[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04W 88/18 (2009.01)

[12] 发明专利申请公布说明书

[21] 申请号 200910170023.6

[43] 公开日 2010 年 1 月 27 日

[11] 公开号 CN 101636000A

[22] 申请日 2009.9.1

[21] 申请号 200910170023.6

[71] 申请人 中兴通讯股份有限公司

地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦法务部

[72] 发明人 江有志

[74] 专利代理机构 信息产业部电子专利中心

代理人 梁 军

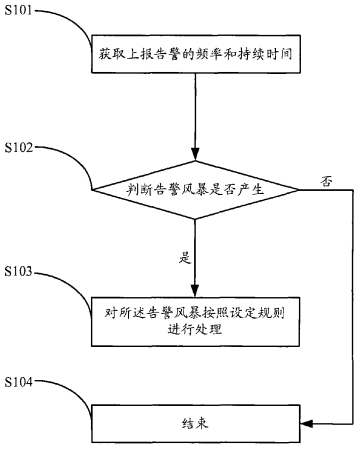
权利要求书 2 页 说明书 10 页 附图 5 页

[54] 发明名称

一种告警风暴的处理方法及处理装置

[57] 摘要

本发明公开了一种告警风暴的处理方法及装置，所述方法包括以下步骤：获取上报告警的频率和持续时间；当所述上报告警的频率和持续时间均大于各自预先设置的阈值时，则判断告警风暴产生，对所述告警风暴按照设定规则进行处理。 所述装置包括：告警处理设置单元、告警信息获取单元、告警风暴判断单元和告警风暴处理单元。 本发明通过根据告警的频率和持续时间来判断告警风暴的产生，可以对已知或未知告警产生的告警风暴进行处理，提高网管系统的灵活性、稳定性和一致性；另外，通过对告警的转存，在告警风暴结束后，再对告警进行恢复处理，避免丢弃某些具有重要意义的告警，也有效减轻了服务器端的负荷。



1、一种告警风暴的处理方法，其特征在于，所述方法包括以下步骤：

获取上报告警的频率和持续时间；

当所述上报告警的频率和持续时间均大于其各自预先设置的阈值时，则判定告警风暴产生，对所述告警风暴按照设定规则进行处理。

2、如权利要求 1 所述的告警风暴的处理方法，其特征在于，所述对告警风暴按照设定规则进行处理的方法包括：将所述上报告警丢弃或转存到文件系统中。

3、如权利要求 2 所述的告警风暴的处理方法，其特征在于，将所述上报告警转存到文件系统中之后，还包括以下步骤：

当所述告警风暴结束后，将转存到文件系统的上报告警从文件系统中恢复成告警对象，并插入到历史告警库中。

4、如权利要求 1~3 任一项所述的告警风暴的处理方法，其特征在于，在对所述告警风暴进行处理的同时，还包括：

产生一条告警风暴告警，用于提示用户告警风暴的发生；所述告警风暴告警包含的信息包括：引起告警风暴的告警名称、频率和持续时间。

5、一种告警风暴的处理装置，其特征在于，所述装置包括：

告警信息获取单元，用于获取上报告警的频率和持续时间；

告警风暴判断单元，用于根据所述告警信息获取单元获取的上报告警的频率和持续时间，判断告警风暴是否产生；

告警风暴处理单元，用于当告警风暴产生后，对所述告警风暴按照设定规则进行处理。

6、如权利要求 5 所述的告警风暴的处理装置，其特征在于，所述告警风暴处理单元包括：

告警丢弃子单元，用于丢弃产生告警风暴的上报告警；

告警转存子单元，用于将产生告警风暴的上报告警转存到文件系统中。

7、如权利要求 6 所述的告警风暴的处理装置，其特征在于，所述告警风暴处理单元还包括:

告警恢复子单元，用于当所述告警风暴结束后，将转存到文件系统的上报告警从文件系统中恢复成告警对象，并插入到历史告警库中。

8、如权利要求 7 所述的告警风暴的处理装置，其特征在于，所述处理装置还包括:

告警恢复设置单元，用于设置将转存到文件系统的上报告警从文件系统中恢复时，恢复其中一部分或全部。

9、如权利要求 5~8 任一项所述的告警风暴的处理装置，其特征在于，所述告警信息获取单元包括:

计数器，用于记录所述上报告警的数目以及上报告警的发生时间;

告警风暴处理器，用于接收所述上报告警，并更新所述计数器。

10、如权利要求 5 所述的告警风暴的处理装置，其特征在于，所述处理装置还包括:

告警处理设置单元，用于设置上报告警的频率阈值和持续时间阈值，以及设置对告警风暴按照设定规则进行处理的方法。

一种告警风暴的处理方法及处理装置

技术领域

本发明涉及移动通讯领域，特别是涉及网管系统中对于告警风暴的处理方法及处理装置。

背景技术

告警管理作为 TMN（Telecommunications Management Network Model，电信管理网）体系结构提供的重要管理功能之一，其稳定性直接影响到整个网管系统的稳定。对告警管理模块的稳定性与处理效率影响最大的莫过于告警风暴。当告警风暴来到时，其会大量消耗系统资源，导致网管系统反映迟缓甚至崩溃。告警风暴是任何一个网管系统都应该面对的问题，如果没有有效的处理方法，告警风暴会带来无可挽回的损失。

当前的网管系统中，对于告警风暴的处理方法主要是采用用户定制告警制规则的方式来抑制某种类型的告警，使指定类型的告警上报到网管后直接被抛弃，或者只保存到数据库，而并不显示到客户端。

上述方法存在以下缺陷：只能对依靠经验事先已知可能造成告警风暴的告警进行屏蔽，对于未知类型的告警，无处理能力。当未知类型的告警风暴来临时，系统已经来不及做出反应，导致网管系统反映迟缓甚至崩溃。另外，屏蔽告警风暴的时候，如果采取告警风暴期间所有告警直接丢弃的方式，那么可能丢弃某些具有重要意义的告警，进而影响到系统的使用。如果采用将告警保存到数据库，只是不显示到客户端的方式，那么服务器端仍然需要做处理，不能有效减轻服务器端的负荷。

发明内容

本发明要解决的技术问题是提供一种能够对告警风暴进行自适应处理，不会丢失关键数据，且能够提高网管系统的灵活性、稳定性和一致性的告警风暴的处理方法及处理装置，用以解决现有技术不能对未知类型的告警风暴处理，或不能有效减轻服务器端的负荷，以及可能丢弃某些具有重要意义的告警的问题。

为解决上述技术问题，一方面，本发明提供一种告警风暴的处理方法，所述方法包括以下步骤：

获取上报告警的频率和持续时间；

当所述上报告警的频率和持续时间均大于其各自预先设置的阈值时，则判定告警风暴产生，对所述告警风暴按照设定规则进行处理。

进一步，所述对告警风暴进行处理的方法包括：将所述上报告警丢弃或转存到文件系统中。

进一步，将所述上报告警转存到文件系统中之后，还包括以下步骤：

当所述告警风暴结束后，将转存到文件系统的上报告警从文件系统中恢复成告警对象，并插入到历史告警库中。

进一步，在对所述告警风暴进行处理的同时，还包括：

产生一条告警风暴告警，用于提示用户告警风暴的发生；所述告警风暴告警包含的信息包括：引起告警风暴的告警名称、频率和持续时间。

另一方面，本发明还提供一种告警风暴的处理装置，所述装置包括：

告警信息获取单元，用于获取上报告警的频率和持续时间；

告警风暴判断单元，用于根据所述告警信息获取单元获取的上报告警的频率和持续时间，判断告警风暴是否产生；

告警风暴处理单元，用于当告警风暴产生后，对所述告警风暴按照设定规则进行处理。

进一步，所述告警风暴处理单元包括：

告警丢弃子单元，用于丢弃产生告警风暴的上报告警；

告警转存子单元，用于将产生告警风暴的上报告警转存到文件系统中。

进一步，所述告警风暴处理单元还包括：

告警恢复子单元，用于当所述告警风暴结束后，将转存到文件系统的上报告警从文件系统中恢复成告警对象，并插入到历史告警库中。

进一步，所述处理装置还包括：

告警恢复设置单元，用于设置将转存到文件系统的上报告警从文件系统中恢复时，恢复其中一部分或全部。

进一步，所述告警信息获取单元包括：

计数器，用于记录所述上报告警的数目以及上报告警的发生时间；

告警风暴处理器，用于接收所述上报告警，并更新所述计数器。

进一步，所述处理装置还包括：

告警处理设置单元，用于设置所述上报告警的频率阈值和持续时间阈值，以及设置对告警风暴按照设定规则进行处理的方法。

本发明有益效果如下：

通过根据告警的频率和持续时间来判断告警风暴的产生，可以对已知或未知告警产生的告警风暴进行处理，提高网管系统的灵活性、稳定性和一致性；另外，通过对告警的转存，在告警风暴结束后，再对告警进行恢复处理，避免丢弃某些具有重要意义的告警，也有效减轻了服务器端的负荷。

附图说明

图 1 是本发明第一实施例告警风暴处理方法的流程图；

图 2 是本发明第二实施例告警风暴处理方法的流程图；

图 3 是本发明第三实施例告警风暴处理装置的结构示意图；

图 4 是本发明第四实施例告警风暴处理装置的结构示意图；

图 5 是本发明第五实施例告警风暴处理装置的子系统结构图；

图 6 是本发明实施例告警风暴处理方法中告警处理流程图；

图 7 是本发明实施例告警风暴处理方法中后台处理线程流程图。

具体实施方式

为了解决现有技术对告警风暴处理不恰当的问题，本发明提供了一种告警风暴的处理方法及处理装置，以下结合附图以及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不限定本发明。

告警风暴的特征就是告警在短时间内大量地上报，从而大量消耗系统资源导致系统崩溃。如果我们在网管系统接收到告警上报而未真正进行处理之前先进行一个预处理，当发现告警在一段时间内以一个较高的频率上报时，则认为告警风暴发生，对于这些告警进行直接丢弃或者转储到文件系统，则能有效去除垃圾数据，降低网管系统的负载。

本发明的核心思想是根据上报告警的频率以及持续时间来动态的判断告警风暴是否产生。当告警风暴产生时，上报的告警不会再发送到告警模块进行处理，而是直接丢弃或者转储到文件系统中。当转储到文件系统中，待告警风暴过去以后，用户可以自行手动将这些转储到文件系统的告警数据恢复，并转换为历史告警以供用户查看。

图 1 是本发明的实施例 1，本实施例中，对告警风暴的处理方法包括以下步骤：

S101，首先获取上报告警的频率和持续时间。上报告警的频率通过记录告警的个数，以及记录每条告警的发生时间，经过计算获得上报告警的频率；并且记录上报告警的持续时间。

S102，判断告警风暴是否产生。具体步骤如下：将步骤 S101 中获取的上报告警的频率和持续时间，分别与预先设置在系统中的上报告警的频率阈值和上报告警的持续时间阈值进行比较，只有当步骤 S101 中获取的上报告警的频

率和持续时间均大于各自的阈值时，才判定告警风暴产生；两者只有其一超过其设置的阈值，或两者均没有超过其设置的阈值时，则判定没有产生告警风暴。即，假设预先设置在系统中的上报告警的频率阈值为每秒 50 条，上报告警的持续时间阈值为 10 秒，则当步骤 S101 中获取上报告警的频率大于每秒 50 条，且步骤 S101 中获取的上报告警的持续时间大于 10 秒时，则判定告警风暴产生；若步骤 S101 中获取上报告警的频率不大于每秒 50 条，或步骤 S101 中获取的上报告警的持续时间不大于 10 秒时，则判定没有产生告警风暴。当告警风暴产生时，转步骤 S103，否则，转步骤 S104。

S103，对告警风暴按照设定规则进行处理。本步骤中对告警风暴按照设定规则进行处理的处理方法可以为任何对告警风暴处理行之有效的方法，例如，直接丢弃上报告警，或者将告警保存到数据库，或者将上报告警转存到文件系统中。

S104，结束。本步骤的结束是指对本次上报告警的判断、处理过程的结束，并不是所有程序的结束，在结束本次步骤之后，需要对下一时段内的上报告警进行监测，获取下一时段内的上报告警的频率和持续时间，即循环步骤 S101~S104。

通过根据上报告警的频率和持续时间对告警风暴是否产生进行判断，可以准确的判断告警风暴的产生，并且不受告警是否已知或未知的限制，大大提高了系统对告警风暴的处理能力。

图 2 是本发明的实施例 2，本实施例中，对告警风暴的处理方法包括以下步骤：

其中步骤 S201、S202、S205 分别与实施例 1 中的步骤 S101、S102、S104 相同，在此不再详述。当判断告警风暴产生后，包括以下步骤：

S203，将上报告警转存到文件系统中。在将告警对象转储到文件系统的时候，本实施例使用了一个第三方的包 Xstream 来协助处理。Xstream 是一套简单实用的类库，用于序列化对象与 XML（Extentsible Markup Language，可扩

展标记语言）对象之间的相互转换，它具有以下几个特点：灵活易用，无需映射，高速稳定，清晰易懂。本实施例使用 Xstream 来将告警对象转换为 XML 文件并存储到文件系统中，在恢复的时候再由 XML 文件提取告警对象并恢复。

S204，当告警风暴结束后，将转存到文件系统的上报告警从文件系统中恢复成告警对象，并插入到历史告警库中。本步骤中，可以查看在文件系统中存有哪些时段的被转存的告警风暴，选择某个时间段内的告警进行恢复，可以选择恢复一部分或者全部告警，通过解析对应的文件，恢复告警风暴，被恢复的告警会进入历史告警库以备日后察看。

经过测试，直接将告警转储到文件系统耗用的时间，是让告警走完整个网管的处理链所花费的时间的二十分之一，可以大大节省处理的时间和网管的负荷，有利于在告警风暴来时保持系统的稳定。

在实施例 1 步骤 S103 和实施例 2 步骤 S203 进行的同时，还包括以下步骤：

产生一条告警风暴告警，其详细信息包括是何种告警引起了告警风暴，风暴持续时间，频率等信息，提示用户告警风暴的发生。

图 3 是本发明的实施例 3，本实施例中，告警风暴的处理装置包括以下结构：

告警信息获取单元 31，用于获取上报告警的频率和持续时间；

告警风暴判断单元 32，用于根据告警信息获取单元 31 获取的上报告警的频率和持续时间，判断告警风暴是否产生。具体判断方法如下：将告警信息获取单元 31 获取的上报告警的频率和持续时间，分别与预先设置在系统中的上报告警的频率阈值和上报告警的持续时间阈值进行比较，只有当告警信息获取单元 31 获取的上报告警的频率和持续时间均大于各自的阈值时，才判定告警风暴产生；两者只有其一超过其设置的阈值，或两者均没有超过其设置的阈值时，则判定没有产生告警风暴。即，假设预先设置在系统中的上报告警的频率阈值为每秒 60 条，上报告警的持续时间阈值为 8 秒，则当告警信息获取单元 31 获取上报告警的频率大于每秒 60 条，且告警信息获取单元 31 获取的上报告

警的持续时间大于 8 秒时，则判定告警风暴产生；若告警信息获取单元 31 获取上报告警的频率不大于每秒 60 条，或告警信息获取单元 31 获取的上报告警的持续时间不大于 8 秒时，则判定没有产生告警风暴。

告警风暴处理单元 33，用于当告警风暴产生后，对告警风暴按照设定规则进行处理。告警风暴处理单元 33 对告警风暴按照设定规则进行处理的处理方法可以为任何对告警风暴处理行之有效的方法，例如，直接丢弃上报告警，或者将告警保存到数据库，或者将上报告警转存到文件系统中。

图 4 是本发明的实施例 4，本实施例中，告警风暴的处理装置包括以下结构：

告警信息获取单元 41，用于获取上报告警的频率和持续时间；告警信息获取单元 41 进一步包括计数器 411 和告警风暴处理器 412，其中，计数器 411 用于记录上报告警的数目以及上报告警的发生时间；告警风暴处理器 412 用于接收上报告警，并更新所述计数器。

告警风暴判断单元 42，用于根据告警信息获取单元 41 获取的上报告警的频率和持续时间，判断告警风暴是否产生。本实施例中，告警风暴判断单元 42、与实施例 3 中的告警风暴判断单元 32 的结构、功能、作用相同，在此不再重述。

告警风暴处理单元 43，用于当告警风暴产生后，对告警风暴按照设定规则进行处理。

本实施例的告警风暴的处理装置还包括告警处理设置单元 44 和告警恢复设置单元 45。其中，告警处理设置单元 44 用于设置所述上报告警的频率阈值和持续时间阈值，以及设置对告警风暴进行处理的方法；告警恢复设置单元 45 用于设置将转存到文件系统的上报告警从文件系统中恢复时，恢复其中一部分或全部。

告警风暴处理单元 43 进一步包括告警丢弃子单元 431、告警转存子单元 432 和告警恢复子单元 433。其中，告警风暴处理单元 43 对告警风暴按照设定

规则进行处理具体为：当告警处理设置单元 44 设置了对告警风暴进行处理的方法为丢弃上报告警时，在告警风暴产生后，告警丢弃子单元 431 丢弃产生告警风暴的上报告警；当告警处理设置单元 44 设置了对告警风暴进行处理的方法为将上报告警转存到文件系统中时，在告警风暴产生后，告警转存子单元 432 将产生告警风暴的上报告警转存到文件系统中。当告警恢复设置单元 45 设置了将转存到文件系统的上报告警从文件系统中时，告警恢复子单元 433 在所述告警风暴结束后，将转存到文件系统的上报告警从文件系统中恢复成告警对象，并插入到历史告警库中。

本发明上述实施例的实施，可以通过硬件或软件的方式实施，也可以通过软件、硬件结合的方式实施，下面给出通过软件、硬件结合实施的具体实例（实施例 5）。

如图 5 所示，本实施例所述告警风暴处理装置按照 C/S 结构实现，包括客户端和服务器端。

客户端包含一个告警风暴处理规则设置对话框，提供设置告警风暴处理规则信息的界面，包括以下内容：

1、规则名称，及其描述。

2、子规则属性：这里选择当告警风暴来临时使用哪种子规则来处理上报告警，可以选择的选项有直接丢弃和转储到文件系统中。

3、规则属性：在这里我们选择告警风暴处理规则在什么情况下启动，要设置的有持续时间和频率两项，当告警的上报频率达到某个门限值并持续一段时间后，系统会自动启动告警风暴处理规则，当上报频率或持续时间之一不满足条件时系统自动暂停规则。比如我们可以定义当告警上报达到每秒 50 条并持续 10 秒钟后启动规则。

4、同时有一个“告警风暴恢复”菜单，用户点击后会出现一个“告警风暴恢复”对话框，如果处理告警风暴时选择的是转储到文件系统，这个界面中会显示目前在文件系统中存在哪些时段的被转储的告警风暴，则用户可以在客

户端手工选择某个时间段内的告警进行恢复，被恢复的告警会进入历史告警库以备日后察看，用户可以选择恢复一部分或者全部告警。

服务器端告警风暴处理规则处理包含以下内容

1、告警风暴处理器：接收告警后台送来的告警，并更新记数器。

2、记数器：记录告警的数目以及告警的发生时间。

3、后台处理线程：定时查看记数器，判断告警的频率以及持续时间是否达到门限值，以决定是否激活子处理器。

4、子处理器：被后台处理线程所管理，执行实际的屏蔽告警风暴的任务。

告警风暴管理器包含以下内容：

1、告警风暴管理器：其纪录所有被转储到文件系统的告警风暴，响应客户端的请求返回这些告警的信息，并将其从文件系统恢复成告警对象并插入到历史告警库中。

告警处理流程如下：

后台处理流程主要分为两个，一个是告警风暴处理器对上报告警的处理，一个是后台处理线程的流程，下面分别结合图示进行介绍。

告警风暴处理器对上报告警的处理流程如图 6 所示：

当网管系统收到一条上报的告警后，告警模块将其发送到告警风暴处理器处理。

告警风暴处理器更新记数器。注意这里的不是一个简单的记数器，不但要记录告警的个数，还要记录每条告警的发生时间，以便计算告警的持续时间以及频率。

后台处理线程的流程如图 7 所示：

首先后台处理线程启动，查看告警记数器，计算之前一个时间段内的告警频率，即每秒钟内告警的次数，查看告警频率是否一直高于设定阈值。

如告警频率高于设定阈值，需要判断之前是否有已存在并处于激活状态的子处理器。

如无子处理器，则新建一个子处理器并激活，之后子处理器会进行抑制告警风暴的任务，同时产生一条新的告警风暴告警，其详细信息包括是何种告警引起了告警风暴，风暴持续时间，频率等信息，提示用户告警风暴的发生。

如已有子处理器但是其未处于激活状态，则将其激活，同样需要产生一条新的告警风暴告警。

如已有子处理器且处于激活状态，则需要更新之前产生的告警风暴告警的信息，包括持续时间，频率等。

如果告警频率不是高于门限值，则判断之前是否有已经创建并处于激活状态的子处理器，如有，则暂停该规则处理器并恢复之前产生的告警风暴告警。如无，则不做任何处理。

处理完毕后后台处理线程进入休眠状态，等待一段时间后重复执行以上操作，如等待 1 秒钟。

告警风暴的恢复流程如下:

用户点击客户端“告警风暴恢复”菜单。服务器端告警风暴管理器返回当前系统中被保存在文件系统中的告警风暴信息给客户端。

用户在客户端选择所要恢复的告警风暴，服务器端告警风暴管理器解析对应的文件，恢复告警风暴并将其插入到历史告警库中。

综上所述，通过上述实施例可以看出，本发明通过根据告警的频率和持续时间来判断告警风暴的产生，可以对已知或未知告警产生的告警风暴进行处理，提高网管系统的灵活性、稳定性和一致性；另外，通过对告警的转存，在告警风暴结束后，再对告警进行恢复处理，避免丢弃某些具有重要意义的告警，也有效减轻了服务器端的负荷。

尽管为示例目的，已经公开了本发明的优选实施例，本领域的技术人员将意识到各种改进、增加和取代也是可能的，因此，本发明的范围应当不限于上述实施例。

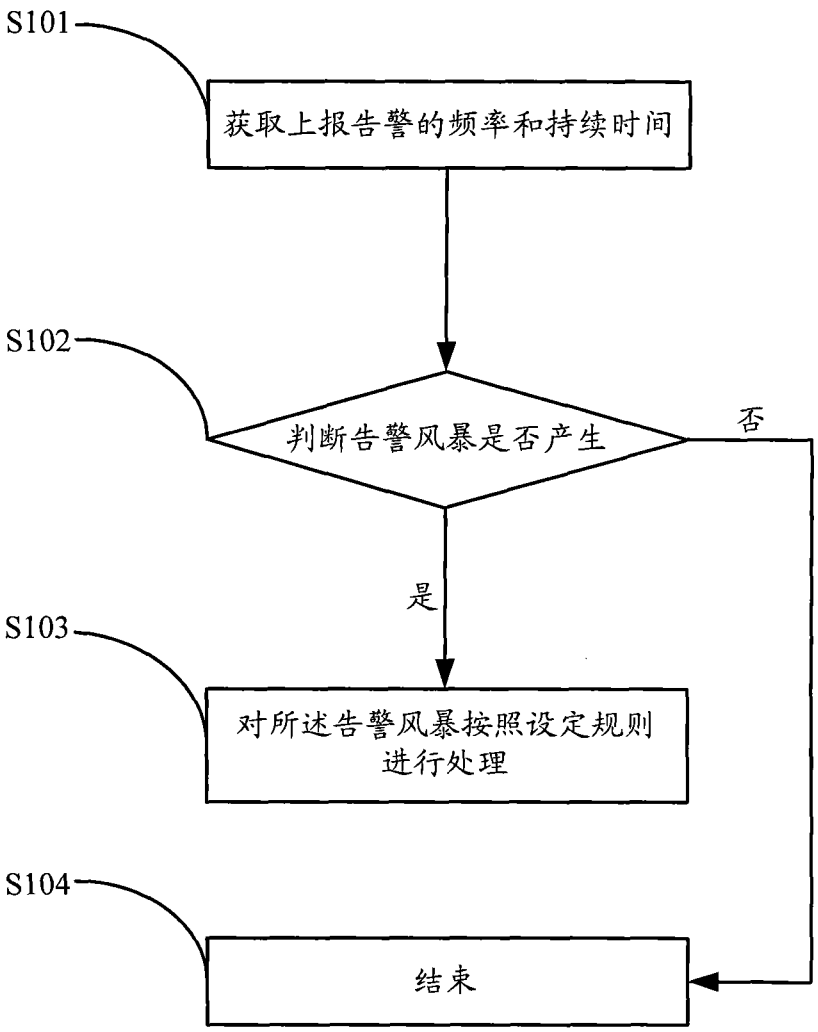

S101
获取上报告警的频率和持续时间
S102
判断告警风暴是否产生
否
是
S103
对所述告警风暴按照设定规则进行处理
S104
结束

图 1

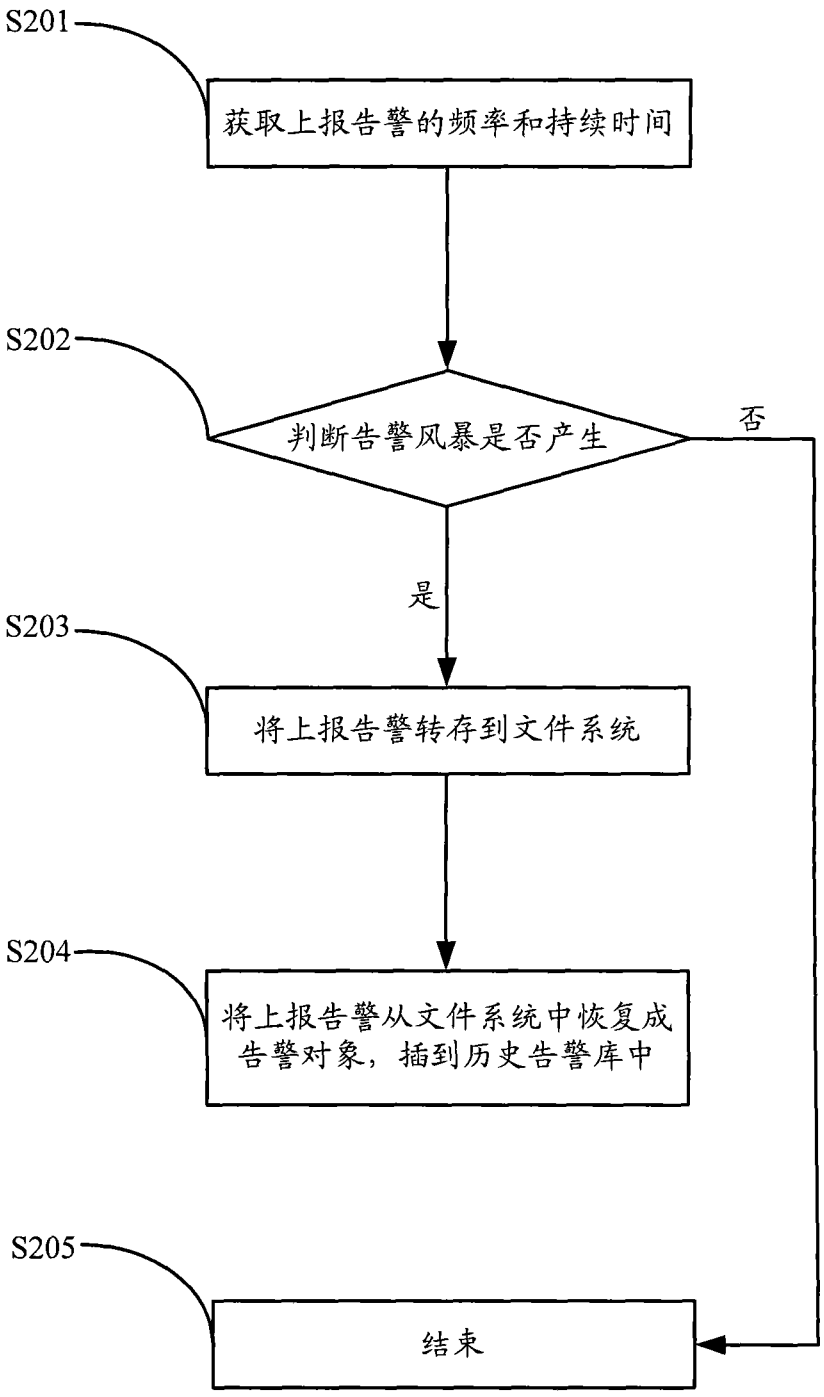

S201
获取上报告警的频率和持续时间
S202
判断告警风暴是否产生
否
是
S203
将上报告警转存到文件系统
S204
将上报告警从文件系统中恢复成告警对象，插到历史告警库中
S205
结束

图 2

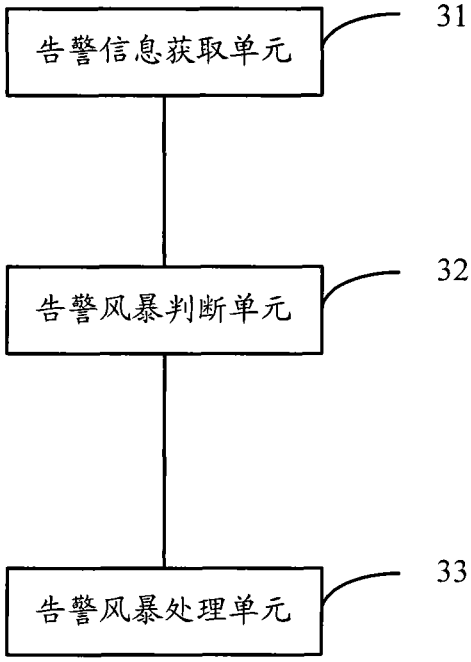

告警信息获取单元
31
告警风暴判断单元
32
告警风暴处理单元
33

图 3

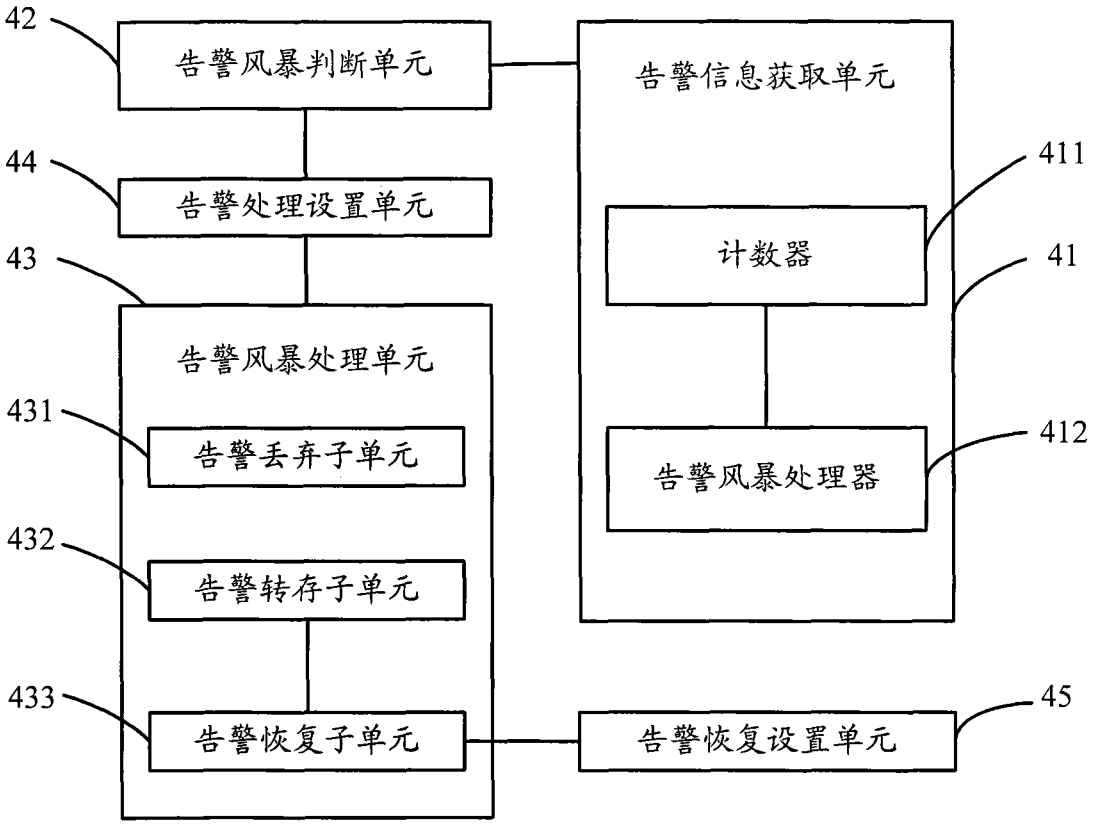

42
告警风暴判断单元
告警信息获取单元
44
告警处理设置单元
411
计数器
43
41
告警风暴处理单元
431
告警丢弃子单元
412
告警风暴处理器
432
告警转存子单元
433
告警恢复子单元
45
告警恢复设置单元

图 4

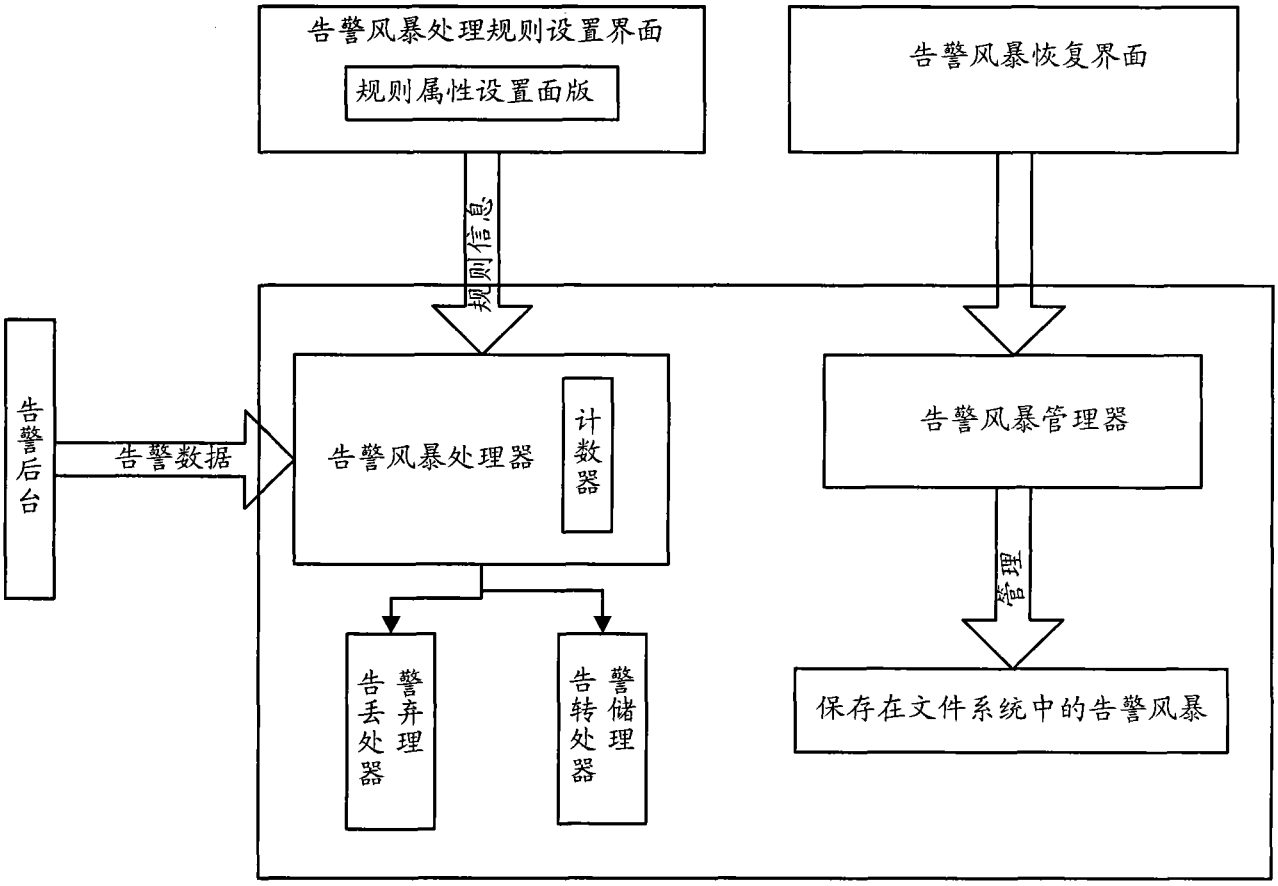

告警风暴处理规则设置界面
规则属性设置面版
告警风暴恢复界面
规则信息
告警后台
告警数据
告警风暴处理器
计数器
告警风暴管理器
告警
告丢处器 警弃理
告转处器 警储理
保存在文件系统中的告警风暴

图 5

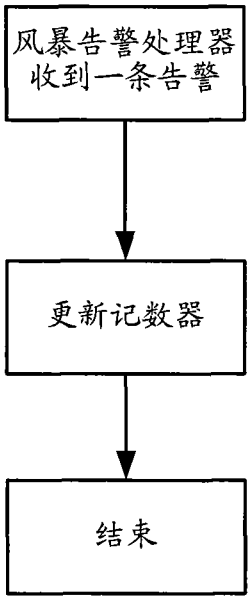

风暴告警处理器收到一条告警
更新记数器
结束

图 6

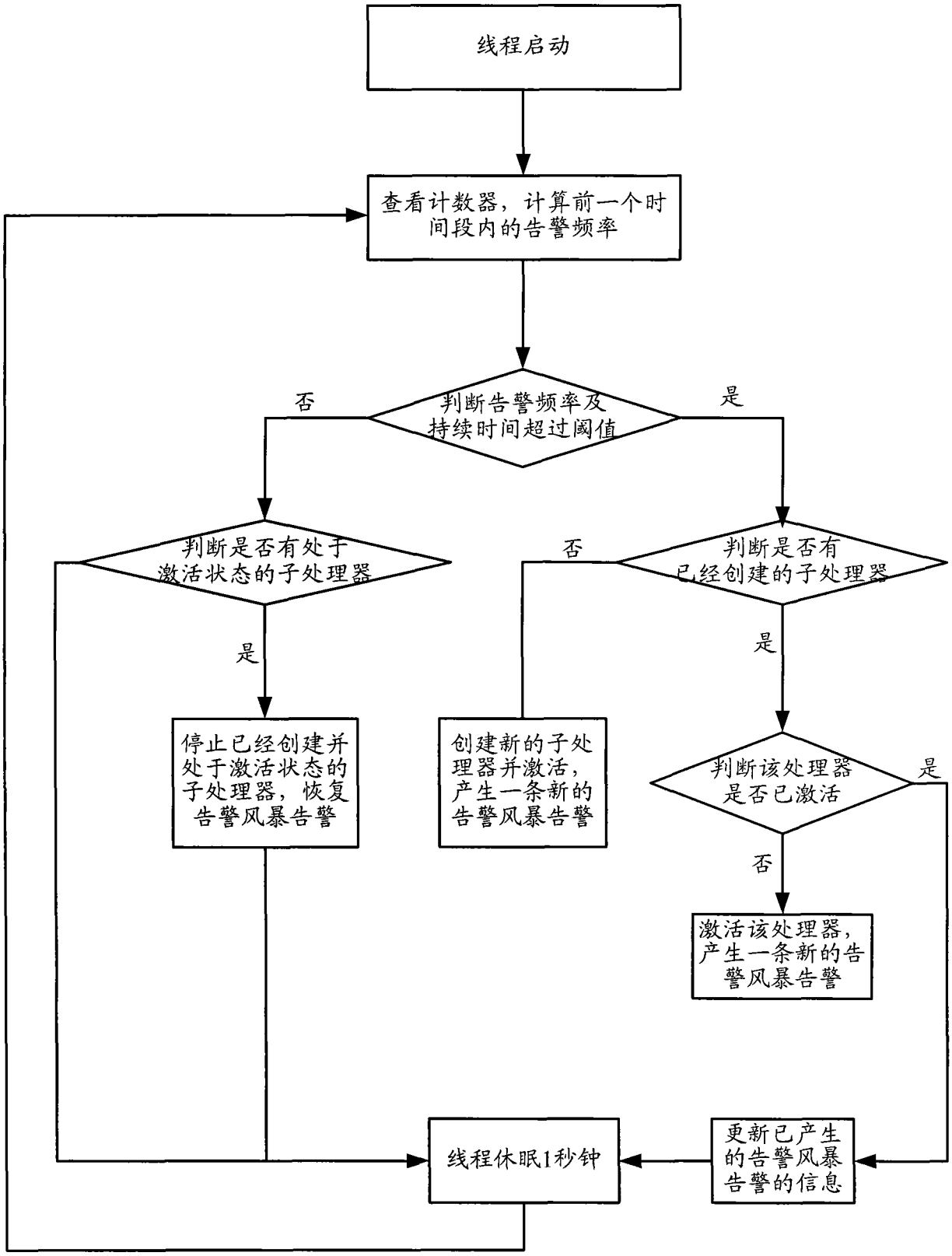

线程启动
查看计数器，计算前一个时间段内的告警频率
判断告警频率及持续时间超过阈值
否
是
判断是否有处于激活状态的子处理器
是
停止已经创建并处于激活状态的子处理器，恢复告警风暴告警
否
判断是否有已经创建的子处理器
是
创建新的子处理器并激活，产生一条新的告警风暴告警
判断该处理器是否已激活
是
否
激活该处理器，产生一条新的告警风暴告警
更新已产生的告警风暴告警的信息
线程休眠1秒钟

图 7