

# Formal Methods for Trustworthy Mobile Computing\*

Huimin Lin  
Chinese Academy of Sciences  
lhm@ios.ac.cn

## Abstract

Mobile computing provides a new paradigm for organizing and implementing computation over the Internet. There are two computational phenomena that involve mobility: code mobility and computation mobility. The former happens when pieces of code (such as Applets) move between computing devices, while the later concerns computation carried out in computing device (such as laptops) which change locations.

Mobile computing has posed serious challenges to the safety and security of Internet-based systems. Theories and techniques are needed to decide if code coming from outside can be trusted, or to determine if a computation movement is safe, and so on. In this talk I will first review some formal methods that have recently been proposed for such purposes. These methods are based on either theorem proving or model checking, and each emphasizes on certain aspects of trustworthy computing. Then I will focus on a model checking approach to mobile computing.

Traditionally model checking is based on modal logics which are appropriate for describing the temporal behaviors of systems. Since in mobile computing processes may evolve not only in time but also in space, efforts have recently been made to extend these logics with spatial modalities (to describe location changes), and to design model checking algorithms for them. However, so far there still lacks a satisfactory approach to introducing recursion into such spatial logics, due to subtle interplay between recursion and first-order quantification. We take the challenging task to extend a spatial ambient logic with fixpoints, yielding a predicate-based mu-calculus in which fixpoint formulas are formed using predicate variables. We also develop an algorithm for model checking finite-control mobile ambients against formulas of the logic, providing the first decidability result for an ambient logic with recursion. The algorithm has been implemented and I will also discuss some implementation considerations.

---

\*Supported by research grants from National Natural Science Foundation of China and Chinese Academy of Sciences