安全的网络编码所面临的挑战和对策

刘外喜[1,2] 余顺争[1] 蔡 君[1]

(中山大学电子通信工程系 广州 510275)[1] (广州大学电子信息工程系 广州 510006)[2]

摘 要 近年来,网络编码以其巧妙的思想展现出生机勃勃的应用前景,但是安全问题一直是其在网络中大规模应用的最大障碍。在现有研究成果上,从网络编码的基本原理出发,按照物理层和网络层两个层面对系统的各个部分进行了更加全方位的安全隐患分析;也给出了针对ACK类和编码类攻击的基于典型集和哈希函数以及马尔可夫模型的防御方法;同时提出了结合利用云计算和网络编码构建计算网络的概念;最后对网络编码的未来研究方向进行了展望。

关键词 网络编码,网络安全,典型集,哈希函数,云计算

中图法分类号 TP393 **文献标识码** A

Secure Network Coding: Challenges and Solution

LIU Wai-xi[1,2] YU Shun-zheng[1] CAI Jun[1]

(Department of Electronic and Communication Engineering, Sun Yat-Sen University, Guangzhou 510275, China)[1]

(Department of Electronic and Information Engineering, Guangzhou University, Guangzhou 510006, China)[2]

Abstract In recent years, network coding has emerged some exciting future because of its smart technology. However, in order to let network coding become popular in the Internet, its security problem must be solved. Firstly, a wide range of attacks were revealed based on our systematic analysis of the components of these frameworks vulnerabilities. Secondly, this paper gave one proposal for ACK attacks and coding attacks based on Typical Set, Hash Functions and Markov model. Thirdly, one thinking named as Computing Network, which integrates Cloud Computing with Network Coding, was proposed. Finally, the open issues and challenges for network coding referring to both theory and application in near future were proposed.

Keywords Network coding, Network security, Typical set, Hash function, Cloud computing

1 前言

2000年,蔡宁和李硕彦等人正式提出网络编码[1,2](Network Coding)的概念,从此网络编码技术就日益受到人们的关注。网络编码的中心思想是:要求中间节点在转发数据包之前对报文进行混合计算,即利用节点的计算能力换取网络的信息传输能力。网络编码的引入最初是为了解决最大流最小割问题,但随着研究的进一步深入,发现网络编码在提高网络吞吐量、改善负载均衡、减小传输延迟、节省节点能耗、增强网络鲁棒性等方面均显示出其优越性,其可广泛应用于Ad Hoc网络、传感器网络、P2P内容分发和网络安全等领域。同时,Shengli Zhang[3]将蔡宁和李硕彦等人的网络编码思想扩展到物理信号层面,也获得了不错的效果。毋庸置疑,网络编码展现了巧妙的思想和生机勃勃的应用前景。

在基于网络编码的网络中,由于网络编码原理本身的特殊性导致对信息的扩散性较强,因此与普通的网络相比,这种情况下的攻击者只要注入很小的恶意信息或对相关信息稍作修改就可能影响一定范围的甚至是整个的网络。也就是说,同样的攻击手段,在该模式网络中的攻击效率更高,传染性更强。

要使网络编码在网络中得到大规模应用,就必须解决其安全问题。著名的短板理论表明整个系统的安全是由其最薄弱部分来决定的,本文从网络编码的基本原理出发按照物理层和网络层两个层面对系统的各个部分进行全方位的安全分析;第2节讨论物理层网络编码,第3节讨论网络层网络编码;第4节提出安全应对措施;最后给出结论和展望。

2 物理层网络编码

物理层的广播特性是无线通信区别于有线通信的特点之一,这一特性帮助人们获得一些通信方式的变化以及通信性能的改善,但正是这一特性的存在也导致了无线网络中出现了诸如隐蔽站和暴露站等特有的冲突问题。在过去的研究中为了避免冲突对接收者的解调和解码造成的干扰,人们尽力地采取各种办法避免冲突的发生。但一个事情总是有其两面

到稿日期:2010-05-31 返修日期:2010-11-12 本文受国家自然科学基金-广东联合基金重点项目(U0735002),国家"863"高技术研究发展计划基金项目(2007AA01Z449),国家自然科学基金(60970146)资助。

刘外喜(1976-),男,博士生,讲师,主要研究方向为网络安全、网络编码,E-mail:liuwaixi@sina.com;**余顺争**(1958-),男,教授,博士生导师,主要研究方向为网络安全、网络行为分析。

性，冲突并不总是有坏处的，物理层网络编码(Physical-Layer Network Coding)[3]的出现使得可以把冲突充分地利用起来，以帮助提高通信的性能。所谓物理层网络编码就是借用网络编码的思想在中间节点对信息在物理层面的电磁波信号进行诸如实数加的编码运算。文献[5]中指出，中继节点可以根据信噪比 SNR 选择两种策略：放大-转发(AF)、解码-转发(DF)。目前，物理层网络编码主要有文献[3,4]所提的两种思想，文献[3]采用 DF，而文献[4]采用 AF。

在文献[3]中，如图 1 所示，以经典的二路中继模型为例，节点 1 和节点 3 需要交换信息，但由于功率覆盖范围的限制，必须通过节点 2 转发。S_1，S_2，S_3 分别表示节点 1、节点 2、节点 3 发送的信息；$s_1(t)$，$r_2(t)$，$s_3(t)$分别表示节点 1、节点 2、节点 3 发送的物理层电磁波信号，对于 QPSK，它们的关系如下：

$$\begin{aligned} r_2(t)&=s_1(t)+s_3(t)\\ &=[a_1\cos(\omega t)+b_1\sin(\omega t)]+[a_3\cos(\omega t)+\\ &\quad b_3\sin(\omega t)]\\ &=(a_1+a_3)\cos(\omega t)+(b_1+b_3)\sin(\omega t) \end{aligned} \tag{1}$$

然后节点 2 把 $r_2(t)$广播到 1,3 号节点，由于节点 1 有参数 a_1 和 b_1，因此可以从收到的合成信号 $r_2(t)$中解析出 a_3 和 b_3，进而通过解调可以获得节点 3 想要传送到节点 1 的信息。节点 3 可以做类似的处理来获得想要的信息。所以通过以上分析可知，物理层网络编码(PNC)和网络层网络编码(NC)实现的方法不一样，但它们完成同样的功能(即 $S_2=S_1\oplus S_3$)，它们之间存在一个映射关系。但是在性能上，只要 2 步的物理层网络编码相对于需要 4 步的传统机制(见图 2)和需要 3 步的网络层网络编码(见图 3)，其吞吐量分别有 100%，50%的提高。

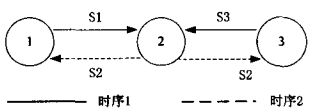

图 1 物理网络编码模型[3]

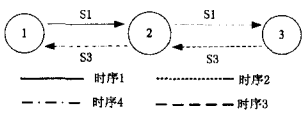

图 2 传统机制模型[3]

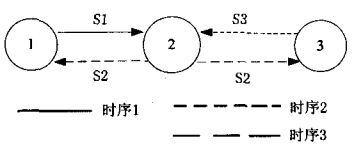

图 3 网络层网络编码模型[3]

在文献[4]中，S. Katti 等人进一步拓展了物理层网络编码思想。它最大的贡献在于消除了文献[3]中的多个约束条件：信号之间同步、有相同的相位平移、有相同的损耗，这使之更加具有实践意义。而文献[4]指出，对于超过 2 跳的无线网络来讲，放大-转发策略不是一个好的选择。

物理层网络编码不仅可以提高吞吐量、减少延迟，同时由于物理链路上传输的是合成信号，因此在某种意义上也提高了物理层面的机密性。文献[6]针对解码-转发策略做了相关实验。利用敌手的 SER(误码率)来衡量偷听的效果。如果敌手的 SER 比正常接收者的 SER 低，说明敌手偷听成功。所以可以通过比较偷听成功的区域范围来衡量技术的效果，范围越小越好。文献[4]的结论是：在内部偷听和外部偷听两种情况下，PNC 可以较大地减少该范围，尤其是在内部偷听的情况下，PNC 可以在整个有效区域范围内让偷听者不成功。

2.1 物理层网络编码中的安全问题

虽然 PNC 展现了一些独特的优势，但要付诸实践还有很多方面需要完善，其中安全问题就是一个重要方面。由于其是工作在物理层，因此无线网络中普遍存在的诸如拥塞攻击、物理破坏等物理层的攻击都会存在。同时，其特殊的工作原理也带来了一些潜在的、特殊的安全隐患。

本文发现针对文献[3]所提方法的攻击隐患主要以下几种[42]：

条件破坏：信号之间同步、有相同的相位平移、有相同的损耗是文献[3]所提方法工作的必要条件，在无线网络的环境中，破坏这三者都是很容易的事情，例如攻击者可能会采用加噪，以及移动、删除同步码的位置等方法来破坏同步；也可以通过改变空间的环境条件来改变信号传播的损耗。

幅度攻击：由文献[3]的原理可知，若采取 QPSK 调制方式，接收点就需要通过判别相位大小来判别信息比特，而由式(1)可知，相位的大小又与幅度 a_1，b_1，a_3，b_3 有关，所以攻击者可以通过放大或缩小信号的幅度来达到攻击的目的，我们把这一类攻击定义为幅度攻击。

文献[4]中消除了文献[3]的约束条件，随之也消除了一些安全隐患，但也存在其自身的一些特定隐患。

在介绍隐患之前，首先简单看一下它的基本原理。该论文中采用 MSK 的调制方式，通过判断相位的变化来判别信息比特，例如，相位增加就判为“1”，减少就判为“0”。如图 1 所示，中继节点 2 接收到的两个信号的合成信号 $y[n]$可表示为式(2)，并被广播到节点 1 和节点 3。

$$y[n]=Ae^{j\theta[n]}+Be^{j\phi[n]} \tag{2}$$

式中，A，B 为两个信号的振幅，$\theta[n]$，$\phi[n]$为两个信号的相位。节点 1 的目的是解析出 $\theta[n]$，$\phi[n]$的变化，从而获取对方的信息比特，节点 3 也类似。

$$\begin{aligned} \theta[n]&=\arg(y[n](A+BD\pm iB\sqrt{1-D^2}))\\ \phi[n]&=\arg(y[n](B+AD\pm iA\sqrt{1-D^2})) \end{aligned} \tag{3}$$

若要从式(2)的合成信号中求出 $\theta[n]$，$\phi[n]$，就必须通过式(3)，其中 $D=\dfrac{|y[n]|^2-A^2-B^2}{2AB}$，所以就必须知道 A，B 值，而 A，B 值可从式(4)、式(5)获得。

$$E[|y[n]|^2]=u=A^2+B^2 \tag{4}$$

$$\delta=\frac{2}{N}\sum_{|y[n]|^2\geq u}|y[n]|^2=A^2+B^2+\frac{4AB}{\pi} \tag{5}$$

式中，E 为期望值。

所以，A，B 值都与合成信号的$|y[n]|^2$(就是能量)有关。

另外，节点 1 和节点 3 如何判断是否收到一个报文，以及如何判断该报文是单个信号还是合成信号呢？在文献[4]中，由于采用的是 MSK，噪声、单个信号、合成信号的能量是不一样的，因此能量大小成为了判断的标准。

能量攻击：从以上原理可知，文献[4]中方法的几个关键处都需要用信号的能量来决定，所以如果敌手通过增加或减少信号的幅度进而改变能量来扰乱系统的判断(这很容易做到)，从而达到攻击的目的，则把这一类攻击定义为能量攻击[42]。

3 网络层网络编码

无线网络在物理层的广播特性和业务流的双向性使得网

络编码可以大幅度提高无线网络的性能。但是，由于无线网络中通信媒体的一些内在固有的特殊性质，诸如高误码率、信号强度的不可预测性、信号的混合叠加以及复杂环境变化的不可预测性等都将使得网络编码在无线网络中的应用充满挑战，同时，其以上的特殊性质也会带来特有的安全问题，即使以前已经普遍存在的攻击在基于网络编码的无线网络中也会产生更大的全局性危害。

在网络编码研究中，根据编码的对象可以分为内部会话(Intra-session)网络编码(见图 4)和交互会话(Inter-session)网络编码[7,9]。内部会话网络编码就是只针对同一个会话的报文进行编码；而交互会话网络编码则可以针对多个会话的报文进行编码。

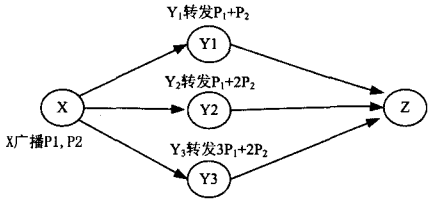

图 4　Intra-session 网络编码的示意图

3.1　Intra-session 网络编码的安全分析

Intra-session 网络编码的基本思想可由图 4 所示的例子来解释。X 点需要把报文 $p1$，$p2$ 广播到 Z 点。首先，X 点根据编码向量(Coding Vector)产生编码后报文(Coded Data)，然后将其不停地广播；中间节点 $Y1$，$Y2$，$Y3$ 根据其收到的报文再一次进行编码，然后将其转发出去；Z 点如果能够获得足够多的独立的编码后数据(Coded Data)，则通过解线性方程组就可以获得原始数据报文 $p1$，$p2$；然后 Z 点向 X 点发送一个确认 ACK；X 点收到 ACK 后就可以按照上面的步骤发送新的内容。这种思想与数字喷泉(Digital Fountain)[8]有某种相似之处。

从以上的例子可以看到，一个 Intra-session 网络编码系统由以下几部分组成[9]：转发节点的选择和转发速率的确定、数据包转发、发送 ACK 确认报文、解码与编码。下面系统地分析各部分存在的安全隐患[9]。

3.1.1　转发节点的选择和转发速率的确定

在该阶段，需要根据整个网络的中间节点与源节点和目的节点的位置关系、节点间的冲突关系、各会话流之间的平衡等因素来将那些可以对提高系统性能做出大贡献的节点选作转发节点，并确定合适的转发速率。

包括中间节点与源节点、目的节点的位置关系以及节点间的冲突关系等因素的链路状态信息是制定正确策略的关键，错误的状态信息导致错误的策略。每个节点都监测着自己所属链路的状态变化，并像路由协议一样，定期地将其向其他节点通告，所以在这一过程中，有可能存在以下攻击[9]：

链路状态伪造和修改：一方面，攻击者可以向其邻居发布虚假的状态信息；另一方面，攻击者也可以修改其所接受到的信息。针对前者，文献[12]通过采用监测式的防御手段来鉴别进而隔离攻击者；至于后者可以通过数字签名技术实现认证。

虫洞(wormhole)攻击：在两个节点间引入一条虚假的带有虚假链路信息的链路，从而改变了整体网络拓扑图的结构。文献[13]提出的 Packt leashs 和文献[14]提出的 TrueLink 方法都需要消耗大量的资源。

虚假路由信息(false routing information)：因为工作原理类似于路由协议，所以攻击者通过发送一些虚假的链路信息来影响系统的工作，比如改变路径拓扑、消耗节点资源、形成循环路由等。

3.1.2　数据包转发

在该阶段，中间节点根据其收到的报文再一次进行编码，然后将编码后的报文按照既定的速率转发出去，主要存在以下两种攻击手段[9]。

1. 污染攻击(Pollution Attack)：所谓污染攻击就是向网络中注入恶意的报文，由于网络编码是要对信息进行混合，并有可能转发后进一步被混合，这种混合信息成为众多中间节点转发或接收者获取信息的必要条件，因此攻击者只需注入少量的恶意报文就可到达污染全局的目的，在网络编码的环境下，该攻击具有更大的传染性。污染攻击是当前被研究最多的，所提方案主要分为以下几种[9]。

基于密码学的方法：该方法的主要思想是：在编码过的数据包中增加额外的认证信息，这样可以让中间节点识别并过滤掉被污染的报文。目前主要有同型哈希函数和同型数字签名，在基于同型哈希函数的机制中，源节点为每一个原始的数据包计算哈希值，并通过可靠信道传输到各中间节点，由于其同型的性质，所以中间节点可以独立地计算出哈希值，达到验证的目的[16]。文献[17]克服了文献[16]中方法计算量大的缺点，主要是利用网络编码的零空间来实现认证。而文献[18]等提出的基于数字签名的方法要求为每一个新文件分发新的公共密钥，并且密钥的大小与文件大小成线性关系，这一要求限制了其在大容量文件分发系统中的使用。文献[19]采取了不同于哈希和数字签名的方法，它主要利用对称密码的方法，但存在带宽消耗大的缺点。

基于信息论的方法：该方法的思想是容忍污染的存在，而不是将它过滤掉。可以通过在报文中增加足够多的冗余信息来方便接收者发现污染的存在[20]，或者通过分布式的协议让接收者在容忍污染报文存在的基础上解析出原始信息[21]。其中，后者在 3 种污染程度情况下分别获得(C-Zo)、(C-Zo)、(C-2Zo)的吞吐量上界，其中 C 是从源点到宿点的网络容量，Zo 是敌手注入恶意报文的容量。这里存在一个潜在问题：如果 Zo 变得无限大，那么系统的吞吐量会变得无限小。文献[22]可以减少 Zo，但前提是只允许节点至多广播一次，而这在实际的无线网络中并不现实，因为在实际系统中，每个节点通常会转发多次。

基于网络纠错码的方法：从原理上讲，网络编码系统中的网络纠错码和面向传统通信网络的经典编码理论是类似的[23]，也存在纠错能力和编码的带宽消耗的互换问题，因此，这样的机制不适合无线网络，因为在无线网络中，敌手很容易通过注入大量的恶意报文来提高误码率从而消耗带宽，进而降低纠错能力。

以上解决方案都是以牺牲系统性能作为代价的，也就是说为了防御污染攻击而运行的协议都会大幅度降低使用网络编码所带来的性能改善。最近，文献[15]提出 DART 和 EDART，它们是一种基于线性校验计算和时间认证的轻量级的解决方案。即使如此，设计一个不依赖于时间同步的轻量级的防污染攻击的方法依然是一个挑战。

2. 包丢弃(Packet Dropping):这种攻击手段具有很强的隐蔽性,因为恶意节点在大多数时间里表现得像正常节点一样,但它们会选择性地丢弃一些敏感且重要的包,从而破坏路由协议。文献[9]显示,即使是单个的包丢弃攻击都会使大多数的会话性能下降40%,而传统的Watchdog方法[24]在此不适用。

3.1.3 发送ACK确认报文

目的节点收到需要的信息后,向源节点发送ACK确认报文。及时并可靠地发送和接受ACK是整个系统正常运行起来的关键,在该阶段,遭受的攻击如下[9]:

ACK注入和修改:敌手通过注入虚假的ACK或修改ACK报文使伪广播技术源点误认为宿点已收到,从而过早地发送下一个报文,这样的攻击导致宿点只能得到部分报文,因而无法通过网络解码运算获得想要的信息。防止此类攻击的主要方法是报文认证,如数字签名。

丢弃ACK:敌手可以利用如前所述的虫洞攻击或虚假路由获得ACK传输的路径,进而使得源点无法发送下一个报文。

拖延ACK:比丢弃ACK更加隐蔽的是,敌手采取在中途拖延ACK的传输,使得源点降低发送速率,进而降低系统的吞吐量。

3.2 Inter-session网络编码的安全分析

交互会话(Inter-session)网络编码的本质是结合利用基于机会的偷听和在中间节点基于机会的编码,其主要思想是:如果一个节点需要向不同的下一跳节点发送不同的流信息,它不是逐个的单播,而是把这些不同流的信息经过编码后统一广播到所有的下一跳节点。

通常Inter-session网络编码可以由以下部分组成:编码机会的发现、报文编码和解码、报文转发、综合路由等。下面系统地分析各部分中存在的安全隐患[9]。

3.2.1 编码机会的发现

如图5所示,根据编码机会被利用的范围,Inter-session网络编码可以被分为区域编码系统和全局编码系统。

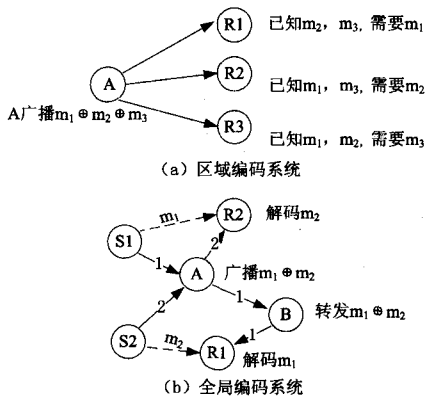

图5 Inter-session网络编码的示意图[9]

如图5(a)所示,在区域编码系统中,只会考虑相邻节点的编码机会,$R1$,$R2$,$R3$都会定期地向A节点汇报自己已有的信息和想要的信息,这样,A节点只要广播$m_1 \oplus m_2 \oplus m_3$一次,就可以全部满足$R1$,$R2$,$R3$的需求。文献[25]中的COPE协议就是一个典型。如图5(b)所示,在全局编码系统中,网络中所有节点潜在的编码机会都会考虑,文献[26]中的DCAR协议就是一个典型。

由以上原理可知,在该阶段,正确地收集包接收信息是发现编码机会的关键,然而在这一收集过程中,有可能遭受如下的攻击[9]:

包接收信息误报告:在区域编码系统中,攻击者可以伪装成真实节点发布一些虚假的包接收信息,这样将导致它的邻居根据这一错误的信息进行错误的编码,而这种错误的编码报文几乎不可能会被任何接收者解码和确认,从而导致发送者总是不断地发送无用的报文。报文认证机制可以防御这样的攻击,但由于包接收信息的数量巨大,因此需要极其轻量级的认证机制,否则系统将不堪重负。

链路状态污染:在区域编码系统中也会根据节点间的链路状态来推测报文接收的情况,所以那些针对链路状态路由协议的攻击也会再次发挥威力,进而掉入到如上段所述的陷阱。

邻居集的污染:根据上文的全局编码系统中的工作原理可知,一个节点编码机会的大小是由它在路由发现过程中所获得邻居集的情况而定的,所以攻击者可以通过恶意修改路由请求报文或通过虫洞攻击误导链路信息致使节点获得错误的邻居集,进而导致节点做出错误的判断进行错误的编码,由于存在许多无法确认的报文,对因此会降低系统的吞吐量。文献[27]所提的Ariadne可以阻止恶意的修改报文,如前所述的预防虫洞攻击的方法也会有所帮助。

3.2.2 编码报文的转发

在该阶段的编码和解码中,中间节点根据自身偷听的信息情况进行完全和部分解码。如图6所示,$Y1$和$Y2$点虽然只进行了部分解码,并产生了一个新的编码报文,但该报文成为了Z点的完全解码的基础。

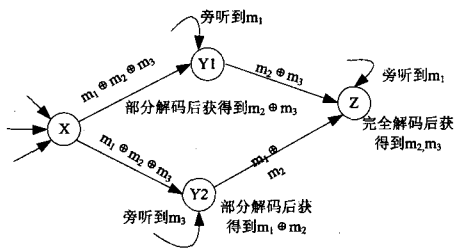

图6 中间节点的部分和完全解码

在该阶段,主要存在以下几种攻击[9]:

ACK注入和修改:通过注入虚假的ACK或修改ACK报文会导致在伪广播技术中过早地结束重发,使宿点只能得到部分报文,从而无法通过网络解码运算获得想要的信息。报文认证是一个可能的办法,由于ACK报文的数量巨大,因此该方法在计算量和带宽方面需要很高效才有实用价值。

污染攻击(Packet Pollution):基本原理与Intra-session的情形类似,由于Inter-session是对多个流的信息进行混合编码,因此这种攻击在该模式下的传染性会更强,而一些在Intra-session模式下的防御手段也会失效。所以针对该模式下的污染攻击的防御研究依然是一个挑战。

过编码(Packet Over-coding):在Inter-session模式下,中间节点针对哪些对象进行编码,是由在编码机会发现阶段所确定的,但如果攻击者针对比既定对象更多的对象进行编码,将会导致接收者无法解码。预防此类攻击的难处在于无法确定哪些报文是正常编码的,哪些是编过码的。由以上原理可知,这是Inter-session模式下的特有攻击之一。

欠解码(Packet Under-decoding):这是Inter-session模式下存在的另外一个特有攻击。由前文的原理知,一个中间节

点的解码结果是其他节点解码的基础，如果攻击者故意只完成既定任务的一部分，那么其他节点将无法工作。

包丢弃(Packet Dropping)：Inter-session 模式下的路由协议相对于传统的路由协议来讲，它是通过鼓励共享路径信息来增加编码的机会，所以在路由的选择过程中，攻击者可以想办法成为路由的一部分，然后在需要对多个流进行混合编码的时候丢弃一部分流的信息，传统的 Watchdog 方法[24]对此很难发现。

3.2.3 综合路由[9]

理论上，Inter-session 网络编码中的编码协议可以与路由协议相互独立地设计。但如果将两者结合在一起，设计出编码感知的路由协议(Coding-aware Routing Protocols)，综合考虑编码机会的多少和链路状态进行选路，可使编码效率最大化进而使系统的性能得到提高。文献[26]的 DCAR 对此进行了初步的实现。

Inter-session 模式下的路由选择综合考虑了链路状态信息和编码效益，所以，攻击者故意释放出自己的编码效益高的信息，从而诱使信息流向攻击者所控制的路由。预防此类攻击的困难在于预防者不仅需要准确地掌握包含链路状态信息的拓扑结构，还需准确地掌握包含编码机会信息的流结构。

3.3 网络编码中的熵攻击

不管是哪种模式下的网络编码，其中心思想均是：中间节点尽可能地捕获更多的编码机会来产生尽量多的有差异的信息报文，而在接收点则尽量快地收集这些有差异的信息报文，从而通过计算尽快地解码出信息来。从信息论的角度看，不确定或有差异就意味着信息可用熵来评估。所以，如果攻击者在中间节点想办法减少甚至消除报文之间的差异，也就是说把一些旧的信息按照合法的编码规则重新编码而产生虚假的新报文，那么接收者从这些虚假的新报文中无法发掘出真正的新信息，这样就可以增加接收点的解码时间，进而降低系统的有效吞吐量的攻击，这种攻击就是在文献[29]中提到的网络编码环境下的熵攻击(Entropy Attacks)。

文献[29]中作者提出的方法的主要思想是：各节点不仅在内容分发上进行合作，而且针对异常信息也是采取互通有无的合作体制。针对文献[29]中存在的效率问题，文献[30]所提方法的主要思想是：因为熵攻击的基本原理就是对旧报文进行编码，那么接收点就可根据接受报文中各报文之间的线性相关度来确定是攻击还是正常报文，同时利用似然概率的确认替代精确的确认来降低算法的计算量，也就是说牺牲一点可以承受的误报率来换取效率的大幅度改善。

3.4 网络编码中的搭线偷听

搭线偷听在各种网络中都是一个严重的危害，不管是有线还是无线，不管是在互联网还是电信网络中。在网络编码出现以前，主要利用密码学领域中的诸如数据加密、哈希函数和消息认证等方式来确保数据的安全传输。但是面对当今用户低延迟、高速率的服务要求，传统的密码学方法存在诸如计算复杂度较大、消息冗余较大等缺点而无法令人满意。因此，人们将网络编码技术引入到了这一领域。为了防止搭线偷听，蔡宁和杨伟豪首先在文献[33]中提出搭线偷听网络(CSWN)模型，并得到如下结论：定义了一类线性 CSWN 码，给出了该线性 CSWN 码是可容许码的充分条件，并给出在满足充分条件的情况下如何构造可容许码，但是该充分条件的验证比较困难，同时是针对不带圈的图的模型；文献[34]在此基础上进一步放松了约束条件，并且扩展到带圈的图的模型上。而文献[35]等文献所提方法的主要思想是：如果用 k 表示敌手可以获得的信息数量，那么就必须在源节点发送的信息中加入 r 个无用的干扰信息，并且 $r\geqslant k$，用信息向量 $m=(m_1,m_2,m_3,\cdots,m_{n-r},z_1,z_2\cdots,z_r)^T$ 表示源节点需要发送的 n 个信息，向量中包含了 r 个干扰信息。也就是说通过牺牲信息的有效传输效率来换取对偷听的防范，它的传输效率降低到 $\frac{n-r}{n}$。同时，一个潜在的危险就是对于任何给定的防御方案(r 就固定了)，敌手只要获取足够多的 k，使 $k\geqslant r$，就可以偷听成功。而在文献[36]中，Majid Adeli 等人做的改进如下：用信息向量 $m=(x_1+f(a),x_2+f(a,x_1),x_3+f(a,x_1,x_2),\cdots,x_{n-1}+f(a,x_1,x_2,\cdots,x_{n-2}),a)^T$ 表示源节点需要发送的 n 个字符，里面每一个信息都是用哈希函数计算后的值，这里 $f(.)$ 是哈希函数，a 是随机字符。由于哈希函数是单向不可逆的，对于敌手来说只有获取全部 n 个字符才能解析出其中的信息，而接收者使用 a 就可以逐步地从 x_1 解析到 x_{n-1}。这里只是用了一个字符 a 就达到了屏蔽所有信息的目的，效率提高了很多。文献[37]则试图将该问题归纳为 Ozarow-Wyner 偷听信道 2 类(Ozarow-Wyne Wiretap Channel of type II)，因此可以使用 Ozarow-Wyner 的编码方法来解决。

3.5 网络编码中的拜占庭攻击

所谓拜占庭攻击，就是比搭线偷听攻击更进一步，攻击者不仅想得到一些有用的消息，还通过多种手段来阻止双方的正常通信，即修改正常传输中的信息或注入一些恶意信息。这种攻击并不是网络编码中独有的现象，但由于在网络编码的环境中，中间节点对接受到的信息进行混合，因此此时拜占庭攻击的危害比普通网络中的更大。Ho 等人[31]在每个报文中嵌入高效的 Hash 函数值，使接收点可以高概率地识别到攻击。Jaggi[21]等人进一步给出了一种多项式复杂度的分布式算法，它可纠正敌手错误，并达到最优组播速率，而这两者都只能在接收点识别攻击，不能在中间节点丢弃恶意报文，无法改善系统的吞吐量，因而不适合那些资源受限的系统。文献[32]利用椭圆曲线算法给出了一种适用于网络编码的签名方案，除了可检测被修改的分组，还加入了对数据的身份认证功能。文献[41]利用网络编码的线性性质检测出攻击，将攻击局限在一跳之内，并可以纠正错误，从而避免报文重传来实现大幅度地节省带宽。

4 针对 ACK 类和编码类攻击的防御研究

如前所述，网络编码在无线网络中的应用存在很多安全隐患，针对其中一部分安全隐患的防御，国内外有一些研究。而以 ACK 注入和修改、拖延 ACK、丢弃 ACK 为代表的 ACK 类攻击和以过编码和欠解码为代表的编码类攻击是网络编码环境下特有的，目前国内外还没有人研究，本文针对这两类攻击提出以下防御思想。

4.1 理论分析

哈希函数由于具有单向性、碰撞约束等优越特性，因此在信息安全领域得到了广泛的应用。本文借鉴文献[36]的思想，利用哈希函数的这些特性构造如下信息向量：

$$m=(x_1+f(a),x_2+f(a,x_1),x_3+f(a,x_1,x_2),\cdots,x_{n-1}+f(a,x_1,x_2,\cdots,x_{n-2}),a)^T$$

式中，$\{x_1,x_2,x_3,\cdots,x_{n-1}\}$是发送端要发送的信息字符序列，$f(.)$是哈希函数，$a$是随机字符。攻击者如果想获取信息序列中的$x_{n-1}$字符就必须获取完整的$\{x_1,x_2,x_3,\cdots,x_{n-2}\}$字符序列，并且还需破译哈希函数和随机字符$a$，这对攻击者来讲无疑是个巨大的困难，而接收者使用$a$就可以逐步地从$x_1$解析到$x_{n-1}$，这里只是用了一个字符$a$就可达到屏蔽$\{x_1,x_2,x_3,\cdots,x_{n-2}\}$的目的，付出的代价仅仅是牺牲$1/n$的传输效率，比之前的方法效率提高了很多。

在信息论中，与大数定理相对应的是渐进均分性(AEP)，它是弱大数定理的直接结果。渐进均分性表明$\frac{1}{n}\log\frac{1}{p(X_1,X_2,\cdots,X_n)}$近似于熵$H$，其中$X_1,X_2,\cdots,X_n$为独立同分布$(i.i.d)$随机变量。$p(X_1,X_2,\cdots,X_n)$是观察序列$X_1,X_2,\cdots,X_n$出现的概率。因而，当$n$很大时，一个观察序列的概率$p(X_1,X_2,\cdots,X_n)$近似等于$2^{-nH}$。从信息论的角度来看，可以用典型集来描述以上现象，典型集(Typical Set)的定义如下：

关于$p(x)$的典型集$A_\varepsilon^{(n)}$是序列$(X_1,X_2,\cdots,X_n)\in\chi^n$的集合，且满足以下性质：

$$2^{-n(H(X)+\varepsilon)}\leqslant p(X_1,X_2,\cdots,X_n)\leqslant 2^{-n(H(X)-\varepsilon)}$$

因此，可以将全体序列组成的集合划分为两个子集：其一是典型集，其二是非典型集。根据典型集的性质，在正常情况下，当n充分大时，$\Pr\{A_\varepsilon^{(n)}\}>1-\varepsilon$，亦即典型集的概率接近于1。

在基于ACK确认机制的通信系统中，发送端用户在正常的网络状态下，都会根据传输路径上各个节点链路层的最小MTU(最大传输单元)和接收端告知的接收窗口来确定发送数据尺寸，而接收端则根据自己已正确收到的报文序号确定自己的ACK确认号，并告诉对方，所以，发送端收到的ACK确认号应该是按照一定规律间隔排列的集合。如图7所示，假设发送方初始序列号为0，在$t1$时刻，发送方发送了N_1长度的数据，在$t2$时刻发送了N_2长度的数据，因此两次的ACK确认号则是(N_1,N_1+N_2)，在后续的时间里，可以依此类推。也就是说ACK序列是由$\{N_1,N_2,\cdots,N_k\}$序列决定的，而$\{N_1,N_2,\cdots,N_k\}$序列是由最小MTU和接收窗口两者之中的小者决定的，在既定的网络中，MTU大小的个数是有限的，而接收窗口的变化范围也是有限数量的，因此$\{N_1,N_2,\cdots,N_k\}$序列将会是由有限个数值组成的集合，并且组成元素是相对固定的。

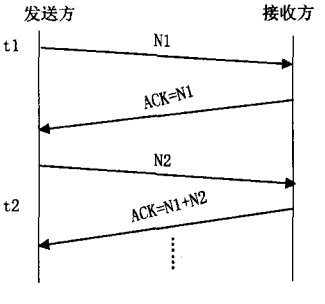

图7 ACK确认机制示意图

因此，我们可以将发送端收到的全体ACK确认号组成的集合分为典型集和非典型集，该典型集的组成元素及其所占概率是相对固定的，而在发生了攻击或网络状态恶化的情况下，该典型集的组成元素以及概率就会发生变化。

4.2 实现的基本思想

4.2.1 ACK类攻击的防御

在研究防御ACK注入和修改、丢弃ACK、拖延ACK等攻击的时候，如上所述的$\{x_1,x_2,x_3,\cdots,x_{n-1}\}$表示的是不同时刻的ACK确认序号组成的序列，并以如上所述的信息向量的方式发给发送方。那么攻击者无法获知每一个真实的ACK确认序号x_{n-1}，只能够获得如$x_{n-1}+f(a,x_1,x_2,\cdots,x_{n-2})$形式的密文，因此他们只能够丢弃对ACK的攻击，或者随机地修改和注入ACK。

从信息论的角度来看，发送端收到的ACK确认序号构成一个集合，在正常情况下，可以证明它是一个典型集，并通过分析可以确定该典型集的构成以及相应的概率。

如果存在攻击，在发送端经过与$f(a)$运算解码后获得的$\{x_1,x_2,x_3,\cdots,x_{n-1}\}$将不会是所期望的典型集，从而可以发现发生错误的概率，并可以按照概率的方式推测出正确的ACK确认序号，进而采取防范措施。防范的措施有：根据典型集的构成，可以按照概率的方式推测出正确的ACK确认序号。

同时，通过分析可以发现，在基于ACK确认机制的通信网络中，当前的ACK确认序号状态都仅与前一时刻的状态有关，而与过去的状态无关，因此典型集中的各元素之间的状态转移可以用马尔可夫模型来描述，可以利用转移矩阵来预测下一状态到达的概率，并检测当前ACK状态出错的概率，从而达到检错纠错的目的。

本文思想的基本步骤如下：

(1)分析正常数据，利用信息论的方法确定ACK确认序号序列典型集的组成元素；

(2)统计每一个元素出现的次数，从而计算每一个元素k出现的频率$P(k)$；

(3)将$P(k)$从大到小排序并编号；

(4)计算使$\sum_{k=1}^{N-1}p(k)\geqslant 0.9999$成立的最小正整数$N$(其中$P(k)$为编号为$k$的元素出现的频率)，将编号为$1-N-1$的元素分别作为马尔可夫过程的一个状态，将剩余的元素合并为马尔可夫过程的一个状态，这样就构造出一个状态数为N的马尔可夫过程[39]。

4.2.2 编码类攻击的防御

根据原理可知，过编码和欠解码攻击是攻击者采用不同于事前确定的参与编码节点策略，要么更多节点参与编码，要么就更少节点参与编码。因此制定一个难以被攻击者破译的参与编码节点策略是防御攻击的关键。

本文根据网络拓扑的情况，确定参与编码节点策略，并定期切换策略。而保证策略安全传输的方法是：将不同时刻参与编码的节点数组织成一个序列，并用上述的$\{x_1,x_2,x_3,\cdots,x_{n-1}\}$来表示，收发双方使用信息向量$m$的加密方式来传递这一序列，因此正如上节理论分析的那样，攻击者将几乎不可能获得真实的参与编码节点的相关信息，也就无法展开攻击了。

结束语 如前所述，在基于网络编码的网络中，存在如此

多的安全隐患，而在当前的研究中，除了污染攻击外，其他攻击的防御方法研究得很少，网络编码缺乏安全保证是其在网络中大规模应用的一个极大障碍，这也为未来开辟了新的研究领域。

网络编码的中心思想是利用节点的计算能力换取网络的信息传输能力，而云计算[38](Cloud Computing)是利用各节点的整体计算资源换取整个网络的服务能力。所以，在未来的研究中，如果将网络编码与云计算结合起来，构建从终端到交换节点、从底层到高层、无处不在的计算网络，并且以网络用户身份、行为可信的网络作为它的平台，定将使目前网络的服务质量得到极大的提升。

本文的主要贡献在于：1)从物理层网络编码的原理出发，首次分析发现其中潜在的条件破坏、幅度攻击、能量攻击等安全隐患。2)综述了当前针对网络编码中已存在安全隐患的防御研究的进展。3)针对 ACK 类和编码类攻击，提出了基于典型集和哈希函数以及马尔可夫模型的防御方法，鉴于 ACK 确认是一个应用很广的通信机制，这一解决 ACK 类攻击的方法将会为其他领域的针对 ACK 确认机制的攻击提供解决思路。4)提出了结合利用云计算和网络编码构建计算网络的概念。

参 考 文 献

[1] Ahlswede R, Cai N, Li S Y R, et al. Network information flow [J]. IEEE Trans on Information Theory, 2000, 46(4): 1204-1216

[2] Li S Y R, Yeung R W, Cai N. Linear network coding[J]. IEEE Trans on Information Theory, 2003, 49(2): 371-381

[3] Zhang Sheng-li, Liew S C. Hot topic: physical-layer network coding [C]// Proceedings of the 12th annual international conference on Mobile computing and networking. Los Angeles, CA, USA, 2006

[4] Katti S, Gollakota S, Katabi D. Embracing wireless interference: Analog network coding[C]// Proc. ACM SIGCOMM. Kyoto, Japan, Aug. 2007: 397-408

[5] Laneman J N, Tse D N C, Wornell G W. Cooperative diversity in wireless networks: Efficient protocols and outage behavior [J]. IEEE Trans. Inf. Theory, 2004, 51(12): 3062-3080

[6] Lu Ke-jie, Fu Sheng-li, Qian Yi. On The Security Performance of Physical-Layer Network Coding [C] // Proc. IEEE ICC 2008Beijing, China, May 2008

[7] Ho T, Lun D S. Network coding: an introduction [M]. Cambridge University Press, 2008: 49-60

[8] Byers J W, Luby M. A digital fountain approach to reliable distribution of bulk data[C]// Proceedings of the ACM SIGCOMM '98 conference on applications, technologies, architectures, and protocols for computer communication. Vancouver, British Columbia, Canada, 1998: 56-67

[9] Dong Jing, Curtmola R. Secure network coding for wireless mesh networks: Threats, challenges, and directions [J]. Computer Communications, 2009, 323(17): 1790-1801

[10] Chachulski S, Jennings M, Katti S, et al. Trading structure for randomness in wireless opportunistic routing [C] // Proc. of ACM SIGCOMM'07. 2007

[11] Zhang X, Li B. DICE: a game theoretic framework for wireless multipath network coding[C]// Proc. of Mobihoc 2008

[12] Dong J, Curtmola R, Nita-Rotaru C. On the pitfalls of using high-throughput multicast metrics in adversarial wireless mesh networks[C]// Proc. of SECON'08. June 2008

[13] Hu Y-C, Perrig A, Johnson D B. Packet leashes: a defense against wormhole attacks in wireless ad hoc networks[C]// INFOCOM. 2003

[14] Eriksson J, Krishnamurthy S, Faloutsos M. Truelink: a practical countermeasure to the wormhole attack in wireless networks[C]// Proc. of ICNP'06. 2006

[15] Dong J, Curtmola R, Nita-Rotaru C. Practical defenses against pollution attacks in intra-flow network coding for wireless mesh networks[C]// Proc. of WiSec'09. 2009

[16] Krohn M, Freedman M, Mazieres D. On-the-fly verification of rateless erasure codes for efficient content distribution[C]// Proc. of Symposium on Security and Privacy. 2004

[17] Kehdi E, Li B. Null keys: limiting malicious attacks via null space properties of network coding[C]// INFOCOM. 2009

[18] Yu Z, Wei Y, Ramkumar B, et al. An efficient signature-based scheme for securing network coding against pollution attacks [C]// Proc. of INFOCOM 08. 2008

[19] Yu Z, Wei Y, Ramkumar B, et al. An efficient signature scheme for securing xor network coding against pollution attacks[C]// INFOCOM. 2009

[20] Ho T, Leong B, Koetter R, et al. Byzantine modification detection in multicast networks using randomized network coding[C]// Proc. of ISIT'04

[21] Jaggi S, Langberg M, Katti S, et al. Resilient network coding in the presence of byzantine adversaries[C]// Proc. of INFOCOM'07. 2007

[22] Wang D, Silva D, Kschischang F R. Constricting the adversary: a broadcast transformation for network coding [C] // Allerton 2007. 2007

[23] Koetter R, Kschischang F R. Coding for errors and erasures in random network coding[J]. IEEE Trans. Inform. Theory, 2008, 54(8): 3579-3591

[24] Marti S, Giuli T, Lai K, et al. Mitigating routing misbehavior in mobile ad hoc networks[C]// Proc. of MOBICOM. August 2000

[25] Katti S, Rahul H, Hu W, et al. Crowcroft, Xors in the air: practical wireless network coding[C]// Proc. of ACM SIGCOMM'06. 2006

[26] Le J, Lui J C S, Chiu D M. DCAR: distributed coding-aware routing in wireless networks[C]// Proc. of ICDCS'08. 2008

[27] Hu Y-C, Perrig A, Johnson D B. Ariadne: a secure on-demand routing protocol for ad hoc networks[J]. Wireless Networks, 2005, 11(1/2): 21-38

[28] Lin Chuang, Peng Xue-hai. Research on Trustworthy Networks [J]. Chinese Journal of Computers, 2005, 28(5): 751-758

[29] Gkantsidis C, Rodriguez P. Cooperative security for network coding file distribution[C]// Proceedings of IEEE INFOCOM. 2006

[30] Jiang Yi-xin, Fan Yan-fei, Shen Xue-min. A self-adaptive probabilistic packet filtering scheme against entropy attacks in network coding[J]. Computer Networks, 2009, (53): 3089-3101

[31] Ho T, Leong B, Koetter R, et al. Byzantine modification detection in multicast networks with random network coding [J]. IEEE Transactions on Information Theory, 2008, 54(6): 2798-2803

[32] Charles D, Jain K, Lauter K. Signatures for network coding[C]// The 40th Annual Conf on Information Sciences and Systems.

Princeton, NJ, 2006
[33] Cai N, Yeung R W. Secure Network Coding[C]// Proc. IEEE Int'l. Symp. Info. Theory. 2002:323
[34] Jain K. Security based on network topology against the wiretapping attack[J]. IEEE Wireless Communications, 2004, 11(1): 68-71
[35] Bhattad K, Narayanan K R. Weakly secure network coding[C]// Proc. NETCOD'05. Riva del Garda. Italy, Apr. 2005
[36] Adeli M, Liu Hua-ping. Secure Network Coding with Minimum Overhead Based on Hash Functions[J]. IEEE Communications Letters, 2009, 13(12): 956-958
[37] Rouayheb S Y E, Soljanin E. On wiretap networks II[C]// Proc. IEEE Int. Symp. Information Theory. Nice. France, 2007: 551-555
[38] Luis M V, Luis Rodero-merino, Juan Caceres, et al. A break in the clouds: toward a cloud definition[J]. ACM SIGCOMM Computer Communication Review, 2009, 39(1): 50-55
[39] Schonlaum, Dumouchelw, Ju Wen-hua. Computer intrusion: Detecting masquerades[J]. Statistical Science, 2001, 16(1): 1-17
[40] 余顺争，唐人亨. 二商品流最大流问题的合成流算法[J]. 北京邮电学院学报，1987，10(2)：21-29
[41] MinJi Kim, Lu'sa Lima, Zhao Fang, et al. On Counteracting Byzantine Attacks in Network Coded Peer-to-Peer Networks[J]. IEEE Journal on Selected Areas in Communications, 2010, 28(5): 692-702
[42] Liu Ai-xi, Yu Shun-zheng. Secure Physical Layer Network Coding: Challenges and Directions[C]// The International Conference on Internet Technology and Applications (iTAP 2010). Wuhan, August 2010
[43] 王静. 网络编码理论及其应用的研究[D]. 西安：西安电子科技大学，2008
[44] 贾春福，钟安鸣，等. 基于系统调用的 Linux 系统入侵检测技术研究[J]. 计算机应用研究，2007，24(4)：147-150

(上接第 6 页)

有不小的差距。因此，如何更好地支持艺术设计工作，更多地模拟艺术家的创作思路；如何更好地解决视频绘制中的连续性问题，并提高绘制效率，都是未来油画风格化的重要研究方向。

参 考 文 献

[1] Haeberli P. Paint By Numbers: Abstract Image Representations [J]. ACM SIGGRAPH Computer Graphics, 1990, 24(4): 214
[2] Litwinowicz P. Processing images and video for an impressionist effect[C]// Proc. SIGGRAPH'97. Addison Wesley Publishing Co, 1997: 407-414
[3] Hertzmann A. Painterly rendering with curved brush strokes of multiple sizes[C]// Proc. SIGGRAPH. ACM, 1998: 453
[4] Gooch B, Coombe G, Shirley P. Artistic Vision: Painterly Rendering Using Computer Vision Techniques[C]// Proc. Non-photorealistic Animation and Rendering. ACM, 2002: 83-90
[5] Hays J, Essa I. Image and video based painterly animation[C]// Proc. Non-photorealistic Animation and Rendering. ACM, 2004: 113-120
[6] Olsen S C, Maxwell B A, Gooch B. Interactive vector fields for painterly rendering[C]// Proc. Graphics Interface. Canadian Human-Computer Communications Society, 2005: 241-247
[7] Zhang E, Hays J, Turk G. Interactive tensor field design and visualization on surfaces[J]. IEEE Transactions on Visualization and Computer Graphics, 2007: 94-107
[8] Lee H, Lee C H, Yoon K. Motion based painterly rendering[J]. Computer Graphics Forum, 2009, 28(4): 1207-1215
[9] Hertzmann A. Fast Paint Texture[C]// Proc. Non-photorealistic Animation and Rendering. ACM, 2002: 03-05
[10] Zeng Kun, Zhao Ming-tian, Xiong Cai-ming, et al. From image parsing to painterly rendering[J]. ACM Transactions on Graphics, 2009, 29(1): 1-11
[11] Hertzmann A, Jacobs C E, Oliver N, et al. Image analogies[C]// Proc. SIGGRAPH. ACM, 2001: 327-340
[12] Wang Bin, Wang Wen-ping, Yang Huai-ping, et al. Efficient example-based painting and synthesis 2d directional texture[J]. IEEE Transactions on Visualization and Computer Graphics, 2004, 10(3): 266-277
[13] Lee H, Seo S, Ryoo S, et al. Directional texture transfer [C]// Proc. Non-photorealistic Animation and Rendering. ACM, 2010: 43-48
[14] Huang Hua, Zang Yu, Li Chen-feng. Example-based Painting Guided by Color Features[J]. The Visual Computer, 2010, 26(6-8): 933
[15] Meier B J. Painterly rendering for animation[C]// Proc. SIGGRAPH. ACM, 1996: 477-484
[16] Green S, Salesin D, Schofield S, et al. Non-photorealistic rendering[C]// Proc. SIGGRAPH Non-photorealistic Rendering Course Notes. AK Peters Ltd, 1999
[17] Hertzmann A, Perlin K. Painterly rendering for video and interaction[C]// Proc. Non-photorealistic Animation and Rendering. ACM, 2000: 7-12
[18] Kovacs L, Sziranyi T. Creating animations combining stochastic paintbrush transformation and motion detection[C]// Proc. International Conference on Pattern Recognition. 2002: 1090-1093
[19] Park Y, Yoon K. Painterly animation using motion maps[J]. Graphical Models, 2008, 70(1): 1-15
[20] Kagaya M, Brendel W, Deng Qing-qing, et al. Video painting with space-time-varying style parameters[J]. IEEE Transactions on Visualization and Computer Graphics, 2010(to appear)
[21] Wang Jue, Xu Ying-qing, Shum H Y, et al. Video tooning[J]. ACM Transactions on Graphics, 2004, 23(3): 574-583
[22] Lin Liang, Zeng Kun, Lv Han, et al. Painterly animation using video semantics and feature correspondense[C]// Proc. Symposium on Non-photorealistic Animation and Rendering. ACM, 2010: 73-80
[23] Bai Xue, Wang Jue, Simons D, et al. Video snapcut: Robust video object cutout using localized classifier[J]. ACM Transactions on Graphics, 2009, 28(3): 1-11
[24] Huang Hua, Zhang Lei, Fu Tian-nan. Video painting via motion layer manipulation[J]. Computer Graphics Forum, 2010, 29(7): 2055-2064
[25] Klein A W, Sloan P J, Finkelstein A, et al. Stylized video cubes [C]// Proc. Symposium on Computer Animation. ACM, 2002: 15-22
[26] Collomosse J P, Rowntree D, Hall P M. Stroke Surfaces: Temporally coherent artistic animations from video[J]. IEEE Transactions on Visualization and Computer Graphics, 2005, 11(5): 540-549