(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0067962
(43) 공개일자 2014년06월05일

(51) 국제특허분류(Int. Cl.)
H04L 12/26 (2006.01) *H04L 12/24* (2006.01)
(21) 출원번호 10-2013-7019843
(22) 출원일자(국제) 2012년01월31일
심사청구일자 2013년10월24일
(85) 번역문제출일자 2013년07월26일
(86) 국제출원번호 PCT/IB2012/050451
(87) 국제공개번호 WO 2012/114215
국제공개일자 2012년08월30일
(30) 우선권주장
11155862.3 2011년02월24일
유럽특허청(EPO)(EP)

(71) 출원인
인터내셔널 비지네스 머신즈 코포레이션
미국 10504 뉴욕주 아몬크 뉴오차드 로드
(72) 발명자
프랭클린, 데이비드, 리차드
영국 그레이터 런던 에스이1 9피제트, 런던, 사우스 뱅크, 76 어퍼 그라운드, 엠/피 데브, 아이비엠 유나이티드 킹덤 리미티드
스튜월트, 크리스티안, 존
영국 그레이터 런던 에스이1 9피제트, 런던, 사우스 뱅크, 76 어퍼 그라운드, 아이비엠 유나이티드 킹덤 리미티드
(뒷면에 계속)
(74) 대리인
허정훈

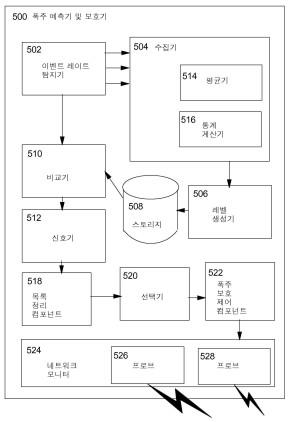
전체 청구항 수 : 총 27 항

(54) 발명의 명칭 **네트워크 이벤트 관리**

(57) 요 약

네트워크 이벤트 폭주를 예측하는 장치는 하나 또는 그 이상의 디바이스들로부터 이벤트 방출들의 레이트들을 탐지하는 이벤트 레이트 탐지기; 복수의 상기 디바이스들로부터 이벤트 방출들의 레이트들의 수집 레이트 및 수집 레이트 추세를 산출하는 수집기; 복수의 시간대들에 걸쳐 복수의 상기 수집 레이트 추세들의 최대 수용가능한 이벤트 레이트값들을 포함하는 복수의 레벨들을 생성하는 레벨 생성기; 상기 복수의 레벨들을 저장하기 위한 스토리지 컴포넌트; 현재 수집 레이트 추세를 상기 레벨들중 선택된 적어도 하나와 비교하기 위한 비교기; 및 상기 현재 수집 레이트 추세가 제1 시점에서 상기 레벨들중 선택된 적어도 하나를 초과할 것을 상기 비교기가 탐지하는 것에 응답하여 예측된 이벤트 폭주 신호를 보내는 신호기를 포함한다.

대 표 도 - 도5



(72) 발명자

딩거, 존

미국 노스캐롤라이나 27703-9135, 더럼, 사우스 마이애미 불러버드 3901, 엠/피 27703, 아이비엠 코포레이션

레이크, 존, 마이클

미국 노스캐롤라이나 27709, 리서치 트라이앵글 파크, 콘월리스 로드 3039, 피오 박스 12195, 디파트먼트 티81/빌딩 503, 아이비엠 코포레이션

특허청구의 범위

청구항 1

네트워크 이벤트 폭주 (a network event flood)를 예측하는 장치에 있어서, 상기 장치는:

하나 또는 그 이상의 디바이스들로부터 이벤트 방출들의 레이트들 (rates of event emissions)을 탐지하는 이벤트 레이트 탐지기 (an event rate detector);

복수의 상기 디바이스들로부터 이벤트 방출들의 상기 레이트들의 수집 레이트 (an aggregate rate) 및 수집 레이트 추세 (an aggregate rate trend)를 산출하는 수집기 (an aggregator);

복수의 시간대들에 걸쳐 (over plural time periods) 복수의 상기 수집 레이트 추세들의 최대 수용가능한 이벤트 레이트값들을 포함하는 복수의 레벨들을 생성하는 레벨 생성기 (a level generator);

상기 복수의 레벨들을 저장하기 위한 스토리지 컴포넌트 (a storage component);

현재 수집 레이트 추세 (a current aggregate rate trend)를 상기 레벨들중 선택된 적어도 하나와 비교하기 위한 비교기 (a comparator); 및

상기 현재 수집 레이트 추세가 제1 시점에서 (at a first point in time) 상기 레벨들중 선택된 적어도 하나를 초과할 것을 상기 비교기가 탐지하는 것에 응답하여 예측된 이벤트 폭주 신호를 보내는 신호기 (a signaller)를 포함하는

장치.

청구항 2

제 1항에 있어서, 상기 수집기는 평균 이벤트 레이트를 계산하기 위한 평균기 (an averager)를 포함하는

장치.

청구항 3

제 1항 또는 제 2항에 있어서, 상기 수집기는 통계적으로-정규화된 수집 레이트 또는 레이트 추세 (a statistically-normalized aggregate rate or rate trend)를 계산하기 위한 통계적 계산기 (statistical calculator)를 포함하는

장치.

청구항 4

제 3항에 있어서, 상기 통계적으로-정규화된 수집 레이트 또는 레이트 추세는 정규화된 추세를 정의하는

장치.

청구항 5

제 4항에 있어서, 상기 정규화된 추세는 최소-자승법 (a least-squares method)에 의하여 계산되는

장치.

청구항 6

상기 청구항들중 어느 한 항에 있어서, 상기 복수의 시간대는: 날중의 시간들 (times of day); 주중의 날들 (days of week); 월중의 날들 (days of month); 또는 연중의 날들 (days of year)중에서 하나 또는 그 이상에 따라 정의되는

장치.

청구항 7

상기 청구항들중 어느 한 항에 있어서, 이벤트 방출들의 최대 레이트를 상기 제1 시점에서 갖는 디바이스로부터 이벤트 방출들의 최소 레이트를 상기 제1 시점에서 갖는 디바이스 순으로 상기 디바이스들의 식별자들의 목록을 내림차순으로 정리하기 위하여 상기 신호기에 응답하는 정리 컴포넌트를 더 포함하는

장치.

청구항 8

제 7항에 있어서, 상기 목록으로부터 이벤트 방출들의 최대 레이트를 상기 제1 시점에서 갖는 상기 디바이스를 선택하고 폭주 보호 모드에 배치하기 위한 후보 디바이스로서 상기 디바이스를 식별하기 위한 제1 선택기를 더 포함하는

장치.

청구항 9

제 8항에 있어서, 상기 폭주 보호 모드는 수신기가 상기 디바이스로부터 이벤트 방출들의 감소된 레이트를 수용하게 하는

장치.

청구항 10

제 9항에 있어서, 상기 수신기는 네트워크 모니터를 포함하는

장치.

청구항 11

제 10항에 있어서, 상기 네트워크 모니터는 프로브를 포함하는

장치.

청구항 12

청구항 8에서 청구항 11중 어느 한 항에 있어서, 상기 후보 디바이스를 상기 폭주 보호 모드에 폭주 보호 디바이스로 배치하기 위한 폭주 보호 제어 컴포넌트 (a flood protection control component)를 더 포함하는

장치.

청구항 13

제 12항에 있어서, 이벤트 방출들의 최소 레이트를 제2 시점에서 갖는 폭주 보호 디바이스를 선택하고 상기 폭주 보호 모드로부터 제거를 위한 후보 디바이스로서 상기 디바이스를 식별하기 위한 제2 선택기를 더 포함하는

장치.

청구항 14

네트워크 이벤트 폭주 (a network event flood)를 예측하는 방법에 있어서, 상기 방법은:

하나 또는 그 이상의 디바이스들로부터 이벤트 방출들의 레이트들 (rates of event emissions)을, 이벤트 레이트 탐지기 (an event rate detector)에 의해서, 탐지하는 단계;

복수의 상기 디바이스들로부터 이벤트 방출들의 상기 레이트들의 수집 레이트 (an aggregate rate) 및 수집 레이트 추세 (an aggregate rate trend)를, 수집기 (an aggregator)에 의해서, 산출하는 단계;

복수의 시간대들에 걸쳐 (over plural time periods) 복수의 상기 수집 레이트 추세들의 최대 수용가능한 이벤트 레이트값들을 포함하는 복수의 레벨들을, 레벨 생성기 (a level generator)에 의해, 생성하는 단계;

상기 복수의 레벨들을, 스토리지 컴포넌트 (a storage component)에 의해서, 저장하는 단계;

현재 수집 레이트 추세 (a current aggregate rate trend)를 상기 레벨들중 선택된 적어도 하나와, 비교기 (a

comparator)에 의해서, 비교하는 단계; 및

상기 현재 수집 레이트 추세가 제1 시점에서 (at a first point in time) 상기 레벨들중 선택된 적어도 하나를 초과할 것을 상기 비교기가 탐지하는 것에 응답하여 예측된 이벤트 폭주를, 신호기 (a signaller)에 의해서, 신호로서 보내는 단계를 포함하는

방법.

청구항 15

제 14항에 있어서, 상기 수집하는 단계는 평균 이벤트 레이트를 계산하기 위한 평균기를 사용하는 단계를 포함하는

방법.

청구항 16

제 14항 또는 제 15항에 있어서, 상기 수집하는 단계는 통계적으로-정규화된 수집 레이트 또는 레이트 추세를 계산하기 위한 통계적 계산기를 사용하는 단계를 포함하는

방법.

청구항 17

제 16항에 있어서, 상기 통계적으로-정규화된 수집 레이트 또는 레이트 추세는 정규화된 추세를 정의하는

방법.

청구항 18

제 17항에 있어서, 상기 정규화된 추세는 최소-자승법 (a least-squares method)에 의하여 계산되는

방법.

청구항 19

청구항 14에서 청구항 18중 어느 한 항에 있어서, 상기 복수의 시간대들은: 날중의 시간들; 주중의 날들; 월중의 날들; 또는 연중의 날들중 하나 또는 그 이상에 따라 정의되는

방법.

청구항 20

청구항 14에서 청구항 19중 어느 한 항에 있어서, 상기 신호기에 응답하여, 이벤트 방출들의 최대 레이트를 상기 제1 시점에서 갖는 디바이스로부터 이벤트 방출들의 최소 레이트를 상기 제1 시점에서 갖는 디바이스순으로 상기 디바이스들의 식별자들의 목록을 내림차순으로, 정리 컴포넌트 (an ordering component)에 의해서, 정리하는 단계를 더 포함하는

방법.

청구항 21

제 20항에 있어서, 상기 목록으로부터 이벤트 방출들의 최대 레이트를 상기 제1 시점에서 갖는 상기 디바이스를 선택하고 폭주 보호 모드에 배치하기 위한 후보 디바이스로서 상기 디바이스를 식별하는 단계를 더 포함하는

방법.

청구항 22

제 21항에 있어서, 상기 폭주 보호 모드는 수신기가 상기 디바이스로부터 이벤트 방출들의 감소된 레이트를 수용하게 하는

방법.

청구항 23

제 22항에 있어서, 상기 수신기는 네트워크 모니터를 포함하는

방법.

청구항 24

제 23항에 있어서, 상기 네트워크 모니터는 프로브를 포함하는

방법.

청구항 25

청구항 21에서 청구항 24중 어느 한 항에 있어서, 상기 후보 디바이스를 폭주 보호 디바이스로서 상기 폭주 보호 모드에, 폭주 보호 제어 컴포넌트에 의하여, 배치하는 단계를 더 포함하는

방법.

청구항 26

제 25항에 있어서, 이벤트 방출들의 최소 레이트를 제2 시점에서 갖는 폭주 보호 디바이스를 선택하고 상기 폭주 보호 모드로부터 제거를 위한 후보 디바이스로서 상기 디바이스를 식별하는 단계를 더 포함하는

방법.

청구항 27

컴퓨터 프로그램에 있어서, 컴퓨터-판독가능 매체상에 저장된 컴퓨터 프로그램 코드를 포함하며, 상기 프로그램 코드는, 컴퓨터 시스템에 로드되어 실행될 때, 상기 컴퓨터 시스템이 청구항 14에서 청구항 26중 어느 한 항의 방법의 모든 단계를 수행하도록 하는

컴퓨터 프로그램.

명 세 서

기 술 분 야

[0001] 본 발명은 네트워크 이벤트 관리의 분야에 관련된 것이다. 특별히, 본 발명은 네트워크 이벤트 폭주 (flood)를 예측하여 예측된 폭주로부터 상기 네트워크를 보호하는 장치 및 방법에 관련된 것이다.

배 경 기 술

[0002] 사용가능한 네트워크 관리 시스템들은 많다. 이 시스템들은 네트워크에 걸쳐 이질적인 (disparate) 디바이스들로부터 오류 (fault) 정보를 수집하여 이 정보를 상호연관시키고 (correlate), 분류하고 (categorize), 우선순위를 매겨서 (prioritize) 오퍼레이터 (operator)가 상기 네트워크를 관리하고 그것을 효율적으로 보수 (repair)할 수 있는 형태로 제공한다 (present). 또한, 잠재적 미래의 문제들을 예측하기 위하여 기본적 예측 통계 분석 기법들을 네트워크 디바이스로들부터 수집된 운영 데이터 (operational data)에 적용해 왔다.

[0003] 네트워크 관리는 네트워크내 많은 디바이스들로부터 데이터를 수집하는 것을 포함한다. 알려진 실시예들은 이 작업을 수행하기 위하여 프로브들 (probes) 또는 에이전트들 (agents)과 같은 아주 다양한 모니터링 디바이스들을 사용하는데 이들은 여러 종류의 네트워크 디바이스들 및 시스템들로부터 많은 양의 소스 데이터를 제공해 줄 수 있다.

[0004] 매우 큰 네트워크들을 관리하는 문제들중 하나는 특히 네트워크 캐스케이드 오류 (network cascade failure)가 발생하면 매우 많은 수의 오류 이벤트들을 초래할 수 있는 네트워크 오류 모드들이 존재한다는 것이다. 많은 수의 오류 이벤트들은 네트워크 관리 시스템을 폭주하게 하여 (flood), 그것을 무응답 상태 (unresponsive)로 만들고 오퍼레이터가 오류의 근본 원인을 격리하거나 효율적으로 보수 노력에 우선순위를 매기는 것을 어렵게 한다. 기존의 해결책들에서 (solutions) 일단 상기 오류 이벤트 레이트 (fault event rate)가 주어진 스레시홀드 (threshold)를 초과하면 모니터하는 프로브 (다수의 다바이스들로부터 데이터를 수집한다)는 정지 (shutdown)를

개시하며, 레벨이 상기 스레시홀드이하로 떨어지면 재시작을 개시한다. 하지만, 이 시점까지 캐스케이드 실패(a cascade failure)가 종종 이미 발생하기 시작해서, 많은 다른 디바이스들이 상기 관리 시스템을 폭주하게 만들기 시작한다. 이 기본적 형태의 폭주 보호 (flood protection)가 활성화되기 전에 통상적으로 상기 시스템에는 상주하는 (resident) 많은 수의 오류 이벤트들이 이미 존재할 것이다. 불행하게도, 이러한 해결책은 또한 상기 네트워크를 보수하는데 필수적일 수 있는 정보를 포함한 많은 양의 데이터 손실을 초래한다.

[0005] 또한, 만약 상기 프로브가 다수 디바이스들을 모니터하게 되면, 비록 그들중 하나만이라도 이벤트 폭주를 산출하고 있다면, 모든 디바이스들로부터의 모든 데이터는 소실된다. 따라서, 프로브들이 데이터 폭주를 관리하는 방법에 관한 지능적 중앙 관리는 가능하지 않다.

[0006] 예를 들면, 미국특허번호 제 7539752호는 고정된 스레시홀드를 초과하는 이벤트수를 탐지하여 허용된 이벤트의 수를 줄이도록 (throttled back) 하는 것을 개시한다. 추가적인 사례로서, 미국특허출원번호 제 20100052924호는 고정된 스레시홀드를 초과하는 이벤트수를 탐지하여 이벤트 정보가 버퍼되도록 하는 것을 개시한다. 이것은 이벤트가 폭주하는 동안 시스템을 관리하는 정보가 이용가능하지 않게 됨을 의미한다.

[0007] 기존의 예측 분석 시스템들은 디바이스가 오류 조건을 조성하기 (develops) 전의 단순 진행 (progression)을 디스플레이하는 (display) 디바이스 메트릭스 (metrics)에만 종종 초점을 맞춘다. 예를 들면, 디스크 공간 또는 중앙처리장치 (central processing unit (CPU)) 사용에 대한 선형 추세 (linear trend)를 미래의 문제를 예측하도록 맞춘다든지 (fitting), 또는 비정상적 사용 (abnormal usage)을 표시하기 위하여 이 메트릭스에 대한 이력 (historical) 분석을 수행한다든지 하는 것이다. 다시 말해, 각각의 경우에 있어서, 비정상여부를 결정하기 위하여 상기 예측 데이터는 고정된 스레시홀드에 의존하고, 따라서 이 시스템들은 디바이스 특정 (device-specific) 오류 이벤트 레이트에는 적절하게 접근 (flexible approach) 할 수 없는데, 이는 이 방법이 정보를 수집하고 분석하기가 훨씬 어렵기 때문이다.

[0008] 그러므로, 종래 기술 (present state of the art)에 따른 네트워크 시스템에서 상기 문제들을 해결할 (address) 필요가 있다.

발명의 내용

과제의 해결 수단

[0009] 따라서, 본 발명은 제1 실시예에서, 네트워크 이벤트 폭주를 예측하는 장치를 제공하는데 이 장치는: 하나 또는 그 이상의 디바이스로부터 이벤트 방출들 (emissions)의 레이트들을 탐지하는 이벤트 레이트 탐지기 (event rate detector); 복수의 상기 디바이스들로부터 이벤트 방출들의 상기 레이트들의 수집 레이트 (an aggregate rate) 및 수집 레이트 추세 (an aggregate rate trend)를 산출하는 수집기 (an aggregator); 복수의 시간대들에 걸쳐 (over plural time periods) 복수의 상기 수집 레이트 추세들의 최대 수용가능한 이벤트 레이트값들을 포함하는 복수의 레벨들 (levels)을 생성하는 레벨 생성기 (a level generator); 상기 복수의 레벨들을 저장하기 위한 스토리지 컴포넌트; 현재 수집 레이트 추세 (a current aggregate rate trend)를 상기 레벨들중 선택된 적어도 하나와 비교하기 위한 비교기 (a comparator); 및 상기 현재 수집 레이트 추세가 제1 시점에서 (at a first point in time) 상기 레벨들중 선택된 적어도 하나를 초과할 것을 상기 비교기가 탐지함에 응답하여 (responsive to) 예측된 이벤트 폭주 신호를 보내는 (signalling) 신호기 (a signaller)를 포함한다.

[0010] 바람직하게도, 상기 수집기는 평균 이벤트 레이트를 계산하기 위한 평균기 (averager)를 포함한다. 바람직하게도, 상기 수집기는 통계적으로-정규화된 수집 레이트 또는 레이트 추세를 계산하기 위한 통계적 계산기를 포함한다. 바람직하게도, 상기 통계적으로-정규화된 수집 레이트 또는 레이트 추세는 정규화된 추세를 정의한다. 바람직하게도, 상기 정규화된 추세는 최소-자승법 (a least-squares method)에 의하여 계산된다. 바람직하게도, 상기 복수의 시간대들은: 날중의 시간들 (times of day); 주중의 날들 (days of week); 월중의 날들 (days of month); 또는 연중의 날들 (days of year)중 하나 또는 그 이상에 따라서 정의된다.

[0011] 상기 장치는 상기 신호기에 응답하여 이벤트 방출들의 최대 레이트를 상기 제1 시점에서 갖는 디바이스로부터 이벤트 방출들의 최소 레이트를 상기 제1 시점에서 갖는 디바이스 순으로 상기 디바이스들의 식별자들의 목록을 내림차순으로 정리하기 위한 (ordering) 정리 컴포넌트 (an ordering component)를 더 포함한다. 상기 장치는 이벤트 방출들의 최대 레이트를 상기 제1 시점에서 갖는 상기 목록으로부터 상기 디바이스를 선택하고 폭주 보호 모드에 배치하기 위한 후보 디바이스로서 상기 디바이스를 식별하기 위한 제1 선택기 (selector)를 더 포함한다. 바람직하게도, 상기 폭주 보호 모드는 수신기가 상기 디바이스로부터 이벤트 방출들의 감소된 레이트를

수용하도록 한다. 바람직하게도, 상기 수신기는 네트워크 모니터를 포함한다. 바람직하게도, 상기 네트워크 모니터는 프로브를 포함한다. 청구항 8에서 청구항 11중 어느 한 항에 있어서, 상기 장치는 상기 후보 디바이스를 폭주 보호 디바이스로서 상기 폭주 보호 모드에 배치하기 (placing) 위한 폭주 보호 제어 컴포넌트 (a flood protection control component)를 더 포함한다. 상기 장치는 이벤트 방출들의 최소 레이트를 제2 시점에서 갖는 폭주 보호 디바이스를 선택하고 상기 폭주 보호 모드로부터 제거를 위한 후보 디바이스로서 상기 디바이스를 식별하기 위한 제2 선택기를 더 포함한다.

[0012] 제2 실시예에서, 네트워크 이벤트 폭주를 예측하는 방법이 제공되는데 이것은: 이벤트 레이트 탐지기에 의하여, 하나 또는 그 이상의 디바이스들로부터 이벤트 방출 레이트를 탐지하는 단계; 복수의 상기 디바이스들로부터 이벤트 방출들의 상기 레이트들의 수집 레이트 및 수집 레이트 추세를, 수집기에 의하여, 산출하는 단계; 복수의 시간대들에 걸쳐 (over plural time periods) 복수의 상기 수집 레이트 추세들의 최대 수용가능한 이벤트 레이트값들을 포함하는 복수의 레벨들을, 레벨 생성기에 의하여, 생성하는 단계; 상기 복수의 레벨들을, 스토리지 컴포넌트에 의하여, 저장하는 단계; 현재 수집 레이트 추세를 상기 레벨들중 선택된 적어도 하나와, 비교기에 의하여, 비교하는 단계; 그리고 상기 현재 수집 레이트 추세가 제1 시점에서 상기 레벨들중 선택된 적어도 하나를 초과할 것을 상기 비교기가 탐지하는 것에 응답하여, 신호기에 의하여, 예측된 이벤트 폭주 신호를 보내는 단계를 포함한다.

[0013] 바람직하게도, 상기 수집 단계는 평균 이벤트 레이트를 계산하기 위해 평균기 (an averager)를 사용하는 단계를 포함한다. 바람직하게도, 상기 수집 단계는 통계적으로-정규화된 수집 레이트 또는 레이트 추세를 계산하기 위해 통계적 계산기 (a statistical calculator)를 사용하는 단계를 포함한다. 바람직하게도, 상기 통계적으로-정규화된 수집 레이트 또는 레이트 추세는 정규화된 추세를 정의한다. 바람직하게도, 상기 정규화된 추세는 최소-자승법에 의하여 계산된다. 바람직하게도, 상기 복수의 시간대들은 날중의 시간들; 주중의 날들; 월중의 날들; 또는 연중의 날들중 하나 또는 그 이상에 따라서 정의된다. 상기 방법은: 상기 신호기에 응답하여, 이벤트 방출들의 최대 레이트를 상기 제1 시점에서 갖는 디바이스로부터 이벤트 방출들의 최소 레이트를 상기 제1 시점에서 갖는 디바이스순으로 상기 디바이스들의 식별자들의 목록을 내림차순으로, 정리 컴포넌트에 의하여, 정리하는 단계를 더 포함한다. 상기 방법은 이벤트 방출들의 최대 레이트를 상기 제1 시점에서 갖는 상기 목록으로부터 상기 디바이스를 선택하고 폭주 보호 모드에 배치하기 위한 후보 디바이스로서 상기 디바이스를 식별하는 단계를 더 포함한다. 바람직하게도, 상기 폭주 보호 모드는 수신기가 상기 디바이스로부터 이벤트 방출들의 감소된 레이트를 수용하게 한다. 바람직하게도, 상기 수신기는 네트워크 모니터를 포함한다. 바람직하게도, 상기 네트워크 모니터는 프로브를 포함한다.

[0014] 상기 방법은 상기 후보 디바이스를 폭주 보호 디바이스로서 상기 폭주 보호 모드에 배치하는 폭주 보호 제어 컴포넌트에 의하여 수행되는 단계를 더 포함한다. 상기 방법은 이벤트 방출들의 최소 레이트를 상기 제2 시점에서 갖는 폭주 보호 디바이스를 선택하고 상기 폭주 보호 모드로부터 제거를 위한 후보 디바이스로서 상기 디바이스를 식별하는 단계를 더 포함한다.

[0015] 세번째 실시예에서, 하나의 컴퓨터 프로그램이 제공되는데 이것은 컴퓨터-판독가능 매체상에 저장된 컴퓨터 프로그램 코드를 포함하며, 컴퓨터 시스템에 로드되어 실행될 때, 상기 컴퓨터 시스템으로 하여금 상기 제2 실시예에 의한 방법의 모든 단계를 수행하도록 해준다.

도면의 간단한 설명

[0016] 본 발명의 바람직한 실시예가 다음에 첨부되는 도면들을 참조하여, 오직 예로서만, 기술될 것이다

도 1은 본 발명의 바람직한 실시예의 실행에 적합한 하나의 예시적인 다층 (multi-tiered) 네트워크 이벤트 관리 시스템의 다이어그램을 나타낸다;

도 2는 본 발명의 한 실시예에 의하여 레벨을 생성하는 하나의 방법을 단순화된 흐름도 (flowchart) 형태로 나타낸다;

도 3 및 4는 조합하여 본 발명의 한 실시예에 의하여 잠재적인 이벤트 폭주 문제를 해결하는 예시적인 하나의 방법을 단순화된 흐름도 형태로 나타낸다; 그리고

도 5는 본 발명의 한 실시예에 의하여 예를 들면 필드-프로그램가능 게이트 어레이 (a field-programmable gate array) 또는 어플리케이션-특정 (application-specific) 디바이스등의 하드웨어로, 또는 디바이스를 제어하도록 구성된 펌웨어로 구현될 수 있는 장치 또는 논리적 구성 (arrangement)을 단순화된 개념도 (schematic) 형태로

나타낸다.

발명을 실시하기 위한 구체적인 내용

[0017] 도 1은 본 발명의 바람직한 실시예의 구현에 적합한 하나의 예시적인 다층 (multi-tiered) 네트워크 이벤트 관리 시스템 (100)의 다이어그램을 나타낸다.

[0018] 모니터되는 디바이스들이 (102)에서 도시되는데; 이 예에서는, 프로브 1에 의하여 상기 디바이스들 (102) (디바이스1, 디바이스2... 디바이스 n)가 모니터된다.

[0019] 프로브 1은 프로브 104 세트들중의 하나이며 (프로브 1, 프로브 2... 프로브 m) 원시 오류 데이터 (raw fault data)를 모니터하고, 그것을 정규화된 오류 이벤트 (normalized fault events)로 전환하여 오브젝트서버들 (ObjectServers) (106)의 수집층 (collection layer)으로 보낸다.

[0020] 상기 수집층은 또한 디바이스 특정 (device specific) 폭주 보호가 켜질 수도 또는 꺼질 수도 있는 층이다. 층 (106)은 수집 오브젝트서버들의 층 (수집 오브젝트서버1, 수집 오브젝트서버2... 수집 오브젝트서버k)이다.

[0021] 수집 (Aggregation) 오브젝트서버 (108)은 이벤트 폭주에 의하여 가장 악영향을 받는 (most adversely affected) 네트워크 관리 시스템층이고, 그래서 이 층은 소켓 기반의 커뮤니케이션 시스템을 통하여 상기 프로브들을 제어하는 층이다.

[0022] 오브젝트서버들의 디스플레이층은 상세히 도시되지는 않지만, 디스플레이층에 대한 게이트웨이들 (gateways)은 도면번호 (110)에 도시되었다. 오브젝트서버들의 상기 디스플레이층은 이벤트 목록들 (Event Lists)에 데이터를 피드하는데 (feed) 이것들은 오퍼레이터들로 하여금 오류 데이터와의 상호작용을 하도록 허용한다.

[0023] 단일 오브젝트서버 시스템에서, 상기 프로브들은 모두 상기 오브젝트서버에 데이터를 피드하고 또한 그것에 의하여 제어된다.

[0024] 본 발명에 의한 하나의 바람직한 실시예에서, 디바이스 특정-오류 이벤트 레이트 데이터는 중앙으로 모인다. 이 데이터는 요약되어 저장되는데, 이는 디바이스 이벤트 레이트의 이력 데이터베이스를 구축하기 (build up) 위함이다. 이 이력 데이터는 선형 추세 알고리듬 및 이전 사용 기준선 (a baseline of previous usage)을 산출하는 알고리듬을 이용하여 분석된다. 동일 분석이 또한 전체적인 네트워크 이벤트 레이트를 위하여 수행되는데, 모든 개별 디바이스 이벤트 레이트를 합산함으로써 (summing) 수행된다. 이 프로세스는 하나 또는 그 이상의 레벨들의 설정을 허용하며, 이것은 여러 변화들 (variations)을 고려할 수 있는데, 예를 들어 날중의 시간들, 주중의 날들, 월중의 날들에 따른 변화들을 고려할 수 있고, 또는 이벤트 트래픽 (traffic) 양에서 계절적 변화들과 같은, 더 큰 시간대의 변화들 (variabilities)에 따라서도 변화들을 고려할 수 있다.

[0025] 도 2로 돌아오면, 본 발명의 한 실시예에 의하여 그러한 레벨을 생성하는 방법이 단순화된 흐름도 형태로 도시되어 있다.

[0026] 시작 (START) 단계 (200) 이후, (202)에서, 디바이스 이벤트 레이트 데이터가 컬렉트된다. 이 동작은 오랜 (protracted) 기간에 걸쳐 수행될 수 있으며, 이는 이벤트 레이트들이 앞에서 설명한 방식대로 시간에 따라 변화하기 때문에 이 이벤트 레이트들을 나타내는 이벤트 레이트 데이터의 상당히 많은 양 (an appropriately large quantity)을 추출하기 위해서이다. (204)에서, 상기 디바이스 이벤트 레이트 데이터가 저장되는데, 예를 들면, 데이터베이스와 같은 데이터 저장소 (store)에 저장되고, 이 데이터의 각 샘플은 시간 레퍼런스 (time reference)와 연관되어 있다. 디바이스 이벤트 레이트 데이터의 수집 (aggregation)을 위한 하나 또는 그 이상의 시간 레퍼런스들이 (206)에서 선택된다. 하나의 구체적인 사례로서, 디바이스 이벤트 레이트 데이터 수집을 위해 선택된 상기 시간 레퍼런스는, 전술한 바와 같이, 날중의 시간 레퍼런스 (a time of day reference), 주중의 일 레퍼런스 (a day of the week reference), 또는 이와 유사한 레퍼런스가 될 수도 있다. (208)에서, 선택된 하나 또는 그 이상의 시간 레퍼런스들에 대한 상기 디바이스 이벤트 레이트 데이터는 시스템 전체 이벤트 레이트 (a system-wide event rate)를 파악하기 (give) 위하여 수집되는데, 이것으로부터, (210)에서, 이벤트 레이트 데이터의 레벨 (예를 들어, 기준선 (baseline), 스레시홀드 또는 이력 최대 수용가능 레벨)이 산출되어 하나 또는 그 이상의 시간 레퍼런스들과 연관된다. 하나 또는 그 이상의 시간 기준들과 연관된 상기 레벨 이벤트 레이트 데이터는 (212)에서 저장되고, 상기 시스템은 계속 (CONTINUE) 단계 (214)에서 다른 프로세싱으로 계속 진행된다.

[0027] 이 이벤트 레이트 데이터는 이벤트 레이트 데이터의 추세를 예측하여 (trend) 특정 디바이스에서 잠재적인 미래

의 문제들을 예측하는 이벤트 정보를 산출하기 위해 사용된다. 그것은 또한 이전 동작 (previous activity)의 이력 기준선 (an historical baseline)을 파악하여 만약 동작에 현저한 변화가 있다면 오류 이벤트를 디스플레이하기 위해 사용된다. 결국, 전체 이벤트 레이트의 추세는, 오류 이벤트 관리 시스템을 압도하기 전에, 이벤트 폭풍을 일으킬 (an event storm building) 가능성이 존재하는지를 결정하도록 진행된다. 상기 특정 디바이스 이벤트 레이트 추세들은 그 다음에 상기 디바이스들로부터의 이벤트 피드들 (event feeds)을 감소된 이벤트 레이트 폭주 보호 모드로 자동적으로 배치시키도록 (put) 하기 위하여 사용된다. 일단, 상기 예측된 이벤트 폭주가 회피되면, 그 다음 상기 동일 기술들은 역으로 (in reverse) 디바이스 이벤트 피드들을 정상 운영으로 회복시키기 위하여 사용된다.

[0028] 상기 제어 (controlling) 오브젝트서버는 자동화된 프로세스를 운영하는데, 이 프로세스는 상기 오브젝트서버내 상주하는 특정 디바이스로부터 모든 오류 이벤트들의 탤리 (tally)에 변화를 추가한다 (adds up). 디바이스는 노드, 가령 네트워크상의 호스트 이름에 의하여 식별된다. 이로써 샘플 기간 동안 (예를 들면, 매 5분마다) 디바이스당 이벤트 레이트를 알 수 있다. 디바이스가 폭주 방지 모드에 배치되더라도, 상기 감소된 수의 이벤트들은 프로브에서 들어오는 이벤트들의 수를 반영하는 탤리 카운트들 (tally counts)을 증가시킨다. 이것은, 프로브에서 상기 폭주 모드가 어떠하든지간에, 상기 이벤트 레이트 계산은 상기 디바이스에 의하여 발생된 오류 이벤트의 수에 대하여 정확하다는 것을 의미한다.

[0029] 디바이스당 이벤트 레이트들은 타임 스탬프 (time stamp)와 함께 저장된다. 이러한 이력 기록은 이제 다음의 방식으로 분석된다:

[0030] 첫째, 최소-자승 라인 핏 (least-squared line fit) 또는 다른 통계적 핏 방법이 상기 디바이스 이벤트 레이트 추세의 근사값을 내는데 (approximate) 사용된다. 만약 상기 선형 추세 분석이 미래 주어진 시간내에 (예를 들어, 한 주) 수용가능한 (구성가능한) 스레시홀드를 초과할 것으로 나타낸다면, 그 다음 예측되는 오류 이벤트가 네트워크 관리 시스템내에 디스플레이되고, 오퍼레이터는 이 디바이스를 위한 해결 조치 (remedial action)에 우선순위를 두도록 (prioritize) 할 수 있다. 이로써 특정 디바이스로부터 들어오는 오류 이벤트들의 수가 증가함을 식별하고 이를 오퍼레이터에게 경보한다 (alerts).

[0031] 둘째, 디바이스를 위해 주중의 같은 날에 같은 시간으로부터의 이벤트 레이트들은 평균되어 이력 레벨 (an historical level)을 산출한다. 데이터의 두 개의 확장된 기간들 (two extended periods) (예를 들어 주들 (weeks))의 최소값이 이 레벨을 초기에 구축하는데 필요하다. 당업자에게는 자명하듯이, 평균이 되는 주들 데이터 (weeks' data)의 수는 구성가능하다 (configurable). 만약 상기 디바이스 오류 이벤트 레이트가 구성가능 분량만큼 (by a configurable amount) 이 디바이스에 대한 이력 레벨과 다르다면, 오류 이벤트는 네트워크 관리 시스템내에 디스플레이되어, 오퍼레이터가 이 디바이스를 위한 해결 조치에 우선순위를 두도록 할 수 있다. 이 테스트는 또한 "정상성의 회랑 (corridor of normality)"이라 불리며 하나의 시스템에서 주중, 월중, 등의 같은 시간 및 날에는 유사한 동작이 기대된다는 원칙에 기초한다. 이 어플리케이션 (application)에서, 상기 레벨 자체는 또한 네트워크를 개선하기 위한 도구로서 사용될 수 있는데, 그것은 동일 디바이스들이 각 기간 동안 동일 시간에 실패하는지를 보여줄 수 있을 것이기 때문이다. 이것은 오퍼레이터가 문제의 원인을 찾아내는데 (pinpoint) 도움을 줄 수 있다. 이것이 유용할 수 있는 전형적인 예는 디바이스들이 주말 동안 정지되고 월요일 아침 동일 시간에 기동 (brought up)하는 경우이며 - 이것은 차례로 가능한 네트워크 오류 이벤트들을 일으키는데, 이 이벤트들은 보통 무시할 수 있다. 만약 기계가 기동하는데 (come up) 실패하면 파괴적인 결과들을 가져올 수 있으며 상기 레벨 변화는 신속히 이를 식별할 것이다.

[0032] 당업자에게는 자명하듯이, 현재 추세를 기준선 또는 이력 최대 (a baseline or historical maximum)에 대하여 비교하는 것은 반복적 (iterative)일 수 있으며, 그 결과 특정 임시 상황 (a particular temporal situation)과 관련된 몇몇 기준선 또는 이력 최대 측정값이 설정되거나, 또는 어느 특정한 경우에 있어서 일부 추가적인 휴리스틱 (heuristic)을 적절한 레벨의 선택에 적용하는 것이 필요할 수도 있다. 예를 들어, 휴일 기간을 포함하는 네트워크 정지후 1월 1일 월요일에 시작하는 근무 주간을 상상해 보자. 바람직한 실시예에 따른 시스템에서는, 월요일을 위한 제1 레벨, 근무 주간의 첫째날을 위한 제2 레벨, 그리고 그 달의 첫째날을 위한 제3 레벨이 있을 수 있다. 이 상황에서, 본 발명의 바람직한 실시예는 사용할 적절한 레벨 또는 이력 최대를 선택하기 위해 규칙들을 정교하게 적용한다. 상기 규칙은, 예를 들면, 스레시홀드값을 결정하기 위해 최저의 레벨을 선택하기 위한 것일 수도 있다. 많은 대체적인 구성들은 당업자에게는 자명할 것이다.

[0033] 도 3 및 도 4는 다함께, 본 발명의 한 실시예에 따른 잠재적인 이벤트 폭주 문제를 해결하는 예시적인 방법을 단순화된 흐름도 형태로 도시한 것이다.

[0034] 상기 방법은 시작 단계 (300)에서 시작하고, 단계 (302)에서 디바이스 이벤트 레이트 데이터가 수집된다. (304)에서, 시스템 전체의 라인 핏 (a system-wide line fit)이 계산되는데, 바람직하게도, 예를 들어, 최소-자승 핏 (a least-squares fit) (304)를 사용한다. 테스트 단계 (306)에서, 전체 (total) 추세 레이트는 제1 미래 시스템 최대값과 비교된다. 당업자에게 자명하듯이, 상기 제1 미래 시스템 최대값과 관련된 기간은 특정 네트워크 시스템의 필요에 따라 구성될 수 있다. 바람직한 실시예의 레벨 구성요소에 관하여는 상기 설명으로부터 더욱 명백할 것이지만, 여기에서 최대값은 선택을 위해 적용가능한 규칙들에 따른 하나 또는 그 이상의 레벨값들로부터 선택되었을 것이다. 만약 상기 비교의 결과가 부정적이라면, 상기 프로세스는 단계 (411)에서 계속된다. 만약 상기 응답이 긍정적이라면, 단계 (310)에서, 각각의 디바이스에 대하여 라인 핏이 산출되고, 단계 (312)에서, 이 값은 제1 미래 시스템 최대 전체 이벤트 레이트의 기대되는 시점에서 디바이스당 이벤트 레이트 (the per device event rate)를 예측하는데 사용된다. 각 디바이스를 위해 단계 (312)에서 산출된 값은, 단계 (314)에서, 디바이스의 목록을 내림차순으로 (in descending order) 산출하는데 사용되고, 내림차순은 제1 미래 시스템 최대 전체 이벤트 레이트의 기대되는 시점에서 최대 디바이스당 이벤트 레이트를 갖는 디바이스로부터 제1 미래 시스템 최대 전체 이벤트 레이트의 기대되는 시점에서 최소 디바이스당 이벤트 레이트를 갖는 디바이스 순서로 한다. 단계 (316)에서, 폭주 보호 모드 상태에 있지 않은 최상위 디바이스 (타겟 디바이스)가 상기 목록으로부터 식별된다. 단계 (318)에서, 상기 타겟 디바이스를 위해 상주 오류 이벤트를 갖는 모든 프로브들을 찾고, 단계 (320)에서, 상기 타겟 디바이스는 폭주 보호 목록에 추가되는데, 이는 상기 디바이스를 모니터하는 각각의 프로브를 위해서이다. 단계 (322)에서, 상기 보호 목록은 모든 프로브들로 보내지고, 단계 (324)에서, 사용자 이벤트가 트리거되는데 (triggered), 이는 시스템 사용자에게 폭주 보호가 상기 디바이스를 위하여 활성화되었다는 것을 경보 (alert)해 주기 위함이다.

[0035] 상기 프로세스는 도 4의, 단계 (400)에서, 계속된다. 단계 (402)에서, 새로운 계산을 제공하기 위하여 상기 타겟 디바이스 이벤트 데이터가 시스템 전체의 추세 계산으로부터 제거되며, 테스트 단계 (404)에서, 시스템을 위해 그 결과로 나온 추세 레이트 (the resultant trend rate)는 상기 제1 미래 시스템 최대값과 비교된다. 만약 테스트 단계 (404)에서의 결정이 부정적이라면, 상기 프로세스는 시작 단계 (300)으로 되돌아온다. 만약 테스트 단계 (404)의 결과가 긍정적이라면, 테스트 단계 (408)에서, 모든 디바이스들이 이미 폭주 보호 모드에 있는지에 관한 결정이 이루어진다. 만약 상기 결정이 부정적이라면, 상기 프로세스는 단계 (315)로 되돌아온다. 만약 상기 결정이 긍정적이라면, 테스트 단계 (412)에서, 추가적인 (further) 테스트가 수행되어 단계 (402)에서 결과로 나온 (resultant) 추세 레이트가 다음의 미래 시스템 최대값보다 큰지를 결정한다. 만약 상기 결정이 긍정적이라면, 상기 프로세스는 시작 단계 (300)으로 되돌아온다. 만약 상기 결정이 부정적이라면, 단계 (416)에서 디바이스당 라인 핏 (a per device line fit)이 계산되고, 단계 (418)에서, 디바이스당 이벤트 레이트가 단기간에 걸쳐 예측된다. 각 디바이스를 위해 산출된 값은 디바이스의 목록을 내림차순으로 산출하는데 사용되며, 이때 내림차순의 순서는 최대 디바이스당 이벤트 레이트를 갖는 디바이스로부터 최소 디바이스당 이벤트 레이트를 갖는 디바이스로 한다. 단계 (422)에서, 폭주 보호 모드 상태에 있는 상기 목록내 최하위 디바이스 (the lowest device)를 찾아 타겟 디바이스가 되도록 한다. 단계 (424)에서, 상기 타겟 디바이스는 그것을 모니터하는 모든 프로브들을 위해 상기 보호 목록으로부터 제거되며, 단계 (426)에서, 상기 보호 목록은 모든 프로브들로 보내진다. 단계 (428)에서, 사용자 이벤트가 트리거되어 시스템 사용자에게 폭주 보호가 상기 디바이스를 위해 비활성화되었다는 것을 통지하고, 단계 (430)에서, 상기 프로세스는 시작 단계 (300)으로 되돌아온다.

[0036] 다음의 슈도-코드 명세 (pseudo-code specification)는 당업자에게 좀 더 상세하고 익숙한 용어 및 스트럭처로, 지능 폭주 제어 알고리듬이 24시간으로 셋팅된 단기간 및 48시간으로 셋팅된 좀 더 긴 기간을 갖는 하나의 예시적인 시스템에서 어떻게 작동하는지를 설명한다.

[0037] 1. 이벤트 레이트 샘플 기간의 구성가능한 수 (a configurable number)를 대기한다.

[0038] 2. 지난 24시간 (the last 24 hours)*동안 전체 이벤트 레이트 데이터합의 최소-자승 라인 핏 (a least-squared line fit)을 산출한다.

[0039] 3. 상기 추세가 전체 이벤트 레이트가 오브젝트서버가 다음 24시간*내에 처리할 수 있는, 선택된 기준선에 따라 조정된, 최대값을 초과할 것이라고 예측하는가?

[0040] 4. 만약 그렇지 않으면, 17로 간다.

[0041] 5. 각 디바이스를 위해 이벤트 데이터 레이트의 최소-자승 핏을 산출한다.

[0042] 6. 전체 이벤트 레이트가 오브젝트서버가 처리할 수 있는, 선택된 기준선에 따라 조정된, 최대값을 초과할 시점

에서 (at the time) 각 디바이스를 위해 예측된 이벤트 레이트를 계산한다.

[0043] 7. 예측된 이벤트 레이트에 관하여 정리된 (sorted) 디바이스들의 목록을 산출한다. 첫번째가 최상위이다.

[0044] 8. 아직 폭주 보호 모드에 있지 않은 제1 디바이스를 찾는다.

[0045] 9. 상주 이벤트를 사용하여 이 디바이스를 위해 상주 오류 이벤트들을 산출한 모든 프로브들을 찾는다.

[0046] 10. 디바이스를 모니터하는 모든 프로브들을 위해 디바이스의 이름을 폭주 보호 목록에 추가한다.

[0047] 11. 폭주 보호 목록(들)을 프로브(들)로 보낸다.

[0048] 12. 디바이스가 폭주 보호 모드에 배치되었다는 것을 표시해서 사용자가 시스템이 자동으로 행한 것을 알도록 하는 이벤트를 산출한다.

[0049] 13. 전체적인 이벤트 레이트 최소-자승 추세 (the total event rate least-squared trend)로부터 디바이스 이벤트 레이트를 차감한다.

[0050] 14. 상기 새로운 추세는 전체 이벤트 레이트가 오브젝트서버가 다음 24시간*내에 처리할 수 있는, 선택된 기준선에 따라 조정된, 최대값을 초과할 것을 예측하는가?

[0051] 15. 만약 그렇다면, 그리고 모든 디바이스들이 폭주 보호 모드에 있지 않다면, 8로 간다.

[0052] 16. 1로 간다.

[0053] 17. 상기 추세는 전체 이벤트 레이트가 오브젝트서버가 다음 48시간*내에 처리할 수 있는, 선택된 기준선에 따라 조정된, 최대값을 초과할 것을 예측하는가?

[0054] 18. 만약 그렇다면, 1로 간다.

[0055] 19. 각 디바이스를 위하여 이벤트 데이터 레이트의 최소-자승 핏을 산출한다.

[0056] 20. 24시간 타임*내 각 디바이스를 위한 예측된 이벤트 레이트를 계산한다.

[0057] 21. 예측된 이벤트 레이트에 관하여 정리된 디바이스의 목록을 산출한다. 첫번째가 최상위이다.

[0058] 22. 폭주 보호 모드에 있는 목록에서 마지막 (last) 디바이스를 찾는다.

[0059] 23. 상기 디바이스 이름을 그 디바이스를 모니터하는 모든 프로브들을 위해 폭주 보호 목록으로부터 제거한다. 단계 9에서 처리동안 이 디바이스를 위해 발견된 프로브들을 사용한다.

[0060] 24. 상기 폭주 보호 목록(들)을 프로브(들)로 보낸다.

[0061] 25. 디바이스가 폭주 보호 모드로부터 벗어났다는 것을 표시하여, 사용자가 시스템이 자동으로 행한 것을 알도록 하는 레절루션 (resolution) 이벤트를 산출한다.

[0062] 26. 1로 간다.

[0063] *시간들의 수는 조정될 수 있다.

[0064] 도 5로 돌아와서, 도 5는, 본 발명의 한 실시예에 따라, 디바이스를 제어하도록 구성된 하드웨어로, 예를 들어, 필드-프로그램가능 게이트 어레이 또는 어플리케이션-특정 디바이스로 구현되거나 또는 펌웨어로 구현될 수 있는 장치 또는 논리적 구성을 도시하고 있다.

[0065] 도 5의 장치는 이벤트 레이트 데이터를 수집기 (504)에 제공하는 이벤트 레이트 탐지기 (502)를 갖는 네트워크 폭주 예측기 및 보호기 메커니즘 (500)을 포함한다. 수집기 (504)는 데이터를 수집하는데 (aggregate), 바람직하게 평균기 (514) 및 통계 계산기 (516)에 의하여 데이터를 수집하며, 상기 수집된 데이터를 레벨 생성기 (506)에 제공한다. 레벨 생성기 (506)은 스토리지 (508)에 생성된 레벨들을 저장한다. 비교기 (510)은 이벤트 레이트 탐지기 (502)로부터 현재의 이벤트 레이트 데이터를 수신하여 그것을 스토리지 (408)에 저장된 하나 또는 그 이상의 레벨들과 비교하도록 구성된다. 예측된 이벤트 폭주를 표시하는 비교기 (510)에 의하여 산출된 비교 결과에 기초하여, 신호기 (512)는 메커니즘 (500)의 폭주 보호기 부분을 포함하는 컴포넌트들에 신호를 보내게 되는데 (is prompted to), 상기 예측된 이벤트 폭주에 대한 그들의 상대적인 기대 기여 (relative expected contribution)를 표시하는 기준에 따라 디바이스들의 정리된 목록 (an ordered list)을 산출하기 위해 목록 정리 컴포넌트 (518)에서 조치를 시작하도록 함으로써 그렇게 한다. 목록 정리 컴포넌트 (518)은 그것의 정리된

목록을 선택기 (520)에 제공하는데, 이것은 폭주 보호 모드에 배치될 디바이스 또는 디바이스들을 선택하고 폭주 보호 제어 컴포넌트 (522)가 네트워크 모니터 (524)에 적절한 명령들 (commands)을 발행하도록 한다. 네트워크 모니터 (524)는 차례로 (in turn) 프로브 (526), (528)등에서 이벤트들의 수용을 제어한다.

[0066] 그러므로, 만약 전체적인 시스템에 대한 선형 추세 (the linear trend)가 상기 네트워크 관리 시스템이 다음 24시간 (이것은 다른 시간 기간들에 대해서도 설정될 수 있다)내에 데이터의 폭주에 의하여 압도될 것이라는 것을 표시하면, 각 디바이스에 대한 상기 추세들을 분석하여 이 미래 폭주에 가장 큰 기여를 제공하는 디바이스를 찾는다. 그 다음 이 디바이스를 모니터하는 프로브는 이 디바이스로부터의 데이터의 레이트를 감소시키라는 명령을 송신받고, 오류 이벤트가 상기 네트워크 관리 시스템에 디스플레이되어 상기 변화가 표시된다.

[0067] 그 다음 전체 시스템 추세 분석이 반복되는데, 계산에서 상기 디바이스를 포함하지 않은 채로 반복된다. 만약 상기 전체 시스템으로부터 이 디바이스를 제거해도 주어진 타임 프레임내에서 시스템을 압도할 것이라는 미래의 추세가 여전히 나오게 된다면, 상기 폭주에 대하여 다음으로 최고의 (the next highest) 기여를 산출할 것으로 예측되는 디바이스가 이벤트 감소 모드에 배치될 것이다 (put into). 이 프로세스는 반복되는데, 상기 전체 네트워크 관리 시스템이 예측되는 캐스케이드 고장 (cascade failure)에 의하여 더 이상 폭주되지 않는 상태가 될 때까지 반복된다.

[0068] 이벤트 레이트 데이터는 모든 네트워크 디바이스들로부터 수집되는데, 그들이 폭주 보호 모드에 배치되었는지 아닌지 간에 수집된다. 만일 전체 추세가 상기 전체 시스템이 좀 더 긴 시간내에, 말하자면 48시간내에 폭주되지 않을 것이라는 것을 표시한다면, 폭주 보호 모드에 있는 디바이스로부터의 오류 이벤트 데이터는 정상 운영 (normal operation)으로 회복된다. 디바이스 오류 이벤트들은 최하위 이벤트 레이트 추세들을 갖는 이벤트들이 첫째로 정상 운영으로 돌아오는 식으로 회복된다. 상기 변화를 표시하는 하나의 레절루션 이벤트가 상기 관리 시스템에 추가된다. 디바이스들을 폭주 보호 모드에 추가할 때보다 더 긴 예측 기간이 사용되는 이유는 상기 전체 추세에서 경미한 변동 (slight fluctuations)이 있을 때 상기 디바이스들이 계속적으로 (constantly) 보호 모드 안팎으로 (in and out of protection mode) 스위치되지 않도록 하기 위해서이다.

[0069] 본 발명의 바람직한 실시예들은 상기 네트워크 관리 시스템이 얼마나 많은 데이터를 처리할 수 있는지를 자동적으로 그리고 지능적으로 관리할 수 있게 해준다. 이것은 심지어 극심한 이벤트 폭주 상황하에서도, 상기 네트워크 관리 시스템이 응답할 수 있고 (responsive), 정보를 제공하며 (informative) 또한 유용함을 보장한다.

[0070] 본 발명의 바람직한 실시예의 전부 또는 일부의 방법은 상기 방법의 단계들을 수행하기 위하여 구성된 논리적 구성 요소들 (elements)을 포함하여, 하나의 장치 또는 복수의 논리적 장치들에서 적절히 그리고 유용하게 구현될 수가 있으며 또한 상기 논리적 구성 요소들은 하드웨어 컴포넌트들, 펌웨어 컴포넌트들 또는 그것들의 조합을 포함할 수 있슴은 당업자에게 자명할 것이다.

[0071] 본 발명의 바람직한 실시예에 따라서 전부 또는 일부의 논리적 구성은 상기 방법의 단계들을 수행하기 위한 논리적 구성 요소들을 포함하는 하나의 논리적 장치에서 적절히 구현될 수가 있으며, 또한 상기 논리적 구성 요소들은 논리 게이트와 같은 컴포넌트들, 예를 들면, 프로그램가능한 논리적 어레이 또는 어플리케이션-특정 집적 회로와 같은 컴포넌트들을 포함할 수 있슴은 당업자에게 마찬가지로 자명할 것이다. 상기 하나의 논리적 구성은 또한 그러한 어레이 또는 회로에서 일시적으로 또는 영구적으로 논리적 스트럭처들을, 설정하도록 인에이블링 구성 요소들 (enabling elements)내에서 구현될 수 있고, 그러한 설정은 예를 들어, 가상 하드웨어 디스크립터 언어 (virtual hardware descriptor language)를 사용하여 할 수 있으며, 이 언어는 고정 또는 전송가능한 캐리어 매체를 사용하여 저장 및 전송될 수 있다.

[0072] 위에서 설명된 상기 방법 및 구성은 하나 또는 그 이상의 프로세서들 (도면에서는 도시되지 않음)상에서 실행되는 소프트웨어로 또한 적절하게 전부 또는 일부 수행될 수 있으며, 또한 소프트웨어는 자기 또는 광학 디스크등과 같은 어떤 적합한 데이터-캐리어 (역시 도면에서는 도시되지 않음)상에 운반되는 하나 또는 그 이상의 컴퓨터 프로그램의 구성 요소들의 형태로 제공될 수 있다는 것을 이해할 수 있다. 데이터의 전송을 위한 채널들은 마찬가지로, 유무선 신호-운반 매체 (wired or wireless signal-carrying media)와 같은 신호-운반 매체뿐만 아니라 모든 설명된 저장 매체를 포함한다.

[0073] 본 발명은 또한 컴퓨터 시스템에서 사용될 컴퓨터 프로그램 제품으로서 적절히 구현될 수 있다. 상기 구현 (implementation)은 일련의 컴퓨터 판독-가능 명령들을 포함할 수 있고, 이 명령들은 예를 들면, 디스켓, CD-ROM, ROM, 또는 하드 디스크와 같은 컴퓨터 판독가능 매체와 같은 유형의 (tangible) 매체에 고정될 수도 있거나, 또는 모뎀이나 기타 인터페이스 디바이스를 통하여 컴퓨터 시스템에 전송가능하게 될 수 있는데, 이러한 전

송은, 광학 또는 아날로그 통신 라인등을 포함하나 이에 국한되지 않는 유형의 매체를 통해서, 또는 마이크로웨이브, 적외선 또는 기타 전송 기술등을 포함하나 이에 국한되지 않는 무선의 기술을 사용하여 무형으로(intangibly) 할 수 있다. 상기 일련의 컴퓨터 판독가능 명령들은 이전에 설명된 기능의 전부 또는 일부를 구현한다.

[0074] 당업자는 상기 컴퓨터 판독가능 명령들이 많은 컴퓨터 아키텍처들 또는 운영 체제들에서 사용되는 다수의 프로그래밍 언어들로 쓰여질 수 있다는 것을 이해할 것이다. 또한, 상기 명령들은 반도체, 자기 또는 광학등을 포함하나 이에 국한되지 않는, 현재 또는 미래의, 어떠한 메모리 기술을 사용하여 저장될 수 있고, 또는 광학, 적외선 또는 마이크로웨이브등을 포함하나 이에 국한되지 않는, 현재 또는 미래의, 어떠한 통신 기술을 사용하여 전송될 수 있다. 상기 컴퓨터 프로그램 제품은, 예를 들면, 시스템 ROM 또는 고정 디스크상에 컴퓨터 시스템에 의해 사전-로드되어 (pre-loaded), 동반하는 인쇄된 또는 전자 문서, 예를 들면, 쉬링크-랩된 (shrink-wrapped) 소프트웨어와 함께 착탈식 매체로서 배포될 수도 있고, 또는, 예를 들어, 인터넷 또는 월드와이드웹과 같은 네트워크를 통해서 서버 또는 전자 게시판 (electronic bulletin board)으로부터 배포될 수 있다 (distributed).

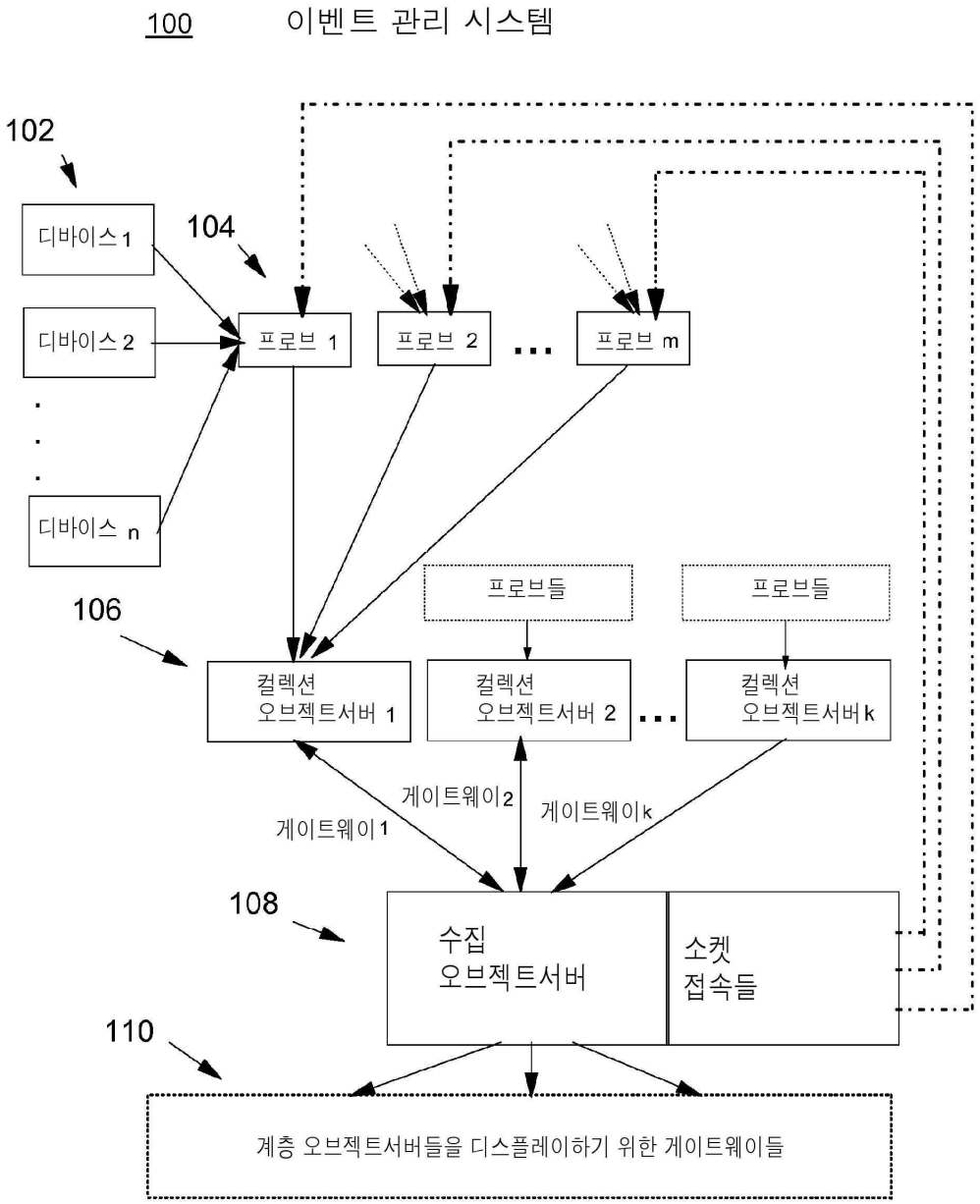
[0075] 한 가지 대체 실시예로서, 본 발명의 바람직한 실시예는 서비스를 제공하는 (deploying) 컴퓨터 구현 방법의 형태로 실현될 수 있는데, 이 서비스는 컴퓨터 인프라스트럭처 (infrastructure)에 제공되어 실행될 때, 상기 컴퓨터 시스템이 상기 방법의 모든 단계를 수행할 수 있도록 동작가능한 컴퓨터 프로그램 코드를 제공하는 단계를 포함한다.

[0076] 다른 대안으로서, 본 발명의 바람직한 실시예는 기능적인 데이터를 그 안에 갖는 데이터 캐리어 (carrier)의 형태로 실현될 수 있는데, 상기 기능적인 데이터는, 컴퓨터 시스템에 로드되어 동작될 때, 상기 컴퓨터 시스템이 상기 방법의 모든 단계를 수행할 수 있게 해주는 기능적인 컴퓨터 데이터 스트럭처를 포함한다.

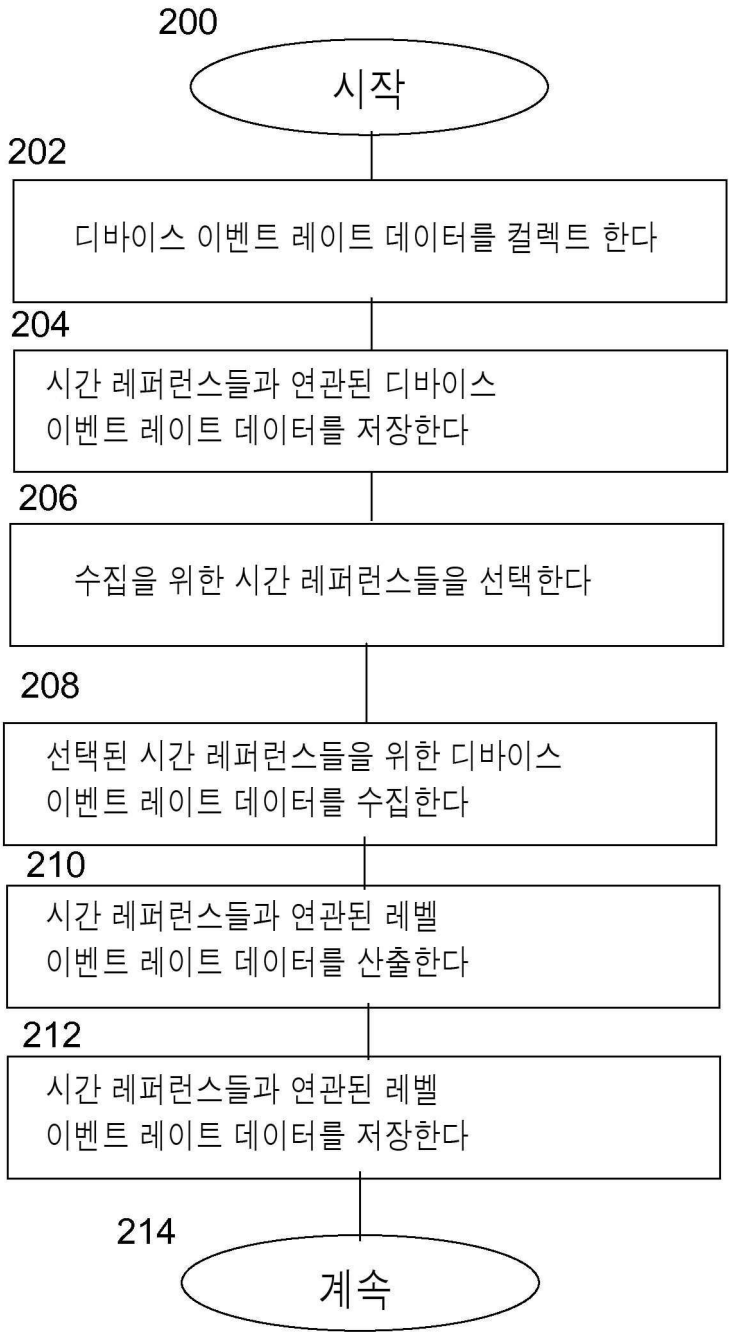
[0077] 본 발명의 범위를 벗어나지 않고 상기 예시적인 실시예들에 대한 많은 개량들과 변형들이 만들어질 수 있슴은 당업자에게 자명할 것이다.

도면

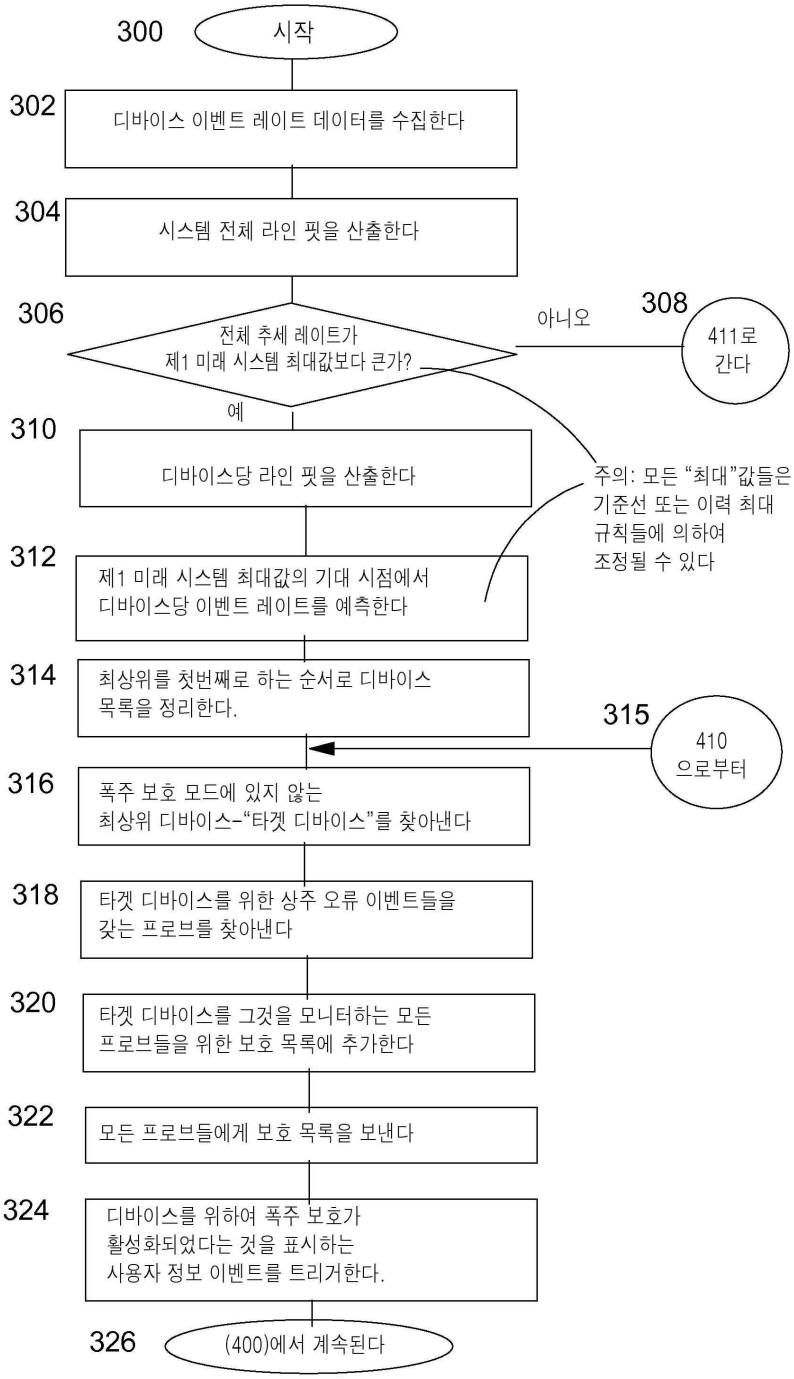
도면1


100
이벤트 관리 시스템
102
디바이스 1
104
디바이스 2
디바이스 n
프로브 1
프로브 2
프로브 m
106
프로브들
프로브들
컬렉션 오브젝트서버 1
컬렉션 오브젝트서버 2
컬렉션 오브젝트서버 k
게이트웨이 1
게이트웨이 2
게이트웨이 k
108
수집 오브젝트서버
소켓 접속들
110
계층 오브젝트서버들을 디스플레이하기 위한 게이트웨이들

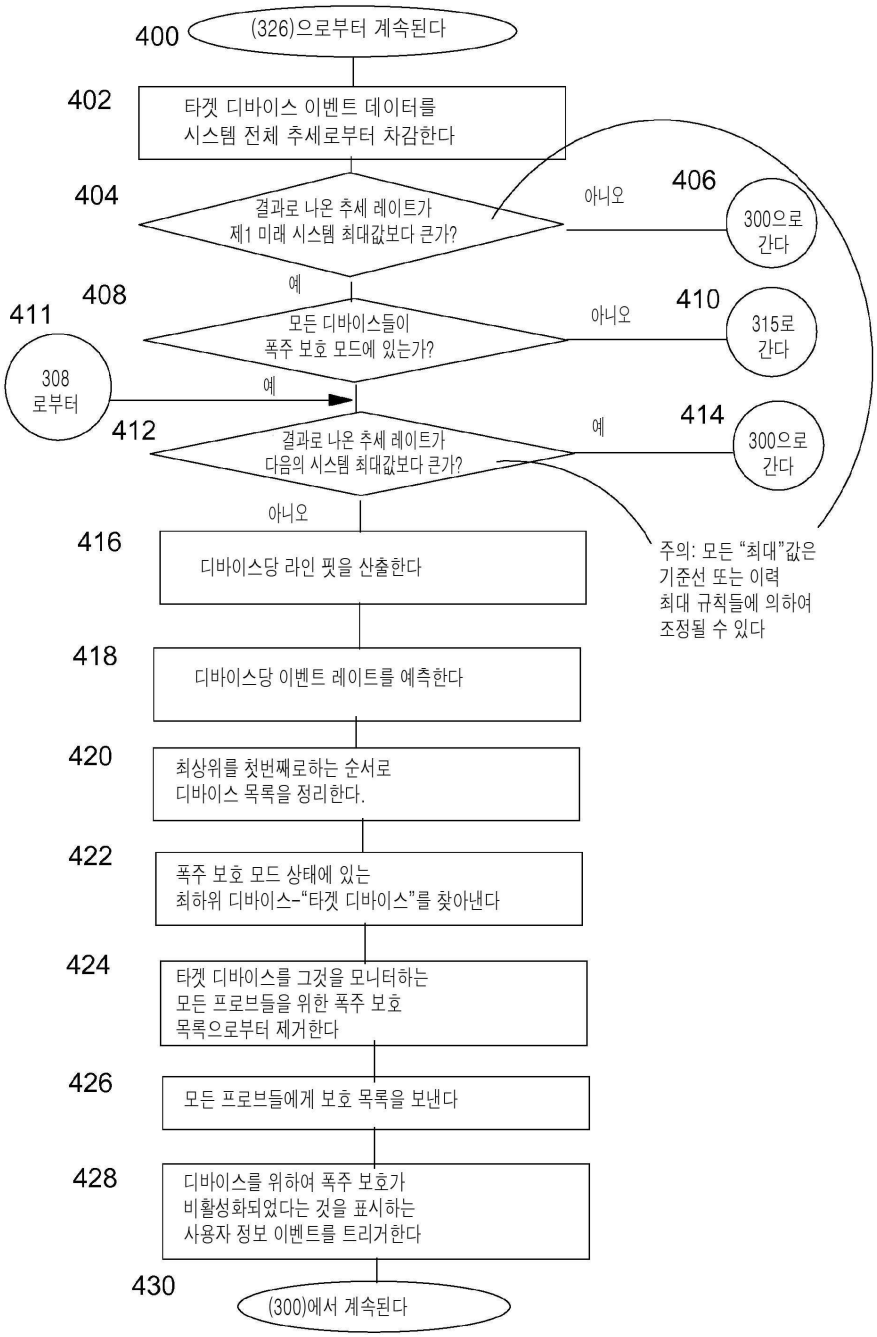
도면2


200
시작
202
디바이스 이벤트 레이트 데이터를 컬렉트 한다
204
시간 레퍼런스들과 연관된 디바이스
이벤트 레이트 데이터를 저장한다
206
수집을 위한 시간 레퍼런스들을 선택한다
208
선택된 시간 레퍼런스들을 위한 디바이스
이벤트 레이트 데이터를 수집한다
210
시간 레퍼런스들과 연관된 레벨
이벤트 레이트 데이터를 산출한다
212
시간 레퍼런스들과 연관된 레벨
이벤트 레이트 데이터를 저장한다
214
계속

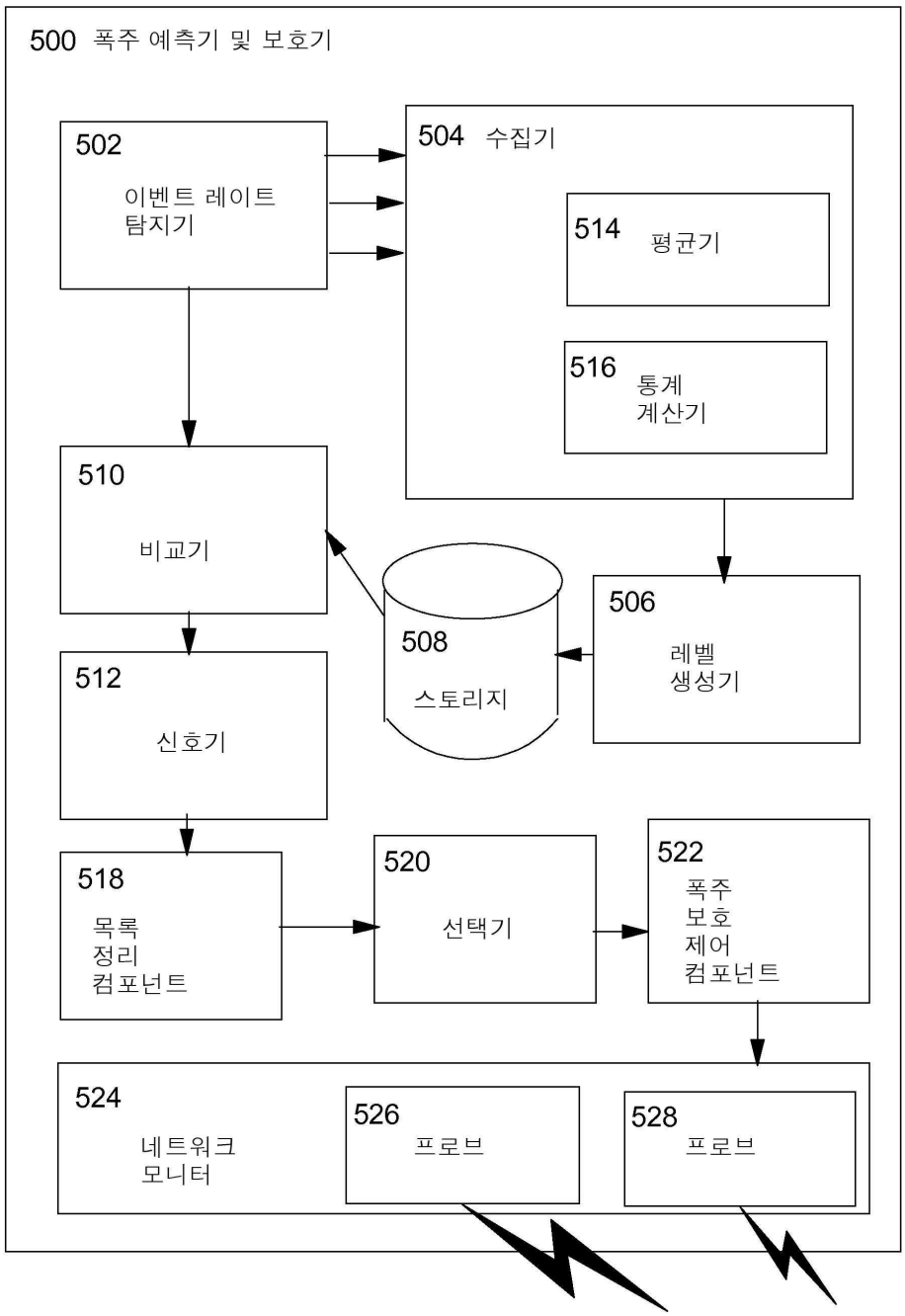
도면3


300
시작
302
디바이스 이벤트 레이트 데이터를 수집한다
304
시스템 전체 라인 핏을 산출한다
306
전체 추세 레이트가
제1 미래 시스템 최대값보다 큰가?
아니오
308
411로
간다
예
310
디바이스당 라인 핏을 산출한다
주의: 모든 "최대"값들은
기준선 또는 이력 최대
규칙들에 의하여
조정될 수 있다
312
제1 미래 시스템 최대값의 기대 시점에서
디바이스당 이벤트 레이트를 예측한다
314
최상위를 첫번째로 하는 순서로 디바이스
목록을 정리한다.
315
410
으로부터
316
폭주 보호 모드에 있지 않는
최상위 디바이스-"타겟 디바이스"를 찾아낸다
318
타겟 디바이스를 위한 상주 오류 이벤트들을
갖는 프로브를 찾아낸다
320
타겟 디바이스를 그것을 모니터하는 모든
프로브들을 위한 보호 목록에 추가한다
322
모든 프로브들에게 보호 목록을 보낸다
324
디바이스를 위하여 폭주 보호가
활성화되었다는 것을 표시하는
사용자 정보 이벤트를 트리거한다.
326
(400)에서 계속된다

도면4


400
(326)으로부터 계속된다
402
타겟 디바이스 이벤트 데이터를
시스템 전체 추세로부터 차감한다
404
결과로 나온 추세 레이트가
제1 미래 시스템 최대값보다 큰가?
아니오
406
300으로
간다
예
408
411
308
로부터
모든 디바이스들이
폭주 보호 모드에 있는가?
아니오
410
315로
간다
예
412
결과로 나온 추세 레이트가
다음의 시스템 최대값보다 큰가?
예
414
300으로
간다
아니오
416
디바이스당 라인 핏을 산출한다
418
디바이스당 이벤트 레이트를 예측한다
420
최상위를 첫번째로하는 순서로
디바이스 목록을 정리한다.
422
폭주 보호 모드 상태에 있는
최하위 디바이스-"타겟 디바이스"를 찾아낸다
424
타겟 디바이스를 그것을 모니터하는
모든 프로브들을 위한 폭주 보호
목록으로부터 제거한다
426
모든 프로브들에게 보호 목록을 보낸다
428
디바이스를 위하여 폭주 보호가
비활성화되었다는 것을 표시하는
사용자 정보 이벤트를 트리거한다
430
(300)에서 계속된다
주의: 모든 "최대"값은
기준선 또는 이력
최대 규칙들에 의하여
조정될 수 있다

도면5


500 폭주 예측기 및 보호기
502
이벤트 레이트
탐지기
504 수집기
514 평균기
516
통계
계산기
510
비교기
508
스토리지
506
레벨
생성기
512
신호기
518
목록
정리
컴포넌트
520
선택기
522
폭주
보호
제어
컴포넌트
524
네트워크
모니터
526
프로브
528
프로브