Summary

Formal Modeling and Analysis of Mobile Ad hoc Networks

Wireless ad hoc networks, in particular mobile ad hoc networks (MANETs), make communication easier and more flexible. However, their protocols tend to be difficult to design, due to the topology-dependent nature of wireless communication, and their distributed and adaptive operations to cope with a dynamic topology. Therefore it is desirable to model and verify such protocols using formal methods. To this aim, we introduce constrained labeled transition systems (CLTS) as a semantic model, to compactly capture the behavior of MANETs while mobility is implicitly specified. The transitions are constrained so as to indicate conditions over the underlying topology for which the behavior is valid. We present two modeling languages with different computation models to address main challenges of modeling MANETs, such as local broadcast, underlying topology, and its changes.

The first approach, presented in Chapter 3, is an algebraic framework for modeling and analysis of MANET protocols. The framework abstracts away from data link layer services by assuming reliable synchronous (local) broadcast. We discuss how the non-blocking property of local broadcast is guaranteed by making network processes input-enabled. We define the appropriate equivalence relation in this setting and provide a process theory to verify MANET protocols using equational reasoning. To utilize our complete axiomatization for analyzing the correctness of protocols at the syntactic level, we introduce a precongruence relation which abstracts away from a sequence of multi-hop communications, leading to an application-level action preconditioned by a multi-hop constraint over the topology. We illustrate the applicability of our framework through a simple routing protocol. To prove its correctness, we introduce a novel proof process, based on our precongruence relation.

The second approach, presented in Chapter 4, is an actor-based modeling language, with the aim to reduce the labor of modeling and generating the state space. We discuss how MANET protocols can be modeled efficiently at the semantic level, to make their verification feasible. This framework abstracts away from data link layer services by providing asynchronous (local) broadcast, unicast, and multicast communications, while assuming that message delivery is in order and is guaranteed for connected receivers. We illustrate the applicability
of our framework through two routing protocols, flooding and AODVv2-11, and show how their state spaces are reduced efficiently by the proposed techniques implemented in a tool. Furthermore, we demonstrate a loop formation scenario in AODV, found by our analysis tool. This has led to an adaptation of the AODV standard.

To model check MANET protocols with respect to the underlying topology and connectivity changes, we introduce a branching-time temporal logic which is interpreted over CLTSs in Chapter 5. The path quantifiers are parameterized by multi-hop constraints over topologies, to discriminate the paths over which the temporal behavior should be investigated; paths that violate the multi-hop constraints are not considered. A model checking algorithm is presented to verify MANETs, under the assumption of reliable communication. It is applied to analyze a leader election protocol and the packet-delivery property of AODVv2-11.

Software product lines (SPLs) facilitate reuse and customization in software development by genuinely addressing the concept of variability. Product Line Calculus of Communicating Systems (PL-CCS) is a process calculus for behavioral modeling of SPLs, in which variability can be explicitly modeled by a binary variant operator. The transitions of underlying semantic models are constrained to indicate the set of products (families) for which the behavior is valid. Hence, to extend the results over CLTSs, we study different notions of behavioral equivalence for PL-CCS in Chapter 6, based on Park and Milner's strong bisimilarity. These notions enable reasoning about the behavior of SPLs at different levels of abstraction. We study the compositionality property and the mutual relationship among these notions. We further show how the strengths of these notions can be consolidated in an equational reasoning method. Finally, we designate the notions of behavioral equivalence that are characterized by the property specification language for PL-CCS, called multi-valued modal $\mu$-calculus.