Nutzung der Internet-Radio-Technologie zur Übertragung von GNSS-Daten

Harald Gebhard, Lehrstuhl für Kommunikationstechnik, Universität Dortmund

1 Einleitung

Die Echtzeitübertragung von GNSS-Daten zur Lösung einer Reihe von Geophysikalischen Problemen (Wettervorhersage, Seismologie, Vulkanologie etc.) oder zur Korrektur einer Positionsbestimmung (DGNSS) entspricht aus kommunikationstechnischer Sicht weitgehend der Problemstellung, wie sie bei klassischen Rundfunkübertragungen (Fernsehen, Radio) auftritt. So mag es nicht verwundern, dass die Übertragung von GNSS-Daten ursprünglich über klassische Rundfunkkanäle wie terrestrische Langwelle, UKW oder eine Satellitenübertragung erfolgt ist und teilweise noch erfolgt. Darüber hinaus ist es natürlich auch möglich, die GNSS Daten leitungsgebunden oder mobil (GSM) über Telefonverbindungen zu übertragen.

Die derzeitige rasche Entwicklung des Internets hat ermöglicht, dass traditionelle Rundfunkanwendungen wie Radio oder Fernsehen auch als Echtzeitdatenstrom über das Internet empfangbar sind. Dabei bietet die Vielzahl von angebotenen Internet-Zugangstechnologien (leitungs- oder funkbasiert) die Möglichkeit, Inhalte über unterschiedlichste Wege wie Breitbandkabel, Satellit, DSL oder Mobilfunk zu den Endkunden zu übertragen. Dabei entfällt für die Diensteanbieter die kostenintensive Schaffung einer eigenen Infrastruktur (Sendenetz oder Einwahlknoten).

Betrachtet man diese laufenden Entwicklungen und zieht zusätzlich in Betracht, dass die benötigten Datenraten für GNSS-Beobachtungen im Vergleich zu einem Fernseh- oder Radioprogramm verschwindend gering sind, erscheint es naheliegend, das Internet auch für die kostengünstige Echtzeitübertragung von GNSS-Daten zu nutzen.

Die Generierung von GNSS-Daten erfolgt dabei im einfachsten Fall unmittelbar im GPS-Empfänger einer Referenzstation, kann aber auch aus der Vernetzung von Beobachtungen einer Anzahl von Referenzstationen hergeleitet werden. Der erzeugte Datenstrom muss dann über einen Server unter Verwendung eines geeigneten Protokolls über das Internet zugänglich gemacht werden. Dabei müssen für das System-/Protokolldesign neben einer möglichst globalen Verfügbarkeit (auch mobil) Internet-Sicherheitskonzepte sowie die Möglichkeit eines professionellen Server-Hostings berücksichtigt werden. Nur durch professionelles Server-Hosting in einem Rechenzentrum, beispielsweise in der unmittelbaren Nähe des wichtigsten deutschen Datenverkehrsknotens (De-CIX), kann dauerhaft eine höchstmögliche Verfügbarkeit der Daten über unterschiedlichste Zugangsprovider (z.B. T-Mobil, Vodafone, T-Online) erreicht werden.

Der Beitrag gliedert sich wie folgt: In Abschnitt 2 werden das Systemdesign und die verwendeten Internet-Technologien diskutiert, während auf die einzelnen Systemelemente in Abschnitt 3 näher eingegangen wird. Das aus den Überlegungen entstandene Format „Networked Transport of RTCM via Internet Protocol“ (Ntrip), welches in weiten Teilen dem Internet-Radio „ICE/SHOUTCAST-Protokoll“ entspricht, wird in Abschnitt 4 vertieft, wobei auf die Protokollkommunikation der einzelnen Systemelemente eingegangen wird.

2 Das Systemdesign

Das flexible Internetprotokoll ermöglicht in der Theorie unterschiedliche Lösungsansätze zur Realisierung einer Internet-Echtzeitübertragung. Es kann einerseits zwischen Unicast-Kommunikation (Punkt-zu-Punkt) und Multicast-Kommunikation, und andererseits zwischen gesichertem (TCP) und ungesichertem (UDP) Transport gewählt werden. Dabei ist aber nicht gewährleistet, dass alle möglichen Lösungsansätze auch im gesamten Internet unterstützt werden.

So scheitert der auf den ersten Blick vielversprechende und netzwerktechnisch elegante Multicast-Ansatz daran, dass IP-Multicasting-Dienste derzeit und wohl auch in absehbarer Zeit nicht über eine mobile Internetverbindung (GSM, GPRS, EDGE und UMTS) erreichbar ist. Gegen die alleinige Verwendung einer ungesicherten UDP-Übertragung sprechen vor allem die oft mangelnde Transparenz gängiger Sicherheitskonzepte für das Internet. Die teilweise mehrstufig angeordneten Firewalls und Proxyserver unterstützen meist nur das TCP-Protokoll, so dass für eine möglichst globale Verfügbarkeit (über alle Zugangsnetze) nur die Kombination Unicast/TCP in Frage kommt.

Nach der Frage der Kommunikation und des Transportes, stellt sich nun die Frage nach den Systemelementen. Klassische Internet-Kommunikation beruht meist auf dem Client/Server-Modell. Dabei steht ein Kommunikationspartner (Server) für Anfragen zur Verfügung. Dieser Server überträgt in unserem Fall GNSS-Daten. An diesen Server stellen Clients über das Internet Anfragen, welche von dem Server beantwortet werden.

Sicherheitstechnisch sind dabei die Server deutlich schwieriger zu schützen als die Clients, da die Server dadurch, dass sie auf Anfragen warten, über diese offene Schnittstelle (Port) angreifbar sind. Internet Server stehen meist außerhalb eines geschützten Firmennetzes. Clients hingegen, wie beispielsweise jeder Internet Explorer, stellen bei korrekter Implementierung keinerlei Sicherheitsrisiko dar, da von ihnen nur aktive Anfragen auf andere Server ausgeführt werden aber kein Zugriff von anderen auf die eigene Applikation ermöglicht wird. Auch lässt sich ein lokales Intranet, das nach außen nur durch TCP-Clients kommuniziert, sehr effektiv durch Firewalls oder Proxyserver schützen.

Die vorangegangenen Überlegungen führen zu dem Schluss, dass eine Systemarchitektur aus drei Systemelementen zweckmäßig ist. Dabei werden die Datenquellen und Datenempfänger als TCP-Clients konzipiert und können so hinter gängigen Firewalls betrieben werden. Beide Elemente kommunizieren mit dem TCP-Server, der als Splitter konzipiert ist und die angelieferten Datenströme für anfragende Empfänger vervielfältigt.

Der eigentlichen TCP-Übertragung wird nun HTTP als Applikationsprotokoll übergeordnet. Dadurch wird erreicht, dass die komplette Kommunikation von allen TCP Clients (Datenquellen und Datenempfänger) sowie eine mögliche Fernadministration über einen einzigen geöffneten TCP-Port (z.B. Port 80) stattfinden kann, was ein Sicherheitskonzept für den Server deutlich erleichtert. Das wird dadurch ermöglicht, das HTTP neben der eigentlichen Datenübertragung auch definierte Kommandos über die TCP-Verbindungen überträgt.

3 Networked Transport of RTCM via Internet Protocol (Ntrip)

Die Überlegungen des vorherigen Abschnitts führen zu der in Abbildung 1 dargestellten Ntrip-Systemarchitektur. Dabei kommunizieren die NtripServer und NtripClients implementiert als TCP-Clients mit dem NtripCaster (TCP-Server). Jeder GNSS-Datenquelle wird ein zugehöriger NtripServer zugeordnet, der die Daten beispielsweise über eine Serielle Schnittstelle oder über eine TCP-Verbindung erhält und sie an den NtripCaster weiterleitet. Dabei erfolgt die Generierung der GNSS-Daten im einfachsten Fall unmittelbar im GPS-Empfänger einer Referenzstation. Alternativ können die GNSS-Daten auch aus der Vernetzung von Beobachtungen einer Anzahl von Referenzstationen hergeleitet werden.

Alle am NtripCaster anliegenden Datenströme können nun von autorisierten Empfängern (NtripClients) abgerufen werden. Dabei stehen den Empfängern eine ständig aktualisierte Übersicht aller in Echtzeit abrufbaren Datenströme in Form einer „Source-Table“ zur Verfügung. Mit diesen Informationen kann von der Empfänger-Software, wie im nächsten Abschnitt noch näher beschrieben, der passende GNSS-Datenstrom über eine Source-ID angefragt werden.

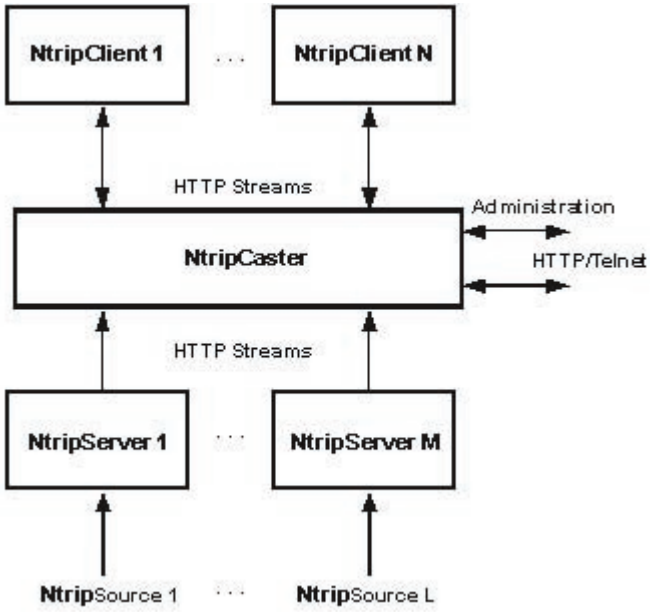

Abb. 1. *Ntrip System*

Das Systemkonzept ermöglicht dank HTTP auch die Möglichkeit der Fernwartung des NtripCasters über einen HTML-Browser (InterentExplorer) oder über eine Kommandozeilen-basierte Telnetverbindung. Dieses Eigenschaft ist vor allem in Hinblick auf ein professionelles Server-Hosting von sehr großer Bedeutung.

3.1 Ntrip Kommunikation

Die in Ntrip verwendete Protokollkommunikation basiert weitgehend auf dem aktuellen Internet-Radio ICE/SHOUTCAST-Protokoll, welchem wiederum eine leicht modifizierte Form des HTTP 1.1. Protokolls zugrunde liegt.

Dabei werden ausschließlich nicht-persistente Verbindungen verwendet. Das heißt, dass eine Verbindung nach eine(m,r) Request/Response beendet wird. Grundsätzlich besteht eine HTTP-Kommunikation aus dem Austausch von Objekten und Nachrichten über eine TCP-Verbindung. Dabei stellen HTTP-Clients (hier NtripClient und NtripServer) Anfragen an den HTTP-Server (hier NtripCaster), welcher darauf mit einer Aktion oder einer Fehlermeldung reagiert.

Ein NtripServer hat die Aufgabe, einen GNSS-Datenstrom kontinuierlich einem NtripCaster zuzuführen. Dazu verbindet sich der NtripServer mit dem NtripCaster (Host, Port) und sendet eine Servernachricht. Diese enthält neben einem Passwort zur Authentifizierung eine Source-ID und eine Angabe über die verwendete Version des NtripServer Programms. Der Server reagiert bei korrekten Angaben auf die Anfrage mit dem Kommando „ICY 200 OK“. Sollte die Anfrage scheitern, so antwortete der Server abhängig von dem aufgetretenen Problem mit „ERROR – Bad Password“ oder mit „ERROR – Mount Point Taken or Invalid“.

Ein NtripClient sendet nach erfolgreichem Verbindungsaufbau eine Empfängernachricht an den NtripCaster. Dabei wird dem NtripCaster mit Hilfe der Source-ID mitgeteilt, welchen der anliegenden GNSS-Datenströme er an den Client übertragen soll. Damit sich eine NtripClient einen Überblick über die angebotenen Datenströme auf einem Server machen kann, wird eine aktuelle Übersicht aller angebotenen Datenströme, genannt „Source-Table“, übertragen. Damit kann der NtripClient sekundengenau überprüfen, welche GNSS-Daten zugehörig zu welcher Position (z.B. Frankfurt; 50,12°; 8,68°) in welchem Format (z.B. RTCM 2.2;3(19),16(59),18(1),19(1)) für welches Navigationssystem (z.B. GPS+GLO) anliegen. Die Source-Table beinhaltet darüber hinaus noch viele weitere Informationen. Einen vollständigen Überblick bietet die Ntrip-Dokumentation in *Gebhard u.a. 2003.*

Die NtripCaster-Implementierung ermöglicht dank HTTP eine Fernwartung des Casters und somit den entfernten Betrieb mit professionellem Server-Hosting in einem Rechenzentrum. Über die Fernwartung können alle systemrelevanten Parameter (Auslastung, abliegende Datenströme, Verbindungsdauern etc.) im laufenden Betrieb überwacht, und gegebenenfalls angepasst werden. So können Datenströme an andere NtripCaster freigegeben werden oder auch bestimmte NtripClients oder NtripServer von einem Caster ausgeschlossen oder während des Betriebs von einem Caster entfernt werden.

3.2 Standardisierung

Standards sind im Zusammenhang mit Kommunikationstechnik von erheblicher Bedeutung. Proprietäre Lösungen können hier das Zusammenspiel verschiedener Systemkomponenten erheblich behindern und die Implementierung komplexer Techniken verzögern, sobald die Dienste verschiedener Hard- und Software-Firmen in Anspruch genommen werden sollen oder müssen. Für Ntrip wurde von Beginn an die Zusammenarbeit mit den Herstellern von GPS-Empfängern gesucht. Im Anschluß an Abstimmungsprozesse mit Firmen und erste Realisierungen einzelner Systemkomponenten wurde Kontakt zur „Radio Technical Commission for Maritime Services“ (RTCM) und insbesondere dessen für Differentielle Satellitenpositionierung zuständigen Special Committee 104 gesucht. Diese Institution, in der alle bedeutenden Hersteller von Positionierungs- und Navigationsgeräten vertreten sind, befaßte sich in der Vergangenheit überwiegend mit der Standardisierung der Inhalte von DGNSS-Datenströmen. Mitte des Jahres 2002 wurde ergänzend eine Arbeitsgruppe „Internet Protocol“ eingerichtet, die sich nun auch mit einer Standardisierung der Transportmechanismen bei Datenübertragungen via Internet beschäftigen soll. Die Arbeitsgruppe besteht im Wesentlichen aus Vertretern namhafter GNSS-Firmen.

Die Ntrip-Dokumentation *Gebhard u.a. 2003* wurde als Diskussionsgrundlage für einen neuen RTCM-Standard angenommen, der Einzelheiten der Übertragung von GNSS-Daten über Internet regeln soll. Mit der Herausgabe der ersten Version eines Standards ist, nach ausführlicher Abstimmung, nicht vor Mitte des Jahres 2004 zu rechnen.

4 Zusammenfassung

Es wurde in diesem Beitrag, basierend auf Internet-Radio-Technologie, mit Ntrip ein System zur Echtzeitübertragung von GNSS-Daten via Internet vorgestellt. Die Generierung von GNSS-Daten erfolgt dabei im einfachsten Fall unmittelbar im GPS-Empfänger einer Referenzstation, kann aber auch aus der Vernetzung von Beobachtungen einer Anzahl von Referenzstationen hergeleitet werden.

Der Vertriebsweg Internet ermöglicht es, weltweit GNSS-Daten über die unterschiedlichsten Zugangstechnologien anzubieten, ohne eigene Kommunikationsnetze aufbauen und betreiben zu müssen. Dienstnutzer profitieren zusätzlich von voraussichtlich fallenden Preisen bei den mobilen/stationären Internetzugängen. Dadurch können die GNSS-Daten kostengünstig für unterschiedlichste Anwendungen angeboten werden.

Das in diesem Beitrag vorgestellte Systemkonzept basiert auf drei Systemkomponenten: NtripServer, NtripClient und NtripCaster. Die verwendete Kommunikation gründet dabei weitgehend auf HTTP 1.1, welche um die Source-Funktionalitäten (Servernachricht, Source-Table) ergänzt wurde.

Durch die integrierten Authentifizierungsmaßnahmen der NtripServer wird gewährleistet, dass nur authentifizierte und somit vertrauenswürdige Datenströme an den NtripCaster angelegt werden können. Ferner gewährleisten die unterschiedlichen Authentifizierungsmaßnahmen der NtripClients (Basic und Digest) einen geschützten Zugriff auf die Datenströme. Dabei kann, abhängig von Benutzernamen/Paßwort, den Nutzern flexibel der Zugriff auf einzelne Datenquellen eingeräumt werden. Zusätzlich kann dabei konfiguriert werden, ob einem registrierter Nutzer auf verfügbare Datenströme zeitgleich nur einzelner oder z.B. 20 Zugriffe gleichzeitig gestattet sind. Darüber hinaus ermöglicht die Authentifizierung eine sekundengenaue Abrechnung der empfangenen Datenströme.

Beim Systemdesign für Ntrip wurden die Schwerpunkte auf eine globale Verfügbarkeit (Zugangsnetze), auf das Zusammenspiel mit Internet-Sicherheitsmechanismen (Firewall, Proxyserver), auf die Möglichkeit eines professionellen Server-Hosting (Trennung von Datenquelle und Zugangsserver, Fernadministration) und auf die Massennutzung (1500 simultane Nutzer von 300 Datenquellen) gelegt.

Das System ist seit Ende 2002 als neuer, experimentaler Internetdienst ständig verfügbar. Dabei stieg die Anzahl der verfügbaren Quellen sukzessive auf derzeit über 130 Datenströme unterschiedlicher Formate (RTCM 2.0, 2.1, 2.3, Rohdaten, RTCA). Es existieren inzwischen eine Reihe von Softwareimplementierungen für NtripClient und NtripServer unter verschiedenen Betriebssystemen (Windows, Windows-CE, Linux, PalmOS). Die NtripCaster Referenzimplementierung verwendet das Betriebssystem Linux.

5 Literatur/Quellen

Gebhard, H., G. Weber u.a. (2003):
Networked Transport of RTCM via IP (NTRIP) – Design – Protocols – Software.
RTCM Paper 167-203/SC104-315, Juni 2003
http://igs.ifag.de/index_ntrip.htm