[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)

[12] 发明专利说明书

专利号 ZL 200510068429.5

[45] 授权公告日 2010 年 1 月 27 日

[11] 授权公告号 CN 100586060C

[22] 申请日 2005.4.29
[21] 申请号 200510068429.5
[30] 优先权
[32] 2004. 9. 9 [33] US [31] 10/937,051
[73] 专利权人 国际商业机器公司
地址 美国纽约
[72] 发明人 阿布西什克·辛格
[56] 参考文献
CN1472914A 2004.2.4
US2004/0034776A1 2004.2.19
CN1298499A 2001.6.6
US6584566B1 2003.6.24
密码编码学与网络安全——原理与实践. William Stallings, 第 154. 158 页, 第 290. 291 页, 电子工业出版社. 2004
审查员 张臻贤
[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
代理人 李 颖

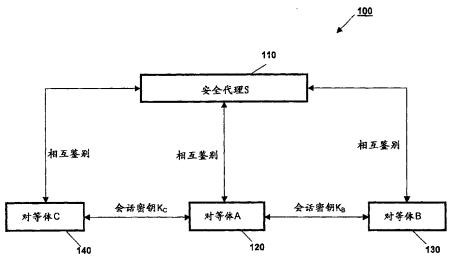
权利要求书 3 页 说明书 8 页 附图 4 页

[54] 发明名称

建立安全对等通信的方法和装置

[57] 摘要

一种用于安全的对等通信的协议，它的建立是基于现有的密码技术和加密算法。对等体(120、130、140)和中央安全代理(110)要经历相互鉴别的过程。新产生的临时值用于鉴别，且随机的会话密钥用于会话。安全代理(110)为对等体(120、130、140)之间的通信产生独特的会话密钥。由于安全代理(110)独立地鉴别请求对等体(120)和被请求对等体(130、140)，所以安全代理(110)消除了被请求对等体(130、140)和请求对等体(120)之间的相互鉴别的负担。安全代理(110)把会话密钥发送给被请求对等体(130、140)和请求对等体(120)。



1. 一种用于建立安全对等通信的方法，包括以下步骤：

通过判定在请求对等体发送给安全代理的请求中是否包括安全代理先前发送给请求对等体的消息编号，来使用安全代理鉴别请求对等体；

通过判定在该请求对等体请求与之通信的被请求对等体发送给安全代理的消息中是否包括安全代理先前发送给该被请求对等体的消息编号，来使用安全代理鉴别该被请求对等体；

把加密的会话密钥从安全代理分发到请求对等体和被请求对等体；以及

使用会话密钥加密请求对等体和被请求对等体之间的通信。

2. 如权利要求 1 中所述的方法，还包括在请求对等体产生消息编号的步骤。

3. 如权利要求 1 中所述的方法，还包括在被请求对等体产生消息编号的步骤。

4. 如权利要求 1 中所述的方法，还包括在安全代理处为请求对等体和被请求对等体产生消息编号的步骤。

5. 如权利要求 1 中所述的方法，其中请求对等体请求与多个被请求对等体进行通信，并且加密的会话密钥被分发到所有被请求对等体。

6. 如权利要求 1 中所述的方法，其中鉴别步骤包括交换使用公开与私秘密钥对加密的消息编号。

7. 如权利要求 1 中所述的方法，还包括用请求对等体鉴别安全代理的步骤。

8. 如权利要求 1 中所述的方法，还包括用被请求对等体鉴别安全代理的步骤。

9. 如权利要求 1 中所述的方法，其中请求对等体请求与多个被请求对等体进行通信，并且不同的加密会话密钥被分发到相应的被请

求对等体。

10. 一种使得能够实现安全的对等通信的装置，该装置包括:

通过判定在请求对等体发送给安全代理的请求中是否包括安全代理先前发送给请求对等体的消息编号，来使用安全代理鉴别请求对等体的装置;

通过判定在该请求对等体请求与之通信的被请求对等体发送给安全代理的消息中是否包括安全代理先前发送给该被请求对等体的消息编号，来使用安全代理鉴别该被请求对等体的装置;

把秘密的会话密钥从安全代理分发到请求对等体和被请求对等体的装置; 以及

使用秘密的会话密钥加密请求对等体和被请求对等体之间的通信的装置。

11. 如权利要求 10 中所述的装置，还包括在请求对等体产生消息编号的装置。

12. 如权利要求 10 中所述的装置，还包括在被请求对等体产生消息编号的装置。

13. 如权利要求 10 中所述的装置，还包括在安全代理处为请求对等体和被请求对等体产生消息编号的装置。

14. 如权利要求 10 中所述的装置，其中请求对等体请求与多个被请求对等体进行通信，并且加密的会话密钥被分发到所有被请求对等体。

15. 如权利要求 10 中所述的装置，其中使用安全代理鉴别请求对等体的装置和使用安全代理鉴别被请求对等体的装置分别与请求对等体和被请求对等体交换使用公开与私秘密钥对加密的消息编号。

16. 如权利要求 10 中所述的装置，还包括用请求对等体鉴别安全代理的装置。

17. 如权利要求 10 中所述的装置，还包括用被请求对等体鉴别安全代理的装置。

18. 如权利要求 10 中所述的装置，其中请求对等体请求与多个

被请求对等体进行通信，并且不同的加密会话密钥被分发到相应的被请求对等体。

建立安全对等通信的方法和装置

技术领域

本发明涉及对等通信。具体地说，本发明涉及建立安全对等通信的方法和装置。

背景技术

对等系统——即分散、分布式结构的特征属性是它具有最弱的链路。除了与先前已知的和信任的伙伴之间使用外，安全问题仍然是采用对等系统的主要障碍，因为许多对等应用要求对等体（peer）之间的安全通信。

对等体之间安全通信的关键问题是对等体的鉴别。另一个问题是通过使用“新鲜的”（fresh）保密会话密钥来建立安全的会话。“新鲜”这一概念对避免重放攻击来说是很重要的。重放攻击包括通信的拦截以及随后通过重新传送拦截到的通信来冒充发送人。通过使用“新鲜的”或新的会话密钥，可以避免通过重新发送进行的冒充。

安全的对等通信可使用一些技术来实现，如被设计用于服务器和客户端之间的通信的安全套接字层（SSL）技术。安全套接字层技术可应用于对等通信，但并不是打算用于或特别适合对等体间的安全通信。

因此，这就无疑地要求一种改进的实现安全的对等通信的方法。

发明内容

基于现有的密码技术（即对称与非对称密钥的使用）和加密算法（如 Rivest-Shamir-Adleman 或 RSA 算法）建立一种用于安全的对等通信的协议。这里描述的协议为对等通信提供鉴别与会话安全，但不是基于通常的客户端－服务器范例，而是被设计为通过减轻对等体在

管理安全性方面的大量负担来用于对等通信。

这些对等体和用作安全代理的中央服务器要经历相互鉴别的过程。新产生的消息编号用于鉴别，且随机的会话密钥用于会话。（这种消息编号在这里可称为“临时值”（nonce））。这些对等体可安全地进行通信，即使它们是第一次通信且彼此没有对方的信息。

由于在相互鉴别之后所有的对等体都在安全代理处注册，所有的对等体都知道该安全代理。安全代理执行为通信对等体产生独特的会话密钥的任务。由于服务器独立地鉴别请求对等体和被请求对等体，所以安全代理消除了请求对等体和被请求（响应）对等体之间的相互鉴别的负担。该安全代理把会话密钥发送给请求对等体和被请求对等体。

该方法解除了对等体产生会话密钥和管理对等体的大量公开密钥的负担。该负担转移到了中央安全代理，该代理更可能具有自由地处理执行这些任务的足够的资源(如中央处理能力、以及随机存储器)。

该方法的另一个好处是不要求对等体从认证中心（Certificate Authority）获取数字认证。相反，每个对等体都具有中央安全代理的公开密钥，且中央安全代理有每个对等体的公开密钥。协议使用公开/私秘密钥来提供相互鉴别，并使用对称密钥提供会话安全，这相对于使用非对称密钥的数据加密来说有更少的网络通信量。

附图说明

图 1 是这里描述的对等通信协议中所包含的实体的示意图。

图 2A 和 2B 共同形成了对等网络中安全通信的建立所包含的步骤的流程图。

图 3 是典型地适用于对等网络的计算机系统的示意图。

具体实施方式

图 1 示意性地表示了根据这里描述的协议的对等网络 100 中所包含的实体。安全代理 S 110 具有与对等体 A 120、对等体 B 130、以及

对等体 C 140 的通信链路。网络 110 可包括更多的对等体，虽然三个对等体已足够阐明所描述的安全协议的操作。

在请求对等体 120 和被请求对等体 130 与 140 之间的初始通信期间，安全代理 S 100 与对等体 120、130、140 相互鉴别。

实体、假设和符号

考虑下面的在描述对等通信装置中使用的实体。

对等体 A 120 想要使用被请求的对等体 B 130 与 C 140 的资源或服务的客户端。

对等体 B 130 与 C 140 请求对等体 A 120 与之进行通信的被请求对等体 B130 与 C 140。

安全代理 S 100 利于请求和被请求对等体之间的安全通信的代理或一组"胖"客户端或服务器。

如下编号的假设也适用。

1、对等体 A 120 使用任何适当的对等体发现技术确定想要与哪个或哪些被请求对等体（该情况下是对等体 B 130 和对等体 C 140）进行通信。

2、所有的对等体向安全代理 S 110 注册，随后获得安全代理 S 110 的公开密钥，反之亦然。

3、所有的对等体和安全代理 110 具有它们各自的公开/私秘密钥对。假定用如 RSA 或类似的鲁棒算法产生公开/私秘密钥对。

这里使用的关于对等体 A 120、B 130 与 C140 以及安全代理 S 110 的符号如下所示。

A、B、C →对等体{A、B、C}

S→安全代理

P_A、P_B、P_C、P_S→脚标的对等体 A、B、C 或安全代理 S 的公开密钥

P_A（）→使用对等体 A 的公开密钥对括号内的数据加密

$n_{(a,b,c,s1,s2,s3)}$ →临时值，即在特定处理时间间隔内可与其它消息编号区分的消息编号。（在一种实施例中该临时值是随机产生的独特的消息编号。）

K_B, K_C →如 K_B 的秘密会话密钥和对称密钥是在对等体 A 和对等体 B 之间使用的对称密钥

通信协议

对等体 A 120 要与对等体 B 130 与 C 140 安全地通信。下面的列表 1 略述了启动对等体 A 120 和对等体 B 130 与 C 140 之间的安全通信所包含的一系列步骤。

表 1

步骤	交互作用	发送的消息
步骤 1	A→S	$P_S(n_a)$
步骤 2	S→A	$P_A(n_a, n_{s1})$
步骤 3	A→S	$P_S(n_{s1}, Peers\{B,C\})$
步骤 4	S→B	$P_B(n_{s2})$
	S→C	$P_C(n_{s3})$
步骤 5	B→S	$P_S(n_{s2}, n_b)$
	C→S	$P_S(n_{s3}, n_c)$
步骤 6	S→B	$P_B(n_b, K_B)$
	S→C	$P_C(n_c, K_C)$
步骤 7	S→A	$P_A(n_a, (\{peer, key\} \rightarrow (\{B, K_B\}, \{C, K_C\}))$
步骤 8	A→B	K_B(数据)
	A→C	K_C(数据)

步骤 1 至 3 包含请求对等体、对等体 A 120 和安全代理 S 110 的相互鉴别。

步骤 4 至 6 包含与被请求对等体 B 130、C 140 以及安全代理 S 110 的相互鉴别有关的事件。步骤 6 还包含对应的保密对称密钥的分发。

步骤 7 包含对等体 A 在和对等体 B 130 与 C 140 通信时使用的保密会话密钥的分发。例如，对等体 120 使用 K_B,K_C 分别与对等体 B 130 和对等体 C 140 进行通信。

步骤 8 包含请求对等体 A 120 启动与被请求对等体 B 130 与 C 140 的安全通信。

图 2A 与 2B 更具体地按流程图解了这些步骤。请求对等体 A 120 产生一个临时值并在步骤 202 把它发送到安全代理 S 110。该临时值使用安全代理 S 110 的公开密钥加密。安全代理 S 110 在步骤 204 使用安全代理 S 110 的私秘密钥解译传送的临时值。在该步骤中，安全代理 S 110 产生自身的临时值，然后使用对等体 A 120 的公开密钥对产生的临时值进行加密（并解译来自对等体 A 120 的临时值）。被加密的临时值返回到对等体 A 120。

在步骤 206，对等体 A 120 判定安全代理 S 110 在步骤 204 中发送的消息是否对先前从对等体 A 120 发送到安全代理 S 110 的临时值进行了加密。通过使用对等体 A 120 的私秘密钥对从安全代理 S 110 接收的消息进行解密来实施该判定。如果对等体 A 120 未接收到自身的临时值作为答复，那么安全代理 S 110 在步骤 208 就被判定为伪造的安全代理。否则，如果对等体 A 120 接收到自身的临时值，那么安全代理 S 110 就被认为是合法的，然后程序进行到步骤 210。

对等体 A 120 在步骤 210 提取安全代理 S 110 发送的临时值，然后创建一个新的请求，该请求指定对等体 A 120 想与之进行通信的对等体 B 130 和 C 140。该请求包括提取的安全代理 S 110 的临时值，对等体 A 120 使用安全代理 S 110 的公开密钥对新请求进行加密，然后把加密后的请求发送到安全代理 S 110。

安全代理 S 110 在步骤 212 接收来自对等体 A 120 的加密后的请求，据此判定安全代理 S 110 是否已经接收到安全代理 S 110 在步骤 204 发送给对等体 A 120 的临时值。如果安全代理 S 110 未从对等体 A 120 接收到自身的临时值作为答复，那么对等体 A 120 在步骤 214 就被判定为伪造的请求对等体。否则，如果安全代理 S 110 从对等体 A

120 接收到自身的临时值作为答复，那么对等体 A 120 就被认为是合法的请求对等体，然后程序进行到步骤 216。

安全代理 S 110 在步骤 216 为对等体 A 120 希望与之通信的每个被请求的对等体（在该情况下，为对等体 B 130、C 140）产生独特的临时值。安全代理 S 110 产生的这些临时值中的每个临时值都被使用相应被请求对等体的公开密钥进行加密，然后传送到由请求对等体 A 120 指定的被请求对等体。对等体 B 130 和 C 140 中的每个被请求对等体在步骤 218 产生它们自身的临时值，并提取安全代理 S 110 在步骤 216 中发送的临时值。这些临时值形成发送到安全代理 S 110 的回复，并被使用安全代理 S 110 的公开密钥进行加密。

在步骤 220 判定安全代理 S 110 是否在步骤 218 中发送到安全代理 S 110 的消息中接收到自身的临时值作为答复。如果安全代理 S 110 未从被请求对等体接收到自身的临时值作为答复，那么该被请求对等体在步骤 222 就被判定为伪造的被请求对等体。如果每个被请求对等体都用安全代理 S 110 在步骤 216 发送的临时值对安全代理 S 110 作出响应，那么每个被请求对等体就被认为是合法的。在这种情况下，安全代理 S 110 与请求对等体、以及与被请求对等体相互鉴别。安全代理 S 110 为每个被请求对等体 B 140 和 C 130 产生会话密钥。然后程序中的步骤 224 和 232 并行进行。

在步骤 232，安全代理 S 110 把包含对等体的临时值和会话密钥（K_B 或 K_C）的消息发送到每个被请求对等体，其中的临时值和会话密钥使用被请求对等体的公开密钥进行加密。被请求对等体使用该会话密钥与请求对等体 A 120 进行通信。

安全代理 S 110 在步骤 224 还把产生的会话密钥（K_B 或 K_C）发送到请求对等体 A 120。安全代理 S 110 发送会话密钥以及由请求对等体 A 120 的公开密钥加密的请求对等体的临时值。

在步骤 226 判定对等体 A 120 是否从安全代理 S 110 接收到自身的临时值。如果对等体 A 120 未接收到自身的临时值，那么安全代理 S 110 在步骤 228 被认为是伪造的安全代理。否则，安全代理 S 110 被

认为是合法的，然后程序进行到步骤230。在步骤230，对等体A 120用分别用于对等体A 120和对等体B 140以及对等体A 120和对等体C 130之间的通信的会话密钥加密它的请求（如文件下载，或任务执行），然后对等体A 120把请求发送到对应的被请求对等体。在步骤238中，在请求对等体A 120和被请求对等体B 140以及对等体A 120和被请求对等体C 130之间建立安全的通信。

在步骤234判定被请求对等体130、140是否从安全代理S 110接收到自身的临时值作为回复。如果被请求对等体未接收到自身的临时值，那么安全代理S 110在步骤228就被判定为伪造的安全代理。否则，安全代理S 110就被认为是合法的，在步骤238中，在由步骤230启动的对等体之间建立安全通信。

计算机硬件

图3是典型地适于用作图1的对等网络中的对等体120、130或140或安全代理S 110的计算机系统300的示意图。计算机软件在安装在计算机系统300上的合适的操作系统下运行，且可认为包含用于实现特定步骤的多种软件代码装置。安全代理S 110可被实现以迎合单个服务器或一组服务器中的预期负荷。一组"胖"客户端也能够用于迎合预期负荷。

计算机系统300的组件包括计算机320、键盘310和鼠标315、以及视频显示器390。计算机320包括处理器340、存储器350、输入/输出（I/O）接口360、365、视频接口345、以及存储设备355。

处理器340是执行操作系统和在操作系统下运行的计算机软件的中央处理单元（CPU）。存储器350包括随机存储器（RAM）和只读存储器（ROM），且在处理器340的指令下使用。

视频接口345连接到视频显示器390并为视频显示器390上的显示提供视频信号。操作计算机320的用户输入从键盘310和鼠标315提供。存储设备355可包括盘驱动器或任何其它合适的存储介质。

计算机320的每个组件都连接到包括数据、地址、以及控制总线

的内部总线 330，以允许计算机 320 的组件通过总线 330 彼此进行通信。

计算机系统 300 可使用通向表示为因特网 380 的网络的通信信道 385 经由输入/输出（I/O）接口 365 连接到一个或多个其它的类似的计算机。

计算机软件可以记录在便携式存储介质上，在这种情况下，计算机系统 300 从存储设备 355 访问计算机软件程序。可供选择地，可由计算机 320 从因特网 380 直接访问该计算机软件。在任何情况下，用户都能使用键盘 310 和鼠标 315 与计算机系统 300 相互作用，以操作运行在计算机 320 上的程序化的计算机软件。

其它配置或类型的计算机系统可同样地适用于执行辅助实现这里所描述的技术的计算机软件。对相关技术领域的技术人员来说显而易见的是，可以对这里所描述的技术和装置进行多种变化和修改。

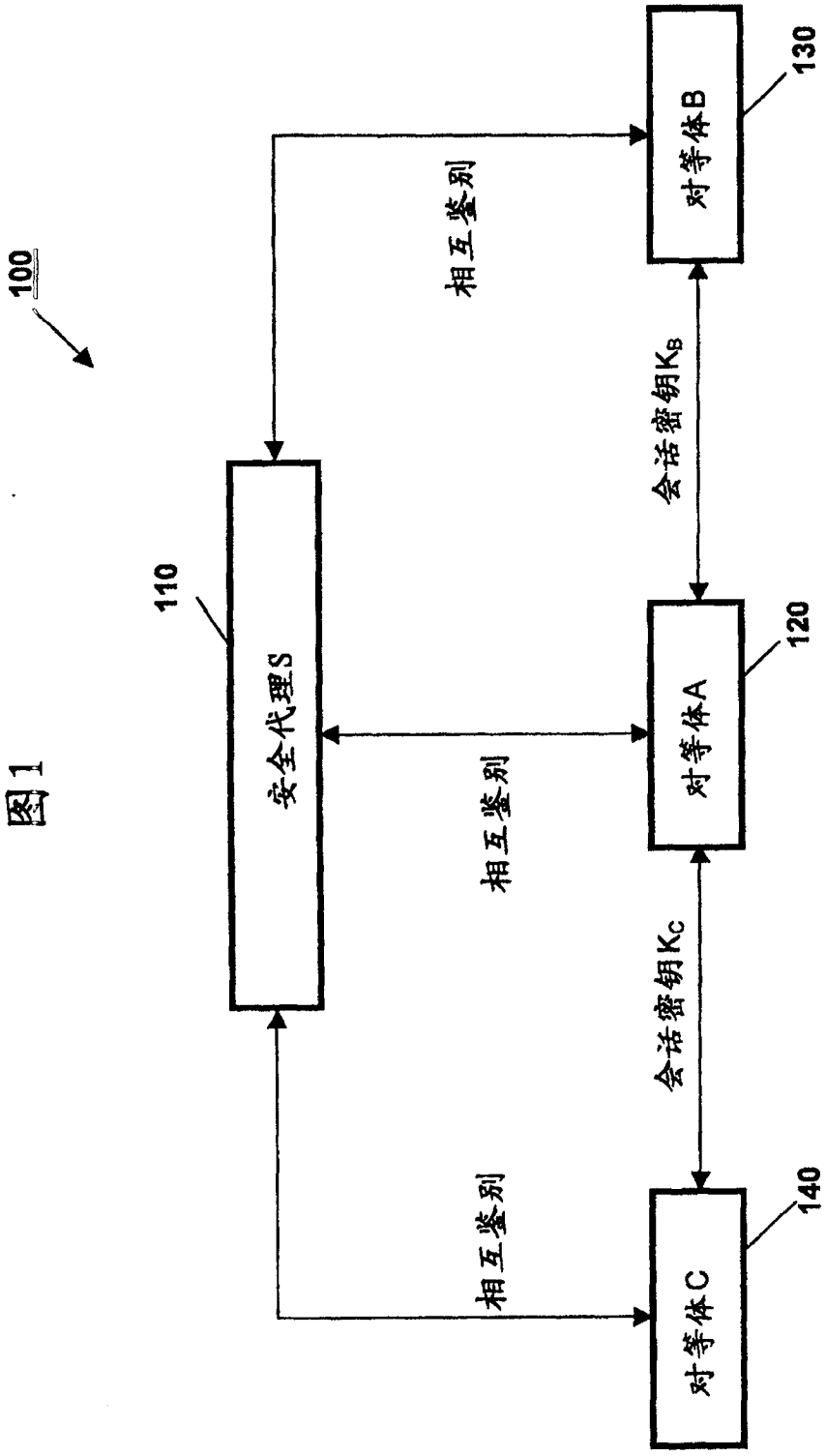
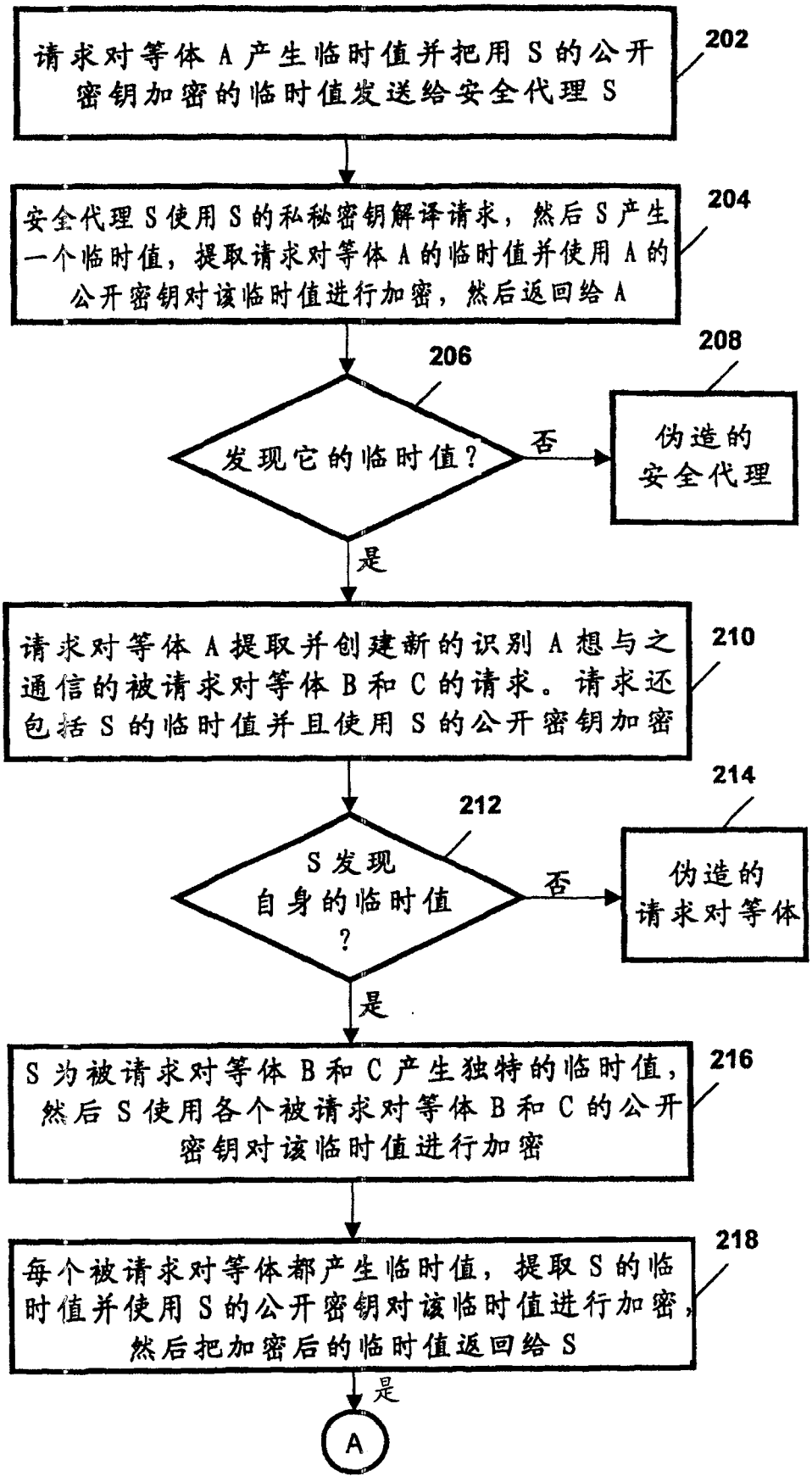

100
安全代理S
110
对等体A
120
对等体B
130
对等体C
140
相互鉴别
相互鉴别
相互鉴别
会话密钥K_B
会话密钥K_C

图1

图2A


请求对等体A产生临时值并把用S的公开密钥加密的临时值发送给安全代理S
202
安全代理S使用S的私秘密钥解译请求，然后S产生一个临时值，提取请求对等体A的临时值并使用A的公开密钥对该临时值进行加密，然后返回给A
204
206
发现它的临时值？
否
208
伪造的安全代理
是
请求对等体A提取并创建新的识别A想与之通信的被请求对等体B和C的请求。请求还包括S的临时值并且使用S的公开密钥加密
210
212
S发现自身的临时值？
否
214
伪造的请求对等体
是
S为被请求对等体B和C产生独特的临时值，然后S使用各个被请求对等体B和C的公开密钥对该临时值进行加密
216
每个被请求对等体都产生临时值，提取S的临时值并使用S的公开密钥对该临时值进行加密，然后把加密后的临时值返回给S
218
是
A

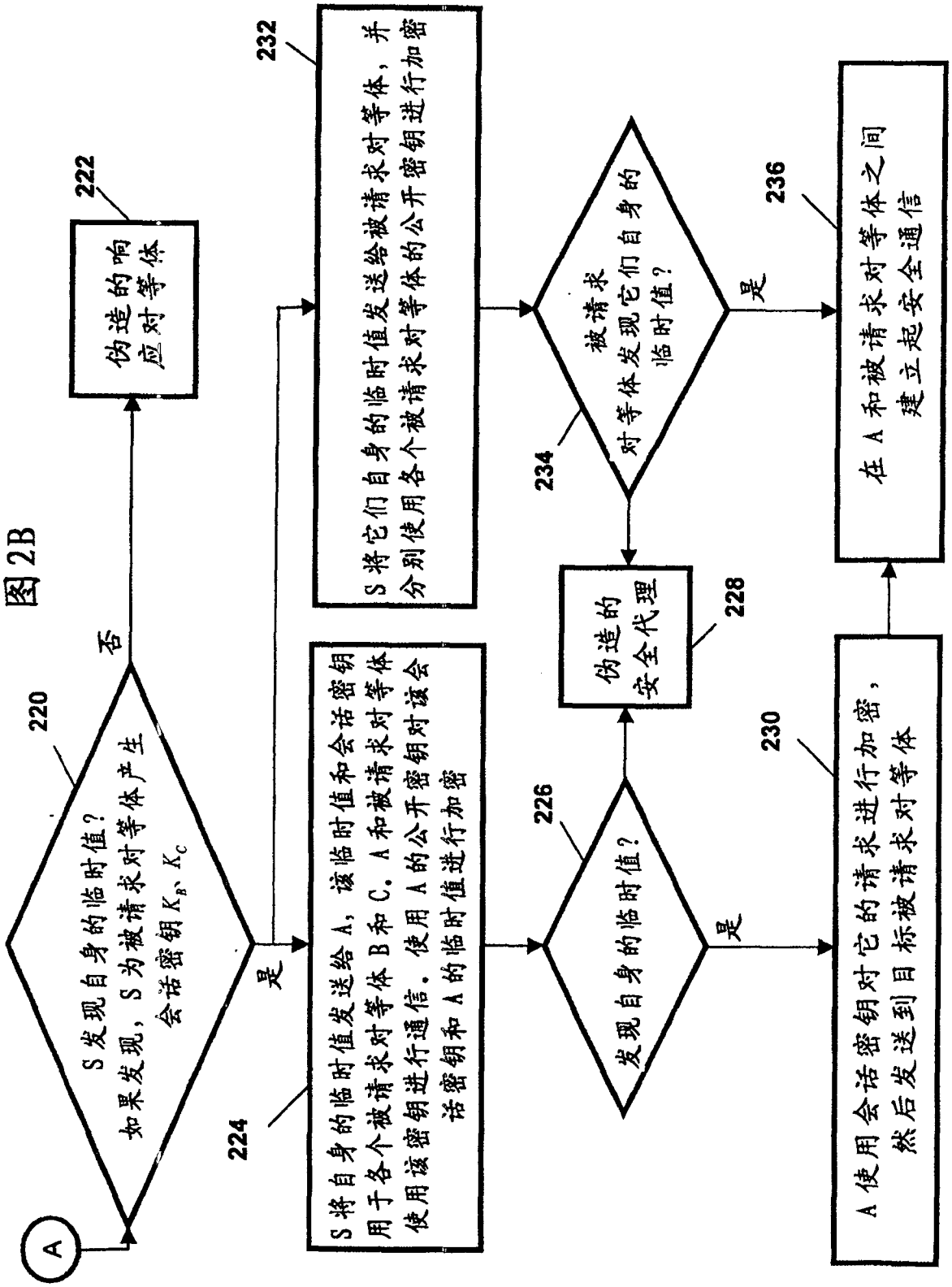
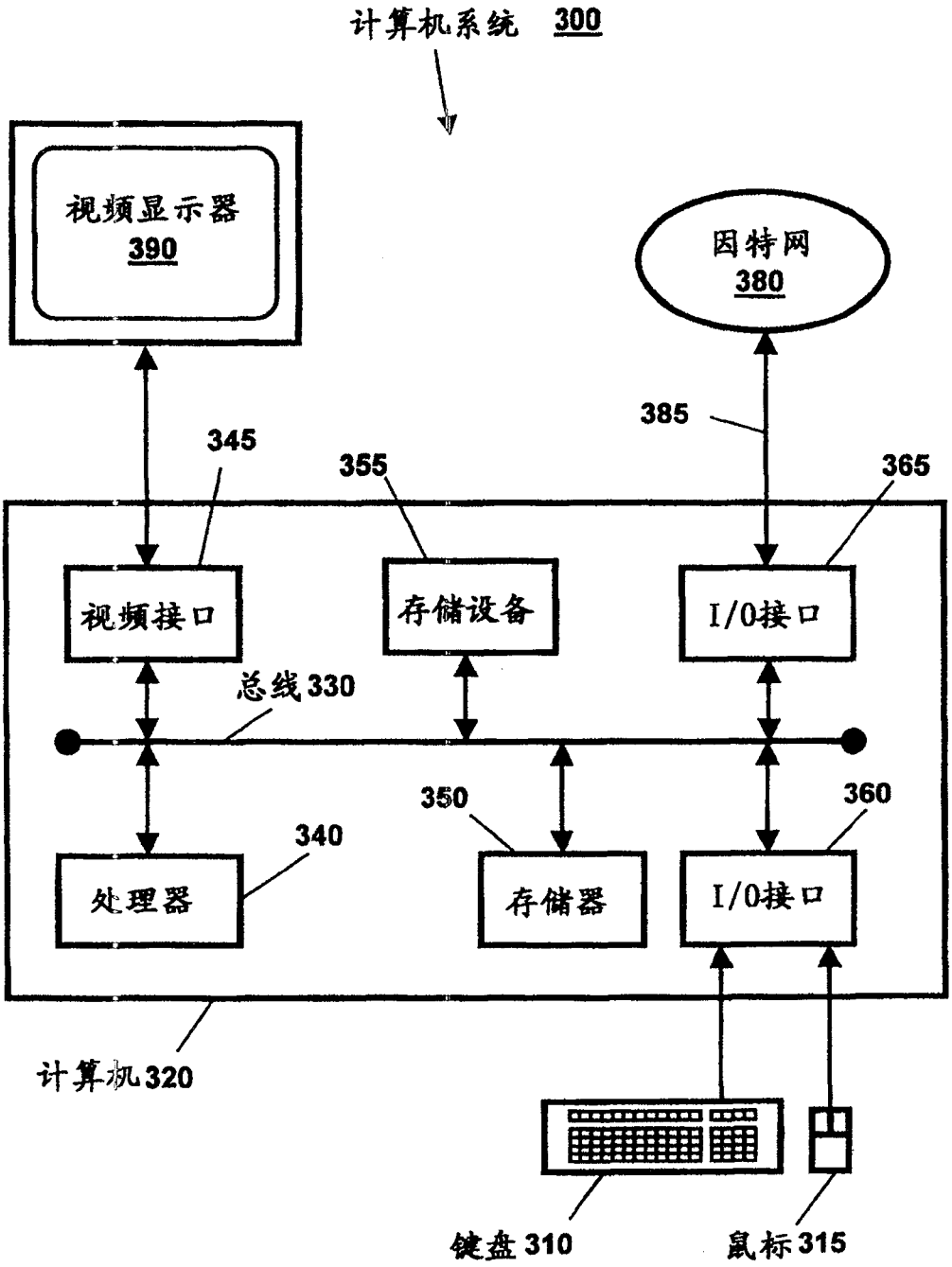

A
S发现自身的临时值？
如果发现，S为被请求对等体产生会话密钥 K_B、K_C
220
否
伪造的响应对等体
222
是
S将自身的临时值发送给A，该临时值和会话密钥用于各个被请求对等体B和C。A和被请求对等体使用该密钥进行通信。使用A的公开密钥对该会话密钥和A的临时值进行加密
224
S将它们自身的临时值发送给被请求对等体，并分别使用各个被请求对等体的公开密钥进行加密
232
发现自身的临时值？
226
是
伪造的安全代理
228
被请求对等体发现它们自身的临时值？
234
是
236
A使用会话密钥对它的请求进行加密，然后发送到目标被请求对等体
230
在A和被请求对等体之间建立起安全通信

图2B

图3


计算机系统 300
视频显示器 390
因特网 380
385
345
355
365
视频接口
存储设备
I/O接口
总线 330
350
360
340
处理器
存储器
I/O接口
计算机 320
键盘 310
鼠标 315