Egy elosztott diagnosztikai protokoll formális verifikációja és implementációja

Sisak Áron VI. Inf., aron@inf.bme.hu

Konzulens: Bokor Péter, petbokor@mit.bme.hu
Méréstechnika és Információs Rendszerek Tanszék

Napjainkban az elosztott rendszerek szinte mindenütt megtalálhatóak. Ezek hibatűrésének biztosításához elengedhetetlen megfelelő diagnosztikai protokollok használata, azaz a hibás egységek azonosítása. Az *elosztott diagnosztikai* algoritmusok lehetővé teszik a diagnosztikát anélkül, hogy újabb – dedikált diagnosztikai – egységgel bővítenénk a rendszert (ami jelentősen csökkenti a rendszer hibatűrését), kihívást jelent ugyanakkor relatív bonyolultságuk, főként a jó csomópontokban létrehozandó egységes diagnosztikai kép kialakítása miatt. A dolgozat egy, a DECOS projektben kifejlesztett, elosztott diagnosztikai protokoll formális verifikációjával és implementációjával foglalkozik.

Egy rendszer *formális verifikációja* esetén a rendszer modelljéből kiindulva, matematikai pontossággal bizonyítjuk, hogy a rendszer megfelel bizonyos helyességi kritériumoknak. Diagnosztika esetén például ilyen tulajdonság lehet a diagnosztikai helyesség, azaz, hogy minden hibásnak diagnosztizált egység valóban hibás. A formális verifikációs technikák közül a *modellellenőrzés*re koncentrálunk, ami lehetővé teszi az automatizált bizonyítást (munkánk során a SAL modellellenőrző keretrendszert használjuk).

A modellellenőrzés csak korlátozott méretű modelleket tud kezelni, ugyanakkor az (elosztott) *hibatűrő* protokollok rendszerint nagy állapotteret eredményeznek, még akkor is, ha a viselkedés sokféleségét egy ún. hibamodell korlátozza. Így már kisméretű rendszerek (4-5 csomópont) esetén is kezelhetetlen méretű modellekhez juthatunk. Az állapottér robbanásának kezelésére egy újszerű *absztrakció*s technikát alkalmazunk, amely az elosztott diagnosztikai protokollokra jellemző, modelltérben rejlő szimmetriát használja ki a modell egyszerűsítésére.

Az algoritmus egy hibrid hibamodellt használ, különbséget téve különböző hibaosztályok között, így a legrosszabb esetben fellépő hibákat feltételező hibamodellekhez képest nagyobb hibatűrés érhető el. A hibafedést illetően a protokoll leírása nem tartalmaz pontos adatokat, így a modellellenőrzés járulékos feladataként a dolgozat tárgyalja az algoritmus *hibatűrés*ének – azaz a tolerált hibák és a csomópontok száma közötti összefüggésnek – pontos meghatározását.

A DECOS diagnosztikai protokollt a tervezett célplatformokra fejlesztették ki (tekintettel a hibamodellre, csomópontok közötti kommunikációra, stb.). Egy ilyen architektúra a TTTech cég idővezérelt klasztere, amely a TTP kommunikációs protokollt valósítja meg. A dolgozathoz kapcsolódóan, a BME MIT tanszék TTTech klaszterén elkészült a protokoll egy *implementáció*ja, amely lehetővé teszi a formális verifikáció eredményeinek tesztelését.

Irodalom
1. Leonardo de Moura et al.: SAL 2, *volume 3114 of LNCS* (2004)
2. Serafini, M. et al.: On Exploiting Symmetry To Verify Distributed Protocols. *Fast abstract, The International Conference on Dependable Systems and Networks* (2006)
3. Kopetz H. et al.: The Time-triggered Architecture. *Proc. of the IEEE*, 91(1): 112–126 (2003)