Internship subject (Master 2 or Master 1)

Protocols validation using Open Automata

Advisors: Rabéa Ameur-Boulifa

contact: rabea.ameur-boulifa@telecom-paris.fr

Context

As applications grow increasingly complex, concurrency and communication assume ever more significant roles in their design process. Specifically, highly concurrent communication models require genuinely scalable communication architectures. To tackle the substantial engineering complexity involved, designers typically organize a communication network into a series of layers. Each layer functions as a 'black box,' offering services that the higher layer above it can utilize. Generally, these upper layers provide communication services with superior properties and build upon the foundational services offered by the lower layers.

Although ensuring the correctness of communication protocols is a sensible concern, we still lack efficient, reliable, and automatic mechanisms to conclusively prove the correctness of a given protocol. This gap in effective and manageable verification techniques significantly impacts how protocols are developed and tested. The reliability and interoperability of protocols depend on their precise definition and implementation. For instance, in the initial version of Bluetooth, devices from different vendors couldn't communicate. This issue arose because certain aspects of the standard were open to interpretation, leading different vendors to implement it in divergent ways, resulting in incompatible devices. Even today, the IETF (Internet Engineering Task Force) [2] requires rapid assessment of the accuracy of the correctness and limitations of internet drafts.

In the theory of communication and concurrency [3], validating the correctness of systems involves analyzing behavioral equivalences between components. In our prior work [5, 4], we developed a new model of communication and concurrency called Open Automata. This model provides a suitable and practical theoretical framework for reasoning about complex concurrent systems.

Objectives

The objective of the internship is to go beyond theoretical aspects and demonstrate, through experimentations, the relevance of Open Automata for modelling and analysing real-life distributed applications and network protocols. More specifically, the internship would follow the following steps:

- Familiarization with technical material: the semantics of Open Automata [5] on which the models are based. In particular the VERCORS plateform [1] which is Java platform dedicated for the analysis and verification of safety and security properties of distributed applications.

- Model one state of the art IETF protocol selected within the Open Automata formalism.
- So we will assess the strength and the expressive power of the formalism, and propose extensions or enhancements if necessary.

References

[1] https://team.inria.fr/scale/software/vercors/

[2] The Internet Engineering Task Force, http://www.ietf.org/

[3] R. Milner. Communication and Concurrency. Prentice-Hall International, Englewood Cliffs, 1989.

[4] Rabéa Ameur-Boulifa, Quentin Corradi, Ludovic Henrio, Eric Madelaine: Refinements for Open Automata . 21st International Conference on Software Engineering and Formal Methods, SEFM 2023, Eindhoven, Netherlands. pp.11-29, (Extended version) ⟨hal-04193421⟩.

[5] Rabéa Ameur-Boulifa, Ludovic Henrio, Eric Madelaine: Compositional equivalences based on Open pNets. Journal of Logical and Algebraic Methods in Programming, 2022, 131, pp.100842. ⟨hal-03894031⟩.