(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 105450444 A
(43)申请公布日 2016.03.30

(21)申请号 201510777904.X

(22)申请日 2015.11.16

(71)申请人 成都科来软件有限公司
地址 610041 四川省成都市高新区天府大道中段801号

(72)发明人 罗鹰 王翔 林康

(74)专利代理机构 成都九鼎天元知识产权代理有限公司 51214
代理人 郭彩红

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

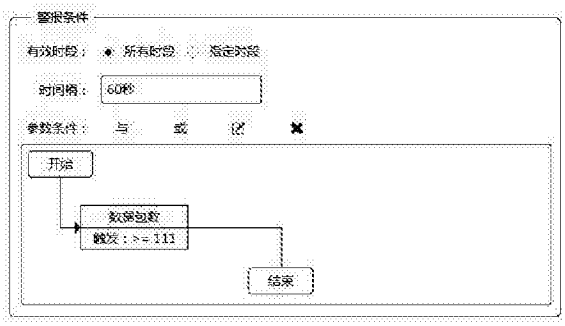
权利要求书1页 说明书4页 附图4页

(54)发明名称

一种基于网络数据的网络参数警报配置系统及评估系统

(57)摘要

本发明提供了一种基于网络数据的网络参数警报配置系统及评估系统，包括条件参数设置模块和条件参数关系设置模块；所述条件参数设置模块，用于设置满足警报条件的各个子条件；所述条件参数关系设置模块用于设置各个子条件之间的逻辑与或关系。能够满足复杂警报条件，使多种条件参数在一个警报配置中触发；能够让使用者了解所配置的参数与条件在网络中带来的分析结果和产生的价值。



CN 105450444 A

1.一种基于网络数据的网络参数警报配置系统，通过警报条件设置模块实现网络参数警报配置，所述警报条件设置模块包括有效时段设置模块和警报桶设置模块，其特征在于：所述警报条件设置模块还包括条件参数设置模块和条件参数关系设置模块；所述条件参数设置模块，用于设置满足警报条件的各个子条件；所述条件参数关系设置模块用于设置各个子条件之间的逻辑与或关系。

2.根据权利要求1所述的网络参数警报配置系统，其特征在于：所述条件参数设置模块能够设置两项以上的子条件；所述条件参数关系设置模块，选择需要关联设置的子条件，并设置所选子条件之间的逻辑与或关系。

3.根据权利要求1所述的网络参数警报配置系统，其特征在于：所述条件参数设置模块最多只能设置两项子条件；所述条件参数关系设置模块，设置所有子条件的逻辑与或关系。

4.根据权利要求2或3所述的网络参数警报配置系统，其特征在于：还包括条件参数修改模块，用于修改某子条件的参数。

5.根据权利要求2或3所述的网络参数警报配置系统，其特征在于：还包括条件参数删除模块，用于删除某已经建立的子条件。

6.一种基于网络数据的网络参数警报评估系统，其特征在于，包括时间范围设置模块，探针设置模块，条件参数设置模块和条件参数关系设置模块；所述条件参数设置模块，用于设置满足警报条件的各个子条件；所述条件参数关系设置模块用于设置各个子条件之间的逻辑与或关系；还包括警报评估模块，对现有设置条件下产生的警报条件数据进行显示。

7.根据权利要求6所述的网络参数警报评估系统，其特征在于：所述条件参数设置模块能够设置两项以上的子条件；所述条件参数关系设置模块，选择需要关联设置的子条件，并设置所选子条件之间的逻辑与或关系。

8.根据权利要求6所述的网络参数警报评估系统，其特征在于：所述条件参数设置模块最多只能设置两项子条件，所述条件参数关系设置模块，设置所有子条件的逻辑与或关系。

9.根据权利要求7或8所述的网络参数警报评估系统，其特征在于：还包括条件参数编辑模块，用于修改子条件警报参数。

10.根据权利要求7或8所述的网络参数警报评估系统，其特征在于：还包括警报时间占比统计模块，用户统计未触发警报时间与触发警报时间的占比。

一种基于网络数据的网络参数警报配置系统及评估系统

技术领域

[0001] 本发明涉及一种网络参数警报配置系统及评估系统，特别是涉及一种基于网络数据的网络参数警报配置系统及评估系统。

背景技术

[0002] 当今社会网络的安全与稳定是必不可少的，为了让网络更健康的运行人们更多的会使用分析软件来了解网络运行情况。相当多的分析软件通过配置相应警报参数与条件后，对使用者的网络状况进行分析。这种分析能大大提升网络的运行维护能力和故障处置效率，有效的减少故障时间。但在此过程中使用者往往不能准确的抓住配置过程中需要的警报参数与条件，从而造成分析结果不能体现相应价值甚至有可能错误的估计当前网络状况。

[0003] 相当多的技术是给予使用者一种推荐的参数或条件，此方法在特定的环境下带来的结果可能并不是该网络中真正需要关注的，且不能直观的让使用者了解他所配置的参数与条件在网络中可能带来的分析结果和产生的价值。

发明内容

[0004] 本发明首先要解决的技术问题是提供一种能够满足复杂警报条件，使多种条件参数在一个警报配置中触发的基于网络数据的网络参数警报配置系统；其次要解决的技术问题是，提供一种能够让使用者了解所配置的参数与条件在网络中带来的分析结果和产生的价值的，基于网络数据的网络参数警评估系统。

[0005] 本发明采用的技术方案如下：

一种基于网络数据的网络参数警报配置系统，通过警报条件设置模块实现网络参数警报配置，所述警报条件设置模块包括有效时段设置模块和警报桶设置模块，其特征在于：所述警报条件设置模块还包括条件参数设置模块和条件参数关系设置模块；所述条件参数设置模块，用于设置满足警报条件的各个子条件；所述条件参数关系设置模块用于设置各个子条件之间的逻辑与或关系。

[0006] 有效时段是指所设置警报条件有效的有效时段，包括所有时段设置单元和指定时段设置单元。条件参数设置模块用于设置满足某单个报警条件的参数范围，由单个参数或两个以上的参数范围设置形成一个子条件；条件参数关系设置模块，用于设置子条件之间的逻辑与或关系，如设置同时满足两个子条件(逻辑与关系)或满足其中一个子条件(逻辑或关系)时进行报警。满足复杂警报条件，使多种条件参数在一个警报配置中触发，便于使用者更多样化，更直观，更准确的对网络数据进行警报的配置，而不是单一化的以单参数进行数据配置。

[0007] 还包括条件参数修改模块，用于修改某子条件的参数。

[0008] 还包括条件参数删除模块，用于删除某已经建立的子条件。

[0009] 所述条件参数设置模块能够设置两项以上的子条件；所述条件参数关系设置模

块，选择需要关联设置的子条件，并设置所选子条件之间的逻辑与或关系。

[0010] 在条件参数设置模块设置两项以上的子条件，选择需要使用的子条件，并设置他们之间的逻辑与或关系，完成报警条件的设置。各子条件能够重新修改、删除或填加。

[0011] 所述条件参数设置模块最多只能设置两项子条件；所述条件参数关系设置模块，设置所有子条件的逻辑与或关系。通过修改条件参数更改子条件，或者重新建立子条件。

[0012] 一种基于网络数据的网络参数警报评估系统，其特征在于，包括时间范围设置模块，探针设置模块，条件参数设置模块和条件参数关系设置模块；所述条件参数设置模块，用于设置满足警报条件的各个子条件；所述条件参数关系设置模块用于设置各个子条件之间的逻辑与或关系；还包括警报评估模块，对现有设置条件下产生的警报条件数据进行显示。

[0013] 时间范围设置模块用于设置警报的时间区间，探针设置模块用于设置数据获取的探针。条件参数设置模块用于设置满足某单个报警条件的参数范围，由单个参数或两个以上的参数范围设置形成一个子条件；条件参数关系设置模块，用于设置子条件之间的逻辑与或关系，如设置同时满足两个子条件(逻辑与关系)或满足其中一个子条件(逻辑或关系)时进行报警。警报评估模块显示当前设置条件下产生的警报条件数据，包括参数条件，及相应参数条件下的警报数量，让使用者了解所配置的参数与条件在网络中带来的分析结果和产生的价值。网络警报评估过程中提供时间范围，不同的探针(网络数据获取源)，IP地址等数据过滤条件方便使用者更为精确且详细的了解参数是否配置正确且有价值。

[0014] 所述条件参数设置模块能够设置两项以上的子条件；所述条件参数关系设置模块，选择需要关联设置的子条件，并设置所选子条件之间的逻辑与或关系。

[0015] 所述条件参数设置模块最多只能设置两项子条件，所述条件参数关系设置模块，设置所有子条件的逻辑与或关系。

[0016] 还包括条件参数编辑模块，用于修改子条件警报参数。

[0017] 还包括警报时间占比统计模块，用户统计未触发警报时间与触发警报时间的占比。

[0018] 与现有技术相比，本发明的有益效果是：能够满足复杂警报条件，使多种条件参数在一个警报配置中触发；能够让使用者了解所配置的参数与条件在网络中带来的分析结果和产生的价值。

附图说明

[0019] 图1为本发明其中一实施例的网络参数警报配置流程图。

[0020] 图2为图1所示实施例的逻辑与或关系警报配置示意图。

[0021] 图3为本发明其中一实施例的子条件逻辑与或关系图。

[0022] 图4为本发明其中一实施例的网络参数警报评估设置流程图。

[0023] 图5为本发明其中一实施例的网络参数警报分析结果—评估趋势图。

[0024] 图6为图5所示实施例的警报分析结果—3D饼图。

具体实施方式

[0025] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，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用以解释本发明，并不用于限定本发明。

[0026] 本说明书(包括摘要和附图)中公开的任一特征，除非特别叙述，均可被其他等效或者具有类似目的的替代特征加以替换。即，除非特别叙述，每个特征只是一系列等效或类似特征中的一个例子而已。

[0027] 基于Web页面，如图1所示。使用者在配置网络警报时，对参数条件的筛选相当重要。而为了给使用者更加全方位且准确的分析结果。与或关系图至关重要，现有技术只能做到单一的添加警报要想使警报满足复杂的多条件参数往往需要配置多条警报设置，而本技术方案中只需要按所需逻辑配置出与或关系图即可满足多种条件参数在一个警报配置中触发，关系图中有与、或、编辑、删除等模块操作，默认会选中一个配置好的最后一个参数，点击编辑与删除分别是对此选中项进行对应操作，点击与、或则是配置(网络参数与参数值，见图2)一条新参数与选中项的关系，配置完成后新参数自动为新的选中项，可以通过点击参数更改选中项。当用户配置的参数满足条件时系统会告知使用者网络中有异常的情况发生。

[0028] 如图3所示，当用户的网络中存在数据包数大于100且上行数据包数大于50且每秒发送数据包数大于10，或者数据包数大于100且下行数据包数大于20且上行字节数小于50时系统会将以上这两种情况判断为警报告知。但是使用者并不能很准确的知道此时配置的警报是否有价值且是否符合自身网络情况。比如用户配置一条警报，为数据包数大于10，但是也许在一定环境下普遍的网络数据的数据包数都会大于10，这样会触发很多不必要的警报且完全没有分析价值。

[0029] 这时当使用者点击启用评估功能，系统将会打开一个新页面(如图4所示)，使用者可以直接使用或对刚刚配置的与或关系图进行参数的重新编辑，操作与配置时一样。点击开始评估，系统将获取在对应过滤条件下(如:时间，数据获取的探针，指定的IP地址等)的所有相关参数(与或关系图中所配置参数)数据并以图表的形式进行展现(如图5和图6所示)。

[0030] 根据以上分析结果，用户可以通过自身网络情况对此份配置进行评估，如此时的警报配置过高未产生任何警报或警报过低产生大量的警报，用户会认为未达到预期价值则可继续修改参数进行评估。如认为已完全满足需求，则可以点击应用参数，系统将会把此时评估的与或关系图直接回填至图一的配置页面并生成一份对用户网络真正有价值的警报配置。

[0031] 在网络警报评估中以趋势图(如图5所示)的形式展示此警报触发情况，根据不同需求此方法做到能将上百万个时间为分级单位的历史网络数据同时进行还原展现且支持图表的缩放与下载功能，此趋势图中分别以不同的线或点直观的展示出此时段产生的历史网络数据、用户配置参数的基准线以及产生的警报数量，而当数据超过基准线时则会触发警报。

[0032] 如图5所示，X轴为评估时选中的时间范围，左侧Y轴代表警报数量，右侧Y轴代表与或关系图配置参数的历史数据单位，最上方由点与点连接构成的抛物线为与或关系图中参数的趋势图，中间的方点代表警报产生数，最下方的点与点连接的直线则代表基准线即评估时与或关系图对应配置参数警报条件。由图可见，当抛物线低于直线时，对应X轴的时间

点上并未警报数量，而当抛物线高于直线时，对应X轴上方产生警报数量即为警报已触发。

[0033] 如图6所示，在评估中以3D饼图的形式展示用户所配置的警报在此时段产生警报的时间与未产生警报的时间的占比情况。

[0034] 以图5和图6此两种方式更直观的让用户了解当前配置在网络中带来分析结果和产生的价值。评估完成后可快速回填当前评估的与或关系图参数生成警报，无需其他任何繁琐操作。

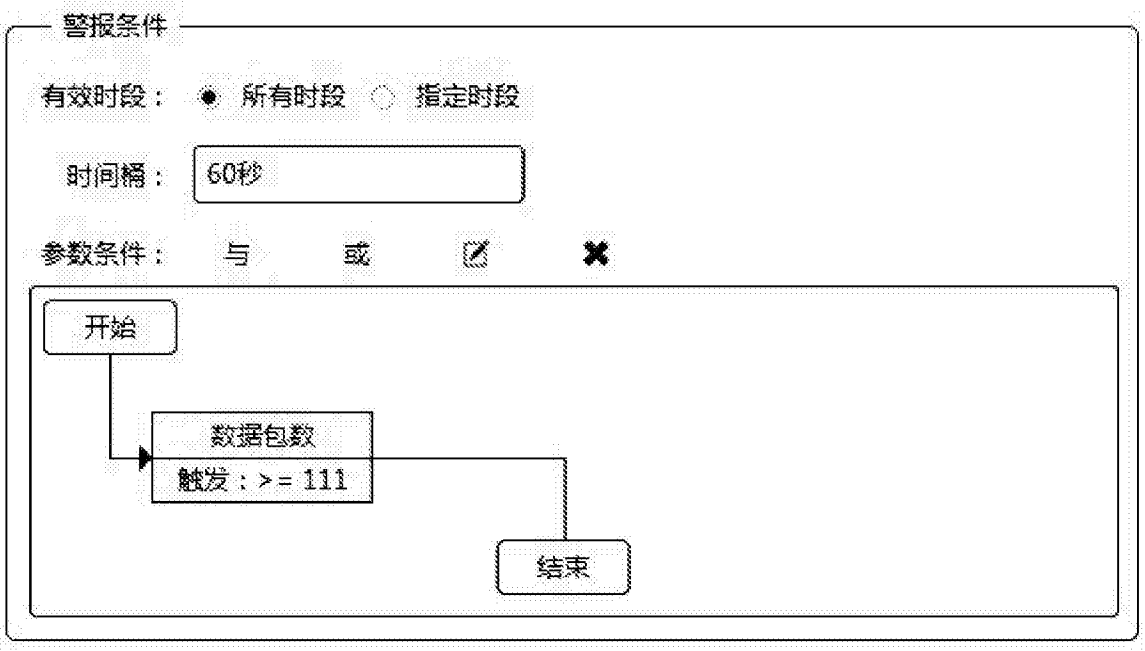

警报条件
有效时段：
所有时段
指定时段
时间幅：
60秒
参数条件：
与
或
开始
数据包数
触发：>= 111
结束

图1

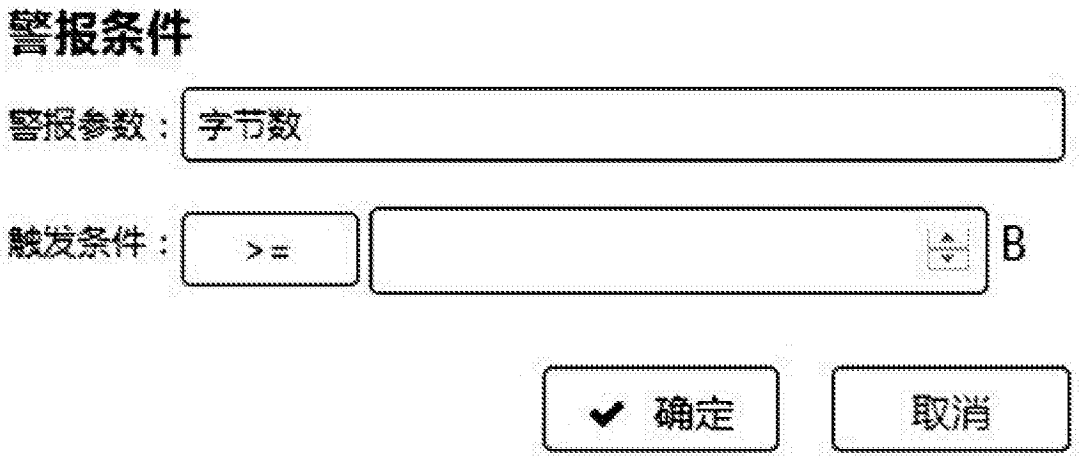

警报条件
警报参数：
字节数
触发条件：
>=
B
确定
取消

图2

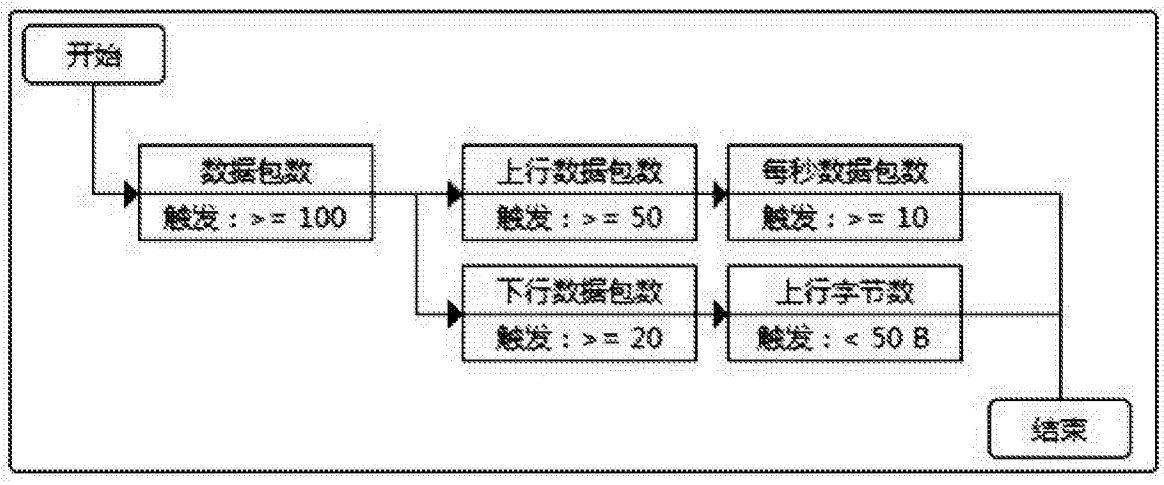

开始
数据包数
触发：>= 100
上行数据包数
触发：>= 50
每秒数据包数
触发：>= 10
下行数据包数
触发：>= 20
上行字节数
触发：< 50 B
结束

图3

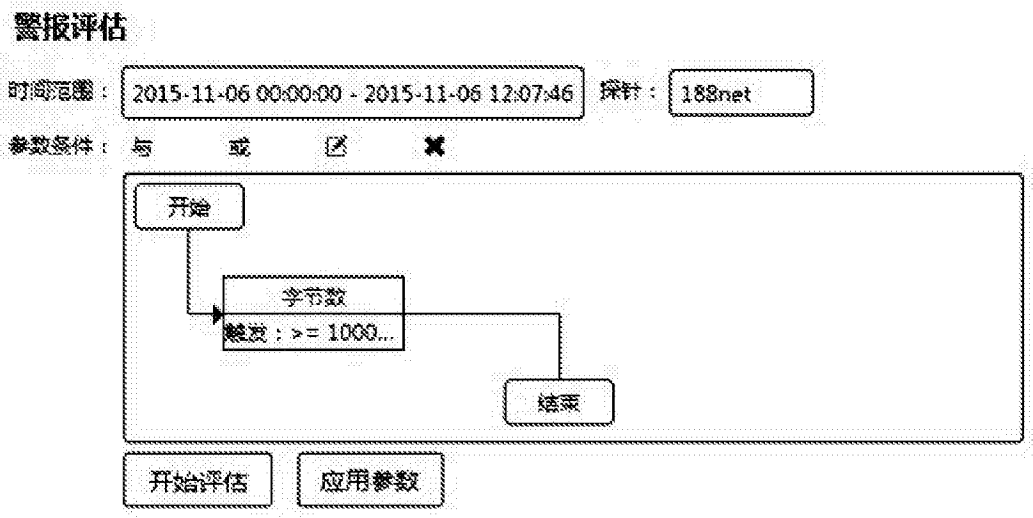

警报评估
时间范围：
2015-11-06 00:00:00 - 2015-11-06 12:07:46
探针：
188net
参数条件：
与
或
开始
字节数
触发：>= 1000...
结束
开始评估
应用参数

图4

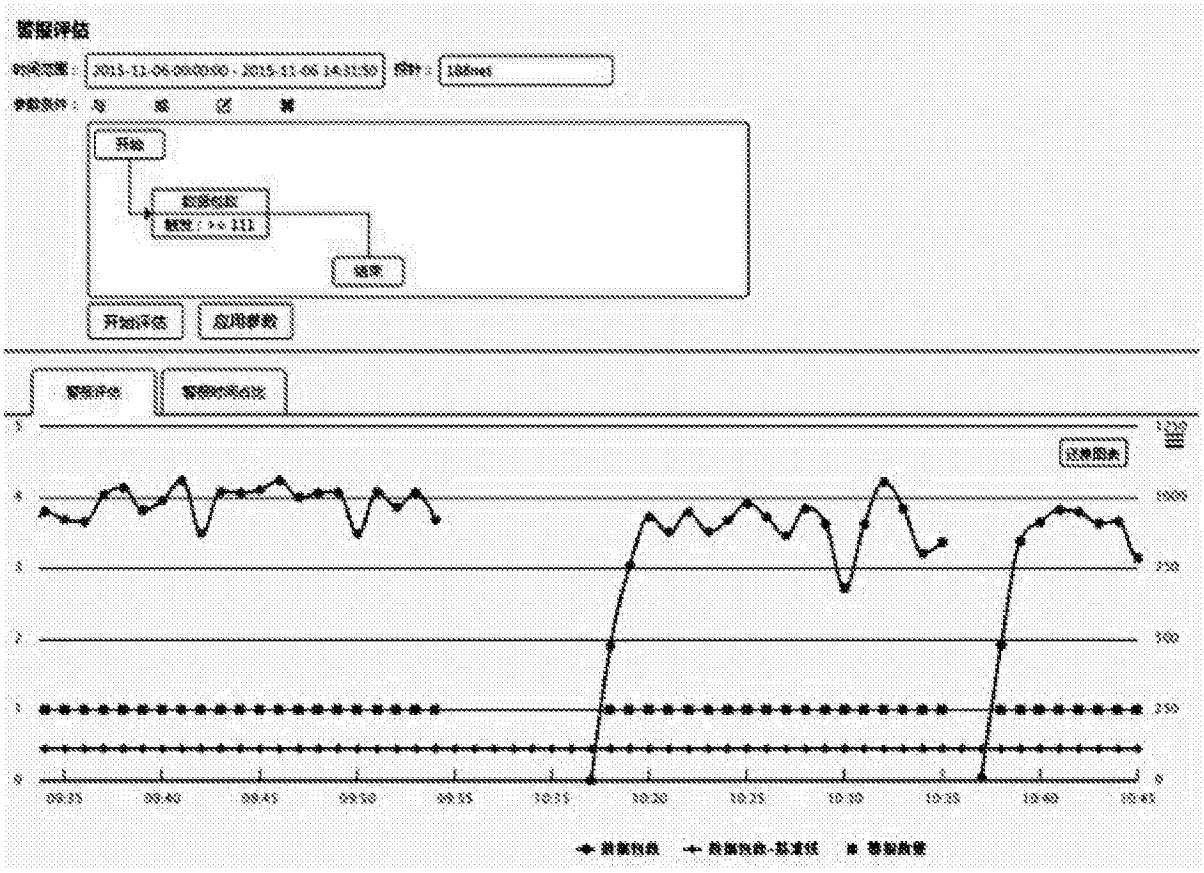


图5

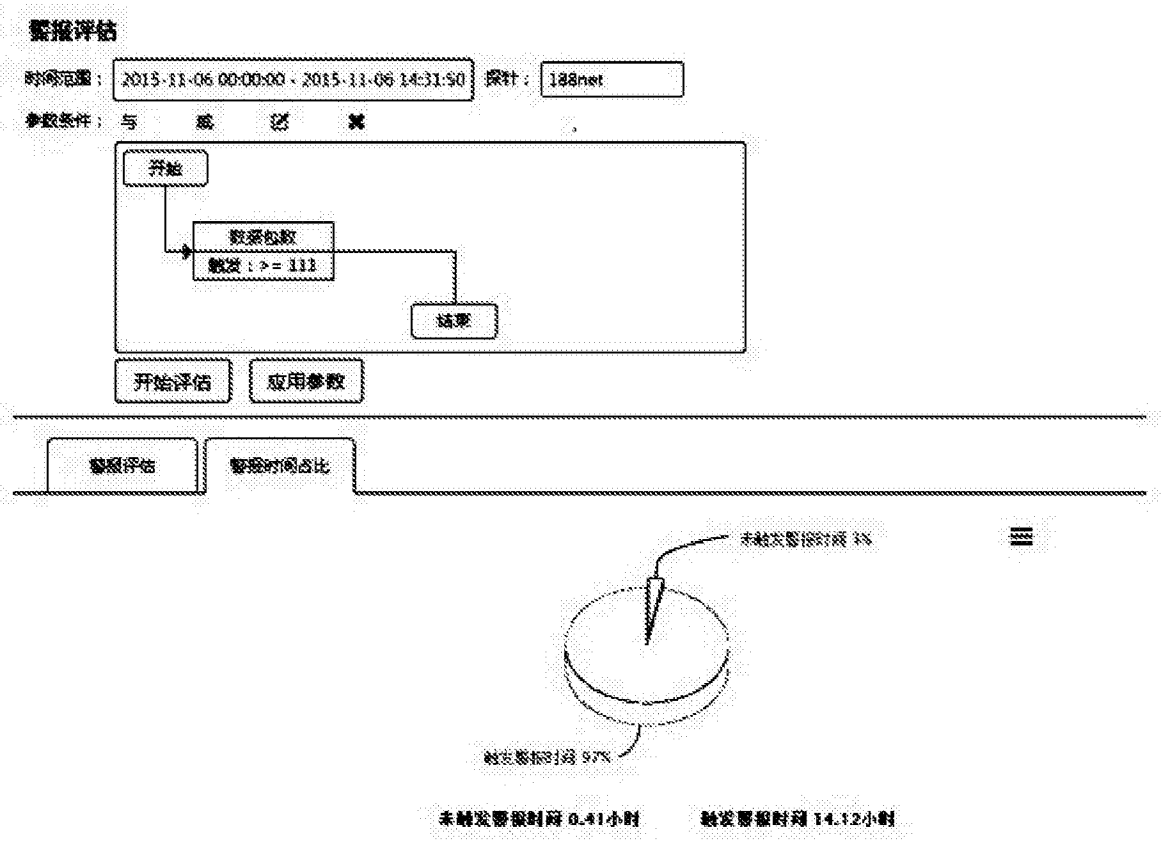

警报评估
2015-11-06 00:00:00 - 2015-11-06 14:31:50
188net
开始
结束
开始评估
应用参数
未触发警报时间 0.41小时
触发警报时间 14.12小时

图6