* 导言

互联网的无处不在表明了其巨大成功，并肯定了一个像其过去一样充满希望的未来。 这些年来，应用程序、服务和相关技术的发展在很大程度上决定了我们今天使用互联网的方式。 然而，互联网核心体系结构并没有表现出同样的效果。 事实上，通过协议补丁程序来维持不断增长的安全性、移动性和可用性需求已经变得困难重重。网际网络体系结构与其当前需求之间的这种不匹配极大地推动了人们对一种更好的体系结构的需求，这是一种更动态、更模块化和更适应性的体系结构，以适应我们今天的经验和对未来的展望[99]。

信息中心网络（Information-Centric Network，ICN）范式[25，53]正是通过克服当前的互联网缺陷，将主要网络实体从主机转移到内容，从而在网络层直接请求和路由命名内容，为未来的互联网赢得了学术界和工业界的极大关注。 基本上，ICN模型直接在网络层上使用应用层名称定义内容请求，而不是当前的IP模型，在当前的IP模型中，网络层负责处理机器地址。 ICN方法应该重新考虑Internet基础，并设计一个本机ICN环境，嵌入安全性、移动性支持和缓存等特性。

从安全的角度来看，ICN范式对网络层架构的转变改变了与网络安全相关的许多方面。 命名内容而不是命名方式改变了安全模式，从保护主机和链接到保护内容，因此，命名内容需要真实性和完整性保护机制，以避免众所周知的攻击，如网络欺骗。 此外，命名内容能够将内容与其位置分离，从而允许部署网络内缓存，使得网络中的任何人可以从任何地方检索内容。 尽管这带来了明显的好处，但它也对网络缓存内容的隐私和访问控制提出了新的挑战。

此外，由于路由和转发是通过内容名执行的，因此ICN还提出了有关监视和审查的安全性问题。 很明显，ICN为当前Internet上还未出现的潜在安全威胁提供了便利； 然而，即使是来自Internet的已知攻击也可能破坏ICN体系结构，这一点在应用于ICN特殊性时可能会得到强调。 因此，ICN中的安全性应该以不同于传统网络的方式提供。 因此，需要特别关注ICN中的安全方面，以确保体系结构的鲁棒性，能够满足当前和未来的Internet需求，更重要的是，ICN范式被视为内容出版商的一种可行技术。

本文旨在提供有关网络层直接命名内容所带来的安全威胁及其应对措施的广泛观点和见解。 本文的主要贡献是对ICN安全问题及其可能的解决方案进行了系统的组织、分类和讨论。 本文不为特定的攻击提出新的解决方案； 而是讨论了可能的解决方案，并为有关这些方案的研究提供了参考。 我们期望这篇文章将为更好地理解当前的ICN安全问题打开方向，并为未来的工作提供新的有关威胁和潜在方向的见解。

本研究考虑了三种主要ICN体系结构中的安全威胁:(i)命名数据网络、以内容为中心的网络(NDN/CCN1)、(ii)信息网（Net-INF）和(iii)发布-订阅互联网技术(PURSIT)。 本文反映了在这些ICN体系结构中对安全性的研究量。 由于其中一些结构（如NDN/CCN）比其他结构更受关注，因此对每个体系结构讨论详略不同。 因此，本文讨论的解决方案大多与NDN/CCN体系结构有关。

已经发表了一些其他调查，涉及国际通信网络的安全问题[1，107]。 我们的文章通过分析、分类和组织更多关于ICN安全的论文，并通过对当前研究和观点的深入了解，对它们进行了补充和更新

1CCN是雅各布森（Jacobson）等人提出的最初的ICN体系结构。 [54]。 NDN是一种较新的体系结构[127]，主要受CCN的启发，最初基于相同的代码库（以前称为CCNX，最近更名为NDNX）。 在本文中，我们使用缩写NDN/CCN来表示这两种体系结构，因为它们与本综述相关的特性是等效的。

未来的作品。 提出了一种全新的ICN安全攻击分类和组织方式，为ICN领域的攻击和对策提供了新的视角。 有关ICN体系结构中某些特定攻击的影响及其对安全要求的详细审查，请参阅Abdallah等人的文章。 [1]。

本文的其余部分结构如下:第2节介绍了ICN的主要实体，解释了它们的基本操作（2.1），并介绍了ICN体系结构中可能存在的漏洞和攻击者类型（2.2）。 然后，我们讨论了主要ICN方面的威胁、攻击和措施，分为三大类:内容命名安全（第3节）、路由器安全（第4节）和缓存安全（第5节）。 第6节讨论了ICN安全对有效采用ICN体系结构的挑战和机遇，并列出了未来的研究方向。 第7节提供了最后的评论。

* 以信息为中心的网络

自从互联网问世以来，我们看到我们使用它的方式在不断变化。 在互联网上提供的服务中，内容分发目前是最常用的服务。 事实上，产生实时内容的应用程序，如Netflix和Spotify，代表了全球月流量最高的类别，在北美超过50%，并预计在未来几年会增长[99]。 然而，Internet在有效地分发内容以响应不断增长的通信量方面显示出缺陷，这是通过点对点通信设计用于资源共享的体系结构遗留下来的问题。 事实上，已经提出并部署了应对这种新内容需求的解决方案，例如多播协议、对等网络(P2P)和内容分发网络(CDN)。 然而，这种解决方案是在传统IP网络的基础上叠加而成的，继承了这种协议的局限性。

因特网的低效率也延伸到其他领域[93]:同一数据的多份拷贝正在被传送，导致因特网服务提供商的费用增加；（2）因特网服务提供商的费用增加； IP体系结构中不存在对流量优化的本地支持； 网络拥塞和高传播延迟； 安全重点是连接，而不是内容； 面向连接的协议，防止移动性； 能源管理薄弱，因为需要更多的硬件来执行冗余任务，终端用户交付性能差，尤其是在流媒体流方面。 因此，将Internet体系结构演变为更适合内容分发的体系结构的观点构成了ICN范式背后的主要推动力。 然而，Internet协议(IP)寻址的缺陷不仅推动了这一变化，而且希望将结构嵌入到功能中，以提供适应性、安全性、移动性、自组织性和自然进化性，解决当前的一些问题并预测其他问题。

2.1以信息为中心的网络范式

Jacobson等人将ICN与IP模型进行了比较。 54着重指出两个显著的区别:网络路由的内容和路由的方式。 就路由而言，IP路由器传统上通过网络将IP数据包路由到目的机器，而ICN路由器则应该将对指定内容的请求路由到最佳可用副本。 因此，IP命名计算机，而ICN命名内容。 为了将请求从用户路由到目的机器，IP路由器由路由基础设施（即自治系统）支持，并且请求必须遵循通往目的机器的路由层次结构。 此外，网络节点还通过域名服务(DNS)服务器将用户可读的域名转换为IP地址。 ICN范例还将请求路由到内容发布者； 但是，由于它提供了在路由器中缓存内容的方法，因此这些方法可以满足用户的需要，而不需要请求一直返回到发布服务器。 在ICN中，我们观察到三个不同于传统IP网络的主要域:

1. 命名、(ii)路由和转发以及(iii)缓存。 在下面，我们将突出显示这些域中的每一个。
   * 命名:由于ICN命名的是内容项而不是主机，因此对可伸缩性存在真正的顾虑。 Internet上的内容项比主机多得多，命名方案应该明确标识所有此类内容。 基本上，ICN中的命名方案分为两种主要的方法:平面命名[29]和分层命名[103]。 两者都有优点和缺点:虽然平面命名允许更好的命名持久性，因为它与任何位置或组织无关，但它也限制了路由性能目的的名称聚合。 相比之下，分层命名通过名称前缀层次结构优化路由信息聚合和性能，但共享相同前缀的内容组可能必须由相同的位置一起处理。 它对于在特定上下文中命名内容项也很有用，便于管理操作。 还有属性值命名方案[12]，其中表示内容能力的一组属性被映射到内容名称中。 属性值命名方案主要在移动和物联网环境下进行了研究[90]。
   * *路由和转发:ICN ARCHI中考虑了两种主要的转发方案:*

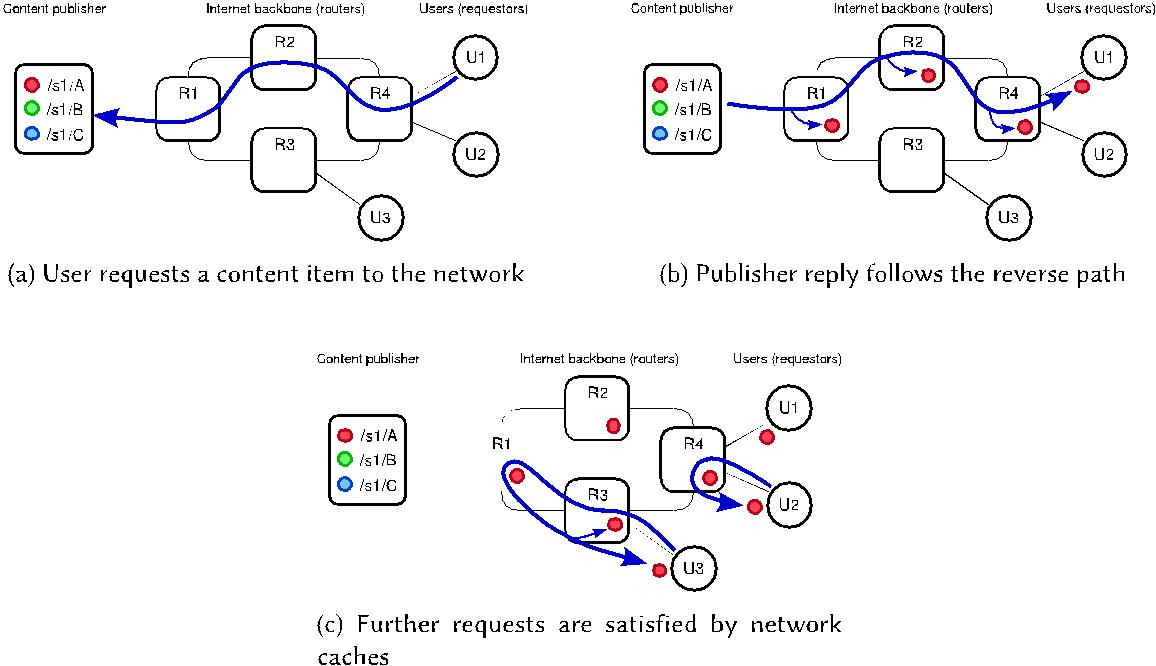
结构:基于名称的路由[54]和支持名称解析服务(NRS)的基于名称的路由[4，25]。 路由器填充有分层前缀和相应的传出接口，并存储请求状态信息以将内容转发回请求者。 使用这种路由方案，路由器直接根据内容名称转发内容。 在支持名称解析服务的路由方案中，路由发现的作用类似于传统的DNS:NRSS将内容名称映射到一组位置； 然后由NRS解析请求，并使用从NRS检索的位置通过基于拓扑的路由协议转发请求。

* + 缓存:针对ICN体系结构提出了三种不同的缓存解决方案:路径上缓存、路径外缓存和对等缓存。 On-Path缓存机会主义地探索本地内容流行度，以优化内容传递。 它根据通过路由器的内容请求数在路由器中缓存内容。 离路缓存由已定义的服务器执行，与现在的CDN非常相似，并且还由内容的流行度来维持。 对等缓存是在移动环境中处理的，在移动环境中，用户的设备可以用作内容缓存，以向附近的设备提供更好的内容可用性。 缓存还通过缓存逐出策略（如最近使用最少(LRU)和使用最少(LFU)）管理内容项的逐出[125]。

迄今为止，已经提出了各种ICN体系结构，例如NDN/CCN[54，127]、NetInf[25]、Pursure[33]和面向数据的网络体系结构(DONA)[62]。 尽管这些体系结构共享相同的基本组件（命名内容、按内容名路由和网络缓存），但它们在实现方面具有特殊性。 在本综述中，我们旨在系统整理有关ICN核心功能漏洞的安全文献； 因此，我们不讨论这种体系结构的特殊性。 在本文中，我们将ICN的原则和要求称为ICN范式。 我们称为ICN体系结构的ICN实例集。 我们认为这一澄清是有效的，因为这种区分并非总是明确的。

关于ICN术语，RFC 7927[64]定义了三个主要术语:命名数据对象(NDO)或简单的数据对象是可从网络请求的可寻址信息段； 发布者是将NDO发布到网络的实体（发布者不一定是NDO创建者，它可能只是为真正的创建者托管数据对象）； 而请求者是向网络发出对命名数据对象的请求的实体。 在本文中，术语内容和数据对象是可互换使用的； 术语publisher用于表示

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |



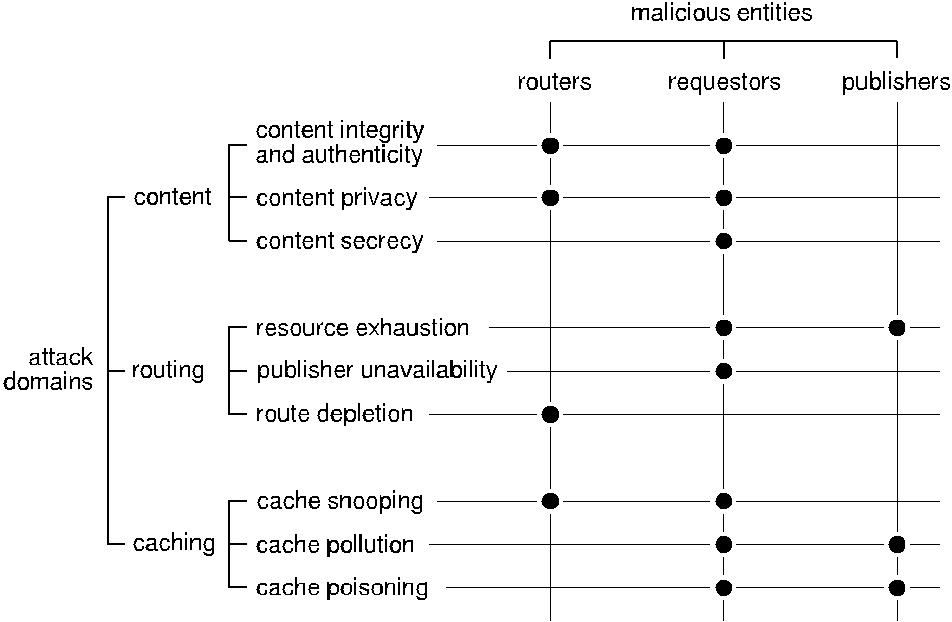
图。 1.基本的ICN内容分发模型。

产生内容的实体（其创建者或制作者）和使其可供网络使用的实体； requestor和user这两个术语被认为是等价的； 最后，术语“源”指定提供数据对象的通用实体，可以是发布者或缓存。

图1描述了ICN通信模型中内容如何流动的一个简单示例，它使用NDN/CCN体系结构作为对ICN通信模型的支持。 首先，发布者使内容对用户可用，在本例中是在前缀/s1/下，用户通过应用程序或搜索机制了解这些内容。 用户将对内容项的请求发送到网络（图1(a))，而不指定特定的计算机或地址。 路由器根据它们的路由表将请求路由到内容发布者，检查它们的缓存是否有缓存命中。 包含有效载荷的回复遵循相反的路径（图1(b))。 当内容通过路由器转发时，它们可以将副本存储在缓存中，通过满足更多请求而不将其路由回发布服务器，提供了推理带宽、链路质量或可用连接的方法，如图1(c)所示。

2.2国际竞争网络的安全问题

尽管采用ICN模式有很大的好处，但它所代表的网络层的深刻变化总会带来新的安全挑战。 例如，所有ICN体系结构都必须提供名称-内容完整性检查机制，使用户能够检查检索到的内容是否被篡改。 此外，还应处理内容真实性问题，以提供评估内容来源的手段。 与基于IP的路由相比，基于内容的路由需要在每台路由器中处理更多的管理信息，例如NDN/CCN中的转发信息库(FIB)和挂起兴趣表(PIT)结构。 由于挂起的请求由每台路由器存储，因此它们可能容易受到恶意用户的拒绝服务(DOS)攻击，这些恶意用户向它们大量发送请求[114]，因此它们应该受到保护。 ICN引入的缓存机制也可能成为恶意用户的攻击目标，需要注意避免众所周知的攻击（如缓存污染和缓存监听）的解决方案，以及仅对授权用户访问缓存内容进行控制的机制。 隐私是ICN体系结构的另一个问题，



图。 2.安全威胁及其涉及的恶意实体的分类和组织。

因为内容项是按名称请求的，可以缓存在中间路由器上； 恶意实体不应通过内容名称访问隐私敏感信息。 ICN不使用源地址的概念； 因此，将内容绑定到请求者并不简单，因为这样可以保护她的隐私。 然而，在某些特定情况下，内容名称可能会泄露足够的信息，从而妨碍用户的隐私。

总的来说，我们认为探究ICN漏洞的攻击可能由参与网络的任何实体触发:用户、内容发布者、路由器和缓存监护人。 我们称这些实体中的任何一个为恶意实体，其目的是探索ICN体系结构中的漏洞，以扰乱网络或危及用户和内容发布者的隐私。 这些恶意实体可能以被动或主动的方式出现，具体取决于它们与网络的交互。 虽然被动攻击很难检测，但由于恶意实体不与网络交互，因此可以分析主动攻击，因为恶意实体与其他网络实体交互以发出攻击。 此外，我们假设恶意实体可以单独行动，也可以通过与其他恶意实体串通来扩大损害。 我们还考虑了发起攻击的资源可能有限的恶意实体，以及可用于攻击的计算能力高的恶意实体，如路由器、发布者和政府。

为了更好地理解攻击如何影响ICN行为，我们将分析分为三个主要领域:内容安全、路由器安全和缓存安全。 图2说明了每个域及其各自的攻击类别，以及最有可能触发它们的恶意实体。 对于内容的安全性，我们期望由于内容命名缺乏安全性而缓解的攻击，导致对内容完整性、隐私和未经授权的访问的威胁。 对于路由器安全，我们处理的攻击旨在破坏网络的结果，如资源耗尽，发行者不可用，路由耗尽的ICN模型。 最后，Cache中的安全性包括对网络内缓存的攻击，如Cache监听、Cache污染和Cache中毒。 每一类攻击都可能由ICN模型中的不同漏洞或安全缺陷触发，详见下一节。

在接下来的章节中，我们系统地介绍和组织了文献中讨论的针对ICN的主要攻击，并在适用的情况下提出了挫败这些攻击的对策。 我们

特别针对攻击者引入的故意故障，尽管ICN体系结构也容易发生其他故障，如物理和设计故障。 我们还介绍了包含ICN攻击的组合及其相应的类别、目标、漏洞的表，以及对缓解这些攻击的对策的参考文献。 在这些表中，我们的目标是准确地指定作者在其论文中使用的攻击的名称，即使其中一些攻击可能具有相同的功能。 我们选择坚持作者使用的命名约定，以帮助阅读器识别这些相似性。 这些表格分为三部分，每一部分列出一个攻击类别，放在相应部分的末尾。 尽管不同的ICN体系结构[5、25、33、53]在实现方面具有特殊性，但它们共享相同的基本ICN组件（命名内容、按内容名路由和网络内缓存）。 因此，我们对涉及ICN范例的核心功能的安全问题感兴趣，并且将不讨论此类体系结构的特殊性。

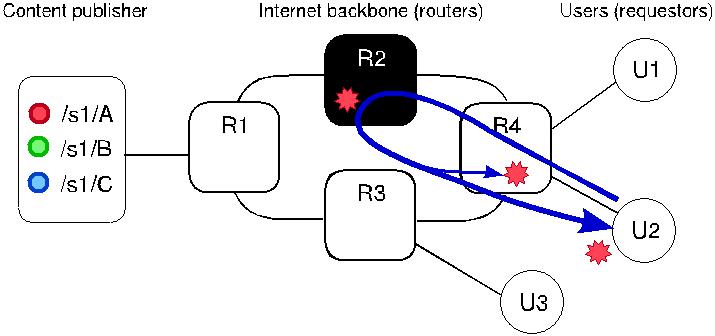
3内容安全

内容命名方案是任何ICN体系结构的核心，因此是最关键的安全机制之一。 与保护内容名称同样重要的是保护内容本身。 主要由于ICN范例引入的内容位置独立性，内容容易受到完整性和真实性、隐私和保密性方面的威胁。 事实上，名称和内容安全一直是ICN设计者的一个主要问题，并且已经研究了大量的漏洞和解决方案。 在本节中，我们将内容命名安全问题分为三组:内容完整性和真实性、内容优先级和内容保密。 内容完整性和真实性威胁包括旨在修改和篡改合法内容有效载荷、欺骗网络和用户或在网络中注入虚假内容的攻击，就好像这些内容来自真正的发布者一样。 内容隐私攻击的目的是通过篡改通信信道来篡改用户和内容发布者的敏感信息（第5节讨论了缓存引起的隐私问题），并可能导致审查和用户监视。 最后，保密问题包括旨在向未经授权的实体授予对缓存内容项的访问权限的攻击。 下面将详细介绍这些攻击及其对策。

3.1内容完整性和真实性

由于内容可能由第三方实体（如路由器和移动设备）分发和缓存，而不仅仅是由内容发布者控制的服务器，因此它会受到针对其完整性和真实性的攻击[50，97]。 恶意实体可以通过截获内容项并修改其有效载荷来篡改内容项； 他们还可以伪造内容并将其注入网络，就像它来自真正的出版商一样。 这类攻击简单且相对容易发起:首先，内容名称对网络实体可见； 因此，恶意实体相对容易地以流行内容项为目标。 第二，因为内容可以由任何网络实体保存，所以内容发布者对其没有控制权。 但是，恶意路由器由于其在网络中的特权位置，更容易发起这些攻击。 图3描述了这个场景； 当用户U2请求内容/S1/A时，路由器R2生成伪造的内容并作出响应。 此攻击对用户造成极大的损害，因为预期用户将从内容发布者本身以外的位置接受内容； 因此，它们容易受到与原始请求不对应的已损坏/可疑内容的攻击。

对内容完整性和真实性的关注对于任何ICN设计都是至关重要的，事实上，自命名方案的概念提出以来，就一直在考虑采用数字签名性质来保证内容完整性和来源[45]。 应当指出，内容完整性和真实性是两个密切相关的问题。 内容完整性威胁的大多数解决方案也适用于内容真实性问题。 在大多数ICN体系结构中，内容本身



图。 3.国际竞争网络中的诚信威胁。

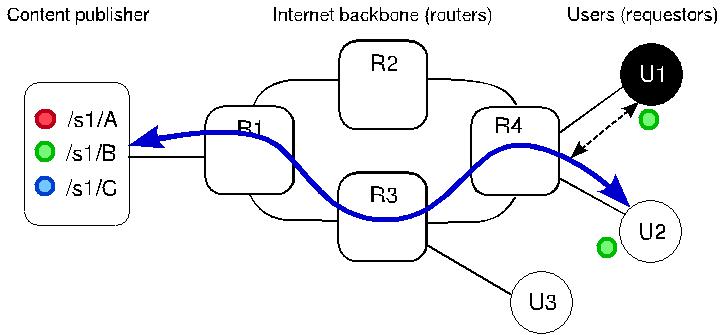
可以保证其完整性和真实性，从而允许其位置独立性。 例如，NDN/CCN体系结构通过验证内容与其名称之间的链接来确保完整性。 这由内容发布者执行，内容发布者对从内容名称到内容[103]的映射进行数字签名。

使用数据对象内容的加密哈希来命名数据对象，可以检查对象的完整性。 因此，在接收到内容时，用户能够通过与内容发布者或在元数据的支持下对抗内容散列和证书来检查其完整性和证明一致性。 此模式在使用平面命名方案的体系结构中采用，如NetInf[24]，但也可以应用于分层命名方案，如NDN/CCN[13，41]。 应该注意，只要加密哈希函数是可信任的，这种方法就可以工作； 在使用基于哈希的名称绑定的体系结构中，中断的哈希函数将允许您轻松发布具有相同名称的不同内容。 或者，还提出了基于身份的加密以评估内容项[48、50、109、129]的完整性和真实性，其中内容名称用作内容发布者验证其真实性的公钥。 然而，这样的方案仍然需要使用允许验证内容完整性的辅助工具。

与关注内容真实性一样重要的是寻址发布者真实性，其中用户能够识别和信任内容发布者。 用户可以基于关于内容发布者的信任信息来决定接受或拒绝内容，从而涉及信任管理机制[123]。 由于用户能够从内容本身评估完整性和真实性，他们还应该确保用于对内容进行签名的公钥是可信的。 ICN还提出了内容认证的传统公钥基础设施的替代方案，主要探讨分布式和分散式机制，如使用分布式哈希表(DHT)[117，118]、社交图[74]和传统的DNS类机制[75]。 另一种解决方案是将公钥拆分为多个冗余分散在网络上的部分； 用户可以从任何实体检索它们以验证内容完整性[55，61]，甚至可以使用边缘路由器来验证进入其网络的所有内容的真实性[60]。 研究人员还探索了一种方案，通过使用一种记帐服务来验证旧数据，该记帐服务可以在任何时候对数据签名进行认证[124]。 信任管理方案设计中的主要挑战是密钥和证书的可伸缩性和撤销[82]，因为密钥和证书也可以存储在不受控制的缓存中。

3.2内容隐私

任何ICN体系结构的主要机制之一是基于名称的路由，它同时使内容名称对网络可见。 这是一个问题，因为名称可能包含有关内容项的语义信息，从而妨碍隐私实践。 恶意实体可以利用此功能根据内容名称监视、筛选和阻止用户的请求

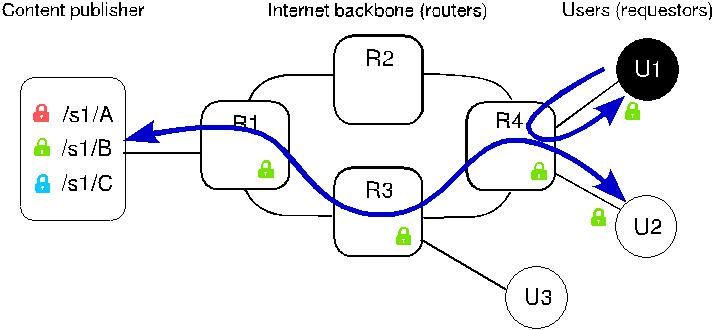


图。 4.ICN中的隐私威胁。

[20]。 例如，恶意实体可以使用具有内容名称的黑名单来阻止/删除，然后监视频道（和高速缓存）以将内容与黑名单匹配。 由于路由器处于网络的战略位置，能够访问网络流量，因此它们是发起此类攻击的最佳候选路由器。 图4说明了U1通过监视通信信道和了解U2请求的内容来试图侵犯U2隐私。 或者，恶意实体可以简单地检查缓存和通道中的关键字[10]。 尽管很难确定请求内容的特定用户，但内容监视和检查可能会拒绝服务或谴责敏感的内容项。 同样的策略也可用于监视用户请求，其中恶意用户窃听通信信道以找出内容名称并推断用户首选项[2]。

从隐私的角度来看，在ICN中确保隐私的主要对策是隐藏或屏蔽来自网络实体的内容请求[106]。 Bloom过滤器[14]已经为此目的在ICN中被广泛地探索，因为该方案允许网络实体（例如路由器）测试特定内容名称是在路由表中还是在高速缓存中，而不暴露内容名称[16，79]。 在请求内容之前，用户为分层名称中的每个子组件计算Bloom过滤器。 然后，路由器对内容标识符执行最长前缀匹配。 由于这种方法将内容标识符转换为随机位串，因此有助于防止黑名单匹配和用户分析。 或者，也可以使用同态加密来隐藏请求，同时允许路由器和内容发布者检查所请求的内容是否在其内容集中，以确保内容发布者或第三方元素（例如窃听者）都不能推断或发现用户正在请求的内容[33]。

另一种用于在ICN中请求内容时向用户提供隐私的方法是通过使用例如封面文件来屏蔽内容。 这种解决方案的思想是在检索内容时为合法和恶意用户创建计算不对称性，避免黑名单攻击。 基本上，发布者将合法内容与封面内容混合在一起。 为了检索内容，用户需要使用安全通道从发布者收集一些辅助信息，即内容哈希和用于生成覆盖内容的算法。 由于内容项是在覆盖块中检索的，因此需要恶意用户进行大量的计算工作，以便在事先不知道额外信息的情况下发现所请求的内容，而私密用户可以使用在安全侧信道中检索的信息来容易地提取所需的内容[10]。 对于在内容检索中需要隐私的用户来说，另一个想法是在内容的已知电路中将请求与每个路由器的公钥封装在洋葱路由覆盖层中。 接收到请求后，电路中的每个节点提取其加密层，并将请求转发到下一个节点。 这一直进行到请求到达发布者为止，发布者将以纯文本形式接收请求[26，101,108]。 此外，用户可以根据请求对内容名进行编码，并且具有



图。 5.ICN中的未经授权访问威胁。

完全保密，并得到内容出版商的支持[106]。 然而，此解决方案通常会损害网络内缓存的好处，从而对网络和缓存性能产生负面影响。

由于审查的可能性，隐私也是内容发布者关注的一个问题，这主要是因为内容名称可能包含发布者（生产者）标识。 虽然审查不应由网络本身处理，但ICN行为可能会缓解审查； 因此，必须讨论这种威胁。 ACS等人提出了一套避免对内容发布者进行监视和审查的预防性措施。 [2]，例如使用组签名、环签名和确认签名，这些签名允许用户验证内容的签名是否有效，但不具体标识哪个发布者对其进行了签名，从而保证内容发布者的匿名性。 另一个想法是在可靠的、固有的身份下使用短暂的身份。 永久身份受用户信任； 从那里，可以根据需要向其他内容发布者提供不同的身份，而不公开哪个发布者正在对内容进行签名。

3.3内容保密

在ICN中实施访问控制策略来保护内容的保密性是一个非常值得关注的问题，特别是由于ICN范式提出的网络内缓存基础设施[52，73]。 由于检索到的内容沿途由不可靠的实体（如路由器、移动设备或类似CDN的基础结构中的第三方服务器）缓存，内容发布者在管理和实施对其内容的访问控制方面面临问题。 当考虑付费或版权内容时，这个问题更加令人关注，因为没有帐户/订阅的用户可以访问受保护内容的缓存副本。 任何用户，不管她的计算能力如何，都可以从缓存中检索未经授权的内容，因为它们在回复之前不会验证用户的访问权限。 图5介绍了一个基本的未经授权的访问场景，因为U1从路由器R4缓存中检索一个受保护的内容，这是合法用户U2以前请求的。 仅将内容的名称限制为授权用户是不够的，因为ICN中的路由和转发是直接根据内容的名称执行的，因此可以容易地发现名称。 因此，这种类型的应用程序需要一个更健壮和合适的解决方案，以便在ICN中使用。 尽管访问控制问题是ICN范例的固有问题，因为网络缓存，恶意实体也可能受益于用于访问受保护内容的传统攻击，如Sybil攻击[84]。

在ICN中维护内容保密的基本操作是通过内容加密，确保只有具有有效密钥的用户才能访问它[17、49、53、72、116、130]。 然而，取决于所采用的加密解决方案，加密内容可能会在缓存与访问控制的权衡上出现问题，这主要是因为使用传统对称加密为特定用户加密的内容可能无法缓存给其他用户，而其他用户将无法解密[76，95]。 至

针对这一问题，提出了一种用于ICN访问控制的特殊加密机制。 例如，基于属性的加密(ABE)为共享公共属性的一组用户加密内容，因此只有当用户的密钥满足嵌入在密文或密钥本身中的访问控制策略时，用户才能够解密内容[52，69，70，92]。 在ABE方案中，缓存的内容可以在同一组中的用户之间共享。 在广播加密(BE)模型中，内容发布者使用唯一的对称密钥加密内容，并分发在广播组公钥下加密的对称密钥。 广播组中的每个用户可以使用她的单独私钥来解密对称密钥。 在BE模型中，缓存的内容也可以在同一广播组中的用户之间共享[49，84，94，126]。 然而，如果这样的解决方案使用相同的密钥来为大组加密内容，则密钥泄漏可能是一个问题，因为任何具有该密钥的用户都可以检索内容，即使是未经授权的内容[78]。

探索的另一种加密方案是代理再加密(PRE)[11]。 在基于预置的解决方案中，使用对称密钥对内容项进行加密。 对称密钥用内容发布者的公钥加密，要恢复对称密钥，用户必须用内容发布者[119]检索重新加密密钥。 这种解决方案的一个常见问题是对称密钥公开。 一旦用户有了对称密钥，他们就可以访问缓存的内容，即使他们没有被授权。 预解决方案变体是用不同于非对称密钥对的私钥加密每个内容； 因此，内容项可以由所有用户通过高速缓存共享，而内容公钥如果被公开，则仅与COR响应用户的公钥一起有效[77]。 还探讨了不同的策略，例如混合对称和非对称加密技术[49、76、104、126]以及构建可与任何基于加密的解决方案[47、63]结合使用的访问控制框架。 然而，最近的研究表明，基于加密的解决方案不足以保证内容的保密性，这主要是因为攻击者很容易根据内容的受欢迎程度推断出内容，即使这些内容是加密的[42]。

除了基于加密的解决方案之外，研究人员还提出了基于基础设施的替代解决方案，例如使用授权服务器来验证策略[31、32、36、102]。 这种解决方案的一个问题是，它们通常假定内容保管人（例如，高速缓存）在将内容发送给用户之前验证访问策略。 由于某些原因，这些假设在Internet环境中可能难以确保。 访问控制决策涉及评估定义在用户和内容上的规则。 对于验证访问请求的缓存，它需要评估内容发布者为该内容和该用户定义的访问控制规则。 这意味着应该为每个高速缓存提供（和更新）它可以存储的所有内容和它可以服务的所有用户的访问规则，这是不可伸缩的。 否则，缓存可能会将访问决策外包给知道所有规则的授权服务器，从而为每个内容请求增加额外的延迟。 还考虑使用访问控制列表[15，44]； 然而，它更适合于受控环境，例如位于小地方的传感器网络，而不是Internet。 另一个想法是直接在路由器上使用访问级别，这样路由器只能缓存发布者授权给[71]的内容项。 这种解决方案假定路由器操作系统被修改以符合附加到内容项的访问规则，并且路由器本身在转发和缓存过程中强制执行这些规则。 这意味着缓存应该能够评估和应用内容发布者定义的访问规则，这需要对每个请求进行更多的处理。 此外，这还在整个网络中为所有发布者和缓存强加了公共访问控制模式。

访问控制的另一个方面是使用考虑到ICN特性的防火墙来支持网络管理。 例如，这可用于强制执行本地安全策略。 防火墙规则是通过名称或发布者阻止内容来实现的。 如果某个发布服务器变得恶意，则可以实现规则以避免来自该发布服务器的内容到达

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 表1。 ICN攻击概述、分类及内容对策 | | | |  |
|  |  |  |  |  |
| 攻击 | 类别 | 漏洞 | 对策 |  |
| 锻造内容 |  | 非加密内容 |  |  |
| 内容重命名 | 内容完整性 | 不良内容-名称 |  |  |
| 绑定/哈希 |  |  |
|  | 和真实性 |  |  |
|  |  | [13、24、45、48、50、62、75 |  |
| 内容损坏 | 缺乏内容 |  |
|  |  |
|  | 加密 |  |  |
|  |  |  |
| 名称监视列表 |  | 命名的网络路由 |  |  |
|  |  |  |  |
| 内容分析 | 内容隐私 |  |  |
| 内容 |  |  |
|  |  |  |
| 姓名隐私 |  |  |
|  |  |  |  |
|  |  |  |  |  |
| 发布者隐私 |  | 加密密钥标识 | [2] |  |
|  | 出版商 |  |
|  |  |  |  |
|  |  | 缓存受保护 | [15、31、32、36、44、47、49 |  |
| 未经授权的访问 |  |  |  |
| 内容保密 | 内容 |  |
|  |  |  |
|  |  |  |  |
|  |  |  |  |  |
| Sybil（模拟） |  | 凭据检查 | [84] |  |
|  |  |  |  |  |

网络。 此外，还可以根据关键字检查内容，以便进行筛选。 此外，由于每个内容必须由其发布者签名，因此防火墙可以配置为忽略具有无效签名的内容，例如[44]。

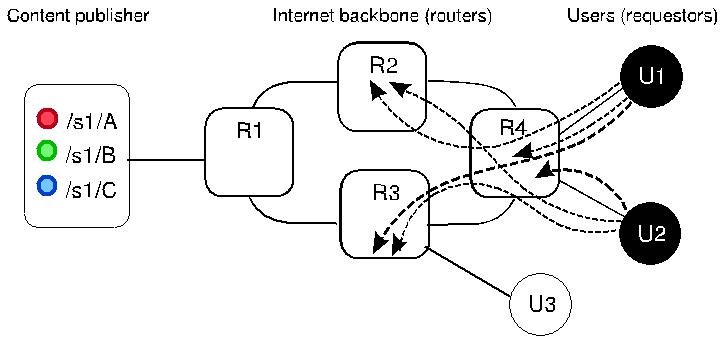
表1列出了针对ICN内容安全的攻击和对策的工作汇编。

* 路由器中的安全性

路由器为网络层的核心层执行路由和转发等基本服务。 除了管理和更新所有路由信息外，它还负责查找网络中的内容，将请求和内容转发回请求者。 由于ICN模式给网络层带来了新的特性，路由器功能中也出现了新的威胁，这主要是由于网络层中直接基于名称的转发造成的。 然而，即使是已知的拒绝服务攻击也可能阻碍ICN转发。 我们将ICN中的路由器攻击分为三类:资源耗尽、发布服务器不可用和路由耗尽。 资源耗尽攻击包括恶意实体，它们要求路由器进行不必要的计算。 Publisher Unavailability Groups攻击内容发布者，以限制或停止内容分发。 最后，路由耗尽攻击的目标是中断路由路径，例如通告无效路由。 在本节中，我们将详细介绍这些组中的每一个。

4.1资源枯竭

为了能够将内容转发回请求者，基于有状态路由的ICN体系结构（如NDN/CCN）要求路由器保留每个接口接收和转发的请求的记录，直到通过返回路径的内容或超时过期消耗了请求为止。 该机制被指出可能容易受到拒绝服务（DoS）攻击，这些攻击旨在中断合法用户的转发服务或使网络过载并禁用它。 该漏洞的利用已在文献中进行了广泛讨论，网络中的任何用户都可以有效地利用该漏洞。 例如，恶意用户或一组合谋用户可能会发出过多的请求，从而耗尽挂起的请求条目的可用内存，并拒绝



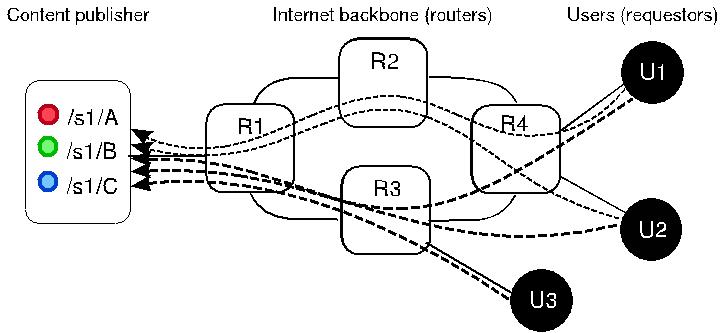
图。 6.国际竞争网络资源枯竭威胁。

为合法用户提供的服务。 路由器是否对挂起的请求条目采用速率限制并不重要，因为恶意用户很容易超过此限制[112]。 但是，由于对相同内容的请求条目进行聚合以提高性能，因此即使恶意用户以分布式方式发送相同内容的请求突发，此攻击也是无效的或最小化的。 要禁用这种自然防御，恶意用户应该发出过多的伪造请求，以便用伪造的条目填充挂起的请求表，从而导致合法请求被丢弃[3、18、21、23、28、34、59、110、112]。 如图6所示，在分布式攻击者同时工作的情况下，这种攻击将更具攻击性，并且很难检测到[43]。 在本例中，U1和U2一起耗尽了路由器R4的资源，由于其挂起的请求记录中的请求量，路由器R4可能无法再接受任何请求。

所有这些泛洪攻击都有一个共同的后果:它们导致挂起的请求条目过期。 为了避免在泛洪攻击的对策中探索该特性，用户可能与恶意内容发布者串通，以避免检测到过多的请求过期[65，111,114]。 在这种情况下，恶意发布者会在挂起的请求条目超时到期之前立即回复伪造的请求，从而导致路由器相信通道拥塞。 结果，重新传输被触发，扩大了损害。 两个被破坏的路由器也可以利用这些攻击来减缓内容转发，迫使其他路由器中的挂起请求条目在内容传递完成之前过期，从而导致重新传输风暴[111]。

在ICN中缓解泛洪攻击的第一次尝试建议对挂起的请求表使用哈希函数来保存存储，或者总是接受新的请求，丢弃最旧的请求[65]。 然而，这些都是简单的想法，可以延迟攻击的后果，但不能避免它们。 更复杂的解决方案基于监视和识别路由器中的异常请求量[89]。 例如，路由器可以监视未满足请求率[7-9、30、34、43、56、58、59]、未决请求表[21]上的条目数量或每个接口上的请求数量[3、88]。 因此，在路由器识别出对同一接口中的不同内容项的异常请求量的情况下，它们可以限制来自这样的接口的被接受请求量，可能最小化泛洪的后果，同时允许来自该接口的合法请求具有被满足的公平机会。 一些解决方案允许路由器之间共享这些结果，从而帮助其他路由器避免泛洪攻击或从泛洪攻击中恢复[43，116]。

兴趣NACK（非确认）数据包也可用于避免路由器等待恶意兴趣超时过期。 使用NACK，路由器可以满足路由器中的请求，从而将PIT从恶意条目中解脱出来，如果是这样的话[122]。 此外，路由器可能会在返回恶意用户的途中对可疑请求做出响应，以清理挂起的请求表，从而将此类攻击的影响降至最低[23]。 另一种解决方案是采用经过身份验证的请求，作为路由器识别发出过多请求的恶意用户的手段[15]。 还有，



图。 7.ICN中发布者不可用威胁。

采用基于无状态转发的ICN体系结构将使恶意条目与PIT[40，115]分离。

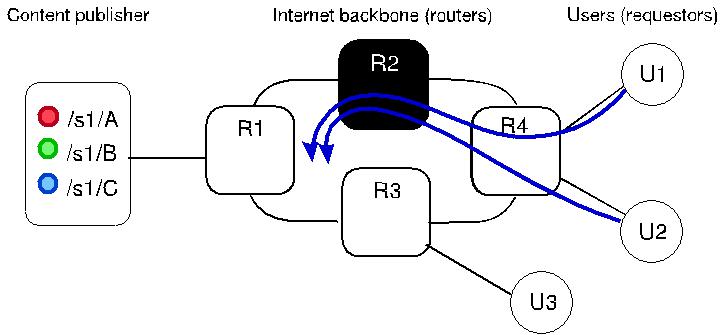
4.2发行者不可用

正如发送过多的请求会中断合法用户的路由服务一样，将请求集中到唯一的发布服务器或特定的名称空间也会禁用整个名称空间或发布服务器，例如在传统的IP网络DoS攻击中。 饱和受害资源并使合法用户无法访问内容的最基本方法是发送大量对同一内容发布者的请求，其中恶意用户合谋向网络中的同一受害服务器发送请求[34，65]，如图7所示。 此攻击需要向同一发布服务器发出大量请求才能生效； 无论如何，它不需要攻击者提供大量的计算能力，因为一组用户的协调就足以部署它。

然而，针对ICN基础设施中的这种攻击，需要恶意用户进行一些特殊的准备。 例如，它们需要确保路径上的任何缓存都不能满足内容，并且内容请求被路由到受害者，并且每个请求都在路由器中创建新的挂起的请求表条目。 为了颠覆这种逆境，恶意用户可以发送具有相同前缀的伪造数据请求，从而诱导路由机制将请求转发到前缀发布者，同时防止在高速缓存[3、21、34、113]中找到内容。 由于这些攻击的性质，用于减轻泛洪攻击的监控解决方案也可以应用于这些情况。 特别是针对发布服务器不可用攻击，路由器可以采用一些度量标准，例如监视对相同内容发布服务器的请求数量，减少转发到此前缀的请求[65]，从而避免恶意请求淹没内容发布服务器。

4.3路由损耗

为了正确地将内容请求转发给发布者或可用的缓存副本，每台路由器都需要保持其转发信息库(FIB)已更新且没有恶意条目。 对FIB的威胁可能会使合法域无法访问，或允许恶意用户将路由重定向到恶意内容或路由器以进行监视。 此攻击要求攻击者能够访问路由通告； 因此，它需要颠覆路由器或内容发布者。 恶意内容发布者可能会宣布许多属于不同域的恶意内容，直到表已满并且无法从合法域注册有效内容为止[43]。 它们还可能以推断路由更新收敛时间的速率发布内容，导致缓存内容信息不正确、误导路由、甚至为其他攻击打开安全漏洞等问题[111]。 或者，一个



图。 8.国际竞争网络路由耗尽威胁。

恶意路由器可能会向网络通告有效内容，并在请求内容检索时延迟回复甚至不回复，从而导致用户服务中断[34、73、112]。 如果几个恶意路由器串通宣布通向热门内容的路由，然后延迟回复，则会加剧此攻击[111]。 图8描述了路由器R2通告到/s1/content items的路由的场景，但是，它不是将请求转发到/s1/，而是简单地丢弃在以前的路由器中发出挂起请求的请求。

路由信息条目也可能受到被动监视的威胁，因为恶意路由器可以通告到许多内容项的路由，但不会将所有内容项都保留在其缓存中。 这里的目标是拦截对此类内容的任何请求，然后将其转发到正确的位置。 由于用户不受此攻击的直接影响，攻击者可以监视网络中请求的内容，而不会被发现[111]。 当考虑到协作网络（如移动ad hoc网络）时，这种攻击可能更加危险，在协作网络中，用户设备自然被放置为转发数据包的路由器。

Gasti等人。 [34]认为NDN/CCN体系结构本身具有抵抗前缀劫持攻击的弹性，这主要是因为路由更新经过签名，因此可以验证，防止恶意用户注册假路由。 但是，当恶意路由器具有其他路由器接受和验证的有效加密密钥时，此对策不适用。 此外，面临此类攻击的网络可以受益于异常行为的监视，类似于应用于请求泛洪攻击的解决方案。 此外，路由劫持可能被通往受害者内容的多条路由颠覆，但如果攻击者以分布式方式串通并攻击发布者，则路由劫持将无效[111]。 最后，Lauinger[65]提出了一些建议，以防止在请求数据包中滥用特殊位，从而限制此类位的使用，例如只允许在本地请求上使用作用域字段，或者要求希望设置作用域字段的请求具有数字签名，从而暴露了攻击者的身份。

表2提供了ICN路由方面的攻击和对策的汇编，以及它们所探讨的漏洞和目标实体。

* 缓存中的安全性

缓存机制是ICN体系结构最突出的特性之一。 它的目的是通过在用户附近放置内容副本来改进网络中的内容分发； 这减轻了拥塞和延迟问题，特别是对于流行的内容，如视频流。 在传统网络中存在一组众所周知的对高速缓存系统的威胁。 然而，在ICN体系结构中，随着这些威胁在全球范围内扩展到Internet:恶意网络实体（发布者和路由器）可以发布、更新和分发可能很难检测到的恶意内容。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 表2。 路由器上的ICN攻击概述、分类及对策 | | | | |
|  |  |  |  |  |  |
|  | 攻击 | 类别 | 漏洞 | 对策 | |
|  | 愚弄率限制 |  |  |  |  |
|  |  |  |  |  |  |
|  | 洪水泛滥 |  |  |  |  |
|  |  |  |  |  |  |
|  | 挂起利息表(PIT)攻击 |  |  |  |  |
|  |  |  |  | [3、7-9、15、21、23 | |
|  | 流动封锁 |  |  |
|  |  | 资源 |  |  |  |
|  | 突发脉冲 |  |  |
|  |  | 筋疲力尽 |  |  |  |
|  | 长时间攻击 |  |  |
|  |  |  |  |  |  |
|  | 干扰 |  |  |  |  |
|  |  |  | 有限存储 |  |  |
|  | 强迫进行昂贵的计算 |  |  |  |
|  |  |  | 对于请求状态 |  |  |
|  | 超时 |  |  |  |
|  |  |  |  |  |  |
|  | 通过填充可用内存实现DOS |  |  | [65] |  |
|  |  |  |  |  |  |
|  | 带宽损耗 |  |  |  |  |
|  |  |  |  |  |  |
|  | 单目标DDoS |  |  |  |  |
|  |  | 出版商 |  |  |  |
|  | 针对内容发布者的DoS |  | [23，65] |  |
|  |  | 不可用 |  |  |
|  | 具有特殊位的DOS |  |  |
|  |  |  |  |
|  |  |  |  |  |  |
|  | 远程启动的过载 |  |  |  |  |
|  |  |  |  |  |  |
|  | 由于发行者速度慢而堆积请求 |  |  |  |  |
|  | 纤维污染 |  |  |  |  |
|  |  |  |  |  |  |
|  | 路线劫持 |  |  |  |  |
|  |  |  | 未经验证 |  |  |
|  | 死亡之路 | 路线 |  |  |
|  |  | 路线 | [34、65、111] |  |
|  | 前缀劫持黑洞 |  |
|  | 耗尽 |  |
|  |  | 公告 |  |  |
|  | 侵权内容状态 |  |  |
|  |  |  |  |

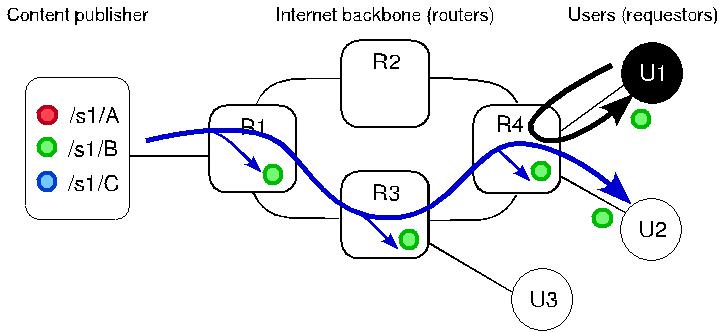
路由拦截

路由误用

我们将ICN中的缓存攻击分为三组:缓存侦听、缓存污染和缓存中毒。 缓存侦听攻击包括恶意用户，目的是通过分析缓存中存储的内容项来分析Internet上的用户行为。 缓存污染组攻击的目标是用不受欢迎或不相关的内容而不是受欢迎的内容填充缓存，从而使缓存无效。 最后，缓存中毒不同于先前的组，它处理的攻击旨在用非法、伪造或伪造的内容填充缓存。 本节列出了有关ICN缓存系统的文献中探讨的攻击以及缓解这些攻击的解决方案。 由于对传统网络缓存的广泛了解，ICN中的缓存攻击得到了广泛的关注，因此有很多解决方案。

5.1缓存侦听

ICN中使用的最有趣的缓存策略之一是基于内容流行度和与附近用户的相关性来存储内容。 然而，该策略使缓存成为关于用户在因特网上的兴趣的信息的相关代表，可以对其进行探索以获得关于用户或用户组的敏感信息[83]。 尽管这些攻击一般可以由用户发起，因为它不需要太大的计算能力，但内容发布者可以更好地从窥探缓存来推断用户的行为中受益。 即使很难精确地确定特定用户的行为，例如，内容发布者也可以使用窥探来推断区域中用户的偏好并将其用于广告。 此外，政府机构还可以使用窥探



图。 9.ICN中的缓存侦听威胁。

监视和阻止特定内容。 靠近受害者的恶意用户（例如同一接入路由器中的恶意用户）对用户隐私构成更大的风险，因为他们与更少的用户共享同一缓存，从而为窥探者的行为提供了便利[91]。 窥探器能够列出缓存的内容、监视内容访问，甚至复制会话[65]，如图9所示，其中用户U1窥探路由器R4以查找缓存中存储的内容项，检索用户U2先前请求的内容的副本。

用于高速缓存窥探的策略包括通过监视内容名称和请求特定内容名称直到它被高速缓存返回来进行高速缓存探测，以及通过向高速缓存请求随机名称来进行高速缓存探测，其中不包括在随后的请求中已经获得的名称。 NDN/CCN体系结构特有的一个特别令人担忧的方面是排除字段[53]，因为它可用于将查询专门限制到路径2中的第一个高速缓存； 如果监听程序从特定缓存检索内容项，则该缓存下的用户最近检索了该内容[65]。 这些威胁在考虑路径上缓存时更令人担忧，因为它们传统上基于路由器，更准确地表示用户的行为。 除了考虑检查缓存以推断用户行为的恶意实体外，隐私入侵攻击[73]还考虑泄漏用户敏感信息的恶意内容发布者，尽管这不是ICN独有的威胁，也不是ICN体系结构控制下的威胁。

另一种推断给定内容是否在高速缓存中并且因此推断附近的用户最近是否访问了这样的内容的方法是通过来自附近高速缓存和来自发布者的答复之间的时间差[16，86]。 恶意用户可以向缓存发出探测，以测量其往返时间(RTT)。 然后，它对它要监视的内容发出请求，并测量它的RTT。 通过分析这两个RTT，恶意用户推断内容是从缓存还是从其他任何地方检索的[65]。 该策略还可用于通过探测发布者以发现其RTT，然后请求所监视的内容来推断发布者最近是否生成了某些特定内容。 如果来自第二个请求的RTT低于第一个请求的RTT，则可以安全地推断这样的内容最近由发布者提供给一些用户，并且存储在一些路由器的高速缓存中。 尽管此攻击是可行的，并且对用户隐私和匿名性构成威胁，但一致认为，将特定用户与缓存中的内容相关联并非易事，可能需要额外的信息[2]。

如果政府或行业通过监视内容请求来监视用户并披露其内容访问、隐私和匿名性，则此类攻击会带来更大的隐私风险。 这是ICN体系结构的一个基本问题，因为网络知道在其上传输的内容项。 如果路由器能够从语义上解释内容名称，情况可能会更糟，因为

* 由于这一原因和其他原因，排除字段将从当前的NDN协议规范中删除（此时为0.3）[87]。

恶意ISP、政府和行业的审查和监控会容易得多。 与传统网络中的深度数据包检查工具不同，ICN体系结构中的高速缓存允许探听者在较长的时间窗口上检索信息，在传统网络中，探听者需要策略性地定位并具有足够的能力来以线速检查数据包[16]。 然而，关联用户和缓存副本并非易事，可能需要其他信息。

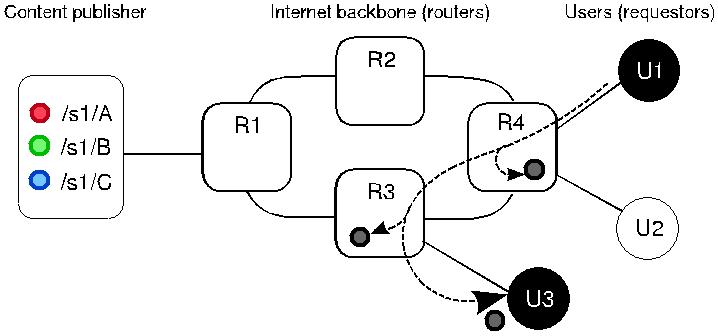
作为解决ICN模式中Cache窥探攻击的第一个对策，提出了一组可能的预防措施，以减轻ICN中针对此类攻击的漏洞，例如限制用户可以使用排除字段的内容名称部分和最长的前缀匹配，从而设置用户必须具有请求它的名称内容的哪一部分的先验知识[65，66]。 此外，禁用或限制在请求数据包中使用exclude字段可以防止恶意用户将搜索限制在本地缓存中，在本地缓存中，威胁会被放大。 除了预防之外，在很短的时间窗内以很高的命中率监视来自同一链路的异常请求等事件等检测操作也是一种替代方法[91]。

面对基于定时的缓存窥探，基本策略是延迟来自缓存的响应以均衡响应时间，从而避免恶意用户通过从发布者和缓存检索的内容之间的定时差异推断缓存的内容[16，65，85，86]。 另一个想法是计算用户请求相同内容的次数； 来自同一用户的请求直接从高速缓存中响应，并且基于从发布服务器到用户的跳数，对不同用户应用定时延迟。 协作缓存的使用可以用来破坏定时攻击，因为路由器根据内部状态（如可用存储）及其在转发路径中的位置来缓存内容项。 因此，恶意用户很难推断检索到的内容是否在缓存中。

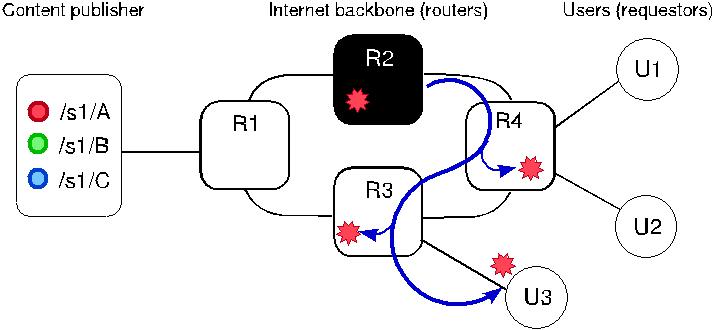
为了避免恶意用户窥探点对点对话产生的内容，主要思想是使内容名称变得不可预测，例如，通过使用临时名称、通过隧道请求或通过将随机组件附加到内容名称[2]。 此随机组件需要在通信方之间达成一致。 他们选择并安全地共享一个秘密种子，并使用它来创建和请求内容。 因此，内容名称仅由两个通信方知道，从而防止恶意用户探测缓存。 此外，向网络隐藏内容名称可有助于避免恶意用户推断哪些内容项与用户相关； 然而，增加隐私会损害性能[83]。

5.2缓存污染

由于ICN体系结构中的缓存填充可能依赖于用户的访问模式，因此恶意用户可能会用不感兴趣的内容填充缓存，从而破坏缓存带来的性能提升。 此外，所有用户都可以潜在地充当到网络的高速缓存，就像在所有节点都潜在地参与路由和转发任务的移动网络中一样，这意味着它们对其高速缓存的内容和高速缓存访问具有无条件的控制。 高速缓存污染攻击[43]是非侵入性的，因为恶意用户的交互看起来像正常的交互。 例如，恶意用户可以请求大量不受欢迎的内容，以破坏内容的局部性并降低缓存效率[22，65，120]。 路径上缓存更容易受到此类攻击，因为路由器用于缓存的内存有限； 如果缓存了不相关的内容项，则将向内容发布者转发更多对有效内容的请求。 另一方面，为了污染非路径缓存，必须通过勾结大量用户来扩大攻击，以最大化对不受欢迎的内容和虚假的受欢迎的兴趣的请求量。 图10显示了两个用户，U1和U3，它们合谋污染它们之间的缓存。 在这种情况下，U3从U1请求不受欢迎的内容，在R4和R3的缓存上保留此不感兴趣内容的缓存副本，这可能会取代合法的受欢迎内容。



图。 10.将污染威胁隐藏在ICN中。



图。 11.ICN中的高速缓存中毒威胁。

监视缓存上的内容是避免缓存污染的最有效的解决方案[57，121]。 例如，可以使用用于检测和监视其他操作的相同的监视机制来防止高速缓存污染，因为它们已经预见到高速缓存监视度量[22，43，120]。 具体地说，在短时间内监视对同一前缀的传入内容请求对于监视高速缓存污染攻击特别有用[121]。

5.3缓存中毒

Cache中毒攻击对ICN体系结构构成了严重威胁，因为它们的主要优点是容易生成和分发内容。 恶意用户可以填充其缓存并使用伪造的内容满足合法请求，这些内容随后将沿着转发路径缓存。 此外，如果可以预期流行内容的内容名称，恶意用户可能预先生成虚假内容并与其他人串通以请求该内容，以便沿着高速缓存传播该内容。 然后，当原始内容变为可用并且合法用户开始请求时，缓存中包含内容的路由器将为合法请求传递伪造内容[30，34，38，73]。 然而，污染缓存并非易事，可能需要攻击者的额外准备，例如颠覆路由系统[68]，并且可能需要更大的计算能力，因为它们应该尽可能多地向缓存传播虚假内容。 例如，图11举例说明了路由器R2预期流行内容的名称的情况； 它在用伪造的内容填充缓存时为无意中的用户生成和分发内容。

关于虚假内容分发，ICN依赖于缓存内容驱逐或用户明确排除不希望的内容的策略，这通常不足以避免缓存中毒[38]。 让路由器在缓存所有内容项签名之前验证它们是自然的对策，因为它可以防止路由器缓存虚假内容。 然而，这可能严重

影响路由性能，因为路由器需要检查所有传入内容的签名，并且还应该部署信任机制（可能是特定于应用程序的）。 或者，路由器只能在被请求从其缓存中提供内容时验证签名，以防止伪造内容扩散到其他路由器和用户[51]。 此外，使用从用户请求中排除的内容的信息也会导致同样的问题:路由器需要对用户进行身份验证，以避免恶意用户故意排除有效内容[39，65]。 另一种避免缓存中毒的方法是部署具有非法内容名称的黑名单； 然后，路由器可以拒绝它们的传递，并定期使用内容发布者重新验证缓存条目[65]。 然而，为了有效地避免缓存中的虚假内容，更健壮的对策似乎是必要的。

Cache中毒攻击对策的基本途径是检查内容证明； 例如，只有当传入接口与发出请求的传出接口匹配时，路由器才可以接受缓存内容项[51]。 假设用户具有预先知道内容名称的手段，一种解决方案是在内容请求[34]中包括静态内容的散列作为替代组件。 因此，在接收到这样的内容时，用户可以确保该内容是对她的请求的正确答案。 对于动态内容，其思想是将内容发布者的公钥的散列包含到请求中； 每台中间路由器都应检查返回的内容是否引用相同的公钥。 但是，在这种情况下，恶意用户可能与恶意内容发布者串通，恶意内容发布者使用不同的加密密钥对每个内容进行签名，迫使路由器请求每个密钥，从而延迟内容签名检查。 此外，恶意发布者可能会延迟向路由器发送密钥，并选择需要更多计算资源来验证的密钥和签名。 这种情况导致路由器拒绝向合法用户提供服务，甚至停止验证签名，从而导致短暂的安全漏洞。

如果负载过高，路由器可以停止检查内容签名，或者在遇到可疑的内容发布者时，仅当路由器具有足够的空闲处理能力时，路由器才能验证内容签名[35，37，39]； 然而，它可能导致不必要的性能损失。 或者，他们只在内容在高速缓存中存储足够长的时间时才提出签名检查[65]。 由于在NDN/CCN中数据包被签名，Dibenedetto和Papadopoulos[27]建议终端主机报告其路由器检测到的坏数据包。 然后，每台路由器验证数据包签名，如果需要，将其从缓存中删除，将报告转发到上游，并调整转发策略以避免该内容的来源。

表3列出了ICN安全攻击和对策的最后一部分，ICN缓存机制中的分组攻击及其相应的类别、目标、漏洞以及缓解这些攻击的对策。

* 挑战和未来展望

有效地保护计算系统的安全通常不是一项微不足道的任务[100]。 互联网带来了额外的挑战，因为它的普及和无处不在的存在给用户带来了匿名的感觉。 随着互联网上有更多的应用程序，更多的用户公开他们生活的许多方面的信息，例如信用卡号码、银行账户、地址、日常事务、私人生活等。 随着物联网[81]的出现，从家用电器到保健设备，预计一切最终都将连接到互联网。 因此，安全方面变得更加令人担忧，因为敏感内容（例如，关于用户的健康）需要保证只有授权用户才能访问和修改它。

如Abdallah等人所述。 [1]ICN安全解决方案应确保内容的完整性和真实性，验证内容的来源，并保护用户隐私。 考虑到可用性和可伸缩性问题，这个Scope语句并不容易实现。 而ICN本身是本机的

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 网络层命名内容:ICN模型的安全性分析 | | | | | | 44:21 | |  |
|  | 表3。 ICN攻击概述、分类及缓存对策 | | | | |  |  |  |
|  |  |  |  |  |  | |  |  |
|  | 攻击 | | 类别 | 漏洞 | 对策 | | |  |
|  | 缓存侦听 | |  |  | [65，91] |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 定时攻击 | |  |  | [16、65、86] |  |  |  |
|  |  |  |  | 缓存答复 |  |  |  |  |
|  | 请求监视 | | 缓存侦听 |  |  |  |  |
|  |  |  | 任何用户 | [2、16、66、67、83] | |  |  |
|  | 对象发现 | |  |  |
|  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 数据流克隆 | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 监测和审查 | |  |  | [16] |  |  |  |
|  | 缓存污染 | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 内容存储(CS)DOS | | 缓存污染 |  | [22，43，65，120，121] | |  |  |
|  |  |  |  |  |  |
|  | 局部性干扰 | |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 假地点 | |  |  |  |  |  |  |
|  |  | |  | 缓存 |  |  |  |  |
|  | 缓存中毒 | |  |  |  |  |  |
|  |  |  |  | 验收政策 |  |  |  |  |
|  | 假内容注入 | |  | [27、34、35、37-39， | | |  |
|  |  |  |  |  |  |
|  | 内容篡改 | | 缓存中毒 |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  | 缓存中不需要的内容 | |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 缓存误用 | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 垃圾邮件 | |  |  | [30] |  |  |  |
|  |  |  |  |  |  |  |  |  |

在某种程度上，容易受到一些众所周知的攻击（如DoS），在将其部署到现实世界中之前，还应该解决其他重要的安全问题。 下面，我们将讨论一些我们认为对ICN中安全基础的演变非常重要的想法:

新体系结构中的旧威胁:深入检查基于IP的网络中已知的攻击（例如网页劫持、流量拦截和垃圾邮件）的可行性和对ICN体系结构的影响，将使ICN安全领域受益。 深入研究这些攻击有助于发现新的漏洞，也有助于防御这些漏洞，这可能是ICN范例本身提供的。

移动环境中的安全漏洞:移动环境对ICN中的安全构成了额外的挑战，因为所有设备都应该充当内容缓存，从而提高了缓存侦听、监视和审查的可能性。 解决移动ICN安全漏洞和威胁的工作仍然很少。 应当更多地调查ICN模式在移动环境中的影响，因为ICN可能容易受到当前移动威胁的影响，甚至在移动网络中引入新形式的漏洞。

用户隐私与恶意活动检测:以前关于对用户的互联网流量进行未经授权的监视和间谍活动的案例增加了对用户隐私和匿名性的担忧。 为了充分考虑作为当前Internet的替代方案，ICN体系结构必须遵守用户权限和有关用户隐私的国际规则。 要解释这些机制的含义并不容易，如何同时启用隐私和恶意活动检测也不清楚。 此外，确保各国政府仅为安全目的而不是为审查目的收集用户的通信模式，或防止滥用这种信息来胁迫或威胁个人，这超出了技术所能提供的范围:它要求用户行为得当，公民对政府活动保持警惕。

攻击影响评估:深入了解ICN中的攻击潜力是一个很大的挑战。 我们列出了几项研究工作，提出了潜在的安全性

ICN存在的问题； 然而，在仿真或实际的ICN部署中，只有很少的网络能够有效地显示和分析此类攻击的影响。 这样的分析和讨论对于真正理解哪些方面需要进一步研究，然后将研究正确地定位于更安全的ICN体系结构非常重要。

更好地评价解决方案:迄今为止，调查文献中提出的许多解决方案没有得到深入评价。 更现实和详细的评估对于更好地理解所提解决方案的行为至关重要，包括有效性、间接费用、副作用和权衡[6]。 已经为ICN体系结构开发了许多测试床[46、80、98、105]，应该更广泛地使用它们来提供有关ICN安全解决方案的更好知识。 特别是，阻碍内容缓存或限制重新请求率的解决方案可能会对用户体验产生负面影响，应该更好地进行调查[107]。

可伸缩性问题:这里描述的许多安全解决方案直接影响可伸缩性、ICN体系结构的存在理由和中心特性。 例如，一些解决方案使用集中式实体进行访问控制强制[31、32、36、102]或密钥真实性验证[96]。 在评估ICN上下文中的攻击的安全解决方案时，可伸缩性应该是一个前台属性。

容错:一些建议的解决方案基于可能构成单一故障点的第三方实体[32]。 这些实体除了影响系统的可伸缩性外，还可能成为DoS攻击的目标，损害整个网络。 期望从解决方案中获得一些受控冗余，以利用容错性和可伸缩性。

信任管理:密钥与其所有者之间的绑定应该通过信任机制来保证。 ICN并不强制实施特定的信任管理方案，而是让应用程序来定义自己的信任机制和来源。 目前Internet中使用的方法，如分层公钥基础设施(PKI)，在ICN中也可以采用，但更可扩展的方法，如SPKI/SDSI[19]，更适合ICN的分散性，如Zhang等人所述。 [128]。

密钥吊销:除了检查密钥与其所有者之间的绑定之外，客户端还需要验证给定密钥是否仍然有效（即，它未被吊销）。 由于密钥是数据内容，因此可以将其存储在网络缓存中并从网络缓存中检索，因此，如果密钥的颁发者吊销了密钥，则密钥可能会过时。 在ICN[82，96，123]中提出了一些检查密钥状态的方法，但更通用的解决方案，可能与信任管理方案集成，将是受欢迎的。

ICN范式为研究人员提供了将安全性嵌入到Internet核心的机会，并重新思考在传统Internet体系结构中哪些是有效的，哪些是不成功的。 然而，随着新的威胁的出现，新的攻击被发现，新的安全措施被提供，保护网络的安全将始终是一项持续的努力。 从嵌入到体系结构中的健壮和巩固的安全基础开始，研究人员将能够提供更好和更快的对策，将互联网变成一个更安全的地方。

7总结发言

ICN模式是一种很有前途的未来Internet体系结构，它提供了一种更适合于内容分发的Internet。 然而，从安全的角度来看，ICN面临着巨大的挑战。 在本文中，我们组织、分类、讨论和探讨了有关ICN中的安全漏洞、攻击和对策的文献，涉及三个关键的ICN方面:内容、路由器和缓存。 我们注意到，虽然内容和

内容名称（如完整性和隐私）已经得到广泛解决，对路由器和缓存的威胁仍然需要关注，尤其是当它们允许虚假或损坏的内容到达用户时。 因此，需要进一步研究安全解决方案和度量，以利用ICN作为一个完整的、健壮的体系结构，能够满足当前和未来对性能、移动性和安全性的需求。 我们期望，这种知识系统化能够为读者提供深入了解ICN攻击和漏洞的方法，帮助他们在发现漏洞点以及新的解决方案和对策以减轻这些漏洞方面构建未来的工作。