Wireless Sensor Network for Wide-Area High-Mobility Applications

Ignacio del Castillo*[a], Roberto Esper-Chaín[a], Félix Tobajas[a] , Valentín de Armas[a]
[a]Instituto Universitario de Microelectrónica Aplicada (IUMA)
Departamento de Ingeniería Electrónica y Automática (DIEA)
Universidad de Las Palmas de Gran Canaria, 35017, Spain

ABSTRACT

In recent years, IEEE 802.15.4-based Wireless Sensor Networks (WSN) have experienced significant growth, mainly motivated by the standard features, such as small size oriented devices, low power consumption nodes, wireless communication links, and sensing and data processing capabilities. In this paper, the development, implementation and deployment of a novel fully compatible IEEE 802.15.4-based WSN architecture for applications operating over extended geographic regions with high node mobility support, is described. In addition, a practical system implementation of the proposed WSN architecture is presented and described for experimental validation and characterization purposes.

Keywords: Wireless Sensor Networks, IEEE 802.15.4, Hierarchical Networks, Heterogeneous Devices.

1. INTRODUCTION

A Wireless Sensor Network (WSN) is a set of heterogeneous sensing nodes organized into a cooperative network [1], [2]. Each node combines sensing, processing, and short-range wireless communication capabilities. Nodes are commonly deployed in large numbers in order to implement cooperative sensing and control applications. Typical applications include environmental information and control, smart energy, fire detection, health monitoring systems, and many others [3], [4]. WSN provide significant advantages over wired sensing networks, due to their easy deployment and high configurability. The introduction of very low cost wireless transceivers and microcontrollers allows for the development of very cost-effective solutions, driven by a rapid growth in the market, which is expected to continue for years.

In WSN, information travels across the network, routed by some of the nodes with routing capability. Routing techniques must be configured for each application and network configuration. Large development and research efforts are currently in progress in order to reduce computational requirements and memory footprint by implementing efficient routing techniques [5]. Network dynamic self-organization and self-healing characteristics are of great interest.

In order to guarantee interoperability among devices, several standards have emerged. For PHYsical (PHY) and Media Access Control (MAC) layers, IEEE 802.15.4 has become a dominant standard which has been implemented in diverse low-cost commercial transceivers [6], reducing time-to-market. For higher layers, several standards coexist, principally ZigBee and 6LoWPAN. ZigBee is a proprietary standard for which successful products have been introduced on the market in recent years [3], [5], [7]. On the other hand, IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) is an open standard, which eases the convergence with IP networks, being a reduced implementation of IPv6 over IEEE 802.15.4 [8]-[11].

The specification of these standards is oriented to a static node structure, where routers have a previously planned spatial distribution. With this structure, routing information can be calculated at deployment time and loaded in nodes. However, dynamic routing techniques have limited efficiency and produce undesirable effects when large networks or highly mobile nodes are used [12], [13].

* idelcastillo@iuma.ulpgc.es ; phone +34 928 451246; fax +34 928 451083; www.iuma.ulpgc.es

2. WSN ARCHITECTURES IN WIDE AREA, HIGH MOBILITY ENVIRONMENTS

Nowadays, ZigBee and 6LoWPAN are the most popular standards for the development and deployment of WSN structures. Both of them are network-level protocols based on the IEEE 802.15.4 standard, so they share PHY and MAC layers. However, none of the existent network level protocols, even those that can modify their available settings, are presented as a valid solution to ease the deployment of wide area WSN. The main reason is that all of the communication standards are intended for use with a centralized structure, having a unique central router node responsible for starting up the network, or receiving the data frames transmitted by any device belonging to the WSN [14], [15].

The practical solution proposed in this paper consists of a decentralized architecture based on the existence of several coordinator nodes that, using a wireless communication standard, allows the deployment of wide area, high mobility WSN. Fig. 1 shows a graphic image of the proposed WSN architecture. In Fig. 1, lower case letter nodes represent the mobile sensor nodes that are responsible for performing the sensing function for which they are developed, and that transmit the available information to coordinator nodes, represented by capital letters. Coordinator nodes are responsible for transmitting all received data frames from each sensor node that belongs to the network, to a central recording and processing node using an IEEE 802.15.4 interface. This functionality is achieved by connecting a standard GPRS device to each coordinator node. GPRS devices used for data transmission from coordinator nodes to the recording and processing node, are physically connected using Controller Area Network (CAN) protocol, which allows an acceptable binary rate using a floating bus-to-bus protocol that minimizes data system loss in systems operating under noisy environments. The recording and processing node, whose main function is to record the data frames received from any node belonging to the network, has the capability of processing the received information.

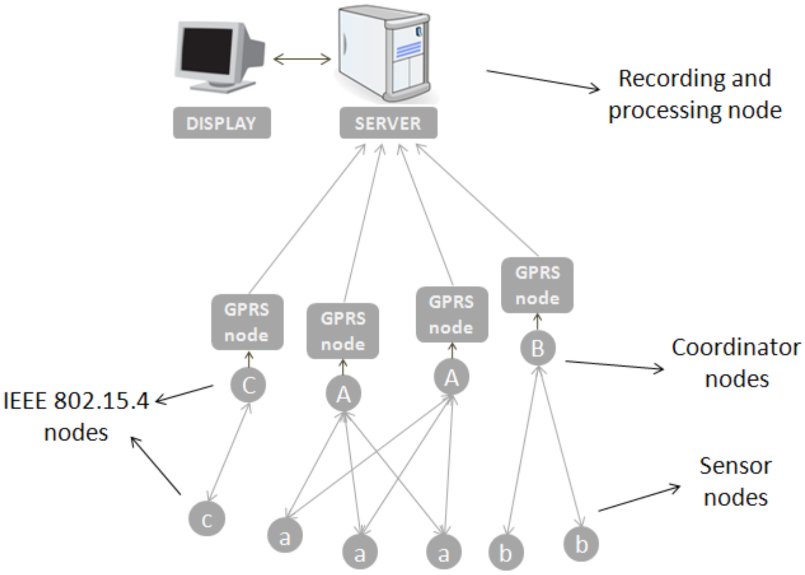

Figure 1. Proposed IEEE 802-15-4 based WSN architecture.

In the proposed network architecture, the low level system consists of an IEEE 802.15.4 based WSN, fully composed of IEEE 802.15.4-compatible devices that support all the standard functionalities. Using the IEEE 802.15.4 standard as basis gives the proposed WSN a typical star structure mostly used in Wireless Personal Area Networks (WPAN). As a consequence, the proposed network will gain several advantages, many of them derived from using a standard protocol.

However, the use of a WSN-oriented standard as a basis does not mean that it will not be necessary to make improvements in order to reach the pursued objective of fully complying with the requirements of a wide area, high mobility WSN architecture. It is important to take into account that IEEE 802.15.4 compatibility must be maintained in the design of the proposed network architecture. Nevertheless, a WSN with all nodes having high mobility to face diverse and complex issues should be taken into account in the architecture and protocol design. In the first place, due to the mobile nature of the nodes belonging to the network, several coordinator nodes have to be available, even if they are operating simultaneously in the same spatial region. This feature will allow data frames proceeding from sensor nodes to be transmitted to the recording and processing node. In second place, due to the mobility of the coordinator nodes, they must have the capability to coexist and work over the same communication radio channel, even if more than one coordinator node belonging to the same network is online over the same region. This feature will make it possible for a sensor node to select the coordinator node to which it will connect. In addition, coordinator nodes should have additional functionalities that allow the deployment of several network structures.

When a huge number of mobile sensor nodes must be monitored, reuse of the communication facilities improves the network's efficiency [16], [17]. For this reason, all the elements should cooperate to conform to a single network. In the proposed architecture sensor nodes are data producers, but only have low-range transmission capability, since GPRS transmission might have a significant cost with a high number of supported nodes. As a consequence, multiple sensor nodes must be associated to reuse coordinator node's GPRS communication facilities. The model of operation of the proposed WSN architecture requires a high rate of re-association, which must be performed in an agile way, with no human intervention. In a standard IEEE 802.15.4 implementation, this process requires a significant overhead of data transmission back and forth with the coordinator node by means of GPRS communications. In the proposed WSN architecture, multiple coordinator nodes can coexist, and do not compete for sensor connections, minimizing the required GPRS data bandwidth.

A sensor node belonging to a network should be capable of determining which coordinator node within its range is valid for establishing a connection in order to send data frames to it. If more than one coordinator node exists within its range, the sensor node will be able to select which one belongs to its network, and connect to it, discarding those coordinator nodes that, even if they are using the same radio channel or communication standard, do not belong to the same network as the sensor node. Furthermore, based on the proposed approach, several networks belonging to different organizations are able to coexist.

3. PROPOSED IEEE 802.15.4 BASED COMMUNICATION PROTOCOL

The main reason why the IEEE 802.15.4 communication standard has been used as a basis for developing the WSN proposed in this paper is because it defines and regulates PHY and MAC levels, leaving the upper layers free for the required application. One of the most important ideas in this standard is the definition of two kinds of available devices according to their intended use and functionalities: Reduced Functionality Devices (RFDs) and Full Functionality Devices (FFDs). In addition, all devices that implement IEEE 802.15.4 standard can be addressed using a 64-bit extended address field.

According to the IEEE 802.15.4 standard specifications, the network is always established by an FFD device, which is responsible for setting up all the configuration parameters, for instance the radio electric channel used, the connection capabilities, and the Personal Area Network Identifier *(PANId)*, which consists of a 16-bit field that identifies the network. After that, once the network has been established by the FFD node, RFD devices, usually including sensor nodes with pending data frames that are to be sent, search for an available FFD within their range that permits the association by performing a scan in one, or several radio channels. Once the association has been successfully established, and after the node validation process, the sensor node can send available data frames to the coordinator node for transmission to the recording and processing node. However, according to the IEEE 802.15.4 standard specifications, the existence of more than one coordinator node belonging to the same network and simultaneously operating on the same radio channel is not possible. This issue represents a functional limitation for the deployment of a WSN intended to cover a wide geographic area with mobile nodes, since, due to the wide mobility feature of the nodes belonging to it, there are common situations where more than one coordinator node could be simultaneously operating in the same radio channel and within the same range. Because of this limitation, and with the objective of improving the standard functional specifications in order to ease the deployment of wide mobility WSN, some IEEE 802.15.4 standard premises, specifications, and functional descriptions have been improved maintaining full standard compatibility. Those improvements will be introduced in order to develop a communication protocol that fixes and successfully complies with the functional requirements of the WSN proposed in this paper, allowing a large number of sensor nodes dispersed over a wide geographic region to connect to any coordinator node belonging to the network, even with several coordinator nodes using the same radio frequency channel and simultaneously operating within the same region of space.

IEEE 802.15.4 devices will be assigned a fixed 64-bit extended address based on the IEEE *Extended Unique Identifier* (EUI-64). In this paper, the EUI-64 identifier is assumed to be defined as a concatenation of a 24-bit *Organizational Unique Identifier* (OUI), issued by the IEEE Registration Authority (IEEE-RA), and a 40-bit *Extension Identifier* (EI) assigned by the manufacturers [18]. The IEEE-RA has no control over the assignment of the EI field. In this paper, a field division of the EI is proposed. Fig. 2 shows the EUI-64 identifier assigned to an IEEE 802.15.4 device (top) and the proposed field segmentation (bottom), where the 40-bit *Extension Identifier* is divided into three fixed fields. The most significant 16 bits correspond to the *network identifier*, denoted as *groupID*, which represents the network group to which the devices belong. The next 16 bits correspond to the physical number of the device, denoted as *deviceID*. With this field size, it is possible to identify up to 64K devices belonging to the same network. The last 8-bit field includes information about the node functionality, where different custom functionalities supported by the nodes can be represented in binary format.

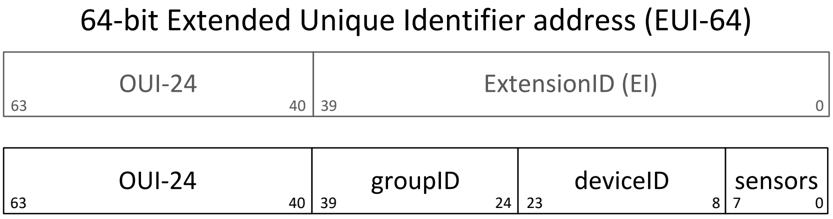

Figure 2. 64-bit IEEE EUI-64 identifier (top), proposed EI field segmentation (bottom).

The proposed field segmentation provides great flexibility and allows a unique identification of each of the wireless sensor nodes belonging to a network. However, some practical scenarios like device duplicity and the existence of two devices with the same *deviceID* should be taken into account. These possible duplicity scenarios could arise because IEEE 802.15.4 is a free and open communication standard, where the devices implementing the PHY and MAC layers are commercial devices, and thus it is possible that other IEEE 802.15.4 devices may operate using the same radio channel and physical settings, including the extended address. Also, the device can operate simultaneously with and over the same geographic area as any other device belonging to a network based on the IEEE 802.15.4 standard communication protocol, and using the same functional behavior.

The WSN architecture proposed in this paper uses a novel authentication protocol based on the interchanging of encoded message frames, which allows validation between coordinator and sensor nodes, and checks that both devices belong to the same network before they are able to interchange data frames.

In Fig. 3, the coexistence of several network structures, with diverse coordinator nodes operating simultaneously in the same radio channel within the same range, is represented. Every sensor node connects only to coordinator nodes that share the same *groupID* field and selects the coordinator node that has a better Link Quality Indicator (LQI) level.

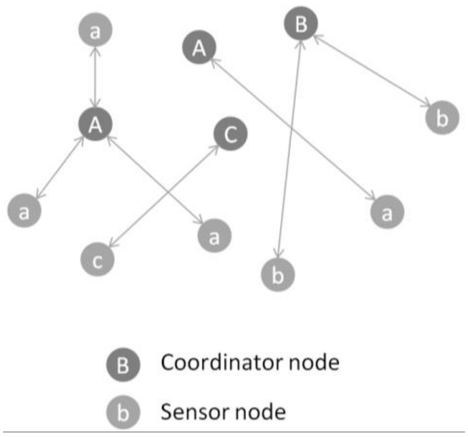

Figure 3. Coexistence of WSN in the proposed network architecture. Each letter represents the *groupID* field.

4. IMPLEMENTATION OF THE PROPOSED IEEE 802.15.4 BASED COMMUNICATION PROTOCOL

4.1 Coordinator node

Fig. 4 shows a functional flow diagram of the proposed coordinator node behavior, where the most important states and processes are represented. Every coordinator node starts its operation in the *System startup* state, where all the control variables and system configuration parameters are set to their initial values. After that, it starts up the WSN in the *Network establishment* state, setting the same value in the *PANId* field as in its *deviceID*. Once the network has been established, the coordinator node stays in idle state, waiting for incoming associate requests sent by sensor nodes that need to establish communication with a coordinator node that is operating within its range. The *Association process* state and *Authentication process* state are used by the coordinator node to allow any sensor node to associate with it and send data frames through it. Data frame transmission between the sensor and coordinator nodes is performed in the *Data reception* and *Acknowledgment* states. Each data frame received is temporally stored in the *Buffer* state. Finally, the coordinator node sends the data frames received by sensor nodes to the recording and processing node in the *CAN Transmission* state.

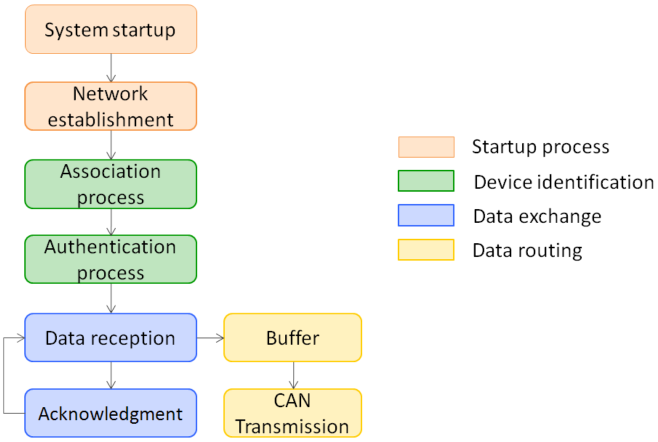

Figure 4. Coordinator node functional flow diagram.

Fig. 5 shows a flow diagram of the communication protocol between a sensor node and a coordinator node, from the coordinator node side, in the association process. The establishment of communication between sensor node and coordinator node starts on the coordinator side with the reception of an association request from a sensor node, denoted as *Association indication*. After that, the coordinator node verifies that the *groupID* field of the sensor node matches its *groupID*, and proceeds to register the sensor node address in the device list. Next, it transmits a confirmation response to the sensor node, denoted as *Associate confirm*, which finalizes the association process, with the coordinator and sensor nodes being successfully associated. Both devices, coordinator and sensor nodes, exchange fixed length hexadecimal frames containing a codified message used as a validation message, which serves to prevent any device not belonging to the network sending messages through it.

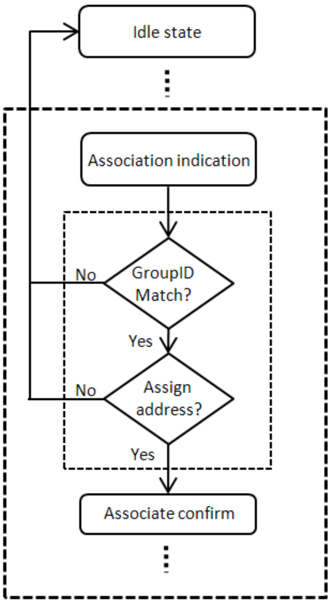

Figure 5. Coordinator node association process flow diagram.

4.2 Sensor node

Fig. 6 shows a simplified flow diagram representing the functionality of the proposed sensor node. In the same way as a coordinator node, each sensor node starts its operation in the *System startup* state, where all the system control variables and configuration parameters are set to their initial values. Once the system is initialized, a configurable timer that signals when a new measurement has to be performed is started. Then, the system remains in *System task* state until an incoming event occurs, such as a timer event indicating a new measurement. The *Association process* and *Authentication process* states are used by the sensor node to check that the selected coordinator node belongs to the same network and allows data frames to be transmitted through it. After being successfully authenticated, the sensor node proceeds to send its available data frames to the coordinator node in the *Data transmission* state, which acknowledges each data frame successfully received in the *Acknowledgment* state.

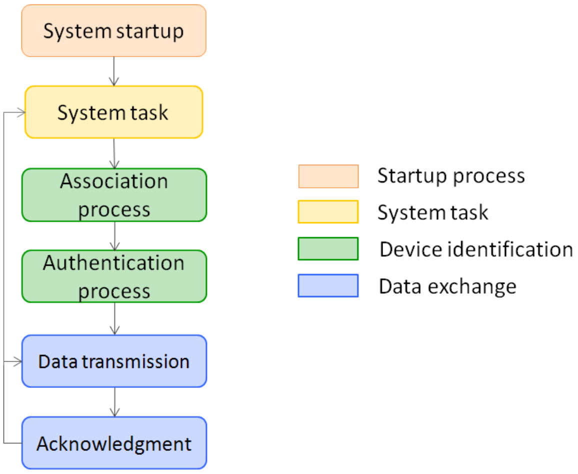

Figure 6. Sensor node functional flow diagram.

Fig. 7 shows a flow diagram of the communication protocol between a sensor node and a coordinator node from the sensor node side in the authentication process. The process of finding and selecting a coordinator node starts after the sensor node transmits a *Scan Command*, staying in the *Wait for responses* state over a predefined period of time. The sensor node establishes a timeout period for receiving the coordinator responses. Coordinator nodes within the range proceed to send a response containing the required information, which consists of the extended address of the coordinator node, the name of the established network, and their functional capabilities. When the sensor node timeout expires, it performs an analysis of each coordinator node response received in order to determine whether there is any valid coordinator node to which the sensor node can connect, and if more than one exists, it determines the best candidate. For that purpose, every coordinator node response is evaluated according to the following priorities:

a) The coordinator node groupID is checked to match the sensor node field, as the coordinator node has to belong to the same network as the sensor node.

b) The LQI parameter of the received coordinator node response is checked, and the best candidate for connection is the coordinator node with the highest LQI level.

Once a coordinator node has been selected, an association request will be sent. If the result of this process is successful, the coordinator node will receive an association indication that will be confirmed by sending an association confirmation response to the sensor node. Once the association process has been successfully completed, the coordinator and the sensor nodes will perform a data frame exchange in order to verify that both devices belong to the same network, being reciprocally authenticated. After being authenticated, the sensor node can send pending data frames to the coordinator node for retransmission to the recording and processing node.

Every data frame sent by the sensor node will be acknowledged by the coordinator node by sending an ACK frame. Once the sensor node has successfully transmitted all the data frames to the coordinator node, it passes to idle state and waits for any incoming event.

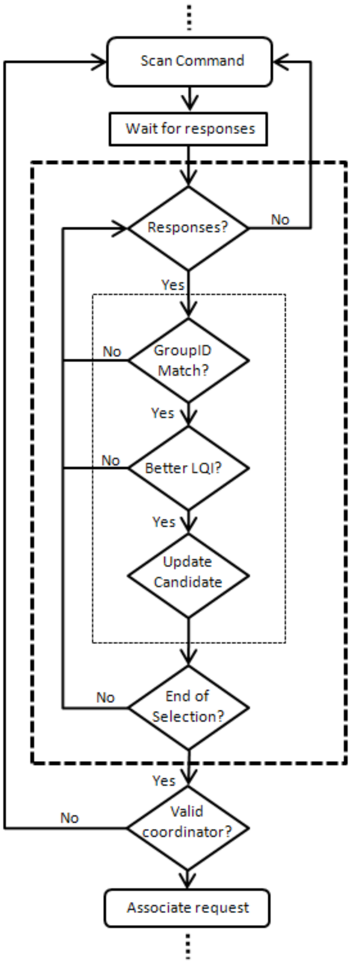

Figure 7. Sensor node association process flow diagram.

5. EXPERIMENTAL VALIDATION

From among the multiple applications of wide area, high mobility WSN, a real temperature monitoring network for a cooled vehicle fleet has been selected in order to experimentally validate the proposed solution. Industrial food distributor companies have to check and control the temperature of their products to ensure it is kept under a threshold from the origin until delivery at the destination. By periodically performing temperature measurements of a cooled container, it is possible to monitor the optimal condition of the goods during transportation [19]-[21].

Fig. 8 shows a functional diagram of the developed application. IEEE 802.15.4 coordinator (C) and sensor (D) nodes based on the proposed communication protocol are installed on each vehicle. The coordinator nodes retransmit the measured temperature information periodically received from the sensor nodes in its range. Every coordinator node is connected using a CAN interface to a mobile device that allows data to be transmitted to the central recording and processing node using GPRS communications.

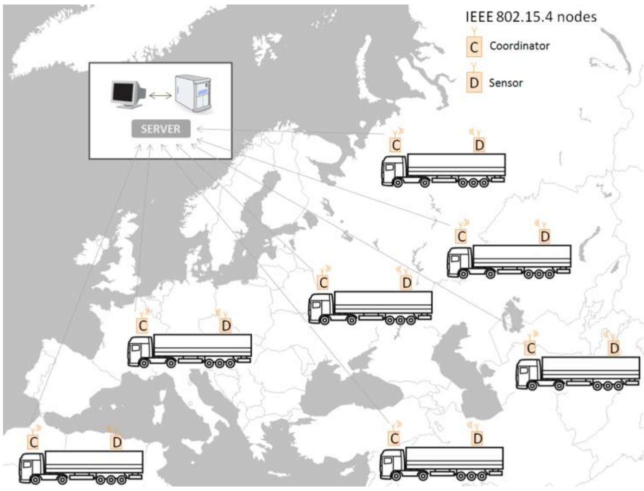

Figure 8. Proposed experimental application diagram.

The physical deployment of the proposed network is based on IEEE 802.15.4 standard modules, using compatible radio transceivers. The radio device operates on the 868 MHz ISM band and is connected to an 8-bit RISC microcontroller that implements IEEE 802.15.4 MAC functionalities and data acquisition functions.

Fig. 9 shows an image of the implemented hardware platform for automotive environment validation. The Printed Circuit Board (PCB) design is constrained by the selected IP66 outdoor enclosure shape. The dimensions of the PCB are 45 mm × 60 mm. The developed automotive hardware platform includes a DC-DC converter, which powers up the system from any battery voltage above 10 V, a removable flash memory for data measurement and startup configuration storage, Universal Serial Bus (USB) communication capabilities for debugging and testing purposes, a Real Time Clock (RTC) with calendar, used to provide precise timed events, and even an over-the-air bootloader firmware that allows the system to be updated remotely.

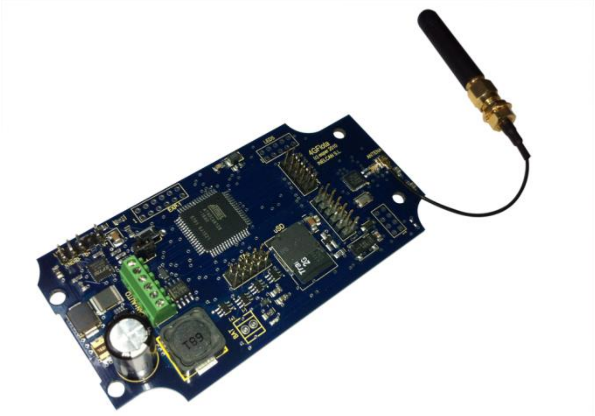

Figure 9. Hardware platform developed for experimental validation.

Fig. 10 shows a representative graphic example of different connection scenarios that could arise during the establishment of communication between a coordinator node and a sensor node in the application environment developed for experimental validation. In Fig. 10a), a sensor node that performs a scan in order to select a coordinator node within its range finally selects the coordinator node of another vehicle belonging to the network, because it receives a better value of LQI than the coordinator node installed on the vehicle to which the sensor node is connected. Fig. 10b) represents a typical situation in which each sensor node transmits the information using the coordinator node that is installed on the same vehicle in which each sensor node is located. Fig. 10c) represents the scenario where all the sensor nodes transmit their information using the same coordinator node, a situation that can be usual in some scenarios, like truck bays.

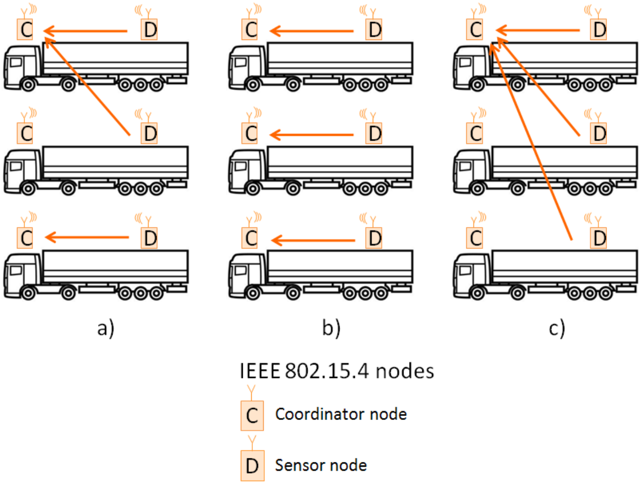

Figure 10. Coordinator node selection process scenarios.

Fig. 11 represents some scenarios where different WSN coordinator nodes coexist and every sensor node proceeds to establish a connection only with nodes belonging to the same network. Fig. 11a) shows a scenario in which, instead of there being several coordinator nodes belonging to different networks, each sensor node selects only a coordinator node that belongs to the same network. Fig. 11(b) shows a situation where a sensor node uses a coordinator node belonging to the same network, but installed on a different vehicle for data transmission. Fig. 11(c) shows how every sensor node selects the same coordinator node for transmitting data frames. The recording and processing node is always the destination node to which all the data frames are transferred.

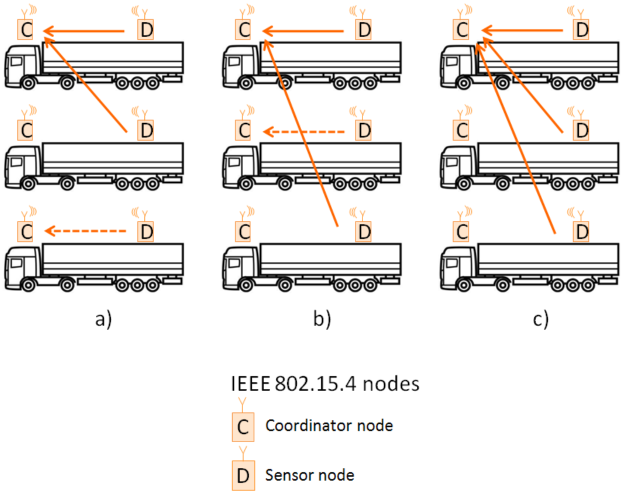

Figure 11. Coexisting networks communication scenarios.

Thanks to the proposed extended address segmentation, the deployment of several IEEE 802.15.4 based wireless sensor networks using the same radio channel, is supported. With the proposed architecture, an unlimited extended geographic mobility node-based flexible WSN can be deployed. Also, the possibility of using several coordinator nodes belonging to the same network allows each sensor node to always establish communication with the best candidate, which contributes to improve the flexibility of the system. Moreover, the proposed IEEE 802.15.4 based WSN, in which more than one coordinator node is operating in the same range, minimizes the possibility of network blocking due to coordinator node malfunction or failure, since there is usually more than one coordinator node available to which a sensor node can connect. In this way, typical coordinator node dependency, which occurs in most IEEE 802.15.4 standard based networks, can be solved.

6. EXPERIMENTAL PERFORMANCE RESULTS

In order to characterize the IEEE 802.15.4 based WSN performance, several functional coordinator and sensor nodes based on the proposed communication protocol have been implemented using the developed automotive hardware platform.

6.1 Firmware Code Size

For experimental validation purposes, solution firmware of the proposed coordinator node and sensor node has been loaded in the developed hardware platform. Table 1 summarizes a statistical comparison of the required resources for the standard IEEE 802.15.4 based and the proposed IEEE 802.15.4 based coordinator and sensor nodes.

Module	No. of files	RAM size (bytes)	Binary code size (bytes)
Coordinator node	54	1,458	23,408
Coordinator node (proposed)	71	2,614	37,176
Sensor node	44	1,273	19,960
Sensor node (proposed)	56	1,709	28,984

Table 1. Summary of firmware implementation size.

As Table 1 shows, implementing the proposed solution nodes requires an almost 14 KB of additional flash memory than the standard IEEE 802.15.4 solution for the coordinator node, and around 9 KB in the case of the sensor node. In the same way, the proposed coordinator node firmware requires about 1.15 KB of additional RAM memory for full functionality, and a further 0.5 KB for the proposed sensor node. Note that in both types of proposed node almost two thirds of the total required system resources are related to standard IEEE 802.15.4 support.

6.2 Communication Protocol Performance

In order to measure the time required for performing data acquisition and communication processes between the implemented sensor and coordinator nodes, an experimental performance test has been developed for different scenarios with up to four visible nodes.

Table 2 shows the average time required for completing the communication process between a sensor node and a coordinator node in the proposed communication protocol. Latencies have been obtained using an 8-bit RISC architecture running at 16 MHz.

Number of visible nodes (1 coordinator)	**Average communication time (seconds)**
1 node	2.56
2 nodes	2.65
3 nodes	2.77
4 nodes	2.82
Total average	**2.7**

Table 2. Summary of communication protocol performance.

From Table 2, the average connection time obtained from experimental measurements is around 2.7 seconds, which means that by using a periodic data transmission with a connection period of 60 seconds, the system will stay in power-down mode for 95.5% of the base time period, thus minimizing power consumption. This average time includes finding and selecting a coordinator node, association and authentication processes, and data exchange, even if retransmissions are required. As the proposed system behavior is coordinator-node oriented, the coordinator node reconnection process and system communication rejoining due to link failure, are considered as new connection processes.

6.3 Power Consumption

The proposed solution node power consumption depends on the functionality of the node belonging to the WSN. In that way, due to the nature of its functionality, the proposed solution coordinator nodes must stay in active mode most of the time, including the CPU core and the IEEE 802.15.4 transceiver block. Alternatively, the proposed solution sensor node should stay in low power consumption mode, setting off the CPU core, the IEEE 802.15.4 transceiver, and all the functional hardware blocks that are not required, such as memory devices and data acquisition blocks.

In Fig. 12, the proposed coordinator node power consumption with a 3.3V system power supply, is represented. As the proposed coordinator node must stay in active mode at all times, after the power-up time, and once all the peripherals are started up, its power consumption remains constant during its entire functionality. Measured proposed coordinator node power consumption under normal functionality is about 22.48 mA, including the power consumption of the continuous operation of the CPU core, IEEE 802.15.4 transceiver, and CAN transceiver.

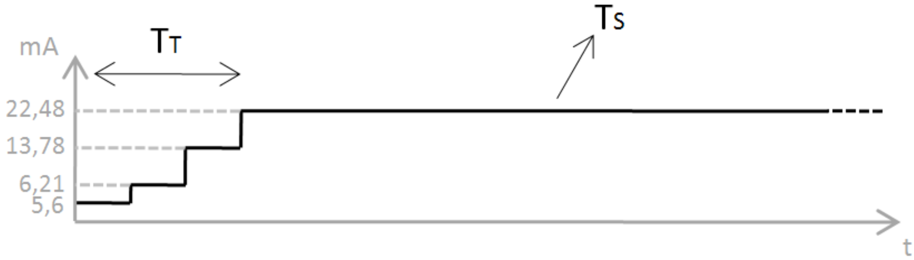

Figure 12. Proposed coordinator node measured power consumption. T_T is the coordinator node startup period, where all the functional blocks are switched on gradually; T_S is the static average power consumption.

As the WSN node's power consumption minimizing method consists mainly in minimizing the module activity during idle periods, where no system management is required, the module power consumption depends directly on four key parameters: the first is the power consumption during normal or active mode operation, where system management processes are active, including the CPU core and the IEEE 802.15.4 transceiver in transmitting or receiving mode. The second parameter refers to the power consumption when the system is under low power mode. In this case, only the minimum of required functional blocks remain active, such as the power supply block. The third is related to the time period required for data acquisition and communication processes with the coordinator node, where the sensor node acquires the physical parameter to be measured, and transmits it to the coordinator node, a task that requires the system to be in active mode. The fourth parameter is the time period where the system is in low proper mode, which practically matches the selected transmitting period.

Fig. 13 shows a graphical representation of the proposed sensor node power consumption during normal functionality using 3.3V for the system power supply. The node has been configured to transmit the temperature measured every 60 seconds, setting low power mode during the remainder of the measuring period. The measured sensor node power consumption under active operation is about 19.2mA with an average time of activity of 2.7 seconds, and 496.2 µA with low power mode during the remaining time period. This sets an average power consumption of 1.33 mA for the selected parameters under normal functionality.

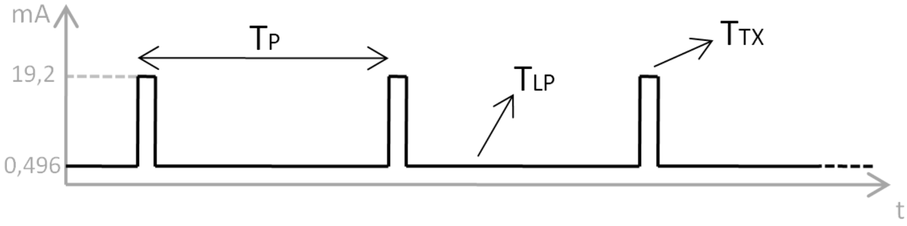

Figure 13 Proposed sensor node power consumption; T_P is the time period between consecutive data transmissions; T_{LP} is the low power consumption time period; T_{TX} is the transmission time period.

Table 3 shows a statistical summary of the power consumption of the two types of node implemented in the proposed solution, by selecting a period of 60 seconds for data acquisition and frame transmission.

Module	Peak power consumption (mA)	Average power consumption (mA)
Coordinator node	-	22.48
Sensor node	19.2	1.33

Table 3. Summary of node power consumption.

In Fig. 14, the total power consumption of the proposed sensor node depending on the selected transmission period, in seconds, is represented. As Fig. 14 shows, widening the transmission period implies a reduction in the average power consumption of the sensor node, becoming closer to the low power mode consumption, where the majority of functional system blocks are inactive.

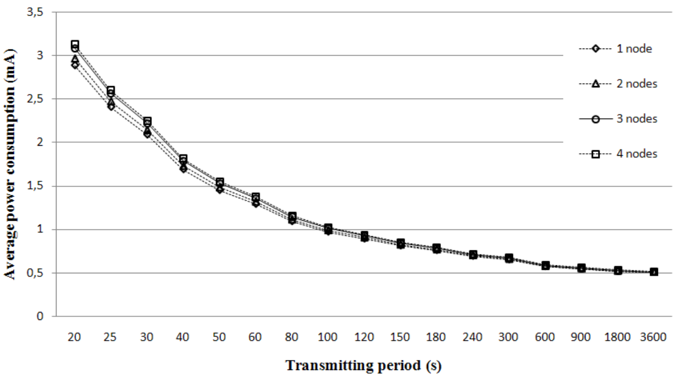

Fig. 14. Proposed sensor node average power consumption as a function of the transmission time period.

6.4 Features

Table 4 shows a comparison between highlighted features of communication standards for WSN development, and the proposed approach.

Standard	Unique central node	Max. number of nodes	Authentication in NWK layer
ZigBee	Yes	2^{64}	No
6LoWPAN	Yes	2^{64}	No
BluetoothLE	Yes	2^{1}	Yes
Proposed	No	2^{16}	Yes

Table 4. Standard feature comparison.

As Table 4 shows, there is no available communication standard for WSN deployment that allows more than one central node belonging to the same network, which in some cases results in a limited architecture for wide area, high mobility WSN deployment. The proposed network architecture supports WSN structures with more than one coordinator node in order to allow the development of wide geographic area networks without the need for deploying several networks. Also, the available WSN standards usually support an oversized node address field size, allowing a WSN to be created with more nodes than are usually needed. In other cases, they only support point-to-point communication between two devices that do not meet the requirements for WSN with deployment of several sensor nodes. The proposed WSN architecture supports a self-authentication process between nodes, allowing the coexistence of several different networks operating within the same range and over the same radio channel, with up to 65536 different nodes belonging to the same WSN.

7. CONCLUSION

The work described in this paper consists of the development, implementation, deployment, and experimental validation and characterization of an IEEE 802.15.4 based WSN architecture intended for use in wide area applications with high mobility nodes. Among the significant improvements of the proposed solution is a functional WSN modification that makes possible the coexistence of multiple coordinator nodes belonging to the same network, and where any sensor node that belongs to it may establish a connection and exchange data frames. This feature is possible thanks to the proposed field segmentation of the extended address assigned to each node, allowing the sensor nodes that want to connect to a coordinator node, to select those nodes that belong to the same network and proceed to validate the association using a frame exchange based validation protocol. Thus, the resulting WSN provides a great flexibility, allowing the coexistence of several coordinator nodes operating simultaneously and geographically redundant coverage of the multiple sensor nodes that are operating in the range of any of these coordinator nodes. Finally, the deployment of an experimental WSN for monitoring the temperature in a cooled vehicle fleet over a wide geographic is presented. The proposed solution eases the development of devices used for consumer applications such as wearable electronics, environmental sensing, identification, or authentication, by supporting spontaneous self-configuration.

REFERENCES

[1] B. Kim, J. Park, Ch. Kan and D. Eom, "An implementation of wireless sensor network", IEEE *Trans. Consumer Electron.* Vol. 50, no. 1, pp 236-244, Feb. 2004

[2] M. A. Lopez-Gomez and J. C. Tejero-Calado, “A lightweight and energy-efficient architecture for Wireless Sensor Networks,” IEEE *Trans. Consumer Electron.*, vol. 55, no. 3, pp. 1408–1416, Aug. 2009.

[3] H. Cho, H. Jang, and Y. Baek, “Practical localization system for consumer devices using Zigbee networks,” *IEEE Trans. Consumer Electron.*, vol. 56, no. 3, pp. 1562–1569, Aug. 2010.

[4] K.-I. Hwang, B.-Jo Choi and S.-H. Kang, “Enhanced self-configuration scheme for a robust ZigBee-based home automation,” *IEEE Trans. Consumer Electron.*, vol. 56, no. 2, pp. 583–590, May 2010.

[5] J. Li, X. Zhu, N. Tang, J. Sui, “Study on ZigBee Network Architecture and Routing Algorithm”, *2010 2nd International Conference on Signal Processing Systems (ICSPS),* pp V2-389-393, July 2010, Delian (China)

[6] *15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*, IEEE Standard 802.15.4-2006, Sept. 2006.

[7] S. H. Kim et al. “UPnP-ZigBee internetworking architecture mirroring a multi-hop ZigBee network topology,” *IEEE Trans. Consumer Electron.*, vol. 55, no. 3, pp. 1286–1294, Aug. 2009.

[8] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, “Transmission of IPv6 packets over IEEE 802.15.4 networks,” IETF RFC 4944, Sept. 2007.

[9] N. Kushalnagar, G. Montenegro, and C. Schumacher, “IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, assumptions, problem statement, and goals,” IETF RFC 4919, Aug. 2007.

[10] D. Johnson, C. Perkins, et al, “Mobility Support in IPv6,” IETF RFC 3775, June 2004.

[11] J. Kim, R. Haw, E. J. Cho, C. S. Hong, and S. Lee, “A 6LoWPAN sensor node mobility scheme based on proxy mobile IPv6”, *IEEE Trans. Mobile Computing,* Issue 99, Nov. 2001.

[12] J. N. Al-Karaki and A. E. Kamal, “Routing techniques in Wireless Sensor Networks: a survey,” *IEEE Wireless Commun. Magn.,* vol. 11, no. 6, pp. 6–28, Dec. 2004.

[13] H. Zhang and H. Shen, “Energy-efficient beaconless geographic routing in Wireless Sensor Networks,” *IEEE Trans. Parallel Distrib. Syst.,* vol. 21, no. 6, pp. 881–896, Jun. 2010.

[14] X. Wang, “Constructing a 6LoWPAN Wireless Sensor Network Based on a Cluster Tree”, IEEE Transactions on Vehicular Technology, vol. 61, no. 3, pp. 1398-1405, March, 2012

[15] A. Haffiz Shuaib and A. Hamid Aghvami, “A routing scheme for the IEEE-802.15.4-enabled Wireless Sensor Networks,” *IEEE Trans. Veh. Technol.*, vol. 58, no. 9, pp. 5135–5151, Nov. 2009.

[16] W. Wang, F. Xie, and M. Chatterjee, “Small-scale and large-scale routing in vehicular ad hoc networks”, *IEEE Trans. Veh. Technol.,* vol 58, no. 9, pp 5200–5213, Nov. 2009.

[17] S. Pileggi, “A multi-domain framework for Wireless Vehicular Sensor Network”, *IEEE Int. Conf. Ultramodern Telecommunications & Workshops ICUMT’09,* pp 1–8, St. Petersburg, Oct. 2009.

[18] *Guidelines For 64-bit Global Identifier (EUI-64)*, IEEE Standards Association, 2011.

[19] M. Rodelgo-Lacruz et al. “Base technologies for vehicular networking applications: review and case studies”, *IEEE Int. Symp. Industrial Electronics 2007, ISIE 2007*, pp 2567–2572, Vigo (Spain), June 2007.

[20] J. Bian, R. Seker, S. Ramaswamy and N.Yilmazer, “Container communities: Anti-tampering Wireless Sensor Network for global cargo security”, *17th Mediterranean Conf. Control and Automation, 2009. MED '09*, pp. 464–468, Thessaloniki (Greece), July 2009.

[21] S. De Lausnay et al. “Zigbee as a means to reduce the number of blind spot incidents of a truck”, *IEEE 22nd Int. Symp. Personal Indoor and Mobile Radio Communications (PIMRC)*, pp. 1239–1243, Toronto (Canada), Sept. 2011.