http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 13 (5): 989-995, 2014
ISSN 1812-5638 / DOI: 10.3923/itj.2014.989.995
© 2014 Asian Network for Scientific Information

ACFRI: An Anti-collusion and Fair Reputation-based Incentive Mechanism in Wireless *ad hoc* Sensor Networks

[1]Cheng Chang, [2]Ye Wang, [1]Xinyu Wang and [3]Yongsheng Fu
[1]College of Computer Science, Zhejiang University, Hangzhou, 310027, China
[2]School of Computer and Information Engineering, Zhejiang Gongshang University, Hangzhou, 310018, China
[3]AliPay (China) Internet Technology Company, China

Abstract: The lifetime of *ad hoc* networks is limited by the battery life of individual sensors. As deployed sensors may be owned and supported by different stakeholder, they are selfish agents by instinct, only maximizing their own utility. However, selfish behaviors degrade the network performance significantly. To address this problem, we propose an Anti-Collusion and Fair Reputation-based Incentive mechanism (ACFRI). The ACFRI mechanism measures the reputation of each node based on not only the past routing behaviors but also the evaluated residual energy. Only the neighbor node is responsible for punishment on selfishness of the source node. Other nodes on the routing path can monitor routing behaviors of the source node and punish the neighbor node if it colludes with the source node. The ACFRI mechanism can achieve fairness by the objective reputation and make collusive behaviors unattractive. The experimental results show that the ACFRI mechanism can punish selfish nodes and achieve fairness and anti-collusion successfully, under 10% throughput overhead.

Key words: Wireless *ad hoc* sensor network, packet forwarding, selfish behavior, fairness, collusion

INTRODUCTION

A wireless *ad hoc* sensor network is a decentralized and self-organized network without any pre-established infrastructure, where the transmission range of each sensor is limited due to the energy constraint. With cheap sensors, this type of network provides an efficient solution to autonomous environmental monitoring (Cerpa *et al*., 2001). A single sensor has its own local controller and uses low-power wireless transceivers to periodically transmit its recorded data to a central receiver. The communication beyond the transmission range relies on intermediate nodes to forward packets. It may be reasonable to assume that nodes would sacrifice their own battery life and relay messages for other nodes. However, there are many negative cases in real deployment. For example, wireless *ad hoc* sensor networks are proposed for forest fire detection. Individual landowners supply and support individual sensors, yet gain benefit from the entire sensor network (Kremens *et al*., 2002). Thus, these sensors are selfish agents by instinct, only maximizing their own utility (saving battery) (Rogers *et al*., 2005). For a selfish sensor with constrained energy, it may be not cost-efficient to forward packets that are not directly beneficial to it. It has been proven that the probability of cooperation among nodes is very low without a specific mechanism for cooperation stimulation (Felegyhazi *et al*., 2006).

In this study, we focus on "selfish behavior" excluding malicious behaviors. For the selfish behavior, the disruption of network operations is only a side effect of the node's limiting use of its resources. In contrast, malicious behaviors are characterized by an active intent in disrupting communication among nodes. Furthermore, a malicious node does not conserve its own resources to achieve its objective of causing maximum harm. Although there are many reputation based solutions to selfish behaviors in the literature, two drawbacks are not covered well.

Unfairness: The fairness objective should consider the resource which is to be fairly allocated. Here the resource is the throughput attained by each node. Exist mechanisms are not effective to measure reputation value to avoid unfairness. The unfairness problem consists of two aspects (1) The reputation value based on the past behaviors is not sufficient to be used for the judgment on selfishness and (2) Few chance to increase the reputation for nodes with fewer neighbors in the network.

Corresponding Author: Cheng Chang, College of Computer Science, Zhejiang University, Hangzhou, 310027, China

Collusion: The collusion between any two nodes means no reputation validation by both nodes (Zhong and Wu, 2007). For example, two sensors owned by a single stakeholder may collude unconditionally. Existing countermeasures cannot prevent collusion. For any selfish node, if the punishment only depends on neighbors' judgment, collusive behavior can bring profits shared by collusive nodes.

In this study, we propose an Anti-Collusion and Fair Reputation-based Incentive (ACFRI) mechanism to encourage packet forwarding and suppress selfish behaviors. Node degree, past routing behaviors and residual energy are used to measure the reputation value. All nodes on the routing path can monitor the collusive behaviors and increase bad reputation for the collusive nodes. In summary, our proposed mechanism has the following contributions (1) To mitigate unfairness, three factors are used to achieve objective reputation value: Node degree, past routing behaviors and residual energy, (2) The neighbor node is responsible for punishment on selfishness of source node, (3) Other nodes on the routing path can increase bad reputation for neighbor node if no validation for the selfishness of the source node. Thus, collusive behaviors are not attractive and (4) The performance of ACFRI is analyzed in comparison with existing mechanisms.

ASSUMPTION AND MOTIVATION

Assumption: All nodes are rational in the network and desire to get forwarding services from other nodes. Some selfish node may refuse cooperation because of its limited resources. The unique identification can be guaranteed (Kargl *et al*., 2006). Fake or mock identification problem is not considered in this study. Meanwhile, mobility is out of scope in sensor networks.

Node degree represents the numbers of neighbors in 1-hop. A connection from originated node to destination node by immediate nodes' relaying is called flow. 1-hop topology information is exchanged in 1-hop neighborhood so that the information of neighbor in 2-hops is available.

Each node operates in a promiscuous mode: Listen to every packet sent by its 1-hop neighbors. Thus, a node will not miss any packet, even if it is not destined for the node. A node keeps track of the total number of packets that each neighbor has received while observing the abnormal behaviors that its neighbors exhibit, e.g., packet drop.

Motivation: To identify and punish selfish behaviors, there are two steps in the SORI mechanism (He *et al*., 2006). First, each node calculates the reputation value of its neighbors based on the monitoring data, including packets transmitted and forwarded. Second, each node exchanges reputation information only with their neighbors. By two steps, each node can judge when to cooperate and a node with low reputation will be punished by all of its neighbors (who share the reputation information about its misbehavior). However, we observe that there are three obstacles for SORI to work in wireless *ad hoc* sensor networks:

- **Unfair reputation for node with fewer neighbors:** As shown in Fig. 1a, edge node m and n never get chance to improve their reputation in SORI mechanism, since no node will request them to forward packets. Thus, it is inevitable that both m and n will be punished by neighbors after they transmit some packets. But they do not intend to be selfish. Moreover, there are many nodes with only one or two neighbors in real deployment environment which must be covered by the incentive mechanism
- **Unfair reputation only based on the past behaviors:** In SORI, if a node sends many packets but its neighbors have few activities (transmission), this node does not have chances to forward packets and will lose progressively its reputation and, eventually, it will be treated as selfish. Thus, the past behavior cannot always indicate future behavior. We need consider the left capability of each node that can be used to improve its reputation
- **No countermeasures to prevent collusion:** If u and v are collusive nodes in Fig. 1b, u can send all data to x without reputation validation which is the same for v sending packets to y. SORI only depends on 1-hop neighbors' monitoring and neighbors can share the reputation information, collusion cannot be handled

In this study, ACFRI mechanism is proposed to enhance SORI mechanism and address these obstacles.

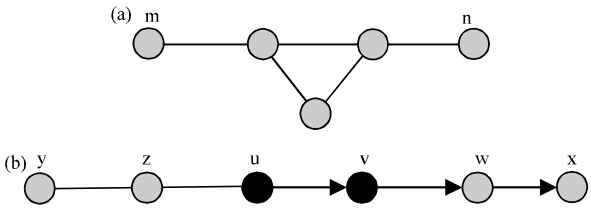

Fig. 1(a-b): Unfair and collusive samples in SORI mechanism (a) Both m and n are edge nodes and (b) u and v are collusive nodes

We use the node degree to describe the possibility that a node can improve its reputation. To address the unfairness problem, node degree, past routing behavior and residual energy are used to measure the reputation. To avoid collusion, routing monitoring is required for all nodes on the routing path. Each node keeps a node list for packet sending and forwarding. If there are collusive behaviors between source node and its neighbor, other nodes can detect the selfishness and punish the neighbor node. Therefore, collusive behavior is unattractive any more.

ANTI-COLLUSION AND FAIR REPUTATION-BASED INCENTIVE MECHANISM

Monitoring on routing behaviors: For any node u, routing monitoring is used to collect information about packet sending and forwarding behaviors. The packet header contains the identity information of the source node and forwarded nodes. Node u keeps track of two metrics for the node (denoted by x) that has sent and forwarded packets to u:

- **Fpu(x) (Forwarded Packet):** The total number of packets that node x have forwarded
- **SPu(x) (Sent Packet):** The total number of packets that node x have sent

Additionally, node u can observe the packet dropping by its neighbors which should be treated as a selfish behavior. DPu(x) (Drop Packet) represents the total number of packets that node x have received but drop, if $x \in N(u)$.

Here, the rejection or the modification on control packets is out of our scope and not covered. By monitoring the control packets, u knows the routing path of flow through itself. Thus, u can maintain a node list (denoted by NLu) which contains all nodes that have sent or forwarded data packets to u directly or indirectly. The two metrics are updated by the following rule. When node x transmits a packet to node u for forwarding, all nodes on the routing path between x and u is P, then SPu(x) = SPu(x)+1 and FPu(y) = FPu(y)+1 for $\forall y \in P$.

Residual energy model: There are two parts of energy consumption for sensor nodes: Collect target information and transmit it to sink nodes. In this study, we only focus on the energy consumption of information transmission. A sensor node can be in one of the four stats (Mahfoudh and Minet, 2008). Transmit, Receive, Idle or Sleep. The energy consumptions for each state are Et, Er, Ei and Es. Es is too small to be considered. Idle is the normal state if no activities happen. Our energy model is designed to evaluate the consumption in the packet forwarding activities: Transmit and Receive.

Since, every node cannot trust the residual energy information in the HELLO message from its neighbors, we propose a simplified energy model to evaluate the residual energy. Assume that all nodes transmit the packet with the same energy Et and receive the packet with the same energy Er. Thus, the source node costs Et and the relaying node costs Er+Et, including receiving and forwarding.

Let Et = e and Er = $\alpha \times e$, where $\alpha \leq 1$ (Mahfoudh and Minet, 2008). All nodes are initially equipped with the energy E = M×e for data transmission, where M is a non-zero integer. The residual energy ratio of node x evaluated by u (denoted by REu(x)) can be used to describe the future capacity for packet forwarding:

$$RE_u(x) = 1 - \frac{SP_u(x) \times E_t + FP_u(x) \times (E_r + E_t)}{M \times e} = 1 - \frac{SP_u(x) + FP_u(x) \times (\alpha + 1)}{M} \quad (1)$$

Objective reputation: Based on the monitoring data on routing packet passing through u, u can build a record of the reputation for every source node of the packet. To address the collusion problem, the reputation value only takes account of the monitoring data on node u, instead of all 1-hop neighbors in SORI:

- Given FPu(x) and SPu(x), node u can create a record called local evaluation record (denoted by LERu(x)), for the past routing behaviors of node x. The first situation occurs if $x \in N(u)$, whereas the second situation occurs if $x \notin N(u)$:

$$LER_u(x) = \begin{cases} \dfrac{FP_u(x)}{FP_u(x) + SP_u(x) + DP_u(x)} \\ \dfrac{FP_u(x)}{FP_u(x) + SP_u(x)} \end{cases} \quad (2)$$

- For $x \in N(u)$, node u can create a record called packet drop rate (denoted by PDRu(x)), for the past dropping behaviors of node x:

$$PDR_u(x) = \frac{DP_u(x)}{FP_u(x) + SP_u(x) + DP_u(x)} \quad (3)$$

- Node u calculate the overall evaluation record of x (denoted by OERu(x)), by combining the record for

past routing behavior and the residual energy ratio for future capacity

- If x∈N(u), the residual energy need consider the PDR to evaluate the optional activities in the future. For example, if a node drops all packets from others, its residual energy cannot be used to evaluate its future capability for cooperation. Thus, (1-PDRu(x)) is weight for the REu(x)
- If x∉N(u) u cannot observe all x's behaviors. Thus, the evaluated Reu(x) is larger than the real residual energy. To reduce the gap, (1-σ)×REu(x) is used to evaluate the real residual energy, where σ is the selfishness tolerance threshold discussed in next section:

$$OER_u(x) = \begin{cases} LER_u(x) + (1 - PDR_u(x)) \times RE_u(x) \\ LER_u(x) + (1 - \sigma) \times RE_u(x) \end{cases} \quad (4)$$

Punishment: With the reputation value OERu(x) obtained, punishment is discussed in this section. Let N(x) represents all neighbor nodes in the transmission range of x (excluding x itself) and node degree d(x) = |N(x)| represents the number of nodes in the transmission range of node x. To address collusion problem, there are two scenarios for punishment:

- If x∉N(u), we employ the similar punishment method in SORI. If OERu(x) is lower than a selfishness tolerance threshold, node u takes punishment action by dropping the packets with possibility pu(x) originated from x:

$$p_u(x) = \begin{cases} 1 - \frac{\sigma}{d(x)}, \text{if } (q > \frac{\sigma}{d(x)}) \\ 0, \text{otherwise} \end{cases} \quad (5)$$

- If $x \notin N(u)$, is on the routing path of the connection generated by x and is not the destination node. Let v∈N(x) is the first forwarding node for the connection. If OERu(x) is lower than a selfishness tolerance threshold, node u takes punishment action by increase bad reputation for node v with possibility pu(x), e.g., SPu(v) = SPu(v)+1. Since, u cannot monitor all routing behaviors of x, x is treated a node with d(x) = 1 and assigned with the selfishness tolerance:

$$p_u(x) = \begin{cases} q - \sigma, \text{if } (q > \sigma) \\ 0, \text{otherwise} \end{cases} \quad (6)$$

where, q = 1-OERu(x) and 0<σ<1 is the selfishness tolerance threshold to avoid punishment on the possible packet collision.

In summary, the trustworthy objective quantification of reputation is achieved due to the following factors:

- The records from monitoring routing behaviors only depend on the node itself. Thus, it brings no benefit to impersonate a node with a good reputation or broadcast bad reputation for other nodes
- The reputation of a node is measured by the routing record and the residual energy. So, the punishment can be mitigated for the nodes with ability to increase their reputation in the future, if they have sufficient energy
- The monitoring is operated by all nodes involving in the connection. Each selfish node is only punished by its neighbors. However, if a neighbor node colludes with the source node and forwards packets without reputation validation, the bad reputation for this neighbor node will be increased by other nodes on the routing path. Without collusion from neighbors, collusive behaviors among two unconnected nodes cannot get any benefit. Therefore, the collusive behaviors are not attractive any more
- The selfishness tolerance:

$$\left(\frac{\sigma}{d(x)}\right)$$

is employed for both probable transmission collision (Huang *et al*., 2007) and fairness for nodes with lower degree in the network. Since, a node with lower degree gets fewer chances to increase reputation by forwarding packets, it gets a higher selfishness tolerance

SIMULATION AND EVALUATION

Here, ACFRI is compared with SORI under various settings. The simulations aim at demonstrating the efficiency, fairness and anti-collusion in our mechanism.

Simulation setting: To evaluate the performance of ACFRI, we modify the original DSR (Johnson *et al*., 1999) implementation in NS-2 (NS Developing Group, 1995) to support our energy evaluation model. Each node is turned off when the number of sending and forwarding packets reaches the maximum value M = 1000. We use IEEE 802.11

Table 1: Simulation parameters

Parameters	Settings
Radio transmission rate (m)	250
Transmission data rate (Mbits sec^{-1})	2
Data rate of CBR connection (packet sec^{-1})	1
Antenna height (m)	1.5
No. of nodes	50
Maximum packets M	1000
Simulation time (sec)	1000
σ in SORI	0.1
Simulation area (m^2)	670×670

(Brenner, 1997). Distributed Coordination Function (DCF) as the medium access control layer protocol (Kumar *et al.*, 2006). The physical layer model is the two-ray propagation model. We use the static node deployment for the sensor network. The constant bit rate (CBR) traffic model is employed for all the connections. Other simulation parameters are listed in Table 1.

For each simulation, N_{conn} connections are randomly generated and a new connection will be generated after an existing connection is terminated. Each simulation is executed for 1000 sec and each connection lasts for 10 sec.

For selfishness simulation, 5 among 50 nodes are randomly selected and assigned as selfish nodes. Two types of selfish behavior are covered (1) Dropping all packets from other nodes and (2) Two neighbor nodes collude with each other in forwarding packet without reputation validation.

Performance evaluation: Here, we use network throughput to measure efficiency and a fairness index to measure fairness. Let t denotes the simulation time (t = 1000) and pr(u) denotes the number of packets correctly received by node u. Nw and Ns denote the set of well-behaving nodes and selfish nodes, respectively. The average throughput of well-behaving nodes (denoted by Tw) and selfish nodes (denoted by Ts) is calculated as follows:

$$T_w = \frac{\sum_{u \in Nw} pr(u)}{|N_w| \times t}, T_s = \frac{\sum_{u \in Ns} pr(u)}{|N_s| \times t} \quad (7)$$

The fairness index $\lambda \in [0; 1]$ is calculated as follows (Jain *et al.*, 1984):

$$\lambda = \frac{(\sum_{i=1}^{n} x_i)^2}{(n \times \sum_{i=1}^{n} x_i^2)} \quad (8)$$

where, n is number of the connections, $1 \le i \le n$ and xi is the throughput of ith connection. High λ means better fairness among the well-behaving nodes.

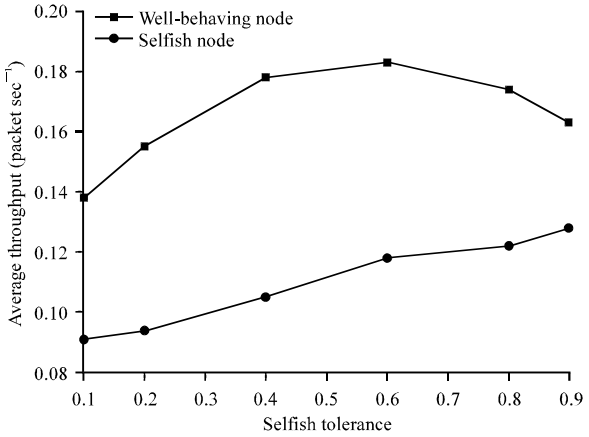

Fig. 2: Impact of selfishness tolerance σ

Impact of selfishness tolerance: Before experiments, we have to figure out how to tune the selfishness tolerance ¾ in Eq. 4-6. When σ = 0, the punishment is tough by dropping almost 100% packets from both selfish nodes and well-behaving nodes with d = 1. Furthermore, a dropping action may be occasionally triggered by collision, rather than selfish behavior. Thus, if σ = 0, two neighbors may keep increasing the dropping probability and consequently fall into a retaliation situation. A proper setting for σ can help well-behaving nodes mitigate these situations and increase the robustness of network stability. Contrastively, let σ = 1 will connive selfish behaviors with no punishment. This part is to evaluate the impact on the throughput by selfishness tolerance σ.

For each simulation, we set N_{conn} = 10. The average node degree is d = 4. Figure 2 shows that a small selfish tolerance (¾ = 0:1) degrades both well-behaving and selfish nodes, because even sending 10 packet in a single connection will cause dropping action due to the small tolerance. In contrast, a large selfish tolerance (σ = 0.9) increase the performance of selfish nodes without any benefit for well-behaving nodes, since even selfish nodes with few energy are not punished with 100% possibility of dropping action (p<80%). So, there is a trade-off between the throughput of a selfish node and the robustness of network stability. The maximum throughput gap between well-behaving nodes and selfish nodes is achieved with $\sigma \in (0.2, 0.6)$. We choose σ = 0.4 in the following simulations.

Fairness: To evaluate the fairness for all well-behaving nodes, we do simulation in two mechanisms: One is our proposed ACFRI and the other one is SORI. For each simulation, we set N_{conn} = 10. As shown in Fig. 3, we observe that a better fairness is achieved in ACFRI than

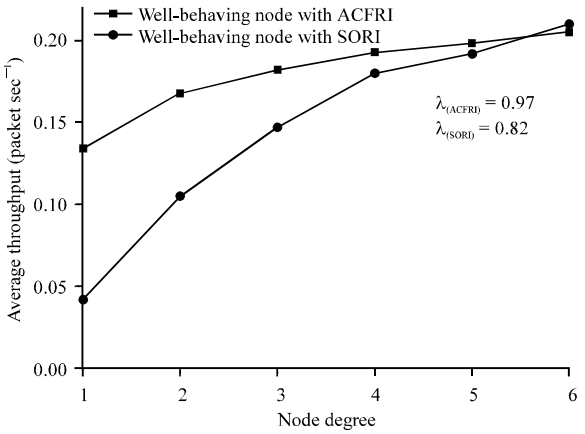

Fig. 3: Fairness: Throughput vs. node degree d for ACFRI and SORI

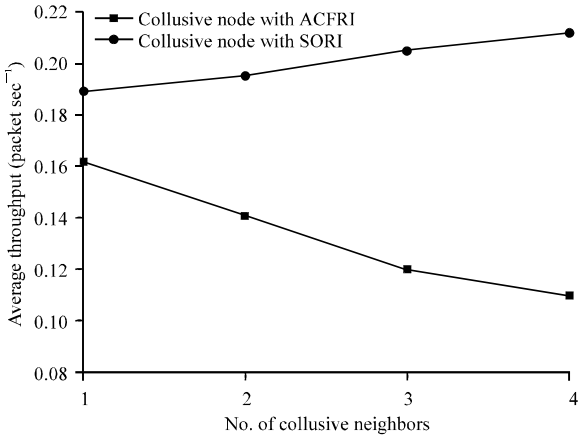

Fig. 4: Collusion impact: Throughput vs. No. of collusive nodes for ACFRI and SORI

SORI (λ_{ACFRI} = 0.97 and λ_{SORI} = 0.82). Note that the fairness index gap 0.15 is remarkable for Jain's measure rule (Jain *et al*., 1984).

The throughput is unequal for the nodes with low degree in SORI. For the nodes with only one neighbor (d = 1), no chance of forwarding packets is available. Thus, they are treated as selfish nodes that drop all packets (not destined to themselves). Node with higher degree achieve better throughput since they get more chances to earn the reputation by forwarding packets. Different from SORI, ACFRI enhances fairness by the residual energy evaluation and node degree: the higher selfishness tolerance is for the nodes with more residual energy and lower node degree. So, it can be observed in Fig. 3 that the throughput gap is small for nodes with different degrees in ACFRI. Meanwhile, we observe that SORI node with d = 6 performs better than ACFRI node, since that the node with highest degree deserves high reputation in SORI.

Anti-collusion: This experiment is to illustrate the impact of collusive behaviors in the two mechanisms. For each simulation, we set N_{conn} = 10. As mentioned in the previous section, only the collusion between neighbors can get benefit in both ACFRI and SORI mechanisms. In this experiment, let a node u with four neighbors is elected to be the source of collusion. We use the number of collusive nodes in u's neighborhood to represent the extent of collusion. Here collusion means no reputation validation and increasing throughput for each other.

As shown in Fig. 4, the performances of collusive nodes are totally different. In SORI, only the neighbor is involved in the punishment on the selfishness of source nodes. When only one neighbor v colludes with u, u and v can send packets through each other without validation. Thus, u and v can get benefits on the throughput. Figure 4 shows that when more neighbors are involved in collusion, more benefit on throughput is achieved. In contrast, in ACFRI, collusion is suppressed effectively. Besides the neighbor v, other nodes on the routing path observe the selfishness too. They will increase the bad reputation for v if no punishment is executed on u. When a node colludes with more neighbors, it will be assigned with more collusive tasks, i.e., forwarding neighbor's packets without validation. Under this situation, the increased bad reputation will be a big obstacle for the throughput of neighbors and cannot be ignored. Therefore, the throughput is decreased for the collusive nodes in ACFRI.

Overhead: Here, the overhead incurred by our mechanism is evaluated by comparing to SORI and the original DSR protocol. The throughput under different number of connections is used to measure the overhead. For each simulation with different number of connections, we set the pairs (N_{conns}, M) in {(10, 1000), (20, 2000), (30, 3000), (40, 4000), (50, 5000)}. No reputation mechanism is employed in the original DSR.

Figure 5 plots the average throughput from 10-50 connections. Without any incentive mechanism, the selfish nodes are treated in the same way as the well-behaving nodes in the original DSR protocol. It can be observed that the throughput of well-behaving nodes under both ACFRI and SORI mechanisms is reduced by comparing to original DSR. Here, by overhead, we mean this throughput reduction. For both incentive mechanisms, packet collision may cause mis-calculation of the reputation measure, leading to improper punishment on the well-behaving nodes (He *et al*., 2006). Note that the overhead incurred by both incentive

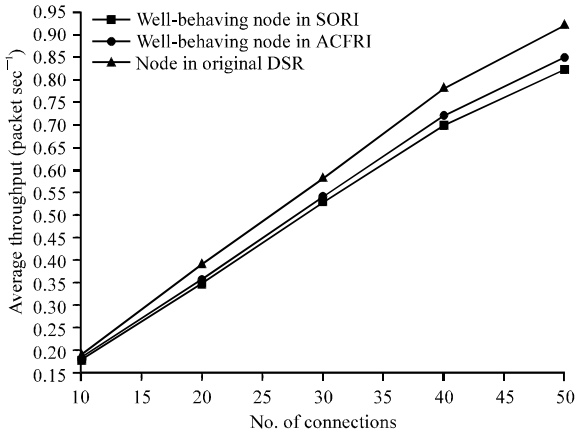

Fig. 5: Overhead: Throughput vs. No. of connections for ACFRI and SORI

mechanisms is about 10%. The overhead in ACFRI stems from the monitoring of all nodes on the routing path which is vital for anti-collusion. The source nodes are assigned with low reputation in the simulation initial phase in SORI, since they haven't get any chance to forward packets yet. ACFRI can reduce this error with residual energy evaluation. Thus, the incurred overhead by SORI is a little larger than that of ACFRI, because the proposed residual energy model can reduce the improper punishment in SORI.

CONCLUSION

In this study, we propose an Anti-Collusion and Fair Reputation-based Incentive (ACFRI) mechanism to encourage cooperation and achieve fairness for all the nodes in wireless *ad hoc* sensor networks. A simplified energy model is introduced based on the routing monitoring. To enhance the fairness, the reputation value in ACFRI is not only based on the past behaviors but also the evaluated residual energy of each node. The punishment on selfishness is executed by the neighbor of the selfish node. To suppress collusion, all nodes on the routing path are involved in routing monitoring and punish the neighbor if no punishment on the selfish behaviors of the source node. The experimental results show that in our proposed mechanism, selfish behaviors are punished through smaller throughput. Fairness is enhanced for all well-behaving nodes and collusion is punished effectively, under 10% throughput overhead.

REFERENCES

Brenner, P., 1997. A technical tutorial on the IEEE 802.11 protocol. BreezeCOM Wireless Communications. http://courses.csail.mit.edu/6.885/spring06/papers/Brenner-printable.pdf

Cerpa, A., J. Elson, D. Estrin, L. Girod, M. Hamilton and J. Zhao, 2001. Habitat monitoring: Application driver for wireless communications technology. ACM SIGCOMM Comput. Commun. Rev., 31: 20-41.

Felegyhazi, M., J.P. Hubaux and L. Buttyan, 2006. Nash equilibria of packet forwarding strategies in wireless *ad hoc* networks. IEEE Trans. Mobile Comput., 5: 463-476.

He, Q., D. Wu and P. Khosla, 2006. A secure incentive architecture for *ad hoc* networks. Wirel. Comm. Mob. Comput., 6: 333-346.

Huang, X., J. Wang and Y. Fang, 2007. Achieving maximum flow in interference-aware wireless sensor networks with smart antennas. *Ad Hoc* Network, 5: 885-896.

Jain, R., D. Chiu and W. Hawe, 1984. A quantitative measure of fairness and discrimination for resource allocation in shared computer systems. DEC Technical Report TR-301, September 1984. http://www.cse.wustl.edu/~jain/papers/fairness.htm

Johnson, D.B., D.A. Maltz and J. Broch, 1999. DSR: The Dynamic Source Routing Protocol for Multihop Wireless *ad hoc* Networks. In: In *ad hoc* Networking, Perkins, C.E. (Ed.). Addison-Wesley, USA., pp: 139-172.

Kargl, F., S. Schlott and M. Weber, 2006. Identification in *ad hoc* networks. Proceedings of the 39th Annual Hawaii International Conference on System Sciences, January 4-7, 2006, Hawaii, USA., pp: 233c.

Kremens, R., A. Gallagher and A. Seema, 2002. Low cost autonomous field-deployable environment sensors. Proceedings of the Conference Report Unattended Radiation Sensor Systems for Remote Applications, April 15-17, 2002, Washington, DC., USA., pp: 190-199.

Kumar, S., V.S. Raghavan and J. Deng, 2006. Medium access control protocols for ad-hoc wireless networks: A survey. *Ad hoc* Networks J., 4: 326-358.

Mahfoudh, S. and P. Minet, 2008. Survey of energy efficient strategies in wireless *ad hoc* and sensor networks. Proceedings of the 7th International Conference on Networking, April 13-18, 2008, Cancun, Mexico, pp: 1-7.

NS Developing Group, 1995. The network simulator-ns-2. http://www.isi.edu/nsnam/ns/.

Rogers, A., E. David and N.R. Jennings, 2005. Self-organized routing for wireless microsensor networks. IEEE Trans. Sys. Man Cybern. Part A: Syst. Hum., 35: 349-359.

Zhong, S. and F. Wu, 2007. On designing collusion-resistant routing schemes for non-cooperative wireless *ad hoc* networks. Proceedings of the 13th Annual ACM International Conference on Mobile Computing and Networking, September 9-14, 2007, Montreal, Canada, pp: 278-289.