STOCHASTIC DEPENDABILITY EVALUATION OF APPLICATIONS IN MOBILE ENVIRONMENTS

Máté KOVÁCS
Advisor: István MAJZIK

I. Introduction

As information technology advances car, ship, train and airplane manufacturers increasingly tend to take advantage of its services. Embedded systems are used to make the vehicles' existing functionalities more reliable and precise, as well as extend the driver's safety and comfort.

The HIDENETS project envisions a traffic environment where vehicles are in constant connection with each other and with the so-called fixed infrastructure by means of ad-hoc wireless network technologies, and use various applications during the travel. The goal of the project is to establish methodologies for the development of highly dependable services and applications based on the unreliable network infrastructure. Examples to these applications are [1]:

- In case of a car accident, it is very important to study the circumstances of the accident to find the right cause. The *distributed black box* application constantly conveys information on position, speed, acceleration, etc. to the surrounding vehicles and the fixed infrastructure, so it can support the investigation of an accident.
- The *platooning* application lets a platoon of cars be driven by only one driver in the front. The rest of the cars autonomously follow the track of the first, meanwhile keeping due distance from each other. This functionality is possible if all the cars are in constant connection with each other, and periodically transmit and receive dynamic information on their positions.
- The *traffic sign extension* allows for the dynamic adjustment of speed limits on road sections and the fine tuning of traffic sign periods of junctions based on the traffic load.

Some of the applications themselves, and the underlying middleware consisting of the HIDENETS services are going to be implemented to demonstrate the usability of the development methodology. In order to guarantee the dependability, multiple verification and evaluation phases have to be involved in the development process of these services and applications.

II. Stochastic Evaluation of the Dependability of Mobile Applications

We present a holistic evaluation workflow (illustrated in Figure 1) that integrates several tools and model transformation steps to compute the probability of the successful execution of a series of user activities (user workflow) in a dynamic HIDENETS environment. In the figure models are represented as parallelograms, while model transformation steps are depicted as straight rectangles.

The dynamic HIDENETS environment means that the user relies on functions built upon the services of the fixed infrastructure and ad-hoc domains, and tries to execute the activities in an environment that is characterized by changes: the activities are distributed (include collaboration with other users), the users may move, and the mobility and network traffic influence the availability and quality of the services. The user is considered as the driver of a car equipped with a HIDENETS node, or the administrator of a component in the fixed infrastructure. In the following we refer to the *scenario* as a concept that involves all user-related and environment-related changes.

The inputs of the evaluation workflow are comprehensive and include the outputs of several specific evaluation steps (that were also developed in the HIDENETS project). The main aspects are the description of the user workflows, the structure of the applications used by the users, the dependability parameters of specific services or resources included in these applications, the traffic and the mobility pattern.

The three sets of input models (views depicted in a dotted frame in Figure 1) of the scenario being evaluated are as follows:

- Each user workflow specifies the user activities in terms of application usage (the mobility aspects like speed and direction are not addressed in the user workflow, they are included in the topology model). There is a user workflow for each participant of the scenario to be evaluated. The workflow is to be provided by a UML based workflow editor.
- Each topology model represents the information on the evolving ad-hoc topology of network connections. There is a topology model for each technology that can be used for communication. This is to be computed by an existing mobility trace generator and network topology generator tool-chain reported in [2] and in [3].
- The application-service dependency models define how the given applications depend on the services, hardware or software components of nodes. These dependencies are to be described by UML architecture diagrams.

The output of the evaluation, that is the computed probability of successful execution of a user activity sequence, can be used to characterize the user workflow in a best case or worst case situation (e.g., whether it is possible to execute the activities at all in case of extreme network conditions), to compare different execution strategies at the user level (e.g., whether it is reasonable to rely on given functions or it is better to use other ones), or to compare different environment options (e.g., compare routes with different traffic and infrastructure conditions and use the one that is characterized by a higher probability of successful execution for a given workflow).

The evaluation workflow follows the approach of *multilevel modeling addressing phases* [2]. Hierarchical multilevel modeling is used by considering communication, architecture, application and user levels, while the multi-phase approach is utilized to model the changes induced by the user activities and the varying environment conditions.

The architecture of the HIDENETS components are captured by hierarchic models of several layers:

- *User level.* This level provides high-level QoS and resilience attributes as perceived by the users. It describes the users' profiles, that is how the users interact with the application and how their requests are mapped to the different components of the application and the supporting architecture.
- *Application level.* This level describes the system behavior from the application point of view. The applications differ in their technical properties, in their mechanisms, in their interfaces, and they can impose different communication and middleware level requirements.
- *Architecture level.* This is the part of the system capturing the behavior of the main hardware and software components that can affect the application-level measures. It describes how the application components and services of the application level are implemented on these resources.
- *Communication level.* It captures the communication aspects of the system. It addresses the link layer (considering several types of networks like WLANs, UMTS and GPRS), the network layer (IP-based) and the transport layer (considering several types of protocols like TCP and UDP).

III. State-space Reduction Techniques

Given the scenario in the form of input models described in Section II. the evaluation workflow can produce the probability of the successful execution of the involved user workflows. In order to keep the state space of models being directly analyzed under control, multiple techniques are used. The basic idea is that those components and submodels the dependability parameters of which are independent of the environment should be evaluated in isolation.

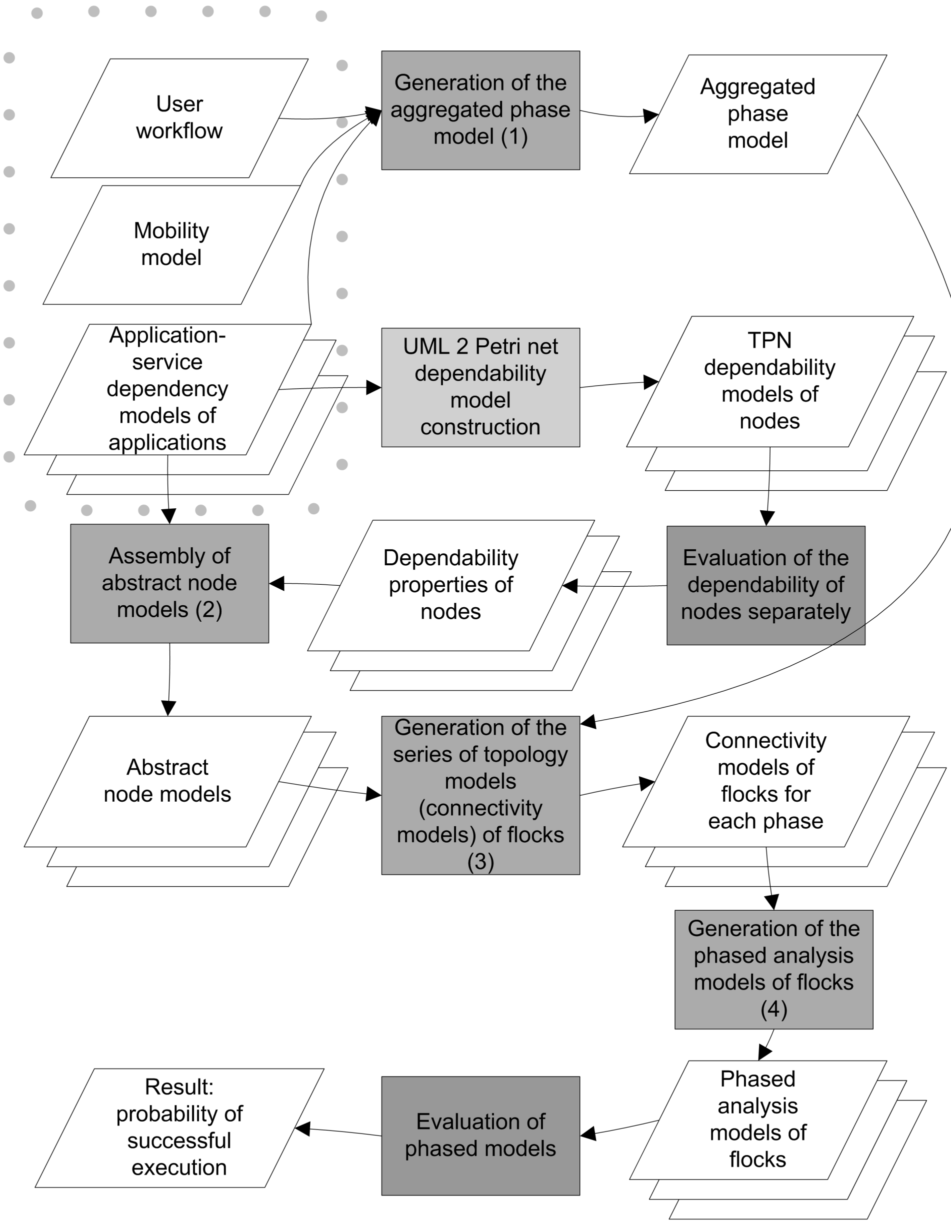

Figure 1: Evaluation Workflow

A. Evaluating HIDENETS Nodes in Isolation

The stochastic failure and repair processes of the HIDENETS nodes themselves are independent from that of other nodes and the network connections. As it is illustrated in Figure 1 the dependability models of nodes (generated from object models extended with parameters given in the form of stereotypes and tagged values) are evaluated separately. The applied model transformation [4] produces the Timed Petri Net representation of object models. These models are then solved resulting in the dependability properties of the individual nodes.

Further steps of the evaluation workflow deal with HIDENETS nodes in the form of *abstract nodes*. Abstract nodes represent the composite models of nodes by singular objects with dependability parameters reflecting those of the original ones.

B. Evaluating Flocks

The number of nodes participating in a scenario is unlimited. However, the set of nodes in a scenario may have independent subsets in the sense that the members of different sets do not know about the existence of each other, and do not communicate with each other. These self-contained subsets are called *flocks*. Since flocks are independent, the evaluation of a scenario can be broken down to the evaluation of the flocks found in it.

C. *Scenarios as Phased Mission Systems*

In this evaluation workflow time is dealt with in a discrete manner. Transformation step 1 in Figure 1 assembles a series of static views that constitutes the scenario. In each view the network topology, the connection parameters and the dependability parameters of nodes are considered static, but any of these might vary during the atomic phase changes. At this stage the scenario is represented as a series of static topology views among abstract nodes. The dependability of these models are evaluated by DEEM [5] or Möbius [6] using an algorithm that only need to keep the state space of one phase in the memory, thus making the evaluation efficient.

IV. Conclusion

The goal of the HIDENETS project is to create dependable services based on unreliable, ad-hoc network infrastructures. Ad-hoc, wireless network connections will provide means to communication for mobile nodes and those of the fixed infrastructure.

The evaluation of such infrastructures and technologies from the dependability point of view is non-trivial for several factors: realistic mobility traces have to be generated, models with large state spaces need to be evaluated, time and dynamicity in the environment have to be dealt with.

This paper introduced a modeling methodology that is capable of capturing every aspect that is necessary to capture a scenario. Additionally we try to tackle the problem of state space explosion with several techniques.

References

[1] M. Radimirsch, E. V. Matthiesen, G. Huszerl, M. Reitenspieß, M. Kaâniche, I. E. Svinnset, A. Casimiro, and L. Falai, “Use case scenarios and preliminary reference model,” HIDENETS Deliverable D1.1, October 18 2006.

[2] P. Lollini, A. Bondavalli, J. Arlat, M. Clemetsen, L. Falai, A. F. Hansen, M. B. Hansen, M. Kaâniche, K. Kanoun, M. Kovács, Y. Liu, M. Magyar, I. Majzik, E. V. Matthiesen, A. Nickelsen, J. J. Nielsen, J. G. Rasmussen, T. Renier, and H.-P. Schwefel, “Evaluation methodologies, techniques and tools (final version),” HIDENETS Deliverable D4.1.2, December 17 2007.

[3] M. N. Jensen and A. Nickelsen, “Evaluation of routing dependability in MANETs using a topology emulator,” M.S. thesis, Aalborg University, Aalborg, Denmark, 2007.

[4] I. Majzik, A. Pataricza, and A. Bondavalli, “Stochastic dependability analysis of system architecture based on UML models,” in *Architecting Dependable Systems*, R. de Lemos, C. Gacek, and A. Romanovsky, Eds., pp. 219–244, Berlin, 2003. Springer Verlag.

[5] A. Bondavalli, S. Chiaradonna, F. Di Giandomenico, and I. Mura, “Dependability modeling and evaluation of multiple-phased systems using DEEM,” *IEEE Transactions on Reliability*, 53(4):509–522, 2004.

[6] University of Illinois at Urbana-Champaign, *Möbius*, 2006.