Experimental Evaluation of a Routing Protocol for WSNs: RPL robustness under study

Karel Heurtefeux
Qatar Mobility Innovations Center
Doha, Qatar
Email: karelh@qmic.com

Hamid Menouar
Qatar Mobility Innovations Center
Doha, Qatar
Email: hamidm@qmic.com

Najah AbuAli
College of Information Technology
UAE University,
Al Ain, United Arab Emirates
Email: najah@uae.ac.ae

***Abstract*—This paper presents experimental results on the Routing Protocol for Low-Power and Lossy Networks (RPL). The RPL properties in terms of delivery ratio, control packet overhead, dynamics and robustness are studied. The results are obtained by several experimentations conducted on 2 large wireless sensor network testbeds composed of more than 100 sensor nodes each. In this real-life scenario (high density and convergecast traffic), several intrinsic characteristics of RPL are underlined: path length stability but reduced delivery ratio and important overhead. To investigate the RPL robustness, we observe its behavior when facing a sudden death of several sensors and when several sensors are redeployed. RPL shows good abilities to maintain the routing process despite such events. However, the paper highlights that this ability can be reduced if only few critical nodes fail. To the best of our knowledge, it is the first study of RPL on such large platform.**

I. Introduction

Wireless Sensor Networks (WSNs) are formed by hundreds or thousands of low energy wirelessly interconnected sensor devices. Due to constraints such as energy and computation capability, nondeterministic sensor failures, links instability, and distrusted environments, designing robust routing protocols is quite challenging. Recently, WSNs have been brought into reality with the effective deployment of sensor nodes. In this context, the Routing Over Low power and Lossy networks (ROLL) working Group was formed in Internet Engineering Task Force (IETF) to develop an adapted routing solution. After 4 years, RPL was adopted by IETF in March 2012 [1].

Motivation. RPL is one of the first routing standards available for WSNs. RPL is a recent protocol and only few studies have been conducted on it [2]–[4]. Therefore, the understanding of its behavior in realistic scenarios and environments is important and worth to investigate.

Contributions. The contributions of this paper include:

- Firstly, a study evaluating the RPL performance on a large and dense WSN platform has been conducted, and the influence of transmission power is investigated.
- Secondly, this paper presents 2 scenarios allowing to evaluate the RPL robustness (i.e. its capacity to deal with node and link failures).

Novelty. As per our best knowledge, this is the first study evaluating both performance and robustness of RPL in real scenarios based on real and large platforms.

The rest of this paper is organized as follows. Section II provides an overview of previous work insisting on information which is relevant in the context of this paper: previous studies on RPL and the robustness concept is discussed. In Section III, we briefly describe RPL. In Section IV the WSN experimentation platforms, parameters and scenarios are detailed. In Section V, the experimental results on the RPL behavior and performance are presented. Section VI introduces the experimental results on RPL robustness. Finally, Section VII concludes this contribution and discusses potential further work directions.

II. Related Work and Scope

In this section, a comprehensive overview of proposed RPL performance studies is presented. A discussion on the robustness concept is also proposed and compared with other similar notions such as survivability and resilience.

A. Performance Studies on RPL

Before the standardization of RPL protocol, the authors in [5] experimentally exposed that the gradient-based routing, proposed by IETF ROLL, was robust against topological changes. The routing process of RPL is based on such gradient. They implemented a gradient-based protocol, similar to RPL, on TI eZ430-RF2500 platform (MSP430 microcontroller with 2.4GHz CC2500 radio). To investigate their protocol robustness, they deployed 12 nodes during 8 hours, sufficiently far from each other to obtain weak links. The node degree variation and delivery ratio are measured. Despite the constantly changing topology, 74% of sent packets are reached the sink. However, the robustness was not studied in case of nodes outage or adding new nodes. Moreover, the small number of deployed nodes reduces drastically some common issues: collision, interference or bottleneck [6].

In [4] and [2], the authors present a performance evaluation of RPL based on simulations. In [4], the simulations are performed with topology and link quality data from a real sensor network. The authors investigated path quality, routing table size, control packet overhead and connectivity. They observed that the number of control packets decreases during the simulations and the stabilization of the DODAG (Destination Oriented Directed Acyclic Graph). In [2], the authors show that RPL allows a fast network set-up: however, contrary to [4], they also find that RPL has an important control packet overhead during the simulation. In this study, the considered

hypotheses on the simulation environments are strong: Unit Disk Graph (UDG) and uniform packet error rate. They do not reflect what is generally observed in real environments. For instance, the packet error rate is often more important next to the sink due to a bigger congestion.

More recently, [3] presents the most relevant research effort proposed for RPL, and an experimental performance evaluation of RPL. The experimentations are based on 30 TelosB motes, and give a performance evaluation in terms of packet loss, packet delay, DODAG time convergence and power consumption. However, the authors did not investigate the impact of power transmission on packet delivery ratio, the overhead nor the robustness against node failures.

B. Concept of Robustness

In the literature, several close concepts such as self-stabilization [7], [8], resiliency [9] and survivability [10] have been discussed.

In a distributed system (such as WSNs), the self-stabilization [7], [8] enables an algorithm to withstand transient faults and the system recovers in finite time without external intervention. In other words, an algorithm is self-stabilizing if and only if:

- Starting from any state, it is guaranteed that the system will eventually reach a correct state. This properties is called convergence.
- If the system is in a correct state, it is guaranteed to stay in a correct state, provided that no fault happens (closure).

This fault-tolerance concept is very useful but define the property of self-stabilization for an algorithm is known to be a difficult task. For complex protocols, such as RPL, working on MAC and physical layers, inside an operating system and deployed on a real sensor network, the legitimacy of the network state cannot be evaluated easily. To help overcome this difficulty, several simplifications of the hypotheses are needed: for instance, ideal physical layer, or simplified routing protocols [11], [12]. However, this requires to deploy the algorithms on a simulator and avoids to consider the consequences of a real environment on the protocol behavior.

The authors in [9] define the resiliency in a route failures context. They measures the likelihood that, when the route has failed, an alternate path is available. This definition focuses on a very specific problematic (the multipath routing) and does not deal with common issues encountered in routing.

In [10], the authors define the survivability as the ability of the information system to provide essential services in the presence of attacks or failures, and recover full service in finite time. Survivability is conceptually close to the robustness. However, from our point of view, this definition is general, considering both security and fault tolerance. The security issues are out of scope of this paper. The robustness is defined as a requirement to accommodate hardware and software failures, asymmetric and unidirectional links, or limited range of wireless communication [13]. This definition is more suitable to the study of wireless network robustness. In this paper, we study the robustness to the node/link failures and topological changes due to removed/added nodes to the network.

As per our best knowledge, this is the first study in its kind evaluating both performance and robustness of RPL in real scenarios based on real and large platforms. We believe that the understanding of RPL's behavior in realistic scenarios and environments is important and worth to investigate.

III. RPL Overview

RPL [14] is a hierarchical, proactive and IPv6 distance vector protocol. It constructs a DODAG and the data packets are routed through it. DODAGs have the property that all edges are destination oriented in such a way that no cycles exist. Thanks to the DODAG, each node has a rank, which defines the node's position relative to other nodes with respect to the DODAG root. The node's rank strictly increases from the root towards the leaf nodes. The rank is computed depending on the DODAG's Objective Function (OF): hop counts, link metrics (expected transmission count (ETX) [15], i.e. the expected number of transmissions required to successfully transmit and acknowledge a packet on the link or the Link Quality Indicator (LQI)) or other constraints. To build and maintain its logical topology (route, parents, neighbors table), RPL uses IPv6 control messages:

- DIO: DODAG Information Object (multicast). A DIO packet carries information that allows a node to discover a RPL instance, learn its configuration parameters, select a DODAG parent set, and maintain DODAG. DIO packets are firstly sent by the root (or sink) and then periodically by each node of DODAG. In absence of changes in the DODAG structure, the period duration increases exponentially.
- DIS: DODAG Information Solicitation (multicast). A DIS packet is used when a node joins the network in order to solicit a DIO from a RPL node.
- DAO: Destination Advertisement Object (unicast). A DAO packet is used to propagate destination information upwards along the DODAG. The message is unicast by a child to the selected parent to advertise their addresses and prefixes. When a node receives a DAO, it updates its routing table.

Finally, RPL has been designed to deal with constraints in energy and channel capacity. As a result, to reduce the control messages overhead, RPL uses a slow proactive process to maintain a routing topology but a reactive process to resolve routing inconsistencies. The reader is invited to refer to [14] for more details on RPL.

IV. Methodology and materials

A. Platforms description

The SensLAB platform [16] is a set of 1000 sensor nodes available as a testbed for distributed embedding sensor network applications and distributed systems research. In this study, we used a subset of 200 nodes on Lille and Rennes platforms. The nodes are deployed in an indoor environment. SensLAB nodes are composed of 2 WSN430 boards (one open node and one control node) connected by one gateway board. The purpose of the control node and the gateway board is to offer the essential SensLAB features: firmware deployment on open node; radio environment and power monitoring; configurable sensor polling on control node (temperature, light); remote

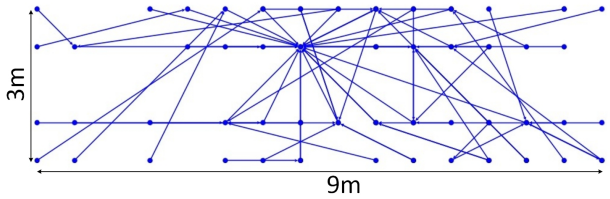

Fig. 1. RPL Logical Routing Topology with a - 25dBm transmission power on the Lille SensLAB platform.

	INRIA Lille	INRIA Rennes
Environment	Indoor	Indoor
Sensor Node position (3D)	Random	Random
Number of sensor nodes	100	100
Radio chip	TI CC2420	TI CC2420
Transmission power	$-25\ dBm$ to $-5\ dBm$	$-10\ dBm$
Frequency	2.4 GHz	2.4 GHz
Experiment duration	2 h	1 h
DATA packet period	45 s	45 s
MAC protocol	sicslomac	sicslomac

TABLE I. SUMMARY OF THE EXPERIMENT PARAMETERS.

software update ability for control nodes and gateway. In other words, each node is connected in an "out-of-band" fashion, to a node handler using testbed infrastructure. We are able to monitor a set of metrics (sent or received packets, RSSI, noise level, temperature, light or energy level), without using wireless communications nor back end data collected by a sink. The open nodes are notably composed of:

- MSP430 core (MSP430F1611, offering 48 kbyte ROM, and 10 kbyte RAM) ;
- TI CC2420: a single-chip 2.4 GHz IEEE 802.15.4 compliant RF transceiver and emitting between -25 and 0 dBm (0.003 and 1 mW) with maximum transmission rate of 250 kbps ;
- Omnidirectional PCB antenna ;
- Varta Polyflex rechargeable battery.

For more details, we invite the reader to consult [16] and [17].

B. Experiment parameters and scenarios

Sensor nodes are equipped with the open source operating system Contiki, which is specially designed for low-power and memory-constrained devices. Contiki includes several lightweight network mechanisms: the uIP TCP/IP stack [18], the Rime stack [19] and the uIPv6 stack [20]. In this study, the uIPv6 stack is used, which provides IPv6 networking and contains RPL routing protocol. As a MAC layer, the sensor nodes use a simple MAC layer called sicslomac for packaging radio packets into 802.15.4 frames.

We define 3 scenarios. In each scenario, sensor nodes periodically send data packets to one specific node, called the sink. Note that in this study, the MAC layer is not investigated. A network is able to run multiple instances of RPL concurrently. However, in these experiments, only one instance is running in the network. Thanks to the "out-of-band" infrastructure, each packet sent or received is monitored.

Scenario 1. The experiments take place on the INRIA Lille platform and last for 2 hours (which corresponds to more than 50000 IPv6 packets exchanged for each experiment). The sink is selected at the center of the platform and it collects all data packets. At the beginning of each experimentation, 100 nodes are switched on together and start working immediately. In Section V, we present the results coming from 4 experimentations following the scenario 1 with a transmission power from -25 dBm to -5 dBm. The goal of the scenario 1 is to investigate the influence of the physical topology on the measured metrics and to highlight the RPL's performances in a dense WSN. Figure 1 shows the Lille experimental testbed for the evaluation of RPL in a multi-hop topology. It is common that some of the sensor nodes could not participate to the routing because they are isolated (without DODAG neighbors), therefore they do not appear in this figure.

The scenarios 2 and 3 are defined to stress the self-healing nature of RPL by removing and adding nodes to the network. They allow the observation of its robustness. According to the scenarios 2 and 3, WSNs are deployed on INRIA Rennes platform using a -10 dBm transmission power. The duration of each experimentation is set to one hour.

Scenario 2. At the beginning of the experimentation, 100 sensors are active. A central node is selected as sink and the other nodes send periodically data packets to the sink. After 20 minutes, 20% of sensor nodes are switched off, which is a good tradeoff to observe the impact of a significant outage without disconnecting all the nodes from the sink. These nodes are selected randomly among all the active nodes (excluding the sink). After 20 minutes, the same "dead" sensor nodes are switched on.

Scenario 3. As in scenario 2, 100 sensors are active at the beginning of the experimentation. After 20 minutes, only 2 nodes are switched off. However, these 2 nodes are judged to be *critical*. We have observed from the experimentations on Lille platform that some specific nodes are selected to be preferred parent by numerous sensors. These nodes are identified as critical nodes, because they are aggregating an important number of other nodes. 20 minutes after the death of 2 critical nodes, we switch them on again.

The scenarios 2 and 3 give us the opportunity to observe how RPL reacts when a large part of sensors or critical sensors are not available. It also underlines how the network adapts to the event when new nodes are added. Note that we wait for 20 minutes between removing or adding sensors to let enough time to RPL to recover and stabilize.

Table I sums up the essential experiment parameters and platform description.

C. Evaluation Metrics

To gain insight concerning the RPL performances and robustness, the following metrics are measured:

- **Data Packet Delivery Ratio** represents the ratio between the total number of packets successfully received by the sink and the number of packets sent by the sources. This is an important metric to evaluate the success of routing functionality, i.e., packet delivery;
- **Control Packet Overhead** is the number of control packets sent by the nodes. As explained in Section III, RPL uses 3 types of control messages: DIO, DAO

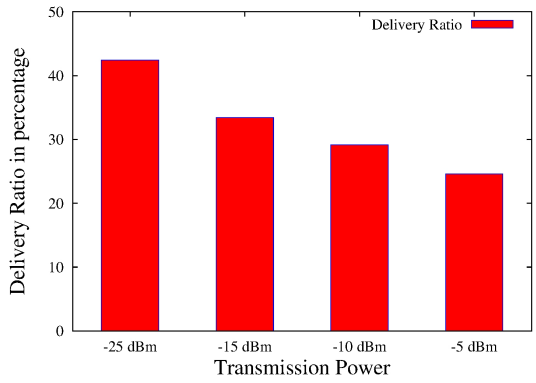

Fig. 2. Scenario 1: Delivery ratio according transmission power.

and DIS. A high control overhead may adversely affect delivery ratio;

- **Number of Update per Minute** is the number of update per minute of the neighbor tables. This metric is an indicatior of the network *dynamicity*;
- **Average Path Length** is the number of hops crossed for each received packet. This allows to determine the number of forwarding nodes of a route.
- **Average Rank Level** is the relative position within the DODAG and is used by the RPL core to enable a degree of loop avoidance and verify forward progression towards a destination. It is computed based on the Objective Function (OF), which is, by default, a combination of Expected Transmission Count (ETX) and hop distance. A variation of this metric indicates a sensitivity to the link instability.

V. RPL Behavior: Experimental Results

The numerical results presented in this section are from 4 experimentations and are not averaged. As a result, standard deviation or confidence intervals can not be computed. However, numerous experimentations have been done and the behavior highlighted in this section is very similar in all experimentations. It also exists strong similarity between RPL behavior and performance observed on Lille and on Rennes platforms. In this section, the experimentations are guided by the scenario 1.

A. Data Packet Delivery Ratio

Numerous studies show poor packet delivery rates from several WSN deployments [6], [21]. The authors in [6] undertake a measurement study on a large-scale and dense sensor network deployed in the wild, GreenOrbs. They underline that some intermediate sensor nodes bottleneck the entire network and the importance of the environment and how it may have an unpredictable impact on the sensor network. Zhao et al. in [21] show that a large part of the link experienced more than 10% packet loss. Packet loss can be caused by many reasons: asymmetric links, fading, multipath, signal attenuation, interferences or collisions.

However, RPL has been developed especially to consider lossy networks. Despite its conception, the results show that

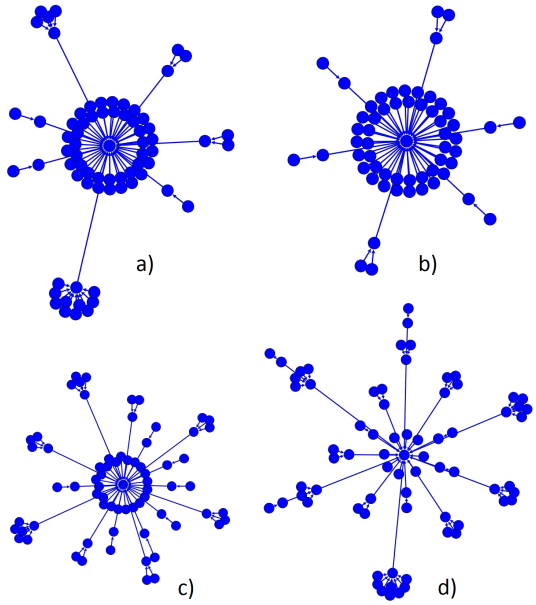

Fig. 3. Scenario 1: RPL Logical Routing Topology with a transmission power of a) - 5dBm; b) -10dBM; c) -15dBm and d) -25dBm. For greater clarity, sensor nodes are positioned according their distance, in hops, to the sink (in center).

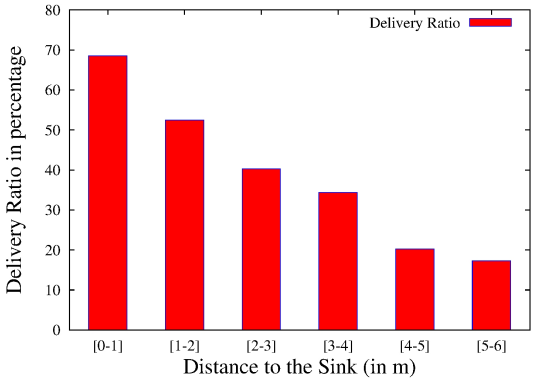

Fig. 4. Scenario 1: Delivery ratio versus distance to the sink.

RPL experiences an important packet loss. For instance, Figure 2 illustrates the delivery ratio obtained with different transmission powers. Contrary to what we expected, the best performance is obtained with the lower transmission power. This is due to the logical routing topology based on DODAG which creates a serious congestion at the sink. The logical routing topology is represented in Figure 3. An important number of 1-hop nodes is observed in the cases a) and b). This configuration leads to a bottleneck, which avoids the data messages to reach the sink. On the other hand, a lower transmission power increases the average path length (in hops), but also limits the interferences and the bottleneck effect near the sink.

Figure 4 represents the delivery ratio according to the distance with a -25dBm transmission power. The sensor nodes are categorized in the network according to their euclidian distance to the sink. Note that a sensor node sometimes switches its parent, resulting in dynamic routing paths to the sink of different hop counts. Consequently, we considered an

euclidian distance instead of a hop distance. Such a result is not surprising. It is now well known that a part of the data packets is lost during the forwarding process (due to packet queue overflow and collisions). Moreover, if a sensor node is distant from the sink, the path to reach this sink will be composed of links longer and weaker than the average. Such results are directly related to the choice of the Objective Functions and raise questions about the effectiveness of the default OF based on the ETX metric to select routes.

B. Control Packet Overhead

In this section, the ratio between data packets and control packets is studied. In a dynamic environment with a proactive protocol such as RPL, control packets are used to build and update the DODAG, compute the routes and maintain neighborhood and routing tables. When the network is steady, the routing topology is maintained using a low-rate beaconing process. On the other hand, if an inconsistency is detected, the beacon rate is increased temporarily. This mechanism, governed by Trickle timers [22], is supposed to reduce the amount of control packets while quickly resolving routing issues.

However, our results show that the amount of control messages is higher than data messages. These results differ from those obtained in [4] but they are similar to those obtained in [2], both are based on simulations. Figure 5 illustrates the ratio between control messages (composed of DIS, DIO and DAO messages) and data messages. Whatever the transmission power, the ratio between IPv6 control messages and data messages stays relatively stable. Among the control messages, a large part is composed of DAO messages, while DIO and DIS messages represent only 20% and less than 1% respectively. There are several reasons of this proportion. Firstly, DIS packets are used by a sensor node joining or leaving the network; DIS messages are sent at the very beginning of the network life and when a node is being disassociated with the network (as shown in Figure 6). Figure 6 shows the overhead versus the time. We observe on this figure that the DIS traffic is negligible and a considerable part of the overhead is sent at the *birth* of the network. Afterwards, DIS and DIO are sent periodically. Secondly, DIO and DIS messages have the scope of a link. It means they are not forwarded while DAO message is used to propagate destination information upward along the DODAG. These results mean that a large part of energy is wasted for routing signaling. A better timers calibration is clearly required and could eventually solve this issue. To explain such part of control packets, the dynamicity of the network is studied in the next section.

C. Dynamicity

Such results (low delivery rate and large overhead) are the consequence of an important dynamicity even if the network is static (without mobility). In WSN, the physical links are transilient and not robust. In [23], the authors showed that a large part of links was not symmetric or only temporarily. Figure 7 illustrates this instability by underlining the number of neighbors update (add or remove a neighbor from the neighborhood table) per minute. The routing logical structure, as well as the DODAG, can be impacted by such instability because it affects parent-child connection and path metrics

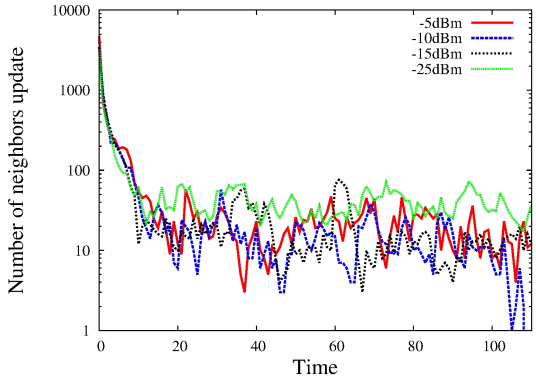

Fig. 7. Scenario 1: Evolution of the number of update per time unit.

(hop count and ETX). Figure 8 illustrates the evolution of the average rank level (ARL) during the experimentation. The stabilization of the ARL is observed 20 minutes after the deployment. Once a node has joined a DODAG, RPL limits the possibility for a child to change its preferred parent, in order to prevent resulting instabilities. However, this limitation seems not to be efficient at the beginning of the experimentation, when the metrics highly evolve. Moreover, when stabilized, important changes are still possible in DODAG, as shown on Figure 8 for the -15 dBm experiment (60 minutes after the deployment).

Despite the evolution of the average rank level, the average path length (i.e. the distance in number of hops between a source and the destination) remains steady (Figure 9). When a child selects another preferred parent (in order to decrease its rank level or because its parent is not available), the new preferred parent does not increase the path length to the destination. It means that the efficiency of the routing process, in other words, the ability to find the shortest paths is preserved.

VI. RPL Robustness: Experimental Results

The outcomes presented in this Section are the results of experiments guided by the scenarios 2 and 3 defined in Section IV-B.

A similar network behavior is observed as studied in [24], the presence of three distinct phases with particular characteristics: the birth, the working life and the death. The **birth phase** corresponds to the progressive arrival of nodes during the network deployment followed by the phase when nodes discover their neighborhood. In RPL, each node diffuses DIO and DAO packets to indicate its presence and transmits information on its state. During the first moments of life (birth), the sensors have generally a partial vision of their neighborhood during the transmission of their first messages. Because of the progressive deployment, the neighboring appears to be dynamic and evolutionary. This leads to transient errors during the preferred parent choice. We observe the time necessary before stabilization of the routing (or logical) structure. On the Figures 10 and 11, a latency from 10 to 15 minutes is observed between the physical birth of the network (when the nodes are deployed) and its logical birth (when the routing structure is stable). The nodes are deployed and switched on in few seconds. However, an important exchange of DIO and DAO

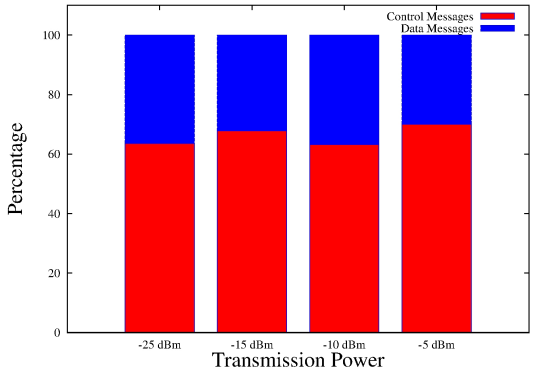

Fig. 5. Scenario 1: Ratio between control messages and data messages with different transmission power.

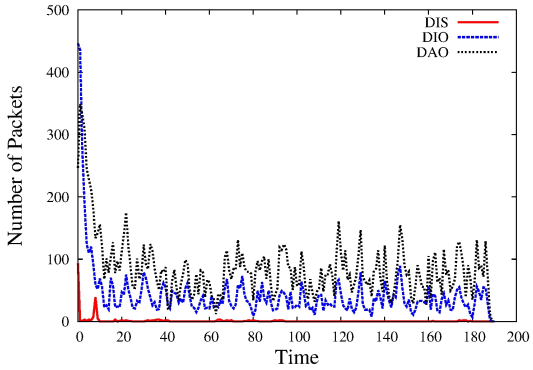

Fig. 6. Scenario 1: RPL overhead in WSN with 100 sensor nodes and a -25 dBm transmission power for DIS, DIO and DAO messages.

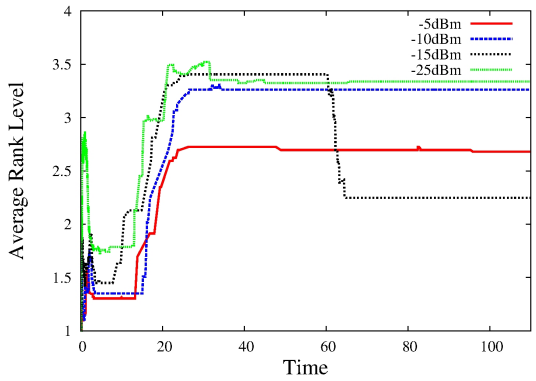

Fig. 8. Scenario 1: Evolution of Average Rank.

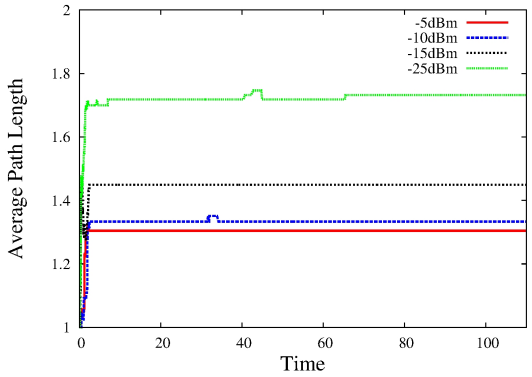

Fig. 9. Scenario 1: Evolution of Average Path.

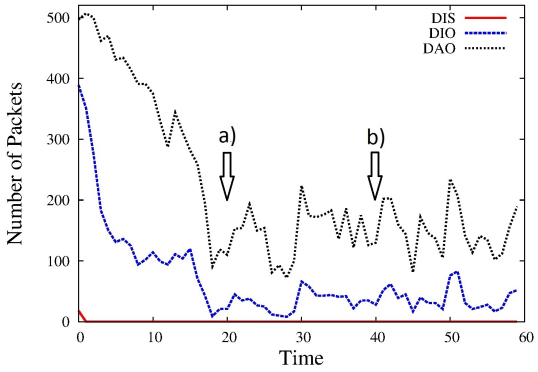

Fig. 10. Scenario 2: Evolution of the RPL overhead when 18 randomly selected sensors are removed (a) and when the same 18 nodes are switch on again (b).

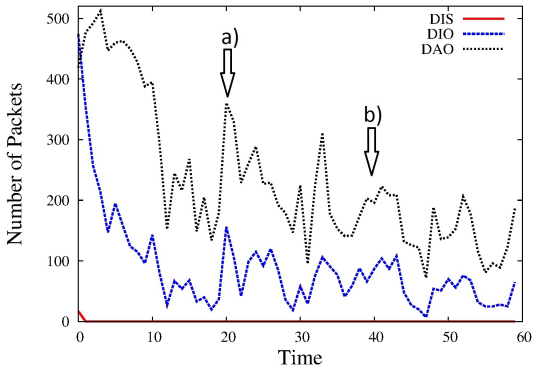

Fig. 11. Scenario 3: Evolution of the RPL overhead when 2 critical sensors (101 and 42) are removed (a) and when the same 2 nodes are switch on again (b).

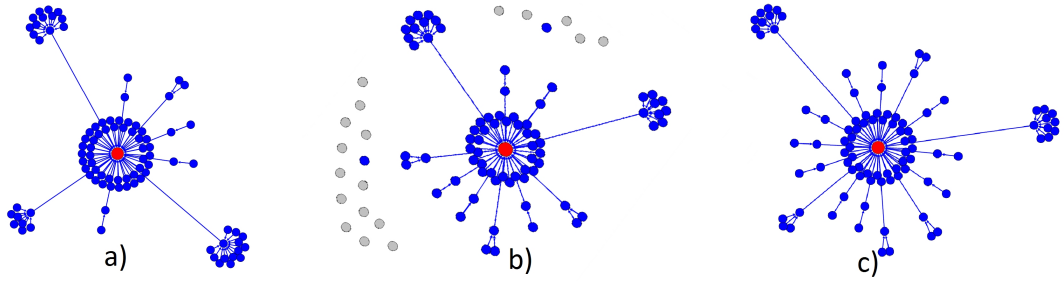

Fig. 12. Scenario 2: Evolution of the RPL Logical Routing Topology 20 minutes after the deployment (a), 20 minutes after we switch off 18 randomly selected sensors (b) and 20 minutes after we switch on again the same 18 nodes (c). Grey nodes represent dead nodes, while blue nodes are the node alive. For greater clarity, sensor nodes are positioned according their distance, in hops, to the sink (in center and in red).

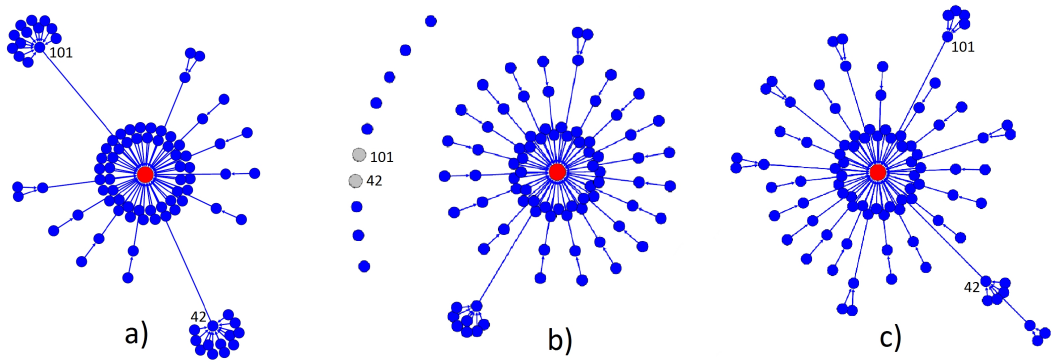

Fig. 13. Scenario 3: Evolution of the RPL Logical Routing Topology 20 minutes after the deployment (a), 20 minutes after we switch off 2 critical sensors (101 and 42) (b) and 20 minutes after we switch on again the same 18 nodes (c). Grey nodes represent dead nodes, while blue nodes are the node alive. For greater clarity, sensor nodes are positioned according their distance, in hops, to the sink (in center and in red).

messages is observed. This is typically the behavior of new arrived nodes, which use DIO to probe their neighborhood for nearby DODAGs and DAO to inform parents of their presence and reachability to descendants.

The phase of **working life** begins as soon as the logical topology is stabilized. At this phase, sensor nodes are able to send their data packets to the sink. In terms of routing structure, we remarks similar logical topologies on Lille and Rennes platforms: few nodes form "hubs", connecting numerous 2-hop nodes to the sink (Figures 3.a and 3.b and Figures 11.a and 12.a). Concerning the overhead (i.e. control packets), the same pattern is observed as in network birth and working life (Figures 6 and 10): a high number of DAO and DIO messages is exchanged during the first 10 minutes of the network's life, afterwards, the number of messages is stabilized between 100 and 200 packets per minute.

The **death phase** begins when several nodes are removed. The self repairing of the logical topology is necessary, when one or several nodes disappear or become unavailable. Because of a certain inertia, the nodes have not immediately the perception of the death of a neighbor. This last phase can be assimilated to the self-healing process.

For the scenario 2, when 20% of the nodes are removed (Figure 10 a)), only few changes are observed; the total number of exchanged control packets is constant. In fact, the number of sent control packets per node is increased. However, it counterbalanced by the effect of removed nodes, which do not send packets. In terms of logical topology, the structure is not impacted deeply. The difference between the cases a) and b) is not significant (Figure 12). Despite almost 20% of dead nodes, only 2 nodes are alive and disconnected from the sink. The particular structure aforementioned limits the delivery ratio. However, as far as the outage probability is a random and uniform process, it increases the robustness because the routing relies on only few "critical" nodes.

When the dead nodes are switched on 20 minutes after their death, the new logical topology is different from the initial one (Figure 12.c). The "hub" nodes have disappeared and the routing is shared among a larger number of nodes. When a new node arrives in a stable DODAG, it selects its preferred parent among several other nodes based on stable ranks. At the birth, the nodes select their parents with a partial vision of their neighbors. The first node to obtain a better rank attracts an important number of children. Then, the children are limited, by RPL, to change their parent to avoid instability. This phenomenon creates "hub" nodes. A limited impact on the amount of control packets is observed on the Figure 10 (b), when the dead nodes are switched on.

For the scenario 3, when the 2 critical nodes (nodes id: 42 and 101) are removed, a significant impact on the amount of sent control packets is observed on Figure 11 a). The number of DIO and DAO packets is significantly increased. More than 500 packets are sent per minute. We observe a similar impact on Figure 13. It illustrates a serious consequence of the death of 2 critical nodes. The difference between the cases a) and b) is important: a part of the 2-hop sensors chose other parents to reach the sink, while some of them stay unconnected.

When the dead nodes are switched on 20 minutes after their death, the new logical topology is similar to the topology observed before (Figure 13.c). The disconnected nodes select the nodes 42 and 101 as preferred parents. As in the scenario 2, a limited impact on the amount of control packets is observed on the Figure 11 (b), when the dead nodes are switched on.

VII. Conclusion and Future Work

A routing protocol should cope with the network dynamics inherent to WSNs. In this paper, we conducted a study on 2 large WSN plateforms with 100 nodes each. The behavior of RPL, deployed in a dense sensor network and a real environment, is investigated. Firstly, the efficiency in terms of delivery rate, control packet overhead and dynamicity is studied. Secondly, the self-healing nature of RPL is studied when several nodes are removed or added to the network. Two scenarios have been investigated: the death and reappearance of several randomly selected nodes and few critical nodes. This paper presents, to the best of our knowledge, the first experimental results of RPL's robustness on a such important platform. The main contribution of this work is that we have identified several key behaviors of RPL protocol in a large and dense WSN:

- The strong stability of the path length despite the instability of the physical topology;
- The stabilization of the logical routing structure takes time but stay relatively stable once built;

- Despite the efficiency of the routing protocol to find shortest path, the delivery rate is particularly low for very dense networks;
- The major part of the IPv6 traffic is composed of control packets. This traffic increases the canal contention and favors collisions.
- The stability of the routing structure is preserved even when a large part of randomly selected sensor nodes is removed.
- However, due to its particular logical structure ("hub" nodes aggregating numerous children nodes), the RPL stability is broken if some critical nodes fails.

Finally, RPL could be considered as a smart routing protocol, when an adaptive period is considered for the control messages as well as an efficient shortest path route is built. Even in a very dense network, RPL is able to work and transmit a non negligible part of the traffic. Thanks to its gradient-based routing mechanism, RPL is robust against topological changes and is inherently self-healing. However, the routing metrics, as defined by default, favor the creation of "hubs", aggregating most of 2-hops nodes. These nodes are the points-of-failure of the logical structure.

Future works. To be more efficient, the Trickle mechanism should be adapted and a better calibration of the timers is clearly required. We also plan to investigate the impact of the objective function on the stability and the efficiency of RPL. Recently, an relevant work has been done in this direction to adapt RPL to a vehicular network [25]. In addition, the MAC layer mechanisms, not studied here, have certainly an impact on the performance of RPL and need to be investigated.

VIII. Acknowledgments

This work was made possible by NPRP grant #NPRP4-553-2-210 from the Qatar National Research Fund (a member of The Qatar Foundation). The statements made herein are solely the responsibility of the authors.

References

[1] "Internet engineer task force," http://www.ietf.org.

[2] N. Accettura, L. Grieco, G. Boggia, and P. Camarda, "Performance analysis of the rpl routing protocol," in *Mechatronics (ICM), 2011 IEEE International Conference on*, april 2011, pp. 767 –772.

[3] O. Gaddour and A. KoubíA, "Survey rpl in a nutshell: A survey," *Comput. Netw.*, vol. 56, no. 14, pp. 3163–3178, Sep. 2012. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2012.06.016

[4] J. Tripathi, J. de Oliveira, and J. Vasseur, "A performance evaluation study of rpl: Routing protocol for low power and lossy networks," in *Information Sciences and Systems (CISS), 2010 44th Annual Conference on*, march 2010, pp. 1 –6.

[5] T. Watteyne, K. Pister, D. Barthel, M. Dohler, and I. Auge-Blum, "Implementation of gradient routing in wireless sensor networks," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, 2009, pp. 1–6.

[6] Y. Liu, Y. He, M. Li, J. Wang, K. Liu, L. Mo, W. Dong, Z. Yang, M. Xi, J. Zhao, and X.-Y. Li, "Does wireless sensor network scale? a measurement study on greenorbs," in *INFOCOM, 2011 Proceedings IEEE*, april 2011, pp. 873 –881.

[7] E. W. Dijkstra, "Self-stabilizing systems in spite of distributed control," *Commun. ACM*, vol. 17, no. 11, pp. 643–644, Nov. 1974. [Online]. Available: http://doi.acm.org/10.1145/361179.361202

[8] S. Dolev, *Self-stabilization*. Cambridge, MA, USA: MIT Press, 2000.

[9] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 5, no. 4, pp. 11–25, Oct. 2001. [Online]. Available: http://doi.acm.org/10.1145/509506.509514

[10] R. Ellison, R. Linger, T. Longstaff, and N. Mead, "Survivable network system analysis: a case study," *Software, IEEE*, vol. 16, no. 4, pp. 70–77, 1999.

[11] S. Dolev, "Self-stabilizing routing and related protocols," *Journal of Parallel and Distributed Computing*, vol. 42, no. 2, pp. 122 – 127, 1997. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0743731597913174

[12] J. Ben-Othman, K. Bessaoud, A. Bui, and L. Pilard, "Self-stabilizing algorithm for energy saving in wireless sensor networks," in *Computers and Communications (ISCC), 2011 IEEE Symposium on*, 2011, pp. 68–73.

[13] J. P. G. Sterbenz, R. Krishnan, R. R. Hain, A. W. Jackson, D. Levin, R. Ramanathan, and J. Zao, "Survivable mobile wireless networks: issues, challenges, and research directions," in *Proceedings of the 1st ACM workshop on Wireless security*, ser. WiSE '02. New York, NY, USA: ACM, 2002, pp. 31–40. [Online]. Available: http://doi.acm.org/10.1145/570681.570685

[14] A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, "Rpl: Ipv6 routing protocol for low-power and lossy networks," March 2012. [Online]. Available: http://www.rfc-editor.org/rfc/rfc6550.txt

[15] D. S. J. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," *Wirel. Netw.*, vol. 11, no. 4, pp. 419–434, Jul. 2005. [Online]. Available: http://dx.doi.org/10.1007/s11276-005-1766-z

[16] "Very large scale open wireless sensor network testbed," http://www.senslab.info, 2010.

[17] "Chipcon inc, cc2420 datasheet," http://www.ti.com/product/cc2420, 2008.

[18] A. Dunkels, "Full tcp/ip for 8-bit architectures," in *Proceedings of the 1st international conference on Mobile systems, applications and services*, ser. MobiSys '03. New York, NY, USA: ACM, 2003, pp. 85–98. [Online]. Available: http://doi.acm.org/10.1145/1066116.1066118

[19] A. Dunkles, "Rime: A lightweight layered communication stack for sensor networks," in *Proceedings of the European Conference on Wireless Sensor Networks (EWSN), Poster/Demo session*, Delft, The Netherlands, jan 2007. [Online]. Available: http://dunkels.com/adam/dunkels07rime.pdf

[20] M. Durvy, J. Abeillé, P. Wetterwald, C. O'Flynn, B. Leverett, E. Gnoske, M. Vidales, G. Mulligan, N. Tsiftes, N. Finne, and A. Dunkels, "Making sensor networks ipv6 ready," in *Proceedings of the 6th ACM conference on Embedded network sensor systems*, ser. SenSys '08. New York, NY, USA: ACM, 2008, pp. 421–422. [Online]. Available: http://doi.acm.org/10.1145/1460412.1460483

[21] J. Zhao and R. Govindan, "Understanding packet delivery performance in dense wireless sensor networks," in *Proceedings of the 1st international conference on Embedded networked sensor systems*, ser. SenSys '03. New York, NY, USA: ACM, 2003, pp. 1–13. [Online]. Available: http://doi.acm.org/10.1145/958491.958493

[22] P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. Ko, "The trickle algorithm," March 2011. [Online]. Available: https://tools.ietf.org/html/rfc6206

[23] K. Heurtefeux and F. Valois, "Is rssi a good choice for localization in wireless sensor network?" in *Advanced Information Networking and Applications (AINA), 2012 IEEE 26th International Conference on*, march 2012, pp. 732 –739.

[24] ——, "Topology control algorithms: a qualitative study during the sensor networks life," in *Mobile Adhoc and Sensor Systems, 2007. MASS 2007. IEEE Internatonal Conference on*, oct. 2007, pp. 1 –7.

[25] K. C. Lee, R. Sudhaakar, J. Ning, L. Dai, S. Addepalli, J. P. Vasseur, and M. Gerla, "A comprehensive evaluation of rpl under mobility," *International Journal of Vehicular Technology*, vol. 2012, p. 10, 2012.