基于 IPv6 的源地址验证在接入网及自治域间研究

(申请清华大学工学硕士学位论文)

培 养 单 位 ： 网络科学与网络空间研究院

学　　科 ： 网络空间安全

研 究 生 ： 况　鹏

指 导 教 师 ： 刘　莹　研究员

二〇二一年一月

Research on source address verification based on IPv6 between access network and autonomous domain

Thesis Submitted to

Tsinghua University

in partial fulfillment of the requirement

for the degree of

Master of Science

in

Cyberspace Security

by

Kuang Peng

Thesis Supervisor: Professor Liu Ying

January, 2021

学位论文指导小组、公开评阅人和答辩委员会名单

指导小组名单

李 XX	教授	清华大学
王 XX	副教授	清华大学
张 XX	助理教授	清华大学

公开评阅人名单

刘 XX	教授	清华大学
陈 XX	副教授	XXXX 大学
杨 XX	研究员	中国 XXXX 科学院 XXXXXXX 研究所

答辩委员会名单

主席	赵 XX	教授	清华大学
委员	刘 XX	教授	清华大学
	杨 XX	研究员	中国 XXXX 科学院 XXXXXXX 研究所
	黄 XX	教授	XXXX 大学
	周 XX	副教授	XXXX 大学
秘书	吴 XX	助理研究员	清华大学

关于学位论文使用授权的说明

本人完全了解清华大学有关保留、使用学位论文的规定，即：

清华大学拥有在著作权法规定范围内学位论文的使用权，其中包括：（1）已获学位的研究生必须按学校规定提交学位论文，学校可以采用影印、缩印或其他复制手段保存研究生上交的学位论文；（2）为教学和科研目的，学校可以将公开的学位论文作为资料在图书馆、资料室等场所供校内师生阅读，或在校园网上供校内师生浏览部分内容；（3）按照上级教育主管部门督导、抽查等要求，报送相应的学位论文。

本人保证遵守上述规定。

（保密的论文在解密后遵守此规定）

作者签名：_____　　导师签名：_____

日　　期：_____　　日　　期：_____

摘　要

论文的摘要是对论文研究内容和成果的高度概括。摘要应对论文所研究的问题及其研究目的进行描述, 对研究方法和过程进行简单介绍, 对研究成果和所得结论进行概括。摘要应具有独立性和自明性，其内容应包含与论文全文同等量的主要信息。使读者即使不阅读全文，通过摘要就能了解论文的总体内容和主要成果。

论文摘要的书写应力求精确、简明。切忌写成对论文书写内容进行提要的形式，尤其要避免“第 1 章……；第 2 章……；……”这种或类似的陈述方式。

关键词是为了文献标引工作、用以表示全文主要内容信息的单词或术语。关键词不超过 5 个，每个关键词中间用分号分隔。

关键词：关键词 1；关键词 2；关键词 3；关键词 4；关键词 5

Abstract

An abstract of a dissertation is a summary and extraction of research work and contributions. Included in an abstract should be description of research topic and research objective, brief introduction to methodology and research process, and summarization of conclusion and contributions of the research. An abstract should be characterized by independence and clarity and carry identical information with the dissertation. It should be such that the general idea and major contributions of the dissertation are conveyed without reading the dissertation.

An abstract should be concise and to the point. It is a misunderstanding to make an abstract an outline of the dissertation and words “the first chapter”, “the second chapter” and the like should be avoided in the abstract.

Keywords are terms used in a dissertation for indexing, reflecting core information of the dissertation. An abstract may contain a maximum of 5 keywords, with semi-colons used in between to separate one another.

Keywords: keyword 1; keyword 2; keyword 3; keyword 4; keyword 5

目 录

插图和附表清单

符号和缩略语说明

PI	聚酰亚胺
MPI	聚酰亚胺模型化合物，N-苯基邻苯酰亚胺
PBI	聚苯并咪唑
MPBI	聚苯并咪唑模型化合物，N-苯基苯并咪唑
PY	聚吡咙
PMDA-BDA	均苯四酸二酐与联苯四胺合成的聚吡咙薄膜
MPY	聚吡咙模型化合物
As-PPT	聚苯基不对称三嗪
MAsPPT	聚苯基不对称三嗪单模型化合物，3,5,6-三苯基-1,2,4-三嗪
DMAsPPT	聚苯基不对称三嗪双模型化合物（水解实验模型化合物）
S-PPT	聚苯基对称三嗪
MSPPT	聚苯基对称三嗪模型化合物，2,4,6-三苯基-1,3,5-三嗪
PPQ	聚苯基喹噁啉
MPPQ	聚苯基喹噁啉模型化合物，3,4-二苯基苯并二嗪
HMPI	聚酰亚胺模型化合物的质子化产物
HMPY	聚吡咙模型化合物的质子化产物
HMPBI	聚苯并咪唑模型化合物的质子化产物
HMAsPPT	聚苯基不对称三嗪模型化合物的质子化产物
HMSPPT	聚苯基对称三嗪模型化合物的质子化产物
HMPPQ	聚苯基喹噁啉模型化合物的质子化产物
PDT	热分解温度
HPLC	高效液相色谱 (High Performance Liquid Chromatography)
HPCE	高效毛细管电泳色谱 (High Performance Capillary lectrophoresis)
LC-MS	液相色谱-质谱联用 (Liquid chromatography-Mass Spectrum)
TIC	总离子浓度 (Total Ion Content)
ab initio	基于第一原理的量子化学计算方法，常称从头算法
DFT	密度泛函理论 (Density Functional Theory)
E_a	化学反应的活化能 (Activation Energy)
ZPE	零点振动能 (Zero Vibration Energy)
PES	势能面 (Potential Energy Surface)
TS	过渡态 (Transition State)

TST	过渡态理论 (Transition State Theory)
$\Delta G^{\neq}$	活化自由能 (Activation Free Energy)
κ	传输系数 (Transmission Coefficient)
IRC	内禀反应坐标 (Intrinsic Reaction Coordinates)
ν_i	虚频 (Imaginary Frequency)
ONIOM	分层算法 (Our own N-layered Integrated molecular Orbital and molecular Mechanics)
SCF	自洽场 (Self-Consistent Field)
SCRF	自洽反应场 (Self-Consistent Reaction Field)

第 1 章　绪论

1.1　研究背景与意义

IP 源地址伪造导致网络安全问题日益凸显，借助伪造源地址发起的分布式拒绝服务攻击 (DDoS) 是当前互联网面临的重要安全威胁之一[1-5]。如图所示，主机使用未分配给它的 IP 地址作为源地址发送报文的行为叫做 IP 源地址伪造，或者简称为源地址伪造。借助伪造源地址，攻击者可以发送多种类型的网络攻击，其中危害最大也最受关注的是分布式拒绝服务攻击（DDoS）。基于源地址伪造的 DDoS 攻击可以分成两类：第一类是攻击者伪造源地址向受害者主机发送 DDoS 攻击，源地址伪造在这类攻击中充当着隐匿攻击者的作用，由于这类攻击的攻击目标是伪造报文的目的地址，因此也将这类攻击记为 d-DDoS。d-DDoS 的攻击原理如图所示。第二类是攻击者伪造受害者主机的源地址向反射节点发送报文，骗取反射节点的回复，以此造成 DDoS 攻击，源地址伪造在这类攻击中充当着反射的作用，由于这类攻击的攻击目标是伪造报文的源地址，因此也将这类攻击记为 s-DDoS。如图所示，在 s-DDoS 中，攻击者 a 使用攻击目标 v 的地址作为源地址发送请求到一些无辜的主机 i1,i2,...,in，而它们的回复报文将淹没 v。

d-DDoS 攻击举例（YCP SYN Flooding）

s-DDoS 攻击举例（DNS 反射、使用 ICMP 的 Smurf 攻击，使用 UDP 的 Fraggle 攻击，NTP 反射攻击）（在 Smurf 攻击中，攻击者使用受害者的 IP 地址作为源地址，发送 ICMP 请求到一个广播的目的 IP 地址；位于目的广播域内的主机都会响应这个 ICMP 请求，并将响应发送给受害者）

造成 IP 源地址伪造攻击泛滥的根源在于当前互联网体系结构设计上的缺陷，当前互联网采用分组交换的通信范式，在这种通信范式下，被传输的数据被切分成块，每块数据被加上头部信息后称之为 IP 分组，每个分组独立在网络中传输。由于 IP 分组在路由器中的正确转发仅仅依赖于分组的目的地址，因此路由器对 IP 分组的源地址不做检查，这使得攻击者可以任意修改发送的报文的 IP 源地址而不会影响分组的正常转发。

除了使用伪造源地址发起网络攻击外，主机使用伪造的源地址发送报文，还可能导致以下后果：第一，报文无法溯源。源地址用于标识报文发送者的位置，而使用伪造的源地址将导致无法找到报文发送者的位置。第二，可信基础被破坏。IP 地址往往作为可信标识符与网络主机甚至用户的身份相关联，一些网络系统常常根据报文的源地址进行授权、验证和资源分配，而伪造源地址的使用将破坏这一

可信基础。[此处对刘冰洋博士论文需要更改] 源地址伪造不仅危害网络安全，还给网络可信、管理、计费、测量等造成诸多麻烦。它使得基于源地址的验证和授权不再可靠、基于源地址的网络管理不再有效、基于源地址的网络计费不再准确、基于源地址的网络流量统计和测量不再权威。当人们创建新的网络应用时，还要考虑到诸如如何识别伪造请求、如何防御伪造攻击等问题，增加了系统的复杂度，给网络创新和发展增添了障碍。

存在的对 IP 源地址伪造进行防御的方法大致可以分成两类：第一类叫做伪造源地址追溯技术。这类技术通过在攻击时定位攻击发起的位置，以便能够在攻击发起处设置过滤机制来抑制攻击；或者在攻击结束后追溯到攻击源头，进而揭示攻击者的身份，以便对不法的攻击发起者进行法律追责或起到威慑作用。第二类叫做源地址验证技术，通过识别和过滤伪造报文，在攻击发生的时候前摄地或主动地抑制伪造攻击。RFC 5210 定义了源地址验证的体系结构（SAVA）[6]，如图所示，它按照部署位置和功能的不同，将互联网上的源地址验证分为三个层。自底向上，分别是接入网源地址验证、自治域内源地址验证和自治域间源地址验证。接入网源地址验证通过报文监听建立绑定规则，将伪造报文在其转发过程中的第 1 跳交换机予以丢弃，能够实现主机粒度的源地址验证。自治域内源地址验证进行 IP 前缀粒度的源地址验证，用于过滤域内用户发起的伪造报文。自治域间源地址验证进行 AS 粒度的源地址验证，可通过不同自治域的相互协作传递过滤规则，达到过滤域外源地址伪造报文的效果。

基于 IPv6 网络进行源地址验证易于部署实施，并且有着更为广泛的应用：IPv4 的局限性：（1）IPv4 地址枯竭，[Internet 规模的快速扩大，地址空间分配不均]（2）路由可扩展性的局限 [核心网路由器路由表条目数过大，地址规划的层次性不够]（3）NAT 技术的局限 [破坏了 IP 端到端模型，影响网络性能，影响端到端的网络安全] 现有的基于 IPv4 的互联网已经部署和运行多年，直接在其上部署新的源地址验证机制比较困难，并且代价高昂。IPv4 地址空间有限，网络地址转换（NAT）被广泛使用在现有网络上，而 IPv6 协议巨大的地址空间使得每一个接入网络的端系统都获得一个全局唯一的真实 IP 源地址成为可能。IPv6 巨大的地址空间，为基于真实 IPv6 地址的应用提供了机遇（追溯审计的 NIDTGA 应用）。

[研究源地址验证技术的原因。综上所述，为了从根本上解决上述问题，必须要加强源地址的真实性和可信性。因此，研究源地址验证技术，对于改善互联网的安全、可信、管理和创新，具有重要的意义。本文从安全性着手，研究通过源地址验证来防御网络攻击的问题。] 因此基于 IPv6 的源地址验证在接入网及自治域间的研究具有重要意义。

1.2　论文的主要工作及贡献

本文的主要工作是设计在 IPv6 下接入网及自治域间的源地址验证方案，为下一代互联网提供安全可信基础，增强网络管理和控制能力，促进基于 IPv6 可信应用的发展。如图所示，本文主要包括三部分的工作：基于 P4 的接入网源地址验证增强方案设计、基于 SRv6 的自治域间的源地址验证方案设计和原型系统的设计与实现。本文的主要创新点和贡献点如下：

- 基于 P4，提出了接入网源地址验证增强方案 P4SAVI
- 基于 SRv6，提出了自治域间源地址验证 SRP
- 设计并实现了一个接入网及自治域间源地址验证的实验床原型系统

1.3　论文的组织结构

本文的组织结构如下：第 2 章介绍论文研究的相关工作。第 3 章介绍基于 P4 的接入网源地址验证增强方案设计，并对其安全性、可扩展性进行了分析。第 4 章介绍了基于 SRv6 的自治域间的源地址验证方案设计，包括系统设计、算法设计、安全性分析等。第 5 章介绍了原型系统的设计与实现，并验证第 3、4 章提出的机制，评估性能及开销。最后，第 6 章对已提出的工作进行总结和展望。

第 2 章　相关工作

2.1　源地址验证

2.1.1　接入网源地址验证

存在的接入网源地址验证技术可以分成三类：端口绑定类技术、自验证技术、端到端验证技术。

2.1.1.1　端口绑定类技术

基于 EAP（Extensible Authentication Protocol）[7] 扩展的方法在对用户进行认证的同时，向用户分配地址，并将此地址绑定到交换机的端口上。这种方式的优点是在地址分配时就已经将用户和地址进行了绑定，因此有利于追溯地址的使用。缺点是这种方式实际上不兼容现有的地址分配方式，而且需要对主机和交换机都进行一定的修改。

Ethane[8] 是一个较为革新的绑定类技术，实际上是 OpenFlow 的雏形和一种应用。在 Ethane 中，源地址和设备接口的绑定并非是由设备本身决定的。网络中的管理服务器在处理用户的信息后，在接入设备上配置相关的规则。Ethane 实际上建立的是地址和用户身份的绑定关系。这种管理理念较为激进，在现在的网络中，大多数情况下使用的还是主机和地址的绑定关系。

IP Source Guard[9] 依赖于监听 DHCP 报文或者基于手动绑定，建立地址和交换机端口之间的绑定关系，并且利用此绑定来过滤报文。IP Source Guard 是 Cisco 公司的私有技术，很多厂商也实现了类似的过滤技术。IP Source Guard 及同类技术尽管得到了较为广泛的部署，但是存在一些问题：技术细节没有公开，也没有标准化；不能用于 IPv6 环境。

SAVM-SeND[10]，一个使用 SeND 协议提供源地址验证的解决方案。其假设 IPv6 网络下的所有主机配置上了 SeND 协议，想提供一个在所有地址分配情景下控制源地址伪造的机制；此外，它支持主机有着多个接口，每个接口有着多个 MAC 地址，端口移动性，可在接入网实现主机粒度的过滤。但它对主机协议栈进行了修改，并且绑定表项内容过多，需要耗费存储空间大。

SAVI[11] 要求所有传统二层交换机均部署 SAVI 才生效

VAVE[12]

SAV-Switch[13]

SDN-SAVI[14]

SAVSH[15]

SIPAV-SDN[16]

2.1.1.2　自验证技术

2.1.1.3　端到端验证技术

2.1.2　自治域内源地址验证

2.1.3　自治域间源地址验证

2.2　重复地址检测

2.2.1　重复地址检测拒绝服务攻击

重复地址检测被节点用来决定它想配置的地址是否已被另外一个节点使用。在将单播地址分配给接口前，必须要进行重复地址检测，而不管它们是通过静态配置、无状态地址自动配置（Stateless Address Autoconfiguration, SLAAC）[17] 还是动态主机配置（Dynamic Host Configuration Protocol for IPv6, DHCPv6）[18]。如表2.1所示，在重复地址检测中，NS 消息的源地址是未定义的，目的地址是一个 solicited-node 的组播地址，在这种情形下，NS 消息将被组播；NS 消息中的目标地址是一个节点（A）想要配置的暂时地址。当 NS 消息中的目标地址发生重复时，另外一个带有该地址的节点（B）将会回复 NA 消息。不同于 NS 消息，NA 消息中的源地址是 B 的接口地址，目的地址是一个 all-node 的组播地址，这意味着 NA 消息将组播至相同链路①的所有节点上；NA 消息中的目标地址是节点 A 想要进行重复地址检测的 IPv6 地址。

表 2.1　重复地址检测中 NS、NA 消息的比较

消息	源地址	目的地址	目标地址
NS	Unspecified	Solicited-node multicast address	Tentative address
NA	Interface address	All-node multicast address	Interface address

在重复地址检测过程中，主机首先组播 NS 消息以验证它想要配置的 IPv6 地址的唯一性。通常，另外一个主机会回复 NA 消息当它发现这个 IPv6 地址重复时。然而，这很容易让一个恶意的主机来伪造 NA 消息因为这里不存在安全机制来验证 NA 消息的发送者是否拥有这个 IPv6 地址。例如，图2.1展示了针对重复地址检测的拒绝服务攻击。当主机 C 想要配置一个全球单播地址 $\texttt{IP}_1$ (e.g.,

① 在这篇文章中，术语 “链路” 指的是由路由器限定的拓扑区域，在转发报文时递减 IPv4 TTL 或者 IPv6 跳数限制，与 RFC 4903[19] 中的定义一致。

2402::cf4e:3c0a:8490:88e1), 它首先组播 NS 消息到链路上以验证 $\texttt{IP}_1$ 的唯一性. 然而，这条链路上的攻击者可以回复一个伪造的 NA 消息以表明 $\texttt{IP}_1$ 已被另外一个节点使用。当主机尝试配置另外一个地址 $\texttt{IP}_2$ (e.g., 2402::f0f6:9824:f8e4:8900) 并且发送另外一个 NS 消息去验证 $\texttt{IP}_2$ 的唯一性时, 攻击者仍然可以发动攻击通过发送另外一个伪造的 NA 消息以表明 $\texttt{IP}_2$ 也被使用。这个结果导致主机 C 不能给它的网络接口配置任何 IPv6 地址。

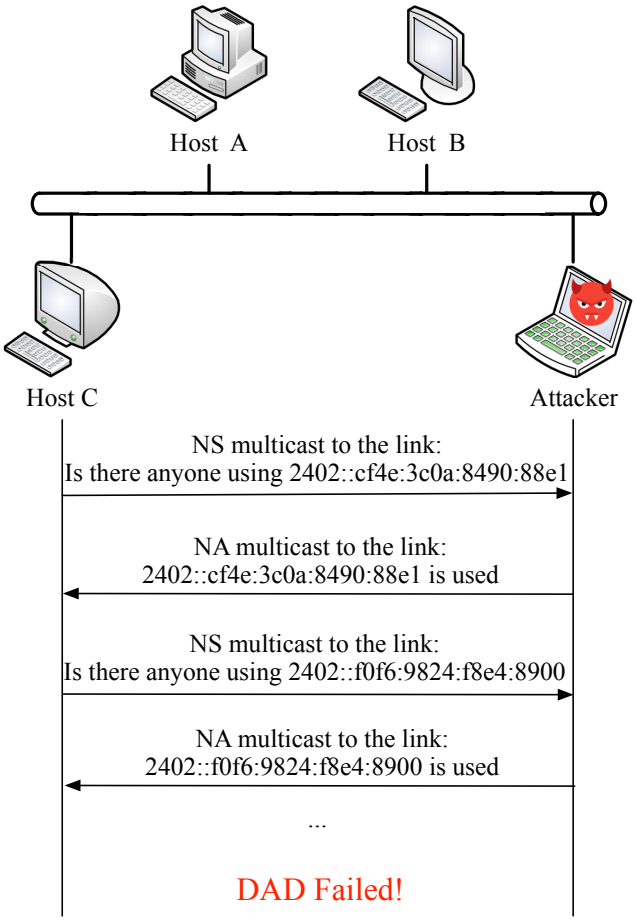

图 2.1　针对重复地址检测的拒绝服务攻击。主机 C 不能配置配置任何地址在它的接口上当攻击者发动拒绝服务攻击时。

表 2.2　Test results of spoofed target addresses on link-local address autoconfiguration.

Operating System	**Source Address = Target Address**	**Source Address ≠ Target Address**
Ubuntu 16.04	Three tentative link-local addresses	Three tentative link-local addresses
CentOS 7.6	Three DAD-failed link-local addresses	Three DAD-failed link-local addresses
Windows 10	No link-local addresses	No link-local addresses
Windows 7	No link-local addresses	No link-local addresses
macOS 10.15	No link-local addresses	No link-local addresses

表 2.3　Test results of spoofed NA messages in different address assignment mechanisms.

Address Assignment Mechanism	**Source Address = Target Address**	**Source Address ≠ Target Address**
SLAAC	No global unicast addresses	No global unicast addresses
DHCPv6	No global unicast addresses	No global unicast addresses
Manual Configuration	No global unicast addresses	No global unicast addresses

2.2.2　针对重复地址检测拒绝服务攻击解决方案

当前，存在的预防针对重复地址检测进行拒绝服务攻击的解决方案可以划分成三类: 隐藏目标地址, 认证 NDP 消息, 统一回复 NA 消息。(1) 隐藏目标地址: 这类解决方案的核心想法是在重复地址检测过程中隐藏 NS 消息中的目标地址。DAD-match[20] 以及 Pull Model[21] 将目标地址的哈希值而不是将目标地址直接嵌入 NS 消息中。其它主机计算它们自身地址的哈希值并将其与 NS 消息中的哈希值进行比较以决定是否需要回复 NA 消息。Wang et[22] al 提出了一种掩盖部分目标地址的机制，其它主机比较未掩盖的部分目标地址，如果未掩盖的部分目标地址重复，就回复标准的 NA 消息，然后主机收集所有 NA 信息，以确认地址是否唯一。虽然这种解决方案可以减轻对重复地址检测的拒绝服务攻击，但它们需要修改 NDP 和主机协议栈，这将使得它们难以在当前网络中部署。(2) 认证 NDP 消息：这类解决方案通过在 NDP 消息中添加消息认证码以增强重复地址检测的安全性。Trust-ND[23] 以及 Secure-DAD[24] 是这类解决方案的典型代表，它们各自使用 SHA-1 以及 UMAC 哈希函数来计算消息认证码。然而，由于其自身设计，Trust-ND 容易遭受碰撞攻击。此外，一个攻击者仍然可以使用 SHA-1 来计算正确的消息认证码并将其附加在伪造的 NA 消息上以发动针对重复地址检测的拒绝服务攻击。Secure-DAD 并没有解决在新接入主机与链路中已经存在的主机之间密钥共享问题，如果所有主机共享相同密钥, 在相同链路的攻击者仍然可以发动拒绝服务攻击。如果一个新接入主机需要与链路上所有主机建立共享密钥，攻击者仍然可以使用这个密钥计算消息认证码并发动拒绝服务攻击，更不用提主机之间密钥交换的可扩展性问题。此外，它们均在 NDP 消息中引入了新型选项，这需要对 NDP 以及主机协议栈进行修改。（3）统一回复 NA 消息：这类解决方案利用一个中央的可靠节点来统一地回复 NA 消息，而忽视由其它节点发出的 NA 消息。Nelle et al[25] 使用 SDN 交换机充当 NDP 代理来拦截所有 NDP 消息并将它们统一转发至 SDN 控制器。由于控制器存储了所有已分配的 IPv6 地址，如果一个暂时地址重复，它将回复一个 NA 消息。Rule-Based 机制[26] 使用中央节点来存储所有已配置的 IPv6 地址，其它节点必

须要接收它的确认消息以验证一个暂时地址是否重复。然而，SDN 遭受一系列的安全问题[27-29]，例如拒绝服务攻击。它们均需要一个中央节点来存储所有的 IPv6 地址，这就成为了一个单点故障，一旦出现安全问题，整个网络就会瘫痪。此外，Rule-Based 机制同样需要对 NDP 进行修改。

表 2.4对现有解决方案进行了比较，并总结了其局限性。

表 2.4　存在解决方案的比较

类型	机制	安全性	轻量级	鲁棒性	可部署性
隐藏目标地址	DAD-match[20]	51		51	
	Pull Model[21]	51		51	
	Wang et al.[22]	51		51	
认证 NDP 消息	Secure-DAD[24]			51	
	Trust-ND[23]			51	
统一回复 NA 消息	Nelle et al.[25]		51		51
	Rule-based[26]	51	51		

2.3　可编程设备以及 P4

P4[30] 是一门基于可重配置匹配行为表 (Reconfigureable Match Tables, RMT) 模型[31] 的用于可编程交换机 ASICs(Application-Specific Integrated Circuits) 芯片的领域特定语言。如图2.2所示，RMT 包含五个组件：解析器、入口流水线、队列、出口流水线、逆解析器。解析器用于提取用户自定义的头部字段。入口和出口流水线包含一个逻辑 match-action 阶段的序列，用于匹配特定的头部字段并执行对应的动作。入口流水线和出口流水线之间的队列系统与公共的数据缓冲区相关联，用于存储数据包。在出口流水线之后，逆解析器用于重新构建数据包。此外，P4 支持带状态的组件，例如寄存器、计数器，以便直接在数据平面上存储状态。一个 P4 程序只定义了数据平面的功能，需要来自控制平面的流规则来决定对每个数据包采取哪个动作。

考虑到灵活性，我们强调可编程设备带来的防止重复地址检测上拒绝服务攻击的新机会。在重复地址检测场景中，P4 中的可编程解析器可被定义来提取 NS 及 NA 消息中的目标地址。此外，P4 可以利用带状态的寄存器直接在数据平面维护绑定表。因此，P4DAD 可以监测重复地址检测的过程以建立主机的合法地址与交

换机端口之间的绑定表，并且使用它们去过滤伪造的 NS 以及 NA 消息。考虑删掉

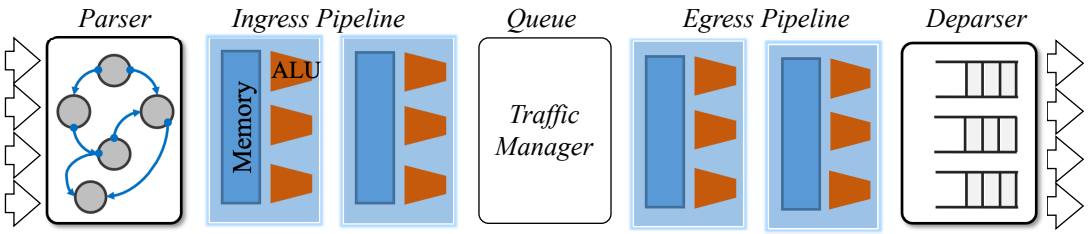

图 2.2　交换机芯片结构

2.4　IPv6 分段路由 SRv6

第 3 章　基于 P4 的接入网源地址验证增强

第 4 章　基于 SRv6 的自治域间源地址验证

4.1　问题描述

4.2　系统设计

第 5 章　基于 IPv6 的源地址验证的原型系统

5.1　试验床原型设计

5.2　接入网源地址验证增强的实现与验证

5.3　基于 SRv6 的自治域间源地址验证的实验与验证

5.4　本章小结

第 6 章　总结与展望

6.1　工作总结

6.2　未来展望

参考文献

[1] Handley M, Rescorla E. Iab," internet denial-of-service considerations[R]. RFC 4732, December, 2006.

[2] Mahjabin T, Xiao Y, Sun G, et al. A survey of distributed denial-of-service attack, prevention, and mitigation techniques[J]. International Journal of Distributed Sensor Networks, 2017, 13 (12): 1550147717741463.

[3] Specht S, Lee R. Distributed denial of service: Taxonomies of networks, attacks, tools, and countermeasures[J]. Princeton University Department of Electrical Engineering Technical Report CE-L, 2003, 3.

[4] Mirkovic J, Reiher P. A taxonomy of ddos attack and ddos defense mechanisms[J]. ACM SIGCOMM Computer Communication Review, 2004, 34(2): 39-53.

[5] Lau F, Rubin S H, Smith M H, et al. Distributed denial of service attacks[C]// Smc 2000 conference proceedings. 2000 ieee international conference on systems, man and cybernetics.'cybernetics evolving to systems, humans, organizations, and their complex interactions'(cat. no. 0: volume 3. IEEE, 2000: 2275-2280.

[6] Wu J, Bi J, Li X, et al. A source address validation architecture (sava) testbed and deployment experience[J]. IETF RFC5210. Internet Engineering Task Force, Fremont, CA, 2008.

[7] Aboba B, Blunk L, Vollbrecht J, et al. Extensible authentication protocol (eap)[J]. 2004.

[8] Casado M, Freedman M J, Pettit J, et al. Ethane: Taking control of the enterprise[J]. ACM SIGCOMM computer communication review, 2007, 37(4): 1-12.

[9] Bhaiji Y. Network security technologies and solutions (ccie professional development series)[M]. Pearson Education, 2008.

[10] Lin P, Bi J. A novel send based source address validation mechanism (savm-send)[C]// 2009 Ninth Annual International Symposium on Applications and the Internet. IEEE, 2009: 149-152.

[11] Wu J, Bi J, Bagnulo M, et al. Request for comments: number 7039 Source Address Validation Improvement (SAVI) Framework[M/OL]. RFC Editor, 2013. https://rfc-editor.org/rfc/rfc7039.txt. DOI: 10.17487/RFC7039.

[12] Yao G, Bi J, Xiao P. Source address validation solution with openflow/nox architecture[C]// 2011 19Th IEEE international conference on network protocols. IEEE, 2011: 7-12.

[13] Jinlong H, Yisheng W. Source address validation based ethernet switches for ipv6 network[C]// 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE): volume 3. IEEE, 2012: 84-87.

[14] Liu B, Bi J, Zhou Y. Source address validation in software defined networks[C]// Proceedings of the 2016 ACM SIGCOMM Conference. 2016: 595-596.

[15] Chen G, Hu G, Jiang Y, et al. Savsh: Ip source address validation for sdn hybrid networks[C]// 2016 IEEE Symposium on Computers and Communication (ISCC). IEEE, 2016: 409-414.

[16] Meena R C, Nawal M, Bundele M. Sipav-sdn: Source internet protocol address validation for software defined network[J]. Network, 2019, 3(S1): S2.

[17] Narten D T, Jinmei T, Thomson D S. Request for comments: number 4862 IPv6 Stateless Address Autoconfiguration[M/OL]. RFC Editor, 2007. https://rfc-editor.org/rfc/rfc4862.txt. DOI: 10.17487/RFC4862.

[18] Mrugalski T, Siodelski M, Volz B, et al. Request for comments: number 8415 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)[M/OL]. RFC Editor, 2018. https://rfc-editor.org/rfc/rfc8415.txt. DOI: 10.17487/RFC8415.

[19] Thaler D. Request for comments: number 4903 Multi-Link Subnet Issues[M/OL]. RFC Editor, 2007. https://rfc-editor.org/rfc/rfc4903.txt. DOI: 10.17487/RFC4903.

[20] Al-Ani A K, Anbar M, Manickam S, et al. DAD-Match: Technique to Prevent DoS Attack on Duplicate Address Detection Process in IPv6 Link-local Network[J/OL]. J. Commun., 2018, 13 (6): 317-324. https://doi.org/10.12720/jcm.13.6.317-324.

[21] Yao G, Bi J, Wang S, et al. A Pull Model IPv6 Duplicate Address Detection[C/OL]// Proceedings of the 35th Annual IEEE Conference on Local Computer Networks, LCN 2010. Denver, Colorado, USA, 2010: 372-375. https://doi.org/10.1109/LCN.2010.5735746.

[22] Wang X, Cheng H, Yao Y. Addressing With an Improved DAD for 6LoWPAN[J/OL]. IEEE Communications Letters, 2016, 20(1): 73-76. https://doi.org/10.1109/LCOMM.2015.2499250.

[23] Praptodiyono S, Hasbullah I H, Kadhum M M, et al. Securing Duplicate Address Detection on IPv6 Using Distributed Trust Mechanism[J]. Int J Simulation—Systems, Sci Technol, 2016, 17 (26).

[24] Rehman S U, Manickam S. Improved Mechanism to Prevent Denial of Service Attack in IPv6 Duplicate Address Detection Process[J]. Int. J. Adv. Comput. Sci. Appl, 2017, 8(2): 63-70.

[25] Nelle D, Scheffler T. Securing IPv6 Neighbor Discovery and SLAAC in Access Networks Through SDN[C/OL]// Proceedings of the Applied Networking Research Workshop, ANRW 2019. Montreal, Quebec, Canada, 2019: 23-29. https://doi.org/10.1145/3340301.3341132.

[26] Rehman S U, Manickam S. Rule-based Mechanism to Detect Denial of Service (DoS) Attacks on Duplicate Address Detection Process in IPv6 Link Local Communication[C]// Proceedings of 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO). IEEE, 2015: 1-6.

[27] Scott-Hayward S, O'Callaghan G, Sezer S. SDN Security: A Survey[C/OL]// Proceedings of 2013 IEEE SDN for Future Networks and Services, SDN4FNS 2013. Trento, Italy: IEEE, 2013: 1-7. https://doi.org/10.1109/SDN4FNS.2013.6702553.

[28] Scott-Hayward S, Natarajan S, Sezer S. A Survey of Security in Software Defined Networks[J/OL]. IEEE Commun. Surv. Tutorials, 2016, 18(1): 623-654. https://doi.org/10.1109/COMST.2015.2453114.

[29] Ahmad I, Namal S, Ylianttila M, et al. Security in Software Defined Networks: A Survey[J/OL]. IEEE Commun. Surv. Tutorials, 2015, 17(4): 2317-2346. https://doi.org/10.1109/COMST.2015.2474118.

[30] Bosshart P, Daly D, Gibb G, et al. P4: Programming Protocol-Independent Packet Processors[J/OL]. Computer Communication Review, 2014, 44(3): 87-95. https://doi.org/10.1145/2656877.2656890.

[31] Bosshart P, Gibb G, Kim H, et al. Forwarding Metamorphosis: Fast Programmable Match-Action Processing in Hardware for SDN[C/OL]// Chiu D M, Wang J, Barford P, et al. Proceedings of the 2013 Conference of the ACM Special Interest Group on Data Communication, SIGCOMM 2013. Hong Kong, China: ACM, 2013: 99-110. https://doi.org/10.1145/2486001.2486011.

附录 A　补充内容

附录是与论文内容密切相关、但编入正文又影响整篇论文编排的条理和逻辑性的资料，例如某些重要的数据表格、计算程序、统计表等，是论文主体的补充内容，可根据需要设置。

A.1　图表示例

A.1.1　图

附录中的图片示例（图 A.1）。

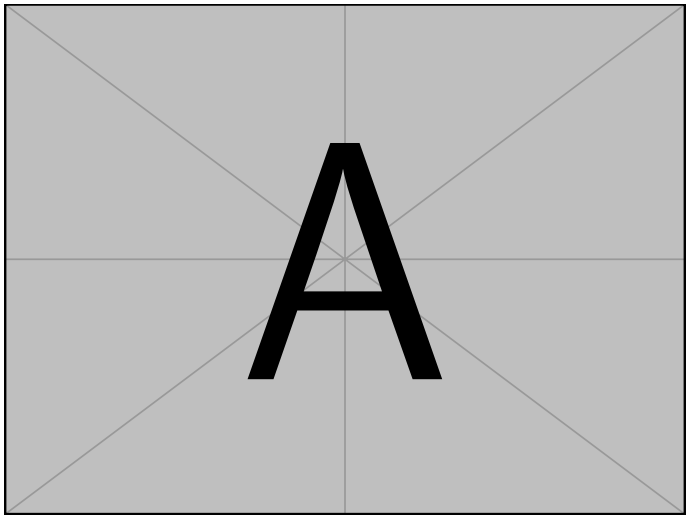

图 A.1　附录中的图片示例

A.1.2　表格

附录中的表格示例（表 A.1）。

表 A.1　附录中的表格示例

文件名	描述
thuthesis.dtx	模板的源文件，包括文档和注释
thuthesis.cls	模板文件
thuthesis-*.bst	BibTeX 参考文献表样式文件
thuthesis-*.bbx	BibLaTeX 参考文献表样式文件
thuthesis-*.cbx	BibLaTeX 引用样式文件

A.2　数学公式

附录中的数学公式示例（公式 (A-1)）。

$$\frac{1}{2\pi \mathrm{i}} \int_{\gamma} f = \sum_{k=1}^{m} n(\gamma; a_k) \mathscr{R}(f; a_k) \tag{A-1}$$

致　谢

衷心感谢导师刘莹老师对本人的悉心指导。在硕士三年期间，我的点滴成长都离不开刘老师的帮助和教诲。在日常的讨论与交流中，刘老师用言传身教的方式向我展现了对待学业和科研应有的认真负责、求实创新的态度。她为人亲和，兼容并包，关注学生个人发展，尊重学生的意愿，在我求学和研究的过程中给予了我极大的自由度，让我可以选择自己喜爱的领域进行学习和研究，同时又帮助我把握方向、聚焦问题，使我顺利完成硕士毕业课题的研究工作，并且极大地锻炼了我发现和解决问题的能力，使我终身受益。

感谢帮助过我的全体老师，他们包括但不限于吴建平教授、毕军教授、李星教授、徐明伟教授、徐恪教授、李贺武老师、李风华老师、马云龙老师、傅怡琦老师、潘丽老师、陆川老师等。感谢实验室的孟伟彬、操佳敏、李媛、王士诚、刘明星、徐一迟、张丰露同学，以及已经毕业的何林、贾溢豪、刘保君、颜建昊、步佳昊、李智涛师兄以及李丽姗师姐，感谢他们的陪伴，我的硕士生涯因为与各位同学的相识相处而变得丰富多彩。感谢各位专家学者在百忙之中抽出宝贵的时间阅读我的论文。感谢我的父母、女朋友、家人、同学、朋友在这三年对我的关心与帮助。

声　明

本人郑重声明：所呈交的学位论文，是本人在导师指导下，独立进行研究工作所取得的成果。尽我所知，除文中已经注明引用的内容外，本学位论文的研究成果不包含任何他人享有著作权的内容。对本论文所涉及的研究工作做出贡献的其他个人和集体，均已在文中以明确方式标明。

签　名：_____ 日　期：_____

个人简历、在学期间完成的相关学术成果

个人简历

1995 年 11 月 13 日出生于江西省宜春市高安县。

2014 年 9 月考入西安交通大学计算机科学与技术专业，2018 年 7 月本科毕业并获得工学学士学位。

2018 年 9 月免试进入清华大学网络科学与网络空间研究院攻读工学硕士学位至今。

在学期间完成的相关学术成果

学术论文：

[1] Kuang P, Liu Y, He L. P4dad: Securing duplicate address detection using p4[C]// ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 2020: 1-7.

[2] 况鹏, 刘莹, 何林, 等. 基于 IEEE 802.1 x 的嵌入用户身份标识的 IPv6 地址生成方案 [J]. 电信科学, 35(12): 15-23.

[3] Bai J, Bi J, Kuang P, et al. Ns4: enabling programmable data plane simulation[C]// Proceedingsof the Symposium on SDN Research. 2018: 1-7.

专利：

[4] 何林, 刘莹, 况鹏. 地址检测的方法、装置、交换机及存储介质: 中国, CN202010245453.6. (中国专利申请号.)

指导小组学术评语

论文提出了……

答辩委员会决议书

论文提出了……

论文取得的主要创新性成果包括:

1. ……

2. ……

3. ……

论文工作表明作者在 ××××× 具有 ××××× 知识，具有 ×××× 能力，论文 ××××，答辩 ××××。

答辩委员会表决，（× 票/一致）同意通过论文答辩，并建议授予 ××× （姓名） ××× （门类）学博士/硕士学位。