

Untersuchung und Implementierung des "Context as a key"-Verfahrens (Einzel- oder Teamarbeit)

Die Distributed an Ubiquitous (DUS) Forschungsgruppe arbeitet zusammen mit internationalen Partnern an verschiedenen Forschungsprojekten. Die angebotene Studien- und Diplomarbeit soll diese Forschungsgruppe unterstützen.

Aufgabenstellung

Die Vision des Ubiquitous Computing ist es, den Computer als Gerät verschwinden zu lassen und durch "intelligente Gegenstände" zu ersetzen. Diese kommunizieren selbständig im Ad-Hoc-Verfahren untereinander, so daß ein Eingreifen von außen (durch Administratoren) überflüssig wird.

Die Daten werden in der Regel unverschlüsselt über die RF-Schnittstelle gesendet. Eine geschützte Übertragung setzt einen sicheren Austausch des Verschlüsselungskeys voraus.

Ein entsprechender Ansatz ist die gleichzeitige aber voneinander unabhängige Bestimmung über ein externes Ereignis (z.B. Audiosignal). Unter gewissen Bedingungen berechnen alle Sensorknoten unabhängig voneinander den gleichen Key. Zur Erhöhung der Sicherheitsstufe wird dieser zyklisch neu ermittelt. Stimmen die Keys der Übertragungspartner überein findet eine gesicherte Übertragung statt.

Ziel dieser Studien- und Diplomarbeit ist die Untersuchung und Implementierung des "Context as a key" - Verfahrens. Prinzipiell kann ein Key über das Leistungs- bzw. Frequenzspektrum des Audiosignals bestimmt werden. Einen sinnvollen Key erhält man (nur) dann, wenn geeignete (d.h. charakteristische) Frequenzblöcke aus dem Spektrum des Signals zur Gewinnung herangezogen werden. Teilaufgabe der Arbeit wird es sein, das Verfahren auf eine möglicherweise notwendige Adaption hin zu untersuchen.

Die Schwerpunkte der Arbeit liegen in den Bereichen Mustererkennung und Signalverarbeitung. Zunächst ist eine geeignete Methode zur Bestimmung des Verschlüsselungskeys zu ermitteln und zu testen (Matlab o.ä.). Anschließend ist das Verfahren in einer geeigneten Programmiersprache (C++/JAVA) zu implementieren.

Was wir bieten

- + Integration in europäische und internationale Projekte
- + Hoher Anwendungsbezug und sehr gute Kontakte zur Industrie
- + Kreatives, dynamisches Arbeitsumfeld mit internationaler Ausrichtung
- + Direkten Kontakt zum Institut, zur Forschungsgruppe und deren Mitgliedern

Anforderungen

- + Kenntnisse in einer der Programmiersprachen C/C++/JAVA
- + Grundkenntnisse in Matlab hilfreich
- + Selbständiges, kommunikatives Arbeiten, Kreativität
- + Fließend deutsch
- + Bereitschaft neue Fähigkeiten zu erlernen
- + Persönliche Initiative und Anwesenheit am Institut

Kontakt

Monty Beuster
DUS Forschungsgruppe am IBR
Mühlenpfordtstr. 23 38106 Braunschweig
Tel.: 0531 / 391-3295
beuster@ibr.tu-bs.de

<http://www.ibr.cs.tu-bs.de/dus/>

