一体化标识网络映射缓存 DoS 攻击防范方法研究

万 明[1,2],张宏科[3],尚文利[1],沈 烁[4],刘 颖[3]
(1.中国科学院沈阳自动化研究所,辽宁沈阳 110016;2.中国科学院网络化控制系统重点实验室,辽宁沈阳 110016;
3.北京交通大学下一代互联网互联设备国家工程实验室,北京 100044;4.中国互联网络信息中心互联网基础技术开放实验室,北京 100190)

摘 要: 为了抵御一体化标识网络中接入路由器可能遭受的映射缓存 DoS 攻击,本文提出了一种基于双门限机制的映射缓存 DoS 攻击防范方法.该方法设计了一种基于迭代思想的谜题机制降低映射缓存中映射信息条目的增加速率,并采用了映射信息可信度算法识别和过滤映射缓存中恶意的映射信息条目.仿真实验与性能分析表明,该方法能够有效地抵御映射缓存 DoS 攻击,防止映射缓存溢出.

关键词: 一体化标识网络;映射缓存 DoS 攻击;双门限机制;谜题机制;可信度
中图分类号: TN911.23 **文献标识码:** A **文章编号:** 0372-2112 (2015)10-1941-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.10.010

An Efficient Approachto Defend DoS Attack Against Mapping Cache Under Identifier-Based Universal Network

WAN Ming[1,2], ZHANG Hong-ke[3], SHANG Wen-li[1,2], SHEN Shuo[4], LIU Ying[3]
(1. *Shenyang Institute of Automation Chinese Academy of Sciences*, *Shenyang*, *Liaoning* 110016, *China*;
2. *Key Laboratory of Networked Control System Chinese Academy of Science*, *Shenyang*, *Liaoning* 110016, *China*;
3. *National Engineering Laboratory for Next Generation Internet Interconnection Devices*, *Beijing Jaotong University*, *Beijing* 100044, *China*;
4. *DNSLAB*, *China Internet Network Information Center*, *Beijing* 100190, *China*)

Abstract: In order to prevent the potential DoS attack against mapping cache under identifier-based universal network, this paper proposes an efficient defense approach based on double-threshold scheme. This approach not only designs a novel puzzle challenge mechanism based on iterative idea to decrease the growth rate of mapping entries, but also presents the trust value algorithm of mapping information to identify and filter out the malicious mapping entries. In particular, our analytical results show that, this approach is efficient and feasible to prevent the DoS attack against mapping cache, and resists the mapping cache overflow.

Key words: identifier-based universal network; DoS attack against mapping cache; double-threshold; puzzle challenge; trust value

1 引言

在当前互联网体系结构中,IP 地址承载了过多的语义:在传输层标识用户的身份信息,在网络层标识用户的拓扑位置信息.这种 IP 地址的双重语义是引发当今互联网路由可扩展性以及安全性问题的根本原因之一,为此,通过将 IP 地址的双重语义分开,实现身份与位置分离的设计思想已经成为未来互联网理论与技术研究的热点之一.在众多的身份与位置分离解决方案中,基于网络的分离解决方案得到了广泛的研究,典型的有 LISP(Locator/ID Separation Protocol)[1]、Ivip(Internet vastly improved plumbing)[2]以及一体化标识网络[3~5]等,这种方案不需要修改或更新主机的协议栈及上层应用,仅仅由网络中具有特殊位置的路由器完成身份与位置的分离映射,具有较好的可扩展性.其中,一体化标识网络通过采用标识分离映射技术,引入接入标识 AID(Access IDentifier)与交换路由标识 RID(Switch Routing IDentifier)的概念,实现了终端的身份信息与位置信息的分离.

相比传统互联网,一体化标识网络改变了网络基本

收稿日期:2012-11-14;修回日期:2013-06-25;责任编辑:郭游
基金项目:国家自然科学基金(No.61232017,No.61202428,No.61164012);国家 863 高技术研究发展计划(No.2012AA041102-03);中央高校基本科研业务费专项资金(No.2013JBM004);DNSLAB 资助

的通信机制,这不仅带来了诸如路由可扩展性、移动性等优势,而且也在一定程度上提高了网络安全性,例如位置隐私性、核心网安全性等[5].然而,由于网络攻击的种类多种多样、方式层出不穷,新引入的协议体系与设备也可能带来一些新的安全挑战.在一体化标识网络中,为了能够完成对用户数据的快速转发,提高响应效率,每个接入路由器都会在映射缓存暂时存储通信对端的映射信息.并且每条映射信息都对应一个计时器,记录此条映射信息的活跃期 TTL(Time-to-Live),TTL 初始被设定为映射缓存超时时间.倘若某条映射信息在 TTL 期满之前仍被使用,则相应的计时器将重置;倘若某条映射信息在 TTL 值期满时一直没有被使用,则此条映射信息将被删除.然而,这种设计可能导致接入路由器遭受潜在的恶意威胁——映射缓存 DoS 攻击[6].如图 1 所示,当一个或多个恶意攻击者产生大量无用的映射信息条目超过接入路由器映射缓存的容量时,就会导致映射缓存的溢出,中断正常的用户通信,甚至会造成整个接入网瘫痪.

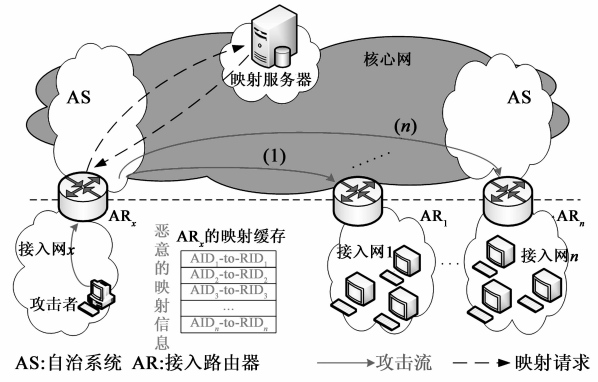

图1 映射缓存DoS攻击示例

从拓扑位置上看,接入路由器是用户网络接入核心网络的接入点,处于接入网与核心网的边界地带,接入网用户能够直接访问接入路由器.由于接入路由器所承担工作的关键性和复杂性,使得接入路由器容易成为恶意攻击者的首选目标,而且接入路由器参与了数据层面和控制层面的所有工作,一旦被攻破将威胁到整个网络.因此,本文结合一体化标识网络结构特点与通信机制,提出了一种基于双门限机制的映射缓存 DoS 攻击防范方法——MapFence.该方法在接入路由器的映射缓存中设置双门限机制防止映射缓存的溢出,保障了接入路由器的可用性,以及合法用户通信的不间断性.首先通过设计一种新颖的基于迭代思想的谜题机制,降低了映射缓存中映射信息条目的增加速率,然后通过提出映射信息可信度算法,识别和过滤了映射缓存中恶意的映射信息条目,确保了映射信息条目的真实性.接入路由器是一体化标识网络的关键基础设施,保障接入路由器的安全,防止其遭受映射缓存 DoS 攻击,不仅为映射机制的正常运作提供了安全基础,而且在一定程度上提高了一体化标识网络的安全性与可靠性.

2 基于双门限机制的防范方法

2.1 主要设计思想

当接入路由器遭受映射缓存 DoS 攻击时,为了防止映射缓存在短时间内被大量无用的映射信息所填满,首要任务就是降低发往不同目的地址的数据包的到达率(注:映射缓存中不存在此类数据包目的地址的映射信息条目,本文将此类数据包命名为初始数据包).MapFence 设计了一种新颖的基于迭代思想的谜题机制达到这一目标,这是因为接入路由器在发送新的映射请求之前,必须首先获得恶意攻击者提供的正确谜题答案,而计算谜题答案需要恶意攻击者花费一定 CPU 时间,这就降低了初始数据包的到达率,间接减缓了发送映射请求的速率,减小了映射缓存中映射信息条目的增加量.

虽然谜题机制可以降低无用的初始数据包到达率,但当攻击者的攻击强度很大时或者当大量恶意攻击者同时发起映射缓存 DoS 攻击时,仍然容易造成映射缓存溢出.为了解决这一问题,MapFence 提出映射信息可信度算法来计算属于同一终端的映射信息的可信度.当某一终端的映射信息可信度小于接入路由器预设定的阈值 LV_t 时,接入路由器将通过过滤器清除掉属于这一终端的映射信息条目,保障映射缓存中映射信息的真实可信性,并在一定时间内过滤掉此终端之后所有的数据包.

MapFence 通过双门限机制充分结合了基于迭代思想的谜题机制与映射信息可信度算法.也就是说,在映射缓存中设置两个门限,门限 1 小于门限 2.当映射缓存中的映射信息条目数达到门限 1 时,接入路由器触发基于迭代思想的谜题机制;当映射缓存中的映射信息条目数继续增加到门限 2 时,接入路由器触发映射信息可信度算法,图 2 给出了 MapFence 的基本工作原理.

为了防止部署 MapFence 后接入路由器的性能下降,门限 1 和门限 2 的具体取值应该根据接入网络的实际情况进行设定,综合考虑接入路由器的影响因素,例如,接入路由器自身的最大处理能力、接入网中的用户数以及单位时间内每个用户的映射信息条目数等.

2.2 基于迭代思想的谜题机制

谜题机制是一种有效的 *DoS* 攻击防御方法[7,8],它将计算负担转移给恶意攻击者,能够快速抑制攻击流量的突发性.基于迭代思想的谜题机制通过迭代算法将质因数分解[9]和离散对数问题完美结合,是一种 CPU

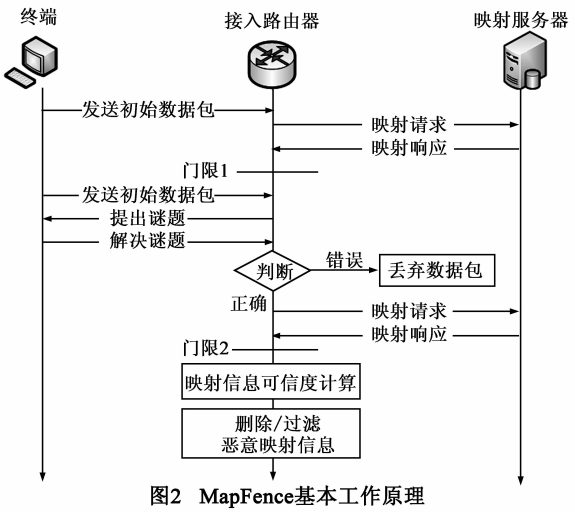

图2　MapFence基本工作原理

限制型谜题算法.

2.2.1　谜题构造算法

接入路由器首先选取一系列素数 $a_1 \cdots a_n$,通过公式(1)计算大数 K.

$$K = \prod_{i=1}^{n} a_i, i \in [1, n] \tag{1}$$

选取一个大的质数 q,同时在$[0, q-1]$选择一个随机数 r. x_1 是在$[r, (r+l) \bmod (q-1)]$区间内随机选择的一个谜题答案,其中 l 是接入路由器指定的可变大数.

然后,接入路由器通过使用公式(2)计算 y_n.

$$\begin{cases} y_i = f(x_i) = i * a_i^{x_i} \bmod q \\ x_{i+1} = f(x_i) \end{cases}, i \in [1, n] \tag{2}$$

式(2)成功运用了迭代算法的基本思想,每一个迭代的底 a_i 是大数 K 的一个质因子,其中 K 的所有质因子按升序序列排列,例如,如果 $u \leqslant v$,那么 $a_u \leqslant a_v$. 公式(2)中的迭代次数 i 能够保障在序列 x_1 到 x_n 中不存在周期循环. 原因如下:如果仅仅运用离散对数等式 $y_i = a_i^{x_i} \bmod q$,由于模数运算,在序列 x_1 到 x_n 中就可能存在周期的循环,即 $x_l = x_{l+c}$. 因此,当一个恶意攻击者发现迭代过程的循环规律时,它就可能找到捷径而逃避大量的计算开销.

另外,由于引入了模运算,在区间$[r, (r+l) \bmod (q-1)]$可能存在不同的 x_1 经过公式(2)计算后得到同一个 y_n. 为了解决这个问题,接入路由器需要利用公式(3)计算所有 x_i 的和 Sum:

$$Sum = \sum_{i=1}^{n} x_i, i \in [1, n] \tag{3}$$

至此,谜题构造算法结束,相应的谜题集是$\{K, q, r, l, y_n, Sum\}$.

2.2.2　谜题验证方法

当一个终端收到接入路由器的谜题后,它首先计算 K 的质因数分解,得到所有的质因子 $a_1 \cdots a_n$. 然后,根据等式(2)和(3),终端通过暴力破解在区间$[r, (r+l) \bmod (q-1)]$查找候选谜题答案 x',并且计算 y_n' 和 Sum'. 如果 $y_n' = y_n$ 且 $Sum' = Sum$,则终端认为 x' 为谜题的答案,然后将 x' 发送给接入路由器.

当接入路由器收到终端解决的谜题答案 x' 后,它仅仅需要对比 x' 和自己保留的 x_1. 若两者一致,则接入路由器向映射服务器查询之前数据包目的地址的映射信息;若两者不一致,则接入路由器丢弃之前的数据包.

2.3　映射信息可信度算法

在接入路由器的映射缓存中,每一条映射信息都拥有一个计时器记录其超时时间,从而判断是否应该删除此条映射信息. 一般情况下,正常的通信行为是连续的、双向的,它的信息交互时延是平均的数据包往返时延 RTT(Round Trip Time). 因此,一个正常映射信息条目的计时时间应该在 0 到最大 RTT 时间内变化. 相反,映射缓存 DoS 攻击是单向的、不连续的行为,它产生的映射信息并不会被真正使用,相应的 TTL 将要一直减小到 0. 基于这个基本原则,本文定义映射信息可信度计算如公式(4)所述.

$$TV = \frac{u+1}{u+v+2} \tag{4}$$

式(4)借鉴 Jφsang 模型[10],采用概率论的二项事件后验概率理论. 其中,TV 为映射信息可信度,u 为接入路由器映射缓存中属于某一终端的合法的映射信息条目数,v 为接入路由器映射缓存中属于同一终端的恶意的映射信息条目数. 映射信息条目的合法性由以下原则判断:若映射缓存中某一映射信息条目的计时时间大于临界值 t_{MR},则认为此条映射信息是合法的;若映射缓存中某一映射信息条目的计时时间小于临界值 t_{MR},则认为此条映射信息是恶意的. 其中,t_{MR}是接入路由器根据自己的网络实际情况预先设定的时间值,例如 5 倍的平均 RTT 时间. 考虑下面的情况:如果一个合法的终端拥有大量的映射信息条目,这些映射信息条目的计时时间小于 t_{MR};同时拥有很少的映射信息条目,这些映射信息条目的计时时间大于 t_{MR}. 因此,依据公式(4)计算的映射信息可信度可能非常低. 为了降低这种误报率,本文规定当属于同一终端的映射信息条目总数超过一个预设值 N_t 时,接入路由器才计算此终端的映射信息可信度.

通过映射信息可信度算法来识别映射缓存 DoS 攻击的主要原因如下:一方面,我们不能仅仅通过属于某一终端的映射信息条目数量来简单识别映射缓存 DoS 攻击,这是因为,终端有可能使用大量的映射信息来完成同一服务,例如,一次 P2P 服务. 另一方面,为了隐藏

自己,恶意攻击者可能使用一小部分映射信息完成某些服务,而使用一大部分无用的映射信息来溢出映射缓存,因此,我们也不能仅仅通过映射信息是否正在被使用来简单识别映射缓存 DoS 攻击.然而,映射信息可信度算法同时考虑了映射信息的数量和使用问题,避免了上述两种情况的发生.

3 性能分析与仿真实验

3.1 谜题机制的优势分析

谜题机制是一种易于实现且非常有效的 DoS 攻击防御方法,它仅仅需要安装一个用于谜题解决的计算软件,对于现在的网络技术水平来说,如此的软件完全可以通过浏览器的插件来实现[8].基于迭代思想的谜题机制主要优势总结如下:

无状态性 基于迭代思想的谜题机制的所有参数都是由接入路由器产生,各参数之间没有关联,换句话说,恶意攻击者不可能根据之前的谜题猜测下一个谜题,即基于迭代思想的谜题机制是无状态的.

良好的计算保障 谜题的解决需要进行质因数分解和模指数迭代运算,恶意攻击者无法找到获得谜题答案的捷径来逃避大量的计算,解决谜题的计算量要远远大于构造谜题的计算量.

抗预计算 由于恶意攻击者无法预期随机数 r 和可变大数 l,因此谜题机制具有抵抗预计算的能力.

抗并行计算 由于采用了迭代算法,恶意攻击者无法同时完成质因数分解和离散对数这两次运算,因此谜题机制具有抵抗并行计算的能力.

易验证 接入路由器仅仅需要一次对比就能完成谜题答案的验证.

细粒度的难度可调节性 这个特性关系到谜题粒度问题[11].根据不同的攻击强度,接入路由器可以从质因数分解的大数 K、迭代次数 n 和查找范围$[r,(r+l)\bmod(q-1)]$这三个方面任意调节谜题机制的难度,因此解决谜题所需要的花费可以进行细粒度的调节.

3.2 防御效果分析

仿真假设:假设接入路由器映射缓存的容量为 200,仿真时间为 100 秒,映射缓存 DoS 攻击在第 21 秒开始.合法映射信息条目的平均增加速率服从泊松分布,为 0.8 条每秒,而恶意映射信息条目增加速率是其 20 倍,为 15 条每秒.另外,假设映射缓存中门限 1 为 120,门限 2 为 170,$N_t=50$,$LV_t=0.2$,$t_{MR}=10$ 秒,$TTL=60$ 秒.同时,我们调整谜题机制的难度,让解决谜题所花费的时间在 0 至 2 秒间变化.

图 3 描述了接入路由器映射缓存中合法的映射信息条目数随时间的变化.在正常情况下,即网络中不存在映射缓存 DoS 攻击,映射缓存中合法映射信息条目数在第 51 秒达到平衡,在 45 条左右波动.然而,当网络中发生映射缓存 DoS 攻击时,映射缓存在第 33 秒时被恶意映射信息条目占满,合法的映射信息条目数迅速降为 10 条左右,倘若我们加大攻击强度,合法的映射信息条目数将要减少到 0.另外,从图 3 中也可以发现,当在接入路由器上实施 MapFence 后,合法的映射信息条目数在第 57 秒达到稳定,其曲线基本与正常情况下一致.

图 4 描述了接入路由器映射缓存中恶意的映射信息条目数随时间的变化.当映射缓存 DoS 攻击发生时,恶意的映射信息条目数在第 33 秒后迅速增加至 190.而当实施 MapFence 后,由于映射信息条目数在 27 秒达到门限 1,攻击者开始执行谜题机制,恶意的映射信息条目随之开始缓慢增加,直至 63 秒时超过门限 2,接入路由器执行映射信息可信度计算,由于攻击者的映射信息可信度远小于实验假设的限定值 $LV_t=0.2$,接入路由器过滤掉所有恶意映射信息,即图中恶意的映射信息条目数在第 63 秒迅速降为 0.攻击者的映射信息可信度计算如下:

$$TV=\frac{(125-118)+1}{125+2}=0.063 \tag{5}$$

其中,125 为恶意的映射信息条目数,118 为恶意的映射信息计时器时间小于 50 秒的条目数.

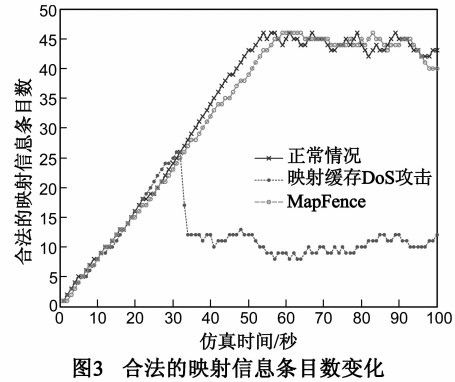

图3 合法的映射信息条目数变化

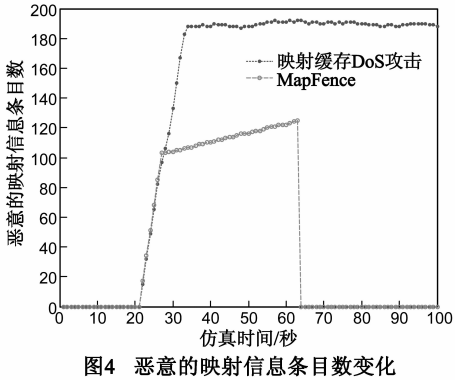

图4 恶意的映射信息条目数变化

综上所述,MapFence 能够有效减缓映射缓存的溢

出,从而防范映射缓存 DoS 攻击.一方面,谜题机制的使用可以降低映射缓存中映射信息的增加速率,确保了合法用户映射信息条目的可用性.另一方面,通过映射信息可信度算法,接入路由器可以识别和过滤恶意的映射信息,进一步保障了映射缓存中映射信息的真实可信性.

3.3　防范方法比较分析

3.3.1　与 Rate Limiting 仿真比较

速率限制 Rate Limiting 是一种著名的防范 DoS 攻击的方法[12],本小节将 MapFence 与 Rate Limiting 进行对比,说明 MapFence 的优越性.不失一般性,假设当映射缓存中映射信息条目数超过门限 1 时,接入路由器开始执行 Rate Limiting,限制映射信息条目的增加速率为 1.5 条每秒.图 5 给出了接入路由器映射缓存中合法的映射信息条目数随时间变化的比较结果,我们发现,MapFence 能有效的保障合法的映射信息条目的数量,而 Rate Limiting 会降低合法的映射信息条目的数量,这是因为 Rate Limiting 不仅仅降低恶意的映射信息条目的增加速率,同时也会影响合法的映射信息条目的增加速率.

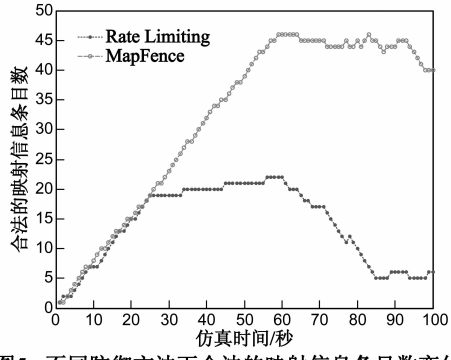

图5　不同防御方法下合法的映射信息条目数变化

图 6 给出了接入路由器映射缓存中恶意的映射信息条目数随时间变化的比较结果,我们发现,Rate Limiting 方法下恶意的映射信息条目数总是大于 MapFence 方法下恶意的映射信息条目数,另外,当实施 Rate Limiting 时,恶意的映射信息条目会一直存在,它的数量在 86 秒时达到 83 条后保持平衡.然而,由于采用了映射信息可信度算法,MapFence 在 63 秒时判别和过滤掉恶意的映射信息,因此恶意的映射信息条目不会在映射缓存中继续保留.

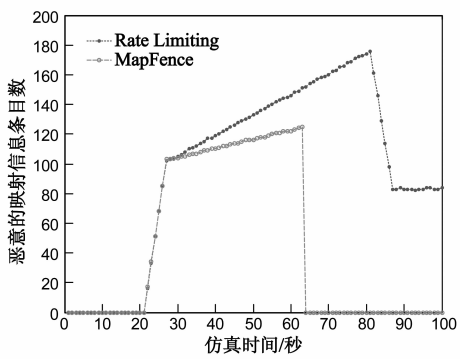

图6　不同防御方法下恶意的映射信息条目数变化

虽然 Rate Limiting 方法也能够减缓映射缓存 DoS 攻击的强度,防止映射缓存的溢出,但它同时也影响了合法用户的正常通信行为.同时,Rate Limiting 无法识别和过滤恶意的映射信息,这将引起接入路由器不必要的资源浪费.因此,在防范映射缓存 DoS 攻击方面,MapFence 更优越于 Rate Limiting 方法.

3.3.2　定性比较分析

随着 DoS 攻击种类多样、攻击方式各异、攻击位置不同,DoS 攻击的防范技术一直是网络安全领域的研究热点,研究人员已经从不同角度提出了新颖独特的防范方法[13~18].在文献[19]的分析基础上,表 1 给出了几种著名 DoS 攻击防范方法的简单定性比较.从表中可以看出,每一种防范方法都有其自身的优势和不足.TVA[15]、Portcullis[16]和 NetFence[17]都需要对现有网络通信协议进行修改,可部署性差.StopIt[18]虽然不需要修改现有网络通信协议,但是它需要 ISP 部署 StopIt 服务器,并与路由器协商过滤规则.而 MapFence 不改变一体化标识网络的基本通信协议,仅仅实施在接入路由器上,可部署性强,同时采用映射信息可信度算法区分恶意的映射信息流量,在防范映射缓存 DoS 攻击方面具有较强的优势.

表 1　几种 DoS 攻击防范方法的定性比较

防御方法	部署位置	可部署性	区分流量	控制流量	控制方式	网络协议修改
TVA	客户端、路由器	难	是	是	Network Capabilities	需要
Portcullis	客户端、路由器	难	是	是	谜题机制	需要
NetFence	路由器	难	是	是	Congestion Feedback	需要
StopIt	StopIt 服务器、路由器	适中	是	一定程度	过滤规则	不需要
Rate Limiting	路由器	易	否	是	速率限制	不需要
MapFence	接入路由器	易	是	是	谜题机制	不需要

3.4 映射缓存超时的影响评估

为了说明不同映射缓存超时时间对 MapFence 的影响,本小节在映射缓存超时时间分别为 40 秒、50 秒、60 秒和 70 秒的情况下进行仿真实验,并对比分析实验结果.图 7 和图 8 分别给出了不同映射缓存超时时间下映射缓存中合法和恶意的映射信息条目数随时间的变化,从图中可以看出,当实施 MapFence 后,映射缓存超时时间的变化并没有对合法的映射信息条目数产生明显的影响,也就是说,随着映射缓存超时时间的增加,合法的映射信息条目数也相应的增长,这与正常情况保持一致.而映射缓存超时时间的变化会对恶意的映射信息条目数产生影响:当映射缓存超时时间分别为 60 秒和 70 秒时,接入路由器会通过映射信息可信度算法识别和过滤掉恶意的映射信息条目,而当映射缓存超时时间分别为 40 秒和 50 秒时,恶意的映射信息条目仍然存在于接入路由器的映射缓存中.出现这种情况的主要原因是,由于偏小的映射缓存超时时间和谜题机制的作用,映射缓存中映射信息条目数没有超过门限 2,因此接入路由器并没有进行映射信息可信度的计算.

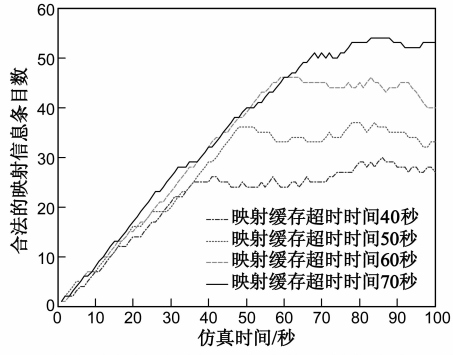

图7 不同映射缓存超时时间下合法的映射信息条目数变化

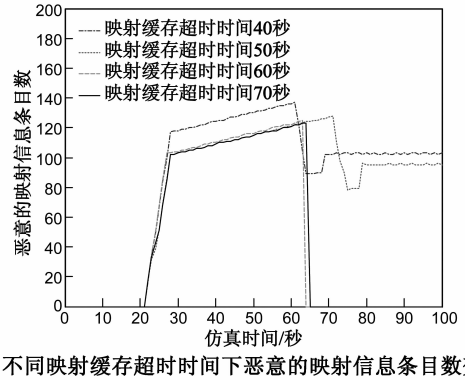

图8 不同映射缓存超时时间下恶意的映射信息条目数变化

因此,当实施 MapFence 时,应该根据实际情况仔细考虑映射缓存超时时间的影响.一方面,太小的映射缓存超时时间会影响 MapFence 的防御效果;另一方面,太大的映射缓存超时时间会增加映射缓存的存储容量,造成接入路由器存储及计算资源的浪费[20].

4 总结

本文在分析一体化标识网络中接入路由器可能遭受映射缓存 DoS 攻击的基础上,提出了一种基于双门限机制的防范方法.该方法设计了一种基于迭代思想的谜题机制减缓映射信息条目的增加速率,采用了映射信息可信度算法识别和过滤恶意的映射信息条目,并通过双门限机制进行有效结合,最终防止了映射缓存的溢出,抵御了映射缓存 DoS 攻击,从而保障了一体化标识网络中接入路由器的可用性.在目前以数据/内容为中心的未来互联网体系架构中,中间路由节点也需要缓存数据内容等相关信息,这就有可能面临与映射缓存 DoS 攻击相似的安全问题,因此未来的研究工作重点着眼于如何对本文所提出方法的改进,以抵御数据/内容中心网络中路由节点遭受缓存 DoS 攻击.

参考文献

[1] Farinacci D, Fuller V, Meyer D, et al. The locator/ID separation protocol (LISP)[S]. IETF Internet Standard, RFC 6830, Jan. 2013.

[2] WhittleR. Ivip (Internet vastly improved plumbing) architecture [S]. Internet Draft, draft-whittle-ivip-arch-04, Mar. 2010.

[3] 张宏科,苏伟.新网络体系基础研究——一体化网络与普适服务[J].电子学报,2007,35(4):593 - 598.
Zhang Hong-ke, Su Wei. Fundamental research on the architecture of new network——universal network and pervasive services[J]. Acta Electronica Sinica, 2007, 35(4): 593 - 598. (in Chinese)

[4] 李世勇,秦雅娟,张宏科.基于网络效用最大化的一体化网络服务层映射模型[J].电子学报,2010,38(2):282 - 289.
Li Shi-yong, Qin Ya-juan, Zhang Hong-ke. Mapping model for the service layer of universal network based on network utility maximization[J]. Acta Electronica Sinica, 2010, 38(2): 282 - 289. (in Chinese)

[5] 董平,杨冬,秦雅娟等.新一代互联网移动管理机制研究[J].电子学报,2008,36(10):1916 - 1922.
Dong Ping, Yang Dong, QinYa-juan, et al. Research on the mobility management scheme in future Internet[J]. Acta Electroniea Sinica, 2008, 36(10): 1916 - 1922. (in Chinese)

[6] Saucez D, Iannone L, Bonaventure O. LISP threats analysis [S]. IETF Internet Draft, draft-ietf-lisp-threats-04. txt, Feb. 2013.

[7] Fallah M. A puzzle-based defense strategy against flooding attacks using game theory[J]. IEEE Transactions on Dependable and Secure Computing, 2008, 7(1): 5 - 19.

[8] Y Gao, W Susilo, Y Mu, et al. Efficient trapdoor based client puzzle against DoS attacks[A]. Network Security[C]. New

York: Springer, 2010. 229 – 249.
[9] F Tegeler and X M Fu. SybilConf: computational puzzles for confining sybil attacks[A]. Proceedings of INFOCOM 2010 on Computer Communications Workshops[C]. New Jersey: IEEE Press, 2010. 1 – 2.
[10] Jφsang A, Ismail R, Boyd C. A survey of trust and reputation systems for online services provision[J]. Decision Support Systems. 2007, 43(2): 618 – 644.
[11] S Tritilanunt, C A Boyd, E Foo, et al. Toward non-parallelizable client puzzles[A]. Proceedings of 6th International Conference on Cryptology and Network Security[C]. Berlin: Springer-Verlag, 2007. 247-264.
[12] J V E Molsa. Effectiveness of rate-limiting in mitigating flooding DoS attacks[A]. Proceedings of the Third IASTED International Conference on Communications, Internet, and Information Technology[C]. Calgary: ACTA Press, 2004. 155 – 160.
[13] Khanna S, Venatesh S S, Fatemieh O et al. Adaptive selective verification: an efficient adaptive countermeasure to thwart DoS attacks[J]. IEEE Transactions on Networking, 2012, 20(3): 715 – 728.
[14] C Barna, M Shtern, M Smit, et al. Model-based adaptive DoS attack mitigation[A]. Proceedings of 2012 ICSE Workshop on Software Engineering for Adaptive and Self-Managing Systems[C]. New Jersey: IEEE Press, 2012. 119-128.
[15] Yang X W, Wetherall D, Anderson T. TVA: A DoS-limiting network architecture[J]. IEEE/ACM Transactions on Networking, 2008, 16(6): 1267-1280.
[16] B Parno, D Wendlandt, E Shi, et al. Portcullis: protecting connection setup from dnial-of-capability attacks[A]. Proceedings of ACM SIGCOMM 2007[C]. New York: ACM Press, 2007. 289 – 300.
[17] X Liu, X W Yang, Y Xia. NetFence: preventing Internet denial of service from inside out[A]. Proceedings of ACM SIGCOMM 2010[C]. New York: ACM Press, 2010. 255 – 266.
[18] X Liu, X W Yang, Y B Lu. To filter or to authorize: network-layerDoS defense against multimillion-node botnets[A]. Proceedings of ACM SIGCOMM 2008[C]. New York: ACM Press, 2008. 195 – 206.
[19] 孙长华, 刘斌. 分布式拒绝服务攻击研究新进展综述[J]. 电子学报, 2009, 37(7): 1562 – 1569.
Sun Chang-hua, Liu Bin. Survey on new solutions against distributed denial of service attack[J]. Acta Electroniea Sinica, 2009, 37(7): 1562 – 1569. (in Chinese)
[20] J Kim, L Iannone, A Feldmann, A deep dive into the LISP cache and what ISPs should know about it[A]. Proceedinds of the 10th International IPIF TC 6 Networking Conference (NETWORKING 2011)[C]. Berlin: Springer-Verlag, 2011. 267 – 278.

作者简介

万　明　男, 1984 年 3 月出生于内蒙古通辽市. 2013 年 1 月获得北京交通大学工学博士学位, 现就职于中国科学院沈阳自动化研究所, 助理研究员. 主要研究方向: 下一代互联网网络架构与安全、工业控制网络信息安全技术.
E-mail: ming305.bjtu@gmail.com

张宏科　男, 1957 年生于山西大同市. 博士, 教授, 北京交通大学博士生导师. 主要研究方向: 下一代互联网理论、路由理论与技术、传感器网络理论与技术等.
E-mail: hkzhang@bjtu.edu.cn