Journal of System Simulation

Volume 28 | Issue 2 Article 8

8-17-2020

Research and Design of All-purpose Simulation Platform of Fault Injection

Wenbin Yao
School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China;

Zhao Ling
School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China;

Wang Zhen
School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China;

Yao Xiang
School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China;

Research and Design of All-purpose Simulation Platform of Fault Injection

Abstract

Abstract: Focusing on the limited injection position and single target system problems existing in the simulation research of fault injection, combined with the NS2 simulation technology and fault injection method, an all-purpose simulation platform of fault injection was proposed. *The layered model of the targeted information system was constructed, whose topology information and service performance information was given by the matrix, and improved the generality of the simulation platform of fault injection. Based on the configuration information, the platform constructed the fault library, which brought the cost reduction and reliability promotion of the system faults. The quadruple design of the fault configuration implemented the injection of any fault and reduced the configuration complexity.* The simulation test results show that the simulation platform can simulate systems with any kind of requirements, and ensure the correctness and effectiveness of any fault injected at anytime and anywhere.

Keywords

system modeling, system simulation, fault design, fault injection

第 28 卷第 2 期 系统仿真学报© Vol. 28 No. 2
2016 年 2 月 Journal of System Simulation Feb., 2016

故障注入通用仿真平台的研究与设计

姚文斌，赵玲，王真，姚翔
(北京邮电大学计算机学院，北京市 100876)

摘要：针对故障注入仿真研究注入位置受限、平台单一等问题，结合 NS2 仿真平台和故障注入技术，*提出故障注入通用仿真平台设计方案。该方案为系统建立层次结构模型，并以矩阵形式提供拓扑和服务能力信息，提高了故障注入仿真平台的通用性；基于系统配置信息构建故障库，降低了系统故障分析成本，并提高了故障来源的可靠性；设计四元组配置格式实现任意组合故障的注入，降低了故障注入配置的复杂性。*仿真实验结果表明，基于该方案构建的仿真平台能够实现满足任意需求的目标系统仿真，并能够保证任意时间任意位置注入故障的正确性和有效性。

关键词：系统建模；系统仿真；故障设计；故障注入
中图分类号：TP391.9 文献标识码：A 文章编号：1004-731X (2016) 02-0315-07

Research and Design of All-purpose Simulation Platform of Fault Injection

Yao Wenbin, *Zhao Ling*, *Wang Zhen*, *Yao Xiang*
(School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: Focusing on the limited injection position and single target system problems existing in the simulation research of fault injection, combined with the NS2 simulation technology and fault injection method, an all-purpose simulation platform of fault injection was proposed. *The layered model of the targeted information system was constructed, whose topology information and service performance information was given by the matrix, and improved the generality of the simulation platform of fault injection. Based on the configuration information, the platform constructed the fault library, which brought the cost reduction and reliability promotion of the system faults. The quadruple design of the fault configuration implemented the injection of any fault and reduced the configuration complexity.* The simulation test results show that the simulation platform can simulate systems with any kind of requirements, and ensure the correctness and effectiveness of any fault injected at anytime and anywhere.

Keywords: system modeling; system simulation; fault design; fault injection

引言

随着信息化的发展，人们对信息系统的依赖程度越来越高，而信息系统可信性也成为人们日益关注的话题。故障注入技术是通过人为地向信息系统中注入故障，然后观察系统的行为来对系统可信性进行验证的一项技术[1]。按照注入的方式的不同，故障注入包括：基于硬件的故障注入、基于软件的故障注入和基于仿真的故障注入 3 种方式。基于硬件的故障注入技术可能对目标硬件设备带来永久性的损害从而加大容错系统有效性的成本；基于软件的故障注入方式大多只针对特定的硬件环境[2]，使其应用范围受限；软件实现的仿真属于全数字仿真，不仅是评测容错机制的一种有效方法而且还具

收稿日期：2014-10-20 修回日期： 2014-12-19;
基金项目：国家 863 计划(2012AA012600)；
作者简介：姚文斌(1972-)，男，黑龙江哈尔滨，博士，教授，博导，研究方向为信息安全与灾备技术、可信计算与容错计算；赵玲(1989-)，女，河北沧州，硕士生，研究方向为信息安全与灾备技术、信息化系统建模与仿真。

有灵活性好,开发成本低,注入过程易于控制等优点[3],并且不会损害实际设备而且通用性高。因此,使用软件仿真方式对故障注入展开研究引起众多研究人员的关注。

当前,针对故障注入的仿真研究日益广泛。文献[4]建立列车运行控制仿真平台,通过仿真故障注入方式有效验证了其故障处理机制,文献[5]结合双变迁 Petri 网和故障注入方法,提出了一种基 BEDTPN 网的飞机交流供电系统建模方法,通过仿真故障的扰动和变迁运动,仿真故障对系统组件的影响。文献[6]基于 NI PXI/LabvewRT 实时仿真平台,为双余度电刹车系统设计了仿真实验环境。但是,以上方案均针对特定的信息系统,通用性受限。文献[7]基于实物仿真方式,能够实现不同层次不同类型故障的注入,但是该方法将对每个层次的故障进行单独注入,没有考虑到层次之间的组合故障。文献[8]基于半实物仿真方式,对雷达系统进行多故障模式注入,该方案中仅选择总线处进行故障注入,注入位置受限制。文献[9-10]基于 VHDL 设计了一种故障注入技术工具,并结合软件方式在仿真器中进行了实现,该工具只能以硬件设备作为注入目标。文献[11-12]通过建模方法对网络可靠性进行了分析,但该方法假设故障不会同时发生,不能对多故障情况下的网络进行分析。文献[13]仅对内存故障进行建模和仿真注入分析。当前故障注入仿真研究仍具有注入位置受限制、仿真平台单一的问题。

针对上述问题,本文研究并设计了故障注入通用仿真平台 ASPBOFJ (All-purpose Simulation Platform Based on Fault Injection)。基于实际系统应用环境对目标信息系统建立层次结构的仿真模型,进而实现对任意建设需求下的信息系统平台的仿真,在此基础上,利用提出的故障库生成算法,自动分析并获取信息系统所有的可能进行故障注入的位置和类型,通过提供一种四元组配置方案作为故障配置接口,能够在任意时刻在任意位置进行多个有效故障的注入。

1 仿真平台架构

ASPBOFJ 仿真平台的总体设计目标是建立通用的信息系统仿真模型,并在仿真环境下通过参数配置的方式实现信息系统的灵活仿真。平台通过对仿真系统信息的自动收集,实现任意时刻任意位置的可配置故障注入。ASPBOFJ 仿真平台包括管理控制、系统配置、目标系统仿真、故障注入、故障检测和数据采集 6 个功能模块,并包含配置库和故障库作为系统数据支撑。

ASPBOFJ 仿真平台的组成架构如图 1 所示。

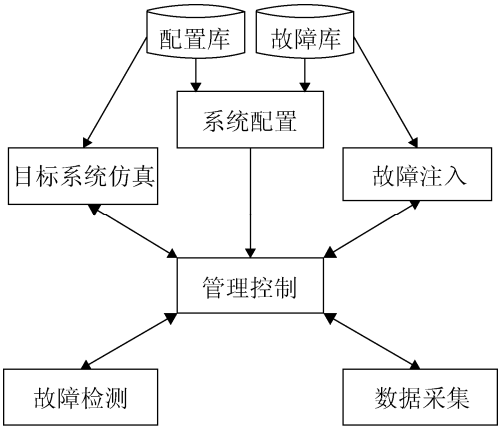


图 1 ASPBOFJ 系统组成

1) 管理控制

管理控制整个仿真平台架构的核心功能,负责管理调度系统配置功能、目标系统仿真功能、故障注入功能、故障检测功能和数据采集功能完成目标信息系统的仿真,以及向目标仿真系统注入故障的操作。

2) 系统配置

系统配置是仿真平台的输入模块。基于用户需求,更新配置库信息,基于本文提出的信息系统通用模型,设置系统参数配置矩阵,实现对目标信息系统在拓扑连接、网络性能方面的配置,同时根据本文提出的故障库生成算法,构建信息系统的故障库。在此基础上,进一步实现对目标信息系统、故障模式、故障控制时间、数据采集间隔及系统故障检测的时间周期的配置。

3) 目标系统仿真

目标系统仿真通过信息系统的配置信息,完成

对信息系统设备情况、链路连接情况和网络情况的仿真实现。

4) 故障注入

通过对系统的结构和配置信息分析，自动获取目标系统所有可能的故障位置，经过格式处理之后，完保存到故障库文件中。在此基础上，通过接口配置向运行中的目标仿真系统的注入任意故障。

5) 故障检测和数据采集

故障检测模块负责在目标系统运行过程中定时检测系统是否发生故障。 数据采集模块主要实现对仿真业务数据、仿真过程追踪数据、系统各组成部件的性能监控数据的采集，以作为故障检测与分析、评价仿真系统是否满足仿真需求及验证 ASPBOFJ 平台故障注入能力的数据支撑。

6) 配置库和故障库

配置库和故障库是 ASPBOFJ 平台的支撑层，可根据不同的系统配置进行更新，配置库中存储目标系统中可能用到的设备资源、链路资源和网络资源类型，以及对应的性能参数信息。故障库中存储所有可能注入的故障信息。其中，配置库基于用户需求，在仿真开始之间由管理员执行修改更新操作，而故障库则是由故障库自动生成算法创建，同时提供人工修改接口。

2 建模与方案设计

2.1 目标系统建模设计

信息系统利用自身的软硬件资源、网络通信和数据资源，通过执行输入、加工、存储和控制操作为用户提供服务。其中，提供给用户输入操作的相关资源可抽象为用户交互层；提供交互数据传输的连接设备、网络链路等资源可抽象为网络通信层；而提供应用服务的服务器、存储器设备、数据资源和加工、存储和控制操作可抽象为应用处理层。

信息系统仿真模型如图 2 所示。

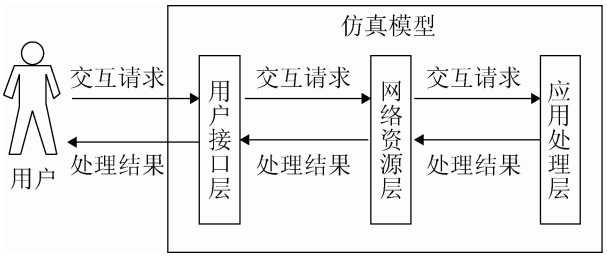


图 2 目标信息系统仿真通用模型

2.2 故障注入通用仿真方案设计

2.2.1 目标系统仿真设计

假设配置库提供设备类型个数为 $C1$，链路类型个数为 $C2$，则管理控制模块为信息系统提供的仿真参数包括：信息系统节点个数 n，信息系统参数矩阵 $A=\{a_{i,j}\}$，当 $i=j$ 时，$a_{i,j}$ 表示设备类型编号，当 $i\neq j$ 时，表示链路类型编号。其中，$a_{i,j}\in[0,C1+C2]$，$i\in\{1,2,\cdots,n\}$，$q\in\{1,2,\cdots,n\}$。

仿真流程如下所述。

1) 获取目标信息系统配置信息。系统按照先行后列的顺序对信息系统的信息矩阵 A 进行遍历；

2) 创建仿真节点，并进行节点配置。当遍历对象为对角线元素时，检测该设备节点是否已经创建，如果已经创建，则继续遍历，否则创建仿真节点，并根据该元素值在配置库中匹配该设备的类型，容量、端口个数等规格参数，以创建变量的形式对仿真节点进行规格配置；

3) 创建网络链路，并进行网络配置。当遍历对象为非对角线元素。检测该链路连接的两个节点是否已经创建，若均已创建，则建立单工链路，并根据该元素值在配置库中匹配网络参数，以创建变量的形式对仿真链路进行规格配置，否则，创建两个仿真节点，再重复以上操作。

仿真流程如图 3 所示。

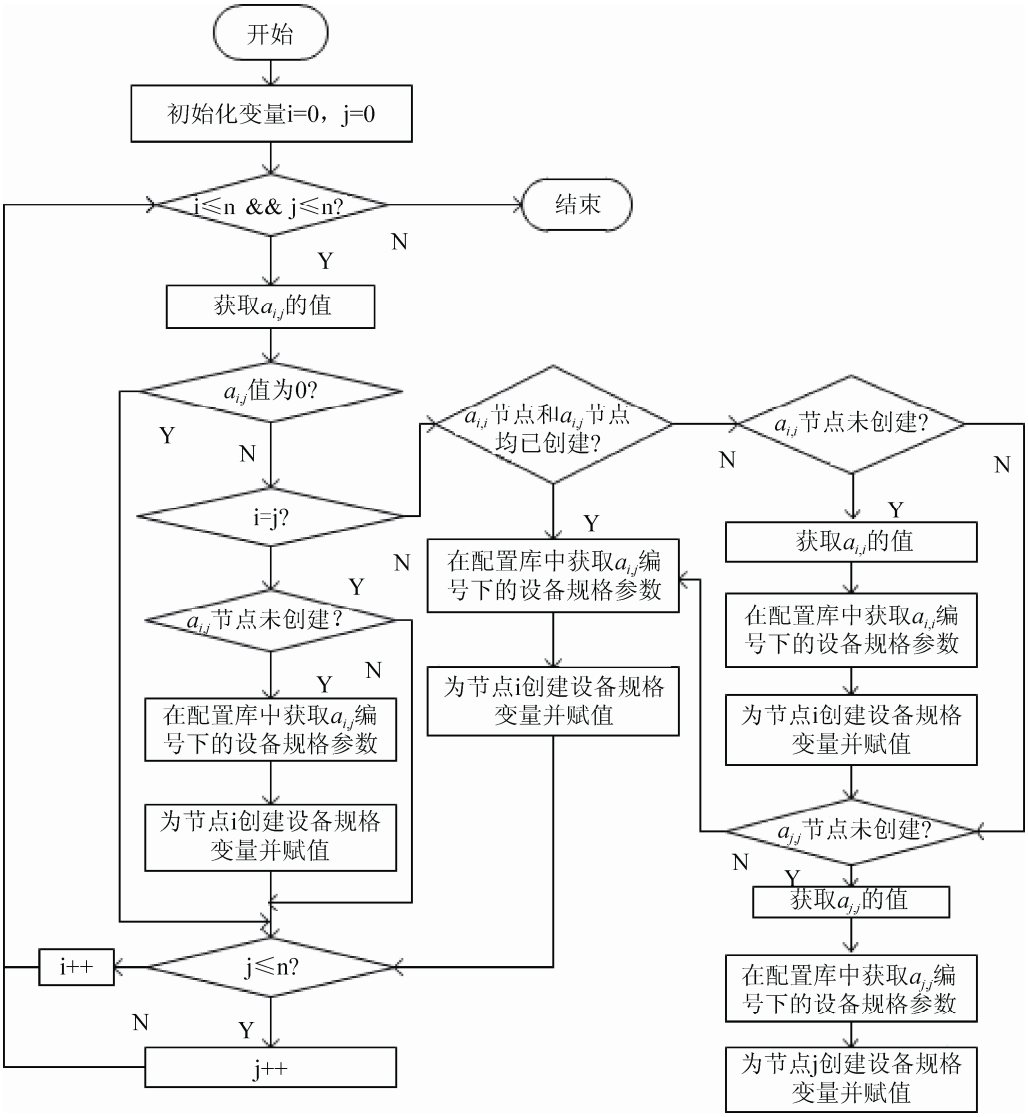


图 3 目标系统仿真流程

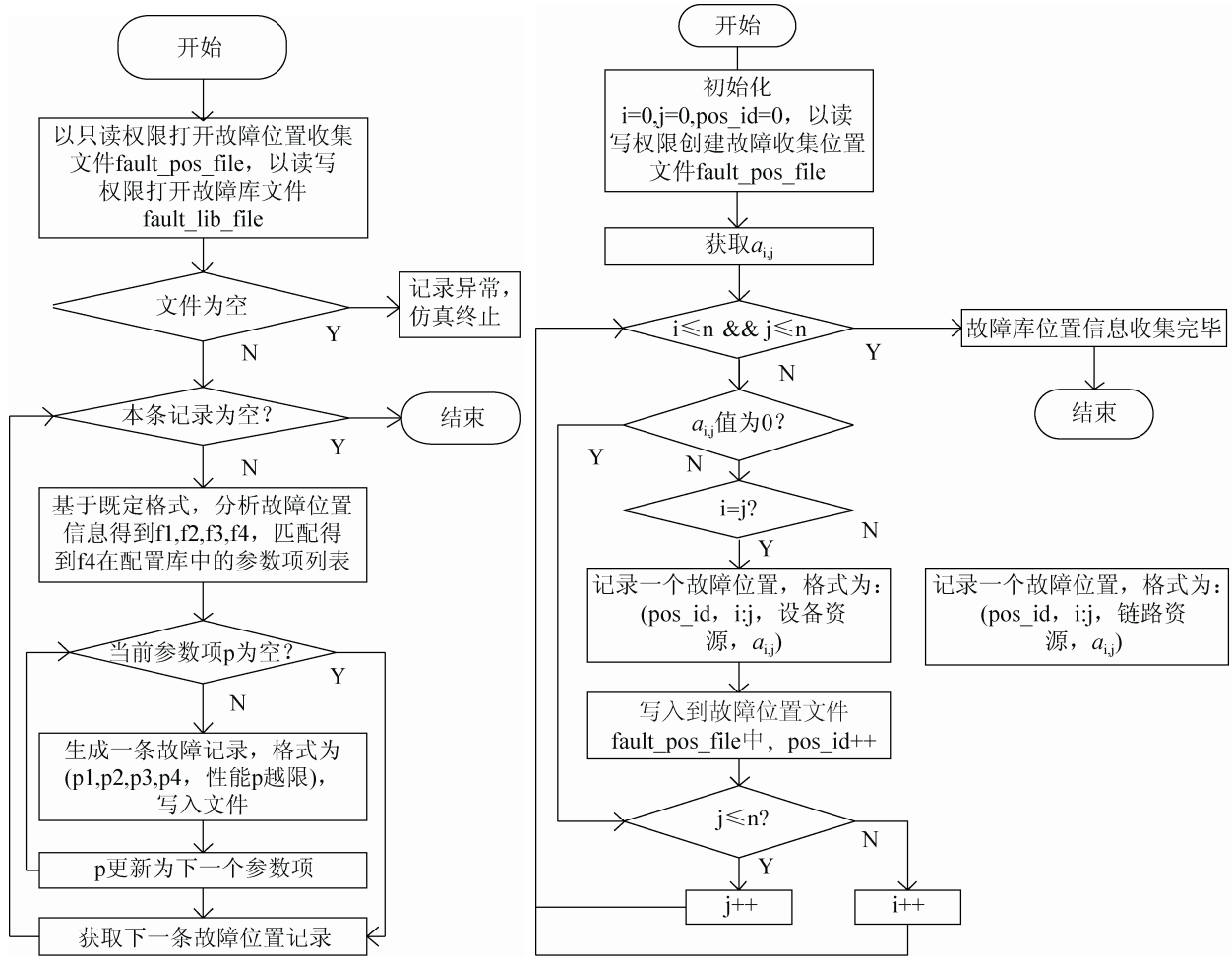
2.2.2 故障库自动生成算法设计

在基于仿真的信息系统环境中，系统设备或者网络链路均可能因为断电、人为误操作等原因导致不能正常运行。假设管理控制模块为信息系统提供的仿真参数包括：信息系统节点个数 n，信息系统参数矩阵 $A=\{a_{i,j}\}$。当 $i=j$ 时，$a_{i,j}$ 表示设备类型编号，当 $i\neq j$ 时，表示链路类型编号。

故障自动生成算法步骤如下所述：

1) 基于信息系统参数矩阵 $\boldsymbol{A}$，对于每一个非 0 位置上的设备或链路，设定为系统可能发生故障的一个注入位置，并按照(编号 pos_id，位置 i:i，设备资源或链路资源，性能类型编号)的格式存储于故障位置收集文件 fault_pos_file 中，流程如图 4(a)所示。

2) 基于 fault_pos_file 文件，对每一条故障位置记录，收集配置库中值 $a_{i,j}$ 对应的设备或链路资源的性能参数，以其每一项性能参数极限值作为一重故障类型，生成一条故障信息记录，存储于故障库文件 fault_lib_file 中，流程如图 4(b)所示。



(a) 故障位置收集流程图 (b) 故障库生成流程图

图 4 故障库自动生成算法

2.2.3 故障注入算法设计

基于故障库自动生成算法确定故障库信息，从中选择任意故障，按照格式配置故障参数，可实现任意时刻任意位置任意故障的注入。四元组故障参数配置格式如下所示：

$$\left(N, \underbrace{id_1 / id_2 / \cdots id_n}_{\mathrm{ID}}, \underbrace{bt_1 / bt_2 / \cdots bt_n}_{\mathrm{BT}}, \underbrace{et_1 / et_2 / \cdots et_n}_{\mathrm{ET}}\right)$$

其中，字段 N 表示故障个数，字段 ID 表示故障模式编号集合，字段 BT 表示故障开始时刻集合，字段为 ET 故障结束时刻集合。ID 字段包括 n 个故障模式编号 id_i，BT 字段包括 n 个故障开始时刻 bt_i，ET 字段包括 n 个故障结束时刻 et_i，字段间使用分隔符“/”。

故障注入步骤如下所述：

1) 状态初始化。将目标系统和其组成单元的状态变量值初始化为“0”，即为正常状态。

2) 遍历字段 ID。获取当前故障模式编号 id_i；

3) 故障库匹配。以 id_i 为关键字，在故障库中找到此种故障模式对应的故障位注入位置 p；

4) 故障注入。使故障注入位置 p 处的单元的状态变量值在故障开始时刻 bt_i 到故障结束时刻 et_i 时间段内保持为“1”，即故障状态，在 et_i 时刻之后恢复为“0”，即正常状态；

5) 判断是否注入完毕，若所有故障已经注入完毕，则执行步骤 6)，否则继续执行步骤 2)；

6) 故障注入结束。

3 仿真实验

3.1 仿真环境

操作系统：Windows 操作系统

软件环境：Cygwin 软件，NS2 仿真软件

硬件环境：1 台 Intel(R) Xeon(R) 2.27 GHz 处理器，8 GB 内存和 320 GB SCSI 硬盘的服务器。

3.2 仿真场景

测试使用目标信息系统的架构如图 5 所示，设置仿真开始时刻为 0.1 s，仿真结束时刻为 30 s，通信流量符合指数 On/Off 分布。

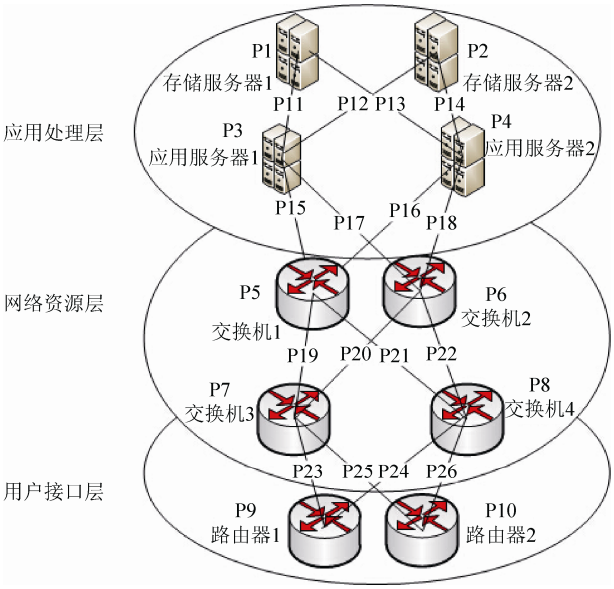


图 5 目标系统架构

测试向目标信息系统注入有 4 个独立故障组成的组合故障。设置故障位置为 P15-P18 编号的网络链路，并设置注入时刻为 8.0 s，故障结束时刻为 15 s，则形成故障参数如下：(2, P15/P16/P17/P18, 8.0/ 8.0/8.0/8.0, 15.0/15.0/15.0/ 15.0)。

3.3 仿真结果

基于信息系统架构，按照故障注入设计方案，故障库中存在 26 个可注入位置。利用 NS2 仿真平台对系统进行仿真，利用 NAM 工具追踪到的信息系统的状态变化情况如图 6 所示。

```
l -t 8 -s 6 -d 4 -S DOWN
v -t 8 link-down 8 6 4
l -t 8 -s 4 -d 6 -S DOWN
v -t 8 link-down 8 4 6
l -t 8 -s 4 -d 6 -S DOWN
v -t 8 link-down 8 4 6
l -t 15 -s 5 -d 3 -S UP
v -t 15 link-up 15 5 3
l -t 15 -s 5 -d 3 -S UP
v -t 15 link-up 15 5 3
l -t 15 -s 3 -d 5 -S UP
```

图 6 系统状态数据

在系统状态数据中，–t 为时间，–s 为源节点编号，–d 为目的节点编号，–s 为链路状态(UP 为正常状态，DOWN 为故障状态)。监视数据显示，ASPBOFJ 仿真平台正确地按照故障注入参数完成了故障注入，并引起相应系统单元的状态变化，有无故障注入情况下的仿真运行数据量变化如图 7 所示。

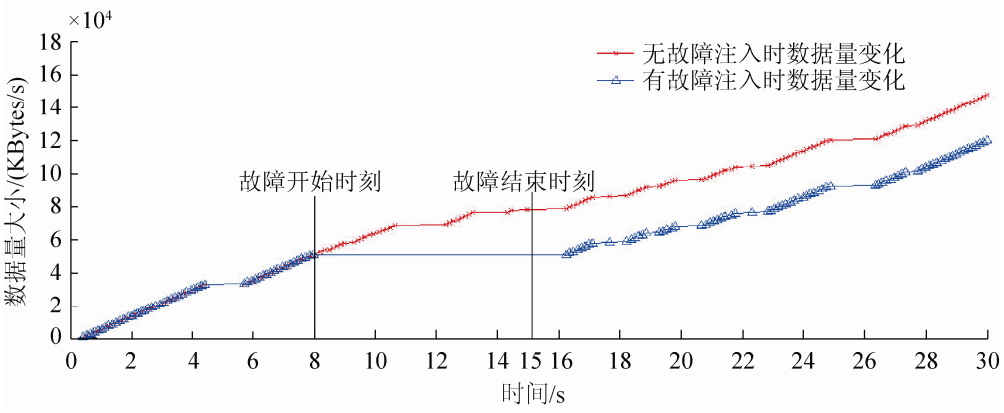


图 7 无故障注入情况下的仿真数据量变化情况对比

自 8 s 时刻故障开始至 15 s 时刻故障结束，数据量变化值保持为 0，说明系统此时不能正常和用户进行通信，与网络链路断路的影响结果一致。数据结果证明了本系统注入故障的正确性和有效性。

4 结论

本文研究并设计了一种故障注入通用仿真平台 ASPBOFJ，通过对信息系统通用仿真模型的建立，设计一种故障库生成算法对信息系统进行故障导入。实验结果表明，ASPBOFJ 仿真平台能够实现任意需求的信息系统仿真，并能够保证任意时间任意位置注入故障的正确性和有效性。

但是，目前 ASPBOFJ 平台仅能向目标信息系统注入随机类型离散故障，而缺少对持续故障、间歇故障和渐变不等幅故障的注入支持能力，如何实现通用类型的故障注入模型是下一步研究的主要方向。

参考文献:

[1] 胡嘉伟, 江建慧. 一种面向软件可靠性评估的故障注入机制的设计与实现 [J]. 计算机辅助设计与图形学学报, 2012, 24(6): 741-751.

[2] 李志宇, 黄考利, 连光耀. 基于测试性设计的软件故障注入研究综述 [J]. 计算机测量与控制, 2013, 21(5): 1113-1114.

[3] 马存宝, 陈敬松, 刘坤. 基于FLSIM的实时飞行故障仿真系统 [J]. 计算机仿真, 2007, 24(10): 59-62.

[4] 尹青, 蔡伯根, 上官伟, 等. 故障注入方法在列车运行控制仿真系统中的应用 [J]. 铁道通信信号, 2013, 49(1): 66-70.

[5] 董健康, 秦庆霞, 刘家学, 等. 基于BEDTPN的飞机供电系统故障仿真 [J]. 系统仿真学报, 2012, 24(10): 2215-2221.

[6] 戴成建, 董世良. 双余度电传刹车系统仿真试验环境设计与应用 [J]. 系统仿真学报, 2011, 23(增1): 123-126.

[7] 花良浩, 殷芝霞, 杨蒲. 无人机故障注入与故障诊断实时仿真平台研制[J]. 计算机应用与软件, 2013, 30(8): 106-142.

[8] 吴喆, 景博, 余思奇,等. 基于半实物仿真的测试性验证系统设计与实现[J]. 计算机测量与控制, 2013, 21(9): 2349-2351.

[9] 李志宇, 黄考利, 连光耀. 基于半实物仿真的故障注入系统设计[J]. 计算机测量与控制, 2013, 21(3): 570-576.

[10] 曾宪炼, 马捷中, 任向隆, 等. 基于VHDL的故障注入技术 [J]. 计算机工程, 2010, 36(11): 244-249.

[11] Pournaghdali F, Rajabzadeh A, Ahmadi M. VHDLSF: A simulation-based multi-bit fault injection for dependability analysis [C]// 2013 Third Computer and Knowledge Engineering International Conference, Mashhad, Iran. USA: IEEE, 2013: 354-360.

[12] Qi-tao Gan, Bjarne E H. Dependability modeling and analysis of networks as taking routing and traffic into account [C]// Next Generation Internet Design Internet Design and Engineering, Valencia, Spain. USA: IEEE, 2006: 8-32.

[13] 伍文, 孟相如, 刘芸江, 等. IP 网络可生存性模型中故障模型的构建和仿真 [J]. 小型微型计算机系统, 2013, 3(3): 567-571.

(上接第 314 页)

[15] Jessica L. Development of a Small Sonar Altimeter and Constant Altitude Controller for a Miniature Autonomous Underwater Vehicle [D]. Virginia, USA: Virginia Polytechnic Institute and State University, 2005.

[16] 方学东. 基于大圆航线的RANV航路规划 [J]. 中国民航飞行学院学报, 2006, 17(2): 3-6.

[17] Aydan C. Constant altitude–constant mach number cruise range of transport aircraft with compressibility effects [J]. Journal of Aircraft (S0021-8669), 2006, 43(1): 125-131.

[18] 高晓光. 航空军用飞行器导论 [M]. 西安: 西北工业大学出版社, 2004.

[19] D Yang, J Zhou, T Chen. The design of flight control law based on integral separation PID algorithm [C]// Proceedings of the 2011 International Conference on Electronics and Optoelectronics. USA: IEEE, 2011, **7**: 29-31.

[20] 李世秋, 郑成军, 陶德桂. 小型无人靶机掠海定高飞行控制系统设计与实现 [J]. 现代电子技术, 2009, 32(19): 62-65.

[21] 郭乃林, 王建辉, 雷英杰. 军事训练想定中的三维航迹仿真模型 [J]. 系统仿真学报, 2002, 14(4): 534-538.

[22] H Xu, J Huang, Y Zhou. Design of multi-mode flight control system for unmanned helicopter [C]// Proceedings of the 30th Chinese Control Conference. USA: IEEE, 2011, 7: 3660-3663.