内容中心网络中 DoS 攻击问题综述

李 杨[1,2], 辛永辉[1], 韩言妮[1], 李唯源[1], 徐 震[1]

[1]中国科学院 信息工程研究所 信息安全国家重点实验室 北京 中国 100093
[2]中国科学院大学 网络空间安全学院 北京 中国 100049

摘要 “内容中心网络”(Content Centric Networking, CCN)是未来互联网架构体系群中极具前景的架构之一。尽管 CCN 网络的全新设计使其能够抵御目前网络存在的大多数形式 DoS 攻击, 但仍引发了新型的 DoS 攻击, 其中危害较大的两类攻击是兴趣包泛洪攻击和缓存污染攻击。这两类 DoS 攻击利用了 CCN 网络自身转发机制的安全逻辑漏洞, 通过泛洪大量的恶意攻击包, 耗尽网络资源, 并导致网络瘫痪。与传统 IP 网络中 DoS 攻击相比, CCN 网络中的内容路由、内嵌缓存和接收者驱动传输等新特征, 对其 DoS 攻击的检测和防御方法都提出了新的挑战。本文首先介绍 CCN 网络的安全设计和如何对抗已有的 DoS 攻击, 然后从多角度描述、比较 CCN 中新型 DoS 攻击的特点, 重点阐述了兴趣包泛洪攻击和缓存污染攻击的分类、检测和防御方法, 以及它们所面临的问题挑战, 最后对全文进行总结。

关键词 内容中心网络; DoS 攻击; 兴趣包泛洪攻击; 缓存污染攻击
中图法分类号 TP309.2 DOI 号 10.19363/j.cnki.cn10-1380/tn.2017.01.007

A Survey of DoS Attack in Content Centric Networking

LI Yang[1,2], XIN Yonghui[1], HAN Yanni[1], LI Weiyuan[1], Xu Zhen[1]

[1] State Key Laboratory Of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2] University of Chinese Academy of Sciences, Beijing 100049, China

Abstract Content Centric Networking (CCN) is one of the most promising architectures in the future Internet architecture. Although the new design in the CCN network can withstand the most network DoS attacks, it still leads to the new types of DoS attack, including interest flooding attack (IFA) and cache pollution attack (CPA) which is two kinds of attacks with greatest harm. These two types of DoS attacks exploit the security logic vulnerabilities of the CCN network forwarding mechanism itself, through flooding a large number of malicious attacks packets, exhausting the network resources, resulting in network paralysis. Compared with traditional IP DoS attacks, the new features of CCN network, such as content routing, embedded caching and receiver driven transmission, put new challenge to the detection and defense of DoS attacks. This paper firstly introduces the security design of CCN network and how to prevent the existing DoS attacks, then describes and compares the CCN new DoS attacks' characteristics from a variety of angles, and then explains the classification, detection and defense methods, and their problems of the IFA and CPA in details, and finally concludes the paper.

Key words Content Centric Networking; DoS attack; interest flooding attack; cache pollution attack

1 概述

互联网用户对接入内容的访问量和移动流量的增长在不断增加, 根据思科预报, 从 2014 年到 2019 年, 年度 IP 流量将增至三倍, 达到创纪录的 2ZB[1]。推动流量增长的因素包括全球互联网用户、个人设备和机器对机器(M2M)连接的增加, 更快的宽带速度, 以及更高级的视频服务等。到 2019 年全球 IP 流量将达到每月 168 EB, 全球 IP 网络传送的流量几乎与之前所有“互联网年”传送的流量总和(从 1984 年到 2013 年底)一样多。2014 年至 2019 年的全球移动互联网流量将会增长 10 倍, 每月达到 24.3EB。

为了适应互联网应用由发送者驱动的端对端通信模式向接收者驱动的海量内容获取模式的转变, 从网络体系架构层面(而非以网络中间件方式)提供对可扩展和高效内容获取的原生支持, 同时增强网络对移动性和安全性的支持, 研究界近年来提出了一类以信息/内容为中心的新型网络体系架构[2], 典

通讯作者: 韩言妮, 博士, 助理研究员, Email: hanyanni@iie.ac.cn。
本课题得到国家自然科学基金 (No. 61202419); 中国科学院战略性先导科技专项(No. XDA06010306)资助。
收稿日期: 2016-06-22; 修改日期: 2016-10-21; 定稿日期: 2016-12-22

型的如 DONA[3], CCN[4], PSIRP[5], NetInf[6]。有兴趣的读者可以进一步参考相应的综述文献[7-9]。

内容中心网(Content Centric Networking, CCN)[4]自提出以来便受到广泛关注与认可, 经过命名数据网络(Named Data Networking, NDN①)[10]项目的深入研究与论证, 已成为当前比较成熟的未来网络体系结构[11-12]。相比较传统网络, CCN 在设计中已加入了一定的安全机制, 其基本理念是保护内容本身, 而并非保护网络和链路连接的安全。同时, CCN 网络的全新设计使其能够抵御目前网络存在的大多数形式的 DoS 攻击。但 CCN 在解决传统网络问题的同时, 产生了新型的 DoS②攻击, 其中危害较大的两类攻击是兴趣包泛洪攻击[13-15]和缓存污染攻击[16-18]。这两类 DoS 攻击利用了 CCN 网络转发机制本身的安全逻辑漏洞, 通过泛洪大量的恶意攻击包, 耗尽网络资源, 导致网络瘫痪。

虽然 DoS 攻击的特征及相关的检测和防御技术已经在 TCP/IP 网络中得到了较为广泛的研究, 但 CCN 网络中的内容路由、内嵌缓存和接收者驱动传输等新特征致使传统的 DoS 攻击的检测和防御方法均无法直接无缝地移植到 CCN 网络中。得益于全球各国对未来网络体系架构研究的支持, 近年来许多研究人员都致力于 CCN 中的 DoS 攻击研究, 在兴趣包泛洪攻击和缓存污染的检测和防御方法等多个研究领域进行了开拓性的探索, 并提出了创造性的研究成果。本文正是以此为背景, 对 CCN 网络的现有研究成果加以评述, 对相关的研究思路进行溯源和比较, 并指出未来的研究方向。本文剩余部分的组织结构如下: 第 2 节对 CCN 的协议架构和安全设计加以概述, 重点分析了 CCN 如何对抗已有的 DoS 攻击; 第 3 节主要从多角度描述 CCN 中新的传输模式所引发的新型 DoS 攻击; 第 4 节和第 5 节分别对兴趣包泛洪攻击和缓存污染攻击的分类、检测和防御方法加以详细阐述, 并且指出了他们所面临的问题和挑战; 最后, 第 6 节对全文进行总结。

2 CCN 的安全

CCN 的全新设计理念使其在内容路由, 网络缓存和传输协议等方面呈现出不同于传统 IP 网络新特征。同时, CCN 在设计之初就将安全作为网络的原生需求, 重在保护内容本身的安全, 并且试图避免 TCP/IP 网络中常见的 DoS 攻击。下面首先介绍 CCN 的基本概念, 然后简要分析 CCN 中的安全设计, 最后详细阐述 CCN 如何对抗已有 DoS 攻击。

2.1 CCN 概述

在所有未来网络的提议中, CCN 是备受关注的一个架构。CCN 是 2009 年美国帕罗奥多研究中心公(PARC)的 Van Jacobson 教授等人提出来的新型下一代网络体系结构。2010 年 9 月, 美国 NSF 批准的 4 个未来网络体系结构项目中就包括该网络体系结构。此外, 开源网络协议 CCNx[19]和基于 NS3 的 NDNSim[20]模拟器可以用来评估 CCN 研究实现。

CCN 网络是一个基于内容的网络。CCN 中的核心思想是它对网络中的每个内容命名, 而不是使用主机和节点的 IP 地址。当需要获取一个内容/服务时, 网络节点将发送一个包含所需内容/服务名字的请求。该请求按照内容名字进行路由, 而不是 IP 地址。值得注意的是, 网络节点不需要连接到一个特定的服务器来获取数据。然后, 网络将相应数据对象返回给该节点。另一个重要的概念是, 网络部署内嵌的网络缓存。每当数据包通过一个网络缓存节点时, 它将被缓存(或者根据策略进行缓存)。而每当请求在中间节点命中时, 中间节点将直接按照请求路径返回内容。

2.1.1 CCN 中的数据包

在 CCN 网络环境中, 有两大数据包类型: 兴趣数据包(Interest)与内容数据包(Data), 以下简称兴趣包和数据包。兴趣包与内容包在 CCN 的网络传输中是一一对应的关系, 一个兴趣包最多只对应着一个内容包。

表 1 兴趣包

字段	字节长度
Type	2
ContentName	变长
MinSuffixComponent	2
MaxSuffixComponent	2
PublisherPublicKeyDigest	32
Exclude	5
Scope	5
InterestLifetime	2
Nonce	6

兴趣包是 CCN 网络环境中的数据请求包, 具体的字段结构如表 1 所示。兴趣包中的“PublisherPublicKeyDigest”字段是兴趣包的可选项, 表示内容提供者的公钥摘要信息。“Exclude”字段也是兴趣包的可选项, 在和该兴趣包前缀相匹配的内容中, 满足“Exclude”字段的内容名称会被屏蔽掉。“Scope”字段指明了兴趣包可以被转发的跳数。

①为了方便起见, 本文将不区分 CCN 和 NDN, 而统一用 CCN 来表示。
②本文不区分 DoS 和 DDoS 攻击, 而统一用 DoS 来表示, 所述内容对 DoS 和 DDoS 都适用。

表 2　数据包

	字段	字节长度
SignedInfo	Type	2
	Signature	变长
	ContentName	变长
	PublisherPublicKeyDigest	32
	Timestamp	6
	ContentType	3
	KeyLocator	3
Content		分片大小

内容包作为兴趣包的响应数据包, 封装了兴趣包所请求的内容, 具体的字段结构如表 2 所示。内容包中, 除了有所请求的内容数据, 也同样有“ContentName”字段, 与兴趣包的“ContentName”字段一致。内容包中包含了内容提供者的数字签名和相应的加密信息。加密信息用来验证签名和数据内容。内容包的“Signature”字段是签名信息。签名将名称与内容相结合, 无论何时、何地、通过什么方式获取到内容包, 内容包的签名信息都能够提供完整性、准确性认证以及数据源的身份认证。内容包的“SignedInfo”中的“PublisherPublicKeyDigest”字段表示内容提供者的公钥摘要信息, 可用于获得秘钥及内容鉴权。

2.1.2　CCN 的转发逻辑

CCN 网络是一种接收者驱动的网络架构模型, 其网络中间节点被称为内容路由器。网络用户通过向网络中的上游节点发送兴趣包来请求希望得到的网络内容。一旦某个上游节点具有该兴趣包所请求的内容, 该节点会将该内容封装在内容包中并且沿请求路径返回。

内容路由器在 CCN 包括三个主要的数据结构: (1)转发信息库(Forwarding Information Base, FIB), 即路由表; (2)内容存储器(Content Store, CS)和(3)待定兴趣表(Pending Interest Table, PIT)。FIB 就是内容路由器中的路由表, 而本地内容存储器 CS 缓存每一个通过的数据包。PIT 为每个转发出去的兴趣包维护一个兴趣包传入接口表项, 返回的数据包根据该表项信息将相应的数据包沿原路径返回给请求者。一个 PIT 条目包含一个 CCN 的名字和一个或者多个输入接口, 用来记录哪些接口收到了该内容的请求。图 1(a)描述了 CCN 中兴趣包查找和转发过程。当一个内容路由器接收了一个包含内容名称的兴趣包时, 它先检查它的 CS。如果缓存副本存在, 则将此副本发送回传入接口。如果缓存副本不存在, 但该内容名称的 PIT 条目已被创建, 将传入接口添加到该条目中然后请求兴趣包被删除。如果匹配 PIT 条目不存在, 将创建一个新的条目, 然后兴趣包按照 FIB 进行转发。如果在 FIB 中没有发现匹配的路由, 根据具体的路由策略该兴趣包可能被丢弃或广播。

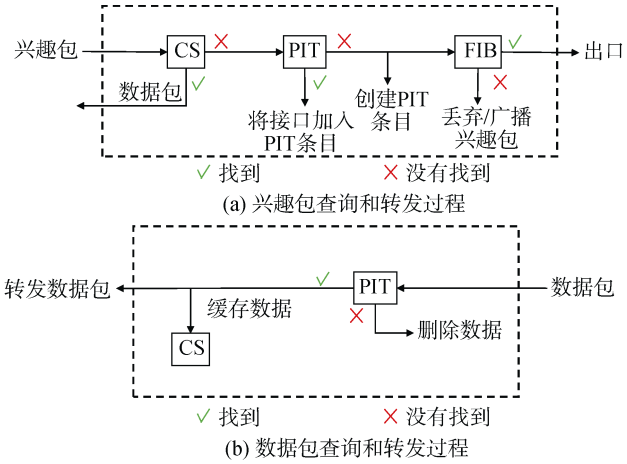

图 1　CCN 中报文查询和转发过程[13]

图 1(b)描述了数据包的查找和转发过程。当内容路由器收到数据包时, 首先查找 PIT。如果在 PIT 中找到该条目, 则数据包先缓存到 CS 中, 然后按传入接口依次转发, 最后将 PIT 中的该条目删除。如果发现 PIT 中没有该条目, 内容路由器则将数据包删除。CCN 的数据获取过程保证一个兴趣包只能收到一个数据包。

2.2　CCN 中的安全设计

CCN 建立在基于内容安全的概念之上, 强调保护并信任内容本身, 而不是传统的保证内容传播路径的安全。CCN 中所有内容通过数字签名来验证, 通过加密保护私有内容。CCN 采用“自验证”命名规则, 将密文摘要和内容提供商的 key 加入到命名结构中去。每一段数据片段都连同它的命名被签名, 安全地绑定数据和命名。这个签名是强制性的, 应用也不能被豁免。绑定数据发布者信息的签名, 可以实现数据源认证。

文献[21]指出, CCN 安全机制的核心理念是让负载更接近源。换言之, 减少数据与用户之间的跳数可以有效避免中间系统对数据的破坏, 使数据正确、有效到达用户端的概率更高。CCN 具备动态内容缓存能力, 可减少内容传输过程中所通过的中间机构, 减少内容到用户之间的跳数。

CCN 的安全模型也方便了发布者和消费者之间的信任建立。这为发布者、消费者和应用提供了大量可供选择和定制的灵活的信任模型。

CCN 的以内容为中心的安全方法, 可以扩展到

内容访问控制和基础设施安全。CCN 内容访问控制的主要方式是加密, CCN 不需要受信的服务器或者目录来制定访问控制策略, 因为只有授权用户能够解密私人内容。CCN 并不针对网络安全的问题提出解决方案, 只提供解决内容合法性的机制, 并对机制的有效性进行保障。当然, 也需要网络路由中的签名和对数据的控制提供所需的路由协议安全。

2.3 CCN 中安全的相关研究

尽管 CCN 在设计之初就将安全作为网络架构的原生需求, 将安全理念融入到网络架构设计中, 但其仍然不可避免的存在一些安全问题。文献[22]对信息中心网络(Information Centric Networking, ICN)研究中安全攻击进行了综述分析, 将所有的攻击分为四大类: 命名相关的攻击, 路由相关的攻击, 缓存相关的攻击和其他攻击。

命名相关的攻击利用 ICN 中与位置无关的命名特点, 攻击者可以在网络任何位置监视用户请求/数据, 根据某些规则过滤或删除用户请求/数据[23-24], 同时用户隐私受到极大威胁。现有的与命名攻击相关的解决方案, 比如 mix-nets[25], Tor[26], Freedom[27], Anonymizer[28]和 Freenet[29]都不能很好的适用于以内容为中心的 CCN 网络结构。Arianfar 等人[24]提出了一种针对 CCN 命名攻击的解决方案, 该方案并不需要内容发布者和用户之间共享密钥并且适用用户较多的场景。Ion 等人[30]设计了一套基于属性加密和路由隐私的方案, 其基本思想是将分布式访问控制策略应用到内容中, 并在内容上指定这些策略。该方案支持大规模的应用部署, 且不需要共享密钥。

路由相关的攻击旨在通过泛洪大量请求使得 CCN 基础设施和网络节点忙于计算、存储和更新等操作, 从而导致拒绝服务。已有许多论文对 DoS 攻击及其检测/预防机制进行讨论[31-33]。目前互联网上广泛讨论的对策包括 IP 追踪[34], 包过滤[35]和速率限制[36]。然而这些技术由于都依赖节点的 IP 地址而不能用在 CCN 中。CCN 中通过泛洪对不存在内容的请求来攻击网络中间节点的攻击方式在很多文章中被提及[13-15], 而通常采用的解决方式是限制请求速率。方案[11,15]提出了通过限制每个用户的速率来解决路由相关攻击, 这在 CCN 中是比较难以实现的, 因为 CCN 中没有主机标识符, 攻击者可以很容易地创建大量超过指定的限速要求的请求。

缓存相关攻击包括窥探用户隐私和缓存污染。现有的解决方案主要针对现网单一大缓存, 对 CCN 这种泛在化的缓存并不适用。Mohaisen 等人[37]提出了一种针对缓存窥探行为的用户隐私保护方案, 但是该方案没有考虑不同的缓存策略。CacheShield 策略[18]根据目标内容的请求次数确定存储概率, 避免缓存流行度小的内容, 从而降低污染内容进入缓存的概率。文献[38]提出了一种按照内容排名的顺序进行缓存决策方法, 从而区分合法内容和恶意内容。

其他攻击是指除以上三种攻击之外的任何形式的攻击, 包括现网中的各种攻击方式。文献[39]提到了通过非法接入达到破坏内容分布以降低 ICN 服务效率的一种攻击形式, 并且提出了一种基于接入控制实体来限制非法接入的防御方式。文献[40]还提出了一种基于 ICN 智能电网的安全覆盖层协议。

文献[22]通过对比以上各种攻击的危害程度指出, 路由相关攻击和缓存相关攻击中的 DoS 攻击方式对网络造成的破坏最为严重, 因为这两种攻击方式可以采取分布式的攻击模式, 从而很容易造成大范围的影响。因此本文重点关注与路由和缓存相关的危害较大的两类 DoS 攻击: 兴趣包泛洪攻击和缓存污染攻击。

2.4 CCN 对抗已有的 DoS 攻击

传统 TCP/IP 网络中的 DoS 攻击有多种形式, 可根据不同的模式特征将其分为以下三种[15,41]; 而 CCN 网络的内在优势, 使得在 TCP/IP 中的这些 DoS 攻击都能够一定程度甚至完全避免。

(1) 带宽耗尽型攻击

这是一种常见的 DoS 攻击形式。攻击者自己或者通过控制僵尸机向被攻击目标泛洪 IP 数据包, 使得被攻击目标的网络或服务器资源达到饱和, 从而使正常用户到被攻击者目标之间的网络线路不可达, 或使网络无法正常提供服务。一般情况下, 这种攻击会使用 TCP、UDP 或 ICMP 以最高的数据速率向受害者发送数据流。

在 CCN 环境中, 如果发起该类型攻击的的话, 攻击者需要自己或者通过控制僵尸机向被攻击目标发送大量的针对某个存在的内容的兴趣包。然而, 在 CCN 网络中, 中间内容路由器会将从不同接口传入的对相同内容的请求兴趣包删除, 而仅仅将传入接口加入到 PIT 的对应表项中, 使得大量的相同内容的请求在网络边缘被汇聚掉, 而无法到达被攻击目标。更重要的是, 一旦某个内容请求被节点转发并得到相应的内容回复后, 该传输路径上的所有节点的缓存中都会存储该内容数据。对于已请求过的真实内容的再次请求可能会被中间节点缓存满足而不再被转发到被攻击目标。CCN 网络这种新型的传输转发机制限制相同的攻击兴趣包到达被攻击目标处, 所以该类型攻击很难对被攻击目标产生预期的影响。

(2) 反射型攻击

反射型攻击中包含攻击者、被攻击目标和二级受害者(反射器)。这种攻击主要是使用反射器使被攻击目标出现流量过载。攻击者向众多反射器发送大量的 IP 数据包, 并将这些数据包的源 IP 地址伪造成被攻击目标的地址。这些反射器会将这些数据包的回复发送给被攻击的目标。

CCN 网络同样能够抵御该种类型的攻击。因为在 CCN 网络中, 数据包不再携带源地址和目标地址, 而是将路径信息记录在网络中间节点的 PIT 中。答复请求的数据包只会按照原有路径返回给请求者。因此无法利用反射器将流量引向被攻击目标。尽管 CCN 网络节点支持多播和广播, 即便在最糟的情况下, 即网络中每个节点都对兴趣包进行广播发送, 其回复的内容包也会受到节点接口数目的限制, 不会对网络造成较大影响。因而, 唯一有效的反射型攻击要求攻击者和被攻击目标在同一物理网段中, 否则无效。

(3) 前缀劫持的黑洞型攻击

在前缀劫持攻击中, 一旦某个自治域被错误地配置或恶意篡改, 使其对外宣告一些实际上无效的伪路由信息, 这样会使得其他自治域将这些流量转发给该自治域, 该自治域就如同“黑洞”一样接收了其宣告地址的所有流量, 而该自治域最终只能将这些伪地址的流量丢弃。一旦路由信息被篡改, 路由节点很难监测到该问题, 也很难从中恢复, 因此这种攻击对网络造成的影响很大。

CCN 网络同样能够抵御前缀劫持攻击。首先, 在 CCN 网络中, 所有的路由更新信息都有数字签名, 并和内容数据包一样能够进行身份认证, 这就使前缀劫持攻击的风险降到了最低。而且, CCN 网络节点与传统 IP 网络节点相比, 能够获取更多的网络信息, 用于检测网络在内容传输过程中的异常。另外, CCN 网络的多路径转发机制能够探索网络中的冗余拓扑, 在网络遭受攻击时可以快速选择备用路由方案进行应对。

3　CCN 中的新型 DoS 攻击

CCN 在解决传统网络问题的同时, 引入了新型的 DoS 攻击。这类攻击利用了 CCN 网络转发机制本身的安全逻辑漏洞, 通过泛洪大量的恶意攻击包, 耗尽网络资源, 导致网络瘫痪。与传统的 IP 网络中 DoS 攻击相比, CCN 网络中的内容路由、内嵌缓存和接收者驱动传输等新特征, 对其 DoS 攻击的检测和防御方法都提出了新的挑战。

3.1　新型 DoS 攻击分类

CCN 中的 DoS 攻击分类如图 2 所示[42]。图中每个分支显示了用不同的方法来实现攻击的方式和目标。

DoS 攻击的一种形式是使请求内容无法访问:

(1) 干扰内容源。由于虚假的内容请求无法在网络中间节点得到满足, 故可以通过泛洪大量虚假兴趣包直达内容源。也可以利用兴趣包的特殊位, 使得中间节点缓存无法命中而使大量的兴趣包抵达内容源。通过以上方式泛洪大量兴趣包至内容源, 将使内容源资源耗尽, 网络拥塞, 从而无法为正常用户提供服务。

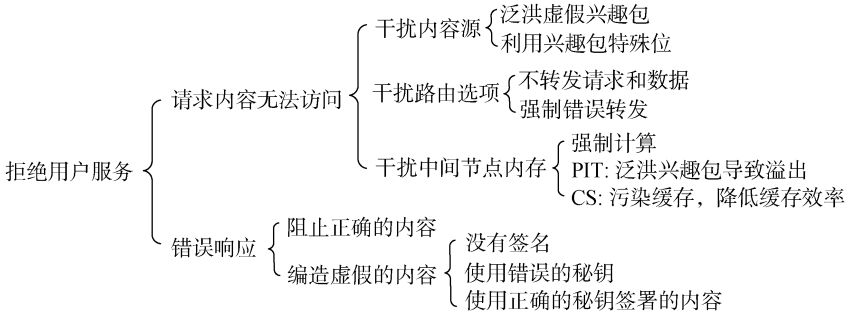

图 2　CCN 中 DoS 攻击分类[42]

(2) 干扰路由选项。通过恶意篡改路由选项, 破坏路由协议, 使得请求和内容不被转发或者被错误转发, 从而导致无法为正常用户提供服务。

(3) 干扰中间节点内存。一种是要求路由器进行代价昂贵的计算来减慢处理速度, 减缓发送请求。另外, 通过泛洪大量的兴趣包使 PIT 溢出来耗尽路由器内存, 导致合法请求无法加载到 PIT 进行转发。还有一种是通过污染 CS, 使得内容无法就近从中间节点的缓存上获取, 甚至用来传播非法内容。

拒绝服务的另一途径是提供错误的响应:

(1) 阻止正确的内容。有效的内容被路由器阻止, 从而被用户认为是无效的, 攻击者可以重播(或产生)

一个“内容不存在”的响应来拒绝合法用户的请求。

(2) 编造虚假的内容。直接反馈给用户虚假编造的内容。虚假内容包括: 没有签名的内容; 使用错误密钥生成的内容; 使用过期的正确密钥生成的内容。

3.2 各种新型 DoS 攻击分析

下面从攻击方式、影响、对策和风险几个角度对以上各种 DOS 攻击进行详细的描述[42], 他们之间的对比可见表 3。

(1) 通过泛洪虚假兴趣包对内容源进行攻击

攻击方式: 攻击者为不存在的内容构造大量不同的名称, 然后利用这些伪造的内容名称发送大量的虚假兴趣包。由于网络中间节点缓存无法命中, 兴趣包将直接路由到内容源, 即可以达到淹没源和拒绝为合法客户提供服务的目的。

对策: 路由器可以通过记录 PIT 的条目数、无响应兴趣包的数量、兴趣包过期的比例等来检测攻击。如果路由器检测到一定数量的无响应的可疑兴趣包, 路由器可以减缓对该前缀兴趣包的转发速率。

风险: 中等。尽管可能被漏检, 但仍可以检测得到。在内容源攻击被检测到之前, 中间路由器的 PIT 应该已经检测到了攻击, 通过采取相应的防御措施, 攻击很难影响到内容源。攻击需要拥有一个僵尸网络和大攻击流量。

(2) 利用兴趣包特殊位对内容源进行攻击

攻击方式: CCN 的兴趣包可以指定其无法从缓存中获得被检索到的内容。攻击者可以向给定的内容源发送大量的兴趣包, 并指定其不会从缓存中获取响应。通过这种方式内容源将被兴趣包淹没, 拒绝为合法用户服务。

对策: 限制使用兴趣包的特殊选项。例如, 只允许在本地范围内转发的兴趣包使用特殊选项。

风险: 低。通过限制使用兴趣包的特殊选项可以最大程度的降低风险。攻击需要拥有一个僵尸网络和大攻击流量。

(3) 通过不转发或强制错误转发对路由选项进行干扰

攻击方式: 攻击者可以通过控制路由器来干扰正常的路由选择, 使路由器对指定的兴趣包或者数据包不转发或者强制错误转发。例如, 当路由器上的某个 PIT 选项超时后, 它将删除挂起的兴趣包, 不再做任何转发响应。如果攻击者在受控路由器上对某些兴趣包设置不同的超时配置, 就可以达到阻止内容被转发的目的。

对策: 阻止攻击者非法控制网络中间路由器, 加强路由器接入控制管理。

风险: 低。攻击者需要非法入侵控制大量网络路由器。

(4) 通过强制计算对路由器进行攻击

攻击方式: 这种攻击建立在路由器需要对内容签名进行验证的假设之上。攻击者向产生恶意内容的数据源发送请求, 每个数据项都是不同的, 并使用不同的密钥签名。为了验证签名, 路由器必须从内容源告知的位置检索密钥。攻击者可以请求大量内容, 要求路由器做昂贵的线速计算, 这最终会耗尽路由器资源, 对其它用户服务产生影响。

对策: 当负载变的太高, 停止验证签名(路由器对内容数据的签名验证在 CCN 中是可选项)。另外, 签名验证可以被延迟, 直到处理能力足够时再进行。

风险: 低。攻击可以被检测到, 因为其需要一个共谋的内容源和潜在的大量攻击流量。

(5) 通过泛洪兴趣包对路由器 PIT 进行攻击

攻击方式: CCN 路由器需要在内存中保留 PIT, 包含每个已经收到并转发, 但没有收到应答的兴趣包。通过请求大量不同的、不存在的内容, 以填满 PIT, 耗尽路由器为保持通信状态而预留的内存, 这样攻击者可以降低或破坏路由器向其它用户提供服务。

然而, 高比例的没有响应的兴趣包都会被路由器检测到。因此, 攻击者可以通过勾结共谋内容源来改进攻击效果。共谋内容源对虚假兴趣包进行响应, 并在路由器的 PIT 表项即将超时时发送响应回复。这种方式将使得填满 PIT 的请求数量最小化。路由器仍然可以检测到对共谋内容源前缀的频繁访问, 因此攻击者可以使用几种不同的前缀来逃避检测。

对策: 采取先进先出策略, 放弃在 PIT 表头部的兴趣包, 而不是在尾部的。也就是说, 一个新的兴趣包始终会取代了最老的挂起的兴趣包。这使得 PIT 很难被填满。另外, 可以设计检测机制及早发现对少量名称前缀进行大量请求的行为。

风险: 高。兴趣包泛洪攻击很容易发起, 因为即使没有太多关于网络数据和拓扑的知识也可以很容易地创建不存在的名称。通过伪造不存在的内容名称, 攻击者可以针对特定的内容提供商或旨在破坏网络基础设施。不过, 这种攻击需要拥有一个僵尸网络和很大的攻击流量。

(6) 通过污染缓存降低缓存效率进行攻击

攻击方式: 通过利用广泛的路由器缓存, 攻击者不断地对某些低流行度的文件或者非法文件发送请求, 使该文件一直保留在缓存中。这种人为的大量的请求改变了缓存内容的流行度分布, 降低了缓存效率, 增加了带宽需求, 将可能导致对网络基础设

施合法请求的拒绝服务。攻击者还可以利用这种攻击方式来保留已经从原服务器删除的文件或者攻击者发布的非法内容, 使其仍可对广泛的用户可见。

对策: 为了防止非法内容的检索, 可以定义名称审查列表, 路由器不提供列表上的内容。缓存也可以被迫定期更新内容与原来的内容源。另外, 可以设计算法用于检测这种攻击。

风险: 中等。为实现相同的攻击效果, 需要较高的请求频率。同时攻击需要一个僵尸网络和大攻击流量。

(7) 通过阻止正确的内容进行攻击

攻击方式: 路由器认为有效的内容是无效的, 阻止其通过, 然后反馈给用户“请求的内容不存在”。

对策: 对内容进行签名验证, 并阻止攻击者非法控制网络中间路由器, 加强路由器接入控制管理。

风险: 低。攻击者需要非法入侵控制大量网络路由器。

(8) 通过编造虚假的内容进行攻击

攻击方式: 攻击者可以通过以下三种方式编造虚假内容来欺骗用户。一种是任意产生没有签名的内容, 该内容的有效性无法得到验证; 另外一种是利用假的密钥产生内容, 再将假的密钥发给用户, 使其相信内容有效; 最后一种是利用已经过期的密钥或者窃取密钥来生成内容。

对策: 强制要求内容进行签名验证, 并加强密钥分发和管理。

风险: 低。攻击者需要窃取或伪造密钥, 难度较大。

表 3 CCN 中新型 DoS 攻击对比

名称	攻击对象	攻击方式	影响范围	对策	风险
泛洪兴趣包	内容源	泛洪大量虚假兴趣包	内容源中间节点	PIT过期兴趣包检测	中等
利用兴趣包特殊位	内容源	利用兴趣包特殊位, 使兴趣无法在中间节点满足	内容源	限制使用兴趣包的特殊选项	低
干扰路由选项	中间节点的路由选项	控制路由器, 对指定的兴趣包或者数据包不转发或错误转发	中间节点	阻止攻击者控制路由器	低
强制计算	中间节点计算资源	联合恶意内容源强制中间路由节点进行签名验证	中间节点链路带宽	停止或推迟签名验证	低
PIT溢出	中间节点的PIT	泛洪大量虚假兴趣包, 或与共谋内容源合作填满中间节点PIT	内容源中间节点链路带宽	PIT先进先出策略; 设计高效的检测机制	高
缓存污染	中间节点的CS	攻击者不断地对某些低流行度的文件或者非法文件发送请求	中间节点链路带宽	定义名称审查列表; 缓存被迫定期更新内容与原来的内容源	中等
阻止正确内容	内容	路由器认为有效的内容是无效的, 阻止其通过	中间节点	对内容进行签名验证, 并阻止攻击者非法控制路由器	低
编造虚假内容	内容	编造虚假内容来欺骗用户	中间节点链路带宽	强制要求内容进行签名验证, 并加强密钥分发和管理	低

3.3 小结

通过上述分析可以看出, 在所有的 CCN DoS 攻击中有两种方式风险最高, 对网络影响最大: 一种是兴趣包洪泛攻击(Interest Flooding Attack, IFA), 另一种是内容/缓存污染攻击(Cache Pollution Attack, CPA)。IFA 主要是将大量兴趣报文发送至被攻击者, 造成沿途网络资源消耗, 如路由器 PIT 资源以及计算资源, 从而使请求节点的请求得不到正常回复的一种攻击方法。而 CPA 是指篡改、伪造路由器中 CS 中缓存的 Data 报文, 从而使请求者不能获得正确的数据。下面我们将就这两种典型的攻击做详细的阐述。

4 兴趣包泛洪的 DoS 攻击

CCN 网络中, 兴趣包基于 FIB 表信息进行转发, 同时兴趣包状态也将记录在 PIT 中, 用于指导后续返回的对应数据包的反向转发。即兴趣包的转发过程需占用路由器的内存资源以完成包状态记录功能。而且, 每个兴趣包或数据包的到达过程, 均触发路由器 PIT 的条目添加、删除等更新操作。另外, 若路由器 PIT 记录的兴趣包无法找到对应内容的数据包, 则该兴趣包在 PIT 中的对应条目将一直保存到 PIT 条目生存时间超时。一般而言, 该时长远大于网络的内容获取平均往返时延, 这延长了 PIT 模块对路由器资源的占用时间。因此, PIT 的引入, 在提供网络测量、回传路由等功能优势的同时, 也在一定程度上增加了路由器的工作负担, 给某些网络攻击者危害内容中心网络有了以可乘之机。

因此, 在 CCN 网络环境下, 攻击者可能会把网络节点的 PIT 作为攻击目标, 发动 DoS 攻击, 这种攻击被称作兴趣包泛洪攻击。在发动 IFA 时, 攻击者会

控制大量的僵尸机连续地发送兴趣包。当发送兴趣包的速率足够高, 其在 PIT 中添加条目的速率远远高于 PIT 中删除条目的速率时, 网络节点的 PIT 会在很短的时间内被填满, 此时正常用户的兴趣包会被直接丢弃, 无法处理, 如图 3 所示。CCN 网络的 IFA 攻击有点类似带宽消耗, 它是利用洪泛兴趣包来消耗中间路由节点存储资源、计算资源、网络带宽资源, 从而使合法兴趣包请求无法获得相应数据。

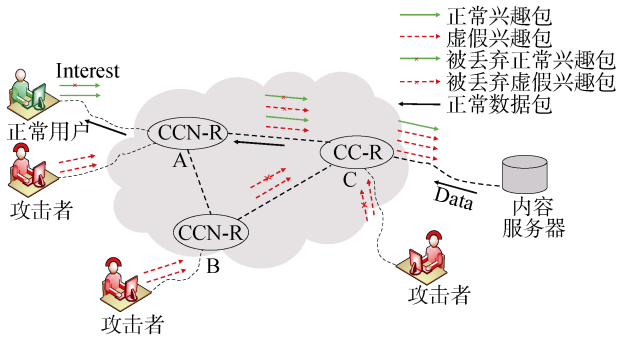

图 3 CCN 中的 IFA 攻击

IFA 这种攻击形式具有以下三个特征:

(1) 请求的内容不存在。IFA 希望其发送的攻击兴趣包能够在网络节点的 PIT 中添加条目, 并使条目在 PIT 中滞留尽可能长的时间。攻击者需要构造内容并不存在的虚假兴趣包, 因为这样 PIT 中的条目不会得到任何内容包的响应, 会在 PIT 中滞留到超时才被删除。需要注意的是, 伪造的虚假兴趣包需要拥有正确的数据源前缀, 否则该兴趣包可能因为无法在 FIB 中找到路由匹配项而被直接丢弃。

(2) 高速率发包。IFA 要在短时间内充满网络上的 PIT, 需要高速率发送大量的兴趣包, 以保证 PIT 中添加表项的速率远远高于 PIT 中因超时而删除表项的速率。

(3) 分布式攻击。为避免个别攻击者过高速率的发送兴趣包而被网络抑制, 在 IFA 中, 必然会采用分布式的大量僵尸机同时向网络发起进攻, 分布式攻击是 IFA 的一大特征。

只有同时具备以上三个特征, 才能对 CCN 网络产生攻击影响, 不管缺少哪个特征, 都不可能达到很好的攻击效果。

4.1 IFA 分类

4.1.1 按攻击对象分类

如前所述, 按照攻击对象的不同, IFA 可以分成: (1)对内容源的攻击和(2)对中间节点 PIT 的攻击。在对内容源攻击的同时, 往往会首先对中间节点造成攻击。一个好的 CCN 网络防御体系应该在内容源检测到 IFA 之前, 中间路由器的 PIT 已经检测到攻击。因此通过采取相应的检测防御措施, CCN 力图在攻击到达内容源之前被抑制。所以对中间节点 PIT 攻击对策的研究成为 CCN 网络中 IFA 攻击的关注热点。

4.1.2 按请求的内容是否真实存在分类

根据攻击兴趣包所请求的内容是否真实存在, 将 IFA 分成三种攻击类型[15]: (1)请求的是静态真实内容数据; (2)请求的是动态真实内容数据; (3)请求的是不存在的内容数据。第(1)和第(3)种攻击类型攻击的主要目标是网络的基础设施, 第(2)种攻击类型除了能够攻击网络之外, 还可以对数据源产生攻击。

第(1)种对真实存在的内容数据的 IFA 攻击效果并不明显, 因为 CCN 网络中间节点自身的缓存机制的作用。在进行该种类型的攻击时, 攻击者第一次发送兴趣包, 可能会造成 PIT 的波动, 但在之后发送兴趣包时, 就近的网络节点会使用缓存中的数据直接进行回复, PIT 不再会添加新的条目。

第(2)种攻击, 由于请求的是实时的动态真实数据, 是无法从网络节点的缓存中直接得到回复的, 因此这种攻击的兴趣包会到达内容源, 从而消耗带宽和网络节点的 PIT 资源, 并同时对内容源产生攻击。

对于这类攻击, CCN 网络中间节点的 PIT 汇聚机制可以有效的减少网络的带宽和 PIT 资源的消耗。因为当节点收到请求同样的数据名时, 节点会检查该数据名是否存在 PIT 中。若存在, 说明该节点已经转发过请求该数据名的兴趣包, 且该兴趣包暂时未得到回复, 节点将添加接收该兴趣包的端口到相应 PIT 项的入端口列表, 以便收到数据报文时回复用。因此, 该类兴趣包也不能对网络造成多少影响, 属于正常的请求流量, 对 PIT 资源消耗有限。当然, 这种攻击对 CCN 网络节点的影响程度和节点到数据源的距离相关, 距离数据源越近的网络节点的 PIT 收到的攻击影响也越大。

另外, 第(2)种攻击对内容源产生一定的影响。因为内容数据是需要数字签名和加密的, 数据源在对每一个请求的数据包进行加密处理时, 其自身的资源消耗和代价很高。这种攻击造成的直接结果是内容源超负荷, 无法再为其它正常用户的请求提供服务。然而, 如果网络带宽足够大, 数据源的处理能力足够高, 数据生成能力足够强, 能够快速响应并回复内容数据, 那么其攻击效果便会大打折扣。

第(3)种攻击中, 攻击者所发送的兴趣包不可能得到数据回复, 因为其请求的是实际上并不存在的内容。这种兴趣包不会被网络节点丢弃, 反而会被转发到数据源。当数据源发现请求的内容不存在时会

直接将兴趣包丢弃, 而不会产生过多的负载。但网络节点中的 PIT 会一直记录这些兴趣包请求的条目, 直到定时器超时将条目删除。网络节点是这种攻击的首要对象, 也是受影响最大的受害者。因此, 当大量请求任意伪造的数据名的 兴趣包到达时, 节点的 PIT 资源将耗尽。除此之外, 正如其它洪泛攻击一样, 同时将消耗节点的计算资源, 网络带宽资源。

这类攻击的特点为: (1)针对某一特定内容名字前缀; (2)使用携带虚假名字的恶意兴趣包进行网络泛洪。前者保证了攻击流量的高度聚合; 而后者最大程度地减少了恶意兴趣包流量由于网络缓存命中而被削减的程度, 从而使得攻击流量可被路由到网络深处, 大量占用沿途路由器的PIT内存资源, 对CCN网络造成严重的危害。这种类型的攻击易于发动且易造成严重的危害效果, 成为 CCN 网络中 IFA 攻击的主流类型。

4.2 IFA 检测方法

IFA 作为 CCN 网络架构的主流安全威胁之一, 有关其检测策略的研究也成为了网络安全领域的研究热点。经过上述分析, 本节将主要对请求的是不存在的内容数据的虚假兴趣包泛洪攻击的检测方法展开讨论。

4.2.1 基于 PIT 异常状态的统计量

一种常用的方法是基于 PIT 异常状态的统计。因为 CCN 网络中间节点的 PIT 为每一个收到的兴趣包保留一个状态, 并且为每一个转发的数据包动态的删除一个 PIT 表项。该机制特性使 CCN 节点具有一定统计功能, 因此, 可以通过 PIT 状态的变化作相应统计。统计的粒度可以是基于整个 PIT 空间的统计, 基于端口的统计, 甚至是基于数据名的统计。根据这些统计信息, CCN 中间节点可以做出 IFA 攻击判断。可用来做攻击检测的统计量如下:

(1) PIT size。指某一时刻节点整个 PIT 空间所有条目的数量[14]。在正常情况下, PIT size 会稳定在一个值附近, 该值与用户的发包速率和链路带宽时延积相关, 波动范围不大。当遭受 IFA 攻击时, PIT size 会在短时间迅速上升。所以可以通过设定其阈值来检测 IFA。

(2) PIT 占用率。与 PIT size 类似, 反映节点 PIT 的空间使用情况。其值等于 PIT size 与 PIT 空间最大值之间的比值[43-44]。当该值超过警戒阈值时, 可以判断 IFA 发生。

(3) 兴趣包满足率。指某段统计周期内, 节点/每个接口发出的数据包与节点/每个接口收到的兴趣包的比值[14,45]。正常情况下, 在网络达到稳态的是, 该值应该是近似 1 的一个值, 这样 PIT size 也会维持在一个稳定的范围内。故可以通过该比值的异常变化来判断 IFA 攻击的发生。

(4) PIT 过期条目数量。指某段统计周期内, 节点 PIT 空间中由于生存时间超时而过期被删除的条目数量总和[46]。在正常的网络状态下, PIT 过期条目数量应该比较小, 在网络发生拥塞是会相应增多。但该值在短时间内突然的增加应该考虑 IFA 攻击发生。

(5) PIT 过期率。与 PIT 过期条目数目类似, 反映节点 PIT 过期条目数量占比的大小。其值等于某段统计周期内, PIT 过期条目数量与 PIT size 的比值[43]。

4.2.2 基于 CCN 流平衡原理

可以根据 CCN 流平衡原理来检测 IFA 攻击[15]。CCN 网络传输机制维持兴趣包和数据包的一种内在平衡。即每向上游发送一个兴趣包, 最多只会产生一个数据包向下游回复。因此, 可以依据下面三个值来判断 IFA 攻击发生:

(1) 每个出口发出的还未收到回复的兴趣包数量(pending interest, PI)。根据流平衡原理, 每个路由器可以根据每个接口下游连接在超时之前所能接受的数据的能力, 来决定每个出口的最大 PI 数量。该值与平均的内容包大小、PIT 条目的生命期以及链路的带宽延迟积相关。如果 PI 远远超过上限, 则可以认为发生 IFA 攻击。

(2) 每个入口的兴趣包数量。根据相同的流平衡原理, 路由器可以很容易地探测到其下游节点发送太多的超出其链路处理能力的兴趣包, 可以认为 IFA 攻击发生, 因此将拒绝接收过多的兴趣包。

(3) 每个命名空间的 PI 数量。当某一个命名前缀空间受到攻击时, 中间路由器会检测到其 PIT 空间中该前缀空间大量过期兴趣包。因此路由器可以通过限制发往该前缀空间的 PI 数量来抑制攻击。

4.2.3 基于流量行为特征

近年来的大量研究表明, 网络流量都具有明显的突发性和长相关性[47], 而网络的自相似性特性可以很好地描述流量这些特性, 所以, 自相似性已成为网络流量的重要特性并以此作为流量异常检测的基础。现今已有大量计算机学科领域的算法和模型被使用在网络流量的异常检测方面, 信息熵[48]作为系统有序化程度的一个度量, 能检测出 DoS 攻击对于正常网络流量随机性所产生的影响; 文献[49]采用小波分析方法利用网络流量在时间尺度上的多重分形, 在小波域内对网络流量进行分解, 通过计算网络流量的Hurst 指数, 根据正常与异常流量Hurst 指数的偏差来检测异常; 文献[50]提出了基于 Trie 树

的 HHH 检测方法, 并通过剪枝重构来减少算法执行时间; 文献[51]采用 SVM 支持向量机的方法来进行流量异常检测; 文献[52]提出一种融合 k-means 的聚类检测算法, 该文增量地构建流量矩阵, 增量地使用 PCA 主成分进行异常检测。

目前, 还没有任何研究使用上述方法对 CCN 网络中的流量异常进行检测分析, 这些方法对 CCN 网络的对称流量模型是否有效也尚未可知, 这些或许可以成为 IFA 攻击的研究热点和方向。

4.3 IFA 防御方法

IFA 对 CCN 网络构成了潜在的威胁, 该恶意攻击一旦发生, 对网络造成的影响将十分恶劣。目前已经有诸多相关研究, 提出了多种防御对策。IFA 的防御方法主要有以下 6 种:

(1) 基于端口的流量限制

流量限制的防御方式包括基于流平衡的方式和令牌桶的方式。前面的 4.2.2 小节讲述了基于 CCN 流平衡原理进行 IFA 检测的三种方法, CCN 路由器通过分别限制每个出口发出的 PI 数量, 每个入口的兴趣包数量和每个命名空间的 PI 数量, 可以对 IFA 进行抑制, 这里就不再赘述。下面介绍一下令牌桶限流机制。

Alexander 教授及其团队成员提出了基于端口流量限制的 IFA 攻击防御方式[45]。这种方式是对令牌桶算法的改进—token bucket with per interface fairness 算法。该算法主要是使每个出端口都有相应的限制值, 当每个端口发出的兴趣包超出了该限值, 这些报文将在队列中挂起。当允许发出报文的时候, 从入端口的队列中均等地将接受的报文转发出去。在这一方案中, 通过某个接口转发出去的令牌能够平均分配给其它接口。

这种方案虽然在一定程度上能够丢弃掉一些恶意攻击包, 但同时也放行了很多的恶意攻击包, 甚至有可能丢弃一些正常的请求包。因为该方案只关注如何平均分配令牌的问题, 并没有真正的检测和区分出哪个数据包是正常包, 哪个数据包是攻击包。

(2) 恶意前缀判别

IFA 防御的核心问题是如何从大量的兴趣包中判别出攻击包和正常包。一种常用的判别方法是分别统计每个命名前缀空间的兴趣包满足率或者 PIT 过期率。具体统计方法详见 4.2.1 小节。通过设定阈值或者将统计值排名靠前的命名前缀认为是恶意的前缀, 然后采取相应的抑制措施。

这种方法虽然可以检测出恶意前缀, 但同时也会造成误判从而伤害合法用户。当网络拥塞或者发生攻击时, 靠近内容源的路由器首先会因 PIT 溢出而丢弃后来的兴趣包, 包括合法的和恶意的兴趣包, 那么在网络边缘的路由器上的 PIT 中合法兴趣包也因为上游的丢弃而超时, 所以合法兴趣包的满足率和 PIT 过期率也会超过阈值, 被判定为恶意兴趣包而遭到抑制。另外, 即使是恶意兴趣包, 也往往会使用合法的前缀加伪造的内容名称, 因为攻击者一般是为了攻击某个网站域名, 只有使用合法的前缀才能到达数据源。如果攻击者是为了攻击网络路由器上的 PIT, 也往往选择使用合法的前缀加伪造的内容名称, 因为伪造的前缀会由于无法在路由器 FIB 表上找到匹配项而被丢弃, 达不到攻击的目的。因此, 攻击者使用合法前缀展开攻击会导致发出该前缀的合法用户被误认为攻击者。

(3) 邻居通告

CCN 路由器判别出恶意前缀后, 可以采取向相邻路由器发送反馈包的方式, 限制该前缀兴趣包的转发速率[14,44,46]。当路由器收到协同防御包时, 提取出异常名称前缀, 采用类似 TCP 中拥塞避免机制, 即基于和式增加积式减少(Additive Increase Multiplicative Decrease, AIMD)的方法限制携带异常名称前缀的兴趣包转发速率。即使恶意用户不理睬协同防御包, 其它路由器也会限制异常前缀兴趣包的转发速率, 而网络中其它合法兴趣包传输速率不受影响。

(4) Push back

当 CCN 节点根据上述数据统计方法, 检测到恶意前缀, 路由器就会抑制该前缀兴趣包的转发。由于兴趣包中不像 IP 数据包那样包含源地址信息, 也不包含数字签名信息, 因此在发生攻击时, 无法及时地判定攻击源。但是, CCN 基于 PIT 的对称回传路由机制使得逐跳溯源变得容易实现且不可抵赖。所以, CCN 节点可以将抑制信息反馈给上一跳节点, 加速上一跳节点的同步。这样沿着上一跳节点逐层反馈直到攻击源头。

CCN 节点可以构造一条抑制信息, 逐跳向攻击源头传递抑制信息。更为巧妙地做法是伪造数据包溯源, 这样就不需要定义额外的数据格式和通信流程。文献[13]提出了这种“兴趣包回溯(Interest traceback)”机制, 在判定出恶意前缀后, 路由器通过伪造数据包并回复恶意兴趣包请求, 使路由器 PIT 中的非法条目因收到“对应数据包”而被满足, 并最终反向定位到接入路由器, 从而在接入路由器入口处限制 IFA 恶意兴趣包的准入速率。

(5) 兴趣包认证

IFA 攻击的产生的部分原因是由于路由器缺乏对兴趣包的验证。所以通过强制中间路由器对兴趣

包签名验证可以解决这一问题。然而, 这会引发隐私问题[42], 并将引入一种新的 DoS 攻击——通过强制计算对路由器进行攻击(见 3.1 小节中的讨论)。

(6) SDN 方式

软件定义网络(Software Defined Network, SDN), 是由美国斯坦福大学 clean slate 研究组提出的一种新型网络创新架构, 其核心技术 OpenFlow 通过将网络设备控制面与数据面分离开来, 从而实现了网络流量的灵活控制, 为核心网络及应用的创新提供了良好的平台。SDN 的网络控制器拥有全网视图, 可以快速准确的搜集全网监控节点的兴趣包信息, 因此可以及时发现网络异常攻击流量, 能够避免重复检测和过分响应, 快速抑制攻击源并保护合法用户[53-54]。但是, SDN 的集中控制思想与 CCN 纯分布式逻辑相违背, 如何将二者融合是需要重点考虑的问题。另外 SDN 的控制器本身容易成为 DoS 攻击的对象, 需要考虑如何避免单点失效问题。

4.4 挑战

尽管目前有很多针对 CCN 网络中 IFA 攻击的研究, 但 IFA 的检测和防御还面临着诸多的挑战。

(1) 过分依赖检测阈值

4.2 小节中讲述的大部分 IFA 检测方法都使用阈值进行判断, 但没有一个能够可靠地给出阈值是如何设置的。一个不合理的阈值将导致频繁误判从而引发错误的响应。例如, 就 PIT 过期率来说, 过高的阈值将导致检测迟缓, 网络攻击已经造成很大的破坏后才检测到攻击; 而过低的阈值会导致网络过分响应, 无法区分网络正常流量波动和 IFA 攻击。

(2) 节点间协作

节点间协作有助于 IFA 攻击的检测和防御, 但同时也带来了很多安全隐患。

所谓协作检测, 是指各个 CCN 网络节点之间传递控制信息, 通过合作机制来判定攻击行为。在进行攻击期间, 被攻击目标和距离目标较近的网络节点能够通过 PIT 占用率等参数直接判断是否遭受了 IFA, 但是在攻击路径上距离目标较远的网络节点却很难确定目前是否受到 IFA 攻击。而网络节点之间的合作检测机制能够在网络节点之间传递检测信息, 更快更准确地判定 IFA。合作检测机制同时还可以在网络节点之间传输攻击的特征信息, 通过多个网络节点之间的信息反馈选择最优的攻击响应方案。

协作防御机制主要是指 4.3 小节中讲述的邻居通告和 push back 机制。网络节点通过协作方式限制恶意前缀兴趣包的转发, 并通过逐跳溯源来抑制攻击源。

但是, 大多数的节点间协作方案需要路由器之间彼此依赖。因此, 当路由器被攻击者控制时, 它可以给邻居发送虚假通知来破坏正常的网络通信。然后这些邻居也可以将这些假消息传播给网络中的其它路由器以造成更为严重的影响。因此, 节点结协作方案要审慎使用。

(3) 对合法用户的伤害

基于端口的流量限制和恶意前缀判别会造成对合法用户的伤害。

只按接口限制兴趣包速率, 不区别正常兴趣包和恶意兴趣包, 会导致合法用户发送正常兴趣包的传输速率也将受到限制(这部分的详细分析可参见 4.3 小节)。因此在设计 IFA 防御措施时要充分考虑合法用户的请求不受影响。

(4) 应对突发流

网络中时常会出现流量波动, 因此一个鲁棒的 IFA 检测和防御措施需要能够区分网络突发流和 IFA 攻击流。即 IFA 的检测方式要可以抵御突发流的干扰。尤其在使用阈值来判断的 IFA 检测方案时, 其阈值的设定更需要谨慎合理。

(5) 及时发现且避免过分响应

一个好的 IFA 检测机制需要在攻击发起的初期就能发现攻击, 避免其对网络造成大的伤害。但同时, 又要避免过分响应, 将网络的常规波动误认为攻击, 而影响合法用户的服务。

(6) 开销小

最后, IFA 检测和防御机制要尽量减小网络的额外开销, 尽量避免定义新的包格式和通信流程。

4.5 分析与比较

根据上述对 IFA 攻击检测与防御方法的分类描述和对这些方法面临的挑战的分析, 我们给出了目前各种 IFA 攻击检测与防御方法对比, 详见表 4。

5 缓存污染的 DoS 攻击

对于 CCN 而言, 其实现高效内容检索的主要创新之处是采用广泛节点内嵌泛在缓存的做法机制, 每个 CCN 节点都带有缓存空间用于存储高请求频度的内容。当内容应答数据包沿着请求的反向路径进行回传时, 沿途各个节点会按照一定策略在沿途各个节点进行缓存, 当这些节点再次接收到相同内容请求时, 首先在节点缓存空间中进行检索, 若检索到并则直接予以回传。然而, 新型网络结构中的新特点往往会带来新的安全威胁, 普遍节点内嵌泛在缓存的做法在提高网络效率的同时也会带来新的安全问题, 例如隐私泄露、缓存污染等[42], 本节主要针对 CCN 中的缓存污染问题展开讨论。

表 4　IFA 攻击检测与防御方法对比

方案	IFA 检测		IFA 防御		独立/合作	对针合法用户	开销	部署位置
	检测方法	检测位置	防御方法	区分突发流				
UMP [55]	统计假设检验理论	PIT	无	能	独立	保护	中	全网路由器
Traceback [13]	PIT 过期条目数目	PIT	Push back	不能	协作	误伤	小	全网路由器
Poseidon [14]	PIT size; 每接口兴趣包与发出数据包的比例	PIT 出口	接口限速 邻居通告	能	协作	保护	小	全网路由器
DoS & DDoS [15]	每个出口 PI 数量; 入口兴趣包数量; 名字空间 PI 数量	出口 入口 PIT	Push back	不能	协作	误伤	小	全网路由器
Token Bucket [45]	兴趣包满足率	出口	接口限速 Push-back	能	协作	误伤	中	全网路由器
Tang [56]	相对强度系数 RSI: 兴趣包/(兴趣包+数据包)	出口 入口 PIT	-	能	协作	保护	小	全网路由器
Three phases [56]	PIT 过期条目数目	PIT	接口限速 邻居通告	能	协作	减小误伤	中	边缘路由器
SDN [53-54]	监控路由器上的 PIT size	监控路由器	SDN 流调控	能	独立	保护	大	监控路由器中央控制器
DPE [43]	PIT 过期条目数目	PIT	将恶意前缀与 PIT 解耦	能	协作	保护	大	全网路由器
AIMD [44]	PIT 占用率; 兴趣包满足率	PIT	接口限速 邻居通告	不能	协作	误伤	中	全网路由器

缓存污染攻击(Cache Pollution Attack, CPA)是指攻击者通过利用广泛的路由器的缓存, 攻击者不断地对某些低流行度的文件或者非法文件发送请求, 使该文件一直保留在途经路由器的缓存中, 达到人为降低节点缓存中用户关注流行内容的存储比例, 降低节点的请求命中率, 增加内容获取时延的目的。CPA 攻击在影响路由节点造成严重危害的同时, 也使内容请求者与提供者双方都受到影响, 相当于对请求者与提供者同时进行了攻击, 并且使人们对 CCN 的可行性和高效性产生质疑。

CCN 中的 CPA 攻击实际上是一种拒绝服务攻击, 它比传统网络中的 DoS 攻击更加灵活, 更有挑战, 危害更大。首先, 缓存污染攻击具有隐蔽的特点, 它不需要使用洪泛的方式来攻击数据源, 关闭服务器也无法阻止非法内容驻留缓存。其次, 该攻击方式可以请求真实存在的非流行内容, 而不是只请求虚假内容来污染缓存, 与 IFA 攻击相比更加难以检测。最后, 目前互联网高速缓存还没有高效的反污染机制方案可以用来借鉴, 所以即使是简单的、蛮力的污染攻击也可以相当成功。因此迫切地需要研究 CCN 网络架构中 CPA 攻击的实施方式以及应对措施, 以保证网络服务的高效性以及安全性。

5.1　CPA 分类

CCN 中 CPA 攻击主要分为以下两类[17]: (1)破坏内容分布特性的攻击(Locality-disruption Attack, LDA), 攻击者通过恶意请求大量低流行度的合法内容, 提高了污染内容的流行度, 破坏内容的整体分布特征, 使低流行度内容尽可能长的驻留于缓存之中, 达到降低缓存效率的目的; (2) 伪造内容分布特性的攻击(False-locality Attack, FLA), 攻击者针对某一类流行度内容或者非法内容发送恶意请求, 并且周期性地对这些内容进行请求, 请求的频率应当保证不破坏内容的流行度分布规律(例如 Zipf 分布), 以此来构造虚假的内容请求规律, 保证污染内容长期占据网络节点缓存而不被发现。这两种攻击手段, 前者平滑了到达节点的内容请求分布, 后者锐化了到达节点的内容请求分布。通常网络提供内容总量远大于单个节点缓存, 因此该类攻击对 CCN 边缘与内部节点均会产生较大影响。

5.2　CPA 检测方法

针对 CPA 两种类型的攻击, 目前的检测方法主要是围绕对兴趣包和内容包的检测展开的, 下面将分别介绍。

5.2.1 对兴趣包的检测

对兴趣包的检测可以分为以下 4 种:

(1) 重复请求比率

一般情况下, 通过跟踪来自某用户的重复请求比率可以判断 FLA 攻击行为[16-17]。因为在 FLA 攻击中, 攻击者总是要通过重复请求来保证污染内容(非流行)长期占据网络节点缓存。但由于 CCN 中的请求并不携带用户地址, 只能在 CCN 的边缘路由器进行统计, 而且这种方法不适用于检测 LDA。

(2) 命中率

正常情况下, 在网络达到稳态时, 网络中的缓存命中率也会相应的达到稳定值, 波动范围不大。当发生 LDA 和 FLA 攻击时, 网络节点缓存的命中率会出现比较明显的变化。因此, 可以根据缓存节点命中率的变化来检测 CPA 攻击。当缓存命中率明显上升时, 则遭受 FLA 攻击的可能性较大; 当缓存命中率明显下降时, 则遭受 LDA 攻击的可能性较大[16-17]。但是, 当两种攻击同时发生时, 这种检测方法将失效。

(3) 兴趣包分布变化

虽然存在 LDA 和 FLA 两种攻击方式, 但究其机理, 不难发现, 其本质都是到达 CCN 节点的兴趣包请求分布出现异常, 进而改变缓存中存储内容的分布, 以达到攻击目的。正常情况下, CCN 节点接收的兴趣包请求通常设定服从某种分布(比如 Zipf), 出现 LDA 攻击时, 兴趣包请求分布变的平坦; 出现 FLA 攻击时, 兴趣包请求分布在被攻击处变的锐化。因此, 可以通过检测各内容请求规律的变化来判断攻击是否发生。有多种方式可以用来检测请求内容的分布变化。

文献[57]提出一种轻量级的检测机制, 首先进行请求兴趣包分布抽样, 然后动态统计兴趣包的分布波动, 同时根据抽样分布动态计算判决门限, 若波动大于门限则判断出现攻击。该算法计算复杂度较低, 更易于实现。

文献[58]提出了一种基于随机内容请求的检测机制, 通过将到达的请求内容名映射为某一矩阵位置, 在该位置记录此内容的请求数量。当矩阵秩降至门限以下, 判断出现攻击。该方法不依赖内容请求的源地址, 可适用于 CCN, 但运算量过大。文献[59]使用 Flajolet-Martin 算法捕捉兴趣包流的特征来鉴别攻击的产生。该方法具有开销小性能好的特点。文献[60]使用模糊神经推理的方法, 从输入输出的对应关系推断出 CPA 攻击的形式, 并且采取具体的缓存替换算法现在内容存储。

虽然这些检测与防御方法针对其各自设定的场景时效果显著, 但是在面对分布式或逐渐增强的攻击时却效果不明显, 因为无法检测到内容分布特性的突变, 则无法判断攻击是否发生。

(4) 兴趣包中的 Exclude 字段

文献[38]提出了一种按照内容排名的顺序进行缓存决策的 CPA 防御方法, 其中内容被“Exclude”标记的时间和次数会影响到内容的排名。具体的做法是当用户收到内容并通过签名验证发现虚假内容后, 发出一个新的兴趣包, 将其中的“Exclude”字段填上虚假内容的名字, 这样网络路由器会记录这个名字并进行排序, 使其难以再驻留到节点缓存中。该方法只可以用来检测虚假内容的 FLA 攻击。

5.2.2 对数据包的检测

对数据包的检测可以分为以下 3 种:

(1) 内容的生命期

正常情况下, 在网络达到稳态时, 网络中节点缓存的内容平均存活时间也会相应的达到稳定值, 波动范围不大。出现 LDA 攻击时, 内容平均存活时间变短, 出现 FLA 攻击时, 内容平均存活时间变长[16-17]。因此, 可以根据缓存节点内容平均存活时间的变化来检测 CPA 攻击。

(2) 缓存内容存储分布变化

CPA 攻击的本质都是改变 CCN 缓存中内容的分布, 以达到攻击目的。这种检测方法和前面“兴趣包分布变化”检测方法机理类似, 这里就不再赘述。

(3) 签名验证

要求 CCN 路由器对收到的数据包进行签名验证可以检测出基于非法内容的 FLA 攻击, 但由于签名验证的线速要求, 将大大增加路由器的负荷, 引发新的攻击——“通过强制计算对路由器进行攻击”, 参见前文 3.2 小节的详细介绍。

5.3 CPA 防御方法

目前, 关于 CCN 中 CPA 的研究工作主要集中在检测问题, 对于如何防御, 可查文献并不多。由于一些 CPA 防御方法与 IFA 的防御方法相类似, 这里对以下几种 CPA 防御方法做一简要介绍。

(1) 设置存储阈值限制内容缓存

目前主流 CPA 防御方法是设置缓存的存储阈值, 即根据设定的概率决定是否将获取内容存入缓存。已有策略主要是文献[18]提出的 CacheShield, 该策略根据目标内容的请求次数以及经验参数(内容平均请求次数估计值以及概率调节参数)确定存储概率, 避免缓存流行度小于所设定阈值的内容, 从而降低污染内容进入缓存的概率。

但是该策略不能防御 FLA 攻击, 仅对 LDA 一定

的抑制作用, 且效果不甚理想。而当攻击请求较多时, 该方法的防御效果也会明显下降。

(2) 缓存策略

缓存策略包括放置策略和替换策略。放置策略是指决定什么内容要缓存在哪个节点上。而替换策略是指在缓存空间全部占满的情况下, 再有新的内容到来需要缓存时, 替换哪个已有的缓存内容。CCN 中可以采取不同的缓存策略来抵制 CPA 攻击。其策略的本质还是通过限制内容缓存来达到预防 CPA 攻击的目的。文献[61]对不同的业务分类并采取不同的缓存策略, 通过不同内容的差异性缓存来限制攻击的影响范围。

(3) 邻居通告

与 IFA 攻击防御中的邻居通告方法机理类似, CCN 用户或者路由器通过签名验证发现非法数据包后, 可以采取向相邻路由器发送反馈包, 限制该非法数据包的缓存。文献[38]的通告方式是用户发出一个新的兴趣包, 将其中的“Exclude”字段填上虚假内容的名字, 用来提醒其它节点不要缓存该内容。这种防御方式只对 FLA 攻击有效。

(4) Push back

同理, 当 CCN 节点根据签名验证等方式检测到异常前缀, 路由器就会抑制该前缀兴趣包的转发。CCN 节点可以将抑制信息逐跳溯源到攻击源头, 从根本上抑制攻击的产生。其具体防御方式可以参考 4.3 小节。这种防御方式也只对 FLA 攻击有效。

(5) 自验证请求和内容

文献[15]中指出, 通过引入自验证请求和内容机制(Self-certifying Interest/Content), CCN 路由器可以判定某个给定的内容是否是某个特定的请求的“正确答案”。这里需要解决 CCN 中人类可读的命名(Human-readable Naming)向自验证命名转换的问题, 具体可以通过在兴趣包和数据包中的名字后加入 hash 值来解决。

5.4 挑战

总结现有的 CPA 攻击检测和防御手段, 可以发现这些方案仍然面临诸多问题和挑战。

(1) 缓存决策的影响

CCN 中的 CPA 攻击是基于网络普遍缓存的特性才得以实施的, 缓存策略无疑会对攻击形态以及防御手段产生巨大影响[18]。现有解决思路仅仅通过设计攻击检测算法等方式对缓存污染攻击进行拦截, 忽略了缓存决策的作用。此外, 随着未来各类缓存决策算法的增多, 当前的防御手段覆盖面将会更加有限[61]。缓存替换算法在缓存污染攻击分析中也起着重要的作用。文献[17]观察到恶意用户对高速缓存污染的影响, 过度依赖于所使用的替换算法。

(2) 多种攻击同时进行

现有方法多是设定一种具体攻击的场景, 进而采取相应的攻击检测或者防御手段。虽然针对其预设场景优化较好, 但面对更加复杂的网络环境中多种攻击类型并存的情况则显得性能不佳甚至难以取得效果, 导致了网络资源的浪费。一个高效的检测和防御手段要能够有效针对多种攻击同时发生的场景。

(3) 缓存节点众多带来的复杂性

CCN 网络中 CPA 攻击与单一缓存服务器遭受攻击有着很大的不同。例如, 在一个给定的路径上的攻击可能导致其它不在该路径上的 CCN 路由器受到影响。与内容分发网络(CDN)不同(缓存放置在离用户近的地方, 减少骨干网络拥塞), CCN 节点将普遍采取增量部署, 并逐渐成长为复杂的拓扑结构。由于可以在网络中任何位置进行内容请求的汇聚和分裂, 使得在 CPA 攻击下 CCN 的缓存行为和性能很难预测[18]。

目前 CPA 攻击研究更多的关注单一的孤立节点, 而对于 CCN 这种泛在的网络化内嵌缓存研究并不多, 其中一个缓存节点遭到攻击对其它缓存节点的影响还未可知。

(4) 主动与被动策略

CPA 的检测和防御中, 主动策略是指实时运行的, 避免攻击发生的策略, 即在此策略下攻击无法产生实质影响。比如, CacheShield[18]策略, 攻击内容无法直接注入缓存。而被动策略并不一定实时运行, 是在攻击发生后, 已经产生了一定的影响才检测到的攻击产生, 再采取防御措施, 而此时网络已经受到了影响。

主动策略虽然比被动策略更能及时检测到攻击和抑制攻击影响, 但是主动策略往往需要实时运行, 给网络带来了较重的负荷, 而且由于限制苛刻, 往往会因为过度反应而对合法用户请求的内容造成影响。

(5) 节点间协作

如 4.4 小节所述, 节点间协作的 CPA 的检测和防御方法是一把双刃剑, 既能带来好处也会引发隐患。在设计具体的策略时, 要充分考虑节点间协作的利弊。

(6) 开销小

最后, CPA 检测和防御机制要尽量简单且易于实现, 要减小网络的额外开销, 要与 CCN 已有协议兼容尽量避免定义新的包格式和通信流程。

5.5 分析与比较

根据上述对 CPA 攻击检测与防御方法的分类描述和对这些方法面临的挑战的分析, 我们给出了目前各种 CPA 攻击检测与防御方法对比, 详见表 5。

表 5　CPA 攻击检测与防御方法对比

方案	CPA检测			CPA防御		被动/主动	适用范围	开销	部署位置
	检测方法	适用攻击	检查内容	防御方法	缓存算法的影响				
SCIC [15]	自验证请求和内容	FLA	兴趣包 数据包	自验证请求和内容	无影响	主动	全部缓存	大	边缘和核心路由器
Bloom[16-17]	重复请求; 存活时间; 命中率	FLA LDA	兴趣包 数据包	-	使用各种替换算法	被动	单个缓存	小	边缘路由器
CacheShield[18]	请求次数	LDA	兴趣包	设置存储阈值	本身就是缓存替换算法	主动	全部缓存	中	边缘和核心路由器
Ranking [38]	基于内容排名(新旧, exclude)	FLA	数据包	邻居通告	本身就是缓存替换算法	主动	全部缓存	中	边缘和核心路由器
Lightweight[57]	请求包的分布变化, 抽样值	LDA	兴趣包	-	LRU效果好 LFU不好	被动	全部缓存	小	边缘和核心路由器
Random [58]	请求包的分布变化, 矩阵的秩	LDA	兴趣包	-	无影响	被动	单个缓存	大	核心路由器
ELDA [59]	请求分布变化, LFM	FLA LDA	兴趣包	-	只分析了LRU	被动	全部缓存	小	边缘和核心路由器
ANFIS [60]	神经模糊推理	FLA LDA	数据包	缓存替换算法	本身就是缓存替换算法	被动	全部缓存	大	边缘和核心路由器
CPADS [61]	基于兴趣包特征分布; 数据包到达速率	FLA LDA	兴趣包 数据包	区分业务; 边缘缓存渐进缓存	不同的缓存策略不同的防御方式	主动	全部缓存	大	边缘和核心路由器
CPDP [62]	内容存储分布; 请求分布	FLA LDA	兴趣包 数据包	设置存储阈值	本身就是缓存替换算法	被动	单个缓存	中	核心路由器

6　总结

随着互联网应用从以面向主机的端到端通信为主转向以接收者驱动的海量内容获取为主, 研究界近年来提出了多种以信息/内容为中心的新型网络体系架构, 旨在从体系架构层面支持高效可扩展的内容获取应用模式, 解决互联网面临的流量爆炸问题。在这类网络架构中, CCN 是备受关注的一个架构。CCN 在设计中已加入了一定的安全机制, 使其能够抵御目前网络存在的大多数形式的 DoS 攻击。但 CCN 在解决传统网络问题的同时, 产生了新型的 DoS 攻击。本文对近年来国际上在该领域的主要研究成果进行了回顾与总结, 分析了 CCN 网络的新型 DoS 攻击类型和特征, 综述了 CCN 网络中 DoS 若干主要问题的研究现状, 包括 IFA 攻击的检测和防御方法和 CPA 攻击的检测和防御方法等, 并进行了深入的分析对比, 同时指出可能面临的挑战。总的来说, 对 CCN 网络的 DoS 研究刚处于起步阶段, 具有广阔的研究空间, 无论在理论模型还是检测防御优化方法方面都有大量关键问题需要进行开拓性的探索和深入细致的研究。这些问题的解决和完善对于规划、设计和运营未来的 CCN 网络具有重要的理论价值和实践指导意义。

参考文献

[1] Index, C. V. N. (2015). *Forecast and Methodology, 2014-2019 White Paper*. Technical Report, Cisco.

[2] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, “A survey of Information-Centric Networking,” *Communications Magazine, IEEE*, vol. 50, no. 7, pp. 26–36, 2012.

[3] T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, and I. Stoica, “A data-oriented (and beyond) network architecture,” *ACM SIGCOMM Computer Communication Review*, vol. 37, no. 4, pp. 181–192, 2007.

[4] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, “Networking Named Content,” in *Proc. ACM CoNEXT,* pp. 1-12, 2009.

[5] S. Tarkoma, M. Ain, and K. Visala, “The publish/subscribe internet routing paradigm (PSIRP): Designing the Future Internet architecture.” in *Proc. Future Internet Assembly*, pp. 102–111, 2009.

[6] C. Dannewitz, D. Kutscher, B. Ohlman, S. Farrell, B. Ahlgren, and H. Karl, “Network of information (NetInf) - an Information-Centric Networking architecture,” *Computer Communications*, vol. 36, no. 7, pp. 721–735, 2013.

[7] S. Paul, J. Pan, and R. Jain, “Architectures for the future net-

works and the next generation Internet: A survey", *Computer Communications,* vol. 34, no. 1, pp. 2–42, 2011.

[8] J. Choi, J. Han, E. Cho, et al., "A survey on content-oriented networking for efficient content delivery", *IEEE Communications Magazine*, vol. 49, no. 3, pp. 121-127, 2011.

[9] G. Zhang, Y. Li, T. Lin, "Caching in information centric networking: A survey," *Computer Networks*, vol. 57, no.16, pp. 3128-3141, 2013.

[10] Zhang L, Jacobson V, Estrin D, et al., "Named Data Networking (NDN) Project". Technical Report, *University of California*, Los Angeles, 2014.

[11] C. Yi, A. Afanasyev, I. Moiseenko, L. Wang, B. Zhang, and L. Zhang, "A case for stateful forwarding plane," *Computer Communications*, vol. 36, no. 7, pp. 779–791, 2013.

[12] D. Perino, and M. Varvello, "A reality check for content centric networking," in *Proc. ACM SIGCOMM Workshop on Information-Centric Networking*, pp. 44-49, 2011.

[13] H. Dai, Y. Wang, J. Fan, and B. Liu, "Mitigate DDoS attacks in NDN by interest traceback," in *Proc. IEEE INFOCOM, NOMEN Workshop*, pp. 381-386, 2013.

[14] A.Compagno, M. Conti, P. Gasti, and G. Tsudik, "Poseidon: Mitigating Interest flooding DDoS attacks in Named Data Networking," in *Proc. LCN*, pp.630–638, 2013.

[15] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, "DoS and DDoS in Named Data Networking," in *Proc. IEEE International Conference on Computer Communications and Networks (ICCCN)*, pp. 1–7, 2013.

[16] Y. Gao, L. Deng, A. Kuzmanovic, and Y. Chen, "Internet cache pollution attacks and countermeasures," in *ICN*P. *IEEE Computer Society*, pp. 54–64, 2006.

[17] L. Deng, Y. Gao, Y. Chen, and A. Kuzmanovic, "Pollution attacks and defenses for Internet caching systems," *Computer Networks*, vol. 52, no. 5, pp. 935–956, 2008.

[18] M. Xie, I. Widjaja, and H. Wang, "Enhancing Cache Robustness for Content-Centric Networking", in *Proc. IEEE INFOCOM,* pp. 2426-2434, 2012.

[19] Project ccnx: http://www.ccnx.org/.

[20] A.Afanasyev, I. Moiseenko, L. Zhang et al., "ndnSIM: NDN simulator for ns-3," Technical report, *University of California*, Los Angeles, 2012.

[21] D. Smetters, and V. Jacobson, "Securing Network Content," Technical report, *Palo Alto Research Center*, 2009.

[22] E. G. AbdAllah, H. S. Hassanein, and M. Zulkernine, "A Survey of Security Attacks in Information-Centric Networking," *IEEE Communications Surveys & Tutorials*, vol.17, no. 3, pp. 1441-1454, 2015.

[23] C. Dannewitz, J. Golic, B. Ohlman, and B. Ahlgren, "Secure naming for a network of information," in *Proc. IEEE INFOCOM*, pp. 1–6, 2010.

[24] S. Arianfar, T. Koponen, B. Raghavan, and S. Shenker, "On preserving privacy in content-oriented networks," in *Proc. ACM SIGCOMM Workshop ICN*, pp. 19–24, 2011.

[25] D. L. Chaum, "Untraceable electronic mail, return addresses, digtal pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[26] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second generation onion router," in *Proc. 13th USENIX Security Symp.*, pp. 21-38, 2004.

[27] Freedom System 2.0 Architecture, https://gnunet.org/sites/ default/files/freedom2-arch.pdf

[28] Anonymizer, http://www.anonymizer.com

[29] I.Clarke, T.W. Hong, S. G. Miller, O. Sandberg, and B.Wiley, "Protecting free expression online with Freenet," *IEEE Internet Computing*, vol. 6, no. 1, pp. 40–49, 2002.

[30] M. Ion, J. Zhang, M. Schuchard, and E. M. Schooler, "Toward content centric privacy in ICN: Attribute-based encryption and routing," in *Proc. ASIA CCS*, pp. 513–514, 2013.

[31] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

[32] A.Keromytis, V. Misra, and D. Rubenstein, "SOS: An architecture for mitigating DDoS attacks," *IEEE Journal on Selected Areas in Communications,* vol. 22, no. 1, pp. 176–188, 2004.

[33] J.Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Computer Communication Review,* vol. 34, no. 2, pp. 39–53, 2004.

[34] L.Lu, M. C. Chan, and E. C. Chang, "A general model of probabilistic packet marking for IP traceback," in *Proc. ASIACCS*, pp. 179–188, 2008.

[35] E. Kline, A. Afanasyev, and P. Reiher, "Shield: DoS filtering using traffic deflecting," in *Proc. 19th IEEE ICNP*, pp. 37–42, 2011.

[36] A.Mohaisen, X. Zhang, M. Schuchard, H. Xie, and Y. Kim, "A DoS limiting network architecture," *ACM SIGCOMM Computer Communication Review*, vol. 35, no. 4, pp. 241–252, 2005.

[37] A.Mohaisen, X. Zhang, M. Schuchard, H. Xie, and Y. Kim, "Protecting access privacy of cached contents in information centric networks," in *Proc. SIGCOMM*, pp. 1001–1003, 2013.

[38] C.Ghali, G. Tsudik, and E. Uzun. "Needle in a Haystack: Mitigating Content Poisoning in Named-Data Networking," in Proc. SENT, pp.1-10, 2014.

[39] N. Fotiou, G. F. Giannis, and G. C. Polyzos, “Access control enforcement delegation for information-centric networking architectures,” in *Proc. 2nd Edition ICN Workshop*, pp. 85–90, 2012.

[40] B.Vieira and E. Poll, “A security protocol for information-centric networking in smart grids,” in *Proc. SEGS*, pp. 1–10, 2013.

[41] C.Douligeris, and A. Mitrokotsa, “DDoS attacks and defense mechanisms: classification and state-of-the-art,” *Computer Networks*, vol. 44, no. 5, pp. 643–666, 2004.

[42] T. Lauinger, “Security & scalability of Content-Centric Networking [Master’s thesis],” *TU Darmstadt*, the Netherlands, 2010.

[43] K.Wang, H. Zhou, Y. Qin, Jia Chen, and H. Zhang. “Decoupling Malicious Interests from Pending Interest Table to Mitigate Interest Flooding Attacks”. in *Proc. IEEE Globecom workshop MENS*, pp.963-968, Dec. 2013.

[44] J.Q. Tang, H.C. Zhou, Y. Liu and H.K. Zhang, “Mitigating Interest Flooding Attack Based on Prefix Identification in Content-centric Networking,” *Journal of Electronics & Information Technology*, vol.36, no. 7, pp. 1735-1742 (in Chinese), 2014.
(唐建强, 周华春, 刘颖, 张宏科“内容中心网络下基于前缀识别的兴趣包泛洪攻击防御方法”, *电子与信息学报*, 2014, 36 (7): 1735-1742。)

[45] A.Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang, “Interest flooding attack and countermeasures in Named Data Networking,” in *Proc. IEEE IFIP Networking Conference*, pp. 1–9, 2013.

[46] V. G. Vassilakis, B. A. Alohali, I. D. Moscholios, and M. D. Logothetis, “Mitigating Distributed Denial-of-Service Attacks in Named Data Networking,” in *Proc.the Eleventh Advanced International Conference on Telecommunications,* pp.18-23, 2015.

[47] X. Cheng, and K. Xie, “Network Traffic Anomaly Detection Based on Self-Similarity Using HHT and Wavelet Transform,” in *Proc. The Fifth International Conference on Information Assurance and Security*, pp. 710-713, 2009.

[48] A.Lakhina, M. Crovella, and C. Diot, “Mining anomalies using traffic feature distributions,” *Computer Communication Review*, vol. 35, no. 4, pp. 217-228, 2005.

[49] Y. Zhang, and Z. Ge, “Network anomography,” in *Proc. ACM SIGCOMM*, pp.317-330, 2005.

[50] H. Yang, and K. Du, “Identification of Anomalous Traffic Clusters for Network-Wide Anomaly Analysis,” Journal of Computer Research and Development, vol. 46, no. 11, pp. 1847-1853, 2009.

[51] H. Li, X. Guan, X. Zhan, and C. Han, “Network Intrusion Detection Based on Support Vector Machine,” *Journal of Computer Research and Development*, vol. 40, no. 6, pp. 799–807, (in Chinese), 2003.
(李辉, 管晓宏, 昝鑫, 韩崇昭“基于支持向量机的网络入侵检测”, *计算机研究与发展*, 2003, 40(6): 799-807。)

[52] Y. Qian, and M. Chen, “ODC: A method for online detecting &classifying network-wide traffic anomalies,” *Journal on Communications*, vol. 32, no. 1, pp. 111–121, (in Chinese), 2011.
(钱叶魁, 陈鸣 “ODC 在线检测和分类全网络流量异常的方法”, *通信学报*, 2011, 32(1) : 111－121。)

[53] H. Salah, J. Wulfheide, and T. Strufe, “Coordination Supports Security: A New Defence Mechanism Against Interest Flooding in NDN,” in *Proc.LCN,* pp.73-81, 2015.

[54] Salah, H., Wulfheide, J., and Strufe, T.. “Lightweight coordinated defence against interest flooding attacks in NDN,” In *Computer Communications Workshops (INFOCOM WKSHPS), 2015 IEEE Conference,* pp. 103-104, 2015.

[55] T. Nguyen, R. Cogranne, and G. Doyen, “An optimal statistical test for robust detection against interest flooding attacks in CCN,” in *Proc. IFIP/IEEE International Symposium on Integrated Network Management (IM),* pp. 252-260, 2015.

[56] J. Tang, Z. Zhang, Y. Liu, and H. Zhang, “Identifying Interest flooding in Named Data Networking,” in *Proc. IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*, pp. 306–310, 2013.

[57] M.Conti, P. Gasti and M. Teoli, “A lightweight mechanism for detection of cache pollution attacks in Named Data Networking”, *Computer Networks*, vol. 57, no. 16, pp. 3178-3191, 2013.

[58] H. Park, I. Widjaja, and H. Lee, “Detection of Cache Pollution Attacks Using Randomness Checks,” in *Proc. IEEE ICC,* pp.1096-1100, 2012.

[59] Z. Xu, B. Chen, N. Wang, Y. Zhang, and Z. Li, “ELDA: Towards Efficient and Lightweight Detection of Cache Pollution Attacks in NDN”, in *Proc. LCN*, pp.82-90, 2013.

[60] A.Karami, and G. Manel, “An ANFIS-based cache replacement method for mitigating cache pollution attacks in Named Data Networking,” *Computer Networks*, vol. 80, no. 7, pp. 51-56, 2015.

[61] L. Zheng, H. Tang, and G. Ge, “Cache pollution attack defense scheme based on cache diversification in content centric networking,” *Journal of Computer Applications*, vol. 35, no. 6, pp. 1688–1692 (in Chinese), 2015.
(郑林浩, 汤红波, 葛国栋 “内容中心网络中基于多样化存

储的缓存污染防御机制”，*计算机应用*, 2015, 35 (6): 1688-1692。)

[62] Y. Zhu, Z.K. Mi, and W.N. Wang, “Cache pollution defense technologies in content centric networking,” *Journal of Nanjing University of Posts and Telecommunications*, vol.35, no. 2, pp. 27-33 (in Chinese), 2015.
(朱轶, 糜正琨, 王文鼐“内容中心网络缓存污染防御技术研究”，*南京邮电大学学报*, 2015, 35 (2): 27-33。)

李杨 于 2009 年在韩国庆北大学电子工程专业获得工学博士学位。现任中国科学院信息工程研究所副研究员。研究领域为内容分发网络、未来网络。研究兴趣包括: 网络安全检测和防御, 网络缓存优化技术。Email: liyang@iie.ac.cn

辛永辉 于 2013 年在电子科技大学网络工程专业获得学士学位。现在中国科学院信息工程研究所信号与信息处理专业攻读博士学位。研究领域为未来网络、网络安全。研究兴趣包括: 内容中心网络安全。Email: xinyonghui@iie.ac.cn

韩言妮 于 2010 年在北京航空航天大学计算机软件与理论专业获得博士学位。现任中国科学院信息工程研究所第 5 研究室助理研究员。研究领域为 SDN 网络、虚拟资源管理调度。Email: hanyanni@iie.ac.cn。

李唯源 于 2012 年在北京交通大学通信工程专业获得学士学位。现在中国科学院信息工程研究所信号与信息处理专业攻读博士学位。研究领域为内容中心网络。研究兴趣包括: 缓存、多径转发。Email: liweiyuan@iie.ac.cn

徐震 于 2005 年在中国科学院软件研究所信息安全专业获得工学博士学位。现任中国科学院信息工程研究所正高级工程师。研究领域为网络安全与系统安全。研究兴趣包括: 云安全、可信计算、移动终端安全技术。Email: xuzhen@iie.ac.cn