文章编号:1001 - 9081(2006)11 - 2536 - 03

基于场景模型的 BGP-4 健壮性测试

戴经国[1,2],王乐春[2],钟海荣[2],张春元[2]
(1. 湖南人文科技学院 计算机科学技术系, 湖南 娄底 417000;
2. 国防科学技术大学 计算机学院,湖南 长沙 410073)
(djghzp@163.com)

摘 要:提出了一种系统实现协议健壮性测试的新方法。该方法通过深入分析 BGP 的路由信息处理过程,建立场景模型来描述决策过程和更新过程的应用环境和控制参数,并基于该模型提出了健壮性测试案例生成方法。路由协议 BGP 的实际测试应用表明,该方法避免了组合爆炸问题,生成的反向测试集的检错能力是正向测试集的 2.3 倍。

关键词:BGP 协议;路由信息处理;场景模型;健壮性测试;测试集
中图分类号: TP393.04 **文献标识码**:A

Robustness-testing of BGP-4 based on scenario model

DAI Jing-guo[1,2], WANG Le-chun[2], ZHONG Hai-rong[2], ZHANG Chun-yuan[2]
(1. *Department of Computer Science and Technology, Hunan University of Humanities Science and Technology, Loudi Hunan* 417000, *China*;
2. *School of Computer Science, National University of Defense Technology, Changsha Hunan* 410073, *China*)

Abstract: A new systematic robustness testing approach was proposed. Based on the analysis of RI-PRO, the scenario model was built to describe the applied environments and control parameters in decision and route update process. Then a new generation method of robustness—testing suite was presented. Some critical techniques related to the approach were investigated, such as the relationship set and the searching spaces of the robustness testing. Robustness testing of BGP indicates that this approach can avoid combinational explosion. Compared with positive test suit, the error-detecting ability of negative test suit generated by this approach is enhanced by 1.3 times.

Key words: BGP protocol; RI-Pro; scenario model; robustness-testing; test suit

0 引言

Internet 协议的健壮性原则[1]是“严以律己,宽以待人”,它要求协议实现对发出的信息要严格,同时对接收的信息要大度。目前,BGP-4(Border Gateway Protocol 4)[2]已经成为 Internet 域间路由的事实标准,是 Internet 体系结构中的核心控制组件。复杂的网络环境对 BGP 的健壮性提出了巨大的挑战,协议实体的任何实现缺陷以及错误使用都将直接影响到 Internet 的连通性、可靠性和安全性。在 BGP 应用到 Internet 之前,除了进行一致性和互操作测试以外,必须对 BGP 实现进行健壮性测试。

路由协议用于动态地更新路由表,其功能可以分成两部分:网络通信(Network Communication,NC)和路由信息处理(Routing Information Processing,RI-Pro)。NC 主要实现底层网络访问,检测本地网络连接变化,并为路由信息流提供稳定可靠的通信。文献[3]给出了 BGP 协议 NC 部分的健壮性描述——RFSM 模型,并且提出了基于该模型的健壮性测试案例的生成解决方案。

RI-Pro 是路由协议的核心内容,其主要功能是路由信息的计算和路由表的更新,以及新的路由信息的生成和传播。RI-Pro 是协议测试的主要对象。目前一些商用测试系统,如 HP 公司的 RouterTester,IXIA 公司的 ANVL 等,虽然可以对 BGP 的 RI-Pro 过程进行一致性测试,并且可以进行某些强度测试,但这些测试都是根据 ISO9646[4]设计的,因此都没有脱离一致性测试的框架。

本文在深入分析 BGP 协议处理过程的基础上,对 RI-Pro 进行抽象,提出了场景模型。并在该模型的基础上,提出了健壮性测试案例的生成方法。

1 RI-Pro 分析与场景模型

1.1 RI-Pro 分析

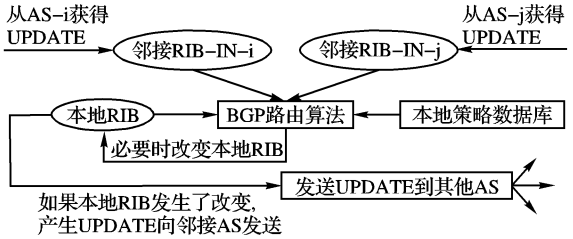

图 1 BGP 路由更新处理过程

文献[2]制定了 BGP 的 RI-Pro 的标准。在该标准中,RI-

收稿日期:2006 - 05 - 17;**修订日期**:2006 - 06 - 26 **基金项目**:国家自然科学基金资助项目(60573103)

作者简介:戴经国(1962 -),男,湖南双峰人,副教授,硕士,主要研究方向:网络基准测试、信息安全; 王乐春(1971 -),男,山东德州人,博士,主要研究方向:网络基准测试、协议工程; 钟海荣(1971 -),男,湖南耒阳人,博士,主要研究方向:分布式计算; 张春元(1964 -),男,福建福州人,教授,博士生导师,博士,主要研究方向:分布式计算、微处理器.

Pro 的功能是根据接收到的 UPDATE 消息中的路由项进行新路由的计算、决策和发布。路由更新处理过程如图 1 所示。

在协议实现中,由于协议实现者只需保证该实现与标准保持外部可观察的一致性,往往依据自身对协议的理解和实际需要,对处理过程进行修改。如 Cisco 就对协议规定的第二个阶段——最佳路由选择进行了较大的修改。

RI-Pro 的实现和标准规定可能差别很大。要生成通用的测试集就必须对该过程进行重新抽象建模,使得新模型既保持原有协议标准规定的外部可观察的内容,同时又丢弃原协议的一些对于测试没有价值的细节描述,并且还要增加许多专门用于协议健壮性测试的内容。构建的新模型必须有利于协议的健壮性分析,并且可以辅助生成健壮性测试案例。

1.2　RI-Pro 场景模型

所有的会话、输入、输出和控制信息构成了该更新过程的应用环境。所谓 RI-Pro 的场景模型是指刻画路由更新处理和决策过程应用环境的模型。该模型重新对 RI-Pro 进行描述,不再研究 RI-Pro 的内部过程和实现方法,只研究在控制参数设定的应用环境下,在特殊选定的激励下,RI-Pro 的行为表现和输出结果。图 2 为 BGP 的 RI-Pro 的场景模型。

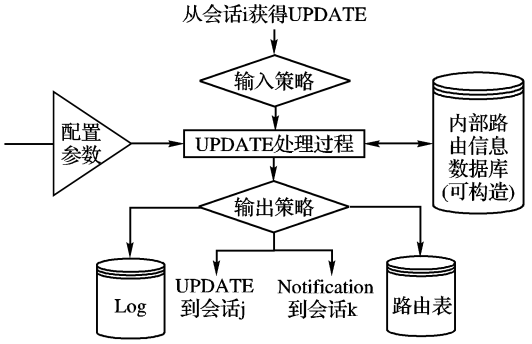

图 2　路由更新处理过程的场景

其中会话集合包括外部会话和内部会话;输入集合包括 UPDATE 输入和本地 RIB 库;输出集合包括输出 UPDATE、路由表、Log 文件和 Notification 事件;控制集合包括输入策略库、BGP 配置参数和输出策略库。

1.3　场景模型的形式化描述

场景模型可由 $< S, I, K, O, \Delta >$ 五元组表示,其中 S 为会话集合,I 为输入集合,K 为控制集合,O 为输出集合,Δ 为关系集合,具体定义为:

$S = \{S_e, S_i\}$,S_e 为 BGP 外部会话集合,S_i 为 BGP 内部会话集合。

$I = \{u_i, D, I'\}$,u_i 为输入更新报文,用于添加或删除路由。D 为路由重发布集合。I' 为外部不可见的本地路由库,可以通过更新报文输入或路由重发布可对该库的内容进行控制。

$D = \{s_i, c_i, f_i, P\}$,s_i 是静态路由,c_i 是直连路由,f_i 是缺省路由,集合 P 是其他路由协议生成的路由集合。

$P = \{p \mid p$ 是其他路由协议生成的路由$\}$,这些路由用于路由协议之间的重发布。

$K = \{E, Z, H\}$,E 为输入策略集,Z 为 BGP 配置参数,H 为输出策略集。

$E = \{\varepsilon_1, \varepsilon_2, \varepsilon_3, \cdots\}$,$\varepsilon_i$ 为一条输入策略。

$Z = \{\zeta_1, \zeta_2, \zeta_3, \cdots\}$,$\zeta_i$ 为配置的一个参数。

$H = \{\eta_1, \eta_2, \eta_3, \cdots\}$,$\eta_i$ 为一条输出策略。

$O = \{u_o, T, l, n\}$,u_o 为输出更新报文,T 为路由表,l 为 Log 文件,n 为 Notification 事件,T 为路由表,T 定义为:

$T = \{r_1, r_2, r_3, \cdots\}$,$r_i$ 为路由表中的一项。

$\Delta = \{\delta \mid \delta$ 为一种组合关系$\}$,δ 是抽象关系,表示相关或制约关系。如 $k_i \delta k_j (k_i, k_j \in K)$ 就表示两个控制参数之间存在着 δ 制约关系。

该场景模型对协议规定的 RI-Pro 进行了较大改造,取消了三阶段处理过程和 RIB 的分类,对外部不可见的所有内部计算和决策都不予考虑。但是该模型对协议规定的外部输入、输出和可观察动作不仅予以全部保留,并且重新归类。该模型中组合关系的使用,赋予了该模型以灵魂,使得该模型不是对 RI-Pro 外部行为的简单重复描述,更不是把 RI-Pro 的处理过程退化成只能从外部观察的黑盒;而是从外部所有可利用资源的关系上重新审视该处理过程。从外部可观察行为上来说该模型与原处理过程是相同的,但是在认识上,该模型不再单纯研究 RI-Pro 的功能,而是研究 RI-Pro 的所有可控资源的关系,因此深化了对 RI-Pro 的认识。

RI-Pro 的实现者和测试者都可以使用该场景模型。实现者在实现 RI-Pro 时可以通过分析场景的变化,对未来应用场景进行全面的考虑,不会单纯地使用协议描述进行实现,从而增强协议实现的健壮性。测试者通过生成控制参数和输入数据,来分析路由处理过程的实现情况,或者判断路由器接入实际网络前是否错误地配置了参数和策略。这样就不再需要对处理过程的协议文本进行内部细节的讨论。

2　基于场景模型的测试集合生成

场景模型中 S, I, K 集合元素的值确定后,就可以构造出 RI-Pro 的一个应用场景 π。应用场景是指场景模型中的一个确定实例,是 RI-Pro 完成路由计算和决策过程所需要的输入数据和控制参数构成的假想应用环境,简称为场景。用于测试 RI-Pro 的案例就是特定的应用场景。如果场景 π 的元素符合协议规定所有制约关系 δ,则 π 为 RI-Pro 的正常场景,正常场景反映了 RI-Pro 正常的参数配置、策略定义和输入数据的处理路径。如果 π 的元素之间违反了参数之间的制约关系,出现了矛盾关系 δ',则 π 为 RI-Pro 的一个异常场景,异常场景反映 RI-Pro 在异常输入和错误配置情况的处理情况,本文以后所使用的制约关系 δ,将是指参数之间出现的矛盾制约关系。

最简单的健壮性测试集合生成方法是组合方法。组合 S, I, K 的独立元素就可以生成 RI-Pro 的应用场景集合 Π。Π 是包含了所有正常场景和异常场景的全集。但是该方法不仅有组合爆炸问题,并且在生成的场景集中很难找出具有代表性的测试场景,因此该全集 Π 主要用于理论分析。

2.1　测试集生成方法

场景模型的灵魂是关系集合 Δ。Δ 集合的每一个元素都是一种矛盾关系 δ,表示该场景中出现了导致 RI-Pro 异常或错误的关系。本文从以下几方面构建了关系集合 Δ:

1）协议规定

BGP 的 RI-Pro 的标准[2]中给出了许多制约关系,在协议一致性测试时,要测试协议实现是否遵循了这些制约关系。但是在健壮性测试中通过变异等方法违反这些制约关系,来测试协议实体是如何健壮地处理这些异常和错误。

如协议对 UPDATE 报文给出了详细的语法和语义规定。当违反这些规定时就产生了矛盾关系,如 UPDATE 语法错误 δ_s 就有 11 种,还有更深层次的语意错误,如路由黑洞 δ_h 和路由环路 δ_l 等。

2)研究成果

1996 年,Varadhan[5] 首先观察到 BGP 的路由振荡问题。G. Griffin[6] 用 SPVP 模型描述了 BGP 协议的振荡行为,并针对该模型引入图论知识给出了路由收敛的充分条件。路由振荡的矛盾关系就可以从这些研究成果中提取出来。

3)Internet 实例

目前有多个研究组织在监视 Internet 上 BGP 的运行,不断公布 BGP 的统计数据和事故实例。同时路由设备厂家在自身的 BGP 出现问题之后也在不断地进行改进,软件的每一次升级都要通告该次升级改善了哪些脆弱性环节。利用这些已有的大量原始数据,可以找出事故实例所蕴含的矛盾关系。如发生在 1997 年 4 月 25 日的著名 AS7007 事件[7] 和 2001 年 4 月 AS3561[8] 事件等。

4)扩展

每一个 δ 关系都有自身的输入数据,为了发现更多类似的矛盾关系,我们在一定范围内对已知的矛盾关系进行扩展。扩展已有矛盾关系的关键问题是找到扩展所使用的搜索空间,即矛盾关系在多大的空间中进行扩展。BGP 的矛盾关系扩展主要在配置信息搜索空间和路由搜索空间进行。

2.2 测试案例构造原则

场景模型中关系集合 Δ 表明了导致 RI-Pro 错误的原因。因此 Δ 不仅是场景模型的灵魂,也是测试目的的体现,更是构造场景的依据。健壮性测试案例的生成就是根据 Δ 集合中的关系元素重新构造应用场景。下面给出使用矛盾关系 δ 重新构造场景时要遵循的原则:

1)构造场景时一个场景中只有一个矛盾关系;

2)构造的场景必须尽量简单,要排除场景中其他无关因素的干扰;

3)尽量使用缺省配置,不要涉及与矛盾关系没有直接联系的参数、策略、更新报文和路由信息库;

4)构造的场景还要反映该矛盾关系的一般性特征,要使用具有代表性的测试环境和测试激励。

2.3 实现和实际测试结果

根据 5 年多 BGP 协议开发、测试和实际应用方面的积累,以及 Cisco,NANOG,Agilent 等研究机构提供的原始数据,我们获得了大量的 BGP 健壮性缺陷实例。利用这些原始数据、协议规范和 BGP 众多的研究成果,我们用本文提出的方法生成了 BGP 的 RI-Pro 的反向测试集。

IXIA 公司的 ANVL[9] 测试系统被 250 多家公司用于协议一致性和互操作性测试。依托该测试系统整体框架,为了方便向 SUT 注入错误,我们扩展了 BGP 的参考实现,并实现了反向测试集,形成 BGP 健壮性测试集合。

ANVL 也利用协议规范生成了一致性测试集合,表 1 列出了 ANVL 生成的 RI-Pro 正向测试集和基于场景模型生成的反向测试集的检错能力对比(Cisco 7200, ISO version 11.3)。

Wisconsin 大学的研究组最早对软件健壮性进行了研究。他们开发的测试工具——Fuzz[10] 可以对 Unix 和 Windows NT 进行健壮性测试。和 Fuzz 只使用了随机输入流测试相比,本文提出的方法可以生成更有效的测试案例。当被测对象出现失败时,Fuzz 不能指出失败的原因,而本文使用的方法是基于矛盾冲突关系,通过场景分析可以非常容易找到实现的健壮性缺陷所在。

Ballista[11] 是 Carnegie Mellon 大学用来分析商业软件健壮性缺陷的研究项目。和 Ballista 通过将协议消息头部字段作为参数进行分析,定义出一组有效和无效的测试值的方法相比,本文提出的方法可以产生更多不同类型的测试案例。

表 1 正向和反向测试的检错能力对比

Testsuit	No	Fails	Ratio(%)
Positive	57	6	10.5
Negative	96	23	23.9

3 结语

本文给出了适于描述 RI-Pro 的场景模型,提出了基于该模型的健壮性案例的生成方法,并讨论了该方法的关系集合以及搜索空间等问题。通过实际应用可以获得以下结论:该方法是一个系统的健壮性测试方法,它避免了盲目地查找矛盾关系所产生的组合爆炸问题,生成的测试案例针对性强,并可以从已有的矛盾发现新的矛盾;该方法是一种软件测试和通信协议测试相结合的测试方法,生成的测试集比单纯依靠规范生成的测试集扩大 1 倍,实际测试结果显示检错能力是正向测试的 2.3 倍。健壮性测试应用于核心路由器的 BGP 开发后,对实现中脆弱环节的查找、定位和修正起到了重要的作用,提高了实现实体的健壮性。

参考文献:

[1] RFC 1123, Requirements for Internet Hosts - Application and Support[S], 1989.

[2] RFC1771, A Border Gateway Protocol 4 (BGP-4)[S], 1995.

[3] WANG L, ZHU P, GONG Z. Study of Robustness Testing Based on RFSM[A]. Proceedings of INC2004[C]. Plymouth, UK, 2004. 234 - 242.

[4] ISO9646(1-7), Conformance testing methodology and framework [S], 1994.

[5] VARADAN K, GOVINDAN R, ESTRIN D. 96-31, Persistent route oscillations in inter-domain routing[R]. USC/ISI, 1996.

[6] GRIFFIN TG, SHEPHERD FB, WILFONG G. Policy Disputes in Path Vector Protocols[A]. Proceedings of the 7th International Conference on Network Protocols[C], 1999. 41 - 62.

[7] WO SA. Wow, AS7007 NANOG mail archives[EB/OL]. http://www.merit.edu/mail.archives/nanog/1997-04/msg00340.html, 2006 - 02.

[8] FARRAR J. C&W Routing Instability. NANOG mail archives[EB/OL]. http://www.merit.edu/mail.archives/nanog/2001-04/mes00209.html, 2006 - 03.

[9] http://www.ixiacom.com/products/caa/anvl_testsuitedesc.php l [EB/OL], 2006 - 03.

[10] FORRESTER JE, MILLER BP. An Empirical Study of the Robustness of Windows NT Applications Using Random Testing[EB/OL]. http://www.cs.wisc.edu/~bart/fuzz l, 2006 - 02.

[11] HELMY A. USC-CS-TR-99-716, Systematic Test Synthesis for Multipoint Protocol Design[D]. Computer Science Department, University of South California, 1999.