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 12 (20): 5577-5582, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.5577.5582

Load Balancing Mechanism and Selfish Nodes Detection in Peer-to-Peer Network

[1,2]Min Liu and [3]Ying Li
[1]Changsha Aeronautical Vocational and Technical College,
410014, Changsha, China
[2]School of Information Science and Engineering, Central South University,
410083, Changsha, China
[3]School of Information Engineering, Jiaozuo University, 454000 Jiaozuo, China

Abstract: Due to its limited resources and other objective factors and subjective attitude of the impact of peer nodes in the network often exhibit selfishness. Therefore, encourage selfish nodes cooperate to detect and become an important research by allowing nodes to freely express their subjective forward attitude. To achieve the detection of selfish nodes, it is taking into account not only the quality of the link and node energy and other objective factors that determine the path forward probability and taking into account the path under the influence of selfish nodes forwarding the subjective probability. To select the path with the highest probability of integrated transponder, it is reducing the impact of selfish nodes when the node selfishness spend time re-designed a punishment mechanism based load balancing to encourage cooperation model participation and cooperation of nodes according to the degree of harm node selfishness. The right is taken appropriate punitive measures between nodes monitoring mechanism and strict punishment mechanism to ensure the implementation of strategic defense. The simulation results show that the detection and load balancing not only in the energy constrained and rational selfish nodes case seeking to the appropriate route, but also to inspire too selfish nodes actively participate in the network.

Key words: Peer-to-peer network, detection mechanism, load balancing mechanism, selfish node

INTRODUCTION

In recent years, with the other models in the successful operation of a wired network and wireless communication technology, rapid development, especially in the increasingly complex needs of users for collaborative work between the node and resource sharing has put forward higher requirements, the emergence of a new class of application network-peer to peer network. peer network technology psince the birth of the spirit of "sharing" concept, but in fact has been shown that many nodes just want to get from a peer to peer network services provided by other nodes, instead of the other nodes is willing to sacrifice in the early days, closed peer to peer network all nodes belong to the same organization, it is possible to cooperate with each other to complete a goal of reunification, but with communication devices, such as PDA, mobile phone, etc., the rapid development and popularization of nodes may come from different organizations, although the composition of an open peer to peer network, but because each organization's goals are different nodes, coupled with their own resources, such as node processing power, battery power, etc. is limited, there is inevitably a certain node selfishness, which enjoy more resources and services of other nodes, less share their resources and services to achieve savings of their own resources the purpose, therefore, if the node is not considered in the choice of route of selfish nodes, it will lead to not successfully transmitted data packets reach the destination node. Therefore, how to detect the network and its excitation selfish nodes cooperate to ensure network performance, peer to peer network of important issues need to address (Charilas and Panagopoulos, 2010).

The study had proposed the peer to peer network for selfish nodes detection and load balancing. The basic idea is to forward the Subjective Forwarding Probability (SFP) to describe the activities of the network node selfishness, an Objective Forwarding Probability (OFP) to describe its forwarding capability, the route selection, by considering all the nodes on the path Forward Probability (FP), in order to achieve the detection of selfish nodes, while, if the node degree of selfishness too high, then

Corresponding Author: Min Liu, Changsha Aeronautical Vocational and Technical College, 410014, Changsha, China

through penalty based load balancing mechanisms to encourage selfish nodes to improve their subjective probability forwards, to achieve cooperation (Gui *et al*., 2010).

SELFISH NODE DETECTION MECHANISM

Network model: Traditional route algorithms often had based on one or a combination of a number of indicators as selection criteria, such as number of hops, latency, etc., For example, AODV that is, the number of hops as the routing indicators in recent years, there have been some reflect the path quality indicators, which represents the link correctly transmitting a packet transmission times required, each node periodically broadcasts the neighbor probe packets of fixed size (Wang *et al*., 2011). While recording received over a period of time from its neighbor probe packet information to detect the actual number of packets received and should receive a proportion of the number of probe packets is the corresponding link delivery ratio, but did not consider either of these indicators of selfish nodes, either directly away selfish nodes. reality selfish nodes may only have a certain degree selfish, not completely selfish as in the prior two next hop node to be selected, one for co-node link bandwidth and other objective factors that determine its forwarding capability is 0.5, which can only be successfully forwarded packets received half. Another is selfish nodes, forwarding capacity of an objective, but the selfishness of 0.2, with 80% probability of being forwarded to close the data packet (Yoo and Agrawal, 2006). Clearly the overall performance from the point of view, we should choose a higher likelihood of selfish nodes forwarding. Rather than the traditional mechanisms for cooperation, as selected node, so we introduced to describe the probability of forwarding nodes for packet forwarding actual situation and forwards with subjective probabilities represent nodes participating in the network activities of subjective attitudes. The objective Probabilistic forwarding link bandwidth has node to process speed and other objective conditions under node forwarding capability (Yoo *et al*., 2010).

Objective probability of forward node: Objective factors refer to the properties of things themselves for forwarding probability, the node's objective factors objective factors can be divided into internal and external objective factors two kinds. Former mainly refers to the limit by the forwarding probability of node energy, while the latter refers to the process by the node capacity and the corresponding link bandwidth and other objective factors limit the forwarding probability:

- **Inner objective forwarding probability:** The peer to peer network, the energy is an important node and limited resources for the node, generally, the energy, the more the higher the degree of participation in network operation; for the network, the data traffic sent to more adequate energy nodes, avoiding the low-energy nodes can improve the performance and extend the network lifetime:

$$\text{IOFP} = \text{energy\_rate} = \frac{\text{Remaining\_energy}}{\text{intial\_energy}} \tag{1}$$

The Eq. 1 shows the residual energy of the node and the ratio of the initial energy that their Inner Objective Forwarding Probability (IOFP). The residual energy of the node had the higher IOFP.

- **External objective forwarding probability:** The External Objective Forwarding Probability (EOFP) reflects the ability of nodes and corresponding links, the channel quality is closely related to the previous studies have shown that, in general, the more the link attribute measurement, the more accurate the resulting channel quality but also taking into account the accuracy and computational problems. In current, the wireless link quality metrics are four parameters: the Received Signal Strength Indication (RSSI), signal-to-interference-plus-noise ratio (SINR), Packet Delivery Ratio (PDR) and Bit Error Rate (BER). PDR is currently the largest and most cost-effective use of metrics, so we use PDR to represent nodes EOFP

In the peer to peer network, the adjacent node uses the HELLO packet exchange information in order to ensure network connectivity. Each node periodically (every d seconds) broadcast a TTL (time to live) value of a HELLO packet hop neighbors to it, so we use the node j per unit time i actually received from the neighbor HELLO packet number and should receive as the ratio between the number of external objective forwarding node j probability, namely:

$$\text{EOFP} = \frac{\text{rec}(w)}{\text{send}(w/d)} \tag{2}$$

In Eq. 2, rec (w) of node j in w seconds received from the neighboring node i number of the HELLO packet, send (w/d) represents the w seconds, the node i, the number of packets sent HELLO , EOFP includes a node i to node j and the link between the forwarding capacity of node j, we use it to describe the node j to node i information from an external forwarding probability objective.

Subjective forwarding probability: Subjective factors refer to things in their own wishes. Forwarding node subjective probability mainly refers to the open peer to peer network, each node in the network other organizational entities for data transmission degree of willingness to participate in the process due to limited resources of nodes and some nodes may run in this network can't obtain the relevant benefits, so there is a certain need to allow some nodes selfishness, or they may be directly out of this run for the losses caused by a greater overall performance, so we introduction of subjective probabilities to describe forwarding node selfishness, ranging from (0, 1). The SFP lower the higher the degree of node selfishness, the greater the likelihood of dropped packets. Subjective forwarding probability mechanism allows freely expressed will of selfish nodes, thus reasonable to save energy. The other nodes can also be routed, according to the actual situation to avoid SFP lower nodes to ensure data transmission.

Detection of selfish nodes: The foregoing analysis shows that traditional network nodes forwarding probability that node forwarding capability, but in the peer to peer network nodes forwarding probability determined by three factors is its subjective probability and forwards inside/outside objective of forwarding probability plot, as shown in Eq. 3 below, both objective and reflects the ability of nodes, but also reflects the node subjective approach:

$$FP_i \; SEP_i \times IOFP_i \times EOFP_i \qquad (3)$$

In order to know each other's neighbor forward probability, we conducted a HELLO packet to the necessary changes. The HELLO packet size (2m+5)×4byte (m the number of neighbors), much larger than the general network connectivity only to ensure the HELLO packet, the packet is closer to normal size, so to obtain a more accurate link quality. The probability of the node by forwarding parameters, so that the path the transmission probability is the probability that all the nodes along the forwarding of the product, namely:

$$TP_{path} = \prod_{i \in path} FP_i \qquad (4)$$

LOAD BALANCING MECHANISM

Routing load and penetration are closely related, the higher-degree nodes, a node routing load the greater the current, the typical structure of the protocol does not consider the selected node as the node of the load and the size of the routing table entry pointer, node-degree difference between the larger, so that the routing nodes between the load are quite different. To reduce the load difference between nodes, the study method to migrate a logical link, the link from the overloaded node migration to the light load nodes, while reducing the load routing nodes overloaded, while increasing the light load routing nodes, thereby reducing the load difference between nodes.

For any node, if it knows the system load distribution cases, the more it made relative to the more reasonable choice. Taking into account without increasing network overhead, each node when sending a message both to its own load information into the message. The load information load data structure contains the following members: node, the actual system is a node address; requesting node load requestLoad; node routing load routingLoad; total load node, load = request Load×w_r+routingLoad; the node-degree; record reverse junction node receives a message of recent time.

For any node n, its statistical load information includes the following three aspects: (1) A list of the node itself, load information loadList, elements Load structure type T junction calculated once every cycle load their own request, routing load and knot point of penetration and added to the list. Load information is counter_node_load_list, (2) The reverse junction of structure type elements load after junction node b receives a message, if the reverse load information of the node contains a list of update, or else add a record and record the current time, the delete list expired load information, (3) Load information finger_node_load_list node routing table, type of structure elements load with stable algorithm to update the routing tables updated, when the first node N0 claim 5 routing table entry, the node N19 assuming response node N19 entrained in the response message sent to their average loading information node N0, N0 after receiving the message updates finger_node_load_list.

STRATEGY PROOF

This detection and load balancing mechanisms have ensured the strategy proof.

Proof: Strategy proof refers to asymmetric information game. All participants had no motive to lie to other participants or hide their private information herein, the node's private information. There are three: SFP, IOFP and EOFP. Them, IOFP because of its nature strictly monotone decrease, will be found to lie once, so that no false information about the node rational IOFP. The process running on the network, the probability of the node to be the actual forwarding upstream neighbor obtained by monitoring Watchdog mechanism, thereby to obtain SFP and the actual EOFP their actual product and we can see through their reports HELLO packet with EOFP SFP product, so falsely will be found.

Moreover, the node information was discovered lying about in the future network life cycle without any income, the nodes lie in order to get more revenue, so rational node does not lie, in order to achieve the strategic defense.

SIMULATION EXPERIMENTS

The study had used NS2 simulation software to achieve the related mechanisms (Yu and Jin, 2008). Fifty nodes randomly distributed in a rectangular plane scene. Each node uses IEEE 802.11 wireless network interface, transmission distance of 250 m, moves to follow Random Waypoint Mobility Model: The node to a certain speed to a target position is selected at random, followed by a pause wait time, then randomly select a destination and its move uniformly distributed node speed 0-20 m sec^{-1} between the network simulation time is 600 sec. The nodes residence time are 0, 60, 120, 300 and 600 sec. When the residence time to zero, the node remains in motion; when the residence time of 600 sec, the nodes remain in a static state. Randomly selected network be 40 nodes, two end nodes as a group of CBR connections, a total of 20 connections, each of the source node generates 512 bits per second data packets and transmitted:

- **Node selfishness impact on network performance:** In the specific evaluation of the proposed mechanism, the first analysis of the node selfishness hazards for network performance in order to more accurately and impartially test performance, we use AODV as the underlying protocol here, set the selfish nodes are not made of the received to their information packet, according to their selfishness discarded. Suppose node has sufficient energy

  AODV(x) of x is selfish nodes. The number of nodes in the network representing the percentage of the total number can be seen, when the network node does not selfish, AODV good performance; however, with the proportion of selfish nodes in the network increases, the network performance is getting worse, when the proportion of selfish nodes in the network accounted for 20%, the network performance is almost reduced to half of the original; when the ratio increased to 50%, that is half the nodes in the network selfish node, delivery rate of only 5%, almost negligible

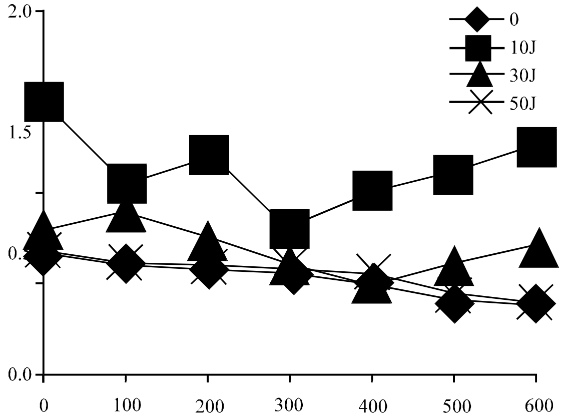

Fig. 1: Comparison of network performance under different number of selfish nodes

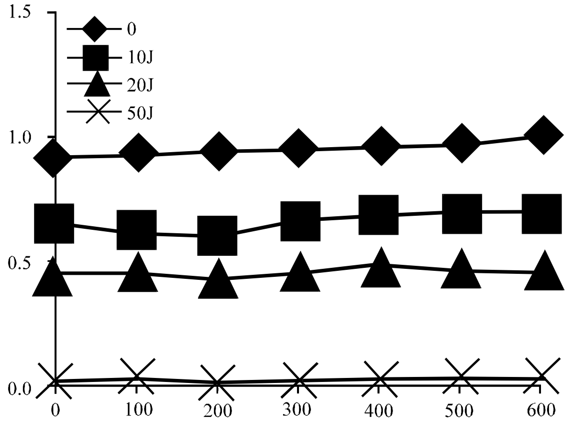

Fig. 2: Comparison of network performance under different degree of selfish nodes

Figure 1 is a test network, all the nodes are selfish nodes (selfish different degrees) case performance. AODV(x) of x represents the average selfish nodes in the network level can be seen, with the increase in average node degree selfish, network performance is getting worse when the average node degree is 0.1 selfish, network performance under normal conditions is about 2/3. When selfish nodes are increased to 0.5, the probability of each node has the performance of selfish half when the delivery rate of only about 13%

It can be seen from the above experiments, even if the network node has only a small part of the performance of the selfish, packet delivery rate will be decreased significantly. Therefore, must be able to detect and avoid the selfish nodes, if necessary load balancing to improve performance

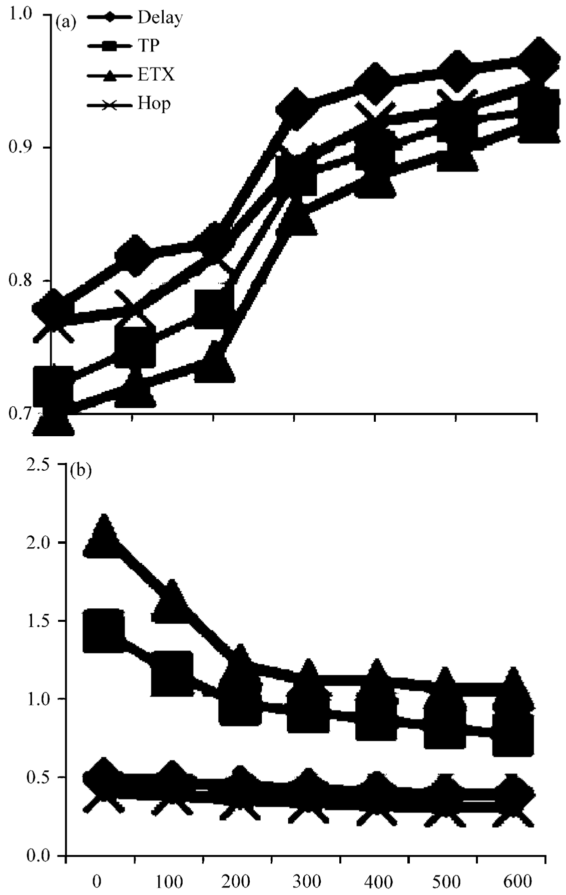

Fig. 3(a-b): Performance comparison under no selfish node and enough energy, (a) Packet delivery ratio and (b) Routing overhead

- **Detection mechanism performance:** After analyzing the node selfishness and energy limited impact on network performance, we then analyze the performance of detection mechanism, first analyze the situation in unlimited (selfish nodes do not exist in the network, the node sufficient energy) performance under the Note, due node energy is sufficient and no selfish node, so the text of the IOFP and SFP are set to 1, which is equivalent to transmission probability compared with other three kinds of routing metric performance

  From Fig. 3a can be seen in the unrestricted case, when the node is at rest, the use of standard transmission probability as routing performance slightly higher than the use of hops, latency and ETX as routing standards of performance, because it is measured by the quality of the most accurate path; when the node is in motion, the use of hops as a routing standards of performance is best because it's the fastest response, able to adapt to the situation in constant motion node in Fig. 3b represents a four-way standard overhead kinds comparison experiment, ETX used as reference in the set of probe packets periodically to measure channel quality, TP and ETX also have used with a similar probe packets to measure channel quality in order to ensure fairness, hops and delay in the probe packets is set to do the same, but their detection package includes only the address of the source node, neighbor probe packet is received and no action, so overhead is relatively small

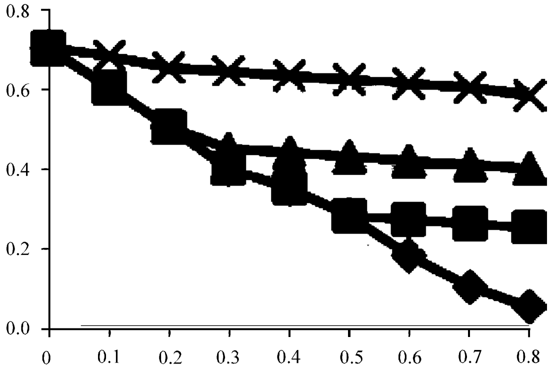

Fig. 4: Performance of detection and load balancing mechanism with different thresholds

- **Detection and load balancing mechanism performance:** Finally, we will detect and load balancing mechanisms combine analytical performance. Nodes initial energy is set to 30J, the network is in a dynamic environment

Since we set the node does not happen rational selfishness class 1, class 2 to consider here only selfishness Fig. 4 indicates that when the node type 2 selfish behavior, different subjective probability threshold β for forwarding network performance. When node's selfishness has degree above the threshold, it needs to be punished. as can be seen from the figure, by penalizing mechanism allows nodes SFP upgraded to allow threshold can improve network performance, but slightly lower than the beginning of SFP network is threshold, mainly because of selfish nodes with the corresponding period of being punished.

CONCLUSIONS

The study has proposed by selfish nodes affect the performance of the peer to peer network problem. The detection mechanism by allowing nodes to freely express their will achieve detection mechanism subjective forward. It is resulting in the routing path when it is necessary to consider other objective factors that determine the quality of the transponder capacity, but also consider selfish decision node along the subjective willingness to participate at the same time. The node energy factors are also taken into account, balanced energy and prolong the network lifetime.

REFERENCES

Charilas, D.E. and A.D. Panagopoulos, 2010. A survey on game theory applications in wireless networks. Comput. Networks, 54: 3421-3430.

Gui, C.M., Q. Jian, H.M. Wang and Q.Y. Wu, 2010. Repeated game theory based penalty-incentive mechanism in internet-based virtual computing environment. J. Software, 21: 3042-3055.

Wang, B., C.H. Huang, W.Z. Yang, F. Dan and L.Y. Xu, 2011. An incentive-cooperative forwarding model based on punishment mechanism in wireless ad hoc networks. J. Comput. Res. Dev., 48: 398-406.

Yoo, Y. and D.P. Agrawal, 2006. Why does it pay to be selfish in a MANET? IEEE Wireless Commun., 13: 87-97.

Yoo, Y., S. Ahn and D.P. Agrawal, 2010. Impact of a simple load balancing approach and an incentive-based scheme on MANET performance. J. Parallel Distrib. Comput., 70: 71-83.

Yu, Y.J. and H. Jin, 2008. A survey on overcoming free riding in peer-to-peer networks. Chin. J. Comput., 31: 1-15.