(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1685687 B
(45)授权公告日 2013.10.30

(21)申请号 03823268.5

(22)申请日 2003.09.22

(30)优先权数据
60/414,942 2002.09.30 US
60/445,265 2003.02.05 US

(85)PCT申请进入国家阶段日
2005.03.29

(86)PCT申请的申请数据
PCT/IB2003/004110 2003.09.22

(87)PCT申请的公布数据
WO2004/030311 EN 2004.04.08

(73)专利权人 皇家飞利浦电子股份有限公司
地址 荷兰艾恩德霍芬

(72)发明人 M·罗斯纳 R·克拉辛斯基
M·A·埃普斯泰因

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 刘红 王勇

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
WO 0193434 A2,2001.12.06, 全文.
WO 0235036 A1,2002.05.02, 说明书第3页第20-25行,第7页第1-30行,第8页第12-22行,第9页第1-19行、图1,图3.
WO 0069111 A2,2000.11.16, 全文.

审查员 范文婧

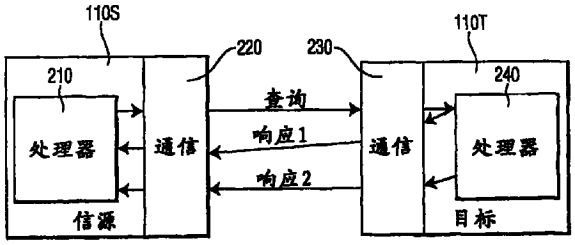
权利要求书1页 说明书3页 附图1页

(54)发明名称

确定目标节点对于源节点的邻近性的方法

(57)摘要

一种系统和方法根据在节点验证协议中传送消息所需要的时间来确定目标节点对源节点的邻近性。该节点验证协议包括查询响应序列,其中源节点将查询传送给目标节点,并且目标节点将相应的响应传送给源节点。目标节点被配置为传送两个对该查询的响应:一旦接收到该查询时立即发送的第一响应,和基于该查询的内容的第二响应。根据在源节点上该查询的传送和第一响应的接收之间的持续时间来确定通信时间,并比较第二响应与该查询的对应性,以验证目标节点的可靠性。



CN 1685687 B

1. 一种确定目标节点对于源节点的邻近性的方法，包括：

在目标节点与源节点使用相应的数字证书来验证彼此的公用密钥的鉴别阶段之后，立即在目标节点上准备第一响应，其中第一响应包括使用源节点的公用密钥加密的并使用目标节点的专用密钥签名的随机数，其中在鉴别阶段之后立即执行随机数的加密和签名，以便这个加密的和签名的响应在从源节点接收到查询之后立即可用于从目标节点发送给源节点；

将查询从源节点传送给目标节点；

在目标节点上接收到该查询之后且在解密该查询之前，立即将第一响应从目标节点传送给源节点；

在源节点上接收第一响应；

在目标节点上处理该查询，以便据此生成有助于目标节点及其第一响应的验证的第二响应；

将第二响应从目标节点传送给源节点；

确定在传送该查询和接收到第一响应之间的通信时间的测量；和

根据通信时间的测量，确定目标节点的邻近性。

2. 权利要求 1 的方法，其中：

该查询以及至少第一响应和第二响应之一对应于密码的密钥交换协议的至少一部分。

3. 权利要求 2 的方法，其中：

该密钥交换协议对应于 Needham-Schroeder 密钥交换协议。

4. 权利要求 1 的方法，其中：

该查询以及至少第一响应和第二响应之一对应于 OCPS 协议的至少一部分。

5. 权利要求 1 的方法，其中：

该查询包括基于目标节点的公用密钥对项的加密；和

该查询的处理包括根据目标节点的专用密钥来解密该项，以便包括在第二响应中。

6. 权利要求 5 的方法，其中：

该查询的处理还包括使用源节点的公用密钥来加密该项和随机数，以形成第二响应的至少一部分。

7. 权利要求 1 的方法，其中：

确定邻近性包括将通信时间与区分本地节点和远程节点的阈值进行比较。

8. 权利要求 1 的方法，还包括：

根据邻近性，限制与目标节点的通信。

9. 权利要求 1 的方法，还包括：

根据邻近性，限制目标节点对系统资源的访问。

确定目标节点对于源节点的邻近性的方法

技术领域

[0001] 本发明涉及通信安全领域，并且尤其涉及验证网络上节点的邻近性的系统和方法。

背景技术

[0002] 网络安全通常可以通过区分网络上的“本地”节点和“远程”节点来提高。通过类似的方式，可以根据节点是本地的还是远程的，对于分配资料给节点施加不同的权力或限制。本地节点例如通常位于特定的物理环境内，并且可以假定在该物理环境内的用户被授权访问该网络和／或被授权接收来自其它本地节点的文件。另一方面，远程节点易受未授权物理访问的影响。另外，网络上未授权的入侵者通常通过电话或其它通信信道来远程地访问网络。因为网络对通过远程节点的未授权访问的敏感性，通过在远程节点上采取严格的安全措施和／或访问限制，可以提高网络安全性和／或复制保护，同时不使用这些相同的限制来阻碍本地节点。

发明内容

[0003] 本发明的一个目的是提供一种有助于确定网络上的节点是本地的还是远程的系统和方法。本发明的另一个目的是使这一确定与验证网络上节点的可靠性的系统或方法相结合。

[0004] 通过一种有助于确定在诸如开放复制保护系统 (OCPS) 的节点验证协议内的源节点和目标节点之间通信时间的系统和方法来实现这些目的和其它目的。根据与询问响应协议相关的通信延时来确定目标节点对源节点的邻近性。节点验证协议包括查询响应序列，其中源节点向目标节点传送查询，而目标节点向源节点传送相应响应。为了区分实际通信时间和生成与该查询对应的响应所需要的时间，将目标节点配置为传送两个对该查询的响应：一旦接收到该查询立即发送的第一响应和基于该查询的内容的第二响应。根据在源节点上该查询的发送和第一响应的接收之间的持续时间来确定通信时间。比较第二响应与该查询的对应性，以验证目标节点的可靠性，并且比较通信时间与阈值，以确定目标节点相对于源节点是本地的还是远程的。

附图说明

[0005] 图 1 图示节点网络的示例方框图；

[0006] 图 2 图示根据本发明执行查询响应协议的源节点和目标节点的示例方框图。

[0007] 在所有的附图中，相同的标号是指相同的单元或者执行基本上相同功能的单元。

具体实施方式

[0008] 图 1 图示节点 110 的网络 150 的示例方框图。将节点之一即节点 D110 图示为远离其它节点 110。根据本发明，每个节点 110 被配置为能够确定每个其它节点 110 的邻近性。

在本发明的典型实施例中，邻近性确定限制于确定另一节点是“本地的”还是“远程的”，尽管使用在此公开的技术可以实现更加具体的距离确定。

[0009] 图 2 图示根据本发明的执行查询响应协议以确定目标节点 110T 对源节点 110S 的邻近性的源节点 110S 和目标节点 110T 的示例方框图。源节点 110S 包括启动查询的处理器 210 和将查询发送给目标节点 110T 的通信设备 220。目标节点 110T 通过其通信设备 230 接收查询并返回相应响应。为了保证第一响应对应于所传送的查询，该协议要求目标节点 110T 通过处理器 240 处理该查询的至少一部分，并在第二响应中包括该处理的结果。

[0010] 源节点 110S 被配置为测量查询响应处理所消耗的时间，并根据该测量结果来确定目标节点 110T 的邻近性。在常规的查询响应协议中，查询响应时间包括传送查询与响应的时间以及在目标节点 110T 上处理该查询并生成响应的时间，并因而常规查询响应协议中的查询响应时间通常并不适合于确定通信时间。

[0011] 根据本发明，将目标节点 110T 配置为提供对该查询的两个响应。目标节点 110T 接收到查询之后提供立即响应，并且随后在处理过查询之后提供后续响应。源节点 110S 被配置为测量发送查询和接收到来自目标节点 110T 的第一响应之间的持续时间，以确定目标节点 110T 到源节点 110S 的相对邻近性。源节点还被配置为根据来自目标节点 110T 的第二响应验证目标节点 110T 的可靠性。在优选实施例中，通过第一响应或第二响应的内容，可以将第一响应的可靠性验证为始发自目标节点 110T。

[0012] 使用公知的技术，可以利用所确定的从源节点 110S 发送查询和从目标节点 110T 接收第一响应之间的通信时间来计算源 110S 和目标 110T 之间的距离。如上面指出的，在典型的实施例中，使用通信时间来确定目标 110T 是本地的还是远离源 110S。在本发明的优选实施例中通过比较通信时间与标称阈值来进行这一确定，通常不超过若干毫秒。如果通信时间低于阈值，则将目标 110T 确定为本地的，反之，将其确定为远程的。也可以使用多个阈值来提供目标 110T 距离源 110S 的远程度的相对测量。

[0013] 在典型的实施例中，源 110S 使用远程 / 本地邻近性确定来控制随后与目标 110T 的通信，和 / 或根据邻近性来控制目标节点对诸如数据和处理的系统资源的访问。例如，一些文件可以被允许仅传送给本地节点，可以要求加密与远程节点的所有通信，可以禁止一些文件的洲际传输，等等。

[0014] 在本发明的优选实施例中，上面的查询响应处理被合并在例如密钥交换处理的节点鉴别处理内，其通常包括一个或多个查询响应序列。

[0015] OCPS 协议例如包括鉴别阶段、密钥交换阶段、密钥生成阶段和随后的数据传输阶段。通过如在 Menezes 等人的“应用加密手册 (Handbook of Applied Cryptography)”中描述的改进的 Needham-Schroeder 密钥交换协议来执行密钥交换阶段。

[0016] 在鉴别阶段，源节点 110S 和目标节点 110T 中的每个节点使用相应的数字证书来验证彼此的公用密钥。

[0017] 在密钥交换阶段开始时，源 110S 生成包括随机数和随机密钥的消息。源 110S 随后使用目标 110T 的公用密钥来加密该消息，并将加密后的消息作为上述查询发送给目标 110T。根据本发明，源节点 110S 在将这些加密内容发送给目标 110T 时启动定时器。

[0018] 在常规的 OCPS 协议中，目标 110T 使用目标 110T 的专用密钥来解密来自源 110S 的随机数和随机密钥。目标 110T 生成包括新的随机数、新的随机密钥和解密的来自源 110S 的

随机数的消息，并使用源 110S 的公用密钥加密该消息，以形成将要传送给源 110S 的响应。目标 110T 也使用目标的专用密钥来签名该响应。

[0019] 根据本发明，一旦接收到查询，在上述随机数和随机密钥的解密 之前，目标 110T 将第一响应发送给源 110S。在本发明的一种优选实施例中，目标 110T 将新的随机数作为第一响应发送给源 110S，并随后通过作为第二响应发送的常规 OCPS 响应的附录来验证这个新的随机数。在另一种优选实施例中，目标 110T 将常规 OCPS 响应的一部分包括在第一响应内，该第一响应包括加密的和签名的新随机数，随后是常规 OCPS 响应的其余部分。

[0020] 在第一优选实施例中，第二响应包括使用源 110S 的公用密钥加密的和使用目标 110T 的专用密钥签名的资料 (material) 内的第一响应的随机数。

[0021] 在第二优选实施例中，第一响应包括使用源 110S 的公用密钥加密的和使用目标 110T 的专用密钥签名的新随机数。在鉴别阶段之后立即执行新随机数的加密和签名，以便这个加密的和签名的响应在从源 110S 接收到查询之后立即可用于从目标 110T 发送给源 110S。在发送第一响应之后，目标 110T 使用目标 110T 的专用密钥解密来自源 110S 的查询，并生成包括新随机密钥和解密的随机密钥的新消息。随后，目标使用源 110S 的公用密钥加密该新消息，使用其专用密钥签名该消息，并将该查询内包含的加密的和签名的响应发回给源 110S，从而对于源 110S 验证目标 110T 的身份。

[0022] 当源节点 110S 接收第一响应时，它结束上述定时器，从而建立在源 110S 和目标 110T 之间往返通信时间的测量。一旦接收到第二响应，源节点 110S 使用目标 110T 的公用密钥验证签名的消息，并使用源 110S 的专用密钥来解密来自该响应的随机数和随机密钥。

[0023] 为了确认密钥交换，源 110S 将解密的新随机数发回给目标 110T。源 110S 和目标 110T 二者根据合适解密的随机数的接收来控制后续通信。根据本发明，源 110S 也根据确定的通信时间来控制后续通信。

[0024] 如果验证两个节点，则源 110S 和目标 110T 之间的后续通信使用作为随机密钥、公用密钥和对话索引的组合的对话密钥来加密通信。

[0025] 上文仅仅描述本发明的原理。因而，对于本领域的技术人员来说，显然将能够设计出各种安排，这些安排尽管在此未明确描述或图示，但是实施了本发明的原理，并因而落在随后的权利要求书的精神和范畴之内。

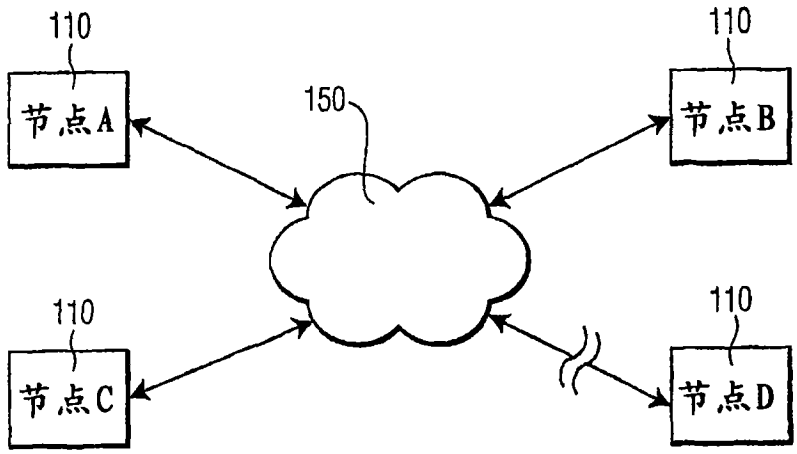

110
节点A
110
节点B
150
110
节点C
110
节点D

图 1

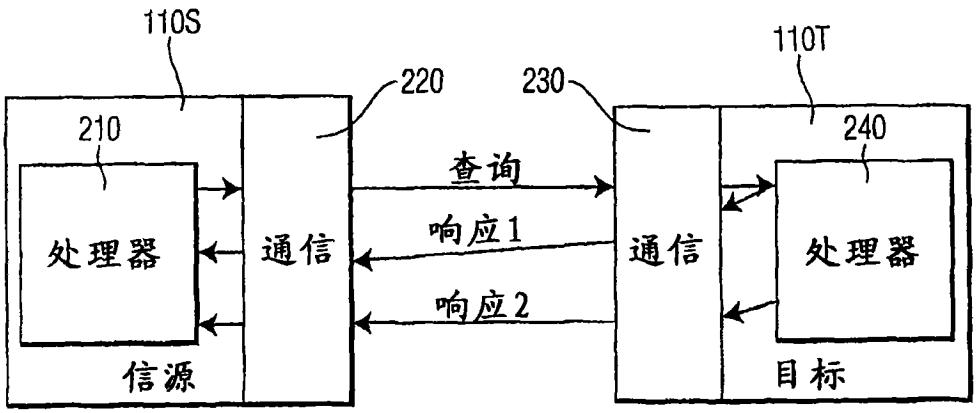

110S
220
230
110T
210
240
查询
响应1
响应2
处理器
通信
通信
处理器
信源
目标

图 2