Journal of Logical and Algebraic Methods in Programming 85 (2016) 34–66

Contents lists available at ScienceDirect

Journal of Logical and Algebraic Methods in Programming

www.elsevier.com/locate/jlamp

Modeling and analyzing mobile ad hoc networks in Real-Time Maude

Si Liu[a,*], Peter Csaba Ölveczky[b,*], José Meseguer[a]

[a] Department of Computer Science, University of Illinois at Urbana-Champaign, USA
[b] Department of Informatics, University of Oslo, Norway

ARTICLE INFO

Article history:
Received 31 October 2014
Received in revised form 22 May 2015
Accepted 26 May 2015
Available online 9 June 2015

Keywords:
Mobile ad hoc networks
Formal specification
Model checking
Real-Time Maude

ABSTRACT

Modeling and analyzing mobile ad hoc networks (MANETs) pose non-trivial challenges to formal methods. Time, geometry, communication delays and failures, mobility, and uni- and bidirectional wireless communication can interact in unforeseen ways that are hard to model and analyze by current process calculi and automatic formal methods. As a consequence, current analyses tend to abstract away these physical aspects, so that—although still quite useful in finding various errors—their simplifying assumptions can easily fail to model details of MANET behavior relevant to meet desired requirements. In this work we present a formal framework for the modeling and analysis of MANETS based on Real-Time Maude to address this challenge. Specifically, we show that our framework has good expressive power to model relevant aspects of MANETs, and good compositionality properties, so that a MANET protocol can be easily composed with various models of mobility and with other MANET protocols. We illustrate the use of our framework on two well-known MANET benchmarks: the AODV routing protocol and the leader election protocol of Vasudevan, Kurose, and Towsley. Our formal analysis has uncovered a spurious behavior in the latter protocol that is due to the subtle interplay between communication delays, node movement, and neighbor discovery. This behavior therefore cannot be found by analyses that abstract from node movement and communication delays.

1. Introduction

Mobile ad hoc networks (MANETs) are self-configuring networks made up of mobile nodes (laptops, smart phones, vehicles, sensors, etc.) connected by wireless links. They are increasingly popular and well suited for deployment in ad-hoc environments. They have an extensive range of applications, including wireless sensor networks, ambient intelligence, personal area networks and wireless local area networks, cooperating "smart" cars, alternative communication infrastructure for emergency response during accidents and natural disasters, which may disable other existing infrastructure, and so on.

The formal analysis of MANETs is challenging, because the relevant requirements for correctness and performance are themselves non-trivial and go beyond the usual requirements for standard network protocols. In particular, both mobility and wireless communication under mobility are essential for MANETs and need to be seriously taken into account when analyzing them under realistic patterns of node movement. Only thus can MANET protocol designers reasonably determine whether or not a MANET protocol implementation will be useful and will meet its desired requirements.

* Corresponding author.
E-mail address: peterol@ifi.uio.no (P.C. Ölveczky).

http://dx.doi.org/10.1016/j.jlamp.2015.05.002
2352-2208/

1.1. Formal modeling and analysis challenges

Both mobility and wireless communication in MANETs depend on *physical* characteristics such as: (i) geometric *location* of nodes; (ii) *speed* and *direction* of mobile nodes; (iii) wireless *transmission ranges* based on each node's battery *power* and *distance* between nodes; and (iv) *communication delays* in both the sender and the receiver. Therefore, although usually not described that way, MANETs are in fact *cyber-physical systems* (CPSs). This means that their formal modeling, and the formal verification of their relevant requirements must sufficiently address essential physical characteristics such as mobility and communication and their interactions. For example, a moving node may be within range of another node when the other node started a message send, but may have already moved out of such a range by the time when the message is actually sent. Furthermore, as usual with many other CPSs, there is no easy separation between *correctness requirements*, including safety-critical ones, and *physical behavior*, since timing, distance, motion, and other physical, quantitative aspects may be essential for correct behavior.

All this means that the formal modeling and analysis of MANETs presents a number of non-trivial challenges, including:

1. The need to model node movement realistically.
2. Modeling communication. There is a subtle interaction between wireless communication, which typically is restricted to distances of between 10 and 100 meters, and node mobility. For example, nodes may move into, or out of, the sender's transmission range *during* the communication delay; furthermore, the sender may itself move during the communication. Modeling communication in MANETs is therefore challenging for process languages, which are usually based on fixed communication primitives.
3. Since the communication topology of the network depends on the *physical locations* of the nodes, such locations must be taken into account in the model. However, if not handled carefully this can lead to very large state spaces, which can makes direct model checking analysis unfeasible.

We discuss related work on the formal analysis of MANETs in much more detail in Section 6. Such work includes research where MANETS are expressed in the languages of various model checkers, e.g., [4,8,12,19], and approaches representing MANETs in various process calculi, e.g., [31,32,17,26,43,15,18,27,11,13,43,16,42,28,21,44,45]. We can summarize our more detailed discussion in Section 6 by stating that in prior work on the formal analysis of MANETs there is still a substantial gap between a more abstract modeling level—at which various physical aspects are omitted—and the actual level at which MANETs need to be analyzed to take into account those physical aspects essential to ensure that relevant requirements are met. Of course, any actual errors found even at a more abstract level are still very valuable. The main issue, however, is that other realistic potential problems may be easily abstracted away when they are not reflected in the given formal model. This fact is illustrated by our analysis in Section 5 of the well-known leader election algorithm by Vasudevan, Kurose, and Towsley [47], where our analysis has uncovered a spurious behavior that is due to a very subtle interplay between node movement, communication delays, and neighbor discovery. This problematic behavior therefore cannot be found using standard formal analysis methods that abstract away node movement and communication delays.

1.2. An expressive formal modeling and analysis framework for MANETS

To meet above challenges (1)–(3) a suitable formal and analysis framework for MANETS is needed. To the best of our knowledge this is not yet available in prior work, and is therefore a key motivation behind the present work. We see: (i) *expressiveness* to meet challenges (1)–(3); and (ii) *compositionality* as two main requirements that such a formal framework should meet. Requirement (i) is obvious from the prior discussion. The need for requirement (ii) is amply illustrated throughout the paper but deserves some explanation. The key point is that, typically, the formal requirements of a MANET protocol will need to be analyzed under various assumptions such as:

- various *mobility models*;
- various *wireless communication models*, such as unidirectional or bidirectional communication; and
- possibly in composition with other auxiliary protocols.

To put it briefly, to address relevant requirements formal analyses will almost never consider the given MANET protocol *in isolation*: they will need to consider it *in composition with* other formal models of mobility, communication, and of other MANET protocols. Compositionality, therefore, becomes a highly desirable feature of a MANET formal framework.

Our proposed answer to the *expressiveness* requirement for a MANET formal framework is the use of Real-Time Maude [35]. Because of its expressiveness and flexibility to define models of communication—and to model physical aspects such as geometric location, speed, and distance—as we show in the paper Real-Time Maude is well suited for formally modeling MANETs and, to the best of our knowledge, provides for the first time a reasonably detailed formal modeling framework for them. In particular, we formalize in Real-Time Maude:

- the most popular models for node mobility, and