文章编号: 1001-0920(2019)05-1043-06 DOI: 10.13195/j.kzyjc.2017.1491

无线多跳网络安全路由算法

冯 维, 杨凯通†, 徐永鑫, 吴端坡, 刘 晴

(杭州电子科技大学 通信工程学院，杭州 310018)

摘 要: 针对窃听者相互合作下的无线多跳网络,提出一种考虑物理层安全的路由算法. 该算法在假定未知窃听者位置及其信道状态信息 (CSI) 的前提下, 得到系统端到端安全连接概率 (EESCP) 表达式, 通过最大化网络EESCP,得到一种使用传统Bellman-Ford算法即可实现的最短路径路由算法,并在此基础上进一步提出一种改进的Bellman-Ford算法. 仿真结果表明,所提出的算法不仅适应于不同规模的网络,而且相较于传统算法能够极大地提高网络的安全性能.

关键词: 无线多跳网络；物理层安全；路由算法；端到端安全连接概率；最短路径路由

中图分类号: TP393 **文献标志码:** A

Secure routing in wireless multi-hop networks

FENG Wei, YANG Kai-tong†, XU Yong-xin, WU Duan-po, LIU Qing

(Communications Engineering Academy，Hangzhou Dianzi University，Hangzhou 310018，China)

Abstract: This paper proposes a physical-security-based routing algorithm for a wireless multi-hop network in the presence of multiple colluding eavesdroppers. The algorithm firstly obtains end-to-end secure connection probability (EESCP) without the knowledge of the locations of the eavesdroppers as well as the channel state information (CSI). Then, a shortest-path routing algorithm, which can be simply realized using traditional Bellman-Ford method, is introduced by solving the EESCP maximization problem. Furthermore, an improved Bellman-Ford algorithm is designed to get higher security level. The simulation results demonstrate that the proposed algorithm can be applied to a network of arbitrary size, and has significantly higher security performance compared with the traditional ones.

Keywords: wireless multi-hop network；physical layer security；routing algorithm；end-to-end secure connection probability；shortest-path routing

0 引 言

随着无线通信技术的发展,各种无线通信网络和网络协议[1]被广泛开发应用,但是无线信道的开放性使得无线通信的安全问题也日趋严峻[2]. 传统方法通过以密码学为基础的相关加密技术来解决这一问题[3],然而随着计算机运算速度的加快,破解技术进一步提高,这种基于网络层及以上各层的方法正面临着重大的挑战. 基于此,物理层安全技术[4]出现在公众视野. 物理层安全技术以窃听信道模型为基础,包含信道编码、秘钥协商、协作干扰等技术[5],作为上层安全的补充,具有可靠性高、计算量小、复杂度低、信道适应性好等特点,弥补了传统信息安全技术的不足,极大地增强了整个系统的安全性能.

目前已有大量文献针对物理层安全技术展开研究[6-7]. 文献[6]针对单跳网络,通过设计合理的天线选择技术提高合法用户的接收信噪比,并利用同频同时全双工技术加入人工噪声来降低窃听者端的接收信噪比,以实现信息在物理层的安全传输. 文献[7]讨论了网络存在一个或多个窃听者的情形中,单个源-目的对的安全通信问题. 以上研究都取得了较好的结果,但是这些研究结果针对的都是单跳或者两跳中继网络,无法直接应用到无线多跳网络.

目前,还只有少量文献针对无线多跳网络的物理层安全问题展开研究. 文献[8]利用随机几何知识分

收稿日期: 2017-11-06；**修回日期:** 2018-01-16.

基金项目: 国家自然科学基金项目(61671192, 61501158)；浙江省自然科学基金项目(LY16F010012, LY14F010019)；浙江省教育厅一般科研项目(Y201533647)；浙江省科协青年科技人才培育工程项目(2016YCGC009)；杭州电子科技大学“电子科学与技术”浙江省一流学科A类开放基金项目(GK178800207001/024).

责任编委: 李忠奎.

作者简介: 冯维(1984−), 女, 讲师, 博士, 从事无线网络资源分配优化算法及其应用等研究；吴端坡(1993−), 男, 讲师, 博士, 从事无线网络通信等研究.

†通讯作者. E-mail: ykt1408@163.com.

析了无线网络中合法用户和窃听者的密度对物理层安全性能的影响,并在此基础上得到了一个通信安全图,同时定义了任意合法节点与其邻居间的安全容量表达式,但得到的是一种极限结果,只能对算法最终结果进行检验,并没有设计具体的实现算法. 文献[9]通过波束赋形等方法提高物理层安全性能,但是其研究基于信道状态信息(CSI)或窃听者位置已知这样一种假设. 这种假设通常不符合实际情况,因为窃听者一般以一种被动的方式工作,即他们只是试图从合法的节点中听到尽可能多的信息,而不是试图主动地阻止(即通过干扰,信号插入)合法的节点,所以合法用户往往不知道窃听者的位置及其CSI.

基于此,本文针对中继节点采用解码转发模式的无线多跳网络,考虑窃听者位置和CSI未知且窃听者相互勾结的场景,提出一种安全路由算法. 该算法首先根据信息论角度的物理层安全定义,定义已知路由的端到端安全连接概率(End-to-end secure connection probability, EESCP),并且求得该连接概率的表达式;然后基于该表达式,得到能最大化EESCP的路由算法,并进一步对其进行改进. 该路由算法可以利用经典Bellman-Ford算法实现,具有良好的安全性和可扩展性.

1 系统模型

1.1 系统模型

本文考虑一个无线多跳网络中存在多个相互勾结的窃听者E_j,其集合为G,可以表示为$G=\{E_j|j=1,2,\cdots\}$. 窃听者密度为λ,合法节点和窃听者位置均服从泊松分布,窃听者处于被动状态,窃听者位置和CSI均未知. 用$\varphi=\langle N_1,N_2,\cdots,N_{M+1}\rangle$表示一条$M$跳路由,$N_i$为该路径上的第$i$个节点,$P_{N_i}$为节点$N_i$的发射功率. 假定网络中每个节点都配备全向天线和有限的能量供应,节点工作在时分复用模式,中继节点采用解码转发方式传输数据.

1.2 问题建模

信息从节点N_i传输到N_{i+1}时,合法节点N_{i+1}和窃听者E_j的接收信噪比$\lambda_{N_iN_{i+1}}$和$\lambda_{N_iE_j}$分别为

$$\lambda_{N_iN_{i+1}}=\frac{P_{N_i}}{d^{\alpha}_{N_iN_{i+1}}}|h_{N_iN_{i+1}}|^2, \tag{1}$$

$$\lambda_{N_iE_j}=\frac{P_{N_i}}{d^{\alpha}_{N_iE_j}}|h_{N_iE_j}|^2. \tag{2}$$

其中:P_{N_i}为合法节点N_i的发送功率,$d_{N_iN_{i+1}}$和$h_{N_iN_{i+1}}$分别为节点N_i与N_{i+1}之间的距离和信道衰落系数,α为路损因子,$d_{N_iE_j}$和$h_{N_iE_j}$分别为节点N_i与E_j之间的距离与信道衰落系数. 本文假定$|h_{N_iN_{i+1}}|^2$和$|h_{N_iE_j}|^2$服从均值为1的指数分布,根据文献[10]安全速率的定义,可得链路的单跳保密速率为

$$[\log_2(1+\lambda_{N_iN_{i+1}})-\log_2(1+\lambda_{N_iE_j})]^+, \tag{3}$$

其中$[x]^+=\max(x,0)$.

因为中继节点采用解码转发方式,所以窃听者可以联合多跳的信号窃取所传信息. 对于已知路由φ,其可实现的保密速率可表示为

$$\Big[\log_2\Big(1+\min_{i=1,2,\cdots,M}\lambda_{N_iN_{i+1}}\Big)-\log_2\Big(1+\sum_{E_j}\sum_{i=1}^{M}\lambda_{N_iE_j}\Big)\Big]^+. \tag{4}$$

其中:$\min\limits_{i=1,2,\cdots,M}\lambda_{N_iN_{i+1}}$为消息传输路径上合法节点接收的最小信噪比,只有当整条路径上最危险的那一跳安全时,该信息才能最终安全传输;$\sum\limits_{E_j}\sum\limits_{i=1}^{M}\lambda_{N_iE_j}$表示在窃听者相互勾结、互相传递消息的情况下,窃听者所能从整条路径获得的最大信噪比. 当整条路径的保密速率大于0时,认为该路由是安全的,所以建模该路径EESCP为

$$Q=\Pr\Big\{\log_2\Big[1+\min_{i=1,2\cdots M}\Big(\frac{P_{N_i}}{d^{\alpha}_{N_iN_{i+1}}}|h_{N_iN_{i+1}}|^2\Big)\Big]-\log_2\Big[1+\sum_{E_j\in G}\sum_{i=1}^{M}\Big(\frac{P_{N_i}}{d^{\alpha}_{N_iE_j}}|h_{N_iE_j}|^2\Big)\Big]>0\Big\}, \tag{5}$$

其中$\Pr\{\cdot\}$表示概率. 由式(5)可知,EESCP越大说明路由安全的程度越高,因此本文以获取最大的EESCP为目标来求得路由算法,即寻求满足下式的路由:

$$\varphi=\arg\max_{\{\varphi_i|i=1,2,\cdots\}}Q, \tag{6}$$

其中$\{\varphi_i\mid i=1,2\cdots\}$表示从源到目的地的路由集合.

2 安全路由算法

2.1 EESCP

为了求得满足式(6)的路由,首先将式(5)改写为

$$Q=\Pr\Big\{\log_2\Big[\frac{1+\min\limits_{i=1,2,\cdots,M}\Big(\frac{P_{N_i}}{d^{\alpha}_{N_iN_{i+1}}}|h_{N_iN_{i+1}}|^2\Big)}{1+\sum\limits_{E_j\in G}\sum\limits_{i=1}^{M}\Big(\frac{P_{N_i}}{d^{\alpha}_{N_iE_j}}|h_{N_iE_j}|^2\Big)}\Big]>0\Big\}. \tag{7}$$

根据对数函数的性质,式(7)可等效为

$$Q=\Pr\Big\{\Big[1+\min_{i=1,2,\cdots,M}\Big(\frac{P_{N_i}}{d^{\alpha}_{N_iN_{i+1}}}|h_{N_iN_{i+1}}|^2\Big)\Big]>\Big[1+\sum_{E_j\in G}\sum_{i=1}^{M}\Big(\frac{P_{N_i}}{d^{\alpha}_{N_iE_j}}|h_{N_iE_j}|^2\Big)\Big]\Big\}. \tag{8}$$

进一步,将式(8)简化为

$$Q=\Pr\Big\{\min_{i=1,2,\cdots,M}\Big(\frac{P_{N_i}}{d^{\alpha}_{N_iN_{i+1}}}|h_{N_iN_{i+1}}|^2\Big)>\sum_{E_j\in G}\sum_{i=1}^{M}\Big(\frac{P_{N_i}}{d^{\alpha}_{N_iE_j}}|h_{N_iE_j}|^2\Big)\Big\}. \tag{9}$$

由于$|h_{N_iN_{i+1}}|^2$服从均值为1的指数分布,由概率论最值分布可知,$\min\limits_{i=1,2,\cdots,M}\Big(\frac{P_{N_i}}{d^{\alpha}_{N_iN_{i+1}}}|h_{N_iN_{i+1}}|^2\Big)$是服从均值为$\dfrac{1}{\sum\limits_{i=1}^{M}\frac{d^{\alpha}_{N_iN_{i+1}}}{P_{N_i}}}$的指数分布,令

$$z=\min_{i=1,2,\cdots,M}\Big(\frac{P_{N_i}}{d^{\alpha}_{N_iN_{i+1}}}|h_{N_iN_{i+1}}|^2\Big),$$

$$t=\sum_{E_j\in G}\sum_{i=1}^{M}\Big(\frac{P_{N_i}}{d^{\alpha}_{N_iE_j}}|h_{N_iE_j}|^2\Big),$$

$f(z,t)$为z和t的联合概率密度. 因为z,t相互独立,所以$f(z,t)=f(z)f(t)$,有

$$\begin{aligned}Q=\Pr(z>t)&=E_{G_E}\Big\{\int_{-\infty}^{+\infty}\int_{t}^{+\infty}f(z,t)\mathrm{d}z\mathrm{d}t\Big\}=\\&E_{G_E}\Big\{\int_{-\infty}^{+\infty}f(t)\int_{t}^{+\infty}f(z)\mathrm{d}z\mathrm{d}t\Big\}=\\&E_{G_E}\Big\{\int_{-\infty}^{+\infty}f(t)\mathrm{e}^{-\sum\limits_{i=1}^{M}\frac{d^{\alpha}_{N_iN_{i+1}}}{P_{N_i}}t}\mathrm{d}t\Big\}=\\&E_{t,G_E}\{\mathrm{e}^{-\sum\limits_{i=1}^{M}\frac{d^{\alpha}_{N_iN_{i+1}}}{P_{N_i}}t}\}.\end{aligned} \tag{10}$$

其中:$E\{\cdot\}$为求均值符号,G_E为窃听者的位置. 令

$$t=\sum_{l=1}^{W}\frac{P_l}{d^{\alpha}_l}|h_l|^2=\sum_{l=1}^{W}\beta_l|h_l|^2.$$

其中:l为网络中存在的窃听链路数,P_l为链路l的发送功率,W为总的窃听链路数,$d_1,d_2,\cdots,d_l,\cdots,d_W$为按照由小到大排列后的窃听链路距离变量,$\beta_l=d^{\alpha}_l/P_l$. 假设所有$\beta$中有$a$个不相等的数值,用$\beta_1,\beta_2,\cdots,\beta_a$表示,$k_i$表示每个$\beta_i$中对应相等元素的个数,所以$k_1+k_2+\cdots+k_a=W$. 根据文献[11]可得

$$f(t)=\Big\{\sum_{i=1}^{a}\beta_i^{k_i}\mathrm{e}^{-t\beta_i}\sum_{j=1}^{k_i}\frac{(-1)^{k_i-j}}{(j-1)!}t^{j-1}\times\sum_{m_1+\cdots+m_a=k_i-j}\prod_{l=1,l\neq i}^{a}\binom{k_l+m_l-1}{m_l}\times\frac{\beta_l^{k_l}}{(\beta_l-\beta_i)^{k_l+m_l}}I_{(0,+\infty)}(t)\Big\}. \tag{11}$$

将式(11)代入(10),可得

$$\begin{aligned}Q=&E_{G_E}\Big\{\int_{-\infty}^{+\infty}\sum_{i=1}^{a}\beta_i^{k_i}\mathrm{e}^{-t\beta_i}\sum_{j=1}^{k_i}\frac{(-1)^{k_i-j}}{(j-1)!}t^{j-1}\times\sum_{m_1+\cdots+m_a=k_i-j}\prod_{l=1,l\neq i}^{a}\binom{k_l+m_l-1}{m_l}\times\frac{\beta_l^{k_l}}{(\beta_l-\beta_i)^{k_l+m_l}}I_{(0,+\infty)}(t)\mathrm{e}^{-\sum\limits_{i=1}^{M}\frac{d^{\alpha}_{N_iN_{i+1}}}{P_{N_i}}t}\mathrm{d}t\Big\}=\\&E_{G_E}\Big\{\sum_{i=1}^{a}\beta_i^{k_i}\sum_{j=1}^{k_i}\frac{(-1)^{k_i-j}}{(j-1)!}\times\sum_{m_1+\cdots+m_a=k_i-j}\prod_{l=1,l\neq i}^{a}\binom{k_l+m_l-1}{m_l}\times\frac{\beta_l^{k_l}}{(\beta_l-\beta_i)^{k_l+m_l}}\int_0^{+\infty}t^{j-1}\mathrm{e}^{-t(\sum\limits_{i=1}^{M}\frac{d^{\alpha}_{N_iN_{i+1}}}{P_{N_i}}+\beta_i)}\mathrm{d}t\Big\}=\\&E_{G_E}\Big\{\sum_{i=1}^{a}\beta_i^{k_i}\sum_{j=1}^{k_i}\frac{(-1)^{k_i-j}}{(j-1)!}\times\sum_{m_1+\cdots+m_a=k_i-j}\prod_{l=1,l\neq i}^{a}\binom{k_l+m_l-1}{m_l}\times\frac{\beta_l^{k_l}}{(\beta_l-\beta_i)^{k_l+m_l}}\times\frac{1}{\Big(\sum\limits_{i=1}^{M}\frac{d^{\alpha}_{N_iN_{i+1}}}{P_{N_i}}+\beta_i\Big)^{j}}\Gamma(j)\Big\},\end{aligned} \tag{12}$$

其中$\Gamma(\cdot)$为伽玛分布. 假设所有节点的发射功率相同,将β代入式(12),可得

$$\begin{aligned}Q=&E_{G_E}\Big\{\sum_{i=1}^{a}d_i^{\alpha k_i}\sum_{j=1}^{k_i}\frac{(-1)^{k_i-j}}{(j-1)!}\times\sum_{m_1+\cdots+m_a=k_i-j}\prod_{l=1,l\neq i}^{a}\binom{k_l+m_l-1}{m_l}\times\frac{d_l^{\alpha k_l}}{(d_l^{\alpha}-d_i^{\alpha})^{k_l+m_l}}\times\frac{1}{\Big(\sum\limits_{i=1}^{N}d^{\alpha}_{N_iN_{i+1}}+d_i^{\alpha}\Big)^{j}}\Gamma(j)\Big\}.\end{aligned} \tag{13}$$

实际场景中窃听者到合法节点的距离很少有完全一样的,所以进一步假设所有β均不一样,可得到如下EESCP:

$$Q=E_{G_E}\Big\{\sum_{l=1}^{W}\frac{d_1^\alpha d_2^\alpha\cdots d_W^\alpha}{\prod\limits_{o=1,o\neq l}^{W}(d_o^\alpha-d_l^\alpha)}\times\frac{1}{\sum\limits_{i=1}^{N}d_{N_iN_{i+1}}^\alpha+d_l^\alpha}\Big\}. \tag{14}$$

2.2 路由算法

下面分析所得到的端到端安全连接概率Q值. 对于式(14),$d_1,d_2,\cdots,d_l,\cdots,d_W$均为只与窃听者位置相关的距离分量,由统计几何知识可知,最终可以转化为对窃听者位置的积分. 令

$$S=\sum_{l=1}^{W}\frac{d_1^\alpha d_2^\alpha\cdots d_w^\alpha}{\prod\limits_{o=1,o\neq l}^{W}(d_o^\alpha-d_l^\alpha)}\times\frac{1}{\sum\limits_{i=1}^{N}d_{N_iN_{i+1}}^\alpha+d_l^\alpha},$$

进一步根据单个窃听者远、近两种情况分析系统的端到端安全连接概率Q.

1) 当$d_l^\alpha\gg\sum\limits_{i=1}^{N}d_{N_iN_{i+1}}^\alpha$或$d_l^\alpha\approx\sum\limits_{i=1}^{N}d_{N_iN_{i+1}}^\alpha$时,即对于较大的窃听距离,$S\approx\sum\limits_{l=1}^{W}\frac{d_1^\alpha d_2^\alpha\cdots d_w^\alpha}{\prod\limits_{o=1,o\neq l}^{W}(d_o^\alpha-d_l^\alpha)}\times\frac{1}{d_l^\alpha}$或$S\approx\sum\limits_{l=1}^{W}\frac{d_1^\alpha d_2^\alpha\cdots d_w^\alpha}{\prod\limits_{o=1,o\neq l}^{W}(d_o^\alpha-d_l^\alpha)}\times\frac{1}{2d_l^\alpha}$,由结果可见,$\sum\limits_{i=1}^{N}d_{N_iN_{i+1}}^\alpha$的大小对结果影响很小,可以忽略. 对应的物理含义是:远距离的窃听路径对消息传输安全影响很小.

2) 当$d_l^\alpha\ll\sum\limits_{i=1}^{N}d_{N_iN_{i+1}}^\alpha$时,即对于较小的窃听距离,$S\approx\frac{1}{\sum\limits_{i=1}^{N}d_{N_iN_{i+1}}^\alpha}\sum\limits_{l=1}^{W}\frac{d_1^\alpha d_2^\alpha\cdots d_w^\alpha}{\prod\limits_{o=1,o\neq l}^{W}(d_o^\alpha-d_l^\alpha)}$. 可以看出,$\sum\limits_{i=1}^{N}d_{N_iN_{i+1}}^\alpha$的作用不能忽略. 这种选择在物理上可以解释为:当窃听者处于很近的位置时,选择的路由将在很大程度上影响系统的安全概率.

对于系统拓扑而言,针对选定的路由,可以分为以下3种情况讨论系统的EESCP:

1) 如果$d_1,d_2,\cdots,d_l,\cdots,d_W$均较大,则可得$Q\approx E_{G_E}\Big\{\sum\limits_{l=1}^{W}\frac{d_1^\alpha d_2^\alpha\cdots d_w^\alpha}{\prod\limits_{o=1,o\neq l}^{W}(d_o^\alpha-d_l^\alpha)}\times\frac{1}{d_l^\alpha}\Big\}$为一个很大的常数. 这种选择基于这样一种事实:如果窃听者位置都相对较远,则系统一定能得到很大的安全连接概率.

2) 如果$d_1,d_2,\cdots,d_l,\cdots,d_W$均较小,即安全性能最差的情况,则有

$$Q=\frac{1}{\sum\limits_{i=1}^{N}d_{N_iN_{i+1}}^\alpha}\times E_{G_E}\Big\{\sum_{l=1}^{W}\frac{d_1^\alpha d_2^\alpha\cdots d_w^\alpha}{\prod\limits_{o=1,o\neq l}^{W}(d_o^\alpha-d_l^\alpha)}\Big\}=K\times\frac{1}{\sum\limits_{i=1}^{N}d_{N_iN_{i+1}}^\alpha},$$

其中$K=E_{G_E}\Big\{\sum\limits_{l=1}^{W}\frac{d_1^\alpha d_2^\alpha\cdots d_w^\alpha}{\prod\limits_{o=1,o\neq l}^{W}(d_o^\alpha-d_l^\alpha)}\Big\}$为一正的常数,取决于窃听者位置服从的分布函数. 这个结果意味着:如果选定路由的$\sum\limits_{i=1}^{N}d_{N_iN_{i+1}}^\alpha$越小,则系统便能拥有更大的安全连接概率.

3) 如果$d_1,d_2,\cdots,d_l,\cdots,d_W$部分较大,部分较小,则综合1)和2)可知,系统的安全连接概率既取决于窃听者的位置,也取决于$\sum\limits_{i=1}^{N}d_{N_iN_{i+1}}^\alpha$的大小. 窃听者位置通常是未知的,能够控制的只能是使得$\sum\limits_{i=1}^{N}d_{N_iN_{i+1}}^\alpha$最小.

综合1)~3),为了满足条件(6),需要找到满足下式的路由:

$$\min\ \sum_{i=1}^{N}d_{N_iN_{i+1}}^\alpha. \tag{15}$$

很明显,式(15)通过经典的Bellman-Ford算法非常容易实现,该最短路径算法(算法III)的路由权重函数为

$$w(d)=d_{N_iN_{i+1}}^\alpha. \tag{16}$$

同时,考虑到这样一个事实:当链路跳数增加时,给窃听者带来更多窃听机会,使窃听信噪比更大,将所选路由的跳数这一因素考虑进去,进一步优化结果,得到如下路由目标:

$$\min\ M\sum_{i=1}^{N}d_{N_iN_{i+1}}^\alpha. \tag{17}$$

该路由算法由于跳数与距离耦合在一起,非常难实现,所以使用下列改进的Bellman-Ford算法实现.

Step 1: 在每H跳中以$d_{N_iN_{i+1}}^\alpha$为权值,通过遍历找到该跳的最短路由集合R_1,由于权值中没有负值,在运行Bellman-Ford算法时不必考虑存在环路无法收敛的情况.

Step 2: 计算集合R_1中所有路由的指标值

$M\sum_{i=1}^{N} d_{N_iN_{i+1}}^{\alpha}$,得到指标集合$R_2$.

Step 3: 比较集合R_2中所有值,以最小值为该跳的选择路由.

Step 4: 回到Step 1进行$H+1$跳的循环,直到找到目的节点为止.

3　仿真与性能分析

为了分析路由算法的性能,在第1阶段仿真不同的节点密度下最短路径算法、改进的最短路径算法和采用遍历的方法求出的最佳路由之间的性能对比,在第2个阶段进一步将所提出算法与最小跳数路由算法进行比较.

3.1　不同密度下的性能对比

本节在不同的节点密度下仿真算法的性能,仿真参数如下: 网络拓扑图选取为50 m × 50 m的正方形区域,节点位置服从泊松分布,节点密度较低时,共生成52个节点,其中1和52分别代表源节点和目的节点. 节点密度较高时,共生成122个节点,其中1和122分别代表源节点和目的节点. $\alpha=4$,窃听者密度λ为10^{-6}. 用算法I,算法II和算法III分别代表遍历法、改进的最短路径法和最短路径算法.

图1为低节点密度下3种算法所选择的路由对比图,相应的EESCP依次为0.997 4、0.997 2、0.996 8,可以看出算法I～算法III是非常接近的,尤其是算法I和算法II,只有一跳不同. 综合考虑了跳数和节点间距离之后的算法II计算出的路由显然比仅考虑节点距离的算法III更接近于遍历出的基准路由. 通过EESCP的值也可以明显看出,所提出的算法II和算法III具有非常好的安全性能,其中算法II性能更好.

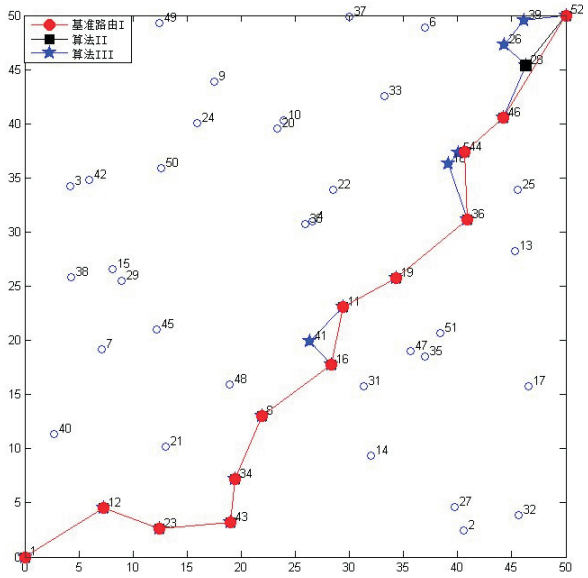

图1　低节点密度时算法路由示例

图2进一步仿真了高节点密度下相应路由对比图,相应的EESCP依次为0.998 0、0.997 9、0.997 4. 综合两者可以看出算法I～算法III仍然非常接近,且算法I和算法II的安全连接概率几乎相等. 相对于低节点密度时,安全连接概率随着节点数目增多相应有一定增加. 这是因为随着节点密度增加,网络可选的路由数目也进一步增加,安全连接概率也有一定提高.

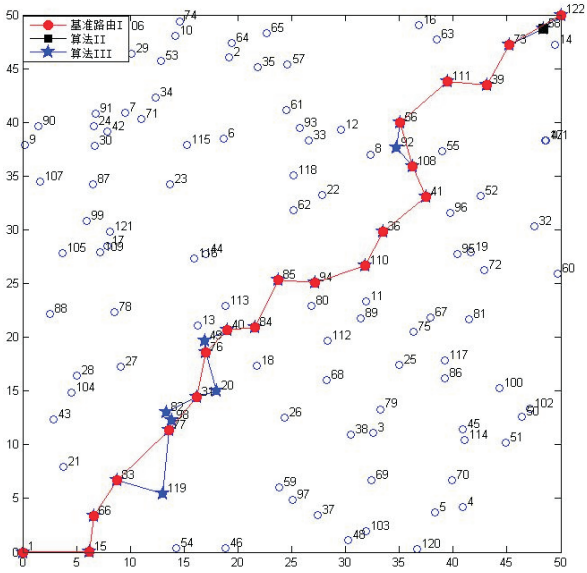

图2　高节点密度时算法路由示例

综上可知,所提出的优化算法适用于低密度和高密度的所有情况.

3.2　与其他路由算法性能对比

本节选取没有考虑物理层安全的最小跳数路由算法作为比较,进一步分析所提出算法的安全性能. 下面用算法IV表示该最小跳数路由算法.

首先,比较了几种路由算法在窃听者密度为λ为10^{-5}时的安全性能. 其他仿真参数均与第3.1节低节点密度仿真场景相同. 由图3可以看出,算法IV选择的路径偏离最优路径最远. 相应的EESCP依次为0.861 3、0.844 2、0.828 5、0.765 0. 相对于所提出算法,算法IV具有最小的EESCP值. 这是因为: 算法IV选择最小跳数N时,也就意味着它选择的每一跳距离d都是非常大的,所以其使得$d_{N_iN_{i+1}}^{\alpha}$的总和大于所提出算法,其EESCP值更小,安全性较低.

同时仿真了不同窃听者密度下各算法的EESCP. 随着窃听者密度的增加,可供网络选择的安全路径也越来越少,离所选路由较近的窃听者数目也越来越多,窃听距离也越来越近,这一情况对于任何一个路由算法而言都是无法避免的,所以所有路由算法的EESCP都越来越低. 同时可以看到,在窃听者密度为10^{-5}时,所提出算法比算法IV的EESCP值高

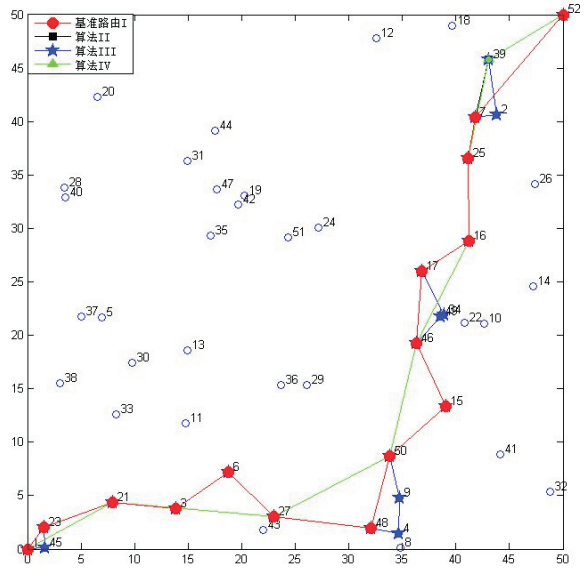

图 3 不同路由示例

2%; 在窃听者密度为10^{-4}时, 所提出算法比算法IV的EESCP值高8%; 在窃听者密度为10^{-3}时, 所提出算法比算法IV的EESCP值高近20%. 也就是说, 所提出算法性能下降速度远低于最小跳数路由算法, 在窃听者密度越高时, 所提出算法相对于传统算法的优势也越明显.

表 1 不同窃听者密度下各算法安全概率

λ	10^{-6}	10^{-5}	10^{-4}	10^{-3}
基准路由I	0.996 3	0.980 5	0.750 9	0.373 0
算法II	0.996 1	0.970 5	0.727 9	0.343 8
算法III	0.995 6	0.960 1	0.719 2	0.309 1
算法IV	0.994 8	0.923 7	0.644 4	0.165 4

4 结 论

本文针对解码转发模式下的无线多跳网络, 提出了一种考虑物理层安全的路由算法. 该算法考虑窃听者的位置以及CSI均为未知这一更加现实的场景, 设计出一种基于传统Bellman-Ford算法即可实现的路由算法, 在此基础上, 得到的改进Bellman-Ford算法更进一步地提高了系统的安全性能. 仿真结果表明, 该算法不仅在低密度的网络能找到安全性能较好的路由, 在高密度网络也同样适用. 而且, 由与传统最小跳数路由的对比也可以发现, 所提出算法具有更高的安全性能, 特别是随着窃听者密度的增加, 这种性能优势也愈加明显.

参考文献(References)

[1] 梁英, 于海斌, 曾鹏. 应用PSO优化基于分簇的无线传感器网络路由协议[J]. 控制与决策, 2006, 21(4): 453-456.
(Liang Y, Yu H B, Zeng P. Application of PSO to optimize routing protocol based on clustering wireless sensor networks[J]. Control and Decision, 2006, 21(4): 453-456.)

[2] 吴数根. 无线通信系统安全与策略研究[D]. 北京: 北京邮电大学信息工程学院, 2008.
(Wu S G. Wireless communication system security and strategy research[D]. Beijing: College of Information and Engeneering, Beijing University of Posts and Telecommunications, 2008.)

[3] 戴必峰. 密码加密技术概述[C]. 中国航海学会通信导航专业委员会2007年学术年会. 大连: 通力电梯有限公司, 2007: 231-234.
(Dai B F. Overview of cryptographic encryption technology[C]. 2007 Annual Conf of Communication and Navigation Committee of China Maritime Society. Dalian: Tongli Elevator Company, 2007: 231-234.)

[4] 龙航, 袁广翔, 王静, 等. 物理层安全技术研究现状与展望[J]. 电信科学, 2011, 27(9): 60-65.
(Long H, Yuan G X, Wang J, et al. Physical layer security technology research status and prospects[J]. Telecommunications Science, 2011, 21(9): 60-65.)

[5] 刘在爽, 王坚, 孙瑞, 等. 无线通信物理层安全技术综述[J]. 通信技术, 2014, 47(2): 128-135.
(Liu Z S, Wang J, Sun R, et al. Wireless communication physical layer security technology overview[J]. Communication Technology, 2014, 47(2): 128-135.)

[6] 张亚军, 梁涛, 柳永祥, 等. 联合发端天线选择和收端人工噪声的物理层安全传输方法[J]. 电子与信息学报, 2015, 27(9): 2183-2190.
(Zhang Y J, Liang T, Liu Y X, et al. Physical layer safe transmission method for joint origin antenna selection and terminating artificial noise[J]. J of Electronics and Information Technology, 2015(9): 2183-2190.)

[7] Dong L, Han Z, Petropulu A P, et al. Improving wireless physical layer security via cooperating relays[J]. IEEE Trans on Signal Processing, 2010, 58(3): 1578-1888.

[8] Pinto P C, Barros J. Physical-layer security in stochastic wireless networks[C]. Int Conf on Communication Systems. Singapore: IEEE, 2009: 975-979.

[9] He B, Zhou X, Abhayapala T D. Wireless physical layer security with imperfect channel state information: A survey[J]. ZTE Technology J, 2013, 11(3): 11-19.

[10] Zhou X, Ganti R K, Andrews J G. Secure wireless network connectivity with multi-antenna transmission[J]. IEEE Trans on Wireless Communications, 2011, 10(2): 425-430.

[11] Jasiulewicz H, Kordecki W. Convolutions of erlang and of pascal distributions with applications to reliability[J]. Demonstratio Mathematica, 2003, 36(1): 231-238.

(责任编辑: 郑晓蕾)