



(12) 发明专利

(10) 授权公告号 CN 101518112 B

(45) 授权公告日 2012. 08. 15

(21) 申请号 200780034277. 4

G09C 1/00 (2006. 01)

(22) 申请日 2007. 09. 18

(56) 对比文件

(30) 优先权数据

60/845, 634 2006. 09. 18 US

US 2004/0228490 A1, 2004. 11. 18,

CN 1550116 A, 2004. 11. 24,

(85) PCT申请进入国家阶段日

2009. 03. 16

审查员 牛晓佳

(86) PCT申请的申请数据

PCT/US2007/078803 2007. 09. 18

(87) PCT申请的公布数据

W02008/039662 EN 2008. 04. 03

(73) 专利权人 英特尔公司

地址 美国加利福尼亚州

(72) 发明人 J·沃尔克 M·赵

(74) 专利代理机构 中国专利代理(香港)有限公

司 72001

代理人 柯广华 王丹昕

(51) Int. Cl.

H04L 9/32 (2006. 01)

H04W 12/04 (2009. 01)

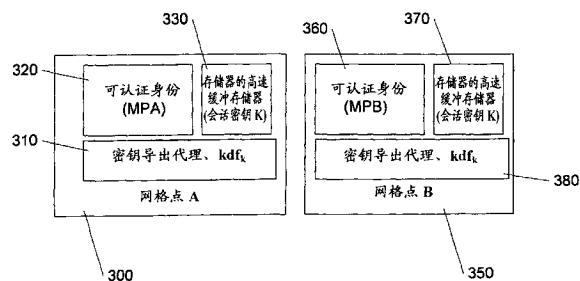
权利要求书 3 页 说明书 4 页 附图 3 页

(54) 发明名称

用于无线网络网络中的安全通信的密钥导出的技术

(57) 摘要

与用于网格网络的网格链路建立协议兼容的密钥导出流程和密钥层次。可使用是表示为 Kdf_K 的密钥导出函数的单加密原语, 其中 K 是缓存的成对主密钥。函数 kdf_K 的结果可用于导出密钥, 所述密钥用于对链路建立和随后在该链路上交换的数据进行保护。



1. 一种用于在无线网络网络中建立安全链路的方法,包括:

响应于具有网格网络中的远程点的地址的消息,计算一个或多个加密密钥;

与所述网格网络的所述远程点交换一个或多个伪随机值;

至少部分基于所述一个或多个加密密钥和一个或多个伪随机值生成密钥值;以及

将所述生成的密钥值用于与所述网格网络的所述远程点的安全通信,

其中,至少部分基于所述一个或多个加密密钥和一个或多个伪随机值生成密钥值包括估计:

$$KCK || KEK \leftarrow kdf_k(0x00 || \max(MPA, MPB) || \min(MPA, MPB))$$

其中,“ $\leftarrow$ ”表示将密钥导出函数(kdf_k)的表达式赋值给变量 $KCK || KEK$,且其中,“ $KCK || KEK$ ”表示导出的密钥确认密钥与导出的密钥加密密钥的级联,所述密钥加密密钥在链路建立中用于分配广播密钥,并且“ $||$ ”表示级联,“ $\max(MPA, MPB)$ ”表示MPA和MPB中的较大者而“ $\min(MPA, MPB)$ ”表示MPA和MPB中的较小者,其中MPA表示所述远程点的地址而MPB表示本地点的地址。

2. 如权利要求1所述的方法,其中,所述消息包括信标消息。

3. 如权利要求1所述的方法,其中,所述消息包括探测响应消息。

4. 一种用于在无线网络网络中建立安全链路的方法,包括:

响应于具有网格网络中的远程点的地址的消息,计算一个或多个加密密钥;

与所述网格网络的所述远程点交换一个或多个伪随机值;

至少部分基于所述一个或多个加密密钥和一个或多个伪随机值生成密钥值;以及

将所述生成的密钥值用于与所述网格网络的所述远程点的安全通信,

其中,至少部分基于所述一个或多个加密密钥和一个或多个伪随机值生成密钥值包括估计:

$$KDK \leftarrow kdf_k(0x01 || \max(MPA, MPB) || \min(MPA, MPB))$$

其中,“ $\leftarrow$ ”表示将密钥导出函数(kdf_k)的表达式赋值给变量KDK,且其中,“KDK”表示导出的密钥导出密钥,将用于构建网格链路建立协议所建立的会话密钥,并且“ $||$ ”表示级联,“ $\max(MPA, MPB)$ ”表示MPA和MPB中的较大者而“ $\min(MPA, MPB)$ ”表示MPA和MPB中的较小者,其中MPA表示所述远程点的地址而MPB表示本地点的地址。

5. 如权利要求4所述的方法,其中,所述消息包括信标消息。

6. 如权利要求4所述的方法,其中,所述消息包括探测响应消息。

7. 一种用于在无线网络网络中建立安全链路的方法,包括:

响应于具有网格网络中的远程点的地址的消息,计算一个或多个加密密钥;

与所述网格网络的所述远程点交换一个或多个伪随机值;

至少部分基于所述一个或多个加密密钥和一个或多个伪随机值生成密钥值;以及

将所述生成的密钥值用于与所述网格网络的所述远程点的安全通信,

其中,至少部分基于所述一个或多个加密密钥和一个或多个伪随机值生成密钥值包括估计:

$$KCK || KEK || TK \leftarrow kdf_k(\max(MPA, MPB) || \min(MPA, MPB) || \max(RA, RB) || \min(RA, RB))$$

其中,“ $\leftarrow$ ”表示将密钥导出函数(kdf_k)的表达式赋值给变量 $KCK || KEK || TK$,且其中,“ $KCK || KEK || TK$ ”表示导出的密钥确认密钥、导出的密钥加密密钥以及数据加密密钥的级

联, RA 是由所述网格网络的所述远程点所创建的随机值, 而 RB 是由所述网格网络的本地点所创建的随机值, 并且“||”表示级联, “max(MPA, MPB)”表示 MPA 和 MPB 中的较大者而“min(MPA, MPB)”表示 MPA 和 MPB 中的较小者, 其中 MPA 表示所述远程点的地址而 MPB 表示本地点的地址。

8. 如权利要求 7 所述的方法, 其中, 所述消息包括信标消息。

9. 如权利要求 7 所述的方法, 其中, 所述消息包括探测响应消息。

10. 一种用于在无线网络中建立安全链路的装置, 包括:

用于响应于具有网格网络中的远程点的地址的消息计算一个或多个加密密钥的部件;

用于与所述网格网络的所述远程点交换一个或多个伪随机值的部件;

用于至少部分基于所述一个或多个加密密钥和一个或多个伪随机值生成密钥值的部件; 以及

用于将所述生成的密钥值用于与所述网格网络的所述远程点的安全通信的部件,

其中, 用于至少部分基于所述一个或多个加密密钥和一个或多个伪随机值生成密钥值的部件包括用于对下列项进行估计的部件:

$$KCK || KEK \leftarrow \text{kdf}_k(0x00 || \max(MPA, MPB) || \min(MPA, MPB))$$

其中, “ $\leftarrow$ ”表示将密钥导出函数 (kdf_k) 的表达式赋值给变量 KCK || KEK; 且其中, “KCK || KEK”表示导出的密钥确认密钥与导出的密钥加密密钥的级联, 所述密钥加密密钥在链路建立中用于分配广播密钥, 并且“||”表示级联, “max(MPA, MPB)”表示 MPA 和 MPB 中的较大者而“min(MPA, MPB)”表示 MPA 和 MPB 中的较小者, 其中 MPA 表示所述远程点的地址而 MPB 表示本地点的地址。

11. 如权利要求 10 所述的装置, 其中, 所述消息包括信标消息。

12. 如权利要求 10 所述的装置, 其中, 所述消息包括探测响应消息。

13. 一种用于在无线网络中建立安全链路的装置, 包括:

用于响应于具有网格网络中的远程点的地址的消息计算一个或多个加密密钥的部件;

用于与所述网格网络的所述远程点交换一个或多个伪随机值的部件;

用于至少部分基于所述一个或多个加密密钥和一个或多个伪随机值生成密钥值的部件; 以及

用于将所述生成的密钥值用于与所述网格网络的所述远程点的安全通信的部件,

其中, 用于至少部分基于所述一个或多个加密密钥和一个或多个伪随机值生成密钥值的部件包括用于对下列项进行估计的部件:

$$KDK \leftarrow \text{kdf}_k(0x01 || \max(MPA, MPB) || \min(MPA, MPB))$$

其中, “ $\leftarrow$ ”表示将密钥导出函数 (kdf_k) 的表达式赋值给变量 KDK; 且其中, “KDK”表示导出的密钥导出密钥, 将用于构建网格链路建立协议所建立的会话密钥, 并且“||”表示级联, “max(MPA, MPB)”表示 MPA 和 MPB 中的较大者而“min(MPA, MPB)”表示 MPA 和 MPB 中的较小者, 其中 MPA 表示所述远程点的地址而 MPB 表示本地点的地址。

14. 如权利要求 13 所述的装置, 其中, 所述消息包括信标消息。

15. 如权利要求 13 所述的装置, 其中, 所述消息包括探测响应消息。

16. 一种用于在无线网络网络中建立安全链路的装置,包括:

用于响应于具有网格网络中的远程点的地址的消息计算一个或多个加密密钥的部件;

用于与所述网格网络的所述远程点交换一个或多个伪随机值的部件;

用于至少部分基于所述一个或多个加密密钥和一个或多个伪随机值生成密钥值的部件;以及

用于将所述生成的密钥值用于与所述网格网络的所述远程点的安全通信的部件,

其中,用于至少部分基于所述一个或多个加密密钥和一个或多个伪随机值生成密钥值的部件包括用于对下列项进行估计的部件:

$$KCK || KEK || TK \leftarrow kdf_k(\max(MPA, MPB) || \min(MPA, MPB) || \max(RA, RB) || \min(RA, RB))$$

其中,“ $\leftarrow$ ”表示将密钥导出函数(kdf_k)的表达式赋值给变量 $KCK || KEK || TK$,且其中,“ $KCK || KEK || TK$ ”表示导出的密钥确认密钥、导出的密钥加密密钥以及数据加密密钥的级联, RA 是由所述网格网络的所述远程点所创建的随机值,而 RB 是由所述网格网络的本地地点所创建的随机值,并且“ $||$ ”表示级联,“ $\max(MPA, MPB)$ ”表示 MPA 和 MPB 中的较大者,“ $\min(MPA, MPB)$ ”表示 MPA 和 MPB 中的较小者,其中 MPA 表示所述远程点的地址而 MPB 表示本地地点的地址。

17. 如权利要求16所述的装置,其中,所述消息包括信标消息。

18. 如权利要求16所述的装置,其中,所述消息包括探测响应消息。

用于无线网络网络中的安全通信的密钥导出的技术

本申请要求 2006 年 9 月 18 日提交的 US 临时专利申请号 60/845634 的优先权。

技术领域

[0001] 本发明的实施例涉及无线通信。更具体而言,本发明的实施例涉及无线网络网络(wireless mesh network)的安全性。

背景技术

[0002] IEEE 802.11s 是对 IEEE 802.11 标准开发的改进,该标准完成时旨在提供给无线局域网(WLAN)标准增加网格能力的协议。网格体系结构允许数据在由多个无线跳(hop)构成的路径上转发。授权 IEEE 802.11s 以在转换时没有降低安全性且没有使服务质量(QoS)退化的情况下通过增加网格能力改善数据传输的吞吐量。该改进带来的优点之一是在网格网络上提供视频流媒体的能力。发明内容附图说明在附图中,以示例方式而不以限制的方式示出本发明的实施例,图中相同参考标号是指类似单元。图 1 是电子系统的一种实施例的框图。图 2 示出网格网络的两点之间的链路建立的一种实施例。图 3 是可如本文所述那样进行通信的两个网格点的一种实施例的框图。

具体实施方式

[0003] 在以下描述中,给出了许多具体细节。但是没有这些具体细节也可实施本发明的实施例。在其它情况下,没有详细示出众所周知的电路、结构和技术以免混淆对本说明的理解。

[0004] 视频流分配给网格网络设计施加了约束,因为必需建立网格上的对等链路而不管与 Wi-Fi 媒体有关的噪声。已存在针对安全对等链路建立过程是否可在足够短的时间帧中完成以满足视频流分配所施加的约束的关注。

[0005] 一种技术是通过将安全握手覆盖在基本对等链路建立协议之上而加速建立安全对等链路的流程。如果无线 LAN 网格点(MeshPoint:MP)具有先验知识和先前建立的成对主密钥(Pairwise MasterKey:PMK)的控制,则该方案可允许它们省略安全链路建立过程中的某些步骤。假如 MP 频繁地丢失某些链路上的连通性,则该方法可增强网格上的视频流应用的用户体验。在一种实施例中,本文所述的技术在比使用 802.11i 密钥层次进行链路建立过程的更早阶段使用密钥,这意味着 802.11i 密钥流程以 802.11s 要求不能正确工作。

[0006] 网格网络的各网格点可为电子系统。图 1 是电子系统的一种实施例的框图。图 1 中示出的电子系统旨在表示电子系统(有线的或无线的)的范围,包括例如桌上型计算机系统、膝上型计算机系统、蜂窝电话、包括蜂窝使能 PDA 的个人数字助理(PDA)、机顶盒。备选电子系统可包括更多、更少和/或不同组件。

[0007] 电子系统 100 包括通信信息的总线 105 或其它通信装置以及耦合到总线 105、可处理信息的处理器 110。虽然以单个处理器示出电子系统 100,但是电子系统 100 可包括多个处理器和/或协同处理器。电子系统 100 还可包括耦合到总线 105 并可存储信息以及可被

处理器 110 执行的指令的随机存取存储器 (RAM) 或其它动态存储装置 120 (被称为主存储器)。主存储器 120 还可用于在处理器 110 执行指令期间存储临时变量或其它中间信息。

[0008] 电子系统 100 还可包括耦合到总线 105、可存储处理器 110 的静态信息和指令的只读存储器 (ROM) 和 / 或其它静态存储装置 130。数据存储装置 140 可耦合到总线 105 以便存储信息和指令。例如磁盘或光盘的数据存储装置 140 及对应驱动器可耦合到电子系统 100。

[0009] 电子系统 100 还可经总线 105 耦合到例如阴极射线管 (CRT) 或液晶显示器 (LCD) 的显示装置 150, 以便向用户显示信息。包括字母数字和其它按键的字母数字输入装置 160 可耦合到总线 105 以向处理器 110 通信信息和命令选择。另一类型的用户输入装置是向处理器 110 通信方向信息和命令选择并控制显示器 150 上的光标移动的光标控制 170, 例如鼠标、跟踪球或光标方向按键。

[0010] 电子系统 100 还可包括网络接口 180 以提供对例如局域网的网络的接入。例如, 网络接口 180 可包括具有可表示一个或多个天线的天线 185 的无线网络接口。例如, 网络接口 180 还可包括经由例如可为以太网电缆、同轴电缆、光缆、串行电缆或并行电缆的网络电缆 187 与远程装置通信的有线网络接口。

[0011] 在一种实施例中, 网络接口 180 可例如通过符合 IEEE802.11 标准而提供对局域网的接入, 和 / 或无线网络接口可例如通过符合 **Bluetooth®** (蓝牙) 标准而提供对个人区域网络的接入。**Bluetooth®** 是由 Bluetooth SIG 公司 (Bluetooth SIG, Inc.) 所拥有的注册商标。其它无线网络接口和 / 或协议也可被支持。

[0012] IEEE 802.11 标准可包括例如 IEEE 802.11b、IEEE 802.11g 以及本文没有具体提到的其它 IEEE 802.11 标准。IEEE 802.11b 与 1999 年 9 月 16 日核准的名为《局域网和城域网, 第二部: 无线 LAN 媒体接入控制 (MAC) 和物理层 (PHY) 规范: 在 2.4GHz 波段的更高速物理层扩展》("Local and Metropolitan Area Networks, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4GHz Band") 的 IEEE Std. 802.11b-1999 以及其它相关文档对应。IEEE802.11g 与 2003 年 6 月 27 日核准的名为《局域网和城域网, 第二部: 无线 LAN 媒体接入控制 (MAC) 和物理层 (PHY) 规范, 修订 4: 在 2.4GHz 波段的进一步更高速率扩展》("Local and Metropolitan Area Networks, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 4: Further Higher Rate Extension in the 2.4GHz Band") 的 IEEE Std. 802.11g-2003 以及其它相关文档对应。在由 Bluetooth 特别兴趣小组公司 (Bluetooth Special Interest Group, Inc.) 在 2001 年 2 月 22 日出版的《Bluetooth 系统规范: 核心、版本 1.1》("Specification of the Bluetooth System: Core, Version 1.1") 中描述了 Bluetooth 协议。

[0013] 本文所述的是与用于网格网络的网格四 - 消息链路建立协议兼容的密钥导出流程和密钥层次。在一种实施例中, 可使用作为表示为 kdf_K 的密钥导出函数的单加密原语, 其中 K 是缓存的成对主密钥。在一种实施例中, 可使用 kdf_K 来导出对链路建立及随后在该链路上所交换数据进行保护的密钥。

[0014] 密钥导出过程可在两个网格点之间完成。第一网格点被称为网格点 A, 并由其 IEEE 802.11MAC 地址 MPA 标识。第二网格点被称为网格点 B, 并由其 IEEE 802.11MAC 地址

MPB 标识。在一种实施例中,网格点 A 和网格点 B 可维持缓存的成对主密钥 K。如在 IEEE 802.11i 中所定义,所述成对主密钥 K 可为授权令牌,授权令牌的拥有证明接入无线通信信道的授权。在备选实施例中,可用不同于 MAC 地址的信息获得标识。

[0015] 以下描述假设成对主密钥 K 只在网格点 A 和网格点 B 之间被共享。该描述还假设 K 以超出本说明书范围的某种安全模式建立并可以本领域中已知的任意方式实现。

[0016] 因为只有 A 和 B 知晓 K,所以 K 可被用来向 A 认证 B 或向 B 认证 A。因此,本文所述的技术假设 A 和 B 知晓 K 的预期目的,所述预期目的包括建立 A 和 B 之间的新链路。在一种实施例中,IEEE802.11MAC 地址可以按编字典方式 (lexicographically) 排序,因此较大、较小、最小和最大的概念是定义明确的。

[0017] 函数 kdf 可基于伪随机函数。这意味着即使密钥导出中使用的输入仅单个位不同,对于攻击者而言使由 kdf 根据 K 所计算出的两个不同密钥关联在运算上也是不可行的。图 2 示出网格网络的两点之间的链路建立的一种实施例。

[0018] 在 A 或 B 希望与另一个建立安全链路时,它使用 K 来计算:

$$KCK \parallel KEK \leftarrow kdf_K(0x00 \parallel \max(MPA, MPB) \parallel \min(MPA, MPB))$$

$$KDK \leftarrow kdf_K(0x01 \parallel \max(MPA, MPB) \parallel \min(MPA, MPB))$$
 其中,“ $a \leftarrow b$ ”表示将表达式 b 赋值给变量 a;“ $a \parallel b$ ”表示 a 和 b 的级联;KCK 表示导出的密钥确认密钥 (key confirmation key)——又称为授权密钥,在链路建立期间使用;KEK 表示导出的密钥加密密钥 (key encryption key),在链路建立中用于分配广播密钥;KDK 表示导出的密钥导出密钥 (key derivation key),其将用于构建由网格链路建立协议所建立的会话密钥。KDK 用于与网格链路建立协议的第二消息合作导出 IEEE 802.11 数据加密密钥 TK 的网格模拟:

$$TK \leftarrow kdf_{KDK}(\max(RA, RB) \parallel \min(RA, RB))$$
 其中,RA 是由 A 在其第一链路建立消息中所提供的随机比特字符串,而 RB 是由 B 在其第一链路建立消息中所提供的随机比特字符串。

[0019] 该过程将导出的密钥分别与 A 和 B 的 MAC 地址 MPA 和 MPB 结合。可断言导出的密钥只可用于 A 和 B 之间的通信。因为本文所述的技术假设 kdf 基于伪随机函数,所以对于攻击者而言从任意其它密钥知晓密钥之一在运算上是不可行的。

[0020] 为保护链路建立协议,使用第一信息中的 KCK 和 KEK 是有利的,因为该协议工作于对等模型。这允许 KCK 在 IEEE 802.11s 网格中的使用比 802.11i 密钥导出所能够的更早,以便保护对等模型内的链路建立协议。在一种实施例中,802.11i 密钥导出流程为:

$$KCK \parallel KEK \parallel TK \leftarrow kdf_K(\max(MPA, MPB) \parallel \min(MPA, MPB) \parallel \max(RA, RB) \parallel \min(RA, RB))$$
 其中,RA 是由 A 产生的随机值,RB 是由 B 产生的随机值。这将所述密钥结合到链路建立示例。

[0021] IEEE 802.11i 协议可切实可行地利用这种技术,因为该技术基于客户机-服务器模型,在该模型中可推迟密钥使用直到第二链路建立消息。这种推迟在传统的对等模型中是不可能的。尤其是,如果在对等模型中将密钥导出推迟到第二消息,则对于 A 和 B 而言使用 KCK 来互相认证变得不可行。

[0022] 图 3 是可如本文所述进行通信的两个网格点的一种实施例的框图。网格点 300 和网格点 350 可配置为更大的网格网络 (在图 3 中未示出) 的部分,并可利用本领域已知的任意无线协议、例如 IEEE802.11 标准进行通信。

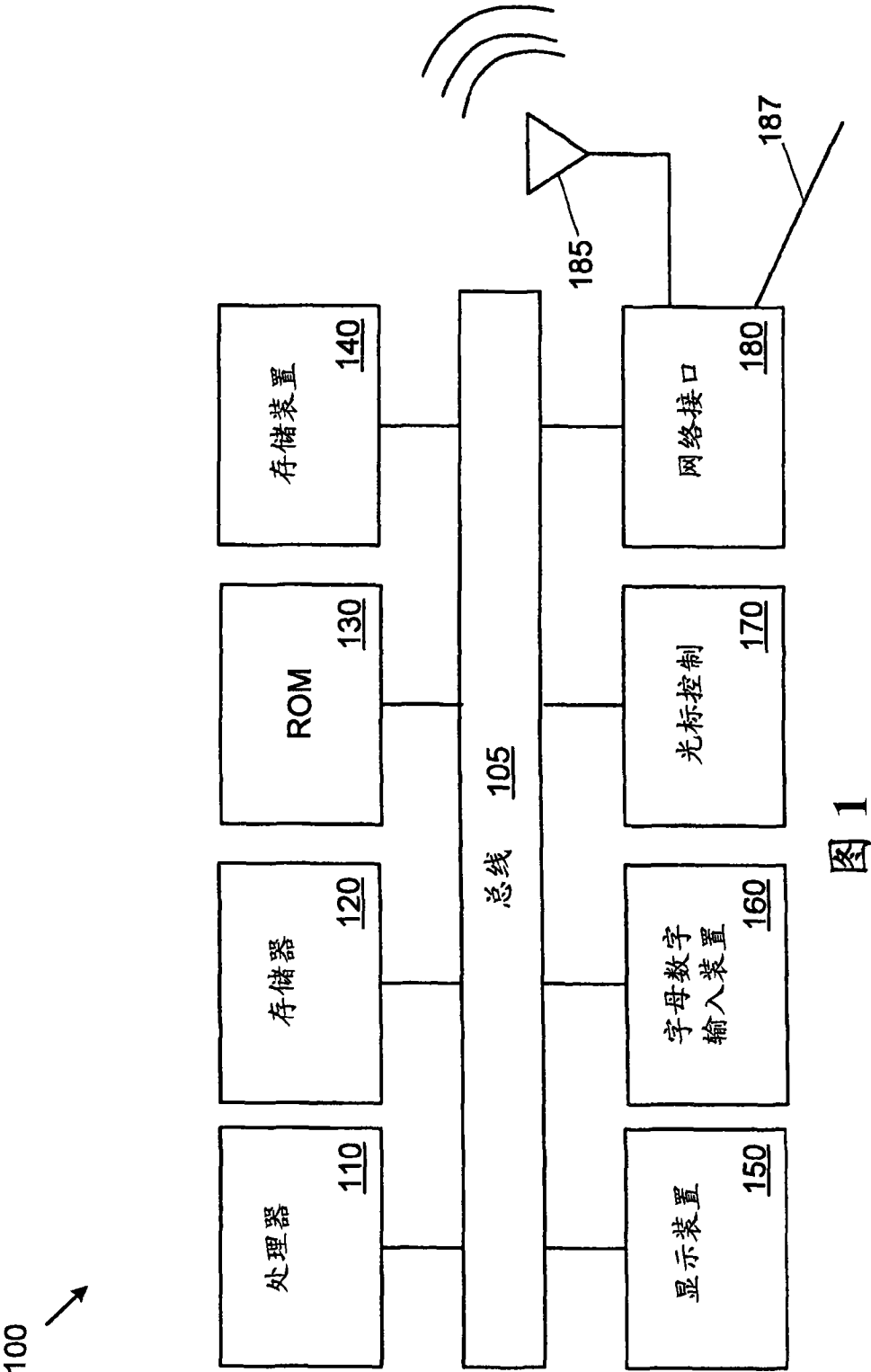
[0023] 各网格点可包括可被用来导出如上所述的加密密钥的密钥导出代理 (310 和 380)。可将密钥导出代理实现为硬件、软件、固件或其任意组合。各网格点还可包括可用来

存储要被如本文所述那样使用的密钥信息的高速缓冲存储器 (330 和 370)。高速缓存存储器可以通信方式与对应密钥导出代理耦合。各网格点还可包括可用于网格网络内的安全通信的可认证身份 (authenticated identity) (320 和 360)。各网格点还可包括其它组件和 / 或单元, 例如处理器、存储装置、输入 / 输出装置等 (图 3 中未示出)。

[0024] 因此本文所述的技术能够将链路认证的构建和密钥加密密钥从会话加密密钥中分离。在 IEEE 802.11i 中, 所有这些密钥被一起导出。这种分离使安全性能被覆盖到网格链路建立协议之上。这种覆盖对使用 IEEE 802.11i 方法来做密钥导出不是可行的, 因为在对等模型中相互认证对使用 IEEE802.11i 方法是不可行的, 除非通过将链路建立消息的数量增加到超过四个。

[0025] 在说明书中对“一种实施例”或“实施例”的引用表示结合该实施例所述的特定特征、结构或特性被包含在本发明的至少一种实施例中。短语“在一种实施例中”在本说明书中各个位置的出现不一定都指同一实施例。

[0026] 既然已经根据若干实施例描述了本发明, 那么本领域技术人员将理解本发明不限于所述实施例, 而是可在随附权利要求书的精神和范围内进行改进和变更。本说明书因此要被视为示例性的而不是限制性的。



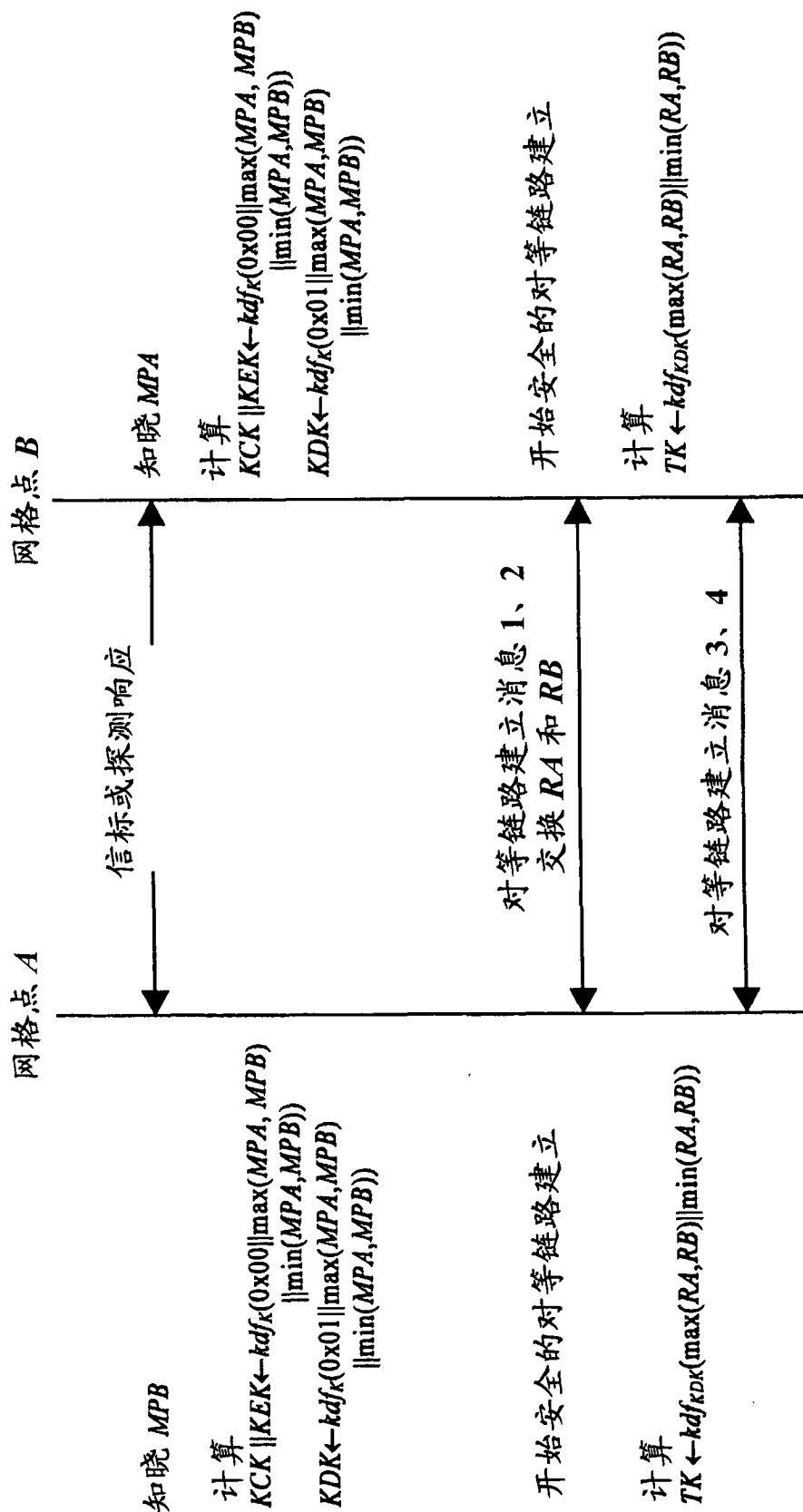


图 2

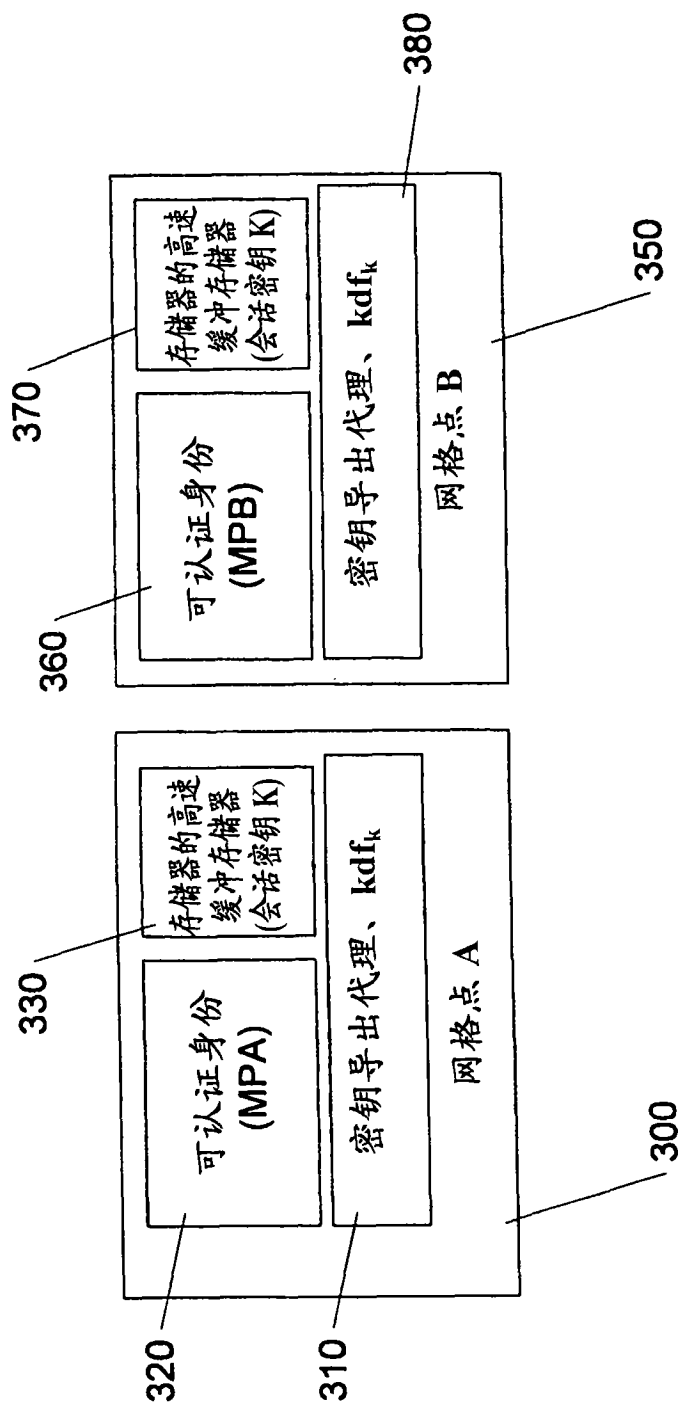


图 3