COMP90018 Mobile Computing Systems Programming

Frederick Zhang & Yungang Feng

09/11/2017

Week 1: Introduction

1.1 Mobility Impacts (CN VM)

- Voice communication
- Computing
- Navigation
- Media

1.2 Evolution of Phones (TV CG)

- Voice
- Text
- Connectivity
- General Purpose

1.3 Context (D.A.M.P.)

- Differences to desktops
- Movement
- Posture
- Activities

1.4 Technical Constraints (BLINDERS PM)

- Disconnections
- Bandwidth
- Latency
- Network heterogeneity
- Security
- Energy usage
- Risk to data
- Memory
- Processing
- I/O

1.5 Mobile beyond Phones

Luggable -> Portable -> Wearable -> Insertable

Week 2: User Research & Ideation

2.1 Core areas of the UX (CUDA U)

- Usability: a measure of a user's ability to arrive on a site, use it easily, and complete the desired task.
- Useful content: the site should include enough information in an easily digestible format that users can make informed decisions.
- Desirable/Pleasurable content: the user can form an emotional bond with the product or website.
- Accessibility: content for the learning disabled needs careful consideration in order to provide a more complete user experience.
- Credibility: the site should be able to engender trust in the users.

2.2 Norman's Responses

- Visceral Design: the subconscious reaction based on appearance. (Look, Feel, Sound)
- Behavioral Design: the reaction that stems from the ease of difficulty of use. (Function, Understandability, Usability, Physical feel)
- Reflective Design: the reaction that derives from self-image, experience and memories.

2.3 Shared Value

- Desirability: wishes of stakeholders - Do they want this
- Feasibility: your ability to deliver - Can we do this
- Viability: whether you should even start the project - Should we do this

2.4 Double Diamond (Problem -> Solution)

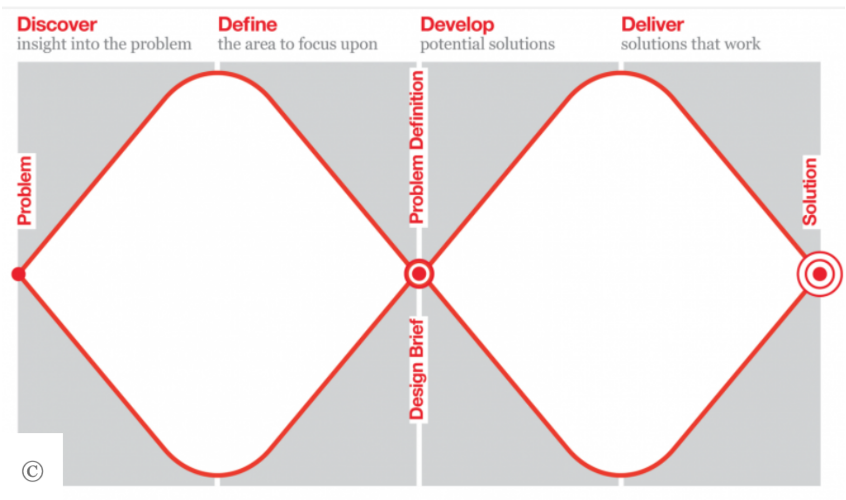

Figure 1: Double Diamond

Four phases in double diamond:

1. **Discover** insight into the problem (Divergent thinking)
2. **Define** the area to focus upon (Convergent thinking)
3. **Develop** potential solutions (Divergent thinking)
4. **Deliver** solutions that work (Convergent thinking)

2.5 Methods (TALL Plus)

2.5.1 Looking (Observational Methods)

- Ethnography: It is a qualitative orientation to research that emphasizes the detailed observation of people in naturally occurring settings.
- Shadowing: The researcher accompanies the user and observes how they use the product or service within their natural environment.
- Video diary: It collects quantitative data which is self-reported by participants over a period.

2.5.2 Learning Methods

- Cultural probes
- Technology Probes: draw from Social Science, Design and Engineering
- Competitor analysis

2.5.3 Asking Methods

- Questionnaires
- Interviews
- Contextual inquiry
- Guessability
- Experience sampling

2.5.4 Prototyping Methods

- Sketching
- Task flows
- Paper prototypes
- Wireframes
- High fidelity prototypes

2.5.5 Testing Methods

- Common myths about reasons for not doing it
- Large and multiple studies
- Discount usability
- Eye tracking
- Brainstorming

Week 3: Mobile Interaction Design

3.1 Waves of Mobile Computing

- Portability: reducing the hardware size to make it possible to move them relatively easily
- Miniaturization: radically smaller, enabling usage on the move
- Connectivity: Wireless data networks on the move
- Convergence: bringing device types together
- Divergence: specialized functionality rather than generalized ones
- Apps: building app for different kinds of functions
- Digital ecosystems: pervasive and interrelated technologies working together

Traditional phone	Current phone
tactile	touch
indirect	direct
key press	gestures
single key press	multi-touch
portrait	portrait or landscape

Table 1: Traditional and Current phone

3.2 4C Framework

	Many Users	Many artifacts
sequential	Communality • Personalization: the artifact is personalized to each user • Generalization: the artifact allows different users to immediately interact without any knowledge of their identity	Continuity • Synchronization: a user's data is synchronized across artifacts • Migration: the state of a user's activity is migrated from one artifact to another
simultaneous	Collaboration • Division: the artifact is divided into independent sections and each user can interact with it simultaneously • Merging: the artifact merges all users' interaction	Complementarity • Extension: interaction with an artifact is extended to another • Remote control: one artifact is used to control another

Table 2: Caption

Week 4: Processing Sensor Data

4.1 Challenges in Sensor Data

1. The sensor data on time t will strongly influence sensor at time $t + 1$
2. Data samples are discrete: no idea of what happens between 2 samples; not enough data point
3. Noise: may lose some information

4.2 Filters

Name	Description	Cons	Pros
Mean filter	Create the window of a given size, wait till window full, each value will be replaced by the mean value in the given window.	Easy to implement, efficient, great cost benefit	laggy, no dynamic models, susceptible to outliers
Weighted Mean filter	The old measurement still has effect, the newer, the larger effect.		
Median filter	computing/pick the median in time window	same as mean filter, plus good for sharp edge, alway use exist data	same as mean filter
Kalman filter	make most likely prediction based on dynamic model; use sensor data to correct the prediction	Dynamic model of the system; No lag; tunnable trade-off between model and measurement; uncertainty measurement	parameters not intuitive; overshooting
Particle filter	Generate hypotheses -> compute weights -> resample	general; continuous or discrete values; great result	lots of memory; very slow

Table 3: Filters

Week 5: Context and Activity Recognition

5.3 Context

1. Location
2. User's identity
3. Time of the day
4. Sound levels
5. Light levels
6. User's motion

5.4 Context awareness

1. Context display (GPS track your location)
2. Context augmentation (photo with location info)
3. Context-aware configuration (config how devices are used)
4. Context-triggered actions (change brightness)
5. Contextual adaptation of the environment (turn on heating when go to sleep)
6. Contextual mediation
7. Context-aware presentation (switch portrait to landscape)

5.5 Characteristics of Human Activity Recognition Systems (R.A.G.E.S.)

- Execution
  - online: process data as they come
  - offline: recorded all of the data before handle
- Generalisation
  - user independent: data for everyone
  - user specific: single person data
  - temporal: both cases
- Recognition
  - continuous: stream of data
  - segmented
- Activities
  - periodic
  - sporadic
  - static
- System model
  - stateless
  - stateful

5.6 The Process Pipeline

5.6.1 Choosing Sensors

1. what is it measuring
2. accuracy and precision
3. range of the sensor
4. resolution of sensitivity of the sensor
5. sampling rate or frame rate
6. cost

5.6.2 Pre-processing

1. Interpolation: deal with lower sampling rate, but will make up data that doesn't necessarily exist
2. Down sampling: deal with higher sampling rate

5.6.3 Segmentation

1. sliding window
   - non-overlapping sliding window
   - overlapping sliding window
2. energy based
3. additional context sources

5.6.4 Feature Extraction

Find the features based on the data in the segment window

5.6.5 Classification

- Hidden Markov Models
- Dynamic Time Wrapping
- kNN
- AdaBoost
- SVM
- Random Forest

5.7 Evaluation

1. Precision: $TP/(TP+FP)$
2. Recall: $TP/(TP+FN)$
3. F1 Score: $2*Precision*Recall/(Precision+Recall)$

Week 6.1 RFID

6.1 History of RFID Tags

6.1.1 Radar

- To warn of aircrafts
- Could detect only presence of an aircraft
- No friend or foe distinction

6.1.2 First Active RFID System

- Watson-Watt: first active identify friend or foe (IFF) system
- Each aircraft had a transmitter
- After transmitter received a radar signal it broadcast a signal back identifying an aircraft as friendly

6.2 RFID Technology

6.2.1 Tag

- Microchip connected to an antenna
- Can be passive, semi-passive, active
- No battery: passive
- Semi-passive: circuit is battery-powered except communication
- Promiscuous (true for most) or secure
- Interrogate/query tags via radio signals

6.2.2 Reader

- Interrogate/query tags via radio signals

6.2.3 RFID (Radio Frequency Identification)

- Reader (base station) sends a radio interrogation signal
- RFID tag backscatters its ID
- Proximity-based technology: determine the tag location by measuring the signal's time of flight (in theory)

6.2.4 Characteristics

- No line-of sight necessary (in contrast to barcodes)
- Resist environmental conditions
- RFID tags with read & write memory (nonvolatile EEPROM)
- Smartcard functionality (JavaCard): cryptographic computations for personal contact cards

6.3 Passive RFIDs

6.3.1 Operation

- Do not need an internal power source
- Operating power is supplied by the reader
- Electrical current induced in the tag's antenna by the radio signal pulse of the reader

6.3.2 Features

- Can be used for distance of up to 3 metres
- Can be very small
- Very cheap

6.4 Active RFIDs

6.4.1 Operation

- Own power source (battery life expectancy: up to 10 years)

6.4.2 Features

- Cost: a few dollars (much more expensive)
- Size: as small as a small coin (relatively larger)
- Support read ranges up to 100 metres (wider range)
- Deployment in more difficult RF situations (more enduring, e.g. in water)
- Tags have typically a higher scanning reliability
- Combination with sensors (vibration, light, humidity, ...)

6.5 RFID: Technical Features

6.5.1 Data Rate

- $9.6 - 115 kbit/s$

6.5.2 Devices

- Reader: simultaneous detection of up to 256 tags, scanning of up to 40 tags per second
- Response time of an RFID tag: less than 100 milliseconds

6.5.3 IDs

- Typically 64 or 96 bit (up to 128 bit)

6.6 RFID Frequencies

1. LF: Low Frequency ($125 - 134.2 kHz$, $140 - 148.5 kHz$)
   - Good penetration of materials including water and metal
   - Widely adopted (and used longer than HF)
   - No collision protocol available
   - Typical read range: 30cm (shortest)
2. HF: High Frequency ($13.56 MHz$)
   - Provides anti-collision protocols
   - Up to 1m read range (short)
3. UHF: Ultra-High Frequency ($868 - 928 MHz$)
   - Difficult to penetrate of water and metal
   - Read range: up to 3m (longest)
4. Microwave: $2.4 - 5.8 GHz$ or UWB: $3.1 - 10 GHz$
   - Read range: up to 2m (long), projected up to 200m for UWB (ultra-long)
   - High data rate

6.7 Pros and Cons of RFID

6.7.1 Advantages

- Very cheap, high volume, large variety
- Long industry experience
- Scanning even with high speeds possible ($300km/h$)
- No maintenance, simple to manage

6.8 Disadvantages

- No quality of service
- Only passive data acquisition (asymmetric communication)
- Possible interference with ISM bands

6.9 EPC (Electronic Product Code)

- Created by Auto-ID centre
- Successor of universal product codes (12 digit barcodes)
- Unique number to identify an item in the supply chain
- Specifies manufacturer, product category, item

6.10 Anti-Collision & Singulation

6.10.1 Problem

- RFID tags are simple and cannot communicate with other tags
- High probability that two tags in communication range respond simultaneously
- Collision: response on the same frequency at the same time

6.10.2 Anti-Collision and Singulation and Protocols

- Algorithms to identify all tags
- Anti-collision: trade time for the possibility to interrogate all tags
- Singulation: identify (iterate through) individual tags

6.10.3 ALOHA Protocol

1. Simple idea
   - Based on the classical ALOHA protocol (Abramson, 1970)
   - "Tag-Talks-First" behaviour: tag automatically sends its ID (and data) if it enters a power field
   - If a message collides with another transmission, try resending it later after a random period
2. Collision types
   (a) Partial
   (b) Complete
3. Terminologies

   Switch-off After a successful transmission a tag enters the quiet state

Slow down Reduced the frequency of tag responses

Carrier sense

- No carries sense possible (tags cannot hear each other)
- Use ACK signal of the reader in communication with another tag
- Reader broadcasts a MUTE command to other tags if it interrogates one tag

4. Frame Vulnerability

   - Partial overlap leads to a maximum throughput of a 18.4% (assuming a Poisson distribution)

5. Slotted ALOHA

   - "Reader-Talks-First": use discrete timeslots SOF (start-of-frame) and EOF (end-of-frame)
   - A tag can send only at the beginning of a timeslot
   - Leads to complete or no collision
   - Increased maximum throughput of 36.8%
   - "Early end": reader sends out an early EOF

6. Frame-Slotted ALOHA

   - Group several slots into frames
   - Only one tag transmission per frame
   - Limits frequently responding tags
   - Adaptive version: adjust the number of slots per frame

7. Comparison

Table 4: Comparison between ALOHA, Slotted and Frame-slotted

Protocol	+	-
ALOHA	Adapts quickly to changing numbers of tags Simple reader design	Worst case: never finishes Small throughput
Slotted ALOHA	Doubles throughput	Requires synchronisation Tags have to count slots
Frame-slotted ALOHA	Avoids frequently responding tags	Frame size has to be known or transmitted; similar to slotted ALOHA

6.10.4 Binary Tree Protocol

- "Reader-Talks-First" behaviour: reader broadcasts a request command with an ID as a parameter
- A sub-tree T is searched by an identifier prefix
- Only tags with an ID lower or equal respond
- An interrogated tag is instructed to keep quiet afterward
- Repeat algorithm until no collision occurs or all tags are quiet

6.11 RFID Applications

- E-passports
- Transportation payment
- Electronic toll collection
- Vehicles
- Supply chain & inventory management
- Prevention
- Product tracking
- Human implants
- Altering
- Authentication
- Identification
- Monitoring

6.12 Status Quo of RFID Systems

- No authentication
  - Readers are blind: if tags does not reply, readers does not know about it
  - Tags are promiscuous and reply to any reader
- No access control
  - Malicious reader can link to a tag
  - Malicious tag can spoof a reader
- No encryption
  - Eavesdropping possible (especially for the reader)
- Man-in-the-middle attack

6.13 Privacy Concerns

6.13.1 Unauthorised Surveillance

- Simple RFID tags support no security mechanisms
- Permanent RFID serial numbers can compromise privacy (RFID tag remains intact even after disposal of goods)

6.13.2 Potential Risks

- Tags in goods might be a potential risk (high gain antennas allow RFID scanning over larger distances)
- Threat: scanning of assets of high value

6.14 RFID Tag Privacy

- Killing: tag deactivation
- User intervention
- Silencing: metal lining
- Active jamming
- Hash-locking
- Encrypting: silent tree walking
- One time identifies (pseudonym rotation)
- Hiding: blocker tags
- Keyless "Encryption"
- Effective against sniffing and tracking
- Effectiveness drops sharply with more items
- Shamir tags: unknown tags take long time to read
- Impedes tracking & unauthorised identification

6.15 RFID Tag Authenticity

6.15.1 Threats

- Cloning: copying existing tags
- Forgery: creating new tags with a valid identity
- Relabeling

6.15.2 Track & Trace

- Application anticipates tag movements, detects and reports anomalies and duplicates

6.15.3 Approaches

- Static authentication
  - Tag identifier includes a digital signature
  - Protects against forgery, but not cloning
- Static authentication with public-key protocol
  - Tag authenticates reader by public-key protocol
  - Encrypts digital signature with reader's public key
- Pseudonym tag with mutual authentication
  - Tag presents one-time identifier
  - Reader sends corresponding one-time PIN
  - Tag returns its own one-time PIN for authenticity
  - Protection against both threats if enough identifiers
- But: key exchange
  - Reader must know password
  - A single password is a bad password

- If more passwords: reader needs to know with tag it is

- Solution?
  - Reader checks many passwords
  - How does the reader know about the password

6.16 RFID Security Schemes

6.16.1 Rolling code schemes (cheap)

- Common pseudo-random number generator in transmitter and receiver to produce a sequence
- Transmitter sends code in sequence
- Receiver compares this code to its calculated code
- Implementation compares within the next n codes

6.16.2 Challenge-response protocols (expensive)

- Secret information is never communicated insecurely
- Reader issues a challenge to the tag
- Tag responds with a cryptographic encoding using a key

6.17 RFID "Bill of Rights"

- Consumers should have the right
  - To know whether products contain RFID tags
  - To have RFID tags removed o deactivated when they purchase products
  - To use RFID-enabled services without RFID tags
  - To access an RFID tag's stored data
  - To know when, where and why tags are being read

6.18 RFID Future Directions

6.18.1 Super-distributed RFID infrastructures

- Massive number of tags are placed on an object
- Redundancy: a single tag becomes insignificant
- Leads to discretisation of the world around us

6.18.2 Applications

- Indoor localisation and positioning
- Collaboration
- Distributed storage of information

Week 6.2 Mobile Games

6.19 Low-Level UI

6.19.1 Tasks of a low-level API

- Precise control about what is drawn
- Control about the location of an item
- Handle basic events such as key presses
- Access specific keys

6.19.2 User Interfaces vs. Games

Table 5: Comparison of User Interface and Games

UI is event driven	Game is time-driven
UI is updated in response of to user input	Run continuously
Events: pressing a soft key, selecting an item, etc	Updates occur with and without user input

6.20 The Purpose of a Game API (memorise sub-titles)

6.20.1 Screen Buffer & Layers

1. `GameCanvas`
   - Dedicated screen buffer (`Graphics` object)
   - Supports incremental updates (instead of rendering entire frame)
   - Flush graphics: display contents of buffer
2. Layers
   - Sprites and tiled layers
   - Can be visible or invisible

6.20.2 Key Polling

- Query the status of keys
  - Is a key pressed and which key is pressed
  - Duration of a key press
  - Are keys pressed simultaneously
  - Are keys pressed repeatedly

6.20.3 Sprites

1. Definition
   - Figure in a 2D that is part of a larger (game) scene
   - Parts can be transparent
   - A sequence of sprites enables animation
2. Animations
   - Frame sequence of a sprite
   - Ordered list of frames to be shown
   - Sprite is n frames
   - Frames can be omitted, repeated

6.20.4 Tiles

- Tile is a small (rectangular) image that can be combined with other tiles to larger images
- 2D games with large background images are composed of tiles
- A set of tiles is small; little memory required

6.20.5 Collision Detection

1. Collision rectangle
   - Each sprite has a collision rectangle; usually the size of the sprite
   - Can be smaller to exclude parts of the sprite
2. Boundary-level detection (fast)
   - Test if two collision rectangles intersect
3. Pixel-level detection (precise)
   - Collision if opaque pixels touch

6.21 Features of Mobile Game Development

1. Processing and network
   - Less CPU power, (usually) no hardware acceleration, less memory, intermittent network connections
2. Hardware
   - Input capabilities
   - Screen size
3. Portability
   - Sensors: location, acceleration, camera, etc
   - Context-awareness, use environment as part of the game
   - Device as controller
   - Mixed reality games, location-based games, etc

6.22 Tips for Good UIs

Table 6: UI Design Tips

Prefer	Avoid
Relative positioning	Absolute positioning
Text extensively	Many pictures
Compress images	Large images
Reduce image size	Animations (except games)
Separate page sets	Horizontal scrolling

6.23 Usability Guidelines for (Mobile) Games

6.23.1 Game Start

1. Opening screen
   - Splash screen
   - Limit the number of screens before the game start
2. Main menu
   - Game's main menu: custom graphics
   - Avoid using UI components with standard graphics
   - Help item

6.23.2 Game Controls

1. General design
   - Avoid the need for pressing two keys simultaneously: difficult on small keyboard
   - Now: gestures
   - One key ōne command
2. In-game design
   - Pause the game and show the main menu

6.23.3 Pause & Save

1. Single-player games
   - Provide save game capability
   - Provide pause game capability
2. Two-player games
   - Pause mode applies to both players
   - Provide information about why the game is paused
3. Multiplayer games
   - Interruption of one player does not impact other players
   - Switch player to background or drop player from the game

6.23.4 Feedback

1. Status information
   - Health, points, level, score, etc
   - Not too much technical information
2. Clear feedback on game goals
   - Computed level, bonus level is reached, etc
   - Essential elements require visual feedback: game is playable without sounds
3. Multiplayer games
   - Who has won, who has lost
   - Show a user's performance by using *you* instead of a name
   - Challenges: feedback that a challenge has been sent successfully

6.23.5 Game Experience

1. Easy to learn but difficult to master
2. Rewards
3. Difficulty level

6.23.6 Noise Pollution

1. Sound volume
   - Default: close to regular volume
   - Enable different sound levels for background music and game sounds
   - Ability to turn sounds off quickly
   - No high-pitched sounds
2. Bluetooth multiplayer games
   - Synchronised the background music

6.23.7 Distinctive Graphics

1. Avoid
   - Small text on the screen
2. Appearance of game objects and characters
   - Easily understood
   - Different items should look different
3. Multiplayer games
   - Identify who is who
   - But: always the same colour for the same player

6.23.8 Post Game

1. High score lists
2. Easy restart

6.23.9 Criteria for Mobile Games

1. Easy to learn
2. Interruptible
3. Subscription
4. Social interactions
5. Take advantage of smartphones

6.23.10 Optimising Mobile Games

1. Guideline
   (a) First complete the game, optimise later
   (b) 90/10 rule
      - 90 percent of execution time
      - 10 percent of the code
      - Use a profiler
   (c) But
      - Aim to improve the actual algorithms before resorting to low-level techniques
2. Why not to optimise
   - Introduction of bugs
   - Decrease of the portability of code
   - Spending a lot of time for little results
   - Only optimise code if the game is unplayable otherwise
3. Optimisation tricks
   - Use `StringBuffer` instead of `String`
   - Access class variables directly
   - Use local variables
   - Variables are more efficient than arrays
   - Count down in loops
   - Use compound operators
   - Remove constant calculations in loops
   - Reuse objects
   - Assign null to unused objects & unused threads

Week 7.1 Location Privacy

7.1 Introduction

7.1.1 Definition

1. Location-based services (LBS)
    - Services that integrate a mobile's device location with other information
    - Available at least since 1970s
2. Mobile operators
    - Voice
    - Data (SMS, MMS, Video)
    - Location information
3. Push vs. Pull
    - User receives information without an active request
    - User actively pulls information from the network

7.1.2 Applications

- Infotainment services
- Tracking services
- Information dissemination services
- Emergency support systems
- Location-sensitive billing

7.1.3 Location-based Service Generations

- 1st Generation
    - Manual user input of location information
    - Driving directions, nearby POIs, weather information
- 2nd Generation
    - Location information is acquired automatically within a couple of kilometres
    - Similar services as in 1st generation
- 3rd Generation
    - High position accuracy & automatic initiation of services
    - Asset tracking, street-level routing and positioning, etc

7.1.4 LBS and their required accuracy

- High
    - Asset tracking
    - Directions
    - Emergency
- Medium to high
    - Advertising
    - Car navigation

    - POI

- Low
    - Fleet management
    - News
    - Traffic information

7.1.5 Location Engine

1. (Reverse) Geocoding
    - Translate street address to latitude & longitude and vice versa
    - Difficult if not complete information available
2. Routing & navigation
    - Compute best route: A^*, Dijkstra, etc
    - Best: shortest, fastest, simplest
3. Proximity search
    - Spatial DBs: POIs such ATMs, hotels, gas stations, etc

7.2 Importance of Location Privacy

7.2.1 Privacy Concerns

- "They know where you are: new technologies can pinpoint your location at any time and place. They promise safety and convenience – but threaten privacy and security."
- Lack in privacy-aware systems

7.2.2 Location Privacy Statue Quo

1. Status quo of current mobile systems
    - Able to *continuously* monitor, communicate and process information about a person's location
    - Have a high degree of spatial and temporal precision and accuracy
    - Might be linked with other data
2. Import research issue
    - Techniques for protecting location privacy are required

7.2.3 Importance of Location Privacy

1. Location-based spam
    - Unsolicited advertising
2. Personal safety
    - Stalking
    - Assault
3. Intrusive inferences
    - Person's political views
    - Individual preferences
    - Health conditions

7.3 Techniques for Location Privacy

7.3.1 Stealth

1. Stealth
   - Ability to be a location without anyone knowing you are there
2. How
   - Use of passive devices such as GPS
3. Disadvantages
   - Active devices such as mobile phones cannot preserve stealth
   - Access of information overrides stealth

7.3.2 Anonymity-Based Approaches

1. Idea
   - Separate location information from an individual's identity
   - Special type is *pseudonymity*: an individual is anonymous but has a persistent identity (a pseudonym)
2. Disadvantages
   - Vulnerability to data: a person's identity can be inferred from his or her location over time, in particular from homes or offices
   - A barrier to authentication and personalisation
   - Efficacy in sparsely populated areas?

7.3.3 *k*-Anonymity

1. Sweeney (2000)
   - Analysis of microdata
   - Anonymised health records: DoB, Gender, ZIP code
   - Uniquely identified medical records of the governor of Massachusetts (DoB, Gender, ZIP are *quasi identifiers*
   - 87% of population can be identified
2. Database: k-anonymity (Sweeney 2002)
   - A table is k-anonymity if every record in the table is indistinguishable from at least $k-1$ other records with respect to quasi identifiers

7.3.4 Anonymity: Cloaking

1. Spatial cloaking
   - Gruteser & Grunwald use quadtrees
   - Adapt the spatial precision of location information about a person according to the number of other people in the same quadrant
2. k-anonymity
   - Individuals are k-anonymity if their location information cannot be distinguished from $k-1$ other individuals
3. Temporal cloaking
   - Reduce the frequency of temporal information

7.3.5 Basic Model

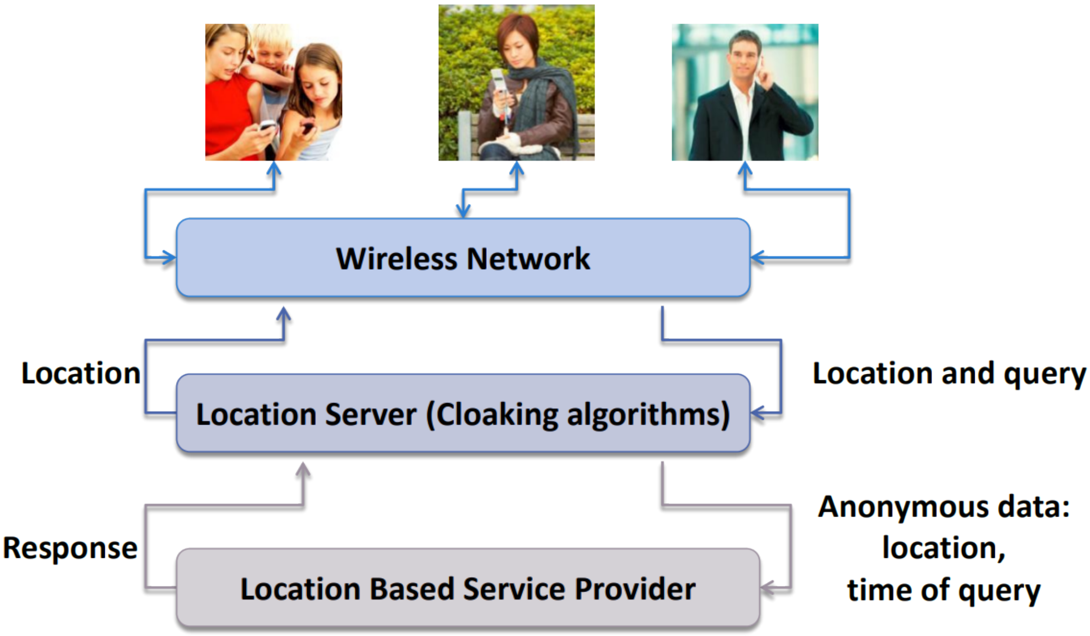

Figure 2: Location Privacy Basic Model

7.4 Location Privacy Through Obfuscation

1. Idea
   (a) Mask an individual's precision
   (b) Deliberately degrade the quality of information about an individual's location (imperfect information)
   (c) Identity can be revealed
2. Assumption
   - Spatial imperfection ≈ privacy
   - The greater the imperfect knowledge about a user's location, the greater the user's privacy

7.5 l-Diversity

7.5.1 Attacks on k-anonymity

- Homogeneity attack
- Background attack

7.5.2 l-Diversity

1. l-Diversity Principle
   - A q*-block is l-diverse if contains at least l "well represented" values for the sensitive attribute S
   - A table is l-diverse if every q*-block is l-diverse
   - An attacker needs $l-1$ damaging pieces of background knowledge to eliminate all $l-1$ possible sensitive values
2. LBS
   - POI or content of queries

7.6 Decentralised Approach to Location Privacy

7.6.1 Centralised Approach

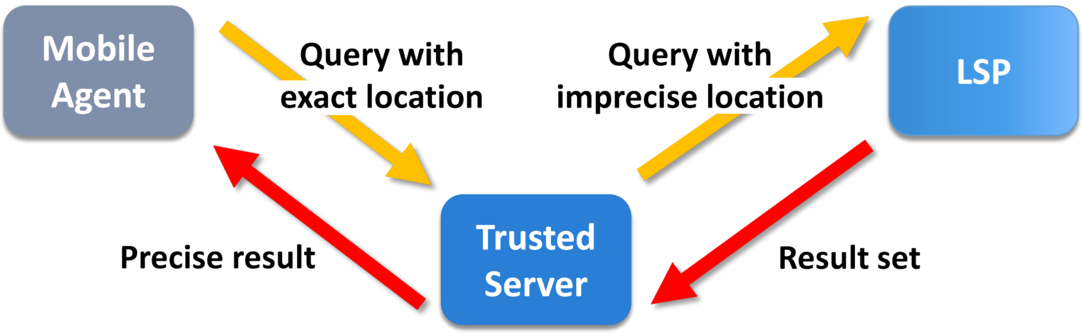

Figure 3: Centralised Approach

- Limitations
  - Communication overheads
  - Security threats
  - Single point of failure

7.6.2 Decentralised Approach

1. Idea
   - Use WPANs (spontaneous local ad-hoc networks), e.g. Bluetooth or 802.11
   - Clique: form spontaneous local ad-hoc networks that are wirelessly connected
   - Do no disclose your precise position to anyone (obfuscation) including your neighbours
2. Two roles
   - Hide service request from mobile phone operator, i.e. separate an agent's request (query requester) from the agent requesting this service (query initiator)

Week 7.2 Mobile GUIs

7.7 Mobile Programming Flavours

1. Server-based approach
   - Create a web service
   - Client (the mobile device accesses the content via a browser
2. Device-based approach
   - Develop application with an SDK
   - Deploy the application locally on the mobile device

7.8 UX Design Principles

1. Minimise the amount of work required for a task

   Progressive disclosure Show only some information and let user choose if they require more details

   Use examples Instead of (long-winded) descriptions use examples

   Affordances of objects If an object is clickable make sure it looks it

   Limit features Only provide the features that users need; otherwise you end up with a bad user experience

   Use defaults Less typing and interaction speeds up tasks

2. Acknowledge limitations of users

   Focus Only show information that is required

   Easy readability Use headers and short blocks of information

   Avoid multitasking Humans are not good at this

   Preference or performance People prefer short line lengths but read better at longer ones

3. Acknowledge user mistakes

   Anticipation Be prepared for user mistakes, i.e. anticipate and prevent them

   User confirmation If actions or errors have significant implication, use confirmation dialogs

   Prefer prevention Prevention of errors is better than correction

   Break difficult tasks up into smaller ones Easier for users to avoid errors

   Transparent automatic error correction Support this but make it explicit to users

4. Acknowledge human memory

   Monitor user behaviour User action is more reliable than user surveys

   Do not rely on human memory Keep tasks simple between views and pages; people can only remember 3 to 4 things at a time according to newer research

5. Various tidbits

   Attention Decide whether to stand out in terms of being different or novel (colours, design, fonts, etc.) or if a task has to avoid distraction

   Feedback Users have to know what happens, in particular, for long lasting tasks

   Easy access to more information People crave for information

   Grouping Objects that are close (or of the same colour) are assumed to go together

   Canonical perspectives Help to identify objects

7.9 History of J2ME/Java ME

1990 Java

- Internal project at Sun Microsystems

1995 JDK 1.0

- Applets & servlets

1999 Division of Java

- Java 2 Enterprise Edition (J2EE)
- Java 2 Standard Edition (J2SE)
- Java 2 Micro Edition (J2ME)

2000 Mobile phones begin to support J2ME

2004 250 million mobile phones support J2ME

2005
- 700 million mobile phones support J2ME
- Most mobile phone manufacturer support J2ME

MIDlet Like applets or servlets MIDlets (MID = mobile information device) have a small number of states

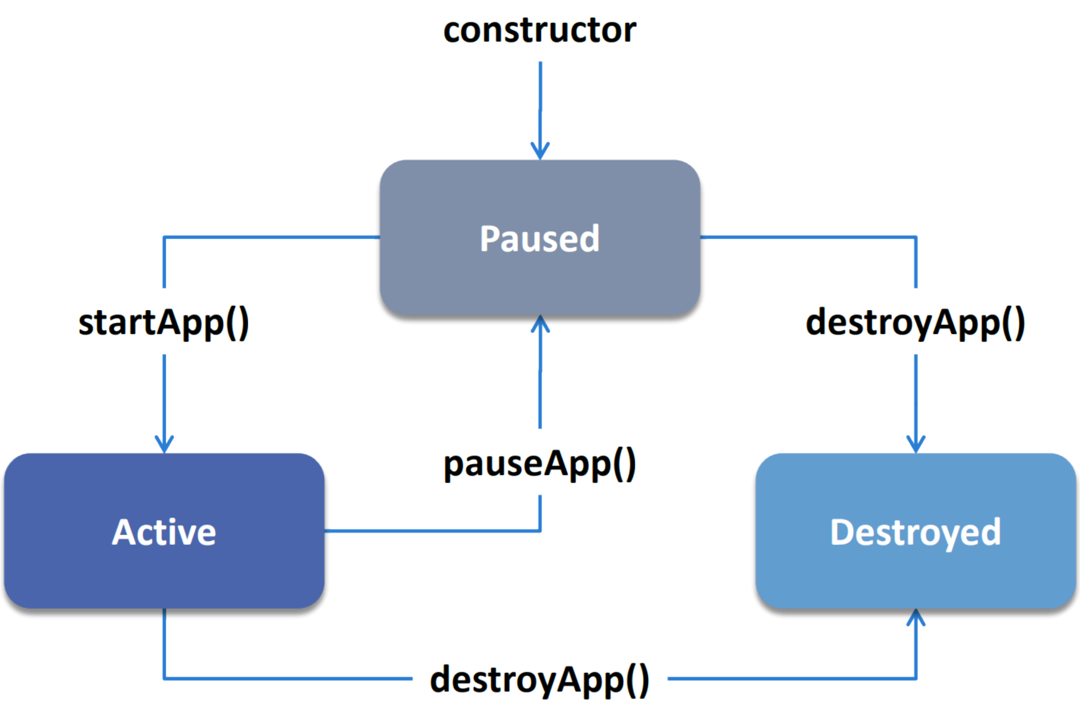

Figure 4: Life Cycle of a MIDlet

7.10 MIDP (Mobile Information Device Profile) GUI Programming

7.10.1 MIDP vs AWT

- AWT (abstract window toolkit) is designed for PCs
- AWT is designed for a pointing device (mouse)
- AWT supports window managements (resize windows, move windows)
- Smartphones have different requirements
  - A single screen; no overlapping windows (no window manager required); no complex tables
  - Input often limited to keypad or virtual keyboards

7.10.2 Input Mechanisms

1. Keypad input
   - Mobile phones: 12-digit keypad
   - Good for numbers, cumbersome for text
   - Predictive input technology: T9 = text on 9 buttons; only one button press per letter required
2. Keyboard input
   - Bluetooth keyboards
   - Thumb-based keyboards (BlackBerry devices)
   - Virtual keyboards
3. Pen-based input
   - Touchscreen with a stylus
   - Soft keyboards
   - Character recognition
   - Handwriting recognition
   - Graffiti (Palm OS)
4. Voice input
   - Simple commands
   - Earlier: VoiceXML where complex commands are recognised by a server
   - Now: Siri

7.11 UI Support

7.11.1 Introduction

1. Large heterogeneity of mobile devices
   - Screen size, screen orientation, input capabilities, etc
2. Abstraction
   - Use abstract descriptions: provide a "Cancel" button
   - Less code in your application
3. Discovery
   - Learn a device's capabilities at runtime

7.11.2 High-Level User Interfaces

1. Goal: portability
   - High degree of abstraction
   - No dedicated control of look and feel
   - Benefit: application uses native look and feel
   - Good end-user experience
2. Consequences
   - Drawing is performed by the OS of the device
   - Navigation & low-level functions are done by the device

7.11.3 Low-Level User Interfaces

1. Goal: precise control and placement
   - Games, charts, graphs, etc
   - Control of what is drawn on the display
   - Handle events such as key presses and releases
   - Access specific keys
2. Consequences for portability
   - Platform-independent methods (use keys defined in canvas)
   - Discover the size of the display, orientation, other capabilities (e.g., sensors)

7.12 (MIDP) GUI Guidelines

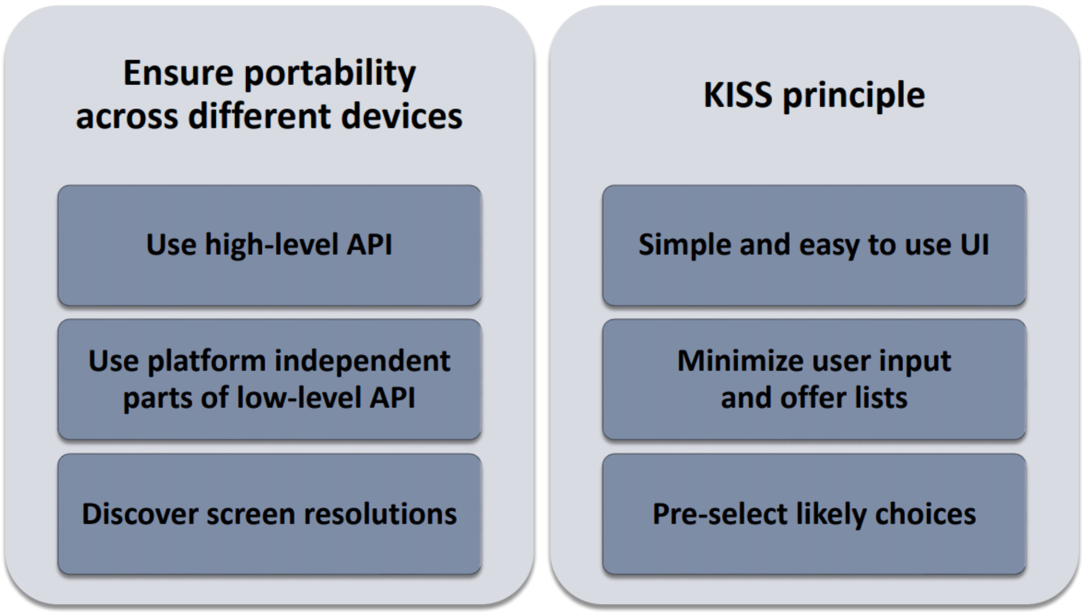

Figure 5: (MIDP) GUI Guidelines

7.13 UI Elements

- Buttons
- Checkboxes & radio buttons
- Switches
- Segmented controls
- Stepper
- Slider
- Popup menus
- Pickers
- Text fields iOS: `UITextField`, `UITextView`, `UILabel`
- Text fields Android: `TextView`, `EditText`, `Attributes`
- Images

- Lists
- Alerts & Dialogs
- Collections
- Scroll views
- Navigation
- Refresh

Week 8 Wireless Sensor Networks

8.1 Preliminaries

- Communication
  - Communication is expensive(use only if necessary)
  - A node communicates only with its neighbors
  - Wire less addvantage: all neighbors in broadcasting range listen

8.2 Topology Control

- Estabilish communication with other nodes
  - Discovery of nodes in communication range
  - Topology is determined by communication range
  - Adjust communication range (save energy)
- Critical transimission range: minimum transmission range to connect all nodes
- Assumption: all nodes have the same transmission range r
- Locations are known a priori
- Nodes locations are not known accurately

8.3 Criteria for routing algorithms (SUQ)

1. Size of the routing table
2. Quality of the route for a given destination
3. Update cost

8.3.1 Mobile ad hoc NET (MANETs) VS. WSNS

WSNs are MANETs
Differences:

- Scalability: number of node is potentially larger
- Fault tolerance: sensor nodes are more prone to failure
- Energy-awareness: nodes have a very limited amount of energy

8.4 Terminology

1. Routing: transport messages between two nodes
2. Data dissemination: transport messages from a node to many nodes
3. Broadcasting: transport messages from a node to all nodes
4. Data gathering: transport messages from nodes to a sink
5. Base station: node providing a gateway or central processing
6. Sink: node requesting information
7. Source: node generating information
8. Interest: message requesting a certain type of information

8.5 Sensor Network Architectures

8.5.1 Layered architecture

A single powerful base station with layers (nodes with the same hop-count to the base station)

8.5.2 Flat architecture

Each node has the same role

8.5.3 Hierarchical or clustered architecture

- nodes are organized into clusters
- nodes in a cluster send their messages to cluster heads
- cluster heads send the messages to a base station

8.6 Topology-based routing

- Approach: use information about links in the network
- Proactvie protocols: compute routes before routing
- Reactive protocols: discoveer routes on-demand
- Hybrid protocols: compute routes once, then update

8.7 Flooding vs Gossiping

	Technique	Advantage	Disadvantage
Flooding	each node that receives a message broadcasts this message if: the node is not a goal node; the maximum hop count is not reached	no topology maintenance; no complex route discovery	Implosion: receive same message from different neighbors; Duplication: nodes send the same message to their neighbors; Resource blindness: not aware of the energy levels of the mobile device
Gossiping	Limited broadcast: nodes broadcast received messages to a randomly selected neighbor	no implosion and lower overhead	long travel time for messages; no delivery guarantee

Table 7: Flooding vs Gossiping

8.8 Locality insensitivity

Destination is a few hops away but the entire network is flooded.
Solution: Flood with growing radius; slow flooding

8.9 Source routing

Nodes store routing information for other nodes.
Ideas:

- source node stores the whole path to the destination
- source node encodes the path with every message
- nodes on the path remove their ID from the message before relaying the message to the next node.

8.10 Dynamic source routing

8.11 Improving source routing

1. Caching of routes
2. Local search: flooding with TTL+1
3. Hierarchy of nodes: nodes with the same IP prefix are in the same direction
4. Clustering
5. Implicit acknowledgment: symmetric links

8.12 Directed Diffusion

8.12.1 Characteristics

1. Data centric
2. Request driven
3. Localized reinforcement and repair
4. Multi-path delivery

8.12.2 Directed Diffusion: Design Choices

Diffusion Element	Design Choices
Interest Propagation	Flooding; Constrained or directional flooding based on location; Directional propagation based on previously cached data
Data Pata propagation	Reinforcement to single path delivery; Multipath delivery with selective quality along different paths; Multipath delivery with probalistic forwarding
Data Caching and Aggregation	For robust data delivery in the face of node failure; For coordinated sensing and data reduction; For directing interests
Reinforcement	Rules for deciding when to reinforce; Rules for how many neighbors to reinforce; Negative reinforcement mechanisms and rules

Table 8: Design Choices

8.13 Rumor Routing

8.13.1 Query flooding

- A node interested in an event floods the network
- Transmission for n nodes: Q x n (Q number of queries)

8.13.2 Event flooding

- A node sensing an event floods the network
- Transmission for n nodes: E x n (E number of events)

8.14 Low-Energy Adaptive Clustering Hierarchy (LEACH)

8.14.1 Goal

- minimize energy dissipation in SNs
- all nodes consume a similar amount of energy

8.14.2 Architecture

- Hierarchical protocol
- Select random nodes as cluster heads
- Periodic reselection cluster heads after a steady phase

8.14.3 Disadvantages

- "Hot Spot" Problem: nodes on a path from an event-congested area to the sink may drain
- Stationary Sink: may be unpractical
- 1 hop neighbors: basic algorithm assumes any node can communicate with sink but: extensions are possible

8.15 Threshold sensitive Energy Efficient Network protocol (TEEN)

8.15.1 Cluster head sends hard and soft thresholds

1. Hard threshold: a member only sends data to CH only if data values are in the range of interest
2. Soft threshold: a member only sends data if its value changes by at last the soft threshold

8.15.2 Advantages

- good for time-critical applications
- less energy consumption compared to proactive approaches
- hard and soft threshold can be adapted depending on applications

8.15.3 Disadvantages

- Inappropriate for periodic monitoring such as habitat monitoring
- Ambiguity between packet loss and unimportant data

8.16 Sensor Protocols for Information via Negotiation (SPIN)

Communicating raw sensor data is expensive, but meta=data about sensor data is not. Extend lifetime of the system. Solves flooding disadvantages.

8.17 Localization

Means for a node to determine its physical position.

8.17.1 Importance

1. Increase the use of sensor readings
2. Essential in some communication protocols

8.17.2 Why not locate nodes during deployment

1. Large number of nodes
2. Mobile nodes
3. Air-drop, hostile environment

8.17.3 Limits of GPS

1. Indoor environment, under foliage, next to high-rise buildings
2. Cost in terms of hardware and energy expenditure

8.18 Range-based methods

8.18.1 Idea

1. Absolute point-to-point distance estimates
2. Angle estimates

8.18.2 Localization by Landmarks

Compute a node's location from 3 or more landmarks (a node that knows its own location), least-square technique for n landmarks nodes to improve precision

8.18.3 Distance estimate techniques

1. Received Signal Strength Inverse (RSSI)
2. Time On Arrival (TOA): one-way delay; round-trip delay
3. Time Difference of Arrival (TDOA)
4. Angle of Arrival (AOA)

8.18.4 Iterative Multilateration

Nodes recursively compute position estimates and spread position information.
Probliem: errors accumulate

8.18.5 Collaborative Multilateration

Collaborate and use all available measurements are used as constraints. Solve for the positions of multiple unknowns simultaneously.

8.19 Range-free Methods

No absolute range estimates are used. Normally more cost-effective, but less accurate than range-based methods.

1. Centroid Approach
2. Distance Vector Hop (DVH)
3. Approximate Point in Triangle (APIT)
4. Ring Overlapping ased on Comparison of RSSI (ROCRSSI)

	Centroid	DV-Hop	APIT
Accuracy	Fair	Good	Good
Node Density	>0	>8	>6
Degree of Irregularity	Good	Good	Good
GPS Error of Anchors	Good	Good	Good
Overhead	smallest	largest	small

Table 9: Caption

8.20 Sample attack scenario

1. Pretend to be close to the sink
2. Attract many packets
3. Drop some or all of them
4. DoS attacks for geographic routing protocols

Week 9 Mobile Networks

9.1 Wireless Wide Area Networks

9.1.1 Fundamentals

1. Analog signals

   - Continuous electrical signals varying in time
   - Usually analog signals are not smooth waveforms
   - Voice overlays carrier signal
   - Used in 1st generation wireless signals

2. Digital signals

   - Use of analog signals to transmit numbers
   - Conversion into bits
   - Transmission: streams of 1's and 0's
   - Used in all 2nd generation networks

9.1.2 Benefits of Digital Networks

1. Efficiency

   - Higher data transfer than analog networks
   - Enables compression for higher efficiency
   - Smaller power consumption

2. Security

   - Simple eavesdropping for analog signals with radio tuner
   - Even true for encrypted packets on analog networks
   - Digital networks: encryption of different strengths

3. Degradation and restoration

   - Degraded signals can be restored because each bit is either 0 or 1
   - Leads to better sound quality with less interference

4. Error detection

   - Parity bit signals if transmission was successful
   - Otherwise: retransmission or even error correction

5. Features

   - Caller ID and call answer
   - Data traffic

9.1.3 Switching Mechanisms

1. Circuit Switching

   - Establish a physical connection between sender and receiver
   - Used for landline telephone networks
   - Good voice but inefficient for data transmission
   - Lost connection results in long connection times

2. Packet switching

- Share a connection between users
- Divide data into small units with destination address
- Receiver restores original data format
- No dedicated connection is established (quick)
- Basis for 3G networks

9.1.4 Signal Propagation

1. Transmission range
   - Communication with low errors
2. Detection range
   - Detection but no communication (or with too many errors)
3. Interference range
   - Signal cannot be detected
   - Signal is part of the background noise

9.1.5 Issues in Wireless Transmission

1. Problems for wave propagation
   - Large objects -> shadowing & reflection (important indoors)
   - Small objects -> signal diffusion (scattering)
   - Large edges and corners -> signal deviation (diffraction)
   - Variation in medium density -> signal change and reflection (refraction)
2. Multipath propagation
   - Signal takes different paths between sender and mobile device

9.1.6 Multiplexing

1. Idea
   - Multiple channels share one medium with minimal interference
2. Multiplexing in 4 dimensions
   - Space
   - Frequency
   - Time
   - Code
3. Guard spaces
   - Reduce risk of interference between channels
4. Space Division Multiplexing
   (a) SDM
      - Communication using a single channel
      - Space channels physically apart to avoid interference

   (b) Cellular network
      - Reuse frequencies if certain distance between the base stations
      - How often can we reuse frequencies?
      - Graph colouring problem

5. Frequency Division Multiplexing
    (a) FDM
        - Division of spectrum into smaller non-overlapping frequency bands with guard spaces between to avoid overlapping
        - Channels gets band of the spectrum for the whole time
    (b) Advantages
        - No dynamic coordination required
        - Can be used for analog networks
    (c) Disadvantages
        - Waste of bandwidth if traffic distributed unevenly
        - Guard spaces
6. Time Division Multiplexing
    (a) TDM
        i. A channel gets the whole spectrum for a short time
        ii. All channels use same frequency at different times
        iii. Co-channel interference: overlap of transmissions
    (b) Advantage
        - High throughput for many channels
    (c) Disadvantage
        - Precise clock synchronisation
7. Combining FDM & TDM
    (a) FDM/TDM
        - Each channel gets a certain frequency band for a certain amount of time
        - More efficient use of resources
    (b) Advantage
        - Higher data rates compared to CDM
        - More robust against interference and tapping
    (c) Disadvantage
        - Precise clock synchronisation
8. Code Division Multiplexing
    (a) CDM
        - Each channel has a unique code (chipping sequence)
        - All channels use the same frequency
        - Each code must be sufficiently distinct for appropriate guard spaces
        - Uses spread spectrum technology
    (b) Advantages
        - No coordination and synchronisation required
        - Bandwidth efficient
    (c) Disadvantage
        - Lower user data rates

9.2 Wireless Personal Area Networks

9.2.1 Overview of Wireless Networks

Table 10: Four Types of Networks

Type	Coverage	Function	Cost	Throughput	Standards
WPAN	Personal space, 10m	Cable replacement	Very low	$0.1Mbps$ - $4Mbps$	IrDA, 802.15, Bluetooth
WLAN	Building, 100m	Extension, alternative to wired LAN	Low - medium	$1Mbps$ - $540Mbps$	802.11a, b, g, n, ac
WWAN	City or country	Extension of LAN	Medium - high	$8Kbps$ - $2Mbps$	GSM, TDMA, CDMA, GPRS, EDGE, WCDMA
Satellite	Global	Extension of LAN	Very high	$2Kbps$ - $19.2Kbps$	TDMA, CDMA

9.2.2 WPANs

1. WPANs: wireless personal area networks
   - Short range communication (personal space)
   - Low power consumption
   - Low cost
   - Small networks
   - No pre-existing infrastructure or direct connectivity other networks
2. Standards (sorted by data rate in descending order)
   - UWB (Ultra-wideband)
     - Wireless monitors, data transfer from digital camcorders, wireless printing of digital pictures
     - File transfer among cell phones and mobile devices
   - Bluetooth
   - ZigBee
3. Body area networks
   (a) Idea
   - Use natural electrical conductivity of the human body to transmit electronic data ($2.4KB/s$ up to $400KB/s$)

   (b) Possible applications
   - Car or phone recognises a user
   - Pay by touching a device in a bus
   - Device configures itself through touch
4. Ultra Wide Band
   (a) UWB
   - Possible successor of Bluetooth for transmitting high data rates at short ranges
   - Operates in the $3.1 - 10.6GHz$ frequency band
   - Radio always transmits at $640Mbps$ but maximum actual data rate is $480Mbps$ due to error correction

   (b) Applications

- Stream compressed video short distances, e.g. from a set-top box to a TV from a camcorder to a PC
- Wireless printing and wireless monitors

(c) Features

- P_t is transmit power and P_r is receive power or receiver sensitivity, and d is distance: $d \sim (P_t/P_r)^{\frac{1}{2}}$ or $P_r \times d^2 \sim P_t$
- Send a short pulse of an electrical charge into an antenna instead of varying the frequency or power level of a wave
- Signal cannot be detected by conventional radios

(d) High power efficiency

- Data is transmitted in short periods of time, i.e. the radio is mostly in low power state

(e) Security

- Stronger security than Bluetooth and WLAN
- All devices have unique IDs
- Generate cryptographic checksums to ensure that a message originated from a specific device ID
- Cryptographic sequence number: guards against replay attacks

(f) Future applications

- Precise location systems and real time location systems
- Precision radar imaging technology, even through walls

5. Bluetooth

(a) Goal

- Ad-hoc wireless connectivity for electronic devices
- Low-cost replacement for wires

(b) Name

- Suggested by Ericsson
- Harald Bluetooth
  - Viking king in Denmark, 10th century
  - United the country and introduced Christianity

(c) Radio technology

- Short range: 10m - 100m
- Unlicensed ISM (Industrial, Scientific and Medical) frequency band ($2.45GHz$)
- $1mW$ transmission power

(d) Networking

- Point to point: serial wire replacement between 2 devices
- Point to multipoint: ad-hoc networking of up to 8 devices

(e) Bluetooth vs IrDA

Table 11: Bluetooth vs. IrDA

	Bluetooth	IrDA
Medium	Radio waves	Infrared Light
Obstacles	Radio waves penetrate obstacles	Light is blocked by obstacles
Alignment	Omni-directional	Narrow focused beam
Data rate	$2Mbps$	$1-4Mbps$
Range	10-100m	2m
Energy	More power	Less power
Price	Moderate ($10)	Cheap ($1)

(f) Bluetooth applications

- Headsets for mobile phones
- Peripherals: mouse, keyboard, printer
- Game controllers
- File transfer for mobile devices
- Remove control

(g) Piconets (Ad-hoc network of up to 8 active devices)
- One device acts as a master, the other devices as slaves
- Each active slave has a 3-bit active member address; up to 7 active slaves
- Additional slaves synchronised to the master but not active are called parked
- A parked device has an 8-bit parked member address; up to 255 parked slaves

(h) Scatternets
- Connecting 2 up to 10 piconets
- A device acts a master in one piconet and as a slave in another piconet
- Devices were expected 2008

(i) Bluetooth Specification
   i. Specification
      - Radio technology
      - Software stack
      - Profiles
   ii. Spread spectrum frequency hopping
      - Packets are transmitted to a receiver over 79 hop frequencies in a pseudo random pattern
      - Transmitter switches hop frequencies 1600 times per second
   iii. Bluetooth security
      - Authentication and data encryption

(j) Bluetooth Pairing (Trusted relationship between two devices)
- Share a secret passkey
- Passkeys are stored on the device's file system (and not the Bluetooth chip)
- Trusted devices can encrypt data for exchange (128 bit)
- Trusted devices can cryptographically authenticate the identity
- Device either require pairing or asks whether a remote device can use its services

6. ZigBee

(a) Goal
- Wireless standard for sensing and control applications
- Highly reliable and secure, interoperable
- Started in 1999 and completed (1.0) end of 2004

(b) ZigBee (IEEE 802.15.4: low rate WPAN)
- Extremely low power
- $200Kbps$ maximum
- Sensors, interactive toys, smart badges, remote controls, home automation
- Routing protocol: AODV

(c) Introduction
   i. Standard for control and sensor networks
      - Developed by the ZigBee alliance
      - Based on the IEEE 802.15.4 standard
   ii. IEEE 802.15.4
      - Coded into the chip CC2420
      - SunSPOTs have this chip

- Requires a license (not free)
- Huge address space (64 bit IEEE address)
- Dual PHY
  - $2.4GhZ$ (16 channels), $250kbps$
  - $868/915MHz$ (1/10 channels), $20/40kbps$
- Power
  - Designed for months to years on batteries
  - Optimised for low-duty cycle (less than 0.1%)
  - 50m range (5-500m environment dependent)

iii. Compliance

- Requires no changes to the code
- Not ideal for research purpose

(d) ZigBee vs Bluetooth

Table 12: ZigBee vs Bluetooth

	ZigBee	Bluetooth
Network	Smaller packets over a large network: 2^64	Larger packets over a small network: 8
Memory Requirement	4-32KB	250KB
Network Joining	Rapid in milliseconds	Long in seconds
Cost	Less than a dollar	Several dollars
Bandwidth	$20 - 250kbps$	$1Mbps$
Range	10-100m	10m (up to 100m)
Battery Lifetime	Years	Days