Universität Salzburg
Fachbereich Computerwissenschaften
Seminar aus Informatik
Betreuung: Univ.-Prof. Dipl.-Ing. Dr.techn. Wolfgang Pree
Sommersemester 2011/2012

Seminararbeit

Sensor Web Enablement (SWE)/ Sensor Observation Service (SOS)

Simo Lukic, Simo.Lukic@stud.sbg.ac.at
Kurt Eschbacher, Kurt.Eschbacher@stud.sbg.ac.at

Inhaltsverzeichnis

1. Vision Sensor Web

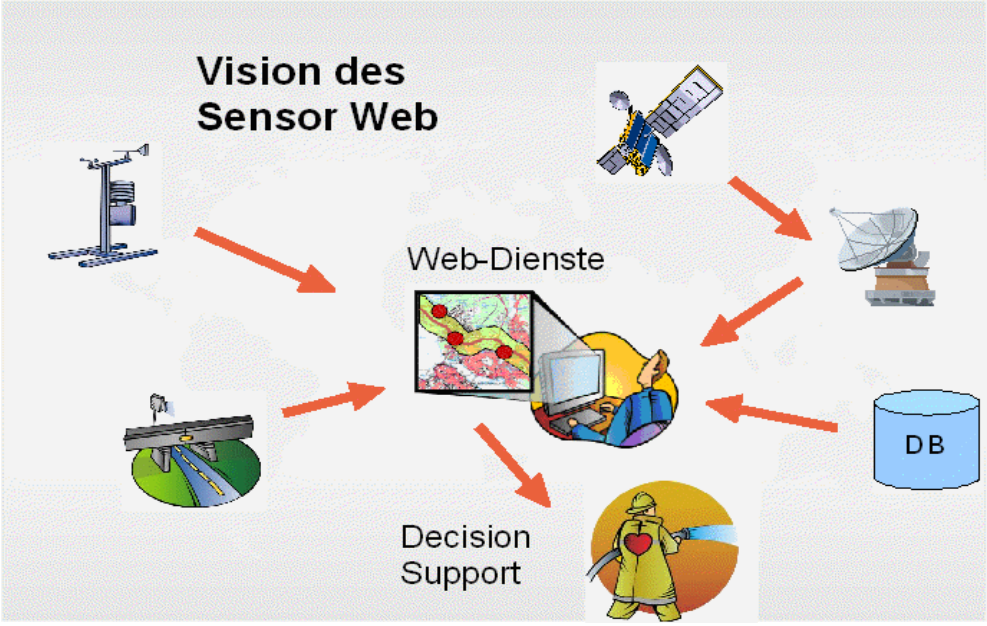

Abbildung 1: Vision Sensor Web

Geoinformationssysteme stellen einen systematischen Zusammenschluss, von allen zur Erfassung, Verarbeitung und Repräsentation von Geodaten notwendigen Hard- und Softwarekomponenten dar. Unter Geodaten kann man sich im weitesten Sinne digitale Informationen, die einen räumlichen Bezug haben und durch diesen näher charakterisiert werden, vorstellen. Diese digitalen Informationen können dabei sowohl direkt durch physikalische Messungen von Sensoren oder indirekt, durch eine Bearbeitung von Primärdaten repräsentiert sein.[1]
Um die lokal gemessenen und errechneten Geodaten effektiv verarbeiten zu können ist meist eine Bündelung dieser notwendig. Gewisse Geodaten liefern erst durch den Bezug mit anderen Geodaten eine konkrete Aussage zur gewünschten Fragestellung. Messwerte ergeben im Allgemeinen ohne einen konkreten Bezug zu Raum und Zeit keinen Sinn und haben keine Aussagekraft. Um etwa die genau Position und die Bewegungsrichtung eines Tornados ermitteln zu können ist es notwendig viele Messdaten von Wetterstationen und Sensoren eines betroffenen Gebietes gemeinsam zu verarbeiten. Einzelne Sensordaten liefern nur lokale Ereignisse und lassen für sich alleine betrachtet keine zuverlässigen Prognosen zu.
Aus diesem Beispiel lässt sich auch schon erahnen, dass für eine optimale Verarbeitung von Geodaten nicht nur zuverlässige Sensoren notwendig sind, sondern dass auch die Vernetzung dieser von essentieller Bedeutung ist. Gerade die stetig zunehmende Anzahl von Sensoren erfordert Vernetzungslösungen und Protokolle, die sowohl offen im Bezug auf die zu erfassenden Geodaten als auch sicher in Bezug auf Daten- und Zugriffsintegrität sind.[2]

1. Vision Sensor Web

1.1 Notwendigkeit eines Sensor Netzwerkes

An Anlehnung an das Internet wurde der Gedanke eines Sensor Webs aufgegriffen. Die Entwicklung und Entstehung des Sensor Web kann zum Teil mit der Entstehung des Internets verglichen werden.[3]
Die Technik entwickelt sich immer rasanter und die Miniaturisierung technischer Geräte schreitet weiter voran. Digitale Sensoren werden bereits kostengünstig und energieeffizient in Größendimensionen entwickelt, so dass sie ohne Probleme als „embedded measuring devices“ z.B. in Smartphones, Fahrzeugen oder Turnschuhen [8] eingebaut werden können. Diese digitalen Sensoren finden immer mehr Einzug in unser Privatleben und die Technik ermöglicht die Entwicklung unserer Gesellschaft in Richtung “pervasive monitoring”.[4]

Low-cost und low-power Messstationen, welche Umwelteinflüsse messen, werden immer erschwinglicher, genauer und zuverlässiger in ihrer Messung. Diese einzelnen Sensoren können vom Besitzer abhängig vom Kontext und Einsatzgebiet zu Sensornetzwerken zusammengefasst werden. Durch den Zugriff auf lokale Sensoren und die Einbindung bzw. Analyse von live Daten können wir in Echtzeit mit Hilfe von Geographischen Informationssystem (GIS) ein aktuelles Bild unserer Umwelt darstellen. Die Begriffe „live Daten“ und „Echtzeit“ dürfen in diesem Kontext nicht als besonders streng formulierte zeitliche Verzögerung betrachtet werden. So sind, abhängig vom Kontext und Einsatzgebiet der Sensoren, Messdaten mit einer zeitlichen Verzögerung zwischen einigen Sekunden bis einigen Minuten noch vollkommen akzeptabel. All diese heterogenen Sensornetzwerke generieren eine enorme Anzahl von sinnvollen Messdaten, mit deren Hilfe Rückschlüsse auf bestimmte Sachverhalte geschlossen werden können.

Das größte Problem dieser heterogenen Sensornetzwerke ist die fehlende Interoperabilität mit anderen Sensornetzwerken und Systemen.[10] Die meisten bestehenden Sensor-netzwerke sind monolithisch und in sich abgeschlossen - als “externer” Nutzer besteht keine Möglichkeit für einen Zugriff auf die Messaten. So kann es sein, dass zwe verschiedene Sensornetzwerke in naher Umgebung die gleichen Umweltparameter messen und die Betreiber weder einen Austausch der Messdaten vornehmen können noch überhaupt wissen, dass es ein anderes ähnliches Sensornetzwerk in der Nähe gibt.
Diese vorhandenen Missstände bezüglich der Abgeschlossenheit und fehlender Interoperabiltät gilt es zu beheben.

1.2 Sensor Web Enablement Initiative

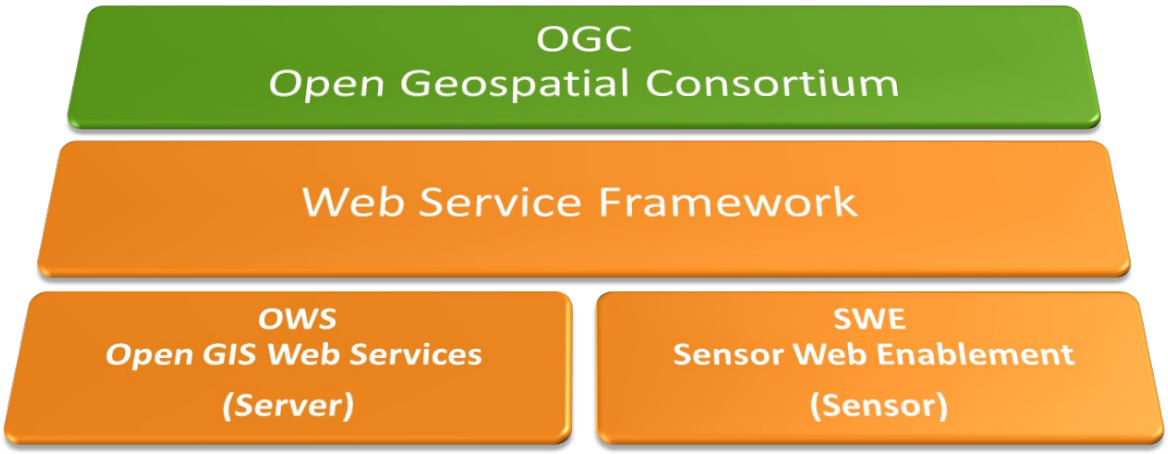

Abbildung 2: OGC und die Sensor Web Enablement Initiative

Um bestehende Probleme zu lösen und Barrieren zu überwinden, die sich aus der Abgeschlossenheit und Heterogenität bestehender Sensoren und Sensornetzwerke ergeben, wurde die Sensor Web Enablement (SWE) Initiative [11] durch das Open Geospatial Consortium (OGC) ins Leben gerufen. Das OGC ist eine internationale Organisation mit über 450 Mitgliedern, welche sich aus Universitäten, privaten Unternehmen und Regierungsorganisationen zusammensetzt. Das OGC befasst sich mit der Entwicklung offener Standards für die raumbezogene Informationsverarbeitung und hat es sich zum erklärten Ziel gemacht die Integration der heterogenen Sensornetzwerke in ein interoperables offenes Sensor Web voran zu treiben. In diesem Prozess der Standardisierung setzt das OGC auf schon bestehende und bewährte Standards, und entwickelt selber in Einbindung ihrer Mitglieder, welche sich aus unterschiedlichsten Interessengruppen zusammensetzen, selber offene Standards.[5][9]
Es wird energisch die Vision des Sensor Web verfolgt, in welches verschiedenste Sensornetzwerke, unabhängig von ihrer technischen Ausführung, eingebunden werden können. Das erklärte Ziel der SWE Initiative ist es, dass Sensoren über das Internet auffindbar, steuerbar und nach Messdaten abfragbar sind. Schlussendlich sollen die Daten auch genutzt werden können um für die Bevölkerung einen Mehrwert zu generieren. Durch die Standardisierung und Errungenschaften der SWE Initiative soll eine allgemeine Interoperabilität erreicht werden. Ein wesentliches Interesse für ein derartiges Sensornetzwerk mit live Daten besteht natürlich auch von bestimmten staatlichen Institutionen und Einsatzkräften. Bei einem etwaigen, durch natürliche oder künstliche Abläufe ausgelösten Katastrophenfall wäre es damit leichter möglich sich ein detaillierteres Bild der Situation vor Ort zu machen. Im Allgemeinen möchte man aus den Observationen und Wahrnehmungen der Sensoren schnell relavante Informationen extrahieren um dadurch das nötige Wissen und Verständnis zu schaffen um auf bestimmte Situationen richtig und entsprechend zu reagieren.[5]

1.3 SWE Framework

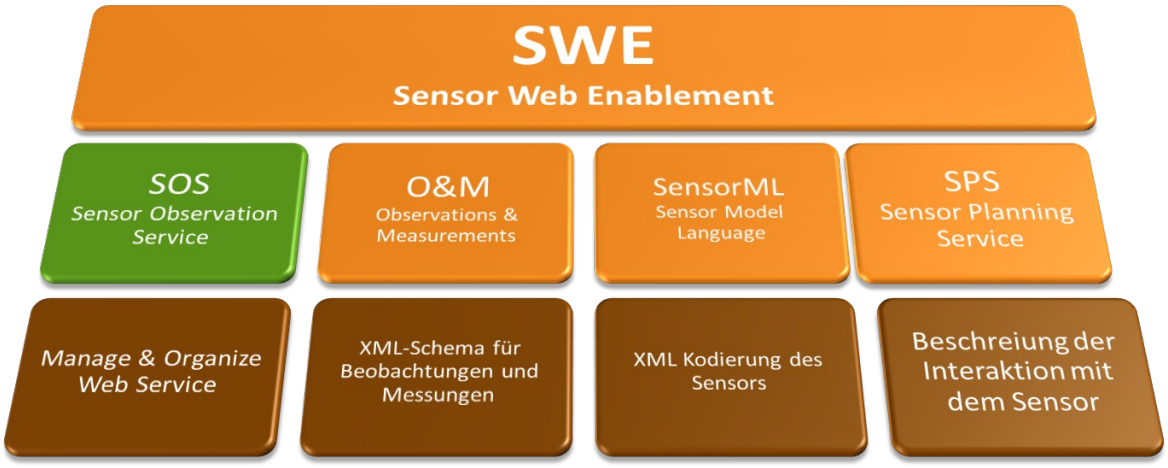

Abbildung 3: Ergebnisse der SWE Initiative

Das OGC hat im Sensor Web Enablement (SWE) Framework eine Reihe von technischen Standards und Begriffsdefinitionen ausgearbeitet um einen hohen Grad an Interoperabilität zwischen den einzelnen Sensornetzwerken zu erreichen.[9] Dabei wurden verschiedene Bereiche der Forschung, des Geschäftslebens oder auch der Unterhaltungsindustrie miteinbezogen und berücksichtigt um die unterschiedlichen Bedürfnisse bezüglich der Sensoren und des Kommunikationsverhaltens der jeweiligen Bereiche Rechnung zu tragen.
Das SWE Framework [12] setzt sich aus einer Reihe von definierten Services und Standards zusammen. All diese Standards behandeln jeweils einen Teil der Problematik, die es zu überwinden gilt um die Vision des Sensor Webs zu verwirklichen. In Kapitel 2 wird das Herzstück (Sensor Observation Service) der SWE Errungenschaften näher betrachtet.
Durch diese, auf breiter Basis erarbeiteten Standardisierung, ist die Grundlage für die schnelle und kosteneffiziente Entwicklung von disziplinübergreifenden und interoperablen Sensoren und Sensornetzwerken gegeben.[7]
Die Sensortechnologie und die Nachfrage bzw. der Wunsch nach Vernetzung mit “real-time” oder “near real-time” abfragbaren Daten und Visualisierung der gemessenen Phänomene in Applikationen ist ein weiterer, an Bedeutung gewinnender, Aspekt in Bezug auf SWE. Gerade in Disziplinen mit einer sehr hohen Anzahl unterschiedlichster Sensoren, Geodaten und dem Fehlen detaillierter Kenntnisse über die einzelnen zugrundeliegenden physikalischen Vorgänge bei der Auswertung, ist eine entsprechende Visualisierung der Daten essentiell - weshalb auch dieser Aspekt näher betrachtet wird. Als mögliche Einsatzszenarien können Bereiche der Anlagensicherheit, die Kontrolle industrieller Prozessabläufe, urbanes Monitoring oder der Risikoabschätzung beim Notfalleinsatz staatlicher Einsatzkräfte angeführt werden.

2. Sensor Observation Service

Der Sensor Observation Service (SOS) [13] ist mit seinem Standard eine der bedeutendsten Errungenschaften der SWE Initiative. Der SOS stellt ein standardisiertes Interface für WebServices zur Verfügung um Messdaten und Metadata von heterogenen Sensornetzwerken und den einzelnen Sensoren abzufragen. Zur Anwendung soll der SOS Standard in jenen Situationen kommen, in welchen Sensordaten verwaltet und zwischen verschiedenen Teilnehmern interoperabel austauschbar sein sollen. Der SOS ist primär ausgelegt worden um einen einfachen, schnellen Zugriff und Austausch von Observationen und Messdaten zu erlauben. Mit Hilfe anderer Services der SWE Initiative können heterogene Sensornetzwerke als SOS veröffentlicht werden (in Katalogen) und dadurch von Nutzern angefragt werden.

Mit dem Sensor Observation Service sind weitere Services und Standards eng verknüpft:

- Sensor Model Language (**SensorML**): Dient der konkreten Beschreibung der Sensoren und deren Prozesse in vorgegebener XML Dokumentstruktur.
- Sensor Planning Service (**SPS**): Mit diesem Service werden jene Interfaces definiert, die es erlauben Sensoren zu steuern bzw. nach Messdaten abzufragen.
- Observations & Measurements (**O&M**): Dieser Standard bietet ein streng typisiertes und abstraktes Modell für Observationen und Messungen. Durch ein XML Schema kann die Struktur des Dokumentes definiert werden, welches die Messdaten enthält.

2.1 Operationen des SOS

Die Kernfunktionalität (mandatory) des SOS setzt sich aus 3 Operationen zusammen:

- **GetCapabilities**: Liefert Metadaten und ausführliche Beschreibungen der Funktionalität und zur Verfügung gestellten Operationen durch den SOS Server. Ein XML Dokument, welches detaillierte Informationen zu den Sensoren (Messstationen), abfragbaren Messzeiträumen und verfügbaren Observed Property (Phänomene) enthält.

- **DescribeSensor**: Liefert Metadaten und ausführliche Beschreibungen einer konkret angefragten Messstation (Observation Offering).

- **GetObservation**: Bietet Zugriff auf Observationen und Messwerte durch SOS. Erlaubt räumliche, kontextspezifische und zeitliche Filterung. Die Antwort des Services erfolgt in einem Observations & Measurements vordefiniertem Format.

Neben der Kernfunktionalität gibt es eine Reihe weiterer Operationen (optional), welche den SOS abrunden und weitere Robustheit bzw. Funktionalitäten hinzufügen.

- **InsertSensor**: Der Betreiber des Sensornetzwerkes bzw. SOS kann während des aktiven Betriebs einen neuen Sensor zum System hinzufügen.
- **DeleteSensor**: Ermöglicht die kaskadenartige Löschung eines Sensors und der verbundenen Observationen.
- **InsertObservation**: Ermöglicht das Eintragen von Observationen mit Messwerten eines im System vorhandenen Sensors (wird korrekt in Datenbanken abgespeichert).
- **GetResult**: Ermöglicht das Abfragen von Messwerten ohne jedoch den Overhead des XML Dokuments mit Metadaten zu erhalten. Geeignet für Situationen, in denen die Antwortzeit und Speicherverbrauch eine kritische Rolle spielen.
- **GetFeatureOfInterest**: Erlaubt direkten Zugriff auf Observationen und Messwerte realer Objekte (Feature Of Interest/Messstation), falls welche vorhanden sind.
- **GetObservationByID**: Erlaubt Zugriff auf konkrete Observationen mit Messwerten indem an den SOS nur die ID der gewünschten Observation übergeben wird.

Die Implementierung dieser Operationen verleiht dem SOS einen interaktiven Charakter und erlaubt es sowohl dem Betreiber des Sensornetzwerkes auf standardisierte Art und Weise Daten in das System einzuspielen als auch dem Nutzer diese Daten ohne Behinderung des Betriebes abzufragen. Die Abgeschlossenheit von bestehenden monolithischen Sensornetzwerken kann somit durch die Implementierung eines SOS aufgebrochen werden und eine domänenübergreifende Nutzung der vorhandenen Messdaten kann erreicht werden. Der Standard zum SOS stellt ein strukturiertes und methodisches Vorgehen zur Implementierung der notwendigen Operationen [13] um Interoperabilität zwischen heterogenen Sensornetzwerken zu ermöglichen.
Da die Implementierung aufgrund der Komplexität und Mächtigkeit des vollständigen Standards relativ viel Zeit für die Betreiber von Sensornetzwerken in Anspruch nehmen würde, sind die meisten Operationen optional zu implementieren. Das Weglassen bzw. gezieltes Optimieren dieser optionalen Operationen kann einen SOS schlanker und performanter machen. Vor allem beim Zugriff durch mobile Geräte [14] auf angebotene Services kann dies eine entscheidende Rolle bei der Akzeptanz der Nutzer spielen. Die Bereitstellung der Daten und der Zugriff sollen plattformunabhängig und barrierefrei gestaltet werden. Da jeder SOS die verpflichtende Operation GetCapabilities implementieren muss, kann der Nutzer alle benötigten Metainformationen zu dem Service abfragen und damit klar einsehen welche Operationen in welcher Form vom SOS angeboten werden.

2.2 Kernelemente des Standards

Um jedoch die Operationen fehlerfrei in einen SOS zu implementieren, bedarf es einer weiteren Definition bestimmter allgemeiner Begriffe.

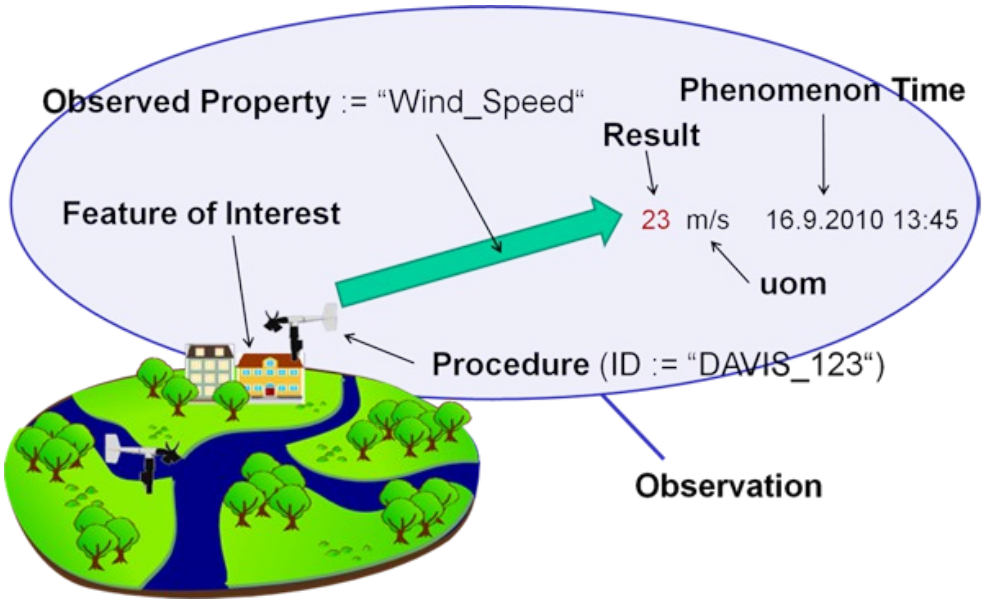

Abbildung 4: Begriffe im SOS Standard

- **Sensor**: Eine technische Einheit, welche konkrete Messwerte, physikalische und chemische Eigenschaften, zu einem bestimmten untersuchten Phänomen (Observed Property) digital liefern kann. Meistens werden mehrere Sensoren zu einer Messstation zusammengefasst.
- **Feature of Interest** (FOI): Repräsentiert ein Objekt in der realen Welt.
- **Measurement**: Der konkret ermittelte Messwert (physikalische Einheit).
- **Procedure**: Eine Procedure kann ein Sensor, Algorithmus oder Simulation zur Erzeugung von Messwerten bei einer Observation sein.
- **Observation**: Ein Vorgang, welcher einen Messwert bei einem Feature of Interest zu einer konkret beobachteten Observed Property/Phenomän liefert. Besonders wichtig ist hier die Zeit, zu welcher die Observation durchgeführt wurde.
- **Observed Property/Phenomena**: Phänomene wie z.B. Lufttemperatur, Niederschlag, die durch eine Procedure bei einem Feature of Interest gemessen werden können.
- **Observation Offering**: Eine logische Gruppierung von Observationen, durchgeführt durch eine Procedure, welche alle benötigten Metadaten bezüglich der Observed Properties und der Observationen anbietet.

Das OGC hat großen Wert auf die detaillierte Definition und formale Beschreibung der Operationen und vor allem der XML Elemente, welche die relevanten Informationen beschreiben, gelegt. Es wurde enormer Aufwand betrieben um ein sehr robustes Framework zu entwickeln, damit es allgemein für das Sensor Web anwendbar ist und sich nicht auf spezifische Einsatzgebiete beschränken muss. Jedes XML Element ist genau beschrieben und besitzt ein eigenes Validierungsschema. Um Eindeutigkeit zu gewährleisten benutzt der SOS Standard 12 Namespaces. Der SOS Standard beinhaltet eine große Anzahl komplexer Schemata und über 700 komplexe Typen. Ziel war es nicht unbedingt neue Schemata oder komplexe Typen einzuführen, sondern auf bestehende Standards und Kodierungen aus Geography Markup Language (GML), SensorML oder O&M zurück zu greifen. Dadurch soll die Interoperabilität zwischen den verschiedenen Sensoren, Netzwerken und Themengebieten garantiert werden. Ziel ist es einen Grad der Standardisierung zu erreichen um vollautomatisierte Workflows ab der Messung von z.B. bestimmter Umweltparameter bis hin zum Anbieten der aufgearbeiteten Daten in visualisierter Form.

Eine wichtige Rolle spielen Filter. Diese erlauben es bei der Anfrage an einen SOS mit einem GetObservation, aus den Unmengen von Observationen und Messdaten, die aufgezeichnet worden sind, nur jene Messdaten zu erhalten, auf welche der Filter zutrifft. Bei den Filtern setzt der SOS auf schon definierte Standards des OGC und Kodierungen aus O&M. Um ein bildhaftes Verständnis zur Nutzung des SOS Konzeptes zu erhalten, werden nachfolgend kurz zwei Usecases beschreiben.

2.3 Bereitstellung SOS Messdaten

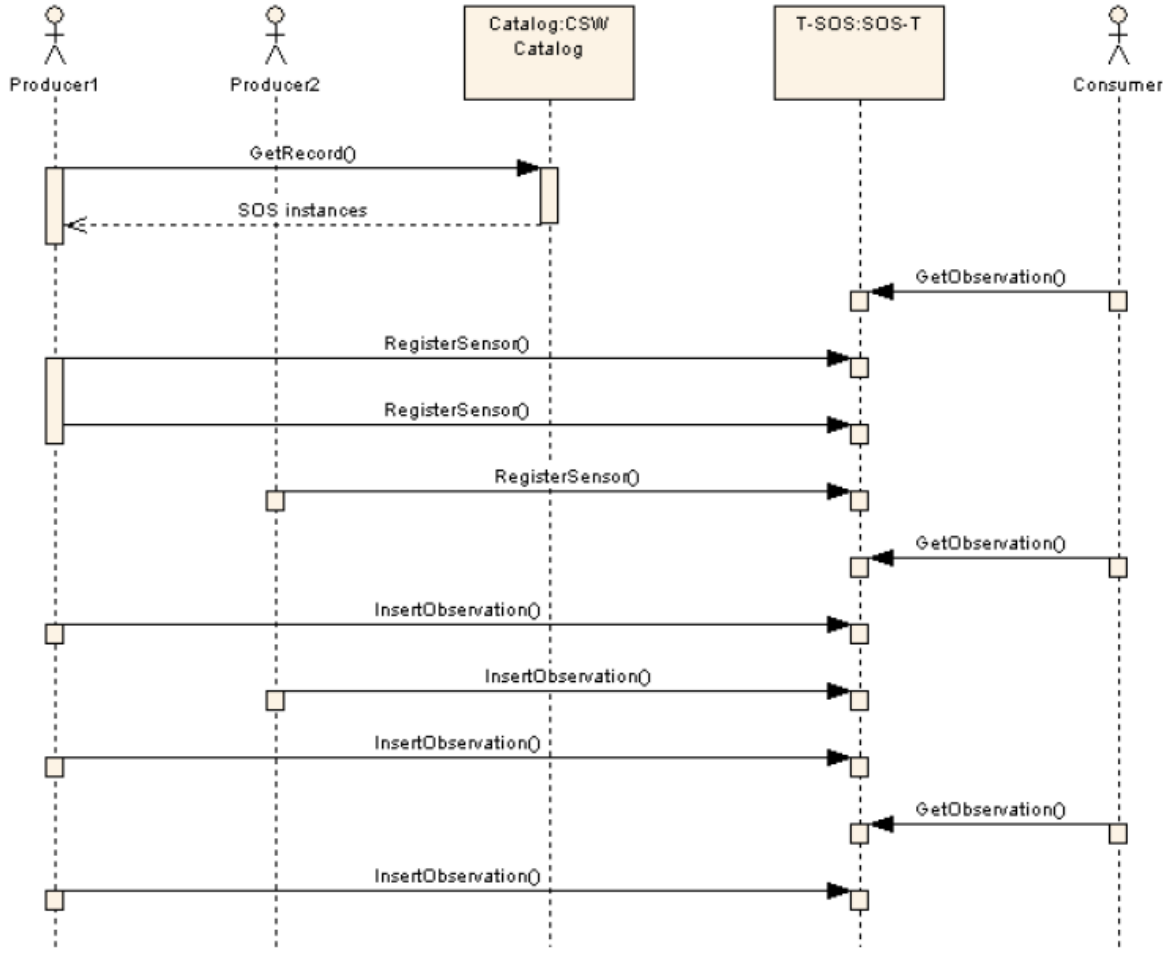

Abbildung 5: Bereitstellung SOS Messdaten

Dieser Usecase beschreibt die Nutzung eines SOS aus der Perspektive des Sensornetzbetreibers. Der SOS stellt die Schnittstelle zwischen den Messdaten (Producer), die sich in den meistens Fällen in einer DB befinden, und dem Nutzer (Consumer) dar. Der Producer ist im Grunde ein heterogenes Sensornetzwerk, welches zu bestimmten Phänomenen Messdaten liefern kann. In unserem Usecase möchte der Producer seine Messdaten und das Sensornetzwerk in Form eines SOS anderen Nutzern zur Verfügung stellen. Das Veröffentlichen nach Außen, als ein SOS, wird über einen Catalogservice (Index für veröffentlichte SOS) erledigt. In diesem Catalogservice, können Consumer dann nach entsprechenden SOS suchen. Nach dem Veröffentlichen im Catalogservice kann der Producer neue Sensoren zum Netzwerk mit der Operation RegisterSensor hinzufügen oder mit DeleteSensor entfernen. Der Betrieb des SOS muss nicht unterbrochen werden. Neue Messdaten, welche durch Procedures generiert werden, können ohne Probleme mit der Operation InsertObservation in einer standardisierten Art und Weise in das System eingespielt werden.

2.4 Abfragen der SOS Messdaten

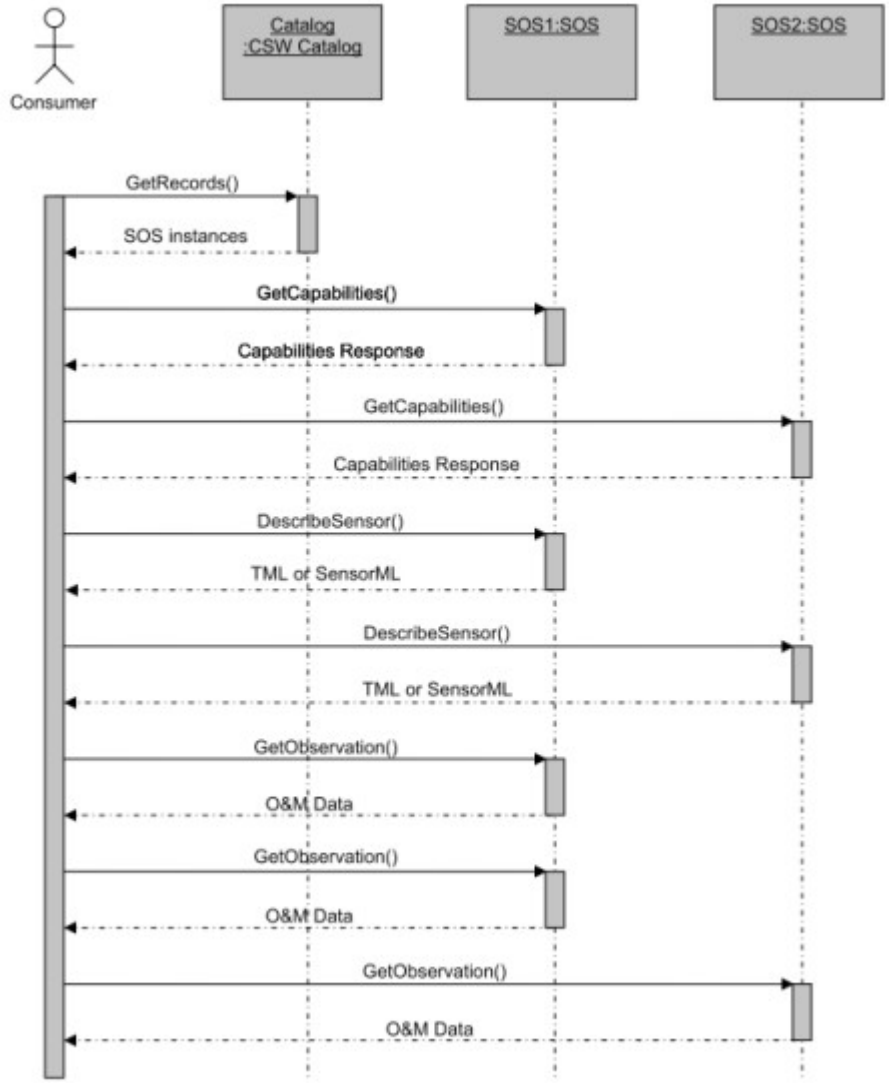

Abbildung 6: Abfragen der SOS Messdaten

Damit ein Nutzer (Consumer) einen SOS nach Messdaten abfragen kann, sind erst bestimmte Metadaten erforderlich. Um einen SOS zu finden, kann der Nutzer Catalogservices (Index) nach einem gewünschten SOS durchsuchen. Sobald der gewünschte SOS gefunden wurde, können die dazugehörigen Metainformationen (z.B. URL des Services, Themengebiet, Lizenzen) vom Catalogservice abgerufen werden. Im nächsten Schritt schickt der Nutzer eine GetCapabilities Anfrage an den SOS. Die GetCapabilities Antwort liefert dem Nutzer alle benötigten Informationen über die implementierten Operationen des Services und welche weiteren Abfragen möglich sind. Mit der Operation DescribeSensor kann der Nutzer zusätzliche weitere Metainformationen eines einzelnen Sensors abfragen oder mit der Operation GetObservation eine Anfrage bezüglich der gewünschten Messdaten abschicken.

2.5 SOS Operation GetObservation

Der SOS nutzt zur Kommunikation zwischen den einzelnen Teilnehmern stark typisierte XML Dokumente. Im Standard sind alle erlaubten XML Tags und ihre Bedeutung genau beschrieben. Diese strengen Regelungen sollen die Interoperabilität gewährleisten. Nachfolgend sehen wir eine recht einfache GetObservation Anfrage (Filter) eines Clients an einen SOS Server.

```
<?xml version='1.0' encoding='UTF-8'?>
<sos:GetObservation xmlns:xsi='http://www.w3.org/2001/XMLSchema-
instance' xmlns:gml = 'http://www.opengis.net/gml'
 xmlns:ogc = 'http://www.opengis.net/ogc'
 xmlns:sos = 'http://www.opengis.net/sos/1.0'
 xmlns:om = 'http://www.opengis.net/om/1.0'
 xsi:schemaLocation='http://www.opengis.net/sos/1.0
http://schemas.opengis.net/sos/1.0.0/sosAll.xsd'
 service='SOS' version='1.0.0'>

 <sos:offering>org:aut:Salzburg</sos:offering>
 <sos:eventTime>
     <ogc:TM_After>
         <ogc:PropertyName>om:sampleTime</ogc:PropertyName>
         <gml:TimeInstant>
             <gml:timePosition>2012-07-1T12:45:00</gml:timePosition>
         </gml:TimeInstant>
     </ogc:TM_After>
 </sos:eventTime>
 <sos:observedProperty>urn:ogc:def:AirTemperature</sos:observedProperty>
 <sos:observedProperty>urn:ogc:def:RelHumidity</sos:observedProperty>
 <sos:responseFormat>text/xml;subtype="om/1.0.0"</sos:responseFormat>
</sos:GetObservation>
```

Listing 1: GetObservation

Ein Client kann ein solche individuelle Anfrage als Filter nur nach der Auswertung des GetCapabilities XML Dokumentes formulieren. Die Operation GetCapabilities liefert alle notwendigen Metainformationen zu einer SOS Instanz.

Deutung des GetObservation XML Dokumentes:

- In `<sos:offering>` wird das Observation Offering (Messstation), zu welcher wir Messwerte erhalten möchten, angegeben. Aufgrund der Informationen in GetCapabilities wissen wir, dass dieser SOS eine Observation Offering mit dem Namen “org:aut:Salzburg” hat.
- In `<sos:eventTime>` wird der zeitliche Filter festgelegt. In diesem Beispiel sollen alle Messwerte, welche seit dem 1. Juli 2012 12:45:00 gemessen und in die DB eingetragen sind, abgerufen werden.

- In `<sos:observedProperty>` wird festgelegt zu welchen Umweltparametern (Lufttemperatur und Luftfeuchtigkeit) die Messwerte geliefert werden soll.
- In `<sos:responseFormat>` wird festgelegt, dass die Serverantwort in einem Observations & Measurements XML Dokument stattfinden soll.

Dies ist nur eine einfache GetObservation Anfrage, aber es wird deutlich, wie strukturiert die Daten angefragt werden können. Nachdem die Anfrage zu einem konkret ausgewählten SOS geschickt wurde, ist es die Aufgabe des Services die Anfrage auf ihre Korrektheit zu überprüfen. Bei auftretenden Problemen wird eine Fehlermeldung an den Client zurückgeschickt. Bei erfolgreicher Anfrage, erstellt der Service eine GetObservationResponse und schickt diese an den Client.

Deutung der GetObservationResponse (dies ist nur ein Ausschnitt der XML Antwort):

```
<om:result>
<swe:DataArray>
 <swe:elementCount>
   <swe:Count>
     <swe:value>960</swe:value>
   </swe:Count>
 </swe:elementCount>
 <swe:elementType name="org:aut:Salzburg_Type">
   <swe:DataRecord>
     <swe:field name="feature">
       <swe:Text definition="urn:ogc:data:feature"/>
     </swe:field>
     <swe:field name="AirTemperature">
       <swe:Quantity definition="urn:ogc:def:property:OGC:AirTemperature">
         <swe:uom code="Cel"/>
       </swe:Quantity>
     </swe:field>
     <swe:field name="RelativeHumidity">
       <swe:Quantity definition="urn:ogc:def:property:OGC:RelativeHumidity">
         <swe:uom code="%"/>
       </swe:Quantity>
     </swe:field>
     <swe:field name="Time">
       <swe:Time definition="urn:org:def:property:OGC:Time:iso8601"/>
     </swe:field>
   </swe:DataRecord>
 </swe:elementType>
 <swe:encoding>
   <swe:TextBlock blockSeparator="@@" decimalSeparator="." tokenSeparator=","/>
 </swe:encoding>
 <swe:values>17,17.9,80.5,2012-07-01T12:50:00+00@@17,18.5,79.5,2012-07-
01T13:05:00+00@@....
 </swe:values>
</swe:DataArray>
</om:result>
```

Listing 2: GetObservationResponse

- In `<swe:values>` wird die Anzahl der zurückgelieferten Observationen angegeben. In diesem Beispiel werden 960 Observationen zum Client zurück geschickt.
- In `<swe:DataRecord>` und `<swe:field>` wird die Reihenfolge der Elemente/Observed Prooperty angegeben, in welcher sich diese in einem Datensatz/Observation in `<swe:values>` befinden. Dies ist notwendig, damit der Client die Messwerte zu den zurückgelieferten Attributen zuordnen kann.
- In `<swe:values>` sind die Observation mit den einzelnen Messdaten enthalten. Jeder Messwert/Attribut ist durch einen Beistrich getrennt. Jede Observation wird durch "@@" getrennt.

Somit ergibt sich aus dem String „`17,17.9,80.5,2012-07-01T12:50:00+00@@`" die folgende Deutung:

- `Feature of Interest :` `17 (org:aut:Salzburg)`
- `AirTemperature:` `17.9 Celsius Grad`
- `RelativeHumidity (Luftfeuchtigkeit):` `80.5 %`
- `Time (Zeitpunkt der Messung):` `1. July 2012 12:50:00`

Die allgemeine Dokumentstruktur für jene XML Dokumente, die zwischen dem Client und SOS verschickt werden, ist vorgegeben. Die auftretende Reihenfolge von XML Tags ist ist in GetObservation klar definiert und erleichtert somit, sollten sich Probleme ergeben, die Fehlerquellensuche. Im Standard sind auch zu jeder Operation Exception Codes definiert, welche dem Nutzer spezifisch mitteilen, warum und wo ein Fehler aufgetreten ist.

Neben der Implementierung von Operationen serverseitig im SOS, muss auch jede Client Applikation Operationen (individuelle Softwarelösung) implementieren, um aus den XML Dokumentantworten des SOS, die angefragten Daten sinnvoll zu extrahieren (parsen) und in gewünschter Form für weitere Verarbeitung zur Verfügung zu stellen. Diese Lösungen müssen individuell an die Applikation, welche die Daten weiterverarbeiten wird, angepasst werden. Das ist auch eine der Herausforderungen für die weitere Verbreitung des Sensor Web im Bereich der Client Applikationen. Es müssen Modelle und Implementierungen entwickelt werden, welche die zugrunde liegende Komplexität abstrahieren. Durch einfache Anpassungen, ohne Expertenwissen, sollen diese als Schnittstellen zwischen der XML Dokumentantwort und der eigenen Applikation dienen.

3. Management von Zugriffsrechten auf Geodaten

Die letzte Dekade gehörte dem Internet und der allgemeinen Vernetzung diverser technischer Geräte. Unabhängig davon ob im Büro, in den eigenen vier Wänden, in unserer Freizeit oder im Urlaub, die meisten Menschen haben die Möglichkeit ihre Konnektivität und Zugriff auf ihre persönlichen elektronischen Daten aufrecht zu erhalten. Die nächste Dekade kann dem “pervasive monitoring” gehören. Sensoren haben eine solche Miniaturisierung und geringe Herstellungskosten erreicht, dass sie ohne Probleme als “embedded measuring devices” in Sportschuhe, Bekleidung oder Smartphones eingebaut werden können. Auch die Medizin bedient sich vermehrt von “remote monitoring” um in-situ (vor Ort) Messungen vorzunehmen, diese aber dann an eine zentrale Stelle zu übermitteln und dort schnellere Entscheidungen zu treffen.

3.1 Messdaten sind wertvoll

Das Sensor Web kann sich aus einer vielzahl verschiedenster Sensornetzwerke zusammensetzen. Die ausgearbeiteten Standards von OGC im Zuge der Sensor Web Enablement Initiative erlauben es Sensornetzwerke von öffentlichen Institutionen, von Forschungseinrichtungen, von Firmen oder privat betriebene Sensoren an ein Sensor Web anzubinden. All diese Sensornetzwerke sammeln Messdaten, abhängig von ihren Einsatzgebieten, zu konkret messbaren Parametern - Umweltparameter (z.B. Lufttemperatur, Radioaktivität), Biometrieparameter (z.B. menschlicher Puls) oder Ortsbestimmung (Tracking von Wildtieren, die mit einem Sensor versehen wurden).
Messdaten sind nicht nur besonders wertvolle Daten, sondern auch schützenswerte Daten. Deswegen müssen bei verteilten und heterogenen low-power Sensornetzwerken einfache Sicherheitsmechanismen und Rechteverwaltungen eine entscheidende Rolle spielen.[6]

Die herausfordernde Frage ist es nun wie Sicherheitsmechanismen und Zugriffsregelung auf bestimmte Sensoren und die vorgenommenen Observationen bei verteilten und heterogenen low-power Sensornetzwerken umgesetzt werden können ohne eine größere Belastung, bei den Betreibern und Besitzern dieser Sensornetzwerke, zu verursachen.
Die Messdaten werden über definierte WebService Schnittstellen für die Nutzer zur Verfügung gestellt. Die einfachen Messdaten, welche als Rohdaten betrachtet werden können, müssen erst erhoben, in den meisten Fällen dann aufgearbeitet und in ein standardisiertes Format gebracht werden. Dies verursacht natürlich Aufwand und Kosten, ist aber notwendig, damit die Daten interoperabel und für weitere Nutzung über die Schnittstelle an den Nutzer übergeben werden können. Mit der Bereitstellung von Daten übernimmt der Datenanbieter auch einen bestimmten Grad an Haftung bezüglich der Korrektheit und Vollständigkeit der Daten.

Der unkontrollierte Zugriff auf die Messdaten und Observationen würde eine definitive Mehrbelastung für die Infrastruktur des Sensornetzes bedeuten und würde im schlimmsten Falle die Performance des Systems soweit minimieren, dass dem eigentlichen Besitzer dadurch ein optimales Arbeiten und Zugreifen auf die Messdaten nicht mehr möglich wäre.

3.2 Motivation und exemplarisches Beispiel für Zugriffsregelung

Zum besseren Verständnis kann folgendes exemplarisches Beispiel angeführt werden. Ein Geodatenanbieter betreibt einen Server mit einem SOS WebService, welcher das gesamte Straßennetz in Österreich darstellen kann. Über eine Schnittstelle kann der WebService von einer Applikation (Client) aufgerufen werden und das Straßennetz kann auf einer Karte in der Applikation visualisiert werden. Da die Bereitstellung der Daten mit Kosten verbunden ist, möchte der Geodatenanbieter Lizenzen verkaufen, welche genau festlegen, welcher Kunde auf welchen Teil der Karte zugreifen darf. Der Besitzer einer Lizenz, die den Zugriff auf die Daten für das Salzburgland erlaubt, soll auch nur diese Daten abrufen können. Ein Zugriff auf das Kartenmaterial für z.B. Tirol würde verwehrt werden. Durch Lizenzen und Policen kann der Anbieter genau steuern wie die verfügbaren Daten und Services sinnvoll von den Kunden genutzt werden können.

3.3 Kontrolle über die eigenen Messdaten behalten

Um die Bedenken der Sensornetzbetreiber bzw. Messdatenanbieter zu zerstreuen und sie dazu zu bewegen ihr Sensornetz an das Sensor Web anzuschließen (im Catalogueservice der breiten Öffentlichkeit bekanntgeben) muss dem Betreiber ein Mechanismus angeboten werden, welcher die volle Kontrolle über fremde Zugriffe auf das eigene System garantiert. Der Betreiber muss in der Lage sein eindeutig festzulegen welcher Nutzer oder Nutzergruppe welche Messdaten zu welchen Messzeitpunkten von welchen Sensoren abfragen darf. Kein unbefugter Zugriff darf auf die Daten und somit eine Beanspruchung der Hardware/Infrastruktur erfolgen.

Der Schutz vor unbefugten Zugriffen auf Geodaten wird auch seitens der Europäischen Union forciert und auch verlangt. Von öffentlichen Einrichtungen, welche planen Geodaten der breiten Öffentlichkeit zur Verfügung zu stellen, wird verlangt Mechanismen einzuführen um Zugriffe kontrollieren und protokollieren zu können.
Bei Geodaten lassen sich thematisch Zugriffsbeschränkungen am einfachsten durch Bounding Boxes oder Kartenebenen/Layer realisieren.

- Eine Bounding Box beschreibt einen rechteckigen Ausschnitt einer Karte. Durch die Angabe von 2 Koordinatenpunkten, welche durch die Diagonale verbunden sind, wird ein rechteckiger Bereich auf der Karte aufgespannt. Eine komplexere Form, wenn mehrere Koordinatenpunkte verfügbar sind, wäre die Definierung eines Polygons, welches eine feinere Fläche auf der Karte aufspannen kann. Die Berechnung der Abfrageergebnisse wird komplizierter je feiner eine Bounding Box definiert wird.
- Eine digitale Karte setzt sich meistens aus mehreren Kartenebenen/Layern zusammen und dabei beinhaltet jede Ebene einen bestimmten Satz von Informationen. Eine Ebene kann z.b. nur die geografischen Grenzen einer Region beinhalten. Eine andere Ebene würde das Straßennetz abbilden. Und eine weitere Ebene die Gewässer oder Gebirge. Dem Nutzer steht es frei Kartenebenen ein- oder auszublenden.

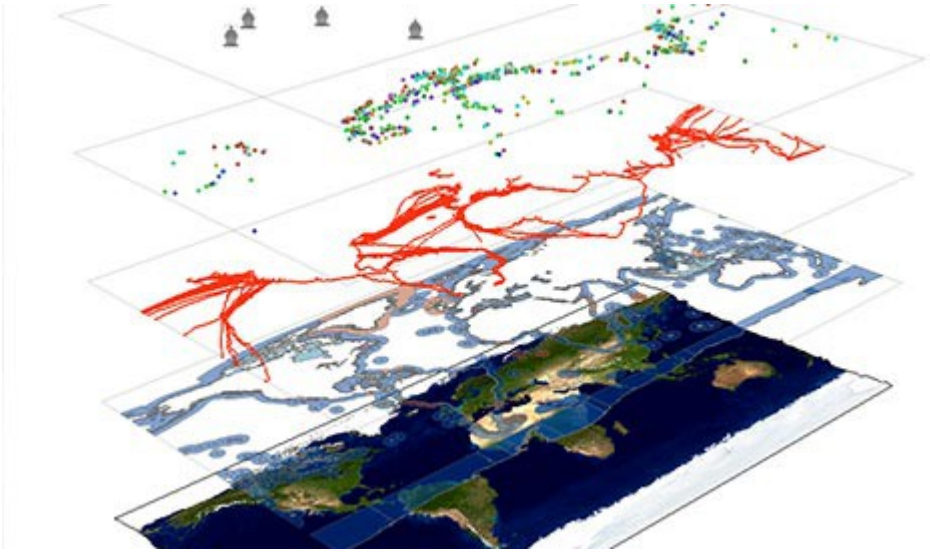

Abbildung 7: Verschiedene Kartenlayer

Das OGC hat im Zuge der SWE Initiative und Standardisierungsverfahren selber keinen Standard aufgestellt, der klar regelt, wie der Zugriffsschutz umzusetzen ist. Im sicherheitskritischen und kommerziellen Bereich gibt es schon proprietäre Lösungen, die jedoch umfassende Einarbeitungs- und Verwaltungszeit erfordern und auch mit hohen Lizenzkosten zu Buche schlagen. Diese Lösungen sind auch nicht vordergründig im Sinne der Vision des Sensor Web entwickelt worden. Zu nennen wären hier die Softwarelösung ArcGIS, mit einer vielzahl von Applikationen und Modulen, von ESRI und “Security & Geo-Rights Management” von “52°North”.[6] Die Konzepte und Lösungen mit SAML und XACML bieten auch sehr gute Sicherheitsmechanismen, sind jedoch aus Performancegründen für verteilte low-power heterogene Sensornetze nicht besonders geeignet.

3.4 Lightweight Tripple-A Ansatz

Ein neuer “lightweight” Ansatz zur Regelung der Zugriffe und zum Schutz (Wahrung der vollen Kontrolle) von Geoinformationsdiensten in verteilten und heterogenen Sensornetzwerken, ohne Änderung der bestehenden Infrastruktur und Services, wird in [6] beschrieben. Bei dem Tripple-A Konzept werden keine proprietären Standards oder Technologien eingesetzt, die Umsetzung stützt sich auf vorhandene OGC Standards und eine simple Client-Server Kommunikation mit HTTP, GET, POST oder SOAP kommt zur Anwendung. Um den Overhead und die allgemeine Verwaltung zu reduzieren werden die 3 Aspekte des tripple-A (Authentifizierung, Autorisierung und Abrechnung) Ansatzes mit bestehenden und bewährten Mitteln umgesetzt. Unter einem tripple-A System können wir ein System verstehen, welches die Steuerung von Anfragen, seitens des Nutzers, die Überprüfung ob Zugriffe auf bestimmte Daten dem konkreten Nutzer gewährt oder verwehrt werden sollen und die Abrechnung der entstandenen Kosten, regelt.

- Authentifizierung wird mit OpenId gelöst. OpenId ist ein dezentrales Authentifizierungssystem (Nachweis der Identität), welches es dem Nutzer ermöglicht sich bei einem OpenId-Provider zu registrieren. Bei der Registrierung erhält der Nutzer eine eindeutige URL als Benutzer-ID. Durch diese einmalige Registrierung kann sich der Nutzer bei allen weiteren Webdiensten, sofern sie OpenId unterstützen, einloggen.
- Autorisierung wird mit OAuth gelöst. OAuth ist ein offenes, standardisiertes Protokoll, welches es einem Nutzer ermöglicht, Applikationen (meistens Webanwendungen) zu autorisieren, Dienste oder bestimmte Daten für andere Applikationen zur Verfügung zu stellen. Der Nutzer hat dabei volle Kontrolle welche Dienste welche Daten austauschen können. Das Hauptmerkmal ist, dass die Dienste Daten austauschen können, ohne jedoch die konkreten Logindaten des Nutzers kennen zu müssen. Hierbei werden Tokens seitens OAuth verwendet und der Nutzer muss diese vorher nur bestätigen.
- Abrechnung muss individuell abhängig vom Sensornetz und den angebotenen Diensten gelöst werden.

Mit dem lightweight tripple-A Ansatz wird das Konzept der Trennung von Aufgaben und Zuständigkeiten verfolgt und die bestehende Infrastruktur des Sensornetzes bzw. Services muss nicht verändert werden. Zwischen dem Nutzer und dem SOS WebService eines Geodatenanbieters wird nun eine neue Schicht, nämlich ein Sicherheitsproxydienst, eingeführt.

Dieser setzt sich aus 2 Hauptelementen zusammen:

- Sicherheitsdienst (Security Service): Dient als Proxy der Annahme von Requests, die an den WebService gerichtet sind. Leitet den Request mit dem mitgeschickten Identifikationstoken weiter an AAAS. Nach der Authentifizierung und Autorisierung durch das AAAS wird der Request an den vorgesehenen WebService abgeschickt und die Antwort an den Client zurück übermittelt.
- AAAS (Authentifizierung, Autorisierung und Abrechnung Service): Im AAAS findet die Authentifizierung des Nutzers statt, allgemeine Verwaltung der Nutzerdaten (einzelne Nutzer oder Nutzergruppen), Autorisierung der Rechte und die Abrechnung über die anfallenden Kosten für den Nutzer. Durch das AAAS behält der Sensornetzbetreiber die volle Kontrolle über die Zugriffe auf sein System. In einer Datenbank können Sicherheitstoken zu bestimmten Nutzern abgelegt und zu jedem Sicherheitstoken kann genau festgelegt werden in welchem Rahmen der Zugriff auf die Daten und die WebServices erlaubt werden soll.

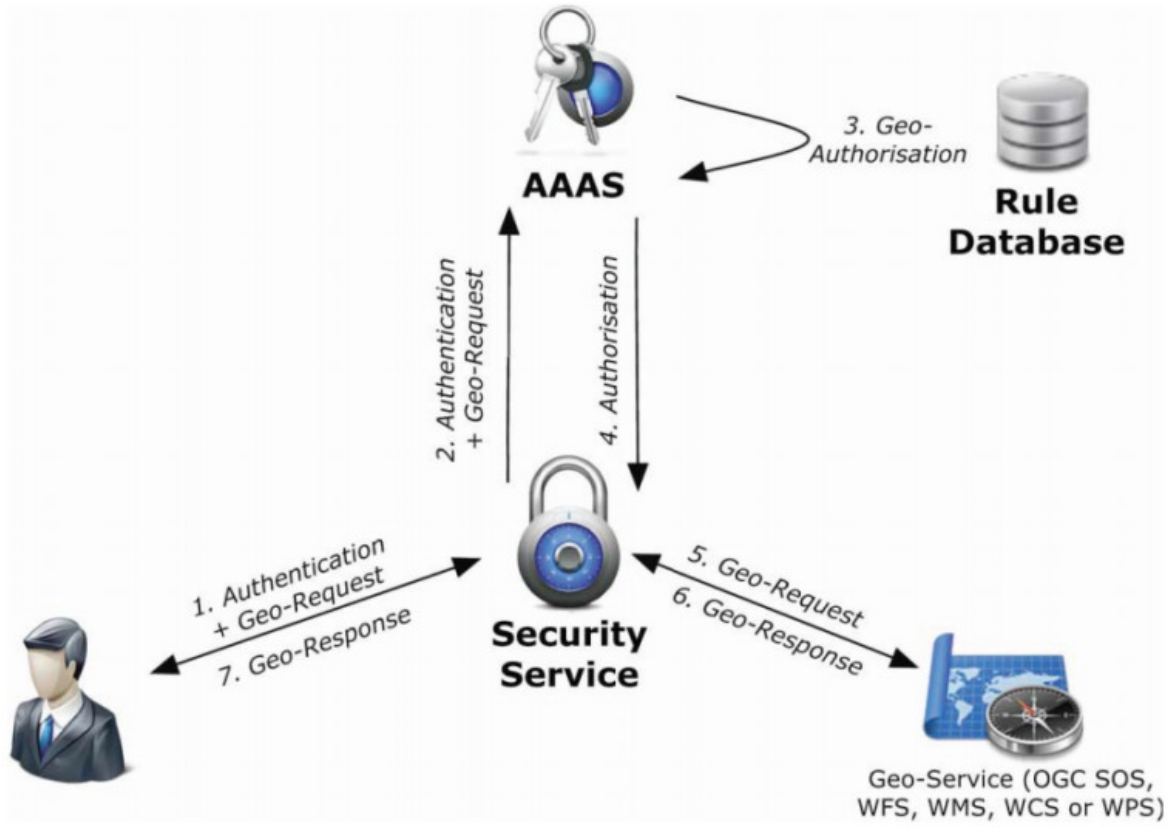

Abbildung 8: Tripple-A Securitymodell

In der Abbildung 8 wird ein allgemeiner Ablauf einer Anfrage an ein Sensornetz mit integriertem Proxy als Sicherheitsdienst dargestellt. Bevor die Abfrage jedoch abgesetzt werden kann, muss sich der Nutzer ein Sicherheitstoken vom Authentifizierungssystem zuschicken lassen. Dieses Sicherheitstoken wird mit der Anfrage an das System dann eingebettet mitgeschickt. Somit fällt ein umständliches und ständiges manuelles Anmelden im Sensorsystem weg. Außerdem muss sich der Nutzer mit dem Sicherheitstoken nur bei dem Sicherheitsdienst authentifizieren und der konkrete WebService, zur Auslieferung der Daten, muss sich darum nicht kümmern.

Nachdem der Nutzer das Sicherheitstoken erhalten hat, wird es im ersten Schritt gemeinsam mit der Anfrage an einen gewünschten SOS geschickt. Die Adresse zum Service hat der Betreiber eines Sensornetzes über einen Catalogue (Indexseiten) breiten Öffentlichkeit mitgeteilt. Bevor die Anfrage den SOS jedoch erreicht, kommt diese zuerst zum vorgeschaltenem Sicherheitsdienst, einem Proxy, welcher die Anfrage an das AAAS weiter leitet. Im AAAS findet nun die Authentifizierung und Autorisierung, anhand des Tokens, statt. Hier wird nun entschieden ob die Anfrage des Nutzers vom Service abgearbeitet werden soll. Sobald der Sicherheitsdienst das OK vom AAAS erhält, wird die Anfrage weiter zum SOS weitergeleitet und die tatsächliche Abfrage und Abarbeitung der Daten kann nun stattfinden.

4. Synchronisation von Sensordaten

Neben den für Sensornetzwerken essentiellen und bereits erörterten Aspekten wie Kommunikation und Datenintegrität ist auch die zeitliche und örtliche Synchronisation von Geoinformationsdaten und den erfassenden Sensoren von großer Bedeutung.

4.1 Synchronisationsproblematik

Sensornetzwerke bestehen meist aus einer sehr hohen Anzahl von Sensoren, welche über einen großen geographischen Bereich verteilt sind. Handelt es sich um “low cost” Sensoren, oder ist an dem Ort, an dem ein Sensor positioniert ist, nur eine sehr eingeschränkte Energieversorgung möglich, so ist der jeweilige Sensor meist nicht selbst in der Lage seine Position z.B. über ein integriertes GPS-Modul zu bestimmen oder sich mit einem Satelliten zeitlich zu synchronisieren.[16]
Deshalb wäre eine manuelle Synchronisation der Sensoren notwendig, was aber aufgrund der erwähnten Randbedingungen schwierig und zeit-, bzw. kostenintensiv sein kann. Außerdem birgt eine einmalige und nicht periodisch wiederholte Kalibrierung und Referenzierung die Möglichkeit mit sich, dass spätere Veränderungen der vorher kalibrierten Parameter oft nur schwer erkennbar sind. Gerade ein zeitlicher Drift der internen Zeitbasis, der zu fehlerhaften Messinterpretation führt, ist ein bekanntes Problem. Probleme die auf solche Phänomene zurückzuführen sind, betreffen vor allem Sensoren, die nur unidirektional von Sensor zur Station kommunizieren, bei Sensoren die Daten sammeln und dann gesammelte Daten Paketweise übertragen.[15]

4.2 Synchronisationsprotokolle

Ein Ansatz um dieses Synchronisationsdefizit zu lösen bieten kollaborative, selbst organisierende Algorithmen als Bestandteil des Kommunikationsprotokolls. Viele kollaborierende Algorithmen zur Positionsbestimmung nutzen Laufzeitmessungen von Mehrfachausbreitungen zur Positionsbestimmung. Um durch diese Methode verlässliche Positionsbestimmungen zu erhalten ist eine zeitliche Synchronisation der einzelnen Nodes essentiell.[17]
Es existieren natürlich zahlreiche Clock-Synchronisations-Protokolle, aber gerade bei den meist stark eingeschränkten Ressourcen der Sensoren, speziell in Bezug auf Energieversorgung, Übertragungsbandbreite und Rechenperformance sind viele dieser Protokolle ungeeignet. Auch wenn sich etwa im Bereich der Computernetze eine Kombination aus NTP (Network Time Protocol) und GPS als äußert präzise erwiesen hat [18], und auch für manche Konfigurationen von Sensornetzwerken, die nicht mit den oben angeführten Ressourcenrestriktionen belegt sind, gute Ergebnisse liefert, so sind doch eigene Time Protokolle für Sensornetzwerke notwendig.

Speziell für die Anwendung in Sensornetzwerken wurden die beiden Protokolle

- RBS (Reference Broadcasting Synchronization) und
- TPSN (Timing-Sync Protocolfor Sensor Networks)

entwickelt.

4.3 Reference Broadcasting Synchronization

Bei RBS wird ein Multi-Hop Clustering Verfahren verwendet. Dabei wird von einer zentralen Stelle ein Synchronisationssignal an alle verbundenen Knoten gesendet (einer der beiden orangen Knoten in Abbildung 9). Jeder Knoten (blau) teilt dann in seiner nächsten Nachricht dem adressierten Empfänger mit, wann er laut seiner Zeit die Synchronisation erhalten hat. Danach wird nach einer linearen Regression aus den erhaltenen Daten die gemeinsame Zeit berechnet.[19]

Abbildung 9: Multi-Hop Clustering

4.4 Timing-Sync Protocol for Sensor Networks

TPSN basiert auf der Berechnung der Round Trip Time, in einer generierten Baum Struktur wie in Abbildung 10 dargestellt. Dabei erfolgt die Auswahl der Wurzel ohne spezielle Regel. Der Baumstruktur folgend werden Kinder mit ihren Eltern synchronisiert. Die Synchronisation erfolgt in Runden was den großen Vorteil hat, dass die Synchronisation periodisch wieder angestoßen wird und es so zu eine periodischen Synchronisation des Netzwerks kommt.[20]

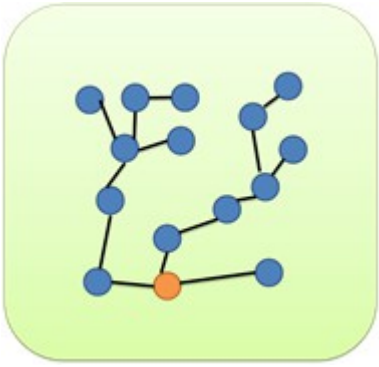

Abbildung 10: Baumstruktur der TPSN

Messdaten ohne konkreten Bezug zu Raum und Zeit machen keinen Sinn und besitzen keine Aussagekraft. Die Wahl des geeigneten Zeit-Synchronisation-Verfahrens und damit auch die Ausgangsbasis für eine zuverlässige Lokalisation ist immer von den Eigenschaften des Sensornetzwerkes abhängig und muss darauf abgestimmt werden.
Eine weitere wesentliche Rolle spielt der Kontext in welchem die Messungen vorgenommen werden. Unterschiedliche Einsatzgebiete erfordern unterschiedlich scharf formulierte und verlangte zeitliche Verzögerungen bzw. einen Zeitdeterminismus. So ist es bei der allgemeinen Messung von Umweltparametern wie z.B. Lufttemperatur oder Niederschlagsmenge vollkommen in Ordnung wenn die Abweichungen einige Sekunden betragen. Dennoch können wir mit der Einbindung dieser „live Daten“ Echtzeit Aussagen treffen, die ein aktuelles Bild der Umwelt widerspiegeln. Diese Ungenauigkeit würde jedoch bei der Überwachung von technischen Prozessen (SCADA GIS) in einem Industriewerk natürlich zu Problemen führen und stellt andere Anforderungen an die Sensoren in einem für dieses Szenario ausgelegtes Sensornetzwerk.

5. Konklusion

Die technische Entwicklung und Standardisierung im Bereich des Sensoring und Monitoring für das Sensor Web schreiten immer rasanter voran. Die Beschäftigung mit dem Thema Sensor Observation Service als Teilbereich von Sensornetzwerken im Allgemeinen lässt unter anderem auch aufgrund der Menge an verfügbaren wissenschaftlichen Publikationen neuesten Datums darauf schließen, dass dieser Forschungsbereich das Interesse eine großen Zielgruppe geweckt hat. Unsere Recherche zu der Thematik zeigt auch, dass es vielfältige Anwendungsmöglichkeiten aus den unterschiedlichsten Bereichen der Wirtschaft und Umwelt gibt. Gerade die auf breiten Schultern ausgearbeiteten Spezifikationen und Standards erlauben zukünftig eine immer bessere Vernetzung von Sensoren und Sensornetzwerken.
Interoperabilität der Messdaten führt nicht nur zum Austausch und Vernetzung dieser Messdaten, sondern auch zum Austausch von Ideen, Ansichten und Erkenntnissen unter den beteiligten Personen. Die umfassende Observation und Wahrnehmung bestimmter Phänomene der Umwelt und das Bereitstellen der Messdaten dient einem höheren Ziel. Aus den Messdaten sollen Informationen extrahiert werden, welche neues Wissen schaffen und beitragen ein besseres Verständnis über bestimmte Sachverhalte zu erhalten. Nicht nur im globalen Hinblick, sondern vor allem lokal mit einer größeren Relevanz für den Nutzer. Schlussendlich hilft uns dies besser auf bestimmte Ereignisse und Situationen zu reagieren und weisere Entscheidungen zu treffen.
Wie an der Implementierung der in Kapitel 2 (SOS) und Kapitel 3 (Sicherheit der Daten) betrachteten Funktionalitäten und Protokolle zu erkennen ist, profitiert die Entwicklung des Sensor Observation Service erheblich von Erfahrungen, Methoden, Formalismen und Protokollstrukturen aus dem Bereich der Computernetze. Gerade das Vorbild des Internets und die Portierung von dessen Errungenschaft auf ein “Internet der Sensoren” ermahnt aber zu Vorsicht. Ein Aspekt der vermutlich nicht nur subjektiv wahrgenommen, eher von untergeordneter Bedeutung in diesem Zusammenhang behandelt wurde, ist der der Datensicherheit und des Datenschutzes. Wenn Sicherheit der Daten und Kontrolle der Zugriffe erst im nachhinein in ein, für den freien Austausch von Informationen vorgesehenes Netzwerk integriert wird, kann das zu erheblichen Problemen und Unsicherheiten führen. Durch einfache Zugriffsregelungsmechanismen bleiben Messdatenanbieter, unabhängig davon ob ein kommerzielles Unternehmen oder ein kleines privates Sensornetzwerk, in voller Kontrolle über die Zugriffe auf ihre Messdaten und Auslastung der WebServices. Obwohl das Sensornetz an das Sensor Web angeschlossen ist, die Existenz der breiten Öffentlichkeit bekannt ist, behält der Betreiber alle Rechte und kann Zugriffe regeln. Wir glauben, dass solche Zugriffsregelungsmechanismen nicht in der Regel benutzt werden um sein Sensornetz von der Außenwelt abzuschotten, sondern eher die Betreiber animieren den Zugriff nach bestimmten Kriterien zu erleichtern.
Sowohl die technische Entwicklung der Sensoren an sich als auch die Entwicklung und Weiterentwicklung von Standards zur Interoperabilität werden immer weiter vorangetrieben. Unter anderem durch neue Generationen von Smartphones, die neben ihren eigentlichen Funktionen auch als hoch komplexe Sensoren gesehen werden müssen, erfährt der Begriff des Pervasive-Monitorings eine immer größer werdende Bedeutung für unseren

5. Konklusion

Alltag. Stationäre Messstation haben sich bewährt, doch die Zukunft wird durch mobile und agile Sensoren geprägt werden. Eine neue wesentliche Rolle wird der Mensch als „citizen sensor“ in Kombination mit „embedded measuring devices“ spielen. Nicht nur die Temperatur oder Niederschlag werden gemessen, sondern der Lärm einer Umgebung, Zustand von Straßen oder Gebäuden (Nutzer bewerten / laden Foto online über ihr Smartphone). Die Menschen möchten sich mitteilen und sobald die Technik verfügbar ist, werden sie auch bestimmte individuelle Parameter ihrer lokalen Umwelt und des Umfeldes in das Sensornetz zur Verfügung stellen. Man sollte auch vor den ganzen Befürchtungen um den “gläsernen Menschen” nicht den enormen Vorteil und das Potential von Sensornetzwerken außer acht lassen. Gerade in immer wieder auftretenden Notfällen und Katastrophen hat diese Technologie ebenso Vorteile wie im Umweltmonitoring und Umweltschutz.
Wie auch aus dem “No free Lunch” Theorem aus der Kombinatorischen Optimierung bekannt, gibt es auch in diesem Fall keinen Nutzen ohne Kosten und es liegt am Konsumenten selbst, ob sich ein Konzept und die Technologie durchsetzen oder nicht.

Quellen

[1] Sherman, G.
Desktop GIS: Mapping the Planet with Open Source Tools
Pragmatic Bookshelf, 2008

[2] Marzban, C.
On the Notion of "Best Predictors": An Application to Tornado Prediction 1999

[3] Havlik, D; Schade, S; Sabeur, Z.A.; Mazzetti, P; Watson, K; Berre, A.J.; Mon, J.L.
From Sensor to Observation Web with Environmental Enablers in the Future Internet. Sensors 2011

[4] Resch, B; Mittlboeck, M; Lippautz, M.
Pervasive Monitoring - An Intelligent Sensor Pod Approach for Standardised Measurement Infrastructures
Sensors 2010, vol. 10

[5] Brauner, J; Schaeffer, B.
Integration of GRASS functionality in web based SDI service chains. Proceedings of the academic track of the 2008 Free and Open Source Software for Geospatial (FOSS4G) Conference, incorporating the GISSA 2008 Conference, 2008

[6] Resch, B; Shulz, B; Mittlboeck, M; Heistracher, T.
Pervasive geo-security – a lightweight tripple-A approach to securing distributed geo-service infrastructures
International Journal of Digital Earth 2012

[7] Bleier et al.
SANY - an Open Service Architecture for Sensor Networks
SANY IP, 2009

[8] NIKE, INC.: Nike+ Tracking http://nikeplus.nike.com/plus/ (12.7.2012)

[9] Open Geospatial Consortium, Inc.: OpenGIS Standards and Specications
http://www.opengeospatial.org/standards/ (27.05.2012), 1994-2012

[10] Resch, B.
Geo-sensor Web – Echtzeitmessungen für Ubiquitäre Monitoring-Systeme
HMD Journal Praxis der Wirtschaftsinformatik, 2010, vol. 276

[11] Bröring, A; Echterhoff, J; Jirka, S; Simonis, I; Everding, T; Stasch, C; Liang, S; Lemmens, R;
New Generation Sensor Web Enablement
Sensors 2011, vol. 11

[12] http://www.opengeospatial.org/domain/swe (5.7.2012)

[13] Stasch, C; Bröring, A; Echterhoff, J;
OGC Sensor Observation Service Interface Standard 2011

[14] Tamayo, A; Viciano, P; Granell, C; Huerta, J;
Sensor Observation Service Client for Android Mobile Phones 2011

[15] Sivrikaya, F; Yener, B.
Time synchronization in sensor networks: A survey
IEEE Network, 2004, vol. 18

[16] Römer, K.
Time Synchronization and Localization in Sensor Networks 2005

[17] Bulusu, N; Jha, S.
Wireless Sensor Networks: A Systems Perspective
Artech House: Norwood MA, USA, 2005

[18] Mills, D. L.
Internet time synchronization: the network time protocol
IEEE Trans. Commun. 1991, vol. 10

[19] Elson, J; Girod, L; Estrin, D.
Fine-grained network time synchronization using reference broadcasts.
In Fifth Symposium on Operating Systems Design and Implementation (OSDI 2002), 2002

[20] Ganeriwal, S; Kumar, R; Srivastava, M.B.
Timing-sync protocol for sensor networks. In Proceedings of the 1st international conference on Embedded networked sensor systems
Los Angeles, CA, USA, 2003