doi:10.3969/j.issn.1000-436x.2014.11.008

认知无线 Mesh 网络中满足 QoS 的高吞吐量安全路由协议

邝祝芳[1,2]，陈志刚[2]，王国军[2]，刘蕙[3]

(1. 中南林业科技大学 计算机与信息工程学院，湖南 长沙 410004；
2. 中南大学 软件学院，湖南 长沙 410083；3. 密苏里州立大学 计算机科学系，密苏里州 斯普林菲尔德 65897)

摘 要：提出了一种综合考虑链路安全、链路冲突、链路可靠度与链路可用带宽的路由判据 SIEB。SIEB 包括链路安全和链路性能 2 个方面，在 SIEB 的链路安全权值计算中，为了抵御各种洞攻击，提出了基于两跳邻居反馈的链路信任值计算方法。在此基础上，提出了链路安全权值计算算法 LSWC 和链路性能权值计算算法 LSPC，提出了分布式满足 QoS 约束的路由协议 SIEBP，SIEBP 的目标是：构造安全的路由路径，并且最大化网络吞吐量。仿真结果表明，SIEBP 能达到预定目标，构造的路径能抵御黑洞、灰洞、虫洞等攻击，并且获得了较高的网络吞吐量。

关键词：认知无线 Mesh 网络；安全路由；链路冲突；链路可用带宽；路径可靠度
中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2014)11-0069-12

Secure and high throughput routing protocol with QoS constraints in cognitive wireless Mesh networks

KUANG Zhu-fang[1,2], CHEN Zhi-gang[2], WANG Guo-jun[2], LIU Hui[3]

(1. School of Computer and Information Engineering, Central South University of Forestry & Technology, Changsha 410004, China;
2. School of Software, Central South University, Changsha 410083, China;
3. Department of Computer Science, Missouri State University, Springfield, MO, 65897, the United States)

Abstract: A routing metric SIEB which includes link security, link conflict, link reliability and link available bandwidth was proposed. The SIEB includes link security and link performance two aspects. In order to resist various hole attack, the link trust value based on two hop neighbor feedback is computed in link security weight computing of SIEB. On this basis, a link security weight computing algorithm LSWC and a link performance weight computing algorithm LSPC were proposed, and a distributed routing protocol SIEBP with QoS constraints in cognitive wireless Mesh network was proposed. Finding safety routing path and maximizing the network throughput are the objective of SIEBP. Simulation results show that SIEBP routing protocol can achieve expectation goal. It can not only find safety routing path which can resist black hole attack, gray hole attack and worm hole attack, but also obtain a higher network throughput.

Key words: cognitive wireless Mesh network; secure routing; link conflict; link available bandwidth; link reliability

1 引言

认知无线电(CR, cognitive radio)技术于 1999 年由 Mitola 博士首次提出，其核心功能是对频谱进行感知，并有效地进行频谱资源的分配和共享[1]。次用户(SU, secondary user)在不干扰主用户(PU, primary user)的前提下，伺机使用这些 PU 未使用的频谱空穴[2]。

认知无线 Mesh 网络（CWMN, cognitive wireless Mesh network）是一种结合了 CR 的无线 Mesh

收稿日期：2014-08-20；**修回日期**：2014-10-22
基金项目：国家自然科学基金资助项目(61309027, 61379057, 61073186)；湖南教育厅优秀青年基金资助项目(13B148)；中国博士后科学基金资助项目(2013M542136)
Foundation Items: The National Natural Science Foundation of China (61309027, 61379057, 61073186); Scientific Research Fund of Hunan Provincial Education Department (13B148); Supported by China Postdoctoral Science Foundation (2013M542136)

网络[3]。CWMN 中的 Mesh 节点能够感知 PU 未使用的频谱，动态地接入到这些空闲频谱，提高网络吞吐量。

CWMN 与其他无线网络一样，也面临着被窃听、恶意干扰、选择性转发等常见的安全威胁。CWMN 是一种动态的网络，这种动态性主要来源于 2 方面：一是 CR-Mesh 节点可用频谱动态变化，二是 CWMN 网络拓扑结构动态变化。这种动态性给 CWMN 带来了新的安全挑战。静态的安全防御措施已经不能提供安全的保证[4]，CWMN 作为一种新型的无线网络，其安全问题是一个需要研究的重要课题。

在 CWMN 中，CR-Mesh 节点伺机利用空闲频谱，提高频谱利用率、网络吞吐量的同时，也带来了新的安全挑战。随着 CR 技术的提出，学者们针对物理层和 MAC 层开展了一些研究[5~7]，比如物理层的攻击有模仿主用户(PUE, primary user emulation)攻击[8]、频谱感知数据篡改(SSDF, spectrum sensing data falsification) 攻击[9]等；MAC 层的攻击有拒绝服务(DoS, denial of service)攻击[10]、报告错误选择帧(reporting false selection frame)攻击[11]等。

主要研究的是认知无线 Mesh 网络中满足 QoS 约束的安全路由与频谱(信道)分配问题。目标是构造能抵御黑洞、灰洞、虫洞等攻击的安全路由路径的情况下，提高网络吞吐量，达到路径安全与高吞吐量同时优化的目的。QoS 约束指带宽约束。

近年来，针对无线 Mesh 网络[12,13]、无线 ad hoc 网络[14]、无线传感器网络[15]等无线多跳网络中的安全路由问题，已经取得了较多的研究成果。但是这些研究成果不能直接应用于认知无线 Mesh 网络。

随着 CR 的出现，已提出认知无线网络中的路由指标[16]主要关注网络吞吐量、延迟、链路稳定性等性能，较少考虑网络安全。针对 CWMN 中路由算法构造的单条路径可能没有可用信道的问题，提出了集中式的自适应满足 QoS 约束的多路径构造与频谱分配算法 SA2JR，目标是最大化无线业务接收率[4]。DING 等[17]研究了认知无线 Mesh 网络中多源的视频点播问题，目标是最小化单个会话消耗的总带宽，单个会话消耗的总带宽越小，则同时会话的数目越大。MUMEY 等[18]以最大化吞吐量为目标，提出了一种认知无线 Mesh 网络中基于动态规划的路由与信道分配方法。

CWMN 中安全路由问题目前处于研究的早期阶段，研究成果还很少，面临较多挑战。针对认知无线多跳网络的安全路由问题取得了一些研究成果[19~26]。

WU[19]针对认知无线 Mesh 网络中，由于动态频谱、动态拓扑给多跳路由带来易受攻击性，提出了基于信任机制的信道分配和路由模式，并且在信任机制的计算中还采用了入侵检测技术。GUO[20]研究了认知无线网络中考虑最优能耗的安全路由问题，首先，将原问题转化为 0~1 整数规划问题，然后，提出了基于信任机制的最优能耗安全路由算法 SDRA。

YUAN[21]提出了新的认知无线网络中的路由攻击 RPU(routing toward primary user)，在 RPU 攻击中，恶意节点连续路由大量数据分组到主用户，目的是对主用户产生干扰，增加次用户的传输延迟。针对 RPU 攻击，提出了基于信任度传播的机制，首先构造一条从源点到目的节点的初始路由路径，在初始路径上的所有节点都记录着其他节点的信度信息，源节点利用最后的信道值，能检测出恶意节点。

ZHU[22]针对认知无线网络中的干扰攻击(jamming attack)，提出了基于博弈理论的动态安全路由框架。HOW[23]针对认知无线网络中自私节点的存在，提出了跨层的自私避免路由协议 SARP。ZHANG[24]针对认知无线网络中网络层受到的选择性转发攻击，提出了基于信任评估的安全信任模型，以及基于信任值的奖惩机制。JO[25]研究了认知无线 ad hoc 网络中的自私攻击，并且提出了自私攻击检测技术 COOPON。LI 研究了认知无线网络中，当主用户需要其授权频谱时，次用户必须进行频谱切换时容易受到的一种跟踪用户攻击 (TUA, tacking user attack)，针对 TUA，提出了信道选择信息隐藏模式 CSIH。SORRELLS[26]针对认知无线网络中的异常频谱使用攻击(ASUA, anomalous spectrum usage attack)，提出了一种跨层的安全框架。

虽然 CWMN 和认知移动自组织网络（CRAHN, cognitive radio ad hoc network）都属于认知多跳网络，但是已有研究主要针对于 CRAHN，CWMN 与 CRAHN 的区别在于其骨干网静止，并且没有能量限制。

研究工作的创新如下：1) 研究认知无线 Mesh 网络中满足 QoS 约束的安全路由与频谱分配问题，是为了构造安全路由路径的情况下，提高网络吞吐

量，从而达到路径安全与高吞吐量同时优化的目的；2) 提出了综合考虑链路安全、链路冲突、链路可用带宽与链路可靠度的路由判据 SIEB，SIEB 包括链路安全和链路性能 2 个方面，为了抵御各种洞攻击，提出了基于两跳邻居反馈的链路信度计算方法；3) 基于路由指标 SIEB，提出了链路安全权值计算算法 LSWC 和链路性能权值计算算法 LSPC，提出了分布式的满足 QoS 约束的路由协议 SIEBP。

2　网络模型及问题描述

2.1　网络模型

将由静止的 CR-Mesh 路由器和 CR-Mesh 网关组成的认知无线 Mesh 网络建模为一个简单无向图 $G=(V,E)$，其中 V 表示 CR-Mesh 路由器和 CR-Mesh 网关的集合。E 表示链接 2 个能相互通信的 CR-Mesh 路由器的无线链路集合。每个节点 $v_i\in V$ 都有一个感知的可用信道集合 K_i。所有节点 $v_i\in V$ 都具有相同的通信距离 T_R 和干扰距离 I_R。一般情况下 $3T_R>I_R>T_R$，假设 $I_R=2\times T_R$。假设存在一个公共控制通道(CCC, common control channel)用于各 SU 之间传递控制信息。

$d(v_i,v_j)$表示节点 v_i 和节点 v_j 之间的物理距离。2 个 CR-Mesh 路由器能相互通信必须满足以下条件：1) 相同的可用信道不为空，即 $K_i\cap K_j\neq\Phi$；2) 满足通信距离的约束，即 $d(v_i,v_j)<T_R$。

$X=\{x_{(u,v)}\}_{nn}$，$x_{(u,v)}=k$ 表示无线链路(u,v)分配信道 k，$x_{(u,v)}=0$ 表示没有给无线链路(u,v)分配任何信道，并且，规定每条无线链路只能分配一个信道，或不分配任何信道。

当前网络中的可用信道集合为 K，B^k 表示信道 $k\in K$ 的带宽，单位为 Mbit/s，由于不同的信道通常具有不同的带宽，因此，对于不同的信道 i 和 j，$B^i\neq B^j$。

无线链路(u_1,v_1)和(u_2,v_2)相互冲突必须满足以下条件：1) $d(u_1,u_2)\leqslant I_R$ 或 $d(u_1,v_2)\leqslant I_R$ 或 $d(v_1,u_2)\leqslant I_R$ 或 $d(v_1,v_2)\leqslant I_R$；2) 2 条无线链路分配相同的信道，即 $x_{(u_1,v_1)}=x_{(u_2,v_2)}$。用 $I^k(u,v)$表示与无线链路(u,v)在信道 k 的冲突链路集合。

$\Psi=\{l^k_{(u,v)}\mid u,v\in V,k\in K\}$ 表示无线链路负荷的集合，$l^k_{(u,v)}$ 表示无线链路(u,v)在信道 k 的负荷，单位为 Mbit/s。

无线链路(u,v)在信道 k 的可用带宽 $B^k_\psi(u,v)$ 定义如式(1)所示，其中 $\frac{l^k_{(a,b)}}{B^k}$ 表示无线链路(a,b)传输负荷 $l^k_{(a,b)}$ 需要占用的带宽比例。

$$B^k_\psi(u,v)=B^k\left(1-\sum\nolimits_{(a,b)\in I^k(u,v)}\frac{l^k_{(a,b)}}{B^k}\right)\tag{1}$$

2.2　问题描述

在认知无线 Mesh 网络中，存在一类干扰、阻断、截听、选择性丢弃数据分组等严重威胁数据传输的攻击行为。其中网络层的攻击类型主要包括：黑洞攻击(black hole attack)、灰洞攻击(gray hole attack)、虫洞攻击(worm hole attack)等。

黑洞攻击：当数据传送经过俘获(compromise)节点时，数据或被敌手(adversary)阻截而不能继续进行传输，或被敌手获悉，使经过这些区域的数据存在严重的安全威胁，类似于经过“黑洞”一样，故称为黑洞攻击。

灰洞攻击又称选择性转发攻击(SFA, selective forwarding attack)：另外一种对认知无线 Mesh 网络数据传输危害性较大，而且难以检测与抵御的攻击行为。灰洞攻击是敌手通过智能方式有选择性地丢弃数据分组以阻止关键敏感信息的传送，导致网络不能观察与感知重要信息，或由于关键信息的缺失导致决策失误。

虫洞攻击：在 2 个攻击节点间建立一条高质量高带宽的通路，攻击节点 x_1 记录接收到的数据分组，通过此高质量数据通路将数据分组传递到另一攻击节点 x_2；在 CWMN 中，对选择最高吞吐量或最短路径的路由协议来说，虫洞将吸引较大的网络流量，造成严重的安全威胁。

综上所述，这类攻击最重要的特征就是破坏、干扰、截听、阻断 CWMN 的数据传输，降低 CWMN 的吞吐量。称其为洞攻击(HA, hole attack)。

设 $\Delta=\{\gamma_i=(s_i,d_i,b_i)\}$为无线业务需求集合，其中 s_i 和 d_i 表示无线业务 γ_i 的源点和目的点，b_i 表示无线业务 γ_i 的带宽约束。

为了更好地描述所研究的问题，给出了一个简单的网络拓扑示例，如图 1 所示，分布着 7 个 CR-Mesh 路由器。节点下面花括号中的数字表示节点感知的信道集合，如节点 A 下面的{1, 3,5}表示节点 A 感知的信道集合。假设系统中有 5 个可用信道，即 $K=\{1,2,3,4,5\}$，这 5 个可用信道的带宽分别是 B={20,19,24,16,35}。

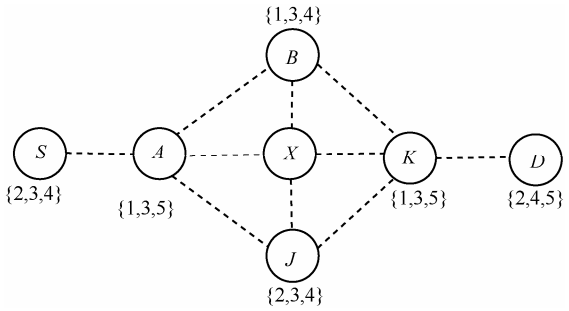

图 1　认知无线 Mesh 网络拓扑

在认知无线 Mesh 网络中，由于主用户占用授权信道的时变性，次用户感知的可用频谱资源的动态变化性，上述的洞攻击非常容易发生，任意攻击节点只需向邻居节点有意地报告错误的可用信道，引诱数据传输至攻击节点即可产生洞攻击。

无线业务 γ_1=(*S*,*D*,10)的源点为 *S*，目的节点为 *D*，带宽约束为 10 Mbit/s。设 *X* 节点是攻击节点，向相邻的节点虚假报告感知的可用信道，比如，*X* 节点向 *A*、*B*、*J* 与 *K* 节点报告其感知的可用信道集合为{1,2,3,4,5}。各无线链路的可用信道集合与信道的可用带宽，如表 1 所示。

表 1　无线链路可用信道集合与各信道的可用带宽

(u,v)	$K_u \cap K_v$	$B_\psi^k(u,v)$
(S, A)	{3}	$B_\psi^3(S,A)=24$
(A, B)	{1,3}	$B_\psi^1(A,B)=20$，$B_\psi^3(A,B)=24$
(A, J)	{3}	$B_\psi^3(A,J)=24$
(A, X)	{1,3,5}	$B_\psi^1(A,X)=20$，$B_\psi^3(A,X)=24$，$B_\psi^5(A,X)=35$
(B, K)	{1,3}	$B_\psi^1(B,K)=20$，$B_\psi^3(B,K)=24$
(J, K)	{3}	$B_\psi^3(J,K)=24$
(K, D)	{5}	$B_\psi^5(K,D)=35$

在认知无线 Mesh 网络中，路由路径构造必须与频谱分配联合考虑。如果路由判据是无线链路最大可用带宽，则在没有攻击节点 *X* 的情况下，为无线业务 γ_1构造的路由路径应该是 $S \to^3 A \to^1 B \to^3 K \to^5 D$，表示无线链路(*S*, *A*)分配信道 3，无线链路(*A*, *B*)分配信道 1，无线链路(*B*, *K*)分配信道 3，无线链路(*K*, *D*)分配信道 5。当存在攻击节点 *X* 的情况下，节点 *X* 向相邻的节点虚假报告其感知的可用信道，比如，节点 *X* 向节点 *A*、*B*、*J* 与 *K* 报告其感知的可用信道集合为{1,2,3,4,5}，其节点 *X* 感知的可用信道集合为{3,4}。在这种情况下，为无线业务 γ_1 构造的路由路径为 $S \to^3 A \to^5 X \to^5 K \to^5 D$，如表 2 所示。

其实，无论什么路由判据，攻击节点都可以虚假报告迎合路由判据的可用信道集合，使构造的路由路径经过攻击节点，从而引发各种洞攻击。

表 2　　无线业务 γ_1 的路由路径

$\gamma_i=(s_i,d_i,b_i)$	是否存在攻击节点	路径
(*S*,*D*,10)	不存在	$S \to^3 A \to^1 B \to^3 K \to^5 D$
	存在	$S \to^3 A \to^5 X \to^5 K \to^5 D$

3　路由判据 SIEB

在认知无线 Mesh 网络中，由于主用户使用信道的差异，CR-Mesh 节点所处地理位置的差异，各 CR-Mesh 节点感知的可用信道的差异，CWMN 中的路由与频谱分配问题必须联合考虑，这给攻击节点对 CWMN 发起攻击、降低频谱利用率、降低网络吞吐量提供了便利的条件。

为了抵御攻击节点对 CWMN 进行黑洞、灰洞、虫洞等攻击，提出了新的路由判据 SIEB，SIEB 不仅考虑了如何抵御洞攻击，而且还尽量最大化网络吞吐量。SIEB 包括 2 个部分，定义如式(2)所示。

$$\text{SIEB}=\alpha(1-SW^k(v,w))+\beta PW^k(v,w) \qquad (2)$$

其中，$\alpha+\beta=1$，$SW^k(v,w)$ 表示链路安全权值，$PW^k(v,w)$ 表示链路性能权值，分别用于抵御洞攻击和提高网络吞吐量。

3.1　链路安全权值函数

路由判据是路由协议选择下一跳的依据，在 CWMN 中，如果攻击节点虚报迎合路由判据的可用信道集合，非常容易引发各种洞攻击，为了有效地抵御 CWMN 中的洞攻击，提出了链路安全权值计算函数 $SW^k(v,w)$。

链路安全权值的计算不是直接通过相邻的单跳邻居的反馈进行计算的，而是基于两跳邻居反馈的信度计算的。因此，在 SIEB 中，为了达到安全性和高吞吐量的同时优化，所有 CR-Mesh 节点不仅保存单跳邻居的信息，还保存两跳邻居的信息。

链路安全权值是基于节点信任值计算的，因此，在 CWMN 中，所有 CR-Mesh 节点都需要计算并存储邻居节点的信任值，信任值越高，节点是攻击节点的可能性越小；信任值越低，节点是攻击节点的可能性越大，给邻居节点提供虚假可用信道的攻击节点将会被赋予较低的信任值。节点信任值 TVN(*v*, *w*)的计算如式(3)所示。

$$\mathrm{TVN}(v,w)=\frac{Pa(v,w)}{Pf(v,w)} \tag{3}$$

$Pf(v,w)$表示节点 v 传输给下一跳节点 w 的数据分组的数量，$Pa(v,w)$表示节点 v 从两跳邻居节点 u 接收到确认接收的数据分组的数量，如图 2 所示。

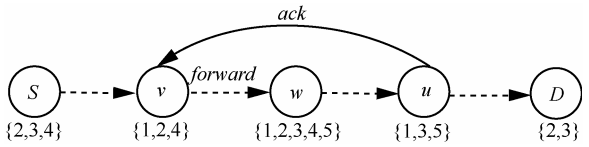

图 2　两跳邻居反馈示意

假如节点 v 传输了 100 个数据分组给节点 w，即 $Pf(v,w)$=100，节点 u 从节点 w 接收了 80 个数据分组，则节点 u 给节点 v 反馈 $Pa(v,w)$=80。

假如节点 w 是攻击节点，对网络发起灰洞攻击，进行选择性转发，致使节点 u 从节点 w 接收到的数据分组非常少，节点 v 可以非常快地通过节点 u 的反馈检测出节点 w 是攻击节点。对于黑洞攻击，节点 u 从节点 w 接收到的数据分组为零，给节点 v 反馈 $Pa(v,w)$=0。

当节点 v 检测出节点 w 的信任值 $\mathrm{TVN}(v,w)$小于信任值阈值 T_{tsh1}，立即通告无线业务源点重新进行路由发现过程。

在利用节点信任值检测出攻击节点的同时，还应该尽量减少对非攻击节点的误判，即节点 w 的信任值很低，不是因为节点 w 制造了洞攻击，而是因为无线链路在某信道的传输质量实在太差引起的，这种情况下不应该认为节点 w 是攻击节点。因此，还应该考虑无线链路分配不同信道时的信任值。

节点 w 的信任值 $\mathrm{TVN}(v, w)$是节点 v 根据历史无线业务计算而得。根据历史的节点信任值，可以计算出无线链路分配不同信道的情况下链路安全权值，$SW^k(v,w)$ 表示无线链路(v, w)分配信道 k 的情况下的链路安全权值，其计算如式(4)所示。

$$\begin{aligned} &SW^k(v,w)=\min_{(v,w)\in Pi\&x(v,w)=k}\{\mathrm{TVN}(v,w)\} \\ &\forall\gamma_i\in\Delta,\forall k\in K_v\cap K_w \end{aligned} \tag{4}$$

其中，P_i 表示历史无线业务 γ_i 的路径。对于无线链路(v,w)的所有可用信道 $\forall k\in K_v\cap K_w$，采用式(4)计算无线链路(v,w)分配信道 k 的链路安全权值。

如果算得 $SW^k(v,w)$ 的值为零，则认为节点 w 为黑洞，直接放入攻击节点集合 $\mathrm{HAN}(v)$。另外，如果 $SW^k(v,w)$ 小于信任值阈值 T_{tsh1}，认为节点 w 为攻击节点，加入攻击节点集合 $\mathrm{HAN}(v)$。

在构造安全路由路径的情况下，还希望最大化网络吞吐量，因此，需要更加准确地定义无线链路的安全权值，减少对非攻击节点的误判。无线链路$(v,\ w)$的平均安全权值 $SW(v,w)$ 的定义如式(5)所示。

$$SW(v,w)=\frac{1}{\left|K_v\cap K_w\right|}\sum\nolimits_{k\in K_v\cap K_w}SW^k(v,w) \tag{5}$$

其中，$SW(v,w)$ 表示无线链路(v, w)所有可用信道的平均信任值。如表 3 所示的情形，可以认为节点 w 不是攻击节点，可能是信道 1 的质量的确太差造成的，因为当无线链路(v, w)分配信道 2 和信道 4 的情况下，获得了较高的信任值。

表 3　　无线链路平均信任值

$SW^k(v,w)$	$SW(v,w)$
$SW^1(v,w)$ =0.3	
$SW^2(v,w)$ =0.9	$SW(v,w)$ =0.7
$SW^4(v,w)$ =0.9	

如果无线链路(v,w)的平均安全权值小于信任值阈值 T_{tsh2}，认为节点 w 是攻击节点，将其加入攻击节点集合 $\mathrm{HAN}(v)$，在选择下一跳时，避开选择节点 w。节点 w 是攻击节点的判断依据，如式(6)所示。

$$SW(v,w)<T_{tsh2} \tag{6}$$

3.2　链路性能权值函数

路由判据 SEIB 不仅考虑路由安全，还考虑了网络吞吐量，因此，提出链路性能权值函数 $PW^k(v,w)$。

主要的目标是构造能抵御洞攻击的路由路径，并且最大化网络吞吐量。最大化网络吞吐量主要通过链路性能权值函数 $PW^k(v,w)$ 达到。$PW^k(v,w)$ 的定义如式(7)所示。

$$PW^k(v,w)=\lambda_1 FI^k(v,w)+\lambda_2 FB^k(v,w)+\lambda_3 FR^k(v,w) \tag{7}$$

其中，$\lambda_1+\lambda_2+\lambda_3=1$，$FI^k(v,w)$ 表示无线链路(v, w)分配信道 k 的情况下的冲突集因子，如式(8)所示。其中 $I^k_{(v,w)}$ 表示(v,w)分配信道 k 的情况下的冲突集合，$N(v)$ 表示节点 v 的邻居节点集合。

$$FI^k(v,w)=\frac{\left|I^k_{(v,w)}\right|}{\sum_{u'\in N(v)}\left|I^k_{(v,u')}\right|} \tag{8}$$

$FB^k(v,w)$ 表示无线链路(v,w)分配信道 k 的情况下的消耗带宽比，如式(9)所示。其中 $B^k_\psi(u,v)$ 表示无线链路(v,w)分配信道 k 的情况下的可用带宽，如式(1)所示。

$$FB^k(v,w)=\frac{(1-B^k_\psi(v,w)/B^k)}{\sum_{u'\in N(v)}(1-B^k_\psi(v,u')/B^k)} \tag{9}$$

$FR^k(v,w)$ 无线链路(v,w)分配信道 k 的情况下的可靠度因子，如式(10)所示

$$FR^k(v,w)=\frac{(1-RW^k(v,w))}{\sum_{u'\in N(v)}(1-RW^k(v,w))} \tag{10}$$

其中，$RW^k(v,w)$ 表示无线链路(v,w)分配信道 k 的可靠度，如式(11)所示。

$$RW^k(v,w)=\frac{Pn^k(v,w)}{Sn^k(v,w)} \tag{11}$$

其中，$Pn^k(v,w)$ 与 $Sn^k(v,w)$ 分别表示节点 v 和节点 w 之间相同可用信道 k 的使用概率和稳定度。$Pn^k(v,w)$ 的定义如式(12)所示，$Sn^k(v,w)$ 的定义如式(13)所示。

$$Pn^k(v,w)=\max\{P^k(v),P^k(w)\} \tag{12}$$

$$Sn^k(v,w)=\max\{S^k(v),S^k(w)\} \tag{13}$$

其中，$P^k(v),P^k(w)$ 分别表示节点 v 和节点 w 感知的信道 k 被 PU 使用概率。$S^k(v),S^k(w)$ 分别表示节点 v 和节点 w 感知的信道 k 的稳定度，表示 CR-Mesh 节点的通信被 PU 打断的概率。信道的使用概率越低，稳定度越高，信道的可靠度越高。

4 路由协议 SIEBP

4.1 路由信息交互

SIEBP 协议有 2 种控制分组用于路由发现：从无线业务源节点到目的节点的路由请求分组 RREQ，以及从无线业务目的节点到源节点的路由回复分组 RREP。RREQ 与 RREP 通过公共控制信道传输。

RREQ 控制包中包括：源节点地址（source ID），目的节点地址（destination ID），QoS 约束，路径安全权值，路径性能权值，路径中间节点列表（intermediate ID），以及与上一跳和下一跳使用的信道，最后是否分配这些信道，由 4.4 节的路径计算与频谱分配过程确定。RREQ 控制分组的结构如图 3 所示。

SeqID	source ID	destination ID	QoS	Path-SW	Path-SP	SIEB	intermediate ID

图 3 RREQ 控制分组

Path-SW 表示路径安全权值，定义如式(14)所示。

$$\text{Path-SW}=\max\{SW(a,b)\},(a,b)\in P_i \tag{14}$$

Path-SP 表示路径性能权值，定义如式(15)所示。

$$\text{Path-SP}=\max\{SP(a,b)\},(a,b)\in P_i \tag{15}$$

4.2 分布式路由发现

为了减少路由开销，路由发现采用按需分布式。当无线业务源节点需要向目的节点发送数据时，触发分布式路由发现过程，源节点发送路由请求分组 RREQ 之前，以及除目的节点之外的所有节点收到 RREQ 数据分组之后，首先，计算链路安全权值，并判断邻居节点中的攻击节点，避免下一跳选择这些攻击节点，然后，计算与非攻击节点之间链路的性能权值，其次，计算路由判据，最后，对所有非攻击节点，通过公共控制信道发送 RREQ 路由请求分组，直到到达目的节点。

每个 RREQ 都包含一个唯一的序列号 SeqID，结构如图 3 所示。每个节点收到相同序列号 SeqID，即重复分组时，节点会计算并比较当前数据分组的路由判据 SIEB，如果当前接收 RREQ 的 SIEB 大于记录的 SIEB，则丢弃当前接收的 RREQ 数据分组，否则，更新当前记录的 SIEB、Path-SW 和 Path-SP。

重复次过程，直到 RREQ 到达目的节点或被丢弃。当目的节点接收到 RREQ 数据分组之后，首先，根据式(14)和式(15)计算 Path-SW 和 Path-SP，然后，计算 SIEB，对于具有相同序列号 SeqID 的数据分组，比较 SIEB 的大小，选择具有较小 SIEB 的路径。等待一个常数时间 T_{wait} 以便比较更多的 RREQ 数据分组。

分布式路由发现算法 DRDA 的伪代码，描述如图 4 所示，其中链路安全权值计算算法 LSWC 和链路性能权值计算算法 LSPC 在 4.3 节链路权值计算中描述。

DRDA 算法

输入：$G=(V,E)$, v,$\gamma_i=(s_i,d_i,b_i)$

输出：Path-SW、Path-SP、SIEB

1) ***if*** (($v==s_i$)|| (v *receives* RREQ(u)&& $v!=d_i$))
2) LSWC(v);//*computing link seure weight*
3) LSPC(v);//*computing performance weights*
4) RREQ(v)　RREQ(u);//*reconstruct* RREQ
5) ***while*** ($\forall w \in N(v)-\mathrm{HAN}(v)$){
6) ***while*** ($\forall k \in K_v \cap K_w$){
7) $\mathrm{SIEB}^k \leftarrow \alpha(1-SW^k(v,w))+\beta PW^k(v,w)$
8) }//*end while*
9) $k \leftarrow \arg\min_{k\in K_v\cap K_w}\{\mathrm{SIEB}^k\}$;
10) *update* Path-SW *in* RREQ(v);
11) *update* Path-SP *in* RREQ(v);
12) *compute* SIEB *according* to (2);
13) *update* SIEB *in* RREQ(v);
14) *insertw into* Intermediate IDs;
15) *send* RREQ(v) *to node* w;
16) }//*end while*
17) ***else if*** (v *receives* RREQ(u) && $v==d_i$) {
18) *compute* Path-SW *according to* (14);
19) *compute* Path-SP *according to* (15);
20) *compute* SIEB *according to* (2);
21) *compare* SIEB *with the same* SeqID;
22) *decide the route for* γ_i;
23) }//*end if*

图 4　算法 DRDA 的伪代码描述

4.3　链路权值计算

提出了链路安全权值计算算法 LSWC 和链路性能权值计算算法 LSPC。LSWC 算法的伪代码描述如图 5 所示。

LSWC 算法

输入：$G=(V,E)$, v,$\gamma_i=(s_i,d_i,b_i)$

输出：$SW^k(v,w)$, HAN(v)

1) ***while*** ($\forall w \in N(v)-u$){
2) ***while*** ($\forall k \in K_v \cap K_w$){
3) *compute* $SW^k(v,w)$ *according* to (4);
4) ***if*** ($SW^k(v,w)<T_{tsh1}$) {
5) $\mathrm{HAN}(v) \leftarrow \mathrm{HAN}(v)\cup\{w\}$;
6) *break*;
7) }//*end if*
8) }//*end while*
9) *compute* $SW(v,w)$ *according to* (5);
10) ***if*** ($SW(v,w)<T_{tsh2}$) {
11) $\mathrm{HAN}(v) \leftarrow \mathrm{HAN}(v)\cup\{w\}$;
12) }//*end if*
13) }//*end while*

图 5　算法 LSWC 的伪代码描述

节点 v 计算与其邻居节点分配不同信道的链路安全权值如图 6 所示。

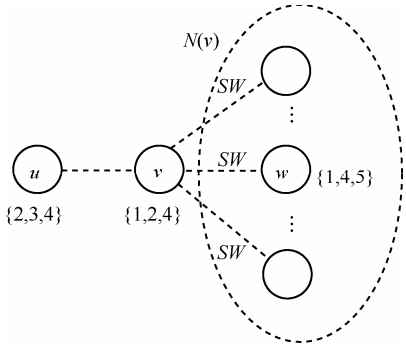

图 6　计算与邻居节点的 *SW* 值

LSPC 算法的伪代码描述如图 7 所示。

LSPC 算法

输入：$G=(V,E)$, v,$\gamma_i=(s_i,d_i,b_i)$, HAN(v), $x(v,w)$

输出：$PW^k(v,w)$

1) ***while*** ($\forall w \in N(v)-\mathrm{HAN}(v)$){
2) ***while*** ($\forall k \in K_v \cap K_w$){
3) *compute* $\mathrm{B}_\psi^k(v,w)$ *according to* (1);
4) ***if*** ($x(v,w)!=0$) {
5) ***if*** ($x(v,w)==k \,\&\&\, B_\psi^k(v,w)<b_i$)
6) *break*;
7) }
8) *compute* $FI^k(v,w)$ *according to* (8);
9) *compute* $FB^k(v,w)$ *according to* (9);
10) *compute* $FR^k(v,w)$ *according to* (10);
11) *compute* $PW^k(v,w)$ *according to* (10);
12) }//*end while*
13) }//*end while*

图 7　算法 LSPC 的伪代码描述

4.4　路径计算与频谱分配

目的节点根据最小的 SIEB 的 RREQ 数据分组构造路由回复数据分组 RREP，RREP 包含路径经过的中间节点向量，以及各无线链路分配的信道和 SIEB 信息，目的节点按反向路径将 RREP 发送给源节点，并对经过的中间节点以及无线链路分配信道。

4.5　路由维护与修复

通过 4.2 节的分布式路由发现过程，建立安全的路由路径，但因无线网络存在动态性，为了保证当前路径的吞吐量，路径中所有传输节点在传输过程中一直给两跳父节点反馈确认接收的数据分组的数量，判断链路安全权值是否小于信任值阈值，

进行洞攻击检测。一旦检测出洞攻击，向源节点发送路由错误信息 REER(routing error packet)。源节点收到 REER 之后重新进行路由发现过程构造新的路由路径。

5 时间复杂度分析

定理 1 LSWC 算法的时间复杂度是 $O(|V||K|)$。

证明 在 LSWC 算法中，对于所有节点计算其与下一跳节点分配不同信道时的链路安全权值，每个节点最多拥有$|V|$个邻居节点，每个节点最多拥有$|K|$个信道，每个节点的处理时间复杂度为 $O(|V||K|)$。因此，LSWC 算法的时间复杂度是 $O(|V||K|)$，证毕。

定理 2 LSPC 算法的时间复杂度是 $O(|V||K|)$。

证明 在 LSPC 算法中，对于所有节点计算其与下一跳节点分配不同信道时的链路性能权值，同样，每个节点最多拥有$|V|$个邻居节点，每个节点最多拥有$|K|$个信道，每个节点的处理时间复杂度为 $O(|V||K|)$。因此，LSPC 算法的时间复杂度是 $O(|V||K|)$，证毕。

定理 3 DRDA 算法的时间复杂度是 $O(|V||K|)$。

证明 在 DRDA 算法中，对于非目的节点，首先，调用 LSWC 算法和 LSPC 算法分别计算链路安全权值和链路性能权值，根据定理 1 和定理 2 的结论，其处理时间复杂度为 $O(|V||K|)$，然后，对节点 v 的所有邻居节点，以及每一个邻居节点的可用信道，计算路由判据 SIEB，处理时间复杂度为 $O(|V||K|)$，构造并发送 RREQ 数据分组需要常数时间 $O(1)$，每个节点总的处理时间复杂度为 $O(|V||K|)$。对于目的节点，只需要计算和比较 SIEB，处理时间复杂度 $O(|V||K|)$为常数 $O(1)$。因此，DRDA 算法的时间复杂度是 $O(|V||K|)$，证毕。

6 仿真与分析

为了验证提出的路由协议 SIEBP 的有效性，实现了 SIEBP、DRCA 以及 RCS-DPCS[26]算法。DRCA 与 RCS-DPCS 都是认知无线 Mesh 网络中的路由算法，他们的共同点在于认为认知无线 Mesh 网络中没有攻击节点，没有考虑 CWMN 中的安全问题，区别在于 DRCA 算法以最小化每个会话消耗的总带宽为目标。RCS-DPCS 算法以最大化端到端吞吐量为目标，选择 DRCA 与 RCS-DPCS 进行比较的原因是因为这 2 个算法在 CWMN 中能有较高的网络吞吐量。仿真采用 NS2[27]网络模拟器。

仿真的网络拓扑结构为 2 500 m×2 500 m 的区域，T_R=50 m，I_R=100 m，CR_Mesh 节点数$|V|$=80，攻击节点比例为 r，取值 0、0.1、0.2、0.3，共 4 种情况，每个攻击节点的攻击概率用分组丢失率 p 表示，取值 0、0.25、0.5、0.75、1，共 5 种情况，p=1 表示黑洞攻击。可用信道数为$|K|$=12，各信道的带宽属于[0,50]，并且随机产生，PU 随机地占用授权信道，信道使用概率、信道稳定度随机产生，其范围属于[0,1]。默认情况下，r=0.2，p=0.5，$\alpha=0.5$，$\beta=0.5$，$T_{tsh1}=0.3$，$T_{tsh2}=0.6$，$\lambda_1=0.4$，$\lambda_2=0.3$，$\lambda_3=0.3$，$T_{\text{wait}}=100$ ms。以下的实验结果均为 500 次独立仿真结果的均值。

仿真主要以攻击节点比例、攻击节点分组丢失率作为参数，从以下 4 个方面进行仿真：1) 平均分组投递率；2) 平均端到端延迟；3) 平均吞吐量；4）平均路由开销。

6.1 平均分组投递率比较

分析比较攻击节点比例、攻击节点分组丢失率对平均分组投递率的影响。仿真结果如图 8 和图 9 所示。

由图 8 可知，当攻击节点数为零时，即网络不存在攻击节点时，SIEBP、DRCA 与 RCS-DPCS 的平均投递率相差不大。当存在攻击节点时，SIEBP 的平均投递率高于 DRCA 和 RCS-DPCS，随着攻击节点比例的增大，SIEBP 的优势更明显，这是因为，DRCA 与 RCS-DPCS 没有攻击节点检测机制，而 SIEBP 能通过节点信任值的计算检测出攻击节点，并且避开攻击节点构造路由路径。攻击节点达到 30%时，SIEBP 的平均投递率比 DRCA 和 RCS-DPCS 高 27%。

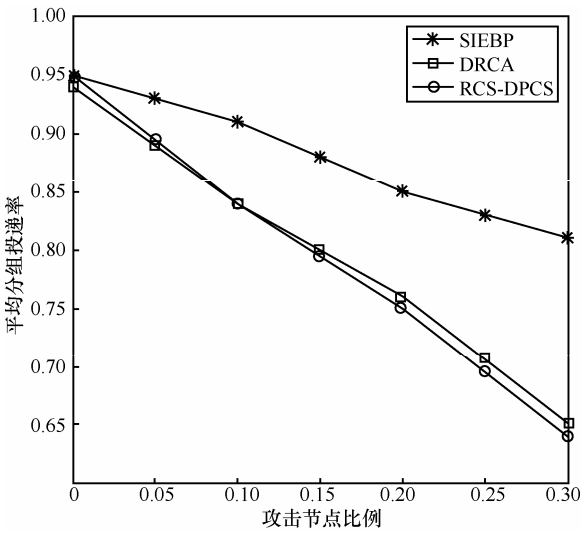

图 8 攻击节点比例对平均分组投递率的影响

由图 9 可知，随着攻击节点分组丢失率的增大，SIEBP、DRCA 与 RCS-DPCS 的平均分组投递率减少。SIEBP 的平均投递率高于 DRCA 和 RCS-DPCS，随着攻击节点分组丢失率的增大，SIEBP 的优势更明显，这是因为 SIEBP 能通过节点信任值的计算检测出攻击节点，并且避开攻击节点构造路由路径。当出现黑洞攻击，即 p=1 时，SIEBP 的平均分组投递率为 81%，比 DRCA 和 RCS-DPCS 高 37%。

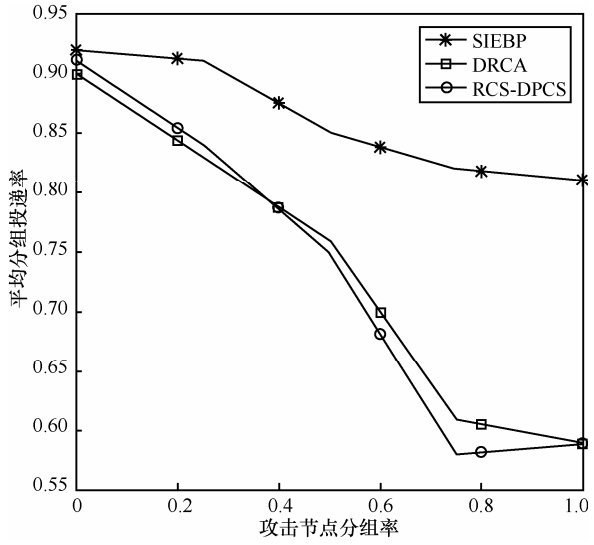

图 9　攻击节点分组丢失率对平均分组投递率的影响

6.2　平均端到端延迟比较

分析比较攻击节点比例、攻击节点分组丢失率对平均端到端延迟的影响。仿真结果如图 10 和图 11 所示。

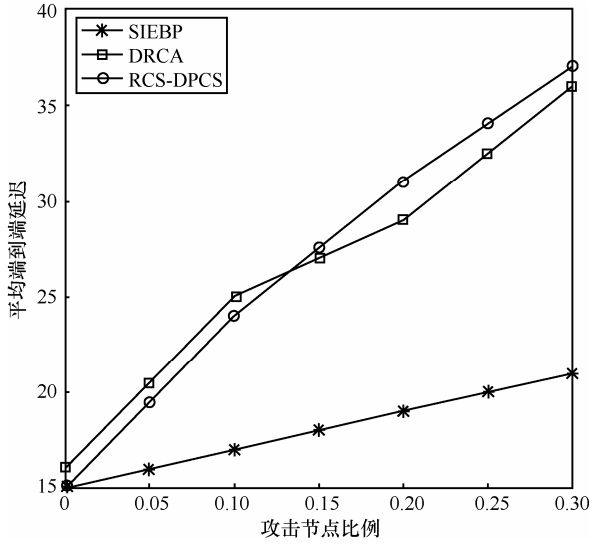

图 10　攻击节点比例对平均端到端延迟的影响

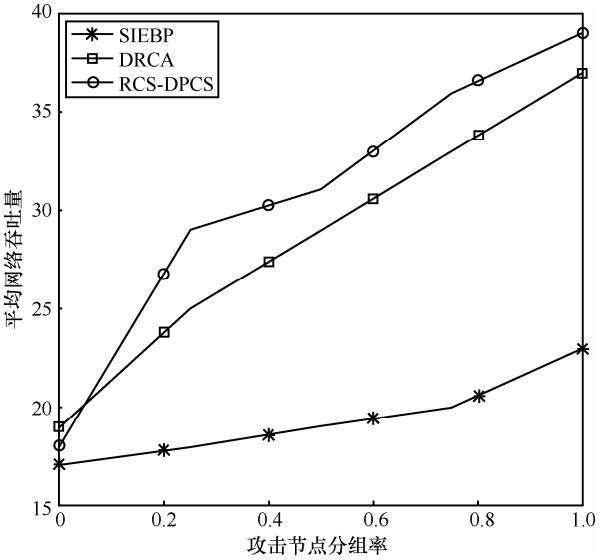

图 11　攻击节点分组丢失率对平均端到端延迟的影响

由图 10 可知，随着攻击节点比例的增大，SIEBP、DRCA 与 RCS-DPCS 的平均端到端延迟增大，这是因为攻击节点的增多，导致重新路由发现的频率提高，平均端到端延迟随之增加。DRCA 与 RCS-DPCS 增大的幅度大于 SIEBP，这是因为 DRCA 与 RCS-DPCS 重复路由发现可能还是会选择攻击节点，而 SIEBP 不会再次选择攻击节点。当 r=30%时，DRCA 和 RCS-DPCS 的平均端到端延迟比 SIEBP 高 71%。

由图 11 可知，随着攻击节点分组丢失率的增大，SIEBP、DRCA 与 RCS-DPCS 的平均端到端延迟增大。SIEBP 的平均端到端延迟比 DRCA 和 RCS-DPCS 低，这是因为 SIEBP 有攻击节点检测机制，能够避开攻击节点构造路由路径。当 p=1 时，DRCA 和 RCS-DPCS 的平均端到端延迟分别比 SIEBP 高 61%和 70%。

6.3　平均吞吐量比较

分析比较攻击节点比例、攻击节点分组丢失率对平均吞吐量的影响。仿真结果如图 12 和图 13 所示。

由图 12 可知，当攻击节点数为零时，即网络不存在攻击节点时，SIEBP、DRCA 的平均吞吐量低于 RCS-DPCS，这是因为，RCS-DPCS 的目标是最大化网络吞吐量。随着攻击节点比例的增大，SIEBP、DRCA 与 RCS-DPCS 的平均吞吐量降低，这是因为，攻击节点越多，路径重新路由的概率增大，将影响网络的平均吞吐量。当存在攻击节点时，SIEBP 的平均吞吐量明显高于 DRCA 与 RCS-DPCS。SIEBP 高出 DRCA 的

最小值和最大值分别是：47%和 90%。SIEBP 高出 RCS-DPCS 的最小值和最大值分别是：15%和 25%。

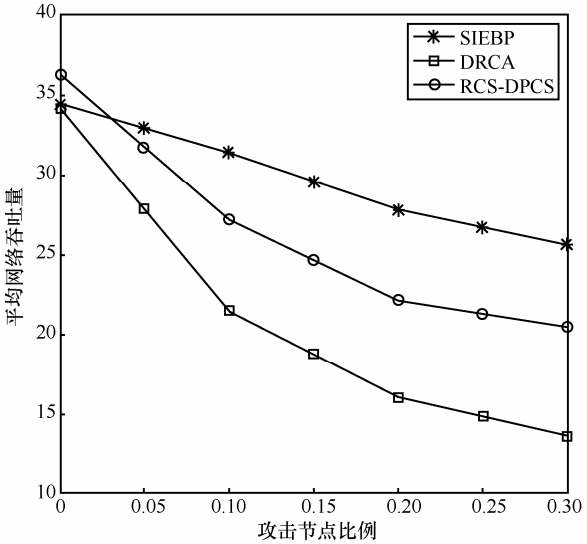

图 12 攻击节点比例对平均吞吐量的影响

由图 13 可知，随着攻击节点分组丢失率的增大，SIEBP、DRCA 与 RCS-DPCS 的平均吞吐量降低，这是因为攻击节点分组丢失率越高，成功传输的数据分组越少，路径重新路由的概率增大，所以网络的平均吞吐量越低。当 p=1 时，SIEBP 的平均吞吐量分别比 DRCA 和 RCS-DPCS 高 72%和 22%。

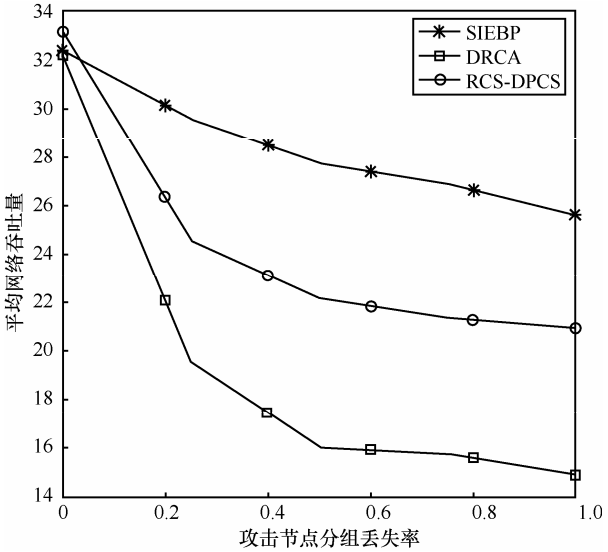

图 13 攻击节点分组丢失率对平均吞吐量的影响

6.4 平均路由开销比较

分析比较攻击节点比例、攻击节点分组丢失率对平均路由开销的影响。仿真结果如图 14 和图 15 所示。

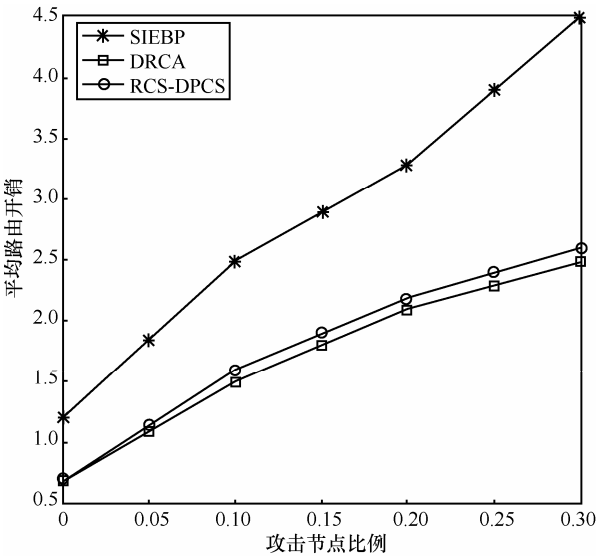

图 14 攻击节点比例对平均路由开销的影响

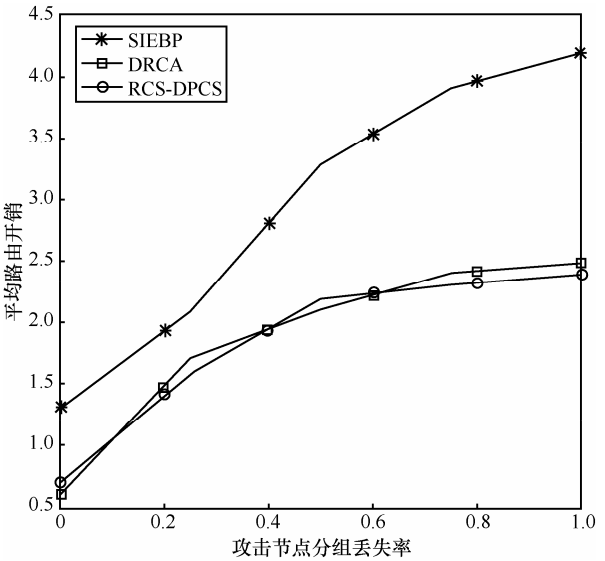

图 15 攻击节点分组丢失率对平均路由开销的影响

由图 14 可知，随着攻击节点比例的增大，SIEBP、DRCA 与 RCS-DPCS 的平均路由开销增大，这是因为，攻击节点越多，重新进行路由发现的频率提高，路由发现需要的控制分组随之增多。SIEBP 的平均路由开销高于 DRCA 和 RCS-DPCS，这是因为，SIEBP 的 RREQ 控制分组中包含链路安全与链路性能等权值信息，并且 RREQ 的发送是通过单播传输的，对每一个邻居节点传输一个，SIEBP 进行路由发现需要发送的 RREQ 分组比 DRCA 和 RCS-DPCS 多。

由图 15 可知，随着攻击节点分组丢失率的增大，SIEBP、DRCA 与 RCS-DPCS 的平均路由开销增大，这是因为攻击节点分组丢失率越大，路

由路径重新构造的概率增大，路由开销随之增大。SIEBP 的平均路由开销高于 DRCA 和 RCS-DPCS，攻击节点分组丢失率越大，这种趋势越明显。这是因为，SIEBP 协议的 RREQ 控制包含源节点与目的节点地址、QoS 约束、路径安全和性能权值，路径中间节点列表，以及与上一跳和下一跳使用的信道等，SIEBP 的 RREQ 控制分组本身就比 DRCA 和 RCS-DPCS 的路由请求分组大，所以，攻击节点分组丢失率越大，这种趋势越明显。当 p=1 时，SIEBP 的平均路由开销比 DRCA 和 RCS-DPCS 高 75%。

7　结束语

通过大量的仿真发现，SIEBP 对于各种洞攻击，不仅能构造安全的路由路径，而且还能获得高的网络吞吐量。比 RCS-DPCS 的平均吞吐量高 25%，而 RCS-DPCS 是以最大化网络吞吐量为目标，也被认为是目前 CWMN 中针对最大化网络吞吐量这个性能指标最优的算法，因此，认为 SIEBP 达到了路径安全与高吞吐量同时优化的目的。下一步工作将研究降低 SIEBP 路由开销的方法和机制，以及进行理论建模和数学分析。

参考文献：

[1] MITOLA J. Cognitive radio: making software radio more personal [J].IEEE Personal Communication, 1999, 6(4):13-18.

[2] AKYILDIZ I F, LEE W Y, VURAN M C, *et al*. Next generation /dynamic spectrum access/cognitive radio wireless networks: a survey[J]. Computer Networks, 2006, 50(9):2127-2159.

[3] CHOWDHURY KR, AKYILDIZ I F. Cognitive wireless Mesh networks with dynamic spectrum access [J].IEEE Journal on Selected Areas in Communications, 2008, 26(1):168-181.

[4] 邝祝芳, 陈志刚, 邓晓衡. 自适应的认知无线 Mesh 网络 QoS 约束的由与频谱分配算法[J]. 通信学报, 2011,32 (11):59-70.
KUANG Z F, CHEN Z G, DENG X H. Self-adaptivejoint routing and spectrum allocation algorithm with QoS constraints in cognitive wireless Mesh networks[J]. Journal on Communications, 2011, 32(11): 59-70.

[5] PARVINA S, HUSSAINB F K, HUSSAINB O K,*et al*.Cognitive radio network security: a survey [J]. Journal of Network and Computer Applications, 2012, 35(6):1691-1708.

[6] 裴庆祺, 李红宁, 赵弘洋等.认知无线电网络安全综述[J].通信学报，2013,34(1):144-158.
PEI Q Q, LI H N, ZHAO H Y, *et al*. Security in cognitive radio networks[J]. Journal on Communications, 2013, 34(1):144-158.

[7] FRAGKIADAKIS A G, TRAGOS E Z, ASKOXYLAKIS I G. A survey on security threats and detection techniques in cognitive radio networks [J]. IEEE Communications Surveys & Tutorials,2013, 15(1), 428-445.

[8] XIN C S, SONG M. Detection of PUE attacks in cognitive radio networks based on signal activity pattern[J].IEEE Transactions on Mobile Computing,2014,13(5):1022-1034.

[9] RAWAT A S, ANAND P, CHEN H, *et al*. Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks [J].IEEE Transactions on Signal Processing, 2011, 59(2): 774-786.

[10] AKTER L, NATARAAN B. Distributed approach for power and rate allocation to secondary user in cognitive radio network[J]. IEEE Transactions on Vehicular Technology, 2011, 60(4)：1526- 1538.

[11] CHEN R L, PARK J M, HOU Y T, *et al*. Toward secure distributed spectrum sensing in cognitive radio network[J]. IEEE Communications Magazine, 2008, 46(4):50-55.

[12] YI P,TONG T H, LIU N, *et al*. Security in wireless Mesh networks: challenges and solutions[A]. International Conference on Information Technology[C]. New Generations, 2009.423-428.

[13] LIN H, HU J, MA J F, *et al*. A role based privacy-aware secure routing protocol for wireless Mesh networks[J]. Wireless Personal Communications, 2014, 75(3):1611-1633.

[14] AGRAWAL S, JAIN S, SHARMA S. A survey of routing attacks and security measures in mobile Ad-Hoc networks[J]. Journal of Computing, 2011, 3(1): 41-48.

[15] ZIN S M, ANUARA N B, KIAHA M L M, *et al*. Routing protocol design for secure WSN: review and open research issues[J]. Journal of Network and Computer Applications, 2014, 41(1):517-530.

[16] YOUSSEF M, IBRAHIM M, ABDELATF M, *et al*. Routing metrics of cognitive radio networks a survey[J]. IEEE Communications Surveys & Tutorials, 2014, 16(1):92-109.

[17] DING Y, XIAO L. Video on demand streaming in cognitive wireless Mesh networks[J]. IEEE Transactions on Mobile Computing, 2013, 12(3): 412-423.

[18] MUMEY B, TANG J, JUDSON I R, *et al*. On routing and channel selection in cognitive radio Mesh networks[J]. IEEE Transactions on Vehicular Technology, 2012, 61(9): 4118-4128.

[19] WU G F, ZHAG J, HE Z P. A trust mechanism-based channel assignment and routing scheme in cognitive wireless Mesh networks with intrusion detection[J]. Journal of Electronics (China), 2010, 27(5): 728-734.

[20] GUO J W, ZHOU X W. Secure distributed routing algorithm with optimizing energy consumption for cognitive radio networks[J]. Wireless Personal Communications,2013,72(4):2533-2550.

[21] YUAN Z, HAN Z, SUN Y L, *et al*. Routing toward primary user attack and belief propagation-based defense in cognitive radio networks[J]. IEEE Transactions on Mobile Computing, 2013, 12(9): 1750-1760.

[22] ZHU Q Y, SONG J B, BASART. Dynamic secure routing game in distributed cognitive radio networks[A]. 2011 IEEE Global Telecommunications Conference (GLOBECOM 2011)[C]. 2011.1-6.

[23] HOW K C, MA M, QIN Y. A cross-layer selfishness avoidance routing protocol for the dynamic cognitive radio networks[A]. 2011 IEEE GLOBECOM Workshops[C]. 2011:942-946.

[24] 张光华, 张玉清, 刘雪峰.认知无线电网络中基于信任的安全路由模型[J]. 通信学报, 2013,34(2):56-64.
ZHANG G H, ZHANG Y Q, LIU X F. Trust based secure routing model for cognitive radio networks[J]. Journal on Communications, 2013, 34(2):56-64.

[25] JO M, HAN L Z, KIM D, *et al*. Selfish attacks and detection in cognitive radio Ad-Hoc network[J]. IEEE Network, 2013, 27(3): 45-50.

[26] SORRELLS C, POTIER P, QIAN L J, *et al*. Anomalous spectrum usage attack detection in cognitive radio wireless network[A]. 2011 IEEE International Conference on Technologies for Homeland Security (HST)[C]. 2011.384-189.

[27] FALL K, VARADHAN K. NS manual[EB/OL]. http://www.isi.edu/nsnam/ns/ns-tutorial/index.html.

作者简介：

邝祝芳（1982-），男，湖南耒阳人，中南大学副教授，主要研究方向为下一代宽带无线通信系统、认知无线 Mesh 网络。

陈志刚（1964-），男，湖南益阳人，中南大学教授、博士生导师，主要研究方向为网络计算与分布式处理。

王国军（1970-），男，湖南长沙人，中南大学教授、博士生导师，主要研究方向为可信计算与信息安全。

刘蕙（1975-），女，湖南长沙人，密苏里州立大学副教授，主要研究方向为无线网络、网络计算与可信计算。

（上接第 68 页）

[13] GRIPPO L, SCIANDRONE M. On the convergence of the block nonlinear Gauss-Seidel method under convex constraints[J]. Operations Research Letters, 2000, 26(3):127-136.

[14] BOYD S, VANDENBERGHE L. Convex Optimization[M]. England: Cambridge University Press, 2004.

[15] ZOU J, XU H. Auction-based power allocation for multiuser two-way relaying networks[J]. IEEE Trans Wireless Commun, 2013, 12(1): 31-39.

[16] WANG B, HAN ZH, LIU K J R. Distributed relay selection and power control for multiuser cooperative communication networks using stackelberg game[J]. IEEE Trans Mobile Computing, 2009, 8(7): 975-990.

[17] HAMMERSTROM I, WITTNEBEN A. Power allocation schemes for amplify-and-forward MIMO-OFDM relay links[J]. IEEE Trans Wireless Commun, 2007,6(8):2798-2802.

作者简介：

冯文江（1963-），男，四川西充人，博士，重庆大学教授、博士生导师，主要研究方向为宽带无线接入技术、认知无线电、通信信号处理等。

蒋卫恒（1985-），男，湖北枝江人，重庆大学博士生，主要研究方向为网络控制与优化、博弈论以及最优化理论。

邓艺娜（1991-），女，四川南充人，重庆大学硕士生，主要研究方向为认知无线电。

袁杨（1991-），男，四川南充人，重庆大学硕士生，主要研究方向为认知无线电。