A TLA Solution to the Specification and Verification of the RLP1 Retransmission Protocol

Abdelillah Mokkedem, Michael J. Ferguson, and Robert deB Johnston

INRS-Telecommunications
16, Place du Commerce, Nun's Island
Québec H3E 1H6, Canada
Email: mokkedem@inrs-telecom.uquebec.ca

Abstract. This paper presents a series of TLA$^+$ specification/implementations that lead to an implementation of the retransmission policy of RLP1, the Radio Link Protocol proposed for TDMA (Time Division Multiple Access) digital cellular radio. Both safety and liveness properties are proved for SWPInitial, a very abstract, but formal, specification of a sliding window protocol. The rest of the work consists of a series of refinements which finally result in a model of RLP1. Each refinement step is formally proved. In all cases the most difficult part of the proof is for liveness. We prove, formally and rigorously, and parametrised by the window size $N$, that the model of RLP1 obtained from the last refinement step is an implementation of the initial specification SWPInitial, and thus inherits safety and liveness properties proved for all the higher-level specifications. The specifications are written in TLA$^+$, a formal language based on TLA, and proofs are given in Lamport's hierarchical proof-style. Most proof steps are checked mechanically in Eves.

1 Introduction

In this paper, we investigate the use of TLA (Temporal Logic of Actions) due to Lamport [1,8,9], for the specification and verification of a series of sliding window protocols, the last of which captures the actual retransmission algorithm of an early version of the real protocol RLP1 (Radio Link Protocol) [13]. RLP1 is the data link protocol for TDMA (Time Division Multiple Access) digital cellular radio and has recently been standardized by TIA (Telecommunications Industry Association). RLP1 is the first protocol that has been standardised where there was a formal language, namely SDL [2], that was the definitive specification of the standard rather than informal text [4,5]. In addition, the entire protocol, including connection processing and retransmission algorithm was modeled and validated [5] during the actual standardisation using a combination of SDL and Promela/SPIN [6].

TLA is a (linear) temporal logic with an associated specification/implementation methodology [9] for refining abstract specification to a concrete implementation. This methodology was used to create a sequence of models for that
started with simple finite, but unbounded sets as data structures, unbounded naturals for message identifiers, and a conventional retransmission algorithm, and then incrementally added detail for creating finite and bounded data structures and identifiers, finally adding the retransmission details of RLP1. Each new specification was proven to be an implementation of the previous specification, and various invariants and liveness theorems that were relevant to the new specification were proved. The TLA specification/implementation methodology ensures that the implementation inherits all the invariants and theorems that were true of the previous specification. The complete proofs, which may be found in [11], have been done with sufficient low-level detail that it has been possible to check the low level action steps with the theorem prover Eves [3,12] (developed by ORA Canada). Due to space limitations, most proofs have been omitted from the paper. However, because of the difficulty of proving non-trivial liveness properties, an example of such a proof is given in Section 4.

The paper is organised as follows: Section 2 gives a brief description of TLA and Section 3 gives a brief description of the retransmission algorithm of RLP1. Sections 4 to 7 give the series of specifications that add the detail necessary to create the final RLP1 specification. These are

Section 4: SWP with unbounded naturals as message identifiers, complete receiver state feedback, fixed window of size N, and message retransmission if unacknowledged. Sender State consists of the (unbounded) sets of Acknowledged messages (A) and Sent messages (S), and the Receiver state by the (unbounded) set of Received messages (R).

Section 5: The unbounded Receiver and Sender states are represented by finite bounded structures consisting of lower window edges, message maps, and the actions to manipulate them.

Section 6: The naturals used for message ids are replaced by ids modulo M.

Section 7: The Basic and Pre-emptive retransmission modes for RLP1 are added.

Section 8 discusses a simple unification and improvement of the algorithm for declaring a message known lost while Section 9 concludes.

2 A Short Introduction to TLA and TLA+

TLA is a (linear) temporal logic. Temporal logic formulas contain flexible variables that may change with a change in state while rigid variables do not. The meaning $[S]$ of a TLA formula $S$ is a boolean function on behaviors, where a behavior is an infinite sequence of states and a state is an assignment of values to all flexible variables. A behavior $\sigma$ satisfies a formula $S$ iff $[S](\sigma)$ equals TRUE. A formula is valid iff it is satisfied by all behaviors. A full description of TLA may be found in [9]. TLA+ is a formal language based on TLA and Zermelo-Fraenkel set theory [10]. Figure 1 gives the complete set of inference rules for TLA and Figure 2 the meaning of TLA+ keywords and symbols.