

基于博弈的 DTMSN 路由选择和信任决策

崔平付 任 智 曹建玲

(重庆邮电大学移动通信技术重庆市重点实验室 重庆 400065)

摘 要 针对延时容忍移动传感器网络中节点自私性检测存在未考虑节点由于自身问题不能转发数据而引起信誉值计算不精确和重传数据造成能量浪费的问题,通过引入剩余能量和能否进行数据转发的两个概念,结合相应的惩罚机制,进一步提高了延时容忍移动传感器网络中节点自私性检查的准确度,同时可以延长网络的生存时间。对于现有延时容忍移动传感器网络中缺乏相应的激励机制,引入博弈的思想,通过理论证明,在条件允许的情况下节点会选择合作的行为,从而增加节点主动转发数据的积极性,提高网络的投递成功率,减少网络开销。

关键词 延时容忍移动传感器网络,自私性检测,信誉值,惩罚机制,博弈

中图法分类号 TP393 文献标识码 A

Game-based Routing Selection and Trust Decisions for DTMSN

CUI Ping-fu REN Zhi CAO Jian-ling

(Chongqing Key Lab of Mobile Communications Technology, Chongqing University of Post and Communications, Chongqing 400065, China)

Abstract To deal with the inaccurate calculation problem and energy waste caused by the node can not forward the data for the reason of itself, which has not been thought by the previous detection of selfishness for delay tolerant mobile sensor networks, this paper introduced the concepts of the remaining energy and the flag that can or not forward the packages to improve the previous. Also the mechanism of punishment is used to avoid the sham information of energy and flag. Both of all make the value of credit better. The thought of game is also used in this paper to stimulate the cooperation in the good condition, the theoretical also say the same. For the reason of game, the node can cooperate with each other more, increasing the initiative of forwarding data, which can improve the success rate and reduce the overhead of network.

Keywords Delay tolerant mobile sensor networks, Detection of selfishness, Value of credit, Mechanism of punishment, Game

1 引言

延迟容忍网络(Delay Tolerant Network, DTN)^[1]是一种网络拓扑变化频繁、各节点之间间歇连通的网络。近几年来延时容忍技术被引入无线传感器网络,并且根据节点是否具有移动的功能,可以把延迟容忍传感器网络分为延时静止传感器网络和延时容忍移动传感器网络。DTMSN(Delay Tolerant Mobile Sensor Networks)^[2]的关键技术是设计适合移动传感器网络的路由算法,不少相应的算法已被研究者提出。这些算法可以根据是否有转发的情况分为直接传输和中继传输。DT(Direct Transmission)^[3]是直接传输的典型代表,基本思想是源节点携带数据到达目的节点的通信范围内后,才进行数据的发送。Flooding^[3]是一种常用的贪婪算法,该算法的每一个携带数据的节点将数据包发送给所有邻居节点。RED^[4]是根据对方节点消息转发的成功与否,来选择下

一跳中继节点。SPAD^[5]根据节点的运动轨迹以及与目标节点(sink 节点)的最小欧氏距离综合得出一个转发概率,选择概率大的节点来进行数据的转发。NPD^[6]是一种在 SPAD 的基础上提出的一种基于节点优先级的数据转发策略。文献[7]将信誉问题引入网络中,通过信誉检测选取信誉高的节点进行数据的传输。文献[8]针对移动传感器网络的信任问题,采用博弈论的思想提出了一种信任决策模型并对其进行动态分析。文献[9]在文献[8]的基础上引入反思机制完善了该模型。文献[10]在文献[9]的基础上提出了数据的重传并完善了节点策略的调整机制。

2 节点信任博弈

2.1 策略判定

每个节点对于收到的数据有两种不同的处理策略:信任和不信任。若信任,则转发对方节点数据包;若不信任,则丢

本文受教育部长江学者和创新团队发展计划(IRT1299),国家自然科学基金(60972068),重庆市自然科学基金(cstc2012jjA40051)资助。

崔平付(1989—)男,硕士生,主要研究方向为基于博弈的移动传感器网络路由算法, E-mail: 455414313@qq.com(通信作者);任 智(1971—),男,博士,教授,主要研究方向为宽带无线移动通信网络及网络优化;曹建玲(1974—),女,硕士,副教授,主要研究方向为无线传感器网络路由算法。

弃对方的数据包。与策略判定相关的符号描述如表 1 所列。

表 1 博弈中的主要符号

G_t	采用信任策略,并成功转发数据信任度的收益
G_c	采用信任策略,并成功转发数据的收益
C	发送数据包的代价
L	对方不信任,自己发送数据的代价
a	调价因子
T	节点信任值

2.2 数据交互过程

本文数据交互过程如图 1 所示。

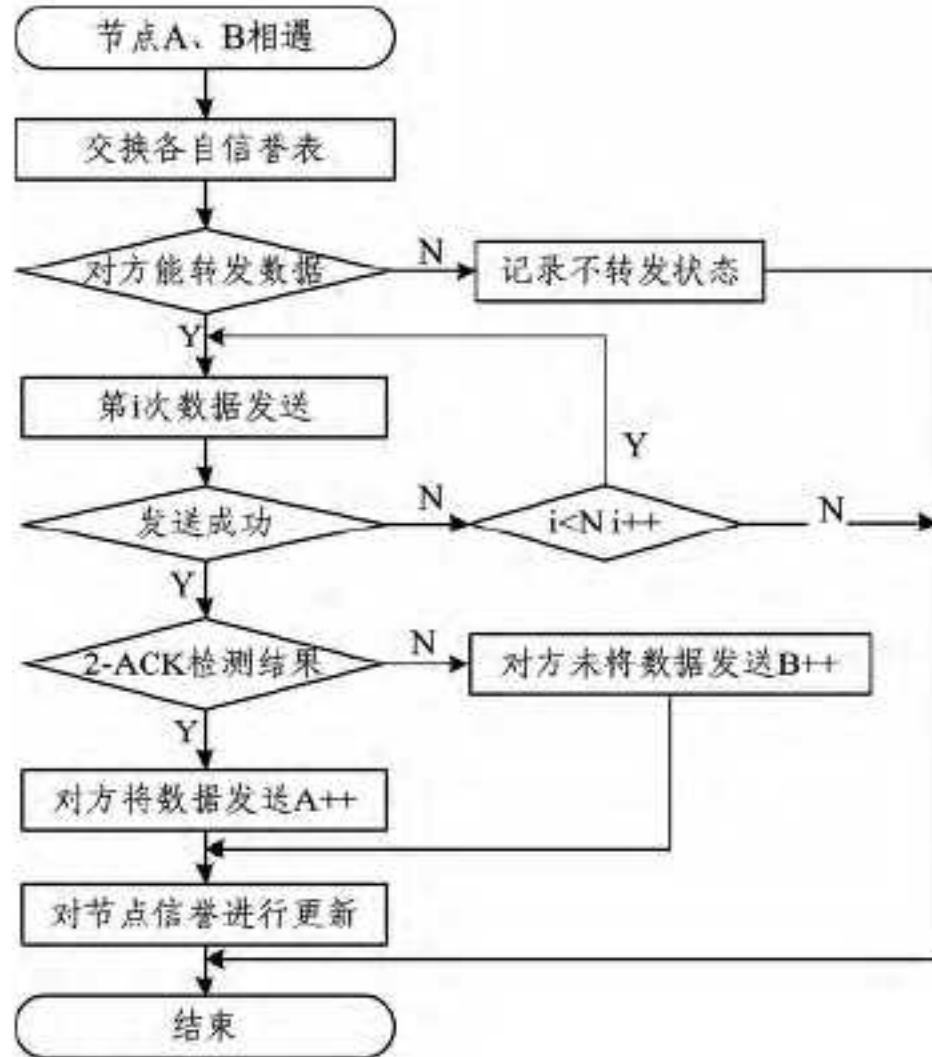


图 1 数据的交互过程

图 1 中 N 表示最大重传次数,在节点相遇时交换信誉表,根据预先设定的阈值和信誉表中 $Flag$ 标志位来综合选取下一跳节点。对于 $Flag$ 为 0 的节点,若根据能量和对方信誉值得出与 $Flag$ 相同的判断,即使对方选择不转发数据,也依旧不认为对方是自私的。如果判断相反,则记录这次不转发行为,不进行节点信誉值的更新。在以后的时间,若发现该节点有转发或者发送目的节点不是 sink 节点的行为,则认为上次不转发行为是自私行为,进行信誉值改变,并通过信誉表的交换来传播该节点的欺骗行为,减少其它节点对于自私节点的转发来达到惩罚的目的。节点在转发其它节点的数据时,首先选择信誉高的节点进行数据的转发,激励节点合作的积极性,提高网络转发的积极性。

两节点相遇时,首先交换各自节点信誉记录矩阵,格式如表 2 所列。

表 2 节点信誉记录矩阵

	i	j	k	
i	E_c	D_{ij}	D_{ik}	
j	D_{ji}	$Flag$	D_{jk}	
k	D_{ki}	D_{kj}	1	
.....				1

表 2 中, E_c 表示节点剩余能量, $Flag$ 为节点能否转发数据的标志位。节点能量受限制时,会拒绝转发其它节点的数据包,以保证需要向目的节点发送数据时自己有足够的能量来发送必要的数据。 D_{ij} 表示节点 i 对节点 j 合作行为的统计,表示 j 为 i 转发的消息数和 i 向 j 发送的消息数的比值,由式(1)表示:

$$D_{ij} = \frac{\alpha_{ij}}{\alpha_{ij} + \beta_{ij}} \quad (1)$$

其中, α 为合作行为计数器, β 为不合作行为计数器。式(1)也被称为直接信誉值,同时存在其它节点的间接信誉值,例如 k 对于 j 信誉值的统计,称为 I_{ij-k} 在数值上 $I_{ij-k} = D_{jk}$; 节点的综合信誉值计算由节点的直接信誉值和间接信誉值综合所得,如式(2)所示:

$$T_{ij} = \frac{1}{\sum_{k \in N} D_{ik}} \sum_{k \in N} (D_{ik} * D_{kj}) \quad (2)$$

其中, N 表示为节点 i 提供节点 j 的信誉值的节点集合,包括除去 j 之外的网络节点。

2-ACK 的行为检测如图 2 所示。

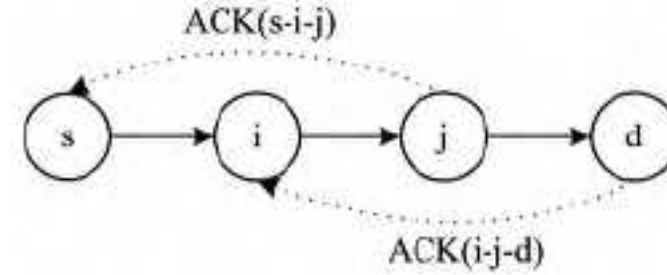


图 2 2-ACK 节点行为检测

下一条节点接收到数据之后再主动向其上两条跳节点发送 ACK 确认机制,以表示上一跳节点有成功转发数据。该 ACK 消息在网络中以泛洪的消息进行传播,通过监听下两条节点的 ACK 消息,来判断下一跳节点是否正确转发消息。

2.3 能耗分析

进行如下的假设:

P 表示节点在任意一次发送数据成功的概率, NC 表示一次交互中,数据发送失败的代价,用 C_F 表示, $N = \{1, 2, 3, 4, \dots\}$ 。

发送成功的用 C_S 表示。 C_S 的计算如式(3)所示:

$$C_S = E(x) = \sum_{k=1}^N k C P\{x=k | x \leq N\} = \frac{qC}{1-(1-q)^N} \sum_{k=1}^N k (1-q)^{k-1} \quad (3)$$

其中, K 表示第 K 次时数据发送成功,由式(4)表示:

$$P\{x=k | x \leq N\} = \frac{P\{x=k, x \leq N\}}{P\{x \leq N\}} = \frac{(1-q)^{k-1} q}{1-(1-q)^N} \quad (4)$$

令 $\omega = 1 - (1-q)^N$, 可将式(3)简化为:

$$C_S = E(x) = \frac{\omega - Nq + Nq\omega C}{q\omega} \quad (5)$$

C_F 与 C_S 满足: $C_F \geq C_S$ 。

2.4 信任博弈

2.4.1 A、B 中有一个节点选择信任策略

假设 A 选择信任策略,收益如表 3 所列。

表 3 A 选择信任策略, B 选择不信任策略

Num	A-S	A-F	B-S	A 收益	B 收益	概率
1	1	1	1	$G_T - L + \alpha T - 2C_S$	$G_C - C_S$	ω^3
2	1	0	1	$\alpha T - C_S - C_F - L$	$-L - C_S$	$\omega^2(1-\omega)$
3	1	0	0	$\alpha T - C_S - L$	$-L - C_F$	$\omega(1-\omega)$
4	0	1	1	$G_T + \alpha T - C_S - C_F - L$	$G_C - C_S$	$\omega^2(1-\omega)$
5	0	0	1	$\alpha T - 2C_F - L$	$-C_S - L$	$\omega(1-\omega)^2$
6	0	0	0	$\alpha T - L - C_F$	$-L - C_F$	$(1-\omega)^2$

2.4.2 A、B 都选择信任策略

当 $A、B$ 都选择信任策略时, $A、B$ 每个节点都有两种行为产生,如表 4 所列。

表4 A、B都选择信任策略

Num	A-S	A-F	B-S	B-F	A收益	B收益	概率
1	1	1	1	1	$G_T + G_C + \alpha T - 2C_S$	$G_T + G_C + \alpha T - 2C_S$	ω^4
2	1	1	1	0	$G_T - L + \alpha T - 2C_S$	$G_T + \alpha T - C_S - C_F$	$\omega^3(1-\omega)$
3	1	0	1	1	$G_C + \alpha T - C_S - C_F$	$G_T + \alpha T - 2C_S - L$	$\omega^3(1-\omega)$
4	1	0	1	0	$\alpha T - C_S - C_F - L$	$\alpha T - C_S - C_F - L$	$\omega^2(1-\omega)^2$
5	1	0	0	1	$\alpha T + G_C - C_S$	$G_T - C_F + \alpha T - C_S - L$	$\omega^2(1-\omega)$
6	1	0	0	0	$\alpha T - L - C_S$	$\alpha T - L - 2C_F$	$\omega(1-\omega)^2$
7	0	1	1	0	$G_T - G_F + \alpha T - C_S - L$	$G_C + \alpha T - C_S$	$\omega^2(1-\omega)$
8	0	0	1	0	$\alpha T - 2C_F - L$	$\alpha T - C_S - L$	$\omega(1-\omega)^2$
9	0	0	0	0	$\alpha T - C_F - L$	$\alpha T - C_F - L$	$(1-\omega)^2$

2.4.3 A、B都选择不信任策略

当A、B两节点都选择不信任策略时,收益如表5所列。

表5 A、B都选择不信任策略

Num	A-S	B-S	A收益	B收益	概率
1	1	1	$-L - C_S$	$-L - C_S$	ω^2
2	1	0	$-L - C_S$	$-L - C_F$	$\omega(1-\omega)$
3	0	1	$-L - C_F$	$-L - C_S$	$\omega(1-\omega)$
4	0	0	$-L - C_F$	$-L - C_F$	$(1-\omega)^2$

综上所述,当A、B都采用信任策略时,收益相等,为 $\omega^2 G_T + \omega^2 G_C + \omega^2 L + \alpha T - (1-\omega^2)C_F - (\omega + \omega^2)C_S - L$ 。当A、B两节点中有一个节点采用信任策略,另一个采用不信任的策略时,采用信任策略的节点的期望收益为: $\omega^2 G_T + \alpha T - (1-\omega^2)C_F - (\omega + \omega^2)C_S - L$,不信任策略的收益为: $\omega^2 G_T + \omega^2 L - (1-\omega)C_F - \omega C_2 - L$ 。当节点都采用不信任策略时,双方的收益相为: $-(1-\omega)C_F - \omega C_S - L$ 。

结论,DTMSN节点博弈模型为3维组合 $G_3(P, S, U)$,其中P是玩家集合,为网络中的任意两个相遇节点,S为节点的策略集合, $S = \{\text{信任}, \text{不信任}\}$;U是参与博弈的双方的收益形成的矩阵,可由表6表示。

表6 博弈双方的收益矩阵

	1	信任	不信任
		(a, a)	(b, c)
2	信任	(c, b)	(d, d)

表6中,

$$a = \omega^2 G_T + \omega^2 G_C + \omega^2 L + \alpha T - (1-\omega^2)C_F - (\omega + \omega^2)C_S - L \quad (6)$$

$$b = \omega^2 G_T + \alpha T - (1-\omega^2)C_F - (\omega + \omega^2)C_S - L \quad (7)$$

$$c = \omega^2 G_T + \omega^2 L - (1-\omega)C_F - \omega C_2 - L \quad (8)$$

$$d = -(1-\omega)C_F - \omega C_S - L \quad (9)$$

表6中每种情况用小括号来表示,第一个元素表示在该情况下博弈参与者 P_1 的收益,第二个元素表示在该情况下博弈参与者 P_2 的收益。

3 信任博弈理论分析

定义 在标准式博弈 $G = \{S_1, \dots, S_n; U, \dots, U_n\}$ 中,n表

示参与者的个数。如果参与者的战略组合 $\{S_1^*, S_2^*, \dots, S_n^*\}$ 满足对每一参与者 i, S_i^* 是它针对博弈中其它 $n-1$ 个参与者所选战略组合 $S_1^*, S_2^*, \dots, S_{i-1}^*, S_{i+1}^*, \dots, S_n^*$ 的最优反应战略,那么称战略组合 $\{S_1^*, S_2^*, \dots, S_n^*\}$ 是该博弈的一个纳什均衡。即:

$$U_i(S_1^*, S_2^*, \dots, S_{i-1}^*, S_i^*, S_{i+1}^*, \dots, S_n^*) \geq U_i(S_1^*, S_2^*, \dots, S_{i-1}^*, S_i, S_{i+1}^*, \dots, S_n^*) \quad (10)$$

性质1 当 $\omega^2 G_T + \alpha T - (\omega - \omega^2)C_F - \omega^2 C_S > 0$ 时,信任是该博弈的纳什均衡。

证明,由上述定义可得对于DTMSN的信任博弈,若信任是博弈的纳什均衡,那么对于参与博弈的两个节点 P_1, P_2 而言,信任策略应该满足以下两个条件:1)信任策略是对对方任何策略的最优反应;2)采用信任策略获得的收益要不小于采用不信任策略所获收益。由于本博弈 P_1, P_2 处于对等关系,因此证明信任对于 P_1 满足以上两个条件即可得到信任是本文博弈的纳什均衡。

对于条件1,由表6可知,当 P_2 采取信任策略时, P_1 的收益分别为 a, b ,对应于 P_1 采取信任策略和 P_1 采取不信任策略。可得式(11):

$$a - b = \omega^2 G_C + \omega^2 L \quad (11)$$

其中, ω, G_C, L 均为大于零的数,显然 $a - b > 0$,即当 P_2 采取信任策略时, P_1 的最优反应为信任策略。当 P_2 采取不信任策略时, P_1 的收益分别为 b, d ,对应于 P_1 采取信任策略和 P_1 采取不信任策略。可得式(12):

$$b - d = \omega^2 G_T + \alpha T + \omega^2 C_F - \omega^2 C_S \quad (12)$$

可知 $b - d > \omega^2 G_T + \alpha T - (\omega - \omega^2)C_F - \omega^2 C_S > 0$,即当 P_2 采取不信任策略时, P_1 的最优反应为信任策略。

综合式(11)、式(12)可得,无论 P_2 采取信任或者不信任策略中的哪种策略, P_1 对其的最优策略都是信任策略。

对于条件2,为证明方便,可首先假设 P_2 采取信任策略的概率为 x ,则 P_2 采取不信任策略的概率可描述为 $1-x$ 。

由上述条件可得, P_1 采用信任策略可获得的期望为:

$$E_t = xa + (1-x)b \quad (13)$$

P_2 采用不信任策略可获得的期望为:

$$E_d = xc + (1-x)d \quad (14)$$

由 $a - c = \omega^2 G_T + \alpha T - (\omega - \omega^2)C_F - \omega^2 C_S > 0$ 且 $b - d > 0$ 可得,对于任意的 $0 \leq x \leq 1, E_t > E_d$ 。即无论 P_2 采取哪种策略, P_1 采取信任策略获得的收益都要大于其采取不信任策略获得的收益。

综合可得,信任是博弈参与者 P_1 的最优策略,同时由于 P_2 与 P_1 处于对等关系,因此信任也是博弈参与者 P_2 的最优策略。

(信任,信任)是一种参与者都不会违背的战略组合,故信任是本博弈的纳什均衡。证毕。

性质2 当 $\omega^2 G_T + \alpha T - (\omega - \omega^2)C_F - \omega^2 C_S < 0$ 时,本博弈不存在纳什均衡。

证明,同样地,需要证明以上两个条件。

对于条件1,当 P_2 采用信任博弈时,由于 $a - c = \omega^2 G_T + \alpha T - (\omega - \omega^2)C_F - \omega^2 C_S < 0$ 即 $a < c, P_1$ 对于 P_2 的最优反应为不信任。当 P_2 采用不信任策略时, P_1 的收益分别为 b, d ,

且 $b-d=\omega^2 G_T+\alpha T+\omega^2 C_F-\omega^2 C_S$, 由于 $C_F \geq C_S$, 因此 $b-d > 0$, 即 $b > d$ 。此时, 对于 P_2 采取不信任策略, P_1 的最优反应为信任。

综上所述, 当 $\omega^2 G_T+\alpha T-(\omega-\omega^2) C_F-\omega^2 C_S < 0$ 时, 不存在对于 P_2 的任何策略, P_1 的最优反应都是一样的。所以当 $\omega^2 G_T+\alpha T-(\omega-\omega^2) C_F-\omega^2 C_S < 0$ 时, 本博弈不存在纳什均衡。证毕。

4 仿真分析

本文采用 OPNET 14.5 为仿真工具, 对文中所提基于博弈和信誉的移动传感器网络转发策略进行仿真。

将文献[10]提出的 TE(T-Epidemic)和 TSW(T-Spray and Wait)与本文提出的改进算法添加到 Epidemic 和 Spray and Wait 算法上, 不同的自私节点比例的情况下对在自私节点的检测率、投递成功率、网络开销 3 个指标进行对比。

(1) 自私节点的检测

实验结果如图 3 所示。

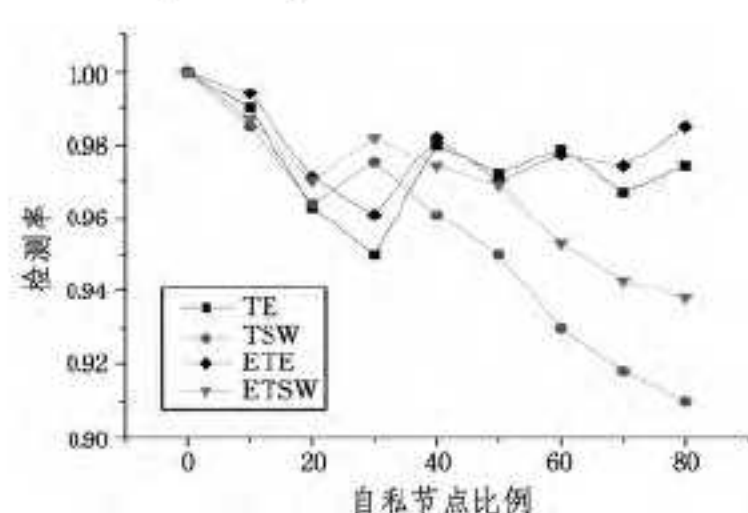


图 3 自私性检测率

由图 3 可知, 在相同的条件下新的策略比原有的策略更具优势, 同时节点自私性的检测率都在 90% 以上。

(2) 发送成功率

发送成功率指的是目的节点接收的数据与源节点发送的数据的比率。实验结果如图 4 所示。

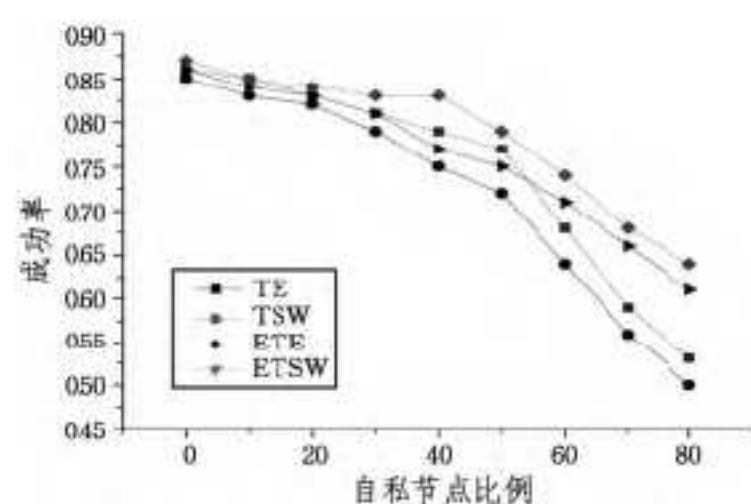


图 4 发送成功率

由图 4 可知, 基于博弈的机制由于能够对节点的自私性起到一定的抑制作用, 因此在发送成功率上与原有的相比有一定的提高和改善。

(3) 网络开销

网络开销定义为转发消息总数和交付成功的消息数的比率。实验结果如图 5 所示。

由图 5 可知, 由于 ETSW 和 ETE 在中间节点的选取上

选择更可信、更愿意转发数据的节点进行数据的中间传递, 因此新算法和原算法相比在网络开销上有不少的改善。

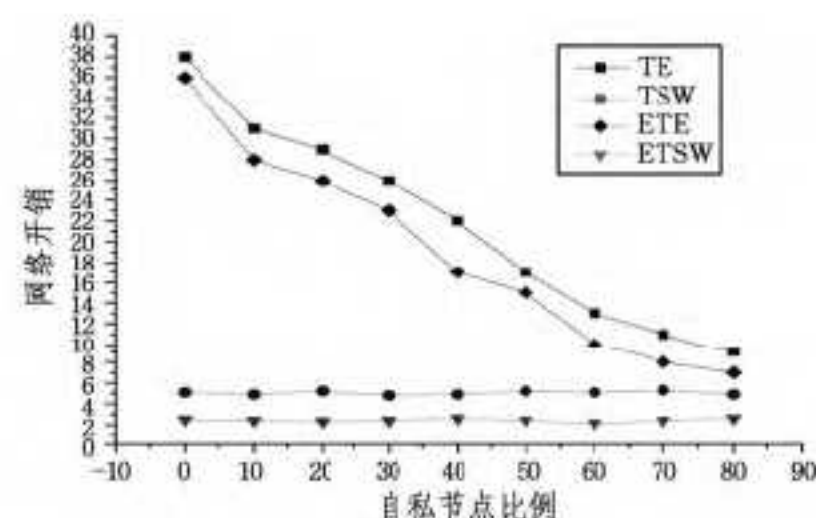


图 5 网络开销

结束语 本文对已有的延迟容忍移动传感器网络中自私行为检测机制中存在的计算不精确的问题进行了改善, 提高了节点自私检测的精确性; 同时引入博弈的思想激励节点之间的合作, 激发节点参与合作的积极性, 通过提高节点之间的相互合作, 提高了数据传递的成功率, 并在一定程度上降低了网络的开销。

参考文献

- [1] Burleigh S, Hooke A, Torgerson L, et al. Delay-tolerant networking: an approach to interplanetary Internet[J]. Communications Magazine IEEE, 2003, 41(6): 128-136
- [2] Leguay J, Friedman T, Conan V. DTN routing in a mobility pattern space[C] // Proceedings of the 2005 ACM SIGCOMM Workshop on Delay-tolerant Networking. ACM, 2005: 276-283
- [3] Jackson R S, Voss S G, Wilson Z C, et al. An Athymic Rat Model for Mandibular Osteoradionecrosis Allowing for Direct Translation of Regenerative Treatments[J]. Otolaryngology Head & Neck Surgery, 2015, 153(4): 526-31
- [4] Wu H, Wang Y, Dang H, et al. Analytic, simulation, and empirical evaluation of delay/fault-tolerant mobile sensor networks[J]. IEEE Transactions on Wireless Communications, 2007, 6(9): 3287-3296
- [5] 朱金奇, 刘明, 龚海刚, 等. 延迟容忍移动传感器网络中基于选择复制的数据传输[J]. 软件学报, 2009, 20(8): 2227-2240
- [6] 刘唐, 彭舰, 王建忠, 等. 延迟容忍移动传感器网络中基于节点优先级的数据转发策略[J]. 计算机科学, 2011, 38(3): 140-143
- [7] 唐作用, 袁艺嘉, 董永强, 等. 基于信誉值维护的机会网络自私节点检测机制[J]. 通信学报, 2012(z2): 217-221
- [8] 沈士根, 马绚, 蒋华, 等. 基于演化博弈论的 WSNs 信任决策模型与动力学分析[J]. 控制与决策, 2012, 27(8): 1133-1138
- [9] 李紫川, 沈士根, 曹奇英. 基于反思机制的 WSNs 节点信任演化模型[J]. 计算机应用研究, 2014, 31(5): 1528-1531
- [10] Li Y, Xu H, Cao Q, et al. Evolutionary Game-Based Trust Strategy Adjustment among Nodes in Wireless Sensor Networks[J]. International Journal of Distributed Sensor Networks, 2015, 2015: 1-12