SharkNet
Systembeschreibung
Version 0.0.6

Dustin Feurich

8. Januar 2018

Inhaltsverzeichnis

Kapitel 1

Überblick

1.1 Einleitung

Durch die rasante Entwicklung des Internet of Things (IoT) ist das Interesse an einen semantischen Datenaustausch spürbar gestiegen. Wurde in den letzten Jahrzehnten noch fast ausschließlich klassisch über die Zieladresse der Datenpakete geroutet, so werden jetzt auch die Metadaten dieser Datenpakete beim Routing zunehmend beachtet. Das Routing erfolgt hierbei also inhaltsbasiert und ermöglicht ein Routing nach den Interessen der Kommunikationsteilnehmer. Der Datenaustausch zwischen diesen Teilnehmern kann beim inhaltsbasierten Routing sowohl per klassischer Client-Server Architektur, als auch Peer-To-Peer (P2P) erfolgen. In dieser Arbeit wird der Datenaustausch über P2P erfolgen, was mehrere Vorteile bietet:

- Die Verbindungen zwischen Kommunikationsteilnehmern (Peers) können spontan aufgebaut werden, es wird keine Serverinfrastruktur benötigt.
- Die Daten liegen ausschließlich bei den Peers selbst. Da es keine Zwischenstation für die Datenpakete gibt, erhöht dies die Vertraulichkeit der Kommunikation immens.
- Nahezu alle Kommunkationsanwendungen verwenden das Internet um den Datenaustausch zu ermöglichen. Eine Verbindung mit dem Internet ist jedoch nicht zu jeder Zeit und an jedem Ort verfügbar. Weiterhin kann auch hier auf den Zwischenservern die Kommunikation gespeichert und an Dritte weitergegeben werden.

Kapitel 2

Verwandte Veröffentlichungen

Es gibt zahlreiche wissenschaftliche Paper, die Semantisches oder Inhaltsbasiertes Routing zum Thema haben. Viele diese Paper sind jedoch entweder schon mindestens zehn Jahre alt, oder beinhalten nicht exklusiv den Datenaustausch über Peer-To-Peer. Im Folgenden wird jeweils die Grundidee von vier Arbeiten vorgstellt, welche ausschließlich den semantischen Datenaustausch über P2P zum Inhalt haben.
Strassner et. al. präsentieren ein hybrides Routing, bei dem sowohl semantisch als auch traditionell geroutet wird. Die Peers bauen hierbei ein *small world* Netzwerk auf, bei dem jeder Peer viele kurze und nur wenige lange Verbindungen zu anderen Peers hat. Es werden zwei semantische Strukturen definiert - *node profiles* und *object profiles* - welche beide anhand von Metadaten beschrieben werden. Ein Interesse wird mit Hilfe des *node profils* formuliert, das dann an die anderen Peers direkt geschickt wird. Interessiert sind die Peers an die Objekte. Durch eine semantische Ähnlichkietsanalyse wird überprüft, ob ein Peer entweder direkt ein Objekt an den anfragendne Peer liefert, oder ob er das *node profile* an andere Peers weiterleitet. Das *node profile* wird an den Peer weitergeleitet, bei dem die Ähnlichkeitsanalyse zwischen *node profile* und *object profile* am höhsten ist und sich außerdem physisch in Reichweite befindet.
David Faye et. al. stellen in Ihrer Ausarbeitung ein semantisches und abfrageorientiertes (Query) Routing vor. Die neuartige semantische Struktur ist hierbei die *expertise table*, in der mit Metadaten festgehalten ist, welcher Peer über welches Wissen verfügt. Anders als in Sharknet sind die Peers nicht gleichberechtigt, sondern in zwei Kategorien eingeteilt: normale Peers und Super-Peers. Ein Super-Peer verwaltet mehere normale Peers und besitzt dafür eine *expertise table*. Sie reichen die Anfragen entweder an andere Super-Peers weiter oder lassen diese von normalen Peers auswerten. Ein Interesse wird mit Hilfe einer Anfrage gestellt, diese Anfrage wird durch den Routingalgorithmus an das relevante Ziel gesendet. Dies läuft folgendermaßen ab:

- Ein Peer fomuliert sein Iteresse mit einer Query und sendet diese an seinen zuständigen Super-Peer, der im Paper als *Godfather* bezeichnet wird.
- Der *Godfather* wertet nun mit der Query und den *expertise tables* aller verfügbaren anderen Super-Peers aus, an welche Super-Peers er die Query weiterreicht.
- Nachdem ein Super-Peer auf dieser Art eine Query erhalten hat, kann er diese nun entweder abermals an andere Super-Peers weiterleiten oder sie von einen seiner zugeordneten Peers ausführen lassen.
- Das Ergebnis der Ausführung wird nun an den eigentlichen Absender der Query zurückgeleitet.

Einen anderen Ansatz mit komplett gleichberechtigten Peers stellt Antonio Carzaniga et. al. vor, bei dem parallel zwei Protokolle ausgeführt werden. Dies umfasst zum einen das *Broadcast Routing Protocol* und zum anderen das *Content-based Routing Protocol*. Das Broadcast Protokoll ist für das physische Versenden der Nachrichten zwischen den Peers verantwortlich und baut eine Spanning-Tree Topologie auf. Die Nachricht wird zunächst ohne Einschränkung an alle Peers geschickt, die erreichbar sind. Das eigentliche Routing geschieht durch das *Content-based Routing Protocol*. Folgende semantische Strukturen werden benutzt:

- Eine *Message* besteht aus typisierten Attributen
- Ein *predicate* ist eine Disjunktion von Konjunktionen von Bedingungen (constraints), die sich auf einzelne Attribute beziehen
- Die *content-based forwarding table* enthält die von den Peers gesetzten *predicates*

Eine Funktion wertet anhand der *forwarding table* aus, an welche Peers die Nachricht weitergeleitet werden soll. Zusätzlich wird durch das Broadcast Protokoll ermittelt, welche Peers sich physisch in Reichweite befinden. Die Nachricht wird nun alle Peers geschickt, die in beiden Mengen vorkommen. Diese Funktionsweise ähnelt SharkNet, da in der Anwendung die Nachrichten ebenfalls per Broadcast verschickt werden. Die semantische Auswertung erfolgt in SharkNet jedoch durch Profile, die vom Nutzer dynamisch festgelegt werden können und nicht durch eine sich automatisch aufbauende Tabelle.
Luca Mottola et. al. haben eine sich selbst reparierende Baumtopolgie entworfen, mit der inhaltsbasiertes Routing in mobilen Ad Hoc Netzwerken realisiert werden kann. Laut Mottola et. al. benötigt eine Topologie in Form eines Baums bei ad hoc Netzwerken eine stetige Selbstreparatur, die durch das dynamische Entfernen und Hinzufügen von mobilen Geräten notwendig sei. Diese Topologie wird während der Programmausführung auf den

Peers stetig angepasst, um auch bei einem häufigen Peerwechsel weiterhin benutzbar zu sein. Die Baumstruktur ist dabei für das inhaltsbasierte Routing essentiell. Das Routing erfolgt über das publish-subcribe Prinzip, wobei die Peers Nachrichten zu den Themen bekommen, die sie für die sie sich angemeldet (subscribt) haben.
Der wesentliche Unterschied zwischen den vorgestellten Veröffentlichungen und dieser Arbeit sind einerseits die Eingangs- und Ausgangsprofile, mit denen natürliche Personen eingehende und ausgehende Nachrichten semantisch filtern können und andererseits die Präsentation einer konkreten mobilen Applikation, die diese Art des Routings verwirklicht. Außerdem unterscheiden sich die dafür verwendeten semantischen Strukturen deutlich von anderen Veröffentlichungen.
Da diese Arbeit jedoch nicht nur das semantische Routing, sondern mit Sharknet auch ein dezentrales Netzwerk realisiert, soll an dieser Stelle kurz das bereits bekannte dezentrale soziale Netzwerk Diaspora vorgestellt werden.
Jeder Benutzer kann in Diaspora einen eigenen Server benutzen, welche als Pod bezeichnet werden. Diese Pods beinhalten die Benutzerdaten und werden vom Besitzer des Pods verwaltet. Der umfassende Datenschutz ist bei Diaspora jedoch nur dann gegeben, wenn jeder Benutzer auch einen eigenen Webserver benutzt, um damit seinen Pod zu hosten. In der Realität wird häufig aber kein eigener Webserver benutzt, außerdem ist die direkte Kommunikation zwischen den Pods nur eingeschränkt möglich. So lassen sich zum Beispiel keine Kontaktlisten von anderen Pods crawlen, auch wenn diese sie zur Verfügung stellen würden. Dies hat zur Folge, ein Teil der Benutzer sich ausschließlich mit anderen Pods verbinden, die dann zu Sammelpods werden.

Kapitel 3

Grundlagen

3.1 Routing

3.1.1 Traditionelles Routing

Routingalgorithmen werden benötigt, um Pfade für den Datenverkehr innerhalb eines Netzwerks zu finden. Beim traditionellen Routing erstellt jeder Router eine Routingtabelle, die Netzwerkadressen und Netzmasken enthält. Anhand dieser Tabelle, bei der diese Adressen auch Geräte zugeordnet sind, können dann Pakete durch das Netzwerk weitergeleitet bzw. geroutet werden. Bei der Suche nach einer geeigneten Route durch das Netzwerk wird klassischerweise ein Longest Prefix Match durchgeführt. Bei einem Treffer wird das Paket im entsprechenden output port weitergeleitet, ansonsten wird der default link genommen. Die Routingtabellen werden durch eine Analyse der vorhandenen Netzwerktopologie aufgestellt. Sollte sich die Topolgie im Betrieb ändern, muss daher auch die Routingtabelle angepasst werden. Routingschemata werden üblicherweise als Graphen dargestellt, wobei die Knoten die Kommunikationsteilnehmer und die Kanten die Leitungen zwischen den Teilnehmern darstellen. Die Kanten enthalten auch Informationen über die Kosten für die Paketübertragung zwischen Knoten. Die Kosten beziehen sich dabei meistens auf die physikalische Länge der Leitung, je länger die Leitung desto höher sind auch die Kosten. Da es bei der Wegfindung zwischen zwei nicht direkt benachbarter Knoten häufig mehrere Alternativen gibt, werden die nötigen Gesamtkosten die zwischen Anfangs- und Zielknoten auftreten, bei der Wahl des Pfades berücksichtigt. Beim traditionellen Routing wird also vorrangig nach den kostengünstigsten Pfaden zwischen Knoten innerhalb eines Netzwerks gesucht.
Routing-Algorithmen lassen sich in zwei Klassen aufteilen:

- Globaler Routing-Algorithmus: Hierbei ist das komplette Netzwerk bereits vor der

Berechnung der kostengünstigsten Route bekannt. Es können direkt alle möglichen Pfade zwischen Ausgangs- und Zielknoten und deren Gesamtkosten bestimmt werden.

- Dezentraler Routing-Algorithmus: Die Knoten haben hierbei nur Informationen über die Knoten und Kanten, welche sich in der Nähe befinden, das komplette Netzwerk ist nicht bekannt. Das Finden eines geeigneten Pfades kann also nur iterativ von Knoten zu Knoten geschehen und nicht bereits im Voraus.

Da das Ziel dieser Arbeit ein semantischer Broadcast ist, bei dem sich die Kommunikationspartner vorher nicht kennen müssen, wird es sich bei dem Algorithmus um einen dezentralen Routing-Algorithmus handeln.
Eine weitere wichtige Unterscheidung bei Routing-Algorithmen ist die Frage, ob diese statisch oder dynamisch gestaltet sind:

- Statische Routing-Algorithmen werden benutzt, wenn sich die Kanten zwischen den Knoten nur selten ändert. Die Netzwerktopologie bleibt also konstant.

- Bei Dynamischen Routing-Algorithmen werden bei sich häufig ändernden Netzwerktopologien eingesetzt. Sie müssen anders als die statischen Algorithmen den stetigen Wechsel von Knoten, Kanten und Kosten beachten.

Das Ergebnis dieser Arbeit wird in einer mobilen Applikation eingebunden werden und soll von natürlichen Personen per Smartphone bedient werden können. Der Routing-Algorithmus muss also zwingend dynamisch sein, da Menschen mit ihren Smartphones anders als andere Netzwerkgeräte konstant in Bewegung sind. Da bei einem Broadcast unabhängig von den Kosten die Nachricht zunächst an alle Personen geschickt werden wird, handelt es sich zusammengefasst um einen dezentralen, dynamischen und lastinsensitiven Routing-Algorithmus.

3.1.2 Inhaltsbasiertes Routing

Beim inhaltsbasierten Routing wird für die Bestimmung des Pfads nicht die Zieladresse des Pakets ausgewertet, sondern die semantische Beschreibung des Paketinhalts. Jedes Paket verfügt daher über eine Inhaltsbeschreibung, wobei dann alleine diese Beschreibung abhängig ist, an welchen Knoten die Nachricht weitergeleitet wird. Eine wichtige Voraussetzung für diese Art von Routing ist ein Peer-To-Peer (P2P) Netzwerk, da die Pakete stets nur von Punkt zu Punkt gesendet werden. Die Peers müssen ebenfalls ein Interesse formulieren können, anhand dessen bestimmt werden kann, ob ein Paket für sie relevant ist. Dies geschieht meist über themengesteuerte Abonnements, Peers können über diese

Abonnements ihr Interesse an einer bestimmten Gruppe von Paketen bekunden. Es gibt zwei unterschiedliche Arten, diese Abonnements innerhalb eines Netzwerks zu verwalten:

- Die Abonnements werden ausschließlich vom Peer selbst für die Auswertung herangezogen, andere Peers können diese nicht berücksichtigen. Die Pakete müssen nach der Auswertung durch den Peer dann an alle verfügbaren Peers in der Nähe weitergeleitet werden, da deren Abonnements unbekannt sind.
- Die Peers teilen Ihre Abonnements den anderen Teilnehmern im Netzwerk mit. Dadurch können die Pakete nun gezielt nur an die Peers weitergeleitet werden, die sich für das Paket auch interessieren.

Beide Lösungsansätze haben Vor- und Nachteile. So hat der zweite Ansatz den Vorteil, dass nicht bei jedem Peer eine semantische Prüfung der Paketbeschreibung erfolgen muss, da diese Filterung bereits beim sendenden Peer vorgenommen worden ist. Der entscheidende Nachteil dieses Ansatzes ist jedoch, dass sämtliche Modifikationen an bestehenden Abonnements jedem Peer im Netzwerk mitgeteilt werden muss. Bei der App dieser Arbeit ist davon auszugehen, dass Benutzer ihre Abonnements (bzw. Profile) häufig editieren, was zu einer Flut an Benachrichtigungen zu anderen Peers führen könnte. Es ist bei dem Ad-Hoc Broadcast auch nicht realistisch davon auszugehen, dass jeder Peer die Abonnements der anderen Peers kennt, bevor der Benutzer eine Nachricht versendet. Da das Protokoll vorrangig von leistungsstarken Smartphones und nicht von eher leistungsschwachen Kleinstgeräten benutzt werden soll, ist der durch die wiederholte semantische Auswertung der Paketbeschreibung nötige Aufwand vernachlässigbar. In dieser Arbeit wird daher der erstgenannte Lösungsansatz verfolgt.

3.1.3 Broadcast-Routing

Wenn ein Paket an alle interessierten Peers innerhalb eines Netzwerks verschickt werden soll, wird ein Broadcast-Routing benötigt, da das bisher beschriebene Unicast-Routing nur die Wegfindung zwischen zwei Knoten realisiert. Häufig sind für einen Knoten nicht alle anderen Knoten des Netzwerks direkt erreichbar, es werden also Zwischenstationen benötigt welche die Nachricht weiterleiten. Anders als beim Unicast-Routing ist die Anzahl der Pfade also variabel, je nachdem wie viele Knoten das Paket an ihre Nachbarknoten weiterleiten. Wenn ein Knoten eine Nachricht an alle Nachbarknoten schickt und diese sie wiederum an ihre Nachbarknoten schicken, wird dieser Ansatz *flooding* genannt. *Flooding* kann bei unbedachtem Einsatz zu Schleifen führen. Hierbei erhält und versendet ein Knoten wiederholt Nachrichten, die er bereits verwertet hat. Dieser endlose Ping-Pong-Effekt zwischen den Nachbarknoten führt dann zum sogenannten *Broadcast storm*, der

das gesamte Netzwerk unbrauchbar macht. *Flooding* muss also zwingend kontrolliert werden, die Knoten müssen unabhängig von der semantischen Überprüfung der Nachrichten prüfen können, ob sie eine eingehende Nachricht bereits verwertet haben. In der Praxis wird meistens einer der folgenden drei Lösungsansätze für dieses Problem gewählt:

- Beim sequenznummerkontrollierten *Flooding* schickt jeder Knoten seine Adresse und eine Broadcast-Sequenznummer an seine Nachbarknoten. Dadurch kann jeder Knoten eine Tabelle anlegen, die bereits empfangene Pakete den Nachbarknoten zuordnet. Bei eingehenden Paketen wird nun vorher überprüft, ob dieses Paket bereits in der Liste eingetragen ist.

- Das *Reverse Path Forwarding* (RPF) lässt die Pakete nur dann an Nachbarknoten weiterleiten, wenn der das Paket absendende Knoten das Paket über den kürzesten Pfad erhalten hat. Es werden alle Pakete verworfen, die nicht auf dem kürzesten Unicast-Pfad zurück zur Quelle liegen. Die Nachricht wird außerdem nicht an den Nachbarknoten weitergeleitet, der auf diesen kürzesten Pfad liegt.

- Der wohl bekannteste Ansatz ist der Aufbau eines *Spanning Tree*, der alle Knoten genau einmal enthält. Die Knoten leiten die Nachrichten nur an ihre Baumnachbarn weiter. Dadurch können Schleifen vollständig vermieden werden.

In dieser Arbeit wird eine angepasste Variante des sequenznummerierten *flooding* benutzt, um *Broadcast storms* auszuschließen. Dies wird in Unterkapitel x.x genauer erläutert.

3.2 Shark

3.2.1 Shark Framework

Das Protokoll soll auf der Basis des Shark Frameworks entwickelt werden. Das Framework wurde von Prof. Dr.-Ing. Thomas Schwotzer entworfen, um die Entwicklung von semantischen Peer-To-Peer Anwendungen zu erleichtern. Es ist mit seinen semantischen Strukturen und Auswertungsmethoden für dezentrale Anwendungen geeignet. Das Wort Shark steht für Shared Knowledge - Verteiltes Wissen.
Das Framework definiert, dass jeder Benutzer (Peer) über eigene Wissensbasis verfügt, welche mit semantischen Annotationen versehenes Wissen des Benutzers speichert. Jede in der Wissensbasis gespeicherte Information muss daher auch semantisch beschrieben werden, bevor es in der Wissensbasis abgelegt werden kann. Informationen werden semantisch mit Wörtern beschrieben, wofür im Framework die Klasse *Semantic Tag* und von dieser Klasse ableitende Klassen benutzt werden. Es werden *Semantic Tags* statt normale

Zeichenketten benutzt, da die fast jede Sprache semantische nicht eindeutige Wörter wie beispielsweise Homonyme aufweist. Die Tags können innerhalb von Behältern gespeichert werden, wobei es drei Arten von Behälter gibt:

- *Sets* enthalten *Semantic Tags* ohne Beziehungen zwischen den Tags zu speichern.
- *Taxonomies* speichern zusätzlich zu den Tags noch gerichtete Beziehungen. Diese gerichteten Beziehungen zwischen den Tags können entweder den Wert *sup* oder *sub* annehmen und ermöglichen somit eine hierarchische Anordnung der Wörter.
- Das *Semantic Net* verhält sich wie eine *Taxonomy*, die Beziehungen können hierbei aber beliebige Werte (in Form von Zeichenketten) annehmen. Dadurch können beispielsweise Verwandschaftsbeziehungen dargestellt werden.

Die Behälterklassen werden dann dazu benutzt, die Informationen zu beschreiben. Informationen werden mit Hilfe von sieben Dimensionen beschrieben, wobei dafür bis zu sieben Behälter und ein Literal verwendet werden.

Tabelle 3.1: Dimensionen einer Information

Dimension	Definition
Topics	Thematische Beschreibung der Information
Types	Um was für eine Art handelt es sich bei der Information
Approvers	Welche Peers haben diese Nachricht
Receivers	An welche Peers ist die Information gerichtet
Senders	Welche Peers haben diese Nachricht versendet
Locations	An welchen Orten ist diese Information relevant
Times	In welchen Zeiträumen ist diese Information relevant
Direction	Literal welches den Eingang und Ausgang der Information bestimmt

Dieses Unterkapitel ist nur eine rudimentäre Zusammenfassung über das Shark Framework, einen ausführlichen Überblick über das Framework bietet der Shark Developer Guide.

3.2.2 ASIP

Innerhalb der letzten drei Jahre wurde ein grundlegendes Protokoll für Shark entwickelt, welches die zwei zentralen Befehle bezüglich der Kommunikation zwischen Peers vorgibt und den Namen *Ad hoc Semantic Internet Protocol* trägt. Die ebenfalls vom Protokoll für Shark neu eingeführten Strukturen können im entsprechenden Repository auf Github eingesehen werden.[x] In der folgenden Abbildung alle Bestandteile der semantischen Strukturen in ASIP abgebildet.

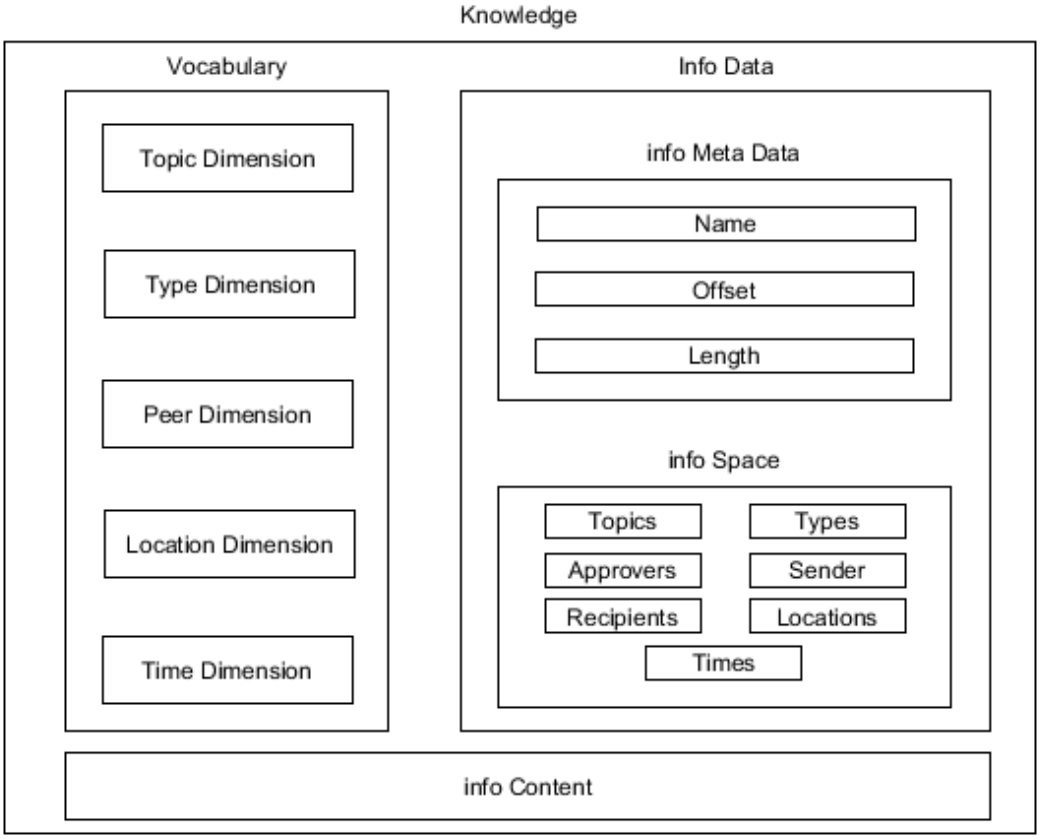

Abbildung 3.1: Die ASIP/Shark Bestandtteile im Überblick

Die beiden wichtigsten Kommandos des Protokolls sind:

- Insert: Dieser Befehl wird dazu benutzt, um neue Informationen (bzw. Wissen) von anderen Peers der eigenen Wissensbasis hinzuzufügen. Dieses Wissen ist folgendermaßen unterteilt:
  - Das Vokabular des Peers welches alle ihm bekannten Wörter enthält. Die Wörter sind wiederum in die fünf Dimensionen Topic, Type, Peer, Location und Time unterteilt.
  - Der eigentliche Informationsinhalt in Form eines byte Streams mit Rohdaten.
  - Technische Metadaten über den Informationsinhalt wie beispielsweise die Anzahl der Bytes
  - Semantische Metadaten über den Informationsinhalt in Form der in Tabelle x.x beschriebenen sieben Dimensionen, technisch umgesetzt mit Behältern von *Semantic Tags*.

- Expose: Neben dem Hinzufügen von neuen Wissen haben Peers auch die Möglichkeit, ihr Interesse an neuem Wissen gegenüber anderen Peers zu bekunden. Dies geschieht über den Befehl *Expose*, wobei auch hier das Interesse in Form der in Tabelle x.x dargestellten sieben Dimensionen formuliert wird.

[...]

3.2.3 SharkNet

SharkNet ist ein dezentrales soziales Netzwerk für Android Geräte und wurde von Michael Schwarz und Prof. Dr.-Ing. Thomas Schwotzer von 2015 bis 2017 entwickelt. Es kann durch die folgenden drei Kernaspekte beschrieben werden:

- Dezentraler Datenaustausch ohne der Verwendung eines Servers
- Eine Public-Key-Infrastruktur, womit die Kommunikationspartner sich gegenseitig authentifizieren können
- Ausschließliche Benutzung von Open-Source Bilbiotheken und Protokollen

Sharknet bildet die Grundlage für diese Arbeit und wurde an diversen Stellen weiterentwickelt, wobei auch einige Probleme im Bereich der Kommunikation zwischen den Peers behoben werden mussten. Die ursprüngliche Zielgruppe von SharkNet sind Schüler der Katholischen Theresienschule Berlin, die als Testpersonen SharkNet anstelle von Facebook oder anderen servergebundenen sozialen Netzwerken nutzen sollten. Über die Webseite `http://sharedknowledge.github.io/` kann bereits ein Prototyp heruntergeladen werden, dieser enthält aber noch nicht die eigentliche Kernfunktionalität, daher keinen Chat bzw. Gruppenchat. Ein wichtiger Bestandteil dieser Arbeit ist es daher, neben dem semantischen Broadcast auch die normale Chatfunktionalität für den Endanwender benutzbar zu machen.
[...]

Kapitel 4

Bluetooth

4.1 Aufgabe der Komponente

Die über SharkNet abgeschickten Nachrichten werden über Bluetooth übertragen. Die Komponente ist dabei ausschließlich für die kabellose Übertragung von Daten bzw. Nachrichten verantwortlich, die Ortung von potentiellen Kommunikationspartern erfolgt über die Wifi-Direct Komponente. Auch die Filterung von bereits bekannten oder semantisch uninteressanten Nachrichten wird nicht innerhalb dieser Komponente, sondern innerhalb der Semantischen Routing Komponente vorgenommen.
Da es in SharkNet neben normalen Chats auch Gruppenchats und einen semantischen Broadcast gibt, erfordert der Datenaustausch mit Bluetooth kein Pairing der miteinander kommunizierenden Geräte. Dies trägt maßgeblich zur Benutzerfreundlichkeit bei, da insbesondere beim semantischen Broadcast sonst ständig Anfragen zum Pairing auf dem Gerät erscheinen würden und vom Benutzer zusätzliche Interaktionen erforderlich wären.

4.2 Architektur

4.2.1 Überlick

Im folgenden UML-Klassendiagramm sind alle Bestandteile der Bluetooth Komponente von SharkNet abgebildet.

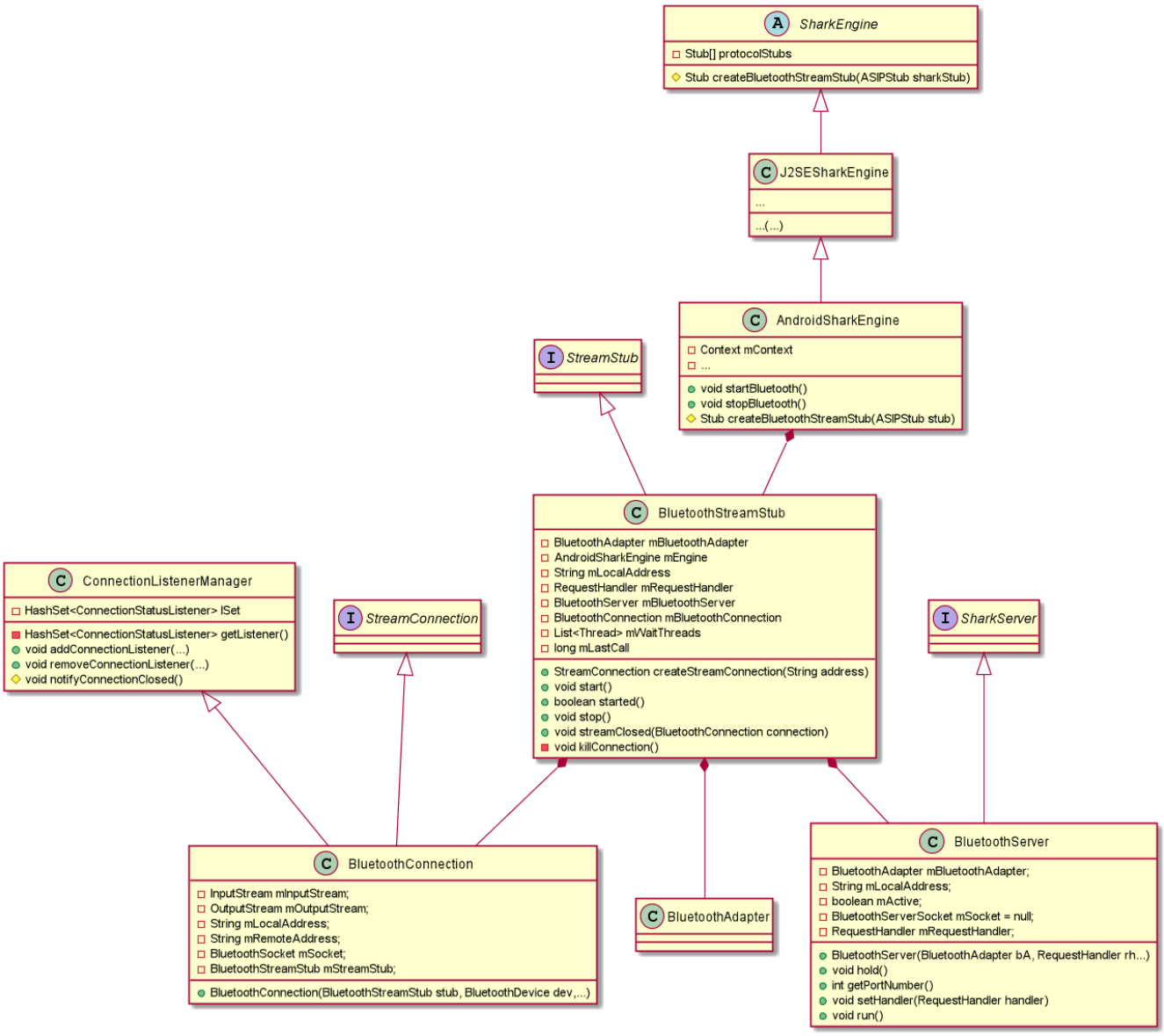

Abbildung 4.1: Die Bluetooth Klassen im Überblick

Im Zentrum dieser Hierarchie steht die Klasse *BluetoothStreamStub*. Eine Instanz dieser Klasse befindet sich als Attribut in der Klasse *AndroidSharkEngine*, von der aus alle Protokolle wie NFC, Wifi-Direct oder Bluetooth gesteuert werden. Sie stellt daher auch Methoden wie *startBluetooth()* oder *stopBluetooth()* bereit.

4.2.2 Schnittstellendefinitionen

Anhand der Klassenhierarchie der Bluetooth-Komponente lässt sich erkennen, dass die folgenden drei Schnittstellen implementiert werden:

- *StreamStub*: Mit Hilfe von Implementierungen dieses Interfaces können streamba-

sierte Ende-zu-Ende Verbindungen zwischen zwei Geräten hergestellt werden. Die Klasse BluetoothStreamStub öffnet und schließt daher die Verbindungen zu anderen Geräten per Bluetooth.

- *StreamConnection*: Das Shark Framework definiert mit dem Interface StreamConnection das Verhalten einer streambasierten Verbindung zweier Geräte. Dieses Interface ist nicht zu verwechseln mit gleichnamigen Interface von Java ME. Klassen wie *BluetoothConnection*, welche dieses Interface implementieren, bauen in ihren jeweiligen Konstruktur die Verbindung mit ihrem jeweiligen Protokoll auf. In der Klasse *BluetoothConnection* erfolgt dies über das Bluetooth-Protokoll RFCOMM.

- *SharkServer*: Eine dieses Interface implementierende Klassen wartet bei der bestehenden Verbindung auf Datenpakete, nimmt diese an und leitet sie an einen *Request Handler* weiter. Die Klasse *BluetoothServer* nimmt daher die Datenpakete an, die per bestehender Bluetoothverbindung eintreffen.

4.3 Nutzung

4.3.1 Code

Der Code dieser Komponente kann hier `https://github.com/SharedKnowledge/SharkNet-Api-Android/tree/master/api/src/main/java/net/sharksystem/api/shark/protocols/bluetooth` betrachtet werden. Wie auch die anderen Implementierungen von Übertragungsprotokollen, befindet sich auch die Bluetooth-Implementierung im Projekt *SharkNet-Api-Android* im Package *protocols*.

4.3.2 Deployment / Runtime

4.4 Test

4.5 Ausblick

Es ist empfehlenswert, die von Android gestellten Bluetooth Klassen durch die dazu äquivalenten Bluetooth Low Energy (BLE) Klassen entweder zu ersetzen oder zumindest eine Alternative zu dem klassischen Bluetooth Package zu bieten. BLE verbraucht weniger Akkuleistung als das klassische Bluetooth, kann dafür aber nur eine geringere Menge an Daten pro Verbindung unterstützen. Da die mit SharkNet verschickten Nachrichten

auch trotz der semantischen Annotationen nur wenige Kilobyte benötigen, stellt dies für SharkNet kein Hindernis dar.

Kapitel 5

WiFi

5.1 Aufgabe der Komponente

Über die WiFi-Direct Komponente vermitteln die Peers ihre Kontaktdaten an alle verfügbaren Peers in der Nähe. Dies geschieht über den Expose Befehl des ASIP Protokolls, bei dem ein ASIP-Interesse an die Wissensbasis von anderen Peers gesandt wird. Dies beinhaltet unter anderem die Bluetooth MAC-Adresse, mit der dem Peer dann anschließend Nachrichten per Bluetooth geschickt werden können. Das Verschicken der Bluetooth Mac-Adresse via WiFi-Direct ermöglicht es daher, dass für die darauf folgende Bluetooth-Verbindung kein Pairing benötigt wird.
Die Komponente ist der elementare Bestandteil des Peer-Radars, der alle sich in der Nähe befindlichen Peers anzeigt und die Kommunikation mit diesen erlaubt. Das Radar ist wiederum dafür erforderlich, neue Chats mit Peers anzulegen oder einen semantischen Broadcast ohne Bluetooth-Pairing zu ermöglichen.

5.2 Architektur

5.2.1 Überlick

Im folgenden UML-Klassendiagramm sind alle Bestandteile der WiFi-Direct Komponente von SharkNet abgebildet.

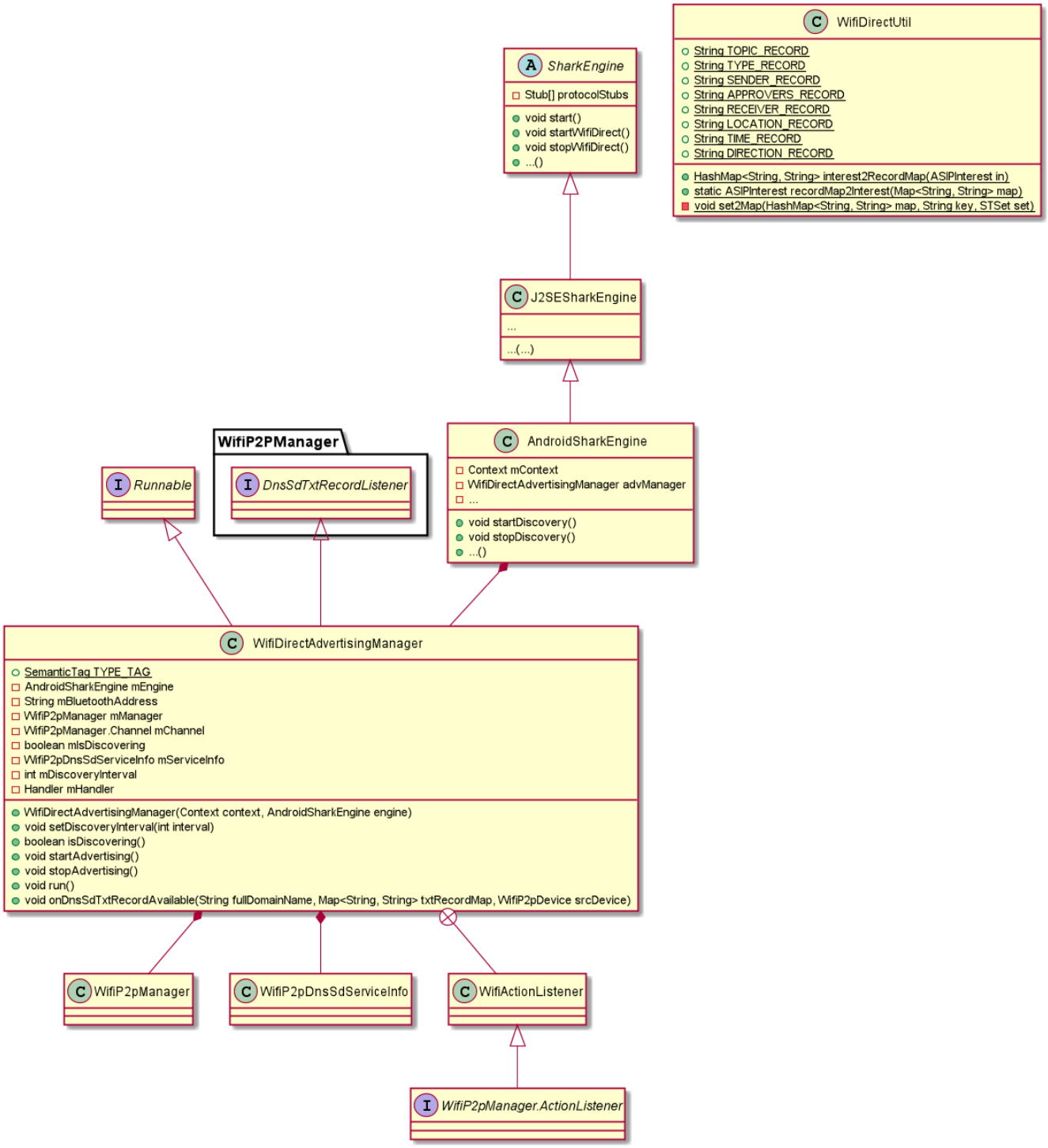

Abbildung 5.1: Die WiFi-Direct Klassen im Überblick

Im Zentrum dieser Hierarchie steht die Klasse *WiFiDirectAdvertisingManager*. Eine Instanz dieser Klasse befindet sich als Attribut in der Klasse *AndroidSharkEngine*, von der aus alle Protokolle wie NFC, Wifi-Direct oder Bluetooth gesteuert werden. Über die Engine kann daher auch das Radar per *startDiscovery()* Methode gestartet oder über

die *stopDiscovery()* Methode beendet werden. Das Starten oder Stoppen der kompletten WiFi-Komponente erfolgt dagegen in der Klasse *SharkEngine*, die den Ausgangspunkt der Vererbungshierarchie darstellt.
Die Klasse *WifiDirectUtil* bietet statische Methoden an, mit denen ASIP-Interessen in Hashmaps umgewandelt werden können und umgekehrt. Dies ist notwendig, da die von Android gestellte Basisklasse *WifiP2PManager* bei der Anmeldungen von Services keine ASIP-Interessen, sondern Hashmaps als Parameter akzeptiert.

5.2.2 Schnittstellendefinitionen

Wie im vorherigen Unterkapitel erläutert liefern die beiden Methoden *startDiscovery()* und *stopDiscovery()* die Funktionalität, um Peers zu finden und andere Peers über das eigene Interesse in Kenntnis zu setzen.
Bei Aufruf der *startDiscovery()* Methode wird innerhalb der Engine ein neuer *WifiDirectAdvertisingManager* angelegt und anschließend dessen *startAdvertising()* Methode aufgerufen. Innerhalb der *startAdvertising()* Methode wird sich nun auf der dritten Schicht des OSI-Modells begeben, wie der folgende Codeausschnitt zeigt:

Listing 5.1: Peer Semantic Tag

```
1 HashMap<String, String> map = WifiDirectUtil.interest2RecordMap(
      interest);
2 mServiceInfo = WifiP2pDnsSdServiceInfo.newInstance("_sbc", "_presence
      ._tcp", map);
3 mManager.addLocalService(mChannel, mServiceInfo, new
      WifiActionListener("Add_LocalService"));
4 mManager.clearServiceRequests(mChannel, new WifiActionListener("Clear
      _ServiceRequests"));
5 WifiP2pDnsSdServiceRequest wifiP2pDnsSdServiceRequest =
      WifiP2pDnsSdServiceRequest.newInstance();
6 mManager.addServiceRequest(mChannel, wifiP2pDnsSdServiceRequest, new
      WifiActionListener("Add_ServiceRequest"));
```

Nachdem in der erste Zeile eine Hashmap auf dem Interesse erzeugt worden ist, wird diese Hashmap in Zeile zwei als Parameter für die Erzeugung einer Service Information benutzt. Anschließend wird dem *WifiP2PManager* ein neuer lokaler Service hinzugefügt, wobei dieser Service die zuvor erzeugte Service Information enthält. Nachdem etwaige vorherige Service Requests beseitigt worden sind, wird der neue WifiP2P Service Request hinzugefügt. Dadurch wird nun an alle Geräte in der Nähe, die auf WifiP2P Service Requests warten, dieser zur Verfügung gestellt.

Neben dem Hinzufügen von Services, müssen diese aber auch empfangen und ausgewertet werden. Dies ist der Grund, warum der *WifiDirectAdvertisingManager* das Interface *Runnable* implementiert. In der dadurch implementierten Methode *run()* werden die von anderen Geräten gesendeten Service Requests empfangen.

Listing 5.2: Peer Semantic Tag

```
1 mManager.discoverServices(mChannel, new WifiActionListener("Discover␣
    Services"));
2 mHandler.postDelayed(this, mDiscoveryInterval);
```

Sollte ein Service gefunden und erfolgreich eine Peer-To-Peer Verbindung zwischen zwei Geräten aufgebaut werden können, wird nun die aus Listing x.x bekannte Hashmap an das Gerät gesendet, welches den Service gefunden (discovered) hat. Dabei wird automatisch die Methode *onDnsSdTxtRecordAvailable* aufgerufen, welche die empfangene Hashmap in ein ASIP-Interesse umwandelt und dann der Engine weiterreicht.

Listing 5.3: Peer Semantic Tag

```
1 ASIPInterest interest = WifiDirectUtil.recordMap2Interest(
    txtRecordMap);
2 mEngine.handleASIPInterest(interest);
```

5.3 Nutzung

5.3.1 Code

Der Code dieser Komponente kann hier `https://github.com/SharedKnowledge/SharkNet-Api-Android/tree/master/api/src/main/java/net/sharksystem/api/shark/protocols/wifidirect` betrachtet werden. Wie auch die anderen Implementierungen von Übertragungsprotokollen, befindet sich auch die WiFi-Direct-Implementierung im Projekt *SharkNet-Api-Android* im Package *protocols*.

5.3.2 Deployment / Runtime

5.4 Test

5.5 Ausblick

Kapitel 6

Broadcast

6.1 Aufgabe der Komponente

Die Broadcast Komponente ermöglicht es den Benutzern von SharkNet, Nachrichten an andere Benutzer zu schicken. Dabei können auch andere Komponenten, wie etwa der semantische Eingans- und Ausgangsfilter zum Einsatz kommen, was jedoch nicht zwingend erforderlich ist. Falls auf einen Eingangsfilter oder Ausgangsfilter verzichtet werden sollte, werden wie bei einem klassischen Broadcast die Nachrichten an alle sich in der Nähe befindlichen Geräte versendet. Inwiefern der klassische Broadcast vom Benutzer semantisch eingeschränkt werden kann, lässt sich in der Komponentenbeschreibung der Komponente Semantischer Filter in Erfahrung bringen.

6.2 Architektur

6.2.1 Überlick

Die folgenden Komponenten werden von der Komponente Broadcast zwingend benötigt:

- WifI
- Bluetooth
- Persistenz

Optional sind hingegen die Komponenten:

- Semantischer Filter

6.2.2 Überlick

Die Komponente bildet sich vorrangig aus sieben Klassen, wovon drei sich innerhalb des SharkFrameworks und vier sich innerhalb der App befinden. Diese sieben Klassen werden nun ausgehend von der folgenden Abbildung kurz beschrieben.

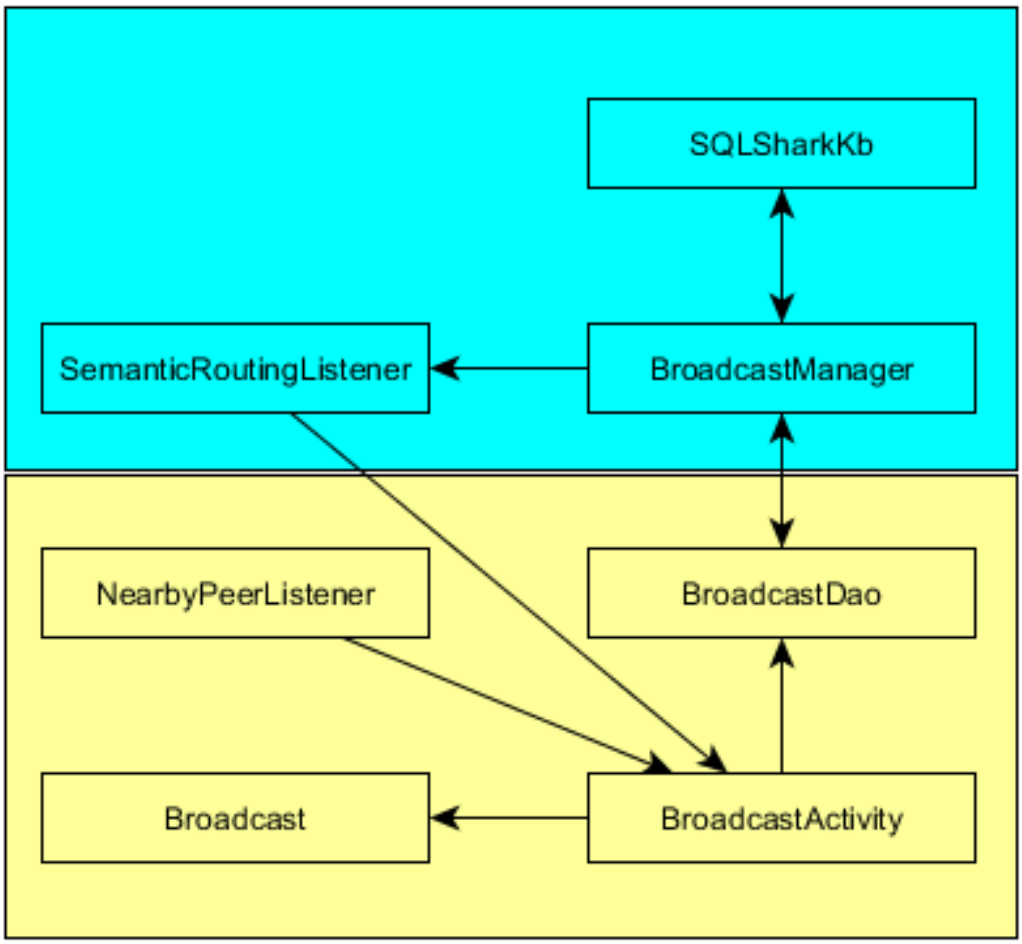

Abbildung 6.1: Die Klassen der Broadcast Komponente

- Die SQLSharkKb ist eine Implementierung der Shark Knowledgebase mit SQLite. Mit ihr werden sämtliche Daten wie bsp. die Nachrichten, semnatische Annotationen oder auch Benutzerprofile gespeichert. Sie nimmt ausschließlich Anfragen von Klassen aus dem SharkFramework entgegen.

- Der BroadcastManager ist die direkte Schnittstelle zwischen dem Framework und der App. Er nimmt Broadcast-Objekte vom BroadcastDao entgegen und lässt diese gegebenfalls von der SQLSharkKb speichern. Sollte eine neue Nachricht den Peer

erreichen, wird vom BroadcastManager die Nachricht auf ihre semantische Relevanz hin überprüft und im Erfolgsfall der Wissenbasis des Peers hinzugefügt.

- Der SemanticRoutingListener liefert neue vom BroadcastManager akzeptierte Nachrichten an die BroadcastActivity

- Der BroadcastDao nimmmt von der BroadcastActivity veränderte Nachrichten in Form eines Objekts vom Typ Broadcast entgegen, baut diese in für das Shark-Framework vewertbare Objekte vom Typ ASIPSpace um und leitet diese an den BroadcastManager weiter.

- Wann immer die Anzahl der sich in Reichweite befindlichen Peers ändert, wird die BroadcastActivity vom NearbyPeerListener mit einer angepassten Liste von Peers versorgt.

- Die BroadcastActivity ist die Schnittstelle zwischen Benutzer und App. Sie nimmt neue Nachrichten vom Benutzer entgegen, wobei das Hinzufügen von semantischen Annotationen optional ist. Sie benutzt die Entitätsklasse Broadcast um die Nachrichten in einer Klasse zu bündeln, welche bei Aktualisierungen an das BroadcastDao weitergereicht wird.

6.2.3 Schnittstellendefinitionen

6.3 Nutzung

Die Komponente ist in der App innerhalb der *BroadcastActivity* eingebunden. Der Endanwender kann über die diese Activity und die dazugehörige XML-Datei die Nachrichten versenden, betrachten und mit semantischen Annotationen versehen, wobei Letzteres auch die Komponente Semantische Filter betrifft.
Die Komponente kann aber auch in eigenen Activities benutzt werden ohne die vorgegebene *BroadcastActivity* benutzen zu müssen. Der Entwickler muss bei seiner eigenen Activity dafür lediglich von der Klasse *BaseActivity* erben. Die Klasse *BaseActivity* stellt das Attribut *mApi* vom Typ *SharkNetApi* bereit, mit dem durch die Methoden *getBroadcast()* und *updateBoradcast(...)* der Broadcast geliefert und verändert werden kann.

6.3.1 Code

Der Code dieser Komponente kann hier `https://github.com/SharedKnowledge/SharkNet/tree/master/app/src/main/java/net/sharksystem/sharknet` betrachtet werden.

6.3.2 Deployment / Runtime

...

6.4 Test

6.5 Ausblick

Der Austausch von Nachrichten mit mehreren Geräten in der Nähe funktioniert grundlegend sicher, aber noch nicht komplett fehlerlos. So kann es bei hoher Last seitens der Benutzer passieren, dass einige Nachrichten nicht empfangen werden können, obwohl sie gemäß dem eingestellten semantischen Filter akzeptiert werden müssten.

Kapitel 7

Semantischer Filter

7.1 Aufgabe der Komponente

Über den Broadcast erhält der Benutzer eine Vielzahl an Nachrichten von anderen Benutzern, von denen einen Großteil für ihn irrelevant sind. Der Semantische Filter ist dafür verantwortlich, dem Benutzer nur die für ihn interessante Nachrichten zu akzeptieren und in seine Wissensbasis einfließen zu lassen. Er ist damit neben dem Broadcast die wichtigste Komponente dieser Arbeit. Neben dem bereits beschriebenen Eingangsfilter gibt es noch einen Ausgangsfilter, der für die etwaige Weiterleitung von Nachrichten an andere Peers verantwortlich ist.
Die Benutzer können ihre Filter über ein Menü innerhalb des Profilbereichs einstellen, wobei dies keine Pflicht ist. Wenn keine Filter gesetzt sind, werden alle Nachrichten akzeptiert und weitergeleitet, sofern diese nicht bereits zuvor empfangen worden sind.

7.2 Architektur

7.2.1 Überlick

Der semantische Filter gliedert sich in verschiedene Teilfilter, diese Trennung richtet sich nach den bereits bekannten Dimensionen des Shark Frameworks. Um den Gesamtfilter mit den kleineren Teilfiltern dynamisch zusammensetzen zu können, wurde das Entwurfsmuster Kompositum gewählt. Mit Hilfe dieses Musters müssen nur jeweils die Teilfilter gesetzt werden, die für den Benutzer auch eine Relevanz haben. Die folgende Klassenhierarchie verdeutlicht dieses Verhältnis:

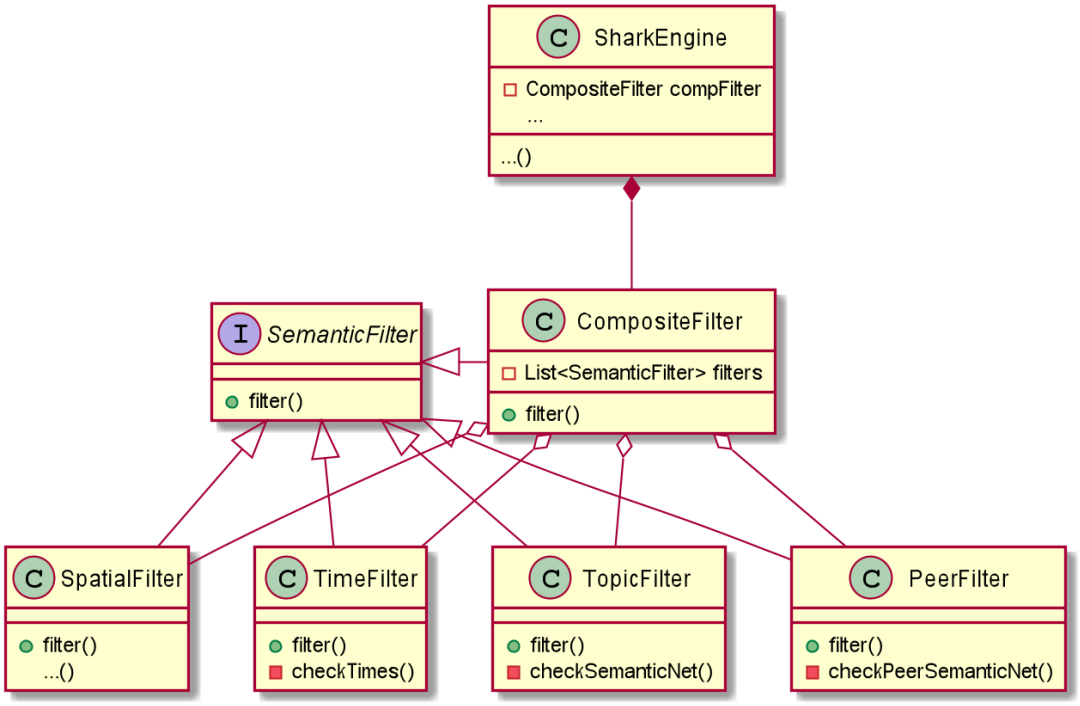

Abbildung 7.1: Klassenhierarchie des semantischen Filters (Auszug)

- Die *SharkEngine* enthält das Kompositum und stellt Methoden zur Erzeugung und Anpassung dafür bereit. Weiterhin ist diese Klasse von der App aus erreichbar, wodurch über die App abhangig von den Eingaben des Benutzers die Filter gesetzt oder entfernt werden können.

- Das Interface *SemanticFilter* wird von allen Teilfilterklassen und der Kompositumsklasse implementiert. Die einzige zu implementierende Methode ist dabei die Filtermethode, die einen booleschen Wert zurückliefert.

- Der *CompositeFilter* besitzt eine Liste aus allen Teilfiltern, ermöglicht durch Polymorphismus. Bei Aufruf der Filtermethode werden sämtliche Teilfilter angewandt, die sich in der Liste befinden. Näheres dazu befindet sich im Unterkapitel 7.3.1 Code.

- Die Relevanz der Themen werden durch den *TopicFilter* geprüft. Der Filter kann für die beiden Dimensionen Topics und Types verwendet werden.

- Die Dimensionen Sender, Approvers und Receivers werden durch den PeerFilter abgedeckt. Da die Dimension Sender in Gegensatz zu Approvers und Receivers nur ein SemanticTag, jedoch kein SemanticNet enthält, findet eine Fallunterscheidung am Anfang der Methode statt.

- Der *TimeFilter* kontrolliert, ob sich mindestens einer der Zeiträume, die sich im semantischen Profil und in der empfangenen Nachricht befinden, überschneiden.

- Die spatiale Auswertung findet im *SpatialFilter* statt, sie wird im Rahmen einer Bachelorarbeit von Maximilian Öhme entwickelt.

7.2.2 Code

Wie bereits im Überblick angerissen, führt der *CompositeFilter* keine eigene semantische Filterung durch, sondern lässt dies fachgerecht von den Teilfiltern ausführen. Im folgenden Codeausschnitt ist erkennbar, dass der sequentielle Aufruf der Teilfilter sofort abgebrochen wird, wenn ein Teilfilter ein *false* liefert.

Listing 7.1: Filtermethode im Kompositum

```
1  boolean isInteresing = true;
2  int i = 0;
3  while (isInteresing && i < childFilters.size()) {
4  isInteresing =  childFilters.get(i).filter(message, newKnowledge,
       entryProfile);
5  i++; }
6  return isInteresing;
```

Angenommen es handelt sich bei der ersten Iteration der Schleife um eine Instanz der Klasse *TopicFilter*, welche ihre Filtermethode aufruft, dann würde es zunächst zur folgenden Auswertung kommen:

Listing 7.2: Filtermethode des TopicType Filters (Auszug)

```
1  if (activeEntryProfile == null) return true;
2  switch (dimension){
3    case TOPIC:
4      if (activeEntryProfile.getTopics() instanceof SemanticNet) {
5            isInteresting = checkSemanticNet(activeEntryProfile.
                 getTopics(), newKnowledge);
6          }
7          else {
8            isInteresting = checkSemanticTag(newKnowledge,
                 activeEntryProfile);
9      }
10 break;
```

Es wird zunächst wie auch bei allen anderen Teilfiltern überprüft, ob überhaupt ein semantisches Profil vom Benutzer gesetzt worden ist. Falls nicht, wird die Auswertung sofort mit einem *true* als Rückgabewert beendet. Es wird nun wie auch beim *PeerFilter* Überprüft, um welche Dimension es sich bei der Filterauswertung handelt. In Zeile vier von Listing 7.2 wird überprüft, ob es sich nur um ein einzelnes Tag oder um ein gesamtes SemanticNet handelt. Dadurch wird der Besonderheit in Shark Rechnung getragen, dass eine Dimension entweder durch ein einzelnes Tag oder durch ein komplettes Semantisches Netz beschrieben werden kann. Der folgende Auszug zeigt die Auswertung eines Semantischen Netzes:

Listing 7.3: Auswertung des Semantischen Netzes (Auszug)

```
1 SemanticNet resultNet = SharkCSAlgebra.contextualize(inputNet,
    profileSet, fp);
2         if (resultNet == null || resultNet.isEmpty()) {
3                 return false;
4         }
5         else {
6                 return true;
7         }
```

Für die Auswertung wird die vom SharkFramework bereitgestellte Funktionalität der Kontextualisierung von Semantischen Netzen benutzt. Die in Zeile dafür aufgerufene Methode benötigt dabei drei Parameter. Diese umfassen das Semantische Netz des Benutzerprofils und das Semantische Netz der Nachricht innerhalb dessen zugeordneten Dimensionen, sowie die Fragmentierungsparameter der Kontextualisierung.

7.2.3 Schnittstellendefinitionen

7.3 Nutzung

7.4 Test

7.5 Ausblick

Kapitel 8

Sonstiges

In der folgenden Grafik sind alle Bestandteile der WifiDirect Komponente von SharkNet abgebildet.

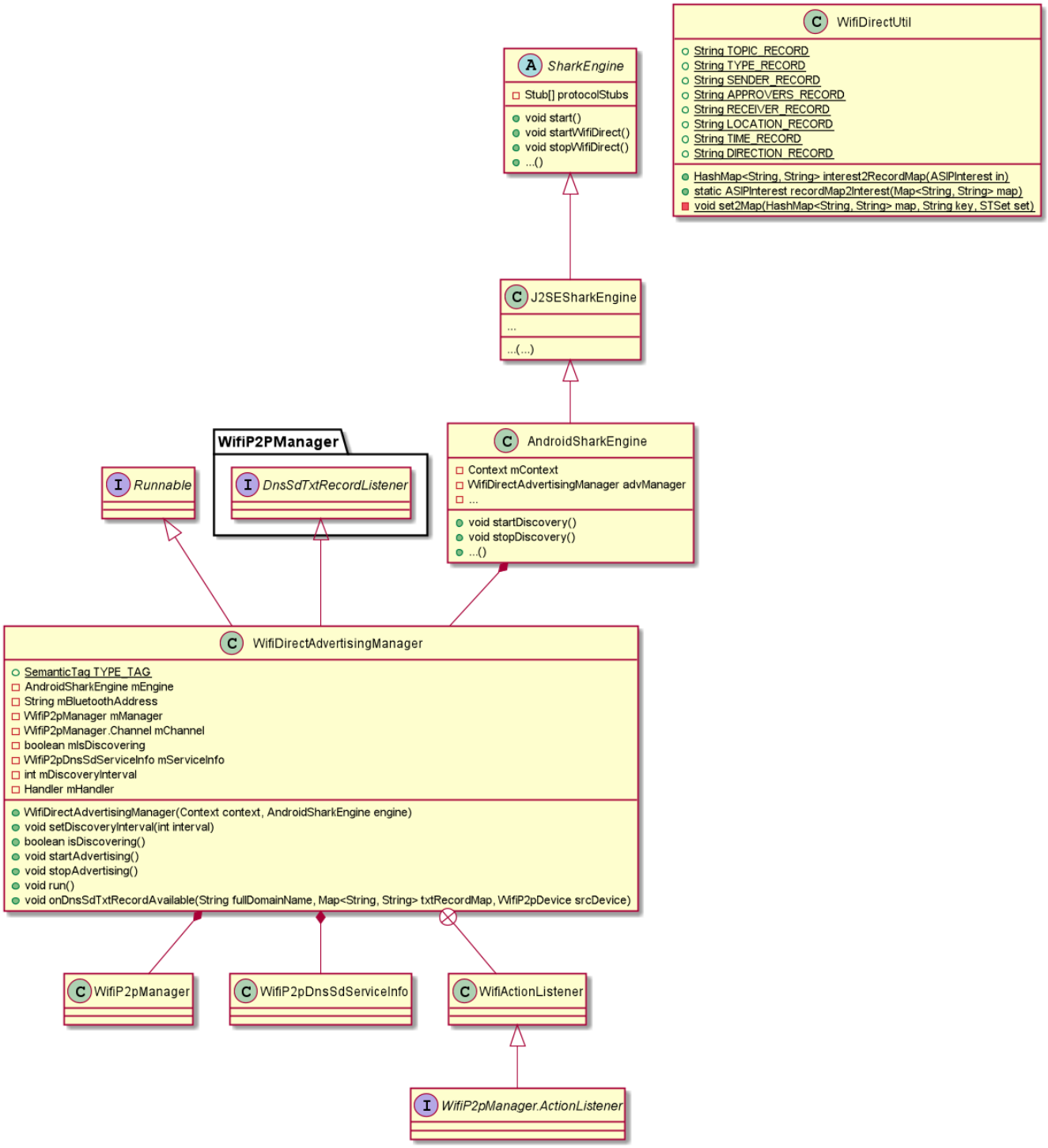

Abbildung 8.1: Die WifiDirect Klassen im Überblick

In der folgenden Grafik sind alle Bestandteile der Radar Komponente abgebildet.

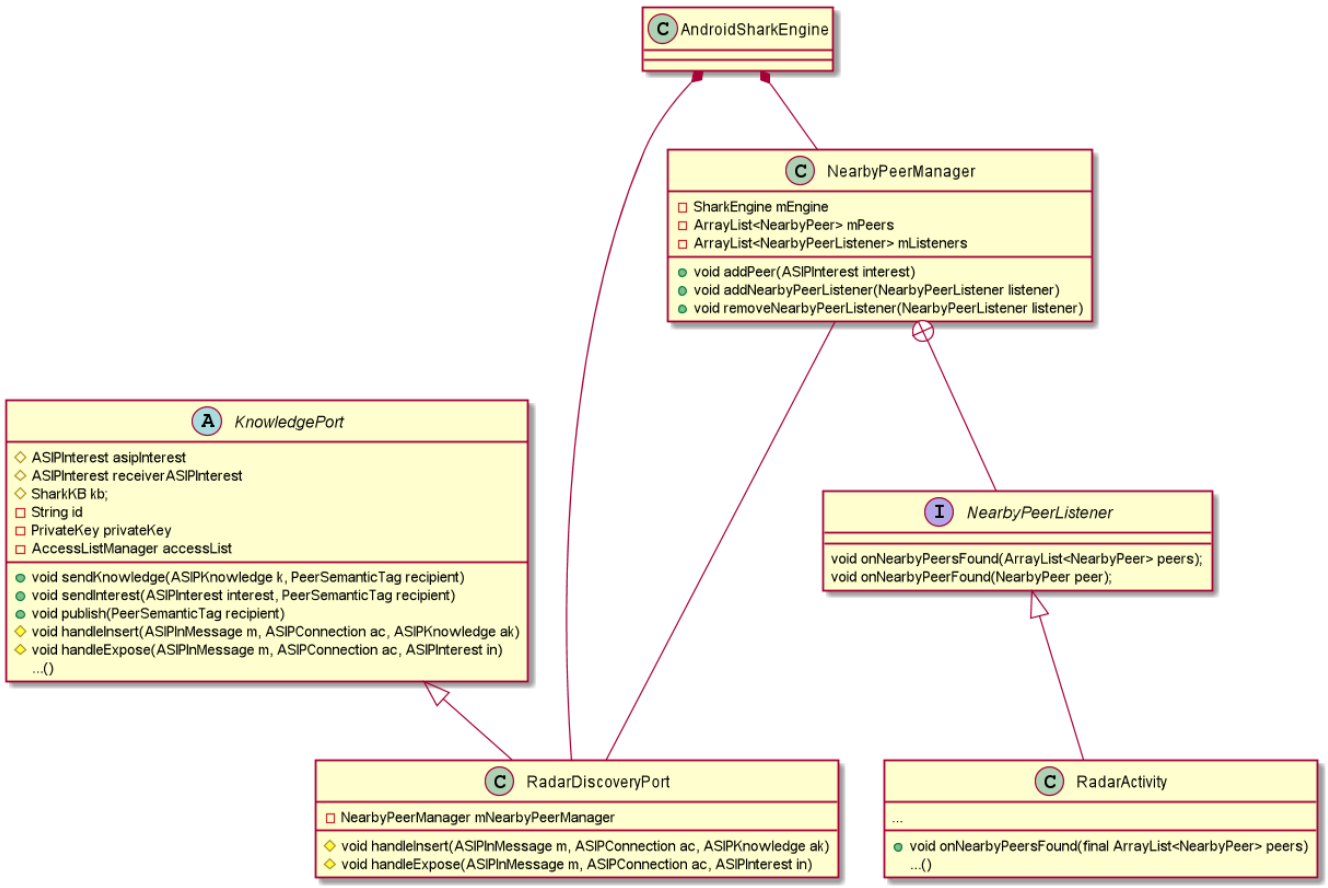

Abbildung 8.2: Die Radar Klassen im Überblick

Im folgenden Aktivitätsdiagramm wird das Versenden von Nachrichten per Broadcast abgebildet

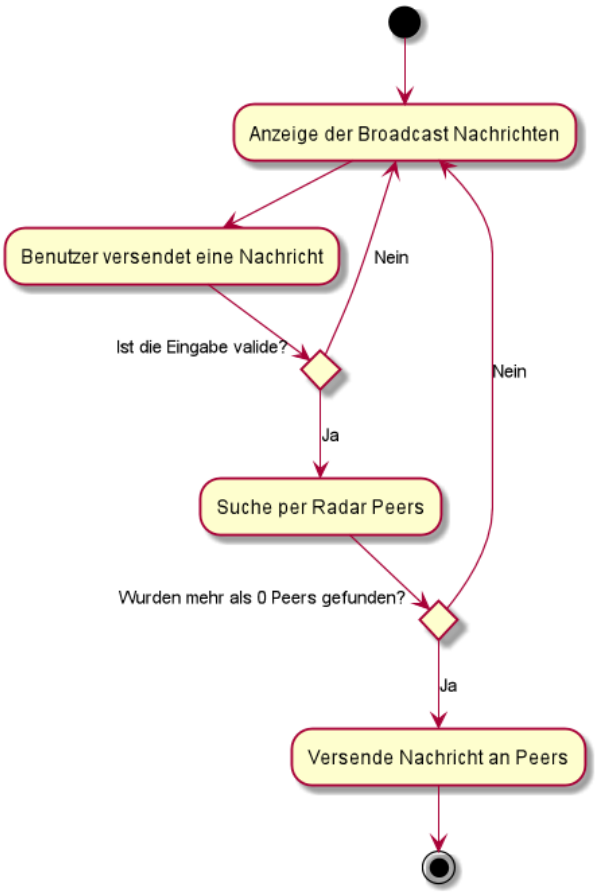

Abbildung 8.3: Versenden von Nachrichten per Broadcast in SharkNet

Im folgenden Aktivitätsdiagramm wird das Empfangen von Nachrichten per Broadcast abgebildet

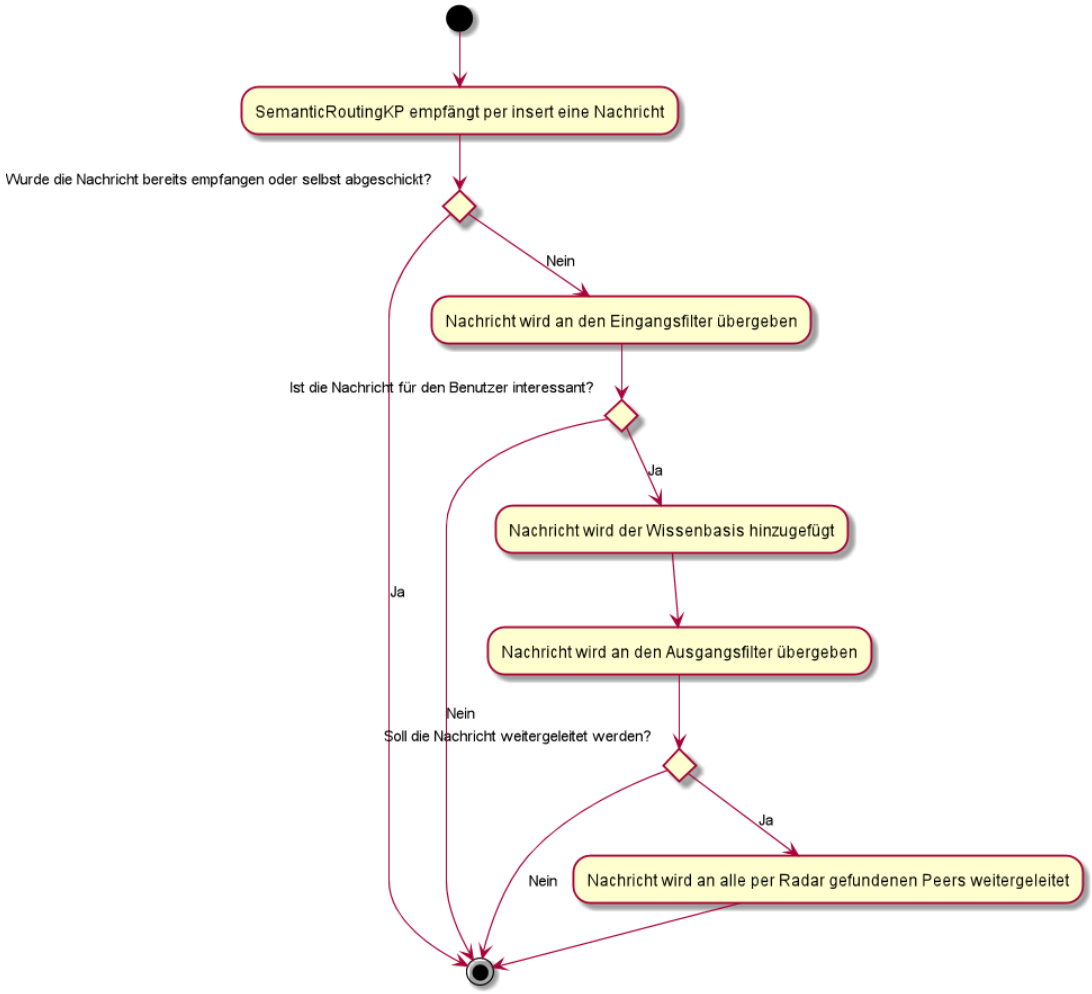

Abbildung 8.4: Empfangen von Nachrichten per Broadcast in SharkNet

Im folgenden Aktivitätsdiagramm wird Filterung von Nachrichten per Eingangsfilter abgebildet

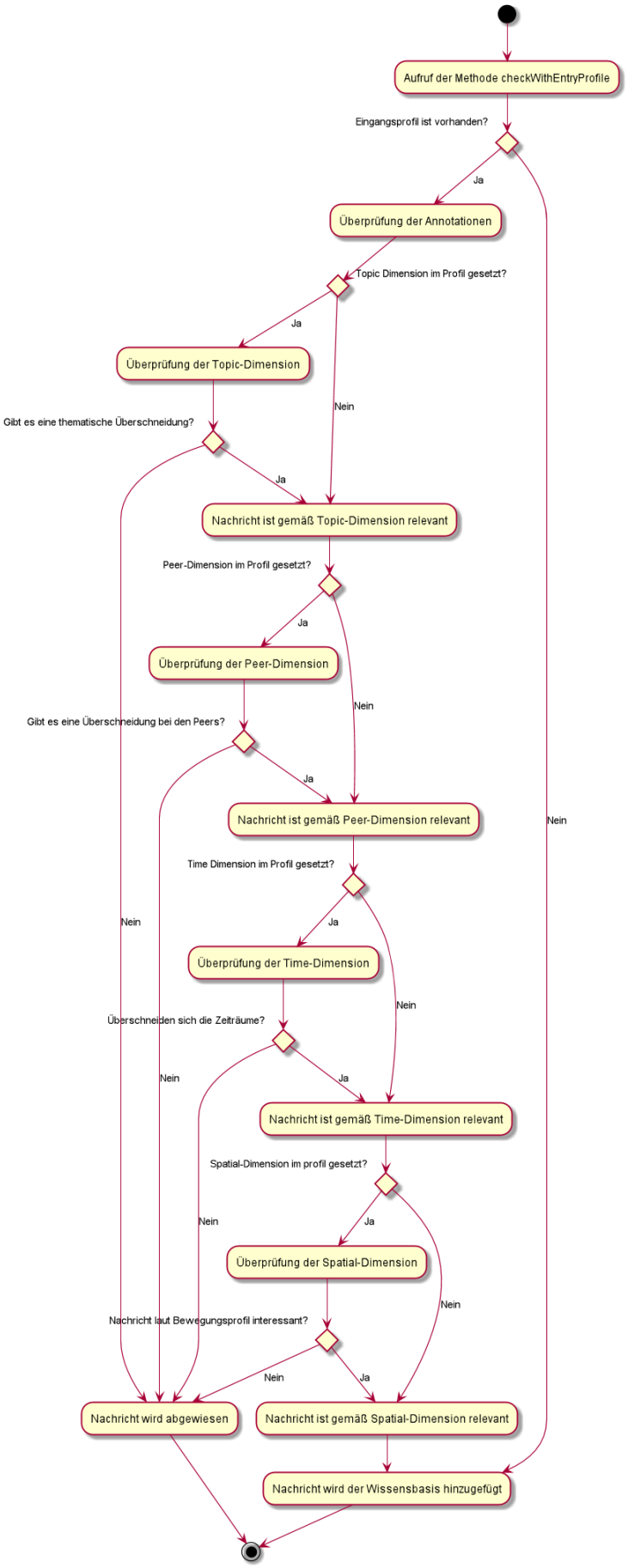

Abbildung 8.5: Filterung von Nachrichten per Eingangsfilter in SharkNet

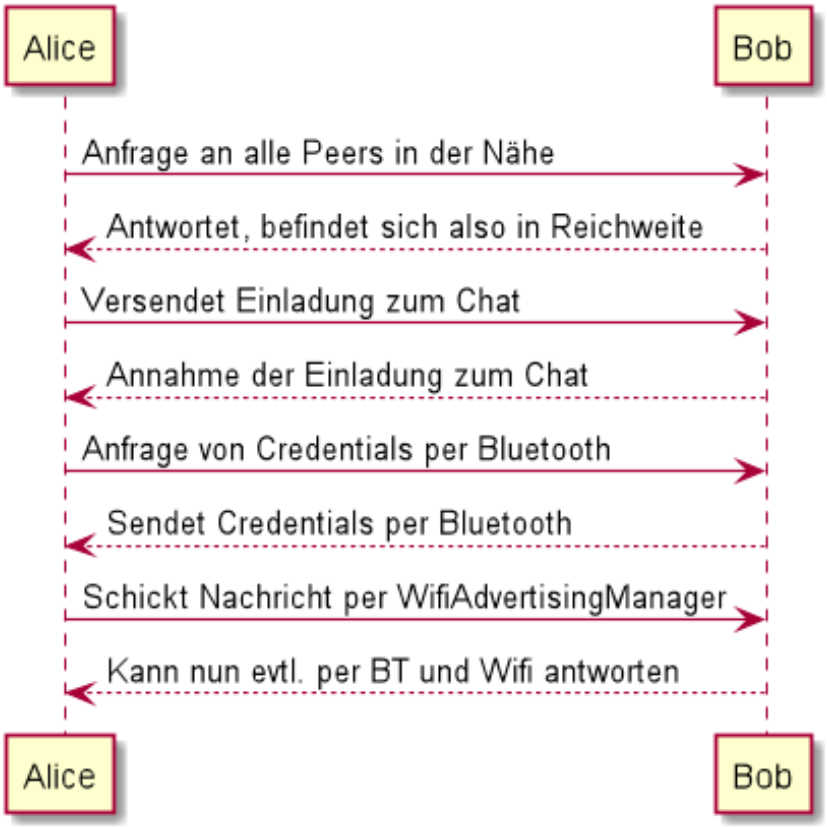

Abbildung 8.6: Kommunikation per Chat