ABSTRACT

The scope of the thesis is the modeling and verification of mobile systems using algebraic specification techniques. A mobile system is a computing and/or a communication system where the notion of location of its components is of major criticality and its change affects system's behavior. Due to the special characteristics of such systems, and the rapid proliferation of mobile devices, networks and services, the requirements for reliability, security and functionality has led to the development of formal methods for mobile systems. Formal methods, which are techniques, languages and tools based on mathematics, provide an unambiguous, strict mathematical description or specification which is used for effective design, analysis and verification of desired properties of the system.

An important branch of formal methods are algebraic specification languages with a rigorous basis on mathematical logical systems or combinations of them. Such a language is CafeOBJ, an executable, new generation algebraic specification language, member of the OBJ family languages. Its main characteristic that differentiates it from other formalisms is its direct support to behavioural specification paradigm since it embeds special hidden sorts and behavioural operators in its syntax. Behavioural specification is based on hidden algebra and supports an object oriented style of algebraic specification. It also supports specification of distributed concurrent systems as abstract state machines and verification of safety properties of them through theorem proving techniques such as simultaneous induction and coinduction.

Based on the above specification techniques, MobileOBJ is proposed, that is an algebraic framework for specification and verification of mobile systems. The specification of the mobile system, protocol or procedure consists of specification modules which describe either data types as visible sorts, or the system as a Mobile Observational Transition System, a kind of behavioural object. Based on this specification, verification of properties of the mobile system using theorem proving techniques is feasible. Since the transitions of the system are specified as equations makes the method easier to read, understand and learn than other related methods, which prerequisite deeper knowledge of theorem proving.

Next, the integration of Mobile Observational Transition Systems with Timed and Hybrid Observational Transition Systems is performed to capture not only the discrete but also the continuous characteristics of mobiles systems, such as timing constraints, resource scarcity or distance. To demonstrate the applicability and practicality of the framework, a number of case studies are conducted.

Security aspects of mobile systems are of major importance, and it was inevitable to take them into account. Authentication protocols for sensor networks and multicasting settings have been formally specified, and safety properties of them have been verified.

In the last section of the thesis, a protocol algebra is proposed inspired by the module algebra and the hierarchical object composition technique based on hidden algebra. The preservation of some properties of the component protocols to the composed protocol for some operators of the algebra has been proved. Finally, a number of applications of the algebra are presented.

Keywords:

Mobile Systems, Formal Methods, Algebraic Specification Languages, Formal Verification, CafeOBJ, MobileOBJ, Mobile Observational Transition Systems, Theorem Proving, Induction, Behavioural Specifications, Hidden Algebra, Abstract Data Type, Abstract State Machine, Mobile Communication Protocols, Security Protocols, Protocol Algebra, Protocol Composition