基于信号传播特性的物理层密钥生成方案

胡晓言,金 梁,黄开枝,钟 州,张胜军
(国家数字交换系统工程技术研究中心,河南郑州 450002)

摘 要: 传统基于接收信号强度的物理层密钥生成方案在窃听者靠近合法方时,合法方的密钥易被窃听者获取.针对该问题,在分析密钥误比特率的基础上,提出一种基于信号传播特性的物理层密钥生成方案.方案根据接收信号强度的实测样本估计大尺度衰落模型,提取出多径效应影响下的小尺度参数量化生成密钥.实验结果表明相比于传统方案,本方案在室内环境窃听距离大于0.6倍波长以后,窃听方密钥误比特率大于0.48;在室外环境窃听距离大于1倍波长后窃听方密钥误比特率为0.47,实现了安全可靠的物理层密钥生成.

关键词: 物理层安全;密钥生成;信号传播特性;接收信号强度;密钥误比特率
中图分类号: TN918.91 **文献标识码:** A **文章编号:** 0372-2112(2019)02-0483-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2019.02.032

Physical Layer Secret Key Generation Scheme Based on Signal Propagation Characteristics

HU Xiao-yan, JIN Liang, HUANG Kai-zhi, ZHONG Zhou, ZHANG Sheng-jun
(*National Digital Switching System Engineering & Technological R&D Center, Zhengzhou, Henan* 450002, *China*)

Abstract: The existing physical layer secret key generation scheme is not sufficiently secure when the eavesdropper keeps close to the legitimate user to get the correlated channel characteristics. To solve the problem, this paper analyzes the secret key bit error rate and proposes a physical layer secret key generation scheme based on signal propagation characteristics. We calculate the large scale fading model which parameters is fitted by the measured sample, in order to get the small scale parameter of received signal strength indication under the effect of multipath fading to quantify into binary secret bit. The experimental results show that compared with the traditional scheme, in the indoor environment, after eavesdropping distance is greater than 0.6 wavelength, the eavesdropper key bit error rate is greater than 0.48. And in the outdoor environment, after the eavesdropping distance is greater than 1 wavelength, the eavesdropper key bit error rate is 0.47. Secure and reliable physical layer secret key generation is achieved.

Key words: physical layer security; secret key generation; signal propagation characteristics; received signal strength indicator(RSSI); secret key bit error rate

1 引言

随着无线通信技术的迅速发展,其安全问题也备受关注[1].尤其对于资源受限的通信节点,现有基于计算复杂度的传统加密技术开销较大,难以应用.近年来,物理层密钥生成技术受到了人们的重视,通信双方利用无线信道固有的时空变化性和短时互易性,将信道特征参数作为随机源生成密钥[2],在正常通信的同时免去了密钥分发,是解决无线通信安全难题的理想途径.

无线信道具有丰富的特征信息,其中接收信号强度(receive signal strength indicator,RSSI)变化快速且易于测量,是密钥生成技术常用的随机源[3,4].在已有的研究中,Aono T[5]等人利用波束成型技术人工加快RSSI的变化,提高了密钥生成速率.Suman Jana[6]等人提出自适应的密钥生成方案ASBG,将RSSI划分到多个区间进行量化.Ye C[7]等人提出了Level-Crossings方案,并基于802.11协议开发了实验平台,分别利用信道脉冲响应和RSSI生成了密钥.Zhu X[8]等人在文献[6]的

收稿日期2017-09-29;修回日期:2018-05-03;责任编辑:郭游
基金项目:国家"863"高技术研究发展计划(No.2015AA01A708);国家自然科学基金(No.61471396,No.61521003,No.61601514,No.61501516)

基础上进行了改进,应用于车联网通信.

现有方案多假设窃听者与合法方的信道特征参数不相关[3~9].然而无线信号的传播受路径损耗和遮挡的影响,在接收机一定范围内测得的 RSSI 具有相似的大尺度衰落特性.当窃听者靠近合法方时,可以窃听到与合法方相关的 RSSI,合法方密钥存在被预测的风险[10].

针对以上问题,本文首先分析了基于 RSSI 的密钥生成信道模型,然后分析了现有方案的密钥误比特率,在此基础上提出一种基于信号传播特性的物理层密钥生成方案,最后在实际环境中测试了方案的安全性.

2 系统模型与问题分析

2.1 信道模型

本文考虑的密钥生成信道模型如图 1 所示,*Alice* 和 *Bob* 为合法通信双方,两者互相发送探测信号并测量 *RSSI*,得到相关的测量值用于密钥生成.不失一般性,假设被动窃听者 *Eve* 可以窃听到 *Alice* 发送的探测信号,并测量得到 *RSSI*.本模型中三者均配备单天线.

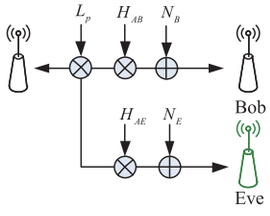


图1 信道模型

如图 1 所示,H_{AB}、H_{AE}分别表示 Alice 与 Bob 之间的合法信道和 Alice 与 Eve 之间的窃听信道的小尺度衰落,P_s、L_P 分别表示探测信号发送功率和信号的大尺度衰落.为了便于分析,本文模型中假设 Alice 可以准确测量 Bob 发送探测信号的信号强度值 X,而 Bob 和 Eve 的 RSSI 测量值 Y 和 Z 受到噪声 N_B 和 N_E 的影响,三者的 *RSSI* 可表示为:

$$\begin{cases} X = P_s \cdot L_P \cdot H_{AB} \\ Y = X + N_B \\ Z = P_s \cdot L_P \cdot H_{AE} + N_E \end{cases} \tag{1}$$

本文模型考虑窃听者 Eve 靠近合法方 Bob,但距离大于半个波长,即小尺度衰落 H_{AB}与 H_{AE}相互独立[11],大尺度衰落 L_P 相同.其中,小尺度衰落 H_{AB}、H_{AE}服从均值为 0 方差为 σ^2 的对数高斯分布.大尺度衰落为关于信号传播距离 x 的函数,且 Alice、Bob 的距离与 Alice、Eve 的距离在任意时刻均为 x(单位 m).本文忽略阴影衰落的影响,将大尺度衰落 L_P 建模为对数距离衰减模型,距离 x 处的大尺度衰落可表示如下[12]:

$$L_P(x) = -L_P(x_0) - 10\eta \log_{10}(x) \tag{2}$$

式中 η 为大尺度衰落系数,$L_P(x_0)$为近地参考距离 x_0 处的信号强度衰减,假设参考距离 $x_0 = 1\text{m}$,为方便表示令 $P_0 = 10\log(P_s/1\text{mW}) - L_P(x_0)$.现有研究[6~8]大多以 dBm 单位设计基于 RSSI 的量化方法,因此对式(1)取对数表示为:

$$\begin{cases} y_A(x) = P_0 - 10\eta\log_{10}(x) + h_{AB} \\ y_B(x) = y_A(x) + n_B \\ y_E(x) = P_0 - 10\eta\log_{10}(x) + h_{AE} + n_e \end{cases} \tag{3}$$

其中,$y_A(x)$、$y_B(x)$和 $y_E(x)$分别表示距离为 x 时 Alice、Bob 和 Eve 的 RSSI 测量值(单位 dBm),h_{AB}和 h_{AE}表示取对数后的小尺度衰落.相应地,Bob 和 Eve 的 RSSI 测量误差 n_B、n_E 服从 $\mathcal{N}(0,\sigma_n^2)$.Alice 和 Bob 在不同距离处互发 N 次探测信号后,Alice、Bob 和 Eve 测量得到的 RSSI 可以表示为$\{y_A(x_i)\mid i\in[1,2,\cdots N]\}$、$\{y_B(x_i)\mid i\in[1,2,\cdots N]\}$和$\{y_E(x_i)\mid i\in[1,2,\cdots N]\}$.此时,合法通信双方 Alice 和 Bob 可以将 $y_A(x)$和 $y_B(x)$作为相关的随机源生成密钥.在本文中,我们考虑最坏的情况,Eve 采用同样的密钥生成方案,利用测量值 $y_E(x)$生成密钥.

2.2 安全性分析

为了准确衡量密钥生成方案的安全性,本小节首先分析三者量化后的密钥误比特率.考虑传统均值量化方法,合法双方和窃听者均以 RSSI 测量值的均值为门限进行 1 比特量化.由于 Alice、Bob 和 Eve 接收信号的大尺度衰落相同,因此 RSSI 的均值也是相同的,均值量化门限 Q 可表示如下:

$$Q = \sum_{i=1}^{N} y_A(x_i) = \sum_{i=1}^{N} y_B(x_i) = \sum_{i=1}^{N} y_E(x_i) \tag{4}$$

合法双方 Alice 和 Bob 的密钥误比特率为:

$$\begin{aligned} P_e^{AB} &= \Pr(y_A(x)\geq Q, y_B(x) < Q) \\ &\quad + \Pr(y_A(x) < Q, y_B(x)\geq Q) \end{aligned} \tag{5}$$

首先以 $L_P(x) - Q \geq 0$ 为例进行分析,将式(3)、(4)带入式(5)中的第一项,并根据全概率公式展开得:

$$\begin{aligned} &\Pr(y_A(x)\geq Q, y_B(x) < Q) \\ &= \Pr(y_B(x) < Q \mid y_A(x)\geq Q)\Pr(y_A(x)\geq Q) \\ &= \left[\int_0^{+\infty} \Pr(h_{AB} + n_B + \varepsilon < 0 \mid h_{AB} + \varepsilon = t)\cdot \right. \\ &\quad \left. \Pr(h_{AB} + \varepsilon = t)\,\mathrm{d}t \right] \Pr(y_A(x)\geq Q) \\ &= \left[\int_{-\infty}^{+\infty} \operatorname{erfc}\left(\sqrt{\frac{(t+\varepsilon)^2}{2\sigma_n^2}}\right)\exp\left(-\frac{t^2}{2\sigma^2}\right)\mathrm{d}t\right]\cdot \\ &\quad \frac{1}{2\sqrt{2\pi\sigma^2}}\Pr(y_A(x)\geq Q) \end{aligned} \tag{6}$$

式中 $\operatorname{erfc}(\cdot)$为互补误差函数.由上式易知,当 $L_P(x) - Q < 0$ 时结果不变.同理,对于 P_e^{AB} 的第二项有:

$$\Pr(y_A(x) < Q, y_B(x)\geq Q)$$

$$= \left[\int_{-\infty}^{+\infty} \mathrm{erfc}\left(\sqrt{\frac{(t+\varepsilon)^2}{2\sigma_n^2}}\right)\exp\left(-\frac{t^2}{2\sigma^2}\right)\mathrm{d}t\right]\cdot \frac{1}{2\sqrt{2\pi\sigma^2}}\Pr(y_A(x)<Q) \tag{7}$$

最后,合并式(6)和式(7)可得:

$$P_e^{AB} = \frac{1}{2\sqrt{2\pi\sigma^2}}\int_{-\infty}^{+\infty}\mathrm{erfc}\left(\frac{|t+\varepsilon|}{\sqrt{2\sigma_n^2}}\right)\cdot\exp\left(-\frac{t^2}{2\sigma^2}\right)\mathrm{d}t \tag{8}$$

不失一般性,以 Alice 为例分析合法方与窃听者的密钥误比特率. 由于小尺度衰落 h_{AB}、h_{AE}、n_e 相互独立,且 ε 为常数,因此 Alice、Eve 的误比特率 P_e^{AE} 可表示为:

$$\begin{aligned}P_e^{AE} &= \Pr(y_A(x)\geq Q, y_E(x)<Q) + \Pr(y_A(x)<Q, y_E(x)\geq Q)\\ &= \frac{1}{2}-\frac{1}{2}\mathrm{erf}\left(\frac{\varepsilon}{\sqrt{2\sigma^2}}\right)\mathrm{erf}\left(\frac{\varepsilon}{\sqrt{2(\sigma+\sigma_n)^2}}\right)\end{aligned} \tag{9}$$

根据误差函数的单调性,易知误比特率 P_e^{AE} 和 P_e^{AB} 均随量化偏差 ε 的减小而增大. 当 $\varepsilon=0$ 时,Alice、Bob 和 Eve 只对 RSSI 的小尺度变化进行量化,多径效应引起的小尺度衰落是影响每个测量值量化成“0”或“1”的主要因素,因此 P_e^{AE} 有最大值 0.5. 当 $\varepsilon>0$ 时,随着量化偏差的逐渐增大,Alice、Bob 和 Eve 的 RSSI 测量值被划入同一量化区间的概率逐渐增大,导致 P_e^{AE} 和 P_e^{AB} 均逐渐减小. 为了保证合法双方的通信安全,物理层密钥生成技术首先需要确保合法双方密钥的安全,使窃听者密钥的误比特率 P_e^{AE} 趋于 0.5,再通过减小测量误差或密钥协商,使合法双方密钥的误比特率 P_e^{AB} 尽可能减小.

3　方案概述

根据以上分析,传统的密钥生成方案由于量化偏差 $\varepsilon>0$,难以保证密钥的安全. 针对该问题,本文所提方案首先消除大尺度衰落的影响,获得随机性更强的小尺度衰落参数;然后通过等概率双门限量化生成密钥,并利用 BCH 码纠正错误密钥比特,具体步骤如下.

3.1　基于信号传播特性的大尺度衰落消除

首先在密钥量化前对合法通信双方的 RSSI 测量参数进行预处理,消除大尺度衰落的影响. 本方案中,合法通信双方在测量 RSSI 的同时记录双方之间的通信距离,然后将自身的 RSSI 测量值和相应的距离 x_i 带入式(3). 由于只需估计大尺度衰落,因此在忽略小尺度衰落和噪声后,得到含有未知参数 η 和 P_0 的观测值表达式如下:

$$y_{PL}(x_i) = P_0 - 10\eta\log_{10}(x_i) \tag{10}$$

以合法方 Alice 为例,Alice 以 $y_A(x_i)$ 与 $y_{PL}(x_i)$ 的偏差平方和最小为准则,计算大尺度衰落模型参数 η 和 P_0. 偏差平方和函数可表示如下:

$$J_{\mathrm{LS}}(n,P_0) = \sum_{i=1}^{N}\left[y_A(x_i)-y_{PL}(x_i)\right]^2 \tag{11}$$

对上式 $J_{\mathrm{LS}}(n,P_0)$ 中的 η 和 P_0 分别求偏导可得待估的未知参数,得到大尺度衰落模型 $y_{PL}(x)$. Bob 可采用同样方法得到 $y_{PL}(x)$,然后 Alice 和 Bob 从原始数据中减去相应距离处的大尺度衰落,得到新的随机源 y'_A、y'_B 生成密钥. 注意到,尽管 Eve 也可以用同样方法获取 $y_{PL}(x)$ 并得到 y'_E,但由于小尺度衰落不相关,Eve 无法从 y'_E 中获取有用信息.

3.2　密钥量化和密钥协商

经过上一小节的预处理后,为了减小量化后合法方的密钥误比特率,本方案采用如图 2 所示的双门限等概率量化方法:Alice 和 Bob 首先将 y'_A、y'_B 划分为 β 个量化区间,使样本落入每个量化区间的概率相等,然后在相邻的量化区间之间设置两个量化门限,并舍弃处于上下量化门限之间的样本,最后将量化输出的 K 转化为格雷码[13]的形式,分别得到密钥序列 K_a 和 K_b. 本方案可以通过调整量化参数 α 和 β,得到不同密钥生成速率的密钥序列. 在量化完成后,Alice 和 Bob 协商纠正不一致的密钥比特. 本方案的协商方法主要分为以下三步:

(1) Alice 和 Bob 分别记录量化结果为 e 的密钥比特的位置索引 W_a 和 W_b,然后 Bob 发送 W_a 给 Alice.

(2) Alice 接收后删除 $W_a \cup W_b$ 位置的量化结果,然后根据 BCH 码和自身剩余的密钥 K_a 计算校验位 S_b. 再将 S_b 和 W_b 一起发送给 Bob.

(3) Bob 接收后首先根据 W_b 删除 $W_a \cup W_b$ 位置的量化结果,然后将校验位 S_b 与剩余密钥序列组合后译码纠错,纠正与 Alice 不一致的密钥比特.

1. 输入: $\{y'(x_i)\mid i\in[1,2,\cdots N]\}$: 消除大尺度衰落后的RSSI
　　α : 双门限间隔;　　β : 量化区间数
2. 初始化: $F(z)=\Pr[y'(x)\leq z]$: 统计RSSI的分布
　　$Q_j^+ = F^{-1}(j/2^\beta+\alpha/2), j=1,2,\cdots,\beta-1$: 上门限
　　$Q_j^- = F^{-1}(j/2^\beta-\alpha/2), j=1,2,\cdots,\beta-1$: 下门限
3. 量化: for i = 1 to n
　　if $y'(x_i)\in(Q_j^+, Q_{j+1}^-)$
　　K(i) = j
　　elseif $y'(x_i)<Q_1^-$
　　K(i) = 0
　　elseif $y'(x_i)>Q_{\beta-1}^+$
　　K(i) = $\beta-1$
　　else
　　K(i) = e
　　end for

图2　双门限等概率量化算法

4 实验环境

为了验证本文所提方案的安全性,我们搭建了如图 3 所示的密钥生成实验平台. 该平台由采用 LoRa 调制技术的无线收发模块和 Nucleo-F411RE 微控制器组成,Alice,Bob 和 Eve 均采用相同的硬件设备和配置参数. 该平台中 Alice 搭载在 DJI-M100 无人机上,在生成密钥的同时 Alice 作为数传模块接收控制指令,Bob 和 Eve 连接在 PC 机上,分别作为合法方和窃听者的无人机地面控制站. 实验中,Alice 和 Bob 以 50ms 的间隔在 433MHz 频率上互相发送数据包,同时测得所有数据包的 RSSI,并利用 GPS 模块测量 Alice 与 Bob 的距离. Eve 作为被动窃听者,可以接收到 Alice 发出的所有数据包并测出 RSSI,但不发送任何信息.

我们在两种不同的环境下进行实验. 实验 1 在包含桌椅和床柜的非视距环境中进行,Bob 和 Eve 静止放在寝室中,Alice 在走廊中移动. 实验 2 在如图 4 所示的室外视距环境中进行. Alice 沿着图示路线运动,Bob 和 Eve 静止放在操场中,本文将 Bob 与 Eve 的距离称为窃听距离. 为了测试本方案在保证密钥一致性的基础上,对于未知位置的被动窃听者的防护能力,在每次实验中,们以合法方密钥误比特率小于 10E-3 为目标调整量化参数 α 和 β,并对比合法方和窃听者的密钥.

图3 密钥生成实验平台

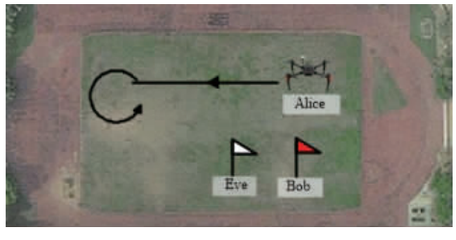


图4 室外实验环境

5 结果分析

5.1 实验结果

本小节总结并分析了本方案的实验结果. 我们在室内和室外环境下一共测量了10^6 个 RSSI 样本,与生成的密钥比特一同存储在 Nucleo-F411RE 微控制器中用于后续分析. 在图 5 中展示了窃听距离为 1 倍波长时,室内和室外环境中 Alice、Bob 和 Eve 的其中一组 RSSI 测量值,表 1 展示了窃听距离大于 1 倍波长、$\beta=2$、采用 (31,15) BCH 码时的密钥误比特率和密钥生成速率统计结果. 其中,密钥生成速率为每个 RSSI 样本生成的密钥比特数(单位 bit/sample).

从图 5 可见,Alice、Bob 和 Eve 三者的大尺度衰落相同,RSSI 测量值存在相似的变化轨迹,而 Alice 与 Eve 的小尺度变化不同. 这表明在窃听距离为 1 倍波长时,本文假设的信道环境与实际环境相匹配,本方案利用与窃听者不相关的 RSSI 小尺度变化生成的密钥是安全的.

由表 1 可见,基于本方案的实验平台在实际环境中,合法通信双方密钥误比特率仅为不到 0.001%,窃听者的密钥误比特率接近 0.5,可以保证合法双方的安全通信,而窃听者几乎无法预测合法方的任何密钥.

表 1 密钥生成实验结果

	室内环境	室外环境	
Alice 移动速度	0.5m/s	1m/s	3m/s
合法方密钥误比特率	9.1E-4	9.3E-4	9.9E-4
窃听者密钥误比特率	49.05%	48.36%	48.15%
密钥生成速率(bit/sample)	1.894	1.422	1.301

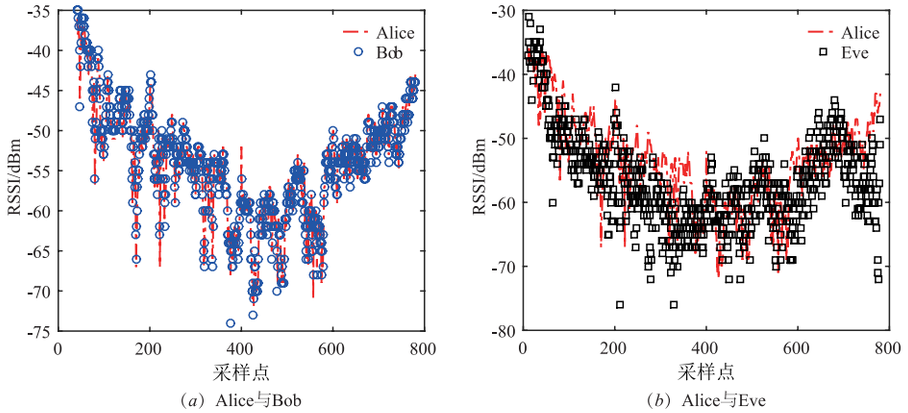
5.2 方案对比与分析

本小节利用实际测量得到的 RSSI 样本,仿真分析了不同方案的窃听者密钥误比特率. 一共选取了文献[6]的 ASBG 方案,文献[3]的 HRUBE 方案和文献[14]针对物联网节点设计的方案这三种经典方案(分别对应图 7 和图 8 的传统方案 1、2 和 3)与本方案进行对比,RSSI 样本分别在室内环境和室外环境中获取.

图 7 展示了室内环境中不同窃听距离的条件下,窃听者 Eve 的密钥误比特率实验结果,横轴为窃听距离与波长的比值. 由图可见,随着窃听距离的增加,四种方案的窃听者密钥误比特率均有所升高. 这是因为随着窃听者远离合法方,窃听者 Eve 与合法方测量得到的 RSSI 的相关性逐渐减小. 其中,本方案在窃听距离大于 0.6 倍波长以后,Eve 窃听者密钥误比特率大于 0.48,此时 Eve 已经几乎无法获得任何密钥信息. 而对于传统方案,文献[6]采用分段量化的方法在一定程度上消除了大尺度衰落的影响,但在窃听距离小于 1.6 个波长以内时,三种方案的窃听者密钥误比特率都始终较低. 这是由于传统方案没有根据信息衰落模型完全消除大尺度衰落的影响,导致合法方与窃听者的 RSSI 存在相关性,使合法生成的密钥与窃听者较为相似.

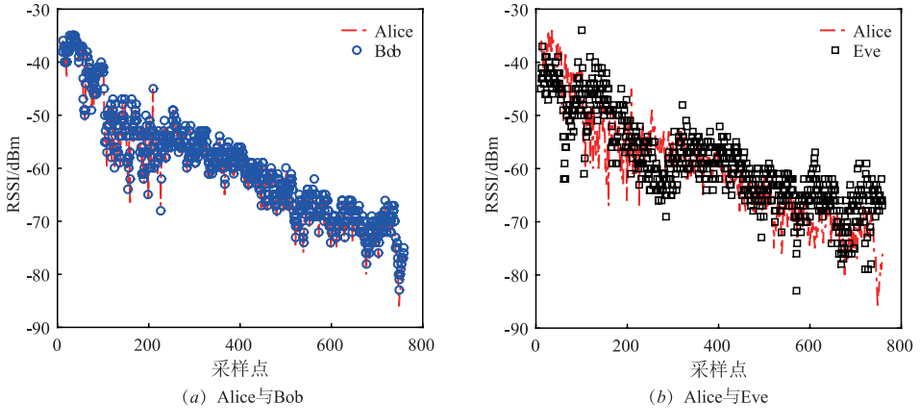
图 8 展示了室外环境下的窃听者密钥误比特率测试结果. 从图中不难发现本方案的窃听者密钥误比特率依然相比传统方案较高,但相比室内环境较低,只有在窃听距离大于一个波长时才能使窃听者误比特率接近 0.47.

这是因为室外环境中的散射体较少,大尺度衰落对信号功率的影响较大,使得窃听者与合法方的 RSSI 测量值相关性更强,窃听者的密钥误比特率也更低.



(a) Alice与Bob　　(b) Alice与Eve

图5　室内环境RSSI采样值示意图



(a) Alice与Bob　　(b) Alice与Eve

图6　室外环境RSSI采样值示意图

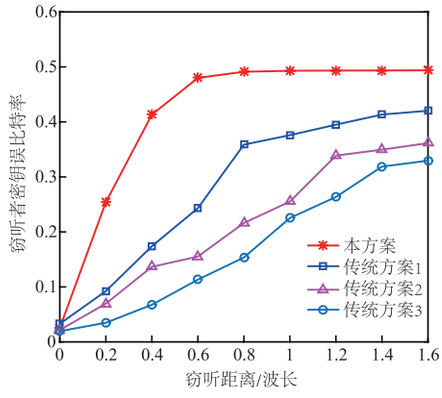


图7　室内环境窃听者误比特率对比

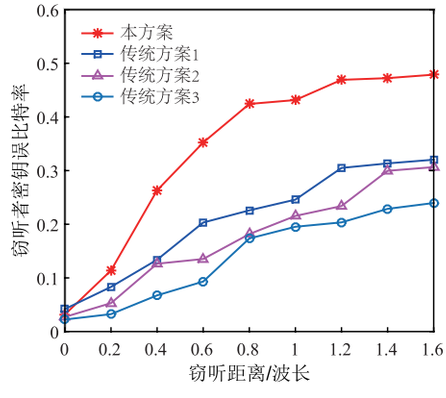


图8　室外环境窃听者误比特率对比

以上测试结果表明本方案在窃听者距离合法方一个波长左右时,增大了窃听者获取合法方密钥的难度,并且在散射体丰富的通信环境中安全性更好.

6　总结

针对基于接收信号强度的密钥生成方案在窃听者靠近合法方时,合法方的密钥易被窃听者获取的问题,本文在分析密钥误比特率的基础上提出了一种基于信号传播特性的物理层密钥生成方案. 实验结果表明,本方案在室内环境窃听距离大于0.6 个波长以后,窃听方密钥误比特率大于 0.48;在室外环境窃听距离大于 1 个波长后窃听方密钥误比特率接近 0.47,相比传统方

案的窃听者密钥误比特率均有一定提高.

另外,实验中发现 RSSI 的测量误差限制了密钥的一致性,且合法通信双方静止时难以获得随机变化的 RSSI 生成密钥.因此如何在静态信道环境中获取互易性更好的密钥生成随机源,将是我们下一步的研究方向.

参考文献

[1] 孙宏,杨义先. 无线局域网协议 802.11 安全性分析[J]. 电子学报,2003,31(7):1098 – 1100.
SUN Hong, YANG Yi-xian. On the security of wireless network protocol 802.11[J]. Acta Electronica Sinica, 2003,31(7):1098 – 1100. (in Chinese)

[2] Hershey J E, Hassan AA, Yarlagadda R. Unconventional cryptographic keying variable management [J]. IEEE Transactions on Communications,1995,43(1):3 – 6.

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

[4] 李鑫,李兴华,杨丹,马建峰. 基于矢量量化的高效随机物理层密钥提取方案[J]. 电子学报,2016,44(2):275 – 281.
LI Xin,LI Xing-hua,YANG Dan,MA Jian-feng. A high-speed random key extraction scheme based on vector quantization[J]. Acta Electronica Sinica,2016,44(2):275 – 281. (in Chinese)

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

[6] Premnath S N,Jana S,Croft J,et al. Secret key extraction from wireless signal strength in real environments [J]. IEEE Transactions on mobile Computing,2013,12(5):917 – 930.

[7] Ye C,Mathur S,Reznik A,et al. Information theoretically secret key generation for fading wireless channels [J]. IEEE Transactions on Information Forensics and Security, 2010,5(2):240 – 254.

[8] Zhu X,Xu F,Novak E,et al. Using wireless link dynamics to extract a secret key in vehicular scenarios [J]. IEEE Transactions on Mobile Computing, 2017, 16 (7): 2065 – 2078.

[9] Mathur S,Trappe W,Mandayam N,et al. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel[A]. 14th ACM international conference on Mobile computing and networking[C]. San Francisco, California, USA,2008. 128 – 139.

[10] Edman M, Kiayias A, Tang Q, et al. On the security of key extraction from measuring physical quantities [J]. IEEE Transactions on Information Forensics and Security, 2016,11(8):1796 – 1806.

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

[12] Erceg V,Greenstein L J,Tjandra S Y,et al. An empirically based path loss model for wireless channels in suburban environments[J]. IEEE Journal on selected areas in communications,1999,17(7):1205 – 1211.

[13] Ye C,Reznik A,Shah Y. Extracting secrecy from jointly Gaussian random variables[A]. IEEE International Symposium on Information Theory [C]. IEEE, 2006. 2593 – 2597.

[14] Margelis G,Fafoutis X,Oikonomou G,et al. Physical layer secret-key generation with discreet cosine transform for the Internet of Things[A]. 2017 IEEE International Conference on Communications[C]. IEEE,2017. 1 – 6.

作者简介

胡晓言 男,1992 年出生. 国家数字交换系统工程技术研究中心在读硕士研究生. 研究方向为物理层安全.

金 梁(通信作者) 男,1969 年出生. 教授、博士生导师,研究方向为移动通信技术、阵列信号处理、物理层安全等.
E-mail:liangjin@263.net

黄开枝 女,1972 年出生. 教授、博士生导师,研究方向为移动通信技术、物理层安全等.

钟 州 男,1982 年出生. 讲师,研究方向为移动通信技术、物理层安全等.

张胜军 男,1988 年出生. 在读博士研究生,研究方向为移动通信技术、物理层安全.