面向物联网多跳中继系统的协作密钥生成方法

肖帅芳，郭云飞，黄开枝，金梁
（国家数字交换系统工程技术研究中心，河南 郑州 450002）

摘 要：针对物联网多跳中继系统中密钥生成方法速率低的问题，提出一种基于网络编码的协作密钥生成方法。在各节点完成信道估计后，中继节点采用安全网络编码技术辅助通信双方获取相同信道的估计值，同时辅助信息不泄露该信道的任何信息，最后通信双方直接在公共信道上协商得到相同的密钥。理论分析和仿真结果表明，该方法可以有效地提高可达密钥速率，同时增加传输路径，选取跳数少、信道变化大的传输路径，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；多跳中继系统；网络编码
中图分类号：TN918.82
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018036

Cooperative secret key generation for multi-hop relaying systems in Internet of things

XIAO Shuaifang, GUO Yunfei, HUANG Kaizhi, JIN Liang
National Digital Switching System Engineering and Technological R&D Center, Zhengzhou 450002, China

Abstract: The achievable key rate of secret key generation method in multi-hop relaying systems was relative low in Internet of things. A cooperative secret key generation algorithm based on network coding was proposed to improve the achievable key rate. Firstly, all the nodes send training sequences in turn to estimate the channels. After that the relays employ secure network coding technique to assist the two legitimate users to obtain the correlative observations of the same wireless channel, with nothing leakage about the channel information to the eavesdropper. Finally, the two legitimate users agreed on a common secret key directly over the public channel. Theoretical and simulation results validate the performance of the proposed secret key generation algorithm, and obtain that increasing the wireless transmission paths, selecting the transmission path with less hops and larger variance channels can further improve the achievable secret key rate.

Key words: physical layer security, secret key generation, Internet of things, multi-hop relaying systems, network coding

1 引言

物联网作为连接物理世界与人类社会的桥梁，已经深入人们生活的方方面面[1]。与此同时，物联网的安全问题也越来越引起学术界的关注，成为限制其发展的重要制约因素[2]。物联网的一个重要的安全威胁是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[3]。

近年来，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新的思路，引起学者们的广泛关注[4~7]。Maurer[8]最早针对无线物理层密钥生成技

收稿日期：2017-09-27；**修回日期**：2017-12-10
基金项目：国家自然科学基金资助项目（No.61379006, No.61501516, No.61521003）；国家高技术研究发展计划（“863”计划）基金资助项目（No.2015AA01A708）
Foundation Items: The National Natural Science Foundation of China (No.61379006, No.61501516, No.61521003), The National High Technology Research and Development Program of China (863 Program) (No.2015AA01A708)

术开展了研究，提出利用共享随机信息进行密钥生成的方法，并给出可达密钥速率的上下界。在此基础上，Ahlswede 等[9]提出源模型和信道模型，定义密钥容量，并给出 2 种模型下密钥容量的上界。以上研究奠定了无线物理层密钥生成技术的理论基础。由于无线信道具有随机性和互易性，合法通信双方将互易的无线信道作为共享的随机源，分别对无线信道进行估计，可以得到相关的观测值，从而生成共同的密钥。同时窃听者距离合法用户的距离超过半个波长（分米级）即可认为窃听信道与合法信道独立，这在实际的通信场景中很容易满足，从而保证了窃听者无法获知密钥的任何信息，因此，许多学者针对基于无线信道的密钥生成方法开展研究[10~13]。利用无线物理层密钥生成技术，合法通信双方可以从共享的无线信道中直接提取密钥，不需要进行密钥分发，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[14]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[15]针对车联网场景，提出一种基于接收信号强度的实用物理层密钥生成方案。文献[16]针对物联网的特点，提出一种基于离散余弦变换的物理层密钥生成方法，并验证了所提方法可以提高密钥生成的速率和能量效率。

物联网中存在许多能量受限的弱节点（如传感器节点），较低的发送功率导致其传输距离受限，因此，需要通过中继节点多跳传输才能满足合法通信双方的通信需求，而多跳中继系统是物联网中的一种典型应用场景。然而现有物理层密钥生成技术的研究主要集中在合法通信双方存在直达链路（单跳可达）的情况，针对多跳中继系统的研究仅限于经过一次中继转发（2 跳可达）的情况。Csiszar 等[17]首先针对中继节点辅助合法通信双方生成密钥的方法进行研究，推导出可达密钥速率，并给出密钥容量的上界。文献[18]研究双向中继系统的密钥生成，提出 4 种基于放大转发（AF, amplify-and-forward）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，从而降低可达密钥速率。文献[19]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成对密钥协商，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。文献[20]研究了存在主动攻击者的双向中继网络的密钥生成，提出一种可以有效地提高密钥速率的密钥生成方法。文献[21]提出利用多个非信任中继提高密钥速率的密钥生成方法。

针对物联网多跳中继系统中的密钥生成方法尚没有文献研究，而直接采用基于 AF 的密钥生成方法的可达密钥速率较低。为解决该问题，本文提出了一种基于网络编码的协作密钥生成方法。首先，合法通信双方和中继节点发送训练序列进行信道估计，由于合法通信双方之间不存在直达链路，二者无法获取相关的信道估计信息。然后，中继节点采用安全网络编码技术参与协作，辅助合法通信双方获取相同信道的估计值，同时辅助信息不泄露该信道的任何信息。最后，合法通信双方在公共信道上进行密钥协商，以二者通过中继辅获取的相关观测值为密钥源，生成相同的密钥。此外，通过推导所提方法的可达安全速率，从理论上证明了该方法不泄露密钥源的任何信息。蒙特卡洛仿真表明，所提方法相比于 AF 方法可以显著提高可达密钥速率，且增加传输路径数量和选取跳数少、信道变化幅度大的传输路径，可以进一步提高可达密钥速率，从而为多条传输路径的场景下，进一步提高可达密钥速率指明了方向。

2　系统模型

针对物联网多跳中继系统中的密钥生成进行建模，如图 1 所示。Alice (A)与 Bob (B)为合法通信双方，均为单天线。Alice 与 Bob 之间是 N($N \geqslant 2$)跳可达的，即二者之间不存在直达链路，需要经过 $N-1$ 个中继节点 $\mathrm{Relay}_1(\mathrm{R}_1)$、…、$\mathrm{Relay}_{N-1}(\mathrm{R}_{N-1})$ 依次转发，才能实现通信。假设中继节点均是友好可信的，也配备单天线。在这些合法节点的通信范围内，存在一个潜在窃听者 Eve（E）试图窃取保密信息。为了实现保密通信，Alice 与 Bob 首先在中继节点的帮助下生成共享的密钥，然后利用生成的密钥对保密信息加密处理后，发送给对方。与文献[17]一致，假设 Alice 与 Bob 之间存在无噪的公共信道，满足 Alice 与 Bob 密钥协商的需求。虽然 Alice 与 Bob 之间没有直达链路，但它们可以通过多跳传输路径进行通信，并采用纠错信道编码保证协商信息的无误差传输，相当于在 Alice 与 Bob 之间搭建了一条无噪的公共协商信道，该无噪公共协商信道是公开的，Eve 也可以收到在公共信道上传输的任何信息。

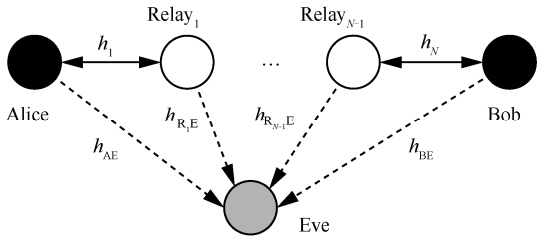


图 1 物联网多跳中继系统中的密钥生成建模

节点之间的信道建模为准静态块衰落信道，即在一个相干时间 T 内信道是不变的，在不同的相干时间之间为独立的衰落信道。不同节点之间的信道是相互独立的，且满足互易性，令 h_{ij} 为节点 i 到节点 j 的信道增益，则 $h_{\mathrm{AR}_1}=h_{\mathrm{R}_1\mathrm{A}}=h_1$，$h_{\mathrm{R}_{N-1}\mathrm{B}}=h_{\mathrm{BR}_{N-1}}=h_{N-1}$，$h_{\mathrm{R}_{l-1}\mathrm{R}_l}=h_{\mathrm{R}_l\mathrm{R}_{l-1}}=h_l$，$l=2,\cdots,N-1$。假定 Alice、Bob、$\mathrm{R}_1,\cdots,\mathrm{R}_N$ 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，考虑对称信道，将信道增益 $h_1,\cdots,h_N$ 均建模为均值为 0、方差为 σ_h^2 的高斯随机变量，且它们是相互独立的。其他衰落信道模型的分析方法类似，很容易进行推广。

由于 Eve 的位置未知，Eve 可能会窃听到任意一个合法节点发送的信号，考虑最不利的情况，即 Eve 可以观测到 Alice, Bob, $\mathrm{R}_1,\cdots,\mathrm{R}_N$ 发送的全部信号。h_{AE}，h_{BE}，$h_{\mathrm{R}_1\mathrm{E}},\cdots,h_{\mathrm{R}_{N-1}\mathrm{E}}$ 分别表示 Alice、Bob、$\mathrm{R}_1,\cdots,\mathrm{R}_N$ 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，不参与通信过程和密钥生成过程。为了不被发现，Eve 与 Alice、Bob、$\mathrm{R}_1,\cdots,\mathrm{R}_N$ 之间保持半个波长（分米级）以上的距离，这保证 $h_{\mathrm{AE}},h_{\mathrm{BE}},h_{\mathrm{R}_1\mathrm{E}},\cdots,h_{\mathrm{R}_{N-1}\mathrm{E}}$ 与 $h_1,\cdots,h_N$ 均是不相关的，使 Eve 无法估计出 $h_1,\cdots,h_N$ 的任何信息。此外，密钥生成过程是公开的，即 Eve 知晓密钥生成的整个处理流程，但它无法获知任何与密钥相关的信息。

基于上述模型，提出基于安全网络编码的协作密钥生成方法。中继节点采用网络编码协作，辅助 Alice 与 Bob 获取相关的信道观测值，从而生成相同的密钥。

3 基于网络编码的协作密钥生成方法

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 可分别估计出自身相邻的信道信息；然后，为了使 Alice 与 Bob 获取相关的共同信息，中继节点采用安全网络编码技术参与协作，使 Alice 与 Bob 获得相同信道的估计值；最后，Alice 与 Bob 直接在公共信道上进行密钥协商生成相同的密钥。基于网络编码的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，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 分成 3 个时隙 T_1、T_2、T_3，时隙分配如图 2 所示。

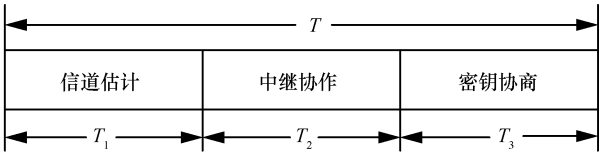


图 2 一个相干时间 T 内的时隙分配

3.1 信道估计阶段

在 T_1 时隙，Alice、Bob、$\mathrm{R}_1,\cdots,\mathrm{R}_N$ 轮流发送已知的训练序列 $\boldsymbol{x}$，各节点根据接收到的信号，采用迫零算法对相邻的信道进行估计，令 $\tilde{h}_{m,\mathrm{L}}$ 表示节点 L 对信道 h_m 的估计值，$\boldsymbol{n}_{m,\mathrm{L}}$ 表示节点 L 在估计 h_m 时接收的噪声，$\mathrm{L}=\mathrm{A},\mathrm{B},\mathrm{R}_1,\cdots,\mathrm{R}_{N-1}$，$m=1,\cdots,N$。这样，Alice 可以估计出信道 h_1，得到

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

其中，$(\cdot)^{\mathrm{T}}$ 表示向量或矩阵的转置，$\|\cdot\|$ 表示向量的模。容易得到 $\tilde{h}_{1,\mathrm{A}}$ 是均值为 0、方差为 $\frac{\sigma_h^2+\sigma_n^2}{\|\boldsymbol{x}\|^2}$ 的高斯随机变量，假设每个节点用于信道估计的时间均为 T_{ce}，发送功率均为 P_{ce}，可得 $\|\boldsymbol{x}\|^2=P_{\mathrm{ce}}T_{\mathrm{ce}}$，因此，$\tilde{h}_{1,\mathrm{A}}\sim\mathcal{N}\left(0,\sigma_h^2+\frac{\sigma_n^2}{P_{\mathrm{ce}}T_{\mathrm{ce}}}\right)$。同样地，Bob 可以估计出信道 h_N，得到

$$\tilde{h}_{N,\mathrm{B}}=h_N+\frac{\boldsymbol{x}^{\mathrm{T}}}{\|\boldsymbol{x}\|^2}\boldsymbol{n}_{N,\mathrm{B}} \tag{2}$$

其中，$\tilde{h}_{N,\mathrm{B}}\sim\mathcal{N}\left(0,\sigma_h^2+\frac{\sigma_n^2}{P_{\mathrm{ce}}T_{\mathrm{ce}}}\right)$。中继节点 $\mathrm{R}_i(i=1,\cdots,N-1)$ 可以估计出信道 h_i 和 h_{i+1}，得到

$$\tilde{h}_{i,\mathrm{R}_i}=h_i+\frac{\boldsymbol{x}^{\mathrm{T}}}{\|\boldsymbol{x}\|^2}\boldsymbol{n}_{i,\mathrm{R}_i} \tag{3}$$

$$\tilde{h}_{i+1,\mathrm{R}_i}=h_{i+1}+\frac{\boldsymbol{x}^{\mathrm{T}}}{\|\boldsymbol{x}\|^2}\boldsymbol{n}_{i+1,\mathrm{R}_i} \tag{4}$$

其中，$\tilde{h}_{i,\mathrm{R}_i},\tilde{h}_{i+1,\mathrm{R}_i}\sim\mathcal{N}\left(0,\sigma_h^2+\frac{\sigma_n^2}{P_{\mathrm{ce}}T_{\mathrm{ce}}}\right)$。同时，Eve 可以估计出信道 h_{AE}、h_{BE} 和 $h_{\mathrm{R}_i\mathrm{E}}(i=1,2,\cdots,N-1)$，得到 $\tilde{\boldsymbol{h}}_{\mathrm{E}}=\left(\tilde{h}_{\mathrm{AE}},\tilde{h}_{\mathrm{BE}},\tilde{h}_{\mathrm{R}_1\mathrm{E}},\tilde{h}_{\mathrm{R}_2\mathrm{E}},\cdots,\tilde{h}_{\mathrm{R}_{N-1}\mathrm{E}}\right)$。

经过以上信道估计过程，Alice 得到 $\tilde{h}_{1,\mathrm{A}}$，Bob 得到 $\tilde{h}_{N,\mathrm{B}}$，二者并无相关的共同信息，需要在接下来的中继协作阶段，通过中继节点协作，使 Alice 与 Bob 获得相关的共同信息。

3.2　中继协作阶段

在 T_2 时隙，中继节点 $\mathrm{R}_1,\cdots,\mathrm{R}_N$ 分别发送辅助信息 $s_{\mathrm{R}_1},\cdots,s_{\mathrm{R}_{N-1}}$，协助 Alice 与 Bob 获取相同信道的观测值。为了保证私密性，中继节点采用安全网络编码技术，使 Eve 无法获取该信道的任何信息。

当 N 为奇数时，即 $N=2k+1$（$k=1,2,3,\cdots$），处于链路中间位置的 2 个中继节点 R_k 和 R_{k+1}，R_k 经 k 跳可达 Alice，R_{k+1} 经 k 跳可达 Bob，二者均在信道估计阶段获得 h_{k+1} 的估计值，分别为 $\tilde{h}_{k+1,\mathrm{R}_k}$、$\tilde{h}_{k+1,\mathrm{R}_{k+1}}$。$\mathrm{R}_k$ 和 R_{k+1} 分别采用安全网络编码技术，生成辅助信息 $s_{\mathrm{R}_k}=\tilde{h}^{\Delta}_{k,\mathrm{R}_k}\oplus\tilde{h}^{\Delta}_{k+1,\mathrm{R}_k}$ 与 $s_{\mathrm{R}_{k+1}}=\tilde{h}^{\Delta}_{k+2,\mathrm{R}_{k+1}}\oplus\tilde{h}^{\Delta}_{k+1,\mathrm{R}_{k+1}}$，其中，$\tilde{h}^{\Delta}_{m,\mathrm{L}}$ 为 $\tilde{h}_{m,\mathrm{L}}$ 的量化，Δ 为量化间隔。然后分别对 s_{R_k} 与 $s_{\mathrm{R}_{k+1}}$ 进行纠错编码，并经过调制后发送给 R_{k-1} 与 R_{k+2}。由于进行了纠错编码，且 R_{k-1} 与 R_{k+2} 已经分别估计出信道 h_k 与 h_{k+2}，可以精确恢复出 s_{R_k} 与 $s_{\mathrm{R}_{k+1}}$。R_{k-1} 利用自身估计出的 h_k 和 s_{R_k} 可以得到 h_{k+1} 的估计值为

$$\tilde{h}^{\Delta}_{k+1,\mathrm{R}_{k-1}}=\tilde{h}^{\Delta}_{k,\mathrm{R}_{k-1}}\oplus\left(\tilde{h}^{\Delta}_{k,\mathrm{R}_k}\oplus\tilde{h}^{\Delta}_{k+1,\mathrm{R}_k}\right)\tag{5}$$

同样地，R_{k+2} 利用自身估计出的 h_{k+2} 和 $s_{\mathrm{R}_{k+1}}$ 可以得到 h_{k+1} 的估计值为

$$\tilde{h}^{\Delta}_{k+1,\mathrm{R}_{k+2}}=\tilde{h}^{\Delta}_{k+2,\mathrm{R}_{k+2}}\oplus\left(\tilde{h}^{\Delta}_{k+2,\mathrm{R}_{k+1}}\oplus\tilde{h}^{\Delta}_{k+1,\mathrm{R}_{k+1}}\right)\tag{6}$$

这样，R_{k-1} 与 R_{k+2} 均可获得信道 h_{k+1} 的估计值，且二者分别经 $k-1$ 跳可达 Alice 与 Bob。由此，经过 $k-1$ 次相同的协作保密传递，Alice 与 Bob 均可得到 h_{k+1} 的估计值，分别为

$$\tilde{h}^{\Delta}_{k+1,\mathrm{A}}=\tilde{h}^{\Delta}_{1,\mathrm{A}}\oplus\tilde{h}^{\Delta}_{1,\mathrm{R}_1}\oplus\tilde{h}^{\Delta}_{2,\mathrm{R}_1}\oplus\tilde{h}^{\Delta}_{2,\mathrm{R}_2}\oplus\cdots\oplus\tilde{h}^{\Delta}_{k+1,\mathrm{R}_k}\tag{7}$$

$$\tilde{h}^{\Delta}_{k+1,\mathrm{B}}=\tilde{h}^{\Delta}_{N,\mathrm{B}}\oplus\tilde{h}^{\Delta}_{N,\mathrm{R}_{2k}}\oplus\tilde{h}^{\Delta}_{N-1,\mathrm{R}_{2k}}\oplus\tilde{h}^{\Delta}_{N-1,\mathrm{R}_{2k-1}}\oplus\cdots\oplus\tilde{h}^{\Delta}_{k+1,\mathrm{R}_{k+1}}\tag{8}$$

此时，Alice 与 Bob 得到了相关信息 $\left(\tilde{h}^{\Delta}_{k+1,\mathrm{A}},\tilde{h}^{\Delta}_{k+1,\mathrm{B}}\right)$。

当 N 为偶数时，即 $N=2k$（$k=1,2,3,\cdots$），处于链路中间位置的中继节点 R_k 将 $\tilde{h}_{k,\mathrm{R}_k}$ 与 $\tilde{h}_{k+1,\mathrm{R}_k}$ 分别量化后求模 2 加，生成辅助信息 $s_{\mathrm{R}_k}=\tilde{h}^{\Delta}_{k,\mathrm{R}_k}\oplus\tilde{h}^{\Delta}_{k+1,\mathrm{R}_k}$。然后对 s_{R_k} 进行纠错编码，并经过调制后发送给 R_{k-1}，由于进行纠错编码，且 R_{k-1} 已经估计出信道 h_k，可以精确恢复出 s_{R_k}。R_{k-1} 利用自身估计出的 h_k 和 s_{R_k} 可以得到 h_{k+1} 的估计值为

$$\tilde{h}^{\Delta}_{k+1,\mathrm{R}_{k-1}}=\tilde{h}^{\Delta}_{k,\mathrm{R}_{k-1}}\oplus\left(\tilde{h}^{\Delta}_{k,\mathrm{R}_k}\oplus\tilde{h}^{\Delta}_{k+1,\mathrm{R}_k}\right)\tag{9}$$

此外，在信道估计阶段 R_{k+1} 已经得到 h_{k+1} 的估计值 $\tilde{h}_{k+1,\mathrm{R}_{k+1}}$，这样 R_{k-1} 与 R_{k+1} 分别得到 h_{k+1} 估计值 $\tilde{h}^{\Delta}_{k+1,R_{k-1}}$ 与 $\tilde{h}_{k+1,R_{k+1}}$，且 R_{k-1} 经 $k-1$ 跳可达 Alice，R_{k+1} 经 $k-1$ 跳可达 Bob。经过与前述方法类似的协作保密传递，Alice 与 Bob 均可得到 h_{k+1} 的估计值，分别为

$$\tilde{h}^{\Delta}_{k+1,\mathrm{A}}=\tilde{h}^{\Delta}_{1,\mathrm{A}}\oplus\tilde{h}^{\Delta}_{1,\mathrm{R}_1}\oplus\tilde{h}^{\Delta}_{2,\mathrm{R}_1}\oplus\tilde{h}^{\Delta}_{2,\mathrm{R}_2}\oplus\cdots\oplus\tilde{h}^{\Delta}_{k+1,\mathrm{R}_{k-1}}\tag{10}$$

$$\tilde{h}^{\Delta}_{k+1,\mathrm{B}}=\tilde{h}^{\Delta}_{N,\mathrm{B}}\oplus\tilde{h}^{\Delta}_{N,\mathrm{R}_{2k-1}}\oplus\tilde{h}^{\Delta}_{N-1,\mathrm{R}_{2k-1}}\oplus\tilde{h}^{\Delta}_{N-1,\mathrm{R}_{2k-2}}\oplus\cdots\oplus\tilde{h}^{\Delta}_{k+1,\mathrm{R}_{k+1}}\tag{11}$$

此时，Alice 与 Bob 也得到了相关信息 $\left(\tilde{h}^{\Delta}_{k+1,\mathrm{A}},\tilde{h}^{\Delta}_{k+1,\mathrm{B}}\right)$，令量化间隔 Δ 趋近于 0，则量化带来的误差可忽略不计。Alice 与 Bob 即可将 $\left(\tilde{h}^{\Delta}_{k+1,\mathrm{A}},\tilde{h}^{\Delta}_{k+1,\mathrm{B}}\right)$ 作为密钥源，协商生成相同的密钥。

3.3　密钥协商阶段

在 T_3 时隙，Alice 通过公共信道向 Bob 发送协商信息 $\boldsymbol{\Phi}$，Alice 与 Bob 根据共同信息 $\left(\tilde{h}^{\Delta}_{k+1,\mathrm{A}},\tilde{h}^{\Delta}_{k+1,\mathrm{B}}\right)$ 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 需要满足以下条件（给定任意的 $\varepsilon>0$ 和充分大的 n）。

$$\begin{aligned}&\frac{1}{n}I(K;\boldsymbol{\Phi})\leqslant\varepsilon\\&\frac{1}{n}H(K)\geqslant R_s-\varepsilon\\&\frac{1}{n}\log|\mathcal{K}|\leqslant\frac{1}{n}H(K)+\varepsilon\end{aligned}\tag{12}$$

其中，$I(X;Y)$ 为随机变量 X 与 Y 的互信息，$H(X)$ 为随机变量 X 的熵，$\mathcal{K}$ 为密钥 K 的有限字符集，$|\mathcal{K}|$ 为 $\mathcal{K}$ 的基数。

为了使 Alice 和 Bob 得到相同速率为 R_s 的密钥，Alice 可采用 Slepian-Wolf 编码，通过无噪公共协商信道发送协商信息 $\boldsymbol{\Phi}$ 给 Bob，以生成相同的密钥 K。虽然协商信息 $\boldsymbol{\Phi}$ 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 $\tilde{h}^{\Delta}_{k+1,\mathrm{A}}$ 量化为二进制序列 $\tilde{\boldsymbol{h}}^{\Delta}_{\mathrm{A}}$，同样地，Bob 也可将估计出的 $\tilde{h}^{\Delta}_{k+1,\mathrm{B}}$ 量化为二进制序列 $\tilde{\boldsymbol{h}}^{\Delta}_{\mathrm{B}}$。然后，Alice 随机地将 $\tilde{\boldsymbol{h}}^{\Delta}_{\mathrm{A}}$ 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 $\tilde{\boldsymbol{h}}^{\Delta}_{\mathrm{A}}$ 典型序列，这样每个典型序列包含 2 个索引：所在子集索引号和子集内的序列索引号。Alice 估计出 $\tilde{h}^{\Delta}_{k+1,\mathrm{A}}$ 得到 $\tilde{\boldsymbol{h}}^{\Delta}_{\mathrm{A}}$ 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索引号作为协商信息通过无噪公共协商信道发送给 Bob，Alice 需要向 Bob 发送 $H(\tilde{\boldsymbol{h}}^{\Delta}_{\mathrm{A}}\,|\,\tilde{\boldsymbol{h}}^{\Delta}_{\mathrm{B}})$ 比特信息，其中，$H(X\,|\,Y)$ 表示在给定随机变量 Y 时，随机变量 X 的条件熵。Bob 收到协商信息后，结合自己估计出的 $\tilde{\boldsymbol{h}}_{\mathrm{B}}$ 对应的序列 $\tilde{\boldsymbol{h}}^{\Delta}_{\mathrm{B}}$，就可以任意接近 1 的概率恢复出 $\tilde{\boldsymbol{h}}^{\Delta}_{\mathrm{A}}$，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 即使获取子集索引号，依然不知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。物联网多跳中继系统中的密钥生成过程如算法 1 所示。

算法 1　物联网多跳中继系统中的密钥生成过程

步骤 1　信道估计：Alice, Bob, $\mathrm{R}_1, \cdots, \mathrm{R}_N$ 分别发送训练序列，Alice 估计出 $\tilde{h}_{1,\mathrm{A}}$，Bob 估计出 $\tilde{h}_{N,\mathrm{B}}$，R_i 估计出 $\tilde{h}_{i,\mathrm{R}_i}$ 与 $\tilde{h}_{i+1,\mathrm{R}_i}$。

步骤 2　中继协作：$\mathrm{R}_1, \cdots, \mathrm{R}_N$ 采用安全网络编码技术参与协作，协助 Alice 与 Bob 分别估计出 $\tilde{h}^{\Delta}_{k+1,\mathrm{A}}$ 与 $\tilde{h}^{\Delta}_{k+1,\mathrm{B}}$，且保证 Eve 无法获取信道 h_{k+1} 的任何信息。

步骤 3　密钥协商：Alice 根据 $\tilde{h}^{\Delta}_{k+1,\mathrm{A}}$ 生成互不相关的密钥 K 和协商信息 $\boldsymbol{\Phi}$，并将 $\boldsymbol{\Phi}$ 通过无噪公共协商信道发送给 Bob，Bob 利用 $\boldsymbol{\Phi}$ 和 $\tilde{h}^{\Delta}_{k+1,\mathrm{B}}$ 生成相同的密钥 K。

3.4　密钥生成方法示例

下面，以 $N=3$、4 为例，阐述 3 跳链路和 4 跳链路密钥生成方法的具体实现过程。当 $N=3$ 时，$k=1$，链路中有 2 个中继节点 R_1 与 R_2，如图 3 所示，密钥生成过程如算法 2 所示。

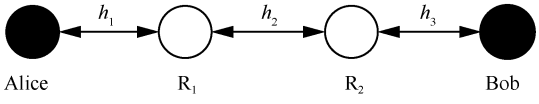


图 3　3 跳链路的密钥生成系统模型

算法 2　3 跳链路密钥生成过程

步骤 1　信道估计：Alice, Bob, R_1 和 R_2 分别发送训练序列，Alice 估计出 $\tilde{h}_{1,\mathrm{A}}$，Bob 估计出 $\tilde{h}_{3,\mathrm{B}}$，R_1 估计出 $\tilde{h}_{1,\mathrm{R}_1}$ 与 $\tilde{h}_{2,\mathrm{R}_1}$，$\mathrm{R}_2$ 估计出 $\tilde{h}_{2,\mathrm{R}_2}$ 与 $\tilde{h}_{3,\mathrm{R}_2}$。

步骤 2　中继协作：R_1 采用安全网络编码技术，利用 $\tilde{h}_{1,\mathrm{R}_1}$ 与 $\tilde{h}_{2,\mathrm{R}_1}$ 生成辅助信息 $s_{\mathrm{R}_1}=\tilde{h}^{\Delta}_{1,\mathrm{R}_1}\oplus\tilde{h}^{\Delta}_{2,\mathrm{R}_1}$，将 s_{R_1} 发送给 Alice，然后 Alice 利用 $\tilde{h}_{1,\mathrm{A}}$ 与 s_{R_1} 估计出 $\tilde{h}_{2,\mathrm{A}}$。同时 R_2 采用安全网络编码技术，利用 $\tilde{h}_{2,\mathrm{R}_2}$ 与 $\tilde{h}_{3,\mathrm{R}_2}$ 生成辅助信息 $s_{\mathrm{R}_2}=\tilde{h}^{\Delta}_{2,\mathrm{R}_2}\oplus\tilde{h}^{\Delta}_{3,\mathrm{R}_2}$，将 s_{R_2} 发送给 Bob，然后 Bob 利用 $\tilde{h}_{3,\mathrm{B}}$ 与 s_{R_2} 估计出 $\tilde{h}_{2,\mathrm{B}}$。Eve 也可以知晓 s_{R_1} 与 s_{R_2}，但它不知信道 h_1 与 h_3，也就无法获取信道 h_2 的任何信息。

步骤 3　密钥协商：Alice 根据 $\tilde{h}_{2,\mathrm{A}}$ 生成互不相关的密钥 K 和协商信息 $\boldsymbol{\Phi}$，并将 $\boldsymbol{\Phi}$ 通过无噪公共协商信道发送给 Bob，Bob 利用 $\boldsymbol{\Phi}$ 和 $\tilde{h}_{2,\mathrm{B}}$ 生成相同的密钥 K。

当 $N=4$ 时，$k=2$，链路中有 3 个中继节点 R_1、R_2 与 R_3，如图 4 所示，密钥生成过程如算法 3 所示。

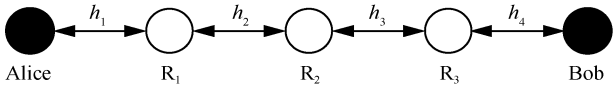


图 4　4 跳链路的密钥生成系统模型

算法 3　4 跳链路密钥生成过程

步骤 1　信道估计：Alice, Bob, R_1, R_2 和 R_3 分别发送训练序列，Alice 估计出 $\tilde{h}_{1,\mathrm{A}}$，Bob 估计出 $\tilde{h}_{4,\mathrm{B}}$，R_1 估计出 $\tilde{h}_{1,\mathrm{R}_1}$ 与 $\tilde{h}_{2,\mathrm{R}_1}$，$\mathrm{R}_2$ 估计出 $\tilde{h}_{2,\mathrm{R}_2}$ 与 $\tilde{h}_{3,\mathrm{R}_2}$，$\mathrm{R}_3$ 估计出 $\tilde{h}_{3,\mathrm{R}_3}$ 与 $\tilde{h}_{4,\mathrm{R}_3}$。

步骤 2　中继协作：R_2 采用安全网络编码技术，利用 $\tilde{h}_{2,\mathrm{R}_2}$ 与 $\tilde{h}_{3,\mathrm{R}_2}$ 生成辅助信息 $s_{\mathrm{R}_2}=\tilde{h}^{\Delta}_{2,\mathrm{R}_2}\oplus\tilde{h}^{\Delta}_{3,\mathrm{R}_2}$，并将 s_{R_2} 发送给 R_1，R_1 利用 $\tilde{h}_{2,\mathrm{R}_1}$ 与 s_{R_2} 估计 $\tilde{h}_{3,\mathrm{R}_1}$；然后，$\mathrm{R}_1$ 与 R_3 采用安全网络编码技术，分别生成辅助信息 $s_{\mathrm{R}_1}=\tilde{h}^{\Delta}_{1,\mathrm{R}_1}\oplus\tilde{h}^{\Delta}_{3,\mathrm{R}_1}$ 与 $s_{\mathrm{R}_3}=\tilde{h}^{\Delta}_{4,\mathrm{R}_3}\oplus\tilde{h}^{\Delta}_{3,\mathrm{R}_3}$，并发送给 Alice 与 Bob。这样，Alice 利用 $\tilde{h}_{1,\mathrm{A}}$ 与 s_{R_1} 估计出 $\tilde{h}_{3,\mathrm{A}}$，Bob 利用 $\tilde{h}_{4,\mathrm{B}}$ 与 s_{R_3} 估计出 $\tilde{h}_{3,\mathrm{B}}$。同时 Eve 也可以知晓 s_{R_1}、s_{R_2} 与 s_{R_3}，但它不知晓信道 h_1、h_2 与 h_4，也就无法获取信道 h_3 的任何信息。

步骤 3　密钥协商：Alice 根据 $\tilde{h}_{3,\mathrm{A}}$ 生成互不相

关的密钥 K 和协商信息 $\boldsymbol{\Phi}$，并将 $\boldsymbol{\Phi}$ 通过无噪公共协商信道发送给 Bob，Bob 利用 $\boldsymbol{\Phi}$ 和 $\tilde{h}_{3,\mathrm{B}}$ 生成相同的密钥 K。

4　安全性分析

本文的密钥生成方法中，Alice 与 Bob 得到了相关观测值 $\left(\tilde{h}_{k+1,\mathrm{A}}^{\Delta},\tilde{h}_{k+1,\mathrm{B}}^{\Delta}\right)$，Eve 得到了窃听信道估计值 $\tilde{\boldsymbol{h}}_{\mathrm{E}}=\left(\tilde{h}_{\mathrm{AE}},\tilde{h}_{\mathrm{BE}},\tilde{h}_{\mathrm{R_1E}},\tilde{h}_{\mathrm{R_2E}},\cdots,\tilde{h}_{\mathrm{R}_{N-1}\mathrm{E}}\right)$ 和所有中继节点发送的辅助信息 $\boldsymbol{s}_{\mathrm{R}}=\left(s_{\mathrm{R}_1},s_{\mathrm{R}_2},\cdots,s_{\mathrm{R}_{N-1}}\right)$。以可达密钥速率衡量所提方法的安全性，根据 Maurer 的研究成果[8]，满足式(12)的密钥 K 的可达密钥速率为

$$R_s=\frac{1}{T}I\left(\tilde{h}_{k+1,\mathrm{A}}^{\Delta};\tilde{h}_{k+1,\mathrm{B}}^{\Delta}\mid\tilde{\boldsymbol{h}}_{\mathrm{E}},\boldsymbol{s}_{\mathrm{R}}\right)\tag{13}$$

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

首先以 2 跳和 3 跳为例，计算可达密钥速率。当 $N=2$ 时，只有一个中继节点 R_1，$k=1$，Alice 与 Bob 得到了相关观测值 $\left(\tilde{h}_{2,\mathrm{A}}^{\Delta},\tilde{h}_{2,\mathrm{B}}^{\Delta}\right)$，Eve 得到了窃听信道估计值 $\tilde{\boldsymbol{h}}_{\mathrm{E}}=\left(\tilde{h}_{\mathrm{AE}},\tilde{h}_{\mathrm{BE}},\tilde{h}_{\mathrm{R_1E}}\right)$ 和 R_1 发送的辅助信息 s_{R_1}，可达密钥速率为

$$R_{s,2}=\frac{1}{T}I\left(\tilde{h}_{2,\mathrm{A}};\tilde{h}_{2,\mathrm{B}}\left|\tilde{h}_{\mathrm{AE}},\tilde{h}_{\mathrm{BE}},\tilde{h}_{\mathrm{R_1E}},s_{\mathrm{R}_1}\right.\right)\tag{14}$$

根据互信息的性质，可以得到

$$\begin{aligned}&I\left(\tilde{h}_{2,\mathrm{A}};\tilde{h}_{2,\mathrm{B}}\mid\tilde{h}_{\mathrm{AE}},\tilde{h}_{\mathrm{BE}},\tilde{h}_{\mathrm{R_1E}},s_{\mathrm{R}_1}\right)\\&=I\left(\tilde{h}_{2,\mathrm{A}};\tilde{h}_{2,\mathrm{B}},\tilde{h}_{\mathrm{AE}},\tilde{h}_{\mathrm{BE}},\tilde{h}_{\mathrm{R_1E}},s_{\mathrm{R}_1}\right)-\\&\quad I\left(\tilde{h}_{2,\mathrm{A}};\tilde{h}_{\mathrm{AE}},\tilde{h}_{\mathrm{BE}},\tilde{h}_{\mathrm{R_1E}},s_{\mathrm{R}_1}\right)\\&\overset{(a)}{=}I\left(\tilde{h}_{2,\mathrm{A}};\tilde{h}_{2,\mathrm{B}},s_{\mathrm{R}_1}\right)-I\left(\tilde{h}_{2,\mathrm{A}};s_{\mathrm{R}_1}\right)\\&=I\left(\tilde{h}_{2,\mathrm{A}};\tilde{h}_{2,\mathrm{B}}\mid s_{\mathrm{R}_1}\right)\end{aligned}\tag{15}$$

因为窃听信道 h_{AE}、h_{BE}、$h_{\mathrm{R_1E}}$ 与 h_1、h_2 均独立，因此 $\tilde{h}_{\mathrm{AE}}$、$\tilde{h}_{\mathrm{BE}}$、$\tilde{h}_{\mathrm{R_1E}}$ 与 $\tilde{h}_{2,\mathrm{A}}$、$\tilde{h}_{2,\mathrm{B}}$、s_{R_1} 均不相关，这样由互信息的定义可得步骤 (a) 成立。此外，根据异或运算的性质，且 h_1 与 h_2 独立，容易得到 $I(\tilde{h}_{1,\mathrm{A}}^{\Delta}\oplus\tilde{h}_{1,\mathrm{R}_1}^{\Delta}\oplus\tilde{h}_{2,\mathrm{R}_1}^{\Delta};\tilde{h}_{1,\mathrm{R}_1}^{\Delta}\oplus\tilde{h}_{2,\mathrm{R}_1}^{\Delta})=0$，$I(\tilde{h}_{2,\mathrm{B}}^{\Delta};\tilde{h}_{1,\mathrm{R}_1}^{\Delta}\oplus\tilde{h}_{2,\mathrm{R}_1}^{\Delta})=0$，即 $I(\tilde{h}_{2,\mathrm{A}}^{\Delta};s_{\mathrm{R}_1})=0$，$I(\tilde{h}_{2,\mathrm{B}}^{\Delta};s_{\mathrm{R}_1})=0$。因此，式(14)可简化为

$$\begin{aligned}R_{s,2}&=\frac{1}{T}I\left(\tilde{h}_{2,\mathrm{A}};\tilde{h}_{2,\mathrm{B}}\mid s_{\mathrm{R}_1}\right)\\&=\frac{1}{T}\lim_{\Delta\to0}I\left(\tilde{h}_{2,\mathrm{A}}^{\Delta};\tilde{h}_{2,\mathrm{B}}^{\Delta}\mid s_{\mathrm{R}_1}\right)\\&=\frac{1}{T}\lim_{\Delta\to0}\left[I\left(\tilde{h}_{2,\mathrm{A}}^{\Delta};\tilde{h}_{2,\mathrm{B}}^{\Delta},s_{\mathrm{R}_1}\right)-I\left(\tilde{h}_{2,\mathrm{A}}^{\Delta};s_{\mathrm{R}_1}\right)\right]\\&=\frac{1}{T}\lim_{\Delta\to0}\left[I\left(\tilde{h}_{2,\mathrm{A}}^{\Delta};\tilde{h}_{2,\mathrm{B}}^{\Delta}\right)+I\left(\tilde{h}_{2,\mathrm{A}}^{\Delta};s_{\mathrm{R}_1}\mid\tilde{h}_{2,\mathrm{B}}^{\Delta}\right)\right]\\&=\frac{1}{T}I\left(\tilde{h}_{2,\mathrm{A}};\tilde{h}_{2,\mathrm{B}}\right)\end{aligned}\tag{16}$$

当 $N=3$ 时，有 2 个中继节点 R_1 和 R_2，$k=1$，Alice 与 Bob 得到了相关观测值 $\left(\tilde{h}_{2,\mathrm{A}}^{\Delta},\tilde{h}_{2,\mathrm{B}}^{\Delta}\right)$，Eve 得到窃听信道估计值 $\tilde{\boldsymbol{h}}_{\mathrm{E}}=\left(\tilde{h}_{\mathrm{AE}},\tilde{h}_{\mathrm{BE}},\tilde{h}_{\mathrm{R_1E}},\tilde{h}_{\mathrm{R_2E}}\right)$，$\mathrm{R}_1$ 发送的辅助信息 s_{R_1} 和 R_2 发送的辅助信息 s_{R_2}。类似地，可达密钥速率可以表示为

$$R_{s,3}=\frac{1}{T}I\left(\tilde{h}_{2,\mathrm{A}};\tilde{h}_{2,\mathrm{B}}\left|\tilde{h}_{\mathrm{AE}},\tilde{h}_{\mathrm{BE}},\tilde{h}_{\mathrm{R_1E}},\tilde{h}_{\mathrm{R_2E}},s_{\mathrm{R}_1},s_{\mathrm{R}_2}\right.\right)\tag{17}$$

同样地，根据互信息的性质以及 $\tilde{h}_{\mathrm{AE}}$、$\tilde{h}_{\mathrm{BE}}$、$\tilde{h}_{\mathrm{R_1E}}$、$\tilde{h}_{\mathrm{R_2E}}$ 与 $\tilde{h}_{2,\mathrm{A}}$、$\tilde{h}_{2,\mathrm{B}}$、s_{R_1}、s_{R_2} 均不相关，可得

$$R_{s,3}=\frac{1}{T}I\left(\tilde{h}_{2,\mathrm{A}};\tilde{h}_{2,\mathrm{B}}\mid s_{\mathrm{R}_1},s_{\mathrm{R}_2}\right)\tag{18}$$

此外，根据异或运算的性质以及 h_1、h_2、h_3 相互独立，可得

$$\begin{aligned}R_{s,3}&=\frac{1}{T}I\left(\tilde{h}_{2,\mathrm{A}};\tilde{h}_{2,\mathrm{B}}\left|s_{\mathrm{R}_1},s_{\mathrm{R}_2}\right.\right)\\&=\frac{1}{T}\lim_{\Delta\to0}I\left(\tilde{h}_{1,\mathrm{A}}^{\Delta}\oplus\tilde{h}_{1,\mathrm{R}_1}^{\Delta}\oplus\tilde{h}_{2,\mathrm{R}_1}^{\Delta};\tilde{h}_{3,\mathrm{B}}^{\Delta}\oplus\tilde{h}_{3,\mathrm{R}_2}^{\Delta}\oplus\right.\\&\quad\left.\tilde{h}_{2,\mathrm{R}_2}^{\Delta}\left|\tilde{h}_{1,\mathrm{R}_1}^{\Delta}\oplus\tilde{h}_{2,\mathrm{R}_1}^{\Delta},\tilde{h}_{2,\mathrm{R}_2}^{\Delta}\oplus\tilde{h}_{3,\mathrm{R}_2}^{\Delta}\right.\right)\\&=\frac{1}{T}\lim_{\Delta\to0}I\left(\tilde{h}_{1,\mathrm{A}}^{\Delta}\oplus\tilde{h}_{1,\mathrm{R}_1}^{\Delta}\oplus\tilde{h}_{2,\mathrm{R}_1}^{\Delta};\tilde{h}_{3,\mathrm{B}}^{\Delta}\oplus\tilde{h}_{3,\mathrm{R}_2}^{\Delta}\oplus\tilde{h}_{2,\mathrm{R}_2}^{\Delta}\right)\\&=\frac{1}{T}I\left(\tilde{h}_{2,\mathrm{A}};\tilde{h}_{2,\mathrm{B}}\right)\end{aligned}\tag{19}$$

结合 $N=2$、3 时的密钥速率计算，可以得到 N 跳链路的可达密钥速率为

$$\begin{aligned}R_{s,N}&=\frac{1}{T}I\left(\tilde{h}_{k+1,\mathrm{A}};\tilde{h}_{k+1,\mathrm{B}}\mid\tilde{\boldsymbol{h}}_{\mathrm{E}},\boldsymbol{s}_{\mathrm{R}}\right)\\&\overset{(b)}{=}\frac{1}{T}I\left(\tilde{h}_{k+1,\mathrm{A}};\tilde{h}_{k+1,\mathrm{B}}\mid\boldsymbol{s}_{\mathrm{R}}\right)\\&=\frac{1}{T}\lim_{\Delta\to0}I\left(\tilde{h}_{k+1,\mathrm{A}}^{\Delta};\tilde{h}_{k+1,\mathrm{B}}^{\Delta}\left|s_{\mathrm{R}_1},s_{\mathrm{R}_2},\cdots,s_{\mathrm{R}_{N-1}}\right.\right)\\&\overset{(c)}{=}\frac{1}{T}I\left(\tilde{h}_{k+1,\mathrm{A}};\tilde{h}_{k+1,\mathrm{B}}\right)\end{aligned}\tag{20}$$

步骤 (b) 成立是因为窃听信道 $\tilde{\boldsymbol{h}}_{\mathrm{E}}$ 与 $\tilde{h}_{k+1,\mathrm{A}}$、$\tilde{h}_{k+1,\mathrm{B}}$、$\boldsymbol{s}_{\mathrm{R}}$ 均不相关，步骤 (c) 成立是依据异或运算的性质及 $h_1,h_2,\cdots,h_N$ 之间相互独立。式(20)证明了本文所提方法不会泄露密钥源的任何信息。

5 性能仿真

为了验证所提方法的安全性能，并分析影响可达密钥速率的因素，基于 Matlab 工具进行一些仿真实验。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 100 000 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 estimator）工具包，估计式(20)中相应信道增益估计值之间的互信息。

首先，针对 $N=2$、3、4 时所提密钥生成方法的可达密钥速率进行仿真，假设相干长度 $T=10$，各信道的增益方差均为 $\sigma_h^2=1$，各节点信道估计时的发送功率 $P_{\mathrm{ce}}=1$，发送时间 $T_{\mathrm{ce}}=1$。仿真本文的基于安全网络编码（SNC）的密钥生成方法的可达密钥速率随信噪比（SNR, signal-to-noise ratio）的变化曲线，并与基于放大转发（AF）[18]的密钥生成方法对比，如图 5 所示。

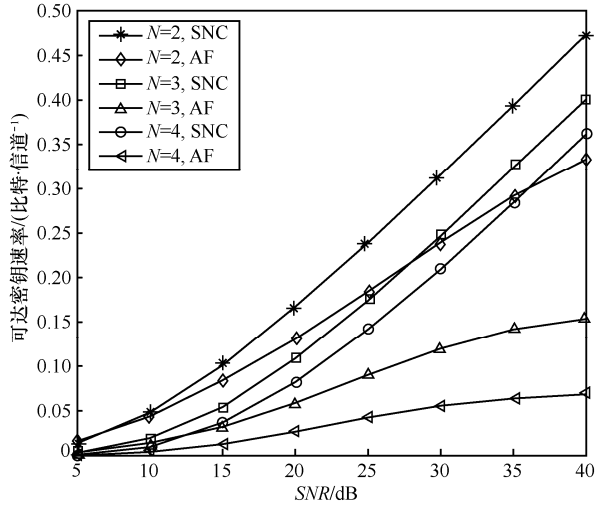


图 5 可达密钥速率随信噪比的变化曲线

由图 5 可以看出，上述 2 种方法的可达密钥速率均随着 *SNR* 的提高而增长，这是因为随着 *SNR* 的提高，采用 2 种方法估计的信道误差均减小，密钥源的熵增加。在跳数相同的情况下，SNC 方法的可达密钥速率明显大于 AF 方法的可达密钥速率。例如，当 $SNR=30$ dB，$N=3$ 时，每利用一次信道 SNC 方法比 AF 方法多产生约 0.13 bit 密钥。这是因为在 SNC 方法中，中继发送采用安全网络编码生成的辅助信息，不泄露密钥源的任何信息，而在 AF 方法中，中继直接放大转发，泄露了作为密钥源的信道部分信息，导致可达密钥速率降低。此外，在 2 种方法中，跳数的增加都会导致可达密钥速率的降低，这是因为噪声的存在会导致信道估计产生误差，而跳数增加使信道估计误差累积增大，从而导致合法通信双方获取的共同信息减少，降低密钥源的熵。

在物联网应用场景中，中继节点数量众多，在 Alice 与 Bob 之间可能存在多条传输路径，虽然在通信时只选取一条最优传输路径，但在密钥生成的过程中，为了提高密钥生成速率，可以利用多条传输路径生成密钥，在通信时只选取一条最优传输路径加密传输，因此本文仿真了传输路径数量（N_{path}）对可达密钥速率的影响。针对 2 跳链路和 3 跳链路（N=2、3），分别选取 N_{path}=1、2、3 进行仿真。假设相干长度 $T=20$，各信道增益的方差均 $\sigma_h^2=1$，各节点信道估计时的发送功率 $P_{\mathrm{ce}}=1$，发送时间 $T_{\mathrm{ce}}=1$。中继节点之间的距离均大于半个波长（符合实际的通信场景），保证所有信道之间都是相互独立的，可达密钥速率随 *SNR* 的变化曲线如图 6 所示。

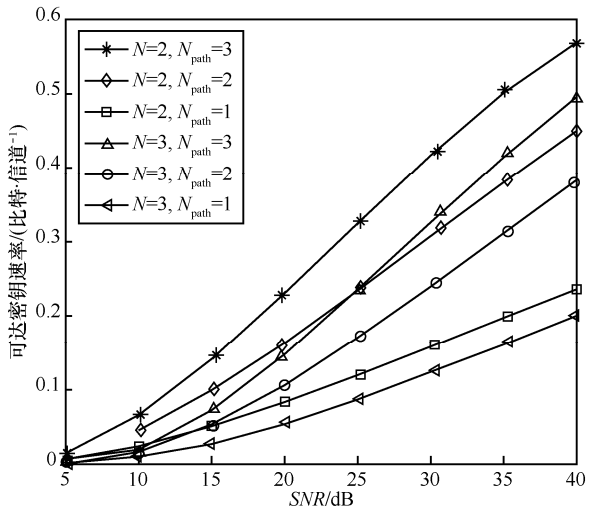


图 6 多路径下 SNC 方法的可达密钥速率变化曲线

由图 6 可以看出，在低 *SNR* 区域，由于噪声太大，传输路径数量的增加对可达密钥速率的影响不大，但随着 *SNR* 的升高，在高 *SNR* 区域，传输路

径数量的增加能显著提高可达密钥速率。例如，当 $SNR=30\,\text{dB}$ 时，在 2 跳链路中每增加一条路径至少可以使可达密钥速率提高 0.1 比特/信道（比特/信道是指每利用一次信道产生密钥的比特数），在 3 跳链路中每增加一条路径至少可以使可达密钥速率提高 0.08 比特/信道。这是因为参与密钥生成的传输路径数量的增加，会导致 Alice 与 Bob 之间的共同信息的增加，增大密钥源的熵，从而提升 Alice 与 Bob 之间的可达密钥速率。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，选取多条传输路径共同产生密钥将是有效的解决途径。需要注意的是，图 6 中 $N=2$, $N_{\text{path}}=1$ 与 $N=3$, $N_{\text{path}}=1$ 时的可达密钥速率是图 5 中 $N=2$, SNC 与 $N=3$, SNC 时的一半，这是因为图 6 的可达密钥速率是在相干长度 $T=20$ 时获得的，而图 5 是在 $T=10$ 时得到的。

由于可达密钥速率是由合法通信双方信道估计值的互信息决定的，而二者的互信息与信道的方差有关，因此针对单条传输路径的场景，仿真了信道方差对可达密钥速率的影响。假设相干长度 $T=10$，各节点信道估计时的发送功率 $P_{\text{ce}}=1$，发送时间 $T_{\text{ce}}=1$，针对 2 跳链路和 3 跳链路（$N=2$、3），分别选取 $\sigma_h^2=1$、2、4 进行仿真实验，可达密钥速率随 SNR 的变化曲线如图 7 所示。

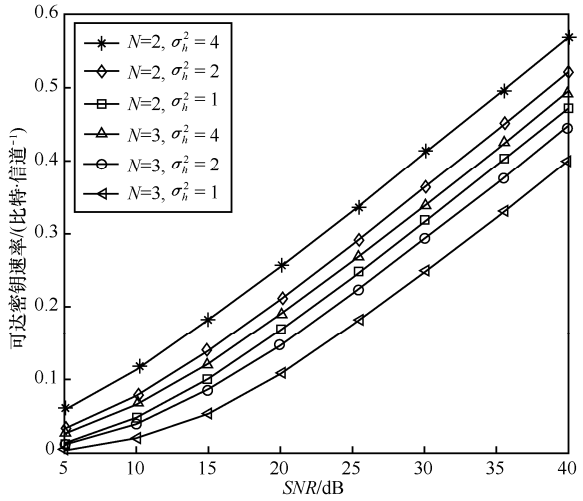


图 7　不同信道方差对 SNC 方法可达密钥速率的影响

由图 7 可以看出，在跳数相同的情况下，信道的方差越大，可达密钥速率就越大。例如，当 $SNR=30\,\text{dB}$，$N=2$ 时，$\sigma_h^2=4$ 的可达密钥速率比 $\sigma_h^2=1$ 提高约 0.1 比特/信道；当 $SNR=30\,\text{dB}$，$N=3$ 时，$\sigma_h^2=4$ 的可达密钥速率比 $\sigma_h^2=1$ 提高约 0.09 比特/信道。这是因为信道增益建模为高斯随机变量，信道的方差越大，密钥源的熵就越大，可达密钥速率就相应地得到提升，这为多条传输路径场景下的传输路径选择提供了指导。

6　结束语

本文针对物联网中的多跳中继系统进行研究，提出一种基于网络编码的协作密钥生成方法。由于合法通信双方之间不存在直达链路，二者无法获取相关的信道估计信息，中继节点采用安全网络编码技术参与协作，辅助合法通信双方获取相同信道的估计值；合法通信双方直接在公共信道上进行密钥协商，以二者通过中继辅助获取的相关观测值为密钥源，生成相同的密钥。该方法的主要优点是：中继节点采用安全网络编码协作，不泄露作为密钥源的信道的任何信息；密钥协商过程不需要中继节点的参与，降低中继节点协作的代价。此外，通过推导所提方法的可达安全速率，从理论上证明了该方法不泄露密钥源的任何信息。蒙特卡洛仿真表明，所提方法与放大转发方法相比可以显著提高可达密钥速率，且增加传输路径数量和选取跳数少、信道变化幅度大的传输路径，可以进一步提高可达密钥速率，从而为多条传输路径的场景下，进一步提高可达密钥速率指明了方向。

参考文献：

[1] LINDQVIST U, NEUMANN P G. The future of the Internet of things[J]. Communications of the ACM, 2017, 60(2): 26-30.

[2] 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.

[3] MUKHERJEE A, FAKOORIAN S A, HUANG J, et al. Principles of physical layer security in multiuser wireless networks: a survey[J]. IEEE Communications Surveys & Tutorials, 2014, 16(3): 1550-1573.

[4] ZENG K. Physical layer key generation in wireless networks: challenges and opportunities[J]. IEEE Communications Magazine, 2015, 53(6): 33-39.

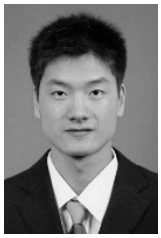
[5] XU P, CUMANAN K, DING Z, et al. Group secret key generation in wireless networks: algorithms and rate optimization[J]. IEEE Transactions on Information and Security, 2016, 11(8): 1831-1846.

[6] YANG E, WU X. Information-theoretically secure key generation and management[C]//IEEE International Symposium on Information Theory. 2017: 1529-1533.

[7] ZHANG H, LIANG Y, LAI L, et al. Multi-key generation over a cellular model with a helper[J]. IEEE Transactions on Information and Security, 2017, 63(6): 3804-3822.

[8] MAURER U M. Secret key agreement by public discussion from common information[J]. IEEE Transactions on Information and Security, 1993, 39(3): 733-742.
[9] AHLSWEDE R, CSISZAR I. Common randomness in information theory and cryptography—part I: secret sharing[J]. IEEE Transactions on Information and Security, 1993, 39(4): 1121-1132.
[10] YE C, MATHUR S, REZNIK A, et al. Information-theoretically secret key generation for fading wireless channel[J]. IEEE Transactions on Information and Security, 2010, 5(2): 240-254.
[11] ZHANG J, DUONG T Q, MARSHALL A, et al. Key generation from wireless channels: a review[J]. IEEE Access, 2016, 4: 614-626.
[12] PENG Y, WANG P, XIANG W, et al. Secret key generation based on estimated channel state information for TDD-OFDM systems over fading channels[J]. IEEE Transactions on Wireless Communications, 2017, 16(8): 5176-5186.
[13] ZHANG J, HE B, DUONG T Q, et al. On the key generation from correlated wireless channels[J]. IEEE Communications Letters, 2017, 21(4): 961-964.
[14] CASTEL T, TORRE P V, 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. 2016: 1-5.
[15] 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.
[16] MARGELIS G, FAFOUTIS X, OIKONOMOU G, et al. Physical layer secret-key generation with discreet cosine transform for the Internet of things[C]//IEEE International Conference on Communications. 2017: 1-6.
[17] CSISZAR I, NARAYAN P. Common randomness and secret key generation with a helper[J]. IEEE Transactions on Information and Security, 2000, 46(2): 344-366.
[18] SHIMIZU T, IWAI H, SASAOKA H. Physical-layer secret key agreement in two-way wireless relaying systems[J]. IEEE Transactions on Information and Security, 2011, 6(3): 650-660.
[19] LAI L, LIANG Y, DU W. Cooperative key generation in wireless networks[J]. IEEE Journal on Selected Areas in Communications, 2012, 30(8): 1578-1588.
[20] ZHOU H, HUIE L M, LAI L. Secret key generation in the two-way relay channel with active attackers[J]. IEEE Transactions on Information and Security, 2014, 9(3): 476-488.
[21] THAI C D T, LEE J, QUEK T Q S. Physical-layer secret key generation with colluding untrusted relays[J]. IEEE Transactions on Wireless Communications, 2016, 15(2): 1517-1530.

[作者简介]



肖帅芳（1989-），男，河南许昌人，国家数字交换系统工程技术研究中心博士生，主要研究方向为无线物理层安全、无线网络与信息安全等。

郭云飞（1963-），男，河南郑州人，国家数字交换系统工程技术研究中心教授、博士生导师，主要研究方向为新型网络体系结构、网络与信息安全等。

黄开枝（1973-），女，安徽滁州人，国家数字交换系统工程技术研究中心教授、博士生导师，主要研究方向为无线物理层安全、移动通信网络与信息安全等。

金梁（1969-），男，北京人，国家数字交换系统工程技术研究中心教授、博士生导师，主要研究方向为无线物理层安全、无线通信网络与信息安全等。