Int. J. Communications, Network and System Sciences, **2013, 6, 236-243**
http://dx.doi.org/10.4236/ijcns.2013.65026 Published Online May 2013 (http://www.scirp.org/journal/ijcns)

Utility-Based Node Cooperation Mechanism in Wireless Sensor Networks

Xiaohui Lin*, Junling Zhang, Can Hu, Yide Huang, Bin Chen, Ning Xie, Hui Wang
Shenzhen Key Lab of Advanced Communications and Information Processing,
Faculty of Information Engineering, Shenzhen University, Shenzhen, China
Email: *xhlin@szu.edu.cn

Received March 14, 2013; revised April 12, 2013; accepted May 6, 2013

ABSTRACT

In wireless sensor networks, due to the energy and resource constraints, nodes may be unwilling to forward packets for their neighbors. This can render severe deteriorations in the network performance and malfunctions of the system. To tackle such selfish behaviors and enhance the cooperation among sensors, based on reputation and energy consumption of each node, we present a utility function to punish the malicious nodes and encourage cooperation among nodes. Specifically, we firstly give a mixed strategy Nash equilibrium solution for the two nodes. Then we extend the model to multi-nodes scenario. With the unity function, each sensor's reputation is evaluated according to its degree of cooperation. The extensive simulation results have shown the effectiveness of the mechanism, in that the cooperative behaviors are encouraged, which can ensure the normal functioning of the network system.

Keywords: Wireless Sensor Networks; Selfish Node; Game Theory; Reputation; Energy

1. Introduction

Wireless sensor networks (WSNs) have recently penetrated deeply into our society and drawn considerable attentions from the academia and industry. WSNs are composed of a large number of cheap and tiny senor nodes deployed in monitored areas. Compared with traditional networks, wireless sensor networks have dynamic topology and are characterized by their non-centralized structure, self-organized and multi-hop features. As a novel technology in acquiring and processing information, WSN has been widely applied in many fields, such as military affairs, industry, agriculture, health care, and environmental monitoring, etc. [1].

However, in the deployment of WSN, one of the key concerns is the limited energy constraint, which has restricted the capabilities of sensor nodes in data communication, computing, and information processing.

Specifically, to conserve limited energy, some selfish nodes may be unwilling to forward data for their neighboring nodes, which can cause the decrease in network throughput and the severe deterioration in system performance. Therefore, to guarantee network performance, cooperation among sensors should be definitely encouraged, and reasonable incentive mechanisms [2-4] should also be designed to fulfill this target.

*Corresponding author.

2. Related Work

Thus far, many different methods have been proposed to tackle the selfish issues of nodes. Generally, they can be classified into three categories.

2.1. Reputation Based Mechanism

In this mechanism [5,6], if a node successfully forwards data packets for its neighbors, the reputation of this node will be increased; otherwise if it drops packets, the reputation will be decreased. When the reputation value drops below a threshold, the node is either punished or isolated. In [7], Marti uses a watchdog algorithm to identify misbehaving nodes. In addition, they also design a path rater to enhance the routing quality by deleting these selfish nodes from the path. Similarly, by using the idea of Watchdog, authors in [8] propose CONFIDANT (Cooperation of Nodes Fairness in Dynamic Ad-hoc Networks) protocol, which aims at detecting and isolating misbehaving nodes.

2.2. Credit-Payment Mechanism

This mechanism is similar to reputation-based one. The

difference is that the mechanism introduces a concept of virtual currency or credits as payment to a cooperating neighbor from which a node has received service. A sending node will pay its neighbor who has successfully forwarded packets for it. On the other hand, if a non-cooperative neighbor refuses to provide service, it will forfeit its virtual currency or credits as a punishment. If the virtual currency is used up, it cannot send its own packets anymore [9].

In [10], Buttyaan *et al.* propose Packet Purse Model (PPM), in which, a type of virtual currency called "nuglets" is used. In PPM, each packet is loaded with nuglets by the source. Each forwarding node can take some amount of nuglets as reward for the forwarding services, thus stimulating the cooperative behaviors of the neighbors.

2.3. Game Theory Mechanism

Game theory provides analytical tools to predict the outcome of complex interactions among rational entities. A game consists of a set of players, a set of strategies available to players, and a specification of payoffs for each combination of strategy [11,12]. The cooperation among sensors can also be model as a game. By properly designing the utility function in the game, the high throughput can be guaranteed and energy consumption can also be balanced [13,14]. In [15], a repeated game model for WSN is proposed, and punishment mechanism is also employed to encourage the cooperation of sensor nodes.

3. Model and Assumptions

In this paper, we will design a utility function based on reputation and energy consumption of nodes to encourage cooperation among nodes. We will also propose a mechanism to monitor the malicious nodes and selfish nodes. Firstly, we give the system model and basic concepts and assumptions.

3.1. Node Entity

A node has the following attributes:

1) ID-Every node has its unique ID.

2) Type. The nodes are categorized into three types—normal nodes, malicious nodes and selfish nodes. Normal nodes always cooperate. Malicious nodes always drop packets from neighbors. Selfish nodes occasionally participate in forwarding packets (with some probability). We assume that, at the beginning, selfish nodes drop packets more often. When their reputation values fall below a certain threshold, they begin to behave like normal nodes and forward more packets for others.

Transmission Range. Nodes can only communicate with their neighbors which are within their transmission range. The distance between two nodes can be written as

$$d=\sqrt{\left(x_2-x_1\right)^2+\left(y_2-y_1\right)^2}$$

where, $\left(x_1,y_1\right),\left(x_2,y_2\right)$ are coordinates of two nodes. If the value of d is less than or equal to the transmission range (in this paper, we set d to 10), the two nodes can be considered as neighbors.

1) Reputation. We assume the initial reputation of every node is $R_0=10$. Nodes participating in packets forwarding can gain some reputation as a reward (this increment of reputation is defined as R_{inc}), while those who act selfishly will lose some reputation as a punishment (this decrement of reputation is defined as R_{dec}).

2) Energy. The initial energy level of all nodes at the beginning in the network is E_0. When sending/forwarding and receiving packets, node will consume some amount of energy. A node will die when its energy is depleted.

3.2. Network Setup

In this paper, the simulated network is demonstrated in **Figure 1**. The area is 30×30 m with 10 nodes, which are numbered from 0 to 9. Neighbors are connected by straight line. One malicious node (node 6) and two selfish nodes (node 0 and 4) are included into the network.

3.3. Cooperation Modeling

We assume each node will send packets to each other in the network. Each packet is included the following information-sequence number, source node, and destination node.

We design a utility function, which takes node reputation and energy consumption into consideration. The utility function can be expressed as

$$U_i\left(t\right)=S_i\left(t\right)\cdot f_i\left(t\right)\cdot\left[B_i\left(t\right)-C_i\left(t\right)\right]-\left[1-f_i\left(t\right)\right]\cdot P_i\left(t\right) \quad (1)$$

where $S_i\left(t\right)$ is a Boolean variable, which indicates whether node i can participate in packet forwarding based on its residual energy $E_i\left(t\right)$.

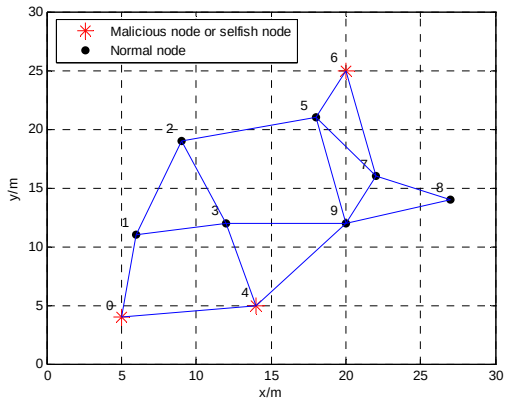

Figure 1. Node topology (30 × 30 m).

$$S_i(t)=\begin{cases}1, E_i(t)>Eth\\ 0, \text{otherwise}\end{cases}$$

Only when the residual energy level of node i is higher than the minimum energy threshold Eth, can it participate in the packet forwarding. Otherwise, it will be excluded from the network if its energy falls below the threshold level. $f_i(t)$ is the forward probability, which has to be decided by the game strategy. We set the average value of total utility U_{mean} as the threshold (will be illustrated later, see Equation (7)), and when the utility of a neighboring node is less than this threshold, node i will drop packets from this neighbor. $B_i(t), C_i(t)$ and $P_i(t)$ denote the benefit, cost and punishment in a node's packet forwarding respectively. Specifically, benefit and punishment refer to the increment and decrement of reputation, respectively, while cost refers to the energy consumed by node in packet forwarding.

We average the reputation values that all neighbors assign to a node at the end of each round and get reputation of that node. In **Table 1** we list the definitions of the parameters to be used in the paper. According to the above definitions, we have:

Table 1. Parameters and descriptions.

Parameters	Descriptions
$R_i(t)$	the current reputation of node i
$R_{ik}(t)$	reputation assigned to node i by its neighboring node k in period t
$n_{ik}^f(t)$	the number of packets forwarded by node i for node k in period t
$n_{ik}^d(t)$	the number of packets from node k but dropped by node i in period t
K_i	the number of neighbors of node i
$E_i(t)$	the current energy of node i
$E_{ik}^t(t)$	transmitting energy consumption for packets from node i to its neighbor node k in period t
$E_{ik}^r(t)$	energy consumption by node i to receive packets from node k in period t
$n_{ik}^t(t)$	the number of packets transmitted by node i for node k in period t
$n_{ik}^r(t)$	the number of packets received by node i from node k in period t
$n_{ik}^s(t)$	the number of packets sent by node i to node k in period t
Et	transmitting energy consumption for one packet
Er	receiving energy consumption for one packet
$F_i(t)$	the total number of forwarding packets by node i in period t
$D_i(t)$	the total number of packets dropped by node i in period t
α, β	normalized weight factors, $\alpha, \beta \in [0,1]$

$$E_i(t)=E_i(t-1)-\sum_k\left[E_{ik}^t(t)+E_{ik}^r(t)\right],$$
$$E_{ik}^t(t)=n_{ik}^t(t)\cdot Et, E_{ik}^r(t)=n_{ik}^r(t)\cdot Er,$$
$$n_{ik}^t(t)=n_{ik}^f(t)+n_{ik}^s(t),$$
$$B_i(t)=\frac{1}{k}\sum_k n_{ik}^f(t)\cdot R_{inc},$$
$$C_i(t)=\sum_k\left[E_{ik}^t(t)+E_{ik}^r(t)\right],$$
$$P_i(t)=\frac{1}{k}\sum_k n_{ik}^d(t)\cdot R_{dec}.$$

In the paper, we only consider alive nodes, thus we let $S_i=1$. Therefore, Equation (1) can be written as

$$\begin{aligned}&U_i(t)\\&=f_i(t)\cdot\left[\frac{\sum_k n_{ik}^f(t)\cdot R_{inc}}{K_i}-\sum_k\left(n_{ik}^f(t)\cdot Et+n_{ik}^r(t)\cdot Er\right)\right]\\&-\left[1-f_i(t)\right]\cdot\left[\frac{\sum_k n_{ik}^d(t)\cdot R_{dec}}{K_i}\right]\end{aligned}\quad(2)$$

We consider the packet forwarding at the relay nodes. The packet forwarding decision making at a node is illustrated in **Figure 2**. In the proposed utility function, if a node is always forwarding packets for its neighbors, then we have $n_{ik}^r(t)=n_{ik}^f(t)$. Therefore, the above equation can be rewritten as

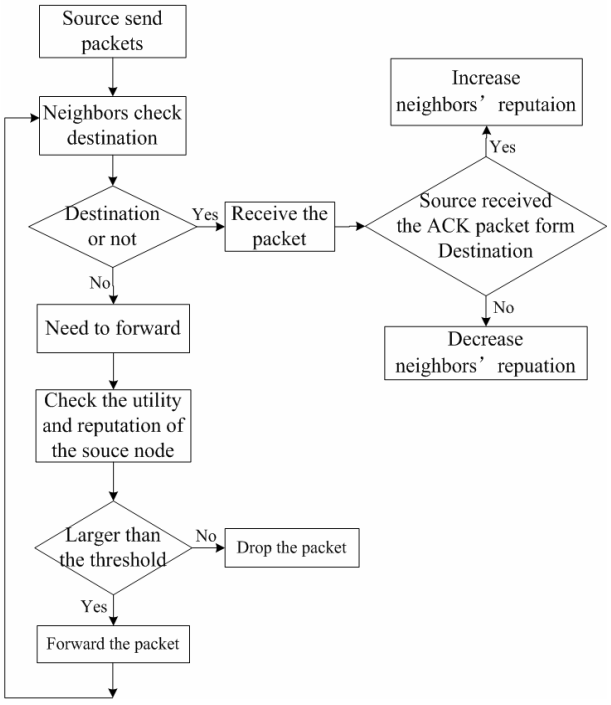

Figure 2. Packet delivery at sensor node.

$$U_i(t) = f_i(t)\cdot\left[\frac{\sum_k n_{ik}^f(t)\cdot R_{inc}}{K_i} - \sum_k n_{ik}^f(t)\cdot(Et+Er)\right] - \left[1-f_i(t)\right]\cdot\left[\frac{\sum_k n_{ik}^d(t)\cdot R_{dec}}{K_i}\right]$$

where $R_i(t) = \frac{1}{K_i}\sum_k R_{ik}(t)$,

$R_{ik}(t) = n_{ik}^f(t)\cdot R_{inc} - n_{ik}^d(t)\cdot R_{dec}$,

Let $F_i(t) = \sum n_{ik}^f(t), D_i(t) = \sum_k n_{ik}^d(t)$ and $U_i(t)$ can be further simplified as

$$U_i(t) = R_i(t) - F_i(t)\cdot(Et+Er) \quad (3)$$

After normalization, $U_i(t)$ can be expressed as:

$$U_i(t) = \frac{R_i(t)}{R_0} - \frac{F_i(t)\cdot(Et+Er)}{E_0 - E_i(t)} \quad (4)$$

Note that, the above utility function consists of two parts. The first part is the ratio of the current global reputation value of the node to the initial reputation value, and the second part is the ratio of the forwarding energy consumption of the node to the total energy consumption.

To reflect the effects of reputation and energy on the utility, we add two adjustable weight factors—α and β, and have the newly defined utility function given by:

$$U_i(t) = \alpha\cdot\frac{R_i(t)}{R_0} - \beta\cdot\frac{F_i(t)\cdot(Et+Er)}{E_0 - E_i(t)} \quad (5)$$

The total utility of the *n* nodes in the network is given by

$$U_{\text{total}}(t) = \sum_{i=1}^{n} U_i(t). \quad (6)$$

The average utility of total utility is

$$U_{\text{mean}}(t) = \frac{U_{\text{total}}(t)}{n}. \quad (7)$$

4. Game Model

4.1. Two Nodes Game Model

In this model, we let nodes *i* and *j* be two forwarding nodes. According to above analysis, the behaviors of two nodes can be described as the classic "prisoner dilemma problem". The payoff matrix of nodes *i* and *j* can be expressed as listed in **Table 2** [12].

We consider packets forwarding between the two neighboring nodes, and let $Er = 0.02$ J, $Et = 0.05$ J. So the energy consumption can be written as

Table 2. Payoff matrix of two nodes.

Node *i* \ Node *j*	Cooperate	Non-Cooperate
Cooperate	$R_{inc}^i(t) - E_{ij}(t)$, $R_{inc}^j(t) - E_{ji}(t)$	$-R_{dec}^i(t) - E_{ij}(t)$, $-R_{dec}^j(t)$
Non-Cooperate	$-R_{dec}^i(t)$, $-R_{dec}^j(t) - E_{ji}(t)$	$-R_{dec}^i(t)$, $-R_{dec}^j(t)$

$E_{ij} = E_{ji} = Et + Er = 0.05 + 0.02 = 0.07$ J. Let $R_{dec} = 1$, now we need to find the proper R_{inc}.

The behaviors of different nodes can be complicated-normal nodes always cooperate, and malicious nodes never cooperate, and selfish nodes only participate in packet forwarding with a certain probability. Let the forwarding probability of node *i* and *j* be f_i and f_j respectively, then the mixed strategies for the two nodes are $\sigma_i = (f_i, 1-f_i)$ and $\sigma_j = (f_j, 1-f_j)$ respectively. Thus the expected payoff of node *i* is given by:

$$\begin{aligned} & v_i(\sigma_i, \sigma_j) \\ &= f_i\left[f_j\left(R_{inc}^i - E_{ij}\right) - \left(1-f_j\right)\left(R_{dec}^i + E_{ij}\right)\right] \\ &\quad + \left(1-f_i\right)\left[f_j\left(-R_{dec}^i\right) - \left(1-f_j\right)R_{dec}^i\right] \\ &= f_i\left(f_j R_{inc}^i + f_j R_{dec}^i - R_{dec}^i - E_{ij}\right) - \left(1-f_i\right)R_{dec}^i \\ &= f_i\left(f_j R_{inc}^i + f_j R_{dec}^i - E_{ij}\right) - R_{dec}^i \end{aligned} \quad (8)$$

We differentiate this payoff with respect to f_i, and let the differentiation value equal to zero:

$$\frac{\partial v_i}{\partial f_i} = f_j R_{inc}^i + f_j R_{dec}^i - E_{ij} = 0 \quad (9)$$

Then we have:

$$f_j^* = \frac{E_{ij}}{R_{inc}^i + R_{dec}^i} \quad (10)$$

Similarly, for the other node, we have:

$$f_i^* = \frac{E_{ji}}{R_{inc}^j + R_{dec}^j} \quad (11)$$

With Equations (10) and (11), the best-responses of the two nodes are shown in **Figure 3**. We get three Nash Equilibrium points-mixed strategy NE (Nash equilibrium), and two pure strategies NE (both nodes cooperate, and neither nodes cooperates). From the results, we can see that the strategy-(cooperate, cooperate) has the highest payoff for the two nodes, with which we can achieve Pareto Optimality [16]. Therefore, cooperation is the best strategy for a node.

4.2. Multi-Node Game

Then we extend the two-node game to multi-node sce-

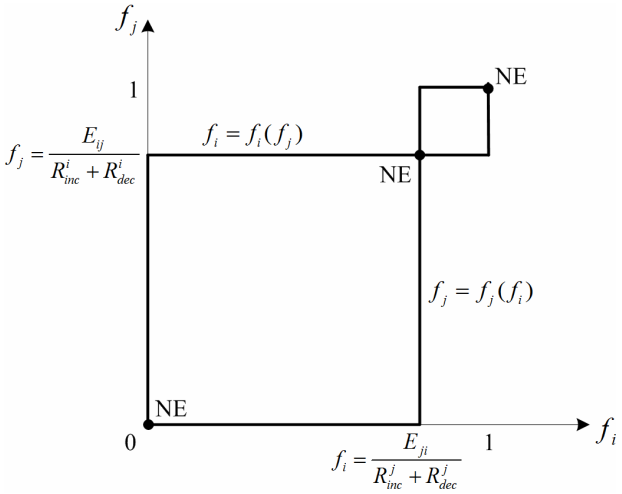

Figure 3. The best responses of two neighbor nodes.

nario. Without loss of generality, we consider the utility of node i. To encourage cooperation among nodes, the utility of cooperation should be larger than that of non-cooperation, *i.e.*,

$$\alpha \frac{F_i(t) \cdot R_{inc}}{K_i \cdot R_0} - \beta \frac{F_i(t) \cdot (Et + Er)}{E_0 - E_i(t)} > -\alpha \frac{D_i(t) \cdot R_{dec}}{K_i \cdot R_0}$$

which can be further simplified as:

$$\alpha \frac{F_i(t) \cdot R_{inc} + D_i(t) \cdot R_{dec}}{K_i \cdot R_0} > \beta \frac{F_i(t) \cdot (Et + Er)}{E_0 - E_i(t)} \quad (12)$$

5. Performance Analysis and Simulation Results

We calculate the NE of the proposed game model with C++ and MATLAB, and set the node's strategy according to these NEs. We use DSDV as the routing protocol. **Table 3** shows the parameter setting.

We firstly compare the proposed mechanism with the scenario that without incentive. The simulated results are shown in **Figure 4**. We can observe that, if there is no incentive, nodes will be unwilling to forward packets, which will lead to high drop packet rate. While the selfish behavior of nodes is effectively restricted by the proposed mechanism, which can remarkably lower the packet loss rate as shown in the figure.

It is observed that the proposed mechanism can restrict the behaviors of selfish nodes. Specifically, a selfish node should avoid being isolated by increasing the forwarding probability (with more cooperation behaviors). Note that a malicious node never cooperates. We set a utility threshold $U_{th}(t)$ to differentiate the selfish nodes from malicious nodes (if the utility is lower than the threshold, the node will be treated as malicious node and excluded from the network). Hence the selfish nodes can increase the forwarding probability when its utility is

Table 3. Parameters setting in the experiment.

Parameters	R_0	E_0	E_t	E_r
Values	10	80J	0.05J	0.02J

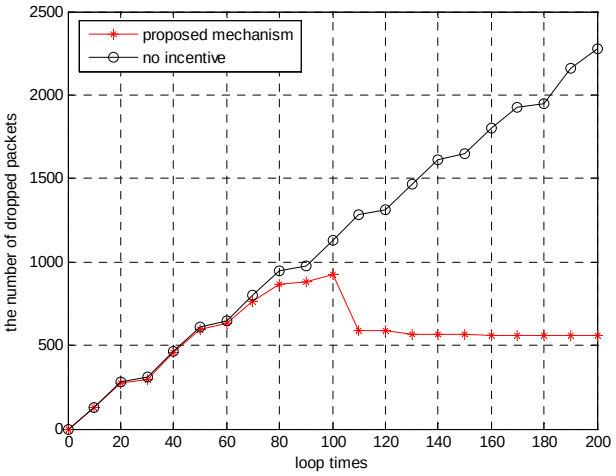

Figure 4. Number of packets dropped with time.

lower than the threshold (we set $U_{th}(t) = U_{\text{mean}}(t)$). In some papers [e.g. 4,5], the utility function is simply based on reputation, and selfish nodes will be excluded from the network once identified. The isolation of these malicious nodes can lead to the decrease in the number of packet drop as shown in **Figure 5**.

In **Figure 5**, compared with the proposed mechanism, the reputation-based mechanism can reduce the packet loss rate to zero when the malicious nodes are identified and isolated (after round time 100). This, however, can lead to unbalance in energy consumption among nodes, which can further incur early energy depletion for the nodes in the reputation-based mechanism as illustrated in **Figure 6**. Instead, in the proposed game approach, as the selfish nodes are rational, each node adaptively adjusts its forwarding probability to maximize its own utility and avoid being isolated, thus more nodes will survive and packet relay is more evenly distributed among the network. This can definitely extend the network lifetime.

Another problem need to solve is setting of R_{dec} and R_{inc}. We let $\alpha = \beta = 0.5$, and substitute these values into Equation (12), then we have

$$\frac{F_i(t) \cdot R_{inc} + D_i(t)}{10K_i} > \frac{F_i(t)(Et + Er)}{E_0 - E_i(t)}$$

which can be further Simplified as:

$$R_{inc} > \frac{10K_i(Et + Er)}{E_0 - E_i(t)} - \frac{D_i(t)}{F_i(t)} \quad (13)$$

We determine the range of R_{inc} through extensive experiments and find that $R_{inc} = 0.4$, $R_{dec} = 1$ is the proper parameter set that can ensure the cooperation of nodes.

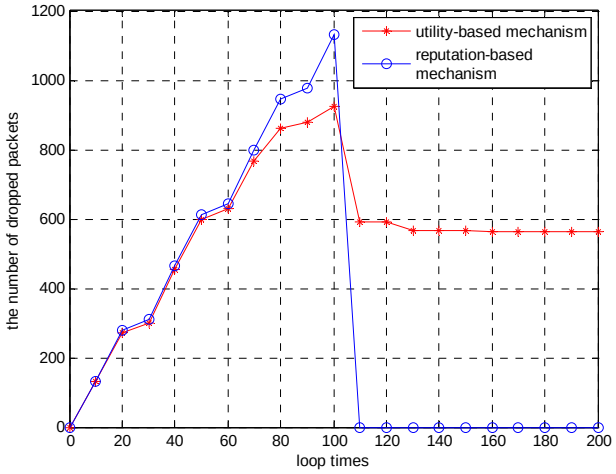

Figure 5. Number of packets dropped.

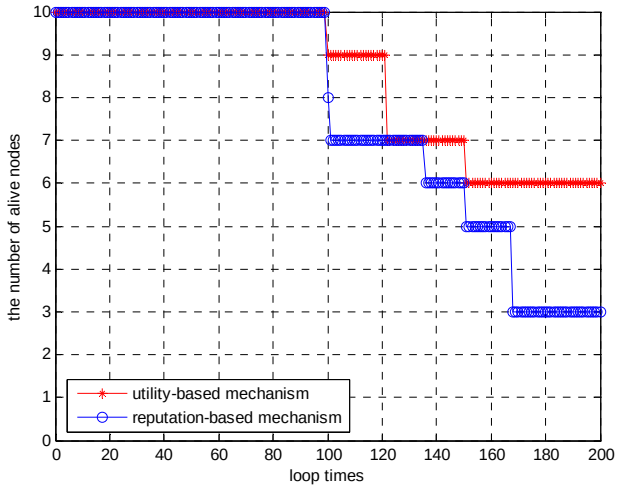

Figure 6. Number of nodes alive versus time.

5.1. The Effect of Reward and Punishment

We let $\alpha = \beta = 0.5$, and simulate four scenarios using different values of Reward and Punishment. Obviously, the smaller the R_{inc}, the smaller the reward achieved, and relatively the harsher the punishment. The reward and punishment parameters are set as the follows:

1) Scenario 1: $R_{inc} = 0.1, R_{dec} = 1$
2) Scenario 2: $R_{inc} = 0.2, R_{dec} = 1$
3) Scenario 3: $R_{inc} = 0.3, R_{dec} = 1$
4) Scenario 4: $R_{inc} = 0.4, R_{dec} = 1$
5) Scenario 5: $R_{inc} = 0.5, R_{dec} = 1$

It can be seen from **Figure 7**, the packet loss rate is high in either scenario 1 (small reward value) or scenario 5 (large reward value). This phenomenon is reasonable since when the reward for packet forwarding is small, selfish nodes can only get low incentive in packet forwarding (utility is low), thus its strategy is to decrease the forwarding probability and save energy. On the other hand, a large reward value can lead to longer time in identifying the selfish nodes, which can lead to more packet drop by the selfish nodes. Scenario 4 shows the best performance. In the 100th round, the packet loss rate dropped rapidly because the malicious node is identified and excluded from the network. Also, with the incentive mechanism, the selfish nodes can gradually adjust its probability and cooperate more in packet forwarding.

Figure 8 is the number of nodes alive with time. In the 100th round, the malicious node is identified and excluded from the network. Nodes in scenario 1 have the longest lifetime, and hence, with regard to lifetime, parameter setting in scenario 1 is optimal. However, it also shows bad performance in packet loss rate. Thus, depending on different criteria and preference, the parameter setting should be flexible and adjustable.

5.2. Eight Effects

We set $R_{inc} = 0.4$, $R_{dec} = 1$ and simulate three scenarios with different values of α and β.

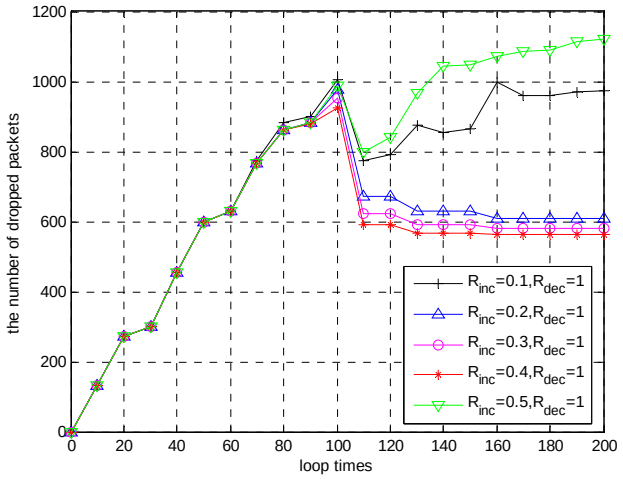

Figure 7. Number of packets dropped.

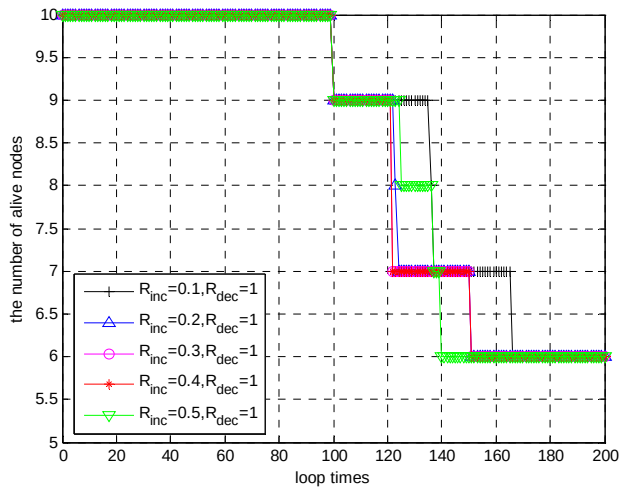

Figure 8. Number of nodes alive versus time.

1) Scenario 1: $\alpha = \beta = 0.5$
2) Scenario 2: $\alpha = 0.3, \beta = 0.7$
3) Scenario 3: $\alpha = 0.7, \beta = 0.3$

Figure 9 is the number of packets dropped with time. It is observed that parameters in scenario 1 show the best performance. The packet loss rate in scenario 2 is much higher than the other two. That's because the utility function assigns large weight to the energy part while small weight to reputation part, which causes selfish nodes to care more about energy saving instead of the reputation, leading to a high packet loss rate. By assigning equal weights to both parts, scenario 1 can strike a balance in between. We can also observe that, before the first 100 rounds, the packet loss rate increased steadily because the malicious node has not been identified. Afterwards malicious node is identified and isolated, and also due to the effect of incentive mechanism, the network performance can be maintained at a steady level.

Figure 10 is the number of node alive with time. It is shown that scenario 2 has the best performance. As analyzed above, in scenario 2, nodes care more about energy saving. Therefore, there is a tradeoff between energy consumption and performance, and we should find a balance point in between (e.g. $\alpha = \beta = 0.5$).

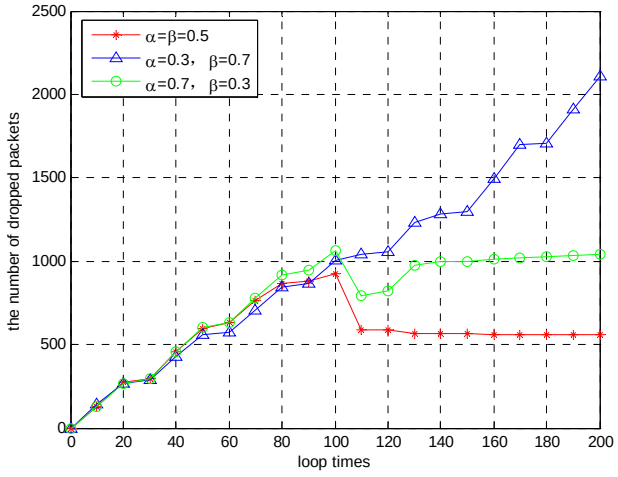

Figure 9. Number of packets dropped.

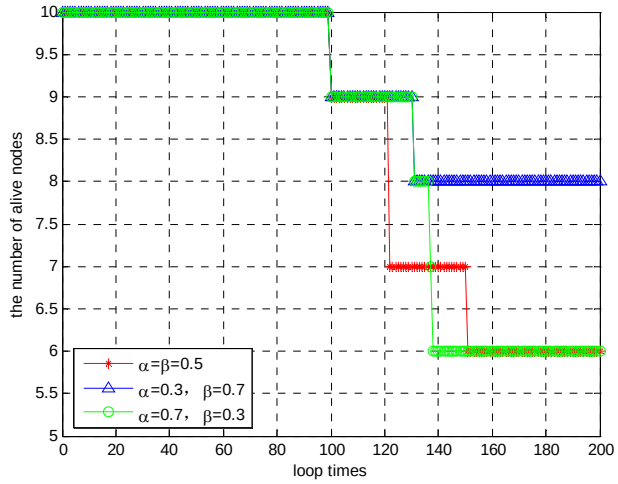

Figure 10. Number of nodes alive versus time.

6. Conclusion

In this paper, we propose a utility-based game mechanism to enhance the cooperation among sensor nodes. In the mechanism, reputation and energy of the nodes are taken into consideration. We have also derived the Nash equilibrium solution to the game and extended it to a multiple-node scenario. With the mechanism, by properly tuning the related parameters, malicious node can be identified and isolated, and at the same time, selfish behaviors can also be restricted. Additionally, simulation results show that the network performance of our mechanism is better than that of conventional punishment mechanism, in which selfish nodes will be directly removed from the network once identified. Instead, in the proposed method, selfish node is not excluded, and with the incentive mechanism, the selfish node can adjust its behavior, thus balancing the energy consumption and enhance the network lifetime. Finally, we have also illustrated the effects of different parameters on the network, which can provide a guideline for the optimization of the mechanism.

7. Acknowledgements

The research was jointly supported by research grant from Natural Science Foundation of China under project numbers NSFC60602066, NSFC60773203, NSFC60902016, NSFC61001182 and NSFC61171071, 973 Program under the project number 2013CB336700, and grants from Foundation of Shenzhen City under project numbers JC201005250035A, JC201005250047A, JC201005280404A JC201005280556A, JCYJ20120613115037732, and ZDSY20120612094614154.

REFERENCES

[1] I. F. Akyildiz, S. Weilian, Y. Sankarasubramaniam, *et al*., "A Survey on Sensor Networks," *IEEE Communications Magazine*, Vol. 40, No. 8, 2002, pp. 102-114. doi:10.1109/MCOM.2002.1024422

[2] S. Vikram, N. Pavan, C. F. Chiasserini, *et al*., "Cooperation in Wireless Ad Hoc Networks," *Proceedings of the INFOCOM* 2003 *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications*, San Franciso, 30 March-3 April 2003.

[3] E. Altman, A. A. Kherani, P. Michiardi and R. Molva. "Non-Cooperative Forwarding in Ad-hoc Networks," Technical Report INRIA Report No. RR-5116, 2004..

[4] P. Marbach and Q. Ying, "Cooperation in Wireless Ad Hoc Networks: A Market-Based Approach," *IEEE/ACM*

Transactions on Networking, Vol. 13, No. 6, 2005, pp. 1325-1338. doi:10.1109/TNET.2005.860109

[5] P. Michiardi and R. Molva, "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," *Proceedings of the IFIP TC*6/*TC*11 6*th Joint Working Conference on Communications and Multimedia Security*, Deventer, 3-5 September 2002, pp. 107-121.

[6] S. Bansal and M. Baker, "Observation-Based Cooperation Enforcement in Ad Hoc Networks," Technical Paper, 2003.

[7] S. G. Marti, T. J. Giuli and K. Lai, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," MOBICOM, Boston, 2000, pp. 255-265.

[8] S. Buchegger and J. L. Boudec, "Performance Analysis of the CONFIDANT Protocol Cooperation of Nodes-Fairness in Dynamic Ad-Hoc Networks," *ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Lausanne, 9-11 June 2002, pp. 226-236. doi:10.1145/513800.513828

[9] S. Zhong, J. Chen and Y. R. Yang, "Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks," *Proceedings of the INFOCOM* 2003 *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications*, San Franciso, 30 March-3 April 2003.

[10] L. Buttyaan and J. P. Hubaux, "Nuglets: A Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks," Technical Report No. DSC/2001/001, Swiss Federal Institute of Technology (EPFL), Lausanne, 2001.

[11] R. Gibbons, "Game Theory for Applied Economists," Pricenton University Press, Princeton, 1992.

[12] M. J. Osborne and A. Rubinste, "A Course in Game Theory," The MIT Press, Cambridge, 1994.

[13] D. Levin, "Punishment in Selfish Wireless Networks: A Game Theoretic Analysis," *Proceedings of the ACM Workshop on the Economics of Networked Systems* (*NetEcon* 2006), Ann Arbor, 11 June 2006.

[14] H. Zhu, J. Zhu and K. J. R. Liu, "A Cartel Maintenance Framework to Enforce Cooperation in Wireless Networks with Selfish Users," *IEEE Transactions on Wireless Communications*, Vol. 7, No. 5, 2008, pp. 1889-1899. doi:10.1109/TWC.2008.061014

[15] Y. Lu, J. Shi and L. Xie, "Repeated-Game Modeling of Cooperation Enforcement in Wireless Ad Hoc Network," *Journal of Software*, Vol. 19, 2008, pp. 755-756. doi:10.3724/SP.J.1001.2008.00755

[16] J. Harsanyi and R. Selten, "A General Theory of Equilibrium Selection in Games," Cambridge University Press, Cambridge, 1988.

