

Replace this file with `prentcsmacro.sty` for your meeting,  
or with `entcsmacro.sty` for your meeting. Both can be  
found at the [ENTCS Macro Home Page](#).

# Formal Methods in the Wireless Network Domain

Ansgar Fehnker

*National ICT Australia<sup>1</sup>  
Locked Bag 6016  
The University of NSW  
Sydney NSW 1466  
Australia*

Formal Methods have a long track record of developing tools, methods and techniques, to verify protocols, software and hardware systems. Wireless Networks combine these areas in a characteristic way. Due to the nature of the network nodes, hardware is comparatively small as is the software running on it. Due to the nature of the network algorithms and protocols should be distributed and concurrent. An important aspect of a wireless networks is that nodes use multi-hop communication on an unreliable medium, and that the network is subject to dynamic changes and environmental interference. This talk presents experience from a research project on Formal Methods in the wireless network domain, and in particular how model checking can help with the design of the different aspects of wireless networks, and how they can position themselves with respect to network simulators, the main tool for developers other than testing in this realm.

The project Formal Methods of Performance Analysis of Wireless Network Applications (PEWNA) was a small-scale three year project within the Formal Methods program of National ICT Australia. The PEWNA project demonstrated the use of formal methods, in particular model checking, for wireless applications, and it applied them successfully to time-synchronization protocol, gossiping protocols, and power management protocols.

The purpose of model checking however differed for the different applications. Model checking was of course used to show correctness [4]. But for protocols that are known to fail for some problematic configurations, it can be also used to identify all problematic scenarios [5]. The counterexamples then help to address some of the problematic scenarios, even though complete correctness will not be achieved. Another use of model checking it to use for optimization to compute optimal op-

---

<sup>1</sup> National ICT Australia is funded through the Australian Government's *Backing Australia's Ability* initiative, in part through the Australian Research Council.

eration schedules [6]. Finally, we used model checking tool to obtain performance and network measures, such a reception rates, for given protocols [1,2,3].

Given the different purposes, there are roughly speaking two use cases for formal methods. The most traditional and most common use case is to use them to thoroughly analyze a protocol or system [3,4,5,6]. For this it is necessary to develop detailed models, and use the full range of tools and techniques to tackle the problem. This use case assumes an expert user. Any improvements can be leveraged to any implementation of the protocol, which justifies the effort. On the other hand there is the case when model checking is used in the design process to compute performance measures for many iterations of a wireless network design [1,2]. Each time the designer makes a change to the topology or the network parameters, the analysis has to be repeated. To become feasible, we need abstract modelling templates such that the response time of the model checker remain acceptable. The aim is that model checking will become transparent to the user, and just one tool among others to assess the quality of the current network design. This use case targets non-experts in formal methods, with a background in wireless network design.

The main motivation at the beginning of the PEWNA project was the observation that simulation, the main tool used in the wireless network domain, is fraught with problems. It has for example been observed in that different simulators can produce vastly different results, even for very simple protocols. The size of networks that can be simulated are typically several orders of magnitude higher than the size of networks that can be model checked. However, this is a skewed comparison, since simulation, especially in the presence of probabilistic protocols and a probabilistic environment, cannot provide complete coverage. The strength of simulation to provide very detailed illustrative traces for debugging. Furthermore, model checking can be used to provide performance measures that are difficult if not impossible to obtain by simulation. The project showed that for formal methods to be successful in the wireless network domain, it is not necessary to compete with simulation tools, but that they can position themselves as valuable tools in their own right.

## References

- [1] Boulis, A., A. Fehner, M. Fruth and A. McIver, *Cavi – simulation and model checking for wireless sensor networks*, in: *Quantitative Evaluation of Systems (QEST 2008)* (2008).
- [2] Fehner, A., M. Fruth and A. McIver, *Graphical modelling for simulation and formalanalysis of wireless network protocols*, in: *Proc. Workshop on Methods, Models and Tools for Fault-Tolerance (MeMoT'07) at the 7th International Conference on Integrated Formal Methods (IFM'07)*, 2007.
- [3] Fehner, A. and P. Gao, *Formal verification and simulation for performance analysis for probabilistic broadcast protocols*, in: *Ad-Hoc, Mobile, and Wireless Networks, 5th International Conference, ADHOC-NOW 2006, Ottawa, Canada, August 17-19, 2006*, Lecture Notes in Computer Science **4104** (2006), pp. 128–141.
- [4] Fehner, A. and A. McIver, *Formal techniques for the analysis of wireless networks.*, in: T. Margaria, A. Philippou and B. Steffen, editors, *S2nd International Symposium on Leveraging of Formal Maethods, Verification and Validation (IEEE-ISOLA)*, IEEE proceedings, 2006.
- [5] Fehner, A., L. van Hoesel and A. Mader, *Modelling and verification of the lmac protocol for wireless sensor networks*, in: J. Davis and J. Gibbons, editors, *Proceedings of the 6th International Conference on Integrated Formal Methods, IFM 2007, Oxford, Britain*, Lecture Notes in Computer Science (2007), pp. 253–272.
- [6] McIver, A., *Quantitative mu-calculus analysis of power management in wireless networks*, in: *International Colloquium of Theoretical Aspects of Computing (ICTAC 2006)*, Lecture Notes in Computer Science (2006).