TrANTHOCNET:信任性蚁群自组织路由算法

刘衍珩,张 婧,王 健
(吉林大学计算机科学与技术学院,吉林长春 130012;吉林大学符号计算与知识工程教育部重点实验室,吉林长春 130012)

摘 要: 移动自组网依靠多点协作完成路由任务,可信的路由协议需要节点之间建立一定的信任关系,但大多数信任路由模型只追求路由的信任性而忽略了健壮性.本文基于 ANTHOCNET 算法,设计了兼顾信任性和健壮性的 TrANTHOCNET 算法.引入模糊 Petri 网的形式化推理算法处理节点之间的不确定关系,并利用位置信息对信息素实时更新以提高路由健壮性.实验结果表明 TrANTHOCNET 较 ANTHOCNET、AODV 和 T-AODV 均表现出较强的抵抗恶意节点攻击的能力,在路由性能方面也验证了本算法的有效性.

关键词: 移动自组网; 模糊 Petri 网; 蚁群算法; 信任路由
中图分类号: TP393.08 **文献标识码:** A **文章编号:** 0372-2112 (2012)02-0319-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.02.018

TrANTHOCNET: Confidence Ant Colony Routing Algorithm in MANET

LIU Yan-heng, ZHANG Jing, WANG Jian
(*College of Computer Science and Technology, Jilin University. Changchun, Jilin* 130012, *China*;
Key Laboratory of Symbolic Computation and Knowledge Engineering of Ministry of Education, Jilin University. Changchun, Jilin 130012, *China*)

Abstract: Mobile ad hoc network relies on multi-point to complete routing tasks in collaboration, relationship of trust need to be established in the trusted routing between two nodes, but most of trust routing model only pursue the confidence of route whereas neglecting robustness. Basing on ANTHOCNET algorithm, the TrANTHOCNET algorithm is designed while taking into account both routing confidence and routing robustness. We introduce Fuzzy Petri Net formalized reasoning process algorithm to deal with the uncertain relationship among nodes, and use location information to update pheromone in real time which enhances routing robustness. The experiment results show that the TrANTHOCNET behaves better than ANTHOCNET, AODV and T-AODV when facing malicious nodes, it also has been proved effectively in routing performance.

Key words: mobile ad hoc network; fuzzy petri net; ant colony algorithm; trusted routing

1 引言

ANTHOCNET[1]是一种依据蚂蚁觅食活动、以 ACO (Ant Colony Optimization)算法为基础和面向移动自组网的路由算法.它较目前常用的 AODV(Ad hoc On Demand Distance Vector)协议具有更低的端到端延迟.移动自组网拓扑变化频繁,即使信息素高的路径也可能随时断开而无法继续连通.另外,移动自组网中经常存在自私和恶意节点发起如丢包、欺骗和共谋等攻击等行为,ANTHOCNET 算法对这样的恶意节点无能为力.

Petri 网[2]技术能够很好地描述并发行为,可方便地与其他技术和理论融合,是研究离散事件动态系统的一种有力工具.模糊 Petri 网[3,4](Fuzzy Petri Net, FPN)比普通 Petri 网具有更强的表示能力.为了简化模糊 Petri 网模型,文献[5]提出了一种形式化推理算法,将模糊 Petri 网与矩阵运算相结合,简化了模糊推理过程.MANET 的移动特性产生大量的不确定信息,模糊 Petri 网能对不确定信息进行很好地处理且计算精度高.本文将采用形式化推理算法来评估网络中节点之间的推荐信任值.

2 信任路由模型及协议

MANET 中数据包的传递依靠节点间合作完成,因此设计信任评估机制对提高网络性能具有重要意义.一般的信任评估过程由信息收集、信息分析和动作执行组成.目前的信任模型根据其实现方法可以分为[6]:基于信息理论、基于社会网络和群体理论、基于图论和基于

收稿日期:2011-03-17;修回日期:2011-10-20
基金项目:国家自然科学基金(60973136,61073164);欧盟 BTG 合作项目(155776-EM-1-2009-1-IT-ERAMUNDUS-ECW-L12);吉林大学基本科研业务费项目(201103136)

博弈理论.文献[7]提出的基于信息理论的信任机制采用请求应答机制获得节点间的信任评价,导致一些额外的开销,也缺乏安全性.文献[8]提出的信任机制基于社会网络和群体理论将网络分成一跳且不相连的簇,通过轮换最信任的簇首选择信任路由,但当恶意节点增多的时候,将导致信任度高的节点无法参与路由.基于图论的信任模型依赖于对图的实时分析,计算复杂度高,不适于实时性要求高的移动自组网,例如文献[9]提出的基于图论的信任模型仅完成了对信任路由的选取,并没有很好地分离恶意节点.文献[10]属于基于博弈理论一类的,该模型的选择策略需要一个中心负责评估,这就产生两个问题:由谁执行评估和多长时间能选出一个可接受的策略集.文献[11]基于 AODV 协议增加了攻击检测功能,同时在节点之间建立了信誉机制,但该算法仅考虑了节点评价的主观因素,忽略了节点移动等客观因素.AntTrust[12]算法基于多 Agent 系统对 ACO 算法增加了信任机制,实现三方面信任信息源(有过交互的邻居节点、没有过交互的邻居节点和外部节点)的采集需要在每个节点上安装监听蚂蚁,产生过多的额外开销,而且该算法待定参数较多,增加了算法的复杂性.

本文针对移动节点信任关系的不确定性,利用模糊 Petri 网的形式化推理算法,借助节点间的通信次数以及路径上的信息素完成节点间间接信任值的计算,降低了计算复杂度;通过监听转发结果奖惩节点,有效地隔离恶意节点,完成信任网络的构建;同时在更新信息素时通过将预测的节点的移动趋势转化成信息素的变化量,提高了目标路由的健壮性.

3 TrANTHOCNET

基于 ANTHOCNET 算法的路由建立和路由扩展过程且引入信任概念,改变了信息素的更新机制以及数据包转发规则,设计了兼顾路由信任性和健壮性的 TrANTHOCNET(Trusted ANTHOCNET)算法.利用直接信任值表征节点之间过去的交互结果,模糊 Petri 网估算节点之间的间接信任值,依据节点的位置信息、移动方向和运动速度更新信息素,改变原算法中信息素的取值范围,从大于 1 变为[0 - 1],在转发数据包决策下一跳时考虑节点间的信任值和路径上的信息素,算法中包含:反应式前向蚂蚁、反应式后向蚂蚁、主动式前向蚂蚁、主动式后向蚂蚁、修复前向蚂蚁和修复后向蚂蚁,各有分工.综合每种蚂蚁获得的信息完成对最优路径的寻找.

源节点 s 向目的节点 d 发送数据包的执行过程如下:

(1)节点 s 查看自己的路由表是否有到达目的节点 d 的路由,若有则利用路由表中的路由传递数据包,否则将数据包存在缓存区,启动路由建立过程,建立可用路由,同时启动路由扩展过程;

(2)路由网建立之后,节点 s 从路由表中获取可到达目的节点 d 的下一跳节点集合 T;

(3)利用模糊 Petri 网形式化推理算法估算 s 与 T 中每个节点之间的间接信任值,与 s 和 T 中每个节点之间的直接信任值取平均值,同时综合信息素的值,选出最优的下一跳节点 i;

(4)节点 s 向节点 i 发送数据包,同时监听节点 i 的行为和更新节点 s 和节点 i 之间的信任值,根据 i 的行为给出更新节点 s 和节点 i 之间的直接信任值;

(5)节点 i 转步骤 1 继续转发数据包,直至到达目的节点 d.

下面逐一介绍每一步的主要环节.

3.1 路由建立与路由扩展

3.1.1 反应式路由建立

反应式路由建立过程由反应式前向蚂蚁和反应式后向蚂蚁两种控制包完成.其目的是快速寻找可用于数据包传输的路由.

当源节点 s 向目的节点 d 发送数据包且在路由表中没有到达 d 的可用路由或者中间节点 s 转发到达目的节点 d 的数据包没有可用的下一跳时,s 启动反应式路由建立过程,如图 1 所示,坐标单位为 cm.①节点 s 生成一只反应式前向蚂蚁,广播给邻居节点,反应式前向蚂蚁中包含源节点的 ID 号及其位置信息、目的节点的 ID 号以及一条该蚂蚁从源节点 s 到达目的节点 d 经历的节点链表;②邻居节点收到反应式前向蚂蚁时,如

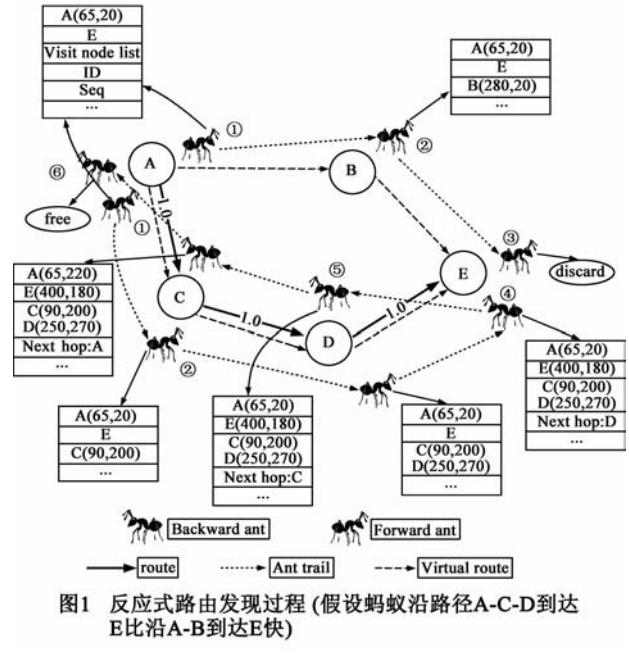

图1 反应式路由发现过程(假设蚂蚁沿路径A-C-D到达E比沿A-B到达E快)

果自己有到达目的节点 d 的路由时则按照此路由转发该蚂蚁,否则继续广播该蚂蚁.反应式前向蚂蚁每到达一个节点存储当前节点的位置信息(x,y)以用于信息素的更新;③当节点收到重复的前向蚂蚁时,则直接丢弃;④当反应式前向蚂蚁到达目的节点 d 时,被转变成反应式后向蚂蚁,添加变量 totalpheromone 存储反应式后向蚂蚁沿途释放的信息素总量,携带反应式前向蚂蚁所携带的信息;⑤反应式后向蚂蚁不被广播,它将沿着前向蚂蚁访问过的路径原路返回源节点 s,每经过一个节点 i,更新 i 到目的节点 d 的平均跳数,在路径(i,k)上释放信息素,节点 k 为后向蚂蚁经历的上一跳节点;⑥直至回到源节点 s,该蚂蚁被丢弃.随后,源节点 s 向目的节点 d 发送数据包.至此反应式路由建立过程结束.

当中间节点 i 发现到达目的节点 d 有多条可用路由时,按照概率 P_{ik}^{d}从备选的节点中选择最优的下一跳节点 k 传递反应式前向蚂蚁,备选的下一跳节点与节点 i 之间的信任值要大于一个阈值 δ:

$$P_{ik}^{d}=\frac{(\tau_{ik}^{d})^{\beta}}{\sum_{j\in N_{s}^{d}}(\tau_{ij}^{d})^{\beta}} \tag{1}$$

其中,τ_{ik}^{d}表示当前节点 i 经节点 k 到目的节点 d 的路径(i,k)上的常规信息素值,同一条路径到达不同目的节点的信息素值也不尽相同. N_{s}^{d} 为节点 i 邻居中可到达目的节点 d 的节点集合;$\beta\geqslant 1$,为控制蚂蚁寻路行为的参数.

反应式后向蚂蚁每到一个节点更新路由表中的路由信息,跳数的更新方式如下:

$$h_{ik}^{d}=\alpha h_{ik}^{d}+(1-\alpha)h \tag{2}$$

其中,h_{ik}^{d}为节点 i 经节点 k 到达目的节点 d 的平均跳数历史记录;h 表示当前节点 i 经节点 k 到达目的节点 d 的跳数;$\alpha\in[0,1]$表示对新信息的采纳程度.

当前节点 i 经节点 k 到达目的节点 d 的路径(i,k)的信息素按式(3)更新:

$$\psi_{ik}^{d}=\alpha\psi_{ik}^{d}+(1-\alpha)\Delta\psi_{ik}^{d} \tag{3}$$

其中,ψ_{ik}^{d}表示当前节点 i 经节点 k 到目的节点 d 的路径(i,k)上的信息素值,常规信息素和虚拟信息素的更新均利用此式,$\Delta\psi_{ik}^{d}$表示信息素的变化量.

3.1.2　信息素变化量的计算方法

蚁群算法通过更新路径上的信息素体现网络中路径的好坏,因此要实时更新信息素,以保证路径上信息的新鲜性.本算法预测节点的运动趋势,将运动距离和移动方向转化成信息素的变化量.算法中每个节点存有信息素表,记录着常规信息素和虚拟信息素,所有类型的后向蚂蚁负责常规信息素的更新,稍后会介绍虚拟信息素的更新方式.信息素的取值范围为$[0,1]$(信息素初始化为 0).反应式后向蚂蚁更新信息素时,从后向蚂蚁的访问节点链中获取前向蚂蚁存储的当前节点 i 和上一跳节点 k 的位置信息(x_{i1},y_{i1})和(x_{k1},y_{k1}),表示为向量 $\boldsymbol{r}=(x_{k1}-x_{i1},y_{k1}-y_{i1})^{\mathrm{T}}$,从后向蚂蚁携带信息中获取这两个节点当前的位置信息(x_{i2},y_{i2})和(x_{k2},y_{k2}),表示为向量 $\boldsymbol{t}=(x_{k2}-x_{i2},y_{k2}-y_{i2})^{\mathrm{T}}$,利用式(4)求得两个向量之间夹角的余弦:

$$\cos\theta=\frac{\boldsymbol{r}\cdot\boldsymbol{t}}{|\boldsymbol{r}|\times|\boldsymbol{t}|} \tag{4}$$

其中,$\cdot$表示两个向量的内积,$|\boldsymbol{r}|$和$|\boldsymbol{t}|$分别表示向量 $\boldsymbol{r}$ 和 $\boldsymbol{t}$ 的模,信息素的变化量为:

$$\Delta\tau_{ki}^{d}=\frac{(1+\cos\theta)\times\Delta d}{2l},\cos\theta\in[-1,1] \tag{5}$$

其中,l 表示当前节点 i 到目的节点 d 的跳数,$\cos\theta$ 的取值范围为$[-1,1]$,$\frac{(1+\cos\theta)}{2}$将取值范围约束到$[0,1]$,当 $\cos\theta$ 取 1 时,说明两节点运动相对静止,该式取值为 1;当 $\cos\theta$ 取值为 0 时,说明运动变化为 90 度,此时该式取值为 0.5;当 $\cos\theta$ 取 -1 时,此时节点运动到与原来相反的方向,该式取值为 0.Δd 为记录的节点 i 和节点 k 之间的距离与当前这两个节点之间的距离之比,当 $\Delta d\geqslant 1$ 时说明节点之间的距离变小,此时算法中按 $\Delta d=1$ 处理;$\Delta d<1$ 时,预测两个节点可能向相反的方向运动,蚂蚁释放的信息素的量要按比例相应地减少,用两节点之间的距离变化和运动角度变化来衡量节点间的相对运动,减小估计误差. l 作为分母使得当前节点距离目的节点越近,在该路径上留下的信息素越多.

当后向蚂蚁到达源节点时改变更新信息素的策略为:

$$\Delta\tau_{ki}^{d}=\frac{totalpheromone}{l} \tag{6}$$

Totalpheromone 为后向蚂蚁在经过的路径上释放信息素的总量,使用源节点经该下一跳到达目的节点 d 的路径上的信息素平均量衡量该条路径的优劣.

3.1.3　主动式路由扩展

该过程与原 ANTHOCNET 的主动式路由扩展相同,分为两部分:信息素扩散和路由扩展.信息素扩散过程利用 Hello 机制将可用的信息素在整个网络中传播,路由扩展过程历经会话的开始至结束,该过程搜寻从源节点到目的节点之间更多可用路由.

3.2　数据包传递

经过路由建立和扩展过程,每个节点建立起各自的路由表,源节点开始向目的节点传递数据包,同时每个节点还维护一个信任表,表中包含对其他节点的直接信任值,由于路由是单向的,因此该信任值不具有对称性,直接信任值的获取通过监听节点的转发行为进

行更新,取值范围为[0,1].初始化时任意节点之间的信任度为0.5,代表陌生关系,超过0.5时表示信任,低于0.5表示不信任.源节点 s 向目的节点 d 发送数据包时,转发路径上的每个中间节点根据信息素和信任值进行实时的路由选择.

3.2.1 数据包转发规则

节点 s 选择下一跳发包,利用节点 s 与可到达目的节点 d 的邻居节点 i 之间的信任值与信息素计算将数据包转发给节点 i 的概率 p_{si}^{d}:

$$P_{si}^{d}=\frac{(\tau_{si}^{d})^{\beta_1}(T_{si}^{'})^{\beta_2}}{\sum_{j\in N_s^d}(\tau_{sj}^{d})^{\beta_1}(T_{sj}^{'})^{\beta_2}} \tag{7}$$

其中,$T_{si}^{'}$为节点 s 与节点 i 之间直接信任值和间接信任值的平均值,间接信任值的计算将在下一节介绍.

节点 s 将数据包转发给下一跳节点 i 的同时启动定时器,在有限时间内监听下一跳节点 i 是否转发了节点 s 发给它的数据包,若成功转发则增加节点 s 与节点 i 之间的直接信任值作为奖赏,否则相应地减少信任值作为惩罚,奖惩方式[13]如式(8)所示.

$$T_{si}(t)=\begin{cases}T_{si}(t-1)-T_{si}(t-1)\cdot e^{\frac{\eta(s,i)}{\eta(s,i)-1}}, & \text{dec}\\ T_{si}(t-1)+(1-T_{si}(t-1))\cdot e^{\frac{\eta(s,i)-1}{\eta(s,i)}}, & \text{inc}\end{cases} \tag{8}$$

其中,T_{si}为节点 s 和节点 i 之间的直接信任值,$\eta(i,j)$为两节点速度相似比.如果节点 i 不成功转发数据包的次数比成功转发数据包的次数大于阈值,则直接将相应的直接信任值设置为0.不成功传递可能是由于链路断裂,也可能是因为恶意节点的存在,通过若干次实验证明设置阈值为2能更好地识别恶意节点.如此直到将数据包传递到目的节点 d.

3.2.2 模糊 Petri 网

由于移动自组网的拓扑变化频繁,节点间的信任关系无法长久维持,具有不确定性,模糊 Petri 网很适合处理不确定关系,因此 TrANTHOCNET 算法利用模糊 Petri 网模拟节点间信任关系的演化.节点间信任关系包括直接信任和间接信任,如果节点间有过会话历史,彼此将对对方的行为做出评价,否则借助其他节点的推荐,实现对陌生节点行为的评价.

依据文献[5]定义 TrANTHOCNET 算法中 FPN 的六元组表示形式为

$$(P,T,I,O,\tau(t),S_0(P))$$

其中:$P=\{p_1,p_2,\cdots,p_n\}$为命题的有限集合,命题表示节点之间的信任关系;$T=\{t_1,t_2,\cdots,t_n\}$为推荐规则的有限集合,规则由命题组成;I 是定义在 P 映射到 T 上的模糊关系,表示命题到推荐规则的对应关系和连接的权系数,满足 $0<I(p_i,t_j)\leqslant 1$;O 是定义在 T 映射到 P 上的模糊关系,表示推荐规则到命题的连接情况和每个输出连接的可信度,满足 $0<O(t_i,p_j)\leqslant 1$;$\tau(t)$是定义在推荐规则集合 T 上取值范围为[0,1]的实数函数,表示规则的触发阈值;$S_0(P)$是定义在命题集合上取值范围为[0,1]的实数函数,表示命题在推理开始时的初始标记状态,即已知命题的可信度,未知命题的可信度为0.

根据对 TrANTHOCNET 算法中 FPN 的定义,结合模糊 Petri 网矩阵推理形式,通过实例1描述具体的形式化推理过程:

实例1 假设有两条推荐规则并且由这两条规则得到推荐规则3(下面提到的1,2,3,4为节点号):

规则1:由 $U1$ 和 $U2\rightarrow U5$

规则2:由 $U3$ 和 $U4\rightarrow U6$

规则3:由 $U5$ 和 $U6\rightarrow U7$

$P=\{U1,U2,U3,U4,U5,U6,U7\}$,$T=\{$规则1,规则2,规则3$\}$.

命题 $U1$ 表示节点1信任节点2且通信次数为4,初始信任值为0.6,信息素为0.5;命题 $U2$ 表示节点2信任节点3且通信次数为6,初始信任值为0.4,信息素为0.3;命题 $U5$ 表示节点1接受节点2的推荐,初始信任值为0;命题 $U3$ 表示节点1信任节点4且通信次数为1,初始信任值为0.8,信息素为0.4;命题 $U4$ 表示节点4信任节点3且通信次数为9,初始信任值为0.5,信息素为0.2;命题 $U6$ 表示节点1接受节点4的推荐,初始信任值为0;命题 $U7$ 表示节点1信任节点3,初始信任值为0.

φ_{ij}为通信次数比,如有 $\varphi_{11}=4/(4+6)=0.4$,$\varphi_{12}=0.6$,$\varphi_{23}=0.1$,$\varphi_{24}=0.9$.$\varphi_{35}=(4+6)/(4+6+1+9)=0.5$,$\varphi_{36}=0.5$.$\Phi_{ij}$的值为节点间信息素的乘积.$\Phi_{51}=0.5*0.3=0.15$,$\Phi_{62}=0.08$,$\Phi_{73}=0.15*0.08=0.012$,$S_0=[0.6,0.4,0.8,0.5,0,0,0]$,$\tau=[0.2,0.2,0.2]$.因此可得到输入矩阵和输出矩阵为:

$$\boldsymbol{\Delta}=\begin{bmatrix}0.4&0&0\\0.6&0&0\\0&0.1&0\\0&0.9&0\\0&0&0.5\\0&0&0.5\\0&0&0\end{bmatrix},\ \boldsymbol{\Gamma}=\begin{bmatrix}0&0&0\\0&0&0\\0&0&0\\0&0&0\\0.15&0&0\\0&0.08&0\\0&0&0.012\end{bmatrix}$$

(1)利用 $E=\boldsymbol{\Delta}^{\mathrm{T}}\cdot S_0$ 计算推荐规则左部的可信度,得 $\boldsymbol{E}=[0.48,0.53,0]$;

(2)将矩阵 $\boldsymbol{E}$ 中 E_i 小于变迁阀值的项赋值为 0,$\boldsymbol{E}=[0.48,0.53,0]$;

(3)利用 $\boldsymbol{S}'=\boldsymbol{\Gamma}\cdot H$ 计算推荐规则右部的可信度,$\boldsymbol{S}'=[0,0,0,0,0.072,0.0424,0]^{\mathrm{T}}$;

(4)利用 $\boldsymbol{S}=\boldsymbol{S}_0\oplus\boldsymbol{S}'$ 计算当前可得到的所有命题的可信度,得到 $\boldsymbol{S}=[0.6,0.4,0.8,0.5,0.072,0.0424,0]^{\mathrm{T}}$;

(5)利用 $\boldsymbol{S}$ 代替 $\boldsymbol{S}_0$,反复执行(1)~(4)步,直到 $\boldsymbol{S}$ 不再发生变化.可得最终的推理结果为:$\boldsymbol{S}=[0.6,0.4,0.8,0.5,0.072,0.0424,0.003]^{\mathrm{T}}$.

即节点 1 对节点 2 的信任度为 0.003,这个信任程度是非常低的,原因是路径上的信息素比较少,当节点之间的信任度比较低时,也会出现类似的结果,即对推荐信息并不信任.在 TrANTHOCNET 算法运行之初,节点间的交互贫乏时就会出现上述情形,这是合理的.网络中有可能存在恶意节点,因此在选择信任路径时设定阈值进行约束.

4　模拟实验

实验环境为网络仿真工具 Qualnet 5.0.场景大小为 2400m × 800m.节点在实验区域内被随机放置,采用 RWP(Random Waypoint)移动模型,停留时间为 30s.随机选取源节点和目的节点.共产生 20 对 CBR(Constants Bit Rate)数据传输,数据传输将在 0 ~ 100s 内随机选择一个时间启动,模拟时间为 500s,每个实验的采样间隔均为 10s.由于如何确定最优组合参数使蚁群算法求解性能最佳一直是一个极其复杂的优化问题,大多情况依据经验而定[14],因此本文通过多次实验,发现将参数 β,β_1 和 β_2 取值为 3,因子 α 取值 0.7 时算法的收敛性和性能最好.在实验图中,R 表示节点的通信半径,N 表示网络中节点的总量,*MaxSpeed* 表示节点运动的最大速度,*MinSpeed* 表示节点运动的最小速度.吞吐量定义为在单位时间内到达目的节点的字节数.丢包率为运行时间内网络中丢弃的数据包总量与所有节点生成的数据包总量之比.抖动为相邻数据包的延迟差与相邻数据包的序号差之比.平均延迟为所有数据包到达目的节点的时刻与源节点发包时刻之差的平均值.

图 2 给出当恶意节点不存在时,ANTHOCNET,TrANTHOCNET,AODV 和 T-AODV 四个算法的性能比较.T-AODV[15]在 AODV 算法中添加信任机制,仅通过节点的过往行为,建立节点之间的信任关系.从图中可以看出,TrANTHOCNET 算法的吞吐量和延迟略差于 ANTHOCNET 算法,由于 TrANTHOCNET 中节点选择下一跳时,会考虑两者之间的信任值,如果邻居节点的信任值小于阈值,则该节点将不作为备选的下一跳,因此减少了下一跳的选择,或者导致没有下一跳,致使网络的性能降低.AODV 和 T-AODV 协议在本实验中设定的场景下,吞吐量和丢包率要优于 ANTHOCNET,但延时和抖动要比 ANTHOCNET 差,因为统计数据包的发包时间和收包时间时,被丢弃包的收包时间被记为 -1,发包时间必定小于收包时间,在计算延时和抖动时,被丢弃包不被计算在内.T-AODV 要略优于 AODV,因为 T-AODV 协

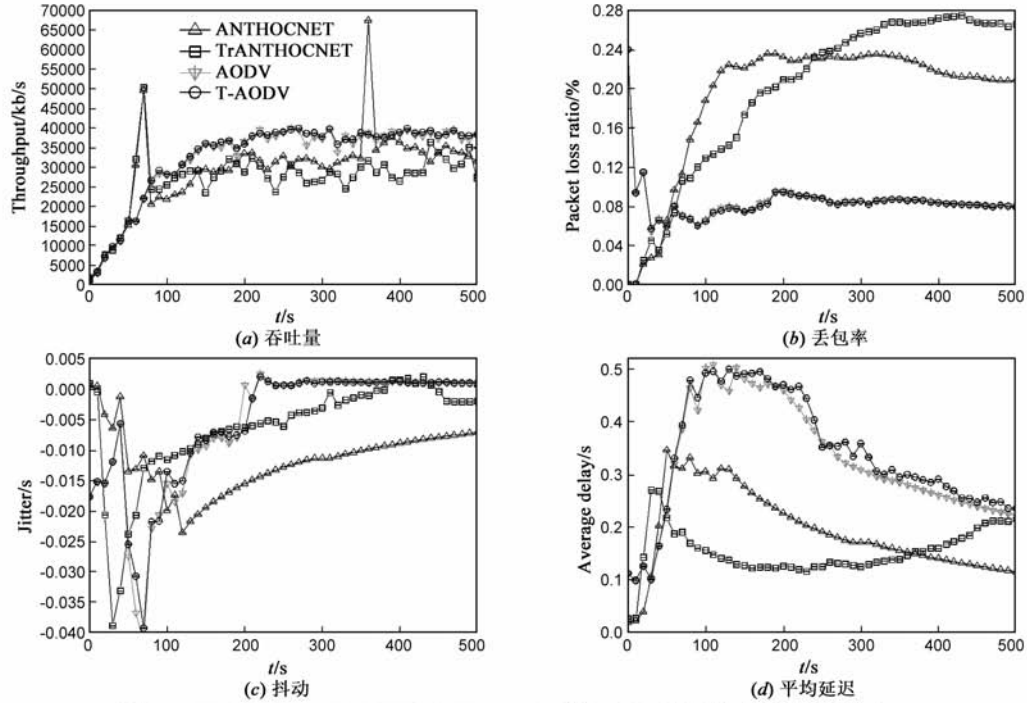

图2　ANTHOCNET、TrANTHOCNT、AODV和T-AODV在网络中没有恶意节点情况下的性能对比,参数R=250m,N=100,*MaxSpeed*=10m/s,*MinSpeed*=0m/s

议中根据节点的行为考虑了节点之间的信任关系,较AODV稳定,可以看出当网络中没有恶意节点时,相差不是很明显.

图3给出了ANTHOCNET和TrANTHOCNET在没有恶意节点情况下的蚂蚁数量统计.从图中可以看出由于TrANTHOCNET算法中选择下一跳节点依赖节点间的信任值,导致某些时候找不到下一跳,再次启动路由发现过程,而路由建立过程采用广播反应式前向蚂蚁的方式,会造成网络中反应式蚂蚁的增多.

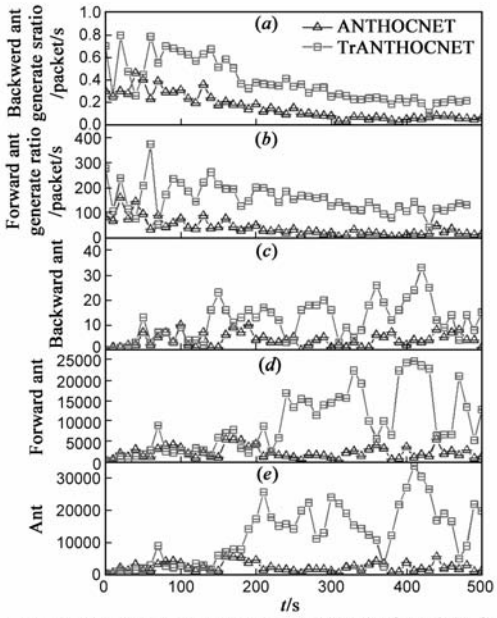

图3 ANTHOCNET和TrANTHOCNET在网络中没有恶意节点时对蚂蚁数量的统计.(a)后向蚂蚁的平均生成率;(b)前向蚂蚁的平均生成率;(c)当前时刻后向蚂蚁的数量;(d)当前时刻前向蚂蚁的数量;(e)当前时刻蚂蚁的总量

下面对网络中存在20%恶意节点时的四种算法进行性能比较.恶意节点表现为直接丢弃收到的数据包但可以正常接收和转发蚂蚁和控制包,结果如图4所示,当网络中存在20%恶意节点时,AODV协议在处理恶意节点时较ANTHOCNET表现出较差的吞吐量和较高的丢包率,这是由于ANTHOCNET中蚂蚁释放的信息素一定程度上起到抵制恶意节点的作用.TrANTHOCNET的各项性能指标均优于ANTHOCNET,且T-AODV协议的各项指标介于两者之间,由于链路存在不稳定性,而T-AODV仅根据节点的过往行为更新节点之间的信任关系,以及路径的信任值,TrANTHOCNET协议中利用模糊Petri网实现节点之间间接信任的评估,增加了建立链路的可信性,T-AODV则缺失这一点,但较优于AODV和ANTHOCNET,说明TrANTHOCNET能有效地遏制恶意节点的存在,选择信任且健壮的路径转发数据包.图4(c)中ANTHOCNET和TrANTHOCNET算法的曲线都出现了不同程度的抖动,并且前者要比后者大,是因为蚁群算法一般可分为两个时期:搜索期和稳定期,搜索期为路由建立过程,会表现出不稳定性,说明TrANTHOCNET中添加的信任机制在抵抗恶意节点具有较好的鲁棒性.如图5所示,由于恶意节点的存在,为了抵抗网络中恶意节点的行为,导致频繁的启动路由建立过程,增

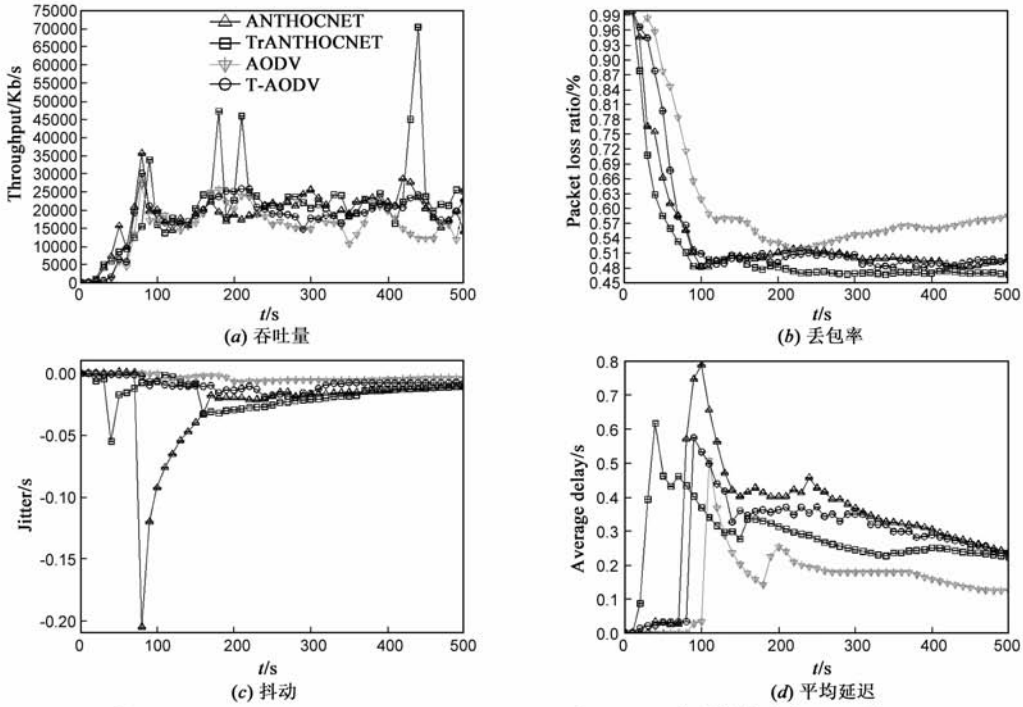

图4 ANTHOCNET、TrANTHOCNET、AODV和T-AODV在网络中含有20%恶意节点时的性能比较,参数为*R*=250m,*N*=100,*MaxSpeed*=10m/s,*MinSpeed*=0m/s

加了网络中的蚂蚁数量,但对比图 3 和图 5 可以发现恶意节点加入并没有导致蚂蚁数量的显著增加,体现本算法具有稳定性.

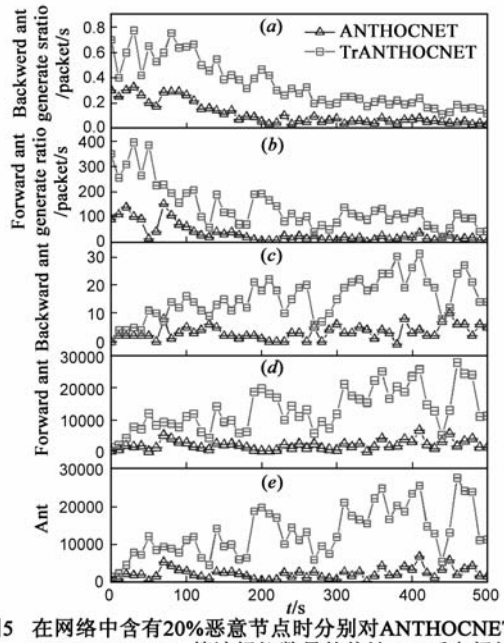

图5　在网络中含有20%恶意节点时分别对ANTHOCNET和TrANTHOCNET算法蚂蚁数量的统计.(*a*) 后向蚂蚁的平均生成率;(*b*) 前向蚂蚁的平均生成率;(*c*) 当前时刻后向蚂蚁的数量;(*d*) 当前时刻前向蚂蚁的数量;(*e*) 当前时刻蚂蚁的总量

图 6 给出了不同恶意节点比例对 TrANTHOCNET 的影响.从图4(a)中可以看出恶意节点比例增大曲线波动较大,说明网络的稳定性变差,按平均值计算,恶意节点越多,吞吐量越小.另外,随着恶意节点的增多,丢包率越大.抖动和平均时延随着恶意节点的增多呈现减小的趋势,因为恶意节点表现为直接丢弃收到的包,在计算抖动和时延时不将其计算在内.图 7 中显示随着恶意节点的增多网络中蚂蚁的数目反而减少,这是因为实验中随机选取源节点和目的节点,网络中恶意节点增多,有些恶意节点被选为源节点,数据包从应用层传递到路由层就被本节点丢弃,网络中的数据包减少,路由建立的过程启动次数减少,生成的蚂蚁数量因此而降低.

5　结束语

近年来,如何提高 Ad hoc 网络路由的安全性成为了研究热点,本文通过对路由层的协议添加信任,利用获取的节点位置信息,预测节点的相对运动路线,以保证路由的安全性.仿真结果表明本文提出的 TrANTHOCNET 算法能够有效地抵制恶意节点的存在,构建具有健壮性和信任性的路由,提高网络性能,验证了使用模糊 Petri 网描述无线网络中的不确定关系的可行性与精确性.但是算法中为了构建健壮且信任的路由,增大了额外的开销——蚂蚁数量增多,需要针对此问题并结合实际的应用场景和环境进一步完善 TrANTHOCNET 算法.

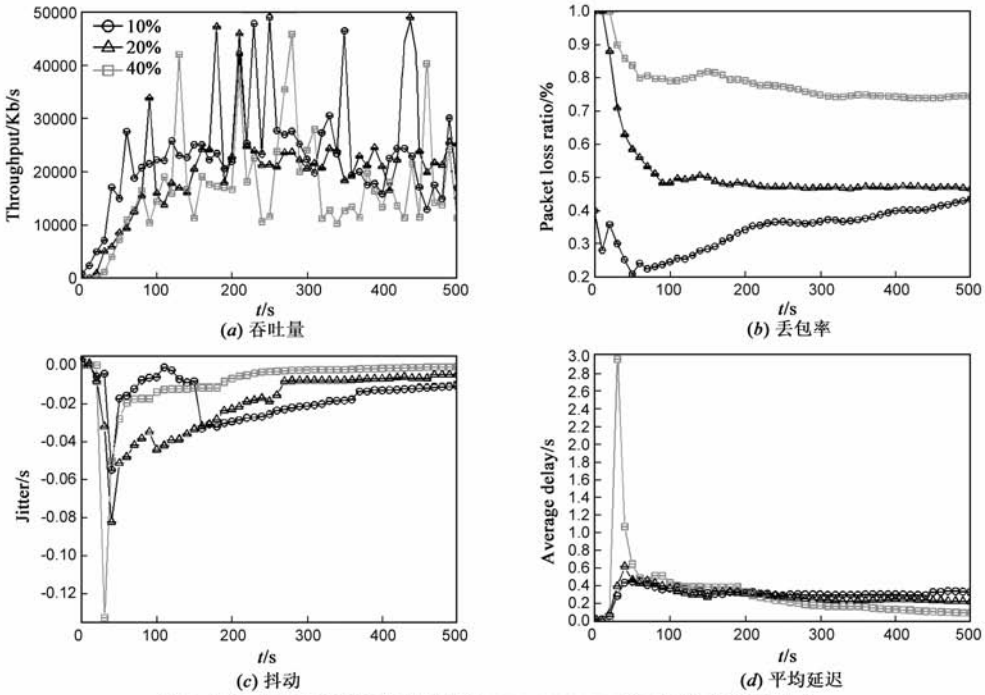

图6　网络中恶意节点的含量分别为10%,20%,40%时对算法性能的影响,参数为*R*=250m,*N*=100,*Maxspeed*=10m/s,*Minspeed*=0m/s

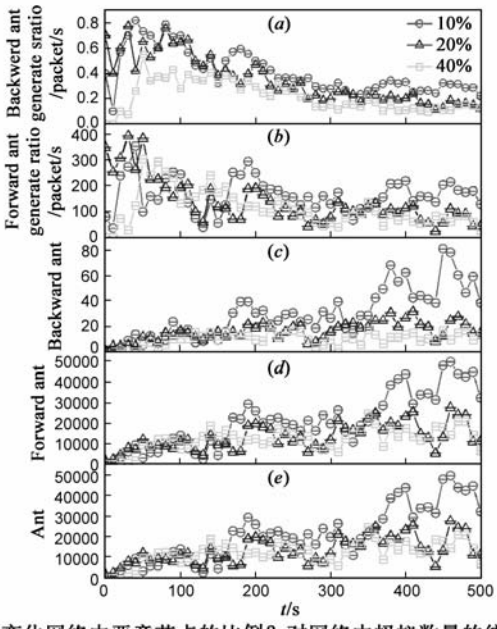

图7 变化网络中恶意节点的比例? 对网络中蚂蚁数量的统计. (a) 后向蚂蚁的平均生成率;(b) 为前向蚂蚁的平均生成率; (c) 为当前时刻后向蚂蚁的数量;(d) 为当前时刻前向蚂蚁的数量;(e) 为当前时刻蚂蚁的总量

参考文献

[1] Gianni Di Caro, Frederick Ducatelle, et al. AntHocNet: an adaptive nature-inspired algorithm for routing in mobile ad hoc networks[J]. European Transactions on Telecommunications, 2005,16(5):443 – 455.

[2] 林闯.随机 Petri 网和系统性能评价[M].北京:清华大学出版社,2005.1 – 18.

[3] CARL G LOONEY. Fuzzy petri nets for rule-based decision-making[J]. IEEE Transactions on Systems, Man, and Cybernetics Society,1988,18(1):178 – 183.

[4] 何新贵.模糊 Petri 网[J].计算机学报,1994,17(12):946 – 950.
He Xin-gui. Fuzzy petri net[J]. Chinese Journal of Computers, 1994,17(12):946 – 950.(in Chinese)

[5] 贾立新,薛钧义,茹峰.采用模糊 Petri 网的形式化推理算法及其应用[J].西安交通大学学报,2003,37(12):1263 – 1266.
Jia Li-xin, Xue Jun-yi, Ru feng. Fuzzy petri net based formalized reasoning algorithm with applications[J]. Journal of Xi'an Jiao Tong University,2003,37(12):1263 – 1266.(in Chinese)

[6] Mejia M, Pena N, et al. A review of trust modeling in ad hoc networks[J]. Internet Research,2009,19(1):88 – 104.

[7] Yan Lindsay Sun, Wei Yu, et al. Information theoretic framework of trust modeling and evaluation for ad hoc networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2):305 – 317.

[8] Haidar Safa, Hassan Artail, et al. A cluster-based trust-aware routing protocol for mobile ad hoc networks[J]. Wireless Networks,2010,16(4):969 – 984.

[9] George Theodorakopoulos, John S Baras. Trust evaluation in ad hoc networks[A]. Proceedings of the 3rdACM Workshop on Wireless Secunity[C]. Philadelphia, PA, United states: Association for Computing Machinery,2004:1 – 10.

[10] Marcin Seredynski, Pascal Bouvry, et al. Modeling the evolution of cooperative behavior in ad hoc networks using a game based model[A]. 2007 IEEE Symposium on Computational Intelligence and Games[C],2007:96 – 103.

[11] 李▮,刘军.基于 AODV 协议的自组网络安全机制的研究[J].电子学报,2006,34(2):272 – 276.
Li Zhe, Liu Jun. The research on security mechanism based on aodv routing protocol in mobile ad hoc network[J]. Acta Electronic Sinica,2006,34(2):272 – 276.(in Chinese)

[12] C Aguilar Melchor, B Ait Salem, et al. AntTrust: A novel ant routing protocol for wireless ad-hoc network based on trust between nodes[A]. Proceedings of the Third International Conference on Availability, Security and Reliability[C]. Barcelona, SPAIN: Secure BusinessAustria,2008.1052 – 1059.

[13] Jian Wang, Yanheng Liu, et al. A trust propagation scheme in VANETs[A]. Proceedings of IEEE Intelligent Vehicles Symposium[C]. China, Xi'an: Intelligent Vehicles Symposium, 2009.1067 – 1071.

[14] 吴春明,陈治,等.蚁群算法中系统初始化及系统参数的研究[J].电子学报,2006,34(8):1530 – 1533.
Wu Chunming, Chen Zhi, et al. The research on initialization of ants system and configuration of parameters for different TSP problems in ant algorithm[J]. Acta Electronic Sinica, 2006,34(8):1530 – 1533.(in Chinese)

[15] A. Menaka Pushpa M. E. Trust based secure routing in aodv routing protocol[A]. 2009 IEEE International Conference on Internet Multimedia Services Architecture and Applications [C]. Bangalore, India: IEEE Computer Society,2009:1 – 6.

作者简介

刘衍珩 男,1958 年出生于吉林松原,博士,吉林大学教授,博士生导师,主要研究方向为移动 IP 和网络 QoS、网络安全与可信.

张 婧 女,1986 年出生于吉林松原,吉林大学硕士研究生,主要研究方向为复杂网络和无线传感器网络.

王 健(通信作者) 男,1981 年出生于黑龙江加格达奇,吉林大学讲师,博士,主要研究方向为级联动力学和复杂网络.
E-mail: wangjian591@gmail.com