Mündliche FP Kurs 1679 "Mobile Computing" für Master of Computer Science
Prüfer: Herr Dr. Jörg Roth
Beisitzer: Frau Dr. Keller
Datum: 26.09.2005
Dauer: ca 30 min
Note: 2

1 Welche Verfahren auf der Bitübertragungsschicht gibt es ?

- CDM,TDM,FDM,SDM

2 CDM erklären

- Was ist ein Chip, Codewort, Spreizccode ?
- Welche Bedingungen gibt es, damit mehere Sender mit unterschiedlichen Speiz-codes arbeiten können ?

3 WLAN Verfahren erklären

- PCF & DCF erläutern (Hidden-Terminl, NAV,RTS,CTS,Contention Window erläutern)

4 WLAN Sicherheit

- Authentizierung und Verschlüsselung erklären (aufmalen, IV, XOR,RC4 usw. Blockschaubild erzeugen !)
- Challenge Response im WLAN Umfeld erklären (Wer schickt die Zufallszahl ?)
- Warum kann ein verschlüsseltes Datenpaket mit geändertem CRC wert “simuliert” werden
- Wie kann die Verschlüsselung entschlüsselt werden ? Erhält man bei der Entschlüsselung den symetrischen, geheimen Schlüssel ? Warum benötigt man diese Schlüssel nicht, um Datenpakete wieder im Klartext zu erhalten ? Wie kann der Angreifer Klartext einschleusen und verschlüsseln ?
- Warum können Datenpakete mit Hilfe von wiederkehrenden IV “entscchlüsselt werden ?
- Was macht der IV ?
- Aufzählung der Möglichkeiten, eine WLAN Verbindung zu verschlüsseln ?
- MAC Filterung unter WLAN erklären. Warum ist diese Filterung nicht sicher ?

Einstufung Kurs 1679
Den Kurs kann ich jedem empfehlen. Der Umfang bzw. die Themenvielfalt ist aber nicht zu unterschätzen. Insbesondere enthält das Thema/ der Kurs min. 400 Abkürzung :-). Die Betreung in der Newsgroup ist gut. Evtl. Fragen werden ziemlich schnell & ausführlich beantwortet.
Prüfer
Frau Dr. Keller und Herr Dr. Roth kann ich jedem als Prüfer empfehlen. Sind sehr ruhig und stellen präzise, klare Fragen.
Die Benotung liegt auf einem gerechten Level. Es ist wichtig, das die Prüfungsanworten sicher und nicht zu langsam kommen !
Lernhinweis
Die Einsendeaufgaben sollten in jedem Fall bearbeitet werden, sind aber freiwillig. Es gibt Schwerpunkte in dem Kurs die in jedem Fall jeder wissen sollte. Dazu zählt z.B. Verfahren der Bitübertragungsschicht, WLAN PCF/DCF, WLAN & Bluetooth Verschlüsselung, Positionsbestimmung + Berechnung Pseudoentfernung.

Gedächtnisprotokoll Diplomprüfung Praktische Informatik Teil 2
Kurs 1679 Mobile Computing
Prüfer Dr. Roth
Beisitzerin Frau Scheben
Datum 22.8.2005
Note 1,0 (Frau Scheben sei Dank!)

Funkschnittstelle welche Methoden gibt es?
- Raum, Zeit, Frequenz und Codemultiplexverfahren kurz erklärt

Welche dieser Verfahren werden bei GSM-Mobiltelefonie wie genutzt?
- Raum, Zeit, Frequenzmultiplex
- Raum:
    - Aufteilung des Raumes über Cluster von Zellen
    - Idealisierte identische Form von Zellen im Cluster
    - Bei GSM 7 Zellen je Cluster
    - 1 Basisstation je Cluster
    - Abstand von Basisstationen mit gleicher Frequenz D = r * $\sqrt{3 * k}$, wobei r den Radius der Zellen und k die Anzahl der Zellen im Cluster an gibt.
- Zeit:
    - 8 Zeitschlitze (Slots)
    - 1 Zeitschlitz pro Gerät
    - Zeitschlitze für Up und Downstream um 3 BP versetzt, damit Geräte nicht gleichzeitig senden und empfangen müssen
- Frequenz:
    - Aufteilung der dem Mobilfunkbetreiber zugeordneten Frequenzen auf die Zellen (Beispiel D1 57 Kanäle auf 7 Zellen 8 Kanäle pro Zelle)
    - Auf unterschiedlichen Frequenzen kann gleichzeitig gesendet werden

WLAN (802.11) – Übertragungsverfahren auf der Luftschnittstelle?
- Infrarot
- Frequenzwechsel
- Codespreizung

Welches davon hat sich durchgesetzt bzw. welches wird gar nicht genutzt ? (Er war sich nicht sicher ob er das bevorzugte im Kurs genannt hatte)
- nicht genutzt wird Infrarot
- (durchgesetzt hat sich wohl die Codespreizung sagte Herr Dr.Roth)

802.11 MAC-Schicht
- CSMA/CA-Verfahren kurz erklärt inkl. Wartezeiten DIFS, SIFS und PIFS, sowie zufallsabhängiger Komponente

Was versteht man unter Contention Window?
- Contention Window und Exponential Backoff kurz erklärt
- Vorteile / Nachteile großer/kleiner Contention Windows erläutert

Koordiniertes Verfahren ?
- PCF erklärt

Sicherheit bei Datenübertragung im WLAN unter 802.11?

- WEP Verfahren erklärt
    - symmetrisches Verfahren,
    - Stromchiffre XOR Verknüpfung
    - Fester Schlüsselanteil und Initialisierungsvektor
    - Problematik Schlüssellänge für Sicherheit

Stichwort Sicherheit der Verschlüsselung und Initialisierungsvektor, wo liegt das Problem?

- kurzer Initialisierungsvektor ist nicht wirklich sicher

Wie kann ein Angriff aussehen?

- Hier hatte ich nicht wirklich Ahnung und zahlreiche Hilfsversuche von Dr. Roth waren auch nicht wirklich erfolgreich. Hören wollte er im Endeffekt, dass sich bei großen Datenmengen die Initialiseirungsvektoren nach einiger Zeit wiederholen. Und das Klartextangriffe relativ schnell zum Erfolg führen.

Damit war die Zeit dann auch abgelaufen. Dank der ansonsten sehr flüssigen ausführlichen und korrekten Beantwortung sämtlicher anderen Fragen führte der Totalausfall bei der letzten Nachfrage dank der Fürsprache von Frau Scheben nicht zur Abwertung auf 1,3. Sondern es erging Gnade vor Recht und ich bekam doch noch die 1,0.
Nicht nur deshalb kann ich Herrn Dr. Roth als Prüfer empfehlen. Die Prüfungsfragen sind fair und bei Problemen versucht er einem durch Nachfragen und Hilfestellungen doch noch den rechten Weg zu weisen.
Allen Nachfolgern viel Glück bei Ihren Prüfungen

Masterprüfung (MSc.) Praktische Informatik – Mobile Computing 1679
Gedächtnisprotokoll
Prüfer: Hr. Dr. J. Roth
Beisitzer: Fr. Dr. D. Keller
Zeit: 11.10.2004
Dauer: ca. 25-30 Minuten
Note: 1,3

Nach einer kurzen Begrüßung mit den Prüfern ging es auch direkt los. Die Prüfungsatmosphäre war freundlich und die anfängliche Nervosität verflog auch schnell. Die Prüfungsfragen wurden klar gestellt. Wenn man die Frage nicht richtig verstanden hatte, wurde diese von Hrn. Roth etwas anders formuliert oder es folgte eine etwas präzisiere Fragestellung. Alle Fragen waren im Zusammenhang gestellt. Lag man mit der Antwort nicht ganz richtig, konnte man das am Gesichtsausdruck des Prüfers sehen und ich hatte die Möglichkeit mich zu verbessern, eine andere Formulierung zu wählen oder die Sache genauer zu erklären.

Die Fragen, die mir (in etwa) gestellt wurden:

Mobilität im Internet

- Wie kommen Mobile Rechner an eine Adresse ?

=> DHCP genau erklärt

- Warum ist diese Vorgehensweise für Mobile IP nicht geeignet ?
- Wie funktioniert Mobile IP ?
- Warum Tunneling bei Mobile IP ?
- Wie funktioniert Cellular IP und warum Cellular IP ?
- Wie wird sichergestellt, dass beim Handoff keine Pakete verloren gehen ?

Add-Hoc Routing:

- Klassifikation der Routing-Verfahren ?
- Wieso Add-Hoc Routing ?
- Wie genau funktioniert DSR ?
- Was passiert wenn eine Verbindung gelöscht wird ?
- Was genau wird gelöscht ?

=> Natürlich nur die Routingstrecke über die unterbrochene Verbindung

- Welche Informationen sind in den Paketen enthalten

=> Neben Zieladresse auch Quelladresse („Source“), sowie die Hops.

Positionsbestimmung:

- Welche Basistechniken gibt es ?

=> COO, TOA, TDOA, AOA, Signalstärke

- Was wird gemessen ?

=> Entfernung zum Sender

- Genauigkeit der Verfahren und Fehlerquellen

- Wie funktioniert GPS ?

=> Genaue Erklärung (Pseudoentfernung nicht vergessen)

- Wie lautet die Formel zu Berechnung der Pseudoentfernung (auf Papier)

=> Hier kam ich leider ins stocken und konnte auch die Formel nicht 100%ig zu Papier bringen.

Dann war die Zeit auch schon um. Nach einer kurzen Besprechung der Prüfer, bekam ich meine Note. Diese musste leider Aufgrund der Fehler bei der letzten Frage auf 1,3 nach unten korrigiert werden. Trotz der Menge und Komplexität des Stoffes war ich aber zufrieden. Hr. Dr. Roth kann als Prüfer nur empfohlen werden.

Viel Glück bei eurer Prüfung.

Mündliche Masterprüfung Kurs 1679 "Mobile Computing"

Prüfer: Dr. Jörg Roth
Beisitzer: Dr. Keller
Datum: 10.9.2004
Dauer: 25 min
Note: 2,3

- Funkübertragung Verfahren allgemein (nur ganz kurz erklären)
  * Zeitmultiplex
  * Raummulitplex
  * Frequenzmultiplex
  * Codemultiplex

- Codemultiplex genauer erklären mit Beispiel (Nutzdaten, Spreizwort) auf Papier. Codierung und Decodierung. Da kam ich ins Schleudern, da ich mich in den Details verlor. Eigentlich wollte er nur hören, dass sich das Spreizwort mit allen Chips auf jedes Bit der Nutzdaten verteilt. Einige Studenten scheinen jeden Chip des Spreizwortes auf ein Bit Nutzdaten zu verteilen.

- WLAN: CSMA/CA mit Bestätigung an einem Beispiel mit 2 Stationen (FRAME/ACK/DIFS/CIFS/Contention Window auf Papier). Hier vergass ich komplett das Contention Window. Da hat er mich dann mit geschickten zusätzlichen Fragen drauf gestossen, dass noch etwas fehlt. So konnte ich das noch nachliefern. Dann wollte er noch wissen, wie auf Kollisionen reagiert wird. Ich lag mit meiner Vermutung, dass es verdoppelt wird, goldrichtig. Leider hab ich es auch als Vermutung geäussert und er wollte auch den Begriff ("Exponention Backoff") hören, so dass ich da nicht so gut aussah.

- WLAN Authentifizierung nur ganz grob. Ich wusste nur "Challenge Response Verfahren" und dass bei Empfang einer verschlüsselten Nachricht ohnehin davon auszugehen ist, dass der Sender auch authentifiziert ist. Er meinte, dass man nicht auf eine verschlüsselte Nachricht warten will, bis die Authentifizierung vorliegt. Er wollte hören, dass A eine Zufallszahl zu B schickt, B diese verschlüsselt und das Ergebnis zu A zurückschickt. A vergleicht das dann mit dem Ergebnis der eigenen Verschlüsselung der Zufallszahl.

- WLAN Verschlüsselung komplett auf Papier. Das klappte sehr gut. Dann wollte er noch die Angriffspunkte zu WEP. Leider konnte ich ihm nicht erklären, wo genau das Problem mit dem kurzen IV ist.

Nach 25 Minuten beendete er die Prüfung dann recht plötzlich. Ich kann mir vorstellen, dass er noch mehr hätte hören wollte.

Insgesamt war ich wohl zu langsam und zu unsicher bei der Beantwortung der Fragen und einige Sachen wusste ich gar nicht bzw. konnte ich nicht erklären (Exponential Backoff, WLAN Authentifizierung, Problem von kurzen IV bei WEP), so dass ich denke, dass ich mit der Note noch recht gut gefahren bin. Kurs und Prüfer kann ich eigentlich nur jedem empfehlen.

Prüfungsprotokoll für Kurs 1679 Mobile Computing am 19.01.04
Prüfer: Dr. Roth
Beisitzer: Dr. Keller
Zeit: 30 min
Note: 1,3

Über folgende Themen hat mir Dr. Roth Fragen gestellt:

Wie bekommen mobile Rechner ihre Adressen?
Also habe ich DHCP erklärt.
Dr. Roth hat noch einige Fragen zu DHCP gestellt, wie z.B. Ablauf von DHCP, Adressierung des Client der noch keine Adresse hat. Warum ist die Adresse so wichtig (da wollte Dr. Roth hören, dass der mobile Rechner auch Dienste anbieten kann und um die zu nutzen braucht man die Adresse)

Es ging weiter zu Mobile IP und Cellular IP. Wozu braucht man Mobile IP und wie funktioniert es, wozu braucht man dann noch Cellular IP und wie funktioniert es.

Was sind die Probleme bei der Transportschicht im Vergleich drahtgebunden und drahltlos?
Split Connection Verfahren. Snoop Agent und I-TCP erklären und Vergleichen.

Positionsbestimmung (laut Dr. Roth sein liebstes Thema ☺)
Die Grundlegenden Verfahren nennen und einen Satz zur Funktionsweise sagen. (COO, TOA, TDOA, AOA)
Satellitenanavigation erklären.
Also GPS und die Funktionsweise. Ich habe das Bild aus dem Skript aufgezeichnet und erläutert.
Uhrenproblem erklären.
Welche Entfernung wird gemessen? (Pseudoentfernung)
Von der Berechnung im Detail will er nichts hören. Man muss erwähnen können welche Werte zu messen sind.

Dies waren die Themen meiner Prüfung. Es gab noch ein paar Fragen mehr in den einzelnen Themenbereichen, an die ich mich aber so genau nicht mehr erinnern kann. Alle Fragen waren sehr gut gestellt. Bei Verständnisproblemen änderte Dr. Roth die Formulierung. Die Athmosphäre war sehr gut. Beide waren sehr locker und lustig. Ich kann Dr. Roth als Prüfer dringend empfehlen. Die Benotung ist auch sehr fair, da ich zwei oder drei Fragen nicht beantworten konnte.

Prüfungsprotokoll 1679 „Mobile Computing“ 19. 12. 2003

Prüfer **Dr. Roth**

Beisitzer **Dr. Keller**

Dauer **25 min**

Note **1,0**

Bitübertragungsschicht

- Verfahren zur Mehrfachausnutzung von Funkressourcen nennen und beschreiben: Raum-, Zeit- Frequenz- und Codemultiplex.
- Prinzip des Codemultiplex erklären: An einem aufgemalten Signal mit drei Bit erklären. (Wichtig: Die Chips sind natürlich nicht so breit wie die Bits.) Rekonstruktion des Ursprungssignals.
- Probleme dieses Verfahrens : Orthogonalität der Spreizcodes, Problem der unterschiedlichen Signalstärke, Synchronisation.

Sicherungsschicht

- Zugriffsverfahren auf das Funkmedium: CSMA/CD geht nicht, daher CSMA/CSA. DCF, mit RTS/CTs, mit PCF erklärt.
- Wie wird das Hidden Terminal Problem hier gelöst: Freibleiben des Funkmediums, RTS/CTS bzw. PCF

GSM-Mobiltelefonie

- Sicherheitsziele: Authentikation nur des Teilnehmers; Abhörsicherheit der Luftschnittstelle von Dr. Roth nachgeliefert: kein Tracking des Teilnehmers (Bewegungsprofile)
- Welche Verschlüsselungsverfahren, wo untergebracht. A3, A5, A8, Ki, Kc.
- Warum A3, A8 auf der Karte: Theoretisch nicht auslesbar. Seitenangriff erwähnt
- Challenge Response Verfahren aufmalen: (hier brauchte ich etwas Starthilfe, habe ich auch bekommen) und erklären, xor-Verknüpfung der Daten mit dem Schlüssel, Stromchiffre.

Positionsbestimmung - Satellitennavigation

- Satellitennavigation ausführlich erklärt, Laufzeitbestimmung, Kugelschalenschnitt, Uhrenproblematik, Lösungsverfahren (nur ansprechen, nicht genau erklären).
- Möglichkeiten, die Genauigkeit zu erhöhen. Mehr Sdatelliten, DGPS, WAAS erklärt. Bildung des Korrekturfaktors satellitenweise, was wird eigentlich genau korrigiert?

Schlussbemerkung

1679 ist ein umfang- und detailreicher Kurs. Die Prüfung verlor sich aber nicht in implementierungsabhängigen Details, sondern blieb auf einem fairen Level, sie war aber durchaus auch nicht geschenkt. Die Prüfungsatmosphäre war ruhig und freundlich. Insgesamt kann ich Kurs und Prüfer sehr empfehlen.

Prüfungsprotokoll
Mobile Computing – 01679
Prüfer: Dr. Jörg Roth, Beisitzerin: Dr. Daniela Keller (Lehrgebiet Prakt. Inf. II)
Datum: 19.12.03
Prüfungsdauer: 20 min.
Note: 1,0

Fragen:

Positionsbestimmung:

Grundlegende Verfahren (ToA/TDoA, CoA, Messung der Signalstärke, AoA, visuell)
Details Erklären anhand von GPS

- Funktionsprinzip von GPS
  (4 Satelliten senden Zeitsignal -> Gleichung mit 4 Unbekannten lösbar, 4. Satellit zum Ausgleich der Uhrenfehler vor allem beim Empfänger …)
- Weitere Verfahren
  - DGPS
    Kontrollstation am Boden sendet Korrektur-Signal pro Satellit über Funk an Empfänger im Umkreis (Stichwort Pseudoentfernung)
  - WAAS
    Senden des Korrektursignals über geostationäre Satelliten, die genau einen bestimmten Bereich abdecken

WLAN

- Verschlüsselung über WEP
  - Funktionsprinzip von WEP (Schlüssel, IV, Nachricht + ICV -> XOR verknüpft an den Empfänger)
  - Authentifizierung über Challenge-Response-Prinzip (Erklärung)
  - Sicherheitsprobleme (kurze Schlüssel, kurzer IV -> kommt nach relativ kurzer Zeit wieder vor …)

Routing-Verfahren anhand von DSR erklären

- Ablauf (Request, Response, Maintainance, Fehlerbehandlung)

Problematik der schnurlosen DÜ auf Ebene 4 des OSI-Modells
Probleme bei TCP (für Festnetzverbindung ausgelegt -> reagiert bei Fehlern für wireless falsch)
Möglicheikten:
Split-Connection mit I-TCP oder Snoop-Protokoll
Erklärung des Snoop-Protokolls und Vorteile gegenüber I-TCP nennen

Prüfungseindruck:
Herr Roth ist ein sehr angenehmer Prüfer, bei dem vorhandene Nervosität schnell verschwindet. Die Fragen können detailliert werden, bei Problemen gibt er jedoch Hilfestellung.
Allgemein ist die Bewertung fair und die Prüfungsatmosphäre sehr angenehm.
Dr. Roth ist als Prüfer sehr zu empfehlen.