Asynchrone Kommunikation bei objektorientierten verteilten Systemen mit Echtzeitbedingungen

Marc Schanne
Software Engineering (SE)
FZI Forschungszentrum Informatik
schanne@fzi.de

Zusammenfassung

Mit dem wachsenden Einsatz von verteilten Anwendungen mit Echtzeitanforderungen in eingebetteten Systemen wächst das Interesse an objektorientierten Programmiertechniken, um sicherheits- und geschäftskritische Systeme zu entwickeln. Die hier vorgestellte Methodik verwendet asynchrone Kommunikation bei der einfachen Entwicklung solcher verteilten Anwendungen und definiert eine objektorientierte Umgebung, die nebenläufige Programmierung mit Kontrollfäden erlaubt und bei der Kommunikation Ende-zu-Ende-Vorhersagbarkeit, Rechtzeitigkeit, Schnelligkeit und Echtzeitbedingungen garantieren kann. Mit Einsatz einer Java-VM, die die "Real-Time Specification for Java" (RTSJ) unterstützt, mit prioritätsbasierter Ablaufkoordinierung, einem Software-Entwurfsmuster für asynchronen Nachrichtenempfang und abfertigung und der Nutzung von COTS Hardware- und Software-Komponenten ist es möglich, Echtzeitanforderungen zu unterstützen und dies bereits durch statische Analyse zu verifizieren.
Schlagworte: Echtzeit, Nachrichtendienst, Vernetzung, Eingebettete Systeme

Einführung

Diese Kurzfassung des Workshopbeitrags [3] präsentiert die aktuelle Forschungsarbeit zu EDV- und Netzwerk-Modellen für sicherheits- und geschäftskritische Java Anwendungen ("High-Integrity Java Applications", HIJA[1]) [1, 2]. Der darin vorgestellte Nachrichtendienst, das EventChannelNetwork (ECN) [4] ist für moderne Echtzeitbusse und netzwerke optimiert und [3] bietet eine Anforderungsanalyse, die die Nutzung asynchroner und direkter Publiziere/Abonniere-Nachrichtenkommunikation motiviert. Dieser Artikel führt die notwendigen Fachbegriffe kurz ein und über eine Diskussion verwandter Arbeiten wird eine Methodik für den Entwurf verteilter Anwendungen in eingebetteten Systemen unter Echtzeitanforderungen definiert. Es werden sicherheits- und geschäftskritische Systeme sowohl für Regelungstechnik, Automation, Avionik oder Automobiltechnik, als auch Anwendungen in Telekommunikation oder Multimedia adressiert. Für weiterführende Quellen und Referenzen sei aufgrund der Kürze dieser Zusammenfassung auf andere Beiträge des Autors sowie auf die Webseite des Dissertationsprojektes [4] verwiesen.

[1] IST-511718, Forschungsprojekt im 6. Rahmenprogramm der Europäischen Kommission

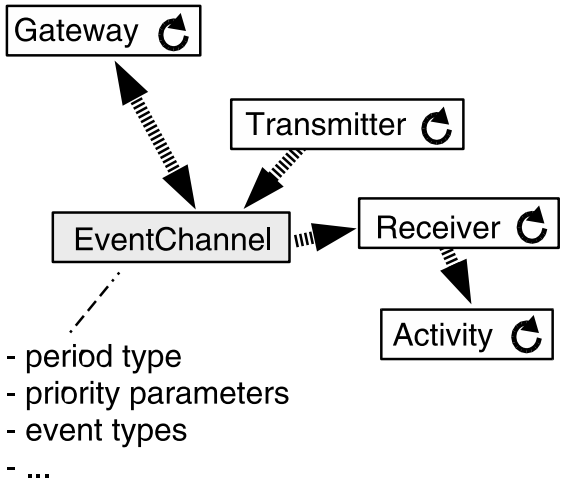

Abbildung 1: Nachrichtenkanal mit Attributen

Fachbegriffe und Grundlagen

Aus der Anforderung an Rechtzeitigkeit und Erfüllung der Kommunikation in gegebenen Zeitgrenzen lässt sich eine Klassifizierung von Echtzeit mit harten und weichen Anforderungen ableiten. Diese Einteilung definiert sich über die schlechteste anzunehmende und die durchschnittliche Ausführungszeit.

Alle Antworten mit harten Zeitschranken müssen innerhalb des verfügbaren Zeitfensters ausgeführt sein. Wenn das System eine Zeitschranke nicht einhält ist das Gesamtsystem unvorschriftsmäßig und im Bereich eingebetteter Systeme mit sicherheits- und geschäftskritischen Anwendungen kann dies zu Gefahr für Leib und Leben, Schädigung der Umgebung oder zu signifikanten finanziellen Verlusten führen.

Weiche Zeitanforderungen werden durch die Forderung nach einer durchschnittlichen Antwortzeit charakterisiert. Verfehlte Zeitschranken äußern sich in Mängeln der allgemeinen Dienstqualität und nicht im vollständigen Systemausfall.

Neben Echtzeitbedingungen müssen Anwendungen in eingebetteten Systemen auch mit Einschränkungen bei Ressourcen für Verarbeitungsgeschwindigkeit, Speicherkapazität, Kommunikationsbandbreite und verfügbarer Energie umgehen. Um diesen Einschränkungen gerecht zu werden implementiert das ECN einen einfachen verbindungslosen und asynchronen Nachrichtendienst für verteilte Komponenten sowohl für Systeme mit harten, als auch mit weichen Echtzeitbedingungen. Das in [5] vorgestellte Entwurfsmuster mit Empfänger-Kollektiv, Aktivitätsmanager

und Warteschlangen ist in beiden Versionen identisch. Die Kommunikation findet transient ohne zentrale Administrationseinheit statt und verwendet die im Umfeld eingebetteter Systeme weit verbreiteten Netzwerke oder Feldbussysteme mit Rundruf[2]. Der themenbasierte Publiziere/Abonniere-Nachrichtendienst mit "Push"-Übertragungsmodell nutzt diese ohne großen Protokolloverhead effizient aus. Die dynamische Version des ECN für flexible und weiche Echtzeitbedingungen bietet ein Fehlermodell mit "Exceptions", mit dem die Anwendungsschicht auf Fehler in der Kommunikation oder der Verarbeitung reagieren kann [7]. In der statisch verifizierbaren Implementierung für harten Echtzeitbedingungen ist dies nicht vorgesehen und Ausnahmen bewirken einen Fehler des Systems.

Verwandte Arbeiten

Verwandte Arbeiten im Bereich plattformunabhängiger Kommunikation und architekturneutraler Kommunikation identifiziert [3] bei der Object Management Group (OMG) und ihrer Definition eines Objekte/Dienste-Informationsmodells für heterogene Applikationen. Mit der Echtzeiterweiterung der "Common Object Request Broker Architecture" (RT-CORBA) werden Echtzeit- und sicherheits- oder geschäftskritische Systeme adressiert. Ein weiterer Ansatz der OMG, um mit beschränkten Ressourcen und typischen Problemen eingebetteter Systeme umzugehen, stellt die MinimumCORBA Spezifikation dar. Beide Spezifikationen sind zwar orthogonale Weiterentwicklungen der CORBA Rahmenarchitektur, aber die Integration der unterschiedlichen Anforderungen für eine CORBA-Implementierung auf eingebetteten Systemen mit beschränkten Ressourcen und Echtzeitbedingungen bleibt unklar. Auch die TCP/IP-Orientierung von CORBA und die Bereitstellung von asynchronen Kommunikatonsdiensten auf Basis synchroner Kommunikation müssen beim Einsatz mit eingebetteten Systemen kritisch betrachtet werden.

Konzepte die von Hardware-Seite die Erfordernisse von verteilten Echtzeitsystemen angehen sind ebenfalls in der aktuellen Entwicklung. Mit der "Open System Architecture - Platform for Universal Services" (OSA+) wird auf einer Dienste-orientierten Mikrokern-Architektur eine Auftragsbearbeitung eingeführt. Die zu komplexe Infrastruktur einer CORBA Middleware wird durch eine reduzierte Mikrokern-API ersetzt. Auf diesem Kern mit nur 6 Funktionen müsste eine objektorientierte Schnittstelle zur Nutzung in hochsprachlich entwickelten, sicherheits- oder geschäftskritschen Systemen aber erst noch implementiert werden.

[2] Die Anforderungsanalyse [3] diskutiert auch die grundsätzliche Eignung für Punkt-zu-Punkt-Kommunikationsnetze wie z.B. deterministisches Ethernet.

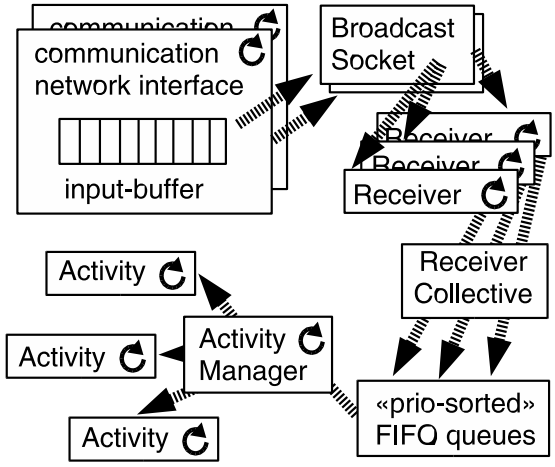

Abbildung 2: Datenfluss beim Nachrichtenempfang

Methodik

Das ECN erfüllt mit einem direkten Publiziere/Abonniere-Nachrichtendienst die Anforderungen für Echtzeit und Verteilung in modernen und zukünftigen sicherheits- und geschäftskritischen Systemen.

Neben aktiven Kommunikationskomponenten[3] wird der Nachrichtendienst im wesentlichen über logische Nachrichtenkanäle definiert (vgl. Abb. 1). Mit diesen können Nachrichten zu einem Thema gruppiert werden und über Attribute wie Häufigkeit und Verarbeitungsfristen wird die Priorität der verarbeitenden Kontrollfäden bestimmt. Aus diesen Informationen sowie verfügbaren Pufferkapazitäten der Netzwerkzugangspunkte zum verwendeten physikalischen Kommunikationsnetzwerks wird die notwendige Speicherkapazität der Nachrichten-Speicherschlangen berechnet [6].

Struktur und Interaktion

Das ECN trennt zwischen Empfang und Verarbeitung der eingehenden Nachrichten [7], Abbildung 2 zeigt die aktiven Elemente sowie Puffer und Schlangen beim Empfang von Nachrichten. Um die Verarbeitung aller Nachrichten gewährleisten zu können verwendet des ECN ein Kollektiv von Empfängerkontrollfäden mit höchster Priorität, sie werden periodisch ausgeführt und sind dafür verantwortlich, eintreffende Nachrichten direkt entgegenzunehmen oder aus dem Hardware-Puffer des Netzzugangspunktes zu lesen und sie in ein Warteschlangesystem einzureihen. Die Weiterverarbeitung erfolgt mit Kontrollfäden, die abhängig von den Attributen der zugeordneten Nachrichtenkanäle mit "rate monotonic" Zuordung feste Ausführungsprioritäten erhalten, Tabelle 1 zeigt ein Beispiel für mögliche Prioritäten für die Ablaufkoordinierung. Sporadische[4] Nachrichten werden dabei in

[3] Sender, Empfänger und Brücken zwischen verschieden physikalischen Netzwerken

[4] Aperiodisch mit einer Mindestzwischenzeit

example	release	deadline	priority
receiver S	sporadic	./.	highest
receiver 1	periodic	./.	highest a)
receiver 2	periodic	./.	highest a)
manager	periodic	./.	higher
handle	waiting	short	high b)
handle	waiting	medium	medium b)
handle	waiting	long	low b)

a) abhängig von Empfangspuffergröße und Periode der Nachrichtenkanäle auf dem phys. Netzwerk
b) Zuordnung nach "deadline monotonic"

Tabelle 1: Ablaufkoordinierung aktiver Objekte

einem periodisches Muster behandelt und eine statische Analyse der Ablaufkoordinierung ermöglicht.

Softwareentwurfsmethode

Beim Einsatz mit Systemen unter harten Echtzeitbedingungen ist eine statische Analyse der Ablaufkoordinierung notwendig. Das ECN ist in diese Analyse integriert und die Attribute der verwendeten Nachrichtenkanäle sind statisch bekannt und können in einer XML-Beschreibung auch für die Programmgenerierung genutzt werden.

Durch die Trennung zwischen Geschäftslogik und Kommunikationssystem ist es so möglich für die Verwendung des ECN Programmierkonstrukte der 5. Generation mit Beschreibung von Systemvoraussetzungen und Leistungsanforderungen zu definieren um ein höheres Maß an Zuverlässigkeit, Genauigkeit und Sicherheit zu erzielen.

Beispiel für diese Beschreibung ist die Nutzung von Hardware- oder Laufzeitsystemprofilen.

```
<node name="system">
 <hw-spec>uri</hw-spec>
 <socket name="ttp">
  <code>TTPSocket.instance()</code>
  <buffer>200</buffer>
 </socket>
```

Außerdem wird mit Definition von Nachrichtenkanälen die Publiziere/Abonniere-Interaktion zwischen Dienstgeber- und Dienstnehmerkomponenten definiert und die Festlegung von Prioritäten für die Empfangs- und Ausführungskontrollfäden berechnet.

```
<channel id="13" name="status">
 <periodic>100ms</periodic>
 <deadline>80ms</deadline>
 <event id="1" name="A">
  <size>50</size>
 </event>
</channel>
```

Ausblick

Durch die Integration in europäische Forschungsprojekte versucht die vorgestellte Dissertation realistische Einsatzszenarien als Testumgebung zu nutzen. Die Verifikation der Vorteile einer asynchronen, nachrichtenbasierten Publiziere/Abonniere-Kommunikation für aktuelle und zukünftige eingebettete Systeme mit sicherheits- oder geschäftskritischen Anforderungen ist Ziel weiterer Arbeiten [4].

Weitere Forschungsaktivitäten untersuchen, ob das ECN zur Implementierung asynchroner Interaktion mit Future-Objekten aus der "Concurrent"-API von Java 5 auch über entfernte Aufrufe mit harten oder weichen Echtzeitbedingungen geeignet ist. Die direkte Ausnutzung von Rundruf-orientierten Netzwerken und Bussystemen mit dem hier vorgestellten Nachrichtendienst soll für die Implementierung von Gleiche-zu-gleiche-Netzwerkprotokollen mit eingebetteten Systemen ausgenutzt werden. Eine Implementierung des Industriestandards Pastry auf Basis des ECN soll z.B. überflüssigen Protokollstapel einer Lösung mit dem synchronen, entfernten Methodenaufruf (RMI) verhindern. Mögliches Ziel bei der Weiterentwicklung des skalierbaren Publiziere/Abonniere-Nachrichtendienstes ist auch die Verteilung von Daten nach der "Data Distribution Specification" (DDS) der OMG und so eine weitere Standardisierung des ECN.

Literatur

[1] HIJA. High Integrity Java Applications. Project Website. http://www.hija.info, 2004.

[2] HIJA. D8.1 - White Paper. Technical report, The Open Group, June 2005.

[3] M. Schanne. Anforderungsanalyse für asynchrone Kommunikation beim Entwurf von objektorientierten, verteilten Systemen unter Echtzeitbedingungen. In *Workshop Zuverlässigkeit in eingebetteten Systemen. Ada Deutschland Tagung 2005*, pages 23–37, October 2005.

[4] M. Schanne. Event Channel Network. Project Website. http://www.eventchannelnetwork.org, 2005.

[5] M. Schanne. Real-Time Communication with a Receiver Collective, Activity Manager, and Queues. In *Proceedings of IADIS Internatonal Conference Applied Computing 2005*, 2005.

[6] M. Schanne. Real-Time Communication with Direct Publish/Subscribe Event Service. In *Internal report 3rd Workshop on Java Technologies for Real-time and Embedded Systems (JTRES) OOPSLA 2005*, October 2005.

[7] M. Schanne and Dr. J. J. Hunt. Remote Event Service Design. Technical report, FZI Forschungszentrum Informatik, 2004. D4.2 describing the HIDOORS event channel network.