

Mobilität im Internet

Wie kommen Mobile Rechner an eine Adresse ?

Dynamic Host Configuration Protocol (DHCP)

- DHCP geht auf BOOTP zurück, dass entwickelt wurde um festplattenlose Rechner in Netzwerke einzubinden ohne diese jedes Mal manuell zu konfigurieren. Der Rechner sucht sich einen Server im Netzwerk, der ihn im Hochlaufen mit den nötigen Parametern versorgt.
- DHCP konzentriert sich darauf, den Rechner mit den netzwerkspezifischen Parametern zu versorgen ist aber BOOTP-kompatibel.
- Eigenschaften:
 - o Ein Rechner (DHCP-Client), der in ein Netzwerk eingebunden wird bekommt auf Anfrage automatisch eine freie IP-Adresse zugewiesen.
 - DHCP-Client wird physikalisch ins Netz eingebunden, da er noch keine Netzwerkparameter kennt sind seine Kommunikationsmöglichkeiten stark eingeschränkt
 - Die Kommunikation baut auf dem unzuverlässigen Transportprotokoll User Datagram Protocol (UDP) auf.
 - Üblicherweise werden Netzwerkparameter beim Booten des Clients gesetzt, damit nach dem Start alle Netzwerkfunktionen genutzt werden können. Dafür muss aber das Betriebssystem zu lassen, dass UDP-Nachrichten noch vor dem kompletten Rechnerstart versendet und empfangen werden können.
 - In Client ohne IP-Adresse kann als Ziel nicht angesprochen werden. Ein Server, der dem Client eine IP-Adresse zuweisen möchte muss deshalb die Nachricht direkt an die MAC-Adresse senden.
 - Relay Agents ermöglichen es DHCP-Anfragen aus Subnetzen ohne eigenen DHCP-Server an Subnetze mit DHCP-Server weiter zu leiten. (moderne Router können als Relay Agents verwendet werden.)
 - Der Client gibt per Broadcast eine Suchmeldung nach einem DHCP-Server aus (DHCPDISCOVER)
 - Der DHCP-Server sendet als Antwort eine mögliche Netzwerkkonfiguration (DHCPOFFER)
 - Manuell: Hierbei wird die DHCP-Anfrage automatisch an den Systemadministrator weitergeleitet, der manuell eine freie IP-Adresse aus einem dazu hinterlegten freien IP-Adressbereiches des Netzes (Scope/Range) vergibt.
 - Automatisch: Eine freie IP-Adresse wird auf unbegrenzte Zeit vom DHCP-Server automatisch vergeben
 - Dynamisch: Eine freie IP-Adresse wird automatisch für eine bestimmte Zeit zugeteilt (Lease). Nach Ablauf der Zeit muss die Anfrage erneut gestellt werden, sonst kann die IP-Adresse erneut frei vergeben werden.
 - o Besonders für mobile Rechner geeignet, da diese sich häufig nicht aus dem nur kurzzeitig genutzten Netz abmelden.
 - o Das Lease enthält 3 Zeiten:
 - Gültigkeit des Leases
 - T1: Zeit nach der der Lease über eine erneute DHCPREQUEST zu erneuern ist.
 - T2: Zeit nach der die erneute DHCPREQUEST für den Lease vom DHCP-Server positiv quittiert worden sein muss, sonst muss ich der Client einen neuen Lease besorgen, wenn er über die Gültigkeit des aktuellen Lease hinaus im Netz bleiben will.

FAQ-Liste Mobile Computing (1679)

- Der Rechner wird mit zusätzlichen Informationen über das Netzwerk versorgt (Subnetmask, Dynamic Name Server (DNS)-Adresse, Router-Adresse)
- Optional werden Informationen zu weiteren Servern des Netzes übertragen (Mailserver, Webserver,..)
 - Nimmt der Client die Netzwerkkonfiguration an, sendet er dem Server eine Anfrage über IP (DHCPREQUEST), mit der er explizit einwilligt, die angebotene Netzwerkkonfiguration zu nutzen
- Die Übertragung der Informationen, sowie die Einstellung der Parameter auf dem Rechner erfolgt vollständig ohne manuelle Konfiguration durch einen Benutzer
- Ein mobiler Rechner muss lediglich in physischen Kontakt mit einem Netzwerk kommen, dass DHCP unterstützt um ihn analog einem stationären Rechner in dieses Netzwerk einzubinden
- Sicherheitsaspekt
 - Die automatische Vergabe von IP-Adressen an fremde Rechner ist sicherheitstechnisch problematisch, da Rechnern aus dem eigenen Netz in der Regel höhere Zugriffsrechte und Privilegien zu stehen, als Rechnern aus anderen Subnetzen, möchte man in der Regel nicht jedem fremden Rechner eine Subnetzadresse zuweisen.
 - Umgekehrt sind sich einbindende Rechner auf die Vertrauenswürdigkeit des DHCP-Servers angewiesen, damit er sie nicht anweist, Nachrichten über nicht vertrauenswürdige Rechner zu leiten.
 - Lösungsansatz ist die gegenseitige Identifizierung von Client und Server vor Vergabe der IP-Adresse. Hierzu sind jedoch MAC-Adressen nur bedingt geeignet, da sie leicht gefälscht werden können.

Warum MobileIP und wie funktioniert es?

- Bietet ein mobiler Rechner selber Dienste an reicht es nicht ihn über DHCP- in ein fremdes Subnetz einzubinden, da er für Dienstanutzer erstmal nicht unter dieser neuen IP-Adresse bekannt und damit unauffindbar ist.
- Bei Mobile IP bekommt ein mobiler Rechner deshalb eine IP-Adresse zugewiesen, die er auch in fremden Netzwerken behält. Er ist damit stets unter einer festen Adresse erreichbar.
- Rechner Typen im Konzept von MobileIP:
 - Mobile Host: Der mobile Rechner, der sich zwischen verschiedenen Subnetzen bewegt und dabei durch eine eindeutige IP identifiziert wird.
 - Corresponding Host: Kommunikationspartner, der Rechner der Kontakt zum mobilen Rechner aufnehmen will.
 - Home Agent: Der Heimagent ist der Rechner im Heimatnetzwerk (Heimnetz) des mobilen Rechners, der den mobilen Rechner dort vertritt, so lange sich der mobile Rechner nicht in seinem ursprünglichen Subnetz aufhält. Der Home Agent ist ständig über den aktuellen Aufenthaltsort des mobilen Rechners informiert.
 - Foreign Agent: Der Fremdagent befindet sich im aktuellen Subnetz (Fremdnetz (Visiting Network)) des mobilen Rechners und leitet eingehende Pakete an den mobilen Rechner weiter.
- 2 Adressen pro mobilem Rechner:
 - Heimadresse: Adresse unter der der mobile Rechner permanent erreichbar ist.
 - Care-of-Adresse: IP-Adresse, die der mobile Rechner in fremden Netzen verwendet
 - Foreign-Agent-Care-of-Adresse: Ein Fremdagent übernimmt die Weiterleitung ankommender Pakete an den mobilen Rechner. Mehrere mobile Rechner können die gleiche Foreign-Care-of-Adresse nutzen

FAQ-Liste Mobile Computing (1679)

- Collocated-Care-of-Adresse: Netzwerkadresse des mobilen Rechners im Fremdnetz wird direkt dem Heimagenten als Weiterleitungsadresse übermittelt. Es gibt keinen Fremdagenten. Die Collocated-Care-of-Adresse ist für jeden mobilen Rechner im Fremdnetz verschieden.
- Arbeitsweise / Verfahren
 - Agent Discovery
 - Über Agent Discovery ermittelt der mobile Rechner zunächst, ob er sich im Heimnetz oder einem Fremdnetz befindet. Gleichzeitig ermittelt er welcher Rechner im Subnetz der Heim-/Fremdagent ist.
 - Agent Advertisement: Die Agenten senden periodisch Broadcastnachrichten an alle Rechner des Subnetzes. Rechner die den Netzwerkverkehr mit hören, können so die Agenten identifizieren
 - Agent Solicitations: Der mobile Rechner sendet eine Aufforderung an alle Rechner des Subnetzes ein Agent Advertisement durchzuführen und erzwingt damit eine Verkürzung der Wartezeit.
 - Wird kein Advertisement empfangen geht der mobile Rechner erstmal davon aus, dass er sich im Heimnetzwerk befindet und der Heimagent gestört ist.
 - Er versucht dann den Router des Heimnetzwerkes zu erreichen um diese Annahme zu bestätigen.
 - Befindet er sich nicht im Heimnetzwerk versucht er daraufhin einen DHCP-Server zu erreichen um eine Subnetzadresse zu erhalten, die er so dann als collocated-care-of-Adresse an seinen Heimagenten weiterleitet.
 - An Hand der Advertisementnachrichten kann der mobile Rechner seinen Standort feststellen, insbesondere kann er feststellen, ob sich sein Standort seit dem letzten Advertisement verändert hat.
 - Registrierung
 - Hat der mobile Rechner eine Care-of-Adresse (über Fremdagent oder eigen), nimmt er zu seinem Heimagenten Kontakt auf und teilt ihm die aktuelle Care-of-Adresse mit. (Registration Request)
 - Der Heimagent führt eine Liste die jedem von ihm vertretenen Mobilien Rechner die jeweils aktuelle Care-of-Adresse zuordnet. Er bestätigt den aktualisierten Eintrag. (Registration Reply)
 - Da theoretisch jeder beliebige Rechner sich als mobiler Rechner ausgeben könnte und so alle Pakete an sich umleiten könnte wird der Registrierungsdialog über einen gemeinsamen geheimen Schlüssel (Message Digest) abgesichert.
 - Kehrt ein mobiler Rechner in sein Heimnetzwerk zurück deregistriert er sich beim Heimagenten und übernimmt seine Datenpakete wieder direkt selber.
 - Eine Deregistrierung ist auch beim Verlassen eines fremden Netzes erforderlich, wenn der mobile Rechner anschl. für eine bestimmte Zeit unerreichbar ist, damit der Heimagent entsprechend reagieren kann.
 - Da Rechner häufig einfach ausgeschaltet werden ohne die entsprechende Deregistrierung vorzunehmen, können Registrierungen für eine bestimmte Zeit vorgenommen werden, sie sind dann vor Zeitablauf für eine weitere Periode zu bestätigen, sonst werden sie automatisch gelöscht.
 - Tunneling
 - Pakete legen auf dem Weg zum mobilen Rechner einen Umweg über den Heimagenten zurück.

FAQ-Liste Mobile Computing (1679)

- Der Kommunikationspartner kennt ja ausschließlich die Heimadresse des mobilen Rechners.
- Befindet sich der mobile Rechner in einem Fremdnetz, nimmt der Heimagent das Paket für ihn entgegen und kapselt es mit einem weiteren Paket,
- das er an die aktuelle Care-of-Adresse weiterleitet (IP-Tunneling).
- Beim Empfänger wird das ursprüngliche Paket wieder entpackt und dem Empfänger übergeben.
 - Bei Foreign-Care-of wird das Entpacken vom Fremdagenten durchgeführt.
 - Beim Collocated-Care-of durch den mobilen Rechner selbst.
- Das Antwortpaket des mobilen Rechners selbst, kann direkt an den Kommunikationspartner versandt werden, vorausgesetzt die Router des Fremdnetzes lassen den Versand von IP-Paketen mit fremden Absenderadressen aus dem lokalen Netz zu. Ist dies nicht der Fall wird auch die Antwort wieder über den Heimagenten getunnelt (Reverse Tunneling). Hierbei packt der Heimagent das Tunnelpaket aus und verschickt das reine Antwortpaket an den Kommunikationspartner.
- Durch das Tunnelverfahren brauchen bestehende Implementierungen nicht geändert zu werden.
- Zukunftsaussichten
 - Das Verfahren ist auf Grund der zahlreichen erforderlichen Zusatzrechner unter IPv4 noch relativ aufwendig, deshalb werden unter IPv6 folgende Vereinfachungen direkt eingearbeitet:
 - Es gibt nur noch collocated-Care-of-Adressen. Der Fremdagent wird damit überflüssig
 - Die Funktionalität des Heimagenten wird in den Heimrouter eingearbeitet, damit entfällt der Heimagent als eigenständiger Rechner.
 - Mobile Rechner informieren involvierte Router, wenn sie sich in ein neues Netzwerk begeben. Das aufwendige Routen über den Heimagenten kann damit entfallen.

Wie funktioniert Cellular IP und warum Cellular IP ?

- Bei MobileIP ist bei jedem Zellenwechsel eine neue Registrierung notwendig. Für cellulare Netze, in den Rechner häufig die Zelle wechseln (z.B. Mobilfunknetze) ist Mobile IP deshalb ungeeignet.
- CellularIP bietet deshalb einen zweistufigen Ansatz:
 - Ein MobileIP-Netzwerk vermittelt Pakete an den mobilen Rechner nur grob an das Netzwerk in dem sich der mobile Rechner aktuell befindet.
 - Erst innerhalb der Netzwerkes werden die Pakete über cellularIP an den mobilen Rechner vermittelt.
 - Der Heimagent wird in der Regel nicht von einem Zellenwechsel informiert, solange sich der mobile Rechner innerhalb eines einzigen Zugriffsnetzwerkes aufhält, müssen nur die Routingtabellen des Zugriffsnetzwerkes angepasst werden.
 - Nur beim Wechsel in ein anderes Zugriffsnetzwerk wird der Heimagent informiert.
 - Die Verbindung von Zugriffsnetzwerk und MobileIP-Netzwerk erfolgt über einen Gatewayrechner, dessen Adresse als foreign-care-of-adresse von den mobilen Rechnern genutzt wird.
- Routing
 - Gatewayrechner sendet periodisch Beacon-Nachrichten im Zugriffsnetzwerk aus, die über Fluten verteilt werden.¹

¹ Fluten: Beim Fluten werden Nachrichten an alle Nachbarn weitergeleitet, außer an den von dem die Nachricht gekommen ist.

FAQ-Liste Mobile Computing (1679)

- Jeder Rechner merkt sich im Routing Cache von welchem Rechner er die Beacon-Nachricht erhalten hat, damit kennt er den nächsten Nachbarn in Richtung Gateway.
- Sendet umgekehrt ein mobiler Rechner Pakete zum Gateway, merkt sich jeder Rechner auf der Route die Adresse des Vorgängers.
 - Mobile Rechner die länger keine Nutzdaten verschicken halten die Route durch RouteUpdate-Nachrichten für das Gateway aktuell
- mit Hilfe der RoutingCaches wird so eine Route vom/zum Mobilten Rechner erstellt.
- Einträge im RoutingCache werden nach der Zeitspanne RoutingTimeOut gelöscht, damit ist gewährleistet, dass alte Routingeinträge für längst wieder abgewanderte mobile Rechner den RoutingCaches nicht belasten.
- Handover (Handoff)
 - Wird vom mobilen Rechner durchgeführt, wenn die Signalstärke zu stark absinkt.
 - 2 Verfahren
 - Hard Handoff: der mobile Rechner sendet beim Zellenwechsel ein Routeupdate zur neuen Basisstation. Alle Rechner auf der Strecke zum Gateway ändern dadurch ihren Eintrag.
 - Rechner die nicht auf der Route liegen insbesondere die alte Basisstation löschen den Eintrag erst nach Routetimeout
 - Semisoft Handoff: der Rechner schaltet nicht direkt hart zur neuen Basisstation um, sondern empfängt eine zeitlang noch Pakete von beiden Basisstationen, um Paketverluste zu vermeiden, bis das RouteUpdate das Gateway erreicht hat. Erst danach werden nur noch Pakete der neuen Basisstation empfangen.
- Paging:
 - Inaktiver Zustand während dem mobile Rechner nicht mehr an der Kommunikation teilnehmen um Batteriestrom zu sparen, in dem die Funkschnittstelle außer Betrieb genommen wird.
 - Der inaktive Rechner sendet jedoch periodisch Page-Update-Nachrichten zum Gateway um die Routinginformationen im PageCache der Rechner auf der Route aktuell zu halten.
 - Page Einträge sind jedoch wesentlich länger gültig als Routeeinträge und müssen deshalb wesentlich seltener versendet werden.
 - Mit Page Paketen meldet ein Gateway einem inaktiven Rechner, dass für ihn Datenpakete vorliegen. Der inaktive Rechner reagiert darauf mit einem Routeupdate und die Datenpakete können zugestellt werden.

Add-Hoc Routing:

Klassifikation der Routing-Verfahren ?

- Adaptive Verfahren automatische Reaktion auf Netzwerkveränderungen - Nicht adaptive Verfahren Routing anhand fester Tabellen (nicht für adHocNetze geeignet)
- Proaktive Verfahren halten Routingtabellen zu sämtlichen Rechnern im Netz vor, selbst wenn noch nie ein Paket geschickt wurde – reaktive Verfahren ermitteln Routen bei Bedarf, d.h. wenn ein Paket versandt werden soll.
- Distance-Vector-Verfahren Knoten tauscht nur mit seinem Nachbarknoten Distanzinformationen über Knoten aus, die sich nicht in der Nachbarschaft befinden – Link State Verfahren übermittlung der Distanzinformationen zum unmittelbaren Nachbarn wird über das gesamte Netzwerk verteilt.
 - Link-State-Verfahren
 - suchen von Nachbarknoten über „Hello“-Pakete. Nachbarn beantworten Hello-Pakete und werden so erkannt.
 - Echo-Pakete messen die Distanz zu den Nachbarn, da diese die Echopakete sofort beantworten müssen. (Verwendet man nur die Anzahl der

FAQ-Liste Mobile Computing (1679)

Zwischenschritte als Distanz kann die Versendung von Echo-Paketen unterbleiben)

- Topology control Message (TC) werden periodisch oder bei Veränderungen der Distanzinformationen erzeugt und enthalten neben der Knotenadresse und der Sequenznummer eine Liste der Nachbarn mit den entsprechenden Distanzen
- Versenden des TC an alle Knoten des Netzwerkes mittels fluten
 - Hat ein Knoten ein bestimmtes TC-Paket schon mal erhalten und weitergeleitet wird es von ihm vernichtet.
- Aus den gesammelten Distanzinformationen kann sich jeder Knoten ein Abbild des Netzwerkes erstellen und z.B. mit dem algorithmus von Dijkstra Tabellen für die Wegeauswahl generieren.

Wieso Add-Hoc Routing?

- Keine feste Infrastruktur die mit vorgegebenen Netzwerkadressen das Routing unterstützt.
- Sehr dynamische Struktur, die Rechner bewegen sich, die Wegeauswahl muss häufig angepasst werden.
- Keine ausgezeichneten Router vorhanden, jeder Rechner muss Pakete weiterleiten können.
- Häufig geringe Reichweite der einzelnen mobilen Kommunikationspartner macht Durchleitung der Pakete erforderlich.

Wie genau funktioniert Dynamic Source Routing (DSR)?

- Reaktives Verfahren
- Route Discovery: ermittelt möglichst optimalen Weg zum Zielknoten.
 - Liegt für den gewünschten Zielknoten kein Eintrag im Cache vor. Wird eine Nachricht an alle Nachbarn versandt, ob diese den Zielknoten kennen, zusammen mit einer Wegeliste, in der der Anfragende Knoten als initiator schon eingetragen ist.
 - Die Nachbarn tragen sich selber auf der Liste als Folgeknoten ein und überprüfen ob sie schon einen Pfad zum Ziel kennen oder selbst das Ziel sind.
 - Kennen sie den Pfad zum Ziel, hängen sie ihn an die Wegeliste an und schicken sie auf dem umgekehrten Weg zurück zum anfragenden Knoten (Route Reply)
 - Gibt es unidirektionale Verbindungen, ist der direkte Rückweg ggf. nicht möglich.
 - Der Rücksender erstellt dann ein RouteDiscoveryPaket zum ursprünglichen Anfrager und hängt das RouteReplyPaket als Information an, damit ist sichergestellt, dass die Antwort ankommt, vorausgesetzt es gibt einen Rückweg.
 - Kennen sie das Ziel nicht, schicken sie die verlängerte Anfrage an alle ihre Nachbarn mit Ausnahme desjenigen von dem die Anfrage gekommen ist.
 - Existieren zu einem Ziel schon viele Cacheeinträge kann es zu eine Ansturm von Route-Reply-Paketen kommen, dies kann vermieden werden, in dem ein Knoten vor Weiterleitung eines Routereplypaketes einige Zeit wartet bevor er das Paket weiterleitet und derweil darauf achtet, ob Reply-Pakete mit kürzerer Route unterwegs sind.
- Route Maintenance überwacht den einmal entdeckten Pfad zum Ziel
 - Kann ein Paket auf dem einmal erstellten Pfad nicht versandt werden. sendet der Knoten, der den Fehler feststellt ein Errorpaket an den Absender.
 - Jeder Knoten der das Errorpaket weiterleitet, löscht den entsprechenden Routeneintrag in seinem Cache und guckt, ob ihm evtl. schon eine alternativ Route bekannt ist, dann könnte das ursprüngliche Paket über den alternativen Weg geschickt werden

FAQ-Liste Mobile Computing (1679)

- Ein Knoten, der einen kürzeren Weg für ein von ihm weitergeleitetes Paket kennt kann unaufgefordert einen Route-Reply an den Sender schicken, dass den kürzeren Weg enthält.

Funkübertragung Verfahren allgemein (nur ganz kurz erklären)

Raummultiplex (SDM Space Division Multiplex)

- Funksignale verlieren mit Abstand zur Senderquelle an Stärke, so dass in ausreichender Entfernung eine weitere Übertragung über denselben Kanal nicht mehr gestört wird. Deshalb können Funkressourcen bei einer zellularen Aufteilung der Gesamtfläche mehrfach genutzt werden.
- Des weiteren können durch Antennen mit Richtungscharakteristik Funksignale so gesteuert werden, dass nur ein schmales Segment der Funkzelle abgedeckt wird. Damit können dieselben Ressourcen innerhalb einer Zelle mehrfach verwendet werden.

Frequenzmultiplex (FDM Frequenz Division Multiplex)

- Mehrere Sender verwenden gleichzeitig das Funkmedium, aber jeder nutzt eine andere Frequenz, der Empfänger kann durch einstellen einer bestimmten Frequenz einen speziellen Sender herausfiltern (z.B. Radioprogramm).
- Innerhalb eines Frequenzbandes benötigt jeder Kanal eine gewisse Breite, zusätzlich müssen zwischen benachbarten Kanälen gewisse Abstände eingehalten werden. Damit kann ein verfügbares Frequenzband nicht in beliebig viele Kanäle geteilt werden.
- Für einen Duplexkanal zwischen Sender und Empfänger werden im Frequency Division Duplex Verfahren Uplink (mobiles Gerät zur Basisstation) und Downlinkkanal (Basisstation zum mobilen Endgerät) um eine konstante Frequenz gegeneinander verschoben.
- Frequency Hopping, dass Springen zwischen Frequenzen in einer festgelegten Pseudozufallsfolge, soll verhindern, dass durch Störung einer Frequenz ein Endgerät dauernd nicht erreichbar ist.

Zeitmultiplex (TDM Time Division Multiplex)

- Beim Zeitmultiplex teilen sich mehrere Sender eine Frequenz in dem sie nacheinander das Medium für eine bestimmte Zeit verwenden.
- Die Zeiträume der Belegung werden Zeitschlitze (Slots) genannt.
- Um Kollisionen zu vermeiden müssen die Zeitschlitze der Geräte synchronisiert werden
 - o Zentrale Synchronisation. Hier gibt es einen ausgezeichneten Sender (Basisstation), der den anderen Sendern Zeitschlitze zum Senden zur Verfügung stellt.
 - o Dezentrale Synchronisation. Die beteiligten Stationen handeln die Zeitschlitze untereinander aus. Es gibt keinen „Master“.
- Wird ein Duplexkanal über Zeitmultiplex genutzt, so spricht man von Time Division Duplex. Hierbei wird Up- und Downlink zeitversetzt das Senderecht eingeräumt.

Codemultiplex (CDM Code Division Multiplex)

- o Gleichzeitige Übertragung von Daten auf einer Frequenz
- o Spezielle Codierung stellt sicher, dass der Empfänger die überlagerten Daten rekonstruieren kann.
- o Schlüsselkomponente des Codemultiplexverfahrens ist der Spreizcode, der jedem Sender zugeordnet wird. Ein Empfänger muss den Spreizcode seines Senders kennen um das empfangene Signal filtern zu können.
- o Der Spreizcode ist die unendliche Aneinanderreihung eines speziellen Codeworts, dessen einzelne Bits als Chips bezeichnet werden.
- o Jedes Bit der Nutzdaten wird zunächst auf die Länge des Codewortes „aufgebläht“ und dann mit dem Codewort multipliziert. (Dazu wird die binäre 0 auf -1 und die binäre 1 auf 1 abgebildet.)
- o Das resultierende Signal wird übertragen. Da bei wird es in der Regel von mehreren anderen Signalen überlagert werden.

FAQ-Liste Mobile Computing (1679)

- Das empfangene überlagerte Signal wird jetzt vom Empfänger wiederum mit dem Spreizcode multipliziert.
- Das Resultat ändert sich noch mit dem Takt des Chips des Spreizcodes und muss noch über die Länge des Codewortes integriert werden, um die ursprünglichen Nutzdaten zu erhalten.
- Voraussetzungen, damit es so einfach funktioniert:
 - Der Empfänger kennt den exakten Beginn des Spreizcodes und ist mit dem Sender synchronisiert, denn ist der Spreizcode nur um ein Bit verschoben, kann das ursprüngliche Signal nicht rekonstruiert werden.
 - Zur Synchronisation kann der Empfänger das Signal abhören und den Spreizcode solange verschieben, bis eine charakteristische Sequenz empfangen wird.
 - Rauschen wird ignoriert und die Signalstärke als fest angesehen.
- Die von den verschiedenen Sendern verwendeten Spreizcodes müssen zueinander orthogonal sein. Zwei Vektoren $x(x_1, x_2, x_3, \dots)$ und $y(y_1, y_2, y_3, \dots)$ sind orthogonal, wenn das Skalarprodukt gleich null ist, d.h.: $0 = \sum_{i=1}^n x_i * y_i$
- Sätze von Spreizcodes können über die Walsh Hadamard-Matrix berechnet werden. Die Walsh-Hadamard-Matrizen haben als Dimensionen Zweierpotenzen und sind rekursiv definiert: $H_1 = [1]$ $H_n = \begin{bmatrix} H_{n/2} & H_{n/2} \\ H_{n/2} & -H_{n/2} \end{bmatrix}$
- Eine Zeile der Walsh-Hadamard-Matrix wird Walsh-Sequenz genannt. Walsh-Sequenzen sind zueinander orthogonal, so dass sie als Spreizcodes in Frage kommen.

WLAN

Zugriffsverfahren auf das Funkmedium:

- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) verringert Kollisionswahrscheinlichkeit zusätzlich wird durch Quittungsverfahren erreicht, dass im Falle von Kollisionen Nutzdaten nicht unerkannt verloren gehen.
- Distributed Coordination Function /DCF)
 - Einfaches CSMA/CA (verbindlich)
 - Sendewillige Station hört für eine Wartezeit, die sich aus einer konstanten Wartezeit und einer zufallsabhängigen Wartezeit zusammensetzt, das Medium ab.
 - Findet eine Sendung statt, wird bis zum Ende der Belegung unterbrochen. Danach beginnt zunächst wieder die feste Wartezeit die mit der reduzierten Zufallswartezeit verlängert wird (Backoff)
 - Ist das Medium frei, wird gesendet.
 - Konstante Wartezeiten (Interframe Spaces)
 - Distributed Control Function Interframe Space (DIFS) bevor Sendung
 - SIFS (Short Interframe Space) vor senden der Empfangsbestätigung (ohne zusätzliche Zufallswartezeit). Kürzer als DIFS. Dadurch automatisch priorisiert.
 - Zufallsabhängige Wartezeit, wird aus einem ganzzahligen Zufallswert multipliziert mit einem konstanten Zeitfaktor berechnet.
 - Contention Window Zeit die bei maximaler Zufallszahl gewartet wird.
 - Große Contention Window geringe Kollisionswahrscheinlichkeit jedoch geringer Datendurchsatz

- Kleine Contention Window höhere Kollisionswahrscheinlichkeit, aber höherer Datendurchsatz
- Optimale Contention Window Größe wird über Exponential Backoff ermittelt.
 - Mögliche Contention Window Größen: 7,15, 31,63, 127, 255
 - Es wird bei 7 begonnen, kommt es zu Fehlern wird die Größe des Contention Window schrittweise erhöht, bis das Maximum erreicht ist.
- Empfangene Nachrichten werden mit ACK Signal bestätigt, für das nur SIFS abgewartet werden muss..
- Ursachen für ausbleibende Quittungen:
 - Nachricht ging durch Kollision verloren
 - Quittung ging durch Kollision verloren
- Bei fehlender Quittung muss Sender den Frame erneut senden, jedoch mit der üblichen Wartezeit.
- CSMA/CA mit RTS/CTS (optional)
 - Nicht immer kann eine Station erkennen, dass das Medium belegt ist, da nicht alle Stationen zueinander in Sendereichweite sein müssen.
 - Das Medium wird um Störungen zu vermeiden von der sendewilligen Station und der Empfangsstation durch einen Request to Send (RTS) und Clear To Send (CTS) Dialog für andere Stationen für eine Zeitdauer Net Allocation Vector (NAV) gesperrt.
 - Hierbei reicht es, wenn fremde Stationen eines der beiden Signale RTS/CTS mit hören, um diese für NAV in den Wartezustand zu versetzen.
 - Zwischen RTS und CTS wird lediglich SIFS abgewartet.
 - Kollisionen werden zwar verringert, jedoch erhöhter Verwaltungsaufwand
 - Da mit großen Frames die Bitfehlerhäufigkeit steigt, gibt es einen speziellen Fragmentierungsmodus, der es erlaubt die Nachricht auf mehrere Framepakete zu verteilen, ohne dass jeweils eine neue RTS/CTS Nachricht zwischen Empfänger und Sender ausgetauscht werden muss.
- Point Coordination Function (optional)
 - Nur in Infrastrukturmodus verfügbar, da Access Point (oder andere ausgezeichnete Station) für Koordination erforderlich. (Point Coordinator)
 - Der PCF-Modus ermöglicht Garantien bzgl. Verzögerung und Bandbreite.
 - Für den Aufruf zum Wechsel von Distributed Coordinate Function- (DCF) und Point Coordinate Function-Modus (PCF) gibt es eine spezielle Wartezeit Point Coordinate Function Interframe Space (PIFS) die in der Länge zwischen SIFS und DIFS liegt, d.h. Quittungen und RTS/CTS-Frames sind höher priorisiert, aber andere sendewillige Stationen stehen zurück.
 - Beim Aufruf in den PIFS Modus wird eine NAV-Zeit mitgegeben, für die die Stationen in den Wartemodus versetzt werden bzw. in der sie nur auf Anfragen des Point Coordinators antworten.
 - Der Point Coordinator fragt nacheinander alle Stationen ab.
 - Zwischen den einzelnen Sendevorgängen wird nur SIFS abgewartet ⇒ hoher Durchsatz an Daten
 - Nach Abfrage der letzten Station sendet der Point Coordinator den EndCF Frame, der es den Stationen ermöglicht wieder in den normalen Distributed Coordinate Function-Modus überzugehen.

Probleme bei der Transportschicht im Vergleich drahtgebunden und drahtlos?

Split-Connection-Verfahren (Hauptvertreter Indirect TCP (I-TCP))

FAQ-Liste Mobile Computing (1679)

- Auf der drahtgebundenen Strecke wird TCP unverändert eingesetzt.
- Die zweite Verbindung ist speziell für den drahtlosen Verkehr entwickelt
- Die Basisstation verwaltet beide Verbindungen und übergibt die Nachrichten einer Verbindung jeweils an die andere Verbindung.
- Vorteile
 - o Überlastungskontrolle kann für den jeweiligen Abschnitt optimiert werden.
 - Drahtgebunden Verbindung Herabsetzung der Paktrate
 - Drahtlose Verbindung schnelles Nachsenden defekter Pakete
 - o Die drahtlose Verbindung kann zusätzliche Funktionen integrieren ohne die stationäre Gegenstelle damit zu belasten:
 - Verbindungsabbrüche
 - Bewegen des Rechners im Raum
 - Reduktion verfügbarer Bandbreite
 - o Die Basisstation kann für den mobilen Rechner Verwaltungsaufgaben für die Verbindung übernehmen.
 - Z.B. kann ein vereinfachtes Transportprotokoll zwischen mobilem Rechner und Basisstation, damit der mobile Rechner nicht den kompletten TCP-Protokollstapel beherrschen muss, obwohl der stationäre Sender sein gewohntes TCP-Protokoll verwendet.
 - MobileTCP verwendet beispielsweise zwischen Basisstation und mobilem Rechner kein Sendefenster, sondern ein einfaches Quittungsverfahren und spart zusätzlich durch ein Kompressionsverfahren, dass redundante Informationen aus Paketköpfen eliminiert Bandbreite ein.
- Wechselt ein mobiler Knoten die Basisstation sind davon auch laufende Verbindungen betroffen. I-TCP löst dieses Problem im Bereich der Transportschicht
 - o Die Verbindungsrelevanten Daten (Verbindungsparameter, Status der Sendepuffer,..) werden von der alten Basisstation an die neue übergeben. Dadurch muss keine neue Verbindung aufgebaut werden.
- Nachteile von Split-Connection-verfahren:
 - o 2 facher Verwaltungsaufwand der Basisstation, durch 2 Verbindungen.
 - o Verletzung der Ende zu Ende Semantik von TCP, da die Basisstation die TCP-Quittung ausstellt ist nicht wirklich garantiert, dass die Pakete auch die mobile Station fehlerfrei erreicht haben.

Snoop-Protokoll

- Arbeitet auf der Vermittlungsschicht und Kombiniert Automatic Repeat Request (ARQ)-Verfahren mit der Sendewiederholung auf Transportebene.
- Die Basisstation schreibt ein sogenannter SnoopAgent alle Pakete die die Basisstation auf dem Weg zum mobilen Rechner passieren in einen Puffer mit.
- Gleichzeitig wird der Quittungsverkehr in Richtung des stationären Rechners vom SnoopAgent abgehört.
- Pakete für die positive Quittungen vorliegen werden vom SnoopAgenten aus dem Puffer gelöscht
- Fehlt jedoch laut Quittung ein Paket beim mobilen Rechner fängt der SnoopAgent die negative Quittung ab und sendet das fehlende Paket aus seinem Puffer nach.
- Vorteile:
 - o Keine Änderung des TCP-Kommunikationsprotokolls in den Endpunkten.
 - o Ende zu Ende Semantik von TCP bleibt erhalten. Bestätigte Pakete sind auch wirklich angekommen
 - o Geht der Zustand der Basisstation durch Ausfall verloren wird schlimmstenfalls direkt auf das klassische TCP-Verfahren zurückgegriffen es kommt also höchstens zu Performanceverlusten.

FAQ-Liste Mobile Computing (1679)

- Vereinfachter Wechsel der Basisstation der Snoop-Puffer muss nicht zwingend übertragen werden und die neue Basisstation muss nicht zwingend das Snoop-Protokoll beherrschen.
- Problem: verschlüsselte Übertragung
 - Hier werden ggf. auch die Kopfinformationen des Paketes, sowie Quittungen verschlüsselt, damit kann der SnoopAgent nicht mehr die Sequenznummern der Pakete mitlesen die für ein erneutes Senden erforderlich sind.
 - Der Ausweg die Basisstation mit den Schlüsseln auszustatten setzt hohes Vertrauen in die Basisstation voraus.

Fast Retransmission

- Bei der Umstellung zwischen den Basisstationen kann es zu Verlusten von Quittungen des mobilen Rechners kommen, die zu einer Herabsetzung der Paketübertragungsrate im reinen TCP führen würden.
- Deshalb sendet beim fast retransmission verfahren die mobile Station direkt nach der Umstellung auf die neue Basisstation eine Folge von positiven Quittungen über bisher erhaltene Pakete, damit wird die Eigenschaft von TCP ausgenutzt, bei positiven Quittungen über eine reduzierte Anzahl Pakete die fehlenden Pakete nach zu senden ohne die Paketrate zu reduzieren.
- Vorteile:
 - Kombinierbar mit anderen Verfahren
 - Nur das Verhalten des mobilen Knotens muss modifiziert werden.

Selektive Quittung

- Standardmäßig werden bei TCP nur ununterbrochene Folgen korrekt empfangener Pakete quittiert. Fehlt ein einzelnes Paket werden auch alle vielleicht schon korrekt übertragenen Folgepakete noch mal gesendet.
- Selective Acknowledgments (SACK) erweitern den Quittungsmechanismus von TCP so, dass erfolgreich empfangen Blöcke jeweils spezifiziert durch Anfang und Ende quittiert werden und so nur diejenigen Pakete wiederholt werden müssen, die tatsächlich fehlen.
- Explizit Loss Notification (ELN)
- Expliziter Hinweis an den Sender auf einen speziellen Paketverlust erleichtern das schnelle Nachsenden der erforderlichen Information.
- Der Paketverlust ist auf Empfängerseite jedoch relativ schlecht feststellbar, so dass keine ELN generiert werden kann.
- Remote-Socket-Architektur
- Verwendet nur zwischen Basisstation und stationärem Sender TCP, zum mobilen Rechner wird ein spezielles Last Hop Protocol (LHP) gefahren.
- Die Basisstation dient aus Sicht des stationären Rechners als Stellvertreter für den mobilen Rechner.
- User Datagram Protocol (UDP)
- Unzuverlässiger verbindungsloser Datentransport
- Keine Garantien, keine Überlastungskontrolle
- Keine Ansätze zur Verbesserung
- Probleme verursachen Anwendungen die UDP nutzen, aber von der fast fehlerfreien Übertragung in drahtlosen Netzen ausgehen und deshalb Übertragungsfehler nicht in der Anwendung auffangen

GSM-Mobiltelefonie

Grundlagen zellulärer Mobilfunknetze

- Verhalten elektromagnetischer Wellen
 - Idealiert breiten sich elektromagnetische Wellen kugelförmig um einen Sender aus.
 - Die Wirkung elektromagnetischer Wellen reduziert sich mit dem Quadrat des Abstandes, d.h. verdoppelt man den Abstand von Sender und Empfänger reduziert sich die Wirkung der Wellen auf ein Viertel.

FAQ-Liste Mobile Computing (1679)

- In realen Umgebungen kommt es zu vielfältigen Abweichungen von diesem Ideal, durch Gebäude und Geländeformen, sowie elektromagnetische Störquellen nimmt die Wirkung von elektromagnetischen Wellen mit der 4. Potenz ab, d.h. verdoppelt sich die Entfernung von Sender und Empfänger sinkt die Sendeleistung um das 16fache.
- Isolation von Kanälen
 - Die elektromagnetischen Wellen von verschiedenen Transmissionen überlagern sich beim Empfänger.
 - Eine einfache Isolation durch die Verwendung mehrere Leitungen, wie es in drahtgebundenen Netzen üblich ist, ist bei drahtlosen Netzen nicht möglich.
 - Die Trennung erfolgt deshalb über den Einsatz von Raum-, Zeit-, Frequenz- oder Code-Multiplexverfahren ggf. in Kombination.
- Die begrenzte Reichweite elektromagnetischer Wellen führt zum Konzept der zellularen Netze.
 - Die Fläche auf der sich potentielle Mobilfunkteilnehmer befinden, wird durch ein Netz von Zellen abgedeckt.
 - Jede Zelle deckt einen bestimmten Bereich ab und enthält eine Stationäre Basisstation (Sende-/Empfangsstation)
 - In den Übergangsbereichen zwischen zwei Zellen kommt es zu Überlappungen, d.h. ein Teilnehmer befindet sich im Bereich von 2 oder mehr Basistationen.
 - Vorteile:
 - Die Distanz die das mobile Endgerät zur nächsten Basisstation überbrücken muss ist relativ gering (D-Netz max. 35km im E-Netz max. 8 km)
 - Zellen die einen gewissen Abstand haben können dieselben Frequenzen benutzen ohne sich gegenseitig zu stören.
 - Nachteil:
 - Es müssen entsprechend viele Basisstationen errichtet und miteinander vernetzt werden, was hohe Kosten verursacht.
- Zur Planung Abdeckung der Fläche mit identischen Clustern aus „idealisierte“ identisch großen 6 eckigen Zellen. Dabei gilt:
 - F_{Ges} ist die Menge aller Frequenzen, die einem Mobilfunkbetreiber zugeordnet sind.
 - $F_i \subseteq F_{Ges}$ paarweise verschieden für alle i aus $\{1, 2, \dots, k\}$, wobei k die Anzahl der Zellen pro Cluster wiedergibt, so dass die Vereinigungsmenge aller F_i F_{Ges} entspricht.
 - Der Abstand D zweier Basisstationen derselben Frequenz wird berechnet mit $D = R\sqrt{3 \cdot k}$, wobei k die Anzahl der Zellen im Cluster und R den Radius der Zellen wieder gibt.
 - Der Abstand zwischen zwei Basisstationen muss dabei hinreichend groß sein, damit Störungen minimiert werden.
 - Je größer der Abstand, desto kleiner die Anzahl der Frequenzen, die auf eine einzelne Basisstation entfallen.
 - Im GSM-Netz wird eine Clustergröße von 7 Zellen verwendet.

Architektur und Eigenschaften von GSM-Netzen (Global System for mobile Communication)

- Grundstein der Entwicklung von GSM war 1982 die Groupe Special de Mobile, die einen europäischen digitalen Mobilfunkstandard entwickeln sollte. Diese Gruppe wurde 1989 von der European Telecommunication Standards Institute als Technical Comitee aufgenommen.
- GSM wurde so ausgelegt, dass viele Millionen Kunden pro Netzwerk versorgt werden können.
- Mehrere Mobilfunkanbieter können die gleiche Fläche abdecken ohne sich gegenseitig zu stören.

FAQ-Liste Mobile Computing (1679)

- Eine Vollständige Flächenabdeckung je Netz wird angestrebt. Diese ermöglicht es den Teilnehmern überall innerhalb eines Landes mobil zu telefonieren.
- Die Bewegung des Teilnehmers von einer Mobilfunkzelle in eine andere wird auch während einer laufenden Verbindung ohne Unterbrechung durch Handover sichergestellt.
- Durch Roamingabkommen der Mobilfunkbetreiber unterschiedlicher Länder, bleibt der Teilnehmer auch im Ausland unter seiner gewohnten Rufnummer erreichbar.
- Neben den Sprachdiensten werden auch Dienste zur Übertragung von Textnachrichten (SMS = Short Message Service) und spezialisierte Webprotokolle (WAP Wireless Application Protocol) die es ermöglichen Informationsseiten ähnlich Internetangeboten auf dem Handy darzustellen angeboten.
- Das GSM-Netzwerk besteht aus 3 Subsystemen:
 - o Betriebssystem (OMSS= Operation and Maintenance System)
 - Dient der Administration und Kontrolle des Netzwerks
 - Die Kontrolle erfolgt über das Operation and Maintenance Center (OMC)
 - Verwaltung der Geschäftsrelevanten Daten (Kundendaten, Endgeräte, Gebühren, Statistik)
 - Sicherheitsmanagement
 - Netzwerkkonfiguration
 - Vertrauliche Daten über Kunden und Schlüssel sind im Authentication Center (AUC) gespeichert, sie dienen dazu Kunden zu identifizieren und registrierte Dienste freizuschalten.
 - Im Equipment Identity Register (EIR) werden die Seriennummern (IMEI) der Endgeräte gespeichert
 - White List enthält die Gerätenummern der registrierten Geräte
 - Black List enthält die Gerätenummern der Geräte die nicht mehr betrieben werden sollen (verloren, gestohlen). Sie wird zwischen den Netzbetreibern ausgetauscht
 - Gray List (optional) speichert Nummern von Geräten, die zwar operabel sind, deren Software oder Ausstattung jedoch veraltet ist oder Fehlfunktionen aufweist.
 - o Vermittlungssystem (SMSS = Mobile Switching und Management System)
 - Vermittelt die Nutzdaten innerhalb des Netzes und stellt eine Anbindung anderer Netze zur Verfügung
 - Kern sind die Mobile Switching Center (MSC), die jeweils mehrere BSC verwalten.
 - Pro Netzwerk können dabei mehrere MSC existieren, die jeweils sogenannte Service Areas verwalten.
 - Der MSC wickelt den Netzverkehr zwischen den Funksubsystemen ab und vermittelt Verbindungen zu externen Netzen über das Gateway Mobile Switching Center (GMSC) bzw. für internationale Gespräche über das International Switching Center (ISC).
 - MSRN (Mobile Station Roaming Number) wird vergeben, wenn der Benutzer in ein fremdes Netz wechselt. Diese Nummer ist für Anrufer und Angerufenen transparent und dient nur der technischen Abwicklung zwischen den Netzbetreibern.
 - Darüber hinaus ist der MSC für die Lokalisierung der Benutzer über 2 Datenregister zuständig:
 - Home Location Register (HLR)
 - o Daten von Teilnehmern, die sich im aktuell im Zuständigkeits Bereich des MSC befinden.
 - o Einträge werden nur temporär vorgenommen, verlässt ein Kunde die Service Area werden die Daten gelöscht.

- Neben eigenen Kunden können auch Kunden fremder Netze (z.B. im Rahmen Roaming) in das Register aufgenommen werden.
- MSISDN (Mobile Subscriber ISDN) eigentliche Telefonnummer des mobilen Gerätes
 - 3 Ziffern Nationalcode (049)
 - 2-3 Ziffern Code des Mobilfunkbetreibers (171,172,..)
 - max. 10 Ziffern Anschlussnummer
- Visitors Location Register (VLR)
 - Daten von Teilnehmern, die sich im aktuell im Zuständigkeits Bereich des MSC befinden.
 - Einträge werden nur temporär vorgenommen, verlässt ein Kunde die Service Area werden die Daten gelöscht.
 - Neben eigenen Kunden können auch Kunden fremder Netze (z.B. im Rahmen Roaming) in das Register aufgenommen werden
- Funksubsystem (BSS = Base Station Subsystem)
 - Bindet die Mobilfunkteilnehmer an das Netzwerk an
 - Die Kommunikation zwischen Endgerät und GSM-Netzwerk erfolgt über Base Transceiver Stations (BTS).
 - Je Funkzelle existiert eine BTS.
 - LAI (Location Area Identity) und CI (Cell Identifier) identifizieren international eindeutig jede Zelle.
 - LAI und CI werden von der Basisstation permanent gesendet, so dass jedes Endgerät weiß, wo es sich gerade befindet.
 - Mehrere BTS werden von einem Base Station Controller (BSC) kontrolliert,
 - Das BTS beherbergt:
 - das eigentlichen Sende- und Empfangssystem
 - Protokollarbeit zur Datenübertragung über die Funkschnittstelle
 - Die eigentliche Datenverarbeitung erfolgt im Base Station Controller
 - Die BSC sind auch für das Handover eines Teilnehmers in eine andere Zelle verantwortlich
 - Der Datenverkehr innerhalb des GSM-Netzes wird mit Ausnahme des Kontaktes BTS-Endgerät in der Regel leitungsgebunden über Glasfaser oder Richtfunkstrecken abgewickelt.
- Adressierung von Geräten und Benutzern:
 - GSM unterscheidet Endgeräte und Benutzer bei der Identifizierung
 - Benutzer werden an Hand ihrer SIM (Subscriber Identity Modul) identifiziert, auf der folgende Informationen gespeichert sind:
 - PIN (optional)
 - Daten der persönlichen Konfiguration (Telefonnummern)
 - Eintreffene aber noch nicht gelöschte SMS-Nachrichten
 - Technischen Daten des Mobilfunkbetreibers (Frequenzen)
 - IMSI (International Mobile Subscriber Identity) weltweit eindeutige Nummer, die den Benutzer auch in fremden Netzen identifiziert. (Nicht zu verwechseln mit der Rufnummer des Anschlusses! = MSISDN)
 - Die IMSI ist in der Home Location Register Datenbank gespeichert
 - TMSI (Temporary Mobile Subscriber Identity) Um die Identität des Benutzers zu schützen, wird in der Kommunikation zwischen Netz und

Benutzer nicht die IMSI verwendet, sondern regelmäßig eine neue TMSI ausgehandelt und gespeichert.

- Endgeräte werden über eine weltweit eindeutige IMEI (International Mobile Station Equipment Identity) identifiziert. Die IMEI ist in der Equipment Identity Register Datenbank gespeichert:
- Die Luftschnittstelle
 - GSM verwendet eine Kombination aus Frequenz Division Multiple Access (FDMA) und Time Division Multiple Access (TDMA), sowie Space Division Multiple Access (SDMA), da ein zellulares Netz vorliegt.
 - Vom Endgerät zur Basisstation (Uplink) wird das Frequenzband 890-915 MHz genutzt
 - Von der Basisstation zum Endgerät (Downlink) das Frequenzband 935-960 MHz
 - Jedes Band wird in 124 Kanäle à 200 kHz aufgeteilt und von 1 – 124 durchnummeriert.
 - Für die Bidirektionale Kommunikation werden jeweils die Kanäle mit der gleichen Kanalnummer genutzt, die immer um 45 MHz gegeneinander verschoben sind.
 - Die beiden freien Bänder von je 100 kHz am Ende der Frequenzbänder dienen dem Sicherheitsabstand zu anderen Diensten.
 - Analog wird im DCS1800 (GSM1800) eine Aufteilung in 372 Kanäle auf die Frequenzbänder 1710-1785 MHz und 1805-1880 MHz abgebildet.
 - Durch Frequenzhopping wird vermieden, dass eine Störung auf einer Frequenz über einen längeren Zeitraum die Verbindung eines bestimmten Endgerätes zur Basisstation stört.
 - Die 124 GSM-Kanäle teilen sich in Deutschland D1 und D2 mit je 57 Kanälen.
 - Davon bekommt jede Basisstation eines Mobilfunkbetreibers jeweils rund 1/7 zugeordnet, d.h. ca. 8 Frequenzen je Basisstation
 - Damit trotz der beschränkten Frequenzanzahl möglichst viele Teilnehmer telefonieren können, werden die Kanäle jeweils in 8 sich zyklisch wiederholende Zeitschlitze von je 0,5ms Dauer (Burst Periode BP) aufgeteilt.
 - Ein bestimmtes Endgerät benutzt immer nur Zeitschlitze mit der selben Nummer für die Übertragung.
 - Die Zeitschlitze für Up- und Downlink sind gegeneinander um 3 BP verschoben, damit kein mobiles Endgerät gleichzeitig senden und empfangen muss.
 - Innerhalb einer Burst Periode wird ein sogenannter Burst gesendet.
 - Normal Bursts dienen der Datenübertragung
 - Frequency Correction Bursts dienen dem mobilen Endgerät zur Frequenzkorrektur
 - Synchronisation Burst dienen der zeitlichen Synchronisation zwischen Endgerät und Basisstation
 - Dummy Bursts werden gesendet, wenn weder Nutz- noch Verwaltungsdaten anstehen
 - Access Bursts Zugriff des mobilen Endgerätes auf die Basisstation ohne vorherige Anmeldung
 - Ein Burst enthält 114 Bit Nutzdaten aufgeteilt in zwei Sequenzen à 57 Bit.
 - Theoretische Obergrenze 24.700 Bit/s praktisch werden jedoch nur 13.000 Bit/s für die Sprach und 9.600 Bit/s für die Datenübertragung erreicht.
- Handover und Roaming
 - Bewegt sich ein Teilnehmer von einer Zelle zur Anderen bzw. wird die Signalqualität aus anderen Gründen zu schlecht, muss die Verbindung neu konfiguriert werden (Handover)
 - Intracell Handover: Aus Gründen der Signalqualität wird innerhalb einer Zelle auf eine neue Frequenz umgeschaltet

FAQ-Liste Mobile Computing (1679)

- Intercell Handover: Umschaltung der Kommunikationsverbindung durch das Vermittlungssystem auf eine neue Basisstation. Gleichzeitig wird vom mobilen Endgerät die Frequenz gewechselt.
 - Internes Handover: Die beteiligten Basisstationen werden vom gleichen Basis Station Controller (BSC) verwaltet.
 - Externe Handover: Die beteiligten Basisstationen werden von unterschiedlichen BSC verwaltet.
- Unabhängig von der Verlagerung der Verbindung behält ein einmal zuständiges Mobile Switching Center (MSC) die Kontrolle über die Verbindung als sogenannter Anker-MSC. Die Verbindung wird lediglich logisch in den Bereich des anderen MSC erweitert.
- Network-originated Handover: Der Handover wird vom Funksubsystem initiiert, damit kann der Handover-algorithmus geändert werden, ohne dass die Endgeräte angepasst werden müssen.
- Entscheidung zum Handover:
 - Empfangspegel sinkt unter einen gegebenen Schwellenwert
 - Bitfehlerhäufigkeit steigt über einen gegebenen Schwellenwert
 - Maximale Entfernung zwischen Endgerät und Basisstation ist erreicht
- Roaming
 - Eigenschaft des Mobilfunknetzes, die es ermöglicht einen Teilnehmer an beliebigen Orten anzurufen, ohne dass dieser explizit seinen Aufenthaltsort hinterlegt. Der Aufenthaltsort wird vom Netz automatisch bestimmt.
 - Nutzung fremder Netze mit denen kein Vertrag vorliegt, wenn die Mobilfunkanbieter ein Roaming-Abkommen unterzeichnet haben. (Ermöglicht telefonieren im Ausland)

Positionsbestimmung:

Welche Basistechniken gibt es?

- Cell of Origin (COO)
 - Drahtlose Übertragungssysteme haben nur eine beschränkte Reichweite. Ausgestrahlte Signale können nur in bestimmten Bereichen (Zellen) wahrgenommen werden. Aus der Identifikation der Zelle kann man Rückschlüsse auf die Position ziehen
- Time of Arrival (TOA) / Time Differenz of Arrival (TDOA)
 - Elektromagnetische Signale bewegen sich mit Lichtgeschwindigkeit. Die Laufzeit kann mittlerweile präzise bestimmt werden. Ermittelt man den Zeitunterschied zwischen Aussenden und Empfang eines Signals, kann auf die Entfernung geschlossen werden.
- Angle of Arrival (AOA)
 - Werden Antennen mit Richtungscharakteristik verwendet, kann ermittelt werden aus welcher Richtung ein bestimmtes Signal eintrifft.
- Signalstärke
 - Aus der Signalstärke kann auf den Abstand zum Sender geschlossen werden, da die Signalstärke mit dem Quadrat des Abstands vom Sender abnimmt. (Wird allerdings durch äußere Einflüsse ungenau.)

Satellitennavigation erklären.

- Verfahren mit 3 Satelliten
 - 3 Satelliten mit bekannter Position erforderlich
 - Abstand von den 3 Satelliten wird ermittelt
 - Satellit sendet ein Signal, das den Zeitpunkt des Aussendens (t_S) codiert enthält.
 - Der Empfänger vergleicht diesen Zeitpunkt mit der internen Uhr zum Zeitpunkt des Empfangs (t_E).
 - Für die Entfernung r vom Satelliten gilt dann: $r = c \cdot (t_E - t_S)$, wobei c für die Lichtgeschwindigkeit (300.000 km/s) steht
 - terrestrischer Schnittpunkt der 3 Kugeln = Position des Empfängers
 - Kritischer Punkt exakte Zeitmessung Fehler von $1\mu s$ führt zu 300m Entfernungsunterschied.
 - Die exakte Uhrzeit des ganzen Navigationssystems wird als Systemzeit bezeichnet.
 - Benutzung von Atomuhren in den Satelliten

FAQ-Liste Mobile Computing (1679)

- Hinzuziehung eines weiteren 4. Satelliten zur Steigerung der Genauigkeit
 - Sei $t^s = tS + dtS$ (unbek. Abweichung der Satellitenzeit zur Systemzeit)
 - analog sei $t^E = tE + dtE$ (unbek. Abweichung des Empfängers zur Systemzeit)
 - $dt = tE - tS$ exakte Laufzeit des Signals
 - $d^t = t^E - t^S$ ermittelte Laufzeit des Signals
 - Berechnet wird stets nur die Pseudoentfernung $p = c \cdot d^t = r + c \cdot (dtE - dtS)$
 - Sei nun $dtS = 0$, da die Satelliten ja über genau gehende Atomuhren verfügen, die ständig überwacht und synchronisiert werden.
 - R wird über die Position des Empfängers und des Satelliten in einem kartesischen Koordinatensystem ausgedrückt..
 - Für die Pseudoentfernung p gilt dann: $p = r + c \cdot dtE = \sqrt{(sx - ex)^2 + (sy - ey)^2 + (sz - ez)^2} + c \cdot dtE$
 - Die Gleichung enthält 4 Unbekannte, deshalb ist zur exakten Positionsbestimmung der 4. Satellit erforderlich. Das resultierende Gleichungssystem aus 4 Gleichungen mit 4 unbekanntem ist nicht linear. Die Lösung erfolgt bspw. über iterative Näherungslösungen, die auf Taylor-Reihen basieren.

Wie funktioniert Global Positioning System (GPS)

- 24 Satelliten befinden sich auf 6 Bahnen mit je 4 Satelliten pro Bahn im Umlauf um die Erde im Abstand von ca. 20200km (zeitweise sind aus Ersatz/Reservegründen sogar bis zu 28 Satelliten auf den Umlaufbahnen unterwegs.)
- Die Satelliten sind so angeordnet, dass von jedem Punkt der Erde aus mindestens 5 und maximal 11 jederzeit über dem Horizont „sichtbar“ sind. Durch Gebäude oder andere Abschattungen kann es sein, dass nicht stets alle „sichtbaren“ Satelliten auch erreichbar sind, aber die benötigte Anzahl von 4 ist in aller Regel verfügbar.
- 2 Dienste zur Positionsbestimmung:
 - Precise Positioning Service (PPS) mit einer Genauigkeit von 22m in der Horizontalen und 27,7 m in der Vertikalen.
 - Der Dienst ist verschlüsselt und kann nur von den Streitkräften der USA und NATO entschlüsselt werden.
 - Standard Positioning Service (SPS) ist für zivile Nutzer verfügbar und verfügt über eine Genauigkeit von 25m in der Horizontalen und 43m in der Vertikalen.
 - Der Dienst wurde bis Mitte 2000 künstlich durch Selective Availability (SA) verfälscht, dass die Uhrzeiten der Satelliten zufällig veränderte und die Bahninformationen verfälschte, so dass die Genauigkeit auf 100, in der Horizontalen und 156m in der Vertikalen beschränkt war.
 - Frequenz 1575,42 Mhz für PPS und SPS bzw. 1227,6 MHz nur für PPS
 - Erkennung der Satellitensignale über CodeDivisionMultipleAccessverfahren.
 - Jeder Satellit hat ein eigenes Pseudo-Random-Noise-Signal (PRN)
 - Der Empfänger kennt alle PRN-Signale und kann so aus den überlagerten Signalen aller Satelliten einzelne Satelliten herausfiltern.
 - Messung der Signallaufzeit mit PRN
 - Der Empfänger verschiebt das ihm bekannte PRN-Signal solange auf der Zeitachse, bis es exakt mit dem vom Satelliten empfangenen Signal übereinstimmt. Aus der Verschiebung kann er dann die Laufzeit des Signals berechnen.
- Aufteilung in Segmente
 - Benutzersegment = Endgeräte zur Positionsbestimmung,
 - können teilweise auch zur Geschwindigkeitsmessung herangezogen werden
 - Zeit zwischen zwei Positionsmessungen messen und den Abstand zwischen den beiden Positionen durch diese Zeit teilen.
 - Dopplereffekt nutzen: Bewegte Objekte erfahren eine Frequenzverschiebung der empfangenen Signale, die Größe der Verschiebung ist ein Maß für die eigene Geschwindigkeit
 - Ablesen der genauen Uhrzeit
 - Nicht möglich ist jedoch die Messung der Ausrichtung (aktueller Winkel des Gerätes) hierzu sind andere Verfahren nötig.
 - Kontrollsegment = Territoriale Kontrollstationen
 - Verwaltung der Satelliten und Korrektur der Satelliten eigenen Daten (Systemzeit, Position, Bahndaten)
 - Monitorstationen berechnen Korrekturdaten, die an die Master Control Station (MCS) weitergeleitet werden.
 - Aufgaben der Master Control Station

FAQ-Liste Mobile Computing (1679)

- Sammeln der Korrekturdaten von den Monitorstationen
 - Berechnung von Korrekturinformationen für die Satelliten
 - Übertragung der Bahn- und Positionsinformationen an die Satelliten.
 - Korrektur der Atomuhren der Satelliten
 - Einrichten neuer Satelliten
 - Raumsegment = Satelliten
 - Autonome Energieversorgung über Sonnensegel
 - 16MHz CPU
 - Programmiert in ADA
 - Fehlerquellen
 - Uhrenfehler
 - Schwankungen in der Umlaufbahn, denn die Gravitationskräfte von Sonne und Mond stören die Umlaufbahnen
 - Störungen der Atmosphäre
 - Störungen der Ionosphäre
 - Multipath-Fehler (reflektierte Signale in der Umgebung des Empfängers)
 - Verfahren zur Genauigkeitserhöhung
 - Differential Global Positioning System (DPGS)
 - Einrichtung zusätzlicher Basis- (Korrektur-)Stationen auf der Erde, deren Position bekannt ist.
 - Die Basisstationen führen für sich selbst Positionsbestimmungen via Satellit durch, da die Positionsbestimmung fehlerbehaftet ist, ergeben sich Differenzen zur tatsächlichen Position
 - Anhand der Differenzen werden Korrekturdaten ermittelt, die den Benutzern im Umkreis der Basisstation mitgeteilt werden, da davon ausgegangen wird, dass bei Ihnen sehr ähnliche Fehler vorliegen.
 - Voraussetzung:
 - Die Entfernung zwischen Empfänger und Korrekturstation ist nicht zu groß
 - Die Korrekturen werden zeitnah übertragen.
 - Die Station und der Benutzer nutzen dieselbe Satellitenauswahl zur Positionsbestimmung (Korrekturdaten stimmen nur für bestimmte Konstellation) Umgehung:
 - für jeden Satelliten werden Korrekturdaten zur Pseudoentfernung ermittelt und verteilt, so dass die Auswahl der Satellitenkombination keine Rolle mehr für den Korrekturwert spielt.
 - Die Genauigkeit erhöht sich hierdurch auf 1-3m
 - Wide Area Augmentation System (WAAS)
 - Im Gegensatz zu DPGS wird die Verteilung der von den Monitorstationen ermittelten Korrekturdaten nicht direkt über terrestrische Sender durchgeführt, sondern mit Hilfe geostationärer Satelliten.
- Bildung des Korrekturfaktors Satelliten weise, was wird eigentlich genau korrigiert?
- der Abweichungsfaktor der Pseudoentfernung

Sicherheit Authentifizierung und Verschlüsselung

Authentifizierung nur ganz grob.

- Zweifelsfreie Feststellung, dass der Kommunikationspartner auch der Kommunikationspartner ist, für den er sich ausgibt.
 - Pro Nachricht
 - Unterzeichnung mit privatem Schlüssel \Rightarrow Nachricht kann Absender eindeutig zu geordnet werden.
 - Pro Verbindung
- "Challenge Response Verfahren"
 - Digest-Challenge (Frage) und Digest-Response(Antwort)-Nachrichten System
 - Nur wenn die Antwort zur Frage passt, gilt der Partner als authentifiziert.
 - Gerät 1 berechnet einen einmal Schlüssel (Pseudozufallszahl bspw. Aus Zeitstempel und privatem Schlüssel verschlüsselt diesen mit einer Hashfunktion (MD5) und schickt dies zusammen mit der Benutzerinformation (Realm) zur Authentifizierungsanfrage an Gerät 2
 - Gerät 2 ermittelt die zur Realm gehörige Information (z.B. Kennwort) verschlüsselt diese seinerseits zusammen mit dem Einmalschlüssel und schickt die Antwort an Gerät 1
 - Gerät 1 seinerseits kennt die Antwort auf die Frage (Kennwort. Zur BenutzerID) und berechnet selber mit dem Einmalschlüssel und dem Kennwort die Hashfunktion (MD5)

FAQ-Liste Mobile Computing (1679)

stimmt das Ergebnis von Gerät 1 mit dem von Gerät 2 übermittelten Ergebnis überein, Gilt Gerät 2 als Authentifiziert.

- GSM-Authentifizierung und Verschlüsselung
 - o Sicherheitsziele:
 - Schutz vor nicht autorisiertem Telefonieren
 - Schutz vor Abhören einer Sprach oder Datenverbindung (durch 3.)
 - Schutz vor der Bestimmung des Aufenthaltsortes durch 3. (Der Mobilfunkbetreiber muss die Zelle ja kennen.)
 - o 3 kryptografische Funktionen (A3,A5 und A8), davon 2 (A3 und A8) auf der SIM-Karte und einer (A5) im Mobiltelefon gespeichert.
 - o 2 Schlüssel (Ki [Identifikation/SIM-Karte]) und Kc [Verschlüsselung])
 - o Challenge-Response-Verfahren
 - Mobilfunkbetreiber sendet Zufallszahl (128Bit) an Mobiltelefon
 - Mobiltelefon und Betreiber wenden A3 zusammen mit dem gemeinsam bekannten Schlüssel Ki (128Bit) auf die Zufallszahl an.
 - Das Mobiltelefon schickt sein Ergebnis (32 Bit) an den Betreiber
 - Der vergleicht und gibt die Verbindung frei, wenn die Authentifizierung stimmt.
 - o Aus der Identifizierung (Ki) und der Zufallszahl wird mit Hilfe der Funktion A8 ein gemeinsamer geheimer Schlüssel für die Verbindung (Kc) von Mobilfunkbetreiber und Mobiltelefon berechnet.
 - o Die Nutzdaten werden dann über die Funktion A5 mit dem Schlüssel Kc für die Übertragung über die Luftschnittstelle verschlüsselt.
 - Es handelt sich um eine Stromchiffre, d.h. jedes Bit der Nutzdaten wird mit genau einem Bit des Schlüssels mittels XOR verknüpft.
 - o Sicherheit und Roaming
 - Beim Roaming wird die Identifikation durch den Mobilfunkbetreiber des Heimatnetzes durchgeführt, d.h. die Zufallszahl, das Ergebnis der Authentifizierung und Kc (64 Bit) werden beim jeweiligen Heimatmobilfunkbetreiber angefragt.
 - A5 ist einheitlich über Betreibergrenzen hinweg spezifiziert, die Verschlüsselung ist somit kompatibel.
 - o Anonymität
 - GSM verwendet nach erfolgreicher Authentifizierung nicht die weltweit eindeutige IMSI (International Mobile Subscriber Identity), sondern eine jeweils Temporär vergebene TMSI (Temporary Mobile Subscriber Identity), die zusammen mit der Local Area Identity (LAI) dem Mobilfunkbetreiber eine eindeutige Identifikation ermöglicht, die sich aber bei jedem Zellwechsel ändert.
 - o Kritik am Sicherheitskonzept
 - Die Funktionen für die Berechnung der Schlüssel sind nicht offen gelegt und können deshalb nicht wissenschaftlich untersucht werden.
 - A5 ist mittlerweile rekonstruiert und die Verschlüsselung zumindest theoretisch gebrochen
 - A3 und A8 verwenden den Algorithmus COMP128, der Schwächen hat, so kann der Schlüssel Ki aus einer Reihe von Authentifizierungsanfragen an eine SIM-Karte berechnet werden, die danach dupliziert werden könnte.
 - Kc ist zu kurz um Brute-Force-Angriffen zu widerstehen.
 - Die Basisstation identifiziert sich nicht gegenüber dem Mobiltelefon, nur umgekehrt erfolgt eine Authentifizierung

WLAN Verschlüsselung

- 3 Sicherheitskonzepte
 - o Authentifizierung mittels Zugriffslisten
 - Nur Rechner mit hinterlegter Rechneradresse können zugreifen
 - Problem, Rechneradressen können problemlos geändert werden
 - o Gemeinsames Kennwort für alle Access Points und Stationen über die dann jede Station jede Station authentifizieren kann (Test ob sie im Besitz des Kennwortes ist)
 - o Stationen und Access Points verschlüsseln alle Pakete mit Hilfe des gemeinsamen Kennwortes
 - Verschlüsselung über Wired Equivalent Privacy (WEP)
 - Jeder Teilnehmer im Netz erhält über einen sicheren Pfad einen geheimen Schlüssel
 - Aus dem geheimen Schlüssel wird eine Pseudozufallsfolge generiert, die mit den Daten im Rahmen einer Stromchiffre mit XOR verknüpft wird.

- Jedes zu sendende Paket wird mit dem Schlüssel symmetrisch verschlüsselt.
- Da der Empfänger über dieselbe Pseudo-Zufallsfolge verfügt, kann er durch nochmaliges Anwenden der XOR-Verknüpfung die Daten wieder herstellen.
- Der geheime Schlüssel wird relativ selten geändert. Zur Erschwerung der Analyse wird deshalb zusätzlich zum geheimen Schlüssel ein sogenannter Initialisierungsvektor (IV), der bei jedem Paket verändert werden muss im Klartext dem Paket beigefügt.
- 2 Schlüssellängen
 - 40 Bit fester Schlüssel und 24 Bit Initialisierungsvektor
 - 104 Bit fester Schlüssel und 24 Bit Initialisierungsvektor
- Der geheime Schlüssel und der Initialisierungsvektor werden verkettet und dienen als Eingabe für den Pseudozufallszahlengenerator (Pseudo Random Number Generator, PRNG), der mit dem Verfahren RC4 aus der Eingabe eine scheinbar zufällige Folge von Bits berechnet.
- Den Nutzdaten wird zur Überprüfung der Integrität der Daten auf der Empfängerseite noch eine Cyclic Redundancy Check (CRC)-Prüfsumme angehängt. (Integrity Check Value ICV), bevor die Daten verschlüsselt werden.
- Auf der Empfängerseite wird nach Übertragung der Daten und der Entschlüsselung der ICV neu gebildet und überprüft, stimmt er nicht, wird das Paket verworfen.
- Identifikation kann vor dem Nachrichtenaustausch im Rahmen Challenge-Response-Verfahren erfolgen.
 - Dem zu identifizierenden Teilnehmer wird ein 128 Bit Zufallsfolge unverschlüsselt geschickt.
 - Diese muss vom Empfänger mit WEP-Verschlüsselt zurückgesandt werden.
 - Nur wenn nach der WEP-Entschlüsselung die ursprüngliche Folge wieder erhalten wird, gilt der Kommunikationspartner als identifiziert
- Kritik an WEP
 - Alle Teilnehmer gelten als Vertrauenswürdig, kein Schutz vor Angreifern, die selbst am drahtlosen Netz teilnehmen dürfen
 - Der kurze 40 Bit Schlüssel bietet keinen Schutz vor Brute-Force-Angriffen.
 - Einige WLAN_Karten ändern den Initialisierungsvektor gar nicht bzw. nicht häufig genug
 - Algorithmus RC4 gilt mittlerweile als nicht mehr sicher, da bei „schwachen“ Schlüsselkombinationen die Kenntnis nur weniger Schlüsselbits genügt um auf die gesamte Ausgabe zu schließen.
 - 24 Bit Initialisierungsvektor ist zu kurz um ausreichend viele Permutationen zu zulassen, wenn mit hoher Netzlast gearbeitet wird.
 - CRC—Verfahren ist ungeeignet die Integrität der Pakete zu sichern, da CRC linear ist, kann ein Angreifer einige Bits des Originalpaketes ändern und eine neue CRC-Summe berechnen, ohne den kompletten Klartext des Paketes zu kennen.