SNMP Parameters for 802.11 Network Performance Measuring

Waldeck Ribeiro Torres
Engineering Department
Fluminense Federal University
Rio de Janeiro – RJ – Brazil
P.O. Box 24.210-240
waldeck@gmail.com

Maria Luiza D'Almeida Sanchez
Engineering Department
Fluminense Federal University
Rio de Janeiro – RJ – Brazil
P.O. Box 24.210-240
mluiza@midiacom.uff.br

ABSTRACT
Reliability and stability are essential conditions for proper operation of any communication system, it is more critical if we talk about wireless networks. Some applications are not fault tolerant for data loss or even synchronization issues; it means that administrators should care not only about application itself but with physical layer as well. By tracking performance and status using open source and standardized protocol is possible to correct or predict possible operational problems at network. In this paper we describe relevant 802.11 SNMP MIB set of parameters with suggestions of optimum values to each one. We also describe some data correlation possibilities, measurement scenarios and cases studies to be used as reference for wireless network administration. The proposal is to correlate gathered data from wireless nodes with environmental information.

Categories and Subject Descriptors
C.2.2 [**SNMP Management**]: Measurement Parameters – *Measurement scenario, Relevant Telecom OID, monitoring.*

General Terms
Management, Measurement, Documentation, Performance, Reliability, Experimentation, Security, Theory.

Keywords
SNMP, Wireless, Optimization, Network, Mesh.

1. INTRODUCTION
Simple Network Management Protocol – SNMP - is a popular and wide deployed protocol for network management built upon open standards running in Client-Server mode. Client is represented by the Network Management System – NMS that communicates with the Agents, acting as Servers, collecting the local information gathered through a specific Management Information Base – MIB – at each equipment.

NMS organizes and arranges remotely gathered data from one or more monitored agents making possible to: determine service availability, data collecting, receive events from agents, storing and reporting on network information. Most professional-grade network hardware come with a SNMP agent built in, called SNMP Enabled device. Agent information is openly available at internet.

SNMP standards are defined in a series of documents, called request for comments or RFCs, proposed by the Internet Engineering Task Force (IETF). Nowadays we have three active versions of the protocol: v1, v2c and v3. The third version has embedded all features from earlier versions with implementation of security schemes.

802.11 And 802.11x refers to a family of specifications [8] developed by the IEEE working group for wireless LAN technology. 802.11 specify an over-the-air interface between a wireless client and a base station or between two wireless clients.

802.11 SNMP MIB information is defined at annex D of ISO/IEC and IEEE Standard [8]; it contains the description of each parameter that may be monitored in 802.11 networks. The relevant information for wireless dependent applications, discussed at this paper, is inside of "Counter32" Group.

These data in conjunction with other collected information from other MIB or external source, like environmental, will compound the vision at NMS used by network administrator to act in order to improve, correct or optimize network performance, reliability and throughput.

This paper describes the relevant SNMP 802.11 MIB object identifier that reflects physical layer performance status parameters in order to be used to develop applications that follow-up network status and provide wireless nodes monitoring.

2. RELATED WORK
There are some researches in wireless network performance around the world but the focuses are mainly based on mobility, throughput or routing issues. The ReMesh Team [1, 12] describes the measurement of their university campus mesh network based on OLSR [17] Expected Transmission Counts embedded route metric. Even it is a reasonable metric and it daemon has a process consumption lower than SNMP daemon, this measurement is just applicable to OLSR protocol networks

SOMITAS 2008, February 14, Quebec, Canada

DOI 10.4108/ICST.AMBISYS2008.2915

and has nothing to do with over-the-air interface measurement part, essential for wireless nodes.

Some research for TCP performance in ad hoc networks has been discussed by Lim, Xu and Gerla [2] since it is severely affected due to link failures during transmission. This investigation help to identify what issues involving multi-path data reception is degrading TCP performance. Such information leads to support actions to be taken in order to minimize impact on whole wireless nodes and should be correlated with data within scenario

Holland and Vaidya et al describes the Explicit Link Failure Notification (ELFN) scheme used to improve TCP performance over multi hop ad hoc networks. It proposes that intermediate nodes notify the TCP sender when a link failure happens [3].

This is a scheme similar to the Explicit Congestion Notification (ECN) technique originally proposed in the wired networks. As this control is located at OSI layer 2 [13], like Lim et al research [2], is not possible to identify what the root cause of TCP datagram failure. Since TCP sender assumes that packet loss is due to congestion [14, 15, 16] instead any kind of problem in lower OSI layers.

Jeremie et al discuss in their paper [4] the quick development of wireless networks and the need of having a framework to help in research about optimization and protocol development for MANET's, mainly for routing algorithms, and useful as basis for other wireless networks monitoring as well.

Vinicius and Ricardo [9] introduces an SNMP agentx extension to follow up and make possible to change and optimize OLSR parameters for a live network and mobile nodes, while Nguyen and Pascale [10] discuss around interferences effects results in Network Simulator2 tool and proposes some improvements on protocol by implementing bandwidth reservation mechanisms, these interference effects simulation is important if we have a ambient system located at a very changing environment.

Some proprietary tools are supplied by access point vendors such as Cisco, Netgear, and Lucent. These tools are typically installed on the device itself and allow information to be accessed via proprietary MIB SNMP through their web interface. Their effectiveness, however, is generally limited by insufficient documentation, the need of vendor specific software and the proprietary nature of such tools.

3. WHAT TO MEASURE

Administration is sometimes a very complicated activity in production networks environments, even worse to apply to wireless network. Define what to measure and pursue the goal to be achieved is the holy graal of network administration personnel around the world

It is well knows that we have, at least, five kind of network management [11]:

- Configuration management
- Fault management
- Security management
- Performance management
- Accounting management

Define what to measure in order to get enough information to perform above actions is quite difficult since there is a lot of information to be processed. The best and rational way to proceed with this task is define previously what kind of management is desired and then collect related data.

In this paper we define what kind of data, in a very basic shape, we should take into consideration to perform fault and performance management. It is based on 3 great groups of parameters: Climatologic, Topographic and SNMP 802.11 MIB as Core of measurement package.

Of course there are some other non described items that help to compound the data interpretation, like the broadly implemented TCP/IP SNMP Management Information Base found in almost all SNMP enabled devices (IF-MIB, IP-MIB, RFC1213-MIB and HOST-RESOURCES-MIB for some implementations).

Besides measured items itself, Network Routing parameters should be changed to optimal values in order to get the desired performance, just keeping in mind that we are dealing with a life behavior network topology sometimes.

4. CLIMATOLOGIC PARAMETERS

Even it is not a main topic of this paper, is essential to comment about this since the network may be affected due to path loss effect in outdoor.

As the transmitted signal traverses the atmosphere its power level decreases at a rate inversely proportional to the distance traveled and proportional to the wavelength of the signal. As the frequency rises, absorption effects become more important. At microwave or higher frequencies, absorption by molecular resonance in the atmosphere (mostly water - H_2O and oxygen - O_2) is a major factor in radio propagation.

Distance/Frequency	915 MHz	1920 MHz	2.450 GHz	5.7875 GHz
100 meters	71.68	78.11	80.23	87.70
200 meters	77.69	84.13	86.25	93.72
500 meters	85.66	92.09	94.21	101.68
1,000 meters	91.68	98.11	100.23	107.70
2,000 meters	97.69	104.13	106.25	113.72
5,000 meters	105.66	112.09	114.21	121.68
10,000 meters	111.67	118.11	120.23	127.70

Table.1- Typical free space path loss

As we can see in table 1 the free space path loss increases as distance and frequency increase. For 802.11b wireless range (2.450 GHz) the loss is around 80dB for 100 meters, it means a reduction of 1x10-8 in power ratio. This loss is even higher in presence of fog and worse when raining. Then, weather conditions and annual climate changes should be considered as factor for wireless performance as well. These data, even not possible to be obtained via standard SNMP MIB, should be collected via external equipment sources.

5. TOPOGRAPHIC PARAMETERS

Another aspect that influences wireless performance is the topographic distribution of nodes. Even it is a matter of

network planning, it is important to know the distribution and positional location of every node related to other ones in order to select special points of relaying route tables, for instance.

A point to mention regarding the importance of topographical awareness is the non-isotropic irradiation pattern for commercial wireless antennae. Isotropic antenna, by definition, equally transmits (or receives) electromagnetic radiation from any arbitrary direction.

Figure 1 shows one typical irradiation pattern for a commercial wireless antenna, we clearly see that beam aperture is 30 degrees. It means that it is possible that 2 antennas in line of sight may not be electromagnetically visible by each other if the ranges of pattern irradiation beam not match.

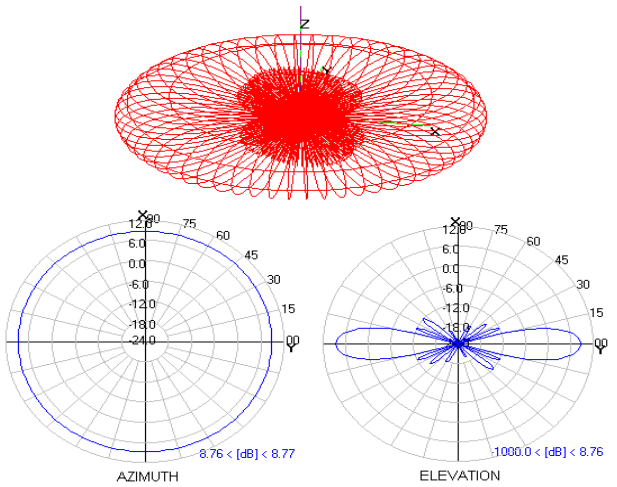

Figure.1- 12-18 dBi Gain Typical Pattern

One of various possible solutions to implement the insertion of this information at MIB, is to use the wide deployed RFC1213-MIB by filling manually the "system" objects fields (OID 1.3.6.1.2.1.1) with information collected during the site survey phase, as described at table 2 below:

Object Identifier	OID	Proposed Usage	Format
sysDescr	1.3.6.1.2.1.1.1	Free text to explain specific conditions/services at node	N/A
sysContact	1.3.6.1.2.1.1.4	Node NMS Group / Adm Region / Adm Name	group1/mpr01/john doe
sysName	1.3.6.1.2.1.1.5	Node Identification / Location	(ID)neighborhood/building/room name
sysLocation	1.3.6.1.2.1.1.6	The Physical Location - coordinates	AA° BB' CC" N/S - XX° YY' ZZ" W/E (Elevation)

Table.2- Proposed use of RFC1213 MIB Fields

So, the awareness of network node distribution, in conjunction with all other information help network administrator for decision making for new nodes, Multipoint Relays or repeaters placement.

6. THE CORE: MIB PARAMETERS

Hereby we describe very briefly each simple network management protocol OID that can be used as measuring parameter making the relation with other OID and how to interpret them.

No formula to be included here, since the idea is just to select and group the 802.11 MIB information to be manipulated later. The figure 2 should be used as a guide for each mentioned SNMP leaf.

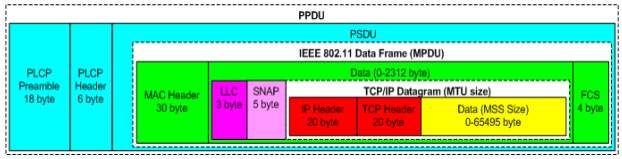

Figure.2-Physical Layer Convergence Protocol Data Unit

6.1 Transmitted Fragmentation

This is an important parameter since we have different MTU for different internet backbone links. Tracking the fragmentation volumes within wireless network we can adjust the MTU in order to improve the payload for each transmitted frame.

SNMP Object Name	dot11TransmittedFragmentCount
Object Identifier (OID)	1.2.840.10036.2.2.1.1
Syntax	Counter32
Max Access	Read-only
Optimal Condition	Tend to zero

6.2 Transmitted Multicast Frames

Some facilities implemented in 802.11 protocol may represent an issue if misused; one example is the DTIM (Delivery Traffic Indication Message). It is commonly referred in some Access Points as "DTIM Interval", with default value 100, and is used to inform Stations in power-save mode to "wake-up" to receive data. As low as this value, more Multicast traffic is generated.

SNMP Object Name	dot11MulticastTransmittedFrameCount
Object Identifier (OID)	1.2.840.10036.2.2.1.2
Syntax	Counter32
Max Access	Read-only
Optimal Condition	Lower as possible

6.3 Number of failed transmission attempts

This counter is incremented whenever a MSDU (MAC Service Data Unit) is not transmitted successfully due to the number of transmit attempts. This value should be as lower than possible.

SNMP Object Name	dot11FailedCount
Object Identifier (OID)	1.2.840.10036.2.2.1.3
Syntax	Counter32
Max Access	Read-only
Optimal Condition	Tend to Zero

6.4 Number successful retransmission

This counter is incremented whenever a MSDU (MAC Service Data Unit) is successfully transmitted after one or more retransmissions, it reflects the situation of radio link status.

SNMP Object Name	dot11RetryCount
Object Identifier (OID)	1.2.840.10036.2.2.1.4
Syntax	Counter32
Max Access	Read-only
Optimal Condition	Tend to Zero

6.5 Number duplicated received frames

This counter is incremented whenever a duplicated frame is received. Duplication condition is indicated by sequence control field. Duplicated frame indicate bad routing table scheme and should be corrected.

SNMP Object Name	dot11FrameDuplicateCount
Object Identifier (OID)	1.2.840.10036.2.2.1.6
Syntax	Counter32
Max Access	Read-only
Optimal Condition	Tend to Zero

6.6 Number of Clear to Send

This counter is incremented whenever a "Clear to Send" is received for each ”Request to Send” sent. The RTS/CTS function is used to control station access to the medium and minimize collisions. The primary reason for implementing RTS/CTS is to minimize collisions among hidden stations. If the packet transmitted by the access point is larger than the set threshold (0 -- 2347 bytes), it will initiate the RTS/CTS function. Recommended value = 500.

SNMP Object Name	dot11RTSSuccessCount
Object Identifier (OID)	1.2.840.10036.2.2.1.7
Syntax	Counter32
Max Access	Read-only
Optimal Condition	Follow Number of Sent MSDU

6.7 Number of Failed RTS

This counter is incremented whenever a “Clear to Send” is not received for each Request to Send sent. High values means that value set it too low or “other side” station is too busy.

SNMP Object Name	dot11RTSFailureCount
Object Identifier (OID)	1.2.840.10036.2.2.1.8
Syntax	Counter32
Max Access	Read-only
Optimal Condition	Tend to Zero

6.8 Number of Failed Acknowledgements

This counter is incremented whenever an expected ACK is not received. Bad link conditions lead this value to increase.

SNMP Object Name	dot11ACKFailureCount
Object Identifier (OID)	1.2.840.10036.2.2.1.9
Syntax	Counter32
Max Access	Read-only
Optimal Condition	Tend to Zero

6.9 Number of Successful Incoming Packets.

This counter shall be incremented for each successfully received MPDU (MAC Protocol Data Unit) of type Data or Management.

SNMP Object Name	dot11ReceivedFragmentCount
Object Identifier (OID)	1.2.840.10036.2.2.1.10
Syntax	Counter32
Max Access	Read-only
Optimal Condition	Follow number of received packets

6.10 Number of FCS error.

This counter shall increment when an FCS error is detected in a received MPDU (MAC Protocol Data Unit). Noisy environments, bad/corroded connectors increase this count.

SNMP Object Name	dot11FCSErrorCount
Object Identifier (OID)	1.2.840.10036.2.2.1.12
Syntax	Counter32
Max Access	Read-only
Optimal Condition	Tend to zero

6.11 Number of Sent Frames.

This counter shall increment for each successfully transmitted MSDU (MAC Service Data Unit). This counter should be used as reference to other counters.

SNMP Object Name	dot11TransmittedFrameCount
Object Identifier (OID)	1.2.840.10036.2.2.1.13
Syntax	Counter32
Max Access	Read-only
Optimal Condition	Not Applicable

6.12 Current TX power Level.

The Transmission Power Level currently being used to transmit data. This parameter should be used as reference in decision making by network administration.

SNMP Object Name	dot11CurrentTxPowerLevel
Object Identifier (OID)	1.2.840.10036.4.3.1.10
Syntax	1…8 (each Level Set in mW)
Max Access	Read-write
Optimal Condition	Not Applicable

7. CROSSING PARAMETERS

To get directions to manage network and take decisions for either optimization or expansion, we need to collect, store and cross these data in a proper way. The very basic for data collection, no matter what kind, is to define the sample rate. It should be the same for all KPI involved to make possible comparison and result crossing.

In this part, we will discuss some sampling and data crossing possibilities for each 802.11 MIB mentioned above and how to compare it with themselves or other non-SNMP parameters, in order to make possible to develop a basic set for NMS setup for network management.

7.1 Transmitted Fragmentation

The sampling rate for transmitted fragmentation checking may be set by hour since it does not suffer external interference. Historical register give support to administrator for network expansion.

7.2 Transmitted Multicast Frames

As transmitted fragmentation, multicast frames just increase network traffic. It also may be followed by hour for the same reasons mentioned previously. It is information that support administrator in network expansion.

7.3 Number of failed transmission attempts

This KPI is related with link quality and link quality for wireless networks is directly related with signal strength and signal/noise value. For mobile nodes we have to cross node positional information with other nodes to verify the increase or reduction of this value. For fixed nodes these data should have, beside positional location from other nodes, the weather conditions at measurement time.

For both, the sample rate should be as short as possible considering the severity of condition. For fixed nodes, historical data is key information to define scenario.

7.4 Number successful retransmission

This counter complements the previous counter and is more useful for fixed nodes due to your less dynamic change condition.

7.5 Number duplicated received frames

A duplicated frame indicates that topology is changing too fast or there is a loop. By following this KPI hourly, it is possible to fix the condition of network changes and correlate data with weather or topographical info to discover the trigger of increase condition.

7.6 Number of Clear to Send

Once detected that number of collision start to increase in function of time, RTS/CTS should be activated at nodes and this KPI should be followed. Optimal conditions are when values closely match with number of sent Frames. Threshold set at nodes make the fine tune to network performance.

7.7 Number of Failed RTS

This counter complements the previous counter. It may also indicate environment noisy conditions. Is useful to results with RSSI Historical data can support to figure out if network growing is related as well.

7.8 Number of Failed Acknowledgements

One of more versatile parameters to tune network peers. Fine adjustment for fixed pairs can be made observing and correlating trends of other parameters like received signal strength, climate conditions or environmental changes in topology.

For mobile users, graph trends in function of node physical positions may help to define boundaries of transmission cell.

7.9 Number of Successful Incoming Packets.

This value over number of received packets and RSSI value at sampling moment help to indicate the maximum limit of coverage of each node for transmission purposes.

7.10 Number of FCS error.

FCS errors should just correlate with RSSI during sample time slice. Very useful to adjust new nodes setup. It is to be used during commissioning phase.

7.11 Number of Sent Frames.

This counter should be stored as basis for previous counters mentioned here.

7.12 Current TX power Level.

This counter should be stored as basis for previous counters mentioned here. It should be paired with RSSI for peer's nodes.

8. CASE STUDIES

To exemplify the usage of these 802.11 MIB SNMP parameters and show how helpful for network administration it may become if data is properly correlated with other available information, we will study some possible scenarios and related optimization actions.

8.1 Different throughput along year.

For this scenario, initially we need to check the behavior of the network. The idea is to verify if these changes are cyclic or not. Obviously we need to arrange data in function of time to observe trends. Continuous increase of *dot11FCSErrorCount* and *dot11FailedCount* in function of *dot11TransmittedFrameCount* indicate that network environment is changing. Good examples are: A build under construction in the line of sight of two or more nodes or trees on your natural growing movement.

If this change occurs in a cyclic way, the idea is to cross above data graphs with other environmental information. An example is to collect and group historical annual or monthly climatologic data, to be compared with rain distribution in order to get any correlation.

Corrective methods would be: create additional mid-way hop points to get around obstacles, elevate antenna position or even change antenna to directional ones for continuous low-performance issues. Cyclic occurrences need a more accurate attention in order to make adjusts accordingly the problem, it may imply in change antenna position, change MPR, divide cell in one or more transmission sectors or change transmission channel.

8.2 Good coverage, low throughput.

In some cases we may have a good signal reception for all nodes, but slow network performance. Electromagnetic interference sources and bad network parameters are main causes of low throughput.

To catch bad network configuration we need to create a graph of *dot11TransmittedFragmentCount* parameter versus *dot11TransmittedFrameCount*, around 5% of fragmentation is quite acceptable, higher values should be adjusted by changing MTU parameters in nodes

Multicast frames may also be followed in same way, as described above. Graphical follow-up of *dot11MulticastTransmittedFrameCount* in function of *dot11TransmittedFrameCount* help, by example, administrators to check if DTIM parameters in nodes should be changed.

Due to nature of wireless network, multipath reception may affect severely performance, mainly if the network has nodes too much near to it other. Administrators should follow the *dot11FrameDuplicateCount* whenever a new node is added or it has your location changed.

8.3 Hidden / Exposed node issue.

This is a well know issue in wireless networks, it can be detected by following-up the behavior of *dot11FailedCount* counter in function of time. Increase in this OID count results may indicate that investigated node is suffering of Hidden / Exposed phenomena. Activation of RTS/CTS helps to minimize collision.

Optimal values for RTS/CTS may be achieved by following *dot11RTSSuccessCount* histograms. Higher values indicate good transmission condition and fewer collisions.

9. CONCLUSION

No matter what the objectives of running applications over wireless networks communications, items like: performance, throughput, reliability and security are essential to be closely tracked in order to avoid threaten the main application usability.

Awareness of online network status is useful to clearly define application behavior when an abnormal environment condition occurs. Some SNMP parameters, like ones described on this paper, when properly tracked and correlated with both topographical and climatologic environmental information can contribute to keep applications running transparently on wireless ambient.

Even not used directly by application, usage of open standardized protocols for network monitoring and administration is a key condition to facilitate integration and benchmarking between other systems besides contribute with system architect in decision making for designing projects.

10. ACRONYMS

CTS = Clear to Send

FCS = Frame Check Sequence

KPI = Key Performance Indicator

LLC = Logical Link Control

MANET = Mobile Ad-hoc Networks

MIB = Management Information Base

MPDU = MAC Protocol Data Unit

MPR = Multi Point Relay

MSDU = MAC Service Data Unit

MSS = Maximum Segment Size

MTU = Maximum Transmission Unit

NMS = Network Management System

OID = Object Identifier

PLCP = Physical Layer Convergence Protocol

PPDU = PLCP Protocol Data Unit (PLCP + MPDU)

PSDU = PLCP Service Data Unit (SDU)

RSSI = Received Signal Strength Indicator

RTS = Request to Send

SNAP = Sub Network Access Protocol

SNMP = Simple Network Management Protocol

11. REFERENCES

[1] Débora C. Muchaluat-Saad, Luiz C. Schara Magalhães, Célio V.N. Albuquerque, Douglas Vidal Teixeira , Diego Passos: Mesh Network Performance Measurements, Universidade Federal Fluminense,2005.

[2] Haejung Lim, Kaixin Xu, Mario Gerla: "TCP Performance over Multipath Routing in Mobile Ad Hoc Networks", 2001

[3] G. Holland and N. H. Vaidya, "Analysis of TCP performance over mobile ad hoc networks," Proceedings of ACM MobiCom'99, Aug. 1999.

[4] Jeremie Allard, Paul Gonin, Minoo Singh and Golden G. Richard III "A User Level Framework for Ad hoc Routing" Dept. of Computer Science University of New Orleans, New Orleans, 2002.

[5] A. Nasipuri, R.Castaneda, and S.R. Das, "Performance of multipath routing for on-demand protocols in mobile ad hoc networks," ACM/Kluwer Mobile Networks and Applications (MONET), vol. 6, no. 4, pp. 339–349, 2001.

[6] M.K. Marina and S.R. Das, "On-demand multipath distance vector routing in ad hoc networks," Proceedings of the International Conference for Network Procotols (ICNP), pp. 14–23, Nov. 2001.

[7] K.Wu and J. Harms, "Performance study of a multipath routing method for wireless mobile ad hoc networks," Proceedings of the IEEE Int'l Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS), pp. 99–107, 2001.

[8] ISO/IEC and IEEE Standard "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications", Annex D "ASN.1 encoding of the MAC and PHY MIB", 1999.

[9] Pacheco, V. M. , Puttini, R. S. . An Administration Structure for the OLSR Protocol. In: Computational Science and Its Applications - ICCSA 2007, 2007, Kuala Lumpur. Proceedings of ICCSA 2007 - LNCS 4706 Part II, 2007. p. 790-803.

[10] Nguyen, D. Q., Minet P. Interference Effects on the OLSR Protocol: NS-2 Simulations Results Third Annual Mediterranean Ad Hoc Networking Workshop, Bodrum Turkey, June 2004.

[11] ITU-T Recommendation M.3400, TMN Management Functions, February 2000.

[12] D. Passos , D. V. Teixeira, D. C. Muchaluat-Saade 2, L. C.Magalhães2, Célio V. Albuquerque: Mesh Network Performance Measurements, Universidade Federal Fluminense,2005.

[13] H. Zimmermann, OSI Reference Model — The ISO Model of Architecture for Open Systems Interconnection, IEEE Transactions on Communications, vol. 28, no. 4, April 1980, pp. 425 – 432.

[14] J. Postel. Transmission control protocol. RFC 793, September 1981.

[15] M. Allman, V. Paxson, and W. Stevens. TCP congestion control. RFC 2581, April 1999.

[16] S. Floyd and T. Henderson. The NewReno modification to TCP's fast recovery algorithm. RFC 2582, April 1999.

[17] Clausen, T. and Jacquet, P. , "Optimized Link State Routing Protocol", RFC 3626, Internet Engineering Task Force (IETF), October 2003.