

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 29/06 (2006.01)



[12] 发明专利说明书

专利号 ZL 03823282.0

[45] 授权公告日 2010 年 1 月 6 日

[11] 授权公告号 CN 100579111C

[22] 申请日 2003.9.22 [21] 申请号 03823282.0

[30] 优先权

[32] 2002.9.30 [33] US [31] 60/414,944

[32] 2003.2.5 [33] US [31] 60/445,263

[86] 国际申请 PCT/IB2003/004123 2003.9.22

[87] 国际公布 WO2004/030312 英 2004.4.8

[85] 进入国家阶段日期 2005.3.29

[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·A·埃普斯泰因

F·格鲁米奥克斯

[56] 参考文献

US6367018B1 2002.4.2

CN1239618A 1999.12.22

CN1304604A 2001.7.18

An architecture for a global Internet hostdistance estimation service. FRANCIS P ET AL. INFO-COM 99. EIGHTEENTH ANNUAL JOINT CONFERENCE OF THE IEEE COMPUTER AND COMMUNICATIONS SOCIETIES. PROCEEDINGS. IEEE, Vol. 1. 1999

TCP/IP ILLUSTRATED. W. Richard Stevens, 85.96, ADDISON WESLEY. 1994

审查员 殷跃

[74] 专利代理机构 中国专利代理(香港)有限公司

代理人 李亚非 王忠忠

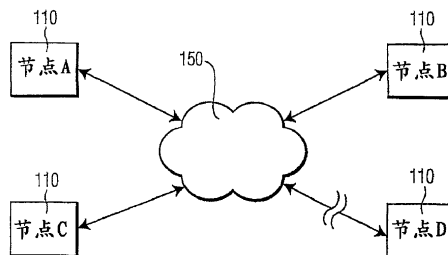
权利要求书 2 页 说明书 5 页 附图 1 页

[54] 发明名称

确定目标节点到源节点的邻近程度的方法以及网络节点

[57] 摘要

一种系统和方法将定时参数包含在诸如 OCPS 之类的节点验证协议内,以便简化目标节点与源节点的邻近程度的判定。该节点验证协议包括一个在源节点与目标节点之间的查询-响应序列。源节点基于实施这个查询-响应序列所需要的时间量度来建立源节点与目标节点之间的距离下限,其中实施所述序列所需要的时间包含了传送查询和响应所需要的时间,以及处理查询和产生响应所需要的时间。目标节点包括一个处理查询并产生对源节点的响应所需要的时间量度。源节点从总的查询-响应时间中减去这个时间,以便确定通信所耗费的时间。



1. 一种确定目标节点到源节点的邻近程度的方法，包括：
将来自源节点的查询传送到目标节点；
将来自目标节点的响应传送到源节点，来自目标节点的响应包含了处理查询和产生响应所需要的处理时间的量度；
在源节点接收该响应；
确定传送查询和接收响应之间的查询-响应时间量度；以及
基于通信时间来确定目标节点的邻近程度，所述通信时间取决于查询-响应时间量度与处理时间量度之间的差值。
2. 权利要求 1 的方法，其中，查询和响应与密码密钥交换协议的至少一部分相对应。
3. 权利要求 2 的方法，其中，密钥交换协议与 Needham-Schroeder 密钥交换协议相对应。
4. 权利要求 1 的方法，其中，查询和响应与 OCPS 协议的至少一部分相对应。
5. 权利要求 1 的方法，其中，在目标节点中的处理时间量度是预先定义的。
6. 权利要求 1 的方法，其中，确定邻近程度包括将通信时间与用于区分本地和远程节点的阈值相比较。
7. 权利要求 1 的方法，还包括基于邻近程度来限制与目标节点的通信。
8. 权利要求 1 的方法，其中，目标节点对该响应执行了加密签名。
9. 一种网络上的节点，包括：
通信设备，被配置成接收来自源节点的查询并且向源节点传送相应的响应；
处理器，被配置成对该查询进行处理并且从中产生响应，
其中，
该响应包括处理查询和产生响应所需要的处理时间量度。
10. 权利要求 9 的节点，其中，处理器被配置成对查询进行处理并且产生响应，以此作为密码密钥交换协议的一部分。
11. 权利要求 10 的节点，其中，密钥交换协议与

Needham-Schroeder 密钥交换协议相对应。

12. 权利要求 9 的节点，其中，查询和响应与源节点启动的 OCPS 协议的至少一部分相对应。

13. 权利要求 9 的节点，其中，处理时间量度是预先定义的。

14. 权利要求 9 的节点，其中，处理器还被配置成对响应进行加密签名。

15. 一种网络上的节点，包括：

通信设备，被配置成向目标节点传送查询并且接收来自目标节点的相应的响应，来自目标节点的响应包含了在目标节点处处理查询和产生响应所需要的处理时间的量度；以及

处理器，被配置成：

产生查询，

接收响应，

测量产生查询和接收响应之间的查询-响应时间，以及

基于通信时间来确定目标节点相对于该节点的邻近程度，所述通信时间取决于查询-响应时间与处理时间之间的差值。

16. 权利要求 15 的节点，其中，处理器被配置成产生查询并且接收响应，以此作为密码密钥交换协议的一部分。

17. 权利要求 16 的节点，其中，密钥交换协议与 Needham-Schroeder 密钥交换协议相对应。

18. 权利要求 15 的节点，其中，查询和响应与由该节点启动的 OCPS 协议的至少一部分相对应。

19. 权利要求 15 的节点，其中，处理时间量度是预先定义的。

20. 权利要求 15 的节点，其中，处理器被配置成基于通信时间与用于区分本地节点和远程节点的阈值的比较结果来确定邻近程度。

21. 权利要求 15 的节点，其中，处理器还被配置成基于邻近程度来控制它与目标节点进行的后续通信。

确定目标节点到源节点的邻近程度的方法以及网络节点

技术领域

本发明涉及通信安全领域，尤其涉及一种验证网络上的节点的邻近程度的系统和方法。

背景技术

网络安全往往可以通过区分网络上的“本地”节点和“远程”节点而得以增强。例如，本地节点通常处于某个特定的物理环境内，并且可以假设授权处于该物理环境内部的用户访问网络。另一方面，远程节点则很容易受到未授权的物理访问。此外，网络上的非授权入侵者通常是借助电话或其他通信信道远程访问网络的。由于网络容易受到经由远程节点的未授权访问，因此，通过对远程节点实施严格的安全措施或者对其施加访问限制，可以增强网络安全，而本地节点则不会受到上述约束条件的阻碍。

发明内容

本发明的一个目的是提供一种系统和方法，以便简化网络上关于节点是本地节点还是远程节点的判定。本发明的另一个目的是提供一种系统和方法，以便简化网络上关于节点是本地节点还是远程节点的安全判定。本发明还有一个目的是将这种判定与验证网络上节点的可靠性的系统和方法集成。

这些及其他目的是通过一种系统和方法实现的，该系统和方法将定时参数包含在诸如开放式防拷贝系统（OCPS）之类的节点验证协议中，以简化目标节点与源节点的邻近程度的判定。节点验证协议包括一个查询-响应序列，在这个序列中，源节点向目标节点传送一个查询，目标节点则向源节点传送一个相应的响应。源节点基于实施这个查询-响应序列所需要的时间量度来建立源节点与目标节点之间的距离下限。并且实施该序列所需要的时间包含了传送查询和响应所需要的时间，以及处理查询和产生响应所需要的时间。目标节点包括一个处理查询并向源节点产生响应所需要的时间量度。源节点从总的查询

-响应时间中减去这个时间，以便确定通信耗费的时间。这个通信时间将会与一个阈值相比较，由此可以判定目标节点相对源节点而言是本地节点还是远程节点。

附图说明

图 1 描述的是节点的网络的一个实例框图。

图 2 描述的是依照本发明来实施查询-响应协议的源节点和目标节点的实例框图。

贯穿整个附图，相同的参考数字表示相同的元件或是基本上执行相同功能的元件。

具体实施方式

图 1 描述的是节点 110 的网络 150 的一个实例框图。节点之一(节点 D 100)被描述为远离其他节点 110。依照本发明，对节点 110 中的每一个进行配置，以便能够判定每一个其他节点 110 的邻近程度。在本发明的一个典型实施例中，邻近程度的判定被限于判定其他节点是“本地节点”还是“远程节点”，虽然也可以使用在此公开的技术来实施更详细的距离判定。

图 2 描述的是源节点 110S 和目标节点 110T 的实例框图，该源节点 110S 和目标节点 110T 依照本发明实施查询-响应协议以确定目标节点 110T 到源节点 110S 的邻近程度。源节点 110S 包括一个启动查询的处理器 210、以及一个将查询传送到目标节点 110T 的通信设备 220。目标节点 110T 借助其通信设备 230 来接收查询，并且返回一个相应的响应。为了确保该响应对应于所传送的查询，所述协议要求目标节点 110T 借助处理器 240 来处理至少一部分查询，并且将处理结果包含在响应中。

源节点 110S 被配置来测量查询-响应过程所耗费的时间，在图 2 中这个时间是用 $T_{\text{查询-响应}}$ 280 描述的。这个查询-响应时间 280 包含了传送查询和响应的时间 ($T_{\text{通信}}$ 260) 以及在目标节点 110T 处理查询和产生响应所需要的时间 $T_{\text{处理}}$ 270。依照本发明，对目标节点 110T 进行了配置，以将处理时间 270 的一个量度包含在为源节点 110S 提供的响应中。源节点 110S 则从查询-响应时间 280 中减去处理时间

270, 以便确定通信时间 260。通过使用已知技术, 可以用所确定的通信时间 260 来计算源 110S 与目标 110T 之间的距离。如上所述, 在一个典型的实施例中, 使用了通信时间 260 来判定目标 110T 相对于源节点 110S 而言是本地节点还是远程节点。在本发明的一个优选实施例中, 该判定是通过将通信时间 260 与一个大小通常最多为几微秒的标称阈值进行比较来完成的。如果通信时间 260 低于这个阈值, 则判定目标 260T 是本地节点; 否则判定该节点是远程节点。

在一个典型的实施例中, 源 110S 使用了远程/本地邻近程度判定来控制其与目标 110T 的后续通信。例如, 某些文件可能只允许传送到本地节点, 并且与远程节点所进行的全都通信都需要加密等等。可选地, 可以定义多个阈级来区分不同的距离范围, 例如远程目标节点与源节点是否同处一个国家等等。

应该注意的是, 未授权节点可以通过提供一个虚假处理时间来破坏上述过程。在本发明的一个优选实施例中, 上述查询-响应过程被集成在诸如密钥交换过程之类的节点鉴定过程中, 其中该节点鉴定过程通常包含了一个或多个查询-响应序列。通过将查询-响应过程集成在节点鉴定过程内部, 可以验证所报告的处理时间都是可靠的。

例如, OCPS 协议包括鉴定阶段、密钥交换阶段、密钥生成阶段以及后续的数据传输阶段。密钥交换阶段是经过被修改的 Needham-Schroeder 密钥交换协议来实施的, 如在 Menezes 等人编著的“Handbook of Applied Cryptography (应用密码术手册)”一书中所描述的那样。

在鉴定阶段, 每一个源 110S 和目标 110T 节点都会鉴定对方的公用密钥。

当开始密钥交换阶段时, 源 110S 使用目标 110T 的公用密钥来加密一个随机数和一个随机密钥, 并且将这两个加密信息项传送到目标 110T。依照本发明, 当向目标 110T 传送这些加密信息项时, 源节点 110S 将会启动一个定时器。

目标 110T 使用目标的私有密钥来解密随机数和随机密钥。目标 110T 产生一个新随机数和一个新随机密钥, 并且使用源 110S 的公用密钥来加密新随机数、新随机密钥以及来自源 110S 的解密随机数, 以形成一个传送到源 110S 的响应。可选地, 目标 110T 可以使用目标

的私有密钥来对该响应进行签名。依照本发明，目标 110T 还将实施解密、加密和签名所需要的时间量度包含在所签名的响应中。可选地，这个处理时间也可以是通过使用源的公用密钥而被加密的。由于这个解密、加密和签名过程通常会在指定目标节点耗费相同时间量，因此优选地对目标节点进行配置，使之提供一个预定处理时间，以此作为实施该处理的时间量度。通过对响应进行签名，目标 110T 可以将所报告的处理时间绑定给当前响应中的其他参数，由此避免未授权的利用一个使用源 110S 的公用密钥加密的替换时间来代替加密处理时间。

当源节点 110S 接收到响应时，它会终止前述定时器。源节点 110S 将会使用目标 110T 的公用密钥来验证该被签名的消息，并且使用源 110S 的私有密钥从响应中解密出随机数和随机密钥。如果响应内的处理时间被加密，则这时源节点 110S 会使用源 110S 的私有密钥来对其解密。依照本发明，源 110S 会从定时器测得的从源 110S 发送加密查询与从目标 110T 接收加密响应之间的持续时间中减去处理时间，以便确定源 110S 与目标 110T 之间的往返通信时间。

为了确认密钥交换，源 110S 会将经过解密的新随机数传送回目标 110T。源 110S 和目标 110T 都是基于对正确解密的随机数所进行的接收来控制后续通信的。依照本发明，源 110S 还基于所确定的通信时间来控制后续通信。

如果验证了这两个节点，则源 110S 和目标 110T 之间的后续通信是通过使用作为随机密钥、公用密钥和会话索引的组合的会话密钥来对通信进行加密的。

在上文中仅仅描述了本发明的原理。因此应注意，本领域技术人员将能够设计不同的方案，虽然在这里并没有明确描述或显示这些方案，但是这些方案均体现了本发明的原理，因此这些方案全都处于本发明的精神和范围以内。其中举例来说，在上述 OCPS 协议中，通过对传送所加密的响应与接收来自源 110S 的解密随机数之间的过程进行计时，还可以将目标节点 110T 配置用来确定源节点 110S 的邻近程度。在这个实施例中，源 110S 被配置成将处理加密响应和传送解密随机数所需要的时间量度包含在最后一个密钥交换消息中，其中该消息包含了由源 110S 执行了数字签名的解密随机数。目标 110T 从其所

测量的传送与接收之间的时间中减去这个处理时间，以便确定目标-源-目标的往返通信时间，并且由此确定源 110S 与目标 110T 的邻近程度。对本领域普通技术人员来说，根据本公开，这些和其他系统配置和优化特性都是显而易见的，并且这些和其他系统配置和优化特性全都包含在下列权利要求的范围以内。

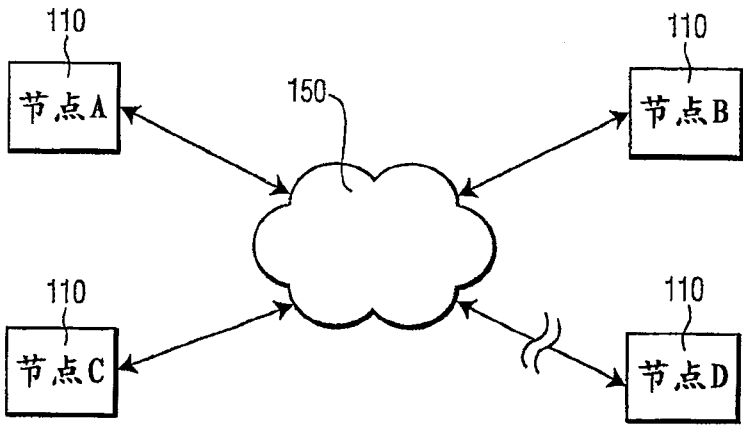


图 1

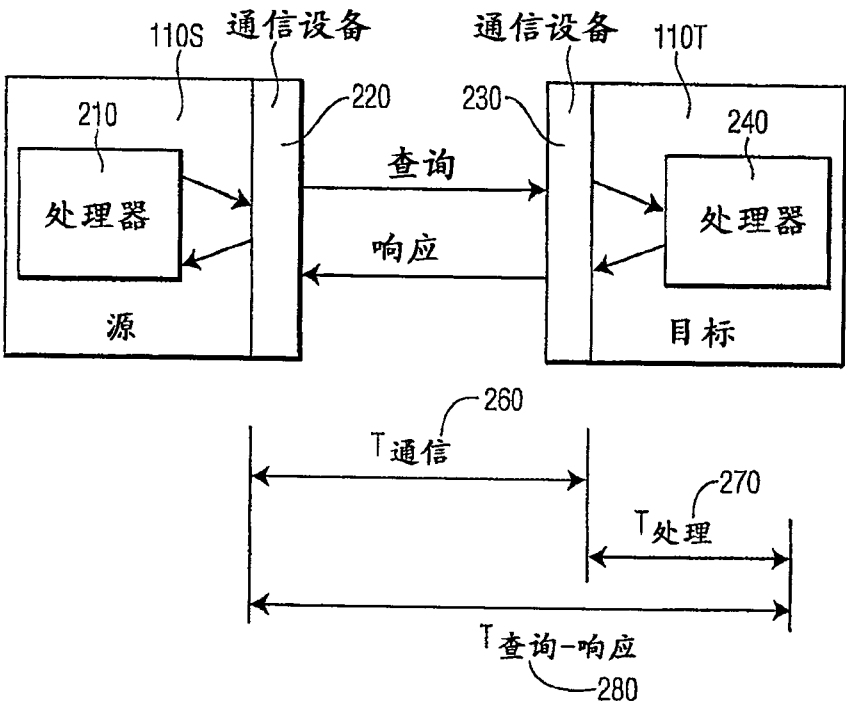


图 2