

文章编号:1001-9081(2012)01-0066-04

doi:10.3724/SP.J.1087.2012.00066

网络编码下的网络电视条件接收系统关键技术

李伟键^{1,2*}

(1. 广东技术师范学院 计算机科学学院, 广州 510665; 2. 华南理工大学 计算机科学与工程学院, 广州 510641)

(*通信作者电子邮箱 weijianlee@126.com)

摘要: 网络编码的主要优点是提高网络吞吐量、均衡网络负载以及提高带宽利用率, 尤其适合无线网络、Ad Hoc、P2P 以及流媒体传输等领域, 在构建 IP 网络电视方面具有巨大的潜力。研究在网络编码下构建网络电视的条件接收系统, 提出了一种基于随机网络编码(RLNC)和 SPOC 模型的轻量级加密方法和一种高效的层次组密钥分发管理方案。所提方案具有加密数据量非常小的优点, 适合用于网络电视实时流媒体加密, 同时结合 MPEG 多分辨率的特点, 可以针对各种付费用户, 根据不同的收费提供不同网络视频质量。性能分析表明, 所提方案利用网络编码提高了网络吞吐量, 同时加密数据量远小于传统的 IP 网络电视加密方法, 层次组密钥分发管理方案有效解决了密钥分发问题。

关键词: 数据安全与计算机安全; 网络编码; 条件接收系统; 层次组密钥分发管理; 多分辨率; 网络电视

中图分类号: TP393.08; TN918.3 **文献标志码:**A

Key techniques of conditional access system for Internet-TV based on network coding

LI Wei-jian^{1,2*}

(1. School of Computer Science, Guangdong Polytechnic Normal University, Guangzhou Guangdong 510665, China;
2. School of Computer Science and Engineering, South China University of Technology, Guangzhou Guangdong 510641, China)

Abstract: Network coding has the advantage of providing higher network throughput, using bandwidth efficiently and balancing the traffic, which is suitable for wireless networks, Ad Hoc, P2P content distribution and streaming media service, especially for Internet-TV. The authors did some research into the conditional access system for Internet-TV under network coding, proposed a scheme for conditional access technique based on Random Linear Network Coding (RLNC) and Secure Practical Network Coding (SPOC), and hierarchical key distribution. This scheme also provided different media quality to different paying customers. The scheme has low-complexity cryptographic overhead, and it is thus suitable for the real-time encryption of streaming media. The performance analysis shows that the proposed scheme improves the throughput of Internet-TV, the quantity of encrypted data is far less than the traditional methods, and the hierarchical group key distribution effectively solves the problem of key distribution.

Key words: data and computer security; network coding; conditional access system; hierarchy group key distribution; multi-resolution; Internet-TV

0 引言

Ahlswede 等^[1]在 2000 年的 IEEE 信息论会刊上首次提出了网络编码(Network Coding)的概念并从理论上证明:如果允许网络节点对传输的信息按照合适的方式进行编码处理(如模二加、有限域上的运算等),而非限于存储和转发,则基于该方式的网络多播总能够实现理论上的最大传输容量(最大流最小割)。网络节点对传输信息进行操作和处理的过程,就称为网络编码。网络编码的主要优点是可以提高网络吞吐量、均衡网络负载以及提高带宽利用率,尤其适合无线网络、Ad Hoc 及 P2P 等领域。Koetter 等^[2]运用离散随机过程的方法,给出了一种线性网络编码的构造方法,说明 LCM(Linear-Code Multicast) 系统中转移矩阵 M_i 的构造过程,并证明,只要能够保证最终形成的转移矩阵 M_i 满秩,则对应的信宿节点通过 $y = z \times M_i$ 就能准确译出信源发送的原始信息。Ho 等^[3]、Chou 等^[4-5]提出了一种可行的分布式网络编码的实现方法:随机网络编码(Random Network Coding, RNC),该方法基于一种随机选择编码向量的策略:对于除了

信宿节点外的所有中间节点,只要在一个足够大的有限域上随机选择它们输入链路到输出链路的映射,而且各节点映射关系的选取是相互独立的,就能以较高概率使各个信宿节点对应的系统转移矩阵 M 满秩,即各信宿节点能以较高的概率成功译码。Cai 等^[6]最先研究了单信源有向无圈网络中数据安全多播问题,给出了搭线窃听的网络通信模型,并且构造了在信息论意义上的安全网络编码,即窃听者无论偷听所给定偷听范围内的哪个窃听集都无法恢复出原始信息。Lima 等^[7-10]给出了一种通用威胁模型下的新的安全框架——SPOC(Secure Practical Network Coding),该框架的危险模型不再局限于假设攻击者只能通过搭线窃听有限的通信链路,而是攻击者可以获取网络中通信的所有数据,也能获取编码和解码系数。SPOC 利用随机网络编码(Random Linear Network Coding, RLNC)本身固有的安全特性,通过加密源节点的编码系数来保证安全,并且在文献[7]中证明该方法是信息论上安全的。SPOC 的优点是加密数据量很小,尤其适合于流媒体加密。

另一方面,随着因特网的发展以及带宽的提升,多媒体内

容服务已经成为因特网上极其重要的网络服务。越来越多的商业网站提供音视频内容服务,人们也越来越习惯于从因特网上获取音视频信息。因此,若能将数字电视网络上面的巨大媒体资源引入到IP网上,一方面可以丰富IP宽带网上的业务量,促进IP宽带网络的普及和发展;另一方面,网络平台的扩充,将给节目运营商带来更多的收视用户,从而可以降低成本,增加收入。

考虑到多媒体源的版权问题,需要对其进行加密防止网络上的非付费用户非法收看,这需要更加高效的,不同于传统的端对端的加密方法:条件接收系统^[11]。而为了适应不同网络质量下的音视频传输,人们提出了多分辨率的MPEG标准^[12]。该标准引入一种多分辨率编码方法,把视频流变成多层次,根据网络质量提供不同层的音视频,音视频质量由能接收到的层的数量决定。同时,随着因特网上音视频服务的发展,尤其是未来三网融合,需要考虑根据不同收费提供不同的收看质量。用户可以根据需要,付出不同的费用收看不同质量的视频。

网络编码具有提高网络吞吐量、均衡网络负载以及提高带宽利用率的优点,尤其适合无线网络、Ad Hoc、P2P以及流媒体传输等领域,因此本文希望构建基于网络编码的网络电视条件接收系统。与传统的数字媒体有条件接收系统一样,基于网络编码的网络电视条件接收系统需要解决如下两个关键问题。

1) 数字视频加密方法的安全性与实时性。数字视频数据量大、实时性强,加/解密操作会增加运算负担;同时,用户端设备运算能力和资源有限。因此需要快速、有效的加密方案。

2) 密钥管理的复杂性和可扩缩性。密钥管理是安全系统中最复杂的部分,条件接收系统涉及的用户数量很大,需要寻找一种高效、可扩缩性的密钥管理方案。

本文研究在网络编码下构建网络电视的条件接收系统,主要工作如下。

1) 提出一种基于RLNC和SPOC模型的轻量级加密方法。该方法具有加密数据量非常小的优点,适合用于网络电视实时流媒体加密,同时结合MPEG多分辨率的特点,可以针对各种付费用户,根据不同的收费提供不同网络视频质量。

2) 提出一种适用于网络编码的高效层次组密钥分发管理方案,大大减少了分发密钥的数量。

1 SPOC 安全框架

在RLNC环境下,SPOC安全加密框架按照如下方式工作:其中包括源节点、中间节点以及接收节点。中间节点按照随机网络编码方式进行工作即可,不需做任何修改,也不需要知道加密细节。而源节点、接收节点进行下述加密操作。

对于源节点,执行如下步骤:

- 1) 使用某种密钥交换机制,在源节点和接收节点间交换共享密钥k,用于加密全局编码矩阵A(称为锁定系数);
- 2) 对于h个报文,产生 $h \times h$ 全局编码矩阵A,对报文进行网络编码;
- 3) 产生一个 $h \times h$ 的单位矩阵I,把I的每一行向量(称为非锁定系数)加入到每个编码后的报文头;
- 4) 把A相应的每一行向量使用密钥k进行加密,加入报文头。

对于中间节点,与RLNC相同操作。对于收到的报文,产生随机编码系数对报文头(包括锁定系数、非锁定系数)、报文数据进行网络编码。

对于接收节点,执行如下步骤:

- 1) 通过非锁定系数,计算出加密的锁定系数;
- 2) 对锁定系数进行解密,可以得到全局编码矩阵A;
- 3) 通过非锁定系数和锁定系数,可以构造解码矩阵;
- 4) 使用高斯消元法,求得源节点发送的数据。

图1给出了该方法实现的例子。考虑网络编码经典的蝴蝶网络,考虑单源多接收节点的多播情况。

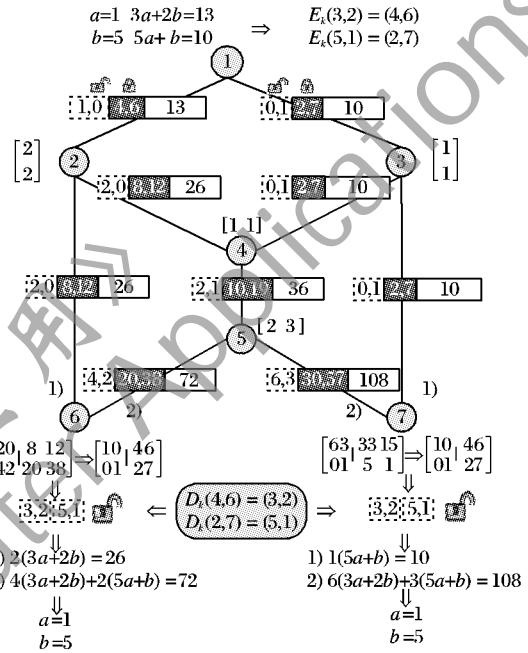


图1 SPOC 安全框架

假设源节点1要发送信息至接收节点6和7。1需要实现和6、7协商好加密算法还有密钥k。对于加密算法,只需要其输入明文和输出密文大小相同(如3DES、AES)即可。

假设源节点1要发送的数据为 $a = 1, b = 5$ 。则节点1先产生全局编码矩阵 $A: \begin{bmatrix} 3 & 2 \\ 5 & 1 \end{bmatrix}$ 。采用某一种加密算法对A的每一行向量加密,假设结果为 $E(3,2) = (4,6), E(5,1) = (2,7)$ 。源节点1把单位矩阵I的每一个行向量和相应的加密了的A的行向量放在报文包头,把网络编码值放在报文数据段,发送数据。中间节点按照传统网络编码的方法,处理包头和数据部分。

接收节点可以根据包头的锁定数据恢复加密系数 $\begin{bmatrix} 4 & 6 \\ 2 & 7 \end{bmatrix}$,通过解密操作,恢复 $A: \begin{bmatrix} 3 & 2 \\ 5 & 1 \end{bmatrix}$ 。所以其他节点由于没有共享密钥k,从而无法恢复A。拥有了A之后,接收节点便可以恢复原有数据。

采用SPOC的优点是加密数据量很小,尤其适合于流媒体加密。

2 条件接收系统方案

2.1 加密方法描述

本文引入图1的SPOC安全框架作为条件接收系统,对数据进行实时、轻量级加密,其中视频服务器为源节点1,6,7等

接收节点为最终用户。假设采用 MPEG 对传输的流媒体编码为 1 层, 则源节点与接收节点交换 l 个共享密钥 k_1, k_2, \dots, k_l 。

1 分别采用密钥 k_i 加密第 i 层数据包, 如图 2 所示, 假设通过 MPEG 编码为 3 层, 分别采用密钥 k_1, k_2, k_3 加密全局编码矩阵 A 的每一行向量, 为了使得译码成功, 需要构造的必须全局编码矩阵 A 为下三角矩阵。

因此, 只具有 k_1 的接收节点只可以译码第 1 个报文, 具有 k_1, k_2 的接收节点只可以译码第一二个报文, 具有 k_1, k_2, k_3 的接收节点可以译码第 1、2、3 个报文。

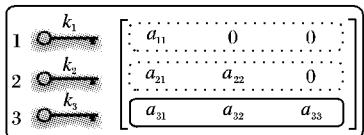


图 2 数据加密模式

图 2 方法容易遭受已知明文攻击: 假设 n^2 个已知明文密文对, 则可以构造 n^2 个关于 $a_{11}, \dots, a_{1n}, \dots, a_{n1}, \dots, a_{nn}$ 共 n^2 个变量的线性方程, 即使没有拥有 k_1, k_2, \dots, k_n 个密钥也可以猜出全局编码矩阵 A , 从而可以解码得到原始数据。

为此, 本文进行了改进, 如图 3 所示。

$$\left\{ \begin{array}{l} \boxed{a_{11}(b_1 \oplus k_1)} + 0 + 0 = \gamma_1 \\ \boxed{a_{21}(b_1 \oplus k_1)} + \boxed{a_{22}(b_2 \oplus k_2)} + 0 = \gamma_2 \\ \boxed{a_{31}(b_1 \oplus k_1)} + \boxed{a_{32}(b_2 \oplus k_2)} + \boxed{a_{33}(b_3 \oplus k_3)} = \gamma_3 \end{array} \right.$$

图 3 改进后的数据加密模式

图 3 中, 本文方法修改了源节点网络编码的模式。源节点把要传送的数据先与密钥异或再传送, 从而使得攻击者明文攻击时候即使拥有了明文 b_1, \dots, b_n , 也无法构造一个 n^2 个变量的线性方程(事实上对于攻击者而言已经变成了 2 次方程), 从而解决了已知明文攻击问题。

2.2 密钥分发管理

在本文使用的框架 SPOC 里边, 需要源节点与接收节点事先交换共享密钥 k_1, k_2, \dots, k_l 。

采用传统的密钥管理方法, 需要加密分发密钥次数为 $\sum_{l=1}^L lt_l$ 。其中: L 为 MPEG 编码层数, t_l 为第 l 层接收节点个数。

考虑有 m 个频道, 共需要加密密钥次数为 $m \sum_{l=1}^L lt_l$ 。在网络编码环境中, 所有数据都是通过广播的方式传播, 需要分发的密钥数量也是 $m \sum_{l=1}^L lt_l$ 。因此大量用户(每一层的 t_l 很大)、大量频道的情况下, 密钥分发通信和计算代价非常高。

2.2.1 层次密钥分发模式

结合网络编码广播的特征, 本文引入高效的层次密钥分发方法来解决这个问题。考虑如图 4 所示的层次结构进行密钥分发。



图 4 单频道的密钥加密分发层次图

本文方法使用密钥 k_2 加密密钥 k_1 , 密钥 k_3 加密密钥 k_2 , 以此类推, 用 k_l 加密 k_{l-1} , 通过网络编码的方式广播出去, 所有节点都可以接收到加密的 $k_1 \dots k_{l-1}$ 。对于接收节点 T , 如果其订购的是第 i 层的收看质量, 则再使用 T 的密钥加密分发密钥 k_i 即可。通过 k_i 可以解密 k_{i-1} , 逐层解密得到 k_{i-2}, \dots, k_2, k_1 。

因此单个频道需要加密和分发的密钥数为 $(L-1)+t$, 其中 t 为接收节点(用户)的个数, m 个频道需要加密和分发的密钥数为 $m((L-1)+t)$ 。

2.2.2 分组的层次密钥分发模式

在多个频道的情况下, 本文方法可以结合采用如下的层次分发方法。考虑在多个频道多个用户下实现多分辨率的流媒体传输的密钥高效分发, 本文引入了分组管理方法把电视频道分成多个组(也即以频道组作为用户的基本收费单位)。图 5 演示了在多个频道的情况下, 如何按照收费标准编制频道分组。

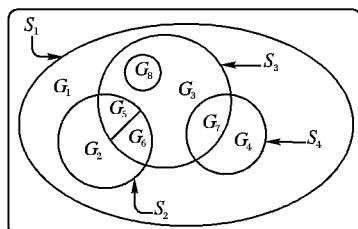


图 5 频道分组

如图 5 所示, 本文方法把所有频道进行分组, 同时组中的频道指定了清晰度(提供该频道的 k_i 密钥, 提供了第 i 层的清晰度), 如图 6 所示。每个组有一个组密钥, 使用组密钥加密 k_i , 然后分发该加密的 k_i 和组密钥即可。假设总共划分了 g 组(g 远小于频道数 m), 则需要加密和分发的密钥数为 $2gt$ 。

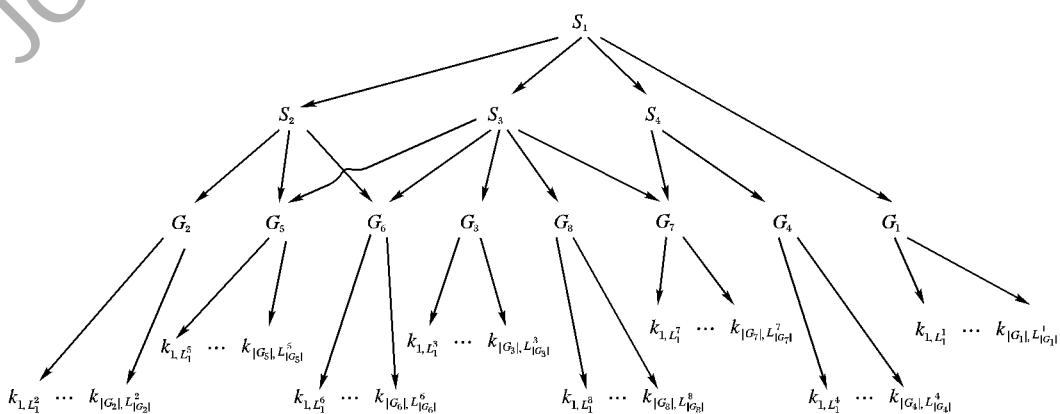


图 6 多频道的密钥加密分发层次图

在这种情况下,对于每个频道广播加密的 $k_1 \cdots k_{L-1}, m$ 个频道共需加密和分发的密钥数为 $m(L-1)$, 同时需加密和分发的组密钥为 $2gt$, 因此总共需要加密和分发的密钥数为 $m(L-1) + 2gt$, 远小于 $m((L-1) + t)$, 更远小于 $m \sum_{i=1}^L lt_i$ 。

3 性能分析

3.1 加密效率分析

采用本文框架,需要加密的数据非常少,图 7 分析了加密数据量。

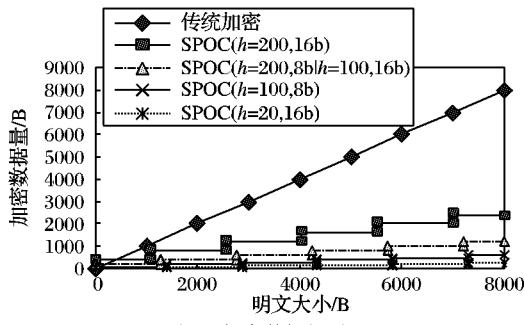


图 7 加密数据量对比

传统加密方法需要对所有传输数据进行加密,因此加密数据量与传输数据成正比。在本框架中只加密编码系数,与传输数据直接没有直接关联,因此加密数据量非常小。

3.2 加密和分发密钥数据量分析

1) 传统密钥分发模式下,对于 t 个用户, m 个频道, 每个频道提供 L 层视频质量, t_l 为收看第 l 层视频质量的用户数, 需要加密分发的密钥数量为 $m \sum_{l=1}^L lt_l$ 。

2) 采用层次密钥分发模式时,需要加密和分发的密钥数为 $m((L-1) + t)$ 。

3) 采用分组的层次密钥分发模式时,需要加密和分发的密钥数为 $m(L-1) + 2gt$, 其中 g 为节目的分组数量,远小于节目数 m 。

图 8 在用户数和频道数固定情况下,比较分析了传统密钥分发模式与层次密钥分发模式在不同层数的传输质量下所需要传输的密钥数,可以看出来传统的密钥分发模式随着视频质量的层数的增加而线性增加,而层次密钥分发模式几乎不会增加。

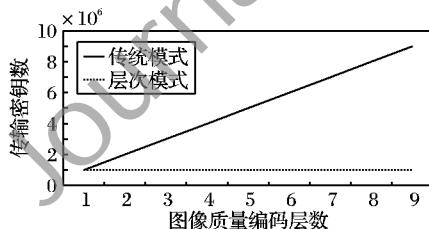


图 8 传统密钥分发模式与层次密钥分发模式传输密钥数比较

图 9 在用户数和视频质量层数固定情况下,比较分析了未分组层次密钥分发模式与分组层次密钥分发模式在不同频道数下所需要传输的密钥数,可以看出来未分组层次密钥分发模式随着频道数的增加而线性增加,而层次密钥分发模式几乎不会增加。

为了直观比较 3 种密钥分发模式下的传输密钥数,本文给出了具体参数下的传输密钥数比较,由表 1 可以看出本文提出的分组层次密钥分发方法不随着频道数和视频质量层数而线性增加,具有明显的优越性。

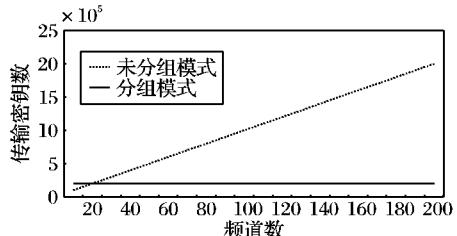


图 9 未分组与分组层次密钥分发模式传输密钥数比较

表 1 3 种密钥分发模式比较

密钥分发模式	用户数 t	频道数 m	视频质量总层数 L	分组数 g	传输密钥数
传统模式	10 000	100	4	—	4 000 000
	20 000	100	4	—	8 000 000
	20 000	200	4	—	16 000 000
层次密钥分发模式	10 000	100	4	—	1 000 300
	20 000	100	4	—	2 000 300
	20 000	200	4	—	4 000 300
分组层次密钥分发模式	10 000	100	4	10	200 300
	20 000	100	4	10	400 300
	20 000	200	4	10	400 600

4 结语

随着因特网的发展尤其是网络编码新技术的发展,网络带宽得到极大提升,人们也越来越习惯于从因特网上获取音视频信息。因此,把数字电视网络上面的巨大媒体资源引入到 IP 网上是大势所趋,一方面可以丰富 IP 宽带网上的业务量,促进 IP 宽带网络的普及和发展;另一方面,网络平台的扩充,将给节目运营商带来更多的收视用户,从而可以降低成本,增加收入。

网络编码的主要优点是提高网络吞吐量、均衡网络负载以及提高带宽利用率,尤其适合无线网络、Ad Hoc、P2P 以及流媒体传输等领域。本文重点研究在网络编码下构建网络电视的条件接收系统的实现,提出了一种基于 RLNC 和 SPOC 模型的条件接收技术和分组层次密钥分发管理方案。本文方案同时结合 MPEG 多分辨率的特点,针对各种付费用户,根据不同的收费提供不同网络视频质量。该方案具有加密数据量非常小的优点,适合用于网络电视实时流媒体加密。

参考文献:

- AHLSWEDE R, CAI N, LI S-Y, et al. Network information flow [J]. IEEE Transactions on Information Theory, 2000, 46(4): 1204–1216.
- KOETTER R, MEDARD M. An algebraic approach to network coding [J]. IEEE/ACM Transactions on Networking, 2003, 11(5): 782–795.
- HO T, MEDARD M, KOETTER R. A random linear network coding approach to multicast [J]. IEEE Transactions on Information Theory, 2006, 52(10): 4413–4430.
- CHOU P A, WU Y, JAIN K. Practical network coding [C]// Proceedings of the Annual Allerton Conference on Communication Control and Computing. Allerton: [s. n.], 2003: 40–49.
- CHOU P A, WU Y. Network coding for the Internet and wireless networks [J]. IEEE Signal Processing Magazine, Special Issue on Signal Processing for Multiterminal Communication Systems, 2007, 24(5): 77–85.
- CAI N, YEUNG R W. Secure network coding [C]// Proceedings of 2002 IEEE International Symposium on Information Theory. Washington, DC: IEEE Computer Society, 2002: 323.

(下转第 81 页)

个的情况开始逐步增加直至7个,并通过实验观察它的传输速率随共享文件个数的变化规律。并由此得到图7,其中示例中的80 b或160 b指实验时使用隐蔽通道传输的文件大小。

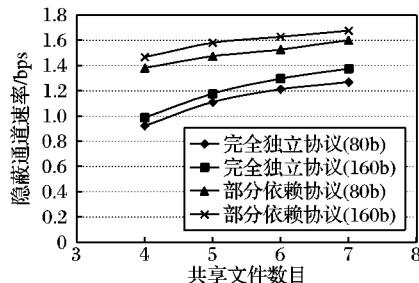


图7 隐蔽通道速率随共享文件数目变化规律

3.3 实验数据分析及结果

通过以上数据,可以看出这种基于共享文件的隐蔽通道可靠性较高。可靠协议与不可靠协议的出错率都为0。

从传输速率上看,只有部分依赖协议的速率较高,其他3种协议的速率相当,但总体来说速率较低。

从传输隐蔽性上看,只有完全独立协议的隐蔽性最好。在实验中,当独立协议隐蔽通道开始传输后,即便将服务器关闭(正常信道切断),隐蔽传输仍可继续进行并完成。

从占用共享文件资源上看,可靠协议与不可靠协议只需要1个共享文件就可以进行隐蔽传输,需要的条件最低;部分依赖协议至少需要2个共享文件;完全独立协议至少需要3个共享文件,需要的共享文件条件最高。

从共享文件数目与传输速率的变化规律看,两种协议的平均速率都随共享文件数目的增加而缓慢增大,当共享文件达到7个时,传输160 b大小的部分依赖协议达到1.675 bps,与其在共享文件为4个的情况下速率1.467 bps相差并不大,并且随着共享文件数目的进一步增加,隐蔽通道被察觉的可能性也不断增大,因此共享文件数目对该类隐蔽通道的传输速率影响并不大。

根据上述实验数据,结合4种协议的设计分析,对基于共享文件的4种协议的特点进行对比总结,如表3所示。

4 结语

通过上述设计和实验,得出该类隐蔽通道的特点如下。

- 1) 传输速率低,性能较低,总体威胁性小。
- 2) 传输可靠性高,出错率较低。
- 3) 独立协议的传输隐蔽性较高,可能持续时间较长,独立性较好,威胁性相对较大;其他协议的传输隐蔽性较低,可能持续时间较短,独立性较差,威胁性相对较小。

(上接第69页)

- [7] LIMA L, MEDARD M, BARROS J. Random linear network coding: A free cypher? [C]// Proceedings of the IEEE International Symposium on Information Theory. Washington, DC: IEEE Computer Society, 2007: 546–550.
- [8] LIMA L, VILELA J P, BARROS J. An information-theoretic cryptanalysis of network coding — is protecting the code enough? [C]// Proceedings of the International Symposium on Information Theory and its Applications. Washington, DC: IEEE Computer Society, 2008: 1–6.
- [9] VILELA J P, LIMA L, BARROS J. Lightweight security for network coding [C]// ICC 2008: Proceedings of the IEEE International Conference on Communications. Washington, DC: IEEE Computer

总体来说,该种网络隐蔽通道在所设置的情景模式下的建立相对较为容易,然而由于其传输速率总体较低,所以对涉密文件的隐蔽性威胁不大。但是由于存在形成完全独立于服务器的、隐蔽性较高的、传输持续时间较长的隐蔽通道的可能,而这种协议下的隐蔽通道在其共享文件达到一定数目后其传输速率也有一定提高,并且,对于隐蔽定时通道目前尚没有一个系统的标识方法^[11],因而其带来的威胁性依然需要引起足够的重视。

表3 4种协议传输性能对比

比较参数	协议			
	可靠协议	不可靠协议	部分依赖协议	完全独立协议
共享文件要求数目	=1	=1	≥ 2	≥ 3
传输速率	低	低	略高	低
传输可靠性	高	高	高	高
隐蔽性	弱	弱	弱	强
对正常信道的依赖性	强	强	强	弱
共享文件数目对传输速率的影响	—	—	小	小

参考文献:

- [1] 张新宇,卿斯汉,马恒太,等.特洛伊木马隐藏技术研究[J].通信学报,2004,25(7):153–159.
- [2] Department of Defense, Computer Security Center. Trusted computer system evaluation criteria [S], 1985.
- [3] BELL D E, LAPADULA L J. Secure computer systems: Mathematical foundations and model, MTR-2547 [R]. Bedford: The MITRE Corporation, 1973.
- [4] 李涛,张凯泽,徐敏.基于FTP协议的隐蔽通道的研究与实现[J].科技风,2008(20):30–30.
- [5] 张念,杨木清.ICMP协议中隐蔽通道的设计与实现[J].网络通讯及安全,2008,2(10):61–63.
- [6] 卢大航.基于网络协议的隐蔽通道研究与实现[J].计算机工程与应用,2003,39(2):183–186.
- [7] 郭浩然,王振兴,王倩,等.基于IPv6报头的隐蔽通道分析与防范[J].计算机工程,2009,35(14):160–162.
- [8] 鞠时光,王昌达.隐通道的仿真分析[J].系统仿真学报,2006,18(6):1488–1492.
- [9] TSAI C R, GLIGOR V D, CHANDERSEKARAN C S. A formal method for the identification of covert storage channels in source code [J]. IEEE Transactions on Software Engineering, 1990, 16(6): 569–580.
- [10] 李丽萍,王建华.网络传输中采用隐蔽通道实现秘密通信[J].计算机科学,2009,36(5):115–117.
- [11] 卿斯汉.高安全等级安全操作系统的隐蔽通道分析[J].软件学报,2004,15(12):1837–1849.

- Society, 2008: 1750–1754.
- [10] LIMA L, BARROS J, MEDARD M. Towards secure multiresolution network coding [C]// ITW 2009: IEEE Information Theory Workshop on Networking and Information Theory. Washington, DC: IEEE Computer Society, 2009: 125–129.
- [11] WANG S Y, LAIH C S. Efficient key distribution for access control in pay-TV systems [J]. IEEE Transactions on Multimedia, 2008, 10(3): 480–492.
- [12] TOSUN A S, FENG W C. Efficient multi-layer coding and encryption of MPEG video streams [C]// ICME 2000: 2000 IEEE International Conference on Multimedia and Expo. Washington, DC: IEEE Computer Society, 2000: 119–122.