基于双变量泊松点过程的无线 Ad Hoc 网络的保密广播传输容量分析

孙晓惠,尹长川
(北京邮电大学北京市网络体系构建与融合重点实验室,北京 100876)

摘 要: 本论文利用双变量泊松点过程对无线 ad hoc 广播网络和非法窃听网络共存的网络场景进行建模,运用随机几何工具,研究了无线 ad hoc 网络的保密广播传输容量,其定义为未发生窃听中断的广播发送节点密度、广播发送节点的相邻接收节点数量的平均值与保密速率的乘积.针对一般衰落和瑞利衰落信道条件,论文推导了造成保密中断的相邻窃听节点数量的平均值和保密广播传输容量的表达式.分析结果表明,与不存在相关性的网络场景相比,广播网络和窃听网络间的相关性会带来的保密广播传输容量的损失.

关键词: 无线 ad hoc 网络; 保密广播传输容量; 双变量泊松点过程; 保密速率
中图分类号: TN92 **文献标识码:** A **文章编号:** 0372-2112 (2014)09-1847-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2014.09.028

Secrecy Broadcast Transmission Capacity of Wireless Ad Hoc Networks Based on Bivariate Poisson Point Process

SUN Xiao-hui, YIN Chang-chuan
(*Beijing Key Laboratory of Network System Architecture and Convergence, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*)

Abstract: We use bivariate Poisson point process(BPPP) to model the scenario where a wireless ad hoc broadcast network coexists with a wiretapping network. By using stochastic geometry tools, we study the secrecy broadcast transmission capacity of wireless ad hoc network, which is defined as the product among the spatial density of broadcast transmissions without secrecy outage, the average number of neighbors of a broadcasting node, and the secrecy rate. We first derive the average number of eavesdropping neighbors that causes secrecy outage and then characterize the secrecy broadcast transmission capacity over general fading and Rayleigh fading channels. Finally, numerical results are presented to show that in comparison to the case without correlation, the correlation between the legitimate nodes and the eavesdroppers degrades the secrecy broadcast transmission capacity.

Key words: wireless ad hoc networks; secrecy broadcast transmission capacity; spatial bivariate Poisson point process; secrecy rate

1 引言

Shannon 的开创性工作奠定了保密通信的理论基础.在文献[1]中,Shannon 将保密通信系统分为三种:隐藏系统(concealment system),隐私系统(privacy systems),和"真正"的保密系统("true" secrecy systems),重点研究了第三种保密通信系统.随后人们对保密通信的理论研究,均集中在第三种保密通信系统的研究.

近些年来,无线通信系统中物理层安全理论受到人们的广泛关注[2].在早期的物理层安全研究中,Wyner[3]提出了点对点通信的窃听信道模型,在其模型中包括一对合法收发节点对和一个窃听节点.有关物理层安全的近期大多研究结果主要从 Shannon 信息论的角度研究具有少数通信节点的信息安全传输问题[4~7](如文献[4]中的模型仅仅由一对合法接收节点和一个窃听节点组成).

而在实际的通信网络中,传输信息的节点数量非常多,如何度量存在窃听场景下大规模网络的安全问题是一个值得探讨的问题.在文献[8]中,假设合法节点和窃听节点服从独立的泊松点过程,Zhou 等人提出了网络保密传输容量(secrecy transmission capacity)的概念.研究结果表明,存在窃听节点场景下,要获得高的安全性,传

收稿日期:2013-04-22;修回日期:2013-06-23;责任编辑:覃怀银
基金项目:国家高技术研究发展计划(863 计划)课题(No.2011AA100706);国家自然科学基金(No.61271257,No.60972073);北京市自然科学基金(No.4122034);教育部博士点基金(No.20120005110007)

输容量的损失是很大的.在文献[9]中,Ao 和 Chen 考虑了存在多个独立共存的 ad hoc 网络和一个独立的窃听网络的场景,将安全传输容量的概念从单播推广到了多播情形,而且首次引入了保密广播传输容量的概念,其定义为未产生窃听中断的广播发送节点密度、广播发送节点的平均相邻接收节点数目和保密速率(secrecy rate)的乘积.在此基础上,作者研究了在保密中断制约的条件下,窃听对广播容量带来的损失,并分析了广播容量最大化对应的最优接入概率的存在性.

在实际的通信网络中,由于窃听网络在主观上都是有意去窃听合法通信网络中的信息传输,即窃听网络的存在及其节点的位置在一定程度上依赖于合法通信网络.因此,窃听网络和合法网络之间会存在某种相关性.但是,目前关于保密网络容量的研究模型,均假设窃听网络和合法通信网络之间相互独立(如文献[8]、[9]).在本文中,我们研究合法网络和窃听网络之间存在相关性时无线 ad hoc 网络的保密广播传输容量.我们运用双变量泊松点过程[10]来对窃听网络和合法网络间的相关性进行建模,并基于此模型,针对一般衰落和瑞利衰落信道条件,推导了无线 ad hoc 网络中的广播节点在存在保密中断约束条件下的相邻窃听节点数量的平均值和保密广播传输容量的表达式.理论分析和数值结果表明,窃听网络与广播网络之间的相关性会引起传输容量的损失,且对于不同程度的网络相关性,使广播容量最大化的最优接入概率不一定存在.

本文后续章节组织如下.系统模型及无线 ad hoc 广播网络保密传输容量的定义在第 2 节中给出.第 3 节给出了基于双变量泊松点过程模型的保密广播传输容量的分析结果.第 4 节给出了数值计算结果,并与不存在相关性的情况下的保密传输容量结果进行比较.最后,第 5 节是本文的结论.

2 系统模型

考虑在二维空间 R^2 区域内,存在一个合法的 ad hoc 广播网络和一个窃听网络.合法网络中的节点(简称合法节点)和窃听网络中的节点(称为窃听节点)共同服从参数为 $\lambda+\mu+\nu$ 的双变量泊松点过程.λ 是独立合法节点的密度,μ 是独立窃听节点的密度,ν 则是由窃听节点和合法节点组成的对点的密度(窃听节点和合法节点组成对点可以解释为窃听节点和该合法节点存在某种关联性.实际中,窃听节点在主观上都是有意去窃听合法通信网络中某个节点的信息传输,此时窃听节点的位置与数量与合法节点的位置和数量存在相关性,即模拟此窃听节点与欲窃听的合法节点组成对点.).由双变量泊松点过程定义[11]可知,合法节点和窃听节点分别服从参数为 $\lambda+\nu$ 和 $\mu+\nu$ 的泊松分布.

假设广播网络使用接入概率为 p 的时隙 ALOHA 协议,即在每个时隙的初始时刻,每个节点以概率 p 成为广播节点.在某一个时隙内,广播节点服从密度为 $\lambda_t=p(\lambda+\nu)$的泊松分布.同时我们假设,每个合法节点不能同时收发信息,即一个合法节点在某个时隙内只能是广播节点或者接收节点.那么接收节点服从密度为 $\lambda_r=(1-p)(\mu+\nu)$的泊松分布.

记 $\Phi=\{X_k\}$为广播网络中节点的位置集合.$\Phi^1=\{X_k\in\Phi:B_k(p)=1\}$和 $\Phi^0=\{X_k\in\Phi:B_k(p)=0\}$分别代表广播节点和接收节点的位置集合.$B_k(p)$是与 X_k、p 有关的独立同分布二项伯努利随机变量.记 $\Phi^e=\{Z_k\}$为所有窃听节点的位置集合.

假设窃听节点均为无源的[12],且窃听节点与合法网络节点具有相同的特征[13].假设窃听者可以窃听所有发送节点发出的信息.

信号在无线传播中受到大尺度路径损耗和小尺度衰落的影响.在本论文中,假设,路径损耗因子 $\alpha>2$,小尺度衰落则分别考虑一般衰落和瑞利衰落两种情况.假设小尺度衰落函数是独立同分布的,且有相同的概率密度函数.每个广播节点的发送功率为 P,数据传输速率为 R.假设整个网络是一个干扰受限的网络,忽略系统和环境中背景噪声的影响.

如图 1,给定广播节点的信息发送速率 R 和保密速率 R_s(保密速率为接收机安全接收信息且不发生窃听中断的速率),如果存在某个窃听者能以 R_e 的速率成功接收到任意广播节点发送的消息,则本次通信是不安全的,即产生保密中断,定义保密中断概率为 ε.反之给定 ε,可以求得最大的保密速率 R_s.信息速率和保密速率之间的差值 $R_e=R-R_s$,是存在窃听而损失的速率.在保密中断约束下的保密广播传输容量 B_{tc}^s定义为[9],

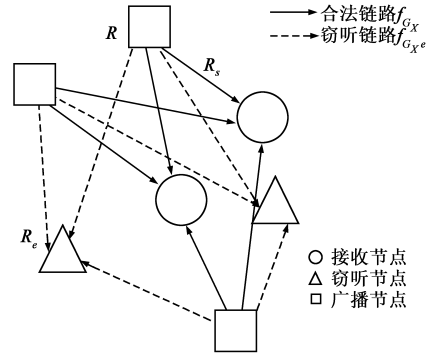


图1 广播发送场景图

$$B_{\mathrm{tc}}^s=\lambda(1-\varepsilon)\beta R_s \tag{1}$$

其中,β 代表每个广播节点的相邻接收节点数量的平均值.

利用文献[9]中的结果,可以得到在一般衰落条件下,一个广播节点的平均相邻接收节点的数量为

$$\beta=\frac{(1-p)\int_{-\infty}^{+\infty}\frac{g_X(t)}{t^{\delta}}\mathrm{d}t}{p(2^R-1)^{\delta}\Gamma(1-\delta)\mathrm{E}[G_X^{\delta}]} \tag{2}$$

其中 $\delta=\frac{2}{\alpha}$,G_X 是信道功率增益,$g_X(t)$是 $\bar{F}_{G_X}(s)$的拉普拉斯逆变换,即满足 $\bar{F}_{G_X}(s)=L\{g_X(t)\}=\int_{-\infty}^{+\infty}\mathrm{e}^{-st}\cdot g_X(t)\mathrm{d}t$,$\bar{F}_{G_X}(s)$是合法链路功率增益的函数,$\bar{F}_{G_X}(s)=\mathrm{P}(G_X>s)$,$\Gamma(x)$是伽玛函数.

当所有的链路均为独立同分布且服从瑞利衰落,且信道功率增益 G_X 归一化均值为 1 的指数分布时,则有,

$$\beta=\frac{(1-p)}{p\Gamma(1+\delta)\Gamma(1-\delta)(2^R-1)^{\delta}} \tag{3}$$

3　广播传输容量分析

在此小节中,我们分别分析在一般衰落和瑞利衰落信道条件下,每个广播节点的相邻窃听节点数量的平均值,由此得到保密速率,并最终求得保密广播传输容量.

假设在坐标原点处存在一个典型的合法接收节点 R_0,其对应的广播节点为 T_0,收到的干扰为:

$$I_0=\sum_{X_k\in\Phi^!\setminus|T_0|}G_{X_k}P\parallel X_k\parallel^{-\alpha} \tag{4}$$

其中,G_{X_k}是从广播节点 X_k 到典型接收节点间的链路功率增益,$\parallel X_k\parallel$ 是从节点 X_k 到典型接收机间的距离.由第 2 节模型可知 G_{X_k}是独立同分布的,且有相同的概率密度函数 $f_{G_X}(k)$.即:$\forall k, f_{G_{X_k}}(k)=f_{G_X}(k)$.

假设离典型合法接收节点最近的窃听者为典型窃听者 E_0,其收到的干扰功率可表示为(假设它希望窃听发送节点 T_0 发出的消息):

$$I_0^e=\sum_{X_k\in\Phi^!\setminus|T_0|}G_{X_k^e}P\parallel X_k^e\parallel^{-\alpha} \tag{5}$$

其中,$G_{X_k^e}$是从广播节点 X_k 到典型接收节点间的链路功率增益(由模型可得,当 $G_{X_k^e}$的概率密度函数为$f_{G_{X_k}}(k)$.则:$\forall k, f_{G_{X_k^e}}(k)=f_{G_{X^e}}(k)$),$\parallel X_k^e\parallel$ 是从节点 X_k 到典型窃听节点间的距离.E_0 接收信号的信噪比为,

$$\mathrm{SIR}_0^e=\frac{G_{X_0^e}P\parallel X_0^e\parallel^{-\alpha}}{I_0^e} \tag{6}$$

3.1　一般衰落情况

给定信息发送速率 R,和保密中断概率限制 ε,可以求得最大的保密速率 R_s.则因存在窃听而损失的速率为 $R_e=R-R_s$.只要存在一条从广播发送节点到窃听节点间的链路可支持速率 R_e,即产生保密中断.可以算得 E_0 成功窃听的概率为($\mathrm{P}(x)$代表 x 的概率):

$$\mathrm{P}(\log(1+\mathrm{SIR}_0^e)\geqslant R_e) \tag{7}$$

由于每个广播节点和窃听节点的工作模式都相同,且链路是独立同分布的,所以每个窃听节点收到的信噪比 SIR_k^e 是同分布的.我们用 SIR^e 代替 SIR_k^e.那么,网络的保密中断概率可以表示为:

$$\mathrm{P}(\log(1+\mathrm{SIR}^e)>R_e)=\mathrm{P}\left(\log\left(1+\frac{G_{X^e}P\parallel X^e\parallel^{-\alpha}}{I^e}\right)\geqslant R_e\right) \tag{8}$$

将满足式(8)的窃听者的集合记为 Ξ^e,此集合中窃听节点的平均数量即为每个广播节点的相邻窃听节点数量的平均值.

由映射原理[14],集合 Ξ^e 服从均值为 β_e 的泊松分布.可以算得:

$$\begin{aligned}
\beta_e&=\int_0^{\infty}\Lambda(r)\mathrm{P}\left(\log\left(1+\frac{G_{X^e}Pr^{-\alpha}}{I^e}\right)\geqslant R_e\right)2\pi r\mathrm{d}r\\
&=\int_0^{\infty}\Lambda(r)\mathrm{P}\left(G_{X^e}\geqslant\frac{(2^{R_e}-1)I^e}{Pr^{-\alpha}}\right)2\pi r\mathrm{d}r\\
&\underline{(a)}\int_0^{\infty}\left[\mu+\frac{\nu}{\lambda+\nu}\left(\lambda+\frac{1}{2\pi\sigma^2}\exp\left(\frac{-r^2}{2\sigma^2}\right)\right)\right]\\
&\quad\times\mathrm{E}\left[\int_{-\infty}^{+\infty}\exp(-t\theta I^e)g_{X^e}(t)\mathrm{d}t\right]2\pi r\mathrm{d}r\\
&=\int_{-\infty}^{+\infty}g_{X^e}(t)\int_0^{\infty}\mathrm{E}_{I^e}[\exp(-t\theta I^e)]\\
&\quad\times\left[\mu+\frac{\nu}{\lambda+\nu}\left(\lambda+\frac{1}{2\pi\sigma^2}\exp\left(\frac{-r^2}{2\sigma^2}\right)\right)\right]2\pi r\mathrm{d}r\mathrm{d}t\\
&\underline{(b)}\int_{-\infty}^{+\infty}g_{X^e}(t)\int_0^{\infty}\exp\{-p(\lambda+\nu)\pi P^{\delta}\mathrm{E}[G_{X^e}{}^{\delta}]\Gamma(1-\delta)t^{\delta}\theta^{\delta}\}\\
&\quad\times\left[\mu+\frac{\nu}{\lambda+\nu}\left(\lambda+\frac{1}{2\pi\sigma^2}\exp\left(\frac{-r^2}{2\sigma^2}\right)\right)\right]2\pi r\mathrm{d}r\mathrm{d}t\\
&=\int_{-\infty}^{+\infty}g_{X^e}(t)\int_0^{\infty}\exp\{-p(\lambda+\nu)\pi R'^{\delta}\mathrm{E}[G_{X^e}{}^{\delta}]\Gamma(1-\delta)t^{\delta}\}\\
&\quad\times\left[\mu+\frac{\nu}{\lambda+\nu}\left(\lambda+\frac{1}{2\pi\sigma^2}\exp\left(\frac{-r^2}{2\sigma^2}\right)\right)\right]2\pi r\mathrm{d}r\mathrm{d}t\\
&=\frac{\left(\mu+\frac{\lambda\nu}{\lambda+\nu}\right)\int_{-\infty}^{+\infty}\frac{g_{X^e}(t)}{t^{\delta}}\mathrm{d}t}{p(\lambda+\nu)R'^{\delta}\mathrm{E}[G_{X^e}{}^{\delta}]\Gamma(1-\delta)}\\
&\quad+\int_{-\infty}^{+\infty}\frac{g_{X^e}(t)}{1+2\pi\sigma^2p(\lambda+\nu)R'^{\delta}\mathrm{E}[G_{X^e}{}^{\delta}]\Gamma(1-\delta)t^{\delta}}\mathrm{d}t
\end{aligned} \tag{9}$$

其中 $\Lambda(r)=\mu+\frac{\nu}{\lambda+\nu}\left(\lambda+\frac{1}{2\pi\sigma^2}\exp\left(\frac{-r^2}{2\sigma^2}\right)\right)$是广播节点 r 处存在窃听节点的条件概率密度函数[11].$\theta=\frac{(2^{R_e}-1)}{Pr^{-\alpha}}$,$g_{X^e}(t)$是 G_{X^e}的累积概率分布函数的拉普拉斯逆变换.(a)是根据,$s=\theta I^e$ 得到.$\mathrm{P}(G_{X^e}\geqslant s)=\int_{-\infty}^{+\infty}\mathrm{e}^{-st}g_{X^e}(t)\mathrm{d}t$.(b)来自于参考文献[9].$R'=2^{R_e}-1$.

我们通过式(9)来计算保密速率.在保密中断约束条件下,我们有,

$$\begin{aligned}&\text{P(保密中断)}\\&=\text{P(集合 }\Xi^e\text{ 中至少存在一个窃听者)}\\&=1-\text{P}(\Xi^e=\phi)\\&\overset{(a)}{\leqslant}1-\exp(-\beta_e)\\&\leqslant\varepsilon\end{aligned}\tag{10}$$

式(10)中,不等式(a)源于 Jensen 不等式.令

$$1-\exp(-\beta_e)=\varepsilon\tag{11}$$

由式(9)和(11),可求得 R_e 的上界,

$$R_e^{\text{upper}}=\log_2(x^{\frac{1}{\delta}}+1)\tag{12}$$

其中 $x=\dfrac{-(d-ac-b)+\sqrt{(d-ac-b)^2+4acd}}{2cd}$, $a=\dfrac{\mu+\dfrac{\lambda\nu}{\lambda+\nu}}{p(\lambda+\nu)}$, $b=\dfrac{\nu}{\lambda+\nu}$, $d=\ln\dfrac{1}{1-\varepsilon}$, $c=2\pi\sigma^2p(\lambda+\nu)$.保密速率的下界可由 $R_s^{\text{lower}}=R-R_e^{\text{upper}}$ 得到.一般衰落条件下的保密广播传输容量下界可通过下式求得:

$$B_{\text{tc}}^s\geqslant p(\lambda+\nu)(1-\varepsilon)\beta R_s^{\text{lower}}\tag{13}$$

其中,β 由式(2)算得.

3.2 瑞利衰落情况

当网络中所有传输链路上的小尺度衰落均服从瑞利衰落,信道功率增益为指数分布,假设其均值为 1.我们可计算每个广播节点相邻窃听节点数量的平均值如下:

$$\begin{aligned}\beta_e&=\int_0^\infty\Lambda(r)\text{P}\left(\log\left(1+\frac{G_{X^e}Pr^{-\alpha}}{I^e}\right)\geqslant R_e\right)2\pi r\text{d}r\\&=\int_0^\infty\Lambda(r)\text{P}\left(G_{X^e}\geqslant\frac{(2^{R_e}-1)I^e}{Pr^{-\alpha}}\right)2\pi r\text{d}r\\&\underline{\underline{(a)}}\int_0^\infty\Lambda(r)\text{E}_{I^e}\left[\exp\left\{\frac{(2^{R_e}-1)I^e}{Pr^{-\alpha}}\right\}\right]2\pi r\text{d}r\\&\underline{\underline{(b)}}\int_0^\infty\left[\mu+\frac{\nu}{\lambda+\nu}\left(\lambda+\frac{1}{2\pi\sigma^2}\exp\left(\frac{-r^2}{2\sigma^2}\right)\right)\right]\\&\quad\times\exp\{-p(\lambda+\nu)\pi\Gamma(1+\delta)\Gamma(1-\delta)R'r^2\}2\pi r\text{d}r\\&=\frac{\nu}{(\lambda+\nu)(2\pi\sigma^2p(\lambda+\nu)R'^{\delta}+1)\Gamma(1+\delta)\Gamma(1-\delta)}\\&\quad+\frac{\mu+\dfrac{\nu\lambda}{\nu+\lambda}}{p(\lambda+\nu)R'^{\delta}\Gamma(1+\delta)\Gamma(1-\delta)}\end{aligned}\tag{14}$$

其中(a)是由 $\text{P}(G_{X^e}\geqslant x)=\text{e}^{-x}$得到,($b$)是由干扰 I^e 的拉普拉斯变换得到.

根推式(11)和(14),有:

$$\begin{aligned}&\frac{\nu}{(\lambda+\nu)(2\pi\sigma^2p(\lambda+\nu)R'^{\delta}+1)}+\frac{\mu+\dfrac{\nu\lambda}{\nu+\lambda}}{p(\lambda+\nu)R'^{\delta}}\\&=\Gamma(1+\delta)\Gamma(1-\delta)\ln\frac{1}{1-\varepsilon}\end{aligned}\tag{15}$$

对式(15)求解,可以得到 R_e 的上界,从而得到瑞利衰落条件下,保密广播传输容量的下界:

$$B_{\text{tc}}^s\geqslant p(\lambda+\nu)(1-\varepsilon)\beta(R-R_e^{\text{upper}})\tag{16}$$

其中,β 由式(3)求得.

4 数值结果及分析

在本节中,我们利用以上分析给出数值结果,并做相应的讨论.以下如无特殊说明,均假设路径损耗因子 $\alpha=4$.

取合法节点的密度为 10^{-2}(即 $\lambda+\nu=10^{-2}$),窃听节点的密度为 10^{-3}(即 $\mu+\nu=10^{-3}$).保密速率 R_s 随接入概率 p 的变化在图 2 中给出($R=32$).可以看出,R_s 是 p 的增函数.对于给定接入概率 p,网络间的相关性越强,速率的损失越大.

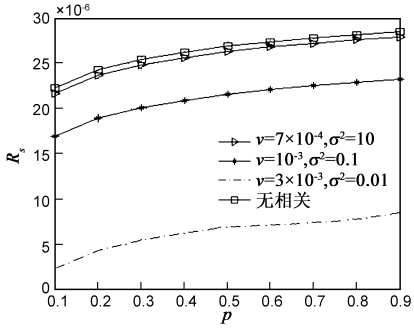


图2 保密速率R_s随接入概率p的变化曲线

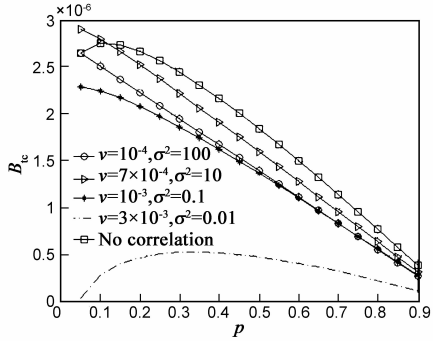


图3 保密广播传输容量B_{tc}^s随p的变化曲线

图 3 示出了保密广播传输容量 B_{tc}^s 随接入概率 p 的关系曲线($R=32,\varepsilon=0.1$).对于给定的 p,B_{tc}^s 随着相关性的增强而减小.相关性越强,因窃听存在而损失的速率 R_e 越大,损失的容量也越多,尤其在接入概率较小时,强相关引起的容量损失尤为明显.如图示,当 $p\approx0.2$ 时,强相关($\nu=10^{-4},\sigma^2=100$)情形下的广播网络保密容量($B_{\text{tc}}^s\approx0.42\times10^{-6}$)仅约为弱相关情形($B_{\text{tc}}^s\approx1.6\times10^{-6}$)时的 1/4.从图中还可以看出,与两网络不存在相关性的情况相比,对于不同相关程度的两网络,此时我们不一定找到一个最佳的媒质接入概率 p 使得 B_{tc}^s 最大.然而,当相关性非常强时(如 $\nu=10^{-4},\sigma^2=100$),存在最优的 p 使 B_{tc}^s 最大;其余相关参数下,并不存在最佳

的 p.

5 结论

在本文中,我们提出了一种基于双变量泊松点过程的新型网络模型对存在相关性的合法广播网络和窃听网络进行建模.运用随机几何相关理论,针对一般衰落和瑞利衰落两种信道条件,分别推导了引发保密中断的平均相邻窃听节点的数量,并由此求得了安全广播传输容量.与不存在相关性的情形相比,结果显示,网络间的相关性会带来保密传输容量的损失,相关性越强,这种损失越明显.

参考文献

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

[2] Y Liang, H V Poor, S Shamai. Information theoretic security [J]. Foundations and Trends Communication Information Theory, 2009, 5(4): 355 – 580.

[3] A Wyner. The wire-tap channel[J]. Bell System Technical Journal, 1975, 54(8): 1355 – 1387.

[4] P K Gopala, L Lai, H E Gamal. On the secrecy capacity of fading channels[J]. IEEE Transactions on Information Theory, 2008, 54(10): 4687 – 4698.

[5] 王育民. Shannon 信息保密理论的新进展[J]. 电子学报, 1998, 26(7): 27 – 34.
Y M Wang. Developments in Shannon's theory of information secrecy[J]. Acta Electronica Sinica, 1998, 26(7): 27 – 34. (in Chinese)

[6] A Khisti, G W Wornell. Secure transmission with multiple antennas I: The MISOME wiretap channel[J]. IEEE Transactions on Information Theory, 2010, 56(7): 3088 – 3104.

[7] A Khisti, A Tchamkerten, G W Wornell. Secure broadcasting over fading channels[J]. IEEE Transactions on Information Theory, 2008, 54(6): 2453 – 2469.

[8] X Zhou, R K Ganti, J G Andrews, et al. On the throughput cost of physical layer security in decentralized wireless networks [J]. IEEE Transactions on Wireless Communications, 2011, 10 (8): 2764 – 2775.

[9] W C Ao, K C Chen. Broadcast transmission capacity of heterogeneous wireless ad hoc networks with secrecy outage constraints[A]. IEEE Proceeding of Globecom Conference[C]. USA: IEEE Press, 2011. 1 – 5.

[10] J E Paloheimo. A spatial bivariate Poisson distribution[J]. Biometrika, 1972, 59(2): 489 – 492.

[11] A Babaei, B Jabbari. Distance distribution of bivariate Poisson network nodes[J]. IEEE Communication Letters, 2010, 14 (9): 845 – 850.

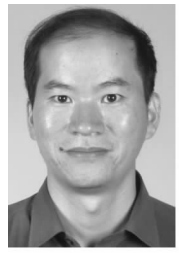
[12] P C Pinto, J Barros, M Z Win. Wireless physical-layer security: The case of colluding eavesdroppers[A]. IEEE Proceedings of International Symposium on Information Theory[C]. USA: IEEE Press, 2009. 2442 – 2446.

[13] Y Liang, H V Poor, L Ying. Secrecy throughput of MANETs with malicious nodes[A]. IEEE Proceedings of International Symposium on Information Theory[C]. USA: IEEE Press, 2009. 1189 – 1193.

[14] J Kingman. Poisson Processes[M]. Oxford: UK: Oxford University Press, 1993.

作者简介

孙晓惠　女,1989 年 1 月 13 日生于新疆省石河子市.现为北京邮电大学硕士,研究方向为无线 Ad hoc 网络容量与网络的安全性问题.
E-mail: sunxiaohui0113@gmail.com



尹长川　男,1968 年 10 月 4 日生于山东省临朐县.现为北京邮电大学教授,研究方向为无线通信中的信号处理与通信网理论.
E-mail: ccyin@bupt.edu.cn