基于汇聚树的 CCN 兴趣包研究

李 涛[1],吕立尧[1],贾庆民[1],张 晨[1],张钰雯[2]
(1. 紫金山实验室未来网络研究中心,江苏 南京 211111;
2. 中国信息通信研究院,北京 100191)

摘 要:信息中心网络(CCN)的转发信息路由(FIB)因为内容存储表(CS)动态变化而频繁的震荡刷新,导致兴趣报文间歇性无路由状态而泛洪;同时因为兴趣包按照最长路由匹配查找进行转发,攻击端利用这一特点,发送大量匹配最长路由的无效明细兴趣报文,从而导致网络待定请求路由(PIT)资源的耗尽。针对如上场景中兴趣包泛洪带来的带宽浪费及数据丢失问题以及兴趣包泛洪攻击带来的资源耗尽问题,在总结目前各种兴趣包研究的基础上,提出了一种兴趣包隧道路由机制,包括 CP(Center Point)选举机制、源端注册机制、慢采样机制、请求端路由机制、CPT(Center Point Tree)机制等。通过如上机制在转发面建立以可灵活配置的 CP 节点为中心的 CPT 隧道,在隧道树对兴趣报文进行引流和分析,并做出相应的转发或者防御策略解决如上问题。仿真结果表明,在网络噪声较大时,可以极大降低丢包率,节省网络带宽;在乱序兴趣包泛洪攻击时,可以实现路由器首跳无源兴趣报文的有效压制。

关键词:汇聚树;源端注册;CP 选举;兴趣包;慢采样
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2022)11-0100-06
doi:10.3969/j.issn.1673-629X.2022.11.015

Research on CCN Interest Packet Based on Aggregation Tree

LI Tao[1],LYU Li-yao[1],JIA Qing-min[1],ZHANG Chen[1],ZHANG Yu-wen[2]
(1. Purple Mountain Laboratories Future Network Research Center,Nanjing 211111,China;
2. China Academy of Information and Communications Technology (CAICT),Beijing 100191,China)

Abstract:The forwarding information routing (FIB) of the information center network (CCN) is refreshed frequently due to the dynamic change of the content storage table (CS),resulting in intermittent flooding of interest packets without routing status. At the same time,because interest packets are forwarded according to the longest route matching search,the attackers take advantage of this feature to send a large number of invalid detailed interest packets matching the longest route,resulting in the exhaustion of network pending request routing (PIT) resources. Aiming at the problem of bandwidth waste and data loss caused by the flooding of interest packets and the problem of resource exhaustion caused by the flooding attacks of invalid interest packets,a interest-packet tunnel routing mechanism is proposed based on the summary of various current interest packet studies,including CP (Center Point) election mechanism,source registration mechanism,slow sampling mechanism,requester routing mechanism and CPT (Center Point Tree) mechanism,etc. Through the above mechanism,CPT tunnel centered on the flexibly configurable CP node is established on the forwarding surface,the interest packets are drained and analyzed in the tunnel tree,and the corresponding forwarding or defense strategies are made to solve the above problems. The simulation results show that when the network noise is large,the packet loss rate can be reduced greatly and the network bandwidth can be saved. In the flooding-attack of out-of-order interest packets,the router can suppress the first hop passive interest packets effectively.

Key words:aggregation tree;source registration;CP election;interest packet;slow sampling

0 引 言

随着互联网业务的蓬勃发展,目前 TCP/IP 网络架构已经越来越难以满足人们的需求,因此以信息为中心的网络通信模型,即 CCN,成为备受关注的焦点[1]。在 CCN 中有三个数据结构,分别是待定请求表(Pending Interest Table,PIT)、内容缓存(Content Store,CS)、路由转发表(Forwarding Information Base,FIB)[2]。路由器收到兴趣包后,首先查找 CS 表,然后查找 PIT 表,最后查找 FIB 明细路由表,如果三个表都没有查找到就会泛洪该兴趣包[3],一般在如下情况会

收稿日期:2021-10-11 **修回日期**:2022-02-24
基金项目:国家自然科学基金(61872078)
作者简介:李 涛(1983-),男,硕士研究生,工程师,CCF 会员(C6168M),研究方向为 CCN 网络、工业互联网等。

引起三个表都查不到的泛洪:(1)随着 CS 动态存储变化,引起 FIB 的实时动态更新,在此过程中由于路由同步时序问题某个时段概率性三个表都查找不到而泛洪该兴趣包;(2)发起 PIT 泛洪攻击时,大多数情况下 FIB 明细路由是不存在的,此时就会按照最长路由匹配转发 PIT 请求而引起泛洪[4]。CCN 设备发起泛洪在网络中查找可能有转发路由的邻接设备,从而达到尽可能将用户请求数据转发至源端来接收数据的目的[5]。因此,基于如上 CCN 网络兴趣包泛洪的特点,该文区分了有效泛洪和无效攻击报文泛洪两种类型,在现有的 CCN 基础上研究并设计了一种可配置的隧道路由机制,通过该机制实现了有效兴趣包的隧道转发和无效兴趣包的源端压制,保证了数据的可靠、安全传输。

1　CCN 兴趣包研究现状

在此背景下,针对兴趣包的优化研究主要分为如下几个方面:

(1)针对泛洪的防御攻击研究。

泛洪数据包给泛洪攻击提供了便利,目前针对 PIT 兴趣包的泛洪攻击主要分为攻击检测和攻击防御,针对此也提出了很多检测和防御的方式和方法。唐建强等人[6]提出使用 AIMD 算法限制带有异常内容名称前缀的兴趣包的转发;经典的 cooperative. Filter 方案[7]要求所有网络设备都参与兴趣包泛洪防御的检测工作,同时各个设备同步网络告警信息,使得下游的网络节点可以及时感知攻击源,在靠近网络源点的位置进行防御;Afanasyev 等人[8]提出了基于端口流量限制的攻击防御方法;Poseidon 方案[9]将兴趣包满足率和 PIT 使用率结合来判断不同接口是否存在兴趣包泛洪攻击;文献[10]提出了一种基于信息熵的分析检测泛洪攻击的算法;吴浔等[11]基于 AIMD 算法改进实现了对泛洪攻击的快速检测。

(2)针对兴趣包转发路径优化研究。

谢人超等人[12]提出了一种兴趣包转发方法,通过设置默认路径转发来解决兴趣包无路由丢失问题;文献[13-15]研究了 SDN、SR 与 CCN 融合架构思想,兴趣包在 SDN 控制下按照分段路由隧道转发机制实现兴趣包的高效有序转发。以上研究中,兴趣包防泛洪攻击防御策略大多集中在对 PIT 占用率、过期条目、过期率、兴趣包满足率等指标进行分析,然后按照相应的阈值进行检测和防御;甚至提出通过路由器对兴趣包进行签名验证来抑制兴趣包攻击[16]。这些研究对于兴趣包泛洪攻击具有一定的抑制作用,但是因为一些算法本身的问题,阈值设定的问题,使得防御攻击失真,同时签名认证也会带来用户信息的泄漏;针对兴趣包转发路径优化研究中,对兴趣包转发路径提出了默认路径转发思想、SDN-SR 转发路径思想等,对于兴趣包泛洪抑制及合理化传输有很大的带宽节省、资源合理有效使用的价值,但是目前相关研究存在很多问题,例如针对海量兴趣包攻击时,大量无效计算上送至 SDN 控制器,导致 CPU 的冲击和带外网络资源的浪费;

在分析各种研究的基础上,该文提出了一种 CCN 兴趣包隧道方案,即在传统 CCN 路由基础上,在转发面上增加了一棵或多棵负载汇聚树来应对兴趣包泛洪问题,即在目的节点-CP(Center Point)-源节点间建立一条或者若干条段式 CPT(Center Point Tree)隧道树,CPT 树上存在基于 CP 的 FIB 隧道路由,该路由可选取代 FIB 路由作为默认兴趣包 CCN 转发路由或者防攻击的目的分析节点路由,作为默认兴趣路由时,在设备上按照默认路由转发至 CP 节点,由 CP 节点负责转接源数据;作为防攻击的目的节点路由时,在明细路由查找不到,按照最长匹配路由转发的同时,将其送到 CP 节点,在 CP 节点结合源注册数据进行泛洪攻击的计算,并将计算结果通过 CPT 树通知源端进行防御。基于该机制,解决了兴趣包泛洪带来的带宽消耗问题、泛洪攻击带来的安全问题、兴趣包丢弃引起的用户体验问题,增强了工程实用性。该方案相较于经典的 cooperative. Filter 等方案,将其防御方案只局限在 CPT 树上设备进行,不需要所有设备参与,有效地减少了网络冗余负载;同时利用兴趣报文的选项机制由用户自定义的灵活的 CP 选举机制,相较于 SDN 兴趣包的路径优化方案,有效节省了大量的告警信息汇总和计算。最后基于该机制给出基于 CPT 树作为默认路由情况下的仿真结果和分析。

2　基于汇聚树的兴趣包缓存机制

本研究引入 CP 节点解决兴趣包泛洪问题,因为 CP 节点的引入,基于现有的 CCN 路由对整个路由寻址体系进行重构。兴趣包引入 CP 节点作为兴趣包的终节点,CP 节点收到兴趣路由后,生成注册兴趣 PIT 路由,即生成请求端到 CP 的一棵 PIT 转发树,待 FIB 路由通告完成后,FIB 路由反向刷新 CP 上的注册 PIT 表,触发 PIT 表按照 FIB 进行源路由器转发,沿途生成 CP 到源的 PIT 转发树;两张 PIT 转发树以 CP 为中心,组成一张完整的 CPT 转发树,完成兴趣包的投递和数据的传输,同时基于灵活选择的集中 CP 节点可以完成策略控制、PIT 泛洪攻击防御计算等功能。因此重构 CCN 路由机制,在兴趣报文中增加如下选项:

(1)注册选项:分为注册报文、去注册报文选项;其中源注册报文选项功能为告知添加 CP 源端的路

由;去源注册报文选项:告知删除 CP 源端的路由。

(2)CP 选项:分为 CP 转发选项、CP 上送选项;其中转发选项功能为告知 CP 该报文由 CP 转发;CP 上送选项功能为告知 CP 检测路由的合法性。

2.1 CP 选举机制

用户根据网络设备位置、性能、容量指标,选择并配置一个主 CP、一个或者多个候选 CP 作为路由的选择依据,对应的 Prefix 路由如下标识:/cp-prefix/time/compute/capability,即将 CP 的创建时间、算力、容量大小纳入路由中,每一个 CP 按照如上格式形成一条命名路由,利用 OSPFN 的 OLSA 扩散出去,因此在每一台设备上形成命名路由的 FIB 表,每一台路由器并不知道哪一个是主 CP 哪个是候选 CP,因此每台设备基于相同的算法计算主 CP,目前计算规则为:time>compute>capability,对于计算胜出的路由,下发转发面并且标记为 CP 路由,主 CP 路由下转发表,根据硬件的支持情况选择候选 CP 路由是否下发以支持快切;主 CP 路由就作为默认路由。同时每一台路由器也可选定制相应的路由策略,来区别选择主 CP。通过策略控制,可以将数据从负载过重的 CPT 隧道上迁移到负载较轻的 CPT 隧道上,保证数据的有效和及时传输。表 1 为 Prefix 路由表,每一台设备收到该表后,进行 CP 选举计算,胜出者作为 CP 路由下发转发面。

表 1 CP 路由表

Prefix	Faces
/cp1-prefix/time/compute/capability	1
/cp2-prefix/time/compute/capability	2

2.2 源端注册机制

基于传统的路由机制,例如 OSPFN,CP 节点作为 CCN 网络的保护汇聚点,需要快速感知源路由的有效性,但是 FIB 通告存在如下问题:

(1)在源路由组装 LSA 发布之后,因为 LSA 的路由同步较慢,CP 节点无法快速感知路由。

(2)OSPF 考虑路由的聚合性,其发布的路由多为聚合路由,CP 节点对于明细路由无法感知。

(3)CP 节点收到恶意攻击的路由,无法进行有效区分,如果一直忙等 FIB 路由通告容易造成攻击的泛洪。

基于如上问题,研究设计了一种机制保证源明细路由快速传递到 CP 汇聚点上,命名为源注册路由机制。该机制在源端 CCN 网关上按照源到 CP 的单向路由发起源路由注册,注册路由为点到点单向兴趣包路由,在沿途按照源节点到 CP 的 FIB 转发即可。CP 端收到注册路由后,形成一个源注册路由表,该路由标识该源信息的有效性。源注册路由表格式如图 1 所示。

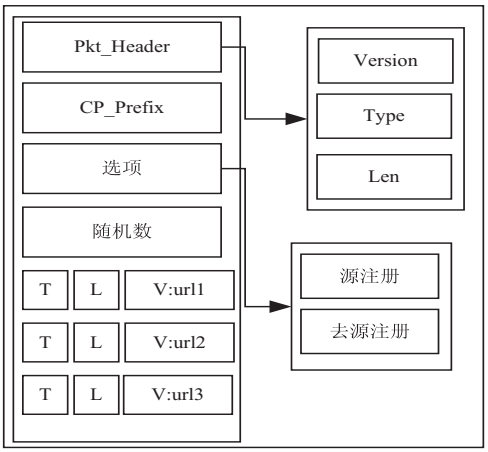

图 1 兴趣报文-源注册报文

其中将 CP Prefix 作为兴趣报文的头,选项中增加了源注册和去源注册选项,标识为注册报文,在兴趣报文后携带相应的源数据的 prefix 的 URL 压缩信息;整个报文作为注册报文封装为兴趣报文格式传输至 CP 端。

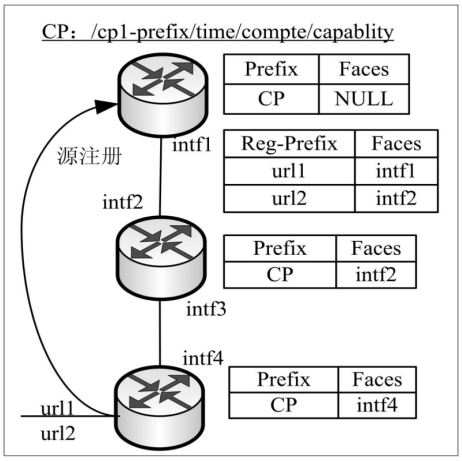

图 2 源注册流程及相应路由表

源路由注册过程如下:

(1)配置的 CP 会生成如图 2 所示的 CP 为目的 Prefix 的 FIB 路由。

(2)源端数据到达第一跳路由器后,组装兴趣包,目的地址为 CP 的 Prefix 路由;内含源端各个明细路由的 TLV 明细 url 表。

(3)沿途路由器检查发现目的为 CP 知名目的地址,按照 CP 的 Prefix 路由转发即可,并按照 CCN 默认路由,生成 PIT 路由。

(4)数据到达 CP 节点后,CP 去掉 CP 兴趣包头,解析生成源请求路由 URL 的明细 FIB 表;如图 2 所示在 CP 节点生成的 Re-Prefix 注册路由,其中出接口标记为注册口。

(5)CP 节点向源节点回复内容消息,该消息按照源注册生成的 PIT 路由回复,为注册停止消息。其格式如图 3 所示。

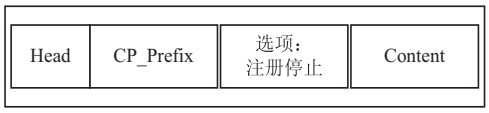

图 3　注册停止报文

其中 CP_Prefix 标识为注册的回复消息,选项中增加了 reg-stop 宏,标识为注册停止消息。内容选项为随机值即可。源节点收到注册回复消息后,标识该源注册兴趣报文正确接收,继续发送下一个压缩源明细注册路由。

2.3　慢采样机制

采样机制为请求端第一跳路由器采用的算法。该机制通过采样兴趣报文发送,保证对采样周期内兴趣包进行抑制的方法来防止无效兴趣包的泛洪。

一般请求端收到 CP 节点传送的首次无源注册路由的兴趣报文后启动采样机制,采样报文的无源注册路由每一次回复,采样周期相应的指数增加。例如,请求端设备启动采样周期为 50 ms 的 prefix1 报文发送至 CP 节点,CP 节点判断该报文无明细注册路由后,回复数据请求端路由无效信息,请求端收到后,将采样周期设置翻倍进行采样,以此类推。

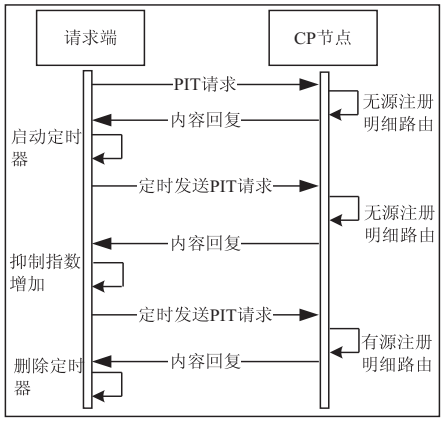

图 4　慢采样机制

图 4 所示为采样机制在先无源注册路由后有源注册路由机制下的基本流程。

(1)CP 节点收到 PIT 请求,检查源注册明细路由情况,发现无源注册路由,回复采样抑制。

(2)请求端收到采样抑制后,启动采样定时器;然后请求端采样定时器到期后,如果有 PIT 请求,继续发送该请求。

(3)CP 收到请求后,发现仍然没有源注册明细路由,继续回复采样抑制消息。

(4)接收端收到后,将采样抑制定时器扩大 2 倍后,启动采样定时器;采样定时器到期后,继续发送 PIT 请求。

(5)CP 端收到 PIT 请求,发现有源注册路由了,回复消息。请求端收到后,删除抑制定时器,正常转发该 PIT 请求。

由于慢采样指数增长的压制机制,对于 10 次以上无源路由注册情况下 PIT 请求,将达到 1 000 倍以上指数增长的压制效率,实现无效兴趣报文的第一跳压制。

2.4　请求端路由机制

源路由机制保证了源明细路由在 CP 节点的汇聚。请求端路由机制则是将请求兴趣路由发送至 CP 节点上,基于该节点完成数据的策略处理和转发。如图 5 所示,该机制的基本流程如下:

(1)请求端发起一个 url1 明细路由请求;R1 收到该 PIT 请求后有三种情况按照 CPT 树转发:检查发现无 FIB 路由,则增加 CP 转发选项将其转入 CPT 树中;检查发现策略路由需要传入 CPT 树中完成攻击检查,增加 CP 上送选项,可选增加 CP 转发选项送入 CPT 树中;检查配置的门限策略,检测发现疑似攻击报文,需要传入 CPT 树中进行准确性校验,增加 CP 上送选项送入 CPT 树中。

(2)R1 组装 PIT 报文,请求 Prefix 为 url1,请求接口为 interest 接口,在图 1 所示兴趣报文中增加携带 CP 选项。

(3)R2 收到报文,发现是 CP 选项兴趣报文,按照 CP 默认路由进行转发,并生成相应的 PIT 路由。

(4)R3 收到后,发现自己为 CP 节点,检查 R3 的注册路由,如果没有注册路由,转步骤 5;如果有注册路由,转步骤 6。

(5)开启 Dead 定时器,该定时器标识路由的有效性和合法性,用户自定义配置 Dead 时间。Dead 定时器到期后,无源注册路由,或者无源前缀路由,则认为是攻击报文,通知请求端采样注册机制抑制该请求报文相应的前缀路由,随着采样注册无有效源路由应答,则请求端采样定时器越来越大,从而从请求端抑制无效兴趣报文的泛洪。具体流程见慢采样机制。

(6)PIT 路由标识为有效路由,等待 FIB 路由通告后,PIT 路由则按照 FIB 路由生成 CP 到源端 PIT 请求路由。

2.5　CPT 树生成

CPT 树为以 CP 为根节点,整个网络节点为叶子的一棵 CCN 网络的隧道树,整个数据在 CPT 树中传输由源注册节点完成注册为前提,由兴趣报文向 CP 节点发起请求开始生成,由 FIB 通告结束为终节点,完成兴趣请求在 CPT 隧道中的传输。该机制以兴趣包的 PIT 路由在 CPT 隧道传输的同时,在 CP 节点完成路由的合法性校验和防攻击检查。

CPT 树 PIT 表项如图 5 所示,Prefix 为请求明细路由,Req-Faces 为 PIT 的请求接口,流程如下:

(1)请求端到 CP 汇聚路由的生成,请求端与 CP

节点按照 CPT 转发树生成请求 PIT 路由。图 5 中以 R3 作为 CP 节点,R1 作为请求端,见请求端路由机制章节,R1-R2-R3 生成以 CP 路由为请求目的的 PIT 路由。

(2)源端到 CP 的 FIB 路由下发:源端按照 OSPF 相应的 LSA 扩散,形成了一条源端与 CP 的路由表;如图 R5-R4-R3 形成一张 URL 的最短匹配路由表。

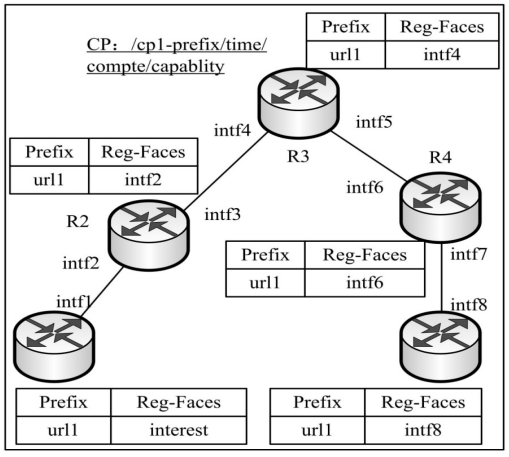

图 5 CPT 树上 PIT 路由表

(3)CP 到源端 PIT 路由的下发:如果 CP 先收到请求端的 PIT 路由后,等待源端 FIB 路由通告后完成 CP 到源端 PIT 请求树的建立;如果 CP 先收到源端 FIB 路由通告,需要完成 FIB 路由对 PIT 路由的反刷动作;最终建立 CP 到源端 PIT 请求树。

(4)注册路由检查:等待 FIB 刷新后,源注册路由完成与 FIB 路由前缀的父子关系确定,即 FIB 路由的前缀路由与注册的 URL 明细路由组成父子关系,例如:URL =/bupt. edu. cn/texts/docs/_ v3, FIB 路由 Prefix:/bupt. edu. cn,双方以/bupt. edu. cn 为父亲,后缀/bupt. edu. cn/texts/docs/_v3 为子。父子关系确定后基于 FIB 聚合路由重新生成 FIB 出接口。

(5)源端数据传输:源端收到 CP 传送过来的兴趣包后,触发数据源沿着 CPT 树上的 PIT 表进行转发,一直送至请求端,数据传输完成后,按照 CCN 协议删除传输的 PIT 路由即可。

(6)防御策略的生成:基于完整的 CPT 树机制,在 CP 节点上,开放相应的 OAM 策略,完成用户自定义防御策略配置的下发。对于配置防御策略的 CP 节点,需要所有明细源注册路由以完成兴趣包攻击的最长路由匹配。

基于如上机制,形成一条以 CP 端为中心的,请求端到 CP 端的 PIT 路由,CP 端到源端的 PIT 路由,两段路由按照时序性依次生成,完成后将组成完整的 CPT 兴趣路由。数据内容数据按照 CPT 树 PIT 路由回复即可。基于该 CPT 树完成正常兴趣包的传输和异常报文的防御策略。

3 仿真实验与结果分析

(1)仿真环境。

在本仿真中采用了 CICN 开源环境,基于 CPT 树机制,如图 6 所示,R1-R2-R3-R4 为 CPT 树,R3 为配置的 CP 节点,CP 节点缓存数量为 2w 条 PIT 路由。验证了如下两种场景:路由震荡情况下兴趣包泛洪抑制效果;无效兴趣包攻击抑制效果。

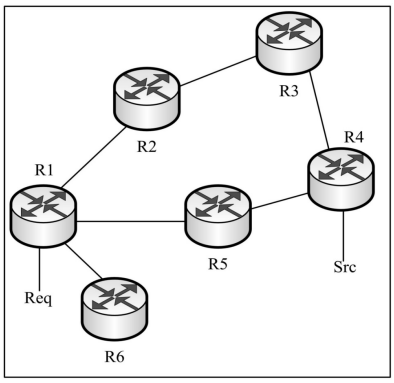

图 6 仿真网络拓扑

图 7、图 8 模拟了在路由震荡情况下 PIT 兴趣包丢包率、带宽消耗的优化前后对比情况。图 9 模拟了无效兴趣包攻击情况下通过下一跳设备的 PIT 表项数量来验证慢采样机制的有效性。

(2)丢包率比较。

如图 7 所示,路由部分:构造 2w 条 FIB 路由,外加 2w 条背景路由,其中现有 FIB 路由随机选取 20% 路由进行震荡;兴趣包部分:每秒发送 5k 个查找 FIB 路由的 PIT 请求报文;定时器部分:为了更直观观察丢包率,将 PIT 老化定时器设置为 100 ms;基于如上的构造在采用 CPT 树机制前后随着时间变化的丢包率对比仿真。显而易见,采用 CPT 树兴趣包缓存机制后丢包率明显低于未优化前的,并达到预期效果。优化后因为通过 CP 缓存,等待 FIB 下发后继续转发,基本实现了完全不丢包;但是随着兴趣包数量越大,CP 节点缓存满了,相对的丢包率就会略有升高,因此在实际部署时,CP 的选择尤为重要。

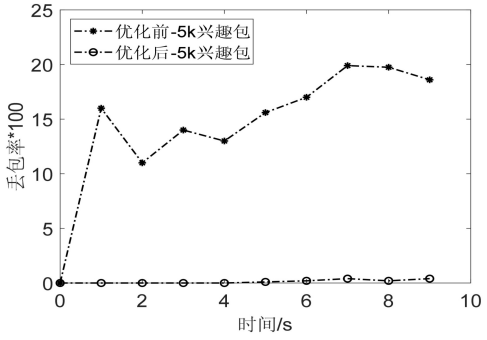

图 7 CPT 机制前后丢包率对比

(3)带宽消耗比较。

图 8 中,路由部分与兴趣包部分的设置与图 7 环

境相同,定时器部分:将 PIT 老化定时器设置为默认值;如拓扑图中首跳 R1 存在 3 条泛洪链路出口,本仿真统计 R1-R5 链路带宽。由图可见,优化后的带宽消耗指标优于优化前的,并且随着兴趣包数量的增加,发现优化前后消耗带宽差距变大。

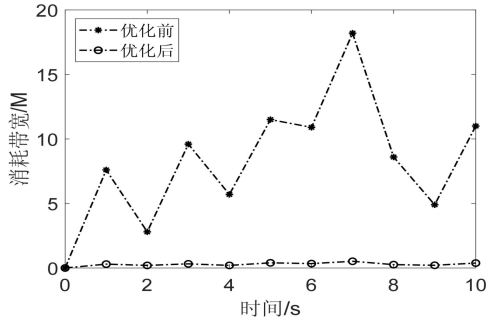

图 8　CPT 机制前后带宽消耗对比

(4)PIT 表项对比。

图 9 中,场景是每秒 1w 个随机无效明细路由兴趣包持续攻击下,测试下一跳路由器 R5 的 PIT 表数量。在采用 CPT 慢采样机制压制情况下,可以看到 R5 的 PIT 数量在 3 秒后呈现指数级的压制,随着时间延长,攻击表项下降明显。

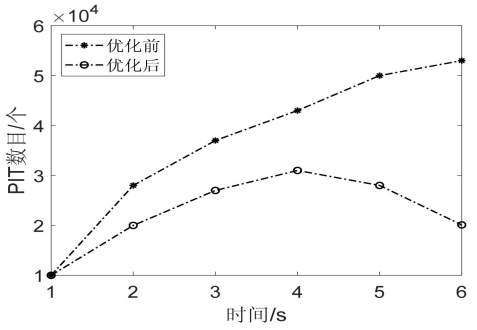

图 9　CPT 机制前后 PIT 表项对比

4　结束语

该文提出的汇聚树的 CCN 兴趣包隧道机制,在路由震荡、兴趣报文泛洪攻击的场景下,通过预先建立 CPT 转发树,在进行相应防御的基础上来保证兴趣包的有效传输;针对 CPT 树流量负载采样情况,提出多候选 CP,保证主 CPT 树切换为备选 CPT 树,解决流量过载问题;根据无效报文攻击问题,提出了慢采样机制,在无效源注册路由情况下,可以实现指数级 PIT 压制,极大降低无效兴趣报文的攻击;考虑了路由扩散的延迟性、动荡性、明细路由的有效性等特点,提出了源注册机制,保证了源路由合法性。仿真表明,在丢包率、带宽消耗、抑制动态无效兴趣报文攻击方面,采用该机制实现明显优于未采用前,是一种可行方案。但是该方案也存在 CP 选举点问题、CPT 树负载问题等,将在后续的项目中持续进行研究和改进。

参考文献:

[1] ZHANG L, AFANASYEV A, BURKE J. Named data networking(ndn)[J]. ACM SIGCOMM Computer Communication Review, 2014, 44(3): 66-73.

[2] CHOI J, HAN J, CHO E, et al. A survey on content-oriented networking for efficient content delivery[J]. IEEE Communications Magazine, 2011, 49(3): 121-127.

[3] 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. Rome: ACM, 2009: 1-12.

[4] AHLGREN B, DANNEWITZ C, IMBRENDA C, et al. A survey of information-centric networking[J]. IEEE Communications Magazine, 2012, 50(7): 26-36.

[5] 陈　震,曹军威,尹　浩. 内容中心网络体系架构[M]. 北京:清华大学出版,2014:13-45.

[6] 唐建强,周华春,刘　颖,等. 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[J]. 电子与信息学报, 2014(7):1735-1742.

[7] WANG K, ZHOU H, QIN Y, et al. Cooperative-filter: countering interest flood attacks in named data: networking[J]. Soft Computing, 2014, 18(9): 1803-1813.

[8] AFANASYEV A, MAHADEVAN P, MOISEENKO I, et al. Interest flooding attack and countermeasures in named data networking[C]//Proc of IF-IP networking conference. Piscataway: IEEE, 2013: 1-9.

[9] COMPAGNO A, CONTI M, GASTI P, et al. Poseidon: mitigating interest flooding DDoS attacks in named data networking[C]//Proc of the 38th annual IEEE conference on local compute networks. Sydney: IEEE, 2013: 630-638.

[10] XIN Y H, LI Y, WANG W, et al. Detection of collusive interest flooding attacks in named data networking using wavelet analysis[C]//2017 IEEE military communications conference (MILCON). Baltimore: IEEE, 2017: 557-562.

[11] 吴　浔,凌　捷. 改进的 CCN 兴趣包泛洪攻击防御方法[J]. 计算机应用研究,2020,37(4):1132-1135.

[12] 谢人超,黄　韬,徐京薇,等. 一种兴趣包转发方法及装置:中国,CN105704032B[P]. 2016-06-22.

[13] 李　根,伊　鹏,张　震. 软件定义的内容中心网络的分段路由策略[J]. 计算机应用研究,2018,35(7):2030-2033.

[14] SYRIVELIS D, PARISIS G, TROSSEN D, et al. Pursuing a software defined information-centric network[C]//Proc of European workshop on software defined networking. Washington DC: IEEE, 2012: 103-108.

[15] MELAZZI N B, DETTI A, MAZZA G, et al. An OpenFlow-based testbed for Information centric networking[C]//Proc of future network & mobile summit. Piscataway: IEEE, 2012: 1-9.

[16] LAUINGER T. Security & scalability of content-centric networking[D]. Schwetzingen: TU Darmstadt, 2010.