ST Journal of System Research
vol 4, number 1 March 2003
Security

Ad hoc network security

Pietro Michiardi - Piero.Michiardi@eurecom.fr
Refik Molva - Refik.Molva@eurecom.fr
Institut Eurécom

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.

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. The key management problem can be partially solved if we make the assumption of an initialization phase of the network during which key-pairs are generated and public key certificates are issued by a common, centralized certification authority. This is the case of managed environment, as defined in [24].

If tamper-proof hardware and strong authentication infrastructure are not available, the reliability of basic functions like routing can be endangered by any node of an ad hoc network. 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 present in section 2 a detailed analysis of security exposures specific to the ad hoc network environment, focusing on the effects that the attacks have on performances in terms of global network throughput and communication delay. The simulation-based analysis is then used to come up with an appropriate security approach which will be exposed in section 4. We outline an original solution based on a cooperative scheme. The suggested cooperative security mechanism is then analyzed from a game theoretical point of view in order to come up with a formal assessment of our algorithm.

2. SECURITY EXPOSURES IN MOBILE AD HOC NETWORKS

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 for our simulations.

2.2 Physical Layer Characteristics

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. This assumption is valid because the protocol selected for the simulations is the MAC 802.11 that provides bi-directional communications.

2.3 Dynamic Source Routing (DSR)

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.

2.4 Simulation based analysis

The simulation study has been carried out in order to analyze the effects of security exposures on essential network functions such as routing and packet forwarding. We focused our attention on the evaluation of network performance in terms of global throughput and delay of a mobile ad hoc network where a defined percentage of nodes were misbehaving. Misbehaving nodes are supposed to operate independently and attacks by several colluding nodes are not taken into account.

Our research pointed out two types of misbehavior: a selfish behavior and malicious behavior. *Selfish nodes* (SN) 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.

We will focus our attention on selfish nodes proposing three different models that have been evaluated for the DSR protocol. We believe that the selfishness problem is of great interest because nodes of a mobile ad hoc network are often battery-powered, thus, energy is a precious resource that they may not want to waste for the benefit of other nodes.

2.4.1 Selfish node of type 1

In the first model, the node systematically does not perform the packet forwarding function which is disabled for all packets that have a source address or a destination address different from the misbehaving node. However, a selfish node that operates following this model participates in the Route Discovery and Route Maintenance phases of the DSR protocol.
The consequence of the proposed model in terms of consumed energy is that the SN will save a significant portion of its battery life neglecting large data packets, while still contributing to the network operation.

2.4.2 Selfish node of type 2

The second model focuses on those nodes that do not participate to the Route Discovery phase of the DSR protocol. The impact of this model on the network operation is more significant than the first one. Indeed, if the node does not participate in the Route Discovery phase, then there will be no route including that node in the path: the consequence is that the packet forwarding function will never be executed. A SN of this type uses the node energy only for its own communications.

2.4.3 Selfish node of type 3

The third model of selfishness we present is more complex: the node behavior follows the energy levels probed by the node. We propose a selfishness model that uses two energy thresholds (T1 ,T2) to determine the node behavior. When the node's available energy falls within the interval [E ,T1) the node behaves properly, executing both the packet forwarding and the routing function (E corresponds to the initial available energy of the node). When the energy level falls in the interval [T1 ,T2) the node will behave as if it was a selfish node of type 1, thus disabling the packet forwarding function. If the energy level is within the interval [T2 ,0) then the same behavior as the one described for a selfish node of type 2 is selected. Whenever a node has no more energy it is possible to set a stochastic recharge phase: within a limited time interval the node's energy is set back to the initial value.

We believe that this selfishness model is more realistic than the others; the objective of our study will be the evaluation of the influence of parameters such as node mobility over the global network performance when nodes behave following this selfishness model.

2.5 Simulation results

The effects of the selfishness models defined in section 2.4 are studied on four different scenarios where the two parameters that define each scenario are *node density* and *node mobility*. We define node density as the number of nodes that form the MANET deployed over an 800 by 800 meter flat space. On the other hand, node mobility is defined as the

average speed each node moves at in the simulation space. We assume a pause time equals to zero, meaning that nodes are constantly moving.

Simulation results are classified in four categories: low node density (20 nodes) and low mobility (2 m/s), high node density (60 nodes) and low mobility, low node density and high mobility (15 m/s), and high node density and high mobility. The simulation run-time for all the families of graphs presented in this section is set to 50 seconds. Also, the CBR source throughput is set to 1 packet per second.

The percentage of selfish nodes (p) is increased for each simulation run and takes values from 0% to 50%: in each simulation run, only p nodes are set to be selfish while the other nodes of the network behaves correctly. The following figures show only the significant results we obtained.

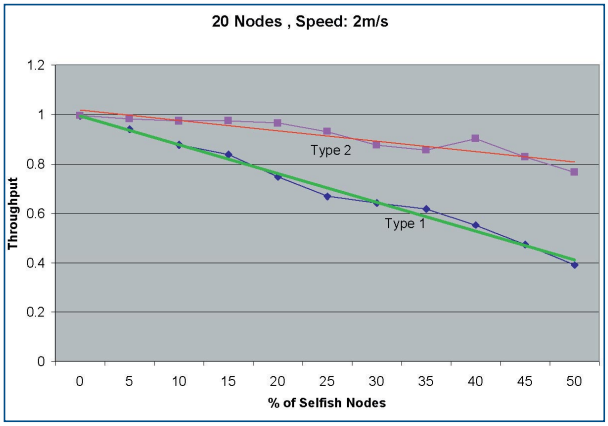

Figure 1. Network Throughput for low and high node density, low mobility.

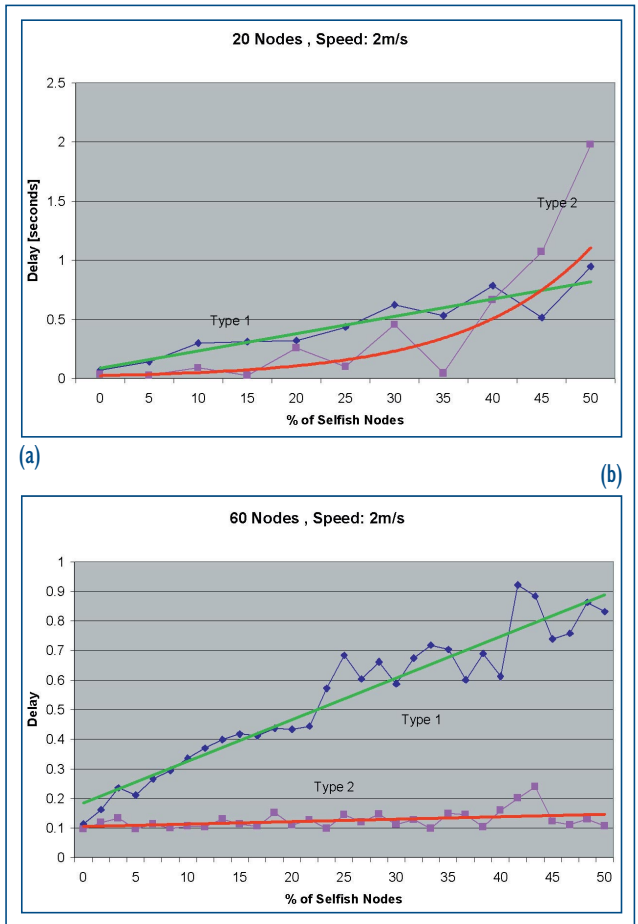

Figure 2. Communication Delay for low and high node density, low mobility.

The analysis of the results obtained with the first two families of simulations (Figure 1 and Figure 2) indicates that the effects of a node selfishness of type 1 are more important than the one caused by a selfishness of type 2. The apparent conclusion is that the mechanism for secure routing in MANET has to focus on the first type of selfishness, obliging misbehaving nodes to correctly perform the packet forwarding function.

However, if a selfish node does not participate in the Route Discovery phase of the DSR then it will never appear in any source route. It is implicit then that also the packet forwarding function will not be correctly executed, thus a mechanism that simply force a node to perform the packet forwarding function can be easily tricked by disabling the DSR function. On the other hand, a mechanism that only

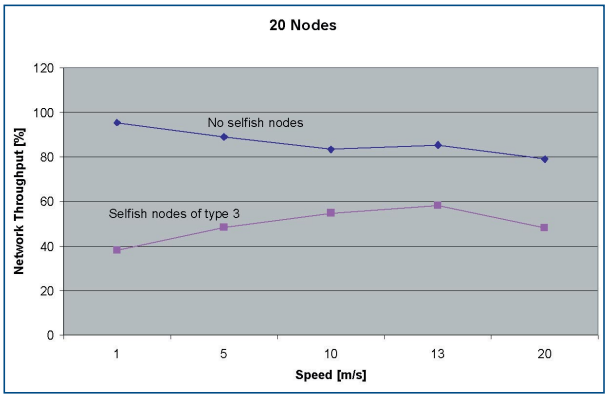

Figure 3. Global Network Throughput vs. Node Speed.

force a selfish node to correctly perform the DSR function does not assure that also the packet forwarding function will be properly executed.

Concluding, it is necessary that the security scheme adopted to face the selfish behavior of a node have to enforce the execution of both the packet forwarding and the DSR functions. Moreover, we believe that a selfish behavior that selectively disables the packet forwarding or the DSR function is not realistic: it is more likely that the node behavior dynamically changes depending on the node's energy level.

The results obtained simulating a MANET where the selfishness model of type 3 was applied to all the nodes of the network pointed out that network performances severely degrade, but the most interesting result has been depicted in Figure 3. The last family of simulations showed an interesting characteristic of the global network throughput. It has already been showed [21, 22] that the global network throughput decreases when the node mobility increases: the reason is that link outage becomes more frequent causing a higher packet loss probability. On the other side, when every node of the network is selfish of type 3, simulation results indicate that T increases when node mobility increases until it reaches its maximum; then it decreases when node mobility increases. We believe that this particular behavior depends on the mobile node topological position in the network. Given that the communication pattern used in the simulation produce a dense traffic, a central node (i.e. a node that has a central position in the MANET) consume more energy than a peripheral node because it acts as relays for other nodes, wasting its energy for routing and packet forwarding. When mobility is low, all nodes located in a central position stay in the central area of the network and consume more energy than peripheral nodes. Energy consumption leads to a selfish behavior: the packet forwarding and the routing functions will not be correctly executed and the network can be partitioned. As it is possible to see in Figure 3. for a 1m/s speed, the global network throughput is drastically reduced. When node mobility increases, the location of a node changes from a central to a peripheral position and vice-versa with a high rate, implying that the energy consumption will be equally distributed among the nodes. The selfish behavior is mitigated and T increases considerably. However, when the node mobility reaches higher values the influence of the link outage over T is more important than the impact of a selfish behavior: speed affects negatively the network performance for speed higher than 13m/s.

The results of the simulation-based analysis of the threats caused by a selfish behavior gave us the basic guidelines for the design of a security mechanism described in section 4 that prevents both selfish attacks (that we will call passive denial of service attacks in the rest of the paper) and some malicious attacks (that we will call active denial of service attacks).

3. RELATED WORK

The area of ad hoc networking has been receiving increasing attention among researchers in recent years and a variety of routing protocols targeted specifically at the ad hoc networking environment have been proposed. However, very few researchers focus on the selfishness problem in MANET and existing work in this area is still in its infancy.

In [2], the authors consider the case in which some misbehaving nodes agree to forward packets but fail to do so. In order to solve this problem, they propose two mechanisms: a watchdog, in charge of identifying the misbehaving nodes, and a pathrater, in charge of defining the best route circumventing these nodes. The paper shows that these two mechanisms make it possible to maintain the total throughput of the network at an acceptable level, even in the presence of a high amount of misbehaving nodes (e.g., 40%). However, the operation of the watchdog is based on an assumption which is not always true (as reckoned by the authors): the promiscuous mode of the wireless interface. Another problem is that the selfishness of the nodes does not seem to be castigated; on the contrary, by the combination of the watchdog and the pathrater, the misbehaving nodes will not be bothered by the transit traffic, while still enjoying the possibility to generate and to receive traffic.

Our scheme differs from the watchdog-pathrater scheme as follows:

- in our scheme misbehaving nodes are stimulated to contribute to the network operations in order to be able to use network services, the pathrater mechanism helps a legitimate user to avoid using misbehaving nodes;
- our scheme is a generic mechanism that can be integrated with several network and application layer functions whereas the watchdog-pathrater scheme is specifically designed for routing;
- unlike the pathrater technique the reputation mechanism we presented does not allow a node to distribute negative ratings about other nodes, so unlike the pathrater technique, our scheme can resist to simple denial of service attacks exploiting this vulnerability.

In [7], the authors present two important issues targeted specifically at the ad hoc networking environment: first, end-users must be given some incentive to cooperate to the network operation (especially to relay packets belonging to other nodes); second, end-users must be discouraged from overloading the network. The solution presented in their paper consists in the introduction of a virtual currency (that they call Nuglets) used in every transaction. Two different models are described: the Packet Purse Model and the Packet Trade Model. In the Packet Purse Model each packet is loaded with nuglets by the source and each forwarding host takes out nuglets for its forwarding service. The advantage of this approach is that it discourages users from flooding the network but the drawback is that the source needs to know exactly how many nuglets it has to include in the packet it sends. In the Packet Trade Model each packet is traded for nuglets by the intermediate nodes: each intermediate node buys the packet from the previous node on the path. Thus, the destination has to pay for the packet. The direct advantage of this approach is that the source does not need to know how many nuglets need to be loaded into the packet. On the other hand, since the packet generation is not charged, malicious flooding of the network cannot be prevented. There are some further issues that have to be solved: concerning the Packet Purse Model, the intermediate nodes are able to take out more nuglets than they are supposed to; concerning the Packet Trade Model, the intermediate nodes are able to deny the forwarding service after taking out nuglets from a packet.

In [10] the authors introduce a mechanism to assure routing security, fairness and robustness targeted to mobile ad hoc networks. However, they present a narrow view of security attacks that nodes of an ad hoc network can experience. Furthermore the mechanism they propose suffers from a denial of service attack performed using the security mechanism itself. Indeed, misbehaving nodes are not prevented from distributing bogus information on other nodes' behavior: the evaluation of a node behavior could then be erroneous and legitimate nodes can be classified as misbehaving nodes.

4. CORE: THE COOPERATIVE SECURITY MECHANISM

In our scheme, 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.

Our research pointed out three possible roles that a node can assume: the *requestor,* the *provider* and the *peer* role. We use the notation requestor when referring to a node asking for the execution of a function *f* and the notation *provider* when referring to any entity supposed to participate to the execution of *f*. We define *peers* those nodes which are not directly involved in a requestor/providers exchange but are able to monitor and enforce the fairness of the exchange itself. Finally, we will use the notation *trusted entity* 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. In the remaining of the paper we assume that the routing protocol used by the nodes of the MANET is the Dynamic Source Routing (DSR) protocol.

4.1 Security Objectives

The mechanism proposed 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: this kind of attacks can be performed by both malicious and selfish nodes, 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.

4.2 Basic Scheme

4.2.1 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].

4.2.2 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 to serve 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.

4.2.3 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.

4.3 Properties of the basic scheme

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

- No rating information is distributed among nodes.
- Global reputation ratings for nodes classified as legitimate (i.e. the reputation rating is positive) gradually decays 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.

5. SCENARIOS

In this section we present some significant scenarios that illustrate the security mechanism proposed in this paper.

5.1 No attack

The following scenario present an ideal situation where no misbehaving nodes are present in the network. We chose as a function *f* to observe the **DSR routing** function: Figure 4 illustrate node a performing a Route Request in order to reach node m. The Route Request has to be broadcasted by nodes b and d which are considered to be node a providers. The result of the correct execution of the Route Request is a Route Reply message which is sent back to node a and which contains the route to the destination. The Route Reply message corresponds to the ACK message we described in [12] and contains the list of the nodes that correctly participated to the DSR protocol.

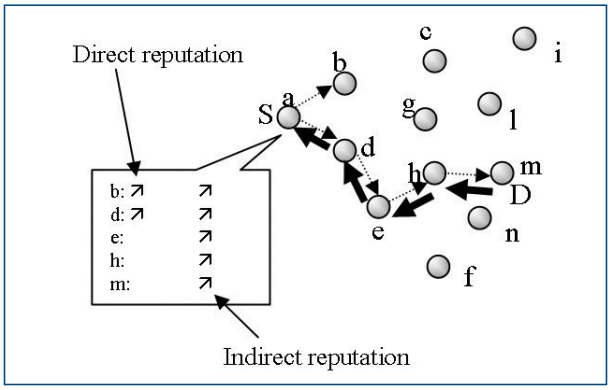

Figure 4: MANET with no misbehaving nodes.

In Figure 4, the dotted lines represent the first validation mechanism, which is used by node a to check the integrity of the ratings obtained by monitoring its visible providers b and d. For sake of simplicity the picture doesn't represent every local validation mechanism for all the nodes of the network. On the other hand, the heavy lines represent the second validation mechanism described in [12]: the ACK message (which corresponds in this case to the result of the execution of the function *f)* is used to update indirect reputation ratings and it's validated by the corresponding mechanism.

5.2 Black Hole Attack (Passive DoS)

The scenario depicted in Figure 5 presents a MANET where node h is misbehaving. Since we consider a passive attack, the misbehaving node could be both a malicious node or a selfish node: in this case the proposed mechanism is unable to detect which kind of misbehavior it has to address. However,

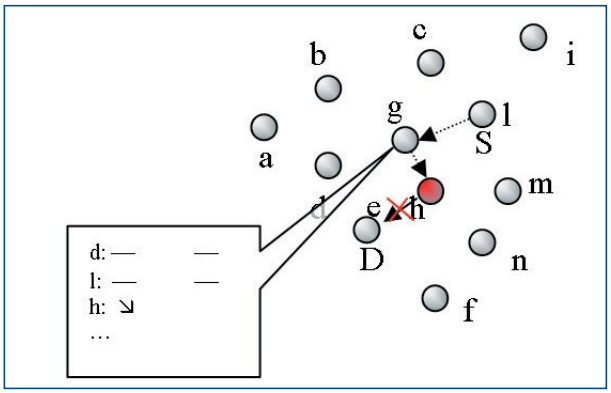

Figure 5. Black hole attack.

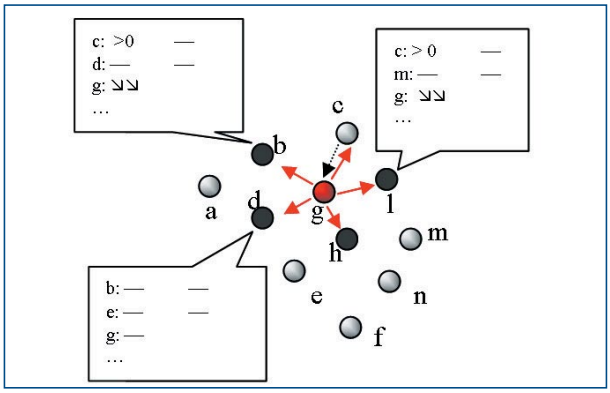

Figure 6: Attack performed using CORE.

our security scheme is able to detect which node is misbehaving and enforce its cooperation.

In Figure 5 we focus on a different network function than the previous example: *f* corresponds to the **packet forwarding function**. Node l, which is the source of the data traffic, has a valid route to node e, which is the destination of the data traffic. We suppose that node l executed the DSR routing protocol and obtained the following route: <l, g, h, e>.
Node h does not execute the packet forwarding function. The dotted line represent the first validation mechanism described in [12]: node g detects that node h is misbehaving with respect to function *f* and decreases the corresponding reputation rating in its local reputation basis. If node h misbehavior continues its reputation will decrease and eventually node h will be excluded from the network.

5.3 Active DoS: DoS using CORE?

The scenario presented in Figure 6 shows a MANET where node g is a malicious node: in this situation g is performing an active DoS attack denying the execution of the function *f* requested by the legitimate node c. As presented in section 4.2.3, the peer validation mechanism detects such misbehavior and enforce node g cooperation.

When node g broadcasts an explicit DoS, simulating the procedure that a legitimate provider would perform in case of a request coming from a misbehaving requestor, peer nodes (that are depicted in dark grey) check whether the explicit DoS was legitimate or not. As nodes b and l have reputation information concerning the requestor (node c) and the rating is in contrast with an explicit DoS, node g misbehavior is punished by decreasing the corresponding subjective reputation information. If node g persist with attacking the network it will then be gradually excluded from the network itself.

5.4 Active DoS: traffic subversion

We present in this section a more complex attack performed by a malicious node that tries to subvert traffic to reach its legitimate destination. In this particular scenario, node m (which is the source of data traffic) request for the execution of both the DSR routing function (*f1* in the picture) and the packet forwarding function (*f2* in the picture). The malicious node (node g) will participate to the DSR protocol, but will fail while executing the packet forwarding function.

As the result of the correct execution of the DSR function, node m will receive a valid route to the destination (node b): for example <m, h, g, b>. However, when performing the packet forwarding function, node g could send the data traffic to node c instead of node b.

The peer validation mechanism implemented in node c can however detect the misbehavior: indeed, the monitoring function detects the mismatching between the MAC address and the IP address forwarded by node g: the forwarded

packet (which also contains the route to the destination) contains the MAC address of node c and the IP address of node b. As a result, node c decreases its subjective reputation corresponding to node g leading to its gradual exclusion from the network if the misbehavior continues.

It should be noticed that in the first phase of the attack node g gains a positive reputation rating because the validation mechanism detects its contribution to the routing function. However, in the second phase of the attack, node g does not perform correctly the packet forwarding function: its global reputation rating should heavily degrade. In [12] we describe how the mechanism outlined in this paper can castigate this kind of active attacks: the global reputation value is calculated giving more relevance to the enforcement of critical functions such as packet forwarding. Furthermore, in [1] it has been shown that the impact of a erroneous execution of the packet forwarding function has more relevance on network performances compared to the erroneous execution of the routing function. The security scheme we propose in this paper is able to enforce the correct execution of both the discussed functions and to adjust the global rating evaluation in order to take into account critical functions.

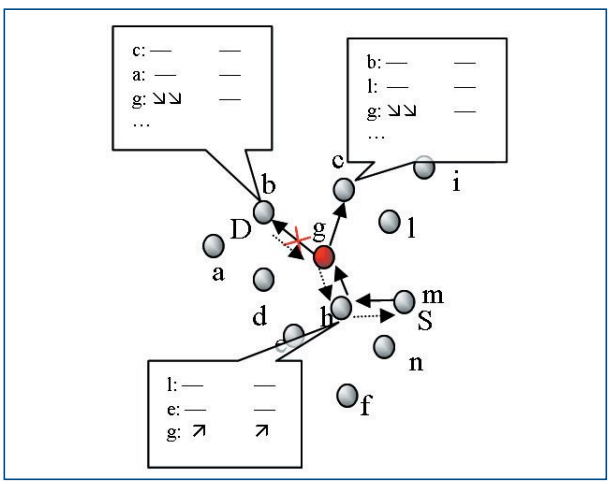

Figura 7: Traffic subversion attack.

6. A GAME THEORETICAL APPROACH

In this section we present a game theoretical approach to the proposed security mechanism with the aim of providing a formal analysis of our mechanism. The mechanism presented in the paper 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. As part of our future work, 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. Trucker 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 confess 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 modelled as the payoff structure of the m-dimensional PD game.

6.1 The preference structure

The analysis presented in this paper relies on a preference structure given by the ERC theory [20]. This theory explains most of the behaviour of players observed in diverse experiments[1], but deviates from the traditional utility concept. The utility of a player is not solely based on the absolute payoff but also on the relative payoff compared to

1 As noted by Bolton and Ockenfels, this theory can generate cooperation in the standard prisoner's dilemma.

the overall payoff to all players. Given a certain relative payoff share, the utility is strictly increasing in the own absolute payoff of the player. Given a fixed absolute payoff, the player is best off when receiving just the equal (fair) share. To both sides of this equal share, i.e. when receiving less or more than the fair amount, utility is lower, even if the absolute payoff does not change[2]. Note that in the prisoner's dilemma, the players have only the discrete choice of cooperating or defecting. Furthermore, the literature also refers to repeated games: for prisoner's dilemma situations cooperation can prevail due to an infinite repetition of the one stage game[3]. In this paper, however, we follow a different approach and study the effect of equity (fairness) preferences for the formation of cooperation.

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

We define the utility function as follows:

$$\alpha_i u(y_i) + \beta_i r(\sigma_i)$$

where α_i, β_i ? 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 node's disutility from disadvantageous inequality is larger than if the node is better off than average, i.e. $r(\frac{1}{N} - x) \le r(\frac{1}{N} + x), \forall x \in \left[0, \frac{1}{N}\right]$.

The types of nodes are characterized by the relative weights α_i, β_i.

6.2 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'. 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:

$$N \cdot B(k+1) - (k+1)C(k+1) \ge N \cdot B(k) - kC(k) \quad (1)$$

"socially desirable"

$$B(k+1) - C(k+1) \ge B(k) - C(k) \quad (2)$$

"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 modelled 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 the gradual exclusion of the node from the network.

It is possible to represent graphically the execution of a sequential PD game by a game tree: in this representation, each player acts sequentially, and each branch of the tree represents the possible set of actions the player can chose. In the following figures a PD game representing the execution of the packet forwarding function (PF) is depicted: in this scenario, 3 mobile nodes (a, b, c) are involved in the transmission of a data flow and they can chose whether to cooperate, i.e. correctly execute the PF function, or defect. The first node (a), which is represented by the root of the tree, is the data source: it has the choice whether to send or not the data packet. The last node (d),

2 Note that such a preference for equity is self-centered only and is distinct from altruism [20]. A player's utility is determined solely by its own absolute and relative payoff.

3 By the Folk theorems, basically any payoff vector can be sustained as a Nash equilibrium under certain circumstances.

which is not represented on the tree, is the destination of the data traffic. For each leaf of the tree a 3-dimensional vector represents the preference structure of the game. Figure 8 and Figure 9 represent the MANET when the security mechanism presented in the paper is not adopted, whereas the Figure 10 represents the game when the payoff structure is compliant with the reputation technique adopted by the proposed security scheme.

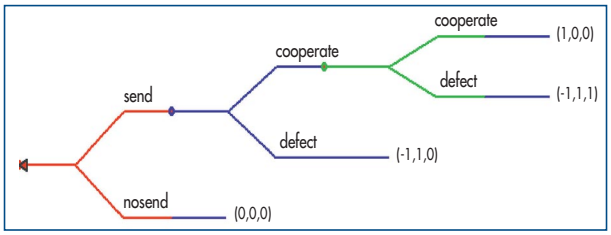

Figure 8: Game tree for a 4-node MANET without security mechanism.

In Figure 8, as an example, the preference vector (-1, -1, 1) indicates that node a and b, who cooperated to the PF function, have a low preference value while node c, who defected, has a positive value because it didn't bear the cost of executing the PF function. Using the backward induction technique, it is possible to reduce the game in order to come up with the best strategy node a should chose: from node c's point of view, if we compare the two vectors (1, 0, 0) and (-1, -,1, 1) it is convenient to chose to defect, so the sub-tree representing c choice can be reduced to a leaf leading to the preference structure (-1, -,1, 1). Iterating this technique, it is possible to find that the solution to the game is that node a shouldn't send the packet.

However it is more significant if the preference structure obliges node a to send the packet, as it is possible to see in Figure 9.

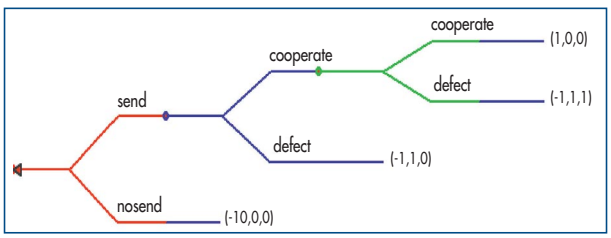

Figure 9: Game tree for a 4-node MANET without security mechanism, source obliged to send data packet.

Using the backward induction technique, however, it is possible to see that even if node a is obliged to send the data packet, node b will defect. Figure 10 represents the PD game when the preference structure represented in the tree is compliant to the payoff structure imposed by the security mechanism proposed in this paper.

As an example, when node b has to choose whether to cooperate or not, if it chooses to defect the payoff structure leads to a negative preference: the vector (-1, -10, 0) states that node a is damaged because it spent energy to send the data packet and that node b is even more damaged because the reputation mechanism implemented in the proposed security scheme will decrease its reputation, leading to its gradual exclusion from the network.

Using the backward induction technique, it is possible to see that the best strategy a node can chose is to cooperate: the last preference vector (10, 5, 5) states that the path on the tree where every node cooperates is profitable for all nodes because node a gets its data packet to the destination, and the nodes that participated to the PF function are rewarded by the security mechanism and their reputation increases.

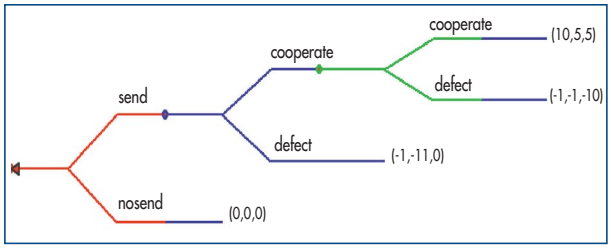

Figure 10: Game tree for a 4-node MANET when the collaborative security mechanism is operational.

6.3 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:

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

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

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

$$\frac{\alpha_i}{\beta_i} \le \delta(k) \quad \text{where} \qquad (4)$$

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

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 given by:

$$\frac{\alpha_i}{\beta_i} \le \delta(k^*-1) \quad \text{for k* nodes playing 'c'} \qquad (5)$$

$$\frac{\alpha_i}{\beta_i} \ge \delta(k^*) \quad \text{for N-k* nodes playing 'd'} \qquad (6)$$

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 $\delta(k^*-1)<0$, there is no chance of having a coalition of size k^*. Here, $\frac{\alpha_i}{\beta_i} > \delta(k^*-1)$ for all types and condition (5) cannot hold for any node[4]. On the other hand, the conditions for a Nash equilibrium given by (5) and (6) immediately imply that if $\delta(k^*-1)<0$ then there are types

$$\left[\left(\frac{\alpha_i}{\beta_i}\right)_{i=1,\ldots,N}\right]$$

of nodes such that k^* nodes cooperate and N-k* nodes free-ride. These types, for example, could be given by $\frac{\alpha_i}{\beta_i} = \delta(k^*-1)$ for i=1,…,k^*, and $\frac{\alpha_i}{\beta_i} = min\{\delta(k^*-1),\delta(k^*)\}$ for i=k^*+1,…,N. This means that, for a given distribution of ERC-types, $\delta(k^*-1)<0$ is necessary but not sufficient to get a coalition size of k^*. For a given payoff structure with $\delta(k^*-1)<0$, however, there exist ERC-types such that k^* is an equilibrium coalition size.

Example. Let , $B(k) = km$, $C(k) = c$, where $c>m$, $r(\sigma) = -\frac{1}{2}\left(\sigma - \frac{1}{N}\right)^2$, and $u(y) = y$. Then, $\delta(k-1)>0$ 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 $\delta()$ is positive. Note that in (4) the denominator of $\delta(k)$ 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, $\delta(0)<0<\delta(N-1)$ and both the situations in which no node cooperates and all nodes play 'c' can establish an equilibrium, provided that all nodes' types are smaller than $\delta(N-1)$.

However, 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.

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

Therefore, in order to obtain $\delta(k)>0$, 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:

$$0 < B(k+1)C(k)Nk + B(k)C(k+1)Nk + 1 - N) + \quad \text{or}$$
$$+C(k)C(k+1)[Nk-2k(k+1)]$$

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

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

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.

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 $\delta(k) < 0$ 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.

7. 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. We will also consider the fact that the basic assumption of the CORE mechanism under which promiscuous node listening is possible might not be true: indeed if we consider ciphered communications at the 802.11 level, it might be impossible to overhear communications and use the proposed validation mechanisms.

8. 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 needs specific to different types of scenario that can be defined for ad hoc networks. We introduced a fundamental distinction between ad hoc networks where an a priori trust relationship exists between the nodes, provided as an example by a common authority, and ad hoc networks where there is no shared a priori trust between the mobile nodes. Our research is focused on MANET where there is a lack of a priori trust relationship between mobile nodes. Countermeasures against node misbehavior in general and denial of service attacks in particular is our very first concern. In this paper we suggested 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 proposed mechanism: it is possible to see that the nodes of a MANET where our security scheme is

not adopted will eventually free ride, whereas with the introduction of our collaborative scheme the best strategy a node could chose is to collaborate.

9. 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*, Institut Eurecom Research Report RR-02-062 - December 2001

[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.

[24] B. Dahill, B. N. Levine, E. Royer, C. Shields, *A Secure Routing Protocol for Ad Hoc Networks*, Technical Report UM-CS-2001-037 University of Michigan, August 2001

[25] Andreas Lange, Carsten Vogt, "*Cooperation in international environmental negotiations due to a preference for equity*", Journal of Public Econimist 2002

Refik Molva is a professor at Institut Eurécom in Sophia Antipolis, France since 1992. He is leading the network security research group that currently focuses on multipoint security protocols, multi-component system security, and security in ad hoc networks. His past projects at Eurécom were on mobile code protection, mobile network security, anonymity and intrusion detection. Beside security, he worked on distributed multimedia applications and was responsible for the BETEUS european project on CSCW over a trans-european ATM network. Prior to joining Eurécom, he worked for IBM as a Research Staff. Member in the Zurich Research Laboratory where he was one of the key designers of the KryptoKnight security system. He also worked as a network security consultant in the IBM Consulting Group in 1997. He is the author of several publications and patents in the area of network security and has been part of several evaluation committees for various national and international bodies including the European Commission.

Pietro Michiardi received the Laurea in electronic engineering from the Politecnico di Torino in 2001. He was granted a scholarship by the European Union to take part in a program in advanced telecommunications engineering at the Eurecom Institute. In January 2000 Pietro joined the Eurecom Institute as a research engineer working on a project for the development of advanced security services for business transactions. Since September 2001 Pietro has been a Ph.D. student at the Eurecom Institute working on routing security for Mobile Ad Hoc Networks.