面向物联网准静态信道的中继协作密钥生成方法

肖帅芳*　郭云飞　白慧卿　金 梁　黄开枝
(国家数字交换系统工程技术研究中心　郑州　450002)

摘　要：针对物联网准静态信道下密钥生成速率低的问题，该文提出一种基于中继节点协作的密钥生成方法。首先，通信双方通过信道估计获得直达信道和部分中继信道信息；然后，中继节点采用网络编码技术参与协作，使得通信双方获取全部中继信道信息；最后，通信双方在直达信道上进行密钥协商，利用直达信道信息、中继信道信息与协商信息共同生成相同的密钥。安全性分析表明该方法能够提高可达密钥速率，并且随着信噪比的提高，可达密钥速率呈线性增长，趋于最优值。蒙特卡洛仿真验证了理论分析的结果，并得出了增加中继节点数量、选取信道变化幅度大的中继节点，可以进一步提高可达密钥速率。

关键词：物理层安全；密钥生成；物联网；中继协作
中图分类号：TN918.82　　**文献标识码**：A　　**文章编号**：1009-5896(2018)01-0050-07
DOI: 10.11999/JEIT170384

Relay Cooperative Secret Key Generation for Quasi-static Channels in Internet of Things

XIAO Shuaifang　GUO Yunfei　BAI Huiqing　JIN Liang　HUANG Kaizhi
(*National Digital Switching System Engineering & Technological Research Center*, *Zhengzhou* 450002, *China*)

Abstract: A secret key generation scheme based on a cooperative relay is proposed to improve the generated secret key rate for quasi-static channels in Internet of things. Firstly, the two legitimate nodes send training sequences to estimate the direct channel information, respectively. After that the relay employs network coding technique to participate the cooperation, and assists the two legitimate nodes to obtain the relay channels information. Finally, the two legitimate nodes agree on a secret key from the direct and relay channels information using the direct channel without the help of the relay. Security analysis results show that the scheme can improve the achievable secret key rate, and the achievable key rate increases linearly with SNR, approaching the optimal rate. Monte Carlo simulation verifies the security analysis results, and obtains that increasing the relay nodes, selecting the relay with a larger variance channel can further improve the achievable secret key rate.

Key words: Physical layer security; Secret key generation; Internet of things; Relay cooperation

1　引言

近年来，以“万物互联”为愿景的物联网得到了学术界的广泛研究[1,2]，尤其是第 5 代移动通信(The Fifth Generation, 5G)在标准制定中将物联网纳入了应用范畴[3]，使得物联网进入普通人的生活变为可能。然而物联网的安全问题成为限制其发展的瓶颈，其中一个重要的安全威胁就是物联网一般采用无线信号作为传输媒介，信息暴露在空中，容易遭受恶意窃听。目前针对物联网保密通信的研究依然是沿用传统无线网络的高层加密体制，但物联网中节点数量巨大，密钥分发难以实现，且节点一般以自组织方式组网，没有可信任的第三方密钥管理中心，物联网的密钥管理面临严峻的挑战[4]。

无线物理层密钥生成技术的出现为保障无线通信安全提供了新的思路[5,6]，由于其利用无线信道的独有特性，合法通信双方直接从共享的无线信道中提取密钥，无需进行密钥分发，也不需要第三方密钥管理中心，且实现复杂度低，比较适用于物联网。文献[7]实验验证了物理层密钥生成技术在无线个域网中应用的可行性。文献[8]针对车联网场景，提出了一种基于接收信号强度的实用物理层密钥生成方案。然而在物联网的一些应用场景中，比如环境监测、智能家居等，节点是固定不动的，周围无线环

收稿日期：2017-04-26；改回日期：2017-09-11；网络出版：2017-11-01
*通信作者：肖帅芳　xiaoshuaifang@gmail.com
基金项目：国家自然科学基金(61379006)，国家 863 计划项目(2015AA01A708)，国家自然科学基金创新群体项目(61521003)
Foundation Items: The National Natural Science Foundation of China (61379006), The National 863 Program of China (2015AA01A708), The Science Fund for Creative Research Groups of the National Natural Science Foundation of China (61521003)

境的变化也十分缓慢，这就导致合法通信双方之间的无线信道是准静态的，此时基于无线信道特性生成的密钥速率很低，难以满足通信双方的保密通信需求[6]。

针对准静态信道下密钥生成速率低的问题已经开展了一些研究。文献[9]在 MIMO 场景下提出了基于随机波束成形的密钥提取方法，发送方对探测信号进行随机波束成形后再发送，接收方相应地做接收随机波束成形操作，反向探测信道是按同样的权值做发送波束成形和接收波束成形处理。最后，通信双方从接收到的信号中提取密钥，相当于将信道随机加权处理后提取密钥，就可以利用权值的随机性提升密钥源的随机性，从而提高密钥生成速率。文献[10]利用发送端为多天线的特点，通过随机改变不同天线上的幅度和相位，构建随机变化的虚拟信道，从虚拟信道中提取密钥，从而提高密钥生成速率。文献[11,12]利用协作节点的干扰来构建随机变化的等效信道，以此保证密钥源的随机性。然而以上方法均需利用多天线或者协作干扰，在资源严重受限的物联网中难以实现[13]。

物联网中节点数量多，且经常需要节点协作来传输信息，这为中继节点辅助的协作密钥生成创造了条件，通过中继节点协作，提取中继信道的随机性，可以增加密钥源的熵，从而提高密钥速率。文献[14]证明了中继节点协作可以提高密钥源的随机性，从而提高密钥容量，并给出了密钥容量的上界。文献[15]研究了双向中继系统的密钥生成，提出了 4 种基于放大转发(Amplify-and-Forward, AF)的密钥生成方案，但放大转发的过程中会导致部分信道信息泄露，从而降低了可达密钥速率。文献[16]研究了无线网络中的协作密钥生成，通过中继节点协作提高了密钥生成速率。但密钥的生成过程中通信双方和中继节点之间均需两两进行密钥协商，复杂度较高。并且中继节点需要多次参与协商，耗费自身很多资源和能量，从节点自私性出发，中继节点可能会拒绝参与多次协商，从而导致密钥生成过程失效。

针对以上问题，本文结合物联网的实际应用特点，提出了一种基于中继节点协作的密钥生成方法。首先针对典型的 4 节点系统(合法通信双方 Alice 与 Bob、一个中继节点 Relay、一个窃听者 Eve)建立了中继节点协作密钥生成模型。在此基础上，首先进行信道估计，使得 Alice 与 Bob 估计出直达信道和部分中继信道信息；然后中继节点采用网络编码技术参与协作，使得 Alice 与 Bob 获取全部中继信道信息；最后合法通信双方在直达信道上进行密钥协商，利用直达信道和中继信道信息与协商信息共同生成密钥。安全性分析表明该方法能显著提高 Alice 与 Bob 间的可达密钥速率，并且随着信噪比的提高，可达密钥速率呈线性增长，趋于最优值。蒙特卡洛仿真验证了理论分析的结果，并通过针对不同中继协作节点数量与不同中继信道方差的仿真，得出了增加中继节点数量，选取信道变化幅度大的中继节点，可以进一步提高 Alice 与 Bob 之间的可达密钥速率，从而为多个中继节点场景下，进一步提高可达密钥速率指明了方向。

2　系统模型

针对物联网中基于中继节点协作的密钥生成系统进行建模，如图 1 所示。Alice (A)和 Bob (B)为合法通信双方，均为单天线。Relay 为中继节点，在 Alice 与 Bob 的通信范围内，可以直接和 Alice, Bob 通信，也配备单天线，假设 Relay 是友好可信的。在这些合法节点的通信范围内，存在一个 Eve 试图窃取保密信息，也配备单天线。Alice 和 Bob 之间可以直接通信，也可以通过 Relay 通信。Alice 与 Bob 之间的直达信道可以满足它们的数据通信需求，即在数据通信阶段，Alice 与 Bob 直接通信，不经过 Relay 转发，Relay 只需参与 Alice 和 Bob 的密钥生成过程。我们考虑实际的通信场景，节点间均不存在无噪的公共信道，节点间的所有通信及协商过程都在无线信道上进行，占用通信资源。

节点之间的信道建模为准静态块衰落信道，即在相干时间 T 内信道是不变的，在不同的相干时间内为衰落信道。不同节点之间的信道是相互独立的，且满足互易性。令 h_{ij} 表示节点 i 到节点 j 的信道增益，则 $h_{AB}=h_{BA}=h_0$, $h_{AR}=h_{RA}=h_1$, $h_{BR}=h_{RB}=h_2$ 。假定 Alice, Bob, Relay 与 Eve 接收到的噪声均为独立同分布的高斯白噪声，均值为 0，方差为 σ_n^2 。为了便于分析，我们将直达信道增益 h_0 建模为均值为 0、方差为 σ_0^2 的高斯随机变量，将中继信道增益 h_1 , h_2 建模为均值为 0、方差为 σ_1^2 的高斯随机变量。其他衰落信道模型的分析方法类似，很容易进行推广。

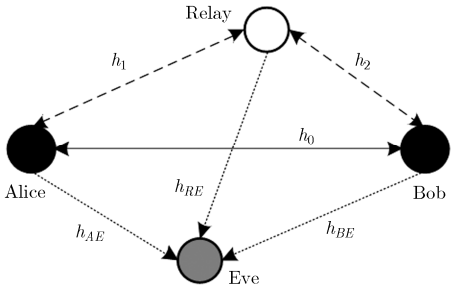

图 1 中继节点协作密钥生成系统模型

Eve 可以观测到 Alice, Bob 和 Relay 发送的信号，h_{AE}，h_{BE}，h_{RE} 分别表示 Alice, Bob, Relay 到 Eve 的信道增益。Eve 为了不暴露身份，仅被动窃听，不发送干扰，不参与通信过程与密钥生成过程。并且为了不被发现，Eve 距离 Alice, Bob 和 Relay 不能很近，满足几个波长以上的距离要求，这保证了 h_{AE}，h_{BE}，h_{RE} 与 h_0，h_1，h_2 均是不相关的，使得 Eve 无法估计出 h_0，h_1，h_2 的任何信息。

基于上述模型，本文提出了基于中继节点协作的密钥生成方法。为了从无线信道信息中生成密钥，首先进行信道估计，Alice 与 Bob 可估计出直达信道信息；然后，为了提高 Alice 与 Bob 之间的共同信息，中继节点采用网络编码技术参与协作，使得 Alice 与 Bob 获取中继信道信息；最后 Alice 与 Bob 直接在直达信道上进行密钥协商，以直达信道和中继信道信息为密钥源协商生成相同的密钥。相对于放大转发方法[15]，该方法不会造成噪声放大，提高了合法通信双方密钥源的相关性；相对于现有中继协作方法[16]，该方法不需要中继节点参与密钥协商，降低了中继节点协作的代价。

3 中继协作密钥生成方法

中继协作密钥生成方法分为 3 个阶段：信道估计、中继协作和密钥协商。考虑一个 Relay 的情况，此时 Alice, Bob 和 Relay 需要分别发送训练序列进行信道估计，占用 3 个时隙，中继协作需要占用 1 个时隙，密钥协商需要占用 1 个时隙。由于密钥生成的过程需要在一个相干时间内完成，可将相干时间 T 均匀分成 5 个时隙 T_1，T_2，T_3，T_4，T_5，即 $T_1=T_2=T_3=T_4=T_5=T/5$，时隙分配如图 2 所示。

3.1 信道估计阶段

在 T_1 时隙，Alice 发送已知的训练序列 $\boldsymbol{x}_A$，此时 Bob 接收到信号 $\boldsymbol{y}_{0,B}=h_0\boldsymbol{x}_A+\boldsymbol{n}_{0,B}$，Relay 接收到信号 $\boldsymbol{y}_{1,R}=h_1\boldsymbol{x}_A+\boldsymbol{n}_{1,R}$，其中 $\boldsymbol{n}_{0,B}$ 与 $\boldsymbol{n}_{1,R}$ 分别为当前时隙内 Bob 与 Relay 的接收噪声。Bob 估计 h_0，得到

$$\tilde{h}_{0,B}=\frac{\boldsymbol{x}_A^{\mathrm{T}}}{\|\boldsymbol{x}_A\|^2}\boldsymbol{y}_{0,B}=h_0+\frac{\boldsymbol{x}_A^{\mathrm{T}}}{\|\boldsymbol{x}_A\|^2}\boldsymbol{n}_{0,B} \tag{1}$$

其中，$(\bullet)^{\mathrm{T}}$ 表示向量或矩阵的转置。Relay 估计 h_1，得到

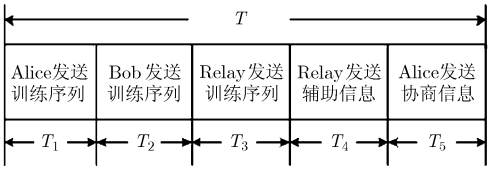

图 2 一个相干时间 T 内的时隙分配图

$$\tilde{h}_{1,R}=\frac{\boldsymbol{x}_A^{\mathrm{T}}}{\|\boldsymbol{x}_A\|^2}\boldsymbol{y}_{1,R}=h_1+\frac{\boldsymbol{x}_A^{\mathrm{T}}}{\|\boldsymbol{x}_A\|^2}\boldsymbol{n}_{1,R} \tag{2}$$

在 T_2 时隙，Bob 发送训练序列 $\boldsymbol{x}_B$，此时 Alice 接收到信号 $\boldsymbol{y}_{0,A}=h_0\boldsymbol{x}_B+\boldsymbol{n}_{0,A}$，Relay 接收到信号 $\boldsymbol{y}_{2,R}=h_2\boldsymbol{x}_B+\boldsymbol{n}_{2,R}$，其中 $\boldsymbol{n}_{0,A}$ 与 $\boldsymbol{n}_{2,R}$ 分别为当前时隙内 Alice 与 Relay 的接收噪声。Alice 估计 h_0，得到

$$\tilde{h}_{0,A}=\frac{\boldsymbol{x}_B^{\mathrm{T}}}{\|\boldsymbol{x}_B\|^2}\boldsymbol{y}_{0,A}=h_0+\frac{\boldsymbol{x}_B^{\mathrm{T}}}{\|\boldsymbol{x}_B\|^2}\boldsymbol{n}_{0,A} \tag{3}$$

Relay 估计 h_2，得到

$$\tilde{h}_{2,R}=\frac{\boldsymbol{x}_B^{\mathrm{T}}}{\|\boldsymbol{x}_B\|^2}\boldsymbol{y}_{2,R}=h_2+\frac{\boldsymbol{x}_B^{\mathrm{T}}}{\|\boldsymbol{x}_B\|^2}\boldsymbol{n}_{2,R} \tag{4}$$

在 T_3 时隙，Relay 发送训练序列 $\boldsymbol{x}_R$，此时 Alice 接收到信号 $\boldsymbol{y}_{1,A}=h_1\boldsymbol{x}_R+\boldsymbol{n}_{1,A}$，Bob 接收到信号 $\boldsymbol{y}_{2,B}=h_2\boldsymbol{x}_R+\boldsymbol{n}_{2,B}$，其中 $\boldsymbol{n}_{1,A}$ 与 $\boldsymbol{n}_{2,B}$ 分别为当前时隙内 Alice 与 Bob 的接收噪声。Alice 估计 h_1，得到

$$\tilde{h}_{1,A}=\frac{\boldsymbol{x}_R^{\mathrm{T}}}{\|\boldsymbol{x}_R\|^2}\boldsymbol{y}_{1,A}=h_1+\frac{\boldsymbol{x}_R^{\mathrm{T}}}{\|\boldsymbol{x}_R\|^2}\boldsymbol{n}_{1,A} \tag{5}$$

Bob 估计 h_2，得到

$$\tilde{h}_{2,B}=\frac{\boldsymbol{x}_R^{\mathrm{T}}}{\|\boldsymbol{x}_R\|^2}\boldsymbol{y}_{2,B}=h_2+\frac{\boldsymbol{x}_R^{\mathrm{T}}}{\|\boldsymbol{x}_R\|^2}\boldsymbol{n}_{2,B} \tag{6}$$

容易得到 $\tilde{h}_{0,A}$，$\tilde{h}_{0,B}$，$\tilde{h}_{1,A}$，$\tilde{h}_{1,R}$，$\tilde{h}_{2,B}$，$\tilde{h}_{2,R}$ 均是均值为0的高斯随机变量。假定Alice, Bob, Relay 发送 $\boldsymbol{x}_A$，$\boldsymbol{x}_B$，$\boldsymbol{x}_R$ 的功率均为 P，则 $\tilde{h}_{0,A}$ 的方差为 $\sigma_0^2+\dfrac{\sigma_n^2}{PT/5}$，即 $\tilde{h}_{0,A}\sim\mathcal{N}\left(0,\sigma_0^2+\dfrac{\sigma_n^2}{PT/5}\right)$。同理可得 $\tilde{h}_{0,B}\sim\mathcal{N}\left(0,\sigma_0^2+\dfrac{\sigma_n^2}{PT/5}\right)$，$\tilde{h}_{1,A}\sim\mathcal{N}\left(0,\sigma_1^2+\dfrac{\sigma_n^2}{PT/5}\right)$，$\tilde{h}_{1,R}\sim\mathcal{N}\left(0,\sigma_1^2+\dfrac{\sigma_n^2}{PT/5}\right)$，$\tilde{h}_{2,B}\sim\mathcal{N}\left(0,\sigma_1^2+\dfrac{\sigma_n^2}{PT/5}\right)$，$\tilde{h}_{2,R}\sim\mathcal{N}\left(0,\sigma_1^2+\dfrac{\sigma_n^2}{PT/5}\right)$。然而此时Alice与Bob的共同信息只有直达信道 h_0 的估计值。

3.2 中继协作阶段

Relay通过信道估计阶段估计出了 $\tilde{h}_{1,R}$ 与 $\tilde{h}_{2,R}$，因此可以通过Relay协作发送辅助信息，增加Alice与Bob之间的共同信息。Relay采用安全网络编码技术，利用 $\tilde{h}_{1,R}$ 与 $\tilde{h}_{2,R}$ 生成辅助信息，在 T_4 时隙，将辅助信息发送给Alice和Bob，以增加二者可获取的共同信息。为了保证私密性，将 $\tilde{h}_{1,R}$，$\tilde{h}_{2,R}$ 分别量化后求模2加，可得到 $S_R=\tilde{h}_{1,R}^{\Delta}\oplus\tilde{h}_{2,R}^{\Delta}$，将 S_R 作为辅助信息。为了实现无差错传输，Relay对 S_R 进行纠错编码，并经过调制后发送给Alice和Bob。虽然Relay与Alice, Bob之间不存在无噪的公共信道，但是Alice

和Bob已经分别估计出信道 h_1，h_2，且Relay对 S_R 进行了纠错编码，相当于构造了无噪的传输信道，使得Alice和Bob可以精确恢复出 S_R。采用的编码调制方案是公开的，Eve也可准确得到 S_R，但由于 S_R 是 $\tilde{h}_{1,R}^{\Delta}$ 与 $\tilde{h}_{2,R}^{\Delta}$ 的异或值，Eve依然无法获取 h_1 或 h_2 的任何信息。此时，Alice利用已估计出的 $\tilde{h}_{1,A}$，可估计 h_2，得到

$$\tilde{h}_{2,A}^{\Delta}=\tilde{h}_{1,A}^{\Delta}\oplus\left(\tilde{h}_{1,R}^{\Delta}\oplus\tilde{h}_{2,R}^{\Delta}\right) \tag{7}$$

Bob 利用已估计出的 $\tilde{h}_{2,B}$，可估计 h_1，得到

$$\tilde{h}_{1,B}^{\Delta}=\tilde{h}_{2,B}^{\Delta}\oplus\left(\tilde{h}_{2,R}^{\Delta}\oplus\tilde{h}_{1,R}^{\Delta}\right) \tag{8}$$

令量化间隔 Δ 趋近于 0，则量化带来的误差可忽略不计。这样，Alice 得到了 $\tilde{\boldsymbol{h}}_A=(\tilde{h}_{0,A},\tilde{h}_{1,A},\tilde{h}_{2,A})$，Bob 得到 $\tilde{\boldsymbol{h}}_B=(\tilde{h}_{0,B},\tilde{h}_{1,B},\tilde{h}_{2,B})$，从而提高了 Alice 与 Bob 之间的共同信息。Alice 与 Bob 就可以通过密钥协商阶段，分别从 $\tilde{\boldsymbol{h}}_A$，$\tilde{\boldsymbol{h}}_B$ 中生成相同的密钥，相对于仅从直达信道 $\tilde{h}_{0,A}$，$\tilde{h}_{0,B}$ 中生成密钥，提升了密钥源的熵。

3.3 密钥协商阶段

Alice 在 T_5 时隙向 Bob 发送协商信息 $\boldsymbol{\Phi}$，Alice 与 Bob 根据共同信息 $(\tilde{\boldsymbol{h}}_A,\tilde{\boldsymbol{h}}_B)$ 与协商信息 $\boldsymbol{\Phi}$，生成相同的密钥 K。密钥 K 与可达密钥速率 R_s 需要满足式(9)的条件，给定任意的 $\varepsilon>0$ 和充分大的 n，

$$\left.\begin{aligned}&\frac{1}{n}I\left(K;S_R\right)\le\varepsilon\\&\frac{1}{n}I\left(K;\boldsymbol{\Phi}\right)\le\varepsilon\\&\frac{1}{n}H\left(K\right)\ge R_s-\varepsilon\\&\frac{1}{n}\lg|\mathcal{K}|\le\frac{1}{n}H\left(K\right)+\varepsilon\end{aligned}\right\} \tag{9}$$

其中，$I(X;Y)$ 表示随机变量 X 与 Y 的互信息，$H(X)$ 表示随机变量 X 的熵，$\mathcal{K}$ 为密钥 K 的有限字符集，$|\mathcal{K}|$ 为 $\mathcal{K}$ 的基数。根据文献[14]的结论，满足式(9)的可达密钥速率为

$$R_s=\frac{1}{T}I\left(\tilde{h}_{0,A},\tilde{h}_{1,A},\tilde{h}_{2,A};\tilde{h}_{0,B},\tilde{h}_{1,B},\tilde{h}_{2,B}\middle|S_R\right) \tag{10}$$

其中，$I(X;Y\mid Z)$ 表示随机变量 X 和 Y 在给定随机变量 Z 时的条件互信息。

为了使 Alice 和 Bob 得到相同的速率为 R_s 的密钥，Alice 可采用 Slepian-Wolf 编码，发送协商信息给 Bob，以消除信道估计中噪声的影响。虽然协商信息可以被 Eve 得到，但协商信息不泄露最终生成密钥的任何信息。Alice 将估计出来的 $\tilde{\boldsymbol{h}}_A$ 量化为二进制序列 $\tilde{\boldsymbol{h}}_A^{\Delta}=\left(\tilde{h}_{0,A}^{\Delta},\tilde{h}_{1,A}^{\Delta},\tilde{h}_{2,A}^{\Delta}\right)^{\mathrm{T}}$，其中 Δ 代表量化间隔。同样地，Bob 也可将估计出的 $\tilde{\boldsymbol{h}}_B$ 量化为二进制序列 $\tilde{\boldsymbol{h}}_B^{\Delta}=\left(\tilde{h}_{0,B}^{\Delta},\tilde{h}_{1,B}^{\Delta},\tilde{h}_{2,B}^{\Delta}\right)^{\mathrm{T}}$。然后，Alice 随机地将 $\tilde{\boldsymbol{h}}_A^{\Delta}$ 的典型序列集合分成不重叠的子集，每个子集包含 2^{TR_s} 个 $\tilde{\boldsymbol{h}}_A^{\Delta}$ 典型序列，这样每个典型序列包含两个索引：所在子集索引号和子集内的序列索引号。Alice 估计出 $\tilde{\boldsymbol{h}}_A$ 得到 $\tilde{\boldsymbol{h}}_A^{\Delta}$ 序列后，将该序列在子集内的索引号作为密钥 K，将该序列所在子集的子集索引号作为协商信息发送给 Bob, Alice 需要向 Bob 发送 $H\left(\tilde{\boldsymbol{h}}_A^{\Delta}\middle|\tilde{\boldsymbol{h}}_B^{\Delta},S_R\right)$ 比特信息，其中 $H(X\mid Y)$ 表示在给定随机变量 Y 时，随机变量 X 的条件熵。在实际的通信中，Alice 与 Bob 之间没有无噪的公共信道，协商信息需要在有噪的信道 h_0 上传输，因此 Alice 需要将协商信息进行适当的编码后发送，Bob 已进行过信道估计，可精确恢复出协商信息。Bob 收到协商信息后，结合自己估计出的 $\tilde{\boldsymbol{h}}_B$ 对应的序列 $\tilde{\boldsymbol{h}}_B^{\Delta}$，就可以任意接近 1 的概率恢复出 $\tilde{\boldsymbol{h}}_A^{\Delta}$，从而得到相同的密钥 K。由于所在子集索引号与子集内的序列索引号是相互独立的，因此 Eve 即使获取了子集索引号，依然不知晓子集内的序列索引号，即无法获取密钥 K 的任何信息。令量化间隔 Δ 趋近于 0，则密钥速率可达到 R_s。

经过以上过程，Alice 与 Bob 即可得到速率为 R_s 的相同密钥 K。中继协作密钥生成方法的整体实现过程如表 1 所示。

4　安全性分析

以可达密钥速率作为保密性能的度量指标，式(10)给出了所提方法的可达密钥速率的表达式。由于 S_R 与 $\tilde{h}_{0,A}$ 和 $\tilde{h}_{0,B}$ 不相关，$\tilde{h}_{0,B}$ 与 $\tilde{h}_{1,A}$ 和 $\tilde{h}_{2,A}$ 不相关，根据互信息的性质可以得到

$$\begin{aligned}R_s&=\frac{1}{T}I\left(\tilde{h}_{0,A},\tilde{h}_{1,A},\tilde{h}_{2,A};\tilde{h}_{0,B},\tilde{h}_{1,B},\tilde{h}_{2,B}\middle|S_R\right)\\&=\frac{1}{T}\Big[I\left(\tilde{h}_{0,A};\tilde{h}_{0,B},\tilde{h}_{1,B},\tilde{h}_{2,B}\middle|S_R\right)\\&\quad+I\left(\tilde{h}_{1,A},\tilde{h}_{2,A};\tilde{h}_{0,B},\tilde{h}_{1,B},\tilde{h}_{2,B}\middle|\tilde{h}_{0,A},S_R\right)\Big]\\&=\frac{1}{T}\Big[I\left(\tilde{h}_{0,A};\tilde{h}_{0,B}\right)+I\left(\tilde{h}_{1,A},\tilde{h}_{2,A};\tilde{h}_{1,B},\tilde{h}_{2,B}\middle|S_R\right)\Big]\end{aligned} \tag{11}$$

表 1 中继协作密钥生成方法实现过程

步骤 1　信道估计：Alice, Bob, Relay 分别发送训练序列，Alice 估计出 $\tilde{h}_{0,A}$ 与 $\tilde{h}_{1,A}$，Bob 估计出了 $\tilde{h}_{0,B}$ 与 $\tilde{h}_{2,B}$，Relay 估计出了 $\tilde{h}_{1,R}$ 与 $\tilde{h}_{2,R}$。

步骤 2　中继协作：Relay 采用网络编码技术，利用 $\tilde{h}_{1,R}$ 与 $\tilde{h}_{2,R}$ 生成辅助信息 $S_R=\tilde{h}_{1,R}^{\Delta}\oplus\tilde{h}_{2,R}^{\Delta}$，将 S_R 发送给 Alice 和 Bob，然后 Alice 利用 $\tilde{h}_{1,A}$ 与 S_R 估计 $\tilde{h}_{2,A}$，Bob 利用 $\tilde{h}_{2,B}$ 与 S_R 估计 $\tilde{h}_{1,B}$。

步骤 3　密钥协商：Alice 根据 $\tilde{\boldsymbol{h}}_A=(\tilde{h}_{0,A},\tilde{h}_{1,A},\tilde{h}_{2,A})$ 生成互不相关的密钥 K 和协商信息 $\boldsymbol{\Phi}$，并将 $\boldsymbol{\Phi}$ 发送给 Bob, Bob 利用 $\boldsymbol{\Phi}$ 和 $\tilde{\boldsymbol{h}}_B=(\tilde{h}_{0,B},\tilde{h}_{1,B},\tilde{h}_{2,B})$ 生成相同的密钥 K。

其中，

$$\begin{aligned} &I\left(\tilde{h}_{1,A},\tilde{h}_{2,A};\tilde{h}_{1,B},\tilde{h}_{2,B}\middle|S_R\right)\\ &\quad=\lim_{\Delta\to0}I\left(\tilde{h}_{1,A}^{\Delta},\tilde{h}_{2,A}^{\Delta};\tilde{h}_{1,B}^{\Delta},\tilde{h}_{2,B}^{\Delta}\middle|\tilde{h}_{1,R}^{\Delta}\oplus\tilde{h}_{2,R}^{\Delta}\right)\\ &\quad=\lim_{\Delta\to0}\Big[I\left(\tilde{h}_{1,A}^{\Delta};\tilde{h}_{1,B}^{\Delta},\tilde{h}_{2,B}^{\Delta}\middle|\tilde{h}_{1,R}^{\Delta}\oplus\tilde{h}_{2,R}^{\Delta}\right)\\ &\qquad+I\left(\tilde{h}_{2,A}^{\Delta};\tilde{h}_{1,B}^{\Delta},\tilde{h}_{2,B}^{\Delta}\middle|\tilde{h}_{1,A}^{\Delta},\tilde{h}_{1,R}^{\Delta}\oplus\tilde{h}_{2,R}^{\Delta}\right)\Big] \end{aligned}\tag{12}$$

由于 $\tilde{h}_{2,A}^{\Delta}=\tilde{h}_{1,A}^{\Delta}\oplus\left(\tilde{h}_{1,R}^{\Delta}\oplus\tilde{h}_{2,R}^{\Delta}\right)$，所以 $I\left(\tilde{h}_{2,A}^{\Delta};\tilde{h}_{1,B}^{\Delta},\tilde{h}_{2,B}^{\Delta}\middle|\tilde{h}_{1,A}^{\Delta},\tilde{h}_{1,R}^{\Delta}\oplus\tilde{h}_{2,R}^{\Delta}\right)=0$。此外，利用条件互信息定义可得

$$\begin{aligned} &I\left(\tilde{h}_{1,A}^{\Delta};\tilde{h}_{1,B}^{\Delta},\tilde{h}_{2,B}^{\Delta}\middle|\tilde{h}_{1,R}^{\Delta}\oplus\tilde{h}_{2,R}^{\Delta}\right)\\ &\quad=H\left(\tilde{h}_{1,A}^{\Delta}\middle|\tilde{h}_{1,R}^{\Delta}\oplus\tilde{h}_{2,R}^{\Delta}\right)\\ &\qquad-H\left(\tilde{h}_{1,A}^{\Delta}\middle|\tilde{h}_{2,B}^{\Delta},\tilde{h}_{1,R}^{\Delta}\oplus\tilde{h}_{2,R}^{\Delta},\tilde{h}_{2,B}^{\Delta}\oplus\tilde{h}_{1,R}^{\Delta}\oplus\tilde{h}_{2,R}^{\Delta}\right)\\ &\quad=H\left(\tilde{h}_{1,A}^{\Delta}\right)-H\left(\tilde{h}_{1,A}^{\Delta}\middle|\tilde{h}_{2,B}^{\Delta}\oplus\tilde{h}_{1,R}^{\Delta}\oplus\tilde{h}_{2,R}^{\Delta}\right)\\ &\quad=I\left(\tilde{h}_{1,A}^{\Delta};\tilde{h}_{2,B}^{\Delta}\oplus\tilde{h}_{1,R}^{\Delta}\oplus\tilde{h}_{2,R}^{\Delta}\right)=I\left(\tilde{h}_{1,A}^{\Delta};\tilde{h}_{1,B}^{\Delta}\right) \end{aligned}\tag{13}$$

此时式(12)可转化为

$$\begin{aligned} I\left(\tilde{h}_{1,A},\tilde{h}_{2,A};\tilde{h}_{1,B},\tilde{h}_{2,B}\middle|S_R\right)&=\lim_{\Delta\to0}I\left(\tilde{h}_{1,A}^{\Delta};\tilde{h}_{1,B}^{\Delta}\right)\\ &=I\left(\tilde{h}_{1,A};\tilde{h}_{1,B}\right) \end{aligned}\tag{14}$$

将式(14)代入式(11)，可得可达密钥速率为

$$R_s=\frac{1}{T}\left[I\left(\tilde{h}_{0,A};\tilde{h}_{0,B}\right)+I\left(\tilde{h}_{1,A};\tilde{h}_{1,B}\right)\right]\tag{15}$$

文献[14]已经研究了存在一个友好辅助节点时的最优可达密钥速率，对应于本文提出的 4 点模型的最优可达密钥速率可表示为

$$\begin{aligned} R_{op}=\frac{1}{T}\Big\{&I\left(\tilde{h}_{0,A},\tilde{h}_{1,A};\tilde{h}_{0,B},\tilde{h}_{2,B}\middle|\tilde{h}_{1,R},\tilde{h}_{2,R}\right)\\ &+\min\Big[I\left(\tilde{h}_{0,A},\tilde{h}_{1,A};\tilde{h}_{1,R},\tilde{h}_{2,R}\right),\\ &I\left(\tilde{h}_{0,B},\tilde{h}_{2,B};\tilde{h}_{1,R},\tilde{h}_{2,R}\right)\Big]\Big\} \end{aligned}\tag{16}$$

由于 h_0，h_1，h_2 之间都不相关，因此 $I\left(\tilde{h}_{0,A},\tilde{h}_{1,A};\tilde{h}_{0,B},\tilde{h}_{2,B}\middle|\tilde{h}_{1,R},\tilde{h}_{2,R}\right)=I\left(\tilde{h}_{0,A};\tilde{h}_{0,B}\right)$，同样可以得到 $I\left(\tilde{h}_{0,A},\tilde{h}_{1,A};\tilde{h}_{1,R},\tilde{h}_{2,R}\right)=I\left(\tilde{h}_{1,A};\tilde{h}_{1,R}\right)$，$I\left(\tilde{h}_{0,B},\tilde{h}_{2,B};\tilde{h}_{1,R},\tilde{h}_{2,R}\right)=I\left(\tilde{h}_{2,B};\tilde{h}_{2,R}\right)$。并且在本文的模型中 h_1 与 h_2 的方差均为 σ_1^2，$I\left(\tilde{h}_{1,A};\tilde{h}_{1,R}\right)=I\left(\tilde{h}_{2,B};\tilde{h}_{2,R}\right)$。这样，式(16)可简化为

$$R_{op}=\frac{1}{T}\left\{I\left(\tilde{h}_{0,A};\tilde{h}_{0,B}\right)+I\left(\tilde{h}_{1,A};\tilde{h}_{1,R}\right)\right\}\tag{17}$$

考虑高信噪比的通信场景，即 σ_1^2 远大于 σ_n^2，当 $\sigma_n^2\to0$ 时，$\tilde{h}_{2,B}^{\Delta}\oplus\tilde{h}_{1,R}^{\Delta}\oplus\tilde{h}_{2,R}^{\Delta}=\tilde{h}_{1,R}^{\Delta}$，因此式(13)可转化为

$$I\left(\tilde{h}_{1,A}^{\Delta};\tilde{h}_{1,B}^{\Delta},\tilde{h}_{2,B}^{\Delta}\middle|\tilde{h}_{1,R}^{\Delta}\oplus\tilde{h}_{2,R}^{\Delta}\right)=I\left(\tilde{h}_{1,A}^{\Delta};\tilde{h}_{1,R}^{\Delta}\right)\tag{18}$$

这样式(14)可转化为

$$\begin{aligned} &I\left(\tilde{h}_{1,A},\tilde{h}_{2,A};\tilde{h}_{1,B},\tilde{h}_{2,B}\middle|S_R\right)\\ &\quad=\lim_{\Delta\to0}I\left(\tilde{h}_{1,A}^{\Delta};\tilde{h}_{1,R}^{\Delta}\right)=I\left(\tilde{h}_{1,A};\tilde{h}_{1,R}\right) \end{aligned}\tag{19}$$

此时 $R_s=R_{op}$，因此 $\sigma_n^2\to0$ 时，所提方法的可达密钥速率是趋于最优的。

由于 $\tilde{h}_{0,A}$ 与 $\tilde{h}_{0,B}$ 均为 0 均值方差为 $\sigma_0^2+\sigma_n^2/(PT/5)$ 的高斯随机变量，根据互信息的性质及高斯随机变量熵的计算公式可得

$$\begin{aligned} I\left(\tilde{h}_{0,A};\tilde{h}_{0,B}\right)&=H\left(\tilde{h}_{0,A}\right)+H\left(\tilde{h}_{0,B}\right)-H\left(\tilde{h}_{0,A},\tilde{h}_{0,B}\right)\\ &=\frac{1}{2}\lg\frac{\left(\sigma_0^2+\frac{5\sigma_n^2}{PT}\right)\left(\sigma_0^2+\frac{5\sigma_n^2}{PT}\right)}{\left(\sigma_0^2+\frac{5\sigma_n^2}{PT}\right)\left(\sigma_0^2+\frac{5\sigma_n^2}{PT}\right)-\sigma_0^2\sigma_0^2}\\ &=\frac{1}{2}\lg\left[1+\frac{\sigma_0^4P^2T^2}{5\sigma_n^2\left(2\sigma_0^2PT+5\sigma_n^2\right)}\right] \end{aligned}\tag{20}$$

同样地，$\tilde{h}_{1,A}$ 与 $\tilde{h}_{1,R}$ 均为 0 均值方差为 $\sigma_1^2+\sigma_n^2/(PT/5)$ 的高斯随机变量，可得

$$\begin{aligned} I\left(\tilde{h}_{1,A};\tilde{h}_{1,R}\right)&=H\left(\tilde{h}_{1,A}\right)+H\left(\tilde{h}_{1,R}\right)-H\left(\tilde{h}_{1,A},\tilde{h}_{1,R}\right)\\ &=\frac{1}{2}\lg\frac{\left(\sigma_1^2+\frac{5\sigma_n^2}{PT}\right)\left(\sigma_1^2+\frac{5\sigma_n^2}{PT}\right)}{\left(\sigma_1^2+\frac{5\sigma_n^2}{PT}\right)\left(\sigma_1^2+\frac{5\sigma_n^2}{PT}\right)-\sigma_1^2\sigma_1^2}\\ &=\frac{1}{2}\lg\left[1+\frac{\sigma_1^4P^2T^2}{5\sigma_n^2\left(2\sigma_1^2PT+5\sigma_n^2\right)}\right] \end{aligned}\tag{21}$$

可求出最优的可达密钥速率为

$$\begin{aligned} R_{op}&=\frac{1}{T}\left[I\left(\tilde{h}_{0,A};\tilde{h}_{0,B}\right)+I\left(\tilde{h}_{1,A};\tilde{h}_{1,R}\right)\right]\\ &=\frac{1}{2T}\left\{\lg\left[1+\frac{\sigma_0^4P^2T^2}{5\sigma_n^2\left(2\sigma_0^2PT+5\sigma_n^2\right)}\right]\right.\\ &\quad\left.+\lg\left[1+\frac{\sigma_1^4P^2T^2}{5\sigma_n^2\left(2\sigma_1^2PT+5\sigma_n^2\right)}\right]\right\} \end{aligned}\tag{22}$$

5 仿真分析

为了验证所提方法的性能，并分析影响可达密钥速率的因素，基于 Matlab 进行了一些仿真实验。假设收发双方均采用数字信号处理，每个实数均采用 16 bit 表示，则各节点估计出来的信道增益均采用 16 bit 数字信号表示，相当于进行了 16 bit 量化，不需要单独的量化过程。采用蒙特卡洛方法进行 $N=100000$ 次实验，每次随机产生一组信道增益值和噪声值，采用 Matlab 中的 ITE(Information

Theoretical Estimators)工具包，估计式(15)中相应信道增益变量之间的互信息。

首先针对一个中继节点协作时所提密钥生成方法的性能进行仿真，参考文献[16]的参数设置，假设相干长度$T=20$，直达信道和中继信道的增益的方差$\sigma_0^2=\sigma_1^2=1$。仿真了该方法的可达密钥速率随信噪比(Signal-to-Noise Ratio, SNR)的变化曲线，并与最优可达密钥速率、放大转发(AF)[15]、以及无中继节点协作[17]时的可达密钥速率的变化曲线对比，如图3所示。可以看出，上述4种方法的可达密钥速率均是随着信噪比的提高而线性增长，本文方法的可达密钥速率变化曲线的斜率与AF、最优可达密钥速率变化曲线相同，并且明显大于无中继节点协作时的可达密钥速率变化曲线。因此本文方法增加的可达密钥速率随着信噪比的提高而不断增大，当SNR = 30 dB时，该方法提高的可达密钥速率可达到每利用一次信道多产生约0.2 bit密钥，比AF方法多产生约0.07 bit密钥。与最优可达密钥速率相比，本文方法由于噪声而产生的性能损失是相对固定的，约为每利用一次信道0.03 bit，不随信噪比变化而变化。因此，随着信噪比的提升，本文方法的性能损失在可达密钥速率R_s中所占比例越来越小，当噪声趋于0时，R_s趋近于最优密钥速率R_{op}。

物联网应用场景中节点众多，有大量中继节点资源可以协作产生密钥，因此我们仿真了参与协作的中继节点数量对可达密钥速率的影响，分别选取3 个中继节点、2 个中继节点、1 个中继节点，并与无中继节点协作时对比。假设相干长度$T=20$，直达信道和中继信道的增益的方差$\sigma_0^2=\sigma_1^2=1$，中继节点之间的距离均满足几个波长以上的要求，使得所有中继信道与直达信道不相关，且不同中继信道之间也是不相关的，可达密钥速率随信噪比的变化曲线如图 4 所示。可以看出，与单个中继节点协作时相同，在多中继节点协作的情况下，可达密钥速率依然随着信噪比的升高而线性增大。中继节点数量的增加能显著提高可达密钥速率，当SNR = 30 dB时，单个中继节点提高的可达密钥速率可达到每利用一次信道多产生约 0.2 bit 密钥，2 个中继节点可多产生约 0.4 bit 密钥，3 个中继节点可多产生约 0.6 bit 密钥，这是因为参与协作的中继节点数量的增加，相当于增加了 Alice 与 Bob 之间的中继信道数量，由于不同中继信道之间是不相关的，中继信道数量的增加能够显著提高密钥源的熵，从而有效提升可达密钥速率。因此，为了提高可达密钥速率，满足高数据速率的加密通信需求，选取多个中继节点协作产生密钥将是有效的解决途径。但是参与协作的中继节点数量的增加会增大密钥生成的总时间，而单次密钥生成过程须在相干时间 T 内完成，因此在 T 固定的情况下，参与协作的中继节点数量存在最大值$N_{R,\max}$，当可利用的中继节点数量大于$N_{R,\max}$时，只能选取$N_{R,\max}$个中继节点参与协作，此时可达密钥速率将不再随中继节点数目的增加而增大。

通过中继节点协作提高密钥速率本质上是通过增加中继信道数量从而提高密钥源的熵，因此在单一中继协作的情况下提高中继信道的熵也是进一步增大密钥速率的一个可行思路。我们针对单个中继节点协作的场景，仿真了中继信道方差对可达密钥速率的影响，假设相干长度$T=20$，分别选取$\sigma_1=3\sigma_0$，$\sigma_1=2\sigma_0$，$\sigma_1=\sigma_0$ 3种情况，并与无中继节点协作时对比，可达密钥速率随信噪比的变化曲线如图5所示。可以看出，中继信道的方差越大，可达密钥速率就越大，当SNR = 30 dB时，中继信道方差$\sigma_1=\sigma_0$时提高的可达密钥速率可达到每利用一次信道多产生约0.20 bit密钥，$\sigma_1=2\sigma_0$时可多产生约0.25 bit密钥，$\sigma_1=3\sigma_0$时可多产生约0.28 bit密钥，这是因为信道增益建模为高斯随机变量，中继信道的方差越大，带来的密钥源熵的增量就越大，可达密钥速率的提升幅度就越大，这为多中继节点场景下的协作中继节点的选择提供了指导。

6　结束语

本文针对物联网准静态信道下密钥生成速率

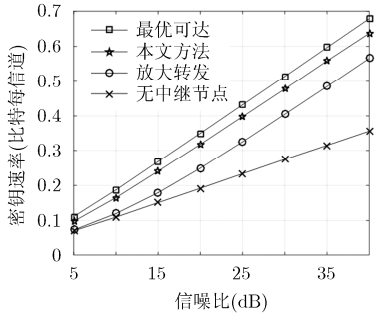

图 3 可达密钥速率随信噪比的变化曲线

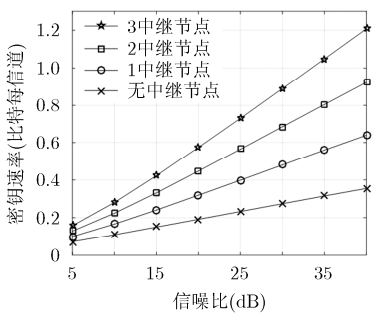

图 4 协作的中继节点数量对密钥速率的影响

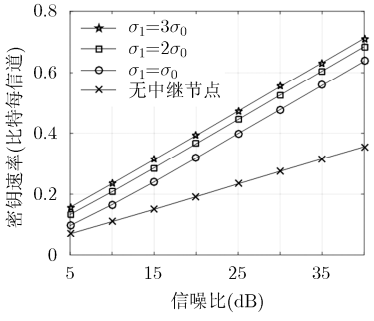

图 5 中继信道方差对密钥速率的影响

低的问题，结合物联网的实际应用特点，考虑中继节点的协作代价，提出了基于中继节点协作的密钥生成方法。该方法通过中继节点协作，提高了 Alice 与 Bob 之间相关信息的随机性，增加了密钥源的熵，从而提高了可达密钥速率。相对于放大转发方法，该方法中的中继节点采用网络编码，不会泄露中继信道信息，提高了合法通信双方密钥源的相关性；相对于现有中继协作方法，该方法不需要中继节点参与密钥协商阶段，降低了中继节点协作的代价。安全性分析表明该方法能显著提高可达密钥速率，并且随着信噪比的提高，可达密钥速率呈线性增长，趋于最优值。蒙特卡洛仿真验证了理论分析的结果，并得出了增加中继节点数量，选取信道变化幅度大的中继节点都可以进一步提高可达密钥速率，这为下一步研究多中继节点协作的密钥生成、以及多中继节点场景下的中继节点选择指明了方向。

参 考 文 献

[1] LINDQVIST U and NEUMANN P G. The future of the Internet of Things[J]. *Communications of the ACM*, 2017, 60(2): 26–30. doi: 10.1145/3029589.

[2] SAHA H N, MANDAL A, and SINHA A. Recent trends in the Internet of Things[C]. IEEE Computing and Communication Workshop and Conference, Las Vegas, USA, 2017: 1–4.

[3] MAVROMOUSTAKIS C X, MASTORAKIS G, and BATALLA J M. Internet of Things (IoT) in 5G Mobile Technologies[M]. Berlin: Springer International Publishing, 2016: 127–227.

[4] SAMAILA M G, NETO M, FERNANDES D A B, *et al*. Security Challenges of the Internet of Things[M]. Berlin: Springer International Publishing, 2017: 53–82.

[5] LIU Y L, CHEN H H, and WANG L M. Physical layer security for next generation wireless networks: Theories, technologies, and challenges[J]. *IEEE Communications Surveys & Tutorials*, 2017, 19(1): 347–376. doi: 10.1109/COMST.2016.2598968.

[6] ZHANG J Q, TRUNG Q D, ALAN M, *et al*. Key generation from wireless channels: A review[J]. *IEEE Access*, 2016(4): 614–626. doi: 10.1109/ACCESS.2016.2521718.

[7] CASTEL T, TORRE P V, and ROGIER H. RSS-based secret key generation for indoor and outdoor WBANs using on-body sensor nodes[C]. International Conference on Military Communications and Information Systems, Brussels, Belgium, 2016: 1–5.

[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*, 2016, 16(7): 2065–2078. doi: 10.1109/TMC.2016.2557784.

[9] MADISEH M G, NEVILLE S W, and MCGUIRE M L. Applying beamforming to address temporal correlation in wireless channel characterization based secret key generation [J]. *IEEE Transactions on Information Forensics Security*, 2012, 7(4): 1278–1287. doi: 10.1109/TIFS.2012.2195176.

[10] HUANG P and WANG X. Fast secret key generation in static wireless networks: A virtual channel approach[C]. IEEE International Conference on Computer Communications, Turin, Italy, 2013: 2292–2300.

[11] CHEN D, QIN Z, MAO X, *et al*. SmokeGrenade: An efficient key generation protocol with artificial interference[J]. *IEEE Transactions on Information Forensics and Security*, 2013, 8(11): 1731–1745. doi: 10.1109/TIFS.2013.2278834.

[12] GOLLAKOTA S and KATABI D. Physical layer wireless security made fast and channel independent[C]. IEEE International Conference on Computer Communications, Shanghai, China, 2011: 1125–1133.

[13] MUKHERJEE A. Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints[J]. *Proceedings of the IEEE*, 2015, 103(10): 1748–1761. doi: 10.1109/JPROC.2015.2466548.

[14] CSISZAR I and NARAYAN P. Common randomness and secret key generation with a helper[J]. *IEEE Transactions on Information Theory*, 2000, 46(2): 344–366. doi: 10.1109/18.825796.

[15] TAKAYUKI S, HISATO I, and HIDEICHI S. Physical-layer secret key agreement in two-way wireless relaying systems[J]. *IEEE Transactions on Information Forensics and Security*, 2011, 6(3): 650–660. doi: 10.1109/TIFS.2011.2147314.

[16] LAI L, LIANG Y, and DU W. Cooperative key generation in wireless networks[J]. *IEEE Journal on Selected Areas in Communications*, 2012, 30(8): 1578–1588. doi: 10.1109/JSAC.2012.120924.

[17] 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. doi: 10.1109/TIFS.2010.2043187.

肖帅芳： 男，1989 年生，博士生，研究方向为无线物理层安全.

郭云飞： 男，1963 年生，教授，博士生导师，研究方向为网络与信息安全.

白慧卿： 女，1988 年生，博士生，研究方向为无线物理层安全.

金 梁： 男，1969 年生，教授，博士生导师，研究方向为移动通信、无线物理层安全.

黄开枝： 女，1973 年生，教授，博士生导师，研究方向为宽带移动通信与异构无线网络安全、无线物理层安全.