HAL
open science

Modelling cooperation in mobile ad hoc networks: a formal description of selfishness

A. Urpi, M. Bonuccelli, Silvia Giordano

To cite this version:

A. Urpi, M. Bonuccelli, Silvia Giordano. Modelling cooperation in mobile ad hoc networks: a formal description of selfishness. WiOpt'03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, Mar 2003, Sophia Antipolis, France. 10 p. inria-00466742

HAL Id: inria-00466742

https://inria.hal.science/inria-00466742

Submitted on 24 Mar 2010

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Modelling cooperation in mobile ad hoc networks: a formal description of selfishness

A. Urpi*, M. Bonuccelli*, S. Giordano†
{urpi,bonucce}@di.unipi.it, silvia.giordano@die.supsi.ch

Abstract - *The advance in wireless technologies makes now viable to start to develop ad hoc networks. However, without a mechanism that prevents misbehaviors, these networks could result easily unreliable. We develop a model, based on game theory, capable of formally explaining characteristics of ad hoc networks (as the nodes' selfishness or the network mobility). It also allows to formally study and analyze strategies for cooperation. As example, we describe a simple strategy that enforces packet forwarding among nodes.*

1 Introduction

A Mobile Ad Hoc Network is a collection of mobile wireless nodes. It has no authority and is dynamic in nature. Energy conservation issue is essential for each node and leads to potential selfish behavior. Nodes can tend to limit their support to other nodes as this costs energy and has no revenue. Thus, despite the fact that technology and networking are here to stay, practical problems certainly arise from being highly uncoordinated. And the nodes move, which introduces uncertainty and complexity into the forwarding process.

The need of mechanisms for stimulate cooperation became evident as ad hoc networks started to be studied for uses different than the military one. However, the general approach followed was proposing a mechanism or a protocol and to study the behavior of the proposed mechanism. Models based on game theory have not been explored much in the ad hoc networks literature. There exist some works ([2, 4, 8, 11]) introducing strategies for cooperation in ad hoc networks that implicitly are based on a game theoretic model. However, these models are nor formal neither general, and they do not derive their strategy from the equilibrium concept. The absence of a general and formal model led to difficulties in comparisons and analytical studies of proposed solutions.

In this paper, we propose an approach to cooperation based on Bayesian games, where the players are the nodes in the network. Consider an ad hoc network where nodes have to periodically choose an action (whether to forward or not to forward) without being fully informed about the traffic in the whole network. Each node is endowed with some information about its neighbors and their actions, which includes its neighborhood, the traffic it sent and has to send, and the traffic it received.

Prior to choosing its next action, a node has an opportunity to analyze the past behavior of its neighbours and its priorities in terms of energy consumption and throughput, and to decide, consequently, how to act. In deciding to whom to forward packets and to whom to discard packets, the node trades-off the costs (energy consumption), the benefits (network throughput) and the collaboration offered to the network by the neighbours. This implicit incentive brings a neighbor to act in a selfish way only when obliged by energy constraints, but each node tends to cooperate with collaborative nodes.

We develop a general model where we include: the Bayesian secret type of each player, that is the classification of nodes in terms of their traffic generation process (energy class); the dynamic process of energy consumption; the payoff of each player, that is the linear combination of the energy spent for some forwarding that goes to success and the throughput expressed in terms of the packets sent over the packets she wanted to send; and the dynamic process of nodes mobility. The generaliza-

*Dipartimento di Informatica, Università di Pisa, Italy
†DIE - SUPSI, Lugano, Switzerland

tion provides a richer model in terms of answering theoretical as well as practical questions. In terms of the networks literature ours is a generic model of ad hoc networks that allows to describe and study new strategies, as well as the protocols and strategies previously published.

Our results establish in a formal way that nodes in ad hoc networks are selfish, and give a theoretical explanation of selfishness. Thus it is formally defined why the dynamic process of communication in ad hoc networks converges to a non-collaborative network with probability one. Furthermore, the energy consumption affects the nodes behavior in a more realistic way: A node evaluates its energy consumption not only in terms of avoiding to forward packets for other nodes, as it is done in other works, but also by reducing the number of its packets sent, whenever there is high probability that the packets will not be forwarded. Finally, we formally proof that, on average, nodes will never forward more packets than they send themselves.

Based on these conclusions, we give the characteristics of the strategies that, enforced by the theoretical aspects solved with our model, exploit the nature of ad hoc networks for enforcing the cooperation among nodes. As an example, we describe a simple strategy that enforces packet forwarding among nodes. The rest of the paper is organized as follows. In Section 2 we discuss the related work. Section 3 introduces the new cooperation model for ad hoc networks. In Section 4 we illustrate the properties of our model, and Section 5 gives an analysis of existing works in terms of our model. Then the characteristics and properties of the enforceable policies that can be derived with our model are presented in Section 6. Finally, we conclude the paper and illustrate the future work (Section 7).

2 Related work

The cooperation enforcement in mobile ad hoc networks is recently receiving great attention, since it is a critical service that must be guaranteed.

In [7], which is the starting point for many other works, Marti et al are not concerned about cooperation itself, but about offered throughput in the network, which is of course affected by selfishness. They do not introduce a formal model to describe their solution, but propose to equip every node with a *watchdog*, a unit that listens to all the communications that arrive to the node, in order to keep under control what is going on in the neighborhood. With these data, selfish nodes can be excluded from routes, making selfishness very advantageous, but not dangerous.

Buchegger and Le Boudec introduce the CONFIDANT protocol in [2]. Again, they do not introduce a formal model, motivating their solution by means of simulation, but it is possible to deduce that they adopt an *evolutionary* approach: they see nodes as an interacting population, and look for a strategy that yields more benefit than any other strategy that a newcomer node can adopt ([5]). Nodes have to be equipped with a watchdog unit, to observe the actions of neighbours, and adapt to their behavior. Moreover, they need to warn themselves about new discovered selfish nodes, with exchanges of alarm messages, in order to cut off misbehaving nodes from all the network services.

The solution proposed in [8, 9] by Michiardi and Molva overcomes some problems related to the alert messages, and introduce the concept of redemption: a misbehaving node can be integrated again in the network if it start cooperating. The reputation of nodes is collected locally, with some indirect deduction about well behaving nodes that can be useful when considering mobility. Authors analyze their solution in game theoretical terms, showing that games can be very useful in such an anarchic setting.

A radically different solution was proposed in [3, 4] by Buttyan and Hubaux. A mobile ad hoc network is modeled as a market, where services are exchanged. A virtual economy, based on a virtual currency called nuglet (or bean), is then introduced, forcing nodes to pay to have their packets forwarded, and to being paid when they forward some data. Selfishness is avoided with a rewarding technique: one node is free to be selfish, but behaving in this way it will soon end its nuglets, and it will not be able to send any packet. Unfortunately, the nuglet manager must be put in a tamper-proof hardware module, since it is not possible to avoid forging or stealing.

In [11], Srinivasan et al. propose a trade-off between the previous solutions, introducing energy as the main concern. They analyze a mechanism based on the TIT FOR TAT strategy (see Sec-

tion 6), that leads to a Pareto efficient point in the network, using game theory as foundation of their analysis. The model however lacks of generality, since authors used many strong assumptions about the nature of communications.

3 A new model

3.1 Definitions and assumptions

We assume that time is discrete and divided in frames $t_1, \ldots, t_n$ (see Section 4 for a discussion on their size, and on the low importance of the synchrony hypothesis, implicitly holding with this assumption). Node i has the following informations at the beginning of frame t_k:

- $N_i(t_k)$, the set of its neighbors[1] during the frame, assumed to be fixed during each frame (see Section 4),
- $B_i(t_k)$, the remaining energy of unit i,
- $\forall j \in N_i(t_k).T_i^j(t_k)$, the traffic node i generated as source, and that it has to send to neighbor j during the frame, in terms of number of packets (j can be the final destination for some of them and just a relay for the remaining),
- $\forall j \in N_i(t_{k-1}).F_j^i(t_{k-1})$, the number of packets, that j forwarded for i during the previous frame (i can be the source for some of the packets, and a relay preceding j in the chain for the others),
- $\forall j \in N_i(t_{k-1}).R_i^j(t_{k-1})$, the number of packets i received as final destination during the previous frame from neighbor j, that could be source for some of them and relay node for the others,
- $\forall j \in N_i(t_{k-1}).\widetilde{R}_i^j(t_{k-1})$ is the number of packets i received from j as final destination, being j the source ($\widetilde{R}_i^j(t_k) \leq R_i^j(t_k)$).

Thinking about a real mobile ad hoc network, it can be difficult to understand how the value of $F_j^i(t_x)$ is known by node i. If in the network communications are symmetric (i.e. $\forall i, j, k.i \in N_j(t_k) \iff j \in N_i(t_k)$), then for example it is possible to use a watchdog unit ([7]), or some higher level mechanisms like end to end acknowledgements. However, it is not the main focus of this paper to explain how to compute all the needed data.

We assume that to send a packet a constant amount of energy c_σ is spent, while receiving has a negligible cost in comparison, since we assume a shared medium where a packet is received anyway from every node in the transmission range of who is transmitting. Nodes are divided in n energy classes $e_1, \ldots, e_n$, each with a specific generation process, without restriction. Associated to every class e_k there is moreover a constant $0 \leq \alpha_{e_k} \leq 1$, defining the importance given to energy by nodes in e_k: if $\alpha_{e_k} = 0$ then energy is not a matter, while at the contrary $\alpha_{e_k} = 1$ implies that energy is a resource tremendously important (see Section 3.2, where the payoff function is defined). The class of node i is indicated by $e(i)$, and it is assumed to be fixed. Finally, we are interested in modeling and understanding selfishness, so malicious behaviors are intentionally not considered. A selfish node does not want to damage any other node, it just wants to save energy while using the network.

3.2 The forwarding game

It is possible to model an ad-hoc network during a single frame by means of a Bayesian game ([10]) in the following way:

- the players are the nodes in the network,
- player i, as action, sets $S_i^j(t_k)$, i.e. the number of packets she[2] will send to every node $j \in N_i(t_k)$ (a fraction of $T_i^j(t_k)$), and $F_i^j(t_k)$, i.e. the number of packets, received from j during previous frame, she will forward for her.
- the secret type of player i is her energy class $e(i)$, that affects her traffic generation distribution,
- her payoff is

$$\alpha_{e(i)} W_i(t_k) + (1 - \alpha_{e(i)}) G_i(t_k) \qquad (1)$$

[1] The neighborhood of a node i is defined, as usual, as the set of nodes that can send packets to i, or from which i can receive, in just one hop.

[2] It is a tradition in game theory to refer to players as female entities.

where $0 \leq \alpha_{e(i)} \leq 1$ is the already introduced class dependent evaluation of energy importance, $W_i(t_k)$ is a measure of the energy spent with success, i.e. the ratio between packets that neighbours forwarded after a request by i, or received as final destination, and sent packets, defined as:

$$W_i(t_k) \triangleq \begin{cases} w(k) & \text{if } S_i(t_{k-1}) + F_i(t_{k-1}) > 0 \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

with

$$w(k) \triangleq \frac{\sum_{j \in N_i(t_k)} (F_j^i(t_k) + \widetilde{R}_j^i(t_k))}{S_i(t_{k-1}) + F_i(t_{k-1})}$$

and $G_i(t_k)$ is the ratio of sent packets over packets that player i wanted to send, defined as:

$$G_i(t_k) \triangleq \begin{cases} g(t_k) & \text{if } \sum_{j \in N_i(t_k)} T_i^j(t_k) > 0 \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

with

$$g(t_k) \triangleq \frac{\sum_{j \in N_i(t_k)} S_i^j(t_k)}{\sum_{j \in N_i(t_k)} T_i^j(t_k)}$$

- player i has a prior belief for every player $j \in N_i(t_k)$, i.e. a distribution on the energy class of j.

It is worth noting that the payoff function is always between 0 and 1, and that sending at least one packet in every frame (if there are packets to send, of course) is always at least as good as not sending anything.
In a few words, every node tries to maximize its payoff function, with the following constraints:

$$c_\sigma(S_i(t_k) + F_i(t_k)) \leq B_i(t_k) \tag{4}$$

$$T_i(t_k) \geq 0, S_i(t_k) \geq 0, F_i(t_k) \geq 0 \tag{5}$$

$$S_i(t_k) \leq T_i(t_k) \tag{6}$$

Constraint 4 means that it can not be spent more energy than the battery can provide and constraints 5 and 6 just better characterize the admissibility space.
A sequence of frames is the infinite repetition of the game, with a discount factor δ depending on the mobility of the network (i.e. the probability to have a neighbor in the transmission range also in following frames): the less a neighborhood is stable, the smaller is δ, since a misbehavior by j in the present frame (i.e. a non cooperative move, as we will see in Section 4) could never be punished if j is moving out of the neighborhood of i in the near future. This approach allows us to model a local knowledge, since the payoff of every player is influenced just by the moves of players modeling neighbor nodes. A discussion on local versus global knowledge strategies is given in Section 6.

3.3 An example

Let us begin with a didactic case: a "mobile" adhoc network with two nodes that mutually need the other node to reach (for example an access point) and that also exchange messages between them (Figure 1). If there is a unique class, then there is not uncertainty about the type of the other node, and the scenario is very simple. In the single shot scenario, Nash equilibria are (of course) dependent on the value of α (and then on the energy class the nodes belong to).
If $\alpha = 0$, nodes do not care about spent energy, and their payoff function is obviously $G_i(t_k)$. For this reason, in all the equilibria of the game, nodes send all the traffic they need to (i.e. $\forall k. S_i(t_k) = T_i(t_k)$, maximizing their payoff) and they forward a number of other node's packets between 0 and the number of packets they were demanded to.
On the contrary, if $\alpha = 1$ nodes are extremely concentrated on power, and their payoff is given by $W_i(t_k)$. There is just one Nash equilibrium in which nodes do not forward any packet, and send just traffic destined to the other node, since both maximize their payoff setting $F_i(t_k)$ to 0.
Finally, if $0 < \alpha < 1$, nodes are sensible to both the goals (which is a more realistic case), then a few equilibria (generally just one) exist, in which $F_i(t_k) = 0$ for both players, and $S_i(t_k)$ is the best tradeoff between wasted energy and throughput needs. It is possible to show that for α small enough, there exist equilibria in which more packets than the ones for the other node are sent.
If there are two different energy classes[3], and $\alpha_{e(1)} \neq 0$ and $\alpha_{e(2)} \neq 0$ (i.e. both units are

[3] As explained in Section 3.1, the energy class a node belongs to is a secret information.

energy constrained), then nothing changes, since for every node the best strategy is not to forward ($F_i^j(t_k) = 0$) and to send a number of packets not much greater than the amount of packets directed to the other node ($S_i^j(t_k) \approx \widetilde{R}_i^j(t_k)$), for α great enough. If $\alpha_e(i) = 0$ for one of the nodes (let us suppose this holds for node 1), then it is possible to prove the following

Proposition 3.1 *If node 1 belongs to class 1 with associated $\alpha_1 = 0$ and node 2 belongs to class 2, with associated $1 \geq \alpha_2 > 0$, then the forwarding game in the single shot has at least $2^{S_2(t_k)}$ equilibria, in which:*

- *node 1 sends all its packets, and forwards any number of node 2's packets between 0 and $S_2(t_k)$ (all the probability assignments to $F_1(t_k)$ have the same payoff, leading to the lower bound on the number of equilibria,*

- *node 2 actions are conditioned by the value of α_2 and by the distribution on the type of node 1.*

The first point follows directly from the definition of the payoff when α_1 is equal to 0: $W_i(t_k)$ does not influence the result, which is maximized when $G_i(t_k) = 1$.
Player 2, on the contrary, can raise her payoff by setting the value of $F_i(t_{k-1})$ to 0 in every frame. After this, if α_2 is near 0, then in all the equilibria she will try to send as much packets as possible, being $G_2(t_k)$ the important part of her satisfaction. When α_2 is closer to 1, the number and the quality of equilibria depends on her prior belief about player 1: if she thinks that the probability of having a class 1 neighbor is high, then there are more "efficient" equilibria, in which player 2 sends more packets than the one destined to player 1, trying to benefit by the power of her neighbor. □

4 Properties of the model

The game theoretical model we presented induces some basic considerations at this point. Selfishness is described and motivated by the a priori lack of thrust among nodes: without any enforcing policy, and in presence of players[4] that care at least a minimum about energy, it is not possible to count on the others' help, and the best strategy (in order to not be used without any advantage for her) is to maximize the personal payoff in a selfish way by being the first that does not help others. This fact, of course, rouses a chain reaction, resulting in every player thinking just to herself, and in a network working just for one hop communications. Note that the situation is dramatically similar to a multi player prisoner's dilemma ([6]). It is of course an extreme case, in which avarice and uncertainty leads to self destruction.

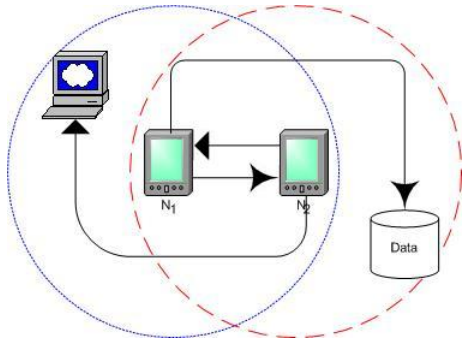

Figure 1: A two nodes ad hoc network.

A first criticism that could be moved to our proposal is the presence of frames, i.e. groups of time slots, that introduce synchrony in a highly decoupled system. In fact we introduced the frame concept just for presentation clearness, but it would be possible to build the same model without them. In fact, in all the proofs we present in this paper, frames are relative to each player, who evaluates what happened using data she collected by herself. Moreover, another possible solution to avoid frames, is to use very short time slots. In every time slot, a node can have to send one packet, and it has to decide whether to send it or not, and whether to forward its neighbours' traffic it eventually received during previous time slot. The more the packet is assumed small on average, the smaller is the time slot duration, leading to a continuous time model to the limit. Frames contain a variable number of time slots, and the duration of frame k can be set to the number of time slots during which communi-

[4] We start here using the terms "node" and "player" interchangeably.

cating nodes (sources, relays and destinations) do not move away from their neighborhood.
Our model is very general. In fact the space of actions, for a single frame, is very loosely limited by simple energetic considerations (energy spent during that frame must not exceed the node energetic capacity), although it would be possible to refine the decision space with many constraints, arriving to a less general solution.
The power of this model is that it allows to design simple mechanisms that enforce cooperation during the network lifetime. We are not claiming that revolutionary solutions come out, since the only possible remedies for a node, at this level, is to watch what its neighbors are doing, and to help them as long as they help it (exactly as in [2, 8, 11]). We claim that it is possible to study optimal behaviors (has a node to be punished forever or not?), while respecting heterogeneity in power capabilities. It is possible to characterize a wide range of enforceable strategies, and it is possible to study in which cases these will succeed without any exception (i.e. the minimum number of nodes in a network employing such a strategy to have a cooperative network). It is also partly possible to analyze already presented solutions, in order to better understand why they work (if they do work), and to show possible enhancements.
Finally, we find very interesting and innovative a feature pointed out by this model: the satisfaction of every node is maximized not only by forwarding less packets for others, but also avoiding to send personal packets if, for some reason, it is believed that neighbors are not going to forward them. This aspect offers a great potentiality at a protocol design level: if it is possible to "introduce" nodes to themselves, i.e. to make them know each other in some way (we are thinking about knowing the energy class every node belongs to), then it is possible to charge every neighbor with a reasonable amount of packets to forward, in order to not overload them, but over all in order to avoid an almost sure packet loss. This fact was evident from the example in Section 3.3: in presence of two energy classes, the equilibria are more efficient when the prior belief of the low powered player is nearer to the real situation. However, this is very difficult because of the mobility, that makes very difficult to really know other nodes, often encountered in rapid and momentary encounters, and because of selfishness, that pushes nodes towards wariness, since other nodes can be pretending to be weaker than they are in the reality to save energy.
It is possible to prove the following

Theorem 4.1 *During a single frame t_k, if $\forall i \in \{1, \ldots, n\}.\alpha_i \neq 0$, in all the Nash equilibria exhibited by the system, $\forall j \in \{1, \ldots, m\}, \forall k.F_i(t_k) = 0$.*

It follows from the payoff definition: since $W_i(t_k)$ affects the payoff for all the players, everyone gets more satisfaction by setting $F_i(t_k)$ to 0. □
In other words: selfishness is the only strategy that can naturally arise in a single frame communication!
It is, however, possible to overcome this effect when introducing repetition, as we will see in Section 6.

5 Analysis of mechanisms

It is possible to capture some of the strategies presented in Section 2 with the model we just presented, in order to show its generality and power.
In the NUGLETS proposal ([3, 4]) a model very similar to our is used, in which selfishness is formally explained with a double goal to optimize for every node (throughput versus lifetime), but having as a constraint in every node that the number of sent packets can not be greater that the number of forwarded packets plus a system dependent constant amount. This should be a strategy (to be enforced, since it is not a sequence of equilibria, as it is easy to show), and not a personal diktat (clearly, a node would prefer to send much more packets than forwarded ones). An interesting point of this proposal is the locality of informations needed by every node: the absence of a watchdog (or similar) mechanism is surely a good feature, since the assumption of bidirectional communications, needed by such a mechanism, is not realistic and widely criticized. However, from another point of view it causes the necessity to embed the desired forwarding strategy, a sort of "consume the same amount of resources you produce", in a tamper-proof hardware module, which can be an obstacle for its application. The same strategy, under the assumptions we made in this paper, can be enforced (See Section 6 for details) under our model, leaving absolute freedom to

nodes on how to accumulate credits and to spend them[5]. The NUGLETS solution can be seen as a special case of the model we are presenting, with a single energy class ($n = 1$) and equal evaluation of energy and throughput ($\alpha = \frac{1}{2}$).

The reputation concept present in CORE and CONFIDANT ([8, 2]) can be easily mapped in our model.

In the CONFIDANT protocol a node is good (and then in the network) or bad (and then isolated), without mid tones[6]. It is equivalent to the following strategy: cooperate with a node until it cooperates, and when it stops, punish it forever blocking its communications. The strategy is too strict: an everlasting punishment surely discourages selfishness, but also reduces the network performances, and does not admit temporary failures, due for example to congestion or energy problems. Moreover, while in the model presented in this paper (see Section 3.2) nodes have access to informations just about neighbors, in [2] a global knowledge is needed, and when a selfish node is discovered, good nodes arranged in a friendship network, start warning themselves with alarm messages, adding overhead (claimed by authors to be low), and enabling malicious nodes to spread false informations about well behaving nodes.

From a theoretical point of view, the proposed solution is not evolutionary stable ([1]): if nodes are seen as a population of randomly interacting players, than TIT FOR TAT and variants are an optimal behavior, in the sense that, on average, players adopting it score better payoffs, and ensure themselves a high survival probability, while deviating players do not survive (and for this reason do not have the opportunity to transmit their genes to following generations). The strict strategy at the base of the CONFIDANT protocol lacks of reactiveness, which is a necessary condition for a strategy to be evolutionary stable (see [1]).

We think the model at the base of the CORE solution is richer, and the proposed mechanism is theoretically more solid. In fact, a strategy of temporary punishment is analyzed: the reputation every node keeps of its neighbors is an elegant way to model uncertainty in understanding whether a node misbehaved or not. A single deviation observed is not taken as a sure fact, but lowers the reputation of the presumed guilty. After a number of consecutive inexplicable actions[7], reputation falls under a critical level, and it can be assumed that, with high probability, that node is selfish (or even malicious, in some cases) and can be punished. However, if that node starts behaving well, after a certain time it will have a good enough reputation, and it will be able to work in the network. In both cases, we have again a single energy class (then $n = 1$) and $\alpha = 0$, i.e. high evaluation of throughput (selfishness is taken as an obvious fact, but not formally described), but a different strategy is enforced.

Finally, it is also possible to give a loose mapping of the GTFT mechanism ([11]). The concept of session present in that proposal (see Section 2 for a reminder) can be simulated imposing that frame duration is equivalent to session duration, and that in each frame just one session is served. This is less general than our model (in fact we allow more sessions to be active during every frame). The next step is to limit the action space of forwarder nodes to {yes,no}, i.e. to accept all the packets that it will receive or to reject them. It is not important, at the model level, if a session in which some forwarder is not going to help is always stopped (as in [11]) or is always started (as in this paper)[8]. The authors studied the problem with n energy classes, and with $\alpha = 0$, but considering energy constraints, transformed in constraints on the power expense rate for every energy class. Again, we are loosing some generality, since we assumed that nodes in the same energy class can have different battery capacities. Authors compute the maximum ratio of sessions to be accepted, in order to have a system working at a Pareto efficient point, and they give a mechanism that enforces that strategy (but they need to know in advance the rate to be enforced). They prove the correctness of their solution by means of game theory, as it is possible with our model.

[5] In fact it is not necessary to introduce the virtual currency nor the counters, which are the core of [3, 4].

[6] Authors claim that it is possible to have multiple levels of reputation, and re-integration of nodes that start behaving well, but in the paper this is not analyzed.

[7] Relying on a watchdog mechanism it is not possible to assert that a missing observation of a forward implies that some messages were not effectively forwarded.

[8] It is a vital question in real cases, of course, since it avoids not needed energy wasting.

6 Enforceable policies

As pointed out in Section 3.2, communications in an ad hoc network can be modeled as an infinitely repeated game. This kind of models can describe situations in which the number of rounds is finite (as it happens in a mobile ad hoc network, where nodes arrive, leave and move away changing neighborhood), but there is not the knowledge on when the game is going to stop. Every node can not be sure that it is going to play the next round with different opponents, since every node is moving.
There are basically two methods to enforce a desirable strategy in a repeated game: punishing deviators, or encouraging who is adopting it, making deviations not interesting to profit maximizer players. We believe that in the case of mobile ad hoc networks it is better to consider punishment based techniques for two reasons:

- rewarding strategies are not easily extensible to scenarios in which malicious entities play. These players are not, in fact, interested in rewards, while they are sensitive to punishments (if they are excluded from network usage, they can not damage other nodes,
- since a unique commodity is exchanged at this level, i.e. forwarding of traffic, the boundary between a punishment and a reward is extremely vague: we are not able to think about a reward that is not a non-punishment, or a punishment which is a not a non-rewarding.

Since we chose the road of punishment for deviations, we can start investigating what is the set of strategies that can be enforced with the solid background of Nash folk theorems ([10], Chapter 8). These theorems offer us a precise way to escape from the only theoretical equilibrium point, which is the non cooperation, as we shown in Section 4[9].
Two first results can be considered negative. Recalling that the discount factor δ can be assumed equal to the probability of having again a node in the neighborhood after a frame (it is a measure of mobility), it is possible to prove the following

Theorem 6.1 *It is possible to enforce a strategy different from non cooperation only for δ close enough to* 1*, or for nodes exchanging a huge amount of packets.*

A deviation during frame t_k advantages player i in the following frame, resulting in a payoff increment of:

$$\frac{F_i(t_k)\left[\sum_{j\in N_i(t_{k+1})}(F_j(t_{k+1})+\widetilde{R}_j(t_{k+1}))\right]}{S_i(t_k)[S_i(t_k)+F_i(t_k)]}$$

In order to be effectively punished, her neighbors can stop traffic from i for L frames, resulting in a loss of payoff for her of:

$$\sum_{l=2}^{L}\delta_{l-1}(u_i(t_{k+l})-u'_i(t_{k+l}))$$

where $u'_i(t_{k+l})$ is the payoff as defined in 1, with $\sum_{j\in N_i(t_{k+l})}F^i_j(t_{k+l})=0$, and $u_i(t_{k+l})$ is the payoff without punishment.
For the punishment to be an effective deterrent, the loss of payoff caused by punishment must be greater than the gain following from a deviation, and it is not hard to note that it can happen just if:

- δ is near to 1, because otherwise the punishment decays too fast,
- $S_i(t_{k+l})$ is very high, making the interruption of packet forwarding extremely costly for i.

□

This theorem formally reflect an obvious fact: if we want mechanisms based only on local information, then it is possible to enforce cooperation only if nodes do not move too much, situation modeled by a high value of δ (see Section 3.2). Informally, this holds because the only way to enforce a behavior which is not a Nash equilibrium of the single shot game is to punish deviating nodes blocking their communications for enough frames, in order to make loss derived from punishment higher than gain obtained by non cooperation. If with high probability a node will not have enough time to punish a misbehaving neighbor, then it is not possible to enforce anything. This is the price paid for local knowledge: if it was possible to spread information about misbehaving nodes, then a moving node would be punished by all the neighbors it encounters, making punishment an

[9] We are not interested in cases of networks mainly composed by nodes not energy constrained.

effective deterrent.
However, if from one side it is possible to study the set of enforceable policies in a not too mobile ad-hoc network (in case of small network, it is not a restrictive hypothesis), from the other side it is interesting to see how evolutionary theory comes in our help.

Lemma 6.2 *It is not possible to force a node to forward more packets than it sends on average.*

From Nash folk theorems applied to δ-discounted repeated games, we know that an action, in order to be imposed on the players, must be enforceable, i.e. at least as good for her than all the other actions. In our case, cooperation is an enforceable action, only if the amount of traffic others forward for a node is at least equal to the amount of traffic it forwards for others, on average, as it follows from the payoff definition in 1 (Section 3.2.) □
Here goes the theory. Unfortunately, in a real world scenario this could be not enough, since the best strategy could be to cooperate until the neighborhood of a node is stable, and start being selfish when it start changing neighbors frequently. For this reason, it is better to use tools borrowed from evolutionary game theory. In [1] it is shown how cooperation can arise in populations of randomly interacting players. The setting is the following: let us suppose that randomly picked nodes start playing the game we introduced in Section 3.2 for a limited number of rounds (eventually knowing an upper bound on the number of plays). After then, another random matching is produced, and so on. The theory tells that even in such an anarchic and chaotic setting, there exist strategies that are stable, and that on average permit the survival of players adopting them. As an example, in [1] it is presented the TIT FOR TAT strategies in a prisoner's dilemma game played in tournaments. In such a strategy, a players start not confessing (and then cooperating with her opponent), and then in every following round she repeats the move her opponent played in the previous round. It is shown that this is a winning strategy, in the sense that almost always the players adopting it win the tournament, and always they arrive in the very first places, no matter how complex are the other players' strategies. It is shown that this result holds because TIT FOR TAT is:

- gentle, i.e. start with cooperation. In fact, players that start with non cooperation are penalized more easily by others, resulting in aggregate results very poor (note that the always confessing strategy wins over TIT FOR TAT in a match, but in the tournament performs very bad),
- reactive, i.e. it changes with the environment, and very fast. A hostile move from an opponent must be punished very quickly, in order to avoid to be exploited for too much kindness, but a return to cooperation must be awarded with reciprocity, in order to benefit from the remainder of the game,
- not envious, i.e. it do not try to destroy the opponent, it just tries to gain the maximum with the most rewarding, even if dangerous, move.

It is then possible to prove the following

Theorem 6.3 *Cooperation can be enforced in a mobile ad hoc network, provided that enough members of the network agree on it, and if no node has to forward more traffic that it generates.*

The second hypothesis is motivated by Lemma 6.2. The first one follows from the observation that, in a population, a new strategy can invade an old one just if in the long run it holds a better payoff to players adopting it. In fact, if in a network just a very few nodes agree on cooperation, and are spatially sparse, while all the others are selfish nodes, cooperating nodes will meet with low probability, and they will not have the opportunity to raise their payoff with mutual cooperation. Instead, they will pass the time fighting against selfish nodes, and losing. □
As an example, we return to the two nodes, two energy classes case shown in Section 3.3, showing how it is possible to enforce the maximum possible cooperation in this scenario. An optimal strategy for player i is the following (the other player is always indicated as j, and some index has been omitted because useless):

Do ut des: During frame t_0, send all the data you produced, and receive all packets j sent. During following frames, send a number of packets that j should be able to forward ($S_i(t_k) \leftarrow$

$\max(F_j(t_{k-1}), \sum_{l<k}(S_j(t_l) - F_j(t_l)))$, and if you are not punishing j, forward for him as many packets as you can ($\min(R_i(t_k), \sum_{l<k}(S_i(t_l) - F_i(t_l)))$. Moreover, record how many packets j forwards. If the difference between sent packets (from frame 0 up to now) and forwarded packets (same temporal extension) is more than a constant c, then punish j, not forwarding for him packets, until it starts cooperating.

This very simple technique leads to cooperation, and is safe against selfish nodes. It is possible to show that, if node i uses it, node j can not obtain more service than it gives (plus a constant), no matter what strategy it uses (it is a Nash equilibrium). This strategy is obviously unfair.

7 Conclusions

We presented a model to describe interaction between nodes in mobile ad hoc networks, with particular attention to the forwarding of packets. Our model is general enough to describe cooperation enforcement mechanism that have been proposed in literature in recent times, and it can be used to understand at what extent a node can be selfish, and how much can we pretend from it.
The model showed to be robust and very powerful for understanding aspects of ad hoc networks that were assumed as true untill now. However, there are several aspects that we want to further consider and investigate. Among them:

- how strict and realistic are our assumptions and how it is possible to obtain the necessary information, even in an approximated way
- to realise and implement a fair strategy
- how to introduce the mobility of the network by means of evolutionary processes
- how to accept less strict constraints to accept less drastic strategies (as in [8, 9]).

References

[1] R. Axelrod. *The evolution of cooperation.* Basic Books, New York, 1984.

[2] Sonja Buchegger and Jean-Yves Le Boudec. Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes — Fairness In Distributed Ad-hoc NeTworks. In *Proceedings of IEEE/ACM MobiHOC*, 2002.

[3] L. Buttyan and J. P. Hubaux. Enforcing service availability in mobile ad-hoc wans. In *Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC)*, Boston, MA, USA, August 2000.

[4] L. Buttyan and J. P. Hubaux. Stimulating cooperation in self-organizing mobile ad hoc networks. *ACM Journal for mobile networks (MONET), special issue on Mobile Ad Hoc Networking*, 2002.

[5] R. Dawkins. *The selfish gene.* Oxford University Press, 1976.

[6] R. D. Luce and H. Raiffa. *Games and Decisions.* John Willey & Sons Inc., 1957.

[7] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the sixth annual international conference on Mobile computing and networking*, pages 255–265. ACM Press, 2000.

[8] Pietro Michiardi and Refik Molva. Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Proc. of the sixth IFIP conference on security communications, and multimedia (CMS 2002)*, 2002.

[9] Pietro Michiardi and Refik Molva. Game theoretic analysis of security in mobile ad hoc networks. Technical Report RR-02-070, Institut Eurecom, April 2002.

[10] M.J. Osborne and A. Rubinstein. *A Course in Game Theory.* The MIT Press, Cambridge, MA, 1994.

[11] Vikram Srinivasan, Pavan Nuggehalli, Carla-Fabiana Chiasserini, and Ramesh R. Rao. Cooperation in wireless ad hoc networks. In *Proceedings of IEEE Infocom 2003.*