A MODEL FOR SECURE MOBILE BROADCASTING SYSTEMS

Victor MORARU
Technical University of Moldova
& Université de la Méditerranée-Marseille (F)
victor.moraru@esil.univ-mrs.fr

Traian MUNTEAN*
Université de la Méditerranée
Parc Scientifique de Luminy-F-13288 Marseille
muntean@esil.univ-mrs.fr

Abstract: In many parallel and distributed applications the broadcasting represents a natural way of communication between processes/objects. In addition mobility is often mandatory, as for instance for the development of applications for the ad-hoc networks. The fusion of these two concepts into one model represents a particular interest for the development of this class of applications and appropriate programming models. An original model that combines mobility and broadcasting was developed by C. Ene and T. Muntean (le bπ-calcul). The "Mobile Ambients" represent also an interesting model for the mobility and ubiquity of applications. The goal of this paper is to study a model of Broadcasting Ambients that we consider to be more appropriate for the ad-hoc networks and ubiquitous applications, reinforcing the mobility and security aspects.

Keywords: mobility, broadcasting, security, formal models, parallel computing

1. INTRODUCTION

Mobile communicating systems can be characterized by the dynamic change of interconnection topology and communication patterns. Two mobility aspects can be distinguished: physical mobility and logical mobility. Physical mobility assumes that the nodes change their place in the network (reconfiguration of the network interconnections) and logical mobility deals with the process/objects migration from one host to another. In our formal model both types of mobility can be modeled in the same way.

Broadcasting is one of the most natural ways of communication for mobile ad-hoc networks, where usually communication uses radio waves. Alas, the broadcasting is a characteristic of such a distributed system with communication topology dependent on all the components' states at a given moment in time. In this class of systems a message sent by one of the components must be received by all the participants, with some property satisfied.

An original model, called *bπ*-calculus [3][2], that combines the mobility and the broadcasting in an original way has been developed in our team by Ene and Muntean. In this paper, we'll extend this model by introducing mobility of mobile ambients (introduced originally by Gordon [1]), because this ambients model presents interesting locality and security properties.

The bπ-calculus is a calculus of mobile processes that communicate only through diffusion. It is inspired by CBS, introduced by Prasad [7], taking into consideration the broadcasting as the only communication primitive, but communications use channels (ports) and the sent values can also be channels names (somehow similar to Milner's π-calculus [5]).

The Mobile Ambients calculus is an abstract model for mobility. It models the two aspects of mobility: code mobility and hosts mobility. An ambient can be viewed as bounded place where computations take place. An ambient can move together with its contents. The calculus of the ambient also deals with security problems as for instance authentication.

The model uses the basic primitives of *π*-calculus [5]: the restriction (*νn*)*P*, the composition *P*|*Q*, the replication !*P* and the nil process **0**. There are also mobility primitives added – the ambients *n*[*P*], the capabilities actions *M.P* and the communication primitives – (*x*).*P* (input) and <*M*> (output). The ambient *n*[*P*] stops the direct interactions between *P* and all other processes, running in parallel with *n*[*P*], but it doesn't stop the internal interactions within *P* (as ambients can be constructed from other ambients forming a hierarchy). The action *M.P* applies the capability presented by *M*, and then continues its execution as *P*. An action affects either the surrounding ambient, either an ambient that run in parallel with the actual process. There are three base capabilities: *in n, out n* and *open n*. The action *in n.P* moves the surrounding ambient inside the ambient *n* which runs in parallel. The action *out n.P* exits the surrounding ambient of its parent ambient and becomes parallel with the actual ancestor. The action *open n.P* "destroys the borders" of the ambient *n* [*Q*] which runs in parallel with *P*.

2. PURPOSE OF THIS PAPER: DEFINING AN EXTENDED MODEL FOR SECURITY

The main goal of this paper is to widen the mobility notion of *bπ*-calculus with a notion of locality and dynamic reconfigurability. We target new programming models applicable in ubiquitous communication systems. The basic notions in our model treat properties like network locality, dynamic neighborhood, vicinity, etc. How does a process know which processes are acting in its neighborhood? How can it change or act on its neighborhood? How to communicate with processes which are in "distant" neighborhoods?

The ambients model expresses the mobility in a quite natural way. Moreover, the ambients present a very good support for expressing security, that is to say, by the authorizations to enter and exit of the ambient. That's why there is a variety of ambients, called "safe ambients", which introduces the co-capacity. The presence of a co-capacity is necessary in the correspondent ambient, in order to have the capacity carried out when moving ambients.

In the bπ-calculus the locality notion doesn't appear explicitly, but the system's structure can change dynamically. The processes exchange communication channels. This gives the power of expression necessary to describe the dynamic nature of the system but it doesn't allow treating the locality as a first class concept. Mobility is expressed thanks to two concepts: the mobility of nodes and the mobility of processes. On the other hand, the diffusion is the unique communication primitive and therefore in this model point-to-point communications became just a particular case of diffusion. The third aspect deals with security and authentication properties to be introduced in the model.

The model presented in this work claims to merge the aspects mentioned above in a coherent way. To simplify, the new model inherits from the bπ-calculus all aspects dealing with primitive broadcasting communication and from mobile ambients some new aspects of locality and security proprieties. In the ambients model, the action of *output* <*M*> sends the message *M* to the surrounding ambient and if there is a process which executes $(x).P$ it replaces all the surroundings of *x* in *P* with *M*. The output is asynchronous and anonymous. There isn't a notion of channel. An ambient can be seen as a sort of environmental channel and the processes, which exit from this ambient can "listen" or send messages on this channel. If there are more than one processes listening, one is chosen in a non-deterministic way. So, the diffusion can be implemented quite naturally: if there are several processes listening, then all of them receive the message.

To formalize, the syntax of the model will be the following:

The syntax:

M,N::=	expression	*P,Q,R::=*	process
X	variable	$(\nu n)P$	Restriction
N	name	**0**	Inactivity
in M	can enter *M*	$P\vert Q$	Composition
out M	can exit *M*	*!P*	Replication
open M	can open *M*	$M[P]$	Ambient
0	null	*M*	Action
M.M´	path	$(x).P$	Input
		<*M*>	Output

The reduction rules for this model will be:

$n[in\ m.P \mid Q] \mid m[R] \rightarrow m[n[P \mid Q] \mid R]$

$m[n[out\ m.P \mid Q] \mid R] \rightarrow n[P \mid Q] \mid m[R]$

$open\ n.P \mid n[Q] \rightarrow P \mid Q$

$<M> \mid (x_1).P_1|(x_2).P_2|\ldots|(x_n).P_n \rightarrow^{*} P_1\{x_1 \leftarrow M\} \mid \ldots \mid P_n\{x_n \leftarrow M\}$

$P \rightarrow Q \Rightarrow P \mid R \rightarrow Q \mid R$

$P \rightarrow Q \Rightarrow (\nu n)P \rightarrow (\nu n)Q$

$P \rightarrow Q \Rightarrow n[P] \rightarrow n[Q]$

$P' \equiv P,\ P \rightarrow Q,\ Q \rightarrow Q' \Rightarrow P' \rightarrow Q'$

Cardelli and Gordon give a coding of the π-calculus to show the power of expression of Mobile Ambient in [4]. In a similar approach we code the bπ-calculus to express the power of expression of the new model. Let us recall the basic entities of the bπ-calculus: the channels and the operations of input and output:

$buf\ n = n[!open\ io]$

$(ch\ n)P = (\nu n)(buf\ n \mid P)$

$n(x).P = (\nu p)(io[in\ n.(x).p[out\ n.P]] \mid open\ p)$

$\overline{n}\ M.P = io[in\ n.<M>]$

Here *io* is a conventional name the requests of writing and reading on a given channel. The channel is represented by an ambient: the name of the channel is the name of the ambient. The communication on the channels is represented as local communications inside the ambient.

We can therefore prove the following:

in order to show that the bπ-calculus is well coded, it must be proved that the following reduction is true (see [6] for the demonstration):

$\overline{n}\ M \mid n(x_1).P_1 \mid \ldots \mid n(x_n).P_n \ \rightarrow^{*} P_1\{x_1 \leftarrow M\} \mid \ldots \mid P_n\{x_n \leftarrow M\}$

in the presence of a buffer buf n:.

4. CONCLUSION AND FUTURE WORK

The model described in this paper presents an interest from different points of view:

- It models mobility of the processes and of the hosts nodes of an ad-hoc network;
- The basic communication is done by primitive diffusion exchange (asynchronous);
- It presents interesting locality and security properties.

Of course our work is by far not finished and further research is needed: for example, the introduction of capacity in the diffusion ambients can give interesting results for the security in mobile system; on the other hand, higher order ambients were too little explored in the literature. It is interesting to try the modification of the capacity, which doesn't move the ambient but makes a clone of it own which could always maintain the communication with the original ambient. These directions will be extensively explored further in V. Moraru's thesis work.

REFERENCES

4. Cardelli L, Gordon AD, *Mobile Ambients*, Theoretical Computer Science, 240(1), July 2000.
5. Ene C. et Muntean T. *Expressivnes of Point-to-Point versus Broadcast Communications*. Lecture Notes in Computer Science, volume 1684, Springer Verlag, 1999.
6. Ene C. *Un Modèle formel pour les systèmes mobiles a diffusion.* Thèse de doctorat, Université de la Méditerranée - Marseille, 2001.
7. Gordon A.D. and Cardelli L. *Equational properties of mobile ambients*. In FoSSaCS'99, volume 1578 of LNCS, pages 212-226, 1999.
8. Milner R. *Communication and Mobile Systems: the π-calculus*. Cambrifge University Press.
9. Moraru V. *Un Modèle formel à diffusion pour Ambients Mobiles.* Thèse de DEA. Université de la Méditerranée - Marseille, 2003
10. Prasad KVS. *A Calculus of Broadcasting Systems.* Science of Computer Programming, 25. 1995