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 8 (5): 757-763, 2009
ISSN 1812-5638

Cooperation Enforcement Among Selfish Nodes in Ad Hoc Networks under Noise

[1]Dongbin Wang, [1]Mingzeng Hu, [2]Hui Zhi and [1]Jianwei Ye
[1]Research Center of Computer Network and Information Security Technology,
Harbin Institute of Technology, Harbin, 150001, People's Republic of China
[2]TravelSky Technology Limited, Beijing, 100190, People's Republic of China

Abstract: In ad hoc networks, the source node can take help of the intermediate nodes to communicate with the destination node by relaying the packets hop by hop. But nodes are constrained with limited resources, so nodes tend to be selfish and cooperative behaviour in forwarding packets for others can not be taken for granted. In the study, we present a two-player packet forwarding game under noise. An incentive-compatible condition under which the selfish one will be deterred from defection by the subsequent punishment and then turn to cooperate is analyzed. The impact of parameter settings of punishment strategy and isolation strategy on cooperation enforcement is discussed. The simulation results show that the proposed packet forwarding approach can effectively stimulate cooperation among selfish nodes under noise.

Key words: Packet forwarding, game theory, punishment, dropping packet detection

INTRODUCTION

A mobile ad hoc network is a self-configuring network that is formed automatically via wireless links by a collection of mobile nodes without the help of a fixed infrastructure or centralized management. Each node in mobile ad hoc networks can communicate directly with other nodes in its radio communication range. If the destination node is not within the transmission range of the source node, the source node takes help of the intermediate nodes to communicate with the destination node by relaying the messages hop by hop.

The mutual cooperation and contribution of packet forwarding among the nodes in the network is needed. However, since the mobile nodes in this network are constrained with limited resources, such as CPU, battery, channel bandwidth and etc, some nodes in the network might not be willing to cooperate for the packet transmission, in order to save their resources. Each node has the goal to maximize its own benefits by enjoying network services and at the same time minimizing its contribution, so nodes may tend to be selfish. A selfish node does not intend to directly damage other nodes, but is unwilling to spend battery life, CPU cycles, or available network bandwidth to forward packets not of direct interest to it, even though it expects others to forward packets on its behalf. Consequently, cooperative behaviour, such as unconditionally forwarding packets for others, cannot be taken for granted. The selfish behaviour can significantly damage network performance (Marti *et al*., 2000).

Recently, many solutions have been proposed to give nodes incentive to cooperate among selfish nodes. Cooperation solely based on the self-interest of the nodes can in theory exist, but in practice, the conditions of such cooperation are never satisfied (Felegyhazi *et al*., 2006). Without introducing any enforcement strategy, it is impossible to enforce the nodes to cooperate. The proposed works mainly focus on pricing-based, reputation system, VCG-based, game theoretic analysis, etc. However one major drawback of the existing strategy on cooperation in ad hoc networks lies in that perfect observation have been assumed and the effect of noise in real environment has not been considered. In ad hoc networks, even when a node has decided to forward a packet for another node, the packet may still be dropped due to link breakage or channel errors. Therefore, how to stimulate cooperation and analyze the efficiency of possible strategies in the scenarios with noise and imperfect observation are still open problems for ad hoc networks.

In the study, we model the interactions among nodes as packet forwarding game under noise and propose the cooperation strategy to stimulate the packet forwarding among selfish nodes and maximize the expected payoff of selfish nodes by using game theoretical analysis. Then the roles of the punishment and isolation in the cooperation enforcement under noise are investigated.

Corresponding Author: Dongbin Wang, Chaoyang District, Yumin Road, Jia No. 3,
National Computer Network Emergency Response Technical Team, A502, Beijing City, 100029, China
Tel: +86-010-82990826 Fax: +86-010-82990827

The simulation results illustrate that the proposed packet forwarding approach can stimulate the cooperation in ad hoc networks under noise.

STATE OF THE ART

One way to enforce cooperation among selfish nodes is to use payment-based schemes, in which a selfish node will forward packets for other nodes only if it can get some payment from those requesters as compensation. For example, a cooperation stimulation approach was proposed by Buttyan and Hubaux (2003) by using a virtual currency called nuglets as payment for packet forwarding, which requires tamper-proof hardware in each node. Another payment-based system, SPRITE (Zhong *et al*., 2003), released the requirement of tamper-proof hardware, but required some online central banking service trusted by all nodes. Although, these schemes can effectively stimulate cooperation among selfish nodes, the requirement of tamper-proof hardware or central billing services greatly limits their potential applications.

Another way to enforce cooperation among selfish nodes is to use reputation-based schemes. In (Marti *et al*., 2000), each node launched a watchdog to monitor its neighbors' packet forwarding activities and to make sure that these neighbors had forwarded the packets according to its requests. Pathrater was used to prevent misbehaving nodes from being on the selected routes when performing route discovery. CORE (Michiardi and Molva, 2002) and CONFIDANT (Buchegger and Boudec, 2002) systems were proposed to enforce cooperation among selfish nodes which aim at detecting and isolating misbehaving node and thus making it unattractive to deny cooperation. Moreover, ARCS was proposed in (Yu and Liu, 2005) to further defend against various attacks, while providing the incentives for cooperation. The above reputation-based schemes can avoid routing packets through the misbehaving nodes which will be contrarily benefit the misbehaving nodes and can not deter the dropping packets behaviour.

Ad hoc VCG was a generalized second best sealed bid auction mechanism and achieves cost-efficiency and truthfulness in (Anderegg and Eidenbenz, 2003). An intermediate node's VCG-payment on the shortest path from a source to a destination was equal to its own declared cost for forwarding a packet plus a premium, which was defined to be the difference of the overall cost of the shortest path that did not contain it as an intermediate node and that of the shortest path with it. VCG mechanism was to make cheating unattractive by making payments as high as a node could possibly expect to obtain by cheating. But VCG has the drawback of budget imbalance and overpayment. Based on VCG, Zhong *et al.* (2005) proposed Corsac, which integrates VCG and cryptographic technique to solve the combined problem of routing and packet forwarding. OURS (Wang *et al*., 2006) had much smaller overpayments than VCG-based solutions.

Besides that, some progress has also been made towards mathematical analysis of cooperation in autonomous ad hoc networks using game theory. Srinivasan *et al.* (2003) provided a mathematical framework for cooperation in ad hoc networks, which focused on the energy-efficient aspects of cooperation. Michiardi and Molva (2003) studied the cooperation among selfish nodes in a cooperative game theoretic framework. Felegyhazi *et al.* (2006) defined a game model and identified the conditions under which cooperation strategies can form equilibrium. Altman *et al.* (2004) studied the packet forwarding problem using a non-cooperative game theoretic framework. Further, Trust modeling and evaluation framework (Sun *et al*., 2006a, b) was extensively studied to enhance cooperation in autonomous distributed networks, which utilized trust (or belief) metrics to assist decision-making in autonomous networks through trust recommendation and propagation. The study of selfish behaviour in ad hoc networks using game theory had also been addressed (Urpi *et al*., 2003; Crowcroft *et al*., 2003). Most of these schemes focus on selfish behaviour and most of them study cooperation enforcement under a repeated game framework.

Present study also falls in the category of cooperation stimulation analysis for autonomous ad hoc networks under a game-theoretic framework. However, there are several major differences which distinguish our work from the existing work. First, we study this problem under more realistic and more challenging scenarios, where the communication medium is error prone and the packet forwarding is not perfect. Second, the detection of misbehaviour under noisy is different from under perfect environment. Third, not only isolation but punishment is introduced in the cooperation enforcement strategy.

REPEATED PACKET FORWARDING GAME

System description and design challenges: In general, when a node wants to send a packet to a certain destination, the requester notifies other nodes in the network that it wants to find a route to a certain destination. Other nodes in the network will make their decisions on whether they will agree to be on the discovered route. Then the requester will determine which route should be used. The sender will get some payoffs if the packets are successfully delivered to the destination and the forwarding effort of relay nodes will also introduce certain costs. In the study, packet forwarding, the most basic networking function is focused on and how to stimulate cooperation is investigated among the intermediate nodes under noisy scenarios.

All nodes are assumed selfish and rational, their objective are to maximize their own payoff, not to cause damage to other nodes. Present goal is not to enforce all of the users to act in a fully cooperative fashion, which has been shown in (Felegyhazi *et al*., 2006) to not be achievable in most situations. Instead, present goal is to stimulate cooperation among nodes as much as possible through playing conditional reciprocal altruism. No tamper-proof hardware or central banking service is assumed.

In the study, some necessary traffic monitoring mechanisms, such as those described in (Marti *et al*., 2000; Buchegger and Boudec, 2002; Michiardi and Molva, 2002), will be launched by each node to keep tracking of its neighbours actions. In general, not all packet forwarding decisions can be perfectly executed. For example, when a node has decided to help another node to forward a packet, the packet may still be dropped due to link breakage or the transmission may fail due to channel errors. In this study, those factors that may cause decision execution error are referred as noise, which include environmental unpredictability and system uncertainty, channel noise, mobility, etc.

Packet forwarding game model: An autonomous mobile ad hoc network with a finite population of users, denoted by N, is considered. Every node is involved in sending its own packets and also forwarding neighbours' packets. We use a discrete model of time where time is divided into slots. A node is assumed to send one packet and forward several packets within one time slot (round). In order to formally analyze cooperation in such networks, we model the interactions among nodes as packet forwarding game and incorporate noise into the game. We study a simple yet illuminating two-player packet forwarding game between node i and node j:

- **Cost:** For the player i, transmitting a packet either for itself or for the others j, incurs cost c_i. Let n_{ij} be the number of packets that player i is requested to forward for node j during one slot
- **Gain:** For each selfish player i, if a packet originated from it can be successfully delivered to its destination, it can get gain g_i, where $g_i>c_i$. Node i will transmit one packet during one time slot
- **Imperfect transmission:** Due to noise, with probability q_i each node can successfully transmit packet to its neighbour

Table 1: The strategies and payoff in the repeated forwarding game

Strategy	(T,F,S)	u_i	Payoff
Cooperation	(1,1,1)	$u_i^t(C)$	$g \cdot q^{l_i} - c - c \cdot n_{ij}$
Defection	(1,0,1)	$u_i^t(D)$	$g \cdot q^{l_i} - c$
Isolation	(0,0,0)	$u_i^t(I)$	0
Punishment	(0,1,0)	$u_i^t(P)$	$-c \cdot n_{ij}$

- **Payoff:** For two-player game, we can model the players' payoff functions in slot. Let T be whether node i transmit one packet, S be whether node j cooperate to forward the packet for node i and F be whether node i forward packets from node j

To simplify the illustration, we assume that $g = g_i$, $c = c_i$ and $q = q_i$ for $i \in n$. Similar to (Lu *et al*., 2008), the payoff of node i during the slot t is the following:

$$u_i^t = T \cdot (S \cdot g \cdot q^{l_i} - c) - F \cdot c \cdot n_{ij} \tag{1}$$

where, u_i is the payoff of node i and l_i is the hops number from node i to the destination in time slot t. Once a node's defection is detected, it will be isolated and punished for several rounds before it can transmit its following packets. If it is isolated, it can neither transmit nor forward packet for other node. And if it is punished, it can not send its own packets and can forward packets for others. The behaviour strategies and payoff are in Table 1.

If the game will be played for an infinite duration our two-player packet forwarding game is similar to the setting of the prisoner's dilemma game in (Osborne and Rubinste, 1994). When the game will be played for an infinite duration, the overall payoff of node i is:

$$U_i = \sum_{t=0}^{\infty} u_i^t \tag{2}$$

The objective of every selfish node in the forwarding game is to maximize U_i. If the gain of transmitting packet is more than the cost of forwarding packets for others, the selfishness will choose to cooperation, but if not, the selfish node may choose to defect to max its payoff.

Nash equilibrium in packet forwarding game: An intuitive strategy for enforcing cooperation in an ad hoc routing game is to isolate the defective node by ensuring that all the node's neighbours play defection in games against it, such as CORE (Michiardi and Molva, 2002). However, being isolated does not expend resources unlike forwarding, so it can get more short-term payoff by defecting than by cooperating. Isolating the defective node maybe encourages the defection and is not always a rational strategy for a node. In the repeated packet forwarding game, if the selfish finds defection can bring more payoff than cooperation, it will continue to defect. Only isolation does not guarantee cooperation among rational nodes, so punishment is introduced into the cooperation enforcement game. Once a node is detected as defective node, it will be punished and isolate for several rounds (time slots). In order to deter the defection, the payoff of the cooperation must be more than the sum on the defection, isolation and punishment. That is:

$$\sum_{k=t}^{t=p+r+1} u_i^k(C) > u_i^t(D) + p \cdot u_i^t(I) + r \cdot u_i^t(P) \tag{3}$$

where, p and r are the number of rounds (time slots) in isolated strategy and in punishment strategy, respectively. So, we can get:

$$\frac{p+r}{p+1} > \frac{|u_i^t(P)|}{u_i^t(D)} = \frac{c \cdot n_{ij}}{g \cdot q^{l_i}} \tag{4}$$

If Eq. 4 is held, Nash Equilibrium, in which every nodes selects the best response strategy to the other nodes' strategies, is reached and no node can improve its utility by unilaterally changing its own packet forward strategy. Briefly, no player can profitably deviate, given the actions of the other players, so the cooperation can be guaranteed.

Theorem 1: In the proposed packet forwarding game, when the punishment rounds increase, the cooperation among selfish nodes will be encouraged.

Proof: Let f(r, p) be the left side of Eq. 4. And we have:

$$f(r,p) = \frac{p+r}{p+1} \tag{5}$$

Then we can have the partial of f with respect to r:

$$\frac{\partial f}{\partial r} = \frac{1}{p+1} > 0 \tag{6}$$

If r increases, f(r, p)will increase too and Eq. 4 will be easier to be filled. So the cooperation will be encouraged if the punishment round increases.

Theorem 2: In the proposed packet forwarding game, when the punishment round is equal to 0, if the isolation round increase, the cooperation among selfish nodes will be encouraged. When the punishment round is more than 1, if the isolation round increase, the cooperation among selfish nodes will be discouraged.

Proof: We have the partial of f with respect to p:

$$\frac{\partial f}{\partial p} = \frac{1-r}{(p+1)^2} \tag{7}$$

If r = 0, we can have ∂f/∂p>0. If p increases, f(r, p) will increase, Eq. 4 will be easier to be filled and the cooperation among selfish nodes will be encouraged.

If r>1, we can have ∂f/∂p<0. If p increases, f(r, p) will decrease, Eq. 4 will be harder to be filled and the cooperation will be discouraged.

SIMULATION AND ANALYSIS

A set of simulations were investigate to evaluate the proposed cooperation enforcement strategies under noise. A random network with 50 nodes was generated. The nodes were randomly distributed in the rectangular area of 1000×1000 m. Each node may either be static or move according to the random way point model in which a node started at a random position randomly, chose a new location and moved toward the new location then randomly moved again after a pause time duration which was set 100 sec in the simulations. In the random network, the maximum distance between which two nodes can directly communicate with each other was set to be 250 m. IEEE 802.11 DCF was adopted as the MAC layer protocol and DSR was used as the route protocol in the simulations. For each simulation, each node randomly picked another node as the destination to sended packets with the packet interval time slot, 1sec. And Watchdog was used to observe the forwarding behaviour and Catch (Mahajan *et al.*, 2005) was used to isolate the defective node. Let g = 1 and c = 0.1 in the simulations. We defined the effective delivery ratio as the ration of the number of packets successfully delivered to the destination, to the number of packets generated to be sent.

Simulation studies with different ratio of selfish nodes: We first focused the simulation studies on different ratio of selfish nodes scenarios in ad hoc networks. For comparison, the nodes would be classified as selfish node and cooperative node. The selfish nodes would only send to their own packets but drop all others' packets. The cooperative nodes would forward the packets for others.

Figure 1 shows the effective delivery ratio with different selfish ratio ranging from 0 to 100%. First, we could see that the ad hoc network had a very high effective delivery ratio when the selfish ratio was zero. But, when the number of selfish nodes increased, the effective delivery ratio without enforcement strategy, where p = 0 and r = 0, dropped dramatically from about

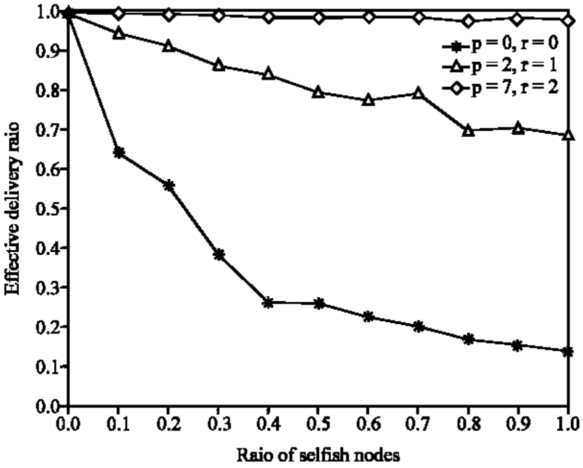

Fig. 1: Effective delivery ratio with different ratio of selfish nodes; the x-axis is the ratio of the selfish nodes and the y-axis is the effective delivery ratio

100 to about 13%. This was ease to understand: since there was no punishment and isolation strategy, the selfish nodes would not forward packets for others nodes to save the forwarding cost for other nodes and max their payoff. It was worth pointing out that, the packets will be successfully delivered, if the destination was within the source transmission range, which was the reason why the effective delivery ratio could reach about 13% when all the nodes were selfish.

Second, we could also see that effective delivery ratio increased a lot when the enforcement strategy existed where p ≠ 0 and r ≠ 0. More p and r were, more effective delivery ratio was. The ratio of selfish nodes varied from 0 to 100% and the effective delivery ratio dropped from about 100 to about 69% when p = 2 and r = 1. But, when p = 7 and r = 2, the effective delivery ratio was stable whatever the ratio of selfish nodes was. Even all the nodes are selfish, the effective delivery ratio still reached about 98%, which was very close to that in the scenario where all nodes cooperate. This was because if the nodes chose to be selfish to drop the packets from others, they would be punished and isolated in the ad hoc network. If the loss of punishment and isolation overwhelmed the benefit gained from the misbehaviour, the selfish would choose to cooperate.

The simulation resulted suggest that the ratio of selfish nodes influenced the effective delivery ratio and punishment and isolation played a very positive role in deterring the selfish nodes' misbehaviour and enforcing all the nodes to cooperate. Even when all the nodes were selfish, the effective delivery ratio still was very close to that in the scenario where there all nodes cooperated.

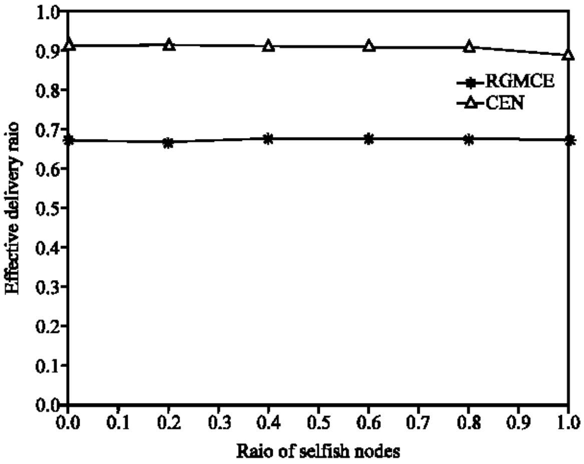

Fig. 2: Effective delivery ratio under noise; the x-axis is the ratio of the selfish nodes and the y-axis is the effective delivery ratio

Simulation studies under noise: Here, we investigated the performance of the proposed cooperation strategy under noise. The proposed cooperation enforcement strategy under noise, CEN in this study and the repeated-game modeling of cooperation enforcement strategy, RGMCE in Lu *et al.* (2008) were compared under noise. For each selfish node, the maximum allowable false positive probability ε was set to be 0.1% and the probability q that each node can successfully transmitted packet to its neighbour, was set to be 0.98 similar to Yu and Liu (2005).

Figure 2 shown the effective delivery ratio under noise. When p = 2 and r = 8. CEN and RGMCE could perform stably when the ratio of selfish nodes varied from 0 to 100% because both them used the punishment and isolation to deter the selfish behaviour. The packet dropping ratio after multi-hop forwarding due to noise was about 8% and the noise greatly affected the effective delivery ratio. The effective delivery ratio of RGMCE and CEN were about 67 and 90%, respectively. CEN outperformed RGMCE about 33% under noise. RGMCE did not consider the scenario under noise and could not distinguish the packet dropping due to noise with the packet dropping due to selfishness. The node which was detected to drop the forwarding packet due to noise would also be mistaken to defect and be punished and isolated right now in RGMCE and then the packets sent by these nodes would be dropped which caused the throughput and effective delivery ratio decreased. CEN investigated the scenario under noise in the ad hoc networks. If some packets dropping happened and is Bad(j) = 0, CEN would not punish and isolate the nodes

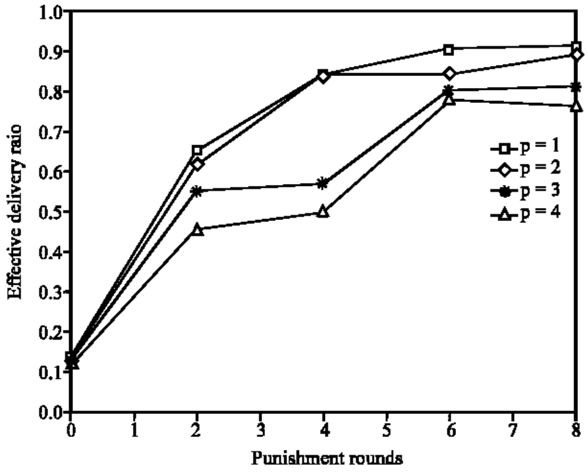

Fig. 3: Effective delivery ratio with different punishment rounds; the x-axis is the rounds of the punishment strategy and the y-axis is the effective delivery ratio

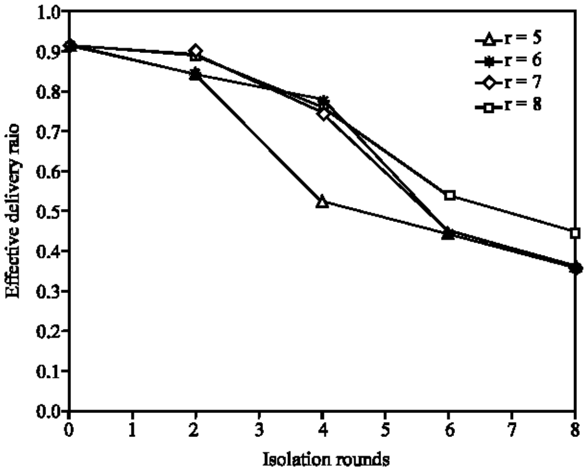

Fig. 4: Effective delivery ratio with different isolation rounds; the x-axis is the rounds of the isolation strategy and the y-axis is the effective delivery ratio

and watch the following behaviour of the nodes. Until is Bad(j) = 1, the punishment and isolation would be carried out.

Simulation studies with different punishment rounds: Now, we studied how the proposed punishment strategies could effectively stimulate the cooperation among selfish nodes under noise. We considered all the nodes were rational and selfish where all the nodes followed the cooperation strategy if Eq. 4 was held or the defection strategy if Eq. 4 was not held. Figure 3 showed the effective delivery ratio under various number of the punishment rounds. When the punishment round increased, the effective delivery ratio increased too, which coincided with Theorem 1. The effective delivery ratio was low and about 13%, when r was equal to 0. But when r increased to 8 and p was equal to 1, the effective delivery ratio increased rapidly and reached about 90%.

Figure 3 demonstrated that the punishment strategy played a very importantly positive role in the cooperation enforcement under noise and could effectively deter the selfish behaviour.

Simulation studies with different isolation rounds: Lastly, we investigated how the isolation strategy affected the effective delivery ratio among rational and selfish nodes under noise. In Fig. 4, the effective delivery ratio was about 90% when p, the isolation rounds was equal to 0. But when p increased, the effective delivery ratio decreased rapidly, which coincided with Theorem 2. Even when r = 8 and p = 8, the effective delivery ratio decreased to 45%. The isolation strategy played a negative role in the cooperation enforcement.

CONCLUSION

In this study, we have formally investigated the cooperation stimulation in ad hoc networks under noisy. Firstly, a simple yet illuminating repeated packet forwarding game is studied. A NASH equilibrium solution is derived and a rational and selfish node will cooperate to forward packets for other nodes only if the benefit of cooperation overwhelms the benefit of the defection and the punishment under noise. The simulation results show the proposed punishment strategy will affectively deter the defection of the selfish nodes and stimulate the cooperation among rational and selfish nodes, but the isolation strategy will encourage the misbehaviour in noisy environment.

ACKNOWLEDGMENT

This study was supported in part by National High Technology Research and Development Program of China under Grant No. 2007AA01Z406.

REFERENCES

Altman, E., A.A. Kherani, P. Michiardi and R. Molva, 2004. Non-cooperative forwarding in ad-hoc networks. Proceedings of IFIP Networking, Waterloo, May 2-6, Springer Press, Canada, pp: 486-498.

Anderegg, L. and S. Eidenbenz, 2003. Ad hoc-VCG: A truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents. Proceedings of the 9th Annual International Conference on Mobile Computing and Networking, Sept. 14–19, ACM New York, USA., pp: 245-259.

Buchegger, S. and J.L. Boudec, 2002. Performance analysis of the CONFIDANT protocol. Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing, June 15, Lausanne, Switzerland, ACM Press, pp: 226-236.

Buttyan, L. and J.P. Hubaux, 2003. Stimulating cooperation in self-organizing mobile ad hoc networks. ACM Mob. Netw. Appli., 5: 579-592.

Crowcroft, J., R. Gibbens, F. Kelly and S. Ostring, 2003. Modelling incentives for collaboration in mobile ad hoc networks. Proceedings of the Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, Mar. 3-5, INRIA Sophia-Antipolis, France, ACM Press, pp: 427-439.

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

Lu, Y., J. Shi and L. Xie, 2008. Repeated-game modeling of cooperation enforcement in wireless ad hoc network. Ruan Jian Xue Bao, 3: 755-768.

Mahajan, R., M. Rodrig, D. Wetherall and J. Zahorjan, 2005. Sustaining cooperation in multi-hop wireless networks. Proceedings of the 2nd Conference on Symposium on Networked Systems Design and Implementation, May 2-4, Boston, USA., USENIX Press, pp: 231-233.

Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehaviour in mobile ad hoc networks. Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Aug. 6-11, Boston, Massachusetts, USA., ACM Press, pp: 255-265.

Michiardi, P. and R. Molva, 2002. CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. Proceedings of the IFIP TC6/TC11 6th Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security, Sept. 26-27, Portoroz, Slovenia, Springer Press, pp: 107-121.

Michiardi, P. and R. Molva, 2003. A game theoretical approach to evaluate cooperation enforcement mechanisms in mobile ad hoc networks. Proceedings of the Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, Mar. 3-5, INRIA Sophia-Antipolis, France, ACM Press, pp: 3-5.

Osborne, M.J. and A. Rubinste, 1994. Nash Equilibrium: A Course in Game Theory. MIT Press, USA.

Srinivasan, V., P. Nuggehalli, C.F. Chiasserini and R.R. Rao, 2003. Cooperation in wireless ad hoc networks. Proceedings of IEEE Infocom, Mar. 30-Apr. 03, San Francisco, CA, USA., IEEE Press, pp: 808-817.

Sun, Y.L., W. Yu, Z. Han and K.J.R. Liu, 2006a. Information theoretic framework of trust modelling and evaluation for ad hoc networks. IEEE J. Sel. Areas Commun., 2: 305-315.

Sun, Y.L., H. Zhu, W. Yu and K.J.R. Liu, 2006b. A trust evaluation framework in distributed networks: vulnerability analysis and defense against attacks. Proceedings of 25th IEEE International Conference on Computer Communications, Apr. 23-29, Barcelona, Spain, IEEE Press, pp: 1-1.

Urpi, A., M. Bonuccelli and S. Giordano, 2003. Modeling cooperation in mobile ad hoc networks: A formal description of selfishness. Proceedings of the Workshop on Modelling and Optimization in Mobile, Ad Hoc and Wireless Networks, Mar. 3-5, INRIA Sophia-Antipolis, France, ACM Press, pp: 1-10.

Wang, W.Z., S. Eidenbenz, Y. Wang and X.Y. Li, 2006. Ours: Optimal unicast routing systems in non-cooperative wireless networks. Proceedings of the 12th International Conference on Mobile Computing and Networking (Mobicom), Sept. 24-29, Angeles, CA, USA., ACM Press, pp: 278-289.

Xu, C.D. and Y. Wang, 2001. Binomial Probability: Probability and Statistics. HIT Press, USA.

Yu, W. and K.J.R. Liu, 2005. Attack-resistant cooperation stimulation in autonomous ad hoc networks. IEEE J. Sel. Areas Commun., 12: 2260-2271.

Yu, W. and K.J.R. Liu, 2007. Game theoretic analysis of cooperation stimulation and security in autonomous mobile ad hoc networks. IEEE Trans. Mob. Comput., 5: 507-521.

Zhong, S., J. Chen and Y.R. Yang, 2003. Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies, Mar. 30, San Francisco, CA, USA., IEEE Press, pp: 1987-1997.

Zhong, S., L. Li, Y. Liu and Y.R. Yang, 2005. On designing incentive-compatible routing and forwarding protocols in wireless ad-hoc networks: An integrated approach using game theoretical and cryptographic techniques. Wireless Netw., 6: 799-816.