Mobiler Friend Finder

Patrick Hornecker

Universität Freiburg

4. März 2010

Überblick

- *Location privacy*
- Aktuelle Entwicklungen
- Ziele
- Genutzte Verfahren
- Analyse
- Demonstartion von *Friend Finder*

Location privacy

- Definition von *location privacy* durch Duckham und Kulik (2006)

  > *"... a special type of information privacy which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others."*

- Bei Verbreitung der Positionsdaten sollte durch den Anwender bestimmbar sein:
  - Zu welchem Zeitpunkt die Daten versendet werden
  - Wie die Positionsdaten versendet werden
  - In welchem Umfang die Positionsdaten versendet werden

Aktuelle Entwicklungen

- *Google Latitude*
  - Versenden der eigenen Positionen
  - Freunde können diese auf einer Karte sehen

Quelle: http://www.google.com/latitude

Aktuelle Entwicklungen

- Anwender kann den Zeitpunkt wählen, zu dem er die Positionsdaten versenden möchte
- Anbieter nutzt ein unbekanntes System um die Daten zu versenden
- Benutzer hat keine Einsicht in dieses System und kann somit Art der Verbreitung nicht kontrollieren
- Auch der Umfang der Verbreitung kann vom Benutzer nicht überblickt werden, da ihm die Einsicht in das System des Anbieters fehlt
- Es ergibt sich somit eine Informationsasymmetrie zwischen Anwender und Anbieter

Ziele

- Ziel ist ein Dienst mit welchem Anwender ihre Positionsdaten versenden können
- Dabei soll der Nutzer bestimmen können
  - Wann seine Daten versendet werden
  - Auf welche Art die Daten versandt werden
  - In welchem Umfang die Positionsdaten weitergegeben werden

Ziele

- Wann die Daten versendet werden
  - Der Nutzer soll den Zeitpunkt frei wählen können, wenn er seine Daten versenden möchte
  - Eine Sitzung soll ohne Vorplanung zu erstellen sein
- Auf welche Art die Daten versandt werden
  - Versenden der Daten durch transparente und verlässliche Struktur
- In welchem Umfang die Positionsdaten weitergegeben werden
  - Anwender kann bestimmen wer seine Positionsdaten einsehen darf

Genutzte Verfahren

- *IRC*-Protokoll um Daten zu versenden
  - *IRC* bietet ein offenes Netzwerk welches frei genutzt werden kann
- Symmetrisches Verfahren um Daten zu verschlüsseln
- 2D-Barcode um Schlüssel zu verteilen
  - 2D-Barcode kann aus Schlüssel erstellt werden
  - Andere Nutzer können diesen sofort in eine Zeichenkette umwandeln

Friend Finder

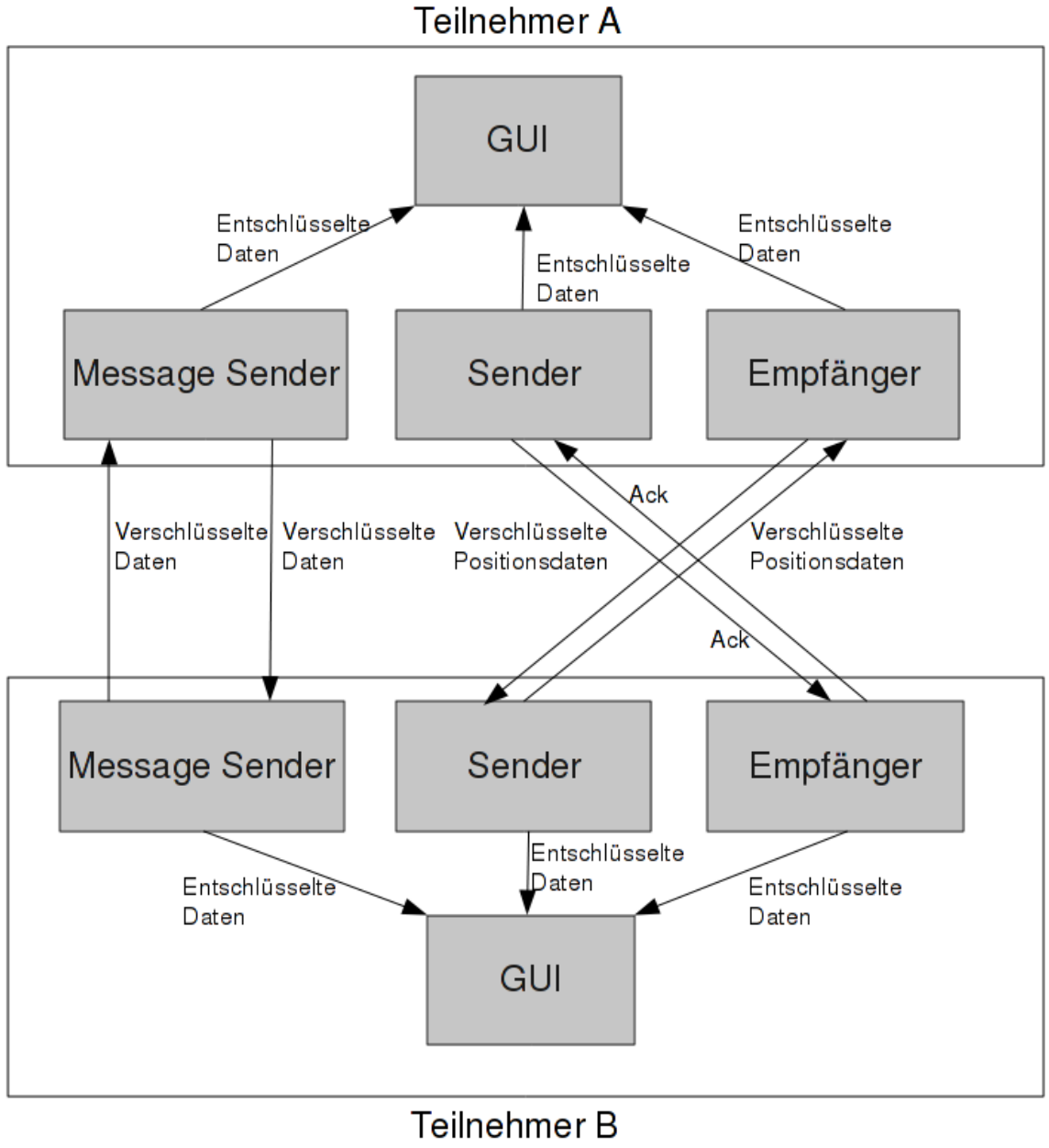
- Implementierte Software im Rahmen der Abschlussarbeit nennt sich *Friend Finder*
- Ist in der Lage Positionen und Textnachrichten im Bezug auf *location privacy* zu versenden
- 2D-Barcodes können aus Zeichenketten generiert werden

Friend Finder - Erstellen von 2D-Barcodes

- In *Friend Finder* können Barcodes aus Zeichenketten, die der Anwender eingibt, erstellt werden
- 2D-Barcodes könnten auch aus bereits generierten Schlüsseln erstellt werden

Quelle: *Friend Finder*

Friend Finder - Versenden und Empfangen von Daten



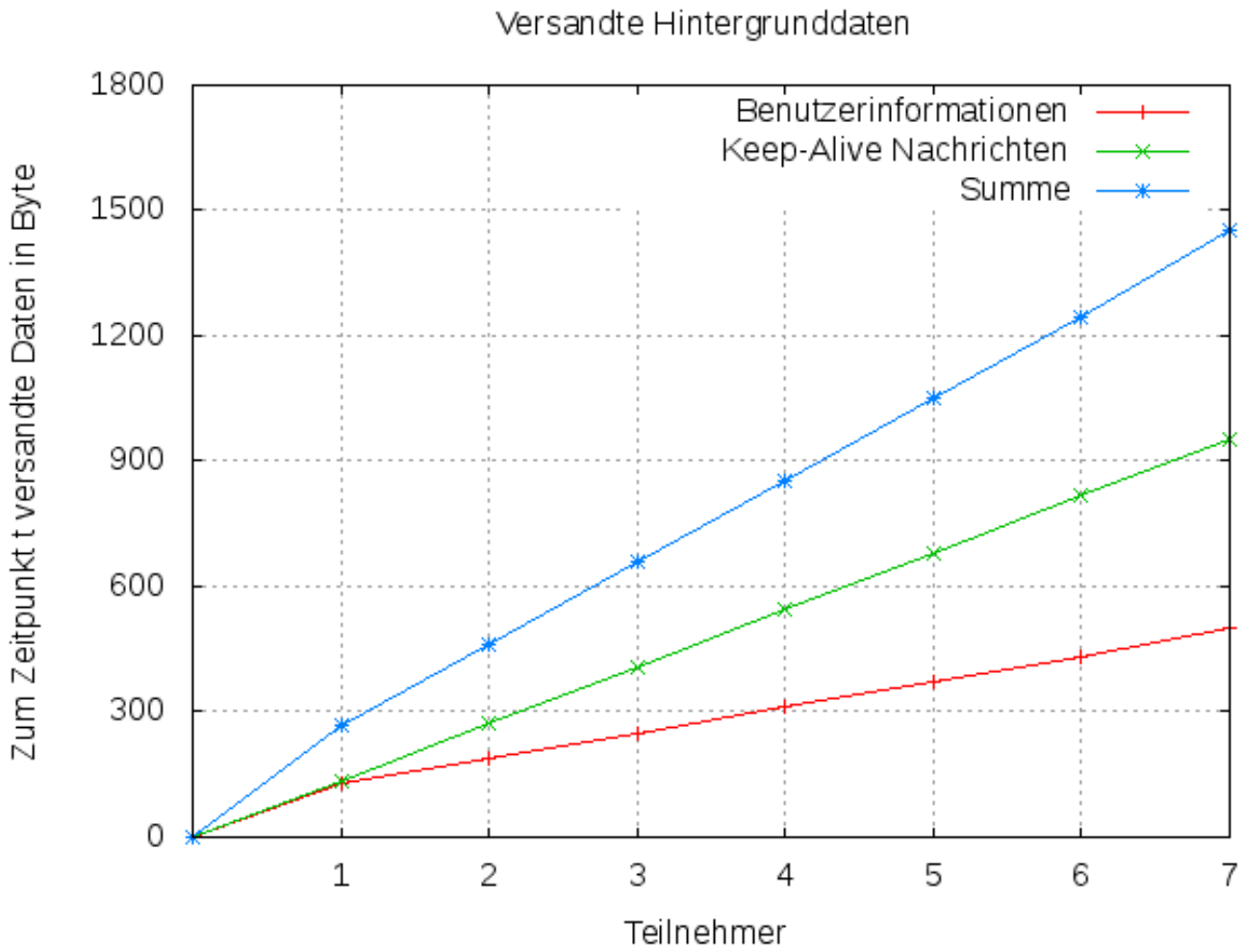
Friend Finder - Analyse

- *Datenoverhead* von *Friend Finder*
- *Friend Finder* im Vergleich zu n einzelnen Verbindungen
- Revidiert *Datenoverhead* den Vorteil eines *IRC-Channels* als *Broadcast*-Medium?

Friend Finder - Analyse: Allgemeiner Datenverkehr

- *Datenoverhead* in *Friend Finder* besteht aus Hintergrunddaten, welche nichts mit dem eigentlichen Dienst zu tun haben
- Alle 30 Sekunden werden zwischen Server und Client *Keep-Alive* Nachrichten ausgetauscht
- Alle 60 Sekunden erhält der Client, auf Nachfrage, Informationen über aktive Benutzer eines *Channels*

Friend Finder - Analyse: Allgemeiner Datenverkehr



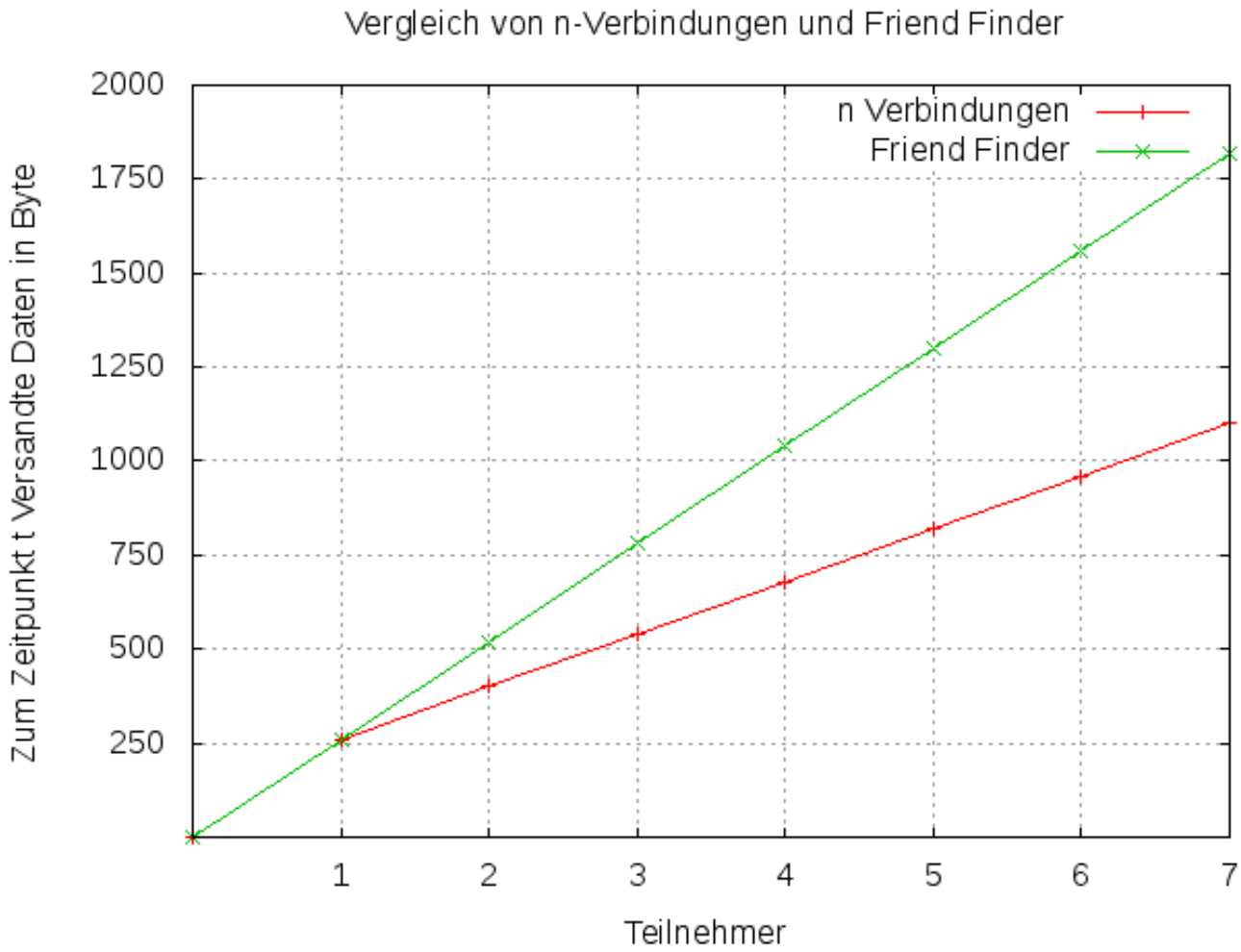
Friend Finder - Analyse: Versenden von Textnachrichten

- Beispielsatz “Hello World” wird in zwei Teile aufgeteilt
- Länge der Textnachricht in unverschlüsseltem Format: 24 Byte
- Textnachricht wird im Anschluss verschlüsselt sowie *Base64* kodiert
- Das *IRC*-Protokoll fügt noch Informationen bezüglich *Channel* und Benutzer hinzu
- Nach Verschlüsselung, *Base64*-Kodierung und Hinzufügen der Informationen hat werden insgesammt 99 Byte versendet
- Somit nimmt die Größe der Daten um Faktor vier zu

Friend Finder - Analyse: Versenden von Positionen

- Die größe eines *Latitude/Longtitude* Paares beträgt unverschlüsselt 32 Byte
- Nach Verschlüsselung, *Base64*-Kodierung sowie hinzufügen von Zusatzinformationen beträgt die Größe im Mittel 140 Byte
- Vergrößerung des Datenvolumens um circa Faktor vier
- Im Anschluss werden vier *Acknowledgements* mit Gesamtgröße 120 Byte versandt
- Datenverkehr pro Versendeter Position:
  $((h + (t \cdot 4)) + (4 \cdot a)) \cdot n$

Friend Finder - Versenden von Positionen



Fazit

- *IRC*-Protokoll gut geeignet für solche Dienste
  - Wenig *Datenoverhead*
  - Eignet sich sehr gut als *Broadcast*-Medium
- Mit Hilfe von 2D-Barcodes können Schlüssel einfach und ohne Vorarbeit weitergegeben werden