Performance evaluation of an AODV-based routing protocol implementation by using a novel in-field WSN diagnosis tool

Gabriel Mujica , Jorge Portilla, Teresa Riesgo

A B S T R A C T

The Wireless Sensor Network research field has been growing and becoming more mature during the last decade since novel technologies and research lines have emerged targeting its usability under different real scenarios. One of the key topics to assure the efficiency and effectiveness of these technologies in final applications is the quality of the service and the reliability of the whole system, which strongly depends on the communication/topology capabilities as well as routing strategies within the WSN. In this context, it is essential to evaluate the implementation of routing algorithms and network connectivity in actual deployments, as a support to theoretical simulation models that cannot predict certain constraints and limitations in the system behavior. These are the main reasons why a real implementation of a flexible AODV-based routing protocol using a modular HW-SW node platform is proposed in this work, in addition to its practical assessment under real conditions by using a novel in-situ WSN performance evaluation tool. This tool has been created as a support for users during the in-field deployment analysis and diagnosis in real environments, in order to correlate theoretical results with the operation of the network beyond the typical study of routing performance with WSN simulators.

1. Introduction and related work

During the last decade the Wireless Sensor Networks (WSNs) have emerged as a key and challenging topic for the research community due to the inherent integration of a wide range of different hardware and software technologies, protocols and new algorithms in order to maximize their performance and feasibility in final applications. One of the most relevant aspects to be considered to assure the efficiency and effectiveness of these technologies in real scenarios is not only the quality of the service of the whole implemented system, but also the robustness and reliability of the network performance, which strongly depends on the communication capabilities as well as topologies and routing strategies within the WSN. In this context, routing problems in WSNs have been studied from different perspectives, depending on the target application, topologies needed for specific scenarios and environments, network mobility and scalability, and data aggregation [1].

On one hand, from the point of view of the network structure to be adopted, three major groups of routing algorithms can be distinguished. The first one is the flat-based routing protocols [2], in which nodes have the same role in order to collaborate in achieving the

goal of the wireless deployment in a reliable way. Flexibility is a key aspect covered in these types of protocols due to the possibility of having different alternatives to disseminate the sensor information, which is important in unstable environments where the quality of the links are prone to be affected. The second group is the hierarchical-based routing protocols, in which two main types of roles are defined. Sensor nodes are used to gather the target measurements whereas cluster nodes retransmit these data to the base station. Such configuration aims to reduce the power consumption of the sensor nodes, since they do not need to include routing capabilities and then special sleep modes can be adopted for the former type of device [3]. However, these routing protocols are mainly intended to be used in stable environments where the probability of communication failures is lower, and the redundancy criteria are not a critical network requirement. The third group is focused on location-based protocols, in which nodes find the routing alternatives by knowing their location (using signal-strength-based algorithms or adding GPS-based hardware to the sensor implementation) with respect to the surrounding neighbor nodes [4].

On the other hand, considering how routes are discovered and created, routing algorithms can also be classified in proactive, in which the mechanism periodically or continuously attempts to determine the routes even if they are not used, so that the corresponding path is already available whenever a node needs to send a packet to a destination point [5]. Although this schema reduces the time delay when a

packet has to be transmitted, it has poor performance in unstable environments where the routes are prone to be changed or in network mobility, in which the frequency of the connectivity reconfiguration is much greater, in addition to its high energy and resource consumption to maintain the routes. In order to cope with these limitations, a second classification is included, the reactive protocols, in which the route determination is performed on demand [5]. This means that the first time a source node needs to send a packet to a destination node the route mechanism will attempt to discover a connection path and then keep such route for subsequent transmissions. Although this schema may increase the delay of the transmission process due to the route request procedure, it is more flexible and less resource consuming in those environments where the connectivity can be more unstable.

Most of the aforementioned mechanisms and the state-of-the-art routing protocols have been evaluated by using simulation tools and modeling process, or some of them by controlled testbeds, which give to some extent an idea of what the functionality of the mechanism will be. However, fewer works focus on implementing and integrating routing protocols in real hardware platforms and tested in actual scenarios in order to analyze the performance and the efficiency of those implementations under real and operational conditions of the deployment, as well as dealing with the resource limitations of sensor nodes. In this context, it is essential to evaluate and validate the implementation of routing algorithms and network connectivity in real deployments, as a support to theoretical simulation models that cannot predict certain constraints and limitations in the behavior of the system. These are the main reasons and motivations why a real implementation of a flexible AODV-based (Ad hoc On-Demand Distance Vector) routing protocol using a modular HW-SW platform has been deeply studied and is proposed in this work, as a support of the Cookie nodes [6] and their integration with an IEEE 802.15.4 based communication layer. AODV is a flat-based routing protocol, which provides Cookies with a greater flexibility that allows the use of any required topology by the target application. It is also within the reactive protocol classification, which is more suitable for reconfigurable and Ad-hoc network topologies, being one of the main targets to be covered by Cookie implementations. The proposed implementation, called CB-AODV (Cookie-Based AODV), aims to help developers to analyze different aspects, constraints and requirements in the use of reactive routing protocols in real WSN application scenarios.

Such an approach brings another important issue for the success of the implementation of routing algorithms along with the network operation. Nowadays there is a lack of well-defined practical tools to analyze and evaluate the implementation of routing protocols and communication topologies in WSNs within their real operational environments and final application scenarios. Most previous works regarding the optimization process of WSN deployments targeted simulation and modeling techniques at the planning stage [7,8], so that the output models serve as a starting point for experts to carry out the commissioning activities following pre-deployment guidelines, which has been studied from a simulation perspective and considering some assumptions at system low-level implementation.

Furthermore, the behavior of routing protocols running in actual hardware platforms might be far from the expected simulation results or even from the testbed scenarios with respect to the final operability of the system, specially in terms of communication performance, due to limitations concerning the core and memory architecture on which routing algorithms are to be implemented, as well as computational and processing limitations that are not taken into account during the modeling process. In this work, a practical assessment of routing protocols (and specially for the CB-AODV implementation) under real conditions is also proposed as another major contribution, by means of creating a novel in-situ WSN evaluation tool (I-DPEs, In-situ Diagnosis & Performance Evaluation System). This tool is proposed to support users during the

in-field deployment configuration, analysis and diagnosis in order to correlate theoretical results with the operation of the network in real environments and under actual conditions, beyond the typical study of routing performance through WSN simulators. Moreover, the aim of this support tool is to provide deployers with the possibility of considering and analyzing in runtime different abstraction levels of the target system implementation to enrich the on-site analysis and assessment. There are works focused on coping with the evaluation of routing protocols from a simulation perspective, such as the framework presented in [8], or the performance analysis of Ad Hoc networks proposed in [9]. However, fewer proposals try to address practical assessment of network connectivity and in-field analysis of routing mechanisms, such as the work presented in [10], or general approaches for evaluating node functionalities [11]. In [12], authors proposed a toolkit for evaluating collection tree protocols from a simulation perspective as well as translating their TinyOS implementation to a controlled testbed, where nodes are connected to PCs to gather data and statistics, which is more focused on a laboratory approach for pre-deployment analysis, similar to the approach proposed in [13], where the network testing information is collected through a sink node which then retransmits the data to a remote performance analysis system, by means of using a wired connection or Wi-Fi. Yet, these types of implementations are more focused on pre-deployment infrastructures where a controlled/rigid network is used, specially targeting the remote analysis of applications' behavior.

The rest of the paper is organized as follows, starting with the CB-AODV implementation and its integration with the HW-SW platform in Section 2. In Section 3 a discussion regarding the proposed in-situ Evaluation Tool together with its main designed capabilities are presented, whereas in Section 4 experimental results and comparisons are analyzed in detail. Finally, conclusions and contributions are provided.

2. CB-AODV design and development

As previously remarked, routing protocols in WSNs are a fundamental part to assure the success and the effectiveness of the target application as well as the quality of the provided service. Since the IEEE 802.15.4 standard [14] (which is the most common communication standard used in WSNs) only includes the PHY and MAC layers and not the upper levels, it is necessary to implement a routing protocol that allows using different network topologies and not only the star topology (where the coordinator has full coverage with the rest of the nodes, and the communication is only possible between a node and the coordinator). Therefore, the routing protocol allows multihop-based networks where the messages hop between different intermediate nodes until they arrive at the final destination.

In this way, the modularity of the Cookie platform [6] allows an easy integration of different communication modules to establish the wireless connection among the deployed nodes, such as the already implemented Bluetooth and ZigBee layers. Thus, in order to deeply analyze network connectivity issues in WSNs from different abstraction levels and specially targeting the study of real implementations of routing protocols, a new communication layer has been designed and implemented based on the IEEE 802.15.4 standard, taking advantage of the ease of prototyping in the Cookie platform, as shown in Fig. 1. The selected module is the well-known CC2420 from Texas Instruments [15], which has been widely used in different node platforms.

This communication layer has been designed to be managed from the processing layers of the Cookie platform, which means that the main processing element (the 8051-based microcontroller) hosts the controllers of the module (such as the RAM managing and configuration command), and the co-processor (the FPGA) allows hardware debugging issues and power mode's triggering. These controllers have been implemented following the HW-SW integration framework [16]

Fig 1. IEEE 802.15.4-based Cookie communication layer.

that defines the low level libraries to efficiently handle the modular platform capabilities, as shown in Fig. 2, where the new module manager and its internal functionalities are highlighted together with the rest of the controllers.

As studied in the previous section, there are various routing protocol strategies that can be adopted depending on the requirements of the WSN deployment as well as the application/scenario constraints to be tackled. Due to the inherent instability nature of the WSN communications, a dynamic mechanism to discover the multi-hop data path between two remote points is a prior decision when implementing a particular routing technique. Moreover, there are design requirements that might determine how nodes shall disseminate data throughout the deployment, such as centralized traffic models, where one or more coordinators serve as sink elements of the data flow; differences in processing, memory and energy constraints according to the sensor features; cooperative models where distributed processing and path redundancy are key aspects to be considered; and mobility or volatile interconnections in which the routing paths are variants during different operational stages.

In Fig. 3, based on the analysis of the main types of categories of routing techniques, different proposals can be distinguished, such as GAF (Geographic Adaptive Fidelity) [17], which uses location information to establish coherent association with surrounding nodes, so that they can determine which of them can sleep while the others route packets; LEACH (Low Energy Adaptive Clustering Hierarchy) [18] in which sensor nodes transmit information to cluster heads that then distribute the data in a compressed fashion to the base stations, so the energy consumption is balanced trying to extend the network lifetime; OLSR (Optimized Link State Routing) [19], that tries to minimize rerouting latencies by maintaining and rediscovering paths so that they can be available even if they have not been demanded, which increases the overhead of the network; RPL (Routing Protocol for Low power and Lossy Networks) [20], that forms a tree topology where each node has its corresponding parent through which it transmits

Fig. 3. Routing protocol classification based on the type of strategies.

packets to a root node; and ZRP (Zone Routing Protocol) [21], that combines the advantages of a reactive mechanism among neighbors while applying a proactive technique among neighborhoods. The well known CTP (Collection Tree Protocol) [22] implemented under TinyOS can be classified as a data-center-based protocol, where the directionality of the data flow is defined from sensor devices to coordinator nodes by using a tree schema based on the quality of the interconnections. Another popular mechanism is the Dynamic Source Routing (DSR) [23], which is a reactive protocol where the entire path between two nodes is stored in the information/control headers of the packets.

Based on the inherent flexibility of the Cookie nodes to be adapted to different WSN application contexts, and also according to the state-of-the-art analysis of the previous section, the AODV-based routing protocol [24] has been selected as the most suitable algorithm to be integrated into the HW-SW platform, due to its adaptability to different network environments, as well as its reconfigurability in ad-hoc network topologies. Taking advantage of the benefits of this routing protocol, a modified version is proposed to be adapted and implemented in a real HW-SW node platform (named CB-AODV), specially targeting large-scale and unstable environments, where a versatile routing mechanism has to be adopted, as described in the following subsections.

Fig. 2. IEEE 802.15.4 module management integration overview in the Cookie HW-SW support platform.

Fig. 4. Example of route discovery from node 1 to node 6.

2.1. Basic operation of the protocol

The AODV protocol uses 4 different types of control messages to create and maintain the routes of the network. These messages are named RREQ (route request message), RREP (route reply message), RERR (route error message) and HELLO. Moreover, every node of the network keeps a routing table with different fields that include information for the maintenance of the routes. When a node decides to send an application packet to another remote node of the network, the first step is to check if it has the route to the destination point in its own routing table. If so, the message is then sent to the next node of the route. This is repeated along the whole path until the packet reaches the final destination. In case that the node does not have information of the route, it will store the packet and start the route request process by broadcasting a RREQ message. The devices that receive this message will rebroadcast it until one of the nodes has information of the route, or the destination itself is the one that receives such request message. In both cases the node will send a RREP to the previous node until it reaches the source node that requested the route, and then the application packet previously stored is finally sent through the discovered path.

In this way, with the propagation of the RREQ, the nodes update their corresponding routing table with the information of the source node, thus creating what is called the inverse route. In addition to this, nodes also create a route table entry with the information of the node from which they received the RREQ, hence creating routes to their neighbor nodes. With the propagation of the RREP, a direct route is created, which implies that the different nodes where the RREP hops create a route to the destination point. In Fig. 4, the process of discovering a route from node 1 to node 6 is shown, as well as the different messages that are sent to carry out the aforementioned procedure.

The computed routes are only valid during a limited period of time, and once they are not used within this timeout they are marked as invalid, and therefore they are no longer available for use. The original routing protocol defines the HELLO messages that are broadcasted periodically by all the nodes of the network in order to maintain the routes. However, as presented in the following subsections, these types of messages are not included in the modified implementation, aiming to have a more efficient performance in terms of power and resource consumption by reducing the network

overhead. Whenever a route changes its state from active to inactive due to not being used in a period of time or due to a link failure in the propagation of a data packet (no acknowledge received in any of the attempts to send a packet to the next hop), the node that detects the failure sends a RERR to all of its precursors nodes, i.e., those nodes that use the former node as their next hop. The precursors will then repeat the same process until the nodes that used the fail route eliminate it from their routing table.

In this overall behavior, in order to effectively perform the routing mechanism, the main information that has to be kept by every node is as follows:

- Destination address.
- Sequence number of the destination node.
- Sequence number state.
- Route state.
- Number of hops.
- Next hop.
- Precursor lists.
- Lifetime of the route.

2.2. CB-AODV – HW-SW adaptation

The AODV routing protocol was initially implemented to be used in MANET networks (mobile ad-hoc networks). Despite all the similarities with respect to the WSNs, the wireless nodes have less processing capabilities and the battery autonomy has to be taken into account in order to enhance the overall lifetime of the deployment. Because of that, it is necessary to adapt the protocol to the WSN characteristics and especially targeting the architecture of the Cookie HW-SW platform and its usage in real application scenarios.

Therefore, the proposed adaptation is focused on adding new functionalities to the original protocol to make the dynamic behavior of the mechanism more efficient, and not including some others aiming to improve and optimize the overall performance of the algorithm for the purpose of the Cookie node connectivity, and thus reducing the resource consumption in this system architecture. The CB-AODV implementation has been fully developed in line with the specific resources of the Cookie hardware platform, so that the memory scheme is highlighted to take full advantage of the architecture.

First of all, there are basic adaptations that have been adopted to guarantee an efficient implementation in terms of power consumption and resource handling, as follows:

Reduction of the control message headers and the routing tables: This is one of the most suitable optimizations because many of the fields of the message frames are not used and some of them can be reduced for most of the applications. The most important fields to be considered are the ID bytes of the messages, involved nodes and their sequence numbers. Additional flags and mask bytes are not needed for the target implementation. Moreover, for those Cookie-based applications where the deployment is partitioned in <255 nodes, the identification fields are optimized to single bytes, so that both the control packets as well as the indexed tables are considerably reduced in terms of memory usage and data access process.

Elimination of the time to live of the routes and suppression of HELLO messages: With this optimization it is possible to reduce overhead of the network (messages are not sent periodically for route maintenance). Moreover, since the dynamics of a WSN is based on having duty cycles in which sensors remain in stand-by, there is no need of expending additional resources to check if the routes have been used for a period of time, thus reducing the implementation size. In any case, even if the deployment requires higher data traffic, routes are maintained by combining three elements: ACK packets during data transmissions (MAC layer), RERR messages, and a new type of dissemination integrity process that is introduced later on in this section. Therefore, the maintenance of the routing paths is checked/performed in a reactive fashion as well (only when needed), thus avoiding wasting energy and simplifying the implementation.

Expanding Ring Search algorithm removed: This algorithm is based on searching the routes by using RREQ messages with a low TTL (time to live, i.e., maximum number of hops that the message can do during the discovery process). If no RREP is received, then the RREQ is rebroadcasted and the TTL is increased until the route is discovered or the TTL has reached its maximum value. This algorithm is used to avoid flooding the network in crowded topologies, at the expense of increasing the latency.

In addition to the aforementioned modifications, new features and additional properties have also been included in the CB-AODV in order to increase its performance without penalizing the memory and processing resources of the architecture. These important characteristics are classified as follows.

Implementation of different types of metrics: The discovery metric is a fundamental parameter used to compare the different route alternatives that can be obtained during a route discovery process. In terms of processing and implementation, the easiest way to make a decision is just register the first path found during the discovery mechanism (no buffers of control messages have to be used to handle different alternatives). However, within the context of dynamic communications of WSN deployments, this approach is not enough to assure the effectiveness of the remote interconnections and the quality of the data transactions. On the other hand, the metric applied in the AODV protocol is the number of hops (i.e., as less number of hops as possible to determine what route is the best), which has poor performance in unstable and “crowded” WSN application environments. This approach could reduce the latency during the packet delivery, but actually, if the different links along the path are unstable in terms of the quality of the connection, transmissions attempts could considerably increase, thus penalizing the time and energy consumption of the involved nodes during the communication transactions.

Therefore, it is fundamental to consider other types of metrics that can discover the best routes in terms of the quality of the interconnections among the wireless nodes. For this purpose, metrics that use a parameter called LDR (Link Delivery Ratio) for measuring the percentage of messages that will be successfully sent between 2 nodes are considered. The main idea is to study the reliability of two remote points in terms of data delivery by calculating the quality of

the transaction between every pair of nodes along the route path, which can be directly calculated by triggering a determined amount of packets between them. Of course, this method cannot be afforded in a real WSN because it is energy and bandwidth consuming, so there are studies in the state of the art [25] in which the main efforts are focused on how to correlate the LDR with the most common data quality indicators, which are provided by the IEEE 802.15.4 layer: LQI (Link Quality Indicator) and RSSI (Radio Signal Strength Indicator).

In the Cookies implementation, a correlation between the LQI and the LDR for the CC2420 radio transceiver has been studied based on the work proposed in [25], but also adding the RSSI parameter to the estimation so that a more complete model can be used. The main target is to obtain a real correlation of both parameters for the Cookie platform by applying an experimental setup with the designed communication layer, so that the prediction model of the data delivery is more adapted to the hardware platform.

Based on this approach, the experiments were configured in a free-space scenario at the ETSII-UPM, considering two Cookie nodes with the same position at the same height (1 m from the ground) and distance samples starting from 1 m up to 35 m. Moreover, the range of the TX power configuration of the radio modules is swept from 0 dBm to -25 dBm, so two levels of interactions are fully considered to guarantee a higher amount of experimental data to be correlated, obtaining up to 4236 test/measurement cases during the testing process in the in-field testbed scenario. As a result, the comparisons and main contributions for the in-field modeling of the communication and quality metrics are presented in the experimental analysis section.

Based on these results as well as considering the analysis proposed in [25], the inclusion of different types of quality-based metrics is taken into account, so that the CB-AODV can be evaluated under several routing discovery decisions, as follows:

- PATH-DR (Path Delivery Ratio) metric: this metric calculates the percentage of messages that theoretically will be successfully sent in a route. It is based on the LDR parameter.
- ETX (Expected Transmission Count) metric: tries to minimize the number of hops by taking into account the possibility of link failures due to the quality of the LDR parameter.
- Number of hops: as explained before, it is the original metric used in the protocol, which consumes less memory resources due to its ease of calculation and implementation.

It is important to highlight that the modularity of the implementation allows changing the corresponding metric depending on the target application and the conditions/requirements of the scenario.

On the other hand, in this work a new type of metric is also introduced: *E-aDM* (Energy-efficient and adaptable Delivery Metric) targeting the enhancement of the network lifetime, by considering energy and resource factors in every computed node calculation. The main idea is to bring the possibility of reconfiguring the influence of every particular node along the path depending not only on the estimation of the LDR, but also on other factors that could affect the performance of specific nodes or neighborhoods during their operational behavior.

The calculation of the metric is obtained on the basis of the PATH-DR mechanism, in which every node computes and incorporates its LDR parameter in the control packet during the discovery process. However, before indexing such indicator, the node first penalizes its value by applying the following expression as a multiplier (1), which includes the elements that could influence its performance in long term operation:

$$\delta = 1 - \gamma \quad (1)$$

where γ is

$$\gamma = (C_{pl}^* w_{pl} + C_{bc}^* w_{bc} + C_{ib}^* w_{ib}) / (w_{pl} + w_{bc} + w_{ib}) \quad (2)$$

Fig. 5. General structure of the new type of message DATA_ERR.

C_{pl} is a neighborhood factor representing the number of precursors that use the node as their next hop, so it can indicate the degree of saturation with respect to other nodes along the path or in the distribution of the routing tasks. The C_{bc} is the energy consumption factor, which expresses the amount of battery level that has been used from the beginning of the node's operation. It is computed as the maximum voltage value of the connected battery minus its runtime measured value. This node's consumption is also correlated with the TX power configuration of the radio communication module to be used, as well as the estimation of the long-term autonomy based on its operational/computational cycle. C_{ib} is a firmware implementation indicator which considers the number of effective functional and processing blocks that have been integrated in addition to the general controllers of the SW support platform to perform application-dependent tasks, so it measures the processing load that the node has in order to carry out its functions. w_{pl} , w_{bc} and w_{ib} represent the weights of every condition according to how critical they are considered for a particular node or deployment. They go from 1 to 5 (1 for those topologies where rely nodes are more critical along the routing path, thus less redundancy; and 5 for those nodes which have higher computational load in terms of processing capabilities within the wireless deployment) and can be reconfigured depending on the target requirements/constraints and the type of deployment plan.

It can be seen that, the greater this factor is (the conditional elements are higher, i.e., the number of precursor nodes, the number of implement blocks and the consumed power), the worse the measured metric would be for a particular node. With this schema, a trade-off between performance and energy efficiency is taken into account, so that energy and routing balance throughout the deployment can be achieved. Moreover, regarding network diagnosis capabilities, the balance of these factors speeds up the detection and debugging of possible non-functional nodes in terms of power consumption anomalies, by means of correlating the number of implemented blocks, the lists of precursor nodes and the power mode configuration with the actual in-field energy spent per node.

New type of message: in addition to the included features, in this work a novel type of message has been implemented for the CB-AODV protocol, called DATA_ERR. The aim of this new control message is to enhance the dissemination capabilities of fragmented information by supporting integrity verification of the data flow, in addition to the local repair and rediscovery processes.

Whenever an intermediate node discovers a link failure when transmitting a data packet, after sending the RERR (to its precursor list) it will also send the originate message to the source node indicating that it is a DATA_ERR message. When the originator of the message receives the DATA_ERR, it will store the data packet and then try to discover an alternative path to send the message, so that an information checking process is performed in order to avoid losing critical data in unstable WSN application environments. This is especially useful when splitting an information stream that targets the reconfiguration of specific functional blocks of the HW-SW platform, where several data packets have to be efficiently sent to assure the correct

configuration mechanism, or in cooperative networks where the efficiency in data distribution is enhanced. The structure of the control packet is similar to the already defined ones, as shown in Fig. 5.

There are also other types of protocol adaptations proposed in the state of the art [26] to reduce the need of memory and processing capabilities as well as the complexity of the protocol by not incorporating some of the functionalities of the technique in such implementations. However, those modifications are not included in CB-AODV (although the modularity of the implementation allows "plug-in/out" several functionalities to be included in the target node, aiming to create a more compressed integration when needed), because they also reduce the performance of the protocol implementation and were no necessary reductions within the Cookie platform context, in which a trade-off between performance efficiency and resource constraints is adopted to assure its flexibility in different application scenarios. Those features are described as follows:

Suppression of the Local Repair mechanism: The Local Repair is a functionality in which an intermediate node discovers a link failure when sending a message and, instead of sending a RERR message, it will try to find an alternative route without the need of notifying such event to the packet source. If the Local Repair mechanism is deleted it is possible to reduce the consumed memory because an output queue is no longer needed when trying to rediscover a new route in order to keep the pending data. However, it decreases the protocol performance, since the dynamic capabilities of fixing localized problems is restricted to the originator of the messages, so that more discovery actions have to be disseminated and wasted. Hence, the Local Repair Mechanism is indeed included in CB-AODV.

Precursor list: As explained before, when a node detects that a route is no longer valid because a failure and no alternatives were found during the local repair mechanism, the RERR messages are sent to the precursor nodes of the route that has failed. This means that, from the implementation point of view, it is necessary to include a record of precursors for every routing table entry, which increases the memory usage. However, this is an important aspect to be considered for a better performance of the protocol, since if precursor lists are not implemented, the propagation of the RERR messages is then carried out as the propagation of RREQ messages is, which may flood the network and they might cause the suppression of routes that did not need to be eliminated. Therefore, in CB-AODV, this feature is fully supported to obtain a better dynamic behavior of the protocol.

Metric implementation: As previously explained, there is a possibility of omitting the inclusion of metrics for selecting more efficient routes when discovering them. In this way, the node only generates a RREP for the first received RREQ and not for the rest that it might receive during the discovery process (even if they are better routes). This option allows reduced memory in the routing tables and the size of the control message frames, but decreases the effectiveness and robustness of the protocol. Moreover, by appropriately applying metrics, a correct balance of the energy consumption of the nodes with respect to communication tasks can be achieved. As described before, in the CB-AODV implementation it is possible to select and customize

Fig. 6. General overview of CB-AODV with the main functional blocks.

this metric capability by changing the configuration of the discovery mechanism according to the application constraints.

Only the final destination is capable of generating RREP messages: This has the advantage that no loops (circular paths in which the message continuously hops never reaching the destination) are made because the intermediate nodes cannot generate RREP. The sequence number is a field in the routing table and in the control messages created to avoid the generation of loops, so if no loops can be created, then sequence numbers are no longer needed. However, this type of mechanism aims to reduce the amount of retransmission packets that can be avoided without wasting energy and processing resources on them. Therefore, the sequence numbers are fully supported in CB-AODV to allow intermediate nodes to generate RREP messages during the discovery procedure.

Elimination of RERR messages: In a very compact implementation, the inclusion of RERR messages can be omitted to decrease the complexity of the protocol, but it can lead to have a quite poor handling of errors especially in unstable scenarios where links are frequently prone to fail.

2.3. Integration of CB-AODV in the Cookies HW-SW platform

The design and integration of CB-AODV has been carried out based on the resources and the modular HW-SW architecture of the Cookie nodes, and on the basis of the developed communication layer. In this way, the libraries that handle the proposed features are included on top of the IEEE 802.15.4 controller that was created to manage the hardware implementation. This set of lightweight libraries, which has been coded in C language for 8051-based architectures, is defined to support the Cookie architecture in an efficient and resource-optimized fashion, unlike other implementations that have been defined to be used over operating systems such as TinyOS.

In summary, the implementation is mainly composed of 3 blocks of libraries, as shown in Fig. 6, where CB-AODV is integrated within the context of the Cookie SW support platform and data processing. The main block (*CB_AODV*) is in charge of performing the main functionalities and the dynamics of the routing mechanism regarding control message coding/decoding and protocol information management, based on the packet frames coming up from the MAC layer handler. *CB_AODV_Table* is in charge of handling the routing tables as well as the reserved memory for this purpose, making use of low-level memory controllers for optimizing the access and management of the routing information entries. On the other hand, *CB_AODV_Queue* controls the input/output buffers as well as the RREQ registers to

handle the protocol information in terms of discovery and dissemination processes. The type of implementation to be downloaded is controlled by using parameters definition that allows making a more compact mechanism (based on the basic behavior of the protocol) or a full/high performance implementation with all the designed capabilities.

It can be also seen that the implementation makes use of different peripheral controllers of the architecture to modularize the data handling, so that the debugging process and the internal usability of the system is highlighted. Besides, as expected, the protocol implementation has been carried out in such a modular way that, from the point of view of the platform users, the application abstraction layer is provided with simple functions for sending packets to and receiving from remote destination points in a *transparent* way.

2.4. Comparison of AODV implementations and proposals

In Table 1, a comparison among different AODV implementations and proposals is shown in detail (based on the comparative analysis proposed in [26]), in which CB-AODV is included. It is important to highlight that there are many proposals in the state of the art that have been analyzed and implemented in simulation, unlike the one presented in this work which has been completely integrated in a new WSN HW-SW platform to be used in industrial applications and real deployments.

The CB-AODV implementation has similar features compared to the NST-AODV, which is one of the most popular AODV implementations for TinyOS, being in this comparison the ones with more characteristics from the original AODV protocol as defined in the RFC and, therefore, the ones that will theoretically have better performance. The main difference between CB-AODV and NST-AODV is that the former one incorporates the precursor lists allowing the protocol to have better efficiency in the propagation of the RERR messages as well as the implicit detection of critical points along the routing path; the inclusion of the DATA_ERR message that targets a more efficient data dissemination process in critical and unstable scenarios; and the proposal of energy-efficient based metrics to enhance the dynamic routing mechanism taking into account the real conditions of every node in the target scenario, thus increasing the performance of the implementation.

As it can be seen in the table, the inclusion of the precursor list has not been added in some of the implementations or proposals. This is because of the additional memory resources that are needed for its inclusion. In CB-AODV, this feature has been added because there is an available internal EEPROM in the core architecture of the Cookie platform, so this free memory space was efficiently used to keep the routing tables. Moreover, as previously explained, another important optimization is also proposed in terms of memory usage. For those applications in which the size of the network is less than 255 nodes, the control message frames can be reduced by means of using a 1-byte-based address field. In this case, the available memory space of the CB-AODV architecture for the routing tables can be also reduced and fixed. This option aims to increase the performance of the protocol since the latency due to routing table entry searching is reduced (memory access) by assigning a predefined position in the table entries for every node, hence speeding up the internal transaction of data processing elements.

2.5. Loop problems

Another key aspect that has been taken into account for the success of the CB-AODV implementation is the possible generation of loops. As explained before, the AODV protocol includes the sequence numbers to avoid this problem. However, the RFC 3561 has some ambiguities and some of the interpretations can yield loops, as detailed

Table 1
Comparison of different AODV implementations and proposals.

	Connectivity maintenance mechanism	Type of Routing Metric	Precursor List implt.	Local Repair mechanism	RERR message	Only destination generates RREP	Specification and/or protocol implementation
AODV RFC 3561	Hello message, LLN, etc.	Hop count	Yes	Yes	Yes	No	RFC experimental
LoWPAN-AODV	LLN	Hop count	No	No	No	Yes	Expired Internet Draft
TinyAODV	LLN (disabled by default)	Hop count	No	No	Yes	Yes	Implemented for TinyOS
AODV-jr	Connect messages (unidirectional traffic)	Fastest RREP	No	No	No	Yes	Implemented for the ns-2 simulator
AODV-bis	Hello message, LLN, etc.	Fastest RREP	No	No	Yes	No	Expired Internet Draft
LOAD	LLN	LQI-based	No	Yes	Yes	Yes	Internet Draft Simulation
NST-AODV	LLN	Multiple metrics	No	Yes	Yes	No	Implemented for TinyOS
CB-AODV	LLN, DATA_ERR	Multiple metrics	Yes	Yes	Yes	No	Implemented for the Cookie HW-SW platform

in [27]. According to such study, every ambiguity has its corresponding interpretations (e.g. 2a and 2b and 2c for the ambiguity 2 in the study) that might end up causing loops. Based on this analysis, there are 4 different interpretations that can cause the generation of loops.

In the proposed CB-AODV implementation, the selected options are the followings:

Ambiguity 1: Updating the unknown (invalid) sequence number in response to a route reply

- The option 1b has been followed in the implementation, since the routing table will be never updated when the sequence number is lower than the one already registered.

Ambiguity 2: Updating with the unknown sequence number

- The option 2c has been followed in the implementation, which avoids the generation of loops while keeping the best route. In this way, if there is a better route to a destination node but the sequence number is unknown (which can happen when receiving RREQ or RREP packets from neighbors that did not originate them, or when receiving RERR messages), the route is changed in the entry table without modifying its sequence number.

Ambiguity 3: Allowing the creation of self-entries in response to a route reply

- The option 3d has been followed in the implementation, thus avoiding the creation of self-entries but without discarding the reply message.

Ambiguity 4: Invalidating routing table entries in response to a route error message

- The option 4c has been followed in the implementation, which does not generate loops since self-entries are not allowed, as explained before.

3. I-DPEs: in-situ diagnosis and performance evaluation system

The performance of routing protocols under realistic conditions is essential to assure the effectiveness and the reliability of the final application where wireless nodes are being used. However, as previously explained, there is a lack of well-defined practical tools to analyze and evaluate the implementation of routing protocols and communication topologies in WSNs under real conditions and final deployments, beyond the simulation/emulation of the modeled algorithms and metrics, since realistic environments include unpredictable situations that cannot be covered in simulation models. Moreover, the behavior of routing protocols running in actual hardware platforms might be far from the expected simulation results, due to limitations concerning the core and memory architecture where routing algorithms are to be implemented as well as computational and processing constraints that are not taken into account during the modeling process, or even during controlled testbed conditions. Therefore, it is crucial to establish an in-field based support mechanism to test and assess a WSN in terms of connectivity and routing capabilities in real deployment scenarios, thus allowing developers to analyze and compare functionalities from different abstraction levels within their implementations in runtime, so that an on-site enhancement of the deployment performance and its operational lifetime can be achieved.

Based on this approach and aiming to test the implemented CB-AODV routing protocol in final application contexts, in this work an evaluation and diagnosis support tool for in-field deployment activities is proposed. The idea is not to fully replace the use of simulators to analyze models and algorithms. Instead, the main target is to provide users with a set of functionalities to compare the behavior of the real deployment with what is expected from the simulation results. A general overview of the proposed architecture is shown in Fig. 7, in which a combination of hardware and software components is integrated in a unique and novel in-field evaluation platform. The

Fig. 7. General view of the I-DPEs architecture.

kernel of the tool is composed of a mobile device which contains the top level application and with which users can move in the target field in order to analyze specific deployment areas. The integration of a commercial AndroidOS-based Tablet connected to a Cookie-based platform that implements the corresponding WSN communication protocol is the basis of the aforementioned architecture. This configuration aims not only to experiment with IEEE 802.15.4 and protocols on top of it (such as CB-AODV, which is the main target) but also to take advantage of the modularity of the Cookie platform by replacing the communication module with other stacks, such as ZigBee or 6LowPAN. The second important part of the implementation is the inclusion of a diagnosis component into the wireless nodes in order to gather information of the deployment from the evaluation tool. This component is able to extract information of the HW-SW implementation for different abstraction levels and forward it to the evaluation tool. Hence, real data can be analyzed in runtime in order to compare the performance of the simulated models with the behavior of the network.

In order to carry out this comparison, available data regarding network/node configurations and simulated parameters have to be taken into account during the commissioning and diagnosis stages of the WSN deployment. As a result of this requirement, a third aspect is included within the scope of the proposed platform, the capabilities of downloading configuration files containing deployment information and network modeling, generated by simulations and planning tools as a pre-deployment stage. With this toolset schema, users are able to analyze theoretical and practical data in order to perform changes and reconfigurations of the network in-field, i.e., during the real deployment and network evaluation. As a result of this analysis, the evaluation tool is capable of generating correlation reports to be uploaded to a remote server in order to refine simulation models in case of needed.

Therefore, the proposed evaluation tool covers two major issues: routing protocol analysis of the implemented CB-AODV as well as network connectivity and performance evaluation of in-field WSN deployments under real conditions, compared to simulation models. The idea is not only to verify the effectiveness of the routing protocol, but also to study those factors that can affect the performance of the network connectivity and node's coverage, which can thus help

users to integrate or customize different metrics depending on the type of network to be finally deployed.

3.1. System implementation – considerations and features

As shown in Fig. 7, one of the main aspects to be highlighted is the integration of a commercial mobile device with the Cookie platform, in order to take advantage of the Android-OS capabilities and the modularity of the Cookie nodes. This integration is made by means of using a serial-interface-based connection, through the available USB of the mobile device. With both platforms, a mobile device that supports WSN communication protocols is then obtained, especially targeting IEEE 802.15.4 based networks. This configuration schema aims to guide users during the deployment and validation stages of the network, by providing a mobile device that indicates and triggers the actions to be performed in-situ.

The basic element that establishes the interactions between the analysis tool and the in-field WSN is a network/deployment model definition, which is a modular input representation of the functional blocks that are implemented in every node, as well as the simulation schema of the network connectivity. Along with the definition of an over-the-air debugging interface between the analysis models and the HW-SW performance of the nodes, the on-site evaluation capabilities are built. These two main aspects are described in detail as follows.

3.1.1. Network/deployment model

This model definition integrates the main functional blocks that are included in every single node to be installed, so it establishes the deployment rules to be followed based on a well-defined structural schema as expressed in Fig. 8. The implementation models are split in four main definition criteria: sensor/actuators, configuration blocks, property blocks and behavioral blocks. From the point of the network definition, the theoretical correlation between low-level connected points is described by including the MAC-level bidirectional simulation of pair of nodes considering quality indicator parameters, transmission power configurations and data representation of the physical location and installation of the nodes, which are the key elements

Fig. 8. Structure of the deployment model as an input of the system.

Fig. 9. Structure of the defined packet framework to interface I-DPEs with node's components.

that can be obtained as an output of a WSN planning stage (Network/connectivity model).

This model definition is materialized by including a JSON object as an input of the diagnosis tool, comprising the aforementioned deployment elements. It is important to highlight that this JSON object can be included either off-line during the pre-deployment stage or on-site by using web-service-based connection to a remote server that provides the downloading methods for the defined JSON files. Hence, whenever a modification in the planning stage is performed to optimize a specific functionality of the system, the diagnosis tool can update the deployment model in runtime, so that the new features can be tested, analyzed and verified in-situ.

3.1.2. Over-the-air interface

On the other hand, in order to carry out the node evaluation tasks in runtime, a set of software support libraries for network diagnosis is proposed, which is included in the HW-SW platform of the Cookie nodes. These components have been created in order to gather relevant data of the deployed nodes by accessing different parameters and configurations of the node implementation in an independent

fashion, which means that the evaluation tool can extract/modify information of specific node functionalities while the WSN application is running, thus without interfering in the node operation. In order to do that, the proposed components are implemented on top of the PHY-MAC layers of the IEEE 802.15.4, so that the evaluation system does not affect the behavior of the routing protocol since the communication from the tool to the nodes is done from a lower abstraction level. This configuration implies that the main requirement to be addressed in order to perform a node evaluation is the capability of being within the radio coverage of the target or, in case of carrying out a diagnosis task that includes more than one node, it is necessary to have coverage with at least one node of the target group. Hence, the main idea is to be as less intrusive as possible during the performance evaluation. Based on this, a set of Java-based abstraction layers has been defined to decode/encode the debugging frames coming from and going to the connected node that serves as the integration element between the diagnosis toolset and the node's debugging blocks.

The representation of the designed diagnosis packet framework is reflected in Fig. 9. Three levels of transactions are defined in this

Fig. 10. In-field relative position of the commissioning device when testing specific deployment areas.

schema. First of all, low-level connectivity actions targeting the in-field bidirectional evaluation of nodes' correlation, as well as quality models of the interconnections; second, actions that target routing protocol implementation, specially regarding entry table description and metrics' implementation, and rediscovery evaluation; third, actions according to the model definition criteria, that is, specific implementation blocks depending on the application scenario. The diagnosis mechanism of a particular node can be exemplified in Fig. 10.

3.1.3. In-situ performance capabilities

In this sense, the main parameters that are considered for the in-situ performance evaluation of the routing protocols and network connectivity can be seen from different abstraction levels and described as follows:

Quality of the interconnections and coverage of nodes. A complete network connectivity schema is generated based on an iterative process in which every node gathers bidirectional information related to their corresponding neighbors/pairs-of-points in terms of quality of the link and radio signal strength. A routing map is also generated based on the path discovery between remote pairs of points. This information can be compared and correlated with simulation models in order to detect possible mismatches between actual and modeled links/paths. Moreover, the routing map can be compared with the connectivity/MAC level in order to evaluate the performance of the routing protocol in terms of efficiency on the metric usage, asymmetry on the remote-pair-points, node isolation, congestion, and loops avoidance. This runtime automatic correlation process can lead deployers to decide whether specific routing and network configuration criteria shall be adopted based on the dynamics of the system behavior.

Metrics. As previously explained in the routing protocol implementation, several metrics have been included for the discovery process. The performance of these metrics in specific application scenarios can be gathered, modified and evaluated based on the comparison of the runtime routing/network map generation and their theoretical calculation.

Sent/received packet ratio, packet loss rate (PLR). A packet delivery test is proposed to evaluate the performance of the routing capabilities as well as parameters regarding path discovery/rediscovery and

route latency. The evaluation tool can launch this test by configuring the remote pairs of points to be assessed (having coverage with at least one of them), the number of packets to be transmitted and the data/parameter setups according to the specific test to be carried out. The diagnosis components of the related nodes calculate the PLR and the result is then presented and stored in the corresponding database of the diagnosis tool I-DPEs.

Route Rediscovery Rate (RDR) – link failure. Every node computes the number of rediscoveries by storing the information of the next hop with which a failure comes out (note that each node only stores coverage information of their neighbor list). This process can help users to detect possible link problems and critical points in specific deployment zones, as well as analyze the impact of the selected metric configuration to avoid the creation of overhead areas.

Power consumption. The power consumption is measured in order to monitor the behavior of the nodes in terms of energy usage, so that battery levels and the consumed current can be analyzed to establish their impact and relationship with the communication performance of the nodes, as well as analyze and estimate the overall lifetime of the deployed nodes to take corrective actions accordingly. Moreover, this functionality is correlated to the analysis of the energy-based metric efficiency so that a better understanding on the behavior of the routing path selection can be carried out.

PHY-MAC layer assessment. This approach gives an important feature to the evaluation tool usage, which is to act as an in-situ "sniffer" device or packet analyzer, by gathering protocol frames regarding exchanged information among the nodes. Therefore, a MAC frame decoder is also included in the proposed functionalities, in order to obtain the interaction of the nodes in a non-intrusive way, containing a format configuration as well as a network/application packet classification. By using the sniffer/packet analyzer capabilities, low-level frames can be monitored in order to evaluate the generation/reception of the packets from a lower abstraction level, so that problems regarding medium access and frame configuration can be detected.

Sensor measurements, RF configuration, node configuration. Key parameters regarding communication and internal peripheral configurations can also be obtained and reconfigured by using the evaluation tool, in order to study the correlation of particular setups with

Fig. 11. Output models automatically generated based on the on-site activities.

the behavior of the deployed devices, according to the network/node definition of the input model.

3.1.4. Output models

As a result of the on-site commissioning activities, the toolset automatically generates output reports which contain information of the network performance as well as the result of the comparative analysis of the simulation models with the real behavior of the wireless nodes (see Fig. 11), so that the planning strategies can be fed back. Hence, these data help developers to refine the pre-deployment stages regarding nodes' connectivity correlation and system configuration, targeting a more accurate development toolset. Based on this, the reports are automatically generated in line with the system functional flow, and they are the followings (the output models follow the modular structure of the input model):

- Location and coordinates: specify whether there were changes on the node's installation and their positions according to the planning stage, and how these modifications can highlight the deployment.
- Node's implementation: includes information regarding the implementation details of the nodes, specially regarding sensor/actuator performance, as well as the behavior of processing blocks.
- Neighbor maps: generate the correlation between the theoretical calculations of the connectivity links at MAC level with the real in-field communication of the nodes. Comparisons in terms of quality metrics are highlighted.
- Routing maps: provide the whole picture of the remote interconnections based on the routing protocol mechanism, including the routing table entries as well as the different paths that have been created in order to satisfy the requirements of the applications. Routing metrics and their analysis are highlighted.
- Critical points: reflect the specific areas of the network that could affect the performance of the deployment, by specifying isolated nodes and bottle necks.
- Path assessment: provides an analysis of the routes by performing remote packet tests so that the network interconnections can be studied.

- General assessment: includes a general view of the main activities performed on-site, in addition to an overall evaluation of the commissioning stage.

It is also important to highlight that, although the feedback process can be performed in runtime, all the deployment activities and the actions carried out automatically by the diagnosis tool or configurations/analysis done by the deployer, are registered and stored internally in the smart device, so that an offline study process can also be carried out to obtain additional details about the performance of the target deployment.

3.2. System functional flow

From the deployer interaction point of view, the basic application flow of I-DPEs is as follows. First, the configuration file generated from the pre-deployment stage can be downloaded, which contains information regarding network simulations, node connectivity, deployment localization, nodes' implementation and initial configuration. As previously described, the main target of this stage is to compare the simulation models of the planning side with the real deployment of the network, in order to modify/validate the location of specific nodes depending on the coverage and link parameters. The relative position of the device in terms of radio coverage is generated based on an in-field node scanning, so that the area of interest is evaluated in order to detect the surrounding nodes upon which it can act on. The node's connectivity correlation is then built based on generating a neighbor detection list per node, which contains the bidirectional information of pairs of points regarding link quality and signal strength. This information is compared and correlated with the simulation model in order to detect possible mismatches between actual and modeled links. In this context, two reports can be generated, the first one containing information of the modification of node position to improve the connectivity to their neighbors, and the second one highlighting the differences found in the correlation process with the current node positions.

Specific pair-points can then be evaluated from the point of view of the routing protocol, by performing a packet delivery test between remote nodes, so that the ratio of loss packets and rediscovery paths

Fig. 12. General view of I-DPEs user interfaces for in-field comparative analysis of the WSN deployment.

can be obtained. A network routing map is subsequently generated and updated according to the iterative process of the packet delivery tests. The parameters related to the routing tables are saved in the network routing map, aiming to detect bottle necks, critical points, disjointed sectors and possible errors during the route discovery process, so that the routing performance can be analyzed, verified in runtime, also considering the designed metrics for the system assessment. Afterward, the network routing map (routing level) can be compared with the network connectivity map (MAC level) in order to evaluate the performance of the routing protocol in terms of efficiency on the metric usage, asymmetry on the remote-pair-points, node isolation/congestion, and loops avoidance (Fig. 12). The generated network map is then encoded in the corresponding report format in order to be sent to the server repository, so that planning tools can analyze/modify the simulation models with respect to the real data.

4. Experimental results and analysis

The proposed CB-AODV routing protocol has been tested and analyzed in real WSN deployments at the Center of Industrial Electronics by means of using the capabilities of the I-DPEs, in order to validate the designed functionalities and components under the Cookie HW-SW architecture. The implementation of the CB-AODV routing protocol has been carried out based on the Cookie support platform [16] by integrating the software components as shown in Fig. 13. In terms of memory usage, the CB-AODV was included in the Cookie processing layer that incorporates an ADuC841 microcontroller from Analog Devices [28], which provides up to 64 KB of flash/program memory as well as 4 KB of data storage. The final implementation fits in 8 KB of program memory and less than 2 KB of data memory (including the support software components for the diagnosis capabilities), which gives enough free memory space for Cookie-based application proposals.

Form the point of view of the Performance Evaluation Tool I-DPEs, the implementation has been carried out by using an Asus Transformer Tablet that includes the Android Ice Cream operating system connected to a Cookie node through the USB socket, so that all the diagnosis capabilities and GUIs were designed using the Java-based coding features of such OS. This configuration schema also provides

Fig. 13. General overview of CB-AODV integrated in the Cookie support platform.

the possibility of easily porting the implementation to other Android-based devices.

Three main different scenarios were used to analyze and evaluate not only the performance of CB-AODV, but also the designed capabilities of I-DPEs, in addition to the study of metric correlations by performing in-field experimental analysis, as described in the following subsections.

4.1. Scenario A: routing protocol verification

This WSN scenario was carried out to analyze and verify the internal implementation of the CB-AODV and its related functional libraries that generate the different stages of the routing mechanism. Two of the topologies used in this scenario to test the CB-AODV are shown in Figs. 14 and 15 (left-side). The experiments were set up based on three main configurations executed by I-DPEs. First of all, in order to verify the expected behavior of the routing protocol and its robustness throughout a period of time, nodes were configured to send packets every second to a random address. The packet loss rate and the network/routing map were then computed by the evaluation tool in order to obtain the degree of success during the

Fig. 14. First topology of the experimental test case and the main comparative results.

Fig. 15. Second topology of the experimental test case and the main comparative results.

transmission/reception process as well as the routing discovery procedure in such conditions. The TX power of the radio transceivers was also configured to modify the node coverage, so that the routing capabilities are evaluated by creating paths with the maximum amount of hops as possible (with the minimum transmission power configuration), which helps developers to assess the performance of the integrated metrics. This random propagation was triggered during five consecutive hours without experimenting problems with particular nodes' implementation.

In this way, as a second test case, one of the nodes was configured by the I-DPEs to send 100 packets with a frequency of one message per second (these parameters can be reconfigured by the tool) to its farthest node, i.e., a data exchange from the two most distant points of the network (nodes 1 and 9 in the figure). The main goal was to analyze the performance of both the PLR and the included metrics, specially the PATH-DR, E-aDM and the ETX, which depend on the link quality parameter. Furthermore, a third test case was also carried out in this scenario, in which a "crowded environment" was set

up by configuring the rest of the nodes to send packets to random addresses, while the two distant nodes continued exchanging data between each other. In this traffic scenario, every node was defined to send packets to a different remote node every second, so that three main capabilities can be tested: first, the discovery process of the source node to the destination point in combination with the support of the discovery actions triggered by the rest of the nodes; the routing table information handling by the nodes according to the packet exchange to the request points (all the nodes are creating new routes, supporting the creation of them by other nodes and establishing the corresponding table correlations/updates based on the request-check-reply actions); the information processing by analyzing how the management of the routing resources in the HW-SW platform can affect the normal operation of the application itself or even loose data during the transaction between two remote points in such situation. Apart from the MAC and routing frames of the protocol, the transmitted packets are composed of application information related to sensor measurements, battery level and energy consumption factors,

data processing indicators and execution status. Metrics and the test configurations were launched by using the evaluation tool, and an iterative execution was done three times per configuration in order to obtain as much information of the network behavior as possible.

In Figs. 14 and 15 (right-side), the main results regarding the proposed scenario are classified according to the applied metric and the differences in traffic conditions, in addition to the computed routing paths, which can be analyzed by means of gathering nodes' information with the tool. The percentage of received packets is very close to 100%, being slightly inferior in the case of traffic conditions. As a result of comparing the metric performances, the ETX has fewer hops than the PATH-DR, as expected (because ETX penalizes the number of hops). However, the percentage of messages that the final node receives is not higher in case of the PATH-DR than with the ETX, as it would be expected. Moreover, in case of the designed E-ADM metric, node 5 was configured to include a higher weight regarding the implemented functional blocks as well as the precursor list factor, so that a redistribution on the network routing rediscovery was obtained in the crowded environment, where packets from node 1 to node 9 follow a slightly different sequence compared to the PATH-DR, as shown in the results, thus verifying the influence of energy conservation based approach and a balanced distribution of the packets.

In addition to the described test cases, scenarios B and C (presented in the subsequent subsections) are also conceived to analyze the behavior of the implemented metrics by using I-DPEs based on providing different network topologies and application constraints, so that the influence of the communication performance can be evaluated through the experimental comparison of the metric results.

4.2. Metric's correlations and experimental characterizations

As described in Section 2, experimental tests were carried out to establish correlations of the quality metrics to be used in CB-AODV and I-DPEs, in addition to the ones already included in the routing implementation. Two Cookie nodes were configured and positioned in an outdoor environment at the same height (1 m from the ground) and distance samples starting from 1 m up to 35 m. Moreover, the range of the TX power configuration of the radio modules is swept from 0 dBm to -25 dBm.

The first model aims to establish an experimental correlation between the RSSI and LQI parameter in order to include it in the simulation chain of I-DPEs so that complete connectivity estimations in terms of RSSI, LQI and LDR can be subsequently generated, analyzed in-field and compared with the real behavior of the deployment. Based on this, in Fig. 16 the main results of the experimental tests are presented including the combination of values in terms of distance

Fig. 16. Experimental correlation of RSSI and LQI obtained and to be included in the in-field comparative studies.

Fig. 17. Experimental correlation of the RSSI and LDR parameters.

plus transmission power configuration, so that a defined correlation pattern between both parameters can be distinguished.

Considering this experimental correlation, a simpler approximation model can be obtained to be included in the in-field simulation of the connectivity map to analyze the real values of the network with what is theoretically expected from the application scenario. Such correlation is expressed in Eq. (3):

$$\gamma = \rho_1 \alpha^3 + \rho_2 \alpha^2 + \rho_3 \alpha + C \quad (3)$$

where ρ_1, ρ_2, ρ_3 are the coefficients of the expressions and respectively defined as 1.1856, -2.7009 and 0.6305, C is the independent factor defined as 106.9160, α is the measured RSSI value (with a typical offset of -40 dBm), and finally γ is the resulting LQI.

Based on this experimental setup and testing process, another important correlation has been established between the RSSI and the LDR parameter to define a threshold value under which the connection between two pairs of nodes can be considered as unstable or critical, so that from the point of view of I-DPEs' estimations those links that are below this value might be marked as unconnected, while from the nodes' implementation point of view the detection of such low values represent a critical connection to be avoided when calculating routing paths. As shown in Fig. 17, the computed threshold value is -85 dBm.

4.3. Scenario B

In this experimental test case the main target is to compare the simulation results of pair-point connectivity metrics with the real values gathered from the in-field deployment by using I-DPEs. The WSN is composed of 16 Cookie nodes deployed at ETSII-UPM in an outdoor environment, by combining in the same deployment a heterogeneous distribution of the nodes in terms of connectivity schema. Based on a simulation model, the input connectivity map of the deployment has been built as shown in Fig. 18 (bottom-left side). According to the experimental results regarding the reliability of the links by defining a minimum RSSI to assure a stable connection between two points (-85 dBm), I-DPEs establishes the correlation points where a connection shall be obtained (in white color). The purple connections directly affected by obstacles are highlighted, so that no links shall be expected in those pairs of points. In red are the values above the defined RSSI threshold, which defines the limit below which the connectivity is not assured.

Based on this, the real connectivity map is built in-field to be compared with the simulated one. Both in simulation and real deployment, the nodes have been configured with a homogeneous transmission power of -5 dBm. In Fig. 18 (upper-right side), the main average experimental results are reflected by computing 4 consecutive tests per link (bidirectional connections) and the comparison with the theoretical calculation are generated and analyzed. Highlighted in white are the real and simulated values between pairs of nodes,

Fig. 18. Comparative analysis of the in-field connectivity with the simulation model, (For interpretation of the references to color in the text, the reader is referred to the web version of this article.)

Fig. 19. In-field connectivity performance of the deployed nodes. (For interpretation of the references to color in the text, the reader is referred to the web version of this article.)

whereas in blue are the connections that were not expected from the simulation but in the real implementation such pairs of nodes did connect. In orange those connections that were not established are represented.

In such cases (connection mismatches), the real values are very close to the defined quality limit, so the estimation is pretty much accurate to predict those links that are prone to suffer instability and, therefore, to be marked as unconnected points. The rest of the simulated pair-points that produce stable connections were indeed validated in the real implementation when establishing the comparison with I-DPEs.

As a result of the diagnosis tool, the average error of the comparative analysis in terms of the simulated and real metrics is 4%, having maximum deviations (12%) in those communications where unexpected/not-considered obstacles have influenced the performance of the connections.

These types of on-site study can be also carried out by graphically comparing the connectivity performance of every pair of points as represented in Fig. 19 for this particular outdoor scenario, in which the orange lines indicate the simulation results while the green ones correspond to the real gathered data. The thickness of the lines matches with the quality and stability of the interconnections

Table 2

Experimental results of the routing strategies by using ETX and E-aDM in the comparative analysis.

ID 8 → ID 13	Test Sample	Number of sent messages	Received messages	Last route
ETX Metric	1	100	100	8→6→5→3→11→13
	2	100	98	8→6→5→4→3→11→13
	3	100	100	8→6→5→3→11→13
E-aDM Metric	1	100	100	8→6→5→3→2→11→12→13
	2	100	100	8→6→5→4→3→2→11→12→13
	3	100	99	8→6→5→3→2→11→12→13

between pairs of nodes. This provides users with the possibility of directly analyzing in runtime how reconfigurations in terms of communication capabilities (consumption modes and transmission power) and location' changes might influence the surrounding neighborhood or even the whole deployment.

Regarding the performance of the routing capabilities based on this real connectivity map, packet delivery tests were triggered to mainly compare the behavior of CB-AODV by including ETX and E-aDM in the study, both targeting quality of the interconnections but the former one penalizing the number of hops and the last one balancing the distribution of the paths. Under these outdoor conditions, tests were launched from different deployment areas, and considering nodes 8 and 13 as pairs of points to show the result analysis, in Table 2 the comparison of the routing metrics for a total of 100 packets per test is represented. It can be seen the effect of hop penalization in ETX, whereas with E-aDM the routing load balance has been distributed among nodes 2, 9 and 11 to guarantee that the creation of

critical points is avoided as much as the deployment topology allows such optimization.

The use of the ETX metric may be suitable for those applications in which transmission and processing delays (based on the hop reduction) are a key factor for the performance of the required service, whereas E-aDM provides a more balanced link correlation among remote points in terms of energy conservation in addition to resource/processing constraint awareness in specific nodes of the deployment. E-aDM allows a more precise tuning of the path selection targeting energy and processing equilibrium among the deployed nodes, although for more directional topologies in which the routing capabilities are more concentrated in specific rely points of the network, ETX can provide good results without specific parametrization. One of the advantages of the proposed evaluation tool is that by using I-DPEs deployers can analyze in real time what metrics can be more adapted and suitable depending of the specific requirements and behavior of the in-field target application.

Fig. 20. Network topology of the deployment scenario and connectivity map.

Fig. 21. Evaluation of the routing rediscovery when detecting errors in route entries.

4.4. Scenario C

In this experimental scenario the main target is to carry out the deployment diagnosis regarding the connectivity evaluation and routing performance along with the validation of the node's implementation in terms the sensor/application functional blocks. The planning configuration is based on an outdoor scenario comprising 9 nodes with a mesh topology, as shown in Fig. 20, and with the inclusion of environmental sensors in the input model: temperature, humidity and light intensity. Based on the comparative analysis of the simulation model with the in-situ connectivity map generation provided by I-DPEs, the computed average error is 4.1% with a maximum deviation of 10.9%, for a transmission power configuration of -10 dBm.

Regarding the performance of CB-AODV, computations of packets delivery tests were performed between nodes 1 and 9 with such intermediate TX power and applying E-aDM by penalizing the node 5 in terms of blocks processing ($w_3 = 4$), and the results generated the creation of a route passing through nodes $1 \rightarrow 6 \rightarrow 9$ with a metric = 99%. Moreover, subsequent delivery tests have been performed to analyze the impact of insulating part of the nodes along the paths in order to verify the dynamic reconfigurability of CB-AODV in such conditions, as the one shown in Fig. 21, where the rediscovery mechanism produces a new route (from node 1 to node 3) of $1 \rightarrow 4 \rightarrow 5 \rightarrow 3$ and with an average delivery ratio of 98% for the total amount of tests (more than 900 in-field test verifications automatically handled by the diagnosis tool).

5. Conclusions and contributions

In this work, two major approaches for the applicability and efficiency of WSN deployments under real applications have been proposed and implemented focused on studying, analyzing and evaluating the performance of routing protocols and network connectivity in realistic environments. A modified AODV-based routing protocol (CB-AODV) for a reactive and flexible Ad-hoc network configuration has been fully implemented and tested into a modular HW-SW platform, which copes with the limitation of resource constraints and memory budget during the design and implementation stages, including an energy-based optimization mechanism for efficiently distributing

the routing discovery process. A complete In-situ Diagnosis and Performance Evaluation System (I-DPEs) was also proposed as a major contribution not only for the CB-AODV assessment, but also to provide users with an on-site network analysis tool for optimizing and validating protocol implementations and node functionalities under real application conditions.

More than a simulation tool, this work presents a clear alternative for developers to address and study the effectiveness of network deployments by comparing generated models with the real behavior of Ad Hoc and multi-hop WSNs, hence obtaining key parameters of the network configuration in runtime and in-field. The real implementation of both novel approaches has been put into context under real deployment scenarios to analyze the main elements and properties that may affect the behavior and the efficiency of the whole systems, by also detecting specific areas where in-field optimizations could be performed at runtime, so that a more appropriate feedback to the planning tasks can be provided to refine the design and development of the target WSN-based applications.

Acknowledgments

The authors would like to acknowledge the support of ARTEMIS JU and the Spanish Ministry of Industry and Commerce for the WSN-DPCM project under grant ART-010000-2011-1.

References

- [1] D. Goyal, M. Tripathy, Routing protocols in wireless sensor networks: a survey, in: Proceedings of Second International Conference on Advanced Computing Communication Technologies (ACCT), January 2012, pp. 474–480.
- [2] K.L. Pang, Y. Qin, The comparison study of flat routing and hierarchical routing in ad hoc wireless networks, in: Proceedings of 14th IEEE International Conference on Networks (ICON), 1, September 2006, pp. 1–6.
- [3] N.A. Pantazis, S.A. Nikolidakis, D.D. Vergados, Energy-efficient routing protocols in wireless sensor networks: a survey, IEEE Commun. Surv. Tutorials 15 (2) (2013) 551–591.
- [4] M. Chen, V. Leung, S. Mao, Y. Xiao, I. Chlamtac, Hybrid geographical routing for flexible energy-delay trade-offs, IEEE Trans. Veh. Technol. 58 (9) (2009) 4976–4988.
- [5] S. Mohseni, R. Hassan, A. Patel, R. Razali, Comparative review study of reactive and proactive routing protocols in MANETs, in: Proceedings of 4th IEEE International Conference on Digital Ecosystems and Technologies (DEST), April 2010, pp. 304–309.
- [6] J. Portilla, A. de Castro, E. de la Torre, T. Riesgo, A modular architecture for nodes in wireless sensor networks, JUCS 12 (3) (March 2006) 328–339.

- [7] L. Riliskis, E. Osipov, Symphony: simulation, emulation, and virtualization framework for accurate WSN experimentation, in: 4th International Workshop on Software Engineering for Sensor Network Applications (SESENA'13), May 2013, pp. 1–6.
- [8] A. Sobeih, J.C. Hou, L.-C. Kung, N. Li, H. Zhang, W.-P. Chen, H.-Y. Tyan, H. Lim, J-Sim: a simulation and emulation environment for wireless sensor networks, *IEEE Wireless Commun.* 13 (4) (August 2006) 104–119.
- [9] M.S. Iqbal, H.S. Al-Raweshidy, Performance evaluation of IEEE 802.15.4 standard for low data rate ad hoc wireless sensor networks, in: Proceedings of International Conference on Control, Automation and Information Sciences (ICCAIS 2013), 25–28 November 2013, pp. 300–304.
- [10] A. Karatzoglou, M. Scholz, T. Riedel, M. Beigl, A prototype of an in-situ radio sensing and visualization device, in: Proceedings of the Ninth International Conference on Networked Sensing Systems (INSS), 2012.
- [11] L. Selavo, G. Zhou, J.A. Stankovic, SeeMote: in situ visualization and logging device for wireless sensor networks, in: Proceedings of the 3rd Conference on Broadband Communications, Networks and Systems BROADNETS, 2006, pp. 1–9.
- [12] S. Wei, M. Hashemi, I. Warsawski, M. Laifenfeld, D. Starobinski, A. Trachtenberg, TeaCP: a toolkit for evaluation and analysis of collection protocols in wireless sensor networks, in: Proceedings of IEEE International Conference on Microwaves, Communications, Antennas and Electronics Systems (COMCAS 2013), October 2013, pp. 1–5.
- [13] Xie Dongliang, Wang Guoying, SPAE: a dynamic wireless sensor network performance analysis and evaluation platform, in: Proceedings of 4th IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT), October 2011, pp. 545–548.
- [14] IEEE Standard Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANS) (1 October 2003).
- [15] CC2420 2.4 GHz IEEE 802.15.4/ZigBee ready RF Transceiver Datasheet, Chipcon products from Texas Instruments.
- [16] G. Mujica, V. Rosello, J. Portilla, T. Riesgo, Hardware-software integration platform for a WSN testbed based on cookies nodes, in: Proceedings of the 38th Conference on IEEE Industrial Electronics Society, IECON, 2012, pp. 6013–6018.
- [17] Y. Xu, J. Heidemann, D. Estrin, Geography-informed energy conservation for ad-hoc routing, in: Proceedings of ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), Rome, Italy, July 2001, pp. 70–84.
- [18] M. Aslam, N. Javaid, A. Rahim, U. Nazir, A. Bibi, Z.A. Khan, Survey of extended LEACH-based clustering routing protocols for wireless sensor networks, in: Proceedings of IEEE 9th International Conference on High Performance Computing and Communication and IEEE 14th International Conference on Embedded Software and Systems (HPCC-ICESS), June 2012, pp. 1232–1238.
- [19] P. Jacquet, T. Clausen, Optimized Link State Routing Protocol (OLSR) (2003) RFC 3626.
- [20] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, RPL: IPv6 Routing Protocol for Low Power and Lossy Networks (March 2012) IETF RFC 6550.
- [21] Z.J. Haas, M.R. Pearlman, P. Samar, The Zone Routing Protocol (ZRP) for Ad Hoc Networks, draft-ietf, July 2002.
- [22] O. Gnawali, R. Fonseca, K. Jamieson, M. Kazandjieva, D. Moss, P. Levis, CTP: an efficient, robust, and reliable collection tree protocol for wireless sensor networks, *ACM Trans. Sens. Netw.* 10 (1) (2013) Article 16, 49 pages.
- [23] D. Johnson, Y. Hu, D. Maltz, The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4 (2009) IETF RFC 4728.
- [24] C. Perkins, E. Belding-Royer, S. Das, Ad hoc On-Demand Distance Vector (AODV) Routing, (2003) RFC 3561.
- [25] C. Gomez, A. Boix, J. Paradells, Impact of LQI-based routing metrics on the performance of a one-to-one routing protocol for IEEE 802.15.4 multihop networks, *EURASIP J. Wireless Commun. Netw.* 2010 (2010) 1–20.
- [26] C. Gomez, P. Salvatella, O. Alonso, J. Paradells, Adapting AODV for IEEE 802.15.4 Mesh Sensor Networks: theoretical discussion and performance evaluation in a real environment, in: Proceedings of the International Symposium on a World of Wireless, Mobile and Multimedia Networks 2006 (WoWMoM'06), Niagara-Falls, Buffalo, NY, June 2006.
- [27] R.J. van Glabbeek, P. Höfner, W.L. Tan, M. Portmann, Sequence numbers do not guarantee loop freedom: AODV can yield routing loops, in: Proceedings of the 16th ACM international conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM'13), NY, USA, November 2013, pp. 91–100.
- [28] Analog Devices, <http://www.analog.com/en/index.html>.

Gabriel Mujica received the degree in Electronic Engineering from the Federico R. Palacio University of Technology and Franche-Comté University, and the M.Sc. on Industrial Electronics from the Universidad Politécnica de Madrid. Currently, he is a Ph.D. candidate and researcher in the Center of Industrial Electronics at UPM, mainly working in the area of wireless sensor networks as well as digital system design and implementation. His main research interests are focused on WSN debugging and optimization, integration of heterogeneous technologies in sensor networks, IoT based HW-SW co-design and efficiency in WSN communication capabilities.

Jorge Portilla received the M.Sc. degree on Physics from the Universidad Complutense de Madrid (UCM) in 2003 and the Ph.D. degree in Electronic Engineering from the Universidad Politécnica de Madrid (UPM), Spain, in 2010, where he is presently an Assistant Professor since 2006, and doing his research at the Industrial Electronics Centre (CEI). His research interests are focused mainly on wireless sensor networks, reconfigurable systems and embedded systems design.

Teresa Riesgo received her M.Sc. and Ph.D. degrees in Electrical Engineering from UPM, in 1990 and 1996, respectively. Since 2003 she is Full Professor of Electronics at UPM. She has been the Director of the Center of Industrial Electronics (CEI-UPM) from 2007 to 2011. She has acted as General and Program Chair of different conferences in the field of Electronic system design and she has published many papers in journals and conferences in the field. Her research interests are focused in embedded system design, reconfigurable systems and wireless sensor networks.