PROFIBUS PROTOCOL EXTENSIONS FOR ENABLING INTER-CELL MOBILITY IN BRIDGE-BASED HYBRID WIRED/WIRELESS NETWORKS

Luís Ferreira, Eduardo Tovar, Mário Alves

Polytechnic Institute of Porto (ISEP-IPP)
Rua Dr. António Bernardino de Almeida, 431
4200-072 Porto, Portugal
E-mail: {llf@dei, emt@dei, malves@dee}.isep.ipp.pt

Abstract: Future industrial control/multimedia applications will increasingly impose or benefit from wireless and mobile communications. Therefore, there is an enormous eagerness for extending currently available industrial communications networks with wireless and mobility capabilities. The RFieldbus European project is just one example, where a PROFIBUS-based hybrid (wired/wireless) architecture was specified and implemented. In the RFieldbus architecture, interoperability between wired and wireless components is achieved by the use specific intermediate networking systems operating at the physical layer level, i.e. operating as repeaters. Instead, in this paper we will focus on a bridge-based approach, which presents several advantages. This concept was introduced in (Ferreira, *et al.*, 2002), where a bridge-based approach was briefly outlined. Then, a specific Inter-Domain Protocol (IDP) was proposed to handle the Inter-Domain transactions in such a bridge-based approach (Ferreira, *et al.*, 2003a). The major contribution of this paper is in extending these previous works by describing the protocol extensions to support inter-cell mobility in such a bridge-based hybrid wired/wireless PROFIBUS networks.

Keywords: Fieldbus, Wireless, Real-time, Industrial Automation

1. INTRODUCTION

PROFIBUS is one of the most popular fieldbus protocols, with several hundreds of thousands of installations currently in operation worldwide. It was standardised in 1996, as EN 50170 (EN 50170, 1996), by CENELEC and, more recently in 2000, by IEC as IEC61158 – Fieldbus Standard for use in Industrial Systems.

In the last years, eagerness emerged concerning extending the capabilities of PROFIBUS to cover functionalities not previously considered: industrial wireless communications (Haehniche and Rauchaupt, 2000; Alves *et al.*, 2002; Rauchhaupt, 2002) and the ability to support industrial multimedia traffic (Pereira *et al.,* 2002).

The RFieldbus European project (Rauchhaupt, 2002) is just one example of that effort, where PROFIBUS was extended for encompassing hybrid wired/wireless communication systems.

This work was partially supported by the European Commission under the project R-FIELDBUS (IST-1999-11316) and by FCT under the project CIDER (POSI/1999/CHS/33139).

In RFieldbus, interoperability between wired and wireless components is achieved by the use of intermediate networking systems operating at the physical layer level (i.e. as repeaters), resulting in a "broadcast" network with a single logical ring (just one token rotating between the masters). The main advantage of such a single logical ring (SLR) approach is that the effort for protocol extensions is not significant.

However, there are a number of advantages in using a multiple logical ring (MLR) approach to such type of hybrid systems. This concept was introduced and discussed in (Ferreira *et al.*, 2002) where a bridge-based approach (thus, layer 2 interoperability) was briefly outlined. In that work, references to how some complex functionalities (such as the handoff between adjacent wireless cells) could be supported with minimum protocol extensions and still maintaining the compatibility with legacy PROFIBUS technologies were briefly described.

The main advantage of a bridge-based solution is that it provides traffic segmentation, thus improved responsiveness for transactions between stations belonging to the same logical ring, and error containment within each domain. In (Ferreira *et al.*,

2003a), all implementation details concerning an Inter-Domain Protocol (IDP) which is able to support Inter-Domain Transactions (IDT) are thoroughly described.

This paper extends previous works on the analysis and proposal of the required protocol extensions to support the inter-domain (inter cell) mobility of wireless nodes, therefore with a particular focus on the handoff functionalities.

The reminder of this paper is organised as follows. In Section 2 some fundamental aspects of the PROFIBUS protocol are presented. Then, in Section 3, we introduce the context and describe the main concepts related to bridge-based hybrid wired/wireless PROFIBUS networks. In Section 4, the mechanisms and protocols for supporting inter-cell mobility of wireless stations are described in detail. The concepts of Global Mobility Manager (GMM) and Domain Mobility Manager (DMM) are introduced. In Section 5, we discuss the approach proposed in this paper, namely concerning some timing characteristics. Finally, in Section 6, we draw some conclusions and outline the ongoing work.

2. RELEVANT ASPECTS OF PROFIBUS

This section addresses some features of the PROFIBUS protocol that are relevant for this paper.

2.1 Message Cycle

In PROFIBUS, master stations may initiate message transactions, whereas slave stations do not transmit on their own initiative but only upon (master) request. A transaction (or message cycle) consists of the request frame from the initiator (always a master station) and the associated acknowledgement or response frame from the responder (either a master or a slave station). The acknowledgement (or response) must arrive before the expiration of the *Slot Time*, otherwise the initiator repeats the request the number of times defined by the *max_retry_limit*, a PROFIBUS Data Link Layer (DLL) parameter.

A PROFIBUS master is capable of executing transactions during its token holding time (T_{TH}), which is given a value corresponding to the difference, if positive, between the target token rotation time (T_{TR}) parameter and the real token rotation time (T_{RR}). For further details, the reader is referred to (EN5017, 1996; Tovar and Vasques, 1999).

2.2 Ring Maintenance Mechanisms

In order to maintain the logical ring, PROFIBUS provides a decentralised (in every master station) ring maintenance mechanism. Each master maintains two tables – the *Gap List* (GAPL) and the *List of Active Stations* (LAS). Optionally it may also maintain a *Live List* (LL).

The *Gap List* consists of the address range from *TS* (*This Station* address) until *NS* (*Next Station* address, i.e., the next master in the logical ring). Each master station in the logical ring starts to check its *Gap* addresses every time its *Gap Update Timer* (T_{GUD}) expires. This mechanism allows masters to track changes in the logical ring: addition (joining) and removal (leaving) of stations. This is accomplished by examining (at most) one *Gap address* per token visit, using the *FDL_Request_Status* frame.

The LAS comprises all the masters in the logical ring, and is generated in each master station when it is in the *Listen Token* state after power on. This list is also dynamically updated during operation, upon receipt of token frames.

The *Live List* mechanism requires an explicit request from the PROFIBUS DDL user (via a management FMA1/2 request). This service returns the list of all active stations (masters and slaves).

2.3 Token Passing Procedure

The token is passed between masters in ascending address order, except for the master with the highest address, that must pass the token to the master with lowest address. Each master knows the address of the *Previous Station* (PS), the address of the *Next Station* (NS) and, obviously, its own address (*This Station* address - TS).

If a master receives a token addressed to itself from a station registered in the LAS as its predecessor, then that master is the token owner, and may start processing message cycles. On the other hand, if a master receives the token from a station, which is not its PS, then it shall assume an error and will not accept the token. However, if it receives a subsequent token from the same station, it shall accept the token and assume that the logical ring has changed. In this case, it updates the PS with the new address.

If after transmitting the token frame, and within the *Slot Time*, the master detects valid bus activity, it assumes that its successor owns the token and is executing message cycles. Therefore, it ceases monitoring the activity on the bus.

In case the master does not recognise any bus activity within the *Slot Time*, it repeats the token frame and waits another *Slot Time*. If it recognises bus activity within the second *Slot Time*, it assumes a correct token transmission. Otherwise, it repeats the token transmission to its next station for the last time. If still, there is no bus activity, the token transmitter tries to pass the token to the next successor of its LAS. It continues repeating this procedure until it founds a successor.

3. BASICS ON HYBRID WIRED/WIRELESS PROFIBUS NETWORKS

3.1 Network Components and Basics on Bridge Operation

A hybrid wired/wireless fieldbus network is composed by stations with a wireless interface (usually radio) that are able to communicate with wired (legacy) stations.

The wireless part of the fieldbus network is supposed to include at least one *radio cell*. Basically, a radio cell can be described as a 3D-space where all associated wireless stations are able to communicate with each other. Our architecture considers two types of domains.

A *Wired Domain* is a set of (wired) stations intercommunicating via a wired physical medium. A *Wireless Domain* is a set of (wireless) stations intercommunicating via a wireless physical medium. In the example of Fig. 1 the following set of wired PROFIBUS master (M) and slave (S) stations are considered: M1, M2, S1, S2, S3, S4 and S5. Additionally, the following set of wireless stations is considered: M3, S6 and S7. Within this set, only M3 and S6 are mobile. All wireless stations are assumed to be PROFIBUS stations with a wireless physical interface, capable of supporting radio communications and the mobility functionalities, like in RFieldbus (Rauchhaupt, 2002). Three bridge devices are considered: B1, B2 and B3.

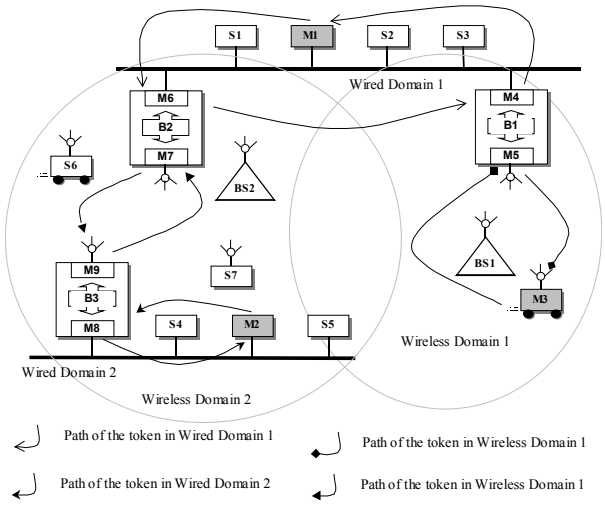

Fig. 1. Wireless PROFIBUS example network

In such a system, all communications are relayed through base stations: BS1 and BS2. Each base station uses two radio channels, one to transmit frames to wireless stations (the downlink channel), and another to receive frames from the wireless stations (the uplink channel). Since all frames in wireless domains are relayed through base stations, the downlink signal quality can be assessed by wireless stations to perform the inter-cell mobility (further detailed in Section 4). We will assume, in the remaining of the paper, that M5 and M7 include the base station functionalities in their wireless front-end, thus, structuring radio cells (wireless domains) 1 and 2, respectively.

Note also that the network operation is based on the Domain-Driven Multiple Logical Ring (MLR) schema, described in (Ferreira, *et al.*, 2002). Therefore, each wired/wireless domain has its own logical ring. In fact, each bridge includes two masters (Fig. 2): one belonging to the wired domain and the other belonging to the wireless domain.

In the example of Fig. 1, four different logical rings exist: {(M3 → M5), (M1 → M4 → M6), (M7 → M9), (M8 → M2)}. Obviously, our approach could be generalised to bridges interconnecting more than 2 domains.

We are also assuming that the network topology is tree-like, and that routing is based on MAC addresses. Traffic is relayed from one bridge master to the other if the destination address is included in the *Routing Table* (RT) of the incoming side. Obviously, every bridge must include two tables (one for each bridge master). This approach imposes the use of a single address space, where every station in the network has a unique MAC address. This implies that bridge masters must read all frames, even if the destination address does not correspond to their own address.

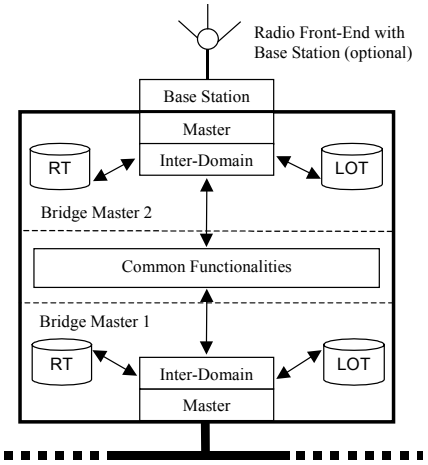

Fig. 2. Bridge components

3.2 Interoperability Between Domains

The communication between stations belonging to different domains; that is, Inter-Domain Transactions (IDT), is supported by the Inter-Domain Protocol (IDP) proposed in (Ferreira *et al.*, 2003a). The IDP not only defines the format of frames exchanged between bridges, but also specific bridge functionalities. In this section, we will just briefly describe the IDP.

When an initiator makes a request addressed to a station in another domain (an Inter-Domain Request), all stations belonging to the initiator's domain discard the frame, except the bridge masters (BMs) belonging to that domain. Only one of these BMs then handles the request frame. We denote this bridge master, i.e. the first bridge master in the path from the initiator to the responder, as BM_i, where i stands for initiator. The relayed frame, denoted as an Inter-Domain Frame (IDF), is coded using the IDP (Ferreira *et al.*, 2003a). Bridges perform routing based on the MAC addresses contained in the frames and on the routing table (RT) of the incoming side.

The IDF embeds the original request (or response) and additional information that allows both the decoding of the embedded frame and the matching between the request and the respective response. The BM_i is capable of matching a response to the related pending request, using the information contained in the IDF embedding the response, and by using the information contained in the *List of Open Transactions* (LOT). The LOT contains information about the request frame, such as destination and source addresses. It also contains a tag, the *Transaction Identifier* (TI), which must be included in the IDF related to the request and also in the respective IDF response.

The IDF embedding the request is relayed by the other bridges in the path until reaching the bridge master that connects to the domain the responder belongs to (the last bridge master in the path) - bridge master BM_r,

where *r* stands for responder. Then, this bridge reconstructs the original request frame and transmits it to the responder, a standard PROFIBUS responder station (e.g., a wireless DP slave).

When BM_r receives the immediate response to that request, it encodes the frame using the IDP. This IDF will be relayed until reaching bridge master BM_i, where it will be decoded and stored.

In order to conclude the transaction, the initiator periodically repeats the (same) request until receiving the related response. When BM_i receives the (repeated) request, it responds to the initiator using the stored response frame meanwhile obtained. This mechanism is completely transparent from the point of view of the initiator, since BM_i emulates the responder in a way that the initiator station considers the responder station as belonging to its domain.

Considering the system scenario illustrated in Fig. 1, Fig. 3 represents a simplified timeline regarding a transaction between master M3 and slave S6.

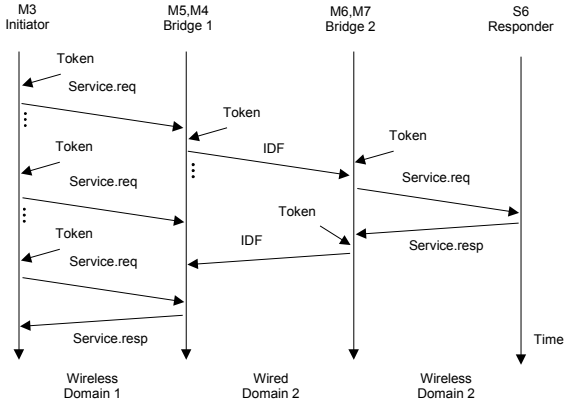

Fig. 3. Example timeline for an Inter-Domain Transaction (IDT) between M3 and S6

4. SUPPORTING INTER-DOMAIN MOBILITY

In RFieldbus, the inter-domain mobility depends on the assessment period (Alves *et al*., 2002), which is periodically triggered by one of the masters (the beacon master). Each base station sends beacons in its radio channel, in order for the wireless stations to assess the quality of the different channels, after which, the wireless stations may switch to the channel offering the best signal quality. Note that as there is only one token rotating (single logical ring system) there is no message loss and no need for specific registration mechanism.

However, the approach described in Section 3 (bridge-based intermediate systems) requires a more sophisticated handoff procedure. The main reason is that the system has multiple logical rings. Mobile wireless stations must implement radio channel assessment and switching mechanisms, and also mechanisms to support stations joining/leaving the logical rings.

In (Ferreira *et al.,* 2002), the authors briefly described the possibility of using the native PROFIBUS ring management mechanisms to support inter-cell (inter-domain) mobility. However, additional mechanisms must be added to guarantee no errors, no loss of frames or frame order inversion concerning inter-domain transactions (IDT).

Therefore, in this paper we propose a hierarchically managed handoff procedure that fulfils these requirements. One master in the overall system implements the global mobility management functionality – the *Global Mobility Manager* (GMM). In each domain, one master controls the mobility of stations belonging to that domain – the *Domain Mobility Manager* (DMM). Finally, the bridges must implement specific mobility services. The GMM must know the addresses of all the bridges and DMMs in the system. Each DMM must know the addresses of the bridges in its domain. For example, and concerning the scenario illustrated in Fig. 1, M1 assumes both the role of GMM and the DMM of wired domain 1. Bridge masters M5, M7 and M8 assume the role of DMMs for wireless domain 1, wireless domain 2 and wired domain 2, respectively.

The role of these management entities and the different phases involved in the proposed handoff will be described next.

4.1 Phases of the Handoff Procedure

The handoff procedure starts with a *Start Handoff Procedure* message sent by the GMM. This message is sent periodically, according to the mobility requirements (e.g. maximum foreseeable speed) of the mobile stations. All bridges in the network relay this message, which then triggers a sequence of actions that are briefly outlined in Fig. 4.

Phase 1

When the bridges receive this message, they stop accepting new IDTs from the masters belonging to their domains. Nonetheless, they keep handling pending IDTs (which are still present in their LOTs) and, importantly, they keep handling IDTs originated in the other domains. After completing all pending IDTs (those from their LOTs), the bridges transmit a *Ready to Start Handoff Procedure* message to the GMM. When the GMM receives such a message from all bridges, it broadcasts a *Prepare for Beacon Phase* message. Note that intra-domain transactions are allowed until this instant.

Phase 2

After the DMMs receive the *Prepare for Beacon Phase* message, and as soon as they receive the token, they do not pass it to other masters in their domains. Each DMM sends a *Ready for Beacon Phase* message to the GMM and starts an *Inquiry* service. During this phase, every DMM sends *Inquiry* frames addressed to bridge masters belonging to its domain. The bridges use the response message to transmit any mobility-related message from its output queue. This procedure minimises the communication latency between the GMM and the DMMs, and keeps small the inaccessibility period of the wired nodes, as it will be shown in Section 5. When a bridge master without domain management capabilities receives the *Prepare for Beacon Phase* message, it will only be able to

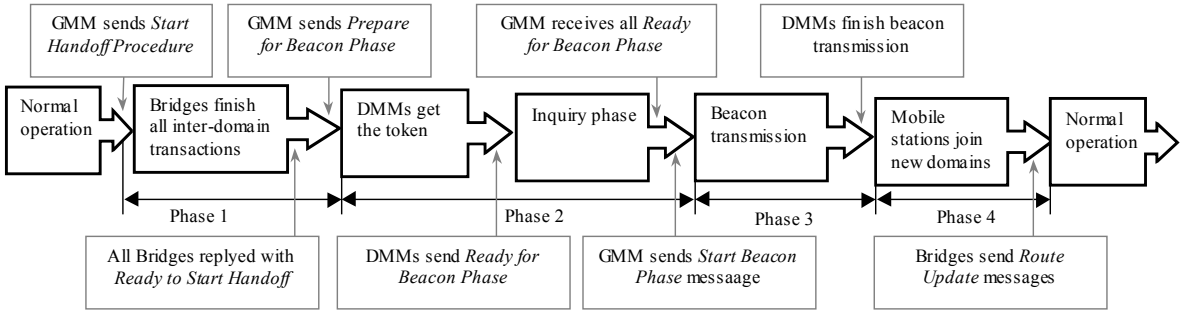

Fig. 4. Handoff Procedure phases (simplified)

communicate using the *Inquiry* service, and it clears all its routing table entries related to mobile nodes.

Phase 3

After collecting all *Ready for Beacon Phase* messages from the DMMs, the GMM starts the assessment phase by broadcasting the *Start Beacon Phase* message. Upon receiving this message, the DMMs start emitting beacons. Wired domains may resume intra-domain transactions, but they are not capable of performing inter-domain transactions (IDTs) while the bridges belonging to their domains do not receive the route update messages related to the mobile nodes. The mobile stations use the beacon frames to evaluate the quality of the different radio channels and to decide if they switch the radio channel (or not). So, every mobile station willing to handoff must switch to the new radio channel, before ending the beacon transmission.

Phase 4

After the end of the beacon phase, every wireless DMM (still holding the token) inquires all mobile stations in order to detect if they still belong to its domain. After this, mobile slaves are capable of answering requests, but mobile masters must still enter the new logical ring using the standard PROFIBUS ring management mechanisms. Since the routing table entries related to mobile stations have been cleared, only when the bridges receive updated routing information, at the end of the Handoff Procedure, they may restart routing IDTs related to mobile stations.

4.2 Details on the Handoff Procedure

State Machine for the GMM. The operation of the GMM is based on the state machine depicted in Fig. 5. We are considering that there is a mobility timer used to trigger the Handoff Procedure in a periodic fashion.

At power on, the GMM enters into the *INACTIVE* state, and the mobility timer is loaded with the Handoff Procedure period (which depends on the dynamics of the mobile stations). When the mobility timer expires (TIMER transition) the GMM state machine enters in the *WRSHP* state (Wait Ready to Start Handoff Procedure message) and the GMM sends the *Start Handoff Procedure* message.

In the *WRSHP* state, the GMM receives *Ready to Start Handoff Procedure* messages from all the network bridges (*READYH* transition). It will only enter into the *WRBP* (Wait Ready for Beacon Phase message) state when all bridges have replied (*ALLRESP1* transition) and then it sends the *Prepare for Beacon Phase* message.

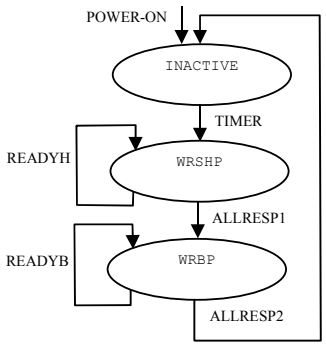

Fig. 5. State machine for the GMM

In the *WRBP* state, the GMM receives *Ready for Beacon Phase* messages from the network DMMs (*READYB* transition). When all DMMs have replied, the state machine enters into the *INACTIVE* state, and the GMM sends the *Start Beacon Phase* message.

State Machine for the DMM. The DMM is responsible for retaining the token, controlling the *Inquiry* service and transmitting beacons (only in a wireless domain). This DMM functionality can be embedded in any type of static master station, but for improved performance (in most cases) it should be located in a bridge master.

The DMM state machine (Fig. 6) goes into the *INACTIVE* state after power-on. Transition *SHP_MSG* is triggered when the DMM receives the *Start Handoff Procedure* message, and enters the *WPBP* (Wait Prepare for Beacon Phase) state, where the DMM waits for the reception of the *Prepare for Beacon Phase* message. This message triggers the transition (*PBP_MSG*) to the *WTOKEN* (Wait Token) state. In this state, the DMM waits until receiving the token from its predecessor, and then (*TOKEN_MSG* transition) it retains the token and sends the *Ready for Beacon Phase* message to the GMM. Following this, the DMM uses the *Inquiry* service in order to exchange mobility-related messages with the bridges in its domain. This service is needed in order to guarantee that all DMMs are able to communicate with the GMM. Nevertheless, if there are no other bridges belonging to the DMM domain, it transmits *void* frames in order to maintain network activity.

When the *Start Beacon Phase* message arrives to the DMM (*SBP_MSG* transition), the DMM starts transmitting beacon frames for a certain period. When this period ends, the DMM tries to detect if mobile stations are located in its domain, by inquiring them using *FDL_Request_Status* frames (*FDL_ST_MSG* transition).

When a DMM is responsible for a wired domain, it does not transmit any beacon frame and thus it passes from the *INQUIRY* state directly to the *INACTIVE* state (*WR_DOM* transition).

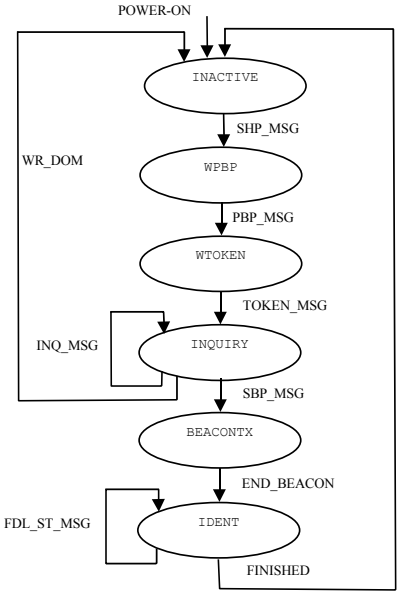

Fig. 6. State machine for a DMM

Other Bridges' Functionalities. The bridge's role during the Handoff Procedure is essentially to ensure that there are no pending IDTs during the Handoff Procedure and to relay mobility-related messages (when the DMMs are in the *INQUIRY* state). So, at power-on (Fig. 7), a bridge goes into the *INACTIVE* state, where it operates normally, relaying IDTs as described in Section 3.2. In this state the bridge can update its *List of Active Stations*, *Live List* or *Gap list,* and consequently its routing table according to the changes in the configuration of the system (*LAS_C*, *LL_C* and *GAP_C* transitions). These transitions also trigger the broadcast of a *Route Update* message. Also, when the bridge receives a *Route Update* message, it updates the routing tables and forwards that message (*RT_UDT* transition).

When a bridge receives the *Start Handoff Procedure* message (*SHP_MSG* transition) it goes into the *WIDT_END* (Wait Inter-Domain Transactions End) state, where the bridge waits until finalising all its open IDTs contained in the LOT. In this state, the bridge masters ignore new IDTs.

The completion of an IDT triggers the *IDT_FINISHED* transition. When all IDTs have been completed, the bridge enters into the *WINQUIRY* (Wait Inquiry message) state (*ALL_IDT_FINISHED* transition). In the *WINQUIRY* state, the bridge only communicates with its domain DMM, using the *Inquiry* service. In this state, when the bridge receives an *Inquiry* frame and it has mobility related messages, it responds (*RESP* transition), otherwise, no response is sent (*NO_RESP* transition).

When the beacon transmission starts, the bridge returns into the *INACTIVE* state and clears the entries related to mobile stations in its routing table (*START_BEACON* transition). Thus, all bridges must know the addresses of all mobile stations in the system. From this point forward, the bridges are capable of relaying IDTs, if requested. Obviously, IDTs related to mobile stations will only be relayed when the bridge receives the related *Route Update* messages.

The description of the mobility related messages can be found in (Ferreira *et al*., 2003b).

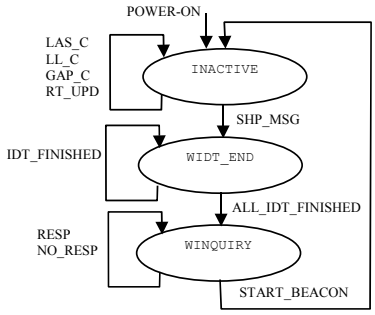

Fig. 7. State Machine for the mobility related functionalities in the bridges

5. EXAMPLE SCENARIO AND TIMING DISCUSSION

In order to outline an example of the Handoff Procedure, we are considering a network scenario as depicted in Fig. 1. For the sake of simplicity, we also consider that there is no additional traffic in the network, except for an Inter-Domain Transaction (IDT) between master M2 and slave S7, an Intra-Domain Transaction between M2 and S5, the token, and mobility-related messages. We are also considering that both M3 and S6 will execute a handoff. Fig. 8 supports the following description.

5.1 Example Scenario

The GMM starts the Handoff Procedure by broadcasting the *Start Handoff Procedure* message (M1.1). After receiving this message, bridges B2 and B1 having no open IDT immediately transmit the message *Ready to Start Handoff Procedure* (B1.1, B2.1).

Bridge B3 has an open IDT, related to request M2.1. Therefore it will only send the *Ready to Start Handoff Procedure* message (B3.1) when the transaction related to M2.1 is completed. After that, master M2 tries again to make the same transaction but bridge B3 ignores it. Note that the intra-domain transaction between M2 and S5 may still carry on.

After receiving the *Ready to Start Handoff Procedure* message from all network bridges (B1.1, B2.1 and B3.1), the GMM broadcasts the message *Prepare for Beacon Phase* (M1.2). When the DMMs M7, M8 and M5 receive that message, they start the *Inquiry* service. So, messages B2.2 and B1.2 are only transmitted when M1 (wired domain 1 DMM) sends the *Inquiry* frames M1.3 and M1.4, respectively addressed to B1 and B2. Message B3.2 is relayed in a similar way until reaching M1.

Also note that masters M8 and M5 do not have any other bridge belonging to its domain, thus they send void frames.

After receiving the *Ready for Beacon Phase* message from all the DMMs in the network (B1.2, B2.2 and B3.2), the GMM sends the *Start Beacon Phase* message (M1.5). When receiving this message, each DMM will start the transmission of beacon messages. The starting time of this phase is slightly different for the different domains due to communication latencies. Also, the duration of the beacon phase must be different for different domains so that all domains finish almost at the same time. The duration of the beacon phase must guarantee that all stations are capable of evaluating all possible radio channels and switch to a new one. Note that in wired domains it is not necessary to transmit beacon frames. Nevertheless, the bridges connecting to these domains must relay the *Start Beacon Phase* (M1.5) message to other wireless domains.

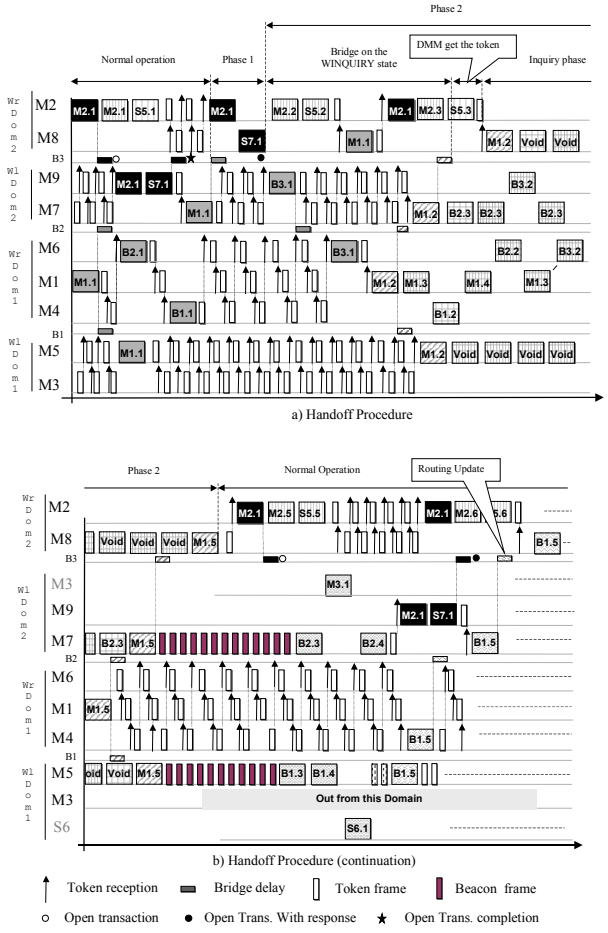

Fig. 8. Timeline for handoff procedure

Before the end of the beacon phase, mobile master M3 and mobile slave S6 switch to the radio channels of wireless domain 2 and wireless domain 1, respectively.

After the end of the beacon phase, wireless DMMs M5 and M7 *Inquire* the mobile stations in the network (M3 and S6) in order to detect if they are located in its domain. M5 and M7 use *FDL_Request_Status* frames addressed to mobile stations S6 (B1.4 and B2.4) and M3 (B1.3 and B2.3).

From this point forward, slave S6 is capable of answering requests, but master M3 must still enter into the new logical ring using the standard ring management procedures. This is illustrated in Fig. 9.

Message B1.5 is the route update message related to station S6, but the message related to station M3 is only sent when M3 effectively enters the logical ring. When master M2 receives the token, it repeats request M2.1, but it will only be relayed by bridge B3 when M9 receives the token, after the end of the beacon phase. Nevertheless, intra-domain transactions in wired domain 2 are possible during this period.

When M3 enters into the new wireless domain, it detects that it was taken out of the ring and goes into the *Listen Token State*. M3 will only be able to enter the new logical ring when its predecessor station starts the *Gap Update* mechanism and subsequently passes the token to M3.

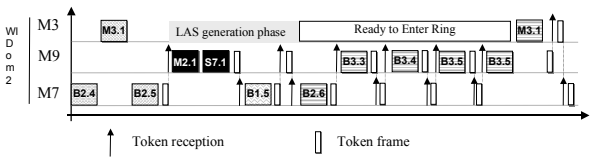

Fig. 9. M3 entrance into the logical ring

Fig. 9 further highlights some details on how the entry of station M3 into the logical ring is performed. In fact, after the switching, station M3 is still on the *Active Idle* state. So, it can return an answer (M3.1) to the *FDL_Request_Status* request B2.3. After that, M3 detects that its predecessor station did not pass the token and enters into the *Listen Token* state, where it re-generates its LAS during two complete token rounds. During this phase M3 will not answer any requests addressed to it. After this phase M3 is ready to enter into the logical ring and is able to reply to any *FDL_Request_Status* frame (indicating its readiness).

M9 uses the *Gap Update* mechanism in order to include M3 in its logical ring, thus it sends *FDL_Request_Status* requests B3.3, B3.4 and B3.5, respectively addressed to stations with addresses 0, 1 and 2 (considering that station M9 HSA is equal to 9). Finally, M9 sends *FDL_Request_Status* request B3.5, which is addressed to M3, it replies with the *Ready to Enter Logical Ring* message, subsequently M9 passes the token to M3. To make the entry procedure fast, master stations must have a low *Gap update* factor.

5.2 A Discussion on Timeliness

Quantifying the duration of the different phases of the handoff procedure enables a notion of the latencies involved in this procedure.

In order to be able to obtain figures for the example presented in Section 5.1, we are making the following assumptions:

- data rate of 1.5Mbps;
- all data frames have equal duration (approximately 154μs);
- the beacon frames (the same type of frame as the token frame) have a duration of 30μs;
- bridge relaying latency is 200μs;
- *Slot Time* is 66μs;
- and wired/wireless bit rates and frame formats are identical.

Using these assumptions, Table 1 presents the results for the example scenario. Note also a second column (in shading) that contains the results for the case of 12Mbps.

The inaccessibility time for the wired domains is equal (for the depicted scenario) to the duration of the inquiry phase, 1640μs and 1450μs, respectively for wired domain 1 and wired domain 2. Only during this time it will not be possible to perform intra-domain transactions (IDTs) in the wired domains. IDTs will only be possible when the mobile nodes join their new domains. Thus, a station in wired domain 2 is not able to exchange messages with S6 for a time span of 5540μs, and with M3 for a time span of 7202μs.

Table 1 Handoff Procedure Timings (in μs)

Time Span	1.5Mb/s	12Mb/s
Time needed by bridge B3 to finish all of its IDT	355	53
Time during which B3 is in WINQUIRY state	1129	169
Time needed until the DMM of wired domain 2 obtains the token	183	28
Duration of the inquiry phase	1450	195
Duration of the beacon phase in wireless domain1	988	148
Duration of the beacon phase in wireless domain2	836	125
Inaccessibility for node S6	2953	443
Inaccessibility for node M3	5774	866

Note however that these are not worst-case values. They only reflect reasonable figures for the actual scenario mentioned in Section 5.1. In fact, these values result from a relaxed scenario in terms of number of concurrent transactions (both inter-domain and intra-domain). Nevertheless, the applications envisaged for wireless applications are not expected to require very tight control loops. Examples of such applications are handheld terminals, AGVs or multimedia devices (Pacheco *et al.*, 2002). It is also obvious that if the bit rate increases to 12Mbps (PROFIBUS already supports it), the latencies involved in the handoff procedure are significantly reduced.

6. CONCLUSIONS AND ON-GOING WORK

In this paper, we have detailed and analysed mechanisms for supporting inter-domain mobility of mobile stations in hybrid wired/wireless bridge-based PROFIBUS networks. In such an architecture, the communication between the different domains is supported by an Inter-Domain Protocol. This protocol enables the use of standard PROFIBUS stations, since the additional functionalities are implemented by specific bridge devices responsible for emulating the behaviour of the responder stations.

In the proposed architecture, mobile/wireless stations may move between different wireless cells using a Handoff Procedure hierarchically managed by the Global Mobility Manager (GMM) and several Domain Mobility Managers (DMMs).

A crucial aspect of the proposed mobility protocol is its ability to cope with the timing requirements of distributed applications. Although in this paper we have discussed some aspects related to timeliness, it is an on-going work the development of a simulation tool, which implements the proposed protocols. This tool is now is now in the last stages of development and will enable further temporal characterisation of the proposed architecture. Another objective of this simulation tool is to assess possible enhancements in the protocol in order to increase its performance, e.g. in order to reduce the time needed by a master to enter into a new logical ring.

In this paper, and for the sake of simplicity, we did not make any references to any kind of error detection/recovery mechanisms, which obviously are necessary. This issue is also being addressed in the related on-going work.

REFERENCES

Alves, M., Tovar, E., Vasques, F., Roether, K. and Hammer, G. (2002). Real-Time Communications over Hybrid Wired/Wireless PROFIBUS-based Networks. In Proceedings of the 14th Euromicro Conference on Real-Time Systems (ECRTS'02), pp. 142-151.

EN 50170 – General purpose field communication system (1996). CENELEC.

Ferreira, L., Alves, M. and Tovar, E. (2002). Hybrid Wired/Wireless PROFIBUS Networks Supported by Bridges/Routers. In Proceedings of the 2002 IEEE International Workshop on Factory Communication Systems, pp. 193-202.

Ferreira, L., Tovar, E. and Alves, M. (2003a). Enabling Inter-Domain Transactions in PROFIBUS Networks. In Technical Report HURRAY-TR-0304.

Ferreira, L., Tovar, E. and Alves, M. (2003b). Inter-Domain Mobility in PROFIBUS Bridge-Based Hybrid Wired/Wireless Networks. In Technical Report HURRAY-TR-0305.

Haehniche, J. and Rauchhaupt, L. (2000). Radio Communication in Automation Systems: the R-Fieldbus Approach. In Proceedings of the 2000 IEEE International Workshop on Factory Communication Systems, pp. 319-326.

Pacheco, F., Pereira, N., Marques, B., Machado, S., Marques, L., Pinho, L. and Tovar, E. (2002). Industrial Multimedia put into Practice. In Proceedings of the 7th CaberNet Radicals Workshop, Bertinoro, Forlì, Italy.

Pereira, N., et al. (2002). Integration of TCP/IP and PROFIBUS Protocols. In WIP Proceedings of the 2002 IEEE International Workshop on Factory Communication Systems, Vasteras, Sweden.

Rauchhaupt, L. (2002). System and Device Architecture of a Radio Based Fieldbus – The RFieldbus System. In Proceedings of the 2002 IEEE International Workshop on Factory Communication Systems, Vasteras, Sweden.

Tovar, E. and Vasques, F. (1999). Real-Time Fieldbus Communications Using PROFIBUS Networks. *IEEE Transactions on Industrial Electronics*, vol. **46**, no. 6, pp. 1241-1251.