

doi:10.13756/j.gtxyj.2019.01.010

无线通信技术

基于贝叶斯联合博弈的无线网络路由算法

刘 宁^{1,2}, 赵中堂^{1,2}, 管 涛^{1,2}

(1. 郑州航空工业管理学院 计算机学院, 郑州 450046; 2. 航空经济发展河南省协同创新中心, 郑州 450046)

摘要:在移动自组织网络中节点自私性难辨,而自私节点不尽全力转发数据会降低网络的可靠性。基于此,将联合博弈论建立在动态贝叶斯框架下,形成了一种基于贝叶斯联合博弈的数据传输算法。算法首先根据各节点的信念更新值发现不良节点;然后根据不良节点预估网络环境,计算各个预估环境的联合信念概率并归一化为联合体存在概率,计算各联合体下各节点的安全效益值,得到所对应的合约;接着运用先验中期拒绝找到贝叶斯稳态合约;最后通过设置安全容量计算权值的方式惩处不良节点,保证联合体内各节点安全容量和收益最大化。仿真结果表明,与其他两种算法相比,所提算法不仅有较少的路由延迟和控制开销比,还有较高的数据包投递率,有效降低了不良节点对网络的不利影响。

关键词:无线网络;博弈论;贝叶斯规则;纳什均衡;自私节点;惩处机制

中图分类号:TP393 **文献标志码:**A **文章编号:**1005-8788(2019)01-0059-07

Wireless Network Routing Algorithm based on Bayesian Joint Game Theory

LIU Ning^{1,2}, ZHAO Zhong-tang^{1,2}, GUAN Tao^{1,2}

(1. School of Computer Science, Zhengzhou University of Aeronautics, Zhengzhou 450046, China;

2. Collaborative Innovation Center for Aviation Economy Development of Henan Province, Zhengzhou 450046, China)

Abstract: In self-organizing networks, nodes are less self-identical, while self-serving nodes do not do their best to forward data to reduce the reliability of the network. Based on this, the joint game theory is established in the dynamic Bayesian framework, and a data transmission algorithm based on Bayesian game is formed. The algorithm first finds out the bad nodes according to the beliefs of each node, and then calculates the joint belief probability of each predicated environment and normalizes the joint existence probability according to the prediction of the network environment by the bad nodes. Next, we calculate the security benefit values of each joint under each joint, and obtain the corresponding contract. Then we use a priori medium to refuse to find the Bayesian steady state contract. Finally, the bad nodes are punished by setting the security capacity to calculate the weights, to ensure that the security capacity and benefits of each node in the federation are maximized and the data is effectively forwarded. The simulation results show that, compared with the other two algorithms, the proposed algorithm not only has less routing delay and control overhead, but also has a higher packet delivery rate, which effectively reduces the adverse effects of the bad nodes on the network.

Key words: wireless network; game theory; Bayesian rule; nash equilibrium; selfish node; punishment mechanism

0 引言

移动自组织网络是由移动节点通过无线链路自组成网、无需中心设备控制和无固定网络拓扑结构的分布式网络,被广泛应用于军事、灾后救援和野外探测中^[1-2]。网络中的节点一旦产生自私行为或被恶意劫持,会严重降低移动自组织网络的效率。针对不良节点检测与发现,学者们进行了大量研究。文献[3]设计了一种本地检测不良节点的安全机制;文献[4]利用基于认证授权的方式对移动自组织网络中的节点颁发数字证书,从而剔除不良节点;文献[5-7]设计了一种筛选不良节点的机制,从而撤销被劫持节点的证书;文献[8]通过评估与邻居节点的相遇持续时间和相对移动性来计算节点的信任度;文

献[9]通过监测邻居节点的数据分组和转发,利用贝叶斯推理计算邻居节点的信任度;Shabut 等人发现了移动自组织网络中节点虚假推荐的原因,并设计算法过滤恶意节点^[10];文献[11]充分考虑了各种信任评价因素的不确定性,并改进了权重计算方法;文献[12]以网络被攻击后所需的恢复时间作为收益定义完全信息静态博弈模型,并分析了网络安全性;文献[13]运用完全信息博弈理论对网络中发生的不良行为进行分析,使模型更符合实际无线网络;文献[14-15]均提出构建随机博弈模型,并在此基础上分别对网络生存性和网络协作传输开展了深入研究。

实际网络中,节点在联合协作中行为时刻变化,会出现不尽全力情况,基于此,本文提出一种新贝叶斯联合博弈路由算法。

收稿日期:2018-05-29

基金项目:国家自然科学基金资助项目(U1504609);河南省科技厅科技计划资助项目(172102210525);河南省高等教育教学改革研究与实践资助项目(2017SJGLX400,2017SJGLX406);河南省重点研发与推广专项资助项目(182102210454)

作者简介:刘宁(1980—),女,河南许昌人。讲师,硕士,主要研究方向为图像处理、无线传感网络。

通信作者:刘宁,讲师。E-mail: liu_ning1980@sina.com

1 贝叶斯联合博弈

1.1 节点合作通信

移动自组织网络中所有节点要进行信息交换^[16-17],信息交换功率的计算公式为

$$\overline{P_{i,j}} = \psi \kappa^2 d_{i,j}, \quad (1)$$

式中: ψ 为信息交换的平均信噪比; κ^2 为噪声水平; $d_{i,j}$ 为网络中节点间的最远距离。源节点 i 向目的节点 j 发送数据的损耗功率为

$$P_i^L = (P' - \overline{P_{i,j}})^+, \quad (2)$$

式中: P_i^L 为源节点 i 用于发送数据的损耗功率; P' 为源节点 i 的发送功率。

源节点 i 向目的节点 j 发送数据的速率为

$$T_{i,j}^S = \frac{1}{2} \log_2 \left(1 + \frac{\overline{P_{i,j}} \cdot |h_{i,j}|^2}{\kappa^2} + \frac{(\boldsymbol{\eta}_S^{\text{opt}})^H h_S^H h_S \boldsymbol{\eta}_S^{\text{opt}}}{\kappa^2} \right), \quad (3)$$

式中: $\boldsymbol{\eta}_S^{\text{opt}}$ 为防止窃听的最大化安全容量权重向量; $h_{i,j}$ 为源节点 i 到目的节点 j 的基带信道增益; h_S 为源点与目的节点间信道; S 为源节点组成的联合体。

源节点 i 向最远的目的节点 j 发送数据时,若有数据点 x 窃听信号,则安全容量损失为

$$T_{i,x}^e = \frac{1}{2} \log_2 \left(1 + \frac{\overline{P_{i,j}} \cdot |g_{i,x}|^2}{\kappa^2} \right), \quad (4)$$

式中, $g_{i,x}$ 为节点与窃听节点间的信道模型。

综上所述,节点 i 在区域内安全传输容量为

$$T_{i,j}^S = \left\{ \frac{1}{2} \log_2 \left[1 + \frac{\overline{P_{i,j}} \cdot |h_{i,j}|^2}{\kappa^2} + \frac{(\boldsymbol{\eta}_S^{\text{opt}})^H h_S^H h_S \boldsymbol{\eta}_S^{\text{opt}}}{\kappa^2} \right] - \max_{1 \leq x \leq X} \frac{1}{2} \left[1 + \frac{\overline{P_{i,j}} \cdot |g_{i,x}|^2}{\kappa^2} + \frac{(\boldsymbol{\eta}_S^{\text{opt}})^H h_S^H h_S \boldsymbol{\eta}_S^{\text{opt}}}{\kappa^2} \right] \right\}^+ \quad (5)$$

式中, X 为窃听点的最大值。

1.2 贝叶斯联合博弈

联合博弈理论研究成员之间收益分配问题。对于协作集体中的收益,当协作成员可以随意转移收益时称为可转移收益型,当协作成员不可随意转移收益时称为不可转移收益型。由于移动自组网络中节点的物理层数据传输受信道和能量等因素影响,各节点间的联合博弈收益不可随意转移,所以本文将节点联合博弈以不可转移收益类型进行理论分析。不可转移收益联合博弈定义为 $[N, V]$, N 为节点集合; $V: 2^N \rightarrow \mathbb{R}$ 为节点联合集合中各节点与实际收益间的映射。

定义1:不可转移收益贝叶斯联合博弈是不完全信息博弈的建模形式,可由五元组 $G = [N, E, P, I, B]$ 表示。式中: N 为贝叶斯联合博弈参与者集

合; E 为贝叶斯联合博弈参与者的环境集合; P 为参与者在各环境下的先验概率; I 为参与者对可能环境下所做的行动集合; B 为参与者的收益函数。

在贝叶斯联合博弈中存在一组可能的博弈环境集合 $E = \{e_1, e_2, \dots, e_n\}$, 参与者可形成任意联合体 $S \in N$ 。 $e(S)$ 为 e 环境下 S 联合体的合约收益值, $I(e)$ 为行动集合 I 下所对应的博弈环境集合, $P(e | I)$ 为在行动集 $I(e)$ 中 e 为真实博弈环境的概率。在每种环境内参与者进行联合博弈分析,并根据自己的收益预测对所处的博弈环境有所行动后所有的博弈参与者对各环境的先验概率。

1.3 博弈合约

在贝叶斯联合博弈中,每个参与者事先并不知道自己和别人的收益,因此参与者需要事先达成收益分配的合约。

定义2:博弈环境集合 E 与参与者收益向量集合 B^S 的映射即为博弈合约,博弈合约 $C^S: E \rightarrow B^S$ 。

$C_i^S(e)$ 为在博弈环境 e 中参与者 $i \in S$ 的收益; 在任意联合体 S 中满足: $\sum_{i \in S} C_i^S(e) \leq e(S)$ 。

1.4 贝叶斯稳态

合约的稳定性是贝叶斯联合博弈考虑的首要问题,每个参与者最关心的是自己在联合博弈中的收益,并且它们对收益的期望会随着评估的不同而改变。先验中期评估中,参与者 i 的联合收益 $B_i^S | I(e_i)$ 为当前预期博弈环境 e_i 在条件概率 $P(e_i | I(e_i))$ 下的收益。先验后期评估中,在当前真实的博弈环境 e_i 下,参与者的联合收益为 $B_i^S | e_i$ 。

在贝叶斯联合博弈中,参与者并非严格履行合约,当不能保证参与者最大收益时,参与者会在不同的先验评估阶段拒绝合约:

先验前期拒绝:联合体 $S \in N$ 先验前期合约 C^N , 当且仅当存在一种合约 C^S 满足 $C_i^S > C_i^N$ 。

先验中期拒绝:联合体 $S \in N$ 先验前期合约 C^N , 当且仅当存在博弈环境 e^* 和合约 C^S 满足 $C_i^S | I(e^*) \cap E^*(C^N, C^S) > C_i^N | I(e^*) \cap E^*(C^N, C^S)$ 。

先验后期拒绝:联合体 $S \in N$ 先验前期合约 C^N , 当且仅当在真实的博弈环境 e^* 和合约 C^S 下满足 $C_i^S | e^* > C_i^N | e^*$ 。

定义3:贝叶斯稳态。当贝叶斯联合博弈集合 N 中的任意成员对先验前期合约 C^N 进行评估时,不存在任何一种合约 C^S 能使参与者的收益更优,这里称合约 C^N 为贝叶斯稳态。

参与者可形成任意联合体 $S \in N, \Phi = \{S_1,$

$S_2, \dots, S_n$ }, 任意两个联合体不存在交集 $S_i \cap S_j = \emptyset$, 即任意参与者只可加入一个联合体 S 中, 那么 N 个参与者可以形成 $2^N - 1$ 个不同的非空联合体。实际移动自组织网络中存在窃听节点, 这势必会影响节点的数据传输, 要使无线网络顺利通信, 联合体成员个数必须大于窃听节点个数。若实际网络中存在 h 个窃听节点, 那么有效联合体个数为

$$Num_N = 1 + \sum_{m=h+1}^{N-1} \binom{N-1}{m} D_m, \quad (6)$$

式中, D_m 为贝尔数, 表示基数为 m 的集合划分数目。

2 贝叶斯联合博弈形成算法

2.1 发现邻居节点

根据邻居节点监测方法, 每个节点都会观察周

$$p_{ij}^{t_{ij}+1}(\alpha=0) = \frac{p_{ij}^{t_{ij}}(1-p_{err})}{p_{ij}^{t_{ij}}(1-p_{err}) + (1-p_{ij}^{t_{ij}}) \left\{ \left[1 - \frac{p_{err}}{(1-p_{ij}^{t_{ij}})(1+p_{err})} \right] (1-p_{err}) + \frac{p_{err}}{(1-p_{ij}^{t_{ij}})(1+p_{err})} \delta \right\}}; \quad (7)$$

一旦监测到节点 j 属于合作节点, 节点 i 会在下一个间隙 $t_{ij} + 1$ 更新节点 j 的合作概率:

$$p_{ij}^{t_{ij}+1}(\alpha=1) = \frac{p_{ij}^{t_{ij}} p_{err}}{p_{ij}^{t_{ij}} p_{err} + (1-p_{ij}^{t_{ij}}) \left\{ \left[1 - \frac{p_{err}}{(1-p_{ij}^{t_{ij}})(1+p_{err})} \right] p_{err} + \frac{p_{err}}{(1-p_{ij}^{t_{ij}})(1+p_{err})} (1-\delta) \right\}}; \quad (8)$$

式(7)、(8)中: $p_{ij}^{t_{ij}}$ 为间隙 t_{ij} 先验信息; p_{err} 为误报率; δ 为漏报率。当所有节点对不良节点 j 更新合作概率后, 利用所有节点对节点 j 的联合信念概率 $p(t_j^{N/\{j}\})$ 来评估:

$$p(t_j^{N/\{j}\}) = \prod_{i \in N/\{j\}} p_j^i(t_j = t_j^i), \quad (9)$$

式中, $N/\{j\}$ 为除节点 j 外的 N 个参与者集合; $t_j^{N/\{j\}}$ 为集合内其他节点 j 的信念向量集合; t_j 为节点 j 的信念; t_j^i 为节点 i 对节点 j 的信念反应; $p_j^i(t_j = t_j^i)$ 为

$$\varphi_i(S) = \begin{cases} \left[\frac{1}{2} \log_2 \left(\frac{\kappa^2 + \overline{P_{i,j}} \cdot |h_{i,j}|^2 + (\boldsymbol{\eta}_S^{\text{opt}})^H B_S \boldsymbol{\eta}_S^{\text{opt}}}{\kappa^2 + \overline{P_{i,j}} \cdot |g_{i,x}|^2 + (\boldsymbol{\eta}_S^{\text{opt}})^H B_g^x \boldsymbol{\eta}_S^{\text{opt}}} \right) \right]^+, & P_i^L > 0 \\ -\infty, & \text{其他} \end{cases} \quad (11)$$

为了找到贝叶斯纳什均衡联合体, 计算出 Num_N 个合约逐一分析, 根据先验中期拒绝机制, 如果没有其他合约 C^S 比当前合约 C^N 中的联合参与者收益更大, 合约 C^N 即为贝叶斯稳态。那么可在实际的物理层数据传输中形成与合约 C^N 对应的联合结构, 在所形成的联合结构体中, 节点间相互合作, 完成数据的传输。但若包含所有参与节点的大联合体是贝叶斯稳态之一, 当算法得到任何一个贝叶斯稳态后即停止搜索, 那么包含所有参与节点的大联合体不用分析就可以确定最终的联合结构, 为此, 本文将包含所有参与节点的大联合体对应的合约 C^N 作

围节点的存在情况, 根据自身功率剩余情况以及与其他节点的距离来确定潜在的合作节点^[18]。依据这种规则可以生成贝叶斯联合博弈者的集合 N 。

2.2 信念更新

为了防止不良节点的出现可能降低网络的传输效率, 节点需要不断更新其信念。同时, 也可以根据信念的波动情况推测节点的移动行为, 为锁定不良节点提供数据基础。在贝叶斯联合博弈参与者集合 N 中, 节点 i 会在第 t_{ij} 间隙监测节点的合作反馈^[19], 节点的类型包括合作节点和不良节点, 即节点 $\varphi \in \{\alpha=0(\text{不良节点}), \alpha=1(\text{合作节点})\}$ 。一旦监测到节点 j 属于不良节点, 则节点 i 会在下一个间隙 $t_{ij} + 1$ 更新节点 j 的合作概率:

节点 j 在节点 i 的信念反应下的存在概率; 将 $p(t_j)$ 归一化为每个贝叶斯联合博弈环境的存在概率。

2.3 贝叶斯联合博弈的形成

将贝叶斯联合博弈表示为 $G = [N, E, P, I, B]$ 五元组, 目的是求取贝叶斯纳什均衡的联合体。根据式(6)可以求出有效联合体个数, 在贝叶斯联合博弈环境集合中计算合约 C^S ,

$$C^S = \{\varphi(S) \in \mathbb{R} \mid \forall i \in S\}, \quad (10)$$

为初始合约。

2.4 基于马尔可夫链的贝叶斯联合体稳定分析

不同联合体调整的状态以一定概率在离散的时间内随机变化的过程近似于离散马尔可夫链^[20]。文章利用离散马尔可夫链验证贝叶斯联合博弈形成算法的稳定性。设离散马尔可夫链状态集合为 $\Theta = \{\Psi_1, \Psi_2, \dots, \Psi_{Num_N}\}$; $p_{\Psi, \Psi'}$ 为联合体状态转移概率:

$$p_{\Psi, \Psi'} = \begin{cases} \sum_{i \in J_{S, S'}} \frac{1}{Num} \frac{1}{|\Psi^*|} \tau_i(\Psi' \mid \Psi), & \Psi^* \neq \Psi \\ 1 - \sum_{\Psi'' \in \Phi, \Psi'' \neq \Psi} p_{\Psi, \Psi'}. & \Psi^* = \Psi \end{cases}, \quad (12)$$

式中: $J_{S,S'}$ 为联合体 S 转移到 S' 的过程中涉及到的节点集合; $\frac{1}{Num}$ 为节点被选中进行联合体转移的概率; $|\Psi^*|$ 为与节点所在联合体大小一致的并包含该节点的联合体个数; $\tau_i(\Psi' | \Psi)$ 为布尔数据, 当有节点在联合体 Ψ' 中的收益大于在联合体 Ψ 中的收益时, 节点会选择离开联合体 Ψ' , 此时 $\tau_i(\Psi' | \Psi)$ 为 1, 反之亦然。由此得到由转移概率 $p_{\Psi,\Psi'}$ 组成的转移矩阵 Q 、状态概率向量 $\vec{v}$:

$$\begin{cases} \vec{v}^T Q = \vec{v}^T \\ \vec{v}^T \vec{1}^T = 1 \end{cases}, \quad (13)$$

式中: $(*)^T$ 表示转置; $\vec{1}^T$ 为元素为 1 的集合; $\vec{v}^T = [v\Psi_1, v\Psi_2, \dots, v\Psi_{Num_N}]^T$, $v\Psi_{Num_N}$ 为联合体 Ψ_{Num_N} 的形成概率; $\vec{1}^T = [\Psi_1, \Psi_2, \dots, \Psi_{Num_N}]^T$; $\vec{v}$ 中的最大值 $v\Psi_*$ 所对应的联合体 Ψ_* 即为当前最稳定的联合体。

2.5 基于惩处机制的贝叶斯联合博弈

本文利用贝叶斯联合博弈算法对节点自私行为进行实时估测, 分析联合体合约, 找到贝叶斯纳什均衡的联合体, 实现数据的安全传输。对于检测的自私节点, 本文通过设置安全容量计算权值的方式惩处不良节点并对联合体结构进行及时调整, 以保证联合体各参与者安全容量和收益的最大化。

设节点自私度为 ρ_j ($0 \leq \rho_j \leq 1$), $\rho_j = 0$ 表示节点为合作节点, 其他情况为不良节点; μ 为节点行为, 且

$$\mu = \begin{cases} 0 & 0 < \rho_j \leq 1 \\ 1 & \rho_j = 0 \end{cases}, \quad (14)$$

当 $\mu = 1$ 时, 表示节点此时是合作的, 反之亦然。

若节点 i 为自私节点, 联合体内其他节点也会以相应的自私度进行自私节点数据的转发, 以这样的方式对自私节点进行惩罚, 则节点 j 在计算安全容量时的权重为

$$\eta_{i,j}^{S_{ew}} = \text{diag}[\eta_{i1}, \eta_{i2}, \dots, \eta_{i|S|}][1 - \rho_j, 1, \dots, 1 - \rho_j]^T. \quad (15)$$

由此, 对存在自私节点的数据转发时, 联合体内各节点安全容量为

$$T_{i,j}^{S_{ew}} = \left\{ \frac{1}{2} \log_2 \left[1 + \frac{\overline{P_{i,j}} \cdot |h_{i,j}|^2}{\kappa^2} + \frac{(\eta_{new}^S)^H h_{i,j}^H h_{i,j} \eta_{new}^S}{\kappa^2} \right] - \max_{1 \leq x \leq X} \frac{1}{2} \left[1 + \frac{\overline{P_{i,j}} \cdot |g_{i,x}|^2}{\kappa^2} + \frac{(\eta_{new}^S)^H h_{i,x}^H h_{i,x} \eta_{new}^S}{\kappa^2} \right] \right\}^+ \quad (16)$$

3 仿真对比分析

3.1 算法有效性

为了验证算法的有效性, 本文使用 NS-2 (Network Simulator-2) 仿真平台, 在 $2.5 \text{ km} \times 2.5 \text{ km}$ 范围内分布着 8 个节点端, 还有两个窃听端和两个目的端。仿真参数设置如下: $\kappa^2 = -90 \text{ dBm}$; 发送功率 $P' = 15 \text{ mW}$; 交换的平均信噪比 $\phi = 10 \text{ dB}$ 。在不完全信息下各节点端分布状态如图 1 所示。

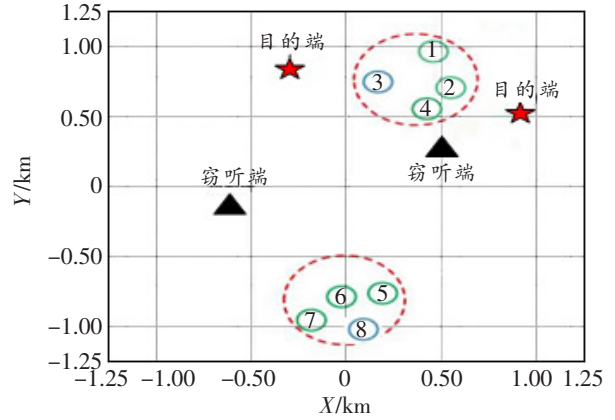


图 1 节点分布状态图

由图可知, 图中有两个联合体, 本文只对 $\{1, 2, 3, 4\}$ 联合体进行分析。在不完全信息下, 利用本文提出的贝叶斯联合博弈算法对节点进行信念更新, 更新后的节点信念如图 2 所示。

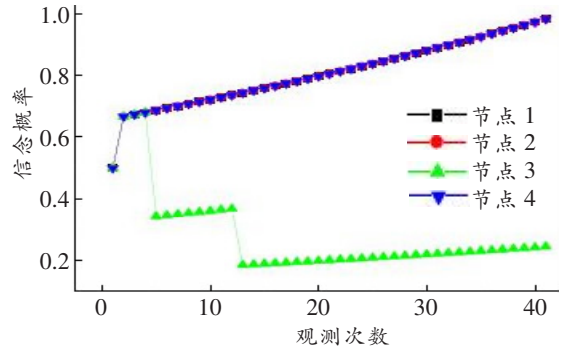


图 2 节点信念更新

由图可知, 节点 1、2 和 4 的合作概率远远高于节点 3, 随着观测次数的增多, 节点 3 的合作概率 < 0.2 , 由此可得节点 3 为不良节点, 根据其他 3 个节点对不良节点 3 的信念更新结果, 可形成 5 种不良节点 3 的预估分布 (估测环境)。

确定不良节点后, 在贝叶斯联合博弈 G 中贝叶斯联合博弈参与者 $N = 4$, 根据式 (6) 求取 $Num_4 = 6$, 可形成 6 种联合体, 分别表示如下: $S_1 = \{1\}, \{2\}, \{3\}, \{4\}$; $S_2 = \{1, 2, 3\}, \{4\}$; $S_3 = \{1, 2, 4\}, \{3\}$; $S_4 =$

$\{1,3,4\}, \{2\}; S_5 = \{2,3,4\}, \{1\}; S_6 = \{1,2,3,4\}$ 。在每个联合体中根据式(7)和式(8)计算节点 1、2 和 4 对节点 3 的信念更新,根据式(9)计算联合信念概率归一化为联合体存在的概率得到所对应的 6 个合约,运用先验中期拒绝找到贝叶斯稳态合约。每种联合体下所有节点的联合安全效益值如图 3 所示。

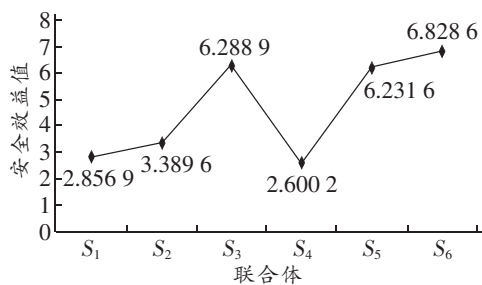


图 3 每种联合体下所有节点联合安全效益值

由图可知,联合体 $S_6 = \{1,2,3,4\}$ 为贝叶斯纳什均衡的联合体,其对应的安全容量效益值也最大,联合体 S_6 对应的合约 C^6 为贝叶斯稳态。运用马尔可夫链就 5 种预估网络环境分析贝叶斯联合体的状态分布。如图 4 所示,联合体 S_6 在 5 种预估网络环境中的状态概率最高。结果验证了经过本文贝叶斯联合博弈形成的贝叶斯稳态与经过马尔可夫链分析得到的贝叶斯稳态是一致的,进一步证明了本算法的有效性。

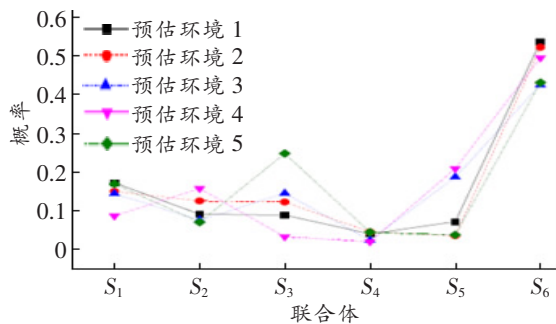


图 4 稳定联合体在预估环境下的概率分布

为了验证本文算法的性能,将本文算法与文献[21]基于动态贝叶斯博弈的数据包转发算法(Packet Forwarding Algorithm Based on Dynamic Bayesian Game, PFDBG)和文献[22]基于联盟形成博弈的机会网络路由(Base on Coalitional Game Routing, BCGR)等同类算法在 NS-2 仿真平台上实现。仿真实验中将 100 个节点随机地分布在 $2.5 \text{ km} \times 2.5 \text{ km}$ 的目标区域内,节点传输范围设为 25 m,数据包大小为 512 bytes,媒体接入控制(Media Access Control, MAC)层协议为 IEEE802.11,报文发送速率为 10 packets/s。节点采用随机路点移动模

型^[23],并设置不同比例的不良节点,节点的最大移动速度分别为 5、15、25、35 和 45 m/s。

3.2 路由延迟

路由延迟为发送数据包至目标节点所需的时间。图 5 所示为在不同的不良节点比例下 3 种算法的路由延迟统计结果。

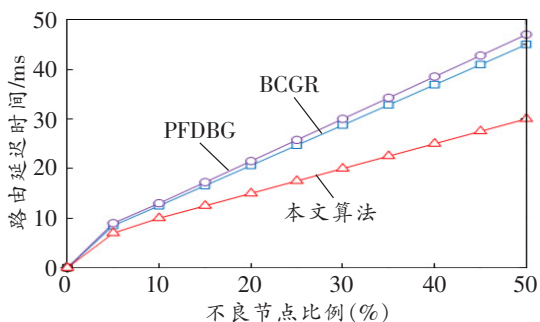


图 5 3 种算法路由延迟统计结果

由图可知,随着不良节点比例的加大,3 种算法的路由延迟随之增加。其中本文算法的性能优于其他两种算法,主要原因是本文算法使用贝叶斯联合博弈策略判断节点类型,针对不良节点采取惩处机制,开销极低。而 PFDBG 仅利用贝叶斯概率预测选择信任度大的节点作为中继节点进行数据转发,并没有考虑周围节点对所选中继节点的信念;BCGR 也是简单地采取贝叶斯预估中继节点,但算法增加了轮询和稳定阶段,一定程度上降低了不良节点被选中的概率。

3.3 数据包投递率

图 6 所示为在不良节点比例一定的情况下(20%),不同的节点移动速度与数据包投递率之间的关系曲线。

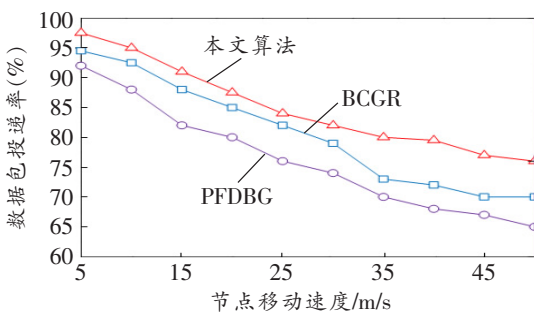


图 6 3 种算法的数据包投递率

数据包投递率是指目的端收到的数据包与发送端发送的数据包之比。由图 6 可知,随着节点移动的加速,3 种算法数据包投递率都在降低,但本文算法基于贝叶斯联合博弈理论及时形成贝叶斯稳态,在稳定的联合体下能有效地转发数据包;PFDBG 选择信任度高的节点作为中继节点,未考虑节点移动

对网络拓扑的影响;BCGR 考虑了不同的生存时间对稳定联合体转发数据的影响,一定程度上提高了数据包的投递率。

3.4 控制开销对比

图 7 所示为在不良节点比例一定的情况下(20%),不同的节点移动速度与路由开销之间的关系曲线。

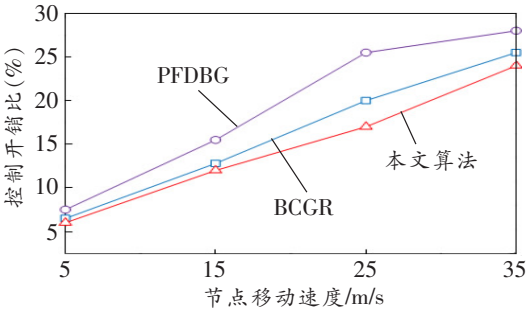


图 7 3 种算法的控制开销比

控制开销反映路由协议用于维持无线网络数据传输的控制信息数量。由图 7 可知,随着节点移动速度的增大,3 种算法的控制开销比也增大,其中,PFDBG 需要支付中继节点费用以激励节点转发数据,BCGR 在轮询和稳定阶段增大了开销。

4 结束语

本文提出了一种基于贝叶斯联合博弈的数据传输算法,实现了在不完全信息环境下寻找稳定联合体。算法根据各节点的信念更新值发现不良节点,通过设置安全容量计算权值的方式惩处不良节点,有效降低了不良节点对网络的不利影响。

参考文献:

[1] Xia H, Jia Z P, Zhang Z Y, et al. A Link Stability Prediction-based Multicast Routing Protocol in Mobile Ad Hoc Networks[J]. Chinese Journal of Computers, 2013,36(5):926-936.

[2] Das T, Roy S. Coordination based Motion Control in Mobile Wireless Sensor Network [C]//International Conference on Electronic Systems. Nagpur, Maharashtra, India; IEEE, 2014:231-236.

[3] Conti M, Di Pietro R, Spognardi A. Clone Wars: Distributed Detection of Clone Attacks in Mobile WSNs [J]. Journal of Computer and System Sciences, 2014, 80(3):654-669.

[4] Deebak B D. Secure and Efficient Mutual Adaptive User Authentication Scheme for Heterogeneous Wireless Sensor Networks Using Multimedia Client -

Server Systems [J]. Wireless Personal Communications, 2015, 87(3):1-23.

[5] Liu W, Nishiyama H, Ansari N, et al. Cluster-based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks[J]. IEEE Transactions on Parallel & Distributed Systems, 2012, 24(2):239-249.

[6] Xu H, Wang R, Jia Z. A Lightweight Certificate Revocation Scheme for Hybrid Mobile Ad Hoc Networks [J]. International Journal of Security & Its Applications, 2016, 10(1):387-402.

[7] Guo C, Xu H, Ju L, et al. A High-Performance Distributed Certificate Revocation Scheme for Mobile Ad Hoc Networks [C]// International Conference on Trust, Security and Privacy in Computing and Communications. Beijing, China; IEEE Computer Society, 2014:156-163.

[8] Feng R, Che S, Wang X, et al. A Credible Routing based on a Novel Trust Mechanism in Ad Hoc Networks[J]. International Journal of Distributed Sensor Networks, 2013(12):333-351.

[9] Wei Z. Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning[J]. IEEE Transactions on Vehicular Technology, 2014, 63(9):4647-4658.

[10] Shabut A M, Dahal K P, Bista S K, et al. Recommendation based Trust Model with an Effective Defence Scheme for MANETs[J]. IEEE Transactions on Mobile Computing, 2015, 14(10):2101-2115.

[11] Xia H, Yu J, Tian C L, et al. Light-Weight Trust-Enhanced on-Demand Multi-Path Routing in Mobile Ad Hoc Networks[J]. Journal of Network & Computer Applications, 2016, 62(C):112-127.

[12] Lye K W, Wing J M. Game Strategies in Network Security[J]. International Journal of Information Security, 2005, 4(1-2):71-86.

[13] White J, Park J S, Kamhoua C A, et al. Game Theoretic Attack Analysis in Online Social Network(OSN) Services[C]//International Conference on Advances in Social Networks Analysis and Mining. Niagara, Ontario, Canada; IEEE, 2014:1012-1019.

[14] Wang C, Miao Q, Dai Y. Network Survivability Analysis based on Stochastic Game Model[C]//Fourth International Conference on Multimedia Information Networking and Security. Nanjing, China; IEEE Computer Society, 2012:99-104.

[15] Yu M, Liu C, Qiu X, et al. Modelling and Analysis of Phishing Attack Using Stochastic Game Nets[C]//In-

- ternational Conference on Cyberspace Technology. Beijing, China: IET, 2013: 300—305.
- [16] 刘觉夫, 王建旭, 王作航. 基于博弈论的多跳认知无线网络协作路由算法[J]. 计算机工程与设计, 2017, 38(5): 1136—1142.
- [17] 刘群, 张立娇. 无线传感器网络中基于拍卖博弈的数据包转发算法[J]. 传感技术学报, 2013, 26(7): 991—997.
- [18] Vasudevan S, Towsley D, Goeckel D, et al. Neighbor Discovery in Wireless Networks and the Coupon Collector's Problem[C]//Proceedings of the 15th Annual International Conference on Mobile Computing and Networking. Beijing, China: ACM, 2009: 181—192.
- [19] Dehnie S. Reliable Cooperative Communications: A Signal Processing Approach[C] //Military Communications Conference. Baltimore, MD, USA: IEEE, 2011: 85—90.
- [20] 朱江, 张玉平. 非完全信息环境中一种基于隐马尔科夫的博弈式功率控制机制[J]. 电子学报, 2016, 44(12): 3004—3010.
- [21] 赵永辉, 史浩山. 一种无线传感器网络数据包转发的博弈论算法[J]. 西安电子科技大学学报(自然科学版), 2010, 37(6): 1125—1132.
- [22] 王英, 魏辰, 李云, 等. 基于联盟形成博弈的异构机会网络路由算法[J]. 重庆邮电大学学报(自然科学版), 2014, 26(5): 611—618.
- [23] Younes O, Thomas N. A Path Connection Availability Model for MANETs with Random Waypoint Mobility [C]//Computer Performance Engineering. Berlin, Heidelberg, Germany: Springer, 2012: 111—126.
-
- (上接第 48 页)
- [7] Narayanan P M. Microstrip Transmission Line Method for Broadband Permittivity Measurement of Dielectric Substrates[J]. IEEE Transactions on Microwave Theory & Techniques, 2014, 62(11): 2784—2790.
- [8] 马闯, 杨晓东, 谢浩, 等. 利用微波传感器检测生化溶液浓度[J]. 化学工程与装备, 2016, 36(4): 215—218.
- [9] Akhtar Z A M J. Time Domain Microwave Technique for Dielectric Imaging of Multi-Layered Media [J]. Journal of Electromagnetic Waves & Applications, 2015, 29(3): 386—401.
- [10] Lee H J, Lee J H, Moon H S, et al. A Planar Split-Ring Resonator-based Microwave Biosensor for Label-Free Detection of Bio-Molecules[J]. Sensors & Actuators B Chemical, 2012, 169(13): 26—31.
- [11] Withayachumnankul W, Jaruwongrungsee K, Tuantranont A, et al. Metamaterial-based Microfluidic Sensor for Dielectric Characterization[J]. Sensors & Actuators A Physical, 2013, 189: 233—237.
- [12] Ebrahimi A, Withayachumnankul W, Alsarawi S, et al. High-Sensitivity Metamaterial-Inspired Sensor for Microfluidic Dielectric Characterization[J]. IEEE Sensors Journal, 2014, 14(5): 1345—1351.
- [13] 何婉霞, 肖中银, 姜逸飞. 基于新型 CSRR 结构的 SIW 双频滤波器[J]. 电子测量技术, 2017, (10): 176—180.
- [14] 李芳, 李超. 微波异向介质: 平面电路实现及应用[M]. 北京: 电子工业出版社, 2011.
- [15] Ebrahimi A, Withayachumnankul W, Alsarawi S F, et al. Dual-Mode Behavior of the Complementary Electric-LC Resonators Loaded on Transmission Line: Analysis and applications[J]. Journal of Applied Physics, 2014, 116(8): P083705-1.