DOI 10.15302/J-SSCAE-2020.06.017

基于雾计算的信息中心网络防火墙技术研究

刘毅，李建华

（上海交通大学网络安全技术研究院，上海 200240）

摘要：信息中心网络（ICN）通过提供面向信息本身的网络协议，包括以内容为中心的订阅机制和以语义主导的命名、路由和缓存策略，在解决当前基于IP地址联网模式的攻击问题方面展现出极大的潜力。本文旨在为ICN提出一种智能防火墙模型，构建基于语义推理的内容隔离防火墙，运用基于雾计算的ICN防火墙技术，感知来自ICN的内容威胁，并针对不同内容生成定制的过滤策略。在分析ICN面临的攻击类型、梳理ICN中雾计算架构发展情况的基础上，从内容防御整体结构、面向主机的单体防御雾模型、面向网络的区域防御雾模型三方面阐述了基于雾计算的ICN防火墙架构；同时为缓解兴趣洪泛攻击，提出了一种面向ICN的检测及防御机制。搭建ndnSIM网络仿真平台，完成了对ICN的缓存命中率、网络通信时延的性能评估，验证了基于雾计算的ICN防火墙技术及相关防御算法的可行性和高效性。

关键词：信息中心网络；雾计算；兴趣洪泛攻击；防火墙

中图分类号：TP3　　**文献标识码：**A

Fog Computing-Based Firewall in Information-Centric Networking

Liu Yi, Li Jianhua

(Institute of Cyber Science and Technology, Shanghai Jiao Tong University, Shanghai 200240, China)

Abstract: The information-centric network (ICN) provides network protocols oriented to information itself, including a content-centric subscription mechanism and semantic-led naming, routing, and caching strategies. It has shown great potential in solving attacks on current IP address based network. This paper aims to propose a smart firewall model for ICN, and to build a firewall based on a semantic inference algorithm to isolate content. The ICN firewall module uses the fog computing paradigm to sense content threats from ICN, and generates customized filtering strategies for different contents. On the basis of analyzing the types of ICN attacks and the development of the fog computing architecture in ICN, this article introduces the fog-based ICN firewall model from three aspects: the overall structure of content defense, the host-oriented defense fog model, and the network-oriented defense fog model. This article also proposes an ICN-oriented detection and defense mechanism in order to alleviate the interest flooding attacks. Finally, by building the ndnSIM network simulation platform, this article evaluates the ICN cache hit rate and network communication delay, and verifies the feasibility and efficiency of the proposed fog computing-based ICN firewall module and defense algorithm.

Keywords: information-centric networking; fog computing; interest flooding attack; firewall

收稿日期：2020-09-10；**修回日期：**2020-10-29

通讯作者：李建华，上海交通大学网络安全技术研究院教授，研究方向为网络空间安全；E-mail: lijh888@sjtu.edu.cn

资助项目：中国工程院咨询项目“网络空间安全保障战略研究”(2017-XY-45)

本刊网址：www.engineering.org.cn/ch/journal/sscae

一、前言

随着网络信息技术的不断发展，下一代网络体系结构对高度可扩展组网结构和高效内容分发机制的需求正在急速增长。信息中心网络（ICN）作为未来网络的重要体系架构之一，提供了面向信息本身的网络协议，如以内容为中心的订阅机制和以语义主导的命名、路由和缓存策略，在解决当前基于 IP 地址的联网模式方面的攻击问题时展现出极大的潜力 [1]。

ICN 作为一种新的网络体系结构，安全问题是该体系结构的重要组成部分。ICN 面临的网络攻击主要来自传统网络旧式攻击的变形、当前网络架构的新型内容攻击。因此，在 ICN 中提出符合其自身网络协议及架构的防火墙系统对确保网络安全有着重要作用。目前，关于 ICN 防火墙技术的研究尚处于起步阶段，已有研究多从 ICN 中的流量上下文 [2]、数据包命名 [3] 等角度来研究拦截算法的实现，而从数据内容出发进行语义分析和拦截的研究甚少。基于此，本文从 ICN 的内容语义层面出发，利用语义的相关性作为网络中威胁内容过滤的切入点，构建 ICN 中的语义推理防火墙。

二、ICN 面临的攻击类型

ICN 将安全模型从保护转发路径更改为保护内容，使其可以为所有网络节点使用。ICN 具有位置独立命名、网络内缓存、基于名称的路由、内置安全性等独特属性。在 ICN 体系结构中，除可对网络流量产生影响的旧式攻击外，还出现了新的攻击方式 [4,5]。攻击者增加了对 ICN 网络架构信息流的控制和审查，易于拦截信息，相应的新式攻击主要有命名、路由、缓存和其他攻击 [6]。

（一）命名攻击

自认证命名是引用最多的 ICN 命名方案，由所有者公钥和所有者分配标签的加密哈希组成。元数据包含由所有者签名的完整公钥和数字摘要。命名攻击分为监视列表和嗅探攻击，这些攻击允许攻击者审查和过滤内容。攻击者还可以获取有关内容流行性和用户兴趣的私人信息 [7]。

（二）路由攻击

分布式拒绝服务（DDoS）攻击造成的危害影响最大。传统网络的 DDoS 攻击多表现为，攻击者控制终端系统向网络发送大量恶意请求，耗尽路由设备资源（如内存和处理能力）。而在 ICN 中，攻击者旨在填充 ICN 路由表，为合法用户造成 DDoS 攻击，这类攻击又称为兴趣洪泛攻击。由于攻击者可以针对可用和不可用的内容发送这些恶意请求，被攻击的路由器试图满足这些恶意请求并将其转发到相邻的路由器，从而实现了恶意请求在网络中被传播。在这种情况下，满足合法请求需要较长的响应时间，如果响应时间超过特定阈值，合法请求则不会被满足，最后因合法用户不断重新传输不满意的请求，使得攻击的影响在 ICN 中逐渐放大，造成网络额外过载。

（三）缓存攻击

攻击者不断发送随机或不受欢迎的请求到网络中，通过更改内容流行性来破坏 ICN 缓存是常见的缓存攻击。恶意请求强制缓存系统存储最不受欢迎的内容并驱逐流行内容。通常，当用户首次请求内容时，会响应原始源中的内容；如果其他用户请求相同的内容，第二个用户将从路由器中最近的可用副本（而不是原始源）获取该请求。如果攻击者成功使网络缓存了不需要的内容，第二个用户请求相同内容时，将从原始数据源获取内容，而不是最近的可用副本；在攻击情况下，第二个用户的请求将在整个路径中作为第一个用户的请求。

三、基于雾计算的 ICN 架构特性

雾计算是一种新兴的计算范式，用于分散化云计算中的处理、存储和控制服务，使其更接近终端用户；作为一种新的计算趋势，与云计算一起为用户提供更高质量、更低延迟的服务，为网络用户带来诸多新体验。融合雾计算模式的 ICN 是一种新型网络架构，通过基于雾层的水平数据传输、在雾节点之间的分布式处理、内置的移动性支持来丰富应用程序。基于雾计算的 ICN 架构具有以下特点。

（一）弱化 ICN 中应用程序对云端支持的依赖

数据可以由本地 / 非本地雾节点的缓存存储，

不必从云节点中获取，因而可将信息中心网络 – 雾计算（ICN–Fog）结构视为分布式协作缓存池。这是 ICN–Fog 的特殊优势，相比之下传统的雾模式只能使用终端设备所连接的本地 / 垂直雾节点的缓存存储。

（二）支持异构终端设备

由于不需要在终端设备中部署 ICN 协议，ICN–Fog 并不依赖终端设备的功能和资源限制，可以接受更广泛的设备种类，且设备仅需连接到本地雾节点上。可以认为，雾节点充当了终端设备的代理，来自终端设备的请求将转换为网络请求，并在 ICN–Fog 内部转发或直接发送到云。对于终端设备生成的数据，雾节点将之存储在缓存存储区中，并发布到 ICN 中供以后使用。

（三）内置用户 / 设备移动性功能

用户 / 设备移动性是 ICN 的内置功能，这归功于接收器驱动的无连接数据通信特性。当终端设备移动到新位置并连接到新的雾节点时，只需要重新发送其感兴趣数据的请求即可。为支持消息生产者的流动性、避免因流动性丢失请求数据，实际应用中需要更加详尽的解决方案。

四、基于雾计算的 ICN 防火墙架构

基于雾计算的 ICN 防火墙架构，利用雾计算的内容感知、地理感知实现了对网络流量的智能识别和细粒度覆盖，以便结合区域内节点数据进行本地运算，进而节省计算和通信成本。具体来看，该防火墙架构中的内容防御整体架构，通过将雾节点部署在网络入口以及连接处，实现了对网络边缘的覆盖。ICN 中面向主机终端设备和网络整体的隔离模式，通过部署基于主机的单体雾防火墙节点和基于网络的区域雾防火墙节点，实现了对相关攻击的防御。

（一）基于雾计算的内容防御整体架构

利用雾计算构建边缘内容防御系统，分为面向主机、网络攻击的两类防御机制。①主机防御雾节点构造在 ICN 主机和网络之间，可实现主机在地理上的无缝覆盖，防止恶意数据进入 ICN，并且每个主机处于一个对应的雾节点的管辖范围内；雾节点的计算显著减轻了配置防御机制主机的负担。②网络防御雾节点连接了不同级别的安全网络，隔离了内外网之间的通信以防止恶意数据在网络之间传播；ICN 的网络防御部署在网关旁边的雾节点上，物理网关会将来自网络内部、外部的数据路由到网络防御雾节点中。

基于雾计算的 ICN 防火墙内容防御场景如图 1 所示。ICN 节点作为终端部署在整个网络的边缘和底层，充当数据创建者来生成数据。由于许多终端无法暴露防火墙服务所需的计算和存储，终端无需配备防火墙。在雾节点上部署防火墙，可以帮助防火墙系统进行更全面的分析，不仅可以发现节点，还可以发现覆盖本地网络的威胁。

雾计算节点部署在 ICN 的中间层，既是“桥梁”，又是安全隔离系统。针对车辆和企业内部网络的不同攻击，可采用两种边缘防御隔离方法。①在 ICN 终端和网络之间构建终端隔离，利用传统终端防火墙优势，隔离终端和 ICN 之间的非法通信；终端隔离在终端和 ICN 节点的下一跳之间部署，以防止恶意数据进入 ICN；至于物理部署，将其放置在可以实现终端无缝覆盖的地理区域上，使每个终端都在一个相应的防雾墙的管辖范围内；雾节点的计算明显降低配置防火墙终端的负担。②建立防止恶意数据在不同 ICN 网络之间传播的网络隔离，考虑了连接不同级别安全网络的传统网络边界，以隔离内网和外网之间的通信；在 ICN 中，网络隔离部署在网关下游的雾节点上，处理转发自物理网关中的数据。

（二）ICN 中面向主机的单体防御雾模型

主机雾防火墙是基于文献 [8,9] 中提出的 7 层雾计算模型所设计（见图 2）：从终端发送的数据包，首先被主机雾防火墙的监视层获取，并在上下文感知层中进行解析以提取组件；然后在策略层中分析兴趣数据包，生成定制化过滤策略；过滤层使用已知和动态的各兴趣包定制过滤策略进行拦截；安全层将定制的策略附加到兴趣包中，并随之在网络中路由，到达对应生产者的主机防火墙中，并被提取和更新到黑名单中。因此，当数据包在其他节点中缓存时，过滤策略可以重复使用，在节点的内置数据库中获取，随后路由层将新数据包转发

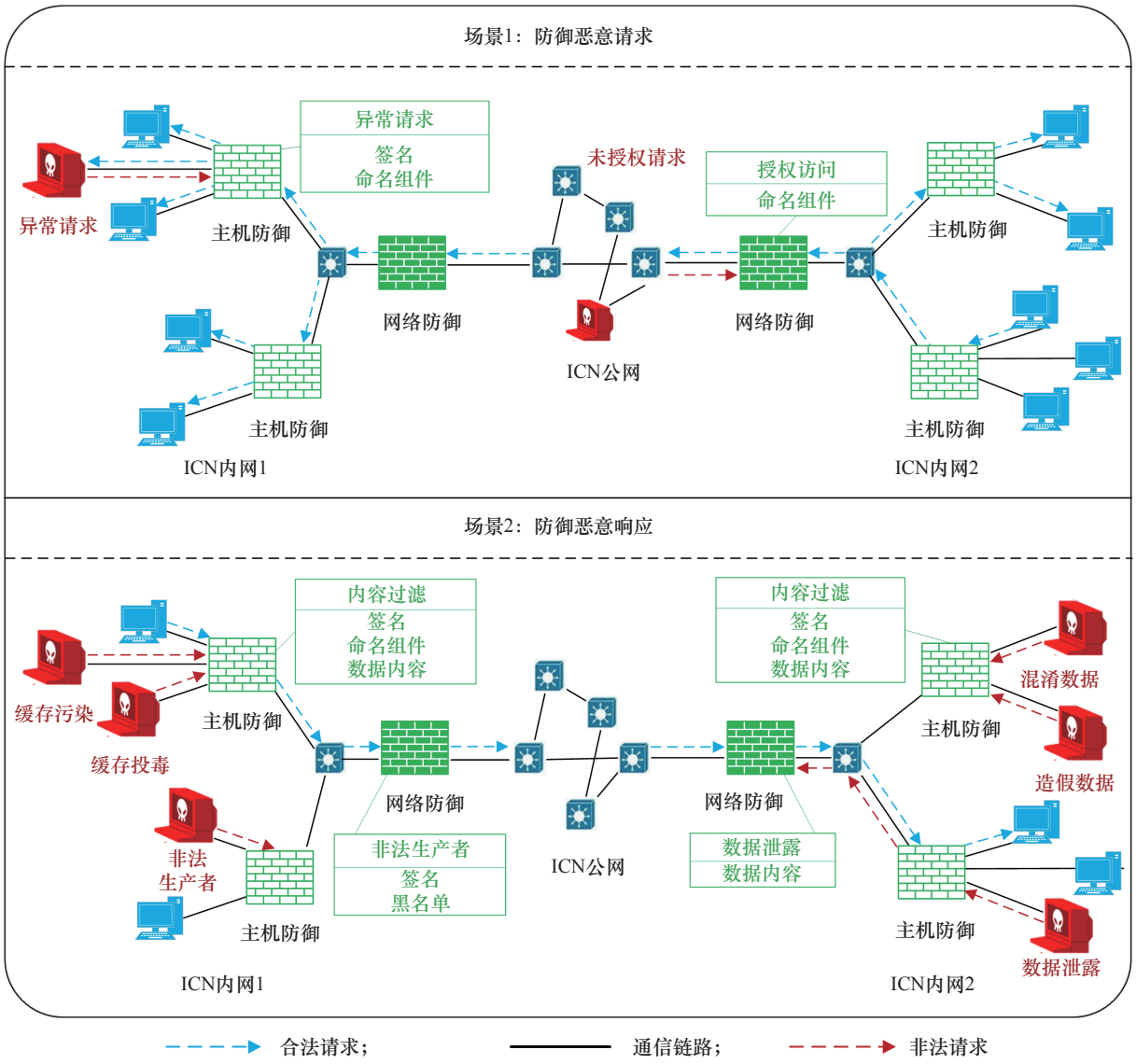

图 1　基于雾计算的 ICN 防火墙内容防御场景

到下一跳。

1. 监视层

监视层检索并记录每个 ICN 节点的所有通信行为，监视对象包括终端、网络拓扑、活动和资源。主机雾防火墙可以访问每个 ICN 节点的所有请求、响应和设备属性，有助于感知用户行为和上下文流量。在监视层中获得的数据、有关设备属性和位置信息的数据放置在网络数据库中，有关通信活动记录的数据放在日志数据库中。

2. 上下文感知层

上下文感知层解析数据包并提取每个数据包的组成部分，包括数据包名称、选择器和转发提示。选择器引用指定的发布者密钥，但不包括响应名称信息；转发路径代表转发对象的授权列表。总之，将数据包的名称、签名、转发信息和内容的组成部分提取到数据库中。

3. 策略层

策略层为不同的数据包动态配置自定义的过滤策略，由关联上下文分析、语义推理、用户配置的策略提取 3 个模块组成。对于兴趣包，选择关联上下文，计算关联权重矩阵以指导推理方向；随后策略层在请求名称和黑名单之间进行语义推理，利用

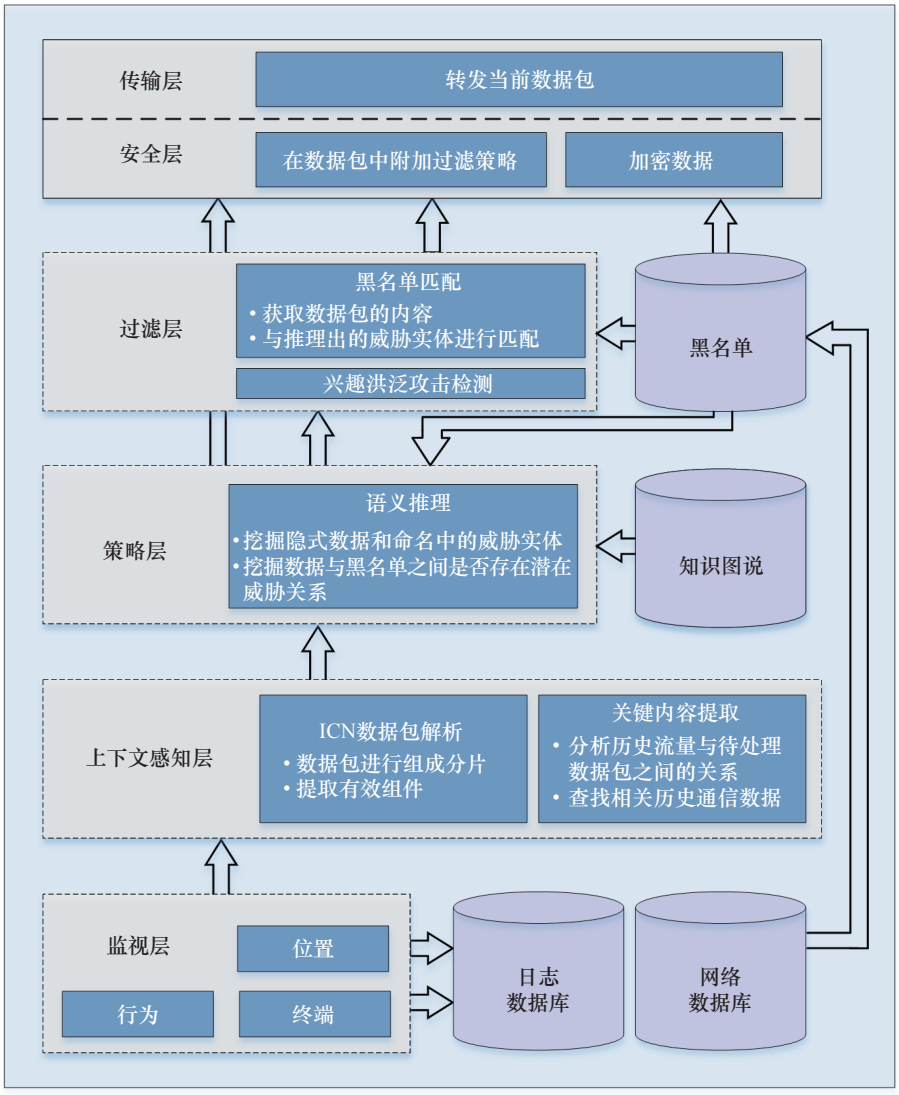

图 2　主机雾防火墙架构

推理构造安全知识策略、发现相关的新实体以扩展黑名单。此外，用户配置的过滤策略是通过组合提取的数据包组件生成的，其中的选择器组件用于限制生产者身份并排除数据包名称，而转发路径用于控制数据包传输。某个特定兴趣数据包的所有策略都可称为兴趣特定策略（ISP）。

4. 过滤层

在过滤层中，对于兴趣数据包需要检查其完整性和有效性，防止恶意节点篡改请求和 ISP；执行基于黑名单的内容匹配来防止异常请求。对于接收到的数据包，其完整性、有效性授权以及用户配置的策略匹配与内容过滤器是有序实现的。过滤层仅对兴趣包名称进行过滤并进行正式的恶意请求检测，而对数据包中的整个内容进行过滤用于防止非法、混淆和虚假的内容攻击。

5. 安全层

安全层由标记模块和加密模块组成。标记模块从策略层添加一个新的 ISP，标记感兴趣的数据包，使用有理由的受威胁实体扩展黑名单，因此其他 ICN 节点在缓存兴趣数据包时可以获取 ISP。相关的主机雾防火墙也可以在监视层中获取 ISP，并将其放置在黑名单数据库中。加密模块为标记的兴趣数据包进行加密，随后传输层将新的数据包转发。

（三）ICN 中面向网络的区域防御雾模型

网络雾防火墙是为防止来自受保护的内网和外网的未经授权访问导致最高数据泄漏而设计的。与主机雾防火墙不同，网络雾防火墙中没有安全层，

路由到网络边界的兴趣数据包已经在其主机雾防火墙中解析为生成的 ISP。

网络雾防火墙的工作流程为：①来自内网和外网的数据包在监视层中接收，记录在不同的数据库中；②数据包在知识分析图的上下文分析层中进行处理，当接收到兴趣分组时，从分组数据库考虑并获取相关的通信上下文；③策略层包含语义推理模块，用于从数据包名称、上下文通信和黑名单之间的关系中找出可能的潜在非法实体；④超出访问权限的外网请求将在过滤层中被拦截，过滤层还检测带有黑名单的发送到外网的数据包，以防信息泄漏；⑤传输层将数据包转发到 ICN。

五、面向 ICN 的兴趣洪泛检测机制

为缓解兴趣洪泛攻击，本文提出了一种面向 ICN 的检测及防御机制：通过在防火墙中收集边缘路由器各接口上对不同名称前缀的兴趣满足率，识别恶意前缀或恶意接口，然后根据不同情况将其丢弃或放慢速度；检测和缓解措施在边缘路由器上执行，边缘路由器直接连接到攻击者，可以快速检测到攻击、更有效地缓解攻击。

（一）ICN 中兴趣洪泛攻击的常见方式

近年来，DDoS 攻击和拒绝服务（DoS）攻击越来越普遍，造成了重大损失。在 DDoS 攻击中，攻击者利用大量受感染的宿主（僵尸）发动攻击；DDoS 攻击易于实例化、技术要求低，但对其防御与缓解却不易。在当前基于 IP 的网络中，DoS 攻击是一种简单有效的攻击，通过各种方式消耗网络带宽和系统资源，使网络无法为正常用户提供服务。得益于超前的架构设计，ICN 可以抵御目前 IP 网络中的许多常见类型 DoS 攻击，如带宽消耗、反射攻击、前缀劫持黑洞等。

ICN 中存在一种新型的 DoS 攻击，称为兴趣洪泛攻击。通过兴趣包洪泛攻击，恶意用户将发送大量相同或不同的兴趣数据包。当攻击者发送大量相同的兴趣包时，由于这些兴趣包会被汇总并最终存储一个数据包，因此 ICN 可以抵御此类攻击；但如果攻击者发送了大量具有不同内容名称的请求时，待处理兴趣表会将这些兴趣包保留，而不会将这些兴趣包汇总，因此 ICN 无法抵御此类攻击。

（二）基于请求满意度以及请求速率的攻击检测门限值模型

该模型基于边缘路由中的请求速率和请求满意度预测兴趣洪泛攻击，计算边缘路由节点在正常状态下的性能状态并将之作为判断攻击发生与否的准则。在计算阈值时，首先假设在此计算过程中没有恶意请求，即研究合法用户的正常行为，含请求速率（*RR*）、请求满意率（*RSR*）。*RR* 即边缘路由节点接口每秒收到的兴趣包平均数，*RSR* 即边缘路由节点接口每秒收到的兴趣包中被响应的比例，两者能够表示路由节点的当下请求状态与过去收到请求之间的关联程度。

一般认为，一个区域内的用户节点在时间上的行为会表现出因果性，同时个体之间会存在一定程度上的请求关联，即某个用户在一定时间内的请求内容存在一定可能性的相似规律或因果性；相同区域内的用户之间也可能存在这类关系。因此，在出现多种指标都在阈值合理范围之外的情况时，可以判定出现了兴趣洪泛攻击。

根据合法用户的 *RR*、*RSR* 得到相应的请求门限值，即最高合法 *RR* 值、最低合法 *RSR* 值。对于数据集中的每个时隙（样本），每个 ICN 路由节点都会记录不同接口的 *RR*、*RSR*。对于每个样本，每个边缘路由都会计算最大 *RR* 值、最小 *RSR* 值。对于所有样本，边缘路由分别计算每个指标的平均值和标准差，从而得到相关阈值。计算过程如下：在最大阈值情况下，阈值在平均值基础上上调一个常数与标准差的乘积；在最小阈值情况下，阈值由在平均值中下浮标准差与常数乘积的量值；通过常数值乘以标准偏差，可以检测出阈值与计算出的平均值之间的差值。

使用以上的门限值可以在检测和预防阶段中有效定义攻击者的行为。请求速率、请求满意度门限值从不同的角度监视攻击者，并将其与合法行为进行比较。对于攻击者而言，在门限值的合法范围内进行有效攻击会变得极其复杂和艰难，使得攻击变得徒劳无功。

六、实验测试与评估

利用 ndnSIM 网络仿真平台，本文搭建了基于雾计算的智能防火墙网络测试环境，通过对网络拦

截争取率、请求满意率、缓存命中以及端到端实验进行评估，验证内容和 DDoS 防御机制的可行性、可扩展性和效率。

（一）防火墙防御兴趣洪泛攻击评估

为评估兴趣洪泛攻击检测机制的性能，在网络拓扑基础上进行洪泛攻击检测实验。为了观察攻击者对边缘路由和与其在同一范围内的合法消费者的直观影响，将拓扑中攻击者和合法消费者的身份关系改为交替存在。

本实验中有两类请求数据库：从 WordNet 18 数据库中选取 300 个三元组作为合法内容，即生产者中存在所选的 300 个三元组中的尾实体，当消费者发送相应的头实体作为兴趣包时，生产者可以响应消费者的请求；从 WordNet 18 中随机选取的与上述实体中存在跨度关系在 10 跳以上的 100 个实体，作为网络中不存在的数据，构成攻击数据库。实验中，合法消费者的请求兴趣包频率为每秒 15 个请求，每个区域的消费者随机在合法数据库中选取三元组头实体并发送请求。

从实验评估结果来看（见图 3），随着攻击者发送网络中不存在数据请求数量的增多，防火墙对兴趣洪泛攻击的识别率也随之增加，这是因为不存在的数据请求会导致路由节点的请求满意率显著下降，与阈值偏差变大。另外可以观察到，请求满意度经历了先显著下降再震荡回升的过程。也就是说，随着网络中攻击数据的增加，大量兴趣包涌入导致整个网络的通信负载逐渐增加，造成通信时延增加，从而使网络整体的请求满意率下降。

（二）防火墙防御效率评估

当防火墙进行分析和阻塞时，网络传输延迟会受到影响，这是因为雾防火墙需要覆盖多个终端，当流量变得极其巨大时，内容需要排队等待被过滤。因此，需要评估由雾防火墙模型提供的防御隔离机制的处理效率。

实验中选择端到端通信延迟来评估防火墙对 ICN 通信传输产生的影响，即从消费者发送兴趣包到生产者接收数据包的用时计算得出，包括每个路由节点之间的传输延迟、防火墙和路由节点的处理延迟。实验模拟了防火墙直接部署在雾节点和终端

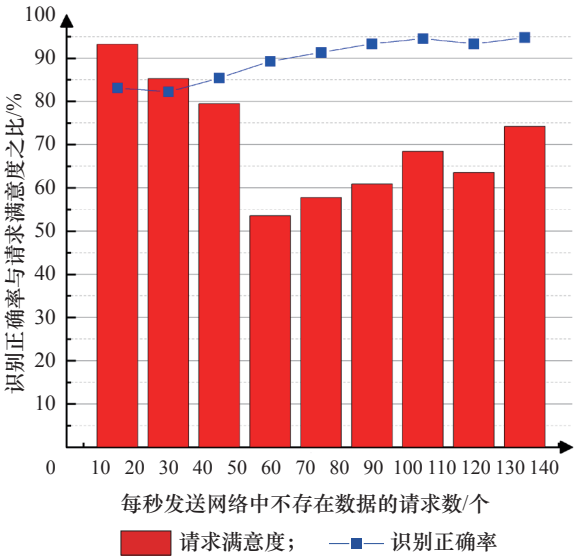

图 3　兴趣洪泛攻击请求满意度及防御正确率

的两种情况，相关网络都设计为具有相同的拓扑、请求和节点，通过更改请求内容的终端频率来获得不同的延迟。

对平均通信延迟进行了统计和比较（见图 4），随着兴趣包请求频率的提高，基于雾计算的防火墙呈现出比终端防火墙更高的处理效率；雾计算防火墙的平均延迟增加得更慢，且几乎比终端部署的防火墙要低。这是因为，尽管雾防火墙可能存在排队现象，但是雾节点提供了至关重要的计算与感知资源来帮助防火墙感知和预测用户的行为、推理防御策略并进行阻止；而通用终端节点无法轻松准确地实行防御，特别是网络流量变大状态；此外部署在终端上的防火墙无法感知附近节点发现的某些威胁，产生了重复的分析时间。

七、结语

为构建针对潜在内容威胁的 ICN 防火墙，本文提出了以内容定向语义推理、基于雾计算的内容威胁防御机制，通过阻止非法内容和意外访问，实现了对内容威胁的边缘防御。仿真结果表明，本文提出的基于雾计算的 ICN 防御机制可以提供高效的隔离防御。内容信息是 ICN 的重要组成部分，在构建 ICN 防火墙防御技术时，从内容信息入手实现全面高细粒度的过滤和拦截，将是后续 ICN 防火墙技术研究的重要发展方向。

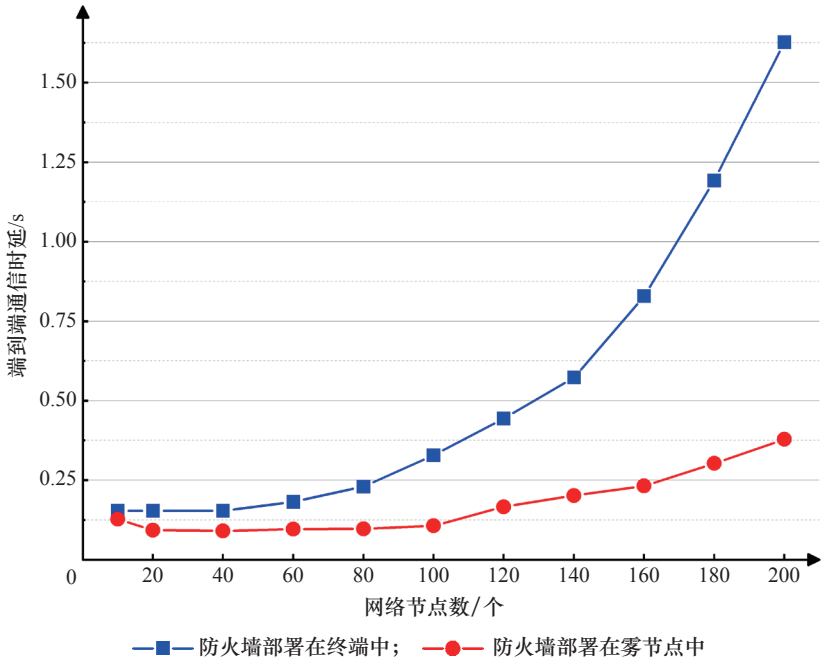

图 4 ICN 端到端延迟比较

参考文献

[1] Arshad S, Azam M A, Rehmani M H, et al. Recent advances in information-centric networking-based Internet of things (ICN-IoT) [J]. IEEE Internet of Things Journal, 2018, 6(2): 2128–2158.

[2] Varas C, Hirsch T. Self protection through collaboration using D-CAF: A distributed context-aware firewall [C]. Glyfada: 2009 Third International Conference on Emerging Security Information, Systems and Technologies, 2009.

[3] Kondo D, Silverston T, Tode H, et al. Name anomaly detection for ICN [C]. Rome: 2016 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), 2016.

[4] La Polla M, Martinelli F, Sgandurra D. A survey on security for mobile devices [J]. IEEE Communications Surveys & Tutorials, 2012, 15(1): 446–471.

[5] Igure V M, Williams R D. Taxonomies of attacks and vulnerabilities in computer systems [J]. IEEE Communications Surveys & Tutorials, 2008, 10(1): 6–19.

[6] AbdAllah E G, Hassanein H S, Zulkernine M. A survey of security attacks in information-centric networking [J]. IEEE Communications Surveys & Tutorials, 2015, 17(3): 1441–1454.

[7] Dannewitz C, Golic J, Ohlman B, et al. Secure naming for a network of information [C]. San Diego: 2010 INFOCOM IEEE Conference on Computer Communications Workshops, 2010.

[8] Zeng D Z, Gu L, Guo S, et al. Joint optimization of task scheduling and image placement in fog computing supported software-defined embedded system [J]. IEEE Transactions on Computers, 2016, 65(12): 3702–3712.

[9] Aazam M, Huh E N. Fog computing: The cloud-IoT\/IoE middleware paradigm [J]. IEEE Potentials, 2016, 35(3): 40–44.