可扩展性增强的动态确定包标记溯源方法

鲁 宁[1),2)] 张嘉伟[2)] 马建峰[2)] 丛 鑫[3)] 史闻博[1)] 王尚广[4)]

[1)](东北大学信息科学与工程学院 沈阳 110819)

[2)](西安电子科技大学计算机学院 西安 710071)

[3)](辽宁工程技术大学电子与信息工程学院 辽宁 葫芦岛 125105)

[4)](网络与交换技术国家重点实验室(北京邮电大学) 北京 100876)

摘 要 僵尸物联网的出现使得拒绝服务攻击(Denial of Service,DoS)的破坏力进一步升级,而源地址伪造是导致DoS攻击一直难以被有效防御的重要原因.为此,研究者提出了可追踪匿名攻击源的IP溯源技术.在已提出的众多IP溯源方法中,动态确定包标记溯源因轻量、高效且易部署等特点,一经提出就立刻受到人们广泛关注.然而,现有方法在面对大规模攻击时仍存在因溯源规模受限、负载过于集中而引发的可扩展性问题.基于此,本文提出一种可扩展的动态确定包标记溯源方法,SEEK.一方面通过设计层次化的溯源联盟体系结构和动态调整包标记概率来均衡溯源设备负载,避免因性能瓶颈而制约系统的可扩展性;另一方面通过动态扩展标签装载域、分层复用标签空间和自适应管理标签来提高标签的可使用量和利用率,避免因标签资源不足而引发溯源规模受限,进而制约系统的可扩展性.通过理论分析和基于大规模真实拓扑的仿真实验,结果表明:相比以往同类典型方案,在绝大多数攻击场景下SEEK在扩展性和高效性方面都能提高20%以上.

关键词 IP匿名;IP溯源;动态确定包标记溯源;可扩展

中图法分类号 TP301 **DOI号** 10.11897/SP.J.1016.2020.01493

A Scalable IP Traceback Approach Employing Dynamic Deterministic Packet Marking in the Large-Scale Networks

LU Ning[1),2)] ZHANG Jia-Wei[2)] MA Jian-Feng[2)] CONG Xin[3)] SHI Wen-Bo[1)] WANG Shang-Guang[4)]

[1)](*School of Information Science and Engineering, Northeastern University, Shenyang* 110819)

[2)](*School of Computer Science and Technology, Xidian University, Xi'an* 710071)

[3)](*School of Electronic and Information Engineering, Liaoning Technical University, Huludao, Liaoning* 125105)

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

Abstract With the development of the Internet of Things (IoT), more and more IoT devices have been connected to the Internet. Everything has two sides and IoT is not an exception. It has brought convenience to people's lives, but also creates a series of issues. For example, attackers can exploit the fragile security and closure of IoT to disrupt the network activities. Denial of Service (DoS) attacks are typical cyber attacks in which the perpetrator seeks to make a machine or network resource (e.g., bandwidth) unavailable to its intended users by temporarily or indefinitely disrupting the legitimate services of a host connected to the Internet. Generally speaking, DoS attacks are launched by thousands of attackers that attempt to overload the system with lots of useless requests. IP spoofing is a common trick in DoS attacks, which can not only

收稿日期:2018-09-13;在线发布日期:2019-07-17.本课题得到国家自然科学基金(61601107,U1708262,61602227)、中国博士后科学基金(2019M653568)、河北省自然科学基金(F2020501013,F2015501122,F2015501105)、中央高校基本科研业务费项目(N2023020)资助.

鲁 宁,博士,副教授,主要研究方向为网络安全.E-mail:luning@neuq.edu.cn.**张嘉伟**(通信作者),博士研究生,主要研究方向为信息安全.E-mail:zjw8512@126.com.**马建峰**,博士,教授,长江学者特聘教授,主要研究领域为信息安全.**丛 鑫**,博士,副教授,主要研究方向为网络安全、网络管理.**史闻博**,博士,教授,主要研究领域为信息安全.**王尚广**,博士,副教授,主要研究方向为服务计算、服务安全.

conceal their locations, but also bypass the defence mechanism. The attacker hides its own IP address and forges the source address, so that the victim cannot identify the locations of those attackers. Quite obviously, such technique makes the DoS attacks become more destructive than before, and difficult to control defense. For this reason, the IP traceback technology has been extensively researched and developed already, which is responsible for disclosing the attack sources. Among these existing IP traceback approaches, the dynamic deterministic packet marking traceback approach termed as DDPM has attracted great attention due to its light weight, high efficiency, and ease to deployment. Its main idea is to make use of the abnormal flow detection system that has been widely deployed on the Internet to establish the audit trails and further traceback to involved attack source. Only when the monitor notices a surge of suspicious network flows, it will apply for a private and unique mark from a globally shared MOD server, and insert it into the suspicious packets' header. At the same time, the MOD server establishes and maintains the mapping relationship between the marks and their related requesting IP addresses. Once detect the DDoS attack, the victim extracts the marks from attack packets and further obtains the attack sources by requesting the MOD server. Although DDPM uses the marking space in a round-robin style to improve the salability, in the face of the large scale networks, it still suffered the following disadvantages: the small number of traceable sources and the load imbalance. Therefore, this paper proposed a scalable dynamic deterministic packet marking approach, termed as SEEK. In order to overcome these drawbacks, SEEK first designs a hierarchical architecture for the traceable alliance and dynamic probabilistic packet marking to balance the load of the relevant traceback devices, and then employs a number of techniques, such as the expansive label-loading space, the reuse label space, and the adaptive label management, to increase the number of available labels and improve their utilization. We perform extensive mathematical analysis and simulations to evaluate our approach. The results show that our approach significantly outperforms the prior apporaches in termes of the scalability and efficiency by more than 20 percent.

Keywords IP anonymous; IP traceback; DDPM; scalability

1 引 言

近几年随着物联网(Internet of Things,IoT)的快速发展,大量廉价的、支持不间断持续工作的 IoT 智能设备(例如摄像头和监视器)正不停地接入互联网.然而,脆弱的安全性和封闭性使得它们成为黑客争相夺取的资源,进而催化了僵尸物联网的产生,而这又为大规模拒绝服务攻击(Denial of Service,DoS)的发起提供了便利条件.2016 年 10 月 21 日,美国顶级域名解析服务提供商 Dyn 就曾遭到一次由 Mirai 僵尸物联网驱动、跨越多个自治域(Autonomous System,AS)、涉及千万级 IP 地址的 DoS 攻击,使得整个东海岸地区网络瘫痪长达 4 个小时之久.随后,德国电信也遭到相似攻击,导致 90 万台路由器下线,近 100 万用户家庭网络服务中断①.通过观察,发现此类攻击有一个明显特征:攻击包的源地址大都被伪造.这不仅造成 IP 数据流分类困难,使得恶意流无法在中间网络被准确地检测和过滤,又造成攻击源追溯困难,使得僵尸网络无法被有效隔离.因此,在攻击发生后,如何有效地抵制源地址伪造就成为 DoS 攻击防御的首要任务.

动态确定包标记溯源(Dynamic Determinic Packet Marking,DDPM)技术正是为解决上述源地址伪造问题而被提出的[1-2].DDPM 是一种典型的基于标签认证的事中追踪方案,其核心思想是:利用当前互联网已经广泛部署异常检测系统的优势,让每个发现可疑匿名流的源端节点都可申请一个私密的、唯一的密钥标签,同时建立和维护该标签与其网络前缀的映射关系,为攻击源追踪做准备.具体溯源流程为可疑网络负责添加标签,而受害端网络负责提取攻击报文的标签,通过检查映射关系进而识别

① http://web.tierpoint.com/radware-ert-2016-2017-report-w

攻击源.与传统 IP 溯源方法(例如 PPM 等[3-15])相比,DDPM 具备以下优势:(1)除了攻击源追踪,还能够重新构建 IP 流标识,为安全设备能够准确地检测和过滤恶意流提供支持;(2)既不需要在匿名行为发生前就开始生成路径片段,也不需要在发生后通过收集片段而重构路径,从而有效地减少了溯源系统对底层网络性能的影响;(3)不仅部署成本较低(只需升级路径入口路由器),且支持增量部署,降低实际部署难度.基于此,DDPM 一经提出,便立即受到广泛关注.

除了源地址伪造,由僵尸物联网驱动的 DoS 攻击还表现出攻击源分布广(可跨越多个自治域)、数量多(可达数万级别)以及攻击时间长(多达数个小时)等特点,然而已有的 DDPM 方法在面对这种大规模 DoS 攻击时存在因标签资源受限和性能缺陷而造成的可扩展性不足问题,具体表现为:(1)攻击源的不确定性决定了溯源系统必然是一种开放式分布控制系统.然而,已有 DDPM 采用单一、细粒度的操作方式和集中化的标签管理方式,使得标签需求量和标签分配中心负载随着攻击规模的增大而迅速增长,影响了系统可扩展性;(2)包标记固然轻量,但也会给参与路由器带来额外操作开销,进而影响数据包转发速率.已有 DDPM 不顾该消极影响,以全概率方式标记每个数据包.一旦参与路由器数量过多,就会影响底层网络的传输性能,进而影响溯源规模;(3)为了使系统能在当前互联网协议下运行、降低部署成本,IP 溯源大都通过重载少量闲置包头字段来定义标签装载域.鉴于不同网络所承载业务类型不同,它们的闲置字段也不尽相同.然而,已有 DDPM 没有考虑底层网络的异构性,通过静态方式来选定装载域,使得域空间无法依据网络类型而快速扩展,而有限的空间无法承载足够多的标签资源,进而限制溯源规模;(4)虽然包头重载限制了标签数量,但是已有 DDPM 并没有设计合理的标签管理策略来提高其利用率.一方面标签回收过快会引发震荡攻击(攻击者通过调节流量模型,诱使源端网络重复检测、反复申请标签,耗尽标签分配中心的计算资源,使其发生服务拒绝),降低系统可靠性,另一方面标签回收不及时会影响其再分配和再利用,进而制约溯源规模.

针对上述挑战,本文提出一种可扩展的动态确定包标记溯源方法(Scalable dynamic dEtErminic pacKet marking,SEEK).首先,立足于真实网络多层次、多粒度的体系结构,借鉴 IP 地址分层复用思想,通过划分标签空间,采用层次化的、粒度可调的溯源标签管理体系结构,既能通过网络分治,解决集中管理带来的服务瓶颈问题,又能通过粒度调整,有效控制标签作用范围,缓解其过度申请问题.其次,分析当前网络路由协议的真实运行情况,依据各级联盟自身网络 IP 包头的实际装载,自适应扩大标签装载域空间,提高标签分配数量,增大溯源规模;然后,建立由 CPU、内存和数据流到达率共同组成的负载评价函数,通过实时评估溯源节点负载状况来计算标记概率,以此为基础,设计一种动态标记策略,降低溯源系统对网络性能的影响;最后,通过分析攻击过程中包标记操作执行速率的变化特征,采用移动平均线与最近最少使用相结合的理论来评估攻击持续时间,进而判定标签回收时机,提高其利用率.

为了验证本文提出的 SEEK 方法,首先对其可扩展性进行了理论分析,然后在基于真实拓扑的攻击场景中对其进行了实验验证,并与其它经典方法进行了对比.结果表明 SEEK 不仅延续了传统方法的优势,且通过改善标签分配数量、标签利用率和包标记操作开销,将溯源规模等指标提升了至少 20%.

本文第 2 节介绍相关工作和研究动机;第 3 节介绍本文方法所依赖底层网络的结构特征;第 4 节介绍本文提出的 SEEK 方法,其中 4.1 节给出方法的整体框架,4.2 节～4.6 节分别介绍标签域重载策略、动态标记策略、标签管理策略、安全策略、可靠性策略等设计细节;第 5 节对 SEEK 的性能进行评估,其中 5.1 节给出理论评估,5.2 节则采用实验仿真手段对分析结果进行补充;第 6 节总结全文并指出下一步的工作重点.

2　相关研究

源地址伪造(也称 IP 匿名)是 DoS 攻击惯用手段之一,截至目前已有不少反匿名技术被提出,特别是清华大学的吴建平、毕军和徐恪团队[15-18]、国防科技大学的卢锡城团队[19]、北京交通大学的张宏科团队[20]为该领域提出了许多卓有成效的解决方案,为包括本文在内的研究奠定了良好的基础.

按照防御行为的先后顺序,已提出的反匿名方法可以划分为预防和响应两类,其中预防的目的是阻止匿名行为的发生,经典方法有源地址认证[16-17,21]、身份与位置分离[20]、出入口边界过滤[18,22]、权证[23]、反向路由验证[24]和基于路由的伪造包过滤[25]等,而响应的目的是在匿名攻击发生后减少它可能带来的

伤害,经典方法有路径标识[26]、基于生存时间的包过滤[27]和 IP 溯源等.后者是前者的重要补充,原因是:首先,部分预防方法(例如 IP 地址空间分层、源地址认证和权证)采用"革新型"研究思路,认为只有从根本上改进和更新现有的互联网协议,才能彻底解决 IP 匿名问题.因此,它们更适合封闭式网络或下一代互联网.而响应方法则大都采用"改良型"研究思路,认为既然现有的互联网协议已经稳定运行了几十年,一旦轻易地变革必然会导致设计和部署上的巨大开销.因此,仅就这部分预防方法来说,在下一代完全可信任的互联网到来之前响应方法研究都将非常重要;其次,虽然也有部分预防方法(例如出入口边界过滤、反向路由验证和基于路由的包过滤)采用了"改良型"研究思路,但是考虑到网络服务提供商(Internet Service Provider,ISP)必然会通过衡量自身利益来决定是否部署,因此反匿名网络的建立必定是一个漫长的、逐渐建立的过程.而在此过程中,位于该网络之外的攻击者依然会逍遥法外,而响应技术则正好可用于识别攻击流和揭露攻击者,进而对其进行阻断和依法处罚.更进一步,即使反匿名网络完全建立之后,由于恶意自治域的存在以及预防技术的自身缺陷(例如面向接入网络和 AS 内部网络的预防技术会因操作粒度过细而导致部署和操作开销巨大等问题,进而可能不被 ISP 广泛接受,而面向 AS 之间网络的预防技术又会因操作粒度过粗而无法应对位于 IP 前缀和 IP 地址层面的匿名问题),攻击者仍能发动大规模匿名攻击,而响应技术正好可以填补这种漏洞,及时地保护受害者.综上所述,响应方法在当前网络安全领域中依然具有非常重要的理论研究价值和现实意义.

本文主要关注响应方法中的 IP 溯源技术.与其它响应技术侧重于解决受害网络端的攻击流识别和过滤问题不同(例如路径标识和基于生存时间的包过滤等),IP 溯源侧重于解决攻击源定位和攻击流过滤问题.需要说明的是,本文不关注攻击路径还原,而关注攻击源定位,原因如下:仅就 DDoS 防御来说,发现攻击包的实际发送源要比还原它的传输路径更加重要;只要能定位攻击源,ISP 理论上就能通过搜集路由表来还原整条攻击路径.IP 溯源基本思路是源地址伪造大都始于终端结点,中间转发节点通常不参与伪造,因此借助它们处理匿名包的契机来建立终端位置指纹,以此替代源地址位置标识.迄今为止,已有数种 IP 溯源方法被提出.按照位置指纹建立的时间顺序,已提出的溯源方法可分为事前、事中和事后三类,其中事前是在攻击发生前就开始无差别地建立指纹信息,为受害者能够随时定位任一攻击源做准备,经典方法有包记录[5-10]、概率性包标记[11-12]、确定性包标记[13]和数据流采样[14-15]等;事中是在源网络端检测到可疑数据流后才开始有选择性地建立指纹信息①,使受害者能够有针对性地定位攻击源,经典方法有动态确定性包标记[1-2];事后是在攻击发生后通过提取上下游数据流的速率变化特征来充作指纹信息,使受害者能够有效定位攻击源所在区域网络,经典方法有控制洪流测试和入口流量测试等.与事前和事后相比,事中方法具备以下优势:(1)较小的溯源开销.既不需要实时、无差别地建立指纹信息,也不需要通过路径重构来识别攻击源,有效地减少溯源存储、计算、协同通信开销;(2)较低的部署难度.只需升级少量边缘路由器,支持增量部署,降低实际部署难度;(3)较高的溯源精度.即使攻击源隐藏它的流量特征,也不会影响指纹信息的正确性,降低溯源精度;(4)多重作用.所建指纹除了可充作攻击源的位置标识,还可充作攻击流的身份标识,这就为安全设备能够准确过滤提供了支持.因此,事中溯源方法更适合防御规模较大、具备隐藏特性的复杂 DoS 攻击.

动态确定性包标记 DDPM 是当前主流的事中溯源方法[1-2].其基本思路是:一旦源网络端的边界路由器检测到任何可疑行为,立即申请一个私密的、唯一的密钥标签,并将它写入已重载的、每个转发包的 Identification 字段,以充作源地址的位置标识.待确定攻击后,受害者依据标签就可识别出标记路由器.图 1 给出 DDPM 的具体操作过程:(1)边界路由器 R_j 一旦检测到可疑流,就检查它是否已被标记.如果是,则忽略它,不做任何操作;否则,向标签分配中心(Marking On Demand server,MOD)申请标签;(2)MOD 服务器回复标签申请且记录一对映射信息(分配的标签,R_j 的地址,时间戳)到数据库;(3)R_j 将分配的标签写入可疑的数据流包头中;(4)鉴于攻击流的聚集效应,越靠近受害网络的下游边界路由器 R_i 越能准确地检测到攻击.一旦发现攻击,R_i 携带已识别的标签立即向 MOD 服务器发起

① 虽然 DDoS 的攻击主机通过模拟正常流量模型能够隐藏流量特征,但是在源自治域的边界仍能捕获些微异常.例如已有研究[28-29]通过观察发现,攻击发生前后进出源自治域边界的数据流比例会发生变化.而且鉴于不同自治域中僵尸主机的数量服从齐夫分布,每当攻击发生,那些拥有较多僵尸主机的自治域从整体上也会显现较为明显流量异常特征.此外,此类方法并不要求较高的检测准确度,只要发现疑似攻击流即可.

确认申请，同时向受害域的系统监视器发送攻击标签通知；(5) 监视器向 MOD 发起探求与受害标签相对应的路由器溯源请求；(6) MOD 服务器通过查验数据库返回 R_j 的地址. 通过分析，不难发现 DDPM 方法存在以下问题：(1) 没有依据底层网络类型来灵活扩展重载字段，加剧了标签资源的短缺；(2) 没有设计合理的标签管理策略，使得本就短缺的标签资源过度消耗；(3) 没有限制中间节点的参与程度(无论检查，还是标记，都需逐包处理)，使得本就因攻击流汇聚而业务繁忙的路由器负载加重；(4) 没有考虑 MOD 服务器过度负载的情况，存在因请求太多而拒绝服务的可能. 这些问题制约了 DDPM 的可扩展性，进而影响了它对僵尸物联网驱动 DoS 攻击的防御效果.

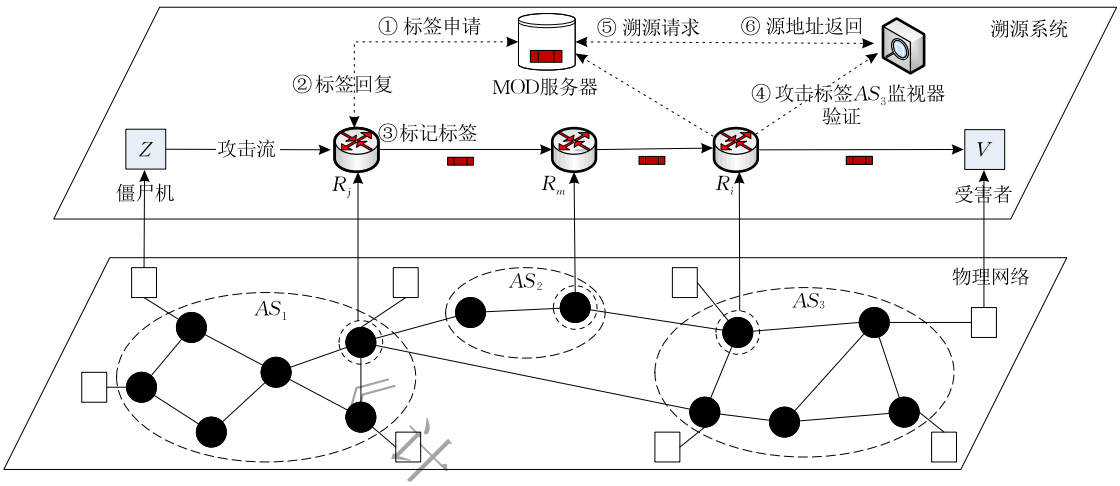

图 1　动态确定性包标记方法的基本框架

针对上述问题，本文希望在继承原有方法优势的前提下，一方面通过动态扩展标签装载域、分层复用标签空间和自适应管理标签等手段来提高标签的可使用量和利用率，避免因标签资源受限而制约系统的可扩展性；另一方面通过构建层次化的体系结构和动态调整包标记概率来减轻溯源设备(包括 MOD 服务器和标记路由器)的计算开销，避免因性能缺陷而制约系统的可扩展性. 本文作者在文献[7]提出一种可动态扩展的高效单包溯源方法 SEE，它与 SEEK 截然不同，主要体现在以下几个方面：SEEK 仅用于 DoS 防御，而 SEE 除了防御 DoS，还用于 IP 指纹取证；SEEK 采用确定性包标记技术，只需入口路由器执行包标记操作，而 SEE 采用反向路由记录技术，需要溯源路由器记录 IP 包的路由转发状态；SEEK 是在事中建立指纹，而 SEE 在事前建立指纹.

3　预备知识

IP 溯源是一种建立在底层路由网络上的开放式分布控制系统，它的设计必然依赖于底层网络的拓扑结构. 本节重点阐述与本文所提方法相关的互联网路由拓扑特征——多粒度和层次性.

3.1　多粒度

互联网规模的不断增加给它的路由管理带来了巨大挑战. 为此，管理者们广泛采用了分治策略来降低互联网路由管理的复杂度，增强系统可扩展性. 所谓分治就是将互联网划分为若干区域，每个区域可单独实现路由管理. 鉴于 IP 地址兼具位置和身份的双重标识，不同位置的区域都被分配了属于自己的地址块. 基于此，区域也可理解为是一个连接单个或多个 IP 前缀的群组. 依据 IP 包头载入原则，对于所有从区域内发送的 IP 包，其源地址必然隶属于该区域所分配的前缀群组，如性质 1 所述.

按照分治区域的粒度，当前互联网可划分为接入网、自治域(Autonomous System，AS)和联盟，其中接入网是互联网路由的入口，主要任务是将终端用户的数据流按照业务分类传输到不同的骨干网，常见协议有 FTT 和 ADSL. 从骨干网的角度来看，接入网就是一个与用户直接连接的 AS 边界路由器；AS 是互联网的基本组成单位，其内的路由器由一个 ISP 来统一管理，且全部运行同一 IGP 路由协议，例如 OSPF，它更容易依据其自身技术、经济能力和用户需求进行统一的优化配置，拓扑结构也更稳定；联盟是由多个 AS 组成的网络，在外界看来，它其实就是一个规模较大的 AS. 不过，它内部运行方式与 AS 不同. 首先，联盟内部 AS 之间运行 EGP 路由协议，例如 BGP；然后，联盟由多个 ISP 共同维护，其拓扑结构会因 AS 之间松耦合的关系(例如隶

属、自身策略、经济、政治、军事等)而时常变化.

依据上述网络划分粒度,从 IP 溯源的角度来看,攻击源也可分为攻击联盟、攻击 AS 和攻击边界路由器三层,其中联盟的地址块包含 AS 地址块,而 AS 地址块又包含边界路由器地址块.与此对应,溯源过程应该先追踪攻击联盟,再追踪攻击 AS,最后为攻击边界.

定义 1. 区域定义为无向图 $G_1=(V,E,A)$,其中节点集 $V=\{v|v$ 是 G 中路由节点$\}$,边集 $E=\{(u,v)|u,v\in V\}$,前缀集 $A=\{a(v)|a(v)$是节点 v 的前缀地址$\}$.

定义 2. IP 数据流定义为一个三元组 $F=(s,i,d)$,其中 s 表示发送区域,i 表示所携带源地址,d 表示目的区域.

性质 1. 给定区域 $G_1=(V,E,A)$和 IP 数据流 $F=(s,i,d)$,如果 $\forall s=v,v\in V$,那么 $i\subset a(v)$.

3.2 层次性

在互联网中,不同 AS 的网络规模悬殊,这就造成它们不平等的路由地位,进而产生层次型的互联结构.所谓层次结构就是将同一粒度的 AS 从下到上划分为多个层次,如图 2 所示.越靠近用户的 AS,其层次越低;越靠近核心网络的 AS,其层次越高.最底层的 AS 称为 Stub,底层以上 AS 统称为 Transit,其中 Stub 负责转发发送源是自己或者目的地址是自己的 IP 包,而 Transit 负责中转.AS 之间的路由选择依赖于它们的商业关系.常见的商业关系主要划分为 3 类:客户-提供者关系 C2P(提供者允许客户通过它到达其他网络,并根据流量收取费用),对等体-对等体关系 P2P(两个自治域之间相互可达,连接产生费用共同承担)和同胞-同胞关系 S2S(两个同属于一个管理机构的自治域之间相互可达,不计费用).分析上述关系可知,无论是 AS 或联盟粒度的 AS,Transit 之间中转大都满足无底谷路由原则,即下层只能向上层或同层转发数据包,而且只要发送节点 u 和目的节点 v 在同一 AS 或其下层

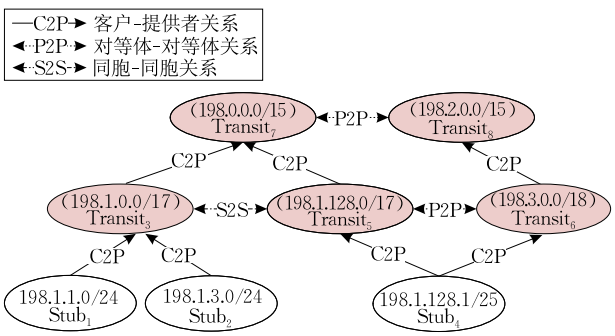

图 2 层次型区域网络模型

AS,u,v 的整条路由路径就都在这一范围内,如性质 2 所述.

定义 3. 层次型 AS 网络定义为有向图 $G_2=(N,L,I)$,其中节点集 $N=\{n|n$ 是 G 中 AS 节点$\}$,链路集 $E=\{(u,v)|u,v\in N\}$,属性集 $I=\{i(u,v)|i(u,v)$是链路(u,v)的类型,描述 AS 之间的商业关系$\}$.

定义 4. 给定 Transit p,范围覆盖 CM_p 表示由 p 及其所有直接或间接客户组成的 AS 集合,定义为一个二元组 $CM_p=\{p_{\text{trst}},t_v\}$.

性质 2. 给定层次型 AS 网络 $G_2=(N,L,I)$,若 $\forall$AS 节点 $u,v\in N$,$\exists CM_p$,s.t.,$u,v\in CM_p.t_v$,那么 u,v 的整条路由路径就都在 CM_p 范围内.

4 可扩展的动态确定包标记溯源方法

本文提出了一种扩展性增强的动态确定包标记溯源方法(Scalable dynamic dEtErminic pacKet marking,SEEK).本节将详细阐述本方法的设计思想和具体实现机制.本节组织结构如下:4.1 节将主要阐述 SEEK 方法的总体设计思路,其中 4.1.1 节介绍它的基本思想;4.1.2 节介绍它的体系结构;4.1.3 节举例说明它的执行过程.4.2 节重点阐述它的核心机制实现方式,其中 4.2.1 节介绍如何在标记路由器高负载的情况下完成包标记操作;4.2.2 节介绍如何在现有网络协议框架下设计可动态扩展的标签装载域;4.2.3 节介绍如何在标签资源不足的条件下回收标签;4.2.4 节介绍如何在开放式分布系统中保证通信的安全性;4.2.5 节介绍如何在标签分配中心高负载的情况下保证服务的可靠性等细节.

4.1 方法总体设计

SEEK 作为一种立足于实际网络体系结构的开放式协同控制系统,它必须既能够在不同自治域间协调工作,同时又保证不伤害底层路由网络的性能.从终端用户角度来看,整个溯源系统应该趋于透明,使它们无需关心任何实现机制就能受益;从系统设计角度来看,溯源系统应以尽量少的通信、存储和处理开销来获得最大限度的溯源实效.具体而言,本方法需要在技术和实施层面达到以下设计目标:(1)性能优化.一方面它应满足任何自治域的标签申请需求,使得它即使在面对大规模的 DoS 攻击时也能以较高的准确率完成溯源;另一方面它的包标记操作应简单轻权,尽可能给路由器带来较小计算开销,

不影响路由器的数据包转发速率；(2) 可靠性. 它的标签管理系统不仅需要提供 7×24 小时不间断服务，而且不会因申请数量过大、负载过重而引发服务质量下降问题；(3) 松耦合. 除了支持增量部署、允许自治域依据自身实际情况灵活部署外，还应保证各个自治域独立性，有效屏蔽网络结构或自身策略变化对底层路由的影响；(4) 安全性. 整个协同过程应安全可信，防止标签被截获、伪造等威胁的发生，增强系统的健壮性. 围绕上述目标，我们展开了对 SEEK 方法的设计.

4.1.1　基本思想

与传统方法无差别分配标签不同，SEEK 通过构建可分层溯源联盟、划分标签空间以及调整标签粒度来完成可重复、多粒度的标签分配，避免标签过度申请和 MOD 过度负载问题. 基于此，SEEK 系统被划分为三个功能层面：一是集中于溯源联盟构建的管理平面；二是完成标签申请、分配和标签验证、回溯的控制平面；三是实现包标记的数据平面. 接下来，我们分别从管理、控制和数据三个层面来阐述 SEEK 的基本思想.

在管理层面，SEEK 摒弃传统方法单一、扁平化的标签分配体系，遵从系统设计简单性和开放性原则，立足于真实网络多粒度、多层次的体系结构，引入联盟模式，建立一个以部署自治域为成员单位的溯源联盟，使只有联盟成员才享有标签申请和 IP 溯源的权利，进一步将所有成员自下而上划分为多层级溯源联盟，每一层级联盟都可抽象为一个整体接入更高层级联盟，构建一个层次化的溯源联盟. 本方法需要 MOD 服务器和 AS 监视器协同工作来完成溯源联盟的构建. 与传统方法不同的是，SEEK 方法给 MOD 服务器和 AS 监视器分别增加了新的职能：(1) 每个联盟都将配署一台 MOD 服务器，除了完成标签分配，还须对下完成本级联盟的成员信息管理，维护一张成员列表，表中记录所有成员前缀信息，对上完成与其他各层级联盟的成员交互；(2) 参与溯源联盟的每个自治域均配属一台 AS 监视器，除了发起溯源请求，还须完成自身注册以及控制和检测标记路由器的运行状态.

在控制层面，与文献[1-2]相同，SEEK 同样需要 MOD 服务器、标记路由器和 AS 监视器协同工作来完成标签申请、分配以及标签验证，其中标签验证、回溯过程与传统方法相同. 为了提高可扩展性，SEEK 采用了与传统方法不尽相同的标签申请条件和标签分配方法. 首先，标签申请除了依赖异常流量检测，还依赖匿名流检测. 后者利用性质 1 描述的 IP 包源地址与区域前缀所存在的隶属关系，使得每个边界路由器(即与用户接入网直接连接的 AS 路由器)都对转发包的源地址进行验证，若不满足关系，就说明该包就是匿名包，可以触发标签申请条件. 如此操作的优势在于：通过严格限定溯源的启动条件来减少不必要的溯源操作. 因为不是所有 DoS 攻击都使用源地址伪造(例如反射攻击和 Flash Crowd)，而引发溯源启动的唯一条件是发生匿名攻击. 然后，MOD 服务器不再使用无差别的标签分配方法，而是使用一种可分层的标签分配方法. 其基本思想是：借鉴 IP 地址分层复用原则，将标签空间依据溯源联盟层次映射为多层子空间，利用性质 2，通过匿名流的入口路由器-目的地址来预判所申请标签的联盟层次，进而在相应标签子空间中选取标签进行分配. 与传统方法不同，SEEK 的分配场景依据分层结构被扩展为 3 类：(1) 单一联盟内分配标签，匿名流的接收主机就位于该联盟(即最底层联盟内成员 AS 互为通信端)，该层 MOD 直接分配；(2) 跨联盟分配标签，匿名流的接收主机位于其他联盟(即隶属于不同层级联盟内成员 AS 互为通信端)，该层 MOD 向上层联盟提出标签申请，由上层 MOD 分配；(3) 非联盟分配标签，匿名流的接收主机不在最高层联盟内(即联盟内 AS 与其他非联盟 AS 互为通信端)，该层 MOD 拒绝分配. 此外，考虑到一旦跨层申请的标签数量太多，最高层的 MOD 就会再次产生标签短缺的问题. 毕竟分割标签空间只是提高了它的利用率，并没有增加它的总量. 为此，本文进一步设计了粒度可调的层次化标签申请方法. 一旦高层联盟 MOD 发现标签资源不足，就会调整追溯粒度，把少量来自同一 AS 或联盟的标签申请进行合并，也就是说属于同一 AS 或联盟的入口边界都将标记相同标签，这能极大减少标签需求量. 虽然上述方法无法达到精准溯源，会将溯源结果放大，即单个标签对应多个入口边界，但是这对溯源精度的影响在可接受范围内. 一方面该方法属于事中溯源，所有追溯到的入口边界必是匿名攻击源，因此不会出现漏报；另一方面被误报的入口边界也不会完全是正常源，至少是可疑攻击源. 上述方法的优势在于：(1) 通过分层管治、逐层配署，解决 MOD 服务器负载过重、服务性能下降问题；(2) 通过逐层划分标签空间、控制标签作用范围以及调整追溯粒度，解决标签资源不足问题.

在数据层面，与传统方法单一的包标记相比，

SEEK 按照匿名流的通信场景将标记路由器的包标记操作扩展为 3 类：(1) 单一联盟内部通信，标记路由器直接在匿名流的标签装载域中写入它向本层 MOD 已申请到的标签；(2) 跨联盟通信，在匿名流的标签装载域中写入它向上层联盟已申请到的标签；(3) 非联盟成员之间通信，无需写入任何标签，这样可以抵制搭便车的非成员域，在一定程度上缓解 DDPM 的部署激励问题. 需要说明的是：一方面虽然 SEEK 的每个标记路由器能够同时申请多个表示不同粒度的标签，但是这并不会造成资源浪费，相反会因下层联盟能够独立分配标签而提高标签重用率，节省资源；另一方面受整个联盟划分层次总数的制约(最多不超过 5 层，一般只有 2 层)，标记路由器所拥有标签数量不会太多，因此标签管理不会特别复杂，开销也不会过大.

定义 5. 溯源自治域定义为 $TS=(G_1,f)$，其中 $G_1=(V,E,A)$ 由定义 1 给出，f 是一种满足单射的 IP 指纹建立函数，给定 $v_i\in V$，$\exists f$，s.t.，$IP_{v_i}=f(v_i)$ 且 $v_i=f^{-1}(IP_{v_i})$，其中 v_i 为 G_1 中路由节点，IP_{v_i} 为 v_i 的 IP 指纹. 就 SEEK 来说，f 指标签申请和包标记操作，IP_{v_i} 指标签.

定义 6. 溯源覆盖范围定义为 $TCM_p=\{p_{\text{trst}},t_{TS}\}$，其中 $p_{\text{trst}}=CM_p.p_{\text{trst}}$，$t_{TS}\subseteq CM_p.t_v$，$CM_p$ 由定义 4 给出. $\forall$ 数据流 $F=(s,i,d)$，若 $F.s\in t_{TS}$，$F.d\in t_{TS}$ 且 $i\notin a(s)$，那么 $\exists f_p$，$v_i\in F.s$，s.t.，$IP_{v_i}=f_p(v_i)$ 且 $v_i=f_p^{-1}(IP_{v_i})$，其中 f_p 指 TCM_p 的 IP 指纹建立函数.

定义 7. 层次化的溯源联盟定义为 $TAA=\{TS_1,TS_2,\cdots,TS_n,TCM_{p_1},TCM_{p_2},\cdots,TCM_{p_m}\}$. $\forall$ 匿名流 $F=(s,i,d)$，若 $F.s=TS_i$，$F.d=TS_j$，那么 $\exists f_{pk}$，$v_i\in TS_i$，s.t.，$IP_{v_i}=f_p(v_i)$ 且 $v_i=f_p^{-1}(IP_{v_i})$，其中 f_{pk} 指满足最小覆盖 (TS_i,TS_j) 的 TCM_{pk} 的 IP 指纹建立函数.

4.1.2 体系结构

本文引入了联盟模式，把所有部署 SEEK 方法的自治域都看作联盟成员. 只有联盟成员才可向 MOD 服务器提出标签申请和溯源服务. 为了达到松耦合的目标，该方法除了允许非成员域或成员域在任何时刻都能选择注册或退出，还允许它们依据实际情况(路由策略、隶属关系、网络结构等)灵活选取划分原则和组合模式建立层次化的联盟体系结构，具体构建过程如下：首先，以靠近真实网络边缘的 AS(包括 Stub 和 Transit)为单位成员，遵循同属性相聚原则，将属性相近的 AS 聚合成多个最底层级溯源联盟；然后，以最底层溯源联盟为基本单位，依据相同属性聚合原则，形成离边缘网络较远的更高层溯源联盟；由此逐层向上构建一个嵌套式联盟结构，直至最高层联盟建立. 以图 2 描述的网络结构为例，构建出图 3 所示的层次化体系结构.

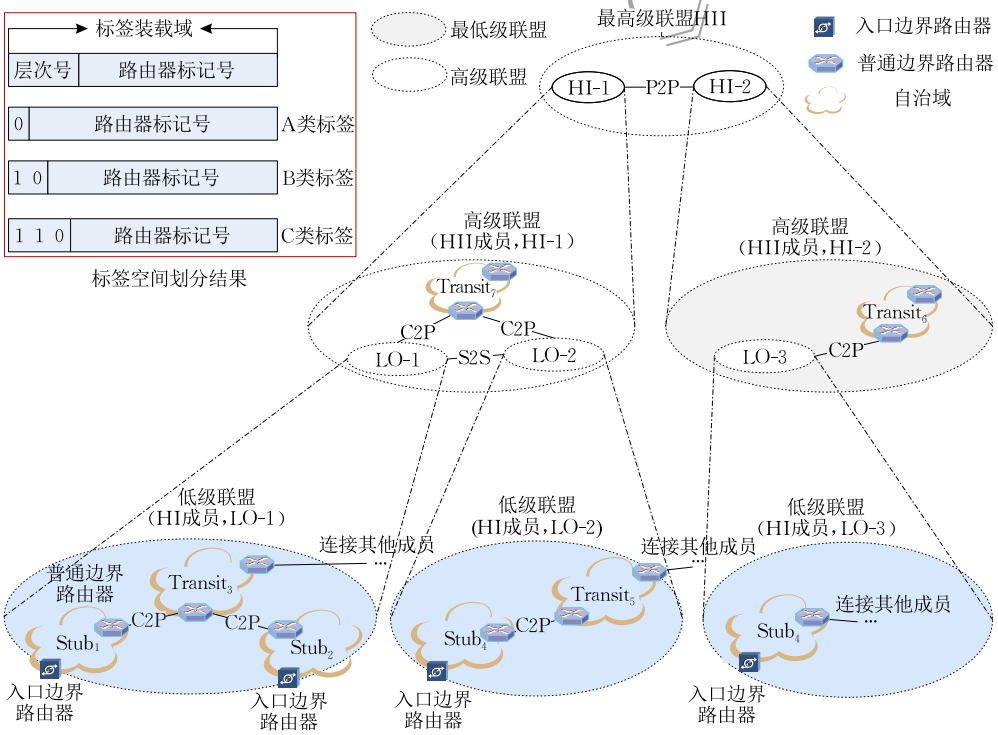

图 3 构建层次化的溯源联盟体系结构(溯源 2)

在层次化的溯源联盟体系中，标签装载域划分为层次号和路由器标记号两部分，其中前者表明该标签所作用的联盟层次，后者表明标签所作用的入口路由器. 如图 3 所示，鉴于联盟分为 3 个层次，标签空间也被划分为 3 类. 标签空间划分借鉴了 IP 地址分类的思想，因此与 IP 网络相似，所分配标签只需保证是通信双方最小覆盖网络的唯一标识即可，也就是说同一层次的不同联盟内部可分配相同的标签，而且定理 2 已经证明这并不会影响溯源精度，因此也就提高了标签重用率. 需要注意的是，标签的层次号由低层到高层逐渐递减，这就意味着前几类标签的数量要远多于后面的数量. 原因如下：因为前几类标签适用范围较大，一类标签甚至需要面向整个网络，而后面的标签只需小范围适用即可，所以我们通过增加前几类标签的数量来达到扩大溯源规模的目的. 每当位于低级联盟的边界路由器向所在联盟的 MOD 提出标签申请后，该服务器通过检查边界路由器的 Loopback 地址和匿名流的目的地址是否包含于它所维护的成员前缀列表，进而判定通信双方是否位于联盟内. 若是，直接分配该层联盟所对应的标签类型；反之，则向上层联盟 MOD 发起申请，开始新一轮的判断. 从底向上逐层申请，直到寻找到覆盖通信双方的联盟. 如若直至顶层也未找到，这就意味着目的 AS 尚未加入联盟，那么直接拒绝申请.

引理 1.　给定受害者 V_1，任给一个以 V_1 为目的地的攻击流 F_i，只要存在标签 L，使得它与 F_i 唯一绑定，那么 L 就具备追溯 F_i 入口路由器的能力.

证明.　假设存在另外一个标签 M，也能够追溯 F_i 入口路由器，那它就一定与 F_i 绑定，根据题设，L 与 F_i 是唯一绑定，那么 $M=L$.　　证毕.

定理 1.　在不影响溯源精度的前提下，目的地址不相同的攻击流可分配任意标签.

证明.　根据定义 2，数据流 $F_i=(s,i,d)$，其中 s 表示发送区域，i 表示所携带源地址，d 表示目的区域. 鉴于 i 可能被伪造，F_i 简化为 (s,d). 也就是说，只要溯源方法能够在传统网络上重新建立与 (s,d) 一一映射的数据流标识，就能在全网准确追溯任何入口路由器. 根据引理 1，在给定 d 的条件下，标签 L 可充当 s 的标识符. 也就是说 $F_i=(L,d)$. 任给 F_1 和 F_2，假设 $d_1\neq d_2$，且 $L_1=L_2$，那么 $F_1\neq F_2$. 只要 $d_1\neq d_2$，标签相同与否就不妨碍数据流标识作用，也就不影响溯源精度.　　证毕.

定理 2.　在层次化的溯源联盟体系结构下，只要将标签空间按照联盟层次划分，就能保证标签具备准确地追溯能力.

证明.　根据定理 1，对于目的地址不同的攻击流，随意分配标签都能保证溯源准确性. 对于目的地址相同、源不同的攻击流，只有分配不同标签才能保证溯源准确性. 为此，我们需证明通过划分标签空间能确保标签分发的唯一性. 在层次化的联盟体系中，给定受害者 V，所有与 V 通信的主机可分为以下 3 类：联盟内、跨联盟和联盟外. 联盟外的主机不用分配标签，故无需考虑，重点关注前两类. 依据标签划分原则，可得出两个结论：(1) 与 V 位于同一联盟的所有主机都被分配标记号不同的标签；(2) 与 V 位于不同联盟的所有主机都被分配层次号不同的标签. 因此，标签空间划分能满足标签唯一性，也能准确追溯.　　证毕.

4.1.3　方法举例

本小节以图 4 为例来说明 SEEK 方法是如何进行标签申请、分配、包标记和溯源验证等过程的. 我们选取图 3 中最底层(LO-1 和 LO-2)和其上一层(HI-1)的两层溯源联盟体系结构. 为了论述简便，我们不失一般性的假设标签长度为 8 位. 根据图 3 描述，整个标签由层次号和路由器标记号两部分组成. 已知整个标签空间依据联盟层次数被划分为 A、B、C 类，下两层分别配属 B 类和 C 类标签，其中 HI-1 是 B 类，其层次号为 10；LO-1 是 C 类，其层次号为 110；LO-2 也是 C 类，其层次号为 110. 因为 SEEK 允许同一层次的各个联盟独立分配标签，所以标签类型相同的 LO-1 和 LO-2 也可以分配相同的路由器标记号，这就使得不同标记路由器可能被分配相同标签. 不过，根据定理 2，这不会影响溯源精度. 基于此，本文不考虑这种场景，着重说明联盟内和跨联盟数据通信时控制和数据层面的处理过程. 为此，我们假设如下攻击场景：联盟 LO-1 内 Stub_1 的边界路由器 R_1 会接入一些僵尸主机，因本文只关注 IP 层溯源，故将所有接入 R_1 的僵尸机统称为攻击者. 攻击者发出的匿名流会同时攻击 V_1 和 V_2 两个受害者，其中 V_1 位于联盟 LO-1，V_2 位于 LO-2. 在以下实例中，MOD 服务器已完成了联盟成员注册和管理等管理层面工作，整个联盟进入稳定工作状态.

(1) Stub_1 的边界路由器 R_1 收到攻击主机向受害者 V_1 和 V_2 发出的数据包 p，利用 p 源地址与 Stub_1 网络前缀的隶属关系来检测匿名攻击的发生.

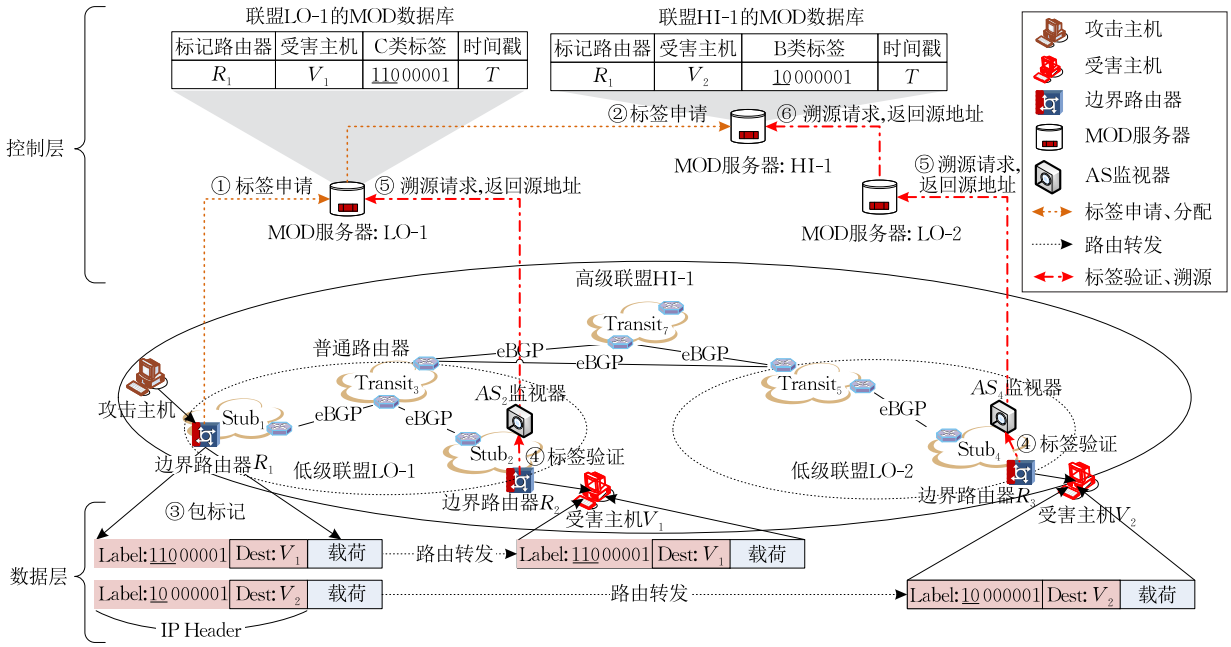

图 4 SEEK 方法的执行过程举例(源于图 3)

一经判定,R_1 随即向 MOD 服务器 LO-1 发起标签申请,请求信息包括:R_1 的 lookback 地址,V_1 和 V_2 的地址. MOD 服务器 LO-1 收到标签申请后,根据地址前缀与自治域的联盟成员映射列表对 R_1 与受害主机依次检查,判定 R_1 属于成员域 $Stub_1$、V_1 属于成员域 $Stub_2$、V_2 不属于该联盟,随机启动如下处理策略:MOD 服务器 LO-1 为数据流(R_1,V_1)直接分配 C 类标签 1100001,并将(R_1,V_1,1100001,T)插入它的数据库以及回复申请,回复信息包括(V_1,1100001);同时向上层 MOD 服务器 HI-1 发出标签申请,请求信息包括(R_1,V_2).

(2)与步骤 1 相似,MOD 服务器 HI-1 收到标签申请后,也是先判定,后处理. 因 R_1 和 V_2 属于联盟 HI-1 成员域,所以 MOD 服务器 HI-1 为数据流(R_1,V_2)直接分配 B 类标签 1000001,并将(R_1,V_2,1000001,T)插入它的数据库,紧接着回复申请,回复信息包括(R_1,V_2,1100001). 如若联盟规模太大而造成标签资源缺乏,那么 MOD 服务器 HI-1 只能把标签粒度从边界路由器扩大到自治域,也就是将($Stub_1$,V_2,1000001,T)插入它的数据库. MOD 服务器 LO-1 收到 HI-1 的回复信息(R_1,V_2,1100001)后,随即将(V_2,1100001)转发到 R_1. 如若收到的回复信息是($Stub_1$,V_2,1000001),那么扫描 MOD 数据库,将所有包含于 $Stub_1$ 的标记路由器、以 V_2 为目的地址的项全部整合成一项,也就是(R_1 &R_i,V_2,1000001,T).

(3)边界路由器(即标记路由器)R_1 收到数据包后,首先对数据包进行分类,提取目的地址为 V_1 和 V_2 的 IP 流,然后依据回复信息(V_1,1100001)和(V_2,1000001)分别对这两种 IP 流执行包标记操作,也就是将标签写入到数据包的标签装载域中.

(4)边界路由器 R_2 和 R_3 收到被标记攻击流后,利用聚集效应快速、准确地检测出攻击,提取攻击标签,分别向 AS_2 和 AS_4 监视器发起标签验证请求(V_1,1100001)和(V_2,1000001).

(5)AS_2 和 AS_4 监视器分别向同层 MOD 服务器 LO-1 和 MOD 服务器 LO-2 发起溯源请求. MOD 服务器 LO-2 和 LO-1 在收到溯源请求(V_2,1000001)和(V_1,1100001)后,分别根据受害主机和标签对 MOD 数据库所有项依次检查,判定标记路由器,进而回复请求. 其中 LO-2 判定标记路由器 R_1,向 R_2 回复请求(R_1,1000001),LO-1 未找到匹配项,向上层 MOD 服务器 HI-1 发送溯源请求.

(6)与步骤 8 相似,MOD 服务器 HI-1 在收到溯源请求(V_2,1000001)后,匹配到标记路由器 R_1,随后向 MOD 服务器 LO-1 回复(R_1,1000001). 如果 HI-1 匹配到自治域 $Stub_1$,那么它立即向包含 $Stub_1$ 的联盟 LO-1 发起溯源请求,LO-1 会查找数据库中所有以 V_2 为目的地址、1000001 为标签的项,将项中标记路由器返回 HI-1. MOD 服务器 LO-1 收到 HI-1 回复信息(R_1,1100001),随即转发到 AS_4 监视器,溯源结束.

4.2　核心机制实现

上一节主要介绍了 SEEK 方法的基本框架，本节将详细讨论它的设计细节，重点解决以下问题：(1) 在现有网络协议框架下，如何重载标签装载域，增大标签分配空间，提高标签分配数量；(2) 在高负载情况下，标记路由器如何高效执行包标记操作，加快路由器的 IP 包处理速度，减轻溯源对底层网络性能影响；(3) 在面对大规模网络攻击时，如何设计合理的标签回收策略，提高标签资源利用率；(4) 随着溯源联盟规模的增大，如何保证标签管理服务的可靠性，避免因负载过重而造成服务质量下降；(5) 在开放系统互联环境下，如何设计通信协议，保证协同过程安全可信.

4.2.1　灵活重载标签装载域

SEEK 方法需要在 IP 包头添设一种用于存放密钥标签的溯源字段，由标记路由器负责填写该字段，使每个匿名包都能通过携带一个私密的、唯一的标签来充当回溯指纹. 本文将溯源字段也称为标签装载域. 为了降低部署成本，SEEK 溯源系统通常采用“改良型”研究思路，即在当前互联网协议下运行. 当前互联网的路由协议主要分为两类：IPv4 和 IPv6. 相比于后者，前者应用范围较广，因此本文重点关注 IPv4①. 根据互联网程序协议规范 RFC791，IPv4 的数据包头不包含标签装载域，因此我们只能重载部分已定义的闲置包头字段来定义标签装载域.

标签装载域作为标签的存放空间，它的长度直接决定了 SEEK 系统可用的标签资源. 很明显，标签数量越多，可回溯的规模也就越大. 如果标签装载域长度能达到 32 位，即与 IP 地址空间相同，那么溯源规模可达整个网络. 但是，在当前网络运行的 IPv4 协议中可重载的闲置包头字段数量一般比较少，只包括服务类型(Type of Service，ToS)、分片标识(Fragment Identification，FI)、保留位(Reserved Flag，RF)三个字段，其中 ToS 有 8 位，FI 有 16 位，RF 有 1 位. 由尚未定义的字段 RF 来充当闲置字段是容易理解的，而由那些曾经被赋予重要作用的字段来充当闲置字段的主要原因是：(1) 考虑到实现复杂性和性能开销，路由设备会依据其自身支撑的业务类型有选择性的设置 IP 包头字段，这也就是说，在某些网络内，ToS 字段会被闲置. 例如，由 ToS 字段支持的区分服务(Differentiated Service，DS)模型或优先级模型是当前流行的 IP 服务质量保证(Quality of Service，QoS)标准，它的设置需要路由设备先后对网络入口数据流量进行分类、标记、整形、队列管理等操作，整个过程既复杂又繁重，一般只有核心网络才会支持 QoS 业务、设置 ToS 字段，而在某些边缘网络，ToS 字段未被使用，属于闲置字段；(2) IP 层是整个 TCP/IP 协议框架的瓶颈，为了减轻它的负载，一方面网络服务提供商不断地减少底层传输网络的异构性，降低因异构而造成的路由操作复杂度，另一方面网络协议设计者不断地推动 IP 层任务上移，减轻它的任务量. 这种互联网演进趋势使得原本重要的包头字段变成闲置字段. 例如，随着 X.25、ATM 网络的消失和 TCP 协议的最大分段大小(Maxitum Segment Size，MSS)的广泛应用，IP 分片使用率已从原来的 0.25% 降低到 0.06%，而且 60% 的分片还是攻击包[30-31]. 因此，FI 作为分片包标识字段，已变得无关紧要. 此外，根据 IP 协议规则，只需给同源分片包的 FI 字段中写入相同的标识即可. SEEK 方法正好满足这一条件(写入相同的标签)，因此重载 FI 字段也能在受害端完成组装. 基于此，在当前网络中，FI 也可当做闲置字段. 综上所述，在重载过程中，FI 和 RF 闲置长度相对稳定，而 ToS 的闲置长度会根据网络所支撑 QoS 业务类型动态变化.

本文将所有闲置字段构成的空间称为闲置空间. 不同 IP QoS 业务会导致不同长度的闲置空间. 根据协议文档 RFC1122、1349 和 2475，ToS 支持的 IP QoS 业务类型可分为五类，闲置空间长度依次为：(1) DS，使用 8 位 TOS 字段，闲置空间 $S_{DS}=length(FI)+length(RF)+0=17$；(2) Priority，使用 3 位 TOS 字段，闲置空间 $S_{Priority}=length(FI)+length(RF)+5=22$；(3) Procedence，使用 3 位 TOS 字段，闲置空间 $S_{Procedence}=length(FI)+length(RF)+5=22$；(4) Priority+Procedence，使用 6 位 TOS 字段，闲置空间 $S_{Procedence+Priority}=length(FI)+length(RF)+2=19$；(5) 不支持 QoS 业务，使用 0 位 TOS 字段，$S_{non\text{-}support}=length(FI)+length(RF)+8=25$. 基于此，本文将闲置空间 S 划分两部分：类型号 C 和标签装载域 F，前者存放闲置空间的编码，后者存放标签，即 $S=C+F$. 根据闲置空间类型数量，类型号需占 3 位，本文分别使用 RF、7^{th}_{TOS} 和 8^{th}_{TOS}，其中 RF 用于说明是否支持 QoS 业务，后两位用于说明所支持 QoS 业务的类型，具体编码方式如图 5 所示.

① SEEK 方法也适用于 IPv6 网络. 但是，由于 IPv4 的数据包头与 IPv6 并不相同，因此标签装载域的重载方式需要重新研究.

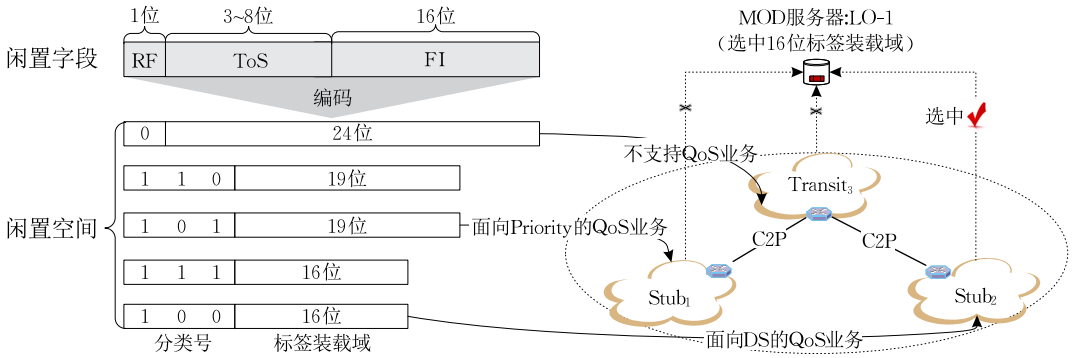

图 5 标签装载域的重载过程举例(源于图 4)

在扁平化的体系结构中,为了使 QoS 类型不同的溯源网络也能正常运行,传统方法选取最小、也最稳定的闲置空间来设计标签装载域,只有 17 位.为了扩大标签装载域长度、提高溯源规模,本文立足于 SEEK 可分层的溯源体系结构,充分利用各联盟可独立分配标签的特点,同时借鉴最小公因数原理,设计一种灵活的标签装载域重载策略.具体过程是:已知每个联盟都维护 MOD 服务器,而且只要通信双方都位于该联盟,该 MOD 就可独立分配标签,也就使得相关标签装载域能够独立重载.为此,MOD 通过收集所有 AS 成员支持的 QoS 业务类型来选定最稳定的闲置空间,进而确定标签装载域.该过程形式化为:给定联盟 $LO=\{AS_1,AS_2,\cdots,AS_n\}$,$F_{AS_i}$ 表示 AS_i 的标签装载域长度,该联盟标签装载域 $F_{LO}=\min\{F_{AS_i},AS_i\in LO\}$.我们以图 4 的最底层联盟 LO-1 为例来说明它的标签装载域重载,具体过程如图 5 所示.假设 LO-1 的 $Transit_1$ 不支持 QoS 业务、$Stub_1$ 支持面向 Priority 的 QoS 业务、$Stub_2$ 支持面向 DS 的 QoS 业务,LO-1 服务器按照大小对闲置空间排序,选取 $Stub_2$ 作为稳定闲置空间,重载标签装载域为 16 位.

4.2.2 自适应包标记

在 SEEK 方法中,标记路由器需要将申请到的标签写入到所有流向受害者数据包的标签装载域中.进一步考虑到标签与目的地址相互绑定,使得标记路由器在完成标签写入之前,还须对到达包按照目的地址进行流分类,也就是划分为若干目的地址不同的数据流.基于此,SEEK 的包标记应先后执行流分类和标签写入两种操作.考虑到标记路由器短缺的计算和内存资源,如何减小包标记操作对计算和内存资源的需求,降低它对数据包转发速率的影响,保证网络传输性能,就显得非常重要.

针对该问题,一种简单、低效的解决方案就是直接升级标记路由器、扩大硬件资源,但是这会给 ISP 带来剧大的部署成本,阻碍溯源系统的大规模部署.为此,基于以下发现:(1)庞大的 DoS 攻击包数量使得攻击源追踪允许选择性标记,无需逐包标记;(2)SEEK 不会因包标记次数减少而降低回溯效率,本文以减少包标记操作次数、降低性能开销为出发点,通过建立由 CPU、内存和数据流到达包数共同组成的负载评价函数,实时评估标记路由器的负载状况来自适应调整包标记概率,提出一种高效的自适应包标记(Adaptive Packet Marking,APM).APM 一般包括两个步骤:模型参数提取和评估函数设计.考虑到标记路由器对快速分组转发能力的需求,APM 必须具有线速处理能力,从而使得模型参数提取过程必须快速、评估函数也必须轻量、高效.

APM 的模型参数包括 CPU 和内存使用率以及数据流的到达包数,其中前者通常能够从操作系统直接读取,而后者需要设计相应的提取算法,故是本节重点关注内容.所谓数据流的到达包数是指数据流在特定时间间隔内 IP 包的到达数量.其提取过程可描述如下:标记路由器先利用标签和目的地址的绑定关系,根据目的地址对 IP 流进行分类,进而提取标签所对应的数据流,然后统计每个数据流在单位时间内的 IP 包到达数.为了能够快速完成上述过程,本文先后引入已经在路由器上广泛实现、能够快速完成 IP 地址搜索的 Trie 树以及基于 FIFO 队列、便于路由器统计、运行的动态流表来分别实现流分类和包统计,通过整合二者,设计一种参数提取器(Parameter Extraction,PE).我们以图 4 的标记路由器 R_4 来说明 PE 的结构,具体参数获取过程如图 6 所示.已知标记路由器 R_4 需要往流向受害者 V_1 和 V_2 的数据流中写入标签,R_4 首先将 V_1、V_2 的 IP 地址插入 Trie 树和动态流表,同时建立二者的指针联系,然后对所有到达的 IP 包进行分类和搜索,选定被标记的流,最后统计被标记 IP 流的到达包数量,将其插入表中.

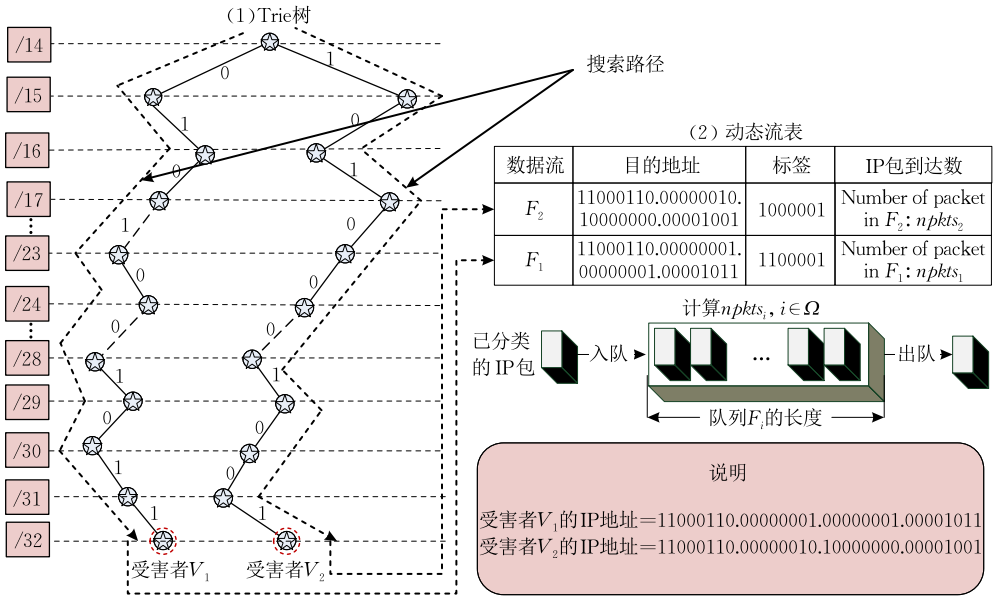

图 6　参数提取过程举例(源于图 4)

APM 的评估函数 F 借鉴文献[13]提出的标记概率公式,将各数据流的带宽占用情况以及路由器的性能使用情况来作为包标记操作的决定因子,且假设二者彼此独立,根据概率乘法定理,获得以下公式:

$$F=t_1\times t_2 \tag{1}$$

其中 t_1 和 t_2 分别表示带宽因子和性能因子. 在这两个因子的协作下,通过及时调整匿名包的标记概率来尽可能减小溯源过程对网络和路由器的影响. 就 t_1 来说,我们遵循攻击流速越大、危害性也越大的基本原则,将它形式化为如下公式:

$$\begin{aligned} t_1=&\{npkts-\min(npkts_j,j\in[1,m])\}/\\ &\{\max(npkts_j,j\in[1,m])-\\ &\min(npkts_j,j\in[1,m])\} \end{aligned} \tag{2}$$

其中 $npkts_j$ 表示以 j 为目的地址的数据流到达包数,m 表示需要标记的数据流数量,以图 6 为例,标记路由器 R_4 需要标记指向 V_1 和 V_2 的数据流,故 $m=2$. 就 t_2 来说,鉴于 CPU 使用率 l_1 和内存使用率 l_2 是路由器的重要性能指标,我们为二者分别给定阈值 $L^i_{\min}$ 和 $L^i_{\max}$,$i\in\{1,2\}$,t_2 随着 l_1 和 l_2 与阈值关系的变化而变化,具体形式化为如下公式:

$$t_2=\begin{cases} 0, & \forall i\in\{1,2\},l_i\geq L^i_{\max}\\ e_1\times\dfrac{L^1_{\max}-l_1}{L^1_{\max}-L^1_{\min}}+e_2\times\dfrac{L^2_{\max}-l_2}{L^2_{\max}-L^2_{\min}}, & \exists i\in\{1,2\},L^i_{\min}<l_i<L^i_{\max}\\ 1, & \forall i\in\{1,2\},l_i\leq L^i_{\min}\end{cases} \tag{3}$$

其中 e_1 和 e_2 表示两个指标各自所占权重,它们之间存在如下关系:(1) $e_1+e_2=1$;(2) $e_1:e_2=\{(l_1-L^1_{\min})/(L^1_{\max}-L^1_{\min})\}:\{(l_2-L^2_{\min})/(L^2_{\max}-L^2_{\min})\}$. 基于此,本文引入归一参数 ε,将 e_1 和 e_2 的形式转化为

$$e_1=\varepsilon\times\frac{l_1-L^1_{\min}}{L^1_{\max}-L^1_{\min}},e_2=\varepsilon\times\frac{l_2-L^2_{\min}}{L^2_{\max}-L^2_{\min}},\varepsilon\in(0,1) \tag{4}$$

上述式(1)~(4)所表达的物理含义可描述如下:为了保证快速转发能力,一旦 $l_1,l_2>L_{\max}$,标记路由器就不再执行包标记操作;当 $l_1,l_2<L_{\min}$,标记路由器就以概率 t_1 执行包标记操作;当存在 l_1 和 l_2 未达到阈值时,标记路由器就以 $t_1\times t_2$ 执行包标记操作.

4.2.3　动态管理标签

在 SEEK 方法中,MOD 服务器需要灵活管理标签资源,以便能够及时向标记路由器进行分配. 为了实现快速分发,本文引入标签资源池(Label Pool,LP),以协商租约形式来分配标签,进而提出一种标签动态管理策略. 其基本原理是:LP 中标签具备“闲”和“忙”两种状态. 正常情况下,所有标签都为空闲状态. MOD 服务器一旦接受标签申请,就从 LP 中随机选取一个标签,以租约的形式分配给相关标记路由器,同时将该标签状态修改为“忙”. 只有租约到期,才可重新修改状态. 很明显,标签租约时间的长短对 MOD 性能会有较大影响. 例如:租约时间过短会引发震荡攻击,使得攻击者通过调节流量模型就能诱导 MOD 服务器反复分配标签,耗尽其计算资源,无法正常工作;租约时间过长则会造成标签回收不及时,阻碍其再分配,降低其利用率. 因此,如何设计合理的标签租约时间就显得非常重

要.

考虑到攻击周期的不确定性,若以静态方式来固定标签租约时间,无论怎么设置,都会引发上述问题.为此,本文以实际攻击的平均周期为基本单位,通过分析当前攻击流变化特征来预测攻击可能持续时间,进而借鉴 KeepAlive 握手协议,以通信协商的方式来动态扩展租约时间.经统计,当前网络中最常见 DoS 攻击的平均持续时间为 5 min[29].基于此,本文建议将标签租约时间的基本扩展单位设为 5 min.图 7 描述了整个协商过程.从左到右的水平方向表示租约时间在逐渐扩展,斜向上的箭头表示由标记路由器发起的请求,而斜向下的箭头表示由 MOD 服务器发起的请求.DoS 攻击过程通常可分为爆发、缓解和终止阶段.相应地,标记路由器租约标签过程包括三个临界点:攻击爆发临界点、攻击缓解临界点和攻击解除临界点,其中前两者联合构成租约期,后两者联合构成宽限期.宽限期的增设能够缓冲标签的回收,避免攻击流震荡而反复申请标签.也就是说标签只有达到宽限期才能被回收.依据图 7 的标号顺序,标签的协商过程描述如下:(1)标记路由器向 MOD 服务器提出标签申请;(2)MOD 服务器接受该申请,并向标记路由器回复标签和它的具体租约期 C_1;(3)标记路由器在 C_1 内通过实时评估当前攻击状态,确定该标签依然处在攻击缓解临界点之前,因此立刻向 MOD 服务器提出 C_2 请求;(4)MOD 服务器并不立刻回应 C_2 请求,而是等到标记路由器的租约期 C_1 快结束时才做出回应;(5)标记路由器在 C_2 内判定该标签已然处在攻击缓解临界点,因此立刻向 MOD 服务器提出宽限期 C_3 请求;(6)MOD 服务器在等到租约期 C_2 快结束时接受 C_3 请求.采用相同的流程,就可扩展到宽限期 C_4;(7)由于标记路由器在 C_4 内没有再发起扩展宽限期的申请,因此 MOD 服务器在 C_4 快结束时发起标签解约通知,同时将 LP 中该标签的状态修改为"闲".需要说明的是:通信协商过程中可能遇到 MOD 服务器故障,图 7 的新的标记路由器就出现这种情况.该路由器在 C_1 发起租约期 C_2 请求后,并没有得到 MOD 回应,因此它自动扩展到 C_2,同时在 C_2 期间不停地提出请求,直到 MOD 服务器恢复服务,回复请求为止.

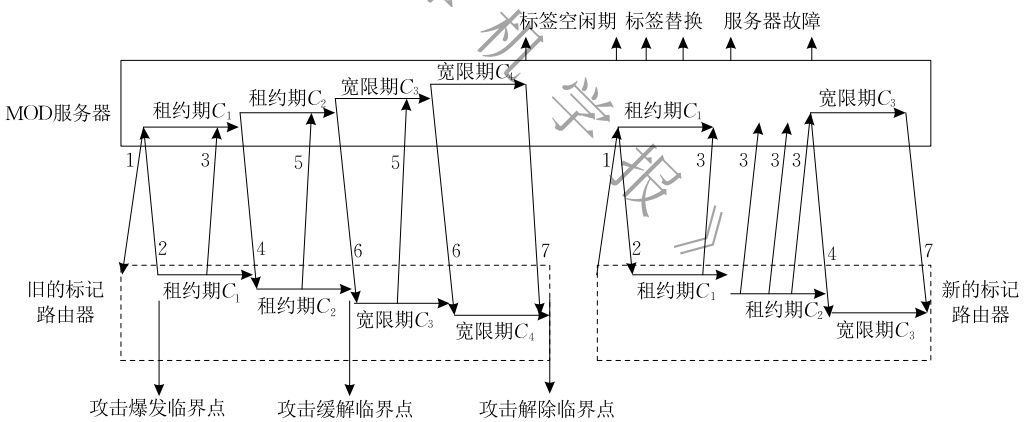

图 7 标签租约时间的通信协商过程

由上文可知,标记路由器租约标签的时间长度取决于租约期和宽限期的扩展次数,而后者则取决于它对攻击缓解和攻击解除临界点的预判.进一步考虑到标记路由器的快速转发能力,如何轻量、准确地预估下一阶段的攻击状态变化就显得非常关键.通过观察我们发现:在攻击状态改变之前,匿名包的数量也会发生波动.基于此,本文通过统计不同时间段内匿名包到达情况,结合移动平均线与最近最少使用相交叉理论,预测下一时间段内攻击状态.具体实现细节可描述为:$\forall$标记数据流 F_i、租约期 C_j 和宽限期 C_k,使用 Egress Filtering 匿名包检测平台来分别统计截至 C_j 和 C_k 结束时 F_i 所含匿名包的数量,以此为基础,计算 F_i 匿名程度的移动平均数 V_i^j 和 V_i^k,此外,分别为 V_i^j 和 V_i^k 设置攻击缓解阈值 μ_1 和攻击解除阈值 $\mu_2$①.如果 V_i^j 大于 μ_1,那么 C_{j+1} 仍是租约期;反之,则是宽限期.如果 V_i^k 大于 μ_2,那么 C_{k+1} 仍是宽限期;反之,则解除该标签,使其进入闲置期.F_i 匿名程度的移动平均数 V_i^j 计算公

① 阈值 μ_1 和 μ_2 取决于 MOD 服务器的性能容量和所抵御的攻击类型:如果性能容量足够大,μ_1 和 μ_2 应该较大,以便加快标签回收过程,提高标签利用率;如果性能容量较小,μ_1 和 μ_2 应该较小,以便减少标签回收次数,通过降低利用率来换取较小的标签管理开销.如果抵抗带宽消耗攻击,可将 μ_1 设置较大而 μ_2 设置较小;如果抵抗降质攻击,μ_1 和 μ_2 都可设置较小.

式如下：

$$V_i^j=V_i^{j-1}-\frac{P_i^{j-1}}{\sum_{n=1}^{j}C_n}+\frac{P_i^j}{\sum_{n=1}^{j}C_n}-\eta \tag{5}$$

其中 V_i^{j-1} 是指 F_i 从标签申请开始到 C_{j-1} 结束时匿名程度的移动平均数；η 是为了降低 V_i^j 的惩罚系数，属于经验值；P_i^{j-1} 是指 F_i 从标签申请开始到 C_{j-1} 结束时匿名程度值，它的计算公式如下：

$$P_i^j=\rho_1\cdot d_i^j+\rho_2\cdot(t_{\text{now}}-t_{\text{pior}}) \tag{6}$$

其中 ρ_1 是指频率权重，ρ_2 是指近因权重，$\rho_1+\rho_1=1$，d_i^j 是指 F_i 从标签申请开始到 C_j 结束时匿名包出现次数，t_{now} 和 t_{pior} 分别表示匿名包的最近一次到达时间和上一次到达时间.

4.2.4　可靠性

SEEK 系统因立足于实际网络而造成联盟成员数量巨大且分布广泛，使得高层联盟的 MOD 服务器负载过重，极易成为性能瓶颈. 为此，本文采用多副本存储技术来构建 MOD 服务器，即由多个位置不同，但配置完全一致、功能地位对等的副本服务器共同提供 MOD 服务，既能均衡负载、避免压力过大而造成系统崩溃，又能提高容错、最大程度保证系统可用.

多副本存储技术在提升系统可靠性的同时也带来了数据一致性难以保证、副本故障恢复困难等问题. 为此，本文以轻量、高效为出发点，分别选用如下技术来解决上述问题：(1) 通过对 MOD 业务特点进行分析，最终选定通信开销较小的最终一致性模型来完成副本数据之间的同步，通过牺牲一致性来换取高可靠性和可用性，原因如下：MOD 的主要任务是成员处理请求(Process Members's Requests，PMR)和标签处理请求(Process Label's Request，PLR)，其中 PMR 必须被及时处理，以便提高用户体验，而 PLR 则允许延后发送，这就意味着 MOD 无需在意成员更新过程中的一致性问题，只要保证最终的所有数据副本彼此一致即可，简单点说就是“只求结果、不看过程”. 然而，不保证过程数据的一致性会造成各个副本可能以不同的顺序看到更新结果，进而导致它们的最终数据不一致. 针对该问题，直观的解决方案是在各个副本时间同步的条件下，通过共享时间片来完成更新排序. 不过，为了校准时间，这会产生大量的通信和计算开销. 为此，我们采用开销较小的向量时钟协议来推断更新发生次序. 鉴于成员更新不会太频繁，该协议性能不会成为系统瓶颈；(2) MOD 副本随时都可能发生一些非预期的故障. 当故障恢复之后，各副本数据不再一致，这就需要数据同步策略. 按照发生时间长短，机器故障可分为临时故障和永久性故障. 若是前者，鉴于 PLR 任务繁重，为了避免在高峰期执行检查点操作，加重系统负载，我们采用自适应检查点机制来同步数据. 每当一个副本发生错误，另一个副本依据当前任务量动态选择时间，执行最后检查点的 PLR 任务. 虽然这会造成 PLR 重复发送，但是接收方只需忽略多余任务即可. 若是后者，鉴于同步数据较多且部分操作可逆，为了加快恢复速度，我们采用 Merkle 哈希树技术快速完成数据同步检测和定位，同时减少同步过程中所需传输数据量.

4.2.5　安全通信

SEEK 系统的开放性允许任何陌生自治域和路由器向 MOD 服务器提出联盟成员注册、退出以及标签申请、租约延期，这为匿名、中间人等恶意攻击的发起提供了可能. 例如：恶意自治域可以假冒非成员域，通过伪造注册请求，强迫它们加入联盟，也可以假冒成员域，通过伪造退出请求，强迫它们离开联盟；恶意路由器可以假冒标记路由器，通过不停地发送标签申请来消耗 MOD 的标签资源；在 MOD 向标记路由器回复标签参数的通信过程中，恶意用户通过充当通信双方的中间人来拦截该消息，并将原有参数替换为其他已分配参数，致使溯源精度降低. 上述攻击方法之所以能够成功，究其原因在于：(1) MOD无法识别成员域监视器和标记路由器的身份；(2) 标记路由器无法确认 MOD 发送的回复消息中标签参数是否被篡改. 简言之，系统模块之间的通信必须嵌入身份认证和消息验证等功能.

本文以低成本、高效率为出发点，引入资源公共标签基础架构(Resource Public Key Infrastructure，RPKI)和对称加密技术来保障 MOD 与 AS 监视器以及 MOD 与标记路由器的双向通信安全. 首先，RPKI 主要保证当 AS 监视器向 MOD 注册时的通信安全. RPKI 是一种已在互联网上顺利运行、面向互联网基础资源的公钥证书体系，主要任务是认证 AS 前缀的所有权(分配关系)和使用权(路由起源通告). 因此，如果能利用它来完成模块之间的身份认证，就能降低部署成本. 然而，RPKI 的设计初衷是为了保障路由安全. 若想将它应用于溯源联盟构建，需略作修改，其中 AS 监视器作为 IP 地址资源持有者，首先用互联网号码资源注册机构颁发的 CA(Certificate Authority)证书的私钥签发一个 EE(End Entity)证书，然后用 EE 证书的私钥产生“路

由源声明(Route Source Attestation,ROA)"签名项,其中包含彼此一一对应的 AS 号码和 IP 地址前缀,最后把 EE 证书和 ROA 上传到 RPKI 资料库发布点,同时把 ROA 嵌入到注册/退出消息,随后将它发送到 MOD;MOD 服务器作为 RPKI 验证者(Relying Party,RP),首先从 RPKI 发布点下载 ROA 对象,将其缓存到本地,然后使用公钥对到达的 ROA 解密,验证 ROA 所含数据是否与请求消息的参数一致.若一致,则证明发送方的身份正确,否则,属于伪造.然后,对称加密主要完成 MOD 与标记路由器之间的安全通信,它既可防止消息被篡改,又可确认发送方身份.当 AS 监视器使用 RPKI 成功向 MOD 注册后,MOD 随即生成对称密钥,并由 RPKI 保护着将其安全传送到 AS 监视器.MOD 将为每个成员域都维护一个密钥.假设位于同一自治域内的 AS 监视器与边界路由器组成信任共同体.它们之间共享对称密钥.每当边界路由器发起标签申请,先对消息内容进行加密,同时生成随机数 N,然后携带相关密文和 N 发起请求;MOD 收到消息后,先利用源 IP 地址和 AS 前缀的归属关系选定密钥,后对消息内容进行解密.若密文有效,则身份和内容都正确;反之,则是伪造.MOD 回复申请时,也使用该密钥对消息内容进行加密,并携带($N+1$)返给标记路由器.标记路由器在收到消息后采用与 MOD 相同的处理方法,随机数 N 的作用是避免重放攻击.

5 性能评价

为了验证提出的 SEEK 方法,本文进行了理论分析和仿真实验,其中 5.1 节将使用理论分析来证明方法的可扩展性,5.2 节则通过基于真实网络拓扑的实验仿真来补充分析结果.

5.1 理论评估

IP 溯源作为一种开放式分布控制系统,可扩展性是评价该系统能否适应大规模匿名攻击的重要评估指标.借鉴文献[16]对可扩展性的定义,溯源系统可扩展性可描述为当溯源联盟成员数量增加后,不会使该系统的各项性能参数发生明显下降,这些参数包括溯源规模 TS(Tracable Scale)、抗攻击能力 AC(Anti-attack Capability)、回溯时间 BT(Backtracking Time)、存储开销 SS(System Storage overhead)、计算开销 SC(System Computation overhead)和通信开销 SM(System coMmunication overhead)等.通过与经典确定标记溯源方法 DPM[13] 和动态确定标记溯源方法 DDPM[1] 进行比较,本节将使用数学方法来分析 SEEK 方法在可扩展性方面的优势.

5.1.1 溯源规模(TS)

溯源规模是指溯源系统能准确识别攻击源的最大数量.溯源规模通常与标签装载域的空间大小成正比,而装载域空间又取决于可重载字段长度.鉴于本文所提出的灵活重载标签域策略能普遍适用于 DPM 和 DDPM,为了公平,本节假设它们都采用该策略,获得相同的标签装载域长度,记为 L.首先分析 DPM,它借鉴 IP 包分片思想,将标签装载域划分为 3 部分:特征区 d、地址碎片区 a 和碎片偏移区 s.受害者首先利用特征值 d 来判定攻击源,然后根据偏移量 s 整理地址碎片 a,进而还原攻击源地址.很明显,特征区长度直接决定可追溯攻击源数量,基于此 $TS_{\mathrm{DPM}}=2^d$.进一步考虑到约束条件 $L=a+s+d$,其中 $a\geq 1, s\geq 1, d\geq 1, 2^s\geq a$,不难推出 $d\leq L-s-1$,$TS_{\mathrm{DPM}}\leq 2^{L-s-1}\ll 2^L$.然后分析 DDPM,通过建立标签与攻击源 IP 地址的映射表,它将标签直接写入标签装载域就能完成攻击源追踪.很明显,标签数量直接决定了可追溯攻击源数量.基于此,$TS_{\mathrm{DDPM}}=2^L$.最后分析 SEEK,它虽然采用与 DDPM 相同的标签绑定方案,但是借鉴 IP 地址分类思想,将标签装载域划分为 2 部分:标签类型区 k 和标签存放区 m,其中 $k+m=L$,不同层次联盟将使用不同类型标签.假设整个网络的联盟层次数为 c 且均匀构建,即相同层次联盟大小相同.我们分两种情况来讨论 SEEK 的溯源规模.一种情况是整个网络只有一个受害者,$TS^1_{\mathrm{SEEK}}=2^{L-1}+2^{L-2}+\cdots+2^{L-c}=2^L\times(1-1/2^c)<2^L$.很明显,联盟层次数 c 越多,TS^1_{SEEK} 越接近 2^L,不过这会增加联盟通信开销.根据文献[29]所述,层次数 c 的取值范围通常为 3、4 或 5,因而 $TS^1_{\mathrm{SEEK}}<2^L$.不过,如果出现标签不足问题,那么 SEEK 可通过调整标签粒度来扩大溯源规模(理论上来说,溯源规模可无限大),而且在单受害者场景下,这对溯源精度影响并不大.基于此,$TS_{\mathrm{DDPM}}\ll TS^1_{\mathrm{SEEK}}$.另一种情况是整个网络存在多个受害者,SEEK 允许在某些场景下可以给不同攻击源反复分配相同标签,即复用标签.例如:给定两个受害者 v_1 和 v_2,以及攻击源 A_1 和 A_2,只要(A_1,v_1)与(A_2,v_2)隶属于不同联盟,A_1 和 A_2 就可共用同一标签;反之,A_1 和 A_2 须使用不同标签.根据从下到上联盟逐层聚合、规模不断增大特征,不难推断出:联盟层次越低,(A,v_1)与(A,v_2)隶属于不同联盟的可能性越高;反

之，隶属于不同联盟的可能性越低. 假设(A,v_1)与(A,v_2)只在最底层隶属于不同联盟，那么v_1和v_2能够复用的标签数达2^{L-c}，也就是将溯源规模增大2^{L-c}. 此时，$TS^2_{\mathrm{SEEK}}\geq 2^{L-1}+2^{L-2}+\cdots+2^{L-c}+2^{L-c}=2^L$. 根据SEEK标签分类原理，联盟层次越高，可复用标签数量越多. 更不用说，SEEK还可通过调整粒度进一步扩大溯源规模. 基于此，可推出$TS^2_{\mathrm{SEEK}}\gg 2^L$. 再考虑受害者数量$n=3$的情况，它的复用标签数量等价于将受害者两两组合，再按照以上方式逐对计算复用标签数，进而求和. 因此，$TS^{n>3}_{\mathrm{SEEK}}\gg 2^L$. 采用数学归纳法，不难证明$TS^{n>1}_{\mathrm{SEEK}}\gg 2^L$. 基于此，$TS_{\mathrm{DDPM}}\ll TS_{\mathrm{SEEK}}$.

综上所述，可得$TS_{\mathrm{DPM}}\ll TS_{\mathrm{DDPM}}\ll TS_{\mathrm{SEEK}}$，这就说明，相比于DPM和DDPM，SEEK方法更适合在大规模网络上部署，也更适合抵御大规模匿名攻击.

5.1.2　抗攻击能力(AC)

抗攻击能力是指溯源系统能抵御多大规模的DoS攻击. 已知溯源方法都使用源标识符来代替攻击源IP地址，例如DPM的源地址特征和DDPM、SEEK的标签. 一旦攻击源数量超过溯源方法所能提供源标识符的最大数量，溯源方法就只能采用轮询法为每个攻击源分配标识符，然而这会造成标识符重叠，进而产生溯源误报，影响防御效果. 本文将标识符从当前分配到下一次分配的间隔时间称一轮分配时间. 很明显，如果攻击持续时间远小于源标识符的一轮分配时间，就不会产生误报，也证明该方法具备较强的抗攻击能力.

DoS攻击的动态性使得每一时刻的攻击参数都可发生变化，因此本文估算在t时刻标识符一轮分配时间$T(t)$. 假设t时刻攻击源数量为$N_{tr}(t)$，源标识符的最大分配数量为TS，攻击持续时间为$D(t)$，根据$T(t)$定义，可得$T(t)=[TS/N_{tr}(t)]\times D(t)$，根据WALD定理，推出$E[T(t)]=\{E[TS]/E[N_{tr}(t)]\}\times E[D(t)]$，其中$E[\cdot]$表示期望值. 进一步将它转换为$\{E[T(t)]/E[D(t)]\}=\{E[TS]/E[N_{tr}(t)]\}$. 我们从两个角度解读该式：一方面只有$\{E[TS]/E[N_{tr}(t)]\}>1$，也就是源标识符数量$TS$大于攻击规模$N_{tr}(t)$，才能无差错溯源；另一方面只有$\{E[T(t)]/E[D(t)]\}>1$，也就是新一轮标识分配时间大于攻击持续时间，才能保证溯源精度，否则就会发生重叠分配，产生误报.

为了估算$E[T(t)]$，就先得估算$E[TS]$、$E[N_{tr}(t)]$和$E[D(t)]$，它们的分析过程如下：(1)根据5.1.1节分析结果，任给溯源方法c，TS_c通常是定值，即$E[TS_c]=TS_c$；(2)$N_{tr}(t)$可表示为$A(t)\times K(t)$，其中$K(t)$表示每个攻击会话所包含子网数，每个子网对应一个攻击源；$A(t)$表示攻击会话数，因为整个网络在t时刻可存在多个DoS攻击. 首先估算$K(t)$. 文献[29]通过对当前流行的Conficker僵尸网络进行层次化分析，发现各自治域网络的僵尸主机数量满足Zipf分布，也就是一个自治域包含僵尸主机数量与它在僵尸数量表里的排名成反比，可表示为$P(X=|K(t)|)=C\times|K(t)|^{-\alpha}=M(t)/B(t)$，其中$C$是统计常量，$|K(t)|$表示随机变量在僵尸数量表里排名(最大排名数就是$K(t)$值)；$M(t)$表示最小自治域所拥有的僵尸数量，经统计$M(t)=1$；$B(t)$表示在$t$时刻整个网络拥有僵尸机的数量. 通过简单转换，可得$|K(t)|=\mathrm{e}^{(1/\alpha)\ln[CB(t)]}$，这就意味着只要已知$\alpha$和$B(t)$，就能确定$|K(t)|$. 已有研究[1]通过收集大量数据，发现每个攻击会话通常只包含数千个僵尸机，也就是说$B(t)\in[1,10000]$. 他们同时对α也展开了统计，得出$\alpha\approx 1.091$. 基于上述推算，可知$E[K(t)]$具有相对稳定的取值范围，大约为[100,3000]，文献[2]将其设置为200. 然后分析$E[A(t)]$. 鉴于僵尸网络的多样性，每一时刻它们都可能发起多个攻击会话. 假设当前互联网存在n个僵尸网络，那么$E[A(t)]$的取值范围为$[1,n]$. 鉴于$E[K(t)]$有限的取值范围，不难推出：$N_{tr}(t)$的上限取决于$E[A(t)]$上限；(3)已有研究通过对过去几年发生的DoS攻击进行统计，发现它们的持续时间具有很大的跳跃性，绝大部分攻击持续时间少于30 min，但也存在少量攻击时间超过了4小时[29]. 根据$\{E[T(t)]/E[D(t)]\}>1$原则，只要有一个攻击会话持续时间超过$E[T(t)]$，就会产生误报. 为此，本文将攻击持续时间设置为$E[D(t)]>240$ min，防止出现小于$E[D(t)]$的情况.

依据上述分析，标识符一轮分配时间可描述为

$$T(t)=\frac{E[TS]}{E[A(t)]\times E[K(t)]}\times D(t)\qquad(7)$$

因为$E[TS]$、$E[D(t)]$和$E[K(t)]$取值较为稳定，所以$T(t)$的值是由变量$E[A(t)]$所决定. 根据5.1.1节，可知$TS_{\mathrm{DPM}}\ll TS_{\mathrm{SEEK}}\ll TS_{\mathrm{DDPM}}$，在相同攻击背景下，代入上述公式，可得$T_{\mathrm{DPM}}(t)\ll T_{\mathrm{SEEK}}(t)\ll T_{\mathrm{DDPM}}(t)$. 我们以举例方式来解读该表达式. 假设标签装载域长度$L=16$，根据文献[2]，$E[TS_{\mathrm{DPM}}]=2^{11}$，$E[TS_{\mathrm{SEEK}}]=2^{16}$，$E[TS_{\mathrm{DDPM}}]=m\times 2^{16}$，$m>1$，$E[K(t)]=3000$，$E[D(t)]=240$ min，如果$T(t)<D(t)$，就须$E_{\mathrm{DPM}}[A(t)]<1$；$E_{\mathrm{DDPM}}[A(t)]<21$；

$E_{SEEK}[A(t)]<m\times 21$，其物理含义为：对于 DPM 来说，只要整个网络在 240 min 内发生一次规模超过 3000 的 DoS 攻击，就会发生溯源误报；对于 DDPM 来说，它允许整个网络在 240 min 内交叉发生 21 次、规模超过 3000 的 DoS 攻击；对于 SEEK 来说，因为不同攻击会话的受害者必然不同，所以它的标识符可重复分配，理论上可以不对 DoS 攻击发生次数进行限制. 因此，相比于 DPM 和 DDPM，SEEK 的抗攻击能力有极大提高.

5.1.3 存储开销(SS)

存储开销是指溯源设备为了建立攻击源与源标识符的映射表而带来的内存开销，其中 DPM 存储开销来自于入口路由器和出口路由器，DDPM 和 SEEK 存储开销来自于入口路由器和 MOD 服务器. 就 DPM 来说，它的源路由器需要存储 1 个标识符和 2^s 个地址碎片，考虑到 $1<s\leq 5$，故 $SS_{DPM}^{Igrs}=1+a\times 2^s<5$ B；它的溯源服务器需要集齐 2^s 个标记包才能还原一个攻击源，假设需要回溯的 n 个攻击源，考虑到 $n\leq 2^{L-s-1}$ 且 $L\leq 25$，$SS_{DPM}^{Egrs}=n\times 2^s\leq 2$ MB. 就 DDPM 来说，它的标记路由器只需存储一个标签，因此 $SS_{DDPM}^{Igrs}=4$ B；它的 MOD 服务器需要保存标签分配记录，包括标签、路由器 IP 和时间戳，每条记录长度为 $L+32+13=45+L$，其中时间戳由 JAVA 提供，考虑到 $L\leq 25$ 且 $n\leq 2^L$，$SS_{DDPM}^{Svr}=n\times(45+L)\leq 256$ MB. 就 SEEK 来说，它的入口路由器可能同时维护多个标签(如图 4 的 R_1)，因此 $SS_{SEEK}^{Igrs}=m\times 4$ B，其中 m 取决于同时发生的攻击会话数；它的每一层 MOD 服务器都需要保存标签分配记录，包括标签、路由器 IP、受害者 IP 和时间戳，每条记录长度为 $L+32+32+13=77+L$，考虑到 $n\leq 2^{L-1}$，$SS_{SEEK}^{Svr\text{-}1}=m\times n\times(77+L)\leq m\times 128$ MB，$m\in Z^+$. 此外，SEEK 还需 MOD 服务器保存联盟前缀，假设每个自治域只有一个 AS 号和前缀，共占用 9 B. 经统计，已知互联网 AS 总数约为 45 k，则每一层 MOD 服务器的最大存储开销 $SS_{SEEK}^{Svr\text{-}2}\leq 0.386$ MB，若使用网络前缀合并操作，还能进一步降低. 基于此，可得 $SS_{SEEK}^{Svr}=SS_{SEEK}^{Svr\text{-}1}+SS_{SEEK}^{Svr\text{-}2}\leq(m+1)\times 128$ MB.

综上所述，DPM、DDPM 和 SEEK 在入口路由器上存储开销都很低，不会给路由器造成性能负担. 另外，SEEK 在服务器上存储开销要高于比较方法，但也在可接受范围内. 倘若能在云平台上实现 MOD 服务器，存储开销过大就不会成为系统性能的瓶颈.

5.1.4 回溯时间(BT)

回溯时间是指溯源系统为了重塑攻击源 IP 地址所耗费时间. 一般来说，时间越短，溯源收益就越大. 溯源方法的回溯时间取决于它所需收集标记包数量. 就 DPM 来说，若标记包之间不存在哈希冲突，那么攻击源重塑问题可被建模为经典的邮票收集问题. 令 u 为所需收集标记包数量，T 为收集齐 u 个标记包所需查验 IP 包的数量，那么 $E[T]=u\times(1+1/2+\cdots+1/(u-1)+1/u)$，其中 $E(\cdot)$ 表示期望，$u=2^s$. 例如，当 $s=5$ 时，$=32$，$E[T]\approx 130$. 因此，$BT_{DPM}=E[T]$. 就 DDPM 来说，它只需要收集一个标记包就可确定攻击源，因此 $BT_{DDPM}=1$. 就 SEEK 来说，虽然它也只需一个标记包就能确定攻击源，但是因采用概率性标记策略，使得标记包收集较困难. 假设包标记概率为 p，那么受害者需要查验大于 $1/p$ 个 IP 包才能收集一个标记包(在攻击发生后，因网络性能不稳定，标记包就可能丢失)，因此 $BT_{SEEK}\geq 1/p$.

综上所述，可得 $BT_{DDPM}\leq BT_{SEEK}\ll BT_{DPM}$，这就意味着在攻击发生后，相比于 DPM，DDPM 和 SEEK 能够更快地识别攻击源，发起过滤请求.

5.1.5 通信开销(SM)

通信开销是指溯源系统为了建立攻击指纹而产生的数据通信量. 一般来说，通信开销既会影响底层网络传输性能，又会增加服务器负担. 就 DPM 来说，它允许各攻击源独立地工作，因此不会产生任何通信开销，$SM_{DPM}=0$. 就 DDPM 来说，它需要攻击源向 MOD 服务器申请标签，假设共有 Γ 个攻击源，鉴于该方法采用集中式体系结构，因此 $SM_{DDPM}=\Gamma$. 就 SEEK 来说，它采用层次化体系结构，使得每个攻击源都依据自身情况逐层由底向上提出标签申请，假设攻击源向 MOD 服务器提出请求是一种等概率事件，联盟共分 M 层，那么每个攻击源通信开销为 $E[x]=1\times(1/M)+2\times(1/M)+\cdots+M\times(1/M)=(M+1)/2$. 基于此，$SM_{SEEK}=\Gamma\times(M+1)/2$.

综上所述，鉴于 $M\in[2,5]$，可得 $SM_{SEEK}>SM_{DDPM}>SM_{DPM}$. 不过，因为 SEEK 将通信开销分散在不同层的 MOD 服务器上，所以较大的通信开销并不会成为 SEEK 的性能瓶颈. 此外，上述通信开销并不会很频繁，因此对底层网络性能的影响可忽略.

5.1.6 计算开销(SC)

计算开销是指入口路由器为了完成包标记操作

而产生的处理开销.已有研究表明路由器的 IP 包头处理开销占路由器整体开销的绝大部分,而包标记恰属于这类操作,因此若能减小包标记次数就能有效减轻它对入口路由器转发性能的影响.就 DPM 来说,它不区分正常包和匿名包,而统一给 IP 包头写入标记值,假设单位时间内到达入口路由器的 IP 包数量为 $npkts_1$,单位包标记处理开销为 C_1,那么 $SC_{DPM}=C_1\times npkts_1$.就 DDPM 来说,它只有在攻击发生后,才对 IP 包进行标记,假设在攻击发生后单位时间内到达中间标记路由器的 IP 包数量为 $npkts_2$,那么 $SC_{DDPM}=C_1\times npkts_2$.需要说明的是 DPM 和 SEEK 的标记路由器是在路径入口,而 DDPM 通常是在中间,结合攻击拓扑的多源单汇性,可得 $npkts_1\ll npkts_2$.就 SEEK 来说,它只对匿名包执行概率性包标记操作,已知单位时间内到达入口路由器的匿名包数量为 $npkts_1$,假设匿名包比例为 p_1,单位时间内包标记概率为 p_2,单位包标记处理开销为 C_2,其中 C_2 略大于 C_1,因为 SEEK 比 DDPM 多执行一种面向目的地址的分流操作,基于此 $SC_{SEEK}=p_1\times p_2\times C_2\times npkts_1$.

综上所述,长时间来看,考虑到计算开销累积,$SC_{DPM}\gg SC_{DDPM}\gg SC_{SEEK}$,因为 DPM 需要一直执行包标记操作,而 DDPM 和 SEEK 只在匿名攻击发生后执行;短时间来看,$SC_{DDPM}\gg SC_{DPM}\gg SC_{SEEK}$,鉴于 DDPM 的标记路由器所处位置,它需要处理更多的 IP 包.不过无论如何,SEEK 的计算开销都相对较低,主要原因在于它极大地减小包标记次数.

5.2　实验评估

根据 5.1 节的理论分析可知,SEEK 方法的性能指标与网络拓扑结构有紧密联系.基于此,本节的仿真实验将在真实网络拓扑上运行,以便对已有理论分析结果进行补充.鉴于 SEEK 方法的性能取决于自治域的规模大小和它们之间的层次关系,本实验采用以下两种真实拓扑数据:(1)美国 UCLA 大学搜集的自治域间商业关系①;(2)CAIDA 搜集的自治域内拓扑结构②.针对前者,本文通过清理和二次开发,获取支持自治域网络模拟软件 C-BGP 的域间拓扑文件,以此为输入参数,搭建自治域网络,模拟真实溯源联盟拓扑结构情况;针对后者,本文通过二次开发,获取支持网络仿真框架 OMNET++的拓扑文件,再结合 IP 网络仿真工具箱 INET 和 DoS 攻击仿真工具 ReaSE,模拟面向 IPv4 网络的匿名攻击场景.本文将设置与文献[6-9]类似的攻击场景.首先,每个路由器都将直连一台主机.为了保证攻击规模,整个网络随机指定一台主机作为受害者,而其他主机皆为攻击主机.然后,除了与受害者通信,攻击者与攻击者之间也可以随机发送消息.最后,将攻击者的 IP 包发送速率设置为 1 Kpps,而正常主机的发送速率则符合正态分布 $N(20\text{ pps},30\text{ pps})$.为了简化实验步骤,假设边界路由器能及时、准确地检测出匿名流,发起标签申请,这不会影响溯源性能指标.上述仿真平台运行在一台虚拟机(Intel 4 core 2.2GHz processor, 4GB of RAM, Ubuntu 16.04)上.

与传统溯源方法相比,SEEK 的先进性在于改善了溯源规模和性能开销,而它们又取决于溯源联盟的拓扑结构.基于此,本节实验首先围绕溯源联盟结构特征展开,然后分析比较溯源规模和性能开销.

5.2.1　溯源联盟的结构特征

根据 4.2 节的描述可知,溯源联盟的结构特征取决于以下因素:自治域所含路由器数量;不同层次自治域所占比例.基于此,本节将运行以下 3 组实验来反映不同层次溯源联盟的规模情况.

(1)第一组实验统计真实网络中不同规模自治域所占比重情况.不同规模自治域所占比重的补充累计分布函数如图 8 所示.超过 80%的自治域所含路由器数量小于 2^5,只有极少数 Transit 自治域所含路由器数量超过 2^{15}.自治域规模箱线图如图 9 所示,其中 $Q_1=1/4$,$Q_3=3/4$.自治域所含路由器数量离散程度较大,但是绝大多数自治域的路由器数量集中在(3,25)之间,其中规模为 10 的自治域最为集中.基于此,不难推出:绝大部分溯源联盟所需标签数都非常少,只有那些包含大规模 Transit 域的溯源联盟可能会出现标签不足的情况.

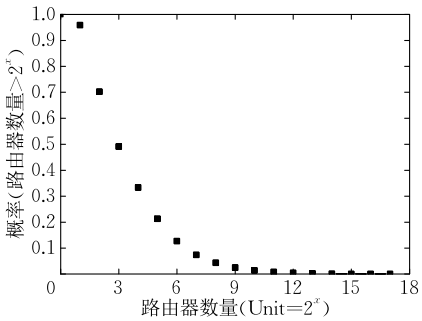

图 8　自治域所含路由器数量的补充累计分布函数

① URL. http://irl.cs.ucla.edu/topology
② URL. http://www.caida.org/data/active/internet-topology-data-kit/2013

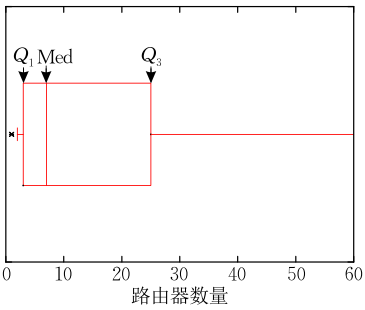

图 9 自治域所含路由器数量箱线图

(2)第二组实验统计真实网络的层次化程度.本组实验重点探讨自治域之间客户-提供者(C-P)连接关系.鉴于 C-P 关系的累加性,本文将未包含 C-P 关系的自治域称为 1 层子联盟;只包含一重 C-P 关系的联盟称为 2 层子联盟;将包含两重 C-P 关系的联盟称为 3 层子联盟,以此类推.不同层次联盟所占各层次联盟总量的比重情况如图 10 所示.从中可看出:几乎所有自治域都参与了 C2P 关系,超过 80% 的子联盟高度都不超过 4,最高子联盟达到 5.这就意味着绝大多数自治域都可参与到溯源联盟构建过程.根据本文所设计的溯源联盟体系结构,溯源联盟高度应有 6 层(Stub 域内也需部署一台 MOD 服务器).依据 SEEK 原理,溯源联盟层次越高,标签空间越分散,各层 MOD 服务器性能开销越平均.

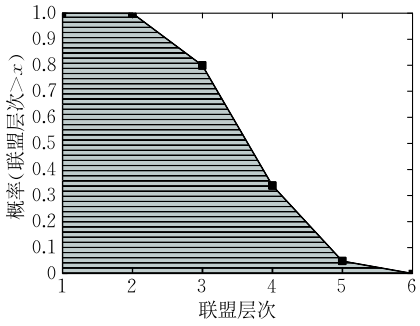

图 10 C-P 层次互补累积分布函数图

(3)第三组实验统计真实网络中多宿主自治域所占比重情况,结果如图 11 所示.无论客户是 Stub 域或 Transit 域,单宿主和多宿主自治域各占了将近 50%.虽然本文在论述 SEEK 原理时是以单宿主自治域为例,但是这并不意味着 SEEK 无法在多宿主自治域上运行.只需提供者在向 MOD 服务器提交注册请求时,将所有客户的网络前缀上传.

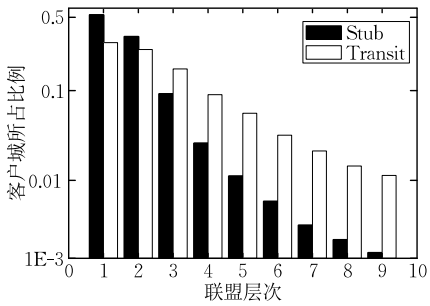

图 11 多宿主自治域数量的分布情况

5.2.2 溯源规模和方法开销

鉴于 5.1 节是从整体上证明 SEEK 方法的先进性,但未能评估不同层次 MOD 服务器的溯源性能和开销,本小节通过运行以下 4 组实验来评估这些指标:

(1)第一组实验统计不同层次联盟所覆盖 Stub 节点和路由路径数量.鉴于 CAIDA 和 UCLA 数据集无法兼容,本实验涉及 Stub 域拓扑都由人工生成,其规模设置为 40.Transit 域只负责转发数据包,所有数据包都由连接 Stub 域边界路由器的主机产生.将各子联盟按照就高不就低原则整合为 6 层溯源联盟,并为各层联盟分配 MOD 服务器.虽然 SEEK 方法要求标签申请必须由边界路由器来提出,但是影响申请数量的主要因素除了边界路由器数量,还有它们之间的路由路径情况.此外,考虑到第 6 层包含所有 Stub 域,而第 1 层 Stub 域内路由器规模又相等,这两层实验无需做.基于此,不同层次联盟所覆盖 Stub 域数量和路由路径数量分别占各层总量的比重情况如图 12 和图 13 所示.从整体上看,联盟层次越高,它所覆盖 Stub 域数量和路由路径数量也越多,其相关 MOD 服务器的性能开销也就越大.然而,从局部来看,4 层联盟所覆盖的 Stub 域数量和路由路径数量在某些时候要略高于

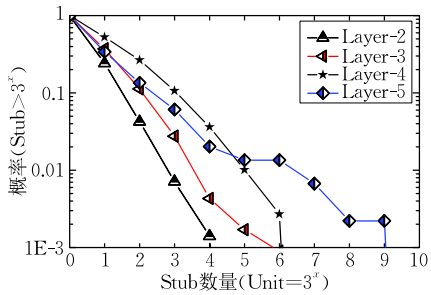

图 12 不同层次联盟所覆盖 Stub 数量分布情况

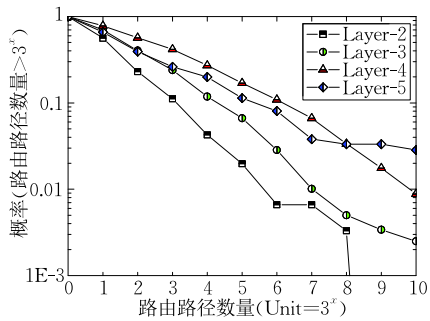

图 13 不同层次联盟所覆盖路由路径数量分布情况

5 层联盟. 原因是 SEEK 采用就高不就低原则，将 1 层子联盟（即未加入 C-P 关系的 Stub 域）注册于 5 层 MOD 服务器，从而造成 6 层联盟所覆盖的 Stub 域数量远高于所有 4 层联盟覆盖 Stub 域的总和，这就造成比例失调. 总之，联盟分布不均匀是造成上述结果的主要原因.

（2）第二组实验统计不同攻击场景下各层 MOD 服务器的标签申请情况. 为了凸显结果，本实验将受害者连接在最底层联盟的边界路由器上. 当只有一个受害者时，剩余主机都为攻击者；当存在两个受害者时，攻击二者的主机各占一半. 考虑到同层 MOD 服务器的地址空间相同，在不同攻击场景下各层所申请标签总量占该层地址空间总量的比例（即标签需求量/标签供应量）情况如图 14 和图 15 所示. 本实验假定标签空间为 16 位，可提供标签量为 2^{16}. 需要说明的是，因标签供应量是有限的，故实验结果存在比值大于 1 的情形. 就 DDPM 来说，它采用集中方式来分配标签，其标签空间固定. 此外，它的标签与边界路由器一一对应，故标签申请数量与受害者数量没有任何关联. 就 SEEK 来说，它通过分层方式来处理标签申请，将标签申请分摊在各层 MOD 服务器上，其中以顶层负载最重，在单受害者场景下，甚至超过了 DDPM. 但是，考虑到 SEEK 的标签能因受害者不同而复用，随着受害者越多，顶层 MOD 服务器接收到标签申请会不增反降，这也证实了 5.1.1 节的分析结果. 本节重点比较所占 Stub 域比重较大的 5 层以下子联盟，不难发现：与 DDPM 相比，SEEK 至少能将溯源规模提升 30%.

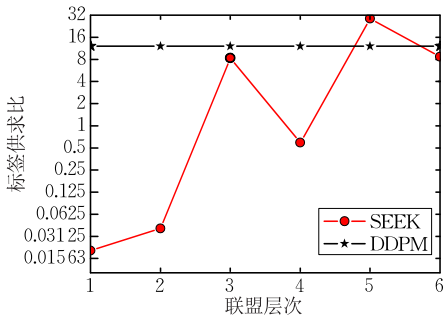

图 14　单受害者攻击场景下各层标签使用情况

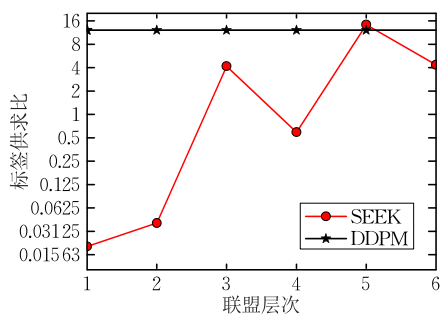

图 15　双受害者攻击场景下各层标签使用情况

（3）第三组实验统计各层 MOD 服务器的存储开销情况. 本实验设置方式与第二组实验相同，分别实现了单受害者和双受害者场景. 不同层次 MOD 服务器的前缀存储开销和标签记录分别占各自数量的比例如图 16 和图 17 所示. 需要说明的是：只有申请到标签的路由器才会被记录，因此一旦标签申请数量超过标签供应量，只能以供应量为记录标准. 就联盟前缀来说，绝大部分 MOD 服务器的存储开销都小于 2^9，而顶层 MOD 服务器数量虽然不多，但是少量服务器存储开销超过了 3^{10}. 不过，根据 5.1 节推论，它最多也不会超过 DDPM. 就标签记录开销来说，受标签空间影响，DDPM 是常量，而 SEEK 将此开销分散到不同层的 MOD 服务器上，在只有一个受害者的情况下，SEEK 顶层 MOD 服务器记录开销要低于 DDPM，这是因为顶层联盟的标签空间较小；随着受害者增多，标签被大量复用，顶层服务器的记录开销会快速增长，甚至超过 DDPM. 仅考虑 Stub 域所占比重较大的 5 层子联盟来说，SEEK 能将标签记录负载下降 20%.

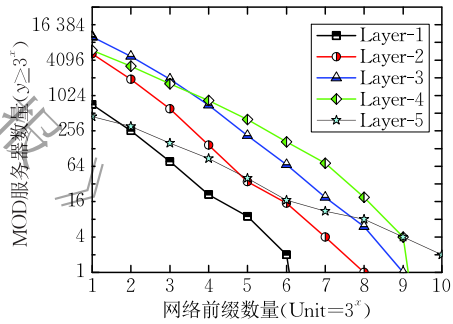

图 16　各层 MOD 服务器的网络前缀存储开销情况

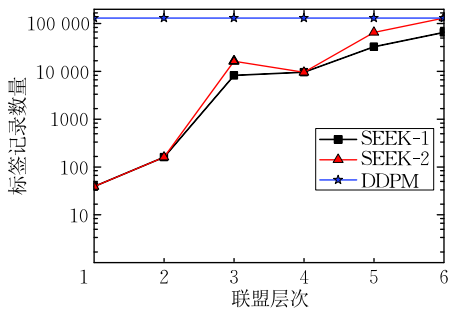

图 17　各层 MOD 服务器的标签记录存储开销情况

（4）第四组实验统计各层 MOD 服务器可能收到的标签请求次数，用来说明当匿名攻击发生时 SEEK 所产生得通信开销. 本实验只实现了单受害者场景. 不同层次 MOD 服务器所接收到标签请求

次数如图 18 所示. 一方面 SEEK 确实减轻了单个 MOD 服务器的负载开销,另一方面随着联盟层次增加,各层 MOD 服务器接收的请求数也会增长.

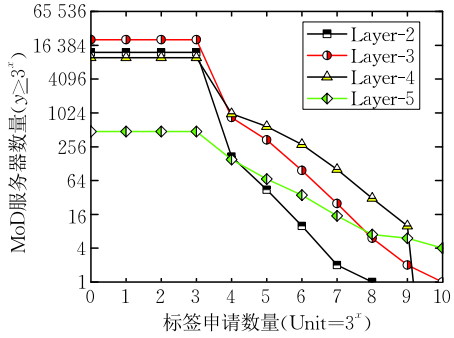

图 18 各层 MOD 服务器通信开销情况

6 结论及下一步工作

僵尸物联网驱动的 DoS 攻击是当前互联网面临的最主要安全威胁,而源地址伪造则是它的常用匿名手段. 基于此,针对 IP 匿名的溯源技术就成为了网络安全领域研究的重点和热点. 在众多已提出的 IP 溯源方法中,动态确定包标记因轻量、高效、易部署等特点备受人们关注. 但是在面对大规模网络时,它存在溯源规模受限、负载不均衡等可扩展性问题. 为此,本文提出一种可扩展的动态确定包标记溯源方法,它具备以下特征:(1)采用层次化、粒度可调的标签管理体系结构,在解决负载过于集中问题的同时提高标签利用率,扩大溯源规模;(2)自适应扩大标签装载域空间,提高标签可用数量,扩大溯源规模;(3)采用基于负载评估的概率性标记策略,降低溯源系统对底层网络的影响;(4)采用基于移动平均线的动态标签回收策略,提高标签重用率,扩大溯源规模.

未来研究工作主要包括:(1)提出的方法因联盟划分不均会产生性能瓶颈问题,影响溯源系统的可用性和可靠性. 若将溯源管理服务器托管到云平台,就能很好地解决该问题. 基于此,如何设计一种基于云的 IP 溯源架构就成为决定溯源系统能否大规模部署的主要问题;(2)提出的方法目前只能追踪到 Stub 域的边界路由器,无法识别隐藏在其后的僵尸机以及控制这些僵尸机的真正攻击者. 特别是随着仿人类行为 DoS 攻击的出现,使得原有基于流量检测的僵尸发现机制面临失效,因此如何设计可定位僵尸机和攻击者的 IP 溯源方法来完成追责、问责就成为了溯源系统能否被广泛应用的关键问题.

参 考 文 献

[1] Yu S, Zhou W, Guo S. A feasible IP traceback framework through dynamic deterministic packet marking. IEEE Transactions on Computers, 2016, 65(5): 1418-1427

[2] Yu S, Sood K, Xiang Y. An effective and feasible traceback scheme in mobile Internet environment. IEEE Communications Letters, 2014, 18(11): 1911-1914

[3] Patel H, Jinwala D C. LPM: A lightweight authenticated packet marking approach for IP traceback. Computer Networks, 2018, 140(7): 41-50

[4] Katyal K, Malik M, Dutta M. Implementation of single-packet hybrid IP traceback for IPv4 and IPv6 networks. IET Information Security, 2018, 12(1): 1-6

[5] Lu Ning, Wang Shang-Guang. An efficient and precise approach for single-packet traceback. Journal of Software, 2017, 28(10): 2737-2756(in Chinese)
(鲁宁, 王尚广. 一种高精度、低开销的单包溯源方法. 软件学报, 2017, 28(10): 2737-2756)

[6] Lu N, Wang Y L, Su S, Yang F C. A novel path-based approach for single-packet IP traceback. Security and Communication Networks, 2013, 7(2): 309-321

[7] Lu Ning, Wang Shang-Guang, Li Feng, et al. A dynamically scalable and efficient approach for single-packet IP traceback. Journal of Software, 2017, 29(11): 3554-3574(in Chinese)
(鲁宁, 王尚广, 李峰等. 可动态扩展的高效单包溯源方法. 软件学报, 2017, 29(11): 3554-3574)

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

[9] Yang M, Yang M. RIHT: A novel hybrid IP traceback scheme. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 789-797

[10] Su L, Divakaran D M, Thing V. Privacy preserving IP traceback//Proceedings of the 4th International Conference on Identity, Security, and Behavior Analysis(ISBA). Singapore, 2018: 1-8

[11] Roy S, Sairam A S. Distributed star coloring of network for IP traceback. International Journal of Information Security, 2018, 17(3): 315-326

[12] Nur A Y, Tozal M E. Record route IP traceback: Combating DoS attacks and the variants. Computers & Security, 2018, 72(8): 13-25

[13] Xiang Y, Zhou W. Flexible deterministic packet marking: An IP traceback system to find the real source of attacks. IEEE Transactions on Parallel & Distributed Systems, 2009, 20(4): 567-580

[14] Cheng L, Divakaran D M, Ang A W K, Thing V L L. FACT: A framework for authentication in cloud-based IP traceback. IEEE Transactions on Information Forensics and Security, 2017, 12(3): 604-616

[15] Tian H, Bi J. An incrementally deployable flow-based scheme for IP traceback. IEEE Communications Letters, 2012, 16(7): 1140-1143

[16] Xu Ke, Zhu Liang, Zhu Min. Architecture and key technologies of internet address security. Journal of Software, 2014, 25(1): 78-97(in Chinese)
(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)

[17] Li Jie, Wu Jian-Ping, Xu Ke, et al. SafeZone: A hierarchical inter-domain authenticated source address validation solution. Chinese Journal of Computers, 2012, 35(1): 85-100(in Chinese)
(李杰, 吴建平, 徐恪等. Hidasav: 一种层次化的域间真实源地址验证方法. 计算机学报, 2012, 35(1): 85-100)

[18] Liu B Y, Athanasios V V. Toward incentivizing anti-spoofing deployment. IEEE Transactions on Information Forensics and Security, 2014, 9(3): 436-450

[19] Lv Gao-Feng, Sun Zhi-Gang, Lu Xi-Cheng. Refining the inter-domain IP spoofing prevention. Chinese Journal of Computers, 2009, 32(3): 552-563(in Chinese)
(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)

[20] Yang Shui-Gen, Qin Ya-Juan, Zhou Hua-Chun, Zhang Hong-Ke. Route optimization mechanism based on identifier/locator split for nested mobile network. Acta Electronica Sinica, 2008, 36(7): 1261-1267(in Chinese)
(杨水根, 秦雅娟, 周华春, 张宏科. 基于身份与位置分离的嵌套移动网络路由优化机制. 电子学报, 2008, 36(7): 1261-1267)

[21] Chen G, Hu G, Jiang Y. SAVSH: IP source address validation for SDN hybrid networks//Proceedings of the Symposium on Computers and Communication. Messina, Italy, 2016: 409-414

[22] Lu Ning, Wang Shang-Guang, Li Feng, et al. Hierarchical anti-spoofing alliance construction approach. Journal of Software, 2019, 30(9): 2791-2814(in Chinese)
(鲁宁, 王尚广, 李峰等. 层次化的反匿名联盟构建方法. 软件学报, 2019, 30(9): 2791-2814)

[23] Jia Q, Sun K. Capability-based defenses against DoS attacks in multi-path MANET communications. Wireless Personal Communications, 2013, 73(1): 127-148

[24] Park K H, Heejo L. 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

[25] Hai D Z, Xin Y, Jaideep C. Controlling IP spoofing through interdomain packet filters. IEEE Transactions on Dependable and Secure Computing, 2008, 5(1): 22-36

[26] Yaar A, Perrig A. StackPi: New packet marking and filtering mechanisms for DDoS and IP spoofing defense. IEEE Journal on Selected Areas in Communication, 2006, 24(10): 1853-1863

[27] Ning W H, Cheng J, Kang S G. Defense against spoofed IP traffic using hop-count filtering. IEEE/ACM Transactions on Networking, 2007, 15(1): 40-53

[28] Mirkovic J, Prier G, Reihe P. Source-end DDoS defense//Proceedings of the 2nd International Symposium on Network Computing and Application. Cambridge, USA, 2003: 1-8

[29] Yu S, Gu G, Barnawi A. Malware propagation in large-scale networks. IEEE Transactions on Knowledge & Data Engineering, 2015, 27(1): 170-179

[30] John W, Tafvelin S. Analysis of Internet backbone traffic and header anomalies observed//Proceedings of the SIGCOMM: Internet Measurement. San Diego, USA, 2007: 111-116

[31] Stocia I, Zhang H. Providing guaranteed services without peer flow management//Proceedings of the SIGCOMM. Boston, USA, 1999: 81-94

LU Ning, Ph.D., assistant professor. His current research mainly includes cyber attack defense, big data security and privacy security.

ZHANG Jia-Wei, Ph.D. candidate. His current research mainly include big data security and privacy security.

MA Jian-Feng, Ph.D., professor, Yangtze River Scholar Professor, Ph.D. supervisor. His current research mainly includes network security, information security, system security.

CONG Xin, Ph.D., assistant professor. His current research mainly includes network management, network security.

SHI Wen-Bo, Ph.D., professor, Ph.D. supervisor. His current research mainly includes information security and cryptography, system security.

WANG Shang-Guang, Ph.D., professor, Ph.D. supervisor. His current research mainly includes service computing, service security.

Background

With the development of the Internet of Things (IoT), more and more IoT devices have been connected to the Internet. Everything has two sides and IoT is not an exception. It has brought convenience to people's lives, but also creates a series of issues. For example, attackers can exploit the fragile security and closure of IoT to disrupt the network activities. Denial of Service (DoS) attacks are typical cyber attacks in which the perpetrator seeks to make a machine or network resource (e.g., bandwidth) unavailable to its intended users by temporarily or indefinitely disrupting the legitimate services of a host connected to the Internet. Generally speaking, DoS attacks are launched by thousands of attackers that attempt to overload the system with lots of useless requests. IP spoofing is a common trick in DoS attacks, which can not only conceal their locations, but also bypass the defence mechanism. The attacker hides its own IP address and forges the source address, so that the victim cannot identify the locations of those attackers. Quite obviously, such technique makes the DoS attacks become more destructive than before, and difficult to control defense. For this reason, the IP traceback technology has been extensively researched and developed already, which is responsible for disclosing the attack sources. Among these existing IP traceback approaches, the dynamic deterministic packet marking traceback approach termed as DDPM has attracted great attention due to its light weight, high efficiency, and ease to deployment. Its main idea is to make use of the abnormal flow detection system that has been widely deployed on the Internet to establish the audit trails and further traceback to involved attack source. Only when the monitor notices a surge of suspicious network flows, it will apply for a private and unique mark from a globally shared MOD server, and insert it into the suspicious packets' header. At the same time, the MOD server establishes and maintains the mapping relationship between the marks and their related requesting IP addresses. Once detect the DDoS attack, the victim extracts the marks from attack packets and further obtains the attack sources by requesting the MOD server. Although DDPM uses the marking space in a round-robin style to improve the salability, in the face of the large scale networks, it still suffered the following disadvantages: the small number of traceable sources and the load imbalance. Therefore, this paper proposed a scalable dynamic deterministic packet marking approach, termed as SEEK. In order to overcome these drawbacks, SEEK first designs a hierarchical architecture for the traceable alliance and dynamic probabilistic packet marking to balance the load of the relevant traceback devices, and then employs a number of techniques, such as the expansive label-loading space, the reuse label space, and the adaptive label management, to increase the number of available labels and improve their utilization. We perform extensive mathematical analysis and simulations to evaluate our approach. The results show that our approach significantly outperforms the prior approaches in termes of the scalability and efficiency by more than 20 percent.

This work is supported by the National Natural Science Foundation of China (Nos. 61601107, U1708262, 61602227), the China Postdoctoral Science Foundation (No. 2019M653568), the Natural Science Foundation of Hebei Province of China (Nos. F2020501013, F2015501122, F2015501105) and the Fundamental Research Funds for the Central Universities (No. N2023020). These projects aim to make advances to the cyber attack defense and the evolution of network security. Achievements of this paper aim to solve the scalable and efficient IP traceback for defending against DDoS attacks.