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 9 (1): 124-131, 2010
ISSN 1812-5638

Enabling Cooperative Ad Hoc Networks under Noise

[1]Dongbin Wang, [1]Xiangzhan Yu, [2]Hui Zhi and [1]Mingzeng Hu
[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, each node depends on other nodes for routing and forwarding packets. However, the selfish nodes will not forward packets for others to save resources which can significantly damage the network performance. Many solutions have been proposed to give nodes incentive to cooperate among selfish nodes. 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. The sporadic transmission errors caused by noise are considered as the dropping selfish behavior which decreases the packet delivery ratio and utility. Monitor, detection, path management and response schemes are proposed for the cooperation among selfish nodes in real in ad hoc networks. The packet dropping selfish behavior will be effectively monitored and can be distinguished with the sporadic transmission errors caused by noise. The selfish node will be detected and isolated from the transmission path gradually. The simulation results demonstrate that the proposed schemes can effectively increase the packet delivery ratio and utility under noise. The cooperative ad hoc network under noise is enabled.

Key words: Ad hoc networks, packet forwarding, cooperation, selfish nodes, packet dropping detection

INTRODUCTION

Mobile ad hoc networks (MANET) are formed dynamically by an autonomous system of mobile nodes that are connected via wireless links without using the existing network infrastructure or centralized administration (Chlamtac *et al*., 2003). The nodes are free to move randomly and organize themselves arbitrarily. Each node in mobile ad hoc networks can communicate with other nodes in its radio communication range. Nodes act both as terminals and routers in ad hoc networks. For communicating with nodes that reside beyond this range, a collection of mobile nodes form the temporary route and the node needs to use intermediate nodes to relay the messages hop by hop.

In many specific applications, such as military or emergency situations, nodes in an ad-hoc network belong to the same authority and pursue a common goal. Therefore, fully cooperative behavior, such as unconditionally forwarding packets to the destination node for the purpose of the source node, can usually be assumed. But in general, the mobile nodes in this network are constrained with limited resources, such as CPU, battery, channel bandwidth and etc. Forwarding packets for other nodes is an energy-consuming network activity that will shorten a node's lifetime. Some nodes in the network might not be willing to cooperate for the packet transmission, in order to save their resources, even though it expects other nodes to forward its packets to the destination. As these networks are spontaneous ones, there is no guarantee to always be in the presence of cooperative nodes behaving in compliance with the routing protocols. Cooperation issues are new compared to traditional infrastructure protocol paradigms. These issues deserve more attention because non cooperation could annihilate the entire advantage of the ad hoc capabilities. Lack of cooperation and the presence of only a few such selfish nodes can dramatically degrade the performance of an entire system (Pirzada *et al*., 2006).

Recently, many solutions have been proposed to give nodes incentive to cooperate among selfish nodes. 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. The packet dropping misbehavior can not be distinguished with the sporadic transmission error caused by noise. In general, the environment is noisy that is caused by unreliable wireless links and full of uncertainty, which may consequently result in that some decisions cannot be

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

perfectly executed or monitored. For example, even when a node wants to forward a packet for another node, this packet may still be dropped or not be overheard due to link breakage. The effect of noise in real environment has been ignored which decreased the packet delivery ratio and the cost of nodes in packet forwarding.

In the study, the challenging problem on cooperation is investigated in the more realistic scenarios, where the packet forwarding and observation are imperfect. We propose a scheme, ECANN to enable cooperative ad hoc networks with selfish nodes under noise. The packet dropping misbehavior will be effective monitored and be distinguished with the sporadic transmission error caused by noise. The simulation shows that the ECANN can increase the networks delivery ratio and cooperative nodes' utility under noise.

STATE OF THE ART

Non-cooperative issues in ad hoc networks have drawn considerable attention over the past few years and it has been shown that the presence of selfish nodes degrades the overall performance of a non-cooperative ad hoc network (Marti *et al*., 2000). Many schemes have been proposed to enforce cooperation in ad hoc networks, which can be roughly classified into several categories: price-based scheme, reputation-based scheme and VCG mechanism.

Price-based schemes introduce services charges to the packet transmission process and usually use micropayment to compensate the resource consumption incurred from the transmission. A virtual currency NUGLET (Buttyan and Hubaux, 2003) is introduced as economic incentive which requires the tamper-proof hardware in each node. Each intermediate node buys a packet for some nuglets and sells it to the next one for more nuglets. Therefore, a node increases its nuglets amount during packet forwarding. The SPRITE (Zhong *et al*., 2003) applied the same idea without the requirement of hardware, but with a credit based system and a central clearing banking service. These schemes can effectively stimulate cooperation among selfish nodes, but the requirement of tamper-proof hardware or central billing services greatly limits their potential applications.

Reputation-based schemes use trustworthiness and reputation information in routing to enforce the cooperation among nodes. In (Marti *et al*., 2000), participating nodes are designed to perform monitoring to overhear the packet transmission and avoid transmission to misbehaving nodes. The CONFIDANT (Buchegger and Boudec, 2002) distributes trustworthiness information among those participating nodes and every node is supposed to keep a reputation list of the nodes with which it has previously interected. He *et al*. (2004) and Refaei *et al*. (2005) evaluated the trust level of a node by aggregating feedback information from its neighbours to reduce the communication overhead. The STRUDEL (Quercia *et al*., 2006) is a distributed framework that tackles the problem of free-riders in Coalition Peering Domains by using a Bayesian trust model to dynamically select and isolate selfish peers. The SAFE (Rebahi *et al*., 2005) aimed at detecting and avoiding misbehaving nodes and whose computation of the reputation is directly proportional to the percentage of the correctly forwarded packets. The ASM (Li and Li, 2008) is a hierarchical reputation system integrated with a global reputation management system and a pricing-based model for effective selfish node punishment. Some proposed schemes can not distinguish the misbehavior caused by noise from that caused by selfish intention and the false positive assertion will degrade the performance of the ad hoc networks.

The VCG Mechanism design was introduced to stimulate the cooperation in the route discovery. The ad hoc-VCG routing protocol for ad hoc networks with selfish agents is a generalized second best sealed bid auction mechanism and achieves cost-efficiency and truthfulness for data transmissions (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. The VCG mechanism was to make cheating unattractive by making payments as high as a node could possibly expect to obtain by cheating. However, it needs $O(n^3)$ control messages for a route discovery and can not provide good performance on metrics such as packet delivery ratio and end-to-end delay. Based on VCG, Corsac is proposed, which integrates VCG and cryptographic technique to solve the combined problem of routing and packet forwarding (Zhong *et al*., 2005). OURS had smaller overpayments than VCG-based solutions (Wang *et al*., 2006). The message overhead of Ad hoc-VCG is high and may exhaust each possible path to find the most energy efficient one. The VCG mechanism also incurs budget imbalance and overpayment.

Most of existing solutions have assumed perfect observation in ad hoc networks and the packet dropping misbehavior can not be distinguished with the sporadic transmission error caused by noise. In this study, the

effect of noise in real environment has been considered and schemes are presented to stimulate cooperation under noise.

SYSTEM DESCRIPTION

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. A sequence of nodes will be requested to help forward packets in the multi-hop path. The intermediate node can intentionally drops packet because forwarding a packet will incur cost. Our 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, our goal is to detect the selfish nodes and the selfish nodes will be isolated from the networks. As a sequence, the selfish nodes' forwarding requests are not satisfied and the path with selfish nodes will be avoided. In the proposed schemes, no tamper-proof hardware or central banking service is assumed.

An autonomous mobile ad hoc network with a finite population of users, denoted by N, is considered. The node is involved in sending its own packets and also forwarding neighbours' packets. Each node $i \in N$ has a type $\theta_i \in \Theta$, where Θ = (cooperativ, malicious). Meanwhile, no node can know the others' type a priori. We assumed that 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.

For each node i, if a packet originated from it can be successfully delivered to its destination, it can get gain g_i and transmitting a packet either for itself or for the others, incurs costc_i, where $g_i > c_i$. Similar to (Yu *et al*., 2007), based on the notations in Table 1, for any node $i \in N$, its utility:

Table 1: Summary of notations

Notations	Description
t_i	The lifetime of the nodes i
R_i (t)	The number of packets that originated from node i and have been successful reached the destinations by time t
Fi (t)	The number of packets that node i has forward for by time t
S_i (t)	The number of packets that node i needs to send by time t
g_i	The gain node i gets for a successfully delivered packet riginating from it
c_i	The cost when node i transmits a packet
U_i (t)	The utility of node i by time t
U (t)	The average utility of the cooperative nodes by time t
N	The set of cooperative and selfish nodes
N_c	The set of cooperative nodes

$$U_i(t) = \frac{R_i(t)g_i - F_i(t)c_i}{S_i(t)} \quad (1)$$

In order to maximize the utility, the successfully delivered packets should increase or the forwarded packets should be decreased. The selfish node will drop the packets that are needed to be forwarded through it and decrease cost in forwarding packets for other nodes. And our goal is to maximize all the cooperative nodes' utility. To simplify the illustration, we assume that $g = g_i$ and $c = c_i$ for $i \in N$.

$$U(t) = \frac{\sum_{i \in N_c} R_i(t)g - F_i(t)c}{\sum_{i \in N_c} S_i(t)} \quad (2)$$

The high ratio of packets successfully delivered to the destination must be kept for the overall maximum utility. Since, the packets dropping conducted by selfish nodes will bring the detriment to U (t), selfish nodes must be detected and isolated from the path.

SCHEME DESIGN

In this section, enforcement scheme in ad hoc networks under noise is proposed, which consists of four main modules: monitor, detection, path manager and response. All of these modules are employed on cooperative nodes. Figure 1 demonstrates these modules and their relationship. Each module is discussed in detail below.

Monitor: The monitor module of each node can passively overhear the communication from each of its neighbours when the wireless interface supports promiscuous mode operation. When the node sends a packet toward the destination through its neighbour, monitor can overhear

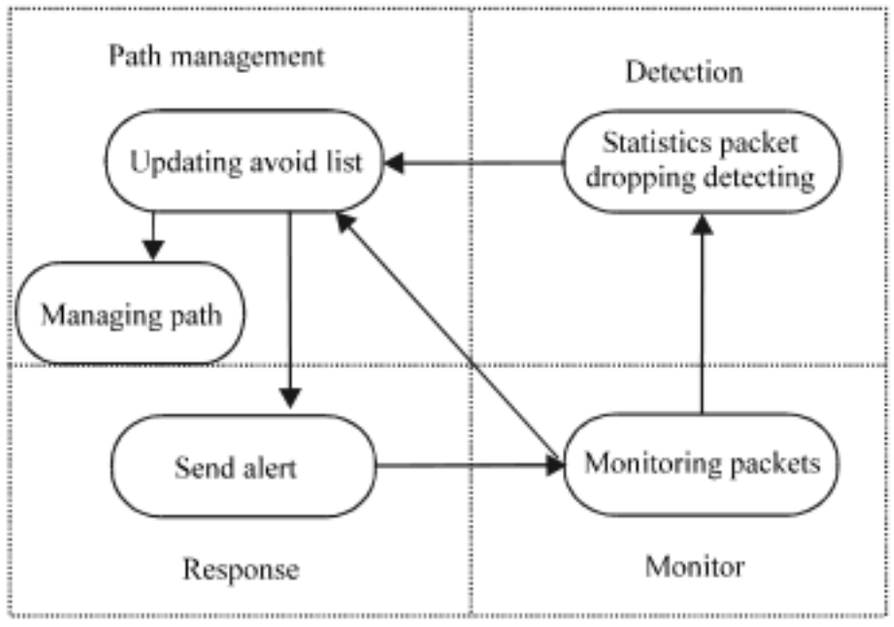

Fig. 1: Modules within each node

its neighbour's transmission and verify that the neighbour has attempted to pass the packet to its next hop node like Watchdog and Pathrater (Marti *et al*., 2000). Monitor keeps a copy of sent packet when sending the packet and compares each overheard packet with kept copies to see if there is a match. If so, monitor asserts that the neighbour have forwarded the packet and report the normal behavior to detection module. If the forwarding behavior of the packet has not been detected for longer than a certain timeout, the abnormal behavior of the neighbour will be asserted and reported. Monitor can check whether the neighbours really forward the packets with contents unchanged, or drop them, or modify the contents.

Detection: Detection module receives the report from Monitor and is responsible for identifying the selfish nodes according to the node's own observations. Every node will be assumed cooperative initially. The neighbour's behavioral history during the last specific time is audited and taken into consideration for identifying the selfish node. The statistical packet dropping detection mechanism is used to distinguish packet dropping caused by selfish behavior from those caused by noise. If the neighbor is thought with sufficient evidence as a selfish node, it will be reported to Path Management and Response module.

Path management: Path management interacts with routing protocol, receives the report about the neighbour's selfish behavior and adds it to the blacklist. The path without nodes in the blacklist will be chosen by Path Management, if the node wants to send packets. Furthermore, when the node receives a packet to forward for the benefit of other nodes, path management decides whether or not forwards packet to the next hop.

Response: Once response module receives the report about the misbehaviour of a node, alerting message will be sent to the source of the concerned route to notify it of the selfish node. Once the node receives the notification of misbehaviour, path management will be invoked.

MISBEHAVIOR DETECTION UNDER NOISE

In wireless ad hoc networks, perfect transmission of packets is generally assumed in ideal scenarios. But in general, not all packet forwarding decisions can be perfectly executed. When a node sends packet to the next-hop node, the next node may not receive the packet successfully due to noise which maybe consists of error prone communication channels, environmental unpredictability, link breakage caused by mobility, hidden-stations problem caused by transmission collision, (Chlamtac *et al*., 2003). The perfect observation on packets forwarding can not be taken for granted under noise too.

In realistic wireless networks, noise is inevitable and can cause severe trouble. 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. Ambiguous packet dropping and imperfect observation of packet forwarding can happen under noise. Figure 2 illustrates the network snapshot of the realistic scenario under noise and imperfect observation, a packet forwarded by B from A, is not received by the next-hop node C and is not overheard by the previous-hop node A due to noise.

How to detect the misbehavior in the scenarios with noise is open problem for ad hoc networks. Distinguishing the misbehavior caused by noise from that caused by selfish intention is a challenging task. The statistical packet dropping detection mechanism is introduced to distinguish packet dropping caused by selfish behavior from those caused by noise. Monitor is used to observe the forwarding behavior of a node. To simplify the analysis, packet dropping is modeled due to noise as follows: For any player i when it has decided to forward a packet to the next-hop node j for any other player, with probability q_d, this packet may be dropped due to noise. When the node j forwards the packet to next-hop node, with probability q_m, the forwarding behaviour of node j can not be successfully overheard by node i. The probability of successful packet forwarding and forwarding monitor can be either estimated by nodes online or trained offline. Let q_e be the probability that node i can not observe the forwarding behavior of node j after it send a packet to node j. So we can have:

$$q_e = 1-(1-q_d)(1-q_m) \tag{3}$$

That is, packet dropping observed by node i under noise can be modeled using a Bernoulli random process. Let $Q_n(k)$ be the probability with which node i observes that k packets are not forwarded by node j when i transmits n packets to node j by time t. we can have:

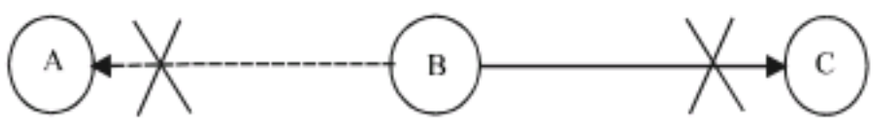

Fig. 2: Packets forwarded by node B

$$Q_n(k) = C_n^k q_e^{\ k} (1-q_e)^{n-k} \quad (4)$$

If $n \to \infty$ and $q_e \to 0$, based on binomial probability and Poisson distribution (Xu and Wang, 2001), we can have

$$C_n^k q_e^{\ k} (1-q_e)^{n-k} \to \frac{\lambda^k}{k!} e^{-\lambda} \quad (5)$$

Where: $\lambda = nq_e$.

Let $Selfish_i(j)$ denote i's belief about j's type, where $Selfish_i(j) = 1$ indicates that i believes j is selfish, while $Selfish_i(j) = 0$ indicates that i believes j is cooperative. Then, the following hypothesis testing rule can be used by i to judge whether j is selfish with ε, the maximum allowable false positive probability:

$$Selfish_i(j) = \begin{cases} 1, & \text{if } \sum_{k=D_i(j)}^{\infty} \frac{\lambda^k}{k!} e^{-\lambda} < \varepsilon \\ 0, & \text{if } \sum_{k=D_i(j)}^{\infty} \frac{\lambda^k}{k!} e^{-\lambda} \geq \varepsilon \end{cases} \quad (6)$$

where, $D_i(j)$ is the number that node i can not observe the forwarding behavior of node j, when i send n packets to node j for forwarding.

When the packets dropping happened, most of previous solutions such as Watchdog and Pathrater can not distinguish packet dropping caused by selfish nodes from those due to transmission error. The proposed statistical packet dropping detection mechanism in the paper can perfectly solve the challenging problem.

SIMULATION RESULTS AND DISCUSSION

A set of simulations are investigate to evaluate the proposed schemes under noise. A random network with 50 cooperative nodes and some selfish nodes is generated. The nodes are randomly distributed in the rectangular area of 1000×1000 m. Each node may either be static or move according to the random waypoint model in which a node starts at a random position randomly chooses a new location and moves toward the new location then randomly moves again after a pause time which is set 100 sec in the simulations. In the random network, the maximum distance between which two nodes can directly communicate with each other is set to be 250 m. IEEE 802.11 DCF is adopted as the MAC layer protocol and DSR is used as the route protocol in the simulations. The simulation time is set 1000 sec. For each simulation, each node randomly picks another node as the destination to send packets with the packet interval time slot, 1 sec. Let g = 1 and c = 0.1 in the simulations.

Transmission error ratio: In ad hoc networks, the ratio of the packets dropping caused by noise plays an important role in packets forwarding. The transmission error ratio q_d under noise is calculated as the ratio between the total number of dropped packets it experienced as the transmitter and the number of packets transmission it has tried as the transmitter. Figure 3 shows the transmission error ratio experienced by different nodes under the above scenario which will be used in the following simulation. Let $q_d = 0.025$ in the following simulations.

Simulation studies under noise: Figure 4 showed the delivery ratio of ECANN and Watchdog and Pathrater (Marti *et al*., 2000) under noise when the simulation ran 1000 sec. The simulation results showed that the delivery ratio of ECANN was more 1.2% than that of Watchdog and Pathrater. When the simulation began, ECANN and

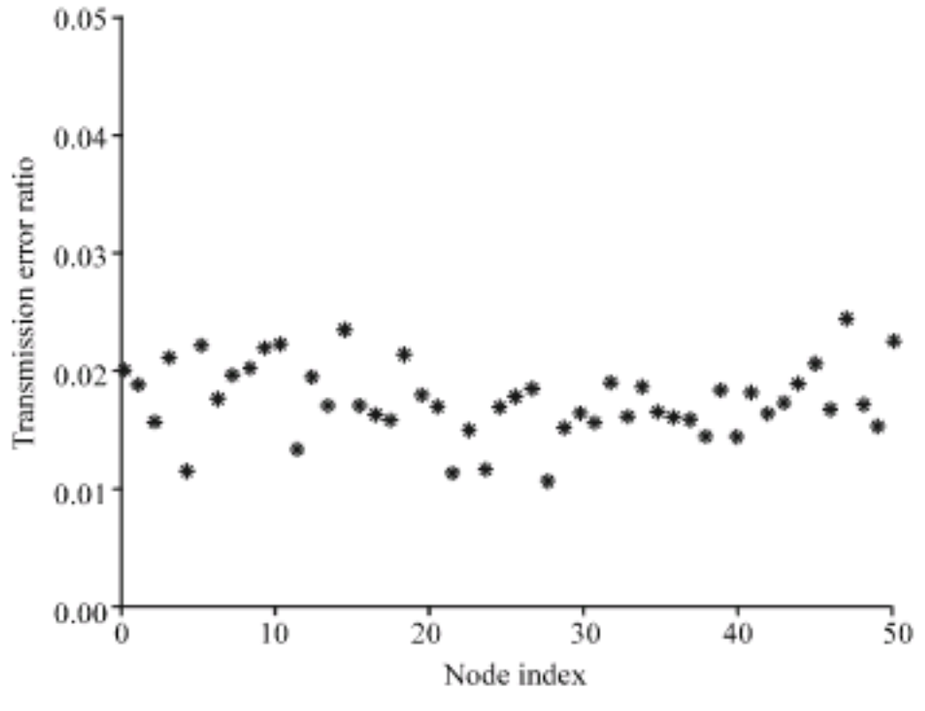

Fig. 3: Transmission error ratio

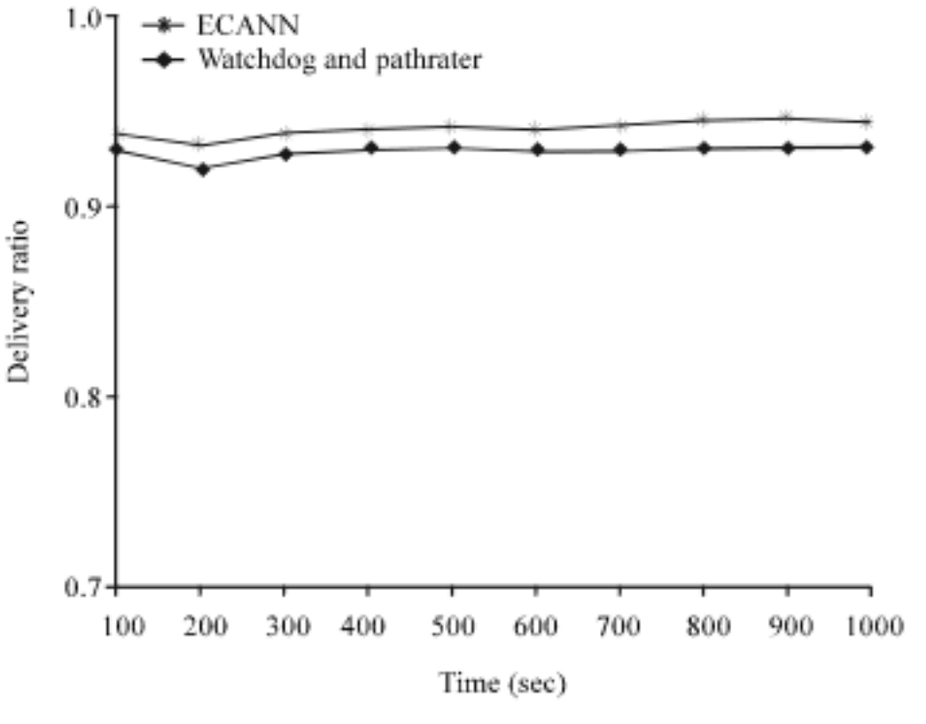

Fig. 4: Comparison of delivery ratio under noise

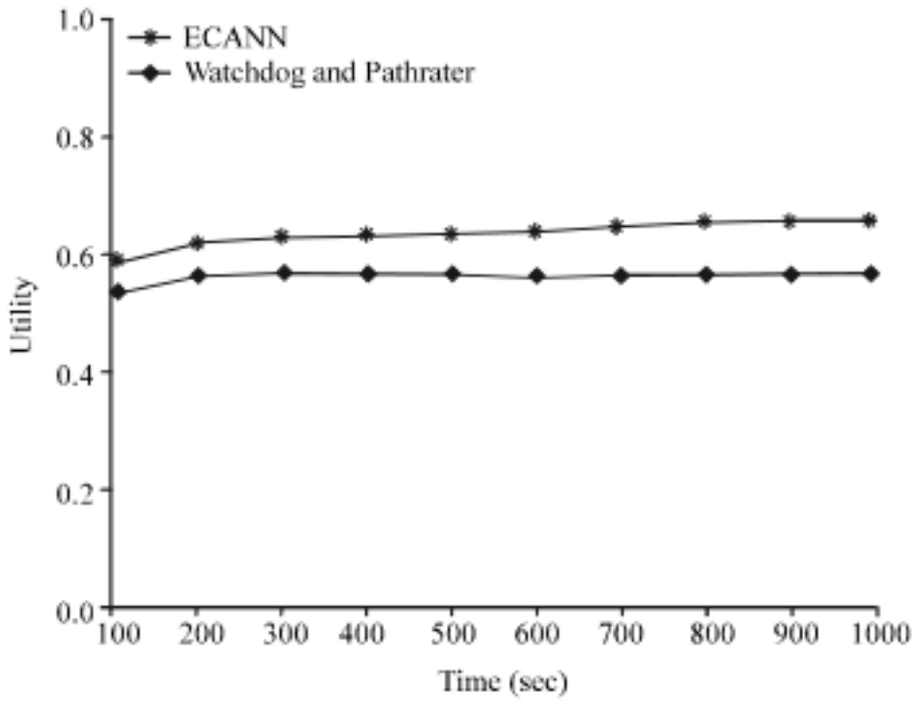

Fig. 5: Comparison of utility under noise

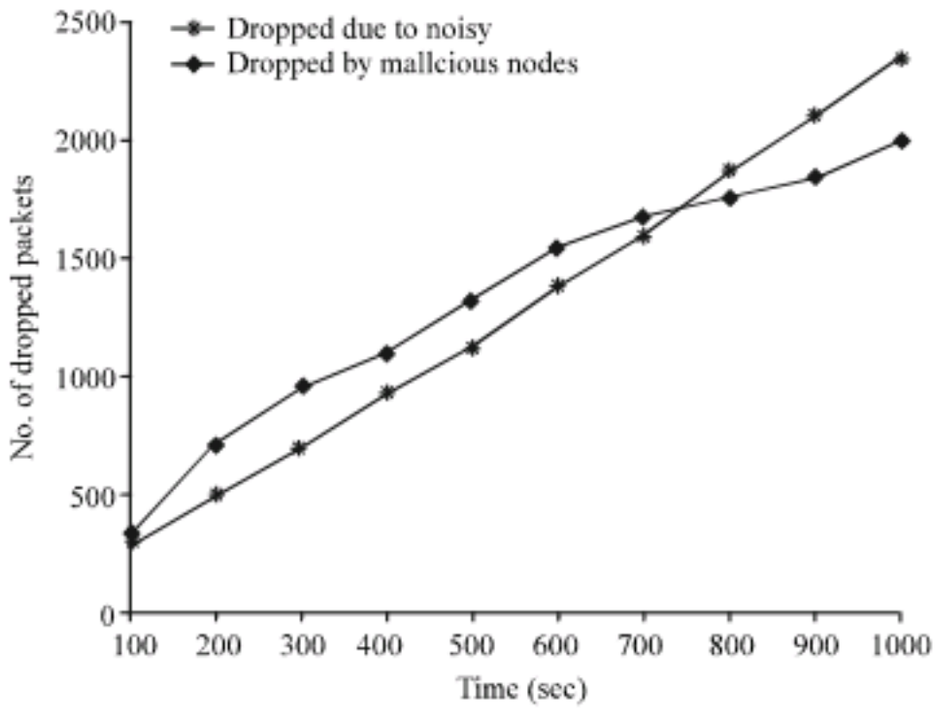

Fig. 6: Number of dropped packets

Watchdog and Pathrater chose the shortest path as the route to transmit packets. When the transmission error caused by noise happened and the packet was dropped, Watchdog and Pathrater would decrease the reputation of the node and reselected the path with most average reputation which did not mean the shortest path and maybe longer than the shortest path. When the sporadic transmission error caused by noise happened, ECANN would not reselect the path until the selfish nodes were detected. So, the path selected by ECANN was not longer than that selected by Watchdog and Pathrater. When the length of the selected path increased, the probability of packet dropping increased under noise. So, the delivery ratio of ECANN was more than that of Watchdog and Pathrater.

Figure 5 showed the utility of ECANN and Watchdog and Pathrater under noise when the simulation ran 1000 sec. The utility of ECANN was more about 0.08 than that of Watchdog and Pathrater under noise because the average length of the path selected by Watchdog and Pathrater was more than that selected by ECANN. When the length of the path increased, more nodes would be selected as the intermediate nodes to forward the packet and the cost for packet forwarding increased too. So, the utility of ECANN was more than that of Watchdog and Pathrater.

Simulation studies of ECANN under noise: The reason for packets dropping consisted of the existence of noise and selfish behavior. Figure 6 showed the increase of dropped packets due to noise and caused by selfish nodes with 10 selfish nodes in the simulation. At first, the number of dropped packets caused by 10 selfish nodes is more than that caused by noise. After 800 sec, the number of the dropped packet caused by noise is constant and

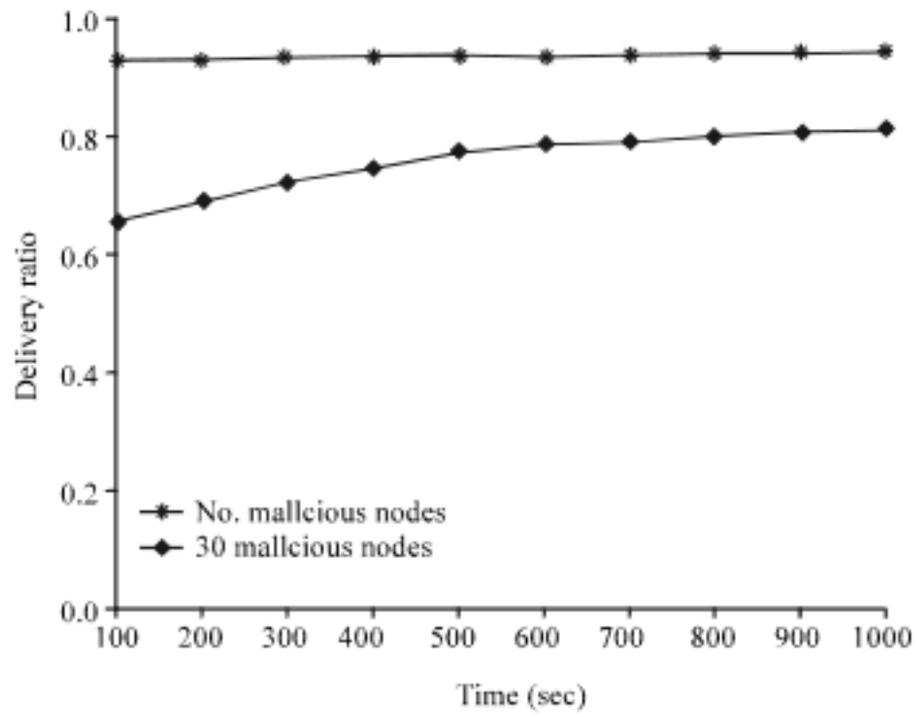

Fig. 7: Delivery ratio

more than the number of the dropped packets by selfish nodes. The probability of packet dropping due to noise would increase evenly. When more selfish nodes were effectively detected and isolated gradually by ECANN from the path that was used to transfer the packet, the number of dropped packets caused by selfish nodes increased slower than that caused by transmission error.

Figure 7 showed that the delivery ratio with 30 selfish nodes increased when more selfish nodes were detected and isolated from the path gradually. When all the selfish nodes are isolated from the transmission path, the following delivery ratio in ECANN would be very close to that with no selfish.

DISCUSSION

From the above simulation results, we could have that the proposed ECANN outperformed Watchdog and

Pathrater (Marti *et al*., 2000) in the delivery ratio and utility under noise. ECANN increased the delivery ratio by up to about 1.2% and the utility by up to about 0.08 compared to Watchdog and Pathrater under noise. ECANN could distinguish packet dropping caused by selfish nodes from those due to sporadic transmission error, but Watchdog and Pathrater could not. When more selfish nodes were detected and isolated from the path by ECANN, the delivery ratio and utility would increase gradually.

CONCLUSION

In this study, we proposed monitor, detection, path management and response to cope with the selfish behavior under noise. The proposed statistical dropping packet detection mechanism can effectively distinguish packet dropping caused by selfish behavior from those caused by noise. The selfish nodes will be isolated from the transmission path gradually. The number of dropped packets caused by selfish nodes decreases and the utility increases continuously. The result in the simulation shows that ECANN increased the delivery ratio by up to about 1.2% and the utility by up to about 0.08 compared to Watchdog and Pathrater under noise. When more selfish nodes were detected and isolated from the path by ECANN, the delivery ratio and utility would increase gradually. The proposed schemes can enable cooperative ad hoc networks under noise gradually.

ACKNOWLEDGMENTS

This study was supported in part by National High Technology Research and Development Program of China under Grant No. 2007AA01Z406, No. 2006AA01Z452 and No. 2009AA012437.

REFERENCES

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. Appl., 5: 579-592.

Chlamtac, I., M. Conti and J.N. Liu, 2003. Mobile Ad Hoc networking: Imperatives and challenges. Ad Hoc Netw., 1: 13-64.

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.

He, Q., D.P. Wu and P. Khosla, 2004. SORI: A secure and objective reputation-based incentive scheme for ad-hoc networks. Proceedings of IEEE Wireless Communications and Networking Conference, Mar. 21-25 Atlanta, GA, United states, IEEE Express, pp: 825-830.

Li, H.S. and Z. Li, 2008. ARM: An account-based hierarchical reputation management system for wireless ad hoc networks. Proceedings of the 28th International Conference on Distributed Computing Systems Workshops, Jun. 17-20 Beijing, China, IEEE Express, pp: 370-375.

Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehavior 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.

Pirzada, A.A., C. McDonald and A. Datta, 2006. Performance comparison of trust-based reactive routing protocols. IEEE Trans. Mobile Comput., 5: 695-710.

Quercia, D., M. Lad and S. Hailes, 2006. Strudel: Supporting trust in the dynamic establishment of peering coalitions. Proceedings of the 2006 ACM Symposium on Applied Computing, Apr. 23-27 Dijon, France, ACM Press, pp: 1870-1874.

Rebahi, Y., V. Mujica and D. Sisalem, 2005. A reputation-based trust mechanism for ad hoc networks. Proceedings of 10th IEEE Symposium on Computers and Communications, Jun. 27-30 Cartagena, Spain, IEEE Express, pp: 37-42.

Refaei, M.T., V. Srivastava and L. DaSilva, 2005. A Reputation-based mechanism for isolating selfish nodes in ad hoc networks. Proceedings of the 2nd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, Jul. 17-21 IEEE Express, San Diego, CA., pp: 3-11.

Wang, W.Z., S. Eidenbenz S, 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., Z. Ji and K.J.R. Liu, 2007. Securing cooperative ad-hoc networks under noise and imperfect monitoring: Strategies and game theoretic analysis. IEEE Trans. Infrom. Forensics Secur., 2: 240-253.

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.