Robuste Komponentensysteme durch Protokollprüfung

Andreas Both (Unister GmbH Leipzig)
Wolf Zimmermann (Universität Halle)

Abstract: Ein robustes und wiederverwendbares Softwaresystem sollte eine komponentenbasierte oder serviceorientierte Softwarearchitektur haben, da idealerweise durch einfaches Austauschen oder Ergänzen von Black-Box Komponenten (insbesondere auch Web-Services) ein Softwaresystem weiterentwickelt werden kann. Dieser Idealzustand ist derzeit nicht erreicht, denn das Zusammensetzen oder Verändern von Komponenten führt häufig zu unerwarteten Effekten. So verhalten sich Komponenten anders als erwartet, wenn sie in einem anderen als dem erwarteten Kontext eingesetzt werden. Es entstehen auf Grund der in vielen Komponententechnologien vorhandenen Nebenläufigkeit Verklemmungen auf Grund der Komponentenkomposition und Komponenten stürzen bei ihrer Ausführung ab, weil sie nicht vorhersehbar genutzt werden. Ursachen sind u.A., dass die Komposition rein syntaktisch an Hand von Schnittstellen erfolgt und dass Komponenten zustandsbehaftet sind. Letzteres bedingt, dass eine unerwartete Aufrufreihenfolge der Dienste einer Komponente fehlerhaftes Verhalten verursachen kann.

Wir schlagen - wie eine Reihe anderer Arbeiten - vor, dass zusätzlich zu den Schnittstellen Komponenten um Protokolle erweitert werden, die die Menge der zulässigen Aufrufreihenfolgen spezifiziert. Die Benutzung einer Komponente C in einem Komponentensystem ist die Menge tatsächlicher Aufrufreihenfolgen. Eine Komponentenprotokoll für Komponente C prüft konservativ, ob deren Benutzung Teilmenge des Protokolls ist. Konservative Prüfung bedeutet, dass zwar Fehlalarme möglich sind, aber Positivmeldungen auf jeden Fall korrekt sind. Die meisten Arbeiten spezifizieren die Protokolle als der Komponenten durch reguläre Ausdrücke und beschreiben das Verhalten von Komponenten durch Petri-Netze wie z.B. van der Aalsts Workflow-Netze. Das Problem der Protokollprüfung wird dann auf ein Erreichbarkeitsproblem auf Petri-Netze reduziert. Diese Vorgehensweise stößt jedoch an ihre Grenzen, wenn rekursive Prozeduraufrufe ohne Beschränkung der Rekursionstiefe erlaubt sind (innerhalb von Komponenten bzw. Services und über Komponentengrenzen hinweg), weil dies zu falschen Positivaussagen führen kann. Unser Ansatz verallgemeinert die bisherigen Protokollprüfungsmethoden auf eine unbeschränkte Nebenläufigkeit und unbeschränkte Rekursionstiefe. Der Vortrag diskutiert die Grenzen bestehender Ansätze und die Verallgemeinerung auf unbeschränkte Rekursionstiefe.

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4