



协作干扰技术的提出、现状和未来展望^{*}

龙 航,王 静,张月莹,王文博

(北京邮电大学泛网无线通信教育部重点实验室 北京 100876)

摘 要:在物理层安全技术的研究中,协作干扰技术是较为特殊的一类,通过引入人为的干扰信号,降低窃听节点的接收性能,进而提升系统的保密容量。本文回顾了协作干扰技术的提出背景,总结了其研究现状,并对未来的发展前景和潜在研究点进行了展望。目前协作干扰技术的研究可以根据干扰信号的不同分为4类,也可根据窃听系统的不同分为简单和复杂场景下的自干扰和外协作干扰技术的研究。

关键词:无线通信;物理层安全;窃听信道;协作干扰

doi: 10.3969/j.issn.1000-0801.2013.01.017

Cooperative Jamming Technique: Proposal, Survey and Future

Long Hang, Wang Jing, Zhang Yueying, Wang Wenbo

(Key Laboratory of Universal Wireless Communication, Ministry of Education,
Beijing University of Posts & Telecommunications, Beijing 100876, China)

Abstract: In the research of physical layer security, cooperative jamming is a special and novel research area. The artificial jamming signal is introduced into the wire-tap system to interfere the eavesdroppers and decrease their signal-to-interference-plus-noise ratios, then the system secrecy capacity can be improved. The background and state-of-the-art of cooperative jamming were reviewed and the future potential research topics were pointed out. Currently, the artificial jamming signal can be divided into four categories. Additionally, in the research of cooperative jamming, self-jamming and introducing jamming systems are investigated with simple and complex scenarios.

Key words: wireless communication, physical layer security, wire-tap channel, cooperative jamming

1 物理层安全技术的发展和协作干扰的提出

随着无线通信技术的发展,基于物理层资源的信息安全技术已成为无线通信和信息安全两个领域的研究热点。无线通信系统物理层资源的多样性为物理层安全技术的研究提供了广阔的空间,也留下了诸多亟待解决的问题。近10年来,无线通信中的物理层技术蓬勃发展,新技术层出不穷,因此,如何充分地开发物理层资源的唯一性和保

密性,物理层安全技术的研究对其进行了深入的探索^[1-3]。

当前,物理层安全技术的基本研究思路有两个方向^[1,3]。其一,以各种窃听信道模型下的保密容量分析为基础,主要思想是如果主信道比窃听信道的可靠性更好,就可以确保在一定码率上的可靠通信。在此类研究中常采用的系统性能指标是保密容量(secretary capacity)和保密中断率(secretary outage probability)。其二,结合传统的加密思想,利用无线信道的特征来产生、管理和分发密钥,从而提高密钥管理的安全性。这一类研究是传统信息安全技术研究在

^{*} 国家科技重大专项基金资助项目(No.2013ZX03003005),国家重点基础研究发展计划(“973”计划)基金资助项目(No.2012CB316005)



物理层上的扩展。

协作干扰(cooperative jamming, CJ)技术是基于上述第一个研究方向,在物理层安全技术兴起后出现的一个分支,其基本思想是通过发送人为的噪声/干扰(artificial noise/jamming)信号,使其对窃听节点的损害大于对合法接收节点的影响,从而达到提升系统安全性的目的(如提升保密容量或窃听节点的中断率)。高斯窃听信道的保密容量表示为源节点(A)—目的节点(B)的互信息量与源节点(A)—窃听节点(E)的互信息量之差。因此,降低窃听节点接收性能也是一种提升系统安全性的方法。

如图1所示,在传统的源—目—窃听(A-B-E)信道模型下,系统保密容量的表达式 $C=[I(A;B)-I(A;E)]^+$ 即 A-B 的互信息量与 A-E 的互信息量之差。在此模型下引入协作干扰节点 J,在 A 向 B 发送信号的同时 J 发送干扰信号, B 和 E 同时接收到 J 的干扰信号,若 E 的接收性能恶化程度超过 B 的接收性能恶化程度,则协作干扰的使用提升了系统的保密容量。

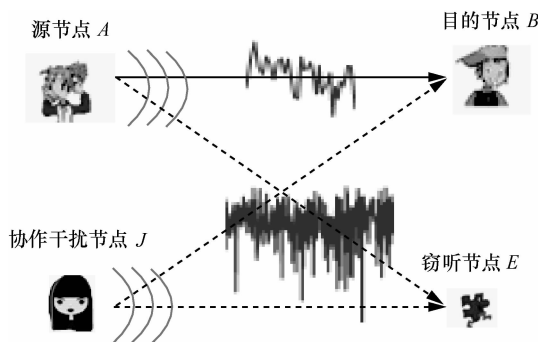


图1 协作干扰示意

协作干扰技术的提出是通信技术研究的一大突破。在传统通信系统中,干扰信号是降低系统性能的因素之一。协作干扰技术将干扰信号转变为有利于系统性能的因素,同时改变了通信系统中多个通信实体的行为,也引入了新的通信实体(协作干扰节点)。协作干扰技术丰富了物理层安全的技术手段,是新兴的物理层安全技术研究热点。

协作干扰技术的起源有两个。2005年,参考文献[4]和参考文献[5]最早提出了使用人为噪声影响窃听节点的接收。源节点装备多天线,同时发送有用信号和人为干扰信号。假设源节点已知 A-B 信道,窃听节点已知 A-B 和 A-E 的信道(因此不能用信道作为密钥)。源节点将人为干扰信号置于 A-B 信道的零空间上,因此在降低窃听节点性能的同时不影响目的节点 B 的接收。2006年,参考文献[6]提

出了协作保密(collaborative secrecy)的概念,利用空闲用户向窃听节点发送干扰信号,使其遭受的损害大于合法目的节点受的影响。

从2005年至今,协作干扰技术的研究发展已经分化出多个类别和形式。根据干扰信号的特征可以将其分为4类。除此之外,还可以根据系统的节点数量和拓扑结构将协作干扰通信系统分为简单场景和复杂场景。下面分别对各类协作干扰技术的研究现状进行总结,并指出进一步研究的若干方向。

2 协作干扰信号的分类

在现有的协作干扰技术研究中,所采用的人为干扰信号可以分为以下4类。

(1) 高斯白噪声

目的节点 B 和窃听节点 E 都将协作干扰信号作为白噪声进行处理,协作干扰同时降低了 B 和 E 的接收性能。使用这种干扰信号形式的如参考文献[7~9]等所述。

(2) 合法节点已知的信号

协作节点根据预先定义的方式产生干扰信号,目的节点 B 通过某种方式预先已知协作干扰信号,因此可以使用自干扰消除(self-interference cancellation, SIC)接收机将其从接收信号中删除,而窃听节点 E 对此未知。这种类型的协作干扰信号对 B 的接收性能没有影响,但可以降低 E 的接收性能。B 对协作干扰信号的先验已知可以通过很多不同的方式获得,例如通过安全的有线连接将干扰信号在协作干扰节点 J 和 B 之间共享^[10],或者 J 就是 B,即人为干扰信号是由目的节点发出的^[11~13],或 B 和 J 通过其他方式提前约定将使用的干扰信号形式^[14~16],或者通过传输协议设计使得 B 提前获知干扰信号形式^[11]等。

(3) 公开码书中的随机码字序列

根据一个所有节点均已知的码书,协作干扰节点使用随机 01 序列进行编码产生干扰信号,目的节点 B 和窃听节点 E 均可针对干扰信号进行译码和删除。因此,协作节点需要通过提升干扰信号的每符号信息量,使其在 E 无法译码成功而在 B 可以译码成功并从接收信号中删除。这类协作干扰信号在窃听信道保密容量分析中普遍使用,例如参考文献[6]和参考文献[17~20]等。

(4) 其他传输链路的有用信号

参考文献[21,22]提出使用相邻小区的上下行传输互为协作干扰;参考文献[23,24]中非授权用户受邀占用收费

表 1 4类人为干扰信号的优缺点对比

人为干扰信号	优点	缺点
高斯白噪声	产生简单	同样降低了合法节点的接收性能
合法节点已知的信号	对合法用户接收性能无影响	要求以某种方式通知合法节点
公开码书中的随机码字序列	若能正确解码干扰信号,则对目的节点的接收性能无影响	要求目的节点使用更复杂的 SIC 接收机;容量分析复杂
其他传输链路的有效信号	无需将发送功率分给人为干扰	需要修改多对传输链路的行为;人为干扰—信号比值可能过大

频段传输并同时充当协作干扰节点;参考文献[25]提出无线系统中的多个传输对同时进行发送,互相构成协作干扰。

根据上述协作干扰信号的分类,可以分别总结各类协作干扰信号的优缺点,见表 1。目前,第 1 类信号由于对系统保密容量性能提升有限,其相关研究也较少。而基于第 4 类干扰信号的研究相对零散,且相互间不存在紧密的联系。当前的研究主要集中于第 2 类和第 3 类干扰信号。

3 协作干扰技术的研究现状

根据窃听信道的拓扑结构,协作干扰技术的研究可以分为简单场景和复杂场景两部分。简单场景下除协作干扰节点 J 外,仅包括源节点 A 、目的节点 B 与窃听节点 E 。复杂场景下除上述节点外,还包括若干个协同中继节点 R 。

3.1 简单场景下的协作干扰

简单场景关注的是直通的源节点—目的节点($A-B$)传输对,在存在窃听节点 E 的情况下采用协作干扰技术。根据干扰信号的来源可以分为自干扰和外干扰两种情况,分别对应由 A 发送有用信号的同时也发送干扰信号和在 A 发送有用信号时引入一个外来的协作干扰节点 J 发送干扰信号。

(1)简单场景下的自干扰

此时系统中存在 3 个节点,源节点 A —目的节点 B —窃听节点 E 。 A 的发送信号中同时包括有用信号和人为干扰。当 A 装备多天线时,可以通过预编码(波束成形)技术,对有用信号和干扰信号采用不同的波束成形矢量。有用信号的波束成形矢量以增强 B 的接收性能为设计目标,干扰信号的波束成形矢量需要避开 $A-B$ 信道,集中干扰 E 的接收。

前述最早出现的协作干扰技术研究^[4,5]即可归为此类。除此之外,参考文献[26]在参考文献[4]的第一种场景基础上讨论了信号与干扰的功率分配问题。参考文献[27,28]对信道状态信息(channel state information, CSI)采用了更严格的假设。参考文献[29]研究了所有节点均有多天线, A 未知 $A-E$ 信道时,以保证 B 的信干噪比为目标的协作干扰设计。本类别的研究比较集中,其区别仅在于各节点天线

数、已知 CSI 的程度及优化目标,时间分布在 2005—2009 年,近 3 年没有更深入的研究面世。

(2)简单场景下的外协作干扰

此时系统中存在至少 4 个节点,源节点 A —目的节点 B —窃听节点 E —协作干扰节点 J 。当 A 向 B 发送信号时, J 发送干扰信号影响 E 的接收,如图 1 所示。前述参考文献[6]提出的方法即属此类。当所有节点只有单天线时,当前的研究点有特殊传输协议设计^[30](协作干扰与 DPC 的结合)、各节点间的功率分配^[14,15,31]、协作干扰节点选择^[32]、分布式协作干扰矢量设计^[32,33]等。当节点装备多天线时,除上述研究点之外,更多的研究内容集中于有用信号(A)^[34,35]和人为干扰信号(J)^[7,9,34,35]的波束成形矢量设计。

如前所述,简单场景下的自干扰技术研究已相对较为成熟,而外干扰技术的研究尚不充分。协作干扰技术研究中,相对成熟的方案设计一般是基于理想 CSI 的假设。然而,基于非理想 CSI 的方案研究对现实应用更有意义,尤其是与窃听节点 E 相关的 $CSI(A-E, J-E)$ 。例如,当节点装备多天线时, $A-E$ 和 $J-E$ 链路的传播方向与 A 和 J 的天线阵间的夹角等信息有助于获得信道的直射径分量或信道分布的相关阵等,而这些信息相比于实时的准确的信道信息更容易获得。因此,基于非理想 CSI 下的协作干扰技术研究和方案设计,是下一步研究开展的潜在方向之一。

3.2 复杂场景下的协作干扰

复杂场景下,窃听系统除源节点、目的节点、窃听节点和协作干扰节点之外,还包括若干个中继节点,同样可以分为自干扰和外干扰两类分别进行总结。

(1)复杂场景下的自干扰

此时系统模型中没有专门的协作干扰节点。系统模型一般为源节点 S —中继节点 R —目的节点 D —窃听节点 E 、 S —多 R — $D-E$ 或者双向中继系统 S_1-R-S_2-E ,干扰信号由 S 和/或 D 发出。当 D 作为干扰节点时, D 可以直接将干扰信号从接收信号中删除,因此不影响 D 的接收性能,但可以降低 E 的接收性能。

如图 2(a)所示, E 即是 R ,参考文献[11]和参考文献[36]



提出了一种简单而巧妙的协作干扰方法。第1阶段, S 向 $R(E)$ 发送信号,同时 D 向 $R(E)$ 发送人为干扰信号;第2阶段, $R(E)$ 向 D 发送混合信号,由于干扰信号由 D 发出,因此可以在接收信号中将其直接删除。

在 $S-R-D-E$ 模型中,参考文献[13]和参考文献[37~39]提出和研究了 D 和 S 轮流发送协作干扰信号的方法。如图2(b)所示,第1阶段, S 向 R 发送信号, E 窃听, D 发送人为干扰;第2阶段, R 向 D 发送信号, E 窃听, S 发送人为干扰。但是,目前中继窃听系统中的自干扰研究并不多,尤其是双向中继系统中的自干扰研究目前仍是空白。

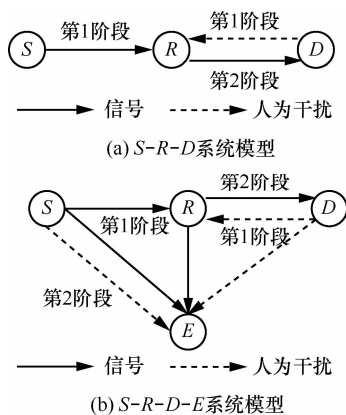


图2 中继窃听系统下的自协作干扰示意

双向中继系统中的自干扰研究可以根据关注的窃听系统的拓扑结构的不同分为如图3所示的两个场景。如图3(a)所示,双向中继系统外的窃听节点可以从两个源节点和中继节点的发送信号中进行窃听;在图3(b)中,中继节点即为窃听节点。在此类场景下,协作干扰信号可以由两个源节点发送。根据针对的双向中继协议的不同,可以分别开展2阶段和3阶段双向中继协议下的协作干扰研究。由于干扰信号和有用信号均由两个源节点发送,功率分配将是协作干扰技术研究中的关键问题。在双向中继系统的自干扰技术研究的基础上,将协作干扰技术与网络编

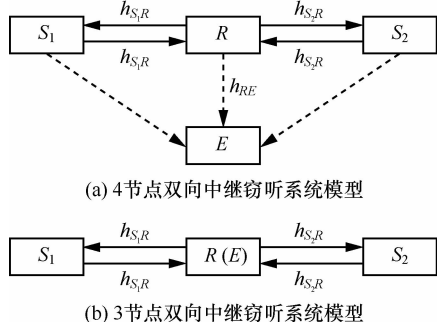


图3 双向中继窃听系统下的自协作干扰示意

码(尤其是物理层网络编码技术)结合进行研究,将具有广阔的前景。

(2)复杂场景下的外协作干扰

此类系统的典型模型是 $S-R-D-E-J$,以图4中的窃听系统为例进行说明。源节点 S 通过多个中继节点($R_1 \sim R_M$)向目的节点 D 进行传输,窃听节点 E 接收 S 和 $R_1 \sim R_M$ 的发送信号进行窃听,多个协作干扰节点($J_1 \sim J_N$)向窃听节点 E 发送人为干扰信号。多个中继节点和协作干扰节点的加入以及中继节点和协作干扰节点的角色可以相互转化,给协作干扰研究带来了极大的灵活性。此类场景下比较集中的研究点有特殊的传输协议设计^[12]、中继节点(组)选择^[8,12,40~42]、协作干扰节点(组)选择^[8,12,16,40,42]、中继转发矢量设计^[43]、协作干扰矢量设计^[12,43]等。

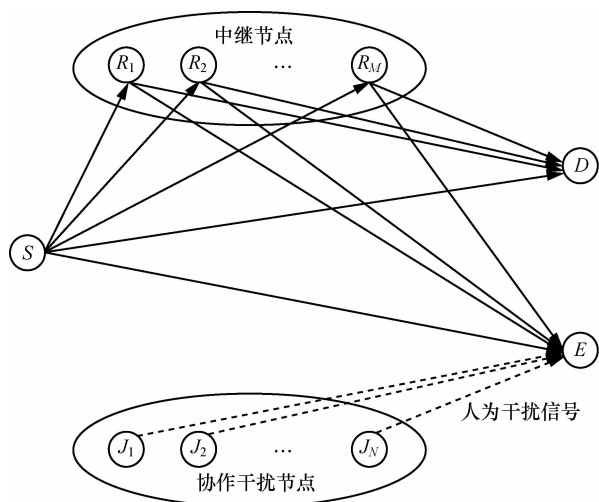


图4 多中继窃听系统中的外协作干扰示意

在复杂场景下对外协作干扰开展进一步研究,可以从以下两个方面入手。

首先,在多重中继窃听系统中,处于源节点和目的节点之间的多个节点既可以作为中继节点转发源节点的信号,也可以作为协作干扰节点发送干扰信号。研究协作节点的协作方式自适应切换(中继和协作干扰)是现有多中继窃听系统中的协作干扰技术的拓展研究方向之一。

其次,由于多个中继节点和协作干扰节点的存在,多重中继窃听系统中的协作干扰技术研究一般假设所有节点(至少是中继节点和协作干扰节点)均已知全局的完美的CSI。这样的假设在研究的初期是简单合理的选择,基于此得到的基本结论和定量结果可以作为新技术或方案研究的性能增益上限和边界。在进一步的研究中,部分CSI的假设是更为合理的选择,例如每个中继节点和协作干扰节

点仅获知与本节点相关的 CSI 或每个信道并非理想已知,考虑 CSI 的误差和节点仅知信道的分布信息等情况下的分布式协作干扰技术研究,可以作为多中继窃听系统中的外协作干扰技术研究的新方向之一。

3.3 其他应用研究

除第 3.1 节和第 3.2 节中总结的研究内容之外,协作干扰研究中还有一些较为零散的内容,主要是基于第 2 节中归纳的第 4 类干扰信号形式,即将系统中本已存在的多个传输链路置于相同的时频资源中进行传输,人为造成干扰,用以影响窃听节点的接收性能。例如,参考文献[23,24]将协作干扰与感知无线电相结合,为了提升传输的安全性,授权用户通过竞价拍卖的方法邀请其他非授权用户充当协作干扰节点。参考文献[21,22]提出使用相邻小区的信号互为协作干扰的方法,即本小区上行传输与邻小区下行传输同时进行,用邻小区基站的下行信号干扰本小区上行传输的窃听节点,达到降低窃听节点性能,提升系统保密容量的目的。

这类协作干扰研究的共同特点是并不增加额外的协作干扰源和人为的干扰信号,而是通过改变其他节点的通信行为,使正常的通信信号起到协作干扰的作用。这类研究思路都较为新奇,其缺陷在于对现有通信系统做了较大的修改,虽然通过将多个传输对集中于相同的时频资源进行传输可以达到干扰窃听端的作用,但是总体看来,带来的问题超过益处。

4 协作干扰技术的未来研究展望

根据对协作干扰技术研究现状的总结,可见中继技术、多天线技术与协作干扰技术的结合是当前的研究热点,尤其在近两年里的研究成果较为突出。但是,协作干扰技术中仍有很多研究领域尚未充分发掘。前文在描述各类协作干扰技术研究现状时,已对未来可以预见的研究方向有所阐述,归纳总结如下。

- 简单场景下的外协作研究,对 $A-E$ 和 $J-E$ 信道状态信息的不同假设下的协作干扰进行研究。
- 双向中继中的自干扰技术研究。当前的双向中继系统中的协作干扰研究集中于引入协作干扰节点后的研究,而自干扰技术的研究尚不充分。推而广之,协作干扰技术与网络编码技术的结合,也是未来可能的研究方向。
- 多中继窃听系统中,中继节点/协作干扰节点的自适应角色转换。在多中继窃听系统中,源节点与目

的节点之间的协作节点,既可以作为中继节点向目的节点转发信号,也可作为协作干扰节点向窃听节点发送干扰信号。协作节点自适应角色转换技术的研究,也是未来研究的方向之一。

- 多中继窃听系统中,基于非完美的部分信道状态的协作中继转发和协作干扰技术研究。考虑每个节点仅已知与本节点相关的信道状态信息或仅已知相关信道的分布等信息的情况,研究多节点的分布式转发和协作干扰技术,将作为未来的主要研究方向之一。

参考文献

- 1 龙航,袁广翔,王静等.物理层安全技术:研究现状与展望.电信科学,2011,27(9):60~65
- 2 吴越,易平,李建华.无线通信中物理层安全问题及其解决方案.中国通信,2011(5):11~19
- 3 杨斌.无线通信物理层安全技术研究.信息安全,2012(6):76~79
- 4 Negi R, Goel S. Secret communications using artificial noise. Proceedings of IEEE VTC Fall, Dallas, TX, USA, 2005: 1906~1910
- 5 Goel S, Negi R. Guaranteeing secrecy using artificial noise. IEEE Transactions on Wireless Communications, 2008, 7(6): 2180~2189
- 6 Tekin E, Yener A. Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy. Proceedings of Allerton Conference on Communication, Control, and Computing (ACCCC), Monticello, IL, USA, 2006
- 7 Dong L, Han Z, Petropulu A P, *et al.* Cooperative jamming for wireless physical layer security. Proceedings of IEEE Workshop on Statistical Signal Processing, Cardiff, UK, 2009: 417~420
- 8 Krikidis I, Thompson J, McLaughlin S. Relay selection for secure cooperative networks with jamming. IEEE Transactions on Wireless Communications, 2009, 8(10): 5003~5011
- 9 Dong L, Han Z, Petropulu A P, *et al.* Improving wireless physical layer security via cooperating relays. IEEE Transactions on Signal Processing, 2010, 58(3): 1875~1888
- 10 Jorgensen M L, Yanakiev B R, Kerkelund G E, *et al.* Shout to secure: physical-layer wireless security with known interference. Proceedings of IEEE Global Telecommunication Conference, Washington DC, USA, 2007: 33~38
- 11 He X, Yener A. Two-hop secure communication using an untrusted relay: a case for cooperative jamming. Proceedings of IEEE GLOBECOM, New Orleans, LA, USA, 2008: 1~5
- 12 Ding Z, Leung K K, Goeckel D L, *et al.* Opportunistic relaying for secrecy communications: cooperative jamming vs relay chatting. IEEE Transactions on Wireless Communications, 2011, 10(6): 1725~1729



- 13 Huang J, Swindlehurst A L. Secure communications via cooperative jamming in two-hop relay systems. *Proceedings of IEEE GLOBECOM*, Miami, Florida, USA, 2010: 1~5
- 14 Han Z, Marina N, Debbah M, *et al.* Physical layer security game: interaction between source, eavesdropper and friendly jammer. *EURASIP Journal on Wireless Communications and Networking*, 2009(11)
- 15 Han Z, Marina N, Debbah M, *et al.* Physical layer security game: how to date a girl with her boyfriend on the same table. *Proceedings of International Conference on Game Theory for Networks*, Istanbul, Turkey, 2009: 287~294
- 16 Zhang R, Song L, Han Z, *et al.* Distributed coalition formation of relay and friendly jammers for secure cooperative networks. *Proceedings of IEEE ICC*, Kyoto, Japan, 2011: 1~6
- 17 Tekin E, Yener A. The general Gaussian multiple access and two-way wire-tap channels: achievable rates and cooperative jamming. *IEEE Transactions on Information Theory*, 2008, 54(6): 2735~2751
- 18 Lai L, El Gamal H. The relay-eavesdropper channel: cooperation for secrecy. *IEEE Transactions on Information Theory*, 2008, 54(9): 4005~4019
- 19 Tang X, Liu R, Spasojevic P, *et al.* Interference-assisted secret communication. *IEEE Transactions on Information Theory*, 2011, 57(5): 3153~3167
- 20 Pierrot A J, Bloch M R. Strongly secure communications over the two-way wiretap channel. *IEEE Transactions on Information Forensics and Security*, 2011, 6(3): 595~605
- 21 Simeone O, Popovski P. Secure communications via cooperating base stations. *IEEE Communications Letters*, 2008, 12(3): 188~190
- 22 Popovski P, Simeone O. Wireless secrecy in cellular systems with infrastructure-aided cooperation. *IEEE Transactions on Information Forensics and Security*, 2009, 4(2): 242~256
- 23 Stanojev I, Yener A. Recruiting multi-antenna transmitters as cooperative jammers: an auction-theoretic approach. *Proceedings of Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, USA, 2011: 1106~1112
- 24 Stanojev I, Yener A. Cooperative jamming via spectrum leasing. *Proceedings of International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)*, Princeton, New Jersey, USA, 2011: 265~272
- 25 Sheikholeslami A, Goeckel D, Pishro-Nik H, *et al.* Physical layer security from inter-session interference in large wireless networks. *Proceedings of IEEE INFOCOM*, Orlando, FL, USA, 2012: 1179~1187
- 26 Zhou X, McKay M R. Physical layer security with artificial noise: secrecy capacity and optimal power allocation. *Proceedings of International Conference on Signal Processing and Communication Systems (ICSPCS)*, Omaha, NE, USA, 2009: 1~5
- 27 Khisti A, Wornell G, Wiesel A, *et al.* On the Gaussian MIMO wiretap channel. *Proceedings of IEEE International Symposium on Information Theory*, Nice, France, 2007: 2471~2475
- 28 Li Z, Trappe W, Yates R. Secret communication via multi-antenna transmission. *Proceedings of Annual Conference on Information Sciences and Systems (CISS)*, Baltimore, MD, USA, 2007: 905~910
- 29 Swindlehurst A L. Fixed SINR solutions for the MIMO wiretap channel. *Proceedings of IEEE Int Conf on Acoustic, Speech and Signal Processing (ICASSP)*, Taipei, Taiwan, 2009: 2437~2440
- 30 Krikidis I, Thompson J S, Grant P M, *et al.* Power allocation for cooperative-based jamming in wireless networks with secrecy constraints. *Proceedings of IEEE GLOBECOM Workshops*, Miami, Florida, USA, 2010: 1177~1181
- 31 Gabry F, Thobaben R, Skoglund M. Outage performance and power allocation for decode-and-forward relaying and cooperative jamming for the wiretap channel. *Proceedings of IEEE ICC Workshops*, Kyoto, Japan, 2011: 1~5
- 32 Dehghan M, Goeckel D, Ghaderi M, *et al.* Energy efficiency of cooperative jamming strategies in secure wireless networks. *IEEE Transactions on Wireless Communications*, 2012, 11(9): 3025~3029
- 33 Zheng G, Choo L C, Wong K K. Optimal cooperative jamming to enhance physical layer security using relays. *IEEE Transactions on Signal Processing*, 2011, 59(3): 1317~1322
- 34 Fakoorian S A A, Swindlehurst A L. Secrecy capacity of MISO Gaussian wiretap channel with a cooperative jammer. *Proceedings of IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, San Francisco, CA, USA, 2011: 416~420
- 35 Fakoorian S A A, Swindlehurst A L. Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer. *IEEE Transactions on Signal Processing*, 2011, 59(10): 5013~5022
- 36 Sun L, Zhang T, Li Y, *et al.* Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes. *IEEE Transactions on Vehicular Technology*, 2012, 61(8): 3801~3807
- 37 Huang J, Swindlehurst A L. Cooperation strategies for secrecy in MIMO relay networks with unknown eavesdropper CSI. *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Wuhan, China, 2011: 3424~3427
- 38 Huang J, Swindlehurst A L. Cooperative jamming for secure communications in MIMO relay networks. *IEEE Transactions on Signal Processing*, 2011, 59(10): 4871~4884
- 39 Liu Y, Petropulu A P, Poor H V. Joint decode-and-forward and jamming for wireless physical layer security with destination assistance. *Proceedings of Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, Pacific Grove, CA, USA, 2011: 109~113

一个空前弱小而且极端孤立的特殊阵营。由于这种双模组合的孤立性以及市场空间很小,并且 CDMA 运营商的主流均已确定采用 LTE FDD,因此 CDMA+TD-LTE 这种双模组合在全球已不存在其他的市场空间和推广价值,因此其产品的产业链支持必然较弱,将无法形成正常发展的产业生态系统。

CDMA 运营商本就已对弱势产业链的不利影响有切肤之痛,而 CDMA+TD-LTE 制式组合的产业链弱势将比 CDMA 更加严重,其结果必然是雪上加霜,导致技术发展滞后,设备价格昂贵,终端产品种类少、价格高、推出时间滞后,无法为用户提供良好的产品和服务,后续演进发展也将失去保障,运营商的业务经营将陷入极端困难和被动的境地。

(4) 国际漫游问题

运营商的国际漫游业务包括漫出和漫入。在移动互联网流量成为运营业务收入主流的 4G 时代,国际漫游变得越来越重要。如果一个 CDMA 运营商在 LTE 上选择了 TD-LTE,其 CDMA+TD-LTE 的覆盖区域便会成为全球覆盖上的“孤岛”。一方面,CDMA+TD-LTE 极弱的产业链必然造成适合其国际漫游的超多模终端设备的品种稀缺和支撑乏力,制约用户的漫游出国。另一方面,由于世界手机产品的主流都不支持 CDMA+TD-LTE 这种双模组合,这又使得该运营商无法承接国际漫游的漫入业务。这种局面将使运营商在全球漫游业务上陷入严重的困境,成为移动互联网时代全球化的“孤岛”和弃儿。

(5) 网络建设投资额外增加的可能性

虽然 TD-LTE 在频谱的有效利用上具有优势,但由于与 FDD 相比,TDD 只能有部分时隙用于信号发射,其上行时隙占比平均只有 FDD 的 50%,因此在频率和带宽相同、

上下行比例为 1:1 时,TD-LTE 的链路预算与 LTE FDD 相比有约 3 dB 的差距,这是 TDD 与 FDD 在覆盖上的天然差距^[5,6]。为了弥补这个覆盖差距,TD-LTE 要么必须采用 8 天线和波束成形技术(而 LTE FDD 只需要 2 天线)获得覆盖的增强,要么则必须额外建设更多的基站。对于 CDMA 运营商来说,8 天线的全面采用将需要改造(如果改造是可能的话)原有的 CDMA 站址,而不采用 8 天线则必须增加可能多达一倍的站址。不论是哪种情况,对于 CDMA 运营商来说都意味着 LTE 投资的额外增加。

必须指出,上面分析的问题,既不是 TD-LTE 的问题,也不是所有运营商选择 TD-LTE 的普遍问题,而是 CDMA 运营商选择 TD-LTE 特有的问题。

综上所述,如果一个 CDMA 运营商在 LTE 上选择 TD-LTE,将会形成通信市场和产业上一个十分弱小和孤立的特殊双模组合,可能导致技术发展滞后,网络建设投资增大,无法形成健康的产业生态环境,终端产品种类缺乏价格高昂,后续的技术演进发展缺乏保障,在业务经营和长期发展上陷入困难和被动。

参考文献

- 1 胡乐明. CDMA 运营商 Ev-Do 与 LTE 共存发展的网络演进策略. 电信科学, 2010(2)
- 2 GSA. Evolution to LTE Report, November 2012
- 3 GSA. Status of the global LTE TDD Market, November 2012
- 4 Ericsson. Ericsson Mobility Report, November 2012
- 5 龙紫薇. LTE TDD 与 LTE FDD 技术比较. http://labs.chinamobile.com/mblog/628_4871, 2008
- 6 Qualcomm. LTE TDD, the Global Solution for Unpaired Spectrum, September 2011

(收稿日期:2013-01-05)

(上接第 114 页)

- 40 Chen J, Zhang R, Song L, *et al.* Joint relay and jammer selection for secure two-way relay networks. IEEE Transactions on Information Forensics and Security, 2012, 7(1): 310~320
- 41 Goeckel D, Vasudevan S, Towsley D, *et al.* Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks. IEEE Journal on Selected Areas in Communications, 2011, 29(10): 2067~2076
- 42 Ding Z, Xu M, Lu J, *et al.* Improving wireless security for bidirectional communication scenarios. IEEE Transactions on Vehicular Technology, 2012, 61(6): 2842~2848

- 43 Guan X, Cai Y, Wang Y, *et al.* Increasing secrecy capacity via joint design of cooperative beam forming and jamming. Proceedings of IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), Toronto, ON, Canada, 2011: 1274~1278

【作者简介】 龙航,男,博士,北京邮电大学信息与通信工程学院讲师,主要研究方向为无线通信物理层技术。王静,女,北京邮电大学硕士研究生,主要研究方向为物理层安全技术。张月莹,女,北京邮电大学博士研究生,主要研究方向为无线资源管理技术。王文博,男,博士,北京邮电大学研究生院院长、教授、博士生导师,主要研究方向为无线通信与网络技术。

(收稿日期:2012-11-01)