基于多协议扩展边界网关协议 BGP4 + 的形式化建模研究①

Research on Formal Modeling of Multiprotocol Extension Border Gateway Protocol BGP4 +

江 魁 黄云森 龚巧华 (深圳大学现代教育技术与信息中心 深圳 518060)

摘要:协议的形式化建模有助于提高其一致性测试集的自动化生成与完备程度,在分析 BGP4 + 协议的基础上,提出了适用于复杂路由协议形式化建模的混合模型建模法,并基于有限状态机与 SDL 两种形式描述技术完成了该协议的形式化建模。

关键词:BGP4 + 形式化建模 有限状态机 SDL

1 引言

多协议扩展边界网关协议 BGP4 + (Border Gateway Protocol)是下一代互联网中最重要的域间路由协议,其功能是在自治系统之间交换网络层可达信息[3]。目前大部分路由器和网络操作系统都已实现对 BGP4 + 的支持,但 BGP4 + 的各种协议实现可能会因为实现者对协议标准的不同理解出现差别和错误,这些问题对于下一代互联网的 IPv6 部署和商用来说都是极大的障碍。BGP4 + 协议的一致性测试正是消除这些障碍的重要环节,它通过对相关协议实现进行完备性和无错误性判定,从而确定检验协议实现是否与协议规范描述的内容一致。

本文对 BGP4 + 协议的形式化建模进行研究,在分析了 BGP4 + 协议的基础上,提出了适用于复杂路由协议形式化建模的混合模型描述法。随后在该方法的指引下,基于有限状态机 FSM(Finite State Machine)和规格说明及描述语言 SDL(Specification and Description Language)两种形式描述技术完成了对 BGP4 + 协议的形式化描述。

2 BGP4 + 协议

BGP4 + 是 BGP4(边界网关协议 4)的增强版本,是一种路径矢量路由协议,能够同时为 IPv6 和 IPv4 携带路由选择信息,与 BGP4 + 协议有关的 RFC 文本主要有 RFC 1771、RFC 2858 和 RFC 2545。BGP4 + 对等体之间通过 TCP 协议的 179 端口建立连接成为邻居,邻居之间携带的路径矢量信息称为路径属性,路径属性又可分为众所周知(Well – Known)的路径属性和可选(optional)的路径属性两大类,路径属性使 BGP 具有很好的灵活性和可扩充性。BGP4 + 扩展了 MP_REACH_NLRI(多协议可达 NLRI)和 MP_UNREACH_NLRI(多协议不可达 NLRI)两个属性,以实现发布支持 IPv6 协议的路由选择信息。BGP4 + 使用更新消息与 BGP4 + 邻居增量交换网络层可达信息,基于属性列表根据预先定义好的策略在到达某个特定网络的可行 AS 路径列表中确定最佳 AS 路径,根据本地策略信息库中所定义的各种策略对从 UPDATE 报文中获得的路由信息进行选择,选择的路由将被存储在本地准备发送给 BGP4 + 对等体的信息库中。

BGP4 + 协议中定义了 OPEN、KEEPALIVE、NOTIFICATION 和 UPDATE 等报文四种报文类型。OPEN 报文用于在 BGP4 + 对等体之间建立通信会话,KEEPALIVE 报文在 BGP4 + 对等体之间维持已建立的通信会话,BGP4 + 对等体双方需要周期性交换 KEEPALIVE 报文,以维持邻居关系;UPDATE 报文用来向 BGP4 + 对等体提供路由选择更新信息,NOTIFICATION 报文用来在发生错误

① 基金项目:深圳市科技计划项目资助,项目编号 200508

时中断 BGP4 + 对等体之间的连接。BGP4 + 协议存在 Idle、Connect、Active、Opensent、Openconfirm 和 Established 六种状态，以及与这六种状态相关的十三种事件，如表 1 和表 2 所示。

表 1　BGP4 + 协议 6 种状态

序号	状态	说明
1	Idle	最开始处于空闲状态
2	Connect	正在等待传输层协议连接的完成
3	Active	试图通过启动 TCP　连接获得一个对等体
4	Opensent	正等待它的对等体发来 OPEN 报文。已经向该对等体发送过 OPEN 报文
5	Openconfirm	在收到 OPEN 报文后，等待对等体发送 KEEPALIVE 或 NOTIFICATION 报文
6	Established	对等协商的最后阶段，该阶段开始与对等体交换 UPDATE 报文

表 2　BGP4 + 协议 13 种事件

序号	事件
1	启动
2	停止
3	传输连接建立
4	传输连接关闭
5	传输建立连接失败
6	传输连接出错
7	连接重试时间超时
8	等待时钟超时
9	KEEPALIVE 时钟超时
10	收到 OPEN 报文
11	收到 KEEPALIVE 报文
12	收到 UPDATE 报文
13	收到 NOTIFICATION 报文

3　混合模型描述法

在对协议的形式化建模过程中，常用的两种模型是状态转换模型与程序设计语言模型。状态转换模型主要包括有限状态机 FSM（Finite State Machine）、带标记的转换系统 LTS（Labeled Transition System）、Petri 网（Petri Net）三种，这类模型提供了形式化的语法，严谨的数学定义和相关的推导规则。在状态转换模型下，协议的实现被认为是由若干个事件驱动的实体组成，这些实体之间通过消息传递机制进行通信，每个实体的特性被描述为一系列响应内部和外部事件的状态转换。状态转换模型的优点是简单明了，易于验证协议的许多特性；缺点是描述复杂协议时由于状态急剧增多容易引起状态爆炸问题[4]。程序设计语言模型主要包括有扩展状态转换语言 Estelle（Extended State Transition Language）、暂时顺序定义语言 LOTOS（Language of Temporal Ordering Specification）与规格说明及描述语言 SDL（Specification and Description Language）等，这类模型有形式化的语法和严谨的数学定义，但没有推理和推导规则。在程序设计语言模型下，协议的实现被认为是一种算法过程，通过该算法过程协议系统的特性能够被无歧义地理解。

在对传统通信协议进行形式化建模时，采用单一的模型即可完成协议的形式化描述。但在对 BGP4 + 这类复杂的路由协议进行形式化建模时，如果不采取一定的策略，会使形式化建模的完成异常困难。因此，我们提出了一种适用于 BGP4 + 这类复杂路由协议的形式化建模方法——混合模型描述法。该方法的实现思想是先根据协议的一致性测试目的及其工作原理将其分成几个独立部分，然后再分别为各部分采用合适的建模方法建立相应的形式模型。例如，对于 BGP4 + 协议，可以根据一致性测试目的将其分成协议状态测试、路由与属性处理测试、错误处理测试三个独立部分。在这三个部分中，协议状态测试部分由于状态数目有限，输入输出事件不多，适合选用基于有限状态机的形式建模方法，确保能够用较少的状态描述协议中适合状态描述的部分；而路由与属性处理测试、错误处理测试两个部分由于描述状态多、状态转换数多、输入输出事件多、处理过程也比较复杂，直接采用状态转换模型描述存在困难，并容易引起状态爆炸问题，因此适合选用基于程序设计语言的建模方法。由此可见，混合模型建模法的特点在于能同时结合状态转换模型和程序语言模型两者的优点，特别适用于类似 BGP4 + 此类复杂协议的形式化描述。在此策略的指引下，我们基于有限状态机与 SDL 两种形式描述技术完成了 BGP4 + 协议的形式化建模。

4　BGP4 +协议的形式化建模

4.1　有限状态机建模

有限状态自动机(Finite State Machine,FSM)具有

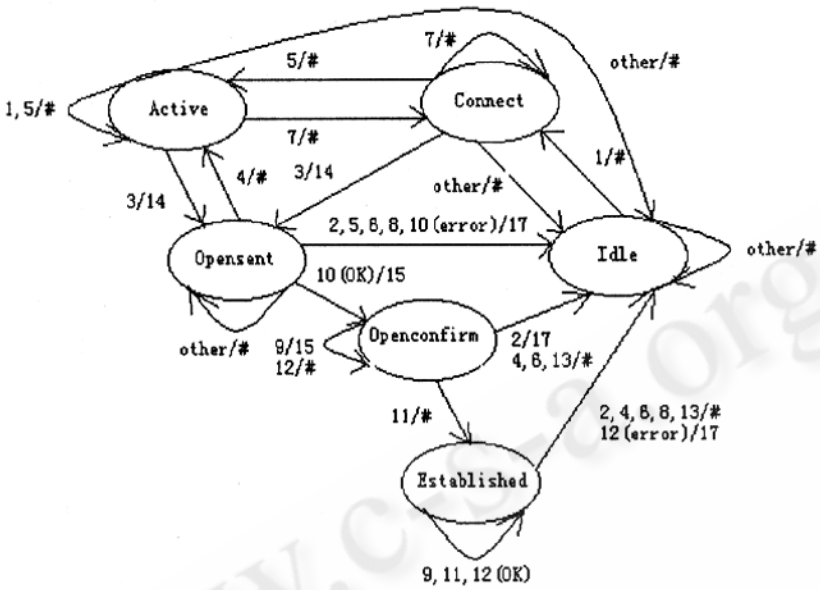

图 1　BGP4 +状态转换部分的有限状态机图

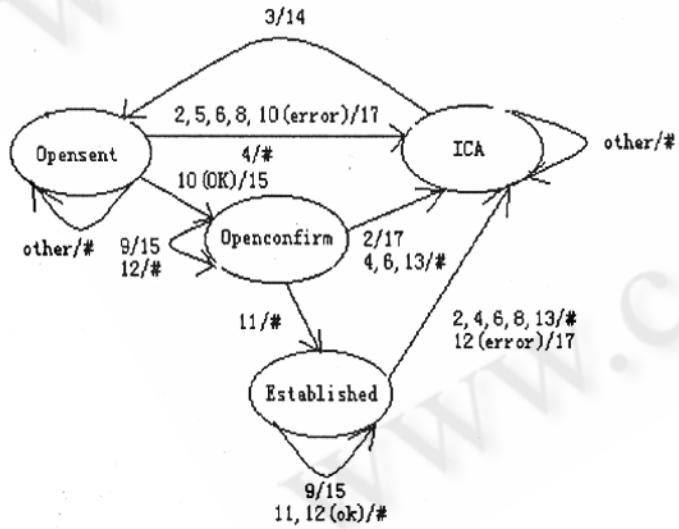

图 2　化简后 BGP4 +状态转换部分的有限状态机图

有限个状态和一个初始状态,输入信号为字母表,自动机收到一个字母将引起状态转移,可以定义为一个五元系统 <S,A,O,M,N>,其中:

S:系统状态集,其中状态数有限;

A:有限输入集;

O:有限输出集;

M:状态转移函数集,是从 S X A 到 S 的映射

N:输出函数集,是从 S x A 到 O 的映射。

有限状态机能够用状态转移图、状态转移矩阵和状态转移表等多种方法表示,其中最常用的是状态转移图[3]。状态转移图中节点表示有限状态机的有限状态,两个状态间用带标记的有向边连接,每条有向边对应一个状态转移。圆圈表示状态,状态名位于圆圈内,与弧线关联的字母为输入/输出对,无箭头端与当前状态相连,箭头端与下一状态相连。(Si,Sj,Ak/Om)表示从 Si 到 Sj 的一条具有输入/输出对 Ak/Om 的边,表明当前有限状态机在状态 Si 时,接收到输入 Ak,产生输出 Om,然后转移到状态 Sj,无起点箭头指向初始状态。

前面介绍过,BGP4 +协议中共有 6 个状态和 13 个事件,为便于按照有限状态机的定义重新进行描述,我们在 BGP4 +协议的基础上添加了 4 个事件,如表 3 所示,在表 1 与表 3 的基础上得到 BGP4 +协议状态部分的有限状态机形式模型,如图 1 所示。

表 3　新添加的四种事件

序号	事件
14	发送 OPEN 报文
15	发送 KEEPALIVE 报文
16	发送 UPDATE 报文
17	发送 NOTIFICATION 报文

图 1 中的 Idle、Conncet 和 Active 均为不可测状态,可以将它们进一步合并,得到简化后 BGP4 +协议状态转换部分的有限状态机模型,如图 2 所示。

4.2　SDL 语言建模

在程序设计语言模型中,Estelle 和 LOTOS 主要适用于 OSI 参考模型中服务和协议的描述,SDL 语言是一个面向对象的形式化语言,专门用于描述面向对象、复杂的事件驱动与实时的通信事件,特别是针对含有并行通讯和行为的实时、分布式系统[6]。该语言适用于

复杂、事件驱动、实时、并行多任务、交互式的系统描

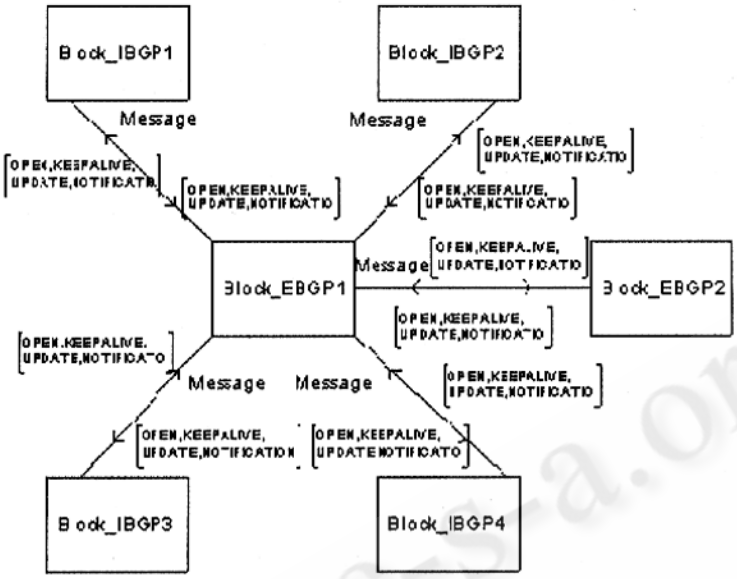

图 3　BGP4 + 协议的 SDL 系统图

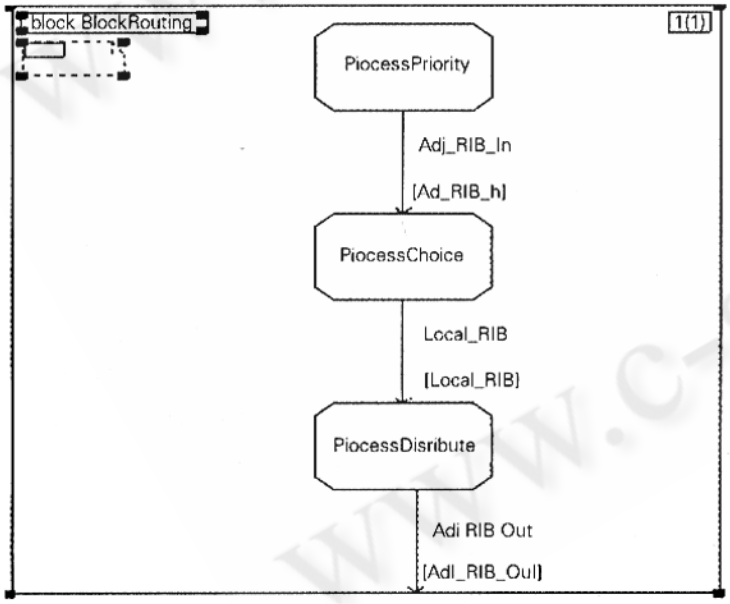

图 4　BGP4 + 路由信息处理功能块图

述，仅可以用来对系统的功能进行说明，也可以描述系统的内部结构和行为。对于 BGP4 + 这类复杂的路由协议而言，各功能部件之间的通信关系和定时器功能是两个主要的概念，而这两个概念能够用 SDL 语言来确切表达。因此我们选用 SDL 语言作为 BGP4 + 协议路由与属性处理和错误处理两个部分的建模方法。

SDL 通过层次结构来对系统进行描述和说明，一个 SDL 说明是一个由许多通过信道互连的功能块(Block)组成的系统(System)，功能块可以包含子功能块，也可以包含了一个或多个并发进程(Process)。进程是系统中的最小处理单元，描述了功能块的行为，相当于一个扩展有限状态机 EFSM(Extended Finite State Machine)，所有处理和操作都在进程中完成。文本描述中定义了在信道上发送的信号，在路由协议中可以是各种报文消息。SDL 有两个有力的补充手段，一个是 ITU 定义和描述系统使用的数据类型和数据值的标准化语言抽象语法符号 ASN.1(Abstract Syntax Notation – one, ASN.1)，通过该语言中定义的编码规则能够描述 BGP4 + 协议中各种数据和协议消息；另一个也是 ITU 定义的消息序列图 MSC(Message Sequence Charts)，MSC 是一种图形化、标准化的形式化描述技术，用来描述系统各组成成分间及其与环境之间的通信。

SDL 能够用 SDL/PR 文字表示法和 SDL/GR 图形表示法两种等价方法描述一个系统，图形文法直观易懂，便于交流，适合于设计开发人员使用，而文本文法更适合于机器理解，因此，实际应用基本采用 SDL/GR。下面以 BGP4 + 协议的路由处理过程为例，说明运用 SDL 对路由协议描述的一个大体框架。图 3 是 SDL/GR 形式描述的 BGP4 + 协议路由处理部分的系统图，系统的功能图相对独立，彼此之间通过信道相互连接，利用信道上传递的信号进行通信，所有信道、信号、预定义数据类型都在系统图中定义。从该图中可以看出，BGP4 + 对等体系统由不同种类的路由器组成，不同的路由器之间以特定的 BGP4 + 协议报文进行通信。由于 BGP4 + 协议的路由处理过程可以分为连接建立、网络拓扑维护、路由信息处理三个过程，因此系统图中的描述内部路由器的功能块 Block_IBGP1 又被进一步划分为计算路由优先级(ProcessPriority)、路由选择(ProcessChoice)与路由分发(ProcessDistribute)三个进程，如图 4 所示。

5　结束语

随着支持 IPv6 路由协议产品的日渐增多，对各种

IPv6 路由协议实现进行一致性测试成为下一代互联网络建设发展的必然要求,形式化建模是一致性测试中最为重要的环节。本文在对 BGP4 + 协议分析的基础上,提出了适用于复杂路由协议形式化建模型的混合模型描述法,并基于该方法,分别使用有限状态机与 SDL 语言完成了 BGP4 + 协议不同部分的形式化建模。BGP4 + 协议中的状态转换部分采用有限状态机进行形式化建模,路由与属性处理、差错信息处理部分采用 SDL 语言进行形式化建模。运用该方法对 BGP4 + 协议进行形式化建模,能够充分结合各种形式化建模方法与被测协议实现的特点,在保证精确描述的同时有效缩小形式化过程中的状态空间,解决了复杂协议描述过程中可能出现的状态爆炸问题,确保了 BGP4 + 协议形式化建模的完备与可靠。下一步将从已建立的协议形式化模型出发,研究一致性测试集的自动生成技术,以提高测试集生成的自动化程度与质量。

参考文献

1 ISO/IEC 9646 – 1. Information technology – open systems interconnection conformance testing methodology and framework Part1 [Z]. General concepts, 1994.

2 古天龙、蔡国永, 网络协议的形式化分析与设计, 北京:电子工业出版社, 2003.

3 T. Bates, Y. Rekhter. IETF RFC 2858. Multiprotocol Extensions for BGP – 4. 2000.6.

4 张冠华、张连华, 一种路由器形式化测试模型的研究, 系统仿真学报,2005.17(1。):154.

5 D. Lee , K. Sabnani , D. Kristol , S. Paul . Conformance testing of protocols specified as finite state machines [J] IEEE Transactions on Communications , 1996,44.

6 ITU – T Recommendation Z. 100, Specification and Description Language(SDL),1999.11.