Game-Theoretic Approach for Improving Cooperation in Wireless Multihop Networks

See-Kee Ng and Winston K. G. Seah, *Senior Member, IEEE*

***Abstract*—Traditional networks are built on the assumption that network entities cooperate based on a mandatory network communication semantic to achieve desirable qualities such as efficiency and scalability. Over the years, this assumption has been eroded by the emergence of users that alter network behavior in a way to benefit themselves at the expense of others. At one extreme, a malicious user/node may eavesdrop on sensitive data or deliberately inject packets into the network to disrupt network operations. The solution to this generally lies in encryption and authentication. In contrast, a rational node acts only to achieve an outcome that he desires most. In such a case, cooperation is still achievable if the outcome is to the best interest of the node. The node misbehavior problem would be more pronounced in multihop wireless networks like mobile *ad hoc* and sensor networks, which are typically made up of wireless battery-powered devices that must cooperate to forward packets for one another. However, cooperation may be hard to maintain as it consumes scarce resources such as bandwidth, computational power, and battery power. This paper applies game theory to achieve collusive networking behavior in such network environments. In this paper, pricing, promiscuous listening, and mass punishments are avoided altogether. Our model builds on recent work in the field of Economics on the theory of imperfect private monitoring for the dynamic Bertrand oligopoly, and adapts it to the wireless multihop network. The model derives conditions for collusive packet forwarding, truthful routing broadcasts, and packet acknowledgments under a lossy wireless multihop environment, thus capturing many important characteristics of the network layer and link layer in one integrated analysis that has not been achieved previously. We also provide a proof of the viability of the model under a theoretical wireless environment. Finally, we show how the model can be applied to design a generic protocol which we call the Selfishness Resilient Resource Reservation protocol, and validate the effectiveness of this protocol in ensuring cooperation using simulations.**

***Index Terms*—Bertrand oligopoly, cooperation, game theory, wireless multihop networks.**

I. Introduction

TRADITIONAL networks assume that network entities or nodes can be designed to have well-defined behaviors and coordinate accordingly to ensure certain network goals are met. The goals which generally arise from the interest of the network operator or the network users at large, can be the optimized use of network resources or the quality of service (QoS) provided to the end users. These goals, however, may not be commonly shared by an individual end user who would always prefer to have better network access, even at the expense of other users. Such selfish behavior has been reported on rogue Transmission Control Protocol sources that do not respond to Explicit Congestion Notification [1].

The increasingly popular wireless networks are much more vulnerable to node misbehavior than the traditional wired networks, particularly the infrastructureless wireless networks like mobile *ad hoc* networks and wireless sensor networks which do not depend on any wired backbone but on members of the network to route packets for one another wirelessly, over multiple hops. Wireless multihop networking is also used to provide access to nodes that are beyond the direct communication range of access points connected to the wired infrastructure. One example of such applications is the rooftop networks [2].

We focus on the problem of selfish behavior in wireless multihop networks as there is a potential for such behavior to occur in the emerging fourth generation networks where communications is envisaged to span multihop wireless links, across nodes that may subscribe to different providers. Selfish behavior and competition at the medium access control layer have been studied by [3] and [4]. In the network layer, the assumption of cooperative relaying of packets among nodes to reach destinations that are beyond the wireless transmission range is no longer valid when nodes exhibit selfish behavior. Helping other nodes consumes precious resources, such as battery power, which is costly and nonbeneficial to a node. Without suitable incentives to encourage nodes to cooperate, most existing protocols that assume cooperation are likely to fail. Pioneering work on mitigating node misbehavior in the routing layer [5]–[8] has highlighted the problem of selfishness and proposed basically two approaches to solve the problem: pricing and watchdog cum punishment. Subsequent efforts have not deviated far from these approaches but have tried to align toward game theory.

Adopting pricing as a solution in [9]–[11] gives rise to the reliance on a central bank or a tamperproof counter, which limits the practicability particularly for a purely infrastructureless network. Punishment methods based on repeated games, proposed by [12]–[15], require the monitoring of transmission activities in the neighborhood, usually through promiscuous listening. Depending on the protocol layer of interest, it is typically unviable for a computationally resource-limited node to process all packets overheard on a high data rate link. Due to its difficulty, coordinating punishment in a multihop environment has been neglected, without which punishments and deviations become indistinguishable. Another major drawback in many punishment schemes is the need for the whole or a large portion of the network to participate in the punishment of one deviating node

Manuscript received December 30, 2008; revised October 21, 2009 and December 17, 2009. First published March 4, 2010; current version published June 16, 2010. This paper was recommended by Associate Editor T. Vasilakos.

S.-K. Ng is with Singapore Technologies Kinetics, Singapore 619523 (e-mail: seekee.ng@gmail.com).

W. K. G. Seah is with the School of Engineering and Computer Science, Victoria University of Wellington, Wellington, 6140, New Zealand (e-mail: winston.seah@ecs.vuw.ac.nz).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSMCB.2010.2042593

making it too severe, inefficient and opens a security hole for denial of service attacks. Considering the unreliable nature of the wireless link, and that most reported work considered only isolated components of the protocol stack, an integrated approach addressing both routing and packet forwarding has been proposed by [16]. Despite the increasing application of game theory in wireless multihop networks, the available results do not adequately model the wireless multihop environment.

In this paper, we apply the theory of imperfect private monitoring in game theory, and through the adaptation and reinterpretation of Aoyagi's game of imperfect private monitoring and communication for the Bertrand oligopoly [17], transform the problem into a wireless multihop game model. While the oligopoly model has been extensively used to study pricing in cognitive radio networks, e.g., [18], work on wireless multihop (relay) networks are just emerging [19]. Our model assumes that routing information is being disseminated in the network with packet loss information which aggregates various wireless transmission errors and buffer overflows. At each node, threshold-based reporting for the receive packet count of a flow occurs at regular periods of the game. This threshold is derived from the packet loss of the participating relay nodes of a flow. The report carries a message that acknowledges the reception of packets from a flow falling below or reaching above the threshold. The model further proves that deviation from the disseminated packet loss information or from an optimum reporting threshold is nonprofitable, thus ensuring truthful routing information dissemination and packet acknowledgments. By obeying the announced packet loss, a node is also participating in the packet forwarding function of the routing layer (at a promised quality). This model accounts for packet errors, buffer overflows, packet forwarding, packet acknowledgements, and routing information dissemination, all of which are important and essential characteristics of multihop wireless networks. In Section II, we provide a brief overview of imperfect private monitoring based on Aoyagi's model, highlighting salient points relevant to our discussion. In Section III, we present the model for a wireless multihop network, and this is followed by the validation of the model in Section IV based on an ideal wireless environment. Next, we show in Section V how this wireless multihop network game model is applied to design a generic protocol which we call the Selfishness Resilient Resource Reservation (SR^3) protocol, and validate the effectiveness of this protocol using simulations. Lastly, the contributions of this paper are summarized in Section VI. Table I lists the notations used in this paper and the derivations of various equations presented in Section III are given in the Appendix.

TABLE I
NOTATIONS USED

Symbol	Description
R	Real numbers
R_+	Non-negative real numbers
I	Set of players (nodes) in the game
i	A player (node) in set I
n	Number of players (nodes) in the game
t	Time period of the game
p, p^t	Price/loss probability profile of the players in set I, in period t
d, d^t	Demand/received packets profile of the players in set I, in period t
r, r^t	Report profile of the players in set I, in period t
p_i, p_i^t	Price/loss probability of player/node i, in period t
d_i, d_i^t	Demand/received packets of player/node i, in period t
r_i, r_i^t	Report of player/node i, in period t
p^*	Collusion price/loss probability profile of the players/node in set I
p^*_{-i}	Collusion price/loss probability profile of the players/node in set I except i
a^*	Collusion price/loss probability profile and reporting rule of the players/node in set I
a^*_{-i}	Collusion price/loss probability profile and reporting rule of the players/node in set I except i
b_i	Any arbitrary reporting rule of player i
$\hat{b}_i$	Threshold base reporting rule of player i
$m_i(p_i)$	Threshold value of player i that is a function of p_i
$s(r)$	Unanimous or non-unanimous report profile
$\underset{j\neq i}{min} f_j$	Minimum f among players in set I except i
$\underset{j\neq i}{max} f_j$	Maximum f among players in set I except i
$\underset{m_i\in R_+}{arg\ min} f(m_i)$	Set of maximizers of f
δ	Discount factor
$v_i(\delta)$	Payoff of player i with discount factor δ
α	Probability of non-unanimous report profile during collusion
α_i	Probability of non-unanimous report profile during collusion at the neighbourhood of i
$\beta_i(p_i)$	Probability of non-unanimous report profile when i unilaterally deviates
sup	Superior
inf	Inferior
a.e	Almost everywhere
λ	Packet generation rate

II. IMPERFECT PRIVATE MONITORING

In imperfect public monitoring, the players observe a common signal in each period which is an inaccurate indication of the actions taken by them. An example is an economic model of collusion between firms [20]. Each firm secretly chooses its production level, and they observe a common market price. The market price is a good but imperfect indicator because of fluctuations in demand levels. No such common signal exists in wireless communications, and thus wireless devices can only rely on locally (privately) available measurements. Game theory models pertaining to imperfect private monitoring are, however, relatively recent, and particularly hard to formulate. The difficulty in private monitoring lies in the lack of recursive game structure and the need to use statistical inference on other players' actions. Using the aforementioned example as above, in this case, the firms engage in secret price cutting. Market price is no longer a good public signal, and the firms rely on observing its own (private) sales volume, which is also imperfect due to demand fluctuations. An interesting class of such games relies on communication [17], [21], [22]. At each stage of the game, the players publicize an indication of their private signals. There is no constraint on what a player can broadcast, but whatever that is sent, will be acted upon by all other players. The equilibrium is constructed such that truthful reporting is sustained, and punishment strategies depend solely on the history of the reports communicated publicly. The analysis is thus simplified to the case of public monitoring.

A. Aoyagi's Game for Dynamic Bertrand Oligopoly

Aoyagi's game is a repeated game with correlated private signals and communication between players [17]. In an oligopoly, the products of the sellers are undifferentiated to the buyers.

If one seller lowers its selling price, the other seller's demand would be negatively affected. The problem in this game is that pricing signals are not reflective of the actual price offered by the other sellers. Sellers may publish a price yet provide secret price cutting to customers privately, and hence cannot constitute a publicly observable signal. The basic idea is to introduce communication between the players. At the end of each stage, the players are to reveal their private signals. Rational players would attempt to lie if it is profitable, and the equilibrium has to be built such that everyone has the incentive to tell the truth. The equilibrium can be constructed based only on the publicly observable history of communication and the analysis becomes similar to the perfect public equilibriums in the case of public monitoring.

B. Game Model

Quoting [17], the model definition is as follows: "The set I of $n(\geq 2)$ firms produce and sell products over infinitely many periods. In every period t, firm i chooses price p_I^t from the set $\Re_+$ of nonnegative real numbers, and then privately observes its own demand $d_i^t \in \Re_+$ whose probability distribution depends on the price profile $p^t = (p_1^t, \ldots, p_n^t)$ of all firms. Denote the demand profile in period t by $d^t = (d_1^t, \ldots, d_n^t)$. We suppose the $d_1^t, \ldots, d_n^t$ are independent, and have identical probability distribution $P(\cdot|p)$ conditional on the price profile p."

The game operates in collusion and punishment phases. In the collusion phase, the price profile $p^* = (p_1^*, \ldots, p_n^*)$ is to be sustained. After each period, each firm i is to make a public report r_i^t. Let b_i represent any arbitrary report rule and $\hat{b}_i$ represent the report rule based on the threshold $m_i(p_i)$:

$$\hat{b}_i(p_i, d_i) = \begin{cases} 1, & \text{if } d_i \geq m_i(p_i) \\ 0, & \text{otherwise.} \end{cases} \tag{1}$$

For each set of n reports, $r = (r_1, \ldots, r_n) \in \{0,1\}^n$, let $s(r) = 0$ if r is unanimous, i.e., $r_1 = \cdots = r_n$, and $s(r) = 1$ otherwise. If $s(r) = 0$, they continue to collude in the next period; otherwise, punishment begins. Therefore, unanimous reports are desirable for all players. The probability of unanimous reports conditioned on d_i is given by the following equation, where $a_i^* = (p_i^*, \hat{b}_i)$:

$$\begin{aligned} P(s(r) =0|d_i, p_i, b_i, a_{-i}^*) &= P\left(\min_{j\neq i}\left(d_j - m_j^*\right) \geq 0|p_i, d_i, p_{-i}^*\right) b_i(d_i) \\ &\quad + P\left(\max_{j\neq i}\left(d_j - m_j^*\right) < 0|p_i, d_i, p_{-i}^*\right)(1 - b_i(d_i)). \end{aligned} \tag{2}$$

The threshold m_i^* is defined as the threshold when the probability of unanimous profiles is maximized under the collusive price profile of p^* and has the following property:

$$\begin{aligned} m_i^* \in \arg\max_{m_i \in \Re_+} \Bigg\{ & P\left(\min_{j\neq i}\left(d_j - m_j^*\right) \geq 0, d_i \geq m_i|p^*\right) \\ & + P\left(\max_{j\neq i}\left(d_j - m_j^*\right) < 0, d_i < m_i|p^*\right)\Bigg\}. \end{aligned} \tag{3}$$

The game follows the T-segmented grim trigger strategy, which divides the repeated game into T separate component games, with each component game being independent of each other. The tth component game, out of a total of T component games, consists of periods $t, T+t, 2T+t, \ldots$. The game starts in the collusion phase and stays in the collusion phase until the report profiles are not unanimous. When this happens, it reverts to the punishment phase. The overall average payoff in each component game is then given by $\upsilon_i(\delta) = (1 - \delta^{\mathrm{T}})g_i^* + \delta^{\mathrm{T}} P(s(r) = 0|a^*)\upsilon_i(\delta)$, where $\delta \in [0,1)$ is the common discount factor for all firms, δ^{T} is the effective discount factor for firm i for a component game with T segments and g_i^* is the stage payoff. When all firms collude by playing $a_i^* = (p_i^*, \hat{b}_i)$, the probability of having nonunanimous report profile is given by:

$$\alpha = P\left(\min_{j\in I}\left(d_j - m_j^*\right) < 0 \leq \max_{j\in I}\left(d_j - m_j^*\right)|p^*\right) \tag{4}$$

and since $P(s(r) = 0|a^*) = 1 - \alpha$, the payoff can be simplified to $\upsilon_i(\delta) = (1-\delta^{\mathrm{T}})g_i^*/(1 - \delta^{\mathrm{T}}(1-\alpha))$. On the other hand, when an arbitrary firm i deviates by unilaterally adopting price p_i while following the reporting rule $a_i = (p_i, \hat{b}_i)$, such that, $g_i(p_i, p_{-i}^*) > g_i^*$ during any collusion period within any component game, the probability of nonunanimous reporting, $\beta_i(p_i)$, and the payoff gained from this deviation, $\upsilon_i(\delta)$, are given by:

$$\begin{aligned} \beta_i(p_i) = & P\left(\min_{j\neq i}\left(d_j - m_j^*\right) < 0, d_i \geq m_i(p_i)|p_i, p_{-i}^*\right) \\ & + P\left(\max_{j\neq i}\left(d_j - m_j^*\right) \geq 0, d_i < m_i(p_i)|p_i, p_{-i}^*\right) \end{aligned} \tag{5}$$

$$\begin{aligned} \upsilon_i(\delta) = & (1-\delta^{\mathrm{T}})g_i(p_i, p_{-i}^*) \\ & + \delta^{\mathrm{T}} P\left(s(r) = 0|p_i, \hat{b}_i, a_{-i}^*\right)\upsilon_i(\delta). \end{aligned} \tag{6}$$

Hence, the maximum payoff that can be gained is given by:

$$\upsilon_i(\delta) = (1-\delta^{\mathrm{T}})\bar{g}_i + \delta^{\mathrm{T}} P\left(s(r) = 0|p_i, \hat{b}_i, a_{-i}^*\right)\upsilon_i(\delta) \tag{7}$$

where $\bar{g}_i = \sup_{p_i \in \Re_+} g_i(p_i, p_{-i}^*)$, $P(s(r) = 0|p_i, \hat{b}_i, a_{-i}^*) \leq 1 - \beta_i$ and $\beta_i = \inf\{\beta_i(p_i) : g_i(p_i, p_{-i}^*) > g_i^*\}$. The result is such that to support collusion, the following inequalities should be satisfied so that no deviation is profitable:

$$\begin{aligned} &(1-\delta^{\mathrm{T}})\bar{g}_i + \delta^{\mathrm{T}} P(s(r) = 0|p_i, \hat{b}_i, a_{-i}^*)\upsilon_i(\delta) \\ &\quad \leq (1-\delta^{\mathrm{T}})g_i^* + \delta^{\mathrm{T}} P(s(r) = 0|a^*)\upsilon_i(\delta) \end{aligned} \tag{8}$$

$$\frac{\delta^{\mathrm{T}}}{1-\delta^{\mathrm{T}}}(\beta_i - \alpha)\upsilon_i(\delta) \geq \bar{g}_i - g_i^*. \tag{9}$$

III. Wireless Multihop Game

Analogies of Aoyagi's problem can be drawn to the wireless multihop network problem. We draw analogy between prices (p) to packet loss probability, and private demand signals (d) to the received packet count from a flow. If one relay node increases the packets it drops, the receiver's received packet count will be affected. The received packet count is a local observation that is a random variable where fluctuations can be caused by traffic source variations and random packet losses. The packet loss probability is a collection of errors caused by buffer overflows and wireless transmission errors arising from causes such as signal fading and collisions. The problem is that relay nodes may publish a loss probability and yet be tempted to quietly drop packets to conserve energy. The difficulty in identifying selfish nodes is that losses, intentional or unintentional, are indistinguishable to observing nodes. Following Aoyagi's approach, communication is introduced. At the end of each stage, the participants of a flow are to reveal their private signals (namely, received packet count). Monitoring nodes decide to cooperate or punish based solely on these revelations. Despite the analogies, Aoyagi's model cannot be directly applied as it requires public reporting of private signals. Global sharing of reports is difficult to accomplish in a wireless multihop network without having to periodically flood the network. Instead, we adopt a regional reporting and punishment approach.

A region is defined as the overlapping reception range of two adjacent relay nodes of a flow. Punishment of a node can be triggered by the observation of nonunanimous reports from its upstream or downstream regions (cf., Fig. 4 and Section V-B for the definitions of upstream and downstream nodes). The upstream region of a node consists of itself, the next upstream node and any node that is able to observe them. The downstream region is similarly defined. Nodes that are out of these two regions are unable to administer punishment on this node because they cannot receive two reports from either region for comparison. Nevertheless, the regions may overlap. Our subsequent analysis will modify Aoyagi's model to reflect the change from network-wide to regional punishments. Our analysis covers linear flows from one source to one destination via a single path, which can be multiplied over the network, flowing parallel to, or intersecting one another. The theoretical model proposed here is applicable to branching, since branches can be considered as a network of linear flows. However, any formal analysis on branching will only be considered in subsequent works.

A. Modeling Multihop Characteristics

Consider the scenario of a single flow where all nodes, except i, are adopting their collusive profiles. From Section II-B, when node i is observing a receive packet count of d_i, providing a packet loss probability p_i, and following the reporting rule b_i, the probability of getting a unanimous report, $s(r) = 0$, is given by:

$$\begin{aligned} P\left(s(r)=0|d_i,p_i,b_i,a^*_{-i}\right) &= P\left(\min_{j=\{i-1,i+1\}}\left(d_j-m^*_j\right)\geq 0|p_i,d_i,p^*_{-i}\right)b_i(d_i) \\ &\quad + P\left(\max_{j=\{i-1,i+1\}}\left(d_j-m^*_j\right)<0|p_i,d_i,p^*_{-i}\right)(1-b_i(d_i)). \end{aligned}$$

Note that the general expression given by (2) is reduced to unanimity of reports between a node and its immediate upstream and downstream nodes, with the first term describing the probability of a unanimous one and the second term describing the probability of a unanimous zero. During collusion, the probability of unanimous reporting is maximized (3) with every neighboring node following the collusive threshold m^*_i, where $i \in I$:

$$\begin{aligned} m^*_i \in \arg\max_{m_i\in\Re_+} \Bigg\{ &P\left(\min_{j=\{i-1,i+1\}}\left(d_j-m^*_j\right)\geq 0, d_i \geq m_i|p^*\right) \\ &+ P\left(\max_{j=\{i-1,i+1\}}\left(d_j-m^*_j\right)<0, d_i<m_i|p^*\right)\Bigg\}. \end{aligned} \tag{10}$$

Based on m_i, it is assumed that there is positive correlation among nodes with regard to the received packet count (demand) and packet loss probability (price) [17]. This assumption, among neighboring nodes, is expressed as follows:

Assumption 1: For each $i \in I$ and $p_i \in \Re_+$, there exists $m_i(p_i) \in [0,\infty]$ such that:

$$\begin{aligned} &P\left(\min_{j=\{i-1,i+1\}}\left(d_j-m^*_j\right)\geq 0|d_i,p_i,p^*_{-i}\right) \\ &\quad \geq P\left(\max_{j=\{i-1,i+1\}}\left(d_j-m^*_i\right)<0|d_i,p_i,p^*_{-i}\right) \end{aligned} \tag{11}$$

$$\begin{aligned} &P\left(\min_{j=\{i-1,i+1\}}\left(d_j-m^*_j\right)\geq 0|d_i,p_i,p^*_{-i}\right) \\ &\quad < P\left(\max_{j=\{i-1,i+1\}}\left(d_j-m^*_i\right)<0|d_i,p_i,p^*_{-i}\right) \end{aligned} \tag{12}$$

for $P(\cdot|p_i,p^*_{-i})$-a.e. $d_i \geq m_i(p_i)$ and $P(\cdot|p_i,p^*_{-i})$-a.e. $d_i < m_i(p_i)$, respectively. (a.e.: common mathematical abbreviation for "almost everywhere.")

When all nodes collude by adopting $a^*_i = (p^*_i, \hat{b}_i)$, the probability of having nonunanimous report profile for the neighborhood of node i is modified from (4) to give (13) where the scope of the unanimous report profile has been reduced from global to local/regional.

$$\begin{aligned} \alpha_i = P\Bigg(&\min_{j=\{i-1,i+1\}}\left(d_j-m^*_j\right)<0 \\ &\leq \max_{j=\{i-1,i+1\}}\left(d_j-m^*_j\right)|p^*\Bigg). \end{aligned} \tag{13}$$

The probability of nonunanimous report profile when node i alone deviates by dropping packets quietly (which is analogous to firm i secretly cutting its price), while following the reporting rule $\hat{b}_i$, is given by:

$$\begin{aligned} \beta_i(p_i) = &P\left(\min_{j=\{i-1,i+1\}}\left(d_j-m^*_j\right)<0, d_i\geq m_i(p_i)|p_i,p^*_{-i}\right) \\ &+ P\left(\max_{j=\{i-1,i+1\}}\left(d_j-m^*_j\right)\geq 0, d_i<m_i(p_i)|p_i,p^*_{-i}\right). \end{aligned} \tag{14}$$

B. Periodic Punishment Approach

Dividing a protocol game into components, like the T-segmented grim trigger strategy adopted in Aoyagi's game, would require tight time synchronization that is usually avoided in distributed systems. Instead, a T-segmented tit-for-tat strategy [14] is adopted, which divides the game into infinitely repeating stages, within which a stage lasts for T periods. The strategy played in the tth stage depends on the report at the end of the $(t-1)$th stage. The game begins in collusion for the first stage, and if the previous report is unanimous, the game continues to the next stage in collusion; otherwise, punishment occurs. Thus, the game payoff is (see Appendix for derivation):

$$\upsilon_i(\delta) = (1-\alpha\delta^T)g^*_i \tag{15}$$

where $\gamma = P(s(r)=0|a^*)$ and $\alpha = P(s(r)=1|a^*) = 1-\gamma$ are, respectively, the probability of unanimous and nonunanimous report profile during collusion.

C. Condition for Efficient Collusion

We now derive the conditions that will encourage nodes to continue colluding. The maximum payoff obtained from deviations, consisting of expected stage payoffs that a node will receive if reports are unanimous, or otherwise, is (see Appendix for derivation):

$$\bar{\upsilon}_i(\delta) = (1-\delta^T)\bar{g}_i + \left[\bar{\gamma}\delta^T + \frac{\bar{\alpha}\gamma\delta^{2T}}{1-\alpha\delta^T}\right]\upsilon_i(\delta) \tag{16}$$

where $\bar{\gamma} = P(s(r)=0|p_i,\hat{b}_i,a^*_{-i})$ and $\bar{\alpha} = 1-\bar{\gamma} = P(s(r)=1|p_i,\hat{b}_i,a^*_{-i})$ are, respectively, the probability of unanimous and nonunanimous profiles during deviation. To support collusion, the following inequalities (17)–(19), must be satisfied so that any deviation is not profitable, and hence undesirable (cf., Appendix):

$$\frac{\delta^T}{(1-\alpha\delta^T)}(\beta_i-\alpha)\upsilon_i(\delta) \geq \bar{g}_i - g^*_i \tag{17}$$

where $\bar{\alpha} \geq \beta_i$. To ensure that a node does not deviate to a strategy that has a lower gain per stage than that of the collusive strategy, but achieves a higher overall gain because the deviated strategy has a higher chance of getting unanimous reports than the collusive one, and consequently suffers from fewer punishments, we assume the following [17]:

Assumption 2: For each $i \in I$, $\alpha \leq \inf_{p_i\in\Re_+}\beta_i(p_i)$.

As a result, (13) and (17) become (cf., Appendix)

$$\delta^T < \frac{\epsilon}{\alpha g^*_i} \tag{18}$$

$$\delta^T \geq \frac{(\bar{g}_i - g^*_i)}{(\beta_i-\alpha)(g^*_i-\epsilon)+\alpha(\bar{g}_i-g^*_i)} \tag{19}$$

where $\epsilon > 0$ is any small number. Combining the inequalities, the following condition should be satisfied for deviation to be unprofitable (cf., Appendix):

$$\begin{aligned}
&\max_{i\in I}\frac{(\bar{g}_i-g^*_i)}{(\beta_i-\alpha)(g^*_i-\epsilon)+\alpha(\bar{g}_i-g^*_i)} \leq \delta^T < \min_{i\in I}\frac{\epsilon}{\alpha g^*_i}\\
&\max_{i\in I}\frac{(\bar{g}_i-g^*_i)}{(\beta_i-\alpha)(g^*_i-\epsilon)+\alpha(\bar{g}_i-g^*_i)} < \min_{i\in I}\frac{\epsilon}{\alpha g^*_i}\\
&\max_{i\in I}\frac{(\bar{g}_i-g^*_i)/\epsilon}{(\beta_i/\alpha-1)(g^*_i-\epsilon)+(\bar{g}_i-g^*_i)} < \min_{i\in I}\frac{1}{g^*_i}\\
&\min_{i\in I}\left[1+\left(\frac{\beta_i}{\alpha}-1\right)\frac{(g^*_i-\epsilon)}{(\bar{g}_i-g^*_i)}\right]\epsilon < \max_{i\in I} g^*_i.
\end{aligned} \tag{20}$$

IV. Game Model Validation

In this section, we apply the wireless multihop game model in a theoretical environment to prove that the model is feasible. We assume that the traffic source follows a Poisson distribution, and the wireless impairments are collectively modeled at each link by a binomial distribution, both of which are common and frequently assumed statistical models for network analysis. The probability distribution of the number of packets s generated by the source of a flow follows a Poisson distribution given by $P(s=x) = (\lambda^x e^{-\lambda}/x!)$ where λ is the mean number of packets generated, while wireless transmission errors are modeled as a loss probability ρ_t. This includes impairments such as propagation loss, signal fading and packet collisions.

A. Modeling Private Observations

The private observations in the oligopoly economic model refer to the private demand levels observed by a firm. The equivalent in the wireless multihop network scenario is the number of packets received by a node. Based on the aforementioned assumptions, the probability distribution of the number of packets, d, received by a node subjected to wireless impairments with a loss probability of ρ_t is given by:

$$\begin{aligned}
P(d) &= \sum_{y=0}^{\infty} P(s=y)\binom{y}{d}(1-\rho_t)^d\rho_t^{(y-d)}\\
&= \frac{e^{-\lambda(1-\rho_t)}\left[\lambda(1-\rho_t)\right]^d}{d!}
\end{aligned} \tag{21}$$

which shows that binomially distributed wireless errors do not alter the packet distribution characteristics at the next hop other than lowering the mean arriving packet count. The choice of binomial distributed errors thus has the advantage of creating symmetry at every node. Next, by assuming that the relaying node maintains a dedicated M/M/1 queue of k packets for the flow, congestion can result in packet loss with loss probability $l_c = \chi^k(1-\chi)/(1-\chi^{k+1})$ where χ is the system load, and given congestion loss probability ρ_c, $P(d)$ becomes:

$$P(d) = \frac{e^{-\lambda(1-\rho_t)(1-\rho_c)}\left[\lambda(1-\rho_t)(1-\rho_c)\right]^d}{d!}. \tag{22}$$

Aggregating the local congestion and packet loss rate at node i with $1-\rho_i = (1-\rho_{i,t})(1-\rho_{i,c})$, the packet received probability distribution at node i, with $\Lambda_i = \prod_{j=0}^{i-1}(1-\rho_j)$, is given by:

$$P(d_i|\rho_0,\rho_1,\ldots,\rho_{i-1}) = \frac{[\lambda\Lambda_i]^{d_i}e^{-\lambda\Lambda_i}}{d_i!}. \tag{23}$$

At the end of a stage in the game, if node i received a total of d_i packets, and the (aggregated) packet loss probability it adopted is ρ_i, the packet received probability of its upstream node $i+1$, conditioned on this knowledge, is given by:

$$P(d_{i+1}|d_i,\rho_i) = \binom{d_i}{d_{i+1}}(1-\rho_i)^{d_{i+1}}(\rho_i)^{d_i-d_{i+1}}. \tag{24}$$

On the other hand, the packet receive probability of its downstream node $i-1$ conditioned that node i received a total of d_i packets, and the packet loss probability it adopted is ρ_i is given by:

$$\begin{aligned}
&P(d_{i-1}|d_i,\rho_0,\rho_1,\ldots,\rho_{i-1})\\
&\quad= \frac{P(d_{i-1},d_i|\rho_0,\rho_1,\ldots,\rho_{i-1})}{P(d_i|\rho_0,\rho_1,\ldots,\rho_{i-1})}\\
&\quad= \frac{(\lambda\Lambda_{i-1}\rho_{i-1})^{d_{i-1}-d_i}e^{-(\lambda\Lambda_{i-1}\rho_{i-1})}}{(d_{i-1}-d_i)!}.
\end{aligned} \tag{25}$$

B. Reporting Strategy

The collusive reporting threshold is the threshold whereby the probability of uniform reporting is maximized when all members are in collaboration. Using (10), we evaluate the threshold, m_i^*, as follows:

$$\begin{aligned} m_i^* \in \arg \max_{m_i \in \Re_+} & \left\{ P\left(\min_{j=\{i-1,i+1\}} \left(d_j - m_j^*\right) \geq 0, d_i \geq m_i | p^* \right) \right. \\ & \left. + P\left(\max_{j=\{i-1,i+1\}} \left(d_j - m_j^*\right) < 0, d_i < m_i | p^* \right) \right\} \\ \equiv m_i^* \in \arg \max_{m_i \in \Re_+} & \left\{ \left(P \min_{j=\{i-1,i+1\}} \left(d_j - m_j^*\right) \geq 0, d_i \geq m_i | \rho^* \right) \right. \\ & \left. + P\left(\max_{j=\{i-1,i+1\}} \left(d_j - m_j^*\right) < 0, d_i < m_i | \rho^* \right) \right\} \end{aligned}$$

where

$$\begin{aligned} P & \left(\min_{j=\{i-1,i+1\}} \left(d_j - m_j^*\right) \geq 0, d_i \geq m_i | \rho^* \right) \\ & + P\left(\max_{j=\{i-1,i+1\}} \left(d_j - m_j^*\right) < 0, d_i < m_i | \rho^* \right) \Bigg\} \\ = & \sum_{d_{i-1}=m_{i-1}^*}^{\infty} \frac{\left(\lambda \Lambda_{i-1}^*\right)^{d_{i-1}} e^{-\left(\lambda \Lambda_{i-1}^*\right)}}{d_{i-1}!} \\ & \times \sum_{d_i=m_i}^{d_{i-1}} \binom{d_{i-1}}{d_i} \left(1-\rho_{i-1}^*\right)^{d_i} \left(\rho_{i-1}^*\right)^{d_{i-1}-d_i} \\ & \times \sum_{d_{i+1}=m_{i+1}^*}^{d_i} \binom{d_i}{d_{i+1}} \left(1-\rho_i^*\right)^{d_{i+1}} \left(\rho_i^*\right)^{d_i-d_{i+1}} \\ & + \sum_{d_{i-1}=0}^{m_{i-1}^*-1} \frac{\left(\lambda \Lambda_{i-1}^*\right)^{d_{i-1}} e^{-\left(\lambda \Lambda_{i-1}^*\right)}}{d_{i-1}!} \\ & \times \sum_{d_i=0}^{m_i-1} \binom{d_{i-1}}{d_i} \left(1-\rho_{i-1}^*\right)^{d_i} \left(\rho_{i-1}^*\right)^{d_{i-1}-d_i} \\ & \times \sum_{d_{i+1}=0}^{m_{i+1}^*-1} \binom{d_i}{d_{i+1}} \left(1-\rho_i^*\right)^{d_{i+1}} \left(\rho_i^*\right)^{d_i-d_{i+1}}. \end{aligned}$$

In the aforementioned expression, the first term is the probability of reporting a "1" (high) and the second term is the probability of reporting a "0" (low). Each term consists of nested cumulative receive packet probabilities of the next node given that a certain packet count has been received at a previous node. Given that the threshold m_i, like the received packet count, is a positive integer, the amount of deviation in the probability of unanimous reports in the presence of the smallest positive deviation (value of one) in reporting threshold (i.e., $m_i^* + 1$) is given by:

$$\begin{aligned} P & \left(\min_{j=\{i-1,i+1\}} \left(d_j - m_j^*\right) \geq 0, d_i \geq m_i + 1 | \rho^* \right) \\ & + P\left(\max_{j=\{i-1,i+1\}} \left(d_j - m_j^*\right) < 0, d_i < m_i + 1 | \rho^* \right) \\ = & P\left(\min_{j=\{i-1,i+1\}} \left(d_j - m_j^*\right) \geq 0, d_i \geq m_i | \rho^* \right) \\ & + P\left(\max_{j=\{i-1,i+1\}} \left(d_j - m_j^*\right) < 0, d_i < m_i | \rho^* \right) \\ & - \Bigg\{ \sum_{d_{i-1}=m_{i-1}^*}^{\infty} \frac{\left(\lambda \Lambda_{i-1}^*\right)^{d_{i-1}} e^{-\left(\lambda \Lambda_{i-1}^*\right)}}{d_{i-1}!} \\ & \times \binom{d_{i-1}}{m_i} \left(1-\rho_{i-1}^*\right)^{m_i} \left(\rho_{i-1}^*\right)^{d_{i-1}-m_i} \\ & \times \sum_{d_{i+1}=m_{i+1}^*}^{m_i} \binom{m_i}{d_{i+1}} \left(1-\rho_i^*\right)^{d_{i+1}} \left(\rho_i^*\right)^{m_i-d_{i+1}} \\ & + \sum_{d_{i-1}=0}^{m_{i-1}^*-1} \frac{\left(\lambda \Lambda_{i-1}^*\right)^{d_{i-1}} e^{-\left(\lambda \Lambda_{i-1}^*\right)}}{d_{i-1}!} \\ & \times \binom{d_{i-1}}{m_i} \left(1-\rho_{i-1}^*\right)^{m_i} \left(\rho_{i-1}^*\right)^{d_{i-1}-m_i} \\ & \times \sum_{d_{i+1}=0}^{m_{i+1}^*-1} \binom{m_i}{d_{i+1}} \left(1-\rho_i^*\right)^{d_{i+1}} \left(\rho_i^*\right)^{m_i-d_{i+1}} \Bigg\}. \end{aligned}$$

Therefore, the increase in unanimous probability when node i deviates from the reporting threshold positively by 1 unit is given by:

$$\begin{aligned} \Delta_i = & \sum_{d_{i-1}=0}^{m_{i-1}^*-1} \frac{\left(\lambda \Lambda_{i-1}^*\right)^{d_{i-1}} e^{-\left(\lambda \Lambda_{i-1}^*\right)}}{d_{i-1}!} \\ & \times \binom{d_{i-1}}{m_i} \left(1-\rho_{i-1}^*\right)^{m_i} \left(\rho_{i-1}^*\right)^{d_{i-1}-m_i} \\ & \times \sum_{d_{i+1}=0}^{m_{i+1}^*-1} \binom{m_i}{d_{i+1}} \left(1-\rho_i^*\right)^{d_{i+1}} \left(\rho_i^*\right)^{m_i-d_{i+1}} \\ & - \sum_{d_{i-1}=m_{i-1}^*}^{\infty} \frac{\left(\lambda \Lambda_{i-1}^*\right)^{d_{i-1}} e^{-\left(\lambda \Lambda_{i-1}^*\right)}}{d_{i-1}!} \\ & \times \binom{d_{i-1}}{m_i} \left(1-\rho_{i-1}^*\right)^{m_i} \left(\rho_{i-1}^*\right)^{d_{i-1}-m_i} \\ & \times \sum_{d_{i+1}=m_{i+1}^*}^{m_i} \binom{m_i}{d_{i+1}} \left(1-\rho_i^*\right)^{d_{i+1}} \left(\rho_i^*\right)^{m_i-d_{i+1}} \\ = & \frac{\left(\lambda \Lambda_i^*\right)^{m_i} e^{-\left(\lambda \Lambda_i^*\right)}}{\left(m_i^*\right)!} \\ & \times \Bigg\{ \sum_{d_{i-1}=0}^{m_{i-1}^*-1} \frac{\left(\lambda \Lambda_{i-1}^* \rho_{i-1}^*\right)^{d_{i-1}-m_i} e^{-\left(\lambda \Lambda_{i-1}^* \rho_{i-1}^*\right)}}{\left(d_{i-1}-m_i\right)!} \\ & \times \sum_{d_{i+1}=0}^{m_{i+1}^*-1} \binom{m_i}{d_{i+1}} \left(1-\rho_i^*\right)^{d_{i+1}} \left(\rho_i^*\right)^{m_i-d_{i+1}} \\ & - \sum_{d_{i-1}=m_{i-1}^*}^{\infty} \frac{\left(\lambda \Lambda_{i-1}^* \rho_{i-1}^*\right)^{d_{i-1}-m_i} e^{-\left(\lambda \Lambda_{i-1}^* \rho_{i-1}^*\right)}}{\left(d_{i-1}-m_i\right)!} \\ & \times \sum_{d_{i+1}=m_{i+1}^*}^{m_i} \binom{m_i}{d_{i+1}} \left(1-\rho_i^*\right)^{d_{i+1}} \left(\rho_i^*\right)^{m_i-d_{i+1}} \Bigg\} \end{aligned} \tag{26}$$

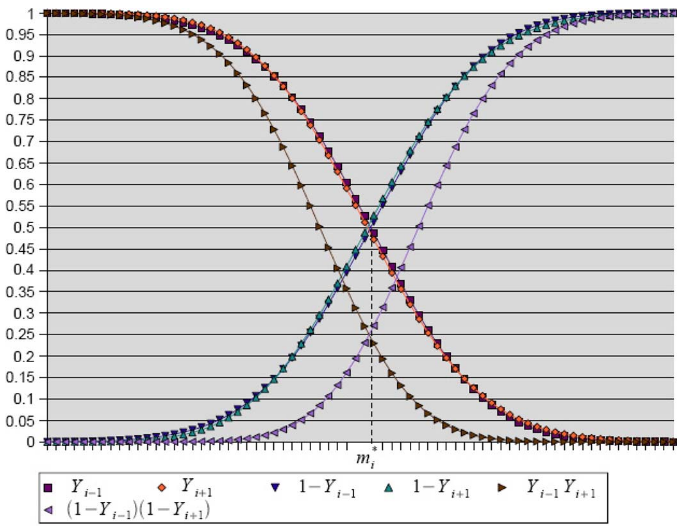

Fig. 1. Optimum cutoff reporting.

To analyze Δ_i, we first define Y_{i-1} and Y_{i+1} as follows:

$$Y_{i-1} = \sum_{d_{i-1}=0}^{m_{i-1}^*-m_i-1} \frac{\left(\lambda\Lambda_{i-1}^*\rho_{i-1}^*\right)^{d_{i-1}} e^{-\left(\lambda\Lambda_{i-1}^*\rho_{i-1}^*\right)}}{(d_{i-1})!}$$

$$= 1 - \sum_{d_{i-1}=m_{i-1}^*-m_i}^{\infty} \frac{\left(\lambda\Lambda_{i-1}^*\rho_{i-1}^*\right)^{d_{i-1}} e^{-\left(\lambda\Lambda_{i-1}^*\rho_{i-1}^*\right)}}{(d_{i-1})!}$$

$$Y_{i+1} = \sum_{d_{i+1}=0}^{m_{i+1}^*-1} \binom{m_i}{d_{i+1}} (1-\rho_i^*)^{d_{i+1}} (\rho_i^*)^{m_i-d_{i+1}}$$

$$= 1 - \sum_{d_{i+1}=m_{i+1}^*}^{m_i} \binom{m_i}{d_{i+1}} (1-\rho_i^*)^{d_{i+1}} (\rho_i^*)^{m_i-d_{i+1}}$$

and plot the various combinations, as shown in Fig. 1. Both Y_{i+1} and Y_{i-1} decreases as m_i increases. Hence, as m_i increases, the increase in unanimous probability slows down and reaches a peak, before it starts to decrease. The peak occurs when $\Delta_i = 0$. This happens when $Y_{i+1} = Y_{i-1} = 0.5$, which means $m_{i-1}^* - m_i = \lambda\Lambda_{i-1}^*\rho_{i-1}^*$ and $m_{i+1}^* = m_i(1-\rho_i^*)$ are at the medians. With the function $\Delta_i = 0$ having a unique solution at $m_i = m_i^* = \lambda\Lambda_i^* (\forall i \in I)$, we can conclude that $m_i^* = \lambda\Lambda_i^* (\forall i \in I)$ is the reporting threshold whereby the probability of unanimous reports is maximized when all nodes report packet loss probability ρ^* during collusion.

C. Correlated Receive Packet Count Signal

When the receive packet count is "positively correlated" across nodes, there exists a single-crossing property of conditional probabilities (11) and (12). By Assumption 1, it means that the conditional probabilities of other nodes unanimously reporting a "1" (high) or "0" (low) increases or decreases, respectively, as the received packet count, d_i, of node i increases. In other words, the higher the receive packet count that node i locally detected, the more likely it is for other nodes to unanimously report a "1" (high) and vice versa. From (24) and (25), we determine the combined probability of its neighbors receiving packets equaling d_{i-1} and d_{i+1}, conditioned on the event that the node i itself has received d_i packets and is adopting a loss rate of p_i, while other nodes are in collusion:

$$\begin{aligned} &P\left(d_{i-1}, d_{i+1} | d_i, p_i, p_{-i}^*\right) \\ &\quad\equiv P\left(d_{i-1}, d_{i+1} | d_i, \rho_i, \rho_{-i}^*\right) \\ &\quad= P\left(d_{i-1}, d_i, \rho_i, \rho_{-i}^*\right) P\left(d_{i+1} | d_i, \rho_i, \rho_{-i}^*\right) \\ &\quad= \frac{\left(\lambda\Lambda_{i-1}^*\rho_{i-1}^*\right)^{(d_{i-1}-d_i)} e^{-\left(\lambda\Lambda_{i-1}^*\rho_{i-1}^*\right)}}{(d_{i-1}-d_i)} \\ &\qquad\times \binom{d_i}{d_{i+1}} (1-\rho_i)^{d_{i+1}} \rho_i^{d_i-d_{i+1}}. \end{aligned} \tag{27}$$

The conditional probabilities of neighboring nodes reporting "1" (high) or "0" (low) are, respectively, as follows:

$$\begin{aligned} &P\left(\min_{j=\{i-1,i+1\}} (d_j - m_j^*) \geq 0 | d_i, p_i, p_{-i}^*\right) \\ &\quad= \sum_{d_{i-1}=m_{i-1}^*}^{\infty} \frac{\left(\lambda\Lambda_{i-1}^*\rho_{i-1}^*\right)^{(d_{i-1}-d_i)} e^{-\left(\lambda\Lambda_{i-1}^*\rho_{i-1}^*\right)}}{(d_{i-1}-d_i)} \\ &\qquad\times \sum_{d_{i+1}=m_{i+1}^*}^{d_i} \binom{d_i}{d_{i+1}} (1-\rho_i)^{d_{i+1}} \rho_i^{d_i-i+1} \end{aligned} \tag{28}$$

$$\begin{aligned} &P\left(\max_{j=\{i-1,i+1\}} (d_j - m_j^*) < 0 | d_i, p_i, p_{-i}^*\right) \\ &\quad= \sum_{d_{i-1}=0}^{m_{i-1}^*-1} \frac{\left(\lambda\Lambda_{i-1}^*\rho_{i-1}^*\right)^{(d_{i-1}-d_i)} e^{-\left(\lambda\Lambda_{i-1}^*\rho_{i-1}^*\right)}}{(d_{i-1}-d_i)} \\ &\qquad\times \sum_{d_{i+1}=0}^{m_{i+1}^*-1} \binom{d_i}{d_{i+1}} (1-\rho_i)^{d_{i+1}} \rho_i^{d_i-d_{i+1}}. \end{aligned} \tag{29}$$

Letting

$$H_{i-1}(d_i) = \sum_{d_{i-1}=m_{i-1}^*}^{\infty} \frac{\left(\lambda\Lambda_{i-1}^*\rho_{i-1}^*\right)^{(d_{i-1}-d_i)} e^{-\left(\lambda\Lambda_{i-1}^*\rho_{i-1}^*\right)}}{(d_{i-1}-d_i)!}$$

$$H_{i+1}(d_i, \rho_i) = \sum_{d_{i+1}=m_{i+1}^*}^{d_i} \binom{d_i}{d_{i+1}} (1-\rho_i)^{d_{i+1}} \rho_i^{d_i-d_{i+1}}$$

we note that both $H_{i-1}(d_i)$ and $H_{i+1}(d_i, \rho_i)$ increase as d_i increases, and consequently, (28) increases while (29) decreases, exhibiting "positive correlation" of receive signal levels across nodes. When all nodes collude, $d_i = m_i^* = \lambda\Lambda_i^* (\forall i \in I)$ is a crossing point. The median of H_{i+1} occurs at $m_i^*(1-\rho_i^*) = m_{i+1}^*$ giving it a value of 0.5. Similarly, the median of H_{i-1} occurs at $\lambda\Lambda_{i-1}^*\rho_{i-1}^* = m_{i-1}^* - m_i^*$ giving it a value of 0.5.

D. Highest Unanimity at Collusion

Assumption 2 describes a condition whereby deviation will always increase nonunanimous reports and consequently increases the likelihood of punishments. A node therefore does not have the incentive to play a strategy that has a lower payoff than the collusive strategy. From (13) and (14), together with (10), and defining A_i and $B_i(p_i)$ as shown hereinafter, we get:

$$\begin{aligned}\alpha_i &= P\left(\min_{j\in\{i-1,i,i+1\}}\left(d_j - m_j^*\right) < 0\right.\\ &\qquad\left.\leq \max_{j\in\{i-1,i,i+1\}}\left(d_j - m_j^*\right)|p^*\right)\\ &= 1 - P\left(\min_{j=\{i-1,i,i+1\}}\left(d_j - m_j^*\right) \geq 0|p^*\right)\\ &\quad - P\left(\max_{j=\{i-1,i,i+1\}}\left(d_j - m_j^*\right) < 0|p^*\right)\\ &\equiv 1 - P\left(\min_{j=\{i-1,i,i+1\}}\left(d_j - m_j^*\right) \geq 0|\rho^*\right)\\ &\quad - P\left(\max_{j=\{i-1,i,i+1\}}\left(d_j - m_j^*\right) < 0|\rho^*\right)\\ &= 1 - A_i \end{aligned} \tag{30}$$

$$\begin{aligned}\beta_i(p_i) &= P\left(\min_{j\in\{i-1,i+1\}}\left(d_j - m_j^*\right) < 0, d_i \geq m_i(p_i)|p_i, p_i^*\right)\\ &\quad + P\left(\max_{j\in\{i-1,i+1\}}\left(d_j - m_j^*\right) \geq 0, d_i < m_i(p_i)|p_i, p_i^*\right)\\ &= 1 - P\left(\min_{j=\{i-1,i+1\}}\left(d_j - m_j^*\right) \geq 0, d_i \geq m_i(p_i)|p_i, p_{-i}^*\right)\\ &\quad - P\left(\max_{j=\{i-1,i+1\}}\left(d_j - m_j^*\right) < 0, d_i < m_i(p_i)|p_i, p_{-i}^*\right)\\ &\equiv 1 - P\left(\min_{j=\{i-1,i+1\}}\left(d_j - m_j^*\right) \geq 0, d_i \geq m_i(p_i)|\rho_i, \rho_{-i}^*\right)\\ &\quad - P\left(\max_{j=\{i-1,i+1\}}\left(d_j - m_j^*\right) < 0, d_i < m_i(p_i)|\rho_i, \rho_{-i}^*\right)\\ &= 1 - B_i(\rho_i) \end{aligned} \tag{31}$$

and Assumption 2 can be reformulated as:

$$\text{For each } i \in I, \quad A_i \geq \sup_{p_i\in\Re_+} B_i(\rho_i) \tag{32}$$

The collusive probability of unanimous reporting A_i occurs when nodes adopt the collusion loss rate (price) p_i^* and threshold reporting strategy of cutoff value m_i^*. The threshold is obtained from the crossing point of (28) and (29) and has the highest probability with respect to any other cutoff values as shown Section IV-B. A node therefore has no incentive to deviate from the collusive cutoff reporting threshold of m_i^* when adopting p_i^*. Nevertheless, a node may decide to deviate from its agreed packet loss rate p_i^* to a loss rate of p_i and choose a different threshold $m(p_i)$ to maximize the deviated unanimous reporting probability B_i.

The relationship between the various distributions are shown in Fig. 2 which plots $H_{i+1}(d_i, p_i^*)$, $1 - H_{i+1}(d_i, p_i^*)$, $P(d_i|p_i, p_{-i}^*)H_{i-1}(d_i)$ and $P(d_i|p_i, p_{-i}^*)(1 - H_{i-1}(d_i))$. When node i adopts the collusive strategy of p_i^*, the two curves $H_{i+1}(d_i, p_i^*)$ and $1 - H_{i+1}(d_i, p_i^*)$ intersect at m_i^* as shown by the thick black lines in Fig. 2. These curves shift to the right as p_i increases above p_i^*, and to the left as p_i decreases below p_i^*. On the other hand, the curves $P(d_i|p_i, p_{-i}^*)H_{i-1}(d_i)$ and $P(d_i|p_i, p_{-i}^*)(1 - H_{i-1}(d_i))$ are independent and invariant of p_i. We observe that the curves $P(d_i|p_i, p_{-i}^*)H_{i-1}(d_i)$ and $P(d_i|p_i, p_{-i}^*)(1 - H_{i-1}(d_i))$ appear to be symmetrical about m_i^*, which is exactly the point where $H_{i+1}(d_i, p_i^*)$ and $1 - H_{i+1}(d_i, p_i^*)$ are also symmetrical about the vertical line at m_i^*. It is not surprising since the packet arrival probability

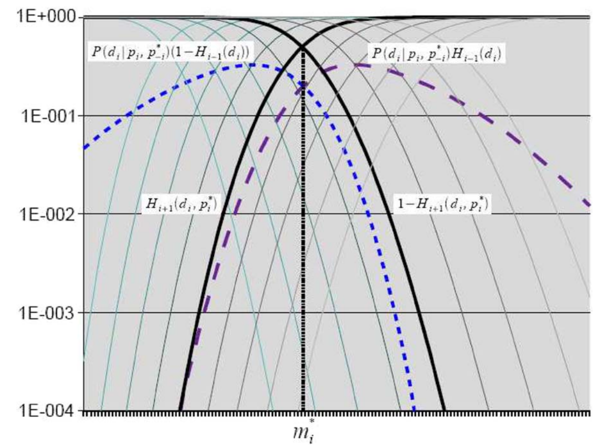

Fig. 2. Graphical evaluation of unanimous probability.

distribution function is a Poisson distribution that can be approximated to a Normal distribution that is symmetric about its mean m_i^*. Similarly, $H_{i-1}(d_i)$ and $1 - H_{i+1}(d_i, p_i^*)$ are approximately symmetrical about m_i^* so that the product $P(d_i|p_i, p_{-i}^*)H_{i-1}(d_i)$ and $P(d_i|p_i, p_{-i}^*)(1 - H_{i-1}(d_i))$ are symmetrical about m_i^*. The symmetrical property helps to simplify the proof of Assumption 2 (32) without going into complex mathematical calculations.

To prove that no deviation is profitable by validating (32), we first express A_i [which is only a special case when $m_i^* = m(p_i^*)$] and B_i, (in (30) and (31), respectively) as follows:

$$\begin{aligned} A_i &= \sum_{d_i=m_i^*}^{\infty} P\left(d_i|\rho^*\right) P\left(\min_{j=\{i-1,i+1\}}\left(d_j - m_j^*\right) \geq 0|d_i, \rho^*\right)\\ &\quad + \sum_{d_i=0}^{m_i^*-1} P(d_i|\rho^*)\\ &\quad \times P\left(\min_{j=\{i-1,i+1\}}\left(d_j - m_j^*\right) < 0|d_i, \rho^*\right)\\ &= \sum_{d_i=m_i^*}^{\infty} P(d_i|\rho^*)H_{i-1}(d_i)H_{i+1}\left(d_i, \rho_i^*\right)\\ &\quad + \sum_{d_i=0}^{m_i^*-1} P(d_i|\rho^*)\left(1 - H_{i-1}(d_i)\right)\left(1 - H_{i+1}\left(d_i, \rho_i^*\right)\right) \end{aligned} \tag{33}$$

$$\begin{aligned} B_i &= \sum_{d_i=m(p_i)}^{\infty} P\left(d_i|\rho_i, \rho_{-i}^*\right)\\ &\quad \times P\left(\min_{j=\{i-1,i+1\}}\left(d_j - m_j^*\right) \geq 0|d_i, \rho_i, \rho_{-i}^*\right)\\ &\quad + \sum_{d_i=0}^{m(p_i)-1} P\left(d_i|\rho_i, \rho_{-i}^*\right)\\ &\quad \times P\left(\min_{j=\{i-1,i+1\}}\left(d_j - m_j^*\right) < 0|d_i, \rho_i, \rho_{-i}^*\right)\\ &= \sum_{d_i=m(p_i)}^{\infty} P\left(d_i|\rho_i, \rho_{-i}^*\right) H_{i-1}(d_i)H_{i+1}(d_i, \rho_i)\\ &\quad + \sum_{d_i=0}^{m(p_i)-1} P\left(d_i|\rho_i, \rho_{-i}^*\right)\left(1 - H_{i-1}(d_i)\right)\\ &\quad \times \left(1 - H_{i+1}(d_i, \rho_i)\right) \end{aligned} \tag{34}$$

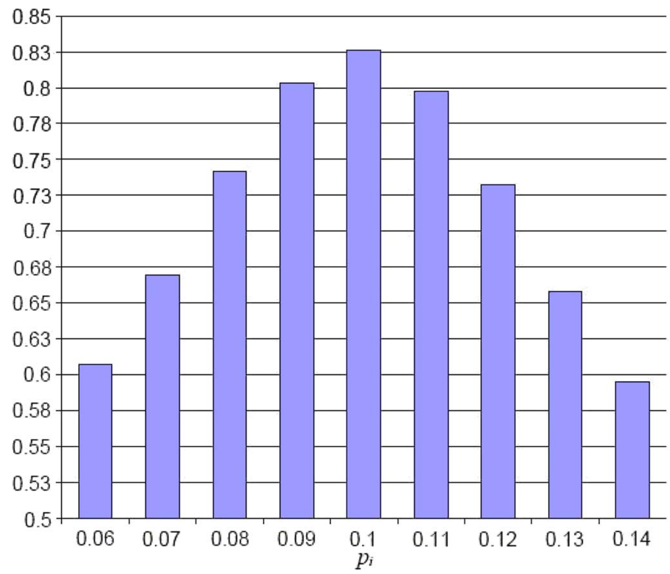

Fig. 3. Unanimous probability (y-axis) at various packet loss rates p_i.

where the probabilities $H_{i-1}(d_i)$ and $H_{i+1}(d_i, \rho_i)$ are obtained from Section IV-C and $P(d_i|\rho_i, \rho^*_{-i})$, which is the packet arrival probability distribution function at node i, is evaluated in (23).

A_i [(33)] comprises a lower summation and a higher summation. The lower summation, which is the probability of having a unanimous "0" (low) report, consists of the summation of the product of the decreasing black line and the dotted (blue) curve from the lower limit to $m^*_i - 1$, in Fig. 2. The higher summation, which is the probability of a unanimous "1" (high) report, consists of the summation of the product of the increasing black line and the dashed (purple) curve from m^*_i to the upper limit.

Similarly, B_i [(34)] consists of a lower summation and upper summation of the same pair of lines except for $\rho_i \neq \rho^*_i$, when the black lines move away from the line of symmetry at m^*_i. The cutoff point of the lower and higher summations is no longer optimum at m^*_i. Regardless of the choice of cutoff value $m(p_i)$, when the black lines diverge, the overall summation decreases, with one of the summations increasing, and the other decreasing in value, until a point when only one summation is dominant and the other is reduced to zero. At that point, the value B_i has the lowest possible probability equaling the area under the dotted (blue) curve or the dashed (purple) curve.

Hence, we have analytically illustrated that as ρ_i deviates from ρ^*_i, which is equivalently a deviation p^*_i to p_i, the probability of unanimous reporting decreases and B_i will always be lower than A_i, thus proving Assumption 2. Fig. 3 further demonstrates the changes in unanimous probabilities as node i adopts a different ρ_i. The probability is maximized when $\rho_i = \rho^*_i = 0.1$.

In this section, we have derived an optimum reporting strategy for the wireless multihop model. In this environment, we have shown that correlation of received packet counts (Assumption 1) exists, proving that threshold reporting is part of the equilibrium strategy in such an environment. We have also shown that abiding by the agreed packet loss probability ensures maximum probability of unanimous report profiles (Assumption 2). This ensures that the nodes will only deviate to strategies that have higher short-term gains. With Assumptions 1 and 2 satisfied, punishment strategies are simplified to regular (public and perfect) repeated games, including the T-segmented grim trigger strategy suggested by Aoyagi or an improved wireless punishment strategy provided in Section III-B.

V. Application of Theoretical Model to Protocol Design

In this section, we demonstrate the application of our theoretical model in designing a generic protocol which is called the Selfishness Resilient Resource Reservation (SR^3) protocol. As the name implies, SR^3 is a resource reservation protocol with collaborative relaying of flows, truthful sharing of QoS parameters and acknowledgments, and coordinated punishment for deviations. The aim of the simulation study is to validate the protocol's functionality and effectiveness, and not the performance in terms of networking metrics as these are highly dependent on other protocol aspects like routing algorithm, medium access control scheme, etc.

A. Protocol Description

Our cooperative protocol is designed based on the wireless multihop game described in Section III. In this game, network nodes are supposed to cooperatively route packets for a flow based on an equilibrium profile a^*, where $a^*_i = (p^*_i, \hat{b}_i)$, such that each node i assures a packet loss probability p^*_i and reports based on the reporting strategy $\hat{b}_i$ using threshold m^* of the locally observed received packet count d_i.

In Section IV, we have derived a theoretical threshold for optimum reporting under collusion given by $m^*_i = \lambda(1 - p^*_{i-1}) \cdots (1 - p^*_0) = \lambda\Lambda_i$ which will be the adopted threshold for this protocol. Information such as the source packet generation rate, λ, and packet error rates, p^*_i, need to be propagated down the flow. Additionally, our protocol has to facilitate reporting and synchronizing of punishment and cooperation phases. Nodes may secretly drop packets resulting in an actual packet loss probability p_i and deviate from equilibrium reporting to b_i, but these strategies are not optimum.

Due to the need for synchronization, a time division multiple access (TDMA) medium access control (MAC) scheme is adopted in our protocol. While synchronization and TDMA slot assignment/scheduling are not easy to achieve in wireless multihop networks, research in this area has advanced considerably and various solutions have been proposed, e.g., [23]–[25].

Similar to various TDMA protocols, our MAC layer has the smallest transmission unit of a time-slot that is reserved for a node within a contention region to avoid collisions. The collection of time-slots makes up a frame. At the head of the frame is a set of time slots dedicated for control information and the data time slots follow thereafter. The time-slots may be statically or dynamically assigned, and a static allocation of the control slots, Table II, to nodes in the sequence of the flow f is assumed for simplicity. Additionally, we also assume that a TDMA time frame is synchronized to a punishment or cooperation period.

Resource reservation is adopted since it fits naturally to the flow-based characteristic of the cooperative protocol. A flow is uniquely identified by a globally unique Source Identity and a locally unique Flow Identity issued at the source, and can be initiated by a resource reservation message which will pass Bandwidth and Loss Rate parameters to members of the flow so that sufficient resources are allocated.

TABLE II
CONTROL SLOT INFORMATION

Control Information				
1.	Size of Flow Table			
2.	Flow Table			
	1.	Source identity		
	2.	Flow identity		
	3.	Next hop		
	4.	Destination		
	5.	QoS Parameters		
		1.	Bandwidth	
		2.	Loss rate	
	6.	Acknowledgments		
		1.	Size	
		2.	Sequence Number Table	
			1.	Sequence number

The Bandwidth (B) is equivalent to the source packet generation rate λ at the source, and the effective packet arrival rate, $\lambda\Lambda_i$, at node i. The Loss Rate is the packet loss rate, p_i^*, introduced at node i. This could be the packet error rate between node i to node $i+1$, or inclusive of the amount of packets that it is going to drop. (Note that node i is not obliged to forward all the packets received but it is optimal for it to be truthful about its intentions). At the next node $i+1$, the Bandwidth is in fact the product of the Bandwidth and Link Quality of node i's QoS parameters. Similarly, it chooses the Loss Rate p_{i+1}^* and the Next Hop based on an existing routing protocol.

Part of the control information also contains a list of link layer acknowledgments for error-free packets that arrived in the last time frame per flow, assuming that each packet is attached with an error detection code. This information is used for threshold-based reporting $\hat{b}_i$. Originally, reporting, according to our wireless multihop model, is an announcement of "1" (high) or "0" (low) depending on whether the received packet rate of a flow is above or below an optimal threshold, m_i^*. Since this value is available as the Bandwidth in node i's QoS parameters which is observable to the neighboring nodes, we can imply a "0" when acknowledgements falls below it, and "1" otherwise. The amount of unacknowledged packets can be used to compute the loss rate in the previous frame.

After the transmission of control information measured based on the activities of the last time frame, a judgment is made by the neighboring monitoring nodes in the region of a flow to punish or cooperate in the current time frame. These nodes will compare the number of acknowledgements to the Reserved Bandwidth reported in the same control information to decide a "1" or "0" and a subsequent punishment or cooperation.

Punishment is administered when reports are not unanimous in a region. There are many ways to administer punishments; for example, at the routing layer, packet relaying sanctions can be imposed on the punished node, while at the MAC layer, allocated data transmission slots can be deallocated and/or requests for data transmission slots denied. We assume that the participating node has a desire to transmit. Otherwise, punishment is impossible as payoffs cannot be affected.

Our protocol is still fairly simple but adequate to demonstrate the concept. First, we assumed the availability of a routing table to start the reservation process. We also assumed a fairly static network whereby the path taken by a flow is not expected to change due to node mobility, thus requiring reestablishment.

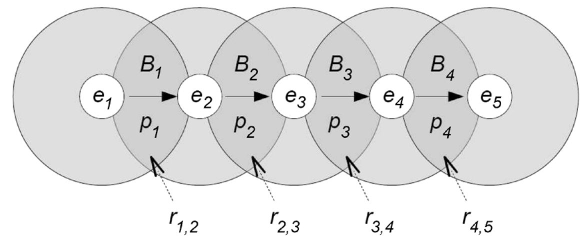

Fig. 4. Network topology.

TABLE III
EXAMPLE OF CONTROL SLOT INFORMATION
DURING BANDWIDTH RESERVATION

Control Information				
1.	Size of Flow Table			
2.	Flow Table			
	1.	Source Identity $= e_1$		
	2.	Flow Identity $= i$		
	3.	Next Hop $= e_2$		
	4.	Destination $= e_5$		
	5.	QoS Parameters		
		1.	Bandwidth, $B_n = B_{n-1} \times p_{n-1}$	
		2.	Loss Rate p_n	
	6.	Acknowledgment Information		
		1.	Size = 0	
		2.	Sequence Number Table = Nil	
			1.	NA

TABLE IV
COOPERATIVE SCENARIO WITHOUT PACKET DROPPING

Node ID	Reserved bandwidth B_n(pkts/frame)	Committed loss rate p_n(/pkt)	Threshold (pkts/frame)	Mean Acks (pkts/frame)
e_1	10,000	0.00200	N.A.	N.A.
e_2	9,980	0.00125	9,980	9,980
e_3	9,968	0.00010	9,968	9,968
e_4	9,967	0.00100	9,967	9,967
e_5	9,957	N.A.	9,957	9,957

At this stage, our model still cannot cover all aspects of the communication protocol. Our approach is to fit as much of a protocol into this model, from which we found that certain characteristics of the network can be aligned with the theory but yet there are still some features that are not captured. The other approach is to fit a theory into a protocol. This approach is daunting at the moment due to the complexity of both networking protocols and game theory. Nonetheless, the former approach provides an insight and direction for the latter, which is the rationale for this paper.

B. Secrets and Lies

To give an example of the protocol operations, the source e_1 attempts to reserve bandwidth for a flow f along a four-hop path to destination e_5, as shown in Fig. 4. In this paper, we refer to the node that is closer to the destination as the downstream node, i.e., e_i's downstream node is e_{i+1} and similarly, e_i's upstream node is e_{i-1}. Node e_n started sending control information described in Table III at time frame $t+n-1$. The effective reserved bandwidth, $B_{n-1}p_{n-1}$, at node e_{n-1}, is the same as the reserved bandwidth, B_n, and the expected flow arrival during collusion, A_n, at the next relay e_n. In equilibrium, the nodes are cooperative and no secret packet dropping is present in the system. Table IV provides a numerical illustration

TABLE V
SIMPLE PACKET DROPPING

Node ID	Reserved bandwidth B_n(pkts/frame)	Flow Arrivals A_n(pkts/frame)	Committed loss rate p_n(/pkt)	Actual loss rate p_n(/pkt)	Threshold (pkts/frame)	Mean Acks (pkts/frame)
e_1	10,000	10,000	0.00200	0.00200	N.A.	N.A.
e_2	9,980	9,980	0.00125	0.00125	9,980	9,980
e_3	9,968	9,968	0.00010	**0.00020**	9,968	9,968
e_4	9,967	**9,966**	0.00100	0.00100	9,967	**9,966**
e_5	9,957	**9,956**	N.A.	N.A.	9,957	**9,956**

TABLE VI
SECRET PACKET DROPPING WITH ACKNOWLEDGMENT LIES

Node ID	Reserved bandwidth B_n(pkts/frame)	Flow Arrivals A_n(pkts/frame)	Committed loss rate p_n(/pkt)	Actual loss rate p_n(/pkt)	Threshold (pkts/frame)	Mean Acks (pkts/frame)
e_1	10,000	10,000	0.00200	0.00200	N.A.	N.A.
e_2	9,980	9,980	0.00125	0.00125	9,980	9,980
e_3	9,968	9,968	0.00010	**0.00020**	9,968	**9,966**
e_4	9,967	**9,966**	0.00100	0.00100	9,966	**9,966**
e_5	9,957	**9,956**	N.A.	N.A.	9,956	**9,956**

TABLE VII
SECRET PACKET DROPPING WITH BANDWIDTH LIES

Node ID	Reserved bandwidth B_n(pkts/frame)	Flow Arrivals A_n(pkts/frame)	Committed loss rate p_n(/pkt)	Actual loss rate p_n(/pkt)	Threshold (pkts/frame)	Mean Acks (pkts/frame)
e_1	10,000	10,000	0.00200	0.00200	N.A.	N.A.
e_2	9,980	9,980	0.00125	0.00125	9,980	9,980
e_3	**9,967**	9,968	0.00010	**0.00020**	**9,967**	9,968
e_4	**9,966**	**9,966**	0.00100	0.00100	**9,966**	**9,966**
e_5	**9,956**	**9,956**	N.A.	N.A.	**9,956**	**9,956**

TABLE VIII
HONEST PACKET DROPPING

Node ID	Reserved bandwidth B_n(pkts/frame)	Flow Arrivals A_n(pkts/frame)	Committed loss rate p_n(/pkt)	Actual loss rate p_n(/pkt)	Threshold (pkts/frame)	Mean Acks (pkts/frame)
e_1	10,000	10,000	0.00200	0.00200	N.A.	N.A.
e_2	9,980	9,980	0.00125	0.00125	9,980	9,980
e_3	9,968	9,968	**0.00020**	**0.00020**	9,968	9,968
e_4	**9,966**	**9,966**	0.00100	0.00100	**9,966**	**9,966**
e_5	**9,956**	**9,956**	N.A.	N.A.	**9,956**	**9,956**

of the equilibrium case, and we assume that in this scenario, the committed loss rates are reflective of the link error rates.

Now, suppose that node e_3 is looking for ways to improve its payoffs. In Table V, it first attempts to drop more packets than what it has committed in its control information. This lowers the number of acknowledgments by the next hop node e_4 to 9966, but because observing nodes in the region of $r_{3,4}$ are still using a threshold of 9967, the probability of detecting a "low" signal from e_4 increases together with the probability of nonunanimous reports in region $r_{3,4}$, and ultimately a loss of payoffs in that region.

Realizing that, node e_3 naively modifies its report to match the increased probability of a "low" signal to reduce nonunanimous reports in the region $r_{3,4}$. It does so by misreporting the number of acknowledgments to node e_2 at a lower value of 9966 (Table VI) which, unfortunately increases the probability of nonunanimous reports in the downstream region $r_{2,3}$ such that there is a loss of payoffs in that region.

Since it does not want to affect region $r_{2,3}$ either, it has to report acknowledgments accurately. Returning to its original strategy, it next tries to modify the reserved bandwidth parameter such that the product of bandwidth and committed loss rate reflects the expected flow arrival volume at e_4. This lowers the threshold for node e_4 in region $r_{3,4}$, which neutralizes the increased probability of detecting a "low" signal due to secret packet dropping and is in fact the optimum bandwidth deviation that achieves a minimum punishment rate. In reality, this is a collusive operating point according to our wireless multihop model because the effective bandwidth (product of reserved bandwidth and loss) truthfully reflects the expected packet arrival at the next hop e_4. We had decomposed the effective reserved bandwidth into the reserved transmission bandwidth and loss rate components so that an increase in loss rate and a decrease in transmission bandwidth appear as two deviations when there is no obvious deviation in the effective reserved bandwidth. On the other hand, none of these changes have an effect on the downstream node. The above is illustrated in Table VII. Eventually, the wayward node realizes that honesty is the best policy and publishes the real loss rate which is inclusive of the link error rate and local packet dropping rates, as shown in Table VIII.

C. Simulation Results

In this section, we present the simulation results for the scenarios in Section V-B. We aim to demonstrate that our protocol is resilient to selfishness and thus show that the applicability of the game model to wireless multihop networks. In our simulation, we assumed that a flow has been established and already in the data transmission phase. We shall investigate

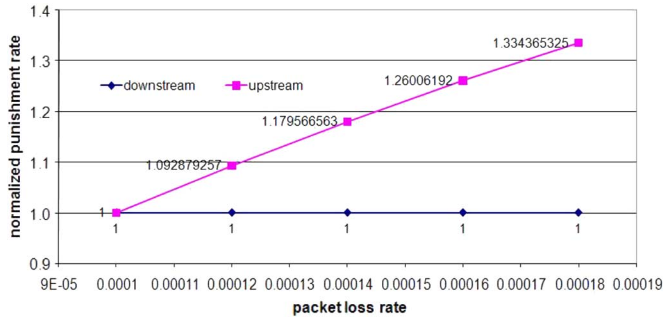

Fig. 5. Collusive packet forwarding.

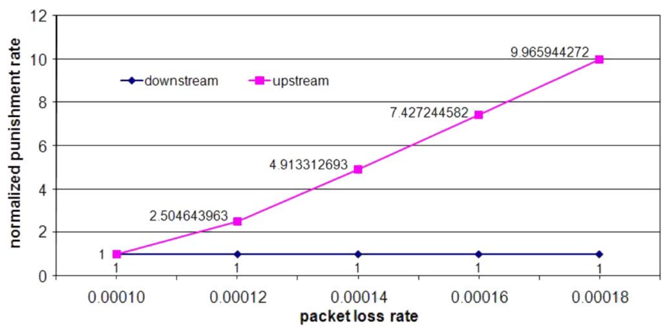

Fig. 6. Upstream and downstream punishments during simple packet dropping.

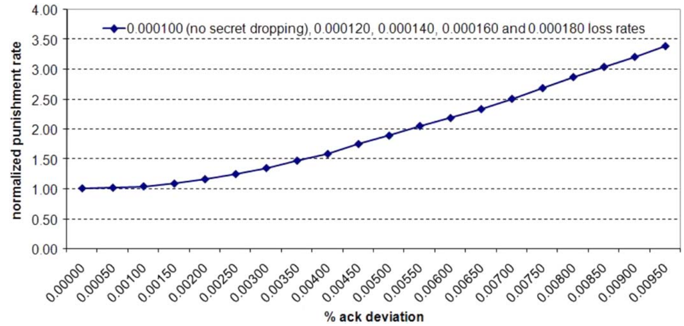

Fig. 7. Downstream punishment for secret packet dropping with acknowledgment lies.

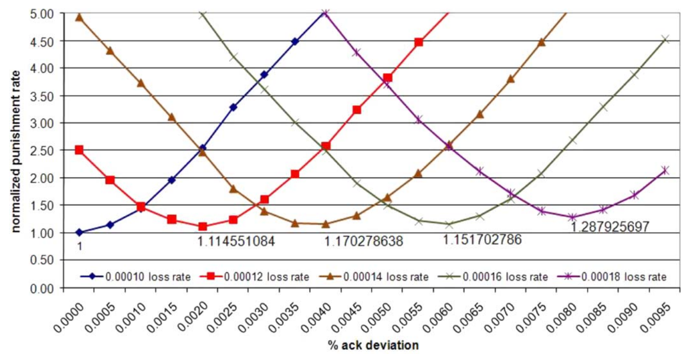

Fig. 8. Upstream punishment for secret packet dropping with acknowledgment lies.

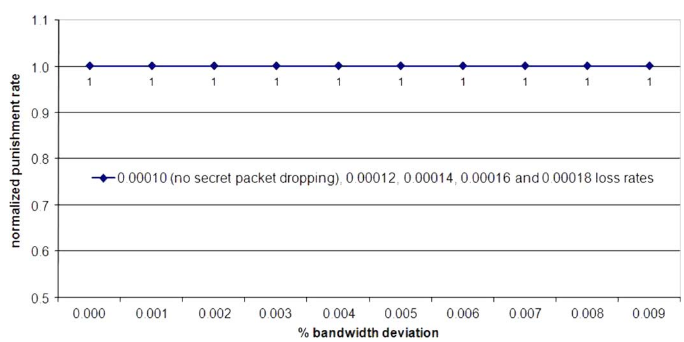

Fig. 9. Downstream punishment for secret packet dropping with bandwidth lies (varying bandwidth deviations).

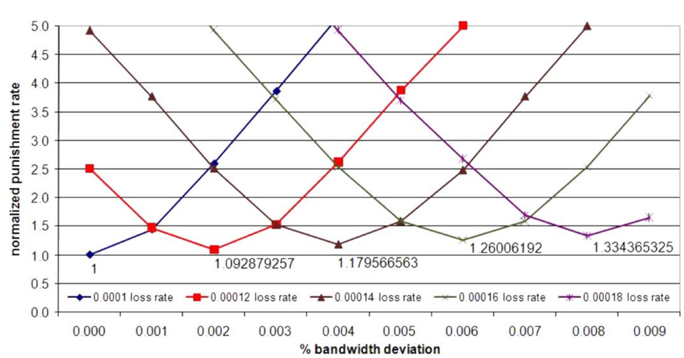

Fig. 10. Upstream punishment for secret packet dropping with bandwidth lies (varying bandwidth deviations).

the punishment rates of different scenarios, focusing on the cooperative and selfish behaviors of relay node e_2 and the associated upstream and downstream nodes and regions.

Our first scenario is a cooperative one. Nodes abide by the committed loss rates of 0.00010, 0.00012, 0.00104, 0.00016, and 0.00018. The punishment rates are normalized with the collusive punishment rate when the lowest of the five loss rates is adopted. Fig. 5 shows the punishment rate for every collusive loss rate adopted. Only upstream punishment rates are affected by differences in the loss rates which are observed to increase as loss rates increase. Next, Fig. 6 shows the results for a simple secret packet dropping scenario. We simulated incremental deviations from the committed loss rate of 0.00010, at values 0.00012, 0.00014, 0.00016, and 0.00018. While deviation has not impacted the downstream region, upstream punishment rates increased sharply, causing a loss of payoffs.

The misreporting of the number of acknowledgments at a lower value increases punishment in both the upstream region and downstream regions. The increase in the downstream region is independent of secret packet dropping and increases sharply with the percentage of misreported acknowledgments, as shown in Fig. 7. There exists an optimum acknowledgment lying level per secret packet dropping rate for the upstream region such that punishment is minimized. Nevertheless, these minimums are still higher than the punishment rate achievable during cooperation (no secret dropping and no acknowledgment lies—denoted by 0.00010 loss rate), as shown in Fig. 8.

In the bandwidth lying scenario, the punishment behavior of the downstream region is unaffected, as shown in Fig. 9. It is independent of secret packet dropping, and remained constant despite bandwidth deviations. On the upstream regions, various optimum deviation points exist and are indicated, as shown in Fig. 10.

However, none of these values is lower than the punishment rate achievable during collusion when it is abiding by the committed loss rate of 0.00010. Note also that for every loss

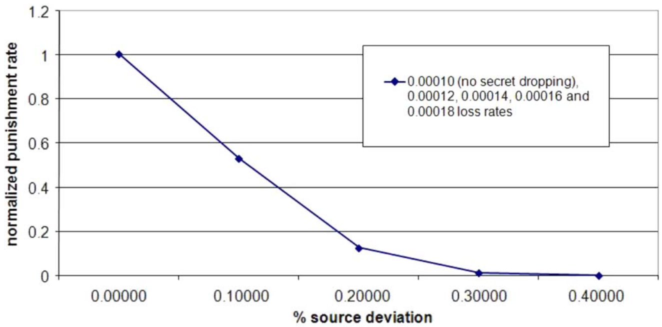

Fig. 11. Downstream punishment for secret packet dropping with bandwidth lies (varying source deviations).

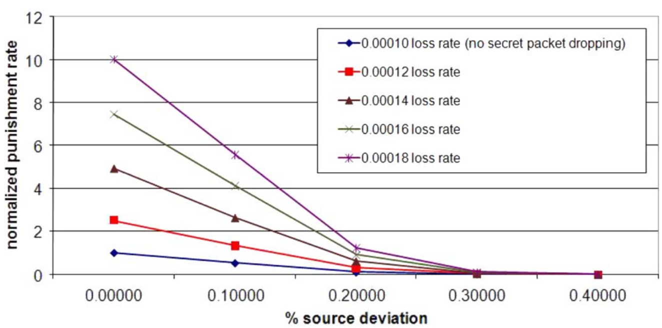

Fig. 12. Upstream punishment for secret packet dropping with bandwidth lies (varying source deviations).

rate, there is a minimum punishment rate achievable. These are really collusion points as explained in Section V-B, and the values coincide with our cooperation scenarios in Fig. 5. Hence, there is no incentive for bandwidth lying during secret packet dropping.

Finally, we simulated source rate deviations at the traffic generator. As the deviations increase, the punishment rates decrease even for selfish nodes, both on the downstream (Fig. 11) as well as the upstream (Fig. 12). Hence, deviation by the source undermines the ability to enforce punishment and therefore a rational source reveals its required bandwidth truthfully. On the other hand, the result also implies that our initial protocol setup phase, whereby no packet is transmitted, will not be subjected to unnecessary punishments.

VI. Conclusion

In this paper, we focus on the problem of selfish behavior in wireless multihop networks as there is a potential for such behavior to occur in emerging network scenarios where communications is envisaged to span multihop wireless links, over nodes that may subscribe/belong to different providers, like in community wireless mesh networks and future generation wireless networks using multihop relays. We search for a sustainable network behavior in wireless multihop networks where cooperation comes at a cost. While these (selfish) users have no malicious intent to disrupt network operations, they are rational users that are sometimes constrained by resources which make them less likely to cooperate. They would require incentives or punishments to encourage cooperation and participation in network operations.

Game theory is exploited to analyze an integrated model of transmission losses, buffer overflows, packet acknowledgments, packet forwarding and routing information dissemination, all of which are important characteristics of wireless networks. Specifically, we applied Aoyagi's game of imperfect private monitoring with communication [17] and adapted it to the wireless multihop environment. Our wireless multihop model provides a guiding design principle for protocols that are robust against selfish users. The analysis is not confined to a particular layer, but is designed to capture the overall behavior of a protocol stack.

In this model, relaying nodes establish a mutual agreement on the collusive packet loss probability (combination of transmission losses and buffer overflows) prior to the transmission of a flow. The negotiation of supported packet loss probability is not different from routing broadcasts with QoS or link quality indications. With this threshold, it is optimal for nodes to report a "1" (high) if their received flow rate exceeds their threshold and a "0" (low) if otherwise. These reports are in fact packet acknowledgments which we have proven to be truthful. We have further proven that the routing information disseminated is also truthful. The local broadcasting of reports allows the coordination of regional punishments. Nodes in a region hear the reports from two neighboring nodes of a flow, and punishment is administered by these nodes in the next stage if nonunanimous reports have been received.

We then validated the model in a theoretical wireless environment using well-accepted statistical models of packet generation and transmission errors. We have proven by mathematical derivations and analysis that assumptions made in our Wireless Multihop Game model are satisfied in this environment. We have also derived a collusive reporting threshold thereby making the model realizable. Our model is theoretically consistent with game theory and technically practical for a distributed, wireless network. We have also proven that the assumptions made for the model are true under a commonly accepted wireless environment. Typical pitfalls, like coordinated global punishments, are avoided and the model fits nicely into existing wireless multihop network protocols, requiring little overheads and modifications. Lastly, we demonstrated how this wireless multihop game model can be applied to design a generic protocol that reveals and discourages selfish behavior among nodes in a wireless multihop network. This protocol, called the Selfishness Resilient Resource Reservation protocol, is then simulated and shown to be effective against selfish node behavior, thus proving that our game model can be applied in realistic scenarios.

There are nevertheless limitations to our model which provide opportunities for future work. First, synchronized reporting is required although we have relaxed the requirement. We envisage that synchronization may not be required ultimately although various wireless technologies have synchronization capabilities which can be exploited for this purpose. Second, reports are to be reliably broadcast which may be hard to guarantee in wireless networks but can be provided by various link layer reliability mechanisms. Third, the model did not capture the medium arbitration function of the link layer as well as other network functions. Finally, we have not answered the question of how the nodes should choose a collaborative packet relay probability. These issues and other issues are left for future study.

APPENDIX

A. Derivation of (15)

The payoff of a cooperative stage is given by g_i^*. If the cooperative game segment lasts T periods, the payoff at the end of the period would be $g_i^* + \delta g_i^* + \cdots + \delta^{T-1} g_i^*$, where δ is the discount factor. The game starts off in cooperation. At the end of one segment, the nodes will each make a report. If unanimous reports are obtained, the game continues in cooperation, which results in an expected payoff of $P(s(r)=0|a^*)[\delta^{\mathrm{T}} g_i^* + \delta^{T+1} g_i^* + \cdots + \delta^{2T-1} g_i^*]$; otherwise, punishment results in no payoffs. Subsequently, cooperation may continue which gives rise to an expected payoff of $P(s(r)=0|a^*)P(s(r)=0|a^*)[\delta^{2T} g_i^* + \delta^{2T+1} g_i^* + \cdots + \delta^{3T-1} g_i^*]$, or revert from a previous punishment given by $P(s(r)=1|a^*)P(s(r)=0|a^*)[\delta^{2T} g_i^* + \delta^{2T+1} g_i^* + \cdots + \delta^{3T-1} g_i^*]$. Given that $g_i' = \sum_{t=0}^{T-1} g_i^* = (1-\delta^{\mathrm{T}}/1-\delta) g_i^*$ is the stage payoff lasting T periods, $\gamma = P(s(r)=0|a^*)$ is the probability of unanimous profile during collusion, and $\alpha = P(s(r)=1|a^*) = 1-\gamma$ is the probability of nonunanimous profile during collusion, we have (note: the term $(1-\delta)$ is for normalization):

$$\begin{aligned}
\upsilon_i(\delta) = (1-\delta)&\\
&\times \big\{ \left[g_i^* + \delta g_i^* + \cdots + \delta^{T-1} g_i^*\right] + P(s(r)=0|a^*)\\
&\quad\times \left[\delta^{\mathrm{T}} g_i^* + \delta^{T+1} g_i^* + \cdots + \delta^{2T-1} g_i^*\right]\\
&\quad+ P(s(r)=0|a^*) P\left(s(r)=0|a^*\right)\\
&\quad\times \left[\delta^{2T} g_i^* + \delta^{2T+1} g_i^* + \cdots + \delta^{3T-1} g_i^*\right]\\
&\quad+ P(s(r)=1|a^*) P(s(r)=0|a^*)\\
&\quad\times \left[\delta^{2T} g_i^* + \delta^{2T+1} g_i^* + \cdots + \delta^{3T-1} g_i^*\right] + \cdots \big\}
\end{aligned}$$

$$\begin{aligned}
\frac{\upsilon_i(\delta)}{(1-\delta)} = {} & g_i' + \gamma\delta^{\mathrm{T}} g_i' + \gamma\cdot\gamma\delta^{2T} g_i' + \gamma\cdot\gamma\cdot\gamma\delta^{3T} g_i' + \gamma\cdot\gamma\\
& \cdot\gamma\cdot\gamma\delta^{4T} g_i' + \cdots + \gamma\cdot\gamma\cdot\alpha\cdot\gamma\delta^{4T} g_i' + \cdots + \gamma\\
& \cdot\alpha\cdot\gamma\delta^{3T} g_i' + \gamma\cdot\alpha\cdot\gamma\cdot\gamma\delta^{4T} g_i' + \cdots + \gamma\\
& \cdot\alpha\cdot\alpha\cdot\gamma\delta^{4T} g_i' + \cdots + \alpha\cdot\gamma\delta^{2T} g_i' + \alpha\cdot\gamma\\
& \cdot\gamma\delta^{3T} g_i' + \alpha\cdot\gamma\cdot\gamma\cdot\gamma\delta^{4T} g_i' + \cdots + \alpha\cdot\gamma\cdot\alpha\\
& \cdot\gamma\delta^{4T} g_i' + \cdots + \alpha\cdot\alpha\cdot\gamma\delta^{3T} g_i' + \alpha\cdot\alpha\\
& \cdot\gamma\cdot\gamma\delta^{4T} g_i' + \cdots + \alpha\cdot\alpha\cdot\alpha\cdot\gamma\delta^{4T} g_i' + \cdots.
\end{aligned}$$

Simplifying further, we obtain:

$$\begin{aligned}
\upsilon_i(\delta) &= (1-\delta) g_i'\\
&\quad + [\gamma\delta^{\mathrm{T}}\upsilon_i(\delta) + \alpha\cdot\gamma\delta^{2T}\upsilon_i(\delta) + \alpha\cdot\alpha\cdot\gamma\delta^{3T}\upsilon_i(\delta) + \cdots]\\
\upsilon_i(\delta) &= (1-\delta) g_i'\\
&\quad + \gamma\delta^{\mathrm{T}}\upsilon_i(\delta)[1 + (\alpha\delta^{\mathrm{T}}) + (\alpha\delta^{\mathrm{T}})^2 + (\alpha\delta^{\mathrm{T}})^3 + \cdots]\\
\upsilon_i(\delta) &= (1-\delta) g_i' + \frac{\gamma\delta^{\mathrm{T}}}{1-\alpha\delta^{\mathrm{T}}}\upsilon_i(\delta)\\
\upsilon_i(\delta) &= \frac{(1-\delta)(1-\alpha\delta^{\mathrm{T}})}{1-\delta^{\mathrm{T}}} g_i'\\
\upsilon_i(\delta) &= \frac{(1-\delta)(1-\alpha\delta^{T})}{1-\delta^{\mathrm{T}}}\frac{1-\delta^{\mathrm{T}}}{1-\delta} g_i^*\\
\upsilon_i(\delta) &= (1-\alpha\delta^{\mathrm{T}}) g_i^*.
\end{aligned}$$

B. Derivation of (16)

The derivation is similar to (15), except that node i made a one-step deviation from the collusive strategy which give rise to a payoff of $\bar{g}_i$, and over T periods $[\bar{g}_i + \delta\bar{g}_i + \cdots + \delta^{T-1}\bar{g}_i]$. The derivation is shown at the bottom of the page where:

$\bar{g}_i' = \sum_{t=0}^{T-1} \bar{g}_i$ is the stage payoff lasting T periods,

$\bar{\gamma} = P(s(r)=0|p_i, \hat{b}_i, a_{-i}^*)$ is the probability of unanimous profiles during deviation,

$$\begin{aligned}
\bar{\upsilon}_i(\delta) = (1-\delta)\Big\{ & [\bar{g}_i + \delta\bar{g}_i + \cdots + \delta^{T-1}\bar{g}_i] + P\left(s(r)=0|p_i,\hat{b}_i,a_{-i}^*\right)[\delta^{\mathrm{T}}\bar{g}_i + \delta^{T+1}\bar{g}_i + \cdots + \delta^{2T-1}\bar{g}_i]\\
& + P\left(s(r)=0|p_i,\hat{b}_i,a_{-i}^*\right) P\left(s(r)=0|a^*\right)[\delta^{2T}\bar{g}_i + \delta^{2T+1}\bar{g}_i + \cdots + \delta^{3T-1}\bar{g}_i]\\
& + P\left(s(r)=1|p_i,\hat{b}_i,a_{-i}^*\right) P\left(s(r)=0|a^*\right)[\delta^{2T}\bar{g}_i + \delta^{2T+1}\bar{g}_i + \cdots + \delta^{3T-1}\bar{g}_i] + \cdots \Big\}\\
\bar{\upsilon}_i(\delta) = (1-\delta)\Big\{ & \bar{g}_i' + P\left(s(r)=0|p_i,\hat{b}_i,a_{-i}^*\right)\delta^{\mathrm{T}} g_i' + P\left(s(r)=0|p_i,\hat{b}_i,a_{-i}^*\right) P\left(s(r)=0|a^*\right)\delta^{2T} g_i'\\
& + P\left(s(r)=1|p_i,\hat{b}_i,a_{-i}^*\right) P\left(s(r)=0|a^*\right)\delta^{2T} g_i' + P\left(s(r)=0|p_i,\hat{b}_i,a_{-i}^*\right) P\left(s(r)=0|a^*\right)\\
& \times P\left(s(r)=0|a^*\right)\delta^{3T} g_i' + P\left(s(r)=1|p_i,\hat{b}_i,a_{-i}^*\right) P\left(s(r)=0|a^*\right) P\left(s(r)=0|a^*\right)\delta^{3T} g_i'\\
& + P\left(s(r)=0|p_i,\hat{b}_i,a_{-i}^*\right) P\left(s(r)=1|a^*\right) P\left(s(r)=0|a^*\right)\delta^{3T} g_i'\\
& + P\left(s(r)=1|p_i,\hat{b}_i,a_{-i}^*\right) P\left(s(r)=1|a^*\right) P\left(s(r)=0|a^*\right)\delta^{3T} g_i' + \cdots \Big\}
\end{aligned}$$

$$\begin{aligned}
\frac{\bar{\upsilon}_i(\delta)}{(1-\delta)} = {} & \bar{g}_i' + \bar{\gamma}\delta^{\mathrm{T}} g_i' + \bar{\gamma}\cdot\gamma\delta^{2T} g_i' + \bar{\gamma}\cdot\gamma\cdot\gamma\delta^{3T} g_i' + \bar{\gamma}\cdot\gamma\cdot\gamma\cdot\gamma\delta^{4T} g_i' + \cdots + \bar{\gamma}\cdot\gamma\cdot\alpha\cdot\gamma\delta^{4T} g_i' + \cdots\\
& + \bar{\gamma}\cdot\alpha\cdot\gamma\delta^{3T} g_i'\bar{\gamma}\cdot\alpha\cdot\gamma\cdot\gamma\delta^{4T} g_i' + \cdots + \bar{\gamma}\cdot\alpha\cdot\alpha\cdot\gamma\delta^{4T} g_i' + \cdots + \bar{\alpha}\cdot\gamma\delta^{2T} g_i'\\
& + \bar{\alpha}\cdot\gamma\cdot\gamma\delta^{3T} g_i' + \bar{\alpha}\cdot\gamma\cdot\gamma\cdot\gamma\delta^{4T} g_i' + \cdots + \bar{\alpha}\cdot\gamma\cdot\alpha\cdot\gamma\delta^{4T} g_i' + \cdots + \bar{\alpha}\cdot\alpha\cdot\gamma\delta^{3T} g_i'\\
& + \bar{\alpha}\cdot\alpha\cdot\gamma\cdot\gamma\delta^{4T} g_i' + \cdots + \bar{\alpha}\cdot\alpha\cdot\alpha\cdot\gamma\delta^{4T} g_i' + \cdots
\end{aligned}$$

$\bar{\alpha} = P(s(r)=1|p_i,\hat{b}_i,a^*_{-i}) = 1-\bar{\gamma}$ is the probability of nonunanimous profiles during deviation,

$\bar{g}_i = \sup_{p_i\in\Re_+} g_i(p_i,p^*_{-i})$ is the superior of the set of payoffs obtained from deviation, and

$\beta_i = \inf\{\beta_i(p_i) : g_i(p_i,p^*_{-i}) > g^*_i\}$ is the inferior probability of nonunanimous profiles during deviation.

Simplifying further, we obtain:

$$\begin{aligned}\bar{\upsilon}_i(\delta) &= (1-\delta)\bar{g}'_i + \bar{\gamma}\delta^{\mathrm{T}}\upsilon_i(\delta) + \bar{\alpha}\gamma\delta^{2T}\sum_{t=0}^{\infty}(\alpha\delta^{\mathrm{T}})^t\upsilon_i(\delta)\\ &= (1-\delta)\bar{g}'_i + \bar{\gamma}\delta^{\mathrm{T}}\upsilon_i(\delta) + \frac{\bar{\alpha}\gamma\delta^{2T}}{1-\alpha\delta^{\mathrm{T}}}\upsilon_i(\delta)\\ &= (1-\delta^{\mathrm{T}})\,\bar{g}_i + \left[\bar{\gamma}\delta^{\mathrm{T}} + \frac{\bar{\alpha}\gamma\delta^{2T}}{1-\alpha\delta^{\mathrm{T}}}\right]\upsilon_i(\delta).\end{aligned}$$

C. Derivation of (17)

This equation is derived from the fact that the payoff obtained from deviation to p_i should not be more than the payoff during collusion. The LHS term, $(1-\delta)g'_i + \gamma\delta^{\mathrm{T}}\upsilon_i(\delta) + (\alpha\gamma\delta^{2T}/1-\alpha\delta^{\mathrm{T}})\upsilon_i(\delta)$, is the payoff obtained from collusion which should not be less than the RHS, $(1-\delta)\bar{g}'_i + \bar{\gamma}\delta^{\mathrm{T}}\upsilon_i(\delta) + (\bar{\alpha}\gamma\delta^{2T}/1-\alpha\delta^{\mathrm{T}})\upsilon_i(\delta)$, which is the payoff obtained from a one step deviation. The derivation is as follows:

$$\begin{aligned}&(1-\delta)g'_i + \gamma\delta^{\mathrm{T}}\upsilon_i(\delta) + \frac{\alpha\gamma\delta^{2T}}{1-\alpha\delta^{\mathrm{T}}}\upsilon_i(\delta) \ge (1-\delta)\bar{g}'_i\\ &\qquad + \bar{\gamma}\delta^{\mathrm{T}}\upsilon_i(\delta) + \frac{\bar{\alpha}\gamma\delta^{2T}}{1-\alpha\delta^{\mathrm{T}}}\upsilon_i(\delta)\\ &\left[\gamma\delta^{\mathrm{T}} + \frac{\alpha\gamma\delta^{2T}}{1-\alpha\delta^{\mathrm{T}}} - \bar{p}\delta^{\mathrm{T}} - \frac{\bar{\alpha}\gamma\delta^{2T}}{1-\alpha\delta^{\mathrm{T}}}\right]\upsilon_i(\delta) \ge (1-\delta)\left(\bar{g}'_i - g'_i\right)\\ &\left[\delta^{\mathrm{T}}(\gamma-\bar{\gamma}) + \frac{\gamma\delta^{2T}}{1-\alpha\delta^{\mathrm{T}}}(\alpha-\bar{\alpha})\right]\upsilon_i(\delta) \ge (1-\delta)\left(\bar{g}'_i - g'_i\right)\\ &\left[\delta^{\mathrm{T}} - \frac{\gamma\delta^{2T}}{1-\alpha\delta^{\mathrm{T}}}\right]\left(\beta_i(p_i)-\alpha\right)\upsilon_i(\delta) \ge (1-\delta)\left(\bar{g}'_i - g'_i\right)\\ &\delta^{\mathrm{T}}\left(\frac{1-\delta^{\mathrm{T}}}{1-\alpha\delta^{\mathrm{T}}}\right)\left(\beta_i(p_i)-\alpha\right)\upsilon_i(\delta) \ge (1-\delta)\left(\bar{g}'_i - g'_i\right)\\ &\frac{\delta^{\mathrm{T}}(1-\delta^{\mathrm{T}})}{(1-\delta)(1-\alpha\delta^{\mathrm{T}})}(\beta_i-\alpha)\upsilon_i(\delta) \ge \frac{1-\delta^{\mathrm{T}}}{1-\delta}\left(\bar{g}'_i - g'_i\right)\\ &(1-\delta^{\mathrm{T}})g^*_i + \left[\gamma\delta^{\mathrm{T}} + \frac{\alpha\gamma\delta^{2T}}{1-\alpha\delta^{\mathrm{T}}}\right]\upsilon_i(\delta) \ge\\ &\qquad (1-\delta^{\mathrm{T}})\bar{g}_i + \left[\bar{\gamma}\delta^{\mathrm{T}} + \frac{\bar{\alpha}\gamma\delta^{2T}}{1-\alpha\delta^{\mathrm{T}}}\right]\upsilon_i(\delta)\\ &\left[\gamma\delta^{\mathrm{T}} + \frac{\alpha\gamma\delta^{2T}}{1-\alpha\delta^{\mathrm{T}}} - \bar{\gamma}\delta^{\mathrm{T}} - \frac{\bar{\alpha}\gamma\delta^{2T}}{1-\alpha\delta^{\mathrm{T}}}\right]\upsilon_i(\delta) \ge (1-\delta^{\mathrm{T}})\left(\bar{g}_i - g^*_i\right)\\ &\left[\delta^{\mathrm{T}}(\gamma-\bar{\gamma}) + \frac{\gamma\delta^{2T}}{1-\alpha\delta^{\mathrm{T}}}(\alpha-\bar{\alpha})\right]\upsilon_i(\delta) \ge (1-\delta^{\mathrm{T}})\left(\bar{g}_i - g^*_i\right)\\ &\left[\delta^{\mathrm{T}} - \frac{\gamma\delta^{2T}}{1-\alpha\delta^{\mathrm{T}}}\right]\left(\beta_i(p_i)-\alpha\right)\upsilon_i(\delta) \ge (1-\delta^{\mathrm{T}})\left(\bar{g}_i - g^*_i\right)\\ &\delta^{\mathrm{T}}\left(\frac{1-\delta^{\mathrm{T}}}{1-\alpha\delta^{\mathrm{T}}}\right)\left(\beta_i(p_i)-\alpha\right)\upsilon_i(\delta) \ge (1-\delta^{\mathrm{T}})\left(\bar{g}_i - g^*_i\right)\\ &\frac{\delta^{\mathrm{T}}(1-\delta^{\mathrm{T}})}{(1-\delta)(1-\alpha\delta^{\mathrm{T}})}(\beta_i-\alpha)\upsilon_i(\delta) \ge \frac{1-\delta^{\mathrm{T}}}{1-\delta}\left(\bar{g}_i - g^*_i\right)\\ &\frac{\delta^{\mathrm{T}}}{1-\alpha\delta^{\mathrm{T}}}(\beta_i-\alpha)\upsilon_i(\delta) \ge \bar{g}_i - g^*_i.\end{aligned}$$

D. Derivation of (18) and (19)

Equation (18) is derived from (15) where we assume that there is a small number ϵ such that:

$$\begin{aligned}\upsilon_i(\delta) = (1-\alpha\delta^{\mathrm{T}})g^*_i &> g^*_i - \epsilon\\ -\alpha\delta^{\mathrm{T}}g^*_i &> -\epsilon\\ \delta^{\mathrm{T}} &< \frac{\epsilon}{\alpha g^*_i}\end{aligned}$$

For this inequality to be true, (18) is required. This inequality is used to substitute $\upsilon_i(\delta)$ in (17) to obtain (19), as follows:

$$\begin{aligned}&\frac{\delta^{\mathrm{T}}}{1-\alpha\delta^{\mathrm{T}}}(\beta_i-\alpha)\upsilon_i(\delta) \ge \bar{g}_i - g^*_i\\ &\delta^{\mathrm{T}}(\beta_i-\alpha)\left(g^*_i-\epsilon\right) \ge \left(1-\alpha\delta^{\mathrm{T}}\right)\left(\bar{g}_i-g^*_i\right)\\ &\delta^{\mathrm{T}} \ge \frac{\left(\bar{g}_i-g^*_i\right)}{(\beta_i-\alpha)\left(g^*_i-\epsilon\right)+\alpha\left(\bar{g}_i-g^*_i\right)}.\end{aligned}$$

E. Derivation of (20)

Combining (18) and (19), and obtaining the intersection for every node i, (20) is derived as follows:

$$\begin{aligned}&\max_{i\in I}\frac{\left(\bar{g}_i-g^*_i\right)}{(\beta_i-\alpha)\left(g^*_i-\epsilon\right)+\alpha\left(\bar{g}_i-g^*_i\right)} \le \delta^{\mathrm{T}} < \min_{i\in I}\frac{\epsilon}{\alpha g^*_i}\\ &\max_{i\in I}\frac{\left(\bar{g}_i-g^*_i\right)}{(\beta_i-\alpha)\left(g^*_i-\epsilon\right)+\alpha\left(\bar{g}_i-g^*_i\right)} < \min_{i\in I}\frac{\epsilon}{\alpha g^*_i}\\ &\max_{i\in I}\frac{\left(\bar{g}_i-g^*_i\right)/\epsilon}{(\beta_i/\alpha-1)\left(g^*_i-\epsilon\right)+\left(\bar{g}_i-g^*_i\right)} < \min_{i\in I}\frac{1}{g^*_i}\\ &\min_{i\in I}\left[1+\left(\frac{\beta_i}{\alpha}-1\right)\frac{\left(g^*_i-\epsilon\right)}{\left(\bar{g}_i-g^*_i\right)}\right]\epsilon < \max_{i\in I} g^*_i\end{aligned}$$

References

[1] S. Shenker, "Making greed work in networks: Game theoretic analysis of switch service disciplines," *IEEE/ACM Trans. Netw.*, vol. 3, no. 6, pp. 819–831, Dec. 1995.

[2] *Nokia Rooftop Wireless Routing, White Paper*, Nokia Networks, 2001.

[3] A. B. MacKenzie and S. B. Wicker, "Selfish users in Aloha: A game-theoretic approach," in *Proc. IEEE VTS 54th—VTC*, Atlantic City, NJ, Oct. 7–11, 2001, pp. 1354–1357.

[4] A. B. MacKenzie and S. B. Wicker, "Stability of multipacket slotted Aloha with selfish users and perfect information," in *Proc. 22nd IEEE INFOCOM*, San Francisco, CA, Mar. 30–Apr., 3, 2003, pp. 1583–1590.

[5] L. Buttyan and J. P. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," *ACM/Kluwer Mobile Netw. Appl.*, vol. 8, no. 5, pp. 579–592, Oct. 2003.

[6] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proc. IFIP TC6/TC11 6th CMS*, Portoroz, Slovenia, Sep. 26–27, 2002, pp. 107–121.

[7] S. Buchegger and J. Y. L. Boudec, "Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks," in *Proc. 10th EMPDP*, Canary Islands, Spain, Jan. 9–11, 2002, pp. 403–410.

[8] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 6th MobiCom*, Boston, MA, Aug. 6–10, 2000, pp. 255–265.

[9] C. U. Saraydar, N. B. Mandayam, and D. J. Goodman, "Efficient power control via pricing in wireless data networks," *IEEE Trans. Commun.*, vol. 50, no. 2, pp. 291–303, Feb. 2002.

[10] L. Anderegg and S. Eidenbenz, "Ad hoc-VCG: A truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents," in *Proc. 9th MobiCom*, San Diego, CA, Sep. 14–19, 2003, pp. 245–259.

[11] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad hoc networks," in *Proc. 22nd IEEE INFOCOM*, San Francisco, CA, Mar. 30–Apr. 3 2003, pp. 1987–1997.

[12] A. Urpi, M. Bonuccelli, and S. Giordano, "Modelling cooperation in mobile ad hoc networks: A formal description of selfishness," in *Proc. WiOpt*, Sophia-Antipolis, France, Mar. 3–5, 2003, pp. 3–5.

[13] S. Bandyopadhyay, "A game-theoretic analysis on the conditions of cooperation in a wireless ad hoc network," in *Proc. 3rd WiOpt*, Trentino, Italy, Apr. 4–6, 2005, pp. 54–58.

[14] V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, and R. R. Rao, "Cooperation in wireless ad hoc networks," in *Proc. 22nd IEEE INFOCOM*, San Francisco, CA, Mar. 30–Apr. 3 2003, pp. 808–817.

[15] Z. Han, C. Pandana, and K. J. R. Liu, "A self-learning repeated game framework for optimizing packet forwarding networks," in *Proc. IEEE WCNC*, New Orleans, LA, Mar. 13–17, 2005, pp. 2131–2136.

[16] S. Zhong, L. Li, Y. G. Liu, and Y. Yang, "On designing incentive-compatible routing and forwarding protocols in wireless ad hoc networks—An integrated approach using game theoretical and cryptographic techniques," in *Proc. 11th MobiCom*, Cologne, Germany, Aug. 28–Sep. 2, 2005, pp. 117–131.

[17] M. Aoyagi, "Collusion in dynamic bertrand oligopoly with correlated private signals and communication," *J. Econ. Theory*, vol. 102, no. 1, pp. 229–248, Jan. 2002.

[18] D. Niyato and E. Hossain, "Competitive pricing for spectrum sharing in cognitive radio networks: Dynamic game, inefficiency of nash equilibrium, and collusion," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 192–202, Jan. 2008.

[19] Y. Xi and E. Yeh, "Equilibria and price of anarchy in parallel relay networks with node pricing," in *Proc. 42nd Annu. Conf. Inf. Sci. Syst.*, Princeton, NJ, Mar. 19–21, 2008, pp. 944–949.

[20] E. J. Green and R. H. Porter, "Noncooperative collusion under imperfect price information," *Econometrica*, vol. 52, no. 1, pp. 87–100, Jan. 1984.

[21] O. Compte, "Communication in repeated games with imperfect private monitoring," *Econometrica*, vol. 66, no. 3, pp. 597–626, May 1998.

[22] M. Kandori and H. Matsushima, "Private observation, communication and collusion," *Econometrica*, vol. 66, no. 3, pp. 627–652, May 1998.

[23] N. B. Salem and J.-P. Hubaux, "A fair scheduling for wireless mesh networks," in *Proc. 1st IEEE Workshop Wireless Mesh Netw.*, Santa Clara, CA, Sep. 26, 2005. [Online]. Available: http://www.cs.ucdavis.edu/~prasant/wimesh

[24] I. Rhee, A. Warrier, J. Min, and L. Xu, "DRAND: Distributed randomized TDMA scheduling for wireless adhoc networks," in *Proc. 7th ACM MobiHoc*, Florence, Italy, May 22–25, 2006, pp. 190–201.

[25] G. Brar, D. M. Blough, and P. Santi, "Computationally efficient scheduling with the physical interference model for throughput improvement in wireless mesh networks," in *Proc. 12th MobiCom*, Los Angeles, CA, Sep. 26–29, 2006, pp. 2–13.

See-Kee Ng received the M.Eng. degree from the National University of Singapore, Singapore, in 2008.

He is currently an Assistant Principal Engineer with the Singapore Technologies Kinetics, Singapore, where he is working on robotics communication and architecture. Prior to this, he has worked for about ten years in the telecommunication sector and defense sector including the Defense Science Organization in Singapore where he was involved in the research and application of mobile *ad hoc* networks, on areas such as swarming, directional communication, and quality of service for medium access controllers.

Winston K. G. Seah (M'87–SM'03) received the Dr. Eng. degree from Kyoto University, Kyoto, Japan, in 1997.

He is currently a Professor of network engineering with the School of Engineering and Computer Science, Victoria University of Wellington, Wellington, New Zealand. Prior to this, he has worked for more than 15 years in mission-oriented research, taking ideas from theory to prototypes, most recently, as a Senior Scientist (networking protocols) with the Institute for Infocomm Research (I^2R), Singapore. He was also an Adjunct Associate Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, and an Adjunct Faculty with the Graduate School for Integrative Science and Engineering, National University of Singapore, Singapore. He is actively involved in research in the areas of mobile *ad hoc* and sensor networks, and codeveloped one of the first quality-of-service models for mobile *ad hoc* networks. His latest research interests include wireless sensor networks powered by ambient energy harvesting, wireless multihop networks, and mobility-enhanced protocols and algorithms for networked swarm robotics and sensing applications in terrestrial and oceanographic networks. He is on the Technical Program Committee of numerous conferences and reviewer of papers for many key journals and conferences in the area of wireless mesh, *ad hoc*, and sensor networks.

Dr. Seah is a professional member of the Association for Computing Machinery. http://ecs.victoria.ac.nz/Main/WinstonSeah