LOW COST WIRELESS SITE SURVEY SYSTEM FOR *WIRELESS*HART NETWORK DEPLOYMENT

MARCOS G. L. LINDAU[1], IVAN MÜLLER[1], JEAN M. WINTER[1], CARLOS E. PEREIRA[1], JOÃO C. NETTO[2], LEANDRO B. BECKER[3]

1. Department of Electrical Engineering
Federal University of Rio Grande do Sul - UFRGS
Porto Alegre, Brazil
{marcos.lindau, ivan.muller, jean.winter}@ufrgs.br, cpereira@ece.ufrgs.br

2. Institute of Informatics
Federal University of Rio Grande do Sul
Porto Alegre, Rio Grande do Sul
netto@inf.ufrgs.br

3. Department of Systems Automation
Federal University of Santa Catarina - UFSC
Florianópolis, Brazil
lbecker@das.ufsc.br

Abstract— Nowadays the control of industrial processes is mostly made through wired links. This system still plays the main role in the field of automation networks. However this tendency is gradually changing by the use of wireless devices. Due to many advantages over the wired links, such as easy installation and greater flexibility, wireless networks are gradually gaining strength and substituting the cables. This tendency leads to new studies about the matter and the development of tools to evaluate these systems. This paper conducts an approach of the most prominent wireless industrial communication protocol, *Wireless*HART, by developing an application that makes possible the analysis and diagnose of this protocol for general performance (Wireless Site Survey). The developed software and firmware, based on a star topology, measures the Link Quality Indicator (LQI) of the received and transmitted packets and counts the valid ones. As the result, this low cost Wireless Site Survey system allows to identify interferences, either due to others networks or simply due to physical obstacles, and the influence of climatic variations on the network as well. A GPS module can also be attached to the system, for geotagging purposes. The conclusions reveal how important this tool is for planning the insertion of field devices at the automation network.

Keywords— Wireless industrial networks, WirelessHART protocol, Wireless site survey systems.

Resumo - Atualmente, o controle de processos industriais é feito na maioria das vezes através de redes cabeadas. Este tipo de sistema ainda é o mais comumente utilizado. Entretanto, esta tendência está gradualmente mudando para as redes sem fio. Devido a várias vantagens sobre as redes cabeadas, tais como facilidade de instalação e grande flexibilidade, as redes sem fio estão ganhando força na substituição dos cabos. Esta tendência leva a novos estudos sobre o assunto e ao desenvolvimento de ferramentas para avaliar estes sistemas. Este trabalho versa sobre um dos mais proeminentes protocolos de comunicação sem fio industrial, o *Wireless*HART. Uma aplicação para análise e diagnóstico geral do protocolo é desenvolvida (sistema de pesquisa de site sem fio). O software e firmware que compõem a aplicação, baseados em uma rede tipo estrela, medem a qualidade do enlace (LQI) dos pacotes recebidos e transmitidos e contabilizam os pacotes válidos recebidos. Como resultado, este sistema de baixo custo permite a identificação da rede como um todo. Um módulo GPS também pode ser adicionado ao sistema, para georeferenciamento. As conclusões revelam o quão importante esta ferramenta é para o planejamento da inserção de dispositivos de campo na rede de automação.

Palavras-chave – Redes sem fio industriais, Protocolo WirelessHART, Sistemas de pesquisa de site.

1. Introduction

Wired devices play an important role in the field of industrial automation. Nonetheless for some years by now, a change of this tendency has occurred, since the development in electronics allowed the use of more sophisticated devices within more powerful processing in less space (Chen, 2010). The use of wired networks, due to frequently maintenance of wires and connectors, can raise the system costs when compared to wireless networks. Besides that wired devices make the control and monitoring process at a particular location of the industrial plant impossible, affecting the efficiency of the automation network. In the other hand the use of wireless devices is gradually increasing basically for presenting a low cost solution, with less need of maintenance, easy installation and more flexibility (Muller, 2011). The step of a wireless network installation in an industrial environment is preceded by the analysis of how good the radios communicate at specific points. Climate changes and interferences of external sources systems, either due to physical barriers or radio waves in the same frequency spectrum are prejudicial effects regarding the transmission and reception of packets. Therefore, in order to dimension and diagnose these interferences in a determined place, it was developed an analysis tool for wireless networks performance

aiming the industrial environment and, thus, aiming the most prominent industrial wireless standard, the *Wireless*HART (WH) protocol. Main issue of this work, this support tool, also called Low Cost Site Survey System, presents two features for real time measurement of the communication quality, which are: the acquisition of the Link Quality Indicator (LQI) in different channels and the counting of valid packets. Through these features it is expected to identify the most appropriate points inside the plant for the wireless network devices to be positioned. For this task, GPS modules are employed, interfaced with the radios, to easy obtain the exact place in which the radios should be allocated.

The remainder of the paper is structured as follows: section II presents the definition and classification of Wireless Site Survey systems. Section III describes the main goals of the application, explaining its features and functions, while Section IV presents the metric utilized to measure the quality of the link, explaining how it is calculated and obtained. The results, regarding the characterization and validation of the developed tool, are presented and analyzed in Section V. Finally, Section VI presents the conclusions and future works.

2. Wireless syte survey

A wireless site survey, also called an RF site survey or wireless survey, is the process of planning and designing a wireless network, to provide a wireless solution that will deliver the required wireless coverage, data rates, network capacity, roaming capability and Quality of Service (QoS) (SECUREDGE Networks, 2013). The survey usually involves a site visit to test for RF interference, and to identify optimum installation locations for access points. There are three main types of wireless site surveys: passive, active, and predictive.

During a passive survey, a site survey system passively listens to the network traffic to detect active access points, measuring signal strength and noise level. However, the wireless adapter being used for a survey is not associated to any of the existing network. For system design purposes, one or more temporary access points are deployed to identify and qualify access point locations.

During an active survey, the wireless adapter is associated with one or several access points to measure round-trip time, throughput rates, packet losses, and retransmissions. Active surveys are used to troubleshoot networks or to verify performance of post-deployment (TAMOGRAPH Networks, 213).

During a predictive survey, a model of the RF environment is created using simulation tools. It is essential that the correct information on the environment is entered into the RF modeling tool, including location and RF characteristics of barriers like walls or large objects. Typically this means the building floor plans are loaded into predictive site survey software to develop a wireless network design. Virtual access points are then placed on the floor plan to estimate expected coverage and adjust their number and location. Predictive site survey tools will account for building materials, square footage, and the number of wireless users, types of applications, antenna models and other variables to provide a reliable predictive wireless plan for your site or facility (DIGITAL AIR Wireless, 2013). The predictive survey, depending on the situation, can also be onsite. In a context where the customer is doing complex wireless functions or it's in a potentially high interference environment (such an industrial one) an onsite survey should be used.

During an onsite survey, an engineer takes the predictive site survey results and tests the wireless design to prove the design in a real world environment. Things like interference (noise) can be measured onsite where as a predictive design obviously can't do that. An onsite survey can identify any devices that may be causing interference and pinpoints its location and verify a proper wireless design. Costs of onsite wireless survey are around $2,500 to$10,000 per building (SECUREDGE Networks, 2013).

3. Development of a low cost wireless site survey system

A. Main goal of the application

The wireless survey system –meant to be used as a predictive onsite tool – consists basically in a set of devices and an application running in a host to collect information to evaluate the link quality of the network. The devices employ a firmware which is responsible for executing all the low level functions, such as executing the communication machine state, while the software is responsible for the interface with the user, providing commands and information of the network. The tool works at 2.4GHz, more precisely from 2405 to 2480 MHz, and inherits some of the IEEE 802.15.4 PHY layer specifications, like the output power and the number of channels (total of sixteen with, 5MHz bandwidth), more details in IEEE Standard 802.15.4 (2011). The main goals of the tool are: counting the packets which were received by the host node, measurement of the transmitted and received LQI in one determined channel, monitoring of the received LQI for different channels over the time (multichannel scan function) and the control of other parameters from the network, such as speed of data acquisition and output power. Depending on the hardware utilized for the site survey system, the tool can also be able to acquire, in geographic coordinates, the location of the system nodes.

B. Network Formation

Looking for an effective way to measure the communication quality between the devices of an industrial environment, this site survey application forms an independent network from the existent industrial one. Using four slave nodes and one host node inserted at the place of interest with the host node connected to a PC via an USB port (see Figure

1), the tool forms a star topology at the local. The host controls the main task that is to converge and manage all the desired information from the others devices and from itself, while the software application runs. Meanwhile, the LQI of the received and transmitted signal is calculated as well as the number of received packets is counted. Thus all the system will work over the analysis of its own modules, which, once located in strategic points of the plant (where the industrial devices should later be inserted), will simulate the industrial devices performance and the communication quality. The results give the user the conditions to know where the devices should be properly installed and how many of them should be necessary to establish a well formed network. Using the same hardware of the one that is already utilized or planned to be inserted, this tool can also be utilized for hardware validation purposes.

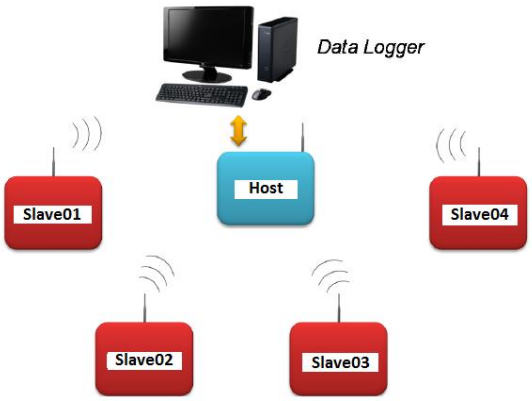

Figure 1 Site Survey System network topology.

C. Site Survey Hardware and Firmware

The firmware is made for the MC13224V platform, a *Freescale Semiconductors* microcontroller. This platform, whose processor is an ARM7TDMI, embeds a low consumption IEEE 802.15.4 radio transceiver with maximum output power of 4.5 dBm. The processing core operates at a rate up to 26MHz and designates its 128Kbyte flash memory (mirrored with 96Kbyte of RAM memory) for upper stack and applications software, which allows the messages to be sent by the host each 255ms for each slave device (when used the standard value for scan speed) for further information see Freescale MC1322x Technical Data (2010). The packet has a 9 bytes size for upload, transmitted from the host to a slave node, and 8 bytes of download, received from the slave. When GPS module is in used a 26 bytes vector is added to the packet. The state machine of the firmware consists of four basic steps, which are: i) the MCU writes the data to be sent to the transmit buffer; ii) it sends the buffer to one slave node; iii) it prepares to receive a message from it and iv) it evaluates whether arrived a valid packet or not. If a valid packet is counted, it transmits the message to the PC and repeats the state machine for the next device, otherwise, it waits a little longer and if, even so a valid packet doesn't arrive, it goes back to the second step. It is important to notice that the communication is done directly between the host device and the slave nodes without the use of transponders. This is due to link quality evaluation between the devices. Figure 2 presents the communication modules that were used for the proposal. They are based on previously developed devices (Muller, 2011) and CEL modules (REF CEL MODULES).

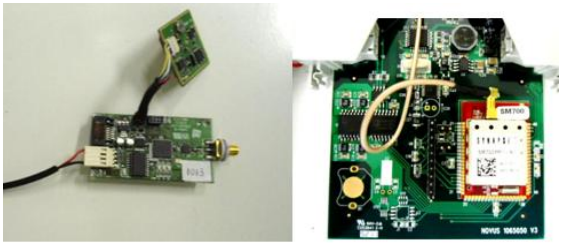

Figure 2 Communication modules (with and without GPS module) employed in this work.

D. Site Survey Software

The site survey software allows passive and active interaction with the radios. Parameters like transmitted and received LQI are not influenced by the software, whose goal is only to collect and save the incoming data. On the other hand, parameters like scan speed, output power, communication channel, geographic position are all controllable by the *Commands_Groupbox* of the software. The scan speed parameter determines the time for executing the communication state machine. Values ranges from 50ms to 255ms. The output power parameter determines the integrated PA output power from -30dBm to +4dBm (plus 20dBm from the nonintegrated PA, then range from -10dBm to +20dBm with a 2dBm resolution). The channel scan parameter (chosen by box object) allows making a channel versus LQI scan during a period of time (also regulated by firmware), set previously as approximately 1 minute per channel. The values can be changed when necessary.

The application GUI has a six tabbed windows. Each tab shows a different parameter of the network. The first tab, Link Quality, displays in dBms the quality of the received and transmitted link during the time, in a range from -96 to -15dBm (Figure 3). The tab incoming data displays all the information in text format separately per device. The LQI_Channel tab displays the link quality indicator as a function of the current channel number and of the time, in a three axis graphic (Figure 4). The Received_Packets tab displays the total number of packets that were received by the host device during the execution of the state machine execution. It is important to note that the counting is made for each slave node separately. The Plant_map tab displays the geographic localization of each device, when connected the GPS module, on the *GoogleEarth* software interface (Figure 5).

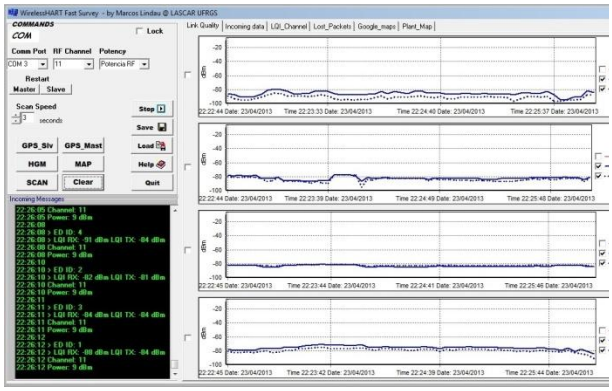

Figure 3. Real time LQI function tab.

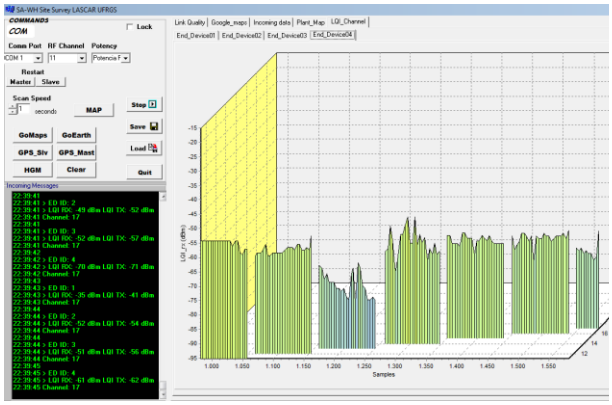

Figure 4 LQI as a function of channel and time.

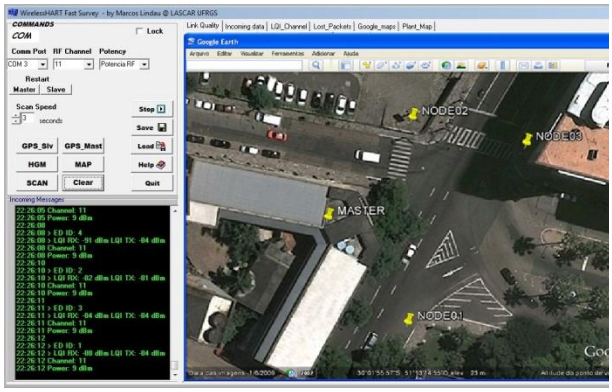

Figura 5. Geographic position of each node from the network.

4. Link quality indicator

A. LQI metric

The accurate determination of the link quality is critical for ensuring the functionalities of a site survey system. There are four primary metrics for capturing the quality of a wireless link: RSSI (Received Signal Strength Indication), SINR (Signal-to-Interference-plus-Noise Ratio), PDR (Packet-Delivery Ratio), and BER (Bit-Error Rate) (Vlavianos, 2008). In this proposal, the low cost site survey system calculates the LQI, parameter related to the RSSI approach, utilizing a primitive which is already implemented in the ROM memory of the MC13224. To understand the concept of LQI, it is important to know the definition of RSSI and the differences between them.

One important factor is that the RSSI is only an indication of the RF energy detected at the antenna. The reported power level could be artificially high because it may include energy from background noise and interference as well as the energy from the desired signal. This situation is worst in an interference prone environment where it is possible to get consistently high RSSI readings yet still have communication errors (DIGI Company, 2013). The RSSI is a signal strength indication and this parameter does not care about the quality or correctness of the signal.

The LQI parameter does not take into account the actual signal strength but the signal quality that is also often linked to the signal strength. This is because a strong signal is likely to be less affected by noise and thus will be seen as cleaner or more correct by the receiver. This metric gives an estimate of how easily a received signal can be demodulated by accumulating the magnitude of the error between ideal constellations and the received signal over the 64 symbols immediately following the sync word. LQI is best used as a relative measurement of the link quality since the value is dependent on the modulation format. To simplify: If the received modulation is FSK or GFSK, the receiver will measure the frequency of each "bit" and compare it with the expected frequency based on the channel frequency and the deviation and the measured frequency offset (TEXAS INSTRUMENTS, 2010). If other modulations are used, the error of the modulated parameter (frequency for FSK/GFSK, phase for MSK, amplitude for ASK, etc.) will be measured against the expected ideal value. There are up to five "extreme cases" that can be used to illustrate how RSSI and LQI work (Texas Instruments, 2010:

1. A weak signal in the presence of noise may give low RSSI and high LQI.
2. A weak signal in "total" absence of noise may give low RSSI and low LQI.
3. A Strong noise (usually coming from an interferer) may give high RSSI and high LQI.
4. A strong signal without much noise may give high RSSI and low LQI.
5. A very strong signal that causes the receiver to saturate may give high RSSI and high LQI.

To measure "link reliability" and not just "signal strength" the application uses the LQI. By definition, the LQI measurement is a characterization of the strength and/or quality of a received packet. The measurement is implemented using a receiver ED (energy detection), which is obtained directly from the host node. The LQI measurement shall be performed for each received packet, i.e. from the packets sent by the slave node and received by the master node and the ones sent by the master node and received by the slave node (IEEE Standard 802.15.4, 2011). It is reported as an integer between 0x00 and 0xFF, where the associated values should be in a range from -96dBm (worst quality) to -15dBm (best quality) for the MC13224.

5. Experimental results

Experiments and tests are being made in order to characterize and validate the developed tool.

A. Software validation

In order to validate the multichannel scan feature of the software, the RF energy of the link is measured as a function of frequency with a spectrum analyzer (SA). The utilized instrument permits to measure the RF power in a range from 100 kHz to 6GHz (for further details see Agilent Users Guide, (2011)). The experiment consists of only one slave node communicating in different frequency channels with the host. The test is made for a complete cycle, from channel 11 to channel 26. To change the channels during the process the implemented feature multichannel scan is utilized. With a 30 seconds interval, settled through the scan speed feature, till the next channel swap, the RF power variation for each channel is plotted as showed at Figure 7. Despite of the success reached in the first channel swapping test, another similar experiment is made in order to analyze this behavior in a tridimensional graph: channel, time and energy (see Figure 8). With the second test it is possible to verify the working of the multichannel scan function during the time axis and, also, that only one slave node is used during the test.

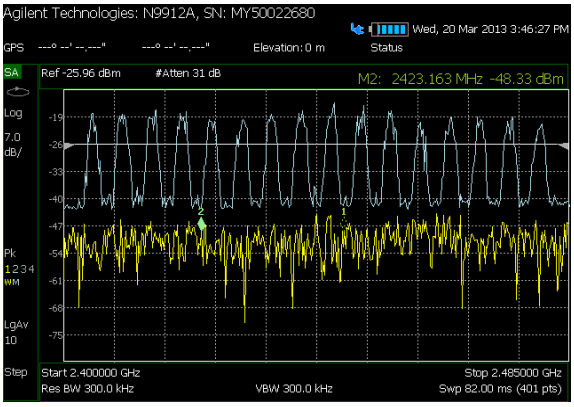

Figure 7 Multichannel Scan Function in 11 different channels.

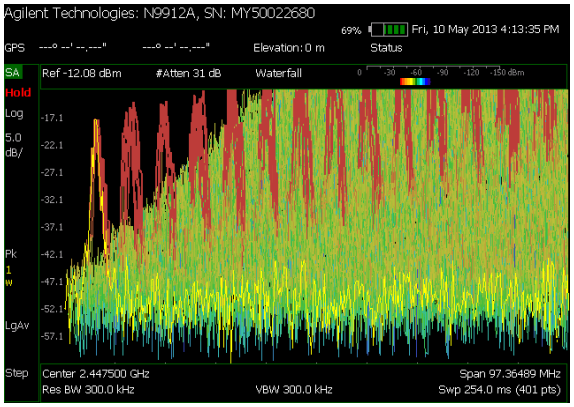

Figure 8 Multichannel scan function during the time.

In order to validate the output power feature, experimental values are obtained using the SA. The output power, settled as a controllable parameter by the application, had already its own RF settings configurations wrote in the ROM with 18 different possible values. This test consists of one node settled as host sending continuously packets. The node is connected to the SA, which measures the device output power, while the standard values are changed by the application. The values are shown in Table 1.

Table 1. Experimental values of output power.

RF Settings	Defined Values(dBm)	Experimental Values (dBm)
0x00	-10	-8.91
0x01	-8	-7.19
0x02	-7	-5.48
0x03	-6	-4.30
0x04	-4	-3.66
0x05	-1	-0.36
0x06	1	0.95
0x07	3	2.36
0x08	4	4.52
0x09	5	4.84
0x0A	9	9.44
0x0B	10	10.52
0x0C	15.50	15.65
0x0D	17	16.40
0x0E	18.5	17.83
0x0F	19	17.98
0x10	21.70	19.68
0x11	23	20.66
0x12	24.50	20.85

An empirical comparison between the pre-settled and experimental values is made by plotting both curves in the same graphic, with real and experimental ones.

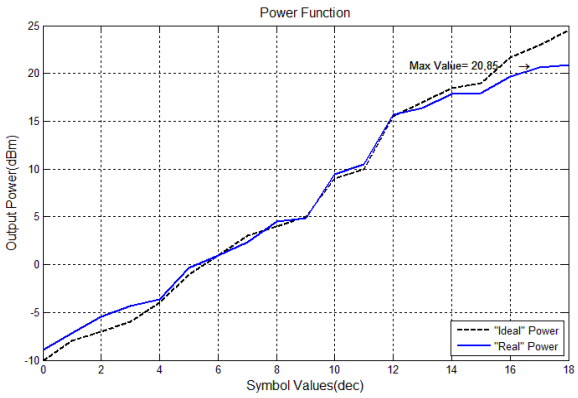

Figure 9. Comparison with theoretical and real power measurements.

For values above 20 dBm the PA saturates thus the saturation occurs (see solid curve).

B. Hardware Limitations

To characterize the maximum reach between two devices in a wide open area, a so called reach test is performed. In a place far away from urban centers without 2.4GHz interference, two communication

modules are positioned with complete visibility between them. The maximum distance obtained is about 2000 meters, with an LQI of -96dBm (received by the host) and the higher power value (20 dBm). The GPS uncertainty at the measurement instant is around 5 meters. Figure 7 shows the RF range experiment.

Figure 7. Geographic positions of the nodes in the range evaluation.

6. Conclusions

In this work, a Low Cost Wireless Site Survey System is developed and tested to perform a WH previous deployment.

The system is useful as an onsite predictive wireless survey tool, where data is collected through the real field experiments. During a long term period, this application allows to reduce time and cost in the planning and commissioning stages, making the development of a automation network much easier and efficient.

Acknowledgment

We would like to express our gratitude to CNPq and Capes, our governmental commissions for post graduation and research on their support for this work. Also we are grateful to Finep for funding of the E3, SA-WH project.

References

D. Chen, M. Nixon, A. K. Mok., *Wireless*HART: Real-Time Mesh Network for Industrial Automation. Springer, 2010

Muller, I.; Netto, J.C.; Pereira, C.E., "WirelessHART field devices," Instrumentation & Measurement Magazine, IEEE , vol.14, no.6, pp.20,25, December 2011

SECUREDGE Networks.; Web page of technical support IT solutions blog [Online] Acessed in Mai of 2013. http://www.securedgenetworks.com/secure-edge-networks-blog/bid/53242/How-much-does-a-wireless-site-survey-cost

TAMOGRAPH Networks.; Web page of technical support from Tamograph solutions [Online] Acessed in Mai of 2013. http://www.tamos.com/htmlhelp/tg/

DIGITAL AIR Wireless Web page of technical support from Digital Air Wireless solutions [Online] Acessed in Mai of 2013. http://www.digitalairwireless.com/wireless-network-services/wireless-site-surveys/post-installation-wireless-survey.html

IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)," *IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006)* , vol., no., pp.1,314, Sept. 5 2011

Freescale, MC1322x. Technical Data. Revision 1.3,2010.

Vlavianos, A.; Law, L.K.; Broustis, I.; Krishnamurthy, S.V.; Faloutsos, Michalis, "Assessing link quality in IEEE 802.11 Wireless Networks: Which is the right metric?," Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on , vol., no., pp.1,6, 15-18 Sept. 2008

DIGI Company. Web page of technical support from Digi Solutions – Knowledge Base Article [Online] Acessed in Mai of 2013. http://www.digi.com/support/kbase/kbaseresultdetl?id=2084

Texas Instruments Company. Web page of technical support from TI E2E Community [Online] Acessed in Mai of 2013. http://e2e.ti.com/support/low_power_rf/w/design_notes/calculation-and-usage-of-lqi-and-rssi.aspx

Aglient Field Fox RF Analyzer N9912A User's Guide; 16.2.2011