(c) Jens.Schneider@fernuni-hagen.de

(c) Jens.Schneider@fernuni-hagen.de

1 KE 1 - Grundlagen der drahtlosen Kommunikation / Mobiltelefonie

1.1 Verfahren zur Funkübertragung erläutern

- Zeitmultiplex – Time Division Multiplex (TDM)
  Mehrere Sender teilen sich über Slots eine Frrequenz
  Nur ein Sender sendet zu einem Zeitpunkt

- Raummultiplex – Space Division Multiplex (SDM)
  Zelluläre Aufteilung der Gesamtfläche. Sendeleistung schwächt sich ab

- Frequenzmultiplex – Frequenz Division Multiplex (FDM)
  Sender benötigt auf einem Frequenzband einen Kanal. (Frequenz Hopping Erweiterung)

- Codemultiplex – Code Division Multiplex (CDM)
  Gleichzeitiges Senden von verschieden Sendern. Über unterschiedliche Spreizcodes Sicherstellung das die Überlagungerung später augelesen werden können

  Binäre Daten (1 == +, 0 == -1)

  Ausgangssignal == Spreizcode * Binäre Daten
  (unter GPS nennt man den Spreizcode PRN == Pseudo Random Noise)

  Probleme: Die Spreizcodes müssen zueinander Orthogonal sein.
  (Binäres Signal, Spreizcode(mit mehreren gleichen Codewörtern, Mehrere Chips auf einem Bit), Synchronisation

  Bei zwei Sendern muss das Skalarprodukt null sein.
  Bei mehr als > 2 Sendern muss die Spreizcodes paarweise Orthogonal sein. (Walsh-Hadamar Matrizen)

  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 nterschiedlichen Signalstärke, Synchronisation.
  (Nutzdaten, Spreizwort)auf Papier. Codierung und Decodierung.
  Eigentlich wollte er nur hören, dass
  sich das Spreizwort mit allen Chips auf jedes Bit der Nutzdaten verteilt.
  Speizcode == Summe der Codewörter
  Chips
  1==1
  0==-1

Time Division Duplex (TDD)
Frequence Division Duplex (FDD)

Duplex
(bidirektionale verbindung von zwei Kommunikationspartnern)

Multiple Access
von mehreren Sendern

1.2 Sieben Schichten des OSI-Referenzmodells aufzählen

- Application Layer (Anwendungsschicht)
- Presentation Layer (Darstellungsschicht)
- Session Layer (Kommunikationssteuerungschicht)
- Transport Layer (Transportschicht)
- Network Layer (Vermittlungsschicht)

(c) Jens.Schneider@fernuni-hagen.de

- Data Link Layer (Sicherungsschicht)
- Physical Layer (Bitübertragungsschicht)

1.3 Wie wird in der Sicherungsschicht des OSI-Referenzmodells Übertragungen gesichert ?

- Automatic Repeat Request (ARQ)
- Forward Error Correction (FEC)

1.4 Welche Schichten werden von IEEE 802 abgedeckt?

- Bitübertragung
- Sicherungsschicht

1.5 Wie werden die Schichten von IEEE 802 genannt ?

- Physical Layer (PHY)
- Media Access Layer (MAC)
- Logical Link Control (LLC)

1.6 Schichten von TCP/IP Referenzmodell aufzählen

- Netzwerk
- Internet
- Transport
- Anwendungsschicht

1.7 Aufzählung Transportprotokolle des Internets

- UDP
- TCP

1.8 Drei Internetprotokolle des Anwendungsschicht (Application Layer) aufzählen

FTP, HTTP, SMTP, Telnet, NNTP, DHCP

1.9 Drei Internetprotokolle der Vermittlungsschicht aufzählen

IP, ICMP, ARP, Multicast IP, Mobile IP

1.10 Unterschiede Funkkommunikation zur drahtgebundenen Kommunikation

- Störanfälligkeit
- niedrige Datenraten,
- Mithören,
- Gesetzliche Regelungen über das Funkmedium

1.11 Welche Verfahren zur Ausnutzung der Funkschnittstelle werden von GSM genutzt?

- Raum(SDM), Zeit (TDM) , Frequenzmultiplex (FDM)

<u>Raum (SDM)</u>

- 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 $D = r * \sqrt{k * 3}$
  wobei r den Radius der Zellen und k die Anzahl der Zellen im Cluster an gibt.

<u>Zeit (TDM)</u>

- 8 Zeitschlitze (Slots)
- 1 Zeitschlitz pro Gerät
- Zeitschlitze für Up und Downstream um 3 BP versetzt, damit Geräte nicht gleichzeitig senden und empfangen müssen

<u>Frequenz (FDM)</u>

- 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

1.12 Mobilfunkgenerationen in Deutschland aufzählen. Welche Provider gibt es?

Erste Generation

- A-Netz
- B-Netz
- C-Netz

Zweite Generation

- D-Netz (Telekom D1, D2-Mannesmann/Vodafone)
- E-Netz (E-Plus, O2)

Dritte Generation

- UMTS

1.13 Warum für Mobilfunk zellulare Netze?

- Reduktion von Mobiltelefon zur Basisstation
- Mehrfachausnutzung von Funkresourcen

1.14 Zwei Aspekte bei der Wahl der Cluster-Größe die zu beachten sind

- Anzahl der Frequenzen beschränkt
- Abstand mit gleichen Frequenzen hinreichend gross

1.15 Welche Daten sind auf der SIM-Karte gespeichert?

- IMSI
- Geheimnummer
- Noch nicht gelöschte SMS
- Konfigurationen von dem Provider
- Konfigurationen von dem Mobiltelefon

1.16 Welche Subsystem kennt GSM

- Funksubsystem
- Vermittlungssubsystem
- Betriebssubsystem

1.17 Welche Komponenten gehören zu dem Funk Subsystem von GSM?

- Mehrere Mobile Station (MS) (Z.b. Mobile Phone, Blackberry)
- Mehrere Base Transceiver Station (BTS)
- Mehrere Base Station Controller (BSC)

1.18 Welche Komponenten gehörten zu dem Vermittlungs Subsystem?

- Mobile Switching Center (MSC) , vergleichbar z.B. einem ISDN-Switch
- Home Location Register Datenbank (HLR)
- Visitors Location Register Datenbank (VLR)
- Gateway MSCs (GMSC)
- International Switching Center (ISC)

1.19 Welche Komponenten gehörten zu dem Betriebs Subsystem?

- Operation and Maintenance Center (OMC)
- Authentication Center Datenbank (AUC)
- Equipment Identity Register Datenbank (EIR)

1.20 Welche Übertragungsraten werden über GSM erreicht?

- 13 000 Bit/s für Sprache
- 9600 Bit/s für Daten

1.21 Welche Verfahren werden unter Phase 2+ zusammengefasst?

- Enhanced Data Rates für GSM Evolution (EDGE)
- Packet Radio Service (GPRS)

- High Speed Circuit Switched Data (HSCSD)

1.22 Aufzählung Dienstgüteklassen von UMTS

- Conversational
- Streaming
- Interactive
- Background

1.23 Aus welchen Komponenten besteht ein DECT Netzwerk?

- Portable Radio Termination (Portable Part)
- Fixed Radio Termination (Radio Fixed Part / Central Control Fixed Part)

2 KE 2 – Drahtlose lokale Netze

2.1 Wie werden Kollision auf der MAC Schicht von IEEE 802.11 verhindert?

Im Gegensatz zu IEEE 802.3 müssen Kollisionen verhindert bzw. reduziert werden.
Sender überdeckt am Sendeort alle Signale anderer Sender
CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)
Wahrscheinlichkeit von Kollisionen verringern
Im Falle von Kollisionen wird durch Quittierungsverfahren der Verlust von Nutzdaten erkannt.

2.2 Wie wird das Hidden-Terminal gelöst ? Mit welchem Verfahren?

Nutzung von RTS/CTS Frames. Jeder Sender hört min. einen RTS oder CTS Frame. In diesen Frames ist der NAV(Net Allocation Vector enthalten). Während dieser Zeit findet keine Bewerbung um das Funkmedium statt
PCF-Verfahren, Es gibt eine Station (i.d.R. der Access Point == Point Coordinator), die einen StartCF Frame setzen. Der Polls Frame setzt einen NAV Zeitrahmen. Während dieser Zeit findet keine Bewerbung um das Funkmedium statt.

2.3 Beschreibung der drei Zugriffsverfahren unter IEEE 802.11 ?

a) einfaches CSMA/CA, verbindlich , DCF (Distributed Coordination Function)
Ad-Hoc Modus/Infrastruktur-Modus

b) einfaches CSMA/CA mit Bestätigung (ACK)
Frame, SIFS,ACK, DIFS + Contention Window
Wie wird auf Kollisionen reagiert? Verdoppelung ? Exponential Backoff

c) b) CSMA/CA with RTS/CTS, optional DCF (Distributed Coordination Function)
Ad-Hoc Modus/Infrastruktur-Modus, Löst das Hidden Termin-Problem
RTS, SIFS,CTS,Frame,NAV, ACK,DIFS (übliche Bewerbung um Funkmedium)

d) PCF (Point Coordination Function), optional,
nur im Infrastruktur Modus, Erfordert Koordination durch Access Point, Verhindet HIdden Termin-Problem
PC, S2...
PIFS
PollS (Kann Nutzlast enthalten), SIFS, Frame, NAV(Net Allocation Vector) , StartCF,EndCF

WIchtige Begriffe für IEEE 802.11
Backoff --> Das Medium wird während der Wartezeit von einer anderen Station belegt.Wartezeit erhöht sich.
Zufallszahl
Wartezeit = konstante Wartezeit DIFS(DCF Interframe Interframe Space) + zufallsabhängige Wartez.
Contention Window
Keine Kollisionsfreiheit

Wahl des Contention Window
Kleines Contention Window == mehr Kollisionen, Wartezeiten klein, bei geringer Last höherer Durchsatz

Grosses Contention Window == weniger Kollisionen, Wartezeiten hoch, Durchsatz sinkt

Bestätigung von Frames (Versenden von Nachrichten an eine Station)
Sender kann Frame nochmal senden (aufgrund von Kollision oder Störung)
Empfänger sendet Bestätigung ACK. Keine Bewerbung auf den Zugriff auf das Funkmedium

Empfänger hat SIFS zu warten. Immer kürzer als DIFS

Exponential -Backoff Verfahren (Contention-Window wird im Fehlerfall vergrössert)
Nach erfogreicher Quittierung durch den Empfänger kann das Contention-Window auf den alten Wert gesetzt werden.

Adaptives Verfahren: Contention Window (7,15,...255) Wird immer mit 7 begonnen. Nach Fehler erhöhen.

2.4 MAC-Schicht, Zugriff auf das Funkmedium – Uhrensynchronisation

Beacon-Frame, TSF, Infrastrukturmodus Beacon kommt über den Access Point
Steht eine Aussendung um das Beacon im Ad-Hoc-Modus an, Bewerbung um Funkmedium, Gewinner sendet Beacon-Frame.

2.5 Reihenfolge von DIFS,PIFS,SIFS,CTS,RTS

SIFS< RTS/CTS /ACK < PIFS < DIFS

2.6 Welche Power-Managment-Mode kennt WLAN 802.11?

- Sleep Mode
- Awake Mode

2.7 Welche Service Sets kennt WLAN 802.11

- Basic Service Set (BSS)
- Independent Basic Service Set (IBSS)
- Extended Service Set (ESS)

2.8 Welche Verfahren zur Bitübertragung (Luftschnittstelle) sind in WLAN 802.11 definiert?

- FHSS (Frequenzsprungverfahren)
- DSSS (basierte auf CDMA, hat sich durchgesetzt)
- Infrarot (hat sich nicht durchgesetzt)

2.9 Welche Phasen durchläuft HIPERLAN/1 bei Zugriff auf das Funkmedium?

- Prioritization Phase
- Contention Phase
- Transmission Phase

2.10 Welche Zustände (Conditions) kennt HIPERLAN/1 beim Zugriff auf das Funkmedium?

- Channel Free Condition
- Synchronized Channel Condition
- Hidden Elimination Condition

2.11 Mit welchen Verfahren spart HIPERLAN/1 Batteriestrom?

Versetzen Station in Doze Mode
Verfahren mit p-Saver, p-Supporter

2.12 Welche Stationstypen unterscheidet Wireless ATM?

- Station

- Mobile Station
- Drahtlose Station
- Drahtlose mobile Station

2.13 Über welches Protokoll wird in HomeRF die Audioübertragung durchgeführt?

DECT

3 KE 3 - Wireless Personal Area Networks (WPANs)

3.1 Welche zwei Teilstandards umfasst IrDA

- IrDA CONTROL (bis 75 kBit/s)
- IrDA Data (bis 16 MBit/s)

3.2 Welche Geschwindigkeiten und Modulationsverfahren werden bei IrDA eingesetzt?

- SIR bis 115kBit/s – RZI

- FIR bis 0,576 MBit /s - RZI
- FIR – bis 1,152 MBit/s - RZI
- FIR – bis 4MBit/s - 4PPM

- VFIR – bis 16MBit/s - HHH (1,13)

3.3 Max. Datenrate für Bluetooth herleiten

1) Die Frequenz wird alle pro Sekunde 1600mal gewechselt
   d.h. 1s/1600 = 625 µs
   1 Slot entspricht 625 µs
2) Die meisten Nutzdaten enthält der Typ DH5 mit 339 Bytes mit 5 Slots
3) 339 / 6 Slots = 339 * 8 / (6*625 µs) ca . 723,3 kBit /s

3.4 Max. Datenrate bei Bluethooth für Daten, wenn beide Richtungen dieselbe Datenrate erhalten

1) Die meisten Nutzdaten werden mit dem Typ DH5 mit 339 Bytes erreicht
2) d.h. 339 Bytes /10 Slots ca. 433, 92 kBit/s

3.5 Datenrate bei Bluetooth für Audio herleiten

- HV1 10 Bytes /2 Slots (jeder zweite Slot wird belegt)
- HV2 20 Bytes /4 Slots (jeder vierte Slot wird belegt)
- HV3 30 Bytes / 6 Slots (jeder sechste Slots wird belegt)

Immer 64 kBytes /Sekunde --> Fehler wirken sich bei geringerer FEC Rate stärker aus !

3.6 Service-Primitive für IrDA aufzählen und erklären

Es gibt 9 Service Primitive für IrDA

DISCOVERY
Suche von Geräte in Reichweite
Erfolgt in NDM Status
Ergebnis Liste von 32 Bit Zufallszahlen von jedem Gerät

NEW_ADDRESS
Gleiche Geräteadressen werden duch diese Operation neu berechnet.

UNITDATA
Unzuverlässiger Broadcast an alle Geräte in Reichweite

CONNECT
Verbindungsaufnahme zu einem anderen Gerät.
Aushandeln von Primary und Secondary (Primary ist meist der der den Connect absendet !)

SNIFF

Gerät möchte Verbindung als Secondary aufnehmen. Spart Strom
DATA
Übertragung von Nutzdaten. Zuverlässiger oder unzuverlässiger Transport
STATUS
Höhere Schichten können Status der Verbindung abfragen
RESET
Die Verbindung wird neu aufgebaut. Beide Partner müssen zustimmen
DISCONNECT
Abbau Verbindung. Gerät geht wieder in NDM

3.7 Unterschiede zwischen IrDA und Funk aufzählen

- Reichweite klein
- Einsatz nur in Gebäuden
- Sichtverbindung zwischen zwei Kommunikationspartnern nötig
- Größere Abhörsicherheit, da nur begrenzter Empfang
- Art der möglichen Störquellen
- Keine hoheitlichen Beschränkungen

3.8 Was ist die wichtigste Aufgabe von IrLAP unter IrDA

Bereitstellung der zuverlässsigen Übertragung

3.9 Was ist die wichtigste Aufgabe von IrLMP unter IrDA

Bereitstellung mehrerer logischer Kanäle

3.10 Welche Zustände gibt es bei IrLAP?

- NDM
- NRM(P)
- NRM(S)

(S) entspricht Secondary
(P) entspricht Primary

3.11 Was sind die wichtigsten Aufgaben von TinyTP von IrDA?

- Flusskontrolle
- Aufteilung von grossen Nachrichten

3.12 Was sind die wichtigsten Aufaben des L2CAP von Bluetooth?

- Bereitstellung von mehreren logischen Kanälen
- Aufteilung von grossen Nachrichten

3.13 Welche Link-Typen unterscheidet Bluetooth?

- Synchronous Connection-Oriented (SCO)
- Asynchronous Connection-less (ACL)

3.14 Über welchen Link-Typ läuft bei Bluetooth die Audioverbindungen?

- Synchronous Connection-Oriented (SCO)

3.15 Welche Modi kann ein Bluetooth Gerät annehmen?

- Active Mode
- Sniff Mode
- Hold Mode
- Park Mode

3.16 Welche Komponenten von IrDA und Bluetooth dienen der Dienstabfrage?

- Information Access Service (IAS) bei IrDA
- Service Discovery Protocol (SDP) Bluetooth

4 KE 4 – Protokolle zur mobilen und spontanen Vernetzung

4.1 Wie kommen die Mobile Rechner an eine Adresse? DHCP erklären !

1) DHCP-DISCOVER
   Client sendet Broadcast an alle Rechner im im Subnetz
2) DHCP-OFFER
   DHCP-Server sendet Angebot an den Client mit mit Netzwerkkonfiguration
3) DHCP-REQUEST
   Sendet der Client
4) DHCP-ACCEPT
   Sendet der Server

T1 = 50% der Lease Zeit (Nach Ablauf von T1 versucht der Client den Lease zu erneuern)
T2 = 87,5% der Lease Zeit (Danach ist ieder Broadcast an alle nötig)

4.2 Ablauf von DHCP, Adressierung des Client der noch keine Adresse hat. Warum ist die Adresse wichtig?

Der DHCP-Server kann über UDP den Client Nachrichten direkt an die MAC-Adresse schicken.

Der mobile Rechner kann auch Dienste anbieten.
Dazu benötigt der mobile Rechner eine Adresse.

4.3 Warum ist DHCP für mobile Rechner nur bedingt nutzbar?

Der mobile Rechner könnte eigene Dienste anbieten. Mit DHCP würde sich die IP Adresse in jedem Netzwerk ändern. Ein potenzieller Dienstnutzer könnte den mobilen Rechner nicht mehr im Netzwerk finden.
Lösung Mobile IP
Die IP bleibt immer unter einer festen Adresse erreichbar.

Nur mit DHCP könnte der mobile Rechner Dienste des loken Netzwerkes nutzen (z.B: drucken oder zentral abgelegte Dateien benutzen)

4.4 Wozu braucht man Mobile IP

Der Mobile Rechner könnte eigene Dienste anbieten und ohne Mobile IP würde die IP-Adresse sich dauernd ändern. Ein Dienstnutzer könnte in diesem Fall den mobilen Rechner nicht mehr wiederfinden.

4.5 Wie funktioniert Mobile IP?

Jeder Mobile Rechner erhält eine IP-Adresse die sich bei Bewegung auch nicht ändert.

Mobile Host (Mobiler Rechner)
Hat immer gleiche IP-Adresse

Corresponding Host
Möchte mit Mobile Rechner sprechen

Home Agent
Im Netzwerk des Home Network. Stellvertreter für den Mobile Host, wenn dieser nicht anwensend.
Kennt den Aufenthaltsraum des Mobile Host.
Hält ein Zuordnung von Care-of-Adress und Homeadress

Foreign Agent
Befindet sich im Visiting Network. Befindet sich da, wo der Mobile Host ist. Leitet Pakete an Mobile Host weiter.

Mobile IP verwaltet zwei Adressen pro Mobilen Rechner(Homeadress) + die Care-Of-Adresse
Foreign-Agent-Care-of-Adresse
Foreign Agent leitet Pakete an Mobile Host weiter. Es kann für mehrere Mobile Host ein Foreign-Agent-Care-Of-Adresse geben.
Collocated-Care-Of-Adresse

IP-V6 Implementierung:
Ein Foreign-Agent wird nicht mehr benötigt.
Ist für jeden Mobile Host im Fremnetzwerk unterschiedlich.

4.6 Welche Rechner sind bei einer Kommunikation über Mobile IP beteiligt?

- Mobile Rechner
- Fremdagent
- Heimagent
- Kommunikationspartner

4.7 Welche Adressen werden für einen mobilen Rechner unter Mobile IP verwaltet?

- Heimadresse
- Care-Of-Adresse (Foreign-Agent-Care-of(IP-V4) und Collocated-Care-of (IP-V6)

4.8 Welche Arbeitsschritte werden bei der Kommunikation über Mobile IP durchgeführt?

1) Agent Discovery
   Der Mobile Host ermittelt ob er sich im Fremdnetzwerk oder im Homenetzwerk befindet.
   ermittlung wo die Agents sind.
2) Registrierung
   Registration Request mit Message Digest Nachricht (Sicherheitsproblem ohne MD !)
   Registration Reply
3) Tunneling
   Tunneling der Anfragen über Fremdnetwerk--> Internet-> Heimnetzwerk
   (Reverse Tunneling) Wenn das Netzwerk keine Absenderadressen aus fremden Netzwerken erlaubt, die nicht aus diesem Netzwerk stammen.

4.9 Warum wird Tunneling bei Mobile IP eingesetzt?

Existierende Routing Protokolle sollten beibehalten werden.

Direktes Tunneling nicht möglich.
Sicherheitsproblem, wenn Paket mit Absenderadresse nicht aus einem bestimmten Subnetz kommt. Die Router unterstellen hierbei ein Sicherheitsproblem. In diesem fall muss der Rückweg über einen Reverse Tunnel laufen.

4.10 Wie funktioniert Cellular IP und warum Cellular IP?

Bei jedem Zellenwechsel ist eine neue Registrierung bei dem Home-Agent notwendig.

- Zweistufiges Netwerk
- Mobile IP Netzwerk vermittelt Pakete zu Mobilen Rechnern nur grob
- Erst innerhalb des Zugriffsnetzwerk wird über Cellular IP vermittelt
- Home Agent kennt nicht die genaue Position des Mobile Host, sondern nur das Netzwerk
- Home Agent muss erst informiert werden, wenn das Netzwerk und nicht die Zelle gewechselt wird.
- Nur die Routing Tabellen des Zugriffsnetzwerkes müssen angepasst werden

Care-of-Adrese ist Gateway Adresse (enhält den Foreign-Agent)

Knoten (Weiterleitung von Pakete), Basisstationen (mit Funkschnittstelle)

Basistationen können in GSM nur Pakete der eigenen Zelle transportieren.

Routing. Wird über Fluten verteilt, Routing Cache, Beacon-Nachricht

Route-Timeout
Werden nach einer bestimmten Zeit aus dem Cache gelöscht

Route-Update
Der Mobile Host aktualisiert die Cache Einträge. Der Route-Timeout wird zurückgesetzt.

4.11 Handover (Handoff) bei Cellular IP beschreiben

Ein Mobile Host, der in eine neue Zelle wandert führt einen Handoff durch.
Der Mobile host führt ständig eine Messung der Signalstärke zur Basisstation durch. Wird eine stärke Signalstärke gemessen,wird ein Handoff durchgeführt.

Es gibt zwei Arten von Handoffs

Hard Handoff
Der Mobile Host sendet Route Update zur neuen Basisstation.
Alle weiteren Rechner auf der Route ändern ihre Route zu dem Gateway
Z.B: die alte Basisstation entfernen die veralteten Route-Einträge erst nach einem Route-Timeout

Semisoft Handoff
Zweistufig

1) alte Basistation sendet eine Ankündigung zur Umschaltung an die neue Basisstation Pakete an dem Mobile host werden an die alte und die neue Basisstation gesendet
2) Nach einer bestimmten Zeit wird ein Hard Handoff durchführt

4.12 Was bedeutet "Paging" unter Cellular IP

Inaktive Rechner ("Rechner hat FUnkschnittstelle nicht ständig in Betrieb") sendet ähnlich zu Route Update, Paging Update zum Gateway Rechner.

Diese Info werden in einem Page Cache gehalten. Sind länger gültig als Route Update Einträge

Gateway möchte Packet an inaktiven Rechner senden

1) Versenden eine Page Paket
2) Entweder im Page Cache enthalten, oder Broadcast an alle Rechner (Ausnahme: von dem Rechner von das Paket kam)
3) Der gesuchte Rechner antwortet mit einem Route Update. Damit sind die Infos wieder im Route Cache & das Paket kann zugestellt werden.

4.13 Wie wird sichergestellt, dass beim Handoff unter Cellular IP keine Pakete verloren gehen?

Nur mit Cellular IP kann nicht sichergestellt werden das bei dem Handoff (allg. Handover) Pakete verloren gehen.
Können durch höhrere Protokolle aufgefangen werden (z.B. TCP)
Handoff (Hard Handoff, Semisoft Handoff)

4.14 DSDV ist die Weiterentwicklung welchen Verfahrens? Welches Problem des älteren Verfahrens wurde gelöst?

Distributed Bellmann Ford (DBF)
Löst das Count- to Infinity Problem

4.15 Nennen Sie ein Link-State-Verfahren, das für Ad-hoc-Netzwerke entworfen wurde.

Optimized Link State Routing (OLSR)

4.16 Bei welchen Netzen scheitern Partial-Reversal-Verfahren? Welches Verfahren löst das Problem?

Partitionierte Netze
Lösung: LMR

(c) Jens.Schneider@fernuni-hagen.de

4.17 Probleme bei der Transportschicht im Vergleich drahtgebunden und drahtlos? Problematik der schnurlosen DÜ auf Ebene 4 des OSI-Modells ?

Bei einem Engpass unterstellt TCP einen Engpass auf einem Router und nicht das Pakete auf der Funkstrecke verloren gegangen sind.
Verfahren zur Überlastungskontrolle (Congestion Control) werden eingesetzt
Pakethäufigkeit wird gesenkt.
Unter TCP heisst das Verfahren Slow-Start Verfahren. Ohne Bestätigung des Empfängers wird die Anzahl der Pakte halbiert.

Paketverluste sind bei drahtlosen Netzwerken kein Merkmal für Engpässe, sondern betreffen die Übertragungsstrecke selber.
Es gibt keine Selektive Quittungen, sondern nur kumulative Quittierungverfahren unter TCP

4.18 Selektive Quittungen für die drahtlose Kommunikation (mit TCP) bescchreiben

Standard TCP - Kumulative Quittung bei TCP
Empfänger bestätigt nur die bis dahin ununterbrochene Folge von empfangenen Paketen.
Der Sender muss alle danach folgenden Paketen nachsenden.

Erweiterung von TCP - Selektive Acknowledgements (SACKS)
Es können Bereiche quittiert werden. Der Sender sendet dann nur diese Pakete nach.

Explizit Loss Notifications
Der Empfänger meldet explizit, dass ein Paket nicht angekommen ist. In der Praxis relativ schwierig umzusetzen

4.19 Nennen Sie drei Transportprotokolle, die für drahtlose Verbindungen optimiert wurden?

- I –TCP (Split-Connection Verfahren)
- Mobile TCP
- Fast Retransmission

4.20 Split Connection Verfahren. Snoop Agent und I-TCP erklären und vergleichen

Split-Connection Verfahren
Aufteilung in zwei Verbindungen, Verbindung 1 – Basisstation und stationärem Rechner
Verbindung 2 – Basisstation und mobiler Rechner
Basisstation verwaltet beide Verbindungen. Der drahtgebunden Teil wird nicht angepasst (TCP)

Verbindungsabrüche, Bewegen des Rechners im Raum
Reduktion der verfügbaren Bandbreite

Indirekt TCP (I –TCP) ein Split Connection Verfahren
Arbeitet auf Transport Schicht
Überlastungskontrolle kann für die jeweiligen Abschnitte optimiert werden. Der drahtgebunden Teil setzt die normale Überlastungskontrolle ein. Der drahtlose Teil kann Pakete neu versenden, wenn diese verloren gehen.
Wanderung zu einer anderen Basisstation . Senderelevante Daten(Verbindungsparameter, Status Sendepuffer) bleiben bei der alten Basisstation

Nachteil
Doppelter Verwaltungsaufwand bei der Basissation
Verletzung der Ende-zu-Ende Sematik von TCP. Eine Quittierung bedeutet nicht, das dieses Paket bei dem Empfänger angekommen ist. Die Basisstation hat schon die Pakete bei der stationären Station quittiert.

Mobile-TCP
Verzichtet auf Sendefenster und nutzt einfaches Quittierungsverfahren um zuverlässige Verbindung sicherzustellen
Kompressionsverfahren im Kopf von Paketen, redundante Informationen werden eliminiert

---

Snoop Protokoll
Arbeitet auf der Vermittlungsschicht
Auf der Basisstation arbeitet ein Snoop Agent.
Hält Cache von Paketen
Hört den Quittierung ab.
Positive Quittierung löschen im Cache die entsprechenden Pakete.
„Negative" Quittierungen werden nicht an den Stationären Rechner weitergeleitet.
Aus dem Cache werden die fehlenden Pakete nachgesendet

Vorteil
Keine Änderung von existierenden Implementierungen von TCP bei den Kommunikationsendpunkten
Ende zu Ende Sematik bleibt erhalten im Gegensatz von I-TCP
Umschaltung zu anderen Basisstationen ohne oder mit Snoop Protokoll möglich.

Nachteil
Bei Verschlüsselung müssen die Paketkopfe gelesen bzw. entschlüsselt werden können. Die Sequenznummer für die Pakete ist notwendig.
Kommunikationspartner müssten Schlüssel an eine möglicherweise nicht vertrauenswürde Basisstation übertragen

---

Fast Retransmission
Löst das Problem des Umschaltens auf eine andere Basisstation
Der mobile Knoten sendet kurz nach dem Umschalten auf eine neue Basisstation eine Folge von positiven Quittungen.
TCP reduziert nur bei dem Ausbleiben jeglicher Quittungen die Pakethäufigkeit.

4.21 Was ist die Remote-Socket Architektur?

Auf dem mobilen Rechner läuft statt TCP ein einfaches Protokoll das für drahtlose Netzt optimmiert wurde.
Last Hop Protokoll (LHP)
Export-Protokoll
Einfache Kommunikations Operationen (Connect, read, write, close). Diese werden in der Basisstation in TCP Aufrufe gewandelt.

Mobiler Rechner: Lokales Socket Module
Basisstation: Export Socket Server

4.22 Warum arbeiten in Praxis Anwendung nicht mehr, wenn das UDP Protokoll eingesetzt wird ?

Im Gegensatz zu zu drahtgebunden Netzen arbeitet UDP in drahtlosen Netz garantiert nicht mehr zuverlässig.
Es sind keine Verfahren zu Überlastungskontrolle integriert.

4.23 Die drei Klassifikation der Routing-Verfahren?

- Adaptive
  Stellen sich auf veränderte Netzwerk Topologien ein
  In Ad-Hoc Netzen verwendet
- Nicht-Adaptive
  Routing wird anhand von festen Tabelleneinträgen vorgenommen

---

- Proaktive (table-driven)
  Halten Tabelleneinträge zu allen denkbaren Knoten im Netzwerk, selbst wenn keine Paket zu diesem Ziel geschickt worden ist.
- Reaktive (on-demand)
  Berechnen die Route zu einem Ziel erst, wenn das Paket versendet werden soll

---

- Distance Vector
  Tauscht nur mit Nachbarknoten Distanzinfos aus. Jede Knoten kann sich ein Bild vom gesamten Netzwerk machen, da auch Distanzinfos über Knoten ausgetauscht werden, die sich nicht in der Nachbarschaft befinden.
- Link-State
  Jeder Knoten ermittelt Distanz zu den unmittelbaren Nachbarn. Die Infos werden an alle Knoten verteilt.

4.24 Wieso Ad-Hoc Routing?

Netze mit sehr hohen Änderungsraten erlauben keine strukturierten Ansätze zur Wegauswahl. Ändert sich die Topologie noch während die Wegauswahlprozesse laufen, müssen Wegeenscheidungen neu getroffen werden. Dabei ist der Verwaltungsaufwand gemessen am Erfolg zu hoch.

Ausweg
Nutzdaten werden über das Fluten an alle Knoten verteilt.

4.25 Ad-Hoc Routing und andere Routing Verfahren aufzählen

- Destination Sequenced Distance Vector (DSDV)
  Nachfolger von Distributed Bellman Ford (DBF)
  Proaktive
  Distance-Vector
- Dynamic Source Routing (DSR)
  Reaktive
- Optimized Link State Routing (OLSR)
  Link-State Verfahren
- Link Reversal Routing (LRR)
  Wegeinfo mit Hilfe von Directed Acyclic Graph (DAG)
- Full- Reversal Verfahren
- Partial-Reversal Verfahren
- Höhenbasiertes Partial-Reversal-Verfahren
  Referenzhöhe Alpha (Reference Level)
  Delta-Höhe Beta (Delta-Level)
  Eindeutigen Knotenkennung i
- Lightweight Mobile Routing(LMR)
- Temporally-Ordered Routing Algorithmn (TORA)
  Statt 3er Tupel 5-Tupel

4.26 Erklärung DSDV & DBF

4.27 Wie genau funktioniert Dynamic Source Routing (DSR) ?

- Reaktives Verfahren
- Source-Routing Verfahren
- Wege werden nur bei Bedarf berechnet
- Sender ermittelt den gesamten Weg zum Ziel und hinterlegt diese Info im Paket
- Auch für Unidirektionale Verbindungen geeignet

- Alle Informationen im Paket sind auch für die “Transport-Knoten” nutzbar und im Cache dieser Knoten speicherbar

Route Discovery Protocol
Sender kann hiermit einen möglichst optimalen Weg zum Ziel ermitteln. Das Verfahren garantiert dies aber nicht.

Route Maintenance Protocol
Ermittelt ob der ermittelte Weg noch benutzbar ist. Stellt sich während des Transportes raus, das der Weg nicht mehr brauchbar ist, so wird dies dem Sender mitgeteilt.
Der Sender ermittelt dann einen neuen Weg.

4.28 Was passiert wenn eine Verbindung bei DSR gelöscht wird?

Der letzte noch erreichbare Knoten schickt ein ERROR-Paket an den Sender zurück. Jeder Knoten, der das ERROR-Packet weiterleitet, löscht alle Cache Einträge, in denen die gelöschte Verbindung vermerkt ist.

Erhält der Sender das ERROR-Paket, so muss dieser ein Route Discovery durchführen um einen neuen Weg zu ermitteln.

4.29 Was genau wird gelöscht bei DSR ?

Natürlich nur die Routingstrecke über die unterbrochene Verbindung. Wird ein Weg nicht mehr nutzbar, so wird ein ERROR-Packet versendet. Jeder Empfänger löscht die Cache Einträge zu diesem Ziel.

4.30 Welche Informationen sind in den Paketen von DSR enthalten?

Neben Zieladresse auch Quelladresse („Source“), sowie die Hops. Das bedeutet das die komplette Wegeinformation in dem Packet enthalten.

4.31 Erklärung OLSR

- Link-State Verfahren
- Proaktiv
- Jeder Knoten enthält Topologie des gesamten Netzes

Ablauf von OLSR

1) Suchen von Nachbarknoten
   Aussendung von „Hello-Paketen“. Ein Knoten in Reichweite muss anworten. Aus dieser Anwort kann der Knoten die Existenz des Nachbarn erkennen.
2) Messen der Distanzen zu den Nachbarknoten
   Über „Echo-Pakete“ an alle Nachbarn wird die Distanz ermittelt, d.h über Laufzeit oder Anzahl der Zwischenschritte
3) Erzeugen eines Kontrollpaketes
   Aus Distanzinfo wird ein Kontrollpaket erzeugt (TC Topologie Control Message)
   TC enthaltenKnotenadresse,Sequenznummer, Liste der Nachbarn mit Distanzen)
4) Senden des Kontrollpaketes an alle Knoten des Netzwerkes
   TC über Fluten verteilen. Das Paket wird vernichtet, wenn die Sequenznummer schon vorhanden ist
5) Erstellen eines Abbilds der Netzwerktopologie
   Tabellen für die Wegeauswahl können erstellt werden (z.B: Alg. von Dijkstra)

Multipoint Relays
Weiterleitung von Kontrollpaketen
Grundgerüst für die spätere Wegauswahl

4.32 Erklärung LRR

- Einfache Wegfindung, muss nicht optimal sein
- Kontrollnachrichten werden reduziert
- Auf Fluten von Distanzinfos wird verzichtet

- Geeignetet für Topolgogien die sich schnell ändern
- Weginfo mit Hilfe von Directed acyclic graphs (DAG)

Ein zieldisorientierter DAG kann in einen zielorietierten DAG transformiert werden, indem die Orientierung einiger Kanten umgekehrt wird.

4.33 Was ist ein Directed Acyclic Graph (DAG)?

zielorientierte DAGs
Nur der Zielknoten besitzt keine Downstreams
(Pfeil nach aussen ! == Downstreams).

zieldisortierte DAGs
Gegenteil von zielorientierten DAGs

DAG Eigenschaften
Jedes Paar von Knoten, die sich in gegenseitiger Kommunikationsreichweite befindet, wird duch eine gerichtete Kante verbunden.
Der Graph ist frei von Zyklen

Für jeden möglichen Knoten wird eine eigenenr zielorientierter DAG aufgebaut
Ein Paket wird immer über die Downstreams weitergeschickt

Zielorietierte DAGs stellen sicher, das kein Paket in einer Sackgasse landet, d.h. der Graph frei von Zyklen ist und nur der Zielknoten besitzt als einziger keine Downstreams.

4.34 Full-Reversal Verfahren

Hat ein Knoten nur noch Upstreams, so werden alle Kanten gedreht ! (Ohne Zielknoten)
Bis ein zielorientierter DAG ensteht

4.35 Partial-Reversal-Verfahren

Auch listenbasiertes Partial-Reversal Verfahren
Alle Downstream umdrehen, wenn noch kein Liste erstellt worden ist,sonst nur die Kanten drehen, die noch nicht in der Liste enthalten sind.

4.36 Höhenbasiertes Partial-Reversal-Verfahren

Zielknoten hat von allen Knoten die geringste Höhe

Höhe eines Knotens
Referenzhöhe α_i - (Reference Level)
Delta Höhe β_i - (Delta Level)
Eindeutige Knotenkennung i

$N_I > N_J$
α +1
β -1

Kann zu einem zieldisortiertem DAG führen, wenn in mehrere nicht verbundene Teile zerfällt.

4.37 Erklärung TORA

Weiterenwicklung des Höhenbasiertes Partial-Reversal-Verfahren.
Löst das Problem partitionierter Netze

Flag Reflextion
Feld Orginator

(c) Jens.Schneider@fernuni-hagen.de

5-Tupel

4.38 Erklärung LMR

Löst das Problem partitionierter Netze
Benutzt gerichtete und ungerichtete Kanten

Start: Nur der Zielknoten besitzt gerichtete Knoten (Upstream)
Anfragepaket (QRY)
Kennt ein Knoten schon ein Weg ? --> RPY

Wenn ein Knoten alle Downstreams verliert, muss ein Failure Query (FQ) versendet werden.
Die Kanten verlieren dann ihre Richtung.

4.39 Dienstsuche in kleinen Netzen (WPANs)

Information Access Service (IAS) - IrDA
Service Discovery Protocol (SDP) - Bluetooth

Bestandteile
Dienstnutzer, Dienstvermittler, Dienstanbieter, Dienstdatenbank

Aktion
Dienstregistrierung, „Suche Geräte in Reichweite“, Dienstsuche, Dienstnutzung

4.40 Dienstsuche in grossen Netzen

Service Location Protokol (SLP)
Protokolle
Benutzt TCP UDP, Multicast IP

Scopes
(Admin Scopes/ Wählbare Scopes) bei grössen Netzen. SLP nutzt Schema ähnlich URL

Bestandteile
Dienstnutzer, Dienstvermittler, Dienstanbieter, Dienstdatenbank,

Aktion
Suche Dienstvermittler, Dienstregistrierung, „Suche Dienstvermittler“, Dienstsuche, Dienstnutzung

---

Java Intelligent Infrastructure (JINI)
Protokolle
Benutzt TCP UDP, Multicast IP
Bestandteile
Dienstnutzer,Lookup-Dienst, Dienstanbieter
==> Kommunikation über Dienstinterface(s)

Aktion
Dienstanbieter Discovery, Join, Dienstnutzer Discovery, Dienstnutzer Lookup, Dienstanbieter Dienstnutzung

4.41 Ablauf Registierung und Dienstnutzung von JINI

Fünf Schritte nötig

1) Discovery Dienstanbieter
   Lookup Dienst wird ermittelt
2) Join (Registrierung einers Dienstes)
   Dienst wird in Lookup Dienst eingetragen
3) Discovery Dienstnutzer
   Dienstnutzer ermittelt Lookup-Dienst
4) Lookup
   Dienstnutzer übermittelt gewünschte Kriterien für Dienst. Rückgabe sind mehrere Dienste die auswählbar sind.
5) Dienstnutzung
   Über Dienstinterface kann der ausgewählte Dienst genutzt werden.

4.42 Wie wird ein Lookup Dienst im Netzwerk von JINI gefunden?

Multicast Request Protocol
Über Multicast Pakete wird der Lookup-Dienst im Netzwerk gesucht

Multicast Announcement Protocol
Der Lookup-Dienst macht über Multicast Pakete auf sich aufmerksam

Unicast Discovery
Der entfernte Rechner muss bekannt sein. Keine Suche im eigentlichen Sinne

4.43 Über welchen Mechanismus nutzen Jini-Clients einen Dienst?

RMI über ein Dienst-Interface

4.44 Welche Daten werden bei einer JINI Join (Registrierung) übermittelt?

- Dienstkennung UUID 128 Bit Nummer
- Dienstinterface RMI
- Attribute, die den Dienst spezifizieren

4.45 Wie nennt man die zeitliche Begrenzung bzw. die Verlängerung bei JINI?

Die Registrierung enthält eine zeitliche Begrenzung, der sog. Lease.
Diese zeitliche Begrenzung lässt sich über „Lease Renewal“ verlängern.

4.46 Wie werden im SLP Protokoll die Directory Agents gefunden ?

1) Potentieller Dienstnutzer senden an eine bestimmte Multicast Gruppenadresse ein Paket
2) Directory Agents können periodische Multicast senden
3) DHCP kann Informationen über das Netzwerk enthalten.

4.47 Weitere Systeme zur Dienstvermittlung aufzählen

1) Universal Plug an Play (UPnP)
   Simple Service Discovery Protocol (SSDP), verwendet Control Points
2) Secure Service Discovery Service (S SDS)
   Ziel: Dienstvermittlung, Authentifikation von Dienstnutzer und Dienstanbieter durch Certification Authority (CA)
   Capability Manager (Welcher Dienstnutzer darf welchen Dienst wie nutzen ?)

5 KE 5 - Positionsbestimmung

5.1 Warum reicht es bei der Satellitennavigation nicht aus, die Entfernungsdaten von drei Satelliten auszuwerten?

Die Uhren der Benutzer und der Satelliten laufen nicht streng synchron.

5.2 Was versteht man unter SA bei dem GPS-System?

Selective Availaibility

Künstliche Verfälschung der Zeitsignale, um eine genaue Positionsmessung zu verhindern.

5.3 Womit werden bei DGPS die Korrekturdaten übermittelt?

Per Basisstationen auf der Erdoberfläche

5.4 Womit werden bei WAAS die Korrekturdaten übermittelt?

Per geostationären Satellit

5.5 Über welche Basisverfahren ist eine Positionsbestimmung in Gebäuden möglich?

- Infrarot
- Funk
- Ultraschall
- Visuell

5.6 Wie kann in GSM-Netzwerken die Position bestimmt werden, ohne Änderungen an den Basisstationen oder Endgeräten vornehmen zu müssen?

Zellen genaue Positionsmessung über das VLR-HLR
Positionsmeldungen an den Mobilen Teilnehmer über Cell Broadcast Channels

5.7 Welches Basisverfahren zur Positionsmessung wird bei Positionsbestimmungen im WLAN verwendet?

Signalstärke

5.8 Warum können aktuelle Netzwerke nicht auf einfache Weise die geographische Position als Zieladresse verwenden?

Aktuelle Netzwerke verwenden zur Addressierung die Netzwerktopologie, die nicht auf einfache Weise auf die geografische Position abgebildet werden kann.

5.9 Welche Kategorien der Positionsbestimmung gibt es? Unterschiede ?

Tracking
Person/ Objekt trägt ein TAG. Das TAG wird vom Netzwerk erkannt. Das Positionssystem kann daraus die Position ermitteln

Positioning
Eine Person/Objekt ermittelt mit Hilfe von sendenden Baken/Beacons selber die eigene Position. Die Positionsdaten sind im Gegensatz zum Tracking relative gut gegen anderen Benutzer geschützt.

5.10 Wie lauten die grundlegenden Verfahren der Positionsbestimmung?

- Cell of Origin – COO
  Funksignal hat nur begrenzte Reichweite, Zellstruktur,
- Time of Arrival – TOA / Time Difference Of Arrival - TDOA (bei GSM E-OTD)
  Zeit zwischen Aussendung und Empfang eines Signals kann gemessen werden (300 000 km/s Lichtgeschwindigkeit)
- Angle of Arrival – AOA
  Durch Richtfunkantennen kann die Position eingeschränkt werden.
- Visuell
  Zum Beispiel Einsatz in einem Leuchturm?
- Signalstärke
  Messung der Signalstärke kann grob auf die Position gemessen werden. Signalstärke wird allerdings z.B. durch Hindernisse verändert.

5.11 Welche Positionsdaten können gemessen werden?

- Längengrad, Breitengrad, Höhe
- Relative Position zu einem gegebenen Punkt
- Orientierung im Raum (Roll-Pitch-Yaw), meist Winkel Himmelsrichtung, können die meisten Positionssysteme nicht
- Geschwindigkeit (Direkt über Positionsbestimmung & zeitl versetzte Positionsmessung p, q über Δt

Seite 243 v =
Bedeutung der aktuelle Position, direkte sematische Position oder über Karten

Location Awareness ==> Positionsdaten berücksichtigen!

5.12 Welche Messfehler gibt es?

Eingesetzte Verfahren zur Positionsmessung

- Umgebungsbedingungen(auch Tageszeit)
- Genauigkeit der Verfahren und Fehlerquellen
- Uhrfehler
- Schwankung der Umlaufbahn
- Störung der Atmosphäre (Druck und Wetter)
- Störung der Ionosphäre (geladenen Ionen stören die Signalausbreitung)
- Multipath Fehler(reflektierende Signale in der Umgebung des Empfängers)

5.13 Was kann nicht über GPS gemessen werden?

Winkelmessung über GPS nicht möglich.

5.14 Satellitenanavigation erklären

Also GPS und die Funktionsweise. Ich habe das Bild aus dem Skript
aufgezeichnet und erläutert.

5.15 Warum ist die Zeitmessung bei der Positionsmessung ein kritischer Punkt?

- Lichgeschwindigkeit sehr hoch
  (300 000km/s 1µs == 300m Unterschied)
- Satellit mit Atomuhr
  Systemzeit == genaue Zeitmessung
  Übertragung der Zeit zum Empfänger nur mit Lichgeschwindigkeit möglich

5.16 Welche Entfernung wird bei GPS gemessen?

4 Satelliten == Es wird die Pseudoentfernung gemessen

- Systemzeit (ts,tu)
- lokal ermittelte Zeit (Dach Δts = ts + δts)
- exakte Systemzeit Laufzeit r = c * Δ t Δ t = Dach tu – Dach ts
- Ermittelte Laufzeit Dach ts + Δ Dach t == Dach tu
- exakte Entfernung r = c * Δt = c *(tu – ts)

Pseudoentfernung

$$p = \sqrt{(s_x - u_x)^2 + (s_y - u_y)^2 + (s_z - u_z)^2} + c * \vartheta t_u$$

4 Unbekannte
Lösung (geschlossene Lösungen, Kalmann Filter, iterative Nährungslösungen über Taylor Reihen)

5.17 Wie funktioniert das GPS (Global Positioning System)?

Erklärung Pseudoentfernung
3 Satelliten bilden genaue Schnittstellen (zwei Schnittstelle) Kugeloberfläche
Mobiles Gerät enthält keine Atomuhr!
4. Satelliten zum Ausgleich (Ausgleich Uhrenfehler Mobiler Benutzer)
Gleichung mit 4 Unbekannten lösbar (siehe oben)
CDMA , jeder Sat. eigener PRN Code !, Empfänger kennt alle Codes)
==> Signallaufzeit, zusätzliche Daten
GPS Geschwindigkeit in drei Dimensionen möglich
Doppler Effekt durch Frequenzverschiebung bei bewegten Objekten
Ermittler einer exakten Uhrzeit möglich (Nebenprodukt)

Winkelmessung über GPS nicht möglich

5.18 Wie funktioniert DGPS (Differential Global Positioning System)

Kontrollstation am Boden sendet Korrektur-Signal pro Satellit über Funk an Empfänger im Umkreis (Stichwort Pseudoentfernung)

Basisstation(Korrektursender), terrestrischer Sender
Basisstation führt GPS Messung selber durch ==> Differenz
Differenz für Mobile Benutzer ähnlich
Der Basissation wird die Differenz mitgeteilt
Enfernung zwischen Basisstation und Mobilen Benutzer darf nicht zu gross sein.
Korrekturdaten müssen zeitnah mitgeteilt werden.

Ablauf Theorie
Basisstation bestimmt eigene Position (bx, by, bz) anhand von GPS
Basissation zieht von der bekannten präzisen Position ab und erhält Diff
Benutzer addiert die Korrekturdaten zur eigenen GPS Position hinzu
Genaure Position für den mobilen Benutzer

Einschränkung
Basissation und Benutzer müssen sich die gleichen Satelliten aussuchen
Einwegkommunikation
Zu viele Kombinationen möglich !

Lösung
Korrektur der Pseudo-Entfernung:

Ablauf
Basissation misst Pseudo-Entfernung zu jedem Satelliten (Formeln)
Basissation sendet jeden Sat. einen Korrekturwert
Benutzer ermittelt Pseudo-Entfernung zu jedem Sat.

Benutzer zieht Korrekturwert von eigenm Pseudo-Entfernung ab.
Fehler heben sich auf

Format zum Versenden der Korrekturdaten ==> RTCM-104
Genauigkeit auf 1 bis 3 m
Häufig an der Küste (UKW und Langwelle)

5.19 Wie funktioniert WAAS (Wide Area Augmentation System)

Senden des Korrektursignals über geostationäre Satelliten, die genau einen bestimmten Bereich abdecken
Geostationärer Satelliten Korrekturdaten
30 Monitorstationen in der USA
Monitorstationen berechnen Korrekturdaten ==> Master Control Station ==> Immarsat 3 Sat geostationär
Geostationär == immer derselbe Bereich wird mit Korrekturdaten versorgt
Sendet auf L1 Frequenz und verwendet einen nicht verwendeten PRN-Code
EGNOS funktioniert ähnlich

5.20 Welche Systeme zur Positionsdatenbestimmung gibt es sonst noch?

Reine Satellitennavigation

- Global Positioning System (GPS)
- Globalnaya Navigationnaya Sputnikovaya Sistema (GLONASS)
- GALILEO – Europäisch, ähnlich GPS bis 2008

Satellitennavigation mit terrestrischen Korrektursendern

- Differential GPS (DGPS)
  GPS Satelliten
  Basissationen/Korrektursender

Satellitennavigation mit geostationären Sendern

- Wide Area Augmentation System(WAAS)
  GPS Satelliten
  Monitorstationen senden zu der Master Control Station
  Geostationäre Satelliten (Immarsat-3)
- European Geostationary Navigation Overlay System(EGNOS)
  Nutzt GPS und GLONASS
  Ähnlich WAAS
  bis 2005 fertig ?

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

Positionsbestimmung - Satellitennavigation
Satellitennavigation ausführlich erklärt
Laufzeitbestimmung, Kugelschalenschnitt, Uhrenproblematik,
Lösungsverfahren (nur ansprechen, nicht genau erklären).
r = c * Δt (echte Enfernung)
P = c * Dach Δt (Pseudoentfernung)

$$p = \sqrt{(s_x - u_x)^2 + (s_y - u_y)^2 + (s_z - u_z)^2} + c * \vartheta t_u$$

5.22 Wie kann die die Genauigkeit zu erhöht werden?

Mehr Satelliten, DGPS, WAAS erklärt.
Bildung des Korrekturfaktors pro Satellit.

5.23 Was wird eigentlich genau korrigiert?

???

6 KE 6 – Sicherheit in mobilen Netzen / Mobile Endgeräte

6.1 Die RSA Verschlüsselung beschreiben

Potenzierung mit nachgeschalteter Modulo Bildung

Verschlüsselung
C(iffrat) = M(essage) hoch e mod n

Entschlüsselung
M(essage) = C(iffrat) hoch d mod n

6.2 RSA - Geben Sie für die Primzahlen p=3, q=11 ein RSA-Schlüsselpaar an. Wählen Sie dazu ein e mit e <= 6

1) Geheime Primzahlen bilden
   p = 3, q =11
2) n = p*q = 3*11 = 33
3) Φ(n) = (p-1) * (q -1) = (3-1)*(11-1) = 20
4) e wählen
   ggT(e, Φ (n)) =1
   1 < e < Φ (n)
   e = 3

TODO

6.3 RSA - Ein Sender, dem Sie den Schlüssel aus Teil 1 gegeben haben, möchte die Nachricht M=15 an Sie versenden. Welche verschlüsselte Nachricht C erhalten Sie

TODO

6.4 RSA - Sie erhalten eine verschlüsselte Nachricht C=19. Wie lautete die ursprüngliche Nachricht M?

TODO

6.5 RSA - Sie fangen eine Übertragung C=4 ab und wissen, dass der öffentliche Schlüssel (e, n)=(3, 15) ist. Versuchen Sie die Nachricht zu "knacken" und den Wert M des Klartextes zu ermitteln.

TODO

6.6 Sicherheit - Nennen Sie mindestens drei Eigenschaften oder Zielsetzungen, die unter dem Begriff "Sicherheit" verstanden werden.

- Vertraulichkeit
- Authentizität
- Integrität aber auch Nicht-Anfechtbarkeit
- Zugriffssteuerung
- Verfügbarkeit

6.7 Sicherheit - Was versteht man unter dem Begriff "Security through obscurity"?

“Sicherheit” durch Geheimhaltung der verwendeten Verfahren

6.8 Sicherheit - Nennen Sie ein symmetrisches und ein asymmetrisches Verschlüsselungs-verfahren

Symetrisch
DES, TDEA, AES
Asymetrisch
RSA

6.9 Sicherheit - Wie bezeichnet man die Schlüssel bei symmetrischen Verfahren, wie bei asymmetrischen Verfahren?

Symmetrische Schlüssel
Secret Key

Asymmetrische Schlüssel
Private Key
Public Key

6.10 Sicherheit Bei welcher Art kryptographischer Angriffe ist die Schlüssellänge von entscheidender Bedeutung?

Brute Force Attack

6.11 Sicherheit Welche Funktionen werden für digitale Unterschriften verwendet?

Hashfunktionen

6.12 WAP - Aus welchen Teilprotokollen besteht WTLS?

- Handshake-Protokoll
- Change-Cipher-Protokoll
- Alert-Protokoll

6.13 OBEX /SyncML - Was verbirgt sich hinter dem Begriff "Nonce"?

Einweg Schlüssel bei dem Challenge Response Verfahren

6.14 Was wird bei Bluetooth unter "Pairing" verstanden?

Aushanndeln eines Link-Keys zwischen zwei Geräten, die noch keine gemeinsamen Schlüssel ausgehandelt haben

6.15 Wie kann im WLAN eine Authentifikation mit Hilfe von Challenge Response durchgeführt werden ?

Die Station schickt an den Empfänger eine unverschlüsselte Zufallszahl. Diese Zufallszahl wird von dem Empfänger verschlüsselt und zurückgeschickt. Da der Empfänger und der Sender das geheime Passwort kennen müssen, kann die Station die unverschlüsselte Zufallszahl auch mit dem geheimen Passwort verschlüsseln. Stimmen beide Verschlüsselte Werte überein war die Authentifikation erfolgreich.

6.16 Wie funktioniert WEP (Wired Equivalent Privacy)?

Sender

1) Initialisierung Vektor (IV) als Klartext im Paket hinterlegen. Der IV sollte bei jedem Paket geändert werden
2) Nutzdaten mit ICV (CRC32) anreichern
3) Zufallszahl mit PRNG(RC4) erzeugen. Eingabe ist der Geheime Schlüssel und der IV
4) Mit Zufallszahl die Nutzdaten XOR verschlüsseln (Stromchiffre)

Empfänger

Der Empfänger erhält den IV als Klartext. Der geheime Schlüssel ist auch dem Empfänger über einen sicheren Kanal mitgeteilt worden. Über den eine 128 Bit Zahl kann Authentifziert werden(Über Challenge Response Verfahren)

6.17 Wie wird in Bluetooth der temp. Initialization key erzeugt ?

PIN + Zufallszahl als Eingabe in E22
Dem zweiten Gerät wird im Klartext die Zufallszahl mitgeteilt. Im Zweiten Gerät wird die PIN eingeben

6.18 Welche Link-Keys gibt es bei Bluetooth?

Unit Key

Zufallszahl + Geräteadresse und E21. Unit Key wird mit XOR und em Initialization Key an das andere Gerät gesendet.

Combination Key

Für jedes Paar von Geräten unterschiedlich. Grössere Hürde für Angriffe

Master Key

Aus mehreren einzelnen Verbindungsschlüsseln kann ein Master key erzeugt werden. Dieser wird für Broadcast im Piconet verwendet

6.19 Authentifzierung in Bluetooth beschreiben

1) Verifier sendet Zufallszahl an Claimant
2) Link Key + Claimant Geräteadresse mit Funktion E1
3) Ergebnis an Verifier senden
4) Vergleichen, ob Ergebnis von Claimant gleich Verifier
5) Ungleich, dann muss vor neuer Authentifzierung gewartet werden

6.20 Verschlüsselung in Bluetooth beschreiben

1) Ciphering Offset (COF) aus ACO der Authentifizierung erzeugen
2) Encryption Key erzeugen über E3 (Zufallszahl, COF,Link Key)
3) Encryption Key + Uhrzeit + Geräteadresse mit E0
4) XOR mit Nutzdaten

6.21 GSM-Mobiltelefonie Challenge Response Verfahren aufmalen?

Die Authentifizierung erfolgt bei GSM mit Hilfe des Challenge Response Verfahren

1) Der Provider schickt Zufallszahl an das Mobilfunktelefon

2) Anhand der IMSI des Mobilfunktelefons kann Ki von dem AUC erfragt werden
3) Mobilfunktelefon ermittelt aus Ki und der Zufallszahl mit K3
4) Rücksenden des Wertes zum Provider
5) Provider vergleicht erzeugte Werte

K3 wird auf der SIM-Karte ausgeführt. Nur das Ergebnis ist auslesbar.

6.22 Wie wird die Verschlüsselung bei GSM durchgeführt ?

1) Provider schickt nachd er Authentifzierung wieder eine Zufallszahl an das Mobilfunktelefon
2) Geheimer Schlüssel ki + Zufallszahl A8
3) Ergebnis ist Kc als Eingabe von A5
4) XOR mit Nutzdaten
5) Versendung an Netzbetreiber

6.23 Warum kann dier Verschlüsselung ohne A3 und A8 in einem fremden Netz durchgeführt werden?

RAND und Kc kann nach der Authentifizerung bei dem AUC des Heimat Providers abgefragt werden.
A5 ist über alle Netze gleich implementiert

6.24 GSM-Mobiltelefonie Warum A3, A8 auf der Karte ?

Der geheime Schlüssel ist somit nicht auslesbar
K5 ist nicht veröffentlich
Mit der Kenntnis von Ki kann ein Duplikat der SIM-Karte erstellt werden, da die IMSI auslesbar ist

6.25 GSM - Welche kryptographischen Algorithmen sind bei GSM auf der SIM-Karte untergebracht?

- A3 Simkarte (bei manchen Mobilfunkbetreibern COMP128)
- A8 Simkarte (bei manchen Mobilfunkbetreibern manchmal COMP128)

- A5 Handy Standard für alle Netze – Encryption Funktion ist nicht veröffentlich worden !!

6.26 GSM-Mobiltelefonie Sicherheitsziele aufzählen

- Nur die Mobile Station wird authentifiziert
- Abhörsicherheit der Luftschnittstelle
- Es soll kein Tracking (Bewegungsprofil) der Mobilen Station von aussen möglich sein. Man-In-The-Middle über IMSI-Catcher Möglich. Der IMSI-Catcher fordert die Mobile Station auf, die Verschlüsselung auszuschalten

6.27 WLAN - Welche Sicherheitskonzepte erlaubt IEEE 802.11?

1) MAC-Filterung auf dem Access Point. MAC Adressen lassen sich bei moderen Karten ändern
2) Geheimes Passwort kennt der Access Point(AP) und die Mobile Station. Hierbei ist eine Authentifikation möglich.Alle Pakete werden mit dem geheimen Passwort über ein symetrisches Verfahren verschlüsselt

6.28 WLAN - Welche Schlüssellängen kennt WEP / WEP2

WEP
40 Bit Schlüssel + 24 Bit IV == 40 Bit Verschlüsselung bei WEP
104 Bit Schlüssel + 24 Bit IV == 128 Bit Verschlüsselung bei WEP
WEP 2
128 Bit Schlüssel + ?? IV bei WEP 2

6.29 WLAN - Welche Sicherheitslücken bestehen bei WEP (Wired Equivalent Privacy)

- Geheime Schlüssel stehen im Widerspruch zu Hot Spots
- 40 Bit Schlüsselraum zu klein
- IV (Initialisierungvektor) wird von einige Karten gar nicht oder zu selten gewechselt. Statistische Analyse sehr einfach
- RC4 (PRNG) nicht sicher. Bei wenigen Schlüsselbits kann auf die gesamte Ausgabe geschlossen werden
- 24 Bit IV bildet zu weniger Permutationen für eine hinreichend grosse Zeitspanne. Bei hoher Netzlast wiederholt sich der IV schon nach einigen Stunden. Erraten von Klartextbits des ersten Pakets. Wörterbücher für alle IV können gesamelt werden.
- An den AP können unverschlüsselte Klartexte gesendet werden. Damit erhält der Angreifer auch die verschlüsselte Chiffre
- CRC „Linearität" Bits können verändert und der CRC neu berechnet werden. Dazu ist nur die Kenntnis von wenigen Klartext Bits notwendig
- WEP2 (> 1999) enthält 128 Bit Schlüssel (aber alten RC4 Algorithmus)
  ==> Absicherung durch höhere Protokolle notwendig (z.B. WTLS)

6.30 Welche Kategorien mobiler Endgeräte kann man unterscheiden?

- Mobile Standard-Computer
- Bordcomputer
- Handhelds
- Wearables
- Chipkarten

6.31 Unterschiede zwischen Notebook und stationärem Computer beschreiben

- Anderer Bildschirm
- Unterschiedliche Tastatur
- Andere Eingabegeräte (Zeiger)
- Stromversorgung
- Laufwerke
- Erweiterungskarten

6.32 Was verbirgt sich hinter dem Begriff Drive-by-Wire?

Indirekte Steuerung von Fahrzeugen über elektronische Stellglieder

6.33 Für welche Anwendungsgebiete sind Chipkarten geeignet?

- Identifikation
- Digitale Unterschrift

6.34 Was ist ein Digitizer?

Eingabeeinheit von PDAs die berührungsempfindlich sind

6.35 Warum sind traditionelle Handschriften für die Eingabe ungeeignet?

Von Benutzer zu Benutzer unterschiedlich
Bei einem Benutzer auch noch verschieden

6.36 Welche Betriebsmodi kennen PalmOS-Geräte?

- Sleep Mode
- Doze Mode
- Running Mode

6.37 Was wird alternativ zu Dateien unter PalmOS verwendet?

- Resourcen
- Datenbanken

6.38 Nennen Sie drei Unterschiede der PalmOS-Entwicklung zu der Entwicklung für Desktop-Computer

- Bildschirmgrösse
- Interaktionsrate

- PC-Konnectivität
- Eingabemethoden
- Energieversorgung
- Speicher
- Dateisystem
- Abwärtskompatibilität

6.39 Was versteht man unter OAL von Windows CE?

OEM-Abstract Layer (OAL)
Trennt den Betriebssystemkern von der Hardware ab.

7 KE 7 – Datenübertragung in mobilen Umgebungen / Plattformen und höhere Dienste

7.1 Über welche Angaben kann ein OBEX-Teilnehmer den Typ eines Objektes erkennen?

- Endung des Dateinamen
- Mime-Typ

7.2 Mit welchem Verfahren werden OBEX-Sitzungsteilnehmer authentifiziert?

Challenge-Response

7.3 Wie kann die Authentifizierung von OBEX überlistet werden?

Man-In-The-Middle. Übernahme der authentifizierten Sitzung auf niedriger Protokollebene

7.4 Nennen Sie drei Arten der Synchronisation unter SyncML.

Zwei-Wege
Client und Server teilen sich nur die partielle Änderung mit

Langsame
Client und Server gleichen alle Daten Feld für Feld ab

Einweg (Client oder Server)
Senden der partiellen Änderungen nur in eine Richtung. Überschreibt evtl. vorhandende Daten

Erneuerung (Client oder Server)
Senden alle Felder in eine Richtung. Sonderfall von der Einweg
Serverinitiierte
Der Server fordert den Client auf eine Synchronisation zu starten. Der Client startet im Normalfall eine Synchronisation

7.5 Wer übernimmt in SyncML die Vergabe lokaler IDs (LUIDs)?

Client

7.6 Wer verwaltet in SyncML die Zuordnung globaler IDs (GUIDs) zu lokalen IDs (LUIDs)?

Server

7.7 Welche Datenverändernden Tags sind in SyncML definiert?

<add>
<copy>
<delete>
<replace>

7.8 Welche Versit-Formate gibt es?

- vCalender
- vCard
- vNote (selten)
- VMessage (selten)

7.9 Welche Wiederholung wird im vCalender-Format durch MD1 2- #3 definiert?

Jeder Vorletzte des Monats, drei Monate lang

7.10 Welche Wiederholung wird im vCalender-Format durch YD1 32- #3 definiert?

Jeder 30.November, 3 Jahre lang

7.11 Welche Ebenen umfasst der WAP-Protokollstapel?

- WAE
- WSP
- WTP
- WTLS
- Transportschicht, Bearers

7.12 Was ist die Aufgabe von WTP in WAP?

Zuverlässiger Nachrichtentransport

7.13 Welches Sicherheitsprotokoll verwendet WAP?

WTLS

7.14 Wo ist der Schwachpunkt des WAP-Sicherheitskonzepts?

Der WAP-Proxy. Hier liegen die Daten kurzzeitig unverschlüsselt vor.

7.15 Wie nennt man die WML-Einheit, die als Ganzes auf einem WAP-Gerät dargestellt werden kann?

Card (Karte)

7.16 Was entspricht einer WML-Datei?

Deck (Kartenstapel)

7.17 Wie erfolgt die Authentifizierung unter SyncML?

In den Nachrichten werden Challenge-Tags eingeführt. Analog zu OBEX

7.18 Kurze Beschreibung Coda, Rover, QuickStep

<u>Coda</u>

- Netzwerkdateisystem für mobile Rechner mit Desktop Leistung
- Optimistische Strategie über Replay-Log
- Keine automatische Konfliktbehandlung
- Nur Datei als Ganzes
- Keine Mobilitäts- Transparenz

<u>Rover</u>

- Nur Operationen die eine Modifikation bewirkt, wird übertragen
- Objektaustausch
- RDOs
- QRPCs
- Kopien der RDOs im Cache
- Mobilitätsbewusstein, d.h. Anwendung wird spez. für den Mobilen Einsatz angepasst
- Konfliktbehandlung auf dem Server. Die Konfkliktbehandlung steht under der Kontrolle der spez. Anwendungen

<u>QuickStep</u>

- Spez. für kleine mobile Rechner
- Datenaustausch zw. mobilen Benutzern
- Unterstützt die Entwicklung Mobilitätsbewuster Anwendungen
- Satzorientierte Daten(banken)
- Datenschutz integriert
- QuickStep-Server ohne Anwendungsspez. Anteile

- Location / Organisation

- Context Awareness integriert (Wer nutzt was, rudim. Hilfsmittel zur Positionsermittlung)

7.19 Welche Konflikte müssen im Coda-System von Hand gelöst werden?

- Änderung einer Datei durch mehrere Benutzer
- Änderung einer Datei während ein zweiter Benutzer diese gelöscht hat
- Zwei oder mehrere Benutzer legen unterschiedliche Dateien mit unterschiedlichem Inhalt mit dem gleichen Dateinamen an.

7.20 Zustände in Coda und Zustände bei schwacher Anbindung beschreiben

Standard Coda
Hoarding (Änderung direkt auf dem Server) --> Emulating (Cache) --> Reintegration (Replay-Log an Server, Abgleich mit Cache)

Coda für schwach angebundene Clients
Hoarding (Änderung direkt auf Server) --> Emulation (Cache) --> Write Disconnected (Lesen vom Server, Schreiben über Protokoll

Verfahren heisst Trickle Reintegration
Voller Abgleich im Modus Write Disconnected heisst Full Reintegration

7.21 Wie werden Objekte in Rover genannt, die auf verschiedenen Rechner lauffähig sind?

RDOs (Relocation Dynamic Objekts)

7.22 Durch welche Komponenten in QuickStep-System werden private Daten geschützt?

Lebenszeitüberwachung und Anonymisierer

7.23 Wie wird das Problem der Konflikte in QuickStep gelöst?

Es gibt keine Konfikte. Nur die eigenen, selbsterstellten Datensätze darf der Benutzer ändern