World Academy of Science, Engineering and Technology
International Journal of Civil and Architectural Engineering
Vol:12, No:10, 2018

Using the Weakest Precondition to Achieve Self-Stabilization in Critical Networks

Authors : Antonio Pizzarello, Oris Friesen

Abstract : Networks, such as the electric power grid, must demonstrate exemplary performance and integrity. Integrity depends on the quality of both the system design model and the deployed software. Integrity of the deployed software is key, for both the original versions and the many that occur throughout numerous maintenance activity. Current software engineering technology and practice do not produce adequate integrity. Distributed systems utilize networks where each node is an independent computer system. The connections between them is realized via a network that is normally redundantly connected to guarantee the presence of a path between two nodes in the case of failure of some branch. Furthermore, at each node, there is software which may fail. Self-stabilizing protocols are usually present that recognize failure in the network and perform a repair action that will bring the node back to a correct state. These protocols first introduced by E. W. Dijkstra are currently present in almost all Ethernets. Super stabilization protocols capable of reacting to a change in the network topology due to the removal or addition of a branch in the network are less common but are theoretically defined and available. This paper describes how to use the Software Integrity Assessment (SIA) methodology to analyze self-stabilizing software. SIA is based on the UNITY formalism for parallel and distributed programming, which allows the analysis of code for verifying the progress property p leads-to q that describes the progress of all computations starting in a state satisfying p to a state satisfying q via the execution of one or more system modules. As opposed to demonstrably inadequate test and evaluation methods SIA allows the analysis and verification of any network self-stabilizing software as well as any other software that is designed to recover from failure without external intervention of maintenance personnel. The model to be analyzed is obtained by automatic translation of the system code to a transition system that is based on the use of the weakest precondition.

Keywords : network, power grid, self-stabilization, software integrity assessment, UNITY, weakest precondition
Conference Title : ICCISE 2018 : International Conference on Critical Infrastructure Systems Engineering
Conference Location : Los Angeles, United States
Conference Dates : October 30-31, 2018

Open Science Index, Civil and Architectural Engineering Vol:12, No:10, 2018 publications.waset.org/abstracts/86956.pdf