# 基于人工噪声的中继网络物理层安全传输机制*

李翔宇, 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:** 针对无线自组织网的不可信中继节点会带来严重安全威胁的问题,提出利用干扰节点保障通信的物理层安全机制。其信息传输分为两个阶段:中继节点获得来自发送端和干扰节点的含人工噪声的信号;目的接收端在干扰节点的协助消噪后还原出原始信息。由于中继节点和窃听者的接收信号始终伴随严重的噪声干扰,系统具有较高的安全性。仿真结果表明,窃听者和干扰节点在处于不同地理位置时,系统均具有较大的安全传输速率。

**关键词:** 物理层安全; 协作中继系统; 人工噪声
**中图分类号:** TN929.53 **文献标志码:** A **文章编号:** 1001-3695(2012)09-3467-03
doi:10.3969/j.issn.1001-3695.2012.09.071

# Physical layer security transmission mechanism of relay network based on artificial noise

LI Xiang-yu, JIN Liang, HUANG Kai-zhi
(*National Digital Switching System Engineering & Technological Research Center, Zhengzhou* 450002, *China*)

**Abstract:** Untrusted relay in self-organizing wireless network will lead to serious security threats. This paper proposed a physi-cal-layer security mechanism based on interference nodes. The transmission was divided into two phases: first, sent signal with artificial noise from the sender and interference nodes to relay, second, restored the original information by receiver with the help of interference nodes. As the signal received by the relay and the eavesdropper were always accompanied with severe interference, security of the system was well guaranteed. Simulation results show that, when the eavesdropper and interference nodes are in different locations, the system always has a large secure-transmission rate.

**Key words:** physical-layer security; cooperative relay system; artificial noise

## 0 引言

近年来,随着无线通信网络的不断发展,特别是中继协作技术的广泛应用,对于中继节点安全性的探讨也日渐成为研究热点。由于其中间节点较多,网络结构复杂,因此面临更大的安全威胁。传统无线通信安全的研究主要集中于密钥加密体制。1975 年,Wyner[1] 提出了物理层安全模型和保密容量(secrecy capacity)的概念,为从物理层提高中继系统安全性提供了可行思路。Goel 等人[2] 在多天线系统中采用发送人工噪声的方式,对窃听者进行干扰,通过借助多中继节点,这种方式能够很好地应用于协作中继网络中。

中继网络安全性的讨论包括不可信的中继节点和外部窃听者两类。针对不可信的中继节点,He 等人[3] 提出了接收者发送干扰信号和一个干扰节点协助干扰两种机制,为解决中继节点不可信的问题提供了可行思路,并在文献[4]中借助编码方式对各种模型下的理论极限进行了计算和分析。Zhang 等人[5] 研究了同时使用多个干扰节点对非可信中继进行干扰的情况,但需要假设接收方对干扰信号已知才能消除干扰提取原始信息。另一方面,针对外部窃听节点,Chen 等人[6] 在传输的不同阶段随机挑选干扰节点进行干扰,并提出了一种切换算法以达到最优,但由于接收端也同样受到干扰,因此整体性能受到影响。Huang 等人[7] 研究了解码转发(decode-and-forward, DF)机制下的协作干扰方法,并与传统 DF 方法进行了性能比较。Zheng 等人[8] 提出了一种针对协作干扰机制的分布式算法,并通过折半查找法计算最佳干扰权值。

上述方法的不足之处在于:文献[7,8]中未考虑中继节点的不可信性,而文献[3,5,6]的干扰机制需要假设干扰节点间有控制中枢或者接收方已知干扰信号,制约了该机制在实际中的应用。因此,本文针对无线自组织网中协作节点不可信和外部窃听者存在的两种情况进行了研究,将每个传输过程分成两个阶段:

a)中继节点获得来自发送端和干扰节点的含噪信号,该信号为人工噪声和信息的叠加。

b)该含噪信号被转发至目的节点,同时各干扰节点发送噪声抵消信号,以帮助目的接收端消除干扰还原出原始信息。

人工噪声能够在各干扰节点根据信道状态信息(channel state information,CSI)自发动态调整,每个节点的人工噪声和噪声抵消信号在目的接收端叠加为零,而由于信道特性的不同,

**收稿日期:** 2012-01-15; **修回日期:** 2012-03-12 **基金项目:** 国家自然科学基金资助项目(61171108)

**作者简介:** 李翔宇(1987-),男,河南淮阳人,硕士,主要研究方向为无线移动通信( luckyxiangyu@gmail.com);金梁(1969-),男,北京人,教授,博导,主要研究方向为无线移动通信;黄开枝(1973-),女,安徽来安人,副教授,硕导,主要研究方向为无线移动通信.

这些干扰在窃听者处依然存在。通过仿真得出，当所选择的干扰节点位于发送端附近时，能够最大限度地保证系统的安全性。

## 1 系统模型

协作中继网络的信道模型如图 1 所示。所有节点处于同一个无线自组织网中，拥有有效的 MAC 层协议进行同步。每个节点只有一根天线，工作于半双工模式，最大发射功率为 $P_t$。节点的结构和功能完全相同，只是在某个传输时间段内分配的角色不同。当 Alice 和 Bob 两个节点需要进行通信时，由于之间距离较远，首先要选择一个节点作为中继节点 Relay，采用放大转发(amplify-and-forward，AF)的方式进行工作，其放大系数为 $\omega$。Relay 节点可能是不可信的，是内部窃听者，在执行正常转发功能的同时进行窃听。同时，系统中还存在只进行被动窃听的外部窃听者 Eve。

因此，为了保证通信信息的安全性，需要选择 $N$ 个协助干扰节点(friendly jammer)$\{J_1, J_2, \cdots, J_N\}$，对 Relay 和 Eve 进行一定的干扰。整个传输过程分为两个阶段：

a)中继节点获得来自发送端和干扰节点的含噪信号，该信号为人工噪声和信息的叠加，如图 1 实线箭头所示。

b)该含噪信号被转发至目的节点，同时各干扰节点发送噪声抵消信号，以帮助目的接收端消除干扰还原出原始信息，如图 1 虚线箭头所示。

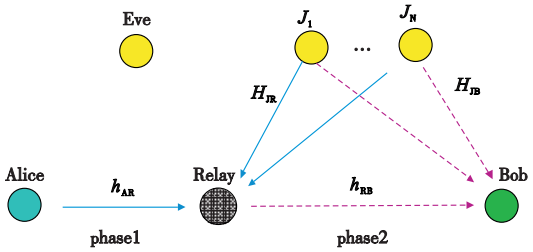


**图1 中继网络信道模型**

Alice 发出的源信息 $s_A$ 在信息集合$\{1, 2, \cdots, 2^{nR}\}$中服从均匀分布，编码器使用的码本服从高斯分布。将系统整个传输过程分为一个个相等的时间周期，每个时间单位传输一个已编码的信源符号。假设信道为受加性高斯白噪声影响的块衰落信道，即在每个时间周期内信道特征不变或者缓慢变化，在各个周期间随机变化。Alice 与 Relay 之间的信道用 $h_{AR}$ 表示，Relay 与 Bob 之间的信道用 $h_{RB}$ 表示。Jammers 与 Relay 之间的信道可以表示为 $\boldsymbol{H}_{JR} = [h_{J_1R}, h_{J_2R}, \cdots, h_{J_NR}]^T$。

同理，Jammers 与 Bob 之间的信道用 $\boldsymbol{H}_{JB}$ 表示。本文所提出的安全传输机制，各干扰节点将利用这些信道特征构造需要发送的人工噪声信号，使得噪声信号在影响 Relay 和 Eve 的同时，到 Bob 处完全抵消。

## 2 传输机制

现有的基于人工噪声的多中继协作安全机制仍然存在一些缺点，有些需要干扰节点间存在一个控制中枢进行统一协调，利用多节点模拟 MISO 系统发送人工噪声；还有一些假设 Bob 已知发送的干扰信号，可以在接收到信号之后自行去除干扰。这两种方式都有一定的应用局限性。因此，如何在没有控制中枢的情况下使噪声在 Bob 处自行抵消，这是需要解决的首要问题。注意到在中继系统中，整个传输过程往往分为两个阶段，Alice 到 Relay 和 Relay 到 Bob，而每个 Jammer 又已知 CSI 和自己发送的干扰信息，因此可以令 Jammer 在第二个阶段发送噪声抵消信号，消除自身前一个阶段所发人工噪声的影响。

整个安全传输机制是基于 AF 模式，以人工噪声的构造为核心。假设每个传输周期 Alice、Relay 和 Bob 都会广播信道探测信息，根据信道互易性，每个 Jammer$J_i$ 都能得到 $h_{J_iR}$和 $h_{J_iB}$，而这些 CSI 对于其他节点来说是未知的。Relay 与 Bob 之间的信道特征 $h_{RB}$以及 Relay 的放大系数 $\omega$ 可作为公共信息进行广播。Jammers 根据以上三个信道状态来构造噪声信号，使得 Relay 和 Eve 在受到严重干扰的同时，Bob 收到的人工噪声信号为 0。具体传输机制如下：

a)Alice 向 Relay 发送信息 $s_A$，同时，$N$ 个 Jammers 向 Relay 发送人工噪声信号$\{s_{J_1}, s_{J_2}, \cdots, s_{J_N}\}$，$E\{|s_{J_i}|^2\} = 1$，则 Relay 收到的信号为

$$s_R = \sqrt{P_A} s_A h_{AR} + w_1 \boldsymbol{H}_{JR} + e_1 = \sqrt{P_A} s_A h_{AR} + \sqrt{P_{J_1}} s_{J_1} h_{J_1R} + \cdots + \sqrt{P_{J_N}} s_{J_N} h_{J_NR} + e_1 \tag{1}$$

其中：$w_1 = \left[\sqrt{P_{J_1}} s_{J_1} \quad \sqrt{P_{J_2}} s_{J_2} \quad \cdots \quad \sqrt{P_{J_N}} s_{J_N}\right]$，$P_A$ 表示 Alice的发送信号功率，$P_{J_i}$表示第 $i$ 个 Jammer 在第一阶段的发送功率，$e_1$ 表示信道高斯白噪声。可见，除了第一项为有用信号之外，其他均为噪声干扰项。

b)Relay 将收到的信息 $s_R$ 放大 $\omega$ 倍之后转发给 Bob，转发所产生的延时和相位变化均计入 $h_{RB}$中，同时，所有 Jammer 节点向 Bob 发送噪声抵消信号$\{t_{J_1}, t_{J_2}, \cdots, t_{J_N}\}$，信号经过归一化 $E\{|t_{J_i}|^2\} = 1$，保证 $\sqrt{P_{J_i1}} s_{J_i} h_{J_iR} h_{RB} \omega + \sqrt{P_{J_i2}} t_{J_i} h_{J_iB} = 0$，则所有噪声在到达 Bob 处时完全抵消，Bob 接收到的信号为

$$\begin{aligned} s_B &= s_R h_{RB} \omega + w_2 \boldsymbol{H}_{JR} + e_2 = \\ &\left(\sqrt{P_A} s_A h_{AR} + \sqrt{P_{J_1}} s_{J_1} h_{J_1R} + \cdots + \sqrt{P_{J_1}} s_{J_N} h_{J_NR} + e_1\right) \times \\ &h_{RB} \omega + \sqrt{P_{J_2}} t_{J_1} h_{J_1B} + \cdots + \sqrt{P_{JN2}} t_{J_N} h_{J_NB} + e_2 = \\ &\sqrt{P_A} s_A h_{AR} h_{RB} \omega + \left(\sqrt{P_{J_1}} s_{J_1} h_{J_1R} h_{RB} \omega + \sqrt{P_{J_2}} t_{J_1} h_{J_1B}\right) + \cdots + \\ &\left(\sqrt{P_{J_1}} s_{J_N} h_{J_NR} h_{RB} \omega + \sqrt{P_{JN2}} t_{J_N} h_{J_NB}\right) + e_1 h_{RB} \omega + e_2 = \\ &\sqrt{P_A} s_A h_{AR} h_{RB} \omega + e_1 h_{RB} \omega + e_2 \end{aligned} \tag{2}$$

其中：$w_2 = \left[\sqrt{P_{J_2}} t_{J_1} \quad \sqrt{P_{J_2}} t_{J_2} \quad \cdots \quad \sqrt{P_{JN2}} t_{J_N}\right]$，$P_{J_i2}$表示第 $i$ 个 Jammer 在第二个阶段的发送功率，$e_2$ 表示信道高斯白噪声。

显然，Bob 接收到的信号没有受到人工噪声的影响。

## 3 保密容量分析

### 3.1 中继节点不可信时的保密容量

为了达到最大的瞬时安全速率，需要 Jammers 的发射功率尽量大，以使 Relay 收到足够多的干扰。因为各 Jammer 满足 $\sqrt{P_{J_i1}} s_{J_i} h_{J_iR} h_{RB} \omega + \sqrt{P_{J_i2}} t_{J_i} h_{J_iB} = 0$，且最大发射功率为 $P_t$，所以 Jammers 的发射功率应满足

$$\begin{cases} \sqrt{P_{J_i1}} |h_{J_iR}| |h_{RB}| \omega = \sqrt{P_{J_i2}} |h_{J_iB}| \\ P_{J_i1}, P_{J_i2} \leqslant P_t \end{cases} \tag{3}$$

设 Relay 节点为不可信中继节点，不存在外部窃听者 Eve。Relay 节点在第一个阶段收到信号的信噪比为

$$\gamma_R = \frac{P_A |h_{AR}|^2}{|w_1 \boldsymbol{H}_{JR}|^2 + \sigma_{e_1}^2} \tag{4}$$

Bob 在第二个阶段收到的信号信噪比为

$$\gamma_B = \frac{P_A |h_{AR}|^2 |h_{RB}|^2 \omega^2}{\sigma_{e_1}^2 |h_{RB}|^2 \omega^2 + \sigma_{e_2}^2} \tag{5}$$

其中:$\sigma_{e_1}^2$ 与 $\sigma_{e_2}^2$ 表示白噪声功率。根据文献[9]的现有结论,系统的保密容量可表示为 $C_{sec} \geqslant \max\limits_{P_X P_{YZ|X}} [I(X;Y) - I(X;Z)]$,则第 $k$ 个时间周期系统的安全传输速率(secrecy rate)可以表示为

$$R_{k,R} = \max\{0, \frac{W}{2}\log(1+\gamma_B) - \frac{W}{2}\log(1+\gamma_R)\} \tag{6}$$

其中:$W$ 为信道传输带宽,在信道特征一定的情况下,$\gamma_B$ 已经确定,只有 $\gamma_R$ 会因为 Jammers 的发射信号不同而不同,可以进行调整。Alice 的发射功率 $P_A$ 最大值也为 $P_t$。

$$\gamma_R = \frac{P_A |h_{AR}|^2}{|w_1|^2 |\boldsymbol{H}_{JR}|^2 \cos^2\alpha + \sigma_{e_1}^2} \geqslant \frac{|h_{AR}|^2}{N|\boldsymbol{H}_{JR}|^2 + \sigma_{e_1}^2} \tag{7}$$

当 Jammers 的干扰信号发射功率均能达到 $P_t$ 时,等号成立。此时系统的保密容量为

$$C_{k,R} = \frac{W}{2}\log\left(1 + \frac{P_t |h_{AR}|^2 |h_{RB}|^2 \omega^2}{\sigma_{e_1}^2 |h_{RB}|^2 \omega^2 + \sigma_{e_2}^2}\right) - \frac{W}{2}\log\left(1 + \frac{|h_{AR}|^2}{N|\boldsymbol{H}_{JR}|^2 + \sigma_{e_1}^2}\right) \tag{8}$$

从式(8)可以看出,当信道状况较好时,$C_{k,R}$ 随 $P_A$、$P_t$、$N$ 的增大均单调递增。

### 3.2　存在外部窃听者时的保密容量

考虑外部窃听者时,先假设 Relay 节点为可信节点。由于 Eve 在传输的两个时间段均能收到信号,因此需要考虑两部分信息量。用 $e_3$、$e_4$ 表示两个阶段的白噪声,$\sigma_{e_3}^2$、$\sigma_{e_4}^2$ 表示其功率,第一阶段 Eve 收到的信号为

$$s_{E,1} = \sqrt{P_A} s_A h_{AE} + w_1 \boldsymbol{H}_{JE} + e_3 = \sqrt{P_A} s_A h_{AE} + \sqrt{P_{J_1}} s_{J_1} h_{J_1 E} + \cdots + \sqrt{P_{J_N}} s_{J_N} h_{J_N E} + e_3 \tag{9}$$

则其信噪比为

$$\gamma_{E,1} = \frac{P_A |h_{AE}|^2}{|w_1 \boldsymbol{H}_{JE}|^2 + \sigma_{e_3}^2} \tag{10}$$

第二阶段 Eve 收到的信号为

$$s_{E,2} = s_R h_{RE}\omega + w_2 \boldsymbol{H}_{JE} + e_4 = (\sqrt{P_A} s_A h_{AR} + \cdots + \sqrt{P_{J_N}} s_{J_N} h_{J_N R} + e_1) h_{RE}\omega + \sqrt{P_{J_1}} t_{J_1} h_{J_1 E} + \cdots + \sqrt{P_{J_N}} t_{J_N} h_{J_N E} + e_4 \tag{11}$$

则其信噪比为

$$\gamma_{E,2} = \frac{P_A |h_{AR}|^2 |h_{RE}|^2 \omega^2}{|w_1 \boldsymbol{H}_{JR} h_{RE}\omega + w_2 \boldsymbol{H}_{JE}|^2 + \sigma_{e_4}^2} \tag{12}$$

由于人工噪声信号的设计满足 $\sqrt{P_{J_i}} s_{J_i} h_{J_i R} h_{RB}\omega + \sqrt{P_{J_i}} t_{J_i} h_{J_i B} = 0$,所以才会在 Bob 处抵消为 0。但由于 Eve 与 Bob 的信道状态不同,显然 $h_{RE} \neq h_{RB}$,$h_{J_i E} \neq h_{J_i B}$。因此,在 Eve 处不能够互相抵消,反而会因为幅度和相位的不同随机变化,使 Eve 的接收信噪比降低。

则第 $k$ 个时间周期的安全传输速率[9]可表示为

$$R_{k,R} = \max\{0, \frac{W}{2}\log(1+\gamma_B) - \max[\frac{W}{2}\log(1+\gamma_{E,1}), \frac{W}{2}\log(1+\gamma_{E,2})]\} \tag{13}$$

由于 Eve 节点的位置未知,如果网络中的节点较多,每次传输时,可在众多信道状态合适的节点中随机选择 $N$ 个节点作为 Jammer 节点,以防止 Eve 处于某些特定位置,可能受到的干扰较小。

## 4　模型仿真

建立一个二维的简易系统模型对上述结果进行仿真。将 Alice、Relay 和 Bob 放在一条直线上,依次间隔 50 m。Alice 的坐标为(0,0),Bob 的坐标为(100,0)。使用两个 Jammer 节点 $J_1$ 和 $J_2$ 对 Relay 和 Eve 进行干扰。信道状态信息包括两个部分:与距离有关的信道衰落;随机的相位变化。如 $h_{AR} = d_{AR}^{-c/2} e^{j\theta}$,$d_{AR}$ 表示 Alice 与 Relay 之间的距离,距离衰落指数 $c$ 取 3.5,$\theta$ 在[0,2π)内均匀分布。信道高斯白噪声功率 $\sigma_e^2$ 为 -60 dBm,节点发射功率 $P_t$ 为 40 dBm,$P_A = P_t$。

a)研究 Relay 为不可信节点的情况,不考虑外部窃听者 Eve 的存在,固定 Relay 的位置移动 Jammer。假设 $J_1$ 和 $J_2$ 的横、纵坐标均在[1,100]内移动,且两个节点距离很近,信道衰落参数相同,$\omega = 200$,$W = 200$ Hz,计算此时系统的保密容量以及两个干扰节点在传输周期内消耗的总功率,总功率上限应为 $4P_t$。

从图 2、3 中可以看出,当 Jammer 的位置在 Relay 附近时,可以达到最大的保密容量,虽然为了保证干扰信号在 Bob 处抵消,发射的干扰信号功率已经很低。但由于距离很近,衰减很小,仍然能够在 Relay 处造成足够大的干扰,两个阶段消耗的干扰总功率也最低。当 Jammer 处于 Bob 附近时,第一阶段需要全功率发射,第二阶段只需很小的功率就能够将人工噪声抵消,因此消耗的总功率也较低。

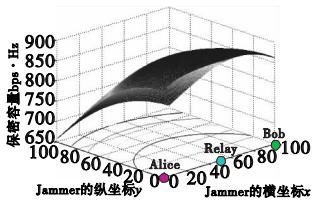


图2　保密容量与Jammer位置的关系

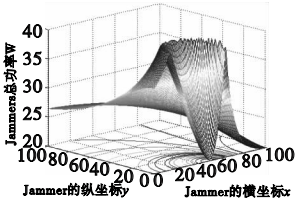


图3　干扰总功率与Jammer位置的关系

b)对存在外部窃听者 Eve 时的情况进行研究,固定 Jammer 的位置移动 Eve。令两个 Jammer 节点位于坐标[80,20]处,$\omega = 200$,$W = 200$ Hz,Eve 的横纵坐标均在[1,100]内移动,计算此时系统的安全传输速率。仿真结果如图 4 所示。

从图 4 中可以看出,当 Eve 离 Alice 较远时,系统的安全传输速率对 Eve 的位置不太敏感,始终保持在较高的状态。但当 Eve 处于 Alice 附近时,因为能够接收到足够多的信息量,而且干扰节点的干扰信息由于距离衰减几乎没有作用,因此安全传输速率为 0。为保证系统的安全性,需要尽量选择离 Alice 较近的 Jammer 节点,将 Jammer 节点放置于坐标[1,1]处,系统的安全传输速率如图 5 所示,可以看出,上述安全问题得到了明显的改善,Eve 处于各个位置时,系统都有较高的安全传输速率。

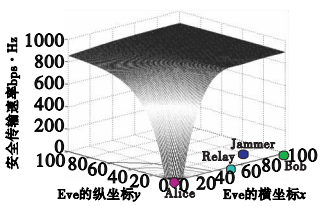


图4　Jammer坐标为[80,20]时系统的安全传输速率

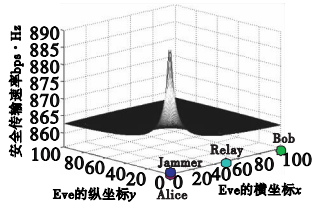


图5　Jammer坐标为[1,1]时系统的安全传输速率

综合上述两个仿真结果,当 Jammer 位置 (下转第 3492 页)

(上接第 3469 页)处于 Alice 附近时,针对不可信 Relay 和外部窃听者 Eve 都能够使系统保持足够高的安全传输速率。因此,在实际系统中,应尽量选择离发送端较近的节点作为协助干扰节点。

## 5 结束语

本文针对无线自组织网中中继节点不可信的问题,提出了一种多中继协作干扰机制。该机制将每个传输过程分成两个阶段:a)中继节点获得来自发送端和干扰节点的含噪信号,该信号为人工噪声和信息的叠加;b)目的接收端在干扰节点的协助消噪后还原出原始信息。人工噪声能够在各干扰节点根据信道状态信息(channel state information,CSI)自发动态调整,每个节点的人工噪声和噪声抵消信号在目的接收端叠加为零,而由于信道特性的不同,这些干扰在窃听者处依然存在。

通过仿真可以看出,当 Relay 为不可信节点时,Jammer 位置离 Relay 越近越好,以较小的功率损耗,即可造成较大的干扰,保证安全传输。当 Eve 存在且离 Alice 很近时,信息传输的安全性还是不能够完全保证,因此应尽量选择离 Alice 较近的 Jammer 节点。

在以后的研究中,还可以对 Alice 与 Jammer 节点之间的功率分配进行更进一步的探讨,以最优化的功率损耗,保证最大的系统安全性。

**参考文献:**


[1] WYNER A D. The wire-tap channel[J]. Bell Systems Technical Journal,1975,54(8):1355-1387.

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

[3] HE Xiang, YENER A. Two-hop secure communication using an untrusted relay: a case for cooperative jamming[C]//Proc of IEEE Global Telecommunications Conference. Los Angeles: IEEE Press, 2008:1-5.

[4] HE Xiang, YENER A. Cooperation with an untrusted relay:a secrecy perspective[J]. IEEE Trans on Information Theory,2010,56(8): 3807-3827.

[5] ZHANG Rong-qing, SONG Ling-yang, HAN Zhu, *et al*. Physical layer security for two way relay communications with friendly jammers[C]// Proc of IEEE Global Telecommunications Conference. 2010:1-6.

[6] CHEN Jing-chao, ZHANG Rong-qing, SONG Ling-yang, *et al*. Joint relay and jammer selection for secure two-way relay networks[C]// Proc of IEEE International Conference on Communication. 2011:1-5.

[7] HUANG Shuang-lin, WEI Jiao-long, CAO Yang, *et al*. Joint decode-and-forward and cooperative jamming for secure wireless communications[C]//Proc of the 7th International Conference on Wireless Communications, Networking and Mobile Computing. 2011:1-4.

[8] ZHENG Gan, CHOO L C, WONG K K. Optimal cooperative jamming to enhance physical layer security using relays[J]. IEEE Trans on Signal Processing,2011,59(3):1317-1322.

[9] CSISZAR I, KORNER J. Broadcast channels with confidential messages[J]. IEEE Trans on Information Theory, 1978, 24(3): 339-348.