研究与开发

安全的物理层网络编码的研究*

刘外喜,胡　晓,唐　冬,郑　晖
(广州大学电子信息工程系　广州 510006)

摘 要　无线信道的广播特性使得其中的碰撞现象普遍存在，充分利用这一特性的物理层网络编码可较大幅度地提高系统吞吐量,但也存在其特有的安全隐患。本文的主要贡献:从物理层网络编码的原理出发,挖掘了其中存在的必要前提破坏、信号强度攻击、信号能量攻击等安全隐患,并提出了应对的基本思路;综述了物理层网络编码的研究现状,并展望了未来的研究方向;提出了结合利用云计算和网络编码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的概念。

关键词　物理层网络编码;网络安全;云计算

1　引言

2000 年，蔡宁和李硕彦等人正式提出网络编码[1,2](network coding,NC)的概念,日益受到人们的关注,其中心思想是: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，可广泛应用于 Ad Hoc 网络[3]、传感器网络[4]、P2P 内容分发[5]和网络安全[6]等领域。同时,Zhang Shengli[7]以及 Katti S[8]等人从不同的角度将蔡和杨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。

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,而著名的短板理论表明整个系统的安全是由其最薄弱的部分来决定的。本文将从物理层网络编码的基本原理着手,分析这一技术存在的安全隐患,也给出了应对的基本思路,最后对网络编码的未来发展方向进行了展望。

2　物理层网络编码的基本原理

所谓物理层网络编码(physical-layer network coding,PLNC)[7]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等方式的编码运算。参考文献[9]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

*　国家自然科学基金广东联合基金重点资助项目(No.U0735002),国家“863”计划基金资助项目(No.2007AA01Z449),国家自然科学基金资助项目(No.60970146),广东省科技计划资助项目(No.2009B060700124)

层网络编码主要有参考文献[7]和[8]所提出的两种思想，参考文献[7]采用 DF，而参考文献[8]采用 AF。

在参考文献[7]中，如图 1 所示，以经典的 2 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。$X1$、$X2$、$X3$ 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：

$$r_2(t)=s_1(t)+s_3(t)$$
$$=[a_1\cos(\omega t)+b_1\sin(\omega t)]+[a_3\cos(\omega t)+b_3\sin(\omega t)](a_1+a_3)\cos(\omega t)$$
$$+(b_1+b_3)\sin(\omega t) \quad (1)$$

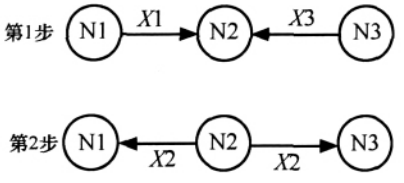

图 1　物理层网络编码模型

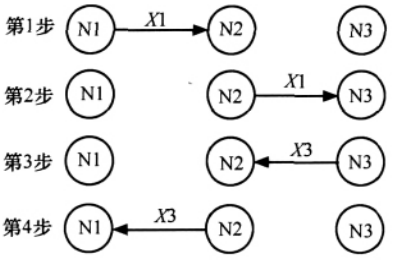

图 2　传统机制模型

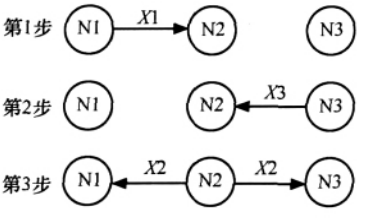

图 3　网络层网络编码模型

物理层网络编码过程如下：节点 2 在收到 $s_1(t)$、$s_3(t)$ 后，把 $r_2(t)$ 广播到节点 1、3，由于节点 1 已知参数 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。通过以上分析可知，物理层网络编码和网络层网络编码实现的方法是不一样的，但它们都完成同样的功能（即 $X2=X1\oplus X3$），存在一个映射关系。但是在性能上，如图 1~3 所示，只要第 2 步的物理层网络编码相对于需要第 4 步的传统的机制和需要第 3 步的网络层网络编码，它的吞吐量上分别有 100%和 50%的提高。

3　物理层网络编码的相关研究工作

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，这一特性帮助我们获得一些通信方式的变化，并能改善通信性能，但这一特性的存在也导致了无线网络中出现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解调和解码造成的干扰，尽力采取各种办法避免冲突的发生。但冲突并不总是有坏处的，对于无线通信网络来说，无线信道的广播特性为网络编码的应用提供了有利条件。

物理层网络编码的出现，可以把冲突充分地利用起来帮助提高通信的性能。在参考文献[7]中，对于同时接收到的相互叠加的电磁波，中继节点将其映射为相应数据比特的异或（进行了网络编码）。研究表明，在高斯白噪声信道中，物理层网络编码能够带来明显的吞吐增益。物理层网络编码不仅体现了网络编码对数据进行合并的思想，同时又考虑了物理层因素，与传统的网络编码技术相比，系统获得了更大的吞吐增益[7,10,11]。

目前，通过物理层网络编码将无线网络的冲突利用起来而改善系统性能的研究有以下两个热点[12]：

- 基于物理层网络编码机制的碰撞淘汰（collision-cancellation）方法的研究。参考文献[13]提出 ZigZag 解码算法是一个独立调制机制，它可以在 IEEE 802.11 环境中实现对多对冲突的报文进行解码，并且它的联合速率（R，R）在容量区域范围之外还可以工作，参考文献[14]中有类似的思想。参考文献[15]提出的 VWID（variable WIDth channels）可实现每个节点吞吐量 30%~110%的提高。
- 基于物理层网络编码机制的联合编码的研究。主要有物理层网络编码和分布信源编码的联合[12]以及物理层网络编码和信道编码的联合[16]。对于后者，在参考文献[16]和[17]中，作者提出将物理层网络编码与 LDPC 或 Lattice 以前后逐个的方式进行联合编码，双向中继信道的容量被证明是可以达到的；而参考文献[18]则提出将物理层网络编码与信道编码以集成的方式进行联合编码，被证明性能是更好的。

同时，物理层网络编码也被当作一种调制解调技术来研究，以期望获得更好的调制解调性能，主要是研究物理

层网络编码与网络编码的映射技术，例如：参考文献[19]中提出基于 THP（tomlinson-harashima precoding）预编码技术的机制；参考文献[20]提出根据两节点相位的差异将中继站映射为不同的星座图。

在参考文献[8]中，Katti S 等人进一步拓展了物理层网络编码思想，其最大的贡献在于消除了参考文献[7]中多个约束条件：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，并指出对于超过 2 跳的无线网络，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，所以在某种意义上也提高了物理层面的机密性。参考文献[21]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防御技术的效果，范围越小越好。参考文献[8]的结论是：在内部偷听和外部偷听两种情况下，物理层网络编码可以较大地减少该范围，尤其是在内部偷听的情况下，物理层网络编码可以在整个有效区域范围内让偷听者不成功。

4 物理层网络编码中的安全问题

虽然物理层网络编码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，安全问题就是其中的一个重要方面。由于其工作在物理层，所以无线网络中普遍存在的诸如拥塞攻击、物理破坏等针对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和特殊的安全隐患。分析后发现，针对参考文献[7]所提方法的攻击隐患主要有以下几种[22]。

（1）必要前提破坏

信号之间同步、有相同的相位平移、有相同的损耗是参考文献[7]所提方法工作的必要前提，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增加噪声以及移动、删除同步码等方法来破坏同步，也可以通过改变空间的各种环境条件来改变信号传播的损耗。

（2）信号强度攻击

由参考文献[7]的原理可知，如果采取 QPSK 调制方式的话，接收点是需要通过判别相位大小来判别信息比特的，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，所以攻击者可以放大或缩小信号的幅度以达到攻击的目的，我们把这一类攻击定义为信号强度攻击。

参考文献[8]消除了参考文献[7]的约束条件，随之也消除了一些安全隐患，但也存在一些其自身特有的隐患。

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。

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

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

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

要从式（2）的合成信号中求出 $\theta[n]$、$\varphi[n]$，就必须通过式（3），其中 $D=(|y[n]|-A^2-B^2)/2AB$，所以就必须要知道 A 和 B 的值，而 A 和 B 的值可从式（4）和式（5）获得：

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

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

其中，$E[]$ 为期望值，所以，A 和 B 的值都与合成信号的 $|y[n]|^2$（就是能量）有关。

另外，节点 1 和 3 如何判断是否收到一个报文以及该报文是单个信号还是合成信号呢？在参考文献[8]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，所以能量大小成了判断的标准。

（3）信号能量攻击

从以上原理可知，参考文献[8]的方法的几个关键处都是需要用信号的能量来决定的，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，从而达到攻击的目的，这是很容易做到的，我们把这一类攻击定义为信号能量攻击[22]。

5 总体安全措施的思考

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，所以与普通的网络相比，这种情况下的攻击者只要注入很小的恶意信息就可能影响一定范围甚至是整个网络。也就是说，同样的攻击手

段,在该模式下的攻击效率更高、传染性更强。所以,在这样的网络中,构建可信网络显得更加重要。

可信网络的定义[23]:网络和用户的行为及其结果是可预期与可管理的。网络的可信性表现在如下 3 个方面:网络用户的可信,主要看网络用户的行为是否符合既定的规范,是否可预期和可管理,对网络设备和数据是否会造成破坏或毁坏;网络服务的可信,主要看网络服务器或服务程序向访问者提供的服务是否真实可靠、不带有欺骗性,对用户终端是否会带来病毒等;网络信息传输的可信性,主要看网络各节点在传输信息过程中是否忠实,不删、不改、不夹带。

如果能做到网络用户的可信,那么网络编码中的诸多安全漏洞都有可能被克服,如上文所说的必要前提破坏、信号强度攻击、信号能量攻击等,从而能够充分发挥出网络编码的诸多优点。

目前,网络用户可信主要包括两个方面的内容——网络用户的身份可信和行为可信。网络用户的身份可信是指网络用户的身份可以被准确鉴定,不被他人冒充;网络用户的行为可信是指网络用户的行为可评估、可预期、可管理,不会破坏网络设备和数据。传统的安全机制可以提供用户的授权和认证,能解决用户的身份可信问题,但并不能处理用户的行为可信问题,因此用户行为的可信是一个研究重点。

6 结束语

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,本文在深入分析物理层网络编码基本原理的基础上,重点分析了必要前提破坏、信号强度攻击、信号能量攻击等安全隐患,认为在基于物理层网络编码的通信环境中,建构可信网络是最彻底和最本质的解决思路。

在未来的研究中,要使物理层网络编码在实际中真正发挥预期的作用,还有很多工作要做,以下是值得关注的研究方向:

- 解决物理层网络编码中关于调制方式独立于编码问题,降低编码中的误码率,实现多信号的编码等来进一步提高性能;
- 如何构建实用的物理层网络编码,以及物理层网络编码与其他调制方式的映射技术;
- 基于物理层网络编码机制的碰撞淘汰机制的相关研究,如基于 VWID 等技术的有向天线、多用户识别等领域[12];
- 跨层的物理层网络编码研究,利用基于物理层网络编码的跨层信息提高无线网络的整体性能[12]。

云计算(cloud computing)[24]也是利用各节点的整体计算资源换取整个网络的服务能力,与网络编码有着异曲同工之妙。如果将网络编码与云计算结合,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,并以网络用户身份、行为可信的网络作为这一计算网络的平台,将使目前网络的服务质量得到极大的提升。

参考文献

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

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

3 Park J S, Lun D S, Soldo F, *et al*. Performance of network coding in ad hoc networks. In: The 25th Military Communications Conf (MILCOM 2006), Washington D C, USA, October 2006

4 Wang D, Zhang Q, Liu J C. Partial network coding: theory and application in continuous sensor data collection. In: The 14th IEEE Int'l Workshop on Quality of Service (IWQoS 2006), New Haven, CT, USA, June 2006

5 Wang M, Li B C. How practical is network coding. In: The 14th IEEE Int'l Workshop on Quality of Service (IWQoS 2006), New Haven, CT, USA, June 2006

6 Ho T, Leong B, Koetter R, *et al*. Byzantine modification detection in multicast networks using randomized network coding. In: The 2004 IEEE Int'l Symp on Information Theory (ISIT'04), Chicago, IL, USA, June 2004

7 Zhang Shengli, Soung Chang Liew. Hot topic: physical-layer network coding. In: Proceedings of the 12th Annual International Conference on Mobile Computing and Networking, Los Angeles, CA, USA, September 2006

8 Katti S, Gollakota S, Katabi D. Embracing wireless interference: analog network coding. In: ACM Sigcomm, Kyoto Japan, Aug 2007

9 Laneman J N, Tse D N C, Wornell G W. Cooperative diversity in wireless networks: efficient protocols and outage behavior. IEEE Trans Inf Theory, 2004, 51(12): 3 062~3 080

10 Popovski P, Yomo H. Physical network coding in two-way wireless relay channels. In: IEEE International Conference on Communication (ICC), Glasgow Scotland, June 2007

11 吕凌,于宏毅. 物理层网络编码分组的机会中继. 电子与信息学报, 2009, 3(7): 1 767~1 770

12 Hu Peng, Mohamed Ibnkahla. A survey of physical-layer network coding in wireless networks. In: 25th Biennial Symposium on Communications, Kingston Ontario Canada, May 2010

13 Gollakota S, Katabi D. ZigZag decoding: combating hidden terminals in wireless networks. In: Sigcomm'08, Seattle WA USA, August 2008

14 Katti S, et al. Symbol-level network coding for wireless mesh networks. Computer Communication Review, 2008, 38(10): 401~412

15 Gummadi R, *et al*. Interference avoidance and control. In: ACM Hotnets-VII, Calgary Canada, October 2008

16 Narayanan K, Wilson M P, Sprintson A. Joint physical layer coding and network coding for bidirectional relaying. In: Proceedings of the 45th Annual Allerton Conference on Communication, Control, and Computing, Monticello, Ill, USA, September 2007

17 Nam W, Chung S Y, Lee Y H. Capacity bounds for two-way relay channels. In: Proceedings of the International Zurich Seminar on Digital Communications (IZS'08), Zurich Germany, March 2008

18 Zhang S, Liew S C. Channel coding and decoding in a relay system operated with physical-layer network coding. IEEE Journal on Selected Areas in Communications, 2009, 27 (5): 788~796

19 Hao Y, Goeckel D, Ding Z, *et al*. Achievable rates for network coding on the exchange channel. In: Proceedings of IEEE Military Communications Conference (MILCOM'07), Orlando, FlA, USA, October 2007

20 Koike A T, Popovski P, Tarokh V. Denoising maps and constellations for wireless network coding in two-way relaying systems. In: Proceedings of IEEE Global Telecommunications Conference (GLOBECOM'08), New Orleans, LA, USA, November- December 2008

21 Lu Kejie, Fu Shengli, Qian Yi. On the security performance of physical-layer network coding. In: IEEE ICC 2008, Beijing, China, May 2008

22 Liu Waixi, Yu Shunzheng. Secure physical layer network coding: challenges and solution. In: The International Conference on Internet Technology and Applications (iTAP 2010), Wuhan, China, August 2010

23 **林闯, 彭雪海. 可信网络研究. 计算机学报**, 2005, 28(5): 751~758

24 Luis M V, Luis R M, Juan C, *et al*. A break in the clouds: toward a cloud definition. ACM Sigcomm Computer Communication Review, 2009, 39(1): 50~55

25 Zhang Shengli, Soung Chang Liew. Applying physical-layer network coding in wireless networks. EURASIP Journal on Wireless Communications and Networking, 2010

Research for Secure Physical Layer Network Coding

Liu Waixi, Hu Xiao, Tang Dong, Zheng Hui

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

Abstract Because of broadcast nature of wireless communication, collision is popular in wireless network. Utilizing the existing interference of different signals received concurrently, physical-layer network coding (PLNC) can significantly improve the throughput of system. However, there are some special security problems for PLNC at this same time. This paper contributes this following: based on analyzing how physical layer network coding to run, some security problems, such as destroying requirement, amplitude attacks, energy attacks, are digged out, and one basic solution is showed to deal with them. Up-to date related issues of PLNC schemes and future trends will be discussed. One thinking which integrate cloud computing with network coding is proposed. Its core idea is to construct one everywhere, terminal-switch, down-top, computing network.

Key words physical layer network coding, network security, cloud computing (**收稿日期**: 2010-06-23)