物联网中一种抗大规模天线阵列窃听者的噪声注入方案

彭建华 张 帅* 许晓明 黄开枝 金 梁

(国家数字交换系统工程技术研究中心 郑州 450002)

摘 要：物联网中无线传输的安全难题是制约其发展的重要瓶颈，物联网终端受限的计算能力与硬件配置以及配备大规模天线阵列的窃听者给物理层安全技术带来了新的挑战。针对该问题，该文提出一种可对抗大规模天线阵列窃听者的轻量级噪声注入策略。首先，对所提出的噪声注入策略进行介绍，并分析了该策略的安全性；然后，基于该策略得到了系统吞吐量的闭式表达式，并对时隙分配系数和功率分配系数进行优化设计。理论和仿真结果表明，通过对物联网系统参数进行设计，所提出的噪声注入策略能够实现私密信息的安全传输。

关键词：物联网；物理层安全；噪声注入

中图分类号：TN915.08 **文献标识码**：A **文章编号**：1009-5896(2019)01-0067-07

DOI: 10.11999/JEIT180342

A Noise Injection Scheme Resistant to Massive MIMO Eavesdropper in IoT

PENG Jianhua ZHANG Shuai XU Xiaoming HUANG Kaizhi JIN Liang

(*National Digital Switching System Engineering & Technological Research Center*, *Zhengzhou* 450002, *China*)

Abstract: The security issue of wireless transmission becomes a significant bottleneck in the development of Internet of Things (IoT). The limited computing capability and hardware configuration of IoT terminals and eavesdroppers equipped with massive Multiple-Input Multiple-Output (MIMO) bring new challenges to physical layer security technology. To solve this problem, a lightweight noise injection scheme is proposed that can combat massive MIMO eavesdropper. Firstly, the proposed noise injection scheme is introduced, along with the corresponding secrecy analysis. Then, the close-formed expression of the throughput is derived based on the proposed scheme. Furthermore, the slot allocation coefficient and power allocation coefficient are optimized. The analytical and simulation results show that the proposed noise injection scheme can achieve the security of private information transmission by designing of the IoT system parameters.

Key words: Internet of Things (IoT); Physical layer security; Noise injection

1 引言

随着移动通信技术的快速发展，下一代5G移动通信系统将不仅关注人与人的通信，更要关注物与物的通信，物联网作为未来5G的重要应用场景，其应用将涉及到人们生活的方方面面[1]。然而，物联网中隐私数据保护问题却面临着严峻的挑战。包括实时位置、健康状态、个人账户等隐私信息将通过开放的无线信道进行传输，窃听者通过采集这些信息便可以直接或间接地追溯到设备使用者方方面面的信息，用户的隐私受到严重威胁。所以，解决物联网中无线数据传输的安全问题，确保终端设备中信息的安全保密，是物联网繁荣发展的前提。

传统移动通信采用密钥体制保证隐私数据的安全[2]，但受限于物联网终端自身低硬件复杂度与低信号处理能力等特点，在其上部署高复杂度的加解密算法会大大增加物联网终端的运行负担，因此基于计算复杂度的安全密钥体制很难用来保证物联网的无线通信安全。作为传统安全手段的重要补充，物理层安全利用无线信道的唯一性、互易性等特性来保证无线通信的安全，为保证物联网场景隐私数据的安全传输提供了新的思路。尽管物理层安全技术不再依赖计算复杂度，但是对于物联网场景，目前大多数物理层安全技术如波束赋形[3,4]和人工噪

收稿日期：2018-04-13；改回日期：2018-09-26；网络出版：2018-10-23
*通信作者： 张帅 2012301200229@whu.edu.cn
基金项目：国家自然科学基金(61501516, 61701538, 61601514)
Foundation Items: The National Natural Science Foundation of China (61501516, 61701538, 61601514)

声[5,6]等依旧过于复杂。考虑到物联网场景中物联网终端低硬件复杂度和低功耗等特点，文献[7]概述了适合物联网场景的物理层安全技术，文献[8,9]考虑采用协助传输和协助干扰的方式实现私密信息的安全传输。但是，以上研究大多假设窃听者配备单天线或者多天线，并没有考虑窃听者具有较强硬件配置的情况。

作为5G的关键技术，大规模天线阵列(Multiple-Input Multiple-Output, MIMO)能够有效提高频谱使用效率和能量效率，在未来有着巨大的发展潜力[10,11]。目前针对大规模MIMO场景物理层安全技术的研究大多假设合法发送方配备大规模MIMO天线，并对该场景的性能进行分析。然而，大规模MIMO技术在提高合法通信性能的同时，窃听者也可以采用该技术提高自身窃听能力。因此要实现物联网场景私密信息的安全传输，一方面要满足方案轻量级的需求，即对于单天线物联网终端，所提出的方案仅需进行一些简单的信号处理便可实现；另一方面，也要考虑方案的防窃听能力。

针对以上需求，本文从物联网终端低硬件复杂度和低功耗等特点出发，同时考虑窃听者配备大规模MIMO天线，提出了一种可以对抗大规模MIMO窃听者的轻量级噪声注入策略。本文主要贡献如下：(1)现有物理层安全研究大多基于多天线技术且需要获得完美的信道状态信息(Channel State Information, CSI)[3–6]，本文考虑物联网实际通信场景，提出了一种可对抗大规模MIMO窃听者的轻量级噪声注入策略，并对该策略每个步骤进行安全性分析。值得指出的是，本文所提出噪声注入策略仅需发送端配备单天线便可实现，且将信号处理的计算复杂度从物联网终端转移到了基站侧。(2)基于3节点通信模型，使用连接中断概率与安全中断概率对系统可靠性与安全性进行刻画，并在绝对安全约束下求出系统吞吐量的闭式解。(3)以最大化系统吞吐量为目标，在可靠性约束下对该方案的功率分配系数和时隙分配系数进行优化，为实际物联网系统提供理论指导。

本文安排如下：第2节对系统模型进行介绍；第3节详细介绍所提出的噪声注入策略，并在每个步骤进行安全性分析；第4节对系统吞吐量进行分析与优化；第5节仿真验证了理论的正确性，并与单天线On-Off策略进行比较；最后总结全文。

2 系统模型

如图1所示，考虑基于时分双工(Time Division Duplexing, TDD)的物联网系统上行通信模型。单天线物联网用户设备(User Equipment, UE)向多天线基站(Base Station, BS)发送私密信号，而配备大规模MIMO的窃听者(Eavesdropper, Eve)对私密信号进行窃听。本文考虑最坏的情况：窃听者可配备无限数量的天线。用N_{b}表示BS配备的天线数，N_{e}表示Eve配备的天线数，则N_{b}为有限的，N_{e}趋于正无穷。

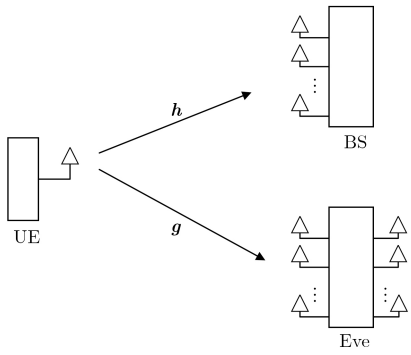

图 1 物联网上行通信模型

UE通过合法信道$\boldsymbol{h}_{\mathrm{ub}}=[h_{\mathrm{ub},1},h_{\mathrm{ub},2},\cdots,h_{\mathrm{ub},N_{\mathrm{b}}}]^{\mathrm{T}}$向BS发送私密信号，其中，$h_{\mathrm{ub},k}$表示UE到BS第$k$个天线的信道。同时，Eve通过窃听信道$\boldsymbol{h}_{\mathrm{ue}}=[h_{\mathrm{ue},1},h_{\mathrm{ue},2},\cdots,h_{\mathrm{ue},N_{\mathrm{e}}}]^{\mathrm{T}}$对私密信号进行窃听，其中，$h_{\mathrm{ue},k}$表示UE到Eve第$k$个天线的信道。假设BS和Eve的天线间距皆不小于半个波长，则以上信道都是相互独立的。同时，考虑采用瑞利块衰落信道模型刻画以上信道；即信道在相干时间T内保持恒定，在不同相干时间内相互独立，且$h_{\mathrm{UI},k}\sim\mathcal{CN}(0,1)$，$i\in(\mathrm{B},\mathrm{E})$。由于该物联网系统工作于TDD模式，因此认为上下行信道为互易的。

假设UE采用Wyner编码$\mathbb{C}\left(2^{nR_{\mathrm{B}}},2^{nR_{\mathrm{S}}},n\right)$[12]，其中$R_{\mathrm{B}}$为主信道编码速率，$R_{\mathrm{S}}$表示私密信息编码速率($R_{\mathrm{B}}\geq R_{\mathrm{S}}$)，$R_{\mathrm{B}}-R_{\mathrm{S}}$表示为保护私密信息而添加的冗余信息速率，$n$为码字的长度，$2^{nR_{\mathrm{B}}}$是码本的大小，$2^{nR_{\mathrm{B}}}$个码字随机组成$2^{nR_{\mathrm{S}}}$个私密信息码字。为了安全发送信息$w\in\left\{1,2,\cdots,2^{nR_{\mathrm{S}}}\right\}$，UE将用随机编码器在$w$位中随机选择一个码字映射为发送信息。考虑到UE计算能力和功耗的限制，考虑采用固定的编码速率$(R_{\mathrm{B}},R_{\mathrm{S}})$。

3 噪声注入策略设计

针对计算能力和功率受限的单天线UE，本节提出了一种可抵御大规模MIMO窃听者被动窃听攻击的噪声注入策略。此方案的基本思想是在UE发送的私密信号上叠加上包含合法信道信息的人工噪声。由于BS可以对合法信道进行探测，获取合法信道CSI，从而消除注入的噪声；而由于信道的空间去相关性，Eve无法获得合法信道的CSI，因此其会受到注入噪声的影响，私密信息的安全性得到

了保证。如图2所示，此噪声注入策略可分为3个步骤，接下来分别对每个步骤进行详细介绍并进行安全性分析。为了公式的简洁，本节将随机选取Eve的一根天线对其接收信号进行分析，在安全性分析时则会考虑Eve配备无限数量天线时带来的影响。

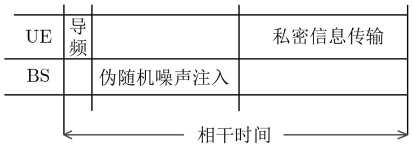

图 2 噪声注入策略时隙分配

3.1 上行信道估计与天线选择

在此阶段，UE会向BS发送一小段导频序列供BS进行信道估计，多天线BS通过导频序列可以估计出合法信号所有的CSI。由于上下行信道的互易性，BS根据估计的CSI选择出下行信道状况最好的天线，与UE进行随后的通信；同时，并将该天线处的CSI存储起来，供后续消除注入噪声使用。由于BS有着较好的硬件条件与计算能力，假设BS能够获得完美的CSI。同时，由于导频长度固定，假设整个上行信道估计和天线选择的过程所占用的时隙是固定的，相干时间内除去导频所占用的时隙，其余时隙为可分配时隙。

安全性分析：假设Eve知道导频序列的全部内容，则Eve可以根据导频序列估计出窃听信道的CSI。由于信道的空间去相关性，且合法信道CSI并没有通过无线信道进行传输，因此Eve无法获得合法信道的相关信息。

3.2 下行噪声注入

在此阶段，BS通过已选择的天线向UE广播伪随机噪声，则UE或Eve任一天线处接收到的信号可表示为

$$y_{i,1}=\sqrt{\tau P_{\mathrm{b}}}h_{\mathrm{b}i}z+n_i,i\in(\mathrm{u},\mathrm{e}) \tag{1}$$

其中，u和e分别代表UE和Eve, $z\sim\mathcal{CN}(0,1)$表示由BS发送的归一化复高斯噪声，P_{B}表示BS的平均发射功率，$n_i\sim\mathcal{CN}\left(0,\delta_i^2\right)$表示UE或Eve处的加性高斯白噪声，$\tau$表示下行噪声注入过程占整个可分配时隙比例，即时隙分配系数。

安全性分析：在此过程中，由于BS没有发送导频序列，因此即使Eve拥有多个天线可获得分集增益，仍旧无法获得信道h_{BE}，从而对噪声z进行解调。同时，窃听者在此阶段中依旧无法获得合法信道CSI的任何信息。

3.3 私密信息传输

由于下行噪声注入阶段中BS没有发送导频序列，UE也无法解调出上阶段注入的噪声z。因此在此阶段中，UE将上一阶段接收到的信号进行归一化，然后与私密信号按照一定的功率分配系数叠加在一起，作为此阶段的发送信号。发送信号可表示为

$$x=\sqrt{\alpha}s+\sqrt{1-\alpha}\,\frac{y_{\mathrm{u},1}}{|y_{\mathrm{u},1}|} \tag{2}$$

其中，s表示归一化后的私密信号且满足$\mathrm{E}\left[|s|^2\right]=1$。$\alpha\in(0,1]$表示分配给私密信号的功率比例，即功率分配系数。BS和Eve的任一天线在此阶段的接收信号可以表示为

$$\begin{aligned}y_{i,2}&=\sqrt{(1-\tau)}P_{\mathrm{u}}h_{\mathrm{u}i}x+n_i\\&=\sqrt{(1-\tau)}P_{\mathrm{u}}h_{\mathrm{u}i}\\&\quad\cdot\left(\sqrt{\alpha}s+\sqrt{1-\alpha}\,\frac{\sqrt{\tau P_{\mathrm{b}}}h_{\mathrm{bu}}z+n_{\mathrm{u}}}{\sqrt{\tau P_{\mathrm{b}}\left|h_{\mathrm{bu}}\right|^2+\delta_{\mathrm{u}}^2}}\right)\\&\quad+n_i,i\in(\mathrm{b},\mathrm{e})\end{aligned} \tag{3}$$

其中，b和e分别代表BS和Eve, P_{u}表示UE的平均发射功率，因为在上行信道估计的时间可忽略，所以此过程占可分配时隙比例为$(1-\tau)$。

安全性分析：此阶段中，如果需要消除注入的噪声，需要知道α, τ, P_{b}, h_{bu}, z, δ_{u}^2等参数。其中，BS在上行信道估计阶段可获得信道h_{bu}，且知道由自身注入伪随机噪声z和自身平均发射功率P_{b}等系数。更进一步假设α, τ, δ_{u}^2为定值，BS在私密信息传输前就能够获得这些定值，因此BS能够完美消除所注入的噪声。而对于配备有无限天线数量的Eve，即使其能够获得α, τ, δ_{u}^2等定值以及P_{b}，一方面，其无法获得随机注入的噪声z；另一方面，其很难获得合法信道的CSI，因此Eve将受到注入噪声的干扰。考虑BS处用选择出的信道状态最好的天线对信号进行接收，Eve处则采用最大比合并(Maximal Ratio Combining, MRC)策略接收信号，由式(3)可得，BS和Eve处信噪比(Signal to Noise Ratio, SNR)分别可表示为

$$\gamma_{\mathrm{b}}=\frac{\alpha\left(1-\tau\right)P_{\mathrm{u}}\left|h_{\mathrm{ub}}\right|^2}{\dfrac{\left(1-\alpha\right)\left(1-\tau\right)P_{\mathrm{u}}\left|h_{\mathrm{ub}}\right|^2}{\tau P_{\mathrm{b}}\left|h_{\mathrm{bu}}\right|^2+\delta_{\mathrm{u}}^2}\delta_{\mathrm{u}}^2+\delta_{\mathrm{b}}^2} \tag{4}$$

$$\gamma_{\mathrm{e}}=\frac{\alpha\left(1-\tau\right)P_{\mathrm{u}}\left\|\boldsymbol{h}_{\mathrm{ue}}\right\|^2}{\left(1-\alpha\right)\left(1-\tau\right)P_{\mathrm{u}}\left\|\boldsymbol{h}_{\mathrm{ue}}\right\|^2+\delta_{\mathrm{e}}^2} \tag{5}$$

其中，h_{ub}为UE到BS信道最优天线的信道，其概率分布函数可表示为$F_{h_{\mathrm{ub}}}(x)=\left(1-\mathrm{e}^{-x}\right)^{N_{\mathrm{b}}}$。$\left\|\boldsymbol{h}_{\mathrm{ue}}\right\|^2$为UE到Eve的信道，服从参数$(N_{\mathrm{e}},1)$的Gamma随机变量。

需要指出的是，物理层安全传统多天线人工噪

声策略需要发送端天线数大于窃听方天线数[13]，这是因为传统人工噪声策略在多维空间分别发送私密信号与人工噪声，当窃听者从更高的维度对信号进行窃听时，则可以将私密信号剥离开来。而对于此噪声注入策略，UE发送的信号为1维的，即使Eve配备无限数量的天线，依旧无法对1维的信号进行分解，因此无法消除注入的噪声。

4 系统吞吐量分析与优化

针对提出的噪声注入策略，本节对私密信息绝对安全下的系统吞吐量进行分析，得出系统吞吐量的闭式表达式；并对功率分配系数α与时隙分配系数τ进行设计，使得系统能够达到最大的吞吐量。

4.1 系统吞吐量分析

对于Eve，考虑其天线数趋于无穷大，可以得到其SNR的上界为

$$\begin{aligned}\gamma_{\mathrm{e}}^{\mathrm{UB}} &= \lim_{N_{\mathrm{e}}\to\infty}\frac{\alpha(1-\tau)P_{\mathrm{u}}\|\boldsymbol{h}_{\mathrm{ue}}\|^2}{(1-\alpha)(1-\tau)P_{\mathrm{u}}\|\boldsymbol{h}_{\mathrm{ue}}\|^2+\delta_{\mathrm{e}}^2}\\ &\overset{a}{=}\lim_{N_{\mathrm{e}}\to\infty}\frac{\alpha(1-\tau)P_{\mathrm{u}}N_{\mathrm{e}}}{(1-\alpha)(1-\tau)P_{\mathrm{u}}N_{\mathrm{e}}+\delta_{\mathrm{e}}^2}=\frac{\alpha}{(1-\alpha)}\end{aligned} \tag{6}$$

其中，步骤a根据大数定律(Law of Large Numbers)可得。由于UE硬件条件的限制，其天线接收灵敏度将远不如BS，即$\delta_{\mathrm{u}}^2\gg\delta_{\mathrm{b}}^2$，因此，我们假设$\delta_{\mathrm{b}}^2\to 0$。在此假设下，BS仅会受到UE发送信号中热噪声的干扰，BS处SNR可被简化为

$$\gamma_{\mathrm{b}}=\frac{\alpha\left(\tau P_{\mathrm{b}}|h_{\mathrm{bu}}|^2+\delta_{\mathrm{u}}^2\right)}{(1-\alpha)\delta_{\mathrm{u}}^2} \tag{7}$$

对于系统的可靠性，使用连接中断概率表示，其定义式为

$$p_{\mathrm{co}}=\mathrm{P}\left(\log_2(1+\gamma_{\mathrm{b}})<R_{\mathrm{b}}\right) \tag{8}$$

将式(7)代入式(8), BS处连接中断概率可表示为

$$p_{\mathrm{co}}=\left(1-\exp\left(-\frac{\delta_{\mathrm{u}}^2}{\tau P_{\mathrm{b}}}\left(\frac{(1-\alpha)\left(2^{R_{\mathrm{B}}}-1\right)}{\alpha}-1\right)\right)\right)^{N_{\mathrm{B}}} \tag{9}$$

对于系统的安全性，使用安全中断概率p_{so}进行刻画，其定义为窃听信道容量$\log_2(1+\gamma_{\mathrm{e}})$大于冗余编码速率$R_{\mathrm{B}}-R_{\mathrm{S}}$的概率。由于Eve处SNR上界仅与功率分配系数$\alpha$相关，因此，通过控制$\alpha\le 1-2^{R_{\mathrm{S}}-R_{\mathrm{B}}}$，可实现私密信息传输的完美安全，即安全中断概率$p_{\mathrm{so}}=0$。因此，安全传输约束下的系统吞吐量[14]可表示为

$$\eta=(1-\tau)(1-p_{\mathrm{co}})R_{\mathrm{S}} \tag{10}$$

命题 1 当Eve信道容量小于冗余信息速率$R_{\mathrm{B}}-R_{\mathrm{S}}$时，能够实现私密信号传输的完美安全。因此使用噪声注入策略，当功率分配系数满足条件$\alpha\le 1-2^{R_{\mathrm{S}}-R_{\mathrm{B}}}$时，可以实现完美安全。值得指出的是，大部分现有物理层安全技术在准静态衰落信道条件下尚无法实现完美安全，如文献[15,16]。

4.2 系统吞吐量最大化

4.2.1 问题描述

系统吞吐量最大化可被描述为

$$\max\quad \eta(\alpha,\tau) \tag{11a}$$

$$\text{s.t.}\quad p_{\mathrm{so}}=0, p_{\mathrm{co}}\le\sigma, 0\le\alpha\le 1, 0\le\tau\le 1 \tag{11b}$$

其中，$\eta(\alpha,\tau)$表达式如式(10)所示，σ表示允许的最大连接中断概率。

4.2.2 可行域分析

由式(9)可得，连接中断概率p_{co}随着α和τ的增大而减小。因此，取最大的α和τ时，可以得到最小的p_{co}。由于安全条件$p_{\mathrm{so}}=0$的限制，因此α最大取值为$1-2^{R_{\mathrm{S}}-R_{\mathrm{B}}}$；同时，$\tau$最大的值为1。因此，系统可靠性限制的可行域可以表示为

$$\begin{aligned}&\sigma:\left(1-\exp\left(-\frac{2^{R_{\mathrm{B}}}\delta_{\mathrm{u}}^2}{P_{\mathrm{b}}}\left(\frac{2^{R_{\mathrm{S}}}-1}{2^{R_{\mathrm{b}}}-2^{R_{\mathrm{S}}}}\right)\right)\right)^{N_{\mathrm{B}}}\\ &\le\sigma\le 1\end{aligned} \tag{12}$$

4.2.3 优化设计

在给定τ的条件下，首先对功率分配系数α进行优化分析。通过命题2可以得到α的优化解。

命题 2 对于任意的τ，在连接中断和安全中断条件的约束下，使系统吞吐量达到最大的α表示为

$$\alpha_{\mathrm{opt}}=1-2^{R_{\mathrm{S}}-R_{\mathrm{B}}} \tag{13}$$

证明 由式(10)可得，随着α的增大，η逐渐增大。考虑到安全性和可靠性约束，α取值范围为$[\alpha_{\mathrm{LB}},\alpha_{\mathrm{UB}}]$，其中$\alpha_{\mathrm{LB}}=1-2^{R_{\mathrm{S}}-R_{\mathrm{B}}}$。因此，在$\alpha=1-2^{R_{\mathrm{S}}-R_{\mathrm{B}}}$时，系统吞吐量最大；同时，可以发现$\alpha$的最优取值与参数$\tau$无关，因此可以得到命题2中的结论。

说明 η随着α的增大而增大，这是因为发送私密信号的功率更大，因此连接中断概率减小，系统吞吐量增大。然而，α不能无限增大，必须有足够的噪声功率以保证系统的私密信号的绝对安全。因此，最优的α取值为满足安全性约束时最大的α值。

接下来，在α取最优值的情况下，对参数τ进行优化分析。通过命题3可以得到τ的优化解。

命题 3 在连接中断和安全中断条件的约束下，使系统吞吐量达到最大的τ表示为

$$\tau_{\mathrm{opt}}=\max\left\{\tau^*,-\frac{2^{R_{\mathrm{B}}}\delta_{\mathrm{u}}^2}{\mathrm{In}\left(1-\sqrt[N_{\mathrm{b}}]{\sigma}\right)P_{\mathrm{b}}}\left(\frac{2^{R_{\mathrm{S}}}-1}{2^{R_{\mathrm{B}}}-2^{R_{\mathrm{S}}}}\right)\right\} \tag{14}$$

其中，τ^*为$\dfrac{\partial \eta}{\partial \tau}=0$的唯一解，可用二分法求解。

证明　根据泰勒级数展开，式(10)中的系统吞吐量可以进一步表示为

$$\eta = R_{\mathrm{S}}\left(1-\tau\right)\left(-\sum_{n=1}^{N_{\mathrm{b}}} C_{N_{\mathrm{b}}}^{n}\left(-\theta\right)^{n}\right) \tag{15}$$

其中，

$$\theta\left(\tau\right)=\exp\left(-\frac{2^{R_{\mathrm{B}}}\delta_{\mathrm{u}}^{2}}{\tau P_{\mathrm{b}}}\left(\frac{2^{R_{\mathrm{S}}}-1}{2^{R_{\mathrm{B}}}-2^{R_{\mathrm{S}}}}\right)\right) \tag{16}$$

令$\dfrac{\partial \eta}{\partial \tau}=0$，可得

$$\sum_{n=1}^{N_{\mathrm{b}}} C_{N_{\mathrm{b}}}^{n}\left(-\theta\right)^{n}+\frac{\partial \theta}{\partial \tau}\left(1-\tau\right)\left(\sum_{n=1}^{N_{\mathrm{b}}} C_{N_{\mathrm{b}}}^{n} n\left(-\theta\right)^{n-1}\right)=0 \tag{17}$$

将式(16)代入式(17)中，化简可得

$$\frac{\sum_{n=1}^{N_{\mathrm{b}}} C_{N_{\mathrm{b}}}^{n}\left(-\theta\right)^{n}}{\sum_{n=1}^{N_{\mathrm{b}}} C_{N_{\mathrm{b}}}^{n} n\left(-\theta\right)^{n}}=\frac{1-\tau}{\tau^{2}}\left(\frac{2^{R_{\mathrm{B}}}\delta_{\mathrm{u}}^{2}}{P_{\mathrm{b}}}\left(\frac{2^{R_{\mathrm{S}}}-1}{2^{R_{\mathrm{B}}}-2^{R_{\mathrm{S}}}}\right)\right) \tag{18}$$

令$f\left(\theta\right)=\dfrac{\sum_{n=1}^{N_{\mathrm{b}}} C_{N_{\mathrm{b}}}^{n}\left(-\theta\right)^{n}}{\sum_{n=1}^{N_{\mathrm{b}}} C_{N_{\mathrm{b}}}^{n} n\left(-\theta\right)^{n}}$，则$f\left(\theta\right)$可进一步化简为

$$f\left(\theta\right)=\frac{1-\theta}{N_{\mathrm{b}}\theta}\left(\left(1-\theta\right)^{-N_{\mathrm{b}}}-1\right),\theta\in\left(0,\theta\left(1\right)\right) \tag{19}$$

对$f\left(\theta\right)$关于θ求1阶导数，可得

$$\frac{\partial f\left(\theta\right)}{\partial \theta}=\frac{1}{N_{\mathrm{b}}\theta^{2}}\left(\left(\theta N_{\mathrm{b}}-1\right)\left(1-\theta\right)^{-N_{\mathrm{b}}}+1\right) \tag{20}$$

由式(20)可得，当$N_{\mathrm{b}}=1$时，$\dfrac{\partial f\left(\theta\right)}{\partial \theta}=0$，$f\left(\theta\right)=1$；当$N_{\mathrm{b}}>1$时，$\dfrac{\partial f\left(\theta\right)}{\partial \theta}>0$，$f\left(\theta\right)$在$\left(0,\theta\left(1\right)\right)$上单调递增，且$\lim_{\theta\to 0} f\left(\theta\right)=1$。又由于$\dfrac{\partial \theta\left(\tau\right)}{\partial \tau}>0$，且$\lim_{\tau\to 0}\theta\left(\tau\right)=1$，所以$\dfrac{\partial f\left(\tau\right)}{\partial \tau}=\dfrac{\partial f\left(\theta\right)}{\partial \theta}\dfrac{\partial \theta}{\partial \tau}>0$，即$f\left(\tau\right)$在$\left(0,1\right)$上单调递增，且$\lim_{\tau\to 0} f\left(\tau\right)=1$。令$g\left(\tau\right)=\dfrac{1-\tau}{\tau^{2}}\left(\dfrac{2^{R_{\mathrm{B}}}\delta_{\mathrm{u}}^{2}}{P_{\mathrm{b}}}\left(\dfrac{2^{R_{\mathrm{S}}}-1}{2^{R_{\mathrm{B}}}-2^{R_{\mathrm{S}}}}\right)\right),\tau\in\left(0,1\right)$，显然$g\left(\tau\right)$在$\left(0,1\right)$上单调递减，且$\lim_{\tau\to 0} g\left(\tau\right)=\infty$，$\lim_{\tau\to 1} g\left(\tau\right)=0$。

由以上分析可得，$f\left(\tau\right)$与$g\left(\tau\right)$有且仅有唯一交点，即$\dfrac{\partial \eta}{\partial \tau}=0$有且仅有唯一解。并且，当$\tau=\tau^*$使$\dfrac{\partial \eta}{\partial \tau}=0$时，网络吞吐量$\eta$可以取得最大值。又由系统可靠性约束$p_{\mathrm{co}}\le\sigma$可得，$\tau\ge-\dfrac{2^{R_{\mathrm{B}}}\delta_{\mathrm{u}}^{2}}{\mathrm{In}\left(1-\sqrt[N_{\mathrm{b}}]{\sigma}\right)P_{\mathrm{B}}}\cdot\left(\dfrac{2^{R_{\mathrm{S}}}-1}{2^{R_{\mathrm{B}}}-2^{R_{\mathrm{S}}}}\right)$。综上所述，最优的参数$\tau$如命题3所示。

5　仿真分析

本小节对采用噪声注入策略的物联网系统物理层安全性能进行数值仿真。首先，给出了时隙分配系数τ与功率分配系数α对系统可靠性与吞吐量的影响。然后，将此噪声注入策略与传统的单天线on-off策略进行比较，揭示所提出的噪声注入策略对系统性能的提升。仿真中系统预设参数如下：$N_{\mathrm{b}}=4$, $N_{\mathrm{e}}=128$, $P_{\mathrm{b}}=20$ dBm, $R_{\mathrm{B}}=2$ bit/s, $R_{\mathrm{S}}=1$ bit/s, $\delta_{\mathrm{u}}^{2}=0.01$, α取值始终保证系统绝对安全。

5.1　系统性能仿真

首先，分析了时隙分配系数τ与功率分配系数α对连接中断概率p_{co}的影响。如图3所示，连接中断概率p_{co}随着时隙分配系数τ的增大而减小，这是因为分配更多的时间用于噪声注入时，BS可以更好地消除注入的噪声，因此系统有着更好的可靠性性能。当功率分配系数α增大时，连接中断概率减小，这是因为将更多的功率分配给私密信号时，BS接收信号SNR增大，因此可靠性增强。

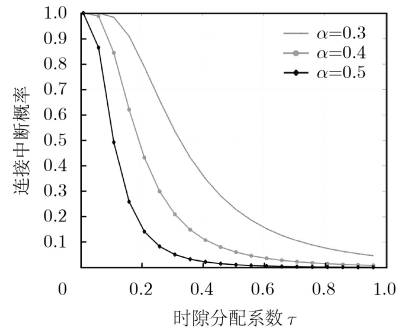

图 3 连接中断概率随参数τ和α的变化

时隙分配系数τ与功率分配系数α对系统吞吐量η的影响如图4所示。系统吞吐量η随着时隙分配系数τ先增大后减小，这是因为增加噪声注入的时间虽然可以提升可靠性，但是会减少用于数据传输的时间，因此存在一个最优的τ使得吞吐量η取得最大。当功率分配系数α增大时，系统吞吐量也会增大，这是因为增大α可以提升系统可靠性，进一步提升系统的吞吐量；但是为了满足系统的安全性约束，α取值并不能无限增大，因此最优α取值为满足安全约束条件下的最大值。

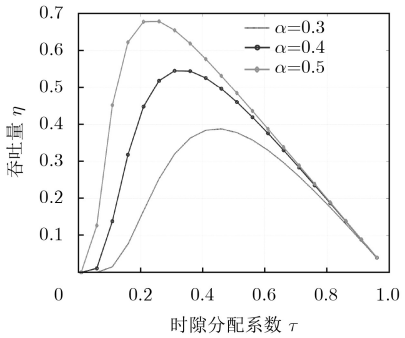

图 4 系统吞吐量随参数τ和α的变化

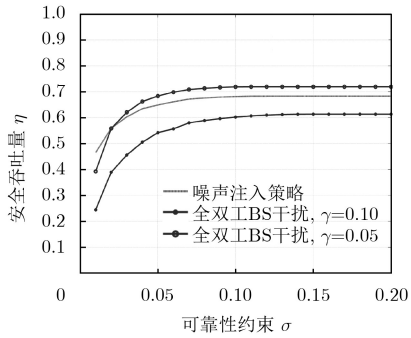

图 6 系统安全吞吐量随可靠性约束的变化

5.2 对比分析

本节中，将本文方案与其他可应用于单天线物联网终端的物理层安全策略进行对比。目前可在单天线物联网终端实现的策略主要包括On-Off策略[17]和全双工BS噪声干扰策略[18]。

图5中，将提出的噪声注入策略与传统On-Off策略进行比较。On-Off策略仿真预设参数如下：P_{u}= 20 dBm, $\delta_{\mathrm{b}}^2 = 0.01$, $\delta_{\mathrm{e}}^2 = 0.01$, N_{b}= 4。与本文接收端策略一致，假设BS采用最优天线选择策略。同时，假设能够获得窃听信道的CSI，则On-Off策略中通过阈值设置使得窃听者无法获取私密信号。噪声注入策略与On-Off策略可实现的最大吞吐量随发射功率变化如图5所示。由图可知，On-Off策略所能达到的最大吞吐量受窃听者天线数影响较大，而噪声注入策略不受窃听者天线数的影响。只有在窃听者天线数较少时，On-Off策略在一定发射功率下的吞吐量会优于噪声注入策略；而当窃听者天线数较多时，噪声注入策略性能显著优于On-Off策略。同时，On-Off策略需要获取窃听信道CSI，该假设在实际物联网场景中难以满足，而噪声注入策略无需获取任何窃听信道信息。

图6中，将噪声注入策略与全双工BS噪声干扰策略进行比较。全双工BS噪声干扰策略仿真预设参数如下：P_{u}= 20 dBm, $\delta_{\mathrm{b}}^2 = 0.01$, $\delta_{\mathrm{e}}^2 = 0.01$。基站工作在全双工模式会给信号接收带来自干扰，目前主要考虑用自干扰消除技术来减轻自干扰对信号

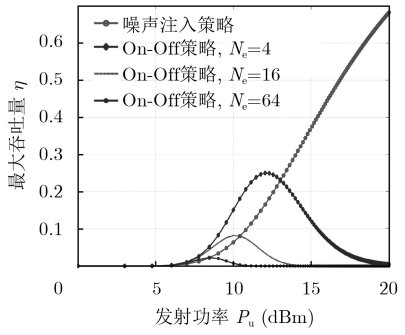

图 5 系统吞吐量随发射功率的变化

接收带来的影响。假设自干扰消除系数为γ，不同自干扰消除水平下全双工BS噪声干扰策略与噪声注入策略对比如图6所示。由图可知，随着可靠性约束的放宽，系统可得到的安全吞吐量逐渐增加。同时，全双工BS噪声干扰策略的性能优劣在很大程度上取决于BS的自干扰消除水平。需要指出的是，噪声注入策略可以通过调整参数实现完美安全，因此其吞吐量也是安全吞吐量。由于全双工BS噪声干扰策略基于BS全双工以及BS天线数大于窃听者天线数的假设，考虑到窃听者配备大规模MIMO的场景，BS只有配备更多数量的天线且具备全双工通信功能才能保证该方案的有效性，这使得该方案在对抗大规模MIMO窃听者时对BS的硬件要求过高，在现实物联网系统中难以实现。

6 结束语

本文针对物联网上行通信场景，考虑能量与计算能力受限的物联网终端和配备大规模MIMO的窃听者，提出一种可实现完美安全的噪声注入策略。该策略通过在私密信号中叠加带有合法信道CSI的人工噪声，使得BS能够成功消除噪声，而Eve无法消除噪声，从而可实现私密信息的完美安全。基于该策略，本文对系统可靠性和安全性进行分析，并得到系统吞吐量的闭式解。进一步，以最大化吞吐量为目标，对时隙分配系数和功率分配系数进行优化。理论和仿真结果表明，通过调整参数，该噪声注入策略可以实现私密信息完美安全。将该噪声注入策略与On-Off策略和全双工BS噪声干扰策略进行对比，噪声注入策略在抗大规模MIMO窃听者上展现出明显优势。需要指出的是，本文的分析基于BS能够完美估计合法信道CSI, BS侧CSI估计不完美时对参数设计以及性能的影响将作为我们以后的工作。

参 考 文 献

[1] AKPAKWU G A, SILVA B J, HANCKE G P, *et al*. A survey on 5G networks for the internet of things:

Communication technologies and challenges[J]. *IEEE Access*, 2017, 99(6): 3619–3647. doi: 10.1109/ACCESS.2017.2779844.

[2] MASSEY J L. An introduction to contemporary cryptology[J]. *Proceedings of the IEEE*, 1988, 76(5): 533–549. doi: 10.1109/5.4440.

[3] 黄开枝, 张波. 异构密集网中一种抗多窃听者的协作安全波束成形方案[J]. 电子与信息学报, 2017, 39(7): 1673–1680. doi: 10.11999/JEIT161152.
HUANG Kaizhi and ZHANG Bo. Cooperative secrecy beamforming scheme resistant to multi-eavesdroppers in dense heterogeneous networks[J]. *Journal of Electronics & Information Technology*, 2017, 39(7): 1673–1680. doi: 10.11999/JEIT161152.

[4] LI Yiqing, JIANG Miao, ZHANG Qi, *et al*. Secure beamforming in downlink MISO non-orthogonal multiple access systems[J]. *IEEE Transactions on Vehicular Technology*, 2017, 66(8): 7563–7567. doi: 10.1109/TVT.2017.2658563.

[5] DENG Yansha, WANG Lifeng, YUAN Jinhong, *et al*. Artificial-noise aided secure transmission in large scale spectrum sharing networks[J]. *IEEE Transactions on Communications*, 2016, 64(5): 2116–2129. doi: 10.1109/TCOMM.2016.2544300.

[6] LIU Chenxi, YANG Nan, MALANEY R, *et al*. Artificial-noise-aided transmission in multi-antenna relay wiretap channels with spatially random eavesdroppers[J]. *IEEE Transactions on Wireless Communications*, 2016, 15(11): 7444–7456. doi: 10.1109/TWC.2016.2602337.

[7] MUKHERJEE A. Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints[J]. *Proceedings of the IEEE*, 2015, 103(10): 1747–1761. doi: 10.1109/JPROC.2015.2466548.

[8] XU Qian, REN Pinyi, SONG Houbing, *et al*. Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations[J]. *IEEE Access*, 2016, 4: 2840–2853. doi: 10.1109/ACCESS.2016.2575863.

[9] KIM J and CHOI J P. Cancellation-based friendly jamming for physical layer security[C]. IEEE Global Communications Conference, Washington, USA, 2016: 16655354. doi: 10.1109/GLOCOM.2016.7841646.

[10] Al-NAHARI A. Physical layer security using massive multiple-input and multiple-output: Passive and active eavesdroppers[J]. *IET Communications*, 2016, 10(1): 50–56. doi: 10.1049/iet-com.2015.0216.

[11] WU Yongpeng, SCHOBER R, NG D W K, *et al*. Secure massive MIMO transmission with an active eavesdropper[J]. *IEEE Transactions on Information Theory*, 2016, 62(7): 3880–3900. doi: 10.1109/TIT.2016.2569118.

[12] WANG Chao and WANG Huiming. Robust joint beamforming and jamming for secure AF networks: Low-Complexity design[J]. *IEEE Transactions on Vehicular Technology*, 2015, 64(5): 2192–2198. doi: 10.1109/TVT.2014.2334640.

[13] HE Biao, SHE Yechao, and LAU V K N. Artificial noise injection for securing single-antenna systems[J]. *IEEE Transactions on Vehicular Technology*, 2017, 66(10): 9577–9581. doi: 10.1109/TVT.2017.2703159.

[14] 黄开枝, 许耘嘉, 丁大钊, 等. 非理想情况下K层密集异构蜂窝网的安全性能分析[J]. 电子与信息学报, 2017, 39(10): 2456–2463. doi: 10.11999/JEIT161376.
HUANG Kaizhi, XU Yunjia, DING Dazhao, *et al*. Secrecy performance analysis of K-tier dense heterogeneous cellular networks with imperfect channel state information[J]. *Journal of Electronics & Information Technology*, 2017, 39(10): 2456–2463. doi: 10.11999/JEIT161376.

[15] ZHANG Yuanyu, SHEN Yulong, WANG Hua, *et al*. On secure wireless communications for IoT under eavesdropper collusion[J]. *IEEE Transactions on Automation Science & Engineering*, 2016, 13(3): 1281–1293. doi: 10.1109/TASE.2015.2497663.

[16] ZHOU Xiangyun, MEKAT M R, MAHAM B, *et al*. Rethinking the secrecy outage formulation: A secure transmission design perspective[J]. *IEEE Communications Letters*, 2011, 15(3): 302–304. doi: 10.1109/LCOMM.2011.011811.102433.

[17] HE Biao and ZHOU Xiangyun. Secure on-off transmission design with channel estimation errors[J]. *IEEE Transactions on Information Forensics & Security*, 2013, 8(12): 1923–1936. doi: 10.1109/TIFS.2013.2284754.

[18] ZHU Fengchao, GAO Feifei, YAO Minli, *et al*. Joint information and jamming-beamforming for physical layer security with full duplex base station[J]. *IEEE Transactions on Signal Processing*, 2014, 62(24): 6391–6401. doi: 10.1109/TSP.2014.2364786.

彭建华：男， 1966年生，教授，博士生导师，研究方向为移动通信网络及信息安全.

张　帅：男， 1994年生，硕士生，研究方向为移动通信安全.

许晓明：男， 1988年生，讲师，研究方向为无线通信及网络信息安全.