Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science 242 (2009) 43–58
Electronic Notes in Theoretical Computer Science
www.elsevier.com/locate/entcs

Probabilistic Analysis of Wireless Systems Using Theorem Proving

Osman Hasan[1] Sofiène Tahar[2]

ECE Department
Concordia University
Montreal, Canada

Abstract

Probabilistic techniques play a major role in the design and analysis of wireless systems as they contain a significant amount of random or unpredictable components. Traditionally, computer simulation techniques are used to perform probabilistic analysis of wireless systems but they provide inaccurate results and usually require enormous amount of CPU time in order to attain reasonable estimates. To overcome these limitations, we propose to use a higher-order-logic theorem prover (HOL) for the analysis of wireless systems. The paper presents a concise description of the formal foundations required to conduct the analysis of a wireless system in a theorem prover, such as the higher-order-logic modeling of random variables and the verification of their corresponding probabilistic and statistical properties in a theorem prover. In order to illustrate the utilization and effectiveness of the proposed idea for handling real-world wireless system analysis problems, we present an analysis of the automated repeat request (ARQ) mechanism at the logic link control (LLC) layer of the General Packet Radio Service (GPRS), which is a packet oriented mobile data service available to the users of Global System for Mobile Communications (GSM).

Keywords: Formal Methods, GPRS, Higher-Order-Logic, Mechanization of Proofs, Probabilistic Analysis, Theorem Proving, Wireless Networks.

1 Introduction

Wireless communication systems are increasingly being used these days in applications ranging from ubiquitous consumer electronic devices, such as cell phones and computers, to not so commonly used but safety critical domains, such as automated highways and factories, remote tele-medicine and wireless sensor networks. The correctness of operation for these wireless systems is very important due to financial or safety critical nature of their applications. Therefore, quite a significant portion of the design time of a wireless system is spent on analyzing the designs so that functionality errors can be caught and reliability and performance metrics can be evaluated prior to production. Probabilistic considerations play a significant role in

[1] Email: o_hasan@ece.concordia.ca
[2] Email: tahar@ece.concordia.ca

doi:10.1016/j.entcs.2009.06.022

such analysis since wireless systems usually exhibit some random or unpredictable elements. For example, wireless channel parameters are often described in terms of their Probability Mass Functions (PMF) instead of the actual mathematical models for all reflection, diffraction and scattering processes that determine the different multi-path components of a wireless channel. Similarly, probabilistic models are used to describe the mobility of communicating stations. Randomized algorithms and probabilistic analysis are also extensively used in the area of wireless networks. A comprehensive survey in this regard is presented in [41].

Today, simulation is the most commonly used computer based probabilistic analysis technique for wireless systems, e.g., see [39,4,15,25]. Most simulation based wireless system analysis softwares provide a programming environment for defining functions that approximate random variables for probability distributions. The random elements in a given wireless system are modeled by these functions and the system is analyzed using computer simulation techniques [11], such as the Monte Carlo Method [31], where the main idea is to approximately answer a query on a probability distribution by analyzing a large number of samples. Statistical quantities, such as expectation and variance, may then be calculated, based on the data collected during the sampling process, using their mathematical relations in a computer. Due to the inherent nature of simulation coupled with the usage of computer arithmetic, the probabilistic analysis results attained by the simulation approach can never be termed as 100% accurate. Thus, simulation should not be relied upon for the analysis of wireless systems, especially when they are used in safety critical areas, such as medicine, transportation and military, where inaccuracies in the analysis may even result in the loss of human lives.

In the past couple of decades, formal methods [16] have been successfully used for the precise analysis of a verity of hardware and software systems. The rigorous exercise of developing a mathematical model for the given system and analyzing this model using mathematical reasoning usually increases the chances for catching subtle but critical design errors that are often ignored by traditional techniques like simulation. Given the sophistication of the present age wireless systems and their extensive usage in safety critical applications there is a dire need of using formal methods in this domain. However, due to the random and unpredictable nature of wireless systems, the usage of formal methods has been quite restricted so far. Some major reasons for this include the restriction to handle random behaviors that can be modeled as a Markov chain only and the inability to precisely reason about statistical properties, such as expectation and variance, in the case of state-based approaches and the fear of huge proof efforts involved in reasoning about random components of a wireless system in the case of theorem proving.

We believe that due to the recent developments in the formalization of probability theory concepts in higher-order-logic [24,19,21,22], we are now at the stage where we can handle the analysis of a variety of wireless systems with random components in a higher-order-logic theorem prover [13] with reasonable amount of modeling and verification efforts. The main motivation of using a higher-order-logic theorem prover for this purpose is the ability to formally analyze a broader range of