基于多径信道随机延时的物理层全算法*

庞宏伟，王雪明，吉 江，李翔宇，金 梁
（国家数字交换系统工程技术研究中心，郑州 450002）

摘 要：针对无线通信遇到的第三方窃听问题，利用无线通信系统信道多径延时丰富的特征，提出了一种保证物理层安全传输的加密算法。该算法中，数据发送用户根据估计的多径延时信息随机提前符号发送时间，使授权用户的同步位置有较强的多径信号到达，授权接收用户在保持同步状态不变的情况下可以正常接收信息。而窃听用户具有不同的信道多径延时特征，接收到的信号幅度和相位会随机变化，难以进行同步跟踪，因此接收到的符号会产生大量的误码，从而提高授权用户之间的安全传输性能。仿真结果表明，该算法能有效提高窃听方的误码率，提高授权用户通信的安全性，从而可在多径环境中有效保证物理层通信安全。

关键词：无线通信系统；物理层安全；信道多径信息；延时信息；同步；误码率
中图分类号：TP391 **文献标志码**：A **文章编号**：1001-3695(2012)08-3039-03
doi:10.3969/j.issn.1001-3695.2012.08.061

Security method of wireless physical layer security based on multipath channel random delay

PANG Hong-wei, WANG Xue-ming, JI Jiang, LI Xiang-yu, JIN Liang
(*National Digital Switching System Engineering & Technological Research Center*, *Zhengzhou* 450002, *China*)

Abstract: For the wire-tapping in wireless communication system, this paper presented an encrypting method based on channel multipath delay-time information to ensure the security of physical layer in wireless communication system. In this method, the transmitter made the time to transmit symbol random with channel multipath delay-time information that estimated, and made the received signal of legitimate receiver stronger at the synchronization location. So the legitimate could receive the information normally. While the received signal of eavesdropper turned random for different channel information, such as phase and range. Then the eavesdropper couldn't recover the information with the random received signal, and the error probability was high, which increased the security of legitimate receiver. The simulations show that the method can keep the eavesdropper's error probability at a high level, so as to increase the system security. Finally, it comes to the conclusion that this method can ensure the security of physical layer in wireless communication system with channel multipath.

Key words: wireless communication system; physical layer secrecy; channel multipath information; delay-time information; synchronization; error probability

0 引言

由于无线通信媒介的广播特性，安全威胁无处不在。日益复杂的无线通信网络使传统的密钥加密体制复杂得难以实际应用，基于信息论的物理层安全问题研究逐渐被人们重视。

1975 年 Wyner 提出了 wire-tap 窃听模型，首次讨论了无线信道对通信系统安全性的影响，并引入了保密容量来衡量系统的安全性能[1]。按照 wire-tap 模型，Csiszár 等人[2]推导出广播信道下，授权用户的保密容量。文献[1,2]的研究引发了利用信息论讨论各种场景 wire-tap 窃听模型的热潮。文献[3]讨论了存在加性高斯白噪声(adding Gaussian white noise, AWGN)情况下的 wire-tap 窃听模型的保密容量。由于 AWGN 在无线通信研究中的基础地位，wire-tap 窃听模型随后被进一步发展。2008 年，文献[4]对已有的 wire-tap 窃听模型下不同应用场景的保密容量、安全信道编码方式等方面做了总结。Wire-tap 模型为无线物理层加密提供了较好的解决思路。

随着研究的不断深入，出现了一些利用无线信道实现物理层安全传输的算法。文献[5,6]采用了向窃听用户发送人工噪声的方式，对窃听用户进行干扰。文献[7,8]提出随机发送天线阵的物理层安全通信系统，根据发射天线的信道信息随机设置发射天线的增益系数，使合法用户的接收信号保持稳定，容易接收，而窃听用户的接收信号随机改变，无法正确解调。文献[9]改进了随机天线阵增益系数的设计方法，提高了期望用户的功率利用率。这几种方法都是在多天线系统中通过随机设置天线的发射增益来实现对授权用户的加密。除此之外，在中继系统中也出现了较多的利用物理层实现安全传输的算法。文献[10,11]分别采用接收者发送干扰信号和外部节点协助干扰的方法，对非可信中继进行适当的干扰，并且计算了这两种方法的保密容量。前一种方法要求授权用户有较强的上行传输能力，后一种方法需要干扰节点掌握全局信道状态信息，并拥有较强的计算能力。文献[12]在此基础上提出了一

收稿日期：2011-12-20 **修回日期**：2012-02-14 **基金项目**：国家自然科学基金资助项目(61171108)

作者简介：庞宏伟(1986-)，男，辽宁锦州人，硕士研究生，主要研究方向为移动通信(panghw2011@gmail.com)；王雪明(1968-)，女，四川资中人，副教授，主要研究方向为信号与系统；吉江(1983-)，男，河南南乐人，博士研究生，主要研究方向为移动通信及物理层安全；李翔宇(1987-)，男，河南周口人，硕士研究生，主要研究方向为移动通信；金梁(1969-)，男，北京人，教授，博导，主要研究方向为移动通信、无线物理层安全.

种更明确、更优化的干扰权值计算方法,但并没有讨论中继非可信的场景。文献[13]提出了一个更均衡的场景,由于中继节点本身也有私密信息需要传输,建立了协作中继广播信道模型。文献[14]提出了一种窃听用户作为中继节点提供错误信道特征参数的场景,详细计算了这种情况下的保密容量域。文献[15]研究了中继节点协助窃听用户干扰正常接收者的情况。可见,目前的安全传输方法大多是通过冗余的天线或者中继节点实现的,很少有关于点对点系统物理层安全传输算法的研究,无线通信系统信道时域延时特征显著,适当地加以利用,从时域角度研究物理层安全传输算法具有重要意义。

针对已有算法的不足,本文根据无线通信系统的多径延时信息,设计物理层加密算法,以实现无线系统信息的安全传输。该算法根据系统信道时域延时特征,提出一种随机提前发送符号位置的物理层安全传输算法。

1 系统模型

本文提及的无线通信安全系统模型主要包括以下三方:Alice、Bob 和 Eve,如图 1 所示。其中,Alice 是数据发送用户,Bob 是授权接收用户,Eve 作为被动窃听用户只接收信息,不发送任何信息。

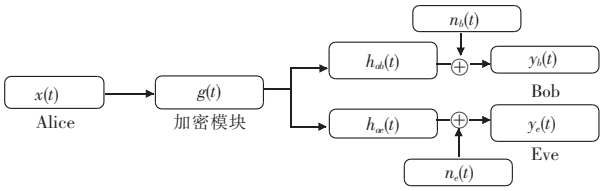


图 1 通信系统模型

在实际通信中,Bob 首先向 Alice 发送未加密的请求信息,该请求信息同时包含用于信道估计的训练序列。Alice 接收请求,并根据接收到的训练序列完成与 Bob 的符号同步,同时估计主信道(发送用户与授权用户之间的信道)时域多径延时特征。根据互易定理,在信道慢变的情况下,可以认为 Alice 和 Bob 之间的收发信道相同。因此 Alice 可以根据估计到的信道时域多径特征对即将发送给 Bob 的信息进行加密。加密模块是根据 Alice 和 Bob 之间的信道多径延时特征设计的,加密后的信息经过主信道后,Bob 会接收到一个相对稳定的信号,因此 Bob 既无须知道 Alice 是如何加密的,也无须知道主信道信息就可以完成正常解密,获得通信内容。而窃听信道(发送用户与窃听用户之间的信道)与主信道的特征不同,Eve 接收到的是一个趋于随机变化的加密信号,无法正确解出 Alice 发送的信息,难以实现窃听。

图 1 中 $x(t)$为 Alice 的发送信号;$h_{ab}(t)$是主信道的冲击响应;$h_{ae}(t)$是窃听信道的冲击响应;$g(t)$为加密模块,主要用于与 $h_{ab}(t)$共同形成稳定的信道,便于 Bob 接收信息,而与 $h_{ae}(t)$共同形成随机快变的信道,防止 Eve 窃听;$n_b(t)$和 $n_e(t)$分别为主信道和窃听信道的加性高斯白噪声,并且 $n_b(t) \sim N(0,\sigma_b^2)$、$n_e(t) \sim N(0,\sigma_e^2)$。由图 1 可以得到,Bob 和 Eve 的接收信号分别表示为

$$\begin{aligned} y_e(t) &= x(t) * g(t) * h_{ae}(t) + n_e(t) \\ y_b(t) &= x(t) * g(t) * h_{ab}(t) + n_b(t) \end{aligned} \tag{1}$$

其中,符号 * 表示卷积运算。

由于地理位置上的不同,信道冲击响应 $h_{ab}(t)$和 $h_{ae}(t)$会有很大的差异,相位、延时、幅度衰落、多普勒频移等特征均不相同,充分利用这些差异可以设计安全传输算法。本系统中,发送信号经过加密处理,Eve 接收到的是随机变化的信号。而且,在通信过程中,Alice 是不发送训练序列的,Eve 难以实现接收同步完成信号跟踪,这样会进一步保证系统的安全性。

2 算法设计

本文根据信道的多径延时特征设计加密算法。

假设主信道冲击响应为

$$h_{ab}(t) = \sum_{n=1}^{N} \alpha_n \delta(t-\tau_n) \tag{2}$$

其中:τ_n 为第 n 条路径的延时;α_n 为对应路径的衰落系数;$n = 1,2,\cdots,N$。

假设窃听信道冲击响应为

$$h_{ae}(t) = \sum_{m=1}^{M} \beta_m \delta(t-\upsilon_m) \tag{3}$$

其中:υ_m 为第 m 条路径的延时;β_m 为对应路径的衰落系数;$m = 1,2,\cdots,M$。

根据估计到的多径延时特征,Alice 随机选择某一条路径的延时 $\tau_r(r \in \{1,2,\cdots,N\})$,在发送符号时,将发送时间随机提前 τ_r。这样在同步位置,Bob 接收到的为第 r 条有效路径的信号。Bob 可以根据接收到的信号恢复 Alice 的发送信息。而 Eve 由于与 Bob 的具有不同的信道多径延时特征,其在同步位置处接收不到有效的多径信号,并且由于延时是随机选择不断变化的,Eve 难以实现反卷积,会有很高的误码率,不能正确地恢复符号,难以解出 Alice 发送的信息。

根据估计得到的多径延时信息,进行加密处理。随机选择的延时为

$$g(t) = \delta(t+\tau_r) \tag{4}$$

其中:$\tau_r \in \{\tau_n, n = 1,2,\cdots,N\}$。

在保证没有码间串扰的情况下,根据随机选择多径延时,将发送端信号脉冲的位置随机提前。主信道的时域特征可以等效表示为

$$\begin{aligned} h_{AB}(t) &= g(t) * h_{ab}(t) = \delta(t+\tau_r) * \sum_{n=1}^{N} \alpha_n \delta(t-\tau_n) = \\ &\sum_{n=1}^{N} \alpha_n \delta(t-\tau_n+\tau_r) \end{aligned} \tag{5}$$

当发送数据为 $x(t)$时,Bob 接收到的信号可以表示为

$$\begin{aligned} y_b(t) &= x(t) * h_{AB}(t) + n_b(t) = x(t) * \sum_{n=1}^{N} \alpha_n \delta(t-\tau_n+\tau_r) + \\ &n_b(t) = \sum_{n=1}^{N} \alpha_n x(t-\tau_n+\tau_r) + n_b(t) \end{aligned} \tag{6}$$

经过同步之后,则 Bob 接收到的信号可以表示为

$$\tilde{y}_b(t) = \sum_{n=r}^{N} \alpha_n x(t-\tau_n+\tau_r) + n_b(t) \tag{7}$$

类似地,可以得到 Eve 的接收信号为

$$\begin{aligned} y_e(t) &= x(t) * h_{AE}(t) + n_e(t) = x(t) * \sum_{m=1}^{M} \beta_m \delta(t-\upsilon_m+\tau_r) + \\ &n_e(t) = \sum_{m=1}^{M} \beta_m x(t-\upsilon_m+\tau_r) + n_e(t) \end{aligned} \tag{8}$$

经过同步之后,则 Eve 接收到的信号可以表示为

$$\tilde{y}_e(t) = \sum_{m=m_r}^{M} \beta_m x(t-\upsilon_m+\tau_r) + n_e(t) \tag{9}$$

其中:$m_r = \{x, \min(\upsilon_x) \geqslant \tau_r\}$。

随机选择延时发送的符号如图 2 所示。这里以 5 条多径举例,其中实线位置为正常的发送位置,而第一条虚线表示实

际的发送位置。通过这种根据信道多径延时随机提前发送脉冲时间的方法,在发送信号经过多径信道后,在 Bob 的同步位置会接收到所选择的某一路有效的多径信号,因此 Bob 无须重新与 Alice 进行同步就可以完成信号的接收和解调过程。而窃听信道的多径延时与 Bob 不同,经过多径信道之后,到达 Eve 同步位置处的就可能没有信号或者幅度很弱的信号,Eve 无法恢复信号,必须重新进行同步,而 Alice 在发送有用的数据信息时,每次都会根据信道多径信息随机选择发送时间,这样 Eve 无法再进行同步,之前根据训练序列进行的同步也变得毫无意义,在没有进行同步的情况下,Eve 会有较高的误码率,难以根据接收信号恢复 Alice 的发送信息,不能实现窃听。

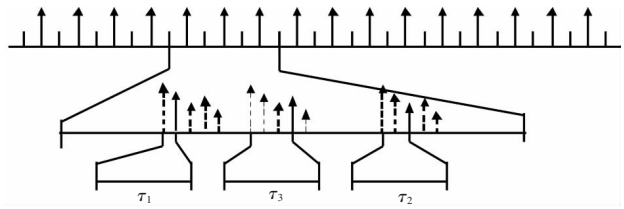


图 2　随机控制发送延时时间示意

这种加密算法,由于发送每个脉冲时只选择了其中的一个路径进行信息的传输,会带来能量的损失和信噪比的降低。这其实是可以做一些补偿的,可以利用多个符号周期重复发送同一个符号信息,来获得信噪比的改善,这样授权用户 Bob 端的接收信息可以表示为

$$y_b(t)=\sum_{k=1}^{N_C}\left(\sum_{n=1}^{N}\alpha_{kn}x(t-\tau_{kn}+\tau_{kr})+n_{kb}(t)\right) \tag{10}$$

其中:N_C 为发送的脉冲数,α_{kn}为第 k 个发送脉冲第 n 条路径的衰减系数;τ_{kr}为第 k 个发送脉冲的随机提前时间;$n_{kb}(t)$为对应的高斯白噪声。

这样,通过接收端对 N_C 个接收脉冲的处理,就可以大大改善接收端的信噪比,同时降低 Bob 端的误码率。不过在改善信噪比的同时,会带来传输速率的损失,当然在对传输速率要求不高、对安全传输要求较高时,以牺牲传输速率换取传输的安全性还是值得的,这需要在实际中做好合适的折中。

另一种提高功率利用率的方法是选择具有最大幅度的路径进行脉冲提前发送。这样,随机延时 τ_{krm}就是幅度最大的路径对应的延时。则授权用户 Bob 端的接收信息可以表示为

$$y_b(t)=\sum_{k=1}^{N_C}\left(\sum_{n=1}^{N}\alpha_{kn}x(t-\tau_{kn}+\tau_{krm})+n_{kb}(t)\right) \tag{11}$$

其中:$\tau_{krm}=\max\{\|\alpha_{kn}\|,n=1,\cdots,N\}$。

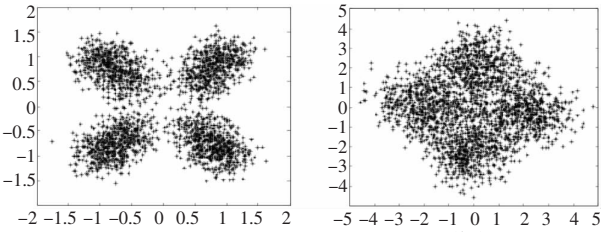
这种改进算法适合使用在瑞利频率选择性衰落信道的环境中,因为这种情况没有明显的视距路径、主径,各条路径幅度变化较大,幅度最大路径所对应的延时不断变化。而对于具有视距路径的赖斯信道,具有明显的幅度最强的主径,主径的延时在一定时间内变化也是有限的,随机延时就失去意义,不能达到加密的效果。

算法对码元持续时间也与常规系统有所不同。假设系统的延时扩展为 T_P,在本算法中,由于将符号发送时间随机提前,最大提前时间差不多是一个符号的持续时间,因此需要保证码元持续时间 $T_M\geq 2T_P$ 才能无码间串扰。而在普通的通信系统中,只要求码元持续时间 $T_M\geq T_P$。本系统在获得安全传输性能的同时降低了信息的传输速率。

3　仿真分析

按照设计的算法,进行仿真验证。仿真过程中,假设信道有 5 条多径路径,由于幅度太小不适合传输,选择每条路径的幅度在 1 ~ 0.4 之间均匀分布,路径延时在 0 ~ 1T_P 之间均匀分布,每次仿真实验传输 1 000 个 QPSK 符号,并加入高斯白噪声。分别对 Bob 和 Eve 的接收信号的星座图以及误码率进行了仿真实验。

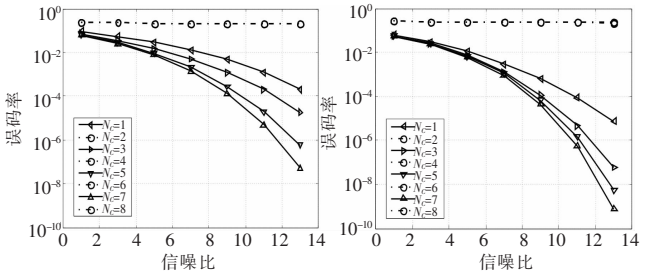
图 3 是 SNR = 10 dB 时,Bob 和 Eve 接收信号的星座图。其中:(a)为 Bob 的接收星座图,还保持着基本的形状,四种信号相对分离,只是由于随机多径的选择,星座分布接近椭圆形,对正常接收不会产生太大的影响;(b)为 Eve 的接收星座图,可以看出星座图已经明显被置乱,四种信号相互参杂在一起,已经分不出明显的界限,难以实现区分完成数据解调。



(a) Bob 接收星座　　(b) Eve 接收星座

图 3　接收信号星座

图 4(a)为随机选择多径发送信息的误码率曲线,并比较利用多个符号周期重复发送同一符号时的误码率性能。圆圈为 Eve 的误码率曲线,可以看出,虽然符号周期 N_C 不断提高,但是 Eve 的误码率几乎没有变化,一直处于较高的状态,这样 Eve 难以正常地恢复信息。三角符号为 Bob 的误码率曲线,可以看出,相对于 Eve,Bob 的误码率明显要低一些,并且随着符号周期 N_C 的提高,Bob 的误码率不断降低。



(a) 随机选择多径　　(b) 选择幅度最大径

图 4　误码率曲线

图 4(b)为选择强度最大多径发送信息的误码率曲线,并比较利用多个符号周期重复发送同一符号时的误码率性能。圆圈为 Eve 的误码率曲线,可以看出,虽然符号周期 N_C 不断提高,但是 Eve 的误码率几乎没有变化,一直处于较高的状态,这样 Eve 难以正常地恢复信息。三角符号为 Bob 的误码率曲线,可以看出,相对于 Eve,Bob 的误码率明显要低一些,并且随着符号周期 N_C 的提高,Bob 的误码率不断降低。

从图 4(b)也可以看出,在选择幅度最大多径发送符号时,Bob 的误码率比完全随机选择多径时明显有所降低,这是由于接收信噪比的相对提高而得到的。在图 4 中还可以看出,随着 N_C 的增大,误码率不断改善,但是改善的空间逐渐变小,因此,不能通过无限地重复增加发送符号周期降低误码率。

4　结束语

本文提出了一种利用信道时域多径延时特性的安全传输算法。该算法中,发送端通过估计通信请求 (下转第 3045 页)

4　结束语

为有效预测网络安全威胁态势的变化趋势,本文采用基于 ARIMA 模型的网络安全威胁态势的预测方法,其实验结果表明:该方法的预测准确性接近 96.7%,具有良好的稳健性,可以为实际网络安全威胁态势的预测提供一定的理论基础;但是该方法对随机趋势的预测存在不足,这也是日后完善该方法的重点。

参考文献:

[1] 中国互联网络信息中心. 第 28 次中国互联网络发展状况统计报[EB/OL]. (2011-07)[2011-12]. http://www. cinnic. cn. research/bgxz/.

[2] QIN Xin-zhou, LEE Wen-ke. Statistical causality analysis of infosec alert data[C]//Proc of Recent Advances in Intrusion Detection. Pittsburgh: Goos G, 2003:73-93.

[3] POTTER B. Software & network security[J]. Network Security, 2004, 2004(10):4-5.

[4] TIM B. Multisensor data fusion for next generation distributed intrusion detection systems[C]//Proc of IRIS National Symposium Draft. 1999:24-27.

[5] JASON. A technique independent fusion model for network intrusion detection[C]//Proc of Midstates Conference on Undergraduate Research in Computer and Mathmatics. 2005:13-19.

[6] PORRAS P, FONG M, VALDES A. A mission-impact-based approach to INFOSEC alarm correlation[C]//Proc of the 5th International Symposium on Recent Advanced in Intrusion System. 2002:95-114.

[7] HARRI S, QU Guang-zhi, DHARMAGADDA T, *et al*. Impact analysis of faults and attacks large-scale network[J]. IEEE Security & Privacy, 2003, 1(5):49-54.

[8] 萧海东. 网络安全态势评估与趋势感知的分析研究[D]. 上海:上海交通大学,2007.

[9] BISHOP C M. Neural networks for pattern recognition[M]. London: Oxford University Press, 1995.

[10] 程文聪. 面向大规模网络安全态势分析的时序数据挖掘关键技术研究[D]. 长沙:国防科技大学,2010.

[11] 李玲娟. 数据挖掘技术在入侵检测系统中的应用研究[D]. 苏州:苏州大学,2008

[12] HAN Jia-wei, MICHELINE K. Data mining: concepts and techniques[M]. San Francisco: Morgan Kaufmann Publisher, 2001.

[13] ZHANG Yong, TAN Xiao-bin, XI Hong-shen. A novel approach to network security situation awareness based on multi-perspective analysis[C]//Proc of International Conference on Computational Intelligence and Security. 2007:768-772.

[14] 韦勇. 网络安全态势评估模型研究[D]. 合肥:中国科学技术大学,2009.

[15] 陈秀真,郑庆华,管晓宏,等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报,2006,17(4):885-897.

[16] 张世永. 网络安全原理与应用[M]. 北京:科学出版社,2003.

[17] 张永铮,云晓春,胡铭曾. 基于特权提升的多维量化属性弱点分类法的研究[J]. 通信学报,2004,25(7):107-114.

[18] GEORGE E P B, GWILYM M J, GREGORY C R. Time series analysis: forecasting and control[M]. 3rd ed. London: Prentice-Hall, 1994.

[19] Honey Project. Know your enemy: statistical[EB/OL]. (2001-07-22). http://old. honeynet. org/papers/stats.

[20] Snort Project. Snort users manual[EB/OL]. (2011-12-07)[2011-12-25]. http://manual. snort. org.

(上接第 3041 页)用户信道的多径延时信息,并根据此信息随机提前发送符号的时间位置,来保证授权接收用户正确地同步接收,而窃听用户由于自然信道不同,难以跟踪同步正确接收。仿真结果表明,该算法能有效提高窃听方的误码率,提高授权用户的安全通信能力。在多径丰富的无线通信环境中,可以有效保证物理层通信安全。

参考文献:

[1] WYNER A D. The wire-tap channel[J]. The Bell System Technical Journal, 1975, 54(8):1355-1387.

[2] CSISZÁR I, KÖNER J. Broadcast channels with confidential messages[J]. IEEE Trans on Information Theory, 1978, 24(5):339-348.

[3] LEUNG S K, CHEONG Y, HELLMAN M E. The Gaussian wire-tap channel[J]. IEEE Trans on Information Theory, 1978, 24(7):451-456.

[4] LIANG Ying-bin, POOR H V, SHAMAI S(Shitz). Information theoretic security[J]. Foundations and Trends in Communications and Information Theory, 2008, 5(4-5):355-580.

[5] NEGI R, GOEL S. Secure communications using artificial noise[C]//Proc of IEEE Vehicle Technology Conference. 2005:1906-1910.

[6] GOEL S, NEGI R. Guaranteeing secrecy using artificial noise[J]. IEEE Trans on Wireless Communication, 2008, 7(6):2180-2189.

[7] LI Xiao-hua, CHEN Mo. Array-transmission based physical-layer security techniques for wireless sensor networks[C]//Proc of IEEE International Conference on Mechatronics & Automation. 2005.

[8] LI Xiao-hua, HWU J. Using antenna array redundancy and channel diversity for secure wireless transmissions[J]. Journal of communications, 2007, 2(3):24-32.

[9] 穆鹏程,殷勤业,王文杰. 无线通信中使用随机天线阵列的物理层安全传输方法[J]. 西安交通大学学报,2010,44(6):62-66.

[10] ZHANG R, SONG L, HAN Z, *et al*. Physical layer security for two way relay communications with friendly jammers[C]//Proc of IEEE Global Telecommunications Conference. 2010:1-6.

[11] HE X, YENER A. Two-hop secure communication using an untrusted relay: a case for cooperative jamming[C]//Proc of IEEE Global Telecommunications Conference. 2008:1-5.

[12] ZHENG G, CHOO L, WONG K. Optimal cooperative jamming to enhance physical layer security using relays[J]. IEEE Trans on Signal Processing, 2011, 59(3):1317-1322.

[13] EKREM E, ULUKUS S. Secrecy in cooperative relay broadcast channels[J]. IEEE Trans on Information Theory, 2011, 57(1):137-155.

[14] MILOSAVLJEVIC N, GASTPAR M, RAMCHANDRAN K. Secure communication using an untrusted relay via sources and channels[C]//Proc of IEEE International Symposium on Information Theory. 2009:2457-2461.

[15] YUKSEL M, LIU X, ERKIP E. A secure communication game with a relay helping the eavesdropper[J]. IEEE Trans on Information Forensics and Security, 2011, 6(3):818-830.