doi: 10.7690/bgzdh.2013.02.012

NDN 安全机制初探

孔思淇，潘泽友，王开云
（中国工程物理研究院计算机应用研究所，四川 绵阳 621900）

摘要：针对当前网络架构安全的问题，以内容中心网络（content-centric networking，CCN）为例对 NDN 的安全机制进行研究。分析 NDN 保护并信任内容本身的安全方式，引出通过减少内容到用户间的跳数，可以有效避免中间系统对数据的破坏的理念，并结合现有的基于 NDN 架构的应用 ACT、VoCCN 和 ANDaNA，分析 NDN 安全机制在真实网络下的应用情况，指出现有 NDN 安全机制存在的漏洞。该分析结果可为今后研究海量数据下的信息过滤问题提供参考。

关键词：内容命名网络；内容中心网络；内容信任；信息安全；安全机制
中图分类号：TP393　　**文献标志码**：A

Research of NDN Security Mechanism

Kong Siqi, Pan Zeyou, Wang Kaiyun
(*Institute of Computer Application, China Academy of Engineering Physics, Mianyang* 621900, *China*)

Abstract: Aim at security problem of network frame, take content-centric networking (CCN) as example to research the NDN security mechanism. Analyze the NDN safety way which on the protection and to trust the content itself. Bring an idea that by reducing the hops between users, it can effectively avoid data to be broken in the intermediate system. Through the existing application ACT, VoCCN and ANDaNA based on NDN framework to analyze the actual application state of NDN security mechanism in real network, point out the existing NDN security mechanism's holes. The analysis results can provide on information filtering under mass data research with reference.

Key words: content named network; content-centric network; content trust; information security; security mechanism

0　引言

内容命名网络（named data networking，NDN）是美国 NSF（自然科学基金）所设立的 FIA 计划资助的 4 个主要项目之一，其目标是使互联网支持不考虑内容存储所在的物理位置，直接提供面向内容的功能[1]。作为一种未来网络的架构，NDN 将传统的 IP 定位模式转变为内容定位，以内容为中心的安全机制是重要的研究方向。NDN 通过命名数据代替地址以定位资源，将数据转变成 first-class 实体。NDN 采用层次式的结构命名设计，命名没有语义，可以来自于应用、机构或全局的约定等，反映在前缀的转发规则上。文献[2]简要介绍了 NDN 的 2 种主要数据包格式和路由方式。

针对当前网络架构安全的问题，主要有 2 类解决方案[3]：第一类方案通过在协议栈中增加一个专门的“安全信任层”来解决安全问题；第二类方案则通过为每一层都分别设计安全机制来保障互联网的安全性。但前者不能保障其他层的安全，后者又使协议栈过于复杂，都无法从根本上解决互联网的安全问题。下一代互联网安全性标准应该在开放、简单和共享为宗旨的技术优势基础上，从网络体系结构上保证网络信息的真实和可追溯，进而提供安全可信的网络服务。笔者针对当前网络架构安全问题，以内容中心网络（content-centric networking，CCN）为例对 NDN 的安全机制进行研究。

1　NDN 安全机制

用户获取网络数据的时候，总是希望从预期的源端得到渴望的文本，并在传输的过程中不被修改。现有的基于文本的认证方式主要有 2 种：首先是通过哈希，这种方式可以评价数据的有效性，但不能确定出处和可用性；其次是签名，这种方式与哈希相反，不能评价数据的有效性，只能确认出处和可用性。

通过文献[4-6]可以得出：NDN 安全机制的核心理念是让负载更接近源。NDN 计划组认为，减少数据与用户之间的跳数可以有效避免中间系统对数据的破坏，使数据正确、有效到达用户端的概率更高。NDN 通过一系列机制来实现这个理念，这些机制关注命名与内容之间的关联，通过内容确认等方法保证 NDN 安全机制无论是在当前基于连接的还

收稿日期：2012-08-02；**修回日期**：2012-08-25
基金项目：国家“九七三”重点基础研究发展规划项目（2010CB328104）；中国工程物理研究院科学技术发展基金（2010B0403063）
作者简介：孔思淇（1986—），男，吉林人，硕士，助理工程师，从事网络体系结构与计算机应用技术研究。

是在未来基于内容的网络连接下都是可以通用的，是有能力保障内容安全的、易部署的。

CCN 是 NDN 计划的一个具体方案，由帕洛阿尔托实验室主导[6]，NDN 安全机制可以透过 CCN 予以体现。CCN 建立在基于内容安全的概念之上，强调保护并信任内容本身，而不是传统的保证内容传播路径的安全。CCN 中所有内容通过数字签名来验证，通过加密保护私有内容。CCN 具备动态内容缓存能力，可减少内容传输过程中所通过的中间机构，减少内容到用户间的跳数。其主要安全机制包括内容确认、管理信任和内容保护与访问控制 3 种。

1.1　内容确认

CCN 采用“自验证”命名规则(self-certifying)，将密文摘要和内容提供商的 key 加入到命名结构中去。CCN 认证将命名与内容相绑定，每个 CCN 数据包中都有签名，此签名基于命名和内容，并使用少量辅助性的数据作为签名验证。主要签名公式为：M(N,P,C) = (N, C, SignP(N,C))，N 是内容 C 的名字，P 是内容提供商，M 为通信文本。这样可以方便内容提供商将多个名字与同一个内容相绑定。CCN 数据是可以公开验证的，即任何人都可以验证命名与内容是否通过某个 key 相绑定。这样做的优点有 3 个：无论 N 是什么，都可以做到本地独立性；解决内容命名格式的验证问题，可以通过前缀追溯信源；方便用户对 P 进行验证(即验证内容提供商是否是命名 N 的合法源)且可以做到完全地自主地本地计算验证。

这个签名公式还能够解决前文提到的现有方法无法完全确保数据有效性、出处和可用性 3 个内容属性(这 3 属性是保证数据安全的必要不充分条件)的问题，步骤如下：

1) 确认给定的<命名，内容>映射是否被特定的 key 标记，可以对内容的有效性进行验证；

2) 确认 key 属于谁，可以定位内容出处；

3) 决定此源是否可接受，即是对内容可用性进行判断。

1.2　管理信任

CCN 对信任的定义是基于上下文的，由特定文本内容及其用途严格决定。

1) 密钥信赖。

针对传统的密钥管理问题，即如何通过公钥将个体与组织联系起来，这种情况下最主要的问题是确定谁是某个内容块的合法签名者。CCN 将其简化为几个方面：首先，将 key 定义为另一种类型的 CCN 数据，只在必须验证内容的时候定位并获取；其次，在第一条的基础上，密钥(内容)提供商只在需要验证文本内容的时候才发布密钥，将 CCN 命名与 key 通过密钥(内容)提供商签名绑定；第三，CCN 不授权通用的信任模型，只针对不同应用/环境应用密钥。如图 1 所示，通过 parc.com 和 george 的 2 次签名，将文件的 key 作为 CCN 数据的一部分，在用户需要验证文本内容时传递给用户，供用户验证文本的发布者。

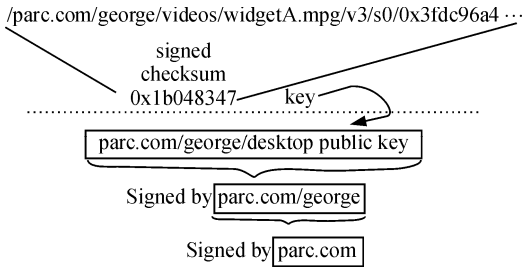

图 1　CCN 密钥信赖示意图

2) 基于证据的安全。

在 CCN 中加入了安全引用的概念，引用的方式类似于受信的超链接和书签。CCN 内容项能够通过目标文本的密文摘要或者其密钥(内容)提供商的 ID 指向其他目标。这与传统形式上的委托类似，但 CCN 的这种方式还可以被用来建立一个内容受信网络，每个文本片都可以作为潜在的“证据”，以证明文本指向的正确性。

1.3　内容保护和访问控制

CCN 内容访问控制的主要方式是加密，CCN 不需要受信的服务器或者目录来制定访问控制策略，因为只有授权用户能够解密私人内容。且 CCN 并不针对网络安全的问题提出解决方案，只提供解决内容合法性的机制，并对机制的有效性进行保障。

CCN 主要面对的攻击包括：兴趣泛洪攻击(interest flood attack)、内容污染攻击(content pollution attack)和 DOS/DDOS 攻击等。

CCN 通过在 Interest 和 Data 之间制造流量平衡来预防数据的过度转发和本地基于数据(此处的数据指的是真实的文件数据，不包括攻击者随机生成的数据包)的 DOS，无论某个数据包被下游的用户请求多少次，存储这个数据包的路由器只向用户方向的直连路由器转发一份数据，由“最后一跳”路由进行大面积分发。

CCN 路由采用 2 种方法来减轻可能发生的“兴趣泛洪攻击”：首先，每个 CCN 中间节点都能看到自身转发的兴趣包(无论这个兴趣包是否成功地检索到数据)，这在 IP 网中是做不到的，CCN 路由器可以在此基础上根据某个前缀成功请求到的数据量，设计算法来限制转发这个前缀所请求的兴趣；其次，CCN 可以像 IP 网封锁 IP 地址一样通过下游路由器限制某个命名前缀的兴趣包转发。

内容污染攻击指的是黑客主动产生恶意内容来匹配合法的请求。针对内容污染攻击，CCN 通常使用签名验证来解决，但这对非核心路由器来说可能负担过重。

2　NDN 安全机制的应用

目前，基于 NDN 架构的应用主要有 ACT[7-8](audio conference tool)，VoCCN[9](voice-over content-centric networks)和 ANDaNA[10](anonymous named data networking application)等，均由 NDN 项目组设计实现，并已进行初步测试，本节主要对其中使用的安全机制进行分析说明。

2.1　ACT

ACT 是基于命名数据范例来支持高鲁棒性语音会议的工具，已在 NDN 测试平台上进行了真实流量测试。其主要目标是：报告已存在的会议；实时交付语音数据；媒体数据处理。在安全方面，ACT 需要提供数据真实性保证、参会人员控制和私人会议匿名管理。ACT 摒弃了传统的集中控制和基于会话的安全方式，采用分布式安全机制来保障会议数据加密和参会人员控制 2 个重要安全需求。在技术上，ACT 采取非对称加密与对称加密相结合的方式保障上述需求。

ACT 的关键元素是“会议发起人(Initiator)”，会议发起人发起会议并掌握着合法参会者名单，它为每个会议产生 2 个“公钥-私钥”对，分别为：“参会人公私钥对”和“会议公私钥对”，同时为加密会议数据产生“会话密钥”。会议发起人在产生“参会人公私钥对”后，将公钥保留，将私钥作为数据的一部分(见 1.2 小节)发布给合法参会者，关于会议的信息由参会人公钥加密，私钥解密；如果合法的参会人想要参加会议，那么会议发起人就用参会人公钥加密会议私钥，然后将其发送给参会人，参会人使用参会人私钥解密后即可加入会议；会议发起人最后建立一个会话密钥(session key)来加密语音数据，使用会议公钥对其加密并发布，合法参会人使用会话密钥来获取语音数据。之所以使用对称加密方式对语音数据进行加密，主要出于节约资源的目的，如果在与会人员众多时使用非对称加密方式，产生的密钥数量将成几何级数上升，另外，人的声音可以通过音色来分辨，不易伪造。

2.2　VoCCN

VoCCN 是基于内容范例的实时会话(VoIP)应用原型系统。其目的是提供比 VoIP 更简单、更安全、扩展性更强的基于 NDN 架构的语音电话服务。VoCCN 的结构、原理与 VoIP 类似，都是维持 2 条信道：信令信道和媒体信道，在 VoCCN 中呼叫方映射一个“SIP(session initiation protocol)请求”到兴趣包内以请求被叫方，网络将兴趣包路由给被叫方，被叫方响应请求，完成信令交互，建立连接。

VoCCN 的安全面临 3 个问题：对话双方的真实性；信令信道的加密；媒体信道的加密。当用户 A 试图与用户 B 通话时，首先会发送预先确定命名的请求文本，B 收到这个文本并产生一个“公钥-私钥”对，自身保留公钥，将私钥发回给 A，这个过程 B 并不去确认 A 的身份(因为当通话开始后自然可以确认)，当通话结束后，A、B 均可以将密钥与自身 ID 相绑定供后续相互确认身份使用；为保证信令通道的安全，VoCCN 使用简单内联信息加密和认证方案，呼叫方使用随机产生的对称密钥 sk 加密 SIP 请求信息，并使用被叫方的公钥加密 sk，打包发送给被叫方，被叫方收到后，用私钥解密出 sk 和 SIP 请求信息，再使用 sk 加密对 SIP 请求信息的响应，传回给呼叫方，完成信息交流；为保证媒体信道的安全，VoCCN 采用 SRTP 协议加密语音。通信过程如图 2 所示。

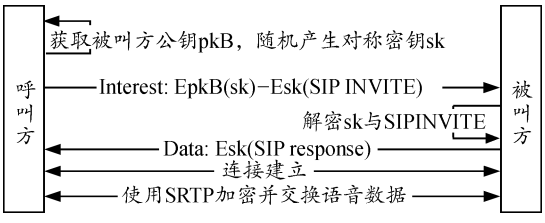

图 2　VoCCN 通信过程

2.3　ANDaNA

ANDaNA 是一种建立于 NDN 基础架构上的覆盖层网络，其目标是解决文献[5]提出的 NDN 架构

所面临的 cache 隐私、命名隐私和签名隐私 3 个挑战，为用户提供隐私保护和匿名功能。它可以看作是 Tor[11]的改编，适用于中小规模的交互式通信，如浏览网页与紧急通信等以低延迟为特征的服务，目前其原型系统运行在华盛顿大学的 ONL[12]平台上。ANDaNA 防止入侵者通过关联用户及其检索的内容进行攻击。

在 ANDaNA 中的每个路由器均被称为 AR(anonymizing router，AR 同时也是 NDN 节点)，AR 通过广播自身的公钥(结合命名空间、组织、公钥指纹及其他辅助信息)加入 ANDaNA 网络，AR 要经常更新自身的公钥来保障签名与加密的安全性。关键的网络流量通过在 2 个 AR 间建立临时虚电路(ephemeral circuits)来传输，在通信内容被交付或超时后，虚电路即被撤销。将临时虚电路两端的 AR 定义为一个“路由对”，将靠近兴趣发起方的路由称为“入口路由”，另一个称为“出口路由”，2 个路由不能同属一个管理域，且不能共享相同的命名前缀，路由对由用户根据辅助信息选择，如图 3 所示。

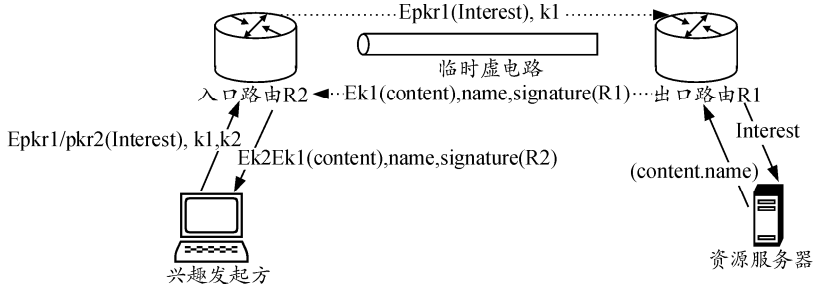

图 3　ANDaNA 传输原理

ANDaNA 提出通过非对称和基于会话的技术来保障 NDN 流量的隐私和匿名：前者主要保证用户兴趣包和返回内容的安全性，当选定了路由对并建立了临时虚电路后，用户使用 2 个 AR 广播的公钥加密兴趣包并发送给入口路由，同时用户产生 2 个对称密钥(k1, k2)，分别分发给出口、入口路由，入口路由用自己的私钥解密后将兴趣包发给出口路由，出口路由再次解密后即按正常的 NDN 内容检索方式检索，当其他路由返回给出口路由一个内容包时，出口路由将此内容包使用 k1 进行加密，然后结合源命名和签名将其发送给入口路由，后者解析前者的信息，去除源命名和签名后使用 k2 对剩下的密文进行再次加密，并附带出口路由发来的源命名和入口路由的签名转发给用户，用户解密获得内容文本并验证源端可信度；后者的目的是减少使用公钥加密所带来的计算开销和密文规模，提供了 DH 密钥交换[13]和 SSL/TLS 协议 2 种方式减少密钥交换的开销。针对 AR 的公钥属于广播发送，攻击者可以进行重放攻击的问题，ANDaNA 采取“每个兴趣只能被响应一次”的原则(见 1.3 小节)，对 cache 中的每个兴趣，如果对它的响应文本还存在于 cache 中并且未过期，无论后续有多少次相同的兴趣请求，均不予响应也不予转发。

3　NDN 安全机制存在的问题

目前，NDN 对于数据安全的做法是对所有数据进行签名，并且接收者通过兴趣来驱动数据的传输，这样可以避免第三方滥发垃圾数据，但也存在几个问题：

首先，存在着对签名管理和签名信任的问题，特别是在发送大文件的时候，对每段数据进行签名会影响效率；

其次，使用兴趣推动数据传输的方式，可能引起“Interest flooding”的问题，而现有的方案对其解决的并不是很有说服力。如 1.3 小节中描述的，以某个前缀成功请求到的数据量为根据，限制转发其所请求的兴趣的前提是，非法的兴趣泛洪所伪造的兴趣包在大多数情况下请求不到任何数据。但实际情况并非如此，如果攻击者控制一些服务主机并主动产生内容来匹配自身非法的兴趣包，也可以自由控制数据请求成功率，进而破坏边缘路由；

第三，对 NDN 的攻击主要通过 DOS/DDOS 来“隐藏/淹没”合法内容，使路由器中有用的数据包被无效的数据所代替。CCN 方案给出的解决办法是用户手动设置合法的内容提供商(publisher)，这样做的效率比较低；

第四，文献[5]提出的 NDN 架构所面临 cache 隐私问题，即如何在查找效率和内容安全之间取得平衡，ANDaNA 中使用对称/非对称密钥混合使用方式来减少系统性能负担，但“每个兴趣只能被响应一次”的安全原则又增加了系统的开销，如何在二者之间取得平衡依然是未来研究的关键问题。

4　总结

笔者阐述了 NDN 架构的特点，结合实例与具体应用详细说明了 NDN 架构的安全机制，并分析了现有安全机制解决方案所存在的问题，可为今后研究海量数据下的信息过滤问题提供参考。

参考文献：

[1] 吴建平，李星，刘莹. 下一代互联网体系结构研究现状和发展趋势[J]. 中兴通讯技术, 2011, 17(2): 10−14.
[2] 任勇，徐蕾，叶王毅，等. 未来网络的研究进展和发展趋势[J]. 中国科技论文在线, 2011, 6(4): 247−255.
[3] 陆璇，龚向阳，程时端. 新一代互联网体系结构[J]. 中兴通讯技术, 2009, 15(5): 53−56.
[4] Diana Smetters, Van Jacobson. Securing Network Content[R]. CA, USA, PARC, 2009.
[5] Van Jacobson, Diana Smetters, James Thornton, et al. Networking Named Content[J]. Communications of the ACM, 2009, 55(1): 117−124.
[6] Zhang LiXia, et al. Named Data Networking (ndn) Project[R]. Aiken SC, USA: PARC, 2010.
[7] Z. Zhu, S. Wang, X. Yang, et al. ACT: Audio Conference Tool Over Named Data Networks[C]// Proceedings of the ACM SIGCOMM workshop on Information-centric networking. New York, ACM, 2011: 68−73.
[8] Zhu Z, Gasti P, Lu Y, et al. A New Approach to Securing Audio Conference Tools[C]// Proceedings of the 7th Asian Internet Engineering Conference. New York, ACM, 2011: 120−123.
[9] Van Jacobson, Diana K. Smetters, et al. Braynard. Voccn: Voice-over content centric networks[C]// Proceedings of the 2009 workshop on Rearchitecting the internet. New York: ACM, 2009: 1−6.
[10] DiBenedetto S, Gasti P, Tsudik G, et al. ANDaNA: Anonymous Named Data Networking Application[C]// Proceedings of the Network and Distributed System Security Symposium. New York: ACM, 2012.
[11] Dingledine R, Mathewsonn N, Syverson P. Tor: The second-generation onion router[C]// Proceedings of the 13th conference on USENIX Security Symposium, 2004. CA: USENIX Association Berkeley Volume 13: 21−21.
[12] Open network lab[EB/OL]. (2012−03−19) [2012−04−05] http://onl.wustl.edu.
[13] W. Diffie M. Hellman. New directions in crypto- graphy [J]. IEEE Trans Information Theory, 1976, 22(6): 644−654.

****

(上接第 39 页)

表 3 中状态 3 对应 00100000，状态 4 对应 00010000，状态 7 对应 00000010。

表 4　BP 神经网络故障诊断结果

样本	诊断输出 (10^{-6})								诊断结果
	节点 1	节点 2	节点 3	节点 4	节点 5	节点 6	节点 7	节点 8	
1	1	116	999986	270	371	14778	0	17	管体过流
2	11	152	11	999999	78	51	0	0	波导故障
3	0	110	0	2078	1332	1303	999999	6	激励故障

5　结束语

实践结果证明：人工神经网络满足了雷达故障自动检测与诊断系统的高可靠性和可维护性要求，是一种具有较大应用潜力和实用价值的新方法。

参考文献：

[1] 张安华. 机电设备状态监测与故障诊断技术[M]. 西安: 西北工业大学出版社, 1995.
[2] 张绪锦. 雷达故障检测与诊断技术的理论研究及实践[D]. 合肥: 合肥工业大学, 2000.
[3] 李明亮，姜秋喜，韩晓玲. 基于网络雷达的一种数据关联算法[J]. 四川兵工学报, 2010, 31(2): 5.
[4] Major Orlando J. Illi, Jr, Dr. Frank L. Greitzer, Lars J. Kangas, Tracy J. Reeve. An artificial neural network system for diagnosis gas turbine engine fuel faults[C]. Wakefield: Presented at the 48th Meeting of the Mechanical Failures Prevention Group, 1994.
[5] Laurie Webster II, Jen-Gwo Chen, Simon S. Tan. Validation of Authentic Reasoning Expert Systems[J]. Information Sciences, 1999, 117: 19−46.
[6] Zhou Z, Hu W, Leung A. A Intelligent Integrated System Scheme for Machine Tool Diagnostics [J]. The International Journal of Advanced Manufacturing Technology, 2001, 18: 836−841.
[7] Yam R C M, Tse P W, Li L, et al. Intelligent predictive decision support system for condition-based maintenance[J]. The International Journal of Advanced Manufacturing Technology, 2001, 17: 383−391.