Performance Analysis of Reputation-based Mechanisms for Multi-hop Wireless Networks

Fabio Milan
Dipartimento di Elettronica
Politecnico di Torino
Turin, Italy
Email: fabio.milan@polito.it

Juan José Jaramillo and R. Srikant
Coordinated Science Laboratory
Dept. of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign
Email: {jjjarami, rsrikant}@uiuc.edu

***Abstract*— Reputation-based mechanisms can be used to sustain cooperation among selfish users in a multi-hop wireless network. In these mechanisms, every node listens to its relaying neighbors, and the misbehaving users are punished by dropping a fraction of their packets, according to a Tit-for-tat strategy. However, packet collisions prevent a node from recognizing a correct transmission, and this results in a distortion in the evaluated reputation. Thus, even if all the nodes cooperate correctly, a perceived defection may eventually lead to throughput loss due to retaliation. A possible way to mitigate this performance degradation is by adding a tolerance threshold to the pure Tit-for-tat strategy, so that a limited number of defections will not trigger any punishment. In this paper, we propose a simple network model to study the impact of collisions on a reputation-based mechanism. Our results show that in a large ring network with uniform random traffic, a simple reputation-based scheme with an optimal choice of tolerance can achieve cooperation for any sustainable load, if the value for a packet to a node is sufficiently high.**

I. Introduction

In a multi-hop wireless network, a packet has to traverse all the nodes in the path from source to destination. Hence, a successful transmission involves cooperation, since every node has to relay the packets generated by or directed to other nodes. If all the nodes are obedient, such as in military systems programmed to behave correctly by a central authority, then cooperation can be taken for granted. On the other hand, a selfish node aims to maximize its own utility with no regard for the overall system-wide outcome; roughly speaking, a selfish node does not want to waste its time, energy or bandwidth resources, and it may drop all the packets belonging to any other node but itself. In the worst case, assuming that every node is selfish, this behavior will eventually give zero throughput to everyone, thus leading to the so-called "Tragedy of the Commons" [1]. The solution to this problem is to provide selfish users with some incentives, in the form of reward for cooperation or punishment for defection.

Proposed incentive schemes belong to two classes: micro-payments, and reputation-based mechanisms. In micro-payment schemes, such as Terminodes [2] or Sprite [3], the nodes possess a certain amount of virtual credit, and if a node wants to send a packet, it has to pay all the nodes in the path that agree to cooperate. So, an uncooperative node will eventually run out of credit and will stop transmitting. The drawback is that a central authority has to manage the transactions and periodically redistribute the credits. Moreover, Terminodes needs a tamper-proof hardware to prevent the users from forging false credits.

In a reputation-based mechanism, such as SORI [4] or Catch [5], every node keeps track of the reputation of its neighbors, *i.e.*, the fraction of packets forwarded by them. When a node has to relay a packet on behalf of a neighbor, it will forward it with the same probability with which the neighbor forwards its packets, with a Tit-for-tat strategy. Compared to micro-payments, the main advantage of these mechanisms is that they do not require any central authority or special hardware. However, it may not be possible to correctly estimate the real reputation of a neighbor. The reason for this is that now every retransmission has two receivers: a forward receiver, *i.e.*, the packet's recipient; and a backward receiver that listens to the channel to check if the transmission effectively takes place. Traditional medium access protocols such as the CSMA/CA of IEEE 802.11 [6] guarantee the absence of collisions only at the forward receiver side, while the backward receiver still suffers from the so-called Hidden Terminal problem [7]. These collisions do not affect the transmission of a packet, but only its correct detection by the listener [8]. If a transmission is perceived as a defection, a cooperating node can be unjustly punished. With a Tit-for-tat strategy, packet collisions may trigger a retaliation process that eventually leads to zero throughput.

The rest of this paper is organized as follows. Section II explores the relation between the network capacity, the packet dropping probability of the nodes and the traffic load. Section III looks more closely at the interaction between two neighbors from a game-theoretic point of view, and proves that a Generous Tit-for-tat strategy can avoid throughput loss. Finally, Section IV concludes the paper.

II. Network Model

Following the early studies on multi-hop wireless networks [9], we consider a ring of N nodes, such that every node has two neighbors. The average traffic generation rate

This work was partially funded by the European Community under the EuroNGI Network of Excellence, by the Italian Ministry of Research under the Famous project, and by Motorola.

of the nodes is $\lambda \geq 0$. We assume that the traffic is uniformly distributed, *i.e.*, the destination of each packet is randomly chosen among the $N-1$ other nodes with probability $1/(N-1)$. The nodes can drop a packet to be forwarded with probability p. From now on, we will also assume that the number of nodes N is an odd number. This implies that for any pair of nodes, there is no ambiguity about which is the shortest path from source to destination. All the results will also hold when N is even, but sufficiently large.

A. Network Capacity Limits

Due to the shared nature of the wireless medium, the capacity of the network is limited. First, a node cannot transmit and receive at the same time. Second, a node cannot transmit while a neighbor is receiving. Moreover, existing MAC protocols, such as the CSMA/CA of IEEE 802.11, do not allow a node to transmit if a neighbor is also transmitting. Hence, in the case of a linear network, we can say that only one node out of three can transmit, *i.e.*, the maximum number of simultaneous transmissions that the network can sustain is $N/3$.

On the other hand, consider the amount of traffic the network is required to transport. The total traffic rate generated by N nodes is $N\lambda$. But a packet has also to go through a certain number of hops to reach its destination. Let H be the discrete random variable describing the number of hops that a packet has to go through. So, the average transmission rate requested to the network, measured in $packets \times hops \times sec^{-1}$, is $NE[H]\lambda$. Note that the average number of hops $E[H]$ depends on both the network size N and the dropping probability p, and we will evaluate it below.

As in Gupta-Kumar's result [10], the network can sustain a traffic λ if the average number of transmissions requested by the nodes in a time window of length T is not greater than the maximum number of simultaneous transmissions in the same time window, or more formally

$$NE[H]\lambda T \leq \frac{N}{3}T$$

Hence, it follows that the average traffic rate is upper-bounded by

$$\lambda \leq \frac{1}{3E[H]} \tag{1}$$

Let us now evaluate the expected number of hops traversed by a packet, considering separately the three cases $p = 1$, $p = 0$ and $0 < p < 1$. First, take $p = 1$, *i.e.*, each node always drops all the packets that transit through it. In this case, it immediately follows that for every value of N the expected number of hops traversed by a packet is one. Hence, when $p = 1$, Eq. (1) becomes

$$\lambda \leq \frac{1}{3}$$

Now consider the case $p = 0$, *i.e.*, each node always forwards all the packets that transit through it. In this case, if D is the discrete random variable describing the distance between source and destination, then the expected number of hops $E[H]$ is equal to the expected distance $E[D]$. Since D is uniformly distributed between 1 and $(N-1)/2$, the expected distance between two nodes is

$$E[D] = \frac{N+1}{4} = E[H]$$

Hence, when $p = 0$, Eq. (1) becomes

$$\lambda \leq \frac{4}{3(N+1)}$$

Finally, we consider the case $0 < p < 1$. To obtain $E[H]$ we condition on the distance D. First, since a packet can be dropped with probability p on its way from source to destination, we can write

$$P[H = h|D = d] = \begin{cases} p(1-p)^{h-1} & 1 \leq h \leq d-1 \\ (1-p)^{d-1} & h = d \\ 0 & \text{else} \end{cases}$$

So, we can calculate the conditional expectation of H given D as follows

$$\begin{aligned} E[H|D = d] &= \sum_{h=1}^{d} hP[H = h|D = d] \\ &= p\sum_{h=0}^{d-1} h(1-p)^{h-1} + d(1-p)^{d-1} \\ &= \frac{1-(1-p)^d}{p} \end{aligned}$$

Now, we can calculate the expected number of hops as

$$\begin{aligned} E[H] &= \sum_{d=1}^{\frac{N-1}{2}} E[H|D = d]P[D = d] \\ &= \frac{1}{p} - \frac{2}{(N-1)p}\sum_{d=1}^{\frac{N-1}{2}}(1-p)^d \\ &= \frac{1}{p} - \frac{2}{N-1}\frac{1-p-(1-p)^{\frac{N+1}{2}}}{p^2} \end{aligned}$$

So, when $0 < p < 1$ and N is sufficiently large, the expected number of hops tends to

$$\lim_{N\to\infty} E[H] = \frac{1}{p}$$

and Eq. (1) becomes

$$\lambda \leq \frac{p}{3} \tag{2}$$

Observe that as the number of nodes N tends to infinity, Eq. (2) holds for for every value of dropping probability $0 \leq p \leq 1$.

B. Transit Traffic

Since a node will not drop the packets it generates, but only those which transit through it, it is necessary to evaluate the rate of the transit traffic λ_T as a function of λ, N, and p. Again, we consider separately the three cases $p = 0$, $p = 1$ and $0 < p < 1$. First, take $p = 0$ and consider a node n. In this case, the number of possible destinations that every source can reach through node n depends on the distance between the source and n. Assuming shortest path routing, the maximum distance between any pair of nodes is

$$d_{max} = \frac{N-1}{2}$$

Then, it follows that two sources which are d_{max} hops away from n will never choose a path through n, except when n is the destination of their packet. Similarly, two sources which are $d_{max} - 1$ hops away from n will choose a path through n with probability $1/(N-1)$. In general, any two sources at distance d from node n will choose a path through n with probability $(d_{max} - d)/(N-1)$. Hence, when $p = 0$, the total traffic that transits through a node is

$$\begin{aligned} \lambda_T &= \frac{2\lambda}{N-1} \sum_{d=1}^{d_{max}-1} (d_{max} - d) \\ &= \frac{N-3}{4}\lambda \end{aligned}$$

Let us now take $p = 1$. In this case, the only transit traffic through node n is the traffic generated by its two neighbors, *i.e.*, those whose distance is one hop away from n. So, the above expression reduces to

$$\begin{aligned} \lambda_T &= \frac{2\lambda}{N-1}(d_{max} - 1) \\ &= \frac{N-3}{N-1}\lambda \end{aligned}$$

Finally, we consider the case $0 < p < 1$. Now, a packet coming from a source at distance d from n will not be dropped before n with probability $(1-p)^{d-1}$, since at least the first hop from the source to the first relay is guaranteed. So, in this case the transit traffic is

$$\begin{aligned} \lambda_T &= \frac{2\lambda}{N-1} \sum_{d=1}^{d_{max}-1} (d_{max} - d)(1-p)^{d-1} \\ &= \left[\frac{1}{p} - 2\frac{1-(1-p)^{\frac{N-1}{2}}}{(N-1)p^2} \right] \lambda \end{aligned}$$

So, when $0 < p < 1$ and N is sufficiently large, the transit traffic tends to

$$\lim_{N \to \infty} \lambda_T = \frac{\lambda}{p} \qquad (3)$$

Observe that as the number of nodes N tends to infinity, the above equation holds for every value of dropping probability $0 \leq p \leq 1$. Together with Eq. (2), this implies that the transit traffic is always bounded by

$$0 \leq \lambda_T \leq \frac{1}{3} \qquad (4)$$

In the next Section we will use Equations (3) and (4) in our game-theoretic model.

	F	D
F	$(\alpha-1,\, \alpha-1)$	$(-\alpha-1,\, \alpha)$
D	$(\alpha,\, -\alpha-1)$	$(-\alpha,\, -\alpha)$

TABLE I

PAYOFF MATRIX OF THE PACKET RELAYING GAME

	C	D
C	$(R,\, R)$	$(S,\, T)$
D	$(T,\, S)$	$(P,\, P)$

TABLE II

PAYOFF MATRIX OF THE PRISONER'S DILEMMA

III. GAME-THEORETIC MODEL

The interaction between two neighboring nodes can be modeled as the two-player strategic game defined in Table I. Every player can choose a strategy from the set $\{Forward,\, Drop\}$. Since relaying consumes nodes' time, bandwidth and energy resources, $Forward$ has a cost of -1, while $Drop$ has no cost. On the other hand, the gain for a forwarded packet is $\alpha > 0$, while the cost of a dropped packet is $-\alpha$. We define the value of a packet to be the difference between the gain from a forwarded packet and the loss from a dropped packet. Thus, the value of a packet is $\alpha - (-\alpha) = 2\alpha$.

A. A Prisoner's Dilemma?

The main characteristic of the Packet Relaying Game is that $Drop$ strictly dominates $Forward$, in the sense that no matter what the opponent does, each player is better off when choosing $Drop$. Since no player can profitably deviate from the strategy profile ($Drop$, $Drop$), this is the Nash Equilibrium in pure strategies. The Packet Relaying Game reminds us of the classic Prisoner's Dilemma [11], defined by the payoff matrix in Table II, together with the inequalities

$$T > R > P > S$$

$$R > \frac{T + S}{2}$$

Indeed, the Packet Relaying Game is equivalent to a Prisoner's Dilemma if and only if the cost of a dropped packet is greater than

$$\alpha > \frac{1}{2} \qquad (5)$$

This can be justified with the observation that the value of a packet 2α is greater than its mere transmission cost. As in the Prisoner's Dilemma, we also assume that the players have no way to communicate but by their strategies. This implies that two nodes cannot exchange any information about a common neighbor. Although proposed reputation-based mechanisms like SORI or Catch provide the exchange of control messages, this feature could produce collusion among nodes, and it is not included in our model.

Since in a data transfer session the number of packets involved is very high, it could seem straightforward to model a repeated interaction between two neighboring nodes as an Iterated Prisoner's Dilemma [11]. However, this is not feasible for two reasons. First, the interaction in the traditional Iterated Prisoner's Dilemma is essentially synchronous, while the burstiness of data traffic requires an asynchronous interaction. To capture this idea, we extend the set of pure strategies of the Packet Relaying Game to the set of all mixed strategies defined by the dropping probability p introduced in Section II. For practical purposes, we can imagine that each single stage of the game is played a sufficient number of times so that each player can establish a confident reputation about the opponent's dropping probability. However, note that since we are not really defining a repeated game, we do not need to introduce a discount parameter to aggregate the payoffs of every single stage.

The second difference is that in the Prisoner's Dilemma, after every stage of the game each player will know for sure which was the action taken by the opponent. Again, for the Packet Relaying Game this is not true. As explained in Section I, packet collisions may prevent a player from successfully hearing a packet being forwarded. This is equivalent to playing the Prisoner's Dilemma in a "noisy environment" [12]. Since each player ignores its opponent's real dropping probability, and essentially overestimates it, we introduce the notion of *perceived defection* rate.

To evaluate the perceived defection rate, consider the following example. Let 1 and 2 be a pair of nodes playing the Packet Relaying Game, and let 3 be the neighbor of 2 along the opposite direction of the ring. Node 2 perceives a defection if node 1 drops the packet with probability p, *or* if node 1 forwards the packet *and* there is a collision with another packet coming from node 3. A packet coming from node 3 can be either a packet generated by 3 itself at a rate λ, *or* a transit packet that 3 forwards with probability $1 - p$. Recalling the definition of transit traffic rate λ_T given in Section II, we can write

$$\hat{p} = p + (1-p)(\lambda + \lambda_T(1-p))$$

Note that the perceived defection rate of each player depends also on the dropping probability of a node involved in another game. To eliminate this externality, for Eq. (3) we can substitute λ with $p\lambda_T$. After some manipulation, the perceived defection rate can be rewritten as

$$\hat{p} = \lambda_T + (1-\lambda_T)p \tag{6}$$

For our simple model, it may be possible to estimate p from $\hat{p}$ and λ_T. However, this model is used to mainly illustrate the ideas behind reputation-based mechanisms. In practical situations, one would not be able to estimate p, therefore, in this paper we assume that nodes can only measure $\hat{p}$.

B. Strategies and Payoff

Tit-for-tat (TFT) is a simple strategy that achieves full cooperation in the Iterated Prisoner's Dilemma [11]. It can be defined as *"Cooperate on the first move, then do what the opponent did in the last move"*. If both players play TFT, the threat of a punishment prevents them from defecting first. For the equivalence of the Packet Relaying Game with the Prisoner's Dilemma, it is natural to study if TFT can be effective to achieve cooperation. But first, we need to extend the traditional definition to fit our game. For a Packet Relaying Game, we say that a player plays TFT if it sets its dropping probability equal to the perceived defection rate of the opponent, or

$$p = \hat{p} \tag{7}$$

To see how TFT behaves with a distorted reputation, it is sufficient to say that the solution of the system of equations (6) and (7) is simply $\hat{p} = p = 1$. To see how this outcome can be reached, let $p_i^{(k)}$ be the dropping probability of player i after iteration k. Then, we iteratively apply (6) and (7) for both players. If we assume without loss of generality that both players initially cooperate, we can write the following equations

$$\begin{aligned}
p_1^{(0)} = p_2^{(0)} &= 0 \\
p_2^{(1)} = p_2^{(1)} &= \lambda_T \\
p_1^{(2)} = p_2^{(2)} &= \lambda_T + (1-\lambda_T)\lambda_T \\
p_1^{(3)} = p_2^{(3)} &= \lambda_T + (1-\lambda_T)\lambda_T + (1-\lambda_T)^2\lambda_T \\
&\vdots \\
p_1^{(k)} = p_2^{(k)} &= \lambda_T \sum_{i=0}^{k-1} (1-\lambda_T)^i
\end{aligned}$$

Note that, in the above calculations, we have assumed that λ_T is independent of p. This assumption requires further justification which we leave for future work. As the number of iterations goes to infinity, we get

$$p_1 = p_2 = \lim_{k\to\infty} p_1^{(k)} = \lim_{k\to\infty} p_2^{(k)} = 1$$

This shows that if both players use TFT, then the punishment of perceived defections will trigger a reciprocal retaliation, and the outcome of the game will be the point in which every packet is dropped, even if both players were willing to cooperate.

A simple way to mitigate this severe throughput loss is to introduce a tolerance threshold δ in the Tit-for-tat punishment scheme. We define the space of Generous Tit-for-tat (GTFT) [13] strategies, as the set of all functions of the form

$$p = \max\{\hat{p} - \delta, 0\} \tag{8}$$

where $0 \leq \delta \leq 1$. Note that if $\delta = 0$, GTFT reduces to TFT, while $\delta = 1$ corresponds to the strategy $Always\ Forward$. From now on, we will refer to a tolerance δ as a particular strategy in the GTFT space.

Before showing that among the GTFT strategies there exists one which achieves full cooperation, we need to complete the definition of the Packet Relaying Game with a payoff associated to each strategy profile. A natural way to build a payoff function is to take the average perceived utility $E(\hat{U}_i)$. For example, the payoff of player 1 is

$$\begin{aligned} E(\hat{U}_1) &= (1-p_1)\left[(\alpha-1)(1-\hat{p}_2)-(1+\alpha)\hat{p}_2\right] \\ &\quad + p_1\left[\alpha(1-\hat{p}_2)-\alpha\hat{p}_2\right] \\ &= p_1 - 2\alpha\hat{p}_2 + \alpha - 1 \end{aligned}$$

Since every player aims to maximize its own payoff, this expression can be further simplified by eliminating the constant term $\alpha - 1$,

$$E(\hat{U}_1) = p_1 - 2\alpha\hat{p}_2 \qquad (9)$$

and similarly for player 2. Note that the payoff of each player is increasing with its dropping probability, and decreasing with the perceived defection rate. Moreover, since for Eq. (5) $\alpha > 1/2$, a perceived loss is weighted more than the gain of dropping a packet. For example, the perceived payoff of mutual cooperation is

$$E(\hat{U}_1) = -2\alpha\lambda_T$$

C. Nash Equilibrium

Once the definition of the game is complete, we want to find a strategy that is a Nash Equilibrium and possibly performs better than simple TFT. We restrict our search to the set of symmetric equilibria. Then, for any value of tolerance δ and transit traffic λ_T, we may be interested in finding which dropping probability p and perceived defection $\hat{p}$ will result. By solving the system of equations (6) and (8) for $\delta < \hat{p}$ and $\delta \geq \hat{p}$, we can write the solution in the form

$$p = \begin{cases} 0 & \text{if } \delta \geq \lambda_T \\ 1 - \frac{\delta}{\lambda_T} & \text{else} \end{cases}$$

$$\hat{p} = \begin{cases} \lambda_T & \text{if } \delta \geq \lambda_T \\ 1 - \frac{1-\lambda_T}{\lambda_T}\delta & \text{else} \end{cases}$$

Since when $\delta = \lambda_T$ the dropping probability is zero and the perceived defection rate is minimized, this strategy profile is a natural candidate for the Nash Equilibrium we are looking for. To prove it, we have to show that no player has an incentive to unilaterally deviate from it. First, observe that if for example player 1 deviates by setting a tolerance $\delta > \lambda_T$, this will not affect the outcome of the game. Therefore, such a deviation does not increase its payoff. Then, assume that player 1 tries to deviate by setting a tolerance $\delta < \lambda_T$. To find the values of p_1 and $\hat{p}_2$ consistent with the strategy profile $(\delta,\ \lambda_T)$, we again apply Eq. (6) and Eq. (8), iteratively

$$\begin{aligned} p_1^{(0)} &= p_2^{(0)} = 0 \\ \hat{p}_1^{(0)} &= \hat{p}_2^{(0)} = \lambda_T \\ p_1^{(1)} &= \lambda_T - \delta \\ \hat{p}_1^{(1)} &= \lambda_T + (1-\lambda_T)(\lambda_T - \delta) \\ p_2^{(1)} &= (1-\lambda_T)(\lambda_T-\delta) \\ \hat{p}_2^{(1)} &= \lambda_T + (1-\lambda_T)^2(\lambda_T-\delta) \\ p_1^{(2)} &= (\lambda_T-\delta)(1+(1-\lambda_T)^2) \\ &\vdots \\ \hat{p}_2^{(k)} &= \lambda_T + (\lambda_T-\delta)\sum_{i=1}^{k}(1-\lambda_T)^{2i} \\ p_1^{(k)} &= (\lambda_T-\delta)\sum_{i=0}^{k-1}(1-\lambda_T)^{2i} \\ \hat{p}_2 &= \lim_{k\to\infty}\hat{p}_2^{(k)} = \lambda_T + \frac{\lambda_T-\delta}{\lambda_T(2-\lambda_T)}(1-\lambda_T)^2 \\ p_1 &= \lim_{k\to\infty} p_1^{(k)} = \frac{\lambda_T-\delta}{\lambda_T(2-\lambda_T)} \end{aligned}$$

By plugging these values into the payoff of player 1 as defined by Eq. (9), we get

$$E(\hat{U}_1) = \frac{(\lambda_T-\delta)(1-2\alpha(1-\lambda_T)^2)}{\lambda_T(2-\lambda_T)} - 2\alpha\lambda_T$$

Hence, player 1 will not increase its payoff by deviating from λ_T if this value is not greater than $-2\alpha\lambda_T$, *i.e.*, if and only if

$$1 - 2\alpha(1-\lambda_T)^2 \leq 0$$

By solving for λ_T, we obtain an upper bound over the transit traffic as a function of the packet value 2α,

$$\lambda_T \leq 1 - \frac{1}{\sqrt{2\alpha}} \qquad (10)$$

This means that if the transit traffic grows beyond this critical threshold, the threat of punishment will not be sufficient to sustain cooperation. The effect is dramatic, for both players will have an incentive to reduce their tolerances, and the Nash Equilibrium will result in mutual defection. On the other hand, since for Eq. (4) the transit traffic is upper-bounded by the network capacity, it is not necessary to have an infinite packet value to achieve cooperation for any feasible load. In this case, since the network capacity is $1/3$, if the packet value is

$$2\alpha \geq \frac{9}{4}$$

then the Nash Equilibrium of the game achieves cooperation for any feasible load.

IV. Conclusion

In this paper, we have proposed a simple model for the optimization and the performance analysis of reputation-based mechanisms for multi-hop wireless networks. The main result is that, for a large ring network with uniform traffic, there exists a Generous Tit-for-tat strategy achieving full cooperation, even in presence of packet collisions. In particular, we showed that if the packet value is finite but sufficiently large, then setting a tolerance threshold equal to the transit traffic is a Nash Equilibrium for the two-player Packet Relaying Game under any feasible load. This guarantees that a network of selfish nodes has the same throughput as that a cooperative network. A straightforward generalization of this work could be exploring how the number of neighbors can affect the results. Despite its limitations, we believe that our approach provides an insight into the issues of reputation-based mechanism design. Probably, the most interesting conclusion is that the efficiency of a reputation-based scheme depends on the value that sources place on their packets. For example, a multimedia streaming source, tolerant to packet losses, can be modeled by a low value of α, although an exact quantification of this parameter is beyond the scope of this work.

References

[1] G. Hardin, "The Tragedy of the Commons," *Science*, vol. 162, no. 3859, pp. 1243–1248, Dec. 13 1968.

[2] 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*, vol. 39, no. 6, pp. 166–174, June 2001.

[3] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks," in *Proc. of IEEE Infocom 2003*, San Francisco, CA, USA, April 2003, pp. 1987–1997.

[4] Q. He, D. Wu and P. Khosla, "SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks," in *Proc. of IEEE Wireless Communications and Networking Conference (WCNC2004)*, Atlanta, GA, USA, March 2004, pp. 825–830.

[5] R. Mahajan, M. Rodrig, D. Wetherall, and J. Zahorjan, "Sustaining Cooperation in Multi-Hop Wireless Networks," in *Proc. second USENIX Symposium on Networked System Design and Implementation (NSDI 05)*, Boston, MA, USA, May 2005.

[6] ISO/IEC and IEEE Draft International Standards, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," ISO/IEC 8802-11, IEEE P802.11/ D10, Jan. 1999.

[7] F. A. Tobagi and L. Kleinrock, "Packet Switching in Radio Channels: Part II – The Hidden Terminal Problem in Carrier Sense Multiple-Access and the Busy-Tone Solution," *IEEE Transactions on Communications*, vol. COM-23, no. 12, pp. 1417-1433, 1975.

[8] S. Marti, T.J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," in *Proc. of 6th Annual International Conference on Mobile Computing and Networking (MobiCom 2000)*, Boston, MA, USA, August 2000.

[9] J. A. Silvester and L. Kleinrock, "On the Capacity of Multihop Slotted ALOHA Networks with Regular Structure," *IEEE Transactions on Communications*, vol. COM-31, no. 8, pp. 974–982, 1983.

[10] P. Gupta and P. R. Kumar, "The Capacity of Wireless Networks," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 388–404, 2000.

[11] R. Axelrod, "The Emergence of Cooperation among Egoists," *The American Political Science Review*, vol. 75, no. 2, pp. 306–318, June 1981.

[12] J. Wu and R. Axelrod, "How to Cope with Noise in the Iterated Prisoner's Dilemma," *The Journal of Conflict Resolution*, vol. 39, no. 1, pp. 183–189, March 1995.

[13] V. Srinivasan, P. Nuggehalli, C.F. Chiasserini and R.R. Rao, "Cooperation in Wireless Ad Hoc networks," in *Proc. of IEEE Infocom 2003*, San Francisco, CA, USA, March 2003.