Towards Formal Modeling and Verification of Context-Aware Systems

Taha Abdelmoutaleb Cherfia
LIRE Laboratory
Software Technologies and Information Systems Department, Constantine 2 University
Algeria
taha.cherfia@univ-constantine2.dz

Faïza Belala
LIRE Laboratory
Software Technologies and Information Systems Department, Constantine 2 University
Algeria
faiza.belala@univ-constanine2.dz

Kamel Barkaoui
Laboratoire CEDRIC
Conservatoire Nationale des Arts et Métiers
CNAM, Paris Cedex 03,
France
kamel.barkaoui@cnam.fr

Context-aware systems are an emerging class of mobile computing systems aiming to provide ubiquitous access to information, communication and computation. These systems are able to sense and adapt their behavior automatically to the current environmental context. In this paper, we present a formal approach based on bigraphical reactive systems for specifying and verifying the main features of context-aware systems. The proposed formalism provides a clear separation between the part of the system which is affected by the context and the remaining part. In order to illustrate its potential, we apply our approach through a motivating case study of a smart home system, and by using the Bigraphical Model Checker (BigMC) for verification purposes.

Formal Verification. Context-Aware Systems. Bigraphical Reactive Systems. Bigraphical Model Checker.

1. INTRODUCTION

Recently, context-aware systems are becoming one of the most promising fields in the wide range of ubiquitous computing (Weiser, 2002). These systems are able to dynamically adapt their behavior in response to changes on context information without an explicit user intervention.

In the literature, there are many definitions of the term “context”, but until now there is no universal one. In (Abowd et al., 2000), a generic definition has been proposed in which context is referred as “any information that can be used to characterize the situation of an entity. An entity is a person, place or object that is considered relevant to the interaction between a user and an application, including location, time, activities and the preferences of each entity”.

Nevertheless, the lack of a solid formal foundation in the most existing definitions, combined with the increasing complexity and diversity of context-aware systems, represent a clear challenge to model and verify such systems. Therefore, the formal modeling represents a crucial and delicate step to reduce complexity and enhance the verification of context-aware systems. As a result, many formal approaches have been introduced to deal with this issue; Pascal Zimmer (Zimmer, 2005) introduced a new process calculus, called *Context-Aware Calculus* (CAC in short), to formally describe the context-aware systems. Likewise, authors in (Siewe, Cau and Zedan, 2009) proposed a logical language CCA (*Calculus of Context-aware Ambients*) for the modeling and verification of context-aware systems.

Furthermore, according to (Birkedal, Debois and Hildebrandt, 2006), one of the principal aims for the theory of Bigraphical Reactive Systems (BRS in short) is to model ubiquitous systems, capturing mobile locality in the place graph and mobile connectivity in the link graph.

Among the recent BRS-based studies in the domain of context-aware systems, we can highlight the following: *Plato-graphical* models (Birkedal, Debois and Hildebrandt, 2006), context and actions (Xu, Xu and Lei, 2011), context and capabilities (Wang, Xu and Lei, 2011) and BiAgents (Pereira, Kirsch and Sengupta, 2012). Nonetheless, only the graphical representation of bigraphical reactive systems has been used to model context-aware systems and their evolution. There has been no information or formal definition of the relationship between the context changes and the system reactions. Furthermore, no formal verification has been performed within these approaches to investigate the correctness of the context-aware models.

Our proposed approach (Cherfia and Belala, 2014) is quite similar to the previous ones since it is based on BRS, but where the context-aware and context-unaware parts of the system, are clearly separated. Each one has its own reaction rules and by using the composition operation defined natively in BRS, we can describe, first the whole context-aware system and then, capture the relationship between the context changes and the system behavior.

Moreover, to illustrate the interest of our approach, we apply it, in this paper, to a simple smart home system focusing on the function of the lightning control service. Besides, in order to assess the feasibility and effectiveness of our proposed approach, we use the Bigraphical Model Checker (BigMC) (Perrone, Debois and Hildebrandt, 2013) to determine whether the composition operation satisfies the reachability property.

The rest of this paper is organized as follows. Section 2 presents a motivating case study of a context-aware home system. Section 3 gives an overview of bigraphical reactive systems. Section 4 briefly introduces our BRS-based approach for modeling the different aspects of context-aware systems. Section 5 describes how we use the BigMC to implement the smart home case study in order to validate the correctness of our proposed approach. Finally, conclusion and future work are given in Section 6.

2. MOTIVATING EXAMPLE

Along with the rapid proliferation of high technologies, particularly in the fields of electronic, communication and control, homes and the way we live in them have changed dramatically in the last decade. Today, the smart home research becomes one of the major sub-domains of ubiquitous computing. Many research institutes and well-known enterprises such as Apple, Microsoft, Cisco, Xerox, MIT, Siemens and IBM, are developing smart housing products and services in order to improve the comfort, convenience and security of inhabitants.

According to the definition given by the UK Department of Trade and Industry (DTI), a smart home is “A dwelling incorporating a communications network that connects the key electrical appliances and services, and allows them to be remotely controlled, monitored or accessed” (King, 2003). Remotely-controlled means that the appliances and services may be controlled within or outside the dwelling.

Technically, a smart home incorporates three main elements: internal network, intelligent control and home automation (Jiang, Liu and Yang, 2004); to provide the inhabitant with a full control over the smart home system. In a bit more details, with a single press on a touchpad, a smart homeowner can control lighting, climate, multimedia, window and door operations, security and surveillance, as well as many other functions.

One of the most well-known smart home services is the lightning control system which is a standalone system serving to deliver the right amount of light only where and when it is needed. For example, setting outdoor lights to go on at sunset and off at daybreak.

3. BIGRAPHS OVERVIEW

According to Milner (2009), a bigraphical reactive system is a bigraph representing the current topology of the system and a set of reaction rules that allow describing its behavior by capturing the context changes.

Structurally, a bigraph is a graphical model emphasizing both locality and connectivity of ubiquitous systems. The figure below depicts the anatomy of bigraphs.

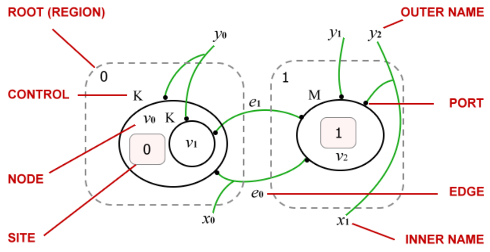

Figure 1: *The anatomy of Bigraphs.*

The dashed line rectangles with rounded corners represent roots (also known as regions) that are used to distinguish significantly different spaces in which nodes can be nested. Nodes can be nested inside one another. Nodes and edges are denoted by v_i and e_i respectively. The small bold points linking nodes to edges are called ports. Each node is characterized by a control, represented by an upper-case letter. The shaded rectangles represent *sites*, which allow nodes to host any content inside. The outer names and inner names represent end points where connections with the outside world can be established.

Moreover, a bigraph consists of two independent sub-graphs (as shown in Figure 2), a place graph (topograph) expressing usually the physical location of nodes and a link graph (monograph) representing the mobile connectivity among them.

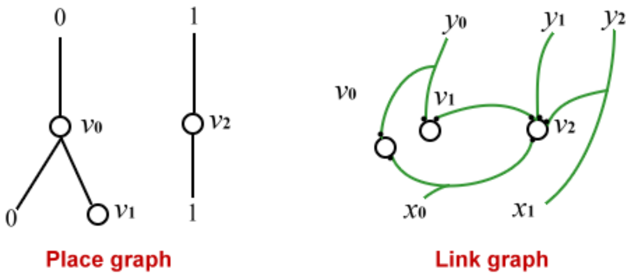

Figure 2: *Place graph and Link graph.*

Formally, a bigraph G over a signature $\mathcal{K}$ takes the form

$$G = (V, E, ctrl, G^{\mathrm{P}}, G^{\mathrm{L}}) : I \rightarrow J$$

To illustrate the bigraph notations, Figure 1 represents a bigraph $G: \langle 2, \{x_0, x_1\}\rangle \rightarrow \langle 2, \{y_0, y_1, y_2\}\rangle$ where the sets of nodes and edges are given by $V = \{v_0, v_1, v_2\}$ and $E = \{e_0, e_1\}$ respectively. $\mathcal{K} = \{K: 2, M: 4\}$ represents the signature of the bigraph G. The interface $I = \langle 2, \{x_0, x_1\}\rangle$ is the inner face of G in which 2 is a finite ordinal representing the number of sites and $X = \{x_0, x_1\}$ is the set of inner names. Similarly, the outer face of G is given by $J = \langle 2, \{y_0, y_1, y_2\}\rangle$ where 2 represents the number of regions and $Y = \{y_0, y_1, y_2\}$ is the set of outer names. Finally, $G^P: 2 \rightarrow 2$ is the place graph of G while $G^L: \{x_0, x_1\} \rightarrow \{y_0, y_1, y_2\}$ is its link graph.

Bigraphs can be also expressed in terms language (Milner, 2008) the primary operations and elements used by the present paper are summarized in Table 1.

TABLE 1: *Algebraic expressions of bigraphs.*

Term	Interpretation
$U \circ V$	Composition of nodes
$U \mid V$	Merge product (Juxtaposition of nodes)
$U \parallel V$	Parallel product (Juxtaposition of roots)
$U.V$	Nesting. U contains V
$U \otimes V$	Tensor product
$K_{\vec{x}}(U)$	Node with control $K$of arity $\vec{x}$
1	The barren (empty) root
d_i	Site numbered i
x/y	Connection from inner name y to outer name x

For example, the following is the corresponding algebraic expression of the bigraph given in Figure 1

$$v0_{y_0}.\left(v1_{y_0,x_0} \middle| d_0\right) \parallel v2_{y_1,y_2,x_0,x_1}.d_1$$

For more details about the theory of bigraphical reactive systems the reader is referred to (Milner, 2009).

4. BIGRAPH-BASED MODEL FOR CONTEXT-AWARE SYSTEMS

Our proposed approach (Cherfia and Belala, 2014) consists in providing a bigraphical reactive systems based approach to formally model the different aspects of context-aware systems. Firstly, we have enriched the bigraph definition to represent the structure of the context-aware system by modeling separately both the context-aware and context-unaware parts of the system. To do so, we use two distinct bigraphs (S and C). $S: K \rightarrow J$ is a bigraph modeling the context-unaware part of the system and $C: I \rightarrow K$ is another bigraph modeling the context-aware part. Then, we combine them together using the composition operation ($S \circ C$) to represent the entire system given by $S_C: I \rightarrow J$.

Moreover, each part of the system (i.e. context-aware and context-unaware parts) has its own reaction rules, namely *context reaction* rules *and internal reaction rules*, respectively. However, these reaction rules are performed independently of each other. That is, a context-aware reaction rule is a sequence of reaction rules occurred in each part of the context-aware system to shift it from one state to another.

To illustrate the effectiveness of our approach to model the different aspects of context-aware systems, in the following, we apply it through a simple lightning control system.

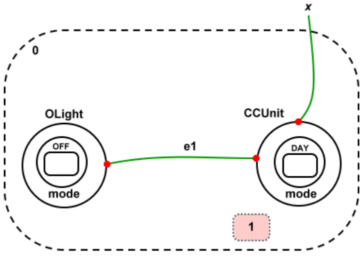

Figure 3: *DAY MODE bigraph.*

As shown in Figure 3, the node DAY nested in CCUnit (Central Control Unit) indicates that the lightning control system is running in DAY MODE (i.e. outdoor lights are OFF). The hyper-edge e₁ linking the node OLight with CCUnit means that the outdoor lights are connected to the central control unit. The site 1 predicted to introduce other context information; such as interior lights, motion sensors, security cameras and so on. Finally, the open link x is used to capture context information.

The algebraic expression of the lightning control system running in DAY MODE is as follows:

$$/x\, OLight.(mode.OFF)|CCUnit_x.(mode.DAY)|d_1$$

4.1. Context-Unaware Bigraph

As mentioned previously, at sunset, the lightning control system switches automatically to NIGHT MODE. Consequently, the occurred reaction represents a context reaction rule. The figure below models the bigraph host $S: K \rightarrow J$ of the new context bigraph.

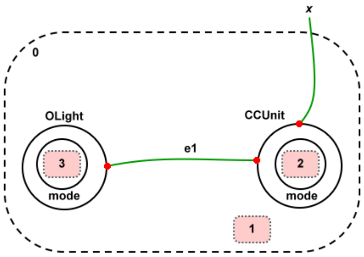

Figure 4: *Bigraph S: Host bigraph.*

Note that DAY and OFF nodes that disappeared and replaced with site 2 and 3 respectively, are *context-nodes* which only appear in DAY MODE.

The algebraic expression of the above bigraphical model is as follows:

$$/x\, OLight.(mode.d_3)|CCUnit_x.(mode.d_2)|d_1$$

4.2. Context-Aware Bigraph

We denote the captured sunset information and light-on event by NIGHT and ON respectively. These nodes are called *context-nodes*, resulting of the context transition introduced in our case study. Formally, the aforementioned nodes are the result of a sequence of context reaction rules (see Table 2) triggered by the captured sunset information.

TABLE 2: *Reaction rules sequence.*

Event	Reaction rule
Sunset	$/x\, OLight.(mode.d_3)\|CCUnit_x.(mode.d_2)\|d_1$ $\rightarrow$ $/x\, OLight.(mode.d_3)\|CCUnit_x.(mode.NIGHT)\|d_1$
Light-On	$/x\, OLight.(mode.d_3)\|CCUnit_x.(mode.NIGHT)\|d_1$ $\rightarrow$ $/x\, OLight.(mode.ON)\|CCUnit_x.(mode.NIGHT)\|d_1$

The figure below depicts a portion of the context bigraph $C: I \rightarrow K$ resulting after the occurrence of the previous reaction rules sequence.

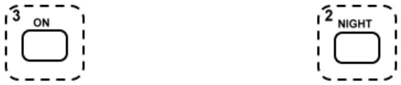

Figure 5: *Bigraph C: Context-Aware Bigraph.*

4.3. Modeling Context-Aware System

The idea behind the separation of the context-aware aspects (Figure 5) of the system from the other aspects (Figure 4) is not only to cope with the complex nature of context-aware systems, but also to make predictive modeling, simple and efficient, by providing a generic way for capturing, structuring and representing the system-context relationships.

That is, the bigraphical model of the lightning control system running in NIGHT MODE S_C (see Figure 6) is given by the composition of the bigraph host and context bigraph presented in Figure 4 and Figure 5, respectively.

Formally, the composition operation occurs if and only if the inner face of S corresponds to the outer face of C; it proceeds by plugging each region of C into its matching site of S, and merging the outer names of C with the inner names of S.

To clarify a bit more, $K = \langle k, Z \rangle$ is the inner face of the bigraph S in which k represents the number of sites where each region i of C containing context-nodes can be planted into the i^{th} site of S. Z is the set of inner names where each inner name is linked to its related outer name of C to form a context-edge.

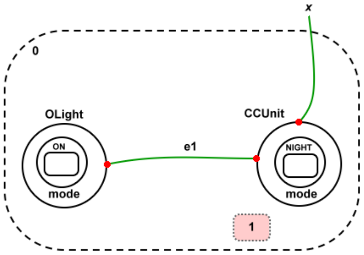

Figure 6: *Bigraph S_C: NIGHT MODE bigraph.*

The algebraic expression of the lightning control system running in NIGHT MODE is as follows:

$$/x\, OLight.(mode.ON)|CCUnit_x.(mode.NIGHT)|d_1$$

Finally, the algebraic expression of the above context-aware reaction rule is as follows:

$$/x\, OLight.(mode.OFF)|CCUnit_x.(mode.DAY)|d_1$$
$$\rightarrow$$
$$/x\, OLight.(mode.ON)|CCUnit_x.(mode.NIGHT)|d_1$$

5. MODEL-CHECKING ANALYSIS

Formal methods are one of the highly-recommended techniques in software design of complex systems in both academia and industry. They offer a powerful potential to achieve an early integration of verification in the design process, to provide more effective verification techniques and to reduce the verification time (Baier and Katoen, 2008).

Recently, research in formal methods has led to the appearance of some very promising verification techniques accompanied by powerful software tools that automate various verification steps, in order to facilitate the early detection of defects. Model checking is one of the most successful strategies for analyzing the correctness of safety-critical systems. It is a formal technique for automatically verifying whether a finite-state system satisfies a given logical property.

In the following, we introduce the Bigraphical model checker BigMC and its grammar, then, we describe how to use it in order to implement and perform some verifications on the lightning control system model.

5.1. BigMC: Bigraphical Model Checker

BigMC (Bigraphical Model Checker) is a model checker specifically designed to operate on any model encoded as a bigraphical reactive systems (Perrone, Debois and Hildebrandt, 2013). It permits the execution of bigraphical reactive systems and checking whether some specification or properties of a particular bigraphical model are true. One of the main benefits of BigMC is its ability to provide a mechanism of state reachability analysis based on properties expressed in terms of matching. In other words, it can find all possible configurations of a particular model, check the specification against them and provide a counter-example in the event that a configuration violates the specification.
The full BigMC grammar is given in the following table.

TABLE 3: *Terms language for bigraphs.*

$$M ::= E; M \mid E$$
$$E ::= \%passive\ k :\ arity$$
$$E ::= \%active\ k :\ arity$$
$$E ::= \%rule\ n\ T \rightarrow T$$
$$E ::= \%property\ n\ P$$
$$E ::= T \rightarrow T \mid T$$
$$T ::= K.T \mid T \mid T \mid T \mid\mid T \mid \$n \mid K \mid nil$$
$$K ::= k[names] \mid k$$
$$names ::= n, names \mid n$$
$$n ::= [a-zA-Z][a-zA-Z0-9]* \mid -$$
$$P ::= matches(T) \mid terminal() \mid !P$$

BigMC grammar is relatively simple since it is based on a term language. In the table above, $\boldsymbol{M}$ refers to a bigraphical model that may be composed from other models or/and expressions $\boldsymbol{E}$. An expression $\boldsymbol{E}$ can be a control ($\boldsymbol{k}$), reaction rules ($\boldsymbol{T} \rightarrow \boldsymbol{T}$), or a property ($\boldsymbol{P}$). A control $\boldsymbol{k}$ must be pre-defined by the declaration of the bigraph signature %**active** and %**passive** commands, which define the arity (number of ports) of a given control as well as whether it is active or passive. Any term of the form $\boldsymbol{T} \rightarrow \boldsymbol{T}$ is considered to be a reaction rule, where the first term $\boldsymbol{T}$ represents the redex, while the second represents the reactum. Finally, the property $\boldsymbol{P}$ is expressed as a logical formula and it is checked whether a given bigraphical model satisfies or violates this formula.

5.2. Reachability Checking

In order to verify the feasibility of our approach, we use the BigMC model checker to encode the lightning control system.

The table below represents the bigraphical specification of the context-unaware part in BigMC terms language.

TABLE 4: *BigMC Specification of a Lightning Control System.*

```
#Central Control Unit Nodes
%active CCUnit : 2;
%active mode : 0;
%passive DAY : 0;

#Outdoor lights Unit Nodes
%active OLight : 1;
%active mode : 0;
%passive OFF : 0;

#Hyper-edges
%name e1;

#Lightning Control System Model
OLight[e1].(mode.OFF)|CCUnit[e1,x].(mode.DAY);
```

The bigraphical specification of the context-aware part represented in Figure 5 is as follows:

TABLE 5: *BigMC Specification of the Context Bigraph.*

```
#Context-Aware Nodes
%passive NIGHT : 0;
%passive ON : 0;
```

Table 6 decodes the sunset and light-on reaction rules listed in Table 2 that are applied to switch the lightning control system to NIGHT MODE.

***TABLE 6:** Specification of the reaction rules.*

```
#Reaction Rules
CCUnit[e1,x].(mode.$2) -> CCUnit[e1,x].(mode.NIGHT);
OLight[e1].(mode.$3) -> OLight[e1].(mode.ON);
```

Once the lightning control system model and the set of reaction rules are defined, the next step consists to specify some properties that must be checked. Here, we focus on proving that the final state corresponding to the bigraph reconfiguration displayed in Figure 6 is eventually reachable by the application of the above reaction rules.

BigMC implements explicit-state checking of properties expressed as matching. Each property is expressed as combinations of two predefined predicates: ***matches ()*** and ***terminal ()***. The *matches()* predicate describes some redex that must be found (or assert that not be found) in every possible agent of a given system as it behaves. The *terminal ()* predicate is true if an only if there are no possible further states reachable by a step of reaction from the current one. Furthermore, predicates can be combined together with the common boolean operators and, or and not (i.e. &&, || and !) to form more complex expressions (Perrone, Debois and Hildebrandt, 2013).

Now, let *final_state* be a reachability property defined as the negation of the buit-in predicate *terminal ().* We note that the final state is a terminal state which does not lead to any further states and there are no reaction rules that can be applied to it.

The specification of the *final_state* property in BigMC is as follows:

***TABLE 7:** Reachability property specification.*

```
#Properties
%property final_state !terminal();
%check
```

The following are the default command-line options for BigMC:

- **-m 1000:** maximum number of steps.
- **-r 50:** reporting frequency.
- **-p:** a command to print new states.

Running BigMC with these options, we prove that the intended state is successfully reached as shown in step 4 of Table 8.

***TABLE 8:** Model-Checking results.*

```
> C:\Progra~1\BigMC/bin/bigmc -m 1000 -r 50 -p
1: (OLight[e1].mode.OFF.nil|CCUnit[e1,x].mode.DAY.nil)
2: (OLight[e1].mode.ON.nil|CCUnit[e1,x].mode.DAY.nil)
3: (OLight[e1].mode.OFF.nil|CCUnit[e1,x].mode.NIGHT.nil)
4: (CCUnit[e1,x].mode.NIGHT.nil|OLight[e1].mode.ON.nil)
[mc::step] Complete!
[mc::report] [q: 0 / g: 4] @ 5
```

6. CONCLUSION

In this paper, we have presented a formal approach based on bigraphical reactive systems to specify and verify context-aware systems. Firstly, we have shown, through a case study of a smart home system, the potential of our approach for a generic and high level modeling of the different aspects of context-aware systems. The proposed approach provides a clear separation between the context-aware part of the system and the remaining one; each part is modeled by a distinct bigraph, and their composition yields a new bigraph describing the whole structure of the context-aware system.

Besides, the behavior of context-aware systems has been characterized by bigraphical reaction rules with respect to both context changes and internal system changes. Then, we have implemented the case study using the BigMC model checker and effectively proven the applicability of our approach.

As a future extension, we intend to evaluate the effectiveness of our approach by checking whether some critical non-functional properties (i.e. security) of a particular bigraphical model are true.

Additionally, we are developing a tool (Cherfia and Belala. 2014) that supports the modeling and execution of any context-aware system encoded as a bigraphical reactive system, in order to apply our approach on large-scale ubiquitous systems.

7. REFERENCES

Abowd, G., Dey, A., Brown, P., Davies, N., Smith, M., Steggles, P. (1999) Towards a Better Understanding of Context and Context-Awareness. *In: Proceedings of First International Symposium, HUC'99, LNCS 1707*. Karlsruhe, Germany, 27-29 September 1999. Springer-Verlag. 304-307.

Baier, C., Katoen, J. P. (2008) *Principles of Model Checking (Representation and Mind Series)*. The MIT Press. Cambridge. England.

Birkedal, L., Debois, S., Hildebrandt, T. (2006) Bigraphical Models of Context-Aware Systems. *In: Foundations of Software Science and Computation Structures, LNCS 3921.* Vienna, Austria, 25-31 March 2006. Springer-Verlag. 187-201.

Cherfia, T. A., Belala, F. (2014) A BRS-Based Modeling Approach for Context-Aware Systems A Case Study of Smart Car System. *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC)*. In press.

Cherfia, T. A., Belala, F. (2014) BigCAS-Tool: A Bigraphical Environment for Modeling Context-Aware Systems. *Submitted to: International Conference on Advanced Aspects of Software Engineering, ICAASE'14*.

Jiang, L., Liu, D., Yang, B (2004) Smart Home Research. *In Proc. of the Third International Conference on Machine Learning and Cybernetics*. Vol. 2, 659-663.

King, N. (2003) *Smart Home - A Definition*. Intertek & DTI. Housing LIN.

Milner, R. (2008) Bigraphs and their algebra*. In: Proceedings of the LIX Colloquium on Emerging Trends in Concurrency Theory*. Electronic Notes in Theoretical Computer Science. 209. 5-19.

Milner, R. (2009) *The Space and Motion of Communicating Agents*. Cambridge University Press.

Pereira, E., Kirsch, C., Sengupta, R. (2012) *BiAgents – A Bigraphical Agent Model for Structure-aware Computation*. Cyber-Physical Cloud Computing Working Papers, CPCC Berkeley.

Perrone, G., Debois, S., Hildebrandt, T. (2013) A verification environment for bigraphs, *Journal of Innovation in Systems and Software Engineering*, Springer-Verlag, 9 (2). 95-104.

Siewe, F., Cau, A., Zedan, H. (2009) The Calculus of Context-aware Ambients, *Journal of Computer and System Sciences*. 77 (4). 597-620.

Wang, J., Xu, D., Lei, Z. (2011) Formalizing the Structure and Behaviour of Context-aware Systems in Bigraphs. *In: First ACIS International Symposium on Software and Network Engineering*. Seoul, Korea, 19-20 December 2011. IEEE. 89-94.

Weiser, M. (2002) The computer for the 21st Century. Pervasive Computing, IEEE, 1 (1). 19-25.

Xu, D.Z., Xu, D., Lei Z. (2011) Bigraphical Model of Context-aware in Ubiquitous Computing Environments*. In: Asia-Pacific Services Computing Conference*. Jeju Island, Korea, 12-15 December 2011. IEEE. 389-394.

Zimmer, P. (2005) *A Calculus for Context-awareness*. BRICS Report Series RS-05-27. Aarhus, Denmark. 21 pages.