

基于仿生学信任信誉模型 BTRM 的无线传感器网络的信任协作研究与实现

孟敬¹, 刘寿强^{2,3}

1. 广东交通职业技术学院, 广州 510800
2. 华南师范大学物理与电信工程学院, 广州 510006
3. 华南理工大学计算机科学与工程学院, 广州 510040

摘要 无线传感器网络通常部署在无人维护、不可控制的环境中,除了具有一般无线网络所面临的信息泄露、信息篡改、重放攻击、拒绝服务等多种威胁外,无线传感器网络还面临传感节点容易被攻击者物理操纵,并获取存储在传感节点中的所有信息,从而控制部分网络的威胁。通过研究蚁群系统中的协作,把基于生物激励信任模型(BTRM)中的信任协作机制应用于无线传感器网络。分析了当前常见的信任协作模型研究现状,归纳出常见的几种信任模型,并提出基于 BTRM 的无线传感器网络的信任协作模拟系统的功能及体系结构。重点论述了基于 BTRM 模型的无线传感器信任协作原理和信任协作模拟系统的设计和实现,通过把 BTRM 中的信任协作机制应用到 WSN 环境中,模拟显示,该机制在输出平均路径长度、平均满意度、平均满意偏差等方面均有较大的改进。

关键词 无线传感器网络;信任协作;蚁群算法

中图分类号 TP311

文献标识码 A

doi 10.3981/j.issn.1000-7857.2011.24.011

Study and Implementation of Wireless Sensor Networks' Trust Collaboration based on Bio-inspired Trust and Reputation Model

MENG Jing¹, LIU Shouqiang^{2,3}

1. Guangdong Communication Polytechnic, Guangzhou 510800, China
2. School of Physics & Telecommunication Engineering, South China Normal University, Guangzhou 510006, China
3. School of Computer Science & Engineering, South China University of Technology, Guangzhou 510040, China

Abstract Wireless sensor networks are usually deployed in the non-controlled environment without maintenance, facing problems of a general disclosure of information, information tampering, replay attacks, denial of service and other threats, and also facing the threat of the mass nodes being easily targeted by physical manipulation, with the information stored in the sensor nodes being taken and used for the manipulators to control a part of the network. Based on the studies of the collaboration of the ant colony system, a trust model based on biologically inspired (BTRM) trust in the cooperation mechanism is proposed for the use in wireless sensor networks. Some trust models of collaboration currently in use are analyzed, and a wireless sensor network based on BTRM collaborative trust simulation software features and software architecture is proposed. The principles and the implementations of the collaborative trust simulation system are discussed. The simulation shows the output average path length, the average satisfaction, the average deviation, which indicates an improved performance.

Keywords wireless sensor networks; trust collaboration; ant colony algorithm

收稿日期: 2011-06-29;修回日期: 2011-07-08

基金项目: 广东省交通科技项目(2007-27);国家自然科学基金项目(61072028)

作者简介: 孟敬,副教授,研究方向为计算机网络通信及其应用,电子信箱:menjin@163.com

0 引言

无线传感器网络(WSN)指在复杂的环境中部署的大规模网络,进行实时数据采集与处理。由于 WSN 通常部署在无人维护、不可控制的环境中,除了一般无线网络所面临的信息泄露、信息篡改、重放攻击、拒绝服务等多种威胁外,WSN 还面临传感节点容易被攻击者物理操纵,并获取存储在传感节点中的所有信息,从而控制部分网络的威胁。用户不可能接受并部署一个没有解决好安全和隐私问题的传感网络,因此,在进行 WSN 协议和软件设计时,必须充分考虑 WSN 可能面临的安全问题,并把安全机制集成到系统设计中。只有这样,才能促进传感网络的广泛应用,否则,传感网络只能部署在有限、受控的环境中。

为抑制网络中的恶意行为,提高节点和服务的可靠性,近年来,国内外在信任机制方面进行了大量的研究工作,提出多种信任模型,常见的信任模型如下。

(1) 基于推荐信任机制,引入正态概率密度函数的概念,对信任度进行描述。提出一种对信任度进行概率分析的评估方法,可动态地适应用户的安全需求,减弱在多路径推荐中由于恶意实体推荐所带来的负面影响,提高信任计算结果的稳定性。分析和模拟试验表明,该模型是必要和有效的,可以更好地解决 P2P 网络带来的安全问题。

(2) 基于可信第三方的信任模型采用 PKI 等技术,在网络中建立集中式认证服务器少数领袖节点(leader peers)来监督整个网络的运行。这类模型依赖于少量中心节点,无法避免可扩展性、单点失效等方面的一系列问题。

(3) 基于共享信息的信任模型。该模型主要根据各个节点共享对其他节点的信誉评定信息,通过广播查询消息来获得这些信息,以此来确定目标节点的信誉度。

(4) 基于反馈信息的信任模型。该模型具有很好的应用灵活性、鲁棒性和较低的成本,且准确度较低和需要收敛时间等问题也可以通过适当的机制和算法加以弥补,适合 P2P 模式分散化、动态可伸缩的特点,是 P2P 应用中信任技术的主要发展方向。

(5) 基于群体信息共享的反馈和评价推荐机制,搜集节点的历史活动信息和反馈作为建立信任的基础,经过一定的存活期后,其获得的信任度逐步收敛到其真实值。

(6) 基于 Bayesian 网络的信任模型。该模型利用 Bayesian 网络,根据用户节点的不同需求和偏好,灵活地给出目标节点的信任值。该模型的不足之处是,在设计的时候没有考虑到恶意的节点,缺少相应的惩罚机制,而且在进行大规模的交易时,计算节点信任值的开销很大。

本文通过对生物界中的蚁群系统进行研究,总结出蚂蚁的信任协作行为,把基于生物激励信任信誉模型(BTRM)中的信任协作应用到无线传感器网络,利用该模型来寻找一条最可信的通向需要的服务路径,并综合计算信任满意度以及平均路径长度^[1-3]。

1 基于蚁群算法信任协作模型

1.1 蚁群算法

蚁群算法(Ant Colony Algorithm,ACA)是一种随机搜索算法,与其他模拟进化算法一样,通过由候选解组成的群体的进化过程来寻求最优解。它是在对自然界中真实蚁群的集体行为研究的基础上,由 Dorigo 等首先提出^[5-8]。仿生学家经过大量的细致观察研究发现,蚂蚁个体之间通过一种称之为外激素(pheromone)的物质进行信息传递,蚂蚁在运动过程中,能够在它所经过的路径上留下该物质,而且蚂蚁在运动过程中能够感知这种物质的存在及其强度,并以此指导自己的运动方向,蚂蚁倾向于朝着该物质强度高的方向移动。因此,由大量蚂蚁组成的蚁群的集体行为便表现出一种信息正反馈现象:某一路径上走过的蚂蚁越多,则后来者选择该路径的概率就越大。蚂蚁个体之间就是通过这种信息的交流达到搜索食物的目的。

蚁群算法模拟真实蚁群的协作过程,算法由许多蚂蚁共同完成,每只蚂蚁在候选解的空间中独立地搜索解,并在所寻得的解上留下一定的信息量。解的性能越好蚂蚁留在其上的信息量越大,信息量越大的解被选择的可能性也越大。算法的最初阶段,所有解上的信息量是相同的,随着算法的推进,较优解上的信息量增加使得算法渐渐收敛。蚁群算法已成功解决了一系列问题,如 TSP 问题、分配问题、Job-shop 问题,所取得的结果无论是在解的质量上还是在收敛速度上,都要优于或至少等效于演化算法(EA)、模拟退火算法(SA)以及其他一些启发式方法。这些初步研究已显示出蚁群算法在求解复杂组合优化问题方面具有并行化、正反馈、鲁棒性强等优越性。

1.2 蚁群基本算法的设计

开始时,所有的 m 个蚂蚁都集中在起点 S 处。蚂蚁 i 从 S 点出发,按照选择策略,从和 S 相关联的边的集合中,选择一条边;然后,再从这条边的另一节点 a 开始,从和 a 相关联的边的集合中,选择另一条边;以此类推,直到搜索到终点 T ,于是,蚂蚁 i 得到一个从 S 到 T 的解。每当蚂蚁选择完一条边后,就马上更新边上的信息量(局部更新)。蚂蚁 i 搜索完后,蚂蚁 j 从 S 出发,按照和 i 相同的方法,搜索出一条从 S 到 T 的路径,得到 1 个解。直到所有的 m 个蚂蚁都进行完搜索,得到 m 个解(包括重复的)。以 m 个解为基础,采用局部搜索算法,进行局部搜索,得到局部最优解。根据局部最优解全局计算信息增量(全局更新),全局更新后,继续迭代直到满足停止条件,停止条件为最大迭代次数。在所求得的所有局部最优解中,值最小的解为所求的全局最优解,即最短路径的距离值。蚁群算法的流程见图 1。

1.3 基于蚁群算法信任协作模型

在无线传感器网络中,网络中的客户端节点需要请求一个服务时,它就发出蚁群,利用 BTRM 模型去寻找可提供需要服务的节点,在寻找过程中,蚂蚁需要根据下一节点的移

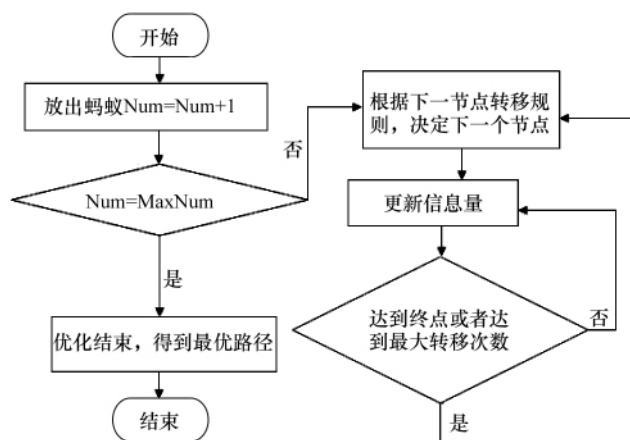


图 1 蚁群算法流程图

Fig. 1 Ant colony algorithm flowchart

动规则,判断下一节点怎么走,当蚂蚁找到自己的服务路径时,更新局部信息量。当所有的蚂蚁都找到服务路径时,更新全局信息量,最后得出可信任的服务路径,并对提供可信服务的节点进行,否则对其进行惩罚。代码描述如下。

```
for i=1 to 循环次数 do
  for k=1 to 蚂蚁数 do
    蚂蚁 k 得到的解←initial node
    for i=2 to 节点数 do
      for k=1 to 蚂蚁数 do
        蚂蚁 k 得到的解←(蚂蚁 k 得到的解)∪(下一节点选择策略)
      更新局部信息量
    for k=1 to 蚂蚁数 do
      if (蚂蚁 k 得到的路径质量>目前最好的路径质量) then
        目前最好的路径质量←Sk
      if (目前最好的路径质量>全局最好的路径质量) then
        全局最好的路径质量←目前最好的路径质量
    for i=1 to 节点数 do
      更新全局信息量
    return 全局最好的路径质量
```

该信任模型需要注意以下 6 个问题:(1) 下一节点的选择;(2) 信息量怎么更新;(3) 怎样衡量路径的质量;(4) 蚂蚁移动和停止返回的条件;(5) 满意度的衡量与判断;(6) 路径的奖励与惩罚。

1.4 信任模型的 6 个问题讨论

下面对模型需要讨论的 6 个问题进行详细说明。为便于说明,信息量更新问题在下面的局部更新和全局更新中分别讨论,满意度的衡量与判断问题并入路径的奖励与惩罚中讨论。其中信任系统中的主要参数以及数学符号说明如下。

α , 信息素启发式因子,用来表示信息素在选择概率上的作用; β , 期望启发式因子,用来表示路径长度在选择概率上

的作用; d_{ij} , 表示节点 i 和 j 之间的距离, i 为出发的节点, j 为到达的节点; $\tau_{ij}(t)$, 表示在 t 时刻节点 i 和 j 之间的路径上残留的信息素; $\eta_{ij}(t)$, 表示节点间的启发函数,通常令 $\eta_{ij}(t)=1/d_{ij}$; ρ , 信息素挥发因子, $\rho \in [0, 1]$; $1-\rho$, 信息素残留因子; φ 即 ϕ , 表示信息素的挥发系数; $S(\text{Start})$, 出发点,是具体的某点; s , 点的集合,是变量; $T(\text{Terminal})$, 终点。

(1) 下一节点选择策略。

当蚂蚁 k 处在节点 r 时,下一个节点 s 的选择规则是

$$pk(r, s) = \begin{cases} \frac{[\tau_r]^\alpha \cdot [\eta_r]^\beta}{\sum_{u \in J_k(r)} [\tau_u]^\alpha \cdot [\eta_u]^\beta} & s \in J_k(r) \\ 0 & \text{其他} \end{cases} \quad (1)$$

其中, $J_k(r)$ 是蚂蚁 k 还没有访问的 r 的邻居集合。

$$s = \begin{cases} \text{argmax}_{u \in J_k(r)} [\tau_u]^\alpha \cdot [\eta_u]^\beta & q \leq q_0 \\ \text{formulae}(1) & \text{其他} \end{cases} \quad (2)$$

当蚂蚁需要选择下一个节点时,它按照上面的规则进行节点选择。

当 $\text{Math.random}() > q_0$ 时,下一节点选择策略描述如下。

获取当前节点 currentNode ;

置当前选择的节点 $\text{Node selectedNode}=\text{null}$;

for currentNode 的所有的邻居 do

if (节点还有未被访问的邻居 and currentNode 的信息素 pheromone 的 α 次方 * heuristic 的 β 次方 > 一个预设的值 $\max$)

$\max = \text{pheromone}$ 的 α 次方 * heuristic 的 β 次方;

$\text{selectedNode} = \text{neighbour}$;

end

返回选择的节点 selectedNode 。

(2) 局部更新信息量。

当蚂蚁在节点 s_1 时,如果它选择了下个节点 s_2 ,那么蚂蚁事实上选择了边 s_1s_2 , 对于 s_1 与 s_2 之间的边的信息量更新规则如下。

$$Ts_{1s_2} = (1-\varphi) \cdot Ts_{1s_2} + \varphi \cdot \Omega,$$

$$\Omega = (1 + (1-\varphi) \cdot (1 - Ts_{1s_2} \cdot \beta_{s_1s_2})) \cdot Ts_{1s_2}$$

每当蚂蚁从一个节点移动到另外的节点时,蚂蚁选择了边 s_1s_2 ,那么就按照上面的公式减少 s_1s_2 边上的信息量,从而增加蚂蚁选择其他边的概率。

局部信息量更新步骤为:

获取当前的节点 s ;

获取 s 的信息素 pheromone ;

获取 s 的启发值 heuristic ;

$$\Omega = (1 + (1-\phi) \cdot (1 - \text{pheromone}) \cdot \text{heuristic}) \cdot \text{pheromone};$$

按照 $(1-\phi) \cdot \text{pheromone} + \phi \cdot \Omega$ 更新边的信息素。

当 m 只蚂蚁从 S 到 T 搜索完后,则求得 m 个解。为了尽可能遍历所有解,需要分别在这些解的邻域中,采用局部搜索算法,求出局部最优解。

(3) 路径质量的衡量。

当蚂蚁 k 返回到它的客户端时,蚂蚁 k 带回它的解 S_k ,客户端必须按照下面的公式衡量这个解的质量:

$$Q(S_k) = \frac{\bar{\tau}_k}{\sqrt{\text{Length}(S_k)}} \cdot \%A_k \quad (3)$$

其中, $\bar{\tau}_k$ 是蚂蚁 k 找到的路径平均信息素; $\%A_k$ 是所有蚂蚁中,得到的解与蚂蚁 k 的解一样的百分比。

在一次迭代中,越多蚂蚁的解与蚂蚁 k 的解一样,则该路径越好,路径上的信息素越高,在相同的条件下,该路径会更优越。所以,在这个模型中,我们选择那些尽可能短的,而且解的百分率最高的为最好的解。

衡量路径的步骤为:

获取蚂蚁 k 的得到的解的路径平均信息素 averagePheromone;

计算所有蚂蚁中,得到的解与蚂蚁 k 一样的百分比 antsPercentage;

计算蚂蚁 k 得到的路径的长度 pathLength;

按照 antsPercentage* averagePheromone/pathLength 计算路径的质量。

(4) 全局更新信息量。

当所有的蚂蚁搜索完毕后,它们都得到局部最优解,接下来对节点之间边的信息量进行全局更新,更新规则如下。

$$Trs = (1-\rho) \cdot Trs + \rho \cdot (1 + Trs \cdot \eta rs Q(S_{\text{Global_Best}})) \cdot Trs$$

全局更新信息量的步骤为:

获取当前服务节点 currentServer;

获取下一个服务节点 nextServer;

获取当前服务节点信息素 pheromone;

获取当前服务节点 heuristic;

当 temp=(1+pheromone*heuristic*maxGlobal)*pheromone;

设置当前服务节点信息素 (1- ρ)*pheromone+ ρ *temp)。

(5) 蚂蚁移动和停止返回的条件。

让蚂蚁 k 在节点 s ,那么 k 需要判断下一步怎么走,是选择下一个节点还是开始回溯。以下是几种情况。

① 节点 s 拥有蚂蚁 k 还没有访问的邻居节点,计算蚂蚁 k 找到的路径平均信息素 $\bar{\tau}_k$,要是 $\bar{\tau}_k$ 大于一个预设的阈值 0.5 时,蚂蚁 k 停止并返回当前的解。

② 节点 s 没有蚂蚁 k 还没有访问的更多的邻居节点,在这种情况下,蚂蚁 k 只好返回。此时,蚂蚁可以按照之前建立的路径回溯,也可以在回溯的过程中,按照上面所说的判断下一节点的规则继续搜索,直到找到需要的节点或者是搜索完整个网络为止。算法描述如下。

for (s 没有邻居节点) or (邻居节点都被访问过了) then

if(s 提供需要的服务) then

停止 并 return 当前节点

else

while(解不为空) do

s 回到上一节点

if(s 有未被访问的邻居) then

按照选择下一节点的规则继续搜索

else if(s 提供需要的服务) then

停止 并 return 当前节点

if(解为空) then

搜索完毕,找不到需要的服务;

else if(r 提供需要的服务) then

if(>阈值 0.5)

停止 并 return 当前节点

(6) 路径的奖励与惩罚。

当 BTRM 选择它认为最可靠的通向可信服务端的路径时,事实上客户端需要服务端的服务,鉴于服务端提供服务的好坏,客户端将对它进行奖励或者惩罚。加入客户端需要的服务与服务端所提供的服务符合时,按照全局信息更新的方法对其进行加分。

假如客户端对服务端所提供的服务不满意,并且不满意度超过预设的值 0.5 时,那么将对其进行惩罚,惩罚的规则是:

$$Trs \leftarrow Trs - \varphi (1 - \text{Sat}) * 2 * df_{rs};$$

$$df_{rs} = \sqrt{\frac{d_{rs}}{L(S_k) \cdot (L(S_k) - d_{rs} + 1)}}, d_{rs} \in \{1, 2, \dots, L(S_k)\} \quad (4)$$

其中, Sat 是客户端对接收到的服务的满意度; d_{rs} 是节点 r 到节点 s 的距离; $L(S_k)$ 是蚂蚁 k 找到的路径长度。

代码描述:

double distanceFactor=Math.sqrt(((double)(i+1))/((L-1)*(L-i-1)));

if (不满意度 >= 惩罚预设值) {

信息素 pheromone -= phi*(1-unsatisfaction)*2*distance-

Factor;

} else {

if (i < L-2) {

pheromone -= phi*distanceFactor;

pheromone *=unsatisfaction*(1-distanceFactor);

}

更新信息素;

而满意度小于预设的值 0.5 的,并且节点在恶意服务路径中,那么对提供服务节点上的每一条边都应做出惩罚。

代码描述:

if (不满意度 < 惩罚预设值)

for (提供恶意服务的所有邻居)

{信息素 pheromone -= phi; pheromone *=不满意度;

更新信息素; }

2 系统设计

2.1 系统功能

该系统实现了建立无线传感器网络,运行模拟器,显示运行变化,显示结果 4 个功能。建立无线传感器网络即为软

件运行建立一个 WSN 环境,该环境是模拟软件运行的基础。运行模拟器即利用 BTRM 模型,模拟节点的信任协作的过程,并得出最终结果。显示运行变化,包括显示节点的移动、显示蚂蚁的邻居范围、节点之间的信息素变化过程。显示结果即显示模拟最终结果,包括输出平均路径长度、平均满意度、平均满意偏差^[3-8]。

2.2 系统结构

系统结构图如图 2 所示。

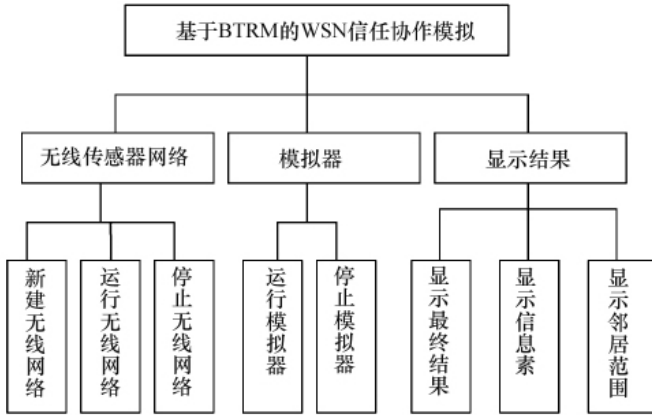


图 2 系统的结构图

Fig. 2 System architecture

2.3 系统功能实现

为软件模拟搭建一个 WSN 环境。图 3 为运行情况,图 4 为显示节点无线范围,图 5 为现实运行最终结果。



图 3 新建无线传感器网络显示节点无线范围

Fig. 3 New wireless sensor network nodes in wireless range of display

有关参数的初始化。对于节点的初始化信息素,取值的大小很重要。例如,当 $\text{initialPheromone} \rightarrow 0$ 时,会造成节点之间互不信任,以至于难以寻找信任的服务节点,当 $\text{initialPheromone} \rightarrow 1$ 时,会造成难以寻找提供欺骗服务的节点,所以,令 $\text{initialPheromone}=0.50$ 。如果参数 α 、 P 设置不当,



图 4 显示节点无线范围

Fig. 4 Display mode wireless range



图 5 运行结果

Fig. 5 Run results

会导致蚁群算法计算量大,蚂蚁寻找信任服务所需的时间较长,初始化 $\alpha=1.0$, $\beta=1.0$, 挥发系数 $\phi=0.01$, 初始化信息素。分别设置 $\text{initialPheromone}=0.1, 0.2, 0.50, 0.60, 0.70, 0.80, 0.90$ 。得出的结果是:BTRM 模型下的信任协作机制可以得到较高的满意度。

3 结论

本文通过分析研究信任模型研究的现状,归纳出几种常见的信任模型,结合生物界的蚁群系统设计基于 BTRM 的无线传感器网络信任协作模拟系统,并用 JAVA 语言开发进行了功能实现。通过研究 BTRM 中的信任协作,研究怎样寻找信任路径的模型,怎样有效防止联合欺诈行为,是具有理论和现实意义的。

该程序在寻找信任路径时耗时较多,算法实用性与性能都需要进一步提高;本文只是考虑了静态 WSN 中的信任协作研究,对于节点之间的行为还没有做全面的考虑,例如,没有考虑节点之间的共谋等因素,下一步可以考虑信任协作模型的动态运行情况,使程序有更强的鲁棒性、适应性^[3-5,9-10]。

参考文献 (References)

- [1] Ganeriwal S, Srivastava M. Reputation-based framework for high integrity sensor networks [C]//Proceedings of the 2nd ACM Workshop on Security of Ad hoc and Sensor Networks, Washington, DC, USA, 2004: 66-77.

- [2] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management[C]//Dale J, Dinolt G. Proceedings of the 17th Symp. on Security and Privacy. Oakland: IEEE Computer Society Press, 1996: 164-173.
- [3] Liang Zhengqiang, Shi Weisong. Analysis of ratings on trust inference in open environments[J]. *Performance Evaluation*, 2008, 65(2): 99-128.
- [4] 姜守旭, 李建中. 一种 P2P 电子商务系统中基于声誉的信任机制[J]. 软件学报, 2007, 18(10): 2551-2563.
Jiang Shouxu, Li Jianzhong. *Journal of Software*, 2007, 18(10): 2551-2563.
- [5] 江自兵, 周鸣争, 梁祥君, 等. 一种基于节点信誉度的无线传感器网络信任模型[J]. 安徽工程大学学报, 2011, 26(1): 58-61.
Jiang Zibing, Zhou Mingzheng, Liang Xiangjun, et al. *Journal of Anhui Polytechnic University*, 2011, 26(1): 58-61.
- [6] 王潮, 贾翔宇, 林强. 基于可信度的无线传感器网络安全路由算法[J]. 通信学报, 2008, 29(11): 105-112.

- Wang Chao, Jia Xiangyu, Lin Qiang. *Journal on Communications*, 2008, 29(11): 105-112.
- [7] OPAALS Consortium, Trust model for the DE, 2008 [EB/OL]. http://files.opaals.org/OPAALS/Year_2_Deliverables/WP04/D4.3.pdf.
- [8] Chen H G, Wu H F, Zhou X, et al. Reputation-based trust in wireless sensor networks [C]//International Conference on Multimedia and Ubiquitous Engineering (MUE'07), 2007.
- [9] Zhang M W, Yang B, Qi Y, et al. Using trust metric to detect malicious acts in WSNs[C]//Eighth ACIS International Conference on software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, IEEE, 2007.
- [10] Hang L, Li L, Tan Q. Act-based trust in wireless sensor network[C]//APWeb Workshops 2006, LNCS 3842, 2006: 214-223.

(责任编辑 林祥磊)

第五届 全国生物进化理论研讨会

时间: 2011.9.25—26
地点: 南京

主办: 中国动物学会生物进化理论委员会

通信地址: 南京市文苑路 1 号, 南京师范大学生命科学学院
邮编: 210046