文章编号：2095-4980(2017)05-0834-07

一种基于信道特征参数的无线通信密钥生成方法

陈许星[1,2]，何遵文[1]，张　焱[1]，陈　翔[2]

(1.北京理工大学 信息与电子学院，北京 100081；2.深圳清华大学研究院，广东 深圳 518057)

摘　要：无线通信由于自身传输信道的开放性，其安全问题相对于有线通信更为突出。物理层安全技术利用无线通信信道天然的多径时变特性，可为无线传输提供物理层加密，因而近年来得到快速发展。针对传统物理层安全中密钥生成速率低、频分双工系统不适用等问题，提出了一种基于信道特征参数的无线通信密钥生成方法。基于宽带信号对多径的辨识力，利用各径间相对时延生成初始密钥，结合码本进行密钥长度扩展，从而生成最终密钥。通过数值分析证明，相对于传统物理层密钥生成方式，所提方法能显著提高密钥生成速率，同时，基于时延信道特征的互易性，该方法可适用于时分双工和频分双工无线通信系统的物理层加密。

关键词：物理层安全；信道互易性；信道特征；多径时延；密钥生成

中图分类号：TN918.8^{+}2　　**文献标志码：**A　　**doi：**10.11805/TKYDA201705.0834

A key generation scheme for wireless communication based on channel characteristics

CHEN Xuxing[1,2], HE Zunwen[1], ZHANG Yan[1], CHEN Xiang[2]

(1.School of Information and Electronics, Beijing Institute of Technology, Beijing 100081, China; 2.Research Institute of Tsinghua University in Shenzhen, Shenzhen Guangdong 518057, China)

Abstract: Due to the openness of propagation channel, the security problem in the wireless communication systems is more serious than that in the wired communication systems. Physical layer security technology adopts the time-variant multipath characteristic of wireless communication channel to ensure security transmission in physical layer. Thus, the physical layer security technology has been developed rapidly in recent years. Traditional physical layer security technologies can just provide low key generation rate, and it cannot be applied to frequency division duplex systems. A scheme of key generation based on channel characteristics is proposed. Based on the multipath identification of wideband signal, this scheme utilizes relative time delays between paths to generate initial key. Then, the length of initial key is extended to generate the final key. The numerical analysis shows that compared with the traditional physical layer key generation scheme, this scheme can significantly improve the key generation rate. And because of the reciprocity of multipath delay, this scheme can be applied to the physical layer encryption of both the Time Division Duplex(TDD) and Frequency Division Duplex(FDD) wireless communication systems.

Keywords: physical layer security; channel reciprocity; channel characteristics; multipath time delay; key generation

目前无线通信在军事和民用领域都有着广泛的应用，但无线通信特有的开放特性导致无线信息传输的安全性较低。传统的解决方法是在网络层通过公私密钥对数据进行加密。但是在动态的无线网络中，对称加密方法需要解决无线通信下密钥分发的难题，密钥分发一方面引入额外的复杂度和成本，无法对密钥进行快速更新或一次一密；另一方面分发过程中容易泄密。而非对称密钥算法需要移动节点较难负担的高功率和高运算成本[1]。

为改进传统网络层加密的这些缺点，基于无线信道的物理层密钥生成方法被提出[2]。这类方法一般用于时分双工(TDD)通信系统，首先需要采集上、下行信道的接收信号强度(Received Signal Strength，RSS)、多径时延信息或相位信息等信道参数，其中接收信号强度最为常用。例如文献[3]中就以接收信号强度为依据，提出了一个环境自适应密钥生成方案。另外文献[4]尝试使用相对时延与平均时延的差值生成密钥。文献[5]给出了一种基于

收稿日期：2016-11-15；**修回日期：**2016-11-24
基金项目：国家 863 科技计划资助项目(2015AA01A708)；深圳市基础研究资助项目(JCYJ20150630153033410；JCYJ20160429170032960)

信道量化隔离带的相位密钥生成新方法。由于相干时间内 TDD 通信系统上下行信道具有互易性，通信双方所采集的信道参数基本一致。然后通信双方分别对所采集的信道参数量化处理得到二进制序列并将其作为初始密钥，由于采集到的信道参数一致性很高，初始密钥一般差别很小。最后通信双方通过信息调和，对初始密钥进行校正，最终获得完全相同的密钥。这种方法的最大特点是利用信道参数获得密钥。其运算成本一般低于传统网络层加密方法，也没有密钥分发的问题。

但是这类方法也有不足之处：一是信道参数的采样间隔必须长于信道变化的相干时间。如果采样间隔短于相干时间，将会造成所采集的信道参数相关性较大，若要考虑去相关则会增加很多运算成本。如果提高采样间隔，则会使单位时间采集到的信道参数样本减少，而导致密钥生成速率降低。特别是当通信系统处于静态环境下，信道变化较慢，相干时间较长，密钥生成速率较低，且安全性不佳；尽管文献[6]中通过引入多天线，提升了密钥生成速率，但相应的设备复杂度和成本也线性提升。二是这类方法依靠 TDD 通信系统上下行信道信道特性的互易性，依靠对接收信号强度的量化处理生成密钥。但实际应用中，大量无线和移动通信系统采用频分双工(FDD)方案。FDD 通信系统中上下行信道频率不同，无线通信在复杂环境下的多径效应会导致频率选择性衰落，亦即不同频率的信号经历相同的传播环境其信道特性不同。因此，FDD 通信系统中上下行信道的接收信号强度不具有一致性，上述物理层密钥生成方法无法有效应用。尽管文献[7]中使用信道增益补偿辅助密钥提取方案应对实践中遇到的非互易信道，文献[8]通过侧信道信息来提取密钥，但相应的计算复杂度也大幅提升。

综上，以上各种密钥生成方案难以在设备、计算复杂度和密钥生成速率之间取得较好的平衡。也没有 FDD 系统下的实用密钥生成方案。本文针对这些问题提出了一种基于信道特征参数的无线通信密钥生成方法，使用导频信号进行信道估计，提取多径时延信息，并生成初始密钥，再结合密码学中的码本机制，以初始密钥作为码本号进行密钥长度扩展，将初始密钥扩展成最终密钥。本方案能以较小运算量极大提高密钥生成速率，解决现有基于无线信道特征提取的物理层密钥生成技术中运算量大，密钥生成速率低，不适用于 FDD 通信系统的问题。

1　系统模型

本文研究的系统见图 1，Alice 和 Bob 代表通信中合法的收发双方，Eve 代表想要获取通信内容的被动窃听者，三者都处于多径衰落环境。设定系统使用 TDD 的通信方式，收发双方均为单天线。信道模型可表示为：

$$h(t)=\sum_{i=1}^{N}A_i\delta(t-\tau_i) \tag{1}$$

式中：$h(t)$为 t 时刻的信道响应；N 为多径数量；A_i 与 τ_i 分别为对应多径的信道增益与时延；$\delta(t)$为 t 时刻的冲激函数。在 Alice 与 Bob 的一次互相发送导频序列的通信过程中，由于 TDD 系统的特点，通信双方向对方发送信息不能同时进行，所以 Alice 向 Bob 发送导频序列时的信道响应和 Bob 向 Alice 发送导频序列时的信道响应可分别表示为：

$$h_{\mathrm{AB}}(t)=h(t) \tag{2}$$

$$h_{\mathrm{BA}}(t)=h(t+\tau_0) \tag{3}$$

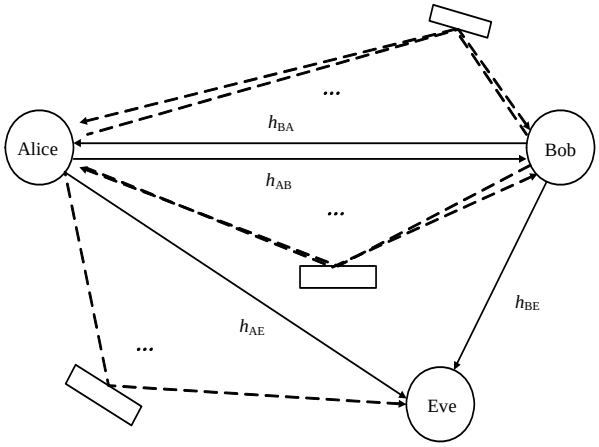

Fig.1 System model
图 1　系统模型示意图

假设导频序列持续时间远短于信道相干时间，则在发送导频序列期间信道响应可看作不随时间变化的定值 h_{AB} 和 h_{BA}。上式中 τ_0 代表 2 次通信间的时间间隔。由信道互易性原理可知，如果 τ_0 小于信道相干时间 τ_{c}，则 $h(t)$ 与 $h(t+\tau_0)$之间有很强的相关性。由此推得，当 τ_0 足够小时，$h_{\mathrm{AB}}=h_{\mathrm{BA}}$ 成立。同样由信道互易性原理可知，仅在 Eve 与 Bob 之间的距离小于相干距离时，才会有 $h_{\mathrm{AB}}=h_{\mathrm{AE}}$。

假设 Alice 与 Bob 分别向对方发送相同的训练序列 $s(t)$，Alice 与 Bob 分别接收到对方的信号可表示为：

$$y_{\mathrm{A}}(t)=h_{\mathrm{AB}}\times s(t)+n_{\mathrm{AB}}(t) \tag{4}$$

$$y_{\mathrm{B}}(t)=h_{\mathrm{BA}}\times s(t)+n_{\mathrm{BA}}(t) \tag{5}$$

Eve 收到的 Alice 与 Bob 的信号可以表示为：

$$y_{\mathrm{AE}}(t)=h_{\mathrm{AE}}\times s(t)+n_{\mathrm{AE}}(t) \tag{6}$$

$$y_{\mathrm{BE}}(t)=h_{\mathrm{BE}}\times s(t)+n_{\mathrm{BE}}(t) \tag{7}$$

式中 $n_{\mathrm{AB}}(t)$ 为 Alice 端的接收噪声，假设其为高斯白噪声，同理 $n_{\mathrm{BA}}(t)$ 为 Bob 端的接收噪声。由上文分析可知，假如 Alice 与 Bob 互相发送导频序列的过程在相干时间内完成时，有 $h_{\mathrm{AB}}=h_{\mathrm{BA}}$。相干距离通常与载波波长同一数量级，实际情况下 Eve 与 Alice 或 Bob 之间的距离不可能小于相干距离，所以 h_{AE}，h_{BE} 与 h_{AB}，h_{BA} 不相关，$h_{\mathrm{AB}}=h_{\mathrm{BA}}\neq h_{\mathrm{AE}}\neq h_{\mathrm{BE}}$。Alice 与 Bob 收到的信号 $y_{\mathrm{A}}(t)$ 与 $y_{\mathrm{B}}(t)$ 区别仅在于噪声不同，而 Eve 收到的信号 $y_{\mathrm{AE}}(t)$，$y_{\mathrm{BE}}(t)$ 与 $y_{\mathrm{A}}(t)$，$y_{\mathrm{B}}(t)$ 没有任何相关性。由此可知 Eve 无法由窃听到的信息获得 Alice 与 Bob 之间的共有信道特性信息。并且信道特性会随时间不断无规律变化，因此基于信道特征参数提取的密钥是可以不断更新的。

同样采用图 1 的系统模型，假设系统使用 FDD 的通信方式，收发双方依然是单天线。FDD 方式下 Alice 与 Bob 同时发送导频序列，此时信道响应可分别表示为：

$$h_{\mathrm{AB}}(t)=\sum_{i=1}^{N}A_{1i}\delta(t-\tau_{1i}) \tag{8}$$

$$h_{\mathrm{BA}}(t)=\sum_{i=1}^{M}A_{2i}\delta(t-\tau_{2i}) \tag{9}$$

式中：N 和 M 分别为上下行信道的多径数目；A_{1i} 和 A_{2i} 分别是上下行信道中第 i 径的增益，τ_{1i} 和 τ_{2i} 分别是上下行信道中第 i 径的时延。多径效应造成的频率选择性衰落的特性导致 Alice 与 Bob 间的上下行信道的信道响应 h_{AB} 与 h_{BA} 并不一致，但多径效应所造成的时延扩展是由反射及散射时传播路径引起的现象，与载波频率无关，仅与传播路径有关。因此可得知 $N=M$，$A_{1i}\neq A_{2i}$，$\tau_{1i}=\tau_{2i}$。而 Eve 与 Alice 或 Bob 之间信号的传播路径与合法信道不同，因此多径时延不同。综上所述，FDD 通信模式下 Alice 与 Bob 之间上下行信道的多径时延信息相同，且随着周围环境的变化而变化。利用多径时延信息提取的密钥适用于 FDD 系统且可以不断更新，具有良好的安全性。

2 密钥生成方案

针对如今各种密钥生成方案难以在设备、计算复杂度和密钥生成速率之间取得较好的平衡，也没有 FDD 系统下的实用密钥生成方案，本文提出一种基于信道特征参数的无线通信密钥生成方法，包括多径时延提取、量化、密钥一致性协商、密钥长度扩展这 4 个阶段，见图 2。

由对系统模型的分析可知，利用多径时延信息提取密钥的方法可以同时适用于 TDD 和 FDD 系统。而为应对通信信道变化较慢导致密钥生成速率较低的情况，结合码本进行密钥长度扩展的方法可以达到提高密钥生成速率的效果。

2.1 多径时延提取

通信开始时通信发起方 Alice 先发送第一导频信号 $s(\tau)$，通信接收方 Bob 接收到数据样本 $r(t,\tau)$，通过将 $r(t,\tau)$ 与第一导频信号的本地样本 $s(\tau)$ 作相关运算，就可以得到信道冲激响应：$h(t,\tau)=r(t,\tau)\otimes s(\tau)$。信道冲激响应 $h(t,\tau)$ 是时间和时延的函数，由 $h(t,\tau)$ 可以算出信道的功率时延谱 $PDP(t,\tau)=|h(t,\tau)|^2$。假设 Bob 接收到数据样本的时间为 t_0，算出信道的功率时延谱为 $PDP(t_0,\tau)$。Bob 接收到导频信号的数据样本后同样发送一段导频信号 $s'(\tau)$。Alice 接收后经相同处理获得 $PDP'(t_0+\Delta t,\tau)$，其中 Δt 应小于相干时间。

如果使用 TDD 通信方式，$PDP(t_0,\tau)$ 与 $PDP'(t_0+\Delta t,\tau)$ 近似相同，上下行信道频率不同。由于频率选择性衰落的原因，$PDP(t_0,\tau)$ 与 $PDP'(t_0+\Delta t,\tau)$ 是不同的，但相干时间内上下行信道各多径分量的到达时间基本一致，所以 $PDP(t_0,\tau)$ 与 $PDP'(t_0+\Delta t,\tau)$ 中各峰值对应的 τ 是相同的。理论上在 FDD 通信系统中，基于多径相对时延生成密钥的方法依然可以使用。

选取功率时延谱上功率最高点，以其为基准在–20 dB 处设置门限。超过这一门限的簇看作是一条多径分量。从区分出的各条多径分量选取最先到达的 n+1 条多径，记录下到达时间 $[t_1,t_2,\cdots,t_{n+1}]$。获得其中相邻多径分量的到达时间间隔 $[\tau_1,\tau_2,\cdots,\tau_n]$。

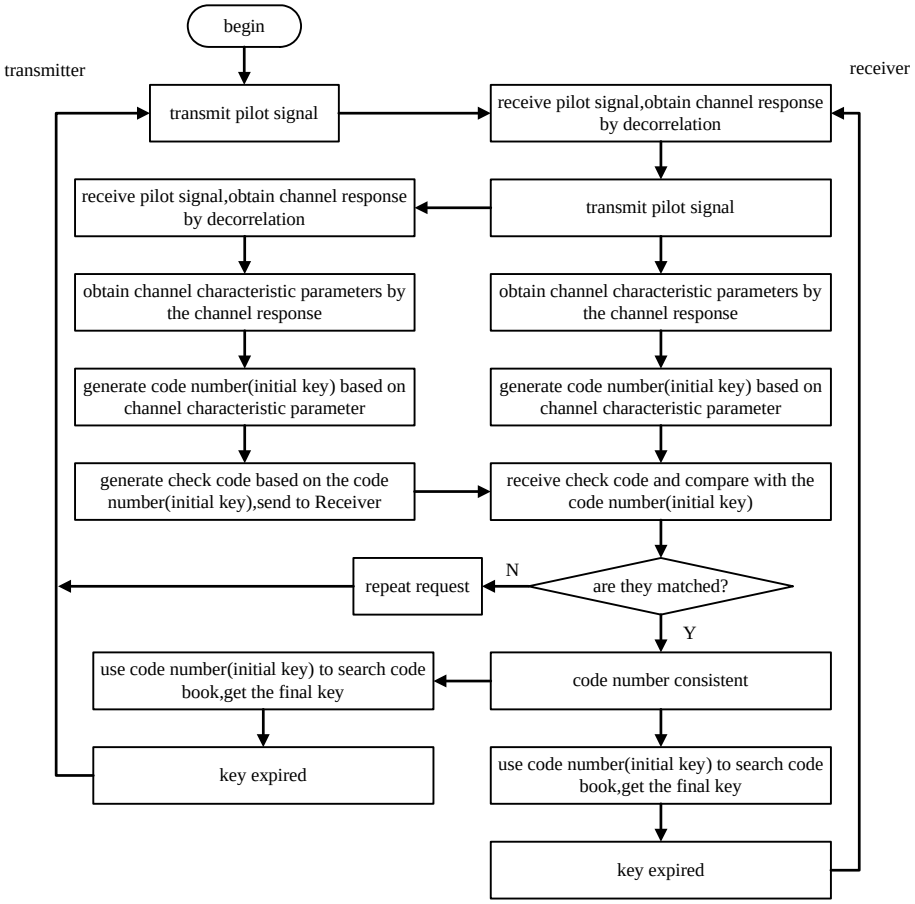

Fig.2 Flow of key generation
图 2 密钥生成方案流程图

2.2 多径时延量化

由多径到达时间 $[t_1,t_2,\cdots,t_{n+1}]$ 求出相邻多径分量的到达时间 $[\tau_1,\tau_2,\cdots,\tau_n]$，其中 $\tau_i=t_{i+1}-t_i$，$i=1,2,\cdots,n$。然后求出 $[\tau_1,\tau_2,\cdots,\tau_n]$ 的平均值 τ_m，将 $\tau_1,\tau_2,\cdots,\tau_n$ 分别与其比较进行量化。量化方式为：

$$d_i=\begin{cases}00, & \tau_i\leqslant\dfrac{\tau_m}{2}\\ 01, & \dfrac{\tau_m}{2}<\tau_i\leqslant\tau_m\\ 10, & \tau_m<\tau_i\leqslant\dfrac{3\tau_m}{2}\\ 11, & \dfrac{3\tau_m}{2}<\tau_i\end{cases},\quad i=1,2,\cdots,n \tag{10}$$

将量化得到的值依次拼接起来，生成长为 $2n$ 位的初始密钥 d_{Alice} 和 d_{Bob}。

2.3 密钥一致性协商

密钥一致性协商有很多种成熟的方案，这里仅以最简单的奇偶校验为例进行说明。Alice 由初始密钥 d_{Alice} 生成奇校验码 e_{Alice} 发送给 Bob，Bob 结合收到的奇校验码 e_{Bob} 与初始密钥 d_{Bob} 判断 d_{Alice} 和 d_{Bob} 是否相同，若有误则通知 Alice 重新执行以上步骤，若无误则反馈无误信息通知 Alice。

2.4 密钥长度扩展

结合码本进行密钥长度扩展的方法，简单来说就是找到一种映射关系(码本)，使长度较短的二进制序列(码本号)映射为长度较长的二进制序列(密码)。例如，以 m 序列作为初始密钥与最终密钥的映射关系，初始密钥相当于码本号，最终密钥相当于码本中对应的密码。图 3 为 n 阶 m 序列的生成示意图，通信双方使用相同的 n 位初

始密钥 $[d_1,d_2,\cdots,d_n]$ 作为初始序列 $[a_0,a_1,\cdots,a_{n-1}]$，经 n 位线性反馈移位寄存器生成 2^n-1 位的 m 序列作为最终密钥序列，以此密钥序列对信息加密进行接下来的通信。

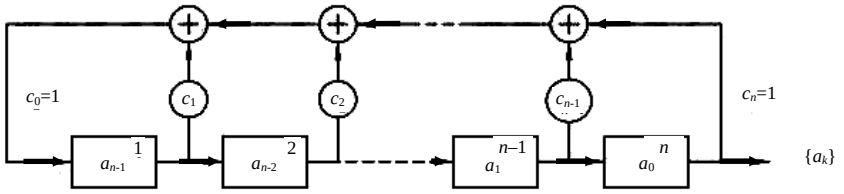

Fig.3 Generation of n order m sequence
图 3 n 阶 m 序列的生成示意图

Alice 与 Bob 结束了一轮通信后，重新执行以上步骤，生成新的密钥，在前后 2 次通信间隔大于相干时间的情况下可以实现一次一密，当通信间隔较短时也可以双方规定好通信次数 N，当密钥使用 N 次后重新生成密钥，还可以双方规定密钥过期时间 T，当密钥使用时间达到 T 时重新生成密钥。

3 仿真结果分析

为了评估所提结合码本的基于多径相对时延的密钥生成方案的性能，采用 IMT-Advanced 标准化信道模型[9]生成宽带随机信道响应，在此基础上生成密钥并与传统方式进行对比。

不失一般性，选取城区非视距场景进行分析。设定载波中心频率为 TD-LTE 常用频段 2.6 GHz，假设多径数目 N=20，噪声为高斯白噪声。Alice,Bob 和 Eve 为单天线节点，其初始位置关系及运动状态随机生成。采样间隔设定为大于相干时间进行 5 000 次采样。每 1 次采样生成 1 次密钥，以生成初始密钥完全一致的次数除以采样次数作为初始密钥的一致概率。

使用上文所提的密钥生成方案，选取 5 条多径。获得 4 个多径相对时延，对这 4 个多径相对时延量化得到 8 位初始密钥。作为对比，选取了传统的基于多径 RSS 信息的密钥生成方法[10]，首先找到功率时延谱上功率最高点，以其为基准在–20 dB 处设置门限，超过这一门限的簇可以看作是一条多径分量。然后，从区分出的各条多径分量选取最先到达的 4 条多径，将这 4 条多径的功率进行量化，获得 8 位初始密钥。

图 4 给出了在不同信噪比下 Alice,Bob 和 Eve 三者生成的初始密钥的一致概率。从图中可以看到，不同信噪比条件下 Eve 生成的初始密钥与 Alice 生成的初始密钥的一致概率一直保持在极低的水平，这表明 Eve 与 Alice 生成的初始密钥一致性很低。使用 RSS 信息生成密钥的方法受噪声影响较大，在信噪比较低的情况下，Alice 和 Bob 生成的初始密钥一致概率很低，表明低信噪比条件下 Bob 与 Alice 使用 RSS 信息生成的初始密钥一致性较低。原因是 RSS 值受噪声直接影响，噪声对其量化值影响很大。而使用多径相对时延的方法受噪声影响较小，在信噪比很小的情况下 Alice 和 Bob 依然能保持很高的初始密钥一致概率，即 Bob 与 Alice 生成的初始密钥一致性一直保持在较高水平。原因在于使用多径相对时延生成密钥时，噪声仅影响对多径信号的判断，并不能直接影响多径相对时延的数值。

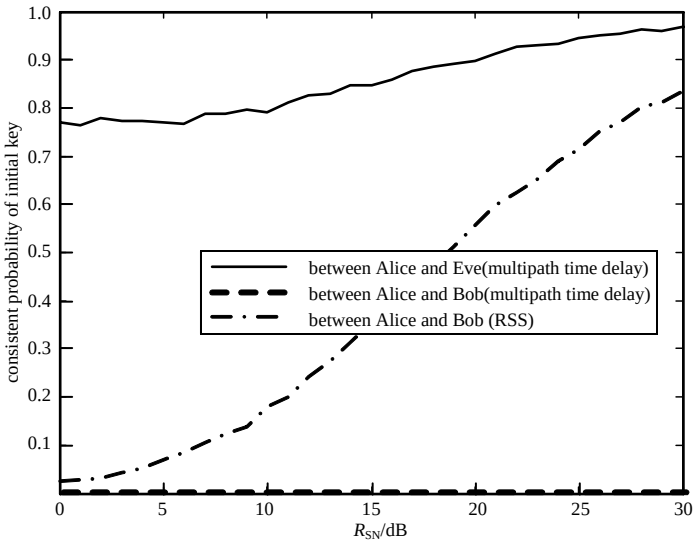

Fig.4 Consistent probability of initial key
图 4 初始密钥的一致概率

传统基于 RSS 生成密钥的方法以各多径的 RSS 量化值直接作为最终密钥使用，而结合码本的密钥长度扩展方法将多径信道信息的量化值作为生成 m 序列的初始序列，将最后生成的 m 序列作为最终密钥使用。所以同样是从多径信道中提取 8 bit 的密钥，本文所提方法可以将其扩展为 255 bit，极大提升密钥生成速率。

图 5 给出了 Alice 和 Bob 之间与 Alice 和 Eve 之间最终密钥的平均相关度。平均相关度是由所选两节点每一次采样生成的最终密钥之间的相关系数取平均求得，代表着最终密钥的相似程度。Alice 与 Eve 生成的最终密钥的平均相关度几乎为零，这代表 Eve 几乎无法获得任何合法信道的有用信息，Eve 无法生成与 Alice 相同的最终密钥。Alice 与 Bob 生成的最终密钥一直保持着很高的相关度，这代表 Alice 与 Bob 获得的合法信道的信息一致性很高。即使在很低的信噪比条件下，Alice 与 Bob 生成的最终密钥依然有很高的一致性。

在 FDD 通信系统中，上下行信道的多径数量和多径时延相同，多径增益不同[11]。可以使用多径时延相同，多径增益不同的设定来模拟 FDD 通信系统的上下行信道。在这种条件下，选取城区非视距场景，设多径数目 N=20，噪声为高斯白噪声，信噪比 10 dB。Alice，Bob 和 Eve 为单天线节点，其位置关系及运动状态随机生成。基于多径相对时延生成密钥和基于 RSS 生成密钥生成的初始密钥见图 6。

在 FDD 通信中，合法节点使用基于 RSS 生成密钥的方式产生的密钥有较大差异，说明基于 RSS 生成密钥的方式并不适用于 FDD 通信系统。这也与上文的分析相符。而合法节点使用基于多径时延生成密钥的方式产生的密钥具有很好的一致性，可见在 FDD 通信系统中基于多径相对时延生成密钥的方法依然可以使用。

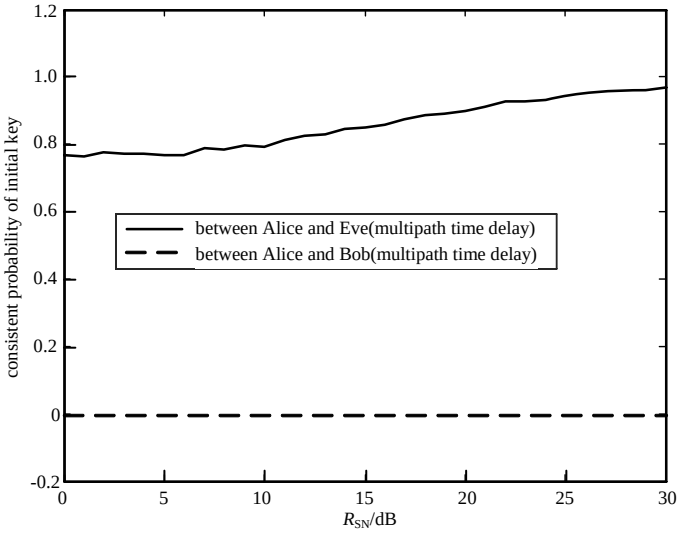

Fig.5 Average correlation of final key
图 5 最终密钥的平均相关度

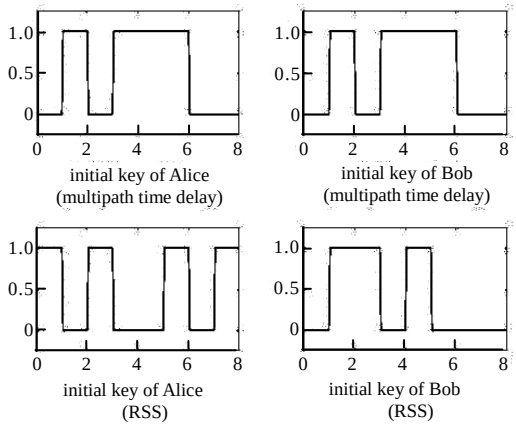

Fig.6 Initial key generation based on RSS and multipath relative time delay
图 6 基于 RSS 生成的初始密钥和基于多径相对时延生成的初始密钥

4　结论

针对现有的物理层密钥生成方法密钥生成速率低，不适用于 FDD 系统的问题，提出了一种基于信道特征参数的无线通信密钥生成方案。该方案利用信道估计方法提取多径时延信息，并生成初始密钥，经密钥一致性协商后，再结合密码学中的码本机制，以初始密钥作为码本号进行密钥长度扩展，将初始密钥扩展成最终密钥。数值结果表明，与传统的基于 RSS 的密钥生成方案相比，本方案具有良好的密钥一致性和抗噪声性能，同时具有更高的密钥生成速率，且适用于 FDD 系统，因而可以为未来高速无线通信网络的大规模应用提供信息安全保障。

参考文献：

[1] 冯文江. 一种用于无线协作通信网络的非对称信道通信密钥生成方法: 201210330144.4[P]. [2016-09-10]. (FENG Wenjiang. An asymmetric channel communication key generation method for wireless cooperative communication networks: 201210330144.4[P]. [2016-09-10].)

[2] MAURER U M. Secret key agreement by public discussion from common information[J]. IEEE Transactions on Information Theory, 1993,39(3):733-742.

[3] 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.

[4] LIU H,WANG Y,YANG J,et al. Fast and practical secret key extraction by exploiting channel response[C]// Proceedings of 2013 IEEE International Conference on Computer Communications. Turin,Italy:[s.n.], 2013:3048-3056.

[5] 盛旺,侯晓赟,朱艳,等. 无线通信中基于量化隔离带的新型相位密钥生成方法[J]. 计算机应用研究, 2014,31(10):3100-3103. (SHENG Wang,HOU Xiaoyun,ZHU Yan,et al. New kind of phase key generation method in wireless communications

based on channel quantization with guard-bands[J]. Application Research of Computers, 2014,31(10):3100-3103.)
[6] HUANG P,WANG X. Fast secret key generation in static wireless networks: a virtual channel approach[C]// 2013 Proceedings IEEE INFOCOM. Turin,Italy:[s.n.], 2013:2292-2300.
[7] 周百鹏,黄开枝,金梁,等. 一种基于多径相对时延的密钥生成方法[J]. 计算机应用研究, 2011,28(6):2196-2198. (ZHOU Baipeng,HUANG Kaizhi,JIN Liang,et al. Scheme of key generation based on multipath relative-delay[J]. Application Research of Computers, 2011,28(6):2196-2198.)
[8] LI H,ZHANG Q,YUAN H. Channel state information based key generation vs. side-channel analysis key information leakage[C]// 2011 International Conference on Network and System Security. Milan,Italy:[s.n.], 2011:264-268.
[9] Report ITU-R M.2135-1. Guidelines for evaluation of radio interface technologies for IMT-Advanced[S]. 2009-12.
[10] JANA S,PREMNATH S N,CLARK M,et al. On the effectiveness of secret key extraction from wireless signal strength in real environments[C]// International Conference on Mobile Computing and NETWORKING. Beijing,China:ACM, 2013:321-332.
[11] LIANG Y C,CHIN F. Downlink channel covariance matrix(DCCM) estimation and its application in Wireless DS-CDMA Systems[J]. IEEE Journal on Selected Areas in Communications, 2001,19(2):222-232.

作者简介：

陈许星(1991-)，男，湖北省荆州市人，在读硕士研究生，主要研究方向为物理层安全.email: 976592037@qq.com.

陈　翔(1980-)，男，长沙市人，博士，副教授，主要研究领域为 5G 移动通信与物联网、卫星通信、软件无线电.

何遵文(1964-)，男，湖北省潜江市人，博士，副教授，主要研究领域为数字移动通信和抗干扰通信.

张　焱(1983-)，男，山东省德州市人，博士，副教授，主要研究领域为第五代移动通信、无线信道建模理论、物理层安全与大数据处理技术.