MELLÉKLET

Egy hibatűrő elosztott protokoll helyességbizonyítása modellellenőrzéssel

Napjainkban az elosztott rendszerek szinte mindenütt megtalálhatóak. Ezek hibatűrésének biztosításához elengedhetetlen megfelelő diagnosztikai protokollok használata a hibás egységek azonosítására. 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 diplomaterv egy, a DECOS projektben kifejlesztett, elosztott diagnosztikai protokoll formális verifikációjával 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 modellellenőrzésre koncentrálunk, ami lehetővé teszi az automatizált bizonyítást (munkánk során a SAL modellellenőrző keretrendszert használjuk).

Az algoritmus egy hibrid hibamodellt használ, különbséget téve különböző hibaosztályok között, így a kizárólag pesszimista hibákat feltételező hibamodellekhez képest nagyobb hibatűrés érhető el.

A hallgató egy korábbi önálló laboratórium valamint egy TDK dolgozat kereteiben már megismerkedett a témával, aminek során ismertette a protokoll egy korábbi változatának modellellenőrzését. Ez a modell ugyanakkor nem veszi figyelembe számos idővezérelt architektúra sajátosságait, helyette teljesen szinkron kommunikációt feltételez teljes gráf hálózati topológiában. A fő problémát az jelenti, hogy a) idővezérelt rendszerekben a lokális órák a globális időtől való eltérése miatt az üzenetek küldésének és fogadásának időpontjáról az egyes csomópontok más-más képet látnak, és b) az idővezérelt architektúrák tipikusan a teljes gráf topológia helyett busz topológiát alkalmaznak (például a TTA, FlexRay időosztásos rendszerek).

A diplomatervben a hallgató feladatai a következők.

- Röviden tekintse át a felhasznált modellellenőrzési technikát és ismertesse a SAL keretrendszert.
- Ismertesse röviden a TTA idővezérelt architektúrát, különös tekintettel a modellezés során figyelembe vett sajátosságokra.
- Ismertesse a verifikálandó protokollt, annak formális modelljét az idővezérelt architektúrák sajátosságainak figyelembevételével.
- Végezze el a protokoll helyességbizonyítását modellellenőrzés segítségével.
- Értékelje munkáját, vázolva az esetleges továbbfejlesztési lehetőségeket is.

Bokor Péter
doktorandusz