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

唐建强* 周华春 刘 颖 张宏科
(北京交通大学电子信息工程学院 北京 100044)

摘 要：针对内容中心网络(Content-Centric Networking, CCN)下的兴趣包泛洪攻击问题，该文提出基于异常名称前缀识别的协同反馈防御方法。利用 CCN 中路由器维持的兴趣包转发状态检测兴趣包泛洪攻击，识别异常名称前缀，并向相邻节点发送异常名称前缀，进行协同防御。与其他方法对比分析结果表明，所提出的基于前缀识别的兴趣泛洪攻击防御方法可以准确地识别异常名称前缀，并快速抑制异常兴趣包的传输，而不影响合法兴趣包的速率。

关键词：内容中心网络；兴趣包泛洪；前缀识别；协同防御
中图分类号：TP393.03 **文献标识码**：A **文章编号**：1009-5896(2014)07-1735-08
DOI: 10.3724/SP.J.1146.2013.01770

Mitigating Interest Flooding Attack Based on Prefix Identification in Content-centric Networking

Tang Jian-qiang Zhou Hua-chun Liu Ying Zhang Hong-ke
(*School of Electronic and Information Engineering*, *Beijing Jiaotong University*, *Beijing* 100044, *China*)

Abstract: As for the interest flooding attack in Content-Centric Networking (CCN), this study proposes a new approach to mitigate interest flooding attack based on abnormal name prefix identification. This study utilizes the forwarding state in CCN routers to detect the interest flooding and identify abnormal name prefixes, and collaboratively defense the attack by sending the identified name prefixes to neighbors. Comparison between results of the proposed approach and others, the proposed approach is able to identify the abnormal name prefixes exactly, and quickly suppress malicious interest flooding without reducing the rate of normal interests.

Key words: Content-Centric Networking (CCN); Interest flooding; Prefix identification; Collaborative defense

1 引言

内容中心网络(Content-Centric Networking, CCN)[1]自提出以来受到广泛关注与认可，经过命名数据网络(Named-Data Networking, NDN)[2]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[3,4]。CCN 对内容进行命名，支持兴趣包(interest)和数据包(data)。兴趣包是内容请求包，携带内容名称等信息；数据包携带内容，用来满足兴趣包。CCN 取消了主机的地址，消除了传统 IP 网络中的源地址伪造攻击和针对特定主机的泛洪攻击。然而，CCN 在解决传统网络问题的同时，引入了新的安全威胁，即路由器需要将未被满足的兴趣包存储在等待兴趣包列表中(Pending Interest Table, PIT)。路由器为兴趣包维持转发状态的特性很容易被攻击者利用，大量恶意兴趣包就能形成兴趣包泛洪攻击，耗尽路由器的 PIT 资源，导致网络拥塞[5−7]。

因此，本文提出基于异常名称前缀识别的兴趣包泛洪攻击协同防御方法。该方法根据 PIT 使用率和兴趣包满足率检测兴趣包泛洪攻击，从 PIT 的过期列表中识别异常名称前缀，并向相邻节点反馈限制携带异常名称前缀的兴趣包转发速率。与其他兴趣包泛洪攻击防御方法对比分析，结果表明所提出的基于异常名称前缀识别的协同防御方法可以准确识别所有异常名称前缀，同时在不降低合法兴趣包速率的前提下，快速抑制恶意兴趣包在网络中传输，减少合法用户受攻击的影响。

2 内容中心网络的兴趣包泛洪攻击

2.1 内容中心网络

内容中心网络(CCN)[1−4]将内容作为网络中的基本元素，对内容进行命名。内容名称格式采用标

2013-11-11 收到，2014-03-18 改回
国家自然科学基金(61271202, 61202428)，北京市自然科学基金(4122060)和中央高校基本科研业务费专项(2013JBM013)资助课题
*通信作者：唐建强 tangjianqiang@bjtu.edu.cn

准的通用资源标识符(Universal Resource Identifier, URI)，例如优酷(youku.com)某个视频文件的名称可以为“ccnx:/ youku. com/ video/123. mp4/ <timestamp>”，其中<timestamp>是时间戳，“/”用于划分名称的组成部分。本文假定一个内容名称的最长前缀包含完整的文件或服务名，比如例子中的最长前缀为“ccnx:/youku.com/video/123. mp4/”。CCN 采用接收者驱动的通信模式，即当接收者发出兴趣包后，数据包才会返回给接收者，且一个兴趣包只被一个数据包满足。

CCN 中路由器根据内容名称转发兴趣包，与内容名称匹配的数据包沿着兴趣包的反向路径传输到达接收者。当路由器接收到兴趣包时，首先查询内容缓存(Content Store, CS)是否存储了对应内容，若有，则返回数据包；否则，路由器查询 PIT 是否已有相同内容名称的条目，若有，则将兴趣包的到达接口添加到对应条目，否则创建一个新的 PIT 条目，存储该兴趣包和到达接口等信息；路由器采用前缀匹配方法向转发信息表(Forwarding Information Base, FIB)查询兴趣包的转出接口，若查到，则转发兴趣包，否则丢弃或广播兴趣包。当路由器接收到数据包时，路由器根据内容名称向 PIT 查询对应兴趣包的到达接口，若找到，则向该接口转发数据包并删除对应 PIT 条目，同时路由器缓存数据包，以满足后续请求相同内容的兴趣包；否则丢弃数据包。

2.2 兴趣包泛洪攻击

CCN 中路由器的计算资源和 PIT 存储空间有限，攻击者发送大量恶意兴趣包就能耗尽路由器的 PIT 存储空间，使路由器无法新建 PIT 条目存储合法用户的兴趣包及到达接口，造成 PIT 溢出和网络拥塞。由于 CCN 采用接收者驱动的通信模式，取消了主机地址，用户根据名称获取内容，攻击者很难针对特定路由器或主机发起兴趣包泛洪攻击。然而，攻击者却很容易针对特定的名称前缀发起兴趣包泛洪攻击。当大量攻击者发送相同前缀的恶意兴趣包时，则兴趣包泛洪攻击类似于 IP 网络中的分布式拒绝服务攻击(Distributed Denial of Service, DDoS)。IP 网络中 DDoS 攻击主要影响特定攻击目标。而兴趣包泛洪攻击与其不同点在于：(1)兴趣包泛洪攻击主要影响网络中的路由器，因为路由器将在 PIT 存储恶意兴趣包并为其维护转发状态，消耗大量计算和存储资源；(2)兴趣包泛洪攻击对内容提供者影响较小，因为内容提供者只需根据内容名称返回对应内容，而没有与恶意兴趣包的发送者保持连接状态。

为了确保兴趣包泛洪攻击的效果，更多地占用路由器 PIT 资源，攻击者需要尽量避免泛洪内容名称相同的兴趣包，并且避免兴趣包所请求内容被 CS 满足。若攻击者发送恶意兴趣包请求真实存在的内容，则需要收集大量不流行内容的名称，这样增加了攻击成本但并不能明显提高攻击效果。因此，攻击者更有可能伪造内容名称，发送大量恶意兴趣包请求不存在的内容。路由器无法在接收到兴趣包时就判断其内容名称的真实性，这些伪造内容名称的恶意兴趣包存储在 PIT 中，不会有对应数据包满足，直到过期才被删除。伪造内容名称的兴趣包泛洪攻击成本低，且对路由器 PIT 存储资源影响大，更可能在 CCN 中发生，因此本文针对伪造内容名称的兴趣包泛洪攻击进行研究。

2.3 兴趣包泛洪防御方法相关研究

自 CCN 被提出以来，兴趣包泛洪攻击受到广泛的关注[5−11]。文献[6]分析了 CCN 中路由节点容易受到兴趣包泛洪攻击而使 PIT 溢出，列举了通过改进 PIT 存储和替换机制、设计无状态的路由转发机制等应对方案，但并未进行分析。文献[7]介绍了针对已存在内容、动态生成内容和不存在内容的兴趣包泛洪攻击，提出了两种应对措施：利用路由器的转发状态限制每个接口接收或转发的兴趣包数量，和利用反馈机制溯源并限制兴趣包转发数量，但只进行了简单分析，没有给出具体分析结果。

文献[8]提出了基于令牌桶的公平接口队列、基于满足率的兴趣包接收与转发和基于满足率的反馈 3 种方法防御兴趣包泛洪攻击，其中基于满足率的反馈方法防御效果最好。基于满足率的反馈方法中路由器分别计算每个接口接收兴趣包的满足率，根据兴趣包满足率设定接口的兴趣包接收速率，并向相邻路由器发送反馈包，限制兴趣包转发速率。文献[9]提出 Poseidon，根据路由器中每个接口接收兴趣包与发出数据包的比例和 PIT 使用率来判断不同接口是否存在兴趣包泛洪攻击；当检测到攻击时，路由器动态调整兴趣包与数据包比例和 PIT 使用率的报警阈值，向相邻路由器发送反馈包，限制兴趣包的转发速率。文献[8]和文献[9]的防御方法可以在全网范围的路由器上部署，它们的兴趣包速率限制反馈包都只单跳回溯到相邻路由器，不会被转发。文献[8]和文献[9]中路由器只按接口限制兴趣包速率，不区别正常兴趣包和恶意兴趣，因此合法用户发送的正常兴趣包传输速率也将受到限制，合法用户受攻击影响较大。

文献[10]提出 TDM 机制，该机制根据 PIT 中的兴趣包过期率检测兴趣包泛洪攻击，并在路由器中限制兴趣包转发速率减少恶意兴趣包对内容提供者的影响。由于 TDM 部署在靠近内容提供者的路由器上，TDM 只能限制发送到内容提供者的恶意兴趣包，不能减少核心网中恶意兴趣包数量，也不能防止核心网路由器中 PIT 溢出。文献[11]提出 Interest traceback 方法，该方法中溯源路由器根据 PIT 利用率检测兴趣包泛洪攻击，通过伪造数据包来满足伪造内容名称的兴趣包，进行溯源防御。溯源路由器伪造的数据包可以沿着伪造兴趣包的传输路径逐跳回溯到攻击者，减少伪造兴趣包占用的 PIT 资源。但该方法未给出溯源路由器的部署位置以及溯源路由器如何获得伪造的内容名称，同时，该方法只在边缘路由器限制攻击者的兴趣包转发速率，增加了方案的复杂度，降低了其防御效果。

3　兴趣包泛洪攻击识别与协同防御

基于前缀识别的协同反馈防御方法主要包括 3 个部分：兴趣包泛洪攻击检测，异常名称前缀识别和协同反馈防御。基于前缀识别的协同反馈防御过程是：路由器周期性地根据兴趣包满足率和 PIT 使用率判断是否存在兴趣包泛洪攻击；若存在，则进一步从过期的 PIT 条目中识别异常名称前缀；最后路由器向相邻节点反馈协同防御包，通知相邻节点限制转发异常名称前缀的兴趣包，如图 1 所示。

3.1 兴趣包泛洪攻击检测

兴趣包泛洪攻击检测主要依据两个参数：PIT 使用率 φ 和兴趣包满足率 S。PIT 使用率 φ 表示当前路由器 PIT 中的兴趣包条目数量与 PIT 可存储兴趣包条目总数的比值。兴趣包泛洪攻击的主要目的是消耗路由器的 PIT 资源，造成网络拥塞，因此 PIT 使用率 φ 是兴趣包泛洪攻击检测的一个重要参数。兴趣包满足率 S 用来表示一段时间内路由器发出的数据包数量和接收并添加到 PIT 中的兴趣包数量的比值。兴趣包满足率 S 可以反映出路由器接收恶意兴趣包占合法兴趣包的比例。

用 $t_1,t_2,\cdots,t_n$ 表示时刻，分别用 $I(t_n)$ 和 $D(t_n)$ 表示第 n 个时间段内到达路由器的兴趣包和数据包数量，则到达路由器的兴趣包的历史平均值和数据包的历史平均值分别可以表示为：$\overline{I}(t_n)=(1-\alpha)\overline{I}(t_{n-1})+\alpha I(t_n)$，$\overline{D}(t_n)=(1-\alpha)\overline{D}(t_{n-1})+\alpha D(t_n)$。其中 $0<\alpha<1$ 是惯性系数，表示长时间段内平均数据数量对当前数据数量的敏感程度。t_n 时刻路由器的兴趣包满足率为：$S(t_n)=\overline{D}(t_n)/\overline{I}(t_n)$。

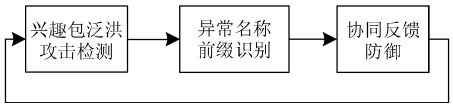

图 1 兴趣包泛洪攻击识别与协同防御过程

由于 CCN 中一个兴趣包只能被一个数据包满足，路由器接收的平均兴趣包数量与发出的平均数据包数量应相等，即 $S(t_n)$ 应约为 100%。

当 PIT 使用率 φ 大于阈值 φ_{T} 时，表明路由器中 PIT 的兴趣包数量超出预警值；当 $S(t_n)$ 值低于阈值 $S_{\mathrm{T}}(t_n)$ 时，表明兴趣包与数据包的一一对应关系出现异常。当路由器 PIT 使用率和兴趣包满足率都达到设定的阈值 φ_{T} 和 $S_{\mathrm{T}}(t_n)$ 时，则网络中存在兴趣包泛洪攻击，触发路由器识别异常名称前缀；而当 PIT 使用率和兴趣包满足率未达到设定的阈值 φ_{T} 和 $S_{\mathrm{T}}(t_n)$ 时，则网络中没有兴趣包泛洪攻击，或存在的兴趣包泛洪攻击对路由器影响较小。

3.2 异常名称前缀识别

CCN 中伪造内容名称的恶意兴趣包没有数据包可以满足，其对应的 PIT 条目直到过期才被删除。当发生伪造兴趣包泛洪攻击时，路由器 PIT 中的过期条目数量增加，且有大量恶意兴趣包的 PIT 过期条目。因此，可以从 PIT 过期条目中识别出受攻击的内容名称前缀。

当异常名称前缀识别被触发时，路由器立即开始收集 PIT 过期条目。路由器提取所有 PIT 过期条目的最长内容名称前缀，计算各名称前缀的过期兴趣包个数 ρ。若 ρ 高于阈值 ρ_{T}，则对应的名称前缀不可达、或内容名称错误、或受到了恶意兴趣包的攻击，存在异常。识别出异常名称前缀后，触发协同反馈防御。阈值 ρ_{T} 反应了网络对错误兴趣包的容忍度。由于攻击者可以伪造内容名称的任意组成部分，为了准确识别伪造名称前缀，需要递减识别前缀的长度。即若已识别的某个异常名称前缀长度为 n，则后续再对该名称前缀识别时，逐次递减名称前缀识别长度，如图 2 所示，直到该名称前缀的过期兴趣包数量低于阈值。

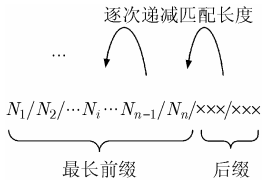

图 2 异常名称前缀识别

3.3 协同反馈防御

协同反馈防御时，路由器向相邻路由器发送协同防御包。协同防御包采用数据包的格式，其携带的内容名称为空，携带的内容为识别的异常名称前缀，其他签名等信息按 CCN 设计进行填充。内容名称为空的数据包不会被转发，路由器验证其签名后可判定是否为协同防御包。当路由器收到协同防御包时，提取出异常名称前缀，采用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。若用户接收到协同防御包，采用基于 AIMD 的方法限制发送异常前缀兴趣包。即使恶意用户不理睬协同防御包，其他路由器也会限制异常前缀兴趣包的转发速率。网络中其他合法兴趣包传输速率不受影响。

路由器中基于 AIMD 的异常前缀兴趣包速率限制方法设计如表 1 所示。当路由器接收到兴趣包时，首先判断其名称前缀是否异常，若是则限速转发，否则正常转发(表 1 中第(1)步)；当路由器接收到协同防御包时，对应的异常前缀兴趣包转发速率指数减小(表 1 中第(2)步)，其中 C 为大于 1 的常数，例如 $C=10$；当路由器接收到携带异常前缀的数据包时，对应的异常前缀兴趣包转发速率线性增加(表 1 中第(3)步)；当路由器 T_{L} 时间内没有再接收到针对异常名称前缀的协同防御包时，删除对异常名称前缀的转发速率限制(表 1 中第(4)步)，T_{L} 根据网络状况设定，如 T_{L} 可以为 30 min。

表 1 基于 AIMD 的异常前缀兴趣包速率限制方法

步骤		
	// prefix	已识别的异常名称前缀
	// r_{prefix}	前缀 prefix 的转发速率
	// C	大于 1 的常数，例如 $C=10$
	/* 当路由器接收到报文 */	
(1)	**case** 兴趣包	
	if 兴趣包的内容名称前缀是异常前缀 prefix	
	以速率 r_{prefix} 转发兴趣包	
	else	
	以 CCN 的原始设计转发兴趣包	
	end if	
(2)	**case** 协同防御包	
	if 协同防御包要求限制前缀 prefix 的转发速率	
	计算 $r_{\mathrm{prefix}}=r_{\mathrm{prefix}}\times e^{-C}$	
	end if	
(3)	**case** 数据包	
	if 数据包的内容名称前缀是异常前缀 prefix	
	计算 $r_{\mathrm{prefix}}=r_{\mathrm{prefix}}+C$	
	end if	
	按 CCN 的原始设计转发数据包	
(4)	**if** 如果 T_{L} 时间内未收到针对前缀 prefix 的协同防御包	
	删除对前缀 prefix 的转发速率限制	
	end if	

4 横向比较

表 2 对比分析了几种兴趣包泛洪攻击防御方法。本文所提出的基于前缀识别的协同防御方法部署在全网路由器中。路由器根据 PIT 使用率和兴趣包满足率检测兴趣包泛洪攻击，并从 PIT 过期条目中识别出异常名称前缀，攻击检测粒度较细。同时，路由器根据名称前缀区分恶意兴趣包，采用单跳回溯的方法向相邻路由器发送协同反馈包，基于 AIMD 方法限制异常名称前缀兴趣包的转发速率，而不影响合法兴趣包的转发速率，速率限制粒度较细，对合法用户影响较小。

表2 兴趣包泛洪攻击防御方法对比

	攻击检测		攻击防御			部署位置
	攻击检测方法	检测粒度	是否溯源	速率限制方法	速率限制粒度	
基于满足率的反馈方法[8]	兴趣包满足率	异常接口	单跳回溯	基于兴趣包满足率的速率限制	按接口限制	全网路由器
Poseidon[9]	PIT 使用率和兴趣包满足率	异常接口	单跳回溯	动态阈值	按接口限制	全网路由器
TDM[10]	兴趣包过期率	异常前缀	否	基于 FIB 的速率限制	按前缀限制	内容提供者端
Interest trackback[11]	PIT 使用率	异常名称	逐跳回溯	边界路由器限制	按攻击者限制	特定位置
本文基于前缀识别的协同防御方法	PIT 使用率和兴趣包满足率	异常前缀	单跳回溯	基于 AIMD 的异常前缀速率限制	按前缀限制	全网路由器

5　验证与分析

本节使用基于 NS3 的仿真工具 ndnSIM[12]进行仿真实验，验证所提出兴趣包泛洪攻击识别与防御方法的有效性，并与其他方案对比分析。ndnSIM 是 CCN 协议栈在 NS3 仿真环境中的实现。通过扩展修改 ndnSIM，增加兴趣包满足率计算模块、异常前缀识别模块和协同反馈包构造器等，使其支持本文所提出的基于前缀识别的兴趣包泛洪攻击防御方法。本文仿真实验中，每个用户发送兴趣包的名称前缀不同，攻击者只伪造文件或服务名，即识别异常前缀时不需要递减前缀匹配长度。

5.1 攻击检测与异常前缀识别分析

本节分析兴趣包泛洪攻击检测的有效性，异常前缀识别的正确性和异常前缀的识别时间。实验拓扑如图 3，该拓扑代表了攻击检测和异常前缀识别的一种最差环境，即单个路由器能否有效检测兴趣包泛洪攻击并识别异常前缀。图 3 所示拓扑中有 200 个用户。随机从 200 个用户中挑选不同数量的用户作为攻击者。普通用户发送兴趣包速率为 200 个/s，攻击者发送伪造内容名称的恶意兴趣包，速率为 1000 个/s。

根据文献[13]，设定 α 为 0.1 或 0.3。路由器检测周期 $T=t_1=\cdots=t_n$ 设定为 1 s 或 2 s。假设路由器可容忍的相同前缀过期兴趣包数量为 10 个/s 或 20 个/s，即 $\rho_{\mathrm{T}}=10$ 个/s 或 $\rho_{\mathrm{T}}=20$ 个/s。设定 φ_{T} 为 80%或 90%，$S_{\mathrm{T}}(t_n)$ 为 90%或 80%。分别对 φ_{T}，$S_{\mathrm{T}}(t_n)$，α，ρ_{T} 和 T 的多种参数组合进行仿真实验，所得的结果基本相同。图 4 画出了 $\varphi_{\mathrm{T}}=80\%$，$S_{\mathrm{T}}(t_n)=80\%$，$\alpha=0.1$，$\rho_{\mathrm{T}}=10$ 个/s 和 $T=1$ s 时，在不同数量攻击者的情况下，路由器识别出的异常前缀数量。从图 4 可以看出，所提出的攻击检测和异常前缀识别方法可以快速地检测到兴趣包泛洪攻击并识别出所有异常名称前缀，异常名称前缀识别时间与受攻击的前缀数量和检测周期几乎无关，且识别所有异常前缀的时间与攻击者个数几乎无关。

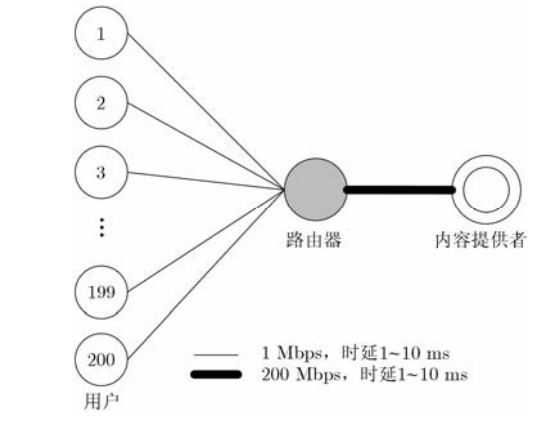

图 3 攻击检测和前缀识别实验拓扑环境

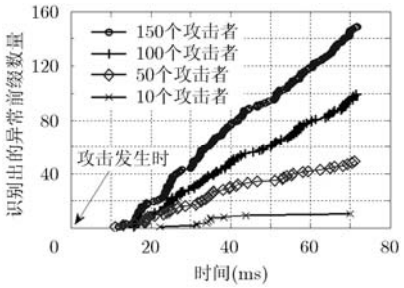

图 4 前缀识别分析结果

5.2 协同反馈防御分析

协同反馈防御的仿真分析在 AT&T 真实网络拓扑中进行。AT&T 真实网络拓扑是由文献[14]中 AT&T 网络(AS7018)修改得到的。从 AT&T 网络中提取 625 个节点，将度不大于 4 的节点作为终端用户，直接与终端用户相连的节点作为网关，其他节点作为骨干节点，如图 5 所示。位于边缘的 296 个节点为终端用户，与终端用户连接的 108 个节点为网关，位于中间的 221 个点为骨干节点。网络中链路带宽和时延按链路类型根据表 3 所限定的范围随机设置。从 296 个终端用户中随机选取 150 个作为攻击者，其他 146 个作为合法用户，攻击者占所有用户的比例约为 50%，高于实际网络情况。从骨干节点中随机选择一个作为内容提供者。网关和骨干节点可存储的最大 PIT 条目数量为 10,000。

仿真分析主要通过对比网络中没有攻击时、只有攻击时和防御攻击时 3 种情况下，兴趣包有效时间(lifetime, lf)为 1 s 或 2 s，以及检测周期 T 为 1 s 或 2 s 等多种条件下，路由器中 PIT 条目数量变化情况，以及合法用户发出兴趣包(Interest)和接收数据包(Data)的数量。兴趣包有效时间是指兴趣包的 PIT 条目在路由器 PIT 表中的有效时间，若在有效时间内兴趣包仍未被满足，则对应的 PIT 条目被删除。由于基于满足率的反馈方法是当前兴趣包泛洪防御效果较好的一个方案[8]，因此本文以该方案作为比较分析对象。在本节的仿真实验中，统一设定 $\varphi_{\mathrm{T}}=80\%$，$S_{\mathrm{T}}(t_n)=80\%$，$\alpha=0.1$，$\rho_{\mathrm{T}}=10$ 个/s，兴趣包泛洪攻击从第 5 s 开始，每个攻击者以固定速率发送伪造内容名称的恶意兴趣包，速率为 1000 个/s。

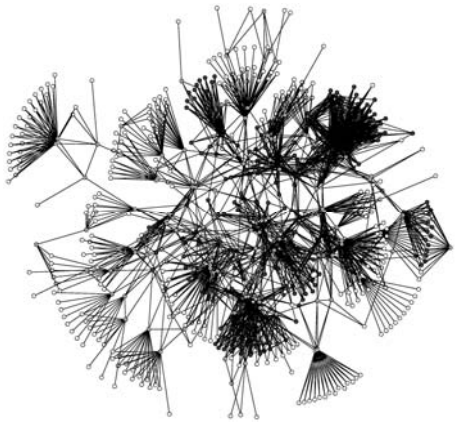

图 5 AT&T 真实网络拓扑示意图

表 3 链路带宽和时延

链路类型	带宽(Mbps)	时延(ms)
骨干节点间	40~100	5~10
网关-骨干节点、网关间	10~20	5~10
终端用户-网关	1~3	10~70

图 6 描绘了网络中所有网关和骨干节点的 PIT 条目总数量。从图 6 中可以看出，当网络中没有攻击时，路由器中 PIT 条目总数量较少，一直维持在 1000 左右；当网络受到攻击而没有防御时，PIT 条目总量从攻击开始时(第 5 s)剧增，远远超过没有攻击时的状态，且兴趣包有效时间较长，PIT 条目总量越大(即当 $\mathrm{lf}=1\,\mathrm{s}$ 时，PIT 条目数量约是 380,000；当 $\mathrm{lf}=2\,\mathrm{s}$ 时，PIT 条目数量约是 490,000)；当进行协同反馈防御时，路由器限制异常兴趣包的转发速率(表 1 中第(1)步)，新加入到路由器中的伪造兴趣包迅速减少，同时路由器中伪造兴趣包的 PIT 条目在过期后被删除，PIT 条目总量很快恢复到没有攻击时的水平。

图 7 描述了大型 AT&T 真实网络拓扑中所有合法用户发出的兴趣包数量以及在不同条件下接收数据包的数量。从图 7 (a)可以看出，当没有攻击时，合法用户发出的兴趣包数量与接收的数据包数量基本相同，每秒约为 5,100 个；当有攻击而没有防御时，合法用户发送的兴趣包数量不变，接收的数据包数量急剧下降，每秒不到 1000 个。从图 7 (b)可以看出，当进行协同反馈防御时，随着路由器中 PIT 条目数量迅速减少，路由器有足够空间为合法用户的兴趣包新建 PIT 条目，合法用户接收数据包的数量可以快速恢复到没有攻击时的水平，恢复时间与路由器中 PIT 条目数量恢复时间一致(如图 6)。

图 8 描述了当 AT&T 真实网络受到兴趣包泛洪攻击，采用基于满足率的反馈方法防御攻击时，合法用户发送的兴趣包和接收的数据包数量。对比图 7 和图 8 可知，采用基于满足率的反馈方法防御攻击时，合法用户发送的兴趣包数量将受到限制，合法用户接收的数据包数量恢复到没有攻击时的水平需要较长时间。由于网络中兴趣包泛洪攻击时不同接口兴趣包满足率变化较大，根据兴趣包满足率计算的兴趣包转发限制速率在很长一段时间具有较大波动，不稳定时间随兴趣包有效时间或检测周期增加而增加。

从图 6 和图 7 中可以看出，兴趣包泛洪攻击能增加路由器中 PIT 条目数量，降低合法用户接收数据包数量。基于前缀识别的协同防御方法中，路由器能识别兴趣包泛洪攻击的异常前缀，只限制伪造前缀恶意兴趣包的转发速率，合法用户发送的普通兴趣包速率不受影响，从而使得合法用户接收数据包的数量可以在较快时间内快速地恢复到没有攻击时的状态。检测周期 T 越短，路由器中 PIT 条目数

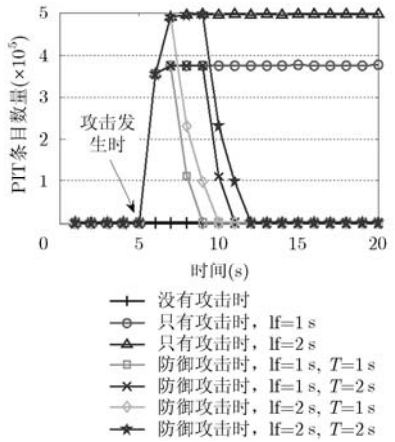

图 6 路由器中的 PIT 条目数量

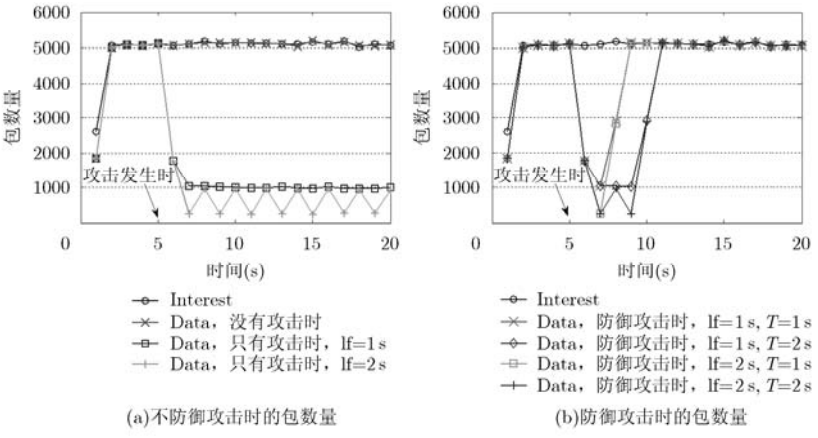

图 7 合法用户发出的兴趣包数与接收的数据包量

量恢复时间越短，合法用户受到的影响越小。另外，兴趣包的有效时间越长，路由器中 PIT 条目和合法用户接收数据包的数量恢复到正常水平的时间越长，攻击造成的影响越严重。对比图 7 与图 8 可知，所提出的基于前缀识别的协同防御方法具有较好的防御效果，路由器的 PIT 条目恢复时间较短，用户发送兴趣包的速率不受影响，且其接收的数据包数量恢复到没有攻击时的状态更快。

5.3 计算开销分析

基于满足率的反馈方法根据异常接口来检测和防御兴趣泛洪攻击，而基于前缀识别的协同防御方法根据异常前缀来识别和防御泛洪攻击。表 4 比较了这两种方法的主要计算开销。在检测识别部分，两种方法都需要周期性的计算，主要计算开销区别在于：基于满足率的反馈方法分别为每个接口计算兴趣包满足率，计算开销正比于接口数量；基于前缀识别的协同防御方法需要识别出异常前缀，计算开销正比于异常前缀的数量。在反馈防御部分，基于满足率的反馈方法需要根据兴趣包满足率为每个接口分别计算速率，同时反馈限制速率，因此速率计算开销和构造反馈包的开销都正比于接口数量；基于前缀识别的协同防御方法利用 AIMD 算法为每个异常前缀计算限制速率，因而速率计算开销和构造反馈包的开销都正比于异常前缀数量。

由于路由器的接口数量有限，而异常前缀数量由攻击者决定，因此基于前缀识别的协同防御方法计算开销较大，且受兴趣包泛洪攻击影响。

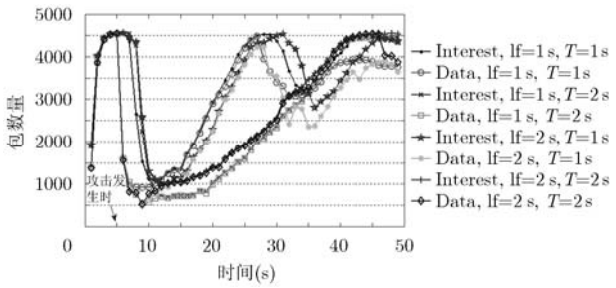

图 8 采用基于满足率的反馈方法时，合法用户发送的兴趣包与接收的数据包数量

表 4 主要计算开销

	检测识别			反馈防御		
	PIT 使用率计算	兴趣包满足率计算	前缀识别	速率计算	构造反馈包	速率限制
基于满足率的反馈方法[8]	无	正比于接口数量	无	正比于接口数量	正比于接口数量	接口
本文基于前缀识别的协同防御方法	1 次/周期	1 次/周期	正比于异常前缀数量	正比于异常前缀数量	正比于异常前缀数量	前缀匹配

6　结束语

本文在分析内容中心网络中的兴趣包泛洪攻击的基础上，提出基于前缀识别的兴趣包泛洪攻击协同防御方法。该方法根据路由器中的 PIT 使用率和兴趣包满足率检测兴趣包泛洪防御攻击，从 PIT 的过期条目中识别出异常的名称前缀，并将异常前缀反馈到相邻节点，限制异常前缀兴趣包的转发速率。所提出的方法相对于其他几种兴趣包泛洪防御方法，检测粒度更细。在 AT&T 真实网络拓扑中仿真实验，验证了所提出的方法可以快速检测兴趣包泛洪攻击并准确地识别出异常名称前缀，抑制兴趣包泛洪攻击，降低路由器和用户受攻击影响。虽然提出的方法相对于基于满足率的反馈方法具有较大的计算开销，但防御效果更好。

参 考 文 献

[1] Jacobson V, Smetters D K, Thornton J D, *et al*.. Networking named content[C]. Proceedings of the 5th International Conference on Emerging Networking Experiments and technologies (CoNEXT), Rome, Italy, 2009: 1–12.

[2] Zhang L, Jacobson V, Estrin D, *et al*.. Named Data Networking (NDN) Project[R]. Technical Report NDN-0001, NDN, October 31, 2010.

[3] Yi C, Afanasyev A, Moiseenko I, *et al*.. A case for stateful forwarding plane[J]. *Computer Communications*, 2013, 36(7): 779–791.

[4] Perino D and Varvello M. A reality check for content centric networking[C]. Proceedings of the ACM SIGCOMM Workshop on Information-Centric Networking, Toronto, Ontario, Canada, 2011: 44–49.

[5] Wählisch M, Schmidt T C, and Vahlenkamp M. Backscatter from the data plane — threats to stability and security in information-centric networking[R]. Technical Report 1205.4778, ArXiv eprint, May 2012.

[6] Lauinger T. Security & Scalability of content-centric networking[D]. [Master dissertation], TU Darmstadt, Schwetzingen, Germany, September 2010.

[7] Gasti P, Tsudik G, Uzun E, *et al*.. DoS and DDoS in named-data networking[R]. Technical Report 1208.0952, ArXiv eprint, August 2012.

[8] Afanasyev A, Mahadevan P, Moiseenko I, *et al*.. Interest flooding attack and countermeasures in named data networking[C]. International Federation for Information Processing (IFIP) Networking, New York, USA, 2013: 1–9.

[9] Compagno A, Conti M, Gasti P, *et al*.. Poseidon: mitigating interest flooding DDoS attacks in named data networking[R]. Technical Report 1303.4823, ArXiv eprint, March 2013.

[10] Wang Kai, Zhou Hua-chun, Luo Hong-bin, *et al*.. Detecting and mitigating interest flooding attacks in content-centric network[J]. *Security and Communication Networks*, 2014, 7(4): 685–699.

[11] Dai Hui-chen, Wang Yi, Fan Jin-dou, *et al*.. Mitigate DDoS attacks in NDN by interest traceback[C]. IEEE INFOCOM Workshop on Emerging Design Choices in Name-Oriented Networking, Italy, April, 2013.

[12] Afanasyev A, Moiseenko I, and Zhang L. ndnSIM: NDN simulator for NS-3[R]. Technical Report NDN-0005, 2012.

[13] Yu Chen, Kai Hwang, and Wei-Shinn Ku. Collaborative detection of DDoS attacks over multiple network domains[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2007, 18(12): 1649–1662.

[14] Spring N, Mahajan R, and Wetherall D. Measuring ISP topologies with rocketfuel[J]. *ACM SIGCOMM Computer Communication Review*, 2002, 32(4): 133–145.

唐建强： 男，1987 年生，博士生，研究方向为网络路由交换技术、网络安全.

周华春： 男，1965 年生，博士，教授，研究方向为网络路由交换技术、移动互联网、网络安全.

刘 颖： 女，1978 年生，博士，副教授，研究方向为网络路由交换技术、普适服务理论技术.