Analysing and Reducing Network Inaccessibility in IEEE 802.15.4 Wireless Communications

Jeferson L. R. Souza and José Rufino
University of Lisboa - Faculty of Sciences
LaSIGE - Navigators Research Team
Email(s): jsouza@lasige.di.fc.ul.pt, ruf@di.fc.ul.pt

***Abstract*—Network inaccessibility is a temporal issue derived from the presence of faults affecting the communication services provided by the medium access control (MAC) sublayer. The occurrence of network inaccessibility represents temporary "communication blackouts", which prevent communications to be performed and may imply disruptions of network operation, therefore compromising the dependability and timeliness of communications. This paper uses an analytical model accounting for network inaccessibility periods in wireless sensor and actuator networks, presenting the IEEE 802.15.4 standard as a case study. The analytical model is then used to derive a set of simple, yet quite effective policies to reduce the durations of the periods of network inaccessibility. The effectiveness of these policies can be evaluated using a tool based on the analytical model, which is being integrated in the NS-2 simulator for validation. Reducing network inaccessibility is a crucial step to enable the use of wireless networking technologies in real-time settings.**

***Index Terms*—wireless sensor and actuator networks, real-time, timeliness, dependability, network inaccessibility.**

I. Introduction

There is a strong demand for the use of wireless sensor and actuator networks (WSANs) on settings with temporal restrictions, where real-time communications are fundamental. In many environments, such as in complex embedded systems aboard autonomous aerial and terrestrial vehicles, WSANs are the perfect communication technology to permit the balance between the needs of real-time networks and the reduction of system size, weight, and power consumption (SWaP), altogether without lessen timeliness and dependability guarantees [12].

A lot of work has been presented, proposing new protocols [1], [3], [4], [13]–[15], [20], [21], modifications on the existent standards [6], [9], [19], and abstract models [10] trying to enhance the real-time guarantees and reliability of wireless communications.

These works, built on analysis focused on timeliness, pay no or little attention to dependability aspects of communications. The fault model (when presented) only considers faults on data domain, disregarding the disruptive effect that faults may have on the medium access control (MAC) sublayer operation and its services. However, such faults may induce temporary "communication blackouts", which lead to the execution of additional procedures to reestablish normal MAC protocol operation. Meanwhile, the MAC protocol is prevented from providing service and the network is inaccessible. When a network inaccessibility incident occurs communications cannot be performed for a period of time. One key point is that the periods of network inaccessibility may have a duration much higher than the normal worst case network access delay. As a consequence, the overall timeliness and dependability properties of the system may be at risk, being compromised at communication service level.

A solution to the problem of controlling network inaccessibility is needed to secure an effective and efficient real-time wireless communications support. Defining a strategy for network inaccessibility reduction is not only a significant but also an essential step towards that goal. Therefore, motivated by a pressing need to attenuate the negative effects caused by network inaccessibility, this paper presents and discusses an analytical model and a set of simple, yet quite effective policies to reduce the duration of network inaccessibility within IEEE 802.15.4 wireless communications [7].

To present our advances the paper is organized as follows: Section II presents an overview of the IEEE 802.15.4 standard. Section III introduces network inaccessibility and presents the analytical model characterising network inaccessibility on IEEE 802.15.4 wireless networks. Section V explains the policies defined to reduce the duration of network inaccessibility on IEEE 802.15.4 communications. Section VI briefly presents a tool for evaluating inaccessibility durations in IEEE 802.15.4 and its preliminary validation using the NS-2 simulator. Section VII analyses the impact of network inaccessibility reduction policies on the timeliness of the standard IEEE 802.15.4 MAC sublayer operation. Finally, section VIII draws the conclusion, and some future work.

II. IEEE 802.15.4 - Overview

The IEEE 802.15.4 [7] has two operation modes dubbed nonbeacon-enabled and beacon-enabled. This paper is focused on the beacon-enabled mode, designed to support traffic with temporal restrictions. In a beacon-enabled mode there is a

This work was partially supported: by the EC, through project IST-FP7-STREP-288195 (KARYON); by FCT/DAAD, through the transnational cooperation project PROPHECY; and by FCT, through the project PTDC/EEI-SCR/3200/2012 (READAPT), the Multiannual Funding Program, and the Individual Doctoral Grant SFRH/BD/45270/2008.

978-1-4799-0537-9/13/$31.00 ©2013 IEEE

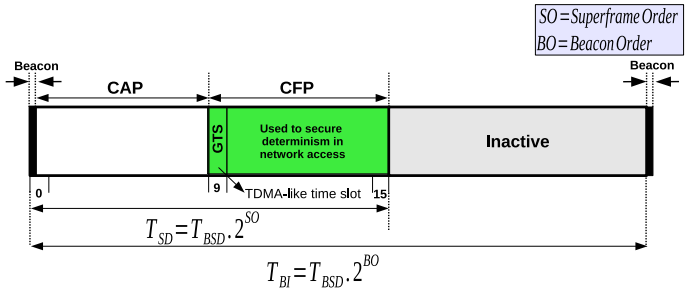

Fig. 1: Superframe structure of the IEEE 802.15.4 in beacon-enabled mode

coordinator node that manages and controls network access. The default superframe structure [7], represented in Fig. 1, is utilised by the coordinator to control the access to the network. The duration of a superframe is calculated utilising a constant that defines the minimum (also known as base) superframe duration, $\mathcal{T}_{BSD}$, and a beacon order exponent, BO, which is utilised to determine the actual time interval between consecutive beacon frames, $\mathcal{T}_{BI}$, as given by:

$$\mathcal{T}_{BI} = \mathcal{T}_{BSD} \cdot 2^{BO} \tag{1}$$

As illustrated by Fig. 1, the default superframe structure has a contention access period (CAP), where nodes compete in equal condition to access the network in a non-real-time manner; a contention free period (CFP), where nodes access the network within exclusive time slots (GTS, the Guaranteed Time Slots) supporting real-time traffic in a similar manner of time division multiple access (TDMA) approaches; and an optional inactive period (IP), where nodes may enter in a power-save mode. Several time slots may be allocated to a node, for exclusive and contention-free network access.

The CAP and CFP together represent the active portion of the superframe structure, which has a duration given by:

$$\mathcal{T}_{SD} = \mathcal{T}_{BSD} \cdot 2^{SO} \tag{2}$$

where SO is the superframe order exponent that defines the duration of this active portion. If $SO = BO$ there is no IP within the superframe.

III. Analysing Network Inaccessibility in IEEE 802.15.4 Wireless Communications

Network inaccessibility is characterised by a temporary lack of network access due to disturbances on MAC sublayer operation. Inaccessibility incidents need to be controlled to enforce real-time operation, meaning: one must ensure that such events have limited duration and rates; violation of such bounds leads to the permanent failure of the network.

The definition of an analytical model, thoroughly characterising network inaccessibility incidents and their durations for the IEEE 802.15.4 MAC protocol has been introduced in [18]. For the purpose of self-completeness, we summarise next some details of such analysis. For the relevant scenarios, we show how the corresponding periods of network inaccessibility are derived, being their worst case durations represented by the superscript (^{wc}).

The beacon frame controls the access to the network, and its reception is essential to maintain all the nodes synchronised within the different periods of the superframe structure. If a beacon frame is not correctly received, a network inaccessibility incident occurs. Thus, a **single beacon frame loss** occurs when only one beacon is lost:

$$\mathcal{T}_{ina\leftarrow sbfl} = \mathcal{T}_{BSD} \cdot (2^{BO} + 1) \tag{3}$$

The value of $\mathcal{T}^{wc}_{ina\leftarrow sbfl}$ is equivalent to $\mathcal{T}_{BI}$ plus an extra $\mathcal{T}_{BSD}$ margin, accommodating the clock skew between a node and its coordinator. The **multiple beacon frame loss** occurs when multiple and consecutive beacons are lost:

$$\mathcal{T}^{wc}_{ina\leftarrow mbfl} = nrLost \cdot \mathcal{T}_{BSD} \cdot \left(2^{BO} + 1\right) \tag{4}$$

where a correct beacon frame is successfully received after the loss of $nrLost$ beacons. The **synchronisation loss** is a special case of the *multiple beacon frame loss* scenario where after the loss of $nrLost$ beacons, the next beacon is also lost. A node loses synchronisation with the network coordinator after a period given by:

$$\mathcal{T}_{ina\leftarrow nosync} = nrLost \cdot \mathcal{T}_{BSD} \cdot \left(2^{BO} + 1\right) \tag{5}$$

To recover from a synchronisation loss, two different strategies were identified in the standard specification [7]. Each individual node chooses the recovery strategy that it should use. We assume that if a data/control frame was received during the last beacon interval, the node assumes an *orphan* status; otherwise, a *re-association* procedure should be carried out. In both recovery strategies, the node looks for a coordinator in a given set of logical channels[1]. After the channel scan, a coordinator realignment or an association procedure is performed within the *orphan* and *re-association* scenarios, respectively. Thus, the worst case duration of network inaccessibility for the **orphan** scenario is given by:

$$\begin{aligned} \mathcal{T}^{wc}_{ina\leftarrow orphan} = \; & \mathcal{T}_{ina\leftarrow nosync} + \\ & \sum_{j=1}^{nrchannels} \left[\mathcal{T}^{wc}_{MAC}(Orphan) + nrWait \cdot \mathcal{T}_{BSD}\right] \\ & + \mathcal{T}_{MLA}(Realign) + \mathcal{T}^{wc}_{MAC\_ack}(Realign) \end{aligned} \tag{6}$$

where: $nrchannels$, represents the number of logical channels to be scanned; $nrWait$, defines the waiting period for a beacon frame in each channel scan; $\mathcal{T}_{MAC\_ack}(frame)$ and $\mathcal{T}_{MAC}(frame)$ represent the delay from request to confirmation of a MAC frame transmission with and without acknowl-

[1] A logical channel is an abstract representation of a radio frequency (RF) channel utilised by the MAC layer to perform its network communications.

edgement; the reference to $\mathcal{T}_{MLA}(action)$ represents the time needed to perform the specified action at the MAC management layer. Without loss of generality, an uniform value of $\mathcal{T}_{MLA}(action) = \frac{1}{10}.\mathcal{T}_{BI}$ is assumed for the duration of each MAC management layer action.

In the **re-association** scenario, a node sends a beacon request ($Beacon\_R$) and waits for the reception of a beacon; upon beacon reception, recovery proceeds with an association ($Assoc\_R$) procedure and the extraction (Ext_R) of control information from the network coordinator:

$$\begin{aligned}\mathcal{T}^{wc}_{ina\leftarrow reAssoc} = \mathcal{T}_{ina\leftarrow nosync} + \\ \sum_{j=1}^{nrchannels} [\mathcal{T}^{wc}_{MAC}(Beacon\_R) + nrWait.\mathcal{T}_{BSD}] + \\ \mathcal{T}_{MLA}(Beacon) + \mathcal{T}^{wc}_{MAC\_ack}(Assoc\_R) + \\ \mathcal{T}_{MLA}(Assoc) + \mathcal{T}^{wc}_{MAC\_ack}(Ext\_R)\end{aligned} \quad (7)$$

Finally, a **coordinator conflict** occurs when more than one coordinator is active within the same network. By default, each network has an identifier, the *source identifier*, which identifies the network uniquely and is used by the coordinator in beacon transmissions. If some other (possibly old) coordinator enters the network operational space, e.g., after having been away from some period of time, the network may have two different coordinators transmitting beacons with the same *source identifier*. To solve such conflict, the current coordinator performs a search within a set of specified logical channels. After the scan in all logical channels, a fresh *source identifier* is selected and, if necessary, a MAC coordinator realignment command is broadcast:

$$\begin{aligned}\mathcal{T}^{wc}_{ina\leftarrow Conflict} = \mathcal{T}_{MLA}(Conflict) + \\ \sum_{j=1}^{nrchannels} [\mathcal{T}^{wc}_{MAC}(Beacon\_R) + nrWait.\mathcal{T}_{BSD}] \\ + \mathcal{T}_{MLA}(Realign) + \mathcal{T}^{wc}_{MAC}(Realign)\end{aligned} \quad (8)$$

IV. Network Parametrisation for Real-Time Operation

The first step towards real-time network operation may simply emerge from the fine-adjustment of a relevant set of network configuration parameters. This is formalised by the following proposition:

***Proposition** 1:* Each node accesses the network in a bounded and known time interval of, at most, $\mathcal{T}_{ac}$.

The guarantees provided by this proposition depends on the network technology, its characteristics and, ultimately, on network configuration parameters. The value of $\mathcal{T}_{ac}$ simply accounts for the raw network access delay observed at MAC sublayer before starting a frame transmission; it does not account for the frame transmission time and it does not include any buffering/queueing effects nor any delays associated with possible frame retransmissions.

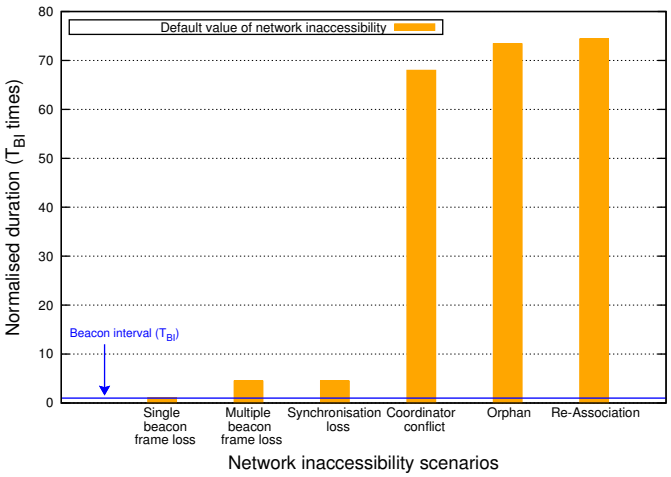

Fig. 2: The default values of IEEE 802.15.4 network inaccessibility durations normalised by, and compared with, $\mathcal{T}_{BI}$ ($\mathcal{T}_{BI} = 123ms$) ($nrWait = 32$; $nrChannels = 16$).

A. IEEE 802.15.4 networks

For the particular case of IEEE 802.15.4 networks operating in beacon-enabled mode, a bounded and known $\mathcal{T}_{ac}$ is secured given the contention-free network access provided by GTS within a period equal to $\mathcal{T}_{BI}$. Therefore:

$$\mathcal{T}_{ac} = \mathcal{T}_{BI} \quad (9)$$

For the remainder of our analysis we use as an example $\mathcal{T}_{BI} = 123ms$ ($BO = 3$; $\mathcal{T}_{BSD} = 15.36ms$), which can provide a reasonable beacon interval for periodic real-time transmissions, still allowing the use of reliable unicast data transmissions (with $SO = BO = 3$, i.e, no IP).

B. IEEE 802.15.4 network inaccessibility

The durations of network inaccessibility incidents defined by the analytical model of IEEE 802.15.4 discussed in Section III are inscribed in Fig. 2, for a standard network configuration ($nrWait = 32$; $nrChannels = 16$). The (real) value of $\mathcal{T}_{BI}$ is used to normalise the duration of network inaccessibility events, as also shown in Fig. 2. Network inaccessibility incidents have very different durations, with some of them much longer than $\mathcal{T}_{BI}$. Long and highly variable periods of network inaccessibility are a source of disruption and unpredictability in network operation.

V. Reducing Network Inaccessibility in IEEE 802.15.4 Wireless Communications

Reducing the network inaccessibility in IEEE 802.15.4 wireless communications is an essential step to enhance network communication properties such as dependability, timeliness, and predictability, which enforce real-time operation. The network characterisation in Section III is crucial to understand how to reduce (or even eliminate) the longest periods of network inaccessibility.

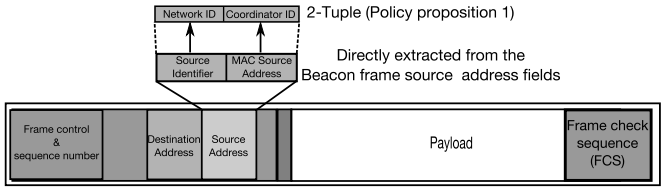

Fig. 3: Representation of a beacon frame.

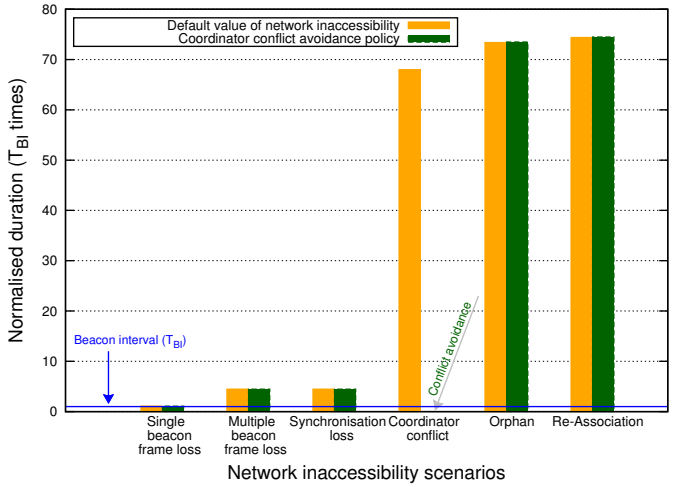

Fig. 4: Impact of the coordinator conflict avoidance policy in the IEEE 802.15.4 network inaccessibility

A. Coordinator conflict avoidance policy

The *coordinator conflict* scenario occurs when two or more coordinators transmit beacons with the same (unique) *source identifier*. A conflict resolution strategy should be triggered after the detection of such scenario (as specified in the IEEE 802.15.4 standard). The duration of network inaccessibility is characterised by the time spent to perform the coordinator conflict resolution. To avoid the coordinator conflict we establish the following proposition:

***Policy proposition** 1:* Each node must use a 2-Tuple $\langle networkID, coordinatorID \rangle$ as a unique compound network identifier, avoiding then coordinator conflicts.

The following check procedure is applied to each received beacon: *If the 2-Tuple* $\langle networkID, coordinatorID \rangle$ *inside the received beacon does not match the 2-Tuple* $\langle networkID, coordinatorID \rangle$ *of the network, the received beacon is discarded.*

Since the *coordinatorID* is directly extracted from the node MAC source address (Fig. 3) and this is unique for each node, the resulting 2-Tuple $\langle networkID, coordinatorID \rangle$ is also unique, for a given network coordinator. No coordinator conflict will ever occur (Fig. 4).

The 2-Tuple beacon check procedure extends and replaces the native IEEE 802.15.4 operation and can be made compatible with the standard specification. This procedure is not hard to implement in modern wireless communication platform [2]. Finally, since the 2-Tuple $\langle networkID, coordinatorID \rangle$ is directly extracted from existing fields in the standard beacon frame, no modification to the standard is required and no overhead is added to MAC sublayer operation.

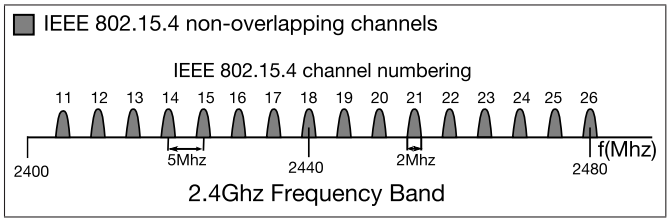

Fig. 5: IEEE 802.15.4 channels within 2.4Ghz frequency band

The presence of malicious entities, which may cause an intentional coordinator conflict problem, are not addressed in this paper. Malicious entities need to be handled with additional techniques to overcome the hazards that they may cause, and will be addressed in a future work.

B. Channel utilisation awareness policy

To reduce the network inaccessibility periods resulting from the *orphan* and *re-association* scenarios, we design a policy that exploits the knowledge of channel utilisation by the network coordinator to reduce the time spent in logical channel scan operations.

In the channel utilisation awareness policy each node is "aware" of the number of logical channels available in the network to search for the presence of the network coordinator, being represented by the following proposition:

***Policy proposition** 2:* Each node is aware of the logical channel utilisation within its associated network, restricting the search for the network coordinator in some $C_a := \{c \mid c \in C \wedge C \subset A\}$, where C_a is the search channel set and A is the set of the available logical channels, being $0 < \#C_a < \#A$.

The nodes use a subset, C_a, of the available logical channels set, A, to confine its channel utilisation scope. Each node is able to search and find the network coordinator within that confined channel search space, reducing then the amount of time needed to find the network coordinator. Restricting the number of logical channels in the channel search space has no impact on network throughput, since only one logical channel is in use at a time. In fact, in the presence of noisy channels, selecting a restricted set of logical channels exhibiting lower error rates, may actually contribute to a potential increase of channel effective throughput, and to reduce the amount of energy utilized to complete a frame transmission successfully.

In the particular case of IEEE 802.15.4 networks there is no mutual channel interference since all the $\#A = 16$ channels are non-overlapping (Fig. 5). Thus, we can choose an arbitrary number of logical channels to include in subset C_a. Figure 6 illustrates the impact of our channel utilisation awareness policy in a IEEE 802.15.4 network, where the value of $\#C_a$ is successively reduced to half, until an optimal $\#C_a = 2$ value is reached. A value of $\#C_a = 2$ minimises the duration of network inaccessibility for the *orphan* and *re-association* sce-

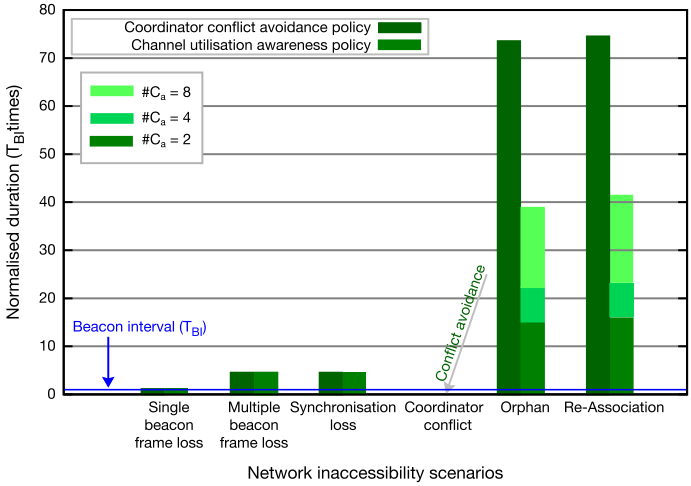

Fig. 6: Impact of the channel utilisation awareness policy in the IEEE 802.15.4 network inaccessibility

narios, while preserves the dependability property of channel diversity.

C. Network dependability awareness policy

The frame check sequence (FCS) is a fundamental mechanism to verify the integrity of a received frame, and therefore to detect accidental errors with an appropriate coverage. When a frame is received with errors, such frame is automatically discarded and nothing is signalised upward (FCS default operation). Only the reception of frames without errors are signalised. The lack of a management notification for such discarded frames prevents the MAC management entities to detect and account for omission errors.

Algorithm 1 presents an extension to the FCS default operation, which introduces a management signalisation to notify the status of the received frame, even if the frame contains errors and must be discarded. Two fundamental additions were proposed: the extraction of the frame header (line 6); and the notification of the received frame status to the MAC management entities (line 14), being such status represented by the *fcs_error* variable. The information within frame header (e.g., source address) may be utilised to identify if the sender is the owner of a *time_slot*, in case of transmissions within CFP.

The improvements proposed in Algorithm 1 are simple, efficient, and not hard to implement off-the-shelf using modern commercially available wireless communication platforms [2].

The notification of the status of the received frame, which is proposed in Algorithm 1, also allows to built accurate error detection and accountability solutions. In particular, an error that destroys a frame is transformed into an omission. Thus, Algorithm 2 presents a simple mechanism to account for channel omissions. The number of consecutive omissions observed by a node within the current logical channel is represented by O_d, the omission degree, in line 2. The value of O_d is cleared every time a frame is received without

Algorithm 1 Extending frame check sequence (FCS) mechanism

```
1:  Initialisation phase.
2:  fcs_error ←false;
3:  Begin.
4:  loop
5:      when Channel.indication(frame) do
6:          frame_header ←MAC.get.header(frame);
7:          if MAC.FCS.check(frame) is OK then
8:              fcs_error ← false;
9:              MAC.indication(frame);
10:         else
11:             fcs_error ← true;
12:             MAC.frame.discard(frame);
13:         end if
14:         MAC.Mgmt.indication(time_slot, frame_header, fcs_error);
15:     end when
16: end loop
17: End.
```

Algorithm 2 Omission degree monitoring

```
1:  Initialisation phase.
2:  O_d ← 0;
3:  k ← The value of the omission degree bound, k, is dependent of the MAC
    layer characteristics and of the network environment. The IEEE 802.15.4
    standard indirectly defines k ← 3;
4:  Begin.
5:  loop
6:      when MAC.Mgmt.indication(time_slot, frame_header, fcs_error) do
7:          if fcs_error is true then
8:              O_d ← O_d + 1;
9:          else if fcs_error is false then
10:             O_d ← 0;
11:         end if
12:     end when
13:     if O_d > k then
14:         MLA.Mgmt.indication(logical_channel, O_d_exceeds_k);
15:     end if
16: end loop
17: End.
```

errors (line 10). When a frame is received, and an error is detected, the procedure increments O_d (line 8). If O_d exceeds an omission degree bound, k, the MAC management entities are notified (line 14). This may be an indication of a heavily disturbed logical channel or it may be a result of the underestimation of the omission degree bound. In any case, the logical channel should be considered failed. Considering only accidental transient faults, the omission degree of a logical channel can be bounded by the following property: *in a known time interval, omission failures may occur in at most k transmissions*. The value of omission degree bound depends on the network error characteristics and on the environment conditions [5]. The IEEE 802.15.4 standard indirectly defines a fixed value of $k = 3$ in its error handling mechanisms. Having the ability to determine the true omission degree bound of a given logical channel is a worthwhile feature, due to the nature of wireless communications, highly susceptible to multiple external disturbances such as signal attenuation, noise and electromagnetic interferences from other signal sources, and multipath propagation interference due to obstacles in the

IEEE 802.15.4 Parameter	IEEE 802.15.4 Standard Configuration	Dependable Adaptation
nrLost	4	$k+1$
nrWait	32	$(k+1).2^{BO}$

TABLE I: Network parametrisation in function of dependability metrics

communication path.

Our network dependability awareness policy is now formulated by the following proposition:

***Policy proposition** 3:* Each node is aware of the dependability characteristics of the network, described by a set of relevant metrics.

The omission degree bound is one of such dependability metrics, but others may be introduced. For example, slight modifications to Algorithm 2 will allow to assess: the average value of the omission degree, the number of omission degree bound violations within a given period and other statistics.

To illustrate how the dependability parameters can be used to improve the characteristics of wireless communications, we use the omission degree bound k to dynamically define some MAC protocol parameters relevant for IEEE 802.15.4 operation, as specified in Table I, thus opening room for the use of (self-)adaptation techniques, e.g., to cope with varying environment conditions. This may be advantageous for decreasing the network inaccessibility durations associated to the *multiple beacon frame loss* and *synchronisation loss* scenarios.

D. Logical channel diversity policy

The violation of the channel omission degree bound, locally-perceived by each node, should be interpreted as a failure indication. To restore communication one must resort to the following propositions:

***Policy proposition** 4:* There are multiple and redundant logical channels, though only one is active at a time.

***Policy proposition** 5:* Every frame is transmitted only in the active logical channel.

***Policy proposition** 6:* In the presence of faults which may lead a logical channel to an incorrect state, a node may switch to a different logical channel.

In particular, one must take advantage of the use of redundant logical channels, specifying the following procedure: *when a node (including the network coordinator) detects that a given logical channel O_d exceeds k, a node switches to another logical channel*. To avoid the occurrence of a permanent physical partitioning of the network, the same channel switching sequence is used by all nodes, defining a deterministic order utilised to switch from one logical channel to another. Furthermore, we assume: *each node must transmit at least one (heartbeat) frame during its allocated GTS to signal node liveness*. As we are also interested to reduce network inaccessibility durations in benefit of a real-time network operation, only nodes with allocated GTS are monitored.

Algorithm 3 Logical channel diversity procedure - COORDINATOR

```
1: Initialisation phase.
2: nrAssocNodes ← 0;
3: channel_idle_status ← true;
4: Begin.
5: loop
6:     when MAC.Mgmt.request(Beacon) do
7:         nrAssocNodes ← MLA.Mgmt.get(NR_ASSOC_NODES);
8:         if channel_idle_status is true ∧ nrAssocNodes > 0 then
9:             MLA.Mgmt.request(Change_Channel);
10:            MLA.Mgmt.request(RESET_NR_ASSOC_NODES);
11:        end if
12:        channel_idle_status ← true;
13:    end when
14:    when MAC.indication(frame) do
15:        channel_idle_status ← false;
16:    end when;
17:    when MLA.Mgmt.indication(logical_channel, O_d_exceeds_k) do
18:        MLA.Mgmt.request(Change_Channel);
19:        MLA.Mgmt.request(RESET_NR_ASSOC_NODES);
20:    end when
21: end loop
22: End.
```

Upon channel switch it may happen that a node detects no traffic activity because it is the only node in that logical channel. The standard MAC protocol of non network coordinator nodes has mechanisms to detect such situations, signalled to MAC management entities through a *synchronisation loss* indication. The MAC protocol of the network coordinator does not have such capability by default. Thus, we enhance the coordinator to detect channel idleness, as specified in Algorithm 3, taking advantage of node liveness signalisation within GTS slots.

Algorithm 3 describes the execution of the logical channel diversity policy in the coordinator node. When the network coordinator is started the variable utilised to store the number of associated nodes, *nrAssocNodes*, and the channel idle status, *channel_idle_status*, are initialised with 0 and *true*, respectively (lines 2 and 3). A channel switch operation is triggered by two different situations. The first channel switching scenario, described by lines 17 to 20, is a direct consequence of a logical channel failure indication, as provided by the signalling that the value of O_d for the current logical channel has exceeded k (line 17); after logical channel switching (line 18) the list of nodes associated with the network coordinator is cleared (line 19).

The second channel switching situation is more complex and involves the results of monitoring logic channel activity during the last beacon interval. The logic channel monitoring actions are in fact quite simple, being described by lines 14 to 16: upon reception of a correct frame indication (line 14), the channel idle status variable is set to $false$ (line 15). The network coordinator monitors logical channel traffic between any two consecutive beacon transmissions: if a frame is

Algorithm 4 Logical channel diversity procedure - NON COORDINATOR

```
1:  Initialisation phase.
2:  receivedFrame ← false;
3:  Begin.
4:  loop
5:      when MLA.Mgmt.indication(logical_channel, O_d_exceeds_k) do
6:          MLA.Mgmt.request(Change_Channel);
7:      end when
8:      when MAC.Mgmt.indication(SYNC_LOSS) do
9:          receivedFrame ← MLA.Mgmt.get(FRAME_FROM_COORD);
10:         if receivedFrame is true then
11:             MLA.Mgmt.request(ORPHAN,#C_a = 1)
12:         else
13:             MLA.Mgmt.request(RE_ASSOCIATION,#C_a = 2);
14:         end if
15:     end when
16: end loop
17: End.
```

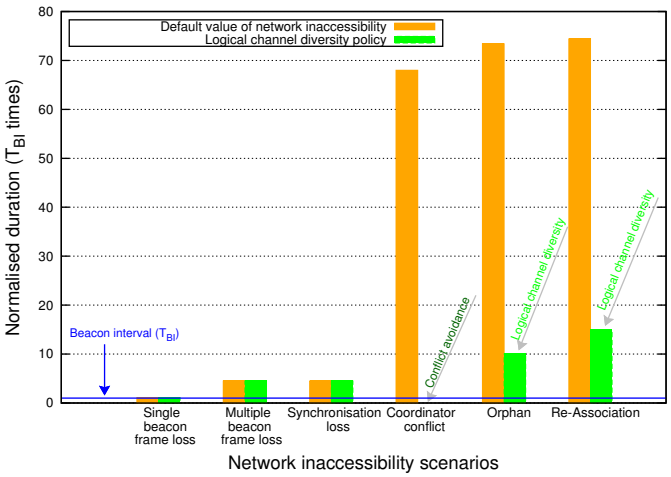

Fig. 7: Impact of the logical channel diversity policy in the IEEE 802.15.4 network inaccessibility ($\#C_a = 1$ and $\#C_a = 2$ for the *orphan* and *re-association* scenarios, respectively).

correctly received, there is no reason, *per se*, to perform a channel switch; if no traffic at all is correctly received within that period and the network coordinator has, at least, one node associated to it (i.e., $nrAssociated > 0$), the logical channel is considered idle (line 8) and the coordinator switches to the next logical channel using a pre-defined channel hopping sequence (line 9); the list of nodes associated with the network coordinator is cleared (line 10).

The boundaries of logical channel monitoring intervals are defined by the periodic issuing of beacon transmission requests, as specified by the management action at line 6. Each time a new logical channel monitoring interval is started (line 6): the logical channel status is evaluated with respect to logical channel idleness (line 8); the value of the channel idle status is set to *true* (line 12); it will remain with that value until a frame is correctly received from the logical channel.

Algorithm 3 should be combined with low-level node failure detection mechanisms to ensure stability in the presence of node crash failures. The logic channel switch procedure (lines 9 and 18) assumes switching to a correct channel, meaning that the value of O_d is cleared ($O_d = 0$). The network coordinator also resets the list of its associated nodes (lines 10 and 19) to avoid a false channel idleness detection within the newly selected logical channel.

Algorithm 4 describes the execution of the logical channel diversity policy at nodes other than the network coordinator. We dubbed such nodes as non-coordinator nodes for the sake of simplicity. When a channel failure indication is received (line 5), a non coordinator node performs a switch operation to other logical channel (line 6), utilising the same pre-defined sequence used by the network coordinator. Provided the network coordinator operates in the same logical channel, and that beacon frames are received by the node, no further action is required to restore communication.

However, it may happen that beacon frames are not received by node. Consequently the node continues inaccessible and may lose synchronisation with the network coordinator (line 8). If some other frame has been received within that period from the network coordinator (line 9), that is a clear indication the network coordinator remains active in the current logical channel and therefore the node declares itself as an orphan node. Since both the network coordinator and the non-coordinator node are on the same logical channel, the node performs an orphan procedure only on this logical channel, being the cardinality of the channel search set $\#C_a = 1$ (line 11). It results in a quick synchronisation re-establishment between the network coordinator and the non-coordinator node. The orphan procedure updates the node information stored by the network coordinator, alerting it about the remaining presence of the node in the same logical channel.

Otherwise, a *re-association* is performed through the execution of the re-association procedure (line 13). The *re-association* procedure is optimised to be performed within only two logical channels, the new logical channel and the previous one (i.e., $\#C_a = 2$). The use of only two logical channels is justified by: (*a*) the network coordinator remains in the previous logical channel with other non-coordinator nodes; or (*b*) the coordinator detects an idle period and switches to the new logical channel, an action that is faster than the detection of a loss of synchronization. While a channel idleness detection has a duration of τ_{BI}, the time required to detect the loss of node synchronisation is, at least, $nrLost = k+1$ times greater than τ_{BI}, as we can see in equation 5 presented in section III. It is worthwhile mentioning that the channel scan process, implicit in the *re-association* procedure, may imply a new logical channel change, upon detection of the network coordinator.

The contributions of this policy, and the general impact of our policies to reduce network inaccessibility in IEEE 802.15.4 wireless communications, are presented in Fig. 7.

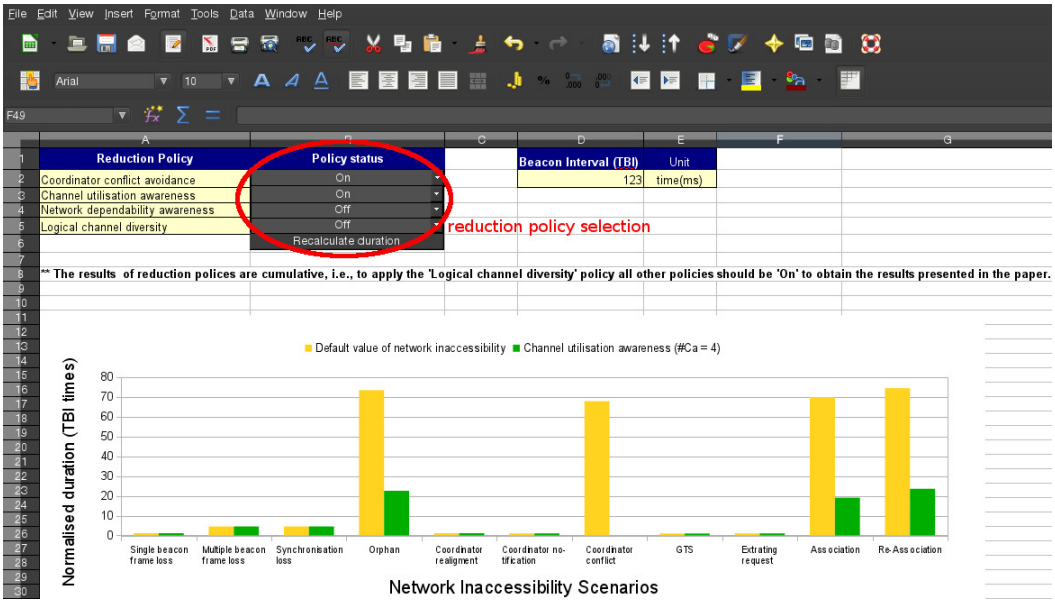

Fig. 8: Use of the network inaccessibility evaluation tool to study the impact of some inaccessibility reduction policies

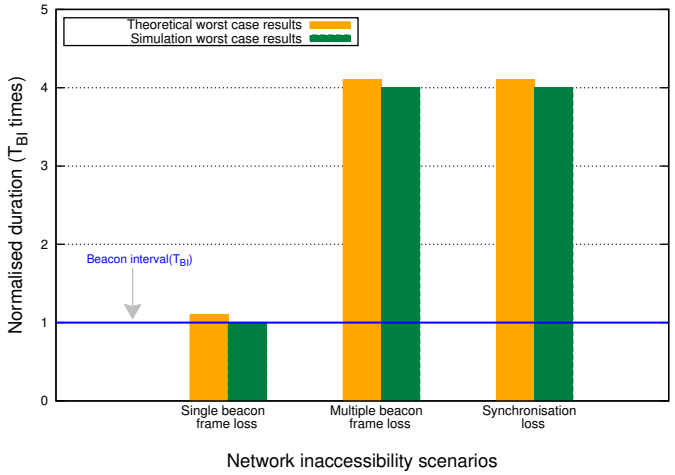

Fig. 9: Preliminary validation of network inaccessibility analysis using the NS-2 simulator and beacon-related scenarios

VI. Network Inaccessibility Analysis: Tool, Results, and Validation

We designed and developed a tool to evaluate the duration of network inaccessibility scenarios as draw from the IEEE 802.15.4 standard. The analysis tool was built on the LibreOffice suite [11].

The tool is a spreadsheet with enhanced LibreOffice macros, which define mechanisms to calculate and verify parameter values, due its specified restrictions. It is also an open source tool available under a GNU General Public License (GPL) version 3, which can be downloaded at: http://www.karyon-project.eu/wp-content/uploads/2012/10/Inaccessibility_IEEE802.15.4_Beacon-enabled-Karyon.ods.

There are different tabs, each one designed to represent constants, parameters, and configurations allowed to be performed on a standard compliant IEEE 802.15.4 network.

The duration of network inaccessibility scenarios are evaluated and visualised as values in milliseconds (*ms*), or as normalised values by $\mathcal{T}_{BI}$ units of time. Figure 8 presents an example of the results obtained from the tool; the set of reduction policies to be used draws from its selection as shown in Fig. 8. The screen capture of Fig. 8 also presents the complete set of network inaccessibility scenarios as presented in [18].

Additionally, we have being working to incorporate the analysis of network inaccessibility on the IEEE 802.15.4 NS-2 module. We already have some preliminary results [16], as illustrated by Fig. 9. This preliminary validation compares a fundamental set of beacon loss scenarios, asserting that our theoretical analysis presents the worst case durations face to simulations performed on NS-2. The incorporation of the remaining scenarios on NS-2 simulator, and therefore the proposed reduction policies requires substantial engineering work to complete and complement the IEEE 802.15.4 NS-2 module. This engineering work needs the implementation of essential management operations to simulate IEEE 802.15.4 networks, and the network inaccessibility durations in total compliance with the IEEE 802.15.4 standard.

VII. Relation with the Standards

On the other hand, the IEEE 802.15.4 specification has been recently enhanced with amendment IEEE 802.15.4e [8], proposing TDMA like schemes to control the access to the network. This amendment aims to enhance IEEE 802.15.4 network operation for the industrial markets, including the utilisation of periodic channel hopping using pre-defined sequences. The operation of these new protocol variants may

benefit from the frame monitoring functions for enhanced dependability introduced in this paper. Conversely, the channel diversity policy can be combined to the now standardised utilisation of channel hopping in IEEE 802.15.4 settings. In practice, all the reduction policies presented in this paper can be easily integrated, and controlled, by a standard compliant solution dubbed *Mediator Layer* [17]. The use of the *Mediator Layer* approach enables and promotes a low level control of communications, which used with the network inaccessibility reduction policies can enhance the dependability and timeliness of the wireless communication standards.

VIII. Conclusion and future work

This paper presented a set of highly effective policies to reduce the negative effects of network inaccessibility on IEEE 802.15.4 wireless networks. The analytical model presented in this paper has shown the limitations of wireless networks to support real-time operation. For example, a standard IEEE 802.15.4 can be affected by network inaccessibility incidents with durations as high as $74.5 \times \mathcal{T}_{BI}$, being $\mathcal{T}_{BI}$ the beacon period. Such long network inaccessibility periods prevents a real-time operation of the network.

However, complemented with frame and channel monitoring mechanisms, a standard IEEE 802.15.4 platform can integrate a set of network inaccessibility control policies that proved to be highly effective in the reduction of the duration of inaccessibility incidents down to $15 \times \mathcal{T}_{BI}$. This is a first step towards solving the difficult problem of enforcing real-time behaviour over wireless networks.

Future research directions of this work includes the study and assessment of new techniques, which exploit multiple communication channels to enhance the reliability of communications; the study of network inaccessibility and the network operation in the presence of malicious attacks; the incorporation of the effects of network inaccessibility in the timeliness model of wireless communications, defining relevant real-time QoS metrics to evaluate if communication network operation is compliant with the level of requirements needed by given applications.

References

[1] I. Aad, P. Hofmann, L. Loyola, F. Riaz, and J. Widmer, "E-MAC: Self-organizing 802.11-compatible MAC with elastic real-time scheduling," in *IEEE International Conference on Mobile Adhoc and Sensor Systems MASS*, October 2007.

[2] ATMEL, *ATMEL AVR2025: IEEE 802.15.4 MAC Software Package - User guide*, ATMEL Coorporation, May 2012.

[3] P. Bartolomeu, J. Ferreira, and J. Fonseca, "Enforcing flexibility in real-time wireless communications: A bandjacking enabled protocol," in *IEEE 14th International Conference on Emerging Technologies & Factory Automation (ETFA)*, September 2009.

[4] E. E-López, J. V-Alonso, A. M-Sala, J. G-Haro, P. P-Mariño, and M. Delgado, "A wireless sensor networks MAC protocol for real-time applications," *Personal Ubiquitous Computing Journal*, January 2008.

[5] D. Eckhardt and P. Steenkiste, "Measurement and analysis of the error characteristics of an in-building wireless network," in *Annual Conference of the Special Interest Group on Data Communication (SIGCOMM)*, 1996.

[6] M. Hameed, H. Trsek, O. Graeser, and J. Jasperneite, "Performance investigation and optimization of IEEE 802.15.4 for industrial wireless sensor networks," in *IEEE 13th International Conference on Emerging Technologies & Factory Automation (ETFA)*, September 2008.

[7] IEEE 802.15.4, "Part 15.4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs) - IEEE standard 802.15.4," 2011.

[8] ——, "Part 15.4: Low-rate wireless personal area networks (WPANs) - amendment 1: MAC sublayer," 2012.

[9] A. Koubâa, A. Cunha, M. Alves, and E. Tovar, "i-GAME: An implicit GTS allocation mechanism in IEEE 802.15.4, theory and practice," *Springer Real-Time Systems Journal*, August 2008.

[10] F. Kuhn, N. Lynch, and C. Newport, "The abstract MAC layer," in *23rd International Symposium on Distributed Computing (DISC)*, September 2009.

[11] LibreOffice, *LibreOffice - The Document Foundation*, LibreOffice, January 2013, avaiable in http://www.libreoffice.org/. Last access- January 30, 2013.

[12] J. Åkerberg, M. Gidlund, and M. Björkman, "Future research challenges in wireless sensor and actuator networks targeting industrial automation," in *9th IEEE Internation Conference on Industrial Informatics (INDIN)*, July 2011.

[13] A. Sahoo and P. Baronia, "An energy efficient MAC in WSN to provide delay guarantee," in *15th IEEE Workshop on Local & Metropolitan Area Networks LANMAN*, June 2007.

[14] M. Sha, G. Hackmann, and C. Lu, "ARCH: Practical channel hopping for reliable home-area sensor networks," in *IEEE 17th Real-Time and Embedded Technology and Application Symposium (RTAS)*, April 2011.

[15] X.-Y. Shuai and Z.-C. Zhang, "Research of real-time wireless networks control system MAC protocol," *Journal of Networks*, April 2010.

[16] J. L. R. Souza, A. Guerreiro, and J. Rufino, "Characterizing inaccessibility in IEEE 802.15.4 through theoretical models and simulation tools," in *4th Simposio de Informática (INFORUM)*, September 2012.

[17] J. L. R. Souza and J. Rufino, "Towards resilient real-time wireless communications," in *25th Euromicro Conference on Real-Time Systems (ECRTS-WiP)*, July 2013.

[18] ——, "Characterization of inaccessibility in wireless networks - a case study on IEEE 802.15.4 standard," in *IFIP 3th International Embedded System Simposium IESS*, September 2009.

[19] Yu-Kai, Ai-Chun, and Hui-Nien, "An adaptive GTS allocation scheme for IEEE 802.15.4," *IEEE Transactions on Parallel and Distributed Systems*, May 2008.

[20] T. Zhou, H. Sharif, M. Hempel, P. Mahasukhon, W. Wang, and T. Ma, "A novel adaptive distributed cooperative relaying MAC protocol for vehicular networks," *IEEE Journal on Selected Areas in Communications*, January 2011.

[21] X. Zhu, S. Han, P.-C. Huang, A. Mok, and D. Chen, "MBStar: A real-time communication protocol for wireless body area networks," in *23rd Euromicro Conference on Real-Time Systems (ECRTS)*, July 2011.