(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 102714652 B
(45)授权公告日 2016.01.20

(21)申请号 201080051601.5
(22)申请日 2010.09.01
(30)优先权数据
0956161 2009.09.09 FR
(85)PCT国际申请进入国家阶段日
2012.05.09
(86)PCT国际申请的申请数据
PCT/FR2010/051823 2010.09.01
(87)PCT国际申请的公布数据
WO2011/030045 FR 2011.03.17
(73)专利权人 QoSMOS 公司
地址 法国巴黎
(72)发明人 杰罗米·托莱特 杰罗米·阿贝拉
(74)专利代理机构 上海天协和诚知识产权代理事务所 31216
代理人 童锡君
(51)Int.Cl.
H04L 29/06(2006.01)
(56)对比文件
US 2005220095 A1,2005.10.06, 说明书第[0006]-[0091]段,附图1、9-10.
US 2006291450 A1,2006.12.28, 说明书第[0063]段.
US 2008134329 A1,2008.06.05, 全文.
US 7212522 B1,2007.05.01, 说明书第3栏第15-19行,第8栏第52-59行.
审查员 孙凯

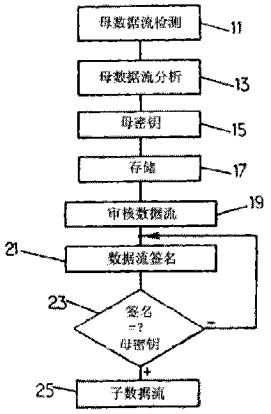
权利要求书1页 说明书4页 附图2页

(54)发明名称

监测数据网络中包括多个数据流的通讯会话

(57)摘要

本发明涉及一种监测整个数据网络的通讯会话的方法,所述会话包括使用第一协议的第一数据流,所述第一数据流称之为母数据流,该母数据流包括允许使用适用于所述会话的第二协议来建立第二数据流的数据,所述第二数据流称之为子数据流,所述方法包括:搜索(13)在数据流中允许建立子数据流的数据;使用这些数据生成(15)和存储(17)签名,称之为母密钥;审核(19)在所述数据网络中使用第二协议的数据流;生成(21)各个所述数据流的签名;比较(23)各个所述数据流的签名和母密钥;并且如果比较结果为正,则确定(25)对应的数据流为会话的子数据流。



CN 102714652 B

1. 一种监测数据网络中的通讯会话的方法，所述会话包括使用第一协议的第一数据流，所述第一数据流称之为母数据流，所述母数据流包括允许使用适用于所述会话的第二协议来建立第二数据流的数据，所述第二数据流称之为子数据流，所述方法包括：

搜索 (13) 在所述母数据流中允许建立子数据流的数据；

生成 (15) 和存储 (17) 适用于所述数据的签名，称之为母密钥；

审核 (19) 在所述数据网络中使用第二协议的数据流；

对于在所审核的数据流中的各个指定数据流：

生成 (21) 所述指定数据流的签名；

比较 (23) 所述签名和母密钥；以及，

如果比较结果为正，则标示所述指定数据流为会话的子数据流。

2. 根据权利要求 1 所述的方法，其特征在于，所述会话包括确定多个子数据流，审核数据流直至确定子数据流的集合。

3. 根据权利要求 1 所述的方法，其特征在于，所述子数据流包括允许使用适用于所述会话的第三协议来建立第三数据的数据，使用所述数据生成签名，以及审核使用第三协议的数据流直至确定对应所述会话的数据流。

4. 根据权利要求 1 所述的方法，其特征在于，所述监测多个会话的方法包括母数据流，生成和存储母密钥，所述数据流使用第二协议，将所述签名与各个母密钥进行比较，以确定所述数据流是否为一个会话的子数据流。

5. 一种监测数据网络中的通讯会话的系统，所述会话包括使用第一 协议的第一数据流，所述第一数据流称之为母数据流，所述母数据流包括允许使用适用于所述会话的第二协议来建立第二数据流的数据，所述第二数据流称之为子数据流，所述系统包括：

第一数据流分析器 (31)，用于搜索在母数据流中允许建立子数据流的数据；

第一签名生成器 (33)，用于使用所述数据生成签名，称之为母密钥；

存储器 (35)，用于存储所述签名；

第二数据流分析器 (37)，用于审核在所述数据网络中使用第二协议的数据流；

对于在所审核的数据流中的各个指定数据流：

第二签名生成器 (39)，用于生成所述指定数据流的签名；

比较器 (41)，用于比较所述签名和母密钥；以及，

标示器 (43)，如果比较的结果为正，则标示对应所述签名的数据流为所述会话的子数据流。

6. 根据权利要求 5 所述的系统，其特征在于，所述系统至少包括连接着数据网络的两个装置，第一装置至少包括存储器、签名比较器以及标示器，第二装置至少包括第一数据流分析器，第一签名生成器以及将所生成的信号传输至第一装置的接口。

7. 根据权利要求 6 所述的系统，其特征在于，所述系统至少包括通过数据网络连接着第一装置的第三装置，并且至少包括第二数据流分 析器、第二签名生成器以及用于将所生成的签名传输至第一装置的接口。

监测数据网络中包括多个数据流的通讯会话

[0001] 本发明涉及监测数据网络中的通讯会话的方法和系统，所述会话包括使用第一协议的第一数据流，该第一数据流称之为母数据流，该母数据流包括允许使用适用于会话的第二协议来建立第二数据流的数据，该第二数据流称之为子数据流。本发明还涉及实施监测方法的计算机程序产品。

[0002] 现有的网络应用通常使用多个会话和协议来执行它们的任务。

[0003] 例如，在视频会议所产生的视频通话中，RTP 会话 (Real Time Protocol - 实时协议）可由 SIP 会话 (Session Initiation Protocol- 会话初始化协议）进行初始化，并且 RTP 会话参数取决于 SIP 会话所交换的信息。

[0004] 诸如防火墙之类的网络监测装置使用状态机制来建立在不同协议会话之间的连接。

[0005] 这种解决方法存在着增加这些装置的复杂性的缺陷，因为状态机制的行为必须针对各个新的网络运用进行设置。此外，不同数据流的处理会引起资源聚集，从而限制通过这些装置的有效带宽，或者需要形成更加昂贵的机制，或者限制所能监测的数据量。

[0006] 因此，有利的是采用有效的硬件和实施资源来监测多协议网络应用的方法和系统。

[0007] 为了克服上述一项或多项缺点，提出一种监测数据网络中的通讯会话的方法，所述会话包括使用第一协议的第一数据流，所述第一数据流称之为母数据流，所述母数据流包括允许使用适用于所述会话的第二协议来建立第二数据流的数据，所述第二数据流称之为子数据流，所述方法包括 ：

[0008] ●搜索在所述母数据流中允许建立子数据流的数据 ；

[0009] ●生成和存储适用于所述数据的签名，称之为母密钥 ；

[0010] ●审核在所述数据网络中使用第二协议的数据流 ；

[0011] ●生成各个所述数据流的签名 ；

[0012] ●比较各个所述数据流的签名和母密钥 ；以及，

[0013] ●如果比较结果为正，则确定所对应的数据流为会话的子数据流。

[0014] 通过定义具有合适签名的各个数据流以及执行简单的签名比较，由计算机来执行该方法就非常迅速和简便，所述方法优选允许对相关的数据流进行简单的分类，并且不需要定义状态机制。

[0015] 本发明所具有的具体特征或优点可以单独使用或者组合使用，包括 ：

[0016] • 所述会话包括确定多个子数据流，审核数据流直至确定子数据流的集合 ；

[0017] • 所述子数据流包括允许使用适用于会话的第三协议来建立第三数据的数据，使用这些数据来生成签名，并且审核使用第三协议的数据流直至确定对应于所述会话的数据流 ；

[0018] • 监测多个会话的方法，包括生成和存储母数据流的母密钥，适用于使用第二协议的数据流，将签名与各个母密钥进行比较，以确定所述数据流是否为一个会话的子数据流。

[0019] 值得注意的是，所述方法有利于应用多个母数据流、子数据流及其定义一个或多

个母数据流之间遗传、具有任何等级遗传的一个或多个子数据流之间遗传的任何类型的树结构。

[0020] 本发明的第二部分中，提出一种计算机程序，其包括存储在计算机可读介质上的程序代码，以当在计算机中执行该程序时可执行上述的方法的步骤。

[0021] 本发明的第三部分中，提出一种监测数据网络中的通讯会话的系统，所述会话包括使用第一协议的第一数据流，所述第一数据流称之为母数据流，所述母数据流包括允许使用适用于所述会话的第二协议来建立第二数据流的数据，所述第二数据流称之为子数据流，所述系统包括：

[0022] • 第一数据流分析器，用于搜索在母数据流中允许建立子数据流的数据；

[0023] • 第一签名生成器，用于使用所述数据生成签名，称之为母密钥；

[0024] • 存储器，用于存储所述签名；

[0025] • 第二数据流分析器，用于审核在所述数据网络中使用第二协议的数据流；

[0026] • 第二签名生成器，用于生成各个所述数据流的签名；

[0027] • 比较器，用于比较各个所述数据流的签名和母密钥；以及，

[0028] • 标示器，如果比较的结果为正，则标示对应所述签名的数据流为所述会话的子数据流。

[0029] 在本发明的实施例中，系统至少包括由数据网络相连接的两个装置，第一装置至少包括存储器、签名比较器和标示器，第二装置至少包括第一数据流分析器，第一签名生成器和将所生成的签名传输至第一装置的接口。它还至少包括由数据网络连接着第一装置的第三装置，并且至少包括第二数据流分析器、第二签名生成器和将所生成的签名传输至第一装置的接口。

[0030] 本发明将通过下文以及参考附图的阐述变得更加明晰，附图包括：

[0031] 图 1 为数据网络的示意图；

[0032] 图 2 为根据本发明实施例的方法的流程图；

[0033] 图 3 为根据本发明第一实施例的监测系统的示意图；以及，

[0034] 图 4 为根据本发明第二实施例的监测系统的示意图。

[0035] 参照图 1，数字数据网络 1 互连着多个装置 3。监测系统 5 连接着该网络，以获取在装置 3 之间所交换的数据。

[0036] 系统 5 监测通过网络 1 所传播的通讯会话。“会话”或应用会话为给定网络应用所产生的数据交换集。

[0037] 例如，如众所周知，当第一装置希望使用 FTP 协议将文件传输至第二装置时，第一装置和第二装置在端口 21 上开始使用 TCP 协议的第一次交换，然后允许在变化但高于 1024 的端口上传输采用 TCP 协议使用 FTP-DATA 的实际文件。所有的这些交换一起构成一个会话。

[0038] 第一个 TCP 在端口 21 的交换并使用 FTP-DATA 传输，下文称之为子会话或简单数据流。

[0039] 第一子会话称之为母的子会话或母数据流，因为其能够在两个装置之间交换数据，并允许建立第二子会话，称之为子的子会话或子数据流。

[0040] 为了监测会话，系统 5 实施下述方法，如图 2 所示意说明。

[0041] 所述系统通过分析所传输的数据，在步骤 11 中监测所述应用会话已经以母数据流的形式建立。

[0042] 然后，在步骤 13 中，系统 5 分析母数据流，以发现用于建立子数据流的数据。例如，在 FTP 会话中，系统 5 将分析所发送的数据包，以确定形成传输的端口。

[0043] 一旦收集到这些数据，系统 5 在步骤 15 中使用这些数据生成称为母密钥的签名。例如，对 FTP 对话，系统 5 从信源装置和接收装置的 IP 地址以及端口数来产生签名。该签名是例如这些数据的 hash（无序）数值。

[0044] 这个母密钥由系统 5 在步骤 17 中存储。

[0045] 随后，系统 5 监测对应于子数据流的数据流，例如在步骤 19 中，因为子数据流使用与之相匹配的协议。

[0046] 在步骤 21 中，计算各个数据流的签名。该签名计算与母密钥计算相类似。例如，对 FTP 会话，计算两个装置的 IP 地址以及端口数的 hash 密钥。

[0047] 在步骤 23 中，将该密钥与母密钥进行比较。

[0048] 如果比较结果为正，则在步骤 25 中，将对应数据流确认为所寻找的子数据流。

[0049] 为方便阐述，下文限制为一个母数据流和一个子数据流。然而，本发明可以简单地适用于多个母数据流和子数据流。

[0050] 于是，如果会话包含母数据流和多个子数据流，则系统将计算尽可能多的母密钥，并且监测多个数据流直至获得子数据流。

[0051] 相反的，多个会话，并因此可以同时监测多个母数据流。

[0052] 然后，将数据流签名与所有母密钥进行比较，直至获得对应的母密钥，以此定义相关的会话。如果没有对应的密钥，这意味着该数据流不属于监测会话中的任一一个会话。

[0053] 所述方法也可简单地适用于包括多个遗传等级的会话，即子数据流包括用于建立其它数据流的数据，并且其行为构成作为其它子数据流的母数据流。根据由子数据流所形成的连接数据，所述系统定义与潜在的子数据流的签名相比较的母密钥。

[0054] 本方法可根据所需技术特征以及处理系统的能力以各种不同的形式准确实施。

[0055] 例如，母密钥集合可以对应于具有会话名字特征的排序向量。一旦计算出数据流的签名，母密钥或密钥的搜索和比较以及对会话的数据流的分配对应于基于索引的操作，这是计算机在资源和速度方面都十分有效的操作。这还能够对多个会话进行监测。

[0056] 如图所示，检测系统 5 还包括：

[0057] ●第一数据流分析器 (31)，用于搜索在母数据流中允许建立子数据流的数据；

[0058] ●第一签名生成器 (33)，用于使用所述数据生成签名，称之为母密钥；

[0059] ●存储器 (35)，用于存储所述签名；

[0060] ●第二数据流分析器 (37)，用于审核在所述数据网络中使用第二协议的数据流；

[0061] ●第二签名生成器 (39)，用于生成各个数据流的签名；

[0062] ●比较器 (41)，将各个数据流的签名和母密钥进行比较；以及，

[0063] ●标示器 (43)，如果比较的结果为正，则标示对应于所述签名的数据流为所述会话的子数据流。

[0064] 该监测系统可以由专用电子电路或者通过由计算机编程的程序代码的计算机程序来执行，所述计算机程序可以存储在计算机的可读介质上，当在计算机上执行本程序时，

则能够执行监测方法的步骤。尤其是，计算机包括能够监听网络中数据传输的网络接口、用于生成密钥和签名的连接着处理器的随机存取存储器、以及用于例如存储签名生成标准的硬盘驱动器之类的非易失性存储器。

[0065] 所述系统的一个具体实施例包括将其分成多个非集中的装置，如图 4 所示。第一装置系列 50 设置在所述数据流的附近，包括数据流分析器 31、37 以及签名生成器 33、39。然后，各自包括与集中装置 54 通讯的通讯接口 52，除了连接着接口 52 的通讯接口 56 之外，所述集中装置 54 还包括用于存储签名的非易失性存储器 35，以及签名比较器 41 和标示器 43。在第一装置 50 中也可以发现最后一个单元，用于在产生数据流的附近来标示数据流。

[0066] 本发明已通过上文以及附图作了阐述。有可能有许多不同的变化例。

[0067] 具体的，监测系统可以包括单一的数据流分析器和单一的签名生成器，用于审核数据流并生成母数据流和子数据流的签名。或者，为了提高速度，可以有与它们相同数量的协议类型。

[0068] 在权利要求中，“包括”一词具有不排除其它元素的含义，以及定冠词“一个”一词具有不排除多个的含义。

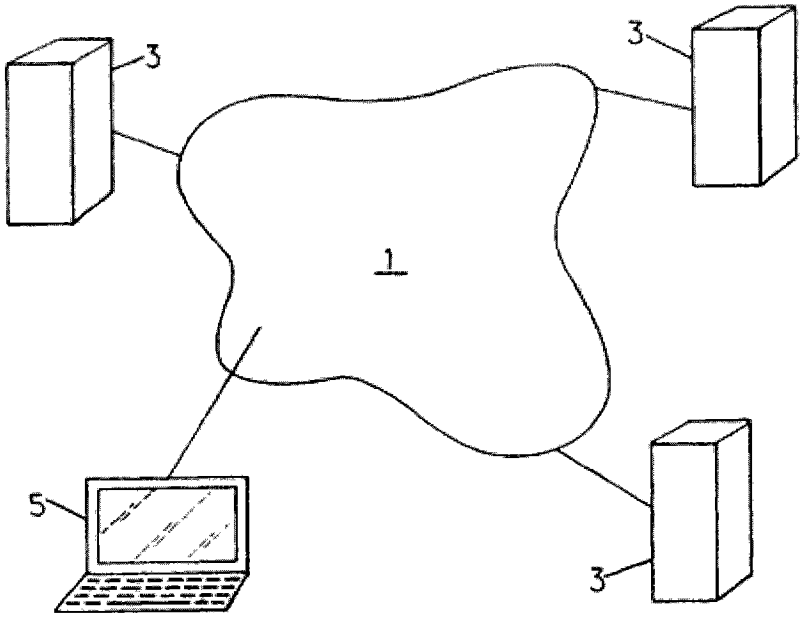

3
3
1
5
3

FIG. 1.

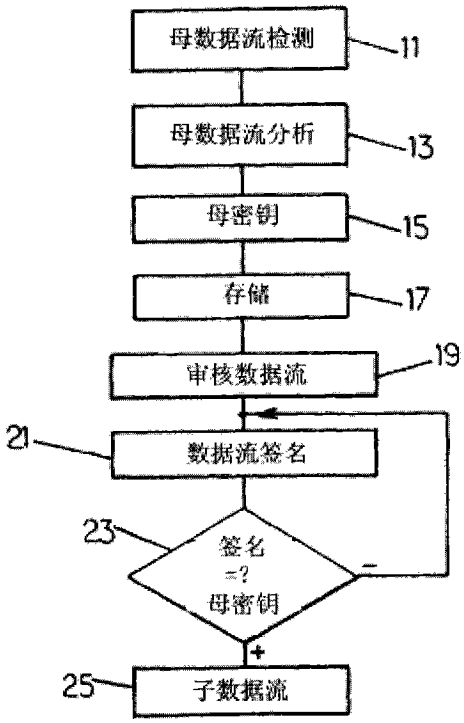

母数据流检测
11
母数据流分析
13
母密钥
15
存储
17
审核数据流
19
21
数据流签名
23
签名
=?
母密钥
-
+
25
子数据流

FIG. 2.

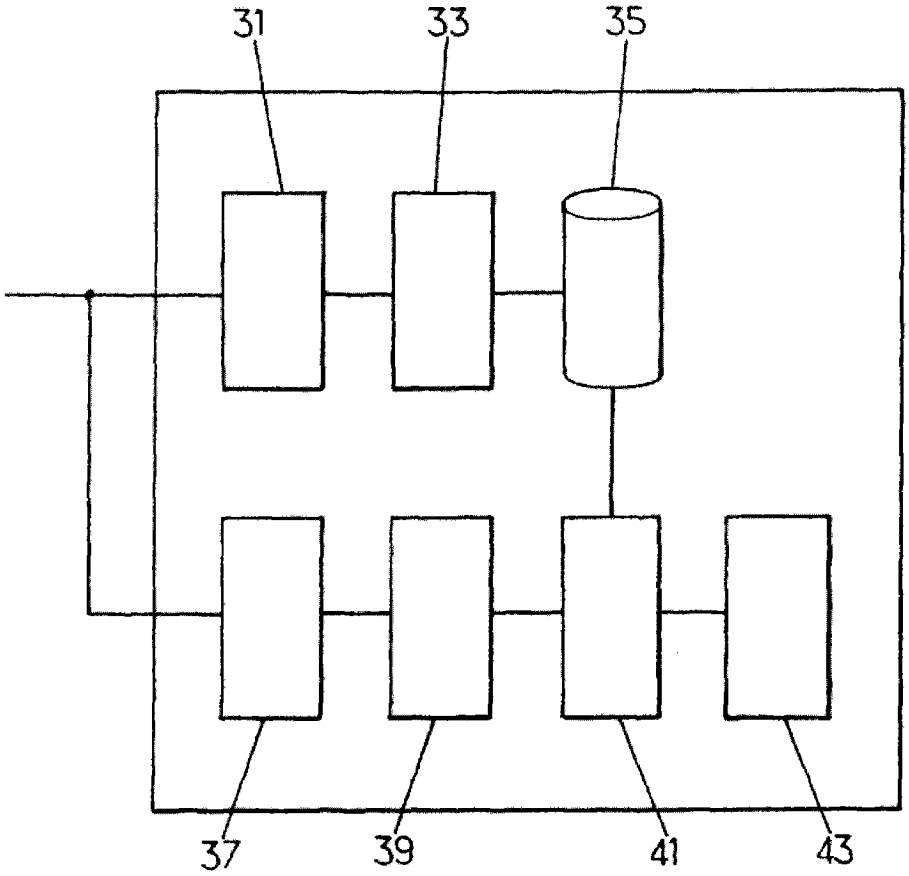


FIG. 3.

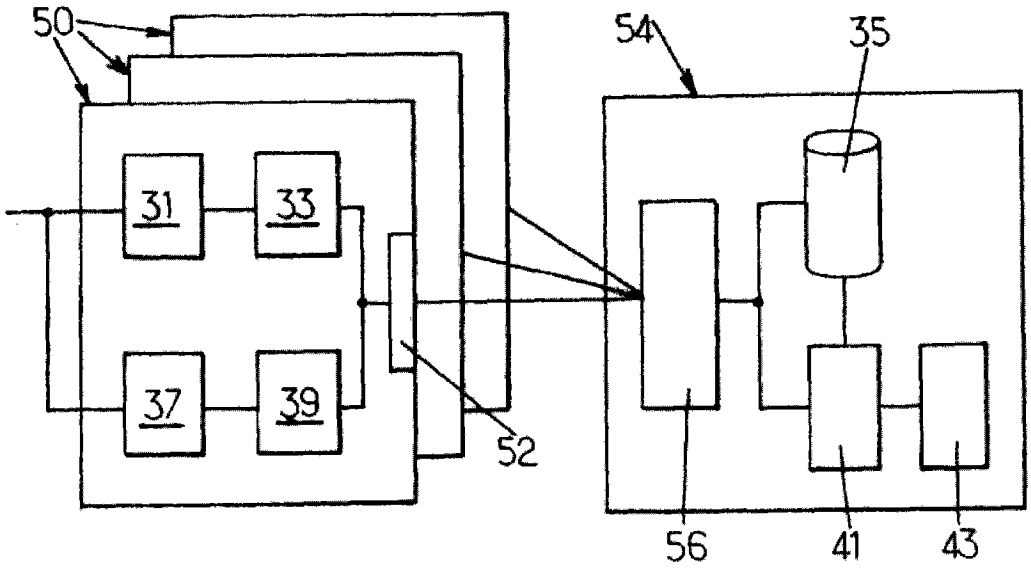


FIG. 4.