Characterization of Inaccessibility in Wireless Networks: A Case Study on IEEE 802.15.4 Standard *

Jeferson L. R. Souza and José Rufino

University of Lisboa, LaSIGE
jsouza@lasige.di.fc.ul.pt, ruf@di.fc.ul.pt

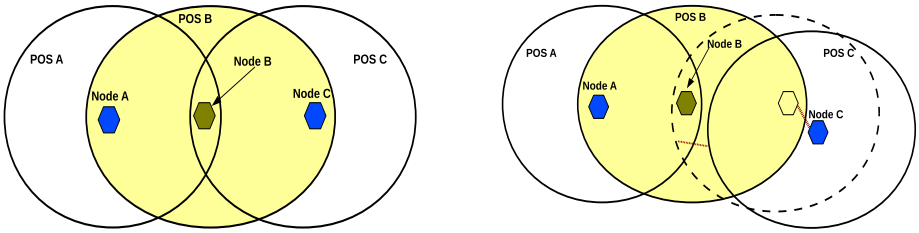
Abstract. Wireless technology has been seen as the communication technology of the future. One of many challenges is the support for predictability and time-bounded communications over this technology. In this way, the control of temporary partitions, called inaccessibility, is of fundamental importance. For this reason, this paper makes a characterization of inaccessibility in wireless networks and describes an exhaustive study about it on IEEE 802.15.4 wireless standard. The knowledge of inaccessibility incidents and their duration is a first step to define means to control network partitioning and therefore to form a basis for supporting real-time communications over wireless technology.

1 Introduction

Industrial and aerospace applications has seen wireless technology as the network infrastructure of the future. The advantages of this technology are the mobility, and mainly the elimination of cables for communication among devices. For example, wireless technologies are seen as relevant communication infrastructure in many kinds of spacecrafts: satellites, and orbital vehicles, with respect to cabling issues; robotic vehicles for planetary exploration. Both applications have real-time constrains and need guarantees about transmission time bounds. The study of the provision of these guarantees in wireless technologies involves the analysis of low-level protocol components and of high-level software layers, present in the wireless network model, and involved in the communication process.

Different characteristics of wireless networks, e.g., bounded delay to transmission of a frame, to handling of omission faults and control of partitions in the network, must be addressed to support real-time communication. In this way, this paper presents a exhaustive study about temporary partitions in IEEE 802.15.4 standard. These partitions are called inaccessibility [1, 2] and this study is important to define means to control inaccessibility in IEEE 802.15.4 networks.

* Faculdade de Ciências da Universidade de Lisboa, Bloco C6, Piso III, Campo Grande, 1749–016 Lisboa, Portugal. This work was partially motivated by our work within the scope of the ESA (European Space Agency) Innovation Triangular Initiative program, through ESTEC Project AIR-II (ARINC 653 in Space — Industrial Initiative), URL: http://air.di.fc.ul.pt). This work was partially supported by FCT through the Multiannual Funding and the CMU-Portugal Programs and the Individual Doctoral Grant SFRH/BD/45270/2008.



(a) Hidden Terminal Problem (b) Node Mobility problem

Fig. 1: Some problems in Wireless networks

A similar study was made successfully for other wired network technologies such as CAN [3, 4], and Token-Bus [5], demonstrating the importance of the study for the support of real-time communication in wired networks. On a similar manner, the control of inaccessibility is one of some desired properties to achieve real-time communication in wireless networks.

The control of timeliness and predictability in input/output operations (wireless network interfaces included) is a fundamental condition in partitioned architectures, such as those we are addressing within the scope of AIR technology [6].

This paper is organized as follows: Section 2 presents the main concept of inaccessibility, explaining the observation of this concept in wireless networks. Section 3 presents an overview of IEEE 802.15.4 standard. Section 4 describes the study of inaccessibility in 802.15.4 networks and shows its impact in the network temporal behavior. Section 5 presents some related works. Finally, section 6 draws some conclusions.

2 What is Inaccessibility ?

Disturbances induced in the operation of medium access control (MAC) protocols may create temporary partitions in the network, derived of the time required to detect and recover from these situations. These disturbances can be produced by external interferences or by some glitches in the operation of the MAC sublayer. A solution for controlling these partitions for LAN-based networks was presented in [7]. These temporary network partitions are called inaccessibility [1, 2] and the definition of this concept 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* ***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.*

The same kind of problems present in wired networks also are present in wireless networks. However, while LAN-based networks may offer additional facilities to allow the transmitter to detect a problem (e.g. collision detection), in wireless networks these mechanisms do not exist in general. For example, in wireless networks, the transceiver of each node cannot receive and transmit data simultaneously. Consequently, the algorithms used in the MAC sublayer do not have means to detect a collision without the support of timeout-based mechanisms, or additional control channels.

These problems may be originated externally or derived of the proximity and position of a node, in relation to operating space of other nodes. The circles in figure 1(a) show the transmission and interference range of three different nodes. In the example presented in figure 1, the node A may overlap, total or partial, the frame transmission of node B and vice-verse. It may result in periods of inaccessibility for the two nodes. The RTS/CTS handshake used in IEEE 802.11 tries to solve the hidden node problem. However, this technique does not solve completely the problem and increase the overhead of a transmission, an unacceptable condition, for example, for wireless sensor networks [8].

The node mobility, provided by wireless technology, allows the change of a node location easily. This mobility may cause connection loss between nodes. Figure 1(b) shows that, after moves, node C is outside of node B Personal Operating Space (POS) and it may cause periods of inaccessibility in both nodes. An environment with a high level of node mobility may cause the occurrence of various periods of inaccessibility if the nodes will move their position to outside range of each other constantly.

The inaccessibility times, in both cases, are the time a node needs to reestablish normal operation of the MAC protocol. The knowledge of inaccessibility time bounds is important to achieve the support of real-time communication over the wireless networks.

This paper presents a study of the IEEE 802.15.4 standard concerning the evaluation of inaccessibility and its impact in a wireless network. For completeness, the next section presents an overview of this standard.

3 IEEE 802.15.4 - Overview

The IEEE 802.15.4 standard [9] was designed for Low-Rate Wireless Personal Area Networks (LR-WPANs). These networks were designed for being used with limited power processor and battery life devices, have a low-cost, very low-power, and consequently short-range wireless communication [10]. A Personal Area Network (PAN) is focused in a personal operating space (POS), i.e., the space around the person or object with some ten meters of radius.

The IEEE 802.15.4 standard defines two operation modes for PAN: beacon-enabled and nonbeacon-enabled. The CSMA/CA [9] protocol can be used, within both modes, to access the medium. Beacon-enabled PAN uses a special structure to control the medium access called superframe structure (cf. figure 2). This structure is time bounded by periodic transmissions of special frames called

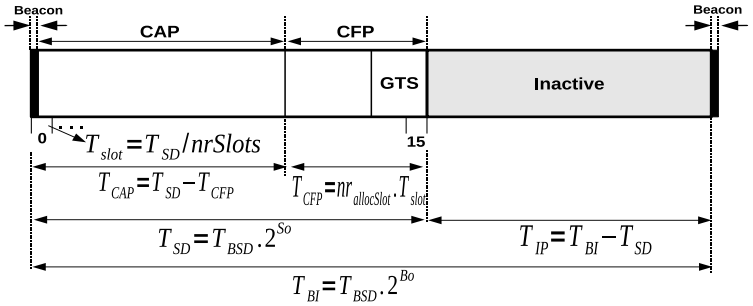


Fig. 2: Superframe Structure

beacon frames. This periodicity is called Beacon Interval (BI) and it is drawn in figure 2.

In this paper, the analyses of the network inaccessibility are focused in a beacon-enabled PAN. The exhaustive study of inaccessibility periods based on IEEE 802.15.4 standard is presented. This study shows the best (^{bc}) and worst (^{wc}) case inaccessibility time bounds in a set of relevant scenarios.

4 Inaccessibility in IEEE 802.15.4

The IEEE 802.15.4 standard has been viewed as a potential technology by industrial, vehicular and aerospace applications. These applications have necessity of real-time communications, i.e., the temporal behavior must be well-defined and the communication infrastructure strongly reliable. One of many challenges of the study of hardware and software components, used within wireless networks, is to define a solution for reliable and real-time communication over this type of networks. The study of inaccessibility is one step in that direction.

The study present in this paper is focused in beacon-enabled PAN that use the superframe structure (Figure 2) to control medium access. Constants and variables used for IEEE 802.15.4 network configuration and parametrisation are the standard values, summarized in tables 1 and 2. The characterization of the inaccessibility scenarios in nonbeacon-enabled PAN was made as an extension of this work and is available in a technical report [11].

Next, we define a set of general equations describing frame transmission times. Equations 1 and 2 are used for unreliable (non acknowledged) frame transmission, and equations 3 and 4 for reliable (acknowledged) frame transmission.

Table 1: Relevant time-related constants of IEEE 802.15.4 Standard

IEEE 802.15.4 Name	**Abbr**	**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

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

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

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

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

where, $\mathcal{T}^{bc}_{ackDelay} = \mathcal{T}_{xvrcmd}$ 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.

4.1 Single Beacon Frame Loss - No Tracking

Let us start our analysis considering that a subset of nodes (may have a single element) in a PAN 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 period of at most $\mathcal{T}_{BSD} \,.\, (2^{BO}+1)$ symbols. If the beacon frame is received before the end of this search period, the frame shall be transmitted in the appropriate portion of the superframe. No 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:

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

After the period of inaccessibility, the node may proceed with the transmission of the frame using the unslotted version of the CSMA/CA algorithm.

Table 2: Relevant integer parameters of IEEE 802.15.4 Standard

IEEE 802.15.4 Name	**Abbr**	**Range**	**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

4.2 Multiple Beacon Frame Loss - Tracking

A beacon-enabled PAN 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 PAN 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 $\mathcal{T}_{BSD} \cdot (2^{BO}+1)$ symbol times. If a beacon frame with the current PAN identifier of the node is not received, this search is repeated from one to at most *nrLost* times. The best and worst-case inaccessibility durations are therefore given by equations 6 and 7, respectively.

$$\mathcal{T}^{bc}_{ina \leftarrow mbfl} = \mathcal{T}_{BSD} \cdot \left(2^{BO} + 1\right) \tag{6}$$

$$\mathcal{T}^{wc}_{ina \leftarrow mbfl} = \left(\mathcal{T}_{BSD} \cdot \left(2^{BO} + 1\right)\right) \cdot nrLost \tag{7}$$

4.3 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 the high layer protocol management entities. The corresponding inaccessibility period is simply given by:

$$\mathcal{T}_{ina \leftarrow nosync} = \left(\mathcal{T}_{BSD} \cdot \left(2^{BO} + 1\right)\right) \cdot nrLost \tag{8}$$

There are a number of causes for 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 hidden terminal problem or node mobility; glitches in the actual PAN coordinator or even its failure. Based on the information it owns, the high layer protocol management entities may take a decision on the appropriate recovery action.

4.4 Orphan Node

If the high layer protocol management entities decide that the node 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 coordinator, previously associated, 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 acknowledges the frame reception; the network becomes accessible. The worst-case inaccessibility time is given by:

$$\mathcal{T}^{wc}_{ina\leftarrow orphan} = \mathcal{T}_{ina\leftarrow nosync} + \mathcal{T}_{HLP}(Orphan) + \sum_{i=1}^{nrchannels} \{\mathcal{T}^{wc}_{MAC}(Orphan) + nrWait \,.\, \mathcal{T}_{BSD}\} + \mathcal{T}^{wc}_{ackDelay} + \mathcal{T}_{ack} \quad (9)$$

where, $\mathcal{T}_{HLP}$ is the normalized (symbol) time taken in the high layer protocol management actions. Should the orphan realignment succeed at the first attempt, the inaccessibility period will be simply given by equation 10.

$$\mathcal{T}^{bc}_{ina\leftarrow orphan} = \mathcal{T}_{ina\leftarrow nosync} + \mathcal{T}_{HLP}(Orphan) + \mathcal{T}^{bc}_{MAC}(Orphan) + \mathcal{T}_{HLP}(Realign) + \mathcal{T}^{bc}_{MAC\_ack}(Realign) \quad (10)$$

4.5 Coordinator Realignment

At a coordinator the need to assist MAC layer management actions starts when a MAC orphan notification command is received. Upon processing by high layer protocol management entities, the acknowledged transmission of a MAC realignment command is requested. The time taken in these actions is seen as inaccessibility in this coordinator. The best and worst inaccessibility times are given by equations 11 and 12, respectively.

$$\mathcal{T}^{bc}_{ina\leftarrow realign} = \mathcal{T}_{HLP}(Realign) + \mathcal{T}^{bc}_{MAC\_ack}(Realign) \quad (11)$$

$$\mathcal{T}^{wc}_{ina\leftarrow realign} = \mathcal{T}_{HLP}(Realign) + \mathcal{T}^{wc}_{MAC\_ack}(Realign) \quad (12)$$

4.6 PAN Conflict Detection

The creation and management of a PAN can be performed by any node with sufficient memory, battery life, and power processor. These nodes are called Full

Function Devices (FFDs). For this reason, there is a possibility of two different PANs in the same POS may render the same PAN identifier. This situation is called a PAN conflict and it can be detected by a PAN coordinator or by its directly associated nodes.

There are two forms to detect a PAN conflict: a beacon frame with the same PAN identifier is received from different PAN coordinators in the same POS; a PAN coordinator receives a PAN ID conflict notification from a node. The former is a local event. The latter involves the transaction of a MAC PAN ID conflict notification command, which may lead to a period of inaccessibility bounded by equations 13 and 14, respectively.

$$\mathcal{T}^{bc}_{ina \leftarrow PAN\_Conflict} = \mathcal{T}^{bc}_{MAC\_ack}(PAN\_Conflict) \tag{13}$$

$$\mathcal{T}^{wc}_{ina \leftarrow PAN\_Conflict} = \mathcal{T}^{wc}_{MAC\_ack}(PAN\_Conflict) \tag{14}$$

4.7 PAN Conflict Resolution

A node is obliged to signal the PAN CONFLICT to the high layer protocol 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 PAN identifiers recorded from the received beacons can be sent to the high layer protocol management entities all at once, as specified in equation 15, or each time a beacon frame is received, as drawn in equation 16. During all this process, the network is inaccessible. The best and worst inaccessibility durations are given by equations 15 and 16, respectively.

$$\mathcal{T}^{bc}_{ina \leftarrow PAN\_R} = \mathcal{T}_{HLP}(PAN\_Conflict) + \sum_{i=1}^{nrchannels} \left\{ \mathcal{T}^{bc}_{MAC}(Beacon\_R) + \mathcal{T}_{BSD}.(2^n + 1) \right\} + \mathcal{T}_{HLP}(Beacon) \tag{15}$$

$$\mathcal{T}^{wc}_{ina \leftarrow PAN\_R} = \mathcal{T}_{HLP}(PAN\_Conflict) + \sum_{i=1}^{nrchannels} \{ \mathcal{T}^{wc}_{MAC}(Beacon\_R) + \mathcal{T}_{BSD}.(2^n + 1) \} + \mathcal{T}_{HLP}(Beacon) \tag{16}$$

where, n is a parameter that determines the total duration of the beacon waiting period at each channel.

If, at the end of the search, the PAN coordinator does not found a beacon frame with its own PAN identifier no further action is taken and the network becomes accessible again. Otherwise, a new PAN identifier is selected and, if necessary, a MAC coordinator realignment command is broadcast. However, some nodes may not be synchronized with the "new" superframe structure, which may induce a loss of synchronization, as explained in Section 4.3.

Table 3: The best and worst cases for $868MHz$ frequency band

PHY (868-868.6 MHz)						
Scenario	**Modulation Technique**					
	BPSK		*ASK*		*O-QPSK*	
	best case (ms)	**worst case** (ms)	**bc** (ms)	**wc** (ms)	**bc** (ms)	**wc** (ms)
$t_{ina \leftarrow sbfl}$	——	12337	——	19739	——	9870
$t_{ina \leftarrow mbfl}$	12336	49344	19738	78951	9869	39476
$t_{ina \leftarrow nosync}$	49344	49344	78951	78951	39476	39476
$t_{ina \leftarrow orphan}$	49367	50935	78957	81483	39483	40744
$t_{ina \leftarrow realign}$	16	257	5	300	5	162
$t_{ina \leftarrow PAN\_Conflict}$	14	262	4	300	4	163
$t_{ina \leftarrow PAN\_R}$	12340	12389	19742	19814	9872	9909
$t_{ina \leftarrow GTS}$	8	216	4	296	3	154

4.8 GTS request

The allocation of GTS is performed sending a MAC GTS request command to the associated coordinator, which should be acknowledged. While the node does not receive this acknowledgment, the network is seen as inaccessible. The best and worst inaccessibility times are given by equations 17 and 18, respectively.

$$\mathcal{T}^{bc}_{ina \leftarrow GTS} = \mathcal{T}^{bc}_{MAC\_ack}(GTS) \tag{17}$$

$$\mathcal{T}^{wc}_{ina \leftarrow GTS} = \mathcal{T}^{wc}_{MAC\_ack}(GTS) \tag{18}$$

This scenario is extremely important because GTS slots can be used for bandwidth reservation. Solutions advanced in the literature try to solve the problem of real-time communications, over IEEE 802.15.4 standard, using GTS allocation mechanisms. The effectiveness of such solutions should be re-analyzed under the scope of a comprehensive network inaccessibility model.

4.9 Results

The table 3 presents the inaccessibility times for $868MHz$ frequency, considering default values of constants and parameters defined in the 802.15.4 standard. A data transfer, under normal network conditions, with frame size equal to **64 Bytes**, and using the $BPSK$ modulation, has a duration $t_{Data} \cong$ **26 ms**. The occurrence of some inaccessibility scenarios, presented in table 3, increase significantly this time. Furthermore, the beacon loss scenarios ($BPSK$ modulation) have inaccessibility periods up to 50 seconds, which are unacceptable for most embedded real-time applications, demonstrating the importance of our study.

5 Related Work

There are some related works that study the temporal aspects of the IEEE 802.15.4 standard. Ramachandran et. al. [12], Tang et. al [13] and Jung et. al. [14] made an exhaustive study about the CSMA/CA protocol in beacon-enabled PANs. Each study described a Markov model to understand its possible operation states and temporal aspects of this protocol. The three works consider a one-hop star topology where all nodes are in the transmission range of each other.

Ramachandran et. al. [12] focus their analysis in the throughput and energy consumption of the IEEE 802.15.4, considering the superframe only with CAP, no presence of MAC-level acknowledgements, and communications only from nodes to PAN coordinator, to simplify their model. Further, the authors make a modification in CSMA/CA parameters to improve performance and energy consumption of applications that do not need reliable data transfer, i. e., the use of acknowledgement to transmit their data.

The Markov model described for [13] allows analysis of the impact of the CSMA/CA parameters, the number of contending devices, and the data frame size on the network aspects such as throughput and energy efficiency. The authors utilize two two-dimensional Markov chains to make their analyzes and verifying that CSMA/CA parameters have a large impact on the network performance, being necessary to adjust these parameters for the network traffic conditions.

Further, Jung et. al. [14] analyze the performance of CSMA/CA protocol under unsaturated traffic conditions. Although the initial assumptions about the topology and the transmission range of the nodes, the authors consider that there are no transmission errors and no channel sense errors.

Huang et. al. [15], Hameed et. al. [16] and Koubaa et. al. [17] propose a modification on the IEEE 802.15.4 GTS allocation scheme. making optimizations in the default scheme used for bandwidth reservation.

Huang et. al. [15] propose an adaptive GTS allocation scheme that use two phases: a classification phase utilized for assigning priorities to nodes; and a scheduling phase where the GTS resources are allocated considering the priority numbers, the superframe length, and the GTS capacity of superframe. This changes are inserted without any modification of the IEEE 802.15.4 standard.

Hameed et. al. [16] propose a GTS allocation scheme called "Earliest Due Date GTS allocation". This modification considers the deadline of each GTS request, assigning the GTS slots for nodes with smaller normalize deadlines within each superframe. This algorithm assumes that no collisions and no packet lost occurs during transmissions.

Moreover, [17] uses network calculus to model the IEEE 802.15.4 behaviour and propose an implicit GTS allocation called i-GAME. The i-GAME allows the use of one slot by multiple nodes, considering available bandwidth resources, traffic specification and deadline requirements for accept or reject a GTS request.

Cena et. al. [18] propose the combination of wired and wireless worlds to provide real-time communication in industrial environments. This work presents

some means to build an hybrid network that incorporates the best of these worlds. Further, this work shows different forms to implement this combination.

Sokullu et. al. [19] show an investigation on possible MAC sublayer attacks on the IEEE 802.15.4. The scenarios presented in [19] describing some temporal problems caused by these attacks in the temporal behaviour of the IEEE 802.15.4 standard.

6 Conclusions

This paper presents the characterization of inaccessibility in wireless networks and does an exhaustive study of inaccessibility in IEEE 802.15.4 standard. This study was based on beacon-enabled personal area network and describes a relevant set of inaccessibility scenarios present on this type of network. Our study shows that the normal operation of MAC sublayer has hidden times that difficult the support of real-time communications. The control of these times, called inaccessibility, and the handling of omission failures can increase the predictability of the network and can be used for supporting real-time communications in lower levels protocols.

Applications timeouts, or other type of solutions used for control the temporal execution of real-time protocols, can use the knowledge of the inaccessibility times to make a fine adjust on its parameters, and provide an enhanced support for execution of real-time applications.

Future work directions will focus on providing means to reduce the periods of inaccessibility; extending the study to other inaccessibility scenarios including scenarios derived of MAC sublayer attacks; to provide support to signal the periods of inaccessibility to high-layers. Additionally, the results of these future works can be used to improve the support of real-time communications, providing the means of analyzing network delays and message schedulability under a performability perspective.

References

1. Veríssimo, P., Rodrigues, L., Baptista, M.: AMp: A Highly Parallel Atomic Multicast Protocol. SIGCOMM Comput. Commun. Rev. **19**(4) (1989) 83–93
2. Veríssimo, P., Marques, J.A.: Reliable broadcast for fault-tolerance on local computer networks. In: In Proceedings of the Ninth Symposium on Reliable Distributed Systems, Alabama, USA, IEEE (1990) 24–90
3. Rufino, J., Verissimo, P., Arroz, G., Almeida, C.: Control of Inaccessibility in CANELy. In: 2006 IEEE International Workshop on Factory Communication Systems, Torino, Italy (June 2006) 34–43
4. Verissimo, P., Rufino, J., Ming, L.: How hard is hard real-time communication on field-buses? In: Fault-Tolerant Computing, 1997. FTCS-27. Digest of Papers., Twenty-Seventh Annual International Symposium on. (Jun 1997) 112–121
5. Rufino, J., Verissimo, P.: A study on the Inaccessibility Characteristics of ISO 8802/4 Token-Bus LANs. In: 11th Annual Joint Conference of the IEEE Computer and Communication Societies, INFOCOM '92. Volume 2., Florence, Italy (May 1992) 958–967

6. Rufino, J., Craveiro, J., Schoofs, T., Tatibana, C., Windsor, J.: AIR Technology: A Step Towards ARINC 653 in Space. In: Eurospace DASIA 2009, Istanbul, Turkey (May 2009)
7. Veríssimo, P., Rufino, J., Rodrigues, L.: Enforcing Real-Time Behaviour on LAN-Based Protocols. In: 10th IFAC Workshop on Distributed Computer Control Systems. (Sept. 1991)
8. Karl, H., Willig, A.: Protocols and Architectures for Wireless Sensor Networks. John Wiley and Sons. Ltd. (2005)
9. IEEE 802.15.4 Standard: 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 Working Group Std. (2006) Revision of IEEE Std. 802.15.4-2003.
10. Gutierrez, J., Naeve, M., Callaway, E., Bourgeois, M., Mitter, V., Heile, B.: IEEE 802.15.4: A Developing Standard for Low-Power Low-Cost Wireless Personal Area Networks. Network, IEEE **15**(5) (September/October 2001) 12–19
11. Souza, J.L.R., Rufino, J.: Characterization of inaccessibility in ieee 802.15.4: A complete study. Technical report, AIR-II Technical Report RT-09-01 (2009)
12. Ramachandran, I., Das, A.K., Roy, S.: Analysis of the contention access period of IEEE 802.15.4 MAC. ACM Transactions on Sensor Networks (TOSN) **3**(1) (2007) 4
13. He, J., Tang, Z., Chen, H.H., Zhang, Q.: An accurate and scalable analytical model for IEEE 802.15.4 slotted CSMA/CA networks. IEEE Transactions on Wireless Communications **8**(1) (Jan. 2009) 440–448
14. Jung, C., Hwang, H., Sung, D., Hwang, G.: Enhanced Markov Chain Model and Throughput Analysis of the Slotted CSMA/CA for IEEE 802.15.4 Under Unsaturated Traffic Conditions. Vehicular Technology, IEEE Transactions on **58**(1) (Jan. 2009) 473–478
15. Huang, Y.K., Pang, A.C., Hung, H.N.: An Adaptive GTS Allocation Scheme for IEEE 802.15.4. IEEE Transactions on Parallel and Distributed Systems **19**(5) (May 2008) 641–651
16. Hameed, M., Trsek, H., Graeser, O., Jasperneite, J.: Performance investigation and optimization of IEEE 802.15.4 for industrial wireless sensor networks. In: IEEE International Conference on Emerging Technologies and Factory Automation, 2008. ETFA 2008. (Sept. 2008) 1016–1022
17. Koubâa, A., Cunha, A., Alves, M., Tovar, E.: i-GAME: An Implicit GTS Allocation Mechanism in IEEE 802.15.4, theory and practice. Springer Real-Time Systems Journal **39**(1-3) (August 2008) 169–204
18. Cena, G., Valenzano, A., Vitturi, S.: Hybrid Wired/Wireless Networks for Real-Time Communications. IEEE Industrial Electronics Magazine **2**(1) (March 2008) 8–20
19. Sokullu, R., Korkmaz, I., Dagdeviren, O., Mitseva, A., Prasad, N.R.: An Investigation on IEEE 802.15.4 MAC Layer Attacks. In: The 10th International Symposium on Wireless Personal Multimedia Communications, Jaipur, India (December 2007)