US007346803B2

(12) **United States Patent**
Ide et al.

(10) **Patent No.: US 7,346,803 B2**
(45) **Date of Patent: Mar. 18, 2008**

(54) **ANOMALY DETECTION**

(75) Inventors: **Tsuyoshi Ide**, Kawasaki (JP); **Kunikazu Yoda**, Yamato (JP); **Hisashi Kashima**, Yamato (JP); **Hiroaki Etoh**, Kanagawa-ken (JP); **Ryo Hirade**, Miura (JP)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 580 days.

(21) Appl. No.: **11/045,918**

(22) Filed: **Jan. 28, 2005**

(65) **Prior Publication Data**

US 2005/0193281 A1 Sep. 1, 2005

(30) **Foreign Application Priority Data**

Jan. 30, 2004 (JP) 2004-023081

(51) **Int. Cl.**
G06F 11/00 (2006.01)

(52) **U.S. Cl.** **714/4**; 714/38

(58) **Field of Classification Search** .... None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,661,668	A *	8/1997	Yemini et al.	702/186
7,107,491	B2 *	9/2006	Graichen et al.	714/37
2004/0221190	A1 *	11/2004	Roletto et al.	714/4
2007/0100875	A1 *	5/2007	Chi et al.	707/102

OTHER PUBLICATIONS

Japanese Publication No. 2003-060704 published on Feb. 28, 2003.
Hajji, hassan, "Baselining Network Traffic and Online Faults Detection," IEEE International Conference on Communications 2003, vol. 1, pp. 301-308.

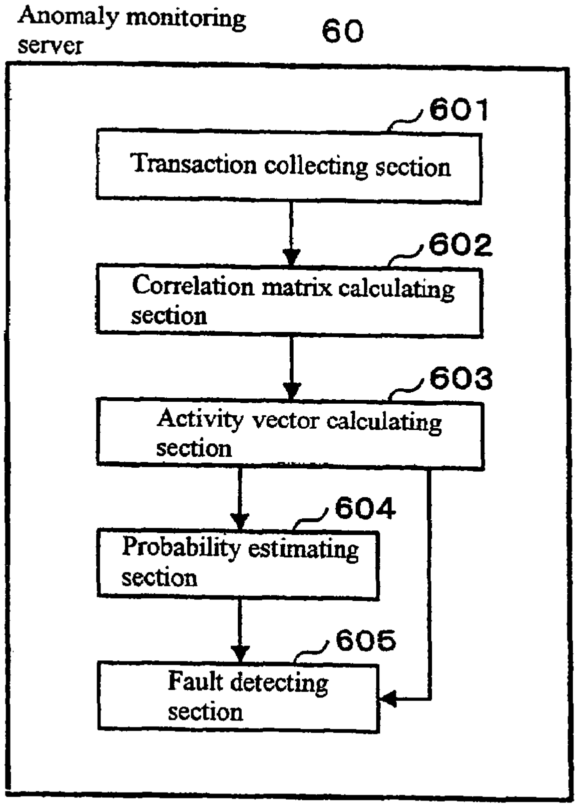
* cited by examiner

Primary Examiner—Christopher McCarthy
(74) *Attorney, Agent, or Firm*—Louis P. Herzberg

(57) **ABSTRACT**

A system such as a Web-based system in which a plurality of computers interact with each other is monitored to detect online an anomaly. Transactions of a service provided by each of a plurality of computers to another computer are collected, a matrix of correlations between nodes in the system is calculated from the transactions, and a feature vector representing a node activity balance is obtained from the matrix. The feature vector is monitored using a probability model to detect a transition to an anomalous state.

28 Claims, 9 Drawing Sheets


Anomaly monitoring server
60
601
Transaction collecting section
602
Correlation matrix calculating section
603
Activity vector calculating section
604
Probability estimating section
605
Fault detecting section