文章编号:1004-9037(2014)03-0341-10

无线通信物理层安全方法综述

胡爱群 李古月

(东南大学信息科学与工程学院,南京,210096)

摘要:随着无线终端数目的急剧增加以及无线网络的开放性,无线通信的安全问题面临着严重的挑战。与传统加密方法不同,无线通信物理层安全方法从信息论的角度出发,旨在实现无条件安全。本文回顾了 Shannon 建立的无线通信物理层安全模型,并着重回顾了由 Wyner 引导的无密钥安全和由 Maurer 引导的基于无线信道密钥的两大物理层安全分支的发展。其中前者通过波束形成或人工噪声的方法增加合法信道和窃听信道之间的差距;后者则利用无线信道的特性,将其作为产生密钥的天然随机源。在第五代移动通信方式下,物理层安全可以实现轻量级的加解密技术,解决传统加解密延时过长的问题。然而虽然物理层安全的理论研究已日趋成熟,该领域在实际应用中仍有很多问题亟待解决。

关键词:无线保密通信; 移动信道; 时分多址; 人工复用; 密钥生成

中图分类号:TN918.82 **文献标识码**:A

Physical Layer Security in Wireless Communication: Survey

Hu Aiqun, *Li Guyue*

(School of Information Science and Engineering, Southeast University, Nanjing, 210096, China)

Abstract: With the rapid increase of wireless devices and the openness of wireless communication, the security problem becomes more and more serious and challenging. Different from traditional key-based cryptography schemes, physical layer security has been proposed to realize unconditional security from the information theory perspective. This paper provides a review of the model of physical layer security built by Shannon and tracks the evolution of security schemes without key leaded by Wyner and secret key-based secrecy schemes leaded by Maurer. Among them, the former aims at widening the channel quality gap between the authorized user and the eavesdropper; while the latter using the wireless channel as a nature random source exploiting the channel characteristics. In the coming fifth generation mobile communication scheme, physical layer security can match it with a lightweight security technology which avoids the long delay in the traditional cryptography. Although the theoretical studies of physical layer security have become maturity, they still face many practical problems to be solved in practical.

Key words: wireless communication security; mobile channel; time division duplex; artificial noise; key generation

引 言

随着科技的发展,无线通信设备急剧增加,各种新型的无线通信网络也正在逐步走向成熟。随着无线网络用户的急剧增加以及无线网络应用范围的不断增大,人们对无线通信的安全性深感忧虑。而无线通信系统中传输媒介的开放性、无线终端的移动性和网络结构的不稳定性也使得传输的可靠性和安全性面临着严峻的考验。传统安全方

基金项目:国家重点基础研究发展计划("九七三"计划)(2013CB338003)资助项目;欧盟第七框架国际合作项目"环境友好的物联网可靠性及安全性研究"资助项目。

收稿日期:2012-05-23;**修订日期**:2013-05-20

案是在网络层通过公私密钥对数据进行加密,往往以牺牲复杂度换取安全性[1-2]。然而在目前正在推广使用的 LTE/4G 甚至在正在完善的 5G 标准中,高的数据传输速率对加解密实时性、复杂度和延时等提出了更加严格的要求。另外,无线传感器网络(Wireless sensor network, WSN)及无线自组织网络(Mobile Ad hoc networks, MANET)等新型网络目前在军事和民用中都得到了广泛的使用。然而这些新型网络中的各个节点通常以电池供电,无法负担传统的加解密算法的功率与成本的开销。此外,传统的加密算法大多基于现有的计算机无法在短时间内对其进行破解。随着拥有迅速执行巨量复杂的因数分解能力的量子计算机的出现,很多传统的加密方法将不再可靠。

与此同时,如何利用无线信道的本质传输特性将原本不利的因素转化成用于维护传输的安全性的方法得到了国内外的广泛关注。作为上层加密方法的一种补充或代替,物理层安全利用信道的多径、互易性、空间唯一性等特征在底层提高无线通信系统的安全性。物理层安全的本质就在于利用信道的噪声和多径特性的不确定性来加密发送信息,使得窃听者获得发送信号的信息量趋向于零。物理层安全的理论基础是 Shannon 建立的物理层安全模型[3]。该模型下的安全是从信息论角度下严格意义上的绝对安全,要求密文数据和明文数据相互独立。然而该结论是一种悲观的结果,因为加密密钥至少达到"一次一密"时才能够达到绝对安全。Wyner 引入了窃听信道的模型[4],表明当窃听者的信道是合法接收者的退化信道时,存在某种方法在保证不泄露给窃听者任何信息的条件下,最大化发送者到合法接收者的传输速率。在 Wyner 模型的启发下,很多文献提出在先验的信道状态信息(Channel state information,CSI)的帮助下设计预编码矩阵的无密钥安全方案。其出发点是利用无线信道以及噪声内在的随机性使得合法接收者的信道优于窃听者来限制非法接收者获得的信息量。然而在文献[5]中,Maurer 认为 Wyner 的退化窃听信道假设未必合理,并最先提出了一种当窃听者的信道优于合法接收者时仍可以进行安全通信的方法。该方法的核心在于让合法通信双方通过公共信道和无差错的反馈信道通信共同产生一组安全密钥。此后,基于信息论安全的物理层安全的研究发展为两条主线[6]:由 Wyner 引导的无密钥安全和由 Shannon 和 Maurer 引导的无线密钥安全机制。

1 安全容量

在以上两个领域的研究中,无线信道安全容量的分析是物理层安全的研究基础。物理层安全的安全容量决定了合法接收端可以正确接收而窃听者却无法获取的信息的最大可达通信速率,以及通信网络能提供的服务质量的高低。图 1 描述了物理层安全的基本模型,其中 Alice 代表发送端,Bob 代表接收端,而 Eve 代表窃听端。

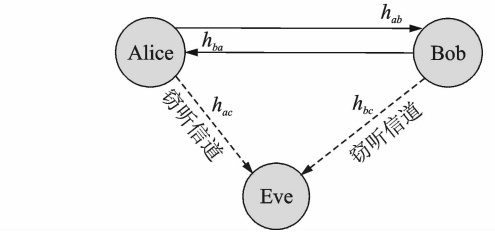

图 1 物理层安全基本模型

Fig. 1 Basic model of physical layer security

1.1 无密钥安全系统下的容量

无密钥安全方案的出发点是合法接收者的信道条件优于窃听者的信道。该模型下的安全容量可以描述为

$$C_S = C_M - C_E \tag{1}$$

式中,C_M 和 C_E 分别为合法接收者和窃听者的信道容量。在衰落信道中,合法接收者和窃听者的信道容量分别为

$$\begin{cases} C_M = \log_2(1+\gamma_M) \\ C_E = \log_2(1+\gamma_E) \end{cases} \tag{2}$$

式中:γ_M 和 γ_E 分别为合法接收信道和窃听信道的信噪比。因此,如果发送端可以获取合法接收者和窃听者完整的信道状态信息,就存在某种方法达到上述的安全容量。在频分双工(Frequency division duplex,FDD)系统中,发送端可以通过接收端的反馈而获得信道状态信息,而在时分双工(Time division duplex,TDD)系统中发送端利用上下行信道的短时互易性获取 CSI。尽管 CSI 的估计非常容易受到天线等硬件设备的影响,获得完美的 CSI 是不现实的,但该假设下的研究指出了系统性能的上界。

Carleial 和 Hellman[7]研究了二进制对称窃听信道的安全容量,Barros 等[8]分析了慢衰落窃听信道的终端安全速率,并指出在窃听信道的信道状况优于合法接收信道的信道状况下,仍可实现保密通信,而 Li 等[9]分析了合法信道为加性高斯白噪声

信道(Additive white Guassian noise，AWGN)，窃听信道为瑞利衰落信道的安全速率。对于平稳衰落的多输入多输出(Multiple input multiple output，MIMO)信道，如果任意天线间的衰落都相互独立，那么 MIMO 系统的安全容量随着天线数的增多而增大[10]。文献[11-12]分别分析了平坦 Rayleigh 衰落信道和 Rice 平坦衰落信道存在空域相关时的系统容量，其结果表明，系统的信道容量在很大程度上会受到多径的相关性的影响。Hero 在文献[13]中设计了多种不同的空时编码在已知各个信道的 CSI 的情形下来实现保密通信。文献[14-18]对不同中继方式下窃听信道的安全容量进行了研究。

除了安全容量，控制窃听端的 SNR 的方法一定程度上可以限制窃听者的行为，但是无法实现完美的安全传输。

1.2　无线密钥共享方案下的容量

令 X 为 Alice 的发送信号，Y 为 Bob 的接收信号，而 Z 是 Eve 的接收信号，$P_{X,Y,Z}$ 为 X，Y 和 Z 的联合分布函数。d 为系统中的相干距离，超出相干距离之外的窃听者获得的信道观测值可以看作和合法双方的信道观测值之间是统计独立的。

在该模型下 Alice 和 Bob 可以从无噪公共信道中获得的最大安全容量可以描述为 $C(X;Y\,||\,Z)$，该速率的上界和下界可以表述为[4]

$$C(X;Y\,||\,Z)\leqslant \min[I(X;Y),I(X;Y\mid Z)] \tag{3}$$

$$C(X;Y\,||\,Z)\geqslant \max[I(X;Y)-I(X;Z),\ I(Y;X)-I(Y;Z)] \tag{4}$$

Ahlswede[19]对该方法进行了理论研究，表明在有一个帮助者可以提供额外的相关信息时，该方法的安全容量可以增大。Maurer 和 Wolf 随后扩展了安全共享密钥的分析，在文献[20]中考虑了存在主动窃听者的情况，并表明在该情况下，如果可以获得一致的安全密钥，那么该系统可以产生和被动窃听情况中相同速率的密钥。

基于密钥共享的物理层方法的另一突破在于利用了无线通信信道内在的互易性和随机性生成信道密钥。鉴于合法接收双方和窃听者的信道之间是相互独立的，文献[21]将接收信号相位差转化成为密钥[21]。在文献[22]中，Renna 和 Bloch 给出了 MIMO 系统模型，在输入高斯信号情况下，系统生成的安全密钥容量为

$$C_{SK}=\max_{Q_X\geqslant 0}\operatorname{logdet}(\boldsymbol{I}+\boldsymbol{H}_b\boldsymbol{Q}_X\boldsymbol{H}_b^{\mathrm{H}})-\operatorname{logdet}(\boldsymbol{I}+\boldsymbol{H}_e\boldsymbol{Q}_X\boldsymbol{H}_e^{\mathrm{H}}) \tag{5}$$

式中：$\boldsymbol{H}_b$ 和 $\boldsymbol{H}_e$ 分别表示合法接收者和窃听者与发送者之间的信道，$\boldsymbol{Q}_X$ 则表示发送信号的发送信号 X 的协方差。

2　无密钥的安全方案

无密钥的安全方案主要集中在多天线系统中对空域冗余的利用，通过对波束成形、人工噪声(Artificial noise，AN)以及中继节点的设计与功率的分配优化系统的安全容量。

2.1　波束成形

波束成形可视为一种预编码技术，其中迫零波束成形技术在 MIMO 通信系统和协作中继网络中应用非常广泛[23]，其核心思想是通过使发射信号位于非法接收者的零空间，避免信息被非目标节点接收。令波束成形向量为 $\boldsymbol{w}$，则其应当满足 $\boldsymbol{w}$ 位于 $\boldsymbol{h}_{ae}$ 的零空间内，即

$$\boldsymbol{h}_{ae}^{\mathrm{H}}\boldsymbol{w}=0 \tag{6}$$

然而，实际上窃听端的 CSI 很难精确获得，并且 CSI 的偏差对 $\boldsymbol{w}$ 的设计影响较大。文献[24]研究了多用户 MIMO 有限反馈系统中的一种收发联合波束成形的方法，该方法采用每个用户酉速率控制的方法，降低了对 CSI 的敏感性和系统的复杂度。文献[25]则研究了在仅知道部分 CSI 情况下的系统设计。文献[15]在放大转发(Amplify-and-forward，AF)、译码转发(Decode-forward，DF)、合作干扰(Cooperative jamming，CJ)3 种中继方式下，对存在一个或多个窃听者的协作通信系统的波束成形矢量进行了设计与讨论。

2.2　人工噪声

人工噪声是一种有效的增强系统安全的手段，通过对发射信号中加入适当的人工噪声，可以保证在合法接收者不受很大影响的同时对窃听者实现强干扰，从而提高用户的安全通信速率。该方法以一部分发送功率作为牺牲，人为地增大合法接收者和窃听者之间的信道条件差距，因此，即便合法接收者信道噪声大于窃听者信道，在该方法下还是可以进行安全传输。

Goel 和 Negi[26]在确知 Bob 的 CSI 的情况下，在 Alice 端产生 AN。因为该 AN 映射在 Bob 的零空间，Bob 端的接收信号不会收到 AN 的影响，而 Eve 端的信号受到了强干扰。文献[27-30]分别讨论了衰落信道、离散无记忆信道和高斯对称干扰信

道下的 AN 设计。文献[31]从服务质量(Quality of service,QoS)的角度将该方法扩展到多窃听者的情况,在安全传输速率和信噪比的约束下对人工噪声方差矩阵和波束成形矩阵进行联合优化。除了可以在发送端发送 AN,Lai 等[32]研究了模加信道下的在接收端发送 AN 的方案,表明如果 Bob 在接收的同时发送均匀分布的 AN,该信道的容量可以达到没有窃听者时的容量。在接收端发送 AN 的方案无需 Alice 与 Bob 之间的 CSI,而接收端可以将 AN 的影响减去[33]。

然而上述方案并没有考虑具体的攻击方式,考虑如图 2 所示一个单输入单输出(Single input single output,SISO)系统,Bob 端通过发送 AN 增强系统的安全速率,而 Eve 拥有两根天线。Bob 和 Eve 端的接收信号分别可以表示为

$$y(t)=h_{ab}s_1(t)+h_{bb}s_2(t)+n(t) \tag{7}$$

$$\boldsymbol{z}(t)=h_{ae}s_1(t)+h_{be}s_2(t)+e(t) \tag{8}$$

式中:$s_1(t)$ 和 $s_2(t)$ 分别为 Alice 端的发送信号和 Bob 端发送的 AN,h_{ab},h_{bb},h_{ae},h_{be} 分别表示 Alice 与 Bob 之间,Bob 的发送天线和接收天线间以及 Alice,Bob 与 Eve 之间的信道响应。当信道的 SNR 足够高,式(8)恰好可以看作基本的盲分离的瞬时线性混合模型

$$\boldsymbol{z}(t)=\boldsymbol{H}\boldsymbol{s}(t) \tag{9}$$

式中:$\boldsymbol{H}$ 是未知混合矩阵,根据盲分离算法可以找到一个分离矩阵 $\boldsymbol{W}$,重构出发送信号 $\hat{\boldsymbol{s}}(t)=[\hat{s}_1(t)\hat{s}_2(t)]^{\mathrm{H}}$

$$\hat{\boldsymbol{s}}(t)=\boldsymbol{W}\boldsymbol{z}(t)=\boldsymbol{W}\boldsymbol{H}\boldsymbol{s}(t) \tag{10}$$

为了抵抗该攻击可以设计人工噪声,可以在 AN 中适当的引入和发送信号的相关,在接收信号和重构信号与发送信号的相关性中作折衷,或使得盲分离的等效混合矩阵随着时间随机变化。

2.3 协作通信

在长距离的无线通信系统中,发送端发射功率有限,因此协作中继必不可少。尽管中继可以有效地抵御无线信道的衰落,中继节点也可能同时窃取转发的信息。中继节点对接收信号的处理方式主要有放大转发(Amplify forward)和译码转发(Decode forward)两种。AF 方式下,中继节点在收到源节点信息后,适当放大后转发目的节点;而 DF 中继方式下,中继节点对接收到的信息先进行解码,再对信号重新进行编码、调制转发目的节点。文献[14]首次对以上各种中继窃听信道模型进行了研究。文献[15]指出即便中继节点不可信,它仍然可以提高系统的安全速率。另外,在不同的中继方式下,系统的安全容量都不同。由于 AF 中继方式无需解码,窃听成功率低,相对 DF 方式可以更加有效地提高系统的安全速率。

如图 2 所示,除了传统的转发(Relay)功能,中继节点还可以作为协作干扰者(Jammer),或者在转发的同时对窃听信号发送干扰信息(Helper)。文献[16]以最大化安全容量为目标,推导出各种不同协作机制下的最佳中继信息加权向量。文献[17-18]分别讨论了多天线和双向中继协作中的物理层安全问题,结合上述的波束成形和人工噪声的方法,有效地提高无线通信系统的安全容量。

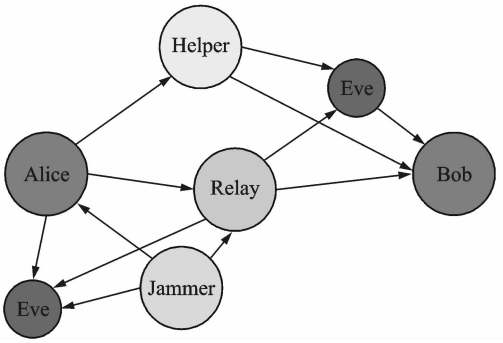

图 2 中继协作

Fig. 2 Relay cooperation

3 无线密钥共享方案

与上文的无密钥安全方案相比,无线密钥共享方案除了理论分析与仿真,众多基于实际应用的密钥生成方案也已经陆续被提出。文献[34]在移动和静止情况下实验证实了基于接收信号强度(Receive signal strength,RSS)生成的密钥生成方案的有效性。MIMO 系统可以满足高数据速率的需求,因而得到了广泛的使用。而在 MIMO 系统下无线密钥共享方案中的密钥的随机性和生成速率都有所提高,部分文献[35]试图探索 MIMO 系统下的信道密钥提取方案。然而出于空间、费用、内耗等方面的考虑,目前文献中的 MIMO 系统只是用多个网卡等分布式节点构成的虚拟 MIMO 网络,至今还没有文献在真正的 MIMO 系统上对无线共享密钥安全方案进行验证。

无线密钥共享方案的典型流程包括信道测量、量化、信息调和与隐私放大 4 个步骤[36]。而衡量一种密钥生成方法的优劣通常有 3 个标准:

(1) 密钥熵:安全方案中密钥熵的大小表明了密钥的随机性。由于信息调和与隐私放大的方法

是公开的,当密钥的随机性不够时,窃听者将更容易破解该安全方案。而 NIST 测试是国际上认可的熵测试方法。

(2) 比特错误率:该方案下的比特错误率不是传统的通信系统下的误码率,而是 Alice 和 Bob 端各自生成密钥的比特不一致。

(3) 密钥生成速率:密钥生成速率指的是在经过了隐私放大阶段丢弃了部分比特后的密钥速率,该方法与信号特征选取、测量值量化以及隐私放大的方法都息息相关。

3.1　互易性验证

移动通信 TDD 系统中,上下行采用相同频率,在无线信道中经历了相似的环境,具有短时互易性。此外,不同空间的无线信道特征是唯一的,当窃听者离合法接收者的距离超过波长的数量级时,无线信道特征将不再相关。在移动通信中,终端的移动或信道环境的变化都将引起信道的特征快速的变化,而这种无线信道的特征的变化是随机的、不可预测的。

尽管无线信道具有短时互易性,在互易性的实验中,测量值是高度相关的,但是并不完全相同。影响互易性的因素可以分为通信系统的半双工性、非对称的硬件指纹以及噪声这 3 类。文献[34]提出通过插值滤波的方法试图将测量值平移到同一个时间点,解决时间差的影响。非对称的硬件指纹是影响测量值一致性最大的因素,尤其在 MIMO 系统中,引入多天线后,天线间的差异、发送接收滤波器的不同将导致测量值相差甚远。文献[37]在频域将硬件指纹建模成为加性分量,并提出一种信道增益补偿(Channel gain compensation,CGC)的方法,统计信道先验信息,对测量值进行补偿。然而实际上硬件指纹可以表述为发送接收滤波器,简单的建模为频域加性分量未必合理。而互易性是无线密钥生成方案的基础,如何对测量值的补偿和修正至关重要。

3.2　特征提取

在信道测量环节中 RSS、时频域信道冲激响应(Channel impulse response,CIR)以及接收信号的相位、时延、包络都是典型的测量变量。这些信道特征有各自的优点和限制,RSS 和信号深衰落的方法的硬件复杂度低但获取的信息模糊[38];CIR 方法的复杂度高,但可以获取高密钥生成速率[39-42];相位、时延可以产生更高的密钥熵,可是无法确保密钥的一致性。

文献[34]利用网卡中已有的 RSSI 测试信道的 RSS 值,虽然基于 RSS 的密钥提取方法易于实现,但是该类方法只提供了无线信道的粗略信息,往往提取密钥比特速率较低。实验表明移动环境中 RSS 的值变化较大,可以产生充分的随机分布的密钥而当通信双方的环境不发生变化时,信号强度的测量值变化很小,产生的密钥信息量严重不足。文献[43-46]利用电子可控式寄生阵列散热(Electronically steerable parasitic array radiator,ESPAR)天线来动态调整发送天线的方向增益来加快接收端信号强度的测量值的变化。相比 RSS 方法,电子可控式寄生阵列散热的多载波可以提供更多信道信息,文献[47-56]在正交频分复用(Orthogonal frequency division multiplexing,OFDM)系统中通过估计 CIR,获得精细的信道信息来提高密钥比特速率。文献[56]从理论上分析比较了 RSS 和 CIR 两种信道特征,并指出由于 RSS 比 CIR 的自由度低,基于 CIR 的方法产生的共享密钥要远远高于 RSS 方案。文献[51]提出了在多径窄带信道下利用均匀分布的相位信息来生成密钥。尽管时延和相位信息的随机性更高,相位和时延在通信系统中很容易受到硬件设备的影响,难以实际应用。

在上述基于无线信道的衰落特性获取信道特征的测量值中,往往存在很大的相关性,导致生成的密钥熵值过低。在生成密钥比特前对采集到的信道测量值进行时域、频域以或空间域去相关可以增强生成密钥的随机性。文献[34]使用了离散卡洛变换(Karhunen-Loeve Transform,KLT)的方法,去除了测得的相邻的 RSS 值之间的时间相关性。文献[39]对测得的导频序列进行白化,而文献[44]则采用了跳频的方法降低相邻时间的测量数据之间的相关性。文献[48]系统中通过 DCT 变换去除时频响应中的冗余。文献[54]研究了 MIMO 下信道相关系数的时间与空间相关性,对信道向量的协方差矩阵作特征值分解消除测量值在时间和空间的相关性。

3.3　量化

在无线密钥共享方案中,测量值的量化方案既要尽可能降低密钥比特错误率,又要产生足够高速率的密钥比特。单门限的量化方法[45]是最简单的方案,量化函数为 $q(x)=\begin{cases}0 & x<L\\ 1 & x>L\end{cases}$,每个测量值可以产生 1 比特的密钥,适用于文献[35]中采用深

衰落作为信道特征的方案，并且 Alice 和 Bob 间生成的密钥一致性高。但是该方法在测量值接近门限时候量化容易出错，而且在信道变化缓慢时，生成的密钥中会出现长串的 0 和 1，随机性差。文献[57]将量化函数改为 $q(x)=\begin{cases}0 & x\leqslant L^{-}\\ 1 & x\geqslant L^{+}\end{cases}$，并将介于两门限之间的测量值丢弃。该方法下的密钥生成速率有所下降。Jana 在文献[34]中提出的 ASBG(分块使用量化器)的方法得到了广泛的认可，该方法采用自适应量化门限，$\begin{cases}q^{-}=\text{mean}-\alpha*\text{std\_deviation}\\ q^{+}=\text{mean}+\alpha*\text{std\_deviation}\end{cases}$。文献[58]在此基础上提出了自适应量化门限的方法，通过协商反复划分量化门限。文献[40]提出了多比特量化的方法，量化的比特数由 RSS 的取值范围决定 $N\leqslant|\log_2\text{Range}|$，将该范围内的值等间隔分为 2^N 个区间，并和 Gray 码一一对应。由于发生错误时 Gray 码间只有 1 比特不同，采用 Gray 码可以提高收发双方的密钥一致性。该方法生成密钥的速率高，但是量化的比特数越多，产生错误的概率就越大。文献[53]提出了带奇偶校验的多比特量化，在初始量化比特后添加一位奇偶校验位，丢弃校验错误的密钥组，并根据错误概率表来调整量化阶数。针对 OFDM 信号，文献[37]为各个子载波提出了频域量化方法。各子载波的量化比特数取决于测得的信道信息的累积分布函数 $\boldsymbol{F}(q_k)$。文献[36]从密钥长度和一致性方面比较了等概率量化、均匀量化和最小均方误差量化 3 种量化方法，并指出在实际的密钥生成过程中，等概量化是一种简单又常用的量化方案。

根据上文所述，每种量化方法都有各自的优缺点，而如何在密钥的一致性和密钥的生成速率中做出折衷仍将是下一阶段要解决的问题。

3.4 信息调和与隐私放大

信息调和环节的目的是纠正通信双方的比特串中不一致的比特的过程，使通信双方有一个共同的高度保密的比特串。然而由于 Alice 和 Bob 在公共信道进行密钥协商，协商过程中部分信息将泄露给窃听者，因而好的信息调和算法应使泄露的信息量尽可能的少。文献[39]提出一种不需要信息调和过程的前向无线密钥生成机制。该方案面向可穿戴式无线生命监护传感器网络。由于该应用背景下的无线设备资源有限，难以负担信息调和环节的高功率要求，只能舍弃信息调和环节。通过将信号用设计好的 Savitzky-Golay 滤波器滤波，该方法最终可以以 99.8%的正确率在半个小时内产生 128 个密钥比特。然而该方案下的缓慢的密钥生成速率难以满足大部分应用场景对安全的要求，因而目前信息调和的环节还是必不可少的。由 Brassard 于 1994 年提出的 Caseade 协议[59]是目前最普遍使用的信息调和方法之一。该方法要求收发双方对其量化后的比特分别分成固定长度的组，并检验每一组的校验位。当发现比特不一致时，继续分组查找，直到确定出错的比特的位置。Caseade 协议的有效性取决于划分的组的大小，如果分组太小，那么泄露到窃听者的信息量就太大，相反的如果分组太大，纠错也将更加困难。该协议在误比特率较小时，该协议能获得较大的信息率；相反误比特率高时，效率较低。Sugimoto 和 Yamazaki[60]通过在第二轮纠错后用 BICONF 基础协议来纠正剩余的错误，优化了 Caseade 协议。BICONF 基础协议的核心思想是让收发双方从量化后的比特中选择相同位置上的子比特串各自检验奇偶校验位，若不相同则通过折半查找来找寻错误比特。由于信息调和本质上也是进行纠错的过程，所以很多信息调和方法是基于纠错编码理论实现的，例如，文献[45]采用了 BCH 码，文献[61-62]采用了低密度奇偶校验码(Low density parity check code，LDPC)编码校正初始量化序列中的不匹配比特，文献[63]则采用了 Reed-Muller 码来实现信息调和。

由于在信息调和的过程中，Alice 和 Bob 泄露了部分信息给 Eve，Eve 可以根据这些信息预测出密钥的部分信息。隐私放大环节将通过舍弃一些信息调和环节已经协商好的密钥，或通过某种映射对密钥进行压缩，使得 Eve 根据已有的消息不能推断出隐私放大后的密钥的任何信息。隐私放大环节往往是以牺牲密钥的生成速率为代价的。Bennett 在文献[64]给出利用 Hash 函数，以二阶 Rayleigh 熵作为随机性的衡量标准，给出了隐私放大的完整证明。Maurer 提出了两种隐私放大的协议：基于通用 Hash 函数和提取器的隐私放大的方法。尽管隐私放大环节并不能增加原有的密钥的随机性，但是却避免了弱密钥导致加密算法出现漏洞的几率。

4 机遇与挑战

随着无线用户对移动通信带宽的需求的增加，第五代移动通信(The fifth generation mobile

communication,5G)的研究已在全球开启。目前,欧盟的 METIS 项目已经开始构建 5G 的基础框架,让用户享受极限的网络体验。其具体的技术目标为将移动数据流量增长 1 000 倍,典型用户速率提升 100 倍,数据速率达到 10 Gb/s,联网设备数量增加 100 倍,端到端时延缩短 5 倍。而尽管目前已经有众多组织和企业开始了 5G 的研发,但还没有全球统一的 5G 技术标准。同样在该技术目标下,5G 系统的安全问题也更加突出。近年来,移动支付与社交网络等应用可以在移动终端上为用户提供更加隐私和机密的任务。而 5G 将带来的更多也更加容易的通信和连接,更多的终端将连接在一起,信息泄露的风险和后果都更严重。而针对上述的 5G 的数据速率,即通信数据的一个比特需要在 0.1 ns 内完成数据的编解码和加解密和调制解调等工作。此外,车载通信等业务需要非常短的延时,否则容易造成事故。传统的分组密码算法或公私钥加密技术往往具有很高的计算复杂性和延时,加解密难以在短时间内完成,很难满足上述速率的要求。

因此,5G 的系统下需要一种在保证安全的同时,可以降低算法的复杂度、时延和功耗的轻量级加解密机制。加解密算法可分为流密码和分组密码两类。对于分组加密算法来说有数种方法可以降低硬件实现的门数:使用更小的分组长度以节省内部触发器所使用的门数。而流密码,又称序列密码,是以一个比特而非一个数据组作为基本处理单元进行处理,具有转换速度快、错误传播低的优点,硬件实现电路更简单。上文所述的基于无线信道互易性特征的密钥生成技术的密钥更新快可以满足安全性的要求。将该密钥与流加密结合,将更加适用于 5G 系统。

然而,物理层安全的技术在实际应用中还存在很多挑战。例如,在无密钥的安全方案中,当空域冗余不足时,基于人工噪声的方法将引入大量噪声,影响正常接收。而在 CSI 无法获取或估计有偏差时,该安全方案将很容易失效。同样地,在无线密钥共享方案中,若无法对信道测量值进行有效的补偿,将无法生成收发双方一致的密钥。而面对主动窃听者,物理层安全的方案往往很脆弱。这两种方案都很难抵抗在物理位置上靠近合法终端的窃听者以及对通信过程持续发送干扰的窃听者的攻击。此外,文献[65]对基于信道互异性的物理层信道特征提取密钥算法进行了脆弱性分析,并实验证明了当窃听者在已知它和合法接收者们之间的信道信息,又知道合法接收者发送的训练序列的情况下,可以重构出周围的物理环境,仿真出信道信息从而窃取密钥信息。因此,如何应对这些主动攻击者将是物理层安全方案要解决的难题。

5　结束语

本文详细综述了无线通信物理层安全方法,回顾了二十余年来由 Wyner 引导的无密钥安全以及由 Shannon 和 Maurer 引导的基于密钥的物理层安全机制的发展。无密钥安全方案主要通过对波束成形、人工噪声以及协作中继的优化设计,增大合法接收者和非法接收者信道条件的差异,从而最大化信道的安全容量。随后,本文从信道测量、测量值量化、信息调和与隐私放大 4 个方面分别讨论了无线密钥生成算法的理论依据并对比了基于各种不同信道特征的密钥的生成算法的优劣。尽管物理层安全的理论分析已经趋向成熟,然而在 CSI 的精确估计上的偏差和信道互异性的不一致导致该方法短时间内还无法得到商用。若需抵御主动窃听者的攻击,物理层安全需要和上层的安全机制适当结合,才可以更大程度上保障无线通信的安全。

参考文献:

[1] Okamoto T, Yamamoto H. Modern cryptography [M]. Japan:Sangyo-Tosho, 1997.

[2] Kasahara M,Sakai R. Cryptography [M]. Kyoritsu, 2002.

[3] Shannon C E. Communication theory of secrecy systems [J]. Bell Sys Tech Journ, 1949,28:656-715.

[4] Wyner A D. The wire-tap channel [J]. Bell Sys Tech Journ, 1975, 54:1355-1387.

[5] Maurer U. Secret key agreement by public discussion from common information[J]. IEEE Trans Inf Theory, 1993, 39(3):733-742.

[6] Mukherjee A,Fakoorian S A A,Huang J, et al. Principles of physical layer security in multiuser wireless networks: A survey [J]. ArXiv Preprint ArXiv: 2010,1011:3754.

[7] Carleial A B,Hellman M. A note on Wyner's wiretap channel [J]. IEEE Trans Inf Theory, 1977, 23(5): 625-627.

[8] Barros J,Rodrigues M R D. Secrecy capacity of wireless channels[J]. IEEE Trans Inf Theory, 2006, 24 (3): 339-348.

[9] Li Z, Yates R, Trappe W. Secret communication with a fading eavesdropper channel[C]// IEEE Inter-

national Symposium on Information Theory. Nice, France:IEEE,2007: 1296-1300.

[10] Xiao C, Wu J, Leong S Y, et al. A discrete-time model for triply selective MIMO Rayleigh fading channels [J]. IEEE Trans Wireless Commun, 2004, 3(5):1678-1688.

[11] Kermoal J P, Schumacher L, Pedersen K I. A stochastic MIMO radio channel model with experimental validation [J]. IEEE Journal on Select Areas Commun,2002(6):1211-1226.

[12] Ozcelik H,Herdin M, Weichselberger W, et al. Deficiencies of "Kronecker" MIMO radio channel model [J]. IEEE Electron Letter, 2003, 39(16): 1209-1210.

[13] Hero A. Secure space-time communication [J]. IEEE Trans Inf Theory, 2003, 49(12): 3235-3249.

[14] Oohama Y. Capacity theorems for relay channels with confidential messages[C]// IEEE International Symposium on Information Theory. Nice, France: IEEE, 2007: 926-930.

[15] He X,Yener A. Cooperation with an untrusted relay: A secrecy perspective[J]. IEEE Transactions on Information Theory, 2010, 56(8): 3807-3827.

[16] Dong L, Han Z, Petropulu A P, et al. Improving wireless physical layer security via cooperating relays [J]. IEEE Trans Signal Processing, 2010, 58(3): 1875-1888.

[17] Huang J,Swindlehurst A L. Secure communications via cooperative jamming in two-hop relay systems[C]// IEEE Global Communications Conference. Miami: IEEE, 2010: 1-5.

[18] Jeong C, Kim I M, Kim D I. Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system[J]. IEEE Trans Signal Processing, 2012, 60(1):310-325.

[19] Ahlswede R, Csisz′ar I. Common randomness in information theory and cryptography-part I: Secret sharing [J]. IEEE Trans Inf Theory, 1993, 39(4): 1121-1132.

[20] Maurer U M, Wolf S. Secret key agreement over unauthenticated channel—Part I: Definitions and bounds [J]. IEEE Trans Inf Theory, 2003, 49(4): 822-831.

[21] Koorapaty H, Hassan A A, Chennakeshu S. Secure information transmission for mobile radio [J]. IEEE Commun Letter, 2000, 4:52-55.

[22] Renna F, Bloch M, RandLaurenti N. Semi blind key agreement over MIMO fading channels [J]. IEEE Trans Commun, 2013, 61(2):620-627.

[23] Dong L, Han A Z, Poor H V. Improving wireless physical layer security via cooperating relays [J] IEEE Trans Signal Process, 2010,58(3):1875-1888.

[24] 卢敏，鄢广增. 多用户 MIMO 系统低复杂度收发联合波束成形方法[J]. 数据采集与处理，2012,27(4): 417-421.
Lu Min, Feng Guangzeng. Joint beamforming scheme with low complexity for multiuser MIMO system [J]. Journal of Data Acquisition and Processing, 2012, 27(4): 417-421.

[25] Pei Y, Liang Y C, The K C, et al. Secure communication in multiantenna cognitive radio networks with imperfect channel state information[J]. IEEE Trans Signal Processing, 2011, 59(4): 1683-1693.

[26] Goel S,Negi R. Guaranteeing secrecy using artificial noise[J]. IEEE Trans Wireless Communications, 2008, 7: 2180-2189.

[27] Zhou X, McKay M R. Secure transmission with artificial noise over fading channels:Achievable rate and optimal power allocation[J]. IEEE Trans Vehicular Technology, 2010, 59: 3831-3842.

[28] Tekin E, Yener A. The general Gaussian multiple-access and two-way wiretap channels: achievable rates and cooperative jamming[J]. IEEE Trans Inf Theory, 2008, 54: 2735-2751.

[29] Tang X, Liu R, Spasojevic P, et al. Interference assisted secret communication [J]. IEEE Trans Inf Theory, 2011, 57: 3153-3167.

[30] Zhu J, Mo J, Tao M. Cooperative secret communication with artificial noise in symmetric interference channel[J]. IEEE Communications Letters, 2010, 14: 885-887.

[31] Liao W C, Chang T H, Ma W K, et al. Joint transmit beamforming and artificial noise design for QoS discrimination inwireless downlink[C]// IEEE International Conference on Acoustics Speech and Signal Processing. Dallas, Texas, USA: IEEE, 2010: 2562-2565.

[32] Lai L E, Gamal H, Poor H V. The wiretap channel with feedback: Encryption over the channel [J]. IEEE Trans Inf Theory, 2008, 54: 5059-5067.

[33] Li W, Ghogho M, Chen B, et al. Secure communication via sending artificial noise by the receiver:outage secrecy capacityregion analysis[J]. IEEE Communications Letters, 2012, 16: 1628-1631.

[34] Patwari N J, Croft S J,Jana S, et al. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements [J]. IEEE Trans Mobile Comput, 2010, 9(1):17-30.

[35] Pawar S, Rouayheb E S, Ramchandran K. Securing dynamic distributed storage systems against eavesdropping and adversarial attacks [J]. IEEE Tran Inf Theory, 2011, 57(10):6734-6753.

[36] 蔡文炳. 基于无线信道特性生成密钥的理论限及量化方法研究[D]. 郑州:解放军信息工程大学, 2013.
Cai Wenbin. Research on theoretical limit and quantization methods in secret key generation based on characteristics of wireless channel[D]. Zhengzhou: PLA Information Engineering University, 2013.

[37] Liu H, Wang Y, Yang J, et al. Fast and practical secret key extraction by exploiting channel response [C]// IEEE INFOCOM. Turin: IEEE, 2013: 3048-3056.

[38] Babak A, Aggelos K, Alejandra M, et al. Robust key generation from signal envelopes in wireless networks[C]// Proc of ACM CCS. Alexandria:[s. n.], 2007:401-41.

[39] Ali S T, Sivaraman V, Ostry D. Zero reconciliation secret key generation for body-worn health monitoring devices[C]// Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks. New York, NY, USA: ACM, 2012: 39-50.

[40] Yasukawa S, Iwai H, Sasaoka H. A secret key agreement scheme with multi-level quantization and parity check using fluctuation of radio channel property[C]// Proc of IEEE ISIT. Toronto, Canada: IEEE,2008:732-736.

[41] Liu H, Yang J, Wang Y, et al. Collaborative secret key extraction leveraging received signal strength in mobile wireless networks[C]// Proc of IEEE INFOCOM. Orlando, FL:IEEE, 2012:927-935.

[42] Croft J, Patwari N, Sneha, et al. Robust uncorrelated bit extraction methodologies for wireless sensors [C]// Proc of ACM/IEEE IPSN. New York: IEEE, 2010:978-988.

[43] Li Z, Xu W, Miller R, et al. Securing wireless systems via lower layer enforcements[C]// Proceedings of the 5th ACM Workshop on Wireless Security. New York, NY, USA: ACM, 2006:33-42.

[44] Yao L, Ali S T, Sivaraman V, et al. Decor relating secret bit extraction via channel hopping in body area networks[C]// 2012 IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications. [S. l.]:IEEE,2012:1454-1459.

[45] Aono T, Higuchi K, Ohira T, et al. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels[J]. IEEE Trans Antennas and Propagation, 2005, 53(11): 3776-3784.

[46] Ohira T. Secret key generation exploiting antenna beam steering and wave propagation reciprocity[C]// Proc of EUMC. London, UK:[s. n.], 2005:23-27.

[47] Chou T H, Draper S, Sayeed A. Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness [C]// IEEE ISIT. Austin, Texas, USA: IEEE, 2010.

[48] Kitaura A, Sasaoka. H. A scheme of private key agreement based on the channel characteristics in OFDM land mobile radio[J]. Electronics and Communications in Japan (Part III Fundamental Electronic Science), 2005, 88(9):1-10.

[49] Hajj E. Shehadeh Y, Hogrefe D. An optimal guard-intervals based mechanism for key generation from multipath wireless channels[C]// NTMS′11. Paris, France:[s. n.], 2011:1-5.

[50] Hajj E. Shehadeh Y, Alfandi O, et al. Intelligent mechanisms for key generation from multipath wireless channels [C] // Wireless Telecommunications Symposium. New York, NY:[s. n.], 2011.

[51] Wallace J W, Sharma R K. Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis[J]. IEEE Trans Inf Forensics and Security, 2010, 5(3):381-392.

[52] Yasukawa S, Iwai H, Sasaoka H. Adaptive key generation in secret key agreement scheme based on the channel characteristics in OFDM[C]// International Symposium on Information Theory and Its Applications, ISITA. Auckland:[s. n.], 2008.

[53] Ali S, Sivaraman V, Ostry D. Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices [J]. IEEE Trans Mobile Computing, 2013(99):1.

[54] Chen C, Jensen M A. Secret key establishment using temporally and spatially correlated wireless channel coefficients [J]. IEEE Trans Mobile Computing, 2011, 10(2):205-215.

[55] Wallace J. Secure physical layer key generation schemes: Performance and information theoretic limits[C]// Proc of IEEE ICC. Bremen, Germany: IEEE, 2009:1-5.

[56] Kitano T, Kitaura A, Iwai H, et al. A private key agreement scheme based on fluctuations of BER in wireless communications[C]// The 9th International Conference on Advanced Communication Technology. Guangwon Do, Korea:[s. n.],2007:1495-1499.

[57] Mathur S, Trappe W, Mandayam N, et al. Radio-te-

lepathy:Extracting a secret key from an unauthenticated wireless channel[C]// Proceedings of the 14th ACM International Conference on Mobile Computing and Networking. San Francisco, California, USA: ACM, 2008:128-139.

[58] Kitaura A, Sumi T, Tachibana K, et al. A private key sharing scheme based on multipath time delay in UWB systems [C] // International Conference on Communication Technology. Guilin: [s. n.], 2006: 1-4.

[59] Brassard G, Salvail L. Secret-key reconciliation by public discussion[C]// Advancesin Cryptology EUROCRYPT'93. Berlin, Heidelberg: Springer, 1994: 410-423.

[60] Sugimoto T, Yamazaki K. A study on secret key reconciliation protocol[J]. IEICE Trans Fundamentals of Electronics, Communications and Computer Sciences, 2000, 83(10):1987-1991.

[61] Madiseh M G, McGuire M L, Neville S S, et al. Secret key generation and agreement in UWB communication channels[C]// IEEE Global Telecommunications Conference. [S. l.]: IEEE, 2008:1-5.

[62] Liu Y, Draper S C, Sayeed A M. Exploiting channel diversity in secret key generation from multipath fading randomness[J]. IEEE Trans Inf Forensics and Security, 2012, 7(5):1484-1497.

[63] Wilson R, Tse D, Scholtz R A. Channel identification: secret sharing using reciprocity in ultra wideband channels[J]. IEEE Trans Inf Forensics and Security, 2007, 2(3):364-375.

[64] Bennett C H, Brassard G, Crepeau C. Generalized privacy amplification [J]. IEEE Trans Inf Theory, 1995, 41(6):1915-1923.

[65] Dottling N, Lazich D, Muller-Quade J, et al. Vulnerabilities of wireless key exchange based on channel reciprocity[C]// Information Security Applications, ser. Lecture Notes in Computer Science. Jeju Island, Korea: [s. n.], 2011:24-26.

[66] Edman M, Kiayias A, Yener B. On passive inference attacks against physical-layer key extraction[C]// Proc ACM European Workshop on System Security, EUROSEC'11. New York, USA: ACM, 2011:1-8.

作者简介:胡爱群(1964-),男,教授,研究方向:通信安全、无线网络安全,E-mail:aqhu@seu.edu.cn;李古月(1989-),女,博士,研究方向:物理层安全。