西安电子科技大学学报 2009, 36(4) 696-701 DOI: ISSN: ISSN 1001-2400 CN: 61-1076/TN

本期目录 | 下期目录 | 过刊浏览 | 高级检索 [打印本页] [关闭]

论文

一种防窃听的随机网络编码

周业军;李晖;马建峰

(西安电子科技大学 计算机网络与信息安全教育部重点实验室，陕西 西安 710071)

摘要：

针对应用随机网络编码进行文件传输时的安全问题，提出了一种防窃听的网络编码算法．应用该算法，窃听者得不到关于信源的任何有意义的信息，称之为弱安全．该算法通过舍弃少量带宽使得随机网络编码能以很高的概率达到弱安全性的要求．另外，当信源和信宿共享有秘密信道时，秘密信道编码算法达到弱安全性要求的概率为1，且能达到网络的最大流．该编码算法仅是在原随机编码体制的基础上对信源和信宿进行了改变，中间节点编码保持不变．

关键词： 网络编码 窃听 网络安全

Random network coding against the eavesdropping adversaries

(Ministry of Education Key Lab. of Computer Network and Information Security, Xidian Univ., Xi'an 710071， China)

(Ministry of Education Key Lab. of Computer Network and Information Security, Xidian Univ., Xi'an 710071， China)

Abstract:

An algorithm against eavesdropping adversaries is presented. By means of this algorithm an eavesdropper is unable to get any meaningful information about the source, which we call practical security. We show that if we give up a small amount of overall capacity, then a random code achieves the practically secure condition at a much higher probability. When there is a low rate secret channel between the source and destination, the shared secret algorithm not only achieves the max-flow but also the practically secure condition at a probability of one. Furthermore, implementing the algorithm involves only a slight modification of the source and destination with the operations at the intermediate nodes remaining unchanged.

Keywords: network coding eavesdropping network security

收稿日期 2008-10-28 修回日期 2008-12-31 网络版发布日期 2009-07-01

DOI:

基金项目:

国家自然科学基金资助(60772136;60633020);863国家高技术研究发展计划资助(2007AA01Z435;2007AA01Z429);广西信息与通讯技术重点实验室资助

通讯作者: 周业军

作者简介:

参考文献：

［1］Ahlswede R, Cai N, Li S-Y R, et al. Network Information Flow ［J］. IEEE Trans on Inf Theory, 2000, 46(4): 1204-1216.
［2］Li S-Y R, Yeung R W, Cai N. Linear Network Coding ［J］. IEEE Trans on Inf Theory, 2003, 49(2): 371-381.
［3］Ho T, Koetter R, Medard M, et al. The Benefits of Coding Over Routing in a Randomized Setting ［C］//IEEE Intl Symp Inf Theory. Yokohama: IEEE Press, 2003: 442.
［4］Ho T, Medard M, Shi J, et al. On Randomized Network Coding ［EB/OL］. ［2007-06-08］. http://web.mit.edu/people/medard/allerton3.pdf.

扩展功能
本文信息
Supporting info
PDF(542KB)
[HTML全文](1KB)
参考文献[PDF]
参考文献
服务与反馈
把本文推荐给朋友
加入我的书架
加入引用管理器
引用本文
Email Alert
文章反馈
浏览反馈信息
本文关键词相关文章
▸ 网络编码
▸ 窃听
▸ 网络安全
本文作者相关文章
▸ 周业军
▸ 李晖
▸ 马建峰
PubMed
Article by Zhou,Y.J
Article by Li,h
Article by Ma,J.F

［5］王静, 刘景美, 王新梅, 等. 一种网络编码的多播路由算法 ［J］. 西安电子科技大学学报, 2008, 35(1): 71-75.
Wang Jing, Liu Jingmei, Wang Xinmei, et al. Multicast Routing Algorithm for Network Coding ［J］. Journal of Xidian University, 2008, 35 (1): 71-75.

［6］Ho T C, Leong B, Koetter R, et al. Byzantine Modification Detection in Multicast Networks Using Randomized Network Coding ［C］//IEEE Intl Symp Inf Theory. Chicago: IEEE Press, 2004: 144.

［7］Jaggi S, Langberg M, Katti S. Resilient Network Coding in the Presence of Byzantine Adversaries ［C］//26th IEEE International Conference on Computer Communications. Anchorage: IEEE Press, 2007: 616 - 624.

［8］Nutman L, Langberg M. Adversarial Models and Resilient Schemes for Network Coding ［C］//IEEE Intl Symp Inf Theory. Toronto: IEEE Press, 2008: 171-175.

［9］Cai N, Yeung R W. Network Coding and Error Correction ［C］//IEEE Inform Theory Workshop. Bangalore: IEEE Press, 2002: 119-122.

［10］Zhang Z. Network Error Correction Coding in Packetized Networks ［C］//IEEE Information Theory Workshop. Chengdu: IEEE Press, 2006: 433-437.

［11］Zhang Z. Linear Network Error Correction Codes in Packet Networks ［J］. IEEE Trans on Inf Theory, 2008, 54(1): 209-218.

［12］孙岳, 杨远, 王新梅. 基于网络编码的多播网络故障恢复［J］. 西安电子科技大学学报, 2007, 34(1): 122-125.
Sun Yue, Yang Yuan, Wang Xinmei. Multicast Fault Recovery on Network Coding ［J］. Journal of Xidian University, 2007, 34(1): 122-125.

［13］Cai N, Yeung R W. Secure Network Coding ［C］//IEEE Intl Symp Inf Theory. Lausanne: IEEE Press, 2002: 323.

［14］Feldman J, Malkin T, Stein C, et al. On the Capacity of Secure Network Coding ［EB/OL］. ［2007-06-08］. http://people.csail.mit.edu/jonfeld/pubs/sflow_Allerton04_final.pdf.

［15］Chanl T, Grant A. Capacity Bounds for Secure Network Coding ［C］//Communication Theory Workshop. Australian: IEEE Press, 2008: 95-100.

［16］Rouayheb S Y E, Soljanin E. On Wiretap Network II ［C］//IEEE Intl Symp Inf Theory. Nice: IEEE Press, 2007: 551-555.

［17］Silva D, Kschischang F R. Security for Wiretap Networks Via Rank-Metric Codes ［C］//IEEE Intl Symp Inf Theory. Toronto: IEEE Press, 2008: 176-180.

［18］Bhattad K, Narayanan K R. Weakly Secure Network Coding ［EB/OL］. ［2007-05-22］. http://netcod.org/papers/06Bhattad N-final.pdf.

［19］Silva D, Kschischang F R. Universal Secure Network Coding Via Rank-Metric Codes ［EB/OL］. ［2008-11-10］. http://arxiv.org/PS_cache/arxiv/pdf/0809/0809.3546v1.pdf.

［20］Jain K. Security Based on Network Topology Against the Wiretapping Attack ［J］. IEEE Wireless Communications, 2004, 11(1): 68-71.

［21］Vilela J P, Lima L, Barros J. Lightweight Security for Network Coding ［C］//Proc of the IEEE International Conference on Communications (ICC). Beijing: IEEE Press, 2008: 1750-1754.

［22］Lima L, Medard M, Barros J. Random Linear Network Coding: a Free Cipher? ［C］//IEEE Intl Symp Inf Theory. Nice: IEEE Press, 2007: 546-550.

本刊中的类似文章

1．暂时无作者信息.基于葱头路由技术和MPLS的隐匿通信模型[J]. 西安电子科技大学学报, 2002,29(4): 513-518

2．林国庆;王新梅 .利用多线程技术改造Snort系统
[J]. 西安电子科技大学学报, 2007,34(6): 887-894

3．王静1;刘景美1;王新梅1;袁荣亮2;刘向阳3 .一种网络编码的多播路由算法
[J]. 西安电子科技大学学报, 2008,35(1): 71-75

4．周华;孟相如;张立;乔向东 .分布式入侵容忍系统的主动恢复算法研究
[J]. 西安电子科技大学学报, 2009,36(2): 378-384

5．暂时无作者信息.基于神经网络的入侵检测系统模型[J]. 西安电子科技大学学报, 1999,26(5): 667-671

6．赵福祥;王育民;赵红云.采用前向安全数字签字的移动代理设计与实现[J]. 西安电子科技大学学报, 2001,28(4): 413-417

7．赵福祥;王常杰;王育民.一个新的隐蔽网络实现方案及应用[J]. 西安电子科技大学学报, 2001,28(1): 31-35

8．赵福祥;赵红云;王育民.基于多帐户的分区电子代理银行支付系统[J]. 西安电子科技大学学报, 2001,28(3): 319-324

9．吕锡香;杨波;裴昌幸;苏晓龙.基于数据挖掘的入侵检测系统检测引擎的设计[J]. 西安电子科技大学学报, 2004,31(4): 574-580

10．张运凯(1;2);马建峰(1);王方伟(2);王长广(2).一种基于防火墙的蠕虫传播与控制模型[J]. 西安电子科技大学学报, 2006,33(1): 33-367

11．孙岳;杨远;王新梅 .基于网络编码的多播网络故障恢复
[J]. 西安电子科技大学学报, 2007,34(1): 122-125

12．詹阳1;庞辽军1;朱晓妍1;王育民2 .一种分布式自治信任计算模型
[J]. 西安电子科技大学学报, 2008,35(3): 469-473

13．史琰;盛敏 .宽带无线接入网中一种编码调度算法研究[J]. 西安电子科技大学学报, 2008,35(3): 388-394

14．吕凌;于宏毅;郭金淮 .基于MAP映射算法的物理层网络编码性能分析[J]. 西安电子科技大学学报, 2007,34(7): 55-58

文章评论

序号	时间	反馈人	邮箱	标题	内容
1	2009-10-21	caragon	caragon@googlemail.com		????????????????????????????????₤????????????????f???ugg ukugg saleugg bootsUGG Bailey Buttonsupra shoesnike dunkMBT Shoes discountugg sale ugg shoes ugg