[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/24 (2006.01)
H04L 12/26 (2006.01)
H04L 29/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200910157214.9

[43] 公开日 2009 年 11 月 18 日

[11] 公开号 CN 101582807A

[22] 申请日 2009.7.2

[21] 申请号 200910157214.9

[71] 申请人 北京讯风光通信技术开发有限责任公司

地址 100086 北京市海淀区人民大学南路三义庙大华天坛大厦一层

[72] 发明人 赵文涛 张世瞳 胡军波 孙忠义 段小军

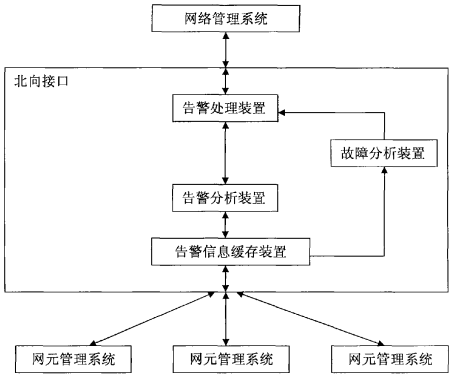
权利要求书 4 页 说明书 13 页 附图 3 页

[54] 发明名称

一种基于北向接口实现网络管理的方法及系统

[57] 摘要

本发明涉及一种基于北向接口实现网络管理的方法及系统，北向接口缓存告警信息，根据网元管理系统的 ID 将所接收的告警信息分组并进行关联分析，将告警信息分为以下类型：过滤告警信息，合并告警信息，压缩告警信息和抑制告警信息，告警分析装置根据告警时间对告警信息进行分析以获得关联告警信息。 故障分析装置根据告警分析装置发送的关联告警信息生成通信设备的依赖关系，告警处理装置根据告警信息类型对告警信息进行相应的处理，根据故障分析装置生成的网络拓扑图中的依赖关系进行告警通知或故障预警。 本发明通过对告警信息的处理降低了北向接口的负载，提高了网络管理系统处理告警信息的效率。



1、一种基于北向接口实现网络管理的系统，所述系统包括：网元管理系统，北向接口和网络管理系统，网元管理系统通过北向接口将告警信息发送给网络管理系统，其特征在于，所述北向接口包括：

告警信息缓存装置，在指定的时间周期内存储网元管理系统上报的告警信息；

告警分析装置，根据网元管理系统 ID 将所接收的告警信息分组，对每组告警信息进行关联分析，将告警信息分为以下类型：过滤告警信息，合并告警信息，压缩告警信息和抑制告警信息；告警分析装置根据告警时间对告警信息进行分析以获得关联告警信息；

故障分析装置，故障分析装置记录多个时间周期的关联告警信息，根据通信设备的基本属性生成虚拟通信设备，基于所述通信设备的路由信息生成网络拓扑图，在网络拓扑图中建立虚拟通信设备的虚拟网络连接，并且根据告警分析装置发送的关联告警信息生成通信设备的依赖关系；

告警处理装置，根据告警信息类型对告警信息进行相应的处理，根据故障分析装置生成的网络拓扑图中的依赖关系进行故障预警。

2、根据权利要求 1 所述的系统，其特征在于，所述告警分析装置对每组告警信息进行关联分析包括：

如果告警信息是缺少网元管理系统 ID，告警设备 ID，告警类型，告警时间，告警级别，告警源地址，告警目的地址，告警源端口号和告警目的端口号中任意一个属性的无效告警信息或告警类型不属于网络管理系统所定义的合法告警类型集合，则将告警信息的类型设置为过滤告警信息；

统计告警设备 ID 和告警类型相同的告警信息，如果上述告警信息的数量小于预定的阈值 K，则将上述告警信息的类型设置为合并告警信息；如果上述告警信息的数量大于等于预定的阈值 K，则将上述告警信息设置为合并告警信息，并将告警类型修改为拒绝服务 DoS（Denial of Service） 攻击；

统计告警设备 ID 相同且告警类型不同的告警信息，将上述告警信息的类型设置为压缩告警信息；

根据告警级别对所有告警信息进行排序，当所有告警信息中告警级别为最高级的告警信息的数量大于其它低级别的告警信息的总数时，则将告警信息的类型设置为抑制告警信息。

3、根据权利要求 1 所述的系统，其特征在于，告警分析装置根据告警时间对告警信息进

行分析以获得关联告警信息包括：

统计告警时间相同的告警信息，将上述告警信息的告警设备 ID 添加到并发集中，在每个指定时间周期内对上述并发集进行更新，确定同时发生告警事件的通信设备。

按照告警时间对告警信息进行排序，将上述告警信息的告警设备 ID 的顺序关系添加到顺序集中，在每个指定时间周期内对上述顺序集进行更新，确定顺序发生告警事件的通信设备。

4、根据权利要求 1 所述的系统，其特征在于，告警分析装置根据告警时间对告警信息进行分析以获得关联告警信息包括：采用串行 WINEPI 算法对告警信息进行顺序模式挖掘，用来发现告警信息的先后顺序关系，以通信设备的 IP 地址和端口号对告警信息进行分组，分别进行数据挖掘，采用滑动窗口来形成事务库，首先生成短的频繁情节模式，然后逐步递推找到大的频繁情节模式，最后找到子情节模式与情节模式之间的顺序关系。

5、根据权利要求 1 所述的系统，其特征在于，所述告警处理装置根据告警信息类型对告警信息进行相应处理包括：

如果告警信息的类型为过滤告警信息，告警处理装置直接删除告警信息缓存装置中的上述告警信息；

如果告警信息的类型为合并告警信息，且上述告警信息的数量小于预定的阈值 K，告警处理装置保留告警时间最早的告警信息，将同类告警信息的最晚告警时间记录到附加字段中，并记录所有被合并的告警信息的总数；

如果告警信息的类型为合并告警信息，且上述告警信息的数量大于等于预定的阈值 K，告警处理装置保留告警时间最早的告警信息，将同类告警信息的最晚告警时间记录到附加字段中，并记录所有被合并的告警信息的总数，并且将告警类型修改为拒绝服务 DoS（Denial of Service） 攻击。

如果告警信息的类型为压缩告警信息，告警处理装置通过将上述告警信息的告警类型和告警时间顺序连接从而将多个告警信息压缩成一个告警信息。

如果告警信息的类型为抑制告警信息，告警处理装置删除告警级别不是当前最高级别的所有告警信息。

6、根据权利要求 1 所述的系统，其特征在于，根据故障分析装置生成的网络拓扑图中的依赖关系进行告警通知或故障预警具体为：

如果并发集中通信设备的告警类型为连接错误、硬件错误或拒绝服务攻击，告警处理装置将并发集中通信设备的详细信息发送给网络管理系统，并标注为连接错误、硬件错误和拒绝服务攻击，网络管理系统收集上述通信设备的详细信息，在进行远程配置或网络管理人员

到现场对通信设备进行维护。

如果并发集中的通信设备的告警类型为软件故障，那么告警处理装置生成软件更新请求，并将上述软件更新请求发送给网络管理系统，网络管理系统根据软件更新请求，对上述并发集中的通信设备进行软件更新。

如果并发集中通信设备的告警类型为掉电告警，告警处理装置将并发集中通信设备的详细信息发送给网络管理系统，标注为掉电告警，当并发集中通信设备出现掉电告警的次数大于阈值时，网络管理人员到现场对通信设备进行维护。

如果根据顺序集中的依赖关系发现某一通信设备将要出现故障时，告警处理装置在上述通信设备出现故障之前对其它通信设备进行预警，所述其它通信设备能够进行应急处理，避免由于所述出现故障的通信设备的失效而带来的数据丢失。

7、一种基于北向接口实现网络管理的方法，所述北向接口包括告警信息缓存装置，告警分析装置，故障分析装置和告警处理装置，其特征在于，包括：

步骤 1，将网元管理系统上报的告警信息存储到告警信息缓存装置；

步骤 2，告警分析装置根据网元管理系统 ID 将所接收的告警信息分组，对每组告警信息进行关联分析，将告警信息分为以下类型：过滤告警信息，合并告警信息，压缩告警信息和抑制告警信息；

步骤 3，告警分析装置根据告警时间对告警信息进行分析以获得关联告警信息；

步骤 4，故障分析装置记录多个时间周期的关联告警信息，根据通信设备的基本属性生成虚拟通信设备，基于所述通信设备的路由信息生成网络拓扑图，在网络拓扑图中建立虚拟通信设备的虚拟网络连接，并且根据告警分析装置发送的关联告警信息生成通信设备的依赖关系；

步骤 5，告警处理装置根据告警信息类型对告警信息进行相应的处理，根据故障分析装置生成的网络拓扑图中的依赖关系进行故障预警。

8、根据权利要求 7 所述的方法，其特征在于，所述告警分析装置对每组告警信息进行关联分析包括：

如果告警信息是缺少网元管理系统 ID，告警设备 ID，告警类型，告警时间，告警级别，告警源地址，告警目的地址，告警源端口号和告警目的端口号中任意一个属性的无效告警信息或告警类型不属于网络管理系统所定义的合法告警类型集合，则将告警信息的类型设置为过滤告警信息；

统计告警设备 ID 和告警类型相同的告警信息，如果上述告警信息的数量小于预定的阈值

K，则将上述告警信息的类型设置为合并告警信息；如果上述告警信息的数量大于等于预定的阈值 K，则将上述告警信息设置为合并告警信息，并将告警类型修改为拒绝服务 DoS（Denial of Service） 攻击；

统计告警设备 ID 相同且告警类型不同的告警信息，将上述告警信息的类型设置为压缩告警信息；

根据告警级别对所有告警信息进行排序，当所有告警信息中告警级别为最高级的告警信息的数量大于其它低级别的告警信息的总数时，则将告警信息的类型设置为抑制告警信息。

9、根据权利要求 7 所述的方法，其特征在于，告警分析装置根据告警时间对告警信息进行分析以获得关联告警信息包括：

统计告警时间相同的告警信息，将上述告警信息的告警设备 ID 添加到并发集中，在每个指定时间周期内对上述并发集进行更新，确定同时发生告警事件的通信设备。

按照告警时间对告警信息进行排序，将上述告警信息的告警设备 ID 的顺序关系添加到顺序集中，在每个指定时间周期内对上述顺序集进行更新，确定顺序发生告警事件的通信设备。

10、根据权利要求 7 所述的方法，其特征在于，所述告警处理装置根据告警信息类型对告警信息进行相应处理包括：

如果告警信息的类型为过滤告警信息，告警处理装置直接删除告警信息缓存装置中的上述告警信息；

如果告警信息的类型为合并告警信息，且上述告警信息的数量小于预定的阈值 K，告警处理装置保留告警时间最早的告警信息，将同类告警信息的最晚告警时间记录到附加字段中，并记录所有被合并的告警信息的总数；

如果告警信息的类型为合并告警信息，且上述告警信息的数量大于等于预定的阈值 K，告警处理装置保留告警时间最早的告警信息，将同类告警信息的最晚告警时间记录到附加字段中，并记录所有被合并的告警信息的总数，并且将告警类型修改为拒绝服务 DoS（Denial of Service） 攻击。

如果告警信息的类型为压缩告警信息，告警处理装置通过将上述告警信息的告警类型和告警时间顺序连接从而将多个告警信息压缩成一个告警信息。

如果告警信息的类型为抑制告警信息，告警处理装置删除告警级别不是当前最高级别的所有告警信息。

一种基于北向接口实现网络管理的方法及系统

技术领域

本发明涉及通信领域中的网络管理技术，具体涉及一种基于北向接口实现网络管理的方法及系统。

背景技术

随着电信技术的迅猛发展和互联网在我国的快速普及，网络正成为社会经济文化科学等各个方面不可或缺的重要组成部分。作为各个设备的制造商，都有自己的网元管理系统(EMS)来管理自己的网络设备。然而 EMS 只能管理制造商自己的网络设备，但是电信运营商需要对这些设备乃至网元管理系统进行管理，这就给网元管理系统提出了要求：设备制造商必须开发自己网元管理系统的接口，以实现综合网管分布式的集中管理。

电信管理网络 TMN(Telecommunication Management Network)是国际电信联盟提出的，它借鉴系统管理框架技术，是为管理电信网和电信业务而定义的结构化网络体系结构。采用商定的具有标准协议和信息的接口，支撑电信网和电信业务的规划、配置、安装、操作及组织，从而使网络的操作、组织管理和维护功能及对网元的管理得以实现。的基本思想之一就是使管理功能与电信功能分离。网络管理者可以通过有限的几个管理节点管理电信网络中分布的电信设备。TMN 是一个完整独立的与电信网分离的管理网络，是各种系统按标准接口互连而成的网络。该网络在一些特定参考点进行管理信息交互，与电信网是管理网和被管网的关系。同时与电信网又不是截然分离的，利用电信网的传送通道来传送管理信息。提供管理业务，从使用者的角度对电信网进行操作、组织与维护。管理业务分为三类通信网日常业务和网络运行管理业务网络维护管理业务网络控制业务。为电信网及电信业务提供了一系列管理功能，分为五种管理功能域性能管理、配置管理、帐务管理、故障管理和安全管理。

如图 1 所示，电信管理网络 TMN 包括：网络管理系统 NMS（Network Management System）和网元管理系统 EMS(Element Management System)。网络管理系统 NMS 主要完成 TMN 中的网络管理层 NML（Network Management Layer）功能，负责对子网内的所有网元设备进行管理。网元管理系统 EMS 主要完成 TMN 电信管理网中网元管理层 EML（Element Management Layer）功能，也就是完成一个或多个移动通信终端的管理功能。网络管理系统 NMS 和网元管理系统

EMS 之间的接口称为北向接口，网络管理设备通过北向接口管理多个网元管理系统，通过多个设备供应商各自的网元管理系统来管理整个子网。

目前，常用的北向接口协议包括：公用对象请求代理体系 CORBA（Common Object Request Broker Architecture）、简单网管协议 SNMP（Simple Network Management Protocol）、web 服务（Web Service）等协议。无论采用哪一种北向接口协议，网元管理系统都需要向网络管理系统上报大量告警信息，因为在复杂、异构的网络结构中，各个网元设备之间相互影响，如果一个网元发生故障，与其相关的一些网元也会发出告警，同时显示其处于故障状态。大量的告警信息会使北向接口出现故障或性能出现瓶颈，网络管理系统会被一系列突发的、对确定故障原因无意义的大量告警事件所淹没。因此，为了更好的诊断故障，需要对故障告警信息进行分析，也就是需要对网络故障告警信息进行相关性分析，压缩冗余告警、定位故障。通过网络故障告警相关性分析，可以将多个告警事件归结成较少的告警事件，过滤掉无意义的告警事件，辅助网络管理系统删除衍生的冗余告警，从海量告警数据中找出故障的根本原因，准确定位故障。帮助网络管理系统采用合理的解决方案，及时排除故障，确保网络正常、可靠的运行。

因此，需要在北向接口中进行告警信息的分析，从海量告警数据中挖掘网络管理系统需要的重要数据。一方面避免了北向接口出现故障或性能出现瓶颈，另一方面能够准确的找出故障的根本原因，以进行最及时的处理。

发明内容

本发明目的在于提供一种基于北向接口实现网络管理的系统，该系统通过对告警信息的处理降低了北向接口的负载，提高了网络管理系统处理告警信息的效率。

一种基于北向接口实现网络管理的系统，所述系统包括：网元管理系统，北向接口和网络管理系统，网元管理系统通过北向接口将告警信息发送给网络管理系统，其特征在于，所述北向接口包括：

告警信息缓存装置，在指定的时间周期内存储网元管理系统上报的告警信息；

告警分析装置，根据网元管理系统 ID 将所接收的告警信息分组，对每组告警信息进行关联分析，将告警信息分为以下类型：过滤告警信息，合并告警信息，压缩告警信息和抑制告警信息；告警分析装置根据告警时间对告警信息进行分析以获得关联告警信息；

故障分析装置，故障分析装置记录多个时间周期的关联告警信息，根据通信设备的基本属性生成虚拟通信设备，基于所述通信设备的路由信息生成网络拓扑图，在网络拓扑图中建立虚拟通信设备的虚拟网络连接，并且根据告警分析装置发送的关联告警信息生成通信设备

的依赖关系；

告警处理装置，根据告警信息类型对告警信息进行相应的处理，根据故障分析装置生成的网络拓扑图中的依赖关系进行故障预警。

其中，所述告警分析装置对每组告警信息进行关联分析包括：

如果告警信息是缺少网元管理系统 ID，告警设备 ID，告警类型，告警时间，告警级别，告警源地址，告警目的地址，告警源端口号和告警目的端口号中任意一个属性的无效告警信息或告警类型不属于网络管理系统所定义的合法告警类型集合，则将告警信息的类型设置为过滤告警信息；

统计告警设备 ID 和告警类型相同的告警信息，如果上述告警信息的数量小于预定的阈值 K，则将上述告警信息的类型设置为合并告警信息；如果上述告警信息的数量大于等于预定的阈值 K，则将上述告警信息设置为合并告警信息，并将告警类型修改为拒绝服务 DoS（Denial of Service） 攻击；

统计告警设备 ID 相同且告警类型不同的告警信息，将上述告警信息的类型设置为压缩告警信息；

根据告警级别对所有告警信息进行排序，当所有告警信息中告警级别为最高级的告警信息的数量大于其它低级别的告警信息的总数时，则将告警信息的类型设置为抑制告警信息。

告警分析装置根据告警时间对告警信息进行分析以获得关联告警信息可以是：

统计告警时间相同的告警信息，将上述告警信息的告警设备 ID 添加到并发集中，在每个指定时间周期内对上述并发集进行更新，确定同时发生告警事件的通信设备。

按照告警时间对告警信息进行排序，将上述告警信息的告警设备 ID 的顺序关系添加到顺序集中，在每个指定时间周期内对上述顺序集进行更新，确定顺序发生告警事件的通信设备。

优选的，所述告警时间相同具有浮动值，所述浮动值由网络管理人员进行设定。

优选的，告警分析装置根据告警时间对告警信息进行分析以获得关联告警信息还可以是：采用串行 WINEPI 算法对告警信息进行顺序模式挖掘，用来发现告警信息的先后顺序关系，以通信设备的 IP 地址和端口号对告警信息进行分组，分别进行数据挖掘，采用滑动窗口来形成事务库，首先生成短的频繁情节模式，然后逐步递推找到大的频繁情节模式，最后找到子情节模式与情节模式之间的顺序关系。

所述告警处理装置根据告警信息类型对告警信息进行相应处理包括：

如果告警信息的类型为过滤告警信息，告警处理装置直接删除告警信息缓存装置中的上述告警信息；

如果告警信息的类型为合并告警信息，且上述告警信息的数量小于预定的阈值 K，告警处理装置保留告警时间最早的告警信息，将同类告警信息的最晚告警时间记录到附加字段中，并记录所有被合并的告警信息的总数；

如果告警信息的类型为合并告警信息，且上述告警信息的数量大于等于预定的阈值 K，告警处理装置保留告警时间最早的告警信息，将同类告警信息的最晚告警时间记录到附加字段中，并记录所有被合并的告警信息的总数，并且将告警类型修改为拒绝服务 DoS（Denial of Service） 攻击。

如果告警信息的类型为压缩告警信息，告警处理装置通过将上述告警信息的告警类型和告警时间顺序连接从而将多个告警信息压缩成一个告警信息。

如果告警信息的类型为抑制告警信息，告警处理装置删除告警级别不是当前最高级别的所有告警信息。

根据故障分析装置生成的网络拓扑图中的依赖关系进行告警通知或故障预警具体为：

如果并发集中通信设备的告警类型为连接错误、硬件错误或拒绝服务攻击，告警处理装置将并发集中通信设备的详细信息发送给网络管理系统，并标注为连接错误、硬件错误和拒绝服务攻击，网络管理系统收集上述通信设备的详细信息，在进行远程配置或网络管理人员到现场对通信设备进行维护。

如果并发集中的通信设备的告警类型为软件故障，那么告警处理装置生成软件更新请求，并将上述软件更新请求发送给网络管理系统，网络管理系统根据软件更新请求，对上述并发集中的通信设备进行软件更新。

如果并发集中通信设备的告警类型为掉电告警，告警处理装置将并发集中通信设备的详细信息发送给网络管理系统，标注为掉电告警，当并发集中通信设备出现掉电告警的次数大于阈值时，网络管理人员到现场对通信设备进行维护。

如果根据顺序集中的依赖关系发现某一通信设备将要出现故障时，告警处理装置在上述通信设备出现故障之前对其它通信设备进行预警，所述其它通信设备能够进行应急处理，避免由于所述出现故障的通信设备的失效而带来的数据丢失。

告警信息的属性包括：网元管理系统 ID，告警设备 ID，告警类型，告警时间，告警级别，告警源地址，告警目的地址，告警源端口号，告警目的端口号和附加字段。

本发明目的在于提供一种基于北向接口实现网络管理的方法，该方法调试方便，速度快，大大提高了网络管理的效率。

一种基于北向接口实现网络管理的方法，所述北向接口包括告警信息缓存装置，告警分

析装置，故障分析装置和告警处理装置，其特征在于，包括：

步骤 1，将网元管理系统上报的告警信息存储到告警信息缓存装置；

步骤 2，告警分析装置根据网元管理系统 ID 将所接收的告警信息分组，对每组告警信息进行关联分析，将告警信息分为以下类型：过滤告警信息，合并告警信息，压缩告警信息和抑制告警信息；

步骤 3，告警分析装置根据告警时间对告警信息进行分析以获得关联告警信息；

步骤 4，故障分析装置记录多个时间周期的关联告警信息，根据通信设备的基本属性生成虚拟通信设备，基于所述通信设备的路由信息生成网络拓扑图，在网络拓扑图中建立虚拟通信设备的虚拟网络连接，并且根据告警分析装置发送的关联告警信息生成通信设备的依赖关系；

步骤 5，告警处理装置根据告警信息类型对告警信息进行相应的处理，根据故障分析装置生成的网络拓扑图中的依赖关系进行故障预警。

其中，所述告警分析装置对每组告警信息进行关联分析包括：

如果告警信息是缺少网元管理系统 ID，告警设备 ID，告警类型，告警时间，告警级别，告警源地址，告警目的地址，告警源端口号和告警目的端口号中任意一个属性的无效告警信息或告警类型不属于网络管理系统所定义的合法告警类型集合，则将告警信息的类型设置为过滤告警信息；

统计告警设备 ID 和告警类型相同的告警信息，如果上述告警信息的数量小于预定的阈值 K，则将上述告警信息的类型设置为合并告警信息；如果上述告警信息的数量大于等于预定的阈值 K，则将上述告警信息设置为合并告警信息，并将告警类型修改为拒绝服务 DoS（Denial of Service） 攻击；

统计告警设备 ID 相同且告警类型不同的告警信息，将上述告警信息的类型设置为压缩告警信息；

根据告警级别对所有告警信息进行排序，当所有告警信息中告警级别为最高级的告警信息的数量大于其它低级别的告警信息的总数时，则将告警信息的类型设置为抑制告警信息。

告警分析装置根据告警时间对告警信息进行分析以获得关联告警信息可以是：

统计告警时间相同的告警信息，将上述告警信息的告警设备 ID 添加到并发集中，在每个指定时间周期内对上述并发集进行更新，确定同时发生告警事件的通信设备。

按照告警时间对告警信息进行排序，将上述告警信息的告警设备 ID 的顺序关系添加到顺序集中，在每个指定时间周期内对上述顺序集进行更新，确定顺序发生告警事件的通信设备。

优选的，所述告警时间相同具有浮动值，所述浮动值由网络管理人员进行设定。

优选的，告警分析装置根据告警时间对告警信息进行分析以获得关联告警信息还可以是：采用串行 WINEPI 算法对告警信息进行顺序模式挖掘，用来发现告警信息的先后顺序关系，以通信设备的 IP 地址和端口号对告警信息进行分组，分别进行数据挖掘，采用滑动窗口来形成事务库，首先生成短的频繁情节模式，然后逐步递推找到大的频繁情节模式，最后找到子情节模式与情节模式之间的顺序关系。

所述告警处理装置根据告警信息类型对告警信息进行相应处理包括：

如果告警信息的类型为过滤告警信息，告警处理装置直接删除告警信息缓存装置中的上述告警信息；

如果告警信息的类型为合并告警信息，且上述告警信息的数量小于预定的阈值 K，告警处理装置保留告警时间最早的告警信息，将同类告警信息的最晚告警时间记录到附加字段中，并记录所有被合并的告警信息的总数；

如果告警信息的类型为合并告警信息，且上述告警信息的数量大于等于预定的阈值 K，告警处理装置保留告警时间最早的告警信息，将同类告警信息的最晚告警时间记录到附加字段中，并记录所有被合并的告警信息的总数，并且将告警类型修改为拒绝服务 DoS（Denial of Service） 攻击。

如果告警信息的类型为压缩告警信息，告警处理装置通过将上述告警信息的告警类型和告警时间顺序连接从而将多个告警信息压缩成一个告警信息。

如果告警信息的类型为抑制告警信息，告警处理装置删除告警级别不是当前最高级别的所有告警信息。

根据故障分析装置生成的网络拓扑图中的依赖关系进行告警通知或故障预警具体为：

如果并发集中通信设备的告警类型为连接错误、硬件错误或拒绝服务攻击，告警处理装置将并发集中通信设备的详细信息发送给网络管理系统，并标注为连接错误、硬件错误和拒绝服务攻击，网络管理系统收集上述通信设备的详细信息，在进行远程配置或网络管理人员到现场对通信设备进行维护。

如果并发集中的通信设备的告警类型为软件故障，那么告警处理装置生成软件更新请求，并将上述软件更新请求发送给网络管理系统，网络管理系统根据软件更新请求，对上述并发集中的通信设备进行软件更新。

如果并发集中通信设备的告警类型为掉电告警，告警处理装置将并发集中通信设备的详细信息发送给网络管理系统，标注为掉电告警，当并发集中通信设备出现掉电告警的次数大

于阈值时，网络管理人员到现场对通信设备进行维护。

如果根据顺序集中的依赖关系发现某一通信设备将要出现故障时，告警处理装置在上述通信设备出现故障之前对其它通信设备进行预警，所述其它通信设备能够进行应急处理，避免由于所述出现故障的通信设备的失效而带来的数据丢失。

告警信息的属性包括：网元管理系统 ID，告警设备 ID，告警类型，告警时间，告警级别，告警源地址，告警目的地址，告警源端口号，告警目的端口号和附加字段。

附图说明

图 1 是现有技术中电信管理网络的结构图；

图 2 是根据本发明具体实施方式电信管理网络的结构示意图；

图 3 是根据本发明实施方式的基于北向接口实现网络管理的方法流程图。

具体实施方式

下面结合具体的实施方式对本发明进行详细说明：

本发明目的在于提供一种基于北向接口实现网络管理的系统，该系统通过对告警信息的处理降低了北向接口的负载，提高了网络管理系统处理告警信息的效率。

如图 2 所示，电信管理网络 TMN 包括：网络管理系统 NMS、网元管理系统 EMS 和北向接口。网络管理系统 NMS 和网元管理系统 EMS 之间通过北向接口进行通信，网络管理设备通过北向接口管理多个网元管理系统，通过多个设备供应商各自的网元管理系统来管理整个子网。

北向接口还包括：告警信息缓存装置、告警分析装置、告警处理装置和故障分析装置。北向接口在指定的时间周期内对其接收的告警信息进行分析，根据分析结果对告警信息进行相应处理，并将处理后的告警信息发送给网络管理系统。上述指定的时间周期由网络管理人员根据网络运行环境和北向接口的缓存大小进行设定，例如，1 小时。在对指定时间周期内的告警信息分析和处理后，清除缓存装置以存储下一时间周期接收的告警信息。

告警信息的属性包括：网元管理系统 ID，告警设备 ID，告警类型，告警时间，告警级别，告警源地址，告警目的地址，告警源端口号，告警目的端口号和附加字段。网元管理系统 ID 用于标识发送告警信息的网元管理系统，例如，网元管理系统 EMS1、网元管理系统 EMS2 和网元管理系统 EMS3。告警设备 ID 用于表示发送告警信息的网络设备的 ID，例如，网络设备 NE1、网络设备 NE2、网络设备 NE3 和网络设备 NE4。告警类型可以是“连接失败”、“软件错误”、“硬件错误”、“掉电告警”、“拒绝服务”等；告警时间的格式为 YYYY－MM－DD HH：MM：SS，例如，2006-6-23 17：25：04。告警级别分为 5 级，告警级别从高到低为 5 级>4 级>3 级>2 级>1 级。告警源地址为发出告警信息的网络设备的 IP 地址，告警目的地址为

网络管理系统的 IP 地址。告警源端口号为发出告警信息的网络设备应用程序端口号，告警目的端口号为网络管理系统的相关端口号。附加字段用于表示合并告警信息的条数，

告警信息缓存装置，用于存储指定的时间周期内网元管理系统发送给北向接口的告警信息。告警分析装置，根据网元管理系统的 ID 将所接收的告警信息分组，对每组告警信息进行关联分析，将告警信息分为以下类型：过滤告警信息（无用的告警），合并告警信息，压缩告警信息，抑制告警信息和关联告警信息。

其中，如果告警信息是缺少网元管理系统 ID，告警设备 ID，告警类型，告警时间，告警级别，告警源地址，告警目的地址，告警源端口号和告警目的端口号中任意一个属性的无效告警信息或告警类型不属于不属于网络管理系统所定义的合法告警类型的集合，则将告警信息的类型设置为过滤告警信息。

统计告警设备 ID 和告警类型相同的告警信息，即同一通信设备针对同一事件发出的相同告警类型的告警信息，如果上述告警信息的数量小于预定的阈值 K，则将上述所有告警信息的类型设置为合并告警信息；（在附加字段中添加告警信息的数量）如果上述告警信息的数量大于等于预定的阈值 K，则将上述告警信息设置为合并告警信息，并将告警类型修改为拒绝服务 DoS（Denial of Service） 攻击。

统计告警设备 ID 相同且告警类型不同的告警信息，将上述告警信息的类型设置为压缩告警信息。告警设备 ID 相同且告警类型不同的告警信息是同一告警设备针对不同事件分别发出的告警信息。

根据告警级别对所有告警信息进行排序，当所有告警信息中告警级别为最高级的告警信息的数量大于其它低级别的告警信息的总数时，则将告警信息的类型设置为抑制告警信息。例如，在指定的时间周期中，所有告警信息中告警级别最高的为 4 级，那么如果告警级别为 4 级的告警信息的数量大于告警级别为 3 级，2 级和 1 级的告警信息数量之和时，则将告警信息的类型设置为抑制告警信息。一个具体的例子为，当前共有 10000 条告警信息，告警级别为 4 级的告警信息 5500 条，告警级别为 3 级的告警信息 2000 条，告警级别为 2 级的告警信息 1500 条，告警级别为 1 级的告警信息 1000 条，可知，所有告警信息中告警级别最高的为 4 级，且告警级别为 4 级的告警信息共有 5500 条，而其它低级别 3 级，2 级和 1 级的告警信息的总数为 4500 时，则将告警信息的类型设置为抑制告警信息。

根据告警时间对告警信息进行分析，统计告警时间相同的告警信息，将上述告警信息的告警设备 ID 添加到并发集中，在每个指定时间周期内对上述并发集进行更新，确定同时发生告警事件的通信设备。考虑网络延迟等原因，所述告警时间相同具有浮动值，所述浮动值由

网络管理人员进行设定，例如，60 秒，90 秒等。如果多个通信设备在多个指定的时间周期内均同时发送告警信息，那么说明上述多个通信设备具有故障并发性。

按照告警时间对告警信息进行排序，将上述告警信息的告警设备 ID 的顺序关系（A--B--C）添加到顺序集中，在每个指定时间周期内对上述顺序集进行更新，确定顺序发生告警事件的通信设备。如果多个通信设备在多个指定的时间周期内均具有相同的顺序关系，例如，通信设备 A 发送告警信息后，通信设备 B 也会发送告警信息，或只要通信设备 A 和 B 发送告警信息，那么通信设备 C 就会发送故障告警信息，那么说明上述多个通信设备具有故障顺序性。

或者，告警分析装置根据告警时间对告警信息进行分析以获得关联告警信息还可以是：采用串行 WINEPI 算法对告警信息进行顺序模式挖掘，用来发现告警信息的先后顺序关系，以通信设备的 IP 值和端口号对告警信息进行分组分别进行数据挖掘，采用滑动窗口来形成事务库，首先生成短的频繁情节模式，然后逐步递推找到大的频繁情节模式，最后找到子情节模式与情节模式之间的顺序关系。

告警处理装置根据告警信息类型进行相应的处理：

如果告警信息的类型为过滤告警信息，告警处理装置直接删除告警信息缓存装置中的上述告警信息；

如果告警信息的类型为合并告警信息，且上述告警信息的数量小于预定的阈值 K，告警处理装置保留告警时间最早的告警信息，将同类告警信息的最晚告警时间记录到附加字段中，并记录所有被合并的告警信息的总数。例如，多条合并告警信息如下

告警设备 ID	告警类型	告警时间	……	附加字段
1101	软件错误	2006-6-23 17:25:04	……	无
1101	软件错误	2006-6-23 17:27:13	……	无
1101	软件错误	2006-6-23 17:31:21	……	无
……	……	……	……	……
1101	软件错误	2006-6-23 19:38:26	……	无

告警处理装置保留告警时间最早的告警信息（告警时间 2006 年 6 月 23 日 17 点 25 分 04 秒），将同类告警信息的最晚告警时间（2006 年 6 月 23 日 19 点 38 分 26 秒）记录到附加字段中，并记录所有被合并的告警信息的总数（共收到 216 同类的告警信息）。

告警设备 ID	告警类型	告警时间	……	附加字段
1101	软件错误	2006-6-23 17:25:04	……	2006-6-23 19:38:26 216

如果告警信息的类型为合并告警信息，且上述告警信息的数量大于等于预定的阈值 K，告警处理设备进行相同的操作，并且将告警类型修改为拒绝服务 DoS（Denial of Service） 攻击，并且过滤同一通信设备相同告警类型的其它告警信息。

告警设备 ID	告警类型	告警时间	……	附加字段
1101	拒绝服务	2006-6-23 17:25:04	……	2006-6-23 19:38:26 216

如果告警信息的类型为压缩告警信息，告警处理装置通过将上述告警信息的告警类型和告警时间顺序连接从而将多个告警信息压缩成一个告警信息。例如，通信设备 1101 发送的 4 条告警类型不同的告警信息：

告警设备 ID	告警类型	告警时间	……	附加字段
1101	连接错误	2006-6-28 17:25:04	……	无
1101	软件错误	2006-6-28 17:27:13	……	无
1101	硬件错误	2006-6-28 17:31:21	……	无

告警处理装置保留告警设备 ID，告警级别，告警源地址，告警目的地址，告警源端口号，告警目的端口号和附加字段，将“连接错误”，“2006-6-28 17:25:04”，“软件错误”，“2006-6-28 17:27:13”，“硬件错误”，“2006-6-28 17:31:21”，“掉电告警”，“2006-6-28 19:38:26” 顺序连接生成压缩告警信息，如下：

告警设备 ID	告警类型	告警时间	告警类型	告警时间	告警类型	告警时间	……	附加字段
1101	拒绝服务	2006-6-28 17:25:04	软件错误	2006-6-28 17:27:13	硬件错误	2006-6-28 17:31:21	……	无

如果告警信息的类型为抑制告警信息，告警处理装置删除告警级别不是当前最高级别的所有告警信息。例如，告警信息为抑制告警信息，且当前告警级别的最高级为 4 级，那么告警处理装置删除告警级别为 3 级，2 级和 1 级的告警信息。

故障分析装置，故障分析装置记录多个时间周期的关联告警信息，根据通信设备的基本属性生成虚拟通信设备，基于所述通信设备的路由信息生成网络拓扑图，在网络拓扑图中建立虚拟通信设备的虚拟网络连接，并且根据告警分析装置发送的关联告警信息生成通信设备的依赖关系；

进一步，告警处理装置根据故障分析装置生成的网络拓扑图中的依赖关系进行告警通知或故障预警：

如果并发集中的通信设备为连接错误或硬件错误，告警处理装置将并发集中的通信设备

的详细信息发送给网络管理系统，并标注为连接错误或硬件错误，网络管理系统收集上述多个通信设备的详细信息，在必要时进行远程配置或让网络管理人员到现场维护。

如果并发集中的通信设备为软件故障，那么告警处理装置生成软件更新请求，并将上述软件更新请求发送给网络管理系统，网络管理系统根据软件更新请求，对上述并发集中的通信设备进行更新。

如果并发集中的通信设备为掉电告警，告警处理装置将并发集中的通信设备的详细信息发送给网络管理系统，标注为掉电告警，当并发集中的通信设备出现掉电告警的次数大于阈值（网络管理人员设定）时，网络管理人员到现场对通信设备进行维护。

根据每个顺序集中通信设备的故障类型进行相应处理，如果根据顺序集中的规则发现某一通信设备将要发出告警信息，那么告警处理装置在通信设备发出告警信息之前对其它通信设备进行预警，所述其它通信设备随即进行应急处理，避免由于该通信设备故障而带来的数据丢失。例如，通信设备 A、B 和 C 之间存在以下依赖关系：只要通信设备 A 和 B 发送告警信息，那么通信设备 C 就会发送故障告警信息。如果发现通信设备 A 和 B 发送了“软件错误”的告警信息，告警处理装置把通信设备 C 将要发生“软件错误”的预警信息发送给网络拓扑图可能访问通信设备 C 的所有通信设备，上述所有通信设备可以提前保存通信状态，发送数据等信息，以避免数据丢失。

图 3 是根据本发明实施方式的基于北向接口实现网络管理的方法，北向接口在指定的时间周期内执行以下步骤并重复多个时间周期，具体步骤如下：

步骤 1，将网元管理系统上报的告警信息存储到告警信息缓存装置；

步骤 2，告警分析装置根据网元管理系统的 ID 将所接收的告警信息分组，对每组告警信息进行关联分析，将告警信息分为以下类型：过滤告警信息（无用的告警），合并告警信息，压缩告警信息和抑制告警信息；

步骤 3，告警分析装置根据告警时间对告警信息进行分析以获得关联告警信息；

步骤 4，故障分析装置记录多个时间周期的关联告警信息，根据通信设备的基本属性生成虚拟通信设备，基于所述通信设备的路由信息生成网络拓扑图，在网络拓扑图中建立虚拟通信设备的虚拟网络连接，并且根据告警分析装置发送的关联告警信息生成通信设备的依赖关系；

步骤 5，告警处理装置根据告警信息类型进行相应的处理，根据故障分析装置生成的网络拓扑图中的依赖关系进行告警通知或故障预警。

其中，所述告警分析装置对每组告警信息进行关联分析包括：

如果告警信息是缺少网元管理系统 ID，告警设备 ID，告警类型，告警时间，告警级别，告警源地址，告警目的地址，告警源端口号和告警目的端口号中任意一个属性的无效告警信息或告警类型不属于网络管理系统所定义的合法告警类型集合，则将告警信息的类型设置为过滤告警信息。

统计告警设备 ID 和告警类型相同的告警信息，如果上述告警信息的数量小于预定的阈值 K，则将上述所有告警信息的类型设置为合并告警信息；如果上述告警信息的数量大于等于预定的阈值 K，则将上述告警信息设置为合并告警信息，并将告警类型修改为拒绝服务 DoS（Denial of Service） 攻击；

统计告警设备 ID 相同且告警类型不同的告警信息，将上述告警信息的类型设置为压缩告警信息。

根据告警级别对所有告警信息进行排序，当所有告警信息中告警级别为最高级的告警信息的数量大于其它低级别的告警信息的总数时，则将告警信息的类型设置为抑制告警信息。

告警分析装置根据告警时间对告警信息进行分析以获得关联告警信息可以是：

根据告警时间对告警信息进行分析，统计告警时间相同的告警信息，将上述告警信息的告警设备 ID 添加到并发集中，在每个指定时间周期内对上述并发集进行更新，确定同时发生告警事件的通信设备。

优选的，所述告警时间相同具有浮动值，所述浮动值由网络管理人员进行设定。

按照告警时间对告警信息进行排序，将上述告警信息的告警设备 ID 的顺序关系添加到顺序集中，在每个指定时间周期内对上述顺序集进行更新，确定顺序发生告警事件的通信设备。

优选的，告警分析装置根据告警时间对告警信息进行分析以获得关联告警信息还可以是：采用串行 WINEPI 算法对告警信息进行顺序模式挖掘，用来发现告警信息的先后顺序关系，以通信设备的 IP 值和端口号对告警信息进行分组分别进行数据挖掘，采用滑动窗口来形成事务库，首先生成短的频繁情节模式，然后逐步递推找到大的频繁情节模式，最后找到子情节模式与情节模式之间的顺序关系。

所述告警处理装置根据告警信息类型进行相应处理包括：

如果告警信息的类型为过滤告警信息，告警处理装置直接删除告警信息缓存装置中的上述告警信息；

如果告警信息的类型为合并告警信息，且上述告警信息的数量小于预定的阈值 K，告警处理装置保留告警时间最早的告警信息，将同类告警信息的最晚告警时间记录到附加字段中，并记录所有被合并的告警信息的总数；

如果告警信息的类型为合并告警信息，且上述告警信息的数量大于等于预定的阈值 K，告警处理设备进行相同的操作，并且将告警类型修改为拒绝服务 DoS（Denial of Service） 攻击，并且过滤同一通信设备相同告警类型的其它告警信息。

如果告警信息的类型为压缩告警信息，告警处理装置通过将上述告警信息的告警类型和告警时间顺序连接从而将多个告警信息压缩成一个告警信息。

如果告警信息的类型为抑制告警信息，告警处理装置删除告警级别不是当前最高级别的所有告警信息。

根据故障分析装置生成的网络拓扑图中的依赖关系进行告警通知或故障预警具体为：

如果并发集中的通信设备为连接错误或硬件错误，告警处理装置将并发集中的通信设备的详细信息发送给网络管理系统，并标注为连接错误或硬件错误，网络管理系统收集上述多个通信设备的详细信息，在必要时进行远程配置或让网络管理人员到现场维护。

如果并发集中的通信设备为软件故障，那么告警处理装置生成软件更新请求，并将上述软件更新请求发送给网络管理系统，网络管理系统根据软件更新请求，对上述并发集中的通信设备进行更新。

如果并发集中的通信设备为掉电告警，告警处理装置将并发集中的通信设备的详细信息发送给网络管理系统，标注为掉电告警，当并发集中的通信设备出现掉电告警的次数大于阈值（网络管理人员设定）时，网络管理人员到现场对通信设备进行维护。

根据每个顺序集中通信设备的故障类型进行相应处理，如果根据顺序集中的规则发现某一通信设备将要发出告警信息，那么告警处理装置在通信设备发出告警信息之前对其它通信设备进行预警，所述其它通信设备随即进行应急处理，避免出于该通信设备故障而带来的数据丢失。

告警信息的属性包括：网元管理系统 ID，告警设备 ID，告警类型，告警时间，告警级别，告警源地址，告警目的地址，告警源端口号，告警目的端口号和附加字段。

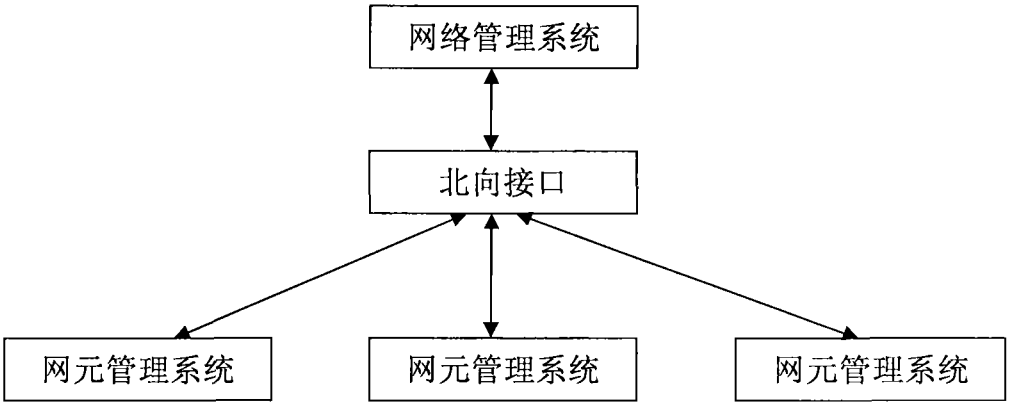


图 1

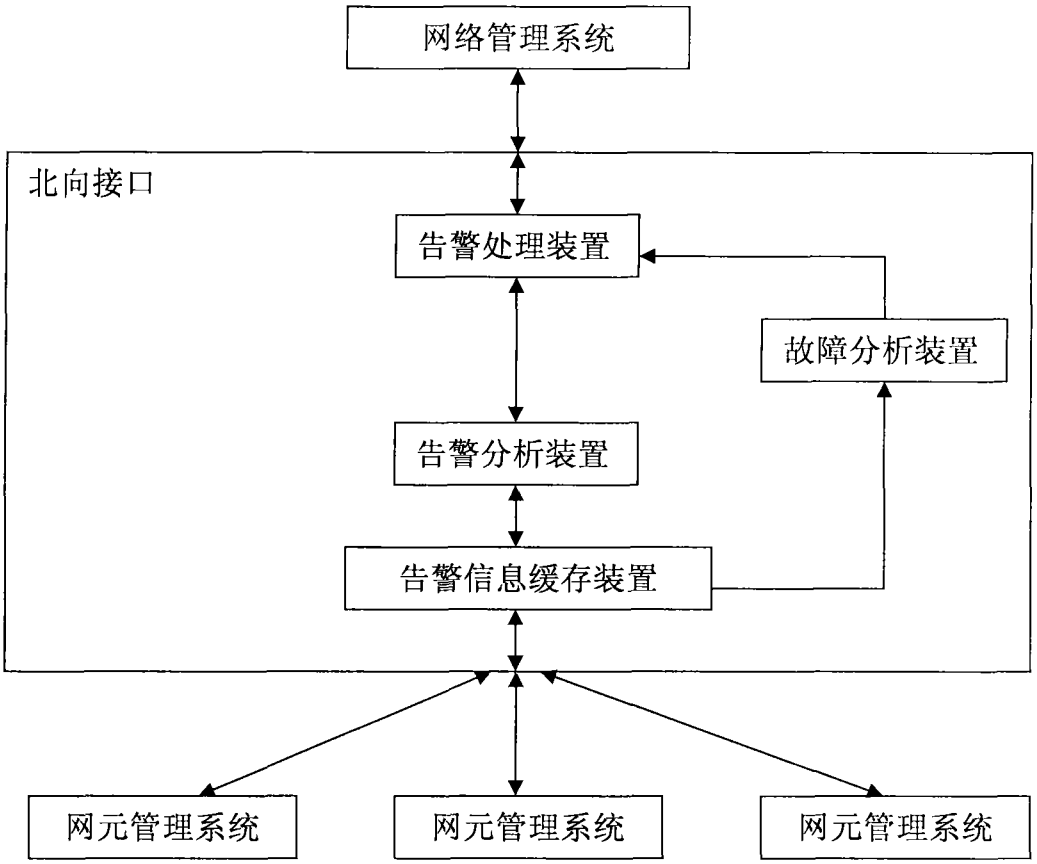

网络管理系统
北向接口
告警处理装置
故障分析装置
告警分析装置
告警信息缓存装置
网元管理系统
网元管理系统
网元管理系统

图 2

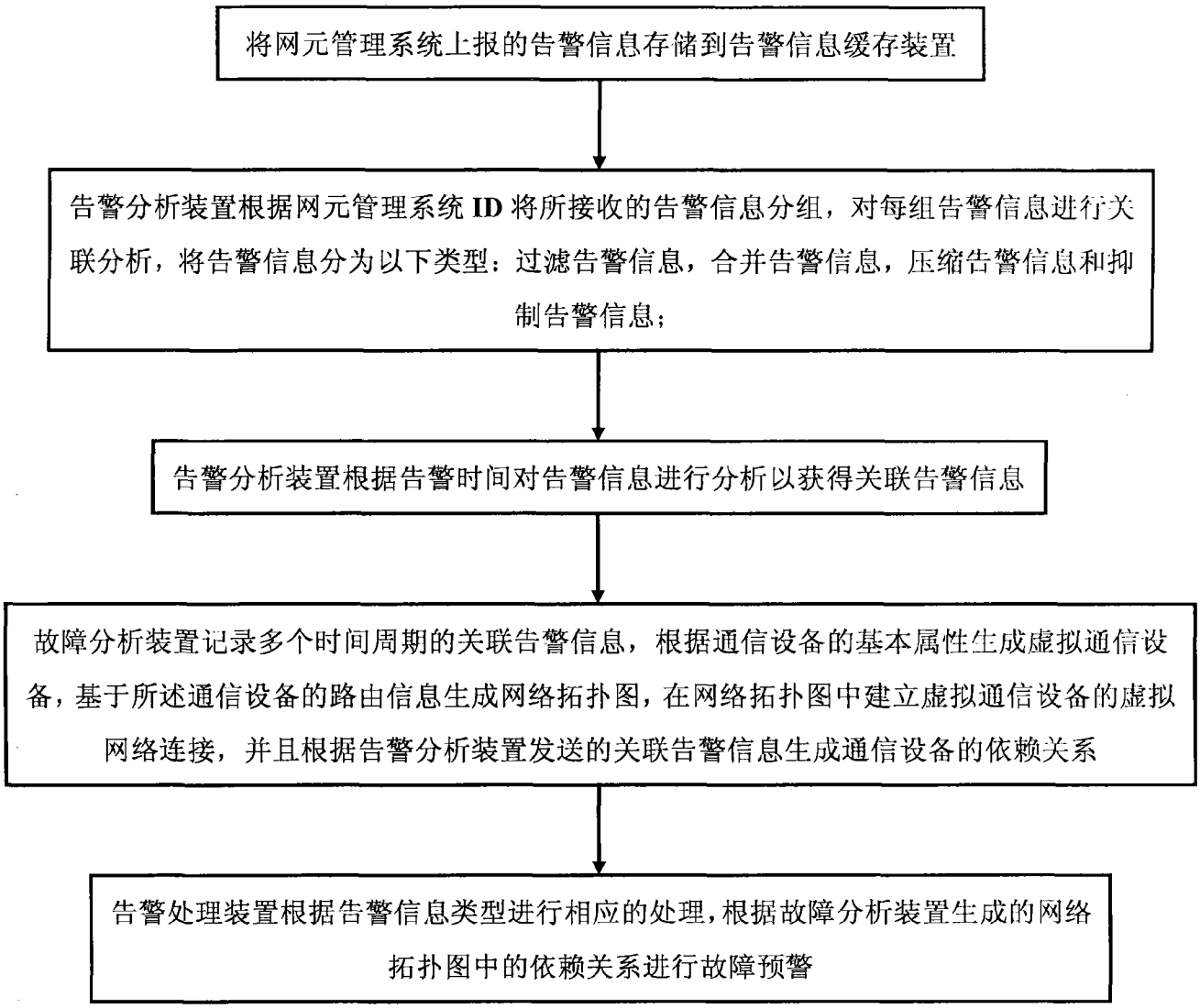

将网元管理系统上报的告警信息存储到告警信息缓存装置
告警分析装置根据网元管理系统ID将所接收的告警信息分组，对每组告警信息进行关联分析，将告警信息分为以下类型：过滤告警信息，合并告警信息，压缩告警信息和抑制告警信息；
告警分析装置根据告警时间对告警信息进行分析以获得关联告警信息
故障分析装置记录多个时间周期的关联告警信息，根据通信设备的基本属性生成虚拟通信设备，基于所述通信设备的路由信息生成网络拓扑图，在网络拓扑图中建立虚拟通信设备的虚拟网络连接，并且根据告警分析装置发送的关联告警信息生成通信设备的依赖关系
告警处理装置根据告警信息类型进行相应的处理，根据故障分析装置生成的网络拓扑图中的依赖关系进行故障预警

图 3