软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2017,28(10):2737−2756 [doi: 10.13328/j.cnki.jos.005149]

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

一种高精度、低开销的单包溯源方法*

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: 鲁宁, E-mail: luning@neuq.edu.cn

摘 要: 混合拒绝服务攻击是当前互联网面临的主要威胁之一,针对它的单包溯源技术已成为网络安全领域研究的重点和热点.鉴于已有的单包溯源研究存在处理开销大、溯源精度低等问题,提出一种高精度、低开销的基于标签交换的单包溯源方法,简称 S3T.该方法的基本思想是借鉴 MPLS 网络的交换路径生成原理,在溯源路由器上建立面向反向路由的追踪痕迹,降低溯源存储开销.然后,通过并行化建立追踪痕迹、灵活配置溯源路由器存储容量和自适应调整追踪痕迹存储时间等手段加快溯源路由器处理 IP 包速率,同时提高溯源精度.通过理论分析和基于大规模真实互联网拓扑的仿真实验,其结果表明,相比以往方案,S3T 在溯源开销和溯源精度方面确实有了很大的改善.

关键词: 网络安全;混合拒绝服务攻击;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.一种高精度、低开销的单包溯源方法.软件学报,2017,28(10):2737−2756. http://www.jos.org.cn/1000-9825/5149.htm

英文引用格式: Lu N, Wang SG, Li F, Shi WB, Yang FC. Efficient and precise approach for single-packet traceback. Ruan Jian Xue Bao/Journal of Software, 2017,28(10):2737−2756 (in Chinese). http://www.jos.org.cn/1000-9825/5149.htm

Efficient and Precise 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: The mixed denial-of-service attacks have become the mainstream threat to the Internet service availability. Tracing an individual attack packet to its origin is an important step in defending against such attacks. For this reason, researchers have proposed several approaches for single-packet IP traceback. However, these prior works suffer from the following disadvantages: The high process overhead at routers and low traceback accuracy. To address the issue, this paper proposes an efficient and precise approach, termed as S3T, for single-packet traceback based on label switching. Borrowing the idea of label switching principle in MPLS networks, its main method is to make use of the reverse routing to set up audit trails, and then employ parallel processing of audit trail establishment, more flexible storage assignment for traceback routers and adaptive adjustment for the audit trail retention time to overcome those drawbacks. Extensive analysis and simulation are carried out to conduct thorough numerical comparisons between S3T and the state-of-the-art approaches. The results show that S3T significantly outperforms the existing approaches in terms of the process overhead at routers, as well as the traceback accuracy.

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

* 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 of China (F2015501122); Doctoral Scientific Research Foundation of Liaoning Province (F201501143)

收稿时间: 2015-12-13; 修改时间: 2016-02-24, 2016-05-13, 2016-08-09; 采用时间: 2016-10-03

拒绝服务(denial-of-service,简称 DoS)攻击在互联网兴起之初就已经产生.近几年,随着黑客技术的不断升级,DoS 攻击正在逐渐演化为一种高级持续性渗透攻击,而引起这种变化的最根本原因是“混合拒绝服务(mixed DoS,简称 MDoS)攻击”的出现[1].与传统 DoS 攻击相比,MDoS 通过整合多重攻击向量(包括高速匿名攻击和低速匿名攻击)使得攻击目标延伸到与受害主机相连的任一容易产生瓶颈效应的实体,极大地提升了攻击成功率,从而带来更大的危害.因此,如何抵御 MDoS 攻击就成为互联网安全保障中一个亟待解决的问题.

在网络攻击发生后,针对它的防御过程通常包括 3 个阶段:威胁预警、攻击定位和恶意流过滤,分别对应威胁检测、溯源和阻断技术.而本文只关注能够通过重构 MDoS 的攻击路径来锁定攻击源的单包溯源技术.溯源作为一种事中反匿名技术,能够有效地抵御那些因事前反匿名技术(例如源认证[2]、出口边界过滤[3]等)的过滤粒度较大而漏报的匿名攻击活动.进一步考虑到 MDoS 攻击向量的多样性,本文主要针对可同时兼顾高速和低速匿名攻击向量的单包溯源方法展开研究.假定将源地址伪造的 IP 包称为攻击包,其中攻击包生成主机和攻击包接收主机分别对应攻击者 A 和受害者 V.攻击路径 P_A 则被定义为一组从 V 到 A 的溯源路由器序列,表示为 $P_A=(N,L)$,其中,N 是中间路由器集合,L 是有向链路集合.在多源攻击场景中,攻击图可由从 V 到 A 的所有攻击路径重叠覆盖生成.图 1 描述了单包溯源网络模型及其处理过程,溯源路由器通过提取和记录每个转发包或路由状态特征来建立追踪痕迹,受害者在攻击发生后仅使用单个攻击包就可取证并还原路径.目前,绝大部分溯源研究只针对高速匿名攻击[4−6],而对可应对 MDoS 攻击的单包溯源研究较少.尽管已有一些研究分别在降低存储开销、支持可增量部署以及增强可操作性等方面取得一定效果,但仍然存在以下不足:(1) 它们大都采用包记录技术来建立追踪痕迹,致使溯源路由器的存储开销与其 IP 包转发量成正比.也就是说,随着运行时间的推移,路由器存储开销将呈线性增长;(2) 它们通常对追踪痕迹采用集中管理方式,致使溯源路由器只能串行处理到达的数据包.很明显,增加额外操作必然会严重降低路由器的包处理速率,从而引发较大的网络时延;(3) 它们没有考虑溯源路由器的负载不均衡性,往往将存储资源平均分配给每个溯源路由器,致使大量高负载设备因存储短缺而出现路径片段被交替覆盖的现象,造成较高的溯源漏报率,影响了溯源精度;(4) 它们没有区分同一溯源路由器上不同追踪痕迹的重要程度,试图通过无差别管理方式来对待所有的追踪痕迹,造成路由器上本就数量有限的存储资源,其中绝大部分被用来建立正常路径的追踪痕迹,而面向攻击路径的追踪痕迹却只能因资源不足进行彼此覆盖,破坏了追踪痕迹的唯一标识性,从而降低了溯源精度.

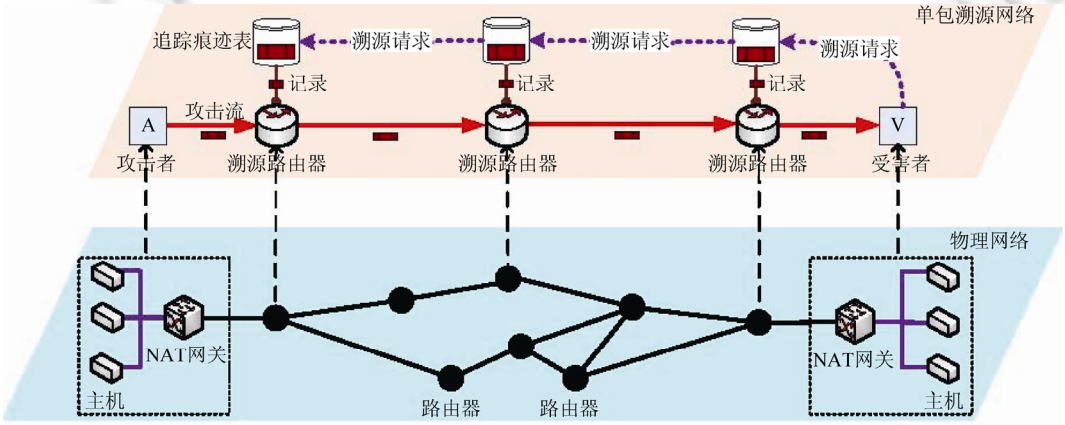


Fig.1 The single-packet IP traceback network model

图 1 单包溯源网络模型

针对上述挑战,本文提出一种高精度、低开销的基于标签交换的单包溯源方法(label switching based single-packet traceback,简称 S3T).首先,它摒弃了传统的包记录技术,借鉴多协议标签交换网络的交换路径生成原理,通过将转发包与路径标识符——标签逐一绑定,完成溯源路由器上下游之间的标签交换,在溯源网络上建立面向传输路径的追踪痕迹,使得溯源路由器的存储开销不再与 IP 包转发量相关,而只与经过它的传输路径数

量有关.其次,它引入溯源接口分流器,代替溯源路由器成为核心处理单元,通过计算路由器接口的中心度来合理地分割标签空间,进一步采用基于资源池管理模型的标签发布策略来实现数据转发包与标签的绑定,完成追踪痕迹的并行化建立,从而加快 IP 包处理速率,减小因溯源处理带来的网络时延.然后,鉴于当前路由协议大多基于最短路径的特征,引入复杂网络的介数理论来估算路由器接口的最大可能负载,以此为依据,灵活配置每个溯源接口分流器的存储容量,降低因交替覆盖带来的溯源漏报率.最后,通过观察网络攻击发生前后标签发布量的变化,使用轻量级的移动平均线理论来预测路径类型,进一步采用延时和及时两种方式来管理攻击痕迹和正常痕迹,提高存储利用率的同时降低因资源不足造成的溯源精度问题.

为了验证本文提出的 S3T 方法,首先对其高效性进行了理论分析,然后在基于大规模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,S3T 方法不仅延续了传统方法的优势,而且还极大地改善了溯源开销和精确度.在基于 CAIDA 拓扑的仿真实验中,溯源存储开销几乎能够被降低 7 倍,处理开销也被减少 1 倍.同时,溯源精度的提升幅度则达到了 20%.

本文第 1 节介绍我们提出的 S3T 方法,其中,第 1.1 节给出方法的整体架构,第 1.2 节~第 1.5 节分别给出追踪痕迹并行化建立、标签管理、存储资源分配、变形包追溯等设计细节.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 基于标签交换的单包溯源方法

本文提出的 S3T 方法采用与传统方法相同的系统模型[7−14]:当 IP 包在网络中传播的时候,具有溯源功能的路由器(简称溯源路由器)负责建立追踪痕迹;当网络攻击发生后,受害者发出溯源请求并由溯源管理器负责取证,重构攻击路径.为此,本文第 1.1 节介绍 S3T 方法的基本框架,即“追踪痕迹建立”和“攻击路径重构”的基本原理,之后各节分别阐述 S3T 方法在不同场景中的设计细节.其中,第 1.2 节介绍如何在现有网络协议框架下建立追踪痕迹;第 1.3 节介绍如何在高速网络下建立追踪痕迹;第 1.4 节介绍如何在面对大规模攻击时建立追踪痕迹;第 1.5 节介绍如何在存储资源不充足的条件下建立追踪痕迹;第 1.6 节介绍如何在变形网络中建立追踪痕迹和重构攻击路径.

1.1 整体思想

S3T 方法的主要难点在于:当数据包在溯源网络(本文把以底层路由网络为基础,由溯源路由器构成的覆盖网络称为溯源网络)上传播的时候,如何在网络上准确地建立面向传输路径的追踪痕迹,以及当网络攻击发生后,如何利用这些痕迹快速地重构出整条攻击路径.为此,本文首先借鉴多协议标签交换(multi-protocol label switch,简称 MPLS)网络中转发等价类的思想,将溯源网络中一组拥有相同传输路径的数据包集合(即这些数据包的目的地址和路径经过节点全部相同)定义为溯源等价类(traceback equivalence class,简称 TEC),并把它作为溯源路由器中最小的处理单位.其次,为了减小溯源路由器的存储开销,设计一种新的更紧凑的溯源路由器标识符(router identification,简称路由器 ID)来取代冗长的 IP 地址,使得部分中间节点标识能够直接存放到数据包的标记域中,不需要它们再记录追踪痕迹.当然,每个溯源路由器还需维护一张路由器 ID 和对应 IP 地址的映射表,称为邻居映射表(neighboring mapping table,简称 NMT),以便它们之间能够正常通信.然后,利用 MDoS 攻击中路由路径无法伪造的特点,参照 MPLS 网络中标签交换路径(label switching path,简称 LSP)建立原则,提出一种取值范围受限的无符号整型标识符——标签,用来区分所有同宿不同源的溯源等价类.基于上述信息,构建一个三元组[目的 IP 地址,上游路由器 ID,标签]作为标记信息,并将它与 TEC 实现唯一性绑定,进而完成三元组与传输路径的一一绑定.一旦绑定成功,就意味着溯源路由器利用该三元组即可识别出所有到达的 TEC.需要指出的是,溯源路由器可以给不同 TEC 分配相同的标签,但前提是它们的目的地址不相同.编码原理及溯源等价类 TEC 与三元组[目的 IP 地址,上游路由器 ID,标签]的具体绑定方法(偏工程操作)如图 2 所示:假设溯源路由器 Ru 将标签 L 指派给即将在下游链路 $Ru\rightarrow Rd$ 上传播的溯源等价类 TEC_F,其中,TEC_F 是指从入口路由器 Re 传播到目的主机 F 的数据包集合(即同源同宿的数据流).$\forall$数据包 $P\in TEC_F$,当 P 到达 Ru 后,Ru 就会把信息[Ru ID,L]写到 P

的标记域中,并且通过路由路径将 P 转发到下游 Rd,其中,标记域是指数据包中极少部分不常用的 IP 包头字段,主要包括 Identification 字段、保留位和分片偏移字段,共 30 位,具体原因在第 1.2 节第 1 段给出表述.根据图 2 可知,通过字段重载操作,标记域在溯源网络中承载的是标签和路由器 ID,已知路由器 ID 占 12 位,因此,标签占 30–12=18 位,这也就是说,标签 L 的取值范围(即标签的容量)是[0,262143].标签取值范围决定了溯源路由器判别同宿不同源的溯源等价类 TEC 的能力,这也意味着本方法能够准确识别 262 144 条同宿不同源的路由路径.当 Rd 收到 P 后,Rd 即可利用 P 中所承载的标记信息[标签 L,Ru ID,目的地址 F]来判断 P 是否属于 TEC_F,进而通过记录这些信息来建立路径片段痕迹.为此,它首先从 P 中提取标记信息[Ru ID,L],然后将它记录到追踪痕迹表(trail management table,简称 TMT),同时指派新的标签 M 给下一个下游链路.从中不难看出:(1) L 只是在 Ru 和 Rd 之间有意义,正是这种松散的绑定方式使得所有溯源路由器的标签发布操作能够完全独立运行,不需要彼此通信共享,减小了开销;(2) 路径一旦建立,Ru 和 Rd 就无需分配新的标签给 TEC_F,也就不再执行记录操作,仅将已记录的路径信息重新写入数据包的标记域即可.最后,遵从 LSP 还原理论,采用基于标签首尾串联的路径片段拼接法来重构攻击路径.具体方法如下:假设溯源管理器收到溯源请求 $Request$=[Rd,M]后,随即就会向 Rd 发出取证请求.然后,Rd 在自身的追踪痕迹表中搜索出标签为 M 的表项.如果查找结果为[Ru ID,L],那么 Rd 通过查找路由器标识符与 IP 地址映射表来判断出 Ru ID 就是指溯源路由器 Ru,进而还原出路径片段 Ru→Rd,然后发出新一轮溯源请求 $Request$=[Ru,L],如此迭代可逐渐还原出整条路径.

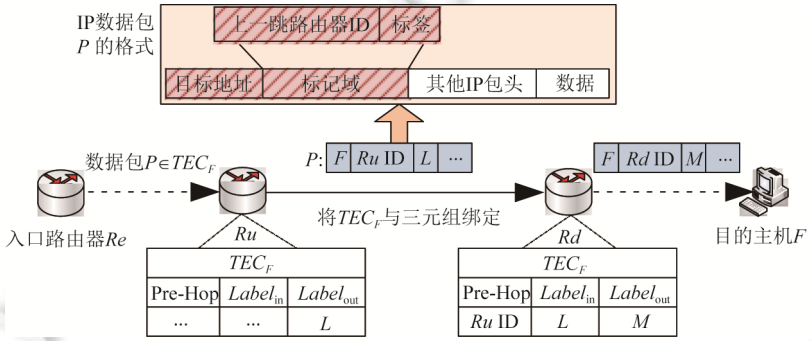


Fig.2 The procedure of binding TEC

图 2 TEC 绑定操作示意图

本文通过举例方式来进一步阐述 S3T 方法的基本思想.在图 3 所示的例子中,TEC_0 表示由攻击者 A 发向受害者 V 的数据包集合,攻击路径 P_A=(N,L)表示 TEC_0 在网络上传播时所遵循的路由路径,其中,N={R_1,R_2,R_3},L={R_1→R_2,R_2→R_3};TEC_1 表示由正常用户 H 发向受害者 V 的数据包集合,正常路径 P_H=(N,L)则是它所对应的路由路径,其中,N={R_2,R_3},L={R_2→R_3}.不失一般性地假设 A 和 H 之间不发生任何通信.

【追踪痕迹建立】当 IP 包 x 到达入口路由器(ingress router,简称 IR)R_1 时,首先利用 x 的目的地址来选定追踪痕迹子表,然后分配标准出标签(standard out label,简称 SOL,SOL 只能由入口路由器分配)3 给 x 并标记[SOL,R_1 ID]到 x 中,最后将它转发到下游路由器 R_2.那么,如何认定 R_1 是入口路由器呢?在一般情况下,由于到达入口路由器的标记域是没有赋值的,因此判别 IR 非常容易.但是,考虑到某些攻击者可能会利用该系统漏洞,通过伪造标记域信息来破坏追踪,为此,R_1 需要将 x 携带的路由器 ID 与 NMT 中所有标识符进行匹配.如果不符合,就可认定 x 是恶意包,进而将 R_1 判定为 IR.此外,为了进一步防止攻击者通过中间人等技术手段来骗取 R_1 的邻居标识符,R_1 可以每隔一段时间为邻居路由器重新着色,通过及时变换标识符的方式来避免被欺骗.当 x 到达某个中间路由器 R_i 时,R_i 首先分配出标签给 x,然后将追踪痕迹[入标签,出标签,R_{i-1} ID]插入到与 x 相关的子表中,同时将[R_i ID,出标签]标记到 x 中,最后将它转发到下游.需要注意的是,如果出现同宿路由汇聚现象,例如 R_2 和 R_3,为了能够清晰地区分 TEC,溯源路由器必须为它们分配不同的出标签.当 x 到达受害者 V 时,就说明 P_H 和 P_A 在溯源网络中已被完全建立.之后,所有路径节点只需执行子表的查找和包标记操作,不再需要执行表插入.追

踪痕迹建立过程如算法 1 所描述.

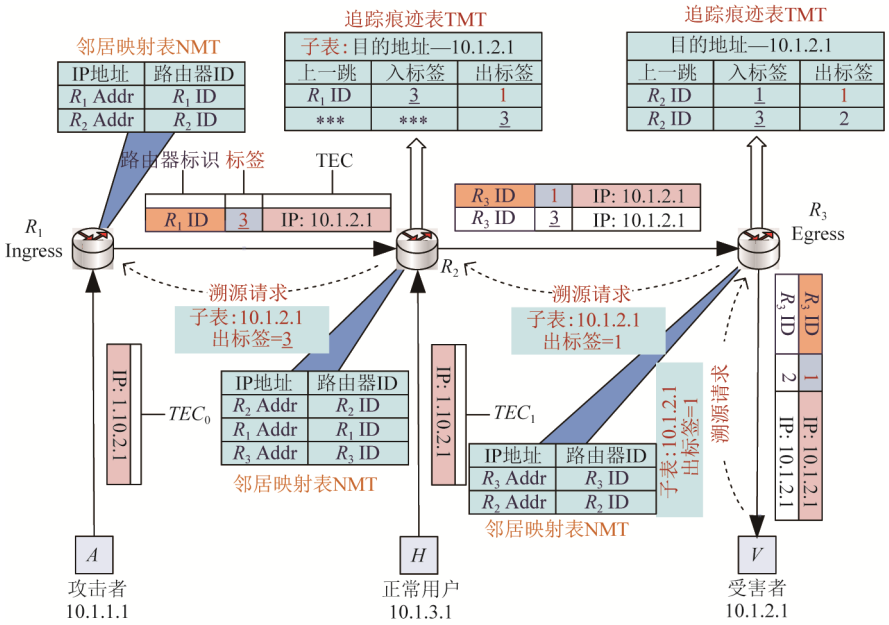


Fig.3 An example of S3T

图 3 对 S3T 方法进行举例

算法 1. 追踪痕迹建立.

1.输入:当前路由器标识符 d,到达 IP 包 P,邻居映射表 NMT,追踪痕迹表 TMT;

2.输出:新标记的 IP 包 P_{new},已更新的追踪痕迹表 TMT_{new}.

3.步骤: **FOR** each packet P **DO**; //针对每一个到达路由器的 IP 包

4. **IF** P.R-ID is contained in NMT **THEN** //判断 IP 包携带的上游路由器 ID 是否合法

5. Use the P.destination to obtain the subtable T from TMT; //利用目的地址来获取子表 T

6. Flag:=false; //标记追踪痕迹是否已经建立

7. **FOR** each item t in T **DO** //通过遍历,判断与 P 相关的追踪痕迹是否已建立

8. **IF** t.prehop-ID=P.R-ID **and** $t.label_{in}$=P.label **THEN** //判断 P 携带信息是否存在

9. Flag:=true; //追踪痕迹已经建立

10. P.R-ID:=d; //标记新的路由器 ID 和标签,生成 P_{new}

11. $P.label:=t.label_{out}$;

12. break;

13. **END FOR**

14. **IF** Flag=false **THEN** //建立新的追踪痕迹

15. Assign a new $label_{out}$ L; //分配标签

16. Construct a new item (P.R-ID,P.label,L) and insert it into T; //生成 TMT_{new}

17. P.R-ID:=d; //标记新的路由器 ID 和标签,生成 P_{new}

18. P.label:=L;

19. **ELSE** //如果 P 所携带信息不合法,那么当前路由器就是入口路由器,无需建立追踪痕迹

20. P.R-ID:=d; //标记新的路由器 ID 和标签,生成 P_{new}

21. P.label:= Standard Out Label;

22. **END FOR**

【攻击路径重构】当网络攻击发生后,受害者首先利用已有的入侵检测技术(intrusion detection system,简称IDS)[15,16]来识别IP匿名包,然后将它们以溯源请求的形式发送给溯源管理器.溯源管理器接收请求后,首先从IP匿名样本包中提取标记信息[上游路由器 ID,标签],进一步识别出离受害者最近的溯源路由器 R_3,然后将[标签:1,受害者 IP:10.1.2.1]以取证请求的形式发送给 R_3.R_3 接收到请求后,首先从 TMT 中选定与该受害者 IP 相关联的子表 10.1.2.1,之后将该标签与所有表项的出标签进行匹配,并将符合表项返回,然后利用 NMT 将该表项的上游路由器 ID 转换为路由器 IP,进而确定 R_2,最后将[R_2,符合表项的入标签]以溯源回复的形式发送给溯源管理器,由此发起新一轮溯源请求.当溯源管理器发现溯源回复的入标签是 SOL 时,也就意味着上游路由器就是路径入口,溯源过程结束.溯源路由器处理取证请求的过程如算法 2 所描述.

算法 2. 攻击路径重构.

1.输入:取证请求 request(目的地址 D,标签 M),邻居映射表 NMT,追踪痕迹表 TMT;

2.输出:取证回复 response(上游路由器 IP 地址 Adr,标签 E).

3.步骤: Use D to obtain the subtable T from TMT; //利用目的地址 D 来获取子表 T

4. **FOR** each item t in T **DO** //通过遍历,获取匹配项

5. **IF** t.label$_{out}$=request.M **THEN** //查找与请求标签相匹配的表项

6. Lasthop-ID=:t.lasthop;

7. response.Adr=:NMT.getAddress(Lasthop-ID); //利用 NMT,将路由器 ID 转换为 IP 地址

8. response.E=:t.label$_{in}$;

9. return response;

10. **END IF**

11. **END FOR**

12. response=:NULL; //所查询的追踪痕迹已经被覆盖,或者该数据包在当前路由器上发生了变形

13. return response;

到目前为止,只是介绍了 S3T 方法的基本框架,下面将详细讨论它的设计细节.

(1) 标记域编码:在对现有网络改动尽可能小的前提下,如何设计标记域,用于存放路径片段?以及如何对标记域进行编码,在不丢失信息的前提下提高其利用率?

(2) 追踪痕迹快速建立:在高速路由器上,如何快速建立追踪痕迹,以便加快路由器的 IP 包处理速度?

(3) 标签管理:在面对大规模网络攻击时,如何管理有限的标签资源,避免标签的重复分配破坏其唯一标识性,进而降低溯源误报率?

(4) 溯源设备存储配置:鉴于溯源设备的负载不均衡,如何合理配置其存储容量,防止追踪痕迹被交替覆盖,降低溯源漏报率?

(5) 变形包追踪:由于攻击包在传播过程中可能发生变形(例如 NAT 和 IP 隧道协议),如何向后兼容,进而实现变形包追踪?

1.2 标记域编码

在追踪痕迹建立过程中,除了记录操作,溯源路由器还同时执行标记操作,用于将路径信息[路由器 ID,标签]写入到标记域中.为了对现有网络协议的改动尽可能地小,本文通过重载 IP 包头的 Identification 字段、保留位和分片偏移字段来设计标记域,其出发点是:随着互联网的不断演进,传统网络(例如 X.25)已逐渐被淘汰,而且随着 TCP 协议中最大分段大小(maxitum segment size,简称 MSS)的广泛应用,在当前互联网中 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[17−19].因此,IP 分片技术已处于淘汰边缘,分片相关字段也就变得无关紧要,进而可做他用.根据 IP 协议,分片相关字段(即标记域)总共占据 30 位.具体标记域编码策略如图 4 所示,前 12 位用来存放路由器 ID,剩余 18 位则用来存放标签.下面将介绍如此编码的原因及其引发的后续操作.

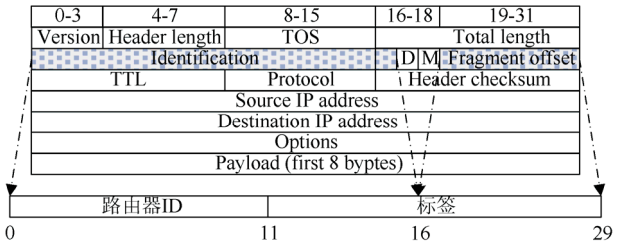


Fig.4 Mark domain encoding

图 4 标记域编码说明

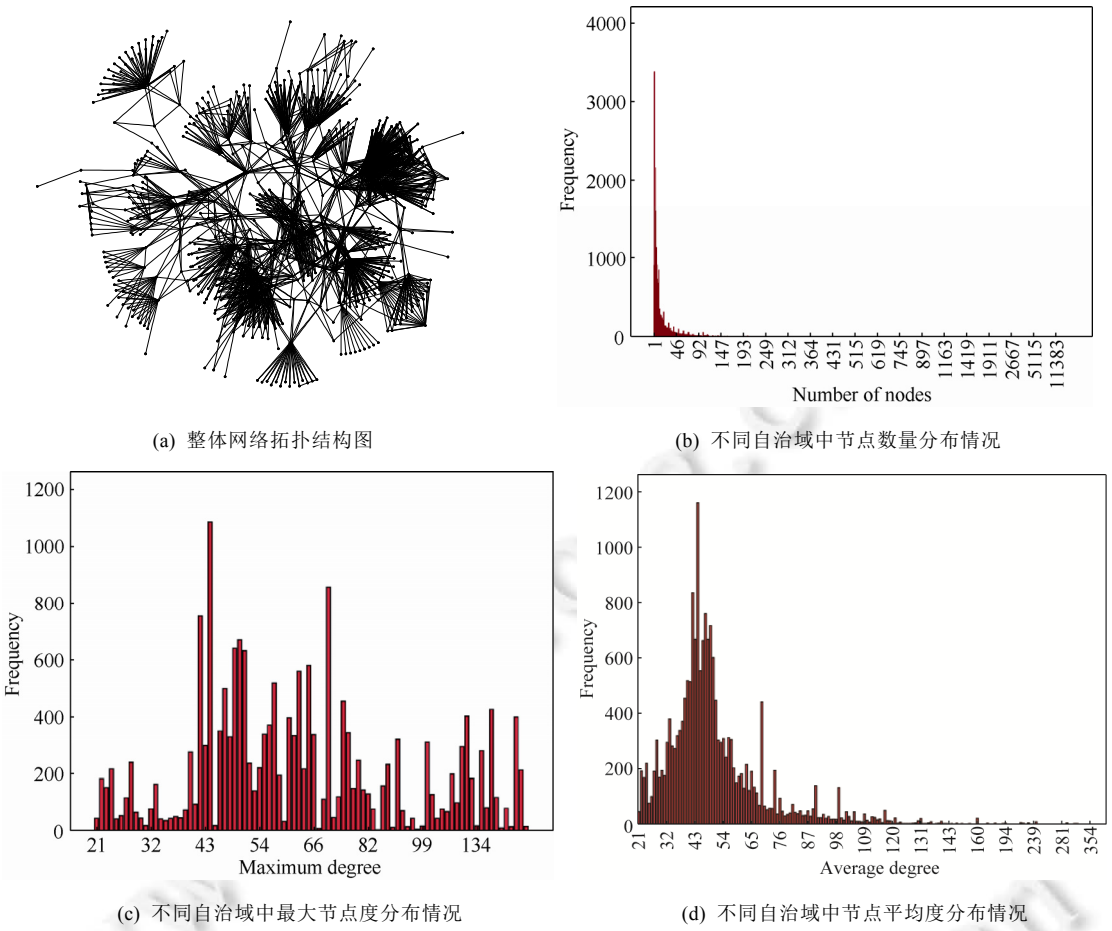
首先,通过理论分析和真实网络数据统计,本文发现:对于任一溯源路由器来说,使用 12 位标识足可以唯一识别它的所有邻居.说明原因之前,需要先探讨路由器标识符(简称路由器 ID)在溯源过程中所起到的作用.根据第 1.1 节的介绍,溯源路由器会利用取证结果(即上游路由器的 ID)在邻居映射表中搜索对应的 IP 地址,进而确定上游路由器的真实身份.由此可以发现整个路径重构过程是逐跳拼接的,而每一次取证只需识别出它的上游邻居.这也就是说,路由器 ID 仅需唯一地标识上下游关系即可,无需全网标识.进一步推断出,如果将整个溯源网络看成是一个简单无向有限图,而且采用图着色理论来对路由器 ID 编码,那么只需要保证 2 跳以内的邻居路由器具有不同的颜色即可.另一方面,要想获得更多的标签资源,就必须尽可能地缩短路由器 ID 所占位数,也就是使用最少的颜色数对路由器着色.因此,路由器标识符编码问题进一步被抽象为 2-距离点着色问题,具体定义如下.

定义 1. 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链路.溯源网络是一种虚拟网络系统,它以底层物理网络为基础.在溯源网络中,节点之间的虚拟链路是逻辑上的,通常对应于底层网络的物理路径,即路由路径.

定义 2. 给定图 $G=(V,E)$,称映射$\pi:V\to\{1,2,\ldots,k\}$为 G 的一个 k 点着色,简称着色,称$\{1,2,\ldots,k\}$为色集.若对 G 中任意两个距离不大于 2 的顶点 u 和 v 均满足$\pi(u)\neq\pi(v)$,则称该着色为正常的.图 G 的正常 k 着色的最小 k 值称为 G 的色数,记为$\chi_{2d}(G)$,简记为χ_{2d}.

通过对网络联合分析组织(cooperative association for Internet data analysis,简称 CAIDA)搜集的互联网路由器级拓扑进行了面向自治域的特征统计和分析[20](结果如图 4 所示),结果表明:当前互联网中绝大部分的自治域节点数 $n<2^{12}$,还有少量自治域的最大节点度 $\Delta>2^7$.根据已经推算出的 2-距离点着色数上界表达式$\min\{\Delta^2+1,n\}$[21],本文将溯源着色数的上界进一步推进到2^{12}.这也就是说,对于任一溯源路由器来说,12 位路由器 ID 就足以唯一标识它的所有邻居.另外,由于 2-距离点着色问题是典型的 NP-hard 问题.本文建议使用求解更加精确且耗时相对较少的基于遗传算法的 2-距离点着色方法[22].

其次,18 位的标签存放空间意味着溯源路由器可分配的标签集合只有[0,*pow*(2,18)−1].鉴于不断扩张的互联网规模,溯源路由器所承载的 TEC 数量也会不断增大,进而导致溯源路由器所需要的标签数量也会激增.然而,受制于有限的标签存放空间,溯源路由器能够支配的标签可能不足.为此,本文借鉴 IP 地址的分级管制思想,提出两级追踪痕迹表.具体方法如图 5 所示:将追踪痕迹表根据 TEC 的目的地址划分为若干个子表,即每个子表都会与一个目的地址相关联,将属于该目的地址的追踪痕迹都存放到该子表,从而使得不同的子表能够享用相同的出标签,在一定程度上提高了标签利用率.值得注意的是:虽然根据目的地址的不同,追踪痕迹表可能包含 3 个子表,但是由于在图 5 中 A 和 H 之间不发生任何通信,因此只有与受害者相关联的子表才会被激活.



(a) 整体网络拓扑结构图 (b) 不同自治域中节点数量分布情况

(c) 不同自治域中最大节点度分布情况 (d) 不同自治域中节点平均度分布情况

Fig.5 The network topological feature description in CAIDA

图 5 CAIDA 数据的网络拓扑特征说明

1.3 追踪痕迹并行化建立

为了应对逐渐增长的流量负担,高速路由器需要维护多张追踪痕迹表以达到同时处理多个 TEC 的能力,进而使得它的追踪痕迹建立速率与 TEC 到达速率相匹配,降低转发时延.为此,本文引入一种具备独立读、写功能的面向接口的硬件设备,称为溯源网络分流器(traceback network probe,简称 TNP),使得路由器上不同接口的 TEC 可以同时被处理,从而更快地建立追踪痕迹.图 6 描述了以 TNP 为核心处理单元的溯源网络图,以及在 TNP 上追踪痕迹表的组织方式.以图中接口数最多的 R_2 为例,它的周围共放置了 3 个 TNP 设备,每个设备都会维护一张具备读、写功能的追踪痕迹表,用来存放所有穿过对应接口的溯源路径信息.这也就意味着,每个追踪痕迹表的存取速度不再需要与 R_2 的 IP 包到达率相匹配,而只需与接口的包到达率相匹配.

溯源网络分流器应该具备以下功能:IP 包解封、追踪痕迹表查询和 IP 包封装.为了保证 TNP 的接入对尽可能小地影响到其他网络设备,本文建议通过升级当前流行的网络分流器(network probe,简称 NP)来实现 TNP,原因是现有的 NP 已经实现接近线速的 IP 包解封和封装功能,而且它还具备独立部署和透明接入等优点.为了完成 TNP 的功能,NP 还需要升级的内容是增添追踪痕迹表.考虑到追踪痕迹表最频繁的操作是表查询,而且是按所存追踪痕迹的部分内容进行查找的,为了高效地执行该操作,本文建议该表使用已被广泛应用的基于内容寻址的相联存储器来实现.该技术可将追踪痕迹表的查询时间降低为 $O(1)$.

鉴于 TNP 每处理一个 IP 包都需按顺序执行 IP 包解封、追踪痕迹表查询和 IP 包封装等操作,本文通过分

析发现,并不是每个动作都需要 TNP 的所有硬件参与执行.例如,IP 包解封操作需要激活包解封相关硬件,而追踪痕迹表查询只需激活相联存储器硬件.这也就是说,TNP 的各部分硬件在某些周期内进行操作,而在某些周期却是空闲的.因此,如果调度恰当,让各个部分紧张工作,即把多条追踪痕迹建立在时间上重叠起来,完全可以提高各个部件的工作效率和运行速度.例如,鉴于 TNP 是按到达顺序来处理 IP 包的,当包解封部件完成对当前 IP 包的操作后,交给追踪痕迹表去继续处理,同时进行下一个 IP 包的解封动作.基于此,本文采用不规则流水线方式来实现 TNP,其原理如图 7 所描述.假设 TNP 处理 IP 包的周期 $T=5t$,其中,IP 包解封和封装各需时间 t,而追踪痕迹表查询所需时间为 $3t$.如果串行处理 4 个 IP 包,那么处理时间为 $20t$;如果流水处理,那么处理时间降低为 $12t$.根据流水线原理,与串行相比,该技术能够将 TNP 完成 n 个连续任务的时间降低 $\left[\sum t_i+(n-1)t_2\right]/n\sum t_i$.

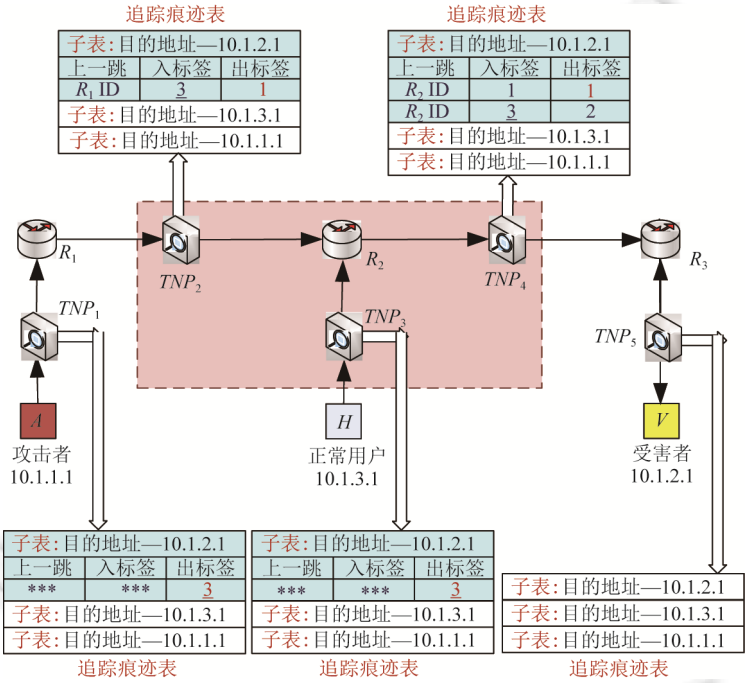


Fig.6 The traceback network with TNP as the core processor

图 6 以 TNP 为核心处理单元的溯源网络图

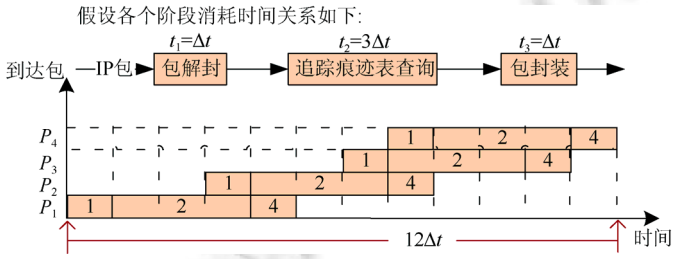


Fig.7 The audit trail establishment based on irregular line operation

图 7 基于不规则流水线的追踪痕迹建立机制举例

如果溯源路由器 R_v 的接口都已经配置 TNP,那么 R_v 的标签空间[0,262143]应该根据各自 TEC 负载,被合理地切割为若干块,并将它们分配给相关的 TNP,进而使得标签唯一性不会因为 TNP 的介入而被破坏.假设 R_v 中某子表的标识符为 D,为了实现并行化,它的标签空间应遵循以下规则进行切割:TNP_i 代表与 R_v 接口相连接的溯源

设备,$Rat(ATT_D^{TNPi})$表示溯源设备 TNP_i 所承载的目的地址为 D 的溯源路径占 R_v 所承载的相关路径的比例.显然,$Rat(ATT_D^{TNPi})$越高,意味着 TNP_i 获得的标签空间也就应该越大;反之亦然.如果溯源系统已被全网部署,鉴于路由协议大都基于最短路径,可以使用复杂网络边介数理论来估算 $Rat(ATT_D^{TNPi})$,公式如下:

$$Rat(ATT_D^{TNPi}) = \sum_{s\in\Omega_{user}} g_D^{TNPi}(s) \Big/ \sum_{TNP_i\in R_v} \sum_{s\in\Omega_{user}} g_D^{TNPi}(s) \tag{1}$$

其中,$g_D^{TNPi}(s)$表示从端用户 s 到端用户 D 的所有经过溯源设备 TNP_i 且流入 R_v 的最短路由路径数量,Ω_{user} 表示溯源网络中端用户集合.以图 6 中 R_2 为例,$Rat(ATT_D^{TNP2})$=1/2,$Rat(ATT_D^{TNP3})$=1/2,那么,$Label_{TNP2}$=[0,131071],$Label_{TNP3}$=[131072,262143].一旦标签空间分割完成,TNP 还将维护一张标签预留表,存放追踪痕迹子表的标签空间.假设溯源路由器 R 的每个接口上都配置 TNP,且经过每个 TNP 的 TEC 数量相同(也就是路由路径数量相同),那么,每个 TNP 被分配的标签空间大小 T=262144×(1/I),其中,I 是该 R 的接口数量.

1.4 标签管理

面对大规模网络攻击,为了更快地分发和更灵活地管理标签,本文撇弃传统的基于取模技术的顺序分发策略,提出基于资源池的标签分发策略.其基本原理是将标签与资源池绑定,如果 TNP 需要创建新路径,资源池就随机选取一个标签分配给该路径,同时将该标签标记为忙状态,不会再被发布;如果因存储或标签资源短缺而需要删除部分追踪痕迹,那么资源池必须重新设置状态信息,以便回收相关标签,进而提高其使用效率.

按照溯源路径的不同,已分配的标签可分为攻击标签和正常标签.很明显,对于溯源来说,前者更为重要,因为它的存在与否直接影响到溯源成功率.为此,本文提出基于移动平均线的标签管理策略,分别采用延时和及时两种方式来对待这两类标签.基本设计思路如下:通过观察攻击发生前后 TNP 中 TEC 到达数量的变化特征来探索其呈现方式及规律,并将经济学中移动平均线理论与最近最少使用原则相结合,建立面向 TEC 的重要性评估模型以预测相关标签类型,进而有偏向性地动态管理标签保存时间,提高溯源精度.需要说明的是,不能依据预测结果直接丢弃攻击包,这会造成大量正常包因预测失准而被丢弃,进而严重影响通信质量.

该策略的具体实现细节描述为:将 TNP 的存储空间分为 GHOST 和 REAL 两类,其中,REAL 的保存时间要高于 GHOST.也就是说,GHOST 的标签采用及时回收,而 REAL 则是延时回收.任给 TEC I,TNP 通过计算重要程度移动平均值 S 来决定 I 的存储位置.如果 S 大于阈值,就将 I 从 GHOST 升至 REAL;如果 S 小于阈值,就将 I 从 REAL 降至 GHOST;如果需要回收,就选择 GHOST 中 S 最小的标签.S 的计算公式如下:

$$S_n(I) = S_{n-t}(I) - \frac{P_{n-t}(I)}{n} + \frac{P_n(I)}{n} - \gamma \tag{2}$$

其中,$S_n(I)$是指 I 的预测结果,n 是指当前时间.t 是计算 $S_n(I)$的时间窗(即移动平均数周期),t 越大,TNP 的计算开销也就越小,但预测精度越低;t 越小,TNP 的计算开销越大,预测精度却越高.为了平衡二者,本文建议 t 应该设置为攻击时间的平均值.γ是为了降低 $S_n(I)$的惩罚系数,属于经验值.$P_n(I)$是 I 的重要程度值,计算公式是

$$P_n(I) = F\cdot m + R\cdot(t_c - t_p) \tag{3}$$

其中,F 是指追踪痕迹出现频率权重,R 是指 I 的近因权重,m 是指 I 的出现次数,t_c 和 t_p 分别是 I 的最近一次到达时间和上一次到达时间.

1.5 溯源设备存储配置

虽然存储资源是溯源系统最主要的开销,但是限于成本和硬件规模等因素,ISP 能够提供的资源数量非常有限.鉴于路由器中各接口承载的溯源路径数量不对等,进而导致 TNP 的负载不均衡,如果直接采用平均法来统一分配存储资源,那么必然会导致部分高负载节点因资源短缺出现溯源漏报现象,而其他空闲节点却出现资源闲置,从而降低了存储资源利用率.为了避免这种情况的发生,本文通过预估溯源设备的负载量,依据结果,及时、合理地分配给定的存储资源,进而提高其利用率.

根据 S3T 方法的追踪痕迹建立原理,TNP 的溯源存储开销将与其所承载的溯源路径成正比.假设 ISP 能够提供的存储资源总量为 n,通过估算每个溯源设备 TNP_i 所承载的溯源路径占全体链路所承载的溯源路径的比

例 $M(TNP_i)$,就可计算出 TNP_i 应该配置的存储容量 $S(TNP_i)=n\times M(TNP_i)$.如果溯源系统已被全网部署,通过引入复杂网络的节点中心度理论,那么 $M(TNP_i)$可计算如下:

$$M(TNP_i)=\sum_{s\in\Omega_{user}}\sum_{t\in\Omega_{user}}g_{TNPi}(s,t)\Big/\sum_{TNP_i\in\Omega_{TNP}}\sum_{s\in\Omega_{user}}\sum_{t\in\Omega_{user}}g_{TNPi}(s,t) \tag{4}$$

其中,$g_{TNPi}(s,t)$表示从端用户 s 到端用户 t 的所有经过溯源设备 TNP_i 的最短路由路径数量,Ω_{TNP} 和 Ω_{user} 表示溯源网络中 TNP 和端用户集合.以图 3 中 TNP_2 为例,由于溯源网络中所有 TNP 地位全部等价,因此 $M(TNP_2)=1/5$.如果存储资源总量 $n=10$,那么,$S(TNP_2)=2$.需要说明的是,由于存储资源的分配是在溯源系统运行之前就已经完成,因此,该策略对于分配算法的时间复杂度敏感度不高,所以,即使节点中心度的计算比较耗时,ISP 也能忍受.

1.6 变形包追踪

鉴于 TCP/IP 协议不会记录任何变形状态信息,为了达到向后兼容和追踪变形包的能力,溯源路由器除了追踪痕迹表,还需要维护一张包变形表(packet transformation table,简称 PTT),用来记录发生变形的 IP 包特征,进而完成包变形前后的映射关系.需要说明的是,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.变形包追踪的具体处理过程如下.

- 在追踪痕迹建立阶段,如果数据包 k 在当前溯源路由器 R_i 中发生变形,那么首先将 R_i ID 与标准变形标签(standard transformation label,简称 STL)0 写入 k 的标记域中,然后计算 k 的特征信息,同时将变形前 IP 包的目的地址和特征信息一起插入到 PTT 中.
- 在攻击路径重构阶段,如果当前溯源路由器 R_i 接收到一个携带标签 STL 的取证请求,那么就说明攻击样本包 k 在 R_i 曾经发生变形.因此,R_i 首先把 R_i ID 和 STL 写入到 k 中,然后计算 k 的特征值,最后利用 PTT 的映射关系来获得变形前攻击样本包的目的地址,之后的过程与算法 2 描述的相同.

上述过程遗留了两个问题尚未解决:一是如何提取 IP 包特征;二是如何存储该特征.针对问题 1,已有研究通过大规模的数据包采集和分析发现:如果选取 IP 包头的若干相关字段(包括版本号、IP 包头长度、TOS 和总长)以及数据载荷的前 8 个字节(共 24 字节)作为 IP 包的特征,那么特征冲突率在广域网中只有 0.00092%,再结合当前网络中 IP 包变形率只有 3%的分析结果[7],上述方法产生特征冲突的概率更会降到 0.00092%×3%,远在警戒线之外.针对问题 2,鉴于溯源路由器每处理一个 IP 包就需要存储 24 个字节,如此庞大的数据量很明显不适合网络设备.为此,本文建议使用一种空间利用率较高且计算相对简单的布鲁姆过滤器来存储特征字段.由于互联网中 IP 包变形率较低,根据布鲁姆过滤器的基本原理[23],该存储方法的误报率也会较低.

2 性能评价

本节通过理论分析和仿真实验对 S3T 方法的性能进行了评价,其中,第 2.1 节使用溯源效果评估模型来证明相较于已有单包溯源方法(SPIE[7]、HIT[11]、WHIT[12]、PSIT[14]),S3T 方法的高效性,第 2.2 节通过基于真实网络拓扑的实验仿真对上述分析结果进行补充.

2.1 溯源效果评估模型

溯源效果评估模型的相关参数和比较结果见表 1 和表 2,具体评价指标如下.

- 追踪痕迹建立开销

追踪痕迹记录数量(number of logging trails,简称 NLT):是指溯源路由器在单位时间内存储追踪痕迹数量.

追踪痕迹生成速率(trail generation ratio,简称 TGR):是指溯源路由器在单位时间内生成追踪痕迹的速率.

- 攻击路径重构开销

溯源路由器查询数量(number of traceback routers,简称 NTR):是指完成溯源任务需要向多少个路由器取证.

- 溯源精度

溯源漏报率(false negative rate,简称 NR):是指由于追踪痕迹的缺失造成攻击路径某些节点被遗漏的概率.

溯源误报率(false positive rate,简称 PR):是指由于追踪痕迹的不准确造成某些无辜的路由器被误报的概率.

Table 1 The parameter description for the single-packet traceback evaluation model

表 1 单包溯源效果评估模型的参数说明

参数	含义	参数	含义
n	单位时间内到达溯源设备的 IP 包数量	$\|Z\|$	最大标签供应量
s	经过某溯源设备的所有路由路径数量	σ	攻击路径或攻击包所占比例
k	溯源路由器的接口数量	Ω	所有路由器承载溯源路径的数量
r	TNP 的 IP 包处理速率	N	路由器所承载的溯源路径数量
l	攻击路径长度	β	布鲁姆过滤器中哈希函数数量
c	当前网络的溯源设备总数	t	记录追踪痕迹的时间
b	存储资源总量	v	经过某溯源设备且以受害者为目的地的路由数

Table 2 The result description for the single-packet traceback evaluation model

表 2 单包溯源效果评估模型的结果说明

比较方法	评价指标				
	NLT($s<<n$)	TGR	NTR	NR($b/(c\times N_{ROUTERmax})\leqslant b/\Omega$)	FR ($\beta/e^{\beta nt/o}<<\|Z\|/n$)
S3T	s+3%×n	$k\times r$	l–1	$[1-b/(c\times N_{ROUTERmax})]\times\sigma$	0
PSIT	s+3%×n	r	l–1	$(1-b/\Omega)\times\sigma$	$(1-\|Z\|/v)\times\sigma$
SPIE	n	r	5×l	0	$(1-\beta/e^{\beta nt/o})\times\sigma$
HIT	1/2×n	$k\times r$	5/2×l	0	$(1-\beta/e^{\beta nt/o})\times\sigma$
WHIT	1/3×n	r	5/3×l	0	$(1-\beta/e^{\beta nt/o})\times\sigma\times(2/3)$

2.1.1 追踪痕迹记录数量

S3T 方法需要溯源路由器记录两种追踪痕迹:普通包和变形包.首先分析普通包的存储开销.假设 n 表示单位时间内到达溯源路由器 R_i 的数据包数量,D 表示单位时间内到达 R_i 且目的地址不相同的数据流数量,B 表示单位时间内到达 R_i 的同宿不同源的 TEC 数量.基于此,单位时间内到达的 TEC 数据量 $M=D\times B$,这意味着单位时间内经过 R_i 路由路径数量 $s=M$.根据 TEC 与三元组唯一绑定原则,可知单位时间内 R_i 分配的标签总数量 s.根据 S3T 的追踪痕迹建立原理,$NLT_{S3T}=s$.其次,分析变形包的存储开销.假设α表示在 R_i 上数据包发生网络协议变形的概率.已有研究[18]表明,路由器中 IP 包发生变形的概率为 3%,即α=3%.因此,$NLT_{S3T}=n\times 3\%$,进一步可推出 $NLT_{S3T}=s+n\times 3\%$.PSIT 和 S3T 都采用基于路由的追踪痕迹建立方法,因此,$NLT_{PSIT}=NLT_{S3T}$;SPIE 方法要求 R_i 记录每个到达包,因此,$NLT_{SPIE}=n$.HIT 采用隔跳记录方法,NLT 大约是 SPIE 的 1/2,即 $NLT_{HIT}=1/2\times n$;WHIT 采用隔两跳记录方法,NLT 大约是 SPIE 的 1/3,即 $NLT_{WHIT}=1/3\times n$.Paxson 等人[24]在对互联网中路由路径存活时间进行统计之后发现:绝大部分的路由路径会至少持续 1 个小时以上.因此,不难推断出 $s<<n$,进而可得($NLT_{S3T}=s+n\times 3\%\approx n\times 3\%$)$<NLT_{WHIT}<NLT_{HIT}<NLT_{SPIE}$.

利用以上结论,我们可推断出即使在流量异常情况下,本文方法也比其他方法更具性能优势.例如:在面对 DDOS 攻击时,本文方法不会因源地址异常而产生较大的存储开销.因为一旦路径建立成功,无论源地址是什么,溯源路由器都不再执行记录操作,所以本方法依然可以正常工作.在面对扫描攻击时,考虑到宿地址异常会产生较多的 TEC,从而使得溯源路由器记录大量路径信息,然而即使是这样,与已有的基于包摘要或基于路由器标记的单包溯源方法相比,本方法的存储开销依然较少.

2.1.2 追踪痕迹生成速率

假设溯源路由器 R_i 有 k 个接口,那么 S3T 和 HIT 方法会在 R_i 周围放置 k 个 TNP,而且到达 R_i 的数据包会被并行处理,从而生成追踪痕迹.假设所有 TNP 的包处理速率都等于 r,那么 R_i 的追踪痕迹生成速率就能够达到 $TGR_{S3T}=TGR_{HIT}=k\times r$.然而,在 SPIE、WHIT、PSIT 方法中,所有到达 R_i 的数据包只能被串行处理,假设 R 的包处理速率也等于 r,那么 $TGR_{SPIE}=TGR_{WHIT}=TGR_{PSIT}=r$.Signaos 等人[25]通过大规模真实拓扑统计,得出当前互联网中路由器的平均度大约是 6.34,即 $k\approx 6$.因此,与 PSIT、WHIT 和 SPIE 相比,S3T 方法能够将 TGR 提升 6 倍.

2.1.3 查询路由器的数量

给定一条攻击路径(R_1,...,R_l),溯源路径重构过程就是从出口路由器 R_l 开始,逆向迭代查询到入口路由器 R_1.在 S3T 和 PSIT 中,每一轮取证请求都可以精确地定位上游路由器.因此,溯源路由器只需发起(l–1)轮溯源请求

(除了入口路由器 R_1)即可,进而可得 $NTR_{S3T}=NTR_{PSIT}=l-1$.在 SPIE 方法中,除了查询攻击路径上的路由器以外,还需要查询它们的邻居路由器.假设路由器的平均度为 m,那么每一轮取证请求都需要查询$(m-1)$个路由器.因此,$NTR_{SPIE}=l\times(m-1)$.HIT 方法要求溯源管理器发送 $l/2$ 轮溯源请求,每轮查询$(m-1)$个路由器,因此,$NTR_{HIT}=1/2\times l\times(m-1)$.WHIT 则需要发送 $l/3$ 轮溯源请求,每轮查询$(m-1)$个路由器,因此,$NTR_{WHIT}=1/3\times l\times(m-1)$.

根据上述结论,不难推断出本文方法不会消耗太多带宽资源,原因是:在追踪痕迹建立阶段,S3T 采用追踪痕迹内嵌方式来建立路径片段,无需额外增加数据流,因此不会消耗带宽资源;在攻击路径重构阶段,S3T 也只需发送十几个溯源请求,不会占用太多带宽资源.

当$m\geqslant(4-3/l)$时,就有$NTR_{S3T}<NTR_{SPIE}<NTR_{HIT}<NTR_{WHIT}$.因此只要攻击路径上路由器平均度超过 3,S3T 方法就优于传统方法.为此,本文对由 CAIDA 组织采集的 19 438 个自治域进行了面向平均度的分析,结果如图 8 所示.虽然平均度超过 3 的自治域数量只占全体自治域的 17%,但是它们绝大部分都是核心域,而且其平均度大多高达 200 左右.这也就是说,如果该条路径属于域内攻击,那么 S3T 的优势可能不明显;而一旦属于跨域攻击,那么 S3T 将拥有巨大优势.

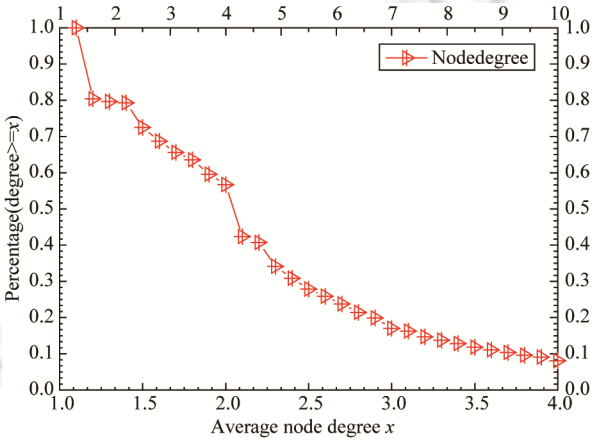


Fig.8 The complementary cumulative distribution function of average node degree

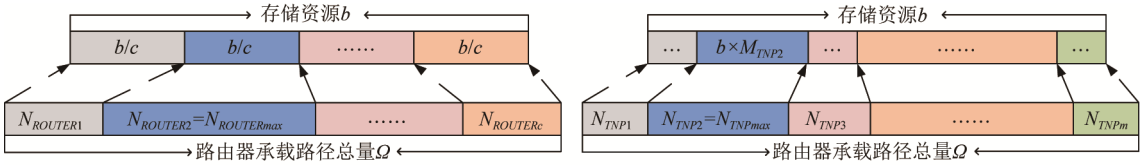
图 8 自治域的平均节点度补充累积分布函数

2.1.4 溯源漏报率

假设溯源网络中路由器数量为 c,ISP 能够提供的存储资源总量为 b.N_{TNPi} 表示 TNP_i 所承载的溯源路径的数量,其中攻击路径所占比例为 σ,M_{TNPi} 表示 N_{TNPi} 占所有路由器承载路径全集 Ω 的比例;$N_{ROUTERi}$ 表示路由器 $ROUTER_i$ 所承载的溯源路径的数量.考虑到追踪痕迹缺失是由溯源设备存储资源不足造成的,本文只分析承载溯源路径数量最多的设备 $TNP_{\max}$ 和 $ROUTER_{\max}$.在 S3T 中,$TNP_{\max}$ 的存储容量 S_{S3T} 依据 $M_{TNP\max}$ 来计算$(S_{S3T}=b\times M_{TNP\max})$,因此,$NR_{S3T}=(1-S_{S3T}/N_{TNP\max})\times\sigma$.PSIT 方法采用平均法来分配存储资源$(S_{PSIT}=b/c)$,$NR_{PSIT}=(1-S_{PSIT}/N_{ROUTERi})\times\sigma$.由定理 1 可知,$S_{S3T}/N_{TNPma}\geqslant S_{PSIT}/N_{ROUTERi}$,进而证明 $NR_{S3T}\leqslant NR_{PSIT}$.此外,SPIE、HIT 和 WHIT 方法都使用布鲁姆过滤器来压缩存储追踪痕迹.依据该数据结构的特点,这些方法只会产生误报率,而不会因存储资源不足产生漏报率,因此,$NR_{SPIE}=NR_{HIT}=NR_{WHIT}=0$.

定理 1. 给定存储总量 b,路由器数量 c,TNP 数量 m,TNP 承载路径总量 Ω.$N_{TNP\max}$ 和 $N_{ROUTER\max}$ 分别表示 $TNP_{\max}$ 和 $ROUTER_{\max}$ 所承载的溯源路径数量.已知 $c\leqslant m$,$M_{TNP\max}=b\times N_{TNP\max}/\Omega$,可推出 $S_{S3T}/N_{TNP\max}\geqslant S_{PSIT}/N_{ROUTERi}$,其中,$S_{S3T}=b\times M_{TNP\max}$,$S_{PSIT}=b/c$.

证明:PSIT 方法的存储资源分配方式如图 9(a)所示,$S_{PSIT}/N_{ROUTER\max}=b/(c\times N_{ROUTER\max})$;S3T 方法的存储资源分配方式如图 9(b)所示,$S_{S3T}/N_{TNP\max}=b/\Omega$.因为 $N_{ROUTER1}+\ldots+N_{ROUTERc}=\Omega$,且$\forall i\in[1,c]$,$N_{ROUTER\max}\geqslant N_{ROUTERi}$,所以 $c\times N_{ROUTER\max}\geqslant\Omega$,进而可推出 $S_{S3T}/N_{TNP\max}\geqslant S_{PSIT}/N_{ROUTER\max}$.



(a) PSIT 的存储资源分配方式 (b) S3T 的存储资源分配方式

Fig.9 Storage resource allocation examples in different single packet IP traceback approaches

图 9 不同方法的存储资源分配示例图

2.1.5 溯源误报率

在基于路径标记的单包溯源方法中,溯源误报率是由于标签空间不足造成的.如果溯源设备中以受害者为目的地址的路由路径数量超过了标签空间最大供应量|*Z*|=262144,那么,该设备不得不破坏标签的唯一标识性(同一标签被多条路径共享),致使追踪痕迹不准确.假设经过某路由器 *R* 且以受害者为目的地的路由路径数量为 $v(v\geqslant|Z|)$,其中,攻击路径所占比例为σ,那么 $PR^R_{PSIT}=(1-|Z|/v)\times\sigma$.与 PSIT 方法不同,在理想情况下,S3T 方法通过预测能够将所有标签都分配给攻击路径,也就是说,能够以 0 误报率重构出 262 144 条攻击路径.如果攻击路径数量大于 262 144,那么 S3T 也会产生误报,但是如此大规模的 DDoS(distributed denial-of-service)攻击并不常见.而且,如果 IDS 及时发现攻击,溯源任务就能够在标签被重复分配之前完成,避免出现溯源误报率.综上所述,任给 TNP_i,$PR_{S3T}\approx0$.在 SPIE、HIT 和 WHIT 方法中,误报率的产生是追踪痕迹压缩造成的.假设 *R* 中布鲁姆过滤器的存储容量为 *o* 和哈希函数个数为 *v*.根据布鲁姆过滤器原理,*R* 的误报率 $f=(1-e^{-nvt/o})^v$,其中,*t* 代表持续记录时间.随着 *t* 的增大,$e^{-nvt/o}$ 会逐渐趋近于 0.利用泰勒公式展开,$f\approx1-v/e^{nvt/o}$.如果攻击包所占比例也为σ,根据文献[13,17,19]可知,$PR^R_{SPIE}=PR^R_{HIT}\approx(1-v/e^{nvt/o})\times\sigma=(3/2)\times PR^R_{WHIT}$.

2.2 仿真实验

仿真实验的目的是补充第 2.1 节的分析结果,特别是相较于已有方法,有明显提高的性能指标:追踪痕迹建立开销和溯源精度.

2.2.1 实验设置

本文使用网络仿真框架 OMNET++[26]、IP 网络仿真工具箱 INET 和 DoS 攻击仿真工具 ReaSE[27]来模拟攻击场景.表 3 显示了仿真实验的网络拓扑数据、运行环境、控制参数、性能指标和对比方法.

Table 3 Experiment environment, topologies, control parameters, performance metrics and compared schemes

表 3 仿真实验中网络拓扑数据、运行环境、控制参数、性能指标和比较方法说明

运行环境	服务器	Intel 2.40GHz dual-core CPU,2GB 和 Windows XP
网络拓扑数据	CAIDA	路由器 1162 和链路 5493
控制参数	攻击者的投入数量	$N_{attacker}$
	攻击持续的时间	A_{time}
	存储资源的总量	S_{tot}
	溯源路径的长度	L_{path}
性能指标	追踪痕迹生成速率	*TGR*
	溯源精度	*TP*
比较的单包溯源方法	基于路径标记的单包溯源方法	PSIT
	基于包记录的单包溯源方法	SPIE
	基于路由器标记的单包溯源方法	HIT, WHIT

在攻击场景中,每个路由器都将直连一台主机,同时指定其中一台主机作为受害者,而攻击者则随机分布在其他主机中.除了与受害者通信,攻击者与正常用户以及正常用户之间也可以随机发送消息.而且在传播过程中,IP 包不会发生分片和变形操作;将攻击者的 IP 包发送速率 A_{rat} 设置为 1 Kpps,而正常主机的发送速率则符合正态分布 *N*(20 pps,30 pps).为了简化实验步骤,每个 TNP 的包处理速率相同,而且存储资源总量 S_{tot} 以 1 161 为基数(S3T 方法的存储开销依赖于路由路径数量,在该攻击场景中,每个目的地址最多对应 1 161 条路由路径),存储单位则是基于路径标记的溯源方法(PSIT、S3T)中每个追踪痕迹的大小ξ_1=48 bit;在基于布鲁姆过滤器的溯源

方法中(SPIE、HIT、WHIT),哈希函数的数量β被设置为 16,因此,其追踪痕迹大小$\xi_2=\xi_1/3=16$bit.此外,本文采用入口路由器记录转发包的方式来实现 HIT 和 WHIT 方法.

2.2.2 追踪痕迹记录概率(logging probability,简称 LP)

为了更有效地衡量追踪痕迹记录数量,本文提出记录比例的概念——路由器记录追踪痕迹的数量与整个网络追踪痕迹平均数量的比值.并以此为基础,设计了两组实验,其中,第 1 组用来说明随着运行时间的推移,不同方法记录比例的变化情况,第 2 组用来探讨 S3T 中记录比例在核心路由器与边缘路由器的变化情况.

第 1 组实验通过搜集不同时间段内路由器转发 IP 包的数量和记录追踪痕迹的数量,计算出各自的记录比例,结果如图 10 所示.与基于包记录的单包溯源方法(SPIE、HIT 和 WHIT 方法)相比,S3T 和 PSIT 方法的记录比例从最少的 37%(WHIT 方法)左右降到了 5%,下降幅度达到了 7 倍,而且在实验中,随着模拟时间的逐渐增大,记录概率依然在减少,甚至降低为 2%.在实验初始阶段,S3T 的记录概率要高于其他方法,原因是整个网络的攻击路径还未完全建立.一旦路径建立,S3T 的记录概率就会一直降低,这也证实了第 2.1.1 节中的分析结果.

第 2 组实验利用所有路由器的记录比例,统计出相关补充累积分布函数,结果如图 11 所示.边缘路由器的记录比例要低于核心路由器,这是因为,经过边缘路由器的路由路径要低于核心路由器.而且在 S3T 方法中,边缘路由器还可能是某条攻击路径的入口路由器,而入口路由器不需要执行记录操作.

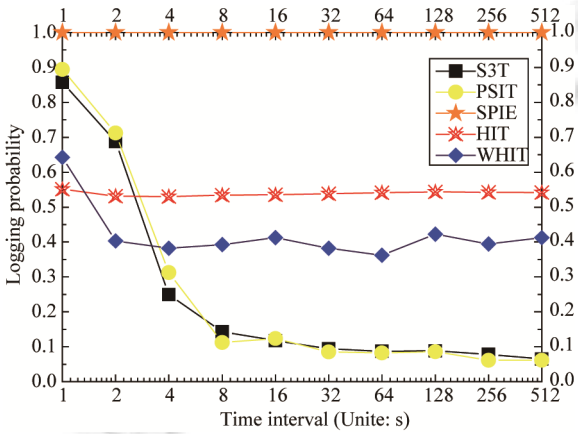


Fig.10 Comparison between S3T and others for logging probability by increasing the attack time interval

图 10 比较不同方法中记录概率随攻击时间的变化情况

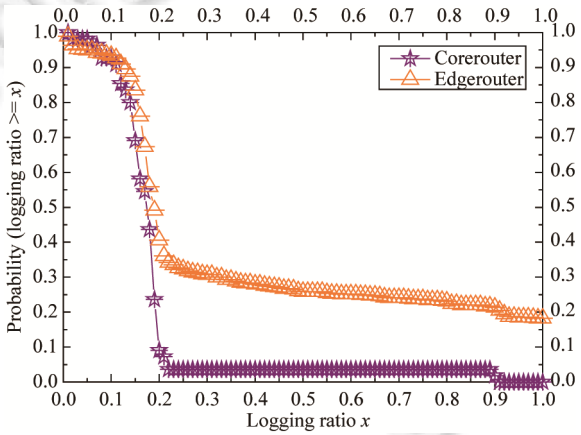


Fig.11 The complementary cumulative distribution function of the logging ratio in S3T

图 11 S3T 方法的记录比例补充累计分布函数

2.2.3 追踪痕迹生成速率(trail generation ratio,简称 TGR)

在溯源设备中,其处理开销与追踪痕迹生成速率成反比.处理开销大,就意味着生成速率低;反之亦然.因此,本文使用追踪痕迹生成速率来进行该指标的验证.本小节设计两组与 TGR 相关的实验:第 1 组用来探索在引入 TNP 后整个溯源网络 TGR 的提升幅度;第 2 组用来说明 S3T 方法可以有效地降低溯源操作对网络延时的影响.

第 1 组实验以 TNP 为计算单位来统计溯源网络中路由器的追踪痕迹生成速率分布情况,进而获得其互补累积分布函数,结果如图 12 所示.与 SPIE、PSIT 方法相比,基于并行处理的单包溯源方法(S3T、HIT、WHIT)将整个网络的 TGR 平均提升了 1 倍,而且如果溯源网络的节点平均度能再升高,那么 TGR 还会进一步提高.此外,繁重的负载已经使得核心路由器成为了溯源网络的转发瓶颈.然而,S3T、HIT 和 WHIT 方法却能够利用核心路由器的邻接度普遍比较大的特点,通过在其周围配置更多的 TNP 来解决该问题.

第 2 组实验通过搜集每个溯源设备单位时间 A_{time}=60s 内 IP 包到达的数量来统计出累积分布函数,结果如图 13 所示.在 S3T 和 HIT 方法中,只有 85%的溯源设备有 IP 包到达,而且溯源设备的最大 IP 包到达数也不超过 $pow(3,4)$,低于 WHIT、SPIE 和 PSIT 方法.因此,在溯源设备的包处理速率都相同的前提下,S3T 和 HIT 方法带来的包转发时延也要远低于这 3 种方法,这就使得前者更适合在高速溯源网络进行部署.

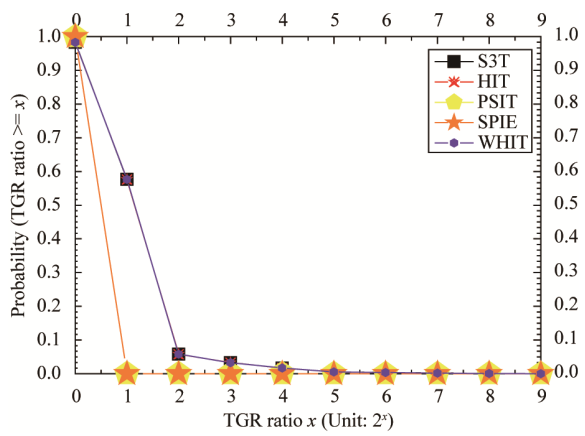


Fig.12 The complementary cumulative distribution function of TGR

图 12 溯源网络中 TGR 的互补累积分布函数

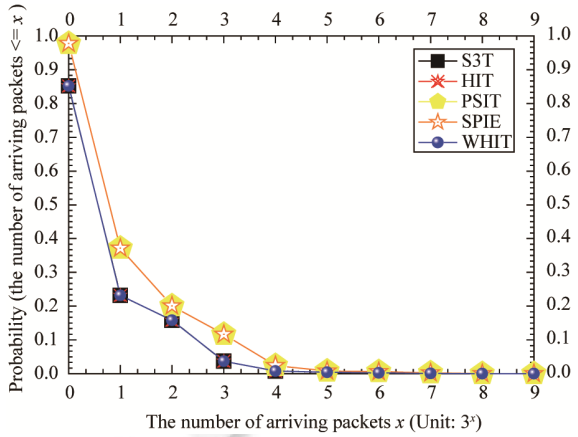


Fig.13 The complementary cumulative distribution function of arriving IP packet number

图 13 溯源网络中各设备 IP 包到达数的累积分布函数

2.2.4 溯源精度(traceback accuracy,简称 TA)

鉴于溯源精度是误报率和漏报率共同作用的结果,第 2.1.4 节和第 2.1.5 节已经给出影响这两个指标的相关因素,并且进行了量化评估,而本小节则从整体出发直接研究溯源精度与这些因素的关系.

第 1 组实验通过计算路由器的平均误报率和漏报率来说明 TA 与攻击者投入数量($N_{attacker}$)之间的关系,其中,A_{time}=60s,S_{tot}=*pow*(1161,2),比较结果如图 14 所示.从整体上看,随着 $N_{attacker}$ 的增多,所有方法的溯源精度都呈递减趋势,但是,基于路径标记的方法明显要高于其他方法,当攻击比例达到 80%时,SPIE、HIT 和 WHIT 方法的溯源精度都会降为 0,因为攻击流速率远大于正常发包量.此外,随着攻击规模的扩大,相比于 PSIT,S3T 方法最终能将溯源精度提升 20%.

第 2 组实验说明 TA 与攻击的持续时间(A_{time})之间的关系,其中,$N_{attacker}$=1161,S_{tot}=*pow*(1161,2.3),结果如图 15 所示.随着 A_{time} 的增大,TA_{S3T} 和 TA_{PSIT} 不会有明显变化,而其他溯源方法都会明显下降,并且下降速度与 A_{time} 的增长速率几乎成正比,原因与第 2.1.1 节分析相同.

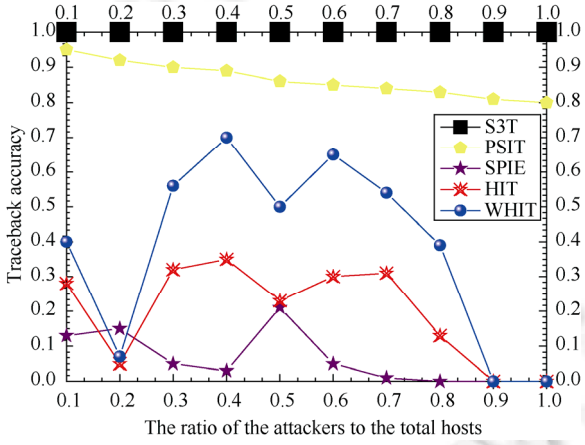


Fig.14 The traceback accuracy by increasing the number of attackers

图 14 不同攻击规模下溯源精度的变化情况

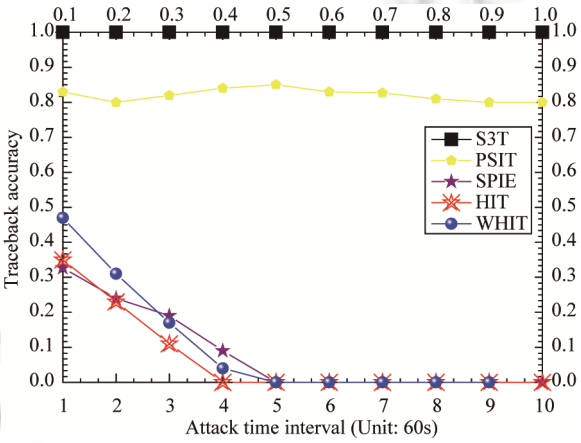


Fig.15 The traceback accuracy by increasing the attack time interval

图 15 不同攻击持续时间下溯源精度的变化情况

第 3 组实验说明 TA 与存储资源总量(S_{tot})之间的关系,其中,$N_{attacker}$=1161,A_{time}=60s,结果如图 16 所示.随着 S_{tot} 的增大,所有方法的溯源精度都在升高,其中,TA_{S3T} 一直保持在 100%,TP_{PSIT} 在 S_{tot}=*pow*(1161,2.1)时也快速提升,只有 SPIE、HIT 和 WHIT 方法在 S_{tot}=*pow*(1161,2.4)之后溯源精度才升到 100%.因此,在存储资源总量一定

的前提下,S3T 方法在溯源精度方面具有明显优势.

第 4 组实验说明 TA 与溯源路径长度(L_{path})之间的关系,其中,$N_{attacker}$=1161,S_{tot}=pow(1161,2.3),A_{time}=60s,结果如图 17 所示,随着 L_{path} 的增大,只有 TA_{S3T} 几乎没有变化,其他方法的精度都在降低,特别是当攻击路径长度增长到 8 时,TA_{PSIT} 降低了将近 20%,而 SPIE、HIT、WHIT 方法几乎降到 0.原因在于攻击路径越长,意味着溯源过程中查询的路由器数量也就越多,这增加了漏报率和误报率的概率.

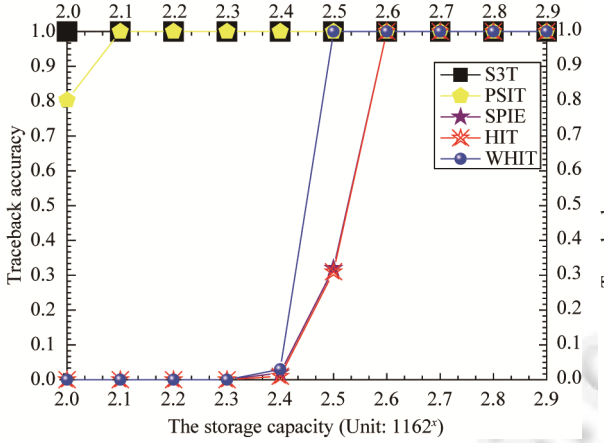


Fig.16 The traceback accuracy by increasing the length of attack path

图 16 不同路径长度下溯源精度的变化情况

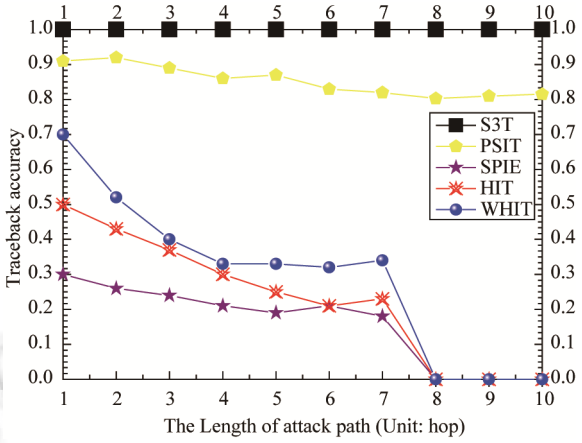


Fig.17 The traceback accuracy by increasing the storage capacity

图 17 不同存储容量下溯源精度的变化情况

3 相关工作介绍

迄今为止,已有数种 IP 溯源方法被提出.然而它们绝大部分都是针对高速 DoS 攻击的,例如确定性包标记溯源方法[5]、基于熵演变的溯源方法[6]和基于 ICMP 消息传递的溯源方法[4]等,而对具备多重攻击向量特征 MDoS 攻击的单包溯源研究得较少.根据追踪痕迹建立方式的不同,可将已有的单包溯源方法划分为 5 类,它们的性能对比情况见表 4.

Table 4 The comparation between the existing single packet approaches

表 4 单包溯源方法对比情况

单包溯源方法分类	评估指标					
	存储开销	计算开销	重构时间	溯源精度	增量部署	变形包追踪
基于包特征提取的单包溯源方法	极大	较大	较长	低	否	否
基于包摘要的单包溯源方法	大	大	长	低	否	**支持**
基于路由器标记的单包溯源方法	较大	**小**	较长	低	**支持**	**支持**
基于接口标记的单包溯源方法	**极小**	大	**短**	**高**	否	否
基于路径标记的单包溯源方法	**小**	较大	**短**	较低	**支持**	**支持**

(1) 基于包特征提取的单包溯源方法[8],其核心是数据包特征提取方法,基本原理是:利用 IP 包传送过程中链路信息无法伪造的特点,溯源路由器通过直接提取和记录数据帧的 MAC 地址和 IP 包头的若干固定字段(包括版本、源地址和目的地址等)和部分数据作为追踪痕迹.在溯源过程中,一方面通过检查路由器所记录的包头信息来取证,另一方面通过 MAC 信息来确定下一跳的搜查节点.虽然该方法实现了自动化溯源,但仍存在以下不足:① 包特征信息可达 60 字节,这对于存储资源本就缺乏的路由器来说是难以容忍的;② 溯源精度低,会频繁重构出错误的攻击路径,致使正常主机被误报,而攻击主机却被漏报;③ 溯源处理开销大,极大地增加了路由设备的额外负担,致使网络传输性能下降;④ 容易泄漏数据,威胁用户隐私.

(2) 基于包摘要的单包溯源方法[7,9,10],其核心是数据压缩算法,基本原理是:通过选取 IP 包头中冲突概率只有 0.00092%的固定字段作为包特征的计算输入参数,同时使用空间利用率较高的布鲁姆过滤器来压

缩和存储数据包摘要,最后采用半洪泛方式在路径回溯时发送溯源请求,逐跳查询摘要信息,确定攻击路径.虽然该方法在一定程度上减小了存储开销(大约是包转发量的 0.5%)并克服了数据泄漏,但却存在以下不足:① 对溯源精度缺乏考虑;② 从网络全局看,溯源存储开销依然很大(在 OC-192 链路上,一个 32 口路由器,每秒转发量可达 40GB);③ 溯源处理开销依然较大;④ 路径重构需要发送大量请求信息,致使本就脆弱的受害网络进一步被恶化.

(3) 基于路由器标记的单包溯源方法[11,12],其核心是路由器重标识算法、标记空间编码策略和隔跳路径重构算法.为了降低路由器存储开销,首先将路由器 ID 分配问题抽象建模为图着色问题,并用相关算法建立路由器 ID,代替 IP 地址;然后将部分溯源路由器 ID 直接写入到目前使用较少的 IP 包头字段,代替包记录;最后将路由器 ID 作为追踪痕迹验证参数,实现隔跳匹配.与方法(2)相比,该方法具备以下优势:将溯源存储开销减少到 IP 包转发量的 1/3,并将路径重构时间缩短到比较方法的一半,为攻击流阻断操作争得响应时间,减少了受害者的损失.但是,面对日益增长的攻击带宽,该方法的存储开销、溯源处理开销和溯源精度等问题依然比较严重.

(4) 基于接口标记的单包溯源方法[13],其核心思想是利用路由器接口固定且数量有限的特点,使用接口号取模操作建立追踪痕迹;路径回溯时,通过反向取模进行网络取证和节点串联.虽然该方法只需要 320KB 的存储资源,且溯源精度可达 100%,但却存在两个不合理的假设:① 只有全网部署,该溯源系统才能正常运行.然而溯源体系结构本应该是一种渐进的、增量的部署,即使部分部署时仍可以获得不同程度的攻击路径还原效果;② 在该溯源网络系统中,每个路由器接口只能连接一个网络设备.然而在 OSPF 协议中多路访问是一种最常见的路由器接口配置类型.在该 OSPF 网络中,每个接口通过交换机可以连接多个路由器.此外,该方法不具备追溯变形包的能力,致使攻击者利用隧道或 NAT 协议,可以将自己隐匿在变形路由器之后.

(5) 基于路径标记的单包溯源方法[14],这是我们早期的研究工作,其核心思想是利用路由路径不可伪造的特点,在溯源路由器上建立一条与路由路径方向相反的溯源路径作为追踪痕迹;在路径回溯中,受害者只需通过标签连接操作还原出整条溯源路径.与上述方法相比,该方法因存储开销小、路径重构时间短、可增量部署以及易于实现等优势而渐受关注.但是,它的集中式发布标签策略依然会带来较大的溯源处理开销,而平均分配存储和无差别回收标签策略则会分别带来严重的溯源漏报率和误报率,进而影响溯源精度.

与这些工作相比,本文的特色在于在降低溯源开销的同时提高了溯源精度.单包溯源方法只有将溯源开销和溯源精度同时考虑在内,才可能被广泛接受和部署,对于 ISP 来说,它希望溯源系统对网络传输性能的影响要尽可能地小,不会妨碍其他业务的正常运营;对于用户来说,它则希望溯源服务质量要尽可能地高,以保证物超所值.此外,本文给出影响溯源开销和精度的客观因素,如果 ISP 在部署溯源系统之时,能够依据网络环境及早提取相关因素,并利用它们合理配置资源,那么溯源效果可以进一步得到提升.

4 结论及未来工作展望

为了克服已有单包溯源方法在应对 MDoS 攻击时存在的处理开销大、溯源精度低等问题,本文提出了一种基于标签交换的单包溯源方法,即 S3T.该方法的基本思想是利用路由路径不能伪造的特点,借鉴多协议标签交换网络的交换路径生成原理,在溯源路由器转发 IP 包的同时建立面向反向路由的追踪痕迹,降低单位痕迹大小.以此为基础,通过并行化建立追踪痕迹、灵活配置溯源路由器存储容量和自适应调整追踪痕迹存储时间等手段提高溯源路由器的包处理速率和资源使用效率.S3T 具有以下显著特征:(1) 建立的基于标签交换的追踪痕迹极大地降低了系统对存储资源的需求;(2) 采用的追踪痕迹并行化建立策略有效地减低了溯源对网络性能的影响;(3) 根据溯源路由器的负载情况,对存储资源的灵活分配提高了资源使用率,进而降低了溯源漏报率;(4) 移动平均线理论用于追踪痕迹重要度评估,不仅能够及时地释放正常痕迹,而且准确地保留攻击痕迹,提高了资源回报率,降低了溯源误报率.S3T 的高效性已经利用理论分析和实验仿真得到了验证.结果显示,S3T 不仅能够降低溯源存储和处理开销,而且在提升溯源精度方面也具有优秀表现.溯源开销的减少有助于提高系统的可扩展

性,而溯源精度的增加有助于提高系统的服务能力.此外,本文方法涵盖的主要操作都比较简单,不涉及过于复杂的运算,对网络性能的影响都不会太明显.例如,溯源标记信息的提取和写入都嵌入到路由器的解包和封包基本过程中,速率非常快;标签分配采用资源池技术,计算复杂度降低为 $O(1)$;标记查找如果采用基于内容寻址的相联存储器来实现,则其查找复杂度也可降低为 $O(1)$,因次本方法在工程操作方面也是可行的.

到目前为止,我们还没有能力在实际网络中对提出的 S3T 方法进行部署和应用,以确认其在仿真环境之外的评估性能.尤其是溯源系统是基于互联网的分布式系统,由于宏大的部署规模、网络的不稳定、攻击行为的不可预测等因素,仿真环境必然会与实际环境存在偏差.另外,提出的方法目前只支持静态增量部署而且容错性能较差,缺少一种增强可操作性的机制,以实现动态增量部署并提高系统健壮性.因此,我们希望在今后,以本文研究为基础构建一个真实网络环境下的实验平台,以增加实验结果的准确性.其目标是在不久的将来为实际环境中的部署和商业应用提供参考和借鉴,以便为网络用户提供可靠的反匿名机制.此外,为了实现追踪粒度多样化和网络拓扑隐私性,如何改进 S3T 方法,使其同时适用于域内、域间网络追踪,具有很强的研究意义.

References:

[1] 2013 Global Application & Network Security Report. The Radware's Emergency Response Team, 2014. http://www.datainter.cz/doc/radware/3_radware_security_report.pdf

[2] Li J, Wu JP, Xu K, Chen WL. An hierarchical inter-domain authenticated source address validation solution. Chinese Journal of Computers, 2012,35(1):85−100 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2012.00085]

[3] 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]

[4] Saurabh S, Sairam AS. ICMP based IP traceback with negligible overhead for highly distributed reflector attack using Bloom filters. Computer Communications, 2014,42(2):60–69. [doi: 10.1016/j.comcom.2014.01.003]

[5] Foroushani VA, Zincir HA. Deterministic and authenticated flow marking for IP traceback. In: Proc. of the 27th Int'l Conf. on Advanced Information Networking and Applications. Barcelona: IEEE, 2013. 397–404. [doi: 10.1109/AINA.2013.60]

[6] Yu S, Zhou WL. Traceback of DDoS attacks using entropy variations. IEEE Trans. on Parallel and Distributed Systems, 2011,23(3):412–425. [doi: 10.1109/TPDS.2010.97]

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

[8] Matsuda S, Baba T, Hayakawa A, Nakamura T. Design and implementation of unauthorized access tracing system. In: Proc. of the Applications and the Internet. Nara: IEEE, 2002. 74–81. [doi: 10.1109/SAINT.2002.994453]

[9] 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]

[10] Jeong E, Lee BK. An IP traceback protocol using a compressed hash table, a sinkhole router and data mining based network forensics against network attacks. Future Generation Computer Systems, 2014,33:42–52. [doi: 10.1016/j.future.2013.10.023]

[11] 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]

[12] Wang YL, Ren J. WHIT: A more efficient hybrid method for single-packet IP traceback using walsh matrix and router degree distribution. IEICE Trans. on Communications, 2013,96(7):1896–1907. [doi: 10.1587/transcom.E96.B.1896]

[13] 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]

[14] 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]

[15] Zhang YZ, Xiao J, Yun XC, Wang FY. DDoS attacks detection and control mechanisms. Ruan Jian Xue Bao/Journal of Software, 2012,23(8):2058−2072 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4237.htm [doi: 10.3724/SP.J.1001.2012.04237]

[16] 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]

[17] John W, Tafvelin S. Analysis of Internet backbone traffic and header anomalies observed. In: Proc. of the 7th SIGCOMM in Internet Measurement. San Diego: ACM, 2007. 111–116. [doi: 10.1145/1298306.1298321]

[18] Stocia I, Zhang H. Providing guaranteed services without peer flow management. In: Proc. of the SIGCOMM'99. Boston: ACM, 1999,29:81–94. [doi: 10.1145/316188.316208]

[19] Gont F. Security assessment of the internet protocol version 4. RFC 6274, 2011. http://www.rfc-editor.org/info/rfc6274

[20] Cooperative Association for Internet Data Analysis (CAIDA). Internet-Topology-Data-Kit. 2013. http://www.caida.org/data/internet-topology-data-kit/release-2013-07.xml

[21] Fu HY, Xie DZ. 2-Distance coloring of graphs. Journal of Southwest China Normal University (Natural Science Edition). 2009,34(3):17–20 (in Chinese with English abstract).

[22] Han LX, Wang YP. Novel genetical algorithm for the graph coloring problem. Journal of Xidian University, 2008,35(2):309–313 (in Chinese with English abstract). [doi: 10.3969/j.issn.1001-2400.2008.02.025]

[23] Tarkoma S, Rothenberg CE, Lagerspetz E. Theory and practice of Bloom filters for distributed systems. IEEE Communications Surveys & Tutorials, 2012,14(1):131–155. [doi: 10.1109/SURV.2011.031611.00024]

[24] Paxson V. Measurements and analysis of end-to-end Internet dynamics [Ph.D. Thesis]. Berkeley: University of California, 1997.

[25] Siganos G, Faloutsos M, Faloutsos P, Faloutsos C. Power laws and the as-level internet topology. IEEE Trans. on Networking, 2003,11(4):514–524. [doi: 10.1109/TNET.2003.815300]

[26] OpenSim. Omnetpp++: Objective Modular Network Testbed in C++. 2013. http://www.omnetpp.org/

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

附中文参考文献:

[2] 李杰,吴建平,徐恪,陈文龙.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. [doi: 10.3724/SP.J.1016.2012.00085]

[15] 张永铮,肖军,云晓春,王风宇.DDoS 攻击检测和控制方法.软件学报,2012,23(8):2058–2072. http://www.jos.org.cn/1000-9825/4237.htm [doi: 10.3724/SP.J.1001.2012.04237]

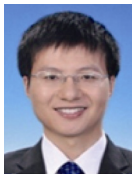
[16] 王尚广,孙其博,杨放春.IMS 网络中的 SIP 洪泛攻击检测.软件学报,2011,22(4):761–772. http://www.jos.org.cn/1000-9825/3818.htm [doi: 10.3724/SP.J.1001.2011.03818]

[21] 伏红勇,谢德政.图的 2-距离着色.西南师范大学学报,2009,34(3):17–20.

[22] 韩丽霞,王宇平.图着色问题的新遗传算法.西安电子科技大学学报,2008,35(2):309–313. [doi: 10.3969/j.issn.1001-2400.2008.02.025]

鲁宁(1984－),男,内蒙古包头人,博士,讲师,主要研究领域为网络安全.

史闻博(1980－),男,博士,副教授,博士生导师,CCF 专业会员,主要研究领域为网络服务与网络智能化,物联网应用技术.



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,CCF 杰出会员,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.