软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2018,29(11):3554−3574 [doi: 10.13328/j.cnki.jos.005330]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

可动态扩展的高效单包溯源方法*

鲁 宁[1,2], 王尚广[2], 李 峰[1], 史闻博[1], 杨放春[2]

[1](东北大学 信息科学与工程学院,辽宁 沈阳 110819)

[2](网络与交换技术国家重点实验室(北京邮电大学),北京 100876)

通讯作者: 王尚广, E-mail: sgwang@bupt.edu.cn

摘 要: 由于能够隐藏攻击位置、避开攻击过滤、窃取用户隐私和增强攻击危害,IP 匿名已被各类网络攻击广泛使用并造成极大的危害.为此,研究者们提出了 IP 溯源——一种能够在匿名攻击发生后揭露攻击主机身份的追踪技术.鉴于已有的 IP 溯源研究在面对大规模网络时存在扩展性差、处理开销大、拓扑隐私泄露等问题,提出了一种可动态扩展的高效单包溯源方法,简称 SEE.该方法采用域间和域内相分离的层次化系统架构模型来弱化自治域之间的溯源联系、避免拓扑隐私泄露,并通过域内溯源网络构建、域内溯源地址分配、域内路径指纹建立和提取、域间反匿名联盟构建和域内到域间的平稳过渡等策略来改善系统的扩展性和处理开销.通过理论分析和基于大规模真实和人工互联网拓扑的仿真实验,结果表明,相对于以往方案,SEE 在高效性和扩展性方面确实有了很大的改善.

关键词: 网络安全;拒绝服务攻击;IP 匿名;IP 溯源;单包溯源

中图法分类号: TP393

中文引用格式: 鲁宁,王尚广,李峰,史闻博,杨放春.可动态扩展的高效单包溯源方法.软件学报,2018,29(11):3554−3574. http://www.jos.org.cn/1000-9825/5330.htm

英文引用格式: Lu N, Wang SG, Li F, Shi WB, Yang FC. Dynamically scalable and efficient approach for single-packet traceback. Ruan Jian Xue Bao/Journal of Software, 2018,29(11):3554−3574 (in Chinese). http://www.jos.org.cn/1000-9825/5330.htm

Dynamically Scalable and Efficient Approach for Single-Packet Traceback

LU Ning[1,2], WANG Shang-Guang[2], LI Feng[1], SHI Wen-Bo[1], YANG Fang-Chun[2]

[1](College of Information Science and Engineering, Northeastern University, Shenyang 110819, China)

[2](State Key Laboratory of Networking and Switching Technology (Beijing University of Posts and Telecommunications), Beijing 100876, China)

Abstract: IP spoofing, as a trick that can conceal the attackers' location, bypass the attack prevention, gather the confidential information and enhance the destructive power, has been prevalent in the current network attacks to further bring about severe damage to the Internet. For this reason, the IP traceback technology that can trace an individual attack packet to its origin and then disclose the attacker identity has been extensively researched and developed. Although the existing research can achieve the purpose of tracking to some extent, they also suffer from the following disadvantages: the leakage of topology privacy, the lack of scalability and the higher processing overhead. To tackle those issues, this paper proposes a dynamically scalable and efficient approach for single-packet IP traceback, termed as SEE. SEE first designs the hierarchical traceback system architecture to weaken the traceability relationships among the autonomous domains, and then employs the intra-AS traceback network construction based on OSPF, the traceback address

* 基金项目: 国家自然科学基金(61601107, 61402094, 61472074); 河北省自然科学基金(F2015501122); 辽宁省科研博士启动基金(F201501143)

Foundation item: National Natural Science Foundation of China (61601107, 61402094, 61472074); Natural Science Foundation of Hebei Province (F2015501122); Doctoral Scientific Research Foundation of Liaoning Province (F201501143)

收稿时间: 2016-11-11; 修改时间: 2017-01-16; 采用时间: 2017-07-13; jos 在线出版时间: 2018-04-27

CNKI 网络优先出版: 2018-04-27 14:58:00, http://kns.cnki.net/kcms/detail/11.2560.TP.20180427.1457.001.html

assignment based on edge-coloring, path fingerprint establishment and extraction based on link-binding, the anti-spoofing alliance establishment based on peer-peer relationship and the stable transition process from intra AS to inter AS to improve the scalability and cut down the processing overhead. Extensive mathematical analysis and simulations are performed to evaluate our approach. The results show that the proposed approach significantly out per forms the prior approaches in terms of the scalability and high-efficiency.

Key words: network security; DoS attacks; IP spoofing; IP traceback; single-packet traceback

2016 年 10 月 22 日发生的美国互联网大规模瘫痪事件表明:一方面,物联网的兴起使得攻击者能够直接利用数目众多且成本较低的智能接入设备发起各种以欺骗、恶意破坏等为目的的网络攻击;另一方面,当前网络系统的安全机制较为薄弱,系统性不强,更缺乏追凶问责的职能[1].在众多网络安全问题中,“IP 匿名”无疑是制约互联网发展的最严重安全隐患之一.一系列臭名昭著的网络攻击,包括 SMURF 攻击、源路由选择欺骗攻击(source routing spoofing)以及造成此次美国互联网瘫痪的同步包风暴攻击(SYN flooding)和 DNS 放大攻击(DNS amplification),都会依赖“IP 匿名”来隐藏攻击位置、避开攻击过滤、窃取用户隐私和增强攻击危害.因此,如何高效防御 IP 匿名,已经成为保证国家经济健康发展的重要问题.

反匿名方法按照动作发生的时间可划分为以下 3 类:预防、缓解和响应[2],其中,

- 预防主要通过改良当前互联网无认证缺陷来避免网络匿名活动的发生,其代表性技术主要包括源地址认证,通常更适合下一代可信网络的建设.
- 缓解则利用当前网络已形成的源-目的约束(例如前缀与子网捆绑、路由对称性等),在中间转发节点上事先建立一套 IP 包过滤规则,尽可能多地阻止匿名包抵达受害者,代表性技术包括出口边界过滤和域间路由过滤.然而,少量但不可忽视的非常规源-目的约束(例如子网内欺骗、非对称路由等)和源路由欺骗的存在使得缓解技术无法彻底根除匿名包.
- 响应则作为一种补充手段,通过弥补当前互联网无状态的不足,使得受害者即使在遭到匿名攻击后也能揭露攻击主机身份,对其进行阻断,与之对应的技术称为 IP 溯源,本文主要关注该类技术:首先,唯一能够阻止攻击者再次犯罪的方法就是抓住他,让他接受法律制裁;其次,网络取证是反网络犯罪法成功建立的重要环节,而溯源正好为实现网络取证提供了所急需的指纹数据;然后,随着带宽消耗型攻击的流行,在靠近攻击源的位置阻断攻击流,能够很好地避免它们在受害者附近聚集;最后,溯源结果能够帮助互联网建立信誉等级,例如,依据攻击主机数量评估所有自治域的信誉度,对于等级较低的自治域,其他自治域可以采用限速或限行的 BGP 路由策略,激励它们清理各自的管辖地区,确保整个网络的清洁.因此,对于受害者和网络服务提供商(Internet service provider,简称 ISP)来说,能够准确地识别出攻击源具有重大战略意义.

虽然 IP 包头的源地址和源站选项字段是虚假的,但是它必会被攻击者到目标机之间的中间路由节点转发,因此整个传输路径是真实的.受此启发,IP 溯源研究就是借助路由器处理 IP 包的契机来建立路径片段信息,以便在攻击发生后能够重构攻击路径.一直以来,国内外绝大部分溯源研究[3,4]都针对高速匿名攻击,然而近来随着低速匿名攻击(例如 LDoS、Ping-of-Death 等)的兴起与泛滥,可同时兼顾高速和低速攻击向量的基于图着色理论的单包溯源开始渐受关注[5−10].为了能够利用单个攻击样本包进行追踪,使溯源系统具备识别多种攻击类型的能力,该技术的基本解决思路是:在已有物理网络上建立一个由溯源路由器(具备路径片段标记和记录功能的路由器)组成的逻辑网络(称为溯源网络),并采用 2-距离点着色理论为溯源网络节点重新编址,以较短的溯源地址来取代冗长的 IP 地址.当 IP 包在溯源网络上传播的时候,转发节点采用边标记边记录的交叉方法来建立路径指纹;当攻击发生后,ISP 通过识别和收集中间节点的指纹信息就可重构出攻击路径.尽管已有一些研究分别在降低溯源开销、减小路径回溯时间以及增强溯源精度等方面取得了一定效果,但是在面对大规模网络时,它们的系统结构扁平化、颜色复用率过低、不支持节点动态加入以及路径指纹建立低效等特性,给互联网安全管理平台带来新的挑战.

- 首先,系统结构扁平化意味着溯源管理粒度较为单一,也就要求自治域之间必须无缝合作,这不仅与当前大规模网络的多极化管理模式相冲突,而且还会造成网络拓扑隐私泄露,阻碍溯源系统规模扩展.例

如,已有方法不分域间和域内,统一管理所有溯源路由器,这无疑忽略了不同自治域(特别是配置了不同策略的自治域,包括安全策略、路由策略等)中路由器行为的差异性,而且在路径重构过程中,会把经过域的网络拓扑泄露给受害域.

- 其次,不支持节点实时加入意味着溯源网络无法动态扩展,一旦溯源系统启动后,如果有溯源路由器申请加入或者退出,那么只能关闭系统,重新部署溯源服务后再启动.例如,已有的方法只支持静态部署,无法及时感知发现新增或失效的溯源节点,造成维护成本高且容错性差,进而制约了溯源系统的扩展性.
- 然后,颜色复用率越低意味着溯源地址越长,这既会增加单个路径指纹的空间占用量,又因标记空间利用率降低而加大指纹记录频率.在这种情形下,传播路径越长,溯源系统的整体开销就越大.例如,标记空间通常只有16位,然而已有方法的溯源地址长度为12位,这就要求每隔一跳就得执行一次指纹记录操作.在大规模网络下,IP包的传播路径必然较长,从而造成较大的系统整体开销.
- 最后,路径指纹建立低效会造成溯源路由器存储资源不足,使得它只能以损失溯源精度的方式来换取存储资源.例如,已有的方法通过在溯源路由器上记录转发包或底层路由特征来建立路径指纹,使得溯源路由器的存储开销与底层网络规模呈正比.一旦网络规模超过某个阈值,造成存储资源不足,为了保证溯源系统正常运行,溯源路由器不得不采用交替覆盖或数据压缩来记录指纹痕迹,使得大量攻击源被遗漏而正常源被误认.

针对上述挑战,本文提出了一种可动态扩展的高效单包溯源方法(scalable and efficient approach for single-packet IP tracEback,简称SEE).该方法遵循功能性内聚和自主合作的原则,采用域内响应、域间过滤的层次化系统架构模型来弱化自治域之间的溯源联系,避免经过域的拓扑隐私泄露.在域内网络中,首先通过重定义OSPF协议的链路状态通告类型来构建溯源网络,在降低网络建立开销的同时,又可利用OSPF更新过程收敛快的特点实现溯源系统的动态扩展;然后,鉴于边着色与2-距离点着色虽然标识作用相同,但前者颜色复用率更高的特点,采用边着色理论为溯源地址分配策略,提升标记空间利用率;最后,利用匿名包样式虽然繁多,但是上下游溯源链路却相对稳定的特点,通过基于链路绑定的路径指纹建立策略,使得存储开销只与溯源虚拟路径有关,而与底层网络的路由路径或转发包数量无关,从而降低了溯源存储开销.在域间网络中,通过采用基于对等关系的出口边界过滤策略来构建以Stub域为基本单元、可激励部署的反匿名联盟,使得域间网络传播的所有IP包都载有可信的网络前缀,从而不经过路径重构就能出识别攻击域.此外,通过在边界路由器的溯源转发表中添加成员域指纹信息,避免因非联盟成员伪造成员域地址而造成攻击域误报,实现域内到域间溯源的平稳过渡.

为了验证本文提出的SEE方法,首先对其高效性和扩展性进行了理论分析,然后在基于大规模人工和真实互联网拓扑的攻击场景中对其进行了实验验证,并与其他经典方法进行了对比.结果表明:SEE方法不仅实现了溯源系统的动态扩展以及拓扑隐私的保护,而且极大地降低溯源开销,其中,溯源路由器的存储开销能够降低到一个固定值0.18MB,在全网部署情况下,几乎不会发生溯源误报和漏报,路径重构开销降低为原来一半.

本文第1节介绍本文提出的SEE方法,其中,第1.1节给出方法的整体框架,第1.2节~第1.6节分别给出域内溯源网络构建、溯源地址分配、路径指纹建立和提取、域间反匿名联盟构建、域内到域间溯源的平稳过渡等设计细节.第2节对方法的性能进行评估,其中,第2.1节给出理论评估,第2.2节则采用实验仿真手段对分析结果进行补充.第3节在介绍相关工作的同时阐明本文的主要贡献.第4节总结全文并指出下一步的工作重点.

1 一种可动态扩展的高效单包溯源方法

与传统方法不同[5−10],本文提出的SEE方法采用域间和域内相分离的层次化系统架构模型,其中,域间网络通过反匿名联盟的构建,使网络服务提供商直接利用攻击包源地址中网络前缀就可定位出攻击域,无需路径重构;域内网络则通过构建溯源覆盖网络以及路径指纹库,使网络服务提供商以攻击路径重构来定位攻击者.

1.1 整体框架

在大规模网络环境下,已有的研究为了追踪攻击源,会把经过域的拓扑结构泄露给受害域.然而,网络拓扑

属于敏感数据,恶意用户利用它能够轻易找到网络的脆弱节点,增加攻击成功率.因此,如何在不影响网络拓扑隐私的前提下实现溯源是非常重要的.IP 溯源的目的是帮助受害者确定攻击源,而路径重构属于它的非功能性需求.以此为出发点,本文以常见的Transit-Stub互联网拓扑模型为基础,综合分析攻击路径上不同边界节点的表现特征,遵循功能性内聚和自主合作的原则,全面权衡溯源过程中域内与域间行为的相关性和特异性,提出一种以域内溯源为核心、辅以域间匿名过滤的可隐藏域间网络拓扑的跨域单包溯源架构,通过分解溯源过程,弱化自治域之间耦合性,达到分阶段管理、灵活控制的目的.在 Stub 域内,我们采用基于图着色理论的单包溯源技术来实现匿名包追踪:首先,以底层路由网络为基础,通过着色方法对溯源节点(即具备溯源功能的路由器)重新编址以及交换邻居溯源节点信息来生成溯源虚拟网络;然后,在该网络上提取和记录转发包的逻辑链路特征来建立路径指纹,以便在攻击发生后可及时收集和整理它们,还原攻击路径.本文将具备溯源功能的 Stub 域称为溯源 Stub 域,所有溯源 Stub 域构成反匿名联盟.在由 Transit 域构成的域间网络内,我们采用已商业化的出口边界过滤技术来完成匿名包清理:首先,在溯源 Stub 域的边界路由器上配置出口边界过滤规则;然后对每个到达边界节点且准备转送出去的 IP 包都率先进行进行检查,如果发现它的源地址不属于本网络范围则选择丢弃,反之正常转发.整个净化过程无需中间 Transit 域的参与,因此在攻击发生后,我们可以在不泄露网络拓扑隐私的前提下完成攻击域的快速定位.假设某溯源 Stub 域的网络前缀为 AS_prefix,路由器 R_1 是该域的边界节点,为了阻止它的匿名包流入域间网络,需要配置以下过滤规则:(1) permit AS_1_prefix any;(2) deny any any.其中,第 1 条表明,只允许源地址属于该 Stub 域的 IP 包通过;第 2 条表明,凡是不满足第 1 条的 IP 包都将被丢弃.

在本文所提的跨域溯源架构中,如图 1 所示,它的溯源功能实体主要包括溯源路由器和过滤边界路由器,前者负责提取路径指纹和构建域内溯源网络,后者负责过滤匿名包.此外,该架构还包括两个管理功能实体:溯源管理器和反匿名联盟管理器.前者主要功能包括:(1) 接收和发起域内溯源任务;(2) 分配溯源地址;(3) 获取溯源网络与底层路由网络的映射关系;4) 向过滤边界路由器下发过滤规则.后者主要功能包括:(1) 维护联盟成员域网络前缀列表;(2) 接受和发起域间溯源任务.按攻击源位置不同,匿名攻击可源于受害域本身,也可源于其他 Stub 域.但无论属于哪种,匿名包源地址都不会受到任何约束.也就是说:就域内攻击来说,它的源地址可隶属于其他 Stub 域;而就域外攻击来说,其源地址也可隶属于受害域.当攻击发生后,受害者首先利用入侵检测技术[11]来识别匿名包,然后以此为样本提取指纹、重构路径.以图 1 为例,在该跨域溯源架构下,路径重构过程可描述如下:无论匿名包中源地址是多少,受害域 AS_2 的溯源管理器都会发起域内溯源请求,通过提取溯源网络上的路径指纹信息来还原该包在本域的转发路径,进而确定入口路由器位置(如何从入口路由器追踪定位到僵尸主机,这属于链路层的溯源技术,并不在本文研究范围),若入口路由器不是边界过滤路由器,就可认为该攻击属于域内攻击,溯源任务结束;反之,则是域外攻击,在此情形下,AS_2 的溯源管理器向反匿名联盟管理器发起域间溯源请求,鉴于域间网络已被净化(也就是说在域间转发的 IP 包中,其源地址网络前缀部分是真实可信的),因此,该管理器将匿名样本包源地址与联盟成员的网络前缀进行逐一匹配:若匹配成功,则可认为匹配项就是攻击域 AS_1,然后向 AS_1 所属溯源管理器发起请求,完成 AS_1 内路径片段的还原任务;如果匹配失败,就意味着攻击域未加入反匿名联盟,出现溯源断层,立即终止溯源任务.

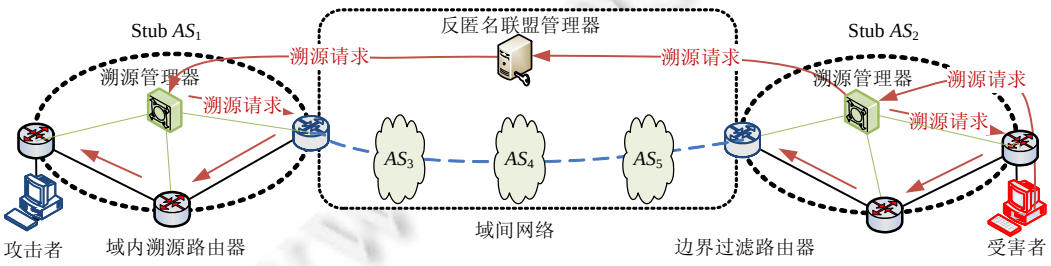


Fig.1 Topology hiding single-packet traceback architecture

图 1 可隐藏域间网络拓扑的跨域单包溯源架构

到目前为止,只是介绍了 SEE 方法基本框架,尚留部分难点未解决,以下各节将详细讨论相关解决策略.

(1) 与底层路由网络相似,域内溯源网络规模也是逐渐增大的.然而,已有的溯源方法只能采用静态方式来配置溯源节点,节点之间无法实时交换信息,从而导致溯源网络系统一旦开启后就无法动态扩展.因此,如何构建可动态扩展的域内溯源网络,实现溯源节点的动态加入和退出?

(2) 如果采用复用率较低的点着色理论为溯源路由器编址,就会导致溯源地址的空间较大,进而使得绝大部分路径指纹需要记录在溯源路由器上.因此,如何设计高效的编址策略、压缩溯源地址空间,使得更多的路径节点指纹能够直接标记到 IP 包头的标记空间,而不是记录到溯源路由器上,从而降低其存储开销?

(3) 存储和计算资源相对缺乏的溯源路由器只能要求以尽可能小的开销来建立路径指纹.然而,已有的方法要么建立基于包特征的路径指纹,致使溯源开销与包转发量成正比;要么建立基于路由的路径指纹,致使溯源开销与底层路由数量成正比.因此,如何在大规模网络中高效地提取和建立路径指纹,降低溯源开销?

(4) 越来越庞大的攻击规模需要尽可能多的 Stub 域加入反匿名联盟.然而,传统的出口边界过滤技术没有遵循“谁部署,谁受益”的激励原则,存在搭便车问题,使得大量未加入联盟的 Stub 域也同时享受着参与者的权利,从而极大地降低了部署积极性.因此,如何激励更多的自治域加入反匿名联盟,增强系统的可扩展性?

(5) 反匿名联盟的形成必然是一个漫长的过程,在此期间,那些非联盟成员主机完全可能伪造联盟内的地址向联盟成员主机发起匿名攻击,使得受害域误认为源地址所指向的自治域就是攻击域,进而造成攻击源误判.因此,如何设计一种从域内溯源到域间过滤的平稳过渡策略,解决联盟扩展过程中的安全问题?

1.2 域内溯源网络构建策略

域内溯源网络的部署投入通常会随着溯源增值服务收益的增加而逐渐增长,因此它的覆盖范围也会逐渐扩大,进而使得溯源网络的构建会是一个动态扩展的过程.这就要求溯源路由器必须随时交换彼此邻居节点的信息,以便及时感知新加入或退出的溯源节点,因而产生大量的网络数据.基于此,选择合理的数据传输方式就显得非常重要.如果采用带外或简单的带内传输,不仅会带来较大的成本和处理开销,而且无法保证数据隐私安全.为此,本文利用当前底层路由网络大多采用开放式最短路径优先协议(open shortest path first,简称 OSPF)的特点,通过扩展该协议的链路状态通告机制(link status advertisement,简称 LSA),提出一种可扩展的域内溯源网络构建策略,通过将所运载的网络数据隐藏于 OSPF 的链路状态,既降低了传输成本,又能利用 OSPF 的完整性保全机制保证运载信息的安全.在此基础上,鉴于本文所提的攻击路径并非底层网络的路由路径,而是以溯源网络为基础、与路由路径相映射的逻辑路径,为了有效地提取攻击路径的逻辑链路特征,溯源路由器需要建立 IP 包在溯源网络上虚拟转发关系表.

在 OSPF 网络中,同类型的邻接路由器利用分布式的链路状态通告 LSA 机制,通过频繁交换彼此的链路状态(其实就是路由器接口描述信息,例如接口 IP 地址、子网掩码、网络类型、cost 值等)来建立一个彼此同步的链路状态数据库,进而描绘出一个可动态扩展的全网拓扑结构图;然后,使用 Dijkstra 最短路径算法生成最短路径树,就能构造出路由转发表.受此启发,本文只需定义一种新的 LSA,就可在底层路由网络上建立域内溯源网络,而溯源节点通过获取溯源网络的拓扑结构,同时结合路由转发表,就能进一步构造出溯源关系表.目前,LSA 类型共有 11 种,其中,前 8 种是常用类型;后 3 种是不透明 LSA,属于备用类型.在不对现有网络设备和网络架构造成影响的前提下,本文把以自治域为作用范围的第 11 种备用 LSA 重新定义为溯源 LSA.各溯源路由器通过彼此传送该类 LSA 就可组成域内溯源网络.以图 2 为例,底层物理拓扑源于 RFC2328 OSPF 版本 2[12],而{R_1,R_3,R_4,R_7,R_{10},R_{12}}已升级为溯源路由器,利用溯源 LSA,它们可获取邻接节点,进而构建溯源网路.即使有新增节点加入或部分节点因故障而退出,OSPF 协议的 LSA 更新机制也能够保证溯源网络系统能够及时感知其节点的动态性,从而增强网络的可扩展性.

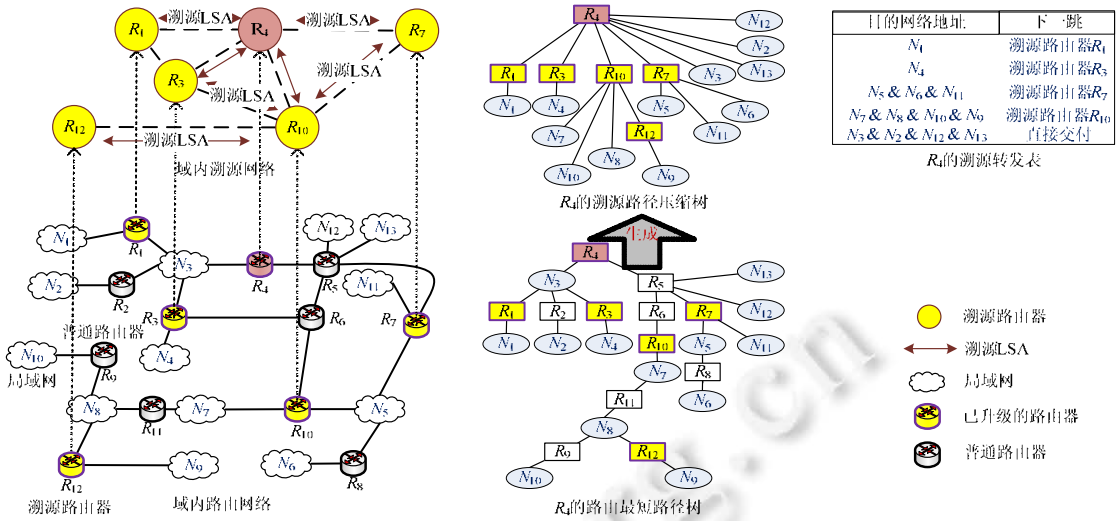


Fig.2 Construction of intra-AS traceback network

图 2 域内溯源网络构建

为了提取溯源网络的链路特征,溯源路由器需要建立一个溯源转发表,该表虽以底层网络节点的最短路径树为基础,却用来描述 IP 包在溯源网络上的虚拟转发关系.以图 2 给出的溯源转发表为例,假设以 N_{11} 为目的地的 IP 包 p 到达了溯源路由器 R_4.在底层路由网络上,根据最短路径树,p 必定先后经过物理链路 $R_4\rightarrow R_5$ 和 $R_5\rightarrow R_7$,而在溯源网络上,这两条链路会被压缩为一条虚拟链路 $R_4\rightarrow R_7$,因此 R_4 只需提取该条链路的特征即可.如果直接使用最短路径树生成溯源转发表会存在以下问题:需要访问大量无用节点,特别是在溯源节点增加或退出的时候,这会带来较大的重复计算.为此,本文定义了一种只包含溯源节点和网络节点的数据结构,称为溯源路径树(trace path tree,简称 TPT).利用它,溯源链路的提取不再需要访问非溯源节点,进而能够降低计算开销.给定溯源路由器 R,利用已建立的底层路由拓扑和溯源拓扑,分别计算出路由最短路径树 RST 和全网溯源路由器集合 TRS.TPT 源自 RST,其构建算法的基本原理就是在先序遍历 RST 的过程中,依据向上就近归属原则,将 TRS 中非溯源节点所关联的网络节点直接变为最近溯源节点的子节点,同时将非溯源节点删除.以图 2 为例,溯源根节点 R_4 包含 R_2,R_5,N_3,R_1,R_3,R_{10},R_7 这 7 个孩子.在先序遍历过程中,鉴于 R_2 是非溯源节点,它的孩子 N_2 按照向上就近归属原则,应上升为 R_4 的孩子,同时删除 R_2;同理,在 R_5 被删除之前,它的两个孩子 N_{12} 和 N_{13} 也被上升为 R_4 的孩子;网络节点 N_3 因为与 R_4 直连,所以不发生变化;至于其他孩子,因为它们是溯源节点,其下层网络节点按照归属原则,不再与 R_4 连接,因此无需变化.基于此,在 TPT 中,R_4 的孩子包含 4 个网络节点(N_2,N_3,N_{12} 和 N_{13})以及 4 个溯源节点(R_1,R_3,R_{10} 和 R_7).此外,为了避免因新增节点或删除节点而造成整个 RST 的重新构建、增加计算开销,通过分析上述节点与 TPT 局部分支的关系,建议使用增量更新算法.基本原理是:根据向上就近归属原则,可知在 TPT 中,更新节点只会影响离它最近的父亲节点.以此为出发点,通过将更新节点加入 TRS 以及从 RST 中提取以其父亲为根节点的局部 RST 树,按照 TPT 构建原理重新建立 sub-TPT,并将其更新到 TPT 中.至此,更新过程结束.

1.3 域内溯源地址分配策略

为了将更多的链路指纹写入到标记域,减轻溯源路由器的负担,域内溯源系统的编址策略必须高效,通过设计较简短的溯源地址来压缩链路状态特征,进而缩短链路指纹.在基于图着色的单包溯源方法中,路径回溯可看作是一个在下游取证、逐跳识别上游的过程,因此它只要求下游所建立的链路指纹能够识别出上游邻居即可.在此背景下,溯源地址仅用于唯一标识上下游节点,无需全网标识.此外,如果用一个无向图 $G(V,E)$表示溯源网络,其中,集合 $V=\{v_1,v_2,\ldots,v_n\}$的元素是溯源路由器,集合 $E=\{e_1,e_2,\ldots,e_n\}$的元素是连接两个溯源路由器的虚拟链

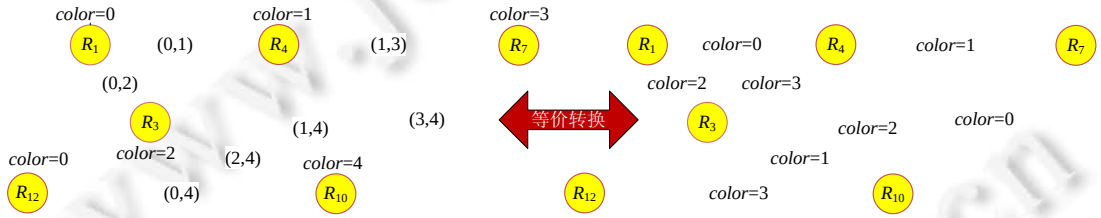
路,那么溯源网络可被看成是一种基于底层路由拓扑的虚拟网络系统.基于此,已有的方法大都将溯源编址抽象为 2-距离点着色问题,即给定映射$\pi_{node}:V\to\{1,2,\ldots,k\}$为 G 的一个 k 点着色,若对 G 中任意两个距离不大于 2 的顶点 u 和 v 均满足$\pi_{node}(u)\neq\pi_{node}(v)$,最小 k 值称为 G 的点色数,记为$\chi_{2d}(G)$.鉴于$\chi_{2d}(G)=n^2$,其中,n 为 G 中最大节点度,已有的研究通过统计当前互联网自治域拓扑结构特征,可知$\chi_{2d}(G)=2^{12}$,也就是说,溯源地址至少需要 12 位[10].此外,溯源网络作为一种基于底层路由拓扑的覆盖网络,当溯源节点数量达到某定值后,其最大节点度存在大于 n 的情形,使得溯源地址进一步增长,超过 12 位,这对于空间狭小的标记域来说依然较为冗余.为此,本文提出一种基于边着色理论的溯源地址分配策略,把最小着色数降低为$(n-1)$的同时,使溯源地址仍然具备上下游识别功能.

本文通过观察发现:就同一溯源网络来说,基于边着色的溯源地址分配和基于 2-距离点着色的溯源地址分配具有相同的标识作用.所谓边着色是指:给定映射$\pi_{link}:L\to\{1,2,\ldots,m\}$为 G 的一个边着色,若对 G 中任意两条链路 l_1 和 l_2 着色,如果 l_1 和 l_2 相邻,那么它们均满足$\pi_{link}(l_1)\neq\pi_{link}(l_2)$,最小 m 值称为 G 的边色数,记为$\chi'(G)$.

如图 3 所示(其溯源网络拓扑源于图 2),

- 在图 3(a)中,任意节点两跳之内被分配的颜色各不相同,进而由节点颜色组成的邻接链路编号也都彼此不同;
- 而在图 3(b)中,通过直接给链路着色,也能使得邻接链路编号各不相同.

而且本文在第 2.1.5 节的定理 2 已经证明:基于边着色的溯源地址分配能够准确地标识出攻击树中所有路径,从而保证较高的溯源精度.当新增溯源节点获得邻边的着色信息后,该节点应立即将它们填充到溯源转发表中.例如在图 3(b)中,溯源节点 R_4 会根据溯源转发表的上下游关系将邻接链路着色信息逐一填入到表的邻居链路编号列中,以便把链路特征及时写入到转发包的标记域,建立路径指纹.



(a) 基于2-距离点着色的溯源地址分配 (b) 基于边着色的溯源地址分配

Fig.3 Equivalent transformation between the 2-distance coloring and the edge coloring

图 3 边着色与 2-距离点着色的等价转换

根据 Vizing 定理,$\forall$无向图 G,则 $n\leqslant\chi'(G)\leqslant n+1$,其中,$n$ 是 G 的最大节点度,$\chi'(G)$是 G 的最小边着色数,这也就是说,$\chi'(G)$与 n 成正比.此外,本文将溯源网路 $G=(V,E)$称为底层路由网络 $G'=(V',E',P')$的路由导出子图,根据定理 1,已知 G 中最大节点度 n 小于等于 G'包含的路由路径数量$|P'|$,因此,$\chi'(G)\leqslant|P'|/2+1$.鉴于 G'包含接入网数量不超过$|V'|$,即每个路由器最多只能连接一个接入网络(即使有多个,也可把它们合并为一个),因而推断出$\chi'(G)\leqslant|V'|+1$.本文对由网络联合分析组织(cooperative association for Internet data analysis,简称 CAIDA)搜集的互联网路由器级拓扑中自治域所含节点数量进行统计[13],结果发现,96.13%的自治域所含节点数量都小于 256,如图 4 所示.基于此,可知$\chi'(G)\leqslant 2^8$,这也就是说,溯源地址只需 8 位就能唯一识别上下游.对于其他极少部分节点数量大于 256 的自治域,部署者可采取一种保守策略,即避免溯源节点无节制地动态加入,使它的最大节点度限定在 256 内,在一定程度上限制了溯源网络的扩展规模,进而降低了攻击路径延伸为路由路径的可能性.但是通过合理规划,这并不会影响溯源性能,例如尽可能地先将边缘路由器升级为溯源路由器,然后再升级核心路由器,这能使得溯源路径更靠近攻击源.

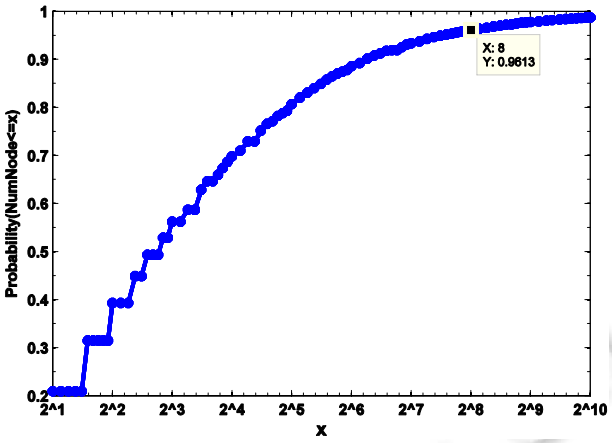


Fig.4 Node number distribution in different ASes

图 4 自治域中节点数量分布情况

定义 1. 域内底层路由网络 $G'=(V',E',P')$,其中,$V'=\{x_i|\forall i\in[0,m]\}$表示路由器集,$E'=\{x_ix_j|\forall x_i,x_j\in V'\}$表示链路集,$P'=\{s\propto t|\forall$接入网前缀 s,t 且 $s\propto t=x_0x_1\ldots x_i$ 是指从 s 到 t 的路由路径所包含顶点序列$\}$表示路由路径集.例如,在图 2 的底层路由拓扑中,路由路径 $N_3\propto N_{11}=R_4R_5R_7$.

定义 2. 域内溯源网络 $G=(V,E)$是一种覆盖网络,其拓扑可看成是底层路由网络 $G'=(V',E',P')$的路由导出子图,其中,V表示溯源路由器集,E 表示溯源链路集.可知,$V\subseteq V'$,$E\nsubseteq E'$且 $E\subset_{sub}P'$,其中$\subset_{sub}$表示溯源链路是路由路径片段.例如在图 2 中,溯源链路 $R_4R_7\subset_{sub}(N_3\propto N_{11}=R_4R_5R_7)$.

定理 1. 给定底层路由网络 $G'=(V',E',P')$,不管溯源网路 $G=(V,E)$如何变化,最大节点度 $n\leqslant|P'|/2\leqslant|V'|$.

证明:由于路由路径 P'是矢量,而节点 V'和链路 E'是标量,根据定义 1,可知$|P'|/2\leqslant|V'|$,而且溯源网络作为底层路由网络的覆盖网络,可知$|V|\in[1,|V'|]$.在底层路由网络拓扑不发生变化的前提下,依据上述推论,本文将溯源网络的规模分为 3 种:

(1) 当$|V|\leqslant|P'|/2+1$ 时,无论溯源节点的位置如何选择,其最大节点度 $n\leqslant|P'|/2$.因为$\forall v\in V$,其邻点数量 $N_G(v)\leqslant|V|-1\leqslant|P'|/2$,进而推出 $n\leqslant|P'|/2$.

(2) 当$|P'|/2+1<|V|<|V'|$时,无论溯源节点如何放置,溯源网络所覆盖的路由路径数量都不会比底层路由网络更多.因此,溯源链路作为底层路由路径片段,$\forall v\in V$,其关联链路数量 $n\leqslant|P'|/2$.

(3) 当$|V|=|V'|$时,溯源网络与底层路由网络重叠,因此二者的最大节点度相同.在底层路由网络中,$\forall v\in V'$,其相邻链路 $E_i(v)$都将承载不同的路由路径,且$|\bigcup E_i(v)|\leqslant|P'|/2$,因此 $n\leqslant|P'|/2$.

证毕. □

1.4 域内路径指纹建立和提取策略

在当前网络环境下,普通路由器往往使用无状态方法来处理数据包,致使受害者难以采集到任何指纹痕迹,更不必说追踪回溯.为此,溯源路由器的主要任务就是利用它转发 IP 包的契机来准确地提炼传播链路的特征,并将其记录到路径指纹库中.然而,网络设备的存储和计算资源一般都比较有限,如何以尽可能小的开销来建立路径指纹就显得非常重要.如果直接记录数据包来获得链路特征,必然会产生较大的存储开销,是以不得不采用存储压缩机制,而这难免会降低路径指纹准确度,进而影响溯源精度.通过探索路由转发与攻击路径形成规律,不难发现转发包的样式虽然繁多,但是其上下游链路却相对稳定.因此,溯源网络只需将转发包和虚拟链路进行绑定,即可建立路径指纹.受此启发,本文提出一种高效的路径指纹建立和提取策略,使得溯源存储开销只与攻击路径所含虚拟链路数有关,而与转发包或底层路由路径数量无关.

路径指纹建立和提取的基本原理如下.

- 首先,鉴于溯源网络中所有链路都已按照边着色理论进行编码,溯源路由器只需将链路编号写入到 IP 包头中就能建立反向上下游链路关系.然而,现有网络协议中所有包头字段都已被使用,如果新增字段,就需要改动网络协议、升级网络设备,从而带来巨大的成本代价.为此,本文通过重载 IP 包头的 Identification 字段来作为标记域,用于存放链路编号,原因是:随着 TCP 协议中最大分段大小(maxitum segment size,简称 MSS)的广泛应用,IP 分片的使用率已经从原来的 0.25%降低到 0.06%,其中,60%的分片包还都是攻击包[14];Identification 字段的作用是产生数据包的标识,使得同一数据包的分片拥有相同的标识.考虑到路由的稳定性,即使本文重载该字段,同一数据的分片包所载链路数据也相同,因此它依然满足字段条件,使得受害者能重装出绝大部分分片包[7].
- 其次,在同宿但不同源的攻击网络中,同一链路可能被多条路径共享.如果仅仅建立反向上下游关系,那么在路径重构过程中并不能准确判别链路归属.为此,引入多协议标记交换网络的标记分发原理,使得溯源路由器能够为每条传输路径独立分配具备唯一性的路径识别符——标记(label),并将它与链路编号一同写入标记域中进行松散地绑定,进而建立一种具备路径特征的反向上下游链路关系.基于此,本文将标记域划分为两部分:前 8 位存放链路编号;后 8 位存放路径标记.原因是:根据第 1.3 节的定理 1,链路编号最大值通常不会超过 2^8;根据图 4,绝大部分自治域的节点数量通常不会超过 256,因此攻击网络的传播路径最多也只有 2^8(对于极少部分节点数量较大的自治域,可采用以下方法减小传播路径数:添加 1 位尚未使用的标志位到标记域,从而将存放路径标记的空间扩大的 9 位;通过限制溯源网络规模将攻击路径数量缩小到规定范围内;将前两种方法混合使用).
- 然后,在溯源系统初始阶段,溯源路由器需要及时提取 IP 包的标记域信息并将它们添加到溯源转发表,才能建立路径指纹.然而,一旦指纹建立成功后,对于后续到达包,溯源路由器只需通过表查询操作来获取标记信息,并将其与 IP 包绑定即可.
- 最后,当攻击发生后,溯源管理器利用攻击样本包所提供的标记信息,依照标签首尾相连方式来识别所有相关虚拟链路,进而拼接出攻击路径.

为了更详细地描述相关设计细节(偏工程操作),本文以图 5 为例进行阐述.图 5 的溯源网络拓扑源于图 2,假设图 2 所描述的自治域就是图 1 的 Stub AS_2(即受害域),其中,R_1 是该域的边界过滤路由器.受害者位于 N_9,与溯源路由器 R_{12} 相连.攻击者有两个:一个来自域内,位于 N_{11},与 R_7 相连;另一个来自域外,与边界过滤路由器 R_1 相连.这就意味着 AS_2 需重构一条片段路径和一条完整路径.假设网络中只有攻击者和受害者之间会发送数据,因此攻击链路包括{R_1→R_4,R_4→R_{10},R_7→R_{10},R_{10}→R_{12}}.

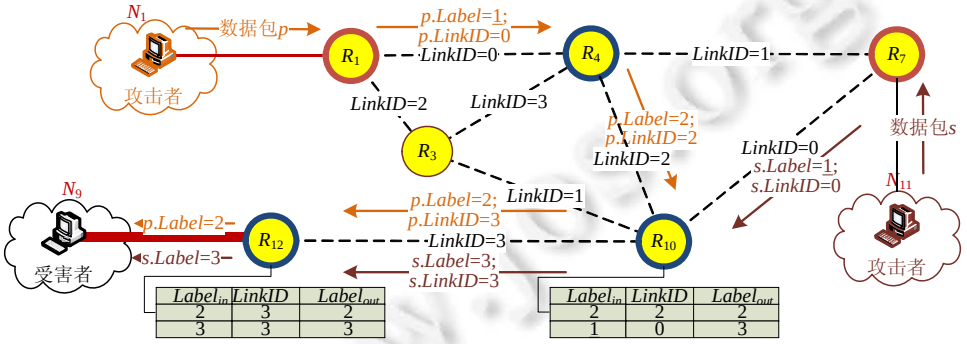


Fig.5 Path fingerprint establishment and matching

图 5 路径指纹的建立和提取

- 域内路径指纹建立

当 IP 包 p 到达入口溯源路由器 R_7,首先根据目的网络地址,通过查找扩展的溯源转发表来确定下一跳溯源路由器 R_{10} 以及邻居链路编号 $LinkID$=0,然后分配标准标记 $Label$=1 给 p,同时将它与链路 R_7→R_{10} 绑定,具体方

法如下:当 p 到达 R_7 后,R_7 把信息[*Label*=1,*LinkID*=0]写到 p 的标记域中,并将 p 转发到 R_{10}.当 R_{10} 收到 p 后,R_{10} 从 p 中提取标记信息[1,0],并将它添加到溯源转发表以及指派新的标记给链路 $R_{10}\rightarrow R_{12}$,至此完成绑定操作.由于下游链路 $R_{10}\rightarrow R_{12}$ 同时被两条同宿但不同源的攻击路径所共享,因此 R_{10} 首先依据 p 携带的标记信息识别出它的来源,然后分配不同的标记给它们,并将其添加到溯源转发表.例如,如果 *p.LinkID*=2,那就说明 p 源于 R_1,R_{10} 分配 *Label*=2;如果 *p.LinkID*=0,那就说明 p 源于 R_7,R_{10} 分配 *Label*=3.最后,将这些标记分别与链路 $R_{10}\rightarrow R_{12}$ 绑定.为了叙述方便,R_{10} 将标记 *label*=3 称为出标记 $Label_{out}$,而 R_{12} 将标记 *label*=3 称为入标记 $Label_{in}$.需要说明的是:为了灵活和安全地管理标记资源,R_{10} 采用已提出的基于资源池的标记分发策略[10],即以随机选取方式来分发标记,避免标记值被恶意用户所预测.此外,考虑到攻击者可能通过伪造标记域信息来欺骗入口路由器,进而破坏追踪,R_7 只需判断到达包所携带的链路编号是否与它的邻居链路编号相符合.如果不符合,即可判定 R_7 是入口路由器.当 p 到达溯源路由器 R_{12},通过查找溯源转发表可知下一跳是直接交付,因此只需依据 p 携带的标记信息识别出它的来源,然后分配不同的标记给它们并写入到 p 中即可.当 p 到达出口路由器 R_{12} 后,路径指纹信息就已经建立完毕.之后,再有 IP 包在路径上传输,就只需执行标记操作,不需再次扩展溯源转发表.值得注意的是,如果出口路由器是过滤边界路由器(即当前自治域是攻击域),那么从该域流入域间网络的数据包只需载有出标记信息即可,不需携带链路地址编号.

如果 p 第 1 个到达的路由器是边界过滤路由器 R_1 而不是 R_7,除了提取 p 中标记信息[*Label*=5]并将其添加到溯源转发表之外,其他操作(包括标记分发和链路绑定)都与普通中间路由器相同,具体原因如下:虽然 R_1 是 p 在受害域中传播时的入口,但是从整条攻击路径来看,它处于中间位置,因此根据链路绑定原理(以中间节点 R_{10} 为例),p 应该除了携带由攻击域边界路由器写入的标记信息,还需载有从攻击域到受害域之间虚拟链路 m 的编号.然而,鉴于域间网络已被净化,仅需分析 p 中源地址网络前缀即可识别攻击域,也就无需在 p 中携带该链路编号,即能实现 p 与虚拟链路 m 的绑定.基于此,攻击域的边界路由器只需在 p 中写入出标记,而受害域的边界路由器也仅需记录该标记就完成链路绑定.这也就意味着 R_7 溯源链路扩展表的上游链路编号 ID 列目前处于空闲状态,没有值写入,在第 1.6 节,我们将对该列有额外的作用说明.

- 域内路径指纹提取

当 Stub 域的溯源管理器接收到携带匿名样本包 p 的溯源请求后,需立即确定匿名包 p 在受害域内的出口路由器.具体方法是:如果溯源请求来自域外,通过将匿名包的目的地址与溯源网络拓扑结构相结合,就能确定 p 从哪个边界过滤路由器流出**,即出口路由器;如果来自域内,采用相同方法,就能确定离受害者最近的溯源路由器,即出口路由器.一旦确定出口路由器后,上述两种情景下溯源过程完全相同,因此本文只拿第 2 种情况举例.假设溯源管理器通过分析发现,p 在本域内出口路由器是 R_{12}.之后,就直接将取证请求[*p*.目的地址,*p*.标记]发送给 R_{12}.R_{12} 接收到请求后,首先从溯源转发表查找出包含 *P*.目的地址的网络前缀,如果有多项,就从匹配结果中选择具有最长网络前缀的路由.然后,从扩展表的 $Label_{out}$ 中找出与 *P.label* 相等的表项,提取出[$Label_{in}$=2,*LinkID*=3].最后,依据 *LinkID*=3 识别出链路 $R_{10}\rightarrow R_{12}$,并发出新的取证请求[*p*.目的地址,$Label_{in}$=2]给 R_{10}.当 R_{10} 收到请求后,立即提取出绑定信息[$Label_{in}$=1,*LinkID*=0],因包含标准标记 1,既可识别出链路 $R_{10}\rightarrow R_7$,又可判定 R_1 是入口路由器,由此结束溯源过程.如果当前取证的溯源路由器已然是域边界路由器,那么提取[$Label_{in}$=5],然后向反匿名联盟管理器发起载有[$Label_{in}$=5,样本包=*p*]的域间请求.反匿名联盟依据 p 的源地址就能识别出攻击域,然后向该域的溯源管理器发起载有[$Label_{in}$=5]的域内溯源请求.

1.5 域间反匿名联盟构建策略

在开放式网络环境下,鉴于当前匿名攻击数量庞大且分布发散,急需尽可能多的 Stub 域加入反匿名联盟,使其具备匿名追踪的能力.然而,传统出口边界过滤技术缺乏激励机制,存在搭便车问题.以图 1 为例,为了避免 AS_1

** 在 Transit-Stub 网络拓扑中,Stub 域通常只有一台边界路由器,用于与外界交互数据,因此一旦确定攻击域,就等于识别出边界过滤路由器.即使在少量的拥有多个边界路由器的 Stub 域(多宿主场景)内,在规定时间内通常也只有一个边界路由器负责向受害域发送 IP 包,因此通过分析 Stub 域的域间路由策略,结合匿名包的目的地址,即可获得边界过滤路由器.

欺骗,需要把源地址不属于 AS_1 的所有匿名包过滤掉,包括那些目的地址不在联盟成员前缀内的包,从而使非联盟成员也获得恩惠.为了解决该问题,强化激励功能,本文引入文献[15]提出的面向对等过滤的反匿名自治域联盟构建策略(mutual egress filtering,简称 MEF),使非联盟成员能从受益者中严格剥离.

该策略的基本思想是:在出口边界过滤的基础上,通过引入过滤对等体(filtering peers,简称 FP),将反匿名联盟看成是一个由过滤对等体组成、建立在自治域网络之上的超网络.如果自治域 AS_i 阻止流向自治域 AS_j 的出网匿名流当且仅当 AS_j 也阻止流向 AS_i 的出网匿名流,那么(AS_i,AS_j)就可构成一组过滤对等体.具体规则说明如图 6 所示.(AS_1,AS_2)构成一组过滤对等体,为了实现对等过滤,AS_1 在其边界过滤路由器需配置以下过滤规则:1) permit AS_1_prefix any;2) deny any AS_1_prefix & AS_2_prefix;3) permit any any.其中,第 1 条表明只允许源地址属于该 Stub 域的 IP 包通过,第 2 条表明凡是目的地址是 AS_2 的匿名包都将被丢弃,第 3 条表明目的地址不在过滤对等体内的匿名包允许通过.只有当所有 AS 都加入过滤对等体时,才能充分发挥出口边界过滤的优势,最终建立可信任的域间网络.如图 6 所示,MEF 方法的有效实施需要由联盟注册模块、规则管理模块和包过滤模块来协同工作完成.它们各自的职能描述如下.

(1) 联盟注册模块.该模块运行于反匿名联盟服务器,主要用于动态维护过滤对等体的信息,管理和控制成员的加盟及退出,并且向规则管理模块实时发布联盟成员信息.

(2) 规则管理模块.该模块运行于溯源服务器,主要任务是与联盟注册模块进行通信,完成自身注册并且获取联盟成员的地址前缀,以及控制本域的边界路由器,下发基于地址前缀的 ACL 规则.

(3) 边界过滤模块.该模块运行于过滤边界路由器,主要任务是通过将 IP 包与 ACL 规则自上而下依次匹配,进而过滤匿名包.

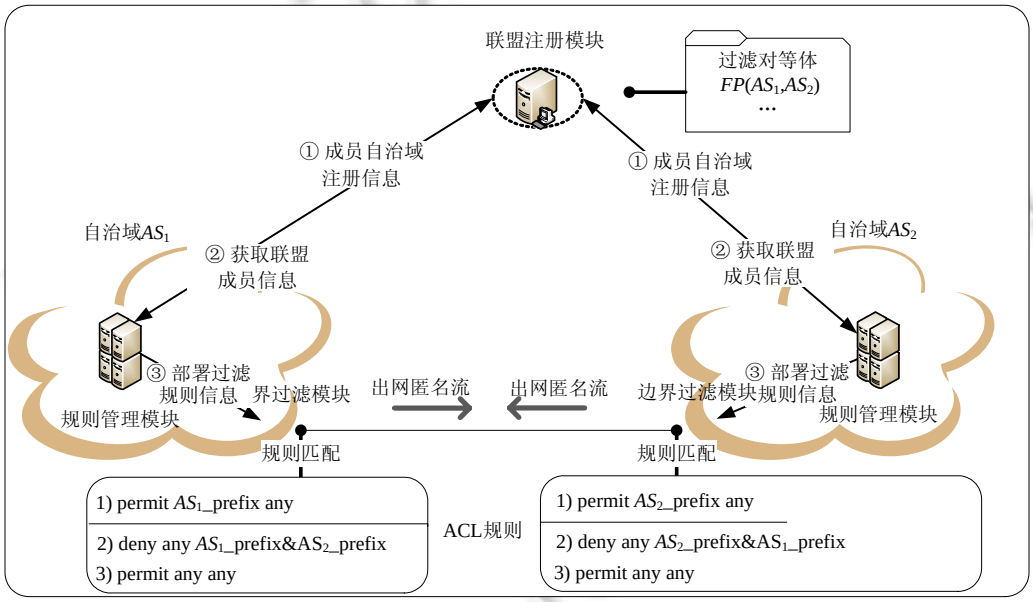


Fig.6 Anti-Spoofing alliance construction

图 6 反匿名联盟构建

1.6 域内到域间溯源的平稳过渡策略

当所有自治域都加入反匿名联盟的时候,反匿名联盟管理器仅凭匿名包的源地址就能确定攻击域.然而在反匿名联盟完全形成之前,非联盟成员则可能利用上述溯源架构中成员域不加验证的系统漏洞发起匿名攻击,通过伪造成员域的前缀地址,使系统在识别攻击域时发生误判.为此,本文提出了一种从域内到域间溯源的平稳过渡策略,排除因非联盟成员伪造成员域地址而造成攻击域误报的情况.该策略的基本思想是:利用边界网关协

议(border gate protocol,简称BGP)中自治域都被分配唯一识别号(AS number,简称ASN)的特点,通过引入轻量的Hash认证技术,使每个准备流出攻击域的转发包都载有相关域ASN的*Hash*值,而受害域只需要记录该*Hash*值.在域间溯源任务发起后,反匿名管理服务器通过源地址分析和ASN双重认证来准确识别攻击域.

自治域在向反匿名管理服务器注册时,除了网络前缀,还需提交它的ASN,而服务器则向自治域随机地指定一个$Hash_k$函数,用于验证成员域.以图1为例描述从域内到域间的安全过渡过程:假设*Hash*−1()是攻击域AS_1的验证函数,AS_1和AS_2分别是攻击域和受害域的ASN号.当IP包p到达攻击域AS_1的边界路由器(AS border router,简称ASBR)时,它除了按照第1.4节介绍的路径指纹建立原理正常写入出标记,还需将*Hash*=*Hash*−1(AS_1)写入到IP包用于标记上游链路标号的空间中,然后再转发出去.由于非联盟成员未被指定*Hash*函数,因此由它转发出去的IP包虽然源地址和标记值可能被假冒为成员域,但是*Hash*值很难被伪造,因为*Hash*函数的分配是随机的,还可以通过不断更新函数来进一步提高伪造难度.当p到达受害域AS_2的ASBR时,将p载有的[标记,*Hash*值]记录到路由器的扩展的溯源转发表中,然后将新分配的出标记和下游链路编号写入到p中即可.当我们将第1.4节的方法扩大应用到域间网络时,鉴于经过边界过滤路由器的攻击路径要远多于域内溯源路由器,从而造成标记资源的过度分配,产生溯源误报率,为此,我们建议采用以下方法避免该问题:(1) 采用文献[13]提出的基于移动平均线的标记管理策略,通过预测标记类型,动态管理标记的分配时间,提高其利用率;(2) 通过及时检测匿名攻击以及发起溯源请求,争取在原标记未被覆盖之前取得指纹信息.在路径指纹提取过程中,当受害域AS_2的ASBR接受到溯源请求,并将p.上游链路编号(即*Hash*)和出标记返回给溯源管理器后,该管理器随即发起域间溯源请求.反匿名联盟服务器首先提取p的源地址,并将它与联盟成员列表中所有网络前缀一一匹配,从而获得匹配成功的*ASN*=AS_1和*HASH*函数=*HASH*−1(),然后计算*hash*′=*HASH*−1(AS_1),最后判断*Hash*与*hash*′是否相同:若是,说明该自治域就是攻击域,立即向相关溯源管理器发起域内溯源请求;否则,该自治域不属于联盟成员,溯源任务结束.需要说明的是:整个验证开销可忽略不计,原因如下:(1) *Hash*函数的计算开销非常小;(2) 边界路由器只需计算一次*Hash*值,第2次直接将它写入转发包即可;(3) 受害域不需要验证到达包,只有溯源任务发起后,才进行验证;(4) *Hash*函数并不需要频繁和大范围更新,只需偶尔重新指派即可,因此通信开销也很小.

2 性能评价

为了验证提出的SEE方法,本文进行了理论分析和仿真实验,其中,第2.1节将使用理论分析来证明SEE的高效性和可扩展性,第2.2节则通过基于人工和真实网络拓扑的实验仿真来补充分析结果.

2.1 理论分析

通过与目前典型的单包溯源方法(包括S3T[10],RHIT[7],SPIE[5],HIT[8])进行比较,本节将使用数学方法来评估SEE的性能,所涉及的指标包括路径指纹建立的存储开销(storage overhead for fingerprints establishment,简称TS)、路径指纹建立的时间开销(time overhead for fingerprints establishment,简称FE)、溯源网络通信开销(traceback communicationoverhead,简称TC)、路径指纹提取开销(fingerprints extraction overhead,简称FE)和溯源精度(traceback accuracy,简称TA).需要说明的是,SEE方法将溯源过程分为域内和域间两阶段,其中,域内网络因存在大量溯源路由器会产生所有上述开销;域间网络通过出口边界过滤来构建,不存在溯源路由器,因此只会产生通信开销.

2.1.1 路径指纹建立的存储开销(TS)

路径指纹建立的存储开销是指溯源路由器为了路径重构需要建立的指纹痕迹数量.SEE方法的路径指纹全部集中在溯源转发表中,因此它的溯源存储开销TS_{SEE}与溯源转发表的条目数量(the number of items,简称NumItem)成正比,而每个条目又会与一个子表相关联,子表的表项数量通常不会超过256个(原因已在第1.3节中阐述).因此,TS_{SEE}=256×*NumItem*.此外,根据溯源转发表定义,∀溯源路由器R_i,其溯源转发表所含条目数量与节点度相关.根据定理1,在底层路由网络$G'=(V',E',P')$给定的前提下,无论溯源网络拓扑如何变化,它的最大节点度$n\leqslant|P'|/2$,如果对应的溯源路由器为R_i,那么它的*NumItem*$\leqslant|P'|/2+1$(包括直接交付).进而推断出SEE方法中

存储开销最大的溯源路由器 $Ts_{SEE}^{\max}(R_i)=256\times(|P'|/2+1)$.按照 P'的定义以及第 1.3 节的推论,可知$|P'|/2\leqslant 256$.此外,子表中每个表项都占 3B(包括 8bit 上游链路 ID、8bit 出标签、8bit 入标签).因此, $Ts_{SEE}^{\max}=256\times257\times3\approx$ 0.19MB,这就是说,SEE 方法溯源存储开销是一个固定值,且只需 0.19MB.

任给溯源路由器 R_i,假设单位时间内到达 R_i的数据包为 s,经过 R_i的路由路径为 r.S3T 采用基于路由路径的指纹痕迹建立方法,随着时间 t 的推移,它的存储开销 $TS_{S3T}=r+n\times t\times3\%$.然而 r 与 P'不相同,前者是基于 IP 地址的路由路径,后者是基于网络前缀的路由路径,前者可汇聚压缩成为后者,因此可知 $P'<<r$;SPIE 方法要求 R_i 记录每个到达包作为指纹痕迹,因此 $TS_{SPIE}=n\times t$;HIT 采用隔跳记录方法,其存储开销大约是 SPIE 的 1/2,因此 $TS_{HIT}=1/2\times n\times t$;RHIT 方法采用基于接口标记的指纹痕迹建立方法,它的存储开销已被验证为 TS_{RHIT}=0.313MB.

综上所述,除 SEE 和 RHIT 的存储开销是定值以外,其他方法的存储开销都会随着运行时间的增长而不断增大;通过比较,又有 $Ts_{SEE}^{\max}<TS_{RHIT}$.因此,就存储开销来说,SEE 方法无疑更具优势.特别是在流量异常情况下,本文方法的优势更加明显.例如:在面对 DDOS 攻击或扫描攻击时,传统方法大都会因流量异常而增加存储开销;然而在本文方法中,一旦溯源路径建立成功,无论源地址和目的地址是什么,溯源路由器都不再执行记录操作.

2.1.2 路径指纹建立的时间开销(FE)

路径指纹建立的时间开销是指溯源系统为了建立一条路径指纹所需要花费的时间,间接反映了系统对底层网络 IP 包转发效率的影响.SEE,S3T 和 HIT 都是基于覆盖网络的单包溯源方法,支持增量部署,其规模可以远小于底层路由网络.假设任意两台主机之间路由路径长度的数学期望值为 s,而溯源路径长度为 k,其中 $k<s$.在 SEE 方法中,溯源路由器为了建立指纹痕迹需要查询溯源转发表.如果溯源转发表是基于软件的,那么表查询时间为 $o(m/2)$,整体路径建立所花费的时间为 $FE_{SEE}=k\times o(m/2)$;与 S3T 相似,如果使用基于内容寻址的相连存储器来实现该表,那么查询时间降为 $o(1)$,路径建立时间为 $FE_{SEE}=k\times o(1)$,其中,m 为表长,通常只有 256.在 S3T 方法中,溯源路由器的主要开销也是查询溯源转发表,但是其表长可达 262 144,因此 $FE_{SEE}<FE_{S3T}$.在 HIT 方法中,溯源路由器只需执行哈希查询,它的查询时间为 $o(1)$,路径建立时间为 $FE_{HIT}=k/2\times o(1)$.RHIT 和 SPIE 方法都不支持增量部署,它们的溯源网络必须与底层网络相同.在 RHIT 和 SPIE 中,溯源路由器也只需执行哈希查询,因此它们的查询时间为 $o(1)$,但是路径建立时间却为 $FE_{RHIT}=s\times o(1)$,$FE_{SPIE}=s\times o(1)$.

综上所述,鉴于 $k<s$,可知 $FE_{SPIE}=FE_{RHIT}\geqslant FE_{S3T}\geqslant FE_{SEE}\geqslant FE_{HIT}$.也就是说,若通过硬件来实现溯源转发表,那么与其他方法相比,SEE 的指纹提取开销依然较为理想.

2.1.3 溯源网络通信开销(TC)

溯源网络通信开销是指溯源系统为构建溯源网络而产生的数据通信量,间接反映系统规模的不断增大对底层网络带宽性能造成的影响.SPIE,HIT,S3T 和 RHIT 方法只能采用静态部署,在溯源系统启动后不会产生任何数据通信,因此 $TC_{SPIE}=TC_{HIT}=TC_{S3T}=TC_{RHIT}=0$.但是这也造成系统扩展性和可靠性差等问题,例如,如果有新的溯源节点加入,通常需要将溯源系统全部关闭,重新部署后再启动;如果在运行过程中溯源节点宕机,其他溯源节点因彼此不通信而无法及时感知,进而导致溯源系统失效.SEE 方法能够被动态部署,在系统启动后,溯源节点之间通过彼此交互连接信息来实时感知新增、失效节点,从而实现系统的动态扩展.SEE 将溯源过程分为域内和域间两阶段,其中,构建域内溯源网络的通信数据全部隐藏于 OSPF 协议中,不需要额外开销,因此可知,$TC_{\text{int }ra}^{SEE}=0$. 构建域间反匿名联盟的通信数据全部采用带内传送,假设联盟成员总数为 N,每新增一个成员,成员更新的通信开销为 $TC_{\text{int }ra}^{SEE}=o(N)$.

综上所述,为了实现动态扩展,SEE 方法增加 $o(N)$通信开销,因此不会对带宽有太大的影响.

2.1.4 路径指纹提取开销(PC)

路径指纹提取开销是指路径指纹提取过程中被查询的溯源路由器数量.SEE 方法的路径重构开销只与攻击域涵盖的路径长度 w 有关,而与整条攻击路径长度 l 无关,因此 $PC_{SEE}=w-1$.S3T 和 RHIT 方法不分域间和域内两层,它的路径重构开销直接与 l 有关,而且前者不需要查询入口路由器,因此 $PC_{SEE}=l-1$,$PC_{RHIT}=l$.SPIE 和 HIT 方法除了查询攻击路径节点,还有它们的邻居节点,因此 $PC_{SPIE}=w\times(m-1)$,$PC_{HIT}=1/2\times w\times(m-1)$,其中,$m$ 是平均邻居数量,即节点度.已有研究表明,节点平均度大约是 6.34[16].因此,$PC_{HIT}=1/2\times w\times(m-1)\approx3\times(m-1)$.

综上所述,$PC_{SPIE}\geqslant PC_{HIT}\geqslant PC_{RHIT}\geqslant PC_{S3T}=PC_{SEE}=w-1$.因此,与其他方法相比,SEE 路径指纹提取开销更低.结合第 2.1.3 节的结论,不难推断出本文方法不会消耗太多带宽资源.在溯源网络建立阶段,域内带宽开销可忽略不计,域间带宽开销为 $o(N)$,数量级较低;在溯源路径建立阶段,指纹痕迹直接内嵌于数据包,无需额外增加数据流;在攻击路径重构阶段,仅需发送十几个溯源请求,不会占用太多带宽资源.

2.1.5 溯源精度(TA)

溯源精度是指在溯源过程中攻击路径节点被误报或被遗漏的概率.一般来说,溯源精度的影响因素有两点:指纹建立策略本身和数据压缩工具.例如:S3T 方法较少使用数据压缩工具,但是它将路由路径与指纹痕迹进行绑定,根据它的指纹痕迹建立原理,当指向受害者的路由路径数量超过某一阈值后,就会出现溯源误报率,$TA_{S3T}=1-[1-b/(c\times N_{ROUTER_{\max}})]\times\sigma$, 其中,溯源路由器总量为 c,溯源网络的存储资源总量为 b,攻击路径所占比例为 σ,溯源路由器 $Router_{\max}$ 所承载的溯源路径数量为 $N_{ROUTER_{\max}}$;SPIE 和 HIT 方法虽然不会产生溯源错误,但是由于存储开销太大,不得不使用数据压缩工具,因此产生溯源误报率,$TA_{SPIE}=TA_{HIT}\approx 1-(1-v/e^{svt/o})\times\sigma$,其中,溯源设备的存储容量为 o,哈稀函数个数为 v,系统持续时间为 t,攻击包所占比例为 σ,单位时间内到达设备的数据包为 s.

就 SEE 方法来说,首先,它采用边着色代替 2-距离点着色为溯源网络编址,但通过定理 2 可知,基于边着色的溯源网络不会降低溯源精度;其次,SEE 方法因存储开销较小而没有使用任何数据压缩工具,因此不存在牺牲精度的情形;最后,在反匿名联盟尚未形成之前,可能因溯源过渡机制而产生标记过度使用问题,进而引起溯源误报率,但是第 1.6 节已给出解决策略,从而能有效避免该问题.一旦反匿名联盟完全形成后,我们可以不再使用过渡机制,也就不存在标记过度使用,因此 TA_{SEE} 可达 100%.RHIT 也未使用压缩工具,而且经过验证 TA_{RHIT}=100%.

综上所述,$TA_{SPIE}=TA_{HIT}\leqslant TA_{S3T}\leqslant TA_{RHIT}=TA_{SEE}$=100%.

定义 3(单路). 顶点度 $d_{\max}\leqslant 2$ 且顶点个数大于 1 的无圈单图称为单路,记为 L.

定义 4(超单图). 单图 G_1,G_2 通过共用或重合 n 个顶点或链路组成的无圈单图称为超单图,记为 S.

引理 1. 给定两条单路 L_1 与 L_2,存在公共点集 M,组成超单图 S.$\forall V_i\in M$,如果与 V_i 相联的链路既属于 L_1 又属于 L_2,那么 L_1 与 L_2 完全重合.

证明:因为$\forall V_i\in M$,与 V_i 相联链路既属于 L_1 又属于 L_2,所以 $d(V_i)\leqslant 2$,也就是说,在 L_1 与 L_2 组成的超单图 S 中,$d_{\max}\leqslant 2$.根据定义 3 可知,S 既是单图,也是单路.而 L_1 与 L_2 也为单路,也就说,它们所含的节点全部相同,所以 L_1 与 L_2 为完全重合.证毕. □

引理 2. 任给两条的单路 L_1 与 L_2,存在公共点集 M,组成超单图 S.如果它们不完全重合,并且各自端点在超单图 S 中的度数等于 1,那么必然存在分叉点 $e\in M$,$d(e)\geqslant 2$,且关联的两条链路分别属于 L_1 和 L_2.

证明:假设不存在分叉点,只有非分叉点,即$\forall V_i\in M$,与 V_i 关联的链路要么属于 L_1,要么 L_2.那么$\forall V_i\in M$,存在以下有 3 种情况:(1) V_i 的所有关联边只属于 L_1 或 L_2;(2) V_i 的所有关联边既属于 L_1 又属于 L_2;(3) V_i 的部分关联边既属于 L_1 又属于 L_2,而其余的只属于 L_1 或 L_2.如果是情况(1),那么不存在公共点集 M,这与前提矛盾;如果是情况(2),根据引理 1 可知,L_1 与 L_2 完全重合,这与前提也矛盾;如果是情况(3),必然存在一个节点 x,它的 $d(x)\geqslant 2$,关联链路分别属于 L_1 和 L_2,这与假设矛盾.因此,一个正确的公共点集合中,必然存在分叉点.证毕. □

定理 2. 任给受害者 V,溯源网络都可以通过一组边颜色序列来唯一标识出它的攻击路径树.

证明:与 V 关联的任意两条攻击路径都可看作单路 L_1 与 L_2.由攻击路径树的特征可知,L_1 和 L_2 存在公共点且不完全重合,因此可组成超单图 S,而且入口路由器的边只有一条,所以 L_1 与 L_2 端点的度等于 1.由引理 2 可知,必然存在交叉点 x,它的关联边分别隶属于不同的路径.根据边着色原理,可知关联边的颜色编号必定不同.此外,S 可被看作攻击树的子树,它的每条链路都可按照拓扑位置映射到攻击树,因此 L_1 与 L_2 的颜色序列一定不同.该推论可以应用到多条攻击路径,从而得到受害者可以用唯一颜色序列表示攻击路径.证毕. □

2.2 仿真实验

仿真实验的目的是对第 2.1 节的分析结果进行补充,特别是已有的技术在存储开销和扩展性方面所面临的挑战.在仿真实验中,我们以容易引发 IP 匿名事件的 DoS 攻击网络来对本文方法进行验证.考虑到真实环境的复杂性及实现的困难性,出于简化实验的目的,与文献[8,10]类似,我们也通过搭建网络攻防仿真平台来模拟 DoS

攻击下的 IP 匿名活动情况.

- 首先搭建 IP 网络:使用 OMNET++(OMNeT++4.3 released)和 INET(inet-2.1.0-src.tgz)仿真 IP 网络[17,18],其中,OMNET++是一种可扩展的基于组件模块化的多协议网络仿真软件,主要为通信网络和分布式系统提供基础底层结构和工具;INET 框架在 Omnet++的基础上实现了基本 TCP/IP 协议栈,包括从物理层到应用层的所有协议.
- 其次,使用 Brite 和 ReaSEGUI 获得基于 Omnet++的拓扑文件,其中,Brite 是一种网络拓扑转化软件,我们通过二次开发,使它能够将 CAIDA 公司所收集的互联网路由器级拓扑转化为可支持 Omnet++的拓扑文件;ReaSEGUI 则是一种面向 Transit-Stub 网络的人工拓扑生成工具,由它生成多自治域网络拓扑,只有边界节点才连接用户主机,而核心节点不连接.
- 然后,在 IP 网络上使用 ReaSE 仿真 DoS 攻击,其中,ReaSE 是一种基于 Inet 的攻击场景仿真软件,它可以模拟 DDoS、蠕虫、Web、ping 等流量模型.
- 最后,在该攻击网络上实现不同的单包溯源方法(包括 SEE,S3T 和 HIT).

整个平台搭建流程和不同网络拓扑下其攻击树形式如图 7 所示.该系统平台运行在一台 PC 的虚拟机上(Intel 2core 2.40GHz processor,2.0GB of RAM,VMware Workstation 7.0,CentOS release 5.4),除了仿真任务,还需要收集每个溯源路由器所记录的指纹痕迹数量和攻击路径长度.结果整理任务运行在另一台 PC 机上(Windows XP SP3,Intel 2core 2.40GHz processor,2.0GB of RAM,VS 2008,MATLAB 7.6),主要对收集的指纹数据进行分析和计算.

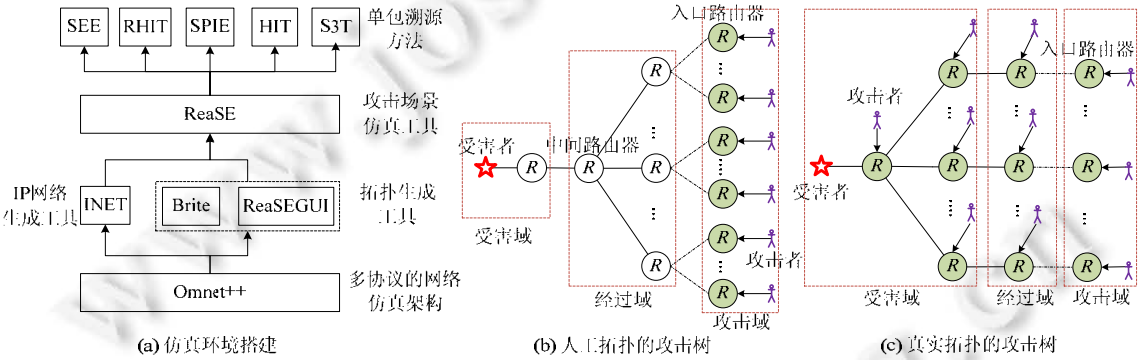


Fig.7 Simulation environment setup and topological structure description

图 7 仿真环境搭建以及拓扑结构说明

在平台搭建完成后,我们通过调整攻击参数来布置不同攻击场景,以便观测溯源性能指标的变化情况,从多角度验证第 2.1 节分析结果的正确性,其调整的攻击参数包括:

(1) 随机地指定一台用户主机作为受害者 V_i,并且选择其他主机作为攻击者;

(2) 攻击者除了与受害者通信,还会与正常用户通信,此外,正常用户之间也会随机发送消息,其中,攻击流速率 A 为 1Kpps,正常流速率符合正态分布 N(20pps,30pps);

(3) 调整自治域中溯源路由器所占比例 ξ,部署不同规模的溯源网络;

(4) 增加边界路由器连接客户主机的数量,扩大底层路由路径规模;

(5) 改变攻击主机所占比例 β,发起不同规模的 DoS 攻击,调整网络中攻击路径数量.

此外,SPIE 和 RHIT 方法不支持增量部署和系统规模扩展,只能被全网部署,因此并不参与实验比较,而比较方法只包括 3 个可扩展的基于图着色理论的单包溯源方法:HIT、S3T 和 SEE.

2.2.1 路径指纹建立的存储开销

第 2.1 节已经给出 SEE 及比较方法关于指纹建立存储开销的计算模型,而本实验主要说明随着模型参数的

变化,SEE 方法在不同网络场景下与已有方法的优势度比较情况,参数包括系统运行时间、攻击规模、溯源网络规模、底层路由规模和溯源路由器类型等.鉴于 SEE 支持区域化部署和管理,而比较方法都不支持,为了方便比较,本实验选择 CAIDA 数据的 7018 自治域作为支撑溯源网络的底层 IP 拓扑(不涉及跨域溯源),其中,每个路由器可直连多台主机.此外,本文提出了溯源记录比的概念,即溯源路由器记录指纹痕迹数量与转发 IP 包数量比值.

第 1 组实验用来说明随着系统运行时间的变化(以 s 为单位),全网溯源路由器平均溯源记录比的变化情况,结果如图 8 所示,其中,所有底层网络路由器被升级为溯源路由器(即溯源网络规模与底层网络完全相同),每个底层路由器都直连两台主机,攻击规模为 80%.与已有的基于图着色的单包溯源方法(HIT 和 S3T 方法)相比,SEE 方法的溯源记录比随着运行时间的逐渐增大而不断地降低,甚至能够减到不足 2%.此外,由于 SEE 方法的存储开销主要集中在溯源网络建立的时间内,因此在实验初始阶段,它的记录概率要高于 HIT.但是一旦溯源网络完成建立,SEE 就无需存储新的追踪痕迹,因而溯源记录比就会一直降低,这也证实了第 2.1.1 节的分析结果.

第 2 组实验用来说明随着攻击规模(即攻击主机占所有主机数量的比例)的增大,全网溯源路由器平均溯源记录比的变化情况,结果如图 9 所示,其中,所有底层网络路由器被升级为溯源路由器,每个底层路由器直连两台主机,系统运行时间为 32s.随着攻击规模的增大,SEE 和 S3T 方法的溯源记录比没有增长,反而降低了.其原因是攻击主机越多,意味着主机之间发送请求数据的概率越少,进而减少了溯源网络产生的路径数量,降低了存储开销.这也进一步说明,SEE 的存储开销只与溯源网络的规模有关,而与网络中转发包的数量无关.

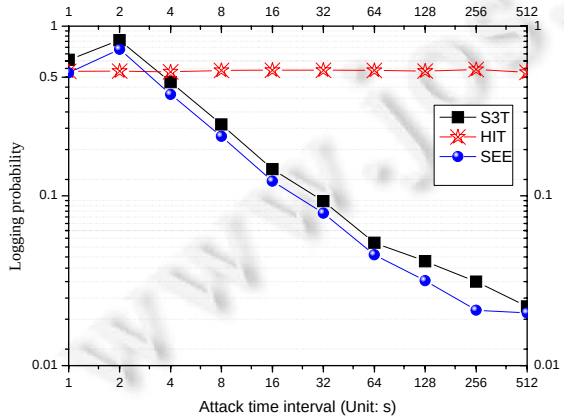


Fig.8 Traceback logging probability at different attack times

图 8 不同攻击时间下溯源记录比

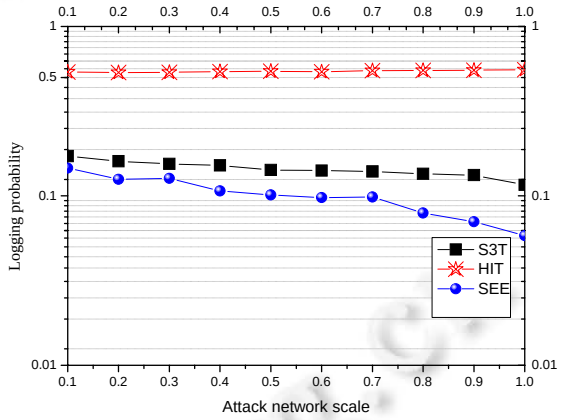


Fig.9 Traceback logging probability on different networks

图 9 不同路由网络规模下溯源记录比

第 3 组实验用来说明随着底层路由规模(即连接底层路由器的主机数量,以台为单位)的变化,全网溯源路由器平均溯源记录比的变化情况,结果如图 10 所示,其中,所有底层网络路由器被升级为溯源路由器,系统运行时间为 32s,攻击规模为 100%.随着路由器连接主机数量的增加(即底层路由网络规模的增大),S3T 方法的溯源记录比也在不断地增长;然而 SEE 方法的增长幅度却很小,甚至几乎为 0.主要原因是,S3T 建立的追踪痕迹不但与路由路径的中间节点相关,而且与端节点也相关;而 SEE 建立的追踪痕迹只与中间节点相关,因此它的存储开销不受底层路由规模的影响,这也是 SEE 方法能够将存储开销降低为一个固定值的重要原因.

第 4 组实验用来说明随着溯源网络规模(即溯源路由器占底层路由器的比例)的增长,全网溯源路由器平均溯源记录比的变化情况,结果如图 11 所示,其中,所有底层网络路由器被升级为溯源路由器,每个路由器直连一台主机,系统运行时间为 128s,攻击规模为 100%.随着溯源路由器数量的增多,SEE 方法的溯源记录比在不断地增长,直至与 S3T 方法相同;而 S3T 方法的变化幅度始终很小;HIT 方法虽在减少,但最多也只能降低到 0.5 左右,其原因与第 3 组实验相同.该结果也从侧面表明:与传统方法相比,SEE 方法更具部署激励功能和扩展性.对于

ISP 来说,溯源系统的投入成本应该与其规模相匹配,即规模越大,投入成本越多;规模越小,投入成本越少.如此才能激励部署,而 SEE 方法恰好满足该条件,进而使它更适合大规模部署.

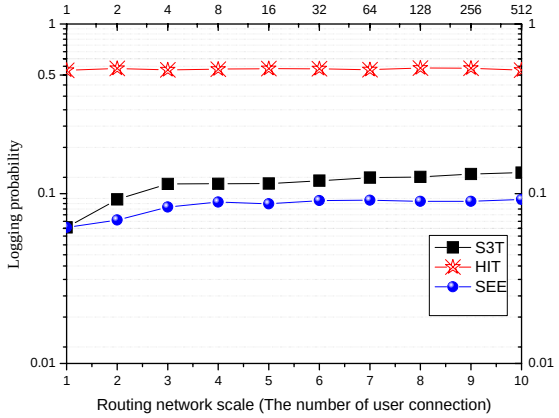


Fig.10 Traceback logging probability on different routing networks

图 10 不同底层路由网络规模下溯源记录比

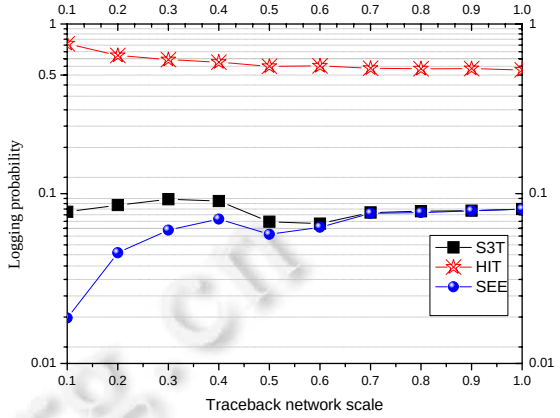


Fig.11 Traceback logging probability on different traceback networks

图 11 不同溯源网络规模下溯源记录比

第 5 组实验用来统计核心和边缘溯源路由器的溯源记录比,获得其补充累计分布函数,结果如图 12 所示,其中 80%底层网络路由器被随机升级为溯源路由器,每个路由器直连一台主机,系统运行时间为 128s,攻击规模为 100%.在基于 SEE 方法的溯源网络中,边界路由器(溯源节点度小于 2)的溯源记录比要远低于核心路由器(溯源节点度大于等于 2),其原因有两个:(1) 经过两种路由器的溯源路径数量差距较大;(2) 边界路由器只需记录路径出口,无需记录入口,而核心路由器两个方向路径都需记录.

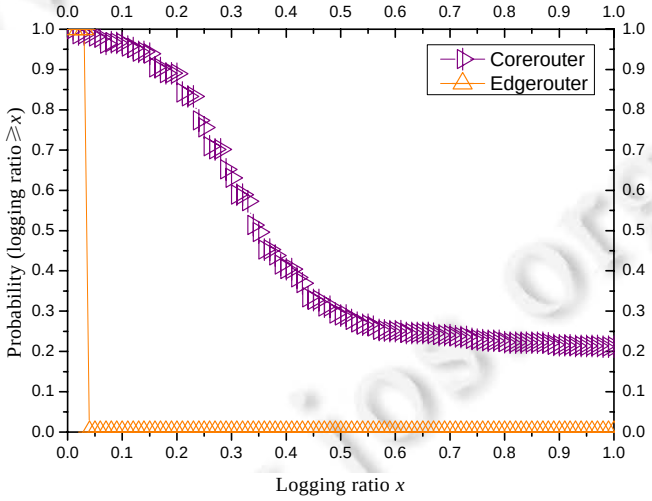


Fig.12 Complementary cumulative distribution functions of traceback logging probability

图 12 溯源记录比的补充累计分布函数

2.2.2 路径指纹提取开销

根据第 2.1 节可知,单包溯源方法的路径指纹提取开销不仅与攻击路径长度有关,而且与溯源网络的节点度大小相关.为此,本实验主要关注各个方法在面对不同长度的攻击路径时,其路径重构开销的变化情况.由于 SEE 方法不需要重构域间路由路径,而比较方法却需要,因此本实验选择面向 Transit-Stub 的多自治域网络拓扑

作为可支撑溯源网络的底层路由拓扑,其自治域的数量可达 50,其中,80%底层网络路由器被随机升级为溯源路由器,系统运行时间为 1 024s,攻击规模为 100%.

第 1 组实验通过搜集不同长度的攻击路径来统计出它的补充累计分布函数,结果如图 13 所示.在使用 Transit-Stub 拓扑搭建的攻击场景中,攻击路径的长度主要集中在 7~8 跳,9 跳路径已经较少,10 跳路径几乎没有.然而,由于 Transit-Stub 是一种具备层次模块性和幂律特性的拓扑结构,因此每个自治域路径长度通常不超过 4 跳,这也就意味着在本实验中,绝大部分攻击路径都是跨域路径.

第 2 组实验用来统计在不同攻击路径的重构过程中,被查询溯源路由器数量的变化情况,结果如图 14 所示.当攻击路径长度小于 4 时,比较方法所查询的溯源路由器数量几乎相同;当大于 4 后,HIT 明显要高于其他两个方法,主要原因是 HIT 除了路径节点以外,还需查询其邻居节点,而后者只需关注路径节点即可;此后,随着长度增大,S3T 所查询路由器数量基本呈线性增长,而 SEE 却几乎没变,甚至降低到 3,其原因是 SEE 通过域间匿名缓解策略来建立反匿名自治域联盟,从而使得受害者不经溯源即可确定攻击域,溯源过程也就进一步被集中在攻击域的内部.再结合上组实验结论可知,长度大于 4 的攻击路径绝大多数都属于跨域路径,这反而使得它的路径重构开销进一步降低.因此,相较于传统方法,SEE 更适合大规模溯源重构.

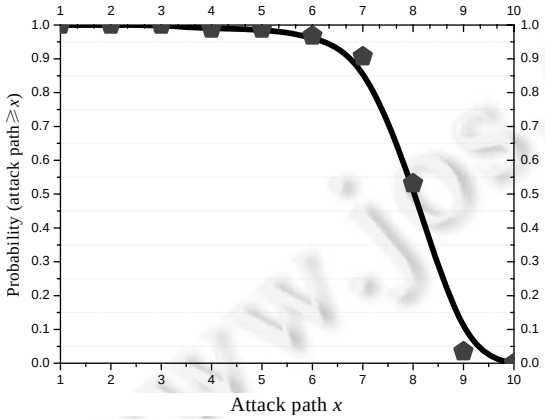


Fig.13 Complementary cumulative distribution functions of the attack paths

图 13 攻击路径的补充累计分布函数

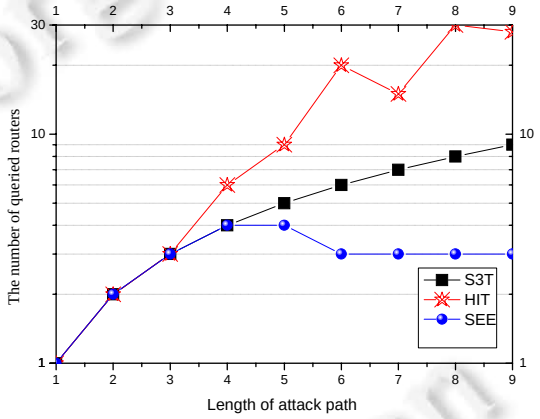


Fig.14 Number of queried routers during path reconstruction

图 14 路径重构所需查询溯源路由器的数量

3 相关工作介绍

英国剑桥大学的研究者[5]最早设计了一种能够同时兼顾存储开销、IP 包处理速度以及数据隐私的单包溯源系统,称为源路径隔离引擎(source path isolation engine,简称 SPIE).基本原理是:利用空间和时间效率较高的布鲁姆过滤器来压缩和存储 IP 包头中部分区分度较高的字段信息,进而建立指纹痕迹.在路径回溯过程中,采用半洪泛式溯源请求发送方式来逐跳搜索路径节点附近的指纹痕迹库,确定攻击路径.该方法虽然减小了存储开销(大约是转发包的 0.5%),同时解决了包特征直接记录而引发的数据隐私泄漏问题,但是它存在以下缺陷.

① 对溯源精度缺乏考虑,导致大量的正常主机被误认为是攻击源;

② 对网络拓扑隐私关注不足,导致经过域的网络拓扑泄漏;

③ 从网络全局看,路由器存储开销依然很大(在 OC-192 链路上,一个 32 口路由器,每秒转发量可达 40GB);

④ 路径重构过程会产生大量溯源请求,从而导致受害者带宽资源进一步被吞噬;

⑤ 不支持溯源节点动态加入致使溯源系统无法实时扩展;

⑥ 不可增量部署.

为了解决以上问题,学者们提出以下一些改进方案.

(1) 针对问题①,巴西帕拉纳联邦大学[6]提出了一种扩展的 SPIE 方法,简称 E-SPIE:首先,通过在原有特征

字段基础上添加 TTL 字段,使得溯源路由器所建立的指纹痕迹能够隐含路径节点时间序列,避免原有方法在某些特殊拓扑中出现误报;然后,通过在溯源路由器接口上单独设置指纹痕迹读写器,使得每个接口都能单独处理数据包,并行化建立指纹痕迹,降低计算开销.虽然 E-SPIE 扩大了 SPIE 的网络适用范围,但是没有从根本上解决存储开销大造成的溯源精度低问题.因此,问题①~问题⑥依然存在.

(2) 针对问题①、问题③和问题④,中国台湾中原大学的研究者[7]利用溯源路由器接口固定且数量有限的特点,提出了一系列基于接口编号压缩的单包溯源方法,简称 RHIT.它的基本原理是:通过逆模运算符来累积攻击路径链路编号,并将它们写入到标记域中.若发生溢出,就将其哈希值记录到路径指纹库.在攻击发生后,通过取模运算,从路径指纹库中提取指纹、确定上下游链路,拼接出攻击路径.与 SPIE 方法相比,该方法具备以下优势:每个溯源路由器最多只有 320KB 存储开销;溯源精度可达 100%;溯源请求发送数量降低到与路径长度相同.但是它有两个强假设条件:所有路由器必须全部开启溯源功能;每个溯源路由器接口只能连接一个网络设备.然而在多路访问网络中,每个接口可以通过二层交换机连接多个路由器,这意味着 RHIT 方法无法解决问题②、问题⑤和问题⑥.

(3) 针对问题①、问题③、问题④和问题⑥,本文作者和美国德州大学达拉斯分校研究者[8−10]利用溯源节点的地址不需要全网唯一标识的特点,提出了一种基于点着色的单包溯源技术,其核心是基于底层路由关系的溯源网络建立策略、基于 2-距离点着色的溯源地址分配策略、融合包标记和包记录的路径指纹建立策略以及基于溯源地址验证的路径重构策略.这类方法虽然在一定程度上降低了溯源开销、提高了溯源精度,但是在面对大规模网络时,它的溯源管理粒度较为单一,既与当前互联网的多级管理模式不相符,又会泄露网络拓扑隐私;不支持节点动态加入和退出,使得溯源网络无法动态扩展;溯源地址过长,造成路径指纹空间占用量以及指纹记录频率过大,最终影响了溯源系统整体开销;路径指纹建立低效,造成溯源路由器存储资源不足,只能牺牲溯源精度来换取存储资源.因此,该类方法并没有很好地解决问题①~问题③和问题⑤.

与已有方法不同,本文采用域间和域内相分离的层次化溯源系统架构模型,使得溯源系统能够被区域化部署与管理,从而彻底解决它们在面对大规模网络环境时溯源低效(问题①、问题③和问题④)和扩展性差(问题②、问题⑤和问题⑥)的问题,其中,域间网络通过出口边界过滤技术来建立反匿名联盟,域内网络通过扩展 OSPF 协议来构建域内溯源系统.对于网络服务提供商来说,高效的溯源方法既能保证服务质量(例如溯源精度、路径重构时间),又能减轻系统对底层网络的性能影响(例如存储开销、带宽开销),而可扩展的溯源方法则能够保证系统被大规模部署和推广.

4 结论及未来工作展望

针对当前互联网中存在的 IP 匿名活动,本文提出一种大规模网络下可动态扩展的高效单包溯源方法,即 SEE.该方法采用域间和域内相分离的层次化系统架构模型来弱化自治域之间的溯源联系,实现溯源系统的高效管理,其中,域间网络不经溯源就可直接识别攻击域,而域内网络则通过建立路径指纹库来重构攻击路径,最终确定攻击源.SEE 具有以下显著特征.

1) 构建基于 OSPF 协议的域内溯源网络,实现溯源节点的动态扩展;
2) 采用基于边着色理论的溯源地址分配策略来压缩地址空间,降低溯源存储开销;
3) 采用基于链路绑定的路径指纹建立和提取策略来改善溯源开销和溯源精度;
4) 构建基于对等关系的反匿名自治域联盟,避免溯源过程泄露自治域的拓扑隐私;
5) 实现域内到域间溯源的平稳过渡,排除非联盟成员引起的攻击域误报.

本文通过理论分析和实验仿真来验证 SEE 方法的高效性和可扩展性.结果显示,SEE 在系统规模不断动态扩大的条件下也能保证较好性能.其中,溯源存储开销只有 0.18MB,而溯源精度几乎高达 100%.此外,本文方法涵盖的主要操作都比较简单,不涉及太复杂的运算,对网络性能的影响都不会太明显,例如,域内溯源标记信息的提取和写入都可直接嵌入到路由器的解包和封包基本操作中;域间匿名过滤则采用已商业化且被广泛使用

的访问控制列表来实现;域内到域间的溯源过渡虽然需要攻击域加载轻量的 *Hash* 值,但是不需要受害域对每个到达包所携带的 *Hash* 值进行验证,它只需记录该 *Hash* 值即可.因次,本方法在工程操作方面也是可行的.

未来的研究工作主要包括:

1) 提出的方法虽然支持增量部署和溯源节点动态加入,但是缺少一种溯源位置优化策略,用来指明在底层路由网络上哪些路由器需要被优先升级为溯源路由器,而哪些路由器可以延后升级,从而使得系统规模无论如何变化,都能尽可能地为用户保证较好的溯源服务质量.
2) 提出的方法缺少部署激励机制:一方面,大量自治域即使不部署溯源功能也能享受溯源自治域为它们提供的溯源服务,产生"搭便车"问题;另一方面,溯源自治域采用无差别的路径指纹提取方式会给相关设备带来许多额外开销.因此,如何设计面向部署激励的单包溯源方法,成为溯源系统能否被 ISP 广泛部署的关键问题.

References:

[1] China information security doctor network. 2016. http://www.secdoctor.com/html/cygc/37794.html

[2] Xu K, Zhu L, Zhu M. Architecture and key technologies of Internet address security. Ruan Jian Xue Bao/Journal of Software, 2014, 25(1):78−97 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4509.htm [doi: 10.13328/j.cnki.jos.004509]

[3] Yu S, Zhou WL, Guo S. A feasible IP traceback framework through dynamic deterministic packet marking. IEEE Trans. on Computers, 2015,65(5):1418−1427. [doi: 10.1109/TC.2015.2439287]

[4] Yao G, Bi J, Vasilakos AV. Passive IP traceback: Disclosing the locations of IP spoofers from path backscatter. IEEE Trans. on Information Forensics & Security, 2015,10(3):471−484. [doi: 10.1109/TIFS.2014.2381873]

[5] Snoeren A. Single-Packet IP traceback. IEEE/ACM Trans. on Networking, 2002,10(6):721−734. [doi: 10.1109/TNET.2002.804827]

[6] Hilgenstieler E, Duarte EP. Extensions to the source path isolation engine for precise and efficient log-based IP traceback. Computer & Security, 2010,29(4):383−392. [doi: 10.1016/j.cose.2009.12.011]

[7] Yang MH, Yang M. RIHT: A novel hybrid IP traceback scheme. IEEE Trans. on Information Forensics and Security, 2012,7(2):789−797. [doi: 10.1109/TIFS.2011.2169960]

[8] Gong C, Sarac K. A more practical approach for single-packet IP traceback using packet logging and marking. IEEE Trans. on Parallel and Distributed Systems, 2008,19(10):1310−1324. [doi: 10.1109/TPDS.2007.70817]

[9] Lu N, Wang YL, Su S, Yang FC. A novel path-based approach for single-packet IP traceback. Security and Communication Networks, 2013,7(2):309−321. [doi: 10.1002/sec.741]

[10] Lu N, Wang SG, Shi WB, Yang FC. An efficient and precise approach for single-packet traceback. Ruan Jian Xue Bao/Journal of Software, 2017,28(10):2737−2756 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5149.htm [doi: 10.13328/j.cnki.jos.005149]

[11] Wang SG, Sun QB, Yang FC. Detecting SIP flooding attacks against IMS network. Ruan Jian Xue Bao/Journal of Software, 2011, 22(4):761−772 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3818.htm [doi: 10.3724/SP.J.1001.2011.03818]

[12] Moy J. OSPF Version 2. RFC 2328, 1998. http://www.ietf.org/rfc/rfc2328.txt

[13] Cooperative Association for Internet Data Analysis (CAIDA). Internet-Topology-Data-Kit. 2013. http://www.caida.org/data/active/internet-topology-data-kit/2013

[14] Stocia I, Zhang H. Providing guaranteed services without peerflow management. In: Proc. of the SIGCOMM'99. Boston: ACM Press, 1999. 81−94.

[15] Liu BY, Athanasios VV. Toward incentivizing anti-spoofing deployment. IEEE Trans. on Information Forensics and Security, 2014, 9(3):436−450. [doi: 10.1109/TIFS.2013.2296437]

[16] Siganos G, FaloutsosM, Faloutsos P, Faloutsos C. Powerlaws and the as-level Internet topology. IEEE/ACM Trans. on Networking, 2003,11(4):514−524. [doi: 10.1109/TNET.2003.815300]

[17] OpenSim. Omnetpp++: Objective modular network testbed in C++. 2013. http://www.omnetpp.org/

[18] OpenSim. ReaSEGUI. 2012. http://i72projekte.tm.uka.de/trac/rease/

附中文参考文献:

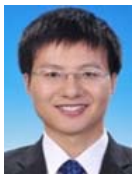
[2] 徐恪,朱亮,朱敏.互联网地址安全体系与关键技术.软件学报,2014,25(1):78−97. http://www.jos.org.cn/1000-9825/4509.htm [doi: 10.13328/j.cnki.jos.004509]

[10] 鲁宁,王尚广,史闻博,杨放春.一种高精度、低存储的单包溯源方法.软件学报,2017,28(10):2737−2756. http://www.jos.org.cn/1000-9825/5149.htm [doi: 10.13328/j.cnki.jos.005149]

[11] 王尚广,孙其博,杨放春.IMS 网络中的 SIP 洪泛攻击检测.软件学报,2011,22(4):761−772. http://www.jos.org.cn/1000-9825/3818.htm [doi: 10.3724/SP.J.1001.2001.03818]

鲁宁(1984－),男,内蒙古包头人,博士,副教授,主要研究领域为网络安全.

史闻博(1980－),男,博士,教授,博士生导师,主要研究领域为应用密码学,信息系统安全,大数据安全及隐私.



王尚广(1982－),男,博士,副教授,博士生导师,CCF 高级会员,主要研究领域为服务计算,移动云计算,车联网,网络安全.

杨放春(1957－),男,博士,教授,博士生导师,主要研究领域为通信软件,网络安全,网络智能化.

李峰(1978－),男,博士,讲师,CCF 专业会员,主要研究领域为机会网络,信任管理.