Characterization of Network Inaccessibility in IEEE 802.15.4 Wireless Networks

Jeferson L. R. Souza and José Rufino

DI–FCUL–TR–2013–01

DOI:10455/6898

(http://hdl.handle.net/10455/6898)

January 2013

Characterization of Network Inaccessibility in IEEE 802.15.4 Wireless Networks

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

Wireless communications are vulnerable to the presence of errors during the network operation. These errors may be originated from different sources such as external electromagnetic interferences, obstacles in communication path, or even glitches in the communication circuitry. Such origins may lead the medium access control (MAC) layer to deviate from its normal operation (without presence of errors), forcing the execution of additional actions to maintain the network operational. The execution of such actions may imply the occurrence of periods of "communication silence", where the network, although not being failed, is not performing communications. These periods of "communication silence" are dubbed network inaccessibility, which may induce inaccurate fault detections and deadline misses. Additionally, the occurrence of network inaccessibility may compromise network properties such as predictability, dependability, and timeliness. Thus, this report presents an exhaustive study about network inaccessibility, using the 802.15.4 standard as a case study. All network inaccessibility scenarios are presented, discussing important steps to achieve predictability, dependability, and timeliness in wireless communications.

I. Introduction

Wireless sensor networks (WSNs) are flexible communication networks with a great interest in many areas with temporal restrictions such as industrial, vehicular, military, and aerospace. The main advantages provided by WSNs are the elimination of cables, mobility, and reduced Size, Weight, and Power (SWaP) consumption.

There are some works trying to provide temporal guarantees on WSNs, namely those proposed in [1]–[6]. However, these works do not pay attention to deviation on the medium access control (MAC) layer service that may be caused by electromagnetic interferences, obstacles in the communication path, mobility or even glitches in communication circuitry. Such deviation forces the occurrence of periods where the network does not provide service, although it cannot be considered in a fail state, which are dubbed network inaccessibility [7]–[9]. The occurrence of network inaccessibility may induce inaccurate fault detections, and deadlines violations, which may put the overall system at risk.

This document presents an exhaustive study of network inaccessibility in IEEE 802.15.4 wireless networks. This study of the IEEE 802.15.4 standard specification is important to the knowledge of how network inaccessibility affects the operation of WSNs, and to show the impact of the network inaccessibility times in the transmission time bounds. Additionally, the characterization of network inaccessibility is a first step towards the provisioning of timeliness, dependability and predictability guarantees in WSNs, using off-the-shelf IEEE 802.15.4 technology.

This work was partially supported by EC, through project IST-STREP-288195 (KARYON) and by FCT through the Multiannual Funding and CMU-Portugal Programs and the Individual Doctoral Grant SFRH/BD/45270/2008.

Document Organization

The remainder of the document is organized as follows. Section II presents the concept of network inaccessibility. Section III discusses the system model used in our analysis, describing the corresponding assumptions and fundamental properties. Section IV presents an overview of the IEEE 802.15.4 standard, while section V characterizes fundamental aspects of the IEEE 802.15.4 service interface. Section VI presents an exhaustive study of network inaccessibility in the IEEE 802.15.4 standard and Section VII discusses the corresponding analytical results, showing that real-time operation over wireless sensor networks is still an open problem. Finally, section VIII concludes the document and presents some future research directions.

II. What is network inaccessibility?

The operation of a MAC layer may be disturbed by errors caused by different sources such as external electromagnetic interferences, obstacles in the communication path, glitches in the node circuitry, or even malicious attacks in the more opened environments. These errors may induce the MAC layer to deviate from its normal operation (without the presence of errors), forcing the execution of actions, such as the transmission of control frames, to maintain the network operational. The period comprised from the detection of such deviation until to the end of execution of all the actions needed to reestablish the normal operation of the MAC layer is dubbed network inaccessibility [7], [8]. During a period of network inaccessibility a node[1] locally experiences a period of "communication silence", being not able to communicate with any other node. The definition of network inaccessibility present in [8] is summarized here:

> *Certain kinds of components may temporarily refrain from providing service, without that having to be necessarily considered a failure. That state is called* ***network inaccessibility****. It can be made known to the users of network components; limits are specified (duration, rate); violation of those limits implies permanent failure of the component.*

III. System Model

The rigorous definition of a system model is a crucial step to understand and describe the fundamental aspects of a wireless (sensor) network operation. Our system model is formed by a set of wireless nodes $X = \{x_1, x_2, \ldots, x_n\}$, being $1 < n \leq \#A$, where A is the set of all wireless nodes using the same communication channel. The set of nodes X itself establishes a node relationship entity dubbed wireless network segment, using a given communication channel and a given wireless network identifier.

A. Assumptions

In our system model the behavior of a wireless network segment is sustained by assumptions utilized to characterize the network communication capabilities and restrictions of wireless nodes. During a wireless network segment operation cycle we use the following assumptions:

[1]Node is the designation for a wireless network device capable of sending and receiving frames, following the specification of the physical and MAC layers currently in use.

1) The communication range of X, i.e., its broadcast domain, is given by: $B_X = \bigcap_{j=1}^{n} B_D(x),\ \forall x \in X$, where $B_D(x)$ represents the communication range of a node x;
2) $\forall x \in A,\ x \in X \iff B_X \subseteq B_D(x)$ or, as a consequence of node mobility, $x \notin X \iff B_X \nsubseteq B_D(x)$;
3) $\forall x \in X$ can sense the transmissions of one another;
4) $\exists x \in X$ which is the coordinator, being unique and with responsibility to manage the set;
5) A network component (e.g., a node $x \in X$) either behaves correctly or crashes upon exceeding a given number of consecutive omissions (the component's *omission degree*, f_o) in a time interval of reference[2], $\mathcal{T}_{rd}$;
6) failure bursts never affect more than f_o transmissions in a time interval of reference, $\mathcal{T}_{rd}$;
7) omission failures may be inconsistent (i.e., not observed by all recipients).

Assumptions 1, 2, and 3 define the physical relationship between nodes within the wireless network segment. Our system model characterizes the relationship between nodes at MAC level, where nodes must be in the communication range of each other to communicate and are able to sense one another (assumption 3). Mobility may drive nodes away from wireless network segment (assumption 2).

In the context of network components, an omission is an error that destroys a data frame. Omissions may be caused by different sources such as node mobility, external electromagnetic interference, fading caused by multipath or transient obstacles on the communication medium, glitches on the MAC layer operation, and malicious attacks. Despite of their importance we are not considering malicious attacks in our analysis, being such topic addressed in future work.

Figure 1 presents a graphical representation of a wireless network segment. In this figure we can see the communication range of each node within X, evidencing the intersection between all communication ranges of all nodes, which delimits the broadcast domain of X. We can also see in Fig. 1 the indication of which node is the coordinator. The management activities of the coordinator comprises the assignment of the current communication channel in use by the wireless network segment, the wireless network segment identifier definition, address space delimitation, and so on.

B. Wireless MAC-level properties

A relevant set of properties, presented in Fig. 2, are defined for the MAC layer and hold for the wireless network segment. In wired networks, it has been proven that those properties are extremely useful for enforcing dependability and timeliness at higher layers [9], [10]. Thus, we are applying those techniques to the realm of wireless networks [11].

Properties WMAC1 and WMAC2 impose correctness in the value domain. Property WMAC1 (*Broadcast*) formalizes that it is physically impossible for a node in the wireless network segment to send conflicting information to different nodes, in the same broadcast [12]. Property WMAC2

[2]For instance, the duration of a given protocol execution. Note that this assumption is concerned with the total number of failures of possibly different nodes.

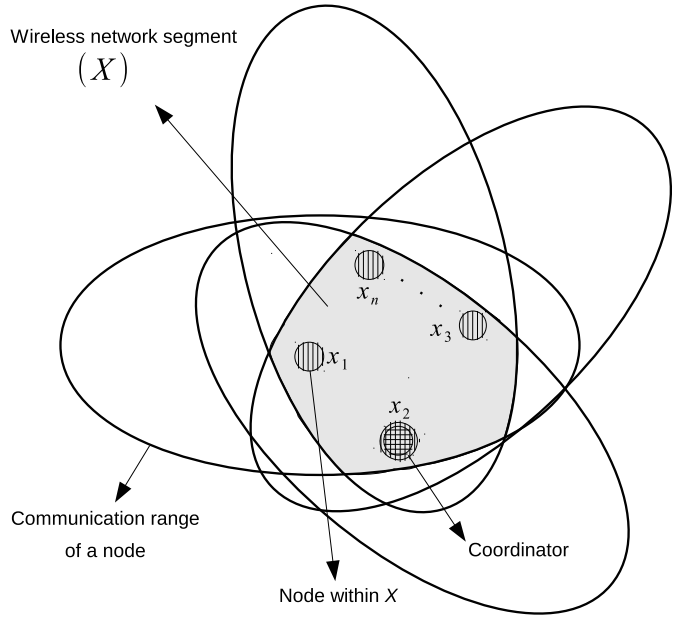

Fig. 1: The graphical representation of a wireless network segment

WMAC1 - ***Broadcast***: correct nodes, receiving an uncorrupted frame transmission, receive the same frame.

WMAC2 - ***Error Detection***: correct nodes detect any corruption done by the network in a locally received frame.

WMAC3 - ***Bounded Omission Degree***: in a known time interval T_{rd}, omission failures may occur in at most k transmissions.

WMAC4 - ***Bounded Inaccessibility***: in a known time interval T_{rd}, a network may be inaccessible at most i times, with a total duration of at most T_{ina}.

WMAC5 - ***Bounded Transmission Delay***: any frame transmission request is transmitted on the network within a bounded delay $T_{td} + T_{ina}$.

Fig. 2: General Wireless MAC-level properties

(*Error Detection*) derives directly from frame protection through a CRC[3] polynomial, as provided by the MAC layer. Frames affected by errors are discarded, usually by the MAC controller itself. This means, frame errors are transformed into omissions. The residual probability of undetected frame errors is negligible [13], [14].

The extension of property WMAC2 to include the signalling of frame discard actions to other protocol entities may significantly contribute to enhance the liveness properties at MAC protocol level. The provisioning of such unconventional primitive can be enabled by emerging controller technology, such as reprogrammable open core MAC layer solutions. No modifications are needed to the IEEE 802.15.4 standard.

Property WMAC3 (*Bounded Omission Degree*) formalizes the failure semantics introduced ear-

[3]CRC - Cyclic Redundancy Check.

lier, being $k \geq f_o$. This property is crucial to implement protocols yielding bounded termination times. For example, the IEEE 802.15.4 specification makes use of the bounded omission degree technique in the definition of a (data/control) frame reliable unicast protocol, at the MAC layer [15].

Considering only the presence of accidental transient faults, the omission degree (i.e., the number of consecutive omission errors during a given protocol execution) of a single channel wireless network infrastructure can be bounded, given its error characteristics [14], [16], [17]. The IEEE 802.15.4 standard defines a MAC protocol configuration parameter equivalent to the channel omission degree bound, k, setting a default value $k \equiv macMaxFrameRetries = 3$ [15].

The *Bounded Omission Degree* property is one of the most complex properties to secure in wireless networks. Securing this property with optimal values and with a high degree of dependability coverage will require the use of multiple communication channels [11]. Although an innovative solution to this problem needs to be further investigated, as soon as achieved it may also provide an effective defence against a class of malicious physical layer attacks, such as radio jamming [11], [18], [19].

The network behavior in the time domain is described by the remaining properties. Property WMAC5 (*Bounded Transmission Delay*) specifies a maximum network transmission delay, which is T_{td} in the absence of faults. The value of T_{td} may include the queuing, network access and transmission delays and it depends on message latency classes and offered load bounds [3], [20]. The value of T_{td} does not include the effects of omission errors. In particular, T_{td} does not account for possible frame retransmissions, such as those foreseen at the MAC level of the IEEE 802.15.4 specification [15]. However, T_{td} may include the extra delays resulting from the queuing effects caused by the occurrence of network inaccessibility.

The bounded network transmission delay includes T_{ina}, a corrective term, which accounts for the worst case duration of network inaccessibility glitches, given the bounds specified by property WMAC4 (*Bounded Inaccessibility*). The network inaccessibility characteristics depend on the network alone and can be predicted by the analysis of the MAC protocol. Some preliminary results on this analysis have been advanced in [17]. This work consolidates and extends those earlier results, doing an exhaustive study of network inaccessibility in IEEE 802.15.4 networks.

IV. IEEE 802.15.4 - Overview

The IEEE 802.15.4 [15] is a standard specified for wireless sensor networks (WSNs) with potential utilization on vehicular, industrial, and aerospatial communications. Each IEEE 802.15.4 network must contain a coordinator that defines the network parameters and characteristics such as addressing, supported channels, and operation mode.

There are two operation modes defined in the standard specification called nonbeacon enabled and beacon enabled. The nonbeacon enabled mode uses a non-slotted version of the carrier sense multiple access with collision avoidance (CSMA/CA) protocol to control the medium access. This control is decentralized, lacking a native support for communications with temporal restrictions.

Conversely, beacon enabled mode has a native specification for supporting communications with temporal restrictions, being the operation mode we are concentrating our further analyses. A coordinator controls the medium access using the superframe structure represented in Fig. 3. The contention access period (CAP), contention free period (CFP), and the optional inactive period are the subdivisions of such structure, bounded by the transmission of a beacon frame used to synchronize nodes for medium access actions on the whole network. In CAP all nodes compete

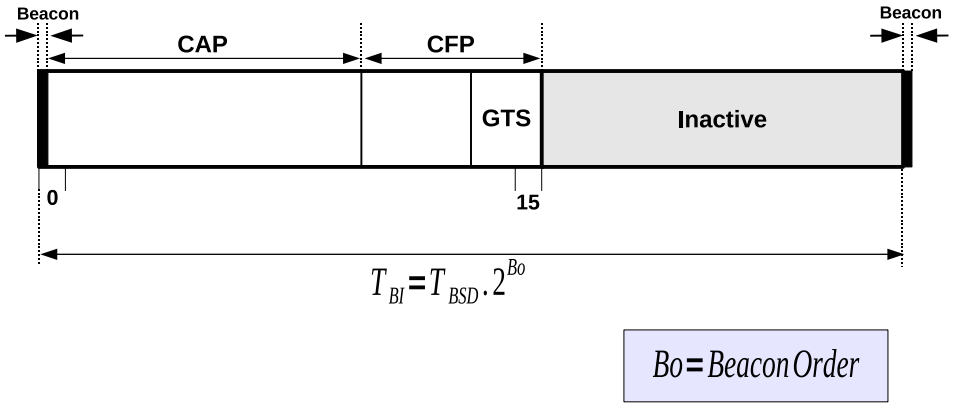

Fig. 3: Superframe Structure of IEEE 802.15.4 Beacon enabled mode

for accessing the medium. For this reason, a slotted version of CSMA/CA protocol must be used to access the medium within CAP [15]. Details of this protocol can be found in [15], [20]–[22].

On the other hand, when CFP exists, i.e., when a coordinator supports the allocation of reserved slots, these slots are called guaranteed time slots (GTS). The CFP always appears at the end of the CAP and each slot must be allocated previously to only one node. This allocation "guarantees" that the medium is free and the aforementioned node can transmit frames without using the CSMA/CA protocol. Furthermore, this feature is used to support the execution of the real time applications [3], [4]. However, the exclusive use of bandwidth reservation is not a complete solution to support the execution of protocols and applications with real-time restrictions.

The inactive period is used to allow all nodes to enter in sleep mode, or shutdown their transceiver, to reduce their energy consumption in a known time interval during each transmission cycle, denoted by superframe duration. The duration of a superframe is controlled by MAC attributes $macBeaconOrder$ (BO) and $macSuperFrameOrder$ (SO), where $0 \leq SO \leq BO \leq 14$. When SO and BO have the same value, the inactive period does not exist, i.e., there is no period that devices may enter in low-power state. The standard values were used in our analyses and are summarized in Tables I and II.

V. IEEE 802.15.4 Service Interface

The standard IEEE 802.15.4 MAC service interface defines two types of service for the transmission of MAC data and control frame. The set of general equations describing frame transmission times is defined next. Equations 1 and 2 are used for unreliable (non acknowledged) frame transmission, and equations 3 and 4 for reliable (acknowledged) frame transmission.

$$\mathcal{T}^{bc}_{MAC}(type) = \mathcal{T}_{backoff} + \mathcal{T}^{bc}_{MAC-type} \quad (1)$$

$$\mathcal{T}^{wc}_{MAC}(type) = \sum_{j=1}^{maxBackoff} \left\{\mathcal{T}_{backoff}.(2^{BE}+1)\right\} + \mathcal{T}^{wc}_{MAC-type} \quad (2)$$

$$\mathcal{T}^{bc}_{MAC\_ack}(type) = \mathcal{T}^{bc}_{MAC}(type) + \mathcal{T}^{bc}_{ackDelay} + \mathcal{T}_{ack} \quad (3)$$

$$\mathcal{T}^{wc}_{MAC\_ack}(type) = \sum_{j=0}^{maxRetries} \mathcal{T}^{wc}_{MAC}(type) + \mathcal{T}^{wc}_{ackDelay} + \mathcal{T}_{ack} \quad (4)$$

IEEE 802.15.4 Name	Abbr.	Range	Default Value
macBeaconOrder	*BO*	0 - 15	8
macSuperframeOrder	*SO*	0 - 15	5
macMinBE	*minBE*	0 - maxBE	3
macMaxBE	*maxBE*	3 - 8	5
macMaxCSMABackoffs	*maxBackoff*	0 - 5	4
macMaxFrameRetries	*maxRetries*	0 - 7	3
macResponseWaitTime	*nrWait*	2 - 64	32
aMaxLostBeacons	$nrLost$	-	4
aNumSuperframeSlots	$nrSlots$	-	16

TABLE I: Relevant integer parameters of the IEEE 802.15.4 standard

IEEE 802.15.4 Name	Identifier	Value (symbol times)
aBaseSlotDuration	$\mathcal{T}_{base}$	60
aBaseSuperframeDuration	$\mathcal{T}_{BSD}$	960
aMinCAPLength	$\mathcal{T}_{minCAP}$	440
aUnitBackoffPeriod	$\mathcal{T}_{backoff}$	20
aTurnaroundTime	$\mathcal{T}_{xvrcmd}$	12

TABLE II: Relevant time-related constants of the IEEE 802.15.4 standard

where, BE is the backoff exponent that defines the length of the CSMA/CA contention window, being $minBE \leq BE < maxBE$ (Table I); $\mathcal{T}^{bc}_{ackDelay} = \mathcal{T}_{xvrcmd}$ and $\mathcal{T}^{wc}_{ackDelay} = \mathcal{T}_{xvrcmd} + \mathcal{T}_{backoff} + \mathcal{T}_{freq}$ are the times to wait the acknowledgment in reliable transmissions. $\mathcal{T}_{freq}$ depends of technology and to simplify we will consider an upper bound $\mathcal{T}_{freq} = 100$ symbols. The reference $type$ in equations (1) to (4) identifies one specific type of MAC frames. The superscripts ^{bc} and ^{wc} used in equations 1 to 4 specify the best and worst case MAC frame transmission times, respectively.

VI. Network inaccessibility in IEEE 802.15.4

This section presents an exhaustive study of network inaccessibility in IEEE 802.15.4 wireless networks. A comprehensive set of scenarios leading to network inaccessibility is thoroughly discussed. For many of them we start with very simple situations that then evolve to less restrictive, and thus more general, operating conditions/fault assumptions. For most of the cases, we explicitly derive best and worst case figures, that we will signal with superscripts ^{bc} and ^{wc}, respectively.

A. Single Beacon Frame Loss

Let us start our analysis considering that a subset of nodes (may have a single element) in a wireless network segment does not track beacon frames. If a node in this set needs to transmit a frame, it should enable the radio transceiver (receive mode) and start a wait and network synchronization period of at most $\mathcal{T}_{BSD} \ . \ (2^{BO} + 1)$ symbols. If the beacon frame is received

[1]The worst case duration, for the wait of an acknowledgement frame, follows the IEEE 802.15.4 standard specification [15].

Frame type	Symbol	Length (bit)	Duration (ms)
Data frames			
Data (Minimum payload)	$\mathcal{T}_{data}^{bc}$	8	0.03
Data (Maximum payload)	$\mathcal{T}_{data}^{wc}$	1016	4.07
Data request	$\mathcal{T}_{Ext\_R}$	320	1.28
Data acknowledgment[1]	$\mathcal{T}_{ack}$	40	1.00
MAC control frames			
Beacon	$\mathcal{T}_{Beacon}$	1016	4.07
Beacon request	$\mathcal{T}_{Beacon\_R}$	64	0.26
Network ID conflict notification	$\mathcal{T}_{Conflict}$	304	1.22
Orphan notification	$\mathcal{T}_{Orphan}$	128	0.52
Realign	$\mathcal{T}_{Realign}$	280	1.12
Association request	$\mathcal{T}_{Assoc\_R}$	312	1.25
GTS request	$\mathcal{T}_{GTS\_R}$	72	0.29
Control request	$\mathcal{T}_{Ext\_R}$	320	1.28
MAC frame acknowledgment[1]	$\mathcal{T}_{ack}$	40	1.00

TABLE III: IEEE 802.15.4 frame durations, using the $2.4\,GHz$ frequency band

before the end of this search period, the frame shall be transmitted in the appropriate portion of the superframe. No network inaccessibility event exists. Otherwise, the operation of the MAC protocol is disturbed by the lack of beacon frame synchronization and the network is inaccessible, as described by equation:

$$\mathcal{T}_{ina\leftarrow sbfl}^{wc} \;=\; \mathcal{T}_{xvrcmd} \;+\; \mathcal{T}_{BSD} \,.\, (2^{BO} \;+\; 1) \tag{5}$$

Since $\mathcal{T}_{xvrcmd} \ll \mathcal{T}_{BSD}$, equation 5 can be simplified to equation 6, which represents the period of network inaccessibility upon the loss of a single beacon in a beacon enabled wireless network segment:

$$\mathcal{T}_{ina\leftarrow sbfl}^{wc} \;=\; \mathcal{T}_{BSD} \,.\, (2^{BO} \;+\; 1) \tag{6}$$

After the period of network inaccessibility, it is assumed a new instance of a beacon frame will be received and the node may proceed with the transmission of the frame using the unslotted version of the CSMA/CA algorithm. The entire period of network inaccessibility is *local* to the node.

B. Multiple Beacon Frame Loss

A beacon-enabled wireless network segment uses the superframe structure for controlling medium access. Under normal operation, a node must receive the beacon frame before it is allowed to transmit data. If some nodes in the wireless network segment do not receive the beacon frame, the network will be inaccessible for such nodes.

Based on the superframe structure of the last received beacon, the node can control the radio interface and track consecutive beacon transmissions. The tracking mechanism is also called beacon synchronization and allows all nodes to know the characteristics of the superframe structure (duration of active and inactive periods, number of allocated GTS slots, etc.).

For tracking a beacon frame, a node searches for beacons during at most $\mathcal{T}_{BSD} \, . \, (2^{BO}+1)$ symbol times. If a beacon frame with the current wireless network segment identifier is not received, this search is repeated from one to at most $nrLost \equiv aMaxLostBeacons$ times. The best and worst case network inaccessibility durations are obtained under the assumption that a beacon frame is successfully received right after the first and the last of the $nrLost$ wait periods. The corresponding periods of network inaccessibility are therefore given by equations 7 and 8, respectively.

$$\mathcal{T}^{bc}_{ina \leftarrow mbfl} = \mathcal{T}_{BSD} \, . \left(2^{BO} + 1\right) \tag{7}$$

$$\mathcal{T}^{wc}_{ina \leftarrow mbfl} = \mathcal{T}_{BSD} \, . \left(2^{BO} + 1\right) \, . \, nrLost \tag{8}$$

These periods of network inaccessibility may *locally* affect only a given set of nodes (this set may have a single element) or its effects may extend to all the nodes of the wireless network segment, but the wireless network segment coordinator.

C. Synchronization Loss

If the search for the beacon frame does not succeed in any of the $nrLost$ tries, a node loses synchronization with its coordinator, being obliged to signal a BEACON LOST event to high layer protocol management entities, such as the *Mediator Layer* management entities [23]. The corresponding period of network inaccessibility up to this point is simply given by:

$$\mathcal{T}_{ina \leftarrow nosync} = \mathcal{T}_{BSD} \, . \, \left(2^{BO} + 1\right) \, . \, nrLost \tag{9}$$

The BEACON LOST event is signaled upon exceeding the allowed maximum number of beacon frame losses, $aMaxLostBeacons \equiv nrLost$. This is in strict conformity with the standard specification and with our system model.

There are a number of causes for network inaccessibility due to loss of node synchronization: a burst of electromagnetic interference in the medium; disturbances in the node receiver circuitry; collisions derived from the presence of obstacles or influenced by the activity of hidden or mobile nodes; and glitches in the coordinator or even its failure. Based on the information it owns, the *Mediator Layer* management entities may take a decision on the appropriate recovery action.

This period of network inaccessibility may affect only a set of nodes or it may include all the nodes of the wireless network segment, but the wireless network segment coordinator.

D. Orphan Node

If the high layer protocol management entities (e.g., the *Mediator Layer*) decide that the device was orphaned, a request is issued to the MAC layer to start an *orphan scan* recovery action, over a specified set of logical channels.

For each logical channel: a MAC orphan notification command is sent; as reply, a MAC realignment command, from the previously associated coordinator, is awaited for during a given period. While the node does not receive the MAC realignment command, the network is inaccessible. Once such MAC command is received, the node terminates the scan and the network becomes accessible. The MAC realignment frame is transferred using the frame reliable unicast service. Thus, the worst case period of network inaccessibility is obtained assuming that the MAC realignment command is received only while scanning the last of the $nrchannels$ logical channels, being its upper bound given by equation 10.

$$\mathcal{T}^{wc}_{ina\leftarrow orphan} = \mathcal{T}_{ina\leftarrow nosync} + \mathcal{T}_{MLA}(Orphan) + \sum_{j=1}^{nrchannels} (\mathcal{T}^{wc}_{MAC}(Orphan) + nrWait \,.\, \mathcal{T}_{BSD}) + \mathcal{T}^{wc}_{MAC\_ack}(Realign) \tag{10}$$

where, $\mathcal{T}_{MLA}$ is the normalized (symbol) time taken in the *Mediator Layer* management actions. Should the orphan realignment succeed at the first attempt, the period of network inaccessibility will be simply given by equation 11.

$$\mathcal{T}^{bc}_{ina\leftarrow orphan} = \mathcal{T}_{ina\leftarrow nosync} + \mathcal{T}_{MLA}(Orphan) + \mathcal{T}^{bc}_{MAC}(Orphan) + \mathcal{T}_{MLA}(Realign) + \mathcal{T}^{bc}_{MAC\_ack}(Realign) \tag{11}$$

which assumes that $\mathcal{T}_{MLA}(Realign) < nrWait.\mathcal{T}_{BSD}$ represents the duration of the *Mediator Layer* management actions at the network coordinator, in response to the MAC orphan notification command. The whole period of network inaccessibility may affect only a single node, a given set of nodes or all the nodes of the wireless network segment, but the network coordinator. In the worst-case, all the N nodes of the wireless network segment, but the network coordinator may be inaccessible, as specified by equation 10, where the superscript ^{mn} signals that multiple nodes may be inaccessible:

$$\mathcal{T}^{wc-mn}_{ina\leftarrow orphan} = \mathcal{T}_{ina\leftarrow nosync} + \mathcal{T}_{MLA}(Orphan) + \sum_{j=1}^{nrchannels} (\mathcal{T}^{wc}_{MAC}(Orphan) + nrWait \,.\, \mathcal{T}_{BSD}) + (N-1) \,.\, \mathcal{T}^{wc}_{MAC\_ack}(Realign) \tag{12}$$

However, since MAC control frames are being exchanged between nodes, the time taken in those actions should be seen as a period of network inaccessibility by all the nodes in the wireless network segment. These *global* periods of network inaccessibility are upper and lower bounded by the duration of the events specified in equations 12 and 13, respectively.

$$\mathcal{T}^{bc}_{ina\leftarrow orphan(mac)} = \mathcal{T}^{bc}_{MAC}(Orphan) + \mathcal{T}^{bc}_{MAC\_ack}(Realign) \tag{13}$$

$$\mathcal{T}^{wc-mn}_{ina\leftarrow orphan(mac)} = (N-1) \,.\, [\sum_{j=1}^{nrchannels} (\mathcal{T}^{wc}_{MAC}(Orphan)) + \mathcal{T}^{wc}_{MAC\_ack}(Realign)] \tag{14}$$

where, N is the number of nodes in the wireless network segment. Equation 13 assumes that a single node has been declared as an orphan, while equation 14 is derived assuming that all the nodes, but the network coordinator, have entered into the orphan state. Equations 13 and 14 do not account for local actions, such as the event detection latencies, frame waiting periods and processing overheads, included in equations 10 to 12.

E. Coordinating Orphan Realignment

At the coordinator the need to assist MAC layer management actions starts when a MAC orphan notification command is received. Upon processing by *Mediator Layer* management entities, the reliable unicast, i.e., the acknowledged transmission of a MAC realignment command, is requested. The time taken in these actions is seen as network inaccessibility by the wireless network segment coordinator. The best and worst periods of network inaccessibility concerning the interaction with a single orphan node are given by equations 15 and 16, respectively.

$$\mathcal{T}^{bc}_{ina \leftarrow realign} = \mathcal{T}_{MLA}(Realign) + \mathcal{T}^{bc}_{MAC\_ack}(Realign) \quad (15)$$

$$\mathcal{T}^{wc-sn}_{ina \leftarrow realign} = \mathcal{T}_{MLA}(Realign) + \mathcal{T}^{wc}_{MAC\_ack}(Realign) \quad (16)$$

On the other hand, if the operation of the network is disturbed in such a way that all the nodes of the wireless network segment, but the wireless network segment coordinator, enter into the orphan state, the corresponding worst case period of network inaccessibility is given by equation 17.

$$\mathcal{T}^{wc-mn}_{ina \leftarrow realign} = \mathcal{T}_{MLA}(Realign) + (N-1) \,.\, \mathcal{T}^{wc}_{MAC\_ack}(Realign) \quad (17)$$

where, it is assumed that the processing of the different MAC orphan notifications by the *Mediator Layer* management entities mostly proceeds in parallel with the transmission of MAC coordinator realignment frames. All these operations may heavily disturb the superframe structure and the corresponding network operation cycle and may even introduce a significant jitter in the forthcoming beacon frame transmissions. Therefore, this period of network inaccessibility should be seen as *global*, i.e. affecting all network nodes.

F. Coordinator Conflict Detection

In general, there is the possibility that two different potential coordinators may render the same wireless network identifier, within the same wireless network segment broadcast domain. A similar scenario may also result from node mobility, when a moving node and potential coordinator enters into the broadcast domain of a functioning coordinator. In any of these scenarios, one have a situation called *coordinator conflict*, which can either be detected by the wireless network segment coordinator or by its directly associated nodes.

There are two forms to be aware of a coordinator conflict: a beacon frame with the same wireless network identifier is received from different coordinators within the same wireless network segment broadcast domain; a coordinator receives a wireless network identifier conflict notification from a node. The former is a local event and does not directly generate a network inaccessibility incident.

The latter involves the reliable unicast of a MAC Coordinator wireless network identifier Conflict notification frame, which may individually lead to a period of network inaccessibility, bounded in the best and worst case by equations 18 and 19, respectively.

$$\mathcal{T}^{bc}_{ina\leftarrow C\_Detection} = \mathcal{T}^{bc}_{MAC\_ack}(C\_Conflict) \quad (18)$$

$$\mathcal{T}^{wc-sn}_{ina\leftarrow C\_Detection} = \mathcal{T}^{wc}_{MAC\_ack}(C\_Conflict) \quad (19)$$

These periods of network inaccessibility should be seen as *global* by all the nodes of the wireless network segment broadcast domain, since it implies the transaction of MAC control frames. In a best case scenario the coordinator conflict will be detected by a single node and only one MAC notification is sent in the wireless network segment, as specified by equations 18 and 19. In the worst case, the conflict will be detected and signalled by all the wireless network segment nodes, but the wireless network segment coordinator, and the corresponding period of network inaccessibility is upper bounded by equation 20.

$$\mathcal{T}^{wc}_{ina\leftarrow C\_Detection} = (N-1)\,.\,\mathcal{T}^{wc}_{MAC\_ack}(C\_Conflict) \quad (20)$$

G. Coordinator Conflict Resolution

A wireless network segment coordinator must signal a COORDINATOR ID CONFLICT to *Mediator Layer* management entities, which in turn will request the MAC layer to perform an active scan. This scan is realized in all currently used logical channels. Scanning each channel involves the transmission of a MAC beacon request command and wait for replies (beacon frames), during a given period.

The identifiers recorded from the received beacons can be issued to the *Mediator Layer* management entities all at once, as specified in equation 21, or each time a beacon frame is received, as drawn in equation 22. During all this process, the network is inaccessible. The best and worst case periods of network inaccessibility are given by equations 21 and 22, respectively.

$$\mathcal{T}^{bc}_{ina\leftarrow C\_Resolution} = \mathcal{T}_{MLA}(C\_Conflict) + \mathcal{T}^{bc}_{MAC}(Beacon\_R) + nrWait.\mathcal{T}_{BSD} + \mathcal{T}_{MLA}(Realign) + \mathcal{T}^{bc}_{MAC}(Realign) \quad (21)$$

$$\mathcal{T}^{wc}_{ina\leftarrow C\_Resolution} = \mathcal{T}_{MLA}(Conflict) + \sum_{j=1}^{nrchannels}[\,\mathcal{T}^{wc}_{MAC}(Beacon\_R) + nrWait.\mathcal{T}_{BSD}\,] + \mathcal{T}_{MLA}(Realign) + \mathcal{T}^{wc}_{MAC}(Realign) \quad (22)$$

If, at the end of the search, the network coordinator does not find a beacon frame with its own identifier, no further action is taken and the network becomes accessible again. Otherwise, a new identifier is selected and, if necessary, a MAC coordinator realignment command is broadcast. Since all these events are originated at the network coordinator, they should be regarded as *global*, i.e., observed by all the nodes in the wireless network segment. If the network coordinator selects a new identifier, some nodes may not be synchronized with the "new" superframe structure, which may induce a loss of synchronization, as explained in Section VI-C.

H. Extract Request

There are two ways to transmit data between a node and a coordinator: the direct and indirect transmission. In the direct transmission, the coordinator sends a data to a node directly, i.e., the coordinator access the medium an send a data frame using a slotted version of CSMA/CA algorithm. Otherwise, in the indirect transmission the coordinator stores the data in a queue and waits the reception of a command that requests the extraction of this data. In this case, the node sends a command to extract data of the coordinator and waits for the reception of an acknowledgement. The node repeat this operation until $maxRetries$ times.

Thus, while the node does not receive the acknowledgement frame the network is inaccessible to it. Additionally, if the node receives an acknowledgement from the coordinator, this node enables its transceiver in receive mode during $\mathcal{T}_{wait}$ and the network may continue inaccessible within this period. The best and worst case network inaccessibility durations are therefore given by equations 23 and 24, respectively.

$$\mathcal{T}^{bc}_{ina\leftarrow extReq} = \mathcal{T}^{bc}_{MAC_{ack}}(ExtReq) \tag{23}$$

$$\mathcal{T}^{wc}_{ina\leftarrow extReq} = \mathcal{T}^{wc}_{MAC_{ack}}(ExtReq) + \mathcal{T}_{wait} \tag{24}$$

where, $\mathcal{T}_{wait}$ is the period, addressed by the attribute $macMaxFrameTotalWaitTime$, that is dependent upon a combination of physical and MAC attributes and constants, being defined in the IEEE 802.15.4 standard [15].

I. Association

The association procedure starts with an active scan in each logical channel available. The active scan involves the send of a MAC beacon request command, for each available logical channel, and the wait for replies (beacon frames), during a given period. After processing the beacon frames, the *Mediator Layer* management entities select a wireless network segment, send an Association Request command, and wait for a confirmation (acknowledgement). However, the association procedure is only done after to extract the information about this association using the indirect transmission method (see subsection VI-H). The best and worst periods of network inaccessibility are given by equations 25 and 26, respectively.

$$\begin{aligned}\mathcal{T}^{bc}_{ina\leftarrow assoc} = {} & \mathcal{T}^{bc}_{MAC}(Beacon\_R) + nrWait.\mathcal{T}_{BSD} + \mathcal{T}_{MLA}(Beacon) + \\ & \mathcal{T}^{bc}_{ina\leftarrow extReq} + \mathcal{T}_{MLA}(AssocReq) + \mathcal{T}^{bc}_{MAC\_ack}(AssocReq)\end{aligned} \tag{25}$$

$$\begin{aligned}\mathcal{T}^{wc}_{ina\leftarrow assoc} = \sum_{j=1}^{nrchannels} & [\mathcal{T}^{wc}_{MAC}(Beacon\_R) + nrWait.\mathcal{T}_{BSD}] + \mathcal{T}_{MLA}(Beacon) + \\ & \mathcal{T}^{wc}_{ina\leftarrow extReq} + \mathcal{T}_{MLA}(AssocReq) + \mathcal{T}^{wc}_{MAC\_ack}(AssocReq)\end{aligned} \tag{26}$$

J. Re-Association

After a synchronization loss, the *Mediator Layer* management entities should decide whether: to consider that the device is orphan; or that an association procedure will be realized again. In case of re-association, a MAC layer should perform a reset operation before beginning the association

procedure. The best and worst network inaccessibility times are given by equations 27 and 28, respectively.

$$\mathcal{T}^{bc}_{ina\leftarrow reAssoc} = \mathcal{T}_{ina\leftarrow nosync} + \mathcal{T}^{bc}_{ina\leftarrow assoc} \tag{27}$$

$$\mathcal{T}^{wc}_{ina\leftarrow reAssoc} = \mathcal{T}_{ina\leftarrow nosync} + \mathcal{T}^{wc}_{ina\leftarrow assoc} \tag{28}$$

K. GTS request

The allocation of a GTS slot is performed using the reliable unicast service to send a MAC GTS request command to the associated coordinator. During this period, the network is seen as inaccessible. The best and worst periods of network inaccessibility are given by equations 29 and 30, respectively.

$$\mathcal{T}^{bc}_{ina\leftarrow GTS} = \mathcal{T}^{bc}_{MAC\_ack}(GTS) \tag{29}$$

$$\mathcal{T}^{wc}_{ina\leftarrow GTS} = \mathcal{T}^{wc}_{MAC\_ack}(GTS) \tag{30}$$

These periods of network inaccessibility are seen as *global* by all the nodes of the wireless network segment. This scenario is extremely important because GTS slots can be used for bandwidth reservation. Several solutions advanced in the literature try to solve the problem of real-time communications, over the IEEE 802.15.4 standard, using GTS allocation mechanisms [3]–[5], [24]. The effectiveness of such solutions should be re-analysed under the scope of a comprehensive network inaccessibility model.

VII. Results: network inaccessibility duration in beacon enabled networks

The characterization of network inaccessibility presented in Section VI allows us to extract some useful information regarding to the temporal behavior of an IEEE 8022.15.4 wireless network. The default values of the IEEE 802.15.4 standard summarized in Tables I and II were utilized for the parameters and constants present in our network inaccessibility characterization. We establish an uniform duration for the management actions, represented by the $\mathcal{T}_{MLA}$ term, which is $\frac{1}{10}$ of the beacon interval, i.e., $\frac{2^{BO}.\mathcal{T}_{BSD}}{10}$. To be able to reproduce all the values obtained by our analysis, Table IV also presents the number of channels ($nrChannels$ parameter) for each frequency band supported by the IEEE 802.15.4 standard. The value of each parameter that is represented in symbols can be converted in bits utilizing Table V, which presents the numbers of symbols per octet in all modulation technique and frequency band.

Frequency Band	**Number of channels**
868-868.6 MHz	1
902-928 MHz	10
2400-2483.5 MHz	16

TABLE IV: Number of channels per frequency band supported by the IEEE 802.15.4 standard

Modulation Technique	Frequency Band		
	868 MHz $(symbols/octet)$	**915 MHz** $(symbols/octet)$	**2400 MHz** $(symbols/octet)$
BPSK	8	8	—
ASK	0.4	1.6	—
O-QPSK	2	2	2

TABLE V: The number of symbols per octet in each modulation technique and frequency band

The impact of the network inaccessibility scenarios in the network temporal behavior is presented within Tables VI to VIII, which groups all frequency bands supported by the IEEE 802.15.4 standard. The results inscribed in these tables show that the periods of network inaccessibility are extremely high, precluding any claim of obtaining a real-time behavior from the network, even if some specifically designed mechanisms are in place, since network inaccessibility incidents may always occur.

With the default network configuration of Table I, the worst case period of network inaccessibility is up to seven times higher than the beacon interval. Figure 4 presents this comparison. However, it should be noted that the beacon interval is in the order of the seconds, a very high value to meet the requirements of most hard real-time applications. If the beacon interval is reduced, the gap between normal network access times and the periods of network inaccessibility may become even higher and the overall system predictability, timeliness and dependability properties may be at risk.

Defining methods and reducing the duration of the periods of network inaccessibility in IEEE 802.15.4 wireless network is of crucial importance for achieving real-time operation. This study is a first but fundamental step towards that direction.

PHY (868-868.6 MHz)						
Scenario	**Modulation Technique**					
	BPSK - $20\,kb/s$		*ASK* - $250\,kb/s$		*O-QPSK* - $100\,kb/s$	
	best case (ms)	**worst case** (ms)	**bc** (ms)	**wc** (ms)	**bc** (ms)	**wc** (ms)
$\mathcal{T}_{ina \leftarrow sbfl}$	——	12337	——	19739	——	9870
$\mathcal{T}_{ina \leftarrow mbfl}$	12337	49345	19739	78952	9870	39476
$\mathcal{T}_{ina \leftarrow nosync}$	49345	49345	78952	78952	39476	39476
$\mathcal{T}_{ina \leftarrow orphan}$	51834	52851	82896	84441	41452	42233
$\mathcal{T}_{ina \leftarrow realign}$	1250	1833	1974	2824	990	1423
$\mathcal{T}_{ina \leftarrow C\_Detection}$	20	609	8	858	7	441
$\mathcal{T}_{ina \leftarrow C\_Resolution}$	2772	2900	4428	4632	2215	2317
$\mathcal{T}_{ina \leftarrow extReq}$	13	612	6	858	5	442
$\mathcal{T}_{ina \leftarrow assoc}$	4032	5351	6407	8313	3208	4182
$\mathcal{T}_{ina \leftarrow reAssoc}$	53377	54695	85358	87265	42684	43658
$\mathcal{T}_{ina \leftarrow GTS}$	13	557	6	845	4	428

TABLE VI: The best and worst cases for $868MHz$ frequency band

PHY (902-928 MHz)						
Scenario	**Modulation Technique**					
	BPSK - $40\,kb/s$		*ASK* - $250\,kb/s$		*O-QPSK* - $250\,kb/s$	
	best case (ms)	**worst case** (ms)	**bc** (ms)	**wc** (ms)	**bc** (ms)	**wc** (ms)
$\mathcal{T}_{ina \leftarrow sbfl}$	——	6169	——	19739	——	3948
$\mathcal{T}_{ina \leftarrow mbfl}$	6139	24673	19739	78952	3948	15791
$\mathcal{T}_{ina \leftarrow nosync}$	——	24673	——	78952	——	15791
$\mathcal{T}_{ina \leftarrow orphan}$	25917	33958	82896	108427	16581	21696
$\mathcal{T}_{ina \leftarrow realign}$	625	917	1974	2823	396	570
$\mathcal{T}_{ina \leftarrow C\_Detection}$	10	305	8	857	3	177
$\mathcal{T}_{ina \leftarrow C\_Resolution}$	1386	8968	4428	28616	886	5727
$\mathcal{T}_{ina \leftarrow extReq}$	7	306	5	858	2	177
$\mathcal{T}_{ina \leftarrow assoc}$	2016	10193	6406	32296	1284	6473
$\mathcal{T}_{ina \leftarrow reAssoc}$	26689	34865	85358	111248	17074	22264
$\mathcal{T}_{ina \leftarrow GTS}$	7	279	5	845	2	171

TABLE VII: The best and worst cases for $915MHz$ frequency band

PHY (2400-2483.5 MHz)		
Scenario	**Modulation Technique**	
	O-QPSK - $250\,kb/s$	
	best case (ms)	**worst case** (ms)
$\mathcal{T}_{ina \leftarrow sbfl}$	——	3948
$\mathcal{T}_{ina \leftarrow mbfl}$	3948	15791
$\mathcal{T}_{ina \leftarrow nosync}$	——	15791
$\mathcal{T}_{ina \leftarrow orphan}$	16581	24897
$\mathcal{T}_{ina \leftarrow realign}$	396	570
$\mathcal{T}_{ina \leftarrow C\_Detection}$	3	177
$\mathcal{T}_{ina \leftarrow C\_Resolution}$	886	8927
$\mathcal{T}_{ina \leftarrow extReq}$	2	177
$\mathcal{T}_{ina \leftarrow assoc}$	890	9280
$\mathcal{T}_{ina \leftarrow reAssoc}$	16681	25070
$\mathcal{T}_{ina \leftarrow GTS}$	2	171

TABLE VIII: The best and worst cases for $2.4GHz$ frequency band

VIII. Conclusion

This report presented the characterization of network inaccessibility in the IEEE 802.15.4 networks. The existence and duration of network inaccessibility are still neglected by existent temporal characterization of wireless communications. Network inaccessibility has a strong negative impact in the temporal behavior of IEEE 802.15.4 networks, being extremely important its characterization. In that way, future work directions will focus on providing means to reduce the periods of network inaccessibility; to provide support to signal the periods of network inaccessibility for higher layers, improving the means of analyzing network delays and message schedulability over wireless networked communications.

References

[1] A. Sahoo and P. Baronia, "An energy efficient MAC in wireless sensor networks to provide delay guarantee," in *15th IEEE Workshop on Local Metropolitan Area Networks (LANMAN)*, June 2007, pp. 25 –30.

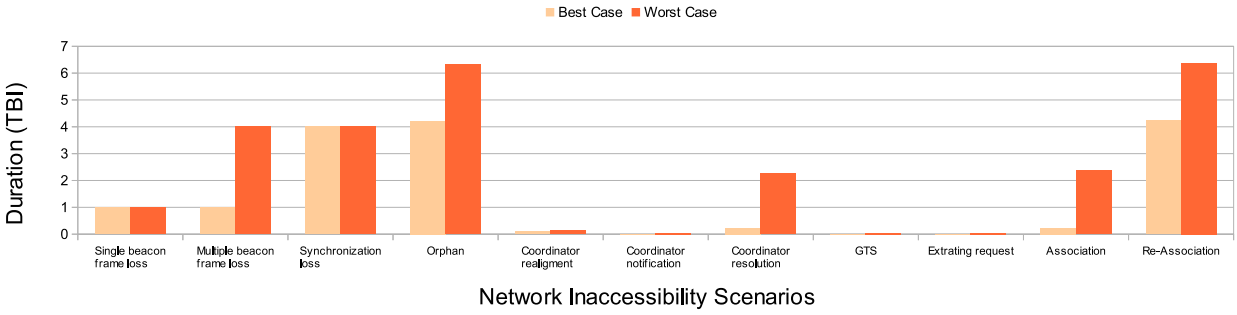

Fig. 4: Network inaccessibility scenarios for the $2.4GHz$ frequency band, normalized by the beacon interval duration, $\mathcal{T}_{BI} = 3932ms$ and $BO = 8$

[2] E. Egea-López, J. Vales-Alonso, A. S. Martínez-Sala, J. García-Haro, P. Pavón-Mariño, and M. V. Bueno Delgado, "A wireless sensor networks MAC protocol for real-time applications," *Personal Ubiquitous Computing*, vol. 12, pp. 111–122, January 2008.

[3] 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 International Conference on Emerging Technologies and Factory Automation (ETFA)*, September 2008, pp. 1016 –1022.

[4] Y.-K. Huang, A.-C. Pang, and H.-N. Hung, "An adaptive GTS allocation scheme for IEEE 802.15.4," *IEEE Transactions on Parallel and Distributed Systems*, vol. 19, no. 5, May 2008.

[5] J. Chen, L. Ferreira, and E. Tovar, "An explicit GTS allocation algorithm for IEEE 802.15.4," in *16th IEEE Conference on Emerging Technologies and Factory Automation (ETFA)*, September 2011, pp. 1 –8.

[6] M.-G. Park, K.-W. Kim, and C.-G. Lee, "Holistic optimization of real-time IEEE 802.15.4/zigbee networks," in *IEEE International Conference on Advanced Information Networking and Applications (AINA)*, March 2011, pp. 443 –450.

[7] P. Veríssimo, L. Rodrigues, and M. Baptista, "AMp: A Highly Parallel Atomic Multicast Protocol," *SIGCOMM Comput. Commun. Rev.*, vol. 19, no. 4, pp. 83–93, September 1989.

[8] P. Veríssimo and J. A. Marques, "Reliable broadcast for fault-tolerance on local computer networks," in *In Proceedings of the Ninth Symposium on Reliable Distributed Systems*. Alabama, USA: IEEE, October 1990, pp. 24–90.

[9] P. Veríssimo, J. Rufino, and L. Rodrigues, "Enforcing Real-Time Behaviour on LAN-Based Protocols," in *10th IFAC Workshop on Distributed Computer Control Systems*, September 1991.

[10] J. Rufino, C. Almeida, P. Veríssimo, , and G. Arroz, "Enforcing dependability and timeliness in controller area networks." in *Proc. of the 32nd Annual Conf. of the IEEE Ind. Electronics Society (IECON)*, Paris, France, November 2006.

[11] J. L. R. Souza and J. Rufino, "Building Fundamental Properties For Real-Time Wireless Sensor Networks," AIR-II Technical Report RT-10-01, Tech. Rep., 2010.

[12] O. Babaoğlu and R. Drummond, "Streets of Byzantium: Network Architectures for Fast Reliable Broadcasts," *IEEE Trans. on Soft. Engineering*, vol. SE-11, no. 6, June 1985.

[13] T. Fujiwara, T. Kasami, A. Kitai, and S. Lin, "On the undetected error probability for shortened hamming codes," *IEEE Trans. on Comm.*, vol. 33, no. 6, June 1985.

[14] D. Eckhardt and P. Steenkiste, "Measurement and analysis of the error characteristics of an in-building wireless network," in *SIGCOMM '96: Conf. Proc. on Applications, Tech., Arch. and Protocols for Computer Comm.*, New York, NY, USA, August 1996.

[15] 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," IEEE P802.15 Working Group, 2011, Revision of IEEE Standard 802.15.4-2006.

[16] M. Petrova, J. Riihijarvi, P. Mahonen, and S. Labella, "Performance study of IEEE 802.15.4 using measurements and simulations," in *Proceedings of the Wireless Communications and Networking Conference (WCNC 2006)*. Las Vegas, USA: IEEE, April 2006, pp. 487 – 492.

[17] J. L. R. Souza and J. Rufino, "Characterization of inaccessibility in wireless networks-a case study on IEEE 802.15.4 standard," in *3th IFIP International Embedded Systems Symposium(IESS)*, ser. IFIP Advances in Information and Communication Technology, vol. 310, Langenargen, Germany, September 2009.

[18] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE Network*, vol. 20, no. 3, pp. 41–47, May 2006.

[19] S. Khattab, D. Mosse, and R. Melhem, "Modeling of the channel-hopping anti-jamming defense in multi-radio wireless networks," in *5th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services (MobiQuitous)*. Dublin, Ireland: ACM, July 2008.

[20] I. Ramachandran, A. K. Das, and S. Roy, "Analysis of the contention access period of IEEE 802.15.4 MAC," *ACM Transactions on Sensor Networks*, vol. 3, March 2007. [Online]. Available: http://doi.acm.org/10.1145/1210669.1210673

[21] J. He, Z. Tang, H.-H. Chen, and Q. Zhang, "An accurate and scalable analytical model for IEEE 802.15.4 slotted CSMA/CA networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 1, pp. 440–448, January 2009.

[22] C. Jung, H. Hwang, D. Sung, and G. Hwang, "Enhanced markov chain model and throughput analysis of the slotted CSMA/CA for IEEE 802.15.4 under unsaturated traffic conditions," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 1, January 2009.

[23] J. L. R. Souza and J. Rufino, "An approach to enhance the timeliness of wireless communications," in *The Fifth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM)*, Lisbon, November 2011.

[24] 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*, vol. 39, no. 1-3, pp. 169–204, August 2008.