An Experimental Analysis of Zigbee Networks

E. Dalila Pinedo-Frausto
Computer Science Dept.
CICESE Research Center
Ensenada, México
epinedo@cicese.mx

J. Antonio Garcia-Macias
Computer Science Dept.
CICESE Research Center
Ensenada, México
jagm@cicese.mx

Abstract— **Zigbee has been touted as a technology that can be embedded in a wide range of products and applications across consumer, commercial, industrial and government markets. However, given the varying requirements for applications in these sectors, we question if Zigbee can really satisfy the needs of these diverse markets. We performed several experiments using commercially available Zigbee software and hardware in order to determine several aspects concerning the reach and limitations of the technology. We analyze the results of our tests and show evidence of where Zigbee can be applied and where it is not suited for.**

Keywords-ZigBee, IEEE 802.15.4, ZigBee Alliance

I. Introduction

As stated in their website, the IEEE 802.15.4 WPAN Task Group 4 was chartered "to investigate a low data r[1]ate solution with multi-month to multi-year battery life and very low complexity. It is operating in an unlicensed, international frequency band. Potential applications are sensors, interactive toys, smart badges, remote controls, and home automation". The 802.15.4 specification [1] deals with physical and MAC layer aspects, so upper layers are left to other parties to define and implement; one of such parties is the Zigbee Alliance, formed by a group of companies interested in defining a low-cost, low-power, wireless networking standard. Beside dealing with the technical aspects of the network, security and application layers, the Zigbee Alliance also provides interoperability and conformance testing specifications, as well as promotion efforts to market the Zigbee standard.

The Zigbee Alliance states that Zigbee technology will be "embedded in a wide range of products and applications across consumer, commercial, industrial and government markets worldwide". However, given the varying requirements of applications for these sectors, it is only natural to ask if Zigbee can be a one-size-fits-all solution covering these requirements. For instance, an industrial application for automatic process control would have far more strict requirements in terms of reliability, latency and scalability than a home automation application.

Even though there have been some papers published [2], [3], [4] that report on the performance of Zigbee networks, most of their results have been obtained with simulators and theoretical analyses. We feel that these results should be complemented with others obtained via experiments with real implementations of Zigbee networks. This would help in having a better understanding about the capabilities of the Zigbee technology and in assessing its applicability to various markets.

This paper intends to point out the capabilities of Zigbee, as it is currently specified and implemented. We provide an unbiased overview based on experiments with commercially available hardware and software. We think this is valuable because potential Zigbee users can know what to expect in actual deployments. We do not intend to provide solutions for any shortcomings found, we just want to point out the current state of things. We believe that understanding a situation is the first step in taking an evolutionary path. We have organized out paper as follows: in section II we give an overview of Zigbee, highlighting its most important features. Section III presents the features of Zigbee that will be tested, the methodology for conducting the tests, and the experimental setup. The actual tests and its results are presented in section IV, and a discussion about them is given in section V. Concluding remarks are then given in section VI.

II. Zigbee and ISA 100 Overview

The Zigbee Alliance designed Zigbee with very different application environments in mind: home automation, commercial buildings, industrial automation, and medical instrumentation. Given this diversity, the first problem the Alliance has been trying to solve is the interoperability between different vendors, which is why their tests suites have had more emphasis on compatibility than on the performance of the protocol.

ZigBee offers a layered architecture based on the MAC and physical layers of the IEEE 802.15.4 standard. This design offers low power consumption and guarantees a longer battery life, which is one of the most important issues of wireless networks. Since ZigBee is based on IEEE 802.15.4 it inherits a low data rate, and a reception distance of about 100 meters (depending on environmental conditions).

For the upper layers one of the most important characteristics of ZigBee is the possibility of using one of two types of routings: mesh and tree. This gives the application

Manuscript received May 15, 2008. This work was supported in part by the Mexican Science and Technology Council (CONACyT).

Dalila Pinedo-Frausto finished her M.Sc. at CICESE Research Center and is now at Ubilogix in Ensenada, México (corresponding author phone: +52-646-175-7014; e-mail: dalila@ ubilogix.com).

J. Antonio Garcia-Macias is a researcher at CICESE Research Center, Ensenada, Mexico (e-mail: jagm@cicese.mx).

978-1-4244-2413-9/08/$25.00 ©2008 IEEE

designer much more freedom to get the maximum gain out of each option depending on the very own needs of the solution they develop.

The protocol also offers a framework application to make easier and faster the development of simple standard applications. Also, in order to promote the reuse of already existing functionalities, libraries and profiles have been created to facilitate the construction of the most frequently needed devices within the application environments that ZigBee has been created for. This is why ZigBee can not only be considered as a simple set of commands for the communication between sensor nodes, but as a whole framework that allows the creation of standard devices, assuring the interoperability between different manufacturers.

Analogous to the IEEE 802.15.4 standard, devices in the network are known as Full Function Devices (FFD) or Reduced Function Devices (RFD). A ZigBee network has three types of devices: two of them, the coordinator (ZC) and the router (ZR), are FFD and there is a RFD called end device (ZED). The ZC is the only one that can form a ZigBee network and is unique within the network. The ZR has the same routing capabilities as the ZC, but can only join a network, never form it. A Zigbee end device, or ZED, can only join the network and has no capacity for routing, it also should always be associated to a parent to be able to communicate and its most important characteristic is the capacity to shut down its radio during defined periods of time to save energy; while it is off its associated parent receives messages addressed to it and saves them so that they can be delivered when the ZED radio is turned on and it requires data from its parent.

The ZigBee architecture, showed in Figure 1. , has a layered design in which every layer offers services to the next higher layer through Service Access Points (SAPs). There are two kinds of SAPs: the Data Entity (DE), dedicated to the transmission of data between layers, and the Management Entity (ME) for the transmission of control and services administration commands.

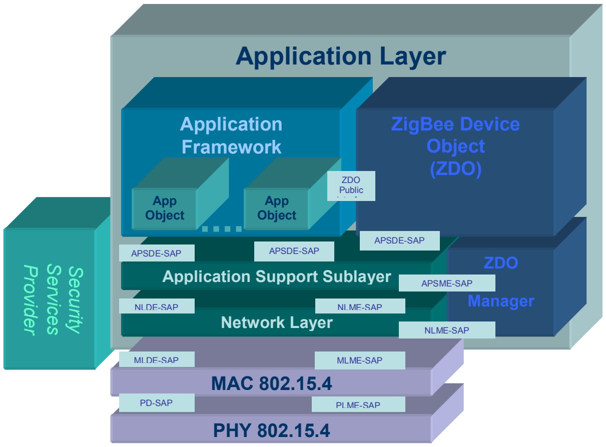

Figure 1. ZigBee Architecture

As mentioned before, the ZigBee protocol sits on top of IEEE 802.15.4 PHY and MAC layers (Fig. 1). Its next higher layer is the network layer (NWK) in charge of the formation of the network, addresses administration, routing, devices discovery, as well as security application and services. On top of the NWK layer there is the Application Support Sublayer (APS) and the ZigBee Device Object (ZDO) with its vertical management plane. The APS layer with its two SAPs (APSME and APSDE) offers an interface between the NWK layer and the upper layers; its main task is to generate the Protocol Data Unit (APDU). It is also in charge of group address filtration, secure transportation of messages, rejection of duplicates from the application, authentication of links, security keys, and administration of devices to groups.

The ZDO is a basic functionality class that offers an interface between the application objects, the profile and the APS layer. It initializes the APS and NWK layers and the Security Services Provider (SSP), this last one used to encrypt and decrypt messages. The main objective of the ZDO is the administration of basic functions of any application device and it is also an interface to the variety of functionalities of ZigBee.

As mentioned before, the ZigBee protocol contains an application framework for the application objects. To define the framework for the specific application environment there is an application profile and a ZigBee Cluster Library (ZCL). The application profile describes the types of devices and the specific clusters from the ZigBee library needed to implement a standard functionality. A cluster is defined as the specification of a distributed functionality in two types of devices: a server and a client. This way a developer can use the standard functionality of the ZCL and also create its own clusters for his own profile, these clusters can also be registered as part of the ZigBee protocol and obtain an specific identification number for the profile.

TABLE I. ISA USAGE CLASSES FOR WIRELESS SENSOR NETWORKS PROTOCOLS.

Safety	Class 0: Emergency action (always critical)	Importance of message timeliness increases
Control	Class 1: Closed loop regulatory control (often critical)	
	Class 2: Closed loop supervisory control (usually non-critical)	
	Class 3: Open loop control (human in the loop)	
	NOTE Batch levels* 3 & 4 could be class 2, class 1 or even class 0, depending on function *Batch levels as defined by ISA S88; where L3 = "unit" and L4 = "process cell"	
Monitoring	Class 4: Alerting Short-term operational consequence (e.g., event-based maintenance)	
	Class 5: Logging and downloading/uploading No immediate operational consequence (e.g., history collection, sequence-of-events, preventive maintenance)	

Since Zigbee was conceived for a wide range of wireless applications, we decided to compare with a standard defined for a focused set of requirements, more precisely for the strict requirements of industrial applications. ISA a leader organization in standards for automation formed in 2005 has formed the ISA 100, a committee for wireless systems for industrial automation. In 2006 this committee delivered two drafts of requirements for industrial wireless sensors networks [7] and [8], which we used as a guideline for the design of our tests. In these drafts, ISA also presented its usage classification of industrial wireless sensor networks. We will eventually refer to this classification when discussing the results of testing ZigBee.

III. Experimental Setup

For our experiments we used the BeeKit package offered by Freescale; this package features a user-friendly environment to aid in the creation of applications based on Freescale´s Simple MAC (SMAC), IEEE 802.15.4 PHY/MAC and BeeStack Zigbee protocol stack. In order to have tests with a ZigBee like application design, we used some of the ZigBee Alliance’s Test Profile 3 (TP2) application commands (e.g., TransmitCountedPackets, an internal) and we implemented two more commands to have full control over the application. Also we used Freescale’s ZigBee Test Client (ZTC) application to measure the quantity of data requests and confirms between layers that passed through APSDE-SAP, NLDE-SAP and MLDE-SAP handlers. A tool that was used extensively during our experiments is the Daintree network analyzer; this combines a USB device that captures packets in a wireless network for a configured channel and graphically shows the structure and contents of Zigbee/802.15.4 packets. On the hardware side, we mostly used Panasonic's PAN802154 module a communication device fully compliant with 2.4GHz ISM band requirements, and ready to be used with Freescale's ZigBee protocol BeeStack. Also, for comparison in some tests we used Freescale’s 13192-EVBs. For maximum WiFi networks noise avoidance, the experiments were done in channel 26 of IEEE 802.15.4 standard.

The outdoors experiments were conducted in a vast (approximately 1000 m^2) and empty parking lot, in order to avoid interferences, and mounting the nodes on top of wood poles with a height of over 1 meter. For the indoor experiments we used the third floor of a 3-story building; distance tests were conducted in a 50 m long hallway, other experiments were conducted in a 6x25 m office space.

IV. Experiments and Results

The development of the tests was based on the idea of verifying the actual capacity of the ZigBee protocol in industrial control and monitoring applications. We first did a revision of the theoretical characteristics of 4 of the most important wired sensor network protocols used today in industry: Ethernet/IP, FF H1, CAN and AS-i. The decision to verify the characteristics of this specific sensor network protocols is based in the classification of the wired communication protocols in industry [6]. Also, as mentioned in the overview section we used the ISA requirements draft as a guideline to the design of our tests. Then, we performed 10 different tests with a focus on some of the most important characteristics of a sensor network, such as bandwidth, data integrity, time response, effects of network size and mesh routing trade off, with variations on topology, data rate transmissions, payload size and distance.

TABLE II. The main tests used in our experiments.

Test Number	Test focus	Variation
1	Data Integrity	Start topology
2		Multi-hop
3		Distance
4	Time Response	Multi-hop
5		Distance
6	Mesh routing	Recovery time
7	Connection Time	Start topology
8		Tree topology
9	Simultaneous Connections	
10	Network Size	Connection

For the star topology tests we used either only ZEDs or ZRs to form the star around the ZC. The maximum depth in multi-hop messages is 5. The minimum payload used in the tests is 1 byte and the maximum payload, is the one Freescale’s BeeStack 2006 can deliver in the APS layer: 80 bytes.

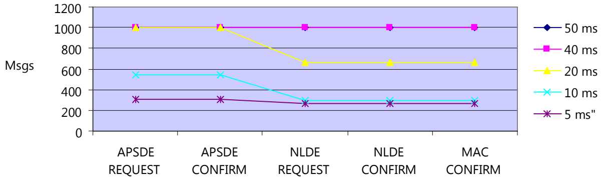

Figure 2. Data requests and confirms passing through SAP-Handlers using different transmission periods.

After a revision of wired sensor networks characteristics, we decided to test using transmission periods of 5, 10 and 20 milliseconds. However, the results of the initial tests show that nodes were not capable to transmit with these periods, as we can observe in Fig. 2. These results made us increase the transmission periods to 40 and 50 milliseconds. Fig. 2 shows the number of messages passing throw the SAP handlers of the stack, we were able to count these messages using the ZTC application mentioned in the ZigBee overview section. In Fig. 2 we can also notice that many NLDE requests with transmission periods of 20 ms and under were lost. A probable reason for this problem is that the tasks queue in the network layer gets filled up to its limit and is not capable of creating the correspondent MAC layer requests to send the messages over the air.

To calculate the actual throughput of ZigBee we started by testing the simplest case of a two nodes network, and then increased the number of children until the maximum of 6 ZRs. First we sent messages varying the transmission period between messages. We used periods going from 5 to 50 ms and found out that only in periods of 40 ms or bigger we could receive 100% of the transmitted messages, with a minimum payload (1 byte). Then for the maximum payload (80 bytes) case, 50 ms was the smallest period that let us receive all the messages. To know how many messages the nodes could transmit in 1 second, we can use the results of test 1 with the 5 ms period since this would make the node try to send messages as soon as it could, so with a maximum payload the number of transmitted messages per second is 15 and 40 with a minimum payload, which corresponds to a 13.4 kbps and 9.4kbps data rate respectively. From these results we can notice two important issues, first only 6% of the 250kbps are being used in the best case with a maximum payload. And second we may need the double of time to send the same quantity of messages with the maximum payload, but we are sending 79 data bytes more over the air which is 4.2 times the total bytes over the air. This means the delay on the transmission is not mainly caused by the increase of data, but by the headers creation. This is more obvious in Fig. 3 and Fig. 4, as we can notice that even though the quantity of transmitted messages does not differ much when the payload grows, the payload bits really do so, meaning that the bigger problem is not the size of the payload, but the creation of the headers.

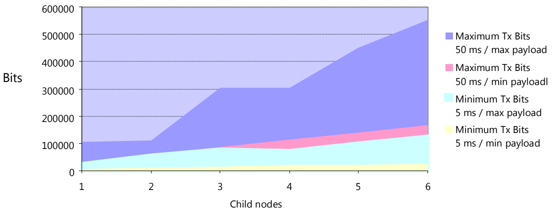

Figure 3. Data integrity with star topology test, bits transmitted over the air

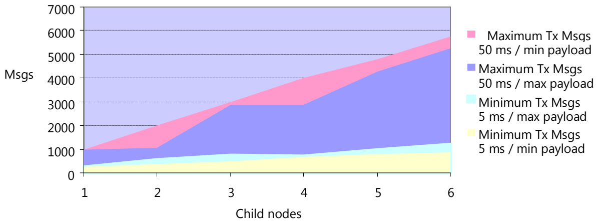

Figure 4. Data integrity with star topology test, messages transmitted over the air

One important result of increasing the children number of the ZC is the obvious limit for reception of messages as Fig. 5 shows. In Fig. 5 we can see a limit of 1650 messages with a 50 ms period an minimum payload. We must remember that each child sends 1000 messages with a specified transmission period, then for example with a period of 50 ms a maximum of 5 messages were sent to the ZC, in total after 50 seconds the ZC should have received 5000 messages, 1000 per children, but after obtaining the messages count of the application in the ZC, we can see it only received a maximum of 1650 messages.

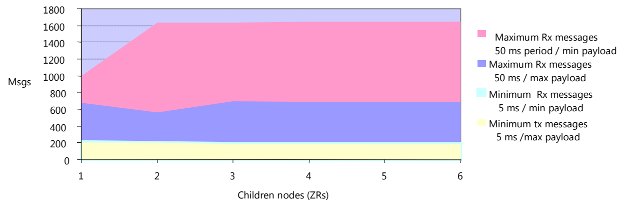

Figure 5. Received messages by ZC in a star configuration

One important ZigBee feature is its multi-hop transmission capacity, but messages might get lost in the process of being forwarded. We tested the multi-hop capacity of ZigBee by sending messages between two nodes being 5 hops away as shown in Fig. 6. First we did the set up of the logical network topology, then ZR1 sends 1000 messages to ZC, after that and without reseting the count on ZC, ZR2 sends another 1000 messages to ZC, and so on until ZR5; that is why in Fig. 7 and Fig. 8 the received messages count increases with the number of hops.

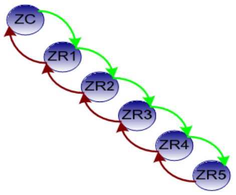

Figure 6. Configuration for multi-hop tests

We found out that for transmission periods of 40 and 50 ms, and with minimum payload, 100% of the transmitted messages were received at the final destination. These results can be seen in Fig. 7.

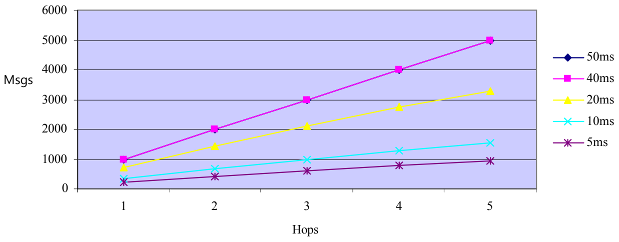

Figure 7. Received messages with minimum payload.

However, as shown in Fig. 8, with a maximum payload size and a 50 ms transmission period 1% of the messages could not be received by the ZC, while for the 40 ms period we had losses of up to 52%.

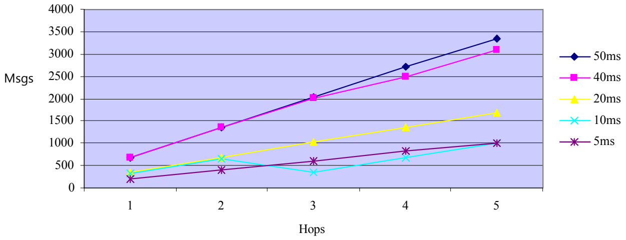

Figure 8. Received messages with maximum payload.

For the data integrity varying distance test we sent messages also with different transmission periods and we separated the nodes increasing 1 meter each time up to 10 and then with increments of 10 meters up to 90, as shown in Fig. 9.

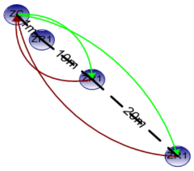

Figure 9. Configuration for time response tests.

This test was performed in the exterior and interior environments mentioned in section III. The results in Fig. 10 show that in an exterior environment and setting the network on the ground the maximum possible distance was 10 meters with loses up to the 30% of the transmitted messages after 5 meters.

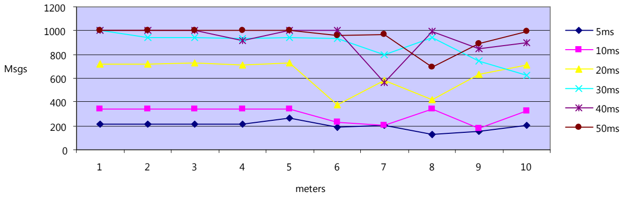

Figure 10. Received messages in exterior, network set up on the ground.

Repeating the test with 1 meter of elevation above the ground gave better results, as we received 100% of the transmitted messages at a distance of 90 meters.

In the interior environment we also repeated the test from 1 to 10 meters on the ground using the two different modules mentioned in section III. In this test with Panasonic's board we observed losses of up to 10% at 15 meters but of 80% at 20 meters. For Freescale's 13192-EVB we had better results without any losses at 20 meters, which was our maximum possible measurement due to the physical conditions of the environment.

For critical industrial applications time delay is one of the most important characteristics of a sensor network. We tested 2 important factors that contribute to time delay: distance and multi-hop transmission. To measure time response delays we used the Daintree SNA software time stamps, whose minimum possible measurement is 1 ms. For the Time response – Distance test, the time response was taken as the difference between the time stamps of a Transmit Request message and its response (in our test application) a ZigBee TP2 command: Transmit Counted Packet message. We found a maximum and minimum delay of 49 and 46 ms respectively when testing in the exterior environment, but the results shown in Fig. 11 do not show the variation in time delay response to be strongly correlated with the distance. Since the variation is not uniform after 30 meters it might have been a problem in the sniffer hardware reception. The maximum distance we could use to perform the test was 75 meters, since this was the maximum capacity of the set up we had with Freescale's sniffer hardware.

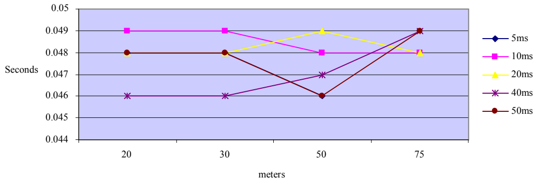

Figure 11. Time response variation with distance in exterior environment, network set up 1 m above the groud.

For the multi-hop test we measured every hop transmission time stamp and we found the average time delay for a hop with a maximum payload to be 17.75 ms and 17.5 ms for a minimum payload. These results are shown in Fig. 12 and prove again that the main cause for the lost messages on data integrity tests is the creation of frames, since a simple retransmission does not take much longer for a maximum payload than for a minimum payload.

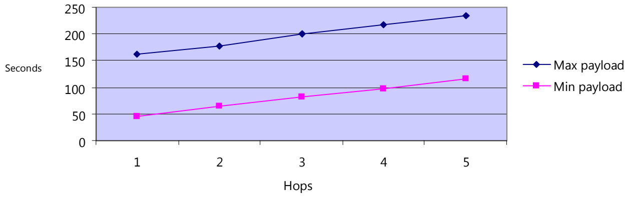

Figure 12. Multi-hop delay.

One of the most important characteristics of ZigBee is its self-healing capacity through mesh routing. So we tested the time cost of mesh routing by measuring the elapsed time between the elimination of one path and the search and creation of another. The test set up uses a diamond topology network as the one shown in Fig. 13. To perform the test we first start sending messages from ZR3 to ZC through ZR1, after some time we turn off ZR1 so that ZR3 needs to find another path to deliver the messages to ZC. The path must be found through ZR2, and we measure the time between the last message sent through ZR1 and the first sent through ZR2; this is what we called mesh routing recovery time.

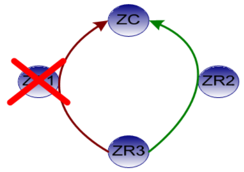

Figure 13. Mesh routing test layout.

The results of this test are shown in Fig. 14 and there we can notice a maximum delay of 126 ms to find the new path when using a 20 ms transmission period. We can also notice the delay gets smaller when the transmit period between the messages is bigger than 20 ms; probably the bigger period permits the node to focus its resources such as memory and processing, to find the new path. The minimum delay we found was 85 ms. When we used maximum payload messages for the tests, with transmit periods under 20 ms it was not possible for the node to find the new path probably for the lack of memory to perform the search. Though for the 20, 40 and 50 ms tests, the node found the new path in less than 90 ms.

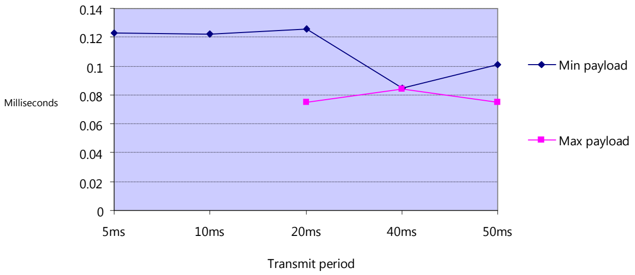

Figure 14. Mesh routing test results.

Another important characteristic of a network is the number of devices that can be connected to it. ZigBee, having 16-bit addresses, can theoretically connect up to 65532 devices, but in reality bandwidth is what limits the number of devices the network can have. It has been shown [4] that the actual bandwidth for a ZigBee network is 157 kbps after taking into account acknowledgements time, headers and inter-frame delays. This means that for a 6 nodes ZigBee network the maximum bandwidth would be 25.4 kbps per node. Probably this is much more than what is needed by many applications, although we must have in mind that for a 1000 nodes network we might at most be able to send 1 message every second without collisions if the area of the network is small enough to let each of the nodes listen to all the other nodes in the network. Anyhow, most of the wired sensor networks we studied had a capacity no bigger than 32 devices. This size was tested in the ZigBee network just by joining the 32 devices and succeeded without any important issues.

Since one of the main problems when increasing the network size is the time it takes to deploy it, we tested the connection time using only ZRs to grow a network in both tree and star topologies. Since a ZR, just like the ZC, has the capacity to respond to a MAC Beacon Request command, and every ZR trying to join the network must save and check every response to decide which is the best node to join, then the time to join the network increases with the number of responding nodes, until it reaches the limit of responses the node can process.

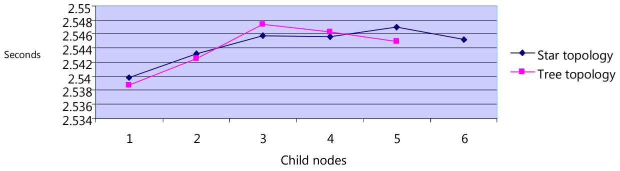

Figure 15. Results of connection time for star and tree network topologies.

For the results shown in Fig. 15, the time of connection increases until the third node is connected, which is the maximum number of Beacon Responses the node can save. From the third to the fifth or sixth ZR connected in the tree or star topology, the difference in the connection time is not bigger than 2ms but between the minimum and maximum time to join the difference in a star topology is 7.2 ms and in a tree topology is 8.6 ms. The maximum time to join was 2.57 seconds and the minimum 2.538. In order to verify that the increase of connection delay was really was due to the responses of other ZRs, we performed the test again on the star network using ZEDs, which do not respond to MAC Beacon Request commands. We found that the average time to join was 2.54 and the difference between the minimum and maximum time to join was 5 ms, which is much less than the 32 ms difference between the maximum and minimum values for the network formed with ZRs.

Since many industrial and commercial applications require a simultaneous connection of all nodes in the network, we also verified how many nodes could be able to join if turned on simultaneously. For this test, we found that the maximum number of joined nodes we could get was 3. The main problem we found in the joining process is the lack of a timeout period for an Association Response command reception. ZigBee uses the IEEE 802.15.4 MAC association process in which the joining node and the responding node inside the network share the network information through the Association Request and Association Response commands. So for instance, when we tried to join 5 nodes to the network, we noticed that the ZC was able to respond to all 5 Association Requests from the joining nodes, but after receiving the Data Requests from them the ZC could only respond to three, leaving the rest of the nodes waiting for an Association Response command. This is more a MAC problem than a ZigBee problem, though it must be considered due to the heavy dependence of Zigbee on IEEE 802.15.4.

V. Discussion

The experiments presented in the previous section show some interesting results concerning the reach and limitations of Zigbee. The use of layered protocol architectures for devices with strong resource limitations has been debated; some consider that a more tight (or even monolithic) architecture should be used, favoring cross-layer optimizations. Zigbee uses a layered approach and our tests show that there is a very considerable overhead for message processing across layers, resulting in increased latency and reduced bandwidth utilization (which is limited by the capacity of the nodes to process incoming/outgoing messages). Our tests show that reception is considerably slower than transmission, and that in all cases (even varying message size) the data rates are much lower than the theoretical value of 250 Kbps; in fact, for a maximum message size Zigbee shows data rates of around 8.3 kpbs, which would be useful for the interconnection of field devices similar to AS-i for instance, but not for more demanding applications found in CANs such as Profibus and similar ones.

Even though the theoretical maximum size of a Zigbee network is over 65000 nodes, in practice, the problems related to bandwidth and delays that network growth can incur should be considered. For instance, our tests showed that for a star network the hub was not able to handle more that 1650 messages. Thus, the actual transmission and reception capabilities of the nodes greatly impact the possible size of the network. For the case of multihop communications, we measured average retransmission times of 17.25 ms. As a network grows and more hops are introduced, the added delays would constitute considerable overhead.

As message sizes can vary from 25 to 128 bytes, care should be taken with the transmission rate in order to avoid reception overcharge, delays and retransmissions. Our tests show that minimum-sized messages can be safely sent at 40 ms rates, but for maximum-sized messages the minimum sent rate is 50 ms. Of course, these rates and message sizes place Zigbee well below the level of wired networks commonly used in industry and other sectors.

Auto-recovery is a feature of Zigbee that gives it an advantage over wired networks, such as AS-i and CAN, as these can not recover routes unless there is an explicit duplication of them. However, we have found recovery times to be between 75 ms and 126 ms; this measure was only for a simple route of two hops and the time will grow with the number of hops in the route.

VI. Concluding Remarks

Based on the results from the experiments we have performed, and from other aspects we have analyzed, we can situate Zigbee as a protocol well suited for applications in classes 3 to 5 according to the usage classes defined by ISA (cf. Table 1). However, it would not be adequate for emergency applications or for closed loop control applications (classes 0 to 2). Up to now, the Zigbee Alliance has focused on the development of Zigbee to properly meet the requirements of home automation applications, and also on achieving interoperability between devices from different vendors. As these goals are met, new markets (including the industrial one) will surely be addressed and performance requirements will take a more prominent place.

References

[1] Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs), IEEE Std. 802.15.4, 2006.

[2] F. Cuomo, S. Della Luna, U. Monaco, T. Melodia, "Routing in ZigBee: benefits from exploiting the IEEE802.15.4 association tree", IEEE ICC 2007, Glasgow, Scotland. June 2007, pp. 3271-3276, 2007.

[3] Wheeler, A. "Commercial Applications of Wireless Sensor Networks Using ZigBee", IEEE Communications Magazine, Vol 45, No 4, April 2007. pp 70-77.

[4] M. Kohvakka, M. Kuorilehto, M. Hännikäinen, T.D. Hämäläinen, "Performance analysis of IEEE 802.15.4 and ZigBee for large-scale wireless sensor network applications". 3rd ACM international Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor and Ubiquitous Networks. Torremolinos, Spain, October 2006.

[5] Sun, T., L. Chan, C. C. Han, G. Yang, y M. Gerla. 2006. Measuring effective capacity of IEEE 802.15.4 beaconless mode. IEEE Wireless Communications and Networking Conference. pp 493-498.

[6] Verhappen, I. 2002. High Speed Ethernet - The enterprise integration enabler. IEC Pros Inc. Technical report. 22 p.

[7] ISA-SP100.11, 2006, Wireless for industrial process measurement and control. Call for Proposal. CFP. 24 p.

[8] ISA-SP100.11, 2007, Technical requirements for time-critical securable wireless industrial field networks. 1. SP100.11 Draft. 90 p.