·移动互联与通信技术· 文章编号：1000-3428(2017)11-0040-05 文献标志码：A 中图分类号：TP391

基于 SDN 架构的网络故障检测与修复系统

薛华威，王宝生，邓文平，高先明

（国防科学技术大学 计算机学院，长沙 410073）

摘 要：在基于机器学习和基于贝叶斯网络的故障检测方法中，检测结果只是基于概率或者历史信息的推断，难以应用于网络故障检测与自动修复系统。针对该问题，提出基于产生式规则的故障检测方法，对已知故障自动下发安全策略进行阻断，对未知故障以告警形式通知网络管理员，同时设计一种自适应轮询算法，进一步减少系统开销并保证故障响应实时性。实验结果表明，该方法能够减少轮询开销，有效抑制报文异常。

关键词：故障检测；产生式规则；状态收集；事件通知；自适应轮询

中文引用格式：薛华威，王宝生，邓文平，等. 基于 SDN 架构的网络故障检测与修复系统[J]. 计算机工程，2017，43(11)：40-44.

英文引用格式：XUE Huawei，WANG Baosheng，DENG Wenping，et al. Network Fault Detection and Repair System Based on SDN Architecture[J]. Computer Engineering，2017，43(11)：40-44.

Network Fault Detection and Repair System Based on SDN Architecture

XUE Huawei，WANG Baosheng，DENG Wenping，GAO Xianming

（School of Computer，National University of Defense Technology，Changsha 410073，China）

【Abstract】Detection results of the fault detection method based on machine learning or Bayesian network are only based on the inference of probability or historical information. Therefore，it cannot be applied to the fault detection and automatic repair system. Aiming at this problem，this paper proposes a fault detection method based on production rules. It makes the known failure be automatically issued and the unknown failure be notified to the network administrator through alarm form. Meanwhile，it proposes a self-adaptive polling algorithm to further reduce the overhead of the system without losing the response time of the fault. Experimental result shows that the proposed method can reduce polling overhead and control message exceptions effectively.

【Key words】fault detection；production rule；state collection；event notification；self-adaptive polling

DOI：10.3969/j.issn.1000-3428.2017.11.007

0 概述

随着互联网高速的发展，越来越多的业务采用“互联网 +”的模式，互联网深入生活的方方面面，如常见的点餐业务美团、出行打车业务滴滴以及支付业务微信、支付宝等。因此，网络系统的安全和稳定是现代生活的基本保证，如果出现崩溃，将会造成日常生活的崩溃或者巨大损失。据统计，一个局域网在一年之内出现的故障次数可高达二十多次，由此产生的网络中断服务时间在十几个小时，而大型运营商如电信、移动等公司，几个小时的中断可能造上亿美元的经济损失，因此，如何保证网络的安全运行，在出现故障时是否能够及时发现并进行适当的修复，是当前最为重要的问题之一。

目前，研究者已提出大量的网络故障检测方法[1-2]，这些方法大多基于贝叶斯网络[3]、人工智能[4-5]、神经网络[6]等技术，通常具有自主学习的功能，但检测结果却是基于历史信息的一种推断，仅供网络管理人员参考，并且不能对故障进行准确定位，因此，不适合网络故障检测和自动修复系统。此外其他一些基于依赖图[7]、决策树[8]的故障检测方式，虽然能有效地保证故障检测的准确性，但却不具备自动修复的功能。

进行故障检测的前提是获取当前网络的状态信息，关于如何降低状态获取时的系统开销，而又能保证故障检测的实时性，目前有较多研究[9-11]，主要分为轮询、事件通知以及轮询 + 事件通知 3 类。其中，轮询规定 T 时间周期定时获取网络状态信息，但存在时间周期如何设置的问题；事件通知采用异步通

作者简介：薛华威（1991—），男，硕士研究生，主研方向为软件定义网络、网络管理；王宝生，教授；邓文平，助理研究员；高先明，博士。

收稿日期：2016-10-09 修回日期：2016-11-18 E-mail：huaweicanfly@163.com

知机制,但存在代理端崩溃无法发送事件通知的问题;轮询 + 事件通知的方式在一定程度上可以解决轮询开销和故障响应时间问题,但却要求在代理端维持网络的状态信息,造成代理端的系统开销和维护开销。

针对上述问题,本文设计基于软件定义网络(Software Defined Network,SDN)架构的网络故障检测与修复系统,采用基于产生式规则的方式进行故障检测,从而实现对已知故障的准确检测和有效阻断。此外,还设计一种自适应轮询方式,在轮询系统开销和故障响应时间之间取得均衡。

1　网络故障检测与修复

本文系统架构借鉴了 SDN 思想,即采用模块化的设计思想,共分为 4 层:用户接口,业务层,控制层,设备层。该系统的总体架构如图 1 所示。

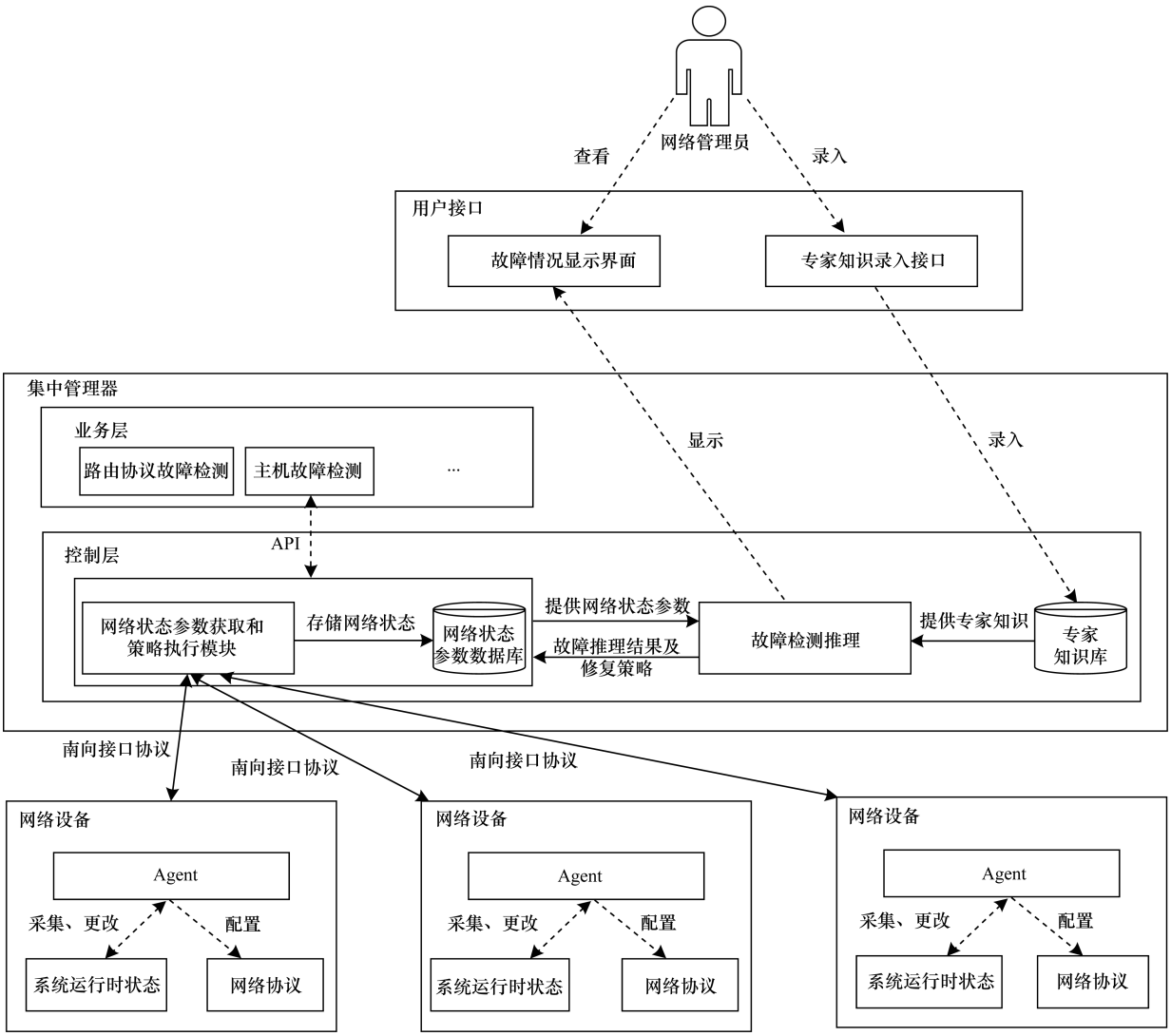


图 1　系统总体架构

系统中各个模块的功能描述如下:

1)用户接口。该模块负责显示网络故障推理模块诊断的故障信息,将故障或者告警显示在图形界面中,供管理人员进行参考;同时提供接口供管理人员录入专家知识到专家知识库中,为故障检测提供依据。

2)业务层。该模块通过调用响应的 API 来进行业务模块的实现,路由故障信息检测模块则调用获取路由状态信息的 API。模块之间相互独立。

3)控制层。该模块包括 3 个子模块:网络状态参数获取和策略执行模块,故障检测推理模块,网络状态数据库和专家知识库。网络状态参数获取和策略执行模块负责执行业务层调用的 API,获取设备层的网络状态信息,并将信息存储到网络状态数据库中。网络故障检测推理模块根据网络状态数据库中信息,由专家知识库进行分析,得出相应的诊断结果,并对已知故障根据专家知识库给出故障修复策略,由网络状态参数获取模块和策略执行模块执行安全策略进行修复。具体处理流程如图 2 所示。

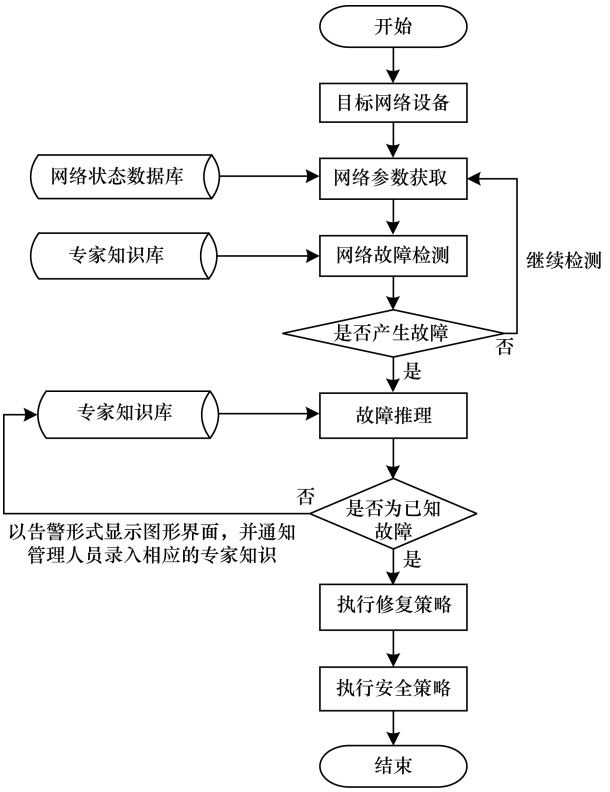


图 2 控制层处理流程

4)设备层。该模块负责获取网络状态信息,并对响应的网络协议进行配置。设备层和控制层通过南向接口协议进行通信,如常见的 CLI、SNMP、NETCONF 等。

2 基于产生式规则的故障检测方法

系统的知识库即使用的是产生式规则,因此,如何定义和实现产生式规则对系统至关重要。

2.1 产生式规则

产生式规则[12]是产生式系统的一个基本概念,通常被用于对产生式系统中的推理过程和行为进行描述。产生式规则的前半部分是条件或者前提,后半部分是结论或者操作,各个条件可以使用逻辑与、或组成不同的组合[13]。当满足产生式的条件也就是前半部分时,应采取相应的动作或者得出相应的结论。

产生式系统的执行过程实际上就是根据控制策略运行产生式规则进行匹配的过程[14],其主要过程有匹配和操作 2 个过程。匹配过程是将当前收集的网络状态信息与产生式规则的条件进行匹配,如果满足条件,则执行后面的结论或者操作。

基于网络的可靠性方面考虑,如果要对故障进行自动修复,则要求故障的诊断必须是无误的、确定性的,即对已知的故障进行自动修复[15],对于未知的故障向网络管理人员告警,由网络管理人员做进一步的分析。针对这一诊断特点,基于产生式规则对网络进行故障检测非常合适。根据网络专家的以往经验或者管理知识,通过归纳,将其抽象为产生式规则,然后进行诊断推理,这种方式不但诊断过程比较简单,而且诊断快速、准确,比较贴近显示中网络管理人员进行故障排错的过程。

2.2 产生式规则的存储与匹配

通常在产生式规则中格式是 IF < 条件 > 或者 < 前提 >,THEN < 结论 > 或者 < 操作 >,使用 AND 和 OR 逻辑连接符号,将多个条件进行连接。如 IF (A AND B)OR C,THEN D,即当 A 和 B 同时满足,或者 C 满足时,得出结论 D 或者执行 D 操作。其中 A、B、C 是网络状态数据库中的数据。

存储方式定义:在产生式规则中,采用树的形式进行存储,树节点是由指针和 value 组成,value 是条件中的属性如 A、B、C 等,树根只有指向子节点指针,value 为空,父子节点间是 AND 关系,兄弟节点间是 OR 关系或者无逻辑关系,树的叶子节点存储策略以及得出的具体某一故障信息。

按上述定义对产生式规则进行存储,形成如图 3 所示的存储结构。

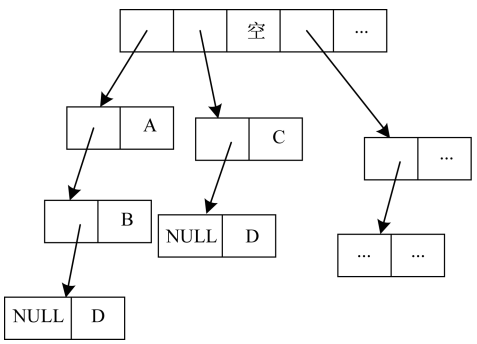


图 3 产生式规则存储结构

收集完网络状态进行故障检测的过程实际上是对上述存储树的一个匹配过程,即从上到下对每一个分支进行匹配,如果遇到不匹配,即返回上上一个分支处,直到所有的分支执行完,即完成了整个网络状态的故障检查,这其实就是一个受限的树的深度优先遍历的过程。

设 $P_1 \sim P_n$ 表示一个树节点的 n 个指针,N_i 表示树的第 i 个节点,N_iP_j 表示第 i 个树节点的第 j 个指针,其中 $i,j \in [1,n]$,Stack 是栈数据结构,算法具体描述如下:

1)遍历根节点,将 $N_0P_1 \sim N_0P_n$ 依次入栈。

2)弹出栈顶元素 N_iP_j。

3)判断 N_iP_j 指向的 N_j 节点是否是叶子节点,如果是叶子节点,则读取该叶子节点的 *value*,执行该策略或者将该故障以告警形式通知网络管理人员,否则进行匹配,如果匹配不成功,则返回 2);如果匹配成功则将 $N_jP_1 \sim N_jP_n$ 依次入栈。

4)重复 2)、3)操作直到栈为空,即完成对网络状态的故障检测。

由于是基于受限的树的深度优先遍历,因此时间复杂度最高为 $O(n^2)$,其中 n 是树节点的数量。

3　自适应轮询算法

为了减少故障响应时间,就要减少轮询周期,即增加轮询系统开销;为了减少轮询的系统开销,就要以牺牲故障响应时间为代价。为解决这一问题,本文提出了自适应轮询算法,以达到系统开销和故障响应时间之间的均衡。

自适应轮询模型定义为:控制器设置 2 个轮询时间周期 T,分别记录为 T_1 和 T_2(规定 $T_1 < T_2$),设 DT 为实际使用的轮询周期,将 DT 初始化为 T_1,然后根据网络状态进行动态调整 DT($DT \in [T_1, T_2]$)。

设 i 是累计无故障的次数,则算法具体描述如下:

1)令 $DT = T_1$,$i = 0$。

2)每隔 DT 时间获取网络状态进行检测,若无故障发生,则 $i++$,$DT += i$;若有故障发生,则 $i = 0$,$DT = T_1$。

3)如果 $DT > T_2$,则令 $i = 0$,$DT = T_1$,重复 2)。

采用上述算法可以避免轮询周期设置不合理的问题,在网络状态良好情况下逐渐增大轮询周期,同时由于网络故障发生具有不确定性,因此 DT 的数值不能无限变大,当 DT 的数值超过 T_2 时,将 DT 设为 T_1,以保证网络故障响应实时性。

4　实验与验证

本节搭建了基于 SDN 架构的网络故障检测与修复原型系统,并对其异常检测时间、策略下发时间等进行测试,然后通过错误配置路由器 OSPF Router-ID 来验证系统有效性。

4.1　实验环境

为评估本文系统,对该系统在校园网内进行了实际部署。集中控制器部署在一台接口带宽为 2 Gb/s的 IBM x3650 服务器上,Agent 代理端部署在校园网内的所有网络设备上,控制器和网络设备采用直连接口进行通信,另外采用 2 台笔记本电脑接入校园网作为 VLC 的客户端和服务器进行交互,测试网络通信情况,实验拓扑如图 4 所示。

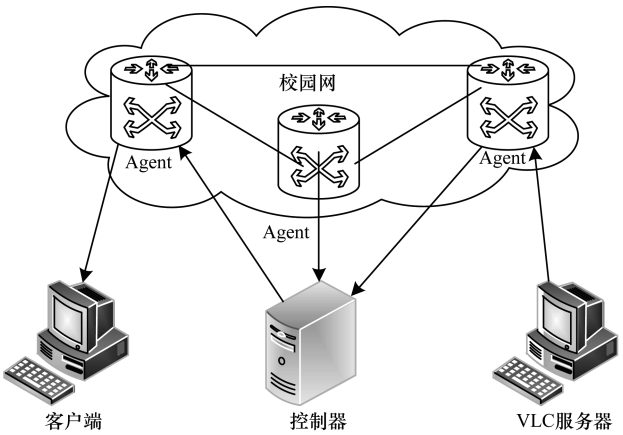


图 4　实验拓扑

4.2　异常检查时间

故障检查时间是指网络异常出现时间到系统检测到网络异常并完成网络异常分析的时间间隔。本文设置 T_1 为 5 min,T_2 为 30 min,因此,实验统计了 30 次异常检测时间,其实验结果如图 5 所示。

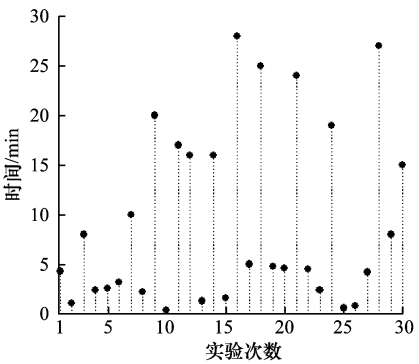


图 5　异常检测时间

通过实验分析异常检测时间可知:异常检测时间分布在 0 min ~ 30 min,这由该系统采集信息节点的自适应轮询机制决定。异常检测最大时间是 30 min,即网络累计无故障次数在 25 次后;最小时间是刚发生故障就达到轮询周期。实验结果表明,自适应轮询周期调整机制可以有效减少轮询开销。

4.3　策略下发时间

策略下发时间是指从检查到异常到进行下发安全策略作用到设备,并返回执行状态时间间隔。因此,本文统计了 50 次策略下发时间,实验结果如图 6 所示。

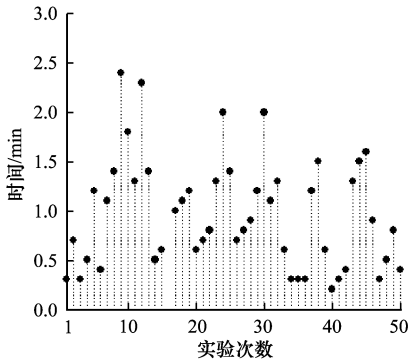


图 6 策略下发时间

通过实验分析策略下发时间可知:策略下发时间大于等于 0.3 s,这是由于控制器每次是按照单个网络设备单个配置命令进行执行的,即非并行执行的,0.3 s 是控制器给一台网络设备下发一条命令的时间,而且策略下发时间在图 6 中表现有长有短,原因是有的异常的解决,即策略的下发需要给多个网络设备下发多条命令。如拓扑一致性检查时,若发现多个路由器的 OSPF 进程发生宕掉事故,则需要给多台路由器下发 OSPF 启动配置命令。

4.4 OSPF Router-ID 冲突

为演示方便,在客户端通过 VLC 协议从 VLC 服务器获取视频流并播放,统计在运行该系统前后视频流报文数随时间的变化情况,本文通过 wireshark 来获取该视频流的报文数。wireshark 生成的报文统计图如图 7 所示。可以看出,在 700 s ~ 1 125 s之间,视频流报文时有时无,即网络处于由 router-id 冲突故障导致的不稳定状态,不停在“抖动”。1 074 s 时部署该系统后,1 125 s 以后视频流报文保持正常,即该系统在 51 s 内检测到异常,(其中约有 50 s 用于信息采集上),并下发安全策略进行了修复,即信息采集以及策略下发共消耗 51 s 左右的时间,这是因为 Router-id 冲突异常只需要给一台设备下发一条命令即可,说明该系统能有效抑制异常。

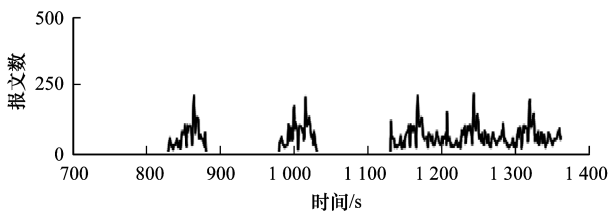


图 7 视频流报文数

5 结束语

本文提出基于 SDN 的网络故障检测与修复系统,通过基于产生式规则的故障检测方式,提高了故障检测的准确性。此外,设计自适应轮询机制,有效地解决了轮询开销和故障响应时间不能均衡的问题。下一步将继续完善本文系统的功能,并将其部署到更大的网络范围中进行验证。

参考文献

[1] 石 磊.网络故障定位与检测技术研究[D].南京:南京理工大学,2006.
[2] 王道平,冯振声.故障诊断专家系统中不确定性问题[J].计算机工程与应用,1998,34(12):33-35.
[3] 李俭川,胡茑庆,秦国军,等.贝叶斯网络理论及其在设备故障诊断中的应用[J].中国机械工程,2003,14(10):896-900.
[4] BHATTACHARYYA S, KUMAR R, HUANG Z. A Discrete Event Systems Approach to Network Fault Management: Detection and Diagnosis of Faults[J]. Asian Journal of Control,2011,13(4):471-479.
[5] DAWES N, ALTOFT J, PAGUREK B. Network Diagnosis by Reasoning in Uncertain Nested Evidence Spaces[J]. IEEE Transactions on Communications, 1995,43(2-4):466-476.
[6] CHENGCAI M, XIAODONG G. Fault Diagnosis with Fault Gradation Using Neural Network Group[J]. Systems Engineering and Electronics, 2009, 31(1): 225-228.
[7] 朱有产,窦炳林.基于依赖图的网络故障定位算法[J].大连理工大学学报,2005,45(s1):73-77.
[8] 曲朝阳,高宇峰,聂 欣.基于决策树的网络故障诊断专家系统模型[J].计算机工程,2008,34(22):215-217.
[9] DINI P, BOUTABA R. Deriving Variable Polling Frequency Policies for Pro-active Management in Networks and Distributed Systems[C]//Proceedings of IFIP/IEEE International Symposium on Integrated Network Management. New York, USA: Springer US, 1997:541-552.
[10] JIAO J, NAQVI S, RAZ D, et al. Toward Efficient Monitoring[J]. IEEE Journal on Selected Areas in Communications,2000,18(5):723-732.
[11] DILMAN M,RAZ D. Efficient Reactive Monitoring[J]. IEEE Journal on Selected Areas in Communications, 2002,20(4):668-676.
[12] 陈 敏,李 旺.计算机网络中的故障定位技术研究[J].国外电子测量技术,2007,26(7):8-11.
[13] ZHAO S,DILLON T S. Incorporating Prior Knowledge in the Form of Production Rules into Neural Networks Using Boolean-like Neurons[J]. Applied Intelligence, 1997,7(4):275-285.
[14] JAIN S,JAIN N K. Learning Techniques in Extended Hierarchical Censored Production Rules (EHCPRs) System[J]. Artificial Intelligence Review,2012,38(2): 97-117.
[15] 李福亮,杨家海,吴建平,等.互联网自动配置研究[J].软件学报,2014,25(1):118-134.

编辑 金胡考