维普资讯 http://www.cqvip.com

传感器网络中基于帕累托最优效用的包转发研究*)

阎毓杰　王　殊
(华中科技大学电子与信息工程系　武汉 430074)

摘　要　本文运用博弈论的观点和方法来解决传感器网络中的包转发问题。为传感器网络建立了包转发模型，分析了节点参与包转发会话所获得的帕累托最优效用，提出了基于帕累托最优效用的包转发算法 POUPF，并证明了该算法能够建立纳什均衡以保证每个节点都获得帕累托最优效用。仿真结果表明：POUPF 能够有效促进节点自发合作，确保了每个节点获得帕累托最优效用；任何偏离 POUPF 节点的包转发行为都会导致所有节点效用的下降。

关键词　传感器网络，包转发，博弈论，纳什均衡，帕累托最优效用

Pareto Optimal Utility Based Packet Forwarding in Sensor Networks

YAN Yu-Jie　WANG Shu
(Department of Electronics and Information Engineering, Huazhong University of Science and Technology, Wuhan 430074)

Abstract　This paper focuses on the packet forwarding problem in sensor networks and provides a solution with the method of Game theory. It designs a system model for packet forwarding and derives the node's Pareto optimal utility. Further, it proposes a POUPF algorithm which propels the nodes to operate at the Pareto optimal utility and constitutes a Nash Equilibrium. The simulation results verify that POUPF assures the nodes to achieve the Pareto optimal utility by stimulating cooperation; deviation at any one node will decrease utilities of all related nodes.

Keywords　Sensor networks, Packet forwarding, Game theory, Nash equilibrium, Pareto optimal utility

1　引言

无线传感器网络是由部署在监测区域内大量的微型传感器节点通过无线电通信形成的一个自组织网络系统，其目的是协作地感知、采集和处理网络覆盖区域里监测对象的信息，并发送给观察者[1]。由于能量受限，信息通常以多跳的方式在节点间传递。如果节点总是转发数据包，则会因能量耗尽而过早死亡。另一方面，如果节点为保存能量而拒绝所有的转发请求，网络的吞吐量将急剧下降，通信就会瘫痪。于是在网络的转发能耗和吞吐量之间存在一个折中[2,3]。节点如何决定转发数据包以实现最大限度节能并保证一定吞吐量也就成为了传感器网络中所要研究的包转发问题。

近年来，研究者们对传感器网络的包转发问题探讨甚少，但在 Ad hoc 网络中涉及到一些相关研究。Ad hoc 网络中的包转发机制通常分为有激励的合作机制和无激励的合作机制[4,5]。有激励的合作机制采用虚拟货币或是信誉制度的方法来激励节点间的合作。在信誉制度中，节点互相观察彼此的行为，形成有关转发的信誉信息并发布在网络中，根据这些信誉信息，每个节点有选择地为其它节点转发数据，例如：拒绝为信誉差的"不合作"节点转发数据包[6]。虚拟货币制度中采用货币激励节点转发数据包，当某个节点想要发送数据包时，就必须付款；同时，如果它为其它节点转发数据包就会得到报酬[7]。另外，在无任何激励并且各节点都理性的情况下，节点间自发的包转发合作在理论上是存在的，网络拓扑结构与通信模式对自发合作的存在有着显著的影响[8,9]。

假定节点都是"理性"的，即每个节点都希望得到更多的转发帮助，同时使自己的能量付出最小，但这种"自利"行为显然会损害整个网络的性能。因此，有必要在节点之间建立一种合作机制，使得每个节点能够根据自身的能量限制以及从其它节点处得到的转发帮助，适当地为其它节点提供包转发服务。博弈论对于解决个体间合作的问题有着诸多优势[10]。运用博弈论的方法，通过寻求满足纳什均衡的包转发算法来确定节点的转发行为，这将为传感器网络中的包转发问题研究提供一个新颖的思路。本文就是基于上述思想，为传感器网络建立了包转发模型，分析了节点参与包转发会话所获得的帕累托最优效用，提出了基于帕累托最优效用的包转发算法 POUPF，并证明了该算法能够建立纳什均衡以保证每个节点都获得帕累托最优效用。仿真结果表明：POUPF 能够有效促进节点自发合作，确保了每个节点获得帕累托最优效用；任何偏离 POUPF 节点的包转发行为都会导致所有节点效用的下降。

全文的结构安排如下：第 2 部分构建包转发模型；第 3 部分分析包转发的帕累托最优效用；第 4 部分提出满足纳什均衡的 POUPF 算法；第 5 部分是仿真与结果分析；最后是对全文的总结。

2　包转发模型

我们考虑具有 N 个节点的传感器网络系统。所有节点分布在 K 个能量等级上。假定 ni 是能级 $i(i=1,2,\cdots,K)$ 上的节点数目，能级 i 上的每个节点都受到功率 ρ_i 的限制，功率

*)基金项目：本文受国家自然科学基金(No. 60472015)以及国家 985 二期工程"基于网格的高性能计算与复杂系统仿真平台建设"的资助。
阎毓杰　博士研究生，研究领域为无线传感器网络，Ad hoc 网络，信号处理。王　殊　教授，博士生导师，研究领域为嵌入式系统，无线传感器网络，信号处理。

维普资讯 http://www.cqvip.com

限 ρ_i 反映了该能级节点的平均能量与所期望的生存周期的比值，并且有 $\rho_1>\rho_2\cdots>\rho_{k-1}>\rho_k$。为分析方便，我们将网络运行时间离散化，并假定：网络在每个时隙内由一个源节点发起会话，通过中继节点转发将数据包传送到汇聚节点，从而完成一次会话。每次会话要持续一整个时隙并且在该时隙内由源节点和中继节点所构成的数据传输路由不发生改变。如果有一个中继节点拒绝转发，那么会话就会失败。会话的类型由路由中能级最高的节点决定。例如考虑由一个源节点与两个中继节点所构成一次会话，如果源节点所处能级为 1，两个中继节点所处能级分别为 2 和 1，则此会话的类型就是 2。一次会话所需的最大中继节点数目记为 M，一次会话需要 $m(m\leqslant M)$ 个中继节点的概率记为 $q(m)$，并且假定 $q(0)=0$，也即每次会话中至少要有一个中继节点。节点在传输、接收和处理数据包时都要消耗能量，其中传输能耗占主导，为此模型中忽略了数据包接收和处理时的能耗，并且假定每一跳的传输能耗为 1 个单位。

每个节点都要根据以前参与会话的历史信息来决定在当前会话里所应采取的转发行为。我们用 $b_h^j(k)$ 表示节点 h 到 k 时隙为止所发起的类型为 j 的会话数；$a_h^j(k)$ 表示节点 h 到 k 时隙为止所成功发起的类型为 j 的会话数；用 $d_h^j(k)$ 表示到 k 时隙为止节点 h 所收到的类型为 j 的会话请求数；用 $c_h^j(k)$ 表示到 k 时隙为止节点 h 成功中继的类型为 j 的会话数。于是，到 k 时隙为止节点 h 对于类型为 j 的会话的吞吐量可以定义如下：

$$\alpha_h^j(k)=a_h^j(k)/b_h^j(k) \tag{1}$$

同样地，定义到 k 时隙为止节点 h 对于类型为 j 的会话的转发率如下：

$$\beta_h^j(k)=c_h^j(k)/d_h^j(k) \tag{2}$$

进一步地，为度量节点 h 从其它节点那里所得到的转发帮助，将平均消耗每单位能量所获得的吞吐量定义为该节点所得到的效用，其表达式如下：

$$U_h^j(k)=\alpha_h^j(k)/\rho_j \tag{3}$$

同样地，为度量节点 h 为转发其它节点的数据包所付出的代价，将平均消耗每单位能量所提供的转发率定义为该节点所付出的代价，其表达式如下：

$$C_h^j(k)=\beta_h^j(k)/\rho_j \tag{4}$$

3 帕累托最优效用分析

假定节点是理性的，则每个节点都要以最小代价来获得最大效用，于是在参与多次会话后，各节点的效用应该达到帕累托最优，也即任何节点都不能提高自身的效用而不损害其它节点的效用。下面就来推导节点参与各类型会话所获效用的帕累托最优值(Pareto optimal point)[11]。

首先考虑处于能级 1 上的两个节点所构成的一次会话，每个节点都依靠对方为自己转发数据，这样一次博弈矩阵可写为表 1：

表 1 一次会话的博弈矩阵

节点 1 \ 节点 2	不转发	转发
不转发	(0, 0)	$(1/\rho_1,0)$
转发	$(0,1/\rho_1)$	$(1/\rho_1,1/\rho_1)$

将一次会话推广到多次会话，节点间的转发过程构成重复博弈的情形[12]。对于有多个中继节点参与的会话，将处在能级 i 的节点参与类型为 j 的会话时接受转发请求的概率记为转发率 σ_{ij}。由于节点是理性的，那么在参与会话时它没有任何动机表现得与其它节点不一样。例如在类型 3 的会话中，处于能级 2 的节点的转发率与处于能级 3 的节点转发率相等，这是因为虽然能级 2 的节点具有更大的功率限，但即使它加大转发率也不会从能级 3 的节点那里得到更多效用。由此可知，会话中不同能级节点的转发率应该是相同的，即有：

$$\sigma_{ij}=\sigma_{jj},\ 1\leqslant i\leqslant j\leqslant k \tag{5}$$

为此，我们将类型为 j 的会话中所有节点的转发率统一记作 s_j。

对于一个参与类型为 j 的会话的节点 h，它作为源节点时平均每时隙内的能量效率 $\Gamma_{hj}^{(s)}$ 可以表示为：

$$\Gamma_{hj}^{(s)}=\frac{1}{N}\cdot\lim_{k\to\infty}U_h^j(k)=\frac{1}{N}\frac{1}{\rho_j}\sum_{m=1}^{M}q(m)\sum_{p_1,\cdots,p_j}\theta(m;p_1,\cdots,p_j)\sigma_j^{(p_1+\cdots p_j)} \tag{6}$$

其中，$1/N$ 是节点 h 作为源节点的概率；$\theta(m;p_1,\cdots,p_j)$ 是一个抽象的多变量条件概率函数，它表示在 h 参与有 m 个中继节点的 j 类型会话时，能级为 $1,2,\cdots,j$ 的中继节点数目分别是 $p_1,p_2,\cdots,p_j$ 的概率；$\sigma_j^{(p_1+\cdots p_j)}$ 是所有中继节点都接受会话请求的概率。

同样，节点 h 作为中继节点时平均每时隙内的能量效率 $\Gamma_{hj}^{(r)}$ 可以表示如下：

$$\Gamma_{hj}^{(r)}=\frac{1}{N}\cdot\frac{1}{\rho_j}\sum_{m=1}^{M}mq(m)\sum_{p_1,\cdots p_j}\theta(m-1;p_1,\cdots p_j)\sigma_j^{(p_1+\cdots p_j)} \tag{7}$$

由于平均每时隙内节点 h 参与各类型会话的总能耗不超过其功率限，于是有：

$$\sum_{j=class(h)}^{K}\rho_j(\Gamma_{hj}^{(s)}+\Gamma_{hj}^{(r)})\leqslant\rho_{class(h)} \tag{8}$$

其中 class(h)是节点 h 所在的能级。

先分析前面提到的由能级 1 上的两个节点所构成简单系统。按式 (8)得到每个节点的总效用不等式，将这两个不等式合并可以得到：

$$\frac{1}{2}\lim_{k\to\infty}U_1^1(k)+\frac{1}{2}\lim_{k\to\infty}U_2^1(k)\leqslant 1 \tag{9}$$

当式(9)取等号时，节点 1 要增加其效用必然会损害节点 2 的效用，这意味着两个节点在经过多次会话的重复博弈后，各自的效用达到了帕累托最优点。

接下来考虑由分布在 K 个能级上的 N 个节点所组成的网络，其能级 i 上有 p_i 个节点，并且 $q(1)=1,M=1$，那么能级 i 上某一节点作为源节点参与所有类型会话时平均每时隙内的总能耗为：

$$\Gamma_i^{(s)}=\sum_{j=i}^{K}\rho_j(\Gamma_{hj}^{(s)}=\frac{1}{N(N-1)}\cdot[\sum_{k=1}^{i-1}p_k\sigma_i+(p_i-1)\sigma_i+\sum_{l=i+1}^{K}p_l\sigma_l] \tag{10}$$

当中继节点能级比 i 小时，会话类型为 i；如果中继节点能级比 i 大，则会话类型和中继节点能级相同。对于该节点作为中继节点时平均每时隙内的总能耗 $\Gamma_i^{(r)}$ 的表达式与上式相同。于是，该节点对于会话类型 i 的帕累托最优转发率 σ_i^* 可以通过求解下面的等式得出：

$$\Gamma_i^{(s)}+\Gamma_i^{(r)}=\rho_i\ 1\leqslant i\leqslant K \tag{11}$$

$$\sigma_j\in[0,1]\ 1\leqslant i\leqslant K \tag{12}$$

将解出的 σ_i^* 带入下面的(13)式，即可得到该节点对于会话类型 i 的帕累托最优效用。

维普资讯 http://www.cqvip.com

$$U_i^* = \lim_{k\to\infty} U_h^i(k) = \frac{1}{\rho_i}\sum_{m=1}^{M} q(m) \sum_{p_1,\cdots,p_i} \theta(m;p_1,\cdots,p_i)\sigma_i^{*(p_1+b\cdots p_i)} \quad (13)$$

特别地，取 $K=1$，解得 $\sigma_i^* = N\rho_1/2; U_i^* = N/2$。可以看到，帕累托最优效用与帕累托最优转发率一样，都只与会话类型有关。

进一步地，将上述讨论模型扩展到有 m 个中继节点参与会话的情形，通过下面的算法解得节点对于各类型会话的帕累托最优效用。

Choose a node in energy class K

Solve $\frac{1}{N}\cdot\sum_{m=1}^{M} q(m)\sigma_K^{*m} + \frac{1}{N}\cdot\sum_{m=1}^{M} mq(m)\sigma_K^{*m} = \rho_k$

Get σ_K^*

for($k=K-1;k>=1;k-$)

{

solve $\frac{1}{N}\sum_{j=k}^{K}\left(\sum_{m=1}^{M} q(m)\sum_{p_1,\cdots,p_j}\theta(m;p_1,\cdots,p_j)\sigma_j^{*m} + \sum_{m=1}^{M} mq(m)\sum_{p_1,\cdots,p_j}\theta(m-1;p_1,\cdots,p_j)\sigma_j^{*m}\right) = \rho_k$

}

Get $\sigma_{K-1}^*,\cdots,\sigma_1^*$

Get $U_K^*,\cdots,U_1^*$

4 POUPF 算法

在前面分析讨论的基础上，我们设计了基于帕累托最优效用的包转发算法(Pareto Optimal Utility based Packet Forwarding，简称 POUPF)，通过促进节点间的合作使得节点的效用达到帕累托最优。该算法中每个节点都要记录自己过去的效用 $U_h^j(k)$ 和代价 $C_h^j(k)$，$j=1,2,\cdots,K$，并依据这两个变量来决定当前的转发行为。

首先考虑简单的情形：网络中有 N 个节点分布在 K 个能级上，并且 $q(1)=1, M=1$。假定节点 h 此时收到一个类型为 j 的会话转发请求时，POUPF 算法如下：

If $U_h^j(k)\geqslant C_h^j(k)-\varepsilon$ and $C_h^j(k)\leqslant\sigma_j^*/\rho_j$ Accept

Else Reject

其中，ε 是一个小的正数。该算法要求节点在它得到的效用几乎要超过它的转发代价，并且该转发代价还未达到帕累托最优代价时，将接受会话中继请求(转发数据包)。这里规定 ε 是一个正数，表明节点所得到的效用即使不足够补偿它所付出的转发代价，也要表现得稍微慷慨一点，这样才能促进与其它节点的合作，最终都获得帕累托最优效用。

上述单中继节点情况下的 POUPF 算法致力于平衡节点得到的效用和付出的代价。而对于多个中继节点参与会话的情形，由于某一节点作为中继节点的概率要比作为源节点的概率大，它所付出的代价会多于得到的效用。这时的 POUPF 算法应改为这样描述：

If $C_h^j(k)\leqslant\sigma_j^*/\rho_j$ and $U_h^j(k)\geqslant\frac{\rho_j U_j^* C_h^j(k)}{\sigma_j^*}-\varepsilon$ Accept

Else Reject

接下来证明 POUPF 算法能够建立纳什均衡[13,14]。

首先还是考虑只有一个中继节点的情况。假设除节点 p 外的 N-1 个节点都遵循 POUPF 策略，并且 $K=1$。那么对于这 N-1 中的任一个节点 h，只要其 $C_h(k)>\sigma^*/\rho$，就会拒绝转发，于是得到 $\limsup_{k\to\infty} C_h(k)\leqslant\sigma^*/\rho=N/2, h\neq p$。由于转发机制与源节点与否无关，故所有节点得到的效用相同，因而有 $\limsup_{k\to\infty} U_h(k)/\rho\leqslant N/2=U^*, h=1,\cdots,N$。这表明如果节点想偏离 POUPF 算法，那么它将得不到帕累托最优效用。这就证明了 POUPF 能够为包转发建立纳什均衡。

然后证明 $U_h(k)$ 和 $C_h(k)$ 收敛于帕累托最优效用 U^*。

对于普通节点 p，定义：

$$\gamma_h(k) = \frac{\text{No. of successful sessions generated by } h \text{ till k}}{k} \quad (14)$$

$$\eta_h(k) = \frac{\text{No. of sessions relayed by } h \text{ till k}}{k} \quad (15)$$

由于 h 作为源节点时是从 N 个节点中选出，h 作为中继节点时是从 $N-1$ 个节点中选出，于是有：

$$\gamma_h = \lim_{k\to\infty}\gamma_h(k) = \lim_{k\to\infty}\frac{\text{No. of successful sessions generated by } h}{k} \cdot \frac{\text{No. of sessions relayed by } h}{\text{No. of sessions relayed by } \bar{h}} = \frac{\lim_{k\to\infty}\rho U_h(k)}{N(N-1)} \quad (16)$$

同样有：

$$\eta_h = \lim_{k\to\infty}\eta_h(k) = \frac{\lim_{k\to\infty}\rho C_h(k)}{N(N-1)} \quad (17)$$

由于系统中所有节点成功发起的会话请求数要与系统中所有节点中继的会话请求数相等，因此：

$$\sum_{i=1}^{N}(\gamma_i(k)-\eta_i(k)) = 0 \quad (18)$$

利用文[15]的结论，可以得到 $\gamma_h(k)-\eta_h(k)$ 收敛于 0。再结合式(16)，(17)则有：$\lim_{k\to\infty} U_h(k)-C_h(k)=0$。在 $U_h(k)-C_h(k)=0$ 要求下，只要 $C_h(k)\leqslant\sigma^*/\rho$，节点 h 就会转发数据包从而增大 $C_h(k)$，故 $\liminf_{k\to\infty} C_h(k)\geqslant\sigma^*/\rho$，结合前面证明的 $\limsup_{k\to\infty} C_h(k)\leqslant\sigma^*/\rho$，于是有 $\lim_{k\to\infty} C_h(k)=\sigma^*/\rho$。又由于 $U_h(k)-C_h(k)$ 收敛于 0，故 $\lim_{k\to\infty} U_h(k)=\sigma^*/\rho$。于是在 $K=1$ 时，$\lim_{k\to\infty} U_h(k)=N/2=U^*$。这就证明了在 $K=1$，并且只有一个中继节点的情形下，遵循 POUPF 的节点所获得的效用和它所付出的代价都收敛于其帕累托最优效用，从而保证了每个节点都获得帕累托最优效用。

在上述分析中，节点的行为只与它所参与的会话类型有关而与它自身的能级无关，所以上述证明能够很容易地推广到 $K\neq1$ 时的情况。进一步地，通过适当缩放式(18)，并给变量加上适当权重 $q(l), l=1,\cdots,m$，也能够将上述证明推广到有多个中继节点的情形。

POUPF 算法具有很好的可扩展性，这是因为节点只需依据自身变量信息来决定转发行为，节点之间无需交换信息，这使得每个节点记录的变量信息与网络的规模(节点数 N)无关。对于能级 i 上的某一节点 h，它要存储 $4(K-i+1)$ 个变量：$a_h^j(k), b_h^j(k) c_h^j(k), d_h^j(k), j=i,\cdots,K$。只需将这些变量转换为相应的效用 $U_h^j(k)$ 和代价 $C_h^j(k)$ 即可决定是否转发数据包。

5 仿真与性能评估(The simulation and performance evaluation)

我们运用 POUPF 策略仿真传感器网络中的包转发过程，通过考察不同条件下节点效用随时间的变化情况来分析 POUPF 算法的性能。

首先考察单一中继节点的情形。仿真中将 30 个节点分布在 5 个能级上，每个能级都有 6 个节点。并给定功率限 $\rho_1=0.026, \rho_2=0.022, \rho_3=0.018, \rho_4=0.014, \rho_5=0.01$。各类型会话的帕累托最优效用的理论值可以依据本文第三部分的算法求出，它们分别是：$U_5^*=15, U_4^*=16, U_3^*=18, U_2^*=22, U_1^*=32$。

为评估 POUPF 的收敛性，仿真中考察了不同类型会话

维普资讯 http://www.cqvip.com

中节点的平均效用在时序上的变化，如图 1。

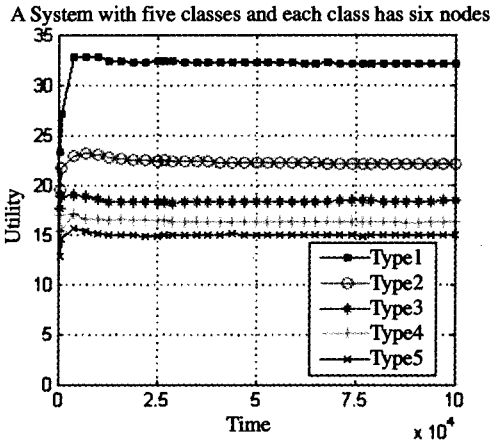

图 1　所有节点遵循 POUPF 时平均效用随时序的变化情况

可以看到：随着时间的推移，节点在各类型会话下的效用逐步收敛于其帕累托最优效用的理论值。这证实了 POUPF 算法能够通过促进节点自发合作，最终保证每个节点获得帕累托最优效用。

为评估 POUPF 策略要求节点慷慨一些（$\varepsilon>0$）的重要性，仿真中将 ε 设为 -0.1，观察到不同类型会话中节点的平均效用在时序上的变化情况如图 2 所示。

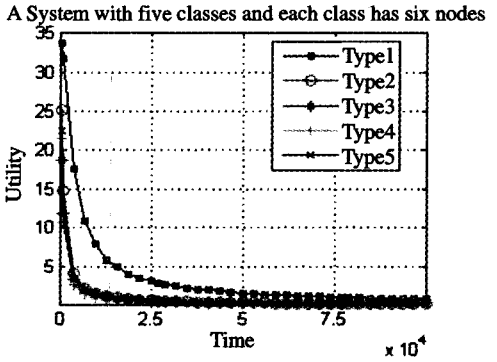

图 2　节点吝啬情况下平均效用随时序的变化情况

可以看到，在节点都吝啬一点（$\varepsilon<0$）情况下，各类型会话的效用都迅速下降并最终趋于 0。这是因为节点的吝啬使得在它所得到的效用大于所付出的代价时才愿意转发数据包，这不利于节点间的合作。只有表现得稍微慷慨一点（即使所得到的效用不足够补偿付出的代价也愿意转发数据包），才能促进与其它节点的合作，最终获得帕累托最优效用。由此看到 POUPF 中对每个节点稍许慷慨的要求至关重要。

为评估 POUPF 策略的纳什均衡性。我们在能级 2 的节点中选取 3 个节点作为“寄生节点”（从不转发数据包），考察不同类型会话中节点的平均效用在时序上的变化情况，如图 3 所示。

可以看到，能级 2 上节点的寄生行为会降低除类型 1 以外所有其它类型会话的效用，且其影响程度随着所参与会话类型的升高而减弱。这是由于源节点所参与的会话类型越高，候选中继节点就越多，从而降低将寄生节点选为中继节点的可能性。于是可以得到结论：任何偏离 POUPF 的节点行为（如寄生行为），都会损害该节点自身以及其它节点的效用，也即任何一个节点都没有偏离 POUPF 的动机，这也就证实了 POUPF 算法能够建立纳什均衡。

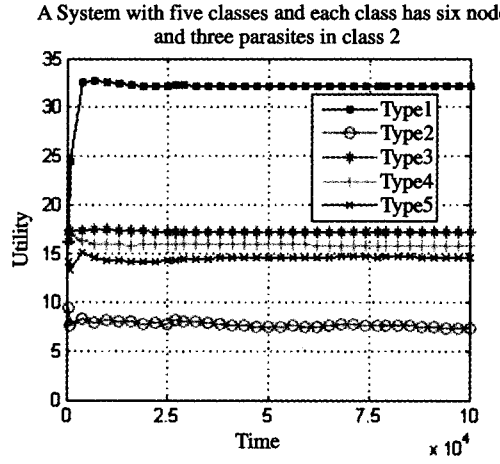

图 3　当有节点偏离 POUPF 时平均效用随时序的变化情况

进一步考察多中继节点的情形。仿真中将 12 个节点分布在两个能级上，每个能级都有 6 个节点，并且 $M=2$，$q(1)=q(2)=0.5$。给定功率限 $\rho_1=0.026$，$\rho_2=0.018$。各类型会话的帕累托最优效用理论值求得为：$U_1^*=19.2$，$U_2^*=9.6$。考察这两种类型的会话中节点平均效用在时序上的变化情况，如图 4 所示：

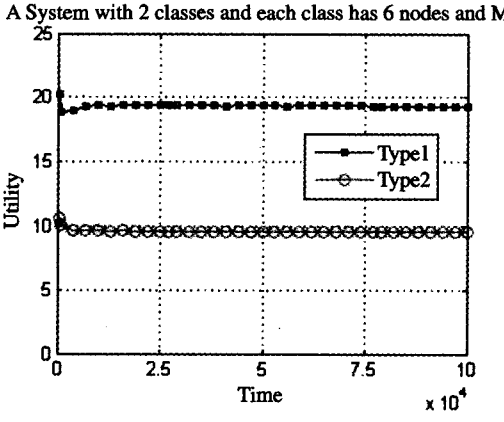

图 4　多中继节点情况下平均效用随时序的变化情况

可以看到，对于两个中继节点的情形，POUPF 也能够通过促进节点间的合作，从而保证各类型会话下的效用达到帕累托最优。对于多中继节点情况下 POUPF 算法要求慷慨的重要性以及纳什均衡性的仿真和结果分析也与前面单个中继节点的情形类似。

结束语　本文运用博弈论的观点和方法来解决传感器网络中的包转发问题。为传感器网络建立了包转发模型，分析了节点参与包转发会话所获得的帕累托最优效用，提出了基于帕累托最优效用的包转发算法 POUPF，并证明了该算法能够建立纳什均衡以保证每个节点都获得帕累托最优效用。仿真结果表明：POUPF 能够有效促进节点自发合作，确保了每个节点获得帕累托最优效用；任何偏离 POUPF 节点的包转发行为都会导致所有节点效用的下降。

参 考 文 献

1　Akyildiz F, Su W, Sankarasubramaniam Y, Cayirci E. Wireless Sensor Networks: A survey. Comput. Networks, 2002, 38(4): 39～422

2　Kannan R, Sitharama Iyengar S. Game-Theoretic Models for Reliable Path-Length and Energy-Constrained Routing With Data Aggregation in Wireless Sensor Networks," IEEE J. Select. Areas Commun., 2004, 22(6)

（下转第 80 页）

维普资讯 http://www.cqvip.com

$$D_i(m_0,m_1,\cdots,m_i)=\sum_{(s_0,s_1,\cdots,s_i)\in\Gamma_i}\frac{e!}{s_0!\ s_1!\ \cdots s_i!}m_0^{s_0}m_1^{s_1}\cdots m_i^{s_i} \quad (2)$$

这里，将较小 i 时的 D_i 写出如下：

$D_0=(m_0)=m_0^e$

$D_1(m_0,m_1)=em_0^{e-1}m_1$

$D_2(m_0,m_1,m_2)=C_e^2m_0^{e-2}m_1^2+em_0^{e-1}m_2$

$D_3(m_0,m_1,m_2,m_3)=C_e^3m_0^{e-3}m_1^3+2C_e^2m^{e-2}m_1m_2+em_0^{e-1}m_3$

$D_4(m_0,m_1,m_2,m_3,m_4)=C_e^4m_0^{e-4}m_1^4+3C_e^3m_0^{e-3}m_1^2m_2+C_e^2m_0^{e-2}m_2^2+em_0^{e-1}m_4$

$D_5(m_0,m_1,\cdots,m_5)=C_e^5m_0^{e-5}m_1^5+4C_e^4m_0^{e-4}m_1^3m_2+3C_e^3m_0^{e-3}m_1m_2^2+2C_e^2m_0^{e-2}m_2m_3+2C_e^2m_0^{e-2}m_1m_4+em_0^{e-1}m_5$

……

……

$D_{t-1}(m_0,m_1,\cdots,m_{t-1})=\{m_0,m_1,\cdots\cdots,m_{t-1}$的多项式$\}$

注意到，含 m_i 的项在 $D_j(j<i)$ 中不出现且 D_i 中含 m_i 的项仅为 $em_0^{e-1}m_i$，$i=0,1,\cdots,t-1$。

定义 $D'_i(m_0,m_1,\cdots,m_{i-1})=D_i(m_0,m_1,\cdots,m_i)-em_0^{e-1}m_i$，从而 D_0,D_1,D_{i-1},D'_i 都是 $m_0,m_1,\cdots,m_{i-1}$ 的多项式$(0\leqslant i\leqslant t-1)$。

$m_1,m_2,\cdots,m_{t-1}$ 可按下述方法递推计算：

取 $i=1$，$D'_1(m_0)=0$，$D_0(m_0)=m_0^e$，解线性方程

$em_0^{e-1}x\equiv B_1\pmod n$，$B_1=E_1/n$，$E_1\equiv C'-D_0(m_0)\pmod{n^2}$

解便是 m_1。因为已知条件中要求 $\gcd(e,n)=1$，$m_0\in Z_n^*$，所以上述方程有唯一解。

假设解密得到了 $m_1,m_2,\cdots,m_{i-1}$，用同样方法，通过解下述线性方程可得 m_i：

$$em_0^{e-1}x\equiv B_i\pmod n,$$

$$B_i=E_i/n^i\quad E_i\equiv C'-\sum_{j=0}^{i-1}n^jD_j(m_0,m_1,\cdots,m_j)-n^iD'_i(m_0,m_1,\cdots,m_{i-1})\pmod{n^{i+1}}$$

递推地，可解密得所有明文 $m_1,m_2,\cdots,m_{t-1}$

解密过程可用下述程序表示：$[x]_N$ 表示 x 模 N

```
Procedure DECRYPTION
INPUT: d, n, C'(:=[(m0+nm1+…+n^(t-1)m(t-1))^e]n')
OUTPUT: m0, m1, …, m(t-1)
(1)C0 := [C']n
   m0 := [C0^d]n
(2)D0 := [m0^e]n^2
   E1 := [C'-D0]n^2
   B1 := E1/n in Z
   A := [(eC0)^-1 m0]n
   m1 := [A B1]n
(3)FOR i=2to (t-1)do
     begin
     SUM := 0
     FOR j=0 to (i-1) do
     begin
     Dj := [Dj(m0,m1,…,mj)]n^(i+1)
     SUM := [SUM+n^d Dj]n^(i+1)
     end
   D'i := [D'i(m0,m1,…,m(i-1))]n^(i+1)
   Ei := [C-SUM-n^i D'i]n^(i+1)
   Bi := Ei/n^i in Z
  mi := [A Bi]n
  end
```

3 讨论

(1)安全性。由于 Takagi[2] 证明了 n-adic 型 RSA 体制与原 RSA 体制的安全性相同，从而我们的体制与 Harn 体制的安全性相同。

(2)性能比较。两个体制的密钥分配阶段是一样的；在加密阶段，Harn 体制需 $2t$ 个模指数运算与 $2t$ 个乘法，而我们的体制仅需一个模 n^t 的指数运算和一个乘法，当然为了使 mod n^t 的指数运算尽可能地快，可选取较小的公钥 e；在解密阶段 Harn 体制需 $3t+2$ 个模指数运算与 t 个乘法，而我们的体制需 2 个模指数运算与解一个模 n 的线性方程组，由于解线性方程组速度较快，因此我们的体制在运行效率上的优势十分明显。

结论 我们用 Takagi[2] 的 n-adic 展开方法给出了 Harn[1] 体制的一个改进体制，所给出的体制与原体制的安全性相同，但运行效率比原体制要高得多。

参考文献

1 Harn L. Public-key Cryptosystem Design Based on Factoring and Discrete Logrithms. IEE Proc. Comput. Digit. Tech., 1994, 14 (3): 193～195

2 Takagi T. Fast RSA-Type Cryptosystems Using N-Adic Expansion, Advances in Cryptology—CRYPT'97. In: B. S. Kaliski Jr, ed. Springer-Verlag Berlin Heidelberg, LNCS 1294, 1997. 372～384

3 McCurley K S. A Key Distribution System Equivalent to Factoring. J. Cryptology, 1988, 1(2): 95～106

4 Lim S, Kim S, Yie I, Lee H. A Generalized Takagi-Cryptosystem with a Modulus of the Form p^rq^s. In: B. Roy, E. Okamoto, eds. INDOCRYPT 2000, LNCS, 1977. 283～294, Springer-Verlag, Berlin, Heidelberg, 2000

5 Hinek M J, Low M K, Teske E. On Some Attacks on Multi-prime RSA. In: K. Nyberg, H. Heys, eds. SAC2002, LNCS 2595, Springer-Verlag, Berlin, Heidelberg, 2003. 385～404

(上接第 35 页)

3 Felegyhazi M, Buttyan L, Hubaux J-P. Cooperative Packet Forwarding in Multi-Domain Sensor Networks. In: Proc. of IEEE PerSeNS 2005, Hawaii, Mar. 2005

4 Marbach P, Qiu Y. Cooperation in Wireless Ad Hoc Networks: A Market-Based Approach. IEEE/ACM Transactions on Networking, 2005, 13 (6): 1325～1338

5 Buttýan L, Hubaux J. -P. Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks. ACM/Kluwer Mobile Networks and Applications (MONET)Special Issue on Mobile Ad Hoc Networks, 2003, 8 (5): 579～592

6 Zhong S, Chen J, Yang Y R. Sprite: A Simple, Cheat-proof, Credit-based System for Mobile Ad hoc Networks. In Proceeding of IEEE IOFOCOM'03, 2003(3): 1987～1997

7 Ileri O, Mau S-C, Mandayam N B. Pricing for Enabling Forwarding in Self-Configuring Ad Hoc Networks. IEEE J. Select. Areas commun, 2005, 23(1)

8 Altman E, Kherani A A, Michiardi P, Molva R. Non-cooperative Forwarding in Ad-hoc Networks. Technical Report INRIA Report No. RR-5116, 2004

9 Felegyhazi M, Hubaux J P, Buttyan L. Nash Equilibria of Packet Forwarding Strategies in Wireless Ad Hoc Networks. IEEE Transactions on Mobile Computing, 2005, 5: 463～476

10 Osborne M J, Rubinstein A. A course in Game Theory, MIT press, 1994

11 MacKenzie A B, Wicker S B. Game Theory and the Design of Self-configuring, Adaptive Wireless Networks. IEEE Communications Magazine, 2001, 39 (11): 126～131

12 Axelrod R. The Evolution of Cooperation, Basic Books, New York, 1984

13 Nash J. Equilibrium Points in N-person Games. Proceedings of the National Academy of Sciences, 1950, 36: 48～49

14 Fudenburg D, Tirole J. Game Theory, Cambridge, MA: MIT Press, 1991

15 Bertsekas D P, Tsitsiklis J N. Neuro-Dynamic Programming, Athena Scientific, Belmant, 1996.