Equilibria for Node Participation in Ad Hoc Networks – An Imperfect Monitoring Approach

Vivek Srivastava and Luiz A. DaSilva
Bradley Department of Electrical and Computer Engineering,
Virginia Polytechnic Institute and State University,
Arlington, VA, USA – 22203.

Abstract **– In self-organizing networks, nodes are expected to perform services (such as forwarding packets) for one another. The design of incentive mechanisms that lead nodes to participate towards a network-wide goal is crucial for the deployment of such networks in commercial environments. In this paper we employ game theory to analyze a behavior-based incentive scheme that helps to achieve a socially optimal solution in the presence of varying node participation levels. Our analysis includes an evaluation of the effectiveness of the scheme in achieving an optimal solution as well as stability considerations. One of the contributions of this work is modeling of imperfect monitoring, recognizing that in practice nodes do not have perfect information regarding their neighbors' actions.**

I. Introduction

A self-organized network comprises independent, autonomous nodes in a distributed architecture without any central or external control. Nodes interact locally to achieve global properties such as connectivity and stability of the entire network [1]. These interactions require nodes to cooperate and trust one another to accomplish various tasks. Examples of self-organized networks include mobile ad hoc networks and sensor networks. In an ad hoc network, each node shares its resources to provide services for others. However, since nodes are resource constrained (e.g. limited battery, low bandwidth) they tend to vary their behavior for voluntarily contributing resources. The variation in behavior arises due to trade-offs experienced by a node in sharing its limited resources. For instance, a node by forwarding packets for others could deplete its limited energy supply. As a result a node would tend to not forward at all unless it derives some benefit in doing so. Such selfish behavior in a self-organized network could lead to a disruption of its normal operation.

One technique to discourage selfish behavior is through the inclusion of an incentive mechanism that leads to node participation in providing services for others. There are two broad approaches in designing such a mechanism:

- Credit-based: In this approach nodes are rewarded (or charged) for the services offered (or requested). Each node is rewarded with actual or virtual currency for services rendered. This currency can then be utilized in requesting services from other nodes. Mechanisms proposed in [2-6] adopt this approach leading to nodes' sharing their resources in order to gain credit. Also, some of these mechanisms are made robust to cheating by fixing prices leveraging the concept of mechanism design [2, 4-6].
- Behavior-based: In this approach nodes are evaluated based on a history of their behavior in the network. Some of the mechanisms which adopt this approach are typically implemented as (a) reputation schemes (such as those proposed in [7, 8]) with each node maintaining a reputation for every other node in the network; or (b) simple heuristics-based schemes in which the threat of retaliation encourages selfish nodes to cooperate. An example of the latter is the tit-for-tat mechanism in which nodes follow a strategy of mimicking the behavior of their peers [9].

A rigorous analysis of incentives for node cooperation in ad hoc environments is crucial for the design of such mechanisms. It provides answers to key questions related to (a) the effectiveness of the designed mechanism in discouraging selfish behavior; (b) stability of the network under the designed mechanism parameters; and (c) robustness to a wide range of node behaviors, including malicious behavior. Note that, typically, malicious behavior is characterized by an active intent of the node to disrupt the network without any consideration for its own resources. We focus on selfish, rather than malicious, behavior in this research.

In this work we employ game theory to analyze an incentive scheme to encourage cooperation among independent selfish nodes. Here, nodes adopt a strategy which exploits the intrinsic 'fear' of punishment if any node fails to cooperate. In particular, we analyze node behavior in forwarding packets for other nodes.

We exercise game theory in our study as it provides a suite of tools to study conflict and cooperation among distributed and independent entities. In addition, it offers solution techniques which can be used to derive conditions under which a socially optimal solution can be achieved. Within the context of node participation, we define social optimality as the scenario where all nodes are willing to make their resources available to others. In this work, we study the problem of varying levels of node participation while forwarding packets for others.

We start with a brief review of related work and follow it up with a description of the game theoretic model employed. The model is then analyzed to determine the equilibrium conditions. We close the paper with a discussion of our main conclusions and directions for future investigation.

II. Related work

In the recent literature, different ad hoc networking games have been proposed to analyze the problem of selfish node behavior in forwarding packets [10-16]. In these games, nodes select the proportion of packets they are willing to forward with the objective of minimizing the use of their resources. A steady state analysis of the game leads to the intuitive conclusion that in the absence of incentive schemes, the best strategy for nodes is to not forward. Furthermore, [10-13, 15, 16] extend the analysis to include heuristics-based repeated game strategies, and derive conditions that lead to a socially optimal solution. However, one of the key assumptions in these models is that each node has perfect knowledge of every other node's forwarding decisions. To obtain this information, a node would need to constantly monitor its neighbors' transmissions, periodically switching the network interface to promiscuous mode of operation. In practice, this approach is costly from the energy consumption stand point and is liable to errors.

In this work, we relax the assumption of perfect knowledge and develop a game theoretic model in which nodes do not explicitly monitor other nodes' actions. Instead, a node observes a random public signal which is correlated to the actions of all other nodes in the game. Note that in these games all nodes observe the same value of the public signal. In addition, since there is no uncertainty regarding the *type* of a node these games differ from repeated games with incomplete information [17]. We adopt a strategy wherein nodes participate pending the activation of a trigger which causes the nodes to switch to not participate, henceforth. This type of formulation is known as a grim trigger strategy [9]. For simplicity of analysis, we assume that this strategy is being followed by all nodes in the network.

The main contributions of this paper are: (a) to develop an imperfect public monitoring game theoretic model for node participation; (b) to analyze the effectiveness of the grim trigger strategy for this model in preventing selfish behavior from disrupting the network; and (c) to determine the stability of the network under this strategy. We develop an infinitely repeated game model of imperfect monitoring with the utility to the node discounted at every stage.

III. Game – theoretic model

We begin with modeling node participation as a single stage strategic form game *G*. Let *N* be the finite, non-empty set of nodes in the network with $n = |N|$ - the cardinality of the set, $(A_i)_{i\in N}$ be the sets of actions available to each player *i*, $A = \times_{i\in N} A_i$ be the joint action space given by the Cartesian product of the individual nodes' action sets, *P* be the random public signal which takes values, *p*, in $\Omega \subseteq R$ and $U_i(a_i, p)$ be the single stage utility function for node *i*. The utility function is stochastic in nature and depends on the realization of the random public signal. We start by expressing utility as the sum of two components, benefit and cost:

$$U_i(a_i, p) = \alpha_i(p) + \beta_i(a_i) \qquad (1)$$

- $\alpha_i(p)$ - benefit accrued by node *i* from the willingness of other nodes to forward node *i*'s packets. The benefit depends on the random signal which reflects the actions played by every node.
- $\beta_i(a_i)$ - cost accrued, in terms of resources shared, by forwarding packets for other nodes. We assume the cost to be a function of the node's own strategy only. Note that the cost is generally negative in value. (The cost incurred by a node does increase if fewer nodes are willing to forward packets. However, this characteristic is not captured by our model).

One of the key challenges in the design of an imperfect monitoring game is the selection of a public signal as it should possess the following properties [18] :

- The signal reflects the actions selected by each node in the network;
- The realization of the signal after each stage is known publicly by all nodes of the game; and
- The signal is randomly correlated to the joint action profile.

For an ad hoc network, one can consider the public signal to be a performance metric which reflects the overall state of the network. From the perspective of forwarding levels, the aggregate network goodput can be one such candidate. It reflects the actions selected by the individual nodes and in the absence of a centralized mechanism, nodes may exchange some indication of goodput experienced by each node and thereby estimate aggregate goodput. The correlation of the public signal to nodes' actions is captured in the parameterization of the distribution function of *p* by the joint action profile of all nodes, $\mathbf{a}$, and denoted by $F(p;\mathbf{a})$. Since the utility is non-deterministic, we define the expected utility, π_i for node *i* as a function of the joint action profile. It is expressed as:

$$\pi_i(\mathbf{a}) = \int_{p\in\Omega} U_i(a_i, p).dF(p;\mathbf{a}). \qquad (2)$$

We consider homogenous action sets for all nodes: each node selects the proportion of packets it is willing to forward, $A_i = [0,1]$. A Nash equilibrium [17] of *G* is the action profile which serves as the mutual best response for every node *i*. Expressing it in terms of the expected utility, if $\mathbf{a}$ is a Nash equilibrium:

$$\pi_i(\mathbf{a}) \ge \pi_i(a_i', \mathbf{a}_{-\mathbf{i}}) \quad \forall a_i' \in A_i \quad \forall i. \qquad (3)$$

For our formulation, it is straight forward to show that in the absence of incentive schemes it is best for nodes to not participate. Therefore, the Nash equilibrium for the singe stage strategic form game is non-optimal.

IV. Repeated Game with Imperfect Public Monitoring

Other equilibria (possibly optimal ones) are achievable when *G* is repeated. In addition, we introduce uncertainty in monitoring actions of other nodes to develop a repeated game with infinite stages in which nodes observe the value of the public signal at the end of every stage. The notion of perfect public equilibrium [18] is adopted as the solution to the repeated game.

A. Model

Let G^{∞} denote the infinitely repeated game with imperfect monitoring. The strategy of node *i* in each stage, *t*, is a function of the past values of the public signal, alone. We denote this *public* strategy as $\sigma_i(t):\Omega^{t-1} \to A_i$, with $\boldsymbol{\sigma}(t)$ - the joint strategy vector in stage *t*. For example, in stage 1 we have $\boldsymbol{\sigma}(1) = \mathbf{a}$. Let Σ_i be the set of repeated game strategies for node *i* such that for any stage *t* $\sigma_i(t) \in \Sigma_i$. The individual stage payoffs for each node are discounted by $\delta \in (0,1)$. Let $v_i(\boldsymbol{\sigma})$ denote the repeated game payoff for node *i*, where $\boldsymbol{\sigma}$ is the joint public strategy profile. The (average) discounted expected game payoff for a node *i* is given by:

$$v_i(\boldsymbol{\sigma}) = (1-\delta)\sum_{\mathbf{t}=\mathbf{0}}^{\infty} \delta^{t-1} \pi_i(\boldsymbol{\sigma}(t)). \quad (4)$$

A public strategy $\boldsymbol{\sigma}$ is a perfect public equilibrium (PPE) if after any stage *t*, $\boldsymbol{\sigma}$ forms a Nash equilibrium from that stage on. Mathematically, after every stage *t*

$$v_i(\boldsymbol{\sigma}) \geq v_i(\sigma_i', \boldsymbol{\sigma}_{-\mathbf{i}}) \quad \forall i \quad \forall \sigma_i' \in \Sigma_i. \quad (5)$$

B. Reduction to a single stage game

In order to simplify the evaluation of a PPE, we exploit the recursive nature of the repeated game and reduce it to an equivalent single stage game. The resulting single stage game can be denoted as $G_w = \left\langle N, \mathbf{A}, \pi_w^i \right\rangle$ where: N is the set of nodes in the network; $\mathbf{A} = \times_{i \in N} A_i$ is the joint action space; and π_w^i is the equivalent expected utility. We express the equivalent utility as:

$$\pi_w^i(\mathbf{a}) = (1-\delta)\pi_i(\mathbf{a}) + \delta \int_{p \in \Omega} w_i(p) dF(p;\mathbf{a}) \quad (6)$$

where, $w_i(p):\Omega \to W$ is a continuation payoff function that maps every possible value of the public signal to a continuation payoff selected from $W \subset \mathbf{R}^n$ for a node *i*. For the repeated game, the equivalent utility represents a sum of the expected payoff for the first stage of the game (due to action $\mathbf{a}$ played) and a continuation payoff for the remaining stages which results due to the correlation of $\mathbf{a}$ with the public signal.

Applying this representation to the repeated game payoff we can then write it as:

$$v_i(\boldsymbol{\sigma}) = (1-\delta)\pi_i(\mathbf{a}) + \delta \int_{p \in \Omega} w_i(p) dF(p;\mathbf{a}). \quad (7)$$

If $\boldsymbol{\sigma}$ is to be a PPE of the repeated game, then $\mathbf{a}$ must be a Nash equilibrium in the first stage of the game. Therefore, we can say that $\boldsymbol{\sigma}$ is a PPE if:

$$v_i(\boldsymbol{\sigma}) \geq (1-\delta)\pi_i(a_i, \mathbf{a}_{-\mathbf{i}}) + \delta \int_{p \in \Omega} w_i(p) dF(p; a_i, \mathbf{a}_{-\mathbf{i}}) \quad \forall i \quad \forall a_i \in A_i. \quad (8)$$

For a detailed discussion on theory of repeated games with imperfect public monitoring, readers should refer to [18].

C. Grim Trigger Strategy

Consider the grim trigger strategy $(\hat{\sigma}_i)$ where each node forwards all the packets it receives $(\hat{a}_i = 1)$ as long as the value of the public signal is above a certain threshold (x), and when below, it ceases to forward. In other words, each node switches to the Nash equilibrium of the single stage game when the signal is below the set threshold. Again, for simplicity we assume that each node adopts the same threshold. The trigger, which is activated as soon as the value of the signal falls below the threshold, is considered grim as the nodes do not switch their action back to forwarding all packets once the punishment (drop every packet) phase has been initiated. Let $\hat{\boldsymbol{\sigma}} = \left\langle \hat{\sigma}_1, \hat{\sigma}_2, \ldots, \hat{\sigma}_n \right\rangle$ denote such a strategy with $\hat{\mathbf{a}} = \left\langle \hat{a}_1, \hat{a}_2, \ldots, \hat{a}_n \right\rangle$ corresponding to the desirable action where every node forwards all packets. The associated payoff received by node *i* is given by:

$$v_i(\hat{\boldsymbol{\sigma}}) = (1-\delta)\pi_i(\hat{\mathbf{a}}) + \delta \int_{p \in \Omega} w_i(p) dF(p;\hat{\mathbf{a}}). \quad (9)$$

Therefore, a node following this strategy continues to receive a payoff v_i until the trigger is activated, after which it receives the Nash equilibrium payoff. Since every node follows the same strategy we can express the continuation payoff function as:

$$w(p) = \begin{cases} v_i & if \quad p > x \\ \pi^{NE} & if \quad p \leq x \end{cases} \quad (10)$$

where, π^{NE} is the Nash equilibrium payoff. The repeated game payoff now reduces to:

$$v_i(\hat{\boldsymbol{\sigma}}) = (1-\delta)\pi_i(\hat{\mathbf{a}}) + \delta[v_i(1-F(x;\hat{\mathbf{a}})) + \pi^{NE} F(x;\hat{\mathbf{a}})]. \quad (11)$$

For $\hat{\boldsymbol{\sigma}}$ to be a PPE, it must be a Nash equilibrium for each node to forward all packets i.e. $\hat{\mathbf{a}}$ should be incentive compatible $\forall i$. Therefore,

$$v_i(\hat{\boldsymbol{\sigma}}) \geq (1-\delta)\pi_i(a_i, \hat{\mathbf{a}}_{-\mathbf{i}}) + \delta[v_i(1-F(x; a_i, \hat{\mathbf{a}}_{-\mathbf{i}})) + \pi^{NE} F(x; a_i, \hat{\mathbf{a}}_{-\mathbf{i}})]. \quad (12)$$

Since at Nash equilibrium none of the nodes forward any packets, we have $\pi^{NE} = 0$. Substituting in (11) and (12), we get:

$$\frac{1-\delta+\delta F(x; a_i, \hat{\mathbf{a}}_{-\mathbf{i}})}{1-\delta+\delta F(x;\hat{\mathbf{a}})} \geq \frac{\pi_i(a_i, \hat{\mathbf{a}}_{-\mathbf{i}})}{\pi_i(\hat{\mathbf{a}})}. \quad (13)$$

Hence the grim trigger strategy is a PPE if the above inequality is satisfied for any deviation a_i and $\forall i$. We base the above derivation on a similar analysis done to determine collusion in repeated games in [19]. We assume that $F(\bullet;\hat{\mathbf{a}})$ stochastically dominates $F(\bullet; a_i, \hat{\mathbf{a}}_{-\mathbf{i}})$ for any profitable deviation a_i i.e. $F(\bullet;\hat{\mathbf{a}}) \leq F(\bullet; a_i, \hat{\mathbf{a}}_{-\mathbf{i}})$ for $\pi_i(a_i, \hat{\mathbf{a}}_{-\mathbf{i}}) \geq \pi_i(\hat{\mathbf{a}})$. This means that for a given threshold value, if a node benefits by deviating from $\hat{a}_i$, it increases the chances of triggering the grim period earlier by risking the public signal to fall below the threshold. It is clear to see that the stochastic dominance property of the distribution function satisfies a necessary condition for the grim trigger strategy to be an equilibrium under a profitable deviation. In addition under the assumption of stochastic dominance, the equilibrium also holds for non-profitable deviations of $\hat{a}_i$.

D. Determination of the threshold range to sustain equilibrium

Even though the distribution function is assumed to be stochastic dominant, it is not sufficient to show that the condition is satisfied for all possible values of the threshold. Therefore, it is important to determine the range of threshold values for which the condition holds. In order to do so, we vary the threshold values and check if the inequality condition is satisfied under a single node deviation from $\hat{a}_i = 1$ to $a_i = 0$. Prior to the determination of the range, we need to specifically characterize the benefit and the cost functions. Since the benefit accrued by a node is expected to increase with an increase in the forwarding levels of the other nodes, we assume it to be linearly correlated to the public signal i.e. $\alpha_i(p) = k_i p$. Here, $k_i \in [0,1]$ parameterizes the perceived benefit for each node. The cost incurred by a node is a function of its own actions and is equal to the node's forwarding level, i.e. $\beta_i(a_i) = -a_i$. For illustration purposes we assume the public signal (which, as discussed previously, could be some indicator of aggregate goodput for the network) to be gamma distributed with the shape parameter of the distribution equal to the sum of the joint actions of the nodes. Hence, the cumulative distribution function is given by $F(p;\hat{\mathbf{a}}) = \dfrac{\Gamma_p(a')}{\Gamma(a')}$ where, $a' = \sum_{i \in N} \hat{a}_i$ is the shape parameter of the gamma distributed random variable. Here, $\Gamma_p(a')$ is the incomplete gamma function, $\Gamma_p(a') = \int_0^p t^{a'-1} e^{-t} dt$. We select the signal to be gamma distributed as it satisfies the necessary requirement of stochastic dominance such that $F(\bullet;\gamma) \le F(\bullet;\mu)$ for $\gamma > \mu$ with $\gamma, \mu > 0$. Substituting the expression for the gamma distribution, the expected utility to any node i when all nodes participate, i.e. $\hat{a}_i = 1 \;\; \forall i$ is

$$\pi_i(\hat{\mathbf{a}}) = \int_{p \in \Omega} (k_i p - 1) dF(p;\hat{\mathbf{a}}) - 1 = k_i E[p] - 1 \qquad (14)$$

where, $E[p]$ is the expected value of p. Since the expected value of a gamma distributed random variable is equal to its shape parameter, we have $\pi_i(\hat{\mathbf{a}}) = k_i a' - 1 = k_i n - 1, \forall i$. Now, if any node deviates from $\hat{a}_i = 1$ to $a_i = 0$ the expected utility reduces to $\pi_i(a_i, \hat{\mathbf{a}}_{-\mathbf{i}}) = k_i a' = k_i(n-1), \forall i$. Replacing the expected utilities, equation (13) now reduces to:

$$n\delta\Gamma_x(n-1)(nk_i - 1) - \delta\Gamma_x(n)(nk_i - k_i) \ge n!(1-\delta)(1-k_i). \qquad (15)$$

We determine the range of threshold values for different network sizes for which equation 15 holds (see Fig. 1). The range is obtained by averaging over 50 different random values of k_i for a fixed value of the discount factor $(\delta = 0.7)$. For the evaluation the incomplete gamma function is numerically computed according to the numerical algorithm presented in [20]. From Fig. 1 we conclude that for larger network sizes, the range of threshold values for which the condition is satisfied is greater. It is easy to deduce this from the condition above since for higher values of n, the inequality $n\Gamma_x(n-1) > \Gamma_x(n)$ holds true over a larger range of x. In addition, this also signifies that as the size of the network increases a node experiences greater benefit in participating and switches to a grim action only for much lower thresholds. This leads to a much wider choice in the selection of the threshold without violating the condition for equilibrium. We also varied the discount factor and observed that for higher values, the range of the threshold tends to increase for a given network size. This is expected as for higher values of δ equation (15) holds true for a broader range of values of x. This signifies that as a node's value for its future payoff improves, it perceives a benefit in participating.

E. Stability of network under the heuristic-based scheme

Apart from evaluating the effectiveness of a scheme in discouraging selfish behavior it is also important to study its effect on network stability, namely how does it affect the sensitivity of individual nodes to changes triggered by actions of its peers? For the grim trigger strategy under consideration a node is triggered to change its action based on a comparison of the realized value of the random signal to a set threshold. We consider the network to be stable if a deviation by a node (or nodes) from $a_i = 1$ to $a_i = 0$ at any stage does not lead to a cascading effect of other node deviations in the subsequent stages. The stability is evaluated in terms of the average number of stages, after nodes (or a node) deviate(s), for which a cascading effect is observed. In addition, we also rate the stability by calculating the percentage of total runs for which a cascading event is observed.

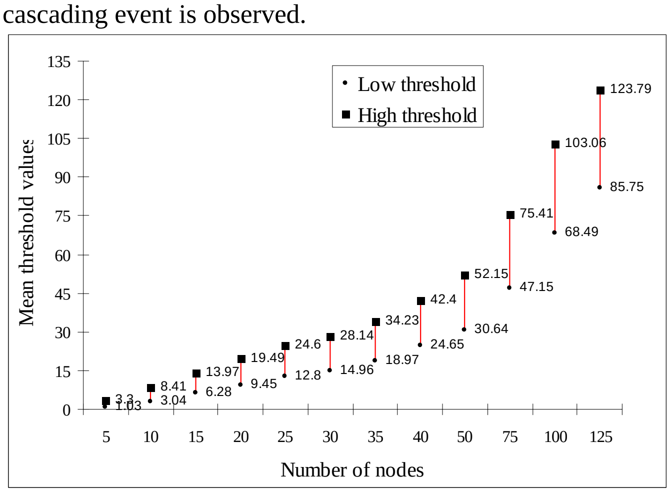

Figure 1. Plot of the mean threshold values for which the equilibrium condition is satisfied for different network sizes.

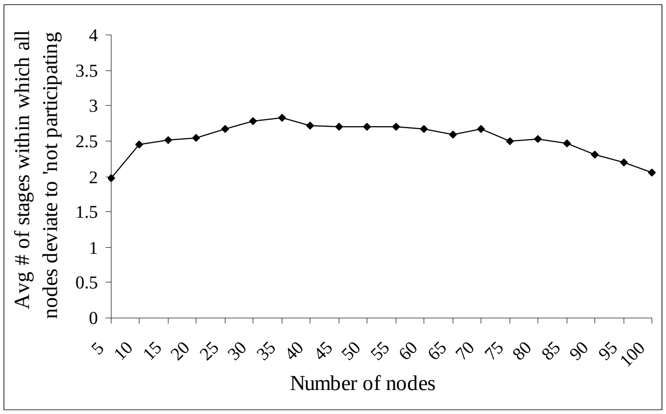

Figure 2. Plot of the average number of stages during which cascading is observed for the grim trigger strategy.

We perform this evaluation by randomly selecting a threshold value for every node from the pre-determined range (shown in Fig.1) for which the strategy is an equilibrium. For every stage we generate a gamma distributed random value, using algorithms proposed in [21] and [22], whose distribution function is parameterized by the joint action of the nodes played in that stage. A node deviates if the generated value is lower than its selected threshold. As a result of this deviation the probability of generating a lower random value in the subsequent stage increases, thereby increasing the chances of further node deviations. Fig. 2 shows the average number of stages, for different network sizes, after which all nodes decide to not participate. From the figure we can conclude that the trigger point for a node following the grim trigger strategy is too sensitive to other nodes' deviations. This is because slight node deviations coupled with the random nature of the public signal causes premature triggering, thereby leading to a cascading effect. Also, we observe, from Fig. 3, that cascading occurs for a high percentage of runs for a given network size. The number of the nodes has little effect on whether the cascading effect occurs.

We therefore "soften" the sensitivity of the trigger by considering two modifications of the grim trigger strategy:

a. The trigger for a node is activated only when the *n*-stage running average of the realized public signal is below the set threshold. Though there is no restriction on how large the value of *n* can be, for our evaluation we assume it to be equal to 3; and

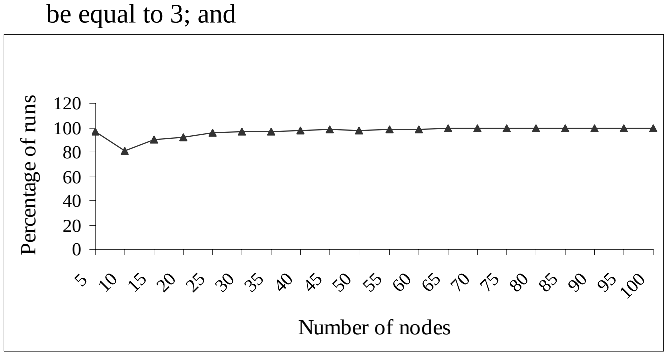

Figure 3. Plot of the percentage of runs for which cascading is observed for traditional grim trigger strategy.

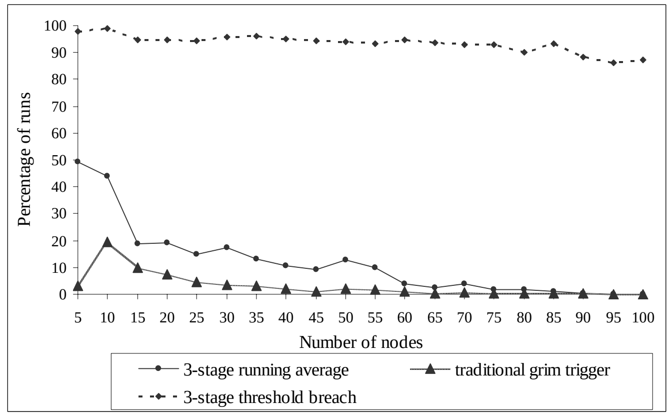

Figure 4. Comparison of the percentage of runs for which cascading is not observed for the grim trigger and modified grim trigger strategies.

b. The trigger for a node is activated when the random signal is below the set threshold for *n* consecutive stages. We again assume *n* to be equal to 3.

Fig. 4 includes a comparison of the percentage of total runs for which cascading is not observed for the two modifications to the grim trigger strategy. We see that nodes following the modified strategies are less sensitive to the randomness of the public signal making them less sensitive to changes in other nodes' behaviors, as expected. Therefore, even though the grim trigger strategy is effective in providing a socially optimal equilibrium, it has a drawback with regards to the stability of the network for nodes following that strategy. A small modification in the trigger leads to significantly more stable behavior.

V. CONCLUSIONS

In this work we presented a game theoretic analysis of a behavior-based scheme in which nodes adopt a grim trigger strategy to induce participation. Under the assumption of first order stochastic dominance of the public signal, we show this strategy to lead to an equilibrium for nodes to participate. For an imperfect monitoring environment we observe that the trigger point for the grim trigger strategy is very sensitive to slight changes in other nodes' actions, potentially making the network unstable. By considering a smoother condition for activation of the trigger we can reduce this sensitivity caused due to the randomness of the public signal. As a future extension to this work, we plan to apply node participation in topology control and route selection, where nodes aim to develop a topology which will guarantee connectivity and end-to-end packet delivery. One of the promising applications of the imperfect monitoring analysis could be to gauge the effectiveness of the grim trigger strategy towards the detection and isolation of a malicious node. We plan to leverage the results from this study in analyzing reputation mechanisms developed to isolate such nodes.

REFERENCES

[1] C. Prehofer and C. Bettstetter, "Self-organization in communication networks: principles and design paradigms," in *IEEE Communications Magazine*, vol. 43, July 2005, pp. 78-85.

[2] L. Anderegg and S. Eidenbenz, "Ad hoc-VCG: A truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents," *9th Annual Intl. Conf. on Mobile Computing and Networking (MobiCom 2003)*, San Diego, September 2003.

[3] L. Buttyan and J. P. Hubaux, "Stimulating cooperation in self-organizing ad hoc networks," *ACM Journal on Mobile Networks and Applications(MONET)*, vol. 8, pp. 579-592, October 2003.

[4] J. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring, "Modelling incentives for collaboration in mobile ad hoc networks," *1st Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, INRIA Sophia-Antipolis, France, March 2003.

[5] S. Eidenbenz, G. Resta, and P. Santi, "COMMIT: A sender-centric truthful and energy-efficient routing protocol for ad hoc networks with selfish nodes," *IEEE Intl. Parallel and Distributed Processing Symposium- Workshop 12*, Denver, April 2005.

[6] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad hoc networks," *IEEE INFOCOM*, San Francisco, April 2003.

[7] S. Buchegger and J. Y. L. Boudec, "Performance analysis of the CONFIDANT protocol: cooperation of nodes – fairness in dynamic ad-hoc networks," *3rd ACM Intl. Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2002)*, Lausanne, Switzerland, June 2002.

[8] M. T. Refaei, V. Srivastava, L. A. DaSilva, and M. Eltoweissy, "A reputation-based mechanism for isolating selfish nodes in ad hoc networks," *2nd Annual Intl. Conf. on Mobile and Ubiquitous Systems (MobiQuitous 2005)*, San Diego, July 2005.

[9] R. Axelrod, *The Evolution of Cooperation*, reprint edition ed. New York: Basic Books, 1984.

[10] E. Altman, A. A. Kherani, P. Michiardi, and R. Molva, "Non-cooperative forwarding in ad hoc networks," INRIA, Sophia-Antipolis, France, Report no. 5116, February 2004.

[11] L. A. DaSilva and V. Srivastava, "Node participation in peer-to-peer and ad hoc networks: A game theoretic formulation," *1st Workshop on Games and Emergent Behavior in Distributed Computing Environments*, Birmingham, UK, September 2004.

[12] M. Felegyhazi, L. Buttyan, and J.-P. Hubaux, "Nash equilibria of packet forwarding strategies in wireless ad hoc networks," *to appear in IEEE Transactions on Mobile Computing*, 2005.

[13] M. Felegyhazi, L. Buttyan, and J.-P. Hubaux, "Equilibrium analysis of packet forwarding strategies in wireless ad hoc networks – the dynamic case," *2nd Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, Cambridge, UK, March 2004.

[14] P. Michiardi and R. Molva, "Analysis of coalition formation and cooperation strategies in mobile ad hoc networks," *Journal of Ad Hoc Networks*, vol. 3, pp. 193-219, March 2005.

[15] V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, and R. R. Rao, "Cooperation in wireless ad hoc networks," *IEEE INFOCOM*, San Francisco, March 2003.

[16] A. Urpi, M. Bonuccelli, and S. Giordano, "Modeling cooperation in mobile ad hoc networks: a formal description of selfishness," *1st Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, INRIA Sophia-Antipolis, France, March 2003.

[17] R. B. Myerson, *Game Theory: Analysis of Conflict*, reprint edition ed: Harvard University Press, September 1997.

[18] D. Abreu, D. Pearce, and E. Stacchetti, "Toward a theoy of discounted repeated games with imperfect monitoring," *Econometrica*, vol. 58, pp. 1041-1063, September 1990.

[19] M. Aoyagi and G. R. Frechette, "Collusion in Repeated Games with Imperfect Public Monitoring," UCLA Department of Economics, Report no. 122247000000000127, April 2004.

[20] W. H. Press, B. P. Flannery, S. A. Teukolsky, and W. T. Vetterling, *Numerical Recipes in C: The Art of Scientific Computing*, 2nd edition ed: Cambridge University Press, October 1992.

[21] P. R. Tadikamalla, "Computer generation of gamma random variables," *Communications of the ACM*, vol. 21, pp. 419-422, May 1978.

[22] N. D. Wallace, "Computer generation of gamma random variates with non-integral shape parameters," *Communications of the ACM*, vol. 17, pp. 691-695, December 1974.