A Game Theoretical Approach to Evaluate Cooperation Enforcement Mechanisms in Mobile Ad hoc Networks

Pietro Michiardi and Refik Molva
Institut Eurecom
2229 Route des Cretes
06904 Sophia-Antipolis, France

Introduction

An *ad hoc* network is a collection of wireless mobile hosts forming a temporary network without the aid of any established infrastructure or centralized administration. In such an environment, it may be necessary for one mobile host to enlist the aid of other hosts in forwarding a packet to its destination, due to the limited range of each mobile host's wireless transmissions. Indeed, as opposed to networks using dedicated nodes to support basic networking functions like packet forwarding and routing, in ad hoc networks these functions are carried out by all available nodes in the network.

However, there is no good reason to assume that the nodes in the network will eventually cooperate, since network operation consumes energy, a particularly scarce resource in a battery powered environment like MANET. The lack of cooperation between the nodes of a network is a new problem that is specific to the ad hoc environment and goes under the name of *node selfishness*. A selfish node does not directly intend to damage other nodes by causing network partitioning or by disrupting routing information (mainly because performing these kind of attacks can be very expensive in terms of energy consumption) but it simply does not cooperate to the basic network functioning, saving battery life for its own communications. Damages provoked by a selfish behavior can not be underestimated: a simulation study available in the literature [8] shows the impact of a selfish behavior in terms of global network throughput and global communication delay when the DSR [7] protocol is used. The simulation results show that even a little percentage of selfish nodes leads to a severe degradation of the network performances.

Several mechanisms that detect and prevent a selfish behavior are available in the literature [10, 11, 12, 13, 14]: we take as a reference the CORE [9] mechanism. In CORE, node cooperation is stimulated by a collaborative monitoring technique and a reputation mechanism. Each node of the network monitors the behavior of its neighbors with respect to a requested function and collects observations about the execution of that function. If the observed result and the expected result coincide, the observation will take a positive value, otherwise it will take a negative value. Based on the collected observations, each node computes a reputation value for every neighbor. The formula used to evaluate the reputation value avoids false detections (caused for example by link breaks) by using an aging factor that gives more relevance to past observations: frequent variations on a node behavior are filtered out. Furthermore, if the function that is being monitored provides an acknowledgement message (e.g., the Route Reply message of the DSR protocol), reputation information can also be gathered about nodes that are not within the radio range of the monitoring node. In this case, only positive ratings are assigned to the nodes that participated to the execution of the function in its totality. The CORE mechanism resists to attacks performed using the security mechanism itself: no negative ratings are spread between the nodes, so that it is impossible for a node to maliciously decrease another node's reputation. The reputation mechanism allows the nodes of the MANET to gradually isolate selfish nodes: when the reputation assigned to a neighboring node decreases below a pre-defined threshold, service provision to the misbehaving node will be interrupted. Misbehaving nodes can, however, be re-integrated in the network if they increase their reputation by participating to the network operation.

An original approach to formally assess the security features of a cooperation enforcement mechanism such as CORE is based on an economic model. In this model, service provision (e.g. the execution of the packet forwarding function) preferences for each node are represented by a utility function. As the name implies, the utility function quantifies the level of satisfaction a node gets from using the network resources. Game-theoretic methods are applied to study cooperation under this new model. Game theory is a powerful tool for modeling interactions between self-interested users and predicting their choice of strategy. Each player in the game maximizes some function of utility in a distributed fashion. The games settle at a Nash equilibrium if one exists, but, since nodes act selfishly, the equilibrium point is not necessarily the best operating point from a social point of view.

In this paper we propose two methods to evaluate the effectiveness of the CORE mechanism based on a cooperative game approach and a non-cooperative game approach: the results obtained using the first approach define a lower bound on the number of legitimate nodes in an ad hoc network when the CORE mechanism is adopted while the second approach describe the asymptotical behavior of a selfish node that is controlled by CORE.

Cooperative games approach

Our first analysis relies on a preference structure in which players, along with their own absolute payoff, are motivated (non-monotonously) by the relative payoff share they receive, i.e. how their standing compares to that of others. With this, we rely on the ERC model by [4] but use a full information framework.

Let the (non-negative) payoff to node *i* be denoted by y_i , *i*, . . . , *N*, and the relative share by $\sigma_i = \frac{y_i}{\sum_j y_j}$. The utility function is given by: $\alpha_i u(y_i) + \beta_i r(\sigma_i)$ where $\alpha_i, \beta_i \geq 0$ and *u()* is differentiable, strictly increasing and concave, and r*()* is differentiable, concave and has its maximum in $\sigma_i = \frac{1}{N}$. Throughout this paper we assume that nodes' disutility from disadvantageous inequality is larger if the node is better off than average, i.e. $r(\frac{1}{N} - x) \leq r(\frac{1}{N} + x), \forall x \in \left[0, \frac{1}{N}\right]$.

In this section we study a simple symmetric *N*-node prisoner's dilemma where each mobile node can cooperate, 'c', or defect, 'd'. In terms of the node misbehavior problem: the node either correctly executes the network functions or it doesn't. Let the total number of cooperating nodes be denoted by *k*. For any given *k*, the payoff to a node is given by *B*(*k*) if the node defects (tries to free-ride). If a node plays cooperatively, it must bear some additional costs *C*(*k*). Its payoff is therefore given by *B*(*k*) - *C*(*k*). We assume decreasing marginal benefits for a node if the number of mobile nodes rises, i.e. *B*(*k*) is increasing and concave. Furthermore, the total cost of cooperation, *kC*(*k*), increases in *k*.

In order to generate the standard incentive structure of a PD game, we assume that

B(*k*+1) - *B*(*k*) < *C*(*k*+1), i.e. playing cooperatively reduces the absolute payoff, given an arbitrary number of 'c'-nodes. To make cooperation more attractive from both the social and the individual point of view, we make the following assumptions:

(1) $N \cdot B(k+1) - (k+1)C(k+1) \geq N \cdot B(k) - kC(k)$ "Socially desirable"

(2) $B(k+1) - C(k+1) \geq B(k) - C(k)$ "Individually desirable"

Furthermore, we assume that payoffs for both cooperating and defecting nodes are non-negative for all *k*.

The reputation measure introduced in [9] is compliant with the incentive structure given by (1) and (2). Cooperation is made attractive from an individual point of view because the cost of participating to the network operation is compensated with a higher reputation value, which is the pre-requisite for a node to establish a communication with other nodes in the network. On the other side, the more nodes have a reputation value that allows them to communicate, the more the cost for participating to the network operation is compensated by a more connected network that increases the nodes' benefits for cooperating.

Next, the Nash equilibria in the one shot PD game under the particular assumption that nodes choose simultaneously is analyzed. Assume that *k* nodes, aside from node *i*, play cooperatively. Then node *i* choose to play 'c' if and only if:

(3) $$\alpha_i u\left[B(k+1) - C(k+1)\right] + \beta_i r\left[\frac{B(k+1) - C(k+1)}{N \cdot B(k+1) - (k+1)C(k+1)}\right] \geq \alpha_i u\left[B(k)\right] + \beta_i r\left[\frac{B(k)}{N \cdot B(k) - kC(k)}\right]$$

This is equivalent to node *i* playing 'c' if:

(4) $$\frac{\alpha_i}{\beta_i} \leq \delta(k) \text{ where } \delta(k) = \frac{r\left[\frac{B(k+1) - C(k+1)}{N \cdot B(k+1) - (k+1)C(k+1)}\right] - r\left[\frac{B(k)}{N \cdot B(k) - kC(k)}\right]}{u\left[B(k)\right] - u\left[B(k+1) - C(k+1)\right]}$$

In order to find feasible coalition sizes, we must therefore study conditions in which $\delta(k)$ is positive. The details concerning the determination of the equilibrium point can be found in [15]. The validity of assumption (1) and (2) made on the payoff structure implies that the condition $\delta(k) > 0$ is necessary and sufficient to state that, for any given vector of types, if a node plays 'c' at the equilibrium, then, in total, at least half of the nodes cooperate.

Non-cooperative games approach

In a second approach, our analysis focused on the identification of preference relations specific to the selfishness problem and the design of a utility function that satisfies this structure. The utility function used to model the selfishness problem takes into account the energy that a node spends for the purpose of its own communications and the energy that the node has to use when participating in the routing protocol and when relaying data packets on behalf of other nodes. Node behavior is represented as the percentage of energy a node dedicates for its own communications and the percentage of energy spent for network operation. Under these assumptions the utility function used to study the strategy chosen by a node is the following:

(5) $$u_{ni}(bi, bj) = E_{self} \cdot (1 - b_i) - b_i \cdot f \cdot (E_R + E_{PF})$$

where b_i corresponds to the strategy (behavior) adopted by node n_i, and b_j is a given strategy selected by all the other nodes in the network: b_i is the variable of equation (5). The term *b* identifies the percentage of energy consumed by a node and ranges from 0 to 1: when a node selects *b* equals to zero it will use all the available energy for its own communications. The other factors that appear in (5) are respectively:

$E_{self} = n \cdot (E_{send} + E_{recv}) = n \cdot (k+1) E_{recv}$, energy spent for own communications

$E_R = (1 - b_j) \frac{n \cdot t}{m} (E_{send} + E_{recv})$, energy spent for participating to the routing protocol

$E_{PF} = (1 - b_j) \cdot t \cdot n \cdot (E_{send} + E_{recv})$, energy spent to relay packets for neighboring nodes

$E_{send} = k \cdot E_{recv}$, respectively the energy spent for sending and receiving one packet
n, the number of packets to send
t, the number of neighboring nodes of node n_i
m, the average number of messages after which a new route discovery phase is needed
f, is a multiplicative factor that models the non-linearity of the second summand of (5)

A “rational” selfish node always tries to maximize equation (5): the maximum determines the strategy b_i chosen by that node, which is always to defect, by selecting the total amount of energy dedicated to other nodes close to zero. Since nodes act selfishly, the equilibrium point is not necessarily the best operating point from a social point of view and pricing emerges as an effective tool to enforce the cooperation among the nodes because of its ability to guide node behavior toward a more efficient operating point. The pricing factor that has been chosen to settle the game at a more socially desirable operating point is the reputation value calculated within the execution of the CORE mechanism. The utility function presented in (5) is modified as follows:

$$(6) \quad u_{ni}(bi, bj) = E_{self} \cdot (1 - b_i) - b_i \cdot f \cdot (E_R + E_{PF}) \cdot r_{ni}$$

where the term r_{ni} corresponds to the normalized reputation value assigned to node n_i and dynamically evaluated by its t neighbors depending on the past strategy adopted by node n_i. The use of a pricing factor modify the position of the maximum of equation (6) with respect to equation (5) evaluated in the same circumstances. By dynamically modifying the position of the maximum, it is possible to impose a selfish node to change its strategy to a fair behavior, as it is possible to see in Figure 1.

The first graph shows the reputation evaluated by the t neighboring nodes of node n_i: the reputation value depends on the behavior of node n_i in the past observations. The second graph depicts the strategy chosen by the selfish node versus time: in a first moment, the node selfishness is still not compensated by the reputation mechanism and the strategy chosen by the node falls to zero (i.e. a pure selfish behavior). However, as soon as the node behavior is detected to be selfish the node reputation starts to fall: a “rational” selfish node will then chose a new strategy that issues from the maximization of equation (6) and that tries to compensate the loss in the reputation factor.

The strategy selection phase stabilizes asymptotically to a fair position where half of the nodes’ energy is used to cooperate with other nodes in the network operation.

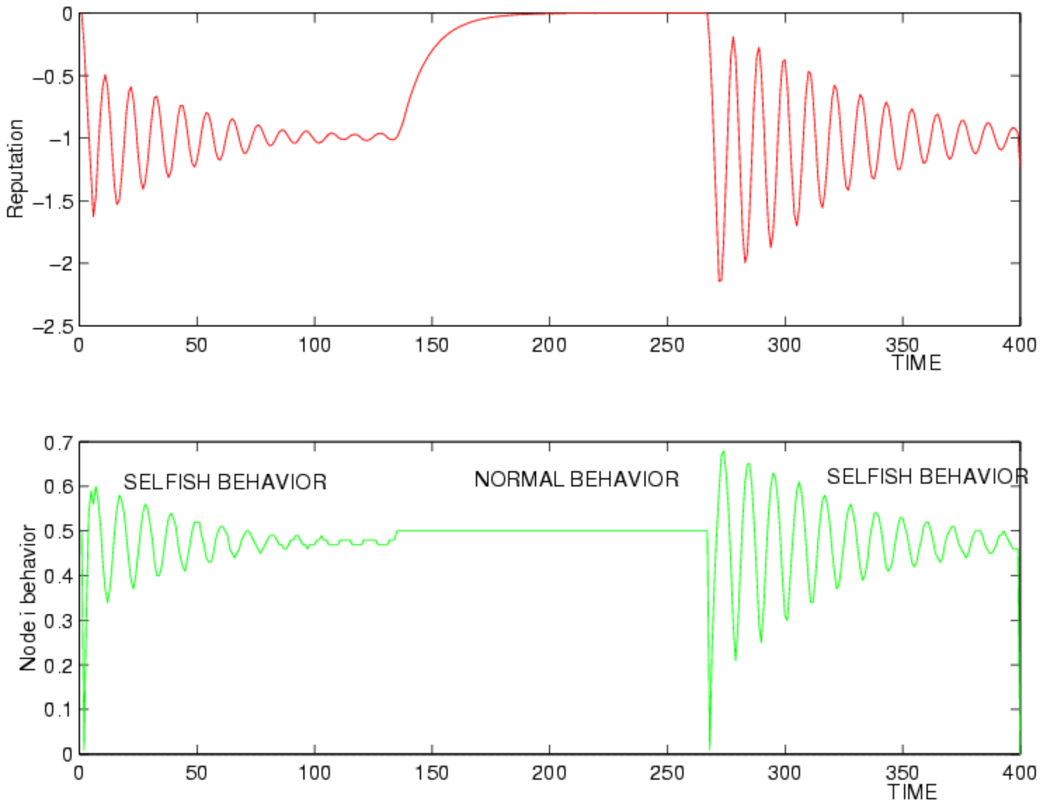

Figure 1. Node behavior when CORE is adopted in the network.

Conclusions

This paper introduces a new approach to investigate on the characteristics of cooperation enforcement mechanisms designed for mobile ad hoc networks. We have shown that the ad hoc paradigm can be modeled using different approaches that have been developed for game theory. When applied to the CORE mechanism, the two approaches presented in this paper allowed us on one side to define a lower bound to the number of cooperating nodes in a network that use CORE and, on the other side, to validate that the reputation technique presented in [9] is a valid tool to obtain an asymptotically fair behavior of the nodes of a MANET that uses CORE as a mechanism to stimulate cooperation.

References

[1] G. Zacharia. Collaborative Reputation Mechanisms for online communities. Master's thesis, MIT, September 1999.
[2] M. J. Osborne, A. Rubinstein, *A course in game theory*, MIT press 1997
[3] R.J. Aumann, J.H. Dreze, *Cooperative games with coalition structure,* International Journal of Game Theory, (1974) 217-237
[4] G. E.Bolton, A. Ockenfels, *ERC: a theory of equity, reciprocity, and competition*. The American Economic Review 2000, 90 166–193.
[5] A. Lange, C. Vogt, *Cooperation in international environmental negotiations due to a preference for equity*, Journal of Public Economics 2002
[6] L.S. Shapley, *Utility comparisons and the theory of games*, Guilbau T (ed.) La decision. Editions du CNRS, Paris, pp. 251-263. Reprinted in: A. Roth (ed.) 1988 The Sahpley Value, Cambridge University Press, Cambridge, pp. 307-319
[7] David B. Johnson, David A. Maltz, *Dynamic Source Routing in Ad Hoc Wireless Networks,* Mobile Computing, edited by Tomasz Imielinski and Hank Korth, Chapter 5, pages 153-181, Kluwer Academic Publishers, 1996.
[8] P. Michiardi, R. Molva. *Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks*. European Wireless Conference, 2002.
[9] P. Michiardi, R. Molva, Core*: A COllaborative REputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks*, IFIP - Communication and Multimedia Security Conference 2002
[10] S. Marti, T. Giuli, K. Lai, and M. Baker. *Mitigating routing misbehavior in mobile ad hoc networks*. In Proceedings of MOBICOM, 2000.
[11] L. Buttyan and J.-P. Hubaux. *Nuglets: a virtual currency to stimulate cooperation in self-organized ad hoc networks*. Technical Report DSC/2001/001, Swiss Federal Institute of Technology -- Lausanne, 2001.
[12] S. Buchegger, J.-Y. Le Boudec, *Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks*, In Proceedings of the 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing, Canary Islands, Spain, January 2002.
[13] S. Buchegger, J.-Y. Le Boudec, *Performance Analysis of the CONFIDANT Protocol,* in proceedings of MobiHoc 2002.
[14] H. Yang, X. Meng, S. Lu, *Self-Organized Network-Layer Security in Mobile Ad Hoc Networks*.
[15] P. Michiardi, R. Molva, *Game theoretic analysis of security in mobile ad hoc networks*, Research Report RR-02-070, Institut Eurecom