认知无线电网络中的频谱感知安全机会路由协议

王 露[1,2] 白光伟[1] 沈 航[1,3] 王天荆[1]
(南京工业大学计算机科学与技术学院 南京 211816)[1]
(南京大学计算机软件新技术国家重点实验室 南京 210093)[2]
(南京邮电大学通信与网络技术国家工程研究中心 南京 210003)[3]

摘 要 针对认知无线电网络中频谱的动态特性及潜在的节点选择性转发问题,提出频谱感知安全机会路由 S2OR 协议。在频谱感知阶段,通过对主用户活动建模来分析认知节点之间链路的可用概率。在路由选择阶段,采用信任管理方式来考查节点转发行为的可靠性,以便选择可信任的中继节点并保证数据传输的完整性。协议通过获取局部网络状态信息,计算由链路可用概率、链路质量和节点信任度构成的综合型指标——期望吞吐率,允许认知节点在此基础上机会式地选择候选转发节点与数据信道。仿真结果表明,S2OR 能够很好地适应频谱动态特性,获取较高的吞吐量,同时减小节点恶意攻击带来的影响。

关键词 认知无线电,机会路由,频谱感知,信任管理
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.10.031

Spectrum-aware Secure Opportunistic Routing Protocol in Cognitive Radio Networks

WANG Lu[1,2] BAI Guang-wei[1] SHEN Hang[1,3] WANG Tian-jing[1]
(College of Computer Science and Technology, Nanjing Tech University, Nanjing 211816, China)[1]
(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093, China)[2]
(National Engineering Research Center for Communication and Network Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)[3]

Abstract This paper proposed a spectrum-aware secure opportunistic routing (S2OR) protocol against the dynamic characteristics of spectrum and the potential selective forwarding attack in cognitive radio networks. During the spectrum sensing phase, the availability probability of link among cognitive nodes is analyzed by modeling primary user activity. During the routing selection phase, a trust management model is exploited to examine node's reliability for packet forwarding, so as to select relay nodes with high trustability and ensure the integrity of data transmission. With the local information, a comprehensive routing metric called the expected throughput, consisting of link availability probability, link quality and node's trustability, is computed. On this basis, cognitive nodes can opportunistically select candidate forwarding nodes and the corresponding data channels. Simulation results demonstrate that S2OR can well adapt to the dynamics of spectrum, result in higher throughput and reduce the impacts of malicious attacks at the same time.

Keywords Cognitive radio, Opportunistic routing, Spectrum sensing, Trust management

1 引言

认知无线电技术为缓解频谱资源紧缺提供了新的手段,其通过感测无线电环境来获取处于空闲状态的可用频谱,从而实现频谱共享和资源的有效利用[1]。在认知无线电网络(Cognitive Radio Network, CRN)中,只要主用户(Primary User, PU)没有占用授权信道,认知用户就有机会伺机接入进行通信。一旦 PU 信号返回,认知用户需立即撤离该信道并寻找新的频谱接入机会,以减小对 PU 通信的干扰。与传统无线网络相比,CRN 中的路由设计面临着一些新的挑战:1)传统路由协议考虑的是固定频谱,不能直接被应用到 CRN 环境中;2)认知无线电技术实现的是动态频谱接入功能,故

到稿日期:2017-09-11 返修日期:2017-12-29 本文受国家自然科学基金项目(61502230,61073197,61501224),江苏省自然科学基金项目(BK20150960),江苏省普通高校自然科学研究项目(15KJB520015),南京市科技计划项目(201608009),南京大学计算机软件新技术国家重点实验室资助项目(KFKT2017B21),南京邮电大学通信与网络技术国家工程研究中心资助项目,江苏省六大高峰人才基金资助项目(第八批)资助。
王 露(1993-),女,硕士生,主要研究方向为认知无线电网络路由协议,E-mail:wl1336361890@163.com;白光伟(1961-),男,博士,教授,博士生导师,CCF 高级会员,主要研究方向为无线传感器网络、移动互联网、网络体系结构和协议、网络系统性能分析和评价、多媒体网络服务质量等,E-mail:bai@njtech.edu.cn(通信作者);沈 航(1984-),男,博士,讲师,硕士生导师,CCF 会员,主要研究方向为无线网络编码、移动互联网、无线多媒体通信协议等;王天荆(1978-),女,博士,副教授,硕士生导师,主要研究方向为认知无线电网络、压缩感知等。

PU 活动直接决定了认知用户接入信道的机会。鉴于以上两点,CRN 中的路由设计应该与频谱感知、信道选择结合起来考虑[2-4]。前期有关频谱感知路由协议的研究工作也对信道分配与路由建立进行了探讨,但大多基于预先设定好的端到端的路由表,不适应信道条件多变的动态频谱接入系统。

在 CRN 路由协议的研究中,安全也是一个不可忽视的问题,比如频谱感知阶段的数据伪造攻击、主用户模仿攻击、网络层的选择性转发攻击等。无论遭遇哪一种攻击,认知用户之间的通信都会受到很大的影响。但是,目前 CRN 路由协议的研究工作大多关注网络延时、吞吐量等 QoS 性能,较少考虑路径安全问题。由于 PU 占用授权信道的时变性,认知节点的通信往往需要建立在动态可用频谱的基础上。在分布式 CRN 环境中,只要任意攻击节点向其邻居节点分享可用的信道信息,就有可能获得数据转发机会,这使得选择性转发等路由攻击在 CRN 环境下更易发生。传统的密钥管理、身份认证等安全机制已经无法解决这种网络内部的节点攻击[5-7]问题,相比之下,利用信任管理机制进行防御更为灵活。

本文提出频谱感知安全机会路由,其在适应 CRN 特性的同时又为数据传输提供了安全保障。在动态频谱接入系统中,当前节点需要根据信道使用的统计信息、局部链路信息等,机会式地选择它的候选转发节点与数据信道。面对网络中潜在的节点选择性转发威胁,通过监测邻居节点的转发行为计算出节点的信任值,并将该信任值与链路可用概率和链路质量进行融合,从而选出高吞吐量的安全路由。

本文第 2 节分析现有的一些 CRN 路由协议及其存在的问题;第 3 节引入网络模型和协议概述;第 4 节深入分析 S2OR 协议的实现过程,包括路由指标的设计与候选节点集合的创建;第 5 节通过仿真的方法对 S2OR 路由机制进行性能分析与评价;最后总结全文。

2　相关工作

近年来,有关 CRN 路由协议的研究也取得了一定的进展。Lin 等[8]提出了频谱感知路由协议 SAOR,着眼于在无线电衰减的信道环境下建立一种可靠的端到端传输算法。该算法利用空闲频谱信息处理大量的动态机会连接问题,提高了数据传输的吞吐量服务。Pan 等[9]提出的路由协议 MCORP 考虑了多信道认知环境,并在构造候选节点竞争集时权衡了能耗与投递率之间的矛盾,旨在通过消耗较少的能量来获取尽可能高的投递率。但是,上述研究工作重点关注的是网络的 QoS 性能,忽略了路由安全。如果网络中存在节点故意丢包,或者为了减少资源消耗选择性地转发部分数据包的情况,那么数据传输的完整性和成功率必然会受到很大的影响。

针对频谱感知过程中节点提供错误信息的攻击,Khasawneh 等[10]提出了认知无线网络安全路由算法。该算法将节点在协作频谱感知阶段的可靠性列为路由指标之一,并结合信道开销、PU 活跃程度进行路径选择。针对数据传输阶段可能受到的丢包攻击,Zhang 等[11]提出基于信任的路由模型。通过对节点转发行为的监测,构建节点之间的信任,并在路由选择阶段结合时延度量来确定传输路径。但是,该路由算法是在可用频谱已知的基础上建立的,并没有通过对 PU 活动进行建模来分析信道的可用概率,忽略了 CRN 中频谱动态变化对链路建立的影响。

路径安全是路由研究的一个重要问题,但现有工作大多没有将路由安全与 CRN 的认知特性进行联合考虑,导致网络性能下降,故本文提出频谱感知安全机会路由方案。

3　系统描述

如图 1 所示,考虑一个多跳的分布式 CRN,多个认知用户和 PU 共享一组数据信道 $C=\{C_1,C_2,\cdots,C_m\}$,每个信道上的认知用户最多被一个活跃的 PU 所影响。认知用户配有两种无线电:1)工作在公共控制信道(Common Control Channel,CCC)上的普通无线电,负责信息交换和数据共享;2)用于数据传输的认知无线电,其可以在多个信道之间进行切换,但同一时刻只能工作在一个信道上。通过 GPS 技术或者其他定位设备,用户可以获取它们的位置信息。为叙述方便,文中所提及的节点均指代认知用户,PU 均指代主用户。

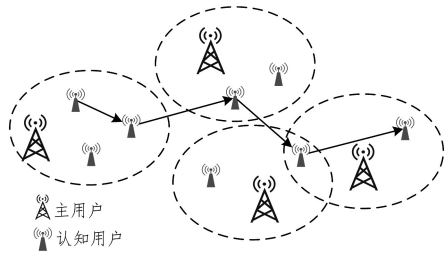

图 1　网络的拓扑结构

Fig. 1　Topology of network

源节点 S 与其传输范围之外的目的节点 D 通信时,需要发起一个多跳传输的过程。如图 2 所示,每一跳传输过程包含 3 个阶段:频谱感知、中继选择、数据传输。节点首先对无线信道进行能量检测,判断可用信道并获取频谱接入机会,然后根据路由机制在空闲信道中选出下一跳转发节点,最后完成数据传输。源节点 S 与每一个中间发送节点 N_i 按照图 2 所示的流程进行操作,便可将数据成功传递给目的节点 D。

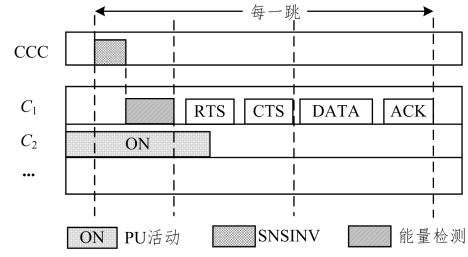

图 2　数据在每一跳中的传输过程

Fig. 2　Transmission process in each hop for data

3.1　频谱感知阶段

为了获取空闲信道,中间发送节点 N_i 利用能量检测技术周期性地感知授权频谱,并将感知信息分享给周边的邻居节点。在感知数据信道之前,N_i 首先利用 CCC 广播感知请求消息 SNSINV(Sensing Invitation),以防止其他节点在此期间利用该信道传输数据。SNSINV 中包含 N_i 及 D 的位置信息,邻居节点利用这些信息可以初步判断自己是否满足转发

节点的要求，比如是否比 N_i 更接近目的节点。SNSINV 消息的传输服从载波监听多址接入/碰撞避免(CSMA/CA)机制，从而在一定程度上避免了同信道的干扰。当检测到该信道为空闲，即没有出现 PU 信号时，N_i 存储该信道信息，并进入下一阶段的握手过程。

3.2 中继选择阶段

在此阶段，N_i 需要从多个候选节点中选出下一跳转发节点，候选节点的选择算法详见第 4 节。当检测到空闲信道时，N_i 便向候选节点广播路由请求消息 RTS。一旦接收到 RTS 请求，候选节点即可按照 N_i 指定的优先级顺序回复应答消息 CTS。优先级越高，回复消息的规避时间越短，越优先回复。每一个候选节点保持对数据信道的监听，直到出现 CTS 消息，或者在规避时间结束之后发送 CTS 回复。N_i 总是选择最先回复的候选节点作为下一跳转发节点，如此便达成了上一跳与下一跳的握手协议。如果 N_i 没有收到任何回复消息，说明该信道中没有可用的候选节点，则回到第一阶段重新检测新的数据信道。

3.3 数据传输阶段

一旦确定好转发节点和空闲信道，N_i 即可进行数据传输。若传输过程中出现 PU 再一次占用该信道的情况，则 N_i 重新感知新的可用信道，或者将通信切换到其他空闲信道上继续传输，以达到维护路由的效果。当发送节点收到来自下一跳的确认信号 ACK 时，则表明数据传输成功。但是在该阶段中通常存在一些威胁数据传输的攻击行为，比如黑洞、灰洞等攻击[5,11]。灰洞攻击又称为选择性转发攻击，节点故意声称其是通往目的节点的最佳下一跳，以获得转发机会，但当其收到数据包时却只转发部分数据包，这严重破坏了数据传输的完整性。针对节点选择性转发攻击，需要采取相应的防御手段，尽可能识别出存在恶意行为的节点，并在路由选择时避开这些节点。

4 频谱感知安全机会路由

考虑到 CRN 中可用信道动态变化的特性，本文采用跨层设计的方法对数据信道与转发节点进行联合选择，以改善路由协议的性能。在存有安全隐患的 CRN 中，影响路由性能的因素有很多，如信道使用的统计信息、链路质量以及节点的可靠性等。为了抵御网络层的节点选择性转发攻击，同时尽可能最大化网络吞吐量，本文设计了一个综合型指标，即期望吞吐率 $ETT(R_i^x)$，以衡量每一跳的中继性能并指导候选节点集的创建。

$$ETT(R_i^x)=\sum_{N_j\in R_i^x} B_x\cdot(1-\lambda_{ij}^x)\cdot Q_{ij}^x\cdot T_{ij}(t) \tag{1}$$

其中，R_i^x 表示节点 N_i 在信道 C_x 上的一组候选转发节点集合，B_x 表示信道 C_x 的最大传输速率，λ_{ij}^x 表示 N_i 与 N_j 之间的链路丢包率，可以通过在两节点之间发送数据分组并测量分组丢失比率来估计 λ_{ij}^x 的大小。另外，$T_{ij}(t)$ 表示当前 t 时刻节点 N_i 对 N_j 的信任程度，Q_{ij}^x 表示 N_i 选择节点 N_j 和信道 C_x 传输数据的链路可用概率，分别用于抵御节点丢包攻击和衡量 PU 活动对数据传输的影响。

4.1 链路可用概率

假设 PU 占用数据信道的时间为独立同指数分布的 ON/OFF 模型[12-13]：ON 表示信道被 PU 占用，此时节点不可以接入该信道；OFF 表示信道空闲，即没有出现 PU 活动，节点可以伺机占用信道进行数据传输。用均值分别为 v_x 和 l_x 的指数型随机变量 V_x 和 L_x 来描述信道 C_x 处于 ON，OFF 状态的持续时间，则信道 C_x 忙碌或者空闲的概率 p_{on}^x，p_{off}^x 可表示为：

$$\begin{cases} p_{\text{on}}^x=v_x/(v_x+l_x) \\ p_{\text{off}}^x=l_x/(v_x+l_x) \end{cases} \tag{2}$$

(1)频谱感知阶段

在频谱感知阶段，每一个认知节点均通过能量检测技术感知授权信道。当节点 N_i 利用能量检测器感知信道 C_x 时，检测概率 $p_{d,x,i}$ 和错误警告概率 $p_{f,x,i}$ 可定义为：$p_{d,x,i}=\Pr(D_x\geqslant\delta_x\mid H_{1,x})$ 和 $p_{f,x,i}=\Pr(D_x\geqslant\delta_x\mid H_{0,x})$。其中，$D_x$ 与 δ_x 分别表示检测到的能量值及检测门限，$H_{1,x}$ 与 $H_{0,x}$ 是对信道 C_x 忙碌或者空闲的假设。$p_{d,x,i}$ 表示一个忙碌的信道被正确检测出来的概率，$p_{f,x,i}$ 反映的是一个空闲信道被误判为忙碌的概率[13-14]。对于节点 N_i 而言，记信道 C_x 的可用概率即空闲信道 C_x 被正确检测出来的概率为 p_i^x：

$$p_i^x=p_{\text{off}}^x\cdot(1-p_{f,x,i}) \tag{3}$$

由于 CRN 信道的动态可用性，两节点之间能否通信不仅与发射功率、距离有关，还与它们的信道可用性有关。假设节点之间对感知结果的决策相互独立，记 N_i 与 N_k 在信道 C_x 上通信的链路可用概率为 q_{ik}^x：

$$q_{ik}^x=p_i^x\cdot p_k^x \tag{4}$$

(2)中继选择阶段

根据系统描述部分的介绍，N_i 检测到空闲信道之后，会在多个候选节点中选出下一跳进行数据传输。候选节点如果在感知过程中同样没有检测到 PU 信号，则可以按照指定的优先级顺序回复 CTS 消息。假设候选节点集中优先级排在第 j 位的节点为 N_j，当前面 $j-1$ 个节点都不可用时，N_j 有机会成为下一跳转发节点，概率 Q_{ij}^x 可通过式(5)得到。

$$Q_{ij}^x=\begin{cases} q_{ij}^x, & j=1 \\ q_{ij}^x\cdot\prod_{u=1}^{j-1}(1-p_u^x), & j\geqslant 2 \end{cases} \tag{5}$$

4.2 节点信任值

为了减小数据传输过程中节点选择性转发的影响，本文采用信任管理的方法对 N_i 的邻居节点进行可靠性考查。在该模型中，信任被定义为节点转发数据包的可靠程度，用0～1之间的数值来对该信任度进行量化与评估。通过对节点转发行为的监测与统计，利用 beta 信誉系统构建 t 时刻 N_i 对邻居节点 N_j 总的信任值 $T_{ij}(t)$。节点的信任值越大，转发数据包的可靠性越高，其被选为候选节点的概率就越大。可以采用改进的“Watchdog”[15]监控技术来监测节点转发行为。如果 N_i 正在对 N_j 进行流量监测，则 N_j 接收或转发数据包的情况对于 N_i 来说是可见的[16]。在此基础上，N_i 便可记录下 N_j 接收到的待转发数据包数，并统计 N_j 成功转发数据包的次数，最后利用 beta 分布函数实现对节点行为的可靠性估计。

beta 分布通常用来表示一个二元事件的后验概率，主要用参数 α，β 和 Γ 函数来表示，如式(6)所示：

$$f(p\mid\alpha,\beta)=\frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\cdot\Gamma(\beta)}p^{\alpha-1}(1-p)^{\beta-1} \tag{6}$$

其中,$0\leqslant p\leqslant 1$,$\alpha>0$,$\beta>0$。

beta 分布的概率期望如式(7)所示:

$$E(f(p|\alpha,\beta))=\frac{\alpha}{\alpha+\beta} \tag{7}$$

对于二元事件$\{X,\overline{X}\}$,用 s 和 f 分别表示 X 和$\overline{X}$出现的次数。通过对式(7)中的 α 和β 进行设置,事件 X 出现的概率密度可以表示为历史统计数据的函数,变量 p 表示 X 出现的概率。

$$\alpha=s+1,\beta=f+1 \tag{8}$$

(1)直接信任评估

在 CRN 中,将节点转发数据包的行为看作独立同分布的二项事件,N_i 监测到 N_j 成功向下一跳转发数据包的事件记为 X_{ij},未转发数据包的事件记为$\overline{X_{ij}}$。在每一个监测时长 τ 内,用 s_{ij} 和 f_{ij} 分别表示监测到的成功转发和未转发的次数。利用二项事件后验概率服从 beta 分布的特性,计算出 N_i 对 N_j 的直接信任值 $T'_{ij}(\tau)$,即节点 N_j 成功转发数据包的概率期望,如式(9)所示:

$$T'_{ij}(\tau)=\frac{s_{ij}+1}{s_{ij}+f_{ij}+2} \tag{9}$$

(2)间接信任评估

除了直接信任评估外,本文还考虑了第三方的间接信任评估,尤其是节点 N_j 刚刚进入网络内部,无法获取 N_i 与 N_j 之间的直接监测信息时,可以通过第三方的间接推荐对 N_j 进行可靠性估计。若 N_k 与 N_j 之间进行过数据传输,并且 N_k 处于 N_i 的一跳传输范围内,则 N_k 可以将其对 N_j 的信任评估值分享给 N_i,即 N_i 从 N_k 处获取关于 N_j 的间接推荐值。为防止节点提供不真实信息,故意诋毁普通节点或者隐瞒恶意节点的行为,同时为了增强信任管理机制的健壮性,融入间接信任评估 $T''_{ij}(\tau)$时必须考虑第三方节点的可信任程度,即:

$$T''_{ij}(\tau)=\frac{1}{n}\cdot\sum_{N_k\in\Omega_i\cap N_k\in\Omega_j}T_{ik}(t)\cdot T'_{kj}(\tau) \tag{10}$$

其中,n 表示同时为 N_i 与 N_j 邻居节点的 N_k 的总数,$T_{ik}(t)$ 表示 N_i 对 N_k 总的信任值,Ω_i 表示 N_i 的邻居节点集合。

(3)信任更新

定义 $T_{ij}(t)$为 N_i 对 N_j 的当前信任度,$T_{ij}(\tau)$为下一个监测期间内 N_i 对 N_j 的信任评估,利用 $T_{ij}(t)$和 $T_{ij}(\tau)$不断更新节点信任值,可以对节点长期以来的表现进行平均信任值的估计,如式(11)所示:

$$T_{ij}(t+\tau)=\omega\cdot T_{ij}(t)+(1-\omega)\cdot T_{ij}(\tau) \tag{11}$$

$$T_{ij}(\tau)=\delta\cdot T'_{ij}(\tau)+(1-\delta)\cdot T''_{ij}(\tau) \tag{12}$$

其中,ω 和 δ 为权重系数,$0<\omega<1$,$0<\delta<1$,节点初始信任值 $T_{ij}(0)=0.5$。为了使节点近期的转发行为对其信任值的估计产生较大的影响,一般将 ω 设置在 0～0.5 之间。

4.3　距离增益

在基于地理位置信息的路由算法中,距离目的节点最近的节点往往会被选为最佳下一跳。这是因为这样能够提供最大的距离增益,减少数据传输跳数,而且以距离增益作为指标的路由更加接近最短路径路由。节点 N_i 的候选转发节点 N_j 所能提供的距离增益 A_{ij} 为:

$$A_{ij}=d_{iD}-d_{jD} \tag{13}$$

其中,d_{iD} 和 d_{jD} 分别表示 N_i,N_j 到目的节点 D 之间的欧几里得距离,且 $d_{iD}=\sqrt{(x_i-x_D)^2+(y_i-y_D)^2+(z_i-z_D)^2}$,$(x_i,y_i,z_i)$,$(x_D,y_D,z_D)$分别表示 N_i 和 D 的坐标。本文同样将距离因素列入路由选择的考虑范畴,按照距离增益大小为候选节点分配优先级,距离增益越大,转发数据包的优先级越高。如图 3 所示,假设 N_j 和 N_k 是 N_i 的两个候选转发节点,由 $A_{ik}>A_{ij}$ 可知,N_k 能够提供更大的距离增益,因此 N_k 可以优先转发数据分组。

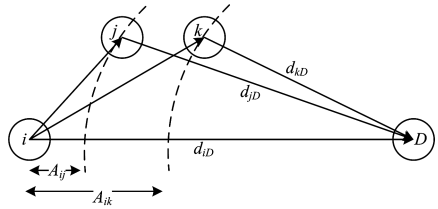

图 3　N_i 与 N_j,N_k 之间的距离增益

Fig. 3　Distance advancement between N_i and N_j, N_k

4.4　算法设计

S2OR 研究的是多跳 CRN 下的路由选择问题,为提高端到端的网络性能,需要为每一跳的发送节点选出高质量的候选链路。每一个中间发送节点 N_i 从其邻居节点集 Ω_i 中选择最佳候选转发节点 R_i^* 和数据信道 C^* 的目标为最大化每一跳的期望吞吐率 $ETT(R_i^x)$。

为获取最佳的 R_i^* 与 C^*,最直观的方法就是进行穷举搜索,将所有数据信道与所有可能的候选节点集进行组合,并计算出每一种组合所获得的期望吞吐率,然后进行比较,从而找出最佳的 R_i^* 与 C^*。设有 m 个信道和 n 个邻居节点,在中继选择阶段有 k 个节点参与排序,则一共需要计算$m\cdot\sum_{k=1}^{n}n!/k!\cdot(n-k)!$次期望吞吐率的值才能得到最佳的 R_i^* 与 C^*。当 n 无限增大时,穷举搜索任务量庞大,不易实现,故本文给出了创建候选节点集的启发式算法,如算法 1 所示。

算法 1　候选节点集的创建

Input:C ,N_i,Ω_i,r

Output:C^*,R_i^*

1. $C^*\leftarrow 0$,$R_i^*\leftarrow\Phi$,$ETT_{max}\leftarrow 0$
2. for each $C_x\in C$ do
3. $R_i^x\leftarrow\Phi$,$R\leftarrow\Phi$,$N_e\leftarrow 0$,$ETT_x\leftarrow 0$
4. while ($\Omega_i\neq\Phi$ && $|R_i^x|<=r$)
5. for each $N_j\in\Omega_i$ do
6. $R\leftarrow R_i^*+N_j$,sort R according to A_{ij}
7. if ($ETT>ETT_x$)then //根据式(1)计算 R 的 ETT
8. $ETT_x\leftarrow ETT$,$N_e\leftarrow N_j$
9. end if
10. end for
11. $R_i^x\leftarrow R_i^x+N_e$,sort R_i^x according to A_{ij}
12. $\Omega_i\leftarrow\Omega_i-N_e$
13. end while
14. if ($ETT_x>ETT_{max}$) then
15. $ETT_{max}\leftarrow ETT_x$,$C^*\leftarrow C_x$,$R_i^*\leftarrow R_i^x$
16. end if
17. end for
18. return (C^*,R_i^*)

输入一组数据信道 C 和 N_i 的邻居节点 Ω_i,候选节点的

最大数目为 r。对于任意一个数据信道 C_x，首先从邻居节点 Ω_i 中选出一个节点 N_j，与候选节点集 R_i^x 中的节点一起按照距离增益 A_{ij} 降序排列，并加入到临时的节点序列 R 中；然后根据式(1)计算出该序列带来的期望吞吐率 ETT，找出使得 ETT 最大的节点并将其加入到候选节点集 R_i^x 中；接着从剩余的邻居节点中重复上述节点选取过程，直到满足最大候选节点数要求或者没有剩余的邻居节点可被选取为止，如此便可获取每一个数据信道的最大期望吞吐率及其相应的候选节点序列；最后通过比较各数据信道的 $ETT(R_i^x)$ 值，返回一个使得期望吞吐率最大的信道 C^* 及相应的候选转发节点集合 R_i^*。当有 m 个信道和 n 个邻居节点时，利用该启发式算法至多需要计算 $m \cdot \sum_{k=1}^{n} k$ 次 ETT 的值即可得出最大期望吞吐率，时间复杂度远小于穷举搜索的时间复杂度。

5 仿真实验与结果分析

本节通过仿真的方法对文中提出的 S2OR 协议进行性能分析。首先介绍实验环境和参数设置，然后对实验结果进行讨论和分析。

笔者在 Matlab 平台上实现了 S2OR，并通过一系列仿真实验将 S2OR 与 OCR[4] 和 LASA[17] 协议的性能进行了对比分析。在 500 m×500 m 的正方形区域内随机分布着多个网络节点，每个节点的通信半径为 120m，源节点、目的节点分别固定在(0,0)和(500,500)。将区域内的节点分为普通节点和恶意节点，通过调节恶意节点的比例可以模拟出不同安全程度下的网络环境。为了实现选择性转发攻击，恶意节点在转发数据分组时以一个随机的概率拒绝转发或丢弃分组[11]。假设网络中有 6 个授权信道可供选择，每一个信道中的 PU 活动服从指数分布的 ON /OFF 模型。参考文献[14]，通过在0～1 之间产生随机数来模拟不同数据信道中 PU 处于 ON 状态的活跃特性。实验的基本参数设置如表 1 所列。

表 1 实验参数

Table 1 Experiment parameters

参数名称	参数值
区域大小	500m×500m
节点数量	[100,200]
节点传输范围/m	120
目的节点 D	(500,500)
最大传输速率/Mbps	2
信道数量	6
数据包大小/bytes	512
恶意节点比例	[0.1,0.8]
候选节点最大数 r	[2,4]
错误警告概率	[0,0.1]
ω	0.3
δ	0.8

为了分析 S2OR 的性能，主要从以下 3 个方面对上述几种协议进行对比分析：分组投递率、端到端延时、网络吞吐量。通过改变节点数量、恶意节点比例、PU 活跃程度等参数，设置不同的实验场景，然后观察协议的性能变化。将每一组实验运行 200 次，通过计算平均值来获取最终的实验数据。

5.1 分组投递率

首先将候选节点数分别设置为 2，3，4，恶意节点比例固定为 0.2，然后通过增加节点数来观察链路分组投递率的变化情况，如图 4 所示。从图 4 可以看出，随着节点数的递增，分组投递率不断变大。这是由于：一方面，网络中的节点分布越密集，一个节点的邻居节点越多，越有可能找到传输性能更好的转发节点；另一方面，当节点数一定时，候选转发节点数越多，分组投递率越大。在本文提出的路由算法中，低优先级的候选节点只有在高优先级节点不可用的情况下才有可能获得传输机会，因此从图 4 中可以看出，再多添加一个候选节点，投递率的增量逐渐减缓。这表明，在研究机会路由时应当选择适量的候选转发节点。在开销方面，候选节点数越多，节点之间的协调成本就越大。

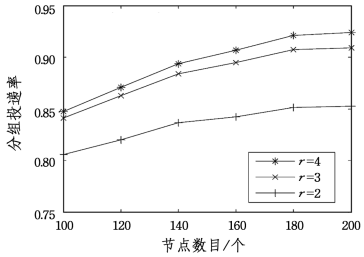

图 4 平均分组投递率随节点数目的变化情况

Fig. 4 Change of average packet delivery ratio with varying number of nodes

5.2 端到端延时

如图 5 所示，通过改变网络中恶意节点的比例来比较 S2OR 与 OCR 和 LASA 在延时方面的差异。端到端延时即数据包从发送端传递到接收端花费的总时间，通过将每一段链路上的延时进行累加，即可得出整个路径的延时。从图 5 中可以看出，随着恶意节点比例的增加，OCR 和 LASA 的平均端到端延时都大于 S2OR，且呈现出明显上升的趋势。对于 OCR 和 LASA 而言，当网络中的节点数目一定时，恶意节点比例越大，其成为转发节点的可能性就越大。恶意节点选择性转发攻击常常引起数据包丢失或分组转发失败，大大增加了重传延时。而 S2OR 在设计路由算法时，考虑了潜在的恶意节点丢包问题，并将节点转发行为的可信度融入路由指标设计中，使得发送节点尽可能选择高可靠性的转发节点，可以有效降低数据包丢失的可能性，从而减少分组重传的次数。

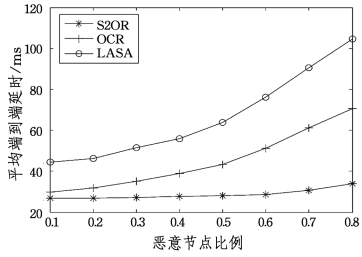

图 5 平均端到端延时随恶意节点比例的变化情况

Fig. 5 Change of average end-to-end delay varying with rate of malicious nodes

5.3 网络吞吐量

图 6 给出了平均吞吐量随恶意节点比例的变化情况。与 OCR 和 LASA 相比，随着恶意节点比例的增加，本文提出的 S2OR 吞吐量小幅度下降，且在相同恶意节点比例的情况下，其平均吞吐量最大。相比于 LASA 协议，OCR 采用的机会路

由思想可以有效缓解链路不稳定的情况，在一定程度上提高了网络吞吐量。但是该协议没有考虑数据传输过程中可能存在的恶意节点攻击问题，无法避免节点选择性丢包对数据传输造成的影响。LASA 虽然权衡了中继距离、传输时延和 PU 活跃程度 3 种因素，但同样没有考虑到网络中可能存在的节点选择性转发攻击。一旦恶意节点被选为下一跳转发节点，由它们发起的丢包行为将直接导致吞吐量的下降。

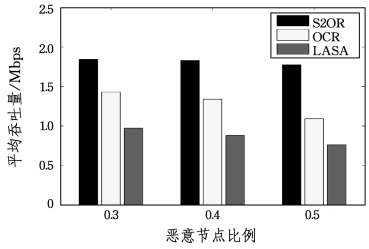

图 6　平均吞吐量随恶意节点比例的变化情况

Fig. 6　Change of average throughput varying with rate of malicious nodes

最后一组实验讨论了 PU 活跃程度对吞吐量的影响，其中节点总数、恶意节点比例分别设置为 200 和 0.2。从图 7 可以看出，3 种路由协议下的吞吐量随着 PU 活跃程度的增加有较为明显的下降趋势，说明在认知网络环境下，PU 活动对认知用户通信的影响较大。值得注意的是，当 PU 活跃程度相同时，S2OR 的吞吐量总是大于 OCR 与 LASA。这是因为该协议的机会路由方式可以有效缓解由 PU 活动带来的链路不稳定性问题，并且 S2OR 在设计指标时融合了链路质量、信道可用性、节点信任度等多种因素，增强了路径的健壮性与可靠性。

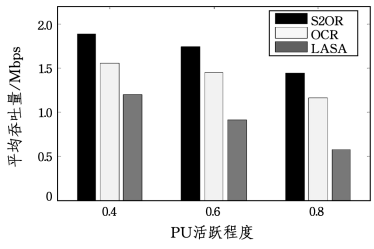

图 7　平均吞吐量随 PU 活跃程度的变化情况

Fig. 7　Change of average throughput varying with PU activity

结束语　本文提出一种带有信任管理的频谱感知安全机会路由协议，一方面分析了 PU 活动对路由选择的影响，另一方面考虑了节点潜在的选择性转发攻击对数据传输的影响。通过对节点转发行为的监测，计算出节点的信任度，其与链路质量、信道可用概率一起构成综合型的路由指标。基于该路由指标，本文进一步设计了创建候选节点集的启发式算法。仿真实验表明，该算法在有安全隐患的 CRN 环境下具有一定的优越性和可行性。

参 考 文 献

[1] AKYILDIZ I F, LEE W Y, CHOWDHURY K R. CRAHNs: Cognitive radio ad hoc networks[J]. Ad Hoc Networks, 2009, 7(5): 810-836.

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

[3] CESANA M, CUOMO F, EKICI E. Routing in cognitive radio networks: Challenges and solutions[J]. Ad Hoc Networks, 2011, 9(3): 228-248.

[4] LIU Y, CAI L X, SHEN X S. Spectrum-aware opportunistic routing in multi-hop cognitive radio networks[J]. IEEE Journal on Selected Areas in Communications, 2012, 30(10): 1958-1968.

[5] WEI Z, TANG H, YU F R. A trust based framework for both spectrum sensing and data transmission in CR-MANETs[C]// IEEE International Conference on Communication Workshop. IEEE, 2015: 562-567.

[6] DING L, SAVAS O, AHN G S, et al. Securing cognitive radio networks with distributed trust management against belief manipulation attacks[C]// IEEE GLOBECOM Workshops. IEEE, 2015: 1-6.

[7] WANG L, WANG Q, ZHANG H. Secure routing algorithm based on trust value for Ad Hoc networks[C]// International Conference on Computer Engineering, Information Science & Application Technology. 2016.

[8] LIN S C, CHEN K C. Spectrum Aware Opportunistic Routing in Cognitive Radio Networks[C]// Global Telecommunications Conference. IEEE, 2010: 1-6.

[9] PAN X, JIANG L, HE C. Spectrum aware multi-channel opportunistic routing in cognitive radio sensor networks[C]// International Conference on Computational and Information Sciences. IEEE Computer Society, 2013: 1558-1561.

[10] KHASAWNEH M, AGARWAL A. A secure routing algorithm based on nodes behavior during spectrum sensing in cognitive radio networks[C]// IEEE, International Performance Computing and Communications Conference. IEEE Computer Society, 2016: 1-8.

[11] ZHANG G, CHEN Z, TIAN L, et al. Using trust to establish a secure routing model in cognitive radio network[J]. Plos One, 2015, 10(9): e0139326.

[12] CUI C, MAN H, WANG Y, et al. Optimal cooperative spectrum aware opportunistic routing in cognitive radio Ad Hoc networks [J]. Wireless Personal Communications, 2016, 91(1): 101-118.

[13] AKYILDIZ I F, LO B F, BALAKRISHNAN R. Cooperative spectrum sensing in cognitive radio networks: A survey[J]. Physical Communication, 2011, 4(1): 40-62.

[14] REN J, ZHANG Y, ZHANG N, et al. Dynamic channel access to improve energy efficiency in cognitive radio sensor networks[J]. IEEE Transactions on Wireless Communications, 2016, 15(5): 3143-3156.

[15] DROMARD J, KHATOUN R, KHOUKHI L. A Watchdog extension scheme considering packet loss for a reputation system in wireless mesh network[C]// International Conference on Telecommunications. IEEE, 2013: 1-5.

[16] MARCHANG N, DATTA R. Light-weight trust-based routing protocol for mobile ad hoc networks[J]. Iet Information Security, 2012, 6(2): 77-83.

[17] YADAV R, MANE A. LASAR: Spectrum aware routing protocol for cognitive radio wireless networks[C]// International Conference on Communication, Information & Computing Technology. IEEE, 2015: 1-6.