# 基于接收机人工噪声的物理层安全技术及保密区域分析

李 为 陈 彬 魏急波 熊春林 张晓瀛
(国防科学技术大学 电子科学与工程学院，长沙 410073)

**摘 要**：提出了一种实现无线通信物理层安全的新方法，并从信息论的角度进行了性能分析。此方法通过合法接收者发送人工噪声来干扰窃听者信道，同时通过抵消技术使得自身不受人工噪声的影响。此方法无需信道信息的反馈，能够对抗多天线的窃听者，具有强的鲁棒性。此外基于地理位置信息提出了一种“保密区域”的新概念，此概念针对不同窃听者位置进行了遍历保密容量分析，可以作为物理层安全的评价标准和设计准则。分析和仿真结果表明所提算法对安全性能的提升较为明显，所提“保密区域”概念能够较好的从地理位置的角度评估物理层安全性能。

**关键词**：物理层安全；人工噪声；保密区域；地理位置
**中图分类号**：TN911 **文献标识码**：A **文章编号**：1003-0530(2012)09-1314-07

# Secure Communications via Sending Artificial Noise by the Receiver: Ergodic Secure Region Analysis

LI Wei CHEN Bin WEI Ji-bo XIONG Chun-lin ZHANG Xiao-ying
(Department of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China)

**Abstract**: A novel approach for ensuring confidential wireless communication is proposed and analyzed from an information-theoretic standpoint. In this method, the legitimate receiver generates artificial noise (AN) to impair the intruder's channel. This method is robust because it doesn't need feedback of CSI and can withstand multi-antenna or colluding eavesdroppers. Furthermore, using the average signal-to-noise ratio, which is only a function of the path-loss, we determine the insecure regions, which is the geographical regions where Eve may decode the secret message. The secure region is the region where Eve cannot decode the message. To improve the probability of communicating securely, the target of our design can be the reduction of the insecure region. For each target value of the secrecy capacity, we derive the secure region for both SISO and MIMO systems when the channels are unknown to the transmitter. Analysis and simulation results in practical environments show that the proposed method has a good performance.

**Key words**: Physical layer security; Artificial noise; Secrecy region; Geometric

## 1 引言

由于电磁波媒介的广播特性，安全性成为无线通信中的突出问题。传统的方法采用密码学途径(如数据加密)来实现信息安全。这类基于密钥的方法，使得非法窃听者需要进行高度复杂的计算处理才可能破译信息。然而当前高性能处理器的不断发展使得对长而复杂的密钥破译成为可能，也使得基于密码学的传统

收稿日期：2012-05-11；修回日期：2012-08-29
基金项目：国家自然科学基金资助项目(61101096)；国家自然科学基金资助项目(61101098)；湖南省杰出青年科学基金资助项目(11jj4055)

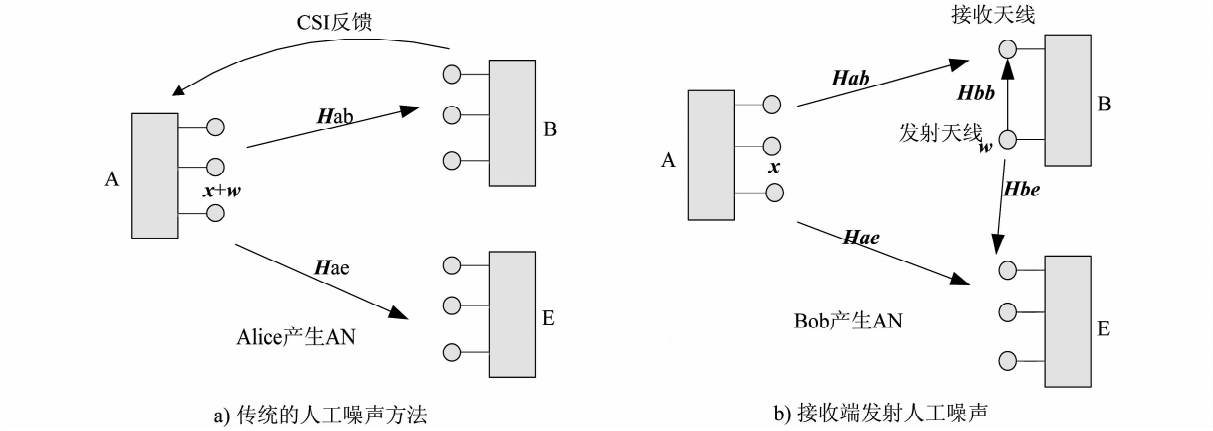
安全机制受到挑战。近年来研究从物理层提供保密通信的能力得到了广泛关注。物理层安全旨在为通信系统提供信息论意义上的安全,从物理层限制窃听者能够获取的比特信息量。通过利用无线信道的物理层性质和随机编码思想,将信息流隐藏在恶化窃听信道的额外噪声中,如果能够确保窃听者的条件信息熵任意接近信源熵,则窃听者从其接收信号中几乎获取不到任何主信道信息,从而可以不借助密钥在无线媒介中实现完全保密。物理层安全机制可以和传统的加密、认证及鉴权等安全策略相结合,进而构建更为安全的无线通信系统。

Wyner 最先引入了窃听信道和保密容量的概念[1]。物理层安全问题包含 3 类节点,发送者(Alice),合法接收者(Bob)和窃听者(Eve)。Alice 需要发送信息给 Bob,同时避免 Eve 窃听到信息。保密容量被定义为 Alice 和 Bob 之间的通信所能达到的不会被 Eve 窃取信息的最高信息传输速率。之后 Wyner 的工作被扩展到高斯信道[2],近期被扩展到 MIMO 信道[3]和衰落信道[4].

为了增加保密容量,文献[5]提出了一种基于人工噪声(AN)的方法。在此方法中,人工噪声由多天线或者协同节点产生,利用波束成型技术插入到 Bob 信道的零空间之中。人工噪声会破坏 Eve 的信道,但不会影响到 Bob 的信道[6,7]。文献[8]将不适定的思想引入无线物理层安全领域。文献[9]进一步研究了联合波束成型矢量和人工噪声矩阵设计来达到 Bob 和 Eve 的信干比约束(SINR)。然而此类算法仍然存在以下需要克服的问题:1)Bob 的信道状态信息(CSI)或者至少是部分信道状态信息,需要反馈到发送节点,这占用了一定的带宽;2)此处信道状态信息的反馈失真会使 AN 泄露至 Bob 的信道中,导致 Bob 的接收信噪比降低,且若 Eve 伪装成 Bob 来反馈其信道状态信息给 Alice 会进一步恶化系统的安全性能。3)当 Eve 具有多个天线或者有多个联合窃听的 Eve 且其天线数目总和大于 Alice 的发送天线数目时,AN 可以被 Eve 计算得到并完全消除。

为了克服以上问题,本文提出一种通过接收机发送 AN 来增加安全容量的方法。如图 1 b)所示,Bob 在接收到 Alice 发送信号的同时,产生 AN 来对抗窃听者,而此处的 AN 能够被 Bob 抵消掉。所提方法具有以下优点:1)Alice 不需要信道信息,所以不需要额外的反馈信道从而节省了带宽,同时也消除了反馈信道不可靠引起的安全隐患;2)已有的方法必须由多天线产生 AN,而所提方法的 AN 既可以由多天线产生也可以由单天线产生,更加具有实用性;3)所提方法并不对窃听者数量及其天线数目做出特殊限制,在对抗多天线窃听者时仍然有较好效果;4)此方法也可以与发送端发射人工噪声的方法相结合,以取得更好的安全性能。

本文的另一项贡献是从地理位置信息的角度研究了物理层安全的性能,提出了保密区域和非保密区域这两个新的概念。已有的物理层安全研究从信号处理的角度设计安全策略,考虑的是信道小尺度衰落特性;往往忽略了由于通信节点位置不同而引起的大尺度衰落特性。本文利用大尺度衰落模型,利用平均信道信息计算出了非保密区域——窃听者在此区域可以正确译码获得保密消息。为了提高安全性,物理层安全策略的设计准则可以以减小非安全区域为目标。




a) 传统的人工噪声方法　　b) 接收端发射人工噪声

图 1　采用人工噪声实现物理层安全

Fig. 1　Secret communication using artificial noise

本文余下部分的组织结构如下:第 2 节描述了系统模型和所提安全机制;第 3 节定义了保密区域的概念,并分析了所提算法的保密性能;第 4 节进行了数值仿真;第 5 节为结束语。

## 2 系统模型

如图 1 b)所示,本文系统模型包括一个具有 $m_A$ 根发射天线的发射端 Alice;一个具有 $n_B$ 根接收天线和 $m_B=1$ 根发射天线的合法接收端 Bob;一个具有 $m_E$ 根接收天线的窃听者 Eve。Bob 在接收到 Alice 信号的同时发送人工噪声 $w(k)$来干扰窃听者 Eve。

该场景建模如下:

$$\boldsymbol{z}(k)=\boldsymbol{H}_{ab}\boldsymbol{x}(k)+\boldsymbol{H}_{bb}\boldsymbol{w}(k)+\boldsymbol{n}(k) \tag{1}$$

$$\boldsymbol{y}(k)=\boldsymbol{H}_{ae}\boldsymbol{x}(k)+\boldsymbol{H}_{be}\boldsymbol{w}(k)+\boldsymbol{e}(k) \tag{2}$$

其中 $k=1,2,\ldots$ 表示时间;$\boldsymbol{x}$ 表示($m_A\times1$)维的发射信号向量,其方差矩阵 $\boldsymbol{K}_x\geqslant\boldsymbol{0}_{m_A}$ 满足功率约束 $Tr(\boldsymbol{K}_x)=P_A$,假设发射端未知 $\boldsymbol{H}_{ab}$ 与 $\boldsymbol{H}_{ae}$ 的信息,那么 $\boldsymbol{x}$ 的方差矩阵可设为 $\boldsymbol{K}_x=\dfrac{P_A\boldsymbol{I}_{m_A}}{m_A}$;$\boldsymbol{w}$ 表示($m_B\times1$)维的人工噪声向量(由接收端发射),其方差矩阵 $\boldsymbol{K}_w\geqslant\boldsymbol{0}_{m_B}$ 满足功率约束 $Tr(\boldsymbol{K}_w)=P_B$,由于 $m_B=1$,那么 $\boldsymbol{K}_w=P_B$;$\boldsymbol{z}$ 和 $\boldsymbol{y}$ 分别表示合法接收者与窃听者的接收信号向量;$\boldsymbol{H}_{ab}$、$\boldsymbol{H}_{ae}$ 与 $\boldsymbol{H}_{bb}$ 分别表示发射端与合法接收端、发射端与侦听端以及合法接收端自身发射天线与接收天线间的信道矩阵;$\boldsymbol{n}$ 和 $\boldsymbol{e}$ 分别表示独立不相关的复高斯白噪声向量,其功率等于 $N_0$。

下面的关键问题是如何设计 AN 信号 $w(k)$,以及 Bob 如何抵消 $w(k)$对自身的干扰。当 Eve 的信道信息对 Bob 完全未知时,最合适的方式是 Bob 发射与接收信号相同频带的高斯白噪声。为了抵消 AN 对于 Bob 的影响。我们采用全双工无线技术[11,12]. 通过天线抵消、射频抵消和数字信号处理抵消,AN 可以被减小到可以接受的程度。图 2 为两天线全双工的射频设计[11]. 发送信号为正信号,经过不平衡变压器后产生一个相反的信号,通过增益控制和延时控制与接收信号叠加,这样抵消掉了大部分发送信号。残余的信号可以通过数字信号处理来抵消。因为发送信号 AN 和信道 $H_{bb}$ 对于 Bob 已知,这样可以在接收机中重构出残余的 AN 进行抵消,具体过程如下:

$$\boldsymbol{z}'=\boldsymbol{z}-\boldsymbol{H}_{bb}\boldsymbol{w}=\boldsymbol{H}_{ab}\boldsymbol{x}+\boldsymbol{n}$$

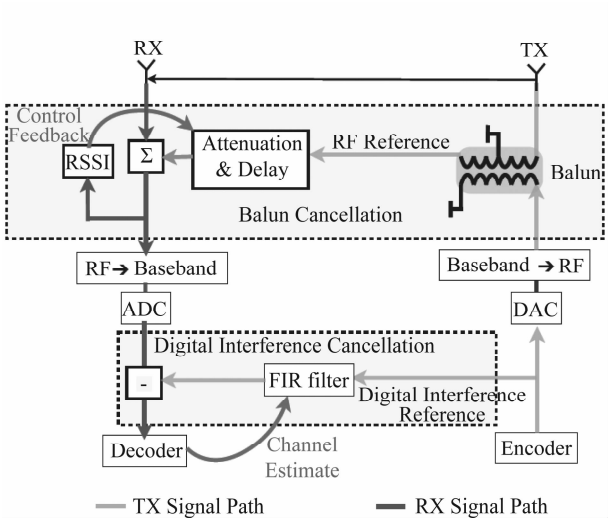



图 2 Bob 自干扰抵消方法[11]

Fig. 2 Cancel the interference on Bob[11]

## 3 保密性能分析

本节分别对 SISO 和 MIMO 两种情况下的保密性能进行分析。对于 Eve,它和 Alice 之间的信道状态信息 $\boldsymbol{H}_{ae}$ 为已知,但是 Eve 与 Bob 之间的信道状态信息 $\boldsymbol{H}_{be}$ 是未知的。因为 Bob 仅仅发射白噪声,Eve 不能够对其进行信道估计,所以 Eve 不能够完全抵消掉 AN 的影响。因此这里假定 Eve 把 AN 当成白噪声处理是合理的。值得注意的是,这里的处理不同于传统的发送端发送人工噪声的方法。在传统方法中,Alice 在发送 AN 的同时也发送包含着数据和训练序列的有效信息,Eve 可以利用这些信息来对信道 $\boldsymbol{H}_{ab}$ 进行估计,所以当 Eve 的天线数目大于 Alice 时可以抵消掉 AN 的影响。

### 3.1 SISO 信道

首先利用文献[13]中的结论推导出 SISO 情况下的保密容量。假定 Alice 和 Bob 之间通过标准的加性高斯白噪声(AWGN)信道进行通信,其噪声方差为 $N_0$。Eve 的接收信号噪声方差为 $N_0+P_B|H_{be}|^2$。那么这里的保密容量可以表示为:

$$C_s=[\log_2(1+\gamma_B)-\log_2(1+\gamma_E)]^+ \tag{3}$$

其中 $\gamma_B=\dfrac{|H_{ab}|^2P_A}{N_0}$, $\gamma_E=\dfrac{|H_{ae}|^2P_A}{N_0+P_B|H_{be}|^2}$; $x^+=\max(x,0)$。

为了考察基于地理位置信息的保密安全特性,我们将根据平均信干噪比来确定保密区域和非保密区

域。将信道信息 $|H_{be}|^2$, $|H_{ae}|^2$ 和 $|H_{ab}|^2$ 用其统计平均值 $\lambda d_{be}^{-\kappa}$, $\lambda d_{ae}^{-\kappa}$, $\lambda d_{ab}^{-\kappa}$ 来替代。其中 $d_{be}$ $d_{ae}$, $d_{ab}$ 分别为 Bob 和 Eve、Alice 和 Eve、以及 Alice 和 Bob 之间的距离。$\kappa$ 为衰落因子,$\lambda$ 为常数,由传播模型和载波频率决定。假定 Bob 的位置和 Alice 的位置已知,定义保密区域如下:

**定义(保密区域):** 给定发送速率 $R_t$,发送功率,和人工噪声功率,安全区域定义为窃听者不能正确解译出保密信息的区域,其数学表达式为

$$R=\{\boldsymbol{\theta}_e \mid C_S \geqslant R_t\} \tag{4}$$

其中 $\boldsymbol{\theta}_e$ 为 Eve 的几何坐标矢量。

由(3)(4)得到保密区域为:

$$R=\{\boldsymbol{\theta}_e \mid \lambda d_{be}^{-\kappa}(2^{-R_t}(1+\bar{\gamma}_B)-1)P_B-\lambda d_{ae}^{-\kappa}P_A+N_0(2^{-R_t}(1+\bar{\gamma}_B)-1)\geqslant 0\} \tag{5}$$

其中 $\bar{\gamma}_B=\lambda d_{ab}^{-\kappa}P_A/N_0$。由(5)进一步可以推出,如果 Eve 的位置满足以下不等式则安全性可以得到保证:

$$f(d_{be},d_{ae})=\alpha d_{be}^{-\kappa}-\beta d_{ae}^{-\kappa}+\chi \geqslant 0 \tag{6}$$

其中 $\alpha=\lambda P_B\chi/N_0$, $\beta=\lambda P_A$, $\chi=N_0(2^{-R_t}(1+\bar{\gamma}_B)-1)$。需要注意的是,以上的结论由信道的统计平均特性得到。在衰落信道通信中,实际系统会采用时间交织技术使得信道在一定时间内的特性平均化。因此保密区域的定义对于物理等安全性的评估具有实际意义。

图 3 显示了不同传输速率 $R_t=5\times10^6$, $1\times10^7$, $1.5\times10^7$, $2\times10^7$ bit/s 的安全区域和非安全区域。此时 Alice 和 Bob 的坐标分别为(0,0)和(1,0),系统带宽为 5MHz。可以看到非安全区域是围绕 Alice 的类似椭圆的形状。

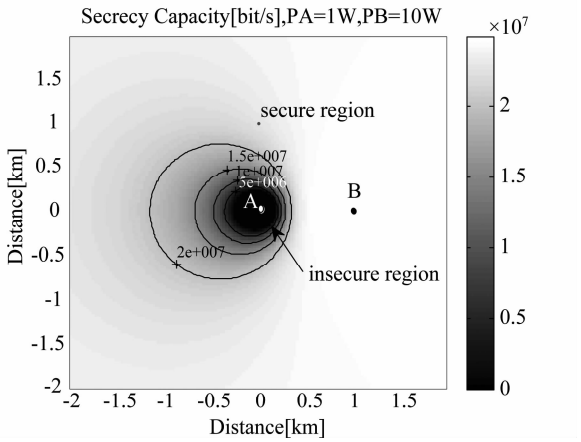



图 3　不同发射速率的安全区域和非安全区域

Fig. 3　secure region and insecure region for different rates

### 3.2　MIMO 信道

MIMO 信道的保密容量由下式给出[13]

$$C_s=\max_{K_X,K_w}\{\log_2\det(I+\Gamma_B)-\log_2\det(I+\Gamma_E)\} \tag{7}$$

其中 $\Gamma_B=H_{ab}K_XH_{ab}^*/N_0$, $\Gamma_E=H_{ae}K_XH_{ae}^*(N_0I_{m_E}+H_{be}K_wH_{be}^*)^{-1}$; *表示共轭转置;$I$ 为单位矩阵。

如果 $H_{ab}$ 和 $H_{ae}$ 对 Alice 已知,可以设计合适的 $\boldsymbol{x}$ 来增加保密容量。然而此模型中信道状态信息未知,所以 $\boldsymbol{x}$ 的协方差矩阵设置为 $K_x=P_AI_{m_A}/m_A$。若 Bob 已知 $H_{be}$,则可以利用波速成型技术设计合适的 $K_w$ 来将噪声信号对准 Eve。这里我们考虑完全被动的 Eve,Bob 不知道 Eve 的信道状态信息,因此噪声只能等方性广播发送;为了降低复杂度 Bob 采用 1 根天线发送噪声已经足够,即 $m_B=1$, $K_w=P_B$。这样剩余的天线可以用来改进合法链路的信道容量。

在 MIMO 情况下我们需要考虑信道的衰落,因此信道状态信息矩阵视为随机矩阵,采用遍历容量来得到保密区域:

$$C_S^{ave}=\underset{H_{ab}}{E}[\log_2\det(I+\Gamma_B)]-\underset{H_{ae},H_{be}}{E}[\log_2\det(I+\Gamma_E)]\geqslant R_t \tag{8}$$

我们将信道矩阵表示为 $HH^*=\lambda d^{-\kappa}H_0H_0^*$,其中 $\lambda d^{-\kappa}$ 表示大尺度衰落部分,$d$ 为通信距离,$H_0$ 为小尺度衰落部分。假设天线间没有相关性,对于瑞利衰落信道,$H_0$ 中的每一个元素服从单位功率的复高斯分布。将所有信道均用以上模型替换,则可以得到[14]:

$$\underset{H_{ab}}{E}[\log_2\det(I_{n_B}+\Gamma_B)]=\int_0^\infty\log_2\left(1+\frac{P_A\lambda d_{ab}^{-\kappa}\zeta}{m_AN_0}\right)\times\sum_{k=0}^{\min\{n_B,m_A\}}\frac{k!}{(k+|m_A-n_B|)}[L_k^{|m_A-n_B|}(\zeta)]^2\zeta^{|m_A-n_B|}e^{\zeta}d\zeta \tag{9}$$

$$\underset{H_{ae},H_{be}}{E}[\log_2\det(I_{m_E}+\Gamma_E)]=\int_0^\infty\log_2\left(1+\frac{P_A\lambda d_{ab}^{-\kappa}\zeta}{m_A(N_0+P_B/m_B\lambda d_{be}^{-\kappa})}\right)\times\sum_{k=0}^{\min\{m_E,m_A\}}\frac{k!}{(k+|m_A-m_E|)}[L_k^{|m_A-m_E|}(\zeta)]^2\zeta^{|m_A-m_E|}e^{\zeta}d\zeta \tag{10}$$

其中 $L_k^m(x)=\frac{1}{k!}e^xx^m\frac{d^k}{dx^k}(e^{-x}x^{-m+k})$。

当发送天线数目 $m_A$ 较大时($m_A\geqslant4$),可以得到更为简化的表达式。

$\lim_{m_A\to\infty} H_{be}H_{be}^{*}=\lambda d_{be}^{-\kappa}m_B I_{m_E}$，$\lim_{m_A\to\infty} H_{ae}H_{ae}^{*}=\lambda d_{ae}^{-\kappa}m_B I_{m_E}$。此时(8)可以化简为

$$\left(1+P_A\lambda d_{ae}^{-\kappa}\left(N_0+P_B\lambda d_{be}^{-\kappa}\right)^{-1}\right)^{m_E}\leqslant 2^{-R_t}\left(1+d_{ab}^{-\kappa}\frac{P_A}{m_A N_0}\right)^{n_B} \tag{11}$$

由(11)进一步得到保密区域为 Eve 的坐标满足以下条件：

$$f(d_{be},d_{ae})=\alpha d_{be}^{-\kappa}-\beta d_{ae}^{-\kappa}+\chi\geqslant 0 \tag{12}$$

其中 $\alpha=\lambda P_B\chi/N_0$，$\beta=\lambda P_A$，$\chi=N_0(2^{-R_t/m_E}(1+d_{ab}^{-\kappa}P_A/(m_A N_0))^{n_B/m_E}-1)$。

### 3.3 实际安全性能和实现问题的进一步讨论

#### 3.3.1 方向性天线窃听者

在前文的分析中，考虑所有的天线均为全向天线。本节讨论 Eve 采用方向性天线的情况。我们考察的无线通信环境为瑞利衰落场景，由于大量反射物的存在，会出现各个方向到达的多径分量。在有用信号和人工噪声叠加以及多径干扰影响下，如何区分信号和干扰，定位 Bob 对于窃听者是个较大的挑战。窃听者可以采用阵列天线，方向图扫描的方法能抵消部分干扰信号，获得窃听性能的提升，但这无疑增加了窃听者的硬件成本和处理运算量。这正是本方法取得的正面效果。所以本方法对于具有方向性天线的窃听者仍然具有干扰效果。

#### 3.3.2 保密区域分析的意义

物理层安全机制的性能与窃听者的位置是相关联的。由于不同位置的窃听者会获得不同的窃听效果，本文提出的保密区域概念正是为了定量的分析不同位置的安全特性，此概念可用于对各种物理层安全策略的性能评估和设计指导，具有重要的意义。从分析中可以看到，本文所提出的方法，其非安全区域在发送者周围，因此可以对此区域重点关注，采用人工排查和巡逻的方法。也可以结合其他策略，例如发送端人工噪声来消除非安全区域。

#### 3.3.3 收发同步的问题

如何保证在 Alice 发送信号的同时，Bob 发射人工噪声，是在实际系统实现中需要考虑的问题。具体可以采用以下两种方法来保证收发的同步：

1) 在同步网络中，各个收发节点有统一的时钟，可以由上层协议来控制收发两端的时钟同步，最终可以达到 Alice 在发送信号的同时，Bob 也发送人工干扰。(类似 TDMA 中的同步技术)

2) 在点对点通信环境下，Alice 在发送信息前会有一段短前缀，用于 AGC 或者同步，这一段前缀不含有用信息，即使被 Eve 接收到也不会泄密。Bob 在收到前缀后立即发送人工噪声，这样不会造成有用信息的泄露。

## 4 仿真分析

为了评价本文所提方案的安全保密性能，仿真中考虑了以下场景。Alice 和 Bob 的坐标分别为(0,0)和(1,0)，系统带宽为 5MHz；Alice 的发送功率为 1W，Bob 的最大发射功率为 1W，噪声能量为 $N_0=-180$dBm/Hz；传播模型(路径衰减 dB)为 $128.1+37.6\log_{10}(d)$[15]，($d$ 为距离，单位 km)。下面的仿真中 Alice 为单天线发射，Bob 为单天线接收，单天线发射人工噪声。图 4 显示了无人工噪声时的保密区域图，可以看到不同发送速率的非保密区域为围绕 Alice 的同心圆。

图 5 显示了 Bob 发射功率为 1W 的人工噪声时的保密区域图。可以看到当发送速率较低时非保密区域为围绕 Alice 的类似椭圆；随着发送速率的增加非保密区域逐渐扩大，最后曲线不再封闭，在高发送速率时，保密区域成为围绕 Bob 的类椭圆。由图还可以得知，当 Eve 越靠近 Bob 时，受到的干扰越大，保密容量也就越大，因此安全性也越高。故而所提方法对抗合法接收者附近的窃听者有着更好的安全效果。

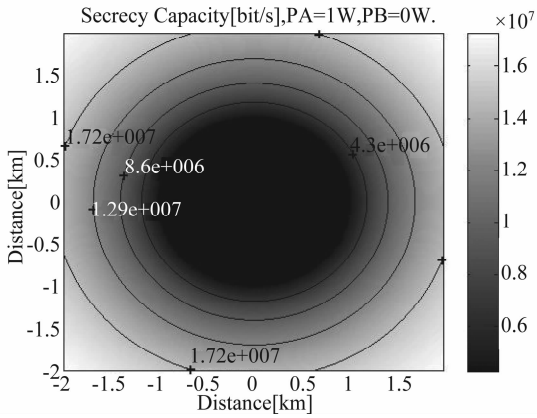



图 4 不发射人工噪声，单天线 Eve

Fig. 4 without AN, single antenna Eve

进一步仿真了多天线 Eve 的场景。图 6 显示了 4 天线 Eve 的保密区域图。图 7 中，考察了 Eve 分别处于(-0.5,0.5)，(0,0.5)，(0.8,0.5)，和(1,0.5)位

置时的保密容量。横坐标为 Eve 的天线数目。可以看到保密容量随着 Eve 天线数目增加而减小,然而若 Eve 处于保密区域,保密容量减小到一定程度将不再变化。此现象说明了 Eve 采取增大天线数目的策略已经无法使保密容量减小,因为天线数目的增多也会接收到更多的人工噪声干扰。

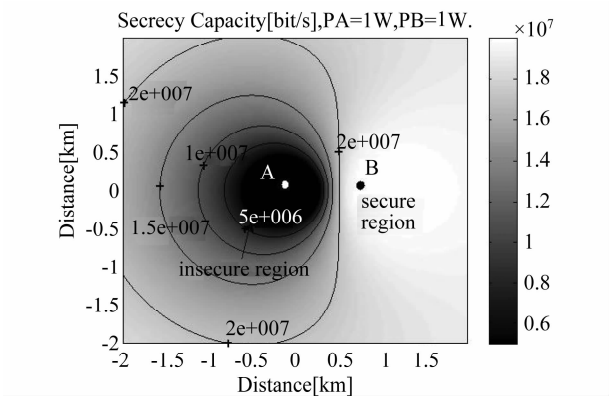



图 5　发射人工噪声,单天线 Eve

Fig. 5　With AN, single antennas Eve

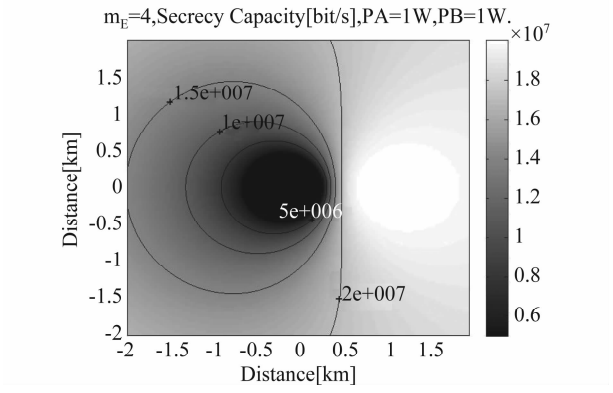



图 6　发射人工噪声,4 天线 Eve

Fig. 6　With AN, 4 antennas Eve

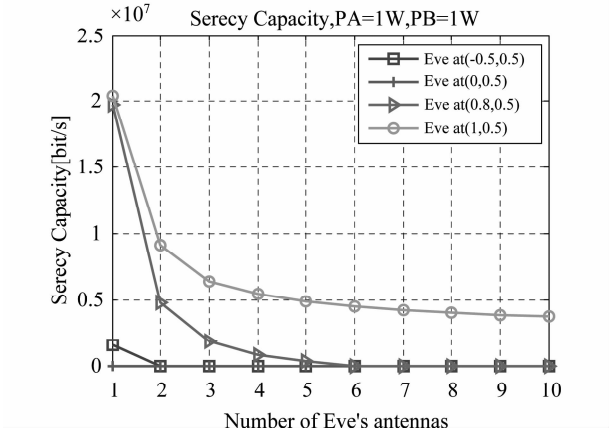



图 7　多天线 Eve 处于不同位置的保密容量

Fig. 7　Eve with multi-antenna at fixed positions

## 5　结论

本文提出了一种基于接收端人工噪声实现物理层安全的方法。并基于地理位置信息提出了保密区域的新概念来评估物理层安全性和指导安全机制的设计。最小化保密区域面积可以作为一种新的物理层安全设计准则。本文对所提算法进行了保密容量和保密区域分析。分析和仿真结果显示所提算法在实际参数设置中能够获得高的安全性能,尤其能够较好的对抗合法接收者附近的窃听者。所提算法还能够有效对抗多天线窃听者。

### 参考文献

[1] A. D. Wyner, The wiretap channel[J], Bell Syst. Tech. J, 1975, 54: 1355-1387.

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages[J], IEEE Trans. Inform. Theory, vol. IT-24, no. 3, May 1978: 339-348.

[3] F. Oggier and B. Hassibi, The secrecy capacity of the MIMO wiretap channel[C], in IEEE Int. Symp. Information Theory (ISIT), Toronto, ON, Canada, 2008: 524-528.

[4] Y. Liang, H. V. Poor, and S. Shamai (Shitz), Secure communication over fading channels[J], IEEE Transactions on Information Theory, Jun, 2008, 54(6): 2470-2492.

[5] S. Goel and R. Neg, Guaranteeing Secrecy using Artificial Noise[J], IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, 2008, 7: 2180-2189.

[6] W. C. Liao, T. H. Chang, W. K. Ma, et al., Joint transmit beamforming and artificial noise design for QoS discrimination in wireless downlink[C], presented at the ICASSP, 2010.

[7] Q. Haohao, C. Xiang, S. Yin, et al., Optimal Power Allocation for Joint Beamforming and Artificial Noise Design in Secure Wireless Communications[C], in Communications Workshops (ICC), 2011 IEEE International Conference on, 2011: 1-5.

[8] 罗文宇,金梁,黄开枝. 保障无线物理层安全的不适定理论与应用[J]. 信号处理,2011,27(11):1749-1756.
Luo W. Jin L, Huang K.. III-Posed Theory and Applications for Guaranteeing the Security of Wireless Physical Layer [J], Signal processing, 2011, 27(11): 1749-1756 (in Chinese)

[9] M. Ghogho and A. Swami, Physical-layer secrecy of MI-

MO communications in the presence of a Poisson random field of eavesdroppers[C], presented at the IEEE ICC Workshop on Physical Layer Security, 2011.

[10] L. Wei-Cheng, C. Tsung-Hui, M. Wing-Kin, et al., QoS-Based Transmit Beamforming in the Presence of Eavesdroppers: An Optimized Artificial-Noise-Aided Approach [J], Signal Processing, IEEE Transactions on, 2011, 59: 1202-1216.

[11] M. Jainy, J. I. Choiy, T. M. Kim, et al., Practical, Real-time, Full Duplex Wireless[C], presented at the MobiCom, Las Vegas, Nevada, USA., 2011.

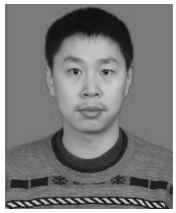
[12] S. W. Kim, Y. J. Chun, and S. Kim., Co-channel interference cancellation using single radio frequency and baseband chain[J], IEEE Transactions on Communications, 2010, 58(7): 2169-2175.

[13] F. O. a. B. Hassibi, The Secrecy Capacity of the MIMO Wiretap Channel[J], IEEE Trans. Inform. Theory, 2011, 57(8): 4961-4972.

[14] I. E. Telatar, Capacity of multi-antenna Gaussian channels [J], Eur. Trans. Telecommun., 1999, 10(6): 585-596.

[15] 3GPP and T. 25.814V7.0.0, Technical Specification Group Radio Access Network: Physical-Layer Aspects for Evolved UTRA (Rel. 7), in ed, 2007.

## 作者简介



李 为(1984-),男,湖北当阳人,国防科学技术大学博士研究生,研究方向为通信信号处理,无线通信网络。
E-mail: liwei. nudt. cn@ gmail. com

陈 彬(1988-)男,江西上饶人,国防科学技术大学博士研究生,研究方向为通信信号处理,无线通信网络。
E-mail: lierbency@ 126. com

魏急波(1967-),男,湖北汉川人,教授,国防科学技术大学博导,IEEE 会员,研究方向为软件无线电技术,通信信号处理,无线通信网络。E-mail: wjbhw@ nudt. edu. cn

熊春林(1980-),男,湖北麻城人,国防科学技术大学讲师,博士,研究方向为通信信号处理。
E-mail: xchlzju@ nudt. edu. cn

张晓瀛(1980-),女,湖南人,国防科学技术大学讲师,博士,研究方向为通信信号处理。E-mail: zxy_nudt@ 163. com