Konszenzus protokollok szimbolikus szimulációval történő helyességbizonyítása

Pintér Norbert V. Inf. , pn552@hszk.bme.hu

Konzulens: Bokor Péter, MIT Tanszék, petbokor@mit.bme.hu

Elosztott hibatűrő protokollok automatikus verifikációja során fellépő állapottér robbanás azt jelenti, hogy a bejárandó állapotok száma a bemenő paraméterek függvényében exponenciálisan nő. Egy természetes megoldás a problémára absztrakció alkalmazása, amellyel jelentősen csökkenthető a bejárt állapottér mérete. Az absztrakció lényege, hogy a rendszert leíró tulajdonságok közül csak a verifikáció szempontjából releváns információt tartjuk meg a rendszer modelljében és azok segítségével modellezzük a rendszerünket. Az úgynevezett szemantikus absztrakciós technikák a rendszerek egy osztályának valamely jellegzetes tulajdonságát kihasználva érik el a redukciót.

A hibatűrő protokollok egy általános osztálya többségi szavazást alkalmaz a hibás csomópontok hatásának kiküszöbölésére. Egy klasszikus példa a Bizánci generálisok problémája, ami egy szinkron konszenzus feladat elosztott rendszerben, úgy, hogy a hibák minőségére semmilyen megkötést nem tehetünk. Ilyen protokollok esetén többféle szimmetrián alapuló absztrakciós technikát lehet alkalmazni az állapottér csökkentésére. Egyes absztrakciók a probléma permutációs szimmetriáját használják ki. Ez azt jelenti, hogy a többségi szavazás kimenetét nem befolyásolja a bemeneti értékek sorrendje.

Egy másik jelenlévő szimmetria a kompenzációs szimmetria, amely esetén helyes üzenetek kompenzálják a hibás csomópontok által küldötteket. Ennek természetesen előfeltétele, hogy az egészséges csomópontok többségben legyenek, amit tipikusan a protokoll hiba hipotézise definiál. A TDK dolgozatban bemutatásra kerülő szemantikus absztrakció a kompenzációs szimmetriát kihasználva képes az állapotér jelentős redukciójára azáltal, hogy a csomópontok által küldött üzenetek tényleges tartalmát elfedi és azokat csakis szimbolikusan reprezentálja. A szimbólumok közötti kapcsolatok leírása pedig matematikai kényszerekkel valósul meg. A szimbolikus változók kiértékelése ”on-demand” jellegű, azaz amikor arra szükség van a verifikáció során.

A dolgozatban az elért eredményeket a klasszikus Bizánci generálisok problémáján keresztül ismertetem – mint demonstratív esettanulmány -, amikor az (esetleges rosszindulatú) generálisok „szóbeli” üzeneteken keresztül kommunikálnak egymással. Az ismertetett absztrakció, azonban, alkalmazható minden üzenetekkel működő és a hibatűrést újraküldéssel megvalósító (ún. kör-alapú) protokoll esetén. A Bizánci generálisok problémája esetében a skálázhatóság jelenti a kihívást, ami azt jelenti, hogy a körök, illetve a hibás csomópontok száma okozza az állapottér robbanását.

A választott verifikációs technika a modellellenőrzés, amely kimerítő keresést (szimulációt) hajt végre a rendszer állapotmodelljén. A modellellenőrző bemenete a rendszer formális leírása, illetve a vizsgálandó kifejezés, kimenete pedig a kifejezés helyessége, vagy pedig egy ellenpélda. A technika legfőbb előnye, hogy teljesen automatikus, azaz nem igényel felhasználói interakciót, mint például tételbizonyítás esetén. A modelleket SAL nyelven implementálom, amely egy általánosan használt modellellenőrző eszköz.