(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104618142 A
(43)申请公布日 2015.05.13

(21)申请号 201410850950.3

(22)申请日 2014.12.30

(71)申请人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)
申请人 奇智软件(北京)有限公司

(72)发明人 朱禄

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
代理人 李相雨

(51)Int.Cl.
H04L 12/24(2006.01)
H04L 12/40(2006.01)

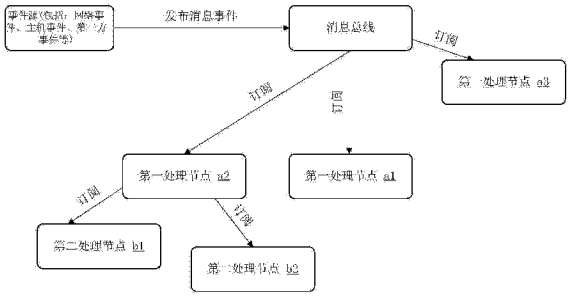
权利要求书2页 说明书15页 附图3页

(54)发明名称

消息订阅方法、处理节点设备和总线设备

(57)摘要

本发明提供一种消息订阅方法、处理节点设备和总线设备，其中，消息订阅方法包括：在事件源通过消息总线发布消息事件时，加载在所述消息总线上的至少一个第一处理节点根据第一配置信息在所述消息事件中获取与所述第一配置信息对应的消息事件；所述第一处理节点根据所述第一配置信息处理获取的消息事件；其中，所述第一处理节点为采用插件形式动态加载在所述消息总线上的节点。上述消息订阅方法能够实现对总线的动态扩展，方便以消息事件为粒度的网络安全产品进行后期维护。



CN 104618142 A

1. 一种处理节点设备，其特征在于，处理节点为采用插件形式加载在消息总线上，所述处理节点包括：

第一获取模块，用于在事件源通过所述消息总线发布消息事件时，根据第一配置信息在所述消息事件中获取与所述第一配置信息对应的消息事件；

处理模块，用于根据所述第一配置信息处理获取的消息事件。

2. 根据权利要求 1 所述的处理节点设备，其特征在于，所述处理节点设备还包括：

加载模块，用于加载至少一个第二处理节点，生成与该第二处理节点对应的第二配置信息；

所述第二处理节点根据所述第二配置信息从所述处理节点订阅或发布的消息事件中获取与所述第二配置信息对应的消息事件，以及处理获取的消息事件。

3. 根据权利要求 2 所述的处理节点设备，其特征在于，所述至少一个处理节点和所述至少一个第二处理节点组成二叉树结构；

或者，

所述至少一个处理节点和所述至少一个第二处理节点组成链式结构。

4. 根据权利要求 1 至 3 任一所述的处理节点设备，其特征在于，所述处理节点设备还包括：

第二获取模块，用于根据所述第一配置信息从另一处理节点中订阅或发布的消息事件中获取与所述第一配置信息对应的消息事件。

5. 根据权利要求 1 至 3 任一所述的处理节点设备，其特征在于，所述事件源包括下述的一种或多种：

服务器中的主机事件源、互联网中的网络事件源和第一处理节点中的事件源、通过所述消息总线发布消息事件的任一接入系统。

6. 根据权利要求 1 至 5 任一所述的处理节点设备，其特征在于，所述第一配置信息包括下述的一种或多种：

在所述消息总线中订阅符合预设规则的消息事件、删除符合预设规则的消息事件、添加符合预设规则的消息事件的属性、发布消息事件、丢弃符合预设规则的消息事件、转发符合预设规则的消息事件、实名制映射符合预设规则的消息事件、关联分析符合预设规则的消息事件、存储符合预设规则的消息事件。

7. 根据权利要求 1 至 6 任一所述的处理节点设备，其特征在于，所述处理模块，具体用于：

修改获取的消息事件的属性，并将修改属性后的消息事件发布；

或者，

丢弃获取的消息事件；

或者，

将获取的消息事件存储在数据库中；

或者，

根据获取的消息事件进行流量统计分析或安全统计分析；

或者，

根据获取的消息事件进行关联分析；

或者，

转发获取的消息事件。

8. 一种总线设备，其特征在于，包括：

加载模块，用于加载插件形式的至少一个第一处理节点；

生成模块，用于根据所述加载模块加载的至少一个第一处理节点，生成该第一处理节点的第一配置信息；

查找模块，用于在事件源通过所述消息总线发布消息事件时，根据所述第一配置信息查找与所述第一配置信息对应的消息事件；

发送模块，用于将查找的消息事件发送所述第一处理节点，以使所述第一处理节点处理发送的消息事件。

9. 一种消息订阅方法，其特征在于，包括：

在事件源通过消息总线发布消息事件时，加载在所述消息总线上的至少一个第一处理节点根据第一配置信息在所述消息事件中获取与所述第一配置信息对应的消息事件；

所述第一处理节点根据所述第一配置信息处理获取的消息事件；

其中，所述第一处理节点为采用插件形式加载在所述消息总线上的节点。

10. 一种消息订阅方法，其特征在于，包括：

消息总线加载插件形式的至少一个第一处理节点，并生成该第一处理节点的第一配置信息；

在事件源通过所述消息总线发布消息事件时，所述消息总线根据所述第一配置信息查找与所述第一配置信息对应的消息事件，将查找的消息事件发送所述第一处理节点，以使所述第一处理节点处理发送的消息事件。

消息订阅方法、处理节点设备和总线设备

技术领域

[0001] 本发明涉及数据处理技术领域，尤其涉及一种消息订阅方法、处理节点设备和总线。

背景技术

[0002] 在现有网络安全产品中，很多产品都是以消息或事件为粒度进行统计或拟合，例如，网络安全产品中入侵检测系统(Intrusion Detection Systems，简称IDS)、入侵防御系统(Intrusion Prevention System，简称IPS)、安全运行中心(Security Operations Center，简称SOC)以及安全网关(Unified Threat Management，简称UTM)等都会以消息事件来作为输入或输出。

[0003] 但是，现有的网络安全产品中以消息事件作为输入或输出的消息总线是固定的，无法进行后期维护，进而无法对网络安全产品进行扩展，导致网络安全产品的效率低，并对产品功能的扩展带来一定限制。

发明内容

[0004] 针对现有技术中的缺陷，本发明提供了一种消息订阅方法、处理节点和总线，能够实现对对消息总线的动态扩展，方便以消息事件为粒度的网络安全产品进行后期维护。

[0005] 第一方面，本发明提供一种处理节点设备，处理节点为采用插件形式加载在消息总线上，所述处理节点包括：

[0006] 第一获取模块，用于在事件源通过所述消息总线发布消息事件时，根据第一配置信息在所述消息事件中获取与所述第一配置信息对应的消息事件；

[0007] 处理模块，用于根据所述第一配置信息处理获取的消息事件。

[0008] 可选地，所述处理节点还包括：

[0009] 加载模块，用于加载至少一个第二处理节点，生成与该第二处理节点对应的第二配置信息；

[0010] 所述第二处理节点根据所述第二配置信息从所述处理节点订阅或发布的消息事件中获取与所述第二配置信息对应的消息事件，以及处理获取的消息事件。

[0011] 可选地，所述至少一个处理节点和所述至少一个第二处理节点组成二叉树结构；

[0012] 或者，

[0013] 所述至少一个处理节点和所述至少一个第二处理节点组成链式结构。

[0014] 可选地，所述处理节点设备还包括：

[0015] 第二获取模块，用于根据所述第一配置信息从另一处理节点中订阅或发布的消息事件中获取与所述第一配置信息对应的消息事件。

[0016] 可选地，所述事件源包括下述的一种或多种：

[0017] 服务器中的主机事件源、互联网中的网络事件源和第一处理节点中的事件源、通过所述消息总线发布消息事件的任一接入系统。

[0018] 可选地，所述第一配置信息包括下述的一种或多种：

[0019] 在所述消息总线中订阅符合预设规则的消息事件、删除符合预设规则的消息事件、添加符合预设规则的消息事件的属性、发布消息事件、丢弃符合预设规则的消息事件、转发符合预设规则的消息事件、实名制映射符合预设规则的消息事件、关联分析符合预设规则的消息事件、存储符合预设规则的消息事件。

[0020] 可选地，所述处理模块，具体用于：

[0021] 修改获取的消息事件的属性，并将修改属性后的消息事件发布；

[0022] 或者，

[0023] 丢弃获取的消息事件；

[0024] 或者，

[0025] 将获取的消息事件存储在数据库中；

[0026] 或者，

[0027] 根据获取的消息事件进行流量统计分析或安全统计分析；

[0028] 或者，

[0029] 根据获取的消息事件进行关联分析；

[0030] 或者，

[0031] 转发获取的消息事件。

[0032] 可选地，所述消息事件为 MAP 消息类型的消息事件；

[0033] 所述消息事件的格式为动态扩展的键 - 值 key-value 格式；

[0034] 和 / 或，

[0035] 所述消息事件的属性包括：所述消息事件的源 IP、目的 IP、源端口号和目的端口号。

[0036] 第二方面，本发明还提供了一种总线设备，包括：

[0037] 加载模块，用于加载插件形式的至少一个第一处理节点，并生成该第一处理节点的第一配置信息；

[0038] 查找模块，用于在事件源通过所述消息总线发布消息事件时，根据所述第一配置信息查找与所述第一配置信息对应的消息事件；

[0039] 发送模块，用于将查找的消息事件发送所述第一处理节点，以使所述第一处理节点处理发送的消息事件。

[0040] 可选的，所述消息总线还包括：

[0041] 删除模块，用于删除加载的至少一个第一处理节点。

[0042] 可选的，所述消息事件为 MAP 消息类型的消息事件；

[0043] 所述消息事件的格式为动态扩展的键 - 值 key-value 格式；

[0044] 和 / 或，

[0045] 所述消息事件的属性包括：所述消息事件的源 IP、目的 IP、源端口号和目的端口号。

[0046] 可选的，所述事件源包括下述的一种或多种：

[0047] 服务器中的主机事件源、互联网中的网络事件源、和第一处理节点中的事件源、通过所述消息总线发布消息事件的任一接入系统。

[0048] 可选的，所述第一配置信息包括下述的一种或多种：

[0049] 在所述消息总线中订阅符合预设规则的消息事件、删除符合预设规则的消息事件、添加符合预设规则的消息事件的属性、发布消息事件、丢弃符合预设规则的消息事件、转发符合预设规则的消息事件、实名制映射符合预设规则的消息事件、关联分析符合预设规则的消息事件、存储符合预设规则的消息事件。

[0050] 第三方面，本发明还提供了一种消息订阅方法，包括：

[0051] 在事件源通过消息总线发布消息事件时，加载在所述消息总线上的至少一个消息事件，所述消息事件为第一处理节点根据第一配置信息在所述消息事件中获取与所述第一配置信息对应的消息事件；

[0052] 所述第一处理节点根据所述第一配置信息处理获取的消息事件；

[0053] 其中，所述第一处理节点为采用插件形式加载在所述消息总线上的节点。

[0054] 可选的，所述方法还包括：

[0055] 所述第一处理节点还用于加载至少一个第二处理节点，生成与该第二处理节点对应的第二配置信息；

[0056] 所述第二处理节点根据所述第二配置信息从所述第一处理节点订阅或发布的消息事件中获取与所述第二配置信息对应的消息事件，以及处理获取的消息事件。

[0057] 可选的，所述至少一个第一处理节点和所述至少一个第二处理节点组成二叉树结构；

[0058] 或者，

[0059] 所述至少一个第一处理节点和所述至少一个第二处理节点组成链式结构。

[0060] 可选的，所述方法还包括：

[0061] 所述第一处理节点根据所述第一配置信息从另一第一处理节点中订阅或发布的消息事件中获取与所述第一配置信息对应的消息事件。

[0062] 可选的，所述事件源包括下述的一种或多种：

[0063] 服务器中的主机事件源、互联网中的网络事件源、和第一处理节点中的事件源、通过所述消息总线发布消息事件的任一接入系统。

[0064] 可选的，所述加载在所述消息总线上的至少一个第一处理节点根据第一配置信息在所述消息事件中获取与所述第一配置信息对应的消息事件之前，所述方法还包括：

[0065] 所述消息总线加载至少一个第一处理节点，生成与该第一处理节点对应的第一配置信息；

[0066] 和/或，

[0067] 所述第一配置信息包括下述的一种或多种：

[0068] 在所述消息总线中订阅符合预设规则的消息事件、删除符合预设规则的消息事件、添加符合预设规则的消息事件的属性、发布消息事件、丢弃符合预设规则的消息事件、转发符合预设规则的消息事件、实名制映射符合预设规则的消息事件、关联分析符合预设规则的消息事件、存储符合预设规则的消息事件。

[0069] 可选的，所述第一处理节点根据所述第一配置信息处理获取的消息事件，包括：

[0070] 所述第一处理节点修改获取的消息事件的属性，并将修改属性后的消息事件发布；

[0071] 或者，

[0072] 所述第一处理节点丢弃获取的消息事件；

[0073] 或者，

[0074] 所述第一处理节点将获取的消息事件存储在数据库中；

[0075] 或者，

[0076] 所述第一处理节点根据获取的消息事件进行流量统计分析或安全统计分析；

[0077] 或者，

[0078] 所述第一处理节点根据获取的消息事件进行关联分析；

[0079] 或者，

[0080] 所述第一处理节点转发获取的消息事件。

[0081] 可选的，所述消息事件为 MAP 消息类型的消息事件；

[0082] 所述消息事件的格式为动态扩展的键 - 值 key-value 格式；

[0083] 和 / 或，

[0084] 所述消息事件的属性包括：所述消息事件的源 IP、目的 IP、源端口号和目的端口号。

[0085] 第四方面，本发明还提供了一种消息订阅方法，包括：

[0086] 消息总线加载插件形式的至少一个第一处理节点，并生成该第一处理节点的第一配置信息；

[0087] 在事件源通过所述消息总线发布消息事件时，所述消息总线根据所述第一配置信息查找与所述第一配置信息对应的消息事件，将查找的消息事件发送所述第一处理节点，以使所述第一处理节点处理发送的消息事件。

[0088] 可选的，所述方法还包括：

[0089] 所述消息总线删除加载的至少一个第一处理节点。

[0090] 可选的，所述消息事件为 MAP 消息类型的消息事件；

[0091] 所述消息事件的格式为动态扩展的键 - 值 key-value 格式；

[0092] 和 / 或，

[0093] 所述消息事件的属性包括：所述消息事件的源 IP、目的 IP、源端口号和目的端口号。

[0094] 可选的，所述事件源包括下述的一种或多种：

[0095] 服务器中的主机事件源、互联网中的网络事件源、和第一处理节点中的事件源、通过所述消息总线发布消息事件的任一接入系统。

[0096] 可选的，所述第一配置信息包括下述的一种或多种：

[0097] 在所述消息总线中订阅符合预设规则的消息事件、删除符合预设规则的消息事件、添加符合预设规则的消息事件的属性、发布消息事件、丢弃符合预设规则的消息事件、转发符合预设规则的消息事件、实名制映射符合预设规则的消息事件、关联分析符合预设规则的消息事件、存储符合预设规则的消息事件。

[0098] 由上述技术方案可知，本发明的消息订阅方法、处理节点设备和总线设备，通过动态加载在消息总线上的至少一个第一处理节点获取消息总线中的消息事件，并处理获取的消息事件，进而可实现对消息总线中输入 / 输出的消息事件进行动态扩展，方便以消息事

件为粒度的网络安全产品进行后期维护，提高网络安全产品的效率。

附图说明

[0099] 图 1 为本发明一实施例提供的消息订阅方法的流程示意图；

[0100] 图 2 为本发明另一实施例提供的消息订阅方法的示意图；

[0101] 图 3 为本发明另一实施例提供的消息订阅方法的示意图；

[0102] 图 4 为本发明另一实施例提供的消息订阅方法的流程示意图；

[0103] 图 5 为本发明另一实施例提供的消息订阅方法的示意图；

[0104] 图 6 为本发明另一实施例提供的消息订阅方法的流程示意图；

[0105] 图 7 为本发明一实施例提供的处理节点的结构示意图；

[0106] 图 8 为本发明一实施例提供的总线的结构示意图。

具体实施方式

[0107] 下面结合附图和实施例，对本发明的具体实施方式作进一步详细描述。以下实施例用于说明本发明，但不用来限制本发明的范围。

[0108] 其中，在本发明的所有实施例中，“/”表示“或者”的关系。

[0109] 图 1 示出了本发明一实施例提供的消息订阅方法的流程示意图，图 2 示出了本发明另一实施例提供的消息订阅方法的示意图，结合图 1 和图 2 所示，本实施例的消息订阅方法如下所述。

[0110] 101、在事件源通过消息总线发布消息事件时，加载在所述消息总线上的至少一个第一处理节点根据第一配置信息在所述消息事件中获取与所述第一配置信息对应的消息事件。

[0111] 其中，所述第一处理节点为采用插件形式动态加载在所述消息总线上的节点。第一配置信息可为消息总线动态加载第一处理节点过程中生成的配置信息，该配置信息用于使第一处理节点按照该配置信息获取消息总线中的消息事件。

[0112] 举例来说，该步骤中的事件源可理解为：服务器中的主机事件源、互联网中的网络事件源、和 / 或，通过所述消息总线发布消息事件的任一接入系统，第三方消息事件源等。

[0113] 本实施例对事件源仅为举例说明，任意能够在消息总线中发布消息事件的均可理解为该消息总线的事件源。

[0114] 102、第一处理节点根据所述第一配置信息处理获取的消息事件。

[0115] 在本实施例中，消息总线可在一服务器的内存中运行，类似一个广播的流，可以广播 / 发布任何消息事件，但不存储该消息事件。该消息总线上可以动态加载多个第一处理节点，如图 2 所示，该第一处理节点可以根据第一配置信息订阅消息总线中广播的消息事件。

[0116] 第一处理节点可以对消息总线中的消息事件进行丢弃、删除消息事件，添加消息属性、存储消息事件等。本实施例不对该第一处理节点进行限定，该第一处理节点可理解为以软件形式实现的插件插入在硬件中实现对消息总线中消息事件的处理。例如，第一处理节点可为订阅插件、消息发布插件等。

[0117] 若第一处理节点向消息总线中发布消息事件，则可认为该第一处理节点为该消息

总线的一个事件源。

[0118] 应说明的是，本实施例中消息总线中的消息事件的格式为键-值格式，即key-value格式。

[0119] 本实施例中的消息订阅方法，通过动态加载在消息总线上的至少一个第一处理节点获取消息总线中的消息事件，并处理获取的消息事件，进而可实现对消息总线中输入/输出的消息事件进行动态扩展，方便以消息事件为粒度的网络安全产品进行后期维护，提高网络安全产品的效率。

[0120] 此外，上述图2中示出的消息总线中消息事件可为MAP类型的消息事件，MAP为移动实体之间传递消息的信令，MAP消息可为包括事务处理能力应用部分(Transaction Capabilities Application Part，简称TCAP)、信令连接控制部分(Signaling Connection Control Part，简称SCCP)、媒体传输协议(Media Transfer Protocol，简称MTP)协议层的协议数据。

[0121] 在图1所示的流程图中，所述方法还包括：多个第一处理节点之间还可以相互订阅消息事件，即，第一处理节点根据所述第一配置信息从另一第一处理节点中订阅或发布的消息事件中获取与所述第一配置信息对应的消息事件。

[0122] 如图3所示，第一处理节点a2根据第一配置信息可从第一处理节点a1中订阅的消息事件中获取与第一配置信息对应的消息事件。

[0123] 举例来说，在图3中，若第一处理节点a1为订阅消息总线中源IP为198.102.151.11的消息事件，并将订阅的消息事件入库。此时，第一处理节点a2可从第一处理节点a1中订阅符合需求的消息事件。由于第一处理节点a1为将订阅的消息事件入库处理，则第一处理节点a2可以订阅第一处理节点a1已经订阅过的所有消息事件。

[0124] 如果第一处理节点a1没有对订阅的源IP为198.102.151.11的消息事件进行入库处理，则第一处理节点a2只能动态实时的订阅第一处理节点a1中订阅的消息事件。即，第一处理节点a2无法订阅所述第一处理节点a1和第一处理节点a2没有建立订阅关系之前第一处理节点a1从消息总线中订阅的消息事件。

[0125] 通常，第一处理节点a1和第一处理节点a2可以构成树型结构，如二叉树结构，本实施例仅为举例说明，不对其进行限定。

[0126] 图4示出了本发明另一实施例提供的消息订阅方法的流程示意图，图5示出了本发明另一实施例提供的消息订阅方法的示意图，结合图4和图5所示，本实施例的消息订阅方法如下所述。

[0127] 401、消息总线动态加载至少一个第一处理节点，生成与该第一处理节点对应的第一配置信息。

[0128] 举例来说，本实施例中的第一配置信息包括下述的一种或多种：

[0129] 在所述消息总线中订阅符合预设规则的消息事件、删除符合预设规则的消息事件、添加符合预设规则的消息事件的属性、发布消息事件、丢弃符合预设规则的消息事件、转发符合预设规则的消息事件、实名制映射符合预设规则的消息事件、关联分析符合预设规则的消息事件、存储符合预设规则的消息事件等等。

[0130] 402、在事件源通过消息总线发布消息事件时，至少一个第一处理节点根据第一配置信息在所述消息事件中获取与所述第一配置信息对应的消息事件。

[0131] 403、第一处理节点根据所述第一配置信息处理获取的消息事件。

[0132] 例如，第一处理节点可根据第一配置信息修改获取的消息事件的属性，并将修改属性后的消息事件发布；或者，第一处理节点可根据第一配置信息丢弃获取的消息事件；或者，第一处理节点可根据第一配置信息将获取的消息事件存储在数据库中；或者，第一处理节点可根据获取的消息事件进行流量统计分析或安全统计分析；或者，第一处理节点根据获取的消息事件进行关联分析（如人名映射）；或者，第一处理节点转发获取的消息事件等等。该处仅为举例说明第一处理节点如何处理获取的消息事件，本实施例不对其进行限定，可根据实际需要进行处理。

[0133] 404、第一处理节点还用于动态加载至少一个第二处理节点，生成与该第二处理节点对应的第二配置信息；

[0134] 所述第二处理节点根据所述第二配置信息从所述第一处理节点订阅或发布的消息事件中获取与所述第二配置信息对应的消息事件，以及处理所获取的消息事件。

[0135] 可理解的是，第 M 处理节点还可动态加载至少一个第 M+1 处理节点，生成与该第 M+1 处理节点对应的第 M+1 配置信息；

[0136] 该第 M+1 处理节点根据第 M+1 配置信息从第 M 处理节点订阅或发布的消息事件中获取与第 M+1 配置信息对应的消息事件，以处理所获取的消息事件。

[0137] 上述 M 取值可为正整数。

[0138] 也就是说，第 M 处理节点和第 M+1 处理节点可构成树型结构，如二叉树结构；或者，第 M 处理节点和第 M+1 处理节点可构成链式结构，本实施例不对其进行限定，图 5 中示出的是构成二叉树结构的第一处理节点 a2 和第二处理节点 b1、b2。

[0139] 本实施例中，在事件源通过消息总线发布消息事件之前，该消息总线需要动态加载至少一个处理节点，以便该些处理节点能够对获取消息总线中的消息事件。

[0140] 举例来说，处理节点可以是产品准入的插件，或者抓取某一源 IP 流量的插件，或者是入侵检查系统分析的插件等。该些插件可以是通过软件实现的，预先加载的一服务器的消息总线中。该消息总线可以把统一格式的消息事件发布，以供加载在消息总线上的多个插件订阅。

[0141] 消息总线上插件的订阅或者插件与插件之间的订阅与该消息总线所在的服务器 / 主机没有关联，且和服务器 / 主机所在的网络也是无关联的。

[0142] 可理解的是，上述任一实施例中，消息总线中的任一消息事件的属性均可包括该消息事件的源 IP、目的 IP、源端口和目的端口等信息。

[0143] 上述实施例中的消息事件的消息格式可动态扩展，进而针对该消息格式而建立的一套基于发布订阅模式的消息总线，消息总线上的订阅插件或发布插件以动态加载的方式挂到消息总线上，以达到可插拔消息总线模式。

[0144] 发布插件通过消息总线发布消息事件，消息总线上动态加载的各种订阅插件，对发布插件发出的消息事件进行处理，例如，删除、添加消息属性发布，丢弃等。

[0145] 本发明实施例中基于上述的消息总线可构建常用的网络安全系统，例如日志服务器、安全审计系统、流量统计系统等。

[0146] 图 6 示出了本发明另一实施例提供的消息订阅方法的流程示意图，如图 6 所示，本实施例的消息订阅方法如下所述。

[0147] 601、消息总线动态加载插件形式的至少一个第一处理节点，并生成该第一处理节点的第一配置信息。

[0148] 举例来说，第一配置信息可包括下述的一种或多种：在所述消息总线中订阅符合预设规则的消息事件、删除符合预设规则的消息事件、添加符合预设规则的消息事件的属性、发布消息事件、丢弃符合预设规则的消息事件、转发符合预设规则的消息事件、实名制映射符合预设规则的消息事件、关联分析符合预设规则的消息事件、存储符合预设规则的消息事件等等。

[0149] 602、在事件源通过所述消息总线发布消息事件时，所述消息总线根据所述第一配置信息查找与所述第一配置信息对应的消息事件，将查找的消息事件发送所述第一处理节点，以使所述第一处理节点处理发送的消息事件。

[0150] 举例来说，本实施例中所述消息事件为 MAP 消息类型的消息事件；

[0151] 所述消息事件的格式为动态扩展的键 - 值格式 (key-value)；消息事件的属性可包括：所述消息事件的源 IP、目的 IP、源端口号和目的端口号。

[0152] 步骤 602 中的事件源可为下述的一种或多种：服务器中的主机事件源、互联网中的网络事件源、和第一处理节点中的事件源、第三方事件源、通过所述消息总线发布消息事件的任一接入系统等。

[0153] 可选地，在具体应用中，上述图 6 所示的方法还可包括下述图中未示出的步骤 603：

[0154] 603、删除加载的至少一个第一处理节点。

[0155] 本实施例的消息订阅方法，消息总线动态加载至少一个第一处理节点，进而向至少一个第一处理节点发送该第一处理节点订阅的消息总线中的消息事件，以使至少一个第一处理节点处理获取的消息事件，进而可实现对消息总线中输入 / 输出的消息事件进行动态扩展，方便以消息事件为粒度的网络安全产品进行后期维护，提高网络安全产品的效率。

[0156] 上述任一实施例中的消息总线 ftms 可以理解为一个主机的 stml，消息总线广播有定义统一类型的消息事件，消息总线上可以定义很多插件即处理节点，每个插件可以对消息事件进行添加、删除、或修改。该消息总线类似于物理总线，在该消息总线上广播的消息事件不被存储，后加载在该消息总线上的处理节点是无法获知处理节点加载之前的消息总线中广播的内容。

[0157] 本实施例的消息总线中加载有多个处理节点，具体应用中，该些处理节点可为采用插件形式加载在消息总线上。

[0158] 图 7 示出了本发明实施例提供的一种处理节点设备的结构示意图，如图 7 所示，该处理节点设备包括：第一获取模块 71 和处理模块 72。

[0159] 第一获取模块 71 用于在事件源通过所述消息总线发布消息事件时，根据第一配置信息在所述消息事件中获取与所述第一配置信息对应的消息事件；

[0160] 处理模块 72 用于根据所述第一配置信息处理获取的消息事件。

[0161] 可选地，所述处理节点设备还包括图中未示出的加载模块；该加载模块，用于加载至少一个第二处理节点，生成与该第二处理节点对应的第二配置信息；

[0162] 所述第二处理节点根据所述第二配置信息从所述处理节点订阅或发布的消息事件中获取与所述第二配置信息对应的消息事件，以及处理获取的消息事件。

[0163] 举例来说，所述第一配置信息包括下述的一种或多种：

[0164] 在所述消息总线中订阅符合预设规则的消息事件、删除符合预设规则的消息事件、添加符合预设规则的消息事件的属性、发布消息事件、丢弃符合预设规则的消息事件、转发符合预设规则的消息事件、实名制映射符合预设规则的消息事件、关联分析符合预设规则的消息事件、存储符合预设规则的消息事件。

[0165] 在本实施例中，所述至少一个处理节点和所述至少一个第二处理节点组成二叉树结构；

[0166] 或者，

[0167] 所述至少一个处理节点和所述至少一个第二处理节点组成链式结构。

[0168] 在另一可能的实现方式中，所述处理节点设备还可包括图中未示出的第二获取模块，该第二获取模块，用于根据所述第一配置信息从另一处理节点中订阅或发布的消息事件中获取与所述第一配置信息对应的消息事件。

[0169] 本实施例中的事件源可包括下述的一种或多种：

[0170] 服务器中的主机事件源、互联网中的网络事件源和第一处理节点中的事件源、通过所述消息总线发布消息事件的任一接入系统。

[0171] 可理解的是，本实施例中的处理模块可具体用于：修改获取的消息事件的属性，并将修改属性后的消息事件发布；或者，丢弃获取的消息事件；或者，将获取的消息事件存储在数据库中；或者，根据获取的消息事件进行流量统计分析或安全统计分析；或者，根据获取的消息事件进行关联分析；或者，转发获取的消息事件。

[0172] 上述任一实施例中的消息事件可为 MAP 消息类型的消息事件；

[0173] 所述消息事件的格式为动态扩展的键－值 key-value 格式；

[0174] 和／或，所述消息事件的属性包括：所述消息事件的源 IP、目的 IP、源端口号和目的端口号。

[0175] 本实施例的处理节点处理获取的消息事件，进而可实现对消息总线中输入／输出的消息事件进行动态扩展，方便以消息事件为粒度的网络安全产品进行后期维护，提高网络安全产品的效率。

[0176] 图 8 示出了本发明实施例提供的一种总线设备的结构示意图，如图 8 所示，该总线设备包括：加载模块 81、生成模块 82、查找模块 83 和发送模块 84；

[0177] 加载模块 81 用于加载插件形式的至少一个第一处理节点；

[0178] 生成模块 82 用于根据所述加载模块加载的至少一个第一处理节点，生成该第一处理节点的第一配置信息；

[0179] 查找模块 83 用于在事件源通过所述消息总线发布消息事件时，根据所述第一配置信息查找与所述第一配置信息对应的消息事件；

[0180] 发送模块 84 用于将查找的消息事件发送所述第一处理节点，以使所述第一处理节点处理发送的消息事件。

[0181] 可选地，所述消息总线还可包括图中未示出的删除模块，该删除模块 84 用于删除加载的至少一个第一处理节点。

[0182] 举例来说，所述消息事件为 MAP 消息类型的消息事件；

[0183] 所述消息事件的格式为动态扩展的键－值 key-value 格式；和／或，所述消息事件

的属性包括：所述消息事件的源 IP、目的 IP、源端口号和目的端口号。

[0184] 本实施例中，事件源可包括下述的一种或多种：

[0185] 服务器中的主机事件源、互联网中的网络事件源、和第一处理节点中的事件源、通过所述消息总线发布消息事件的任一接入系统。

[0186] 所述第一配置信息包括下述的一种或多种：在所述消息总线中订阅符合预设规则的消息事件、删除符合预设规则的消息事件、添加符合预设规则的消息事件的属性、发布消息事件、丢弃符合预设规则的消息事件、转发符合预设规则的消息事件、实名制映射符合预设规则的消息事件、关联分析符合预设规则的消息事件、存储符合预设规则的消息事件。

[0187] 本实施例中的总线可实现对输入 / 输出的消息事件进行动态扩展，方便以消息事件为粒度的网络安全产品进行后期维护，提高网络安全产品的效率。

[0188] 本发明的实施例公开了：

[0189] A1、一种处理节点设备，所述处理节点为采用插件形式加载在消息总线上，所述处理节点包括：

[0190] 第一获取模块，用于在事件源通过所述消息总线发布消息事件时，根据第一配置信息在所述消息事件中获取与所述第一配置信息对应的消息事件；

[0191] 处理模块，用于根据所述第一配置信息处理获取的消息事件。

[0192] A2、根据 A1 所述的处理节点设备，所述处理节点设备还包括：

[0193] 加载模块，用于加载至少一个第二处理节点，生成与该第二处理节点对应的第二配置信息；

[0194] 所述第二处理节点根据所述第二配置信息从所述处理节点订阅或发布的消息事件中获取与所述第二配置信息对应的消息事件，以及处理获取的消息事件。

[0195] A3、根据 A2 所述的处理节点设备，所述至少一个处理节点和所述至少一个第二处理节点组成二叉树结构；

[0196] 或者，

[0197] 所述至少一个处理节点和所述至少一个第二处理节点组成链式结构。

[0198] A4、根据 A1 至 A3 任一所述的处理节点设备，所述处理节点设备还包括：

[0199] 第二获取模块，用于根据所述第一配置信息从另一处理节点中订阅或发布的消息事件中获取与所述第一配置信息对应的消息事件。

[0200] A5、根据 A1 至 A3 任一所述的处理节点设备，所述事件源包括下述的一种或多种：

[0201] 服务器中的主机事件源、互联网中的网络事件源和第一处理节点中的事件源、通过所述消息总线发布消息事件的任一接入系统。

[0202] A6、根据 A1 至 A5 任一所述的处理节点设备，所述第一配置信息包括下述的一种或多种：

[0203] 在所述消息总线中订阅符合预设规则的消息事件、删除符合预设规则的消息事件、添加符合预设规则的消息事件的属性、发布消息事件、丢弃符合预设规则的消息事件、转发符合预设规则的消息事件、实名制映射符合预设规则的消息事件、关联分析符合预设规则的消息事件、存储符合预设规则的消息事件。

[0204] A7、根据 A1 至 6A 任一所述的处理节点设备，所述处理模块，具体用于：

[0205] 修改获取的消息事件的属性，并将修改属性后的消息事件发布；

[0206] 或者，

[0207] 丢弃获取的消息事件；

[0208] 或者，

[0209] 将获取的消息事件存储在数据库中；

[0210] 或者，

[0211] 根据获取的消息事件进行流量统计分析或安全统计分析；

[0212] 或者，

[0213] 根据获取的消息事件进行关联分析；

[0214] 或者，

[0215] 转发获取的消息事件。

[0216] A8、根据 A1 至 A7 任一所述的处理节点设备，所述消息事件为 MAP 消息类型的消息事件；

[0217] 所述消息事件的格式为动态扩展的键 - 值 key-value 格式；

[0218] 和 / 或，

[0219] 所述消息事件的属性包括：所述消息事件的源 IP、目的 IP、源端口号和目的端口号。

[0220] B9、一种总线设备，包括：

[0221] 加载模块，用于加载插件形式的至少一个第一处理节点；

[0222] 生成模块，用于根据所述加载模块加载的至少一个第一处理节点，生成该第一处理节点的第一配置信息；

[0223] 查找模块，用于在事件源通过所述消息总线发布消息事件时，根据所述第一配置信息查找与所述第一配置信息对应的消息事件；

[0224] 发送模块，用于将查找的消息事件发送所述第一处理节点，以使所述第一处理节点处理发送的消息事件。

[0225] B10、根据 B9 所述的总线设备，所述消息总线设备还包括：

[0226] 删除模块，用于删除加载的至少一个第一处理节点。

[0227] B11、根据 B9 或 B10 所述的总线设备，所述消息事件为 MAP 消息类型的消息事件；

[0228] 所述消息事件的格式为动态扩展的键 - 值 key-value 格式；

[0229] 和 / 或，

[0230] 所述消息事件的属性包括：所述消息事件的源 IP、目的 IP、源端口号和目的端口号。

[0231] B12、根据 B9 至 B11 任一所述的总线设备，所述事件源包括下述的一种或多种：

[0232] 服务器中的主机事件源、互联网中的网络事件源、和第一处理节点中的事件源、通过所述消息总线发布消息事件的任一接入系统。

[0233] B13、根据 B9 至 B12 任一所述的总线设备，

[0234] 所述第一配置信息包括下述的一种或多种：

[0235] 在所述消息总线中订阅符合预设规则的消息事件、删除符合预设规则的消息事件、添加符合预设规则的消息事件的属性、发布消息事件、丢弃符合预设规则的消息事件、转发符合预设规则的消息事件、实名制映射符合预设规则的消息事件、关联分析符合预设

规则的消息事件、存储符合预设规则的消息事件。

[0236] C14、一种消息订阅方法，包括：

[0237] 在事件源通过消息总线发布消息事件时，加载在所述消息总线上的至少一个第一处理节点根据第一配置信息在所述消息事件中获取与所述第一配置信息对应的消息事件；

[0238] 所述第一处理节点根据所述第一配置信息处理获取的消息事件；

[0239] 其中，所述第一处理节点为采用插件形式加载在所述消息总线上的节点。

[0240] C15、根据 C14 所述的方法，所述方法还包括：

[0241] 所述第一处理节点还用于加载至少一个第二处理节点，生成与该第二处理节点对应的第二配置信息；

[0242] 所述第二处理节点根据所述第二配置信息从所述第一处理节点订阅或发布的消息事件中获取与所述第二配置信息对应的消息事件，以及处理获取的消息事件。

[0243] C16、根据 C15 所述的方法，所述至少一个第一处理节点和所述至少一个第二处理节点组成二叉树结构；

[0244] 或者，

[0245] 所述至少一个第一处理节点和所述至少一个第二处理节点组成链式结构。

[0246] C17、根据 C14 至 C16 任一所述的方法，所述方法还包括：

[0247] 所述第一处理节点根据所述第一配置信息从另一第一处理节点中订阅或发布的消息事件中获取与所述第一配置信息对应的消息事件。

[0248] C18、根据 C14 至 C16 任一所述的方法，所述事件源包括下述的一种或多种：

[0249] 服务器中的主机事件源、互联网中的网络事件源和第一处理节点中的事件源、通过所述消息总线发布消息事件的任一接入系统。

[0250] C19、根据 C14 至 C18 任一所述的方法，所述加载在所述消息总线上的至少一个第一处理节点根据第一配置信息在所述消息事件中获取与所述第一配置信息对应的消息事件之前，所述方法还包括：

[0251] 所述消息总线加载至少一个第一处理节点，生成与该第一处理节点对应的第一配置信息；

[0252] 和 / 或，

[0253] 所述第一配置信息包括下述的一种或多种：

[0254] 在所述消息总线中订阅符合预设规则的消息事件、删除符合预设规则的消息事件、添加符合预设规则的消息事件的属性、发布消息事件、丢弃符合预设规则的消息事件、转发符合预设规则的消息事件、实名制映射符合预设规则的消息事件、关联分析符合预设规则的消息事件、存储符合预设规则的消息事件。

[0255] C20、根据 C14 至 C19 任一所述的方法，所述第一处理节点根据所述第一配置信息处理获取的消息事件，包括：

[0256] 所述第一处理节点修改获取的消息事件的属性，并将修改属性后的消息事件发布；

[0257] 或者，

[0258] 所述第一处理节点丢弃获取的消息事件；

[0259] 或者，

[0260] 所述第一处理节点将获取的消息事件存储在数据库中；

[0261] 或者，

[0262] 所述第一处理节点根据获取的消息事件进行流量统计分析或安全统计分析；

[0263] 或者，

[0264] 所述第一处理节点根据获取的消息事件进行关联分析；

[0265] 或者，

[0266] 所述第一处理节点转发获取的消息事件。

[0267] C21、根据 C14 至 C20 任一所述的方法，所述消息事件为 MAP 消息类型的消息事件；

[0268] 所述消息事件的格式为动态扩展的键 - 值 key-value 格式；

[0269] 和 / 或，

[0270] 所述消息事件的属性包括：所述消息事件的源 IP、目的 IP、源端口号和目的端口号。

[0271] D22、一种消息订阅方法，包括：

[0272] 消息总线加载插件形式的至少一个第一处理节点，并生成该第一处理节点的第一配置信息；

[0273] 在事件源通过所述消息总线发布消息事件时，所述消息总线根据所述第一配置信息查找与所述第一配置信息对应的消息事件，将查找的消息事件发送所述第一处理节点，以使所述第一处理节点处理发送的消息事件。

[0274] D23、根据 D22 所述的方法，所述方法还包括：

[0275] 所述消息总线删除加载的至少一个第一处理节点。

[0276] D24、根据 D22 或 D23 所述的方法，所述消息事件为 MAP 消息类型的消息事件；

[0277] 所述消息事件的格式为动态扩展的键 - 值 key-value 格式；

[0278] 和 / 或，

[0279] 所述消息事件的属性包括：所述消息事件的源 IP、目的 IP、源端口号和目的端口号。

[0280] D25、根据 D22 至 D24 任一所述的方法，所述事件源包括下述的一种或多种：

[0281] 服务器中的主机事件源、互联网中的网络事件源、和第一处理节点中的事件源、通过所述消息总线发布消息事件的任一接入系统。

[0282] D26、根据 D22 至 D25 任一所述的方法，所述第一配置信息包括下述的一种或多种：

[0283] 在所述消息总线中订阅符合预设规则的消息事件、删除符合预设规则的消息事件、添加符合预设规则的消息事件的属性、发布消息事件、丢弃符合预设规则的消息事件、转发符合预设规则的消息事件、实名制映射符合预设规则的消息事件、关联分析符合预设规则的消息事件、存储符合预设规则的消息事件。

[0284] 上述处理节点、消息总线可执行前述的方法实施例的流程，本发明不再对上述处理节点和消息总线进行详细的举例说明。

[0285] 本发明的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技

术，以便不模糊对本说明书的理解。

[0286] 类似地，应当理解，为了精简本发明公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释呈反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0287] 本领域技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在于该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和／或过程或者单元中的至少一些是互相排斥之处，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0288] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0289] 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的一种浏览器终端的设备中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0290] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

[0291] 最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征

进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围，其均应涵盖在本发明的权利要求和说明书的范围当中。

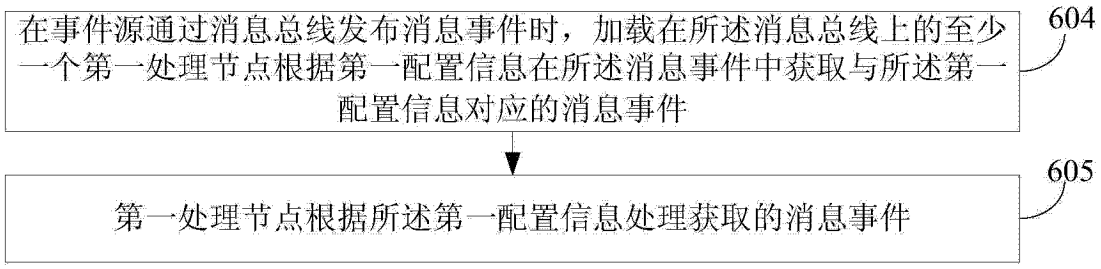

在事件源通过消息总线发布消息事件时，加载在所述消息总线上的至少一个第一处理节点根据第一配置信息在所述消息事件中获取与所述第一配置信息对应的消息事件
604
第一处理节点根据所述第一配置信息处理获取的消息事件
605

图 1

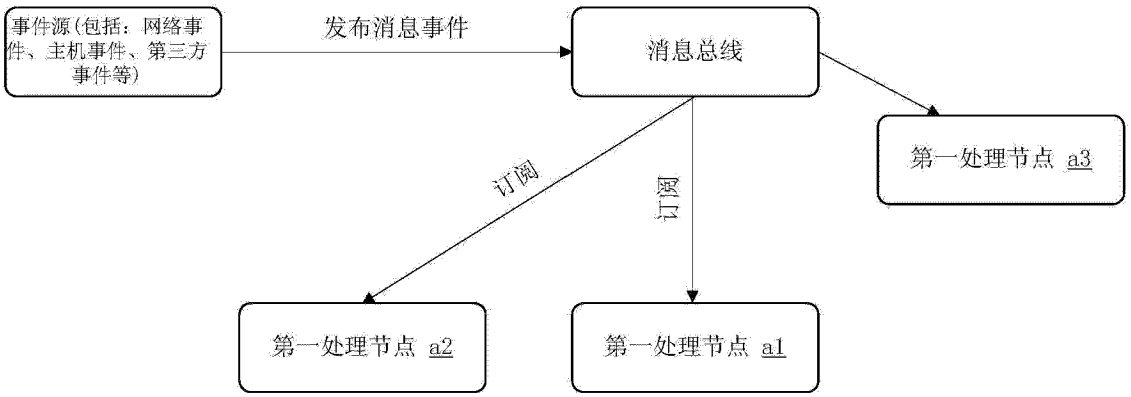

事件源(包括：网络事件、主机事件、第三方事件等)
发布消息事件
消息总线
第一处理节点 a3
订阅
订阅
第一处理节点 a2
第一处理节点 a1

图 2

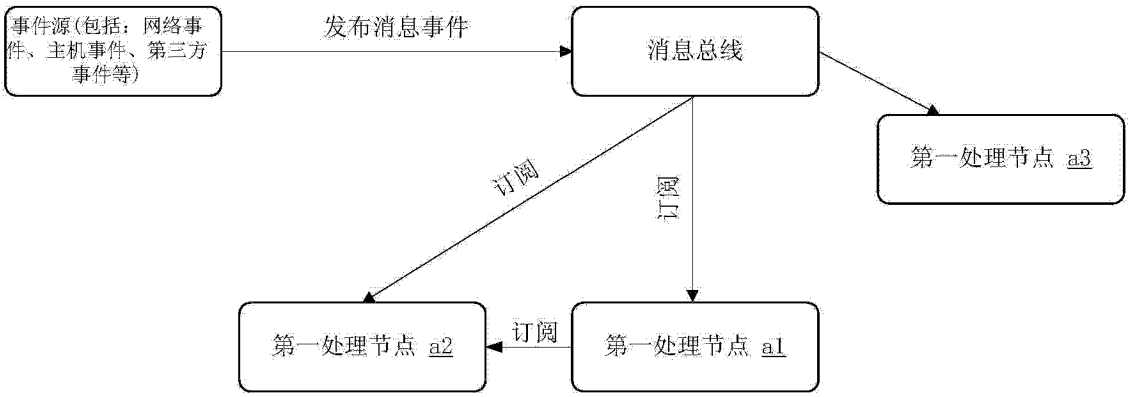

事件源(包括：网络事件、主机事件、第三方事件等)
发布消息事件
消息总线
第一处理节点 a3
订阅
订阅
第一处理节点 a2
订阅
第一处理节点 a1

图 3

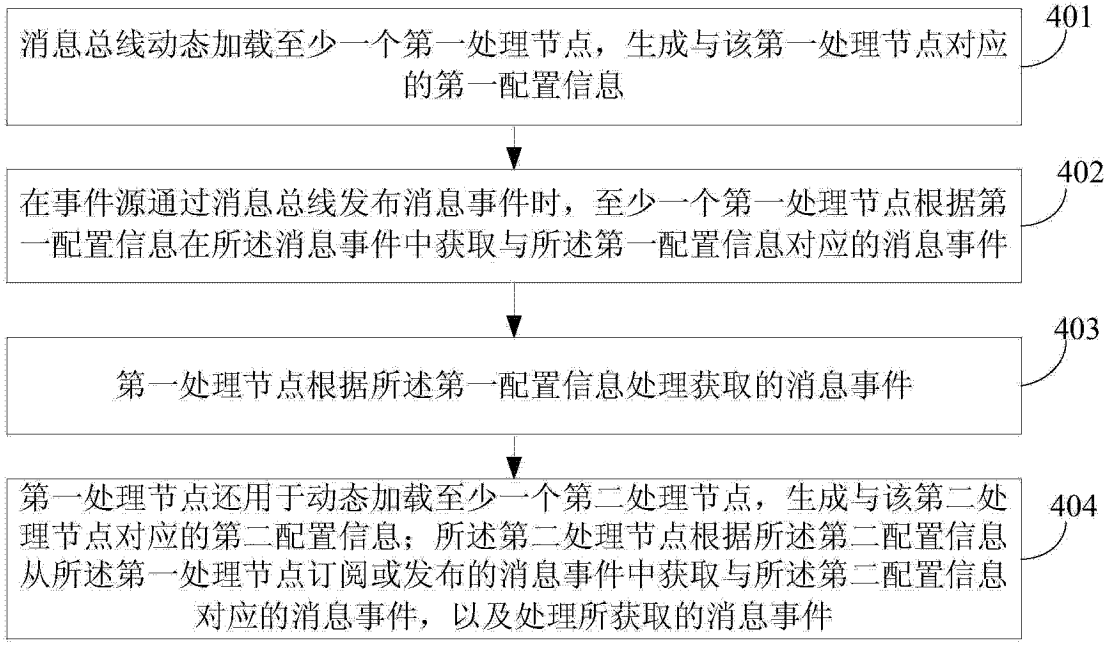

消息总线动态加载至少一个第一处理节点，生成与该第一处理节点对应的第一配置信息
401
在事件源通过消息总线发布消息事件时，至少一个第一处理节点根据第一配置信息在所述消息事件中获取与所述第一配置信息对应的消息事件
402
第一处理节点根据所述第一配置信息处理获取的消息事件
403
第一处理节点还用于动态加载至少一个第二处理节点，生成与该第二处理节点对应的第二配置信息；所述第二处理节点根据所述第二配置信息从所述第一处理节点订阅或发布的消息事件中获取与所述第二配置信息对应的消息事件，以及处理所获取的消息事件
404

图 4

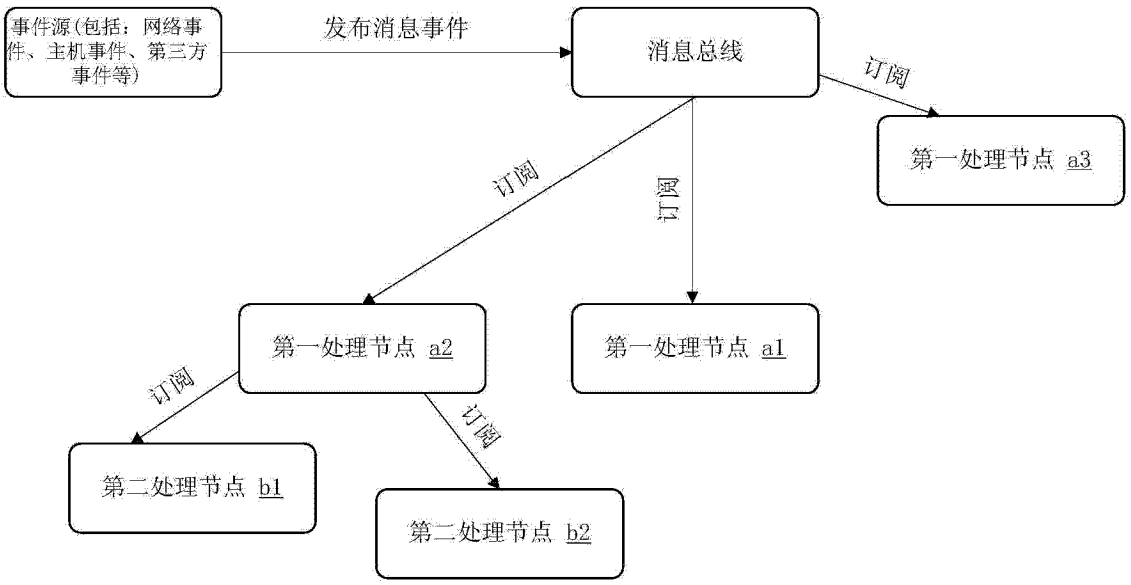

事件源(包括：网络事件、主机事件、第三方事件等)
发布消息事件
消息总线
订阅
第一处理节点 a3
订阅
订阅
第一处理节点 a2
第一处理节点 a1
订阅
订阅
第二处理节点 b1
第二处理节点 b2

图 5

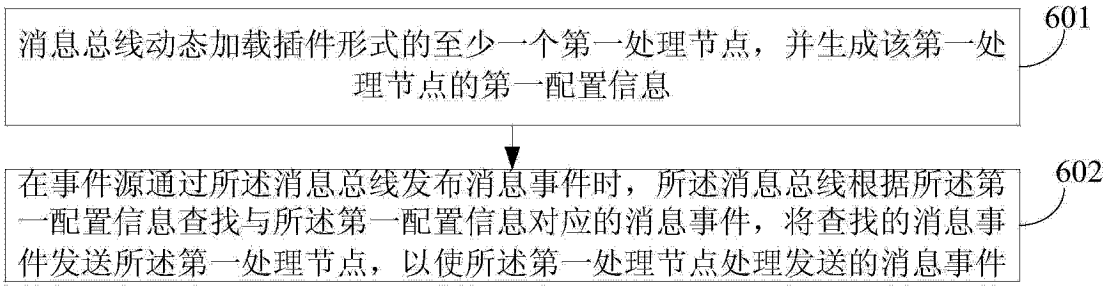

消息总线动态加载插件形式的至少一个第一处理节点，并生成该第一处理节点的第一配置信息
601
在事件源通过所述消息总线发布消息事件时，所述消息总线根据所述第一配置信息查找与所述第一配置信息对应的消息事件，将查找的消息事件发送所述第一处理节点，以使所述第一处理节点处理发送的消息事件
602

图 6

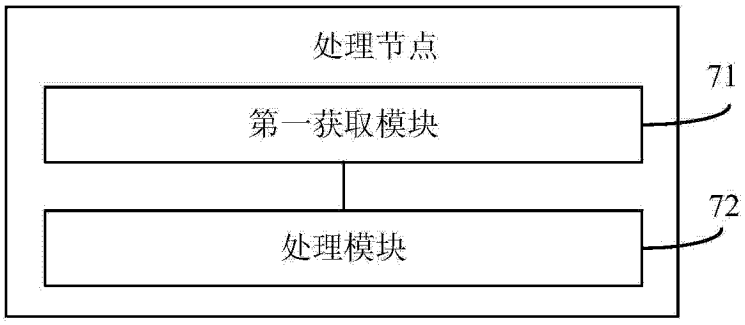

处理节点
第一获取模块
71
处理模块
72

图 7

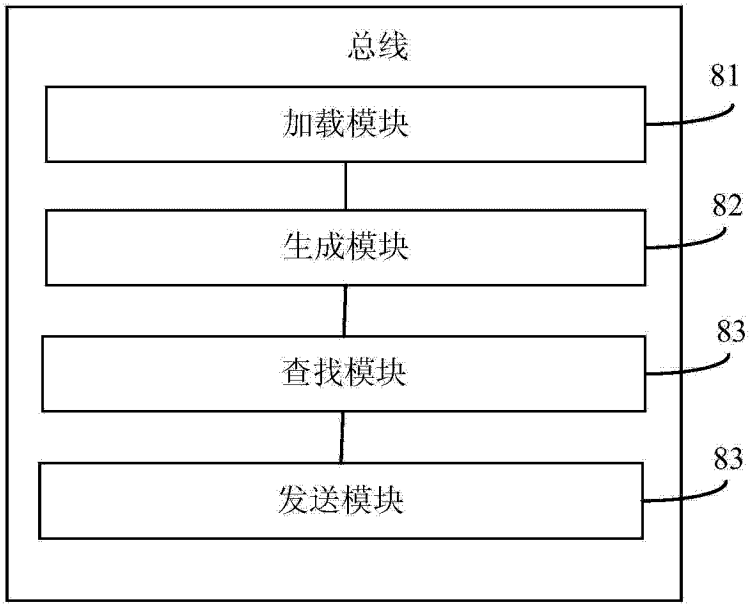

总线
加载模块
81
生成模块
82
查找模块
83
发送模块
83

图 8