P2P and Grid Computing
- Exercise 12 -
- C110 -

Michael Scholz (Matr. 1576630)
Ulf Gebhardt (Matr. 1574373)

H 12.1:

a)
Ein OSN ist eine Platform, die es Personen erlaubt eigene Profile zu erstellen und somit Informationen über sich selbst preiszugeben. Hierbei kann man teilweise zwischen professionellen und privaten Profilen unterscheiden. Nutzer können weiter mit anderen Nutzern in Kontakt bleiben und Daten austauschen. Sie können teils öffentliche, teils private Nachrichten schreiben und ihre Interessen äußern. Durch Funktionen wie Like-Buttons und Smileys können Zustimmung bzw. Abneigung gegenüber veröffentlichten „Posts“ dargestellt werden. Weiter versuchen die Online Network Provider immer mehr Funktionen in ihr Angebot zu integrieren. So sind heute meist schon Videotelefonie (teils sogar mit mehreren Teinehmern), Nachrichtenaustausch, Dateiaustausch und viele weitere Funktionen in den Online Social Networks integriert.

b)
Die OSN Stackholder wollen aus den sozialen Netzwerken eigenen Profit ziehen. So haben die Nutzer meist das Interesse Kontakte zu anderen Nutzern in dem Netzwerk aufzubauen oder zu pflegen, oder Ihre Meinung zu einem Thema innerhalb des Netzwerks kund zu tun.
Der Betreiber des OSN und Firmen, welche mit diesem kooperieren, möchten möglichst viel Gewinn erzielen. So geht es meist um Nutzerdaten bzw. Nutzerverhalten. Betrachetet man beispielsweise Facebook, so wird hier versucht gezielte, nutzer-spezifische Werbung zu plazieren, welche den potentiellen Kunden ansprechen könnte, da seine Nutzung des OSN dem Betreiber des OSN Aufschluss auf des Nutzers Interessen gibt. Zudem hat Facebook mit dem „App-Store“ im sozialen Netzwerk eine weitere Möglichkeit geschaffen auch externe Firmen vom sozialen Netzwerk profitieren zu lassen. Die meisten angebotenen Applikationen benötigen eine Erlaubnis auf die Nutzerdaten zugreifen zu dürfen. Somit gelangen die durch Facebook gesammelten Daten der Nutzer auch an Dritte, die hieraus ihren Nutzen ziehen können. Facebook steigert durch die Applikationen für viele Nutzer die Attraktivität der Platform. So steigen unter anderem die Besuchszeiten. Viele Fachleute sind sich sicher, dass die Betreiber der sozialen Netzwerken darüber hinaus sogar Nutzerdaten an Dritte verkaufen. Dies wird von den Verantwortlichen jedoch immer wieder dementiert.

Betrachtet man also abschließend die Provider der online social networks und die einzelnen stackholder, so handelt es sich um eine klare Win-Win-Situation. Der einzige Verlierer ist meist der Nutzer.

H 12.2:

(i)
Die vorgestellten DHTs stellen keine Anonymität des „reponders“ sicher. Betrachet man beispielsweise Chord, so kann ein Angreifer durch verfolgen der Finger-Tabellen die Netzwerkstruktur herausfinden. Um antwortende Peers anonym zu halten, gibt es eine Erweiterung von Chord, das so genannte „k-anonymity Chord“ [1]. Hierbei ist ein Peer unter k anderen Peers anonym. Hierbei werden die Suchqueries abgeändert.

[1] Ahmet Burak Can, Bharat Bhargava, „Anonymous Access to Trust Information Using k-anonymity Chord“, 2010

(ii)
Für File-sharing bieten sich DHTs an, da ein Hash einen Dateiinhalt identifizieren kann und somit ein DHT Aufschluss über den verfügbaren Inhalt im Netzwerk/auf den einzelnen Clients giben kann. Die meisten Implementierungen von DHTs unterstützen Filesharing oder wurden für Filesharing entwickelt. Vgl.

Kadmelia, welches zwar keine direkte Möglichkeit liefert Dateien auszutauschen, aber welches in prominenten Filesharing Tools(z.B. eDonkey) zum Einsatz kommt um Dateiinhalte im Netzwerk zu lokaliesieren. Ein zweites Protokoll ist dann für den eigentlichen Dateitransfer zuständig.

(iii)
Hierfür bieten sich DHTs nicht perse an. Einzelne Peers könnten in ihren Tabellen Inhalte entfernen bzw. „Blackholes“ erschaffen, indem sie ungültige Einträge hinzufügen oder auch gültige Einträge verfälschen. Allerdings ist ein verteiltes System immer schwerer zu kontrollieren oder abzuschalten, als ein dezentralisiertes.

(iv)
Bei instant messaging können durchaus DHTs eingesetzt werden. Allerdings ist das eher selten der Fall. Bei instant messaging wird bei den größeren Anbietern bisweilen immer noch auf eine Client/Server Lösung gesetzt. Vgl. ICQ, MSN.
Instant messaging ist z.B. in RetroShare mithilfe von DHTs realisiert.

(v)
Bei großen verteilten Datenbanken kommen DHTs beim sogenannten Database Sharding oft zum Einsatz. Database Sharding verteilt eine Datenbank auf mehrere Server. DHTs dienen dann zum Auffinden von Daten innerhalb dieses Datenbank-Server-Netzwerkes. Vgl MySQL Cluster.

(vi)
Bei wireless Sensornetzwerken bieten sich DHTs nicht an. Verteilte Hashtabellen erzeugen im Vergleich mit einer zentralisierten Hashtabelle sehr viel Traffic. Bei wireless Sensornetzwerken sollte man diesen jedoch so gering wie möglich halten, da die Sensoren meist mit Akkus ausgestattet sind und somit „unnötiger“ Traffic eingespart werden soll. Somit erhält man eine längere Akkulaufzeit der einzelnen Sensoren.