 (例如, 确保最终用户隐私), 公用事业计量表消费计价报告消息 $MRup_{u,c,p}$ 还可被加密, 以致只有经授权的公用事业提供商才可访问公用事业计量表数据。

[0044] 在另一个实施例中, 数据集中器 C 持续特定的报告时期 $[RT1, RT2]$, 例如 1 天、1 周或者 1 月, 为都与单个公用事业管理中心相关的多个公用事业计量表 (例如, 为与公用事业提供商 $P2$ 相关的每个公用事业计量表 $U1$ 、 $U3$) 收集和计算一系列的值 $\Delta CPT_{U1,2}$ 、 $\Delta CPT_{U3,2}$ 、 $\Delta CPT_{U1,3}$ 、 $\Delta CPT_{U3,3}$ 、 $\Delta CPT_{U1,4}$ 、 $\Delta CPT_{U3,4}$, 并把这些值连同每个这些值所涉及的公用事业计量表标识符 Uid 一起记录在合并的公用事业计量表消费计价报告 $CR_{c,p}$ 中。在报告时期 $RT2$ 结束之后, 提出的分布式计算系统中的数据集中器 C 与和公用事业计量表的子集 $U1$ 、 $U3$ 相关的公用事业提供商 $P2$ 建立安全通信, 把合并的公用事业计量表消费计价报告 $CR_{c,p}$ 传送给公用事业提供商 $P2$ 。这种解决方案的优点在于每段时间, 每个公用事业提供商只需要为每个数据集中器, 而不是为每个公用事业计量表处理一个合并的消费计价报告消息 $CR_{c,p}$ 。

[0045] 为了识别其在开放的通信网络中的来源和目的地, 合并的消费计价报告消息 $CR_{c,p}$ 还包括源公用事业计量表标识符 Uid 、目的地数据集中器标识符 $DCid$ 和公用事业提供商标识符 Pid 的列表。这些标识符可以是在制造时唯一地与设备相关的整数值, 网络地址标识符或者它们的任何组合。

[0046] 为了确保合并的消费计价报告消息 $CR_{c,p}$ 的完整性, 该消息可被签名, 以致公用事业提供商证实计量报告来自于真实的数据集中器源。为了根据需要, 确保公用事业计量表消费量的保密性 (例如, 确保最终用户隐私), 公用事业计量表消费计价报告消息 $CR_{c,p}$ 还可被加密, 以致只有经授权的公用事业提供商才可访问公用事业计量表数据。这使公用事业提供商能够以与他们和数据集中器协商其报价的频度更低的频度, 例如每月仅仅一次地为计价收集公用事业计量报告, 而不管在该月中, 频度有多频繁地被更新。由于在典型的网络拓扑中, 存在比数据集中器多得多的公用事业计量表, 和服务它们的几个公用事业提供商, 因此总的来说, 能够节约相当大的带宽和处理能力。这将用只是用于举例说明, 而不是对本发明的限制的以下例子例示: 如果某个局部区域中的 1000 个计量表将每 15 分钟向 5 个

可能的公用事业提供商报告,那么它们每天分别需要产生、保护和传送 $24 \times 4 \times 5 = 4800$ 条消息,而仅仅对于该局部区域,每个公用事业提供商每天就需要接收和处理 $24 \times 4 \times 1000 = 96000$ 条消息。借助提出的一种可能的解决方案,公用事业计量表每天只产生、保护和向数据集中器传送 24×4 条消息,不需要与 5 个公用事业提供商建立单独的安全通信通道。数据集中器负责根据预先选择的报价,和来自 5 个公用事业提供商的对应资费表,本地计算和合并 1000 个公用事业计量报告。随后,数据集中器可以为 1000 个公用事业计量表,合并给最多 5 个提供商的计价报告,例如每天仅仅一次,即,每天对于 1000 个公用事业计量表,公用事业提供商只需要接收和处理最多 1000 条单独的消息或者 1 条合并的消息。

[0047] 在数据集中器和公用事业计量表之间的网络不可靠的情况下,公用事业计量消息 DTup 可能丢失。在这种结构中,最好传送计数器指数 CPT,而不是相对差分值 ΔCPT 作为计量数据测量结果 DTup,以致数据集中器仍然能够根据最后接收的消费值和当前消费值,内插丢失的消费值,从而相应地得到可接受的消费计价。

[0048] 另一方面,数据集中器还可向公用事业计量表发送收到确认和 / 或重传询问。

[0049] 假定提供商、中间数据集中器 C1-C4 和公用事业计量表 U1-U8 在通信网络内被互连,并且假定借助标识符 Uid、DCid、Pid,在交换的消息中识别发送者和接收者,那么有利的是,发送给特定接收者(例如,数据集中器 DCid 或者提供商 Pid)的消息可被备选接收者重新路由到适当的接收者。这种漫游可由中间数据集中器进行,或者由会收到消息(例如,公用事业计量表消息 DTup_{u,c} 或者公用事业计量表消费计价报告消息 MRup_{u,c,p})的提供商进行,尽管它不是该消息的适当接收者。例如,如果发送者的消息由于许多原因(比如临时维护,或者针对某个接收者的通信的失败)而不能到达其接收者,那么可以应用这种漫游。

[0050] 数据集中器还可定期地,例如在向公用事业提供商报告合并之后,把关于有关的实际报价和 / 或计价的信息发送给最终用户。

[0051] 数据集中器还可向公用事业计量表发送配置消息,以更新其报告频度。

[0052] 最好,每次必须交换消息或报告时,本发明的方法进行目的在于为连接到目的地数据集中器 C1-C4 的每个公用事业计量表 U1-U8,和为连接到所述公用事业管理中心 P1-P3 的每个数据集中器 C1-C4,分别建立安全通信的步骤。所述通信是通过签名和加密消息来保护的,报告分别由目的地数据集中器 C1-C4 和公用事业管理中心 P1-P3 处理。只有当其被验证装置识别为可信时,消息和报告才被处理。

[0053] 本发明还涉及一种实现上面公开的方法的系统。为此,本发明提出一种用于包含多个公用事业计量表 U1-U8 的智能网内的公用事业消费的计价系统,这些公用事业计量表分别与至少一个公用事业管理中心 P1-P3 相关,并通过中间数据集中器 C1-C4 连接到所述至少一个公用事业管理中心 P1-P3,每个数据集中器是利用数据集中器标识符 DCid 识别的,而每个公用事业计量表 U1-U8 是利用公用事业计量表标识符 Uid 识别的。这些公用事业计量表适合于产生并向它们连接到的或者与之关联的数据集中器发送受保护的公用事业计量表消息 DTup_{u,c}。每个数据集中器适合于产生并向管理中心 P1-P3,尤其是向与该数据集中器处理的公用事业计量表相关的所有管理中心发送受保护的报告,每个管理中心是利用管理中心标识符 Pid 识别的,所述系统包括:

[0054] - 连接装置,用于通过把数据集中器连接到与该数据集中器相关的公用事业计量表的通信网络链路 Luc,和通过把该数据集中器连接到公用事业管理中心,最好连接到多个

公用事业管理中心的通信网络链路 Lcp, 建立通信,

[0055] - 位于数据集中器 C1-C4 内的接收装置, 用于从连接到该数据集中器的每个公用事业管理中心 P1-P3, 接收包含至少一个资费表的受保护的数据集中器消息; 所述资费表包含每 24 小时的至少一个时间间隔 [DT1, DT2], 和与该时间间隔 [DT1, DT2] 相关的费率,

[0056] - 加密 / 解密装置, 和 / 或用于签名和核实在所述公用事业管理中心 (P1-P3)、所述数据集中器 (C1-C4) 和所述公用事业计量表 (U1, U8) 之间交换的所有消息的真实性和完整性的装置,

[0057] - 位于数据集中器内的选择装置, 用于进行所有资费表的所有时间间隔 [DT1, DT2] 的费率的比较, 随后确定每个时间间隔 [DT1, DT2] 的最低费率, 从而得到例如可被保存在数据集中器内的有利资费表,

[0058] - 测量装置, 用于通过读取在每个公用事业计量表的计数器消费指数 CPT, 确定计量数据测量结果 DTup,

[0059] - 用于在每个公用事业计量表 U1-U8 内, 产生受保护的公用事业计量表消息 DTup_{u,c} 的装置; 这些公用事业计量表消息都包括: 计量数据测量结果 DTup, 公用事业计量表标识符 Uid, 数据集中器标识符 DCid 和管理中心标识符 Pid,

[0060] - 公用事业计量表发送装置, 用于把这些受保护的公用事业计量表消息 DTup_{u,c} 传送给适当的数据集中器, 即, 传送给与这些发送装置的公用事业计量表相连的数据集中器,

[0061] - 计算装置, 用于根据几个计量数据测量结果 DTup, 确定利用公用事业计量表在由第一时间 T1 和第二时间 T2 定义的时间间隔 ΔT 内测量的 2 个计量计数器消费指数 CPT 之差计算的计量计数器差分消费值 ΔCPT ,

[0062] - 分配装置, 用于使在由时间 T1 和 T2 定义的时间间隔 ΔT 内, 报出最低费率的公用事业管理中心 P1-P3 与该计量计数器差分消费值 ΔCPT 关联,

[0063] - 数据集中器发送装置, 用于从数据集中器向所述公用事业计量表 U1-U8 关联的公用事业管理中心 P1-P3, 传送受保护的报告, 所述报告至少一方面包含被分配给该管理中心 P1-P3 的计量计数器差分消费值 ΔCPT , 另一方面, 包含所述值 ΔCPT 涉及的公用事业计量表标识符 Uid,

[0064] - 管理所有上述装置的中央处理器。

[0065] 所有上述装置可用特定模块实现, 所述特定模块包含能够实现每个这些模块所涉及的功能的电子组件。

[0066] 按照一个实施例, 系统的每个公用事业计量表还包括可由所述测量装置读取, 用于把与测量计数器消费指数 CPT 的时刻对应的时间和日期 DT 包含在计量数据测量结果 DTup 中的时钟。

[0067] 按照另一个实施例, 系统的目的地数据集中器包括用于在报告时期 ΔRT 内, 收集多个计算的消费值 ΔCPT 的存储器, 之后例如在报告时期 ΔRT 结束时, 在数据集中器的发送装置传送的受保护报告内, 把所述多个计算的消费值 ΔCPT 发送给适当的公用事业管理中心。

[0068] 从而, 本发明的系统包括保护一方面在公用事业计量表和目的地数据集中器之间交换的通信, 和另一方面, 在目的地数据集中器和与这些公用事业计量表相关的至少一个公用事业管理中心之间交换的通信的装置。利用普通手段, 即, 利用应用于由公用事业计量

表发送的公用事业计量表消息 $DTup_{u,c}$, 和应用于由目的地数据集中器发送的报告签名和加密手段, 实现受保护的通信。于是, 系统具备获得公钥证书的装置, 验证这些证书的装置, 产生会话密钥 (一般随机的会话密钥) 的装置, 用这些密钥加密和解密消息的装置, 和在传输完全成功的情况下, 发送和接收确认消息的装置。

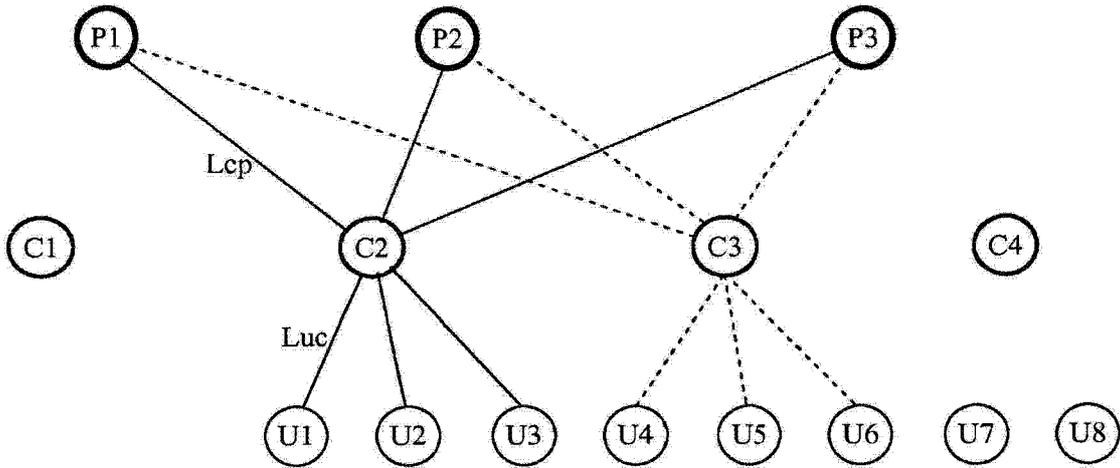


图 1

开始时间	终止时间	资费
22:00	06:00	0.15
06:00	09:00	0.25
09:00	12:00	0.15
12:00	14:00	0.20
14:00	17:00	0.15
17:00	22:00	0.25

表 1-公用事业提供商 P1 资费表

开始时间	终止时间	资费
22:30	05:00	0.10
05:00	22:30	0.20

表 2-公用事业提供商 P2 资费表

开始时间	终止时间	资费	提供商
22:00	22:30	0.15	P1
22:30	05:00	0.10	P2
05:00	06:00	0.15	P1
06:00	09:00	0.20	P2
09:00	12:00	0.15	P1
12:00	14:00	0.20	P1
14:00	17:00	0.15	P1
17:00	22:00	0.20	P2

表 3-数据集中器选择的报价

图 2