Slide 1: Lecture 1: Introduction

IK2555: Mobile and Wireless Network Architectures: Lecture 1

prof. Gerald Q. Maguire Jr. http://people.kth.se/~maguire/

School of Information and Communication Technology (ICT), KTH Royal Institute of Technology

IK2555 Spring 2016 2016.01.08 © 2016 G. Q. Maguire Jr. All rights reserved.

Slide 2

1. Introduction

Lecture notes of G. Q. Maguire Jr.
For use in conjunction with Yi-Bing Lin and Ai-Chun Pang, *Wireless and Mobile All-IP Networks*, John Wiley & Sons; 2005, ISBN: 0-471-74922-2.

Slide 3

Welcome to the course!

The course should be fun.

We will dig deeper into Personal Communication Systems - with a focus on their **architectures**, but we will also examine some of the *protocols* which are used.

Information about the course is available from the course web page:
https://www.kth.se/social/course/IK2555/

Slide 4

Staff Associated with the Course

Instructor (Kursansvarig)

prof. Gerald Q. Maguire Jr. <maguire@kth.se>

Slide 5

Learning Outcomes

Following this course a student should be able to:

- Understand the architecture of existing mobile and wireless networks at a sufficient level to recognize the common features of such networks in **any** mobile or wireless network.
- Based upon recognition of common features, the student should be able to compare and contrast one network architecture with another.
- Describe differences between different types of mobility (such as user mobile, terminal mobility, session mobility) and understand how each type of mobility can be supported.
- Understand the core network protocols and applications in 3rd and 4th generation mobile networks.

Slide 6

Learning Outcomes (continued)

- Read the current literature at the level of conference papers in this area.

  While you may not be able to understand all of the papers in journals, magazines, and conferences in this area - you **should** be able to read 90% or more of them and have good comprehension. In this area it is especially important that develop a habit of reading the journals, trade papers, etc. *In addition, you should also be aware of standardization activities, new products/services, and public policy in the area.*
- Demonstrate knowledge of this area both orally and in writing.

  By *writing* a paper suitable for submission to conferences and journals in the area.

This course should prepare you for starting a Master's thesis project in this area (for undergraduate students) or beginning a thesis or dissertation (for graduate students).

Maguire IK2555, Spring 2016 Slide 6

Slide 7

Prerequisites

Internetwork (IK1550), Protocols and Principles of the Internet (IK2218), Advanced Internetworking (IK2215)

or

Equivalent knowledge in Computer Communications (in this case you need permission of the instructor)

Slide 8

Contents

The focus of the course is on **personal communication systems and their network architecture**. This spans the range from piconets to space probes, but the emphasis will be primarily focus on the range from LEO satellites down to personal area networks.

The course consists of 10 hours of lectures and a project of ~50+ hours effort.

Slide 9

Topics

- Personal Communication Systems (PCS): handoff, mobility, paging
- Network Signaling
- CDPD
- GSM, GPRS, SMS, International Roaming, Operation, Administration, Maintenance
- Number portability, VoIP, Prepaid
- WAP
- Heterogeneous PCS
- Wireless Local Loop (WLL), Enterprise Networks
- Personal Area Networks (PANs), such as Bluetooth and Ultrawideband (UWB)
- Wireless Local Area Networks (WLANs)
- Broadband Wireless Access (BWA)
- Sensor Networks

MAGUIRE IK2555, SPRING 2016 Slide 9

Slide 10

Examination requirements

Written and Oral project reports

Slide 11

Grades: A..F (ECTS grades)

To get an "A" you need to write an outstanding or excellent paper and give an outstanding or excellent oral presentation. (Note that at least one of these needs to be excellent.)

To get a "B" you need to write a very good paper, i.e., it should be either a very good review or present a new idea; and you have to give a very good oral presentation.

To get a "C" you need to write a paper which shows that you understand the basic ideas underlying mobile and wireless networks and that you understand one (or more) particular aspects at the level of an average master's student. In addition, you must be able to present the results of your paper in a clear, concise, and professional manner - and answer questions (as would be expected at a typical international conference in this area.)

Slide 12

Grades (continued)

To get a "D" you need to demonstrate that you understand the basic ideas underlying mobile and wireless networks, however, your depth of knowledge is shallow and you are unable to orally answer in depth questions on the topic of your paper.

If your paper has some errors (**including incomplete references**) or you are unable to answer in depth any questions following your oral presentation the grade will be an "E".

If your paper has serious errors or you are unable to answer basic questions following your oral presentation the grade will be an "F".

Slide 13

Grades (continued)

If your paper or oral presentation are close to passing, but not at the passing level, then you will be offered the opportunity for "komplettering", i.e., students whose written paper does not pass can submit a revised version of their paper (or a completely new paper) - which will be evaluated; similarly students whose oral presentation is unacceptable may be offered a second opportunity to give their oral presentation. If a student fails the second oral presentation, they must submit a new paper on a new topic in order to give an oral presentation on this new topic.

Slide 14

Grades (continued)

Note that there is **no** opportunity to raise your grade, once you have a grade of "E" or higher.

Slide 15

Project

Goals: to gain ***analytical* or *practical*** experience and to show that you have mastered some knowledge in this area and to encourage you to find a topic which interests you (since this will motivate you to really understand the material)

- Can be done in a group of **1 to 3** students (formed by yourself).
  Each student must contribute to the final written and oral report
- Discuss your ideas about topics with the instructor **before** starting.

Slide 16

Assignment Registration and Report

Registration: Tuesday 9 February 2016, to maguire@kth.se
with the subject: "IK2555 topic"

Group members, leader, and topic selected

Slide 17

Written report

The length of the final report should be ~10 pages (roughly 5,000 words) for each student; it should **not** be longer than 12 pages for each student - papers which are longer than 12 pages per student will be graded as "F".

Paper style should be that of a conference paper (but need **not** be formatted in two columns).

Papers should **not** focus on physical and link layer issues as this is **not** a course in radio communication systems, but rather the papers should look at things which have an impact on the architecture or upon which the architecture has an effect.

If there are multiple students in a project group, the report may be in the form of a collections of papers, with each paper suitable for submission to a conference or journal.

Contribution by each member of the group - must be clear (in the case where the report is a collection of papers - the role of each member of the group can be explain in the overall introduction to the papers.

The report should clearly describe: (1) what you have done; (2) who did what; if you have done some implementation and measurements you should describe the methods and tools used, along with the test or implementation results, and your analysis.

Slide 18

Submitting the report

Final Report: written report due Sunday 13 March 2016 at 23:59 + oral presentations to be individually scheduled during week 12 (21-24 March 2016) at a location to be announced.

Send email with URL link for a **PDF** or **PostScript** file and your Zotero RDF file or BiBTeX file to maguire@kth.se

Late assignments will **not** be accepted (i.e., there is no guarantee that they will be graded before the end of the term)

Slide 19

Literature

The course will mainly be based on the book: Yi-Bing Lin and Ai-Chun Pang, *Wireless and Mobile All-IP Networks*, John Wiley & Sons; 2005, ISBN: 0-471-74922-2 and the earlier *Wireless and Mobile Network Architectures*, by Yi-Bing Lin and Imrich Chlamtac, John Wiley & Sons, 2001, ISBN 0-471-39492-0.

We will not focus on Mobile IP in the lectures (since an introduction was given in the internetworking course), see also: [Perkins1998] and [Solomon1998] .

We will refer to other books, articles, and RFCs as necessary - see notes and web.

Maguire IK2555, Spring 2016 Slide 19

[Perkins1998] Charles E. Perkins, Mobile IP: Design Principles and Practices, Addison-Wesley, 1998, ISBN 0-201-63469-4.

[Solomon1998] James D. Solomon, Mobile IP: the Internet Unplugged, Prentice Hall, 1998, ISBN 0-13-856246-6.

Slide 20

Observe proper academic ethics and properly cite your sources!

You will be searching & reading the literature in conjunction with your projects. Please make sure that you properly reference your sources in your report - keep in mind the **KTH Ethics policies.**

In particular:

- If you use someone else's words - they must be clearly indicated as a **quotation** (***with a proper citation***).
- Note also that individual figures have their own copyrights, so if you are going to use a figure/picture/… from some other source, you need to **both cite this source & <u>have the copyright owner's permission to use it</u>**.

Maguire IK2555, Spring 2016 Slide 20

Slide 21

Ethics, Rights, and Responsibilities

At KTH there is a policy of zero tolerance for **cheating, plagiarism, etc.** - for details see relevant KTH policies, such as *http://www.kth.se/student/studentratt*

Before starting to work on your paper read the page about **plagiarism** at *http://www.kth.se/en/student/studentliv/studentratt/fusk-och-plagiering-1.323885*

See also the book: Jude Carroll and Carl-Mikael Zetterling, *Guiding students away from plagiarism*, KTH Learning Lab, 2009, ISBN 978-91-7415-403-0 http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-83704

Maguire IK2555, Spring 2016 Slide 21

Jude Carroll and Carl-Mikael Zetterling, *Guiding students away from plagiarism*, KTH Learning Lab, 2009, ISBN 978-91-7415-403-0

Slide 22

Lecture Plan

1. Introduction
   - Course arrangements/overview/context
   - Personal Communication Systems (PCS): handoff, mobility, paging
2. Network Signaling; CDPD
3. GSM, GPRS, SMS, International Roaming, Operation/Administration/Maintenance
4. Number portability, VoIP, Prepaid
5. WAP, Heterogeneous PCS, 3G, Beyond 3G, 4G
6. Wireless Local Loop (WLL), Enterprise Networks
7. Wireless Local Area Networks (WLANs)
8. Bluetooth: Piconets, Scatternets
9. Ultrawideband (UWB)
10. Broadband Wireless Access (BWA)
11. Sensor Networks
12. Miscellaneous topics

Slide 23

Context of the course

Personal communication systems have been both increasing their number of users and increasing the variety of personal communication systems. Some of these system (such as GSM) have had *growth* rates of millions of new customers each month! Wireless communication systems have been very successful in many places around the world.

- In many countries the 3G license fees were many thousands of euros per potential customer.
- Data is becoming a dominant source of the traffic, rather than conversational voice
- Fourth generation (4G) cellular systems in operation
- Researchers are exploring "Beyond 4G" systems (some talk about 5G systems).

Last of IPv4 addresses were allocated to the regional registrars in 2011⇒ major push for transition to IPv6 - see 'World IPv6 Day', June 8, 2011: *http://isoc.org/wp/worldipv6day/* and *http://www.internetsociety.org/ipv6/results*

See also: RFC 6459: IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS) [Korhonen2012]

Maguire IK2555, Spring 2016 Slide 23

[Korhonen2012] J. Korhonen, J. Soininen, B. Patil, T. Savolainen, G. Bajko, and K. Iisakkila, "IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS)", Internet Request for Comments, vol. RFC 6459 (Informational), January 2012, Available at *http://www.rfc-editor.org/rfc/rfc6459.txt*

Slide 24

Context of the module

Communication systems have been both increasing their number of users and increasing the variety of communication systems. Additionally, increasingly communicating entities are ***not*** people, but rather things.

	number	
Micro controllers	6×10^9 **per year**	[Sakamura2002] *http://doi.ieeecomputersociety.org/10.1109/MM.2002.10015*
People	7×10^9	*http://en.wikipedia.org/wiki/World_population*
Mobile subscribers	$> 5 \times 10^9$	as of end of 2010 *http://www.itu.int/ITU-D/ict/newslog/Mobile+Broadband+Subscriptions+To+Hit+One+Billion+In+2011.aspx*
PCs	$> 1 \times 10^9$	as of June 23, 2008 *http://www.gartner.com/it/page.jsp?id=703807*
Automobiles	59.87×10^6	*http://oica.net/category/production-statistics/*
Commercial vehicles	20×10^6	*http://oica.net/category/production-statistics/*

Ericsson's CEO (Hans Vestberg) predicts the future (~2020) Internet will have 50 billion interconnected devices, while Intel predicts 15 billion connected devices by 2015 [Higginbotham2010].

Increasing numbers of these devices are connected via a wireless link.

Maguire IK2555, Spring 2016 Slide 24

[Sakamura2002] Ken Sakamura, "Farewell message," IEEE Micro, vol. 22, no. 6, pp. 2, 72, Nov.-Dec. 2002, DOI:10.1109/MM.2002.10015

[Higginbotham2010] Stacey Higginbotham, Ericsson CEO Predicts 50 Billion Internet Connected Devices by 2020, GigaOM , Apr. 14, 2010, 10:08am PT, *http://gigaom.com/2010/04/14/ericsson-sees-the-internet-of-things-by-2020/*

Slide 25

Personal Communication Systems (PCS)

The goals of PCS are to provide a mobile user with voice, data, and multimedia at any place, at any time, and in any format.

Thus the system has to *either* provide **universal coverage** or it has to include **interworking with other communication systems**. Thus far, attempts at providing universal coverage by a **globally standard system** have failed (for various technical, historic, economic, and political reasons).

The market has often been fragmented based on: **wide area coverage** (especially for business users), **enterprise** (focused on in-building and on campus), and **homes** (often equated with "personal" or "free-time usage"). However, this market separation is increasingly **converging** rather than further diverging.

Slide 26

PCS interconnectivity and rate of change

Traditionally, various PCS systems were connected to the Public Switched Telephony System (PSTN) and driven by *telephony standards* (and changed at the *rate* of change of telephony standards).

Today, these systems are increasingly connected to the internet and driven by the internet standards & change at internet speeds.

Slide 27

High Tier and Low Tier Cellular, and Cordless

Generally the PCS market has been divided into these three classes:

System	High Tier Cellular	Low Tier Cellular	Cordless
Cell size	large (0.25-38km)	medium (10-100m)	small (10-20m)
User speed	high (≤ 260 km/h)	medium (≤100km/h)	low (≤50km/h)
Handset complexity	high	low	low
Handset power consumption	high (100-800mW)	low (5-20mW)	low (5-10mW)
Speech coding rate	low (8-13kbps)	high (32kbps)	high (32kbps)
Delay or latency	high (≤600ms)	low (≤10 ms)	low (≤10ms)
Costs	high	medium	low (often flat rate)
Examples	GSM, D-AMPS, PDC, cdmaOne, UMTS, …*	CT2, DECT, PHS, PACS	

* 4G systems have attempted to greatly reduce latency

Slide 28

Cellular Telephony

Different means of defining channels:

- **F**requency **D**ivision **M**ultiple **A**ccess (FDMA)
  Advanced Mobile Phone Service (AMPS)
- **T**ime **D**ivision **M**ultiple **A**ccess (TDMA)
  D-AMPS, Global System for Mobile Communications (GSM)
- **C**ode **D**ivision **M**ultiple **A**ccess (CDMA)
  IS-95 (developed by Qualcomm), cdma2000, W-CDMA, …
- **S**pace **D**ivision **M**ultiplexing (SDM)
  Multiple Input Multiple Output (MIMO)

Maguire IK2555, Spring 2016 Slide 28

Slide 29

Low Tier Cellular and Cordless Telephony

Cordless **T**elephony, second generation (CT2)

- 40 FDMA channels, within each 100kHz frequency channel the base station⇒user (**downlink**) and user⇒base station (**uplink**) channels are separated with time division duplexing (TDD) (in every 2 ms long **frame** there is 64bits of downlink user data followed by 64 bits of uplink user data).
- Does **not** support handoffs, primarily supports out-going calls (incoming calls are hard as there is no defined mobility database).

Digital **E**nhanced **C**ordless **T**elephony (DECT)

- formerly: **D**igital **E**uropean **C**ordless **T**elephony
- utilizes a **picocellular** design using TDMA with 24 time slots (generally: 12 voice slots for downlink and 12 voice slot for uplink, i.e., TDD) per frequency channel and 12 frequency channels, automatic dynamic channel allocation based on signal strength measurements
- a call can move from one time slot in one frequency channel to another time slot in another channel - supporting seamless handoffs.

Slide 30

Low Tier Cellular and Cordless Telephony (continued)

Personal **H**andy Phone **S**ystem (PHS)

a TDMA TDD system also supporting dynamic channel allocation - it has been used in Japan for a public low tier cellular system.

Personal **A**ccess **C**ommunications **S**ystem (PACS)

a TDMA system supporting both TDD and frequency division duplex (FDD); it utilized **m**obile-**c**ontrolled **h**and**o**ff (MCHO). It supports both circuit switched and packet switched access protocols.

Slide 31

Mobile Data

RAM Mobile Data (now Velocita Wireless, based on the Swedish Mobitex system)

Was backbone behind Xpress Mail with **BlackBerry**, Interactive Messaging PLUS, and Wireless Internet PLUS,

Mobitex had greater national coverage 90% of Sweden's land and 99.5% of the population, than even the analog 450MHz cellular system, because the Swedish military used it.

Formerly at http://www.mobitex.telia.com/taeckning.htm

Both public Mobitex systems (such as that formerly operated by Telia, now by Multicom Security AB) and private systems (such as the one at Arlanda Airport).

Slide 32

Mobile Data (continued)

Advanced **R**adio **D**ata **I**nformation **S**ystem (ARDIS) {developed for IBM's customer engineers offered indoor coverage} (now Dish Network formerly *TerreStar*, formerly Motient -- was building a 4th Generation all IP network featuring seamless integration between satellite and terrestrial systems [TerreStar2007])

Motient (founded in 1988 as American Mobile Radio Corporation) spun off its XM Satellite Radio unit in 2001; the later has now merged with Sirius Satellite Radio

Maguire IK2555, Spring 2016 Slide 32

[TerreStar2007] TerreStar Corporation, Company Profile, Sept 6, 2007, http://www.terrestar.com/company/index.html

Slide 33

Mobile Data (continued)

Cellular Digital Packet Data (CDPD)

Developed to provide data as an overlay on analog cellular systems; based on Mobile IP.

Slide 34

Paging

Within local paging areas or via satellite.

The key to paging device's high performance is that they **sleep** *most of the time*.

North America utilizes two way paging systems (i.e., the paging system can both send and receive traffic).

Due to the lack of allocation for a return channel two way paging languished in Europe.

Slide 35

Specialized Mobile Radio (SMR)

Taxis dispatching, fleet dispatching, …

The basis for Nextel - using a handset built for them by Motorola to operate over the wide variety of SMR channels which Nextel bought (this is a case where the radio design came *after* the frequencies were "assembled"). Note that Nextel is now Sprint (*http://www.sprint.com*).

The former Nextel® Walkie-Talkie service was replaced by Sprint® Direct Connect® - a push to talk service.

Slide 36

Satellite

Especially **L**ow **E**arth **O**rbit **Satellite** (LEO)

- numerous attempt to field systems - one problem is that most of the time the satellites are over regions {primarily oceans} with few possible customers. Each satellite is only in range for ~10 minutes or so ⇒ frequent handoffs.
- 500 - 2000 km orbit
- US DoD Enhanced Mobile Satellite Service (EMSS) {successor to Iridium, features secure phones and US government secure voice gateway} - https://www.disa.mil/Network-Services/Satellite/EMSS

Slide 37

Satellite (continued)

The footprint (i.e., coverage area of a satellite transponder) for **M**id-**e**arth **o**rbit (MEO) and **Geo**stationary (GEO) satellite - generally cover too large an area and does so with very long delays (due to the distance of these satellites from the earth). However, they are widely used for both their wide coverage area (for example, for paging) and for *one way services* (often broadcast or spot coverage).

For more about LEO systems see [Kalantari and Rylander2006].

Maguire IK2555, Spring 2016 Slide 37

[Kalantari and Rylander2006] Leila Kalantari and Eva Rylander, "Communication Solutions for Forestry Machines", Masters Thesis, KTH Royal Institute of Technology, Communication Systems, Stockholm, Sweden, February 2006. http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-92258

Slide 38

Wideband systems

Wideband Code Division Multiple Access (W-CDMA)

With data rates in rural areas 1.44 kbps, in cities 3840160 kbps, and indoors up to 2 Mbps

http://www.umtsworld.com/technology/overview.htm

Also known as (AKA) UMTS terrestrial radio access (UTRA)

cdma2000

Also known as IS-2000; an evolution of cdmaOne/IS-95 to 3rd generation services: CDMA2000 1X, an average of 144 kbps packet data; 1XEV-DO up to 2 Mbits/sec.; 1XEV-DV even higher peak rates - simultaneous voice and high speed data + improved QoS

TD-SCDMA - one of the several competing Chinese 3G standards

Formerly at: http://www.td-forum.org/en/

Slide 39

Wideband systems standardization

3rd Generation Partnership Project (3GPP)

http://www.3gpp.org/
based on evolved GSM core networks and the radio access technologies

3rd Generation Partnership Project 2 (3GPP2)

http://www.3gpp2.org/

- ITU's "IMT-2000" initiative:
  - high speed, broadband, and Internet Protocol (IP)-based mobile systems
  - "featuring network-to-network interconnection, feature/service transparency, global roaming and seamless services independent of location."
- includes cdma2000 enhancements

Slide 40

Local Metropolitan Area Networks (LMDS)

Point-to-point or Point-to-multipoint (generally wide band) links

- some operators have more than 700 MHz worth of bandwidth available (in aggregate) in a given market (geographic) area
- line-of-sight coverage over distances up to 3-5 kilometers
- data rates from tens of Mbps to >1 Gbps
  Ericsson's 2.5 Gbps system in the 70-80 GHz band (*http://www.ericsson.com/lt/news/1383946*)

Frequency bands between 24 to 31 GHz (licensed spectrum)

UK: 28 GHz band and 10 GHz band

Rest of Europe: 26 GHz band

US: 24 GHz used by Teligent and 39 GHz band licensed by Winstar (now part of IDT)

at least one experimental license in the US in 41.5 GHz to 43.5 GHz

Biggest problem is price of the necessary high frequency components

Slide 41

Point-to-Point Optical links

Free-Space Optics (FSO)

- using laser light sources it is possible to achieve very high speeds (typically OC-3 (155 Mbps), OC-12 (622 Mbps), or 1.25 Gbps; but some systems operate at 2 Gbps and 10 GBps) for point-to-point links
- uses Terahertz (THz) spectrum range
- short ranges - typically below 2 km

See also: *http://www.freespaceoptics.org/*

Slide 42

Wireless Local Area Networks (WLANs)

Generally using one of the following schemes:

- **F**requency **H**opping **S**pread **S**pectrum (FH-SS)
- **D**irect **S**equence **S**pread **S**pectrum (DS-SS)
- **O**rthogonal **F**requency **D**ivision **M**ultiplexing (OFDM)
- IR links

Most of the radios have either used the **I**nstrumentation, **S**cientific, and **M**edical (ISM) bands, **N**ational **I**nformation **I**nfrastructure (NII) bands, or the HiperLAN band.

Data rates have ranged from hundreds of kbps to 54 Mbps, now >>100 Mbps.

Slide 43

WLAN (continued)

See IEEE 802.11 (in its many variants) - some of these standards are available at (those published more than one year ago are free): *http://standards.ieee.org/getieee802/*

Slide 44

Short range radio

low speed wireless links (door locks, wireless sensors, RF ID tags, …)

Personal Area Networks (PANs) - these have generally be relatively low data rate systems, such as Bluetooth (~1-2 Mbps in aggregate).

Near Field Communication (NFC) - typical range of centimeters (when operating in the 13.56 MHz frequency range) see http://www.nfc-forum.org/

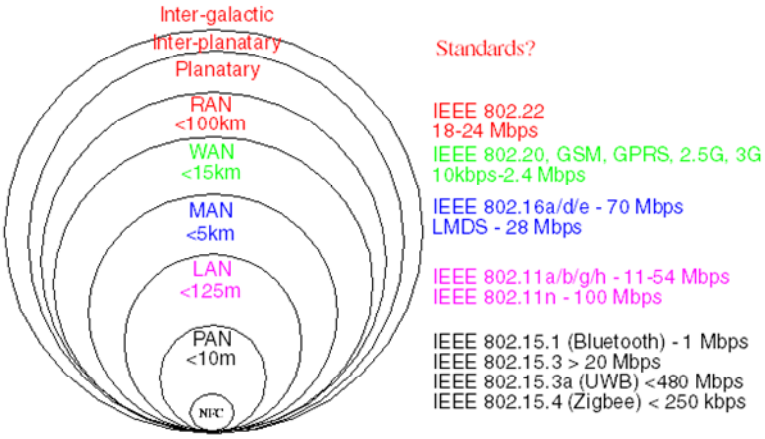
Ultrawideband

- US FCC gave regulatory approval 14 Feb. 2002
- Intel demo'd transmitter and receiver at 100 Mbps
- Intel expects to be able to get 500 Mbps at a few meters dropping to 10 Mbps at 10m.

Slide 45

From PANs to RANs and beyond

Communication range of users - range from ~10^{-3} m to >>10^{6} m:



From Personal Area Networks (PANs) to Regional Area Networks (RANs) inspired by slide 5 of [Cordeiro2006]

⇒ This implies that solutions will involve **heterogeneous** networks.

Maguire IK2555, Spring 2016 Slide 45

[Cordeiro2006] Carlos Cordeiro, Report on IEEE 802.22, IEEE J-SAC, and IEEE DySPAN 2007 tutorials, TCCN meeting at Globecom on November 27, 2006 *http://www.eecs.ucf.edu/tccn/meetings/Report_06.ppt*

Slide 46

Are interplanetary and intergalactic networks relevant to us?

1. Some customers: NASA, European Space Agency, … ; but also scientists/astronomers who want to look back in time
2. Future space explorers & tourists?
3. ⇒ delay tolerant networks (DTNs) - since the one-way delays are very high - perhaps this offers insights into other DTNs

   content distribution by the physical movement of "carriers" near to someone who want the content or someone who will pass it on (and on and on and on!)
4. The communication is going to have to remain uncorrupted for a very long period of time (see for example *Digital Preservation Europe* (DPE) project 2006-2009)
   - Note the Austrian goal of preserving digital documents for 200 years; this is much harder than just copying the bits from one media to another, but also includes issues such as the validity period for a digital signature (for authentication) or encryption (for privacy) and how these properties can be extended for much longer periods of time
   - Where is this storage/archiving/ … going to be ?
   - Who is going to transfer the "documents" to and from the storage repository (repositories)?

Maguire IK2555, Spring 2016 Slide 46

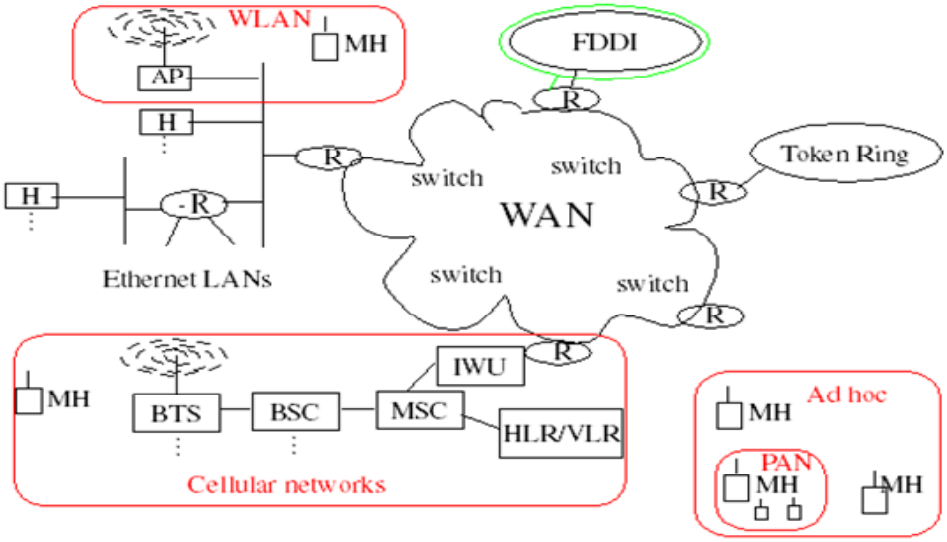
Slide 47

How can we deal with all of these different networks?

- Force a **single winner**
  - Use a single **network architecture**
    ⇒ Everything will be ATM/UMTS/…
  - Use a single **network protocol**: IP, IPX, IBM's Systems Network Architecture (SNA), …
- Live with **multiple winners**
  - **Specialized networks**: a circuit switched PSTN, a cable TV network, …
  - **Niche networks**: local point-to-point links (such as IrDA, Bluetooth, …), RFID, NFC, …

Slide 48

Internet Architecture

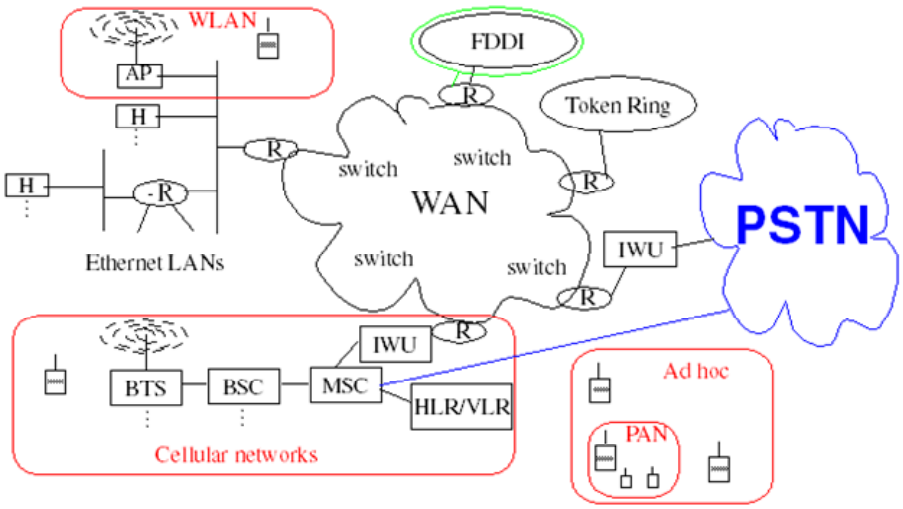


Multiple network technologies - *internetworked* together

Facilitates ***disaggregation*** - since **functionality** can be located anywhere on the internet

Slide 49

More complete Architecture



We will focus on the parts marked in red in the above figure, i.e., Cellular, WLAN, and PAN (and Ad hoc) networks.

Slide 50

Internetworking

Internetworking is

- based on the interconnection (concatenation) of multiple networks
- accommodates multiple underlying hardware technologies by providing a way to interconnect **heterogeneous** networks and makes them inter-operate - via a common network layer.

Many personal communication systems are interconnected to the Public Switched Telephony System (PSTN) - thus there must generally be an *adaptation* to fixed rate (generally 64 kbps) voice coding. Increasingly these systems are also interconnected to the Internet, hence **packet based services** are becoming an increasingly important part of such systems.

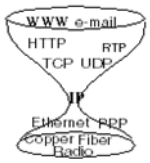
These interconnections have technical, political, and regulatory effects.

⇒ Rise of truly international operators - one logical network independent of geography (independent of the fact that it is built of multiple cooperating & competing networks)

Slide 51

Basic concepts

open-architecture networking	• Each distinct network stands on its own makes its own technology choices, etc ⇒ no changes within each of these networks in order to internet • Based on best-effort delivery of datagrams • Gateways interconnect the networks • No global control
The End2End Argument	Some basic design principle for the Internet: •Specific application-level functions should not be built into the lower levels • Functions implemented in the network should be simple and general. •Most functions are implemented (as software) at the edge ⇒ complexity of the core network is reduced ⇒ increases the chances that new applications can be easily added. See also [Clark2001], [Clark2002]
Hourglass (Stuttgart wineglass) Model	• Anything over IP • IP over anything Note the broad (and open) top - enabling lots and lots of application



Maguire IK2555, Spring 2016 Slide 51

[Clark2001] David D. Clark and Marjory S. Blumenthal, “Rethinking the Design of the Internet: The end to end arguments vs. the brave new world”, In ACM Transactions on Internet Technology, Vol 1, No 1, August 2001, pp 70-109.

[Clark2002] D. Clark, J. Wroclawski, K. Sollins, and R. Braden, “Tussle in Cyberspace: Defining Tomorrow’s Internet”, Proceedings of Sigcomm 2002.

Slide 52

How does this avoid the "B-ISDN debacle"?

Internetworking is completely different from the B-ISDN:

- Rather than a single cell based circuit switched network - the focus is on interconnecting networks via a common network layer protocol
- Lots of products and lots of vendors selling these products
  - note: there is significant competition with a very fast development cycle
- The technology is "good enough" vs. trying to be an improved version of ISDN (think of examples from Clayton Christianson's *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail* [Christensen1997])
- Exploits the very rapid advances at the edge of the network - which *the users pay for*!
- Encourages both cooperation by different network operators and competition between different network operators!

⇒ network connectivity as a commodity using commodity products to deliver a wide range of services

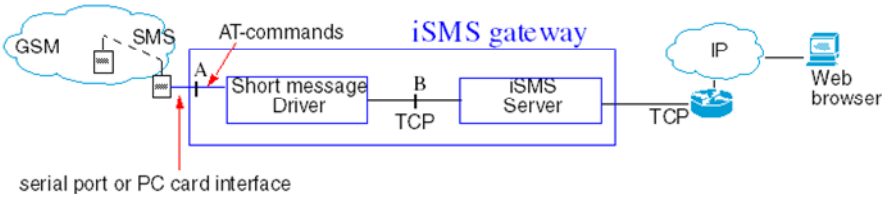
Maguire IK2555, Spring 2016 Slide 52

[Christensen1997] Clayton M. Christensen, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*, Harvard Business School Press, Boston, MA, USA, 1997, ISBN 0-87584-585-1.

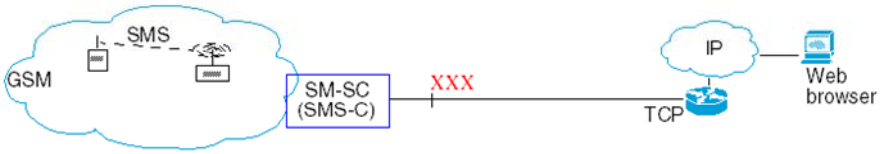
Slide 53

Examples of internetworking

Chapter 1 of Yi-Bing Lin and Ai-Chun Pang's ***Wireless and Mobile All-IP Networks*** shows several examples of internetworking, such as:



A gateway using two mobile stations (Figure adapted from figure 1.10 on page 10 of [Lin2005])



A gateway using the cellular systems short messaging service center (SM-SC);(Figure adapted from figure 1.2 on page 3 of [Lin2005]
Note: some details are saved for later - see [Fältström2008]

Maguire IK2555, Spring 2016 Slide 53

[Fältström2008] Patrik Fältström, "Future of the Internet", Lecture slides, 27 March 2008, http://stupid.domain.name/stuff/future-internet.pdf

[Lin2005] Yi-Bing Lin and Ai-Chun Pang, Wireless and Mobile All-IP Networks, John Wiley & Sons; 2005, ISBN: 0-471-74922-2

Slide 54

Trend: Increasing Data Rates

Wide area

GSM: 14.4kbps per channel

High Speed Circuit Switched Data (HSCSD): combining multiple GSM channels to achieve a higher aggregate rate for a single user

GPRS: hundreds of kbps - by using the GSM time slots in a **packet** oriented manner

3G: Mbps to 10s of Mbps

IMT-Advanced (4G), LTE, LTE-A: 100 Mbps to 1Gbps

Local area

Wireless LAN standard from IEEE

- 802.11 Wireless LAN - 1 Mbps .. 1 Gbps
- 802.15 Wireless Personal Area Network (WPAN) ~1Mbps (and higher)
- 802.16 Metropolitan Area Networks - Fixed Broadband Wireless (10 .. 66 GHz) 10s to 100s of Mbps/channel and lower frequencies with more limited bandwidth)
- 802.20 (aka Mobile-Fi) Mobile Broadband Wireless Access (MBWA) -- IP based

Slide 55

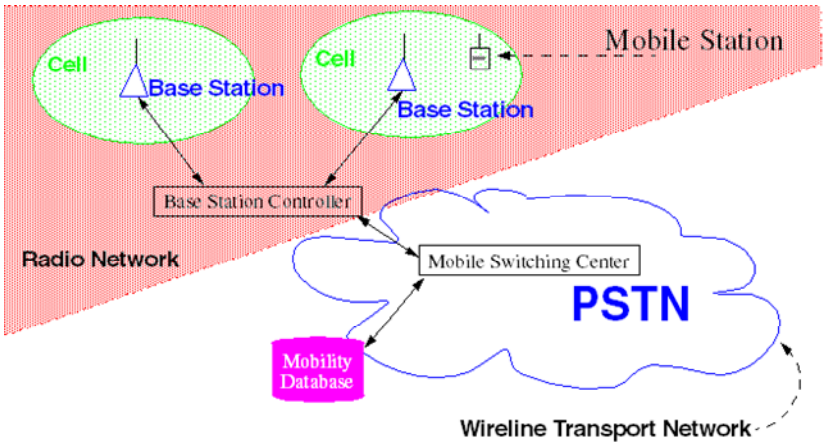
Trends: Shifting from traditional telecommunications to data communications

This is often referred to as the shift to "All-IP" networking. This embodies:

- A shift from *circuit-switched* to **packet-switched**
  such as: from Intelligent network (IN) to IP Multimedia Core Network Subsystem (IMS)
- Introduction of new technologies:
  - Voice over IP (VoIP)
  - Number portability
  - Context-awareness (including location-awareness) in services
- From services being what the telecommunication operator offers *to you* to what **anyone** offers to you. This is accompanied by a major shift in:
  - How services are created
  - Where services are provisioned
  - Where data is stored and who stores it
- Desperate efforts to retain control, market share, high profits, access to dial numbers, and call contents, … - the genie is reluctant to go back into the bottle!

Slide 56

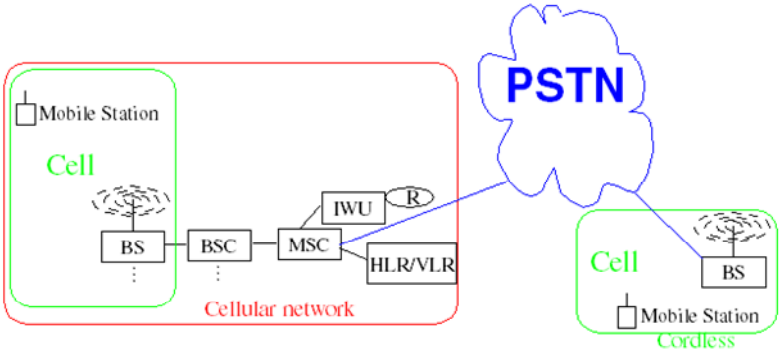
Basic Personal Communication System (PCS) network architecture



Basic PCS network architecture

Slide 57

Example of a PCS Architecture

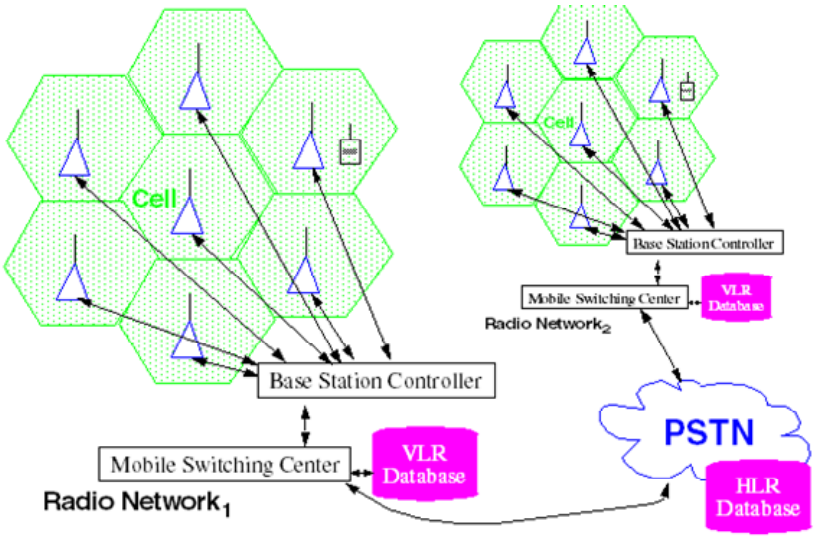


Cellular and Cordless networks

B(T)S = Base (Transceiver) Station, **BSC** = Base Station Controller, **MSC** = Mobile Switching Center, Home Location Register (**HLR**)/Visitor Location Register (**VLR**) provides a Mobility Database, and the PSTN provides the wireline (**backhaul**) transport network.

Slide 58

PCS network architecture supporting Mobility



Basic PCS network architecture

Slide 59

Mobility Management

If mobile only **originates** traffic, then you do **not** have to know where the mobile is *to send traffic to it* - but rather you only have to decide if you will give it service.

If a mobile is to **receive** traffic (without having originated traffic), then someone must know where to send this traffic. This someone can be:

- a server **in** the network (where the user is)
- a server **attached** to the network (where the user is)
- a server **attached to another network** (different from where the user is right now - sometimes this is their "*home*" network)

We will examine mobility management with respect to the **static** decision of where to send traffic, the **dynamics** of maintaining communication despite change in access points (**Handoff**), and the use of **paging** (both in conjunction with mobility management, as an alternative architecture, and as a component of other architectures). See also: §1.4 of [Lin2001] or Chapter 2 of [Lin2005].

Maguire IK2555, Spring 2016 Slide 59

[Lin2005] Yi-Bing Lin and Ai-Chun Pang, Wireless and Mobile All-IP Networks, John Wiley & Sons; 2005, ISBN: 0-471-74922-2
[Lin2001]Yi-Bing Lin and Imrich Chlamtac, *Wireless and Mobile Network Architectures*, John Wiley & Sons, 2001, ISBN 0-471-39492-0

Slide 60

Mobility Management Protocols

Include:

- Mobile IP
- EIA/TIA Interim Standard 41 (IS-41 or ANSI-41)
- Global System for Mobile Communications (GSM) Mobile Application Part (MAP)

Maha Bouaziz and Abderrezak Rachedi, ‘A survey on mobility management protocols in Wireless Sensor Networks based on 6LoWPAN technology’, *Computer Communications*, Oct. 2014 [Online]. DOI: 10.1016/j.comcom.2014.10.004

Slide 61

Macro- vs. Micro-mobility

Macro-mobility == Inter-domain mobility
(a domain is {as usual} a single administrative entity)
Micro-mobility == Intra-domain mobility

In micro-mobility entities **outside** of the current domain *can not* (and need not) see any changes when the mobile moves **within** the domain, while with macro-mobility others can see when a mobile moves, even within a domain.

Slide 62

Getting Service

Once a mobile's identity is know, the policy question is: Should this mobile get service?

The policy question and its answer may involve:

- roaming agreements (generally reciprocal agreements),
- current traffic loads,
- anticipated traffic loads,
- mobile user's priority/class/… ,
- … .

The question of authentication, authorization, and accounting (AAA) for mobile users are topics of a thesis: Juan Caballero Bayerri and Daniel Malmkvist, *Experimental Study of a Network Access Server for a public WLAN access network*, M.S. Thesis, KTH/IMIT, Jan. 2002.

See also IEEE 802.1x Port Based Network Access Control *http://www.ieee802.org/1/pages/802.1x.html*

Slide 63

Locating the user

- we can **track** the user continuously, or
- we can start looking for the user where we last saw them and then expand our **search**, or
- we can **guess** where the user might be
  - based on their patterns of movement (past behavior)
  - their personal schedule (if they give us access to this information), …
- the **user tells us** where they are
  - based on a **schedule** the user can tell us where they are (e.g., every one minute tell the system where you are now) or
  - the **user can listen** for something (for example a page) which causes them to check in or to report their location
- the user can tell their agent/intermediary where they are (i.e., we do **not** actually know where they are), thus we contact them **through their agent** whom we know how to contact.

  Note that this is the method used in SIP - where the user registers their current location(s) and when an incoming call occurs their proxy process this call; the proxy can decide to redirect this call, forward it to one or more of the user's possible locations, …

Slide 64

Handoff Management: Detection & Assignment

Who initiates handoff?

How do you detect that you should handoff?

handover (Europe) ≡ **handoff** (North America)

Slide 65

Handoff/Handover/Automatic Link Transfer

Handoff is the process that occurs when a mobile is "handed over" from one access point to another, i.e., the access point which the mobile is using changes. This is generally one of several types:

Type of handoff	Description
soft	the mobile can communicate with both the **old** and the **new** AP*
hard	the mobile can only communicate with one AP or the other
seamless	If neither the user nor running applications notice the handoff (i.e., there is *no effect on content of data streams* coming arriving to or departing from the mobile)§ (includes both smooth and fast handoffs)
glitchless	in this case the delays due to the handoff are hidden/eliminated from the data stream
smooth	buffering of traffic to the mobile when it is in the process of changing from one AP to another is buffered and then delivered to the new AP†
fast	only a short interruption time between disconnection at the old AP and connection to the new AP
vertical	when the new cell is larger than the current cell (i.e., microcell to macro cell)
horizontal	when the new cell is similar to the current cell (i.e., microcell to micro cell)

Slide 66

Footnotes to previous table

* Generally I will refer to such devices as access points (APs), except when their being a Base Station is particularly important.

§ For seamless and glitchless handoffs see for example, work by Ramón Cáceres and V.N. Padmanabhan [Cáceres and Padmanabhan1998]

† See C. Perkins and K-Y. Wang's scheme for buffering with Mobile IP, requires per mobile buffering associated with the (former) access points [Perkins and Wang1999] .

Maguire IK2555, Spring 2016 Slide 66

[Cáceres and Padmanabhan1998] R. Cáceres and V. N. Padmanabhan, "Fast and Scalable Wireless Handoffs in Support of Mobile Internet Audio", ACM/Kluwer Journal on Mobile Networks and Applications, Vol. 3, No. 4, December 1998.

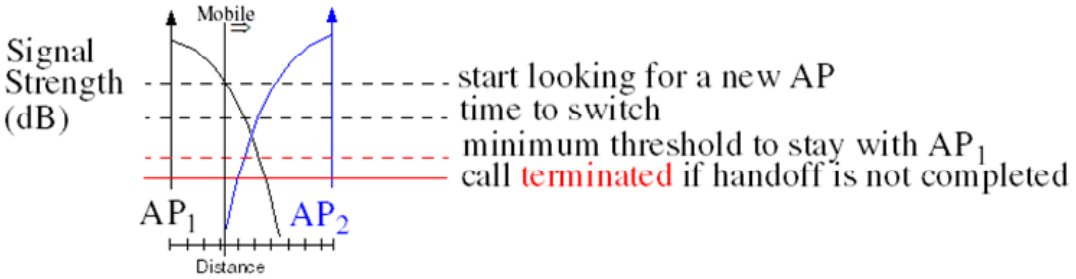
[Perkins and Wang1999] C. Perkins and K-Y. Wang. "Optimized smooth handoffs in Mobile IP", Proceedings of IEEE Symposium on Computers and Communications (ISCC'99), Egypt, July 1999, pp. 340-346

Slide 67

Handoff Criteria

- Signal quality - due to its effect on the ability to deliver data via the link
- Data quality - the effect of errors on the delivered data traffic

With respect to signal quality we can exploit knowledge of general radio signal properties or we can exploit specific situation knowledge (based on our earlier experience or the experience which other mobiles have reported and which we have learned about). A simplified view with respect to signal strength (reality is *much* more complex):



Slide 68

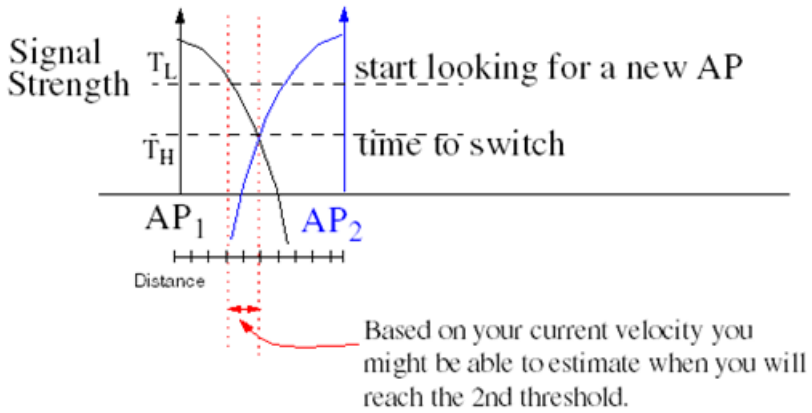
Handoff Goals

- **minimal impact** on traffic - making a handoff at the “right” time
- **tolerance/adaption** for congestion and capacity - the new and old cells may have different levels of *utilization*, *available* bandwidth, … - handoff has to deal with this
- **efficiency** - the handoff should result in *improved* efficiency (in terms of traffic, energy consumption, reduced interference, …) ⇒ the handoff process *itself* should try to minimize the resources it consumes
- improve **availability** - handoff should result in using an AP providing: better bandwidth, lower cost, lower delay, low delay variance, …
- the mobile should be able to use the maximum set of APs (which may involve changing spreading code, modulation, coding, … or changing to a different radio module) in order to achieve a better **system optima**, rather than be restricted to a local single system optima

Slide 69

When to make the decision?

By starting to look for a new AP **before** you need it, there is time to make a decision - **while** you still have connectivity:



T_L - Threshold for **Looking** around, T_H - threshold for **Handoff**

Slide 70

Reality is more complex

Mobile Station (MS) and the Base Station (BS) experience a channel which varies - due to user movement, movement of other users, reflections, diffractions, … ⇒

- Rapid-fading
  - Rayleigh-distributed envelope of the signal strength (often called Multipath fading)
  - If there is also a light-of-sight component, then the distribution is Rician
- Slower fading
  - Shadow fading - a lognormal distribution

Slide 71

Measurements of the channel

Three common measurements of the channel:

- **W**ord **E**rror **I**ndicator (WEI) - based on the receiver being able to decode the received signal correctly
- **R**eceived **S**ignal **S**trength **I**ndication (RSSI) - a measure of the received signal strength (in units of dB) (For some experimental indoor measurements of received IEEE 802.11b RSSI values as a function of distance and angle see the Master 's Thesis by Haruumi Shiode [Shiode2008].)
- **Q**uality **I**ndicator (QI) - related to the signal to interference & noise ratio (S/I) (in units of dB)

As the channel is varying in time and making the measurements takes time - various techniques are used to filter the RSSI and QI measurements:

- window averaging - simply average the last w measurements
- leaky-bucket integration - a simple one-pole low-pass filter

Various schemes exist to try to combat channel problems:

- **diversity techniques** (frequency hopping, multiple receivers, multiple correlators with variable delay lines, multiple antennas, …)
- **signal processing techniques** (bit interleaving, convolutional coding, equalizers, …)

For further information about these techniques - see: [Goodman1997], [Lee1995], [Rappaport2002], [Wesel1998], and [Pahlavan2002].

Maguire IK2555, Spring 2016 Slide 71

[Shiode2008] Haruumi Shiode, In-building Location Sensing Based on WLAN Signal Strength: Realizing a Presence User Agent, Master's thesis, KTH, School of Information and Communication Technology (ICT), Communication Systems, TRITA-ICT-COS COS/CCS 2008-04, ISSN 1653-6347, 2008, 72 pages, http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-91868

[Goodman1997] David J. Goodman, *Wireless Personal Communication Systems*, Addison-Wesley, 1997, ISBN 0-201-63470-8. See the summary in section 2.5 (and in each chapter) for more pointers to additional reading. Carefully note that some of the things which the authors have covered in ch. 2 are *simply their proposals and not (yet) implemented*; but their ideas are worth understanding.

Great coverage about the link layer details and general architectures of AMPS, IS-41, North American TDMA and CDMA, and GSM. Only very brief coverage of CT2, DECT, PHS, and PACS. This is an extremely well written book.

[Lee1995] William C.Y. Lee, *Mobile Cellular Telecommunications: Analog and Digital Systems*, Second edition, 1995, ISBN 0-07-038089-9

[Rappaport2002]Theodore S. Rappaport, *Wireless Communications: Principles and Practice*, 2nd edition, Prentice-Hall, 2002, 736 pages, ISBN: 0-13-042232-0.

[Wesel1998] Ellen Kayata Wesel, *Wireless Multimedia Communications: Networking Video, Voice, and Data*, Addison-Wesley, 1998, ISBN 0-201-63394-9.

[Pahlavan2002] K. Pahlavan and P. Krishnamurthy, *Principles of Wireless Networks*, Prentice Hall PTR, 2002, ISBN 0-13-093003-2. All the usual radio topics

Slide 72

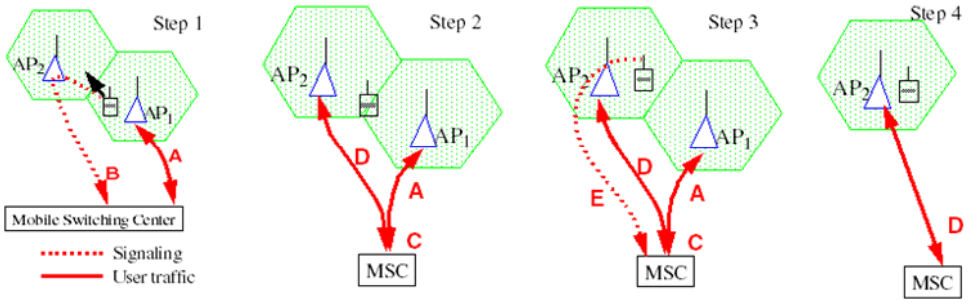
Who makes the handoff decision?

- **N**etwork **c**ontrolled **h**andoff (NCHO) - the network makes the decision: used in CT-2 Plus and AMPS
- **M**obile **a**ssisted **h**andoff (MAHO) - the mobile provides data which the network uses to make the decision: used in GSM and IS-95 CDMA
- **M**obile **c**ontrolled **h**andoff (MCHO) - the mobile decides for itself: used in DECT, PACS, Mobile IP
  - **forward handoff** - mobile initiates handoff and sends the request to the ***new*** AP
  - **backward handoff** - mobile initiates handoff and sends the request to the ***old*** AP

Slide 73

Inter-BS Handoff (aka inter-cell handoff)

When both cells are connected to the same Mobile Switching Center (MSC) the mobile node (MN) can signal that it is going to change cells and identifies the new cell, then MSC sets up the correct resources in the new cell, and can now deliver traffic to the mobile's new cell. In telephony systems this often involves setting up a "bridge" to copy traffic to both the new and the old channels.



Steps in handoff within the control of one MSC (not showing the BSC)

Slide 74

Inter-BS Handoff (continued)

1. Mobile (MN) is using AP_1, all traffic is going via a channel (A) between MSC (via BSC) and AP_1; MN signals via AP_2, its intention for upcoming handoff (via B)
2. MSC creates a bridge (C) and traffic is now sent via both channels (A) and (D)
3. MN signals (via E) that it is ready to use channel D
4. MSC eliminates bridge C and frees channel A, the MN now uses only channel D.

Slide 75

What happens if there are insufficient resources at new AP?

Nonprioritized scheme (handoffs are treated the same as new calls)

If handover is blocked, then keep using the existing channel until either:

- call is over or
- link fails (or forced termination)

Slide 76

To reduce forced termination and improve "call completion" statistics

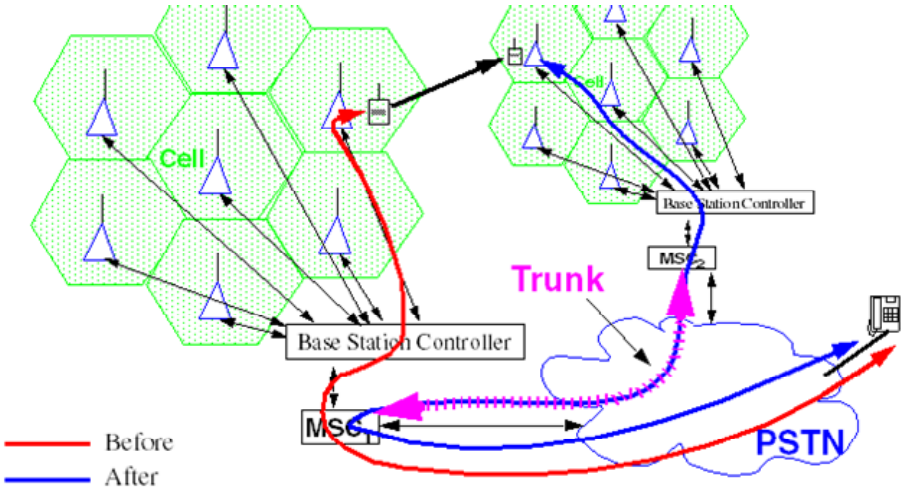
- **Reserved channel scheme** - keep some resources available for handovers (i.e., they under commit)
- **Queuing priority scheme** - exploit cell over lap (called a "handover area" if it exists) to enqueue mobiles waiting for handover
- **Subrating scheme** - downgrade an existing call in the new cell and split the resources with the call being handed over (⇒ the call being handed over is also downgraded). Downgrading often involves changing from a full-rate to a half-rate CODEC.

Some operators base their decision on what to do on **how valuable the handoff customer is** vs. current customers being served in the new cell, i.e., high value customers can cause existing calls of other customers to be terminated.

Slide 77

Inter-system Handoff (aka inter-MSC handoff)

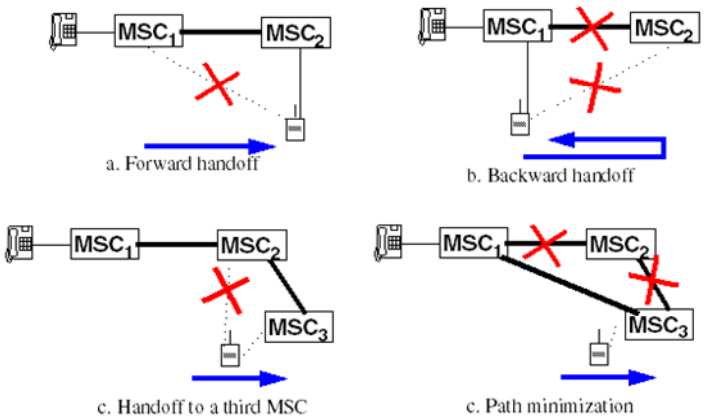
When the two cells are connected to different MSCs the situation is more complex.



Handoffs between two MSCs

Slide 78

What happens if the mobile moves again?



Handoffs between multiple MSCs

Note that the call always goes via the so-called **Anchor MSC** (MSC1), because the phone attached to the PSTN knows nothing about mobility and the originating exchange thinks the call is still in existence (i.e., there was no termination and set up of a new call to or from the fixed phone).

Note: Without path minimization the chain of trunks between MSCs could continue to grow *as long as the call lasts* **and** the *mobile keeps moving* to new MSCs. With voice calls, the call duration is generally rather limited, but with data it could continue for a very long time ⇒ we will need to use another model for dealing with data (addressed later in the lectures).

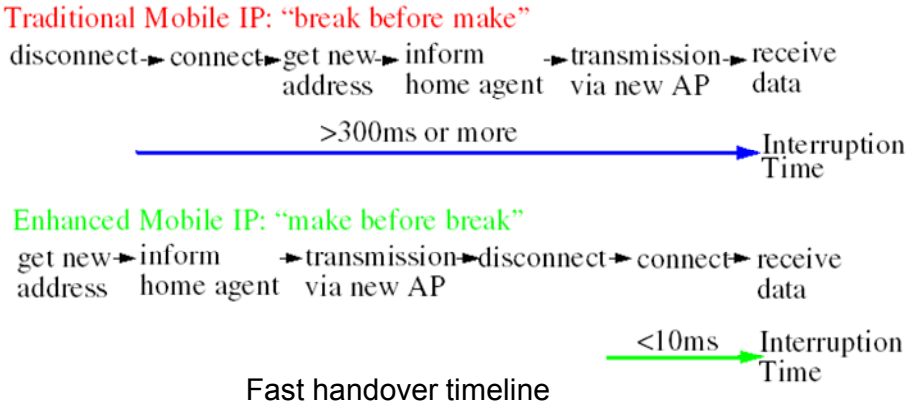
Slide 79

Fast Mobile IPv4 handoff via Simultaneous Bindings

The **Simultaneous Binding** option in Mobile IPv4 allows the Mobile Node to establish a binding for the new AP with its home agent (*before* a handoff). The Home Agent now duplicates all packets destined for the MN for the time of the handoff and relays all data to **both** the old and the new APs. Thus the MN performs the handoff by simply reconfiguring its interface -- which it can generally do within a very short interruption time, i.e. often <10 ms. When the MN physically connects to the new network, it will find that the packets destined for it are already arriving there!

Slide 80

Fast handover timeline



Fast handover timeline

Figure adapted from http://www.ccrle.nec.de/Figure3.gif which is part of http://www.ccrle.nec.de/Handoff.htm - web page is no longer available, but the Internet Archive has a copy of the text at: http://web.archive.org/web/20021121192850/http://www.ccrle.nec.de/Handoff.html

Slide 81

Roaming

Roaming occurs when a user of one PCS is using the services of **another** PCS.

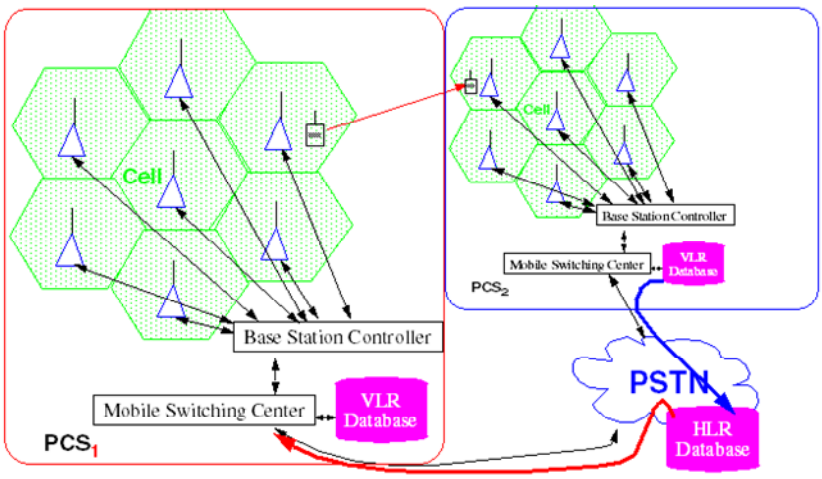
- Roaming is generally based on "roaming agreements" between the operators of the involved PCS systems; i.e., the user's home operator agrees to pay the other PCS operator(s) for carrying this **mobile user's** traffic.

  Note: the agreement is generally about the **user** (often referred to as a "subscriber") - not a specific **device**, thus a user is free to change devices to access the new PCS network. This of course may complicate the authentication, authorization, and accounting (AAA) processes.
- As a side of effect of authenticating and authorizing the user to access the new PCS, the home PCS's mobility database is updated to reflect the fact that this user in located in the other PCS - thus traffic arriving for this user can (should?) be forwarded/redirected to the user's current location. Clearly this raises both:
  - **policy decisions**: Should *this* specific traffic be redirected? Should *all* traffic be redirected? Should this location be reported? …) and
  - **accounting questions** (*Who pays* for carrying the redirected traffic? Is there a *base charge for roaming*? …)

Maguire IK2555, Spring 2016 Slide 81

Slide 82

User roaming



Mobile roams from PCS_1 to PCS_2 (Neither is the home PCS)

When the mobile moves to PCS_2 the local VLR is updated, the HLR is updated, and the former VLR is also updated.

Slide 83

Roaming Management

Two parts:

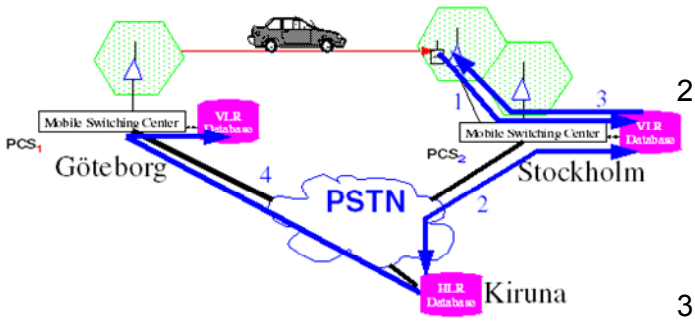
- **registration** (location update) - process whereby MS informs the system of its **current** location
- **location tracking** - the process of locating the user to deliver a call

EIA/TIA Interim Standard 41 (IS-41 or ANSI-41) and Global System for Mobile Communications (GSM) Mobile Application Part (MAP) both define a two-level strategy - which uses two tiers of databases:

- **home location register** (HLR) - exists at the user's *home system*
- **visitor location register** (VLR) - a temporary record at the *visited system*

Roaming example

Gunvor (from Kiruna) has been visiting in Göteborg, now arrives in Stockholm



Mobile roams from PCS_1 to PCS_2

1. When the user (and her MS) arrives in Stockholm, her MS has to register with the VLR for PCS_2.
2. PCS_2's VLR informs the user's HLR in Kiruna of the user's current location (i.e. the HLR should point to the VLR in PCS_2). The HLR sends the user's profile to PCS_2's VLR.
3. PCS_2's VLR informs the mobile (MS) that is has successfully registered.
4. HLR informs PCS_1's VLR to remove their entry for the user.

Slide 85

Of course it could not be this simple!

Discussion left out all the interactions within the PCS (i.e., details of channel assignment & signaling within the cells, between the base station & base station controller, and between the BSC & the MSC) -- it also left out all the interactions with the PSTN†. To reduce the cost of registration one can utilize a **forwarding pointer scheme**:

- **Move operation** (registration) - when moving from VLR to VLR, enter a forwarding pointer into the previous VLR, rather than notifying the HLR
- **Find operation** (call delivery) - when a call comes to the home system, walk the chain and then update the HLR.

†Section 2.3 "Roaming Management under SS7" [Lin2001] describes some of the details of the later.

Maguire IK2555, Spring 2016 Slide 85

[Lin2001]Yi-Bing Lin and Imrich Chlamtac, *Wireless and Mobile Network Architectures*, John Wiley & Sons, 2001, ISBN 0-471-39492-0

Slide 86

Reducing the cost of deregistration

- **implicit deregistration** - only delete records from the VLR when you need the space
- **periodic reregistration** - MS periodically registers with the VLR; if no reregistration within a timeout period, then their record is deleted

Slide 87

Call delivery

An originating Switching Point (**SSP**) (or alternatively a Signal Transfer Point (**STP**)) maintains a cache of the **Mobile Identification Number** (MIN) and the current VLR) - it examines this cache - there are three outcomes:

1. Cache entry not found ⇒ do the lookup of MIN's HLR via **Global Title Translation** (GTT)
2. Cache entry exists **and** is current ⇒ do a lookup in the VLR
3. Cache entry exists, but is **obsolete** ⇒ do the lookup of MIN's HLR via **Global Title Translation** (GTT)

Determining that the cache entry is (*probably*) current is generally done with heuristics.

Slide 88

CT2

Section 2.4 of [Lin2001] describes how CT2 as a call **originating only** system, hence it did **not** need location services, but that it could be *extended* via:

1. sending a page to a user
2. then the user calls into a meeting point - which patches the two (or more) callers together

[Lin2001]Yi-Bing Lin and Imrich Chlamtac, *Wireless and Mobile Network Architectures*, John Wiley & Sons, 2001, ISBN 0-471-39492-0

Slide 89

Back to: Who makes the handoff decision?

Slide 90

Network controlled handoff (NCHO)

Network controlled handoff (NCHO) - the network makes the decision

- BS monitors the signal strength and quality from the MS
- Network uses multiple (current and surrounding) BSs to supervise the quality of all current connections by making measurements of RSSI
- MSC makes the decision when and where to effect the handoff
- Heavy network signaling traffic and limited radio resources at BSs prevent frequent measurements of neighboring links ⇒ long handoff times.

Handoff times: up to 10 seconds or more

Slide 91

Mobile assisted handoff (MAHO)

Mobile assisted handoff (MAHO) - the mobile provides data which the network uses to make the decision; essentially it is a variant of network controlled handoff - but uses the mobile to help reduce the handoff times.

For example, in GSM the MS transmits measurements twice a second ⇒ GSM handoff execution time ~ 1 second

Note in both NCHO and MAHO - if the network can **not** tell the mobile about the new channel/time slot/… to use *before* the link quality has decayed too far, then the call may be terminated.

Slide 92

Mobile controlled handoff (MCHO)

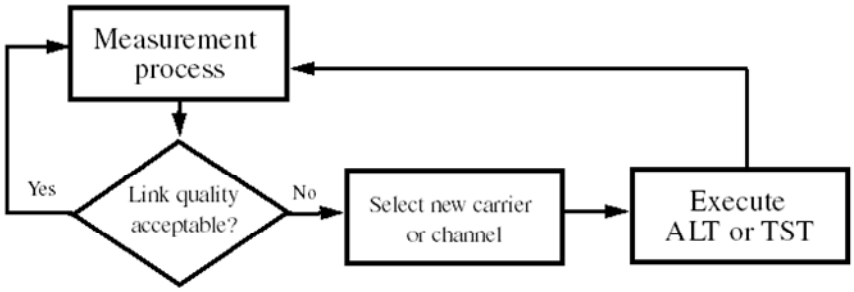
The mobile decides for itself (by monitoring signal strength and quality from the current and candidate base stations), when it finds a “better” candidate it initiates a handoff. In MCHO most of the work is done by the mobile (as it knows who it can hear, how well it can hear them, and can even consider its battery level, etc.)

Two common handoffs:

- **automatic link transfer** (ALT) - transfer between two base stations
- **time slot transfer** (TST) - transfer between channels of a single BS

Slide 93

MCHO (continued)



Different systems use different approaches to the measurement process. For example, some DECT implementations can measures the RSSI of all channels simultaneously. In other systems, the measurement of other channels is done when the device is itself not transmitting or receiving.

Handoff times: DECT 100-500 ms, PACS 20-50 ms.

Slide 94

Handover Failures

- **No available channel/link resources** in the new **BS**
- **Insufficient resources** as determined by the **network** (for example, no available bridge, no suitable channel card {for example, no support for the voice CODEC in use or for the available radio link coding})
- It **takes too long** for the network to set up the new link
- **Target link fails** during handoff

Slide 95

Channel Assignment

Goals:

- achieve high spectrum utilization
- maintain a given service quality
- use a simple algorithm
- require a minimum number of database lookups

Unfortunately it is hard to do all of these at once!

If there is no available channel, then

- new calls are **blocked**
- existing calls that cannot be handed over ⇒ **forced terminations**

Slide 96

Channel Assignment Process

- **Fixed Channel Assignment** (FCA)
- **Dynamic Channel Assignment** (DCA)
- **Quasi-static autonomous frequency assignment** (QSAFA)
- …

Lots of schemes have been introduced to reduce the number of forced terminations, at the cost of increased blocking or decreased efficiency:

- **Nonprioritized scheme** (NPS) - handoff call treated the same as a new call
- **Reserved Channel scheme** (RCS)- reserves some resources for handoffs
- **Queuing Priority scheme** (QPS) - exploit the over lap (handoff area)
- **Subrating scheme** (SRS) - switching CODECs of one or more calls to free resources

Slide 97

Handoff Management: Radio Link Transfer

We will not cover the details of the radio link, but examine some key ideas.

hard handoff: mobile connects only to a single base station at a time

soft handoff: mobile receives/transmits from/to multiple BSs simultaneously

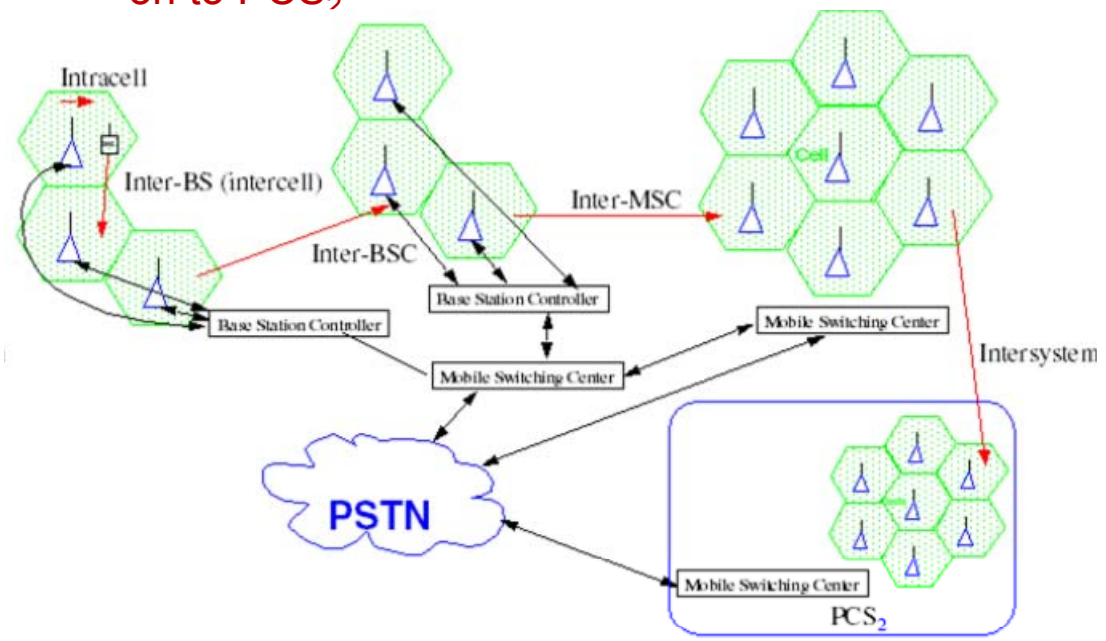
In soft handoff, the network and perhaps the mobile have to figure out how to combine the information from the multiple BSs (in the up and down links respectively).

Link transfers:

1. Intracell
2. Intercell or inter-BS
3. Inter-BSC
4. Intersystem or inter-MSC
5. Intersystem between two PCS networks

Slide 98

Handoffs, mobile moves within PCS_1 and then on to PCS_2



Handoff frequency

With a cellular voice call of 1 minute duration†:

Type of handoff	Probability
inter-BS	0.5
inter-BSC	0.1
inter-MSC	0.05

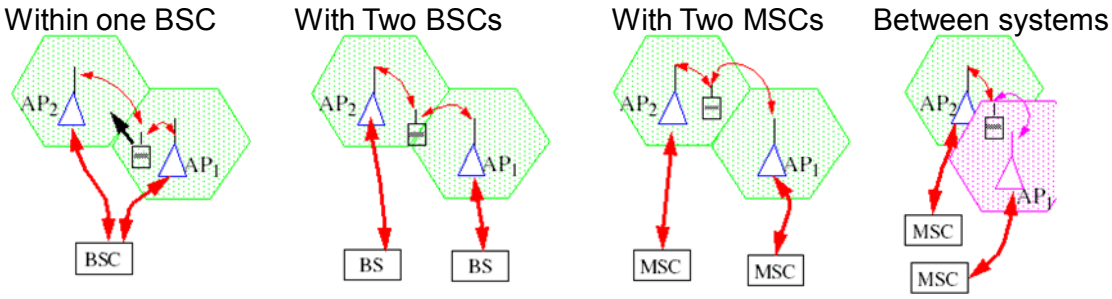
† Note that the probabilities shown are not exact, but rather simply representative of the general order of magnitude one might expect in a macro cellular network.

How do you expect that these might change:

- in a urban LTE network?
- for Internet of Things (OT) devices?

Slide 100

Soft handoff in multiple forms



Some CDMA systems use very precise link level timing to enable the signals from multiple BSs to arrive additively at the mobile - thus leading to a physically stronger signal.

Soft handoffs between systems generally will require that the mobile be able to receive multiple signals - which will use different codes, frequencies, … .

Slide 101

Paging

Originally a one-way personal altering/messaging system to replace voice paging over the public address system.

A transmitter sends a stream of addresses and messages. **Pagers** listen for their address (also called a **cap code**).

Telephone pagers were introduced later by Al Gross (also inventor of the walkie-talkie).

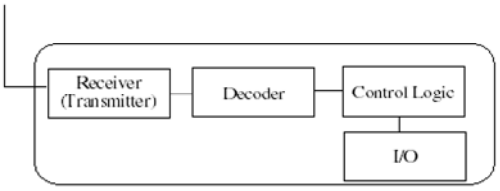
Cap Code	beep (one of ~4 tones) when the pager's address is received by the pager
Tone voice	1970's, allows the sender to record and send a short voice message
Digital display	early 1980's, a callback number (or code) entered by the sender, which appears on the pager's display
Alphanumeric	late 1980's, display a text message

Maguire IK2555, Spring 2016 Slide 101

[Neergaard1942] Charles F. Neergaard, 'What Can the Hospital Do About Noise?', *The Journal of the Acoustical Society of America*, vol. 13, no. 3, p. 217, 1942. DOI: 10.1121/1.1916167

Slide 102

Pager



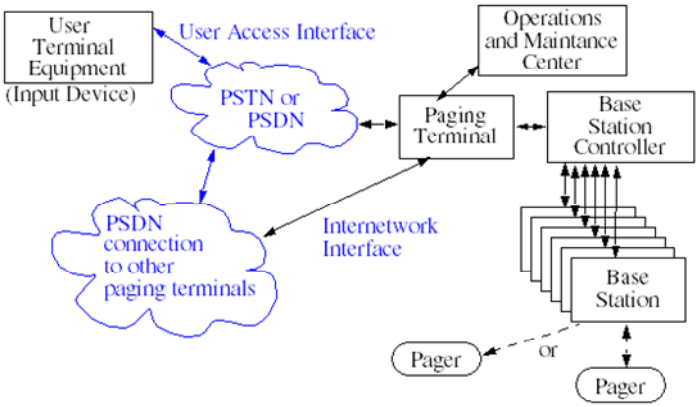
I/O can be a display, a beeper, keypad, audio input/output, vibrator, … .

Control logic supports:

- duplicate message detection
- message locking (to keep message from being overwritten)
- message freezing (to keep message on the screen)
- altering modes (beep, vibrate, …)
- power management

Slide 103

Paging Architecture



A paging terminal has a database of customers, cap code, pager number, types of messages, …; converts voice message to text (for alphanumeric pagers); store in mailbox for pager; forward to other paging terminals; send to relevant Base Station Controller(s)

Slide 104

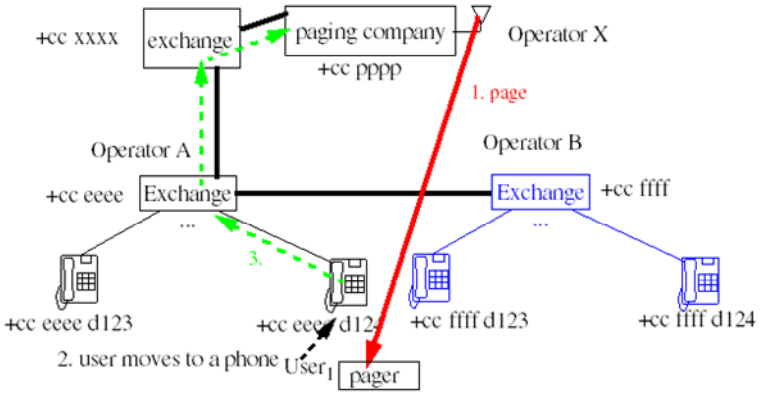
Paging Service area

Service areas: site, local area, region, national, international

If the user has temporarily left the paging service area or if the signal could not reach them, then they would miss the page. Motorola's ReFLEX technology, a two-way paging system, keeps transmitting a paging message until the user's pager sends a confirmation that it has been received.

Slide 105

Introduction of paging systems

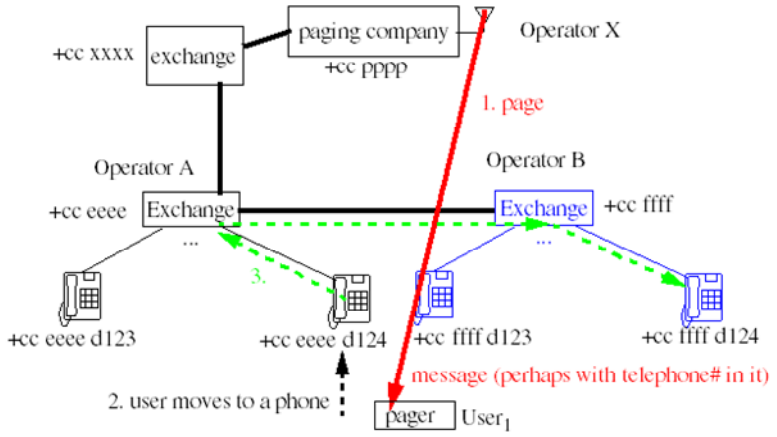


Upon a page (1), user moves to nearest phone (2), calls paging company (3), company operator tells the user what telephone number to call - perhaps they (also) convey a short message.

⇒ A mobile user can be contacted and told by the operator at the paging company to connect to the fixed telephone network. [i.e., make a temporary connection to the (voice) network.]

Slide 106

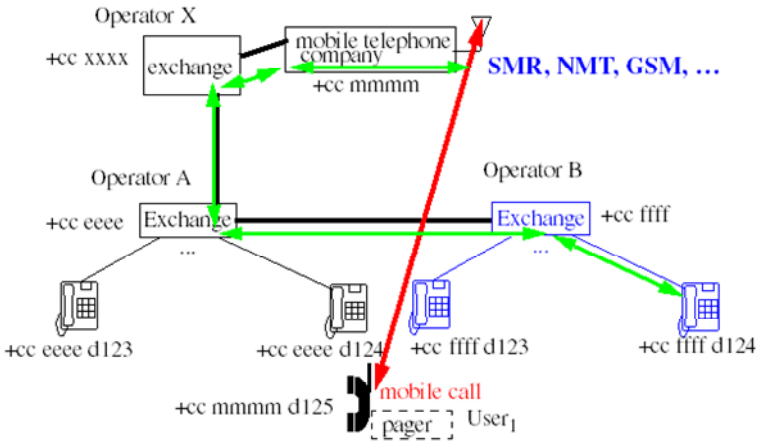
Alphanumeric paging systems



Upon a page (1), user moves to nearest phone (2), calls a number based on the content of the (page) message (3); or perhaps they just consume the short message they received. The mobile user can be contacted and told by a message to call a given number on the fixed telephone network.

Slide 107

Mobile telephone systems



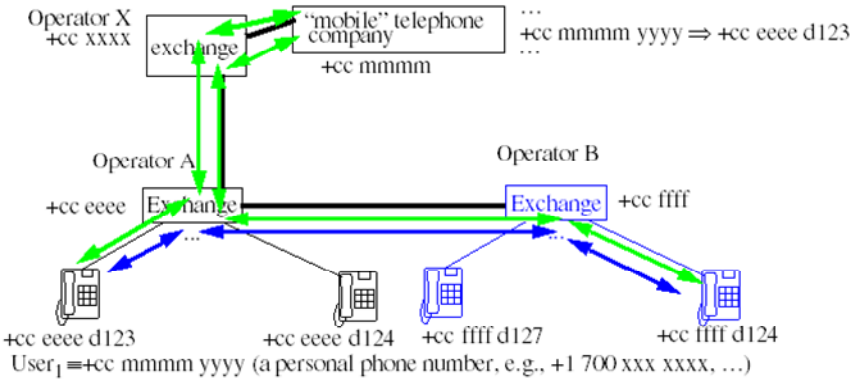
The mobile user is directly reached by the call through the mobile telephone network.

SMR (Specialized Mobile Radio) is a non-cellular radio system.

NMT (Nordic Mobile Telephone), GSM (Groupe System Mobile), and PCS are cellular radio systems.

Slide 108

Mobile but not necessarily wireless



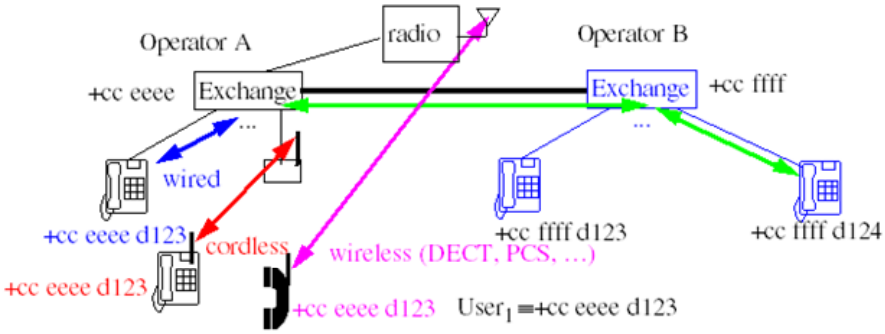
The mobile user is indirectly reached through the fixed telephone network.

- The connection can be via the "mobile" company (hiding the actual location of the user) or
- via redirect directly to the current location of the user.

Thus the mobile operator turns +cc mmmm yyyy into +cc eeee d123 [dynamic address translation].

Slide 109

Local mobility via wireless (or redirects)



The mobile user is reached by **local redirection** (which may utilize local wireless links) of the call coming from the fixed telephone network.

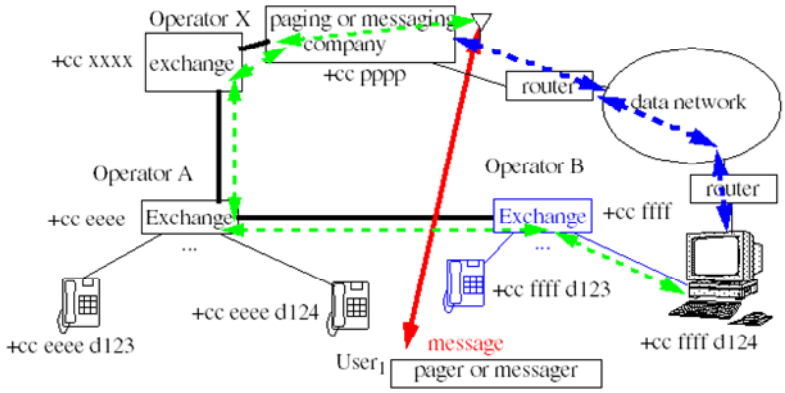
- The local exchange is playing the role of the "mobile" company (hiding the actual location of the user).
- There are multiple instruments (terminals) and user is currently associated with a list of them
- Could involve a non-local redirect

To the external world the user looks like they are always at +cc eeee d123, which the local PBX maps into a specific extension (at the time of the call).

Maguire IK2555, Spring 2016 Slide 109

Slide 110

Two-way paging and messaging systems



Two-way paging or messaging allows exchange of digital messages.

- Traditionally the paging or messaging system was a separate data network, but GSM's **Short Message Service** provides alphanumeric messaging via the GSM infrastructure.
- The messaging device can also be a computer (PDA/notebook/…)
- Connection between the two users can be via the PSTN or a (public) data network

Slide 111

Paging Interworking

Telocator Alphanumeric Protocol (TAP), also known as IXO or PET, defines a 7-bit alphanumeric text message to be sent to paging receivers, with a block size of 256 characters and an effective message length of 1,000 characters

Telocator Data Protocol (TDP) suite: a functional superset of TAP; adopted 1995; **Telocator Message Entry** (TME) protocol - the input protocol for TDP: two-way paging, priority paging, deferred paging, periodic paging, message forwarding, and message deletion.

Telocator Network Paging Protocol (TNPP) used to create networks of paging terminals from different manufacturers (overcomes the proprietary protocols to/from paging terminals - such as Glenayre Link Module, Spectrum Data Link Handler)

Slide 112

Paging - link level

- Older format: British Post Office Code Standards Advisory Group (**POCSAG**)
  - single operator, single frequency
  - maximum of 2 million users
  - two separate tones and then a burst of data; 576 bit preamble then multiple 544 bit batches
- ETSI's European Radio Message System (**ERMES**)
  - 35 bit radio identity code
  - effective transmission rate of 3750 bps
  - each hour is partitions into 60 cycles, each cycle partitioned into 5 subsequences, each subsequence is partitioned into 16 batches
- Philips Telecom's Advanced Paging Operations Code (**APOC**)
- Motorola's **FLEX** (further described on next slide)
  - signals have only a single tone preceding the data burst.
  - Interestingly FLEX paging data is **not** encrypted.
- Motorola's **Generation II FLEX**
  - FLEX G1.9 protocol supports full roaming, time of day updates accurate to one hundredth of a second, and dynamic group messaging
  - Motorola's FLEXsuite™ applications, such as over the air programming, encryption, and compression utilize FLEX G1.9.
  - 1600 and 3200 symbols-per-second

Slide 113

Motorola's FLEX™ protocol†

Supports up to five billion individual addresses and up to 600,000 numeric pagers per channel. Channel can run at 1600 to 6400 bps as needed by operator.

- FLEXion™ an advanced voice paging protocol
- Motorola's Portable Answering Machine - can receive and store voice messages,
- digitally compresses voice messages
- system is aware of the general location of the recipient's messaging unit, therefore sends the message from the closest paging transmitter
- ReFLEX™ a two-way messaging protocol
- Motorola's Advanced Messaging Group has demonstrated the use of a ReFLEX two-way pager to access Hyper Text Markup Language (HTML) content.

160 FLEX technology-based systems in commercial operation in 36 countries, representing 93% of the world's paging subscriber base.

† As of February 2002, Motorola transferred all their paging subscriber device product lines to Multitone Electronics plc, Basingstoke, UK *http://www.multitone.com/* -- this page was based on information from: http://www.motorola.com/MIMS/MSPG/FLEX/protocol/solution.html - unfortunately, this URL is no longer valid

Slide 114

Sleeping for power savings

A major aspect of the link level paging protocols is to enable the pager to spend most of its time **sleeping**.

It does this by **knowing when to listen for its address** and in the case of Motorola if *as the address is being received* more bits fail to match than the error correction could possibly correct, then it goes to sleep immediately.

Some paging receivers do not even wake up the decoder unless the page may be for this device (thus the different parts of the pager may be awakened separately).

Slide 115

Mobile Telephone Systems Timeline(the first two generations: analog + digital)

Year	Standard	System	Technology	Primary markets
1979	NTT's MCS-L1	First commercial mobile phone network	Analogue	Tokyo
1979	AMPS†	Advanced Mobile Phone System	Analogue	US (pre-commercial)
1981	NMT 450	Nordic Mobile Telephone	Analogue	Europe, Middle East
1983	AMPS	Advanced Mobile Phone System	Analogue	North and South America
1985	TACS	Total Access Communication System	Analogue	Europe and China
1986	NMT 900	Nordic Mobile Telephony	Analogue	Europe, Middle East
1991	GSM	Global System for Mobile communication	Digital	World-wide
1992	GSM 1800	Global System For Mobile Communication	Digital	Europe
1993	CdmaOne(IS95)	Code division multiple access	Digital	North America, Korea (1995)
1994	D-AMPS(IS94)	Time Division Multiple Access	Digital	North and South America
1994	PDC	Personal Digital Cellular	Digital	Japan
1995	PCS 1900	Personal Communication Services	Digital	North America
2001	WCDMA	Wideband CDMA	Digital	Europe, Japan
2001	EDGE	Enhanced Datarate for Global Evolution	Digital	Europe
2002	CDMA2000	CDMA2000 1xEV-DO.	Digital	Korea

† April 3, 1973 Motorola vice presidents Marty Cooper and John Mitchell made the first public demonstration of a call from a handheld wireless phone.

For more details see *http://www.umtsworld.com/umts/history.htm*

Maguire IK2555, Spring 2016 Slide 115

Slide 116

Increasing 4G/LTE and LTE-A deployments

TeliaSonera announced on 13 January 2010 their selection of 4G vendors using the 3GPP standard Long Term Evolution (LTE) and System Architecture Evolution (SAE) core technology.

They built out a network in Sweden and Norway using equipment from Ericsson for the core network and equipment from Ericsson and Nokia Siemens Networks for the radio network.

As of the end of 2009, LTE service was introduced in Stockholm and Oslo.

- Samsung provided USB modem dongles.
- Data rates up to 100 Mbps.

LTE-Advanced (LTE-A) proposed as a standard to ITU-T in 2009, deployments began in 2013. Downlink data rates up to 1 Gbps.

Slide 117

References and Further Reading

Course book

Yi-Bing Lin and Ai-Chun Pang, Wireless and Mobile All-IP Networks, John Wiley & Sons; 2005, ISBN: 0-471-74922-2

Yi-Bing Lin and Imrich Chlamtac, *Wireless and Mobile Network Architectures*, John Wiley & Sons, 2001, ISBN 0-471-39492-0. Even more so that the earlier book [2], carefully note that some of the things which the authors have covered are *their own proposals*; but their ideas are worth understanding.

Further details concerning physical and link layer wireless communication

David J. Goodman, *Wireless Personal Communication Systems*, Addison-Wesley, 1997, ISBN 0-201-63470-8. See the summary in section 2.5 (and in each chapter) for more pointers to additional reading. Carefully note that some of the things which the authors have covered in chapter 2 are *simply their proposals and not (yet) implemented*; but their ideas are worth understanding.

Great coverage about the link layer details and general architectures of AMPS, IS-41, North American TDMA and CDMA, and GSM. Only very brief coverage of CT2, DECT, PHS, and PACS. This is an extremely well written book.

Slide 118

CDPD

Mark S. Taylor, William Waung, and Moshen Banan, *Internetwork Mobility: The CDPD Approach*, Prentice-Hall, Upper Saddle River, NJ, 1997. ISBN 0-13-209693-5
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.99.1957&rep=rep1&type=pdf

LEO

Christopher Redding, "Overview of LEO Overview of LEO Satellite Systems", Institute for Telecommunication Sciences National Telecommunications and Information Administration, Boulder, Colorado - lecture slides from 1999 International Symposium on Advanced Radio Technologies: formerly at http://www.its.bldrdoc.gov/meetings/art/art99/slides99/red/red_s.pdf

Slide 119

Fixed Broadband wireless

IEEE 802.16c™, “Air Interface for Fixed Broadband Wireless Access Systems - Detailed System Profiles for 10-66 GHz”, https://standards.ieee.org/findstds/standard/802.16c-2002.html

User profiles

Sudeep Kumar Palat, “Replication of User Mobility Profiles for Location Management in Mobile Networks”, Norwegian University of Science and Technology, Dr. Ing. Dissertation, Dept. of Telematics, 12 Jan. 1998.

Slide 120

Mobile IP

C. Perkins, 'IP Mobility Support', Internet Request for Comments, vol. RFC 2002 (Proposed Standard), October 1996, Available at http://www.rfc-editor.org/rfc/rfc2002.txt .

C. Perkins, 'IP Mobility Support for IPv4', Internet Request for Comments, vol. RFC 3344 (Proposed Standard), August 2002, Available at http://www.rfc-editor.org/rfc/rfc3344.txt .

D. Johnson, C. Perkins, and J. Arkko, 'Mobility Support in IPv6', Internet Request for Comments, vol. RFC 3775 (Proposed Standard), June 2004, Available at http://www.rfc-editor.org/rfc/rfc3775.txt .

Slide 121

Fast handoff

K. E. Malki, 'Low-Latency Handoffs in Mobile IPv4', Internet Request for Comments, vol. RFC 4881 (Experimental), June 2007, Available at *http://www.rfc-editor.org/rfc/rfc4881.txt* .

Micromobility: Cellular IP, HAWAII, Hierarchical Mobile IP

formerly at http://comet.ctr.columbia.edu/micromobility/

E. Fogelstroem, A. Jonsson, and C. Perkins, 'Mobile IPv4 Regional Registration', *Internet Request for Comments*, vol. RFC 4857 (Experimental), Jun. 2007 [Online]. Available: http://www.rfc-editor.org/rfc/rfc4857.txt

Slide 122

Comparison of IP Mobility protocols

P. Reinbold and O. Bonaventure. A Comparison of IP Mobility Protocol. Technical Report Infonet-TR-2001-07, University of Namur, Infonet Group, June 2001. http://citeseerx.ist.psu.edu/doi=10.1.1.21.2328&rep=rep1&type=pdf - formerly available as http://www.infonet.fundp.ac.be/doc/tr/Infonet-TR-2001-07.html

TeleMIP

Subir Das, et al. TeleMIP: Telecommunication-Enhanced Mobile IP Architecture for Fast Intradomain Mobility. *IEEE Personal Communications*, 7(4):50-58, August 2000.

Intersystem Handoff

Janise McNair, Ian F. Akyildiz, and Michael D. Bender, "An Inter-System Handoff Technique for the IMT-2000 System", Proceedings of IEEE INFOCOM Conference, March 2000, pp. 208-216.

Slide 123

Other references

Yi-Bing Lin, “Paging systems: network architectures and interfaces”, IEEE Network, Volume 11, Issue 4, Jul/Aug 1997 Page(s):56 - 6, Digital Object Identifier 10.1109/65.598460

Slide 124

¿Questions?

Slide 125: Lecture 2: Network Signaling and CDPD

IK2555: Mobile and Wireless Network Architectures: Lecture 2

prof. Gerald Q. Maguire Jr. http://people.kth.se/~maguire/

School of Information and Communication Technology (ICT), KTH Royal Institute of Technology

IK2555 Spring 2016 2016.01.08 © 2016 G. Q. Maguire Jr. All rights reserved.

Slide 126

2. Network Signaling and CDPD

Lecture notes of G. Q. Maguire Jr.
For use in conjunction with Yi-Bing Lin and Ai-Chun Pang, *Wireless and Mobile All-IP Networks*, John Wiley & Sons; 2005, ISBN: 0-471-74922-2.

Slide 127

Network Signaling

Interconnection between a PCS Network (PCN) and a PSTN for:

mobility management	tracking the location of mobile users
call control	setting up the call path between a mobile users and the other call party (or parties)
interconnection interfaces	the interconnections themselves
Message routing	information exchange

Mobile Identification Number (MIN) -- the main means of identifying a **MS**
Universal Personal Telecommunication (UPT) number - a number associated with a mobile **subscriber.**

Note there is a distinction between the **device** (a **MS**) and a **user** (as a **subscriber**).

Slide 128

Transaction Capabilities Application Part (TCAP)

For exchanging information which is **not** circuit related.
More than 50 TCAP operations in IS-41 (just) for:

- inter-MSC handoff
- automatic roaming
- operation, administration, and maintenance (OAM)

A TCAP message has two parts: **transaction** and **component**

transaction	QueryWithPermission, Response, ConversationWithPermssion, and Unidirectional (to pass information in one direction)
component	INVOKE, RETURN RESULT (Last), RETURN ERROR, or REJECT

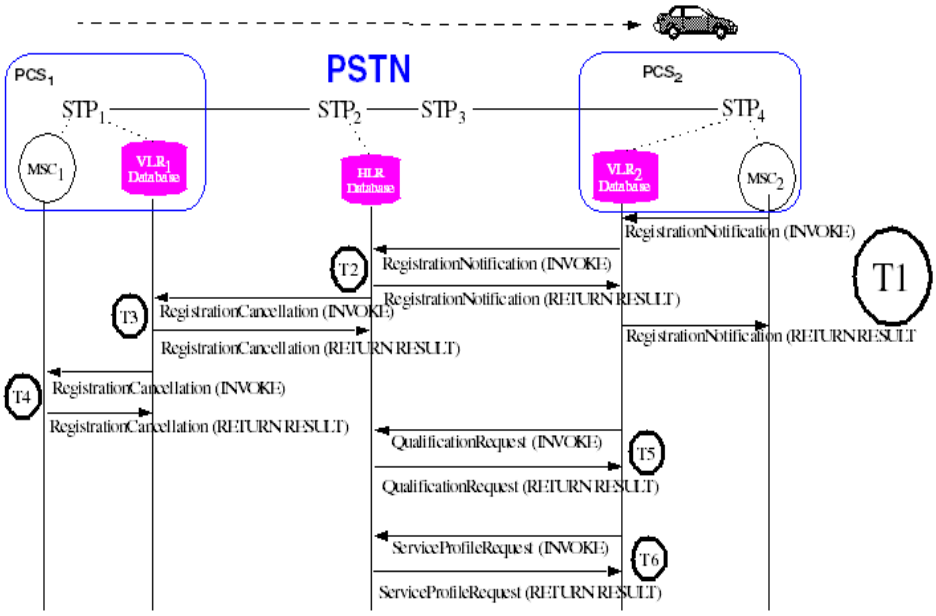
Each TCAP transaction has a **timeout** associated with it and uses **connectionless** transport.

Maguire IK2555, Spring 2016 Slide 128

TIA public documents
ftp://ftp.tiaonline.org/TR-45/

Slide 129

TCAP message flow for a MS registration



Mobile roams from PCS_1 to PCS_2

Slide 130

Transaction 2 (T2) - additional details

Signal Transfer Point$_3$ (STP$_3$) does a table lookup, i.e., **Global Title Translation** (GTT) of the MIN to identify the appropriate HLR's address, then the TCAP message is forwarded from STP$_3$ to STP$_2$ where the HLR is.

GTT is needed because **non-geographic** numbering is assumed {we will return to this later.}.

Slide 131

Automatic Code Gapping (ACG)

- Can use **Automatic Code Gapping** (ACG) to reduce the **rate** at which a network entity such as a MSC sends service request messages to a service control function.
- ACG can be applied automatically when an overload occurs or applied manually for system management.
- ACG can be applied to query messages destined for a specific Point Code and Subsystem Number or for an SCCP Global Title.

3rd Generation Partnership Project 2 (3GPP2), Automatic Code Gapping (Stage 1), 3GPP2 S.R0016, Version 1.0.0, Version Date: December 13, 1999
http://www.3gpp2.org/Public_html/specs/S.R0016_v1.pdf

Purpose: Without automatic code gapping you might overrun the network entity's capacity for processing messages, in which case messages might be lost - then due to the timeouts associated with each transaction, lost messages would cause retries -- further increasing the number of messages!

Note: Anjana Agarwal, Anthony Buttitta, Viraraghavan Sudarsan, and Janice Marie Wunsch, "Automatic code gapping (ACG) for wireless systems", US patent #6,317,601 Nov. 2001 [Agarwal1998]

Maguire IK2555, Spring 2016 Slide 131

Automatic Code Gapping

[Agarwal1998] Anjana Agarwal, Anthony Buttitta, Viraraghavan Sudarsan, and Janice Marie Wunsch, "Automatic code gapping (ACG) for wireless systems", US patent #6,317,601, issued Nov. 2001 (submitted 4 Dec. 1998)
http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=6317601.PN.&OS=PN/6317601&RS=PN/6317601

Slide 132

TIA TSB-51: Authentication, Signaling Message Encryption, and Voice Privacy

- supports authentication over multiple air interfaces (AMPS, TDMA, CDMA) -- GSM authentication is excluded, because the GSM authentication process has been defined in the GSM standards
- provides a method of pre-call validation of (MS) that does **not** require user intervention
- uses **Global Challenge** procedures at registration, call origination, call termination, and at any time using Unique Challenge procedures

  without-sharing (WS) scheme: "shared secret data" (SSD) known only to Authentication Center (AuC) and MS

  sharing (S) scheme: SSD or some aspect of it is shared with the **visited** system
- SSD based on Authentication Key (A-Key) - never transmitted over the air
- includes procedures for generation and distribution of SSD

Slide 133

MIN and ESN

Mobile Identification Number (MIN) - a North American Numbering Plan (NANP) number which is the phone number of a mobile phone

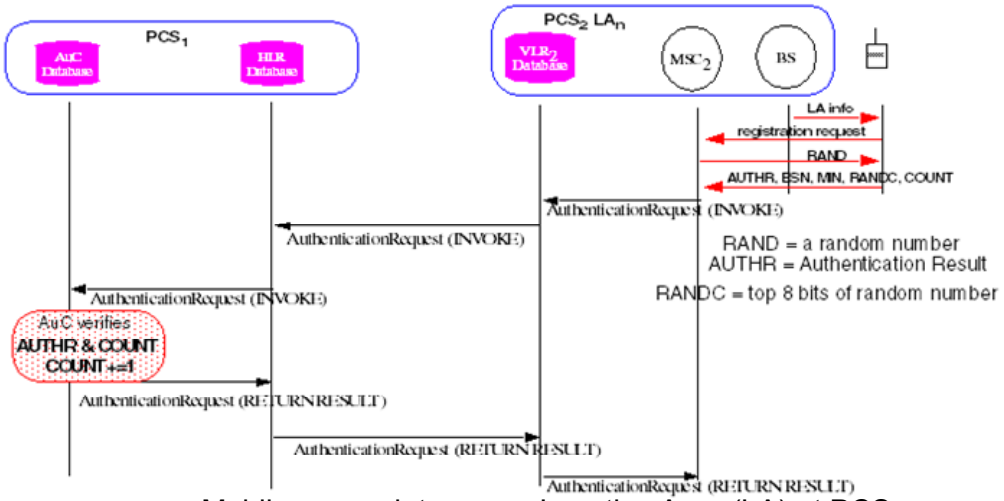
Electronic Serial Number (ESN) - a 32 bit serial number programmed into the phone at manufacture (top 8 bits identify the manufacturer)

In AMPS the MIN and ESN are transmitted in the clear over the air - so it is easy to listen for them and then program another phone with the same values ⇒ **clone**

This lead to hundreds of millions of dollars of fraud ⇒ TSB-51

Slide 134

Without-Sharing Scheme



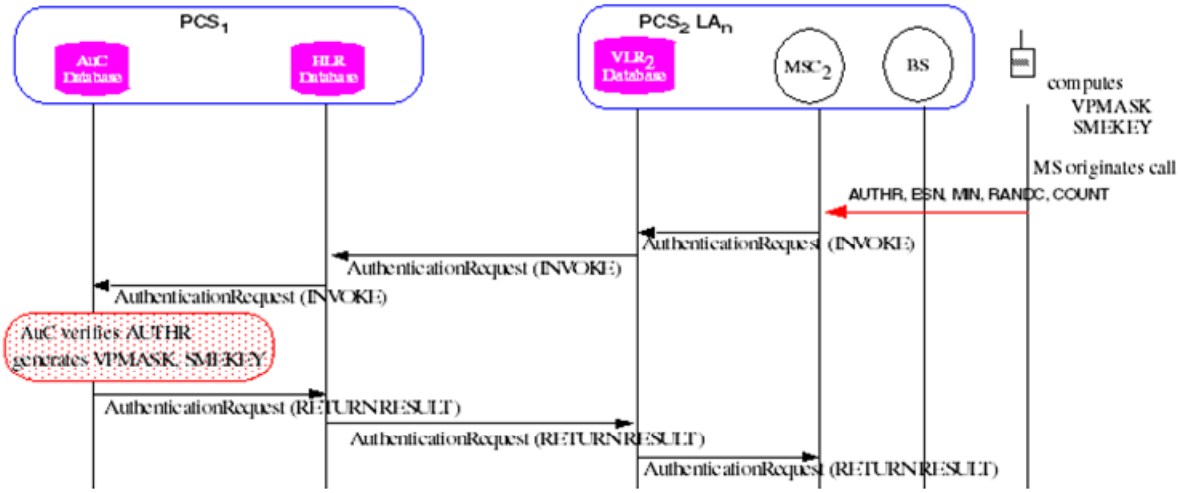
Mobile moves into a new Location Area (LA) at PCS_2

If authentication fails, then the result is RETURN ERROR.

Maguire IK2555, Spring 2016 Slide 134

Slide 135

Without-Sharing Call Origination

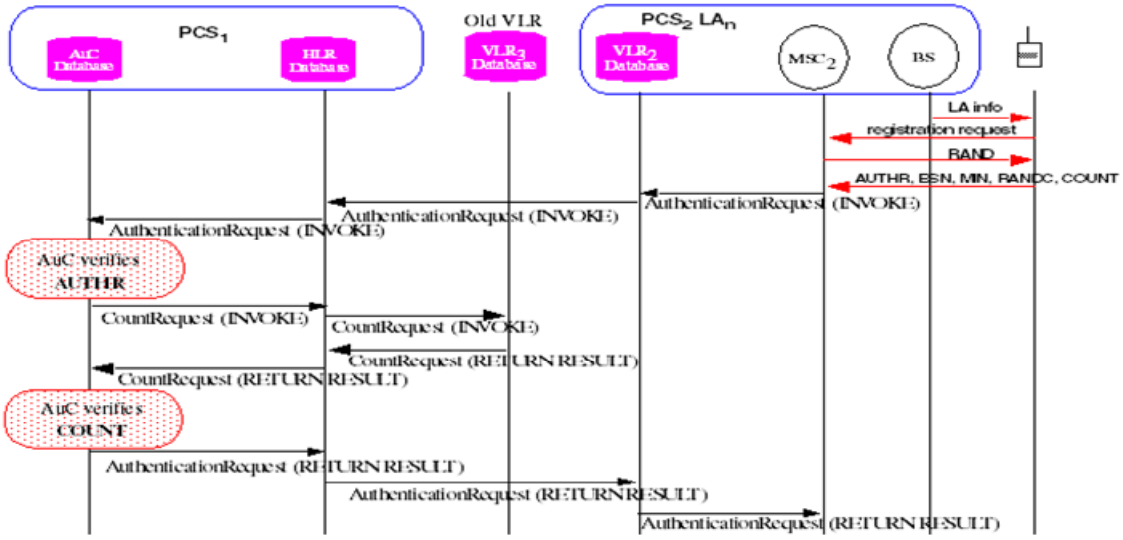


Because of **shared secret data** (SSD) the AuC can generate the same Voice Privacy Mask (VPMASK) and Signaling Message Encryption Key (SMEKEY) as the mobile and passes this information to the operator of PSC_2

Maguire IK2555, Spring 2016 Slide 135

Slide 136

Sharing Scheme

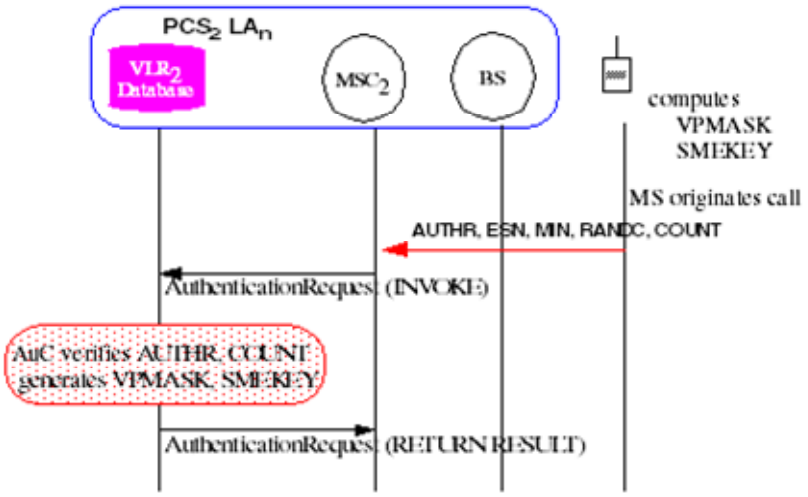


Mobile moves into a new Location Area (LA) at PCS_2 registration using Sharing scheme
Because the SSD was *shared* with the prior VLR_3, we need its value of COUNT.

Maguire IK2555, Spring 2016 Slide 136

Slide 137

Sharing Call Origination



Mobile places a call in PCS_2 using sharing scheme

Note that because the visited system shares the SSD, it no longer has to contact the home PCS's AuC to generate the VPMASK and SMEKEY.

Slide 138

When should you use Without-Sharing vs. Sharing

Use Without-Sharing when the number of registration operations is greater than the number of call originations/terminations.

Can use an adaptive algorithm:

- based on statistics move between Without-Sharing and Sharing schemes
- once you make a call, then use Sharing scheme; but if you move **without** making a call, then revert back to Without-Sharing scheme

Slide 139

Cellular Authentication and Voice Encryption (CAVE) Algorithm

IS-54B - TDMA standard - includes CAVE algorithm [CAVE]

Computes Authentication Result (AUTHR) using SSD, ESN, MIN, a random number (RAND). RAND is typically updated in the system every 20 minutes and SSD is updated for each mobile every 7 to 10 days [Veerasamy].

3 of the 4 IS-54 algorithms have been broken:

- David Wagner (then a University of California at Berkeley graduate student, now faculty member[Wagner]) and Bruce Schneier† & John Kelsey (both of Counterpane Systems) announced that they had broken the **Cellular Message Encryption Algorithm** (CMEA)[Wagner1997] which is used to protect the control channel (for example, dialed digits and alphanumeric pages).
- D. Wagner, L. Simpson, E. Dawson, J. Kelsey, W. Millan, and B. Schneier, "Cryptanalysis of ORYX"[Wagner1998] - shows that the stream cipher used to protect data is breakable with a plain text attack.
- voice privacy depends on a XOR against a generated string - which is generally rather easy to break (as the string is not equal to the message length)

† Author of the popular book: Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Wiley; 2nd edition (October 18, 1996), 758 pages, ISBN-10: 0471117099 and ISBN-13: 978-0471117094.

Maguire IK2555, Spring 2016 Slide 139

TSB-51

[CTIA] Cellular Telecommunications & Internet Association (CTIA) World of Wireless Communication, http://www.ctia.org/

[Veerasamy] Jey Veerasamy, Cellular Authentication, University of Texas at Dallas, was available as http://www.utdallas.edu/~veerasam/cs6385/authentication.ppt can be found at http://web.archive.org/web/20030521041343/http://www.utdallas.edu/~veerasam/cs6385/authentication.ppt

[LinMohan1997] Yi-Bing Lin, Seshadri Mohan, Nelson Sollenberger, and Howard Sherry, "Adaptive Algorithms for Reducing PCS Network Authentication Traffic", IEEE Transactions on Vehicular Technology, 46(3):588-596, 1997

[Wagner1997] David Wagner, Bruce Schneier, and John Kelsey, "Cryptanalysis of the Cellular Message Encryption Algorithm", Crypto'97, 1997. http://www.schneier.com/paper-cmea.html

[Wagner1998] D. Wagner, L. Simpson, E. Dawson, J. Kelsey, W. Millan, and B. Schneier, "Cryptanalysis of ORYX", Fifth Annual Workshop on Selected Areas in Cryptography, SAC'98, Springer Verlag, August 1998, http://www.schneier.com/paper-oryx.html

[Wagner] David Wagner http://http.cs.berkeley.edu/~daw/

[CAVE] CAVE algorithm, formerly available from ftp://ftp.ox.ac.uk/pub/crypto/misc/CAVE.tar.gz

Slide 140

PACS Network Signaling

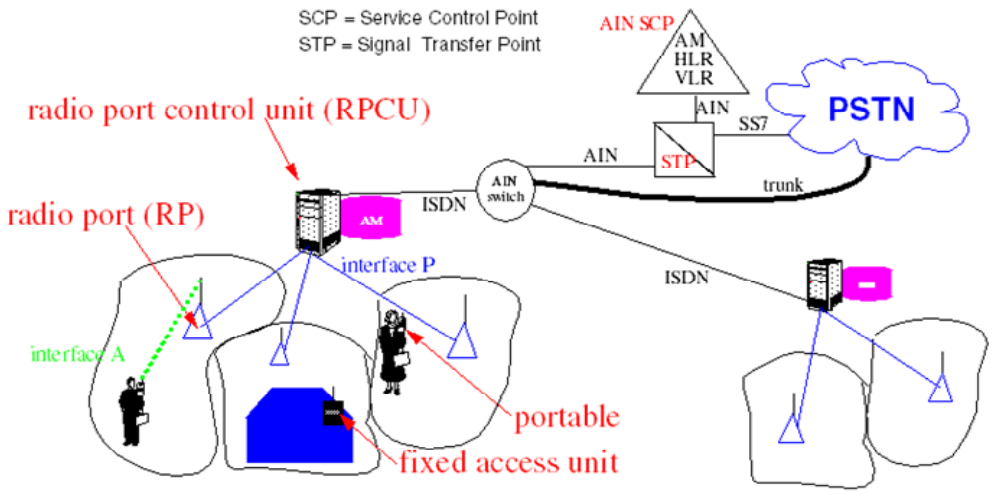
Personal Access Communications Systems (PACS) supports:

- basic call control
- roaming
- handoff management

Does **not** use MSCs or HLR/VLR, but uses Advanced Intelligent Network (AIN) protocol with an Access Manager (AM), AIN switch, and AIN **Service Control Point** (SCP).

Slide 141

PACS Architecture



Slide 142

Access Manager (AM)

The access manager in the **radio port control unit** (RPCU), it provides:

radio control	managing the RPs, trunk provisioning, RP to RP link transfers
non-radio service control	call control (managing the B channels), switching, routing

The RPCU has to deal with **inter-RPCU** handoff (similar to inter-BSC handoff) and inter-radio port (**inter-RP**) handoff.

Note: an AM is also located in the AIN SCP; the two interact with the ISDN/AIN Switch providing tunneling/de-tunneling (i.e., encapsulation) of the ISDN REGISTER messages over AIN.

RPCUs could be connected via an IP network to the VLR, thus bypassing the AIN/ISDN Switch (SSP) for all non-call associated (NCA) signaling.

Slide 143

AIN/ISDN Switch

Note: The textbook often refers to this as the AIN Service Switching Point (SSP).

Uses:

- SS7 ISUP to set up trunk and for **inter-system** handoff
- SS7 TCAP to support mobility management and transport AIN messages between switch and SCP; the AIN messages are basically remote procedure calls (RPC) calls to the SCP
- ISDN for:
  - call control {standard ISDN},
  - automatic link transfer (ALT) {**FACILITY** message for **handoff**}, and
  - non-call associated (NCA) signaling {for example, communication between RPCU and VLR for registration and authentication - **REGISTER** message - which is encapsulated in an AIN NCA-Data message}

Also provides:

- Automatic Code Gapping (for traffic load control)
- Automatic Message Accounting (for access charging)

Slide 144

AIN Service Control Point (SCP)

Provides service logic, databases, and operations to support:

- Home Location Register (HLR)
- Visitor Location Register (VLR)
- Access Manager (AM)
- Authentication Center (AuC)

Communicates with:

- the switch via AIN TCAP
- external PCS databases via IS-41 protocol

Slide 145

PACS Intersystem Handoff

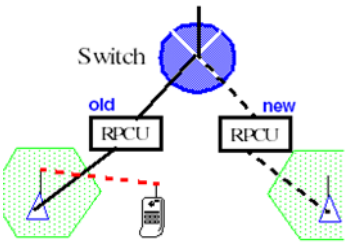
PACS Intersystem Handoff/automatic link transfer (ALT) follows IS-41 anchor switch approach.

Slide 146

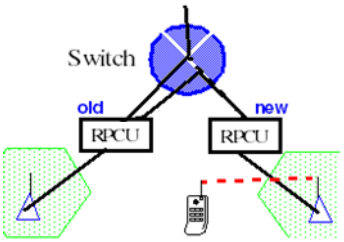
3 alternative inter-RPCU handoff methods

(Switch Loopback, Direct Connection, Three-way Calling Connection):

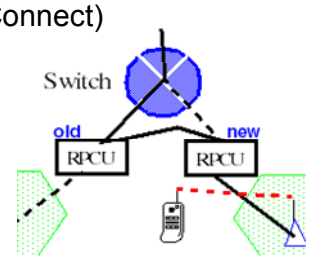
a. Before ALT



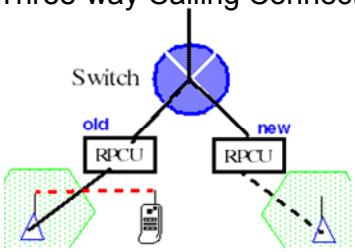
b. After ALT (Switch Loopback)



c. After ALT (Direct Connect)

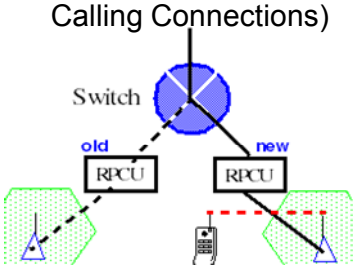


d.During ALT (Three-way Calling Connections)



Note: (d) illustrates that the switch is doing bridging, but the traffic is not using any radio capacity in the new cell - until the mobile arrives

e. After ALT (Three-Way Calling Connections)



Maguire IK2555, Spring 2016 Slide 146

Slide 147

CDPD

In 1992, AT&T Wireless Services developed the **cellular digital packet data** (CDPD) protocol, a **data-only** protocol that (re-)uses the AMPS or IS-136 network. Packets (typically ~1.5 kilobytes) use vacant cellular channels - either an assigned channel or between calls.

CDPD **does not** communicate with the underlying network; but **does** utilize knowledge of this network's channel assignment algorithms to predict when channels will be available for CDPD's use.

Mobile Data Base Stations - do **channel sniffing** to find idle channels

It is essentially an implementation of Mobile*IP [Ioannidis1993a] [Ioannidis1991] [Ioannidis1993b].

For an excellent book about CDPD see [Taylor1997] (note that the full text of this book is available from this site).

Maguire IK2555, Spring 2016 Slide 147

Mobile*IP

[Ioannidis1993a] J. Ioannidis and G. Q. Maguire Jr., The Design and Implementation of a Mobile Internetworking Architecture. Editors: Dejan S. Milojicic, Frederick Douglis, and Richard G. Wheeler, Mobility Processes, Computers, and Agents, Addison-Wesley Pub Co., ACM Press Series, February 1999, 365-377. {Reprint of J. Ioannidis and G. Q. Maguire Jr., The Design and Implementation of a Mobile Internetworking Architecture. USENIX Winter 1993 Technical Conference, pages 491-502. USENIX Association, January, 1993.}

[Ioannidis1991] John Ioannidis, Dan Duchamp, and G.Q. Maguire Jr. IP-based Protocols for Mobile Internetworking. *SIGCOMM'91 Conference: Communications Architectures and Protocols*, pages 235-245. Association for Computing Machinery, September, 1991.

[Ioannidis1993b] John Ioannidis, *Protocols for Mobile Internetworking*, Doctoral Dissertation, Department of Computer Science, Columbia University, 1993.

CDPD

[Taylor1997] Mark S. Taylor, William Waung, and Moshen Banan, *Internetwork Mobility: The CDPD Approach*, Prentice-Hall, Upper Saddle River, NJ, 1997. ISBN 0-13-209693-5
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.99.1957&rep=rep1&type=pdf

Mark S. Taylor, William Waung, Mohsen Banan, *Internetwork Mobility: The CDPD Approach*, Pearson Education, Inc., June 11, 1996
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.99.1957&rep=rep1&type=pdf
Note that this is an on-line version of the entire 300 page book

Salkintzis, "Packet Data over Cellular Networks: The CDPD Approach", *IEEE Communication Magazine*, vol. 37, no. 6, June 1999, pp. 152-159.

Sun Jong Kwon, Yun Won Chung, and Dan Keun Sung, "Performance Analysis of CDPD Sleep Mode for Power Conservation in Mobile End Systems", IEICE Trans. on Communications, Vol. E84B, no. 10, Oct. 2001

Slide 148

Motivation for CDPD

- Most traditional cellular systems (such as AMPS) are **unsuited** for packet data
  - Long call setup times - many seconds (vs. CDPD with from under 1 to 4 seconds)
  - Modem handshaking required - this modem training can often take more time than the data transfer time!
  - Analog providers already have AMPS frequency allocation
- Re-use AMPS channels to provide data service.
  - Must not interfere with existing analog service (viewed as operator's bread and butter)
  - no new spectrum license needed - but you get to make more money with the spectrum you already have (**IFF** you can share the spectrum wisely)
  - This provides an excellent example of multiple services intelligently sharing the spectrum resources - in this case CDPD provides all the intelligence and the existing AMPS device do not have to even be aware of the existence of CDPD.

Goals

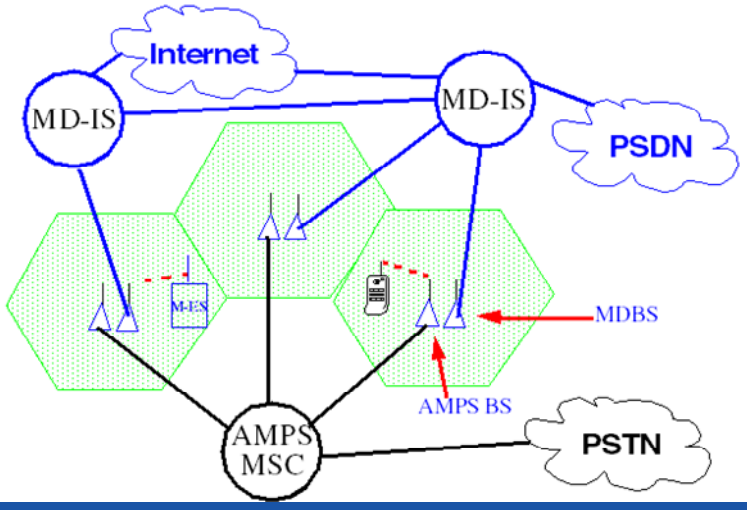
- low speed data: Paging, short message, e-mail, …(achieve 10-12kbps)
- broadcast and multicast (for example, for fleet management)
- "always on-line" packet data service
- transparent to existing AMPS service, but shares spectrum with it

Maguire IK2555, Spring 2016 Slide 148

Slide 149

CDPD network architecture

Mobile End System (M-ES), **Mobile Data Basestation** (MDBS), **Mobile Data-Intermediate System** (MD-IS)



Slide 150

CDPD Entities

Mobile End System (M-ES)

- Subscriber unit - interfaces with the radio at 19.2 kbps
- **Subscriber Identity Module** (SIM) - used to identify subscriber
- Mobile Application Subsystem - actually provides the functionality (could be a PDA, Laptop, embedded processor, …)

Mobile Data Base Station (MDBS)

- controls the radio: radio channel allocation, channel usage, …
- one modem/transceiver per radio channel pair (up & down link)
- generally co-located with the AMPS basestations (so they can share antenna, site, …)

Mobile Data-Intermediate System (MD-IS)

- frame relay switch + packet router
- buffers packets destined to M-ES it knows about (== with TEI assigned)
- supports user mobility by a mobile location protocol

Slide 151

Other entities: Fixed End System (F-ES) - hosts

External F-ESs	traditional non-CDPD host(s)	
Internal F-ESs	hosts **within** the boundaries of the CDPD network; they have access to additional internal network data (usage accounting information, mobile location information, subscriber authentication information, …	
	Accounting Server (AS)	collection and distribution of usage accounting data (each MD-IS periodically sends its usage information to the AS)
	Authentication Server	supports the authentication function in CDPD; may or may not be a part of the MD-IS
	Directory Server	supports directory services within the CDPD network (could support DNS and/or X.500)
	Network Management System	includes configuration management, fault management, performance management and other functions

Slide 152

Limits

- No direct **Mobile End System** (M-ES) to M-ES communication
- radius of a CDPD cell is limited to <10 miles (i.e. < 17km)
- each M-ES can only send two packets back to back - to avoid hogging the channel

Slide 153

Handoffs

Mobile Data Base Station (MDBS) broadcasts a list of **available** channels

When M-ES finds link quality has dropped below a threshold, it checks the channels from the MDBSs that it can hear; if there is a better channel it initiates a link transfer - by switching to the new channel and registering with the new MDBS

MD-IS maintains a **registration directory**

- contains a list of **Temporary Equipment Identifiers** (TEI)
- associated with each TEI is a element **in**activity timer (T203)
- associated with each radio channel stream is a TEI notification timer (T204) - when this timer goes off MD-IS broadcasts a list of TEI's with data buffered for them {mobiles with nothing to send can *sleep* until the next TEI notification frame}
- when a mobile wakes up and hears that there is data for it, it sends a **Receiver Ready** (RR) frame

Slide 154

Connectionless Network Services (CLNS)

CDPD supports both:

- ISO connectionless network protocol
- IP

Slide 155

Roaming Management

Each M-ES has a unique **Network Equipment Identifier** (NEI) which is associated with a home MD-IS (**Mobile Home serving Function** (MHF){analogous to a Mobile IP **Home Agent**}.

Home MD-IS keeps **location directory** of the MD-IS currently serving each of its mobiles (note that the routing is to the current MD-IS, **not** to the M-ES itself)

Each MD-IS keeps a registration directory listing currently visiting mobile (**Mobile Serving Function** (MSF)) {analogous to a Mobile IP **Foreign Agent**}

When a M-ES moves, the home MD-IS *explicitly* cancels the registration at the former MD-IS.

Packet routing is handled just as in Mobile IP.

Slide 156

Multicast

CDPD has explicit provisions for Multicast and enables mobiles to register for a multicast NEI - this must include a **Group Member Identifier** (GMID) which is unique with in the group

Slide 157

CDPD usage

- Very popular for vending machines
- Public safety agencies, Law enforcement, …
  - "because police officers rarely roam outside their well-defined geographic patrol areas"†
- Handheld/laptop IP access

Price Plans: was from $14.95 per month for 250 kilobytes to $39.95 monthly for unlimited usage with a two-year commitment

Of course if you are vending machine you do not buy an unlimited plan, but perhaps if you are vending machine operator you do.

†Formerly available from http://www.proberesearch.com/alerts/2002/wlsdata.htm Available from the Internet Archive as http://web.archive.org/web/20030216141656/http://www.proberesearch.com/alerts/2002/wlsdata.htm

Slide 158

CDPD phaseout

By 2002, GPRS displaced CDPD. With >85% of US subscribers using digital phones ⇒ the AMPS analog networks have decreasing importance; US FCC allows carriers to phase out their analog networks†.

In March 2002, Verizon Wireless announced rate plans for the service based on data transmission volume as part of their rollout of next-generation wireless networks. CDMA 1X (code division multiple access) Express Network pricing:

- $35 a Month for 10 MB, $55 per month for 20 MB, and fees available for up to 150 MB of data
- $99 a month for unlimited service
- data transmission speeds of up to 144 kilobits per second (kbps), with an average transmission rate of 40 to 69 kbps.

Note: Many network operators are no longer supporting CDPD and are turning off service - driven by the lack of an analog network to **overlay**.

† Winter 2008 a number of carriers have announced that they will shutdown their analog networks - which affects services such as GM's OnStar

Slide 159

Ricochet†

Aerie Networks bought the network assets of Metricom at bankruptcy sale. Service only in Denver and San Diego. (Previously 17 market areas). Later these were also shutdown (see http://en.wikipedia.org/wiki/Ricochet_%28Internet_service%29).

The 128 kbps network uses a microcellular-packet-switching, FHSS (Frequency Hopping Spread Spectrum) technology, and is designed for forwarding IP packets.

- Transceivers are deployed in a mesh topology, generally on top of streetlights (for power and low cost space!)
- Designed to be self-configuring and do load-balancing (including routing traffic around congested transceivers)
- $24.99-$27.99 a month
- authentication first using modem's serial number, then via user account and password
- Mean RTT 2450 ms, std. deviation 1500 ms; UDP peak 50-58 kbps
- Developed in 1985 for remote meter reading, in 1994: 28.8 kbps, 2000: 128 kbps

† http://www.ricochet.com/ - for some additional information see [Cherry2002]

Maguire IK2555, Spring 2016 Slide 159

Ricochet

Y. Frankel, A. Herzberg, P. A. Karger, H. Krawczyk, C. A. Kunzinger, and M. Yung. Security issues in a CDPD wireless network. IEEE Personal Communications. Volume 2, Number 4, August 1995. pp. 16-27.

Elan Amir and Hari Balakrishnan, "An Evaluation of the Metricom Ricochet Wireless Network", CS 294-7 Class Project, http://www.lariat.org/Berkeley/node2.html

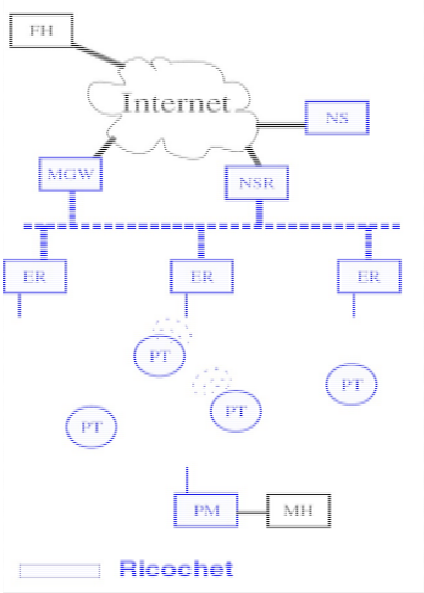
Elan Amir and Hari Balakrishnan, "Performance of the Metricom Ricochet Wireless Network", Summer 1996 Daedalus Retreat, June 1996, http://web.archive.org/web/20040723111756/http://daedalus.cs.berkeley.edu/talks/retreat.6.96/Metricom.pdf

[Cherry2002] S.M. Cherry, "What went wrong at Ricochet?", IEEE Spectrum, Volume 39, Issue 3, March 2002, pp. 60 - 61, Digital Object Identifier 10.1109/6.999196

Slide 160

Ricochet System Architecture

Portable Modems (PM)	Connects the mobile host to the Ricochet network; acts like modem with an extended Hayes AT command set
Pole Top Radios (PT)	Route packets over a wireless link towards or from the nearest wired access point; routing is performed geographically, i.e., based on the latitude and longitude of the pole top radios (PTs) with respect to the final destination.
Ethernet Radios (ER)	Bridges between the wireless and wired portion of the network
Metricom Gateway (MGW)	Maps between IP addresses and Ricochet identifiers and encapsulates packets within Metricom-specific headers and routes the packets to the correct ER. For packets originating from a mobile, decapsulates and forwards the packets on the wired IP network.
Name Server Router (NSR)	Serves as a router to the system name server.
Name Server (NS)	Validate the subscription, based on the PM identification number, and validates service requests.



Maguire IK2555, Spring 2016 Slide 160

Slide 161

¿Questions?

Slide 162: Lecture 3: GSM, GPRS, SMS, Roaming

IK2555: Mobile and Wireless Network Architectures: Lecture 3

prof. Gerald Q. Maguire Jr. http://people.kth.se/~maguire/

School of Information and Communication Technology (ICT), KTH Royal Institute of Technology

IK2555 Spring 2016 2016.01.08 © 2016 G. Q. Maguire Jr. All rights reserved.

Slide 163

3. GSM, GPRS, SMS, Roaming

Lecture notes of G. Q. Maguire Jr.

For use in conjunction with Yi-Bing Lin and Ai-Chun Pang, *Wireless and Mobile All-IP Networks*, John Wiley & Sons; 2005, ISBN: 0-471-74922-2.

Slide 164

Global System for Mobile Communications (GSM)

- designed to be a **digital** (**wide area**) **wireless network**
- driven by European telecom manufacturers, operators, and standardization committees
- very widely used around the world

Note: GSM licenses expired for most operators in Sweden in December 2012 [Ovum 2007], one of the possible alternatives is UMTS900.

Today: there are LTE networks at 800, 900, 1800, and 2600 MHz (with various operators).

Maguire IK2555, Spring 2016 Slide 164

[Ovum 2007] Ovum Consulting, Annex C: GSM-900 and E-GSM bands, Table 1: GSM-900 and E-GSM frequency band allocations in EU-15 countries in 5MHz blocks, in *Market Study for UMTS900: A report to GSMA*, Project Number CLW28, Version V1.1, London, England, February 2007, pg. 114 formerly at http://www.gsmworld.com/documents/umts900_full_report.pdf

Slide 165

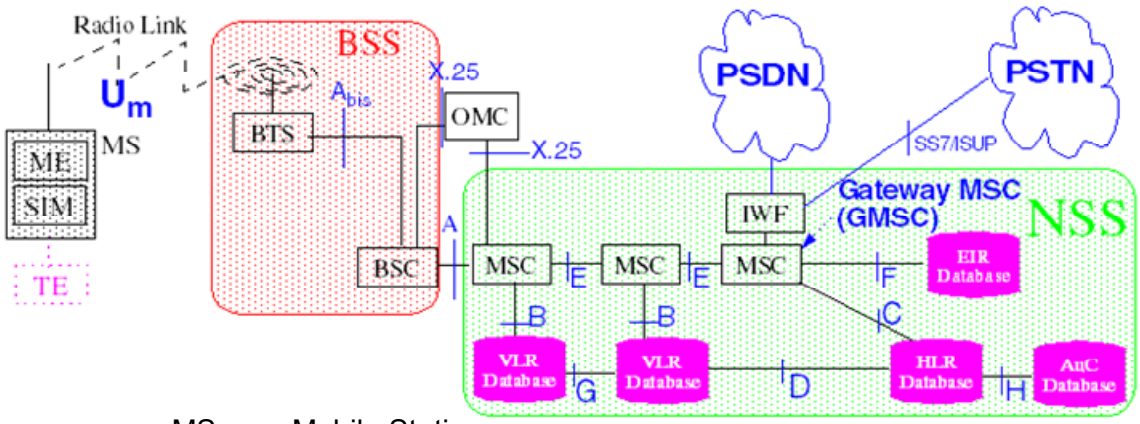
GSM Requirements

- **Service portability**
  - mobile should be able to be used in any of the **participating** countries with international roaming and standardized numbering & dialing (but possibly at different rates!)
  - usable for both wireline services and for mobile service
  - usable when: walking, driving, boating, … (up to 250 km/h)
- **Quality of service and Security**
  - quality at least as good a previous analog systems
  - capable of offering encryption (in some countries this is **off** by default)
- **Good radio frequency utilization**
  - high spectrum efficiency
  - coexistence with earlier systems in the same bands
- **Modern network**
  - follows ITU recommendations - to allow efficient interoperation with ISDN networks
  - supports voice and low rate data
  - standardized mobility and switching support
  - standardized **interfaces** between the subsystems - to allow a mix-and-match system
- **System optimized to limit cost of mobiles (and to a lesser extent to limit the cost of the whole system)**
  - GSM required higher complexity mobiles than earlier analog systems
  - subscriber cost is less than or equal to the then existing analog systems

Maguire IK2555, Spring 2016 Slide 165

Slide 166

GSM Architecture



MS	Mobile Station
BSS	base station system
NSS	network and switching subsystem

Slide 167

Foundation of GSM

Hybrid frequency-division/time-division multiple access

- FDMA - division by frequency of the (maximum) 25 MHz allocated bandwidth into 124 carrier frequencies spaced 200 kHz apart.
  - One or more carrier frequencies assigned to each base station
- Each carrier frequency divided in time, using TDMA
- Fundamental unit of time in this TDMA scheme is a burst period approximately 0.577 ms long
- Eight burst periods are grouped into a TDMA frame (approx. 4.615 ms) = basic unit for the definition of logical channels
- A physical channel is one burst period per TDMA frame
- Slow frequency hopping at up to 217 times per second
  - hopping algorithm is broadcast on the broadcast control channel
  - helps alleviate multipath fading
  - co-channel interference is effectively randomized
  - Note: broadcast and common control channels are not subject to frequency hopping and are **always** transmitted on the same frequency

Infrastructure based on Signaling System 7 (SS7)

Slide 168

GSM contributions

- Location-based mobility management
- Mobile assisted handover
- Temporary Mobile Subscriber ID (TMSI)

Slide 169

Distinctive features of GSM

- Cooperative development by many actors from many countries
- preserved open interfaces between the subsystems (especially between infrastructure elements -- particularly between base stations and switches ⇒ lead to an open market for these subsystems)
- specified a large number of interfaces!
- Phased release - since they could not make all the innovations in time for their targeted 1991 introduction
  - Phase 1 GSM spec. - 100 sections and 5,320 pages!
    - telephony (full rate speech) - with some added features
    - emergency calls
    - data transmission at 2.4/4.8/9.6 kbps (**transparent** {the error correction done by a forward error correction (FEC) mechanism}/**non-transparent** {information is repeated when it has not been correctly received})
    - short message service (SMS)

Slide 170

Distinctive features of GSM

- Phase 2
  - non-voice services (Advice of charge, Calling line identification, Call waiting, Call hold, Conference calling, Closed user groups) and enriched telephony (half-rate speech)
  - High-speed circuit-switched data (HSCSD)
- Phase 2+
  - Multiple service profiles
  - Private numbering plans
  - Access to Centrex services
  - Internetworking with GSM 1800, GSM 1900, Digital Enhanced Cordless Telecom (DECT)
- Phase 2.5
  - GPRS: Global packet radio system
  - Enhanced data rates for GSM (EDGE)

Slide 171

Mobile Station (MS)

- Subscriber Identity Module (SIM)
- Mobile Equipment (ME)
- Mobile Terminal (MT)

Slide 172

Subscriber Identity Module (SIM)

- small form factor - which can be removable and can be moved from one terminal to another (latest card connectors: >5,000 cycles)
  - smart card (generally too large for handsets!)
  - plug-in SIM (the processor and contact from a smart card)
- **user** authenticated via a **Personal Identity Number** (PIN)
- if PIN entered incorrectly, N times, then phone is locked for all but emergency calls, until you enter a **PIN unblocking key** (PUK)
- contains subscriber information:
  - some which is fixed by operator (may include preferred network provider(s))
  - some which is changeable by the user (list of short numbers, phone list, SMS messages, …)
- can be updated via:
  - keyboard or attached terminal equipment or **over the air** (OTA) via SMS message sent by operator/application/… built using SIM Toolkit
- often the SIM is owned by the operator
- profiles - operator/subscription info; SIMs are required to be able to hold at least two profiles
- contains **International Mobile Subscriber Identity** (IMSI)

Maguire IK2555, Spring 2016 Slide 172

Slide 173

SIM card

SIM card showing contacts on the left and the IMSI on the right

Today SIM cards exist in many form factors
including micro-SIM (15×12×0.76mm) and nano-SIM (12.3×8.8×0.67mm)

Slide 174

Phone without and with SIM

Phone without and with SIM card, note the IMEI number and other numders printed inside the back of the phone.

Slide 175

Mobile Equipment (ME)

"the phone" itself - radio and radio interface, display, keyboard, etc.

performs: radio transmission and reception, authentication, handover, encoding & channel encoding.
note: ME without SIM can only make emergency (112) calls

ME identified by International Mobile Equipment Identity (IMEI)

Slide 176

Mobile Equipment (ME)

Radios operate in one or more of the following bands:

System	Uplink(mobile station to base station) (MHz)	Downlink(base station to mobile station) (MHz)	Comments
GSM450	450.4 .. 457.6	460.4 .. 467.6	For migration of NMT 450 operators
GSM480	478.8 .. 486	488.8 .. 496	
GSM850	824 .. 849	869 .. 894	Cellular (800 MHz / 850 MHz) frequency band in Americas
GSM900	890 .. 915	935 .. 960	the original GSM frequency band
GSM1800	1710 .. 1785	1805 .. 1880	also known as DCS1800
GSM1900	1850 .. 1910	1930 .. 1990	also known as PCS 1900

Slide 177

Power saving and interference reduction

- To reduce the MS's power consumption and minimize interference on the air interface, during pauses in speech the MS does not transmit - this is called: **Discontinuous transmission** (DTX)
  "Comfort noise" is artificially generated locally by the MS
- **Discontinuous reception** (DRX)-mobile listens to the paging channel, but only needs to wake up for its sub-channel of the paging channel
- To minimize co-channel interference and to conserve power, both the mobiles and the base transceiver stations operate at the lowest power level that will maintain an acceptable signal quality
  - Power levels can be stepped up or down in steps of 2 dBm from the peak power for the class down to a minimum of 13 dBm (20 milliwatts for MS)
  - only one step at a time and each step takes 60ms
  - there are 16 power levels (i.e., 30 dB of range)
  - terminal is typically only transmitting in one time slot (i.e., 1/8 of the time - so its radiated power is on average 8 dB lower than the set power level)
  - Both mobile station and BTS continually measure the signal strength or signal quality (based on the **bit error ratio**), and pass the information to the base station controller (BSC) which actually manages the power levels.

Slide 178

Classmark

32 bit quantity indicating properties of a mobile station

- revision level
- RF power capability

Class	GSM900	DCS1800	Notes
1	20 W	1 W	For GSM900 classes 1 & 2 - vehicle mounted systems and class 4 - portable terminals
2	8 W†	0.25 W	† 1W average if using a single time slot per frame
3	5 W		
4	2 W‡		‡ 250 mW average if using a single time slot per frame
5	0.8 W		

- (available) encryption procedures
- frequency capabilities (i.e., which bands)
- if the device is SMS capable

Slide 179

User ID ≠ Device ID

IMEI	International Mobile Equipment Identity	15 hexadecimal digits
IMSI	International Mobile Subscriber Identity	15 decimal digits
TMSI	Temporary Mobile Subscriber Identity	32 bits

IMEI consists of:

- Type Approval Code (TAC)
  [Final Assembly Code (FAC) to identify the final assembly plant - 2 digits]†
  Serial number - allocated to the manufacturers - 6 digits
  Check Digit - 1 hexadecimal digit
- International Mobile Equipment Identity and Software Version number (IMEISV) adds a 2 hexadecimal software version number field to the IMEI

An important distinction in GSM is that due to the SIM card the user (or at least IMSI) can be identified separately from the device (MS).

†As of April 1st 2004, the FAC field was eliminated and the previous 6 digit TAC field was expanded to 8 hexadecimal digits

Slide 180

IMSI consists of:

mobile country code (MCC) - 3 digits [66]
mobile network code (MNC) - maximum of 3 digits†
} Home Network Identifier (HNI)
Mobile Station Identification Number (MSIN)

† Note: GSM originally specified 2 digits; 3 digit MNCs are only allocated in North America; for difficulties in transition from 2 to 3 digits [Crowe2002], [ECTRA2000]

TMSI is assigned by the VLR to a visiting subscriber

Maguire IK2555, Spring 2016 Slide 180

[Crowe2002] David Crowe, “IMSI Problems in North America”, IFAST, IFAST#19, 2002.06.06, *http://www.ifast.org/files/IFAST19_015_IMSI.pdf*

[ECTRA2000] “ECTRA Decision on Mobile Network Codes “2013 Change from 2-digits to 3-digits”, GSM Europe, Paris, France, 1st September 2000 formerly at http://www.gsmworld.com/gsmeurope/documents/positions/2000/ectra_web.pdf

Slide 181

Mobile Terminal (MT)

Generally a PDA, PC, …

Interface: serial (DTE-DCE) cable, PCMCIA, IrDA, Bluetooth, …

Slide 182

Part of the extended Hayes AT command set

AT Command	Description	AT Command	Description
+CNMI	New message indication to TE	+CMT	SMS Message Received
+CBM	New Cell-Broadcast Message (CBM)	+CNMA	New Message ACKnowledgement to ME/TE
+CMGC	Send Command	+CPMS	Preferred Message Storage
+CMGD	Delete Message	+CSCA	Service Center Address
+CMGL	List Message	+CSCB	Select Broadcast Message Type
+CMGR	Read Message	+CSDH	Show Text Mode Parameters
+CMCS	Send Message	+CSMP	Set Text Mode Parameters
+CMGW	Write Message to Memory	+CRES	Restore Setting

Slide 183

Base Station System (BSS)

- one or more base transceiver station (BTS) and
- base station controller (BSC)

Slide 184

Base transceiver station (BTS)

Performs: channel coding/decoding and encryption/decryption

BTS includes: radio transmitters and receivers, antennas, the interface to the PCM facility (i.e., backhaul for the voice and control to the BSC), …

About 1/2 the processing is associated with transcoding PCM encoded speech channel to/from GSM coding

Slide 185

Base station controller (BSC)

BTSs are connected to a BSC which manages the radio resources

- call maintenance using the received signal strength sent by mobile stations normally every 480 ms
- initiate handovers to other cells,
- change BTS transmitter power, …

Task breakdown:

call activities	~20-25%
paging and SMS	~10-15%
mobility management	~20-25%
hardware checking/network triggered events	~15-20%

BSCs engineered for about 80% utilization, if overloaded, shed load by: (1) rejecting location updates, (2) rejecting MS originating calls, and (3) ignoring handoffs

Slide 186

Network and Switching Subsystem (NSS)

- MSCs
  Gateway MSC (GMSC) has interconnections to other networks
- Databases
- Gateways

Slide 187

Databases

Home Location Register (HLR)	database for management of mobile subscribers, stores the international mobile subscriber identity (IMSI), mobile station ISDN number (MSISDN) and current visitor location register (VLR) address keeps track of the services associated with each MS an HLR may be used by multiple MSCs
Visitor Location Register (VLR)	caches some information from the HLR as necessary for call control and service provisioning for each mobile currently located in the geographical area controlled by this VLR connected to one MSC and is often integrated into the MSC
Authentication Center (AuC)	a protected database which has a copy of the secret key stored in each subscriber's SIM card this secret is used for authentication and encryption over the radio channel normally located close to HLR
Equipment Identity Register (EIR)	contains a list of all valid mobile station equipment within the network, where each mobile station is identified by its international mobile equipment identity (IMEI) - split into 3 databases: • White list: all known, good IMEIs • Black list: bad or stolen handsets • Grey list: handsets/IMEIs that are uncertain

Slide 188

Equipment Identity Register (EIR)

Optional in a GSM network, i.e., **not** required

EIR block (bars) calls from a particular MS, **not** from a subscriber.

Sometimes the AuC and EIR are combined.

Slide 189

Operation Sub-System (OSS)

- Operation and Maintenance Center
- Service management
  - subscription management for registering new subscriptions, modifying and removing subscriptions, as well as billing information
  - billing
  - fraud detection
  - …

Slide 190

Operation and Maintenance Center (OMC)

Manages the GSM functional blocks: MSC, BSC (and indirectly the BTSs)

Task: to maintain satisfactory operation of the GSM network

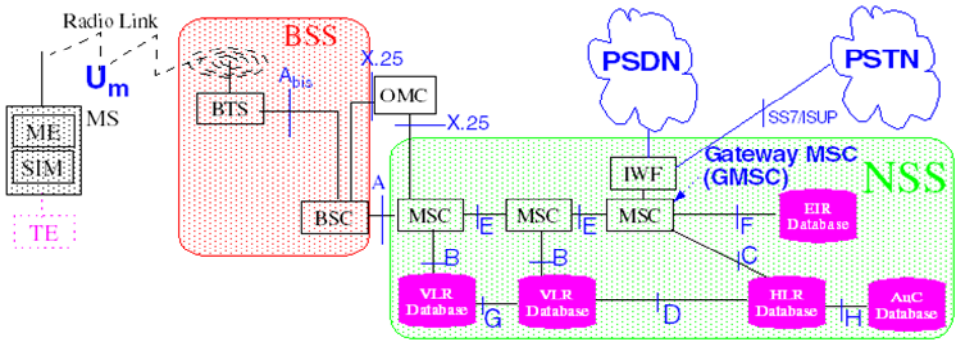
Based on observing system load, blocking rates, handovers, …

Activities:

- Network Management System (NMS) used to modify network configuration
- equipment maintenance aiming at detecting, locating, and correcting faults

Slide 191

GSM Interfaces (just some of them!)

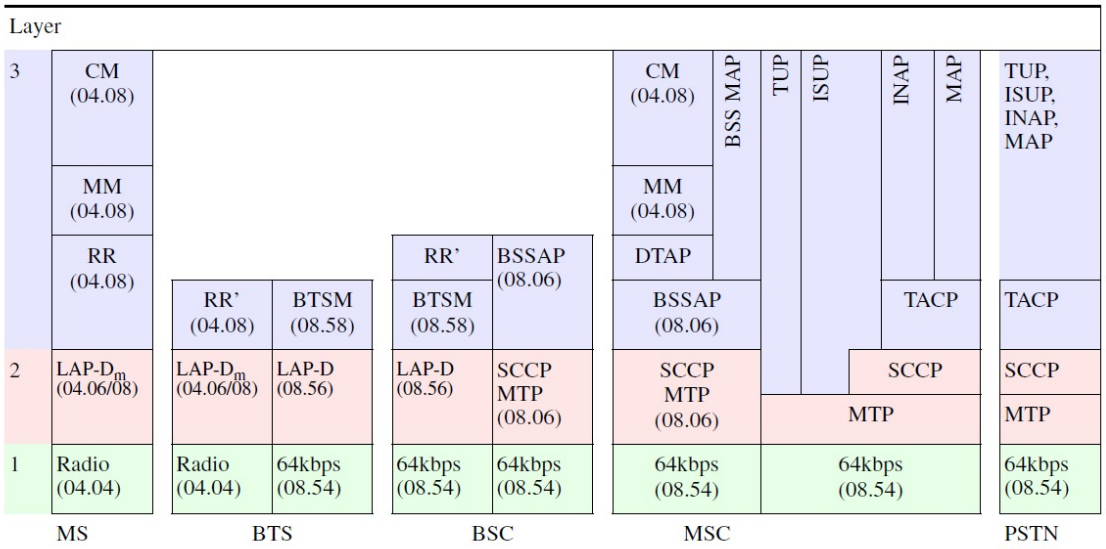


Interface	Description	Interface	Description
U_m	Radio link between MS and BTS	D	between HLR and VLR (MAP/TCAP)
A_{bis}	between BTS and BSC, PCM 2 Mbps, G. 703	E	between two MSCs (MAP/TCAP + ISUP/TUP)
A	between BSC and MSC, PCM 2 Mbps, G. 703	F	between MSC and EIR (MAP/TCAP)
B	between MSC and VLR (use MAP/TCAP protocols)	G	between VLRs (MAP/TCAP)
C	between MSC and HLR (MAP/TCAP)	H	between HLR and AuC

Maguire IK2555, Spring 2016 Slide 191

Slide 192

GSM protocol stack



Numbers in parentheses indicate the relevant ETSI-GSM recommendations.

Slide 193

GSM Layers

- Layer 1: Physical layer
  - physical transmission
  - channel quality measurements
  - GSM Rec. 04.04, PCM 30 or ISDN links are used
    (GSM Rec. 08.54 on A_{bis} interface and 08.04 on A to F interfaces)
- Layer 2: Data link layer
  - Multiplexing of layer 2 connections on control/signaling channels
  - Error detection (based on HDLC)
  - Flow control
  - Transmission quality assurance
  - Routing
- Layer 3: Network layer
  - Connection management (air interface)
  - Management of location data
  - Subscriber identification
  - Management of added services (SMS, call forwarding, conference calls, etc.)

Slide 194

GSM Air interface

- Layer 1 (GSM Rec. 04.04): Um interface
- Layer 2 (GSM Rec. 04.05/06): LAP-D_m protocol (similar to ISDN LAP-D):
  - connectionless transfer of point-to-point and point-to-multipoint signaling channels
  - Setup and tear-down of layer 2 connections of point-to-point signaling channels
  - connection-oriented transfer with in order delivery, error detection and error correction
-

Slide 195

GSM Air interface: layer 3

Layer 3 (GSM Rec. 04.07/08) with sub-layers for control signaling channel functions (BCH, CCCH and DCCH):

- **Radio resource management** (RR): to establish and release stable connection between mobile stations (MS) and an MSC for the duration of a call and to maintain connection despite user movements - functions of MSC:
  - cell selection
  - handover
  - allocation and tear-down of point-to-point channels
  - monitoring and forwarding of radio connections
  - enabling encryption
  - change transmission mode
- **Mobility management** (MM) handles the control functions required for mobility:
  - authentication
  - assignment of TMSI,
  - management of subscriber location
- **Connection management** (CM) - set up, maintain and tear down calls connections:
  - Call control (CC): Manages call connections,
  - Supplementary service support (SS): Handles special services,
  - Short message service support (SMS): Transfers brief text messages

Slide 196

Messages

Neither the BTS nor the BSC interpret CM and MM messages, these messages are exchanged between the MSC or the MS using the direct transfer application part (DTAP) protocol on the A interface.
Radio Resource Management (RR) messages are mapped to or from the base station system application part (BSSAP) for exchange with the MSC:

- Transmission mode (change) management
- Cipher mode management
- Discontinuous transmission mode management
- Handover execution
- Call re-establishment
- RR-session release
- Load management
- SACCH procedures
  - radio transmission control (power & timing, downlink), (measurements, uplink)
  - general information
- Frequency redefinition
  - General information broadcasting (BCCH)
  - cell selection information
  - information for idle mode functions
  - information needed for access
  - cell identity

Maguire IK2555, Spring 2016 Slide 196

Slide 197

A_{bis} interface

Dividing line between the BSC function and the BTS
BSC and BTS can be connected using leased lines, radio links, metropolitan area networks (MANs), LANs {see University of California at Berkeley's ICEBERG}, …

Two channel types exist between the BSC and BTS:

- Traffic channels (TCH): configured in 8, 16 and 64 kbps formats - for transporting user data
- Signaling channels: configured in 16, 32, 56 and 64 kbps formats - for signaling purposes between the BTS and BSC

Each transceiver (transmitter + receiver) generally requires a signaling channel on the A_{bis} interface, data is sent as **Transcoder Rate Adapter Unit** (TRAU)† frames (for a 16 kbps traffic channel (TCH), 13.6 kbps are used for user data and 2.4 kbps for inband signaling, timing, and synchronization)

† It is not defined where TRAU is placed, i.e., it could be part of BTS, BSC, or MSC.

Slide 198

A_{bis} protocols

- Layer 1 (GSM Rec. 08.54)
  - 2.048 Mbps (ITU-T: E1) or 1.544 Mbps (ANSI: T1) PCM facility
  - with 64/32/16 kbps signaling channels and 16 kbps traffic channels (4 per timeslot)
- Layer 2 (GSM Rec. 08.56)
  - LAP-D protocol used for data messaging between the BTS and BSC
  - **Service Access Point Identifier** (SAPI) refers to the link identifier transmitted in the LAPD protocol (inherited from ISDN)
- Layer 3 (GSM Rec. 08.58/04.08)
  - BTS management (BTSM) via three logical signaling connections identified by Service Access Point Identifier (SAPI):
    - SAPI 0 is used by all messages coming from or going to the radio interface
    - SAPI 62 provides O&M message transport between the BTS and BSC
    - SAPI 63 is used for dynamic management of TEIs as well as for layer 2 management functions.

Slide 199

A Interface

Defines interface between the BSC and MSC

TCHs are converted from 64 kbps to 16 kbps in the transcoder equipment, two cases based on where the transcoder equipment (TCE, i.e., TRAU) is located:

at BSC or BTS	traffic channel (TCH) occupies a complete 64 kbps timeslot in the 2 Mbps or 1.544 Mbps PCM link (layer 1, GSM Rec. 08.04)
at MSC	the TCHs are 16 kbps on the A interface

At least 2 time slots on the PCM link are needed for control and signaling purposes.

Slide 200

A interface protocols

Signaling protocol (layer 2+3) between BSC and MSC based on the SS7 standard and is transmitted along with the user data within the PCM facility. Normally timeslot 16 (TS16) of the 64 kbps frame is used.

The following protocols are employed:

- Layer 1 (GSM Rec. 08.04) either 2.048 Mbps (ITU-T: E1) or 1.544 Mbps (ANSI: T1) PCM link
- Layer 2 (GSM Rec. 08.06) SS7-based protocols
  - Message transfer part (MTP) protocol - transmission security between the BSC and MSC
  - Signaling connection control part (SCCP) protocol
  - SCCP connection can be initiated by a mobile station (MS) or an MSC
  - An SCCP connection can involve the following protocols:
  - From the MS:
    - MM: CM service request
    - RR: Paging response
    - MM: Location updating request
    - MM: CM re-establishment request
  - From the MSC:
    - Initiation of an “external handover” (BSSMAP: handover request).
  - MSC manages the SCCP connections

Slide 201

A interface protocols – layer 3

Layer 3 (GSM Rec. 08.08)

- Base station system application part (BSSAP) protocol
- On MSC end:
  - Base station management application part (BSSMAP) protocol - counterpart to the RR protocol on the air interface
  - Direct transfer application part (DTAP) protocol transmits CC and MM messages trans- mitted transparently through the BTS and BSC

Slide 202

GSM Audio

- Speech coding - 20ms (i.e., 160) samples (8kHz @13 bits) are buffered then coded
- Error protection (codec specific)
- Error detection (CRC)
- Muting and Bad Frame Handling (substitution) - GSM 06.91
- Comfort Noise Generation (CNG) - GSM 06.92
- Voice Activity Detection (VAD) - GSM 06.94
- Discontinuous Transmission (DTX) - GSM 06.93)

Manufacturer specific audio features:

- noise cancelling
- spectrum equalization
- echo cancellation

Slide 203

GSM Audio CODECs

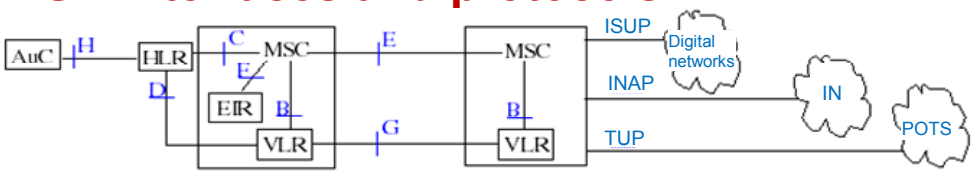
CODEC	Description
Full rate (FR)	13 kbps , Regular pulse excitation - long term prediction (RPE-LTP)
Half rate (HR)	5.65 kbps VSELP
Enhanced full rate (EFR)	12.2 kbps Algebraic Code Excited Linear Prediction (ACELP)
Adaptive Multi Rate (AMR)	ACELP; eight bit rates ranging from 4.75 kbps .. 12.2 kbps - see [3GPP GSM-AMR standards]
Adaptive Multi Rate (AMR) **wideband** - ITU G.722.2 and 3GPP's GSM-AMR WB	codes **16 bit** linear PCM at **16 kHz**; 9 data rates (6.6 .. 23.85 kbps) C callable interface for encoder/decoder

Maguire IK2555, Spring 2016 Slide 203

[3GPP GSM-AMR standards] 3GPP GSM-AMR standards:
•3GPP TS 26.071 V4.0.0 AMR Speech Codec; General Description
•3GPP TS 26.090 V4.0.0 AMR Speech Codec; Transcoding functions
•3GPP TS 26.091 V4.0.0 AMR Speech Codec; Error concealment of lost frames
•3GPP TS 26.092 V4.0.0 AMR Speech Codec; Comfort noise aspects
•3GPP TS 26.093 V4.0.0 AMR Speech Codec; Source controlled rate operation
•3GPP TS 26.094 V4.0.0 AMR Speech Codec; Voice activity detector
•3GPP TS 26.071 V4.0.0 ANSI-C code for AMR speech codec (Code Version 7.5.0)
•3GPP TS 26.074 V4.0.0 AMR Speech Codec; Test sequences

Slide 204

MSC interfaces and protocols



- Mobile Application Part (**MAP**) (GSM Rec. 09.02)
  - controls queries to the different databases in the mobile radio network (HLR, VLR, EIR, …)
  - responsibilities include access and location management, MSC-MSC handover, security functions, O&M, SMS, and supplementary services.
- Transaction Capabilities Application Part (**TCAP**)
  - provides universal calls & functions for handling requests to distributed appl. processes
- ISDN User Part (**ISUP**)
  - controls interworking (e.g. call setup/tear-down) between Public Land Mobile Networks (PLMNs) and other networks, and provides the same basic functionality as TUP
- Intelligent Network Application Part (**INAP**)
  - implements intelligent supplementary services (e.g. free call, time-dependent routing)
- Telephone User Part (**TUP**)
  - implements interworking between PLMNs and other networks
  - used to provide international connections and is being replaced by ISUP

Maguire IK2555, Spring 2016 Slide 204

Slide 205

GSM Logical Channels

Traffic channels		Full-rate (TCH/F) @ 22.8 kbps Half-rate (TCH/H) @ 11.4 kbps	Two way
Signaling channels	Broadcast channels	Frequency correction (FCCH) Synchronization (SCH) Broadcast control (BCCH)	base-to-mobile
	Common control channels	Paging (PCH) Access Grant (AGCH)	
		Random access (RACH)	mobile-to-base
	Dedicated control channels	Stand-alone dedicated control channel (SDCCH) Slow associated control (SACCH) Fast associated control (FACCH)	two-way

Slide 206

Traffic channel (TCH)

Multiframe - group of 26 TDMA frames (120 ms long)

- 24 are used for traffic (voice or user data)
- 1 is used for the slow associated control channel (SACCH)
- 1 is currently unused

TCHs for the uplink and downlink are separated in time by 3 burst periods

- mobile station does not have to transmit and receive simultaneously
- simplifies the electronic circuitry; avoids antenna duplex filters
- reducing complexity helps to cut power consumption

Slide 207

Broadcast channels (BCH)

Carry only **downlink** information - mainly for synchronization and frequency correction.

However, it is the only channel capable of point-to-multipoint communications in which short messages are simultaneously transmitted to several mobiles.

- Broadcast control channel (BCCH)
  - General information, cell-specific; e.g. local area code (LAC), network operator, access parameters, list of neighboring cells, etc. A MS receives signals via the BCCH from many BTSs within the same network and/or different networks
  - tells MS what their initial power level should be
- Frequency correction channel (FCCH)
  - correction of MS frequencies
  - transmission of frequency standard to MS
  - also used for synchronization of an acquisition by providing the boundaries between timeslots and position of the first time slot of a TDMA frame
- Synchronization channel (SCH)
  - frame synchronization (TDMA frame number) and identification of base station
  - reception of one SCH burst provides a MS with all the information needed to synchronize with a given BTS

Slide 208

Common control channels (CCCH)

Uplink and downlink channels between the MS card and the BTS.
Convey information from the network to MSs and provide access to the network.

- Paging channel (PCH)
  - Downlink only
  - MS is informed (by the BTS) of incoming calls via the PCH.
- Access grant channel (AGCH)
  - Downlink only
  - BTS allocates a TCH or SDCCH to the MS, thus allowing the MS access to the network.
- Random access channel (RACH)
  - Uplink only
  - allows MS to request an Stand-alone dedicated control channel (SDCCH) in response to a page or due to a call
  - MS chooses a random time to send on this channel (note: potential collisions with RACH transmissions from other MSs)

PCH and AGCH are transmitted in one channel called the paging and access grant channel (PAGCH) - they are separated in time.

Slide 209

Dedicated control channels (DCCH)

Responsible for roaming, handovers, encryption, etc.

- **Stand-alone dedicated control channel (SDCCH)**
  - communications channel between MS and the BTS
  - signaling during call setup -- before a traffic channel (TCH) is allocated
  - It takes ~480ms to transmit a message via SDCCH
- **Slow associated control channel (SACCH)**
  - always allocated to a TCH or SDCCH
  - used for "non-urgent" procedures: radio measurement data (e.g. field strengths) {information is used for handover decisions}, power control (downlink only), timing advance†, …
  - 260bps channel - enough for reporting on the current cell and up to 6 neighbors about twice per second (if there is no other traffic for this channel)
  - note that the MS is told what frequencies to monitor (BTSs have a color code assigned to them so the that the MS can report on multiple BTSs which are using the same frequency)
- **Fast associated control channel (FACCH)**
  - similar to the SDCCH, but used in parallel to operation of the TCH
  - if the data rate of the FACCH is insufficient, "borrowing mode" is used (i.e., additional bandwidth borrowed from the TCH), this happens for messages associated with call establishment authentication of the subscriber, handover decisions, …
  - It takes ~40ms to transmit a message via FACCH

† Transmission and reception of bursts at the base station must be synchronized, thus the MS must compensate for the propagation delays by advancing its transmission 0 .. 233 ms which is enough to handle cells of radius up to 35 km.

Slide 210

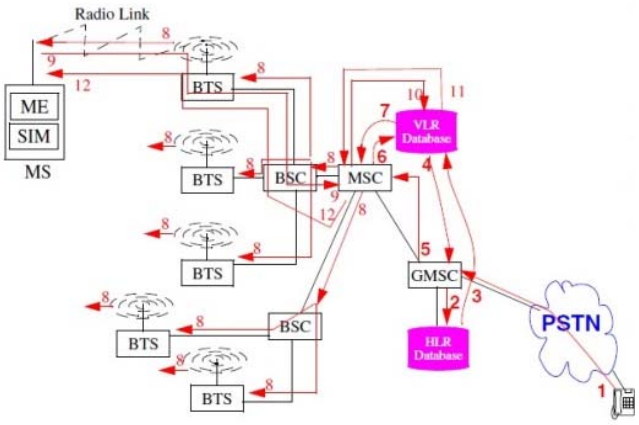
GSM Timing

A **very elaborate** timing structure ranging from 1/4 of a bit (900ns) to an encryption hyperframe (3 hours 28 minutes and 53.76s)!

Unit	Time		
bit	3.69µs		
slot	156.25 bits (577 µs)		
frame	8 slots (4.615 ms)		
traffic multiframe	26 frames (120 ms) or	control multiframe	51 frames (235.4 ms)
superframe	51 traffic multiframes or 26 control multiframes (6.12 s)		
hyperframe	2048 superframes (3 hours 28 minutes and 53.76s)		

Slide 211

Incoming Call



1. incoming call is passed from the fixed network to the gateway MSC (GMSC)
2. based on the IMSI numbers of the called party, HLR is determined
3. HLR checks for the existence of the called number, then the relevant VLR is requested to provide a mobile station roaming number (MSRN)
4. reply transmitted back to the GMSC
5. connection is switched through to the responsible MSC
6. VLR is queried for the location range and reach ability status of the mobile subscriber
7. if the MS is marked reachable, then a radio call is enabled
8. radio call is executed in all radio zones assigned to the VLR
9. reply from the MS in its current radio cell
10. when mobile subscriber telephone responds to the page, then complete all necessary security procedures
11. if this is successful, the VLR indicates to the MSC that call **can** be completed
12. call can be completed

Call from fixed network to MS - we don't know which cell the mobile is in, only its rough location

Maguire IK2555, Spring 2016 Slide 211

Slide 212

Mobility Management (MM)

GSM network keeps track of which mobile telephones are powered on and active in the network. The network keeps track of the last known location of the MS in the VLR and HLR.

Radio sites connected to the MSC are divided into “location areas” (LAs), thus when a call comes for an MS, the network looks for the MS in the last known location area.

Each BTS is assigned (by the operator) a 40 bit ID - called a location area identity (LAI), with three parts:

- mobile country code (MCC) - 3 (hex) digits [E.212]
  http://en.wikipedia.org/wiki/Mobile_country_codes
- mobile network code (MNC) - originally 2, later 3 (hex) digits
- location area code (LAC) - originally 5, later 4 hex digits (= 2 bytes = 65K values)

Within each location area - each cell has a Cell ID (CID)

Cell Global Identity (CGI) = CID, MCC, MNC, and LAC

Maguire IK2555, Spring 2016 Slide 212

[E.212] “The international identification plan for mobile terminals and mobile users”, ITU E.212, revised May 2004
http://www.itu.int/rec/recommendation.asp?type=items&lang=e&parent=T-REC-E.212-200405-I
{note that ITU charges for access to the document}

Slide 213

Security

Use of TMSI rather than IMSI - reduces the need to send IMSI over the air (thus simply listening to the radio link it is harder to identify a given user); there is a pool of TMSIs for each LAC.

Two major aspects of security: Authentication and Encryption

A3	Authentication algorithm
A5	Ciphering algorithm
A8	Ciphering key computation
K_i	secret encryption key - operator determines length, but it can be upto 128 bits
K_c	cypher key, computed based on K_i

Cipher mode management

Connection always starts in non-ciphered mode, because ciphering requires a user specific key and the network has to know the identity of the subscriber before it can be used!

Slide 214

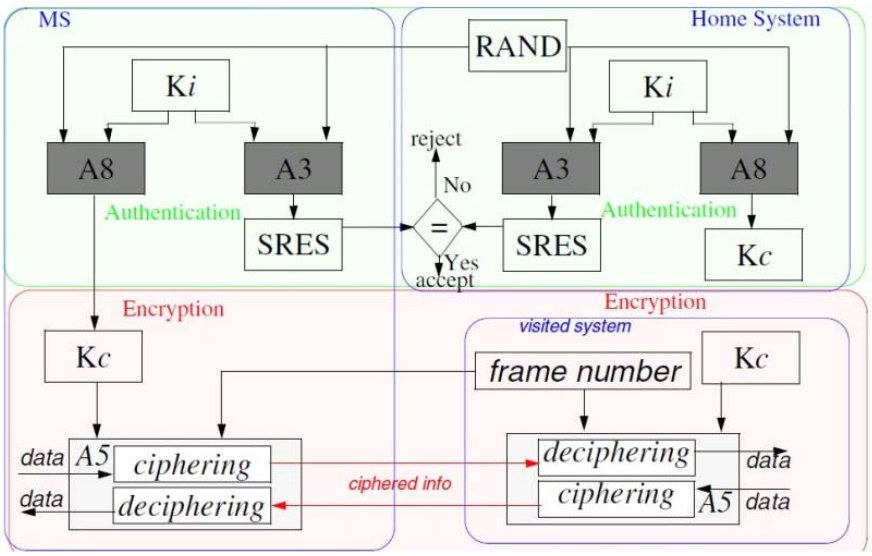
Authentication

User authentication normally takes place when the MS is turned on (user must key in a PIN code on the handset in order to activate the hardware before this automatic procedure can start).

Authentication occurs with each incoming call and outgoing call. This is based on checking that "K_i" (secret encryption key) stored in the AuC matches the "K_i" stored in SIM card of the MS.

Slide 215

Authentication and Encryption



Slide 216

Practical breaking of GSM encryption using readily available tools

The GSM A5/1 algorithm has been criticized for many years. In a presentation Karsten Nohl and Chris Paget, GSM - SRSLY?, 26th Chaos Communication Congress, 27 December 2009†, have shown a **practical** means of intercepting and decrypting GSM calls using readily available hardware and software. See also the related A5/1 Cracking Project‡.

Note that an interesting aspect of their method of computing tables to be used for the actual decryption is the use of multi-core processors such as the graphical processors (GPUs) (found on many graphics cards) and cell processors (found in many gaming systems).

† formerly available from http://events.ccc.de/congress/2009/Fahrplan/attachments/1479_26C3.Karsten.Nohl.GSM.pdf
‡ *http://opensource.srlabs.de/projects/a51-decrypt*

Slide 217

GSM data rates

The following table of data rates is from page 39 of [Jarske2001]

Connection Type†	Two-way delay
TCH/F9.6 T	330 ms
TCH/F9.6 NT	> 330 ms
TCH/F4.8 T	330 ms
TCH/F2.4 T	200 ms
TCH/H4.8 T	600 ms
TCH/H4.8 NT	> 600 ms
TCH/H2.4 T	600 ms

†T = Transparent, NT = Non-transparent

Maguire IK2555, Spring 2016 Slide 217

[Jarske2001] Petri Jarske, The GSM System, Principles of Digital Mobile Communication Systems, 2001 edition, Technical University Tampere, Finland formerly at http://www.cs.tut.fi/kurssit/83150/DigiCom2001.PDF

Slide 218

System engineering

The operator must choose how many of each element (MSC, BSC, BTS, …) to order, what capacity each must have, where to install them, …. However, since traffic does not remain constant installing enough capacity for long term traffic is *not* cost effective ⇒ system engineering is an on-going activity

Note: goal of cellular planning is to choose the cell sites and cell parameters (frequency allocation, capacity, power, etc.) to provide economically continuous coverage and support the required traffic density (not an easy task)

Table of parameters, from page 101 of [Jarske2001]

Area	Parameters	
Cell planning	frequencies beacon frequencies hopping sequences power control parameters	handover parameters cell selection parameters Base Station Identity Code (BSIC)
Dimensioning	# of common channels # of traffic channels	location areas periodic location updating
Load control	overload control parameters	

[Jarske2001] Petri Jarske, The GSM System, Principles of Digital Mobile Communication Systems, 2001 edition, Technical University Tampere, Finland formerly at http://www.cs.tut.fi/kurssit/83150/DigiCom2001.PDF

Slide 219

GSM Network Optimization

Based on network performance & utilization, subscriber behavior, and (QoS) Test methods:

- **Traffic analysis**: the signaling channels in the PCM frame are monitored and analyzed on the A_{bis} and A interfaces
- **Bit error ratio test** (BERT): bit error measurement at the PCM level and the GSM-specific level (TRAU frame)
  - PCM bit error ratio (BER) is used to verify the quality of lines leased from fixed network operators
  - By evaluating the control bits in the TRAU, a bit error probability can be determined (uplink) during actual communications (in-service) {No easy measurement of the downlink BER}
  - More accurate radio link BER measurement (out-of-service) measurement in which the 260 data bits in the TRAU frame are checked using a pseudo-random bit sequence (PRBS)
- **Alarm monitoring** - checking PCM links for layer 1 alarms
- **Network quality test**: lots of measurements - including:
  - island problems, detection of coverage holes, interference, network load regarding signaling and traffic, handover failures, Receive level (RXLEV) surveillance, bit error ratio of a BTS (RXQUAL), multipath interference and propagation delays, frequency interference (due to nearby frequency reuse), call completion/disconnect rate, indications of system overload.

Slide 220

Optimal Cell Planning

Some of the parameters which have to be decided [Abiri2002]:

- **Selecting Site location**
- **Antenna parameters**
  - Tilt, Azimuth, Height, Antenna type
- **Site parameters**
  - **Transmitter power/Dedicated channel power level/Common channel power level**
- **Service parameters**
  - **Power per service**
  - **Enable/disable handover per service**
- **Network parameters**
  - **Handover**
    - **Neighbor lists/Hysteresis/Timers**
  - **Power control policy**
- **Resource management**

Note: first two are sets of parameters are fixed (⇒ a physical change in the site), while the others can be changed under software control.

Maguire IK2555, Spring 2016 Slide 220

[Abiri2002] Ron Abiri, “Migrating to an Advantage: Planning & Optimizing to Maximize Network efficiency & ROI”, Schema Ltd., 2002. formerly at http://www.iec.org/events/2002/natlwireless_nov/featured/f1_abiri.pdf

Slide 221

Features

Call Waiting (CW)	{network-based feature} users with a call in progress receive an audible beep to alert them that there is an incoming call for their MS The incoming call can be: • **accepted** {the original call is put on hold}, • **sent to voice mail**, or • **rejected** {in this case the caller will receive a busy signal}
Call Hold (CH)	allows the MS to "park" an "in progress call", to make additional calls or to receive incoming calls
Call Forwarding (CF)	{network-based feature} allows calls to be sent to other numbers under conditions defined by the user Conditions can be either unconditional or dependent on certain criteria (no answer, busy, not reachable)
Calling Line ID	caller's network to delivers the calling line ID (telephone no.) to the GSM network; GSM telephone displays the originating telephone number
…	

Slide 222

GSM Phase 2+

- **High Speed Circuit Switched Data** (HSCSD)
- **General Packet Radio Service** (GPRS)

Slide 223

High Speed Circuit Switched Data (HSCSD)

Idea is simple	use several time slots out of each TDMA frame for one data connection
Reality	this is taxing for the RF power systems

In the basic GSM model transmit/receive (TX/RX) activities, the terminal can be implemented using **one** frequency synthesizer (even though it takes some time for the synthesizer to change from one frequency to another) - because of the offset of 3 slots between transmit and receiver.

If you only use 2 slots, you just need a synthesizer that changes faster, but at 3 slots you potentially need to transmit and receive at the same time.

At eight time slots (i.e., continuous transmission):

- monitoring neighboring base stations would require an independent receiver
- the terminal will be more expensive than one slot terminals
- power consumption will be **much** higher

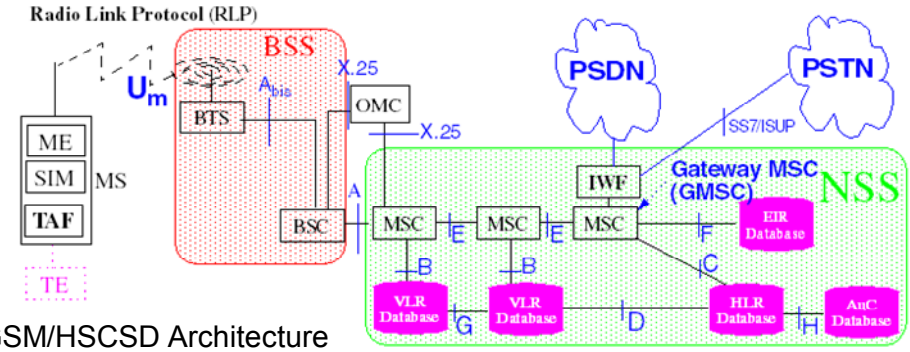
Multi-slot systems have required changes in: ciphering, frequency hopping, and generally radio resource management functions.

Nokia's Card Phone 2.0: HSCSD at up to 43.2 kbps (without data compression)

Slide 224

HSCSD depends on

- **Terminal Adaptation Function** (TAF)
- **Interworking Functions** (IWF)
- enhanced radio link protocol to handle multilink (aka multiple time slot) operation



GSM/HSCSD Architecture

Slide 225

General Packet Radio Service (GPRS)

GPRS features:

- True packet radio system - sharing network and air interface resources
- Volume based charging
- TCP/IP (Internet & Intranet) interworking, SMS over GPRS, (and X.25 interworking)
- Peak data rate from 9.05 kbps .. 171.2 kbps
  - bandwidth may be **asymmetric**, for example: 2 up/4 downlink channels
- Protocols designed for evolution of radio
  - Enhanced Data rates for Global Evolution (EDGE) - a new 3G GSM modulation scheme
  - Migration into 3rd Generation

Slide 226

GPRS nodes

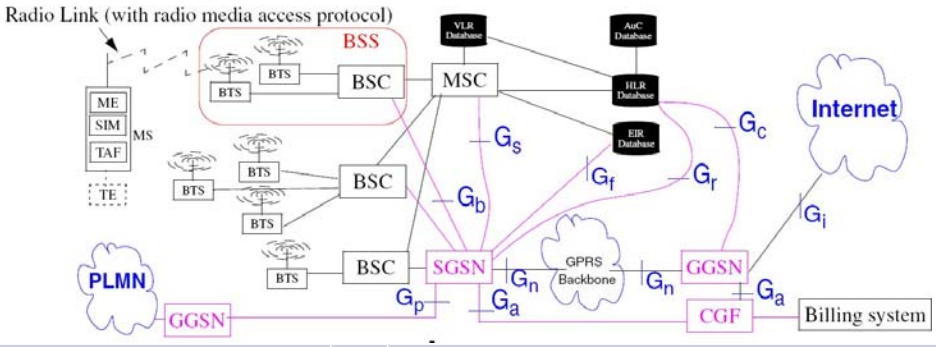
GPRS introduces new network elements:

- **Serving GPRS Support Node** (SGSN)
  authentication & authorization, GTP tunneling to GGSN, ciphering & compression, mobility management, session management, interaction with HLR,MSC/VLR, charging & statistics, as well as NMS interfaces.
- **Gateway GPRS Support Node** (GGSN)
  interfacing to external data networks (basically it is a network router) encapsulating data packets in GTP and forwarding them to right SGSN, routing mobile originated packets to right destination, filtering end user traffic, as well as collecting charging and statistical information of data network usage

GPRS is the result of committees trying to "adapt" Mobile IP to GSM systems.

Slide 227

GSM/GPRS Architecture and Interfaces



G_a	Charging data collection interface between a CDR transmitting unit (e.g. a SGSN or a GGSN)	G_i	reference point between GPRS and an external packet data network (G_i= **i**nternet)
G_b	between a SGSN and a BSS (Gb = **b**ase interface)	G_n	between two GSNs within the same PLMN (G_n = **n**ode)
G_c	between a GGSN and a HLR (Gc = **c**ontext)	G_p	between two GSNs in different PLMNs (Gp interface allows support of GPRS network services across areas served by the cooperating GPRS PLMNs.) (G_p = **P**LMN)
G_d	between a SMS-GMSC and a SGSN, and between a SMS-IWMSC and a SGSN (**not shown**)	G_r	between an SGSN and a HLR (G_r = **r**oaming)
G_f	between an SGSN and a EIR (Gf = **f**raud)	G_s	between a SGSN and a MSC/VLR

Maguire IK2555, Spring 2016 Slide 227

Slide 228

GPRS Coding Schemes

Initially four coding schemes (but only CS1 and CS2 are in early systems)

Coding Scheme	CS1	CS2	CS3	CS4
User Data Rate	9.05 kbps	13.4 kbps	15.6 kbps	21.4 kbps
Correction Capability	Highest			None
Worst-link Budget†	135 dB	133 dB	131 dB	128.5 dB
Maximum Cell Range	450 m	390 m	350 m	290 m
40 bytes (320 bits) of payload see [Mikkonen1999], pg. 33	1956 bits	1132 bits	1018 bits	625 bits
1500 bytes (12000 bits)	55787 bits	32490 bits	27218 bits	19345 bits

The real problem is that GPRS uses *interleaving* to spread the effect of burst errors
- but this means that the delay is always high! Some newer coding schemes try to reduce this delay.

† For comparison with GSM the worst-case link budget is 142.5 dB.

Maguire IK2555, Spring 2016 Slide 228

[Mikkonen1999] Jouni Mikkonen, “Quality of Services in Radio Access Networks”, Dr. Tech. dissertation, Tampere University of Technology, Department of Information Technology, 19 May 1999.

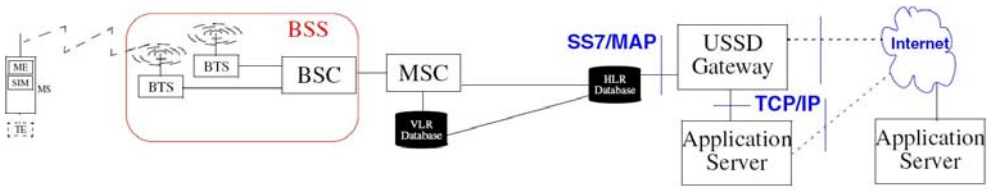
Slide 229

Unstructured Supplementary Service Data (USSD)

When MS can not recognize text - it simply passes it to the network as USSD. USSD supports all digits, asterisk (*), and punt/pound (#) keys. In the form:

(* | #) command_code (2-3 digits) {*parameter}* # total length
up to 200 ASCII characters

A USSD server (or gateway) is connected to the user's HLR via MAP and to servers (which actually provide a specific service) via TCP/IP. USSD is thought to be ~7x faster than SMS for two-way transactions (this is because USSD is session oriented as opposed to SMS's store-and-forward behavior).



Slide 230

USSD continued

Examples:

- set-up or cancel of services like call forwarding
- Swisscom's SIm Card Application Platform (SICAP) prepaid roaming platform†: users dial in a USSD string that includes the telephone number they want to call (e.g., *101*NUMBER#) this is sent to the SICAP platform at their (home) operator, who then connects them to the desired number by dialing them back!

In addition to passing the USSD message to the external application, the USSD Gateway passes:

- originating subscriber's MSISDN
- number of the HLR which handled the USSD
- originating subscriber's IMSI (optional)
- VLR Number (optional)

Disadvantage: USSD and SMS both use the same control channel

†Sold as "GSM Card easyRoam"

Slide 231

Short Message Service (SMS)

Short Message Service (SMS) offers connectionless (message) delivery (similar to "two-way-paging")

If the GSM telephone is not turned on, the message is held for later delivery. To Ensure that each time a message is delivered to an MS, the network expects to receive an acknowledgement from the MS that the message was correctly received.

- SMS supports messages up to 140 octets (160 characters of GSM default Alphabet - see GSM 03.38) in length.
- SMS concatenation - combines several messages
- SMS compression - defined standard for compression of content

With international roaming these messages can be delivered by any GSM network around the world to where the MS currently is.

Two types of messages: **cell broadcast** and **point-to-point service**

Slide 232

SMS message types

User-specific — message is to be display to the user

ME-specific — message is targeted at the mobile terminal itself

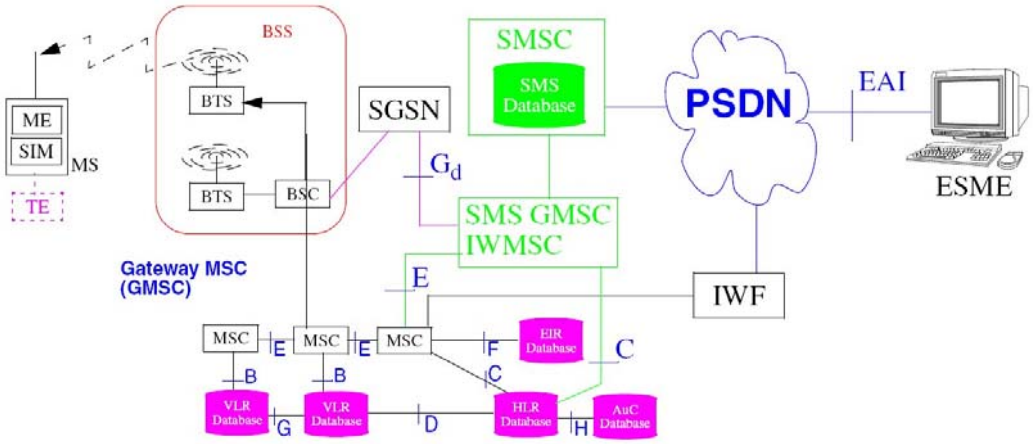
- playing a ring tone
- displaying a business card
- changing the default icon
- …

SIM-specific — message is targeted at the SIM card

- change the balance in a pre-paid card

Slide 233

Short Message Service Architecture



SMSC	Short Message Service Centre
SMS GMSC	SMS Gateway MSC
IWMSC	Interworking MSC
ESME	External Short Message Entities

Slide 234

SMSCs

- High reliability
- High availability
  - Logica's Picasso SMS Centre allows new hardware can be added within 60 seconds, with no service outage
- High performance
  - HP's (formerly Compaq's) AlphaServer™ ES45,over 8,000 SMS deliveries per second with CMG Wireless Data Solutions (formerly CMG Telecommunications) SMSC software [CMG]; note that they have merged with Logica plc forming: LogicaCMG
  - Logica's Picasso SMS Centre supports 1 to 128 nodes with automatic load sharing
- existing SMSCs talk TCP/IP as well as other protocols
- SMS brokers: buy SMS capacity in bulk, they receive your messages and then transfer them to operators that they have agreements with.
- As **each** SMS is charged for the resulting CDR volumes can be very high, e.g., Mannesmann has peak CDR rates as high as 2,500-3,000 CDRs per second ([Lloyd2000], pg. 13).
  - For a performance study of SMS and MMS centers see [Mahdavi2003].
  - William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta, "Exploiting Open Functionality in SMS Capable Cellular Networks" [Enck2005], describes a distributed denial of service via SMS

Maguire IK2555, Spring 2016 Slide 234

[CMG] CMG announces Third-Generation High-Performance SMS Centre: AlphaServer-based SMSC clocks unrivalled 8,000 sustained deliveries per second, Nieuwegein, the Netherlands, Feb. 19th 2001, formerly at http://h18000.www1.hp.com/products/software/in7/art4.html

[Lloyd2000] Glyn Lloyd , Phill Davies, and Andrew Beswick, "Short Messaging Service Centres (SMSCs) Uncovered: More Than Just Text!", Lehman Brothers, November 2000, Pub Codes: 01/07/43/2035, formerly at http://www.airslide.com/pdf/lehman.pdf

[Mahdavi2003] Adrian Mahdavi, "Value Added Services and Content Platforms", M. Sc. Thesis, KTH/IMIT, 25 June 2003. http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-93112

[Enck2005] William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta, "Exploiting Open Functionality in SMS Capable Cellular Networks", 12th ACM Conference on Computer and Communications Security (CCS'05),November 7-11, 2005, Alexandria, VA, USA http://www.smsanalysis.org/

Slide 235

Entering Short Messages

To improve the speed of entering SMSs (and other text):

- **Full keyboards** (such as Ericsson's Chat Board)
- **Onscreen keyboard** (such as Palm's on-screen keyboard)
- **Fitaly keyboard** - arranges letters based on their frequency and probability transitions in English
- **Predictive text input algorithms**
  - Tegic T9 - utilizes numeric keypad and probability to work out probably string e-acute's Octave keyboard
- **Handwriting recognition**
  - Word recognition, such as Psion's CalliGrapher
  - Character recognition, such as Palm's Graffiti and
  - CJKOS - an OS extension for Palm for Chinese, Japanese, and Korean
- **Speech recognition**

Maguire IK2555, Spring 2016 Slide 235

[Burkhardt2002] Jochen Burkhardt, Horst Henn, Stefan Hepper, Klaus Rintdoff, and Thomas Schäck, *Pervasive Computing: Technology and Architecture of Mobile Internet Applications*, Addison-Wesley, 2002, ISBN 0-201-72215-1

Slide 236

SMS shorthand

From “Get 2 grips with SMS-speak b4 it’s 2 L8 !”

afasik	as far as I know	<g>	grin	sc	stay cool
asap	as soon as possible	gr8	great	sol	sooner or later
atw	at the weekend	gsoh	good sense of humour	t+	think positive
awhfy	are we having fun yet?	h2cus	hope to see you soon	t2ul	talk to you later
b4	before	hak	hug and kisses	tuvm	thank you very much
bbfn	bye bye for now	ic	I see	w4u	waiting for you!
bcnu	be see in you	idk	I don’t know	wuwh	wish you were here
brb	be right back	idts	I don’t think so!	X!	Typical woman!
btw	by the way	iow	in other words	Y!	Typical man!
cm	call me	j4f	just for fun		
cu	see you	kc	keep cool		
cul8ter	see you later	khuf	know how you feel		
dk	don’t know	l8r	later		
dur?	do you remember	m8	mate		
e2eg	ear to ear grin	mtfbwu	may the force be with you		
eod	end of discussion	nc	no comment		
F?	Friends?	nwo	no way out		
F2F	Face to Face	o4u	only for you		
fya	for your amusement	O!ic	Oh, I see!		
fyi	for your information	ruok	are you okay?		

Maguire IK2555, Spring 2016 Slide 236

Slide 237

External Application Interface (EAI)

In order to enable non-mobile External Short Message Entities (ESME) to interface with an SMSC one of the following protocols (which all run over TCP/IP) is generally used:

Short Message Peer to Peer (SMPP)	open message-transfer protocol to enable SMPP V5.0 specification released 20 February 2003 [CMG] Initially defined by Logica - now SMSForum
CIMD2	Nokia's Computer Interface to Message Distribution 2 [Nokia]
EMI/UCP	Vodafone's description of CMG's Universal Computer Protocol[Vodafone]

Note:

- this avoids the earlier problem of the interface to the SMSC being closed;
- more and more operators seem to be converging on using SMPP.

[CMG] CMG announces Third-Generation High-Performance SMS Centre: AlphaServer-based SMSC clocks unrivalled 8,000
sustained deliveries per second, Nieuwegein, the Netherlands, Feb. 19th 2001, formerly at http://h18000.www1.hp.com/products/software/in7/art4.html

[Nokia] Nokia's Computer Interface to Message Distribution formerly at http://www.forum.nokia.com/main/1,6566,1_2_5_30,00.html

[Vodafone] Short Message Service Centre (SMSC) External Machine Interface (EMI) Description, Version 4.1, September 2003, formerly at http://www.vodafone.de/downloadarea/UCP-Protokoll_Emi4_1.pdf

Slide 238

SMS performance

See Ssection 1.1.2 of [Lin and Pang2005] for some statistics concerning time to deliver a SMS message and the probability that the mobile station is not available (hence the message can not be delivered).

Observe that Figure 1.7 of [Lin and Pang2005] showing the time to delivery and cumulative distribution function (CDF) of the time to delivery - clearly indicates that message delivery is rather slow - with more than a minute of time required to deliver 90% of the message and even after several minutes there are many messages which are not yet delivered (but which are still deliverable).

For some additional reading about SMS performance see [Mahdavi2003], [Samanta2005], and [Zerfos2006].

Maguire IK2555, Spring 2016 Slide 238

[Lin and Pang2005] Yi-Bing Lin and Ai-Chun Pang, Wireless and Mobile All-IP Networks, John Wiley & Sons; 2005, ISBN: 0-471-74922-2

[Mahdavi2003] Adrian Mahdavi, “Value Added Services and Content Platforms”, M. Sc. Thesis, KTH/IMIT, 25 June 2003. http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-93112

[Samanta2005] Vidyut Samanta, "A Study of Mobile Messaging Services", Master of Science thesis, Computer Science, University of California, Los Angeles, 2005 http://130.203.133.150/viewdoc/download?doi=10.1.1.216.5490&rep=rep1&type=pdf formerly at http://compilers.cs.ucla.edu/vids/thesis.pdf

[Zerfos2006] Petros Zerfos, Xiaoqiao Meng, Starsky H.Y Wong, Vidyut Samanta, and Songwu Lu,"A Study of the Short Message Service of a Nationwide Cellular Network", ACM IMC’06, October 25-27, 2006, Rio de Janeiro, Brazil.

Slide 239

Voice Messaging System (VMS)

A value-added service which redirects incoming calls (i.e., forwards them) to a voice mailbox when MS is turned off, low on battery, left unattended (after ringing for xx seconds) or temporarily out of coverage.

A **Voice Message Alert** (VMA) can be send (via SMS) to the MS to let the user know there is a waiting voice message.

Note that you can use SMS's "replace message" facility - to over-write last VMA - thus there will only be one message with the latest status voice messages (for example saying: "You have N voice messages waiting").

Slide 240

Voice Profile for Internet Mail (VPIM)

Voice Profile for Internet Mail (VPIM) Version 2 (RFC 2421 and RFC 3801) is an application of Internet Mail originally intended for sending voice messages between voice messaging systems

An alternative to VPIM: S. McRae and G. Parsons, 'Internet Voice Messaging (IVM)', *Internet Request for Comments*, vol. RFC 4239 (Proposed Standard), Nov. 2005 [Online]. Available: http://www.rfc-editor.org/rfc/rfc4239.txt

G. Vaudreuil and G. Parsons, 'Voice Profile for Internet Mail - version 2 (VPIMv2)', *Internet Request for Comments*, vol. RFC 3801 (Draft Standard), Jun. 2004 [Online]. Available: http://www.rfc-editor.org/rfc/rfc3801.txt

Slide 241

Enhanced Message Service (EMS)

Allows basic graphics, icons, and sounds to be incorporated in SMS messages. Based on concatenating (i.e., linking together a chain of) several SMS messages

Slide 242

Multimedia Messaging Service (MMS)

MMS Centre (MMSC) - a logical extension of an SMS Centre, but must cope with a larger variety of message types; in addition, it can convert message formats to suit the capabilities of the receiving terminal.

Four key functional elements:

- MMS Relay - engine which transcodes and delivers messages to mobile subscribers
- MMS Server - provides the store in the store-and-forward architecture
- MMS User Databases - user profiles, subscription data, …
- MMS User Agent - an application server which enables users to view, create, send, edit, delete, and manage their multimedia messages

An MMS presentation can utilize a synchronization language (e.g. **Synchronized Multimedia Integration Language** (SMIL)[Ayars2001]) for synchronized presentation.

In addition to store and forward, MMS also supports store and retrieve (via e-mail and web), but it was primarily designed as a person-to-person service.

R. Gellens, 'Mapping Between the Multimedia Messaging Service (MMS) and Internet Mail', *Internet Request for Comments*, vol. RFC 4356 (Proposed Standard), Jan. 2006 [Online]. Available: http://www.rfc-editor.org/rfc/rfc4356.txt

Maguire IK2555, Spring 2016 Slide 242

[Ayars2001] Jeff Ayars, Dick Bulterman, Aaron Cohen, Ken Day, Erik Hodge, Philipp Hoschka, Eric Hyche, Muriel Jourdan, Michelle Kim , Kenichi Kubota, Rob Lanphier, Nabil Layaïda, Thierry Michel, Debbie Newman, Jacco van Ossenbruggen, Lloyd Rutledge, Bridie Saccocio, Patrick Schmitz, Warner ten Kate (Editors), "Synchronized Multimedia Integration Language (SMIL 2.0)", W3C Recommendation, 07 August 2001 - *http://www.w3.org/TR/smil20/*

Open Mobile Alliance, Multimedia Messaging Service V1.3, http://technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases/mms-v1-3

Slide 243

SMS over GPRS

Can send SMS over GPRS - thus avoiding the problem of SMS utilizing the GSM control channel

However, if users send their messages directly via an messaging application or via e-mail -- this could take a lot of revenue away from the operators (as SMS and MMS have a high premium over the cost of simply transferring the bits).

Slide 244

International Roaming

GSM's roaming feature allows a user to make and receive calls in **any** GSM network and to use the same user-specific services worldwide, but this requires a **roaming agreement between the *individual* operators**.

Good news	With worldwide roaming the MS is accessible via the same phone number everywhere!
Bad news	It could be very expensive - much more expensive than you think!

The basic problem is that when you roam to another network (for example, in another country) - your Mobile Station ISDN number (MSISDN) *still looks like it is in your home network*.

Worse: If you are in the same (non-home) network as the person you are calling, this results in two international calls! This is due to tromboning. For four solutions see section 13.2 of [Lin and Chlamtac2001], pages 242-249.

Maguire IK2555, Spring 2016 Slide 244

[Lin and Chlamtac2001] Yi-Bing Lin and Imrich Chlamtac, *Wireless and Mobile Network Architectures*, Chapter 13, pages 239-250 in
Yi-Bing Lin and Imrich Chlamtac, *Wireless and Mobile Network Architectures*, John Wiley & Sons, 2001, ISBN 0-471-39492-0.

Slide 245

Using IP backbone with GSM Roaming

Hamid Shahzad and Nishant Jain's Master's Thesis entitled: "Internet Protocol based Mobile Radio Access Network Architecture for Remote Service Areas" [Shahzad and Jain2007].

They describe a packet optimized IP- GSM Radio Access Network (GRAN) architecture that uses the Internet Protocol (IP) for communications between Base Transceiver Stations (BTS), Base Station Controllers (BSC), and the Network Switching Subsystem (NSS) -- located in a remote (and potentially mobile: ships, planes, etc.) area.

Maguire IK2555, Spring 2016 Slide 245

[Shahzad and Jain2007] Hamid Shahzad and Nishant Jain, "Internet Protocol based Mobile Radio Access Network Architecture for Remote Service Areas", Masters Thesis, Department of Communication Systems, Royal Institute of Technology, October 2007 http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-91940

Slide 246

Enhanced Data Rates for GSM Evolution (EDGE)

- enhanced modulation technique designed to increase network capacity and data rates in GSM networks
- provide data rates up to 384 Kbps.
- EDGE lets operators without a 3G license compete with 3G networks (since the data rates are comparable in the wide area)

GSM/EDGE Radio Access network (GERAN)

The radio interface used in Enhanced Data Rates for GSM Evolution (EDGE)

Slide 247

EGRPS

EGPRS = EDGE -- an extension/enhancement of GPRS including 4 new Data Packet Traffic Channels using 8-PSK modulation and a incremental redundancy mechanism extended to the GMSK based data packet traffic channels.

- Support for simultaneous, multiple radio access bearers with different QoS profiles.
- New bearer classes:

Conversational Class	Voice & video conferencing where small delay is required
Streaming Class	Capable of processing as transfer is taking place, needs somewhat constant delay and throughput
Interactive Class	on-line applications
Background Class	Delay insensitive but requires few errors (may require multiple re-transmissions to hide errors)

Slide 248

Operation/Administration/Maintenance

Operation/Administration/Maintenance (OA&M) follows ITU-T's Telecommunications Management Network (TMN) model, which has several components:

Operations system (OS)	OS uses Operating System Function (OSF) to provide overall management, billing, account, management of mobile equipment, HLR measurement, …
Network Element Functions (NEFs)	provides monitoring and control of network elements: HLR, VLR, AuC, EIR, MSC, BSC, and BTS
Data Communication Network	OS, NEs, and other TMN elements via Data Communication Function (DCF)
Mediation device (MD)	adapts the OS to a specific network element
Q-Adapter (QA)	uses Q-adapter function to adapt non-TMN equipment
Workstation (WS)	OA&M personnel interact with OS via Workstation functions (WSFs)

I personally find this ITU-T speak! But you have to talk the talk to walk the walk!

Maguire IK2555, Spring 2016 Slide 248

Slide 249

Further reading

Sudeep Kumar Palat, "Replication of User Mobility Profiles for Location Management in Mobile Networks", Dr. Ing. dissertation, Norwegian University of Science and Technology, Dept. of Telematics, 12 Jan. 1998.

GSM

M. Mouly and MB Paulet, *The GSM System for Mobile Communications*, Mouly and Paulet, 1992

M. Mouly and MB Paulet, Current evolution of the GSM systems, IEEE Personal Communications, vol. 2, no. 5, pp. 9-19, 1995.

David J. Goodman, *Wireless Personal Communications Systems*, Chapter 7, GSM: Pan-European Digital Cellular System, Addison-Wesley, 1997, ISBN 0-201-63470-8

Marc Kahabka, GSM Pocket Guide revised version Vol. 2, Acterna Eningen GmbH, 72795 Eningen u. A., Germany

Petri Jarske, The GSM System, Principles of Digital Mobile Communication Systems, 2001 edition, Technical University Tampere, Finland formerly at http://www.cs.tut.fi/kurssit/83150/DigiCom2001.PDF

GSM security
http://www.isaac.cs.berkeley.edu/isaac/gsm.html

Mobile Application Part (MAP) ETSI R10 ETSI 08/96, CAA 201 45 - was at http://www.ericsson.com/signaling/cards/map_etsi.shtml

Slide 250

GPRS

Jari Hämäläinen, "Design of GSM High Speed Data Services", Dr. Tech. dissertation, Tampere University of Technology, Department of Information Technology, 4 October 1996.

Don Zelmer, "GPRS, EDGE, & GERAN: Improving the performance of GSM & TDMA Wireless by Packet Capabilities", Cingular Wireless LLC, SUPERCOMM 2001, Atlanta, Georgia, Wednesday, June 6, 2001 formerly at

http://www.atis.org/atis/Pictures/Supercomm01/Presentationfolder/T1P1zelmer3Gtemplate2.PDF

"Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface", GSM 11.14, Version 5.2.0, December 1996 http://www.ttfn.net/techno/smartcards/GSM11-14V5-2-0.pdf

Slide 251

USSD

GSM 02.90: USSD Stage 1 -- only one way communication

GSM 03.90: USSD Stage 2 -- allows two way communication

SMS and Multimedia Messaging Service (MMS)

SMS Forum - formerly at http://smsforum.net/

Palowireless's SMS, EMS and MMS tutorials, (accessed 2003.03.12)
http://www.palowireless.com/sms/tutorials.asp

Gustav Söderström, "Virtual networks in the cellular domain", M. Sc. Thesis, KTH/IMIT, January 2003 -
http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-93117

Logica, "The essential guide to Multimedia Messaging", (accessed 2003.03.12) formerly at
http://www.logica.com/pdf/telecom/Mmsguide.pdf

Operation/Administration/Maintenance

Yi-Bing Lin and Imrich Chlamtac, *Wireless and Mobile Network Architectures*, **Chapter 14**, pp. 252-26

Slide 252

¿Questions?

Slide 253: Lecture 4: Number portability, VoIP, Prepaid, Location Based Services

IK2555: Mobile and Wireless Network Architectures: Lecture 4

prof. Gerald Q. Maguire Jr. http://people.kth.se/~maguire/

School of Information and Communication Technology (ICT), KTH Royal Institute of Technology

IK2555 Spring 2016 2016.01.08 © 2016 G. Q. Maguire Jr. All rights reserved.

Slide 254

4. Number portability, VoIP, Prepaid, Location Based Services

Lecture notes of G. Q. Maguire Jr.

For use in conjunction with Yi-Bing Lin and Ai-Chun Pang, *Wireless and Mobile All-IP Networks*, John Wiley & Sons; 2005, ISBN: 0-471-74922-2.

Slide 255

Database lookups

Local Number Portability (LNP)

Local Number Portability required by the Telecommunications Act of 1996 and a July 1996 order of the Federal Communications Commission (FCC) - similar requirements in Sweden and elsewhere.

LNP (as defined by the FCC): "the ability of users of telecommunications services to retain, at the same location, existing telecommunications numbers without impairment of quality, reliability, or convenience when switching from one telecommunications carrier to another."

LNP implies efficient call-routing must **not be based** on a **physical** location, but rather a **logical routing scheme** for how and where to route a call.

Verizon's cost recovery for providing LNP amounts to US$13.80/line over a 5 year period! In Denmark, donor operator charges the recipient operator a fee of DKK 72 (~9.6€) excl. VAT for the coverage of one-time administrative costs related to the porting of a single subscriber number.

Slide 256

Three kinds of Local Number Portability

- **Service Provider Portability**: subscriber can move to an new provider without a change in number (current requirement)
- **Location** (or **Geographic**) **Portability** (GNP): subscriber can move to a new location/geographic area (future requirement)
- **Service Portability**: if the service (mix) which the subscriber has is not available in their new local exchange, then connect them to where the services are available (future requirement)

Slide 257

Mobile Number Portability (MNP)

Requirement that any mobile (e.g., GSM) subscriber be able to move to a new **operator** or **service provider** and keep the same number (MSISDN)

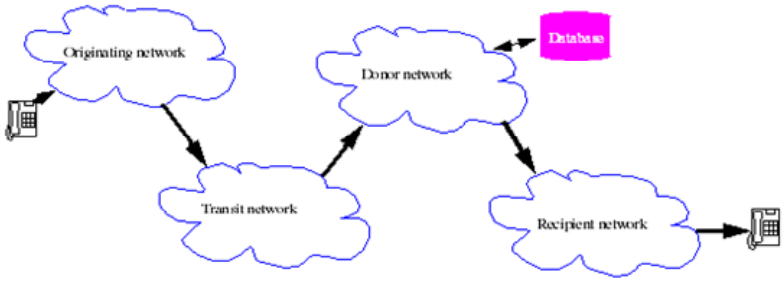
Slide 258

Non-geographic number portability (NGNP)

Numbers (typically) associated with a **service** rather than a **geographic destination**, e.g., freephone, low rate calling numbers, premium rate numbers; requires that the service provider can be changed without a change of number; these all require DB lookup

Slide 259

Call forwarding at donor end

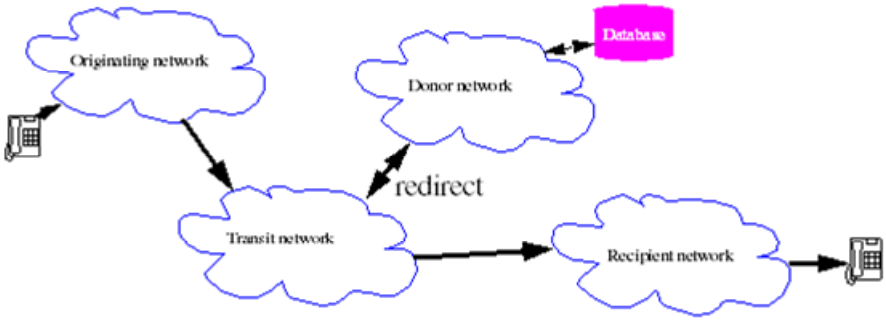


Donor = service provider whom the number is initially associate with

- inefficient in terms of call setup delays and usage of transmission capacity
- can not easily cope with numbers ported more than once, and
- the donor network continues to control first and subsequent portings.

Slide 260

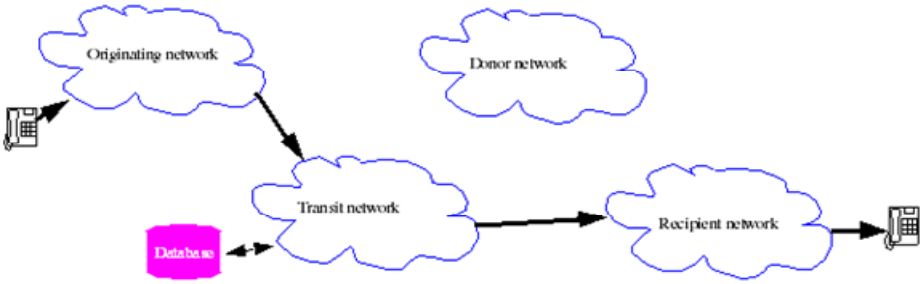
Drop back forwarding



- transit network gets a **redirect** from the donor network, it may be able to pass this all the way back to the originating network (i.e., dropping back through each of the networks to the originating network)
- makes better use of transmission capacity and can handle multiple portings
- the donor network continues to control first and subsequent portings.

Slide 261

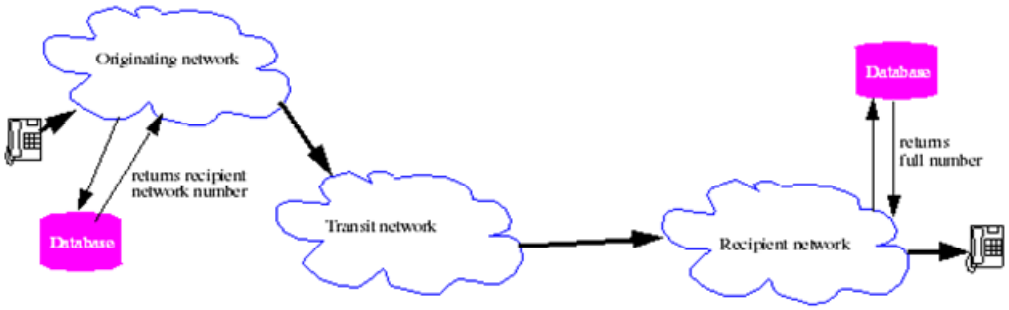
Query on release (QoR) solutions



- Donor network realizes the number has been ported out and sends an **ISUP release** or it might not know anything about this number (i.e., not it its DB any longer) ⇒ releases the call
- Release causes an intermediate point to query a portability database and to redirect the call.
- If the forward signalling indicates that preceding networks have QoR capability, then the release goes all the way to the originating network, which does the DB lookup and reroutes the call to recipient network.

Slide 262

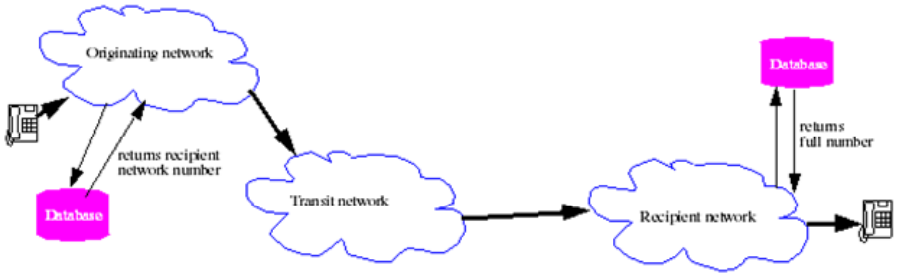
Look up type solutions



- portability database is checked for **all** calls, if the number has been ported, the new number is obtained and the call rerouted (done at first **first exchange** in a network that can access a **portability database**)
- solution is often implemented in North America via modified Signaling Transfer Points (STPs) which can check and translate ported numbers by modifying call setup information
- the donor network now has **no** role, multiple portings easy; but requires lookup of **all** numbers

Slide 263

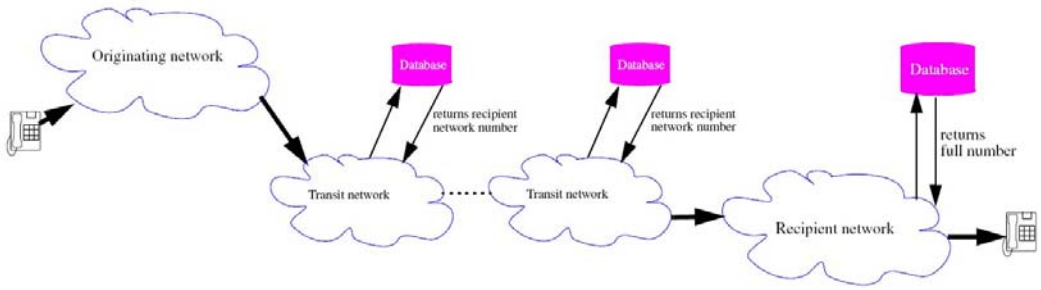
Two stage solutions



- Originating network simply learns the recipient network's number (called a **Logical Routing Number** (LRN), in North America this is a unique 10 digit number for the exchange)
- Recipient network does a second lookup to determine where to deliver the call within their network
- increases the privacy (since the originating network does not learn about the recipient network numbering)

Slide 264

All call/all network solutions



- each network does a lookup, but simply learns the "next" **network's** number
- final recipient network does a second lookup to determine where to deliver the call within their network
- increases the privacy -- since all networks along the path only learn about the "next" network

Who knows the mappings?

Slide 265

Who knows the mappings?

For North America the **Number Portability Administration Center** (NPAC) has **all** the mappings and passes then to the operator's **Local Service Management System** (LSMS) [NPAC].

See also Neustar Number Pool Administration http://www.nationalpooling.com/

Swedish Number Portability Administrative Centre AB (SNPAC) officially appointed as the single operator of the Swedish **Central Reference Database [**SNPAC**]**; interaction follows ITS standard SS 63 63 91 [SS636391].

see also regional numbering plan administrators:

- North American Numbering Plan (NANP) http://www.nanpa.com/ (also performed by NeuStar Inc.)
- …

Maguire IK2555, Spring 2016 Slide 265

[NPAC] North American Number Portability Administration Center (NPAC) (http://www.npac.com)

[SNPAC] Swedish Number Portability Administrative Centre AB http://www.snpac.se/

[SS636391] Number portability in Sweden: Administrative process for number portability, including the administrative interface and the central reference database (Nummerportabilitet i Sverige Administrativa rutiner för nummerportabilitet inkluderande administrativa gränssnitt och central referensdatabas), Swedish Standard SS 63 63 91, 2000-03-14, http://www.its.se/ITS/ss6363x/SS636391-ed2.pdf

[SS636392] Number Portability in Sweden - Network solutions for Service Provider Portability for public digital mobile telephony services, Swedish Standard SS 63 63 92, 2000-03-14, http://www.its.se/ITS/ss6363x/SS636392-ed1.pdf

Slide 266

Nummerportabilitet i Sverige

- Europaparlamentets och rådets direktiv 98/61/EG om nummerportabilitet
- Sverige ändringar i telelagen (1993:597) 1 juli 1999
- Post- och telestyrelsen (PTS) om nummerportabilitet (PTSFS 1999:3 och PTSFS 2000:6).
- PTS beslut 15 augusti 2001 (ärende nr. 01-19102):

Swedish Number Portability Administrative Centre AB
(SNPAC) Peter Myndes Backe 12
118 46 Stockholm
(organisationsnr. 556595-2925)
formerly at http://www.pts.se/Archive/Documents/SE/Beslut for SNPAC.pdf

PTS recommended **All Call Query** (ACQ) as the preferred routing method for Swedish telecommunications networks [Röding], this means that the originating operator will do a lookup of the number to route every call.

Maguire IK2555, Spring 2016 Slide 266

[Röding] Olle Röding, "Number Portability in Sweden: A project summary", YABSA Informatik AB, Saltsjöbaden, Sweden - formerly at http://www.hif.hu/menu6/m6_3/pdf_p/13w5%20yabsa.pdf, the author was responsible for:

- "Principal design and specification of the Central Reference Database for number portability in Sweden"
- "Development & definition of business model and operational model for SNPAC AB", …

Slide 267

EU Document 398L0061

[13.20.60 - Information technology, telecommunications and data-processing] [13.10.30.20 - Research sectors]

Instruments amended: 397L0033 (Modification)

398L0061: Directive 98/61/EC of the European Parliament and of the Council of 24 September 1998 amending Directive 97/33/EC with regard to operator number portability and carrier pre-selection

Official Journal L 268 , 03/10/1998 p. 0037 – 0038

http://www.icp.pt/streaming/98.61.EC.pdf?categoryId=59431&contentId=94157&field=ATTACHED_FILE

Slide 268

Lookup engines

Aeroflex UTMC LNP-Engine (cPCI or PCI board) [no longer UTMC]:

- Stores up to 160 million 16-digit phone number pairs
- Supports 100k lookups/sec. and 10K updates/second

Based upon two Content Addressable Memory Engines:

- custom 100 MHz chip
- lookup in as little as 100 nanoseconds
- partitions memory into up to 8,192 tables, from 256 to 30 million records
- programmable key widths (per table): from 1 to 32 bytes
- programmable association widths (per table) up to 8 megabytes
- performs exact matches, as well as hierarchical, longest-prefix, and proximity matches
- pipelined operation with separate I/O FIFOs
- bulk table load, unload, and count functions
- handles table overflows

There has been lots of efforts to speed up such lookups, see for example [Basso2006]

Maguire IK2555, Spring 2016 Slide 268

[Basso2006] Claude Basso, Jean L. Calvignac, Gordon T. Davis, and Piyush C. Patel, 'Longest prefix match lookup using hash function', US 7089240 B2, 08-Aug-2006.

Slide 269

Routing

Number portability can complicate routing, since you can not base the routing decision on the prefix - but actually have to do a lookup.

Note: There are efforts to introduce global number portability, see: RFC 3482: Number Portability in the Global Switched Telephone Network (GSTN): An Overview[Foster2003]

This RFC discusses how routing prefixes can be used to route a call from one operator to another.

[Foster2003] M. Foster, T. McGarry, and J. Yu, "Number Portability in the Global Switched Telephone Network (GSTN): An Overview", Internet Request for Comments, vol. RFC 3482 (Informational), February 2003, Available at http://www.rfc-editor.org/rfc/rfc3482.txt

Slide 270

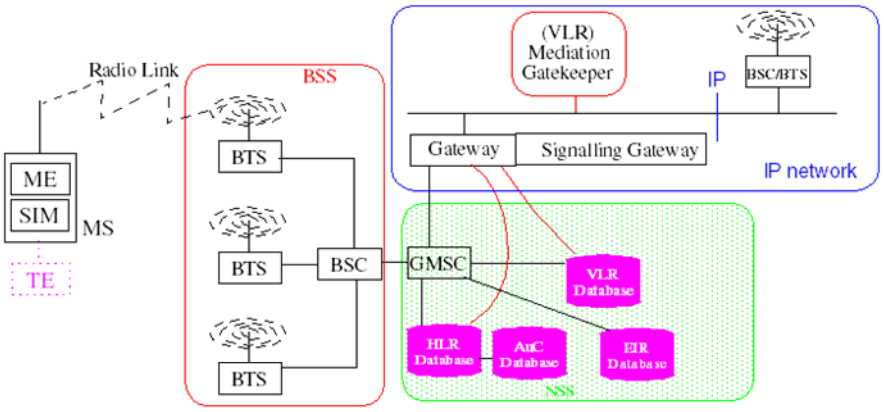
Voice over IP (VoIP)

Integrating VoIP with mobile telephony - see also the course IK2554: Practical Voice Over IP (VoIP): SIP and related protocols
https://www.kth.se/social/course/IK2554/

Slide 271

TIPHON

ETSI's Telecom. and Internet Protocol Harmonization over Network (TIPHON)

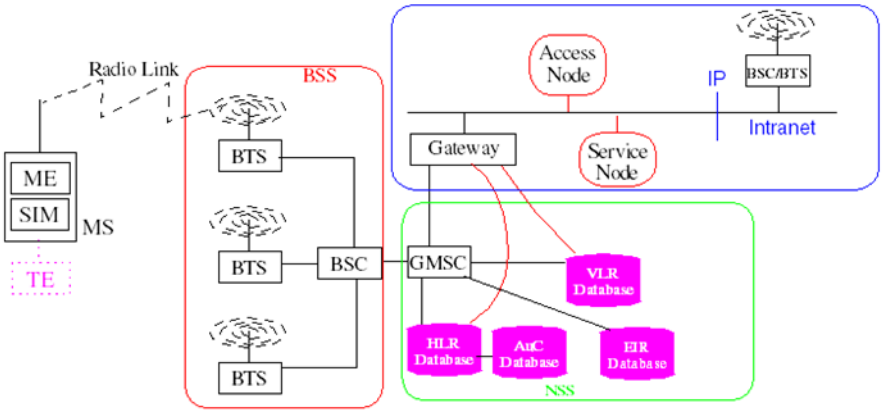


As of 24 September 2003 ETSI combined Services and Protocols for Advanced Networks on fixed network standardization and TIPHON on Voice over IP (VoIP) based networks into one committee, named TISPAN.

Slide 272

Ericsson's GSM on the Net

Olle Granberg, "GSM on the Net", Ericsson Review No. 04, 1998 †



†formerly available from
http://www.ericsson.com/about/publications/review/1998_04/files/1998046.pdf

Slide 273

Prepaid

Customer pays **before** using service.

Advantages:

- operator has the money - all up front (no risk & they can earn interest on it)
- operator saves: no need for: credit checking, invoices, collections, …
- customer: no need for credit worthiness, no need for a contract, immediate service, anonymous service is possible
- since for many cultures and countries there is no tradition or infrastructure for post-paid service - business is strictly cash up front -- prepaid fits well with the expectation of these customers
- prepaid value can be installed in devices (such as toys, jewelry, …)
- many customers will never use up all their balance - it will simply be abandon -- much to the delight of the operator {It is "like printing money"! see: http://en.wikipedia.org/wiki/Seigniorage }

Slide 274

GSM Prepaid

Prepaid credit is either kept in the SIM card or in the network.

When the balance is zero, customer can only receive calls. {this may be limited by the operator}

To refill:

- customer buys a refill/top-up card with a secret code
- dials a freephone number to an Interactive Voice Response server
- enters MSISDN number of their phone + secret code
- system verifies secret code (so code can only be used once), then refills the account

Prepaid comprises 81% of the Latin Americas mobile subscriptions - so it is very important in practice.[Pearson and Rojas2003]

Maguire IK2555, Spring 2016 Slide 274

[Pearson and Rojas2003] Chris Pearson and Erasmo Rojas, Wireless Trends in the Americas: The Proliferation of GSM 850 MHz and EDGE, A press release from
3G Americas, November 2003, formerly at
http://www.3gamericas.org/PDFs/EDGE-GSM850_Nov03_English.pdf

Slide 275

Difference between Mobile and Fixed Prepaid

Mobile servers needs:

- more complex billing system due to more complex **tariffs** (which can be location dependent!)
- more complex billing system due to more complex **taxation** (which can be location dependent!)
- real-time usage metering - which has to cut off service when balance is zero (there is a trade off between accuracy and cost of implementation - if the operator is willing to take some loss, the implementation can relax the real-time constraints)
- increased complexity of customer care: warning customer to refill in a timely fashion (maintaining a credit balance - maintains cash at the operator!)

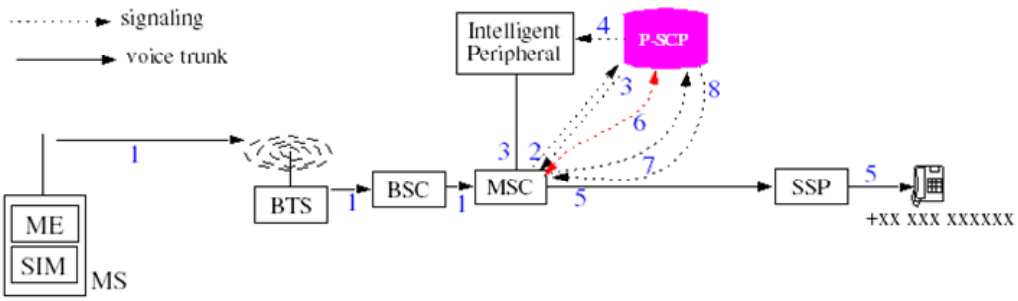
Slide 276

Four alternatives for Mobile Prepaid

- **Wireless Intelligent Network** (WIN)
- Service Node
- Hot Billing
- Handset-Based

Slide 277

Wireless Intelligent Network (WIN)



WIN Prepaid call origination

1. Prepaid mobile customer calls +xx xxx xxxxxx
2. MSC gets WIN call setup trigger, call setup suspended, message sent to Prepaid Service Control Point (P-SCP)
3. P-SCP instructs MSC to set up ISDN (voice) link to intelligent peripheral
4. P-SCP instructs intelligent peripheral to provide **account status notification** (balance, charging rate, …) for this call
5. P-SCP starts countdown timer & instructs MSC to resume call processing -- which connects the call
6. Call terminates: either (a) countdown timer expires (P-SCP instructs MSC to terminate call) or (b) call completes
7. MSC gets WIN call release trigger, sends disconnect message to P-SCP indicating duration of call
8. P-SCP rates the call (computes charges) and debits the prepaid balance, sends current balance and cost of call to MSC

Maguire IK2555, Spring 2016 Slide 277

Slide 278

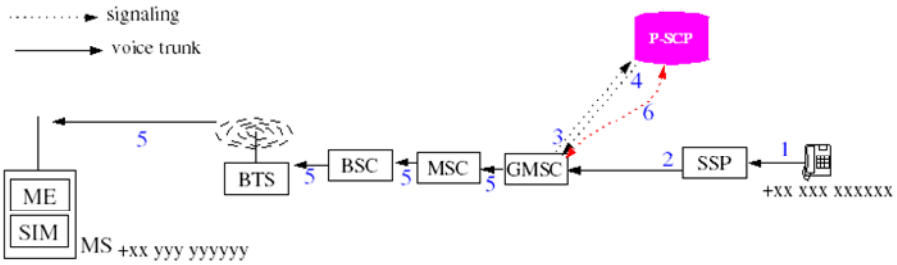
Calling party pays versus Called party pays

Calling party pays style billing - Europe, Taiwan

Called party pays style billing - US (where mobile subscriber pays for ***both*** incoming and outgoing calls)

Slide 279

WIN Call termination when called party pays

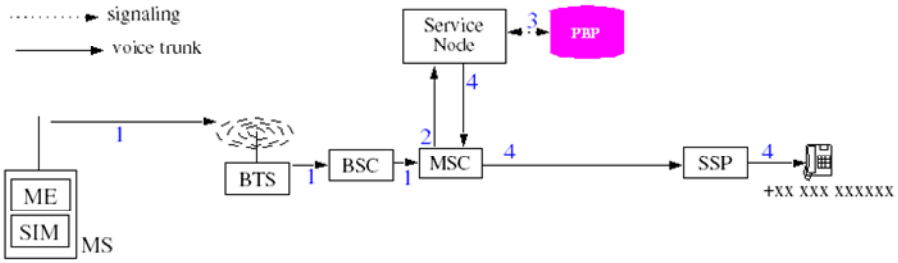


WIN Prepaid call termination

1. Caller dials prepaid mobile customer +xx yyy yyyyyy
2. Call forwarded to gateway GMSC
3. GMSC get a WIN call setup trigger, suspends call processing, sends message to P-SCP
4. P-SCP determines if mobile is allowed to receive this call, if so instructs GMSC to resume call setup procedure
5. GMSC connects the call
6. P-SCP monitors called party's balance and can terminate the call if there is no credit (just as per call origination case)

Slide 280

Service Node



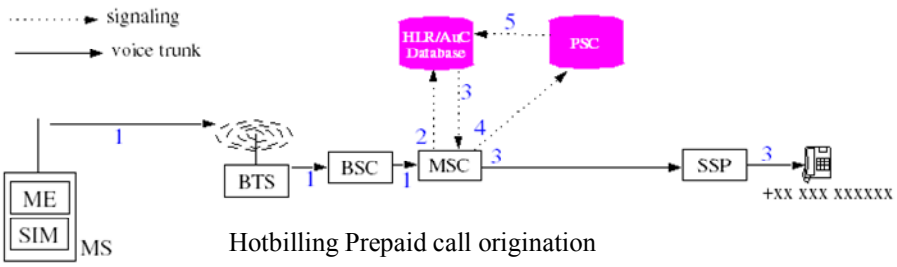
Service Node Prepaid call origination

1. Prepaid mobile dials called party (+xx xxx xxxxxx)
2. MSC detects this is a prepaid customer and sets up trunk to service node
3. Service node consults Prepaid Billing Platform (PBP) to determine if the call should be allowed
4. If so, then a 2nd trunk is setup from the service node via the MSC to the called party

Note: at the cost of the 2nd trunk (and two ports of MSC), this is a very easy service to build - since the MSC does not actually know about the prepaid service - only that it is to connect calls from these customers to the service node.

Slide 281

Hot Billing



Hotbilling Prepaid call origination

1. Prepaid mobile dials called party (+xx xxx xxxxxx) and sends their own IMSI
2. Based on IMSI, MSC asks HLR/AuC if this is a valid service request
3. If verified, HLR/AuC sends customer data and a prepaid tag to MSC, MSC connects call
4. When call terminates, a Call Detail Record (CDR) is sent to the Prepaid Service Center (PSC)
5. PSC debits the account, if the account is out of funds it notified the HLR/AuC to suspend service!

With hot billing the operator is taking a risk (of the cost of the call exceeding the balance), but it is a "**one-call exposure**" and reduces the complexity of the system.

Maguire IK2555, Spring 2016 Slide 281

Slide 282

“one-call exposure” in depth

Since the operator may have no idea of who this customer is, they have no way of collecting on the “bad debt”, thus they try to avoid it:

- Use large values for the initial payment and refill/top-up - thus the account has quite a ways to go before it is depleted (i.e., no low value prepayments)
- prohibit call forwarding to prepaid accounts (since otherwise you could simultaneously forward lots of calls through a given prepaid account at one time and “one-call” suddenly becomes “N-calls”!)
- increase the interval at which CDRs are sent for processing {but this costs in increased load on the PSC} -- in fact the trend is towards the opposite, send bunches of CDRs are one time rather than in “real-time” as calls end {this decreases load on PSC, but increases bad debt exposure} -- in the end it is a business decision of risk/reward

Slide 283

Handset-Based

Uses GSM Phase 2, Advice of Charge (AoC):

- Advice of Charge Charging (AoCC) this is how you debit the balance in the SIM card
- Advice of Charge Information (AoCI)

Builds upon sever SIM data fields:

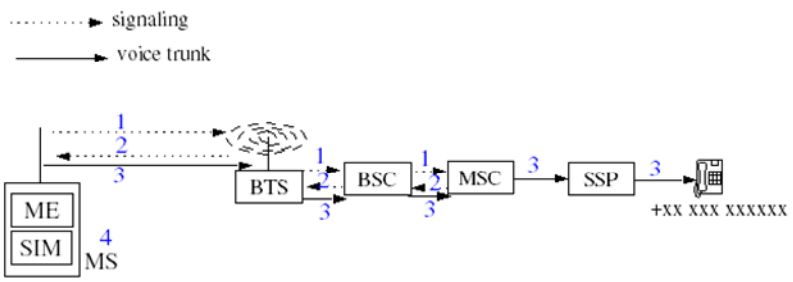
- accumulated call meter (ACM)
- accumulated call meter maximum (ACM*)
- price per unit and currency table (PUCT)

Prepaid service center (PSC) uses SMS messages to execute program in the handset, these applications are controlled by the SIM Toolkit.

- Different sized SIM cards may be needed if large tariff rate tables or complex rating schemes are to be used.
- ACM and ACM* are generally user accessible (via PIN2), but for prepaid cards this access is disabled (either at time of manufacture or via an SMS message when users subscribes to prepaid service).

Slide 284

Handset-Based Prepaid call origination



Prepaid mobile dials called party (+xx xxx xxxxxx)

1. Based on rate plan (+ destination, time/date), MSC sends AoC e-parameters (including ACM and ACM*) to mobile
2. If mobile support AoCC, it ACKs receipt of e-parameters; if MSC gets this ACK, call is connected, otherwise call is denied
3. During call MS uses AoC e-parameters for tariff info; locally decrements credit by incrementing ACM. When ACM reaches ACM*, MS terminates call and informs MSC of call release

Slide 285

Combined Handset-based + Hot Billing

For fraud reduction, Handset-based approach can be combined with the Hot billing approach - thus if PSC thinks there is no credit but SIM claims credit, the PSC can inform operator to: terminate service and/or trigger fraud investigation.

Unfortunately, the disagreement might be legitimate due to poor synchronization (of charging information) between PSC and MS.

Slide 286

Roaming and Prepaid

Lots of problems:

- cannot easily use special MSISDN numbers as this would:
  - prevent operator number portability
  - service portability is not allowed, since you could not change to post paid without changing MSISDN
  - could use IMSI, but this might require software change at visited system
- prepaid charging might not be performed at visited system (because it uses a different prepaid scheme than home system)
  - therefore route the call via the home system - letting it implement the prepaid debiting
  - but this requires a trunk to the home system (⇒ higher charge for a specific prepaid call than a postpaid call) -- this may be too expensive for international roaming
- scalability problems with service node approach (since you use up two MSC ports per call)
- AoC traffic is not encrypted - so the handset can just tamper with or ignore debit commands! ⇒ manufactures working on SIM encryption
- handset-based approach may lock operator to a SIM supplier
- some of the schemes have a high setup cost

Slide 287

Revenue and new services

Carriers generally think in terms of Average Revenues Per User (**ARPU**).

ARPU is defined (by TeliaSonera) as total sales during the period, divided by the average number of subscribers, divided by the number of months in that period.

For example, TeliaSonera Q4 2003 ARPU and MoU figures from [TeliaSonera2004]:

	Customers	ARPU			Minutes of Use (MoU)		
		Prepaid	Post-paid	Avg.	Prepaid	Post-paid	Avg.
Sweden	3,838,000	94 SEK	452 SEK	268 SEK†	56	209	129
Finland	2,428,000			41€‡			164
Norway	1,195,000	129 NOK	560 NOK	351 NOK§	60	267	167

† 227 SEK in 2004 (from TeliaSonera's Annual report for 2004), 179 SEK (Q3 2009) (TeliaSonera Operational data Q3 2009 Excel spreadsheet), ‡ 38€ in 2004, § 339 NOK in 2004

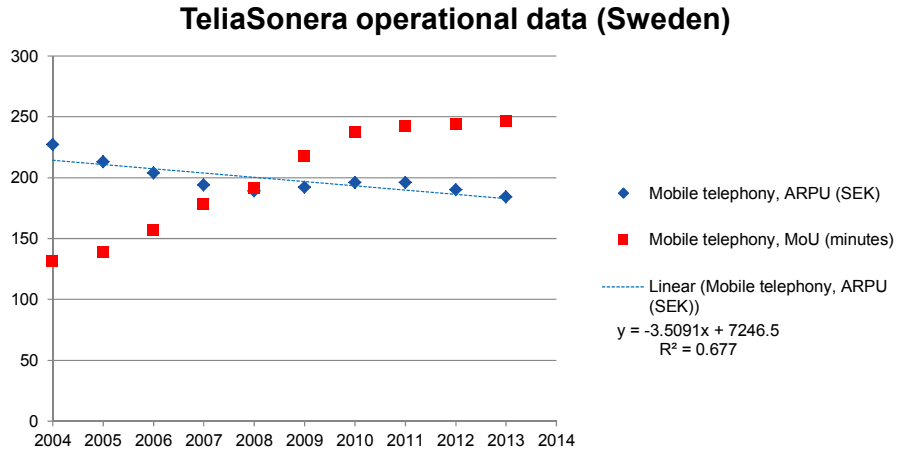
With time and competition ARPU generally **decreases**, hence the pressure to introduce new services which have a higher margin.

Maguire IK2555, Spring 2016 Slide 287

[TeliaSonera2004] TeliaSonera, Year-End Report 2003: Appendix for the telephone conference, February 11, 2004. Formerly at http://www.telia.net/Koncernwebb/Attachment/20040211/Q42003BackupSlidesExternal.ppt

Slide 288

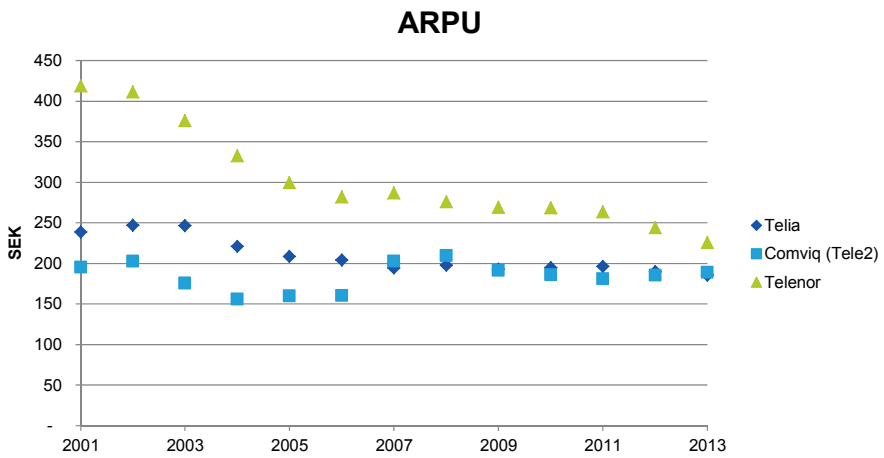
Eroding ARPU – growing traffic per user per month



TeliaSonera's 2013 Annual Report
http://annualreports.teliasonera.com/global/2013/annual%20report/downloads_finala%20pdf/teliasonera_ar2013_eng.pdf

Slide 289

ARPU for three Swedish operators



Data from http://www.cmcrp.org/wp-content/uploads/2013/11/ARPU-by-Firm-and-Country.xlsx

Slide 290

Location Based Services (LBS)

As we have seen it is possible to locate where a user is to within a cell, but it is also possible to refine this positioning via the infrastructure or via other means such as GPS. Popular uses of LBS include:

- Navigation applications
- Location based information
  - Enabling services such as - Where is the nearest X? where X can be gas station, hospital, restaurant, … different responses depending on where you are when you ask for the information
- Location sensitive billing
  - see for example "Virtual enterprise networks" on page 379
- Emergency services
  - US FCC's Wireless E911 Phase II Automatic Location Identification - requires wireless carriers, to provide more precise location information to PSAPs, specifically, the latitude and longitude of the caller to an accuracy of 50-300 meters (depending on the type of technology used).
- Tracking
  - fleet vehicles (such as taxis, service trucks, …)

For an introduction to LBS see [Hjelm2002].

Maguire IK2555, Spring 2016 Slide 290

[Hjelm2002] Johan Hjelm, *Creating Location Services for the Wireless Web*, John Wiley & Sons, 2002, ISBN: 0471402613

Slide 291

Means of determining location

- Passive
  - **Cell identity**
    - especially useful if you have a table of where the cells are
    - completely passive - you just listen to the broadcast of the Cell ID, WLAN AP beacons, etc.
  - Based on **satellite navigation systems**: Global Positioning System (GPS), GLOSNASS, Galileo, …
    - must listen for sufficient data from multiple satellite
- Active
  - Based on **timing**
    - Timing Advance (distance from basestation estimated by the timing advance value)
  - Based on **timing and triangulation**
    - Time of Arrival (TOA)
    - Time Difference of Arrival (TDOA)
    - Enhanced Observed Time Difference (EOTD)
    - Angle of Arrival (AOA)
- Mixed
  - **Assisted GPS** (A-GPS), assisted-x

Slide 292

Geographic Location/Privacy (geopriv)

IETF RFC 3693: "Geopriv requirements", sets out a number of requirements necessary preserve geographic location privacy [Cuellar2004].

The RFC details authorization, security and privacy† requirements for the Geopriv Location Object (LO) and for the protocols that use this Location Object. The LO is used to securely transfer location data.

Additional working drafts:

- Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information [Polk2004]
- DHCP Option for Civil Addresses [Schulzrinne2006]
- Geopriv Policy [Schulzrinne2012]
- A Presence-based GEOPRIV Location Object Format [Peterson2005a]
- A Presence Architecture for the Distribution of Geopriv Location
- Common Policy [Peterson2005b]

† The protection of privacy is based on Privacy Rules set by the "user/owner of the Target".

Maguire IK2555, Spring 2016 Slide 292

IETF Geographic Location/Privacy (geopriv) working group charter - http://www.ietf.org/html.charters/geopriv-charter.html

[Cuellar2004] J. Cuellar, J. Morris, D. Mulligan, J. Peterson, and J. Polk, "Geopriv Requirements", Internet Request for Comments, vol. RFC 3693 (Informational), February 2004, Available at http://www.rfc-editor.org/rfc/rfc3693.txt .

[Polk2004] J. Polk, J. Schnizlein, and M. Linsner, Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information, RFC 3825, July 2004. http://www.ietf.org/rfc/rfc3825.txt

[Schulzrinne2006] H. Schulzrinne, "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information", Internet Request for Comments, vol. RFC 4676 (Proposed Standard), October 2006, Available at http://www.rfc-editor.org/rfc/rfc4676.txt .

[Peterson2005a] J. Peterson, "A Presence-based GEOPRIV Location Object Format", Internet Request for Comments, vol. RFC 4119 (Proposed Standard), December 2005, Available at http://www.rfc-editor.org/rfc/rfc4119.txt .

[Peterson2005b] J. Peterson, "A Presence Architecture for the Distribution of GEOPRIV Location Objects", Internet Request for Comments, vol. RFC 4079 (Informational), July 2005, Available at http://www.rfc-editor.org/rfc/rfc4079.txt .

[Schulzrinne2012] H. Schulzrinne, H. Tschofenig, J. Cuellar, J. Polk, and M. Thomson, "Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information", Internet draft, August 21, 2012, Expires: February 22, 2013 http://tools.ietf.org/html/draft-ietf-geopriv-policy-27

Slide 293

Context aware services

In addition to location it is possible to include other information about the user's context to create context-aware services. See for example:

- Alisa Devlic's licentiate thesis: Context addressed communication dispatch [Devlic2009]
- Bemnet Tesfaye Merha's masters thesis: Secure Context-Aware Mobile SIP User Agent [Tesfaye2009]

Maguire IK2555, Spring 2016 Slide 293

[Devlic2009] Alisa Devlic, Context addressed communication dispatch, Licentiate Thesis, KTH Royal Institute of Technology, School of Information and Communications Technology, TRITA-ICT-COS-0902, April 2009
http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-10282

[Tesfaye2009] Bemnet Tesfaye Merha, Secure Context-Aware Mobile SIP User Agent, Master of Science Thesis, Scholl of Information and Communication Technology, KTH Royal Institute of Technology, TRITA-ICT-EX-2009:63, July 2009
http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-91499

Slide 294

Further reading

Number portability

Tango Telecom,"Number Portability: a white paper", Tango Telecom, wpnp01-18/02/00

Barry Bishop, "LNP, Pooling and IVR: What are the impacts to Public Safety Organizations and Law Enforcement?", Lockheed Martin, formerly at http://www.numberpool.org/law_911_registration/apco.ppt

Prepaid

Gemplus, "Smart Card in Wireless Services" {perhaps a bit biased since they are one of the leading vendors of smart cards}

Slide 295

¿Questions?

Slide 296: Lecture 5: Network evolution: WAP, Heterogeneous PCS, 3G, Beyond 3G, 4G

IK2555: Mobile and Wireless Network Architectures: Lecture 5

prof. Gerald Q. Maguire Jr. http://people.kth.se/~maguire/

School of Information and Communication Technology (ICT), KTH Royal Institute of Technology

IK2555 Spring 2016 2016.01.08 © 2016 G. Q. Maguire Jr. All rights reserved.

Slide 297

5. Network evolution:
WAP, Heterogeneous PCS, 3G, Beyond 3G, 4G

Lecture notes of G. Q. Maguire Jr.

For use in conjunction with Yi-Bing Lin and Ai-Chun Pang, *Wireless and Mobile All-IP Networks*, John Wiley & Sons; 2005, ISBN: 0-471-74922-2.

Slide 298

Wireless Application Protocol (WAP)

Goal: a set of communication protocol standards to make accessing online services from a mobile phone simple

> "The motivation for developing WAP was to extend Internet technologies to wireless networks, bearers and devices."[WAP2002], page 4.

Initially conceived by four companies: Ericsson, Motorola, Nokia, and Openwave Systems Inc. (formerly Unwired Planet)

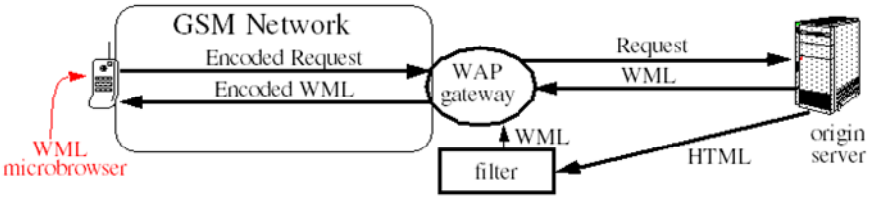
WAP Forum is an industry association to promote WAP, they are now called "The Open Mobile Alliance Ltd."
http://www.openmobilealliance.org/

[WAP2002] WAP Forum, "Wireless Application Protocol (WAP) 2.0 Technical White Paper", (formerly www.wapforum.org), January 2002.

Slide 299

WAP Model

Also called the WAP "Proxy Model" - since WAP gateway acts as a proxy:



The basic (erroneous) thoughts behind WAP were:

- that terminals were "limited" in processing/memory/display,
- that the communication channel was expensive,
- that the operator was "the" natural intermediary in every mobile user's interaction with any services, and
- that a special protocol stack was necessary to "optimize" for the above.

An emphasis was on **push services**: In push services **content** is sent to the user without the user requesting it.

Slide 300

WAP (first round) Summary

Massive failure, because:

- tried to introduce a WAP protocol stack
- did not really provide an **end-to-end service** {because they wanted to keep the operator in the middle of all transactions} - the result is that content was in clear text in the WAP gateway
  - Tthe result was significant security problems - especially because the changes that were introduced into the "WAPified" Secure Sockets Layer introduced problems.
- most operators used SMS to carry the WAP traffic and this was too expensive and had very significant delay problems
- many terminals had problems with their software and each type had its own resolution, size, … - so content had to be prepared for a specific terminal {which increased content development costs - since automatic conversion was not really successful}

WAP 2.0 moves toward being an IP based stack (with HTTP, TLS, and TCP) - although of course they still support their earlier "optimized/wapified" stack. The new model is a direct connection between mobile and HTTP server.

Slide 301

WAP 2.0

Wireless Profiled HTTP (WP-HTTP)	a profile of HTTP for the wireless environment and is fully interoperable with HTTP/1.1. Built on HTTP request/response transaction. Supports message body compression of responses and the establishment of secure tunnels.
Transport Layer Security (TLS)	a wireless profile of the TLS protocol, includes cipher suites, certificate formats, signing algorithms and the use of session resume. Support end-to-end security at the transport level.
Wireless Profiled TCP (WP-TCP)	provides connection-oriented services, optimized for wireless environments and fully interoperable with standard TCP implementations. Builds upon IETF Performance Implications of Link Characteristics (PILC) working group recommendations
Wireless Session Protocol (WSP)	Wireless Transaction Protocol (WTP), Wireless Transport Layer Security (WTLS), Wireless Datagram Protocol (WDP) - as now "Legacy Protocol Layers"[WAP2002]

Maguire IK2555, Spring 2016 301

[WAP2002] WAP Forum, "Wireless Application Protocol (WAP) 2.0 Technical White Paper", (formerly www.wapforum.org), January 2002.

Slide 302

WAP today

WAP has essentially been displaced due to the adoption of HTML browsers in smartphones, as these devices have increasingly become just another IP capable device.

Slide 303

Heterogeneous PCS

Utilize multiple types of radios to exploit the advantages of each to:

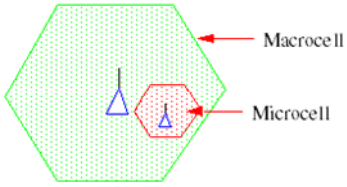
- increase capacity and/or
- increase coverage area and/or
- decrease power consumption and/or
- increase bandwidth and/or
- decrease delay, …

Slide 304

Similar Radio technologies + Same Network technology (SRSN)

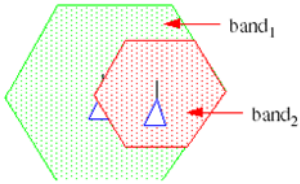
with different power levels

different size cells; for example macrocells with microcells for hotspot coverage; microcells "borrow" radio channels from the macrocellular system - so that they use a different channel than the overlapping macrocell



with different frequency bands

multiband system such as: GSM900+GSM1800macrocell since the cells can overlaps arbitrarily they can of course be of different sizes



Slide 305

Different Radio technologies + Same Network technology (DRSN)

Both using IS-41 as network protocol:

- IS-136 + AMPS
- IS-95 + AMPS

Slide 306

Different Radio technologies + Different Network technologies (DRDN)

Generally high-tier PCS with low-tier PCS Examples:

- AMPS +PACS or GSM +PACS
- GSM + DECT

Slide 307

Tier Handoff

Tier Handoff performs handoffs from one system to another.

For the case of **SRSN:**

different power levels, the macro and microcells use the same air interface and the handoffs is as usual

different bands, just a little harder than usual (because the handset might not be able to listen to more than one frequency at a time).

The case of DRSN is harder and generally requires modification of the handoff of each system, in some cases the handoff might only work in one direction

In the case of DRDN, the easiest is to simply set up a new call (perhaps via automatic redial) in the new network.

Slide 308

Registration for SRSN & DRSN

Fairly straight forward since the systems use the same network technology.
Key problem is: Who does the tier **selection**?

Slide 309

Registration for DRDN

Since the different systems use different registration & authentication and different data may be store in their different HLRs (and VLRs) ⇒ define a new **multitier HLR** to integrate the two.

Implemented via **tier manager:**

Single registration (SR) vs. Multiple registrations (MR) - the former is simpler, the later reduces the registration traffic and decreases the time required for tier handoffs.

Slide 310

Call delivery

SR case	simply query the mobile network's HLR to find where to deliver the call
MR case	either select the tier to try based on some heuristic (for example, always try low-tier first or try the system where the MS register most recently) or page first, then try the one where you get a response

Slide 311

User identity (identities) and MSs

There can be:

- a single identity or several identities
  - user can be associated with a single logical “number” or multiple
  - identities can have a primary association with a MS or no
- single or multiple MSs
  - user can use one (multimode MS) or several MSs
  - Does the user choose which device to use or does the multitier manager?

A hard problem is what to do when the service (for example, streaming video) only makes sense on a subset of the MSs or PCS systems.

Slide 312

Major forces driving heterogeneous PCS

Consolidation/mergers&acquisitions/bankruptcy/… ⇒ new owner may end up owning several different types of systems, examples:

- AT&T acquisition of McCaw's cellular system
- Bell Atlantic merger with NYNEX
- Merger of Vodaphone with AirTouch
- DeutscheTelekom's (T-Mobile) Voicestream Wireless Corp. acquistion of WLAN operations of MobileStar
- …

Slide 313

Internetworking scenarios

There are several alternatives for how tightly the different systems might be coupled [Olaziregi2003]:

- Open coupling
  - No real integration between the systems, except perhaps for sharing a billing system
  - Separate authentication for each system
- Loose coupling
  - sharing a single subscriber database
  - allows centralized billing
  - allows interworking, but has two separate IP address spaces and does not support vertical handoffs (so connections are dropped when the use moves from one network to another)
- Tight coupling
  - an Interworking Unit (IWU)/Radio Network Controller (RNC) interconnects the radio access networks to the SGSNs
  - might require a new set of interfaces Iu (RNC-SGSN) and Iub (RAN-RNC) {RAN = Radio Access Network}
- Very tight coupling
  - an Interworking Unit (IWU) connects the Radio Access Network to the RNC
  - for example, using an interface Iu(RNC-WLAN) to connect WLAN as a cell of the RNC

Maguire IK2555, Spring 2016 313

[Olaziregi2003] Nikolas Olaziregi, Stefano Micocci, Kambiz Madani, Tereska Karran, George R. Ribeiro-Justo, Mahboubeh Lohi, David Lund, Iam Martin, Bahram Honary, Sándor Imre, Gyula Rábai, Jósef Kovács, Péter Kacsuk, Árpad Lányi, Thomas Gritzner, and Mattias Forster, “Chapter 5: Network Architectures and Functions”, in *Software Defined Radio: Architectures, Systems and Functions*, Markus Dillinger, Kambiz Madani, and Nancy Alonistioti (Eds.), Wiley 2003, ISBN 0-470-85164-3, pp. 95-142.

Slide 314

Paradigm shifts

- voice-centric ⇒ data centric
  - shift to packet switching
  - problems: QoS, streaming media
- continually evolving terminals and data applications - end users **expect** the same services (and more) from wireless systems as they expect from wireline systems
- low peak data rates ⇒ high peak data rates
- same service everywhere ⇒ spatially & temporally varying service (especially with respect to achieved data rates)

Slide 315

Third Generation Mobile (3G)

Offering data rates greater than ISDN (144 kbps), typically thought to be 384 kbps and perhaps up to 2 Mbps when stationary near a base station.

Six types of services:

- Interactive multimedia (video conferencing)
- High speed multimedia ("broadcast" TV)
- Medium speed multimedia (web browsing)
- Circuit switched data (FAX)
- Speech (telephony)
- Messaging (e-mail, SMS, …)

All based on CDMA; Europe's Universal Mobile Telecommunications System (UMTS) will be Wideband CDMA (W-CDMA, 25 MHz channel bandwidth):

- ETSI agreed to use a combination of wideband code division multiple access (W-CDMA) and time division multiple access (TD/CDMA) on the air interface
- W-CDMA will be used to cover larger areas
- TD/CDMA for local (indoor) applications

Slide 316

3rd Generation Partnership Project (3GPP)

Original scope was to produce **globally applicable** Technical Specifications and Technical Reports for a **3rd Generation Mobile System** based on evolved GSM core networks and the radio access technologies that they support ⇒ Universal Terrestrial Radio Access (UTRA)†, W-CDMA, UMTS (in Europe) and FOMA (in Japan)

Amended to include the maintenance and development of the Global System for Mobile communication (GSM) Technical Specifications and Technical Reports **including** evolved radio access technologies (e.g. General Packet Radio Service (**GPRS**) and Enhanced Data rates for GSM Evolution (**EDGE**)).

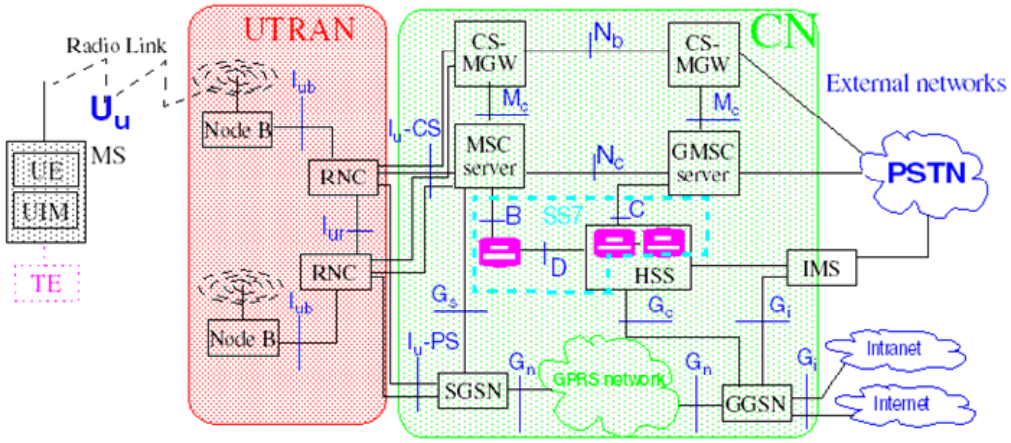
See: http://www.3gpp.org/

ETSI is the 3GPP Secretariat

† Both Frequency Division Duplex (FDD) and Time Division Duplex (TDD) modes.

Slide 317

3G(PP) Architecture



CN = Core network; RNC = Radio Network Controller; IMS=IP Multimedia Subsystem; HSS=Home Subscriber Server; CS-MWG=Circuit Switch Media Gateaway

The division into a circuit switched domain and a packet switched domain - will disappear as the architecture evolves to an "All-IP" network.

Maguire IK2555, Spring 2016 317

Slide 318

3.5G or super 3G

HSDPA + HSUPA sometimes called 3.5G or super 3G

High Speed Downlink Packet Access (HSDPA)

An enhancement to WCDMA providing fast retransmissions over wireless link and fast scheduling to share a high speed downlink.

For further details see [Wang2004] and [Gutiérrez2003]

High Speed Uplink Packet Access (HSUPA)

An enhancement to WCDMA providing sharing of a high speed uplink, called the enhanced dedicated channel (E-DCH); this channel is assigned to one mobile device at a time

Goal: upload (burst) speeds up to 5.8 Mbit/s For further details see [Carnero2004] and [Rosa2005]

For some measurements of achieved **upload** rates see Shuang Di's thesis [Di2009]

Maguire IK2555, Spring 2016 318

[Wang2004] Xiaoxin Wang, "3G HSDPA Performance In Mobile Internet Connections", M. Sc. Thesis, KTH/IMIT, IMIT/LCN 2004-02, March 2004, http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-93068 .

[Gutiérrez2003] Pablo Ameigeiras Gutiérrez, "Packet Scheduling and Quality of Service in HSDPA", Ph.D. Thesis, Aalborg University, Aalborg Øst, Denmark, October 2003. formerly at http://kom.aau.dk/ADM/research/reports/PhDThesis_Pablo_Ameigeiras.pdf

[Carnero2004] José Outes Carnero, "Uplink Capacity Enhancement in WCDMA: Multi Cell Admission Control, Synchronised Schemes and Fast Packet Scheduling", Ph.D. Thesis, Aalborg University, ISBN 987-90834-54-2, ISSN 0908-1224, R04-1011, Aalborg Øst, Denmark, March 2004. formerly at http://kom.aau.dk/ADM/research/reports/Review%20of%20Ph.D.%20Thesis%20Jose%20Outes%20Carnero.pdf

[Rosa2005] Claudio Rosa, "Enhanced Uplink Packet Access in WCDMA", Ph.D. Thesis, AAlborg University,Aalborg Øst, Denmark, February 2005. formerly at http://kom.aau.dk/ADM/research/reports/PHD_Thesis_Claudio_Rosa.pdf

[Di2009] Shuang Di, USB Attached Network Performance: Uplink Performance, Masters thesis, KTH Royal Institute of Technology, School of Information and Communication Technology, TRITA-ICT-EX-2009:2, April 2009 http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-91529

Slide 319

Third Generation Partnership Project 2 (3GPP2)

A collaborative third generation (3G) telecommunications standards-setting project comprising **North American** and **Asian** interests developing global specifications for **ANSI/TIA/EIA-41** "Cellular Radiotelecommunication Intersystem Operations network evolution to 3G", and global specifications for the radio transmission technologies (RTTs) supported by ANSI/TIA/EIA-41.

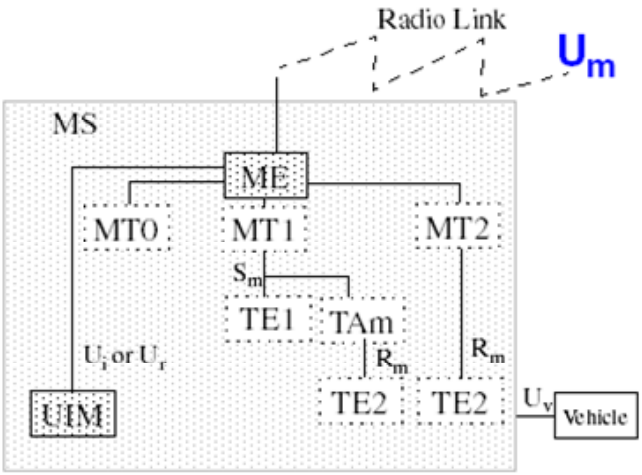
Focus is cdma2000

See: *http://www.3gpp2.org/*

TIA is the 3GPP2 Secretariat

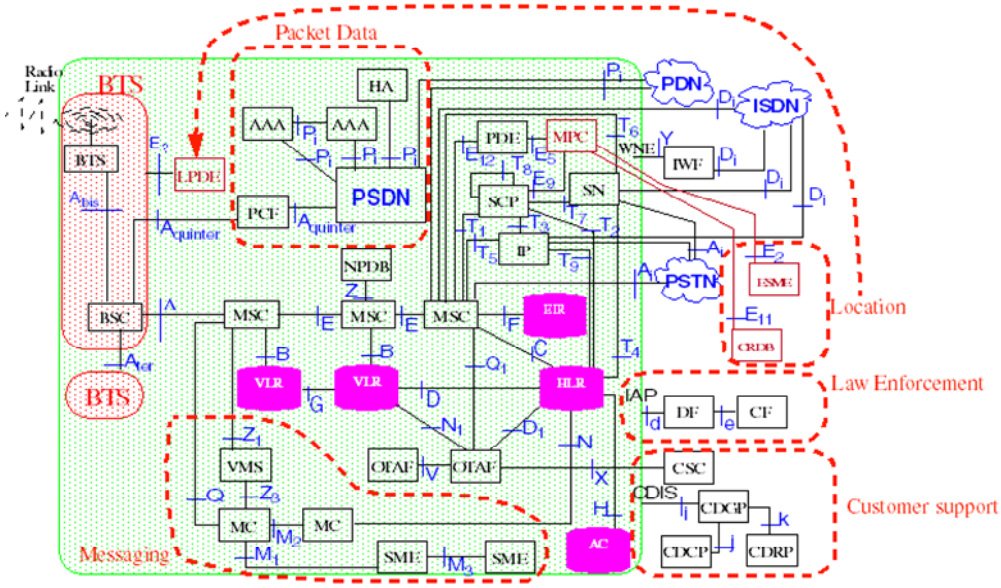
Slide 320

3GPP2 reference model (the mobile)



Slide 321

3GPP2 Architecture (infrastructure and external entities)



Slide 322

Interface	Description
A	between BSC and MSC, PCM 2 Mbps, G. 703
A_i	Analog Interface to PSTN
A_{bis}	between BTS and BSC, PCM 2 Mbps, G. 703
$A_{quinter}$	between BSC and PCF (Packet Control Function)
B	between MSC and VLR (use MAP/TCAP protocols)
C	between MSC and HLR (MAP/TCAP)
D	between HLR and VLR (MAP/TCAP)
D_i	Digital interface to ISDN
D_1	between VLR and OTAF (Over-The-Air Service Provisioing Function)
E	between two MSCs (MAP/TCAP + ISUP/TUP)
E_2	between MPC and ESME (Emergency Service Message Entity
E_5	between MPC and PDE (Position Determining Entity)
E_9	between MPC and SCP
E_{11}	between MPC and CRDB
E_{12}	between MPC and ESME
F	between MSC and EIR (MAP/TCAP)
G	between VLRs (MAP/TCAP)
H	between HLR and AuC
M_1	between MC (Message Center) and SME (Short Message Entity)
M_2	between MCs (Message Centers)
M_3	between SMEs (Short Message Entities)

Maguire IK2555, SPRING 2016 Slide 322

Slide 323

Interface	Description
N	between MC (Message Center) and HLR
N_1	between HLR and OTAF
P_i	Packet interface
Q	between MSC and MC (Message center)
Q_1	between MSC and OTAF
T_1	between MSC and SCP
T_2	between SCP and HLR
T_3	between SCP and IP
T_4	between SN and HLR
T_5	between MPC and IP (Intelligent Peripheral)
T_6	between MPC and SN (Service Node)
T_7	between SN and SCP
T_8	between SCPs
T_9	between IP and HLR
U_i	between UIM and ME
U_m	Radio link between MS and BTS
U_r	between UIM and ME
U_v	between MS and vehicle
V	between OTAFs
X	between OTAF and CSC
Y	between WNE and IWF (Inter-working Function)
Z	between MSC and NPDB

Maguire IK2555, Spring 2016 Slide 323

Slide 324

Interface	Description
Z_1	between MSC and VMS
Z_3	between VMS and MC
d	IAP (Intercept Access Point) interface to DF (Delivery function)
e	between DF and CF (Collection function)
i	CDIS (Call Data Information Service) interface to CDGP (Call Data Generation Point)
j	between CDGP and CDCP (Call Data Collection Point)
k	between CDGP and CDRP (Call Data Rating Point)

Slide 325

3GPP2 abbreviations

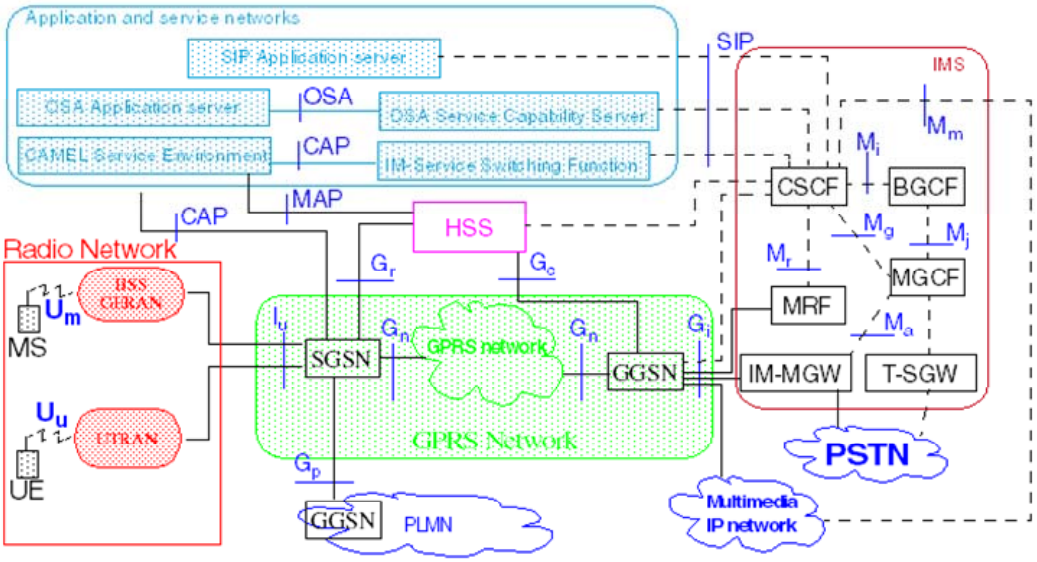
Abbreviation	Explanation
AAA	Authentication, Authorization, and Accounting
AC	Authentication Center (called AuC in GSM)
BTS	Base Transceiver Station
CDCP	Call Data Collection Point
CDGP	Call Data Generation Point
CDIS	Call Data Information Service
CDRP	Call Data Rating Point
CF	Collection Function (for collecting intercept information)
CRDB	Coordinate Routing Database
CSC	Customer Service Centre
DF	Delivery function (for delivering intercepted communications)
ESME	Emergency Service Message Entity
EIR	Equipment Identity Register
HA	Home Agent
HLR	Home Location Register
IP	Intelligent Peripheral
IAP	Intercept Access Point
IWF	Inter-working Function
LPDE	Local Position Determining Entity
MC	Message Centre

Slide 326

Acronym	Explanation
ME	Mobile Equipment
MPC	Mobile Positioning Center
MS	Mobile Station
MSC	Mobile Switching Centre
NPDB	Number Portability Database
OTAF	Over-The-Air Provisioning Function
PCF	Packet Control Function
PDN	Packet Data network
PDSN	Packet Data Serving Node (AKA a router!)
SCP	Service Control Point
SME	Short Message Entity
SN	Service Node
TA/Tm	Terminal Adapter
UIM	User Identity Module
VLR	Visitor Location Register
VMS	Voice Message System
WNE	Wireless Network Entity

Slide 327

All-IP Architecture



IMS=IP Multimedia Subsystem; HSS=Home Subscriber Server; IM-MGW=IP Media Gateaway

Slide 328

Mobile Station Application Execution Environment (MExE)

Building on ideas from WAP, UMTS introduces a Mobile Station Application Execution Environment (MExE) to provide a standard environment for the MS to access the internet and intranet services.

MExE Classmark

classifies the MS based on its capabilities (processing, memory, display, …)

MExE classmark 1	based on WAP
MExE classmark 2	based on PersonalJava (supports JavaPhone Power Monitor package)
MExE classmark 3	based on Java 2ME Connected Limited Device Configuration (CLDC) and Mobile Information Device Profile (MIDP) environment - supports Java applications running on resource constrained devices.
MExE classmark 4	based on ECMA's Common Language Infrastructure Compact Profile - supports CLI based applications running on resource constrained devices (CLI designed to be programming language and OS neutral)

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Mobile Execution Environment (MExE); Functional description; Stage 2 (Release 11), 3GPP TS 23.057 V11.0.0, 2012-09, available from http://www.3gpp.org/ftp/Specs/archive/23_series/23.057/23057-b00.zip

Maguire IK2555, Spring 2016 Slide 328

Further information about these topics can be found at:

PersonalJava™ Application Environment
http://www.oracle.com/technetwork/java/index.html (formerly http://java.sun.com/products/personaljava)

JavaPhone™ API
formerly at http://java.sun.com/products/javaphone

Java 2 Micro Edition (Java 2ME)
formerly at http://java.sun.com/j2me

Connected Limited Device Profile (CLDC) formerly at
http://java.sun.com/products/cldc/

Mobile Information Device Profile (MIDP) formerly at
http://java.sun.com/products/midp/

ECMA's Common Language Infrastructure (ECMA-335) formerly at
http://cedar.intel.com/media/zip/ECMA-335.zip

ECMA's Common Language Infrastructure Technical Report (ECMA-TR-084)
formerly at http://cedar.intel.com/media/zip/ECMA-TR-084.zip

Erik Meijer and John Gough, "Technical Overview of the Common Language Runtime",
http://research.microsoft.com/~emeijer/Papers/CLR.pdf

Slide 329

Common Language Infrastructure (CLI) for MExE devices: Classmark 4

Service discovery and management

Browser installed on a MExE device should support Multi-Purpose Internet Mail Extensions (MIME) type text/vnd.sun.j2me.app-descriptor. Allows user to browse and discover a Java application which can then be downloaded. Capability negotiation information in the request header can determine which application to present.

MID applications (MIDlets) and MIDlet suites are indicated to the user, if the terminal has a display, may be presented as an icon and a tag or as a textual tag

Java Application Description (JAD) file can be downloaded and to determine if the MIDlet is suitable for download and installation

- If it is, then JAR file can be downloaded and installed
- If not, the MExE UE should be able to prompt the user so that the user (they can delete some existing applications if there is not enough space to install the new application)
- If the application chosen already exists on the device, the user should be notified so they can choose to either to download the chosen version or to retain the existing one
- user should be able either to launch the MIDlet immediately or later

Slide 330

CLI MExE Devices

MExE Classmark 4 devices based on CLI Compact Profile spec.: defines runtime environment and APIs available to a CLI based MExE device such that services (specified in the form of language independent classes and interfaces) can control such a device in a standardized way.

CLI Compact Profile Namespaces

- System
- System.Collections
- System.Globalization
- System.IO
- System.Text
- System.Threading
- System.Runtime.CompilerServices
- System.Reflection
- System.Net
- System.Xml

Application management features for a Classmark 4 application

- Discovery
- Download
- Verification
- Installation
- Execution Start
- Execution Pause
- Execution Resume
- Execution Stop
- Execution Terminate
- Uninstall

Slide 331

Support for network protocols

Protocol	Optional?
HTTP/1.1	Mandatory
HTTPS	Mandatory
SOAP	Mandatory
ftp	Optional
mailto	Optional
File	Optional

Slide 332

3G Physical Layer

There has been great fighting over what is the "best" physical and link layer for 3G, due to political, economic, … reasons.

There are several 3G CDMA modes (at least 5 different choices), but there might be some hope for harmonization at the network level (with at least 3 choices: ANSI-41, GSM MAP, and IP)!

Slide 333

Gateway Location Register (GLR)

3GPP introduces a **Gateway Location Register** (GLR) to reduce traffic between VLR and HLR {especially for the case of international roaming}. The GLR is located in the visited network, but is treated by the visited network as the user's HLR (while the user is in the visited network).

Home network treats the GLR as if it were a VLR in the visited network.

While it can clearly reduce signaling costs when the user is not in their home country - the book does not address the question of "Does this really matter?" Since there is an enormous amount of bandwidth available via fibers - does the signaling traffic really matter? Does the GLR reduce the delays for providing service to the user?

Slide 334

3G QoS

Four QoS classes:

conversational	for delay sensitive traffic, with limited transfer delay
streaming	for one-way real-time traffic
interactive	for delay-insensitive traffic such as e-mail, telnet, …
background	for delay-insensitive traffic such as FTP, background bulk transfer of e-mail, …

7 QoS parameters: max/min/guaranteed bit rates, max. packet size, reliability, … Major problems with how to **map** between the QoS of different systems.

Slide 335

UMTS Subscriber Identity Module (USIM)

3GPP specifications:

TS21.111	USIM and IC card requirements
TS22.112	USIM toolkit interpreter; Stage 1
TS31.111	USIM Application Toolkit (USAT)
TS31.112	USAT Interpreter Architecture Description; Stage 2
TS31.113	USAT interpreter byte codes
TS31.114	USAT interpreter protocol and administration
TS31.115	Secured packet structure for (U)SIM Toolkit applications
TS31.116	Remote APDU Structure for (U)SIM Toolkit applications
TS31.120	Universal Integrated Circuit Card (UICC)-terminal interface; Physical, electrical and logical test specification
TS31.121	UICC-terminal interface; USIM application test specification
TS31.122	USIM conformance test specification
TS31.131	C-language binding for (U)SIM API
TR31.900	SIM/USIM internal and external interworking aspects
TS42.017	Subscriber Identity Module (SIM); Functional characteristics
TS42.019	Subscriber Identity Module Application Programming Interface (SIM API); Stage 1
TS43.019	Subscriber Identity Module Application Programming Interface (SIM API) for Java Card; Stage 2
TS51.011	Specification of the Subscriber Identity Module – Mobile Equipment (SIM-ME) interface
TS51.013	Test specification for SIM API for Java card

Slide 336

Wireless Operating System for Handsets

There has been a battle for who will define and dominate the OS market for 3G (and later) handsets - which given the expected handset volume could be a very large market.

Candidates:

- Google's Android
- Apple's iOS
- Microsoft - WinCE, Windows Phone
- linux (e.g., Ubuntu on Samsung Galaxy S III)
- ~~Symbian's EPOC OS - built upon Psion's OS - Symbian formed by Nokia, Ericsson, Motorola)~~
- ~~Open WebOS~~

Worldwide Smartphone OS Market share	
Period	2015Q2*
Android	82.8%
Apple's iOS	13.9%
Windows Phone	2.6%
BlackBerry OS	0.3%
Others	0.4%

* Statistics from IDC Aug 2015, http://www.idc.com/prodserv/smartphone-os-market-share.jsp

Slide 337

Mobile Virtual Network Operator (MVNO)

A virtual operator who uses the physical infrastructure of other operators.

Pyramid Research projects a greater than 3x Return on Investment (ROI) for MVNOs vs. facilities-based UMTS network operator†.

was available from http://www.pyramidresearch.com/info/rpts/mvno.asp

Richard Branson's Virgin Mobile signed up 700k customers in their first year!‡

"Freed from a large subscriber base that is necessary to cover network deployment costs, an MVNO can target a more finely segmented market."§

Mobile Virtual Network Operators: Oftel inquiry into what MVNOs could offer consumers - was available from http://www.oftel.gov.uk/publications/1999/competition/mvno0699.htm

note Oftel was replace by Ofcom http://www.ofcom.org.uk/

† was http://www.pyramidresearch.com/static_content/feature_articles/010402_feature.asp
‡ was http://www.adventis.com/mvno/main.htm
§ was http://www.gii.co.jp/english/pr8818_mvno.html

Slide 338

IP Multimedia Subsystem (IMS)†

One of the major driving forces for 3G telephony (as envisioned by many vendors and operators) is Multimedia. 3GPP has defined an IP Multimedia Subsystem (IMS) and 3GPP2 introduced the MultiMedia Domain (MMD) for third generation CDMA2000 networks - the two were subsequently harmonized.

The first new services include:

- Instant Messaging
- Presence
- Push to Talk over Cellular (PoC) ("walkie-talkie" like services)
  - one of the major features of such services is group communication - i.e., the audio segment can easily be delivered to many users

All of these services are easily added as they are not too demanding of the underlying radio access network[Tadault2004], hence they can be offered via existing 2G & 2.5G networks, as well as via WLANs and even to an ISP's xDSL and cable customers.

†For additional details concerning IMS see: Boris Iv. Kalaglarski and Emilio Di Geronimo's Masters thesis "IMS Interworking"[Kalaglarski and Geronimo2007] and the book by Camarillo & García-Martín[Camarillo and García-Martín2006].

Maguire IK2555, Spring 2016 Slide 338

[Tadault2004] M. Tadault, S. Soormally, and L. Thiébaut, "Network Evolution towards IP Multimedia Subsystem", Strategy White Paper, Alcatel Telecommunications Review, 4th Quarter 2003/1st Quarter 2004

[Kalaglarski and Geronimo2007] Boris Iv. Kalaglarski and Emilio Di Geronimo, "IMS Interworking", Masters Thesis, Department of Communication Systems, KTH Royal Institute of Technology, May 2007 http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-91992

[Camarillo and García-Martín2006] G. Camarillo and Miguel-Angel García-Martín, *The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the cellular worlds*, Second edition, Wiley, 2006, 456 pages, ISBN-10: 0470018186 and ISBN-13: 978-0470018187

Eoin O'Regan and Dirk Pesch, "Performance Estimation of a SIP based Push-to-Talk Service for 3G Networks", The Fifth European Wireless Conference: Mobile and Wireless Systems beyond 3G, February 24-27, 2004, Barcelona,Spain, the paper was submitted 17 December 2003 http://research.ac.upc.edu/EW2004/papers/144.pdf

Slide 339

IMS services

- person-to-person real-time IP-based multimedia communications (e.g. voice, videotelephony, …)
- person-to-machine communications (e.g. gaming).
- integrated real-time with non-real-time multimedia communications (e.g. live streaming with a chat group)
- services combining use of presence and instant messaging; other combinations of services, e.g., surveillance - where a remote camera begins streaming video because of a presence detection event)
- multiple services in a single session or multiple simultaneous synchronized sessions (think of Synchronized Multimedia Integration Language (SMIL)[Ayars2001])
  - should include transitioning from a two party voice call to a multi-party audio and video conference ⇒ no need for special predefined conference services
  - Kristofer Borgström, "MMS Components for Web 2.0", Masters' thesis, KTH, ICT, COS, TRITA-ICT-COS COS/CCS 2008-01, 2008 *http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-91878*

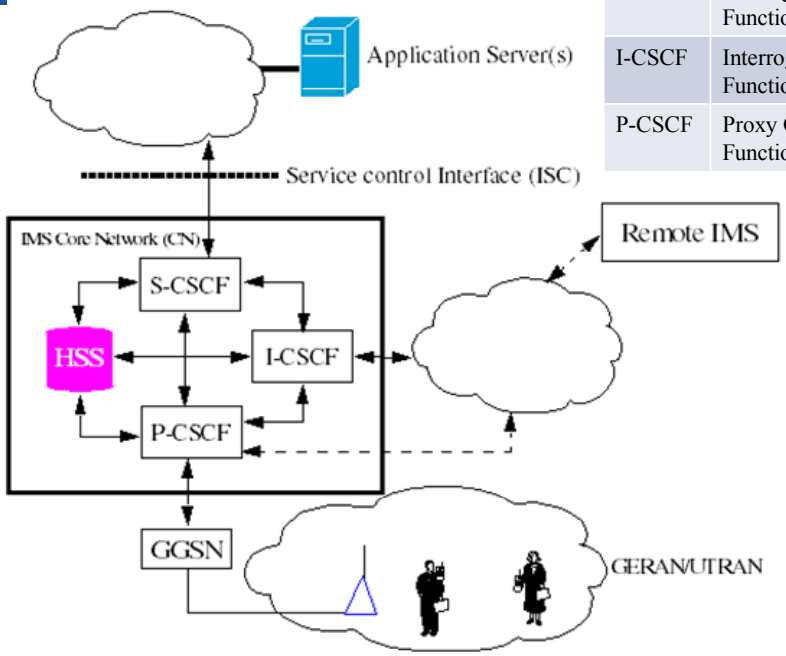
Maguire IK2555, Spring 2016 Slide 339

[Ayars2001] Jeff Ayars, Dick Bulterman, Aaron Cohen, Ken Day, Erik Hodge, Philipp Hoschka, Eric Hyche, Muriel Jourdan, Michelle Kim , Kenichi Kubota, Rob Lanphier, Nabil Layaïda, Thierry Michel, Debbie Newman, Jacco van Ossenbruggen, Lloyd Rutledge, Bridie Saccocio, Patrick Schmitz, Warner ten Kate (Editors), "Synchronized Multimedia Integration Language (SMIL 2.0)", W3C Recommendation, 07 August 2001 - *http://www.w3.org/TR/smil20/*

Slide 340

IMS architecture

HSS	Home Subscriber Server
S-CSCF	Serving Call Session Control Function
I-CSCF	Interrogating Call Session Control Function
P-CSCF	Proxy Call Session Control Function



Maguire IK2555, Spring 2016 Slide 340

Slide 341

“Small” IMS deployments

Dan Peterström, IP Multimedia for Municipalities: The supporting architecture, Master's thesis, KTH, School of Information and Communication Technology (ICT), Communication Systems (CoS), TRITA-ICT-EX; 2009:103, 2009,
http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-91496

Slide 342

Long-Term Evolution (LTE) Radio Networks

In spring 2007, Petter Edström presented a master's thesis entitled: "Overhead Impacts on Long-Term Evolution Radio Networks" describing the impact of frame and protocol overhead on Long-Term Evolution (LTE) Radio Networks [Edström2007].

3GPP's LTE is an evolution of UMTS to support 100Mbps down link and 50Mbps communication with very low latency (<5 ms) - see http://www.3gpp.org/LTE.

Maguire IK2555, Spring 2016 Slide 342

[Edström2007] Petter Edström, "Overhead Impacts on Long-Term Evolution Radio Networks", Masters Thesis, Department of Communication Systems, KTH Royal Institute of Technology, May 2007
http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-91991

Slide 343

Generations of technology versus generative technology

Today there are lots of discussion of future communication systems, such as the cellular variants Theo Kanter calls πG systems[†], next generation internet, … . there is even discussion of **if** there will be a 4th **generation** of cellular systems or **if** we will see the end of *generational* architectures and systems.

For some additional insights on the future of networking, see and Jonathan Zittrain's *The Future of the Internet -- And How to Stop It* [Zittrain2008] (see *http://futureoftheinternet.org/*).

Note that Jonathan Zittrain's book focuses on the fact that upto this point the Internet can be seen as a generative system/technology (i.e., provides high leverage, is highly adaptable, is easy to master, the technology and tools are readily accessible, and there is high transferability {developments can easily be transferred to another user]) - see [Zittrain2008], page 70-73.

[†] Because $3 < \pi < 4$ and π is an irrational number.

Maguire IK2555, Spring 2016 Slide 343

[Zittrain2008] Jonathan Zittrain, The Future of the Internet -- And How to Stop it, New Haven: Yale University Press, 342 pages, 2008. ISBN 978-0-300-12487-3, Web site of the book and blog: http://futureoftheinternet.org/ ; the author's web site: http://www.jz.org/

Slide 344

Initial steps to 4th generation (4G) in 20xx

User deployed access points (base stations)[Unbehaun2002]

As of 16 November 2004, Nippon Telegraph and Telephone DoCoMo have started shipping their Wi-Fi/Cellular Phone - N900iL (supports a 3G FOMA cellular network and Wi-Fi) [NTT2004].

The same day at the 3G World Congress Convention and Exhibition in Hong Kong, Nokia showed real-time streaming video with seamless handoff between two CDMA access networks using Mobile IPv6, the "first Mobile IPv6 call".[Nokia2004]

Maguire IK2555, Spring 2016 Slide 344

[NTT2004] "NTT DoCoMo Ships Wi-Fi/Cellular Phone", TechWeb News, November 16, 2004 http://www.internetweek.com/allStories/showArticle.jhtml?articleID=53200333

[Nokia2004] "Nokia Demonstrates IPv6 Phone", TechWeb News, November 16, 2004 http://www.internetweek.com/allStories/showArticle.jhtml?articleID=53200335

[Unbehaun2002] Matthias Unbehaun, "Self-deployed Wireless Access Networks", Doctoral dissertation, Radio Communication, KTH, 2002. http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-3405

Slide 345

ITU's International Mobile Telecommunications-Advanced (IMT-Advanced)

"Key features of 'IMT-Advanced'

- a high degree of commonality of functionality worldwide while retaining the flexibility to support a wide range of services and applications in a cost efficient manner;
- compatibility of services within IMT and with fixed networks;
- capability of interworking with other radio access systems;
- high quality mobile services;
- user equipment suitable for worldwide use;
- user-friendly applications, services and equipment;
- worldwide roaming capability; and,
- enhanced peak data rates to support advanced services and applications (100 Mbit/s for high and 1 Gbit/s for low mobility were established as targets for research)"

http://www.itu.int/ITU-R/index.asp?category=information&rlink=imt-advanc ed&lang=en

Slide 346

IEEE 802.21

Developing standards to "enable handover and interoperability between heterogeneous network types including both 802 and non 802 networks".

-- IEEE 802.21 http://www.ieee802.org/21/

Slide 347

4G in Asia

- CJK
  - Collaboration between China, Japan, and Korea for beyond 3G international standards
- FuTURE - A Chinese national project with 4 phases:
  - startup
  - 2003-2005 specification
  - 2007-2007 implementation
  - 2008- standardization
- mITF
  - A Japanese forum for 4G and Mobile Commerce
  - Targeting a commercial introduction in 2010
  - DoCoMo has shown 100 Mbps (outdoors) and 1 Gbps (indoors) using MIMO technology
- Wireless Broadband Portable Internet (WiBro)
  - Korean effect for 2.3 GHz with 10MHz bandwidth to support 0.5 to 50 Mbps at speeds up to 50 km/h.

Information on these 4 efforts is from slide 5 of 12 in a Siemens presentation at the Public Launch of the eMobility Platform [Heins2005].

Maguire IK2555, Spring 2016 Slide 347

[Heins2005] Thorsten Heins, "European and global initiatives in perspective", Siemens presentation at Public Launch of the eMobility Platform on 18th March, 2005 formerly at http://www.emobility.eu.org/documents/launch/Siemens%20Presentation.pdf

Slide 348

Wireless Broadband Portable Internet (WiBro)

For further information on WiBro, see the presentation given by Dongwoo Kim, "Overview of WiBro/WiMAX and Its Evolution" at Wireless@KTH on 2007-11-30:

Abstract: "WiBro is presently in service in Korea. Moreover, the spectrum used for WiBro in Korea is recently allocated to future generation mobile systems in WRC and WiBro evolution (so-called 802.16m) has a target towards IMT-2000 advanced. WiBro was attracted as an economic tool of providing mobile data service, which extends existing IEEE 802.16 to mobile WiMAX. This talk will cover WiBro network architecture, technological elements, frame structure and evolutions."

Slide 349

eMobility Platform http://www.ist-emobility.org/
⇒ "Net!Works" http://www.networks-etp.eu/
⇒ NetWorld2020 European Technology Platform http://networld2020.eu/

"eMobility Platform leads the way

In order to serve Europe's need and to maintain its position in the global market for mobile and wireless systems in the 2010-2020 time horizon, it will be necessary to develop large-scale European approaches to system research and development, and to mobile services and applications in the context of digital convergence.

To this end, the eMobility Platform will define and implement a comprehensive research agenda in the mobile and wireless sector." [eMobility2005a]

Driven by a new paradigm: "Individual's quality of life improvement by making available an environment for instant provision and access to meaningful multi-sensory information and content." pg. 3 of [eMobility2005b]

See the vision and mission statement of NetWorld2020 at http://networld2020.eu/vision-mission/

Maguire IK2555, Spring 2016 Slide 349

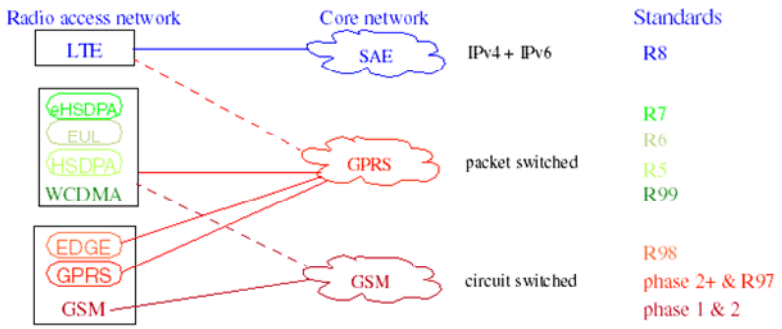
[eMobility2005] eMobility Flyer, from Public Launch of the eMobility Platform on 18th March, 2005 formerly at http://www.emobility.eu.org/documents/launch/Flyer_eMobility_R3.pdf

[eMobility2005b] "Mobile Communications & Technology Platform Strategic Research Agenda: eMobility Staying ahead!", edited by Rahim Tafazolli, Luis M. Correia, and Juha Saarnio, from Public Launch of the eMobility Platform on 18th March, 2005 formerly at http://www.emobility.eu.org/documents/SRA_2005_03_18.pdf

Slide 350

Evolution versus Revolution

Evolution from GSM to LTE - the 3GPP path



Evolution of GSM to LTE (inspired by slide 4 of [Fritze2008]), the phase are from the original GSM specifications, while the releases (indicated as Rxx) are from the 3GPP specifications); dashed links are for legacy connectivity; EUL = enhance uplink

From the initial circuit switched GSM, the evolution has been to packet switch networks, finally to an all-IP architecture. Studies for R14 are currently underway.

Maguire IK2555, Spring 2016 Slide 350

[Fritze2008] Gerhard Fritze, SAE: The Core Network for LTE, Ericsson Austria GmbH, 10 April 2008, http://www.3g4g.co.uk/Lte/SAE_Pres_0804_Ericsson.pdf

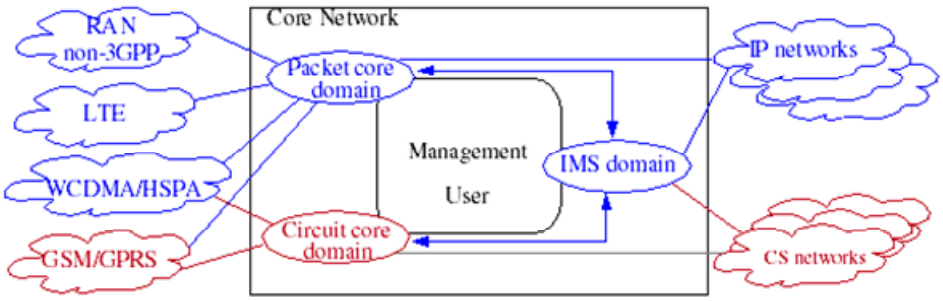
http://www.3gpp.org/ftp/Information/WORK_PLAN/Description_Releases/Rel-14_description_20140924.zip

Slide 351

System Architecture Evolution (SAE)

Formally SAE is the 3GPP work standardization item which concerns the evolution of the packet core network ⇒ the Evolved Packet Core (EPC)

Terminals + RAN (E-UTRAN†) + EPC = the Evolved Packet System (EPS)



EPS architecture showing the 3GPP core network domains and their relationship to the RANs (on the left) and other networks (on the right) (Inspired by Figure 3.1.1 of [Olsson2009].)

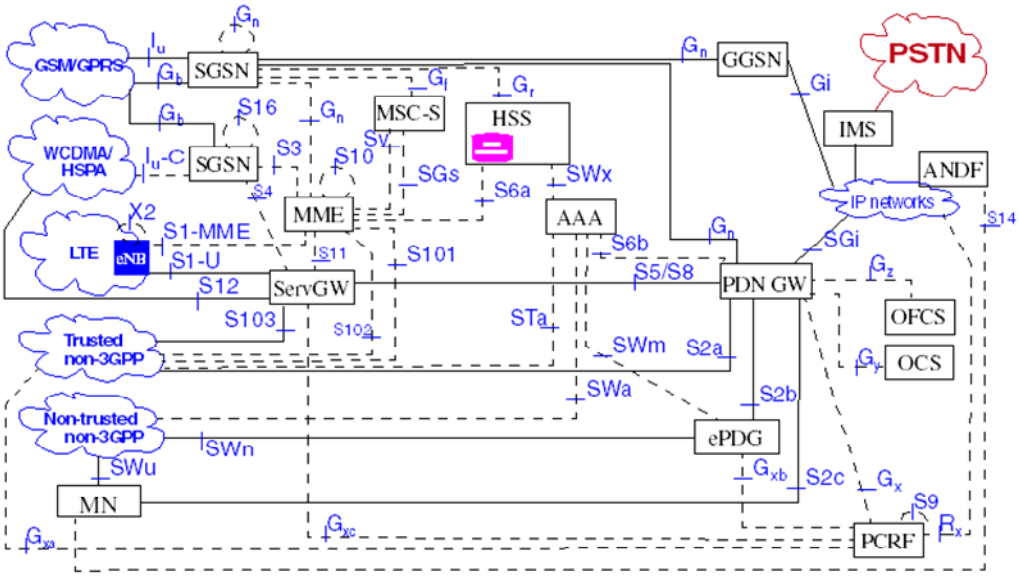
† Evolved UTRAN - a RAN that support 3GPP's Long Term Evolution (LTE) standard

Maguire IK2555, Spring 2016 Slide 351

[Olsson2009] Magnus Olsson, Shabnam Sultana, Stefan Rommer, Lars Frid, and Catherine Mulligan, SAE and the Evolved Packet Core: Driving the Mobile Broadband Revolution, Academic Press, 2009, ISBN 978-0-12-374826-3

Slide 352

SAE architecture

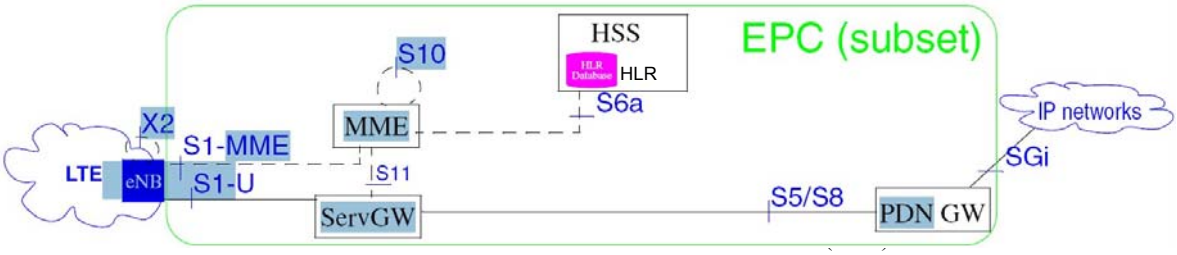


SAE architecture (inspired by Figure 3.1.2 of [Olsson2009])

[Olsson2009] Magnus Olsson, Shabnam Sultana, Stefan Rommer, Lars Frid, and Catherine Mulligan, SAE and the Evolved Packet Core: Driving the Mobile Broadband Revolution, Academic Press, 2009, ISBN 978-0-12-374826-3

Slide 353

Basic elements of the Evolved Packet Core (EPC) for LTE



(inspired by Figure 3.1.1.1 of [Olsson2009])

The essential elements needed for IP connectivity from a LTE network:

- eNB = eNodeB = E-UTRAN NodeB
- MME = Mobility Management Entity
- ServGW = Serving Gateway
- PDN GW = Packet Data Network Gateway
- HSS = Home Subscriber Server

The EPC also includes the typical elements of an IPv4 **and** IPv6 network: switches, routers, DNS servers, NTP time servers, etc.

Maguire IK2555, Spring 2016 Slide 353

[Olsson2009] Magnus Olsson, Shabnam Sultana, Stefan Rommer, Lars Frid, and Catherine Mulligan, SAE and the Evolved Packet Core: Driving the Mobile Broadband Revolution, Academic Press, 2009, ISBN 978-0-12-374826-3

Slide 354

Principles guiding the EPC architecture†

Optimizing data traffic - via a flat IP architecture

- Reduce data traffic delay
- Enable very high data rates
- Facilitate scalability of the system
- Take advantage of the low cost and high performance of IP devices
- Enable internetworking with any type of access network that can support IP

Separate data and control traffic

- Enables separate scaling of infrastructure for data and control
- control traffic signaling scales with number of users or devices and their mobility
- data traffic scales with the particular services that are used and the characteristics of the devices (screen sizes, resolution, processing power, desired/expected quality of experience, …)
- Enables separate optimization of control and data traffic functions Increased flexibility in where the functionality is located
  - data traffic is kept out on the edge of the network (decreasing delays and increasing scalability)
  - control and data traffic can take different paths in the network - but both run over an underlying IP network

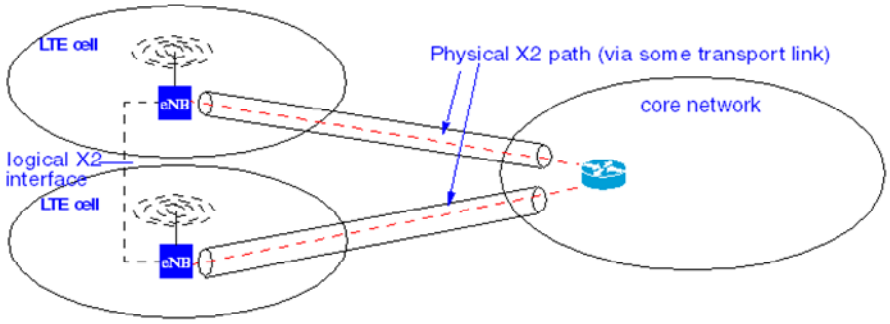
† For details see page29-31 of [Olsson2009]

Maguire IK2555, Spring 2016 Slide 354

[Olsson2009] Magnus Olsson, Shabnam Sultana, Stefan Rommer, Lars Frid, and Catherine Mulligan, SAE and the Evolved Packet Core: Driving the Mobile Broadband Revolution, Academic Press, 2009, ISBN 978-0-12-374826-3

Slide 355

X2 interface



Logical and Physical X2 interface realizations (inspired by Figure 3.1.3 of [Olsson2009])

The X2 interface allows user data traffic between mobile nodes via the core IP network (⇒ reduced delay, ⇒ reduced cost, ⇒ increased data rates and capacity).

In the core network the X2 path could go through a router or a switch.

Maguire IK2555, Spring 2016 Slide 355

[Olsson2009] Magnus Olsson, Shabnam Sultana, Stefan Rommer, Lars Frid, and Catherine Mulligan, SAE and the Evolved Packet Core: Driving the Mobile Broadband Revolution, Academic Press, 2009, ISBN 978-0-12-374826-3

Slide 356

Dual Connectivity

LTE release 12 introduce dual-layer connectivity (connectivity via both a macrocell layer and a lower power layer). [Ericsson2013]

For some of the security issues concerning dual connectivity see:

Katharina Pfeffer, Formal Verification of a LTE Security Protocol for Dual-Connectivity: An Evaluation of Automatic Model Checking Tools, Master's thesis, KTH/ICT/CoS, TRITA-ICT-EX-2014:94, July 2014

http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-148047

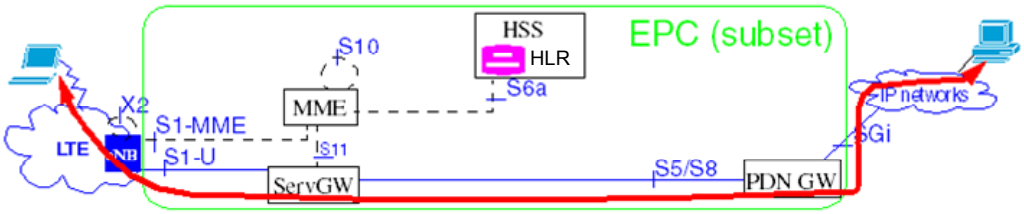
Maguire IK2555, Spring 2016 Slide 356

[Ericsson2013] Ericsson, LTE Release 12 – taking another step toward the Networked Society, Ericsson White paper, #284 23-3189 Uen, January 2013, http://www.ericsson.com/res/docs/whitepapers/wp-lte-release-12.pdf

A. Zakrzewska, D. Lopez-Perez, S. Kucera, and H. Claussen, 'Dual connectivity in LTE HetNets with split control- and user-plane', IEEE, 2013, pp. 391–396 [Online]. DOI: 10.1109/GLOCOMW.2013.6825019

Slide 357

Mobility Management Entity (MME)



MME in EPC for LTE

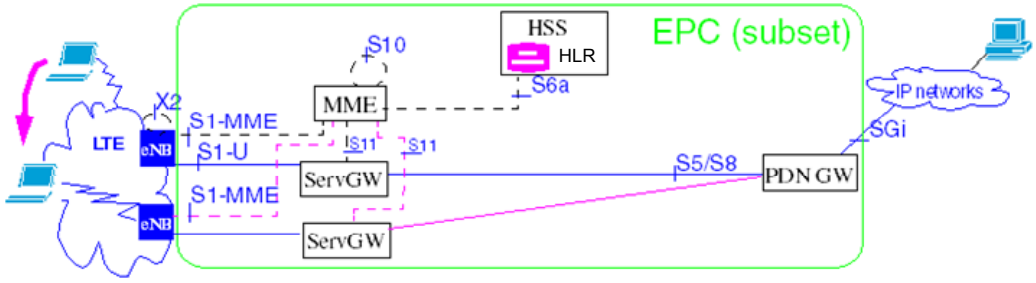
MME handles all of the control plane signaling for LTE: mobility management, security (for devices attaching to the access network), and managing device in *idle mode* (tracking and paging)

MME will authenticate devices based upon subscriber information in the HSS and will update the location information in the HSS (as part of mobility management).

All use data traffic (red path in figure) passes from the ServGW to the PDN GW - the later serves as the mobility anchor point for all external communications (hence it assigns the device its IPv4 and/or IPv6 address).

Slide 358

Mobility between two eNodeBs



Users moves and changes connectivity from one eNodeB to another

Network based mobility:

- S5 is used when the user is not roaming, while S8 is used when roaming
- The GPRS Tunneling Protocol (GTP) can be used over S5/S8 or IETF's Proxy Mobile IP (PMIPv6) [Gundavelli2008] can be used.

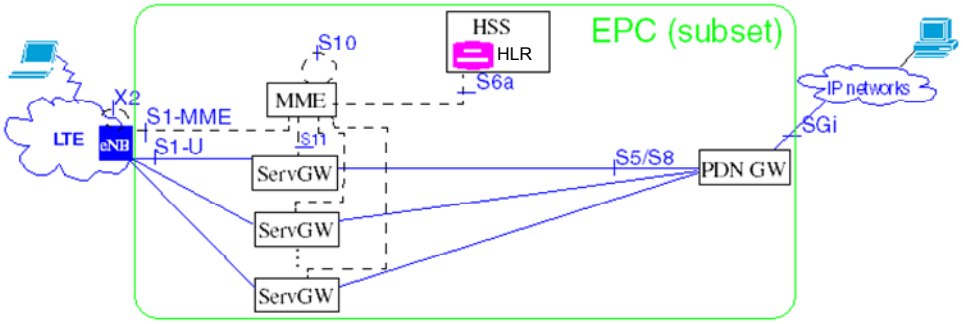
Note that the traffic continues to go through the same PDN GW.

Maguire IK2555, Spring 2016 Slide 358

[Gundavelli2008] S. Gundavelli and K. Leung and V. Devarapalli and K. Chowdhury and B. Patil, Proxy Mobile IPv6, Internet Request for Comments, ISSN 2070-1721, RFC 5213 , RFC Editor, August 2008, http://www.rfc-editor.org/rfc/rfc5213.txt

Slide 359

Scaling for more user data traffic



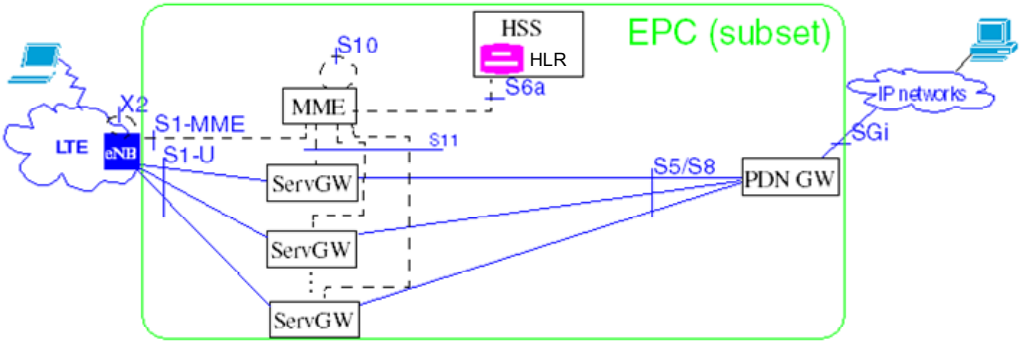
Scaling for more user traffic

Multiple ServGWs attached to a single eNodeB enables increased user data traffic:

- Necessary to meet goals of IMT-Advanced of 1 Gbps downlink and 500 Mbps uplink peak date rates
- May be necessary for some eNodeBs to due to concentration of users or to high demands by one or more users

Slide 360

Moving between ServGWs in a Pool



Scaling for more user traffic

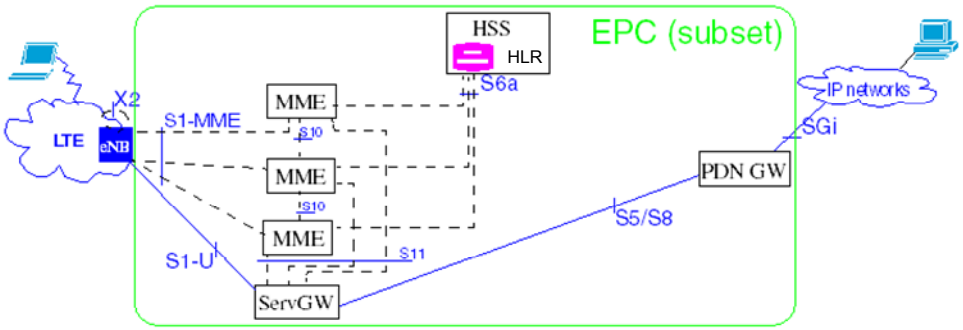
Multiple ServGWs attached to a single eNodeB enables increased reliability and facilitates maintenance.

- dynamic migration of which ServGW being used for a specific data path - to achieve QoS goals, to allow load balancing, maintenance of a ServGW, etc.
- this is an example of resource pooling

Note that the traffic continues to go through the same PDN GW.

Slide 361

Moving between MMEs in a Pool



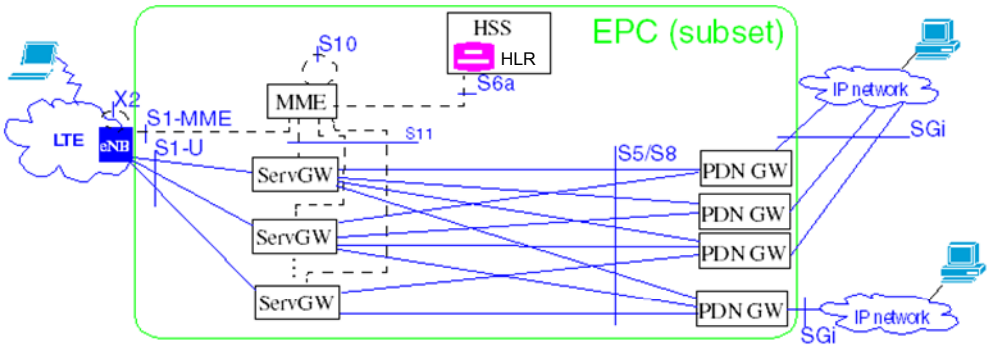
Scaling for more user traffic

Multiple MMEs attached to a single eNodeB enable increased reliability and facilitates maintenance.

- dynamic migration of which MME is being used for a specific terminal allows load balancing, maintenance of a MME, etc.
- this is an example of resource pooling

Slide 362

Multiple PDN GWs



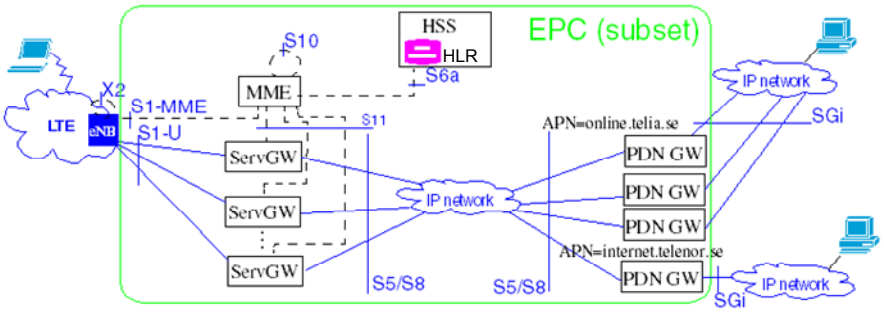
Multiple PDN GWs (logical view)

- Different PDN GWs can be used with different IP networks
- Multiple PDN GWs can be used with a single IP network
- Several logical PDN GWs can be realized in a single device
- A single logical PDN GW could be realized over multiple devices (in a distributed implementation)

Maguire IK2555, Spring 2016 Slide 362

Slide 363

Multiple PDN GWs (another view)



Multiple PDN GWs

The ServGWs and the PDN GWs are really interconnect by an IP network:

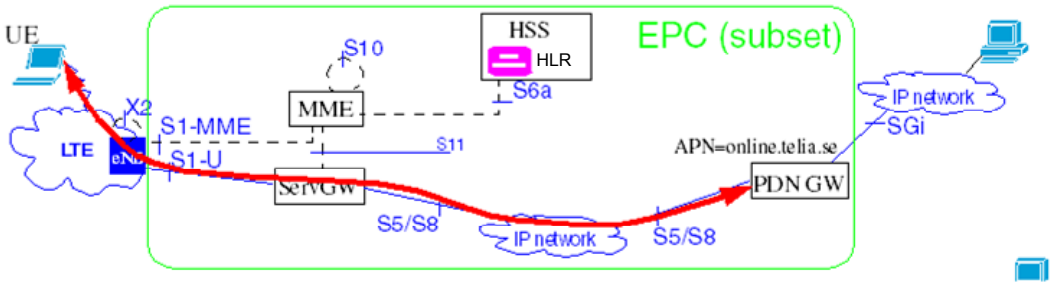
- facilitates scaling with traffic and number of gateways
- permits the different networking elements to be geographically distributed (or clustered)

⇒ offers all the advantages of an IP network

Maguire IK2555, Spring 2016 Slide 363

Slide 364

Tunneling over Core IP network



IP tunnel from UE to PDN GW

Traffic between ServGWs and PDN GWs is carried in a PDN connection (a tunnel) providing the UE with an IPv4, IPv6, or dual stack IPv4/IPv6 address (allocated by the PDN GW).

Each tunnel has a specific QoS, security, charging, policy, mobility, etc.

Slide 365

How does the UE know the address of the PDN GW?

PDN GW is identified by its access point name (APN):

- the operator's DNS will resolve this to the address of a PDN GW that this tunnel is to use
- different requests can be resolved to different IP addresses
- a default APN can be specified for each subscription in the HSS
- the IP address of the PDN GW is within the operator's internal core network (so this address is likely to be in a private IP address space)

Slide 366

How does the UE learn its IP address for a PDN connection?

The UE can learn its own address by:

- as part of the attach procedure (E-UTRAN) or Packet Data Protocol (PDP) context activation (GERAN/UTRAN)
- DHCPv4
- Stateless IPv6 autoconfiguration
  - **each** PDN connection gets a /64 prefix to which it adds its own interface identifier
  - note: this is done so there is **no** need for duplicate address detection ⇒ reduced delay before UE can begin using this address (as compared to the long wait for a typical duplicate address detection process)

When a UE uses a untrusted non-3GPP access network with dual stack mobile IPv6 (DSMIPv6) [Soliman2009] - the UE will get a Care of Address (CoA) for the IPsec tunnel to the evolved packet gateway(ePDG) and it will get an IP address for its PDN connection (this will be used as its Home Address). For details see section 6.1.1.4 of [Olsson2009].

Maguire IK2555, Spring 2016 Slide 366

[Olsson2009] Magnus Olsson, Shabnam Sultana, Stefan Rommer, Lars Frid, and Catherine Mulligan, SAE and the Evolved Packet Core: Driving the Mobile Broadband Revolution, Academic Press, 2009, ISBN 978-0-12-374826-3

[Soliman2009] H. Soliman, Mobile IPv6 Support for Dual Stack Hosts and Routers, Internet Request for Comments, ISSN 2070-1721, RFC 5555, RFC Editor, June 2009, http://www.rfc-editor.org/rfc/rfc5555.txt

Slide 367

Tracking areas

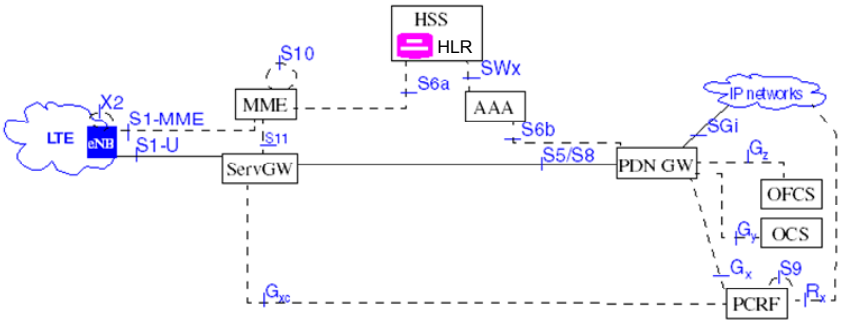
Tracking areas (a list of cell IDs) replace location areas and routing areas and adds a new feature:

UEs can have a TA list - movement within this list does not require a tracking area update (reducing the frequency and number of TA updates)

⇒ different UEs can have different TA lists, hence even correlated movement does not lead to correlated location updates (spreading the TA updates in time and area)

Slide 368

EPC (for LTE) + policy and charging elements



EPC subset for LTE (with policy and charging elements)

To enable the operator to control their network and to bill for services:

- Policy and Charging Rules Function (PCRF)
- On-line Charging System (OCS) and Off-line Charging System (OFCS))
- Authentication, Authorization, and Accounting (AAA)

Slide 369

EPS bearers

To provide the user with a specific quality of experience, EPS bearers are used to carry traffic with a specific QoS. The Policy and Charging Control system provides the QoS specification and the Traffic Flow Templates (TFTs) to be used for a given EPS bearer.

UE and PDN GW (or in some cases the ServGW) use filters based upon a TFT.
A TFT can be specified by a policy for the up-link and another TFT for the down-link.

Filter contains:

- source and destination addresses, source and destination ports, and protocol identifier (protocol number or Next header)
- optionally: IPv6 flow label, source and destination port range, IPsec parameter index (SPI), remote IP addess with a network mask

Note that the source IP address of UE need **not** be specified explicitly, as this address in implicit in the association of the TFT with the EPS bearer.

Slide 370

Interworking with lots of access networks

One of the most important aspects of the evolution has been the increasing internetworking with various types of access networks. See [Olsson2009] for the details of this for a number of the most common access networks.

[Olsson2009] Magnus Olsson, Shabnam Sultana, Stefan Rommer, Lars Frid, and Catherine Mulligan, SAE and the Evolved Packet Core: Driving the Mobile Broadband Revolution, Academic Press, 2009, ISBN 978-0-12-374826-3

Slide 371

3GPP's 5G

Dino Flore and Balazs Bertenyi, 'Tentative 3GPP timeline for 5G', 17-Mar-2015. [Online]. Available: http://www.3gpp.org/news-events/3gpp-news/1674-timeline_5g. [Accessed: 07-Jan-2016]

Target is ITU-R's IMT 2020 process

Driving forces: costs, data services, and Internet of Things

Slide 372

5G Infrastructure Public-Private-Partnership (5G PPP) www.5g-ppp.eu

Project within the EU Horizon 2020, period: 2014 to 2020
See for example: https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf

"Our key challenges for the 5G Infrastructure PPP:

- Providing 1000 times higher wireless area capacity and more varied service capabilities compared to 2010
- Saving up to 90% of energy per service provided. The main focus will be in mobile communication networks where the dominating energy consumption comes from the radio access network
- Reducing the average service creation time cycle from 90 hours to 90 minutes
- Creating a secure, reliable and dependable Internet with a "zero perceived" downtime for services provision
- Facilitating very dense deployments of wireless communication links to connect over 7 trillion wireless devices serving over 7 billion people
- Ensuring for everyone and everywhere the access to a wider panel of services and applications at lower cost"

https://5g-ppp.eu/

Maguire IK2555, Spring 2016 Slide 372

Slide 373

Further reading

Heterogeneous PCS

Ian F. Akyildiz and Wenye Wang, "A Dynamic Location Management Scheme for Next-Generation Multitier PCS Systems", IEEE Transactions on Wireless Communications, Vol. 1, No. 1, January 2002, pp. 178-189.

Janos A. Csirik, "A guide to 3GPP security documents", AT&T Research, http://www.research.att.com/~janos/3gpp.html

Slide 374

MExE

Gavin Stone, “MExE: Mobile Execution Environment”, White Paper, Ronin Wireless, MExE Forum, Dec. 2000

3GPP TS 23.057 V4.4.0 (2001-12) 3rd Generation Partnership Project Technical Specification Group Terminals Mobile Station Application Execution Environment (MExE), Functional description, Stage 2 (Release 4) http://www.3gpp.org/ftp/Specs/2001-12/Rel-4/23_series/23057-440.zip

Slide 375

Technical Specification Group Services and System Aspects (TSG SA), TSGS#19(03)0299, WG2 Meeting #20, Hämeenlinna, Finland, 09-12 June 2003 (for some more details on IMS)
http://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_20/Docs/PDF/SP-030299.pdf

Brough Turner & Marc Orange, "3G Tutorial", Originally presented at Fall VON 2002, NMS Communications, 21 December 2004
http://www.nmscommunications.com/file/3G_Tutorial.pdf

3GPP, UTRA-UTRAN Long Term Evolution (LTE) and 3GPP System Architecture Evolution (SAE), web page, last modified April 2, 2007 formerly at
http://www.3gpp.org/Highlights/LTE/LTE.htm

Ericsson, LTE Release 12 – taking another step toward the Networked Society, Ericsson White paper, #284 23-3189 Uen, January 2013,
http://www.ericsson.com/res/docs/whitepapers/wp-lte-release-12.pdf

A. Zakrzewska, D. Lopez-Perez, S. Kucera, and H. Claussen, 'Dual connectivity in LTE HetNets with split control- and user-plane', IEEE Globecom Workshops (GC Wkshps), IEEE, 2013, pp. 391–396. DOI: 10.1109/GLOCOMW.2013.6825019

Slide 376

¿Questions?

Slide 377: Lecture 6: Wireless Local Loop (WLL) and Enterprise Networks

IK2555: Mobile and Wireless Network Architectures: Lecture 6

prof. Gerald Q. Maguire Jr. http://people.kth.se/~maguire/

School of Information and Communication Technology (ICT), KTH Royal Institute of Technology

IK2555 Spring 2016 2016.01.08 © 2016 G. Q. Maguire Jr. All rights reserved.

Slide 378

6. Wireless Local Loop (WLL) and Enterprise Networks

Lecture notes of G. Q. Maguire Jr.

For use in conjunction with Yi-Bing Lin and Ai-Chun Pang, *Wireless and Mobile All-IP Networks*, John Wiley & Sons; 2005, ISBN: 0-471-74922-2.

Slide 379

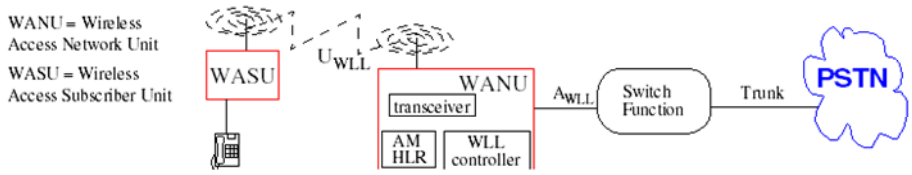
Wireless Local Loop (WLL)

Providing wireless connections to stationary or near stationary stations within a small service area

Generally targeted at the "last mile" or from a point in the neighborhood to the user Advantages of Wireless local loop:

- ease of installation
  - reducing digging, reduce poles, ducts/conduits, …
  - quick installation of new links (i.e., rapid provisioning)
  - largely distance insensitive pricing - at least up to some limit
- concentration of resources (especially at the multiplexer to the high bandwidth backbone)

IS-54 architectural reference model for WLL:



Slide 380

Deployment issues

- **Spectrum**
  - licensed - limited interference, but requires licensing
  - unlicensed - more interference, but no licensing - generally limited in (maximum and average) power
- **Service Quality**
  - Users expect it is going to be the same as wireline service
  - high reliability
  - low risk of fraud (due to others "hijacking" the link)
- **Network planning**
  - should support very high penetration levels (for example >90%)
  - exploits the fact that users are not moving (or rarely move)
  - antenna height, etc. is generally derived from user density

Very popular in the former "East block" of Europe - since there was no need to install a local loop cable to bring users to the local exchange of the PSTN; enabled very rapid provisioning to very large numbers of subscribers.

Slide 381

Wireless Local Loop Technologies

- **Satellite**
  - a great chance for the satellite operators (Hughes Network Systems, Inmarsat International Circular Orbit (ICO), Iridium, Globestar, Odyssey, American Mobile Satellite Corporation (AMSC), Asia Cellular Satellite (ACeS), Thuraya, …)
  - note that some of these operators (such as Hughes) used terrestrial versions of their system
- **Cellular-based**
  - used in rural and sparse urban settings
- **Low Tier PCS** or **Microcellular** based systems
  - PACS, PHS, DECT, …
- **Fixed Wireless Access** (FWA)
  - some times proprietary point-to-point links
  - increasingly LMDS

Slide 382

Enterprise Networks

Networking within an organization - often campus networking. Traditional voice enterprise networks were based on a PBX, today this often extended by cordless telephony, wired LANs, and WLAN systems.

Enterprise based location systems (such as Ericsson DECT mobility server, which enabled redirecting a DECT call to any Ericsson site from the user's home site).

Olivetti& Oracle Research Labs (now AT&T Research Labs) in Cambridge developed an active badge system which used IR emitting badges (called *active badges*) to locate users with in the building. This enabled delivering a phone call to the nearest fixed line phone, logging who visited who, finding people and equipment, … . A subsequent project uses ultrasound for location: *active bats*.

Theo Kanter and colleagues at Ellemtel showed a system in the mid-1990s which utilized SmartBadges (developed at KTH, HP, and Univ. of Wollongong) [Smith and Maguire2006] to locate users and by providing voice gateways the could direct a user's calls to computers, cordless, or mobile phones as appropriate.

Maguire IK2555, Spring 2016 Slide 382

[Smith and Maguire2006] Mark T. Smith and Gerald Q. Maguire Jr., SmartBadge/BadgePad version 4, HP Labs and KTH Royal Institute of Technology, http://people.kth.se/~maguire/badge4.html , June 27, 2006.

Slide 383

Cordless PBXs

For example, Ericsson's MD110 Communication System (aka "Consono") -- which is a DECT based system - simply attaches DECT base stations to their PBX.

Telia provides packages where the user can pay:

- per line/month - fixed
- per line/month - DECT (with local mobility support)
- per line/month - DECT (with mobility support over several exchanges)
- per line - DECT (with local or multiple site mobility) - but only outgoing/incoming trunk costs/month
- …

Consono information was formerly at
http://www.ericsson.com/enterprise/products/md110.shtml/index.shtml)

Slide 384

Virtual enterprise networks

By utilizing location based billing, it is possible to offer an enterprise a **virtual cellular PBX** (à la Centrex systems for fixed telephony). In such a system the operators negotiates a price for providing coverage to a campus or set of coverage areas - typically for a fixed price for a year (or more).

The operator likes this as they know they have a given amount of income and they know what their fixed costs for installing a base station to cover the relevant areas is. As a side effect they may also be able to handle calls for other users -- and not have to pay for renting antenna and other space!

Slide 385

Remoting the office to where the user is

A rapidly growing area of business utilizes Virtual Private Network technology to extend the corporate network (voice, fax, data, file system, etc.) to where the user is and via what ever communications interconnect that is available

(See for example: Ericsson's Virtual Office (EVO))

Slide 386

corDECT

A version of DECT developed by Midas Communication Technologies (http://www.midascomm.com/) and the Indian Institute of Technology, Madras ((http://www.tenet.res.in), in association with Analog Devices Inc., USA.

Provides toll-quality voice together with 35 or 70 kbps Internet service.

Utilizes the DECT air interface, but at the DECT Interface Unit (DIU) it separates the voice (which it forwards to a telephone exchange over an E1 line) and data which it passes on to an ISP. The data is sent using PPP.

For details see: Midas Communication Technologies, "corDECT Wireless Access System", December 2000 (formerly at http://www.tenet.res.in/Papers/cordect.pdf)

Broadband corDECT: up to 336 kbps
(see http://tenet.res.in/Activities/Products/doc/bbCordect.php)

Slide 387

Personal Handyphone (PHS)

Personal Handyphone System (PHS) standard [PHS] is a TDD-TDMA based microcellular wireless communications technology operating in the 1880 to 1930 MHz band.

It is used in public PHS networks, Wireless Local Loop (WLL) and Fixed Wireless Access (FWA) networks, corporate (cordless PBX), and in homes. Like DECT it uses dynamic channel allocation and provides 32 kbps bearer capability on each of the 24 TDMA frame slots. Multiple time slots can be utilized by one user, thus providing up to 128 kbps.

Maguire IK2555, Spring 2016 Slide 387

[PHS] Personal Handiphone MoU (formerly at http://www.phsmou.or.jp/)

Slide 388

Personal Access System (PAS) in China

PAS is a personal network access system that delivers wireless voice and data, based on the Personal Handyphone System (PHS) protocol. It provides both fixed and low mobility services.

PHS was enhanced by UTStar.com :

- features: Caller ID, call forwarding, voice mail
- city-wide and intercity handover and roaming services
- 32 Kbps mobile internet access
- small handsets with >800 hours of standby and ~6.5 h of talk time

Following the breakup of China Telecom, used by the wireline operators to get around the duopoly (only China Mobile and China Unicom can offer cellular services). Ministry of Information Industry (MII) in an internal notice (June 2000) will continue to allowed PAS in county-level cities and counties. In large and medium-sized cities, it may only be used "*where there is a high concentration of population, such as campuses, commercial buildings and special development zones*." While new city-wide PAS deployments will only be allowed in cities of *fewer* than two million people. [Tang and Cheung2001]

PAS is known as "xiaolingtong" in China (see [Sull 2005])

Maguire IK2555, Spring 2016 Slide 388

[Tang and Cheung2001] Joseph Tang and Florence Cheung, "The Threat of PAS in China: Impact on China Mobile and China Unicom", Sun Hung Kai Research Ltd., 3 April 2001, formerly at http://www.shkresearch.com/English/ResearchProducts/DailyProducts/sector/prc/english/20010403sector.pdf

[Sull 2005] Donald N. Sull with Yong Wang, Made In China: What Western Managers Can Learn from Trailblazing Chinese Entrepreneurs, Harvard Business Review Press, 9 June 2005, 231 pages, ISBN-13: 978-1591397151 ISBN-10: 1591397154

Slide 389

Unified Communications

- Integrated messaging
  - Cellular, cordless, fixed lines - are share the same voice mailbox, potentially with interface to e-mail, …
- Synchronizing calendars, phone books, …
- Synchronizing services across many devices (which may be using different networks)
- Ericsson's **Always Best Connected** (ABC) - to use the best technology for the current setting
- See Alexandre Kohen's master's thesis "Unified Communications with Lync 2013" [Kohen2013]

Maguire IK2555, Spring 2016 Slide 389

[Kohen2013] Alexandre Kohen, Unified Communications with Lync 2013, Master's thesis, KTH Royal Institute of Technology, Stockholm, Sweden, TRITA-ICT-EX-2013:230, October 2013 http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-129558

Interview with Mats Lundgren, Bygg UC med genomtänkt kundrelation (whole article in Swedish), TDC Ahead, Winter 2008/2009, pages 12-15. http://download.opasia.dk/pub/song-sverige/ahead/Ahead_vinter_0809_TDC.pdf

Slide 390

¿Questions?

Slide 391: Lecture 7: Wireless LAN (WLAN)

IK2555: Mobile and Wireless Network Architectures: Lecture 7

prof. Gerald Q. Maguire Jr. http://people.kth.se/~maguire/

School of Information and Communication Technology (ICT), KTH Royal Institute of Technology

IK2555 Spring 2016 2016.01.08 © 2016 G. Q. Maguire Jr. All rights reserved.

Slide 392

7. Wireless LAN (WLAN)

Lecture notes of G. Q. Maguire Jr.

For use in conjunction with Yi-Bing Lin and Ai-Chun Pang, *Wireless and Mobile All-IP Networks*, John Wiley & Sons; 2005, ISBN: 0-471-74922-2.

Slide 393

Wireless Local Area Networks (WLANs)

IEEE 802.11 Medium Access Control (MAC) protocol uses Carrier sense multiple access (CSMA) with collision avoidance (CA) medium access scheme.

IEEE 802.11b	1, 2, 5.5 and 11 Mbps - DS-SS Wireless Ethernet Compatibility Alliance certifies its members' equipment as conforming to the 802.11b standard. Compliant hardware is stamped Wi-Fi (Wireless Fidelity) compatible; operates in 2.4GHz band
IEEE 802.11g	enable data transmission speeds of up to 54 Mbps, with backwards compatibility to 802.11b infrastructure; 2.4GHz band
IEEE 802.11a	using OFDM (Orthogonal Frequency Division Multiplexing) achieves upto 54 Mbps; 5 GHz band
IEEE 802.11h	adapts 802.11a to the European HiperLAN/2 requirements; 5 GHz band
IEEE 802.11n	Amendment to IEEE 802.11-2007 called IEEE P802.11n, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Enhancements for Higher Throughput"; target maximum data rate of 248 Mbit/s (Approved October 2009)
IEEE 802.11ad	802.11ad-2012 - Amendment 3: Enhancements for Very High Throughput in the 60 GHz Band - to support upto 7 Gbit/s

Maguire IK2555, Spring 2016 Slide 393

You can get all of these standards from:
http://standards.ieee.org/getieee802/

See also: Sourangsu Banerji, 'Upcoming Standards in Wireless Local Area Networks', *Wireless and Mobile Technologies*, vol. 1, no. 1, pp. 6–11, 2013. DOI: 10.12691/wmt-1-1-2

Slide 394

IEEE 802.11-2012

802.11-2012 - IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (includes Amendments 1 to 10 published in 2008 to 2011):

http://standards.ieee.org/about/get/802/802.11.html

Slide 395

Two possible network configurations

Independent configuration	Mobile stations communicate directly to each other with no access point (base station) support, i.e., peer-to-peer (*ad hoc*) networking
Infrastructure configuration	Mobile stations communicate only via access points (APs)

In "Wi-Fi Direct" one of the devices acts as a "soft access point" – thus it use *infrastructure mode*.

See [Camps-Mur2013]

Maguire IK2555, Spring 2016 Slide 395

[Camps-Mur2013] D. Camps-Mur, A. Garcia-Saavedra, and P. Serrano, 'Device-to-device communications with Wi-Fi Direct: overview and experimentation', *Wireless Communications, IEEE*, vol. 20, no. 3, pp. 96–104, Jun. 2013. DOI: 10.1109/MWC.2013.6549288

Slide 396

Terms

Basic Service Set (BSS) - a group of stations that are under the direct control of a single coordination function (PCF or DCF)

Independent BSS (IBSS) - also known as an *ad hoc* network, defined as a BSS which exist without an access point (AP)

Infrastructure network - a network of wireless stations along with APs, which enables stations in one BSS to communicate with stations in another BSS

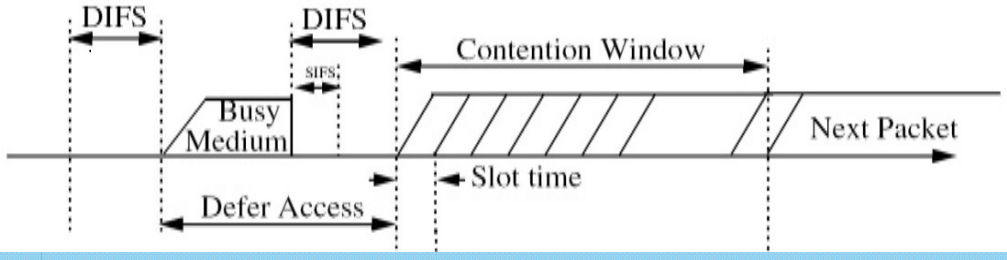
Distribution System (DS) - a backbone network between the two or more access points

Extended Service Set (ESS) a series of overlapping BSSs (each with its own AP) connected together by means of a Distribution System (DS)

Hidden node - a node is said to be hidden when its transmissions cannot be heard by some other node in the network (although it can be heard be one or more other nodes)

Slide 397

IEEE 802.11 Basic Access Method



IFS	Inter Frame spacing - during this time the medium is idle
SIFS	Short IFS - transmission after SIFS is reserved for ACKs, Clear To Send frame, or to send a fragmented MAC protocol data unit (MPDU)
DIFS	if after DCF-IFS (DIFS) a station finds the media free it can transmit a pending packet; otherwise it sets a backoff timer after selecting a random backoff value (BV) {selected from a uniform distribution over [0 .. CW-1], where CW is the width of the contention window in slots} if medium become busy before time goes off, then the value is frozen until the next DIFS interval, where upon it continues the count down CW is doubled after collisions and reset to CW_{min} after a successful transmission
EIFS	Extended IFS - used when the receiver cannot correct the received packet

Maguire IK2555, Spring 2016 Slide 397

Slide 398

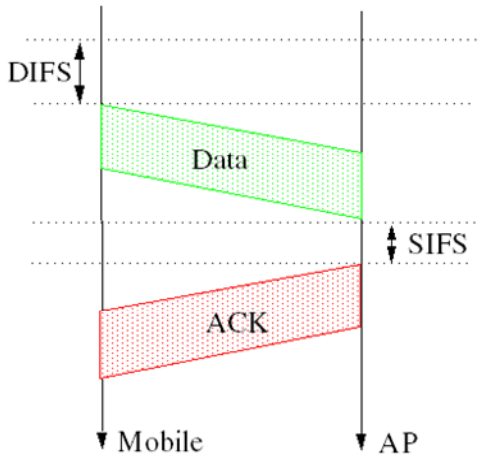
Distribution Coordinating Function (DCF)

Distribution Coordinating Function (DCF) is based on carrier sense multiple access with collision avoidance (CSMA/CA)

Receivers send an ACK if they successfully receive a packet, otherwise the transmitter re-sends.

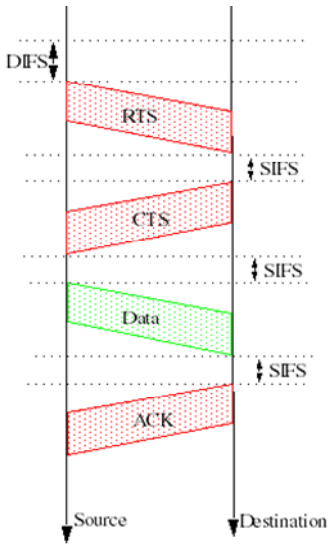
Slide 399

CSMA/CA with ACK in infrastructure network



Slide 400

IEEE 802.11 RTS/CTS mechanism



Slide 401

IEEE 802.11 Frame Format

Frame Control	2 bytes
Duration/ID	2 bytes
Address 1	6 bytes
Address 2	6 bytes
Address 3	6 bytes
Sequence Control	2 bytes
Address 4	6 bytes
Frame Body	0 .. 2312 bytes
CRC	4 bytes

Slide 402

IEEE 802.11 Frame Control

B0	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13	B14	B15
Protocol Version		Type		Subtype				To DS	From DS	More Frag	Retry	PwrMgt	More data	WEP	RSVD
2		2		4				1	1	1	1	1	1	1	1

bits

Protocol Version	currently 00, other values reserved
To DS/From DS	1 for communication between two APs
More Fragments	1 if another fragment follows
Retry	1 if packet is a retransmission
Power Management	1 if station is in sleep mode
More date	1 if there are more packets to the terminal in power-save mode
WEP	1 if data bits are encrypted

Slide 403

Uses of the four address fields

	To DS	From DS	Address 1	Address 2	Address 3	Address 4
Ad hoc mode	0	0	Destination Address	Source Address	BSSID	N/A
AP to STA	0	1	Destination Address	BSSID	Source Address	N/A
STA to AP	1	0	BSSID	Source Address	Destination Address	N/A
For bridging, relaying, etc. (called a wireless distribution system (WDS) frame in IEEE 802.11-1999)	1	1	Receiver Address	Transmitter Address	Destination Address	Source Address

Maguire IK2555, Spring 2016 Slide 403

Darwin Engwer, "WDS" Clarifications, IEEE P802.11 Wireless LANs, document number: IEEE 802.11-05/0710r0, 19 July 2005
http://www.ieee802.org/1/files/public/802_architecture_group/802-11/4-address-format.doc

See also page 2 of SANS Institute, IEEE 802.11: Pocket Reference Guide, www.sans.org
http://www.willhackforsushi.com/papers/80211_Pocket_Reference_Guide.pdf

Slide 404

Startup, then Join a network

- Turn on & discovery phase
  - determine AP or other stations exist
  - get Service Set Identification (SSID) and other parameters
- Negotiate for connection
  - Authentication & Association

Slide 405

Discovery Phase

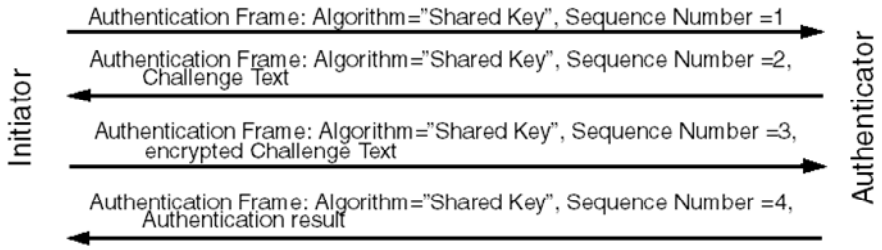
Enter scanning mode: Passive / Active scanning mode

- Passive
  - Listen for a Beacon for ChannelTime period
  - From Beacon get the SSID & parameters
- Active
  - Transmit a probe frame (including the SSID that you wish to join)
  - Wait for a period for responds by AP or other stations

Slide 406

Authentication

- Open system authentication
  - **Default** mode
  - Flow:
    - send: Authentication Frame: Algorithm = ”Open”, Sequence Number = 1
    - response: Authentication Frame: Algorithm = ”Open”, Sequence Number = 2, result=accept/reject
- Shared key authentication
  - Somewhat higher degree of security
  - Need to implement WEP
  - Flow:



Slide 407

Wire Equivalent Privacy (WEP)

IEEE 802.11 featured **Wire Equivalent Privacy (WEP)** - this proved to be rather insecure; there are efforts to fix it - but meanwhile or in any case one can use VPNs.

WEP use for data encryption & shared key authentication

- Encryption of data through RSA RC4 algorithm
- 40-bit secret key + 24-bits Initialization Vector (IV)
- IV in frame in clear text
- Integrity Check Value (ICV) included in frame
- When WEP is enabled, Shared Key Authentication is enabled

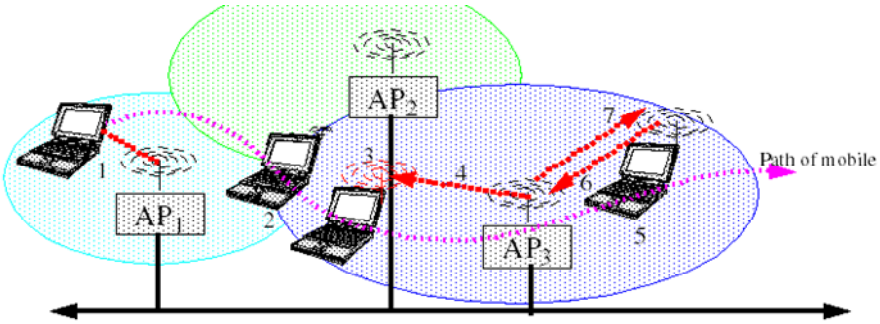
Adam Stubblefield, John Ioannidis, and Aviel D. Rubin, "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP", AT&T Labs Technical Report TD-4ZCPZZ, Revision 2, August 21, 2001 - now available at

http://web.archive.org/web/20030916024638/http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf

see also http://www.cs.umd.edu/~waa/wireless.html

Slide 408

Handoff



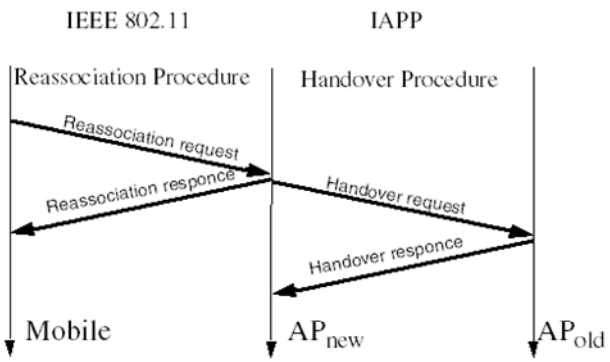
1. Mobile starts with a strong signal from AP_1
2. The signal from AP_1 is now weaker, so mobile starts to look around for a better AP
3. Mobile sends a Probe Request
4. AP_3 send probe response
5. Mobile chooses AP_3 as the best AP
6. Mobile sends Reassociation request
7. 7. AP3 sends a Reassociation Response

Maguire IK2555, Spring 2016 Slide 408

Slide 409

Inter-Access Point Protocol (IAPP)

Project 802.11f: IAPP Inter Access Point Protocol



Slide 410

Fast Handoff

- IEEE 802.11 being used in PDAs, WLAN phones, lots of new devices (especially for multimedia)
  - Multimedia applications sensitive to connectivity loss (when the loss of data exceeds that which the playout buffers can cover up)
  - TCP sensitive to multiple losses
    - Loss of an entire window causes connection to go into slow-start
- basic handoff is fast and simple, but insecure
  - Authentication occurs prior to reassociation so pre-authentication is possible
  - Management frames are not authenticated, thus no cryptographic operations in critical path
  - If APs involved in the handover use the same WEP key, no inter-AP communication is required
- Unfortunately IEEE 802.1x complicates IEEE 802.11 handoff
  - now STAs have dynamic per-session keys
  - authentication occurs **after** reassociation, not before
  - If re-authentication is required, then STAs need to complete authentication before recovering connectivity
  - Authentication and key management methods requiring public key operations (e.g. EAP-TLS) -- this can take several seconds to complete
  - Using a TLS continuation can decrease the number of round-trips (from 3.5 to 2.5)
  - if authentication server is far away, then disconnection time can be large

for further information see [Moore and Aboba 2001]

Maguire IK2555, Spring 2016 Slide 410

[Moore and Aboba 2001]Tim Moore and Bernard Aboba "Authenticated Fast Handoff", IEEE 802.11 Task group i, November 2001, doc. IEEE 802.11 submission
http://www.drizzle.com/~aboba/IEEE/11-01-TBD-I-Authenticated-FastHandoff.ppt

Slide 411

Point Coordination Function (PCF)

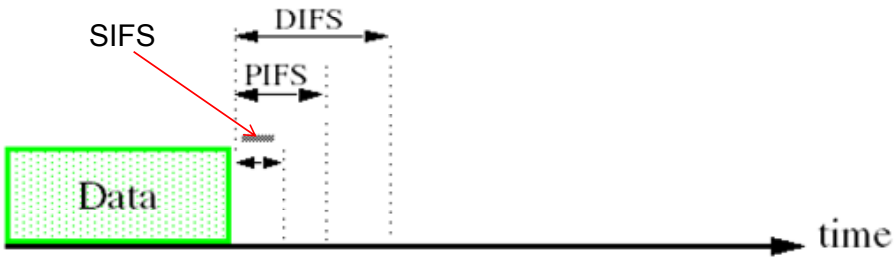
Point Coordination Function (PCF) an optional extension to DCF that provides a time division duplexing capability to accommodate time bounded, connection-oriented services.

AP polls each station:

- enabling the polled station to transmit without contending for the medium
- Contention free period repetition interval (consisting of contention free period (CFP) and contention period (CP) is initiated by the AP through a Beacon frame.
  - If AP finds the medium idle, it waits for a PCF inter frame spacing (PIFS) period of time and then transmits a beacon frame with a polling frame following SIFS seconds after it
  - when a station receives the poll from the AP, the medium is reserved for the duration of its transfer (up to the length of CFP), when the data transfer complete (or the reserved time is up), the AP waits for PIFS seconds and polls another station - it continues until the CP interval is up - then the system operates in DCF mode.
- note: AP can transmit data along with the polling frame

Slide 412

Spacing



PCF Interframe Space (PIFS)

Slide 413

Timing and Power Management

Synchronization (to within 4 µs plus propagation delay) of all clocks within a BSS maintained by periodic transmission of beacons containing time stamp info. AP (in infrastructure mode) is the timing master and generates all timing beacons.

Power saving modes:

awake STAs (aka mobiles) are fully powered and can receive packets at **any** time.

doze
- unable to transmit or receive data, but uses little power
- STA must inform the AP it is entering the doze mode, then AP does not sent packets simply buffers them
- Unicast:
  - When AP has packets queued for STAs in doze state, a traffic indication map (TIM) is broadcast as part of the timing beacon
  - STAs in the doze mode power up receivers to listen for beacons, if identified by the TIM, they return to awake mode and transmit a Power Save Poll (PS-Poll) message so the AP knows that they are ready to receive data
- Broadcast/multicast:
  - buffered broadcast/multicast packets queued in the AP are indicated in a delivery traffic indication message (DTIM) that is broadcast periodically to awaken all STAs and alert them to a forthcoming broadcast/multicast message; the message is then sent **without** the AP **waiting** for PS-Poll messages.

Slide 414

WLAN AP performance

A lot of work has been done to try to understand the details of APs, both their throughput and how they behave during a handoff. For details see:

- Enrico Pelletta's M.Sc. thesis for AP throughput measurements [Pelletta2004] and
- J-O Vatn's technical report [Vatn2003] for handoff/handover details
  - His detailed measurements present some new aspects which others had not seen

Maguire IK2555, Spring 2016 Slide 414

[Pelletta2004] Enrico Pelletta, "Maximum Throughput of IEEE 802.11 Access Points: Test Procedure and Measurements", Masters Thesis, Department of Microelectronics and Information Technology, KTH Royal Institute of Technology, 10th August 2004.https://people.kth.se/~maguire/DEGREE-PROJECT-REPORTS/040622-Enrico-Pelletta.pdf

[Vatn2003] Jon-Olov Vatn, "An experimental study of IEEE 802.11b handover performance nd its effect on voice traffic", Technical Report TRITA-IMIT-TSLAB R 03:01, Telecommunication Systems Laboratory, Department of Microelectronics and Information Technology (IMIT), KTH Royal Institute of Technology Stockholm, Sweden, July 2003. Available at *http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=30DF795425A7119F465B0C64CA4FEF7B?doi=10.1.1.10.5771&rep=rep1&type=pdf*

Slide 415

AAA: IEEE 802.1x - port-based network access control for authentication, authorization, and security [IEEE 802.1x]

IEEE Extensible Authentication Protocol

An authentication protocol which supports multiple authentication mechanisms, runs directly over the link layer without requiring IP and therefore includes its own support for in-order delivery and retransmission. Originally developed for use with PPP: Larry J. Blunk and John R. Vollbrecht, "PPP Extensible Authentication Protocol (EAP) standard", RFC 2284 [Blunk and Vollbrecht 1998].

See also Juan Caballero Bayerri and Daniel Malmkvist, "Experimental Study of a Network Access Server for a public WLAN access network", M.S. Thesis, KTH/IMIT, Jan. 2002 [Bayerri and Malmkvist 2002].

Maguire IK2555, Spring 2016 Slide 415

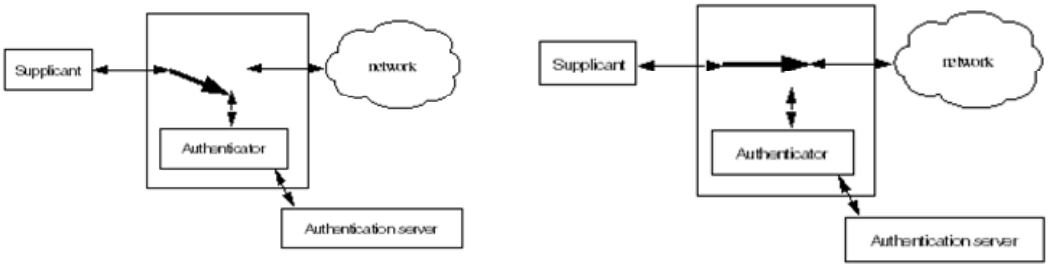
[IEEE 802.1x] IEEE 802.1x Port Based Network Access Control http://www.ieee802.org/1/pages/802.1x.html

[Blunk and Vollbrecht 1998] L. Blunk and J. Vollbrecht, 'PPP Extensible Authentication Protocol (EAP)', Internet Request for Comments, vol. RFC 2284 (Proposed Standard), March 1998, Available at http://www.rfc-editor.org/rfc/rfc2284.txt.

[Bayerri and Malmkvist 2002] Juan Caballero Bayerri and Daniel Malmkvist, *Experimental Study of a Network Access Server for a public WLAN access network*, M.S. Thesis, KTH/IMIT, Jan. 2002. was accessible from http://www.e.kth.se/~e97_dma/FinalReport.pdf

Slide 416

IEEE 802.1x



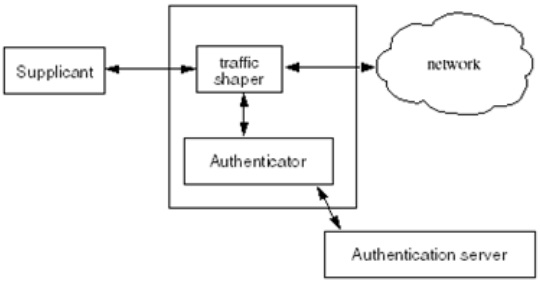
Before authentication After authentication

Supplicant is asking the **Authenticator** for access to the network, the **Authenticator** queries the **Authentication** server to determine if this supplicant should or should not have access to the network.

Slide 417

Does authentication have to occur before giving service?

Taking a page from the credit card industry and from the pre-paid cellular market, it is possible to give some service while doing the authentication
⇒ non-binary authentication



See related theses: [Zhou2008],[Zhang2009],[Guo2010]

Maguire IK2555, Spring 2016 Slide 417

[Zhou2008] Jia Zhou, "Adding bandwidth specification to a AAA Sever", Masters thesis, Royal Institute of Technology, School of Information and Communication Technology, COS/CCS 2008-19, September 2008 http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-91684

[Zhang2009] Hengchong Zhang, Non-binary Authentication: Supplicant, Masters thesis, KTH Royal Institute of Technology, School of Information and Communication Technology, COS/CCS 2009-01, February 2009 http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-91531

[Guo2010] Jia Guo, A New Authenticator: An Alternative to Binary Authentication Using Traffic Shaping, Masters thesis, Royal Institute of Technology, School of Information and Communication Technology, TRITA-ICT-EX-2010:299, November 2010 http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-28758

Slide 418

Roaming

Roaming is dependent on the underlying networks providing you service and if they are to charge -- knowing who to charge and how much to charge.

Unlike macrocellular systems where you generally only face roaming when making large scale movements (between countries or major regions of a country), in WLAN systems the intersystem movement may occur with little of no movement!

Clearinghouse

Clearinghouse to perform settlements between the various operators, see for example Excilan.

Interconnect Provider

Sören Nyckelgård, Telia's Golden Gate and its Interconnect Provider Role, Telia Golden Gate - Technical Overview, was available January 23, 2002 at http://www.telia.se/filer/cmc_upload/0/000/030/185/ResearchGoldenGateTec1Overv2.doc

Slide 419

Roaming (continued)

Martin Altinkaya and Saman Ahmedi, "SIP in an Interconnector and Service Provider Role", M.S. Thesis, KTH/IMIT, Dec. 2001.
http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-93274

[As of 2016.01.07, this thesis had been downloaded from DiVA **308,042** times!]

Since IEEE 802.11 specifies only up to the interface to the IEEE 802.2 link layer all mobility management was outside the scope of the standard.

The IEEE 802.11r task group examined fast roaming, by utilizing faster algorithms and **preauthentication** to avoid some of the performance problems which occurred - this resulted in the IEEE 802.11r Fast Roaming standard [IEEE802.11r].

Maguire IK2555, Spring 2016 Slide 419

[IEEE802.11r] IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks- Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 7: 4.9 GHz-5 GHz Operation in Japan, IEEE Standard 802.11r-2008 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008), IEEE, DOI: 10.1109/IEEESTD.2008.4573292, 2008 , 126 pages

Slide 420

Proxies

Numerous proxy based proposals exist to "improve" performance across wireless links - especially targeted to TCP (most have problems keeping TCP/IP's **end-to-end** semantics)

See:

Luis Muñoz, Marta Garcia, Johnny Choque, Ramón Agüero, and Petri Mähönen, "Optimizing Internet Flows over IEEE 802.11b Wireless Local Area Networks: A Performance-Enhancing Proxy Based on Forward Error Control", IEEE Communications Magazine, December 2001, pp. 60-67.

Slide 421

Lightweight Access Point Protocol (LWAPP)

A "thin" access point technology where control functions are centralized in switches, instead of at each access point node. Some times this is referred to as a "split MAC".

Cisco introduced its WLAN management technology called **Structured Wireless-Aware Network** solution.

For more information about LWAPP see [Cisco2005] and [RFC5412].

See also the IETF working group: Control And Provisioning of Wireless Access Points (capwap) ⇒ now Operations and Management Area Working Group (opsawg)

[Note: capwap working group has concluded its work.]

Maguire IK2555, Spring 2016 Slide 421

[Cisco2005] Cisco Systems, "Understanding the Lightweight Access Point Protocol (LWAPP)",White paper, number: 205327.CX_ETMG_LS_9.05, 2005 formerly at http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6306/prod_white_paper0900aecd802c18ee.pdf

[RFC5412] P. Calhoun, R. Suri, N. Cam-Winget, M. Williams, S. Hares, B. O'Hara, and S. Kelly, 'Lightweight Access Point Protocol', *Internet Request for Comments*, vol. RFC 5412 (Historic), Feb. 2010 [Online]. Available: http://www.rfc-editor.org/rfc/rfc5412.txt

Pat Calhoun, Lightweight Access Point Protocol (LWAPP), IETF 57, July 2003 *http://www3.ietf.org/proceedings/03jul/slides/capwap-3/capwap-3.ppt*

Slide 422

High Performance Radio LAN/2 (HiperLAN/2)

Developed by the European Telecommunications Standard Institute (ETSI) Broadband Radio Access Networks (BRAN)

- Dedicated spectrum (in Europe) at 5 GHz
- uses Orthogonal Frequency Division Multiplexing (OFDM) with 52 subchannels, 48 subchannels for data, and 4 subchannels for pilot symbols
- TDMA/TDD frames with fixed duration of 2ms
- Maximum gross data rate of 54 Mb/s
- MAC protocol was designed to support multimedia services

For more information see HiperLAN2 Global Forum and ETSI standards documents.

This was to be a competitor to IEEE 802.11, but it **failed** in the market.

Slide 423

IEEE 802.11a and 802.11h

IEEE 802.11a and ETSI's HiperLAN/2 standards have nearly identical physical layers, but are very different at the MAC level

IEEE 802.11h adds **Transmit Power Control (TPC)** to limit a device from emitting more radio signal than needed, and **Dynamic Frequency Selection (DFS)**, which lets the device listen to what is happening in the airspace before picking a channel

- TPC and DFS were introduced to satisfy European requirements
- 802.11h is to be sold under the name Wi-Fi5 (to build on the Wi-Fi branding)

IEEE 802.11 working group j to add channel selection for 4.9 GHz and 5 GHz in Japan (and to conform to the Japanese rules for radio operation) [IEEE802.11j].

Maguire IK2555, Spring 2016 Slide 423

[IEEE802.11j] IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks- Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 7: 4.9 GHz-5 GHz Operation in Japan, IEEE Standard 802.11j-2004, IEEE, DOI: 10.1109/IEEESTD.2004.95388, 2004, 40 pages

Slide 424

IEEE 802.11k

This IEEE 802 task group defined Radio Resource Measurement enhancements "to provide mechanisms to higher layers for radio and network measurements"[TG802.11k].

These enhancements will supplement the 802.11 standard(s) by:

- defining and exposing radio and network information to facilitate the management & maintenance of 802.11 networks, while
- maintaining compatibility with the IEEE 802.11 MAC

One of the measurements which they include is "location". Interestingly only the STA divulges its location (thus it can choose to divulge this information or not).

Goal: enable new applications based on this radio and network information, e.g., location-enabled services.

For details see the IEEE 802.11k-2008 standard [IEEE802.11k].

Maguire IK2555, Spring 2016 Slide 424

[TG802.11k] IEEE Task Group 802.11k http://grouper.ieee.org/groups/802/11/Reports/tgk_update.htm

[IEEE802.11k] IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 1: Radio Resource Measurement of Wireless LANs, IEEE Std 802.11k-2008 (Amendment to IEEE Std 802.11-2007), IEEE, DOI: 10.1109/IEEESTD.2008.4544755, 2008 , 244 pages

IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments

Slide 425

IEEE 802.11p

The IEEE 802.11p task group was established to address "Wireless Access for the Vehicular Environment (WAVE)"

In particular, Dedicated Short Range Communications (DSRC) [DSRC] as a general purpose communications link between the vehicle and the roadside (or even between vehicles).

For details see the IEEE 802.11p-2010 standard [IEEE802.11p] and see [Jiang and Delgrossi 2008] for an overview.

See also **platooning** [Segata2015]

Maguire IK2555, Spring 2016 Slide 425

[DSRC] Dedicated Short Range Communications, IEEE web page, accessed 2005.03.24 - formerly at http://grouper.ieee.org/groups/scc32/dsrc/index.html

[IEEE802.11p] IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments, IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009), IEEE, DOI: 10.1109/IEEESTD.2010.5514475, 2010, 51 pages

[Jiang and Delgrossi 2008] D. Jiang and L. Delgrossi, 'IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments', in *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, 2008, pp. 2036–2040. DOI: 10.1109/VETECS.2008.458

[Segata2015] M. Segata, B. Bloessl, S. Joerer, C. Sommer, M. Gerla, R. Lo Cigno, and F. Dressler, 'Toward Communication Strategies for Platooning: Simulative and Experimental Evaluation', *Vehicular Technology, IEEE Transactions on*, vol. 64, no. 12, pp. 5411–5423, Dec. 2015. DOI: 10.1109/TVT.2015.2489459

Slide 426

Multihop

Motorola (formerly MeshNetworks Inc.)

http://www.motorola.com/governmentandenterprise/northamerica/en-us/public/functions/browsesolution/browsesolution.aspx?navigationpath=id_804i/id_2523i

MeshLAN Multi-Hopping software:

- designed for use with Wi-Fi hardware
- extending useful range by adding multi-hopping peer-to-peer capabilities to off-the-shelf 802.11 cards

IEEE 802.11s (ESS Mesh Networking) standard [IEEE802.11s] is emerging to manage wireless backhaul links and to support mesh networks.

Maguire IK2555, Spring 2016 Slide 426

[IEEE802.11s] IEEE Standard for Information Technology -- Telecommunications and information exchange between systems -- Local and metropolitan area networks-- Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 10: Mesh Networking, IEEE Std 802.11s-2011 (Amendment to IEEE Std 802.11-2007 as amended by IEEE 802.11k-2008, IEEE 802.11r-2008, IEEE 802.11y-2008, IEEE 802.11w-2009, IEEE 802.11n-2009, IEEE 802.11p-2010, IEEE 802.11z-2010, IEEE 802.11v-2011, and IEEE 802.11u-2011), IEEE, DOI: 10.1109/IEEESTD.2011.6018236, 2011 , 372 pages

Survey article:

I. F. Akyildiz, X. Wang, and W. Wang, 'Wireless Mesh Networks: A Survey', *Comput. Netw. ISDN Syst.*, vol. 47, no. 4, pp. 445–487, Mar. 2005. DOI: 10.1016/j.comnet.2004.12.001

Slide 427

QDMA (quad-division multiple access)

Motorola (formerly MeshNetworks) QDMA proprietary radio technology was developed (by ITT Industries (www.itt.com)) for and currently used by the military.

- IP from end to end
- supports high-speed mobile broadband access
- infrastructure-free, i.e., ad hoc peer-to-peer networking

Claims they can deliver up to 6 Mbps to each user in a QDMA wireless network.

Products have built-in GPS (Global Positioning System) capabilities and QoS for IP voice and video.

First implemented in 2.4GHz as prototype routers, relays, and PDA-size client devices; now developing equipment for Multichannel Multipoint Distribution Service (2.5GHz) licensed operators.

They had FCC experimental license to build a (US) nationwide 4,000-node test network.

Slide 428

Wireless Internet Service Providers (WISPs)

- **Location specific** WISP - exploiting high value sites (airports, hotels, coffee shops, …)

  Advantages: often have "exclusive" offering

  Disadvantages: users may also want access in other locations -- hence roaming agreements will be important
- **Single site** or **campus** WISP - a subset of the location specific WISP category (e.g., university or corporate campus, a single conference center/exhibition hall)

  Advantages: they know the site very well, generally they have "exclusive" offering, users are trapped - so they will have to pay and pay and pay or it is part of the tele/datacom offering

  Disadvantages: for some sites the users are only there for a short period (hours to days), very high turn over in users (so low administrative costs are very important); in university and corporate campus settings very high demands/expectations

Slide 429

WISPs (continued)

- **Mobile carrier** WISP - mobile (wireless wide area network - WWAN) operator also offering WLAN

  Advantages: they know where their users spend time (from their existing traffic and location data) so they can easily build out hotspots; retain customers with whom they already have a billing relationship

  Disadvantages: offering WLAN might reduce their income (as they might have been able to charge (a lot) for the traffic via the WWAN in these same spots)
- **ISP WISP** - existing ISP that extends their network via WLAN access points

  Advantages: pretty straight forward extension of their existing network, by shipping dual xDSL/cable/… + AP devices†; retain customers with whom they already have a billing relationship

  Disadvantages: offering WLAN might reduce their income since neighbors can share rather than installing their own service
- **WISP** - a pure wireless internet service provider

  Advantages: this is their business

  Disadvantages: this is their business but they depend on an ISP for back haul

† Actiontec Electronics

Slide 430

WISPs (continued)

- **Operator Neutral** WISP - an Internet eXchange (IX) to which several independent ISPs (or WISPs) are connected
  Advantages: enable multiple operators
- **Franchising** WISP
  Advantages: they simply sell the idea, starter kit, supply backup support, …
  Disadvantages: dependent on getting a cut from the franchise
- **Virtual** WISP - no actual network, … - but rather they simply rent/buy capacity for their users; thus their major role is to support and bill users
  Advantages: very low to near zero costs for infrastructure
  Disadvantages: they must provide either high service level and/or low prices to retain their customers
- **Community/Grassroots** WISP - altruistic providers
  Advantages: people making their WLAN available to others "because it is the right thing to do"
  Disadvantages: Support way or many not exist

Herslow, Navarro, and Scholander [Herslow2002] classify the WISPs based on whether they are "for fee" or for "free" and coverage area: hotspot vs. wide area.

Maguire IK2555, Spring 2016 Slide 430

[Herslow2002] Louise Herslow, Carl-Johan Navarro, and Joakim Scholander, "Exploring the WISP Industry - Analysing Strategies for Wireless Internet Service Providers", Masters thesis, Institute of Economic Research, Lund University, Sweden, January 2002. was accessible from http://www.scholander.com

Slide 431

IEEE 802.11v

IEEE 802.11v enables configuration of IEEE 802.11 devices, including information about the network's topology, RF environment, etc.

For details see IEEE 802.11v-2011 [IEEE802.11v]

[IEEE802.11v] IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: IEEE 802.11 Wireless Network Management, IEEE Std 802.11v-2011 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11w-2009, IEEE Std 802.11n-2009, IEEE Std 802.11p-2010, and IEEE Std 802.11z-2010), IEEE, DOI: 10.1109/IEEESTD.2011.5716530, 2011, 433 pages

Slide 432

IEEE 802.11z

When data is to go between two clients in a cell, rather than going via the access point, IEEE 802.11z describes how to set up a direct link between the clients (while remaining associated with a given access point (AP)).

Note: Both devices have to be associated with the same AP

Tunneled Direct Link Setup (TDLS) is a client only mechanism. For details see the IEEE 802.11z standard [IEEE802.11z].

Maguire IK2555, Spring 2016 Slide 432

[IEEE802.11z] IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 7: Extensions to Direct-Link Setup (DLS), IEEE Std 802.11z-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11w-2009, IEEE Std 802.11n-2009, and IEEE Std 802.11p-2010), IEEE, DOI: 10.1109/IEEESTD.2010.5605400, 2010, 96 pages

Slide 433

Further reading

WISPs

David Alvén and Reza Farhang, "Does it take a WISP to manage a wisp of hotspots? - Analysis of the WLAN market from a WISP perspective", Masters Thesis, Department of Microelectronics and Information Technology, Royal Institute of Technology, Sweden, February 2002. was accessible from http://www.e.kth.se/~e96_rfh/wisp_analysis.pdf

IEEE 802.11

see http://www.wi-fiplanet.com/

Slide 434

Misc.

Rusty O. Baldwin, Nathaniel J. Davis IV, Scott F. Midkiff, and Richard A. Raines, "Packetized Voice Transmission using RT-MAC, a Wireless Real-time Medium Access Control Protocol, Mobile Computing and Communications Review, V. 5, N. 3, July 2001, pp. 11-25.

P802.11i, (D8) Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems-LAN/MAN Specific Requirements-Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security, IEEE, 2004, 177 pages.

Guillaume Collin and Boris Chazalet, Exploiting cooperative behaviors for VoIP communication nodes in a wireless local area network, 1F1421 Project report, August 2007, http://people.kth.se/~maguire/.c/DEGREE-PROJECT-REPORTS/070816-Boris-Chazalet_and_Guillaume-final-report.pdf

Slide 435

¿Questions?

Slide 436: Lecture 8: Bluetooth: Piconets and Scatternets

IK2555: Mobile and Wireless Network Architectures: Lecture 8

prof. Gerald Q. Maguire Jr. http://people.kth.se/~maguire/

School of Information and Communication Technology (ICT), KTH Royal Institute of Technology

IK2555 Spring 2016 2016.01.08 © 2016 G. Q. Maguire Jr. All rights reserved.

Slide 437

8. Bluetooth: Piconets and Scatternets

These lecture notes are based on material from:

"Bluetooth: Part 1: Overview", Kjell Jørgen Hole <Kjell.Hole@ii.uib.no>, Norwegian University of Science and Technology, UiB, formerly at http://www.kjhole.com/Standards/BT/BTdownloads.html

which is in turn based on Chapters 1, 2, and 3 of:

Jennifer Bray and Charles F. Sturman, Bluetooth 1.1: Connect Without Cables, 2nd edition, Prentice Hall, 2001, 624 pages, ISBN-10: 0130661066, ISBN-13: 978-0130661067

C. Bisdikian, "An overview of the Bluetooth Wireless Technology", IEEE Communications Magazine, pp. 86-94, Dec. 2001.

Bluetooth specification, http://www.bluetooth.com

Slide 438

Bluetooth

Bluetooth name comes from Danish king Harald Blåtand (Bluetooth), credited with uniting the Scandinavian people during the 10th century.

The idea was that Bluetooth wireless technology would unite personal computing devices.

Slide 439

Bluetooth®

Bluetooth® is a trademark owned by the Bluetooth SIG, Inc., USA.

The Bluetooth Special Industry Group (SIG) formed in Winter of 1998 by Ericsson, IBM, Intel, Nokia, and Toshiba.

Goals

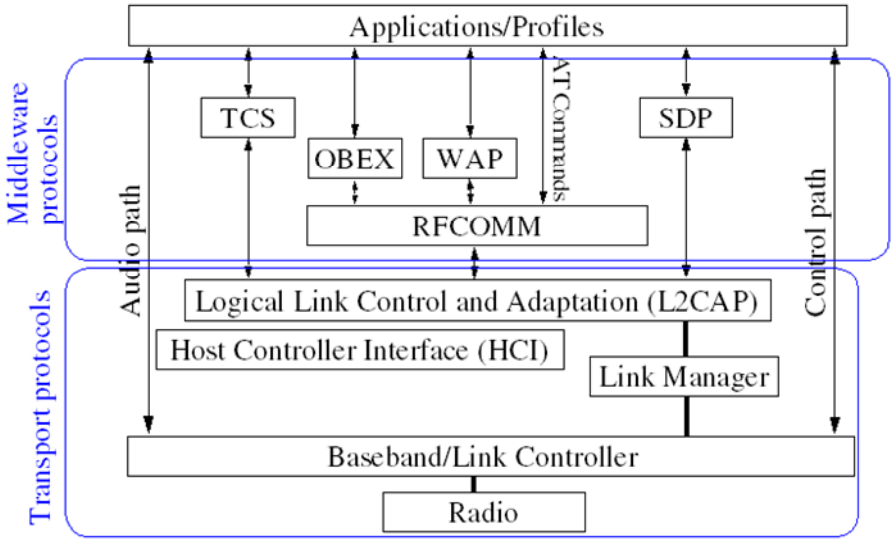
- low cost
- low power
- primarily a cable replacement (to connect mobile phones to headsets)
  - There are those who believe it can be used as a Wireless Personal Area Network (WPAN), hence it was the basis for IEEE 802.15.

Using:

- short-range radio technology
- *ad hoc* networking
- dynamic discovery of other Bluetooth devices & the services they offer

Slide 440

Bluetooth protocol stack



Slide 441

Physical Layer

- Uses 2.4 GHz unlicensed Industrial, Scientific, and Medical (ISM) band (as globally portions of this band are available)
  - many other systems using the same spectrum
    - interference to other systems
    - interference from other systems
  - 2.400-2.4835 GHz, i.e., 83.5 MHz divided into 79 channels with carrier frequencies f = 2402 +k MHz, k = 0, … , 78; Channel spacing is 1 MHz
  - Gaussian Frequency Shift Keying (GFSK) modulation with one bit per symbol
- uses fast (1600 hops/s) frequency hopping spread spectrum (FHSS)
  - 625 microsecond long time slots
  - one hop per packet, but a packet can be 1 slot, 3 slots, or 5 slots long

Maguire IK2555, Spring 2016 Slide 441

Slide 442

Transmit Power

- Low transmit power
- original goal was a 10m radius of operation, but some thought about using Bluetooth for longer ranges ⇒ Transmit Power Classes

Class	Max. output power	Range	Power control
1	100 mW (20 dBm)	100m+	mandatory
2	2.5mW (4 dBm)	10m	optional
3	1 mW (0 dBm)	1m	optional

- most manufacturers produce Class 3 radios
- power control is to reduce both interference and power consumption

Slide 443

Masters versus Slaves

Each Bluetooth device is a Master or Slave†:

- master initiates exchange of data and the slave responds to the master
- in order to communicate devices must use same sequence of frequency hops, hence slaves synchronize to hop sequence of master
- master assigns an **A**ctive **M**ember **add**ress (AM_ADDR) to the slaves participating in active communications within the piconet

Additional devices may be registered with the master and be invited to become active as necessary -- their state is called "**parked**"

Devices not currently associated with any piconet are in **stand-by mode**.

† Version 4.1 of the specification introduces a third alternative: "listening devices"

Slide 444

Frequency Hop Sequence

Each device has a 48 bit IEEE MAC address (called a Bluetooth device address (BD_ADDR)) and a local free-running 28-bit clock that ticks once every 312.5 μs (which corresponds to half the residence time in a frequency when the radio hops at the nominal rate of 1,600 hops/sec.)

Each slave receives the master's address and clock, then uses this to calculate frequency hop sequence

Slide 445

Time Division Multiplexing (TDM)

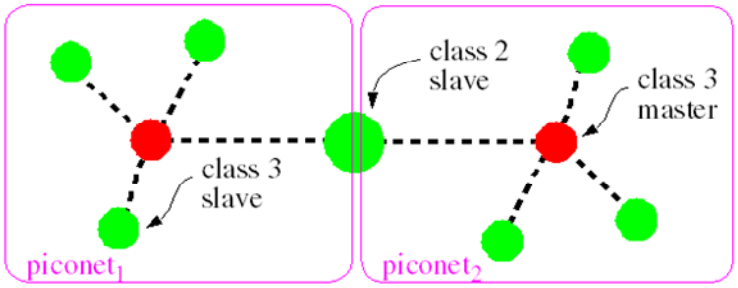
Divide the total bandwidth between Bluetooth devices using a given hop sequence

- Master assigns time slots to slaves
- packets are joined together in transmit and receive pairs; master and slaves alternate in time-division duplex (TDD)

Slide 446

Network Topology

Piconet	• slaves only communicate with the master • maximum of 7 slaves in a piconet (as there are only 3 address bits!)
Scatternet	multiple Bluetooth piconets joined together by devices that are in more than one piconet • Routing of packets between piconets is not defined)



Slide 447

Scatternets

If a device is present in more than one piconet, it must time-share, spending a few slots in one piconet and a few slots in the other

A device may not be master of two different piconets since all slaves in a piconet are synchronized to the **master's** hop sequence, thus if the slaves were all synchronized with a single master -- they would be part of the **same** piconet!

This means that piconets making up a scatternet do **not** coordinate their frequency hopping ⇒ unsynchronized piconets in an area will randomly collide on the same frequency.

Slide 448

Voice + Data support

As an important application of Bluetooth was a cable replacement between handset and headset and this was developed in a telecom company's development lab ⇒ synchronous voice support was the focus of the link protocol design

- Synchronous Connection Oriented (SCO) links for voice
  - circuit-switched connections - 64 kbps in each direction per voice channel (using their own voice coding or) using reserved slots
  - up to three voice channels active at one time (may be to 1, 2, or 3 slaves)
  - ~78% overhead for data! (this is without FEC)
- Asynchronous Connectionless (ACL) links for data
  - ACL Data Packets: 72-bit access code, 54-bit header, 16-bit Cyclic Redundancy Checksum (CRC), and varying amount of data
  - with largest packet (Data High rate, DH5, packet stretching over five slots) ⇒ maximum data rate of ~650 kbps
  - a best effort delivery service - maintains integrity by using retransmissions and sequence members, as well as forward error correction (FEC) **if** necessary
  - a master can have an ACL link to each of several slaves, but only one per slave
  - Broadcast packets: packets that are not addressed to a specific Slave

Maguire IK2555, Spring 2016 Slide 448

Bluetooth 4.1 enables a Wide Band Speech (WBS) CODEC to be added to a chip implementing Bluetooth

Slide 449

Baseband

Baseband controls the radio and is responsible for low level timing, error control, and management of link during a single data packet transfer

Packet types:

- SCO, ACL - carrying payload
- ID packet consists of access code, used during re-connection
- NULL packet consists of access code and header, used for flow control or to pass ARQ
- POLL packet same structure as NULL packet, must be acknowledged
- FHS (Frequency Hop Synchronization)

Slide 450

Baseband Packet formats

LSB				MSB
ID	AC			
(bit count)	68 or 72			
POLL/NULL	AC	BB_Header		
	68 or 72	54 (1/3 FEC)[a]		
FHS	AC	BB_Header	FHS payload	
	68 or 72	54 (1/3 FEC)	240 (2/3 FEC)	
ACL/SCO	AC	BB_Header	ACL or SCO payload	
	68 or 72	54 (1/3 FEC)	0-2744 ({1,2,3[b]}/3 FEC)	
DV	AC	BB_Header	SCO payload	ACL payload
	68 or 72	54 (1/3 FEC)	80	32-150 (2/3 FEC)

a. 54 bits includes the FEC bits (there are 18 bits of information with each bit repeated 3 times)

b. 3/3 FEC implies no FEC

Maguire IK2555, Spring 2016 Slide 450

Slide 451

Baseband Packet formats

AC	⇒	preamble	sync word		trailer
Access code		4	64		4
BB_Header	⇒	AM_ADDR[a]	PDU_TYPE	Flags[b]	HEC[c]
BaseBand header		3	4	3	8
SCO payload	⇒	SCO Data[d]			
ACL payload	⇒	ACL_pld_hdr[e]	ACL_pld_body		CRC

a. Broadcast packet has address zero

b. Flow (= 1 means receive buffer is full), ARQN (ACK represented by ARQN = 1 and NAK by ARQN = 0), SEQN (alternating bit)

c. Header error check (HEC)

d. 30 bytes (240 bits), error control code with rate 1/3, 2/3, or 1 (no FEC) used for source data size of 10, 20, or 30 bytes; note BB_Header flags for ARQN and SEQN are not used - since there is no flow control or retransmission, similarly the HEC is not used

e. L_CH (Logical CHannel) Field (3 bits) indicates whether payload is start or continuation of message, Flow field (1 bit) controls for data transfer at L2CAP level, Length field (8 bits) indicates the number of data bytes in the payload' header ends with 4 undefined bits

Slide 452

Synchronization Word Algorithm

1. Get 24-bit Lower Address Part (LAP) of Bluetooth device address (48 bit IEEE MAC address)
2. Append 6-bit Barker sequence to improve auto-correlation properties
3. XOR with bits 34 to 63 of full length, 64-bit Pseudorandom Noise (PN) sequence
4. Encode resulting 30-bit sequence with (64,30) Bose-Chaudhuri-Hocquenghem (BCH) block code to obtain 34 parity bits
5. 34-bit parity word XOR'd with the remaining bits, 0 to 33 of PN sequence to remove cyclic properties of block code

Note: 34 bits BCH parity word exhibits **very high auto-correlation** and **very low co-correlation** properties, therefore a correlator can be used to obtain a match between the received and expected (reference) synch word

Slide 453

Security

Some think that the high speed, pseudo-random frequency hopping algorithm makes it difficult to listen in on a connection - but of course this is false, because once you know the master's MAC address and clock you can calculate the next hop too!

Authentication and negotiation for link encrypting are both part of the Link Manager Protocol (LMP) specification.

- authentication is based on a challenge/response mechanism based on a common shared secret, a link key is generated through a user-provided PIN
- link level encryption using a public domain cipher algorithm SAFER+† generates 128-bit cipher keys from 128-bit plain text
- Version 4.1 introduces 128 bit AES encryption

† J. L. Massey, On the Optimally of SAFER+ Diffusion, formerly available at http://csrc.nist.gov/encryption/aes/round1/conf2/papers/massey.pdf

Slide 454

Link Control Protocol (LCP)

- configures and controls baseband
- packet level access control - determines what packet is going to be sent next
- high level operations: inquiry and paging
- configures and controls multiple links between devices and piconets
- does **not** require its own packets, but uses the (ARQN and SEQN) bits in baseband packets for SCO and ACL links to signal between link controllers - thus forming a logical LC (Link Control) channel

Slide 455

Link Control states

State	Description
Standby	inactive, radio not switched on
Inquiry	device tries to discover all Bluetooth enabled devices in the close vicinity; uses a special fast hopping sequence; FHS packets with device information, such as clock, frequency hop sequence, and BD_ADDR, received from available devices; ⇒ a list of all available devices
Inquiry Scan	devices periodically enter the inquiry scan state to make themselves available to inquiring devices; a special slow hopping sequence used
Page	master enters page state and transmits paging messages to slave using access code and timing information which it learned earlier
Page Scan	device periodically enters page state to allow paging devices to establish connections
Connection-Active	Slave synchronizes to master's frequency hop and timing sequence. Master transmits a POLL packet to verify link, Slave sends NULL packet in reply
Connection-Hold	device ceases to support ACL traffic for a period of time, keeps Active Member address (AM_ADDR)
Connection-Sniff	device listens in pre-defined time slots only
Connection-Park	device listens for traffic only occasionally, gives up its AM address

Maguire IK2555, Spring 2016 Slide 455

Slide 456

Link Manager

Translates commands from **Host Controller Interface** (HCI) into operations at baseband level to implement the following operations:

- attaching Slaves to a piconet, and allocating active member addresses (AM addr)
- tearing down connections when slaves leave piconet
- configuring links, e.g., controlling Master/Slave switches
- establishing ACL and SCO links
- putting connections one of the low-power modes
- communicates with other LMs using the **Link Management Protocol** (LMP) which is a set of messages, or **Protocol Data Units** (PDUs), whose payloads contain the following fields:
  - single bit Transaction Identifier equal to 0 (1) for PDU sent from Master (Slave)
  - Operation Code (OpCode) defining type of message being sent
  - message parameters
  - PDUs sent as single slot packets on link management logical channel (L_CH = 3)

Slide 457

Host Controller Interface (HCI)

- interface between a host and a Bluetooth module
- having a standard interface enables Baseband and Link Manager to run on a processor in the Bluetooth module while higher layers and applications running on host
- Bluetooth module can wake the host via a message across this interface

Slide 458

HCI Transport Layer

Three different transport interfaces are defined to transfer HCI packets from the host to the Bluetooth module:

USB	Universal Serial Bus
RS-232	serial interface with error correction
UART	Universal Asynchronous Receiver Transmitter, a serial interface without error correction

Slide 459

Logical Link Control and Adaptation Protocol (L2CAP)

L2CAP only transfers data and all applications **must** use L2CAP to send data. provides:

- multiplexing to allow several higher layer links to pass across a single ACL connection
- segmentation and reassembly to allow transfer of packets larger than lower layers support
- Quality of Service (QoS) management for higher layer protocols

Slide 460

L2CAP Signaling

labels packets with channel numbers

L2CAP entities communicate with each other using control channels with a special channel number (used for connecting, configuring, and disconnecting L2CAP connections)

packet contains a length field (2 bytes), a channel identifier (2 bytes), and a data field (0 .. 65535 bytes)

Slide 461

L2CAP Command

More than one command can be sent within a L2CAP packet

OpCode	identifying contents of command
Identifier	used to pair up requests and responses
Length	of data field

Slide 462

Configuring a Connection

Parameters which can be configured are:

- Maximum Transmission Unit (MTU) < 65,535 bytes
- Flush timeout -- time (in milliseconds) a device will spend trying to transmit an L2CAP packet before it gives up
- QoS option can select best effort, or a guaranteed QoS

Slide 463

Disconnecting and Timeouts

Two ways for an L2CAP channel to be closed down:

- disconnection request from higher layer protocol or service
- time out: every time L2CAP sends a packet, a Response Timeout Expired (RTX) time is started; if the RTX timer expires before a response is received, the channel may be disconnected

Slide 464

For A to talk to B

Step 1: Discovering a Bluetooth device:

device A transmits one or more inquiry packets† device B replies with Frequency Hop Synchronization (FHS) packet which contains device class information (including its BD_ADDR)

Step 2: Connecting to service discovery database:

- ACL baseband connection is established
- Logical Link Control and Adaptation Protocol (L2CAP) connection is set up over ACL channel
- L2CAP adds Protocol and Service Multiplexor (PSM) to L2CAP packets to distinguish between different higher layer protocols and services (PSM=0x0001 for service discovery)
- Service Discovery Protocol (SDP) connection over L2CAP channel
- device A receives Dial-Up Networking (DUN) info from B's service discovery database
- device A disconnects

Step 3: Connecting to Bluetooth service:

- ACL link is set up
- device A utilizes Link Management Protocol (LMP) to configure link
- L2CAP connection using the RFCOMM protocol (RS-232 serial cable emulation) is set up (PSM=0x003)
- DUN connection is set up using RFCOMM connection

† A piconet master may explicitly page devices to join its piconet; if it knows their BD_ADDR it can skip the inquiry process and directly paging the device

Slide 465

Service Discovery Protocol (SDP)

- only provides information about services, does not provide access to these services
- “optimized” for usage by devices with limited capabilities over wireless links
  - uses binary encoding of information
  - unique identifiers (UUIDs) describe services and attributes of these services such that you do not need a central registration authority for registering services
  - generally UUIDs are 128 bits long; however, for known services 16-bit and 32-bit UUIDs may also be used.

Slide 466

RFCOMM Protocol

- provides a serial interface over the packet-based transport layers
- emulates the signals on the nine wires of an RS-232 cable
- based on the ETSI 07.10 standard (also used by GSM terminals), allows multiplexing (via L2CAP) several serial ports over a single transport
  - supports flow control on individual channels
  - has a reserved Protocol and Service Multiplexer (PSM) value used by L2CAP to identify RFCOMM traffic
- no error control
- enables legacy applications -- written to operate over serial cables -- to run without modification

Slide 467

RFCOMM Frame Types

Five frame types (the first 4 are control frames):

SABM	Start Asynchronous Balanced Mode (startup command)
UA	Unnumbered Acknowledgement (response when connected)
DISC	Disconnect (disconnect command)
DM	Disconnected Mode (response to a command when disconnected)
UIH	Unnumbered Information with Header check • each RFCOMM channel has a Data Link Connection Identifier (DLCI) • UIH frames with DLCI = 0 are used for control messages, while DLCI ≠ 0 are used data

Slide 468

Telephony Control Signaling (TCS) Protocol

TCS-AT	Telephony control can be performed using the AT command set use the RFCOMM to send and receive control signaling based on the AT command set (for example to implement a dialer application)
TCS-BIN	(BIN stands for the binary encoding of information) Runs directly on top of L2CAP; supports normal telephony control functions such as placing and terminating a call, sensing ringing tones, accepting incoming calls, etc. TCS-BIN supports point-to-multipoint communications as well, for example, a cordless base station can pass the ringing signal of an incoming call to several cordless headsets associated with the base station

Slide 469

Bluetooth Profiles

- specifications for building interoperable applications
- All profiles depend on the Generic Access Profile (GAP) -- defines the basic rules and conditions for connecting devices with each other and establishing Bluetooth links and L2CAP channels.

Profile	Description
serial port profile	defines how RFCOMM runs on top of the Bluetooth transport protocols
generic object exchange profile	defines how objects can be exchanged using the OBEX protocol running on top of RFCOMM

more profiles - such as LAN access

Slide 470

Traditional Profiles

3DSP	3D Synchronization Profile	HFP	Hands-Free Profile
A2DP	Advanced Audio Distribution Profile	HID	Human Interface Device Profile
AVRCP	A/V Remote Control Profile	HSP	Headset Profile
BIP	Basic Imaging Profile	MAP	Message Access Profile
BPP	Basic Printing Profile	MPS	Multi Profile Specification
DI	Device ID Profile	OPP	Object Push Profile
DUN	Dial-Up Networking Profile	PAN	Personal Area Networking Profile
FTP	File Transfer Profile	PBAP	Phone Book Access Profile
GAVDP	Generic A/V Distribution Profile	SAP	SIM Access Profile
GNSS	Global Navigation Satellite System Profile	SDAP	Service Discovery Application Profile
GOEP	Generic Object Exchange Profile	SPP	Serial Port Profile
HCRP	Hardcopy Cable Replacement Profile	SYNCH	Synchronization Profile
HDP	Health Device Profile	VDP	Video Distribution Profile

Maguire IK2555, Spring 2016 Slide 470

https://www.bluetooth.org/en-us/specification/adopted-specifications

Slide 471

Generic Attribute Profile (GATT) Specifications

ANP	Alert Notification Profile	HTP	Health Thermometer Profile
ANS	Alert Notification Service	HTS	Health Thermometer Service
BAS	Battery Service	IAS	Immediate Alert Service
BLP	Blood Pressure Profile	LLS	Link Loss Service
BLS	Blood Pressure Service	LNP	Location and Navigation Profile
CPP	Cycling Power Profile	LNS	Location and Navigation Service
CPS	Cycling Power Service	NDCS	Next DST Change Service
CSCP	Cycling Speed and Cadence Profile	PASP	Phone Alert Status Profile
CSCS	Cycling Speed and Cadence Service	PASS	Phone Alert Status Service
CTS	Current Time Service	PXP	Proximity Profile
DIS	Device Information Service	RSCP	Running Speed and Cadence Profile
FMP	Find Me Profile	RSCS	Running Speed and Cadence Service
GLP	Glucose Profile	RTUS	Reference Time Update Service
GLS	Glucose Service	ScPP	Scan Parameters Profile
HIDS	HID Service	ScPS	Scan Parameters Service
HOGP	HID over GATT Profile	TIP	Time Profile
HRP	Heart Rate Profile	TPS	Tx Power Service
HRS	Heart Rate Service		

Maguire IK2555, Spring 2016 Slide 471

Slide 472

Management

- needed to manage links, but not defined by Bluetooth spec!
- could provide fault, accounting, configuration, performance, and security management
- link level encryption using a public domain cipher algorithm SAFER+ generates 128-bit cipher keys from 128-bit plain text

Slide 473

Low Power Modes

sniff mode	a slave agrees with its master to periodically listen for the master's transmissions; the period is configured through LMP transactions
hold mode	a device (in a piconet) agrees to remain silent (in that particular piconet) for a given amount of time; note: keeps its temporary address, AM_ADDR
park mode	a slave device agrees with its master to park until further notice; relinquishes its active member address, AM_ADDR, periodically listens to beacon transmissions from the master • device can either be invited back (by the master) to active communications using a broadcast transmission during a beacon or • if the slave wants to be unparked, it sends a message to the master in the slots following the beacon

Although the radio is often the biggest power drain on a Bluetooth device, the voltage controlled oscillator (for the Bluetooth clock) also consumes power and can be shut off -- instead you can use a less accurate lower power oscillator when the accuracy of the normal oscillator is not needed (for example when sleeping)

Slide 474

Bluetooth performance when faced with interference

Magnus Karlsson started with ns-2 and the Bluetooth extensions and further extended it to support modeling of a data logger talking to a server in the presence of interference. See [Karlsson2005].

He also implemented a tool to assist in taking experimental data concerning interference as a function of frequency and distance and generating the tables necessary for simulating a Bluetooth link in this environment.

[Karlsson2005] Magnus Karlsson, "Modelling and Evaluation of a Bluetooth Data Logger in the Presence of Interference Sources", Masters Thesis, KTH/IMIT, MIT/LCN 2005-08, April 2005 http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-92292

Slide 475

Bluetooth Hacking

BlueSniff [Spill and Bittau2007] using a Ettus Research Universal Software Radio (USRP™) to implement a Bluetooth protocol stack [Spill2007]. In 2009, the results were extended using aliasing to allow one USRP to receive all of the 80 channels [Ossmann and Spill2009].

T-BEAR - a suite of tools for auditing security in a Bluetooth environment [Davis2005] .

Raúl Siles has a set of lecture slides[Siles2008] on Bluetooth Security that summarizes some of the concerns for the use of Bluetooth in a corporate environment.

Maguire IK2555, Spring 2016 Slide 475

[Spill and Bittau2007] Dominic Spill and Andrea Bittau, BlueSniff: Eve meets Alice and Bluetooth, First USENIX Conference on Offensive Technologies (WOOT'07), USENIX, 6 August 2007 http://www.usenix.org/event/woot07/tech/full_papers/spill/spill_html/

[Spill2007] Dominic Spill, Final Report: Implementation of the Bluetooth stack for software defined radio, with a view to sniffing and injecting packets, Report for Masters Degree, University College London, Computer Science, May 14, 2007, http://www.cs.ucl.ac.uk/staff/a.bittau/dom.pdf

[Ossmann and Spill2009] Michael Ossmann and Dominic Spill, Building an All-Channel Bluetooth Monitor, Lecture slides, ShmooCon 2009, February 2009 http://www.ossmann.com/shmoo-09/ossmann-spill-shmoo-2009.pdf

[Davis2005] Joshua Davis, T-BEAR: Transient Bluetooth Environment AuditoR, version 1.5, 22 July 2005, http://www.sourcefiles.org/Networking/Tools/Wireless/tbear.tar.gz.shtml

[Siles2008] Raúl Siles, Bluetooth Security: To Blue, or Not to Blue: That is the Question, Lecture slides, December, 2008 http://www.raulsiles.com/downloads/BluetoothSecurity_ToBlueOrNotToBlue_RaulSiles_v1.0.pdf

Slide 476

Bluetooth version 4.0

Bluetooth Core Specification version 4.0, adopted as of 30 June 2010 includes Bluetooth **low energy** (BLE) protocol:

- range < 50m
- set up time 3 ms
- ~200 kbps
- supports multicast in addition to unicast communication

Slide 477

Bluetooth low energy aka Bluetooth LE (BLE) and Bluetooth® Smart

http://www.bluetooth.com/Pages/Bluetooth-Smart.aspx

Part of Bluetooth 4.1 Specification - http://blog.bluetooth.com/bluetooth-sig-introduces-new-bluetooth-4-1-specification/ and https://www.bluetooth.org/en-us/specification/adopted-specifications

Interesting features:

- Synchronization an unlimited number of listeners – to support 3D glasses (see *3D Synchronization Profile)*
- Adds support in the protocol adaptation layer for IEEE 802.11n MAC/PHY
- 128 bit AES encryption
- Add support for IPv6 with L2CAP dedicated channels
- Adds dual mode topology, i.e, a device can be a Bluetooth Smart Ready Hub **and** Bluetooth Smart peripheral at the same time
- Coexistence with LTE

Maguire IK2555, Spring 2016 Slide 477

Bluetooth 3DG WG, Blutetooth 3D Synchronization Profile, Version 1.0.1, Document number 3DSP_Spec , 22 October 2013
https://www.bluetooth.org/docman/handlers/DownloadDoc.ashx?doc_id=280584

Slide 478

Bluetooth 4.2

As of Dec. 2014, specifications:
https://www.bluetooth.org/en-us/specification/adopted-specifications

IP and IPv6/6LoWPAN connectivity via Internet Protocol Support Profile (IPSP) and more new features, see:
https://www.bluetooth.com/news/pressreleases/2014/12/03/new-bluetoothspecifications-enable-ip-connectivity-and-deliver-industry-leading-privacy-and-increased-speed

Slide 479

Bluetooth keylogger

Samy Kamkar's KeySweeper http://samy.pl/keysweeper/
Sniffs Bluetooth traffic from Microsoft Bluetooth keyboards

Slide 480

¿Questions?

Slide 481: Lecture 9: Ultrawideband (UWB)

IK2555: Mobile and Wireless Network Architectures: Lecture 9

prof. Gerald Q. Maguire Jr. http://people.kth.se/~maguire/

School of Information and Communication Technology (ICT), KTH Royal Institute of Technology

IK2555 Spring 2016 2016.01.08 © 2016 G. Q. Maguire Jr. All rights reserved.

Slide 482

9. Ultrawideband (UWB)

Lecture notes of G. Q. Maguire Jr.

Slide 483

Ultrawideband

"[a]n intentional radiator that, at any point in time, has a fractional equal to or greater than 0.20 or has a UWB bandwidth equal to or greater than 500MHz, regardless of the fractional bandwidth."

- US FCC

- Often implemented as ~picosecond impulses† ⇒ Very low power (radiate power of 0.1mW to < 1μW (-30dBm)) - as the radio is only emitting for a **very** short time
- very robust to channel impairments such as multipath fading
- Digital technology ⇒ easy for makers of digital chips to design/make/…
- US FCC gave regulatory approval 14 Feb. 2002
  - Intel demo'd a 100Mbps transmitter and receiver and expects to be able to get 500Mbps at a few meters dropping to 10Mbps at 10m
  - http://www.freescale.com/webapp/sps/site/overview.jsp?nodeId=02XPgQhHPR0220 - Trinity chipset 100Mbps at less than 200mW
  - Wireless USB chipsets have been released, see Wisair, Sigma Designs, Alereon, …

† For the underlying theory for why short pulses should be used see [Verdú2002] and [Telatar and Tse2000]. For and introduction to impulse radio see [Win and Scholtz1998].

Maguire IK2555, Spring 2016 Slide 483

[Verdú2002] Sergio Verdú, "Spectral efficiency in the wideband regime", IEEE Transactions on Information Theory, 48(6):1319-1343, 2002.

[Telatar and Tse2000] Emre Telatar and David Tse, "Capacity and mutual information of wideband multipath fading channels", IEEE Transactions on Information Theory, 46(4):1384-1400, 2000.

[Win and Scholtz1998] Moe Z. Win and Robert A. Scholtz, "Impulse radio: how it works", IEEE Communications Letters, vol. 2, no. 2, pp. 36-38, Feb. 1998

Slide 484

Ranging

One of the features of UWB is ranging (distance measurements between transmitter and receiver), see for example Time Domain's PulsON® 410 RCM

http://www.timedomain.com/p400.php

~2cm for line of sight path

See also: [Monge2013]

[Monge2013] Alessandro Monge, Synchronized MAC layer for ultra-wideband wireless sensor network: Design, implementation, analysis, and evaluation, Master's thesis, KTH Royal Institute of Technology, School of Information and Communication Technology, TRITA-ICT-EX-2013:59, April 2013 http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-120580

Slide 485

Ultrawideband adoptions

Multi-Band Orthogonal Frequency Division Multiplexing (MB-OFDM) UWB adopted in:

- Wireless USB
- high speed Bluetooth

Slide 486

Further reading

D. Hélal and P. Rouzet. ST Microelectronics Proposal for IEEE 801.15.3a Alternate PHY. IEEE 802.15.3a/document 139r5, July 2003.

IEEE Standards for Information Technology - Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPAN), IEEE, 2003, ISBN 0-7381-3705-7

James P. K. Gilb, Wireless Multimedia: A Guide to the IEEE 802.15.3 Standard, IEEE Press, 2003, 250 pages, ISBN 0-7381-3668-9

S. Roy, J.R. Foerster, V.S. Somayazulu, and D.G. Leeper, 'Ultrawideband Radio Design: The Promise of High-Speed, Short-Range Wireless Connectivity', Proceedings of the IEEE, vol. 92, no. 2, pp. 295–311, February 2004, DOI:10.1109/JPROC.2003.821910

Slide 487

¿Questions?

Slide 488: Lecture 10: Broadband Wireless Access (BWA)

IK2555: Mobile and Wireless Network Architectures: Lecture 10

prof. Gerald Q. Maguire Jr. http://people.kth.se/~maguire/

School of Information and Communication Technology (ICT), KTH Royal Institute of Technology

IK2555 Spring 2016 2016.01.08 © 2016 G. Q. Maguire Jr. All rights reserved.

Slide 489

10. Broadband Wireless Access (BWA)

Features:

- Data only
- downlink speeds in excess of 500Kbps at a distance of several km
- goal: wireless metropolitan area networking (WMAN), i.e., “last mile” connections

Several contenders:

- IEEE 802.16 aka Worldwide Microwave Interoperability Forum’s **WiMAX** (supported by Intel and Nokia)
- European Telecommunication Standards Institutes (ETSI)’s BRAN HA (Broadband Radio Access Networks HiperAccess) or HiperMAN
- ArrayComm
- Beamreach
- Flarion’ flash-OFDM - IP oriented
- IPWireless’ UMTS-TDD (closely related to 3G’s UMTS-FDD)
- Navini’s synchronous CDMA (SCDMA) - IP oriented

Slide 490

IEEE 802.16

Initial IEEE 802.16 [IEEE 802.16 WG] specification was only for Line-of-Sign environments in the 10 to 66 GHz range.

Several variants:

IEEE 802.16a	• Slotted TDMA (scheduled by base station) in a point-to-multipoint topology (mesh topologies are an option)
	• low latency
	• connection oriented
	• Features: ARQ, 3DES encryption, automatic power control
	• amendment to 802.16 - for 2GHz to 11GHz
	• Several physical (PHY) layers:
	  • Single Carrier PHY
	  • 256 point FFT OFDM PHY (common to WiMAX and ETSI HyperMAN)
	  • 2048 point FFT OFDMA PHY

802.16b	Concerns Quality of Service (QoS)
802.16c/d	Introduces system profiles and specifies combinations of options - goal: increased interoperability
802.16e	add mobility, packet oriented

Maguire IK2555, Spring 2016 Slide 490

[IEEE 802.16 WG] IEEE 802.16 Working Group on Broadband Wireless Access Standards - http://grouper.ieee.org/groups/802/16/

Slide 491

IEEE 802.16 standards continued

802.16-2009	IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems Consolidates and obsoletes IEEE Standards 802.16-2004, 802.16e-2005, 802.16-2004/Cor1-2005, 802.16f-2005, and 802.16g-2007
802.16m-2011	100 Mbit/s mobile and 1 Gbit/s fixed; aka Mobile WiMAX Release 2 or Wireless- MAN-Advanced.

Current status of IEEE 802.16 publications can be found at:
http://grouper.ieee.org/groups/802/16/published.html

Slide 492

WiMAX

http://www.wimaxforum.org

For measurements of the performance of WiMAX in the field see the Masters thesis of Xin Bai [Bai2006].

[Bai2006] Xin Bai, "Broadband Wireless Access in Disaster Emergency Response", Masters Thesis, Department of Communication Systems, KTH Royal Institute of Technology, May 2006 http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-92207

Slide 493

Related IEEE 802.16 work

P802.16n Higher Reliability Networks

⇒ IEEE Standard 802.16n-2013

http://standards.ieee.org/findstds/standard/802.16n-2013.html

P802.16p Enhancements to Support Machine-to-Machine Applications

⇒ IEEE Standard 802.16p-2012

http://standards.ieee.org/findstds/standard/802.16p-2012.html

P802.16r - IEEE Standard for Air Interface for Broadband Wireless Access Systems - Amendment for Small Cell Backhaul (SCB)

http://grouper.ieee.org/groups/802/16/scb/index.html

Project 802.16.3: Mobile Broadband Network Performance Measurements

http://grouper.ieee.org/groups/802/16/mbnpm/index.html

Summary of 801.16 related standards at

http://grouper.ieee.org/groups/802/16/published.html

Slide 494

IEEE 802.20 aka Mobile-Fi

Developed by IEEE Mobile Broadband Wireless Access (MBWA) WG [MBWA]

- **designed** to carry **IP packets** with low latency
- designed for mobile broadband access
- symmetrical wireless rates from 1 .. 4 Mbps
- uses licensed spectrum below 3.5 GHz
- range up to 15 km
- to exploit smart antennas

For a good overview of this standard see:

Radhakrishna Canchi, IEEE Standard 802.20™ MBWA Mobile Broadband Wireless Access Systems Supporting Vehicular Mobility, Slides from IEEE 802 Standards Workshop, Singapore, 11 March 2011

http://www.ieee802.org/minutes/2011-March/802%2520workshop/IEEE_March201 1-Workshop-IEEE80220-Canchi-Draft-v2.pdf

Note that this standard is no longer being developed.

Maguire IK2555, Spring 2016 Slide 494

[MBWA] IEEE Mobile Broadband Wireless Access (MBWA) Working Group - http://grouper.ieee.org/groups/802/20/

Slide 495

IEEE 802.22 Wireless Regional Area Networks (WRANs)

"The charter of IEEE 802.22, the Working Group on Wireless Regional Area Networks ("WRANs"), under the PAR approved by the IEEE-SA Standards Board is to develop a standard for a cognitive radio-based PHY/MAC/air_interface for use by license-exempt devices on a non-interfering basis in spectrum that is allocated to the TV Broadcast Service."

IEEE 802.22 Working Group on Wireless Regional Area Networks (WRANs) [802.22 WG]

See:

- IEEE 802.22-2011: Standard for Cognitive Wireless Regional Area Networks (RAN) for Operation in TV Bands, 1 July 2011
- IEEE 802.22.1-2010: Standard for the Enhanced Interference Protection of the Licensed Devices, 1 November 2010
- http://ieee802.org/22/
- [Jain2010]

Maguire IK2555, Spring 2016 Slide 495

[802.22 WG] IEEE 802 LAN/MAN Standards Committee 802.22 WG on WRANs (Wireless Regional Area Networks) http://www.ieee802.org/22/

[Jain2010] Raj Jain, IEEE 802.22 Wireless: Regional Area Networks, Lecture notes for CSE574S, Washington University in St. Louis, 2010 http://www.cse.wustl.edu/~jain/cse574-10/ftp/j_dwrn.pdf

Slide 496

All IP networks

Numerous efforts have shifted from simply using IP (rather than ATM) in the backbone and have been moving to an all IP network (i.e., IP directly to/from MS and in the infrastructure).

Airvana Inc. (www.airvananet.com): all-IP architecture for radio access network equipment for 3G using CDMA2000 1x Evolution-Data Only (1xEV-DO) wireless technology, data rates up to 2.4 Megabits per second (Mbps) under ideal circumstances, with average sustained rates expected to be 300 to 600 kbps

Some view "4G" as the Fourth Generation **IP-based** wireless network.

Eliminates SS7 (Signaling System 7) telecommunications protocol

Qualcomm (formerly Flarion http://www.flarion.com/)
RadioRouter™ base stations used to build all-IP network

…

Slide 497

Further reading

ARCchart ltd., "The next bout: 3G versus BWA", London, UK, September 30, 2003 - formerly at http://www.3gnewsroom.com/3g_news/sep_03/news_3793.shtml

ARCchart ltd., "WiMAX: The Critical Wireless Standard: 802.16 and other broadband wireless options", October 2003, formerly at http://www.arcchart.com/pr/blueprint/pdf/BluePrint_WiFi_REPORT_I. pdf

Worldwide Interoperability for Microwave Access Forum, "IEEE 802.16a Standard and WiMAX Igniting Broadband Wireless Access", White Paper, formerly at http://www.wimaxforum.org/news/downloads/WiMAXWhitepaper.pdf

Carlos Cordeiro, Kiran Challapali, and Dagnachew Birru, and Sai Shankar N, IEEE 802.22: An Introduction to the First Wireless Standard based on Cognitive Radios, Journal of Communications, Academy Publisher, Vol. 1, No. 1, April 2006

http://www.academypublisher.com/jcm/vol01/no01/jcm01013847.pdf

Carlos Cordeiro, Report on IEEE 802.22, IEEE J-SAC, and IEEE DySPAN 2007 tutorials, TCCN meeting at Globecom on November 27, 2006

http://www.eecs.ucf.edu/tccn/meetings/Report_06.ppt

Carlos Cordeiro, Cognitive Radios: Present and Future Directions, Slides from talk at UCLA, 21 July 2006,

http://medianetlab.ee.ucla.edu/talks/Philips_CR_Cordeiro.pdf

Slide 498

¿Questions?

Slide 499: Lecture 11: Sensor Networks

IK2555: Mobile and Wireless Network Architectures: Lecture 11

prof. Gerald Q. Maguire Jr. http://people.kth.se/~maguire/

School of Information and Communication Technology (ICT), KTH Royal Institute of Technology

IK2555 Spring 2016 2016.01.08 © 2016 G. Q. Maguire Jr. All rights reserved.

Slide 500

11. Sensor Networks

Lecture notes of G. Q. Maguire Jr.

Slide 501

Mobile ad hoc Networks (MANETs)

Ad hoc networks exploit the links which are possible with their neighbors

Mobile *ad hoc* networks (MANETs) exploit the fact that as nodes move the set of neighbors may change.

There may exist gateways between a MANET and fixed infrastructures - see for example the combination of Mobile IP and MANETs (MIPMANET) [Jönsson2000]

Maguire IK2555, Spring 2016 Slide 501

[Jönsson2000] Ulf Jönsson, Fredrik Alriksson, Tony Larsson, Per Johansson, and Gerald Q. Maguire Jr, MIPMANET - Mobile IP for Mobile Ad Hoc Networks, First Annual Workshop on Mobile Ad Hoc Networking & Computing, IEEE/ACM, August 11, 2000, Boston, Massachusetts. http://doi.acm.org/10.1145/514151.514163

Slide 502

Sensor networks

(Wireless) Sensor networks is an emerging area of computer science, driven by advances in micro-electrical-mechanical system (MEMS) micro-sensors, wireless networking, and embedded processing [Estrin1999].

Ad hoc networks of sensors target both commercial & military applications:

- environmental monitoring (e.g. traffic, habitat (HVAC), security, …)
- industrial sensing and diagnostics (devices which reports their usage, wear, problems occurring, …)
- infrastructures (e.g. power, water, waste disposal/stewardship, …)
- battlefield awareness (multi-target tracking, …)
- logistics (for example using "smart packages", "smart packaging" {for example monitoring tampering, temperature, shock, humidity, age, …}, …)
- personnel monitoring (health, safety, location, …)
- …

Maguire IK2555, Spring 2016 Slide 502

[Estrin1999] Deborah Estrin, Ramesh Govindan, John Heidemann and Satish Kumar, "Next century challenges: scalable coordination in sensor networks", Proceedings of the fifth annual ACM/IEEE international conference on Mobile computing and networking. August 15 - 19, 1999, Seattle, WA USA, pp 263-270

Slide 503

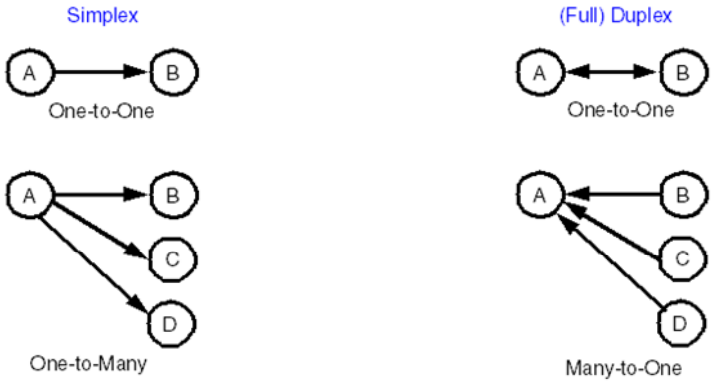
Spectrum of Concerns

- Hardware
- Architecture
- Physical Layer
- MAC Layer
- Applications
- Energy
- …

First we will examine some fundamental concepts in communication and networking, then we will proceed to talk about wireless sensor networks.

Slide 504

Patterns of Communication

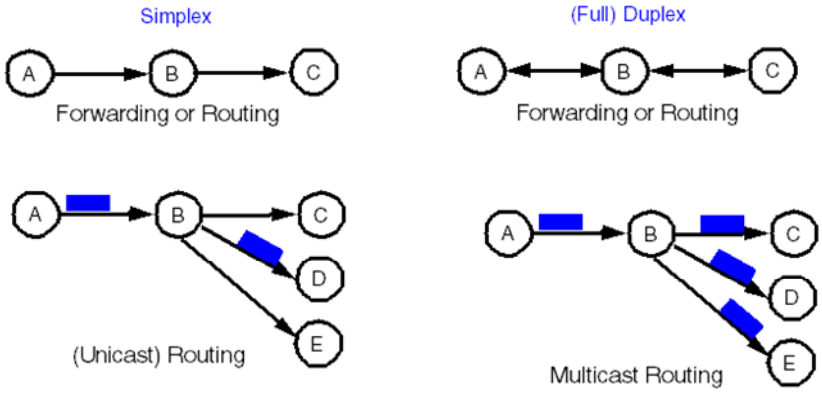


Basic Patterns of (Direct) Communication

Asymmetry: communications between nodes may be asymmetric, i.e., because node α can hear node β, does **not** imply that α can transmit directly to node β.

Slide 505

Mediated Communication



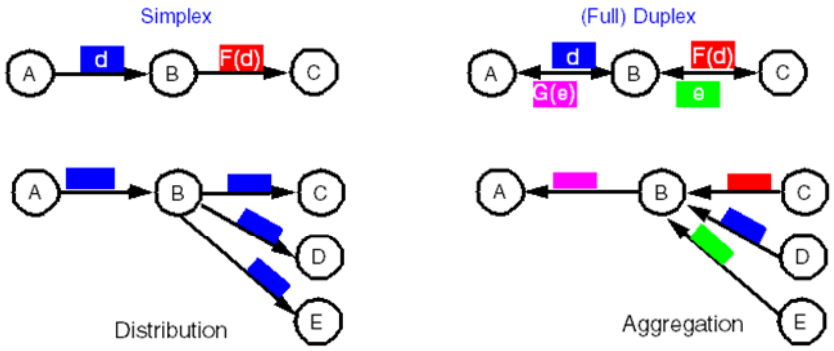
Basic Patterns of (Indirect) Communication

B acts as an **intermediary** between A and C/D/E.

- **Forwarding** is based on **layer 2** (i.e., **link** layer) address
- **Routing** is based on **layer 3** (i.e., **network** layer) address.

Slide 506

Transformations

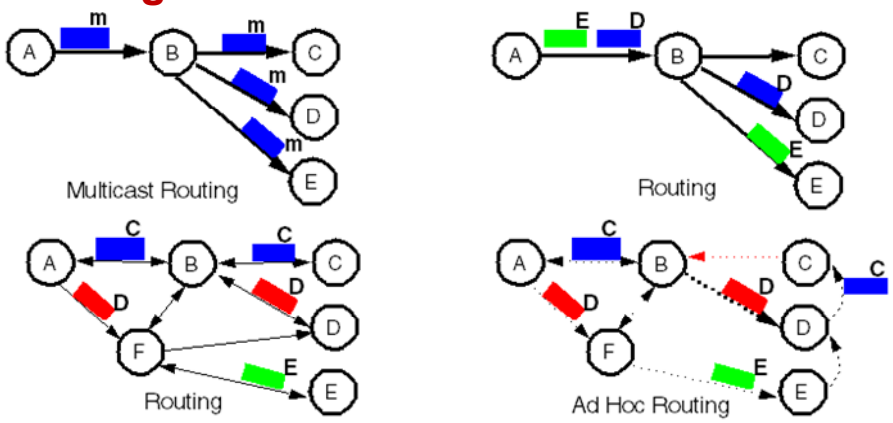


Transformations

- B acts as an **intermediary**
- B **operates** on the **data** as it passes through
  - examples: transcoding, translation, replication, averaging, …

Slide 507

Routing



- B/F/… acts as an intermediary between A and x
- B (or F) **routes** based on the **address -** this routing **choice** can be **time varying** (especially if the nodes are moving)

Slide 508

Ad hoc routing

Ad hoc routing supports self-configuration in the presence of wireless links and *node* mobility. Lots of alternatives:

- direct transmission,
- minimum transmission energy,
- geographic routing,
- multi-hop routing, and
- clustering

Proactive and Reactive routing schemes:

- **Proactive** routing attempts to maintain routes to all destinations at all times, regardless of whether they are needed or not
- **Reactive** routing computes routes *only* when they are needed

Tradeoffs between routing traffic (and energy consumption) vs. **delay**.

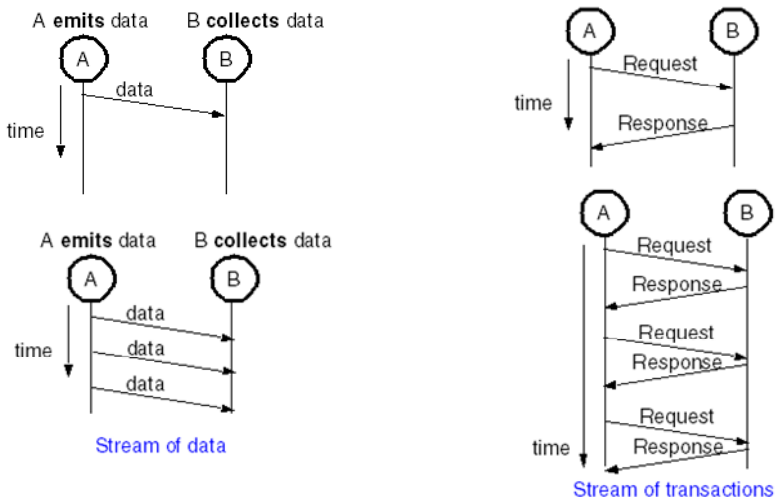
Prof. D. Estrin and her WINS group offered a *hypothesis* that **Internet technologies + ad hoc routing** is sufficient to design sensor network applications [Estrin1999].

Maguire IK2555, Spring 2016 Slide 508

[Estrin1999] Deborah Estrin, Ramesh Govindan, John Heidemann and Satish Kumar, "Next century challenges: scalable coordination in sensor networks", Proceedings of the fifth annual ACM/IEEE international conference on Mobile computing and networking. August 15 - 19, 1999, Seattle, WA USA, pp 263-270

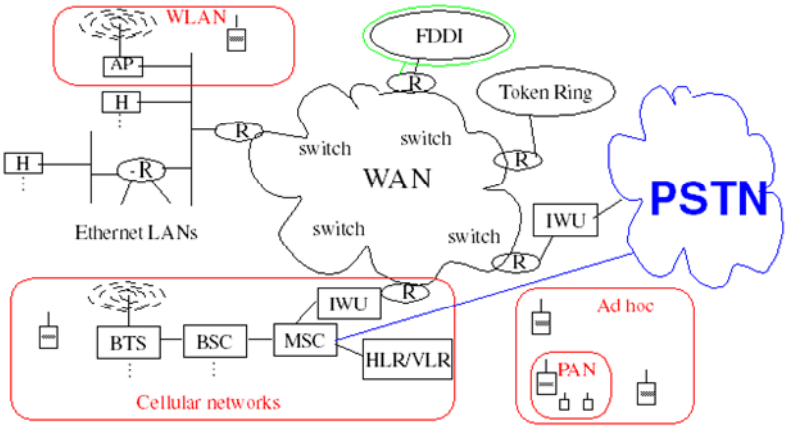
Slide 509

Patterns of Communication in time



Slide 510

Internetworking

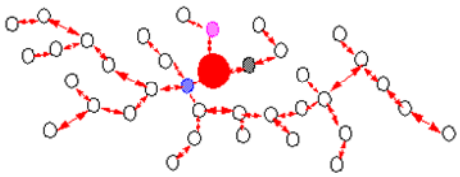


- Routers (R) interconnect (concatenate) multiple networks
- This accommodates multiple underlying hardware technologies by providing a way to interconnect **heterogeneous** networks and makes them inter-operate
- Facilitates disaggregation - since **functionality** can be located anywhere on the internet

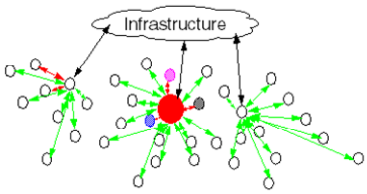
Slide 511

Ad hoc mode vs. Infrastructure mode

Mobile stations communicate **directly** to each other with no access point (base station) support, i.e., peer-to-peer (**ad hoc**) networking



Mobile stations communicate **only** via access points (APs)



Adding Access Points (APs) - (provides connections to the infrastructure, but at the cost of requiring/creating an infrastructure):

- reduces **delay**
- increases **complexity** of some nodes (the access points)
- requires **connectivity** between APs and the **infrastructure**
- may *increase* **power** consumption

Possible to combine both modes {but not in 802.11 WLANs}.

Slide 512

DARPA/IPTO: BAA #99-16: Sensor Information Technology

"... Innovative and effective software for producing communicating sensor information and also for effective and low-cost prototyping kits based on commercial off-the-shelf (COTS) components and/or government furnished equipment (GFE). The technology development is for a new DARPA program, SenseIT (Sensor Information Technology).

Whereas past sensor networks have been **single purpose** and **dependent on a central apparatus** for tasking/polling the sensors, the SenseIT program will pioneer a network-based approach in which the sensor can be **dynamically multi-tasked from multiple points**, i.e. each node will be capable of running multiple simultaneous applications on behalf of different exterior users. In an ideal scenario, queries emanating from one point are automatically routed to the most appropriate sensor nodes, and the replies are collected and fused en route to the designated reporting point(s).

Distributed sensor networks … easily installed with little or no pre-planning, of being self-organizing, and of being capable of supporting sophisticated processing in the field. … **Sensors** will be *tightly integrated* with **a general purpose CPU**, **wireless communications**, and **memory**; multiple sensors can be associated with one node. **Short-range communication** among **10 to 10,000** sensor/computer nodes deployed in an irregular pattern will be supported. "

{*Emphasis* and **bold** added by Maguire}

Maguire IK2555, Spring 2016 Slide 512

DARPA SENSIT project, last modified 27 August 2002, http://www.eng.auburn.edu/users/lim/sensit.html

Slide 513

Self-organizing sensor networks

Built from sensor nodes that:

- spontaneously create an *ad hoc* network vs. a traditionally **engineered** system structure
  - nodes may simply be scattered (thrown at random, shell dispersed, cloud, …)
- assemble the network themselves
  - large to very large numbers (10^3 .. 10^{23}) of sensors
- **dynamically** adapt to device failure and degradation
  - individual failure is going to occur - with large numbers of nodes you can be certain that there will be failed nodes
- manage **movement** of sensor nodes, and
- react to changes in **task** and **network** requirements

⇒ due to their physical size and large number it is simply **not possible** to visit/configure/fix/... individual nodes

⇒ frequent changes in: position, reachability, power availability, tasking, …

Maguire IK2555, Spring 2016 Slide 513

Slide 514

Sensor nodes must be reconfigurable

Reconfigurable smart sensor nodes enable sensor devices:

- to be self-aware,
- self-reconfigurable, and
- autonomous

Benefits are:

- incremental deployment
- no central administration needed
- dynamically adapt to device failure and degradation as well as changes in task and network requirements (high flexibility), and
- support application-specific network and system services by mixing types of sensor nodes and applications

Slide 515

Low Energy Adaptive Clustering Hierarchy (LEACH)

Wendi (Rabiner) Heinzelman: [LEACH] and [Heinzelman1999]

- designed for sensor networks where an end-user wants to remotely monitor the environment.
- The data from the individual nodes must be sent to a central base station, often located far from the sensor network
- Desirable properties for protocols on these networks:
  - Use 100's - 1000's of nodes
  - Maximize system lifetime
  - Maximize network coverage
  - Use uniform, battery-operated nodes
- using **distributed cluster formation** and **local processing** to reduce global communication along with randomized *rotation of the clusterheads* ⇒ allows LEACH to achieve the desired properties while being energy-efficient, hence extending system lifetime

Maguire IK2555, Spring 2016 Slide 515

[LEACH] LEACH formerly at http://nms.lcs.mit.edu/projects/leach/

[Heinzelman1999] Wendi Rabiner Heinzelman, Joanna Kulik, and Hari Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks", Proceedings of the fifth annual ACM/IEEE international conference on Mobile computing and networking. August 15 - 19, 1999, Seattle, WA USA, pp 174-185

Slide 516

Protocols to disseminate information

Sensor Protocols for Information via Negotiation (SPIN) [Heinzelman1999]

- a family of protocols used to efficiently **disseminate** information in a wireless sensor network
- flooding and gossiping waste valuable communication and energy resources sending redundant information throughout the network -- while not being resource-aware or resource-adaptive
- use **data negotiation** and **resource-adaptive algorithms**
- nodes assign a high-level name to their data, called **meta-data**, and perform meta-data negotiations before any data is transmitted ⇒ avoids redundant data being sent throughout the network
- utilize current energy level of the node to adapt the protocol based on how much energy remains
- Simulation shows that SPIN is both more energy-efficient than flooding or gossiping while distributing data at the same rate or faster than either of these protocols.

Maguire IK2555, Spring 2016 Slide 516

[Heinzelman1999] W. Heinzelman, J. Kulik, and H. Balakrishnan, “Adaptive Protocols for Information Dissemination in Wireless Sensor Networks”, Proc. 5th ACM/IEEE Mobicom Conference (MobiCom ’99), Seattle, WA, August, 1999.

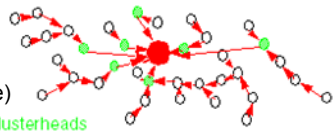
Slide 517

Coordination vs. Centralization

Centralization ⇒ single point of failure, bottleneck, and perhaps energy inefficient

Coordination ⇒ exploiting the large numbers of nodes, highly redundant (hence fault tolerant), …

- another WINS hypothesis: sensor network coordination applications are better realized with **localized** algorithms [Estrin1999]
  - with local (neighborhood) based communication - communication overhead scales well with increasing network size
  - algorithms are more robust to network partitioning and node failures (since they do not depend on global behaviors)
- Clustering
  - localized coordination via a cluster head
  - cluster head can do data aggregation (for example, summarizing local state)
  - can be a two layer model or a multi-layer model
    - communication at low layers, e.g. within a cluster, are short distance, short delay, hopefully low power
    - communication at higher layers, e.g. between clusters, are long distance, long delay, often require more power
    - not all choices of clusterheads are optimal



Maguire IK2555, Spring 2016 Slide 517

[Estrin1999] Deborah Estrin, Ramesh Govindan, John Heidemann and Satish Kumar, “Next century challenges: scalable coordination in sensor networks”, Proceedings of the fifth annual ACM/IEEE international conference on Mobile computing and networking. August 15 - 19, 1999, Seattle, WA USA, pp 263-270

Slide 518

Sensor fusion en route (a form of in-net processing)

Heidemann, et al. use Low-Level Naming ⇒ software architecture with named data and enroute processing for multi-application sensor-network [Heidemann2001]

Maguire IK2555, Spring 2016 Slide 518

[Heidemann2001] John Heidemann, Fabio Silva, Chalermek Intanagonwiwat, Ramesh Govindan, Deborah Estrin, and Deepak Ganesan, “Building Efficient Wireless Sensor Networks with Low-Level Naming”, In Proceedings of the Symposium on Operating Systems Principles, pp. 146-159. Chateau Lake Louise, Banff, Alberta, Canada, ACM. October, 2001.

Slide 519

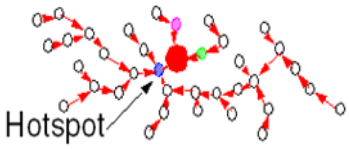
Data Aggregation

At each node receive data, use it in conjunction with local data, transmit new **aggregated** data

Typical operations

- scalar operations (such as sum, average, median, …)
- vector operations (such as logical operations)

Data aggregation reduces the volume of data that must be transmitted - this is very important to avoid **hotspots** in the network (i.e., lots of traffic all headed for the same places and competing to get there) and reduce the energy required to send *meaningful* data



Slide 520

Directed diffusion

Promotes **in-network** processing by building on a data-centric vs. address-centric architecture for the distributed system/network

Using **data naming** as the lowest level of system organization vs. using an explicit sensor/node address, i.e., sensor #46879.

Sensors **publish** data (as **sources**) and clients **subscribe** to data (as **sinks**), both identify data by **attributes** (meta-data) vs. addresses (i.e., data is **not** tied to host identity) [Heidemann2001]

Clients subscriptions (i.e., interest in data) form gradients (with a magnitude and direction) along which direct the data flows (data may also be aggregated along the way)

Wide variety of data dissemination patterns possible: shortest path multicast tree, energy-efficient spanning tree, …

See also: [Heidemann2001], [Elson and Estrin2000], [Elson and Estrin2001], [Ratnasamy2003], [Lindsey2001], [Intanagonwiwat2000]

Maguire IK2555, Spring 2016 Slide 520

[Heidemann2001] John Heidemann, Fabio Silva, Chalermek Intanagonwiwat, Ramesh Govindan, Deborah Estrin, and Deepak Ganesan, "Building Efficient Wireless Sensor Networks with Low-Level Naming", SOSP 2001

[Elson and Estrin2000] Jeremy Elson and Deborah Estrin, "An Address-Free Architecture for Dynamic Sensor Networks", http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.42.9521

[Elson and Estrin2001] Jeremy Elson and Deborah Estrin, "Random, Ephemeral Transaction Identifiers in Dynamic Sensor Networks", In Proceedings of the 21st International Conference on Distributed Computing Systems (ICDCS-21) April 16-19, 2001, Phoenix, Arizona, USA.

[Ratnasamy2003] Sylvia Ratnasamy, Deborah Estrin, Ramesh Govindan, Brad Karp, Scott Shenker, Li Yin, Fang Yu, "Data-centric storage in sensornets with GHT, a geographic hash table", Mob. Netw. Appl., vol. 8, no. 4, pp. 427–442, August 2003, DOI:10.1023/A:1024591915518, Available at http://dx.doi.org/10.1023/A:1024591915518 .

[Lindsey2001] Stephanie Lindsey, Cauligi Raghavendra, and Krishna Sivalingam, "Data gathering in sensor networks using the energy*delay metric", presented at the International Parallel and Distributed Processing Symposium/International Parallel Processing Symposium - IPDPS(IPPS), 2001, pp. 2001–2008, DOI:10.1109/IPDPS.2001.925196, Available at http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=925196.

[Intanagonwiwat2000] Chalermek Intanagonwiwat, Ramesh Govindan, and Deborah Estrin, "Directed diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks", Proceedings of the sixth annual international conference on Mobile computing and networking, ACM, August 6 - 11, 2000, Boston, MA USA, pp 56-67

Slide 521

example values from
[Intanagonwiwat2000]

Tasks and Events

Task (what to look for):

type = four-legged animal	// detect animal location
interval = 20 ms	// send back events every 20 ms
duration = 10 seconds	// ... for the next 10 seconds
rect = [-100, 100, 200, 400]	// from sensors within rectangular region

Attribute-value pairs;
values could be instances,
ranges, hierarchies, …

Event (when there is an observation that matches the task specifications):

type = four-legged animal	// type of animal detected
instance = elephant	// instance of this type
location = [125, 220]	// node location
confidence = 0.85	// confidence in the match
timestamp = 01:20:40	// event generation time

Maguire IK2555, Spring 2016 Slide 521

[Intanagonwiwat2000] Chalermek Intanagonwiwat, Ramesh Govindan, and Deborah Estrin, "Directed diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks", Proceedings of the sixth annual international conference on Mobile computing and networking, ACM, August 6 - 11, 2000, Boston, MA USA, pp 56-67

Slide 522

How did the sensor know it was an elephant?

Signal: extracted from acoustic, seismic, or other data

Matching: waveform matching, …

Confidence: it might **not** be an elephant, but there is some degree of confidence it is versus other possibilities

Slide 523

Caching of data

Intermediate nodes may keep local caches and satisfy requests from these caches

- ✓reduces energy over having to propagate the requests all the way to the source and propagating the answer back
- ✓increases scalability
- ✓increases robustness
- ✓may result in stale data

Caching prevents loops, since if the received data message matches a data cache entry, then there is no need to pass the message farther.

If the cache also retains information about the sink it can do **downconverting** of sample rates - so if one source only wants the data at half the rate of another source and these sources lie on different gradients the node can send data messages at the appropriate rate for the particular gradient [Intanagonwiwat2000] .

Maguire IK2555, Spring 2016 Slide 523

[Intanagonwiwat2000] Chalermek Intanagonwiwat, Ramesh Govindan, and Deborah Estrin, "Directed diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks", Proceedings of the sixth annual international conference on Mobile computing and networking, ACM, August 6 - 11, 2000, Boston, MA USA, pp 56-67

Slide 524

Design space for Diffusion

table from Figure 3 of [Intanagonwiwat2000]

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

Maguire IK2555, Spring 2016 Slide 524

[Intanagonwiwat2000] Chalermek Intanagonwiwat, Ramesh Govindan, and Deborah Estrin, "Directed diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks", Proceedings of the sixth annual international conference on Mobile computing and networking, ACM, August 6 - 11, 2000, Boston, MA USA, pp 56-67

Slide 525

Metrics for evaluating directed diffusion

Average dissipated energy	ratio of total dissipated energy per node in the network to the number of distinct events seen by sinks, e.g., average work per node in delivering useful information
Average delay	measures one-way latency between observation and it being received by each sink (for example, this defines temporal accuracy of location estimates)
Event delivery ratio	ratio of the number of distinct events received to the number originally sent

Generally results are compared to:

- **flooding**
- **omniscient multicast** (each source transmits its events along the shortest path multicast tree to the sink(s)

Slide 526

Congestion

1 Either operate network *far* from congestion or

2 reduce congestion: down conversion, aggregation with data **quality reduction**, …

Note that option #1 is simply over provisioning.

Slide 527

Tiered architectures

Combining a small number of more capable nodes as complements to very large numbers of very limited capability nodes

- Smallest system elements provide: **spatial diversity** and **short range sensing**
- More powerful elements provide more **sophisticated** and performance **intensive** processing functions (as they have greater resources)

Could even exploit robotic elements (i.e., physically mobile nodes) that wonder over the sensor field delivering energy to depleted batteries/capacitors/fuel cells or that deliver (localization), i.e., coordinates to other nodes, or that deliver new fluids/gas/... (or expendables) for sensors {or even **excreters** -- i.e., nodes that release and perhaps even locally manufacturer materials}

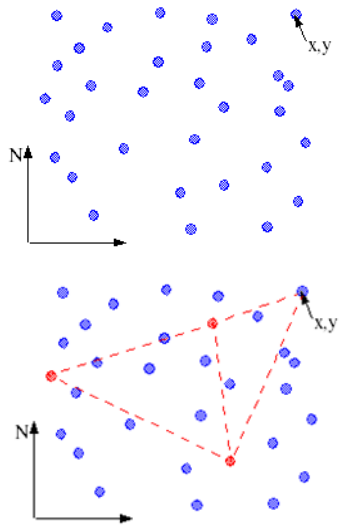
Slide 528

Localization

Some methods of localization:

- map based location
- surveyed location
- using external "markers"
- deriving relative location
- in-network, autonomous localization
- …

See [Niculescu and Nath2003], [Bulusu2001a], [Doherty2001], [Bulusu2000], [Bulusu2001b], [Savvides2001]



Maguire IK2555, Spring 2016 Slide 528

[Niculescu and Nath2003] D. Niculescu and Badri Nath, 'Ad hoc positioning system (APS) using AOA', presented at the INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications., vol. 3, 2003, pp. 1734–1743, DOI:10.1109/INFCOM.2003.1209196, Available at http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1209196

[Bulusu2001a] Nirupama Bulusu, John Heidemann, and Deborah Estrin, "Adaptive Beacon Placement" In Proceedings of the 21st International Conference on Distributed Computing Systems (ICDCS-21), Phoenix, Arizona, USA, April 2001, pp 489-498

[Doherty2001] Lance Doherty, Kristofer SJ Pister, Laurent El Ghaoui, "Convex Position Estimation in Wireless Sensor Networks", Proc. of IEEE Infocom 2001

[Savvides2001] Andreas Savvides, Chih-Chieh Han, and Mani B. Strivastava, "Dynamic fine-grained localization in Ad-Hoc networks of sensors", Seventh annual international conference on Mobile computing and networking 2001. July 16 - 21, 2001, Rome Italy, pp 166-179

[Bulusu2000] Nirupama Bulusu, John Heidemann, and Deborah Estrin, "GPS-less Low Cost Outdoor Localization For Very Small Devices" IEEE Personal Communications Magazine, 7 (5), pp. 28-34, October, 2000

[Bulusu2001b] Nirupama Bulusu, Deborah Estrin, Lewis Girod and John Heidemann, "Scalable Coordination for wireless sensor networks: Self-Configuring Localization Systems, International Symposium on Communication Theory and Applications (ISCTA 2001), Ambleside, Lake District, UK, July 2001.

Slide 529

Mapping where sensors are

A frequent problem is to build a map of where the nodes are. Requires:

- a set of local measurements (at each node or some subset of nodes)
  - for example, measuring signal strength during preambles (as the pattern is well known)
- knowledge of the location of **some** ("marker") nodes
  - it is desirable that they should be far apart to provide a long base line
- target tolerance (i.e., how close solution do you need)

Compute the location of all the nodes, building upon the position of maker nodes - generally by doing **distributed constraint solving.**

Considerations:

- location estimation error and speed of convergence
- where should the markers be (number and distribution)
- complexity (**O**(time), **O**(space), **O**(communications), **O**(energy), …)
- robustness to errors (such as marker positioning errors, lost packets, errors in measurements, …)

Slide 530

Synchronization

- to coordinate sensor sampling
- to organize multiple hop transfers by defining a schedule (to avoid or reduce collisions)

Some approaches:

- high precision clocks at the end - then propagate them inward
  - UC Berkeley group (David Culler, Eric Brewer, Dave Wagner, Shankar Sastry, and Kris Pister) have experimented with timestamping a particular bit in a message - since the during the process of communication the transmitter and receiver are synchronized to a fraction of a bit)
- broadcast clocks (à la GPS)
- chip scale atomic clocks (CSAC - a DARPA program) [Tang2001], [Kitching2003]

  Microsemi Corporation's SA.45s

  http://www.microsemi.com/products/timing-synchronization-systems/embedded-timing-solutions/components/sa-45s-chip-scale-atomic-clock

Coordinating and adapting node sleep schedules enable tradeoffs between fidelity, latency, and efficiency are emerging [Chen2001], [Cerpa and Estrin2002], [Schurgers2002], [Xu2001], [Elson and Estrin 2001].

Maguire IK2555, Spring 2016 Slide 530

[Tang2001] William C. Tang, "Chip-Scale Atomic Clock", Section II: Reprint of Broad Agency Announcement 01-32, the Commerce Business Daily , Publication Date: July 6, 2001; Issue No. PSA-2887, formerly at http://www.darpa.mil/mto/solicitations/BAA01-32/S/Section2.html

[Kitching2003] John Kitching, Local Oscillator Requirements for Chip-Scale Atomic Clocks, Time and Frequency Division, The National Institute of Standards and Technology, 325 Broadway, Boulder, Colorado 80305, April 5, 2003, formelry at http://www.boulder.nist.gov/timefreq/ofm/smallclock/LO%20Requirements.pdf

[Chen2001] Benjie Chen, Kyle Jamieson, Hari Balakrishnan, and Robert Morris, "Span: an Energy-Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks", Proc. 7th ACM MOBICOM Rome, Italy. July, 2001.

[Cerpa and Estrin2002] Alberto Cerpa and Deborah Estrin, "ASCENT: Adaptive Self-Configuring sensor Network Topologies", IEEE Infocom 2002, NYC and Alberto Cerpa and Deborah Estrin, "Ascent: Adaptive Self-Configuring sEnsor Network Topologies", UCLA Computer Science Department Technical Report UCLA/CSD-TR 01-0009, May 2001, formerly at http://lecs.cs.ucla.edu/~estrin/papers/Ascent-UCLA-tech-report.ps

[Schurgers2002] C. Schurgers, V. Tsiatsis, and M. Srivastava, "STEM topology management for efficient sensor networks", IEEE Aerospace Conference, Big Sky MT, March 2002.

[Xu2001] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed Energy Conservation for Ad Hoc Routing", In Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking(ACM MobiCom), Rome, Italy, July 16-21, 2001.

[Elson and Estrin 2001] Jeremy Elson and Deborah Estrin, "Time Synchronization for Wireless Sensor Networks", in Proceedings of the 15th International Parallel & Distributed Processing Symposium, Washington, DC, USA, 2001, p. 186–, Available at http://dl.acm.org/citation.cfm?id=645609.662464 .

Slide 531

Building upon localization and synchronization

Forming sensor arrays which **exploit** their distribution:

- two visual viewpoints ⇒ stereo imaging
- with *N* acoustic viewpoints ⇒ phased array microphone arrays
- with *N* acceleration sensor viewpoints ⇒ phased array seismic, geologic, footfall, vehicle movement, …
- with *N* visual viewpoints ⇒ can use algorithms such as shape from shading, avoid occlusion by (moving or stationary) objects, …
- …

Slide 532

Securing what you send

Asymmetric digital signatures for the authentication are impractical:

- long signatures ⇒ high communication overhead (50-1000 bytes per packet)
- very high computational (and energy) overhead to create and verify the signature
- Gennaro and Rohatgi
  - >1 Kbyte of authentication information per packet, and
  - Rohatgi's improved *k*-time signature scheme: > 300 bytes per packet
- Authenticated streaming broadcast protocol (TESLA) [Perrig2000]
  - uses too much communication and memory ⇒ μTESLA[Perrig2001]
- If the sensor is sending a stream of data, then Secure RTP (SRTP) can be used [Baugher2004]

Maguire IK2555, Spring 2016 Slide 532

[Perrig2000] A. Perrig, R. Canetti, J. Tygar and D. Song, "Efficient authentication and signing of multicast streams over lossy channels", In IEEE Symposium on Security and Privacy (2000).

[Perrig2001] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar. SPINS: Security protocols for sensor networks. In Proceedings of MOBICOM, 2001.

[Baugher2004] M. Baugher, D. McGrew, M. Naslund, E. Carrara, K. Norrman, "The Secure Real-time Transport Protocol", IETF, RFC 3711, March 2004.

Slide 533

Sensors

Former DARPA projects:

- Ultra Low Power Wireless Sensor Project, Prof. Charles G. Sodini, MIT (formerly http://www-mtl.mit.edu/~jimg/project_top.html)
- Power Aware Sensing Tracking and Analysis (PASTA) project
- Network of Embedded Software Technology (NEST) Program
- Wireless Integrated Network Sensors (WINS) Project at UCLA [Pottie and Kaiser2000]
- WEBDUST at Rutgers University

U.S. National Science Foundation initiative: Sensors and Sensor Networks

Commercial R&D

Compaq (nee HP) (WRL) Factoid Project

a portable device small enough to be attached to a key chain, which collects announcements broadcast from devices in the environment, later these can be uploaded via a user's home basestation

Eye-Fi - attaching GPS coordinates to pictures and uploading them opportunistically from the camera via Wi-Fi.

Maguire IK2555, Spring 2016 Slide 533

[Pottie and Kaiser2000] G.J.Pottie and W.J.Kaiser, "Wireless integrated network sensors", Communications of the ACM, Vol. 43, No. 5, May 2000, pp51-58

Slide 534

Millennial Net/

http://www.millennial.net/

"reliable, low-power wireless sensor networks"

See for example their "i-Bean" wireless sensor networking device:

- 2 cm x 2 cm size
- 10 year lifetime on a coin cell - with one report sent per second
- analog and digital interfaces,
- radio transceiver, and
- microcontroller.

Slide 535

Smart dust: 1 cubic mm system

Driven by: advances in hardware and design ⇒ reductions in size, power consumption, and cost for **digital circuitry**, **wireless communications**, and **micro electromechanical systems** (MEMS)

Professors Pister and Kahn leading the "smart dust" program [Kahn2000].

Given limited volume battery supplies: ~1 J; potential power scavaging techniques would enable solar power (1J/day) or indoor lighting (1mJ/day).

However, processing requires about 1nJ per 32 instruction and 100nJ per bit transmitted (Bluetooth) and ~1nJ per bit as a target for picoradios (see also [Rabaey2000]).

Thus Pister and Kahn targeted using free-space optical transmission using external lasers reflected from MEMS corner-cube retroreflector (CCR) ⇒ line-of-sight requirement + advantage of parallel read out using 2D sensors {i.e., a base station can listed to multiple transmitters as long as they appear in different pixels of the receiving sensor)

Maguire IK2555, Spring 2016 Slide 535

[Kahn2000] J. M. Kahn, R.H. Katz, K. Pister, "Emerging Challenges: Mobile Networking for "Smart Dust", J. Comm. Networks, Sept. 2000, pp. 188-196.

[Rabaey2000] Jan M. Rabaey, M. Josie Ammer, Julio L. da Silva Jr., Danny Patel. and Shad Roundy, "PicoRadio Supports Ad Hoc Ultra-Low Power Wireless Networking', IEEE Computer, Vol. 33, No. 7, July 2000, pp 42-48.

Slide 536

Berkeley Motes

Prof. Culler, and students at University of California, Berkeley have built motes as a sensor platform:

CPU	8-bit, 4 MHz
Storage	8 Kbytes instruction Flash 512 bytes RAM 512 bytes EEPROM
Communication	916 MHz radio Bandwidth 10 Kbps
Operating system	TinyOS OS code space 3500 bytes event-driven OS
Available code space	4500 bytes

Slide 537

University of California, Berkeley - Motes

Prototype device [Hill]:

- measures 1 inch by 1.5 inch
- a programmable processor AVR RISC processor (Atmel AT90LS8635)
  - 8-Kbyte In-System programmable Flash Program Memory - 1,000 Write/Erase Cycles
  - 544 bytes SRAM
  - 512 Byte EEPROM - 100,000 Write/Erase Cycles
  - 32 general-purpose registers
  - clock and timers:
    - Real-time Clock (RTC)
    - three flexible timer/counters with compare modes
    - programmable Watchdog Timer with internal oscillator
  - internal and external interrupts
  - a programmable serial UART
  - an SPI serial port
  - 8-channel 10-bit ADC
  - Up to 4 Million Instructions per second throughput at 4 MHz (1 Million Instructions per second / MHz)
  - 3-volt operation
  - Three Sleep Modes:
    - Idle 6.4 mA ⇒ 19.2mW† - stops the CPU while allowing: SRAM, timer/counters, SPI port and interrupt system to continue functioning

† Power Consumption at 4 MHz, 3V, 20°C

Maguire IK2555, Spring 2016 Slide 537

[Hill] Jason Hill, Robert Szewczyk, and Alec Woo (together with Professors David E. Culler and Kristofer S. J. Pister), "TinyOS: Operating System for Sensor Networks", (DARPA) DABT 63-98-C-0038, (DARPA) DABT 63-98-1-0018, and (NSF) RI EIA-9802069, formerly at http://www.eecs.berkeley.edu/IPRO/Summary/01abstracts/szewczyk.1.html

Slide 538

- – Power Save 1.9 mA ⇒ 5.7mW - timer oscillator continues to run, allowing the user to maintain a timer base -- while the rest of the device is sleeping
  - – Power-down <1 μA ⇒ 3μW saves the register contents but freezes the oscillator, disabling all other chip functions until the next interrupt (or hardware reset)
  - they have used the 44-lead, Thin (1.0 mm) Plastic Gull Wing Quad Flat Package (TQFP)
- RF Monolothics TR1000 radio transceiver
  - 916.5 MHz fixed carrier frequency
  - provisions for both on-off keyed (OOK) {up to 19.2 kbps} and amplitude-shift keyed (ASK) modulation operates up to 115.2 kbps
- an extension bus for adding a wide variety of analog and digital sensors and actuators
- Active Message model of communication
  - each Active Message contains the name of a user-level handler to be invoked on a target node upon arrival and a data payload to pass in as arguments
  - handler function extracts the message from the network and either processes the data or sends a response message
  - The network is modeled as a pipeline with minimal buffering for messages.
  - Message handlers must execute quickly and asynchronously
- TinyOS [TinyOS2012]
  - tiny event-driven operating system - occupies 178 bytes of memory
  - propagates events in the time it takes to copy 1.25 bytes of memory
  - context switches in the time it takes to copy 6 bytes of memory
  - supports two level scheduling

Maguire IK2555, Spring 2016 Slide 538

[TinyOS2012] TinyOS, last modified 20 August 2012 , http://webs.cs.berkeley.edu/tos/

Slide 539

Mote message format

Variants of the system exist with Atmega128 processor and a Chipcon CC1000 radio. Other researchers have simply used the physical layer part of Bluetooth (i.e., not including any of the link and higher layers at all).

Message format:

- training sequence of alternating high and low bits (used to equalize the DC balance of the receiver)
- a flag byte was used to signal the beginning of the packet protocol: 01110110 (to differentiate itself more from the training sequence)
- a byte which specifies the total data bytes in the packet
- 1 .. 255 data byes
- a 16 bit CRC (cyclic-redundancy check)

Slide 540

Motes - Routing

Ad hoc routing layer

- determines the routing topology
- enables forwarding of real sensor data up the routing topology to a base-station

At the base-station, the data is now being forwarded into a vSpace base for storage and display.

Slide 541

vSpace

Data is persistently stored using Distributed Data Structures (DDS)

- build on a distributed hash table
- allows multiple clients to simultaneously updating and querying the sensor data
- Queries comes through an HTTP interface
- Users can view an image of the current network routing topology
  - users can zoom in to see detailed information about any of the sensor nodes in the network
  - green lines show routing topology and red lines show connectivity
- They hope to display dynamically generated graphs of sensor data in multiple forms, including:
  - single node time plot
  - aggregate time plots
  - and multiple plots in a single plot

See [Ross2000]

Maguire IK2555, Spring 2016 Slide 541

[Ross2000] Steve Ross, Jason Hill, Mike Chen, Anthony Joseph, Dave Culler, and Eric Brewer, A Composable Framework for Secure Multi-Modal Access to Internet Services from Post-PC Devices, Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), Monterey, California, December 7-8, 2000 (see the link from *http://www.mikechen.com/publications.php*)

Slide 542

Sensor nodes - low power VLSI design

µAdaptive Multi-domain Power aware Sensors (µAMPS) project at MIT http://www-mtl.mit.edu/researchgroups/icsystems/uamps/research/overview.shtm

- AMPS-I: voltage scalable processor, adaptive transmit power, flexible error coding and aggressive subsystem shutdown
- AMPS-II: integrated sensor node: a digital and an analog/RF ASIC (intermediate FPGA implementation of the digital part interfaced with the version-1 radio system.

See the Mobicom 2002 poster Rex Min and Anantha Chandrakasan, "Top Five Myths about the Energy Consumption of Wireless Communication" http://www.rle.mit.edu/media/pr145/06.pdf

see also [Min2001]

Maguire IK2555, Spring 2016 Slide 542

[Min2001] Rex Min, Manish Bhardwaj, Seong-Hwan Cho, Amit Sinha, Eugene Shih, Alice Wang, and Anantha Chandrakasan, "Low-Power Wireless Sensor Networks", in Fourteenth International Conference on VLSI Design, 2001, pp. 205–210, DOI:10.1109/ICVD.2001.902661, Available at http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=902661 .

Slide 543

Rex Min's Myths

- MYTH#5. Abstraction gets in the way of energy savings

  Instead: Create a power aware API - explicitly define and expose tradeoffs:

  set_max_energy(Joules), set_max_latency(ms), set_min_reliability(float probability), set_range(int nearest nodes, Note[] who, float meters)
- MYTH #4. Energy-quality scalability does not work for wireless

  Create an API which gives you explicit control over energy vs. quality.
- MYTH #3. Derivatives of 802.11 will drive emerging low-power nets
  - Microsensors arrays with large numbers of sensors each with 2J to 2KJ of energy and 1 to 54kbps data rate vs. 20KJ to 20MJ for 802.11b at 1 to 54Mbps!
- MYTH#2. Communication energy scales
  - d = distance between the nodes, α = static power, digital signal processing, β = power amplifier, receiver sensitivity

$$E_{bit} = \alpha + \beta d^n$$

Radio	α	Maximum βd^n
2.4 KHz OOK (RFM TR1000 @ 916 MHz)	14 µJ	3.1 µJ
115.2 KHz ASK (RFM TR1000 @ 916 MHz)	372 nJ	65 nJ
11 Mbps Custom (MIT µAMPS-1 @ 2.4 GHz)	570 nJ	740 nJ
11 Mbps 802.11b (Cisco Aironet 350 @ 2.4GHz)	236 nJ	91 nJ
54 Mbps 802.11a (Atheros, ISSCC2002)	14.8 nJ	11 nJ

Maguire IK2555, Spring 2016 Slide 543

Slide 544

Rex Min's Myth #1

- MYTH#1. Multihop saves energy
  Two hops are better than one -- NEVER!
  Since multihop energy > single hop energy

Slide 545

SmartBadge (aka BadgePad): 1997-2001

G. Q. Maguire Jr. (KTH) in conjunction with Mark T. Smith (then of HP Labs, now KTH) and H. W. Peter Beadle (then of the Univ. of Wollongong (Australia)):

- ID card sized, communicates via wireless link to badge server
- temperature, humidity, light, audio in/out, and tilt or 3-axis acceleration
- used in courses at both KTH and Univ. of Wollongong; and numerous MS thesis projects

Version 1- Spring 1997

Version 3 - April 1998

Version 4 - February 2001

SmartBadge series

Slide 546

Power

- Batteries
- Super capacitors
- Fuel cells
- Energy-harvesting utilizing
  - solar cells, movement to electricity conversion (mechanical, piezo-electrics, …)
  - DC boosters

Slide 547

Dilemma

"Since communication is expensive in energy, the cost of the power management algorithm would swamp the savings from power management! **This illustrates the dilemma that so often arises in problems in sensor nets: the seemingly optimal way of solving a problem often results in algorithms whose communication energy costs exceed their benefits.** Therefore, a better strategy is to use algorithms that only shoot for good though sub optimal results but require only locally distributed processing with minimal communication costs." [Estrin2001] †

-- D. Estrin, L. Girod, G. Pottie, and M. Srivastava

⇒ *adaptive duty cycle* (based on needs of the neighborhood and applications, and the rate with which events are likely to happen) -- applies at multiple levels in the system

† The emphasis is as in the original.

Maguire IK2555, Spring 2016 Slide 547

[Estrin2001] D. Estrin, L. Girod, G. Pottie, and M. Srivastava, "Instrumenting the World with Wireless Sensor Networks", International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2001), Salt Lake City, Utah, May 2001

Slide 548

Sensor Modeling Language (SensorML)

SensorML provides an Extensible Markup Language (XML) schema for defining the geometric, dynamic, and observational characteristics of a sensor. Sensors are devices for the measurement of physical quantities.

-- "Sensor Model Language (SensorML) for In-situ and Remote Sensors", Editor: Mike Botts, University of Alabama in Huntsville, Open GIS Consortium Inc., OpenGIS © Project

Document: OGC 02-026r4, Version: 0.7, 2002-12-20

contact: mike.botts@nsstc.uah.edu.

See http://www.opengeospatial.org/

Slide 549

IEEE 802.15: Working Group for Wireless Personal Area Networks (WPAN)

IEEE 802 family -- "standards for low-complexity and low-power consumption wireless connectivity".
http://standards.ieee.org/wireless/overview.html#802.15

IEEE 802.15 (http://ieee802.org/15/) standards development projects:

IEEE 802.15.1	Mb/s WPAN/Bluetooth v1.x derivative work (cooperative effort with Bluetooth SIG, Inc. http://www.bluetooth.com/)
IEEE 802.15.2	Recommended Practice for Coexistence in Unlicensed Bands
IEEE 802.15.3	20+ Mb/s High Rate WPAN for Multimedia and Digital Imaging
IEEE 802.15.3a	110+ Mb/s Higher Rate Alternative PHY for 802.15.3 Uses pulse position modulation (PPM)
IEEE 802.15.4	for low-rate wireless personal area networks (LR-WPANs) - physical + MAC sublayer or 6LoWPAN and ZigBee; 127 octet frame size 250 kbps max for interactive toys, sensor and automation needs

Maguire IK2555, Spring 2016 Slide 549

D. Hélal and P. Rouzet. ST Microelectronics Proposal for IEEE 801.15.3a Alternate PHY. IEEE 802.15.3a/document 139r5, July 2003.

IEEE Standards for Information Technology-Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPAN), IEEE, 2003, ISBN 0-7381-3705-7

James P. K. Gilb, Wireless Multimedia: A Guide to the IEEE 802.15.3 Standard, IEEE Press, 2003, 250 pages, ISBN 0-7381-3668-9

Slide 550

6LoWPAN

IPv6 Low power Wireless Personal Area Network (6LoWPAN) is described in :

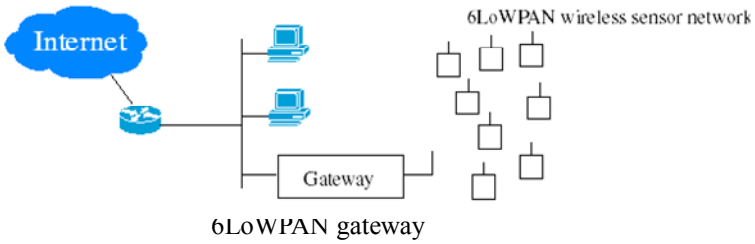
G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, 'Transmission of IPv6 Packets over IEEE 802.15.4 Networks', Internet Request for Comments, vol. RFC 4944 (Proposed Standard), September 2007, Available at http://www.rfc-editor.org/rfc/rfc4944.txt .

Some issues about integrating 6LoWPAN into an IPv6 subnet are addressed in:

Luis Maqueda Ara, Neighbor Discovery Proxy-Gateway for 6LoWPAN-based Wireless Sensor Networks: Design, Implementation, analysis, and evaluation, TRITA-ICT-EX-2011:221, December 2011 http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-53608

Slide 551

Gateways between wireless sensor networks and fixed networks



IPv6 over Low power Wireless Personal Area Networks (6LoWPAN)

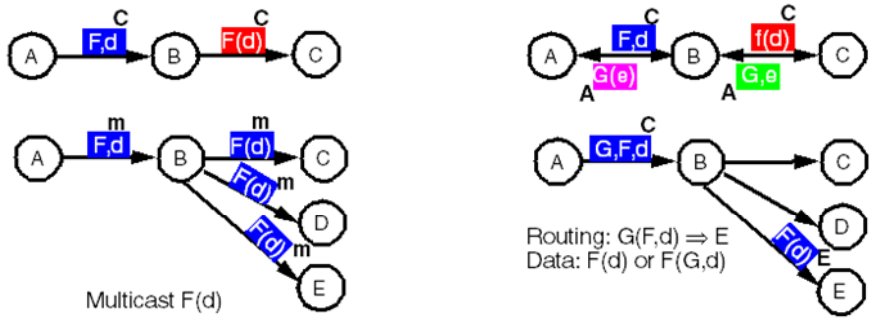
See Luis Maqueda Ara's master's thesis: Neighbor Discovery Proxy-Gateway for 6LoWPAN-based Wireless Sensor Networks: Design, Implementation, analysis, and evaluation [Ara2011] describes how to integrate the 6LoWPAN nodes as IPv6 hosts - *without* their needing to be in a separate IPv6 network.

Maguire IK2555, Spring 2016 Slide 551

[Ara2011] Luis Maqueda Ara, Neighbor Discovery Proxy-Gateway for 6LoWPAN-based Wireless Sensor Networks: Design, Implementation, analysis, and evaluation, Master's thesis, KTH Royal Institute of Technology, School of Information and Communications Technology, TRITA-ICT-EX-2011:221, December 2011, http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-53608

Slide 552

Active networks



B acts as an intermediary between A and x:
(1) **operates** on the **data** as it passes through using the "program" F and/or
(2) **routes** based on the computed **address** using a "program" G

Packets carry the **program** that each node on the path is to execute.
{Even the program(s) can be transformed as the packet propagates.}

Slide 553

Methods used in for research in wireless sensor networks

- Analytic - frequently graph theoretical
- Simulation - frequently using “ns-2”, now: “ns-3” (http://www.nsnam.org/)
- Experiments
  - small scale
  - large scale

Very few large scale experiments

Slide 554

Battery exhaustion attacks & prevention

If the battery is not rechargeable, then draining the battery renders the device useless

Possible prevention: Short Message Authentication CheckK (SMACK) described in:

- Rikard Höglund, Lightweight Message Authentication for the Internet of Things, Master's thesis, KTH/ICT, TRITA-ICT-EX-2014:136, November 2014 http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-156185
- Unfortunately, it takes more power than it saves!

Slide 555

References and Further Reading

Gregory J. Pottie and William J. Kaiser, *Principles of embedded networked systems design*. Cambridge ; New York: Cambridge University Press, 2005, ISBN: 978-0-521-84012-5.

Raquel Aparecida de Freitas Mini, http://www.cs.rutgers.edu/~mini/sensornetworks.html -- an excellent bibliography for this area

Al Demers and Johannes Gehrke, organized a database seminar course: CS735: Sensor Networks and Data Management, Cornell University, 30 November 2001, http://www.cs.cornell.edu/courses/cs735/2001fa/

Ugur Cetintemel, CS 295-1. Pervasive Computing, Course at Brown University, 18 November 2005, http://www.cs.brown.edu/courses/cs295-1/schedule.htm

Jason Hill, Robert Szewczyk, and Alec Woo (together with Professors David E. Culler and Kristofer S. J. Pister), "TinyOS: Operating System for Sensor Networks", (DARPA) DABT 63-98-C-0038, (DARPA) DABT 63-98-1-0018, and (NSF) RI EIA-9802069, formerly at http://www.eecs.berkeley.edu/IPRO/Summary/01abstracts/szewczyk.1.html

RF Monolothics TR1000 radio

ZigBee™ Alliance http://www.zigbee.org/

DARPA SENSIT project, last modified 27 August 2002, http://www.eng.auburn.edu/users/lim/sensit.html

Pennsylvania State University, Reactive Sensor Networks (RSN) project: http://strange.arl.psu.edu/RSN/

First ACM International Workshop on Wireless Sensor Networks and Applications. In conjunction with ACM MobiCom 2002. Sept. 28, 2002

Slide 556

John Heidemann, Fabio Silva, Chalermek Intanagonwiwat, Ramesh Govindan, Deborah Estrin, and Deepak Ganesan, "Building Efficient Wireless Sensor Networks with Low-Level Naming", in Proceeding SOSP '01 Proceedings of the eighteenth ACM symposium on Operating systems principles, 2001, pp. 146–159, DOI:10.1145/502034.502049, Available at http://portal.acm.org/citation.cfm?doid=502034.502049.

WINS project. formerly at http://www.janet.ucla.edu/WINS/

Ultra Low Power Wireless Sensors Project, formerly at http://www-mtl.mit.edu/~jimg/project_top.html

Deborah Estrin, David Culler, Kris Pister, and Gaurav Sukhatme, "Instrumenting the physical world with pervasive networks", IEEE Pervasive Computing, 2002.

D. Johnson and D. Maltz, "Protocols for Adaptive Wireless and Mobile Networking", IEEE Personal Communications Magazine, February 1996.

Ya Xu, John Heidemann, and Deborah Estrin, "Adaptive Energy-Conserving Routing for Multihop Ad Hoc Networks", Research Report 527, USC/Information Sciences Institute, October, 2000. http://www.isi.edu/~johnh/PAPERS/Xu00a.html

Sharad Agarwal, Randy H. Katz and Anthony D. Joseph, "Reducing the Energy Consumption of Group Driven Ad-hoc Wireless Communication", Report No. UCB/CSD-1-1127 January 2001, formerly at http://ncstrl.cs.cornell.edu:80/Dienst/UI/1.0/Display/ncstrl.ucb/CSD-01-1127).

Slide 557

A. Iwata, C.-C. Chiang, G. Pei, M. Gerla, and T.-W. Chen, "Scalable Routing Strategies for Ad-hoc Wireless Networks", IEEE JSAC, August 1999

Paul J. M. Havinga, Gerard J. M. Smit, and Martinus Bos, "Energy-Efficient Adaptive Wireless Network Design", in Proceedings of the Fifth IEEE Symposium on Computers and Communications (ISCC 2000), Washington, DC, USA, 2000, p. 502–, Available at http://dl.acm.org/citation.cfm?id=844383.845460

L. Schwiebert, S. K. S. Gupta, and J. Weinmann, "Research challenges in wireless networks of biomedical sensors", 2001, pp. 151–165, DOI:10.1145/381677.381692, Available at http://portal.acm.org/citation.cfm?doid=381677.381692.

Mani Srivastava, Richard Muntz and Miodrag Potkonjak, "Smart Kindergarten: Sensor-based Wireless Networks for Smart Developmental
Problem-solving Environments", The seventh annual international conference on Mobile computing and networking 2001, July 16 - 21, 2001, Rome Italy, pp 132 - 138

Sameer Tilak, Nael B. Abu-Ghazaleh, and Wendi Heinzelman, "A taxonomy of wireless micro-sensor network models", ACM SIGMOBILE Mobile Computing and Communications Review, vol. 6, no. 2, pp. 28–36, April 2002, DOI:10.1145/565702.565708, Available at http://portal.acm.org/citation.cfm?doid=565702.565708

Slide 558

¿Questions?

Slide 559: Lecture 12: Miscellaneous topics

IK2555: Mobile and Wireless Network Architectures: Lecture 12

prof. Gerald Q. Maguire Jr. http://people.kth.se/~maguire/

School of Information and Communication Technology (ICT), KTH Royal Institute of Technology

IK2555 Spring 2016 2016.01.08 © 2016 G. Q. Maguire Jr. All rights reserved.

Slide 560

12. Miscellaneous topics

Lecture notes of G. Q. Maguire Jr.

Slide 561

Delay Tolerant Networks (DTNs)

Traditional applications generally assumed that to some degree there was:
(1) end-to-end connectivity, (2) low round trip time, and
(3) access to naming/caching/searching/… infrastructures.

Delay Tolerant Networks do not require these assumptions, thus nodes can communicate using an opportunistic exchange of messages (think of the messages as a propagating virus - moving from host to host) (see [Sun2013]) ⇒ epidemic routing protocols [Vahdat and Becker2000].

Key issues include [Crowcroft2008]:

- What application layer data units are bundled into the DTN-layer protocol bundles for transport?
- Actual mobility patterns (social networks, commuting patterns, …)

Metrics include [Crowcroft2008]: Delivery ratio, Delivery Delay, and Delivery Cost

Maguire IK2555, Spring 2016 Slide 561

[Vahdat and Becker2000] Amin Vahdat and David Becker, "Epidemic Routing for Partially-Connected Ad Hoc Networks", Technical Report CS-2000-06, Duke University, July 2000. http://issg.cs.duke.edu/epidemic/epidemic.pdf

[Sun2013] Lan Sun, Epidemic Content Distribution in Mobile Networks: A study of epidemic content distribution characteristic with social relationship evaluation, TRITA-ICT-EX-2013:31, February 2013 http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-118470

[Crowcroft2008] Jon Crowcroft, Eiko Yoneki, Pan Hui, and Tristan Henderson, Promoting Tolerance for Delay Tolerant Network Research, Editorial Note, Computer Communication Review, Volume 38, number 5, October 2008, pp. 63-68. http://ccr.sigcomm.org/online/files/p63-crowcroft.pdf

Slide 562

Space Data Corporation

Space Data Corporation http://www.spacedata.net/ to provide low data rate wireless (messaging and later voice) service to rural and suburban US (about 90% of the land mass, but only 20% of the population); Piggyback their repeaters on US National Weather Service biodegradable latex weather balloons "SkySites".

Each balloon goes up to about 100,000 feet ~ 30km and stays there for ~1.5 days; balloons are launched from 70 sites twice each day; the repeater has power for 16 hours (12 for operation and the rest as a reserve). They expect to use 50,000 balloons per year, each repeater costs US$300

Their business model does not depend on any recovery of balloons (although they are adding GPS to theirs)

- US National Weather Service gets 18% of their back - they put a mailing address and promise to pay the postage on their payloads
- lots of knowledge of winds from 60 years of weather balloons

Space Data has a license for 1.4 MHz of bandwidth nationwide (license US$4.2M)

See also SkySat™ and SkySite®

Slide 563

Intelligent/Smart Spaces

Knowing what is around you is very useful for configuring devices and offering services, there are several proposals for how to do this:

- SUN's Jini
- Microsoft's Universal Plug-and-Play

For further information see Theo Kanter's dissertation "Adaptive Personal Mobile Communication -- Service Architecture and Protocols": http://kth.diva-portal.org/smash/get/diva2:9057/FULLTEXT01

Slide 564

If WLANs are widely available

- How many different places to do you frequently spend time?
- What would happen if you had WLAN access in X% of these places? (perhaps with X > 90%)
- What if you also had VoIP service in all the places you have WLAN access?

⇒ Is there a business case for 3G in urban areas?

⇒ Is there a business case for 3G anywhere?

Handoffs for real-time media: J-O Vatn's dissertation [Vatn2005]

Broadcom Wi-Fi reference design using their BCM1160 Mobile VoIP processor and BCM94318SD WLAN, in addition to their BCM4318 AirForce OneChip which integrates 802.11b/g Baseband, MAC, and radio.

LinkNYC: (planned) 10,000 free public Wi-Fi equipped kiosks in NYC - http://www.link.nyc/

1Gbps WLAN APs

Two 55 inch HD displays - ~$500 million over the next 12 years, mainly due to revenue from these digital mini-billboards [Leswing2016]

See also http://www.intersection.com/ and http://www.sidewalklabs.com/

Maguire IK2555, Spring 2016 Slide 564

[Vatn2005] Jon-Olov Vatn, IP telephony: Mobility and security, Tekn. Dr. Dissertation, Microelectronics and Information Technology, KTH Royal Institute of Technology, TRITA-IMIT-TSLAB AVH 05:01, 2005 http://urn.kb.se/resolve?urn=urn%3Anbn%3Ase%3Akth%3Adiva-260

[Leswing2016] Kif Leswing, 'New York City Is Turning On Its Google-Owned Free Wi-Fi Network - Fortune', *Fortune Magazine*, 06-Jan-2016. [Online]. Available: http://fortune.com/2016/01/05/link-nyc-unveiled/ . [Accessed: 07-Jan-2016]

Slide 565

Over the top (OTT) services

OTT services provide a service independently of the operator, i.e., the cellular operator is simply used as a “pipe”.

Examples of OTT voice services are Skype, Viber, …

Google Project Fi https://fi.google.com/about/ exploits Wi-Fi connectivity when available

⇒ Operators are launching Wi-Fi Calling and voice over LTE (VoLTE) to try to compete with OTT voice services, see for example [La and Hoyle2015], [Dano2015], and http://www.gsma.com/network2020/volte/

Maguire IK2555, Spring 2016 Slide 565

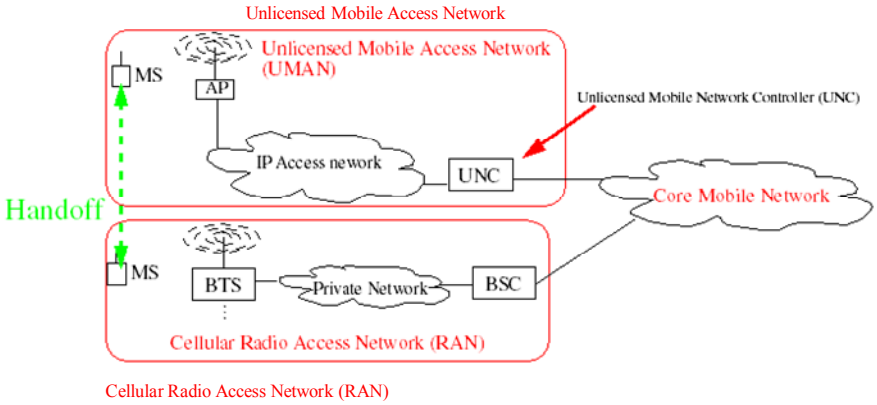
[La and Hoyle2015] Lynn La and Andrew Hoyle, ‘What you need to know about Wi-Fi calling: Curious about Wi-Fi calling and what it entails? CNET has the rundown on what you need to know.’, *CNET*, 08-Oct-2015. [Online]. Available: www.cnet.com/news/what-you-need-to-know-about-wifi-calling/

[Dano2015] Mike Dano, ‘T-Mobile: 1/3 of all calls are now VoLTE’, *FierceWirelessTech*, 11-Nov-2015. [Online]. Available: http://www.fiercewireless.com/tech/story/t-mobile-13-all-calls-are-now-volte/2015-11-11

Slide 566

Unlicensed Mobile Access (UMA)

To provide access to GSM and GPRS mobile services over unlicensed spectrum technologies, e.g., Bluetooth and IEEE 802.11:

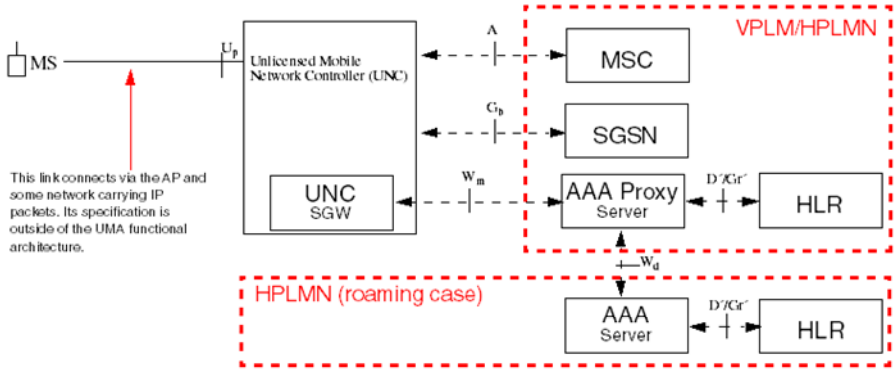


Unlicensed Mobile Network Controller (UNC) plays a role similar to the BSC in 3GPP, but also must deal with Authentication and Authorization. MS must be at least **dual** mode. See: http://www.umatechnology.org/

Slide 567

UMA Functional Architecture

Note that the emphasis in UMA is for operators to be able to offer to their subscribers the ability to roam to and handoff to/from various unlicensed wireless access networks



Slide 568

Near Field Communications

Goal is wireless communications by "touch" or proximity.

- I know whom I'm talking with because I'm beside them.
- I'm indicating that object - by touching it.

Focus is point-to-point over **very short** distances, base on RFID technology at 13.56MHz, data rates upto 424 kilobits/s

Some of the relevant standards: ISO 14443 - Proximity Card and ISO 15693 - Vicinity Card

For example, a NFC phone could act as your transit card (due to the computing capabilities and battery power - it could implemented better security than the storage only cards - such as those used in Stockholm) - it can even be a context dependent multi-card (i.e., able to implement many virtual cards).

There is a large battle over who should control the security element used in conjunction with the NFC interface.

Maguire IK2555, Spring 2016 Slide 568

"Near Field Communication", ECMA, Ecma/TC32-TG19/2005/013, Feb. 2005 http://www.ecma-international.org/activities/Communications/tc32-tg19-2005-013.pdf

"Near Field Communication - Interface and Protocol (NFCIP-1)", ECMA-340 , Second edition, December 2004 http://www.ecma-international.org/publications/standards/Ecma-340.htm

"Near Field Communication Interface and Protocol - 2 (NFCIP-2)", ECMA-352, December 2003 http://www.ecma-international.org/publications/standards/Ecma-352.htm

"NFCIP-1 - RF Interface Test Methods". ECMA-356, June 2004 http://www.ecma-international.org/publications/standards/Ecma-356.htm

"NFCIP-1 - Protocol Test Methods", ECMA-362, Second edition, December 2005 http://www.ecma-international.org/publications/standards/Ecma-362.htm

Slide 569

Radio Frequency Identification

see the course IS2500: RFID Systems, taught by Prof. Mark T. Smith
https://www.kth.se/social/course/IS2500/

Slide 570

Cognitive Radios

What kind of radio should a Software Defined Radio be for the purposes needed now and in the current environment?

This is the question behind Cognitive Radios [Mitola and Maguire1999], first raised in a licentiate [Mitola1999] and dissertation [Mitola2000] by Joseph Mitola III at KTH.

Today cognitive radios have been accepted as a class of radios by the U.S. FCC and there are quite a number of research groups exploring this area and others such as:

- Dynamic Spectrum usage
- Secondary spectrum users

See IEEE J-SAC special issue on Adaptive, Spectrum Agile, and Cognitive Wireless Networks [215] and the Crowncom conference series (http://crowncom.org).

Maguire IK2555, Spring 2016 Slide 570

[Mitola and Maguire1999] Joseph Mitola III and G. Q. Maguire Jr., Cognitive Radio: Making Software Radios More Personal, IEEE Personal Communications, Volume 6, Number 4, August 1999, pp. 13-18.

[Mitola1999] Joseph Mitola III, Cognitive Radio: Model Based Competence for Software Radios, Tekn. Licentiate, KTH Royal Institute of Technology, TRITA-IT 99:04, ISRN: KTH/IT/AVH--99/04--SE, 1999. http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-970

[Mitola2000] Joseph Mitola III, Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio, Tekn. Dr. Dissertation, KTH Royal Institute of Technology, TRITA-IT AVH 00:01, 2000. http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-2987

Slide 571

New mobile services

According to Per Andersson, et al. one of the main reasons for the failure by telecommunication operators to sell new mobile services to enterprise customers was their lack of understanding of the inner logics of these businesses - as opposed to selling mobile subscriptions which were basically the same as fixed subscriptions.

[see P. Andersson, et al. *Mobile Organizations*, to be published (as quoted on pg. 52 of Chapter 2: "Mobile Offerings, Mobility and the Creation of Value from Wireless Offerings" by Per Andersson, Ulf Essler, & Christopher Rosenqvist in *Beyond Mobility*, Per Andersson, Ulf Essler, and Bertil Thorngren (Eds.), EFI Yearbook 2007, Studentlitteratur, ISBN 978-91-44-04928-1).]

Slide 572

Free

Chris Anderson's *Free: The Future of a Radical Price* [Anderson2009] discusses how businesses can make money in an age when lots of things are free (i.e., a price of $0.00)

A key insight is that in the digital economy, when the "margin cost" is near zero, then round down to zero.

⇒ Freeconomics

⇒ Freemium (a free version and a matching premium version)

He gives interesting example of how air travel can be free (pg. 19), how a DVR can be free (pg. 21), how everything in a store can be free (pg. 60), how a car can be free (pg. 81), healthcare (pg. 104), trading stocks (pg. 113), webmail (pg. 115), an exclusive conference (pg. 117), directory assistance (pg. 122), silverware (pg. 141), music CDs (pg. 155), textbooks (pg. 160), university education (pg. 185), and second hand goods (pg. 188).

Maguire IK2555, Spring 2016 Slide 572

[Anderson2009] Chris Anderson, Free: The Future of a Radical Price, Hyperion, July 7, 2009, 288 pages, ISBN-10: 1401322905, ISBN-13: 978-1401322908 or paper back ISBN 978-1-9052-1148-7

Slide 573

Too cheap to meter

"It is not too much to expect that our children will enjoy in their homes electricity too cheap to meter, -- will know of great periodic regional famines in the world only as matters of history, -- will travel effortlessly over the seas and under them and through the air with a minimum of danger at great speeds, -- and will experience a lifespan far longer than ours as disease yields and man comes to understand what causes him to age."

-- Lewis L. Strauss, Chairman of the U.S. Atomic Energy Commission In an address to the National Association of Science Writers 16 Sept. 1954

Today three other technologies are approaching the too cheap to measure point:

- computing power
- digital storage
- communication bandwidth

⇒ faster, better, cheaper -- a "triple play" for on-line services

Slide 574

Working for free

Once you have food, shelter, … (Maslow's subsistance needs†) people move on to social needs, esteem needs, and "self-actualization" - using their cognitive surplus (the energy and knowledge that isn't used for your "job")- page 189 of [Anderson2009]

Hence the importance of:

- community
- visibility
- because I like to do it ("fun")

These are driving forces behind open source software/hardware, web pages, social networks, Wikipedia, … .

See Andrew Lih, *The Wikipedia Revolution: How a Bunch of Nobodies Created the World's Greatest Encyclopedia* [Lih2009]

†"Hierarchy of Needs": physiological, safety, social, esteem, self-actualization; see Abraham H. Maslow, Motivationand Personality, Harper 1954

Maguire IK2555, Spring 2016 Slide 574

[Anderson2009] Chris Anderson, Free: The Future of a Radical Price, Hyperion, July 7, 2009, 288 pages, ISBN-10: 1401322905, ISBN-13: 978-1401322908 or paper back ISBN 978-1-9052-1148-7

[Lih2009] Andrew Lih, The Wikipedia Revolution: How a Bunch of Nobodies Created the World's Greatest Encyclopedia, Hyperion 2009, 272 pages, ISBN-10: 1401303714 and ISBN-13: 978-1401303716
http://wikipediarevolution.com/The_Book.html

Slide 575

What Would Google Do?

Jeff Jarvis' *What Would Google Do? (WWGD)* [Jarvis2009] explores re-thinking how you do business by finding a new world view and seeing things differently

The book is not about what would Google as a business do, but rather what seeing the world as Google sees it - then thinking differently about solving problems could do†.

Rather than thinking about "Will it make money?", start with:

- Will users think it is cool?
- Will it scale to support 100 million users?
- Is there a positive feedback cycle as it grows?

See Buzzmachine.com for more about the book For a counterpoint see: Ken Auletta, *Googled: The End of the World as We Know It* [Auletta2009]

†. I refer to it as "enlighted self-interest"

Maguire IK2555, Spring 2016 Slide 575

[Jarvis2009] Jeff Jarvis, What Would Google Do?, Collins Business, 2009, ISBN 978-0-06-170971-5.

[Auletta2009] Ken Auletta, Googled: The End of the World as We Know It, Penguin Press HC, (November 3, 2009), 400 pages, ISBN-10: 1594202354, ISBN-13: 978-1594202353 - also in paperback from Virgin Books

Slide 576

Future work

Today we can combine:

- **Mobility**: interworking with all different types of access networks
- **Security**: IPsec, TLS, SRTP+MIKEY, … + SIP ⇒ secure VoIP
- **Context and location awareness**: minimizing manual (re-)configuration as users move about and facilitating their interaction with each other & the things around them - Adaptive and Context-Aware Services (ACAS)†
- **Cloud computing**

⇒ **New services**: such as audio services - managing a 3D (or 4D) audio environment, *automatic* call diversion, …

⇒ **New ways of providing and scaling services**: see the Master's thesis: Isaac Albarrán and Manuel Parras, Telecommunication Services' Migration to the Cloud: Network Performance analysis [Albarrán and Parras 2012].

In a challenging environment of **socially correlated** user movements (i.e., classes, meetings, etc.)

† Formerly avialable via http://psi.verkstad.net/acas/ (part of Affordable Wireless Services & Infrastructures project http://www.wireless.kth.se/AWSI/)

Maguire IK2555, Spring 2016 Slide 576

[Albarrán and Parras 2012] Isaac Albarrán and Manuel Parras, Telecommunication Services' Migration to the Cloud: Network Performance analysis, Master's thesis, KTH/ICT/CoS, TRITA-ICT-EX-2012:54, April 2012

Slide 577

New Players

Public services + Profit + Altruism

- Community networks
  - Municipal governments: City of Philadelphia
  - Cooperatives
  - Communities of like minded users: Phon, …
  - Regional and National Governments
  - International organizations, potentially including Non-government Organizations (NGOs)
- Commercial networks: Google, …
  - Another path to their users
- Business networks
  - For their own users (ala PBX like systems and LANs)
  - Open to non-employees (perhaps for a price) - see for example cruise ships [Shahzad and Jain2007]
- Existing communications operators
  - but not in their usual locations (for example, as virtual network operators)
  - raise of national roaming - see Johan Hultell's dissertation [Hultell2008]

Maguire IK2555, Spring 2016 Slide 577

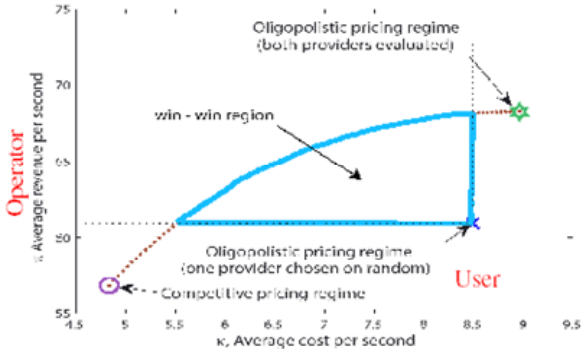
[Shahzad and Jain2007] Hamid Shahzad and Nishant Jain, "Internet Protocol based Mobile Radio Access Network Architecture for Remote Service Areas", Masters Thesis, KTH Royal Institute of technology, School of Information and Communication Technology, COS/CCS 2007-24 http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-91940

[Hultell2008] Johan Hultell Andersson, Cooperative and non-cooperative wireless access: Resource and infrastructure sharing regimes, Dissertation, Department of Communication Systems, School of Information and Communication Technology, KTH Royal Institute of Technology, December, 2008.

Slide 578

Cooperative Wireless Access

Johan Hultell [Hultell2008] points out that it is possible for operators to share access to their networks (à la national roaming) and that this leads to a reduction in the operators revenue of ~10% while the users decrease their cost per bit by ~50%!



Solution space for two providers coexisting (each with an average demand of 1 user/s/AP) Figure 6.15 on page 199 of the dissertation of Johan Hultell [Hultell2008] (appears with his permission)

The advantages of resource pooling are also examined in another paper[Wischik2008]. Advantages include: better handling of bursty traffic, increased robustness against link failure, and easier traffic engineering.

Maguire IK2555, Spring 2016 Slide 578

[Hultell2008] Johan Hultell Andersson, Cooperative and non-cooperative wireless access: Resource and infrastructure sharing regimes, Dissertation, Department of Communication Systems, School of Information and Communication Technology, KTH Royal Institute of Technology, December, 2008.

[Wischik2008] Damon Wischik, Mark Handley, and Marcelo Bagnulo Braun, "The Resource Pooling Principle", ACM/SIGCOMM Computer Communication Review, Volume 38, Number 5, October 2008, pp. 47-52
http://ccr.sigcomm.org/online/files/p47-handleyA4.pdf

Slide 579

Resource pooling

Damon Wischik, Mark Handley, and Marcelo Bagnulo Braun in their article "The Resource Pooling Principle" [Wischik2008] define resource pooling as:

"Resource pooling means making a collection of networked resources behave as though they make up a single pooled resource. The general method of resource pooling is to build mechanisms for shifting load between various parts of the network."

They go on to make two observations:

1. "Resource pooling is often the only practical way to achieve resilience at acceptable cost."
2. "Resource pooling is also a cost-effective way to achieve flexibility and high utilization."

Maguire IK2555, Spring 2016 Slide 579

[Wischik2008] Damon Wischik, Mark Handley, and Marcelo Bagnulo Braun, "The Resource Pooling Principle", ACM/SIGCOMM Computer Communication Review, Volume 38, Number 5, October 2008, pp. 47-52
http://ccr.sigcomm.org/online/files/p47-handleyA4.pdf

Slide 580

Resource pooling examples

Resource pooling can be used for:

- sharing lines/links/sites
- sharing storage
- computing power

This leads to grid computing, computing clouds (or Cloud Computing), …

Consider the proposal for Green IT by Bill St. Arnaud of Canada's CANARIE:

http://green-broadband.blogspot.com/ - put server farms in places with local renewable energy supplies - then move the bits to/from the user

⇒ moving Gigabits/second vs. Gigawatts

This implies the use of dense wavelength division multiplexing (DWDM) over optical fibers from these (often remote) sites to where the users are.

Slide 581

Increasing data traffic

See the Ericsson Mobility Report November 2012 [Ericsson2012] (http://www.ericsson.com/res/docs/2012/ericsson-mobility-report-november-2012.pdf) specifically the Figure 9: "Global total traffic in mobile networks, 2007-2012" http://www.flickr.com/photos/ericsson_images/8201799851/in/set-72157632057816280 on page 9 of the report

Note that this traffic data does **not** include Digital Video Broadcasting - Handheld (DVB-H), Wi-Fi, or Mobile WiMAX traffic.

Maguire IK2555, Spring 2016 Slide 581

[Ericsson2012] Ericsson Mobility Report: On the pulse of the network society, Ericsson, EAB-12:063053, November 2012, http://www.ericsson.com/res/docs/2012/ericsson-mobility-report-november-2012.pdf

Slide 582

Tethering

Increasingly one device with a wide area wireless network interface acts as a router for other devices via Wi-Fi or other radio ⇒ your smartphone as a mobile hotspot

However, not all carriers like this as this means that your devices which large screens (and hence larger amounts of traffic) will be transferring traffic over the wide area network. For more details see: Sarah Jacobsson Purewal,"The ultimate Android tethering guide", PC World, 5 September 2012,

http://www.pcworld.com/article/261928/the_ultimate_android_tethering_guide.html

Slide 583

Wi-Fi to HDMI devices (aka Display dongles)

Google's Chromecast: https://www.google.com/chromecast

- Chromecast app: communicates from your smartphone to a Chromecast device (dongle) with HDMI connector
- Dual band 2.4 and 5GHz, and support for 802.11ac

Intel® Compute Stick

- Intel® Atom™ or Core™ M processor + memory + flash
- Wi-Fi 802.11bgn, Bluetooth 4.0

See also Intel's Wireless Display (WiDi) technology and Miracast and Wi-Fi Alliances' Wi-Fi Direct®

Slide 584

Wi-Fi and unlicensed LTE

Efforts for co-existance of Wi-Fi and unlicensed LTE, see [Lawson2015]

Maguire IK2555, Spring 2016 Slide 584

[Lawson2015] Stephen Lawson, 'Wi-Fi Alliance reaches for peace over unlicensed LTE', *ITworld*, 09-Oct-2015. [Online]. Available: http://www.itworld.com/article/2990978/wi-fi-alliance-reaches-for-peace-over-unlicensed-lte.html . [Accessed: 07-Jan-2016]

Slide 585

Wi-Fi Aware™

Power efficient discovery of nearby devices

Slide 586

What is in the near future?

- Mobile phones today are greater than the computing power as PCs of 2007.
- Access link data rates are increasingly “broadband” data rates.
- Foldable displays, heads up displays, projection displays, etc. are increasing the virtual size of the device’s screen.
- Displays are advancing from color to 3D.
- Phones are not only getting GPS and **sensors**, but also supersensors - such as long range lenses for the camera(s).
- Phones are increasingly the default router for other wireless devices, such as sensors and other peripherals.
- The devices will provide natural language interfaces (speech, writing, signing, etc.) and provide the user with an augmented reality experience.
- Ambient Networking (local devices communicating and using each others information and resources) - potentially leads to emergent behavior.

See also the short executive summary: IBM Institute for Business Value. “Five telling years, four future scenarios”, 2010 [IBM2010]

Maguire IK2555, Spring 2016 Slide 586

[IBM2010] IBM Institute for Business Value. Five telling years, four future scenarios, 2010, 4 pages. http://www-05.ibm.com/cz/gbs/study/pdf/GBE03259USEN.PDF .

Slide 587

This course

This is the last offering of this course.

In the future there will be a new course:
IK2560: Mobile Networks and Services

Slide 588

¿Questions?