



专题:信息中心网络(ICN)

信息中心网络中授权视频访问控制

周自飞¹, 谭小彬¹, 牛玉坤¹, 邹长春²

(1. 中国科学技术大学中国科学院地理空间信息处理技术和应用系统重点实验室 合肥 230027;

2. 美国中佛罗里达大学电气工程与计算机科学系 美国佛罗里达州奥兰多 32816)

摘要:信息中心网络(ICN)能够极大地提高视频内容的传输效率,然而 ICN 中内网缓存机制也给授权视频的访问控制带来了严峻的挑战。授权视频访问控制的目的是保证只有已授权用户才能观看授权视频,防止授权视频被非法观看和使用。在 ICN 中,当授权视频被缓存在路由器上后,便不受视频发布者的控制,任何人都能够从路由器上获取授权视频。目前存在的方案不能很好地解决这个问题,提出了一种基于分割和数字水印的访问控制方案,将授权视频分割成 PCB(public content block,公开内容块)和 CKB(content key block,内容密钥块)两部分,其中 PCB 一般比较大,对所有用户都是相同的,而 CKB 一般比较小,并且采用数字水印技术实现不同的用户对应不同的 CKB,用户必须收到 PCB 和 CKB 之后才能观看视频。通过分析,提出的授权视频访问控制方案在安全性和网络资源优化两个方面具有很好的性能。

关键词:信息中心网络;授权视频;访问控制;数字水印

doi: 10.3969/j.issn.1000-0801.2014.09.008

Access Control for Authorized Video in Information-Centric Networking

Zhou Zifei¹, Tan Xiaobin¹, Niu Yukun¹, Cliff C Zou²

(1. CAS Key Laboratory of Technology in Geo-Spatial Information Processing and Application System,

University of Science and Technology of China, Hefei 230027, China;

2. School of Electrical Engineering and Computer Science,

University of Central Florida, Orlando, Florida 32816, USA)

Abstract: Information-centric networking (ICN) can greatly improve the efficiency of video content, however, in-network caching in ICN also brings us a new access control challenge. The purpose of authorized video access control is to ensure that only authorized users can watch them, and to prevent unauthorized accesses to these authorized videos. In ICN, when authorized videos were cached in the routers, anyone can get and watch them without the authorized videos' producers' permission. The existing methods could not solve this problem well, an access control scheme was proposed that based on splitting and digital watermarking. The authorized video was splitted into two parts, public content block (PCB) and content key block (CKB), respectively. PCB which was generally relatively large, was the same for all users, and CKB which was generally relatively small, was unique for each authorized users using digital watermarking technology. Users must received both PCB and CKB to watch videos. After the analysis, the access control scheme for authorized videos has a good performance in both security and network resource optimization.

Key words: information-centric networking, authorized video, access control, digital watermarking



1 引言

随着网络技术和各种视频服务的兴起以及智能终端的迅速发展,用户对网络视频的访问需求日益增长。根据思科公司的分析报告^[1],2012年全球消费者互联网视频流量占消费者互联网流量的57%,而到2017年这一比例将达到69%。思科公司预计,到2017年每秒钟将有近百万分钟的视频内容通过互联网进行传输,直播视频流量将增加3倍;另外,到2014年,视频内容将占全球移动数据流量的66%^[2]。在网络视频业务中,需要面对大并发量的用户以及他们多样化的需求,这就需要高效的视频内容分发和传输技术。传统基于TCP/IP的互联网架构存在一些根深蒂固的问题,以IP地址为核心、以传输为目的、按照端到端原理设计,使得它难以应付大规模的数据流量和针对多用户的视频内容分发。

TCP/IP架构的局限性促进了其他网络技术的发展,相继产生了一些数据分发技术,如P2P(peer to peer,对等网络)^[3]、CDN(content delivery network,内容分发网络)^[4]、Web cache(网页缓存)^[5]、Pub/Sub(publication/subscription,发布/订阅)^[6]等。这些数据分发技术有助于互联网中内容的访问,能够提高数据传输效率,然而它们通常在网络应用层进行操作,不能利用底层网络拓扑结构的信息使网络达到最佳性能,使得网络中资源的利用率不高,造成了网络资源的浪费。

为了解决目前互联网在可扩展性、移动性、安全性以及效率等方面存在的问题,一种解决方案就是采用新型的通信模式。ICN(information-centric networking,信息中心网络)就是在这一背景下产生的,ICN对内容及其物理位置进行解耦,因为人们更加关心的是内容本身,而不再关心内容在哪里。ICN的网络通信模式由传统的“推”改为“拉”,安全机制直接构建在信息上而不是主机上。另外,它还支持主机移动^[7]。

ICN的另一个重大改变是增加了内网缓存功能,网络中的路由器可以缓存数据,这一重要特征可以提供快速而且有效的内容获取,解决海量信息高效传输的问题,目前关于ICN路由器缓存已有广泛的研究^[8-10]。ICN将会给网络视频行业带来巨大的好处,但也带来了新的安全和隐私问题,例如在授权视频访问控制方面的版权保护问题,将变得更加复杂。网络中具有版权的视频只有在用户被授权后才能观看,如何保护这些授权视频的版权,对于内容出

版商使用互联网进行可靠的视频内容分发来说是一个十分关键的问题。

在传统的P2P网络和CDN中,数字水印是一种最常见的保护视频版权的技术,目前在这方面进行了许多研究工作^[11-13]。然而,内网缓存机制使得授权视频访问控制中的版权保护在ICN中变得更加复杂。当授权视频被缓存在路由器中后,将不再受到视频发布者的控制,任何人都能够在不需要视频发布者允许的情况下从路由器的缓存中获取授权视频并观看。由于视频发布者失去对授权视频的控制,P2P网络和CDN中的方法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。另外,目前ICN中的加密方案也不能够很好地保护授权视频的版权,因为当某个用户泄露解密密钥后,无法判断是谁泄露了密钥,仍然存在所谓的版权保护问题。因此,需要设计一个视频版权保护的访问控制系统,使得在ICN中,虽然任何人都能够从路由器中获取授权视频,但只有已授权用户才能够观看视频。

ICN在路由器中缓存数据,大大提高了视频分发效率,特别适合视频内容的传输,但存在访问控制问题,针对该问题,本文提出一种ICN中基于分割和数字水印的访问控制方案,用来保护授权视频的版权,从而实现高效安全的视频访问控制。基本原理是:针对一个授权视频(用 V 表示),将它分割成两个部分,分别是PCB(public content block,公开内容块)和CKB(content key block,内容密钥块),PCB内容大小远远大于CKB内容大小。PCB可以被缓存在路由器中,任何人都能够从路由器中获取它,这样可以提高传输效率。但如果没有获得CKB,任何人都不能够恢复出 V ,只有被授权的用户才能够从视频发布者那里获取CKB。用唯一且不同的CKB对应不同的已授权用户,而且这些不同的CKB都能和PCB结合在一起恢复出原始的授权视频内容。针对第 i 个已授权用户,CKB用 C_i 表示,在 C_i 中,加入唯一标志该用户的数字水印,利用非对称加密的方式将 C_i 发送给该用户,从而实现授权视频版权保护的访问控制。该方案不仅能实现高效的视频分发,而且能够保护授权视频的版权。

举一个简单的例子,针对一个大小为2 GB(2 048 MB)的视频,视频发布者首先利用基于分割和数字水印的方案将其分割成PCB(如2 000 MB)和CKB(48 MB),并且保证分割后当用户只获取PCB时仍然无法观看电影。PCB可以被缓存在路由器中,结合互联网的特点和用户的分布

情况,大部分用户从路由器中获取特定内容的时间小于从视频发布者那里获取该内容的时间,这样该授权电影有大约 97.66% 的内容可以被用户以更快的速率访问。另外,由于已授权用户离可以获取授权电影的路由器的距离比离授权电影发布者的距离更短,内容传输失败的几率更低,而且重连更快,从而大大提高了数据的传输效率。然后,针对不同的已授权用户,视频发布者在 CKB 中加入不同的数字水印,这些数字水印对用户是不可见和不可更改的,当已授权用户请求该电影的 CKB 时,视频发布者利用 RSA 加密的方法将其传给该用户。只有已授权用户才能够解密 CKB,当已授权用户泄露该解密后的 CKB 时,通过分析其中加入的水印就可以知道是谁泄露了该视频内容。

另外,不考虑在所有网络架构中都存在的一种侵犯版权的行为:当一个授权用户获得授权视频后便可观看该视频,可以通过某种方法(如录制)将该视频保存下来,然后传给其他用户,这样授权视频的版权就受到了侵害。这种行为完全由用户决定,针对这种行为的版权保护方案是技术上难以实现的。本文主要内容集中在信息中心网络中的版权保护的访问控制上。

首先对 P2P 网络和 CDN 以及 ICN 中的授权视频访问控制进行调研,然后提出基于分割和数字水印的访问控制方案,最后对本文进行总结。

2 现有授权视频访问控制方法

2.1 P2P 和 CDN 中授权视频的访问控制

授权视频的访问控制问题主要是指保护授权视频的版权,防止非法用户在没有授权的情况下观看视频内容。网络视频行业的迅速发展给授权视频的版权保护带来严峻的挑战。关于这个问题,研究人员进行了大量研究。参考文献[14]基于对不同 P2P 文件分发技术主要类型的讨论和中国 P2P 版权保护问题,从直接侵权、辅助侵权和技术中立 3 个方面分析了目前中国版权保护的状态,然后预测了中国未来 P2P 文件分发技术的前景。提出关于 P2P 分发技术的文件版权保护应该得到重视,并提到议事日程上,进而提高信息共享的水平。下面介绍一些 P2P 网络和 CDN 中关于版权保护的具体技术。

DRM (digital rights management, 数字版权管理) 技术是一种保护多媒体内容使用权的技术。针对数字媒体, DRM 技术能够用来保护授权视频免遭未经授权的播放或者非法复制,从而达到保护数字媒体版权的目的,已经有

一些 DRM 系统用来保护分布式数字多媒体内容的版权^[15,16]。数字水印技术是一种将一些标识信息直接嵌入数字载体中的信息隐藏技术,而且数字水印的嵌入不影响原始载体的使用价值,有些数字水印甚至不容易被人察觉。通过在数字媒体中隐藏这些数字水印,能够判断数字媒体是否被篡改,还能够确认出内容创建者和购买者,也可以用来传送隐秘信息。

参考文献[17]提出了一种在互联网中针对大规模内容交付的集成的数字版权保护方案,该框架集成了匿名对等身份验证、内容中毒、同行串通检测和声誉聚集 4 个部分,并且对 4 个部分进行了详细讨论。在 P2P 网络下进行研究,使用 DRM 和数字水印技术对 P2P 网络进行版权保护,关于视频的版权保护也进行了相关分析。文中的增强信任机制、流言传播协议和实验结果对未来网络应用具有广泛的影响,这些将扩大 P2P 网络中的合法应用规模。

参考文献[12]提出了一种新颖的针对基于多分辨率小波分解的视频数字水印方法,用来对视频的版权进行保护。所用的数字水印是一个二值图像,通过量化被嵌入第二小波分解级的 LH、HL 和 HH 频带的小波系数中,并且使用一个密钥将水印的每一位分散至多个系数中。使用 9 种不同的攻击方法对不同的视频进行攻击,实验结果表明该方案和算法对攻击具有顽健性,而且嵌入的数字水印是不可见的。本文方案中需要的也是用户不可见和不可篡改的数字水印。

参考文献 [18] 提出了一个 PCP (P2P based content protection) 系统,这个系统基于一个可信模型,专注于解决 P2P 网络中的内容安全、权限管理和访问控制问题。系统采用加密、数字水印和包装技术来保护内容的机密性和完整性,并且支持权限认证和盗版跟踪。针对访问控制,认证被分为证书、身份和信用 3 个方面。PCP 主要用来为 P2P 网络中的内容交付提供一种知识产权保护解决方案。

在 P2P 网络和 CDN 中,DRM 和数字水印是两种主要用来保护授权视频版权的技术,关于这方面的研究还有很多。但由于 ICN 的新特征(主要是内网缓存机制和“拉”的传输模式),上述技术不能直接用于 ICN 中来保护授权视频的版权。由于内网缓存机制,当一个已授权的用户请求一个授权视频并获取视频后,该授权视频将会缓存在路由器中,这时,路由器上缓存的视频已经不受授权视频发布者控制,其他任何人都能够从路由器中获取该视频并观看。这样即使在授权视频中加入数字水印,也难以判断授



权视频的版权是否遭到破坏,因为视频发布者失去了对视频的控制,任何人都可以像合法用户一样从路由器中获取想要观看的内容并观看,数字水印起到的作用仅仅是确认授权视频的拥有者而已。当采用 DRM 方法使用加密技术时,用户将密钥公布以后,任何人都能获取并解密该授权视频,而且视频发布者无法判断是谁公布了该密钥。采用 DRM 和数字水印技术两者结合的方法,也会因为上面所述的缺点而不能很好地保护授权视频的版权。因此针对 ICN 中授权视频的版权保护,需要研究并设计新的访问控制方案。

2.2 ICN 中现有的授权视频访问控制方法

通过上面的分析,知道 P2P 网络和 CDN 中保护授权视频版权的访问控制方案不能直接用于 ICN 中。经过调研,目前关于 ICN 访问控制的研究还很少,尤其是在保护授权视频版权方面,更是少之又少,采用加密技术是 ICN 中保护内容版权的主要方法。

参考文献[19]使用 UCONABC(usage control authorizations, obligations, conditions, 控制核心模型)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。以 NDN(named data networking, 命名数据网络)的网络架构为例进行讨论,在此方案中,数据通过加密进行保护,它的访问过程由一个集中的访问控制列表来管理。但目前这种方案只能在 NDN 中实现;另外,用这种方案保护授权视频的版权时,若密钥被泄露,任何其他人都能够观看视频,而且无法查出是谁泄露了密钥;再者,这种方案是围绕着命名空间原则^[20]组织的,而 ICN 命名有 3 种方式,分别是基于属性的命名、扁平命名和垂直命名,故这种方案不适合 ICN 所有框架。

参考文献[21]使用加密的访问控制方法来保护内容。对内容用密钥 K 进行加密,加密后的内容可以被缓存在路由器中,任何人都能够从路由器中获取加密后的内容。然而只有已授权的用户才能得到对称加密的解密密钥 K ,或者非对称加密的解密密钥 K' ,这样已授权用户就可以通过解密得到可观看的视频。但该方案一个最大的缺点就是针对一个授权视频,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故意泄露该解密密钥,或者不经意间泄露了该密钥,那么所有用户都可以从网络中获取该密钥,然后观看视频。

为了利用 ICN 内网缓存这个能够给授权视频分发带来很大益处的特征,提出一种基于分割和数字水印的访问

控制方案来保护授权视频的版权,从而为授权视频提供一个安全高效的访问控制方案。

3 基于分割的方案

研究的场景如图 1 所示。在 ICN 中,授权视频发布者(authorized video producer, AVP)发布授权视频(V),其中用户 1 和用户 2 是已授权用户,用户 3 是未授权用户。在本文的方案中,视频发布者将 V 分割成两个部分,分别是 PCB 和 CKB,如图 2 所示。其中 PCB 一般比较大,可被缓存在路由器中用来提高视频分发效率,而 CKB 需要进行访问控制,相当于一个广义的密钥,将 PCB 和 CKB 结合在一起能够恢复出原始视频。任何用户必须同时获取 PCB 和 CKB 后才能观看视频,即使用户获取了 PCB,若没有获取 CKB,仍然不能够观看视频。采用不同的方法分别传输 PCB 和 CKB,PCB 可以公开传输,并可以被缓存在它被传输时所经过的所有路由器中,任何用户都可以在不经过 AVP 同意的情况下从路由器中获取 PCB。

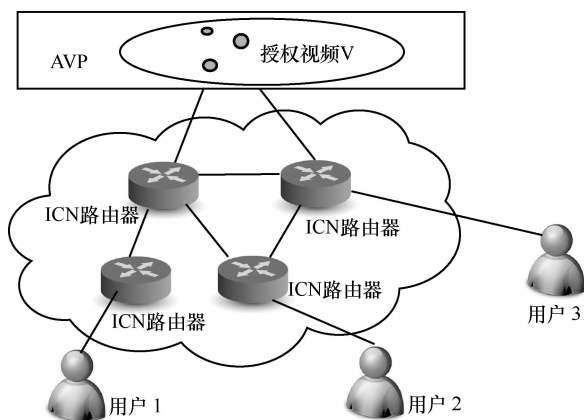


图 1 基于分割和数字水印方案的场景

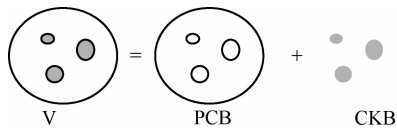


图 2 将授权视频 V 分割成两个部分

用户 1 请求 PCB 时,既可以从 AVP 获取,也可以从路由器中获取。然而,只有已授权用户才能从 AVP 获取 CKB,而且 CKB 的传输是秘密进行的。例如,当用户 1 请求 CKB 时,AVP 利用用户 1 的公钥对 CKB 进行加密,然后将加密后的 CKB 发送给用户 1。当用户 1 收到该内容后,利用自己的私钥对其进行解密便可得到 CKB。这样当用户 1 获得 PCB 和 CKB 后就可以观看授权视频。由于授

权视频大部分内容都被缓存在路由器中,该方案能够极大地提高互联网数据传输的性能,尤其在拥有海量数据的未来网络中,能够给授权视频传输带来很大的好处。

为了保护授权视频的版权,使不同的已授权用户拥有不同的CKB,每个用户的CKB都能够唯一标识该用户,针对第 i 个已授权用户,CKB用 C_i 表示。任何用户必须同时获得PCB和CKB后才能观看视频,而只有已授权用户才能够获取CKB,当某个已授权用户泄露CKB后会使得授权视频的版权遭到破坏,利用本文的方案,通过分析CKB,便可以知道是谁泄露了CKB。在参考文献[21]中,无法判断是谁故意泄露该解密密钥,或者不经意间泄露该密钥,这样仍然存在版权保护问题,基于分割的方案能够很好地解决参考文献[21]中存在的问题。将 V 分割一次后,如何使得到的CKB对应不同的用户?采用在CKB中加入不同数字水印的方法来解决这个问题,下面将讨论基于分割和数字水印的访问控制方案。

4 基于分割和数字水印的访问控制方案

在基于分割的方案中,需要产生不同的CKB来唯一标识已授权用户,这也是本文方案能够提供高效安全的访问控制的关键之处。在本文中,采用数字水印来解决这个问题,针对不同的用户,在CKB中加入唯一标识该用户的数字水印,加入的数字水印是用户不可见和不可篡改的。

如图3所示,将 V 分割后得到CKB,利用数字水印嵌入算法在CKB中加入第 i 个用户的数字水印,得到 C_i ,假设 i 的最大值为 N_1 ,即CKB能够对应 N_1 个用户。每个用户的数字水印各不相同,这样所产生的CKB也各不相同。

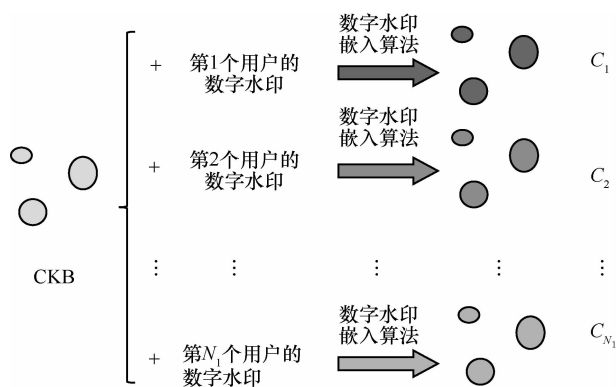


图3 利用数字水印产生不同的CKB

一个视频 V 被分割一次后,得到一个PCB和一个CKB,在该CKB中加入不同的数字水印后,能够对应不同

的授权用户,但在CKB中能够加入的不同数字水印的数量是有限的,即一次分割后得到的CKB对应的用户数量是有限的。一些授权视频对应的用户可能很多,超过了单次分割CKB所能够对应的用户数量,这时可重复采用基于分割和数字水印的方案,得到不同的CKB,从而对应更多的用户。例如,针对一个2GB的电影,假设拥有的已授权用户数量为 N_1+N_2 可以分割成2000MB的PCB和48MB的CKB,假设48MB的CKB能够对应 N_1 个用户,再次将电影分割成2010MB的PCB和38MB的CKB,假设38MB的CKB能够对应 N_2 个用户,这样就能够对应 N_1+N_2 个用户。当然,也可以分割成其他情况。

数字水印的几个重要特点是:安全性、隐蔽性和顽健性。数字水印应该是安全的,难以被篡改和伪造的;加入的数字水印应该不影响原数据内容的正常使用,是不可察觉的;数字水印是具有顽健性的,当经过有意或无意的信号处理后,仍然能够保持部分完整性,并能够被准确鉴别。本文方案中加入的数字水印也应该是安全的,并具有隐蔽性和顽健性。

在本文中,不讨论在CKB中加入数字水印的具体算法,可以采用目前存在的一些数字水印加入算法,对其进行优化改进,这也是未来工作的主要内容,例如可以借鉴参考文献[12]中基于小波变换的数字水印方法。不过所采用的数字水印算法要能使得加入不同数字水印后的CKB能够唯一标识每一位用户,并且具有安全性、隐蔽性和顽健性;所加入的数字水印是用户不可见的,不影响用户观看视频时的用户体验。每个已授权用户的数字水印都是难以篡改和伪造的,这样,一个已授权用户将自己的数字水印篡改成其他用户的数字水印是行不通的,这使得已授权用户无法伪造其他用户发布CKB。由于具有顽健性,任何已授权用户想要破坏自己的数字水印然后发布CKB是困难的,而且当CKB遭到严重破坏后,无法和PCB结合在一起恢复出视频 V 。当已授权用户发布自己的CKB后,通过分析CKB中的数字水印,就能够判断是谁泄露了CKB。加入数字水印后的基于分割和数字水印的访问控制方法如图4所示。在第5节,将从安全性和网络资源优化两个方面对本文的方案进行具体的分析。

AVP保存所有用户的数字水印,当第 i 个用户泄露自己的 C_i 后,AVP通过将 C_i 中的数字水印与AVP保存的所有数字水印相比较,便可以知道是哪个用户泄露了 C_i ,其简单的工作原理如图5所示。

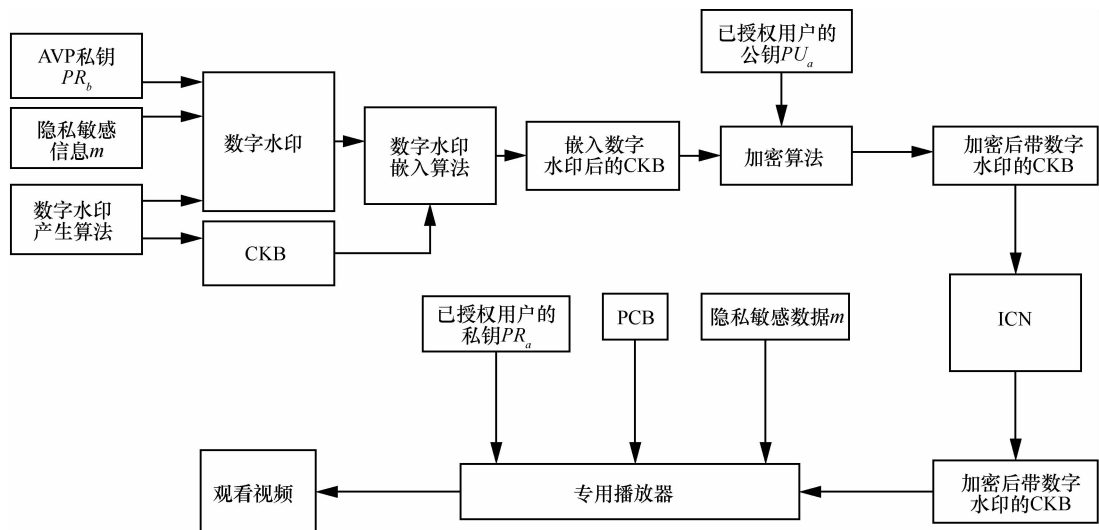


图4 基于分割和数字水印的访问控制方案

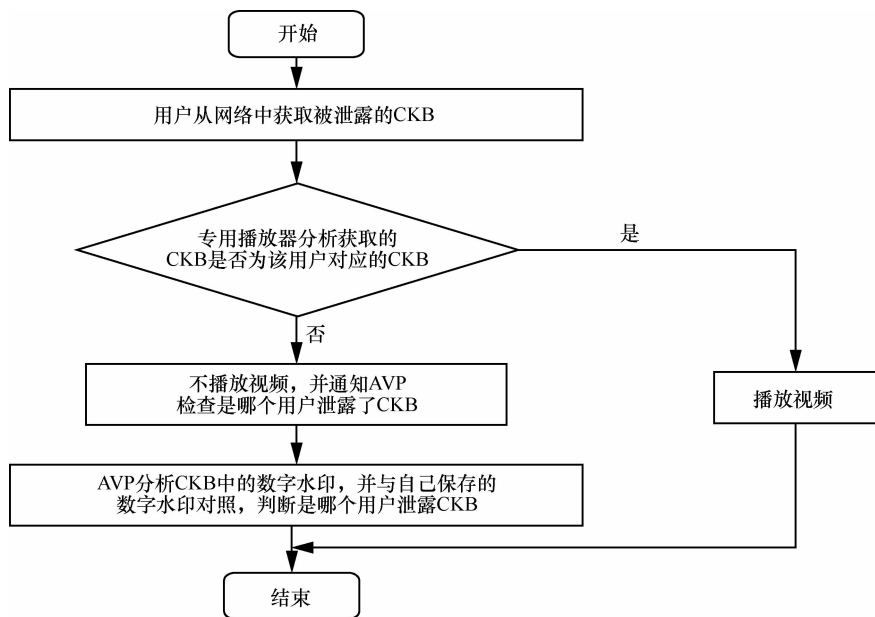


图5 数字水印简单的工作原理

5 方案分析

5.1 安全性

结合图4,首先,AVP生产一个授权视频 V ,将 V 分割成PCB和CKB,由于PCB可被缓存在路由器中,所采用的分割方法要使得用户必须同时获得PCB和CKB后才能观看视频 V 。AVP在CKB中加入数字水印,使得它们能够唯一标识每一个已授权用户。AVP利用自己的私钥 PR_b 和隐私敏感信息 m 通过数字水印产生算法产生数字水印,然后利用数字水印嵌入算法将水印嵌入CKB中。

当已授权用户请求CKB时,AVP用已授权用户的公钥 PU_a 加密嵌入水印后的CKB,得到ECKB,有:

$$ECKB = E(PU_a, CKB) \quad (1)$$

接着AVP通过ICN将ECKB发送给请求的已授权用户。使用专用播放器来播放视频,先用已授权用户的私钥 PR_a 对ECKB进行解密得到CKB,有:

$$CKB = D(PR_a, E(PU_a, CKB)) \quad (2)$$

因为已授权用户的私钥对用户来讲是十分重要的,一旦私钥泄露,该用户的隐私就受到侵犯,所以只有已授权用户才能得到解密后的CKB。专用播放器通过敏感信息分

析 CKB 中的数字水印是否被篡改, 然后结合 PCB 和 CKB 播放视频。利用 RSA 加密传输 CKB 使得基于分割和数字水印的访问控制方案更加安全可靠。

方案中加入的数字水印具有安全性、隐蔽性和顽健性。所加入的数字水印是用户不可见的, 不影响用户体验。每个已授权用户的数字水印都是难以篡改和伪造的, 这使得已授权用户无法伪造成其他用户发布 CKB。顽健性使得任何已授权用户想要破坏自己的数字水印然后发布 CKB 是困难的, 而且当 CKB 遭到严重破坏后, 将无法和 PCB 结合在一起恢复出视频 V。当已授权用户发布自己的 CKB 后, 视频发布者通过将被发布的 CKB 中的数字水印与视频发布者保存的所有用户的数字水印进行对比分析, 就能够判断是谁泄露了 CKB。

由此可知, 本文方案能够很好地解决参考文献[21]中存在的问题, 提供了一个安全的授权视频访问控制方案, 能够很好地保护授权视频的版权。

5.2 网络资源优化

信息中心网络利用内网缓存能够极大地提高视频的分发效率, 这对拥有海量视频数据流量的未来网络来说是极其重要的。在本文方案里, 从授权视频中分割出来的 PCB 可以被缓存在路由器中, 任何用户都能够从距离自己更近的路由器中获取该内容, 减少了网络带宽的使用和用户获取授权视频的时间。另外, 当传输失败时, 不必像传统网络中那样需要重新从源处获取, 而只要从传输失败附近缓存了该内容的路由器中获取, 使得内容重新获取变得更加高效, 对网络性能进行了极大的优化。下面在内容获取时间方面进行具体分析。

假设 T_r 是用户从邻接路由器中获取特定内容的时间, $T_m(d)$ 是用户从中间路由器中获取特定内容的时间, 参数 d 是中间路由器离用户的距离, T_s 是用户从 AVP 获取特定内容的时间。在本文中, 假设所有用户都离 AVP 比较远, 能够从路由器中更快地获取内容, 有 $T_s > T_m(d) > T_r$, 针对授权视频有 $T_s \gg T_r$ 。

设有 N 个已授权用户请求视频 V, 其中有 M ($0 \leq M \leq N$) 个用户可以从邻接路由器中获取 PCB, 其他用户可以从中间路由器中获取 PCB, 所有用户都从 AVP 中获取 CKB。视频 V 的大小为 S_V , PCB 的大小为 S_{PCB} , CKB 的大小为 S_{CKB} , 则有:

$$S_V = S_{PCB} + S_{CKB} \quad (3)$$

$$S_{PCB} \gg S_{CKB} \quad (4)$$

T 是所有已授权用户都获得视频 V 所花费的时间, 则

T 为:

$$T = \sum_{i=1}^N T_{si}(S_{CKB}) + MT_r(S_{PCB}) + \sum_{i=1}^{N-M} T_m(d, i)(S_{PCB}) \quad (5)$$

其中, $T_{si}(S_{CKB})$ 表示第 i 个用户从 AVP 处获得 CKB 所需要的时间, $T_r(S_{PCB})$ 表示用户从邻接路由器中获取 PCB 所需要的时间, $T_m(d, i)(S_{PCB})$ 表示第 i 个用户从中间路由器中获取 PCB 所需要的时间, 该时间还与参数 d 有关。

当所有已授权用户都从 AVP 那里获取视频 V 时, 所用时间为 T_0 , 则:

$$T_0 = \sum_{i=1}^N (T_{si}(S_V)) \quad (6)$$

其中, $T_{si}(S_V)$ 表示第 i 个用户从 AVP 获取视频 V 所需要的时间。

利用本文方案对授权视频 V 进行传输, 所节省的时间为 ΔT , 则:

$$\Delta T = T_0 - T = \sum_{i=1}^N (T_{si}(S_V)) - \sum_{i=1}^N (T_{si}(S_{CKB})) - MT_r(S_{PCB}) + \sum_{i=1}^{N-M} T_m(d, i)(S_{PCB}) \quad (7)$$

化简得:

$$\Delta T = \sum_{i=1}^N (T_{si}(S_{PCB})) - MT_r(S_{PCB}) - \sum_{i=1}^{N-M} T_m(d, i)(S_{PCB}) \quad (8)$$

利用内网缓存, 用户能够从路由器中而不是从 AVP 处获取内容, 则 $\Delta T \geq 0$, 针对授权视频, 有 $T \gg T_0$, 这样能够极大地减少内容获取的时间。例如, 将 2 GB 的电影分割成 2 000 MB 和 48 MB 时, 有 97.66% 的内容能够被快速有效地访问。另外, 互联网中一些授权视频对应的用户可能很多, 可以重复采用基于分割和数字水印的方案, 得到不同的 CKB, 从而能够对应更多的用户。

通过以上分析知, 和其他方案相比, 基于分割和数字水印的访问控制方案能够提供快速而且有效的视频内容分发, 对网络资源具有极大的优化功能, 而且还能够很好地解决 ICN 授权视频的版权保护问题, 是一个快速高效而又安全的授权视频访问控制方案。

6 结束语

保护授权视频版权是一个非常重要的挑战, 这关系到视频行业的发展, 在传统的 TCP/IP 架构中已经有许多这方面的工作, 但在 ICN 中这方面的研究还不多。信息中心网络中内网缓存这个重要特征能够给视频分发带来很大的好



处,用户能够从离自己更近的路由器中获取视频,极大地提高了视频传输效率。但内网缓存也带来了新的访问控制问题,当授权视频被缓存在路由器中后,视频发布者便失去了对它的控制,未授权用户可以从路由器中获取视频并观看。

针对这个问题,提出了一个基于分割和数字水印的访问控制方案,将一个授权视频分割成 PCB 和 CKB,PCB 可缓存在路由器中来提高传输效率,通过在 CKB 中加入数字水印来唯一标识每一个已授权用户,只有已授权用户才能从视频发布者那里获取 CKB,只有同时获得 CKB 和 PCB 后才能观看视频。通过分析,本文方案不仅能够提高授权视频的传输效率,而且能够很好地保护授权视频的版权,提供了一种有效的访问控制技术。

针对采用什么样的技术将一个授权视频分割成两个部分以及怎样在 CKB 中加入数字水印,将是未来工作中研究的重点。

参考文献

- 1 Cisco Visual Networking Index: Forecast and Methodology, 2012-2017. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html, 2014
- 2 Cisco Systems, Inc. Cisco Networks, Cisco's Visual Networking Index Global IP Traffic Forecast 2010-2015. http://www.cisco.com/en/US/netsol/ns827/networking_solutions_sub_solution.html, 2014
- 3 Rhea S, Godfrey B, Karp B, *et al.* OpenDHT: a public DHT service and its uses. *ACM SIGCOMM Computer Communication Review*, 2005, 35(4): 73~84
- 4 Liste M. Content Delivery Networks (CDNs)-A Reference Guide. Cisco World, White Papers, 2001
- 5 Davison B D. A web caching primer. *IEEE Internet Computing*, 2001, 5(4): 38~45
- 6 Eugster P T, Felber P A, Guerraoui R, *et al.* The many faces of publish/subscribe. *ACM Computing Surveys (CSUR)*, 2003, 35(2): 114~131
- 7 夏春梅, 徐明伟. 信息中心网络研究综述. *计算机科学与探索*, 2013, 7(6): 481~493
- 8 Ahlgren B, Dannewitz C, Imbrenda C, *et al.* A survey of information-centric networking. *IEEE Communications Magazine*, 2012, 50(7): 26~36
- 9 Wang S, Bi J, Wu J, *et al.* Could in-network caching benefit information-centric networking. *Proceedings of the 7th Asian Internet Engineering Conference*, ACM, Phuket, Thailand, 2011: 112~115
- 10 Psaras I, Chai W K, Pavlou G. Probabilistic in-network caching for information-centric networks. *Proceedings of the Second Edition of the ICN Workshop on Information-Centric Networking*, Helsinki, 2012: 55~60
- 11 Chung T Y, Hong M S, Oh Y N, *et al.* Digital watermarking for copyright protection of MPEG2 compressed video. *IEEE Transactions on Consumer Electronics*, 1998, 44(3): 895~901
- 12 Preda R O, Vizireanu D N. A robust digital watermarking scheme for video copyright protection in the wavelet domain. *Measurement*, 2010, 43(10): 1720~1726
- 13 Lin E T, Eskicioglu A M, Lagendijk R L, *et al.* Advances in digital video content protection. *Proceedings of the IEEE*, 2005, 93(1): 171~183
- 14 Chen C, Ran C. P2P copyright protection: current states and future prospective with particular on China. *Proceedings of International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM'07)*, Kyoto, Japan, 2007: 57~62
- 15 Djekic P, Loebbecke C. Software piracy prevention through digital rights management systems. *Proceedings of Seventh IEEE International Conference on E-Commerce Technology (CEC 2005)*, München, Germany, 2005: 504~507
- 16 Fetscherin M, Schmid M. Comparing the usage of digital rights management systems in the music, film, and print industry. *Proceedings of the 5th International Conference on Electronic Commerce*, Newport Beach, CA, USA, 2003: 316~325
- 17 Lou X, Hwang K, Zhou R. Integrated copyright protection in peer-to-peer networks. *Proceedings of 27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07)*, Toronto, Canada, 2007
- 18 Yang C, Liu J, Zhang Y, *et al.* The implementation architecture of content protection in P2P network. *Proceedings of International Conference on Computational Intelligence and Security Workshops (CISW 2007)*, Harbin, China, 2007: 455~458
- 19 Hamdane B, Msahli M, Serhrouchni A, *et al.* Data-based access control in named data networking. *Proceedings of 9th International Conference on Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom)*, Austin, Texas, USA, 2013: 531~536
- 20 Smetters D, Golle P, Thornton J. CCNx Access Control Specifications. Technical Report, PARC, 2010
- 21 Jacobson V, Smetters D K, Thornton J D, *et al.* Networking named content. *Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies*, Yangzhou, China, 2009: 1~12

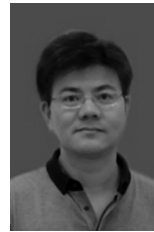
(下转第 86 页)



- 2 Ni Y, Xie L, Liu Q Z. Minimizing the expected complete influence time of asocial network. *Information Sciences* 2010,180(1): 2514~2527
- 3 Klein A, Bhagat P. E-commerce: evidence on a new virtual commerce platform. *Journal of Business Research*, 2010, 4(1): 107~124
- 4 Liang T P, Ho Y T, Li Y W, *et al.* What drives social commerce: the role of social support and relationship quality. *International Journal of Electronic Commerce*, 2011,16(1):69~90
- 5 赵华, 林政, 方艾等. 一种基于知识树的推荐算法及其在移动电子商务上的应用. *电信科学*, 2011,27(6)
- 6 陶彩霞, 谢晓军, 陈康等. 基于云计算的移动互联网大数据用户行为分析引擎设计. *电信科学*, 2013,29(3):30~35
- 7 Li Y, Lu L, Feng L X. A hybrid collaborative filtering method for multiple-interests and multiple-content recommendation in E-commerce. *Expert Systems with Applications*,2005,28(1):67~77
- 8 Jeong B, Lee J, Cho H. Improving memory-based collaborative filtering via similarity updating and prediction modulation. *Information Sciences*, 2010, 180(1): 602~612
- 9 琚春华, 鲍福光. 基于情境和主体特征融入性的多维度个性化推荐模型研究. *通信学报*, 2012, 33(9A):17~27
- 10 Pan W K, Yang Q. Transfer learning in heterogeneous collaborative filtering domains. *Artificial Intelligence*, 2013,197(1): 39~55
- 11 张海燕, 孟祥武. 基于社会标签的推荐系统研究. *情报理论与实践*, 2012, 35(5):103~106
- 12 孟祥武, 胡勋, 王立才等. 移动推荐系统及其应用. *软件学报*, 2013,24(1):91~108

- 13 Ranganathan C, Ganapathy S. Key dimensions of business-to-consumer web sites. *Information & Management*, 2002, 39(6):457~465
- 14 张佩云, 陈恩红, 黄波. 基于社会网络面向个性化需求的可信服务推荐. *通信学报*, 2013(12):49~59
- 15 Hsia T L, Wu J H, Li Y E. The E-commerce value matrix and use case model: a goal-driven methodology for eliciting B2C application requirements. *Information & Management*, 2008, 45(5): 321~330
- 16 DeMeo P, Nocera A, Terracina G, *et al.* Recommendation of similar users, resources and social networks in a social internetworking scenario. *Information Sciences*, 2010,181(1):1285~1305

[作者简介]



琚春华,男,博士,浙江工商大学教授、博士生导师、校长助理,计算机与信息工程学院院长,主要研究方向为智能信息处理、数据挖掘、电子商务与物流优化等。

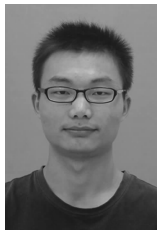
鲍福光,男,浙江工商大学博士生,主要研究方向为智能信息处理、数据挖掘和供应链协同合作。

许舛寰,男,浙江工商大学工商管理学院讲师、博士生,主要研究方向为数据挖掘、智能信息处理等。

(收稿日期:2014-06-12)

(上接第 60 页)

[作者简介]



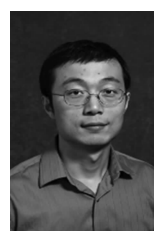
周自飞,男,中国科学技术大学信息科学技术学院硕士生,主要研究方向为安全与隐私保护和信息中心网络。



牛玉坤,男,中国科学技术大学信息科学技术学院硕士生,主要研究方向为安全与隐私保护、智能电网和软件定义网络。



谭小彬,男,博士,中国科学技术大学信息科学技术学院副教授、硕士生导师,主要研究方向为信息安全、无线多跳网络和未来网络架构。



邹长春,男,博士,美国中佛罗里达大学电气工程与计算机科学系副教授、博士生导师,主要研究方向为计算和网络安全、计算机网络和网络建模与性能分析。

(收稿日期:2014-07-25)