基于成对生成策略的无线网络群密钥产生及其分析

代东明 吴晓富

（南京邮电大学 南京 210036）

摘 要 使用无线信道的物理层信息在无线设备间生成私密密钥用于确保移动环境的安全，如今受到了广泛关注。然而在现实环境中，在多个设备之间生成群密钥以确保群安全通信的问题仍然存在挑战。针对无线网络星型拓扑结构，提出一种基于中心节点成对生成策略的群密钥产生方案。相比于文献中提出的利用群内节点间的接收信号强度差分实现提取群密钥的方案，详细分析了它们各自能实现的群密钥容量并给出了数值计算结果。分析表明，提出的基于成对生成策略的群密钥产生方法在密钥率方面优于文献中的差分提取方案。

关键词 相互密钥提取，接收信号强度，群密钥生成，成对生成策略

中图法分类号 TN918.1 **文献标识码** A

Group Secret Key Generation and Analysis in Wireless Network Based on Pairwise-generating Strategies

DAI Dong-ming WU Xiao-fu

(Nanjing University of Posts and Telecommunications, Nanjing 210036, China)

Abstract Secret key establishment within wireless terminals utilizing physical layer information of wireless channel to ensure the security of mobile environment has received wide attention. However, generating group secret key among multiple wireless devices for secure communication in reality environment remains a challenge. This paper proposed a group secret key establishment scheme based on central node pairwise-generating strategies under the star topology in wireless network. Compared with the existing group secret key extraction method using the difference of received signal strength(RSS) among the wireless devices in the group, we gave a explicit analysis and a specific numerical result on the achieva-ble group secret key rate of each one. It shows that our scheme outperforms that of generating group key by leveraging the difference of RSS on key rate.

Keywords Collaborative secret key extraction, Receiving signal strength, Group secret key generation, Pairwise-generating strategies

1 引言

鉴于无线通信固有的信道特征，近年来基于香农信息论的物理层安全技术成为了研究热点。利用无线信道的物理层信息生成密钥的优点在于它可以允许两个在彼此通信范围内的无线设备提取一个可共享的、对称的加密密钥，在该过程中并不需要一个固定的基础设施或安全的通信信道[1-3]。基于互易性，两设备通过在信道相干时间内相互发送采样序列即可独立地提取相同的密钥，此时能够达到理论意义上的安全[4]。

比较信道不同的物理层信息（例如信道相位[5-6]）时，因为接收信号强度（Received Signal Strength，RSS）在无线信道中较容易被获得，所以利用RSS生成密钥是一个更易实现的方案。但是，在多个无线设备中基于RSS来生成密钥以确保群安全通信的问题仍然存在挑战。文献[7-8]主要从理论上分析了生成群密钥的问题。也有相关文献探讨了具体的群密钥提取算法，如基于RSS差分提取群密钥的方案[10]、在图模型下基于网络编码生成群密钥的算法[11]；文献[12]探讨了基于成对独立网络（Pairwise Independent Network，PIN），采用3个节点、4个节点以及多个节点组成的无线mesh网络结构[13]的各自群密钥提取协议；文献[14]将群内节点划分为多个子群进行群密钥提取；文献[15]研究了多对无线节点下同时生成多组共享密钥的问题。

我们考虑了文献[10-11]中各自密钥生成协议的优缺点，由于差分提取方案的实现过程稍显复杂，本文针对多个节点构造的星型无线网络拓扑结构，提出利用中心节点的成对生成策略实现群密钥的提取；随后分析和对比了两种方案分别能够实现的群密钥率[16]（当群内仅有两个节点时，两种方案的密钥率是一致的），并给出了理论上的原因分析；但是当群内节点数至少为3时，所提方案的密钥率明显更大。同时，讨论了所提方案的应用操作细节和实现复杂度，对比了两种方案的通信开销、密钥实现复杂度及整个密钥提取过程对于攻击的健壮性。最终结果表明，所提方案的群密钥率优于差分提取方案。

本文第2节描述了系统的概况，包括信道的建模和攻击者的模型；第3节回顾了差分提取群密钥方案[10]的过程及其

本文受国家自然科学基金（61372123）资助。

代东明（1996－），男，硕士，主要研究方向为无线网络中群密钥提取协议设计及分析，E-mail：Daylock666@163.com（通信作者）；**吴晓富**（1975－），男，博士，教授，博士生导师，主要研究方向为编码与信息论、计算复杂性与密码学、无线通信与深空通信、导航信号处理，E-mail：xfuwu@ieee.org。

群密钥率的计算；第 4 节详细介绍了所提的方案，包括协议的步骤、可实现群密钥率的理论分析及两种方案的群密钥率的比较；第 5 节给出了方案的实现原型和复杂度及健壮性分析；最后总结了本文所做的工作。

2　系统概况

2.1　信道建模

本文构造的星型无线网络拓扑结构如图 1 所示。在任一时隙 t，观察图中结构的中心节点 C 和其他节点 i（$i=1,2,\cdots,n-1$）所构成的无线信道，有：

$$\hat{Y}_{i,j}^{j}(t)=Y_{i,j}(t)+W_{i,j}^{j}(t),\ j=c,i \tag{1}$$

其中，$\hat{Y}_{i,j}^{j}(t)$ 表示在时隙 t 节点 j 获得的关于信道 (j,i) 的观察信息；$Y_{i,j}(t)$ 是实际的信道增益，它对于不同的信道 (j,i) 和时隙 t 而言都属于独立同分布，且针对所有的节点 i 和 j 都有 $Y_{i,j}(t)=Y_{j,i}(t)$，均值为 0，方差为 σ_Y^2；$W_{i,j}^{j}(t)$ 是观察噪声，对于 i 和 j 是独立同分布的；同样，针对每一个 i 和 j，都有均值为 0，方差为 σ_W^2。最后，定义 $\gamma_m=\dfrac{\sigma_Y^2}{\sigma_W^2}$ 为测量 SNR，密钥生成过程中涉及到对 $\hat{Y}_{i,j}^{j}(t)$ 进行量化[10]，其中 m 为量化的级数。由上述假设可知，$\hat{Y}_{i,j}^{j}(t)$ 关于 t 也是独立同分布的，因此后续计算中会直接使用 $\hat{Y}_{i,j}^{j}$。

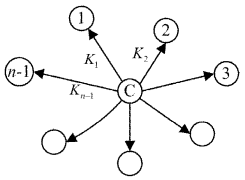

图 1　无线网络星型拓扑结构

2.2　攻击模型

我们所考虑的窃听者是一个被动的对手，其观察的信道增益和其他合法移动设备观察的信道增益是相互独立的。窃听者可以窃听密钥生成过程中的所有公共讨论的信息，且可以获得该过程中的密钥生成算法和对应的参数。假定窃听者与合法设备的距离至少为 $\lambda/2$（波长的一半）[17]，在这种情况下，多径衰落环境的无线信道增益是去相关的，导致从窃听者和合法节点之间可以得到相互独立的信道观察。这就表明窃听者仅能通过自己信道的观察来提取信息[18]。然而，在累积多个无线设备在公共讨论阶段所广播的信道信息的基础上，窃听者还是能够通过用户的增加来获得部分甚至全部的群密钥。为了应对这种情况，合法用户在提取密钥后会进行隐私放大过程。

3　基于接收信号强度差分提取群密钥

3.1　协议步骤

下面简短回顾文献[10]中提出的基于接收信号强度差分提取群密钥的方案，其中涉及的网络拓扑结构如图 2 所示，具体步骤如下：

1）从所有节点中随机选取一个节点作为虚拟中心节点 C，另随机选取一节点作为参考节点，此处选择节点 1。后续计算接收信号强度的差值（Different of Signal Strength，DOSS）时将会基于节点 C 和节点 1 之间的信道。

2）每一个节点 $j(j=1,2,\cdots,n-1)$ 通过互发探针包获得其与节点 C 之间的信道观察 $\hat{Y}_{c,j}^{j}(t)$，对其进行量化得到 $\hat{Y}_{c,j}^{\Delta,j}(t)$。与此同时，节点 C 同样会获得与所有节点 j 之间的信道测量 $\hat{Y}_{j,c}^{c}(t)$。

3）对于所有的 $j=2,3,\cdots,n-1$，节点 C 分别计算相应的 DOSS 值，并将其量化后向其它所有节点广播。

$$\delta_j(t)=\hat{Y}_{j,c}^{c}(t)-\hat{Y}_{1,c}^{c}(t) \tag{2}$$

4）最后，由中心节点 C 发起一个单向的公共讨论，并通过信息和解产生初始密钥。在步骤 3）之后，其他每个节点（包括窃听者）都会获得全部的 DOSS 值，由式(2)便可计算出所有的信道观察 $[\hat{Y}_{1,c}^{\Delta,c},\hat{Y}_{2,c}^{\Delta,c},\cdots,\hat{Y}_{n-1,c}^{\Delta,c}]$；而节点 C 在步骤 2）后便已获得全部信道观察，因此能够利用 Slepian-Wolf 编码产生群密钥。

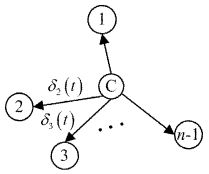

图 2　基于接收信号强度差分提取群密钥的方案

3.2　群密钥率计算

在公共讨论阶段的最后，所有节点都会获得公共信息 $[\hat{Y}_{1,c}^{\Delta,c},\hat{Y}_{2,c}^{\Delta,c},\cdots,\hat{Y}_{n-1,c}^{\Delta,c}]$，随后利用 Slepian-Wolf 编码产生群密钥。节点 C 利用 $2^{TR_{key}}$ 个码字构建一个随机的分层结构，其中 $R_{key}(T)=\dfrac{1}{T}H(\hat{Y}_{1,c}^{\Delta,c},\cdots,\hat{Y}_{n-1,c}^{\Delta,c})$。为了使整个群都能译码公共信息，分层的层数应该不少于 $2^{TR_{bin}(T)}$：

$$R_{bin}(T)=\max_{1\leqslant j\leqslant n-1}\frac{1}{T}H(\hat{Y}_{1,c}^{\Delta,c},\cdots,\hat{Y}_{n-1,c}^{\Delta,c}\mid\zeta_{pub}^{\Delta},\hat{Y}_{c,j}^{\Delta,j}),\quad j=1,2,\cdots,n-1 \tag{3}$$

其中，ζ_{pub}^{Δ} 表示节点 C 广播的全部 DOSS 值集合的量化版本，即 $\zeta_{pub}^{\Delta}=[S_{pub}^{\Delta}(1),\cdots,S_{pub}^{\Delta}(T)](S_{pub}(t)=[\delta_2(t),\delta_3(t),\cdots,\delta_{n-1}(t)])$。由上述分层结构构造的 Slepian-Wolf 编码可知，当 $T\to\infty$ 时，密钥误码率趋于 0。定义渐进群信息率为：

$$\begin{aligned}R_{star}&=\min_{1\leqslant j\leqslant n-1}\lim_{T\to\infty}\frac{1}{T}I([\hat{Y}_{1,c}^{\Delta,c},\cdots,\hat{Y}_{n-1,c}^{\Delta,c}];[\zeta_{pub}^{\Delta},\hat{Y}_{c,j}^{\Delta,j}])\\&=\lim_{T\to\infty}[R_{key}(T)-R_{bin}(T)]\end{aligned} \tag{4}$$

基于节点广播的信息以及自身的观察，窃听者具有边信息 $[\zeta_{pub}^{\Delta},\gamma^e]$，其中 $\gamma^e=[Y_{1,e}Y_{2,e},\cdots,Y_{1,e}]$（这里考虑窃听者对所有的 j 和 t 都有无噪的观察），令：

$$R_e=\lim_{T\to\infty}\frac{1}{T}I([\hat{Y}_{1,c}^{\Delta,c},\cdots,\hat{Y}_{n-1,c}^{\Delta,c}];[\zeta_{pub}^{\Delta},\gamma^e]) \tag{5}$$

由式(4)、式(5)可知，可实现的群密钥率为：

$$R_{star}^{sec}=R_{star}-R_e \tag{6}$$

后续计算的具体步骤[10]不再赘述，最后化简得：

$$R_{star}^{sec}=\log\left(1+\frac{1/(n-1)}{(1+\gamma_m^{-1})^2-1}\right) \tag{7}$$

4　基于中心节点的成对生成策略提取群密钥

4.1　协议步骤

由于利用 RSS 差分实现群密钥生成的方案要计算 $n-2$ 次 DOSS 值，再利用每个节点通过中心节点广播获得的上述 DOSS 计算全部 RSS 值并通过编码产生群密钥，实现过程略显繁琐，因此我们在拓扑结构中选取一个中心节点，提出在中

心节点处结合成对生成策略提取群密钥的方案。可以将协议步骤具体分为 4 步，依旧假设群内共有 n 个节点，每个群成员表示为 j，其中 $j=c,1,2,\cdots,n-1$。因为此处仅讨论协议的整体步骤，所以密钥生成过程所涉及的具体细节（如信道观察、量化、信息和解等过程）不再赘述。则有：

1）与差分提取方案类似，首先从 n 个节点中随机选取一个虚拟中心节点 C，分别与其他 $n-1$ 个节点组成一个类似于星型的无线网络拓扑结构，见图 1；

2）根据节点 C 与其他 $n-1$ 个节点相互间的信道测量 $\hat{Y}_{j,c}^{c}$ 和 $\hat{Y}_{c,j}^{j}$，利用基于 RSS 生成密钥的方案[3]分别产生 $n-1$ 个本地密钥 $K_1,K_2,\cdots,K_{n-1}$；

3）取上述 $n-1$ 个本地密钥中最短的 $K_{\min}=\min(K_1,K_2,\cdots,K_{n-1})$，记 $K_{\min}$ 的长度为 l，则节点 C 可以利用均匀分布从集合 $\{1,\cdots,2^l\}$ 中随机产生密钥串 K_g，很明显其长度由 $K_{\min}$ 决定；

4）节点 C 再将 K_g 通过一次一密系统[19]加密传输给其他 $n-1$ 个节点，至此，群内每个节点都会获得群密钥 K_g。

4.2 可实现群密钥率

由上述步骤可知，在利用信道观察分别产生 $n-1$ 个本地密钥后，中心节点 C 会依据本地密钥的最短长度，利用均匀分布随机产生密钥 K_g，随之通过一次一密的方式广播 K_g 以生成群密钥，所以群密钥的可实现密钥率应该与本地密钥的密钥率直接相关，而节点 C 与其他 $n-1$ 个节点中任一节点 j 所产生的本地密钥 K_j 的密钥率应为两节点间信道观察的互信息[20]：

$$\begin{aligned}C_j&=I(\hat{Y}_{j,c}^{c};\hat{Y}_{c,j}^{j})\\&=h(Y_{j,c}+W_{j,c}^{c})+h(Y_{j,c}+W_{j,c}^{j})-h(Y_{j,c}+W_{j,c}^{c},\\&\quad Y_{j,c}+W_{j,c}^{j})\end{aligned}\tag{8}$$

由于 $Y_{c,j}=Y_{j,c}$，因此通过计算 $\hat{Y}_{j,c}^{c}$ 和 $\hat{Y}_{c,j}^{j}$ 之间的协方差矩阵[21]可知：

$$|\kappa|=\sigma_Y^2\sigma_{W_c}^2+\sigma_Y^2\sigma_{W_j}^2+\sigma_{W_c}^2\sigma_{W_j}^2\tag{9}$$

因为 $W_{i,j}^{i}$ 的方差为 σ_W^2，将其和 $Y_{j,c}$ 的方差 σ_Y^2 代入，整理得：

$$C_j=\log\left(1+\frac{\gamma_m^2}{2\gamma_m+1}\right)\tag{10}$$

将产生本地密钥过程中公共讨论所交换的信息定义为 F，则由文献[11]可知，通过成对生成策略的方法能够使得窃听者在公共讨论阶段所获得的信息十分有限，即：

$$I(K_g;F)\leqslant\varepsilon\tag{11}$$

式(11)说明窃听者在整个密钥提取过程中很难窃听到密钥信息，因此整个群的可实现群密钥率为：

$$C=C_j=\log\left(1+\frac{\gamma_m^2}{2\gamma_m+1}\right)\tag{12}$$

4.3 两种方案群密钥率的对比

在该网络拓扑结构下，差分提取群密钥的方案能够达到的群密钥率已在前文给出。为了比较两种方案下各自群密钥率的大小，定义 $diff$ 为两者的差值，并对其进行化简，可得：

$$\begin{aligned}diff&=C-R_{star}^{sec}\\&=\log\left(1+\frac{\gamma_m^2}{2\gamma_m+1}\right)-\log\left(1+\frac{1/(n-1)}{(1+\gamma_m^{-1})^2-1}\right)\\&=\log\left(1+\frac{(n-2)\gamma_m^2}{(2\gamma_m+1)(n-1)+\gamma_m^2}\right)\end{aligned}\tag{13}$$

在式(13)中，当 $n=2$ 时（即群内仅有两个节点时），上述差值为 0，也即表明当群内节点数为 2 时，本文所提方案的群密钥容量与基于 RSS 差分提取群密钥的方案相同。当然，对差分提取群密钥的过程进行分析后也不难理解，当 $n=2$ 时，由于只有一个节点与中心节点相连，也就不会产生对应的 DOSS 值，因此并不需要向其他节点广播，那么窃听者就不会窃听到任何信息。故在星型拓扑结构中，此时仅需要利用两个节点自身的相互信道观察以产生密钥，这就与我们所提算法中生成本地密钥的想法完全一致，所以此时两种方案的可实现群密钥率会出现相同的情况。

但是当 $n>2$ 时，式(13)的计算结果显然大于 0。至此，我们从理论上证明了基于中心节点成对生成策略提取群密钥的方案在群密钥率方面优于差分提取方案。

式(7)和式(12)中的密钥容量都与信噪比 γ_m^2 有关，仿真比较两种方案在该拓扑结构下分别能够实现的群密钥容量。此处可以采取固定群内节点数 n 并观察密钥率与信噪比 γ_m^2 关系的方式，如图 3 所示。

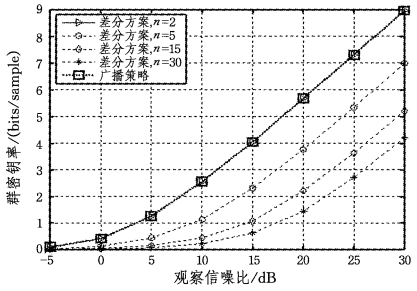

图 3 可实现群密钥率随信噪比 γ_m^2 变化的分析结果

从图 3 可以看出，随着信噪比 γ_m^2 的增加，两种方案的密钥率都呈现上升趋势，这是因为高信噪比会降低利用 RSS 值提取密钥的模糊性，进而提高群密钥的一致性；但是仔细比较两种方案的群密钥率曲线发现，我们的方案实现的密钥率显然更高，如之前理论分析部分提出的，当群内只有两个节点（$n=2$）时，两种方案的密钥容量是相等的，相应地，从图中可以看出两条线是重合的；但是随着节点数 n 的增加，差分提取群密钥的方案[10]所实现的密钥率会不断下降，表明群内节点数越多，越容易受到窃听者攻击，这是因为随着 n 的增加，在中继节点向群内其他节点广播 DOSS 值时，会暴露给窃听者更多的信道统计信息。

5 实现原型和复杂度分析

在本文提出的基于中心节点成对生成策略的群密钥提取算法中，由于采用了相同的星型无线网络拓扑结构，因此也可以继续使用文献[10]中所述的系统原型：一个中心节点和多个协作节点。本文中的中心节点的作用与文献[10]略有差异：1）向协作节点发送探针包以互相获得 RSS 测量值；2）利用现有的点对点密钥生成方案生成本地密钥；3）依据本地密钥的最短长度编码、广播产生群密钥。

我们的方案对探针包有一定的要求：其应包含发送节点 ID、包编号等，以至于流入节点能够分辨出不同节点的不同探针包。在中心节点分别发送和接收探针包后，提取其中的发送节点 ID 和包编号，获得了与对应协作节点间信道的 RSS 值后，可以利用现有的点对点密钥生成方案生成本地密钥。根据上述最短密钥的长度，利用均匀分布随机产生密钥，并通

过一次一密系统[18]加密传输给所有的协作节点。

通过分析可知，对于一个给定的时间元组，上述两方案的计算复杂度较低，都仅为 $O(n)$，这也就意味着对于给定的合法节点，两种算法都具有线性复杂度。但是对于所提方案，由于在产生群密钥之前，中心节点会分别与其他协作节点协商生成 $n-1$ 个本地密钥，因此会进行 $n-1$ 次单独的信息和解，所以这种方案会导致较长的时延，且时延的长短与群内节点数 n 呈正相关。同时，从密钥协商实现的复杂性角度来看，由于该方案需要进行多次单独的信息协商，导致本文方案的密钥协商实现的复杂性较高。由于在生成本地密钥阶段所提方案要进行 $n-1$ 次独立的信息协商，但差分方案仅需要一次最终的密钥协商，而其中任意一次信息协商过程受到攻击都会导致整个群密钥提取的崩溃，因此基于差分方案的群密钥提取[10]对攻击的健壮性显然更强。

结束语　本文针对星型无线网络拓扑结构，提出了一种基于中心节点成对生成策略的群密钥提取的方案，并给出了文献[10]中差分提取方案和本文所提方案的具体实施步骤，同时结合协议步骤理论分析了两者可实现的群密钥率。对群密钥率与差分提取群密钥方案进行了对比，当群内只有两个节点时，两者的可实现群密钥率是一致的，也从理论上分析了出现这种特殊情况的原因；但是当群内节点数至少为 3 时，所提方案的群密钥率明显更高。最后分析了两种方案的实现细节（如探针包的结构）和复杂度情况，分析表明两种方案都具有较低的线性复杂度，但是所提方案在产生本地密钥的过程中需要进行多次单独的信息协商，因此其复杂度较高，且对密钥提取过程中的攻击较为敏感。

参 考 文 献

[1] 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. ACM, 2007: 401-410.

[2] ZHANG J, DUONG T Q, MARSHALL A, et al. Key Generation From Wireless Channels: A Review[J]. IEEE Access, 2016, 4: 614-626.

[3] 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. ACM, 2009: 321-332.

[4] MATHUR S, TRAPPE W, MANDAYAM N, et al. Radio-telepathy: extracting a secret key from an unauhenticated wireless channel[C]// Proceedings of the 14th ACM International Conference on Mobile Computing and Networking. ACM, 2008: 128-139.

[5] SAYEED A, PERRING A. Secure wireless communications: Secret keys through multipath[C]// 2008 IEEE International Conference on Acoustics, Speech and Signal Processing. IEEE, 2008: 3013-3016.

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

[7] NITINAWARAT S, YE C, BARG A, et al. Secret key generation for a pairwise independent network model[J]. IEEE Transactions on Information Theory, 2010, 56(12): 6482-6489.

[8] YE C, REZNIK A. Group secret key generation algorithms[C]// 2007 IEEE International Symposium on Information Theory. IEEE, 2007: 2596-2600.

[9] KIM Y, PERRING A, TSUDIK G. Tree-based group key agreement[J]. ACM Transactions on Information and System Security (TISSEC), 2004, 7(1): 60-96.

[10] LIU H, WANG Y, CHEN Y, et al. Group Secret Key Generation via Received Signal Strength: Protocols, Achievable Rates, and Implementation[J]. IEEE Transactions on Mobile Computing, 2014, 13(12): 2820-2835.

[11] LAI L, HO S W. Key generation algorithms for pairwise independent networks based on graphical models[J]. IEEE Transactions on Information Theory, 2015, 61(9): 4828-4837.

[12] XU P, CUMANAN K, DING Z, et al. Group Secret Key Generation in Wireless Networks: Algorithms and Rate Optimization [J]. IEEE Transactions on Information Forensics and Security, 2016, 11(8): 1831-1846.

[13] THAI C D T, LEE J, QUEK T Q S. Secret group key generation in physical layer for mesh topology[C]// 2015 IEEE Global Communications Conference (GLOBECOM). IEEE, 2015: 1-6.

[14] WEI Y, ZHU C, NI J. Group Secret Key Generation Algorithm from Wireless Signal Strength[C]// Sixth International Conference on Internet Computing for Science and Engineering. IEEE Computer Society, 2012: 239-245.

[15] LAI L, HO S W. Simultaneously generating multiple keys and multi-commodity flow in networks[C]// Information Theory Workshop. IEEE, 2012: 627-631.

[16] CSISZAR I, NARAYAN P. Secrecy capacities for multiple terminals[J]. IEEE Transactions on Information Theory, 2004, 50(12): 3047-3061.

[17] TSE D, VISWANATH P. Fundamentals of wireless communication[M]. Cambridge university press, 2005.

[18] GOLDSMITH A. Wireless communications[M]. Cambridge university press, 2005.

[19] SHANNON C E. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28(4): 656-715.

[20] YE C, REZNIK A, SHAH Y. Extracting Secrecy from Jointly Gaussian Random Variables[C]// IEEE International Symposium on Information Theory. IEEE, 2006: 2593-2597.

[21] WILSON R, TSE D, SCHOLTZ R A. Channel Identification: Secret Sharing using Reciprocity in Ultrawideband Channels[C]// IEEE International Conference on Ultra-Wideband. IEEE, 2007: 270-275.