Quantifying Selfishness and Fairness in Wireless Multihop Networks

Normalia Samian, Winston K. G. Seah and Gang Chen
School of Engineering and Computer Science
Victoria University of Wellington, New Zealand
Email: {normalia.samian, winston.seah, aaron.chen}@ecs.vuw.ac.nz

***Abstract*—In wireless multihop networks, cooperation is of utmost importance to ensure the success of communication. However, due to limited resources especially energy, nodes may be compelled to adopt selfish behaviour by not forwarding packets for other nodes. Selfishness is a very subjective element to be measured because it is hard to determine whether or not a particular node's behaviour is intentional or a consequence of the environment. Most, if not all, published work assumed that this behaviour can be assessed but do not explicitly describe how selfishness is measured or quantified. In this paper, we propose a method to quantify a node's behaviour in forwarding packets for other nodes from the perspective of a single observer node (i.e. first-hand observation) and provide quantifiable metrics to represent the node's actual effort. We show that by using the proposed method, we are able to classify several types of selfishness and fairness behaviour.**

Index Terms*—*wireless multihop network, quantitative measure, forwarding behaviour, selfishness, fairness, cooperation.

I. Introduction

The effectiveness of wireless multihop networks very much depends on the willingness of participating nodes to transmit data for one another. Hence, cooperation plays a vital role in maximizing the success rate of data transfer in wireless multihop communications [1], [2]. However, this is not always the case where there exist some nodes that only want to cooperate if they benefit from their cooperative actions. These nodes, which are commonly known as *selfish nodes*, can jeopardize network operations. The selfish nodes are not necessarily malicious because in most cases, these nodes neither attack nor disrupt the network operation; they are just reluctant to cooperate since the act of doing so will consume their limited resources. Hence, there is a need to detect selfishness and take necessary actions to avoid degradation of network performance. Detecting selfish nodes may also help to identify nodes whose energy are depleting because lack of energy is one of the reasons for not cooperating in packet forwarding [3]. We could therefore adjust the operation of the network to ensure its continued healthy operation, like discovering new routes that comprise relay nodes with more energy. Differentiating a node under stress, due to excessive loads, from selfish nodes is sometimes difficult but this can be partially addressed by our scheme as we consider the input traffic to a relay node, when the information is available. Identifying a stressed node is not within the scope of this paper and problem can be alleviated by employing techniques like load-balanced routing [4].

Most, if not all, published work on cooperation stimulation approaches especially those targeting the network layer assume that selfish behaviour can be assessed but do not explicitly state how. In such cases, selfishness is determined based on a predefined threshold value of a single set of actions such as number of dropped packet and packet forwarding rate of a particular relay node for a requestor [5], [6]. E.g., the packet forwarding rate can be defined as follows [7]:

$$forwarding\,rate = \frac{number\,of\,packets\,forwarded}{number\,of\,packets\,received} \quad (1)$$

based on the total number of packets a node has successfully forwarded in comparison to the number of packets it has received regardless of how many arriving requests that it is handling. The forwarding rate is not determined based on how fast or prompt a relay node responds to any arriving requests where usually the duration of observation to evaluate the forwarding behaviour is not explicitly stated [8]. As such, when the forwarding rate does not meet certain threshold value (evaluated based on a first-hand observation), the node will be deemed as selfish and the behaviour state may either be kept for local reference or disseminated across the network for further action, such as, punishment or path avoidance.

In order to strengthen the selfishness evaluation based on first-hand observation, additional behaviour information is usually obtained from second-hand observation where opinions from other nodes are inquired based on their experiences dealing with the same relay node [5], [8], [9]. The opinions (which are assumed to be reliably evaluated) will then be collected to form evidence of a node's behaviour. This is where the issue of false judgement always occur such that the authenticity of the collected opinions can be questioned due to issues like collusion of nodes declaring forge behaviour or falsely praising a misbehaved node; this problem has been the focus of many existing selfishness detection schemes. To the best of our knowledge, one particular aspect has not been addressed in any existing cooperation stimulation approaches, specifically in determining the right level of cooperativeness/selfishness, by presenting a node's behaviour in a quantifiable form. This aspect will be further discussed in Section III.

In this paper, we propose a method to quantify a node's behaviour in order to derive its degree of cooperativeness/ selfishness. We evaluate the effort by measuring the packet forwarding rate of an observed relay node for different service

978-1-4799-0537-9/13/$31.00 ©2013 IEEE

requestors. The significant indicator is compare and measure, where comparison of effort (i.e. in term of how promptly the observed node forwards packets for different arriving requests) is made prior to measurement is carried out. Having said that, the degree of selfishness is not measured just based on a predefined threshold value of a single set of actions, such as, in Eqn (1) without taking into consideration other possible influencing factors like number of requests the observed node needs to serve simultaneously. Hence, we do not simply regard nodes that dropped packets or nodes that do not meet the forwarding threshold value as selfish because there are times when the act of dropping packets is unintentional due to resource constraint or heavy forwarding loads, thus leading to false judgement by labeling such a node as selfish. Consequently, a continuous false (positive) report about a particular node being selfish could lead to severe network performance degradation because it may be excluded from contributing its effort to the network. Our main contributions can be summarized as follows:

- Metrics to quantify selfishness based on a node's effort in forwarding data packets for requesting nodes;
- Application of (selfishness) metrics to evaluate a node's fairness in forwarding packets for different requestors;
- Classification of different types of selfish behaviour based on the analysis of several typical communication scenarios.

The desired metrics can be used to present a node's actual effort provided that all necessary elements (to be discussed in Section III provides) to establish effective quantification method exist.

The remainder of this paper is organized as follows. In Section II, we discuss related work on selfishness mitigation in wireless multihop networks. Section III provides motivation to quantify a node's effort accurately. We then focus on selfish behaviour that occurs in routing protocols in Section IV. The proposed method to quantify selfishness is presented in Section V followed by the results from our performance studies in Section VI before concluding in Section VII.

II. Related Work

Stimulating cooperation and discouraging selfishness have been extensively studied and the proposed approaches can be broadly classified into incentive-based and punishment-based. In incentive-based methods, incentive can be in the form of payment and reputation that reflects the condition of either profitable or non-profitable incentive. In payment schemes, each node holds some form of virtual credit which will be increased when it forwards packets for other nodes and decreased when it sends its own packets. A rational node would aim to maximize its credits by being cooperative so that it has sufficient credits to send its own packets. Examples of payment-based schemes that use credits to reward cooperative nodes are as proposed in [1], [10], [11].

However, these approaches assume the existence of a central agency to manage the credits transactions (e.g. reward and purchase), which is impractical in a totally distributed and decentralized wireless multihop environment. Reputation is another type of incentive used to stimulate cooperation in wireless multihop networks. A node collects past behavioural information on other nodes based on its own observations, reports from trusted neighbours, or both. The information, indicating their level of selfishness, is used to determine reputation levels of monitored nodes; a level that is lower than a predetermined threshold value simply reflects that a particular node is selfish thus will be avoided in the communication process. Early work on reputation schemes involved monitoring of nodes' activities using a watchdog mechanism [12] and the information gathered is used to rate the node such that a node receiving a low rating will be excluded from routing paths, with various improvements and extensions e.g. [5], [8], [13], [14], [15] as well as, trust establishment frameworks [9], [16], [17].

In trust-based mechanisms, a node collects the information of other nodes' behaviour and rates them with trust values. The punishment-based approach penalizes nodes that behave selfishly by isolating them from routing paths and not forwarding any packets sent by such nodes, to signal that selfish behaviour will not bring any benefit. Most apply the popular game theoretical Tit-for-Tat (TFT) [2], [18], [19]. In TFT strategy, a node will take similar action (i.e. cooperative or selfish) as what the other node has previously. The strategy is played in such a way that a node will be cooperative in the first game stage and subsequent action depends on the opponent's behaviour in the preceding stage. Besides being applied when selfish node has been detected, punishment is also a next step to be taken after node has been rated with low reputation value. Thus, reputation and punishment schemes always work hand in hand, and some of the works on reputation mechanisms described above can also be classified as punishment schemes.

While all the proposed schemes have assumed that selfishness is detectable, they have not explicitly stated how selfishness is actually measured. The focus has been on how to improve the efficiency of the proposed schemes where selfishness detection is assumed. Where some sort of behaviour measurement has been presented, it is based on single set of actions, as show in Eqn (1). This kind of measurement has been the basis of many existing schemes so far, especially for a node that relies on local observation where the information may not be sufficient to conclude that a particular observed node is selfish. How efficiently does each contributor or reputable node collect the selfishness information remains unaddressed, and simply assumed that a node's behaviour can be observed and assessed. This needs to be addressed prior to proposing any cooperation schemes but has mostly been neglected.

III. Quantification of A Node's Effort

Quantification here is defined as an explicit measurement of a node's behaviour that is done by any observing node. Explicit measurement means that a node's behaviour is to be observed, evaluated and assigned with quantifiable metrics that is reflective of the effort demonstrated by that node. Common practice that has been applied in many cooperation stimulation

schemes is to represent a node's behaviour as either good (cooperative) or bad (selfish) without actually stating the level of effort that a node has contributed. The classical watchdog mechanism [12] that has widely been applied in many existing behaviour detection schemes presents a node's behaviour in the form of bit value "0" for selfish node or "1" for cooperative node. Presenting a node's behaviour based on the final decision of an observer node does not reflect the actual level of effort that an observed node has put in, where the evaluation may have not been fairly done. This is especially true when information about selfish behaviour is obtained based on reliance on global reports where a node may perceives that the shared information is correct without getting proper validation on any accusation of misbehaviour or claim of good behaviour of a particular observed node. Without considering the actual effort put in by the node, the observed behaviour may not be accurate. Hence, it is important to have quantifiable metrics that adequately reflects the effort of a particular node rather than just reporting behaviours in binary form, viz. good or bad. This measurement should portray a node's effort where the important elements that must be taken into consideration (if availability is possible) can include:

i) Level of forwarding load that a relay node is handling, e.g. number of connections;
ii) Rate of forwarding effort that a relay node offers to every incoming connection from other nodes;
iii) Rate of packet transmission of other nodes requesting services from the same relay node; and,
iv) Sufficient amount of time to observe and assess a node's behaviour.

These elements are imperative aspects that could assist in obtaining accurate node's behaviour information. With the randomness nature of wireless multihop networks, such information may not be easily obtained but quantification must be made such that the behaviour label can be fairly assigned. The metrics that we are proposing in our study is similar to the E-model that has been applied in Voice over IP (VoIP) as a measure of voice quality [20], [21], [22]. In VoIP, the voice quality is measured based on subjective testing of human's perception towards the speech quality. Hence, the E-model provides a numerical representation of the voice quality by producing a measurement output called an R-Value that is calculated based on elements like delay, jitter and data loss [23] and applied to rate the quality of voice.

Equivalently, from the perspective of wireless multihop nodes evaluating other nodes' effort, having quantifiable metrics of a node's behaviour that enables an observing node to assess the degree of selfishness or cooperativeness a particular node has shown could reflect its actual credibility in the network. The metrics provide flexibility for other nodes to have their own interpretation and let them decide as to whether or not certain level of node's behaviour is sufficient for them rather than getting pre-judged information. A significant challenge in achieving this goal is ensuring the existence of necessary elements or parameters for accurate quantification of a node's behaviour. In the event that required elements are absent, alternative solutions will be considered.

IV. Selfishness in Routing

In routing protocols, packet forwarding is the most fundamental task that must be carried out by nodes in order to ensure the completion of any initiated communication process. However, due to resource constraints, the seemingly simple forwarding process might not be achieved if packets are dropped because the process consumes forwarder's energy [3] without bringing any direct benefit to the forwarder. The risk of energy depletion has given rise to selfishness in routing that leads to degradation of service. In this paper, we will discuss selfish behaviour from the perspective of communication process using, as example protocol, the Ad hoc on-Demand Distance Vector (AODV) routing protocol, which has been ratified by the Internet Engineering Task Force (IETF) [24]. However, our mechanism is fairly general and can be applied to any other routing protocol.

A. AODV Routing Protocol

In the AODV routing protocol, control packets such as route request (RREQ) and route reply (RREP) messages are disseminated across the network whenever a particular node intends to setup a route for transmitting data to its desired destination. An RREQ is broadcasted every time a node would like to setup a new routing path to a destination or if the previously established route has expired. It is thus essential for intermediate nodes to assist in disseminating the RREQ until the path to the intended destination is found and an RREP unicasted back to the source node to establish a bidirectional routing flow prior to actual data transmission. This process can only be successfully accomplished if all nodes cooperate and participate in the forwarding of these control messages.

B. Selfishness in AODV

Several scenarios of selfishness occurring in AODV include:

i) Nodes do not forward the received RREQ messages to their corresponding next hops, the established route does not pass through these nodes;
ii) Nodes do not generate RREP messages in response to RREQs for destinations that they have routes to, or do not assist in unicasting RREPs back to source to complete the route setup process;
iii) Nodes do not advertise Route Error (RRER) messages when link error is detected or whenever necessary, causing other nodes to be unaware of the current faulty state, thus wasting energy transmitting packets that could not reach their intended destinations;
iv) Nodes assist in route setup but do not transmit data packets because they are only interested to use the established route for their own transmission, thus data packets from other nodes do not reach their destinations.

The aforementioned examples of selfish behaviour can arise in real networks and require effective measures to mitigate the adverse effects. While many existing works have been focusing

on misbehaving node detection during route discovery [25] which reflects more obvious selfish behaviour, we aim to detect a more challenging selfish behaviour as described in scenario (iv); such a node can easily switch between cooperative and selfish behaviour to manipulate the routing protocol for its own benefits and ensure that other nodes regard it as trustworthy. Nodes can also exhibit selfish behaviour towards some nodes and not others, resulting in unfairness among nodes.

V. Quantifying A Node's Effort in Packet Forwarding

In this paper, we propose a method to measure the effort of a particular node based on how promptly it is in forwarding packets for different requesting nodes. We aim to use this method to measure the level of selfishness exhibited by a node so that the appropriate decision can be made to classify a node as being selfish or not. Our approach is to rely on the use of the passive acknowledgement mechanisms [12], which requires the observing node to monitors its neighbours' behaviour via promiscuous listening of its neighbours' transmissions, a feature that is widely available with existing wireless communication technologies, like, IEEE 802.11 or WiFi [26]. In addition, we also assume that data transmission is reliable along the routing path with the utilization of channel coding and retransmission mechanisms.

In our design, we assume that the observing node is a well-behaved node that will cooperatively forward packets for its corresponding neighbours. We consider a network scenario where a node (i.e. observing node) that initiated a communication process would like to identify which of its neighbouring nodes sharing the same wireless transmission medium exhibit selfish behaviour. We evaluate the effort by measuring and comparing the observing node's sending rate and the forwarding rate of data packets by the observed node for different requestors. In the following subsections, we describe the design and theoretical basis of the proposed quantification method.

A. Collection of Behaviour Information

In AODV, each node can only monitor or listen to nodes that are within its transmission range to collect local observed information about the behaviour of its neighbours. The adopted monitoring approach in our study is fundamentally similar to [12] except that the information requestor does not rely on other nodes to play watchdog role. The evaluated behaviour is judged based on how promptly a node forwards data packets for requesting nodes and will be divided into several categories:

a) *Fairly cooperative node* - the node is cooperative by forwarding arriving packets and fairly distribute its effort towards different nodes at satisfactory demand level (based on cooperativeness metrics);
b) *Unfairly cooperative node* - the node is cooperative but not providing equal levels of service to different nodes;
c) *Fairly uncooperative/selfish node* - the node is uncooperative by not forwarding packets at satisfactory rate and equally shows its selfishness towards any arriving nodes' requests.

In order to evaluate the proposed quantification mechanism, we consider two scenarios of a simple network topology. Our focus is on how to obtain efficient behaviour information based on the perspective of a single node where information need not be shared with other nodes. This localized and distributed approach makes the mechanism scalable to larger networks without the need to have reliable information from other parts of the network.

The first scenario caters for an observing node that is located within the same wireless transmission range of another node that will forward packets through the same relay node as shown in Fig. 1. There are two data packet flows between source-destination pairs that consist of source nodes, S_i and S_j and corresponding destination nodes D_i and D_j, passing through a common relay node, R. For this scenario, we first assume that source nodes S_i and S_j send data packets at the same rate where each link has a transmission rate of one packet per unit time and optimal scheduling is applied. It is also assumed that both S_i and S_j know the information of each other's flow, such as, the flow identifier (ID) and source and destination addresses. In this scenario (Fig. 1) source node S_i is the monitoring node and listens to the forwarding actions taken by relay node R towards its packets in comparison to the packets sent by node S_j. The data packet arrival at the next hop follows an arbitrary inter-arrival time distribution. The source node S_i starts sending data at time t and will wait for a specified observing time, w_n, to determine whether its data packet gets forwarded by its next hop neighbor R. An extended time, e_n is introduced as an additional observing time when the next hop neighbor R is also handling packets from other nodes, to avoid making a wrong judgement of forwarding misbehaviour for a relay node that is handling heavy loads. The total observation time can be expressed as:

$$T_n = w_n + e_n \tag{2}$$

where n denotes the n^{th} flow that arrived at the relay node. The value of e_n is determined based on the number of known overheard packets that need to be handled by R. For this case, assuming d known data packets (including S_i's own packet) have arrived at relay node R, then the extended time e_n is:

$$e_n = w_n \times (d - 1) \tag{3}$$

In determining e_n, we are aware of the fact that node S_i may not necessarily have heard the accurate number of packets that are handled by node R correctly but this issue is not within the current scope of this paper. Hence, the total observing time T_n is an estimation based on the number of most overheard other data packets that have arrived at node R. Timeout occurs when the total time spent for waiting has exceeded T_n. In this case, node observes how long the relay node R will hold its data packet prior to forwarding (or possibly dropping) the packet and evaluate the relay node's effort based on (1) duration of time that it takes to forward the data packets in comparison

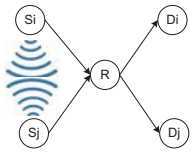

Fig. 1. Two flows scenario where source nodes are within the same wireless transmission range (scenario one).

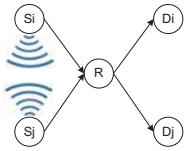

Fig. 2. Two flows scenario where source nodes are not within the same wireless transmission range (scenario two).

to other nodes' packets and (2) total number of data packets it has forwarded. Next, the second scenario uses the same 5-node network topology except that the two source nodes are not within wireless transmission range of each other, as shown in Fig. 2.

Under such a condition, the observing node S_i would not be able to promiscuously listen to the activities performed by node S_j. Hence, information like packet transmission rate of node S_j cannot be acquired by node S_i to compare with its own rate. In addition, the ideal assumptions that have been made in scenario one, such as, nodes send packets at the same rate and know each other's information flow no longer apply. However, such limitation (which is an open problem in wireless networks) would not actually hinder the quantification as node S_i is still able to listen to any active forwarding activities performed by node R for other requestor nodes. All of the equations stated above are still applicable when it comes to dealing with this kind of random scenario. The only difference is that the e_n value is abstractly formulated based on the overhearing of node R's forwarding activities for other nodes without knowing the identities and total number of nodes that R needs to handle. Under such conditions, e_n can be assigned when there is at least one known service requestor competitor (regardless of its sending rate) that node R is handling and comparison is made based on how fairly and promptly node R dispenses its forwarding effort towards arriving requests from both source nodes.

B. Measuring Selfishness and Fairness

Selfishness, or conversely, cooperativeness, is represented by a relay node's effort in forwarding packets for other nodes and this is measured by comparing its forwarding rate with the rate it receives packets from nodes requesting its service. Fairness measures a node's ability to fairly distribute its effort as equally as possible among the other nodes. For simplicity, we divide the fairness level into good and bad fairness where good fairness indicates that the relay node is being fair to all requestors, while the bad fairness means that relay node is selectively bias towards node(s) of its preference in terms of number of data packets being forwarded and the duration of time it takes to forward the packets.

1) Rate of data packets forwarded by relay node: The rate of data packets forwarded is determined based on the measurement of rate of change between two parameters, viz., the number of data packets forwarded (y) and time (t). The aim is to determine the relationship between the two quantities, whereby the number of data packets forwarded is increasing over time forms a non-decreasing function, which we denote by $y = f(t)$. Therefore, the average rate of change of data packets being forwarded at time t can be derived from the gradient of the function at t. The purpose of calculating the gradient is to determine fairness of the relay node R in terms of how fast it forwards data packets for different requestors. In this particular scenario, the gradient or average rate can be measured as follows:

$$V = \frac{\triangle f(t)}{\triangle(t)} \tag{4}$$

As a node's behaviour is stochastic in nature, the function does not have a constant rate of change, and we use the instantaneous rate of change as the indicator.

2) Correlation coefficient of rate of data packets transmitted by sender and relay node: Correlation coefficient is a statistical measure to evaluate the relativity of two variables. In our case, the input variables are the slope values or the instantaneous rate of change for source and relay nodes' forwarding record at different points of time. We look at how these two variables are strongly or weakly related to each other as a reflection of how cooperative or selfish the forwarding behaviour of relay node R is. We denote the rate at which source nodes are sending data packets and the rate at which relay node R is forwarding the packets as $y_1 = g(t)$ and $y_2 = h(t)$ respectively. Given the set of (y_1, y_2) pairs, we compute the correlation coefficient, r, values by using the following equation, where n is the number of observations:

$$r = \frac{n(\sum y_1 y_2) - y_1 y_2}{\sqrt{n(\sum {y_1}^2) - (\sum y_1)^2} \cdot \sqrt{n(\sum {y_2}^2) - (\sum y_2)^2}} \tag{5}$$

If the correlation coefficient value is close to 1, it means that there is a strong positive linear relationship between y_1 and y_2 whereas 0 value depicts no linear relationship among the two values. We propose an example classification of correlation coefficient values to represent different level of cooperativeness and selfishness, as shown in Table I. Based on the two criteria described above, we carry out comparison to measure node's selfishness and fairness metrics as depicted in Table II.

TABLE I
COOPERATIVENESS/SELFISHNESS METRICS

Correlation	Cooperativeness Level
$0.9 < r \leq 1.0$	Very highly cooperative
$0.7 < r \leq 0.9$	Highly cooperative
$0.5 < r \leq 0.7$	Moderately cooperative
$0.3 < r \leq 0.5$	Low cooperative (i.e. highly selfish)
$r \leq 0.3$	Very low cooperative (i.e. very highly selfish)

VI. EVALUATION

This section discusses the evaluation of the proposed quantification method based on two network topologies as shown in Fig. 1 and Fig. 2. We assume that all nodes cooperatively participate in the route discovery process and that a routing

TABLE II
SELFISHNESS AND FAIRNESS MEASUREMENT

Behaviour	Comparison Parameters	Index Measurement	Threshold Value
Selfishness	Sending rate of a node vs. forwarding rate of relay (S_i vs. RS_i; S_j vs. RS_j)	Difference between slope values of the compared parameters	Percentage of slope value difference $> 50\%$ denotes significant selfish behaviour
		Correlation coefficient value between the compared parameters	Refer to Table I
Fairness	Forwarding rates of relay node for different requestors (RS_i vs. RS_j)	Difference between slope values of the compared parameters	Percentage difference $> 50\%$ reflects an unfairness of relay node R.
		Difference between correlation coefficient value of selfishness parameters	Percentage difference of correlation coefficient $> 50\%$ denotes unfairness of relay node R.

TABLE III
SIMULATION PARAMETERS

Parameters	Value
Protocol	AODV
Simulation Time	200 seconds
Traffic Source	CBR
Packet Size (bytes)	512
Channel Capacity	2MB/s
Total Packet Sent	100
Network Topology	Static linear
Number of nodes	5
Radio Propagation Range	250 meters

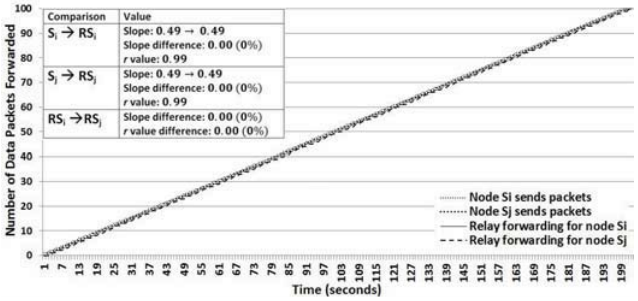

Fig. 3. Fairly Cooperative Node.

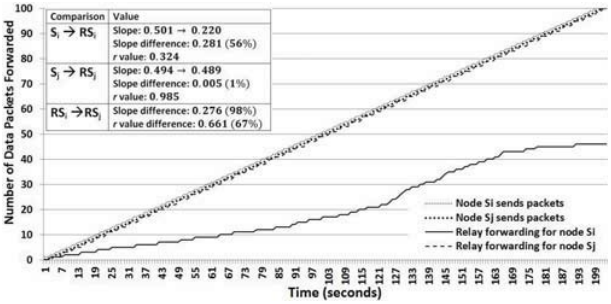

Fig. 4. Unfairly Cooperative Node.

path is available for requesting nodes. Observation starts with the transmission of data packets where every overheard data packets that arrived at relay node R will be recorded in a monitoring buffer and counted to determine the total observation time T_n that needs to be allocated. At the same time, the observing node S_i will also record the forwarding activity of relay node R for source node S_j. In this paper, our focus is on how to obtain efficient behaviour information based on the perspective of a single node (i.e. first-hand observation) where global information on other nodes' behaviour is not required in order to ensure that the approach is scalable [27]. We have used a simple network topology comprising 5 nodes to validate our proposed mechanism and the same observation approach can be applied to any other observer nodes. Each node in the network can perform the same observation procedure to collect local information on neighbouring nodes' behaviour (that need not be shared with other nodes) regardless of network density.

In our study, Qualnet simulator has been used to evaluate the applicability of the proposed mechanism on AODV routing protocol. The simulation parameters used are as shown in Table III.

A. Simulation Results

The proposed method is evaluated through several scenarios based on the following main network conditions:

1) Amount of traffic introduced to the relay node has no variations: In this situation, node S_i and S_j know the information of each other's flow and send data packet at the same rate. Based on this network condition, the first scenario to be considered is where relay node R cooperatively and fairly forwards packets for both nodes S_i and S_j. As shown in Fig. 3, the forwarding rates by the sending nodes and relay coincide with one another. A slope value of 0.49 was obtained for all four forwarding rates showing good fairness displayed by relay node R for both source nodes S_i and S_j.

Similarly, the almost equivalent gradients for each source node's transmission and relay node's forwarding packets reflects a good cooperative behaviour of R. This is strongly supported by correlation coefficient, r values for both forwarding traces of about 0.99, which is significantly high and very close to 1, reflecting very highly cooperative behaviour. Hence, in such a scenario, it can be concluded that relay node R is a fairly cooperative node based on the equivalent slope values obtained and the 0% of gaps between slope and r value difference for both requestor nodes.

Next, we consider the case where relay node R exhibits approximately 50% cooperative behaviour towards source node S_i but offers 100% cooperative forwarding behaviour for node S_j and show how we can quantify this scenario. From the slope values shown in Fig. 4, the rate at which relay node R is forwarding packets for node S_j is almost similar with the rate it receives packets from it, whereas the forwarding rate of relay node R for node S_i shows difference of 56% that indicates selfish behaviour according to Table II. In addition, by looking at the correlation coefficient values, r for nodes S_i

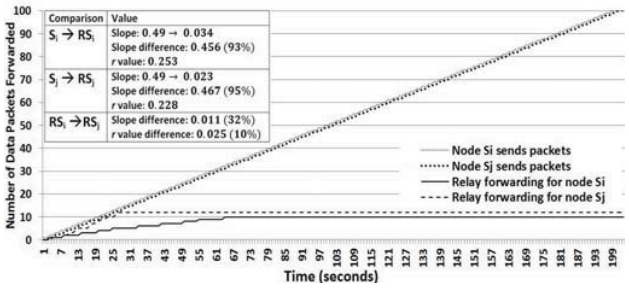

Fig. 5. Fairly Uncooperative Node.

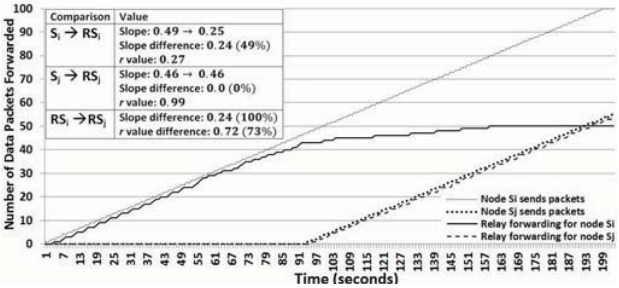

Fig. 6. Unfairly Cooperative Node (Random Sending Rate).

and S_j, which are 0.324 and 0.985 respectively, a difference of 67% that reflects unfairness by R (which is also strengthened with 98% of slope difference value). In this particular scenario, it is not conclusive to say that relay node R is totally selfish considering that it has put in approximately 50% effort to forward data packets for node S_i. However, it is obvious that relay node R is favouring S_j. As previously mentioned, the subsequent actions undertaken by nodes, such as punishment, are based on the adopted policy of the network and beyond the scope of this paper. This is an example of a scenario where if node S_i reports to other nodes that relay node R is being selfish by not diligently forwarding its data packets, then node S_i maybe regarded as lying since node S_j will not be giving the same evaluation of R. Thus, any subsequent report from node S_i towards R might end up being disputed by other nodes having received good cooperation from R.

We now examine the scenario where relay node R exhibits selfishness towards both nodes S_i and S_j. Fig. 5 shows R only forwarded up to 10 to 12 data packets at the beginning prior to stopping its transmission for both nodes. In this kind of scenario, relay node R is unfair in terms of not forwarding data packets at the rate that the two nodes are sending their packets where average rate of change is 0.034 for for node S_i and 0.023 for node S_j. The values show that the forwarding rates for both nodes are very low and worsen by the fact that the rates decreased to 0 when the forwarding process stops after some time, indicating uncooperative behaviour. However, by looking at the r values' small percentage difference of about 10% and also slope difference of 32%, we can say that relay node R is fair, albeit giving equally bad treat to both requestors. Hence, this kind of node behaviour can be labeled as fairly uncooperative (i.e. selfish.)

2) New traffic is being introduced to the relay node creating randomness: Catering for the category of behaviour where a node is unfairly cooperative, this section will show how such classification can still be carried out given a more random network condition. As opposed to the network scenario shown in Fig. 1, in this case, nodes S_i and S_j know the information of each other's flow but do not send data packet at the same rate. Hence, the next evaluated scenario still caters for the nodes' condition illustrated in Fig. 1 but packet sending rates of nodes S_i and S_j are random. In this scenario, node S_i sends data packets earlier than node S_j and node R shows good cooperative behaviour by promptly forwarding the packets sent by node S_i. However, upon receiving node S_j's request to forward its packets, node R starts to slow down its forwarding rate for node S_i. As shown in Fig. 6, node R starts to favour node S_j more than node S_i even though it shows good cooperative behaviour towards node S_i initially. Given the 0.27 correlation coefficient value that indicates very low cooperative behaviour, node R may be labelled as selfish by node S_i.

However, from the perspective of node S_j, node R is a good cooperative relay node for its forwarding rate that is always close to the rate of node S_j's sent packets. This kind of behaviour shown by node R can be classified as unfairly cooperative behaviour. However, if node S_i disseminates a bad report on node R, the report might be disputed by node S_j and S_i may be accused as giving a false report. This is one of the examples where reliance on single set of actions is not sufficient without making fair comparison in judging other node's behaviour. Hence, by presenting a more concise and precise report node S_i could avoid being accused of lying. Hence, given this random scenario, quantification of relay node's effort can still be measured within a shorter period of time as long as the required information is available.

3) Incomplete information and random rate of traffic: Following the previous network scenario where relay node R is being unfairly cooperative, deeper investigation has been made with some information being omitted to see whether or not the same behaviour can be quantified. Under this kind of network condition, as shown in Fig. 2, a more random network scenario has been analyzed where node S_i and S_j do not have any information of each other's flows and do not send data packets at the same rate. Hence, the packet sending rate of node S_j is unknown and cannot be compared with the sending rate of node S_i. Given this lack of information, assessment of the relay node R's effort has to be performed based on the difference between the forwarding rate offered by node R towards node S_i and S_j where the slope of these two values are measured and compared.

As depicted in Fig. 7, when new traffic from node S_j comes, relay node R starts to divert its cooperative effort away from node S_i. In this scenario, node S_i could not determine the rate of sending packets carried by node S_j and with that piece of information missing, the only information that can help node S_i in comparing the effort is based on the forwarding

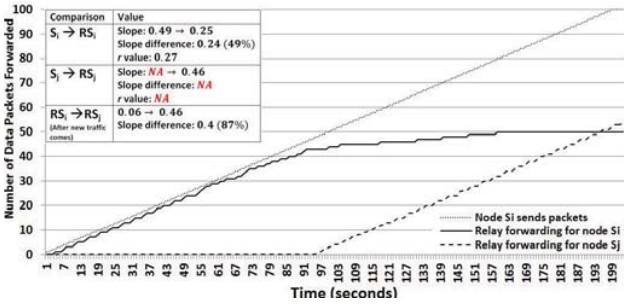

Fig. 7. Unfairly Cooperative Node (Incomplete Information).

rates offered by node R to node S_i and node S_j. As shown, once the service request from node S_j arrived, the slope of forwarding rate for node S_i has dropped to 0.06 that makes the overall slope of forwarding rate go down to 0.25; almost half the expected slope value of 0.49. Having the ability to listen to the forwarding activity performed by node R for node S_j, node S_i could record that the forwarding slope for node S_j is 0.46. In this case, node S_i cannot fully claim that node R is being highly cooperative towards node S_j since node S_i would not be able to evaluate just how promptly node R is in forwarding node S_j's packets. However, having node R still actively forwarding packets for node S_j with 0.46 slope value as opposed to 0.06 value for node S_i that contributes to a percentage difference of 87%, shows that node R is being unfair toward S_i.

It is obvious that with some information lacking, quantification is affected such that a complete conclusion on a node's behaviour cannot be confirmed. Hence, this is one of the major challenges that needs to be catered as part of our upcoming research direction, that is, to provide as sufficient as possible the information required to perform the quantification process and accurately label a node's true behaviour.

VII. Conclusion

In this paper, we have proposed a method for quantifying node selfishness based on its forwarding behaviour in wireless multihop networks. Based on the proposed quantification method, we are able to classify a node's behaviour into several categories of selfishness and fairness that can be used to better assess a node's behaviour. Unlike most existing schemes where selfishness is measured based on a predefined threshold value of single set of actions, we do not simply label a node as selfish without considering its effort in forwarding packets for different arrival requests. This can avoid making a false accusation on a node's behaviour arising from a fair balance between the efforts shown and the loads handled. Our main goal in this paper is to provide an accurate way to determine the metrics of a node's behaviour based on standardized computation even though interpretation of the output may vary. Our quantification method can be integrated into many existing selfishness detection schemes to assist in obtaining strong evidence of selfish behaviour. For example, in order to label certain node as selfish, an observer node needs to support its claim by presenting the selfishness and fairness metrics together with other supporting information.

There are several potential extensions to this study. Firstly, catering for the scenario of more than two preceding nodes $S_1, S_2, ..., S_n$ sending packets through the relay node R, extending the approach to larger network topologies, and analyzing the loss model. Secondly, the current evaluation of selfishness and fairness is solely based on local observation where the selfishness information obtained is used autonomously and we have not taken into consideration exchanging information with other nodes. Last but not least, the monitoring mechanism that we utilized is based on a node implicitly observing other nodes' behaviour using the promiscuous listening mode of wireless communication. Although the approach can provide the necessary information, it is based on assumption that the channel is sufficiently reliable. However, that is not necessary the case in reality because of the weaknesses of the promiscuous listening [12]. When communication channel is unreliable, game theoretical approach of imperfect/perfect public/private monitoring seems to be a promising direction for our future research [18].

References

[1] L. Buttyan and J.P. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," *Mobile Networks and Applications*, vol. 8, no. 15, pp. 579-592, 2002.

[2] F. Milan, J. J. Jaramillo, and R. Srikant, "Achieving cooperation in multihop wireless networks of selfish nodes," in *ACM Workshop on Game Theory for Communications and Networks*, 2006, pp. 1-10.

[3] K. Balakrishnan, J. Deng, and P.K. Varshney, "TWOACK: Preventing selfishness in mobile ad Hoc networks," in *Proc. of IEEE Wireless Communications and Networking Conference (WCNC)*, 2005, pp. 2137-2142.

[4] X. Wang, S. Tagashira, and S. Fujita, "FDAR: A Load-Balanced Routing Scheme for Mobile Ad-Hoc Networks", in *Proc. of ADHOC-NOW*, Lecture Notes in Computer Science, Volume 4686, 2007, pp 186-197.

[5] P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proc. of 6th Joint Working Conference on Communications and Multimedia Security*, 2002, pp. 107-121.

[6] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," *Technical Report cs.NI/0307012*, Computer Science Department, Stanford University, USA, July 2003.

[7] Q. He, D. Wu, and P. Khosla, "SORI: A secure and objective reputation based incentive scheme for ad hoc networks," in *Proc. of IEEE Wireless Communications and Networking Conference (WCNC)*, 2004, pp. 825830.

[8] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the CONFIDANT protocol," in *3rd ACM International Symposium on Mobile Ad hoc Networking & Computing*, 9-11 June 2002, pp. 226-236.

[9] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "A quantitative trust establishment framework for reliable data packet delivery in MANETs," in *3rd ACM Workshop on Security of Ad hoc and Sensor Networks*, 7 November 2005, pp. 1-10.

[10] L. Blazevic, L. Buttyan, S. Capkun, S. Giordano, J. P. Hubaux, and J. Y. Le Boudec, "Self-Organization in mobile ad-hoc networks: the approach of terminodes," *IEEE Communications Magazine*, vol. 39, no. 6, pp. 166-174, 2007.

[11] S. Zhong, Y. R. Yang, and J. Chen, "Sprite: A simple, cheat proof, credit-based system for mobile ad hoc networks," in *IEEE INFOCOM*, 1-3 April 2003, pp.1987-1997.

[12] S. Marti, T. J. Giuli, K. Lai, and M., Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *6th Annual International Conference on Mobile Computing and Networking*, 6-11 August 2000, pp. 255-265.

[13] M. T. Refaei, V. Srivastava, L. DaSilva, and M. Eltoweissy, "A reputation-based mechanism for isolating selfish nodes in ad hoc networks," in *Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services*, 17-21 July 2005, pp. 3-11.

[14] J. J. Jaramillo and R. Srikant, "DARWIN: Distributed and adaptive reputation mechanism for wireless ad-hoc networks," in *13th Annual ACM International Conference on Mobile Computing and Networking*, 2007, pp. 87-98.

[15] D. E. Charilas, K. D. Georgilakis, and A. D. Panagopoulos, "ICARUS: hybrId inCentive mechAnism for coopeRation stimUlation in ad hoc networkS," *Ad Hoc Networks*, vol. 10, no.6, pp. 976-989, 2012.

[16] A. A. Pirzada and C. McDonald, "Establishing trust in pure ad-hoc networks," in *27th Australasian Conference on Computer Science*, 2004, pp. 47-54.

[17] T. Ghosh, N. Pissinou, and K. Makki, "Towards designing a trusted routing solution in mobile ad hoc networks," *Journal of Mobile Networks and Applications*, vol. 10, no. 6, pp. 985-995, 2005.

[18] S. K. Ng and W. K. G. Seah, "Game-theoretic approach for improving cooperation in wireless multihop networks," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 40, no. 3, pp. 559-574, 2010.

[19] B. Niu, H. V. Zhao, and J. Hai, "A cooperation stimulation strategy in wireless multicast networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 5, pp. 2355-2369, 2011.

[20] R. G. Cole and J. H. Rosenbluth, "Voice over IP performance monitoring," *ACM SIGCOMM Computer Communication Review*, vol. 31, no. 2, pp. 9-24, 2001.

[21] J. Q. Walker, "Assessing VoIP Call Quality Using the E-model," *NetIQ Corporation*, 2002.

[22] A. P. Markopoulou, F. A. Tobagi, and M. J. Karam, "Assessing the quality of voice communications over internet backbones," *IEEE/ACM Transactions on Networking*, vol. 11, no. 5, pp. 747-760, 2003.

[23] "The E-model: A Computational Model for Use in Transmission Planning," *ITU-T Recommendation G.107*, Dec. 1998.

[24] C.E. Perkins and E. M. Belding-Royer, "Ad hoc on demand distance vector (AODV) routing," in *IETF Internet-Draft (RFC 3561)*, 2003.

[25] B. Wang, S. Soltani, J. K. Shapiro, and P.-N. Tan, "Local detection of selfish routing behavior in ad hoc networks," in *8th International Symposium on Parallel Architectures, Algorithms and Networks*, 7-9 December 2005, pp. 392-399.

[26] IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Nov. 1997. P802.11.

[27] M. K. Denko, "Detection and prevention of Denial of Service (DoS) attacks in mobile ad hoc networks using reputation-based incentive scheme," *Journal Systemics, Cybernetics and Informatics*, vol. 3, no. 4, pp. 1-9, 2005.