Software Engineering and Applications 软件工程与应用, 2017, 6(1), 1-7
Published Online February 2017 in Hans. http://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2017.61001

Hans汉斯

A Method of Information Tracing Based on ICMP

Ming Zhou, Sudan Li

Department of Computer, National University of Defense Technology, Changsha Hunan
Email: 345843427@qq.com

Received: Feb. 3rd, 2017; accepted: Feb. 21st, 2017; published: Feb. 27th, 2017

Abstract

In order to trace the DOS/DDOS attack source, people study and put forward some practical and feasible traceability methods; one of the most effective is the reverse retrospective program based on ICMP. However, when the attacker and the average user encounter the same path, in the choice of message to generate traceability information is not so accurate. In this paper, we will propose an improved ICMP information tracing method, which aims to improve the accuracy of retrospective attack path, and provide important basis for locating attack source, finding attacker and defending DOS/DDOS attack. The method is mainly to determine the module in the purpose of selecting the high frequency attack flow to enter the interface to generate traceback packets, so that the probability of selecting the attack message more tends to 1. Through the experimental analysis and demonstration, it is nearly 10% higher than the previous method in the generation of effective retrospective information, indicating that the retroactive method is more accurate and effective than before.

Keywords

ICMP, DOS/DDOS, Network Security, Information Traceability

一种基于ICMP信息追溯方法

周　明，郦苏丹

国防科学技术大学计算机学院，湖南 长沙
Email: 345843427@qq.com

收稿日期：2017年2月3日；录用日期：2017年2月21日；发布日期：2017年2月27日

摘　要

为了追溯DOS/DDOS的攻击源，人们研究并提出一些实用可行的追溯方法，其中最有效的当属基于ICMP

文章引用: 周明, 郦苏丹. 一种基于 ICMP 信息追溯方法[J]. 软件工程与应用, 2017, 6(1): 1-7.
https://doi.org/10.12677/sea.2017.61001

的反向追溯方案。但该方法在遇到攻击者和普通用户同一路径时，在选择报文生成追溯信息上就不是那么准确了。此论文中，我们将提出一种改进的ICMP信息追溯方法，目的在于提高追溯攻击路径的准确性，为定位攻击源，找到攻击者，防御DOS/DDOS攻击提供重要依据。其方法主要是在决定模块中有目的性的选择高频率攻击流进入的接口来生成追溯报文，从而使选中攻击报文的概率更加趋于1。通过实验分析论证，在生成有效追溯信息方面比之前的方法高出近十个百分点，表明了此追溯方法较之前是更准确有效的。

关键词

ICMP，DOS/DDOS，网络安全，信息追溯

1. 引言

近年来，我们最常接触的公共网络正遭受着各式各样的网络攻击，越来越多的人们关注到了网络设施的安全。拒绝服务攻击(DOS)和分布式拒绝服务攻击(DDOS)就是其中最具侵略性和破坏性的网络安全问题之一 [1]。

拒绝服务攻击目的在于妨碍和阻止真正需要资源的用户得到应有的服务和资源。这里可以是一种带宽，也可以是一个网络服务系统。它主要是向受害主机发送大量的无用数据流量占用用户所需的所有服务资源，从而中断这些网络或服务器提供的服务。当 DOS 攻击流来自不同的源头时，我们称之为分布式拒绝服务攻击(DDOS)。

在 DOS/DDOS 攻击中，IP 欺骗是一种很常见的恶意网络行为 [2]。DOS/DDOS 攻击随机的伪装 IP 头部的 32 位源地址，从而隐藏攻击源。IP 回溯追踪的目的就是找出真正的 IP 源地址 [3]。现在许多重大的服务都是依赖于互联网上的通信基础设施，一旦遭受 DOS/DDOS 攻击必将对其造成致命的危险。因此，如何预防 DOS/DDOS 的攻击或者将损失减到最小尤为重要。本文主要就针对 DOS/DDOS 攻击，基于 ICMP 扩展出一种更加有效的追溯方法。论文第一部分简要介绍了什么是 DOS/DDOS 功击；第二部分对几个重要的攻击追溯方法进行分析；第三部分提出本文改进方法的设计思想；第四部分重点对算法进行讲解；第五和第六部分是实验的验证结论和对以后研究的展望。

2. 研究背景

DOS/DDOS 攻击的防御主要分四大类 [4]：攻击预防、检测、攻击源标记和回击。攻击源标记的目的就是在包含伪装信息的 IP 数据包源地址域分析找出真正的攻击源头。为了追踪 IP 包的路径，人们通过在中间媒介路由处标记数据包实现攻击路径重构 [5]。中间媒介路由给一个或多个 IP 数据包生成 ICMP 回溯报文，并依托 IP 报文将这些 ICMP 信息报文发送到目的主机。受害主机利用接收到的 ICMP 回溯信息报文，对攻击路径进行重构，找到攻击源。

2.1. 攻击源识别

一旦入侵检测发现了一次攻击行为，最好的回击就是在攻击源阻止攻击流的继续入侵 [6]。很不幸的是，相比伪装 IP 源地址是那么简单易行，追溯攻击源就没有什么简便实用的方法了。为了冲破这些限制，

基于改良路由功能或修改当前协议的许多办法被人们所提出来，目的就是希望能支持 IP 的可追溯性。

2.2. IP 追溯

IP 追溯的设计思想是在路由器上以概率 P 对进入的数据包插入部分路径信息，目标主机通过这些路径信息重构出数据包的路径。当经过源地址和目的地址之间路由时，路由器以概率 P 插入它们的 IP 地址到进入的数据包中 [7]。通过这些路径信息，目标主机能重构出数据包的路径。然而，在当前的互联网 IP v4 协议中并未预留有供携带追溯信息的特殊字段。所以用编程的方法将路径信息压缩到像 IP 头部中可用的 16 位标示字段是很难实现的。

2.3. ICMP 信息回溯

介于 IP 追溯方法的不足，人们提出了 ICMP 信息回溯方法 [8]，在此方法中，当 IP 数据包经过一个路由器时，为避免增加额外的数据流，路由器以一个极低的大约 1/20000 的概率 P 生成一个 ICMP 追溯报文即 iTrace 数据包 [8]。路由器向目的地址和源地址都转发此 ICMP 数据包。在 DOS/DDOS 攻击中，目的节点可以运用这些信息追溯出攻击路径。另一方面，iTrace 数据包提供的信息可以很好的发现反射式拒绝服务攻击的攻击源，因为 iTrace 数据包以一定的概率同时也发往攻击源 IP 地址。路由生成 iTrace 数据包时，通常包含以下几项内容：发送它的路由 IP 地址，前一跳和后一跳 IP 地址，和诱发它的数据包信息。可以看出，我们不需要将路径信息编码到 IP 报头，而是将它存储在 ICMP 报文中，并发送到下一跳路由。下一跳路由接收到 iTrace 数据包时检查 IP 包和 iTrace 数据包是否具有相同的路径，并以此判断是否生成新的 iTrace 数据包或添加路径信息到源 IP 中。

还有一种被动生成 ICMP 追溯报文的方法 [9]，就是运用路由器中路由信息表和包推进表，分别在两个表中添加额外的标识位，以决定是否生成 iTrace 数据包。

2.4. 具有记忆路径的反向 ICMP 追溯

在原来的 ICMP 追溯方法中，因为生成 iTrace 数据包的概率不高，所以需要攻击数据包很多。再有靠近攻击者的路由器攻击率也不高，几乎不能够为真正需追踪的受害者提供高效的 iTrace 信息，而产生的 iTrace 信息也不大适合用于重构攻击路径。

在反向 ICMP 追溯方法中，我们主要是考虑提高那些能为受害者重构攻击路径提供更多有效信息的 iTrace 信息报文的生成机率。为此，改进了路由器中的路由信息表和包推进表。分别在两表项中添加了额外的标识位，用来标识是否真正需要为某个 IP 报文生成 iTrace 数据包和标明生成的 iTrace 数据包信息是否具有高效性。原理很简单，当路由信息表中增加的标识位为 1 时，我们认为需要生成 iTrace 数据包，相反为 0 则不需要。再检查包推进表中新增的标识位是否为 1，1 说明具有高效性，0 那就对我们没有太大利用价值。如 图 1 所示。

基于此，分离出两个不同的功能模块：决定模块和 iTrace 生成模块 [9]。在决定模块中，当入侵检测系统(IDS)告知 BGP 路由器时，BGP 路由会自动检测路由表中目的标识符，如果目的位为 1，表明确实需要生成相应的 iTrace 信息。接着路由表内容会传到包推进表中，通过有效的标识符，可以决定此时生成的 iTrace 信息是否具有利用价值。以标识位置 1 为例。值为 1 表明此处产生的 iTrace 信息具有高效性，那么这个 IP 包的一个拷贝就会被发送到 iTrace 信息生成模块。在生成模块中，实现了上述选定 IP 包相应的 iTrace 信息的生成任务，将路径信息添加到 ICMP 追溯报文中，并发往下一端，之后将此位清零。

3. 增强有效 ICMP 追溯信息的概率

具有追忆路径功能的方法确实能增加那些能为受害者重构攻击路径的提供充足信息的有效报文的机

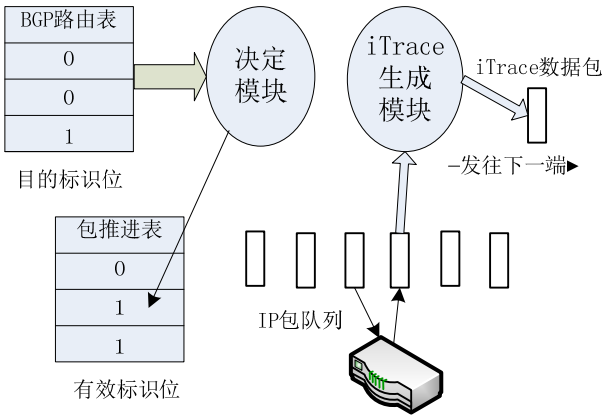

Figure 1. Schematic diagram of reverse tracing
图 1. 反向追溯示意图

率。然而，当普通用户和攻击者有着相同的路径时，想要区分不同的数据流，该方法就显得那么力不从心 [7]。因为普通用户一样在用着相同的路由表和推进表。所以在特定入口选择的 IP 报文所产生的 iTrace 数据包并不一定都是来自攻击源。这种时候用于重构攻击路径提供的数据信息就并不那么可靠。下面我们就提出一种靠近攻击者路由也能增加有效 iTrace 信息报文生成的方法。

此方法是基于记忆路径反向追踪方法而提出的。我们都知道，攻击者的攻击频率肯定是要比普通用户访问的频率高得多。通过提高有效信息的总量，让我们能够更高更准确的重构攻击路径。

假设 *Ai* 是恰巧在平等情况下到相同目的地的数据包。 *p* 为选择数据包生成 iTrace 报文的概率，那么

$$\sum_{i=0}^{K} P(Ai)=1 \text{或} P(\Phi)=0 \text{。}$$

假设 $P(A_k)$ 是选中攻击包生成 iTrace 信息报文的概率，那么

$$P(A_k)+\sum_{i=1}^{k-1} P(Ai)=1 \text{也就是} P(A_k)=1-\sum_{i=1}^{k-1} P(Ai) \text{。}$$

显然想要提高有效 iTrace 信息报文生成的概率，我们要做的就是减少选中普通正常数据包的概率，甚至将其概率尽量降为 0。也就是

$$P(Ai)=P(\Phi) \text{从而} P(A_k)=1-P(\Phi)=1 \text{。}$$

为了提高靠近攻击源的边界路由生成有效 iTrace 信息报文的概率，我们介绍一个算法，并对该算法进行实验分析。

4. 算法

在这部分中，我们重点对此算法思想进行讲解。图 2 是设计的算法。

算法先是根据目标位找出攻击进入接口，对进入流进行计数，检查所有攻击状态的信息是否接收，没有接收全，就通过计数器找到高频率进入的接口。这时关闭其他接口，在此期间选出攻击状态信息的报文生成追溯报文并发往下游路由。如果全部接收，就找到攻击接口同样也可以有效的选出攻击状态的信息报文。

算法的前提是假设攻击者比普通用户发送更多的数据包到目的主机，实际情况也是如此。我们只要找出此类数据流进入的接口，计算出该接口在特定时间内进入目的网络主机的数据包。计时器终止的时候，能很好的计算出进入数据包的进出频率。通常很少有网络主机是相距超过 30 跳的 [8]，计时时间根据

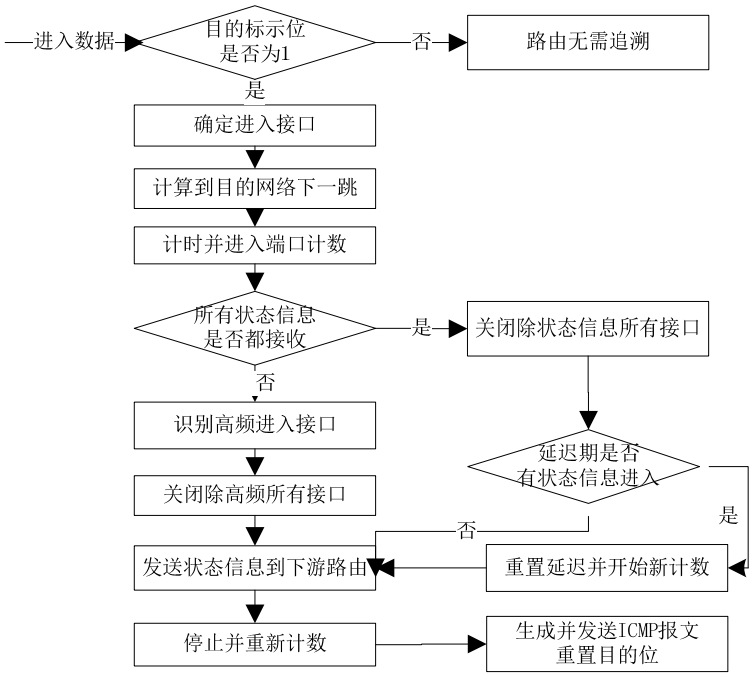

Figure 2. Algorithm flow chart
图 2. 算法流程图

路由下一跳数决定，具体时间计算公式是

$$T = \left(1/\text{下一跳数}\right) * 500\ \text{ms}\ 。$$

因此每一个在攻击路径上的路由都需要计算它到受害主机的下一跳数。例如我们有一个路由，它到受攻击者的平均下一跳数为 7，那么其计时时间为 72 ms，它的下一跳路由的下一跳数为 6，时间为 83 ms。两路由间时间的差异为我们下一步算法通过上游路由位置到下游路由做出决定提供必要依据。在算法中，我们增强了状态信息报文功能，通过报文中定义一个新的标签来识别状态信息 [10]。通信路由检测到一个流量攻击，刚经过攻击路径之间的第一个下游路由就给攻击流量标注为攻击的状态信息。有了状态信息，下游路由就能更好的决定下一步反馈信息。下一路由接到攻击状态信息，表明进入接口收到一个攻击流量，将路由表中目的标识位设为 1。

一旦路由器发现路由表中的目的标识位为 1，它就开始分类计时的为每个进入接口统计到受害者主机的推进包，在此期间，它还监听接收的状态信息。如果在此期间有任何的状态信息进来，它将停止并重新开始计数统计。计时终止后，路由器检查找出发送包到受害者频率最高的输入口并将其他的端口延迟 100 ms。如果端口在延迟期间接收到别的状态信息，它也将停止延迟并重置延迟时间。之后路由根据攻击流向下游路由发送状态信息。在此情况下，路由器延迟除状态报文接口的其他接口，选择推进包，复制并发送到生成模块，产生 iTrace 信息报文。生成模块发送 iTrace 信息报文后，重置路由表和包推进表中的目的位。

5. 实验分析

在这部分，我们在 CORE 上，通过模拟实验对比分析改进方法的可行性。图 3 是我们假设的网络拓扑图。

我们通过一组的模拟实验来测试：

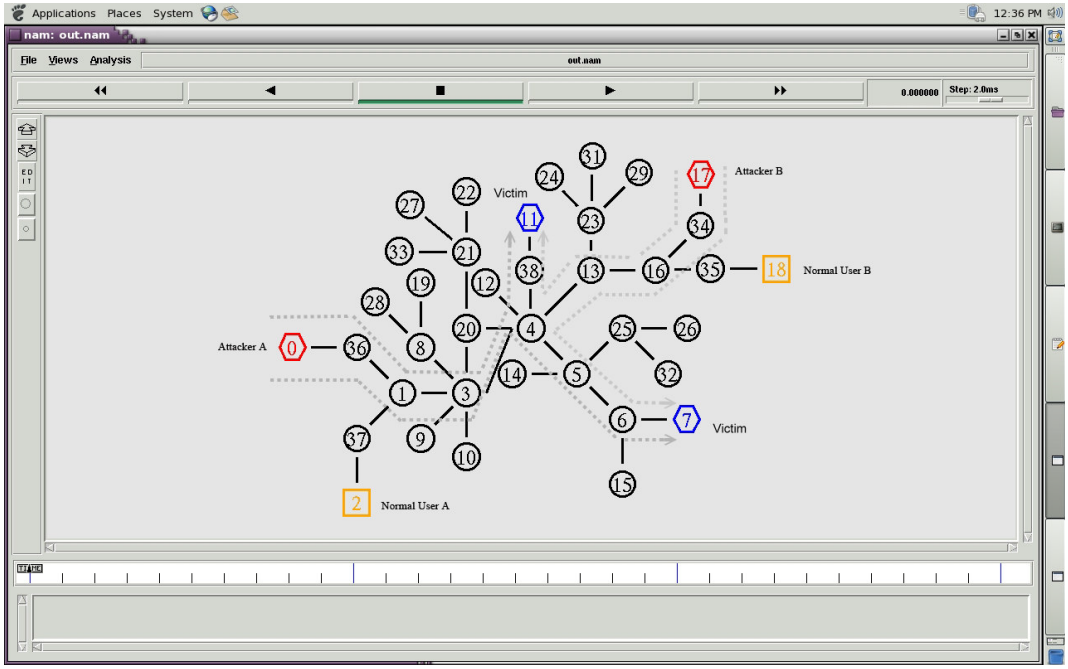

Figure 3. Network topology with attackers
图 3. 含攻击者的网络拓扑

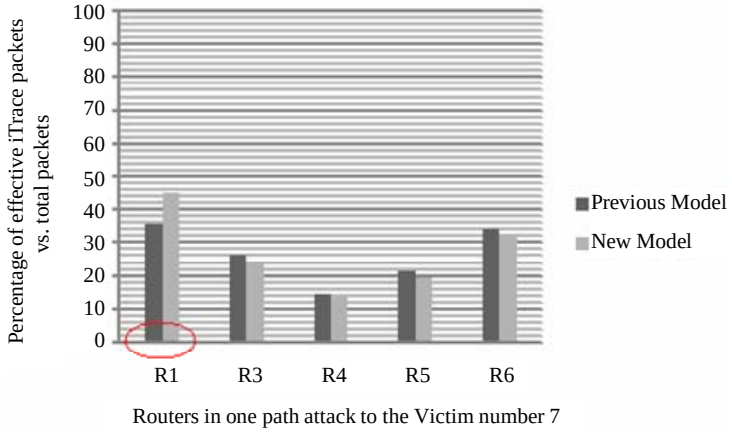

Figure 4. Comparison of effective packet ratio
图 4. 有效数据包比率对比

1) 单个攻击源和单个受攻击服务器，
2) 多个攻击源和单个受攻击服务器，
3) 多个攻击源和多个受攻击服务器。

在上面模拟情况中已经涵盖了普通用户同攻击者利用相同路径发送数据包获取受攻击者服务的情况。在第一种单个攻击源攻击受害者主机的情况，好比仅节点 0 攻击节点 7。其攻击路径是 0→36→1→3→4→5→6→7。图显示了到受害者路径上的路由检测出的有效数据包的百分比。

通过 图 4 我们能看出，接近攻击源和受害者主机的路由所检测出的有效数据包明显增多。在同原来的方法相比，靠近攻击源的路由器 R1 在新方法检测出有效数据所占的百分比比原来的方法多了近 10%，这说明我们提出的方法是有很大效果的。最后通过我们对多个攻击源攻击单个服务器，多个攻击源攻击

多个服务器的两种情况进行的再验证，也同样说明我们新方法在增加有用信息数据包方面是高效。在这就不过多赘述。

6. 结束语

此论文中，我们在研究以前追溯方法的基础上提出了一种能有效提高生成 icmp 追溯报文的方法，通过更多的有效 icmp 追溯报文的数据，更加准确的定位攻击源，找到攻击者，为防御 DOS/DDOS 攻击提供重要依据。在今后过程中，我们将重点研究如何更加准确的分配缓存区的延迟时间，从而使我们的方法达到最佳性能 [11]。

参考文献 (References)

[1] Chen, S.G. and Du, W.L. (2005) Stateful DDoS Attacks and Targeted Filtering. *Journal of Network and Computer Applications*, **30**, 823-840.

[2] Henry, C.J. and Miao, M. (2003) ICMP Traceback with Cumulative Path, an Efficient Solution for IP Traceback. Springer-Verlag, Berlin Heidelberg, 124-135.

[3] Simpson, W. and Karn, P. (1999) RFC 2521: ICMP Security Failures Messages. *Internet Engineering Task Force*.

[4] Haining, W. and Kang, G. (2007) Defense against Spoofed IP Traffic Using Hop-Count Filtering. I*EEE/ACM Transactions on Networking*, **15**, 40-53. https://doi.org/10.1109/TNET.2006.890133

[5] Bellovin, S. (2003) The ICMP Traceback Message. IETF Internet Draft “Draft-Ietf-Itrace-04.txt”, Work in Progress.

[6] Tao, P. and Kotagiri, R. (2007) Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems. *ACM Computing Surveys*, **39**, Article 3.

[7] Atkinson, R. and Kent, S. (1998) RFC 2401: Security Architecture for the Internet Protocol. *Internet Engineering Task Force*.

[8] Ferdous, A. and Barbhuiya, R.S. (2012) An Active Detection Mechanism for Detecting ICMP Based Attacks. 12*th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, Liverpool, United Kingdom, 25-27 June 2012 to June 27, 51-58.

[9] 张翎丽, 任新华, 朱晓军. 具有追忆路径的 ICMP 反向追踪方案[J]. 计算机应用, 2004: 24(s2):107-109.

[10] Felix, W. (2001) On Design and Evaluation of Intention-Driven ICMP traceback. Proc. *IEEE International Conference on Computer Communications and Networks*, Scottsdale, Arizona, USA, 2001, 159-165

[11] 胡延平, 王连杰, 刘武. 基于 ICMP 的网络性能分析[J]. 计算机工程与设计, 2003(4): 30-32.