

文章编号:1001-9081(2015)09-2519-03

doi:10.11772/j.issn.1001-9081.2015.09.2519

基于危险理论的分布式服务异常检测模型

李锦民, 李 涛*, 徐 凯

(武汉科技大学 计算机与科学技术学院, 武汉 430065)

(* 通信作者电子邮箱 705398096@qq.com)

摘要:在分布式环境下,对于大量服务的海量行为数据导致服务异常检测效率低以及服务的动态组合导致服务的不确定性这两个问题,基于危险理论提出了一种分布式服务的异常检测模型。首先,借鉴人工免疫识别异常的生物学过程,利用微分来描述海量服务行为数据的变化,通过构造特征三元组的方法检测异常源;然后,借鉴云模型的思想,通过构造服务的状态云,计算服务间隶属度的方法解决服务的不确定性问题,从而计算出危险区域;最后,通过模拟学生登录选课服务进行了实验。实验结果表明,该模型不仅动态地实现了对服务的异常检测,而且准确地描述了服务之间的依赖关系,提高了异常检测的效率。实验结果证明了该模型的可行性与正确性。

关键词:危险理论; 云模型; 数值微分; 服务起源日志; 人工免疫

中图分类号: TP309 **文献标志码:**A

Anomaly detection model based on danger theory of distributed service

LI Jinmin, LI Tao*, XU Kai

(College of Computer Science and Technology, Wuhan University of Science and Technology, Wuhan Hubei 430065, China)

Abstract: Concerning the problem that a large number of services' massive behavior data leads to inefficiency in anomaly detection of services and dynamic composition of services leads to uncertainty in service under the distributed environment, a new distributed service anomaly detection model based on danger theory was proposed. Firstly, inspired by the biological processes of artificial immune recognizing abnormalities, this paper used differentiation to describe the variation of massive services' behavior data, and constructed characteristic triad to detect abnormal source. Then, service guided by the idea of cloud model, this paper resolved uncertainty among services by constructing status cloud of the services and computing the degree of membership between services, and calculated the danger zone. Finally, the simulation experiments of student for selecting courses were carried out. According to the simulation results, the model not only detects abnormal services dynamically, but also describes of the dependencies between services accurately, and improves the anomaly detection efficiency. The simulation results verify the validity and effectiveness of the model.

Key words: risk theory; cloud model; numerical differentiation; service log origin; artificial immune

0 引言

随着移动互联网、O2O(Online To Offline)的兴起,越来越多的移动应用、互联网应用聚集了海量的用户,为了响应大量用户的请求,以腾讯、Twitter为代表的互联网公司采用分布式服务提高服务能力、提升并发处理性能。以 Twitter 为例, Twitter 部署了约 2 000 个分布式服务,这些服务符合 SOA (Service-Oriented Architecture) 规范,通过动态组合满足不同用户的需求。与此同时,这样就形成了复杂的组合及引用关系,给分布式环境下的服务异常检测带来了困难。

不同于传统的服务异常检测即关注单个服务的行为,分布式服务的异常检测需要根据服务的组合关系发现整体的异常。由于大量用户请求导致的服务海量行为数据,以及服务组合本身的不确定性给服务异常检测带来了挑战:

1) 服务与服务之间的行为时时刻刻都在变化,存在着不确定性,因此难以用简单的静态模型去描述;

2) 服务与服务之间的行为是动态组合的、相互连接的,它们之间存在着依赖关系,因此很难通过单一的服务状态来检测整个分布式服务的异常状态;

3) 海量的服务行为数据,给分布式服务的异常检测的效率带来极大的挑战。

计算机免疫系统,也称为人工免疫系统(Artificial Immune System, AIS),它是受生物免疫系统启发解决实际问题的智能性方法^[1-2]。而机体免疫系统所具有的分布性、自适应性等特征对检测分布式服务下服务异常提供了一个有效的方法。在 1994 年,著名免疫学家 Matzinger^[3]在此基础上提出了一个新观点——“危险模式理论”。该理论从不同的角度阐述了免疫系统的工作机理,它认为:免疫系统要防御的不是“非我”^[4],而是潜在的“危险”,淋巴细胞识别抗原的机理来源于适应性免疫层,而危险模式理论阐述了先天免疫层的工作机理。这一理论的出现为解决海量数据处理问题、降低计算机免疫系统的计算代价提供了新思路。英国诺丁汉大学的

收稿日期:2015-04-23;修回日期:2015-06-28。

基金项目:国家自然科学基金资助项目(61273225);湖北省教育厅人文社科重点基金资助项目(2012D111)。

作者简介:李锦民(1990-),男,四川成都人,硕士研究生,主要研究方向:信息安全、云服务; 李涛(1979-),男,湖北武汉人,副教授,博士,主要研究方向:信息安全、人工免疫、服务计算; 徐凯(1989-),男,湖北孝感人,硕士研究生,主要研究方向:信息安全、云计算。

计算机免疫研究小组^[5]从 2002 年开始尝试将危险模式理论引入计算机免疫学，并将其简称为危险理论，杨鹤等^[6]和李涛^[7]都对危险理论作了深入的分析。

本文将上述问题作为研究点，提出了一套基于危险理论的分布式服务异常检测模型，并给出了该模型的相关结构、主要部分的模块功能以及流程和算法。

1 基于危险理论的分布式服务的异常检测

定义 1 服务。云计算平台下存在服务 $S_i (i = 1, 2, 3, \dots)$ 。

定义 2 服务异常。服务的异常是由用户的行为决定的，即服务的调用次数(invoking times)。当调用次数的变化超过某个范围即认为该服务异常。

定义 3 危险信号。危险信号是所有服务异常的集合，记作异常源 $DS = \{Ds_i | i \in \mathbb{N}\}$ 。

定义 4 依赖(执行)路径。相连的两个服务组成一条依赖(执行)路径，记作 $(S_i, S_j) (i, j = 1, 2, 3, \dots)$ 。

定义 5 危险区域。由依赖路径组成，例如，某个服务执行路径区间发生了异常，将关注点从某个服务扩展到某个区域，可以是一条或多条执行路径。

在文献[8]中详细地阐述了分布式服务的行为捕获方法，该文献通过一个服务起源日志 9 元组描述服务的动态行为，分别为：服务调用 ID、服务调用者、被调用的服务、服务调用次数、站点、调用服务的耗时、当前的时间、输入参数、输出参数、调用结果，即 token, Invoking Service, Service Invoked, location, elapsed time, times tamp, input, output, status。本文使用文献[8]中的服务行为采集方法，并将该 9 元组作为输入数据，借鉴危险理论的相关思想首先定义并识别危险信号，在发现某些服务异常后并以此为基础，根据服务与服务之间的依赖关系计算出危险区域。这样不仅考虑到了服务的动态组合行为还解决了海量数据的处理问题，从而提高了服务异常检测效率。

1.1 模型结构

本文试图研究了一种基于危险理论的分布式服务的异常检测模型，其主要流程如图 1 所示。



图 1 分布式服务的异常检测模型

系统中每一个服务时时刻刻都在变化，具体如服务的调用次数、耗时，并且它们也都是离散的，在图 1 中首先对分布式下的每一个服务进行实时的监测，在“危险信号的表征”这部分是指选取服务的特征点并构造特征三元组，在“危险信号的触发与提取”这部分是指若实时数据所构造的特征三元组超出了历史数据所构造的特征三元组，则认为有可能存在潜在的危险，那么将其标记为异常源，在“计算危险区域”这部分是指通过构造异常源服务与其相连的服务的状态云，计算它们各自的隶属度，确立它们之间的关系，最后通过判断服务间隶属度的大小，若该隶属度小于某个阈值，则输出该服务的危险路径从而得到危险区域。

数学中常利用微分^[9]的方法研究函数的变化规律^[8]，同

样在计算机系统中变化也意味着系统的平衡被打破，预示着危险的产生，其中极值点(特征点)正是曲线趋势发生变化的关键点，通过采集各个特征点来构造特征三元组，使用该三元组能够刻画特征检测点及其与相邻点所构成的曲线的趋势，采集各个特征点所对应的三元组，就能够实现对系统资源运行情况的描述，再对正常运行情况下和待检时计算出的三元组作比较，实现基于特征的变化检测^[10]，进而发现异常源。

云模型^[11-12]是描述不确定事件的有力工具，通过构造两个相连服务的状态云进而计算它们之间的隶属度，若隶属度越大，说明两个服务的变化越相似，那么这两个服务之间越不容易出现异常，反之如果隶属度小于某个阈值说明这两个服务存在着较大的差异，那么越容易出现异常。

1.2 危险信号的提呈

系统中每一个服务时时刻刻都在变化，并且也都是离散的，将这些离散的数据串联起来能够以图形化的方式描述随着时间的变化其变化的特征和趋势。极值点是曲线趋势发生变化的关键点，因此本文方法先将其作为比较变化和表达变化的基础，然后构造特征三元组 $\{f'(x_i)_{left}, f(x_i), f'(x_i)_{right}\}$ 对服务特征变化进行更精确地描述。其中 $f'(x_i)_{left}, f'(x_i)_{right}$ 分别表示了特征点左边(右边)曲线的趋势。

构造特征三元组 采集数据并选取特征点(极值点)，计算特征点 x_i 的左右微分：

$$f'(x_i)_{left} = f(x_i - x_{i-1})/h \quad (1)$$

$$f'(x_i)_{right} = f(x_{i+1} - x_i)/h \quad (2)$$

再通过式(1)和(2)构造特征三元组，其中 h 表示 x_i 与 $x_{i-1}(x_{i+1})$ 之间的距离。

提取危险信号 对实时数据构造的特征三元组与历史数据构造的特征三元组进行比较，若前者大于后者，那么该服务出现异常，并将其纳入危险信号，标记为异常源。

1.3 计算危险区域

定义 6 期望值 Ex 。代表每个服务调用其他服务次数的均值。

熵 En 。相对于期望值而言，代表每个服务调用其他服务次数的跨度。

超熵 He 。熵的不确定性度量，即熵的熵。超熵越大，即隶属度越大，说明服务与服务间的变化越相似。

状态云的生成步骤如下。

1) 计算服务 S 的状态云：

步骤 1 假设与 S 相连的服务有 n 个，把每个服务看成一个云滴，即有 n 个云滴， S 与每个云滴的调用次数看作是该云滴的确定度，记作 $N_i (i = 1, 2, \dots, n)$

步骤 2 计算调用次数的均值：

$$X = \frac{1}{m} \sum_{i=1}^m N_i \quad (3)$$

步骤 3 由式(3)可得期望值：

$$Ex = X \quad (4)$$

步骤 4 通过式(4)可得熵：

$$En = \sqrt{\frac{\pi}{2}} \times \frac{1}{m} \sum_{i=1}^m |N_i - X| \quad (5)$$

步骤 5 3 个数字特征值即可确定一个状态云，所以记服务 S 的状态云 $S(Ex, En, He)$ 。

2) 计算与 S 相连的服务 S_i 的状态云：

步骤1 假设与 S_i 相连的服务有 n 个,把每个服务看成一个云滴,即有 n 个云滴, S_i 与每个云滴的调用次数看作是该云滴的确定度,记作 $N_j(j=1,2,\dots,n)$ 。

步骤2 同计算服务 S 的状态云的方法一样。

步骤3 S_i 的状态云为 $S_i(Ex_i,En_i,He_i)$ 。

3) 计算 S_i 相对于 S 的隶属度:

$$\mu = e^{-\frac{(Ex-Ex_i)^2}{2(En)^2}} \quad (6)$$

当在计算某服务的状态云时,若该服务为叶子节点即再也没有其他服务与之相连,那么不计算该服务的状态云。

2 实验结果及分析

2.1 实验数据来源

本文实验以学生登录选课服务作为研究对象,图2所示为该服务流程,其中服务 S_1 到 S_9 分别代表:注册、系统自动注册、用户注册、主修课程查询、主修课程、课程列表、查询冲突、查询课程、查询注册登记。由于服务的行为是随着用户的行为变化而变化的,比如在选课或查询成绩时,某些服务的行为会发生变化,例如它的调用次数或耗时会猛然增高,出现系统瓶颈。因此为了能尽量模拟真实环境下的学生登录选课服务的变化情况,通过使用 Eclipse 生成正常情况下以及服务行为变化状态下的数据作为实验数据,以达到真实环境的效果,从而找到异常源,计算出危险区域。

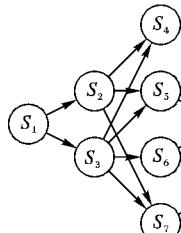


图2 学生登录选课服务流程

2.2 实验步骤及结果分析

2.2.1 危险信号的触发及提取

1) 首先产生单个服务在学生选课或查询成绩时的总调用次数见图3所示,由于服务 S_4, S_8, S_9 为叶子节点,并没有服务可继续调用,因此它们不会产生总调用次数。其中纵坐标代表每个服务的总调用次数,横坐标代表时间序列,即一段时间点。

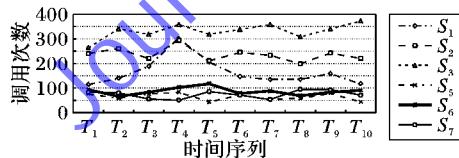


图3 单个服务的调用总次数

2) 从图3中选取特征点构造特征三元组与历史数据构造的特征三元组作比较。通过比较后发现相对于其他服务,服务 S_1 在 T_4 时间段中所构造的特征三元组大于历史数据所构造的特征三元组,那么将该时间点的服务 S_1 纳入危险信号中,并标记其为异常源。

2.2.2 危险区域的计算

1) 由于在 T_4 时间点发现了异常源,因此将 T_4 时间点所有相连的两两服务间的调用次数通过图4显示出来,其中它

们的横坐标 S_i-S_j 代表服务 S_i 调用 S_j 的次数($i, j = 1, 2, 3, \dots$)。

2) 采集 T_4 时间点服务与服务之间的调用次数从而生成服务的状态云并计算它们之间的隶属度进而计算出危险区域,由于并没有使用熵,所以在该实验中构造状态云时超商用 He 代替。由于除了 T_4 时间点以外,其余时间点均为服务之间的调用次数均为正常,因此任意选取一个时间点,构造服务的状态云,计算隶属度在 0.3 左右波动,因此该阈值设定为 0.3。

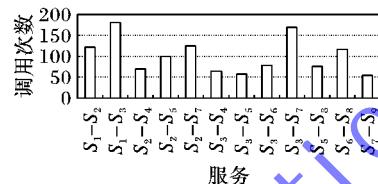


图4 服务与服务之间的调用次数

3) 首先计算 T_4 时间点服务 S_1, S_2, S_3 的状态云以及 S_2 和 S_3 相对于 S_1 的隶属度,状态云分别为 $S_1(142.5, 23.19, He)$ 、 $S_2(100.67, 21.11, He)$ 、 $S_3(99.0, 18.17, He)$,那么 S_2 相对于 S_1 的隶属度为 0.19, S_3 相对于 S_1 的隶属度为 0.17。然后计算 S_5, S_6, S_7 的状态云,以及它们之间的隶属度,由于服务 S_4, S_8, S_9 为叶子节点,因此不纳入状态云的计算,状态云分别为 $S_5(99.0, He)$ 、 $S_6(118.0, He)$ 、 $S_7(62.0, He)$,那么 S_5 相对于 S_2 的隶属度为 0.99, S_7 相对于 S_2 的隶属度为 0.19, S_5 相对于 S_3 的隶属度为 1.00, S_6 相对于 S_3 的隶属度为 0.57, S_7 相对于 S_3 的隶属度为 0.12。

2.2.3 危险区域的输出

通过对隶属度的观察,可知 S_1-S_3 这条路径出现异常的概率要大于 S_1-S_2 这条路径,但是 S_2 和 S_3 相对于服务 S_1 的隶属度均小于 0.3,所以也应该纳入危险区域。由于在 T_4 时间点 S_3 的总调用次数大于 S_2 ,因此 $S_1-S_2-S_7$ 这条路径出现异常的概率比 $S_1-S_3-S_7$ 这条路径可能性要小一些, $S_1-S_3-S_7$ 可能为最危险的路径。

综上所述,该危险区域由 $S_1-S_2-S_7$ 和 $S_1-S_3-S_7$ 这两条路径组成,如图5所示。

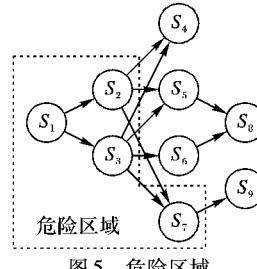


图5 危险区域

3 结语

基于危险理论的分布式服务异常检测模型能够有效地发现异常源并能检测出与异常源相关的依赖路径,从而提高服务异常检测的效率。本文在危险理论的基础上,以“变化感知危险”作为出发点,对模型的部分主要的模块进行了详细的分析和设计,此模型能有效发现异常并得到危险区域。然而,本文仍然存在一些不足,如实验中服务的数量不够多,因此对该模型的可行性验证方面还有待进一步的探索和研究。

(下转第 2541 页)

- 3060–3063.
- [3] KASHYAP N, SINHA G R. Image watermarking using 3-level Discrete Wavelet Transform (DWT) [J]. International Journal of Modern Education and Computer Science, 2012, 4(3): 50–56.
- [4] YADAV S, RAHUL G. Digital watermarking for color images using wavelet transform [EB/OL]. [2015-01-07]. <http://piserjournal.org/wp-content/uploads/2014/05/V13-137-143.pdf>.
- [5] TAO H, ZAIN J M, AHMED M M, et al. A wavelet-based particle swarm optimization algorithm for digital image watermarking [J]. Integrated Computer-Aided Engineering, 2012, 19(1): 81–91.
- [6] ZOPE-CHAUDHARI S, VENKATACHALAM P. Robust copyright protection of raster images using wavelet based digital watermarking [C]// Proceedings of the 2014 IEEE International Geoscience and Remote Sensing Symposium. Piscataway: IEEE, 2014: 3129–3132.
- [7] PREDA R O. Self-recovery of unauthentic images using a new digital watermarking approach in the wavelet domain [C]// Proceedings of the 10th International Conference on Communications. Piscataway: IEEE, 2014: 1–4.
- [8] MEERWALD P, UHL A. Watermark security via wavelet filter parametrization [C]// Proceedings of the IEEE International Conference on Image Processing. Washington, DC: IEEE Computer Society, 2001, 3: 1027–1030.
- [9] WU X, HU J, GU Z, et al. A secure semi-fragile watermarking for image authentication based on integer wavelet transform with parameters [C]// Proceedings of the 2005 Australian Information Security Workshop. Sydney: Australian Computer Society, 2005, 44: 75–80.
- [10] PIVA A, BARTOLINI F, CALDELLI R. Self recovery authentication of images in the DWT domain [J]. International Journal of Image and Graphics, 2005, 5(1): 149–165.
- [11] CHAMLAWI R, KHAN A, IDRIS A. Wavelet Based image authentication and recovery [J]. Journal of Computer Science and Technology, 2007, 22(6): 795–804.
- [12] STOLAREK J. Adaptive wavelet synthesis for improving digital image watermarking [M]// Studies in Computational Intelligence. Berlin: Springer, 2012, 401: 133–143.
- [13] PALANIVEL M, SHANMUGAM A. Improved performance by parameterizing wavelet filters for digital image watermarking [J]. Signal and Image Processing, 2012, 3(1): 29–38.
- [14] TONG X, CUI M. A novel image encryption scheme based on feedback and 3D baker [C]// Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing. Washington, DC: IEEE Computer Society, 2008: 1–4.
- [15] LE H, LI T, SHI L. Improved image encryption algorithm based on Henon hyperchaotic system [J]. Journal of Computer Applications, 2011, 31(7): 1909–1916. (乐鸿辉, 李涛, 石磊. 应用 Henon 超混沌系统改进的图像加密[J]. 计算机应用, 2011, 31(7): 1909–1916.)
- [16] YANG L, SHAO L, GUO Y, et al. Image encryption algorithm based on maze permutation and Logistic chaotic map [J]. Journal of Computer Applications, 2014, 34(7): 1902–1908. (杨璐, 邵利平, 郭毅, 等. 基于迷宫置换和 Logistic 混沌映射的图像加密算法[J]. 计算机应用, 2014, 34(7): 1902–1908.)
- [17] LIU H, STEINEBACH M. Semi-fragile watermarking for image authentication with high tampering localization capability [C]// Proceedings of the 2nd International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution. Washington, DC: IEEE Computer Society, 2006: 143–150.
- [18] ULLAH R, KHAN A, MALIK A S. Dual-purpose semi-fragile watermark: authentication and recovery of digital images [J]. Computers and Electrical Engineering, 2013, 39(7): 2019–2030.

(上接第 2521 页)

参考文献:

- [1] AICKELIN U, DASGUPTA D. Advances in artificial immune systems [J]. IEEE Computational Intelligence Magazine, 2006, 1(4): 40–49.
- [2] DING Y, REN L. Artificial immune systems: theory and applications [J]. Pattern Recognition and Artificial Intelligence, 2000, 13(1): 52–59. (丁永生, 任立红. 人工免疫系统理论与应用[J]. 模式识别与人工智能, 2000, 13(1): 52–59.)
- [3] MATZINGER P. The danger model: a renewed sense of self [J]. Science, 2002, 296: 301–305.
- [4] FORREST S, PERELSON A S, ALLEN L, et al. Self-nonself discrimination in a computer [C]// Proceedings of the 1994 IEEE Computer Society Symposium on Research in Security and Privacy. Piscataway: IEEE, 1994: 202–212.
- [5] AICKELIN U, CAYZER S. The danger theory and its application to artificial immune system [EB/OL]. [2015-01-06]. <http://citeserx.ist.psu.edu/viewdoc/download?doi=10.1.1.11.6815&rep=rep1&type=pdf>.
- [6] YANG H, DONG H, LIANG Y, et al. Artificial cloud danger signals in the immune system define [J]. Computer Engineering and Applications, 2006, 42(10): 34–36. (杨鹤, 董红斌, 梁意义, 等. 人工免疫系统中危险信号的云方法定义[J]. 计算机工程与应用, 2006, 42(10): 34–36.)
- [7] LI T. Computer immunology [M]. Beijing: Publishing House of Electronics Industry, 2004. (李涛. 计算机免疫学[M]. 北京: 电子工业出版社, 2004.)
- [8] LI T, LIU L, ZHANG X, et al. ProvenanceLens: service provenance management in the cloud [C]// Proceedings of the 2014 International Conference on Collaborative Computing: Networking, Applications and Worksharing. Piscataway: IEEE, 2014: 110–114.
- [9] Tongji University, Mathematics Teaching and Research Section. Advanced mathematics [M]. Beijing: Higher Education Press, 1996. (同济大学数学教研室. 高等数学[M]. 北京: 高等教育出版社, 1996.)
- [10] LIANG Y, CAO L, CAI Y. Introduction to danger sensed through numerical differential [J]. Journal of Harbin Engineering University, 2006, 27(Suppl.): 228–232. (梁意义, 曹玲林, 蔡瀛. 危险感知的数字微分初步[J]. 哈尔滨工程大学学报, 2006, 27(增刊): 228–232.)
- [11] LI D, LIU C. Study on the universality of the normal cloud model [J]. Engineering Science, 2004, 6(8): 28–34. (李德毅, 刘常昱. 论正态云模型的普适性[J]. 中国工程科学, 2004, 6(8): 28–34.)
- [12] LI D, LIU C, DU Y, et al. Artificial intelligence with uncertainty [J]. Journal of Software, 2004, 15(11): 1583–1594. (李德毅, 刘常昱, 杜鵑, 等. 不确定性人工智能 [J]. 软件学报, 2004, 15(11): 1583–1594.)