Title: *Formal Verification of Liveness Properties of Distributed System Protocols by Model Checking*

Abstract: A fully automated framework for verifying liveness properties of a class of distributed system protocols is the final objective of this dissertation work. First-order modal logic with arithmetic predicates (FOMLAP) has been chosen to specify the properties to be proved. Also, for complete automation, model checking paradigm is chosen rather than a theorem proving paradigm.

For many distributed systems, all processes executing the protocol have identical behaviour; so one process behaviour is provided using a finite state machine model with data variables referred to as FSMD model. A model checker would need a composite model encompassing all the processes depicting the behaviour of the protocol. A parametric model, however, cannot be constructed forcing the reasoning mechanism to proceed backward, starting from an abstraction of some specific composite state where the property is likely to hold and moving towards some initial composite state.

Conventional model checkers identify the states where a formula holds from the set of states where the constituent sub-formulae of the formula holds. So, a mechanism for decomposing the FOMLAP encoding the property is needed. A terminating decomposition framework for FOMLAP formulae has been devised to identify the constituent literals. The soundness and completeness of the decomposition rules have been treated. The termination, soundness and completeness treatments of the overall framework have also been provided.

The implementation of the model checker has been carried out using a backward reasoning mechanism avoiding construction of the complete composite model; issues pertaining to the indices associated with the chosen state literals have been addressed; finally, an attempt has been made for realizing a parametric verifier. A formal procedure for identification of recurrences occurring during backward reasoning and thereby, detecting scope of induction has been devised.

The model checker provides scale up by two to three orders of magnitude for the HS and LCR protocols, respectively, over the conventional model checking tools like NuSMV or SPIN and permitted a further scale up of one order of magnitude through computational induction.

The soundness treatment of the overall model checking procedure has been provided. A prototype has been implemented as a proof of concept.

To implement a full-fledged parametric model checker (for any value of n) with induction, it requires certain inductive conjectures to be synthesized as first-order formulae and the entire implementation has to be symbolic. This has been kept as a future scope. Similarly, the subgoal of constructing a counterexample, in case of failures, has not been incorporated.