doi:10.3969/j.issn.1001-893x.2016.02.020
引用格式:霍跃华,刘银龙. 内容中心网络中安全问题研究综述[J]. 电讯技术,2016,56(2):224-232. [HUO Yuehua, LIU Yinlong. Survey on security issues in content-centric networking[J]. Telecommunication Engineering, 2016, 56(2):224-232.]

内容中心网络中安全问题研究综述*

霍跃华[1],刘银龙**[2]

(1. 中国矿业大学(北京) 现代教育技术中心,北京 100083;2. 中国科学院 信息工程研究所,北京 100093)

摘 要:内容中心网络(CCN)是一种革命性的网络架构,采用内容路由、网内缓存等技术来提高网络中的内容分发效率,但其自身的结构特点使之面临很多的安全问题。通过对 CCN 网络工作机制的研究,分析了 CCN 面临的非授权访问、隐私泄露、泛洪攻击等安全风险;然后,总结了每种安全风险的解决方案及各自优缺点;最后,展望了未来的研究方向。

关键词:内容中心网络;安全风险;访问控制;隐私保护;泛洪攻击
中图分类号:TN918 **文献标志码**:A **文章编号**:1001-893X(2016)02-0224-09

Survey on Security Issues in Content-centric Networking

HUO Yuehua[1], LIU Yinlong[2]

(1. Center of Modern Education Technology, China University of Mining & Technology (Beijing), Beijing 100083, China;
2. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)

Abstract: Content-Centric Networking (CCN) is a revolutionary network architecture which uses named-based routing and in-network caching to improve the content distribution efficiency, but it faces many security problems because of the structural characteristics. Through researching the mechanism of CCN, this paper analyzes the security threats the system faces, such as unauthorized access, privacy leak and flooding attack, and then summarizes corresponding solutions and their respective advantages and disadvantages. Finally, it provides future research directions.

Key words: content-centric networking; security threats; access control; privacy-preserving; flooding attack

1 引 言

随着 Internet 的快速发展和不断变化,网络应用的主体正逐渐向内容服务转移,以主机为中心的传统 TCP/IP 网络逐渐暴露出许多问题,如不安全、移动性差、可靠性差、灵活性差等。为了解决这些问题,自 2006 年起,国内外学术界开展了多项关于下一代互联网体系结构的研究项目,并提出了多种新的互联网架构,主要有 UC Berkeley 提出的面向数据的网络架构(Data-Oriented Network Architecture, DONA)[1]、欧盟 FP7 的 4WARD[2] 以及发布/订阅式互联网路由范例(The Publish-Subscribe Internet Routing Paradigm, PSIRP)[3]、Palo Alto Research Center 提出的内容中心网络(Content-Centric Networking, CCN)[4] 和中国科学院提出的内容感知网络(Content Aware Network)[5] 等。这些架构都采用了以内容为中心的核心思想,其中 CCN 的网络设计更具有代表性,已成为下一代互联网架构的研究热点。

近年来,许多科研工作者已经对 CCN 中的命名[6-7]、缓存[8]、路由[9] 等关键技术进行了深入的研究,而且 Kim[10] 和 Jeong[11] 等还分别将 CCN 应用到

* **收稿日期**:2015-09-23;**修回日期**:2015-12-31 Received date:2015-09-23;Revised date:2015-12-31
基金项目:国家自然科学基金资助项目(61303251);中国科学院战略性先导科技专项基金资助项目(XDA06010703)
Foundation Item: The National Natural Science Foundation of China (No. 61303251); The Strategic Pilot Project of Chinese Academy of Sciences (XDA06010703)
** **通信作者**:liuyinlong@iie.ac.cn **Corresponding author**: liuyinlong@iie.ac.cn

虚拟专用社区和远程信息服务。已有研究主要关注网络中的内容分发效率,而对 CCN 的安全问题研究较少。由于 CCN 属于开放式的网络架构,尽管能够有效提高内容分发效率,却面临许多安全挑战,如非授权访问、用户隐私信息泄露、泛洪攻击等。

本文主要对 CCN 网络中的安全问题进行分析和总结。

2　内容中心网络原理与特点

2.1　CCN 工作原理

如图 1 所示,CCN 体系沿袭了 TCP/IP 网络的沙漏结构,只是用命名数据代替 IP 地址作为网络标识,直接基于内容名字完成内容的查找和获取等。

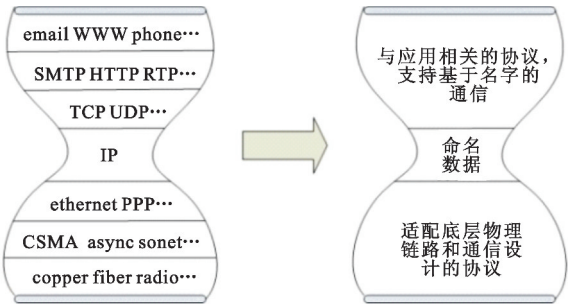

图 1　TCP/IP 网络和 CCN 网络结构对比图
Fig. 1 TCP/IP architecture vs. CCN architecture

CCN 主要利用缓存路由器(Caching Router, CR)对兴趣包(Interest Packet, IntP)和数据包(Data Packet, DatP)进行处理和转发来实现信息交互。

兴趣包的格式如图 2(a)所示,包括内容名字、用户选项和随机数。其中,内容名字表明请求内容的名称,用户选项表示内容请求者的特殊需求,随机数确定接收到的兴趣包是否为之前已经收到的重复兴趣包。数据包的格式如图 2(b)所示,包括内容名字、内容发布者的数字签名和相应的认证信息(内容发布者 ID、公钥等),以向内容请求者提供接收内容的完整性、准确性认证以及对内容发布者的身份认证。

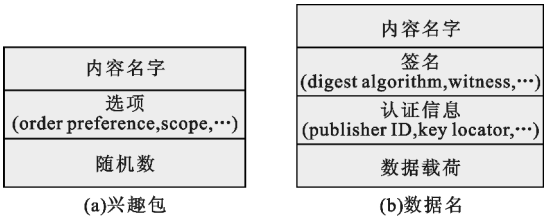

图 2　CCN 包格式
Fig. 2 CCN Packets format

缓存路由器包含 3 个核心功能模块:内容缓存(Content Store, CS)、待定兴趣表(Pending Interest Table, PIT)和转发信息表(Forwarding Information Base, FIB)。接下来,结合图 3 介绍 CCN 中的数据转发。

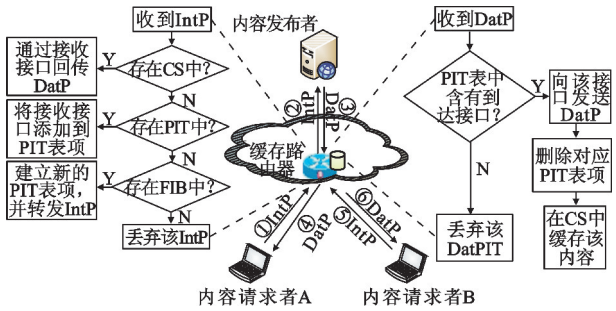

图 3　CCN 数据转发模型
Fig. 3 CCN forwarding model

内容请求者 A 想要获取某一内容 C 时,通过广播方式向缓存路由器 CR 发送含有该内容名字的兴趣包。

CR 接收到兴趣包后,首先查询 CS 是否存储了对应内容,若有,则通过兴趣包的反向路径返回数据包;否则,路由器查询 PIT 是否已有相同内容名字的表项,若有,则将兴趣包的到达接口添加到对应表项,否则创建一个新的 PIT 表项,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 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 CR 接收到来自内容发布者的数据包时,CR 根据内容名字向 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。

内容请求者 B 想要获取相同的内容 C 时,缓存路由器可以直接将 CS 中缓存的内容 C 发送给 B,而不需再向内容发布者请求。这样,既可以降低网络中流量负荷,也可以提高内容请求者 B 获取内容的时延。

2.2　CCN 主要特点

(1)提高了内容分发效率

CCN 中通过缓存路由器缓存经过的内容来提高网络中的内容分发效率。缓存路由器中的缓存与 IP 路由器中的 buffer 缓冲类似,都是用来缓存数据包的。但是,IP 路由器将数据包转发之后不能再利

用该数据包,而缓存路由器还可以重复使用该数据的缓存。对于静态的文件,CCN 几乎达到了最优的内容分发;对于动态文件,在多播和重传的情况下,CCN 的缓存功能也具有优势。

(2)支持多路径路由

传统的 IP 网络中采用最佳路由的方法来防止路由成环,而在 CCN 中,兴趣包中的随机数能够有效地标识重复的兴趣包,一旦发现收到重复的兴趣包,便会将其直接丢弃。因此,CCN 网络节点可以同时向多个接口发送兴趣包,并保证其不成环。而数据包完全按照兴趣包传输相反的路径传输,也不会成环。这种内置的多路径传输机制很好地支持了负载均衡及服务选择功能。

(3)增强了网络的路由安全

与传统 IP 网络相比,CCN 网络的路由安全性得到大大提高。首先,包括路由信息在内的所有网络数据都使用签名机制,能够有效防止它们被伪造或者篡改;其次,由于 CCN 支持多路径路由,网络节点能够检测到由路由劫持导致的异常并尝试选择其他路由,从而可以有效地防范前缀劫持。此外,CCN 网络架构只着眼于内容本身,并不定位某个具体主机或服务器。因此,在 CCN 网络中是不能针对某个具体的主机或服务器目标发送恶意攻击数据的。

3 CCN 中安全问题分析

3.1 CCN 面临的安全威胁

3.1.1 非授权访问

CCN 将内容数据视为核心要素,且内容的多个副本可以存放在网络中的不同位置。该机制有效地提高了网络中的内容分发效率,特别是高流行度内容的分发效率。但是,这种机制也带来了内容非授权访问的安全问题。由于一旦内容被分布出去,就脱离了发布者的控制,攻击者通过接收其他节点的兴趣包就可以获取其中的内容名字,并进而获取内容。例如,网络中具有版权保护要求的视频只有在用户被授权后才能观看,而 CCN 中的缓存机制使得授权视频访问控制中的版权保护难以有效实施。传统保护视频版权的技术(如数字水印)只能够用来验证视频属于该视频发布者,而不能用来保护视频的版权[12]。

3.1.2 用户隐私泄露

CCN 中的用户隐私信息主要面临以下两种泄露风险。

首先,数据签名会泄露内容发布者的身份隐私。为了确保获取内容的真实性和完整性,每个数据包必须带有发布者的签名,且数据包的签名必须能够被所有内容消费者验证。因此,数据包中除了包含内容发布者签名外,还需指明验证签名的公钥或发布者 ID 等信息。攻击者通过这些验证信息就能够获取与发布者身份相关的隐私信息。

其次,缓存机制会泄露内容请求者的检索隐私。一方面,攻击者通过测量获取内容的响应时间就可以判定一个给定内容是否被缓存在一个节点,从而得知相邻用户是否检索、访问了该内容[9];另一方面,用户检索内容的名字易被相邻节点获知,攻击者可以利用请求者的检索信息推测出请求者的行为偏好等隐私信息。

3.1.3 兴趣包泛洪攻击

CCN 中的 PIT 在降低网络负载的同时,一定程度上增加了路由器的工作负担。首先,兴趣包基于 FIB 进行转发,同时兴趣包状态也将记录在 PIT 中用于指导对应数据包的反向转发,因此兴趣包的转发过程需占用路由器的内存资源;其次,每个兴趣包或数据包到达时,均触发路由器 PIT 表项的添加、删除等更新操作,也会占用路由器资源;第三,若兴趣包无法找到相应的内容数据包,则该兴趣包在 PIT 中的对应表项将一直保存,直至表项生存时间超时(一般而言,该时间远大于网络的内容获取平均往返时延[13]),这增加了 PIT 对路由器资源的占用时间。因此,攻击者泛洪大量的恶意兴趣包非法占用路由器待定兴趣表的内存空间,以达到攻击内容中心网络并降低其网络性能的目的[14]。

CCN 中的恶意兴趣包主要分为两类:虚假兴趣包(Fake Interests)和真实兴趣包(Real Interest)。虚假兴趣包是指携带有伪造名字的兴趣包,无法从网络中获取到对应的数据包,从而实现长时间占用路由器待定兴趣表内存资源的目的;而真实兴趣包是携带有真实名字的兴趣包,但名字信息却不断发生变化,即通过类似“轮询”的方式大量取回数据包,实现恶意拥塞网络链路的目的。相应地,使用前一种兴趣包进行攻击的方式称为虚假兴趣包泛洪攻击(Interest Flooding Attack with Fake Interests, IFA-F),而使用后一种兴趣包进行攻击的方式称为真实兴趣包泛洪攻击(Interest Flooding Attack with Real Interests, IFA-R)。

3.2　CCN 安全需求

CCN 的目标是实现高效、安全和易于维护的内容分发,但是 CCN 的内在特征使其面临与 TCP/IP 不同的隐私和可用性的风险,这迫切需要一些新的安全解决方案来检测和阻止所有的潜在攻击。这些解决方案需要满足 4 个安全需要:机密性、完整性、有效性和隐私。

机密性:只有符合条件的实体能够访问安全的信息。

数据完整性:接收端能够识别/鉴定接收内容在传输过程中任何无意或有意的改变。

可认证性:接收端能够验证接收内容的发布者是否合法。

隐私保护:能够对通信节点的身份、行为、通信内容等隐私信息进行保护。

有效性:保证了对于授权实体来说网络中发布的内容必须能够可用和可访问。

4　CCN 安全解决方案现状及分析

本节总结当前针对 CCN 网络中非授权访问、用户隐私泄露和兴趣包泛洪攻击的解决方案,并分析这些方案的优缺点。

4.1　访问控制技术研究

目前关于 CCN 访问控制的研究还很少,内容加密是其中最主要的方法。

在 CCN 设计初期,Jacobson[4] 就基于加密的访问控制方法来保护内容。该方法对内容用对称密钥进行加密,加密后的内容可以被缓存在路由器中,任何节点都能够从路由器中获取加密后的内容。然而,只有授权用户才能得到对称加密的解密密钥,这样已授权用户就可以通过解密得到内容数据。但该方案对于某一个授权内容,所有已授权用户都使用同一个解密密钥,如果一个已授权用户有意或无意间泄露了该密钥,那么所有获得该密钥的用户都可以获取内容,进而导致无法有效地进行访问控制。另外,该方法无法抵御虚假内容攻击(即通过监听兴趣包,攻击者可以利用兴趣包中的内容名字及其自己的密钥、数字签名等生成具有相同内容名字的虚假数据包,并发送给请求者)。

为克服该方法的不足,Hamdane 等[15] 在上述方法的基础上提出了一种改进的访问控制方法,将内容加密与基于 PKI 和 HIBC 的命名系统相结合,并用非对称密钥替换对称密钥以提高内容加密性能。该方法将 HIBC 融入了命名系统,能够有效抵御虚假内容攻击,并降低了系统开销。此外,该方法还为每个授权接入用户(或实体)分配一个不同的密钥,从而能够确定泄露密钥的用户,可以实施更精准的接入控制。文献[16]使用控制核心模型(Usage Control Authorizations, Obligations, Conditions, UCONABC)这种通用和概念上的访问控制方案,提供一个最佳的和安全的以数据为中心的访问控制模型。在此方案中,数据通过加密进行保护,其访问过程由一个集中的访问控制列表来管理。

除了通过对内容加密来进行访问控制,Li 等[17] 提出了一种轻量级完整性认证架构(Lightweight Integrity Verification Architecture, LIVE)来实现有效、可扩展的内容访问控制。该架构采用轻量级的签名生成和验证算法来完成网络中内容签名认证,通过向授权用户分配完整性验证令牌来控制对内容的访问。Wang 等[18] 提出了一种基于会话的接入控制机制(Session-based Access Control, SAC),根据会话业务类型(电子邮件、在线社交、在线游戏、web 访问等)选择性地对会话中的敏感性内容进行加密,并利用从内容提供商(Content Provider, CP)获取的用户账户来区分用户,为不同用户提供不同的密钥以获取对应的内容数据。

以上方案可以用于任何类型内容的访问控制,具有普遍适用性。除此之外,一些研究者还研究了适用于某一特定类型内容的访问控制方法。例如,周自飞等[12] 提出了一种基于分割和数字水印的访问控制方案,用来保护网络中授权视频的版权。该机制的基本原理是:将一个授权视频分割成公共内容块和内容密钥块两个部分,且公共内容块远远大于密钥块。公共内容块可以被缓存在路由器中,任何人都能够从路由器中获取它。只有被授权的用户才能够从视频发布者那里获取密钥块,用唯一且不同的密钥块对应不同的已授权用户,而且这些不同的密钥块都能和功能内容块结合在一起恢复出原始的授权视频内容。但如果没有获得密钥块,任何人都不能够恢复出授权视频,从而实现授权视频版权保护的访问控制。

上述方案在一定程度上都能对 CCN 进行访问控制,但每种方案的控制效果不尽相同,其对比如表 1 所示。

表 1 访问控制方案比较

Tab. 1 Comparison among access control schemes

方案	优点	不足
Jacobson 所提方案[4]	实现简单	无法确定密钥泄露用户,且无法抵御虚假内容攻击
Hamdane 所提方案[15]	能够确定密钥泄露用户、抵御虚假内容攻击,且降低系统开销	只适用于树形网络结构
UCONABC 方案[16]	能够实施精准的访问控制,且配置简单	需要服务器来管理访问控制列表
LIVE 方案[17]	既能使得接受用户验证内容的真实性、完整性,又可以对用户访问进行精准控制	需要向用户分配令牌的服务器,且难以收回授权用户权限
SAC 方案[18]	可以根据会话业务,选择性地进行访问控制,可以降低系统复杂度和开销	需要内容提供商进行配合
基于分割和数字水印的方案[12]	对部分数据进行加密处理,可以减少系统开销	只适用于视频业务

当前已有访问控制方案主要是通过内容加密-密钥分配来实现的,能够对用户的访问权限进行静态的控制。但是,已有方案仍存在不足之处。例如,在实际应用中用户的访问权限通常是发生变化的(比如用户会员到期会导致用户访问权限被取消),而已有方案难以直接应用到此类情况。因此,需要针对现有方案中的不足进行深入研究。

4.2 隐私保护技术研究

目前,对 CCN 中的隐私保护研究主要包括内容发布者身份隐私保护和内容请求者检索隐私保护两类。

4.2.1 内容发布者身份隐私保护研究现状

文献[19]和文献[20]分别提出了基于代理的匿名通信技术 Mixmaster 和 Mixminion,利用单个或多个匿名代理节点根据其他节点需求对数据包进行加解密、增加冗余等,从而使得数据包与源节点失去关联。但是,基于匿名代理的方法通信延迟较高。Dibenedetto 等[21]提出了一种隐藏内容名字和数据信息的安全机制——ANDaNA,采用洋葱路由思想对数据包进行加密保护以提供数据包的匿名性并实现网络的隐私保护。ANDaNA 对一个转发路径中的数据包进行多次加密,这些加密的数据包分别由转发路径中的某一个中继路由器进行解密,最终到达数据包的最终接收方。该机制虽然能够有效保护用户隐私信息,但是数据转发过程中的多次加解密会导致传输时延的增加。图 4 表示使用 ANDaNA 机制后的下载时间与使用前的下载时间比,其中 ANDaNA-A 和 ANDaNA-S 分别表示采用基于非对称加密和采用基于会话加密。由图 4 可以看出,内容越大,使用 ANDaNA 带来的延时也越大。

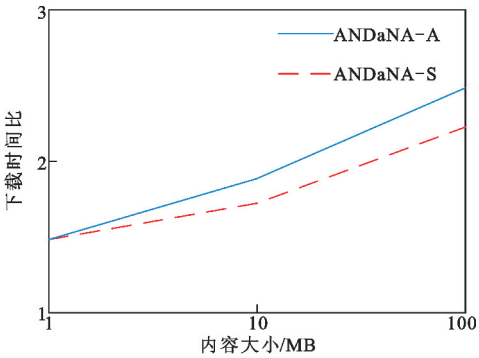

图 4 使用 ANDaNA 前后的下载时延对比图

Fig. 4 Comparison of download time over ANDaNA with respect of baseline

4.2.2 内容请求者检索隐私保护研究现状

文献[19]提出了泛在缓存中存在的 3 种隐私攻击模式,并分别分析了攻击执行的条件和具体流程。文献[20]进一步分析了网络性能与用户隐私的关系,表明用户隐私泄露(特别是内容请求者检索隐私泄露)与缓存策略存在紧密联系。为降低内容请求者检索隐私泄露风险,Mohaisen[22]提出了基于随机延迟的隐私保护方式(Generate Random Delay,GRD),通过对就近缓存内容的响应时间附加额外时延,以使攻击者不能依据数据响应时间执行缓存内容探测,防止信息泄露。但是该方案增大了用户请求时延,导致网络缓存就近响应带来的低时延优势无法发挥。文献[9]指出,在缓存策略设计时,可以通过局部节点的协作缓存,增大请求者的匿名集合,实现用户隐私保护,但是文中并没有给出具体的实现机制。葛国栋等[23]在此基础上,给出了一种基于协作缓存的隐私保护方法(Collaborative Caching Strategy for Privacy Protection,CCSPP),通过构建空间匿名区域、扩大用户匿名集合来增大缓存内

容的归属不确定性,在进行缓存决策时,依据匿名区域对请求内容的整体需求程度,将应答内容存储在沿途活跃度最高的热点请求区域。在保护用户检索隐私的同时,具有更低的平均请求时延,如图 5 所示。

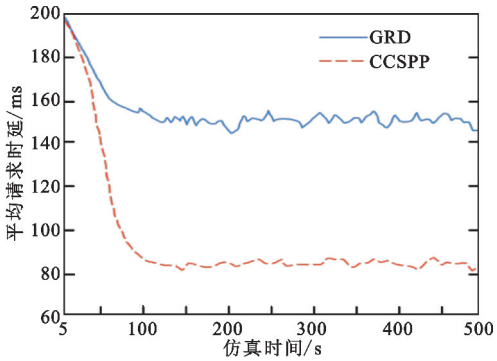

图 5　平均请求时延对比

Fig. 5 Comparison of average request delay between CCSPP and GRD

目前,CCN 中已有的隐私保护方案主要是通过隔断请求者身份与请求者行为、发布者身份等之间的关联,增加匿名区域来实现的。但是,已有方案没有区分用户需求、内容类型等对隐私保护的需求,而在实际中不同用户、不同内容具有不同等级的隐私保护要求。例如,高级用户、隐私内容具有更高的隐私保护要求。因此,需要进一步研究新的隐私保护技术,从而能够根据用户需求、内容类型等因素对用户隐私信息进行自适应保护。

4.3　兴趣包泛洪攻击对抗技术研究

4.3.1　IFA-F 攻击对抗策略

文献[24]设计了 3 种 IFA-F 攻击对抗策略:基于接口公平性的令牌桶机制、基于内容获取成功率的兴趣包接收机制和基于内容获取成功率的反向反馈机制。但上述对策均基于路由器接口来区分兴趣包,而不区分同一接口的兴趣包的不同名字前缀信息,这导致对与恶意兴趣包从路由器同一接口进入、具有不同名字前缀的合法兴趣包准入速率的错误压制。Dai 等[25]提出了一种兴趣包回溯(Interest traceback)机制,通过伪造并回复恶意兴趣包请求的数据包,使路由器待定兴趣表中的非法条目因收到对应数据包而得以被清空,并反向定位到接入路由器,从而在接入路由器入口处基于路由器接口粒度限制 IFA-F 恶意兴趣包的准入速率。然而,该机制仅基于待定兴趣表占用率一项指标来探测 IFA-F 攻击,在突发网络流量存在的情况下会造成较高的误报率。Compagno 等[26]提出了一种缓解兴趣包泛洪攻击的机制,即基于路由器不同接口处兴趣包成功获取到对应内容的概率值,调整路由器对应接口的兴趣包准入速率来抑制 IFA-F 攻击的危害,但其兴趣包速率限制仍然基于路由器接口粒度,不同之处仅在于探测阶段除了考虑兴趣包内容获取成功率之外,还将路由器待定兴趣表占用率作为 IFA-F 攻击探测指标。

上述对策均基于路由器待定兴趣表占用率、待定兴趣表中兴趣包条目内容获取成功率中的一项或多项信息来进行攻击探测,且均不区分兴趣包所携带的不同内容名字前缀信息,而只基于路由器接口粒度限制恶意兴趣包的准入速率,容易造成对合法兴趣包准入速率的错误限制。

4.3.2　IFA-R 攻击对抗策略

目前,针对 IFA-R 攻击的相关研究文献较少。

王凯[27]在其博士论文中对 IFA-R 攻击及其对策进行了深入研究,首次使用 ndnSIM 评估了 IFA-R 的危害效果,并在此基础上提出了一种基于探测周期内路由器待定兴趣表超时条目数量阈值和网络接口数据流量阈值的“双阈值”IFA-R 攻击探测方法:通过动态监测路由器待定兴趣表条目的超时速率以及早发现网络流量异常情况,并通过比较路由器接口探测周期内返回的数据最大流量与该接口对应网络链路限定带宽之间的大小关系,以判定出实际拥塞链路,从而实现对 IFA-R 攻击的探测,为内容中心网络采取必要的 IFA-R 攻击防护措施提供前期预警。

丁锟[28]在分析 IFA 攻击特征的基础上,提出了分布式监测机制,使数据包在网络节点之间进行传输时,能够带有最初网络节点的标识,以方便对兴趣包泛洪攻击的分布式特性进行监测;并提出重传转发机制来重传因误判而被丢弃的正常兴趣包,从而保证正常包的传输。此外,唐建强[29]提出了基于前缀识别的兴趣包泛洪攻击防御方法,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,相邻节点采用基于和式增加积式减少(Additive Increase Multiplicative Decrease,AIMD)的方法限制发送异常前缀兴趣包。该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,但是该方法计算开销较大。

表 2 对比分析了几种兴趣包泛洪攻击对抗方法。

表 2 兴趣包泛洪攻击对抗方法对比
Tab. 2 Comparison of the mitigating interest flooding attack schemes

所提方法	攻击检测方法	检测粒度	对抗方法	对抗粒度	部署位置
文献[24]	兴趣包满足率	异常接口	基于兴趣包满足率的速率限制	按接口限制	全网路由器
文献[25]	PIT 使用率	异常名称	边界路由器限制	按攻击者限制	特定位置
文献[26]	PIT 使用率和兴趣包满足率	异常接口	动态阈值	按接口限制	全网路由器
文献[27]	兴趣包过期率	异常前缀	基于 FIB 的速率限制	按前缀限制	内容提供者
文献[28]	PIT 使用率、兴趣包未响应率和地域分布率	异常前缀	重传转发兴趣包	按 PIT 表项限制	全网路由器
文献[29]	PIT 使用率和兴趣包满足率	异常前缀	基于 AIMD 的异常前缀速率限制	按前缀限制	全网路由器

由以上分析可知,当前兴趣包泛洪攻击对抗方法主要是通过将 PIT 使用率、兴趣包满足率等与某一阈值进行对比来检测是否受到攻击,并在此基础上对兴趣包转发进行限制。虽然现有方法能够在一定程度上降低兴趣包泛洪攻击的影响,但是仍有许多问题没有得到解决。例如:PIT 使用率、兴趣包满足率等阈值的确定;现有对抗技术都是在攻击已经对网络造成负面影响的情况下提出的,缺乏良好的预防措施。因此,还需要针对现在对抗技术的不足进行深入研究。

5 总结与展望

内容中心网络作为一种“革命式”的未来互联网设计思路,正成为下一代 Internet 体系结构的研究热点。内容中心网络直接依据内容的名字完成信息的分发和获取,支持内容数据的泛在缓存,能够有效提高网络内容的分发效率;网络中传输的兴趣包/数据包不携带用户的位置或身份信息,且数据包中含有验证信息,具有一定的安全优势。然而,内容中心网络仍面临非授权接入、用户隐私泄露和兴趣包泛洪攻击等安全问题。本文通过深入 CCN 网络的工作原理,系统分析 CCN 面临的安全风险,并总结各种安全风险的解决对策及其优缺点,从而为相关领域的研究人员提供参考和帮助。

尽管目前已有许多科研工作者对 CCN 中的安全问题进行了研究,且取得许多有价值的研究成果,但仍存在一些未解决的问题需要进一步地研究和完善。

(1)无线内容中心网络中的安全问题研究

随着用户终端和接入网络的移动化、宽带化,越来越多的用户会采用无线终端获取通信业务,无线环境也必然成为 CCN 应用的主要场景之一。由于无线网络中的终端移动、信道动态变化等特点,当前有线 CCN 中安全问题的研究成果难以直接应用到无线环境。如何针对无线 CCN 的特点和安全需求,研究保障安全、可靠、可控数据传输的安全对策是需要进一步研究的问题之一。

(2)复杂网络拓扑下的安全问题研究

当前研究主要是在简单网络拓扑下进行的,虽然简单网络拓扑下的分析模型可用于粗略地分析安全攻击所造成的网络危害效果,但复杂网络拓扑下的危害分析却无法借助上述模型完成。因此,如何科学地建立复杂网络拓扑下的各种攻击安全性分析模型,全面地分析各种攻击的危害,是未来的研究方向之一。

(3)安全对策的原型实现和应用

已有研究主要基于理论分析和网络仿真方式,为进一步验证各安全策略的有效性和实用性,需要搭建真实的网络环境来测试各安全策略的性能。

参考文献:

[1] KOPONEN T, CHAWLA M, GON C, et al. A data-oriented(and beyond) network architecture[C]//Proceedings of 2007 ACM SIGCOMM Conference. Kyoto, Japan: IEEE, 2007: 181-192.

[2] European Union. Project FP7 4WARD[EB/OL]. [2015

-08-20]. http://www.4ward-project.eu.

[3] European Union. Project PSIRP [EB/OL]. [2015-08-20]. http://www.psirp.org.

[4] JACOBSON V, SMETTERS D, THOMTON J, et al. Networking named content[C]//Proceedings of 2009 ACM 5th International Conference on Emerging Networking Experiments and Technologies. Rome, Italy: ACM, 2009: 1-12.

[5] 林涛,唐晖,侯自强. 内容感知网络架构[J]. 中兴通讯技术,2011,14(2):7-9.
LIN Tao, TANG Hui, HOU Ziqiang. Content aware network architecture[J]. ZTE Technology Journal, 2011, 14(2): 7-9. (in Chinese)

[6] DETTI A, CAPONI A, TROPEA G. On the interplay among naming, content validity and caching in information centric networks[C]//Proceedings of 2013 IEEE Global Communications Conference (Globecom). Atlanta, USA: IEEE, 2013: 2108-2113.

[7] BARI M, CHOWDHURY S, AHMED R. A survey of naming and routing in information-centric networks[J]. IEEE Communications Magazines, 2012, 50(12): 44-53.

[8] WANG J, BENSAOU B. Progressive caching in CCN[C]// Proceeding of 2012 IEEE Global Communications Conference (Globecom). Anaheim, CA: IEEE, 2012: 2727-2732.

[9] TAMOI S, KUMWILAISAK W, JI Y. Optimal cooperative routing protocol based on prefix popularity for content centric networking[C]//Proceedings of 2014 IEEE 39th Conference on Local Computer Networks (LCN). Edmonton, AB: IEEE, 2014: 414-417.

[10] KIM D, LEE J. CCN-based virtual private community for extended home media service[J]. IEEE Transactions on Consumer Electronics, 2011, 57(2): 532-540.

[11] JEONG T, HONG J. Content-centric networking for telematics services[C]//Proceedings of 2013 IEEE 4th International Conference on the Network of the Future (NOF). Pohang, Korea: IEEE, 2013: 1-3.

[12] 周自飞,谭小彬,牛玉坤,等. 信息中心网络中授权视频访问控制[J]. 电信科学,2014(9):53-60.
ZHOU Zifei, TAN Xiaobin, NIU Yukun, et al. Access control for authorized viedo in information-centric networking[J]. Telecommunications Science, 2014(9): 53-60. (in Chinese)

[13] YI C, AFANASYEV A, MOISEENKO I, et al. A case for stateful forwarding plane [J]. Computer Communications, 2013, 36(7): 736-749.

[14] WIDJAJA I. Towards a flexible resource management system for content centric networking[C]//Proceedings of 2012 IEEE International Conference on Communications. Ottawa, Canada: IEEE, 2012: 2634-2638.

[15] HAMDANE B, SERHROUCHNI A, FATMI S. Access control enforcement in named data networking[C]//Proceedings of 8th International Conference for Internet Technology and Secured Transactions (ICITST). London: IEEE, 2013: 576-581.

[16] HAMDANE B, MSAHLI M, SERHROUCHNI A, et al. Data-based access control in named data networking[C]//Proceedings of 9th International Conference on Collaborative Computing: Networking, Applications and Worksharing. Austin, Texas, USA: IEEE, 2013: 531-536.

[17] LI Q, ZHANG X, ZHENG Q, et al. LIVE: lightweight integrity verification and content access control for named data networking[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(2): 308-320.

[18] WANG Y, XU M, FENG Z. Session-based access control in information-centric networks: design and analyses [C]//Proceedings of 2014 IEEE International Performance Computing and Communications Conference (IPCCC). Austin, TX: IEEE, 2014: 1-8.

[19] Mixmaster protocol[EB/OL]. [2015-08-20]. http://www.abditum.com/mixmaster-spec.txt.

[20] DANEZIS G, DINGLEDINE R, MATHEWSON N. Mixminion: design of a type iii anonymous remailer protocol[C]// Proceedings of the Symposium on Security and Privacy. Berkeley, CA, USA: Springer, 2003: 2-15.

[21] DIBENEDETTO S, GASTI P, TSUDIK G, et al. ANDaNA: anonymous named data networking application[C]//Proceedings of the Network and Distributed System Security Symposium. San Diego, USA: IEEE, 2012: 1-18.

[22] MOHAISEN A, ZHANG X, SCHUCHARD. Protection access privacy of cached contents in information centric networks[C]//Proceedings the ACM SIGSAC Symposium on Information, Computer and Communications Security. Hangzhou: ACM, 2013: 173-178.

[23] 葛国栋,郭云飞,刘彩霞. 内容中心网络中面向隐私保护的协作缓存策略[J]. 电子与信息学报,2015,37(5):1220-1226.
GE Guodong, GUO Yunfei, LIU Caixia. A collaborative caching strategy for privacy protection in content centric networking [J]. Journal of Electronics & Information Technology, 2015, 37(5) 1220-1226. (in Chinese)

[24] AFANASYEV A, MAHADEVAN R, MOISEENKO I. Interest flooding attack and countermeasures in named data networking[C]//Proceedings of IFIP Networking 2013. New York, USA: IEEE, 2013: 1-9.

[25] DAI H, WANG Y, FAN J, et al. Mitigate DDoS attacks in

NDN by interest traceback[C]//Proceedings of 2013 IEEE Conference on Computer Communications Workshops(INFOCOM WKSHPS). Turin, Italy: IEEE, 2013: 381-386.

[26] COMPAGNO A, CONTI M, GASTI P, et al. Poseidon: mitigating interest flooding DDoS attacks in named data networking[C]//Proceedings of the 38th IEEE Conference on Local Computer Networks. Sydney, Australia: IEEE, 2013: 630-638.

[27] 王凯. 内容中心网络兴趣包泛洪攻击对策研究[D]. 北京:北京交通大学,2014.
WANG Kai. Research on countermeasures for interest flooding attacks in content-centric network[D]. Beijing: Beijing Jiaotong University, 2014. (in Chinese)

[28] 丁锟. 命名数据网络中兴趣包泛洪攻击与防御对策的研究[D]. 北京:北京交通大学,2015.
DING Kun. Research on the countermeasure of interest flooding attack in named data networking[D]. Beijing: Beijing Jiaotong University, 2015. (in Chinese)

[29] 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,2014,36(7):1735-1742.
TANG Jianqiang, ZHOU Huachun, LIU Ying, et al. Mitigating interest flooding attack based on prefix identification in content-centric networking[J]. Journal of Electronics & Information Technology, 2014, 36(7): 1735-1742. (in Chinese)

作者简介:

霍跃华(1981—),男,山西晋中人,2007 年获硕士学位,现为工程师,主要研究方向为网络通信、图像识别;

HUO Yuehua was born in Jinzhong, Shanxi Province, in 1981. He received the M. S. degree in 2007. He is now an engineer. His research concerns network communication and image recognition.

Email: huoyh@ cumtb. edu. cn

刘银龙(1981—),男,安徽宿州人,2011 年获博士学位,现为副研究员、硕士生导师,主要研究方向为未来网络、无线通信和大数据。

LIU Yinlong was born in Suzhou, Anhui Province, in 1981. He received the Ph. D. degree in 2011. He is now an associate researcher and also the instructor of graduate students. His research concerns future network, wireless communication and big data.

Email: liuyinlong@ iie. ac. cn