doi:10.11959/j.issn.1000-436x.2017047

协作干扰下的无线安全增强

张丽娟，刘志宏，张洪波，曾勇，马建峰
（西安电子科技大学网络信息安全学院，陕西 西安 710071）

摘 要：安全通信图（iS-Graph）的安全性能通过增加可控干扰以降低窃听者的信号与干扰比(SIR)来实现。研究无线网络中机密信息的传输，网络中合法节点在协作干扰节点的帮助下实现安全通信，在此基础上提出一种干扰协助的安全通信图，即 jS-Graph。同时，研究了 jS-Graph 的安全属性，提出使用多个独立的干扰节点来干扰窃听者。为应对窃听者靠近发送者或接收者的难题，使用一种协作干扰策略来干扰源节点或目标节点附近的窃听者。结果表明，如果采用协作干扰，无线通信的机密性得以增强。
关键词：协作干扰；随机几何；无线网络；安全图
中图分类号：TP309 **文献标识码**：A

Wireless secure enhancement with cooperative jamming

ZHANG Li-juan, LIU Zhi-hong, ZHANG Hong-bo, ZENG Yong, MA Jian-feng
(Institute of Network and Information Security, Xidian University, Xi'an 710071, China)

Abstract: Secrecy capacity of intrinsically secure communication graph (iS-Graph) can be increased by reducing the signal quality of eavesdroppers with adding controlled interferences. The transmission of secret messages over wireless channels in which the legitimate nodes were aided by cooperative jamming was studied, and a secure communication graph with jamming, jS-Graph was proposed. First, the security properties of jS-Graph was characterized. Then, jamming strategies to confuse eavesdroppers were proposed. To tackle the nearby eavesdropper problem, a two-stage cooperative jamming strategy to jam the eavesdroppers near the source or the destination was applied. The results demonstrate that, with the aid of cooperative jamming the secure communication graph can lead to secrecy gains. These results help to clarify how the presence of eavesdroppers and the cooperative jamming can influence secure connectivity in wireless networks.
Key words: cooperative jamming, stochastic geometry, wireless network, secrecy graph

1 引言

无线信道固有随机性和节点的空间位置可以在物理层为网络用户提供安全保障。为了分析由多个合法节点和多个窃听者节点组成的大规模网络，文献[1]从随机几何的视角提出安全图（secrecy graph）的概念，同时，文献[2,3]从信息论的角度对其进行描述，文献[4,5]研究了其标度律。

一般而言，机密性的提高有 2 种方式：提高合法接收者的信号质量（如通过缩短发送者和接收者的位置）；降低窃听者的信号质量（通过增加可控干扰）。此时干扰作为无线网络安全的有效资源，能够被合法用户使用来增加窃听者的噪声，提高安全通信速率。协作干扰在文献[6~8]中被称为人工噪声，目前，已提出一些相应的干扰策略，如基于高斯噪声[9]、高斯密码本[10]、基于格的结构化码本[11]等。协作干扰同时也可用于保护植入性医疗设备[12]、传感器网络[13]和其他无线网络[14,15]。

在文献[2]中，安全通信图（iS-Graph）描述大

收稿日期：2016-02-23；**修回日期**：2016-11-13
基金项目：国家重点研发计划基金资助项目（No.2016YFB0800601）；国家自然科学基金资助项目（No.U1405255）
Foundation Items: The National Key Research and Development Program (No.2016YFB0800601), The National Natural Science Foundation of China (No.U1405255)

规模无线网络中基于信息论安全性建立起来的安全链路。iS-Graph 是一个有向图 $G=\{\Phi_l, E\}$，其中，Φ_l 是合法节点集合，$E=\{\overrightarrow{x_i x_j}: R_s(x_i,x_j)>\gamma,\ x_i,\ x_j\in\Phi_l\}$ 为边集，γ 是设定的一个阈值，代表通信链路的最小安全速率（secrecy rate），$R_s(x_i,x_j)$ 可表示为

$$R_s(x_i,x_j)=\left[\mathrm{lb}\left(1+\frac{P_{ij}(x_i,x_j)}{\sigma_l^2}\right)-\mathrm{lb}\left(1+\frac{P_{ie^*}(x_i,e^*)}{\sigma_e^2}\right)\right]^+$$

其中，$[x]^+=\max\{x,0\}$，$P_{ij}(x_i,x_j)$ 是合法接收方 x_j 的接收能量，σ_l^2 和 σ_e^2 分别为合法节点和窃听者节点的噪声能量，且 $e^*=\arg\max_{e_k\in\Phi_e} P_{ik}(x_i,e_k)$（$\Phi_e$ 代表窃听者节点集）。γ=0 表明存在安全链路的特殊情形，对应于文献[2]提出的几何模型。

iS-Graph 假设是以网络中没有干扰节点为前提。如果一个窃听者离发送方较近，而接收者离发送方较远时，合法节点之间的秘密通信是不可能的。然而，在协作干扰的情况下，当发送方发送消息时，另一些合法节点会同时发送人工噪声来降低潜在窃听者的信号质量。因此，远离协作干扰节点的合法接收者仍然能够达到所需的信号质量。本文提出一个干扰协作的安全通信图（jS-Graph）。如图 1所示，A、B、C、D 是合法节点，X 是窃听者。iS-Graph 如图 1(a)所示，然而，如果合法节点 A 和 D 同时发送信息，则窃听者 X 不能得到从 A 到 B 或从 D 到 C 的任何消息(如图 1(b)所示)。另一种更复杂的情形如图 2 所示，与 iS-Graph 相比，jS-Graph 有更多边。

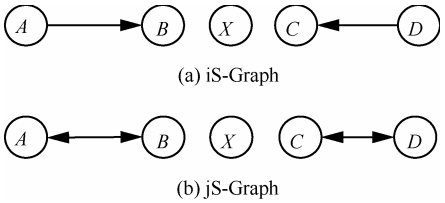


图 1 一个简单例子

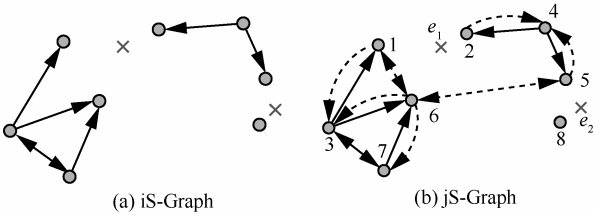


图 2 一个复杂例子

一般而言，如果干扰信号离窃听者近，离接收者远，那么协作干扰就可以提高链路的保密性能(secrecy capacity)。但是，不能将位于源节点和目标节点之间的所有窃听者都击败。本文利用一个分而治之的策略来解决这个问题，这个策略需要源节点产生一条由多个数据分组组成的信息，并且将每个数据分组独立发送。在每次传输中，需要干扰者发送人工噪声来降低一定区域内窃听者的信号质量，这样窃听者就会丢失一些数据分组，从而不能对信息进行解码。如文献[16,17]所述，处理源节点附近的窃听者仍然很困难，如果窃听者离源节点较远，就容易被干扰。为了解决附近窃听者问题，采用一个协作干扰策略来混淆源节点和目标节点附近的窃听者。

2 系统模型

令 $\Phi_l=\{x_i\}_{i=1}^{\infty}\subset\mathbb{R}^2$ 表示合法节点集，$\Phi_e=\{e\}_{i=1}^{\infty}\subset\mathbb{R}^2$ 表示窃听者节点集。设 Φ_l 和 Φ_e 中的节点分别服从密度为 λ 和 λ_E 的独立泊松点过程（PPP，Poisson point process)[18]。假设所有窃听者是静态的，相互之间独立操作。令 $B(x_i,r)$ 是以节点 x_i 为圆心、r 为半径的圆盘。那么 2 个节点 x_i 和 x_j 之间的欧几里得距离为 $d_{x_ix_j}=\|x_i-x_j\|$。

2.1 无线传播特性

如文献[16,19]所述，本文的无线信道衰减模型是基于路径损耗指数 $\alpha>2$ 的大尺度衰减。同时，假设满足以下几点。

1) 网络中所有合法节点和窃听者节点都备有一个全向天线。

2) 合法接收者和窃听者都不得使用任何多用户解码技术，并且将与当前传播同时发生的干扰视为噪声。

3) 网络是一个干扰受限系统。

最后假设将干扰视为噪声，当信噪比高于一个特殊的阈值时，就可以断定传输成功。

2.2 阈值模型

以文献[8]中的可用性和信息论安全为目标，采用阈值模型。节点 x_i 和节点 x_j 之间的 SIR 定义为

$$SIR_{ij}:=\frac{P_i l(x_i,x_j)}{\sum_{k\in\Phi_l,k\neq i,j}P_k l(x_k,x_j)} \tag{1}$$

节点 x_i 和窃听者节点 e 之间的 *SIR* 定义为

$$SIR_{ie} := \frac{P_i l(x_i,e)}{\sum_{k\in\Phi_l,k\neq i} P_k l(x_k,e)} \tag{2}$$

在窃听者节点 e 没有获取任何信息时，节点 x_i 和节点 x_j 之间的可信保密性能[1]为

$$C_{ij}(e) = \left[\text{lb}(1+SIR_{ij}) - \text{lb}(1+SIR_{ie})\right]^+ \tag{3}$$

节点 x_i 和节点 x_j 之间通信的最大保密性能与所有窃听者 Φ_e 相关，$C_{ij} = \min_{e\in\Phi_e} C_{ij}(e)$。

假设源节点 x_i 知道即时发生的合法接收节点 x_j 的接收信噪比 SIR_{ij}，那么源节点和目标节点就可以以相同的安全速率 R_{ij} 进行编码。如果即时的保密性能 C_{ij} 比目标安全速率 R_{ij} 高，那么通信就是安全的。

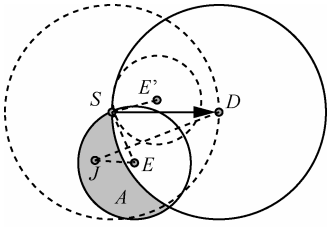
通过下面的方法可以构造 jS-Graph。对每一对节点 $x_i, x_j \in \Phi_l$，如果 C_{ij} 超过阈值 γ，可以得到一条由节点 x_i 指向节点 x_j 的有向边。jS-Graph 是一个有向图 $G(\gamma) := \{\Phi_l, E\}$，其中，$\Phi_l$ 为节点集，边集为 $E := \left\{\overrightarrow{x_i x_j} : C_{ij} > \gamma\right\}$，$\gamma$ 是任何 2 个节点之间安全通信的最小安全速率。在 $\gamma = 0$ 时，节点 x_i 到节点 x_j 的安全连接为 $G(0) := \{\Phi_l, E\}$，此时的边集为

$$E := \left\{\overrightarrow{x_i, x_j} : SIR_{ij} > SIR_{ie}, \forall e \in \Phi_e\right\}$$

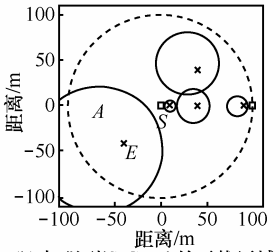
3　协助干扰下的安全通信图

当存在窃听者 E 时，为了使源节点 S 发出的信息能够被接收者 D 安全接收，需要使窃听者 E 的 SIR_{SE} 比接收者 D 的 SIR_{SD} 小很多。此外，需要使 $SIR_{SD} > \gamma_l$ 且 $SIR_{SE} < \gamma_e$，γ_e 可以任意小。

首先考虑一个简单的干扰策略。使源节点 S 和干扰节点 J 以相同的传播能量来传播信息，即 $P_S = P_J$。如图 3(a)所示，如果在阴影区域 A 中有一个干扰节点 J，合法节点 D 将不会被干扰，但窃听者会被混淆，因为 $d_{SD} < d_{JD}$ 且 $d_{JE} < d_{SE}$，这样，$SIR_{SD} = \frac{P_S d_{SD}^{-\alpha}}{P_J d_{JD}^{-\alpha}} > \frac{P_S}{P_J} > \frac{P_S d_{SE}^{-\alpha}}{P_J d_{JE}^{-\alpha}} = SIR_{SE}$。然而，任何干扰节点都不能位于 $B(D, d_{SD})$ 内，因为节点 J 的干扰信号将会覆盖源节点 S 的信号。因此，如果窃听者 E 位于 S 和 D 之间，如图 3(a)中的 E'，那么可用干扰区间就会减少。为了解决这个问题，可以调整干扰节点 J 的传输能量 P_J，使目标节点的 *SIR* 超过给定的阈值 γ_l，而窃听者节点的 *SIR* 小于给定的阈值 γ_e。



(a) jS-Graph的干扰区域A



(b) 加强型jS-Graph的干扰区域

图 3　干扰区域

令 $SIR_{SD} = \frac{P_S d_{SD}^{-\alpha}}{P_J d_{JD}^{-\alpha}} = \gamma_l$，$SIR_{SE} = \frac{P_S d_{SE}^{-\alpha}}{P_J d_{JE}^{-\alpha}} < \gamma_e$ 且 $0 < \gamma_e < \gamma_l$，下面 2 种情况成立。

1) 能量条件

$$\frac{P_S}{P_J} = \gamma_l \left(\frac{d_{SD}}{d_{JD}}\right)^{\alpha} \tag{4}$$

2) 位置条件

$$\left(\frac{d_{SD}}{d_{JD}}\right)^{\alpha} \left(\frac{d_{JE}}{d_{SE}}\right)^{\alpha} < \frac{\gamma_e}{\gamma_l} \tag{5}$$

源节点为 S，目标节点 D 位于位置$(R,0)$处。窃听者节点位于 (x_0, y_0) 处，一个满足条件的圆形区域 A 可以表示为

$$\left(x - \frac{x_0 - aR}{1-a}\right)^2 + \left(y - \frac{y_0}{1-a}\right)^2 = \frac{a[(x_0-R)^2 + y_0^2]}{(1-a)^2}$$

其中，$a = \frac{x_0^2 + y_0^2}{R^2}\left(\frac{\gamma_e}{\gamma_l}\right)^{\frac{2}{\alpha}}$。

如果一个满足式(4)的干扰节点位于此区域内，那么在 (x_0, y_0) 处的窃听者节点将达不到阈值 γ_e。图 3(b)展示的是不同位置窃听者的干扰区域（源节点位于(0,0)，目标节点位于(100,0)）。这种方式构建的安全图称为加强型 jS-Graph。图 4 展示

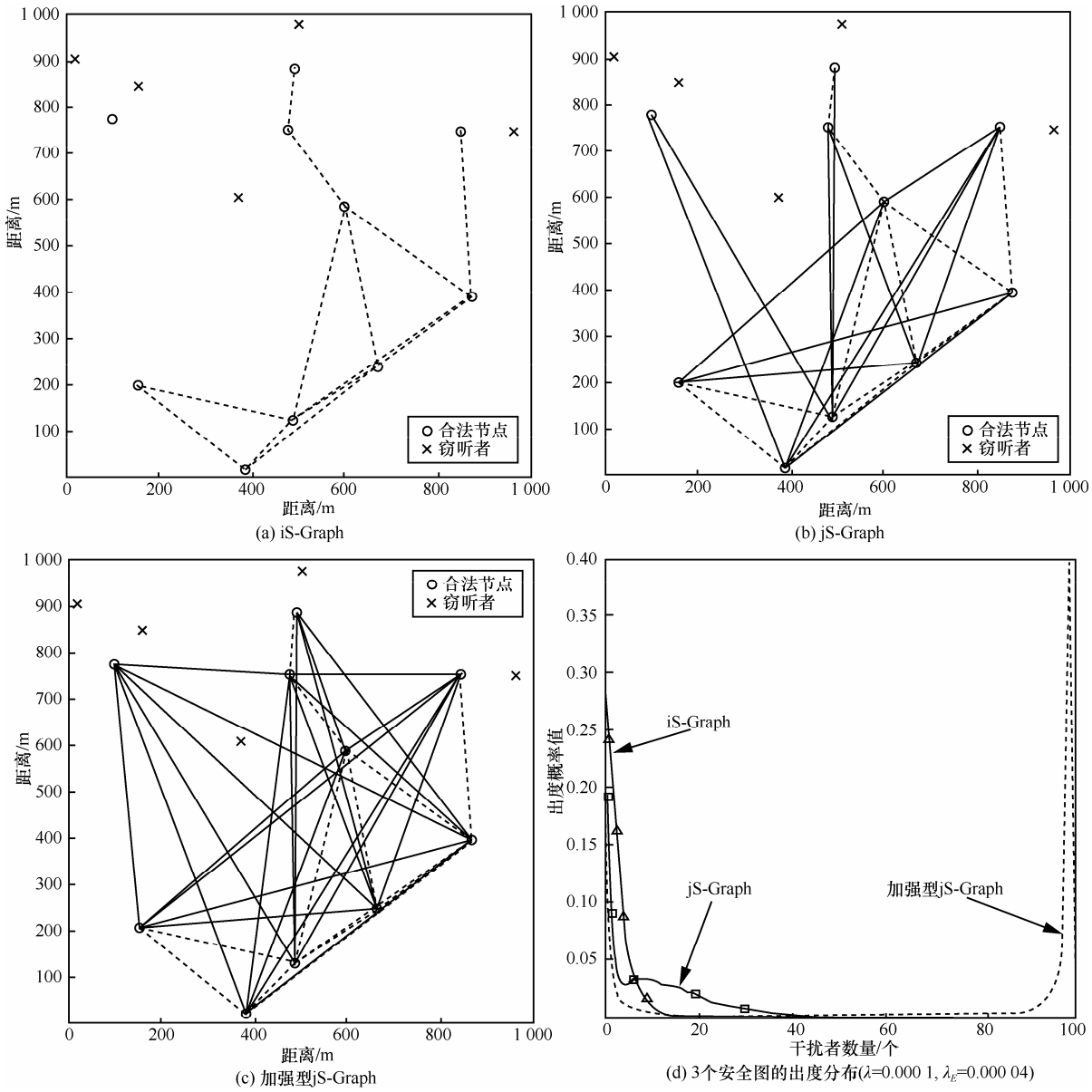


图 4　安全图例

iS-Graph、jS-Graph 以及相对应的加强型 jS-Graph。事实上，每一个节点的传输半径都是有限的。有能量限制的安全图如图 5 所示。

下面分析加强型 jS-Graph 的连通性。计算源节点 S 的出度，记为 d_{out}^{J}。在描述节点出度时首先假设在 $B(S,d_{SD})$ 中只有一个窃听者。

区域 $B(S,d_{SD})$ 中只有一个窃听者 E 时，平均出度 $\overline{d_{\text{out}}^{J}}$ 满足 $\mathbb{E}(\lambda\pi R_1^2)<\overline{d_{\text{out}}^{J}}<\mathbb{E}(\lambda\pi R_2^2)$，其中，$R_k(k=1,2,\cdots)$ 代表节点 S 与距离其 k 个长度的邻居窃听者的距离。根据文献[20]，在 $\mathbb{R}^m$ 上密度为 λ 的泊松点过程，某个节点和与其距离为 n 个长度的邻居节点之间的距离 R_n 服从广义伽马分布，在 2D 情况下，

$$f_{R_n}(r)=\mathrm{e}^{-\lambda\pi r^2}\frac{2(\lambda\pi r^2)^n}{r\Gamma(n)},\mathbb{E}(R_n^{\alpha})=\left(\frac{1}{\lambda\pi}\right)^{\frac{\alpha}{2}}\frac{\Gamma\left(n+\frac{\alpha}{2}\right)}{\Gamma(n)}$$

因此，$\mathbb{E}(R_1^2)=\dfrac{1}{\pi\lambda_E}$，$\mathbb{E}(R_2^2)=\dfrac{2}{\pi\lambda_E}$，且

$$\frac{\lambda}{\lambda_E}<\overline{d_{\text{out}}^{J}}<\frac{2\lambda}{\lambda_E}$$

为了更精确，令 X 为位于窃听者 E 的干扰区域 A 中的干扰节点数量，且窃听者 E 位于区域 S_A 中，那么 X 的分布为

$$\mathbb{P}\{X=k\}=\frac{(\lambda S_A)^k\mathrm{e}^{-\lambda S_A}}{k!},k=0,1,2,\cdots$$

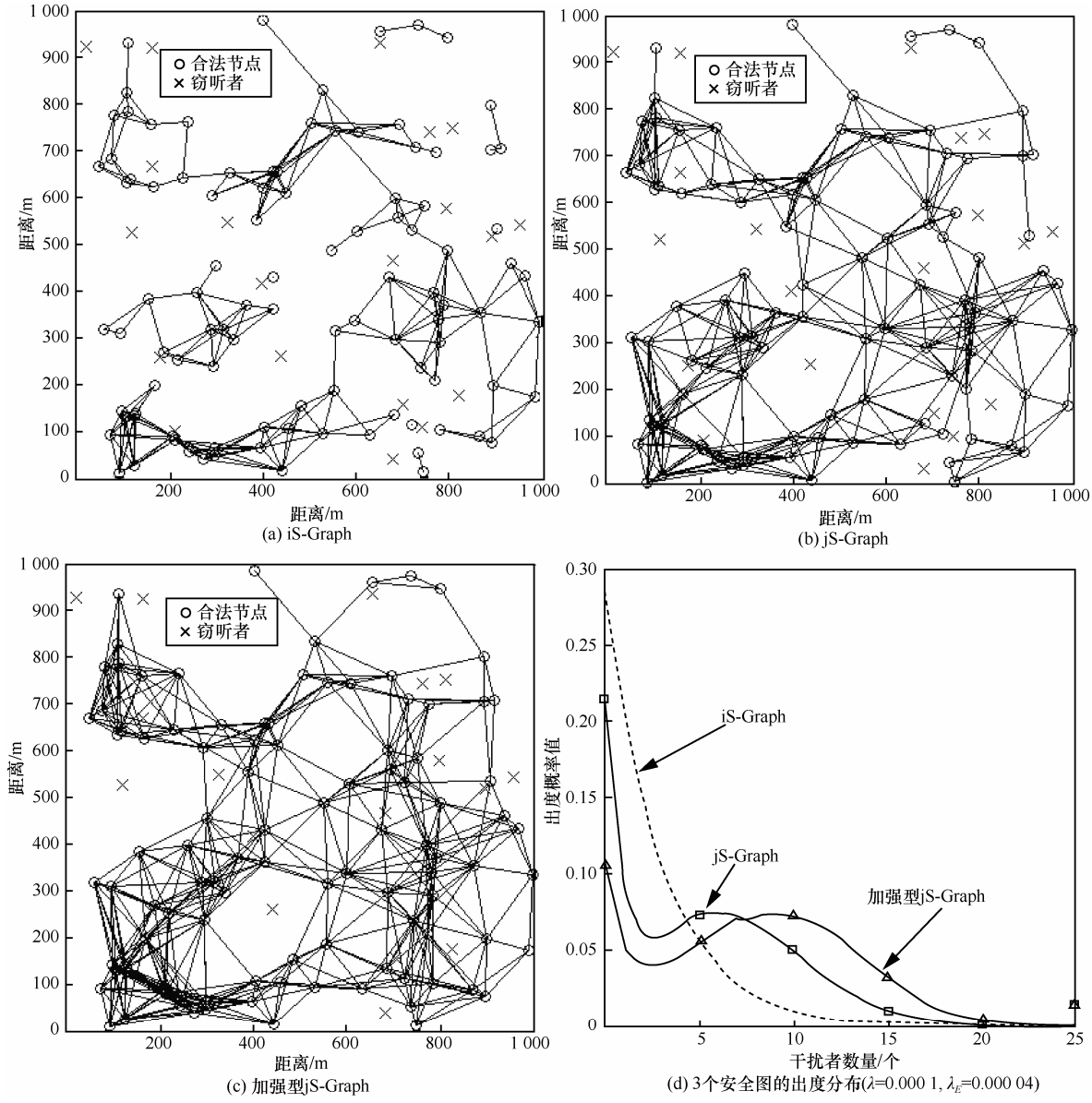


图 5　通信半径 $R<200$ m 的安全图例

因此，从 S 到 D 的安全链路的可能性 $\mathbb{P}\{\overrightarrow{SD}\}$ 是　　其中，

$\mathbb{P}\{\overrightarrow{SD}\}=1-\mathbb{P}\{X=0\}=1-\mathrm{e}^{-\lambda S_A}$，$d_{\mathrm{out}}^J$ 的分布为

$$\mathbb{P}\left\{d_{\mathrm{out}}^J=k\right\}=\binom{N}{k}\mathbb{P}\{\overrightarrow{SD}\}^k[1-\mathbb{P}\{\overrightarrow{SD}\}]^{N-k}$$

其中，$N=\lambda\pi R_2^2$，且平均出度 $\overline{d_{\mathrm{out}}^J}$ 为

$$\begin{aligned}\overline{d_{\mathrm{out}}^J}&=\mathbb{E}[N\mathbb{P}\{\overrightarrow{SD}\}]=\mathbb{E}[\lambda\pi R_2^2(1-\mathrm{e}^{-\lambda S_A})]\\&=\frac{2\lambda}{\lambda_E}-\lambda\pi\mathbb{E}[R_2^2\mathrm{e}^{-\lambda S_A}]\\&=\frac{2\lambda}{\lambda_E}-\lambda\pi\int_0^{\infty}\int_0^{r}\int_{-R}^{R}\int_{-\sqrt{R^2-x^2}}^{\sqrt{R^2-x^2}}r^2\mathrm{e}^{-\lambda S_A}f_{R_2}(r)\cdot\\&\quad f(R)f(x,y)\mathrm{d}y\mathrm{d}x\mathrm{d}R\mathrm{d}r\end{aligned}$$

$$S_A=\pi\frac{a[(x-R)^2+y^2]}{(1-a)^2}$$

$$a=\frac{x^2+y^2}{R^2}\left(\frac{\gamma_e}{\gamma_l}\right)^{\frac{2}{\alpha}}$$

$$f_{R_2}(r)=\mathrm{e}^{-\lambda\pi r^2}\frac{2(\lambda\pi r^2)^2}{r}$$

$$f(R)=\frac{2R}{r^2}$$

$$f(x,y)=\frac{1}{\pi r^2}$$

一般情况下，区域 $B(S,d_{SD})$ 中存在窃听者

$E_1,\cdots,E_p$，干扰者 $J_1\cdots J_k$ 来发送噪声，同时要满足

$$SIR_{SD}=\frac{P_S d_{SD}^{-\alpha}}{\sum_k P_{J_k} d_{J_k D}^{-\alpha}}\geqslant\gamma_l$$

$$SIR_{SE_i}=\frac{P_S d_{SE_i}^{-\alpha}}{\sum_k P_{J_k} d_{J_k E_i}^{-\alpha}}<\gamma_e, i=1,\cdots,p$$

其中，P_{J_k} 是干扰者 J_k 的发送功率。

给定 $E_1,\cdots,E_p$ 的位置，干扰能量最小化的优化问题可以表示为

$$\arg\min_{J_1\cdots J_k\in\Phi_1} P_{J_1}+\cdots+P_{J_k}$$
$$\text{s.t.}\quad SIR_{SD}\geqslant\gamma_l, SIR_{SE}<\gamma_e, i=1,\cdots,p$$

采用一个分而治之的方法来解决这个问题。具体来说，就是对一个信息产生多个数据分组，并且将其独立发送。当数据分组 m_i 发送时，可以选择 E_i 干扰区域中的合法节点发送噪声。如果每个窃听者丢失数据分组的一部分，那么链路 *S*-*D* 就是安全的。

运用上述策略可以得到 *S*-*D* 的安全链路并且获得加强型 jS-Graph，如图 4(c)和图 5(c)所示。图 4(d)和图 5(d)分别展示了通信半径有限制和没有限制时的 iS-Graph、jS-Graph 以及加强型 jS-Graph 的出度分布。

4　窃听者位置未知的干扰策略

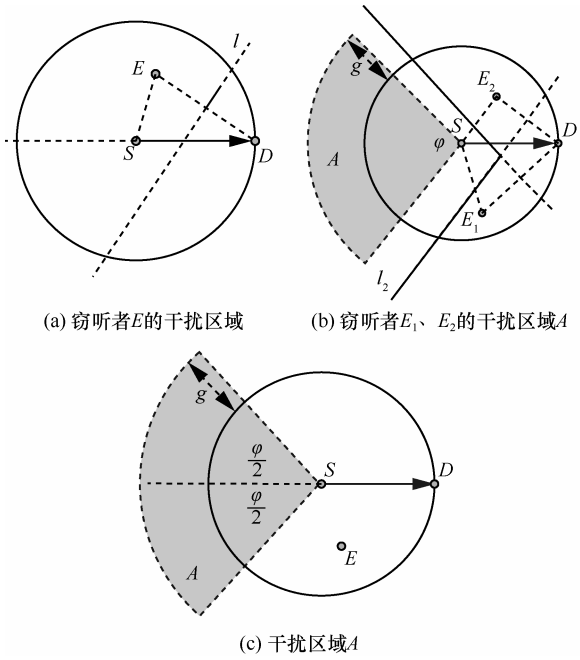
在第 3 节中，为了分析 jS-Graph 的连通性，假设窃听者的位置已知，实际上，窃听者位置是未知的。假设干扰信号始终以恒定功率 P_J 发射高斯白噪声，且 $P_S=P_J$，干扰信号可以根据其位置调整发送功率。

4.1　恒定功率干扰策略

源节点 *S* 和所有的干扰节点 *J* 以相同的发送功率发送信息，即 $P_S=P_J$。如图 6(a)所示，为了干扰窃听者节点 *E*，干扰节点应该位于 *l* 的左边，*l* 是 $\overline{ED}$ 的垂直平分线。

若在区域 $B(S,d_{SD})$ 中有 2 个窃听者节点 E_1 和 E_2，E_1 位于圆盘 $B(S,d_{SD})$ 的下半部分，E_2 位于圆盘 $B(S,d_{SD})$ 的上半部分，如图 6(b)所示，如果干扰节点位于线 l_1 和 l_2 的另一边（与合法节点 *D* 相反的方向），干扰就是有利的。l_1 和 l_2 分别是线 $\overline{E_1D}$ 和 $\overline{E_2D}$ 的垂直平分线。

如果有 *t* 个窃听者，可以画出 *t* 条垂直平分线 $l_1,\cdots,l_t$，干扰节点必须位于所有线的左边。假设选择了一个楔状区域（如图 6(c)）作为干扰区域，在这个区域中的节点将参与干扰。其中，φ 为干扰区域的夹角，g 为通信区域之外的干扰半径。给定 *t* 个窃听者，首先估计这个楔状区域的平均角度。然后，运用文献[18]中的 Campbell 定理计算干扰节点在接收者和窃听者处的聚集干扰 I_D 和 I_E。



(a) 窃听者*E*的干扰区域　(b) 窃听者E_1、E_2的干扰区域*A*

(c) 干扰区域*A*

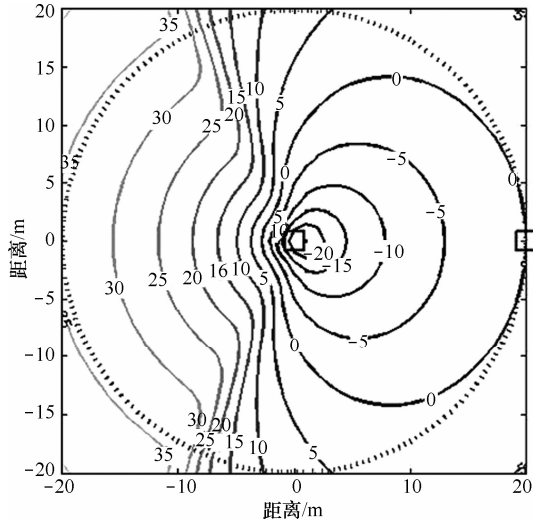
图 6　不同数量窃听者的干扰区域

干扰对安全增益的影响如图 7 所示，发送者和接收者的位置为(0,0)、(20,0)，P_S=P_J=30 dBm，*N*=0 dBm，α=4，图 7 中每一个点代表窃听者潜在的位置，对应的 ρ 值用 dB 表示。从图 7 中可以发现，如果窃听者 *E* 位于 *S* 和 *D* 的背面区域，*E* 就被干扰信号完全混淆。然而，要击败位于 *S* 和 *D* 之间的窃听者非常困难。此外，窃听者越多，安全增益越少。

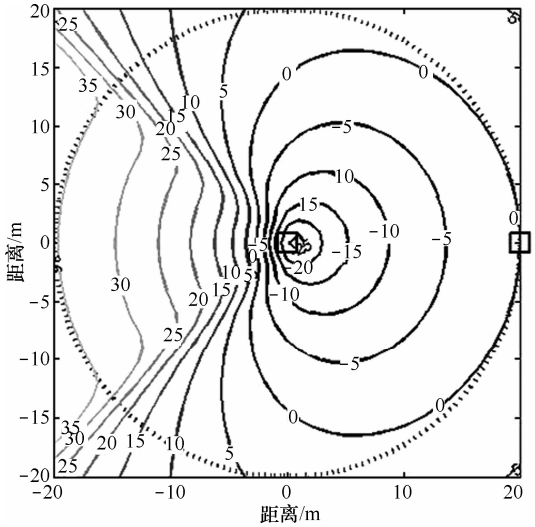
根据以上分析，提出一个简单的干扰策略。

给定发送者 *S* 和接收者 *D*，首先，*S* 向其邻居节点（1 跳或者 2 跳）逐个发送噪声。

对于 *S* 的每一个邻居节点 x_k，接收节点 *D* 记录相应的接收能量为 P_{kD}。然后，*D* 根据接收能量按升序对潜在干扰节点进行排序，获得潜在干扰节点的集合 $\{x_1,x_2,\cdots,x_k\}$。*D* 选择节点 x_1 作为干扰节点，然后添加干扰节点 x_2。对每一个新增加的干扰节点 x_p，接收者 *D* 计算 SIR_{SD}。如果 $SIR_{SD}>\gamma_l$，而下一个增加的干扰节点 x_{p+1} 使 $SIR_{SD}<\gamma_l$，那么就停止增加干扰节点。这样，目标节点 *D* 就获得了一个干扰节点集合 $J=\{x_1,x_2,\cdots,x_p\}$。当 *S* 向 *D* 发送信息时，在 *J* 中的节点就会发送噪声干扰窃听者。



(a) 2 个窃听者, $\lambda=1, g=20$



(b) 10 个窃听者, $\lambda=1,\ g=20$

图 7　干扰对安全增益的影响

上面提到的干扰策略没有使用干扰节点的任何位置信息，只考虑接收信号强度。

4.2　智能干扰策略

假设干扰节点的发送能量是可调节的。给定一对源节点和目标节点以及位置已知的窃听者，存在区域 A，使位于其中的能量为 $\frac{P_S}{P_J}=\gamma_l\left(\frac{d_{SD}}{d_{JD}}\right)^{\alpha}$ 的干扰节点能够成功干扰窃听者。区域 A 满足 $(\frac{d_{SD}}{d_{JD}})^{\alpha}(\frac{d_{JE}}{d_{SE}})^{\alpha}<\frac{\gamma_e}{\gamma_l}$。

如果 $B(S,d_{SD})$ 中有多个窃听者，上面的策略不能在同一时间击败所有窃听者。如果引入多个干扰者进行干扰，能量条件将难以满足，多个窃听者会产生更强的噪声。为了获得对抗窃听者的优势，可以对一个独立的消息产生多个数据分组，这种情况下，只有所有的分组被接收到，消息才可以解码，即使只有一个分组丢失，消息也不会被获取。这些数据分组被独立传输，每次传输中，根据能量情况选择不同的干扰节点产生不同的干扰信号，这样数据分组被依次发送到目标节点，但是对窃听者保密。因此，窃听者会丢失一些数据分组，不能对信息编码。

提出智能干扰策略如下。

1) 干扰节点的选择：源节点随机选择 t 个合法节点作为协作干扰节点 $J_1,J_2,\cdots,J_t$。

2) 干扰节点功率调整：对于干扰节点 $J_i,i=1,\cdots,t$，源节点 S 广播一个控制信号，干扰者 J_i 调整传输功率使目标节点 D 处的 SIR 至少达到 γ_l，即 $SIR_{SD}=\frac{P_S d_{SD}^{-\alpha}}{P_{J_i} d_{J_iD}^{-\alpha}}\geqslant\gamma_l$。

3) 数据分组的构造：对任意的源—目的节点对 S-D，令 M 是从源节点 S 发送到目标节点 D 的 b bit 信息。S 产生 t–1 个随机的 b bit 数据分组 $M_1,\cdots,M_{t-1}$，设置 M_t 使 $M=M_1\oplus M_2\oplus\cdots\oplus M_t$，“$\oplus$”代表比特位的异或操作。任何接收到所有 t 个数据分组的节点都可以计算 M，而丢失一个或多个数据分组的节点将不会得到 M 的信息。

4) 信息传输：源节点 S 的数据分组独立发送。当数据分组 M_i 发送时，干扰节点 J_i 会被激活，并发送随机噪声来干扰 J_i 附近潜在的窃听者，窃听者对应的传输能量为 P_{J_i}。

选择原点处的一个节点作为源节点 S，在$(R, 0)$处的节点作为目标节点 D。在 (x_i,y_i) 处的干扰节点 J_i 的干扰区域 A_i 满足式(5)，可以表示为

$$A_i:\left(x-\frac{x_0}{1-a}\right)^2+\left(y-\frac{y_0}{1-a}\right)^2=\frac{a(x_0^{\,2}+y_0^2)}{(1-a)^2}\quad(6)$$

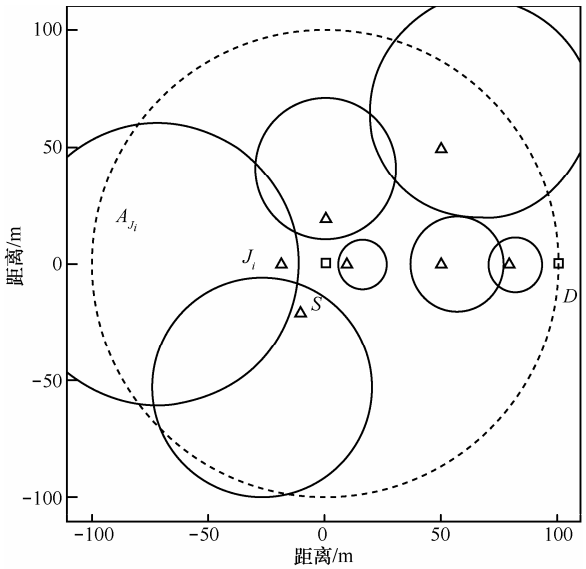
其中，$a=\frac{(x_0-R)^2+y_0^2}{R^2}\left(\frac{\gamma_e}{\gamma_l}\right)^{\frac{2}{\alpha}}$。图 8(a)展示了干扰者节点可以成功使位于区域 A_i 中窃听者 E_i 混淆，图 8(b)展示了干扰者的发送功率 P_J (用 dB 表示即 $\frac{P_J}{P_S}$)。

智能干扰策略中，如果干扰者 $J_1,J_2,\cdots,J_t$ 的干扰区域 $A_1,A_2,\cdots,A_t$ 完全将 $B(S,d_{SD})$ 覆盖，那么 S 到 D 之间的通信就是安全的。如图 8(a)所示，接近 S 或 D 的干扰节点 J_i 有很小的干扰区域 A_i，其中，

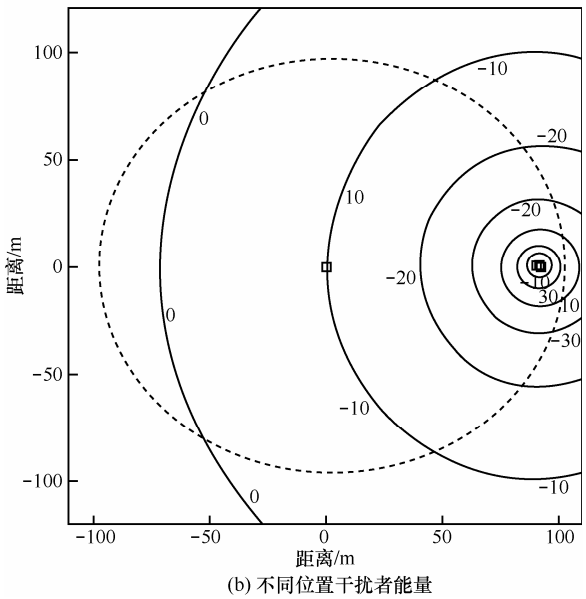
“△”为干扰者位置，“□”为源节点或目标节点所在的位置，下同。因此，对于通信节点对 *S-D* 来说，应该选择 *S* 或 *D* 附近更多节点作为干扰者。下面是一个干扰者选择方式。

对于源目的节点对 *S-D* 和位于 $B(S,d_{SD})$ 中的潜在窃听者 E_i，首先估计距离 $\hat{d}_{SD}$、$\hat{d}_{JS}$ 和 $\hat{d}_{JD}$。干扰者测量其与节点 *S* 和 *D* 之间的距离，然后发送给源节点 *S*。用这 3 个值，可以构建干扰区域的估计值为

$$\hat{S}_i=\frac{a(x_0^2+y_0^2)}{(1-a)^2}=\pi\left(\frac{\gamma_e}{\gamma_l}\right)^{\frac{2}{\alpha}}\frac{\hat{d}_{JD}^2}{\hat{d}_{SD}^2}\frac{\hat{d}_{JS}^2}{\left[1-\left(\frac{\gamma_e}{\gamma_l}\right)^{\frac{2}{\alpha}}\frac{\hat{d}_{JD}^2}{\hat{d}_{SD}^2}\right]^2}$$



(a) 干扰位置和干扰区域



(b) 不同位置干扰者能量

图 8 干扰位置与传输能量

假设 $B(S,d_{SD})$ 中有 *m* 个节点，源节点 *S* 选择 *t* 个干扰节点。每一个节点的估计值 $\hat{S}_1,\hat{S}_2,\cdots,\hat{S}_m$ 按照升序排列，那么源节点 *S* 按照如下概率来选择干扰节点：$\mathbb{P}$(节点 *i* 被选择为干扰者的概率)=$\min\left\{\frac{\hat{S}_{m+1-i}}{\sum\hat{S}}t,1\right\}$。利用这种方式，节点 *i* 的 $\hat{S}_i$ 越小，被选择为干扰者的概率越大。

下面分析智能干扰策略的安全连接的概率。给定点 (x_i,y_i) 处的窃听者 E_i，如在 A_{E_i} 内有至少一个干扰者 *J*，那么概率 $\mathbb{P}\{\exists\text{干扰者}|E_i\}=1-\mathrm{e}^{-\lambda S_{E_i}}$，$S_{E_i}$ 是区域 A_{E_i}，可以表示为

$$S_{E_i}=\pi\frac{a[(x_i-R)^2+y_i^2]}{(1-a)^2},a=\frac{x_i^2+y_i^2}{R^2}\left(\frac{\gamma_e}{\gamma_l}\right)^{\frac{2}{\alpha}} \tag{7}$$

假设 $B(S,d_{SD})$ 中有窃听者 $E_1,E_2,\cdots,E_p$，链路 *S-D* 安全连接的概率为 $P_c=[1-\mathrm{e}^{-\lambda S_{E_1}}]\cdots[1-\mathrm{e}^{-\lambda S_{E_p}}]=\prod_{E_i\in\mathbb{B}}[1-\mathrm{e}^{-\lambda S_{E_i}}]$。

对于服从泊松点过程的 *X*，其生成函数为 $G(v)=\mathbb{E}_{X\in\phi_E}[\prod v(x)]==\exp\left(-\int_{\mathbb{R}^d}(1-v(x))\wedge(\mathrm{d}x)\right)$。因此，安全连接概率的期望为

$$\mathbb{E}(P_c)=\mathbb{E}\left[\prod_{E_i\in\mathbb{B}}[1-\mathrm{e}^{-\lambda S_{E_i}}]\right]=\exp\left(-\int_{\mathbb{B}}\mathrm{e}^{-\lambda S_{E_i}}\lambda_E\mathrm{d}E_i\right) \tag{8}$$

通过上面的分析可知，给定 λ、λ_E，如果 $Q=\lambda_E\int_{\mathbb{B}}\mathrm{e}^{-\lambda S_{E_i}}\mathrm{d}E_i\to 0$，那么 $\mathbb{E}(P_c)$ 接近于 1。

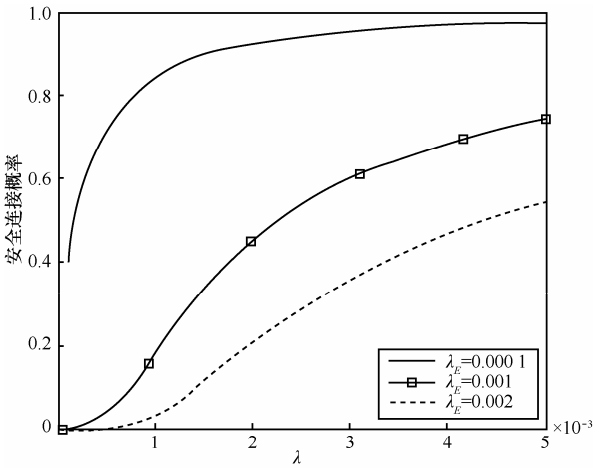
图 9(a)展示安全连接概率和 λ 的关系，其中 $R=100\text{ m},\alpha=4,\gamma_e=1,\gamma_l=2$。给定 λ，λ_E 越高，安全连接概率越低。当 *R* 足够大时，有 $\frac{R^2[(x-R)^2+y^2]}{[R^2-\gamma(x^2+y^2)]^2}\to 1$，即 $S_{E_i}\approx\pi\gamma(x^2+y^2)$，式(8)演变为

$$\begin{aligned}\mathbb{E}(P_c)&=\exp\left(-\int_{\mathbb{B}}\lambda_E\mathrm{e}^{-\lambda S_{E_i}}\mathrm{d}E_i\right)\\&\approx\exp\left(-\int_{\mathbb{B}}\lambda_E\mathrm{e}^{-\lambda\pi\gamma(x^2+y^2)}\mathrm{d}E_i\right)\\&=\exp\left(-\frac{1}{\gamma}\cdot\frac{\lambda_E}{\lambda}(1-\mathrm{e}^{-\pi\gamma\lambda R^2})\right)\end{aligned}$$

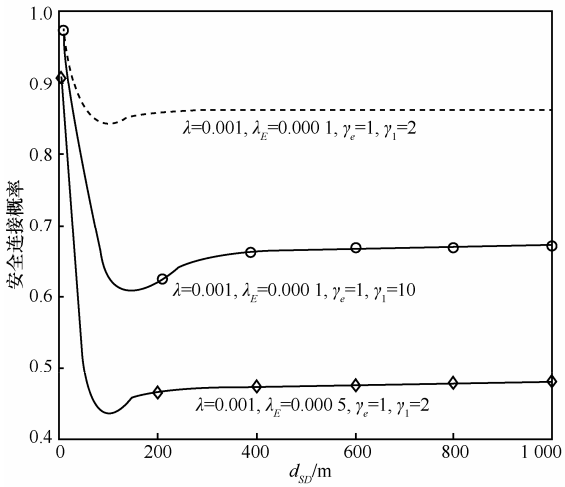
当 $R^2\gg\frac{1}{\pi\gamma\lambda},\mathrm{e}^{-\pi\gamma\lambda R^2}\to 0$

$$\mathbb{E}(P_c) \approx \exp\left(-\frac{1}{\gamma}\frac{\lambda_E}{\lambda}\right) = \exp\left[-\left(\frac{\gamma_l}{\gamma_e}\right)^{\frac{2}{\alpha}}\frac{\lambda_E}{\lambda}\right] \quad (9)$$

图 9(b)描述安全连接概率与 d_{SD} 的关系，当 d_{SD} 增大时，安全连接概率首先减少，达到一个接近于式(9)计算的值，然后慢慢增加到其上限值。当 R 足够大，且 $\lambda > \lambda_E\left(\frac{\gamma_l}{\gamma_e}\right)^{\frac{2}{\alpha}}$ 时，$\left(\frac{\gamma_l}{\gamma_e}\right)^{\frac{2}{\alpha}}\frac{\lambda_E}{\lambda} \to 0$，安全连接概率接近于 1。



(a) 安全连接概率和λ的关系

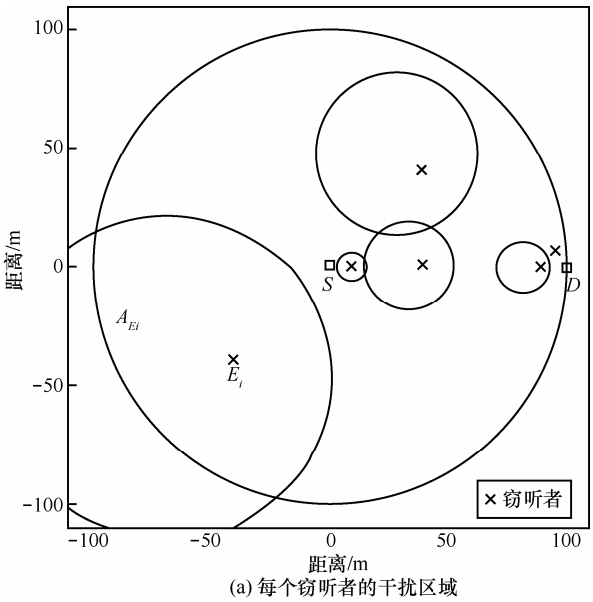


(b) 安全连接概率和d_{SD}的关系

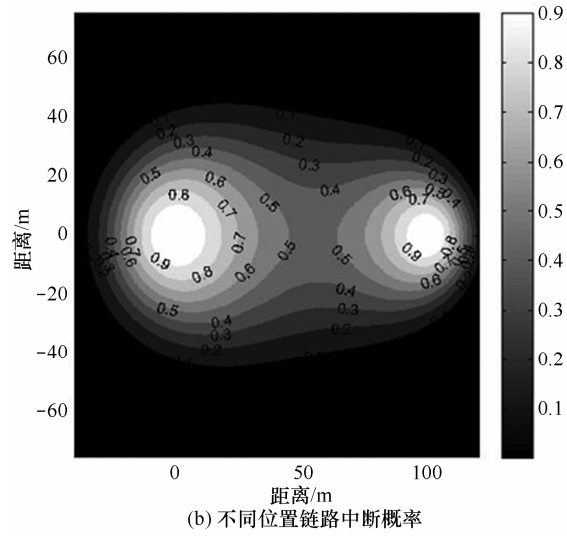
图 9　安全连接概率

5　邻近窃听者问题

如上所述，只有离源节点较近，离目标节点较远的合法节点才可以作为干扰节点，如图 7 所示。图 10 也描述了邻近窃听者问题的场景。文献[21]利用网络编码来解决邻近窃听者问题。然而，当窃听者离源节点很近时，这个策略的保密性将会降低。



(a) 每个窃听者的干扰区域



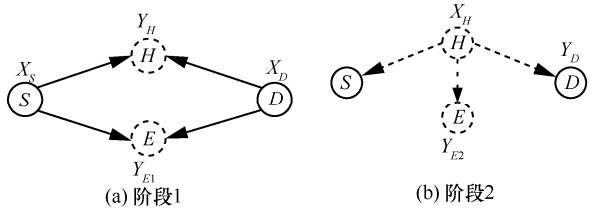
(b) 不同位置链路中断概率

图 10　邻近窃听者问题的场景

Lai 等[22]展示了反馈的正确使用能够加强信道的保密性能。干扰策略中，借助目标节点的协助和中继节点的转发，可以获得较好的安全速率，也可以解决邻近窃听者问题。

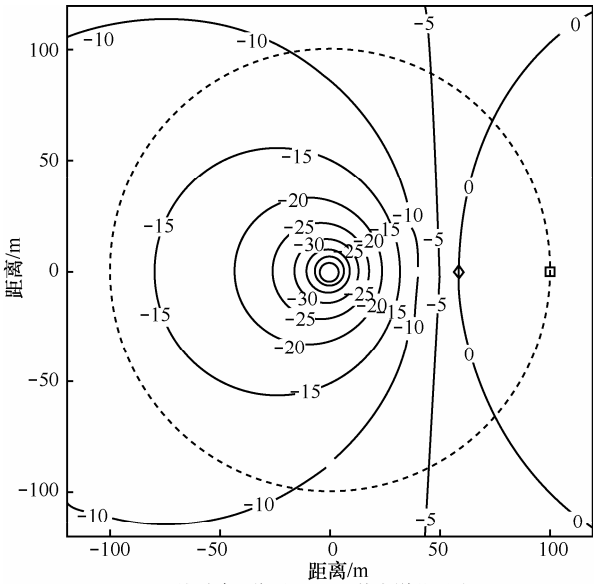
系统模型如图 11 所示。通信在中继节点 H 的协助下进行，由 2 个阶段组成。在第一阶段中，如图 11(a)所示，源节点 S 发送信号 X_S。同一时间，目标节点 D 发送干扰信号 X_D 来混淆窃听者。阶段 1，中继节点 H 接收到的信号是 Y_H。阶段 2，如图 11(b)所示，中继节点 H 发送信号 X_H，X_H 是接收信号经过计算得到的结果。如中继节点转发阶段 1 接收的噪声信号的加权版本（放大转发），即 $X_H = \beta Y_H$，其中，β 是中继节点的放大系数。目标节点 D 在阶段 1 中作为干扰信号 X_D 的发送者，能够取消干扰，但是窃听者不能。

不同位置 2 个阶段干扰策略如图 12 所示。

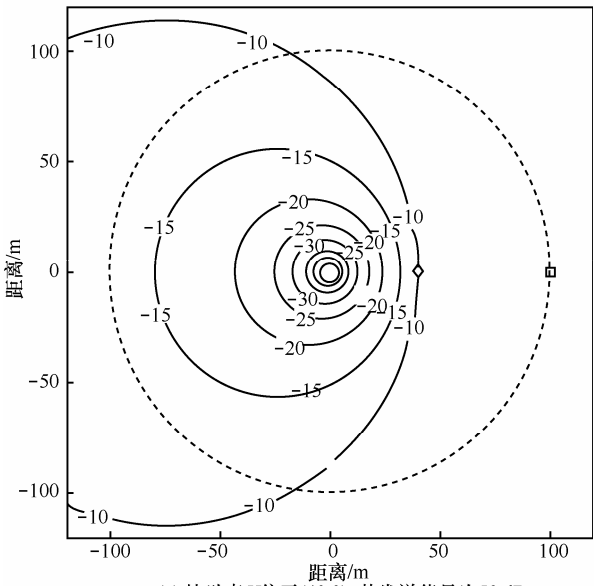


(a) 阶段1　　(b) 阶段2

图 11　2 个阶段协作干扰



(a) 协助者H位于(60, 0), 其发送能量为50 dB



(a) 协助者H位于(40,0), 其发送能量为50 dB

图 12　不同位置 2 个阶段干扰策略

对于窃听者 E 来说，

$$SIR_{SE}^{(1)}=\frac{P_S d_{SE}^{-\alpha}}{P_D d_{DE}^{-\alpha}},SIR_{SE}^{(2)}=\frac{(P_S d_{SH}^{-\alpha})\beta d_{HE}^{-\alpha}}{(P_D d_{DH}^{-\alpha})\beta d_{HE}^{-\alpha}}=\frac{P_S d_{SH}^{-\alpha}}{P_D d_{DH}^{-\alpha}}$$

其中，$\beta=\dfrac{P_H}{P_S d_{SH}^{-\alpha}+P_D d_{DH}^{-\alpha}}$。因此，窃听者可以获得

$$\begin{aligned}SIR_{SE}&=\max\{SIR_{SE}^{(1)},SIR_{SE}^{(2)}\}\\&=\max\left(\frac{d_{DE}}{d_{SE}},\frac{d_{DH}}{d_{SH}}\right)^{\alpha}\frac{P_S}{P_D}<\gamma_e\end{aligned}$$

对目标节点 D，令 N 为噪声，$P_S=P_D$，有

$$\begin{aligned}SIR_{SD}&=\frac{(P_S d_{SH}^{-\alpha})^{\beta}d_{HD}^{-\alpha}}{N}=\frac{\dfrac{P_H}{N}}{d_{HD}^{\alpha}+d_{SH}^{\alpha}\left(\dfrac{P_D}{P_S}\right)}\\&=\frac{\dfrac{P_H}{N}}{d_{HD}^{\alpha}+d_{SH}^{\alpha}}>\gamma_t\end{aligned}$$

数值结果如图 13 所示。为了击败目标节点附近的窃听者，中继节点 H 应该满足以下条件。

1) 连接条件

$$A:\ \frac{\dfrac{P_H}{N}}{d_{HD}^{\alpha}+d_{SH}^{\alpha}}>\gamma_t$$

2) 安全条件

$$B:\ \left(\frac{d_{DH}}{d_{SH}}\right)^{\alpha}<\gamma_e$$

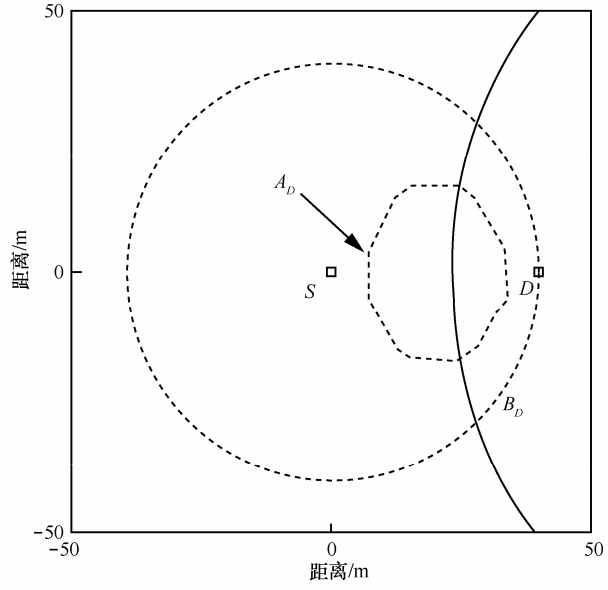
图 13 展示中继节点 H 满足 2 种情况。中继节点 H 位于区域 A 中，给定 H 的位置和 P_H，当 P_H 增大时，区域 A 增大。

上面的策略可以混淆目标节点附近的窃听者，但不能保证源节点附近窃听者的模糊性。为了解决这个问题，使用 2 次两级干扰策略。第 1 轮，使用两级干扰策略，目标节点发送给源节点一个随机数 n_D，在第 2 轮，源节点 S 计算 $n_S=Message\oplus n_D$ 并使用两级干扰策略发送给 D。D 就可以得到 $Message=n_S\oplus n_D$。如果窃听者接近 S，得不到 n_D；如果接近 D，会丢失 n_S。因此，S 到 D 的通信是安全的。

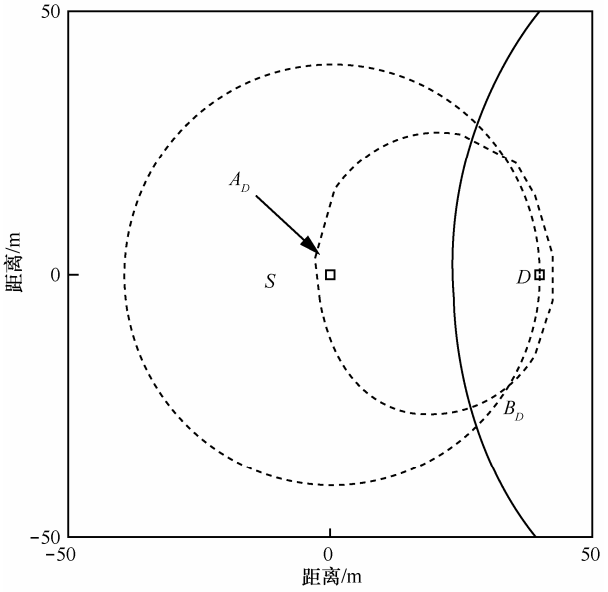
对窃听者 E，如果使用中继节点 H 在节点 S 和 D 的 2 个方向上通信，需满足

$$\min\{SIR_{SE},SIR_{DE}\}=\max\left\{\frac{d_{DH}}{d_{SH}},\frac{d_{SH}}{d_{DH}}\right\}^{\alpha}<\gamma_e$$

此时窃听者不能获得任何信息。如果中继节点位于 S-D 的中点，它能够以最小能量转发信息，此时，$\dfrac{P_H}{N}=\gamma_t(d_{HD}^{\alpha}+d_{SH}^{\alpha})$ 达到最小值。



(a) P_H=56 dBm的干扰区域



(b) P_H=59 dBm的干扰区域

图 13　满足连接和安全情形两级干扰策略，源节点和目标节点分别位于(0,0)和(40,0), $\alpha=3,\gamma_e=-3$ dB, $\gamma_l=10$ dB

当 $0<\gamma_e<1$ 时，需要 2 个中继节点，第 1 轮，从 S 到 D 时中继节点 H_{SD} 需满足 $G:\left(\dfrac{d_{DH_{SD}}}{d_{SH_{SD}}}\right)^{\alpha}<\gamma_e$。如果窃听者位于区域 G 中，则满足安全情况。如果有很多潜在节点作为中继节点，最优中继节点 H_{SD}^{*} 应满足

$$H_{SD}^{*}=\arg\min_{H_i\in\Phi_l}\left\{d_{DH_i}^{\alpha}+d_{SH_i}^{\alpha}\right\}$$

$$\text{s.t.}\quad \left(\frac{d_{DH_i}}{d_{SH_i}}\right)<\gamma_e,i=1,\cdots,m$$

使用同样的方式在第 2 轮找一个靠近 S 的中继节点 H_{DS}。

从上面的分析可知，两级干扰策略能够混淆在源节点或目标节点处的窃听者。然而，当窃听者位于两者之间时，能够获取一些信息。如图 14(a)所示，在干扰区域和 2 个中继节点之间有间隙。为了击败这些窃听者，可以结合两级干扰和智能干扰策略。

下面介绍协作干扰策略。

1) 干扰节点选择和能量调整：源节点随机或根据其他策略选择 t 个合法节点作为协作干扰节点 $J_1,J_2,\cdots,J_t$。对任何一个干扰节点 $J_i,i=1,\cdots,t$，源节点广播一个控制信号，干扰者 J_i 调整传输功率 P_{J_i} 使目标节点 D 处的 SIR 至少达到 γ_l。即 $SIR_{SD}=\dfrac{P_S d_{SD}^{-\alpha}}{P_{J_i} d_{J_iD}^{-\alpha}}\geqslant\gamma_l$。

2) 中继节点选择：选择 2 个中继节点，H_{SD} 对 S 到 D 的传输进行协助，H_{DS} 对 D 到 S 的传输进行协助。

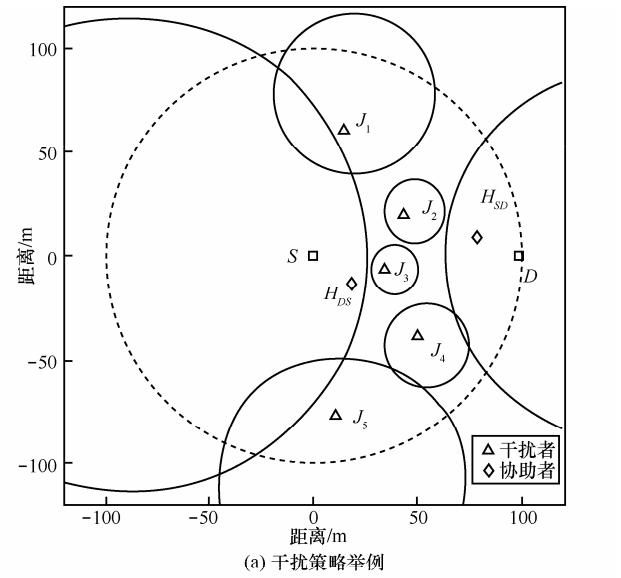
3) D 到 S 的传输：目标节点 D 随机选择信息 M_D，在 H_{DS} 的协助下利用 2 种方式的干扰策略将信息发送给 S。

4) S 到 D 的传输：目标节点 S 随机选择信息 M_S，在 H_{SD} 的协助下利用 2 种方式的干扰策略将信息发送给 D。

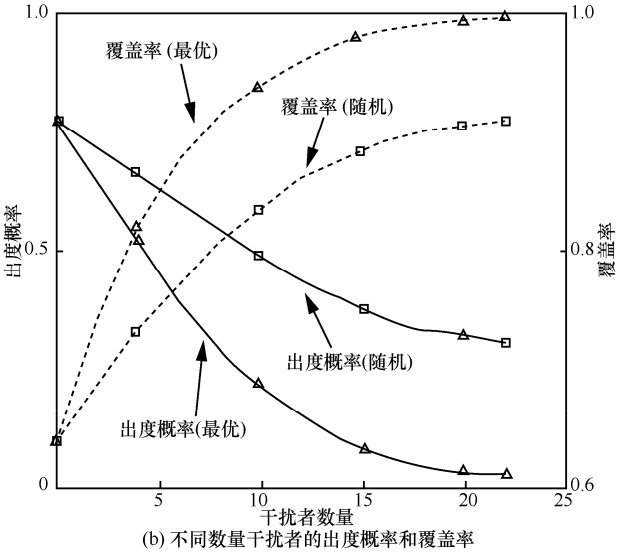
5) 数据分组的构建：令 M 为从源节点 S 发送到目标节点 D 的 b bit 信息。S 产生 t−1 个随机的 b bit 数据分组 $M_1,\cdots,M_{t-1}$，然后设置 M_t 使 $M=M_1\oplus M_2\oplus\cdots\oplus M_t$，“⊕”代表比特位的异或操作。任何接收到所有 t+2 个数据分组的节点都可以计算 M，而丢失一个或多个数据分组的节点将不会得到 M 的信息。

6) 信息传输：在这一步中，源节点 S 的数据分组会独立发送。当数据分组 M_i 发送时，干扰节点 J_i 会被激活，并发送随机噪声来干扰附近潜在的窃听者。

有 2 种方式选择干扰节点 $J_1,J_2,\cdots,J_t$。一种是在 $B(S,d_{SD})$ 中随机选择 t 个节点。如图 14(a)所示，中继节点 H_{SD} 和 H_{DS} 能够干扰 S 和 D 的附近的窃听者，唯一能够被窃听到的区域就是 S 和 D 的中间位置。因此，最好的方式就是选择位于 S 和 D 之间的节点为干扰节点。



(a) 干扰策略举例



(b) 不同数量干扰者的出度概率和覆盖率

图 14　协作干扰举例（源节点和目标节点位于(0,0)和(100,0), $\gamma_e=-7\,\text{dB},\ \alpha=3,\gamma_l=3\,\text{dB},\lambda=0.001,\lambda_E=0.0001$）

对于节点对 *S-D* 和 $B(S,d_{SD})$ 中的潜在窃听者 J_i，干扰者测量其到 S 和 D 的距离，并将距离信息发送给源节点。根据估计值 $\hat{d}_{SJ_i}$、$\hat{d}_{DJ_i}$ 可以构建干扰者 J_i 的估计值为

$$\eta_i=\begin{cases}\dfrac{\hat{d}_{SJ_i}}{\hat{d}_{DJ_i}},\ \hat{d}_{SJ_i}\geqslant\hat{d}_{DJ_i}\\ \dfrac{\hat{d}_{DJ_i}}{\hat{d}_{SJ_i}},\ \hat{d}_{SJ_i}<\hat{d}_{DJ_i}\end{cases}\tag{10}$$

假设 $B(S,d_{SD})$ 中有 m 个节点，每一个节点的估计值 η_i 升序排列为 $\eta_1,\eta_2,\cdots,\eta_m$，源节点选择前 t 个作为干扰者。利用这种方式，接近 *S-D* 中点的节点 i 有很高的概率被选为干扰者。

为了评估协作干扰策略的效率，在不同的场景下实验。由图 14(b)可知，随着干扰者数量增加，$B(S,d_{SD})$ 中覆盖的区域和中继节点的数量也相应增加，因此，安全性增强，如中断概率减少。另外，最优干扰者选择策略的性能优于随机干扰者选择策略。通过实验，验证了提出的协作干扰策略能够提高系统机密性。

6　结束语

对于增强无线网络的安全性来说，协作干扰是一个强有力的工具。与没有干扰协助的 iS-Graph 相比，有干扰协助的安全通信图 jS-Graph 能够获得更好的保密性。为了混淆源节点或目标节点处的窃听者，可以使用两级干扰策略。为了提高不同空间结构的干扰效率，仍然有许多工作要做。一种情况就是目标节点有很多可信任的邻居节点能够共享密钥。这些节点能够参与干扰，干扰信号通过加密安全信道被发送到目标节点，因此，目标节点能够取消干扰。还有一种情况就是使用基于编码设计的更加复杂的干扰策略。

参考文献：

[1] PINTO P C, BARROS J O, WIN M Z. Secure communication in stochastic wireless networks-part I: connectivity[J]. IEEE Trans Inf Forensics Security, 2011,7(1):125-138.

[2] HAENGGI M. The secrecy graph and some of its properties[C]//ISIT. 2008: 539-543.

[3] PINTO P C, BARROS J O, WIN M Z. Secure communication in stochastic wireless networks - part ii: maximum rate and collusion[J]. IEEE Trans Inf Forensics Security, 2011, 7(1):139-147.

[4] GOEL S, AGGARWAL V, YENER A, et al. The effect of eavesdroppers on network connectivity: a secrecy graph approach[J]. IEEE Trans Inf Forensics Security, 2011, 6(3):712-724.

[5] PINTO P C, WIN M Z. Percolation and connectivity in the intrinsically secure communications graph[J]. IEEE Trans Inf Theory, 2012, 58(3):1716-1730.

[6] VILELA J P, BLOCH M, BARROS J, et al. Wireless secrecy regions with friendly jamming[J]. IEEE Trans Inf Forensics and Security, 2011, 6(2):256-266.

[7] GOEL S, NEGI R. Guaranteeing secrecy using artificial noise[J]. IEEE Trans Wireless Communications, 2008, 7(6):2180-2189.

[8] GOECKEL D, VASUDEVAN S, TOWSLEY D, et al. Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks[J]. IEEE J Select Areas Commun, 2011, 29(10): 2067-2076.

[9] LAI L, GAMAL H E. The relay-eavesdropper channel: cooperation for secrecy[J]. IEEE Trans Inf Theory, 2008,54(9):4005-4019.

[10] TEKIN E, YENER A. The general Gaussian multiple-access and two-way wire-tap channels: achievable rates and cooperative jamming[J]. IEEE Trans. Inf. Theory, 2008, 54(6):2735-2751.

[11] HE X, YENER A. Securing wireless communications at the physical layer, chapter cooperative jamming: the tale of friendly interference for secrecy[M]. New York: Springer, 2009: 65-88.

[12] GOLLAKOTA S, HASSANIEH H, RANSFORD B, et al. They can hear your heartbeats: non-invasive security for implantable medical devices[C]//In ACM SIGCOMM, 2011:2-13.

[13] MARTINOVIC I, PICHOTA P, SCHMITT J B. Jamming for good: a fresh approach to authentic communication in WSNs[C]//ACM WiSec. 2009:161-168.

[14] WILHELM M, MARTINOVIC I, SCHMITT J, et al. WiFire: a firewall for wireless networks[C]//In ACM SIGCOMM. New York, NY, USA, 2011:456-457.

[15] BERGER D S, GRINGOLI F, FACCHI N, et al. Gaining insight on friendly jamming in a real-world IEEE 802.11 network[C]//ACM WiSec'14, 2014: 23-25.

[16] AGATAY C, APAR C, GOECKEL D, et al. Secret communication in large wireless networks without eavesdropper location information[C]//Proc INFOCOM. 2012: 1152-1160.

[17] KOYLUOGLU O, KOKSAL C, GAMAL H E. On the secrecy capacity scaling in wireless networks[J]. IEEE Trans Inf Theory, 2012, 58(11):3000-3015.

[18] CHIU S N, STOYAN D, KENDALL W S, et al. Stochastic geometry and its applications, third edition[M]. John Wiley & Sons, Ltd, 2013.

[19] HAN B, LI J. Secrecy capacity maximization for secure cooperative ad-hoc networks[C]//In INFOCOM, 2013 Proceedings IEEE, 2013: 2796-2804.

[20] HAENGGI M. On distances in uniformly random networks[J]. IEEE Trans Inf Theory, 2005, 51(10):3584-3586.

[21] GOECKEL D, CAPAR C, TOWSLEY D. Physical layer security in wireless communications, chapter physical layer secrecy in large multihop wireless networks[M]. CRC Press, 2014: 271-285.

[22] LAI L, GAMAL H E, POOR H V. The wiretap channel with feedback: encryption over the channel[J]. IEEE Trans Inf Theory, 2008,54(11): 5059-5067.

作者简介：

张丽娟（1991-），女，山西吕梁人，西安电子科技大学硕士生，主要研究方向为信息安全、无线传感器网络等。

刘志宏（1968-），男，湖南常德人，博士，西安电子科技大学副教授、硕士生导师，主要研究方向为密码学、信息安全、网络编码、复杂网络、传感器网络等。

张洪波（1991-），男，河南洛阳人，西安电子科技大学硕士生，主要研究方向为物理层安全、信息安全、动态密钥等。

曾勇（1978-），男，湖南石门人，博士，西安电子科技大学副教授、硕士生导师，主要研究方向为信息安全、无线传感器网络等。

马建峰（1965-），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为计算机系统结构和密码学等。