An Approach to Enhance the Timeliness of 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*—Wireless technologies are the present and the future of network communications. However, the support of real-time data transmission in wireless communications — providing support for execution of well-timed networked operations — is still an open issue, not fully addressed by current wireless network standards and technologies. Thus, this paper proposes a solution to enhance the timeliness of wireless communications without a need for fundamental modifications to the standard specifications. The IEEE 802.15.4 wireless network is used as a relevant case study. Our main contributions in this paper are: (a) a proposal to enhance the timeliness of wireless communications; (b) the extension of the data frame transmission service in order to control the effects of temporary partitions caused by disturbances in the medium and medium access control protocols; (c) a strategy to reduce the negative effects caused by the aforementioned disturbances.**

***Index Terms*—medium access control, inaccessibility, wireless communication, real-time systems.**

I. INTRODUCTION

The provision of temporal guarantees on wireless communications is still an open issue. Several approaches [1]–[4] to the problem of enhancing the timeliness of wireless communications assume that the network always operates normally, disregarding the occurrence of disturbances in the medium and medium access control (MAC) protocols.

However, wireless networks are extremely sensitive to external disturbances such as those resulting from electromagnetic interference, or application scenarios requiring intense mobility. These disturbances may lead to the occurrence of temporary partitions, also called periods of inaccessibility, where there may be sets of nodes which cannot communicate with each other [5]. Standard MAC protocols, including those used in wireless communications, can recover from these situations. However, this recovery process takes time and in the meanwhile the network is partitioned. The duration of a period of inaccessibility is dependent on each MAC layer, and must be analyzed for each network, such as the one defined in the IEEE 802.15.4 standard [6].

The occurrence of periods of inaccessibility leads to disruptions in the provision of MAC layer services. Furthermore, the analysis of the wireless protocol stack with a bottom-up approach shows that these disturbances may affect the entire stack, implying that service disruption may propagate upwards, and therefore interfere with the execution of higher layer protocols and applications. Thus, this paper proposes a new component layer executing on top of the MAC exposed interface to control the timeliness of wireless communications and reduce the impact of MAC layer service disruptions on the execution of the entire wireless protocol stack. This component layer improves the MAC layer functionality, mediating and isolating its interaction with higher layers, and allowing the configuration of the MAC layer parameters face to application requirements and environment restrictions.

The IEEE 802.15.4 wireless sensor and actuator network is used as a case study to present the main features of our proposal. A strategy is also presented to control the negative effects induced by the occurrence of periods of inaccessibility in network operation. Our approach does not require fundamental modifications of wireless network standards and therefore is in compliance with existing Commercial Off-the-Shelf (COTS) network components.

The paper is organized as follows: Section II presents a brief description of the system model used in our analysis. Section III presents an overview of the IEEE 802.15.4 standard. Section IV presents our proposal, describing its main components, the advantages of its use, and the improvements introduced at the data link layer service interface. Section V describes our results, extending the characterization of the data frame transmission service, and the strategy to control the periods of inaccessibility on wireless communications, using the IEEE 802.15.4 as a case study. Finally, Section VI draws some conclusions and future directions of this work.

II. SYSTEM MODEL

Our system model is formed by a set of communicating entities (processes/nodes) described by $P = \{p_1, p_2, p_3, ..., p_N\}$. Each entity, p_n, represents a process/node within a wireless network segment with n varying from 1 to N.

In an arbitrary geographic region we assume that all wireless nodes either communicate with each other at only one hop of distance or are out of reach. This means, all communicating wireless nodes are within the region of influence of one another and therefore each node can sense all transmissions of any other node. Hence, we assume the given wireless network

---

This work was partially motivated by our work within the scope of the ESA (European Space Agency) Innovation Triangle 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 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.

segment being composed of N nodes interconnected by a channel. Each communicating node $p_n \in P$ connects to the channel by a transmitter and a receiver. Network components either behave correctly or crash upon exceeding a given number of consecutive omissions, the omission degree bound, k. An omission is an error that destroys a data or control frame. Wireless communication channels are especially susceptible to omission errors, which may be due to a number of causes: electromagnetic interference in the medium; disturbances in a node transmitter/receiver circuitry; collisions derived from transmissions performed by different nodes on the same time; glitches in the network protocol operation; or even effects resulting from node mobility.

Despite its importance, the presence of channel malicious attacks [7], [8] is not considered in this paper, in order to simplify the system model and our analysis. Malicious attacks will be thoroughly addressed in a future work.

The omission of control frames (e.g., a token or a beacon) may generate temporary network partitions, logical rather than physical, called periods of inaccessibility [5]. A period of inaccessibility is a time interval where the network does not provide service although it cannot be considered failed. The characterization of IEEE 802.15.4 inaccessibility with respect to non-malicious disturbances is addressed in [6]. In addition, we assume that the wireless network is, at most, inaccessible i times, during a time interval relevant for protocol execution.

III. IEEE 802.15.4 OVERVIEW

The IEEE 802.15.4 standard specifies that each network must contain a coordinator, which defines the characteristics of the network such as addressing, supported radio channels, and operation mode. Normally, the coordinator is the node with the highest power and energy capabilities to support the execution of management operations required to maintain the network active throughout two operation modes: NonBeacon-enabled and Beacon-enabled. The case study addressed in this work (Section V) assumes a Beacon-enabled operation.

In the Beacon-enabled mode, the access to the wireless medium is controlled by information carried in a special frame sent by the coordinator. This special frame is called beacon and bounds a special structure called superframe, illustrated in Fig. 1. The information inside the beacon helps the nodes to know the entire duration of the superframe, allowing the synchronization and the control of the medium access.

The superframe organization of Fig. 1 identifies two main parts: the active and inactive periods. The active period is mandatory and it is, in turn, constituted by the Contention Access Period (CAP) and the Contention Free Period (CFP). CAP is also mandatory and allows all nodes to compete for the utilization of the shared physical medium. CFP is optional, being designed for bandwidth reservation, and therefore a node may previously allocate a slot, called Guarantee Time Slot (GTS), for exclusive medium access. The slotted version of Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) protocol [9] is used in node competition for medium access during the CAP portion of the superframe. Since GTS slots are reserved to a single node, no contention occurs and, within its allocated slot, the node can freely access the medium.

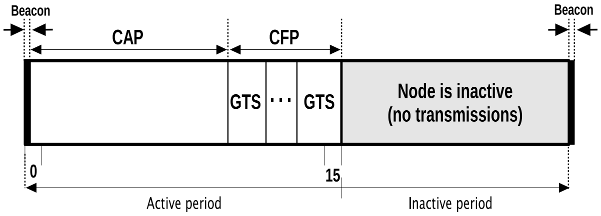

Fig. 1: Superframe structure

Completing the superframe structure the inactive period is optional and designed to optimize energy consumption. Thus, during this period all nodes in the network may turn off their transceivers to accomplish this goal [10].

IV. AN APPROACH TO ENHANCE THE TIMELINESS OF WIRELESS COMMUNICATIONS

Our approach to enhance the timeliness of wireless communications consists of an extensible component layer build around a standard MAC layer, dubbed *Mediator Layer*. This extensible component layer intermediates the communication and provides error isolation between the MAC and higher layers, minimizing the negative effects caused by disturbances in the medium and medium access protocols. The *Mediator Layer* is a standard-compliant solution which extends the MAC layer services with additional features and guarantees, enhancing the timeliness of wireless communications.

As drawn in Fig. 2 the *Real-Time Protocol Suite*, the *Timeliness and Partition Control*, and the *Configuration and Management Control* are fundamental components handling and managing the actions required to secure reliability and timeliness in data communications, thus enhancing the properties of the native MAC service.

The *Real-Time Protocol Suite* is responsible for handling data transmissions. This component enhances the frame transmission service provided by the MAC layer, establishing a foundation to offer a set of different service guarantees, with respect to reliability and timeliness, such as message transmission time bounds. Different protocols, serving requests with different types of requisites, can be incorporated in this component, augmenting the applicability of standard MAC layers on different areas with different requirements, namely on those with strict real-time demands, such real-time control and monitoring.

The *Timeliness and Partition Control* component deals with the temporal aspects related to the data transmission service, controlling and monitoring the timing of the actions within the *Mediator Layer*, and helping to provide resilience against all the occurrences of temporary network partitions. This component monitors the MAC layer to detect the occurrence and to be aware of any partitioning incidents, providing services to the *Real-Time Protocol Suite*. For example, a

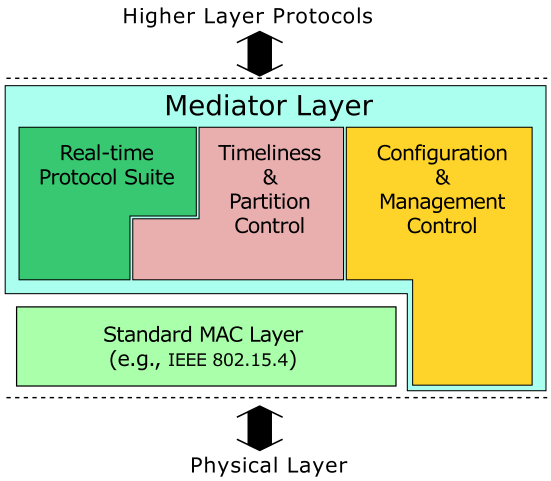

Fig. 2: An approach to enhance the timeliness of wireless communications

timer service controls the temporal execution of protocols, and integrated with the partition control functionality, allows the use of optimal timeout values even in the presence of periods of inaccessibility. Timeout values are automatically extended in this case, thus avoiding a premature and equivocal error propagation to other components and to higher layers.

The *Configuration and Management Control* component manages and controls the configuration of all parameters of the standard MAC layer and the internal parameters of the *Mediator Layer*, respecting realistic application requirements, resource limitations, and environment restrictions. This component makes the *Mediator Layer* (self-)adaptive, and (self-)managed, allowing the possibility to perform some changes in its internal state, and on its configuration profile, thus improving the timeliness of wireless communications.

A. Improving the control of data transmission services

The *Mediator Layer* implements the data layer programming interface. This implementation is represented by MI:

$$MI = \{request,\ confirm,\ indication\}\ . \qquad (1)$$

where the MI set defines the primitives in the *Mediator Layer* service interface. As usual in this kind of interfaces, the primitives are in compliance with the service specification interface described in the IEEE 802.2 standard [11]. Thus, a data transmission service provides three different primitives utilized to request and confirm a data transmission, and to indicate the reception of data.

The services provided by the *Mediator Layer* interface are build on top of MAC level primitives, which description is presented in Table I.

Without the *Mediator Layer*, higher layers shall implement mechanisms to control a frame transmission, ensuring that the frame arrives at its destination. In other words, higher layer protocols shall be: (a) aware of the occurrence of disturbances in the medium and MAC protocols, including periods of inaccessibility; (b) capable to configure parameters of the MAC layer to adapt to different conditions. However, the incorporation of these characteristics increases the complexity of higher layer protocols, forcing each of these protocols to have the capability to cope with low level problems outside the scope of their domains. The introduction of the *Mediator Layer* avoids these design complexities.

Primitives	**Description**
MAC.data.request	It provides a way to request a data transmission to the MAC layer. **Unreliable transmissions only**.
MAC.data.confirm	It provides a local confirmation that a frame has been sent to the medium. **Does not provide any guarantee of delivery at the destination**.
MAC.data.indication	It provides notification about an arrived data frame.

TABLE I: Standard MAC layer primitives for data transmission

The *Mediator Layer* and its components handle all aspects related to a data frame transmission service and its configuration, implying the reduction of the complexity of higher layer protocols. Additionally, with the capability to extend the internal components, our approach also enables the introduction of different types of control mechanisms, transmission protocols, (self-)management and (self-)adaptive strategies, providing an extremely useful service layer. The extension of the MAC data frame transmission service and the control of partition incidents (addressed in Section V-C) are examples of mechanisms implemented in the *Mediator Layer* that improve the services provided to higher layers.

Thus, the *Mediator Layer* is an innovative solution to enhance dependability and timeliness of wireless communications, as low as possible at the protocol stack. Its benefits are flexibly offered at the service interface, being transparently propagated throughout the entire stack, up to highest layer communication protocols and to the applications.

V. Preliminary results: A Case Study on the IEEE 802.15.4 Standard

A. General characterization of the MAC frame transmission service

Based on a user perspective of a MAC frame transmission service we represent in general the time interval required to access the wireless medium as $\mathcal{T}_{W-access}$. The effective time consumed by the node to access the medium is directly related to the medium access protocol in use.

After medium access protocol grants permission to access the medium, a frame is transmitted in the time interval represented by $\mathcal{T}_{MAC-type}$. Hence, equations 2 and 3 represent the best (^{bc}) and worst (^{wc}) cases of MAC frame transmission times.

$$\mathcal{T}^{bc}_{\tau-MAC}(type) = \mathcal{T}^{bc}_{W-access} + \mathcal{T}^{bc}_{MAC-type} \qquad (2)$$

$$\mathcal{T}^{wc}_{\tau-MAC}(type) = \mathcal{T}^{wc}_{W-access} + \mathcal{T}^{wc}_{MAC-type} \qquad (3)$$

These equations contribute to specify a general timeliness representation of a MAC level, presenting simple and easy-to-use formulas to calculate the time bounds of a MAC frame transmission service.

B. The IEEE 802.15.4 Characterization

As we use the IEEE 802.15.4 as a case study to present our results, we calculate the specific bounds of the IEEE 802.15.4 MAC frame transmission service considering a beacon enabled network. All data frame transmissions, with the exception of those performed in the GTS portion of the superframe, need to use of the slotted version of the CSMA/CA protocol [12], [13], analyzed as part of the MAC frame transmission service.

The CSMA/CA is a non-deterministic protocol, and the effective wait value is characterized by a random function, which execution may spam throughout several iterations. In each iteration, the wait time a node uses up is defined by a backoff exponent, as represented by the following equation:

$$\mathcal{T}_{access}(m) \, = \, \mathcal{T}_{backoff} \, . \, (2^{BE(m)} - 1) \tag{4}$$

where, $\mathcal{T}_{backoff}$ is the base value defining the minimum duration of a backoff period. Observing that the variability of the backoff exponent is dependent on the iteration number, m, the value of $BE(m)$ for each iteration is given by the following equation:

$$BE(m) = \begin{cases} minBE & \text{if } m = 0 \\ min(minBE + m, \, maxBE) & \text{if } m > 0 \end{cases} \tag{5}$$

The lower and upper bounds of $BE(m)$ are given by $minBE$ and $maxBE$, respectively. The value assigned to $BE(m)$ in the first iteration is equal to $BE(0) = minBE$. For each additional iteration of the CSMA/CA protocol a new value is calculated for $BE(m)$.

The time needed for medium access under normal IEEE 802.15.4 network operation can thus be characterized, in the best and worst cases, by the following equations:

$$\mathcal{T}^{bc}_{W-access} = \mathcal{T}_{access}(0) \tag{6}$$

$$\mathcal{T}^{wc}_{W-access} = \sum_{m=0}^{maxBackoff-1} \mathcal{T}_{access}(m) \tag{7}$$

where, $maxBackoff$ is the maximum number of iterations.

For the evaluation of absolute access time durations, we assume the use of the $2.4 \, GHz$ IEEE 802.15.4 frequency operation, with a $62.5 \, k \, symbols/s$ symbol rate and with four bits being coded into a single symbol. The default values of Table II are used. Under these conditions, the access to the shared medium may require in the worst case a delay as long as 2563 symbols, i.e., $\mathcal{T}^{wc}_{W-access} \cong 41ms$.

For the maximum frame length of 1016 bits, including headers, the corresponding worst case data frame transmission delay is $\mathcal{T}^{wc}_{\tau-MAC}(data) = 57ms$, assuming no errors during the entire process of a data frame transmission. However, disturbances on the medium and medium access protocols may cause the occurrence of periods of inaccessibility which may induce the occurrence of errors during a data frame transmission.

Parameter	Range	Default	Unit
$maxBackoff$	0-5	4	Integer
$minBE$	0-$maxBE$	3	Integer
$maxBE$	3-8	5	Integer
$\mathcal{T}_{backoff}$	—	20	Symbols

TABLE II: Relevant network parameters defined in the IEEE 802.15.4 standard

C. Dependability and Timeliness of Wireless Communications

Our proposal to control the dependability and timeliness of a frame transmission is divided on two issues: (a) the classical omission error handling present on reliable transmission protocols; (b) and the effective control of periods of inaccessibility.

1) Handling omission errors: Let us consider that the *Real-Time Protocol Suite* component uses a reliable unicast transmission service as an extension of the unreliable transmission service traditionally provided by MAC level standards. This reliable service is a rather classic transmit with acknowledgement (ACK) protocol required to enforce the reliability of a data communication service. To start a reliable transmission some higher level entity shall request a unicast data transmission with delivery guarantee through the *Mediator Layer* programming interface. During protocol execution, the transmitted frame or its associated ACK may be corrupted by disturbances which lead to omission errors. In this case, the destination node does not receive a correct frame, or the sender node does not receive the ACK associated with this frame. As frame corruptions are **transformed into omission errors**, detected when the time interval needed to transmit and receive the corresponding ACK frame ends, the sender node protocol activates a retransmission mechanism and tries to send the frame again, until a maximum number of attempts limited by the bounded omission degree, k, is reached.

However, the occurrence of temporary partitions during a frame transmission may cause a violation of the omission degree limited by k, and therefore the failure of the protocol in delivering the frame to its destination. This happens because the value of k is specified without contemplate the occurrence of periods of inaccessibility, and the standard MAC layer does not provide the additional control provided by our approach.

2) Controlling periods of inaccessibility: Our strategy to handle the occurrence of periods of inaccessibility during a frame transmission **also transforms inaccessibility incidents into omission errors**. A bounded inaccessibility degree, i, is introduced to (self)-adapt and configure the reliable unicast transmission service, and therefore the *Mediator Layer* as well. The combination of i and k (line 8 in Algorithm 1) makes the retransmission mechanism more dynamic, maintaining the timeout used to control reception of the ACK

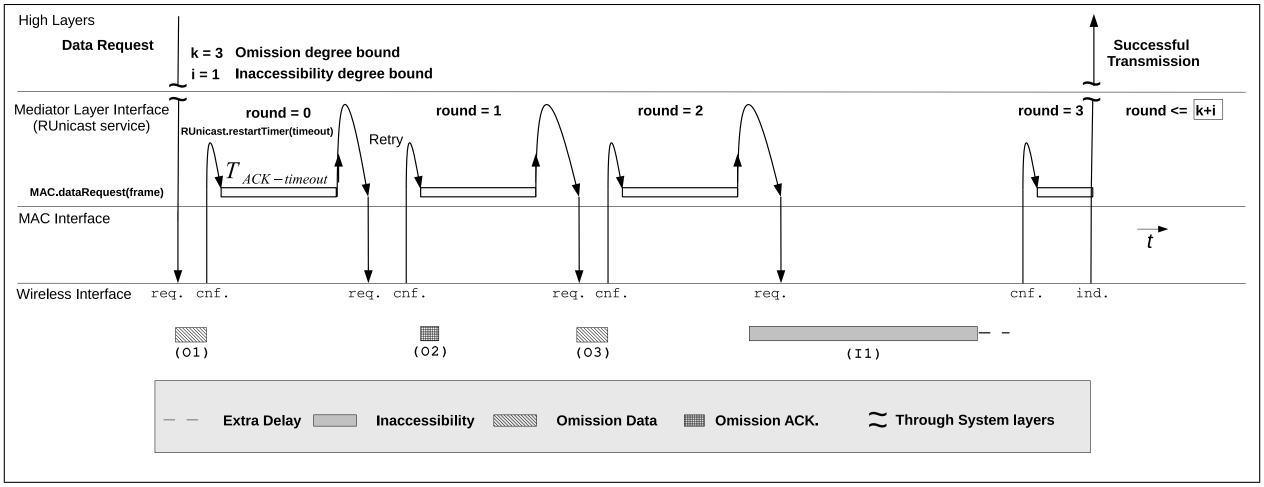

Fig. 3: The Effective Inaccessibility Control Mechanism

($\mathcal{T}_{ACK-timeout}$) with its original and optimized value, and allowing the adaptation of this mechanism to the different durations of each type of inaccessibility scenario (see Table III). The utilization of the same control mechanism for temporary partitions is only possible by the causal relation that exists among the frame transmission request and confirm primitives. Fig. 3 presents a frame transmission mediated by our proposed solution, evidencing that the local confirmation is only provided to the *Mediator Layer* after the actual transmission of the frame on the wireless medium.

Algorithm 1 presents the reliable unicast algorithm with simple, yet fundamental, mechanisms to handle the occurrence of periods of inaccessibility. In Algorithm 1, lines 8 specifies the incorporation of the bounded inaccessibility degree control mechanism in protocol operation, and line 11 the usage of the MAC level confirmation to start the timer which controls the retransmission process (in line 12). The value assigned to the inaccessibility degree bound depends on each network type and its parameters. However, it is reasonable to assume that only one period of inaccessibility would occur during a data transmission, i.e., it is reasonable to assume $i = 1$. The main advantage of such control mechanism is the temporal adaptation of timeout values to the duration of each period of inaccessibility, which may occur at most i times. Although a pure reliability enforcement algorithm only uses k to control the number of retransmissions, the transformation of inaccessibility events into omissions adds i to k and increases the maximum number of retransmissions to $k + i$. That means, the protocol is given a consolidated omission degree bound, K, being $K = k + i$.

In practical terms, this is equivalent to redefining the value assigned to the omission degree bound. This is very important because our control mechanism and the *Mediator Layer*, can be incorporated in any off-the-shelf equipment. In other words, is possible to improve the functionality traditionally offer by the MAC level without change the hardware devices operating in an existent wireless network, being totally transparent to the higher levels.

Algorithm 1 Controlling Inaccessibility (Trapping)

```
 1: Initialization phase.
 2: $k \leftarrow$ omission degree bound;
 3: $i \leftarrow$ inaccessibility degree bound;
 4: $round \leftarrow 0$; accounts for the number of omissions
 5: $ack\_rcv \leftarrow 0$;
 6: Begin.
 7: $RUcast.data.request(pckt)$
 8: while $round \leq \boxed{k+i}\ AND\ ack\_rcv = 0$ do
 9:     $frame \leftarrow pckt$;
10:     $MAC.data.request(frame)$;
11:     when $\boxed{MAC.data.confirm()}$ do
12:         $RUcast.restartTimer(\mathcal{T}_{ACK-timeout})$;
13:         when $MAC.indication(ACK)\ received$ do
14:             $ack\_rcv \leftarrow 1$;
15:         end when
16:         when $RUcast.timer(timeout\_expired)$ do
17:             $round \leftarrow round + 1$;
18:         end when
19:     end when
20: end while
21: if $ack\_rcv = 1$ then
22:     $RUcast.data.confirm(Success)$;
23: else
24:     $RUcast.data.confirm(Failure)$;
25: end if
26: End.
```

The value of the consolidated omission degree bound shall be dimensioned to consider the specific behavior of each MAC level standard. The related transmission technologies shall also be considered to accomplish the maximum efficiency against environment conditions during the provision of a reliable and timely service. Temporary partitions which may occur and disturb a frame transmission during the operation of the network are handled by the activation of the *Timeliness and Partition Control* component, improving the capabilities of the reliable transmission service provided by the *Mediator Layer*.

Scenario	Designation	**Periods of Inaccessibility** best case (ms)	worst case (ms)
Single Beacon Frame Loss - No Tracking	$t_{ina\leftarrow sbfl}$	——	3947.71
Multiple Beacon Frame Loss - Tracking	$t_{ina\leftarrow mbfl}$	3947.71	15790.08
Synchronization Loss	$t_{ina\leftarrow nosync}$	15790.08	15790.08
Orphan Node	$t_{ina\leftarrow orphan}$	15794.15	18421.70
Coordinator Realignment	$t_{ina\leftarrow realign}$	2.24	43.30
Coordinator Conflict Detection	$t_{ina\leftarrow C\_Conflict}$	1.14	42.40
Coordinator Conflict Resolution	$t_{ina\leftarrow C\_Resolution}$	63171.54	63822.54
GTS request	$t_{ina\leftarrow GTS}$	0.66	41.47

TABLE III: IEEE 802.15.4 best and worst periods of inaccessibility for the $2.4GHz$ frequency band [6]

D. Extending the general characterization of a MAC frame transmission service

Traditionally, a MAC frame transmission service is not aware of the occurrence of periods of inaccessibility during the network operation. Thus, we shall extend the general characterization of a MAC frame transmission service to incorporate the duration of these periods. This extension is presented in the following equations:

$$\mathcal{T}^{bc}_{\tau-MAC}(type) = \mathcal{T}^{bc}_{W-access} + \mathcal{T}^{bc}_{MAC-type} + \mathcal{T}_{ina} \qquad (8)$$

$$\mathcal{T}^{wc}_{\tau-MAC}(type) = \mathcal{T}^{wc}_{W-access} + \mathcal{T}^{wc}_{MAC-type} + \mathcal{T}_{ina} \qquad (9)$$

where $\mathcal{T}_{ina}$ represents the duration of a given period of inaccessibility. $\mathcal{T}_{ina}$ is a general term which supports the adaptation of this transmission service to the different durations of each inaccessibility scenario (see Table III). In case of non occurrence of a period of inaccessibility, $\mathcal{T}_{ina} = 0$.

Additionally, to evidence the importance of our proposal and of this control strategy we present in Table III a summary of relevant set of periods of inaccessibility, which if were compared to a data transmission with 1016 bits and transmission time around 57ms, are extremely higher. These values were obtained with an exhaustive analysis of the IEEE 802.15.4 made in [6]. Using the results presented in this paper, the occurrence of a timing fault is detected by the *Mediator Layer*, and its propagation to higher layers is avoided.

VI. CONCLUSION AND FUTURE WORK

The potential of wireless networks to support communications on different kinds of environments and applications, with strict timing restrictions, is still an open issue. In this paper we presented our approach to enhance the timeliness of wireless communications, introducing a new component layer with an effective control strategy, avoiding time faults even in the presence of errors in the medium and medium access protocols. Our approach presented a (self-)adaptive and (self-)managed solution, which being in compliance with standards can be used with the existent COTS components.

Future directions involve: reducing the duration of the inaccessibility scenarios based on mechanisms present in the IEEE 802.15.4 standard; improving the support to periodic traffic and applications with hard temporal restrictions; and defining relevant real-time metrics to evaluate the wireless communications with regard to application requirements and environment restrictions.

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 Internatonal Conference on Mobile Ad hoc and Sensor Systems (MASS)*, October 2007, pp. 1 –10.

[2] 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)*, Sept 2008, pp. 1016 –1022.

[3] 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.

[4] X.-Y. Shuai and Z.-C. Zhang, “Research of real-time wireless networks control system MAC protocol,” *Journal of Networks*, vol. 5, no. 4, pp. 419–426, April 2010.

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

[6] 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.

[7] R. Sokullu, I. Korkmaz, O. Dagdeviren, A. Mitseva, and N. R. Prasad, “An investigation on IEEE 802.15.4 MAC layer attacks,” in *10th Int. Symposium on Wireless Personal Multimedia Communications*, 2007.

[8] P. Radmand, A. Talevski, S. Petersen, and S. Carlsen, “Taxonomy of wireless sensor network cyber security attacks in the oil and gas industries,” in *24th IEEE International Conference on Advanced Information Networking and Applications (AINA)*. Washington, DC, USA: IEEE Computer Society, 2010, pp. 949–957.

[9] L. Kleinrock and F. Tobagi, “Packet switching in radio channels: Part i–carrier sense multiple-access modes and their throughput-delay characteristics,” *IEEE Transactions on Communications*, vol. 23, no. 12, pp. 1400 – 1416, December 1975.

[10] 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, 2006, Revision of IEEE Standard 802.15.4-2003.

[11] *ISO IEC 8802-2:1998, Logical Link Control*, IEEE, 1998.

[12] 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.

[13] 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.