

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

Research Report N° RR-02-063

Prevention of Denial of Service attacks and Selfishness in Mobile Ad Hoc Networks.

Pietro Michiardi – Refik Molva
January 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 denial of service attacks and node misbehaviour are mandatory requirements in MANET. Essential network operations assuring basic connectivity can be heavily jeopardized by nodes that do not properly execute their share of the network operations. We suggest a security mechanism based on a collaborative monitoring technique that prevents active and passive denial of service attacks by enforcing node cooperation. This mechanism can be smoothly extended to basic network functions with little impact on existing protocols. We also investigate on some attacks scenarios in order to analyze the robustness of the proposed security scheme.

Keywords. Security, Mobile Ad hoc Networks, Denial of Service Attacks

Table of Contents.

| | | |
|---------|---|----|
| 1 | Introduction..... | 4 |
| 2 | Basic Scheme..... | 4 |
| 2.1 | Environment..... | 4 |
| 2.2 | Generic Algorithm..... | 5 |
| 2.2.1 | The requestor..... | 5 |
| 2.2.2 | The provider..... | 5 |
| 2.2.3 | Peer validation..... | 5 |
| 2.3 | Security Objectives..... | 5 |
| 2.4 | Reputation Concept..... | 6 |
| 2.4.1 | Definitions..... | 6 |
| 2.4.1.1 | Subjective Reputation..... | 6 |
| 2.4.1.2 | Indirect Reputation..... | 7 |
| 2.4.1.3 | Functional Reputation..... | 7 |
| 2.4.1.4 | Combination of reputation information for multiple functions..... | 7 |
| 2.5 | Validation mechanism..... | 8 |
| 3 | Properties of the basic scheme..... | 9 |
| 4 | Scenarios..... | 9 |
| 4.1 | No attacks..... | 9 |
| 4.2 | Passive DoS..... | 10 |
| 4.3 | Active DoS: bogus explicit DoS..... | 11 |
| 4.4 | Active DoS: traffic subversion..... | 11 |
| 5 | Related work..... | 12 |
| 6 | Conclusions..... | 13 |
| 7 | References..... | 14 |

Prevention of Denial of Service attacks and Selfishness in Mobile Ad Hoc Networks

1 INTRODUCTION

A simulation study presented in [1] showed that the performance of MANET severely degrades in face of simple node misbehavior. 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 increased sensitivity to node misbehavior in ad hoc networks.

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, the reliability of basic functions like routing can be endangered by any node of an ad hoc network. 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. No classical security mechanism can help counter a misbehaving node in this context.

Apart from special cases whereby an a priori trust exists in all nodes, the nodes of an ad hoc network cannot be trusted for the correct execution of critical network functions. Essential network operations assuring basic connectivity can be heavily jeopardized by nodes that do not properly execute their share of the network operations like routing, packet forwarding, name-to-address mapping, etc. Node misbehavior that affects these operations may range from simple selfishness or lack of collaboration due to the need for power saving to active attacks aiming at denial of service (DoS) and subversion of traffic. *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*, on the other hand, aim at damaging other nodes by causing network outage by partitioning while saving battery life is not a priority.

A basic requirement for keeping the network operational is to enforce ad hoc nodes' contribution to network operations and prevent active and passive denial of service attacks.

We propose a security mechanism that prevents denial of service attacks and enforces node cooperation based on a collaborative monitoring technique. The generic mechanism we suggest can be integrated with any network function like packet forwarding, route discovery, network management, and location management.

The remainder of the paper is organized as follows: section 2 introduces the generic algorithm we propose, describes our security objectives and details the underlying mechanisms of reputation and validation. The security mechanism is then illustrated with some attacks scenarios in section 4.

2 BASIC SCHEME

2.1 Environment

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.

2.2 Generic Algorithm

2.2.1 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.

2.2.2 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.

2.2.3 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.

2.3 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:

1. **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.

2. **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 Reputation Concept

The approach presented in this section is used as a basis for the security mechanism that solves the problems due to misbehaving nodes by incorporating a reputation mechanism that provide an automatic method for the social mechanisms of reputation. The proposed technique is compliant to the security requirements exposed in section 2.3: furthermore the formulae presented in the following sections are conceived in order to minimize problems due to false detection of a nodes' misbehavior. As an example, disadvantaged nodes that are inherently selfish due to their precarious energy conditions shouldn't be excluded from the network using the same basis as for malicious nodes: this is done with an accurate evaluation of the reputation value that takes into account a sporadic misbehavior.

2.4.1 Definitions

This section presents the three types of reputation used in our scheme and shows how they are combined. Reputation is formed and updated along time through direct observations and through information provided by other members of the community. Furthermore, we take the stance that reputation is compositional: the overall opinion on an entity that belongs to the community is obtained as a result of the combination of different type of evaluations. We define a subjective reputation, an indirect reputation and a functional reputation.

2.4.1.1 Subjective Reputation

We use the term subjective reputation to talk about the reputation calculated directly from a subject's observation. A subjective reputation at time t from subject s_i point of view is calculated using a weighted mean of the observations' rating factors, giving more relevance to the past observations.

The reason why more relevance is given to past observations is that a sporadic misbehavior in recent observations should have a minimal influence on the evaluation of the final reputation value: as a result, it is possible to avoid false detections due to link breaks and to take into account the possibility of a localized misbehavior caused by disadvantaged nodes.

The general formula to calculate a subjective reputation is:

$$r_{s_i}^t(s_j|f) = \sum \rho(t, t_k) \cdot \sigma_k$$

where $r_{s_i}^t(s_j|f)$ stands for the subjective reputation value calculated at time t by subject s_i on subject s_j with respect to the function f .

$\rho(t, t_k)$ is a time dependent function that gives higher relevance to past values of σ_k .

σ_k represents the rating factor given to the k -th observation: we use a scale that goes from -1 for a negative impression (meaning that the observed result doesn't match with the expected result) to +1 for a positive impression (i.e. when the observed and the expected results coincides).

When the number or the quality of observations collected since time t are not sufficient, the final value of the subjective reputation takes the 0 value, which is used for a neutral impression.

Finally, given that $\sigma_k \in [-1, 1]$ and that $\rho(t, t_k)$ is a normalized value, also $r_{s_i}^t(s_j|f) \in [-1, 1]$.

Note also that the set $\{s_j\}$ is restricted to the set of the neighbors of subject s_i . We use the term neighbor to refer to a subject that is within wireless transmission range of another subject.

2.4.1.2 Indirect Reputation

In our scheme, the subjective reputation is evaluated only considering the direct interaction between a subject and its neighbors. With the introduction of the indirect reputation measure we add the possibility to reflect in our model a characteristic of complex societies: the final value given to the reputation of a subject is influenced also by information provided by other members of the community.

In the reminder of the paper, $ir_{s_i}^t(s_j|f)$ denotes the indirect reputation of subject s_j collected by s_i at time t for the function f .

The information collected through indirect reputation can take only positive values: denial of service attacks based on malicious broadcasting of negative ratings for legitimate nodes are thus prevented and the method is compliant to the second objective described in section 2.3.

2.4.1.3 Functional Reputation

We use the term functional reputation to talk about the subjective and indirect reputation calculated with respect to different functions f . With the introduction of this last type of reputation in our model we add the possibility to calculate a global value of a subject's reputation that takes into account different observation/evaluation criteria. As an example, a subject s_i can evaluate the subjective reputation $r_{s_i}^t(s_j|f(\text{packet forwarding}))$ of subject s_j with respect to the packet forwarding function and the subjective reputation $r_{s_i}^t(s_j|f(\text{routing}))$ with respect to the routing function and combine them using different weights to obtain a global reputation value on subject s_j .

2.4.1.4 Combination of reputation information for multiple functions

Reputation information is combined using the following formula:

$$r_{s_i}^t(s_j) = \sum_k w_k \cdot \{r_{s_i}^t(s_j|f_k) + ir_{s_i}^t(s_j|f_k)\}$$

where w_k represents the weight associated to the functional reputation value.

$r_{s_i}^t(s_j)$ represents the global reputation value that is evaluated in every node: it is the aggregate reputation definition.

The choice of the weights w_k used to evaluate the global reputation has to be accurate because it can affect the overall system robustness. In [1] the authors present a simulation study that points out that even if the enforcement of the execution of both the packet forwarding function and the routing function are mandatory, the former has an important impact on the global performances compared to the latter. This is why a good choice for w_k would emphasize the correctness of the packet forwarding function when evaluating the overall reputation for a node.

Furthermore, the combination of a reputation value evaluated for different functions is a mandatory requirement to solve the traffic subversion problem, as detailed in section 4.

Besides the global reputation value, it is important to know how reliable is that value. Although there are a lot of elements that can be taken into account to calculate how reliable a global reputation is, we propose two of them: the number of evaluations used to calculate the final reputation value and its variance. This approach is similar to that used in the Sporas system [9].

2.5 Validation mechanism

The global reputation is obtained as a combination of local observations made by a subject over a neighboring subject with respect to a defined function f and information collected through indirect reputation measurements. It is necessary to define a validation mechanism (VM) based on feedback information that assures integrity of ratings in the special situation where there is no shared trust between the nodes of the MANET.

We defined three types of validation mechanisms that are used to assure integrity of subjective observations, indirect observations and integrity of explicit DoS messages.

1. The first validation involves a requestor monitoring the providers that are within wireless transmission range and it is used to update the requestors' subjective reputation ratings. Every time a network entity ($s_{i,m}$, monitoring entity) needs to monitor the correct execution of a function implemented in a neighboring entity ($s_{j,o}$, observed entity), it triggers the VM specific to that function (f). If the monitored function is executed properly (i.e. observed and expected results coincides) then the rating factor σ_k associated to the k -th observation will be positive, while if the observation shows that the expected results are not reached (i.e. the function f has not been correctly executed) then the rating factor will be negative. It should be noticed that the term expected result corresponds to the correct execution of the monitored function, which is substantially different from the final result of the execution of the function. A possible implementation of the validation mechanism is provided by Marti et al. [2]. The watchdog technique presented by the authors, relies on the promiscuous mode operation and has some weaknesses that have been described in [2].
2. The second validation mechanism we have defined involves a requestor that evaluates the contribution of the providers concerned in the execution of f . We assure integrity of ratings by introducing an acknowledgement message (ACK) that is sent back to the requestor as the result of the execution of f . The ACK message contains a list of the providers that cooperated with the requestor in order to obtain the result of f . Every node that is on the return path of the ACK message uses the rating information to update its indirect reputation ratings. Only positive rating information is transmitted within the ACK message: a bogus spread of negative ratings from a misbehaving provider is not possible, implying that the security mechanism itself can not be used by misbehaving nodes. On the other side, a misbehaving provider aiming at distributing bogus positive rating information has no direct advantage.
3. As described in section 2.2, before serving a request the provider checks the global reputation rating it has evaluated for the requestor. 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. We defined a last validation mechanism that assures the integrity of an explicit DoS message. The peer validation mechanism assures that legitimate nodes are not damaged by bogus explicit DoS attacks. Whenever a peer entity receives an explicit DoS message for a requestor, it checks whether its local copy of reputation ratings associated to that requestor are consistent with the denial of service. If a legitimate node (a node with a positive reputation rating) received a bogus explicit DoS then the peer entity will decrease its subjective ratings relative to the malicious provider. If the provider persist in damaging other nodes it will gradually be excluded from the network. The peer validation mechanism assures also that traffic subversion is detected and the malicious node that performed the attack is castigated. Any node of the network uses the peer validation to ensure that it is a legitimate recipient of the data traffic either because it is the

destination or because it is on the path to reach the destination. If a misbehavior is detected the node responsible of the traffic subversion will be castigated.

3 PROPERTIES OF THE BASIC SCHEME

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

1. No negative rating information is distributed among nodes.
2. 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.
3. Reputation is hard to build.
4. 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.

4 SCENARIOS

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

4.1 No attacks

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 1 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 section 2.5 and contains the list of the nodes that correctly participated to the DSR protocol.

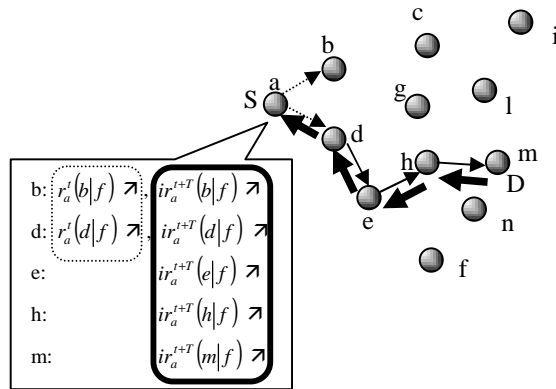


Figure 1. MANET with no misbehaving nodes.

In Figure 1, 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 section 2.5: 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.

4.2 Passive DoS

The scenario depicted in Figure 2 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, our security scheme is able to detect which node is misbehaving and enforce its cooperation.

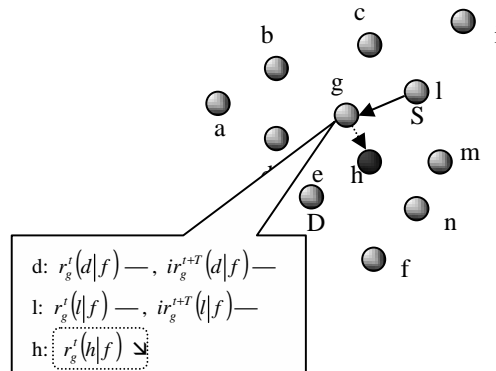


Figure 2. MANET with one misbehaving node performing a passive DoS attack.

In Figure 2 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: $\langle l, g, h, e \rangle$.

Node h does not execute the packet forwarding function. The dotted line represent the first validation mechanism described in section 2.5: 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 g misbehavior continues its reputation will decrease and eventually node g will be excluded from the network.

4.3 Active DoS: bogus explicit DoS.

The scenario presented in Figure 3 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 node c . As presented in section 2.5, the peer validation mechanism detects such misbehavior and enforces node g cooperation.

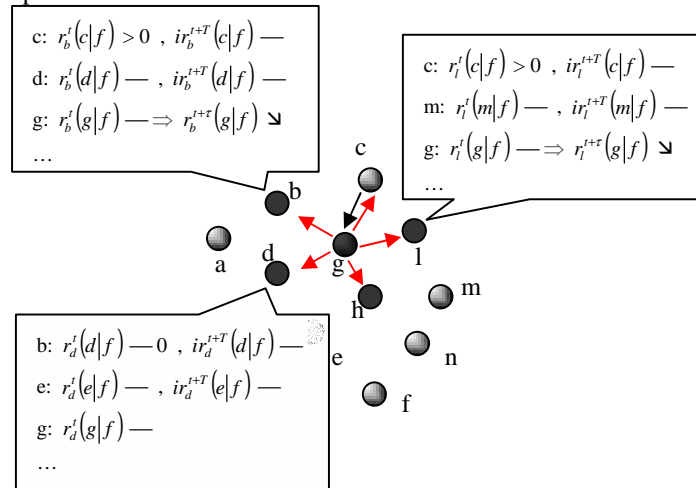


Figure 3. MANET with one misbehaving node performing a bogus explicit DoS.

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 persists with attacking the network it will then be gradually excluded from the network itself.

4.4 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.

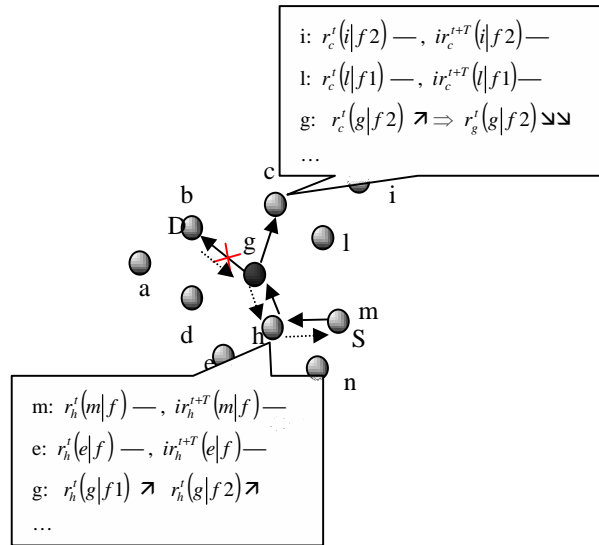


Figura 4. MANET with one misbehaving node performing traffic subversion.

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 $\langle m, h, g, b \rangle$. 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. Section 2.4.1.4 describes how the mechanism presented 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] the authors showed that the impact of an 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.

5 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.

6 CONCLUSIONS

The area of ad hoc network security 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 attacks that range from active denial of service to passive denial of service and node selfishness. This mechanism can be smoothly extended to basic network functions with little impact on existing protocols.

An in-depth analysis of our security scheme is ongoing using our simulation environment. Our goal is to implement a wide choice of attacks using the QualNet network simulator: we enhanced our software by adding passive denial of service attacks perpetrated on the packet forwarding function and the routing function and we plan to add new features including active denial of service attacks and traffic subversion. We also aim at extending our misbehavior model in order to consider eventual collusion between malicious entities.

The analysis of the simulation results is based on an appropriate metric we defined in order to give emphasis to the robustness of a generic security scheme with respect to the percentage of misbehaving nodes present in the network. We also plan to analyze the performances of our mechanism with respect to node mobility and node density: we believe that network characteristics can be used as trigger signals for the fine tuning of our scheme.

7 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, 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.