研究与开发

体域网中一种基于无线信道特征的密钥生成方法研究

黄晶晶

（北京赛西科技发展有限责任公司，北京 100007）

摘　要：无线体域网是以人体为中心的无线网络，受其有限的资源和计算能力的约束，如何保证无线体域网通信节点间共享密钥是当前面临的一大挑战。提出了一种基于超宽带无线体域网信道特征的密钥生成机制，利用超宽带信道多径相对时延与平均时延的差值量化生成密钥，降低了密钥不匹配率，同时引入辅助节点，提高了密钥生成速率。仿真结果表明，该机制能够在兼顾密钥一致性的前提下，获得较高的密钥生成速率并保证密钥的安全性。

关键词：信道互易性；密钥生成；无线体域网；超宽带

中图分类号：TN915.81

文献标识码：A

doi: 10.11959/j.issn.1000−0801.2021260

Research on secret key generation based on wireless channel characteristics in body area network

HUANG Jingjing

Beijing Saixi Technology Development Co., Ltd., Beijing 100007, China

Abstract: Wireless body area network (WBAN) is a human-centered wireless network. With limitations of power and computation capabilities of WBAN, the significant challenge of ensuring security is how to generate a shared key between two entities based on a lightweight symmetric cryptography. To investigate this issue, a secret key generation scheme in ultra-wideband (UWB) WBAN was designed. In this scheme, the difference of multipath relative delay and its average value were chosen as common random source to reduce key mismatch probability. Furthermore, with the aid of relay, secret key generation rate could be increased. Simulation and test results demonstrate that the proposed scheme can achieve a good tradeoff between key match probability and key generation rate. Furthermore, security analysis of the scheme was also provided to validate its feasibility.

Key words: channel reciprocity, secret key generation, WBAN, UWB

1　引言

近年来，无线通信、智能控制、集成电路等技术的发展以及健康医疗需求的提升促使无线体域网（wireless body area network，WBAN）技术成为研究的热点。无线体域网包含具有通信功能的可穿戴式或植入人体内部的轻量级无线传感器，所述传感器感知与人体相关的生理、运动和

收稿日期：2021−06−03；修回日期：2021−12−08

环境信息并上传给手机或计算机等终端设备，从而达到实时监测、远程诊断等目的。上述节点采集或处理的医疗数据涉及个人隐私，因此研究保障所述数据机密性的机制十分必要。

由于 WBAN 传感器节点的供电和计算处理能力受限，显然使用对称加密算法优于利用公钥和认证中心的非对称加密算法。随之而来需要解决的问题是如何在传感器节点和终端设备间共享密钥。传统的解决方案是出厂预配置或使用密钥管理体系[1]。然而，受不同厂商硬件配置的差异和节点动态配对需求的影响，预配置在实际操作中非常不便；而密钥管理体系需要一个可信任的第三方存储密钥，这也会带来潜在的危险和连带责任。此外，若采用 Diffie-Hellman 协议[2]共享密钥，对资源有限的传感器节点而言代价过于昂贵[3]。

为了克服上述缺陷，有学者提出利用人体生理信号生成共享密钥[4]。受此启发，IPI（inter-pulse interval）信号[5]、ECG（electrocardiogram）信号[6-7]相继成为生成密钥的随机信号源。此外，人体生理信号还可用于密钥协商[8-9]。然而，感知相同的人体生理信号会造成硬件成本的大幅提升同时传感器的安放位置也会受到限制。例如，ECG 信号的感知需要靠近心血管。因此，利用体域网无线衰落信道特征生成密钥成为不错的选择。

根据无线信道互易性[10]、空间变化性[11]和时间变化性[12]的特点，合法通信双方能够从信道特征（如接收信号强度、信道冲激响应、相位、时延、到达角度等）中提取密钥。Hershey[13]在 1996 年首次提出利用差分相位检测生成密钥的机制。随后，文献[14-15]进一步阐述了利用信道相位估计提高密钥生成速率的机制。由于现有传感器设备易于获得接收信号强度（received signal strength，RSS），因此有大量文献研究基于 RSS 的密钥生成算法[16-20]。文献[21]是篇综述类文章，介绍了窄带无线通信系统中基于无线信道特征生成密钥的若干种算法。文献[22-24]阐述了利用超宽带信道特征生成密钥的机制，文献[22]推导了合法通信双方互信息的最大界并求出共享密钥的最大长度，指出最大密钥速率与 UWB 通信节点间的最大互信息熵值有关。

在 WBAN 中，Hanlen 等[25]在 2009 年验证了基于近人体信道特征的密钥共享技术的可行性，并证明了信道的随机性和人体的运动能够有效防止窃听者获得密钥信息。随后，Ali 等[26-27]利用可穿戴设备移动时造成信号强度的波动生成共享密钥。文献[28]提出了一种轻量级密钥生成算法，该算法利用现有信号在通信链路上来回变化的趋势提取密钥并给出了系统开销的计算方法。文献[29]提出通过信道跳频增强密钥熵的思想，文献[30]提出通过滤波算法提高密钥一致性的机制，文献[31]研究了 WBAN 中利用信息调和技术进行广播密钥协商的机制。

针对现有基于无线信道特征生成密钥的机制中密钥生成速率和密钥一致性矛盾的问题，本文提出了利用多径相对时延生成密钥的算法，同时引入辅助节点提高密钥生成速率，仿真结果表明所提机制能够在增强密钥一致性的前提下提高密钥生成速率，在两者之间取得较好的平衡。

2　研究背景

2.1　WBAN 信道模型

根据传感器在人体分布位置（体表或体内）的不同，IEEE 802.15.6 工作组将 WBAN 信道划分为 3 种模型，分别是：体内信道（指体内传感器到体内传感器或体内传感器到体表传感器）；体表信道（指体表传感器到体表传感器）；体外信道（指体表传感器到外部终端设备）[32]。IEEE 802.15.4 工作组也给出了 WBAN 的信道模型[33]，重点关注的是超宽带信道在 WBAN 中的应用。本机制的仿真模型采用体表信道模型，该模型下信号多沿人体表层皮肤绕射，信号幅度大致服从均值为 0、标准差为 σ 的对数正态分布，信道冲激

响应可以表示如下：

$$h(t)=\sum_{l=0}^{L-1}\alpha_k \exp(\mathrm{j}\phi_k)\delta(t-\tau_k) \quad (1)$$

其中，L 表示多径数目，ϕ_k 表示多径增益的相位，多径到达时间 τ_k 服从泊松分布，α_k 表示多径信号的幅度增益，α_k 表示如下：

$$20\lg|\alpha_k|=\begin{cases}0 & ,k=0\\ \gamma_0+10\lg\left(\mathrm{e}^{\frac{\tau_k}{\Gamma}}\right)+S & ,k\neq 0\end{cases} \quad (2)$$

其中，γ_0 为 Rician 因子，Γ 为指数衰减因子，$S\sim \log\text{-normal}(0,\sigma)$。

2.2 密钥生成机制评估标准

评价密钥生成机制通常有 3 项指标，具体如下。

- 密钥生成速率：单位时间内每信道可以提取的平均密钥比特数，该指标受采样速率、量化参数、量化方法和信道变化的影响。
- 密钥不匹配率：合法通信节点协商密钥失败的概率，密钥不匹配率越高，密钥一致性越差。
- 密钥随机性：密钥比特序列的熵值，通常用美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）测试工具[34]测试共享密钥的随机性。

2.3 密钥生成机制通信

在本文所提的机制中，WBAN 的覆盖范围为以人体为中心的 2 m 内。人体表有 3 个传感器节点，分别是 Alice、Relay 和 Bob。Bob 为具有强大计算和存储能力的沉没节点或可移动终端设备，Alice 和 Relay 为具有低功耗、弱计算处理能力的普通体域网传感器。Alice 和 Relay 需要在窃听者 Eve 存在的前提下传输采集的医疗数据至 Bob 处，Alice 和 Relay 之间偶尔也会有通信。因此，Alice、Relay 和 Bob 之间需要共享密钥。WBAN 中基于无线信道特征共享密钥的一个常见问题是密钥生成速率较低，本文所提机制利用一个辅助节点 Relay 解决该问题，所提机制的示意图如图 1 所示。

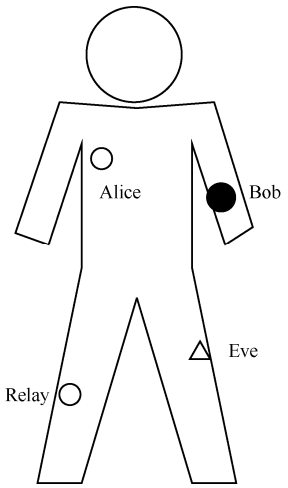

图 1 WBAN 示意图

3 基于无线信道特征的密钥生成机制

本文所提机制的原理如图 2 所示，下面按照 4 个步骤详细阐述该机制的实现过程。

3.1 信道探测

假设 Alice、Bob 和 Relay 的时间同步，Bob 分别向 Alice 和 Relay 发送探测序列 X_t 和 Z_t，且 X_t 和 Z_t 相互正交。Alice 和 Relay 收到探测序列后，分别向 Bob 发送探测序列 X_t 和 Z_t。根据信道互易性的原理可知，在信道的一个相干时间 T_c 内，前向和反向链路理论上应该相同。因此，Bob 和 Alice（或 Relay）能够获得类似的信道特征。同时，由于信道具有时间变化性的特点，信道特征随着相干时间的变化而变化。

3.2 提取多径相对时延

Alice、Relay 和 Bob 的接收信号可以表示为：

$$y_{\mathrm{A}}(t)=h_{\mathrm{BA}}(t)*x(t)+n_{\mathrm{A}}(t) \quad (3)$$

$$y_{\mathrm{R}}(t)=h_{\mathrm{BR}}(t)*z(t)+n_{\mathrm{R}}(t) \quad (4)$$

$$y_{\mathrm{B}}(t)=h_{\mathrm{AB}}(t)*x(t)+h_{\mathrm{RB}}(t)*z(t)+n_{\mathrm{B}}(t) \quad (5)$$

其中，各符号的含义见表 1，$\sigma^2=N_0/2$。

Bob 利用相关函数以及正交序列的性质，分别估算 Alice 和 Relay 发送探测序列的时延，计算过程如下：

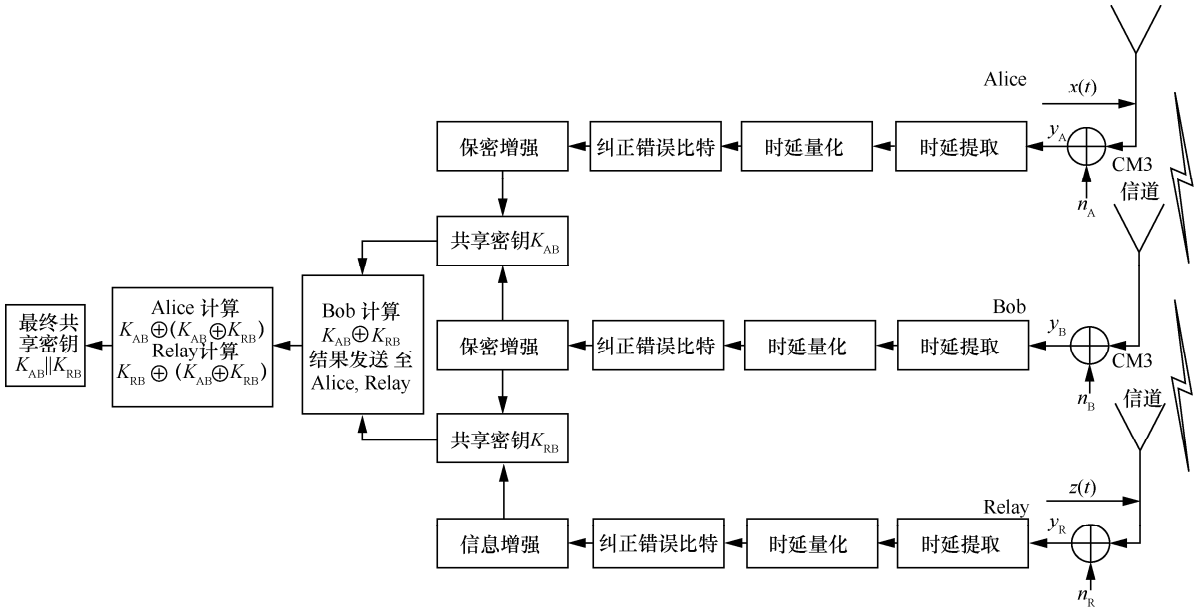

图 2　基于无线信道多径时延的协作式密钥生成机制原理

表 1　符号含义

符号	含义
$x(t)$	X_t 的发送波形
$z(t)$	Z_t 的发送波形
$h_{AB}(t)$	Alice 向 Bob 发送探测序列的信道增益
$h_{RB}(t)$	Relay 向 Bob 发送探测序列的信道增益
$h_{BA}(t)$	Bob 向 Alice 发送探测序列的信道增益
$h_{BR}(t)$	Bob 向 Relay 发送探测序列的信道增益
$n_A(t)$, $n_R(t)$, $n_B(t)$	均值为 0、方差为 σ^2 的加性高斯白噪声

$$R_A(\tau)=\int_0^T y_B(t)x(t-\tau)\mathrm{d}t=\int_0^T\left[z(t)h_{RB}(t)\right]x(t-\tau)\mathrm{d}t+\int_0^T\left[x(t)h_{AB}(t)\right]x(t-\tau)\mathrm{d}t+\int_0^T n_B(t)x(t-\tau)\mathrm{d}t \tag{6}$$

其中，T 是一个数据符号的周期，对于 Alice，第一项的积分结果为 0，根据计算结果找到 $R_A(\tau)$ 的最大值，对应的时延即估计值。

$$R_R(\tau)=\int_0^T y_B(t)z(t-\tau)\mathrm{d}t=\int_0^T\left[z(t)h_{RB}(t)\right]z(t-\tau)\mathrm{d}t+\int_0^T\left[x(t)h_{AB}(t)\right]z(t-\tau)\mathrm{d}t+\int_0^T n_B(t)z(t-\tau)\mathrm{d}t \tag{7}$$

其中，对于 Realy，第二项的积分结果为 0，根据计算结果找到 $R_R(\tau)$ 的最大值，对应的时延即估计值。

Alice 和 Relay 同样采用相关函数法估计 Bob 发送的探测序列的多径时延，只是它们在接收端的检测复杂度比 Bob 的低。

多径时延估计完成后，利用 RAKE 接收机提取上述时延值。多径时延提取原理如图 3 所示。对于脉冲超宽带系统而言，相同发射波形的不同副本在接收端不会重叠，需要选择相应的模板 $m(t)$ 提取多径，上述这些副本与本地模板相乘后进行积分运算，运算结果经过采样送至时延单元和合并单元，再经过检测输出。本方法中 RAKE 接收机采用选择性接收和等增益合并策略。实际应用中，将时间轴平均划分为若干个时间仓，每个时间仓的长度为 $\Delta\tau$，时间仓是接收机能够区分的最小多径间隔，在每个时间仓内仅存在一条多径分量，时间仓的长度即多径分辨率。如果用离散时间信道冲激响应表达式描述信道，则 RAKE 接收机的不同多径分量在时间上的间隔是 $\Delta\tau$ 的整数倍。

以 Alice 为例，假设 RAKE 接收机选择性接

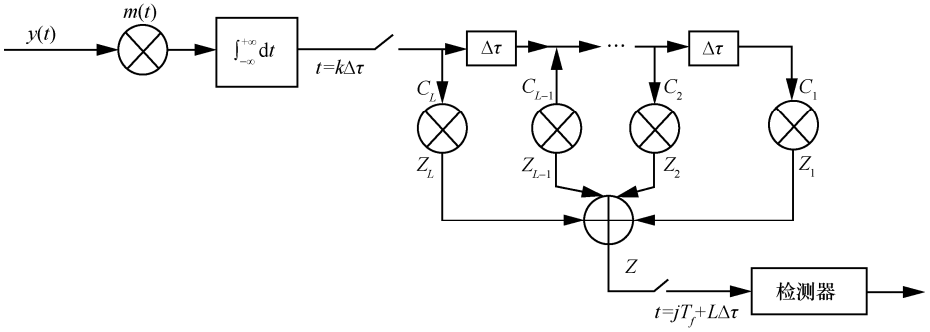

图 3　多径时延提取原理

收能量最大的路径数为 m，信道多径数目为 L（$m \leqslant L$），经过检测，m 条路径的时延为 $\tau_1, \tau_2, \cdots, \tau_m$，则相邻路径间的相对时延为 $\tau_2 - \tau_1, \tau_3 - \tau_2, \cdots, \tau_m - \tau_{m-1}$。将相对时延改写为离散表达式：

$$\tau_2 - \tau_1 = (n_2 - n_1)\Delta\tau \tag{8}$$

$$\tau_3 - \tau_2 = (n_3 - n_2)\Delta\tau \tag{9}$$

$$\vdots \qquad \vdots$$

$$\tau_m - \tau_{m-1} = (n_m - n_{m-1})\Delta\tau \tag{10}$$

因此，多径相对时延的离散值为 $n_2 - n_1$，$n_3 - n_2, \cdots, n_m - n_{m-1}$。以此类推，可以求出 Relay 和 Bob 的多径相对时延离散值。

3.3　量化

Alice、Relay 和 Bob 将得到的多径相对时延离散值通过量化转换成密钥序列。为了减少由噪声造成的通信节点间量化结果的差异，取相对时延离散值与其平均值的差值作为量化随机值。相对时延离散值的平均值计算如下：

$$\delta_{\text{mean\_delay}} = \frac{n_m - n_1}{m - 1} \tag{11}$$

接下来，计算相对时延离散值与其平均值的差值并与阈值 0 进行比较，根据判决结果生成密钥比特，判决准则如下：

$$\text{key} = \begin{cases} 1, (n_m - n_{m-1}) - \delta_{\text{mean\_delay}} \geqslant 0 \\ 0, (n_m - n_{m-1}) - \delta_{\text{mean\_delay}} < 0 \end{cases} \tag{12}$$

如上所述，一次信道探测过程中 m 条路径可以生成 $(m-1)$ 个密钥比特。虽然窃听者 Eve 也可以利用相同的方法生成密钥，但是由于信道具有空间变化性的特点，Eve 无法得到合法通信节点间的共享密钥信息。

3.4　密钥协商和保密增强

由于估计误差和信道噪声的存在，通信双方生成的密钥比特信息可能会存在一些差异。这些错误比特信息可以通过纠错码[35]或 Cascade 协议[36]纠正。考虑到体域网传感器的特点，所提机制选用低复杂度、高效率的 BBBSC 算法[37]。协商的具体过程如下。

Alice（Relay）和 Bob 将密钥比特数据分成长度固定的组，分别计算每组数据的奇偶性，并在公共信道上进行比较。当错误的数据个数为奇数时，如果比较结果不同，则该组数据存在错误，将该组数据一分为二，继续进行奇偶性校验并比较，直到找到这个错误比特数位。为了减少协商过程中密钥信息的泄露，每一次奇偶性检测比较后，就舍弃该组数据的最后一位，错误的比特同样舍弃。当错误的数据个数为偶数时，增加分组长度，继续进行奇偶性检测并比较，直至错误率达到系统预设的错误率。

注意，在密钥协商的过程中窃听者 Eve 可以通过公共信道获得合法通信双方生成密钥的部分信息，此外，由于信道某些时间段变化缓慢造成生成的密钥比特之间存在相关性，因此，需要利用保密增强技术解决上述问题。

假设 Alice 和 Bob 经过密钥协商后的共享密

钥比特序列为 K'_{AB}，Relay 和 Bob 经过密钥协商后的共享密钥比特序列为 K'_{RB}，经过 Hash 函数映射去相干性后分别得到 K_{AB} 和 K_{RB}。接下来的计算过程如下。

Bob：$K = K_{AB} \oplus K_{RB}$；

Alice：$K_{AB} \oplus K = K_{AB} \oplus K_{AB} \oplus K_{RB} = K_{RB}$；

Relay：$K_{RB} \oplus K = K_{RB} \oplus K_{AB} \oplus K_{RB} = K_{AB}$；

经过上述计算后，Alice 和 Relay 分别获得了对方与 Bob 生成的密钥信息，因此，三者之间最终的共享密钥比特序列为 K_{AB} 串接 K_{RB}，记为 $K_{AB} \| K_{RB}$。

4　仿真测试结果分析

为了验证所提机制的正确性，针对第 2.1 节中 WBAN 体表信道模型进行仿真和测试，仿真环境参数设置见表 2。

表 2　仿真环境参数设置

仿真参数	数值
相干时间	83.3 ms
中心频率	3.6 GHz
采样率	10 GHz
平均移动速率	1 m/s
多普勒频移	12 Hz
波长	83.3 mm
γ_0	−4.3 dB
Γ	56.6 ns
σ	4.7

多径数目 m=6 时多径相对时延值量化生成密钥比特的结果如图 4 所示。对于 Alice 而言，多径相对时延分别是 $4\Delta\tau$、$\Delta\tau$、$6\Delta\tau$、$2\Delta\tau$、$3\Delta\tau$，平均相对时延为 $3.2\Delta\tau$。各相对时延与平均时延的差值为 $0.8\Delta\tau$、$-2.2\Delta\tau$、$2.8\Delta\tau$、$-1.2\Delta\tau$、$-0.2\Delta\tau$。根据量化判决准则式（12），可以得到 Alice 的量化结果为 10 100。对于 Bob 而言，多径相对时延分别是 $3\Delta\tau$、$2\Delta\tau$、$4\Delta\tau$、$\Delta\tau$、$2\Delta\tau$，平均相对时延为 $2.4\Delta\tau$。各相对时延与平均时延的差值为 $0.6\Delta\tau$、$-0.4\Delta\tau$、$1.6\Delta\tau$、$-1.2\Delta\tau$、$-0.2\Delta\tau$。同样，可以得到 Bob 的量化结果为 10 100。注意，这里只给出了 Alice 和 Bob 的量化结果，Relay 和 Bob 的量化过程类似，不再赘述。

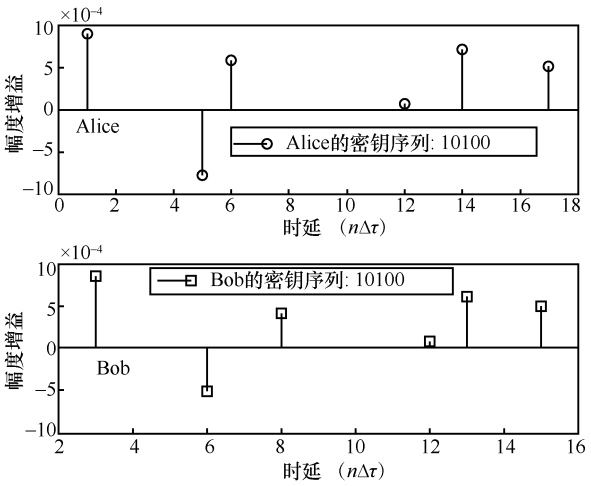

图 4　m=6 时多径相对时延值量化生成密钥比特的结果

多径数目 m=8 时多径相对时延值量化生成密钥比特的结果如图 5 所示。对于 Alice 而言，多径相对时延分别是 $\Delta\tau$、$3\Delta\tau$、$2\Delta\tau$、$4\Delta\tau$、$3\Delta\tau$、$\Delta\tau$、$2\Delta\tau$，平均相对时延为 $2.2\Delta\tau$。各相对时延与平均时延的差值为 $-1.2\Delta\tau$、$0.8\Delta\tau$、$-0.2\Delta\tau$、$1.8\Delta\tau$、$0.8\Delta\tau$、$-1.2\Delta\tau$、$-0.2\Delta\tau$。根据量化准则式（12），可以得到 Alice 的量化结果为 0 101 100。对于 Bob 而言，多径相对时延分别是 $\Delta\tau$、$4\Delta\tau$、$\Delta\tau$、$2\Delta\tau$、$5\Delta\tau$、$\Delta\tau$、$2\Delta\tau$，平均相对时延为 $2.2\Delta\tau$。各相对时延与平均时延的差值为 $-1.2\Delta\tau$、$1.8\Delta\tau$、$-1.2\Delta\tau$、$-0.2\Delta\tau$、$2.8\Delta\tau$、$-1.2\Delta\tau$、$-0.2\Delta\tau$。根据式（12），可以得到 Bob 的量化结果为 0 100 100。

对比图 4 可知，当 m 增加时，量化生成的比特数也随之增加，虽然 Alice 和 Bob 在 m=8 时出现了 1 个错误比特，但是在后续的密钥协商过程中可以查找该错误比特并纠正。同样，Relay 和 Bob 的量化过程类似，不再赘述。

有无辅助节点 Relay 情况下 Bob 的密钥速率随

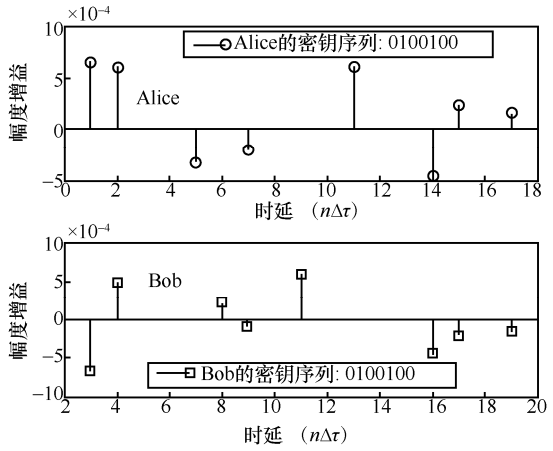

图 5 m=8 时多径相对时延值量化生成密钥比特的结果

信噪比增加的变化曲线如图 6 所示。这里的“bits per channel use”用于度量密钥速率[38]。当提取的多径数目相同时，Relay 的存在使得其在 Bob 与 Alice 交互的过程中，还可以与 Bob 通信，所以 Bob 能够生成更多的密钥比特，但同时也消耗了更多的能量。当提取的多径数目不同而其他条件相同时，密钥生成速率随着多径数目的增加而增大，进一步说明了图 5 结论的正确性。

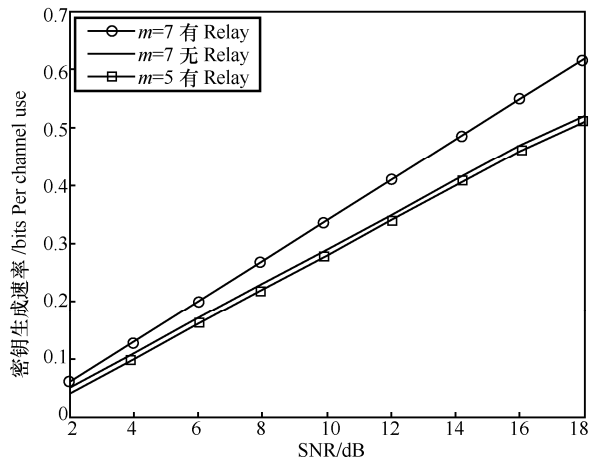

图 6 有无辅助节点 Relay 情况下 Bob 的密钥速率随信噪比增加的变化曲线

多径数目不同时密钥不匹配率随信噪比变化曲线如图 7 所示，Bob 和 Eve 的密钥不匹配率随信噪比增加基本保持不变，在 0.5～0.6，Bob 和 Relay 的密钥不匹配率随信噪比增加逐渐下降，合法通信用户 Bob 与窃听者 Eve 之间的密钥不匹配率 KBob-Eve 远比合法通信双方间的密钥不匹配率 KBob-Relay 高，即合法通信用户与窃听者之间比合法通信用户双方间的密钥一致性差。这是因为信噪比的提升有利于合法通信用户之间获得相关性更高的信道探测结果，从而减少量化值的差异性，降低密钥不匹配率。同时，结合图 6 可知，多径数的增加在提高密钥生成速率的同时，也导致了合法通信双方密钥不匹配率的上升，这是因为随着多径数目的增加量化生成的错误密钥比特数增多。同理，Alice 和 Relay 以及 Eve 的密钥不匹配率随信噪比增加的变化趋势类似。

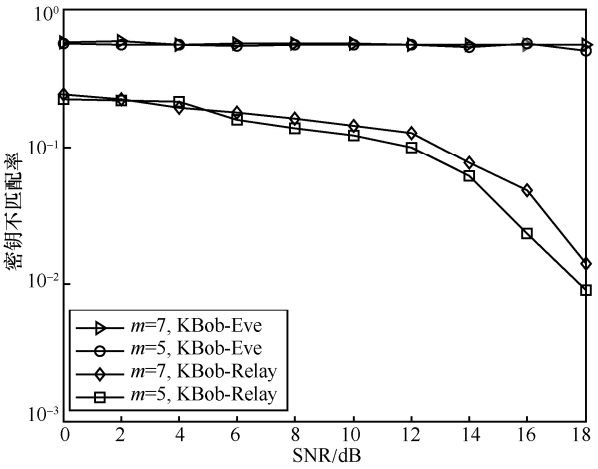

图 7 多径数目不同时密钥不匹配率随信噪比变化曲线

不同密钥生成机制的密钥不匹配率随信噪比变化曲线如图 8 所示，这里选取传统的基于 RSS 的密钥生成机制作为对比机制，基于多径时延的密钥生成机制优于基于 RSS 密钥生成机制，这是因为基本的双门限 RSS 量化阈值的设定可能会对量化结果产生不确定的影响，导致通信双方获得相同密钥的比特概率下降。同时，当其他条件相同时，引入辅助节点会造成密钥不匹配率略有上升，这是由于增加了一个密钥协商方引起量化差异增大。结合图 6 来看，在信噪比为 16 dB 时，引入 Relay 的密钥生成速率比无 Relay 的密钥生成速率增加了 17.02%，而其密钥不匹配率比无 Relay 的密钥不匹配率上升了 12.64%。由此可见，引入

辅助节点带来的密钥速率增加的优势大于密钥一致性下降的劣势。实际应用中，可以根据用户需求选择是否引入辅助节点。

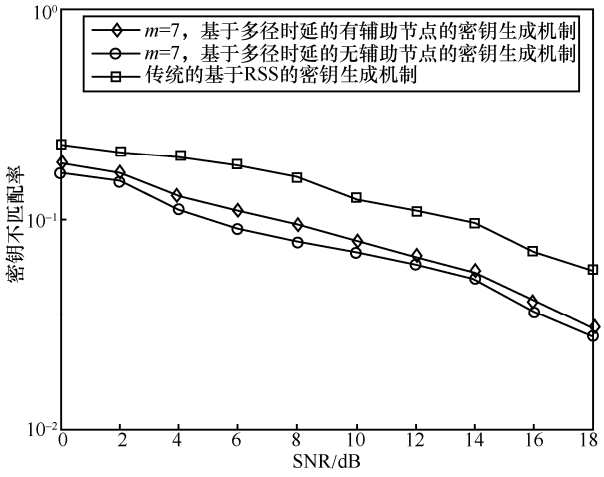

图 8　不同密钥生成机制的密钥不匹配率随信噪比变化曲线

借助 NIST 测试工具，在 Linux 环境下，对最终共享的密钥比特信息进行随机性测试，由于密钥长度受限，选取 NIST 中常用的 8 项指标进行测试验证，测试结果见表 3。所有测试指标的 P-value 值均大于 0.01，由此表明 $K_{AB}\|K_{RB}$ 通过了随机性测试，该密钥比特序列接近真正的随机序列。

表 3　共享密钥 $K_{AB}\|K_{RB}$ 的随机性测试结果

测试指标	测试结果 P-value
频数	0.34
块内频数	0.14
累积和	0.19
离散傅里叶变换	0.31
游程总数	0.03
块内最长游程	0.12
近似熵	0.34
序列	0.57, 0.46

5　安全性分析

所提机制不考虑窃听者发起主动攻击的情况，即假设 Eve 既不能阻塞信道也不能篡改 Bob 与 Alice（Relay）之间的交互信息。同时，Eve 与 Alice（Relay、Bob）的距离不能太近，理论上该距离大于所使用的频率半波长即可保证窃听者所经历的衰落与合法用户经历的衰落不同。以中心频率为 3.6 GHz 的超宽带体域网信道模型为例，其对应的波长为 83.3 mm，实际应用中 Eve 与 Alice（Relay、Bob）的距离大于 41.65 mm 很容易实现。因此，Eve 探测的信道特征值与合法用户之间探测的信道特征值不同。

从信息论的角度来分析，假设 Bob、Alice 和 Relay 测量到的接收信号样值分别是 Y_B、Y_{BA} 和 Y_{BR}，Eve 测量到的来自 Alice、Bob 和 Relay 的信号样值分别是 Y_{AE}、Y_{BE} 和 Y_{RE}。K_{AB} 是 Alice 和 Bob 希望生成的共享密钥，K_{RB} 是 Relay 和 Bob 希望生成的共享密钥。Alice 和 Bob 之间的互信息可以表示为 $I(Y_B;Y_{BA})=K_{AB}$，Relay 和 Bob 之间的互信息可以表示为 $I(Y_B;Y_{BR})=K_{RB}$。在 K_{AB} 的生成过程中，Eve 能够获得的信息为 $I(Y_{AE},Y_{BE};K_{AB})$。由于信道在任意一个无线链路的两端都是独立的，对于任意 $\varepsilon<0$，有 $I(Y_{AE},Y_{BE};K_{AB})\leqslant\varepsilon$ 成立。类似地，在 K_{RB} 的生成过程中，Eve 能够获得的信息为 $I(Y_{RE},Y_{BE};K_{RB})$，对于任意 $\varepsilon<0$，同样有 $I(Y_{RE},Y_{BE};K_{RB})\leqslant\varepsilon$ 成立。因此，Eve 几乎很难获得有关密钥 K_{AB} 和 K_{RB} 的信息。

6　结束语

本文提出了一种基于无线信道多径时延的协作式密钥生成机制，通过利用无线信道的多径时延特征以及引入辅助节点，在兼顾密钥一致性的前提下提高了密钥生成速率。仿真测试结果以及安全性分析表明，本文所提的密钥生成机制能够在密钥生成速率、密钥不匹配率和密钥随机性方面取得良好的性能，并且能够在密钥一致性和密钥生成速率之间取得较好的平衡。针对窃听者发起主动攻击以及窃听者与传感器节点比较接近导致多径衰落不好区分的情形，如何利用体域网无线信道特征生成安全可靠的密钥将成为研究重点。

参考文献：

[1] IEEE B E. IEEE Standard for local and metropolitan area networks part 15.6: wireless body area networks[S]. IEEE, 2012.

[2] DIFFLE W, H-ELLMAN M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.

[3] BLASS, E, ZITTERBART M. Efficient implementation of elliptic curve cryptography for wireless sensor networks[R]. Technical report. Universitat Karlsruhe, 2005: 1-16.

[4] CHERUKURI S, VENKATASUBRAMANIAN K K, GUPTA S K S. Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body[C]. // Proceedings of Parallel Processing workshops. Piscataway: IEEE Press, 2003: 432-439.

[5] POON C C Y, ZHANG Y T, BAO S D. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health[J]. IEEE Communications Magazine, 2006, 44(4): 73-81.

[6] VENKATASUBRAMANIAN K K, BANERJEE A, GUPTA S K S. EKG-based key agreement in Body Sensor Networks[C]//Proceedings of IEEE INFOCOM Workshops 2008. Piscataway: IEEE Press, 2008: 1-6.

[7] OVILLA-MARTINEZ B, DÍAZ-PÉREZ A, GARZA-SALDAÑA J J. Key establishment protocol for a patient monitoring system based on PUF and PKG[C]//Proceedings of 2013 10th International Conference and Expo on Emerging Technologies for a Smarter World (CEWIT). Piscataway: IEEE Press, 2013: 1-6.

[8] VENKATASUBRAMANIAN K K, BANERJEE A, GUPTA S K S. PSKA: usable and secure key agreement scheme for body area networks[J]. IEEE Transactions on Information Technology in Biomedicine, 2010, 14(1): 60-68.

[9] WU Y, Sun Y M, ZHAN L, et al. Low mismatch key generation based on wavelet-transform trend and fuzzy vault in body area network[EB]. 2013.

[10] 龙航, 袁广翔, 王静, 等. 物理层安全技术研究现状与展望[J]. 电信科学, 2011, 27(9): 60-65.
LONG H, YUAN G X, WANG J, et al. Physical layer security: survey and Future Chinese full text[J]. Telecommunications Science, 2011, 27(9): 60-65.

[11] GOLDSMITH A. Wireless Communications[M]. Manchester UK: Cambridge University Press, 2005 :108-109.

[12] 周百鹏. 基于无线信道特征提取的密钥生成技术研究[D]. 郑州: 解放军信息工程大学, 2011.
ZHOU B P. Research on secret key generation utilizing the wireless channel characteristics[D]. Zhengzhou: PLA Information Engineering University, 2011.

[13] HASSAN A A, STARK W E, HERSHEY J E, et al. Cryptographic key agreement for mobile radio[J]. Digital Signal Processing, 1996, 6(4): 207-212.

[14] WANG Q, SU H, REN K, et al. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks[C]//2011 Proceedings IEEE INFOCOM. Piscataway: IEEE Press, 2011: 1422-1430.

[15] WANG Q, XU K H, REN K. Cooperative secret key generation from phase estimation in narrowband fading channels[J]. IEEE Journal on Selected Areas in Communications, 2012, 30(9): 1666-1674.

[16] AZIMI-SADJADI B, KIAYIAS A, MERCADO A, et al. Robust key generation from signal envelopes in wireless networks[C]//Proceedings of the 14th ACM conference on Computer and communications security - CCS '07. New York: ACM Press, 2007: 401-410.

[17] MATHUR S, TRAPPE W, MANDAYAM N, et al. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel[C]//Proceedings of the 14th ACM international conference on Mobile computing and networking - MobiCom '08. New York: ACM Press, 2008: 128-139.

[18] JANA S, PREMNATH S N, CLARK M, et al. On the effectiveness of secret key extraction from wireless signal strength in real environments[C]//Proceedings of the 15th annual international conference on Mobile computing and networking - MobiCom '09. New York: ACM Press, 2009: 321-332.

[19] AONO T, HIGUCHI K, OHIRA T, et al. Wireless secret key generation for fading wireless channels[J]. IEEE Trans on Antennas and Propagation, 2005, 53 (11): 3776-3784.

[20] YE C X, 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.

[21] REN K, SU H, WANG Q. Secret key generation exploiting channel characteristics in wireless communications[J]. IEEE Wireless Communications, 2011, 18(4): 6-12.

[22] WILSON R, TSE D, SCHOLTZ R A. Channel identification: secret sharing using reciprocity in ultrawideband channels[J]. IEEE Transactions on Information Forensics and Security, 2007, 2(3): 364-375.

[23] GHOREISHI MADISEH M, HE S, MCGUIRE M L, et al. Verification of secret key generation from UWB channel observations[C]//Proceedings of 2009 IEEE International Conference on Communications. Piscataway: IEEE Press, 2009: 1-5.

[24] MADISEH M G, MCGUIRE M L, NEVILLE S S, et al. Secret key generation and agreement in UWB communication channels[C]//Proceedings of IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference. Piscataway: IEEE Press, 2008: 1-5.

[25] HANLEN L W, SMITH D, ZHANG J A, et al. Key-sharing via channel randomness in narrowband body area networks: is everyday movement sufficient? [C]//Proceedings of Proceedings of the 4th International ICST Conference on Body Area Networks.

ICST, 2009: 1-8.

[26] ALI S T, SIVARAMAN V, OSTRY D. Secret key generation rate vs. reconciliation cost using wireless channel characteristics in body area networks[C]//Proceedings of 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing. Piscataway: IEEE Press, 2010: 644-650.

[27] 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 - WISEC '12. New York: ACM Press, 2012: 16-18.

[28] TSOURI G R, WILCZEWSKI J. Reliable symmetric key generation for body area networks using wireless physical layer security in the presence of an on-body eavesdropper[C]//ISABEL '11: Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies. 2011: 1-6.

[29] YAO L J, ALI S T, SIVARAMAN V, et al. Decorrelating secret bit extraction via channel hopping in body area networks[C]// Proceedings of 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC). Piscataway: IEEE Press, 2012: 1454-1459.

[30] YAO L J, ALI S, SIVARAMAN V, et al. Improving secret key generation performance for on-body devices[C]//Proceedings of Proceedings of the 6th International ICST Conference on Body Area Networks. ACM, 2011: 19-22.

[31] ALI A, KHAN F A. A broadcast-based key agreement scheme using set reconciliation for wireless body area networks[J]. Journal of Medical Systems, 2014, 38(5): 33.

[32] YAZDANDOOST K Y, SAYRAFIANPOVR K. Channel model for body area network (BAN)[EB]. 2008.

[33] MOLISCH A F, BALAKRISHNAN K, CASSIOLI D, et al. IEEE 802.15.4a channel model - final report[EB]. 2004.

[34] RUKHIN A, SOTA J, NECHVATAL J, et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications[R]. National Institute of Standards and Technology, 2000.

[35] DODIS Y, OSTROVSKY R, REYZIN L, et al. Fuzzy extractors: how to generate strong keys from biometrics and other noisy data[J]. SIAM Journal on Computing, 2008, 38(1): 97-139.

[36] BRASSARD G, SALVAIL L. Secret-key reconciliation by public discussion[M]. Advances in Cryptology — EUROCRYPT '93. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994: 410-423.

[37] 郑严. 公开信道密钥协商中的信息协调[D]. 重庆: 西南大学, 2009.
ZHENG Y. Information Reconciliation of Secret key Agreement on Public Channel[D]. Chongqing: Southwest University, 2009.

[38] LAI L F, LIANG Y B, DU W L. PHY-based cooperative key generation in wireless networks[C]//Proceedings of 2011 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton). Piscataway: IEEE Press, 2011: 662-669.

[作者简介]

黄晶晶（1985− ），女，博士，北京赛西科技发展有限责任公司高级工程师，主要研究方向为工业信息安全。