The Influence of Interference Networks in QoS Parameters in a WLAN 802.11g: a Bayesian Approach

Jasmine P. L. Araújo[a], Josiane C. Rodrigues[a], Simone G. C. Fraiha[a], Hermínio S. Gomes[a], Jacklyn Reis[a], Nandamudi L. Vijaykumar[b], Gervásio P. S. Cavalcante[a] and Carlos R. L. Francês[a]

[a]Federal University of Pará (UFPA), Belém Campus, Augusto Correa Avenue, s/n - Zip code: 66075-900, Belém-Pará, Brazil;
[b]National Institute for Space Research (INPE), Astronautas Avenue, 1758 - Zip code: 12227-010, São José dos Campos-São Paulo, Brazil

ABSTRACT

In spite of the significant increase of the use of Wireless Local Area Network (WLAN) experienced in the last years, design aspects and capacity planning of the network are still systematically neglected during the network implementation. For instance, to determine the location of the access point (AP), important factors of the environment are not considered in the project. These factors become more important when several APs are installed, sometimes without a frequency planning, to cover a unique building. Faults such as these can cause interference among the cells generated by each AP. Therefore, the network will not obtain the QoS patterns required for each service. This paper proposes a strategy to determine how much a given network can affect the QoS parameters of another network, by interference. In order to achieve this, a measurement campaign was carried out in two stages: firstly with a single AP and later with two APs using the same channel. A VoIP application was used in the experiment and a protocol analyzer collected the QoS metrics. In each stage 46 points were measured , that are insufficient for statistically characterize the environment. For expanding this data, an Artificial Neural Network (ANN) was used. After the measurement, an analysis of the results and a set of inferences were made by using Bayesian Networks, whose inputs were the experimental data, i.e., QoS metrics like throughput, delay, jitter, packet loss, PMOS and physical metrics like power and distance.

Keywords: WLAN, QoS, Artificial Neural Network, interference, radio environment, Bayesian Network.

1. INTRODUCTION

Wireless Local Area Networks (WLAN) IEEE802.11 have been widely used in the recent years due to their mobility and for being practical in configuring them. They have been a very practical and important solution to industries, companies and historical constructions due to their flexibility and low cost benefits during their installation and utilization. These technologies usually support traffic data generated by web browsing and email applications. In the recent past, they have been considered for voice communication especially in offices[1]. VoIP delivers voice packets over the Internet and consequently the costs are drastically reduced when compared with conventional telephone calls (PSTN). However, these applications require that WLAN installed are capable to support very strict QoS specifications for voice transmission. ITU-T (International Telecommunication Union) G.114 defines, for real-time services, a tolerable rate of packet loss around 1% to 3% and the allowed delay less than 150 ms but not greater than 400 ms[2]. Due to the sensitivity of the specifications, VoIP has been chosen generally to be evaluated in field tests. With respect to the physical layer, three phenomena exert influence on radio transmission: collisions, radio link quality and interference. Collisions are well known phenomena where several hosts transmit packets to the environment and at the same time it introduces packets with errors that

---

Further author information: (Send correspondence to J.P.L.A.)
J.P.L.A.: E-mail: jasmine@ufpa.br, Telephone: 55 91 3201 7740
J.C.R.: E-mail: josi@ufpa.br, S.G.C.F.: E-mail: fraiha@ufpa.br, H.S.G.: E-mail: herminio@ufpa.br
J.R.: jacklyn@ufpa.br, N.L.V.: E-mail: vijay@lac.inpe.br, G.P.S.C.: E-mail: gervasio@ufpa.br,
C.R.L.F.: E-mail: rfrances@ufpa.br

Broadband Access Communication Technologies II, edited by Raj Jain, Benjamin B. Dingel, Shozo Komaki, Shlomo Ovadia
Proc. of SPIE Vol. 6776, 677604, (2007) · 0277-786X/07/$18 · doi: 10.1117/12.734604

need to be retransmitted. The link quality does not only depend on the noise level but also on the distribution of stations and the topology of the environment (wall positions, furniture density and others). Moreover, the presence of multiple access points may also introduce interference and thus reduce the transmission quality[3]. Such interference leads to receiving packets with errors and at MAC layer, they have to be retransmitted thus affecting the throughput[4]. Added to this fact, the interference may force transmission at lower rates. As already mentioned, the radio environment factors influence the global WLAN performance. But despite this fact very few analyses were conducted to verify this approach, see Refs. 5 to 8. The main objective of this paper is to use computational intelligence by employing Bayesian Networks to verify, aiming at quantifying and characterizing this influence. This work will study specifically the effect of the interference. This is because in any environment with WLAN, it probably will have to coexist with other sources of interferences in the same frequency band, such as, cordless telephones, microwave ovens and access points using the same channel.

This paper is organized as follows: Section 2 presents some basic concepts on KDD (Knowledge Discovery in Database), Data Mining and Bayesian networks; the environment used for obtaining metrics is presented in Section 3 while Section 4 describes the methodology employed in data acquisition; Section 5 presents the data expansion; Section 6 presents the results, the methodology proposal is presented in the section 7 and finally Section 8 concludes the paper.

2. KDD, DATA MINING AND BAYESIAN NETWORKS

The process of knowledge discovery in database (KDD) stands as a technology capable of widely cooperating in the search of existing knowledge in the data. Therefore, its main objective is to find valid and potentially useful patterns from the data. The extraction of knowledge from data can be seen as a process with, at least, the following steps: understanding of the application domain, selection and preparation of the data, data mining, evaluation of the extracted knowledge and consolidation and the use of the extracted knowledge. Once in the data mining stage, considered as the core of the KDD process, methods and algorithms are applied for the knowledge extraction from the database. This stage involves the creation of appropriate models representing patterns and relations identified in the data. The results of these models, after the evaluation by the analyst, specialist and/or final user are used to predict the values of attributes defined by the final user based on new data. In this work, the computational intelligence algorithm used for data mining was based on Bayesian networks.

A Bayesian network is composed of several nodes, where each node of the network represents a variable, that is, an attribute of the database; directed arcs connecting them implies in the relation of dependency that the variable can possess over the others; and finally probability tables for each node. The Bayesian networks can be seen as encoding models of the probabilistic relationships between the variables that represent a given domain. These models possess as components a qualitative representation of the dependencies between the nodes and a quantitative (conditional probability tables of these nodes) structure, that can evaluate, in probabilistic terms, these dependencies. These components together provide an efficient representation of the joint probability distribution of the variables of a given domain. One of the major advantages of the Bayesian networks is their semantics, which facilitates, given the inherent causal representation of these networks, the understanding and the decision making process for the users of these models. Basically, due to the fact that the relations between the variables of the domain can be visualized graphically, besides providing an inference mechanism that allows quantifying, in probabilistic terms, the effect of these relations[9].

3. SCENARIO AND METRICS

The metrics are collected in the second floor of a building of Federal University of Pará. This building is made of bricks and concrete, with lateral glass windows. On the other side, there is a corridor along all the building. In this floor there are only classrooms, that are divided by walls built on bricks. Fig.1 shows some photos of the environment.

3.1 Testbed Features

In the experiment, a network was implemented to use channel 1 (central frequency under 2.412GHz). The architecture of this network, called network under study, is shown in Fig. 2. In this network, an access point(AP1),

Figure 1. pictures of the building. In clockwise: external side with glass windows, classroom, corridor and external side with corridor along.

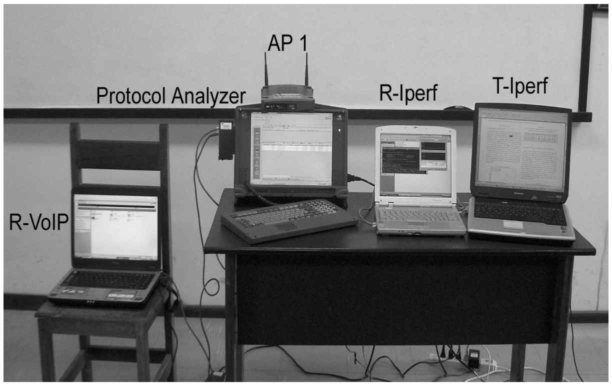


Figure 2. Network under study.

802.11g Linksys© WRT54G Router Speed Booster, was connected to the RADCOM© protocol analyzer[10], using one of its LAN ports. The other port of the protocol analyzer was connected to R-VoIP notebook which received a VoIP call sent by T-VoIP (located in a cart). The T-VoIP notebook was used to make VoIP calls to R-VoIP notebook by using CallGen323 (program that makes 1-minute lasting calls) while Openphone[11] was used to receive calls. Besides the VoIP application, another application was used to share the available bandwidth in the network under study. This application is Iperf program[12] running in a client mode, generating a constant bit rate UDP stream of specified bandwidth (7Mbps). It was an artificial stream, similar to voice communication. This application used two more notebooks, see Fig. 2; T-Iperf notebook was used to transmit the IPerf application and R-Iperf notebook was used to receive it.

The notebook (T-VoIP) used to generate VoIP calls is positioned on a cart that is moved to each point where the measurement is taken after remaining for 3 minutes at the previous location. The cart also carries another notebook to measure the power (called Power-receiver), received by wireless board from several access points, by using Network Stumbler© software[13]. The same notebook was not utilized for both task because the Network Stumbler© does not allow the computer in which this software is running to be connected to a network. Fig.3 shows a picture of the cart with the two notebooks.

Another network, called as interfering network, was installed using the same channel used by network under study. Fig.4 shows the picture of this network, where the notebook called T-Interf transmitted a traffic to other notebook called R-Interf. Iperf[12] was the program used to generate the traffic as it allows to specify the time at which the traffic can be generated.

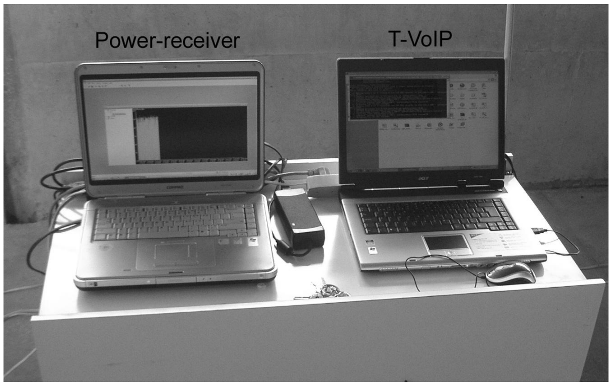


Figure 3. The cart with the VoIP transmitter and power receiver.

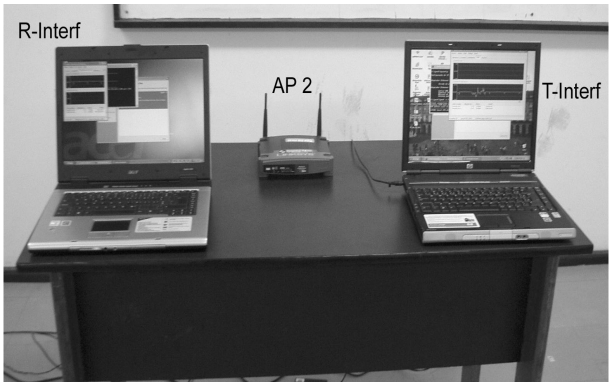


Figure 4. Interfering Network.

4. METHODOLOGY AND MEASUREMENTS

In order to take the measurements, the locations were first selected and then were marked with an adhesive tape. Their distances from the walls were also measured. Fig.5 shows the layout with the located points marked with crosses totalling 46.

Fistly, the network under study was located in the classroom 1. The metrics obtained in the application layer were monitored through loss of packets, jitter, delay, throughput and PMOS by using Performer Media Pro available within the protocol analyzer. A certain number of measurements were collected in an indoor environment. The same process was repeated by adding another network called interfering network, installed in the classroom 6.

Figure 5. Layouts with the location of measurements points.

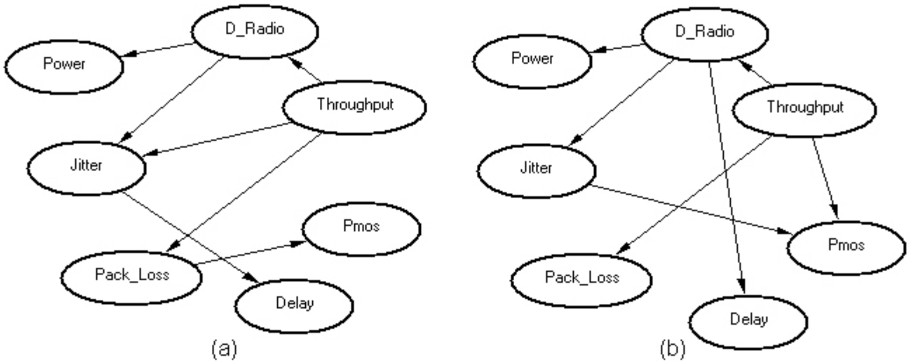


Figure 6. Bayesian networks results without(a) and with(b) interference.

During the measurements, the following parameters were stored: power (via software Netstumbler©), distance transmitter-receiver (obtained after treating data through the locations of the measuring points and access point), jitter, packet loss, PMOS and throughput (measured by protocol analyzer).

After this measurement campaign, data were treated and the measurements were compared. The following sections present the results of this comparison.

5. DATA EXPANSION

As mentioned before, in the second floor, measurements were taken in 46 points and this amount is insufficient for any statisticaly analysis. Therefore, in order to expand this data, a two dimension interpolator was created based on a Neural Network. An Artificial Neural Network (ANN) was used with a backpropagation algorithm, resilient training and 3 layers (16 neurons on the first layer, 8 on the intermediate layer and 1 on the exit layer)[14].

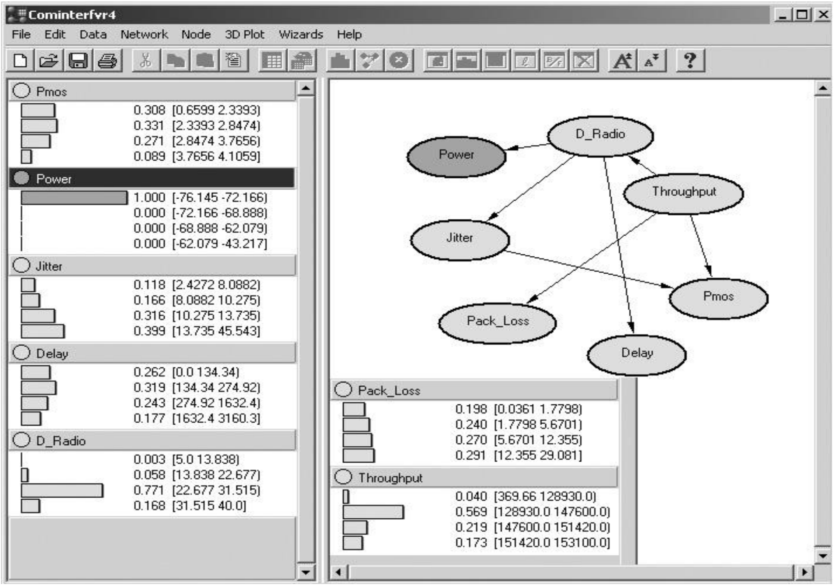
6. SOME INFERENCES BASED ON BAYESIAN NETWORKS

This section discusses the measurements of the application and physical layers as well as the results obtained by using Bayesian networks. The study involves treating the measured data with and without interference with the Bayesian network technique[15]. In any process of knowledge discovery, there is a pre-analysis phase of treatment (soft mining) of the data where information that is not going to contribute to the final result are removed. Hence, the input fields for the Bayesian network were obtained from the protocol analyzer after the pre-analysis. They worked as input to the free version Bayesware Discover© (BDD) commercial software[16].

6.1 Bayesian Networks without Inference

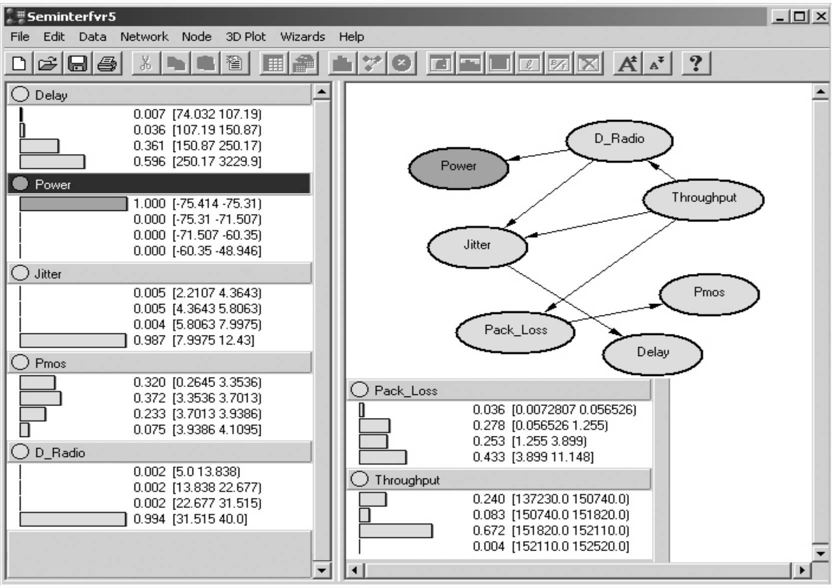
When the Bayesian network is created to analyze the measurements with and without interfering network, each attribute will be turned into a network node as shown in Fig.6(a) and Fig.6(b). In this work Bayesian networks were created representing the actual system that is based on the collected data. This network contains joint probability distribution tables of each node. It is based on dependencies, consisting of attributes i.e., possible values that each variable may assume and their respective probabilities. Once these networks are set and verified that they do represent the actual system and database, inferences are conducted on these Bayesian networks so that the verification of the WLAN network behavior as well as the results obtained from this inference is performed.

The relationship of QoS and physical layer for networks without and with interference can be identified graphically and it can be pointed out that interference has a major impact in the probability relations as observed in the Fig.6(a) and Fig.6(b).



```
○ Pmos
0.308 [0.6599 2.3393]
0.331 [2.3393 2.8474]
0.271 [2.8474 3.7656]
0.089 [3.7656 4.1059]
● Power
1.000 [-76.145 -72.166]
0.000 [-72.166 -68.888]
0.000 [-68.888 -62.079]
0.000 [-62.079 -43.217]
○ Jitter
0.118 [2.4272 8.0882]
0.166 [8.0882 10.275]
0.316 [10.275 13.735]
0.399 [13.735 45.543]
○ Delay
0.262 [0.0 134.34]
0.319 [134.34 274.92]
0.243 [274.92 1632.4]
0.177 [1632.4 3160.3]
○ D_Radio
0.003 [5.0 13.838]
0.058 [13.838 22.677]
0.771 [22.677 31.515]
0.168 [31.515 40.0]
○ Pack_Loss
0.198 [0.0361 1.7798]
0.240 [1.7798 5.6701]
0.270 [5.6701 12.355]
0.291 [12.355 29.081]
○ Throughput
0.040 [369.66 128930.0]
0.569 [128930.0 147600.0]
0.219 [147600.0 151420.0]
0.173 [151420.0 153100.0]
```

Figure 7. Bayesian networks with worst power inference with interference.



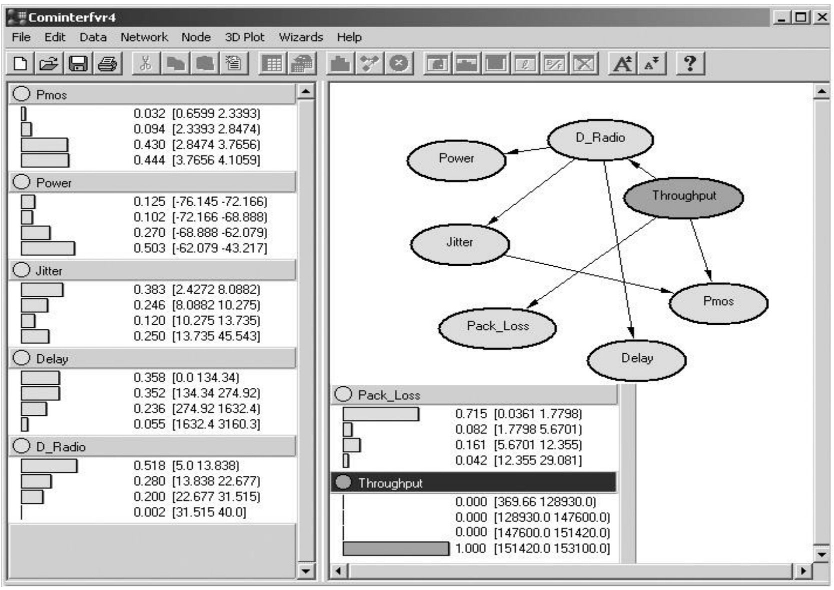
```
○ Delay
0.007 [74.032 107.19]
0.036 [107.19 150.87]
0.361 [150.87 250.17]
0.596 [250.17 3229.9]
● Power
1.000 [-75.414 -75.31]
0.000 [-75.31 -71.507]
0.000 [-71.507 -60.35]
0.000 [-60.35 -48.946]
○ Jitter
0.005 [2.2107 4.3643]
0.005 [4.3643 5.8063]
0.004 [5.8063 7.9975]
0.987 [7.9975 12.43]
○ Pmos
0.320 [0.2645 3.3536]
0.372 [3.3536 3.7013]
0.233 [3.7013 3.9386]
0.075 [3.9386 4.1095]
○ D_Radio
0.002 [5.0 13.838]
0.002 [13.838 22.677]
0.002 [22.677 31.515]
0.994 [31.515 40.0]
○ Pack_Loss
0.036 [0.0072807 0.056526]
0.278 [0.056526 1.255]
0.253 [1.255 3.899]
0.433 [3.899 11.148]
○ Throughput
0.240 [137230.0 150740.0]
0.083 [150740.0 151820.0]
0.672 [151820.0 152110.0]
0.004 [152110.0 152520.0]
```

Figure 8. Bayesian networks with worst power inference without interference.

6.2 Bayesian Networks with Inference

The most relevant results are shown in Fig.7 to Fig.14 for the four inferences that were conducted. The first inference refers to power with the worst value while the second refers to the largest throughput. One can observe (Fig.7) that for the worst values assigned to power (ranging from -76.145 to -72.166 dBm), considering interference, the probability of throughput lying within 128930.0 and 147600.0 bps is 56.9%. When interference is not considered (Fig.8 - ranging from -75.414 to -75.31 dBm), the probability of throughput lying within 151820.0 and 152110.0 bps is 67.2%. Therefore, there was a change in the network under study for this specific parameter, the throughput.

Similarly, results are also shown for other metrics. In the case of packet loss, its probability for network with interference is 29.1% for lying within 12.35% to 29.081% whereas the value is 43.3% for lying within 3.89% to



```
○ Pmos
0.032 [0.6599 2.3393)
0.094 [2.3393 2.8474)
0.430 [2.8474 3.7656)
0.444 [3.7656 4.1059]
○ Power
0.125 [-76.145 -72.166)
0.102 [-72.166 -68.888)
0.270 [-68.888 -62.079)
0.503 [-62.079 -43.217]
○ Jitter
0.383 [2.4272 8.0882)
0.246 [8.0882 10.275)
0.120 [10.275 13.735)
0.250 [13.735 45.543]
○ Delay
0.358 [0.0 134.34)
0.352 [134.34 274.92)
0.236 [274.92 1632.4)
0.055 [1632.4 3160.3]
○ D_Radio
0.518 [5.0 13.838)
0.280 [13.838 22.677)
0.200 [22.677 31.515)
0.002 [31.515 40.0]
○ Pack_Loss
0.715 [0.0361 1.7798)
0.082 [1.7798 5.6701)
0.161 [5.6701 12.355)
0.042 [12.355 29.081]
● Throughput
0.000 [369.66 128930.0)
0.000 [128930.0 147600.0)
0.000 [147600.0 151420.0)
1.000 [151420.0 153100.0]
```

Figure 9. Bayesian networks with largest throughput inference with interference.

11.148% when interference is not considered. Considering now the jitter, its probability for lying within 13.375 ms to 45.543 ms is 39.9% for network with interference. This value increases to 98.7% for lying within 7.9975 ms to 12.43 ms for network without interference.

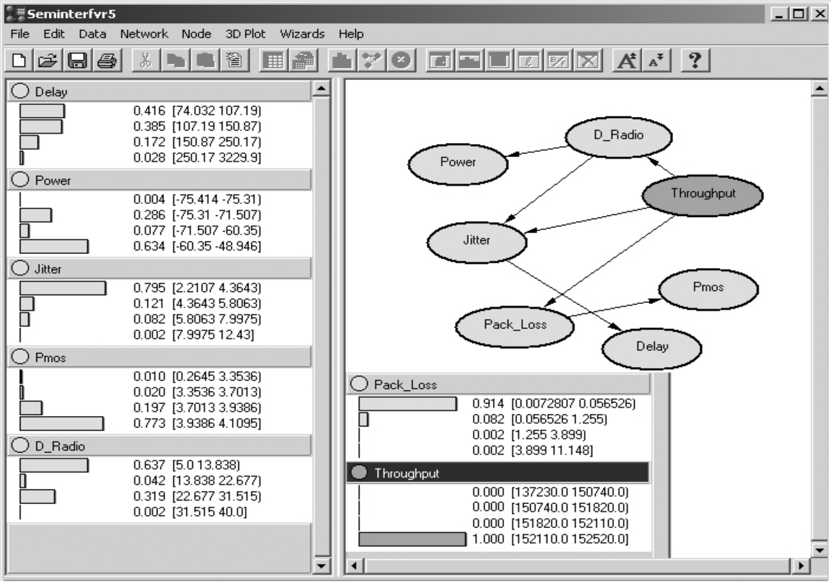
PMOS was also affected by the interference. The probability of PMOS to the network with interference is 33.1% for lying within 2.33 to 2.84 and to the network without interference is 37.2% for lying within 3.35 to 3.7. The delay probability values were 95.7% for lying within 150.87 ms to 3229.9 ms (network without interference) and 73.9% for lying within 134.34 ms to 3160.3 ms (network with interference).

Another evidence showing the influence of interference can be shown in the experiment in which the largest throughput interval was selected. Fig.9 and Fig.10 show the results. The largest throughput for the network with interference lies within 151420.0 to 153100.0 bps whereas for the network without interference lies within 152110.0 to 152520 bps. Now, moving to another parameter, the packet loss, the network with interference presented the largest probability (71.5%) for lying within 0.0361% to 1.7798%. But in the network without interference presented the largest probability (91.4%) for the packet loss to be zero. The probability of jitter to be below 8.08 ms is 38.3% in case of network with interference and the probability to be below 4.36 ms is 79.5% in case of network without interference. PMOS (in the network without interference) has probability of 97% for lying within 3.7013 and 4.1095. The behavior of this metric in network with interference presented the probability of 44% for lying within 3.7656 to 4.1059. However, it can be seen that there is an impact from the interference. The delay probability values were 80.1% for lying within 74.032 ms to 150.87 ms (network without interference) and only 35.8% for lying within 0 ms to 134.34 ms (network with interference), showing that the interference increses delay probability to be higher the maximum recommended in ITU-T guidelines[17].

Another inference conducted is the selection of the largest power in the scenario with and without interference is presented in the Fig.11 and Fig.12.

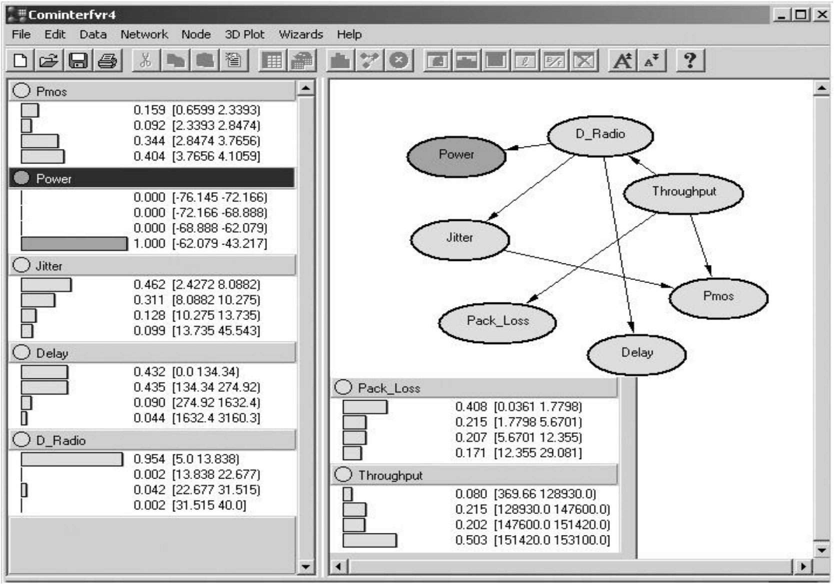
The throughput was affected for the interference because its probabilities values decreased from 63.3% (ranging from 152110 to 152520 bps) to 50.3% for lying within 151420 to 153100 bps. The packet loss for the network without interference is 59.4% to be zero. Considering interference, the probability is 40.8% for lying within 0% to 1.7798%. The jitter probability is 75.1% for lying within 2.2107 ms to 4.3643 ms to the scenario without interference, otherwise in the scenario with interference the probability is 46.2% for lying within 2.42 ms to 8.08 ms.

The PMOS (in the network without interference) has the probability value of 52.8% for lying within 3.9386



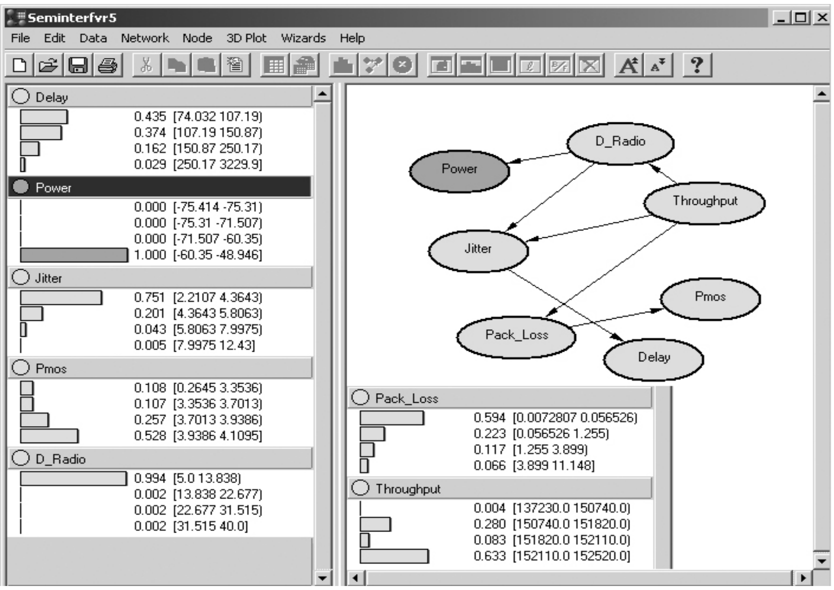
```
○ Delay
0.416  [74.032 107.19)
0.385  [107.19 150.87)
0.172  [150.87 250.17)
0.028  [250.17 3229.9]
○ Power
0.004  [-75.414 -75.31)
0.286  [-75.31 -71.507)
0.077  [-71.507 -60.35)
0.634  [-60.35 -48.946]
○ Jitter
0.795  [2.2107 4.3643)
0.121  [4.3643 5.8063)
0.082  [5.8063 7.9975)
0.002  [7.9975 12.43]
○ Pmos
0.010  [0.2645 3.3536)
0.020  [3.3536 3.7013)
0.197  [3.7013 3.9386)
0.773  [3.9386 4.1095]
○ D_Radio
0.637  [5.0 13.838)
0.042  [13.838 22.677)
0.319  [22.677 31.515)
0.002  [31.515 40.0]

○ Pack_Loss
0.914  [0.0072807 0.056526)
0.082  [0.056526 1.255)
0.002  [1.255 3.899)
0.002  [3.899 11.148]
● Throughput
0.000  [137230.0 150740.0)
0.000  [150740.0 151820.0)
0.000  [151820.0 152110.0)
1.000  [152110.0 152520.0]
```

Figure 10. Bayesian networks with largest throughput inference without interference.



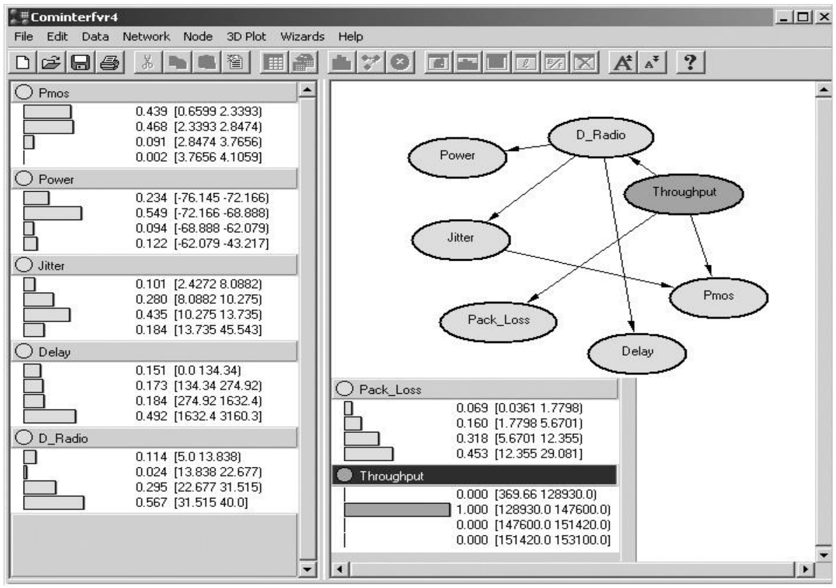
```
○ Pmos
0.159  [0.6599 2.3393)
0.092  [2.3393 2.8474)
0.344  [2.8474 3.7656)
0.404  [3.7656 4.1059]
● Power
0.000  [-76.145 -72.166)
0.000  [-72.166 -68.888)
0.000  [-68.888 -62.079)
1.000  [-62.079 -43.217]
○ Jitter
0.462  [2.4272 8.0882)
0.311  [8.0882 10.275)
0.128  [10.275 13.735)
0.099  [13.735 45.543]
○ Delay
0.432  [0.0 134.34)
0.435  [134.34 274.92)
0.090  [274.92 1632.4)
0.044  [1632.4 3160.3]
○ D_Radio
0.954  [5.0 13.838)
0.002  [13.838 22.677)
0.042  [22.677 31.515)
0.002  [31.515 40.0]

○ Pack_Loss
0.408  [0.0361 1.7798)
0.215  [1.7798 5.6701)
0.207  [5.6701 12.355)
0.171  [12.355 29.081]
○ Throughput
0.080  [369.66 128930.0)
0.215  [128930.0 147600.0)
0.202  [147600.0 151420.0)
0.503  [151420.0 153100.0]
```

Figure 11. Bayesian networks with largest power inference with interference.



```
○ Delay
0.435 [74.032 107.19)
0.374 [107.19 150.87)
0.162 [150.87 250.17)
0.029 [250.17 3229.9]
● Power
0.000 [-75.414 -75.31)
0.000 [-75.31 -71.507)
0.000 [-71.507 -60.35)
1.000 [-60.35 -48.946]
○ Jitter
0.751 [2.2107 4.3643)
0.201 [4.3643 5.8063)
0.043 [5.8063 7.9975)
0.005 [7.9975 12.43]
○ Pmos
0.108 [0.2645 3.3536)
0.107 [3.3536 3.7013)
0.257 [3.7013 3.9386)
0.528 [3.9386 4.1095]
○ D_Radio
0.994 [5.0 13.838)
0.002 [13.838 22.677)
0.002 [22.677 31.515)
0.002 [31.515 40.0]
○ Pack_Loss
0.594 [0.0072807 0.056526)
0.223 [0.056526 1.255)
0.117 [1.255 3.899)
0.066 [3.899 11.148]
○ Throughput
0.004 [137230.0 150740.0)
0.280 [150740.0 151820.0)
0.083 [151820.0 152110.0)
0.633 [152110.0 152520.0]
```

Figure 12. Bayesian networks with largest power inference without interference.



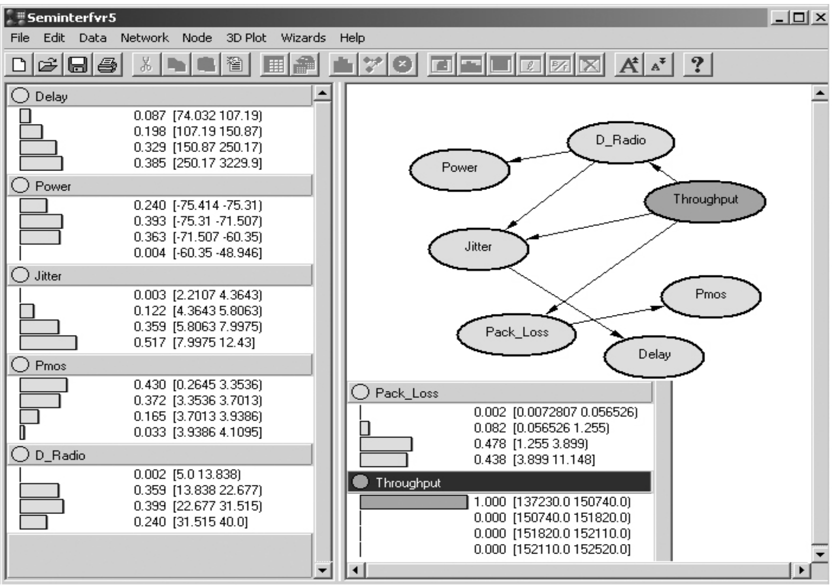
```
○ Pmos
0.439 [0.6599 2.3393)
0.468 [2.3393 2.8474)
0.091 [2.8474 3.7656)
0.002 [3.7656 4.1059]
○ Power
0.234 [-76.145 -72.166)
0.549 [-72.166 -68.888)
0.094 [-68.888 -62.079)
0.122 [-62.079 -43.217]
○ Jitter
0.101 [2.4272 8.0882)
0.280 [8.0882 10.275)
0.435 [10.275 13.735)
0.184 [13.735 45.543]
○ Delay
0.151 [0.0 134.34)
0.173 [134.34 274.92)
0.184 [274.92 1632.4)
0.492 [1632.4 3160.3]
○ D_Radio
0.114 [5.0 13.838)
0.024 [13.838 22.677)
0.295 [22.677 31.515)
0.567 [31.515 40.0]
○ Pack_Loss
0.069 [0.0361 1.7798)
0.160 [1.7798 5.6701)
0.318 [5.6701 12.355)
0.453 [12.355 29.081]
● Throughput
0.000 [369.66 128930.0)
1.000 [128930.0 147600.0)
0.000 [147600.0 151420.0)
0.000 [151420.0 153100.0]
```

Figure 13. Bayesian networks with low throughput inference with interference.

and 4.1095 and this value decreased to 40% for lying within 3.7656 to 4.1069, considering interference. Finally, the delay presents the following values of probabilities: to network without interference 80.9% for lying within 74.032 ms to 150.87 ms and to network with interference is 86.7% for lying within 0 ms to 274.92 ms. The upper limit of the delay with interference increased to 274.92 ms showing again that interference influenced the delay probability.

The last inference conducted is the selection of the low throughput in the scenario with and without interference as are presented in the Fig.13 and Fig.14.

The packet loss for the network with interference with inference of low throughput is 45.3% for lying within 12.355% to 29.081%. Considering the network without interference, the probability is 47.8% for lying within 1.255% to 3.899%.



```
○ Delay
0.087 [74.032 107.19)
0.198 [107.19 150.87)
0.329 [150.87 250.17)
0.385 [250.17 3229.9]
○ Power
0.240 [-75.414 -75.31)
0.393 [-75.31 -71.507)
0.363 [-71.507 -60.35)
0.004 [-60.35 -48.946]
○ Jitter
0.003 [2.2107 4.3643)
0.122 [4.3643 5.8063)
0.359 [5.8063 7.9975)
0.517 [7.9975 12.43]
○ Pmos
0.430 [0.2645 3.3536)
0.372 [3.3536 3.7013)
0.165 [3.7013 3.9386)
0.033 [3.9386 4.1095]
○ D_Radio
0.002 [5.0 13.838)
0.359 [13.838 22.677)
0.399 [22.677 31.515)
0.240 [31.515 40.0]
○ Pack_Loss
0.002 [0.0072807 0.056526)
0.082 [0.056526 1.255)
0.478 [1.255 3.899)
0.438 [3.899 11.148]
● Throughput
1.000 [137230.0 150740.0)
0.000 [150740.0 151820.0)
0.000 [151820.0 152110.0)
0.000 [152110.0 152520.0]
```

Figure 14. Bayesian networks with low throughput inference without interference.

The jitter probability is 51.7% for lying within 7.9975 ms to 12.43 ms to the scenario without interference, otherwise in the scenario with interference the probability is 61.9% for lying within 10.275 ms to 45.543 ms. This metric also was affected by interference increasing the bad values of jitter.

The PMOS (in the network without interference) has the probability value of 43% for lying within 0.2645 to 3.3536 and this value increased to 90.7% for lying within 0.6599 to 2.8474, considering interference. Finally, the delay presents the following values of probabilities: to network without interference 71.4% for lying within 150.87 ms to 3229.9 ms and to network with interference is 84.9% for lying within 134.34 ms to 3160.3 ms. The delay probability value increased to the scenario with interference like the other metrics analyzed as jitter and packet loss. The Bayesian analysis showed once more that interference, in fact, affects QoS parameters.

7. CAPACITY PLANNING AND PERFORMANCE EVALUATION ISSUES: A METHODOLOGY PROPOSAL

In real building there is a very strong trend to find similar scenarios to the presented ones in this paper, where different networks cohabit and where it is desirable that applications with rigid parameters of QoS carry out (e.g.: VoIP). To make this possible, the accomplishment of the following stages is necessary, at least, according to the methodology proposed in this paper:

- Characterization of the environment parameters (physical layer) of the WLAN:

  The presence of obstacles, like walls, environment aspects, among other, on the path of radio transmission attenuates signal power. In this way the reception quality is degraded and the error probability increases The power can vary significantly, since in a short period, due to mobility and the multipath effect. Consequently retransmissions are produced and WLAN performance is influenced. One must also consider the signal-to-noise ratio, often written S/N or SNR, which from 10 decibels we can say that we have a suitable signal, from 10 to 15 decibels is enough, from 15 to 20 it is good signal and 20 onwards is excellent. These numbers are recommended for data; for voice 25 decibels or more are recommended and not to receive a signal from another access point that is working in the same channel and that is greater than 10 decibels[5].

- Survey of the interfering networks:

  - Define the spatial distribution of the wireless network;
  - Mark and obtain the coordinates of access points to be evaluated;
  - Start the application for wireless network to be studied;
  - Use a software for collecting samples of signal level on wireless network;
  - Use an application in the protocol analyzer to store QoS measures;
  - Start application(s) in the interferent wireless network.

- Definition of QoS requirements of the target application:

  There are several available metrics to measure the quality of a connection, such as packet loss rate, one-way delay, jitter, packet loss rate, and throughput. Average one-way delay is probably the most critical parameter for VoIP. If it is too long, conversation flow is compromised and communication may become unnatural. ITU-T guidelines recommend a one-way delay of up to 150 milliseconds[17]. Beyond that, negative consequences gradually accrue. In IEEE 802.11 networks, the one-way delay between client and access point is usually less than 10 milliseconds, and therefore should not be a problem in VoIP.

  Jitter is the packet-to-packet variation in the one-way delay. Most modern systems will use some type of adaptive playback to smooth out the jitter, but this increases the one-way delay, and can introduce artifacts into the speech. In Wi-Fi networks, jitter is generally small, partially because one-way delay and packet sizes are small, too. However, this paper showed that there are times when extreme delay variations can occur with significant impact on voice quality.

  Packet loss rate also affects speech quality, as the decoded speech will present artifacts associated with the lost packets. For VoIP, packet loss rates of up to 1% are generally acceptable[17]. In IEEE 802.11 networks, collisions and other losses are hidden by an automatic re-transmission strategy. Since these retransmissions are transparent to the application layer, the final packet loss rate is typically less than 1% and, therefore, acceptable for typical VoIP applications. Note, however, that as a mobile terminal gets out of the range, the loss rates increase abruptly; quickly making speech communication impossible.

  Throughput: the bandwidth required by a single VoIP connection is significantly less than the nominal capacity of IEEE 802.11 networks. Typical speech codecs require no more than 64 Kbps, while 802.11g offers 54 Mbps. However, if the same access point is used to support multiple calls, we may have a capacity problem[17]. It is important to consider if there are WLANs near to our WLAN, where access points channels of our neighbors do not interfere with ours. Technologies that could produce interference are: Bluetooth, microwaves, some cellular phones and others WLANs, among others[5].

- Characterization of traffic for the target application:
  - Running several iterations of the application target observing patterns and typical curves by means of acquisition of samples and utilization of goodness of fit tests;
  - Definition of probability distribution for each performance measure studied, such as: delay, blocking probabilities and throughput;
  - Definition of the measures that must be considered in the computational models (computational intelligence, optimization and simulation).

- Accomplishment of inferences based on simulation, computational intelligence or analytical models/optimi zation, to verify aspects as: correlation, possible scenarios, scalability, availability and performance.

8. CONCLUSIONS

This paper proposes the use of computational intelligence by employing Bayesian Networks to verify the interference influence in QoS parameters. Bayesian analysis showed this influence with precision, pointing out that interference has a major impact in the 802.11 network performance. The major difference in the work presented here from research cited in Refs. 3 and 7 lies in the field experiments with and without interference. A Bayesian network was used to analyze the data to show an evidence, as shown in Ref. 7, that there is an influence of the radio environment affecting QoS parameters. However, the work presented in this paper includes investigation of other parameters such as delay, jitter, packet loss and PMOS besides throughput that was the only parameter analyzed in Refs. 3 and 7. The work hasn't included any explicit optimization study but some research is in progress in using Bayesian networks for this purpose. The sequence of this work is to draw a roadmap for capacity planning with an optimal number of APs, the cost function will be a Bayesian function and their weights and coefficients will be validated with the use of genetic algorithms and Markov chains for the scenario with and without interference, also proposed in Ref. 9 and validate the hypothesis suggested in Ref. 9 experimentally. The multiple user scenarios was implemented through the Iperfstress application and the Bayesian network was also used to treat the obtained results. It is important to mention that Bayesian network offers an approach to select several scenarios of QoS such that it is possible to guarantee a minimum distance to the AP for VoIP application in an indoor WLAN environment.

REFERENCES

1. K. Medepalli, P. Gopalakrishnan, D. Famolari and T. Kodama, "Voice Capacity of IEEE 80211b 80211a and 80211g Wireless Lans", *Vehicular Telecommunications Conference (Globecomm 2004)*, IEEE Communications Society, Vol.**3**, pp. 1549-1553, 2004.
2. H. Zhai, J. Wang and Y. Fang, "Providing Statistical QoS Guarantee for Voice over IP in the IEEE 802.11 Wireless LANs", *IEEE Wireless Communications*, Vol. **3**, Issue 1, pp. 36-43, 2006.
3. J. L. Lu, K. Jaffres-Runser, J. M. Gorce and F. Valois, "Indoor WLAN Planning with a QoS constraint based on a Markovian Performance Evaluation Model", *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'2006)*, Paper topic area: Design and Analysis of Wireless LAN/WAN, pp. 152-158, 2006.
4. S. G. Glisic, *Advanced Wireless Networks 4G Technologies*, John Wiley and Sons LTDA, 2006.
5. L. E. N. Diaz and J. A. P. Diaz, "A Model for Designing WLAN's 802.11 for VoIP", *Proceedings of the Electronics, Robotics and Automotive Mechanics Conference (CERMA'06)*, IEEE Computer Society, Vol. 2, pp. 110-115, 2006.
6. J. L. Lu and F. Valois, "Performance evaluation of 802.11 WLAN in a real indoor environment", *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications(WiMob'2006)*, Montreal-Canada, pp. 140-147, 2006.
7. S. Garg and M. Kappes,"Can I add a VoIP call?", *IEEE International Conference on Communications (ICC'03)*, Vol.2, pp. 779-783, 2002.
8. W. Wang, S. C. Liew, V. O. K. Li, "Solutions to performance problems in VoIP over a 802.11 wireless LAN", *Vehicular Technology, IEEE Transactions on*, Vol. 54, Issue 1, 2005.
9. A. L. Santana et al., "Strategies for improving the modeling and interpretability of Bayesian Networks", *Data Knowl. Eng. (2006)*, doi:10.1016/j.datak.2006.10.005, 2006.
10. http://www.radcom.com/ acessed in 12/01/2006.
11. http://www.openh323.org/ acessed in 12/05/2006.
12. http://dast.nlanr.net/Projects/Iperf/ accessed in 12/19/2006.
13. http://www.netstumbler.com/ acessed in 12/19/2006.
14. S.Haykin,*Neural Networks: A Comprehensive Foundation*, Prentice-Hall, 1998 (Second edition).
15. J. P. L. Araújo, J. C. Rodrigues, S. G. C. Fraiha, F. M. Lamarão, N. L. Vijaykumar, G. P. S. Cavalcante and C. R. L. Francês, "The Influence of Interference Networks in QoS Parameters in a WLAN 802.11g Environment", *Lecture Notes in Computer Science* (paper accepted by publication), 2007.
16. Bayesware Discoverer,Copyright© 2000, Bayesware Limited. http://www.bayesware.com/, accessed in 01/05/07.
17. A. Conceição, J. Li, D. Florêncio and F. Kon, "Is IEEE 802.11 ready for VoIP?", *In 8th International Workshop on Multimedia Signal Processing (IEEE MMSP)*, Victoria-Canada, 2006.