# Analysis of distributed multi-periodic systems to achieve consistent data matching

Nadège Pontisso, Philippe Quéinnec, Gérard Padiou

# Analysis of Distributed Multi-Periodic Systems to Achieve Consistent Data Matching

(NOTERE 2010 extended version)

Nadège Pontisso, Philippe Quéinnec and Gérard Padiou
Institut de Recherche en Informatique de Toulouse
Université de Toulouse, France
Email: {nadege.pontisso, queinnec, padiou}@enseeiht.fr

***Abstract*—Distributed real-time architecture of an embedded system is often described as a set of communicating components. Such a system is data flow (for its description) and time-triggered (for its execution). This work fits in with these problematics and focuses on the control of the time compatibility of a set of interdependent data used by the system components.**

**The architecture of a component-based system forms a graph of communicating components, where more than one path can link two components. These paths may have different timing characteristics but the flows of information which transit on these paths may need to be adequately matched, so that a component uses inputs which all (directly or indirectly) depend on the same production step. In this paper, we define this temporal data-matching property, we show how to analyze the architecture to detect situations that can cause data matching inconsistencies, and we describe an approach to manage data matching that uses queues to delay too fast paths and timestamps to recognize consistent data.**

***Index Terms*—Distributed system, component-based architecture, real-time, data consistency**

## I. Introduction

Distributed systems are now often built by assembling components which are independently developed or off-the-shelf, and the designer is faced with various challenges, especially when real-time is involved [1]. Various techniques have been proposed to solve interconnection difficulties [2], such as wrapping to expose a regular interface. In a real-time context, these components must be appropriately scheduled using periods, deadlines, priorities, etc [3]. Nevertheless, some problems remain when multiple paths connect two components. Indeed, the correct behavior of a component depends on correct or valid inputs. Independently of the semantic constraints of the inputs (e.g. belonging to a specific range of values), the time validity is also an important aspect in embedded systems. This time validity is often described in terms of availability (having inputs at the right time to start a task) and freshness (having recent enough inputs). Some works have studied the case where a component uses several inputs and these inputs respect a time consistency constraint such as having been produced at the same time. But this constraint is not sufficient: in a complex architecture, an intricate component graph leads to several paths between two components. In such a case, inputs of a component depend on the outputs of the *same* component (a source) by *several paths*. As a path links several components which consume and produce data, this dependency is not on the source value itself, but on the step at which it was produced. Our work fits in this problematic: how can the inputs of a component be consistent with regard to the production step of another component in the situation where several independent paths link these two components?

The data consistency is achieved by delaying fast paths until an adequate matching of inputs is possible. We approach this problem by analyzing the component graph to identify structures where two components are linked by several paths. If two paths have a really asymmetric nature, buffers are used to introduce a delay on the fastest path. In the general case, queues are used to keep data until the slowest data have arrived. As all values are not necessarily useful, we introduce filtering queues which keep only part of their inputs. We present results on the size of the required queues. These results are obtained in the context of periodic components, but make neither assumptions nor constraints on the scheduling.

The paper is organized as follows. Related works are presented in section II. Section III introduces an extensive example, describes what is a consistent data matching, and defines the computation and communication model. In section IV, we present the analysis of the component graph. Section V describes data consistency management, the queue size computations, and the application on the example.

## II. Related Works

In a real-time system, the freshness of data is a standard property. Freshness means that the system uses values which are as recent as possible, or in a specific domain of time validity. But this freshness property is not enough for some applications. Let's consider a toy example (figure 1). This system computes $2x + 3x$, where $x$ comes from an initial component $C_1$, $C_2$ and $C_3$ are used for multiplication, and a last component $C_4$ adds the results of theses multiplications. When $C_1$ emits a flow of values, $C_4$ must not carelessly mix values coming from $C_2$ and $C_3$ but has to add values corresponding to the same $x$. If it behaves like this, we say that $C_4$ does a consistent data matching. If $C_2$ computation takes twice as much time as $C_3$, using freshness only (using the most recent values which reach $C_4$) leads to inconsistent results.

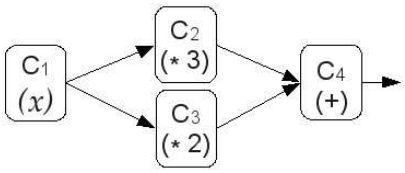


Fig. 1. Computation of $2x + 3x$

Such a system fits well in the synchronous dataflow (SDF) paradigm [4], [5]. SDF is a special case of dataflow, where a program is represented by a directed graph in which each node (called block) represents a computation and each edge specifies a FIFO buffer. In the SDF paradigm, the execution of a block is enacted when it has enough inputs. The objective of the static analysis of a SDF program is to find the necessary buffers between blocks and a scheduling such that a block is executed when its inputs are available.

Data matching is not the goal of SDF graphs. In this toy example, as the system is pure dataflow, consistent data matching can be obtained using SDF analysis. However, SDF theories cannot be used if the system is not a pure data flow system, that is to say if the components are fired based on conditions other than token availability. Particularly, SDF cannot be used if the components are time-triggered.

Moreover, forcing a scheduling to solve this data matching problem may be incompatible with other constraints, such as resources consumption or CPU availability, which are traditionally solved by scheduling analyzes: our goal is to analyze a system without considering a scheduling or a specific scheduler, neither do we want to compute a scheduling.

In the field of dataflow or database, studies mainly focus on the freshness of data (for instance [6], [7], or [8] for an extensive list of references). In [9], the authors determine an algorithm which computes which data need to be up-to-date taking data relationships into consideration. In [10], the variables semantics and their timed validity domain are used to optimize the transaction scheduling in databases. In [11], OCL constraints are used to define the validity domain of variables, and a variation of TCTL is used to check the system behavior and to prevent a value from being used out of its validity domain. However, these works do not consider consistency of *sets* of values.

In [8], the authors introduce a "mutual consistency" between objects in a database. They recognize that guaranteeing individual freshness of objects is insufficient as objects may be related to one another, and that the system should present a logically consistent view of the objects. Their work deals with non-preemptible periodic transactions, and they seek either the right periods and relative deadlines which would guarantee mutual consistency, or if a given set of transactions with their known parameters guarantee mutual consistency. In a sense, they are looking for a correct scheduling of actions so that mutual consistency is preserved. Our work differs from their in that we make similar assumptions concerning the scheduling but have no influence on it.

In [12], the authors do a similar work distinguishing *image objects* and *derived objects*. Image objects are periodically sampled from outside sensors and derived objects are computed from the values of a set of objects. To capture a mutual consistency constraint on the set of values used to compute a derived object, they introduce the notion of *dispersion*. The *age* of a derived object is defined by the ages of the used objects to compute it, and not by the date at which the computation occurs. Given a set of periodic preemptible transactions which read image or derived objects and update derived objects, their goal is to find which concurrency control strategy performs the best. Again, the goal is to find a correct scheduling of the transactions.

Consistency in distributed systems is also an old problem. However it is mainly done from a logical point of view, yielding causal or total order of operations to ensure consistency of values. Some works exist which introduce real-time constraints in broadcasting. For instance $\Delta$-causal protocols ensure the causal consistency of messages arriving by $\Delta$. Research on this topic [13] has concentrated on adaptation issues (adjusting $\Delta$) and optimizing the transmission (reducing the bandwidth overhead by minimizing piggybacking information). The goal of $\Delta$-causality is to favor latency even if ignoring a too late message leads to breaking causality chains. In our case, we seek a consistent matching of messages travelling by different paths. Latency is imposed by the slowest path, and messages on faster paths are delayed to enable this matching.

Our work differs from the works presented above mainly because our goal is not to compute a system scheduling to solve our problem of data matching. Neither do we consider that we know the final scheduling of components or their implantation (for example, the number of CPU). This approach allows to manage systems composed by black boxes that we cannot constrain to have a "good" behavior, for example, we cannot constraint when the components read their inputs. Moreover, even with a configurable system, acting on scheduling can be insufficient to solve data matching problems.

Prior work was done considering same frequency components [14] and it used solutions similar to SDF. In this paper, we consider multiple frequency systems, and it brings forth radically different solutions. An outline of the general analysis was presented in [15]. This paper differs by considerably enhancing this analysis, especially with regard to the filtering queues. Moreover, the full genuine example has not been published before.

## III. Consistent Data Matching

### A. Application Example

Our application example comes from the FUEGO project. The component graph has been developed in collaboration with Thales Alenia Space. FUEGO objective is to detect fires and eruptions, and to observe their evolutions. The system has been conceived as a constellation of satellites in low earth orbit. Each satellite is equipped with an observation instrument (a narrow area sensor) and with a detection instrument (a wide

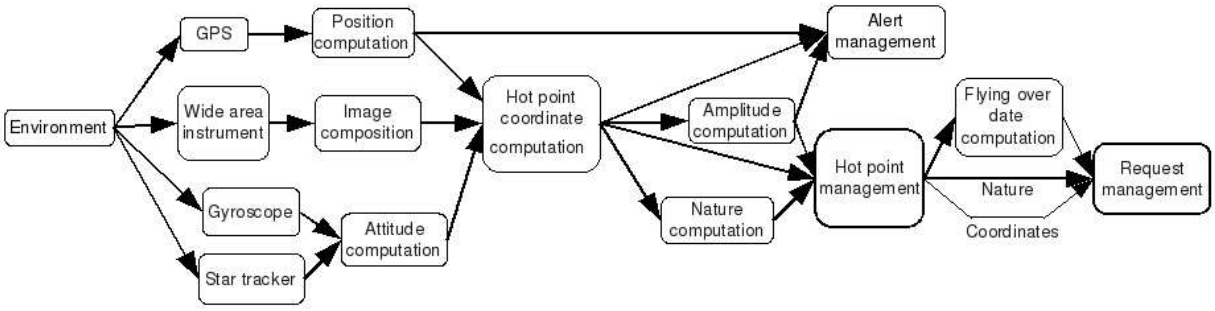


Fig. 2. Application: A Fire Detection Satellite

| Name | Period (in ms) | Minimal Execution Time | Maximal Execution Time |
|---|---|---|---|
| GPS | 1000 | 100 | 200 |
| Position computation | 60 | 20 | 40 |
| Alert management | 1000 | 50 | 200 |
| Wide area instrument | 100 | 60 | 70 |
| Image composition | 1000 | 200 | 400 |
| Coordinate computation | 1000 | 100 | 500 |
| Amplitude computation | 1000 | 20 | 30 |
| Nature computation | 1000 | 30 | 40 |
| Hot point management | 1000 | 50 | 200 |
| Flying over date computation | 1000 | 30 | 30 |
| Request management | 1000 | 50 | 150 |
| Gyroscope | 60 | 20 | 30 |
| Star tracker | 120 | 40 | 60 |
| Attitude computation | 60 | 20 | 30 |

TABLE I
APPLICATION EXAMPLE PARAMETERS

area sensor) which is pointed in front of the satellite. The detection instrument detects fires or eruptions. In such a case, an alarm is sent to a ground mission center and the satellite is requested to do an observation of the zone as soon as possible. A ground control center gathers all observations requests and allocate them between the satellites of the constellation.

We only study the system part in relation with the wide area detection instrument (figure 2). The GPS allows to compute the satellite position. The wide area sensor takes pictures which are linked to compose an image of a wide area. The data sent by the gyroscope and the star tracker are used to compute the satellite attitude (the angle the satellite makes with the earth).

The hot point coordinate computation is made using the image, the satellite position, and its attitude. Having detected a hot point, the system computes its amplitude and its nature (fire or eruption). The coordinate of the hot point, its nature and its amplitude are analyzed by the hot point management component. It records it if this point is new or if it has evolved. The amplitude and the coordinate of the hot point and the position that the satellite had when this point was detected are sent to the ground by the alert management component.

Using the hot point parameters and the actual parameters of the satellite, a component computes the date when the observation instrument flies over the hot point. This date, the point nature, and its coordinates are stored by the request management component. It schedules the hot point observations the satellite has to achieve. Table I displays the parameters of our system. In the numeric applications in this paper, we use null communication times between components to simplify the presentation. The actual analysis uses non null values.

### B. Example of Data Matching Problem

In figure 2, the alert management has to send to the ground a message composed of three values: the coordinates of the detected hot point, its amplitude, and the position that the satellite had when this point was detected. The coordinate computation needs the satellite position to produce the coordinates. The amplitude computation needs the coordinates, hence it also indirectly depends on the satellite position. Thus, the alert management uses three values which depend on the position produced by the position computation component. This set of three values is considered as consistent if they depend on a same computation step of the position computation.

### C. Consistency Formalization

We consider a distributed computation which is modelled by sending events (noted $s$), delivery events (noted $d$) and internal events (noted $i$). We note $s_C$, $d_C$ or $i_C$ an event occurring on a component $C$. We note $d^{C'}$ a delivery event corresponding to the reception of a message coming from the component $C'$ and $d_C^{C'}$ a delivery event occurring on $C$ and corresponding to a message coming from $C'$. The internal events correspond to computation steps and we consider that their durations are (logically) null. We note $\prec$ the relation of temporal precedence between events on a same component.

*1) Direct Influence Relation:* The direct influence relation $\rightarrow$ is defined by:

- For a message $m$, the sending influences its delivery $s(m) \rightarrow d(m)$.

- an internal event influences the sendings that directly follow until the next internal event:
  $\forall s_C, i_C : i_C \prec s_C \wedge \nexists i'_C : i_C \prec i'_C \prec s_C \Rightarrow i_C \rightarrow s_C$
- the last delivery coming from a given component influences the following internal events until the next delivery coming from the same component:
  $\forall d_C^{C'}, i_C : d_C^{C'} \prec i_C \wedge \nexists D_C^{C'} : d_C^{C'} \prec D_C^{C'} \prec i_C \Rightarrow d_C^{C'} \rightarrow i_C$

*2) Influence Relation:* The influence relation, noted $\rightarrow^*$, is constructed by transitive closure of $\rightarrow$.

This influence relation is stronger than the usual causality relation (also called happened-before relation): if $a$ influences $b$ then $a$ causally precedes $b$; the converse is not necessarily true. The influence relation is closer to a memory model description of a distributed system than to a message passing one.

*3) Influence Past:* We define the influence past of an event $i$ as the set of internal events that influence $i$ added to itself:

$$\text{past}(i) \triangleq \{i' \mid i' \rightarrow^* i\} \cup \{i\}$$

*4) Strictly Consistent Execution:* We note $S|C$, the set of events from the set $S$ which occur on component $C$. An internal event set is consistent if it contains at most one internal event by component. An execution is strictly consistent if the influence past of each internal event is a consistent event set:

$$\forall i : \forall C : \text{cardinality}(\text{past}(i)|C) \leq 1$$

*5) Relaxed Consistency:* We consider that each component has a real-time clock. We note $date(i)$, the time at which the internal event $i$ occurs. We call $span(S)$ the maximum time span between events in $S$: $span(S) = \max_{i_1,i_2 \in S}(date(i_1) - date(i_2))$. A $\tau$-relaxed consistent execution is such that:

$$\forall i \ : \ \forall C \ : \ span(past(i)|C) \leq \tau$$

A 0-relaxed consistent execution is actually a strictly consistent execution. Note that in this definition, we use the date of events which are all on the same component: a global synchronous clock is never required.

*6) Consistent Data matching:* If we consider data instead of events, we say that a value $d$ produced by an execution step $S$ influences a value $d'$ produced by a step $S'$ if the internal event corresponding to $S$ influences the one corresponding to $S'$. A data set is consistent if the union of the influence pasts of the internal events which produce the data is consistent. A component does a consistent data matching if its inputs form a consistent data set for each execution step.

### D. Model

We solve our data matching problem in a general setting that does not depend on an effective scheduling or a particular scheduler. We define a general abstract model that grabs just enough requirements to solve our problem without restricting too much the systems where the solution is applied.

*1) Computation Model:* Components are time triggered and we impose that they have a fixed period. Different components may have different periods. During one step of its period, the component reads exactly once every input port, then it performs its computation, and then it writes exactly once every output port. The only requirement is that a component finishes its step before the end of its period. These weak assumptions allow to fully abstract any scheduling considerations. A component step can be instantaneous or can take as long as the full period. Preemption may split it into pieces. In consecutive periods, component steps may have different durations or different relative start times. Different readings of one step can be done instantaneously or separately, and similarly for writings.

*2) Communication Model:* In the same spirit, we make few assumptions about communication. We assume that communication is FIFO and reliable. We use a minimum and a maximum communication time. These boundaries are defined for each couple of components and can vary in the system. By allowing null values, we model a non-transactional memory. On the other hand, non-null values model a communication network. The strict upper bound is natural in a real-time context, for instance when communication is performed via a synchronous bus.

*3) Model Parameters:* To analyze a system queue sizes, some parameters are useful. The mandatory parameters are:

- $T_C$ : the period of component $C$;
- $\Delta_{CC'}$ : a maximum communication delay between components $C$ and $C'$. An upper bound is sufficient.

Optional parameters are (may be set as zero if unknown):

- $e_C$ : a lower bound of the execution time of a step of component $C$;
- $\delta_{CC'}$ : a minimum communication delay between components $C$ and $C'$. A lower bound is sufficient.

## IV. System Analysis

### A. Graph Analysis

To be able to analyze the system, we analyze the component graph as an oriented graph. We are able to easily found problematic configurations searching for subgraphs that we called spindles which detect that several paths exist between two components.

*1) Graph Properties:*

*Simple Path:* A path is a sequence of nodes where there exists an edge between two consecutive nodes. We call a simple path, a path in which all nodes are distinct.

*Separated Paths:* Two simple paths with the same extremities are separated if and only if their sequences do not have any nodes in common except the initial and final nodes.

*2) Spindle:* A *spindle* between two nodes is the set of all simple paths connecting these nodes such that at least two separated paths exist in this set. The initial node of these paths is called the *source*, and their final node the *sink*. In figure 2, the set of the three simple paths between the position computation component and the alert management is a spindle.

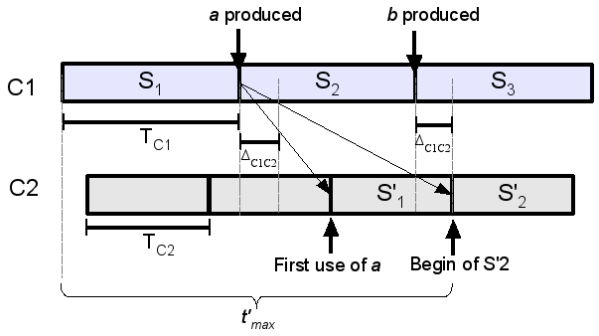


Fig. 3. $t_{max}$ Evaluation

An inconsistent data matching can occur between a component couple $(C, C')$ if and only if there is a spindle between them.

### B. Spindle Analysis

When spindles are found, we analyze how their paths influence the data used by the sink components.

*1) Maximum Path Time:* Let's consider a path $P = (C_1, C_2, ..., C_n)$. We note $t_{max}(P)$ the maximum time between the beginning of the execution of $C_1$, which sends a value $v$, and the use by $C_n$ of a value influenced by $v$ through the path $P$.

To find the maximum path time, the worst case is when each component uses data at the beginning of its period and sends data at the end, and when the phase difference maximizes the lag between the sending and the use of a value.

The maximum time $t'_{max}$ between the beginning of the execution of $C_1$, which sends a value $a$ to $C_2$ and the use by $C_2$ of this value through the path $P$ depends on the time during which $C_2$ can use $a$. As we see in figure 3,

$$t'_{max} = 2T_{C_1} + \Delta_{C_1C_2}$$

First, $C_1$ executes a step $S_1$ which lasts one period and produces the value $a$. This value can be used by $C_2$ after a delay $\Delta_{C_1C_2}$ and until it receives a new value. A new value $b$ is produced by $C_1$ at the end of the step $S_2$. This new value is available for $C_2$ after a delay $\Delta_{C_1C_2}$. We place $C_2$ such that it starts a step at this moment. Thus, at the same time, $C_2$ starts a step and a new value is available. As we do not know what happens exactly, we choose the worst case for $t'_{max}$, which is that $C_2$ starts its computation without reading the value $b$.

The maximum time between the beginning of the execution of $C_1$, which sends a value $v$, and the use by $C_n$ of a value influenced by $v$ through the path $P$ is:

$$t_{max}(P) = \sum_{i=1}^{n-1}(2T_{C_i} + \Delta_{C_iC_{i+1}})$$

*2) Minimum Path Time:* Let $P = (C_1, C_2, ..., C_n)$ be a path. We note $t_{min}(P)$ the minimum time between the beginning of the execution of $C_1$, which sends a value $v$, and the use by $C_n$ of a value influenced by $v$ through the path $P$. $t_{min}(P)$ is the sum of the minimum execution times and the minimum communication delays along the path.

$$t_{min}(P) = \sum_{i=1}^{n-1}(e_{C_i} + \delta_{C_iC_{i+1}})$$

*3) Maximum Gap Between Two Input Data:* Let's consider a spindle between $C_\alpha$ and $C_\beta$ composed of two paths: $P_A = (C_\alpha, C_2, ...C_{n-1}, C_\beta)$ and $P_B = (C_\alpha, C'_2, ...C'_{m-1}, C_\beta)$. $P_A$ has a size of $n$ and $P_B$ a size of $m$. $C_{n-1}$ sends a value $A$ to $C_\beta$ and $C'_{m-1}$ sends a value $B$.

$C_\beta$ uses the values $A$ and $B$. They are influenced by values produced by $C_\alpha$. We analyze the time gap between the starting time of the step of $C_\alpha$ which produced the value which influences $A$ and the starting time of the step of $C_\alpha$ which produced the value which influences $B$.

The maximum gap, noted $gap_{AB}$, is obtained when $A$ is produced using the maximum path time and $B$ using the minimum path time. Moreover, $A$ is read by $C_\beta$ at the beginning of its period and $B$ is read as later as possible.

$$gap_{AB} = t_{max}(P_A) + T_\beta - e_\beta - t_{min}(P_B)$$

Note that $gap_{AB} \neq gap_{BA}$. To analyze a spindle, we have to know the two values $gap_{AB}$ and $gap_{BA}$.

## V. Data Matching Management

Analyzing every spindle in the component graph, we are able to know the worst gap that we can have between two data. For the analyzed application, the designer has to know if this gap is acceptable. If not, the objective is to reduce it.

### A. Imposed Delay

Reducing $gap_{AB}$ can be achieved by introducing a delay into the path $P_B$ in order to increase $t_{min}(B)$. To reach this effect, queues are set on the sink component input. For every execution step, the sink uses the queue head. Data entering the queue take time to propagate to the head depending on the size of the queue. This approach is not so far from an SDF solution.

This lag increases $t_{min}(B)$ (therefore decreasing $gap_{AB}$) but it also increases $t_{max}(B)$, and so it increases $gap_{BA}$. We have to take care of these two effects before using an imposed delay. Moreover, we are never able to guarantee that the set used by the sink component is strictly consistent.

### B. Timestamping

To compose a consistent set with a given consistency tolerance, the sink component must be able to select which data it needs among the received ones. Queues are used on the inputs of the sink, and for each step, the sink has the choice among the data kept in the queues. Thus, the sink needs to know the influence past of a value, which is the same as the influence past of the internal event which has produced this value.

*1) Marks:* A *mark* is a couple $\langle Component\_Id, value\rangle$, where values are taken from any infinite set. Each component has a logical clock $H(C)$ that marks the data produced by the component. This clock "counts" the number of computation steps executed by the component. Thereby, one mark, noted $M_i$, corresponds to a unique internal event $i$, and conversely.

*2) Timestamps:* A *timestamp* is a set of marks that holds the influence past of an event. The timestamp carried by the event $a$ is noted $E_a$. The folowing timestamping rules are used:

- The set $Input(i_C)$ is composed by all the delivery events which were used to compute the internal event $i_C$:
  $Input(i_C) = \{d_C^{C'} : (d_C^{C'} \prec i_C \wedge \nexists D_C^{C'} : d_C^{C'} \prec D_C^{C'} \prec i_C)\}$
- The timestamp of a delivery event is equal to the corresponding sending timestamp.
- The timestamp of a sending event is equal to the timestamp of the most recent internal event that precedes it.
- The timestamp of an internal event $i$ of a component $C$ is equal to the union of timestamps of the delivery events used during this computation step, added to its own mark.

$$E_i = \bigcup_{d \in Input(i)} E_d \ \cup \{\langle C, H(C)\rangle\}$$

and $H(C)$ is incremented.

*Lemma 1 (Marks and Timestamps):*

$$E_i = \{M_i\} \cup \{M_j \mid j \rightarrow^* i\}$$

*Proof:* We note, where $i$ and $i'$ are internal events:

$$\begin{aligned} i \overset{1}{\mapsto} i' &\triangleq \exists s, d : i \rightarrow s \rightarrow d \rightarrow i' \\ i \overset{n}{\mapsto} i' &\triangleq \exists i'' : i \overset{1}{\mapsto} i'' \wedge i'' \overset{n-1}{\mapsto} i' \end{aligned}$$

By the stamping rules :

$$\begin{aligned} E_i &= \{M_i\} \cup \bigcup_{j \mid j \overset{1}{\mapsto} i} E_j \\ &= \{M_i\} \cup \bigcup_{j \mid j \overset{1}{\mapsto} i} \{M_j\} \ \cup \bigcup_{j \mid j \overset{2}{\mapsto} i} E_j \\ &\vdots \\ &= \{M_i\} \cup \bigcup_{n \geq k \geq 1} \bigcup_{j \mid j \overset{k}{\mapsto} i} \{M_j\} \ \cup \bigcup_{j \mid j \overset{n+1}{\mapsto} i} E_j \end{aligned}$$

All $\mapsto$ chains are bounded (initial event)

$$\begin{aligned} &= \{M_i\} \cup \bigcup_{k \geq 1} \bigcup_{j \mid j \overset{k}{\mapsto} i} \{M_j\} \\ &= \{M_i\} \cup \{M_j \mid j \rightarrow^* i\} \end{aligned}$$

□

*Theorem 1:* The timestamps encode the influence relation:

$$i \rightarrow^* i' \Leftrightarrow E_i \subsetneq E_{i'}$$

*Proof:* The direct implication is deduced from the stamping rules and the transitivity of $\rightarrow^*$:

If $i \rightarrow s \rightarrow d \rightarrow i'$, then from the stamping rules:
$\Rightarrow E_{i'} = \{M_{i'}\} \cup E_i \cup X$
$M_{i'}$ is unique and only come from $i'$.
As $i' \not\rightarrow^* i \wedge i \neq i', M_{i'} \notin E_i$
$\Rightarrow E_i \subsetneq E_{i'}$

Using the transitivity of $\rightarrow^*$:
$i \rightarrow^* i' \Leftrightarrow i \rightarrow ... \rightarrow i' \Rightarrow E_i \subsetneq E_{i'}$

The reverse implication comes from the stamping rules and lemma 1:

$$\begin{aligned} E_i \subsetneq E_{i'} \ &\Rightarrow M_i \subsetneq E_{i'} \text{ (lemma 1)} \\ &\Leftrightarrow M_i \subsetneq \{M_{i'}\} \cup \{M_j \mid j \rightarrow^* i'\} \text{ (lemma 1)} \\ &\text{A mark is unique and } i \neq i' \Rightarrow M_i \neq M_{i'} \\ &\Leftrightarrow M_i \subsetneq \{M_j \mid j \rightarrow^* i'\} \\ &\Rightarrow \exists j : M_i = M_j \wedge j \rightarrow^* i' \\ &\text{A mark is unique:} \\ &\Leftrightarrow i \rightarrow^* i' \end{aligned}$$

. □

*Theorem 2:* We note $(E|C)$, the set of marks generated by a component $C$ contained in the set $E$. An execution is consistent if and only if there does not exist several marks coming from a same component in the timestamp of each internal event:

$$\text{Consistent execution} \triangleq \forall i : \forall C : \text{cardinality}(E_i|C) \leq 1$$

*Proof:*

$$\begin{aligned} E_i &= \{M_{i'} \mid i' \rightarrow^* i\} \cup \{M_i\} \\ &= \{M_{i'} \mid i' \rightarrow^* i \vee i' = i\} \\ &= \{M_{i'} \mid i' \in past(i)\} \end{aligned}$$

As two distinct events cannot generate the same mark, the number of marks and the number of events are equal:

$$card(\{M_{i'} \mid i' \in past(i)\}|c) = card(past(i)|c)$$
(with or without the restriction on $c$), and so
$$card(E_i|c) = card(past(i)|c)$$

The condition is equivalent to the consistency condition defined above.

□

*3) Relation to Other Encodings:* Our work is in the same spirit as classical works by Lamport [16] and Mattern [17], which encode the causality relation in distributed computing. However, our influence relation is different from the usual causality relation, and we use a different encoding. The local clock does not act like a Lamport clock (the local clock is not updated using the message timestamp) and the piggybacked timestamps are not Fidge-Mattern vector clocks (we can have more than one mark from the same component).

*4) Mark Generators and Controllers:* An inconsistent data matching can occur between a component couple $(C, C')$ if and only if there is a spindle between them. Consequently, to reduce the number of used marks, only spindle sources are mark generators. Moreover, only sinks are controllers, that is to say components that check the consistency between the marks coming from their spindle source.

### C. Queue Handling

Data can be used as component inputs only when they make a consistent data set. It implies that data coming using the faster paths have to wait for the appropriate marked data coming through the slower paths. This requires to use queues on component inputs to store data coming faster. We analyze the necessary queue sizes in the field of relaxed data matching. As strict consistency is a relaxed consistency of tolerance 0, the results apply to strict data matching.

In the context of relaxed data matching, we use filtering queues. A filtering queue stores data it receives following a given rhythm, for example the queue stores one value out of three. The flexibility of relaxed data matching is exploited to reduce the queue sizes using filtering queues. A regular queue is a filtering queue with a rhythm of 1.

To manage the queues, we choose to keep a value until a more recent value is used. When a value is used, older data are erased but the used one remains buffered. If the frequency of the receiver component is higher than the sender one, the receiver uses the same value for several steps.

In the general case, for a given spindle, the sink has an arbitrary number of inputs involved in this spindle. To find the necessary queue sizes on each input, we analyze the paths two by two. For each couple, the queue sizes of the two inputs are obtained. Then, for each input, we keep the highest queue size that was obtained from the analysis.

In the following, let's consider a spindle between $C_\alpha$ and $C_\beta$ composed of two paths: $P_1 = (C'_1, C'_2, ..., C'_n)$ and $P_2 = (C_1, C_2, ..., C_m)$ where $C'_1 = C_1 = C_\alpha$ and $C'_n = C_m = C_\beta$. We tolerate a gap of $\tau$ between the step starting times of $C_\alpha$ that produce values the $C_\beta$ inputs are influenced by.

*1) Queue Requirements:* First, we have to find where we need a queue.

- If $t_{max}(P_1) > t_{min}(P_2) + \tau$, then it means that the path $P_2$ can be shorter than the path $P_1$ and that the tolerance is not sufficient to reduce this gap. So we need a queue between $C_{m-1}$ and $C_\beta$.
- If $t_{max}(P_2) > t_{min}(P_1) + \tau$, then we need a queue between $C'_{n-1}$ and $C_\beta$.
- If both conditions are true then we need both previous queues. In this case, $P_1$, as well as $P_2$, can outperform the other path.

For the communication between components where the receiver is not a spindle sink, we use a buffer of size one. Each new coming value replaces the previous one.

*2) Queue Size Evaluation:* Let's suppose that $t_{max}(P_1) > t_{min}(P_2) + \tau$. The required and sufficient filtering queue size between $C_{m-1}$ and $C_\beta$ must be determined. The objective is to determine the maximum number of data that must be buffered waiting for a consistent data set to be constructed. We seek this maximum size such that, when the queue is full and a new value comes, it is guaranteed that the consistent value corresponding to the oldest value $v$ will never arrive. Thus, $v$ is useless and can be removed.

The required queue size between $C_{m-1}$ and $C_\beta$ corresponds to the maximum number of data that can be stored in the queue between two data removals by $C_\beta$.The worst case happens when the maximum path time is made by $P_1$ and where $P_2$ takes as little time as possible.

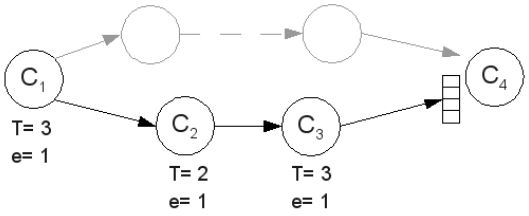


Fig. 4. Example of Spindle

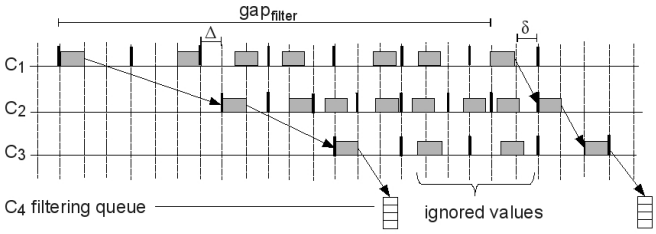


Fig. 5. Behavior of a Filtering Queue

Let's assume that $C_\beta$ uses a regular queue for the path $P_1$ and a filtering queue for the path $P_2$. This filtering queue has a size of $N'$ ($N' \geq 2$) and it stores one value out of $R$.

We use a simple example to present the characteristics of filtering queues. Figure 4 displays a spindle between the components $C_1$ and $C_4$, and the parameters of the components. We use simplified parameters to make easier the illustration. The input of $C_4$ coming from $C_3$ uses a filtering queue. We analyze the black path, and we consider that the communication times between two components are equal to 1 and that the filtering queue stores one value out of three.

Figure 5 illustrates the biggest gap that we can have between two step starting times of the source which produce values that influence two consecutive values in the filtering queue. The tail of an arrow corresponds to the time when a value is produced and its head the time when it is read by another component, or, concerning the value produced by $C_3$, the time when the value is recorded into the queue. The biggest gap is found when the first queue value comes from a source step as old as possible and the second value from a step as recent as possible.

If we consider the path $P_2 = (C_1, ..., C_{m-1}, C_\beta)$ with a filtering queue which stores one value out of $R$ between $C_{m-1}$ and $C_\beta$, the biggest gap between two consecutive data is:

$$\begin{aligned} gap_{filter}(P_2) &= \sum_{i=1}^{m-2} [2T_{C_i} + \Delta_{C_i C_{i+1}}] + (R+1)T_{C_{m-1}} \\ &\quad - e_{C_{m-1}} - \sum_{i=1}^{m-2} [e_{C_i} + \delta_{C_i C_{i+1}}] \\ &= t_{max}(P) - t_{min}(P) + (R-1)T_{C_{m-1}} \\ &\quad - (\Delta_{C_{m-1}C_\beta} - \delta_{C_{m-1}C_\beta}) \end{aligned}$$

If $\tau$ is the expected tolerance, we can find the necessary

recording rhythm $R$ of the queue. The relation between $\tau$ and $R$ is provided by the $gap_{filter}$ computation. To manage a tolerance of $\tau$, we need that:

$$gap_{filter}(P_2) \leq 2\tau$$

The rhythm $R$ of the filtering queue must respect:

$$R \leq \max(1, \frac{2\tau - t_{max}(P) + t_{min}(P) + \Delta_{C_{m-1}C_\beta} - \delta_{C_{m-1}C_\beta}}{T_{C_{m-1}}} + 1)$$

If the rhythm of the filtering queue does not respect this condition, it is impossible to manage a relaxed consistency of tolerance $\tau$.

Knowing the value of $R$, we compute the necessary queue size. When the sink reads a value in the filtering queue at time $t$, the oldest value it can use is influenced by a value produced by a source step which necessarily started before $t - t_{oldmin}(P_2)$:

$$\begin{aligned} t_{oldmin}(P_2) = & \sum_{i=1}^{m-2} [e_{C_i} + \delta_{C_i C_{i+1}}] + (R-1)T_{C_{m-1}} + e_{C_{m-1}} \\ & + (N'-2)RT_{C_{m-1}} + e_{C_{m-1}} + \delta_{C_{m-1}C_\beta} \\ t_{oldmin}(P_2) = & \; t_{min}(P_2) + e_{C_{m-1}} + (N'R - R - 1)T_{C_{m-1}} \end{aligned}$$

At time $t$, in the worst case, on the path $P_1$, the sink has a value influenced by a value produced by a source step which started at $t - t_{max}(P_1)$.

To manage data matching, we have to provide a corresponding value coming from the path $P_2$. Considering relaxed data matching, this corresponding value must be influenced by a source value which was produced by a source step which started between $(t - t_{max}(P_1) - \tau)$ and $(t - t_{max}(P_1) + \tau)$.

The minimum queue size is obtained when:

$$t_{oldmin} = t_{max}(P_1) - \tau$$

The necessary queue size of the filtering queue is:

$$N' = \left\lceil \frac{t_{max}(P_1) - \tau - t_{min}(P_2) - e_{C_{m-1}} + (R+1)T_{C_{m-1}}}{RT_{C_{m-1}}} \right\rceil$$

This queue size allows to store enough data between $C_{m-1}$ and $C_\beta$ to guarantee a data matching with values coming from the path $P_1$. But we have also to take into account the worst data utilization case of the sink. The worst case happens when the data are used at the beginning of a $C_\beta$ period and when the use of a new data is done as late as possible, that is to say when the component has only its execution time left. So, in the worst case, a data is erased $2T_{C_\beta} - e_{C_\beta}$ after its last use.

If $2T_{C_\beta} - e_{C_\beta} > RT_{C_{m-1}}$, we have to add space to store the data that can come into the queue between two sink readings. The final necessary queue size $N$ is:

$$N = \left\lceil \frac{t_{max}(P_1) - \tau - t_{min}(P_2) - e_{C_{m-1}} + (R+1)T_{C_{m-1}}}{RT_{C_{m-1}}} + \frac{2T_{C_\beta} - e_{C_\beta}}{RT_{C_{m-1}}} \right\rceil$$

With strict consistency and a regular queue, $R = 1$ and $\tau = 0$. The necessary queue size becomes:

$$N = \left\lceil \frac{t_{max}(P_A) - t_{min}(P_B) + 2T_{C_\beta} - e_{C_\beta} - e_{C_{m-1}}}{T_{C_{m-1}}} \right\rceil + 2$$

### D. Application Example Analysis

We apply the previous results on the application example figure 2. For the spindles where the path temporal parameters are not very different, the necessary queues have an average size of 6. But the necessary queue size can be very large depending on the system parameters. If we want a strict consistency in the spindle between the position computation and the alert management, we found that we need a size of 102 on the alert management input which is directly linked with the position computation. This happens because we have a large difference between the period of the position computation (60 ms) and the one of alert management (1 second). Actually, we do not need to send the precise position with the alert sent to the ground. We place a filtering queue between the position computation and the alert management. If we tolerate a gap $\tau$ of 300 ms, we can have a recording rhythm of 9. The necessary queue size is 12. We can compare this result with the size of 102 that we need for the same spindle for strict data matching.

In some case, freshness has priority like in the spindle between the environment and the attitude computation. To compute the attitude as precisely as possible, the component has to use the most recent data coming from the gyroscope and the star tracker. Selecting data considering the matching on the environment has no sense here.

If the queue sizes are unacceptable with regard to the resource constraints, the architecture has to be modified. Very large queue sizes are a hint which points to an architectural problem. For example, if we want a strict consistency between the position computation and the alert management, this leads to a very large queue. Instead of having a direct link between this two components, the data sent by the hot point coordinate computation can be composed of the coordinate and the position value. Thus, we can erase the link between the position computation and the alert management, and eliminate the spindle.

## VI. Conclusion

In this article, we identify an important aspect of component-based distributed systems that is not treated in other works: matching of interdependent data. Our analysis is done as soon as the components, their characteristics, and their relations are known, but we consider few constraints on the system scheduling, so this allows us to analyze systems early in their development process.

We first detect the configurations that cause data matching problems, and then we propose a method to manage data matching using a timestamping mechanism to identify dependencies between data. We propose a notion of relaxed data matching and compute the necessary sizes of the queues we have to use on component inputs to manage these constraints.

As strict data matching is a special case of relaxed data matching, the results are applicable to strict data matching.

In some systems, the computed queue sizes are too large with regards to the resource constraints. If this situation happens, it means that the paths are too much unbalanced. It identifies that an architecture redesign is needed. On the other hand, if the queue sizes are acceptable, it means that data matching is guaranteed whatever the final system scheduling is. An open question is how more precise information about the scheduler can be used to reduce the queue sizes, for instance by asserting that certain inconvenient executions are actually prevented from happening. An other question is whether a less regular recording rhythm such as $(m, k)$-firm [18] may be more efficient and more suitable to model real-time network communication.

## REFERENCES


[1] A. Möller, M. Åkerholm, J. Fredriksson, and M. Nolin, "Evaluation of component technologies with respect to industrial requirements," in *30th EUROMICRO conference*. IEEE Computer Society, 2004, pp. 56–63.

[2] C. Szyperski, *Component Software – Beyond Object-Oriented Programming*, 2nd ed. Addison-Wesley, 2002.

[3] J. W. Liu, *Real-Time Systems*. Prentice Hall, 2000.

[4] S. S. Bhattacharyya, P. K. Murthy, and E. A. Lee, "Synthesis of embedded software from synchronous dataflow specifications," *Journal of VLSI Signal Processing Systems*, vol. 21, pp. 151–166, 1999.

[5] C. Fong, "Discrete-time dataflow models for visual simulation in Ptolemy II," Master's thesis, Electronics Research Laboratory, University of California, Berkeley, 2001.

[6] K. Ramamritham, S. H. Son, and L. C. DiPippo, "Real-time databases and data services," *Real-Time Systems*, vol. 28, no. 2-3, pp. 179–215, 2004.

[7] M. Xiong, S. Han, and K. Lam, "A deferrable scheduling algorithm for real-time transactions maintaining data freshness," in *26th IEEE Real-Time Systems Symposium (RTSS 2005)*, 2005, pp. 27–37.

[8] A. K. Jha, M. Xiong, and K. Ramamritham, "Mutual consistency in real-time databases," in *27th IEEE Real-Time Systems Symposium (RTSS 2006)*, 2006, pp. 335–343.

[9] T. Gustafsson and J. Hansson, "Data freshness and overload handling in embedded systems," in *12th IEEE Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA 2006)*, 2006, pp. 173–182.

[10] M. Xiong, R. Sivasankaran, J. Stankovic, K. Ramamritham, and D. Towsley, "Scheduling transactions with temporal constraints: Exploiting data semantics," in *17th IEEE Real-Time Systems Symposium (RTSS'96)*, 1996, pp. 240–253.

[11] S. Anderson and J. K. Filipe, "Guaranteeing temporal validity with a real-time logic of knowledge," in *23rd Conference on Distributed Computing Systems (ICDCS 2003)*. IEEE Computer Society, 2003, pp. 178–183.

[12] X. C. Song and J. W. S. Liu, "Maintaining temporal consistency: Pessimistic vs. optimistic concurrency control," *IEEE Transactions on Knowledge and Data Engineering*, vol. 7, no. 5, pp. 786–796, 1995.

[13] R. Baldoni, R. Prakash, M. Raynal, and M. Singhal, "Efficient $\Delta$-causal broadcasting," *International Journal of Computer Systems Science and Engineering*, vol. 13, no. 5, pp. 263–269, 1998.

[14] N. Pontisso, G. Padiou, and P. Quéinnec, "Real time data consistency in component based embedded systems," in *8th International Conference on New Technologies in Distributed Systems (NOTERE '08)*. ACM, 2008, pp. 1–6.

[15] N. Pontisso, P. Quéinnec, and G. Padiou, "Temporal data matching in component based real time systems," in *IEEE Symposium on Industrial Embedded Systems SIES2009*, Jul. 2009, pp. 62–65.

[16] L. Lamport, "Time, clocks and the ordering of events in a distributed system," *Communications of the ACM*, vol. 21, no. 7, pp. 558–565, 1978.

[17] F. Mattern, "Virtual time and global state in distributed systems," in *International Workshop on Parallel and Distributed Algorithms*. Elsevier, 1989, pp. 215–226.

[18] N. Jia, Y.-Q. Song, and R.-Z. Lin, "Analysis of networked control system with packet drops governed by (m,k)-firm constraint," in *6th IFAC international conference on fieldbus systems and their applications (FeT'2005)*. Elsevier, 2005, pp. 63–70.