The Wi-STARK Architecture For Resilient Real-Time Wireless Communications*

Jeferson L. R. Souza
jsouza@lasige.di.fc.ul.pt

José Rufino
jmrufino@ciencias.ulisboa.pt

Departamento de Informática, Faculdade de Ciências, Universidade de Lisboa, Portugal
Laboratório de Sistemas Informáticos de Grande-Escala (LaSIGE)
Navigators Research Team

ABSTRACT

Networking communications play an important role to secure a dependable and timely operation of distributed and real-time embedded system applications; however, an effective real-time support is not yet properly addressed in the wireless realm. This paper presents *Wi-STARK*, a novel architecture for resilient and real-time wireless communications within an one-hop communication domain. Low level reliable (frame) communications, node failure detection, membership management, and networking partition control are provided; since these low level services extend and build upon the exposed interface offered by networking technologies, *Wi-STARK* is in strict compliance with wireless communication standards, such as IEEE 802.15.4 and IEEE 802.11p. The *Wi-STARK* service interface is then offered as operating system primitives, helpful for building distributed control applications. The one-hop dependability and timeliness guarantees offered by *Wi-STARK* are a fundamental step towards an effective design of real-time wireless networks with multiple hops, including end-to-end schedulability analysis of networking operations.

Categories and Subject Descriptors

C.4 [**Computer System Organisation**]: [Fault tolerance]; C.3 [**Special-Purpose and Application Based Systems**]: Real-time and embedded systems; C.2.1 [**Computer Communication Networks**]: Network Architecture and Design—*Wireless communication*

Keywords

wireless communications, real-time, dependability, timeliness, resilience, fault tolerance, Wi-STARK

1. INTRODUCTION AND MOTIVATION

Advances in microelectronics enable the development and integration of networking computing systems in environments with different levels of criticality, monitoring and controlling physical entities such as nuclear reactors, physical structure of buildings and bridges, and power grids. In these kind of environments, usually known as Cyber Physical Systems (CPS), communications may have safety-critical constrains, implying a mandatory provision of real-time communication guarantees to secure the dependable and timely operation of the entire system.

The literature addressing real-time support on the wireless realm can be classified into two distinct domains: (a) communication protocols and architectures, and (b) schedulability analysis.

The contributions to real-time communication protocols and architectures, such as [16, 17, 18], are concerned with the provision of end-to-end guarantees within multiple hop networks. However, some of them require strong assumptions with respect a global notion of time (synchronised clocks among all nodes of a multiple hop network), which is a problem by itself without an easy solution. Furthermore, the used error model only assumes the loss of data frames, neglecting the effects that control frame errors may have on the operation of the Medium Access Control (MAC) sublayer, which may generate network partitions during long periods of time. These partitions may imply an unpredictable temporal behaviour and thus those protocols and architectures may, at the best, only provide probabilistic real-time guarantees.

The schedulability analysis of wireless networking communications [3, 11, 12] aims to verify if all transmissions can meet their deadlines for a given traffic workload, considering the end-to-end temporal guarantees wanted for a target network. Such end-to-end guarantees depend on the real-time guarantees secured within each single hop. Single hop guarantees can, on its turn, be derived from the temporal behaviour provided by the networking technology (communication protocols included), which must take into account the expected error conditions.

*This work was partially supported by the EC, through project IST-FP7-STREP-288195 (KARYON); by FCT/DAAD, through the transnational cooperation project PROPHECY; and by FCT, through project PTDC/EEI-SCR/3200/2012 (READAPT) and through LaSIGE Strategic Project PEst-OE/EEI/UI0408/2014.

EWiLi'14, November 2014, Lisbon, Portugal.

Conjugating dependability and real-time message delivery guarantees with wireless communications is a difficult problem. Instead of following the classic approach described in the wireless communication literature, and trying to establish those guarantees end-to-end —using a traditional point-to-point communication model —we take a divide to conquer approach, which is motivated by the following statement:

> *If no real-time guarantees can be offered within communications at one-hop of distance, no real-time guarantees can be offered within multiple hop communications at all.*

That means, any dependable real-time message delivery guarantee has to be secured first within the one-hop of distance wireless space, prior to be extended end-to-end, across multiple hops. Thus, this paper presents a design overview of a novel wireless communications architecture dubbed *Wi-STARK*, which has three main goals: (1) taking advantage of the intrinsic broadcast properties of the shared wireless communication medium within one-hop space, (2) providing dependability and real-time guarantees within such one-hop space, and (3) ensuring the feasibility of end-to-end schedulability analysis given the bounded transmission delay guarantees within each single hop. The *Wi-STARK* design is compliant with wireless communications standards, being able to offer at the lowest level of communications a set of useful and semantically rich services such as reliable and timely communications, node failure detection, membership management, and networking partition control. Since these services are built upon the exposed interface offered by current networking technologies, the *Wi-STARK* architecture can be easily implemented using Commercial Off-The-Shelf (COTS) components. The *Wi-STARK* service interface can easily be made available at the operating system Application Programming Interface (API).

To present the details concerning the design of the *Wi-STARK* architecture, this paper is organised as follows: section 2 presents a brief description of the system model, which is the foundation for the design of the *Wi-STARK* architecture; section 3 presents the main components and characteristics of the *Wi-STARK* architecture; section 4 presents the primitives and semantics of the *Wi-STARK* service interface; and finally, section 5 presents the conclusion and future directions of the design and applicability of the *Wi-STARK* architecture.

2. SYSTEM MODEL

All networking communications described in this paper are performed within the scope of a physical and data link layer abstract networking model dubbed Wireless network Segment (WnS), which establishes a broadcast domain where all wireless nodes are one-hop of distance from one another. *This simple approach empowers the achievement of a first and fundamental result: the capability of exploiting the broadcast nature of the shared one-hop communication space.*

The formalisation of the WnS is expressed by a 4-Tuple, $WnS \stackrel{def}{=} \langle X, x_m, C, W \rangle$, where X is the set of wireless nodes members of the WnS; x_m is the WnS coordinator, $x_m \in X$; C represents a set of radio frequency (RF) communication channels; and W represents the set of networking access protocols utilised in the support of frame transmissions. As illustrated in the graphical representation of Fig. 1, the intersection of the communication range of all nodes within the WnS constitutes its broadcast domain, where each node $x_j \in X$ is able to sense any transmission from any other node $x_q \in X$.

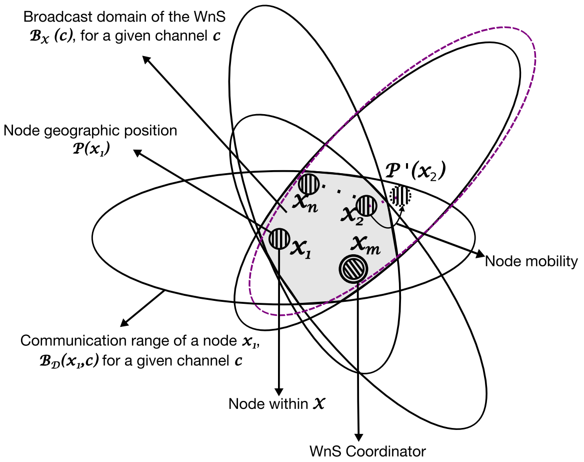

Broadcast domain of the WnS
$\mathcal{B}_X (c)$, for a given channel c
Node geographic position
$\mathcal{P}(x_1)$
$\mathcal{P}'(x_2)$
x_n
x_2
x_1
x_m
Node mobility
Communication range of a node x_1,
$\mathcal{B}_D(x_1,c)$ for a given channel c
Node within X
WnS Coordinator

Figure 1: The Wireless Network Segment (WnS) abstraction

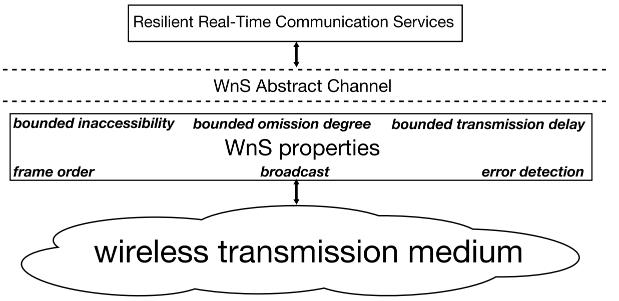
2.1 Fault Model

The failure of a networking component (a channel $c \in C$ or a node $x \in X$) is identified using an omission fault model, where frame errors are transformed into omissions. The occurrence of frame errors may be originated by disturbances caused by the presence of electromagnetic interferences on the communication channel, or malfunction within the node machinery, being accounted as omissions for the purpose of monitoring networking components.

For each received frame, each node $x \in X$ locally accounts observed omissions. When the number of observed omissions exceeds the component's omission degree bound, f_o, the failure of such component can be locally signed. Errors occurred at the wireless communication medium may affect only some nodes, which implies omissions may be accounted inconsistently at the different nodes of the WnS.

Both omissions with origin in the channel and at the channel end-points (i.e., the nodes) are accounted for. When successive frames are received with errors from a given channel input — i.e. a node $x \in X$ — exceeding a given omission degree bound, a *node persistent failure* is detected and signalled; when no traffic is received from node $x \in X$ within a bounded monitoring time interval, a *node crash failure* is detected and signalled.

Each node $x \in X$ may also inconsistently experience a temporary loss of connectivity with the WnS, caused by a phenomenon dubbed network inaccessibility [13]. A period of network inaccessibility may be induced by glitches in the MAC sublayer operation, such as those that may result from the omission of a MAC control frame (e.g., beacon). The network cannot be considered failed; it only enters into a temporary state where the communication service is not



WnS1 - ***Broadcast***: correct nodes, receiving an uncorrupted frame transmission, receive the same frame;

WnS2 - ***Frame Order***: any two frames received at any two correct nodes are received in the same order at both nodes;

WnS3 - ***Error Detection***: correct nodes *detect and signal* any corruption done during frame transmissions in a locally received frame;

WnS4 - ***Bounded Omission Degree***: in a known time interval $\mathcal{T}_{rd}$, omission failures may occur in at most k transmissions;

WnS5 - ***Bounded Inaccessibility***: in a known time interval $\mathcal{T}_{rd}$, a wireless network segment may be inaccessible at most i times, with a total duration of at most $\mathcal{T}_{ina}$;

WnS6 - ***Bounded Transmission Delay***: any frame transmission request is transmitted on the WnS, within a bounded delay $\mathcal{T}_{td} + \mathcal{T}_{ina}$.

Figure 2: WnS abstract channel properties

provided to some or all of the nodes. The loss of connectivity due to transient node mobility is also treated under the inaccessibility model.

Mobility may drive nodes to outside of the WnS, as illustrated in Fig. 1, where node x_2 using channel c moves from the geographic position $P(x_2)$ to the geographic position $P'(x_2)$. In despite of x_2 transmissions at the new position may reach all nodes of the WnS, the transmissions from the WnS coordinator, $x_m \in X$, do not reach node x_2 at position $P'(x_2)$. The permanent mobility of a node to outside of the WnS broadcast domain is then transformed into a *node crash failure* in our fault model.

2.2 WnS abstract channel properties

Communications at the lowest levels of the networking protocol stack can be abstracted by a set of correctness, dependability, and timeliness properties, which are not dependent on any particular networking technology. In the context of the WnS model such properties are seen as being provided by a single abstract communication channel dubbed WnS abstract channel, as illustrated in Fig. 2.

Property WnS1 (*Broadcast*) formalises that it is physically impossible for a node $x \in X$ to send conflicting information (in the same broadcast) to different nodes, within the broadcast domain of the WnS [2], $B_X(c)$, for a given channel $c \in C$ (see Fig. 1).

Property WnS2 (*Frame Order*) is common in network technologies (wireless technologies included), being imposed by the wireless communication medium of each channel $c \in C$, and resulting directly from the serialisation of frame transmissions on the shared wireless communication medium.

Property WnS3 (*Error Detection*) has both detection and signalling facets; the detection facet, traditionally provided by classical MAC sublayers, derives directly from frame protection through a frame check sequence (FCS) mechanism, which most utilised algorithm is the cyclic redundancy check (CRC); the signalling facet is provided by the FCS extension introduced in [15], which is able to signal omissions detected in frames received with errors. No fundamental modifications are needed to the wireless MAC standards, such as IEEE 802.15.4 [8]. The use of such unconventional extension is enabled by emerging controller technology, such as reprogrammable technology and/or open core MAC sublayer solutions, which are present, for example, in the development kits from ATMEL [1]. With the CRC polynomials used in wireless MAC sublayers, the residual probability of undetected frame errors is negligible [4, 5].

Property WnS4 (*Bounded Omission Degree*) formalises for a channel, $c \in C$, the failure semantics introduced earlier in the fault model definition, being the abstract channel omission degree bound, $k \geq f_o$. The omission degree of a WnS abstract channel can be bounded, given the error characteristics of its wireless transmission medium [4, 9, 13].

The *Bounded Omission Degree* property is one of the most complex properties to secure in wireless communications. Securing this property with optimal values and with a high degree of dependability coverage may require the use of multiple RF channels. In [15] we have advanced on how this can be achieved by monitoring channel omission errors, and switch between RF channels upon detecting the channel omission degree bound has been exceeded.

The time domain behaviour of a WnS is described by the remaining properties. Property WnS6 (*Bounded Transmission Delay*) specifies a maximum frame transmission delay, which is $\mathcal{T}_{td}$ in the absence of faults. The value of $\mathcal{T}_{td}$ includes the medium access and transmission delays and it depends on message latency class and overall offered load bounds [6, 10]. The value of $\mathcal{T}_{td}$ does not include the effects of omission errors. In particular, $\mathcal{T}_{td}$ does not account for possible frame retransmissions. However, $\mathcal{T}_{td}$ may include extra delays resulting from longer WnS access delays derived from subtle side-effects caused by the occurrence of periods of network inaccessibility [13]. Therefore, the bounded transmission delay includes $\mathcal{T}_{ina}$, a corrective term that accounts for the worst case duration of inaccessibility glitches, given the bounds specified by property WnS5 (*Bounded Inaccessibility*). The inaccessibility bounds depend on, and can be predicted by the analysis of MAC sublayer characteristics [13].

3. THE Wi-STARK ARCHITECTURE

The *Wi-STARK* is a new low level architecture that takes advantage of the intrinsic broadcast property of the shared wireless communication medium, and of the set of correctness, ordering, dependability, and timeliness properties offered by the WnS abstraction (Section 2.2) to establish a robust, resilient and real-time one-hop communication domain for wireless networks.

The *Wi-STARK* architecture design is open and flexible, being composed by two layers dubbed *Channel Layer* and

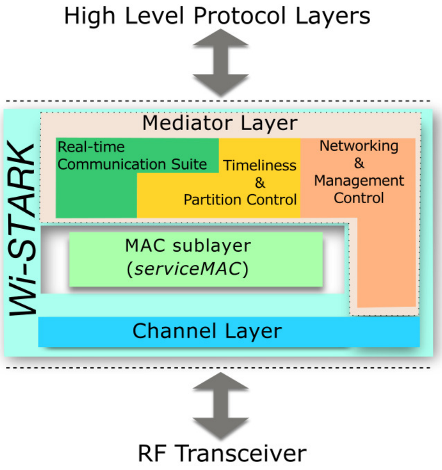

High Level Protocol Layers
Wi-STARK
Mediator Layer
Real-time Communication Suite
Timeliness & Partition Control
Networking & Management Control
MAC sublayer (serviceMAC)
Channel Layer
RF Transceiver

Figure 3: The *Wi-STARK* Architecture

Mediator Layer. As shown in Fig. 3, these layers are by design wrapping the standard MAC sublayer to improve: the control and use of RF communication channels; and, the services offered to high level protocol layers.

3.1 Channel Layer

The *Channel Layer* (Fig. 4) is a thin layer that provides a common interface to transparently control the use of a given RF communication channel $c \in C$ for purposes of frame transmission and reception, incorporating useful extensions to enhance the dependability of communications. A RF communication channel $c \in C$ is an abstract representation of the wireless transmission medium plus a piece of hardware dubbed RF transceiver, which conjugates a residual part of the MAC sublayer, herein called, *basicMAC* and the physical (PHY) layer itself.

The *Channel Layer* extends the *basicMAC* to exploit the exposed RF transceiver interface, and the parametrisation features thereof. In particular, the *Channel Layer* implements: the FCS extension (specified in [15]), which secures the WnS3 property of the WnS; the accounting of channel omissions and the detection of a RF communication channel failure, upon exceeding the omission degree bound, k (accordingly with WnS4); the RF communication channel switch strategy specified in [15].

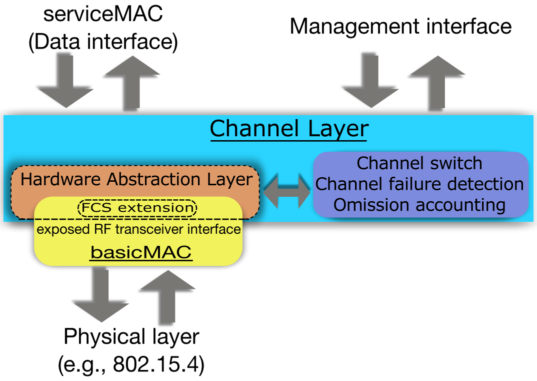


Figure 4: Channel Layer

3.2 MAC Sublayer: serviceMAC

The MAC sublayer illustrated in Fig. 3 is the standard MAC sublayer present in the traditional wireless networking protocol stack, such as those specified within the IEEE 802.15.4 [8] and IEEE 802.11p [7] wireless standards. In the context of the *Wi-STARK* architecture such standard MAC sublayer is dubbed *serviceMAC*, offering only conventional unreliable data frame and management service interfaces. No modifications are needed for its integration in the *Wi-STARK* architecture. In this sense, the *Wi-STARK* architecture is highly flexible supporting the integration of any MAC sublayer, including the real-time variants proposed in [16, 17].

3.3 Mediator Layer

The *Mediator Layer* is an extensible sublayer, specially designed to mediate the communication flow from (and to) the high level protocol layers, as illustrated in Fig. 3. The *Mediator Layer* is responsible for the semantically rich service interface offered by *Wi-STARK*, effectively augmenting the services offered by the standard MAC sublayer. Three main components compose the *Mediator Layer*: the Real-Time Communication Suite, the Timeliness & Partition Control, and the Networking & Management Control.

3.3.1 Real-time Communication Suite

The Real-Time Communication Suite (RTCS) is the component responsible for the data communication services offered by the *Wi-STARK* architecture, as illustrated in Fig. 5. The RTCS includes a *Message Request Dispatcher* that forwards any high level message transmit request to the adequate instance of the RTCS protocol bundle. Messages submitted at the *Wi-STARK* service interface have a maximum length for allowing the encapsulation of their content in exactly one frame, without necessity of fragmentation.

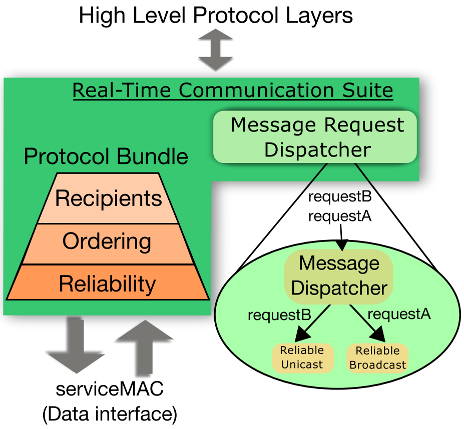
The table of Fig. 5 specifies the fundamental properties (recipients, ordering, and reliability) characterising the different variants of the protocols to be included in the RTCS protocol bundle. For example: a totally ordered reliable message delivery targeting all correct nodes features the well known *atomic broadcast* primitive. This specification is open and extensible: other attributes (e.g., *temporal order*) and other properties (e.g., *urgency*) can be included.

The *Wi-STARK* architecture design provides two fundamental guarantees to the high level protocol layers and applications:

Temporal-bounded communications: every transmitted message[1] is successfully received by all relevant correct nodes of the WnS within a known temporal bound, $\mathcal{T}_{Tx-Data}$.

The value of $\mathcal{T}_{Tx-Data}$ is directly derived from the combination of four important properties of the WnS: WnS3 (*Error Detection*), WnS4 (*Bounded Omission Degree*), WnS5 (*Bounded Inaccessibility*), and WnS6 (*Bounded Transmission Delay*). In the absence of errors, the *Wi-STARK* protocols execute in a single round and the upper bound for all correct nodes of the WnS receiving a message successfully is: $\mathcal{T}_{Tx-Data}^{wc-ne} = 2.\mathcal{T}_{td}$; being $\mathcal{T}_{td}$ the maximum frame transmission delay in the absence of errors.

[1] A message is a high level protocol layer data service unit.



Real-Time Communication Suite	
Property	Attributes

Recipients	Single node (Unicast);
	Multiple nodes (Multicast);
	All nodes (Broadcast)

Ordering	Unordered; Totally ordered
Reliability	Unreliable; Reliable

Figure 5: Real-Time Communication Suite

In the presence of errors, frames[2] may have to be retransmitted and the protocols within the *Wi-STARK* architecture may require more than one round to be executed, up to a limit given by $k+i+1$ (as specified by properties WnS4 and WnS5); all relevant correct nodes can successfully receive **any message transmitted with any reliable communication protocol** provided by the *Wi-STARK architecture* in, at most, $\mathcal{T}^{wc}_{Tx-Data} = (k+i+1) \times (2.\mathcal{T}_{td}) + \mathcal{T}_{ina}$. The timer utilised by reliable protocols to control protocol execution is configured with its optimal value (i.e., $\mathcal{T}_{td}$), and extended (if needed) by the real value of the network inaccessibility, t_{ina}, adding up to at most $\mathcal{T}_{ina}$ [14].

A failure of the RF communication channel in use is detected by the violation of k, the channel omission degree bound (WnS4), being the *Wi-STARK* architecture able to switch to another channel to keep the networking communications operational; the duration of the "communication blackout" resultant from that *channel failure* is then incorporated in the network inaccessibility model through $\mathcal{T}_{ina}$.

Message delivery: every transmitted message is delivered to all relevant correct nodes of the WnS.

Message delivery guarantees emerge from reliable communication protocols of the *Wi-STARK* architecture, which exploit the nature of the shared wireless communication medium (properties WnS1 and WnS2) to offer *totally ordered delivery* guarantees.

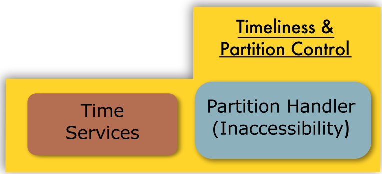

Timeliness & Partition Control
Time Services
Partition Handler (Inaccessibility)

Figure 6: Timeliness & Partition Control

3.3.2 Timeliness & Partition Control

The *Timeliness & Partition Control* (TPC) presents the transversal components that deals with the temporal aspects of the service offered by the *Wi-STARK* architecture. As shown in Fig. 6, the TPC component incorporates *Time Services* that include the management of protocol timers and other services used in the temporal control of *Wi-STARK* components.

The *Partition Handler* is focused to detect the occurrence, and to be aware of any partitioning incidents caused by the presence of periods of network inaccessibility. Controlling networking inaccessibility allows the use of optimal timeout values, which are automatically extended [14] when a period of inaccessibility occurs, preventing the propagation of premature timeout errors to other components and to high protocol layers.

3.3.3 Networking & Management Control

The *Networking & Management Control* component (illustrated in Fig. 7) incorporates all the functionalities of the *Mediator Layer* responsible for managing the dependable operation of each node $x \in X$. The management responsibilities assigned to the *Mediator Layer* include controlling all internal configuration of the *Wi-STARK* architecture, the parameters of the MAC sublayer (*basicMAC* and *serviceMAC* included), and the provision of management services to support the WnS formation.

All configurations can be performed statically or dynamically. The static configuration is target for hard real-time environments where all analyses of the traffic pattern, error conditions, and mobility models are performed offline, being stored in the *Wi-STARK Information Base* (Fig. 7). The *Mediator Layer* (self-)adaptation and dynamic configuration capabilities are related with mixed-critical and soft real-time requirements, which are outside the scope of this paper.

The membership and node failure detection offered by the *Mediator Layer* were designed to control and establish a consistent view of all members of the WnS, which is represented by the abstract set, X.

4. Wi-STARK DATA SERVICE INTERFACE

In the perspective of networking protocol developers, the dependability and timeliness guarantees offered by the *Wi-STARK* architecture are represented by a set of fundamental primitives for transmission and reception of messages to/from the network, which are specified in Table 1.

All of the primitives present in the *Wi-STARK* data service

[2] A frame is the MAC sublayer protocol data unit.

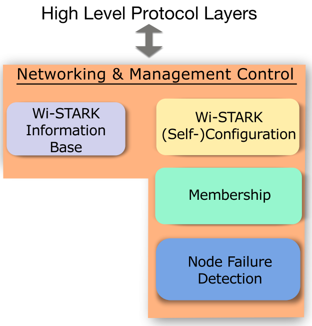

High Level Protocol Layers
Networking & Management Control
Wi-STARK Information Base
Wi-STARK (Self-)Configuration
Membership
Node Failure Detection

Figure 7: Networking & Management Control

Wi-STARK data service interface	
Primitives	**Description**
MLA.Data.request	Requests a message transmission using one of the *Wi-STARK* communication protocols.
MLA.Data.confirm	For reliable services, it confirms message delivery at recipients. Otherwise, it confirms only message transmission.
MLA.Data.indication	Notifies the arrival of a message.

Table 1: *Wi-STARK* data service interface

interface are easily integrated into embedded and real-time operating systems, being available as system calls associated to the wireless networking protocol stack.

5. CONCLUSION

This paper presented the architectural design of *Wi-STARK*, a novel low level architecture for resilient and real-time one-hop wireless communications. The definition of *Wi-STARK* is based on the establishment of an abstract communication model dubbed Wireless network Segment (WnS), which offer a set of correctness, dependability, and timeliness properties to support the design of resilient communication services for wireless networks.

Wi-STARK is compliant with wireless standards such as IEEE 802.15.4 and IEEE 802.11p, being capable to offer support for low level reliable message communication, node failure detection and membership, and networking partition control. Future directions involves the incorporation of the Wi-STARK service interface in the API of embedded real-time operating systems, and the extension of one-hop guarantees for multi-hop networking scenarios.

6. REFERENCES

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

[2] O. Babaoğlu and R. Drummond. Streets of Byzantium: Network Architectures for Fast Reliable Broadcasts. *IEEE Trans. on Soft. Engineering*, SE-11(6), June 1985.

[3] O. Chipara, C. Lu, and G.-C. Roman. Real-Time Query Scheduling for Wireless Sensor Networks. *IEEE Trans. on Computers*, 62(9), September 2013.

[4] D. Eckhardt and P. Steenkiste. Measurement and Analysis of The Error Characteristics of An In-Building Wireless Network. In *2nd SIGCOMM Conference*, 1996.

[5] T. Fujiwara, T. Kasami, A. Kitai, and S. Lin. On The Undetected Error Probability for Shortened Hamming Codes. *IEEE Trans. on Comm.*, 33(6), June 1985.

[6] M. Hameed, H. Trsek, O. Graeser, and J. Jasperneite. Performance Investigation And Optimization of IEEE 802.15.4 For Industrial Wireless Sensor Networks. In *IEEE 13th ETFA Conference*, September 2008.

[7] IEEE 802.11p. Wireless Access in Vehicular Environments - IEEE Standard 802.11p, 2010. Amendment to IEEE Standard 802.11-2007.

[8] IEEE 802.15.4. Part 15.4: Wireless Medium Access Control (MAC) And Physical Layer (PHY) Specifications For Low-Rate Wireless Personal Area Networks (WPANs) - IEEE standard 802.15.4, 2011.

[9] M. Petrova, J. Riihijarvi, P. Mahonen, and S. Labella. Performance Study of IEEE 802.15.4 Using Measurements And Simulations. In *WCNC Conference*, Las Vegas, NV, USA, April 2006.

[10] I. Ramachandran, A. K. Das, and S. Roy. Analysis of The Contention Access Period of IEEE 802.15.4 MAC. *ACM Trans. on Sensor Networks*, 3, March 2007.

[11] A. Saifullah, Y. Xu, C. Lu, and Y. Chen. Priority Assignment For Real-Time Flows in WirelessHART Networks. In *23rd ECRTS Conference*, July 2011.

[12] W. Shen, T. Zhang, M. Gidlund, and F. Dobslaw. SAS-TDMA: A Source Aware Scheduling Algorithm For Real-Time Communication In Industrial Wireless Sensor Networks. *Springer Wireless Networks Journal*, 19(6), August 2013.

[13] J. L. R. Souza and J. Rufino. Characterization of inaccessibility in wireless networks - A Case Study on IEEE 802.15.4 Standard. In *IFIP 3th IESS Conference*, September 2009.

[14] J. L. R. Souza and J. Rufino. An Approach to Enhance The Timeliness of Wireless Communications. In *5th UBICOMM Conference*, Lisbon, Portugal, November 2011.

[15] J. L. R. Souza and J. Rufino. Analysing And Reducing Network Inaccessibility in IEEE 802.15.4 Wireless Communications. In *IEEE 38th LCN Conference*, Sydney, Australia, October 2013.

[16] Y.-H. Wei, Q. Leng, S. Han, A. Mok, W. Zhang, and M. Tomizuka. RT-WiFi: Real-Time High-Speed Communication Protocol For Wireless Cyber-Physical Control Applications. In *IEEE34th RTSS Conference*, December 2013.

[17] Y. Xue, B. Ramamurthy, and M. C. Vuran. SDRCS: A Service-Differentiated Real-Time Communication Scheme For Event Sensing in Wireless Sensor Networks. *Computer Networks*, 55(15), June 2011.

[18] X. Zhu, S. Han, P.-C. Huang, A. Mok, and D. Chen. MBStar: A Real-Time Communication Protocol For Wireless Body Area Networks. In *23rd ECRTS Conference*, July 2011.