基于路由交换范式构建安全可信网络

徐 恪[1] 沈 蒙[2] 陈文龙[3] 等
[1]清华大学
[2]北京理工大学
[3]首都师范大学

关键词：路由交换范式 网络安全

引言

尽管现在有关“棱镜门”的报道已经渐渐平息，但是人们对信息安全的担忧依然无减。互联网已经成为人们交互信息的重要媒介，一旦网络路由交换设备遭到入侵，攻击者就能轻易获取成千上万、甚至数十万台计算机的通信情况。美国国家安全局就曾入侵清华大学主干网。因此，如何保证网络路由交换设备的安全是至关重要的问题。

目前，我国的骨干网（中国电信163、中国联通169）中，国外设备占据了很大比重。思科占据着中国电信163骨干网70%以上的份额，在中国联通169骨干网的份额达到了80%以上。虽然思科已发表声明撇清与棱镜项目的干系，但是我国网络被他国直接破坏的可能性依然存在。目前，各大运营商都在酝酿“去思科化”，比如，中国电信在2013年集中采购核心路由器时就没有选思科的产品。

然而，全部使用国产设备就能保证我国的网络安全吗？这种想法显然过于乐观。随着路由交换技术的不断演进，路由交换设备软硬件开放程度逐步提高，可编程能力不断增强。可编程设备在给功能更新带来方便的同时，也给网络攻击者带来更多的可乘之机。因此，即便完全使用国产设备，网络安全形势依然严峻。

针对网络安全问题，研究者提出了很多解决方案。可信计算的概念最早于1999年由可信计算平台联盟(Trusted Computing Platform Alliance, TCPA)（可信计算组织的前身）提出。其主要思路是通过增强现有的PC终端体系结构的安全性来保证整个系统的安全。网络故障检测和行为验证一直是学术界关注的热点问题。已有的研究主要是针对特定协议提出检测协议配置和运行正确性的方法或者工具。伴随着软件定义网络(Software Defined Network, SDN)的兴起，研究者开始关注OpenFlow的验证问题[1~6]，如验证OpenFlow配置策略的有效性及网络可达性[4,5]、数据平面的正确性[6]等。然而，针对设备层面路由交换异常行为的检测和验证的研究成果还比较少。

路由交换安全问题归纳

网络安全主要指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改和泄露，系统能够连续可靠地正常运行。路由交换设备是网络数据处理与传输的枢纽，也是网络系统的重要组成部分，因此保证路由交换设备的安全对于构建安全可信网络至关重要。

路由交换设备面临众多安全

问题，比如非法访问、拒绝服务攻击、数据泄露等等，其中既有人为因素，也有非人为因素。本文关注的是路由交换系统及其功能模块由于设计缺陷或遭受攻击而导致的数据处理异常问题。

路由交换设备内部通常分为控制平面和数据平面[7]（如图1所示）。控制平面运行不同类型的路由协议，并动态生成路由表。数据平面包括输入接口、交换结构和输出接口。在正常的数据处理过程中，报文经由输入接口进入数据平面后，转发引擎分析其网络协议(Internet Protocol, IP)报头信息，使用转发表查找对应的输出接口，并通过交换网络把报文转发到输出线路上。转发表是根据路由表生成的，其表项和路由表项有直接对应关系，但转发表的格式和路由表的格式不同，更适合实现基于硬件的快速查找。下文统一把控制平面和数据平面的功能模块称为构件。构件化的开发方法实际上已经被各大路由交换设备厂商广泛采用。

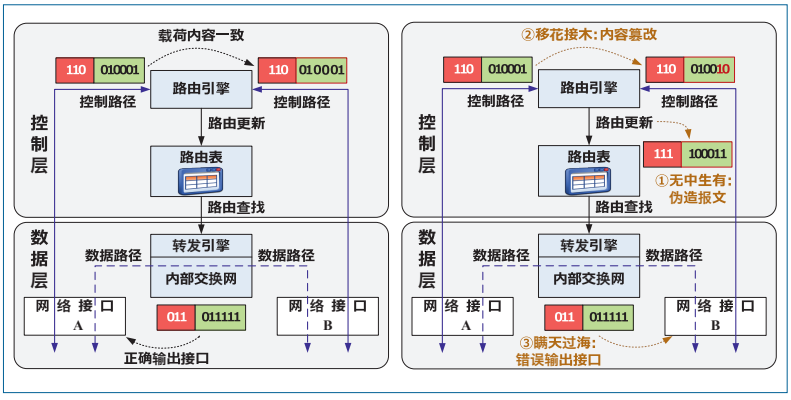

图1 数据处理过程（左）与异常行为（右）示意图

路由交换设备的数据处理异常行为可以归纳为以下几类。

无中生有 指路由交换设备数据转发平面所发送的报文，既不是来自上游路由交换设备，也不是由控制平面产生的。例如，控制平面的恶意构件将与该路由转发相关的敏感信息（如路由转发表项等），通过数据平面将报文发送至特定目的地，从而造成敏感信息泄露。

移花接木 指路由交换设备对报文的内容进行篡改或替换。例如，运行OSPF（Open Shortest Path First，开放式最短路径优先）协议构件的路由器在转发邻居路由器的链路状态广播(Link State Advertisement, LSA)报文时，将其中的相关信息（如网络前缀）进行篡改，从而导致区域内路由器的拓扑混乱，破坏了网络的正常路由。

瞒天过海 指路由交换设备看似正常的数据转发行为违背了相应的规则。例如，交换机可以通过配置转发规则，将符合规则的报文通过对应接口转发至下一跳设备（或者予以过滤），而恶意行为则可能将报文转发至错误的下一跳设备（或者将本应过滤的数据报文进行转发）。再如，恶意行为可以利用看似正常的边界网关协议(Border Gateway Protocol, BGP)报文将非法信息或机密信息传递出去。

路由交换范式

为了保证数据处理的安全可信，我们提出如下建议：**路由交换设备的任何一种数据处理行为都必须事先定义和声明，并且可以验证其实际行为是否与之前的定义一致。**为此，我们引入了路由交换范式的概念。**路由交换范式是指路由交换设备中可验证的规则构成的集合。**

范式可以由网络运营者（即网络设备的管理者）根据业务需求灵活定义（如图2所示）。按照数据处理的层次划分，将路由交换范式分为转发过滤范式和管理控制范式两大类。每一

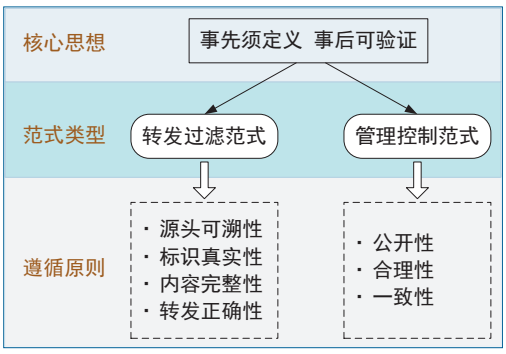

图2 路由交换范式分类及原则

类范式分别遵循若干原则。

转发过滤范式

该范式与路由交换设备的报文转发、过滤行为相对应。为了表述方便，我们将进入路由交换设备的报文集合称为“输入报文集”，离开路由交换设备的报文集合称为“输出报文集”。对于转发过滤范式而言，输出报文集应为输入报文集的子集。其所要遵循的原则包括如下几点。

1. 源头可溯性：对于任意一个输出报文，可以追查其进入路由交换设备的输入接口号；

2. 标识真实性：对于任意一个输出报文，可以验证其报头中的源地址和目的地址未被篡改；

3. 内容完整性：对于任意一个输出报文，可以验证其载荷内容未被篡改；

4. 转发正确性：对于任意一个输入报文，可以验证对其操作的正确性。比如，被转发报文的输出接口是否正确，被过滤（或丢弃）的报文是否符合过滤（或丢弃）规则。

管理控制范式

该范式与路由交换设备的管理控制行为相对应，涉及两类报文：一是管理员对路由交换设备进行配置管理时所产生的管理报文，二是路由交换设备运行网络协议所产生的控制报文。所要遵循的原则包括如下几点。

1. 公开性：任意一个管理控制报文的信息和处理方式须由管理控制行为事先声明；

2. 合理性：任意一个管理控制行为的声明须服从网络管理控制的基本原则；

3. 一致性：任意一个控制报文的信息和处理方式须与声明的内容一致。

上述范式的分类，既能与传统路由交换平台中数据平面和控制平面相对应，又能顺应未来路由交换设备的发展趋势。例如，以 OpenFlow 为代表的软件定义网络，主张控制平面与数据平面分离，由集中式控制器将路由转发规则配置到数据平面中，再由管理控制范式规范控制器的行为，而转发过滤范式用于规范数据平面的行为。再如，未来可编程路由交换设备中[8]，控制平面可以支持第三方开发的功能构件。功能构件的行为需要满足管理控制范式的要求，即须事先声明构件功能、验证声明的合理性、验证功能描述与实际行为的一致性。

我们以防火墙为例介绍路由交换范式的具体体现方式（如图 3 所示）。防火墙位于内部网（如企业园区网、校园网等）与外部网（如互联网）之间，通过数据报文过滤技术，保护内部网免受外部非法用户的入侵，同时防止内部网中未经授权的数据通信流向外部网。因此，防火墙本质上也是一种路由交换设备：符合通行条件的数据报文被转发至相应的输出接口，而不符合通行条件的数据报文则被过滤丢弃。

通常，管理员使用防火墙软件或者功能构件（统称为防火墙软件）提供的管理界面配置过滤规则，这其中涉及管理控制范式。按照管理控制范式的要求，防火墙软件应声明自身具有报文过滤功能，并公布对应的过滤规则。其次，路由交换设备需要对声明的过滤规则进行合理性验证，比如，对以某前缀为目的地址的报文是否违背内部网管理要求进行验证。第三，路由交换平台需要验证防火墙软件生成的路由转发表项是否与所声明的过滤规则一致。

此外，在过滤规则的执行过

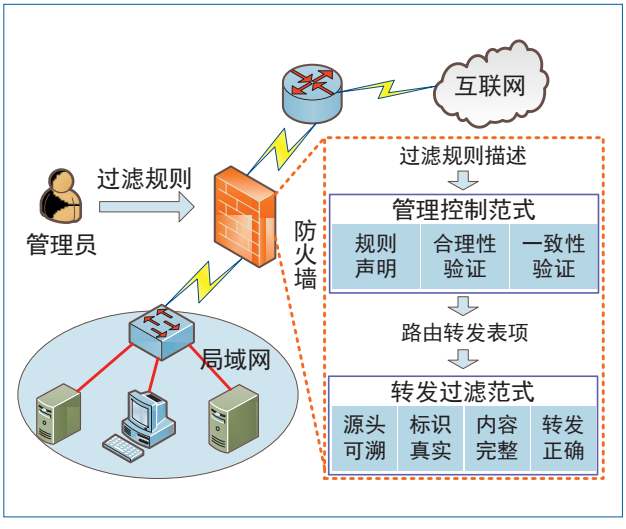

图3　路由转发范式在防火墙中的应用方式

程中还会涉及另一类范式——转发过滤范式。对于数据报文，除了进行源头可溯性、标识真实性、内容完整性验证之外，需要特别关注转发的正确性：符合过滤规则的报文是否被过滤掉，不符合过滤规则的报文是否被转发至正确的输出接口。

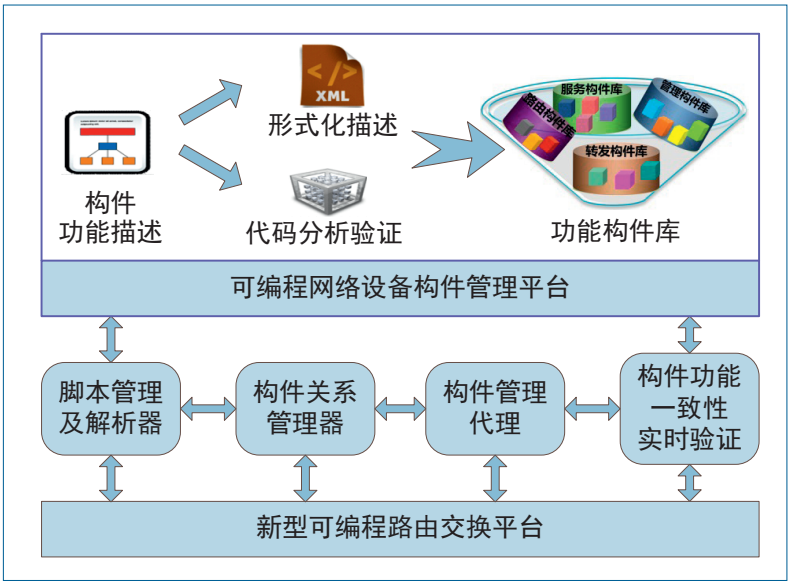

图4　路由交换范式在可编程网络设备中的应用示意

与传统路由交换设备相比，支持功能构件动态加载的新型可编程路由交换设备已经成为路由交换技术发展和演进的主要趋势[8]。网络设备使用者可以购买或者定制满足其需求的功能构件（如防火墙构件、内容分发网络(Content Delivery Network, CDN)构件、流量监测构件等），将其加载到可编程设备中，从而形成类似于现有智能手机应用市场的商业模式。

可编程网络设备的开放性也使得其面临的安全问题更加严重。在这种情况下，路由交换范式可以更好地发挥作用，并规范功能构件的行为。可编程网络设备管理平台按照管理控制范式的要求，对不同类型构件的功能描述进行验证（比如代码分析），将符合功能描述的构件加入功能构件库；构件动态加载过程中，管理控制范式用于规范构件间的组装、连接关系，比如，流量监测构件禁止调用路由更新构件；待构件加载成功后，可编程路由交换平台在运行时，按照转发过滤范式的要求，利用构件关系管理器、构件管理代理等模块对构件功能的一致性进行实时验证。此过程如图4所示。

路由交换范式的验证方式

对于国外厂商生产的路由交换设备，路由交换范式也可以用于保证设备数据处理行为的安全可靠，而无须知道其内部实现细节。其难点在于如何在路由交换设备中验证已定义的范式是否被正确执行。

代码分析　代码分析是确保范式有效性的最直接的办法。给定一段程序代码，根据其语义，构造出一棵代码执行树。其中，节点表示程序所处的执行状态（如判断语句的输入、输出），边则表示连接两个执行状态的语句块（如判断语句的判定条件）。对于任意一个输入参数，其代码执行过程对应于代码执行树中一条从根节点到叶子节点的路径。因此，如果要验证该段代码的有效性，我们需要执行所有的路径，并逐一检验每条路径是否违背程序目标。然而，实际上，这一方法会因状态爆炸问题而变得不可行，即路径数目随着程序分支数呈指数级增长，路径数目过大使得验证过程异常耗时。目前已有很多研究关注状态爆炸问题，并提出了可行的解决方案。比如，文献[6]提出了一种分而治之的验证策略，首先将执行树分解为多个独立的子树，对每个子树进行单独验证，降低状态规模；然后，将多个子树串联验证，以避免路径数目呈指数级增长，从而大大缩短验证时间（从原有的数小时缩短为十几分钟）。

功能模拟　代码分析并非总是可行的。例如，对于第三方开发的功能构件，其源代码由开

发者掌握，对外仅公开构件的功能结构和数据处理流程。针对这种情形，可以使用功能模拟的办法，按照构件的功能描述模拟其内部实现，然后将功能模拟的结果与构件的实际运行结果对照，从而判定构件是否实现了其声明的功能。例如，对于实现过滤功能的构件，假如将过滤规则视为一个变量，按照其功能描述信息执行后得到的逻辑结果称为期望值，而功能模拟后得到的实际结果为观测值。若期望值与观测值一致，则可保证期望的过滤规则被正确执行；否则，意味着存在安全隐患。

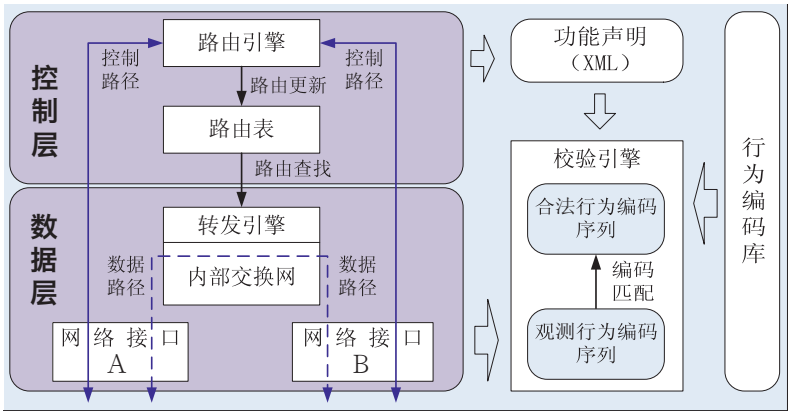

图5　基于动作编码的验证方案

动作编码匹配　前两种方法从构件的层面解决了可查验问题，接下来的难点在于如何从设备层面实现可查验？为此，我们提出了基于动作编码的验证方式（如图5所示）。路由交换平台针对报文进行的单一操作称为动作，比如更新路由表、丢弃报文、更改报头信息、更改报文载荷等。功能模块是由一组动作有序组合而成。例如，数据转发功能对应于“接收报文、查询转发表、更改报头信息、转发报文”这一组动作。若按照动作在路由交换平台中的使用频率进行霍夫曼编码，则每一个动作都对应一个霍夫曼编码。对于新添加的动作，可以直接对霍夫曼编码进行简单扩展。因为新添加的动作的使用频率非常低，所以使用较长的编码对原有的霍夫曼整体编码效率影响不大。

管理控制层面的每一项功能均需要事先声明，例如通过可扩展标记语言 (Extensible Markup Language, XML) 进行功能描述。根据所声明的功能，校验引擎可以生成一组符合管理控制范式定义的动作序列，进而可以得到一组“期望”的动作编码序列作为验证的标准。与此同时，校验引擎观测路由转发平台对报文的每一步操作，记录对应的动作编码，并与期望的合法动作编码序列进行实时匹配。符合功能描述的动作编码会匹配成功；不符合功能描述的动作编码会匹配失败，并触发警告消息。

面临的挑战

现有研究针对网络协议配置和运行正确性等问题提出了一系列验证技术和方法，取得了不错的效果。但是，针对单一网络设备数据处理行为的检查和验证，还须深入研究。基于路由交换范式来确保网络设备行为的安全可靠，是一种有益的尝试，但也面临着诸多挑战，主要有两方面。

效率提升　数据处理与转发是路由交换设备的核心功能。当设备满负荷运行时，所有接口应该能够以线速处理数据报文，交换矩阵能够实现无阻塞数据交换。目前，高速核心路由器的数据交换容量可达数百太字节 (TeraByte[1])。由于路由交换范式的验证需要对输入报文和输出报文进行额外操作，导致设备的数据处理能力受到影响，比如降低端口的吞吐量，增加数据报文处理平均时延等。因此，路由交换范式验证面临的首要挑战是验证效率问题，即如何在保证报文处理实时性的同时降低验证代价。

为了提升范式验证效率，减

[1] 1TB=10^{12}B。

少对设备数据处理能力的影响，可以对进出路由交换设备的数据“流”进行采样，仅针对采样数据进行检测。流的粒度和采样频率可以根据数据流量的规模、速率、相关性等信息进行灵活定义。在数据流量较小的场景中，可以按照传统的五元组（源IP地址、目的IP地址、协议号、源端口、目的端口）定义数据流，并采用较高的采样频率；而在数据流量较大的场景中，可以对传统数据流进一步汇聚，比如按照三元组（源IP地址、目的IP地址、协议号）定义数据流，并使用较低的采样频率。

策略优化 由于前面提到的几种验证方式在可行性、验证效率、实现开销等方面存在差异，因此对路由交换范式的检测往往需要多种方式组合使用，由此带来了路由交换范式的验证问题。该问题可以抽象成一种策略优化问题，即在给定实现代价前提下路由交换范式最大化的验证效率问题（Max问题），或在保证一定验证效率前提下路由交换范式最小化的验证开销问题（Min问题）。因此，路由交换范式验证面临的第二个挑战是，如何抽象和量化不同验证方式的属性特征，并且根据具体验证需求给出最优策略。

结语

开放式可编程的技术路线为路由交换设备的不断演进指明了方向，也带来了更多的安全挑战。本文从路由交换设备行为的角度，提出了路由交换范式，以便检测和发现安全问题。路由交换范式具有层次化结构，可以根据具体的应用需求和场景进行扩展；同时，在实现过程中，该范式不可避免地会影响路由交换设备的处理性能。如何在保证路由交换行为安全可控的前提下，将实现开销降低到可接受范围是未来值得深入探讨和研究的问题。■

徐 恪

CCF杰出会员。2011 CCF青年科学奖获得者。清华大学教授。主要研究方向为计算机网络体系结构、高性能路由器。xuke@tsinghua.edu.cn

沈 蒙

CCF会员。北京理工大学讲师。主要研究方向为网络体系结构、网络虚拟化技术。shenmeng@bit.edu.cn

陈文龙

CCF会员。首都师范大学讲师。主要研究方向为计算机网络体系结构、IPv4/IPv6互联网、物联网。wenlongchen@sina.com

其他作者：徐 磊

参考文献

[1] M. Canini, D. Venzano, P. Peresini, and et al.. A NICE way to test openflow applications. In *Proceedings of NSDI'12*, 2012.

2015院士候选人推选工作启动

根据中国科学院、中国工程院和中国科协关于推荐（提名）院士候选人工作相关规定，2015年度CCF推选院士候选人工作日前启动。

根据中国科协“推荐（提名）院士候选人工作实施办法（试行）”的要求，本学会将组成由陈左宁副理事长牵头并由均为两院院士的CCF会士组成的推选专家委员会负责本学会院士候选人的推选工作。

2015年院士推选强调同行评议和学术导向，根据中国科协要求，本学会推选院士候选人须通过学会分支机构（专业委员会和分部）进行，即被推荐人需要有不少于三位本领域具有正高级职称的同行（须是CCF杰出会员及以上级别）评价、推荐，并通过CCF的分支机构向CCF推选院士候选人工作小组推荐，由专家委员会最终评选后上报。具体要求详见学会网站上的通知，或向学会秘书处(ccf@ccf.org.cn)咨询。

[2] P. Kazemian, G. Varghese, and N. McKeown. Headerspace analysis: static checking for networks. In *Proceedings of NSDI'12*, 2012.

[3] H. Zeng, P. Kazemian, G. Varghese, and N. McKeown. Automatic Test Packet Generation. In *Proceedings of CoNEXT 2012*, Nice, France, December 2012.

[4] A. Khurshid, X. Zou,W. Zhou, and et al.. Veriflow: verifying network-wide invariants in real time. In *Proceedings of NSDI'13*, 2013.

[5] P. Kazemian, M. Chang, H. Zeng, and et al.. Real Time Network Policy Checking using Header Space Analysis. In *Proceedings of NSDI'13*, 2013.

[6] M. Dobrescu and K. Argyraki. Software Dataplane Verification. In *Proceedings of NSDI'14*, 2014.

[7] 徐恪，徐明伟，陈文龙，马东超. 高级计算机网络[M]. 北京：清华大学出版社，2012.

[8] K. Xu, W. Chen, C. Lin, and et al.. Towards A Practical Reconfigurable Router- A Software Component Development Approach, IEEE Network, 2014, 28(5), 74~80.