计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2022,31(4):14−32 [doi: 10.15888/j.cnki.csa.008419]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

国内互联网真实源地址验证研究进展①

甄龙飞[1,2], 吴振强[2], 马　克[1,3]

[1](青海师范大学 计算机学院, 西宁 810008)
[2](陕西师范大学 计算机科学学院, 西安 710119)
[3](青海师范大学 网络中心, 西宁 810008)
通信作者: 甄龙飞, E-mail: 1512368672@qq.com

摘　要: 为了分析我国源地址验证研究领域的研究现状、发展趋势和研究热点, 梳理源地址验证研究的发展趋势, 以推进国家网络数据可信化传输研究的进一步深入. 以中国知网数据库收录的基于源地址验证研究的论文文献为研究的数据来源, 应用文献计量学和科学知识图谱两种方法, 采用可视化工具 CiteSpace 对研究样本进行信息统计、共引统计和聚类分析, 绘制出该研究领域的文献年际变化图和共现聚类、时序分布的知识图谱, 从而进行科学性分析. 研究表明国内的源地址验证研究趋于动态发展, 趋势平稳向好; 核心研究力量: 以吴建平教授为首, 毕军、徐恪等为重要研究专家和以清华大学为首, 解放军信息工程大学、中国科学院大学等为重要的研究机构; 下一代互联网、软件定义网络等为重要的新兴研究热点, 体现了源地址验证研究的未来研究方向及发展趋势.

关键词: 源地址验证; 科学知识图谱; CiteSpace; 研究进展; 发展趋势; 可视化分析; 网络安全

引用格式: 甄龙飞,吴振强,马克.国内互联网真实源地址验证研究进展.计算机系统应用,2022,31(4):14–32. http://www.c-s-a.org.cn/1003-3254/8419.html

Domestic Research Progress of Internet Real Source Address Verification

ZHEN Long-Fei[1,2], WU Zhen-Qiang[2], MA Ke[1,3]

[1](School of Computer, Qinghai Normal University, Xining 810008, China)
[2](School of Computer Science, Shaanxi Normal University, Xi'an 710119, China)
[3](Network Center, Qinghai Normal University, Xining 810008, China)

Abstract: For further research promotion on the trusted transmission of national network data, this study sorts out the development trend of research on source address verification to analyze its research status, development trend, and research focuses in China. Taking the literature on source address verification from the CNKI database as the research data source, this study adopts the methods of bibliometrics and mapping knowledge domains and uses CiteSpace, a visual tool, to carry out information statistics, co-citation statistics, and clustering analysis on the research samples. Then, these data are used to draw the interannual variation map of the literature in this research field and the knowledge map of co-occurrence clustering and time-series distribution for further scientific analysis. The study shows that the research on source address verification in China tends to develop dynamically and the trend is stable and good. Core research strength is headed by Professor Wu Jianping with Bi Jun and Xu Ke as important research experts. Research institutions are headed by Tsinghua University along with PLA Information Engineering University, and Chinese Academy of Sciences as important participants. Next generation Internet and software-defined networks are important emerging research focuses, which reflect the future research direction and the development trend of source address verification.

Key words: source address verification; knowledge graph; CiteSpace; research progress; development trends; visualized analysis; network security

① 基金项目: 青海省自然科学基金创新团队项目 (2020-ZJ-903)
收稿时间: 2021-06-23; 修改时间: 2021-07-14, 2021-07-23, 2021-07-27; 采用时间: 2021-07-30; csa 在线出版时间: 2022-03-22

由于 Internet 数据传输采用无连接的逐跳转发模式, 使网络节点之间的数据包在网络层传输时仅以目的 IP 进行寻址转发, 由此可能导致网络中的恶意节点伪造数据包中源端的 IP 地址以欺骗目的节点进行非法通信窃取目的端用户的相关信息, 导致了基于源地址欺骗类型的网络攻击行为的出现, 如 MITM、洪泛攻击、反射式攻击、DoS/DDoS 攻击等. 由此本段主要介绍源地址验证研究的目的、意义、方法、范围和背景等. 为了预防上述的恶意攻击行为, 在网络数据转发过程中有必要进行源地址验证, 它有助于保护网络层数据传输的整体安全. 源地址验证又称数据源真实性鉴别, 是指网络数据在转发的过程中利用数据包中的源 IP 地址在网路中的传输节点上进行源地址真实性鉴别再进行数据转发, 以保障目的端能接收到真实源端的数据报文进一步保障传输数据的安全. 为此我国在国家“973”项目计划“新一代互联网体系结构理论研究”项目之课题四进行真实 IPv6 源地址寻址体系结构的研究[1], 以此拉开了源地址验证研究的序幕, 使其在国家重点科研项目的支持下进行了深入探索, 研究成果颇丰, 掌握了一定核心的关键技术, 使该研究领域走在了世界前列.

在源地址验证研究漫长的岁月中, 经统计分析得知: 文献 [2–6] 分别从源地址验证研究的基础理论、体系架构、实现及实验情况和关键防护技术的 4 个大方面进行了重要的系统阐述, 表明源地址验证的研究对于新一代互联网 (IPv6) 安全起着重要的作用; 而基于源地址验证研究的综述仅有文献 [7] 一篇且仅阐述了互联网 AS 域间的源地址验证研究的现状和相关技术, 并没有一篇综合性的综述对该领域的研究现状、研究主题、研究热点和发展演化趋势进行详细阐述, 因此本文通过文献计量学的方法统计了近 25 年来对源地址验证研究的文献并采用可视化手段, 对源地址验证研究的文献年际变化、重要作者、科研机构、高索引文献等方面进行了科学性分析, 同时应用 CiteSpace 可视化工具绘制出源地址验证研究的相关科学知识图谱, 如基于关键词共现、聚类、突现、时间线等知识图谱, 呈现出学界对源地址验证研究的研究主题、热点、发展现状及演化趋势, 以把握研究热点领域并进一步了解整体发展趋势, 从而为源地址验证的深入研究与实践提供参考借鉴.

1 数据来源与研究方法

1.1 数据来源与获取

为使科学研究的数据具有一定的代表性、关键性和权威性, 本文采用中国知网数据库 (CNKI) 收录的研究论文作为研究样本的数据来源, 主要通过高级检索来获取研究样本, 使得到的研究结果具有一定的有效性、准确性和真实性. 检索表达式为“主题&全文=源地址验证 or 源地址认证 or 源地址鉴别”, 需要注意的是源地址验证、源地址鉴别、源地址认证均为数据来源真实性鉴别研究课题的术语名词, 其研究内容、意义相同, 所以在以下研究分析中仅以源地址验证一词进行统称. 因此经检索后发现源地址验证一词最早出现于 1997 年, 便将检索时间设为 1997–2021 年, 共检索出 988 篇文献数据, 其中期刊论文 459 篇、博硕论文 366 篇、会议论文 15 篇、特色期刊 (中国教育网络) 126 篇、其他文献 22 篇 (含专题报道、简讯、图书、专利成果等). 然后对检索出的文献数据进行筛选, 剔除无效无用的文献 (含专题报道、简讯、图书、专利成果等), 最终共筛选出 817 篇有效数据作为研究样本.

1.2 研究内容

本文主要通过科学的分析方法对基于源地址验证及其相关研究领域的论文文献进行统计分析和可视化分析, 以可视化为主、计量为辅, 定性定量分析其在国内的发文情况、科研机构及作者的合作情况、主题和关键词的研究情况等, 探寻其内在的发展规律, 以进一步研判国内研究的发展趋势, 并总结出国内的研究现状和聚焦的研究热点.

1.3 研究方法与分析工具

本研究主要使用科学知识图谱和文献计量学两种研究方法对源地址验证的研究领域进行学科性分析, 并以科学知识图谱为主、文献计量学为辅来探寻源地址验证研究的内、外在发展规律. 科学知识图谱[8] 以知识域为研究对象, 并根据研究对象间的强弱联系来构建图网络结构, 通过基于作者、研究机构为主体和基于关键词、参考文献等为主题进行共现聚类的提取, 采用可视化工具呈现并分析该图网络结构, 以进一步分析某一学科领域的知识结构及其科研发展规律. 文献计量学[9] 是以文献为研究对象, 将研究对象整体进行量化分析, 采用数学与统计学的计量方法, 研究文献信息的分布、结构、数量关系及规律, 进而表征重要

文献作者分布的洛特卡定律、文献中词频分布的齐普夫定律和文献信息离散分布的布拉德福定律等.

所谓“工欲善其事, 必先利其器”, 本文采用陈超美教授研发的可视化分析软件 CiteSpace[10] 作为研究样本的主体研究工具, 它是科学知识图谱和文献计量学的通用分析工具之一, 是利用网络寻径算法与共引分析进行计量, 通过动态网络图谱的形式对某一知识领域的研究进展与宏观结构进行了可视化呈现[11]. 基于此, 利用 CiteSpace 的这一可视化特性, 对研究样本进行基于作者、研究机构的共现以及基于关键词的聚类、共现等方法, 通过可视化科学知识图谱, 勾勒出当前源地址验证研究领域的基本研究情况、发展趋势和聚焦的研究热点.

2 研究现状分析

本章通过采用文献计量学的方法, 应用数学和统计学对研究样本进行统计, 计算文献发文量以表现其研究发展的年际变化、计量研究机构发文情况以表现重视该研究领域的科研机构; 并以科学知识图谱的方式用 CiteSpace 对作者共现、机构共现、重要文献引用等情况进行可视化做最终分析, 最后总结出源地址验证研究的国内研究现状.

2.1 发文量统计分析

通过 CNKI 数据库检索出来的论文数据经筛选无效数据后共有 817 篇论文以源地址验证为主题或与其相关的研究为内容的论文进行过公开发表, 相关统计结果见图 1 所示. 根据图 1 中显示的基于源地址验证研究的总发文量、主题发文量、关键词发文量和相关研究发文量的统计, 可分析得出以下内容.

(1) 按总发文量分析, 可以看出从 2000–2009 年发文总量有增有降, 在 2009 年发文总量更是达到了巅峰, 以此可判定 2009 年源地址验证研究领域引发了学界的关注导致发文量激增; 2009–2016 年虽多数年份的总发文量呈下降趋势, 但年发文总量仍高于年均总发文量, 在此期间出现了如物联网、互联网+、大数据、云计算等新兴研究热点, 据此可推断此期间因热点研究的增加减缓了源地址验证领域的研究, 但其作为 IPv6 网络安全的基础难题依然备受关注, 发文总量虽有减少但依然可观; 2017–2019 年源地址验证研究又出现第二次研究高潮, 这段时期 IPv6 网络建设如火如荼, 可推断已步入基于 IPv6 网络的源地址验证的新一轮研究中; 至于 2020 年因新冠疫情爆发各学科研究领域论文发表均受到不同程度的影响, 因此总发文量减少是必然出现的情况; 从总体来看源地址验证研究趋势向好, 虽然该研究方向难度大, 但依然有大批学者跟踪研究. 依照上述源地址验证研究的发展趋势, 可预测 2021 年总发文量虽受新冠疫情波及, 但其发展趋势依然平稳向好.

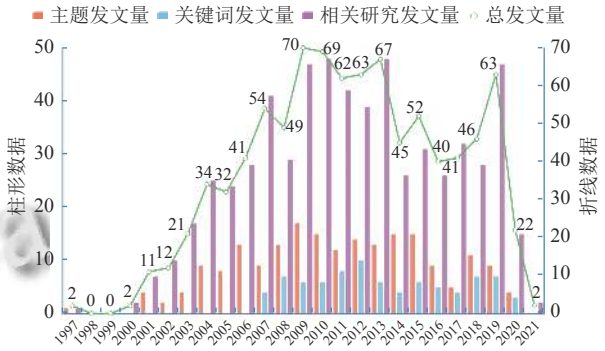

图 1 基于源地址验证研究的发文量统计时序变化

(2) 从主题、关键词发文数来看, 相继从 2000 年和 2007 年开始分别进行相关理论应用和专题研究, 其总发展趋势大体相同, 均呈波形曲线动态平稳发展, 有增有降. 值得注意的是在检索过程中发现源地址验证和源地址鉴别一词分别首次出现于文献 [12] 和文献 [13] 中, 其在文中仅作为一种网络安全防范技术进行引用并没有过多的详述, 据此可推测源地址验证研究在 1997 年以前的中国暂时没有进行该领域的专题研究, 而只是停留在引用国外的研究成果作为技术手段来参考使用, 因此国内在数据源真实性鉴别这一网络安全的基础研究领域上还没有引起重视. 并且以源地址验证为主题和关键词的论文分别在 2001 年和 2007 年发表. 在 2001 年文献 [14] 是以源地址验证的基础原理进行应用设计, 而由时任清华大学网络中心主任、CERNET 专家委员会主任吴建平教授在 2007 年发表的文献 [15] 则是从源地址验证技术理论的本身进行深入研究, 开启了我国从事网络数据源真实性鉴别领域的研究. 据此可进一步推测在 1997–2002 年间我国还停留在源地址验证技术的基础原理和应用层面上进行研究, 而从 2007 年开始我国网络工程专家学者逐渐进入网络数据源地址验证的深层次理论研究中, 激起了一股基于网络数据源验证安全理论的研究浪潮.

(3) 从相关研究发文量可以分析得出在 2007、2009、2010、2013、2019 这 5 个时间节点对基于源地

址验证相关研究的发文量均呈大幅度增长模式, 而究其背后原因是在国家倡导 IPv6 网络大规模部署的背景下导致其网络安全备受业界高度关注, 因此作为网络安全基础研究课题之一的源地址验证专题研究在这几个重要的时间节点内得到了一定的深入探索, 成果颇丰. 值得一提的是清华大学 2005 年在国际上首次提出真实源地址验证技术、2008 年在 IETF 发布了 RFC5210 作为第一个源地址验证体系架构的国际协议标准 (source address validation architecture, SAVA)[16], 随后又在 2013 年发布了 RFC7039 源地址验证改进框架协议 (source address validation improvement, SAVI)[17], 填补了国内在这一专题研究领域的空白, 为 IPv6 网络安全研究奠定了一定基础.

2.2 研究力量及其合作分析

本节从作者、研究机构两方面来分析源地址验证研究力量的分布和合作关系情况, 因此在可视化工具 CiteSpace 中将知识图谱的节点类型分别设置为 author、institution、author&institution, 时间划分为 1997 年至 2021 年, 每 1 年设为一个时间切片, 每个时间切片选取前 50 个, 得到作者共现图谱、重要作者及合作关系图谱、重要科研机构共现图谱和作者及科研机构合作共现图谱, 分别如图 2–图 6 所示. 从 2 个维度、4 个图谱对源地址验证研究的研究力量和合作关系进行科学性分析.

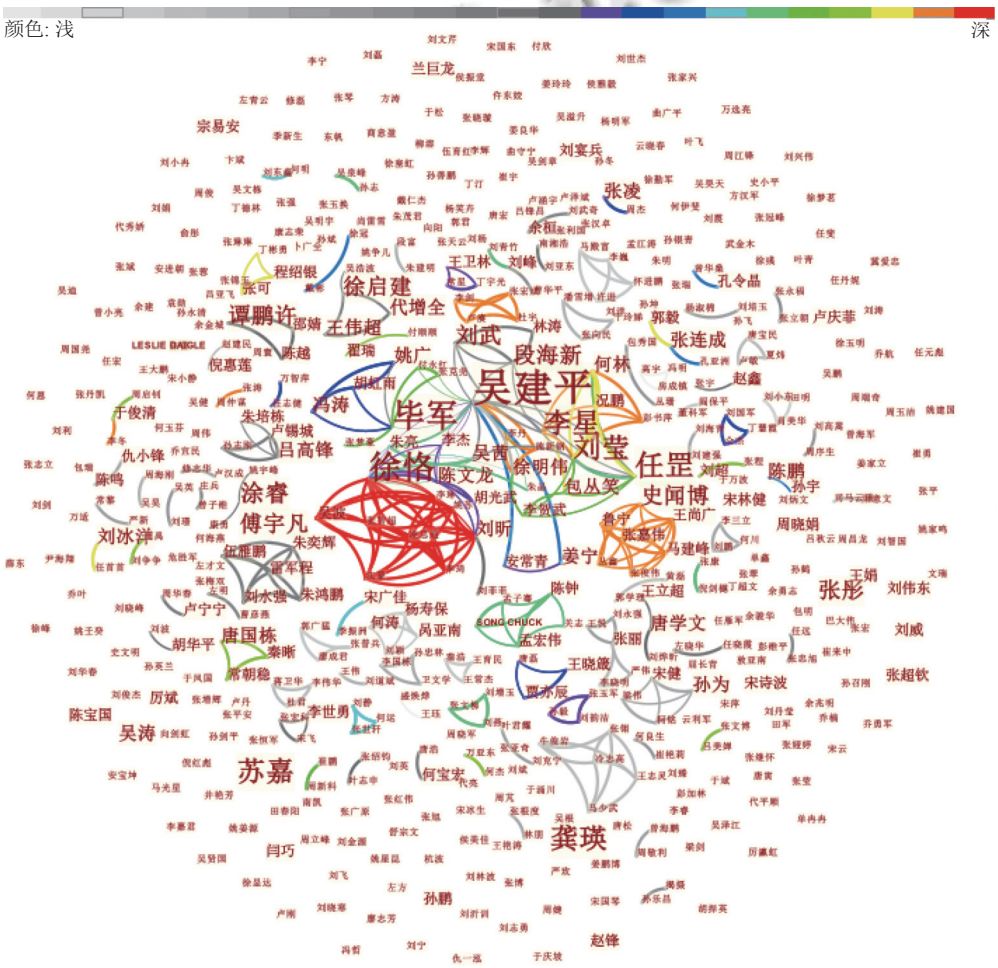

图 2 基于源地址验证研究的科研作者共现图谱

科研作者共现可视化知识图谱可以清晰地辨别出源地址验证研究领域作者发文量的多少以及两个或多个发文作者之间的合作关系强弱, 在图 2 中, 圆形节点表示作者的发文强度, 作者姓名的突出显示表示重要发文作者, 节点连线表示作者之间的合作关系, 连线的粗细代表着合作关系的强弱. 据此可分析出吴建平、毕军、徐恪、刘莹、任罡、李星等人是该领域的重要发文作者, 其中吴建平、毕军、徐恪 3 人的中心性较

大为该领域重要的研究专家, 相互之间形成较强的合作关系且与其周围的作者联系密切; 还有一些重要的发文作者如徐启建、谭鹏许、史文博、涂睿等人为该领域重要的研究学者, 其每个人与其他作者也有或强或弱的合作关系.

为了进一步分析作者间合作强弱关系, 通过 PageRank 算法进行了重要作者关系的提取. PageRank 算法是 Google 的网页排序算法对每个目标网页附上权值[18], 权值大的就靠前显示而权值小的就靠后显示, 因此抽象的应用到了 CiteSpace 软件中用来提取出重要作者之间的合作关系图谱, 如图 3 所示. 在图 3 中可以清晰看出作者之间的抱团关系和合作强弱关系, 其中吴建平与其它重要作者均有直接或间接的合作关系, 合作关系广泛; 其发文作者节点连线的强弱和颜色的深浅表明徐恪、李琳、姚苏、刘昕、李琦、凌思通、张智超、吴波、沈蒙的抱团最紧、合作关系最强.

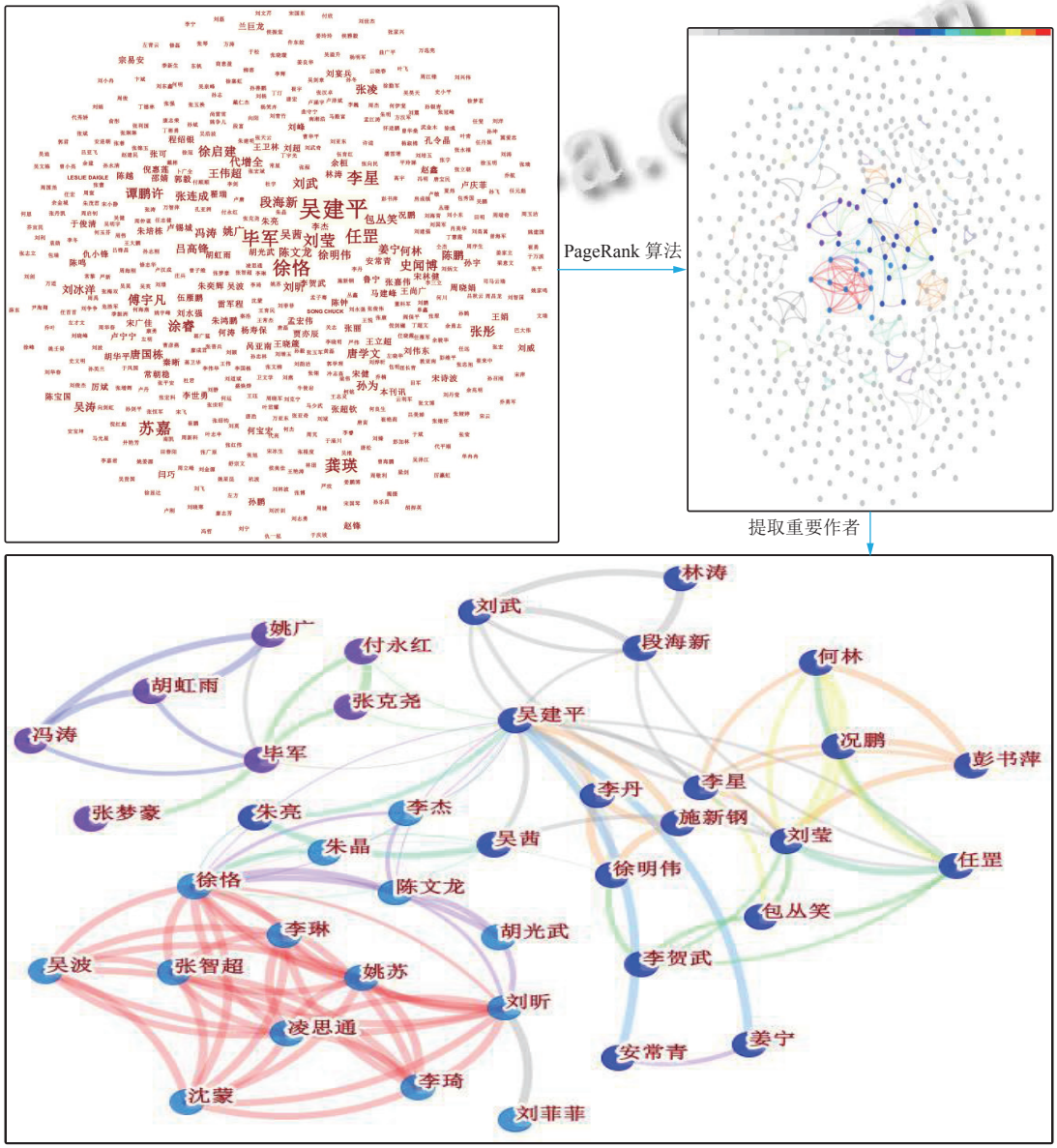

图 3　重要作者及合作关系共现图谱

综上所述, 吴建平、徐恪、毕军为源地址验证研究领域的重要研究专家, 广泛带动了其他计算机网络的专家、学者和科研人员从事源地址验证研究, 如刘莹、任罡、李星、徐启建、谭鹏许、史文博、涂睿等.

又通过 CNKI 数据库所获取到的研究样本统计得知共有 329 所科研院所参与过源地址验证研究, 并通

过 CiteSpace 可视化出重要科研机构共现图谱, 见图 4. 根据图 4 可以看出清华大学、中国科学院大学、北京邮电大学、解放军信息工程大学、解放军理工大学、国防科技大学、北京交通大学、工信部研究院等科研机构为重要的研究机构, 并且通过节点间的连线粗细、颜色深浅可知它们与其他科研机构合作关系有强有弱.

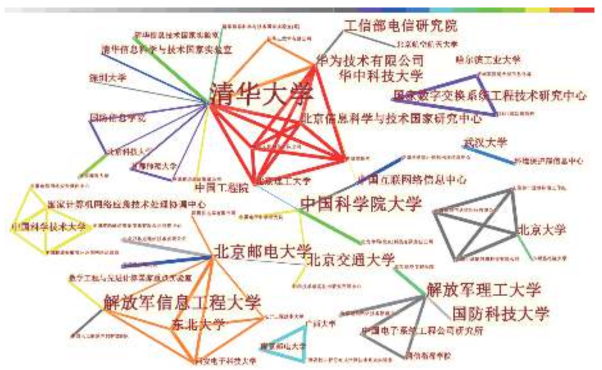

图 4　源地址验证研究的重要科研机构共现图谱

再通过图 5 对重要科研机构的发文量统计分析可进一步得知: 清华大学、解放军信息工程大学、国防科技大学对源地址验证研究领域的独立发文量高, 表明其独立研究能力强, 其中清华大学独立发文量最高, 可以推测清华大学在这一研究领域领先全国各科研院所, 推动了我国在这一研究领域的发展; 北京邮电大学虽独立发文量不突出但与其他科研院所的合作发文量最多, 据此可推测北京邮电大学与其他科研院所合作联系强、交流最多, 如东北大学、西安电子科技大学、解放军信息工程大学等; 可以看出大多数研究源地址验证的科研院所为我国双一流、一流院校或教育科研网 (CERNET) 的重要成员院校, 进一步表明源地址验证专题研究的关键性和重要性.

而根据图 6 所示的知识图谱可以形象的看出作者与科研机构的合作程度, 其中清华大学的节点最大、节点年轮最多、颜色最深、连线也最多表明其对源地址验证研究时间最长、研究能力最强、与研究作者联系最广泛和关系最密切; 毕军的作者节点半径最大, 表明在源地址验证研究领域其影响力最广泛; 北京信息科学与技术国家研究中心、东北大学等的研究作者抱团最紧, 表明合作关系最密集.

2.3　重要文献索引分析

本节着重从源地址验证研究的重要文献引用情况进行统计分析, 在研究样本中统计到 10 篇比较重要且引用数较高的研究论文, 具体文献情况见表 1.

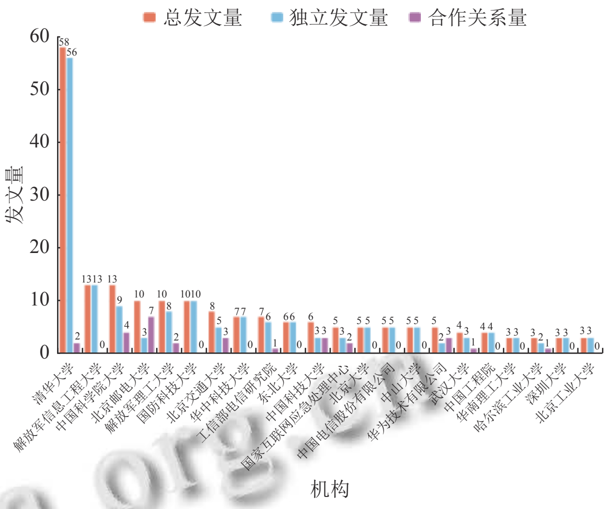

图 5　重要科研机构发文量及合作量统计图

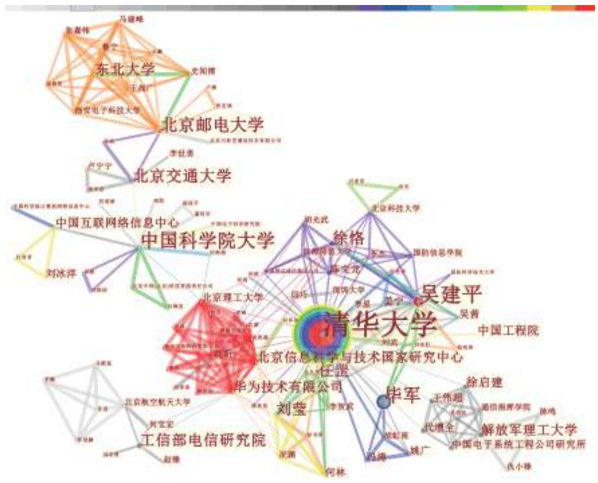

图 6　基于源地址验证研究的作者及机构合作共现图谱

在表 1 中显示由吴建平等发表的文献 [2] 引用数最高, 在文中“从互联网体系结构上找出其安全问题的根源, 确保下一代互联网地址及其位置的真实可信, 增强下一代互联网应用实体的真实可信, 从下一代互联网体系结构上系统地解决互联网安全问题, 是下一代互联网研究的另一个重要技术挑战”[2] 表明了源地址验证研究是下一代网络安全的基础挑战之一, 在文中又有对其做进一步描述“真实地址访问. 现有互联网存在的大量安全问题均是由于互联网对用户的源地址不加验证而带来的, 我们认为在新一代互联网中必须解决用户的真实地址访问的问题, 这将有助于解决安全可扩展和服务可扩展问题”[19]. 通过上述两段话的描述可以总结出源地址验证研究是下一代互联网安全基础的重中之重, 也是国家“973”项目的基础研究课题之一. 再从表 1 中高索引文献又可知源地址验证研究大部分

都是以网络安全为主题, 这说明源地址验证与网络安全息息相关, 其中 10 篇高索引文献中共现作者吴建平、徐恪两人次数最多, 是该领域的重要研究专家, 进一步印证了前节的预测.

表 1 基于源地址验证研究的重要论文统计照

文献编号	题目	作者	发表期刊	出版年份	引用数	下载数
[2]	下一代互联网体系结构基础研究及探索	吴建平, 吴茜, 徐恪	计算机学报	2008	186	2 393
[20]	分布式拒绝服务攻击研究新进展综述	孙长华, 刘斌	电子学报	2009	88	1 115
[19]	新一代互联网体系结构理论研究进展	吴建平, 刘莹, 吴茜	中国科学 (E辑: 信息科学)	2008	83	1 278
[21]	SDN体系结构与未来网络体系结构创新环境	毕军	电信科学	2013	70	1 254
[22]	SDN安全探讨:机遇与威胁并存	戴彬, 王航远, 徐冠等	计算机应用研究	2014	52	1 265
[14]	基于IPv6的防火墙设计	王常杰, 秦浩, 王育民	计算机学报	2001	46	414
[3]	构建基于真实IPv6源地址验证体系结构的下一代互联网	吴建平, 任罡, 李星	中国科学 (E辑: 信息科学)	2008	36	578
[6]	互联网地址安全体系与关键技术	徐恪, 朱亮,朱敏	软件学报	2013	28	516
[23]	互联网自动配置研究	李福亮, 杨家海, 吴建平	软件学报	2013	27	404
[24]	一种基于IPv6物联网分布式源地址验证方案	胡光武, 陈文龙, 徐恪	计算机学报	2012	22	1 561

2.4 研究现状总结

(1) 研究发展趋势. 在研究发展趋势上, 成波形曲线型动态平稳发展, 有增有降, 总体发展趋势平稳向好. 基于此, 基于源地址验证研究分为了 5 个阶段:

第 1 个阶段研究混沌期 (1997 年以前): 学习和建设使用互联网阶段, 单纯学习借鉴国外网络安全技术, 对源地址验证技术没进行过研究;

第 2 阶段研究初始期 (1998–2002 年): 开始攻克互联网的关键技术, 逐渐意识到源地址验证的重要性, 开启源地址验证的研究阶段, 进行初级理论和技术研究;

第 3 阶段研究发展期 (2003–2007 年): 下一代互联网创新探索期, 源地址验证作为其网络安全的基础技术进行共同探索, 初步掌握相关技术原理及应用, 形成初步研究体系;

第 4 阶段研究成熟期 (2008–2013 年): 下一代互联网部署规划期, 同时源地址验证研究取得新进展, 初步取得阶段性成果, 构筑源地址验证体系架构, 成为国际 IETF 组织认证的现行协议标准, 使该研究领域在国际上争得主动权;

第 5 阶段研究深入期 (2014 年至今): 下一代互联网建设应用期, 为使其网络安全进一步得到保障, 因此源地址验证研究步入深水期, 逐渐掌握关键技术, 在国际网络安全领域中逐渐取得主动权.

值得关注的是源地址验证研究的发展与我国下一代互联网建设的发展势头趋于同向, 是因为源地址验证作为下一代网络安全的基础技术应随互联网建设一同发展, 因此国内互联网高速发展的各时期源地址验证研究也得到了关注, 并与之同向发展, 为下一代互联网安全保驾护航.

(2) 研究力量分布与研究地位. 基于源地址验证研究的不断深入, 涌现出大批科研人员及科研院所, 比如在源地址验证研究领域中吴建平、毕军、徐恪等人为具有影响力的重要研究专家, 刘莹、任罡、李星、徐启建、谭鹏许、史文博、涂睿等人为该领域的重要研究学者; 清华大学、中国科学院大学、北京邮电大学、解放军信息工程大学、解放军理工大学、国防科技大学、北京交通大学、工信部研究院等科研机构为该领域重要的研究机构. 通过源地址验证研究的文献的高索引统计分析得知, 源地址验证为我国“973”国家重点计划项目的研究课题之一, 其重要性不言而喻. 在计算机网络的基础数据安全中起着举足轻重的作用, 因此国内大批双一流、一流院校和教育科研网重要成员院校对此进行跟踪研究, 并从未懈怠, 就可看出源地址验证研究在网络安全中的重要地位.

(3) 研究的作用与意义. 计算机网络在发送数据时仅以目的 IP 地址进行数据转发, 而不对转发数据包的源 IP 地址进行校验, 由此可能导致源地址欺骗攻击的出现, 进而发生诸如洪泛攻击、中间人攻击等的网络攻击行为. 为防止此类攻击在计算机网络中蔓延, 在当时源地址验证没有一个固定的定义标准, 因此出现了五花八门的源地址验证技术, 如基于加密验证方式的有网络安全协议 (Internet protocol security, IPsec)[25] 和

防欺骗方案 (spoofing prevention method, SPM)[26]; 基于过滤方法的有入口/出口过滤 (IEF)[27,28]、源地址有效性实施协议 (SAVE)[29]、基于跳数过滤 (hop count filtering, HCF)[30]、基于置信度的过滤 (CBF)[31]、基于路由的分布式包过滤 (router-based distributed packet fliter, DPF)[32] 以及调整跳数过滤 (MHCF)[33]; 基于追溯方法的有基于哈希的 IP 追溯 (SPIE)[34]、基于概率分组标记 (PPM)[35]、基于确定性分组标记 (deterministic packet marking, DPM)[36]、灵活确定性包标记 (FDPM)[37] 和基于确定性流标记 (DFM)[38] 等, 导致上述的源地址验证技术无法做到兼容, 且检验效果防御能力不尽如人意, 无法大规模有效部署和预防源地址欺骗类型的攻击. 为此我国清华大学 2008 年在 IETF 上发表了首个源地址验证体系架构标准 (SAVA), 采用网络分层结构协同预防源地址欺骗以达到可信网络的程度, 分为接入网、AS 域内、AS 域间 (含相邻 AS 和不相邻 AS 两种情况) 三部分[16], 可以针对网络的不同场景分层治理、协同治理, 提升了预防源地址欺骗攻击的综合防御能力. 随着互联网技术的不断更新, 其 SAVA 体系标准也进一步的精炼和补充, 添充了一些新的源地址验证防御思路, 由此出现了源地址验证改进框架协议标准 (SAVI)[17]. SAVI 弥补了原有协议标准上的一些不足, 并进行了改进, 使源地址验证技术体系更加充满了活力, 奠定了我国下一代网络建设的安全基石, 保障了 IPv6 网络的安全, 对我国新一代互联网的部署建设起到一定的安全指导意义.

3 研究热点分析

本章首先使用统计方法对关键词做初步分析, 再使用 CiteSpace 对关键词进行可视化分析. 通过关键词、聚类、时区分布、时间线发展的可视化知识图谱进行综合分析, 进而研判基于源地址验证的研究热点和相关研究主题的演化趋势.

3.1 基于关键词的研究热点分析

关键词分析能反映出源地址验证研究领域的一般研究热点, 利用 CiteSpace 对研究样本进行关键词共现、词频统计、中心性、爆发度等分析, 分辨出高词频、高中心性的研究热点, 并根据爆发度确定研究热点的热点程度, 相关图谱及数据见图 7、表 2.

根据中心性[39] 可以判断关键词的中介程度或发散程度, 通常表现为节点的中心化程度越高, 表明该节点越重要. 由此可根据表 2 的中心性数据判断出 IPv6、网络安全、源地址验证、IPsec、分布式拒绝服务攻击、防火墙、软件定义网络这 7 个关键词中心性较大, 表明它们是源地址验证研究的中心, 是比较重要的研究热点. 但从中心性数据上来看与词频分布并不成正比, 一般情况下, 中心性越大词频出现的程度应该更频繁[40], 但从数据来看分布式拒绝服务攻击和防火墙的中心性较大但它们的词频分布并不高, 这表明分布式拒绝服务攻击和防火墙虽然是研究热点但关注度不足, 应加强在这两个领域的研究. 再根据爆发度 (又称突现性)[41] 可以判断关键词在某个时期突显出来的研究热点, 通常可以发现关键词在某一时间范围内兴起的情况.

图 7 关键词共现图谱

表 2 关键词共现分析统计表

序号	关键词	初始时间	词频	中心性	爆发度	开始年份	结束年份	PageRank
1	IPv6	2001	182	**0.38**	—	—	—	**23.70**
2	网络安全	1997	147	**0.37**	—	—	—	**21.34**
3	源地址验证	2007	83	**0.22**	3.89	2015	2016	**15.04**
4	IPsec	2000	80	0.15	**13.88**	**2002**	**2007**	**10.88**
5	软件定义网络	2013	49	0.10	**16.23**	**2013**	**2021**	**7.62**
6	分布式拒绝服务攻击	2004	43	0.11	3.06	2018	2019	**7.72**
7	互联网	1997	37	0.06	—	—	—	6.48
8	防火墙	1997	32	0.11	8.15	1997	2007	6.24
9	虚拟专用网	2001	31	0.08	6.48	2001	2006	6.66
10	物联网	2011	27	0.05	6.09	2011	2014	4.88

进一步根据表 2 中的爆发度、初始和结束时间, 可以看出软件定义网络、IPsec 的爆发度位列第一、第二, 其强度分别达到 16.23 和 13.88 的高度, 据此可推测 IPsec 在 2002–2007 年、软件定义网络在 2013–2021 年分别是两个时期的重要研究热点和新兴研究热点. 值得注意的是软件定义网络时至今日仍是源地址验证研究的新兴研究热点, 其热点程度依然很强. 最后根

据 PageRank 算法的权值排序得出 IPv6、网络安全、源地址验证、IPsec、软件定义网络、分布式拒绝服务攻击这 6 大研究领域是现在重要的研究热点.

综上所述, 下一代互联网 (IPv6)、网络安全、源地址验证、IPsec、软件定义网络、分布式拒绝服务攻击是重要的研究热点, 其中 IPsec、软件定义网络是新兴的重要研究热点, 但根据爆发年份判断只有软件定义网络到时至今日仍是新兴的重要研究热点, 热度依然很高.

3.2 基于关键词聚类的热点及主题分析

关键词聚类知识图谱[42] 可以分析出研究的主题和热点的研究领域. 因此在第 3.1 节的研究基础上, 继续对研究样本进行寻找聚类操作, 可以进一步得到关键词聚类的科学知识图谱. 为了在聚类分析中得到最好的可视化结果, 引用了两个重要的指标来进行评估, 分别为模块值 (modularity) 和平均轮廓值 (mean sihouette):

(1) 模块值是用来评估聚类效果是否有效的重要指标[43], 以 Q 表示且 $Q\in[0, 1]$. 一般情况下在聚类过程中 Q 值越大表示图谱的聚类效果越好, 越有效. 其中 $Q>0.3$, 表示图谱的聚类效果显著; $Q<0.3$, 聚类效果不佳直接默认屏蔽.

(2) 平均轮廓值是用来衡量网络同质性的重要指标[44], 表示聚类内部的同质性, 以 S 表示且 $S\in[0, 1]$. 一般的若聚类内部成员数量少, 则平均轮廓值降低; 反之若聚类成员数量多则会使轮廓值增加. 其中, 若 $S>0.5$, 则表明聚类合理; 若 $S>0.7$, 则表示聚类结果高度可信.

因此在完成聚类操作后, 得到一个关键词聚类知识图谱, 如图 8 所示. 在该聚类图谱中, 网络节点 N=614, 边 E=996, 网络密度 $Density$=0.0053, 其中 Q=0.7304, 表明聚类的效果很好; S=0.9162, 表明聚类结果是高度可信的. 通过关键词聚类可视化知识图谱, 可知将关键词共划分为 16 类, 仅提取出前 9 大聚类, 分别为网络安全、IPv6、源地址验证、IPsec、分布式拒绝服务攻击、入侵检测、软件定义网络、物联网和加密算法, 其聚类强度随聚类颜色越深而越强. 这些类别中有涉及源地址验证的专题理论研究, 如源地址验证、加密算法; 又有涉及源地址验证的关键技术研究, 如网络安全, 下一代互联网 (IPv6)、分布式拒绝服务攻击、软件定义网络和物联网等; 也有涉及源地址验证的安全技术应用, 如 IPsec、入侵检测等; 还有涉及源地址验证的一些相关研究, 如区块链、多因素认证等. 为了能进一步直观看出各个聚类隐含的其他研究方向 (或称聚类的内部成员), 进行了统计并制成表格形式以进行展示, 如表 3. 其中可以通过各聚类的轮廓值 (silhouette) 表明各聚类结果真实可信.

图 8 基于关键词聚类共现图谱

表 3 关键词聚类分析统计表

聚类	聚类标签	Size	Silhouette	其他研究方向
1	网络安全	71	0.888	互联网; 过渡; 拒绝服务攻击; IP匿名; 源地址验证
2	下一代互联网 (IPv6)	68	0.86	形式化描述; 感知应用网络; BGP多协议扩展; 去中心化
3	源地址验证	59	0.802	接入网; 区块链; 网络层安全; 可信互联网; 准入控制; 互联网审计
4	IPsec	57	0.936	CGA; VPN; AH; 移动IPv6; NAT; 加密; IKE; ESP
5	分布式拒绝服务攻击	54	0.887	聚合签名; 网络监控; ACL; NS2; Netflow; 防御
6	入侵检测	46	0.81	协议簇; 入侵追踪; IP欺骗攻击; 防火墙; 安全策略
7	软件定义网络	33	0.848	流表匹配; 密码标识; 安全控制转发
8	物联网	30	0.946	头部压缩; 负载均衡
9	加密算法	15	0.993	多因素认证; IPsec VPN; 网络传输; 远程接入; 身份鉴别; 运营模式
10	区块链	7	0.993	拒绝服务攻击; 多因素认证; Chord环; 形式化描述; 安全模型; 身份签名

3.3 基于关键词时区分布的热点演化趋势

关键词时区分析采用关键词时区分布图谱[45](如图 9) 和关键词时间线分布图谱[46](如图 10) 进行综合性分析, 推断出研究热点和研究主题的演化发展趋势. 两大知识图谱能够反映出源地址验证研究的热点分布时期、主题与热点的变迁和演化趋势, 并与表 2 中关键词突现爆发度一同分析可对每一个演变阶段的研究热点进行剖析. 图谱中的节点越多表明文献量越多, 则该研究领域处于兴盛期; 反之则处于低谷期. 同时各节点间的连线及连线粗细分别代表了该研究热点的演化过程和传承关系.

根据图 9 和图 10 可以分析得到以下内容.

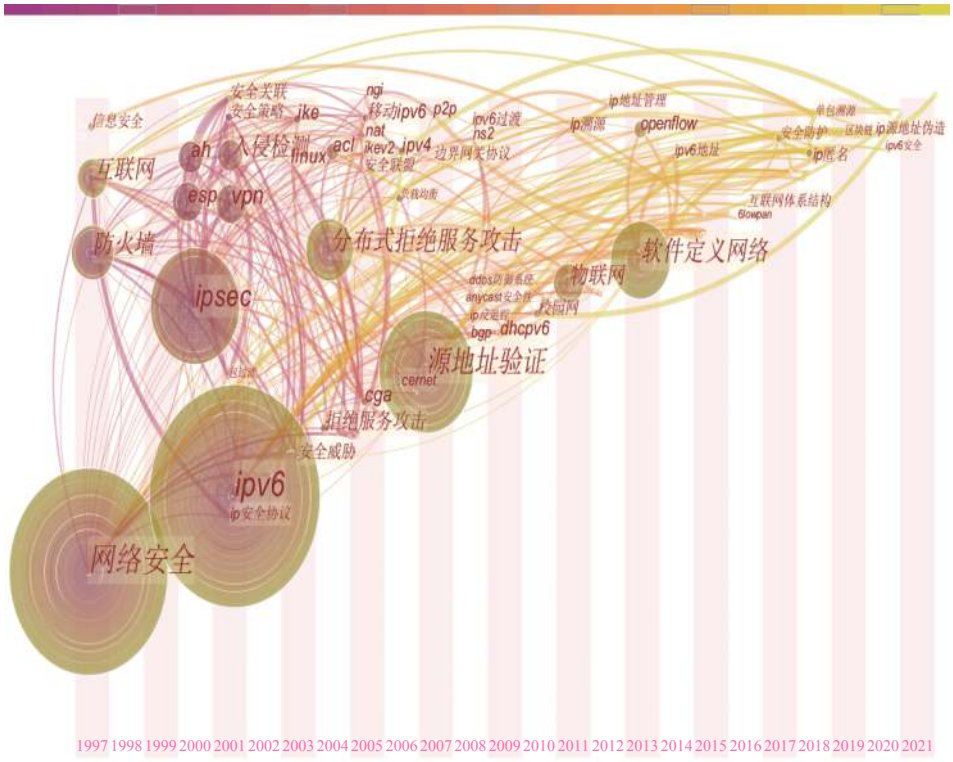

图 9 关键词时区分布图谱

1997–2000 年出现了 6 个研究热点, 按节点大小依次分别为网络安全、IPsec、防火墙、互联网、信息安全、封装安全有效载荷 (ESP) 和认证头 (AH), 再根据节点年轮的颜色变化判断该研究方向的热点强度, 又可看出网络安全、IPsec 是这一时期的重要研究热点, 并且其他研究热点均与网络安全息息相关, 证明它既是当时的时代主题也是现在的重要研究热点, 需要注意的是这一时期的学者只注重于源地址验证技术的应用而不懂其研究原理, 无异于缘木求鱼, 此时期处于源地址验证研究的混沌期;

2001–2010 年出现了下一代互联网 (IPv6)、源地址验证、分布式拒绝服务攻击、虚拟专用网、入侵检测共 5 个主要的研究热点, 同理分析可知前 3 个研究热点到目前为止还是重要关注的研究热点, 其中下一代互联网 (IPv6) 可能是时代的研究主题, 值得一提的是随着国家对于下一代互联网研究的不断深入, 源地址验证作为下一代互联网安全难题之一的基本解决方案, 也逐渐引起了学者的关注, 与此同时开始了源地址验证的专题研究, 搭上了研究下一代互联网的顺风车, 由此进入了源地址验证研究的快速发展期;

2011–2021 年出现了软件定义网络、物联网、OpenFlow 为当代的研究热点, 其中 OpenFlow 是一种实现控制软件定义网络的网络通信协议[47], 再根据节点大小可知软件定义网络是重要的研究热点, 并根据热点突现的爆发度分析又知软件定义网络将是源地址验证未来重要研究方向, 此时我国已掌握了部分源地址验证的关键核心技术, 开始将其扩展应用到各个研究领域中, 进入到源地址验证研究的深入创新应用期.

综上所述, 网络安全、IPsec、下一代互联网 (IPv6)、源地址验证、分布式拒绝服务攻击、软件定义网络是源地址验证研究的重要研究热点, 其中网络安全、下一代互联网 (IPv6)、软件定义网络为各个时期最重要的研究主题, 软件定义网络将是未来的重要研究方向; 其发展趋势从研究混沌期到研究初始期又到研究发展期再到研究深入应用创新期按时代渐变发展, 符合科学研究的一般发展规律. 因此上述研究热点、研究主题、演化发展趋势的总结与第 3.1、3.2 节的分析相对吻合, 所以分析结果具有一定的可信性.

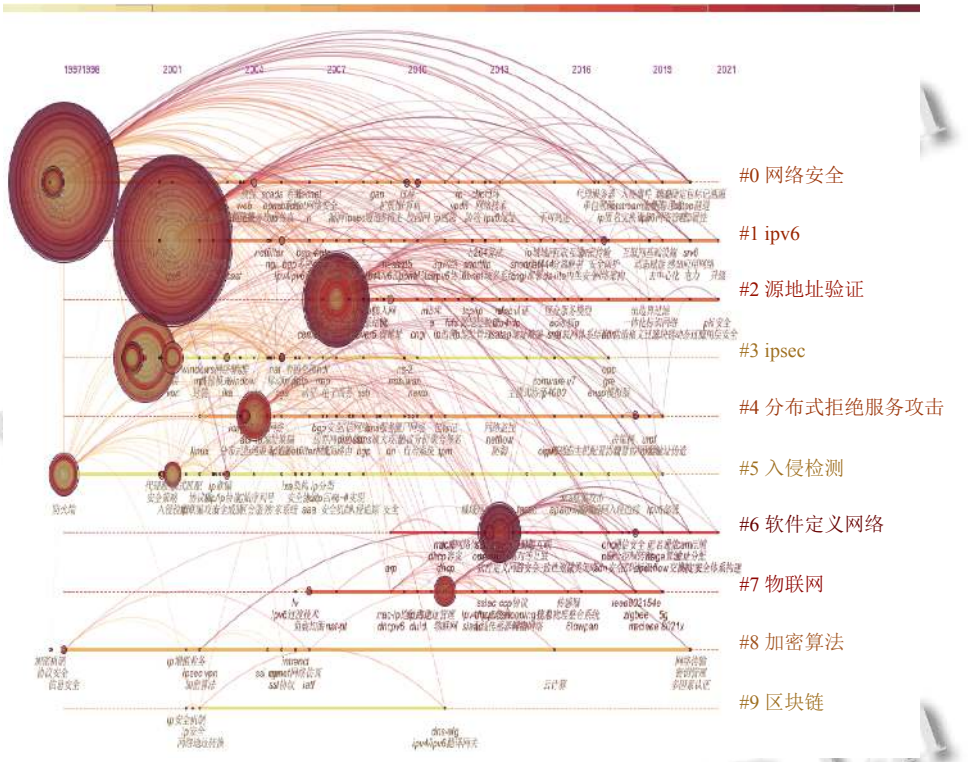

图 10 关键词时间线分布图谱

4 源地址验证研究进展

大量源地址验证技术的层出不穷导致了不同验证方案各有千秋, 出现这种情况的主要原因是: 一方面说明没有一种验证方案优于其余方案, 不具有明显优势, 强调了该研究课题的困难性; 另一方面表明在复杂的互联网环境中, 研究者需对源地址验证研究的各种网络场景具体分析以采取不同的研究策略和验证方法, 再借鉴早期源地址验证方案原理来进行革新, 设计出可行的源地址验证技术, 如 Passport[48]、Base[49] 是对 SPM[26] 验证方案原理的改进; IDPF[50]、SAVE[29] 的设计是基于 DPF[51] 框架思想; RPF[52] 是网络入口过滤 (network ingress filtering, NIF)[27] 的一种扩展方案; SAVA 根据网络层次结构提出协作防御源地址验证架构等等. 这些源地址验证方案均借鉴了前人的设计思想, 进而研究出相应的验证方案, 因此源地址验证研究进展分析对重要验证方案的了解是必要的.

4.1 源地址验证的定义及基本原理

Internet 网络中传输的数据包需经过 TCP/IP 协议栈的处理, 由于 TCP/IP 协议栈是“自顶向下、逐层封装”的网络传输协议, 因此数据包经每一层传输时都要对其进行封装和解封装, 以形成一个包含了源和目的信息的完整数据包, 才能在网络上进行传输最后到达目的终端. 然而, 主机在传输数据包时存在缺陷, 即接收数据的目的主机和在传输路径上的各路由器均不对源 IP 地址进行真实性校验, 仅依靠目标 IP 进行数据转发. 攻击者很容易利用这一缺陷在传输的数据包中填入伪造的源 IP 地址, 就可冒充他人将非法数据报文发送到目的主机处, 进而可以获得目标终端的控制权, 为下一步网络攻击的实施奠定基础. 从技术上来讲, 源地址欺骗威胁来源于传输路径上的路由器只依赖数据报

文的目的 IP 进行转发, 而忽略了验证发送方数据中源 IP 地址的真实可信性, 造成了源地址欺骗的网络威胁, 如恶意源端发动源地址欺骗、身份伪造等攻击, 严重影响网络通信双方的真实性; 或数据包在转发过程中易遭到源地址的恶意篡改、恶意劫持和重定向威胁等现象, 严重影响网络通信过程的可信性; 再或者目的终端缺乏对非法数据的有效识别、过滤等防御能力, 导致通信安全性降低等问题.

现有的源地址验证的工作原理主要有源端加密、路径传输验证和目的端校验的方式来提升网络通信双方的真实性、可信性. 当数据包的源地址遭到发送源端的恶意伪造或中间路由节点的非法篡改时, 下游网络节点、目的端能够及时对数据进行源地址验证, 识别并丢弃或过滤非法的数据, 保证网络通信双方的真实性、可信性和安全性.

4.2 源地址验证经典技术介绍

为了区分各类验证方案的差异, 考查方案的可行性、有效性, 早期的研究者根据方案的设计原理一般将之分为加密认证、报文过滤和事后追踪 3 类, 这 3 类验证方案为后人学者提供了参考借鉴[25–65]. 因此本节将围绕这 3 类验证方案来介绍部分重要的验证方案和基于 3 类验证原理方案的革新技术. 由于这些技术原理的叙述过于繁杂特以图表形式进行概要介绍, 可以简洁明了的展示出各种源地址验证方案的技术原理及优缺点, 分别见表 4、表 5 和表 6.

4.3 源地址验证技术新进展

近些年来由于对源地址验证研究的不断深入, 开始逐渐对不同的网络环境、多元的网络应用和多样的网络威胁进行具有针对性、细致性的研究, 弥补传统验证技术的缺陷, 以使源地址验证的防御效果更加突出, 更能抵御复杂多变网络环境上的各类攻击威胁. 基于此, 产生了众多新型的源地址验证技术, 使数据源可信性研究取得新一步进展. 针对传统验证技术的存储开销问题, Vijayalakshmi 等人[66] 提出了一种新颖的增强分组标记算法, 该算法可直接部署在受害端, 以提供对单个数据包的回溯, 由于该机制不需遍历整个计算机网络或利用带外消息来识别攻击源, 使该标记算法易于应用且不具有存储开销的问题; Suresh 等人[67] 解决了 DPM 验证机制存在的可伸缩性难题, 设计出一种基于确定性多分组标记 (DMPM) 的回溯方案, 利用全局标记分发服务器 (MOD 按需标记[68]) 来标记不信任的数据包, 防御了 DDoS 攻击的威胁; 鲁宁等人[69] 提出一种基于出口过滤的层次化反匿名联盟构建方法 (EAGLE), 克服了出口过滤 (egress filtering) 和基于对等过滤的域间源地址验证方法 (MEF) 的可扩展性差、难以适应增量部署等难题; 而吴波[70] 针对分组转发中源地址与路径验证所面临的开销花费大、转发效率低等问题, 提出了基于数据包随机标记的源地址与路径高效验证机制 PPV, 依据数据流验证的角度设计了 PPV 验证机制, 通过利用数据包随机标识的安全验证, 避免了传统方案的逐跳逐包验证, 降低了分组转发验证的额外通信和验证时延的开销, 提高了分组转发安全验证的效率.

由于软件定义网络具有数据流和控制流分开的特性, 研究者一般采用其作为理想网络和验证方案的研究对象, 如陈国龙等人[71] 提出了基于 SDN 混合网络的验证方案 (SAVSH), 该方案利用 SDN 中央控制器和全局的网络拓扑, 寻找需替换 SDN 交换机的节点并部署相应的过滤规则, 动态校验数据以实现地址前缀级的来源验证; 刘冰洋等人[72] 设计出基于 SDN 的 OpenFlow 协议研究设计出了 SDN-SAVI 的应用程序, 进而对数据平面中的数据包实施 SAVI 以防御源地址欺骗的攻击行为; 张超勤等人[73] 提出基于 SDN 的集成 IP 源地址验证架构 (ISAVA), 依赖 SDN 的增量部署, 在自治域中的每个 AS 边界内部署 SDN 控制器, 通过同步数据包签名验证协议为联盟 AS 控制器间的出站数据建立凭证机制, 以实现 AS 级验证粒度, 具有低部署性高过滤性的优势; 为了克服 SDN 网络源地址验证绑定表易被伪造 AAM 破坏、缺少绑定表更新机制等安全问题, 鲁喻[74] 设计并实现了基于绑定表安全的保障方案, 利用根据主机信息构建的 AAM 验证表, 通过 AAM 验证表和路由通告对 AAM 报文进行验证, 并应用先到先服务策略 (first come first serve, FCFS) 对报文进行处理.

为了适应网络发展的需要, 对于云计算受到 DDOS 的安全威胁, 提出了基于源地址验证的防护技术, 如 Opeyemi[75] 提出了基于主机的主动和被动 OS 指纹识别的验证方法, 依据欺骗性 IP 源的 OS 与真实 IP 源的 OS 进行匹配, 实现云计算环境中 OS 指纹识别验证传入数据包的真实来源性; 由于很难追踪单个数据包的真实来源, 陈永红等人[76] 依据群集匹配追踪相似数据包群集的思想提出了基于盲目的检测方法来验证云计算的数据包真实来源, 进而设计出一种基于 K-调和均值聚类方法和改进轮廓值的新型群集匹配检测算法, 来跟踪数据包簇的真实来源.

表 4 早期重要源地址验证方案

方案类型	验证方案	方案(或技术)原理	优点	缺点
基于加密认证的验证	防欺骗方案(SPM)[26]	一种基于密钥认证的域间源地址验证方案, 通过建立自治域的安全联盟, 使在其内转发传输的数据报中添加与目的端事先协商好的密钥标识来提供数据源真实性的证明, 利用目标网络的边界路由器校验数据报的标识.	具有轻量级验证性、部署简单.	存在AS联盟成员无法区分外向内的反射式攻击的缺点.
	网络安全协议(IPsec)[25]	一种主机粒度的端到端安全认证通信协议, 首先利用ESP对传输数据的分组报文内的有效载荷进行封装, 然后对封装后的报文采用私钥签名的方法得到tag值并标记到AH认证头内, 到达目的端后进行AH认证, 保障所传数据安全性.	充分利用了封装安全有效载荷协议对数据报文内有效载荷的完整性、保密性和认证头协议的数据包的完整性、可靠性和防篡改性的特性.	由于采用逐包的加密认证方法导致计算开销庞大; 复杂的密钥管理也使该方案并不能广泛应用.
基于报文过滤的验证	网络入口过滤(NIF)[27]	一种基于路径过滤的主动入口过滤机制, 需在接入网的边界路由器上手工配置一定的访问控制策略, 形成访问控制列表(ACL)作为网络入接口的边缘过滤器, 并依据ACL可接受的地址前缀列表在网络接口处过滤入境流量.	网络路由器上的广泛部署能预防网络攻击行为.	缺少“谁部署, 谁收益”原则, 缺乏部署激励; 由于静态的ACL需要手动维护导致后期维护工作量大; 若地址前缀发生变化而忘记更新ACL可能导致数据没被接收而过滤掉.
	基于路由器的分布式包过滤 (DPF)[51]	一种源地址验证框架, 依据攻击者可向数据报中插入或删除任意的源地址信息但不能控制该报文的真实传输路径的设想, 它假设IP报文经源端发送到目的端会使用相同的传输路径, 因此AS边界路由器的每条传输链路的数据流量均需来自于固定的自治域, 任何违反此规则的数据都将被丢弃.	一种新型的源地址验证框架方案.	对于入接口的前缀信息学习和维护机制没有过多的研究.
	跳数过滤(HCF)[30]	一种基于报文传输路径长度的被动端系统防御机制, 核心思想是尽管攻击者可以伪造IP报文中的任何字段值, 但却不能伪造数据包到达目的端所经过的路径跳数, 因此可建立IP地址与路径跳数的映射表(IP2HC), 以此作为鉴别合法报文的判断依据, 再使用IP报文中的TTL值进行验证就可准确判断伪造报文进而将其过滤, 保障了传输数据的真实性.	实施复杂度较小、过滤效果较好.	在learning阶段可能受到大量数据报的冲击以绕过HCF过滤; NAT的调整可能导致IP2HC映射表信息的不准确性和路径跳数变化的可能性, 足以威胁其防御效能; 端系统后期需要维护庞大的数据库导致存储、控制开销较大, 难以广泛部署等.
基于事后追溯的验证	概率分组标记(probabilistic packet marking, PPM)[35]	一种基于路由信息的辨识攻击路径的方案, 通过数据包经路由器传输时得到的路由信息, 将部分路径信息概率性填入报文首部中(路径标记阶段), 并据此来重构攻击路径(攻击路径重组阶段), 达到溯源定位的目的.	PPM的概率标记方式给路由器减小了计算和控制开销; 压缩边分片的采样方法解决了路由器开销增大、报文空间需求增多, 可能导致产生一系列问题.	在攻击路径重构阶段需要大量报文来标记信息、运算复杂度较高、方案的健壮性不强, 并且攻击者可以通过伪造报文标记值来破坏重构过程, 进而无法识别攻击路径.
	确定性包标记(DPM)[36]	一种基于报文标记的溯源定位技术. 基本原理是当IP报文从接入子网经路由器传输进入互联网时, 边界路由器与其对应接入子网的接口对传输的IP报文进行包标记, 然后各受攻击端维护一个以源IP地址索引的入口表, 当收到一个数据包时, 检查该数据包的源IP地址是否存在于入口表中, 若存在就可获得入口地址进而转发接收数据, 否则创建并按段号区分高位段或是低位段在表中填入这一对应项.	解决了虚假标记的问题.	当黑客黑入边界路由器时可以肆意篡改正常边界路由器的包标记进而妨碍其恢复溯源路径; 或者由于报文传输时仅能标记一次, 使能重构的路径信息仅为实施标记的路由器节点, 致使因标记节点距离攻击源过远而使溯源效果并不理想, 由此导致了DPM机制的局限性.

表 5 基于 3 类验证原理方案的革新技术

序号	验证技术	应用范围	基本方法及原理	优点	缺点	改进方案
1	IEF[27, 28]	AS域间	基于端的验证方法, 包含两类验证技术. 其中Ingress Filtering 采用边界路由器检查从域外发起的报文, 而Egress Filtering采用边界路由器检查从域内发起的报文, 均可用访问控制列表实现.	防止了本自治域向外和向内的伪造报文攻击, 且两种防御机制不需域间协作.	无法识别从AS域外发送进来的伪造报文, 存在安全性缺失; 缺乏部署激励, 部署收益低, 开销较大等.	MIEF[61]不丢弃所有识别的伪造报文, 仅丢弃攻击自己和联盟的攻击报文, 并采用互助防御思想来过滤数据流量, 并采用前缀压缩算法匹配路由器资源, 提供对等端的完全保护, 降低了开销, 提高部署激励.
2	IDPF[50]		基于DPF验证框架的设计方案, 通过BGP路由信息以交换的方式来通告邻居BGP路由信息的改变, 仅需在网络边缘路由器上配置相应策略, 依据更新的路由信息可验证来自邻域的数据报是否合法.	弥补了动态网络验证的缺陷; 通过路由通告更新路由信息, 使该验证机制不再需要全局路由拓扑; 部署简单.	未能有效解决DPF推断唯一传输路径的问题, 不能过滤所有伪造报文, 效率仅为80%, 过率效果比较粗糙.	—
3	Passport[48]		采用两级的层次式验证体系结构, 既采用了IAHT方式的端到端验证, 又使用了BASE 在转发路径上的验证, 并只对所识别出的伪造报文降低转发优先级, 而并不直接丢弃伪造报文.	部署收益大, 支持增量部署, 减小了报文窃听的风险.	在路由变动时将造成一定误判; Passport的逐包计算方法过于简单, 防窃听能力不足, 若算法过于复杂, 将增大路由器压力; 报文长度增加可能引起分片.	StopIt[62]结合了Passport的验证机制, 主要利用StopIt服务器来执行过滤功能.
4	SAVE[29]		一种路由辅助通信协议, 通过在路由器上建立源地址与入接口的映射关系, 周期性更新边界路由器的映射关系变化, 不仅克服了网络路由不对称引发的问题, 又动态维护了路由映射表, 使任意报文一旦违反了SAVE策略都将被丢弃, 实现基于路由信息的匿名包过滤验证.	周期性更新边界路由器的映射关系变化, 克服了网络路由不对称引发的问题.	部署时间较长、学习路由信息过程易受攻击等.	BASE[49]通过建立源地址与标记值的映射关系表来过滤伪造报文, 由于方案对路径信息进行了标记, 因此具有很好的过滤效果, 其有效性可达90%. 并且BASE不仅比SAVE具有较小的存储开销还支持增量部署.
5	IAHT[53]		一种基于端到端的域间协作验证方法, 每对自治域之间建立安全隧道, 并使用密钥和加密算法对每个报文计算完整性的校验值, 使得对端可以检验发送者的身份.	密钥和相应的加密算法保障了隧道的完整性和不可篡改性.	由于在报文中添加一个验证头和一个新的IP头, 导致验证开销过高、且缺少高性能设备, 未广泛应用部署.	—
6	SMA[54]		一种基于状态机的包标记域间点对点源地址验证方案, 核心思想是部署该方法的AS之间形成联盟, 联盟成员通过采用动态化标记的方法来进行验证, 以达到联盟间的验证防御.	SMA修正了SPM机制中key传递机制不合理的问题, 并采用动态化标记, 使用交互状态机减少交互频率, 进而减少主动交互开销与信息量.	可扩展性低.	—
7	RISP[55]	AS域内 AS域间	采用非对称的报文标记方法, 使用Label标识对发往目的域的报文进行标记并过滤.	实现了IP欺骗报文攻击的检测和过滤机制的联合, 是一种动态的防御机制.	计算和存储开销变小, 细粒度过滤和具有较高的部署激励.	—
8	RPF[52]	AS域内	仅转发路由表信息与源地址一致的数据.	入口过滤的扩展方案.	只能用于对称路由; 受到网络拓扑的限制; 失去了控制流量的方向性.	严格的RPF使用动态ACL; 可行路径RPF添加了替代路由; 松散的RPF只检查路由是否存在; 忽略缺省路由的松散RPF利用了显式路由存在检查[56].

表 5 （续） 基于 3 类验证原理方案的革新技术

序号	验证技术	应用范围	基本方法及原理	优点	缺点	改进方案
9	uRPF[56]	AS域内	基于路由转发表信息来过滤的机制, 开启uRPF的路由设备使用其转发表(FIB)来作为判断依据.	有助于减轻网络攻击的损伤性, 弥补了RPF系列方案的缺点.	极大依赖于对称性, 在进行逆向查找时, 查询开销较大.	严格uRPF要求FIB表中去往报文源地址的接口和报文进入路由器接口必须一致; 可行路径uRPF插入最佳路径前缀和宣布路由的额外前缀; 松散uRPF仅当FIB包含一个或多个前缀时才验证通过; 虚拟路由转发技术(VRF)查询VRF而非FIB表; 增强可行路径uRPF(EFP-uRPF)利用BGP对不同接口接收的多个同源前缀进行更新[63].

表 6 SAVI 接入域源地址验证技术

序号	验证技术	基本方法及原理	优点	缺点	改进方案
1	FCFS-SAVI[57]	基于地址所有权的先来先服务原理, 以主机首次宣称的源地址为绑定锚, 根据绑定表来验证源地址的真实性.	适用无状态地址分配; 使用了邻居发现协议; 不需要更换主机, 不更改协议等.	由于状态丢失可能缺少绑定状态; 保护边界以外无法验证; 需防范DoS攻击和剩余威胁.	王卫林[64]对FCFS-SAVI的数据报文验证算法进行改进, 通过引用快速查询方法和设置标记位来提高验证速率.
2	SAVI-DHCP[58]	在SAVI交换机中启用DHCPv6 Snooping, 监控客户机行为, 完成DHCPv6建立绑定项, 并下发驱动表项以允许转发该源IPv6报文, 确保报文合法性.	针对纯DHCP方案设计和允许DHCP分配地址; 验证安全依赖现有可用协议, 不需定义新协议; 实行源控制, 确保数据合法性等.	数据监听过程代价高昂; 若客户不响应检测探针可能会设置不正确的绑定; 绑定过多可能增加开销或存在绑定数限制等.	蒋雅兰[65]对SAVI-DHCP的CGA签名算法进行了优化, 加快IP地址的生成速率, 弥补了安全性和时间性的缺点.
3	SAVI-SEND[59]	基于SEND协议的细粒度验证方案, 利用SEND协议的DAD邻居请求、DAD邻居广告、NUD邻居请求和NUD邻居广告4个消息内容来配合验证节点, 通过验证源IPv6与端口绑定一致性来鉴别数据真实性. (DAD为重复地址检测; NUD为邻居不可访问性检测)	强化了地址所有权的能力, 弥补入口过滤的不足, 并且可以预防离线IPv6数据的伪造等.	需要防止重放攻击和DoS攻击等.	—
4	SAVI-MIX[60]	该方案可支持多种验证方案, 根据绑定锚的生成算法仲裁出无冲突性的绑定表来进行验证.	使FCFS-SAVI、SAVI-DHCP和SAVI-SEND三种验证技术在网络中混合使用时避免冲突性.	启用SAVI绑定设置率可能增加对DoS攻击的敏感性; SAVI-MIX支持多种验证方法, 可能降低其安全级别.	—

综上所述, 源地址验证研究随网络的不断发展而进一步深入, 逐渐从传统网络环境转变到现有网络环境中, 产生了基于软件定义网、云计算等新型验证防御技术.

4.4 源地址验证方案演进趋势

根据第 4.2、4.3 节对源地址验证技术的介绍, 通过对各类验证技术的汇总, 介绍相关验证方案的最新进展有益于勾勒出源地址验证技术的发展脉络, 并绘制出验证方案的演进知识图谱, 见图 11. 在图中可清晰看出在源地址验证研究的发展过程中, 验证方案的三类设计理念一直贯穿于该领域的研究中. 基于此, 大批专家学者致力于这些验证技术的深入研究, 希望探寻出更为合理的验证方案, 经过不懈努力 SAVA、SAVI 协议相继出现, 使该研究领域迈入了新时代, 能更科学、更微观、更系统的进行研究, 设计出更先进的源地址验证技术, 为下一代网络的安全发展保驾护航.

4.5 研究挑战与机会

现有源地址验证为代表的网络安全防御技术能够识别和过滤非法数据包、溯源追踪恶意节点, 在一定程度上确保了数据传输过程的安全性, 但在高效性、鲁棒性和部署激励等方面具有些许挑战:

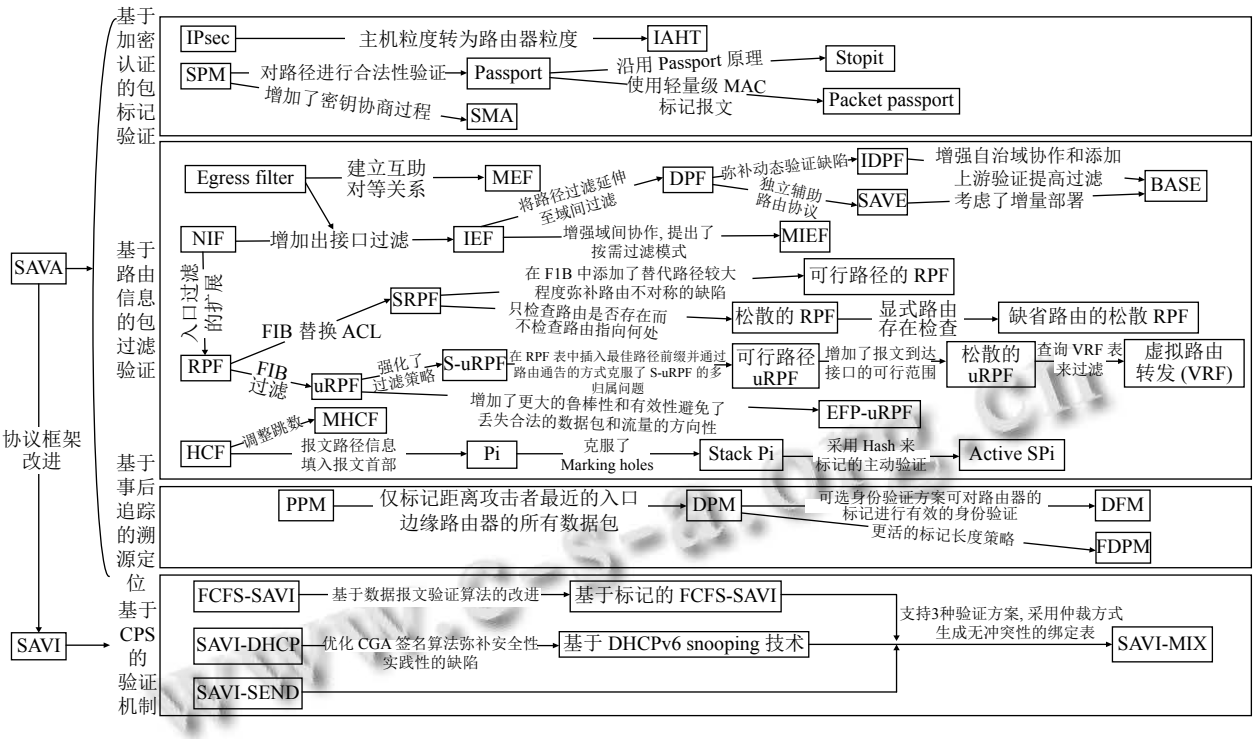

图 11 源地址验证技术进化导向图

(1) 基于加密验证的源地址验证方案不可避免地引入了身份验证标识, 这毫无疑问会造成极大的网络开销, 占用一定的带宽资源, 随之会影响数据包的传输效率, 并且加密验证方案多数采用端验证方式, 缺少在数据传输路径上的验证机制. 即使采用了全路径传输的验证机制也势必会产生极大的计算开销和验证开销. 因此对于源地址路径传输的验证机制开始逐渐着眼于在网络数据传输路径上的关键节点处进行源地址验证, 其中网络数据传输关键节点的识别与关键节点上的源地址验证机制的配合是现在较为棘手的难题.

(2) 基于报文过滤的验证方案现在多采用不同的过滤准则作为访问控制列表的准入策略, 利用路由器对数据包进行过滤验证. 由于该验证方案非常依赖于数据传输过程中的所有全局的网络拓扑信息, 因此在网络拓扑发生变化时会过滤掉部分合法数据包, 导致误判增多. 同时部分验证技术仅具有单向防御能力, 而无法及时阻止来自网络内部的非法数据, 导致防御能力大大降低, 只能做到地址前缀级别的安全防护.

(3) 基于事后追踪的验证方案一般使用边界路由器对传输数据包按照概率进行标记, 在端系统受到攻击后, 利用标记的数据报文和路由器记载的数据传输日志, 对攻击端进行溯源定位, 以追击攻击者实施攻击的真实位置. 但由于溯源定位所需标记数据量极多和溯源追踪算法复杂, 容易大量占用网络资源. 并且该验证方案易受到中间路由节点的恶意干扰, 可能造成溯源定位精度降低、验证机制的可用性变差等, 进而无法实现对发动源地址欺骗与路径篡改等网络威胁的攻击位置准确定位, 其安全防御能力有待进一步提升.

(4) 面临的其他挑战, 如源地址验证方案部署的扩展性问题、集中式激励机制的单点故障威胁问题、难以适应拓扑动态变化的灵活性问题、验证方案的实现困难问题等. 面对上述的种种问题, 在前期部署时应采取“谁部署谁受益”的激励机制和循序渐进的部署原则. 在部署验证方案的前期应该采用最少的部署工作量, 获得了最大的收益时, 而后在进行增量部署, 以达到接近百分百的验证防御效果.

为了解决上述难题和挑战, 科研人员开始逐渐应用 SDN 网络来设计实现源地址验证方案. 因为 SDN 网络将数据流和控制流分开形成了 SDN 网络的数据平面和控制平面, 打破了常规网络的体系架构, 且实现源地址验证的方案可以基于 SDN 的控制器和 OpenFlow 协议来设计, 同时开源了南向和北向的 API 接口, 为源地址验证方案的实现提供了便利条件. 在近 5 年的源地址验证研究中, 大多数科研院所多采用 SDN 来设计

和实现了源地址验证方案, 并对各验证方案进行了对比分析. 虽然利用 SDN 网络为源地址验证提供便利条件, 但也产生了些许难题, 如在规模较大的网络拓扑中控制器主动探测发现异常主机时, 会对相应的主机端口持续进行源地址验证, 导致验证延时过大, 致使网络的安全性有所降低; 控制器对所有传输设备进行数据采集时, 进而对大量数据进行异常检测可能加重控制器的处理负担; 通过设定丢包率和流量阈值来判定异常主机时, 阈值的设定不好控制等. 综上所述, 利用 SDN 网络对于网络数据地址真实可信性研究起着重要的启程转折作用, 为使用传统网络架构进行源地址验证研究提供了一条新的、可行的研究途径.

5 结束语

本文通过对中国知网数据库 CNKI 近 20 年来发表的基于源地址验证研究的论文进行文献统计、可视化分析和归纳整理, 旨在帮助科研人员了解源地址验证研究领域目前在国内的研究现状、研究主题及研究热点, 并通过文献计量学和科学知识图谱的方法, 采用 CiteSpace 可视化工具进行科学性分析, 挖掘出源地址验证研究的核心力量, 包括核心作者及重要科研机构, 并勾勒出源地址验证研究热点的热度轨迹, 以进一步总结该研究领域的发展演化趋势. 为科研人员把握源地址验证研究的未来科研方向提供科学的借鉴依据, 进而不断深入探索, 为将来网络数据的安全性传输保驾护航.

参考文献

1 任罡, 段海新. 973 计划“新一代互联网体系结构理论研究”项目之课题四真实 IPv6 源地址寻址体系结构研究. 中国教育网络, 2007, (5): 26–27.

2 吴建平, 吴茜, 徐恪. 下一代互联网体系结构基础研究及探索. 计算机学报, 2008, 31(9): 1536–1548.

3 吴建平, 任罡, 李星. 构建基于真实 IPv6 源地址验证体系结构的下一代互联网. 中国科学 (E 辑: 信息科学), 2008, 38(10): 1583–1593.

4 毕军, 吴建平, 程祥斌. 下一代互联网真实地址寻址技术实现及试验情况. 电信科学, 2008, (1): 11–18.

5 姚广, 毕军. 互联网中 IP 源地址伪造及防护技术. 电信科学, 2008, 24(1): 26–32.

6 徐恪, 朱亮, 朱敏. 互联网地址安全体系与关键技术. 软件学报, 2014, 25(1): 78–97. [doi: 10.13328/j.cnki.jos.004509]

7 贾溢豪, 任罡, 刘莹. 互联网自治域间 IP 源地址验证技术综述. 软件学报, 2018, 29(1): 176–195. [doi: 10.13328/j.cnki.jos.005318]

8 黄雪娟, 刘金硕, 姚昱. 基于知识图谱的智群计算国内外研究可视化分析. 计算机应用与软件, 2019, 36(12): 72–80.

9 王晓慧. 我国智慧图书馆研究现状与问题——基于 CNKI 文献计量分析. 高校图书馆工作, 2020, 40(2): 7–13.

10 Chen CM, Song M. Visualizing a field of research: A methodology of systematic scientometric reviews. PLoS One, 2019, 14(10): e0223994. [doi: 10.1371/journal.pone.0223994]

11 何鑫, 陈卓, 田丽慧. 2000—2018 年乡村教师队伍建设研究热点与演化趋势研究——基于 CNKI 核心期刊的统计实践探析. 技术经济, 2020, 39(4): 154–163.

12 冯明, 高宇, 房成镇. 帧中继网络的管理. 通信学报, 1997, 18(12): 40–46.

13 盛焕烨, 王珏. 网络安全攻防对策综述. 上海交通大学学报, 1997, 31(8): 85–90.

14 王常杰, 秦浩, 王育民. 基于 IPv6 的防火墙设计. 计算机学报, 2001, 24(2): 219–223.

15 吴建平, 任罡, 李星. IPv6 网络自治系统间源地址验证技术研究. 中国科技论文在线, 2007, 2(10): 715–719.

16 Wu JP, Bi J, Li X, *et al*. A source address validation architecture (SAVA) testbed and deployment experience. IETF. RFC 5210, 2008.

17 Wu JP, Bi J, Bagnulo M, *et al*. Source address validation improvement (SAVA) framework. IETF. RFC 7039. 2013.

18 姜金川, 王冲. 基于学习自动机和用户兴趣的 PageRank 算法研究. 计算机工程与应用, 2020, 56(3): 80–85.

19 吴建平, 刘莹, 吴茜. 新一代互联网体系结构理论研究进展. 中国科学 (E 辑: 信息科学), 2008, 38(10): 1540–1564.

20 孙长华, 刘斌. 分布式拒绝服务攻击研究新进展综述. 电子学报, 2009, 37(7): 1562–1570.

21 毕军. SDN 体系结构与未来网络体系结构创新环境. 电信科学, 2013, 29(8): 6–15.

22 戴彬, 王航远, 徐冠, 等. SDN 安全探讨: 机遇与威胁并存. 计算机应用研究, 2014, 31(8): 2254–2262.

23 李福亮, 杨家海, 吴建平, 等. 互联网自动配置研究. 软件学报, 2014, 25(1): 118–134. [doi: 10.13328/j.cnki.jos.004458]

24 胡光武, 陈文龙, 徐恪. 一种基于 IPv6 的物联网分布式源地址验证方案. 计算机学报, 2012, 35(3): 518–528.

25 Kent S, Seo K. Security architecture for the internet protocol. IETF. RFC 4301. 2005.

26 Bremler-Barr A, Levy H. Spoofing prevention method. Proceeding of the 24th Annual Joint Conference of the IEEE

Computer and Communications Societies. Miami: IEEE, 2005. 536–547.
27 Ferguson P, Senie D. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. IETF. RFC 2827. 1997.
28 Liu BY, Bi J, Vasilakos AV. Toward incentivizing anti-spoofing deployment. IEEE Transactions on Information Forensics and Security, 2014, 9(3): 436–450. [doi: 10.1109/TIFS.2013.2296437]
29 Li J, Mirkovic J, Wang MQ, *et al*. SAVE: Source address validity enforcement protocol. 21st Annual Joint Conference of the IEEE Computer and Communications Societies. New York: IEEE, 2002. 1557–1566. [doi: 10.1109/INFCOM.2002.1019407]
30 Jin C, Wang HN, Shin KG. Hop-count filtering: An effective defense against spoofed DDoS traffic. Proceedings of the 10th ACM Conference on Computer and Communications Security. Washington, DC: ACM, 2003. 30–41.
31 Dou WC, Qi C, Chen JJ. A confidence-based filtering method for DDoS attack defense in cloud environment. Future Generation Computer Systems, 2013, 29(7): 1838–1850.
32 Park K, Lee H. On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internets. ACM SIGCOMM Computer Communication Review, 2001, 31(4): 15–26.
33 Sultana S, Nasrin S, Lipi FK, *et al*. Detecting and preventing IP spoofing and Local Area Network Denial (LAND) attack for cloud computing with the modification of Hop Count Filtering (HCF) mechanism. 2019 International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2). Rajshahi: IEEE, 2019. 1–6.
34 Snoeren AC, Partridge C, Sanchez LA, *et al*. Hash-based IP traceback. ACM SIGCOMM Computer Communication Review, 2001, 31(4): 3–14.
35 Savage S, Wetherall D, Karlin A, *et al*. Network support for IP traceback. IEEE/ACM Transactions on Networking, 2001, 9(3): 226–237.
36 Belenky A, Ansari N. IP traceback with deterministic packet marking. IEEE Communications Letters, 2003, 7(4): 162–164.
37 Xiang Y, Zhou WL, Guo MY. Flexible deterministic packet marking: An IP traceback system to find the real source of attacks. IEEE Transactions on Parallel and Distributed Systems, 2009, 20(4): 567–580.
38 Aghaei-Foroushani V, Zincir-Heywood A. IP traceback through (authenticated) deterministic flow marking: An empirical evaluation. EURASIP Journal on Information Security, 2013, 2013: 5. [doi: 10.1186/1687-417X-2013-5]
39 冉华, 钟娅. 数字出版研究的学术脉络与前沿热点——基于 Web of Science 数据库 (1998—2018) 的可视化分析. 出版科学, 2020, 28(3): 101–107.
40 陈显友. 基于 Citespace 文献计量软件的养老服务供需研究现状与热点分析. 社会科学家, 2020, (1): 35–42.
41 赵亮, 许娜, 张维. 我国数字孪生研究的进展、热点和前沿——基于中国知网核心期刊数据库的知识图谱分析. 实验技术与管理, 2021, 38(11): 96–104.
42 王金丽, 樊勇, 张辉. 区块链文献主题发现及演化研究. 计算机工程与应用, 2020, 56(20): 1–8.
43 管文玉, 凌卫青. 基于文献计量的数字孪生研究可视化知识图谱分析. 计算机集成制造系统, 2020, 26(1): 18–27.
44 傅游, 王浩蓉. 基于 Web of Science 的国际区块链技术文献计量分析. 图书情报导刊, 2020, 5(12): 67–75.
45 刘辉, 康文彦. 国内深度学习研究的知识图谱——基于 381 篇中文核心期刊论文的可视化分析. 教育理论与实践, 2020, 40(1): 50–55.
46 翁晓梅. 基于 CiteSpace 可视化分析的移动语言学习发展研究. 西安外国语大学学报, 2020, 28(3): 70–75, 102.
47 徐玉华, 孙知信. 软件定义网络中的异常流量检测研究进展. 软件学报, 2020, 31(1): 183–207. [doi: 10.13328/j.cnki.jos.005879]
48 Liu X, Li A, Yang XW, *et al*. Passport: Secure and adoptable source authentication. Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation. San Francisco: USENIX Association, 2008. 365−378.
49 Lee H, Kwon M, Hasker G, *et al*. BASE: An incrementally deployable mechanism for viable IP spoofing prevention. Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security. Singapore: Association for Computing Machiner, 2007. 20–31.
50 Duan Z, Yuan X, Chandrashekar J. Constructing inter-domain packet filters to control IP spoofing based on BGP updates. Proceeding IEEE INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Barcelona: IEEE, 2007. 1–12.
51 鲁宁. 攻击源追踪及攻击流过滤方法研究 [博士学位论文]. 北京: 北京邮电大学, 2013.
52 Wijnands IJ, Boers A, Rosen E. The reverse path forwarding (RPF) vector TLV. IETF. RFC 5496. 2009.

53 Kent S, Atkinson R. IP authentication header. IETF. RFC 2402. 1998.
54 于凤国. IPv6 自治域间源地址认证方案在边界路由器上的设计与实现 [硕士学位论文]. 北京: 北京邮电大学, 2015.
55 吕高锋, 孙志刚, 卢锡城. 域间 IP 欺骗防御服务净化机制. 计算机学报, 2009, 32(3): 552–563.
56 Baker F, Savola P. Ingress filtering for multihomed networks. IETF. RFC 3704. 2004.
57 Nordmark E, Bagnulo M, Levy-Abegnoli E. FCFS SAVI: First-Come, first-served source address validation improvement for locally assigned IPv6 addresses. IETF. RFC 6620. 2012.
58 Bi J, Wu JP, Yao G, *et al*. Source address validation improvement (SAVI) solution for DHCP. IETF. RFC 7513. 2015.
59 Bagnulo M, Garcia-Martinez A. Secure neighbor discovery (SEND) source address validation improvement (SAVI). IETF. RFC 7219. 2014.
60 Bi J, Yao G, Halpern J, *et al*. Source address validation improvement (SAVI) for mixed address assignment methods scenario. IETF. RFC 8074. 2017.
61 刘冰洋. 互联网域间源地址验证的可部署性评价模型与方法设计 [博士学位论文]. 北京: 清华大学, 2014.
62 Liu X, Yang XW, Lu YB. To filter or to authorize: Network-layer DoS defense against multimillion-node botnets. ACM SIGCOMM Computer Communication Review, 2008, 38(4): 195–206.
63 Sriram K, Montgomery D, Haas J. Enhanced feasible-path unicast reverse path forwarding. IETF. RFC 8704. 2020.
64 王卫林. 基于无状态地址自动配置的 FCFS SAVI 研究 [硕士学位论文]. 沈阳: 辽宁大学, 2012.
65 蒋雅兰. 基于 SAVI 技术的安全 DHCPv6 系统研究 [硕士学位论文]. 北京: 北京交通大学, 2014.
66 Vijayalakshmi M, Nithya N, Shalinie SM. A novel algorithm on IP traceback to find the real source of spoofed IP Packets. In: Suresh LP, Dash SS, Panigrahi BK, eds. Artificial Intelligence and Evolutionary Algorithms in Engineering Systems. New Delhi: Springer, 2015. 79–87.
67 Suresh S, Ram NS. Feasible DDoS attack source traceback scheme by deterministic multiple packet marking mechanism. The Journal of Supercomputing, 2020, 76(6): 4232–4246.
68 Yu S, Zhou WL, Guo S, *et al*. A feasible IP traceback framework through dynamic deterministic packet marking. IEEE Transactions on Computers, 2016, 65(5): 1418–1427.
69 鲁宁, 李峰, 王尚广, 等. 层次化反匿名联盟构建方法. 软件学报, 2019, 30(9): 2791–2814. [doi: 10.13328/j.cnki.jos.005517]
70 吴波. 面向分组转发全过程的安全增强技术研究 [博士学位论文]. 北京: 清华大学, 2019.
71 Chen GL, Hu GW, Jiang Y, *et al*. SAVSH: IP source address validation for SDN hybrid networks. 2016 IEEE Symposium on Computers and Communication (ISCC). Messina: IEEE, 2016. 409–414.
72 Liu BY, Bi J, Zhou Y. Source address validation in software defined networks. Proceedings of the 2016 ACM SIGCOMM Conference. Florianopolis: ACM, 2016. 595–596.
73 Zhang CQ, Hu GW, Chen GL, *et al*. Towards a SDN-based integrated architecture for mitigating IP spoofing attack. IEEE Access, 2017, 6: 22764–22777.
74 鲁喻. SDN 网络中 IPv6 源地址验证绑定表的安全问题研究 [硕士学位论文]. 武汉: 华中科技大学, 2019.
75 Osanaiye OA. Short paper: IP spoofing detection for preventing DDoS attack in cloud computing. 2015 18th International Conference on Intelligence in Next Generation Networks. Paris: IEEE, 2015. 139–141.
76 Chen YH, Chen X, Tian H, *et al*. A blind detection method for tracing the real source of DDoS attack packets by cluster matching. Proceeding of the 8th IEEE International Conference on Communication Software and Networks. Beijing: IEEE, 2016. 551–555.