MIMODog: How to solve the problem of selfish misbehavior detection mechanism in MANETs using MIMO Technology

Abderrezak Rachedi, Hakim Badis

▶ **To cite this version:**

Abderrezak Rachedi, Hakim Badis. MIMODog: How to solve the problem of selfish misbehavior detection mechanism in MANETs using MIMO Technology. IWCMC'2012, Aug 2012, Limassol, Cyprus. pp.333-337, 10.1109/IWCMC.2012.6314226 . hal-00687192

HAL Id: hal-00687192
https://hal.science/hal-00687192

Submitted on 19 Sep 2012

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

MIMODog: How to solve the problem of Selfish Misbehavior Detection Mechanism in MANETs Using MIMO Technology

Abderrezak Rachedi and Hakim Badis
Université Paris-Est Marne-la-Vallée (UPEMLV)
Gaspard Monge Computer Science Laboratory (UMR 8049 LIGM)
Champs sur Marne, France
Email: {rachedi, badis} @univ-mlv.fr

***Abstract*—Mobile Ad-hoc Networks (MANETs) are based on a fundamental aspect, which is the cooperative parameter. This parameter may compromise the networks. The selfish misbehaving nodes can seriously affect the network performance. Moreover, the existing mechanisms based on the monitoring process to detect the misbehaving nodes are not efficient and suffer from an important false alarm rate. These weaknesses are mainly due to the interferences and the costs of the monitoring process. In MANET based on $SISO$ (Single-Input Single-Output) technology, the interferences at the monitor node compromise the observation and the accuracy of the cooperation report. That is why in this paper, we focus on the MIMO (Multi-Input and Multi-Output) technology to overcome these drawbacks and to significantly improve the monitoring process. We propose a new MAC protocol called MIMODog-SPACE-MAC based on the well-known SPACE-MAC protocol. It allows the monitor node to avoid the collision during the monitoring process by adjusting the antennas weights in order to nullify the signal coming from other nodes than the monitored one. Therefore, the proposed solution contributes to significantly enhance the accuracy of the monitoring process. We show that for a MIMO network with randomly located nodes n, each equipped with M antennas, the achievable number of monitor nodes is $\Theta(\frac{M}{\sqrt{n \ln n}})$. Indeed, theoretical results show that by using MIMODog-SPACE-MAC, the network can have a constant improvement M on an asymptotic number of monitor nodes compared to SISO 802.11 DCF MAC.**

***Index Terms*—MANET, SPACE-MAC, MIMO, Selfish misbehaviors, Monitoring process**

I. Introduction

Mobile Ad hoc Networks (MANETs) are a set of nodes based on the cooperation aspect to form and manage a network without any infrastructure. The nodes in MANETs act as router and terminal at the same time and the lack of cooperation between them implies the absence of any network. That is why it is important to deal with the non cooperative or selfish nodes problem. The problem of selfish nodes is that they keep their energy to transmit and route their own packets. In other words, the selfish nodes refuse to route and forward the packets of other nodes. The question is why do nodes act as selfish and ignore the cooperation aspect? To answer this question, we investigate the motivation of nodes to adopt this misbehavior. First of all, the resources in MANETs are limited in terms of energy, bandwidth, etc. Then, the nodes try to increase their lifetime duration by reducing their energy consumption and the cost of the transmission operation is important in terms of energy. Secondly, when the nodes route and forward the packets of other nodes, this increases the delay of their own packets transmission and reduces their own average throughput. Thus, this operation may be perceived by nodes as punishment and not as global network interest. In order to deal with this problem, many researchers focus on the monitoring mechanisms in order to detect the selfish nodes and to punish them [1], [2], [3], [4]. However, all the proposed mechanisms are based on the classical SISO (Single-Input Single-Output) technology to monitor the communication channel and to detect the non forwarding nodes (selfish behavior). The most cited mechanism is Watchdog. Many proposed solutions are based on it, but it suffers from the high false alarm rate [1]. The main problem of these mechanisms is related to the interference at the monitor node which makes the results of its observations wrong.

That is why we propose a new MAC protocol called MIMODog-SPACE-MAC based on MIMO (Multi-Input Multi-Output) technology, particularly a SPACE-MAC protocol to significantly cancel the potential interferences at the monitor nodes and to enhance the accuracy of the monitoring results. Our contributions are summarized as follows:

- The monitoring problem persists in MANETs, even when we use MIMO technology,
- A new MIMO MAC protocol is proposed to cancel the interferences at the monitor nodes without affecting the total network capacity,
- A different impact on the monitoring process with: DCF MAC, SPACE-MAC and MIMODog-SPACE-MAC is presented and discussed. MIMODog-SPACE-MAC significantly enhances the monitoring process without affecting the network capacity.
- MIMODog network modelling is done and lower and upper bounds of the number of monitor nodes are investigated. Moreover, the obtained numerical results illustrate that the proposed solution overcomes the drawbacks of

classical monitoring mechanisms.

This paper is organised as follows: an overview of cooperation models based on monitoring mechanisms and the SPACE-MAC protocol are given in in section II. Section III illustrates the DCF and SPACE-MAC protocols vulnerabilities in the monitoring process. A new MAC protocol adapted to the monitoring process with more details on its design and its implementation is proposed in section V. Moreover, we present the theoretical model in order to assess the asymptotic bound related to the monitor nodes number. The numerical results are given and analysed. The final section concludes the paper and presents the future works.

II. Related Work

In this section, we present the existing works related to cooperation models in MANETs and the SPACE-MAC protocol.

A. Cooperation Models

Two types of uncooperative nodes can be distinguished: malicious nodes and selfish nodes. The malicious nodes try to attack the system by selecting an uncooperative behaviour and create a disconnection in the network. However, the aim of selfish nodes is to maximize their benefits in terms of QoS (like throughput and delay) and minimize their costs like the energy consumption. In this paper, we focus on the selfish behaviour of the potential cooperative nodes. Cooperation is an important parameter in wireless networks, because without any packet forwarding, the ad hoc network cannot exist and the wireless coverage extension cannot be possible. The concept of cooperative communication (CC) technique in wireless networks was introduced in [5].

In literature, two main solutions were proposed to overcome the problem of selfish nodes. The first one is based on the reputation mechanisms which consist in assessing a node's contribution like forwarding and routing functionalities [4], [1], [6], [7]. The reputation model called CONFIDANT is proposed to share the reputation metric and alarms messages in order to detect and punish the misbehaving nodes [6]. Another model called CORE is proposed to implement the reputation function by using the monitoring technique. Each node computes the reputation value for every neighbour and refuses to provide services to misbehaving nodes when their reputation is lower than a certain threshold . However, all these solutions are based on the classical monitoring mechanism like Watchdog[4]. Consequently, they did not consider the problems of the false observation related to the collision and the performance of the potential relayed nodes.

B. SPACE-MAC protocol: Spatial Reuse Using MIMO Channel-Aware MAC

The SPACE-MAC is a Media Access Control protocol for networks with smart antennas which uses antenna weights to schedule simultaneous transmissions on a single collision domain. Antenna weights are exchanged via control packets (RTS and CTS) [8].

The main contribution of SPACE-MAC work is the fully distributed MAC protocol that exploits the physical layer characteristics and cross-layer techniques to enable spatial reuse in scatter-rich multi-path environments. The main advantage of SPACE-PAC is that it allows multiple data streams at the same time in the same collision area, thereby increasing the overall capacity of the network. The channel control overhead introduced by channel estimation and beam coordination is minimal and effectively countered by the gain provided by the increase in the capacity of the MIMO channels.

In SPACE-MAC, the first station that gains access to the channel determines the silence period. All other stations must remain idle following their transmission until the silence period is completed. In SPACE-MAC, the silence period is required because any station currently involved in the transmission is unaware of any other transmission that began during its data packet or acknowledgement packet transmission phase. Additionally, any station that wishes to transmit must not interfere with this ongoing transmission and must not transmit if it cannot complete its entire packet exchange sequence before the end of the silence period.

Based on the RTS/CTS of the existing transmission and for each new communication in the same geographical vicinity, the new sender/receiver nodes will select their weights so that the signal from any existing communication node is nullified. This problem can be formulated as a quadratic optimization and reduced to an unconstrained optimization problem using the null space method which in turn is an eigenvalue problem. Any new additional transmission is only possible if both nodes of a same pair have enough degrees of freedom. For an M antenna system it can null out at most $M-1$ stations depending on the environment. M is also known as the Degrees of Freedom (DOF). Every time a node nulls out another node, it consumes a DOF.

III. MAC protocols vulnerabilities in monitoring process

A. Case of 802.11 DCF MAC

The monitoring process acts on the different network protocol layers (MAC, Routing, ...). In this work, we focus on the network layer for the monitoring. The monitor node supervises the packet forwarding activities of its neighbor nodes and their packet integrity. Let us consider a small network illustrated in Figure 1.

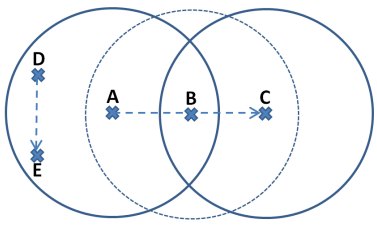

Fig. 1. An ad hoc network scenario

Two simultaneous communications are possible: B-C and D-E. Node A acts as monitor and supervises the packet forwarding activities of node B. When a node B forwards A's packets to node C, the communication between D and E can create a collision at node A and then directly impact the monitoring process. Figure 2 depicts the monitoring problem based on 802.11 DCF MAC.

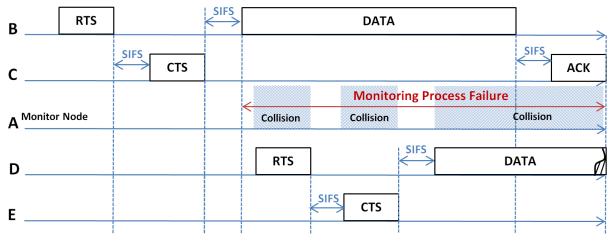

Fig. 2. Monitoring problem based on 802.11 DCF MAC protocol

B. Case of SPACE-MAC

In this section, we will show that the monitor nodes cannot recover collided packets using the standard SPACE-MAC protocol. Let us consider the last network (Figure 1). We assume that all nodes are silent at the beginning, i.e., there is no on-going communication and each node has 4 antennas. Node B wants to forward A's packets to C and D wants to communicate with E. Node B transmits a RTS using the default weight vector, $[1\ 1\ 1\ 1]/\sqrt{4}$, or a random vector. The vector is normalized to have an equal signal power regardless of the number of antennas. The weight vector used to transmit the RTS will be used to transmit the following data packet and to receive the corresponding CTS and ACK. Once node C receives the RTS, it responds with a CTS packet using the current weight vector. The weight vector used to transmit the CTS will be used to receive the following data packet and to send an ACK. The receiver estimates the SIMO (Single-Input Multi-Output) channel vector $h_{BC} = w_B^H H_{BC}$, where w_B is weight vector of node B and H_{BC} is $M \times M$ MIMO channel matrix with elements h_{ij} and the superscript H denotes hermitian operation. In fact, as there is no ongoing communication, nodes C (receiver) and A (monitor) can switch their weight vectors to $w_C = h_{BC}^t$ and $w_A = h_{BA}^t$ which maximize the combined channel and array gain. When a node other than the designated receiver and the neighbor monitor receives the RTS, say node K, it estimates the effective channel H and adjusts the weight vector so that the signal from the RTS sender is nullified (i.e., $h_{BK}C_K = 0$) for the duration of time specified in the RTS duration field. When a node other than the sender of the RTS (B) receives the CTS, say node L, it estimates the effective channel and stores the weight vector for the duration specified in the CTS duration field. After the RTS/CTS handshaking, node B sends, C receives and A supervises a data frame using respectively the weight vectors w_B, w_C and w_A chosen as described above.

Now let us say node D wants to initiate a transmission toward E. Since node D is not currently aware of the antenna weight used by node B (node D cannot overhear B's RTS and C's CTS), it cannot adjust its weight vectors meeting these conditions: $w_D^H H_{DA} w_A = 0$ (D's signals cannot be nullified by A). Consequently a collision will occur at node A. The example shown in Figure 3 describes such a process problem.

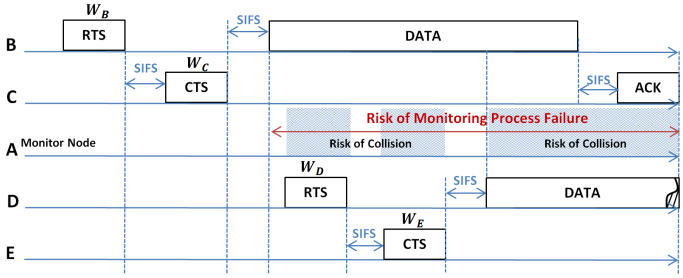

Fig. 3. Monitoring problem based on SPACE-MAC protocol

IV. MIMODOG-SPACE-MAC PROTOCOL

In order to avoid the interferences at the monitor node, each new transmitting nodes must be aware not only about the the weight vectors of the existing transmissions in the cover area, but also about the weight vectors used by the monitor nodes. To deal with this issue, we propose a new MIMO MAC protocol called MIMODOG-SPACE-MAC. The basic idea is that the monitor nodes simulate a real reception by sending CTS packet control before starting their monitoring process. We use the previous example to illustrate our MIMO MAC protocol functioning.

A. Basic protocol operation

When monitor node A hears a RTS packet from its forwarding node B:

1) it estimates the SIMO channel vector $h_{BA} = w_B^H H_{BA}$ and switches its weight vector to $w_A = h_{BA}^t$ to well receive B's packets for monitoring;
2) it sends a CTS packet after a SIFS time using a weight vector $\hat{w}_A$ meeting this condition: $\hat{w}_A^H H_{AB} w_B = 0$ (the A's CTS signal is nullified at B to avoid collisions with C's CTS and to assure that node B will not change its behaviour if it is malicious). The A's CTS contains the weight vector w_A and transmitted using $\hat{w}_A$. The goal of this operation is to make all the future transmitters in the neighborhood believe that node A will receive packets and that its weight vector w_A should be considered.

On reception of the CTS packet from A, each node should estimate the effective channel from A. Now, the transmission of D should ensure that the reception of A is not disturbed. So, it picks W_D meeting $w_D^H H_{DA} w_A = 0$ before transmitting its RTS.

The process is graphically explained in Figure 4.

B. RTS/CTS Control Packet Format

In order to selectively tune in or tune out a particular transmission, the stations have to be aware of the antenna weights that are in use by transmitting stations. This requires

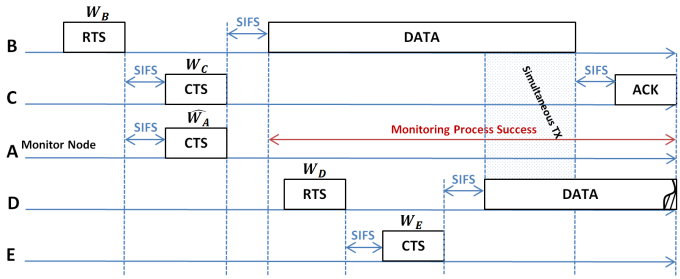

Fig. 4. Monitoring mechanism with MiMoDog-SPACE-MAC

a mechanism to convey the antenna weights to all neighboring stations. MIMODog-SPACE-MAC uses RTS and CTS control packets to convey antenna weights. The proposed format for RTS and CTS control packets is shown in Figure 5. A separate s byte field is inserted in the payload of the RTS and CTS packets that stores M antenna element weights currently in use. A linear function f is used to obtain the value of s. For example, as each antenna weight can be a complex number, we can store them as a pair of real numbers occupying 4 bytes (per one complex number) and so $f(M) = 4M$. RTS and CTS packets are also used to perform channel estimation using pilot symbols embedded in the physical (PHY) preamble.

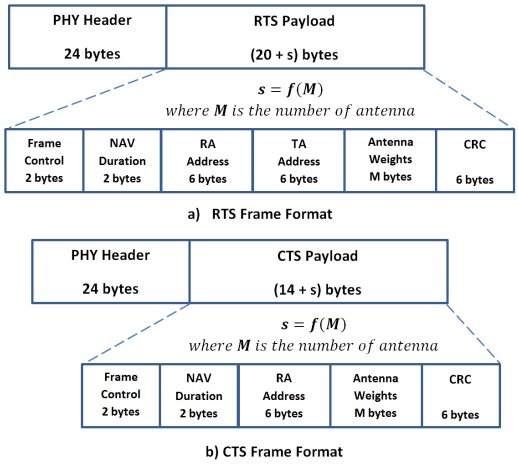

Fig. 5. Access Control Packets

V. MIMODog Network Modeling

In this section, we present a model for MIMODog ad hoc networks which we will use in our bound analysis of the number of monitor nodes. The used model captures MIMO's spatial multiplexing and interference cancellation capabilities at the physical layer.

We consider a random multi-hop MIMO ad hoc network with n nodes, where each node, equipped with M antennas, is randomly located in a unit square area. Each node acts as a source node and transmits data to a randomly chosen destination node. The per-node throughput $\lambda(n)$ is defined as the minimum data rate that can be sent from each source to its destination via multi-hop routing. The maximum data rate that a single data stream can support is W. We assume that a node's transmitter is limited to a transmission range $r(n)$. When a source node cannot transmit data to its destination node in one hop, multi-hop routing is needed to relay the data. Each node also has an interference range $(1+\Delta)r(n)$, where Δ is non negative-constant.

A. Lower bound of the number of monitor nodes

In [9], Gupta and Kumar showed that a capacity lower bound for a single-antenna ad hoc network is $\Omega(\frac{W}{\sqrt{n \ln n}})$ by constructing a feasible routing and scheduling scheme. Thus, by adopting the same routing and scheduling scheme in our MIMODodog ad hoc networks as in [9], a number of monitor nodes lower bound of $\Omega(\frac{M}{\sqrt{n \ln n}})$ can be obtained.

B. Upper bound of the number of monitor nodes

As shown in [10], we partition the unit square of the network into small squares, with the size of each small square being cleverly chosen so that the maximum data rate that can be received by the nodes inside the small square can be accurately computed. This method allows to estimate the number of monitor nodes.

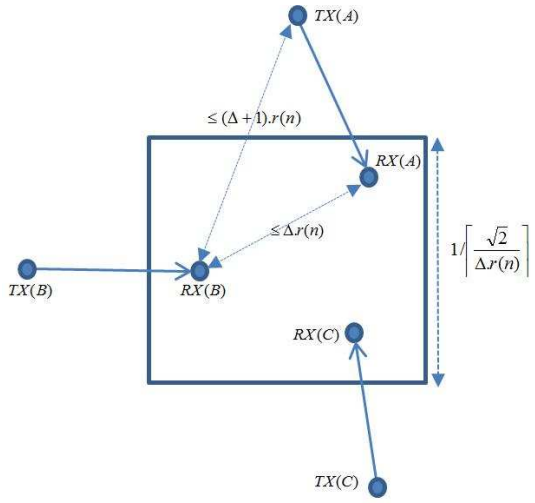

Fig. 6. The receivers in a square with side length

Lemma 1. *For a square with a side length* $1/\lceil \frac{\sqrt{2}}{\Delta.r(n)} \rceil$*, there are at most* $M-1$ *times larger monitor nodes based on MIMODog-SPACE-MAC than with SISO 802.11 DCF MAC.*

Proof: Based on [10], for a square with a side length $1/\lceil \frac{\sqrt{2}}{\Delta.r(n)} \rceil$ (as shown in Figure 6), the maximum number of total data streams that can be received by the nodes inside the square at any time slot for any routing scheme is not greater than M regardless of the number of receiving nodes inside the square. Using our MIMODog-SPACE-MAC, the presence of a monitor node in the square area consumes exactly one DOF. Let $P_j(t,i)$ be the probability that node i is a monitor at time t in a square j. The number of monitor nodes in square j is given by $\sum_{i=1}^{n} P_j(t,i)$. Consequently, the new maximum number of

total data streams that can be received by nodes inside a square j is not greater than $M - \sum_{i=1}^{n} P_j(t,i)$ ($M \geq \sum_{i=1}^{n} P_j(t,i)$).

In the same square and using SISO systems, the maximum number of total data streams that can be received by nodes inside the square is 1. Only one monitor node can be functioning properly. So, there are at most $M-1$ times fewer monitor nodes with SISO 802.11 DCF than with MIMODog-SPACE-MAC. ■

Based on Lemma 1, we can now compute the maximum number of monitor nodes that can be supported in the unit square network by taking the sum of the number of monitor nodes among all small squares.

Theorem 1. *For a random multi-hop MIMO ad hoc network, a number of monitor nodes upper bound for all possible routing and scheduling schemes is* $O(\frac{M}{\sqrt{n \ln n}})$ *with a high probability when* $n \to \infty$.

Proof: The proof is similar to the proof of Theorem 1 in [10]. We can easily obtain this equation:

$$\textbf{NMN} \leq \frac{2M\sqrt{\pi}}{\Delta^2 D\sqrt{n \ln n}} + \frac{2\sqrt{2}M}{\Delta D n} + \frac{M\sqrt{\ln n})}{Dn\sqrt{\pi n}} = O(\frac{M}{\sqrt{n \ln n}}), \quad (1)$$

where NMN is the number of monitor nodes and D is the average length of source-destination lines. ■

Combining the lower and upper bounds of the number of monitor nodes, we can see that the number of monitor nodes in a random multi-hop MIMO ad hoc network with n nodes is $\Theta(\frac{M}{\sqrt{n \ln n}})$.

C. Numerical results

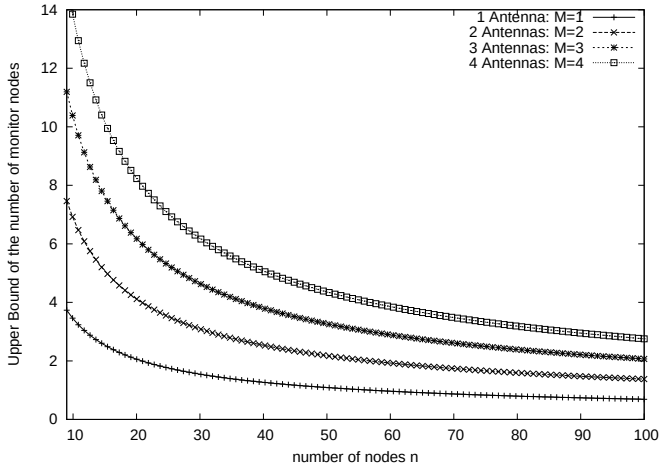

Fig. 7. The upper bounds of the number of the monitor nodes versus the number of nodes

By running 1000 instances, we obtain the average length of source-destination lines $D = 0.52$ (see [10]). We set $\Delta = 1$. Using equation 1 and under different values of $M = 1, 2, 3, 4$ we obtain the results shown in figure 7. With $M = 1$ antenna, MIMODog-SPACE-MAC is exactly the 802.11 DCF MAC. We can extract 2 elements :

- when the number of used antennas increases, the number of monitor nodes increases,
- when the number of nodes increases, the upper bound of monitor nodes decreases. This is explained by the fact that the network is more and more dense with a high multi-hop connectivity and so MIMO interference cancellation is limited.

VI. Conclusion

In this paper, we propose a new scheme for exploiting adaptive antenna arrays in wireless communications in a multi-party propagation channel to efficiently detect the selfish nodes. The proposed scheme nullifies the beam to competing nodes to enable concurrent transmissions and monitor in the same collision domain. A distributed MAC protocol called MIMODog-SPACE-MAC, that supports the exchange of channel state and antenna information is described.

A different impact on the monitoring process with: DCF MAC, SPACE-MAC and MIMODog-SPACE-MAC is presented and discussed. Moreover, we have studied the number of monitor nodes scaling laws for MIMO ad hoc networks with M antennas. We have shown that the number of monitor nodes is at most $M-1$ times larger based on MIMODog-SPACE-MAC than with SISO 802.11 DCF MAC.

In our future works, we plan to evaluate the proposed solution by extensive simulations with different parameters like density of selfish nodes, mobility models, traffic models, etc.

References

[1] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misebehaviour in mobile ad-hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking (MobiCom'00)*, 2000.

[2] A. Rachedi and A. Benslimane, "Toward a cross-layer monitoring process for mobile ad hoc networks," *Security and Communication Networks*, vol. 2, no. 4, pp. 351–368, 2009.

[3] ——, "Cross-layer approach to improve the monitoring process for mobile ad hoc networks based on ieee 802.11," in *IEEE Global Telecommunications Conference (IEEE GLOBECOM 2007), Washington, DC, USA,*, 2007.

[4] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security*, 2002, pp. 107– 121.

[5] A. Nosratinia, T. Hunter, and A. Hedayat, "Cooperative coomunication in wireless networks," *IEEE Communications Letters*, vol. 42, no. 10, pp. 74 – 80, 2004.

[6] S. Buchegger and J. Le Boudec, "Performance analysis of the cofidant protocol," in *Proceedings of 3rd ACM international Symposium on Mobile ad hoc networking & computing*, 2002, pp. 226– 236.

[7] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," in *CoRR*, 2003.

[8] J. S. Park and G. M. L. H. Alok, N., "Space-mac: Enabling spatial reuse using mimo channel-aware mac," in *Proceedings of International Conference Communications (ICC)*, 2005.

[9] P. Gupta and P. Kumar, "The capacity of wireless networks," *In IEEE Transactions in Information Theory*, vol. 46, no. 2, pp. 388 – 404, 2000.

[10] K. Y. Canming Jiang, H.S.Y. and S. Bradley, "On the asymptotic capacity of multi-hop mimo ad hoc networks," *In IEEE Transactions in Wireless Communications*, vol. 10, no. 4, pp. 1032 – 1037, 2011.