On the Robustness of a Novel Reputation Mechanism for Centralized Clustered Ad-hoc Networks

Spyridon Vassilaras, Dimitrios Vogiatzis and Gregory S. Yovanof
Broadband Wireless and Sensor Networks Group
Athens Information Technology,
Markopoulo Ave., PO. Box 68, 190 02, Peania, Athens, Greece
e-mail: {svas,dvog,gyov}@ait.edu.gr

***Abstract* - Although individual node cooperation is necessary for the correct execution of network protocols in Mobile Ad-hoc Networks, it is not always guaranteed. In this paper, we present a reputation mechanism aiming at enforcing node cooperation in clustered Mobile Ad-hoc Networks with centralized control. Misbehavior detection techniques for protocol attacks in the cluster formation phases of the network operation are developed. Statistical methods for selecting the optimal parameters of the reputation scheme are investigated and their efficiency is illustrated through theoretical analysis and simulation results. Special care has been given to issues such as probability of detection of a misbehaving MT and probability of falsely accusing a legitimate node due to non-intentional failures to cooperate. Additionally, the robustness of the reputation mechanism in the presence of multiple malicious or selfish nodes is evaluated.**

***Index Terms* — Ad-hoc networks, MANETs, Cooperation Enforcement, Misbehavior Detection, Reputation Mechanism, Random Walk.**

I. INTRODUCTION

The need for security in wireless networks is of paramount importance for their widespread usage. Apart from classical security issues (such as user, host and message authentication, data confidentiality and integrity, non-repudiation, key management etc.) ensuring the cooperation of nodes emerges as a crucial and complicated problem in *Mobile Ad-hoc Networks* (MANETs). The correct execution of network functions in MANETs relies on the cooperation of the individual nodes that constitute the network. Malicious *Mobile Terminals* (MTs) that intentionally fail to execute their part of a network protocol in order to cause damage and selfish MTs that do not cooperate in order to save precious resources (such as battery power) can severely disrupt proper network operation.

Thus, providing incentive mechanisms that will convince selfish MTs to cooperate and detection mechanisms that will identify malicious MTs and isolate them from the network is a critical issue, which has received considerable attention recently from the research community ([1],[5],[7],[9]).

In the literature of node cooperation enforcement, the proposed solutions can be subdivided into two main categories: trade based schemes and reputation based schemes (see [1] for a more rigorous taxonomy of incentive schemes). In trade based schemes, a node that provides some service to a peer node (e.g. packet forwarding) is rewarded by either another immediate service in exchange or some monetary token that he can later use to buy services from another node (e.g., [2],[3],[4]). In reputation based schemes each node keeps a reputation metric for other nodes he deals with and provides services only to nodes that exhibit good reputation (e.g., [5]-[10]).

In this paper, we present a reputation based scheme for promoting node cooperation and preventing protocol attacks in a special kind of MANETs: Clustered mobile Ad-hoc networks which operate under the coordination and supervision of a central entity. A typical example of such a system is the *Centralized Ad-hoc Network Architecture (CANA),* which has been developed under the IST-BROADWAY project[1]. We are investigating different design parameters for the reputation mechanism to address issues that have to do with the identification of malicious MTs, the detection of selfish behavior and the cooperation enforcement of misbehaving nodes. Furthermore, special emphasis has been given to assessing the robustness of the reputation mechanism against an increasing percentage of misbehaving nodes in the network.

In the first part of this paper, we are developing techniques for rating the conformance of individual MTs to a neighborhood discovery protocol. Sophisticated attacks can be carried out against this protocol in order to provide false information about the node connectivity and disrupt network operation. So far research on secure protocols for MANETs has focused on secure routing and cooperation for packet forwarding. We turn our attention to identifying non-cooperating behavior during the neighborhood discovery and cluster formation operation.

II. CENTRALIZED CLUSTERED MOBILE AD-HOC NETWORKS

Current user needs and modern multimedia network applications require high bit rates for data transfer. To increase the total capacity of such networks, a clustered mobile ad-hoc architecture can be used. In such a setting, a

[1] This work is partly funded by the Commission of the European Community under the BROADWAY project (IST-2001-32686).

specific set of MTs that are closely located and want to exchange data, are organized into a cluster. Each cluster operates in a different frequency channel to avoid interference with neighboring clusters. Communication between MTs that belong to different clusters is achieved with the help of *Forwarding Nodes* (FNs). FNs are MTs which belong simultaneously to two adjacent clusters and serve as bridges to forward data packets among them. An FN is able to communicate in both communication channels, but at each timeslot is only capable of being tuned in one of the two clusters.

The decisions about cluster formation, including assigning FNs, are made by a central entity, commonly known as the *Access Point (AP)* or *Central Controller (CC)*. Thus, the AP assumes the role of the coordinator of the system, having under its supervision the MTs of all clusters. In order to discriminate between pure Ad-hoc clustered networks, from this point on we will be referring to this type of networks as Centralized Clustered Mobile Ad-hoc Networks, e.g. the *Centralized Ad-hoc Network Architecture (CANA)* (see [11],[12] for more details).

MT mobility and changing communication needs dictate a dynamic cluster formation algorithm. Network topology information is gathered by the AP during a *Neighborhood Discovery (ND)* operation, which is performed repeatedly in certain time intervals, in order to adapt to dynamic network conditions. The ND takes place in a predefined channel where all MTs exchange messages at a shorter transmission range, in order to identify their one hop neighbors. When a broadcast *'NextND Phase'* message sent by the AP is received by the MTs, they all enter the ND phase and send *'ND messages'* in specific time slots assigned by the AP (so that collisions do not occur). Then each MT sends to the AP an *MTi-table,* each row of which is filled with the source MAC address of an 'ND message' it has received and the quality of reception (link status). Based on input from all MTs, the AP then decides on the exact cluster topology and communicates it to the MTs.

Typically, the AP has access to the core network through a wireline infrastructure. The AP also is considered to be a trusted entity, adopting thus the role of the security manager in the network. In fact the AP is believed to be the only trusted device in the network; all the MTs may constantly or occasionally misbehave, drop packets, misroute data packets, try to mislead the AP regarding the network topology or develop other forms of misbehavior that we shall discuss in the forthcoming section.

In order to be granted access to the network, an MT has to perform a mutual authenticated with the AP. For this purpose we assume that each MT shares a symmetric encryption key with the AP. This key can be generated through a joint use of a long term pre-shared key and a proper key exchange algorithm (e.g., Diffie-Hellman). The symmetric encryption key can be used by an encryption algorithm (e.g. DES, 3DES) to provide integrity and confidentiality of the transmitted data.

Due to their ad-hoc nature, centralized clustered mobile networks are prone to (well known in the literature of Mobile Ad-hoc Networks) non-cooperative behavior issues. In this type of networks non-cooperative behavior can be encountered not only in the data transmission phase but also during the Neighborhood Discovery phase. Sometimes protocol attacks in the ND phase from *malicious* or *selfish* - though authenticated - nodes can turn out to be more detrimental for the proper network operation, since they affect the information about the network topology yielding thus even to network partitioning.

The key mechanism for addressing these issues is a node reputation mechanism implemented by the AP. The goal of this mechanism is to keep track of misbehaving MTs so that they can be isolated from the network and penalized appropriately. It is clear that misbehavior detection and cooperation enforcement in the ND phase concern any type of clustered mobile ad-hoc networks (e.g., Bluetooth scatternets), irrespective of the type of medium access they utilize or whether they have a central controller or not.

III. NON-COOPERATIVE BEHAVIOR IN THE ND PHASE

In the ND phase, the MTs exchange 'ND messages' in order to provide connectivity information to the AP, as described in the previous section. Unfortunately, the ND protocol is vulnerable to a multitude of non-cooperative scenarios: A malicious node may send a false 'ND message' masquerading as another node, modify the MTi-table by adding or removing rows, or refuse to send an 'ND message'. It can also replay 'ND messages' it has received from other nodes or launch a so called wormhole attack in cooperation with another MT (forward received 'ND messages' via a private channel to an accomplice who will replay them). Replaying and wormhole attacks aim to create the false impression that MTs which are out of range of each other can actually communicate, thus creating disconnected clusters. A selfish node may refuse to send 'ND messages' and/or send an empty MTi-table to the AP so that it won't be asked to participate in any cluster and need to consume energy. All the above attacks against the correct execution of the ND protocol can be divided into two categories:

- MT-i table row removal and refusal to send 'ND messages' constitute passive attacks, which attempt to conceal connectivity information from the AP.
- The remaining illegal actions constitute *active attacks*, which provide the AP with false connectivity information.

The simple authentication scheme presented below is able to defend against all active attacks by one or more non-colluding nodes:

For each new ND phase, the AP generates and includes in the '*Next ND Phase'* message a random number, '*Next ND RN'*. Each MT encrypts this random number with the symmetric key that it shares with the AP and includes the result in the *'ND message'*, as a form of a digital signature. The MTi-tables are also modified to include a column with these encrypted values and a column with the time-slot when the '*ND message'* was received (to defend against replaying attacks). In this way, an addition of a false row to the MTi-table will be detected by the AP, since the encrypted random number in this entry will not decrypt to the correct '*Next ND RN'* with the associated symmetric key. For the same reason an MT cannot impersonate another

MT by putting the other MT's MAC address in its own 'ND message'.

Replaying attacks are also detected by the proposed scheme because each MT gets a specific time slot in which to send 'ND messages' and the '*Next ND RN'* prevents replaying 'ND messages' from previous time slots of the present or a past ND phase. However, two colluding attackers can mount successful active attacks because the first attacker can transmit his encrypted '*Next ND RN'* through a private channel or, worse yet, divulge his secret key to the second one which will be able to successfully impersonate him.

Active attacks are characterized by the fact that they aim at deceiving the AP into believing that two MTs that are out of range of each other can actually communicate. Therefore, upon detecting an active attack, the AP just ignores the fake connectivity information and proceeds with cluster formation without trying to discover the offender and take action against him. Since all active attacks are detected and can cause no damage to the correct execution of the ND protocol, malicious nodes have no incentive to launch an active attack.

IV. THE REPUTATION MECHANISM

On the contrary, passive attacks aim at concealing the fact that two MTs can communicate from the AP. In some cases, the omitted connectivity information cannot be reliably reconstructed by the AP and thus selfish or malicious MTs have a motive to exhibit this kind of behavior. To discourage them from doing so, the AP should try to determine which MT has misbehaved and take appropriate action.

Passive attacks can be detected by comparing the received MTi-tables from different MTs. Let's assume for example that the received MTi-tables at the AP from nodes A and B are inconsistent, indicating that node A has heard from node B, but B has never heard from node A. Then two things might be happening: either B is lying (has removed from its MTi-table the entry corresponding to node A) or node A has not sent 'ND messages' at all (note that the defense mechanism against active attacks prevents the possibility that node A has maliciously added an extra row to its MTi-table). But, if the AP has received at least one other MTi-table containing node A, it can be certain that A actually sent an 'ND message' and thus B is probably the misbehaving node. We say 'probably' because there is a small chance that B never received A's 'ND message' or received it incorrectly due to node mobility or communication link failure. In this case, we have a 'false positive' where B will be accused of having a row removed from its MTi-table while this is not true. There is also the possibility of a 'false negative' where B removes A from its MTi-table but goes undetected from the AP. This happens when i) A has no well behaving neighbors ii) both A and B have removed each other from their MTi-tables or iii) A hasn't received B's 'ND message' due to link failure.

Similarly, the AP suspects a node B of having kept silent during the ND phase if no MT reported having received B's 'ND message'. A 'false positive' in this case occurs when i) there were no other MTs in B's vicinity or ii) all of B's neighbors removed it from their MTi-tables or didn't receive B's 'ND message' due to link failure.

In order to limit the effect of false positives the AP can observe each MT for a larger amount of time than a single ND phase, and compare their behavior to the expected behavior of a well-behaving node. One common way of keeping track of a node's long term behavior is by assigning to it a reputation metric which will be reduced if the node is suspected to have misbehaved and increased otherwise. If this metric falls below a given threshold, the node is considered misbehaving. This way, not only nodes that exhibit consistent misbehavior, but also nodes that misbehave with a certain probability will get detected. Although this scheme is popular in the literature ([5],[6],[10]), it has not been, to the best of our knowledge, analyzed quantitatively. In the remainder of Section IV, we model the evolution of a reputation metric in time as a random process and investigate its efficiency in detecting misbehaving nodes with respect to the probability of wrongly accusing a well behaving node. The percentage of malicious nodes in the network is increased and the robustness of the reputation mechanism is assessed.

A. The reputation metric as a random walk process

Because of the different nature of the 'false positives' in each type of passive attack, the AP will keep two reputation metrics for each MT; r_1 for row removals and r_2 for keeping silent. Both metrics should be initialized at some positive value a_i, i.e. $r_i(0) = a_i > 0, \quad i = 1,2$. r_1 is increased for each legitimate entry in the MT's MTi-table and reduced when there are suspicions that the MT has removed a row from the table. r_2 is updated once at each ND phase according to whether the MT is contained in at least one MTi-table. Therefore, after the k-th 'event' we have: $r_i(k) = r_i(k-1) + \Delta r_i(k)$ with:

$\Delta r_i(k) = -1$, if a suspicious event occurs and

$\Delta r_i(k) = b_i$, otherwise.

If the i-th reputation metric of a node becomes smaller than or equal to 0, this node is considered to have performed a type i passive attack. Clearly, the random process $\{r_i(k)\}$ is a random walk in which the event of a node getting accused for misbehavior is a threshold crossing event [13]. For a well-behaving node, we expect suspicious events of type 1 to occur more or less independently with a small probability P_{loss}, as they are caused by fluctuations in the quality of the wireless link. False positives of type 2 will probably exhibit strong time dependencies, particularly in networks with low node mobility where the number of neighbors a given MT has, changes slowly with time.

Let us first concentrate on $\{r_1(k)\}$ for a well-behaving node which is a random walk with i.i.d. steps. Assuming that we can estimate P_{loss} with a reasonable accuracy[2], we want to set the parameters of the random walk in such a way that the threshold crossing probability (i.e., the probability of wrongly accusing a well behaving node) does not exceed

[2] In any case, a conservative estimate of P_{loss} can be used instead, e.g., the upper end of a 99% confidence interval.

a very small value P_{wrong}. A logical choice for the value of b_1 is:

$$b_1 = \frac{P_{loss}}{1 - P_{loss}} \qquad (1)$$

which results in a zero drift random walk by making the mean value of the per step change in the reputation metric equal to 0. It is well known that a zero drift random walk with infinite horizon will eventually cross any finite threshold with probability 1. To avoid this, we can select an appropriate window size n, and update the reputation metric for k>n, as follows:

$$r_1(k) = r_1(k-1) + \Delta r_1(k) - \Delta r_1(k-n)$$

An upper bound to the threshold crossing probability for a random walk in a finite horizon is given by (see chapter 7.4 in [13]):

$$P_{good}(r_1(k) \le 0) \le \exp[n\gamma(\theta^*) - \theta^* \cdot a_1] \quad (2)$$

where θ^* is the minimizing θ in $\min_{\theta \ge 0}[n\gamma(\theta) - \theta \cdot a_1]$, $\gamma(\theta) = \ln E[\exp(-\theta \cdot \Delta r_1(k))]$ and a_1 the initial value of r_1. Unfortunately, an exact value for this probability cannot be obtained. An exact value can be calculated if we set $b_1 = 0$ (and the suspicious events are i.i.d.) and we will take a little detour to investigate this case before continuing with the zero mean random walk approach (where b_1 is set according to Eq. 1).

B. Measuring empirical frequencies of suspicious events

The reputation metric scheme with $b_1 = 0$ is similar to measuring the empirical frequency of suspicious events in a window of size n and comparing it to the probability of such events. The probability that a well behaving node experiences exactly k suspicious events out of n events follows the binomial distribution:

$$P_{good}(X = k) = \frac{n!}{k!(n-k)!} P_{loss}^k (1 - P_{loss})^{n-k} \qquad (3)$$

Based on this expression we can find an integer a_1, such that $P_{good}(X \ge a_1) \le P_{wrong}$ and $P_{good}(X \ge a_1 - 1) \ge P_{wrong}$. In other words, the value of the threshold $a_1 - 1$ is the maximum number (and the ratio $(a_1 - 1)/n$ the maximum relative frequency) of suspicious events in a sliding window of size n that we can accept without accusing the MT of having misbehaved.

Clearly, under this scheme, a consistently misbehaving node will get caught after a_1 events. However, a more sophisticated malicious node can try to evade detection by misbehaving with some probability P_{mal} and independently from previous events. The probability that an MT which behaves in such a way produces exactly k suspicious events is given by Eq. 3 if P_{loss} is replaced by $P_{mal} + (1 - P_{mal})P_{loss}$. In Fig. 1 we plot the base 10 logarithm of the probability of a misbehaving MT getting accused as a function of $P_{mal} + (1 - P_{mal})P_{loss}$. To generate this plot, we assumed $P_{loss} = 10^{-5}$ and n=10,000, requested that $P_{wrong} = 10^{-10}$ and used these parameters to compute $a_1 = 7$. Fig. 1 shows that the probability of detecting the malicious MT grows very fast approaching 1 for $P_{mal} \approx 10^{-3}$.

In certain applications, it is crucial that the probability of a malicious MT getting detected is lower bounded, i.e., the malicious MT is detected with a minimum probability P_{det}, irrespective of the probability of accusing a legitimate MT. Fig. 2 shows the probability of false positive P_{wrong} as a function of $P_{mal} + (1 - P_{mal})P_{loss}$ for $P_{det} = 0.95$. The rest of the parameters have been kept the same as in the previous case. Clearly, as the probability of behaving maliciously increases, the probability of falsely accusing a legitimate MT diminishes, indicating that for relatively high P_{mal} the confidence when accusing an MT is quite high.

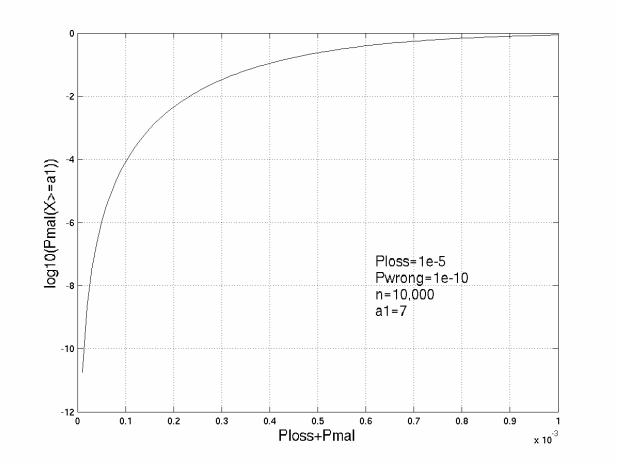

Fig. 1: Probability of a malicious node getting detected as a function of his misbehavior probability

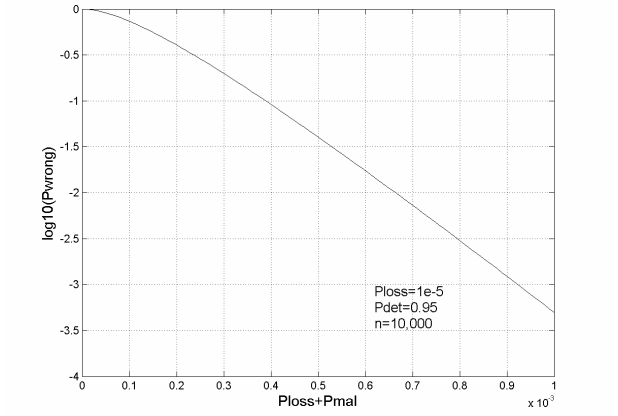

Fig. 2: Probability of a legitimate node getting accused as a function of a malicious' node misbehavior probability

C. Analysis of the robustness of the random walk model

The probability of detection of a malicious user depends on the number of malicious nodes in the network. It is expected that more malicious nodes, colluding or not, can cause greater damage to the network, while at the same time the detection mechanism may not be able to detect neither of them. Fig. 3 shows this probability as a function of the number of malicious users in a network of a total of 50 nodes. The maximum number of malicious nodes ranges from 2% to 40% of the overall number of nodes and we assume that the malicious nodes move randomly inside the cell area and they do not collude with each other.

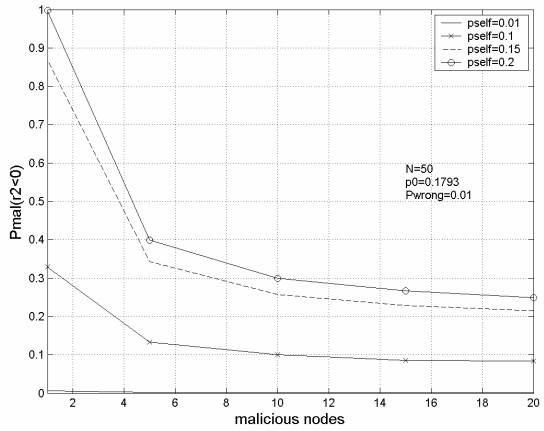

Fig. 3: Probability of a malicious node getting detected as a function of the number of malicious nodes in the cell.

Respectively, Fig. 4 shows the probability of a well-behaving node getting accused as a function of the number of malicious nodes. It can be easily seen that the more malicious nodes in the network, the greater the probability that a legitimate node can be viewed by the AP as if not sending any '*hello messages'* at all and thus being accused of exhibiting non cooperative behavior.

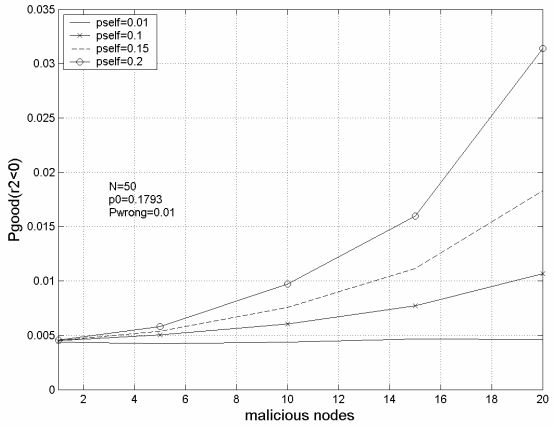

Fig. 4: Probability of a well-behaving node getting accused as a function of the number of malicious nodes in the cell.

The above graphs correspond to a rather low node density. We should note that the robustness of the proposed reputation scheme against multiple malicious nodes heavily depends on the node density.

V. CONCLUSION

So far research on secure protocols for MANETs has focused on secure routing and cooperation for packet forwarding. However, clustered Mobile Ad-hoc networks are also prone to protocol attacks that can take place in the neighborhood discovery and cluster formation operation of the network. In this paper, we have investigated cooperation enforcement for neighborhood discovery and cluster formation for clustered ad-hoc networks with centralized supervision. We have designed a reputation mechanism which is based on scalar reputation metrics and performed a quantitative analysis on methods for selecting step sizes and threshold values. We have treated the evolution of the reputation metric over time as a stochastic process. In our work we addressed the issue of detecting malicious behavior with certain probability and alternatively the dual problem of wrongfully accusing a node for misbehavior, in networks with varying node density. In addition, we evaluated the robustness of the proposed reputation mechanism, by assessing the impact of multiple misbehaving users on the probability of detecting a selfish/malicious node and the probability of wrongfully accusing a legitimate node.

Although our cooperation enforcement mechanism has been designed for clustered Ad-hoc networks with centralized supervision, the issue of appropriately selecting the parameters of a reputation scheme (initial value/ruin threshold, step value) is not different regardless of this scheme being distributed or centralized. Thus, the introduced random walk model for the reputation metric and the associated parameter selection technique can be applied to distributed reputation mechanisms for pure Ad-hoc networks, as well.

REFERENCES

[1] P. Obreiter, J. Nimis, "A Taxonomy of Incentive Patterns - the Design Space of Incentives for Cooperation", Technical Report Nr. 2003-9, May 21, 2003, http://www.ipd.uka.de/DIANE/en/index.html

[2] L. Buttyan, J.P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks", ACM/Kluwer Mobile Networks and Applications, Vol. 8, No. 5, October 2003

[3] N. Salem, L. Buttyan, J. P. Hubaux, M. Jakobsson, "A Charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular Networks", MobiHoc '03, June 1-3, 2003, Annapolis, Maryland, USA

[4] S. Zhong, J. Chen, and R. Yang, "Sprite: A Simple, Cheat-proof, Credit-based System for Mobile Ad-hoc Networks", In IEEE INFOCOM, San Francisco, USA, 2002. IEEE Press.

[5] S. Marti, et al., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Proc. ACM Int'l Conf. Mobile Computing & Networking, Mobicom 2000

[6] S. Bansal and M. Baker, "Observation-Based Cooperation Enforcement in Ad hoc Networks", Research Report cs.NI/0307012, Stanford University, 2003.

[7] P. Michiardi, R. Molva , "Analysis of Coalition Formation and Cooperation Strategies in Mobile Ad hoc Networks", Ad-hoc Networks Journal (Special Issue), Elsevier, 2003

[8] S. Buchegger, J. Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes - Fairness In Dynamic Ad-hoc NeTworks)", Proceedings of MobiHoc 2002, Lausanne, June 2002, pp. 226-236.

[9] S. Buchegger, J.Y. Le Boudec, "The effect of rumor spreading in reputation systems for mobile ad-hoc networks", In WiOpt'03: Modeling and Optimization in Mobile Ad Hoc and Wireless Networks (2003).

[10] H. Miranda and L. Rodrigues. "Preventing Selfishness in Open Mobile Ad Hoc Networks", .In Proceedings of the International Workshop on Mobile Distributed Computing (MDC), pages 440–445, Providence, Rhode Island USA, May 2003. IEEE. (Proceedings the 23rd International Conference on Distributed Computing Systems Workshops).

[11] K. Oikonomou et. al. "A Centralized Ad-Hoc Network Architecture (CANA) Based on Enhanced HiperLAN/2", 14th IEEE PIMRC 2003, Beijing, China, September 7-10, 2003.

[12] S. Vassilaras, D. Vogiatzis, T. Dimitriou, G. Yovanof, "Security Considerations for the Centralized Ad-Hoc Network Architecture", IEEE Int'l Workshop on Ad-Hoc Networks (IWWAN'04), Oulu, Finland, June 2004.

[13] R.G.Gallager, "Discrete Stochastic Processes", Kluwer Academic Publishers.

[14] W. Navidi, T. Camp, "Stationary Distributions for the Random Waypoint Mobility Model", *IEEE Transactions on Mobile Computing*, vol. 3, no. 1, pp. 99-108, January-March 2004