How MIMO cross-layer design enables QoS while detecting non-cooperative nodes in wireless multi-hop networks

Abderrezak Rachedi, Hakim Badis, Abderrahim Benslimane

How MIMO cross-layer design enables QoS while detecting non-cooperative nodes in wireless multi-hop networks

Abderrezak Rachedi[a,*], Hakim Badis[a], Abderrahim Benslimane[b]

[a] *University Paris-Est (UPEM), Gaspard Monge Computer Science Laboratory (LIGM-UMR 8049), 77454 Marne-la-Vallée, France*
[b] *University of Avignon, Computer Science Laboratory of Avignon (LIA), 84911 Avignon cedex 9, France*

Abstract

Wireless Multi-hop Networks (WMNs) are based on the cooperation between nodes. The non-cooperative (selfish) nodes can affect the quality of services (QoS) delivered by the network. The solutions proposed in literature are based on the monitoring mechanism to detect non-cooperative nodes. However, the monitoring mechanism has to tackle a significant false alarm rate. The origin of these issues is mainly related to the interferences and the costs of the monitoring mechanism. In WMNs based on Single-Input Single-Output (SISO) technology, the interferences at the monitor (detector) node can affect the assessment and the accuracy of the monitor node's observation. In this paper, we use Multi-Input and Multi-Output (MIMO) technology to tackle these drawbacks and to perform the monitoring mechanism without affecting the QoS. We propose a new MAC protocol based on the well-known SPACE-MAC protocol, named MIMODog. The collision at the monitor node can be avoided by tuning the antennas' weights. Therefore, the signal coming from other nodes than the monitored one can be nullified. Thus, this solution allows an important improvement of the accuracy of the monitor node's observation. Moreover, we propose a monitoring capacity analysis using graph theory particularly Conflict Graph (CG), and asymptotic study. We illustrate that the capacity consumed in the case of MIMODog is costly compared to SPACE-MAC, but the accuracy of the observation is better. We demonstrate that the number of monitor nodes is $\Theta(\frac{M}{\sqrt{n \ln n}})$ for a MIMO network with randomly located nodes n, each equipped with M antennas. Indeed, numerical results illustrate that by using MIMODog, the network can have a constant improvement M on an asymptotic number of monitor nodes compared to SISO 802.11 DCF MAC.

Keywords: Multi-hop wireless networks, Non-cooperative nodes, MIMO, Monitoring mechanism, Conflict Graph, QoS.

1. Introduction

Wireless Multi-hop Networks (WMNs) are a set of nodes based on the cooperation aspect to form and manage a network. The nodes in WMNs act as router and terminal at the same time and a 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 selfishly 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 WMNs 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, 5]. 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 [1]. Many proposed solutions are based on it, but they suffer from a high false alarm rate. The main problem of these mechanisms is related to the interference at the monitor (detector) node which makes the results of its observations wrong. These mechanisms are mainly considering the IEEE 802.11b/g as MAC protocol, so as far as we know, we are the first authors using Multiple-Input Multiple-Output (MIMO) system with IEEE 802.11n to remove the problem of false observation at the monitor nodes [6].

In this paper, we extend the study of our proposed MAC protocol called MIMODog [6] based on Multi-Input Multi-Output (MIMO) technology, and particularly a SPACE-MAC protocol [7] to significantly reduce the potential interferences at the monitor (detector) nodes and to enhance the accuracy of the monitoring results. The most significant added value consists in i) the modeling of MIMODog to evaluate the impact of the

*Corresponding author
Email addresses: rachedi@u-pem.fr (Abderrezak Rachedi), badis@u-pem.fr (Hakim Badis), abderrahim.benslimane@univ-avignon.fr (Abderrahim Benslimane)

monitoring process on the network performance, ii) the proposition of a monitoring capacity analysis based on graph theory particularly conflict graph, iii) an asymptotic study proposed to investigate lower and upper bounds of the number of monitor nodes.

The contributions of this paper can be summarized in five points:

- We illustrate that the monitoring problem persists in WMNs, even when we use MIMO technology;
- We propose a new MIMO MAC protocol called MIMODog to reduce the interferences at the monitor (detector) nodes without negatively impacting the total network capacity;
- We present and discuss a different impact on the monitoring process with: DCF MAC, SPACE-MAC and MIMODog. MIMODog significantly enhances the monitoring process without affecting the network capacity;
- We propose a monitoring capacity analysis using conflict graph from graph theory for different MAC protocols: DCF MAC, SPACE-MAC and MIMODog;
- We investigate lower and upper bounds of the number of monitor nodes based on asymptotic study for MIMODog. Moreover, the obtained numerical results illustrate that the proposed solution overcomes the drawbacks of classical monitoring mechanisms.

This paper is organized as follows: an overview of cooperation models based on monitoring mechanisms and the SPACE-MAC protocol is given in section 2. Section 3 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 6. In addition, the monitoring capacity and its impact on wireless multi-hop networks is investigated in section 5. Moreover, the theoretical model in order to assess the asymptotic bound related to the monitor nodes number is presented in section 6. The numerical results are given and analysed. The final section concludes the paper and presents our future works.

2. Related Work

In this section, we present the existing works related to the non-cooperative nodes monitoring and the detection models in Wireless Multi-hop Networks (WMNs), and we briefly overview the SPACE-MAC protocol [7].

2.1. Non-cooperative nodes monitoring and detection Models

Two kinds of non-cooperative (selfish) nodes can be distinguished: active and passive selfish nodes. The active selfish nodes, also called greedy nodes, try to get more resources by maliciously manipulating protocols' parameters at MAC and routing layers. For instance, at the MAC layer with IEEE 802.11 DCF mode the active selfish nodes can manipulate the backoff parameters in order to quickly access the channel at the cost of their neighbour nodes [8]. However, the aim of passive selfish nodes is to optimize their benefits in terms of QoS (like throughput and delay) and minimize their costs like the energy consumption without maliciously manipulating protocols' parameters. The typical action of passive selfish nodes is to refuse to forward the packets of other nodes.

In this paper, we focus on the selfish behaviour of the potential cooperative nodes, particularly passive selfish nodes. Cooperation is an important parameter in wireless multi-hop networks, because without any packet forwarding, the ad hoc network cannot exist and the wireless coverage extension is not possible.

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, 9, 10, 11, 12]. The reputation model called CONFIDANT is proposed to share the reputation metric and alarm messages in order to detect and punish the misbehaving nodes [9]. 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.

The second one is based on the economics mechanisms also called price or credit-based mechanisms. In these models the nodes are paid to offer message forwarding services and pay to receive forwarding services. The proposed incentive models for cooperation are using the concept of virtual cash. For instance, many incentive models based on game theory are proposed [13, 14]. The nodes are rewarded for forwarding packets by trading virtual cash with source and next hop nodes [13]. Buttyan and Hubeaux [15] proposed nuglets as credits to manage forwarding transactions. The source node pays relay intermediate nodes by storing nuglets in the packet head. The intermediate nodes acquire the nuglets when they forward the packets. In [16] a hybrid model using the reputation and the price-based mechanism was proposed to overcome the issue of selfish nodes. However, all these solutions are based on the classical monitoring mechanism like Watchdog[4]. The Watchdog mechanism consists in the overhearing of the channel activities in order to detect the non-forwarding (selfish) nodes, but it suffers from a high false positive rate. The main issue of the false observation is related to the collision problem at the monitor (detector) node. Despite, many models are proposed to enhance the false observation [5], but the problem persists. All these models consider the IEEE 802.11b/g as MAC protocol, so as far as we know, we are the first authors using Multiple-Input Multiple-Output (MIMO) system with IEEE 802.11n to remove the problem of false observation at the monitor nodes.

2.2. 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 [1]) [7].

The main contribution of SPACE-MAC 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-MAC is that it enables 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 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 handshake 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.

3. MAC protocols vulnerabilities in monitoring process

In this section, we highlight vulnerabilities in the monitoring process in different cases: classical IEEE 802.11 DCF (with SISO system), SPACE-MAC (with MIMO system), and MIMODog (with MIMO system). In this study, we focus on the origin of the mis-observation of the monitor (detector) nodes.

3.1. Case of 802.11 DCF MAC with single antenna

The monitoring process acts on the different network protocol layers (eg. 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.

[1]RTS: Request to Send / CTS: Clear to Send

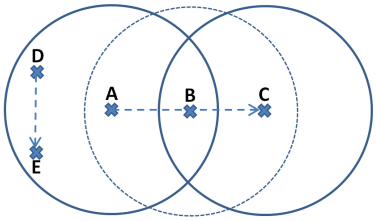

Figure 1: An ad hoc network scenario

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.

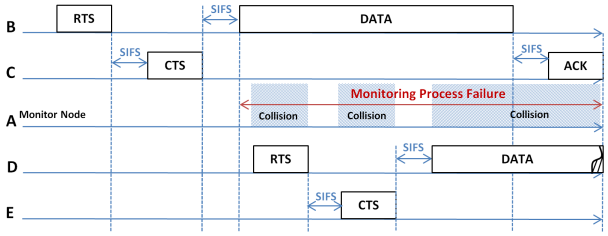

Figure 2: Monitoring problem based on 802.11 DCF MAC protocol

3.2. Case of SPACE-MAC with multiple antennas

In this subsection, we will show that the monitor nodes cannot recover collided packets using the standard SPACE-MAC protocol.

Let us consider the latest network (Figure 1). We assume that all nodes are silent at the beginning, i.e., there is no ongoing 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 an 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 the weight vector of node B and H_{BC} is $M \times M$ MIMO channel matrix with elements h_{ij} and the superscript H denotes an 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 respectively using 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.

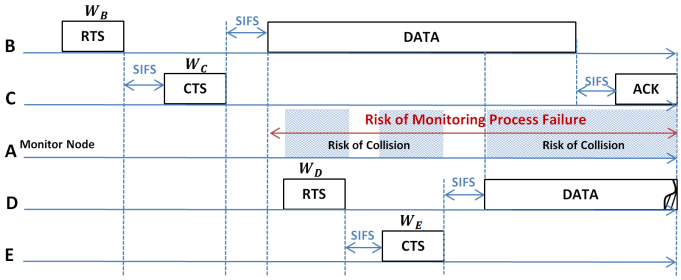

Figure 3: Monitoring problem based on SPACE-MAC protocol

4. MIMODog protocol

In order to avoid any interference at the monitor node, each new transmitting node must be aware not only of the weight vectors of the existing transmissions in the cover area, but also of the weight vectors used by the monitor nodes. To deal with this issue, we propose a new MIMO MAC protocol called MIMODog. 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.

4.1. Basic protocol operation

When monitor node A hears an 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 ensure that node B will not change its behaviour if it is malicious). The A's CTS contains the weight vector w_A and transmits using $\hat{w}_A$. The goal of this operation is to make all future transmitters in the neighborhood believe that node A will receive packets and that its weight vector w_A should be considered.

Once it receives 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.

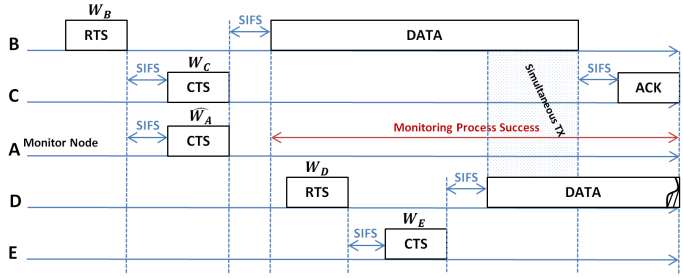

Figure 4: Monitoring mechanism with MIMODog

4.2. 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 used by transmitting stations. This requires a mechanism to convey the antenna weights to all neighboring stations. MIMODog 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 and 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 a channel estimation using pilot symbols embedded in the physical (PHY) preamble.

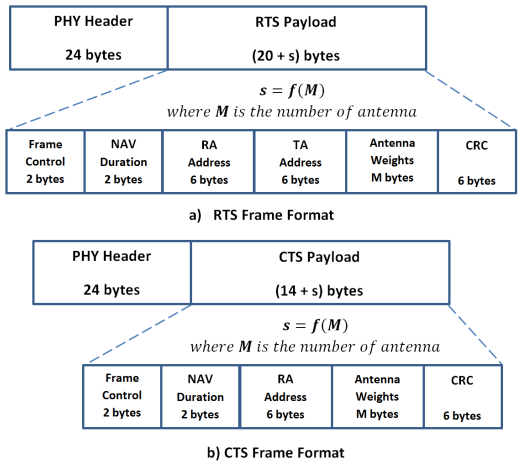

Figure 5: Access Control Packets

5. Monitoring capacity analysis

In this section, we investigate the monitoring capacity and its impact on wireless multi-hop networks. The monitoring capac-

ity for cooperation can be evaluated by the ability of a monitor (detector) node to listen (overhear) its neighbors activities under interference consideration. In this regard, we focus on:

- the computation of the available capacity on the link between the monitor-forwarding nodes;
- the necessary conditions to correctly perform monitoring.

5.1. Preliminary and definitions

The link capacity in a single-hop network can be defined as the physical transmission bit rate of the source, determined by: the Shannon limit, the fixed modulation scheme and the bit error rate. In a wireless multi-hop network (WMN) context, several links share the same transmission medium, and so the link capacity decreases when more simultaneous transmissions occur. The sum of all active data flow throughputs in the same interference area gives the consumed capacity. Consequently, the available link capacity is the difference between the link capacity (in a single-hop network) and the consumed capacity (Figure 6):

$$\textit{Available Link Capacity} = \textit{Link Capacity} - \textit{Consumed Capacity}. \quad (1)$$

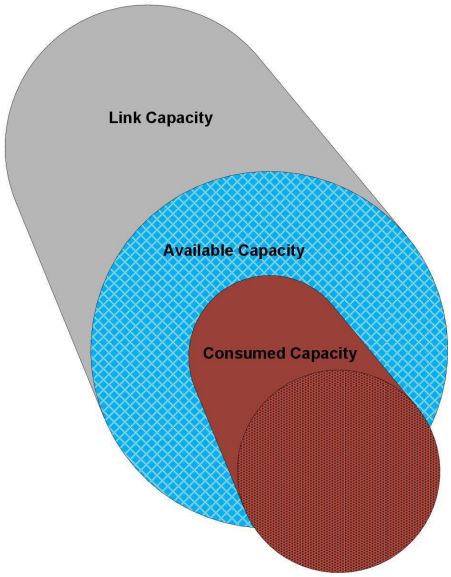

Figure 6: Link Capacity.

Table 1 summarizes the notation used in the next sections.

A WMN can be seen as an *undirected stochastic geometric graph*, called connectivity graph G. Figure 7 shows an example of a connectivity graph. Node b acts as monitor node and node c as forwarding node.
We use the conflict graph to model the interference relationships between links and called it the Links Conflict Graph *LCG*. Every link in connectivity graph G is represented by a node in conflict graph *LCG*. Two nodes in G are connected by an edge if the nodes corresponding to links in G cannot have simultaneous transmissions according to the protocol's interference model. For this purpose and as explained in [17], we use the following interference model: ***any link within distance H from (i, j) is a potential interfering link***. This rule is called the *distance-H interference model*.

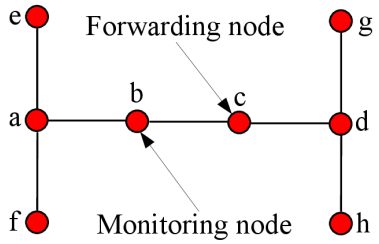

Figure 7: An example of a connectivity graph.

Figures 8.a and 8.b show *distance-2* and *distance-4 LCG*s for the network topology presented in Figure 7. The link between the monitor-forwarding nodes, $2 = (a, c)$, belongs to three cliques[2] in Figure 8.a and to one clique in Figure 8.b. We note that, as *distance-H* of the interference model increases, the number of cliques decreases.

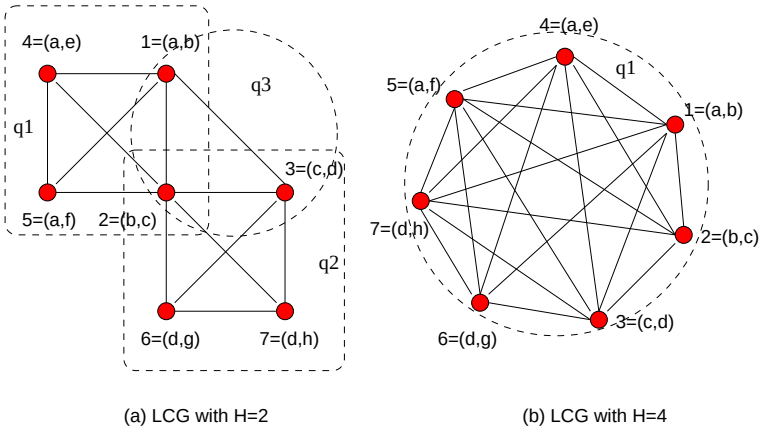

Figure 8: LCGs for network topology.

5.2. Case of 802.11 DCF MAC with single antenna

Based on *LCG*, the *LCG*-nodes in a maximal clique represent the maximal set of mutually contending wireless links, along which only one flow may transit at any given time, consequently only one *LCG*-node in a clique may be active. Accordingly, the sum of the rates of *LCG*-nodes in each maximal clique cannot exceed the capacity of the channel; these conditions are the *clique constraints*. Since the network must satisfy the capacity constraints for all cliques, we can write the clique constraints in a matrix form. We represent a set of flow rates as the column vector $\hat{F}$ of size n, where n is the number of links in the network G and $\hat{F}_i$ is the average flow rate assigned to link i. Let C_i be a column vector of size n with all entries equal to the channel capacity C_i. Hence we have,

[2] A clique in the conflict graph is a set of vertices that mutually conflict with each other.

Table 1: Notation

Symbol	Definition
G	the connectivity graph
G-node	a node in the connectivity graph
G-link	a link in the connectivity graph
LCG	the links conflict graph
LCG-node	a node in the link conflict graph
LCG-link	a link in the link conflict graph
C_i	the capacity on link i within a single-hop network
$F_i(t)$	the instantaneous flow rate utilization on link i at time t
β	the scaling factor
Q_i	the incidence matrix of link i
Γ_i	the available capacity on link i
$\Gamma_{\text{M-F}}$	the available capacity on the link between the monitor-forwarding nodes

$$\forall i \quad Q_i.F \leq C_i. \tag{2}$$

where Q_i is an incidence matrix, which is of order qxn. Here, q is the number of maximal cliques that this link i belongs to, and n is the total number of links. The union of the clique matrices across all the links gives the global clique matrix Q.

Note that the flow rate F_i assigned to link i in an interval of time $]t-\tau, t]$, can be written as:

$$\hat{F}_i = \frac{1}{\tau}\int_{t-\tau}^{t} F_i(r)dr, \tag{3}$$

where $F_i(r)$ is the instantaneous flow rate utilization on link i at time r.

The clique constraints provide a *necessary condition* for a realizable schedule to exist, since there cannot be a feasible schedule over links that form a violated clique constraint. One might hope that these constraints would also be sufficient. Unfortunately, that is only true for a special sub-class of graphs called *Perfect Graphs* [18]. In prior work [19], the authors have proved the sufficiency condition using clique constraints scaled by 0.46 (using a virtual conflict graph). In our work [17], we have generalized the notion of scaling factor, β, according to the used interference model. Clique constraints become:

$$\forall i \quad Q_i.\hat{F} \leq \beta.C_i. \tag{4}$$

As the CG-node can be a part of multiple cliques, it considers all the cliques that it belongs to, and takes the worst case available capacity over all the cliques. The available capacity on a CG-node , i, is

$$\Gamma_i = \min\{(C_i \times \beta) - Q_i\hat{F}\}. \tag{5}$$

Γ_i is the available capacity on link i, taking into account active flows on i, as well as interference from neighboring links.

For example, in Figure 8.a, let the allocated flow on each LCG-node $\{1 = (a,b), 2 = (b,c), 3 = (c,d), 4 = (a,e), 5 = (a,f), 6 = (d,g), 7 = (d,h)\}$ be denoted by $\{\hat{F}_1, \hat{F}_2, \hat{F}_3, \hat{F}_4, \hat{F}_5, \hat{F}_6, \hat{F}_7\}$. Then, the available capacity on the link between the monitor-forwarding nodes, $2 = (b,c)$, is:

$$\Gamma_2 = \min\begin{cases}(C_2 \times \beta) - (\hat{F}_1 + \hat{F}_2 + \hat{F}_3)\\ (C_2 \times \beta) - (\hat{F}_1 + \hat{F}_2 + \hat{F}_4 + \hat{F}_5)\\ (C_2 \times \beta) - (\hat{F}_2 + \hat{F}_3 + \hat{F}_6 + \hat{F}_7)\end{cases}$$

In the same way, from Figure 8.b:

$$\Gamma_2 = (C_2 \times \beta) - (\hat{F}_1 + \hat{F}_2 + \hat{F}_3 + \hat{F}_4 + \hat{F}_5 + \hat{F}_6 + \hat{F}_7).$$

When the forwarding node forwards the monitor node's traffic, say θ, two conditions are necessary for a successful listening by the monitor node:

- The traffic from/to the monitor node should be null. Otherwise, the monitor node cannot hear the forwarding node's activities. The capacity of the link between monitor-forwarding nodes becomes:

$$\begin{cases}\Gamma_{\text{M-F}} = \min\{(C_{\text{M-F}} \times \beta) - Q_{\text{M-F}}\hat{F}\}\\ F_{\text{M-F}} = 0\end{cases} \tag{6}$$

- The available capacity on the link between the monitor-forwarding nodes is more than the amount of the monitored traffic:

$$\Gamma_{\text{M-F}} \geq \theta. \tag{7}$$

However, the previous conditions are not sufficient because a feasible schedule isn't guaranteed.

5.3. Case of SPACE-MAC protocol with MIMO system

The SPACE-MAC protocol operates in M-dimensional space, where M is the degrees of freedom (DoF) of the MIMO

channel. In this case, the interference relationship between different links in the network are conserved in the same DoF. However, the inter-DoF interference is null. Consequently, the capacity of any MIMO link in the network is the sum of all capacities on that link per DOF. Figure 9 illustrates the superposition but independence of the link conflict graphs of the network topology shown in Figure 7. Each DoF has its own *LCG*. All the *LGC*s are similar if we apply the same interference model.

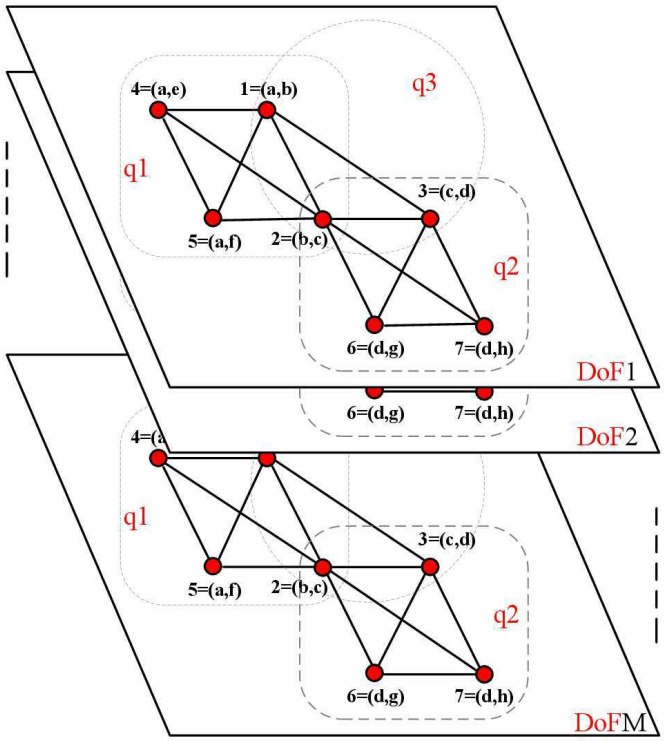

Figure 9: LCGs for network topology.

Let Γ_i^j be the available capacity on link i under DoF i. The total available capacity on link i, Γ_i, is given by the following formula:

$$\begin{cases} \Gamma_i = \sum_{j=1}^{M} \Gamma_i^j \\ \Gamma_i^j = \min\{(C_i \times \beta^j) - Q_i \hat{F}^j\} \end{cases} \tag{8}$$

We assume that at any time slot t and under any DoF, a node can either transmit or receive, but not both. In other words, if a node transmits at time slot t and under DoF m, it cannot transmit or receive at the same time slot under the remaining DoFs. To hear the forwarding node, the monitor node should use the same weight vector used by the forwarding node. This means that the monitor-forwarding pair uses the same DoF. According to the DoF used by transmitter/receiver nodes located in the interference area of the monitor node, we distinguish two cases:

- If no transmitter/receiver node uses the same DoF as that used for monitoring, the monitor node can correctly hear the forwarding node's activity. In this case, the link capacity of the monitor-forwarding nodes is:

$$\begin{cases} \Gamma_{\text{M-F}} = \sum_{j=1}^{M} \Gamma_{\text{M-F}}^j \\ \Gamma_{\text{M-F}}^j = C_{\text{M-F}} & \text{if } j \text{ is the used DoF for monitoring} \\ \Gamma_{\text{M-F}} = \min\{(C_{\text{M-F}} \times \beta) - Q_{\text{M-F}} \hat{F}\} & \text{otherwise} \end{cases} \tag{9}$$

- If there is at least one transmitter/receiver node using the same DoF as that used for monitoring, in this case and following the same reasoning as in section 5.2, two conditions are necessary for a successful listening by the monitor node:
  - The traffic from/to the monitor node should be null. The link capacity of the monitor-forwarding nodes becomes:

$$\begin{cases} \Gamma_{\text{M-F}} = \min\{(C_{\text{M-F}} \times \beta) - Q_{\text{M-F}} \hat{F}\} \\ F_{\text{M-F}} = 0 \end{cases} \tag{10}$$

  - The available capacity on the link between the monitor-forwarding nodes is more than the amount of the monitored traffic:

$$\Gamma_{\text{M-F}} \geq \theta. \tag{11}$$

5.4. Case of MIMODog protocol with MIMO systems

The main goal of the MIMODog protocol is to avoid transmissions and monitoring under the same DoF within the interference area of the monitor node. Consequently, the link capacity of the monitor-relay nodes is similar to that of the SPACE-MAC protocol illustrated in equation 9. The resulting capacity is due to the reservation of the DoF for the monitoring process which demonstrates the advantage of MIMODog protocol. Indeed, to enable a successful monitoring regardless of the nodes activities in the interference area, a capacity reservation is necessary. The SPACE-MAC protocol is a DoF reservation mechanism on the link between a source node and its 1-hop relay node. However, the MIMODog protocol introduces an additional DoF reservation on the predecessor link.

6. Theoretical results of monitoring process

In this section, we present the obtained theoretical results related to the monitoring and its impact on the network capacity.

6.1. Average monitor nodes' number

Let $G = (V, E)$ be a geometric graph with node set v and edge set E, where $|V| = n$ and there is an edge between two nodes u and v with a probability $P(\|u - v\|)$. This probability expresses the relationship between the power of the received signal and the distance. If we apply the the log-normal shadowing model, $P(\|u - v\|)$ can be given as [20]:

$$P(\widehat{\|u - v\|}) = \frac{1}{2}\Big[1 - \text{erf}\Big(3.07 \frac{\ln(\widehat{\|u - v\|})}{\xi}\Big)\Big], \quad \xi \triangleq \frac{\sigma}{\eta} \tag{12}$$

where:

$$\begin{cases} \widehat{\|u-v\|} & \text{is the normalized distance} \\ \sigma & \text{is the standard deviation of shadowing} \\ \eta & \text{is the path-loss exponent} \end{cases}$$

In our work, we consider $\xi = 0$. In other words, we consider only the case where two nodes with distances less than the normalized distance 1 are connected. The mean number of hops is given by [20]:

$$\begin{cases} \overline{hopcount} = \frac{\ln(n)}{\overline{node-degree}} \\ \overline{node-degree} = \frac{2(n-1)}{m(m-1)} \sum_{i=1}^{m} \sum_{j=i+1}^{m} P(\|x_i - x_j\|) \end{cases} \quad (13)$$

where m is the number of small squares containing at most one node.

Any traffic between two nodes in the network has at mean $\overline{hopcount}$ intermediate (forwarding) nodes and so $\overline{hopcount}$ potential monitor nodes. According to the number of source-destination pair, say K, the average monitor nodes' number, $\overline{NMN}$, is

$$\overline{NMN} = k \times \overline{hopcount}. \quad (14)$$

Regardless of the used protocol (IEEE802.11 DCF, Space-MAC and MIMODog), equation 14 remains valid. Using equation 14 and under different values of the number of nodes and degrees of adjacency, we obtain the results shown in figure 14.

In order to study the number of monitor (detector) nodes whatever the monitoring mechanism model used (SISO, MIMO, and MIMODog), we plot in figure 10 the number of monitor nodes (NMN) according to the network density and degrees of neighborhood with different numbers of network traffic flows. We remark that the NMN increases not only with the network density, but also with the number of network traffic flows. However, the NMN significantly decreases when the degree of neighborhood increases. These results are coherent because when the degree of neighborhood is significant the number of potential relayer nodes also increases.

6.2. The impact of monitoring on the capacity

We assume that n nodes are randomly located on the surface of a square flat torus unit area. We use this geometric topology to avoid edge effects, which otherwise complicates the analysis. Each node selects a destination randomly to which is sends $\lambda(n)$ bits/s. We use slotted time for transmission.

The average length of each source-destination pair in terms of links is $\overline{hopcount} + 1$. The average required capacity over the entire network for $\lambda(n)$ successful delivery is at least as follows:

- for 802.11 DCF MAC with single antenna: $(\overline{hopcount} + 1)n\lambda(n)$;
- for SPACE-MAC with M antennas: $\frac{(\overline{hopcount}+1)n\lambda(n)}{M}$. This is because each node can use all its DoFs for spatial multiplexing, and so the total required capacity is divided by the number of DoFs;
- for MIMODog protocol with M antennas: $\frac{(\overline{hopcount}+2)n\lambda(n)}{M}$. As with the SPACE-MAC, the total required capacity is divided by the number of DoFs. However, to allow monitoring without interference, MIMODog protocol extends the interference area of the forwarding node by adding the interference area of the monitor node (see section 4). Consequently, the used protocol interference model becomes distance-(H+1) from the forwarding node, rather than distance-H. In this case, the nodes in the interference area of the monitor node assume the impact of the distance-(H+1) as an increase in the number of hops.

In figure 11, we plot the average consumed capacity in the network according to the network density and the average hop count with different models of monitoring mechanism: SISO ($M = 1$), SPACE-MAC, and MIMODog (the number of antennas is set to 2). We remark that the required capacity in the case of MIMODog is more important than the case of SPACE-MAC particularly when the average hop count increases. However, the worst results are obtained in the case of SISO compared to both models based on MIMO technology.

In order to study the impact of the number of antennas (M), we plot in figure 12 the consumed capacity with different monitoring models. We remark that the gap between the consumed capacity in the case of MIMODog and SPACE-MAC remains constant when the number of antennas increases.

These results illustrate that the monitoring mechanism is costly if we want to reach 0% of misobservation, because MIMODog consumes DoF resources to ensure the monitoring process.

6.3. Asymptotic study of the number of monitor nodes

In this subsection, we focus on the MIMODog asymptotic study of the lower and upper bound of monitor (detector) nodes' number.

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.

6.3.1. Lower bound of the number of monitor nodes

In [21], 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 [21], a number of monitor nodes lower bound of $\Omega(\frac{M}{\sqrt{n \ln n}})$ can be obtained.

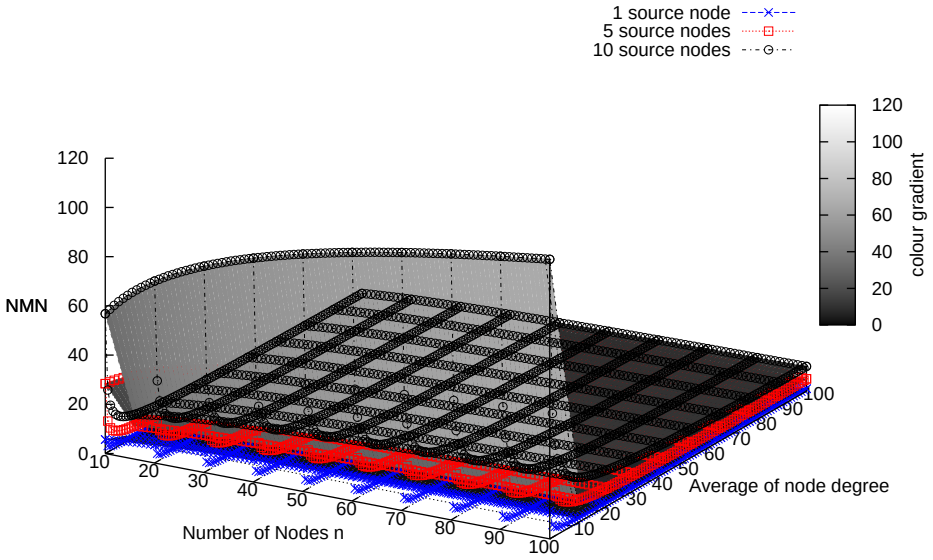

Figure 10: The number of monitor nodes (NMN) versus network density with different degrees of neighborhood.

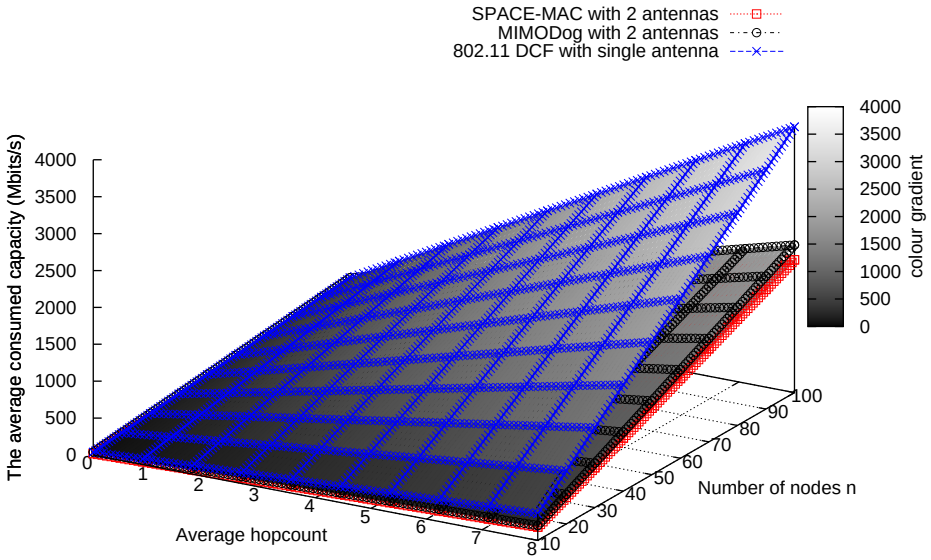

Figure 11: The average consumed capacity in the network according to the network density and the average of hop count with $\lambda(n) = 4$ Mbits/s and $M = 2$.

6.3.2. Upper bound of the number of monitor nodes

As shown in [22], 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 enables to estimate the number of monitor nodes.

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 than with SISO 802.11 DCF MAC.*

Proof. Based on [22], for a square with a side length $1/\lceil \frac{\sqrt{2}}{\Delta.r(n)} \rceil$ (as shown in Figure 13), 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, the presence of a monitor node in the

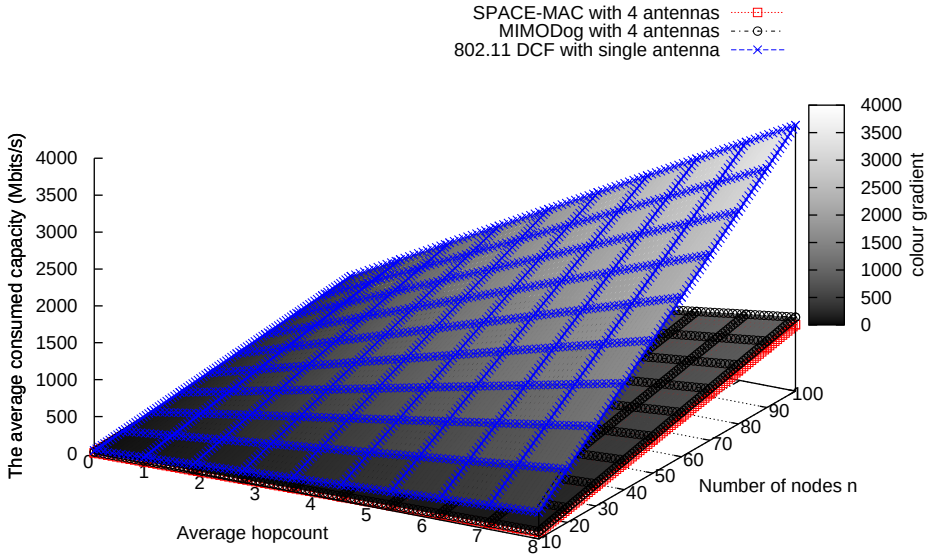

Figure 12: The average consumed capacity in the network according to the network density and the average of hop count with $\lambda(n) = 4$ Mbits/s and $M = 4$.

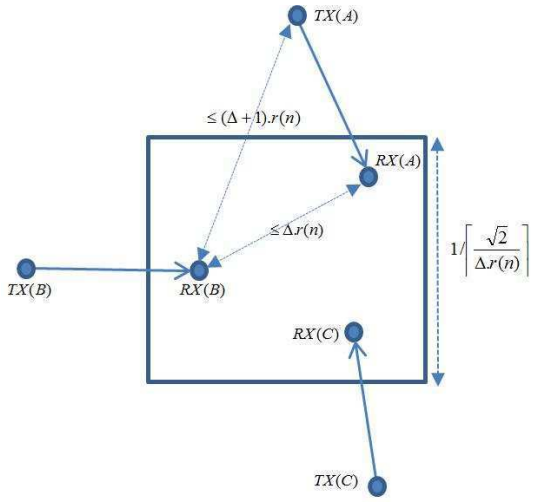

Figure 13: The receivers in a square with side length

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. □

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 [22]. We can easily obtain this equation:

$$\mathbf{NMN} \leq \frac{2M\sqrt{\pi}}{\Delta^2 D\sqrt{n \ln n}} + \frac{2\sqrt{2}M}{\Delta D n} + \frac{M\sqrt{\ln n)}}{Dn\sqrt{\pi n}} = O(\frac{M}{\sqrt{n \ln n}}), \quad (15)$$

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 $\Theta(\frac{M}{\sqrt{n \ln n}})$.

6.3.3. Numerical results

By running 1000 instances, we obtain the average length of source-destination lines $D = 0.52$ (see [22]). We set $\Delta = 1$. Using equation 1 and under different values of $M = 1, 2, 3, 4$ we obtain the results shown in figure 14. With $M = 1$ antenna, MIMODog 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,

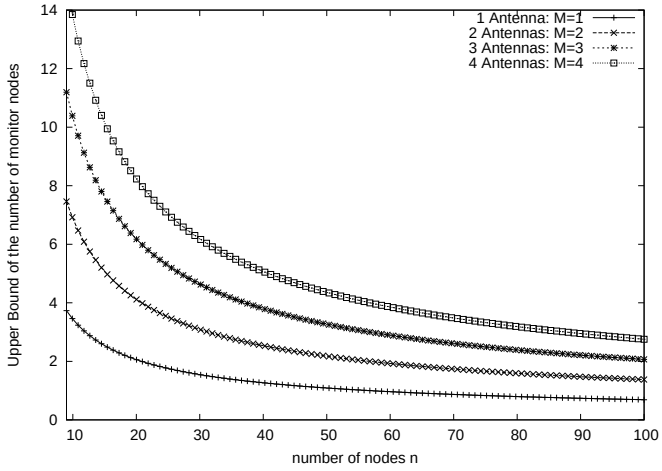

Figure 14: The upper bounds of the number of the monitor nodes versus the number of nodes

- 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.

7. Conclusion

In this paper, we propose a new scheme called MIMODog based on SPACE-MAC protocol for exploiting adaptive antenna arrays in wireless multi-hop networks using a multi-party propagation channel to efficiently detect the selfish (non-cooperative) nodes. The proposed scheme nullifies the beam to competing nodes to enable concurrent transmissions and monitor in the same collision domain. Moreover, we highlight and discuss the different negative impacts on the monitoring process particularly the origin of the false alarm (misobservation) with: DCF MAC, SPACE-MAC and MIMODog. We have shown that the required capacity in the case of MIMODog is more important (but remains close) than the case of SPACE-MAC, due to the allocation of some DoF resources for monitoring. In addition, we have investigated the monitoring process capacity by using conflict graph model. The number of monitor nodes scaling laws for MIMO ad hoc networks with M antennas is evaluated by using asymptotic study. We have shown that the number of monitor nodes is at most $M - 1$ times larger based on MIMODog 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 the density of selfish nodes, mobility models, and traffic models.

References

[1] S. Marti, T. J. Giuli, , K. Lai, M. Baker, Mitigating routing misebehaviour in mobile ad-hoc networks, in: Proceedings of the 6th annual international conference on Mobile computing and networking (MobiCom), 2000.

[2] A. Rachedi, A. Benslimane, Toward a cross-layer monitoring process for mobile ad hoc networks, Security and Communication Networks 2 (4) (2009) 351–368.

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

[4] P. Michiardi, 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] J. Tang, Y. Cheng, Selfish misbehavior detection in 802.11 based wireless networks: An adaptive approach based on Markov decision process, in: IEEE Conference on Computer Communications (INFOCOM), 2013.

[6] A. Rachedi, H. Badis, MIMODog: How to solve the problem of selfish misbehavior detection mechanism in MANETs using MIMO Technology, in: The 8th International Wireless Communications & Mobile Computing Conference (IWCMC) Limassol, Cyprus, 2012.

[7] J. S. Park, N. Alok, M. Gerla, H. Lee, Space-mac: Enabling spatial reuse using mimo channel-aware mac, in: Proceedings of International Conference Communications (ICC), 2005.

[8] M. Raya, I. Aad, J.-P. Hubaux, A. E. Fawal, Domino: Detecting mac layer greedy behavior in ieee 802.11 hotspots, IEEE Transactions on Mobile Computing 5 (2006) 1691–1705.

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

[10] S. Bansal, M. Baker, Observation-based cooperation enforcement in ad hoc networks, in: CoRR, 2003. doi:http://arxiv.org/pdf/cs.ni/0307012.pdf.

[11] T. Chen, A. Bansal, S. Zhong, A reputation system for wireless mesh networks using network coding, Journal of Network and Computer Applications (JCNA) 34 (2) (2011) 535–541.

[12] R. Braga, I. Chaves, C. de Oliveira, R. Andrade, J. de Souza, H. Martin, B. Schulze, RETENTION: A reactive trust-based mechanism to detect and punish malicious nodes in ad hoc grid environments, Journal of Network and Computer Applications 36 (1) (2013) 274–283.

[13] L. Chen, L. Libman, J. Leneutre, Conflicts and incentives in wireless cooperative relaying: A distributed market pricing framework, In IEEE Transactions on Parallel and Distributed Systems 22 (5) (2011) 758 – 772.

[14] A. Rachedi, H. Otrok, N. Muhamed, A. Benslimane, M. Debbabi, A Secure Mechanism Design-Based and Game Theoretical Model for MANETs, ACM Mobile Networking and Applications (MONET) 15 (2) (2010) 191–204. doi:http://dx.doi.org/10.1007/s11036-009-0164-7.

[15] L. Buttyan, J. P. Hubeaux, Enforcing service availability in mobile ad-hoc wan, in: Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing, 2000, pp. 87– 96.

[16] Z. Li, H. Shen, Analysis of a hybrid reputation management system for mobile ad-hoc networks, in: Proceedings of International Conference on Computer Communications and Networks, 2009.

[17] H. Badis, An efficient bandwidth guaranteed routing for ad hoc networks using ieee 802.11 with interference consideration, in: ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems (MSWIM), 2007.

[18] L. Lovasz, A characterization of perfect graph, Journal of Combinatorial Theory 13 (1972) 95–98.

[19] Z. Jia, R. Gupta, J. Walerand, P. Varaiya, Bandwidth Guaranteed routing for Ad hoc Networks with Interference Consideration, in: IEEE Symposium on Computers and Communication (ISCC), 2014.

[20] H. R, V. M. P, Degree distribution and hopcount in wireless ad-hoc networks, in: Proceedings of ICON, 2003, pp. 603 – 609.

[21] P. Gupta, P. Kumar, The capacity of wireless networks, In IEEE Transactions in Information Theory 46 (2) (2000) 388 – 404.

[22] K. Y. Canming Jiang, H.S.Y., S. Bradley, On the asymptotic capacity of multi-hop mimo ad hoc networks, In IEEE Transactions in Wireless Communications 10 (4) (2011) 1032 – 1037.