A Proposal for Zigbee Clusters Interconnection based on Zigbee Extension Devices

Ángel Cuevas, Rubén Cuevas, Manuel Urueña, and David Larrabeiti

Departamento Ingeniería Telemática. Universidad Carlos III de Madrid
{acrumin,rcuevas,muruenya,dlarra}@it.uc3m.es

Abstract. WSNs are becoming an important topic in the research arena. Their low cost and the wide range of applications where wireless sensor networks can be applied, make them an important research and commercial field in the short term. Furthermore, the IEEE 802.15.4 standard for physical and MAC layer in addition with the Zigbee specification for the network and application layer, are an enforcement for WSNs. Much research in WSNs related topics such as energy-aware, MAC protocols, routing protocols, security, location, etc is being carried out nowadays. An open issue is the interconnection between wireless sensor networks where different approaches can be adopted: bridging (extension devices) and proxying (mainly middleware entities). This paper is focused in the bridging approach for Zigbee networks. Our objective is to establish a Zigbee Extension Device Network for the case where the different clusters can not be connected to the same Zigbee network by using the multihop routing protocol defined in Zigbee. A Zigbee cluster is a set of Zigbee nodes. This paper introduces three different solutions to join the disconnected clusters of the Zigbee Network: a central approach (based on the use of a central station) and two distributed approaches; one of them proposes that each Zigbee Extension Device stores the information of all the other Extension Devices within the network while the other uses a P2P Zigbee Extension Device Overlay Network to join the disconnected Zigbee Clusters. The paper includes the analysis of each solution and the comparison among them.

***Keywords*— Zigbee, WSN, interconnection, cluster, overlay, p2p.**

1 Introduction

Recent advances in microelectromechanical systems, low power and highly integrated digital electronics, tiny microprocessors, low power radio technologies, etc, have permitted to develop many kinds of versatile sensors and actuators. These sensors can sense many environmental characteristics like temperature, humidity, pressure, speed, presence, etc. Due to the previous advances, low-cost and low-power wireless sensor are being installed nowadays. Some predictions claim that the price of a sensor will be lower than 1$. Therefore, it will be

possible to develop networks with many unattended sensors. Typical applications for Wireless Sensor Networks (WSNs) are: military, environmental, health, home, environmental control in office building, managing inventory control,etc. Much research has been done in WSNs at all levels: physical, MAC, network and application layers. In [1] general concepts and classifications of the main characteristics within a WSN are studied. In [2] approaches for energy aware, routing, location and security are explained. Finally, [3] makes a taxonomy of the research approaches for routing in WSNs.

Efforts in standardisation have been carried out at different levels. IEEE 802.15.4 [4] is a standard for the physical and MAC layers. Furthermore, the Zigbee Alliance[1], formed by more than 150 partners, has developed an specification for the network and application layers, [5]. The Zigbee Specification operates over IEEE 802.15.4 MAC layer. The IEEE 802.15.4/Zigbee stack seems to be a suitable standard for the application development in WSNs environments.

This paper proposes a solution of an open issue of the IEEE 802.15.4/Zigbee stack. It is the necessity to interconnect WSN. In [6] two different approaches for WSNs (using the IEEE 802.15.4/Zigbee stack) have been identified:

Firstly, the interconnection of different WSN is described. For this purpose, it is necessary the presence of a *gateway* or *proxy*. The role of this proxy is to understand the messages coming from the WSNs, translate them into other messages and route them through a different network (e.g. IP backbone) to get to the target WSN. This proxies are proposed as complex elements which understand application level, so that each application needs a different proxy. [7] proposes a middleware approach using a P2P overlay and UPnP proxies to discover services.

Secondly, the interconnection of clusters (set of Zigbee nodes) is introduced. It is possible a scenario where different clusters of the same Zigbee network were not reachable among them by using multihop wireless routing mechanisms due to the physical distance. In that case, the Zigbee clusters must be interconnected by using another network infrastructure. In this case, the entity which attaches the Zigbee cluster to the infrastructure and allows the communication with other Zigbee clusters (ZCs) is called Zigbee Extension Device (ZED).

Our paper is focused on the second approach, the interconnection of ZCs belonging to an unique Zigbee Network. For this purpose, several architectures are proposed.

Firstly a central architecture is defined. In this approach, all the information about each ZC (i.e., the Zigbee addresses within the cluster and the Cluster ZED) is stored in a Central Station. A ZED uses the central station when inter-cluster communication is needed in order to obtain the IP address of the ZED which is managing the destination ZC.

Moreover, the paper describes two distributed architectures. In the first one each ZED knows all the information about the rest of ZCs (i.e. the ZED and the Zigbee addresses). Therefore, when a ZED receives a Zigbee command for an external Cluster, it searches locally the destination ZED and sends to it

[1] *http://www.zigbee.org*

the command. The other distributed solution is based on peer-to-peer (p2p) technology. Unlike the previous one, the ZEDs locates the target ZED for a certain Zigbee command by launching a search on a p2p overlay formed by all the ZEDs.

The remainder of the paper is organised as follows: In section 2 we present a background of IEEE 802.15.4/Zigbee stack focused mainly in the network layer. In section 3 our Zigbee Extension Device Network proposal is introduced. We analyse and compare the proposed architectures, in section 4. Finally conclusion and future work is presented in section 5.

2 Background

2.1 IEEE 802.15.4

IEEE introduced the standard IEEE 802.15.4 [4], for low rate wireless personal area networks (LR-WPAN). It standardises both physical and MAC layer. The advantages of LR-WPANs are: easy installation, very low-cost, reasonable battery life, reliable data transfer and a flexible protocol stack.

2.2 Zigbee

The Zigbee Alliance introduces in [5] a specification which defines the Network and Application layers working over the IEEE 802.15.4 stack. A good summary of Network and Application layers is shown in [2].

The Zigbee stack is built on top of the IEEE 802.15.4 stack. Network Layer functions are: multihop routing, route discovery and maintenance, security and joining/leaving a network. The network level is also in charge of assigning 16 bit addresses to the newly joined devices.
Three types of devices are defined by Zigbee: end-device, router and coordinator. The first one works as a sensor/actuator. A Zigbee router is a device with routing capabilities. Finally, a Zigbee coordinator is the one which creates the network and manages the network and there is only one per Zigbee Network.
A network address has 16 bits. Therefore, networks up to 65.536 nodes could be developed. Three network topologies could be defined at this level: star, tree and mesh. In the first one, all nodes are directly connected to the coordinator. In the tree topology, a tree is formed with the coordinator as root, and with the end-devices as leaves. Routers are used in this topology to join the different levels in the tree structure. The last topology is a free mesh topology where end-devices can communicate among them by using multihop routing through the routers.
Next, several network layer functions are explained.

2.3 Network Formation and Address Assignment

When a node wishes to join the network, it runs a join procedure. The network layer of this node starts a network discovery procedure. By using the MAC level

the network layer can discover the routers within its radio coverage which are announcing their networks. It is function of the higher layers to decide which network to join. Then, the network layer selects a parent node from those available in the selected network and ask the MAC layer to start an association procedure. The parent node assigns the new node a 16 bit address. Therefore, in a Zigbee network a relationship parent-child is present in the address assignment. In [5] a distributed algorithm is defined to assign addresses. In this algorithm, the Zigbee coordinator sets the maximum number of routers (R_m), end devices (D_m) that each router may have as children and the maximum depth of the tree (L_m).A new router joined to the network receives a range of consecutive addresses based on its depth in the tree. From this range the first one is assigned to the new router while the others can be assigned for this router to their children. These children could be end-devices or other new routers. Nodes at depth Lm are assigned a single address. Also a single address is assigned if the new node within the network is an end-device.

In [2],the mathematical formula to calculate the address range for a router and the method to assign zigbee addresses are explained in detail.

2.4 Routing

Since several topologies are possible, different algorithms are applied depending on which is the current topology.
In a star topology it does not make sense talk about a routing protocol because all the messages are sent to the coordinator.
In a tree topology a tree-based routing algorithm is defined. An end-device always sends the messages to its parent which is a router (or coordinator). When the router receives this message it checks if the destination address is included in its range of addresses. In this case the router is able to route the message to the suitable end-device or router. Otherwise, the router forwards the message to its parent
In the mesh network topology the routing algorithm is more complex. This algorithm is based in Routing Tables (RTs) which can be constructed and updated by using a route discovery algorithm. This mechanism is described in more detail in [2]

2.5 Route Discovery

This process is required in order to create and update routing table entries in the routers and coordinator.
The Route Discovery mechanism is based on Ad Hoc On Demand Distance Vector (AODV) routing algorithm which is explained in [9] Basically, when a node needs a route to a certain destination broadcasts a Route Request message (RREQ). This RREQ travels along the network. The RREQ message accumulates a cost through the path it follows. This cost can be incremented by one in each hop, or other metrics can be used. When the destination node receives the RREQ, it replies a Route Reply (RREP) which travels back along the same path.

The RREP also carries information about the path cost which is incremented hop by hop by the node which forwards the message. Therefore, the originator node will receive several RREPs and it will chose as next hop the node which give back to it a minimum path cost to the destination node. Each intermediate node in the path will do the same, and by doing so the path is established. This process is explained in detail in [2].

3 Zigbee Extension Devices Interconnection Network Architectures

The Zigbee alliance identifies the necessity to interconnect [6] Zigbee Clusters (ZCs), which are a section of a Zigbee network formed by one or more devices, that can not communicate among them using routing mechanisms defined in the Zigbee Specification. To do this Zigbee bridges, which are called Zigbee Extension Devices (ZEDs), are introduced [6]. ZEDs function is to encapsulate the Zigbee stack used in the ZEDs interconnection network which could be based in many technologies (e.g. IP, Ethernet, WiFi....). In this paper is proposed the use of an IP backbone using the stack shown in figure 1.

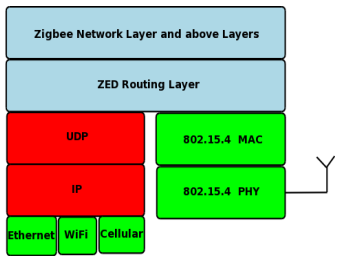

Fig. 1. ZED protocol stack

Thanks to this ZED, a single Zigbee network can be formed by joining ZCs. Thus, there is only one Coordinator within the network and a common address space is used. Typically, the ZEDs joined to the interconnection network are Zigbee Routers, but it is possible that Zigbee End Devices become ZEDs if they implement the interconnection protocol stack, however usually these end devices are very constraints nodes.
We propose three different architectures which are shown in figure 2, to solve the interconnection of ZCs. The principal objective is not to change anything in the current commercial Zigbee devices, but only introducing the ZED provide a full Zigbee connection through the interconnection network.

Two different scopes can be discussed in the proposed solution:

- **Intra-ZED routing:** It is the routing among Zigbee nodes located in the same ZC. It could be based-tree routing or mesh routing. The proposed architectures work with both of them.

– **Inter-ZED routing:** It is the mechanism to communicate ZEDs. The ZEDs have to solve the mapping between Zigbee destination addresses and IP ZEDs addresses, it means the ZED IP address which interconnects the ZC where the destination Zigbee node is located (if the backbone was not an IP backbone, a different mapping would be necessary). The mapping mechanism is different in each one of the proposed architectures. After discovering the destination ZED IP address all the solutions proposed do the same: the Zigbee message received is encapsulated into the UDP/IP stack and it is sent to the destination ZED, this one decapsulates the Zigbee message and forwards it into its ZC.

Following, the proposed architectures to solve the previous issues will be introduced:

1. **ZEDs connected to a central station:**
   This is the most intuitive solution. This central station has to store information about the whole Zigbee network. The minimum information stored in the central station for each ZC is the set of Zigbee addresses assigned to that ZC and the IP address of the ZED which connects that ZC to the Zigbee Network. Extra information could be stored. This central station could be placed in the coordinator if it is powerful enough. Another possibility is to use a monitoring station as a suitable place to allocate our central station (see figure 2).
2. **ZEDs storing information about all other ZEDs within the Zigbee Network:**
   In this approach every ZED has to store information for all the others ZEDs in the interconnection network. Each ZED stores the same information which was stored in the central station in the previous case, the IP addresses of all the ZEDs and the set of zigbee addresses located in the ZC associated to each ZED. In this architecture, the ZEDs form an overlay network. It is a distributed solution (see figure 2).
3. **P2P ZEDs Overlay Network:**
   The last approach introduces the use of P2P Structured Overlay Network in order to interconnect all the ZEDs within the Zigbee network. The proposed P2P network type is a fully distributed, self-organised, structured and searching based on Distributed Hash Table (DHT). All the standard mechanisms of these P2P networks, introduced in [8], could be used: joining procedure to the p2p, distributed storage, searching methods, etc (see figure 2)..

Some issues posed by this approach must be solved in the proposed architectures. The main issues are: join procedure (Zigbee address assignment), routing unicast inter-ZEDs (mapping between Zigbee addresses and IP addresses) and broadcasting inter-ZEDs.

In the join procedure there are two steps. Firstly, a new ZED joins the ZEDs interconnection network receiving the ZEDs IP address of its parent within the Zigbee address tree. This process is solved by different methods in each architecture (see subsection 3.1). Secondly, the new ZED joins the Zigbee Network

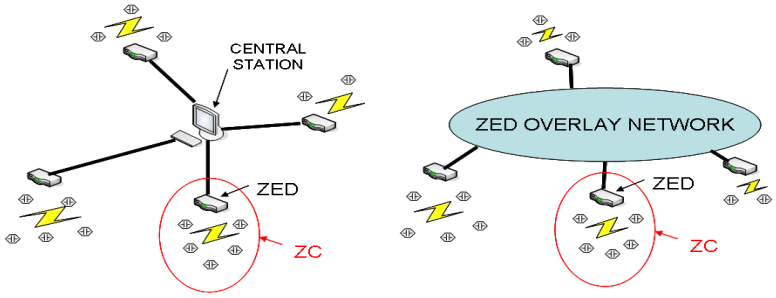

Fig. 2. Proposed architectures to interconnect ZCs by using ZEDs. On the left the scenario of ZEDs connecting to a central station is shown. On the right a figure for the distributed architecture is shown.

sending a Zigbee join message through an UDP/IP tunnel to its parent. This second step is common to all solutions.

In the routing unicast, when a ZED (ZED1) receives a message directed to a Zigbee node which is not located in its ZC, ZED1 has to find the IP address of the destination ZED (ZED2) which is connecting the ZC where the Zigbee destination node is located. This mapping process Zigbee address/IP address is solved using different mechanisms in each proposed architecture (see subsection 3.2). From this point, in all the solutions, the ZED1 sends the Zigbee message to the ZED2 using the IP backbone. The ZED2 decapsulates the message and forwards it into its ZC.

Following Zigbee address assignment, address mapping and broadcasting will be explained. In the next section, advantages and problems of each approach will be explained and also a comparison and suitable scenarios of applications for each one in front of the others is made.

3.1 Zigbee address assignment

In the central station architecture, a new Zigbee ZED has to obtain a position in the Zigbee address tree. In order to complete this process, the new ZED sends a query to the central station asking for a parent, and the central station returns the IP address of the ZED which will be its parent in the Zigbee address tree.

The joining procedure presents a problem in the second approach, because a new method has to be defined when a new ZED wants to join with the Zigbee Network. In somehow, the new ZED, ZED1, has to discover other ZED, ZED2 (e.g. a bootstrapping server could be used).

In the P2P approach, the new ZED follows a two step process. Firstly, the ZED joins the P2P network using a standard P2P mechanism and once it has joined to the P2P network the ZED joins the Zigbee Network. After the ZED has joined the P2P network, it has a number of neighbours, which are other ZEDs. Therefore, the ZED could use these ZEDs to join the Zigbee Network. The new ZED selects one of its p2p neighbours as parent in the zigbee address tree.

3.2 Address mapping

In the central station architecture, eventually, one ZED (ZED1) receives a Zigbee message whose destination is a node which is located in a different ZC. Then, ZED1 sends a query to the central station asking for the IP address of the ZED (ZED2) that is managing the ZC where the zigbee destination node is located. The central station answers to ZED1 giving the ZED2 IP address.

In the second approach the mapping is immediate, when a ZED (ZED1) receives message directed to a zigbee node located in a different ZC, the ZED1 checks in its information table which is the ZED which is managing the ZC where the destination node is located (ZED2).

Finally in the P2P approach, all ZEDs registered in the P2P have to publish its IP address and the set of zigbee addresses in the ZC attached to that ZED. Then, when data message arrives to a ZED (ZED1) and this one checks that the destination node it is not located into its ZC, the ZED1 launches a search query within the P2P using as key the Zigbee destination address. As result ZED1 obtain the IP of the ZED (ZED2) which has the destination node into its ZC

In the central station and P2P an improvement could be developed. When a mapping is established, the current ZED could keep this information into a cache. For example, this is very useful in an application when a sensor/actuator in a ZC communicates frequently with a sensor/actuator located in a different ZC. If the communication uses ACKs, the destination ZED could use a cache as well.

3.3 Broadcasting

In the central station solution, broadcasting is very simple. A ZED receiving a zigbee broadcast message encapsulates it into an UDP/IP packet and sends it to the central station. The central station checks that it is a broadcast message and forwards it to all the ZEDs except the originator ZED. Every ZED receiving the IP packet decapsulates the Zigbee broadcast message and forwards it into its ZC.

In the second architecture, the ZED receiving the zigbee broadcast message, identifies that it is a broadcast message and encapsulates it into the UDP/IP stack. After that, it sends IP packets to all the ZEDs stored in its information table. Each ZED receiving this packet decapsulates the zigbee broadcast message and broadcasts it into its ZC.

In the ZED P2P Overlay Network the broadcasting does not have an intuitive solution as in the previous architectures. When a ZED (ZED1) receives a zigbee broadcast message, it identifies the broadcast message and encapsulates into an UDP/IP packet. The ZED1 sends this packet to the nearest neighbour, this one does the same and it decapsulates the zigbee broadcast message and broadcasts it into its ZC. By doing so, the broadcast message reaches all the nodes into the ZEDs P2P overlay network. For instance, in a P2P ring structure with N nodes, it is necessary to forwards N times the broadcast message.

A better mechanism would be that the ZED1 would send the broadcast packet to all the nodes which it knows in the P2P. In reception of this packet, a ZED (ZEDi) checks if it has received the same packet before (it is necessary to identify the current broadcast message in the P2P overlay and it is not enough with checking that it is a Zigbee broadcast message). If it is true the ZEDi drops the packet. Otherwise, first the ZEDi forwards the IP packet to all the ZEDs that it knows, next, it decapsulates the zigbee broadcast message and broadcasts it into its ZC. All the ZEDs in the P2P repeats the same operation, so that the broadcast message reaches all the nodes into the ZEDs P2P overlay network.

RREQ is a special broadcast message which is sent to a target node. In a typical Zigbee network it is boradcasted everywhere because it is not known where is located the destination node. However, in our proposal, if a ZED receiving a RREQ is able to identify that the broadcast message is a RREQ, it could check the destination Zigbee address, and sends it to the suitable ZED, instead broadcasts the RREQ.

4 Analysis and Comparison of the proposed architectures

4.1 Analysis

The central station approach is a simple and intuitive approach. The principal problem of this solution is that it becomes a unique point of failure. If the central station fails all the network is disconnected and only local ZCs communications are available. Also, all the network information is located in a single point. Hence, if that information is lost the network is disconnected as well. Obviously, the solution to solve these problems is to replicate the information or to use a backup central station just in case the main central station fails. Other problem in this scenario is that some administration is needed. When a new ZED is introduced the information of this ZED must be updated in the database located in the central station. By using a simple protocol (register message) this task could be automatised.

The second approach has several disadvantages. First, a new mechanism must be defined in order to permit new ZEDs to join the Zigbee network. Basically, this mechanism should permit the new ZED to discover another ZED which would become its parent in the zigbee address tree. A bootstrapping server is an immediate solution for this problem another option could be manual configuration in order to join a new ZED the Zigbee Network. Another problem occurs when a new ZED joins the network because the information of this new ZED must be updated in all the nodes within the overlay network, and if the number of ZED is high it could be a hard administration task. On the other hand, the resolution of the IP address of the destination ZED is faster than in the other approaches because third entities are not needed (an improvement using caches for the other solutions has been introduced in 3.2). This is a distributed architecture but the information storage is not distributed.

Finally the ZED P2P Overlay Network has a main disadvantage in front of the other two, which is the delay in the communication because the time used to find

the destination ZED IP address is longer than in the two previous cases. A basic analysis of this will be done in 4.2. Advantages for this architecture is that the ZED P2P Overlay Network is self-configured (the central station approach could be self-configured as well, if a simple register protocol is defined), the information is distributed and replicated and the ZEDs needs little storage capacity (an analysis of the storage capacity in the three architectures will be done in the 4.2), furthermore all these features are given by standard P2P mechanisms.

4.2 Comparison

The central station approach presents a centralised element which usually is a node with a high storage and processing capacity. Therefore, this additional processing capacity could be used ,for instance, to allocate the new ZED in a suitable position within the zigbee address tree.

In contrast to this central approach, the second and third architectures are distributed. Therefore, in the central station approach a unique point of failure is present. This problem could be solved by using a backup central station, but it supposes an extra cost element. This problem is not presnet in the distributed solutions.

In the second approach, ZEDs storing information about all other ZEDs within the Zigbee Network, has a problem in the joining procedure as we explained in 4.1. In the central station and P2P Overlay Network approaches how a new ZED joins the network has been explained in 4.1. Also the second approach is a worse solution than the other two when new ZEDs are added to the Zigbee Network. When a new ZED is added in the second approach, all the other ZEDs have to update their information tables with a new entry for the new ZED. If the number of ZEDs is large, it could be a problem. In the central station approach, only the information stored in the central node needs to be updated. In the P2P architecture, the new ZED has to publish the suitable information in the P2P and it is stored into another ZED by using P2P standard mechanisms.

Therefore, the P2P is self-configured by using P2P standard mechanisms, whereas the other two approaches are not. Obviously, these ones could be transforming in self-configured by defining some mechanisms, but these mechanisms are not standard as in the P2P.

If we do a comparison in terms of delay the best architecture is the second one. We define t as the time used for a communication from ZED to ZED or from ZED to central station and we compare the time to communicate from a ZC1 (ZED1) to another ZC2 (ZED 2). Table 1 shows in the second and third columns a comparison among the delay for each solution to discover the destination ZED (ZED2) for unicast and broadcast respectively. It must be noted that N is the number of ZEDs and the maximum number of hops in a P2P to find the peer storing the desired information is $log_2(N)$ [8].

It must be noted that the real delay will depend on the IP location of the different elements.

Some mathematical analysis can be done to see the information storage in the different approaches. The fourth column in table 1 establish a comparison

	Unicast Delay	*Broadcast Delay*	*Storage Cost*
Centralised Solution	$2 * t$	$2 * t$	N
Distributed Solution	0	t	N^2
P2P Solution	$log_2(N) * t$	$N * t$	k

Table 1. Metrics comparison

between the number of entries which must be stored in each solution. In the central station the value is referred to the central station, whereas in the distributed solutions the values represents the number of entries stored in each ZED. In the P2P solution, in order to get fault tolerance redundancy must be added. Therefore, each entry is stored in k peers. It must considered that each solution has extra storage due to the interconnection network used. For instance, in the P2P solution each ZED has to store information about its neighbours.

4.3 Suitable scenarios for each architecture

If the scenario presents a monitoring central station, something typical in wireless sensor networks, the most suitable architecture is the central station. Operation and management are also simpler form a central station. Furthermore, if the coordinator is a node with high processing and storage capacity it could be used as central station.

The architecture where ZEDs store information about all other ZEDs within the Zigbee Network is applicable in static scenarios where usually new ZEDs do not join the Zigbee Network. It is also applicable to small scenarios, where the information stored in each ZEDs is not too much. This architecture is worse than the others in scenarios where many ZEDs are needed and where new ZEDs are joined frequently.

The P2P ZEDs Overlay Network architecture is suitable in scenarios where high availability is needed (e.g.warfare). Also, in very large WSNs where delay can be trade-off with memory and robustness in unstable clusters.

In special scenarios where ZEDs are joining and leaving frequently (e.g. mobile ZC attaching the ZED network at different locations) the most suitable solution is to use the central station approach if a register protocol has been defined, otherwise the P2P solution would be the best solution.

5 Conclusions and future work

WSN interconnection is an open research issue. The Zigbee alliance [6] defines two possible approaches to solve this problem. The first one is the usage of proxies or gateways. Some research is being carried on in this field, and middleware based approaches have been presented in the literature. This paper is focused on a second approach which is the use of bridges or expansion devices . In particular we have proposed and analysed some Zigbee Extension Device

Interconnection architectures in this paper. Our aim has been to create a single Zigbee network with Zigbee Clusters that are not reachable among them by using standard Zigbee multihop routing protocol and they are members of the same Zigbee Network. We have presented the main issues to solve in order to be able to operate without changing nothing in the commercial Zigbee devices which implement the IEEE 802.15.4/Zigbee stack. With this objective in mind, three approaches has been introduced. Advantages and problems for each architecture have been discussed.

Further work is to implement a ZED into a Zigbee mote and start to develop the centralised model due to its simplicity. In particular, we want to study the case when the interconnection network is a cellular network (e.g 3G) where the setup and communication cost must be minimised.

Acknowledgement

The authors would like to thank the anonymous reviewers for insightful ideas and suggestions that made it possible to write a better article.This paper has been partially granted by the Spanish Government through the IMPROVISA project (TSI2005-07384-C03-027) and the regional government of Madrid through the BIOGRIDNET project (S-0505/TIC-0101).

References

1. I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci. "Wireless sensor networks: a survey", Computer Networks 38 (4) (2002) 393-422.
2. Paolo Baronti, Prashant Pillai, Vince Chook, Stefano Chessa, Alberto Gotta, and Y. Fun Hu. "Wireless Sensor Networks: a Survey on the State of the Art and the 802.15.4 and ZigBee Standards", Technical Report, May 2006.
3. K. Akkaya, M. Younis, "A survey on routing protocols for wireless sensor networks", Ad Hoc Networks 3 (3) (2005) 325-349.
4. Institute of Electrical and Electronics Engineers, Inc., IEEE Std. 802.15.4-2003. "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs)", New York, IEEE Press. October 1, 2003.
5. ZigBee Alliance. "ZigBee Specifications", version 1.0, April 2005.
6. Patrick Kinney. "http://www.zigbee.org/en/documents/SensorsExpo/7-Sensors-Expo-kinney.pdf"
7. Manabu Isomura, Till Riedel, Christian Decker, Michael Beigl, Hiroki Horiuchi. "Sharing sensor networks", Proceedings of the 26th IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW'06), July 2006, pp. 61-66.
8. J. Risson and T. Moors. "Survey of Research towards Robust Peer-to-Peer Networks: Search Methods", Internet Draft, draft-irtf-p2prg-survey-search-00.txt J. Risson and T. Moors: "Survey of Research towards Robust Peer-to-Peer Networks: Search Methods", Accepted to appear in Computer Networks
9. Charles E. Perkins and Elizabeth M. Royer. "Ad-hoc On-Demand Distance Vector Routing", Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 1999), pp. 90-100, New Orleans, LA, USA, February 1999.