Institut Eurécom
2229 Route des Crêtes - BP 193
06904 Sophia-Antipolis, France

Research Report N° RR-02-070

Game theoretic analysis of security in mobile ad hoc networks

Pietro Michiardi – Refik Molva
April 2002

Phone:	e-Mail:
+33.4.93.00.26.45	Piero.Michiardi@eurecom.fr
+33.4.93.00.26.12	Refik.Molva@eurecom.fr

Abstract. *Countermeasures against node misbehavior and selfishness are mandatory requirements in mobile ad hoc networks. Selfishness that causes lack of node activity cannot be solved by classical security means that aim at verifying the correctness and integrity of an operation. In this paper we outline an original security mechanism (CORE) based on reputation that is used to enforce cooperation among the nodes of a MANET. We then investigate on its robustness using an original approach: we use game theory to model the interactions between the nodes of the ad hoc network and we focus on the strategy that a node can adopt during the network operation. As a first result, we obtained the guidelines that should be adopted when designing a cooperative security mechanism that enforces mobile nodes cooperation. Furthermore, we were able to show that when no countermeasures are taken against misbehaving nodes, network operation can be heavily jeopardized. We then showed that the CORE mechanism is compliant with guidelines provided by the game theoretic model and that, under certain conditions, it assures the cooperation of at least half of the nodes of a MANET.*

Keywords. Security, Denial of Service Attacks, Simulation, Game Theory.

Table of Contents.

1. 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. Mobile ad hoc networks (MANET) do not rely on any fixed infrastructure but communicate in a self-organized way.

Security in MANET is an essential component for basic network functions like packet forwarding and routing: network operation can be easily jeopardized if countermeasures are not embedded into basic network functions at the early stages of their design. Unlike networks using dedicated nodes to support basic functions like packet forwarding, routing, and network management, in ad hoc networks those functions are carried out by all available nodes. This very difference is at the core of the security problems that are specific to ad hoc networks. As opposed to dedicated nodes of a classical network, the nodes of an ad hoc network cannot be trusted for the correct execution of critical network functions.

If *a priori trust relationship* exists between the nodes of an ad hoc network, entity authentication can be sufficient to assure the correct execution of critical network functions. A priori trust can only exist in a few special scenarios like military networks and requires tamper-proof hardware for the implementation of critical functions. Entity authentication in a large network on the other hand raises key management requirements.

If tamper-proof hardware and strong authentication infrastructure are not available any node of an ad hoc network can endanger the reliability of basic functions like routing. No classical security mechanism can help counter a misbehaving node in this context. The correct operation of the network requires not only the correct execution of critical network functions by each participating node but it also requires that each node performs a fair share of the functions. The latter requirement seems to be a strong limitation for wireless mobile nodes whereby power saving is a major concern.

With *lack of a priori trust*, cooperative security schemes seem to offer the only reasonable solution. In a cooperative security scheme, node misbehavior can be detected through the collaboration between a number of nodes assuming that a majority of nodes do not misbehave. The threats considered in such a scenario are not limited to maliciousness and a new type of misbehavior called selfishness should also be taken into account to prevent nodes that simply do not cooperate.

We outline in this paper an original mechanism called CORE to enforce node cooperation based on a collaborative monitoring technique. CORE is suggested as a generic mechanism that can be integrated with any network function like packet forwarding, route discovery, network management, and location management. Each network entity in CORE keeps track of other entities' collaboration using a technique called reputation. The reputation metric is computed based on data monitored by the local entity and some information provided by other nodes involved in each operation.

The proposed cooperative security mechanism is then analyzed from a game theoretical point of view in order to come up with a formal assessment of the algorithm.

The remainder of the paper is organized as follows: section 2 illustrates the security scheme used to enforce node cooperation in a MANET focusing on the security objectives addressed by the mechanism and pointing out its properties. The game theoretical approach is detailed in section 3.

2. CORE: the collaborative security mechanism

2.1 Assumptions and background

This section outlines the assumptions that were made regarding the properties of the physical and network layer of the MANET and includes a brief description of the Dynamic Source Routing (DSR), the routing protocol that has been used in our research.

Throughout this paper we assume bi-directional communication symmetry on every link between the nodes. This means that if a node B is capable of receiving a message from a node A at time t, then node A could instead have received a message from node B at time t.

DSR is an on-demand, source routing protocol [23]. Every packet has a route path consisting of the addresses of nodes that have agreed to participate in the routing of the packet. The protocol is referred to as "on-demand" because route paths are discovered at the time a source sends a packet to a destination for which the source has no path. The DSR routing process includes two phases: the Route Discovery phase and the Route Maintenance phase. When a source node (S) wishes to communicate with a destination node (D) but does not know any path to D, it invokes the Route Discovery function. S initiates the route discovery by broadcasting a ROUTE REQUEST packet to its neighbors that contains the destination address D. The neighbors in turn append their own addresses to the ROUTE REQUEST packet and re-broadcast it. This process continues until a ROUTE REQUEST packet reaches D. D must now send a ROUTE REPLY packet to inform S of the discovered route. Since the ROUTE REQUEST packet that reaches D contains a path from S to D, D may chose to use the reverse path to send back the reply. The second main function of the DSR is Route Maintenance, which handles link outages.

In this paper we assume also that misbehaving nodes are supposed to operate independently and attacks by several colluding nodes are not taken into account. The research presented in [1] pointed out two types of node misbehavior: a selfish behavior and malicious behavior. *Selfish nodes* use the network but do not cooperate, saving battery life for their own communications: they do not intend to directly damage other nodes. *Malicious nodes* aim at damaging other nodes by causing network outage by partitioning while saving battery life is not a priority.

2.2 The reputation mechanism

In CORE, MANET nodes can be thought of as members of a community (or subjects) that share a common resource. The key to solve problems related to node misbehavior derives from the strong binding between the utilization of a common resource and the cooperative behavior of the members of the community. Thus, all members of a community that share resources have to contribute to the community life in order to be entitled to use those resources. However, the members of a community are often unrelated to each other and have no information on one another's behavior. We believe that reputation is a good measure of someone's contribution to common network operations. Indeed, reputation is usually defined as the amount of trust inspired by a particular member of a community in a specific setting or domain of interest. Members that have a good reputation, because they helpfully contribute to the community life, can use the resources while members with a bad reputation, because they refused to cooperate, are gradually excluded from the community.

The research carried out in [11] pointed out three possible roles that a node can assume: the *requestor*, the *provider* and the *peer* role. The notation requestor is used when referring to a node asking for the execution of a function *f* while the notation *provider* is used when referring to any entity supposed to participate to the execution of *f.*

Peers are identified as those nodes that are not directly involved in a requestor/providers exchange but are able to monitor and enforce the fairness of the exchange itself. Finally, the notation *trusted entity* is used when referring to a network entity with a positive value of reputation.

Examples of *f* can be the Packet Forwarding function and the Routing function.

2.3 Security Objectives

The mechanism outlined in this paper provides countermeasures to DoS attacks performed by both malicious and selfish nodes when they act as providers. We focus on two different categories of DoS attacks:

- Passive DoS attacks: both malicious and selfish nodes can perform this kind of attacks, indeed we suppose that a passive attack has no energy cost for the attacker. In this case misbehaving providers simply do not perform the requested function f. As an example, when we consider the DSR function a misbehaving node can perform a passive DoS attack simply by not participating to the Route Discovery phase of the protocol.
- Active Dos attacks: this kind of attacks can only be performed by malicious nodes because it costs energy. In this case, malicious nodes acting as providers prevent other providers from serving a request by communicating bogus information on reputation ratings for legitimate nodes, by performing traffic subversion or by using the security mechanism itself causing explicit Denial of Service.

2.4 Basic Scheme

2.4.1 The requestor

The requestor issues a request for the execution of the function f and monitors its execution by the visible providers (i.e. providers that are within the wireless transmission range). The requestor validates the result of the execution of *f* and, based on the outcome of the validation phase, it updates the ratings relative to the monitored providers using the reputation technique [12].

2.4.2 The provider

As a provider receives a request for the execution of a function f, based on the reputation rating associated to the requestor it accepts or denies serving the request. If the requestor is tagged as a misbehaving node the requested function is not executed and an explicit DoS message is broadcasted to all neighbors.

2.4.3 Peer validation

Peer validation is performed in order to prevent a misbehaving provider to explicitly deny the execution of *f* requested by a node with a positive reputation rating. Furthermore, the peer validation mechanism is used to prevent traffic subversion attacks: data traffic forwarded to a bogus destination or through a bogus route is detected and the malicious behavior is castigated.

The result of the proposed algorithm is that nodes that are misbehaving due to maliciousness or selfishness will gradually be isolated from the network.

2.5 Properties of the basic scheme

We summarize in this section the properties of the basic scheme we outlined in this paper.

- No negative rating information is distributed among nodes.
- Global reputation ratings for nodes classified as legitimate (i.e. the reputation rating is positive) gradually decreases along time to prevent DoS performed by idle nodes.
- Reputation is hard to build.
- The proposed mechanism has a low impact on network performance: there is no additional traffic due to the reputation mechanism. Every node of the MANET stores a local copy of the reputation ratings associated to other nodes of the network.

These properties assure:

- The detection of passive DoS attacks and cooperation enforcement: reputation value decrease when misbehavior is detected implying that misbehaving nodes are gradually isolated from the network.
- Active DoS attacks and DoS that uses the security scheme itself are prevented: it is not possible to broadcast negative ratings (and there is no advantage to broadcast positive ratings with the hypothesis that there is no collusion between misbehaving nodes) and bogus explicit DoS that aim at damaging legitimate nodes are prevented by the peer validation mechanism.

3. The game theoretical approach

In this section we present a game theoretical approach with the aim of providing a formal analysis of the security mechanism introduced in this paper. The collaborative scheme outlined in this paper and detailed in [11] is conceived for promoting and stimulating cooperation among “rational” mobile nodes. Nodes are rational, in MANET environment, in the sense they try to maximize their own utilities in a selfish way. Furthermore, we will also consider nodes that act in a non-rational way: maliciousness has a non-negligible cost thus the utility in terms of energy consumption is not maximized.

Albert Tucker introduced the term “prisoner’s dilemma (PD) game” in 1968 to describe social dilemmas situated in the real world. Tucker started with an example: the police arrest two bank robbers. The police are interrogating the criminals in separate cells and offering to set them free if they confess to the crime against their partner. Each criminal faces two choices: to confess or not to confess. If a criminal confesses while his partner does not, the criminal will be set free and his partner will go to jail. If both confess, both will go to jail. If neither of them confesses, both will be free but they will have to share the stolen money. In the classical PD game where the game is played only once, clearly the dominant strategy is to defect regardless of the other player’s move.

This simple game can be extended to the m-dimensional PD game, which can be adapted to represent the strategy to be chosen by the nodes of a mobile ad hoc network. In the rest of the section a symmetric *N*-nodes PD game will be introduced. The mobile nodes of the network can be thought of as the players of the game, which can chose to defect or to cooperate, and the security mechanism presented in this paper can be modeled as the payoff structure of the m-dimensional PD game.

3.1 The preference structure

Our 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 [20] but use a full information framework. This theory explains the behavior of players observed in a rather large group of experiments better than the standard theory.

Let the (non-negative) payoff to node *i* be denoted by y_i , *i*, . . . , *N*, and the relative share by $s_i = \frac{y_i}{\sum_j y_j}$

The utility function is given by: $a_i u(y_i) + b_i r(s_i)$ where $a_i, b_i \geq 0$ and *u()* is differentiable, strictly increasing and concave, and r*()* is differentiable, concave and has its maximum in $s_i = \frac{1}{N}$. Throughout this paper we assume that node’s disutility from disadvantageous inequality is larger than if the node is better off than average, i.e. $r(\frac{1}{N} - x) \leq r(\frac{1}{N} + x), \forall x \in \left[0, \frac{1}{N}\right]$. The types of nodes are characterized by the relative weights a_i, b_i .

3.2 The prisoner’s dilemma

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 execute 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 incentive structure given by (1) and (2) is modeled by the reputation technique used in the cooperative security scheme presented in this paper. The reputation metric [11, 12] represents the payoff that a node of the network receives or loses while operating the network: if the node cooperates its reputation increases, if the node misbehaves its reputation decreases leading to its gradual exclusion from the network.

3.3 The Nash equilibria

In the following section we analyze the Nash equilibria in the one shot PD game under the particular assumption that nodes choose simultaneously. Assume that k nodes, aside from node i, play cooperatively. Then node i chooses to play 'c' if and only if:

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

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

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

In other words, in order to choose 'c' the node must be overcompensated for the loss in absolute gain by moving closer to the average gain. The general conditions for a Nash equilibrium of this ERC-PD game are then given by:

(5) $\frac{a_i}{b_i} \leq d(k^* - 1)$ for k* nodes (playing 'c')

(6) $\frac{a_i}{b_i} \geq d(k^*)$ for the remaining N-k* nodes (playing 'd')

We now have a closer look at the number k of mobile nodes that may possibly cooperate in a Nash equilibrium. On the one hand, as long as $d(k^* - 1) < 0$, there is no chance of having a coalition of size k*. Here, $\frac{a_i}{b_i} > d(k^* - 1)$ for all types and condition (5) cannot hold for any node. On the other hand, the conditions for a Nash equilibrium given by (5) and (6) immediately imply that if $d(k^* - 1) > 0$ then there are types $\left[\left(\frac{a_i}{b_i}\right)_{i=1,\ldots,N}\right]$ of nodes such that k* nodes cooperate and N-k* nodes free-ride. These types, for example, could be given by $\frac{a_i}{b_i} = d(k^* - 1)$ for i=1,…,k*, and $\frac{a_i}{b_i} = \min\{d(k^* - 1), d(k^*)\}$ for i=k*+1,…,N. This means that, for a given distribution of ERC-types, $d(k^* - 1) > 0$ is necessary but not sufficient to get a coalition size of k*. For a given payoff structure with $d(k^* - 1) > 0$, however, there exist ERC-types such that k* is an equilibrium coalition size.

Example. Let $B(k) = km$, $C(k) = c$, where $c>m$, $r(s) = -\frac{1}{2}\left(s - \frac{1}{N}\right)^2$, and $u(y) = y$. Then, $d(k-1) > 0$ if and only if $\frac{1}{N} - \frac{km-c}{Nkm-kc} < \frac{(k-1)m}{N(k-1)m-(k-1)c} - \frac{1}{N}$, or equivalently, $\left(2 - \frac{N}{k}\right) > 0$. Therefore, if in equilibrium some nodes cooperate, then they are at least N/2.

In order to find feasible coalition sizes, we must therefore study conditions in which $d(\,)$ is positive. Note that in (4) the denominator of $d(k)$ is positive, since playing 'd' always maximizes the absolute payoff. The sign of the numerator, however, depends on the number k of cooperating nodes. It is negative for k=0 and positive for k=N-1, since both, defection and cooperation of all nodes equalize nodes' payoffs and thereby maximize $r(\,)$. Therefore, $d(0) < 0 < d(N-1)$ and no nodes unilaterally cooperates whereas all nodes playing 'c' can establish an equilibrium, provided that all nodes' types $\left(\frac{a_i}{b_i}\right)$ are smaller than $d(N-1)$.

In general, there are equilibria where only a certain number k^* of nodes cooperate. Indeed, we assumed that nodes suffer more from disadvantageous inequality than if they are better off than the average, i.e.

$r(\frac{1}{N} - x) \leq r(\frac{1}{N} + x), \forall x \in \left[0, \frac{1}{N}\right]$.

Therefore, in order to obtain $d(k) > 0$, it is necessary that by choosing 'd', a node further deviates from the equal share (1/N) than by playing 'c', i.e.:

$$\frac{B(k)}{NB(k) - kC(k)} - \frac{1}{N} > \frac{1}{N} - \frac{B(k+1) - C(k+1)}{NB(k+1) - (k+1)C(k+1)}.$$

This is equivalent to:

$0 < B(k+1)C(k)Nk + B(k)C(k+1)Nk+1-N) + C(k)C(k+1)[Nk - 2k(k+1)]$ or

(7) $$0 < B(k+1)C(k)\frac{N}{k+1} + B(k)C(k+1)N\frac{k+1-N}{k(k+1)} + C(k)C(k+1)\left(\frac{N}{k+1} - 2\right)$$

(8) $$0 < \left[B(k+1)C(k)\frac{N}{k+1} - B(k)C(k+1)\frac{N}{k}\right] + \left[\frac{NB(k)}{k} - C(k)\right]C(k+1)\left(2 - \frac{N}{k+1}\right)$$

It is possible to use this inequality to study the number k^* of nodes that play cooperatively in equilibrium. First, note that we assumed payoffs to be non-negative and therefore $NB(k) - kC(k) > 0$. Thus, the second summand is negative for $k < \frac{N}{2} - 1$.

For payoff functions that satisfy the requirement that the total cost of cooperation increases more than the total benefits gained by defecting the first bracket in (8) is negative as well. This is equivalent to say that if

(9) $$\frac{(k+1)C(k+1)}{kC(k)} > \frac{NB(k+1)}{NB(k)}$$

holds then the first bracket in (8) is negative.

As a consequence, inequality (8) cannot hold and $d(k) < 0$ for $k < \frac{N}{2} - 1$. Thus, for any given vector of types, if a node plays 'c' at the equilibrium, then, in total, at least half of the nodes cooperate.

Proposition 1. *For any given payoff structure of the PD game with ERC preferences, there is always an equilibrium in which all nodes defect.*

Proposition 2. *Given assumptions (1) and (2), if inequality (9) holds then at least N/2 nodes cooperate.*

Proposition 2 shows that if there is a coalition of cooperating nodes, then it is rather large. The results obtained with the game theoretic approach presented in this section shows that if the security mechanism used to enforce cooperation between the nodes of a mobile ad hoc network is compliant to assumption (1) and (2) and if inequality (9) holds, then at least half of the nodes of the network will cooperate.

CORE has been conceived to make cooperation attractive from both the individual and the social point of view: the cost of cooperation is compensated by higher values of reputation. On the other side, the gain of a node that defects is punished by the lost of reputation, leading to the gradual exclusion of the misbehaving node from the network: CORE is compliant to assumption (1) and (2). Without loss of generality we can also assume that inequality (9) holds: the node that cooperates has to bear some energy costs which are higher than the benefits gained by the same node being selfish. Under this hypothesis proposition 2 assures that at least half of the nodes will cooperate.

4. Future work

The results obtained following the game theoretic approach presented in this paper has still to be verified in the case that malicious nodes are considered. Indeed, inequality (9) may not hold if we consider nodes that have not a real interest in saving energy: in this case the total benefits obtained by a misbehaving node might be higher than the total cost of cooperation. It is part of our ongoing research to establish if inequality (9) persists when malicious nodes are considered. Furthermore we will focus on assumptions (1) and (2) in order to verify if they are necessary and sufficient to be sure that a large fraction of the nodes of a mobile ad hoc network will eventually cooperate.

5. Conclusion

The area of security for ad hoc network has been receiving increasing attention among researchers in recent years. However, little has been done so far in terms of the definition of security requirements specific to ad hoc networks. Security problems in MANET belong to the two fundamental categories: networks with a centralized authority characterizing an a priori trust relationship between the nodes and self-organized networks whereby no a priori trust between the nodes is available.

Countermeasures against node misbehavior in general and denial of service attacks in particular are our very first concern. In this paper we outlined a generic mechanism based on reputation to enforce cooperation among the nodes of a MANET and to prevent passive denial of service attacks due to node selfishness. Furthermore, we proposed a game theoretical approach in order to analyze the robustness of the collaborative mechanism: nodes of a MANET where no security scheme is adopted will eventually free ride, whereas with the introduction of the CORE scheme, the best strategy a node could chose is to collaborate.

6. References

[1] P. Michiardi, R. Molva. Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks. European Wireless Conference, 2002.

[2] S. Marti, T. Giuli, K. Lai, and M. Baker. *Mitigating routing misbehavior in mobile ad hoc networks*. In Proceedings of MOBICOM, 2000.

[3] The Terminodes Project. www.terminodes.org.

[4] L. Blazevic, L. Buttyan, S. Capkun, S. Giordano, J-P. Hubaux, and J-Y. Le Boudec. *Self-organization in mobile ad hoc networks: The approach of Terminodes*. IEEE Communications Magazine, June 2001.

[5] L. Buttyan and J-P. Hubaux. *Enforcing service availability in mobile ad hoc networks*. In proceedings of MobiHOC, 2000.

[6] J.-P. Hubaux, T. Gross, J.-Y. Le Boudec, and M. Vetterli. *Toward self-organized mobile ad hoc networks: The Terminodes Project*. IEEE Communications Magazine, January 2001.

[7] 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.

[8] L. Zhou and Z. Haas. *Securing ad hoc networks*. IEEE Network, 13(6):24--30, November/December 1999.

[9] G. Zacharia. Collaborative Reputation Mechanisms for online communities. Master's thesis, MIT, September 1999.

[10] 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.

[11] 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

[12] P. Michiardi, R. Molva, *Prevention of Denial of Service Attacks and selfishness in Mobile Ad Hoc Networks*, Institut Eurecom Research Report RR-02-063 - January 2002

[13] M. J. Osborne, A. Rubinstein, *A course in game theory*, MIT press 1997

[14] R. Garg, A. Kamara, V. Khurana, *Eliciting cooperation from selfish user: a game theoretic approach towards congestion control in communication networks*, IBM Research Report, IBM India Research Lab, April 2001

[15] R. van den Brink, G. van der Laan, *A class of consistent share functions for games in coalition structure*, Tinbergen Institute, 2001

[16] R.J. Aumann, J.H. Dreze, *Cooperative games with coalition structure*, International Journal of Game Theory, (1974) 217-237

[17] R. van den Brink, G. van der Laan, *Core concepts for share vectors*, CentER and TI discussion paper (1999)

[18] G. Owen, *A value for non-transferable utility games*, International Journal of Game Theory, 1972 467-477

[19] 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

[20] G. E.Bolton, A. Ockenfels, *ERC: a theory of equity, reciprocity, and competition*. The American Economic Review 2000, 90 166–193.

[21] Josh Broch, David A. Maltz, David B. Johnson, Yih-Chun Hu, Jorjeta Jetcheva, *A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols*, Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking, ACM, Dallas, TX, October 1998

[22] Tony Larsson, Nicklas Hedman, *Routing Protocols in Wireless Ad hoc Networks - A Simulation Study*, Master Thesis, LuleÅ Tekniska Universitet

[23] 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.