Universidade Virtual Africana

INFORMÁTICA APLICADA: CSI 5301

COMUNICAÇÕES MÓVEIS E SEM FIOS

Félix Singo

Prefácio

A Universidade Virtual Africana (AVU) orgulha-se de participar do aumento do acesso à educação nos países africanos através da produção de materiais de aprendizagem de qualidade. Também estamos orgulhosos de contribuir com o conhecimento global, pois nossos Recursos Educacionais Abertos são acessados principalmente de fora do continente africano.

Este módulo foi desenvolvido como parte de um diploma e programa de graduação em Ciências da Computação Aplicada, em colaboração com 18 instituições parceiras africanas de 16 países. Um total de 156 módulos foram desenvolvidos ou traduzidos para garantir disponibilidade em inglês, francês e português. Esses módulos também foram disponibilizados como recursos de educação aberta (OER) em oer.avu.org.

Em nome da Universidade Virtual Africana e nosso patrono, nossas instituições parceiras, o Banco Africano de Desenvolvimento, convido você a usar este módulo em sua instituição, para sua própria educação, compartilhá-lo o mais amplamente possível e participar ativamente da AVU Comunidades de prática de seu interesse. Estamos empenhados em estar na linha de frente do desenvolvimento e compartilhamento de recursos educacionais abertos.

A Universidade Virtual Africana (UVA) é uma Organização Pan-Africana Intergovernamental criada por carta com o mandato de aumentar significativamente o acesso a educação e treinamento superior de qualidade através do uso inovador de tecnologias de comunicação de informação. Uma Carta, que estabelece a UVA como Organização Intergovernamental, foi assinada até agora por dezenove (19) Governos Africanos - Quênia, Senegal, Mauritânia, Mali, Costa do Marfim, Tanzânia, Moçambique, República Democrática do Congo, Benin, Gana, República da Guiné, Burkina Faso, Níger, Sudão do Sul, Sudão, Gâmbia, Guiné-Bissau, Etiópia e Cabo Verde.

As seguintes instituições participaram do Programa de Informática Aplicada: (1) Université d'Abomey Calavi em Benin; (2) Université de Ougagadougou em Burkina Faso; (3) Université Lumière de Bujumbura no Burundi; (4) Universidade de Douala nos Camarões; (5) Universidade de Nouakchott na Mauritânia; (6) Université Gaston Berger no Senegal; (7) Universidade das Ciências, Técnicas e Tecnologias de Bamako no Mali (8) Instituto de Administração e Administração Pública do Gana; (9) Universidade de Ciência e Tecnologia Kwame Nkrumah em Gana; (10) Universidade Kenyatta no Quênia; (11) Universidade Egerton no Quênia; (12) Universidade de Addis Abeba na Etiópia (13) Universidade do Ruanda; (14) Universidade de Dar es Salaam na Tanzânia; (15) Universite Abdou Moumouni de Niamey no Níger; (16) Université Cheikh Anta Diop no Senegal; (17) Universidade Pedagógica em Moçambique; E (18) A Universidade da Gâmbia na Gâmbia.

Bakary Diallo

O Reitor

Universidade Virtual Africana

Créditos de Produção

Autor

Félix Singo

Par revisor(a)

Ambrosio Patricio Vumo

UVA - Coordenação Académica

Dr. Marilena Cabral

Coordenador Geral Programa de Informática Aplicada

Prof Tim Mwololo Waema

Coordenador do módulo

Victor Odumuyiwa

Designers Instrucionais

Elizabeth Mbasu

Benta Ochola

Diana Tuel

Equipa Multimédia

Sidney McGregor

Barry Savala

Edwin Kiprono

Kelvin Muriithi

Victor Oluoch Otieno

Michal Abigael Koyier

Mercy Tabi Ojwang

Josiah Mutsogu

Kefa Murimi

Gerisson Mulongo

Direitos de Autor

Apoiado por

Projeto Multinacional II da UVA financiado pelo Banco Africano de Desenvolvimento.

Índice

Descrição Geral do Curso

Bem-vindo(a) ao Módulo de Comunicações Móveis e sem Fios

Caro estudante,

Os avanços nas comunicações nos últimos anos possibilitaram o surgimento de várias tecnologias, que desde então procuram atender a real necessidade de seus usuários, com a melhor qualidade possível. Nos últimos anos a comunicação sem fio ganhou um espaço considerável nas tecnologias de transmissão de dados, deixando de existir apenas nas comunicações de longa distância (feitas através de satélite), para fazer parte de ambientes locais. É na perspectiva do entendimento deste fenômeno de evolução tecnológica que foi pensado este módulo. Nele vais aprender como funcionam as comunicações móveis celulares, as redes sem fios e como estas se relacionam com as redes IP que discutiste nos módulos anteriores.

Pré-requisitos

Para um melhor entendimento desta cadeira, considera-se como pré-requisito a conclusão com sucesso das seguintes disciplinas:

- Introdução à Informática Aplicada (Módulo BJ01)
- Redes de computadores e de comunicação de dados
- Sistemas operativos avançados

Materiais

Os materiais necessários para completar este curso incluem:

- Apontamentos das aulas
- Laboratorio de redes (Kit de antenas e rádios a de até 5GHz)
- Ferramentas de simulação (wi-fi scanner)
- Access Points

Objetivos do Curso

A disciplina tem como objectivo apresentar os fundamentos da computação móvel e sem fios e as diferentes tecnologias e arquitecturas que lhe dão suporte. Além disso, propõem introduzir os principais conceitos relacionados ao uso de dispositivos móveis, tais como plataformas, mecanismos de adaptação, problemas relacionados à tecnologia, suas vantagens e desvantagens, aplicações e casos de uso.

Assim, após concluir este curso, o(a) aluno(a) deve ser capaz de:

- Explicar os conceitos e técnicas que fundamentam a computação móvel e sem fios.
- Identificar a complexidade envolvida na computação móvel.
- Caracterizar os diferentes componentes de rede sem fios, Protocolos.
- Descrever os desafios que as redes sem fios e móveis colocam aos especialistas da área actualmente.
- Analisar os mecanismos de segurança nas redes de móveis e sem fios.

Unidades (4)

Unidade 0: Diagnóstico

Esta unidade faz a apresentação do módulo, seus objectivos de aprendizagem e sugere algumas estratégias de aprendizagem que o aluno poderá seguir.

Unidade 1: Origem e Evolução das Comunicações Móveis e sem Fio

Esta unidade permite obter conhecimento sobre o desenvolvimento das comunicações de rádio. Ele fornece uma compreensão das ondas de rádio e permite fazer as escolhas certas durante a implantação.

Unidade 2: Computação Móvel e sem Fios

Esta unidade discute com pormenores o conceito de computação móvel, olhando para as suas características e desafios. Na unidade são tratados também conceitos sobre WLAN e seu funcionamento; o Espectroelectromagnético; a Arquitectura 802.11, incidindo sobre as suas camadas de Enlace e Física, passando pelo protocolo CSMA/CA.

Unidade 3: Sistemas e normas para a telefonia sem fios

Global System para telemoveis - CDMA Digital Cellular standard (IS-95) - padrao CT2 para Telefones sem fio -Digital European Cordless Telephones (DECT)

Unidade 4: Segurança em sistemas Móveis e sem fio

Criar um ambiente seguro - Topicos- Tecnologias - Outras medidas de segurança WAP - Smart Client Security - Visao Geral da arquitectura Smart Client - Sistemas Operativos Móveis.

Avaliação

Em cada unidade encontram-se incluídos instrumentos de avaliação formativa a fim de verificar o progresso do(a)s aluno(a)s.

No final de cada módulo são apresentados instrumentos de avaliação sumativa, tais como testes e trabalhos finais, que compreendem os conhecimentos e as competências estudadas no módulo.

A implementação dos instrumentos de avaliação sumativa fica ao critério da instituição que oferece o curso. A estratégia de avaliação sugerida é a seguinte:

1	Avaliação formativa da unidade I - Origem e Evolução das Comunicações Móveis	5%
2	Avaliação formativa da unidade II - Computação Móvel e Redes Wireless	10%
3	Avaliação formativa da unidade III - Sistemas e normas para a telefonia sem fios	10%
4	Avaliação formativa da unidade IV - Segurança em sistemas Móveis e sem fio	5%
	Exame Final do Módulo	70%

Calendarização

Unidade	Temas e Atividades	Estimativa do tempo
I	**Origem e Evolução das Comunicações Móveis** - Dados e factos - Tendência actual (mobilidade e interoperabilidade) - Tipos de redes (sem fios e celulares digitais). - Caracterização do canal de comunicação - Comunicação rádio. Acividades: - Comunicações Móveis - Dados & Factos - Caracterização do canal de comunicação - Conceito de Comunicação Rádio - Avaliação formativa	25 horas 10 8 5 2
II	**Computação Móvel e Redes Wireless** - Mobilidade e Interoperabilidade - Desafios da computação móvel - Redes de comunicação sem fios - WLAN e o Padrão IEEE 802.11 - Arquitectura do 802.11 - Protocolo CSMA/CA Actividades: - Introdução a Computação Móvel - Redes de comunicação sem fios - Técnicas de acesso ao meio - Verificação da aprendizagem	30 horas 10 10 8 2

III	**Sistemas e normas para a telefonia sem fios** - Global System para telemoveis - CDMA Digital Cellular standard (IS-95) - Padrao CT2 para Telefones sem fio - Digital European Cordless Telephones (DECT) Acividades: - Acesso Múltiplo - Redes Móveis Celulares - Redes GSM, GPRS, EDGE e UMTS - Verificação da aprendizagem	30 horas 8 10 10 2
IV	**Segurança em sistemas Móveis e sem fio** - Criar um ambiente seguro - Topicos - Tecnologias - Outras medidas de segurança WAP - Smart Client Security - Visao Geral da arquitectura Smart Client - - Sistemas Operativos Móveis. Acividades: - Principais ameaças de segurança em redes móveis - Segurança em redes 3G - Segurança em Redes WiFi - Verificação da aprendizagem	20 horas 6 6 4 2
	Exame Final	2
	Total	120

Leituras e outros Recursos

As leituras e outros recursos deste curso são:

Unidade 0

Leituras e outros recursos obrigatórios:

- AREIAS, Gonçalo Menezes. Wireless IP, Universidade do Minho, 1999.
- MATEUS, Geraldo Robson, Loureiro, Antonio Alfredo, Introdução à Computação Móvel, 11a Escola de Computação, Rio de Janeiro, 1998.
- ARNETT, Matthew Flint; DULANEY, Emmett; HARPER, Eric et al. Desvendando o TCP/IP. Rio de Janeiro: Campus, 1997.

Unidade 1

Leituras e outros recursos obrigatórios:

- MATEUS, Geraldo Robson, Loureiro, Antonio Alfredo, Introdução à computação Móvel, 11a Escola de Computação, Rio de Janeiro, 1998.
- Vestias, Mario, Redes Cisco para Profissionais, 4ª ed., FCA, 2009
- Gouveia, J., Magalhães, A.: Redes de Computadores, 10ª edição, FCA, 2013.

Leituras e outros recursos opcionais:

- Singo, F.: Redes de Comunicação sem Fios, ESTEC, Material Interno, 2014.
- Pedro Vieira, Acetatos da unidade curricular —Comunicações Móveis‖, DEETC/ ISEL, 2007.

Unidade 2

Leituras e outros recursos obrigatórios:

- Vestias, Mario, Redes Cisco para Profissionais, 4ª ed., FCA, 2009
- Boavida, F., Bernardes, M., Vapi, P.: Administração de Redes Informáticas. FCA, 2008.

Leituras e outros recursos opcionais:

- Cota, N.: Acetatos da unidade curricular "Modelos e Simulação em Sistemas de Telecomunicações‖, DEETC/ISEL, 2000.
- Ericksson, —WiMAX tecnologia de banda larga‖, in Workshop WiMAX – Desafios e Oportunidades, ISEL, Lisboa, Portugal, 13 de Dezembro de 2006.

Unidade 3

Leituras e outros recursos obrigatórios:

- Boavida, F., Bernardes, M., Vapi, P.: Administração de Redes Informáticas, 2ª Edição FCA, 2011.
- Manual ITED – Prescrições e Especificações Técnicas das Infraestruturas de Telecomunicações em Edificios, ANACOM – Autoridade Nacional de Comunicações, 2009.
- Monteiro, E., Boavida, F.: Engenharia de Redes Informáticas, 10ª Edição, FCA, 2011.

Leituras e outros recursos opcionais:

- Singo, F.: Redes de Comunicação sem Fios, ESTEC, Material Interno, 2014
- Pinheiro, J. M.,: Infra-estrutura Electrica para Redes de Computadores, 1ª ed., Ciência Moderna, 2008.

Unidade 4

Leituras e outros recursos obrigatórios:

- Vestias, Mario, Redes Cisco para Profissionais, 4ª ed., FCA, 2009
- Zuquete, A.: Segurança em Redes Informáticas, 2ªed., FCA, 2009
- Paula, A.S.: Segurança em Redes Móveis. PUC Paraná, 2013
- Felix, J.A.: Introdução Normativa GSI/PR nº 1, 2008
- Molva, R.: Mobile Network Security. Institut Aurecom - France, 2005
- Azevedo, P.: Manual FTL, Sistemas de Comunicação Móveis.

Leituras e outros recursos opcionais:

- http://www.anacom.pt/
- https://www.meo.pt/
- http://www.vodafone.pt/
- http://www.otmus.pt/
- http://www.zapp.pt/

Unidade 0. Diagnóstico

Introdução à Unidade

O propósito desta unidade é verificar a compreensão dos conhecimento que possui relacionados com esta dis. Não se trata de uma prova de avaliação no sentido mais restrito. Trata-se sim de um teste de verificação. Precisas de saber em ponto partes para esta nova aventura. Por isso, mantenha a sua calma, leia as questões e depois apele a tudo aquilo que já aprendeste sobre redes IP e eventualmente aquilo que já leste em algum livro ou outro material sobre redes wireless e móveis.

Boa aprendizagem

Objetivos da Unidade

Após a conclusão desta unidade, deverá ser capaz de:

1. Estabelecer uma ligação entre Redes IP e redes sem fios
2. Identificar alguns conceitos relacionados com redes sem fios
3. Caracterizar o conceito da mobilidade no contexto da computação.

Avaliação da Unidade

Verifique a sua compreensão!

Instruções

O teste diagnóstico é composto por dez questões da área de comunicações móveis e sem fios. Pode acontecer que muitos dos termos utilizados não sejam ainda do teu domínio. Não desanime e não fique assustado com isso. É sinal de que vais aprender muita coisa nova neste módulo. As sete primeiras questões são de múltipla escolha. Pense primeiro antes de indicar a opção que julgar correcta. Podes consultar algum material se for o caso, isso é também uma forma de aprender. As três últimas questões são de resposta aberta. Dê largas à tua imaginação. No final podes comparar as tuas respostas com as do guião que vem abaixo da prova.

Critérios de Avaliação

A prova vale vinte valores como é costume. A tabela abaixo mostra os pesos das questões. No final da prova, depois da correcção, procure se avaliar usando essa pontuação.

Questões	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Pontos	2.0	2.0	1.5	1.5	1.5	1.5	1.5	3.0	2.5	3.0

Avaliação

1. Em qual país um sistema de telefonia móvel foi utilizado pela primeira vez?

- ☐ Estados Unidos da América
- ☐ Japão
- ☐ Inglaterra

2. Actualmente, qual padrão tecnológico é utilizado na telefonia móvel celular?

- ☐ FDMA
- ☐ GSM
- ☐ IDEN

3. A tecnologia CDMA tem uma abordagem diferente dos demais sistemas. Qual?

- ☐ É baseada em computadores
- ☐ Alterna Frequências
- ☐ Espalhamento dos dados

4. O que significa tecnologia 3G?

- ☐ Três vezes mais espaço para armazenar dados
- ☐ Terceira geração tecnológica
- ☐ Três pessoas falando ao mesmo tempo.

5. Por meio de quais dispositivos uma operadora de celular sabe de quem cobrar as chamadas?

- ☐ Através do telemóvel do usuário
- ☐ SID e FCC
- ☐ MIN e ESN.

6. Quantas frequências são utilizadas para que haja uma comunicação pelo celular?

- ☐ 1
- ☐ 2
- ☐ 3

7. O que possibilita a criação de aparelhos celulares cada vez menores?

- ☐ Transmissores de baixa potência
- ☐ Frequências reutilizáveis
- ☐ Transmissões de alta potência.

8. Para que serve o SSID?

9. As comunicações sem fios necessitam sempre de pelo menos um Access Point?

10. Um dispositivo que detecte uma rede sem fios pode de imediato começar a utilizá-la?

Guião de Correcção

Questão	Sugestão de resposta
Q1	Estados Unidos da América. O primeiro dispositivo de telefonia celular, chamado AMPS (Sistema de Telefonia Móvel Avançado), foi utilizado em 1983, na cidade de Chicago, nos Estados Unidos.
Q2	GSM. O GSM - Sistema Global para Comunicação Móvel ou Global System for Mobile Communications, em inglês - é o padrão internacional na Europa, Austrália e grande parte da Ásia e África.
Q3	Espalhamento de Dados. CDMA é uma forma de espalhamento espectral de dados, o que significa que as informações são enviadas em pequenas partes ao longo de diversas frequências diferentes disponíveis para uso, a qualquer momento, na faixa especificada.
Q4	3ª geração tecnológica. A tecnologia 3G é a mais recente nas comunicações móveis e significa "terceira geração", já que a tecnologia do celular analógico é de primeira geração e a do celular digital/PCS é de segunda geração. Esse sistema se destina aos telefones multimídia, que apresentam largura de banda ampliada e taxas de transferência para acomodar aplicações baseadas na Web e arquivos de vídeo e áudio.
Q5	MIN e ESN. Quando você faz uma chamada de seu telefone celular, ele transmite o ESN (Número Serial Eletrónico) e o MIN (Número de Identificação Móvel) para a rede no início da chamada. O par MIN/ESN é um rótulo exclusivo de seu telefone e é por meio dele que as operadoras identificam o proprietário do aparelho e das ligações.
Q6	Duas. Por ser um dispositivo full-duplex, o celular utiliza duas frequências. Uma para falar e outra independente para a escuta. Com isso, as pessoas podem conversar e ouvir ao mesmo tempo.
Q7	Transmissores de baixa Potência. Os celulares utilizam transmissores de baixa potência, o que possibilita o uso de baterias, pois opera com um consumo de energia pequeno. Dessa maneira, baterias reduzidas representam aparelhos cada vez menores.
Q8	O SSID é usado para identificar a rede. O acesso a um Access Point faz-se com o SSID respectivo. O SSID pode ter até 32 caracteres alfanuméricos.

Q9	Não. Dois ou mais dispositivos podem comunicar-se directamente entre si numa rede WLAN. Este tipo de redes é conhecido por IBSS ou rede Ad-hoc.
Q10	Não. É preciso satisfazer um conjunto de requisitos antes de poder utilizar a rede, nomeadamente deve usar a mesma frequência, o mesmo SSID, deve solicitar uma associação com o AP e, se for o caso, deve autenticar-se.

Leituras e Outros Recursos

As leituras e outros recursos desta unidade encontram-se na lista de "Leituras e Outros Recursos do curso".

Unidade 1. Origem e Evolução das Comunicações Móveis

Introdução à Unidade

No início da década de 1990, a rede telefónica mundial possuía milhões de telefones fixos. A distância deixava de ser um problema, já que tornava-se possível alcançar as pessoas através de seus telefones. Porém, existe uma grande diferença em alcançar o telefone e alcançar a pessoa. Quando a pessoa procurada não estava próxima do seu telefone, não era possível se comunicar com a pessoa. As comunicações móveis foram desenvolvidas para libertarem os dispositivos de comunicação, como o telefone, do par de fios que o prendiam à rede de cabos. Na unidade de aprendizagem que agora começa, vamos discutir este fenómeno e a forma como as tecnologias de comunicação vão evoluindo.

Objetivos da Unidad

Após a conclusão desta unidade, deverá ser capaz de:

1. Descrever os diversos tipos de redes sem fios e móveis existentes do ponto de vista da sua função,
2. Discutir a sua complementaridade, e explicar a forma como evoluíram ao longo do tempo.
3. Descrever a arquitectura das redes móveis celulares e relacionar os seus componentes com a função que desempenham no funcionamento global do sistema.

Termos-chave

Comunicação móvel: aquela onde existe a possibilidade de movimento relativo entre partes ou as partes sistêmicas envolvidas.

WPAN: Rede pessoal sem fio, utilizada para interligar dispositivos electrónicos fisicamente próximos, os quais não se quer que sejam detectados a distância.

WLAN: é uma rede local que usa ondas de rádio para fazer conexão entre seus dispositivos.

WMAN: Redes Metropolitanas Sem Fio. São redes de uso corporativo que atravessam cidades e estados baseadas na tecnologia wimax.

WWAN: são basicamente as tradicionais tecnologias do Telefone Celular de voz e alguns serviços de dados.

Rede sem fios: é uma infraestrutura das comunicações sem fio que permite a transmissão de dados e informações sem a necessidade do uso de cabos – sejam eles telefónicos, coaxiais ou ópticos.

Actividades de Aprendizagem

Actividade 1.1 - Comunicações Móveis - Dados & Factos

Olhando retrospectivamente, percebemos que o telégrafo terá sido o primeiro sistema de comunicação inventado pelo homem que permitia a transferência de palavras faladas a longas distâncias através do chamado código Morse. O mais interessante é que esse sistema era baseado na comunicação com fios. A base científica e tecnológica para tal invenção, foi lançada por Maxwell, através das suas equações descrevendo a propagação de ondas electromagnéticas e os experimentos de Heinrich Hertz que se tornaram o pilar principal para a descoberta da radiotelegrafia por Marconi já no final do século XIX. Como resultado dessas descobertas todas, temos que já em 1901, o Oceano Atlântico era atravessado por sinais de rádio. Este foi o início dos sistemas de comunicação sem fios. O telefone inventado por Alexander Graham Bell foi um segundo sistema de comunicação evoluiu rapidamente e tornou-se uma tecnologia complementar ao telégrafo durante muitos anos. Como se pode perceber, há nomes e factos que estão associados a este movimento evolutivo todo, por isso, iniciemos nossa caminhada dispensando um pouco da nossa atenção a algumas personalidades que deram o seu saber para que hoje possamos nos comunicar em qualquer lugar e a qualquer hora.

Personalidades	Dados e Factos
 (1777 – 1851)	1820, Hans Christian Oersted descobre experimentalmente que a corrente eléctrica produz um campo magnético. André Marie Ampère (1775 – 1836) quantifica essa observação na Lei de Ampère.

André Marie Ampère (1775 – 1836) quantifica essa observação na Lei de Ampère.

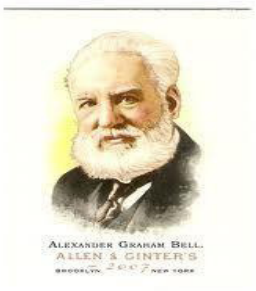
1830, Joseph Henry descobre que a variação do campo magnético induz uma corrente eléctrica mas não publica o resultado. Em 1831, Michael Faraday (1791 – 11867) descobre independentemente esse efeito que passaria a ser conhecido como a Lei de Faraday e, mais tarde, a terceira equação de Maxwell.

(1799 – 1878)

1831, Michael Faraday (1791 – 11867) descobre independentemente esse efeito que passaria a ser conhecido como a Lei de Faraday e, mais tarde, a terceira equação de Maxwell.

1864, James Clark Maxwell modifica a Lei de Ampère, amplia a Lei de Faraday e desenvolve as quatro famosas equações de Maxwell sobre campos magnéticos.

(1831 – 1879)

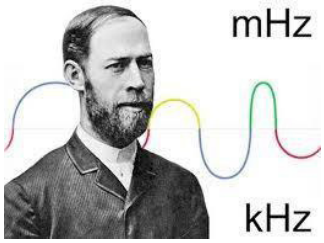


(1847-1922)

Alexender Grahan Bell, Canadiano

- 1876 – transmissão da voz através de sinais eléctricos
- Em 1880, inventou o "photophone"

Alexander Graham BELL, Ph.D., "On the Production and Reproduction of Sound by Light", American Journal of Sciences, Third Series, vol. XX, n°118, Oct. 1880, pp. 305- 324.



(1857-1894)

Heinrich Hertz, Físico alemão

1880 – aproveitando a sugestão de Maxwell, Heinrich Hertz evidencia a propagação de ondas electromagnéticas.

(1874-1937)

Guglielmo Marconi, Físico italiano

· Em 1896, conseguiu a primeira transmissão via rádio

· Em 1901, demonstrou a transmissão de sinais de rádio através do Atlântico

1897 – Marconi fez várias transmissões de rádio de Needles para um navio a 18 milhas da costa.

Pode-se dizer que a primeira aplicação importante das comunicações móveis foi a utilização em navegação.

1905 – Reginald Fesseden realiza experimentos de transmissão em Amplitude Modulada (AM) de voz e música.

1920 – surge a 1ª estação comercial de rádio em Pittsburg (USA)

1921 – O Deptº de Polícia de Detroit faz o 1º uso regular de sistema de rádio móvel em viaturas

1932 – Deptº de Polícia civil de NY usa o mesmo sistema, com 11 canais de voz compartilhadas por até 5000 veículos.

1935 – a Federal Communication Commission autoriza a utilização de 4 canais na faixa de 30MHz e 40MHz

1938 – Regulamentação.

1946 – AT & T coloca em funcionamento um novo sistema operando a 150MHz com 6 canais.

1947 – inaugura-se um sistema de telefonia móvel ao longo da rodovia NY – Boston operando a baixas frequências: 35 – 40MHz

Porém, o que se notou depois foi que essas frequências se propagam a longas distâncias via reflexão na ionosfera, mas que também causam interferências em outros sistemas.

1950 – Deptº de Polícia da Filadélfia implanta o 1º sistema Full-Duplex

1955 – implementa-se a selecção automática de canais vagos pelos equipamentos de rádios móveis.

1960 – surgem os sistemas chamados Trunked que marcam e definem a base dos sistemas de hoje.

1968 – libera-se uma faixa de 75MHz para o serviço de telefonia móvel

Há naturalmente muitos outros factos, dados e muitas outras personalidades que duma ou outra forma estão ligadas ao desenvolvimento das comunicações móveis. Fica como tarefa pesquisares mais nomes e factos ligados a este desenvolvimento.

Tendência actual – universalização baseada na livre concorrência

Mobilidade – factor diferenciador para o utilizador que busca serviços que pode aceder em qualquer parte e a qualquer momento.

- Utilizador desloca-se livremente no espaço
- Utilizador comunica em qualquer momento
- Utilizador comunica com qualquer outro utilizador
- Utilizador acede à rede através de uma ampla gama de terminais

Interoperabilidade dos sistemas de comunicação móvel e a possibilidade de comunicação global que permita a transmissão de voz, dados e aplicações multimídia.

Interoperação com outras redes: suporta comunicação com redes de outros tipos

Requisitos do Sistema

a. Equipamento portátil: terminais de pequena dimensão com baterias de capacidade elevada

b. Grande capacidade de tráfego

c. Técnicas avançadas de autenticação e encriptação

Tipos de redes

1. WPAN - Wireless Personal Area Networks: short distances among a private group of devices

    - É uma rede projectada para curta distância e para baixas taxas de transferências.
    - A tecnologia mais utlizada é Bluetooth
        - HomeRF
        - Zigbee
        - Infravermelho
    - Geralmente mais utilizados para transferência de arquivos.

2. WLAN - Wireless Local Area Networks

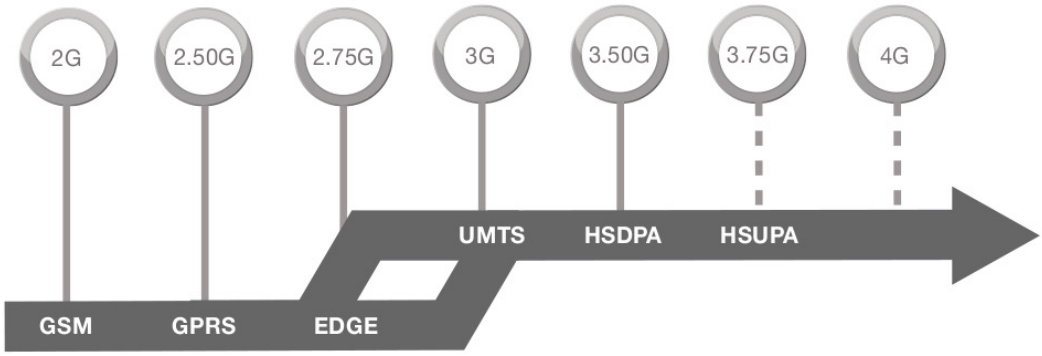
    - Sua principal aplicação é em lugares públicos (universidades, aeroportos,shopping,particulares)
    - O principal problema desse tipo de rede é a frequência, uma vez que operando em 2.4 Ghz (802.11b), pode conduzir a interferência de telefones sem fio

3. WMAN - Wireless Metropolitan Area Networks

    - São redes de uso corporativo que atravessam cidades.
    - Essa conexão é utilizada pelos ISP (Provedor do serviço de Internet) e seus pontos de distribuição.
    - O padrão Wimax (Worldwide Inter-operability for Microwave Access - 802.16) é o mais utilizado
    - O padrão Wi-Max tem como objetivo estabelecer a infra-estrutura final da parte da conexão.

4. WWAN - Wireless Wide Area Networks

    - As redes Wwan são basicamente as tradicionais tecnologias do nosso Telefone Celular de voz e alguns serviços de dados (Wireless Data Services)
    - Alguns dos padrões mais utilizados
        - ***GSM*** (Global System for Mobile Communication)
        - ***GPRS*** (General Packet Radio Service)
        - ***UMTS*** (Universal Mobile Telecommunication System)



Tecnologias WWAN. Fonte: Autor

- High Speed Packet Access – 3.5G
- Universal Mobile Telecommunications System – 3G
- Global System for Mobile Communications
- General Packet Radio Service

Telefonia móvel

- Em 1915 foi efectuada a primeira transmissão de voz transatlântica
- Em 1946, a Bell Telephony Company disponibilizou o primeiro sistema de radiotelefone para uso genérico
- Em 1971 foi introduzido o conceito de rede celular
- Em 1978 entrou em funcionamento a primeira rede celular, em Chicago (USA) – sistema AMPS

Ano	Sistema / Padrão	País
1978 (1984)	AURORA 400 (800)	Canadá
1979	NTT 800	Japão
1981 (1986)	NMT 450 (900)	Escandinávia
1983	AMPS	USA
1985	TACS	Reino Unido
1987	GSM	Europa
1989	TDMA (IS-54 / IS-136)	USA
1993	CDMA (IS – 95)	USA

Redes celulares digitais

- Em 1982, nasce o Groupe Spécial Mobile (GSM)
- Em 1991 o serviço GSM foi lançado no Reino Unido, França, Alemanha e Itália
- Em 2004 deu-se início à exploração das redes de 3ª geração (UMTS)

Redes sem fios

- Em 1971, foi criada, no Hawaii, a ALOHANET, permitindo a troca de dados entre computadores instalados em 4 ilhas do arquipélago
- Em 1996, o grupo de trabalho IEEE 802.11 publicou a primeira norma para redes sem fios - WLANs (usando transmissão por rádio e óptica)
- Em 1999, foi criado o grupo de trabalho IEEE 802.15 com o objectivo de normalizar as redes de área pessoal – PANs, dando seguimento à iniciativa Bluetooth lançada em 1994

Comunicação por satélite

- Em 4 de Outubro de 1957 foi lançado o Sputnik I
- Em 11 de Julho de 1962 foi lançado o Telstar I (AT&T), o primeiro satélite de comunicações

Conclusão

Na actividade de aprendizagem que agora termina, tentamos olhar um pouco a evolução das comunicações móveis. Sem entrarmos em muitos detalhes, também lançamos um olhar sobre as principais tecnologias e padrões que tornam possível este tipo de comunicação. E como nada acontece sem a intervenção do homem, associamos alguns factos importantes deste desenvolvimento com algumas personalidades que deram um grande contributo.

Avaliação

1. Uma das tendências actuais em comunicações móveis é a universalização baseada na livre concorrência, onde o conceito de Mobilidade é chave. Caracterize este conceito.
2. Quais são os padrões mais usados em redes WWAN?
3. Em 1978 entrou em funcionamento a primeira rede celular. Como se chamava esta rede e onde (país) é que foi implementado?
4. Quando é que foi introduzida a telefonia móvel no teu país?

5. Quando é que tu usastes a telefonia móvel pela primeira vez?
6. Caracterize as redes do tipo WPAN.
7. Que entende por conceito de Interoperabilidade em comunicações móveis?
8. Caracterize a tecnologia 3G.

Guião de Correcção

Questão	Sugestão de resposta
Q1	Podemos caracterizar o conceito de mobilidade recorrendo aos seguintes principios: • Utilizador desloca-se livremente no espaço • Utilizador comunica em qualquer momento • Utilizador comunica com qualquer outro utilizador • Utilizador acede à rede através de uma ampla gama de terminais
Q2	Os padrões mais usados em redes WWAN são: • ***GSM*** (Global System for Mobile Communication) • ***GPRS*** (General Packet Radio Service) • ***UMTS*** (Universal Mobile Telecommunication System)
Q3	Em 1978 entrou em funcionamento a primeira rede celular, em Chicago (USA) – sistema AMPS
Q4	Resposta livre
Q5	Resposta livre
Q6	*WPAN - Wireless Personal Area Networks: short distances among a private group of devices* • É uma rede projectada para curta distância e para baixas taxas de transferências. • A tecnologia mais utlizada é Bluetooth • Geralmente mais utilizados para transferência de arquivos.
Q7	Interoperabilidade significa ter a capacidade de Interoperação com outras redes: suporta comunicação com redes de outros tipos.

Q8	3G é apenas um uma sigla que representa a terceira geração (daí o nome 3G) de padrões e tecnologias da telefonia móvel. A tecnologia 3G aprimora a transmissão de dados e voz, oferecendo velocidades maiores de conexão, além de outros recursos, como vídeochamadas, transmissão de sinal de televisão, entre outros serviços.

Actividade 1.2 - Caracterização do canal de comunicação

O que é comunicação móvel ?

Pode-se definir como comunicação móvel aquela onde existe a possibilidade de movimento relativo entre partes ou as partes sistêmicas envolvidas. Como exemplo tem-se a comunicação:

- entre aeronaves,
- entre aeronaves e uma base terrena,
- entre veículos,
- da telefonia celular,
- da computação móvel,
- de algumas classes de sistemas de telemetria, etc..

Uma comunicação fixa (por exemplo um link de micro-ondas entre uma estação rádio base e uma central de comutação e controle de um sistema de telefonia celular) não caracteriza uma comunicação móvel, mas pode fazer parte de um sistema de comunicação móvel.

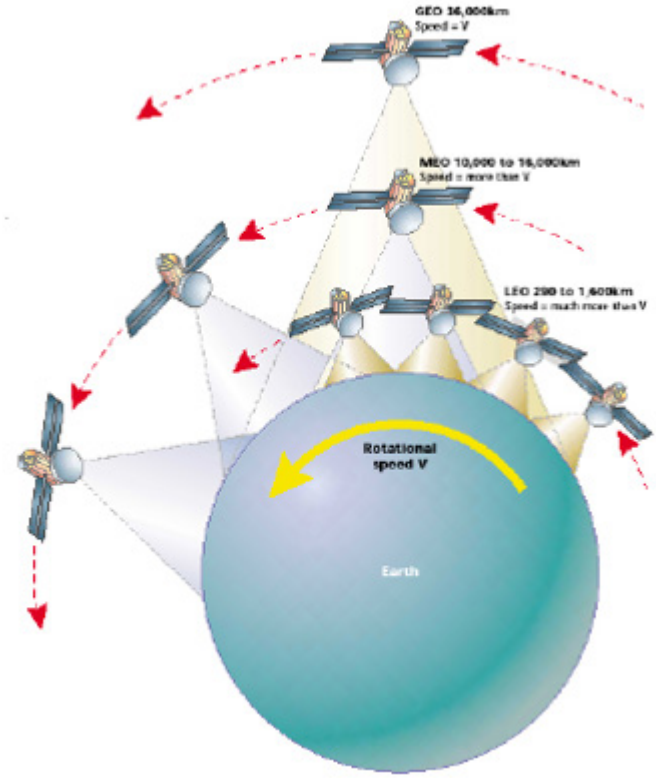
Os canais associados a sistemas de comunicação móvel podem ser agrupados em dois tipos:

- Canal via satélite e o outro canal terrestre.

Sistemas de comunicação móvel via satélite

O canal de comunicação via satélite

- é um canal AWGN (Additive White Gaussian Noise) onde predominam fortes atenuações e muitas vezes grandes atrasos de propagação do sinal.
- Há três categorias nas quais se encaixam
  - Satélites de órbita geossíncrona *(GEO – Geostationary Earth Orbit)*
  - Satélites de órbita média *(MEO - Medium Earth Orbit)*
  - Satélites de órbita baixa *(LEO - Low Earth Orbit)*



Categoria de satélites. Fonte: Wikepedia

Satélites de órbita geossíncrona (GEO – Geostationary Earth Orbit)

- Uma órbita é considerada geossíncrona quando a sua rotação acompanha exactamente a rotação da Terra
- Portanto, tem o mesmo período de revolução da Terra, que é de um dia sideral = 23 h 56 mn 04s.

Satélites de órbita média (MEO - Medium Earth Orbit)

- A órbita média vai de 1 000 a 35 700 km da Terra. Na distância usada pelo GPS - 20 mil km -, os satélites levam cerca de 11 horas para dar uma volta no planeta
- os satélites viajam entre 13000 e 20000 km de altitude

Satélites de órbita baixa (LEO - Low Earth Orbit)

- Aqui os satélites ficam entre 600 e 700 km da Terra e são muito velozes: viajam a 27 400 km/h, dando uma volta no planeta a cada 90 minutos.
- As órbitas podem ser tanto circulares como elípticas, dependendo da necessidade do projecto a ser executado, pois as órbitas elípticas fazem com que o satélite passe mais tempo sobre uma determinada região, facilitando e ampliando o tempo de comunicação entre o satélite e a estação terrestre.

Os serviços oferecidos pelas comunicações móveis via satélite e alguns dos correspondentes sistemas podem ser agrupados nas categorias:

- Serviços de faixa estreita – telefonia e/ou comunicação de dados: Iridium, redes VSAT, Inmarsat Mini-M, ICO, GlobalStar, Odyssey, Aries, Ellipso, Super-GEO.
- Serviços de faixa larga – multimídia: Teledesic, M-Star, Sativod, Spaceway, Astrolink, Cyberstar, KaStar.
- Serviços de mensagem store and forward: Orbcomm, GE Starsys, LEO One, KITComm.
- Serviços de navegação: GPS, Glonass, GNSS-2.

Os sistemas VSAT, Inmarsat, Iridium e GPS são os mais populares.

Aplicações

As aplicações onde a comunicação via satélite são mais indicadas são aquelas em que:

a. Deseja-se espalhar a mesma informação, no link de descida, por uma região geográfica muito extensa como, por exemplo, para a TV e a Internet.

b. Deseja-se atingir localidades remotas como, por exemplo, campos de mineração, madeireiras, propriedades rurais e suburbanas e postos em rodovias.

c. Deseja-se que o tempo de implantação seja muito rápido, ou de uso ocasional, como, por exemplo, para shows, corridas de automóvel, etc.

Canal de comunicação terrestre

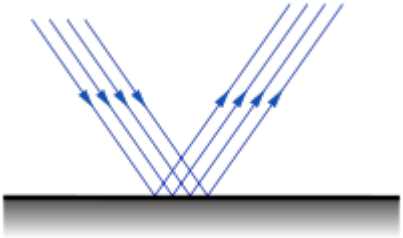
Características principais:

– Propagação por multipercursos e o efeito Doppler

Multipercursos

Pode-se dizer que o multipercurso é originado pelo fenômeno da reflexão, da difração, da refração e do espalhamento do sinal em propagação. Estes fenômenos, quando combinados, acabam por fazer com que o sinal percorra diversos caminhos da origem até o destino, cada qual levando um tempo diferente até atingir o receptor. No receptor, estes sinais são combinados e podem interferir destrutivamente (degradando o nível de sinal no receptor) ou construtivamente (melhorando o nível do sinal) pois, se trata de uma soma vectorial. Os sinais que chegam ao receptor podem ainda estar contando, quando existir, com o sinal de visada directa.

a) Reflexão – ocorre quando a onda rádio incide sobre um objecto de proporções maiores que o comprimento da onda incidente, e que por suas características constituintes, reflecte o sinal em várias direções. Pode haver ou não penetração de parte do sinal incidente, dependendo da constituição da superfície reflectora. Existem dois tipos de reflexão, a especular e a difusa, que possui as características do espalhamento.

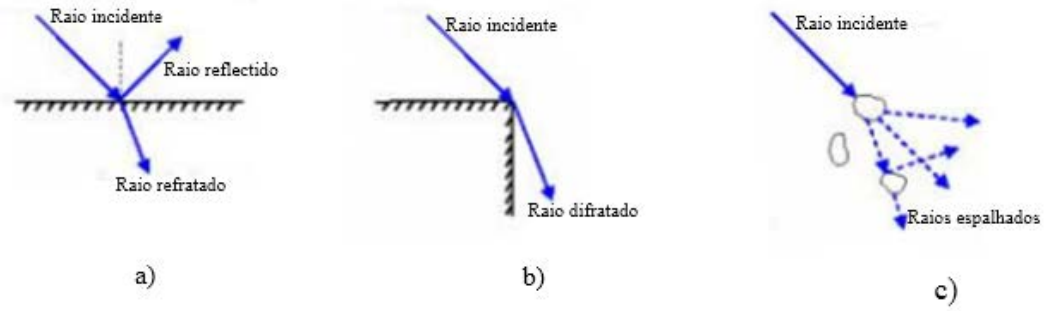


b) Difração – esta ocorre quando uma onda em propagação é obstruída por um objecto em sua extremidade para altas frequências, porém para baixas frequências o sinal é desviado de sua trajectória original atingindo uma região que antes não seria coberta pelo mesmo, ou seja, provavelmente seria uma região de sombra. Este mecanismo de propagação faz uso do princípio de Huygens onde cada ponto de uma frente de onda se comporta como uma fonte pontual irradiando para todas as direções.

c) Refração – este efeito ocorre quando uma onda penetra em um meio cuja densidade é diferente do meio em que se propagava e tem sua trajectória alterada e seu nível de potência reduzido, pois parte do sinal será reflectido. Cada material tem seu coeficiente de reflexão e o de refração.

d) Espalhamento – quando uma onda incide sobre um objecto cujas dimensões são da mesma ordem ou menores que o comprimento de onda do sinal incidente, ocorre a atenuação no sinal e reflexão do mesmo em diversas direções. É por este motivo que as comunicações satélite que utilizam faixas de frequências bastante elevadas, como as bandas Ku e Ka, sofrem com as atenuações provocadas por chuvas e por gases respectivamente, dentre outros males por assim dizer.

Das aulas de física, deve estar recordado dos seguintes fenómenos:



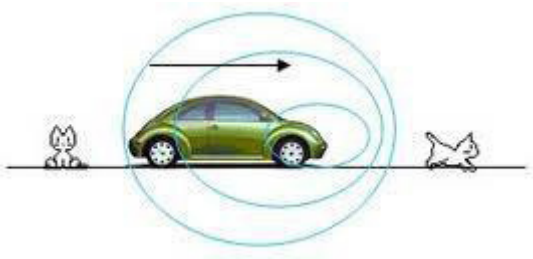
Fenómenos que originam o Multipercurso. Fonte: autor

Portanto,

- O sinal recebido pelo terminal móvel é composto pela soma (vectorial) dos vários sinais oriundos de diferentes caminhos entre o transmissor e o receptor
- Os multipercursos são formados pela reflexão e/ou difração e/ou espalhamento do sinal transmitido em estruturas próximas ao receptor
    - edifícios, árvores, postes, morros, etc.
    - A soma vectorial dos vários sinais dos multipercursos pode resultar em uma interferência construtiva ou destrutiva no sinal recebido.
    - Quanto maior a velocidade de movimentação, mais rápidas serão as variações no sinal recebido
    - Esse fenômeno de alteração na intensidade do sinal recebido é denominado desvanecimento por multipercursos.

Efeito Doppler

- O efeito Doppler é a percepção de uma frequência diferente daquela que está sendo transmitida por uma determinada fonte.
- Esse efeito acontece devido ao movimento relativo entre a fonte e o receptor.
- Quanto maior a velocidade de deslocamento do receptor em relação à direção de propagação da onda de rádio, maior o desvio de frequência percebido.



cuja equação é:

$$fD = \frac{v}{\lambda} cos\theta$$

onde

- fD é o desvio Doppler,
- v é a velocidade do móvel e
- q é o ângulo entre a direcção do movimento e a direcção de propagação da onda electromagnética.

Considerando:

- f0 = frequência aparente percebida pelo observador
- ff = frequência real emitida pela fonte
- v0 = velocidade do observador
- vf = velocidade da fonte
- v = velocidade da onda sonora

Pode-se determinar uma fórmula geral para calcular a frequência percebida pelo observador, ou seja, a frequência aparente f0.

$$\frac{f_0}{v \pm v_0} = \frac{f_f}{v \pm v_f}$$

ou seja,

Supondo que o observador esteja em repouso e a fonte se movimente:

a) A fonte se aproxima do observador

$$f_0 = \left(\frac{v}{v - v_f}\right) \times f_f$$

b) A fonte se afasta do observador

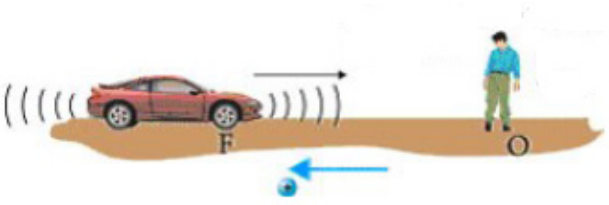
$$f_0 = \left(\frac{v}{v + v_f}\right) \times f_f$$

Exemplo

- Um automóvel, deslocando-se a velocidade de 108 km/h, toca sua buzina, cujo som é uma senóide pura de frequência igual a 1200 Hz. Um homem parado ao lado da estrada percebe uma variação brusca no som, no instante em que o automóvel passa pelo ponto onde se encontra.

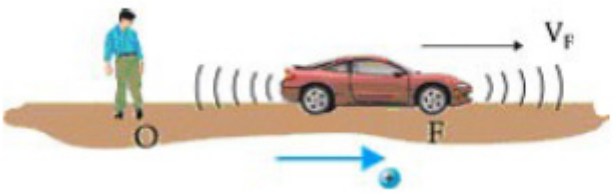
  – *Qual é a variação de frequência percebida pelo homem (observador)?*

a) Antes do cruzamento



$$f_0 = \left(\frac{v}{v - v_f}\right) \times f_f$$

b) Depois do cruzamento



$$f_0 = \left(\frac{v}{v + v_f}\right) \times f_f$$

Resolução

- $v_f = 108$ km/h →
- 108 km/h = 108000 m /3600s → 30 m/s
- $f_f = 1200$ Hz; $v_0 = 0$; $f_0 = ?$
-
- Antes do cruzamento
  - $\frac{f_0}{330} = \frac{1200}{330-30}$
- Depois do cruzamento
  - $\frac{f_0}{330} = \frac{1200}{330+30}$
- $F_r = f0 - f'0$

Conclusão

Na actividade de aprendizagem que agora termina, vimos o que é comunicação móvel na base de alguns exemplos. Caracterizamos o canal de comunicação e ainda discutimos os conceitos de Multipercurso e Efeito de Doppler nas comunicações. Tu podes continuar a ver estes conceitos com alguma profundidade consultado a literatura referenciada.

Avaliação

1. Que entende por comunicações móveis? indique algum exemplo a tua escolha.
2. Diferencie as características básicas das tecnologias 1G, 2G, 2,5G e 3G.
3. Caracterize satélites de orbita geossíncrona.
4. Que tipo de aplicações requerem comunicações via satélite?
5. Quais são as características principais do canal de comunicação via terrestre?
6. Quais as razões que estão por detrás do fenómeno do Multipercurso.
7. Caracterize o chamado efeito de Doppler.
8. Diferencie interferência co-canal e interferência de canal adjacente.

Questão	Sugestão de resposta
Q1	Pode-se definir como comunicação móvel aquela onde existe a possibilidade de movimento relativo entre partes ou as partes sistêmicas envolvidas. Como exemplo tem-se a comunicação da telefonia celular.
Q2	A primeira geração de telefonia móvel era analógica (só transmitia voz) e utilizava a comutação por circuito (canal dedicado). Fazia uso da tecnologia FDMA (Frequency Division Multiple Access), tendo como padrão o AMPS (Advanced Mobile Phone System). No 2G o sinal passa a ser digital, mas a tecnologia de rede ainda é a comutação de circuitos, assim como na Primeira Geração. A primeira tecnologia 2G foi o TDMA, logo em seguida o CDMA, que evoluiu para o GSM. No 2,5G o grande diferencial foi uma técnica avançada de modulação que permitia a comutação por pacotes ao invés de circuitos, a mesma técnica de transmissão adotada pelo IP da arquitetura TCP/IP. Os sistemas 3G provêm serviços de telefonia e comunicação de dados a velocidades maiores que seus antecessores. O padrão 3G especifica, mais exactamente, 144kbps em ambientes móveis, 384kbps em ambientes de pedestres e 2Mbps em ambientes fixos.
Q3	Uma órbita é considerada geossíncrona quando a sua rotação acompanha exactamente a rotação da Terra – Portanto, tem o mesmo período de revolução da Terra, que é de um dia sideral = 23 h 56 mn 04s.
Q4	As aplicações onde a comunicação via satélite são mais indicadas são aquelas em que: a) Deseja-se espalhar a mesma informação, no link de descida, por uma região geográfica muito extensa como, por exemplo, para a TV e a Internet. b) Deseja-se atingir localidades remotas como, por exemplo, campos de mineração, madeireiras, propriedades rurais e suburbanas e postos em rodovias.
Q5	Características principais do canal de comunicação via terrestre são: – Propagação por multipercursos e o efeito Doppler

Q6	O multipercurso é originado pelo fenômeno da reflexão, da difração, da refração e do espalhamento do sinal em propagação. Estes fenômenos, quando combinados, acabam por fazer com que o sinal percorra diversos caminhos da origem até o destino, cada qual levando um tempo diferente até atingir o receptor.
Q7	O efeito Doppler é a percepção de uma frequência diferente daquela que está sendo transmitida por uma determinada fonte. • Esse efeito acontece devido ao movimento relativo entre a fonte e o receptor. Quanto maior a velocidade de deslocamento do receptor em relação à direção de propagação da onda de rádio, maior o desvio de frequência percebido.
Q8	A interferência co canal é aquela que ocorre em consequência do reuso, por parte das células, de um mesmo conjunto de frequências em uma determinada cobertura. Já interferência de canal adjacente é causada por sinais presentes em uma faixa de frequência adjacente a faixa do sinal desejado e provoca imperfeições no filtro do receptor, permitindo que frequências em faixas próximas à faixa requerida sejam recebidas.

Actividade 1.3 - Conceito de comunicação Rádio

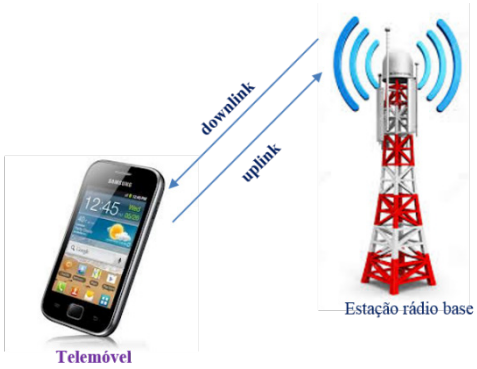
Introdução

O telemóvel é na sua essência um equipamento emissor/receptor porque recebe e emite sinais de rádio. As comunicações de rádio entre um emissor e um receptor podem ser do tipo simplex, half-duplex ou duplex, como foi largamente discutido na disciplina de redes de computadores.

Chama-se CANAL ao conjunto de frequências utilizado para fazer uma transmissão de sinal.

Um canal simplex ou half-duplex necessita apenas de um conjunto de frequências que será comum à emissão e à recepção. Enquanto que um canal duplex obriga a dois conjuntos de frequências, um para emissão, outro para recepção.

À comunicação emissor - receptor chama-se downlink ou ligação descendente e à comunicação receptor - emissor chama-se uplink ou ligação ascendente.



Comunicação Downlink. Fonte: autor

Conceito de plano de frequências

Os sistemas de comunicação móvel usam frequências de rádio para emissão e recepção em duplex.

- Bandas de frequências usadas em MHZ:
- Banda GSM: [890-935 MHz] uplink e [935-960 MHz] downlink
- A banda GSM900 foi posteriormente ampliada entre [880Mhz-890MHz] e [925MHz- 935MHz].

A frequência de uplink é sempre menor que a de downlink, porque as frequências mais baixas se atenuam menos na propagação o que compensa o facto de o telemóvel emitir com potência muito mais baixa do que a estação base à qual vai se ligar.

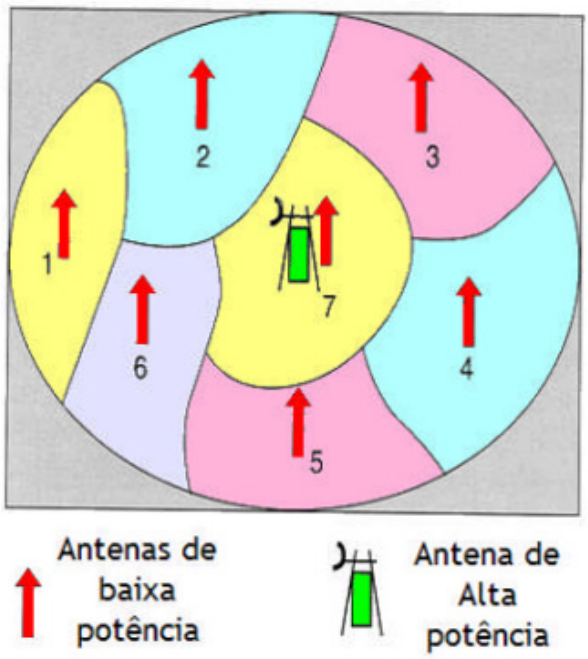
O conceito de célula patenteado em 1972 pelos laboratórios Bell (EUA), foi a chave que veio revolucionar as comunicações móveis.

Em vez de utilizar um emissor de alta potência para cobrir uma área, utilizam-se vários emissores de baixa potência para cobrir a mesma área de modo a que não interfiram entre si.

As antenas não precisam de ser instaladas tão altas e por isso a mesma frequência pode ser reutilizada em distâncias pequenas permitindo maior cobertura para mais assinantes.

A contrapartida destas vantagens é a necessidade de instalar muito mais antenas e equipamentos aumentando o custo das infraestruturas.

Exemplo da diferença do conceito tradicional para o conceito célula.



Alta e Baixa Potência.

A área da figura pode ser coberta por só uma estação rádio de alta potência, como por exemplo 100 canais.

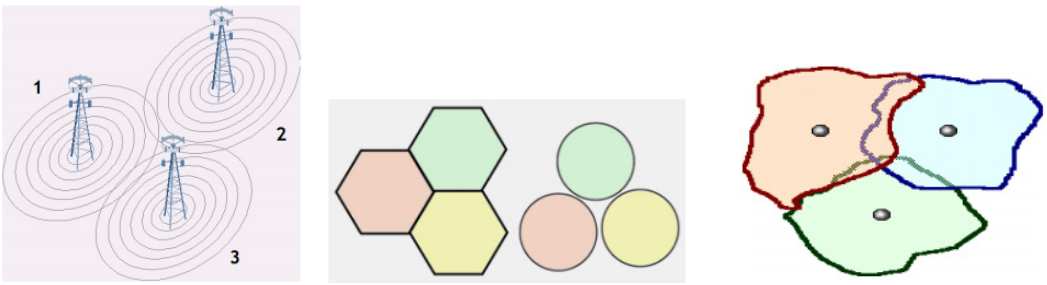
Se utilizarmos estações de menor potência poderemos então atribuir 25 canais para cada uma dessas antenas e repetir os canais atribuídos desde que a distância entre estações seja suficiente para eles não interferirem.

Assim as estações [1 e 7], [2 e 4], [3 e 5] e [6], ao transmitirem 25 canais cada uma totalizarão 175 canais em vez de 100 canais da estação de antena de alta potência.

Este conceito celular permite portanto a reutilização de frequências e o aumento substancial de capacidade de tráfego dentro da mesma área.

Na sua essência cada uma destas células pode ter o formato que se quiser, mas o formato mais intuitivo seria o formato circular porque a antena da célula, se fosse uma antena do tipo isotrópico, transmitiria por igual em todas as direcções.

Contudo, o projecto de redes móveis, fica mais fácil e aproxima-se mais da realidade prática se for utilizada a célula hexagonal.

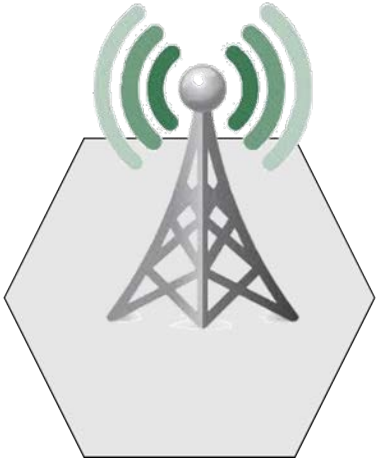


Formatos da célula.

Portanto,

Uma célula representa a área geográfica coberta pelo sinal de rádio emitido pela(s) antena(s) que comunica(m) com os telemóveis.

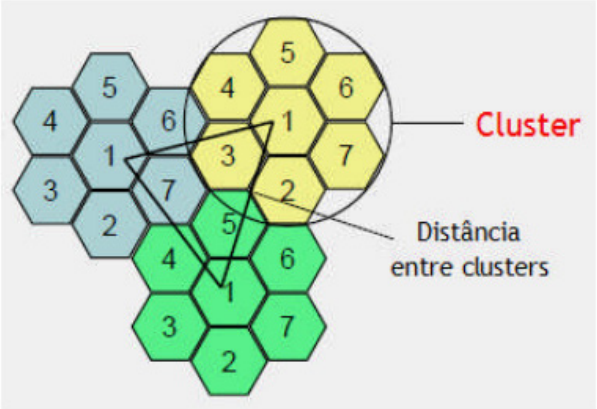
Quando se projecta um sistema celular idealiza-se uma área (célula) totalmente abrangida pelo sinal de rádio que só cobre essa área e não interfere na área (célula) vizinha.



Conceito de célula. Fonte: autor

Conceito de cluster

As células são agrupadas em clusters. Chama-se cluster ao conjunto das células que utiliza todas as frequências disponíveis pelo operador, sem que haja repetição de frequências.

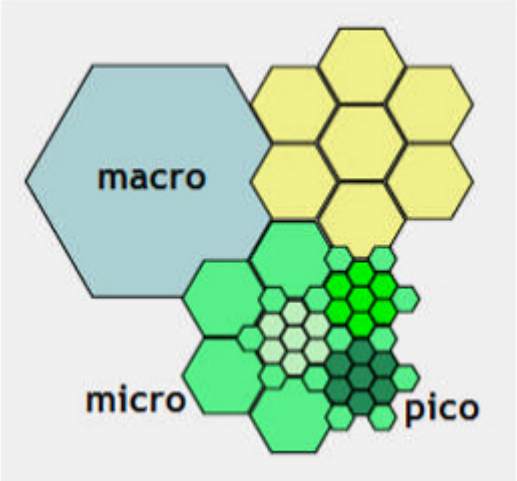


Conceito de Cluster.

Neste exemplo o tamanho do cluster é de 7 células por isso n=7, mas poderia ser de qualquer outro valor. Os valores mais utilizados são 3, 4 e 7.

Ao fazer o projecto de uma rede de comunicações móveis, a distância entre centros de clusters é um dos factores principais a calcular. Ela depende de vários factores, nomeadamente da potência de emissão, do relevo do terreno/obstáculos e do volume de tráfego previsto. Por essa razão o tamanho das células não é predefinido.

As células maiores (também chamadas de macrocélulas) utilizam-se em zonas de pouco tráfego (poucos utilizadores) e dispersos por grande área como acontece nos meios rurais. Podem ter diâmetros de 3 a 35Km embora na prática raramente excedam 10km. Nos meios mais densamente povoados são habituais as microcélulas cobrindo áreas de ruas ou quarteirões (300m a 3 Km).



Conceitos de Macro-, Micro- e Pico-célula.

Em grandes edifícios como centros comerciais ou em casos como o metropolitano utilizam-se picocélulas (30m a 300m) uma vez que as próprias paredes internas dos edifícios limitam o alcance da transmissão e a interferência entre células vizinhas, que assim podem ficar muito juntas.

Excepcionalmente podem utilizar-se nanocelulas (3m-30m).

Sectores

Frequentemente, as células são divididas em sectores o que as torna mais eficientes pois permite maior reutilização de frequências ou seja maior número de chamadas em simultâneo.

As antenas transmitem para dentro da célula e nas células divididas em sectores cobrem apenas uma parte da célula não a célula inteira. Tudo depende da localização da antena em relação à célula. As antenas podem estar localizadas no meio de 3 células (3 sectores), no meio de duas células (2 sectores) ou no centro da célula.

Factor de Reuso

A reutilização de frequências é feita dividindo-se todo o espectro disponível em grupos de frequências. Estes grupos são utilizados em células separadas entre si o suficiente para não haver interferência.

As células que contêm o mesmo grupo de frequências são denominadas co-células. Define-se Factor de Reuso (N) como sendo o número de células adjacentes que utilizam o espectro original, ou seja, o número de grupos de frequências. Quanto menor o factor de reutilização, maior o número de canais por grupo, portanto mais canais por célula e maior volume de tráfego oferecido por cada célula.

Podemos obter o factor de reuso N, dividindo a área total do cluster pela área de uma célula. É possível obter uma relação entre D (distância entre co-células), R (o raio maior do hexágono) e o factor de reuso N.

$$\frac{D}{R} = \sqrt{3N}$$

Á medida que aumentamos o factor de reuso N, ou seja, o número de células por cluster, estaremos diminuindo o número de canais por célula, diminuindo o volume de tráfego por célula. Considerando a diminuição do factor de reutilização, estaremos aumentando o tráfego nas células para um maior número de canais. O oposto é a diminuição da relação D/R implicando uma menor qualidade do sinal recebido.

Interferência Co-canal

A interferência co-canal é aquela que ocorre em consequência do reuso, por parte das células, de um mesmo conjunto de frequências em uma determinada cobertura.

Conclusão

O conceito celular tal como discutido, tem grandes vantagens que podem ser resumidas nos seguintes pontos:

- Permite reduzir a potência de transmissão.
- Permite descentralizar toda a informação.
- Os problemas de cada célula são tratados dentro dela própria.
- Permite um maior número de utilizadores por possibilidade de reutilização de frequências.

Avaliação

1. Qual a diferença entre comunicação half-duplex e duplex?
2. Qual a diferença entre macro-celula e micro-celula?
3. Quais as bandas de frequência utilizadas nas comunicações móveis no teu país?
4. O que é um cluster?
5. O que entende por célula no contexto de comunicações móveis?
6. O que é o Roaming?
7. O que é a BTS (Base Transceiver Station) e qual a sua função?
8. O que é Interferência co-canal?

Questão	Sugestão de resposta
Q1	Half-Duplex é quando existem dois interlocutores, mas não é possível transmitir e receber simultâneamente. enquanto um transmite o outro recebe e vice-versa. Full-Duplex é quando é possível transmitir e receber simultâneamente. Half-Duplex: comunicação walk-talk, são dois rádios porém apenas um rádio transmite por vez, ou seja, um fala e o outro escuta. Full-Duplex: telefone celular , ambos podem falar e ouvir ao mesmo tempo e até discutirem.
Q2	Macrocélulas utilizam-se em zonas de pouco tráfego (poucos utilizadores) e dispersos por grande área como acontece nos meios rurais. Podem ter diâmetros de 3 a 35 Km embora na prática raramente excedam 10km. Microcélulas são células usadas nos meios mais densamente povoados cobrindo áreas de ruas ou quarteirões (300m a 3 Km).
Q3	Resposta livre.
Q4	Chama-se cluster ao conjunto das células que utiliza todas as frequências disponíveis pelo operador, sem que haja repetição de frequências
Q5	Uma célula representa a área geográfica coberta pelo sinal de rádio emitido pela(s) antena(s) que comunica(m) com os telemóveis.

Q6	Roaming ou itinerância é um termo empregado em telefonia móvel mas também aplicável a outras tecnologias de rede sem fio. Designa a capacidade de um usuário de uma rede para obter conectividade em áreas fora da localidade geográfica onde está registado.
Q7	A função da BTS é prover a conexão de rádio para a estação móvel (celular). É composta basicamente de rádios transmissores e receptores TRX, Processador de Sinal, Equipamentos de Controle, Antenas eFeeder Cables. Pode-se dizer que uma BTS é uma célula dentro da estrutura geográfica da rede.
Q8	A interferência co-canal é aquela que ocorre em consequência do reuso, por parte das células, de um mesmo conjunto de frequências em uma determinada cobertura.

Resumo da Unidade

Caro estudante,

Na unidade que agora termina, confrontamo-nos com conceitos básicos das comunicações móveis e sem fios. Começamos por olhar historicamente e de forma evolutiva o surgimento das comunicações móveis, para o efeito resgatamos algumas das personalidades mais eminentes neste percurso. Discutimos as tendências actuais, onde destacamos factores como mobilidade e interoperabilidade dos sistemas. Na segunda actividade de aprendizagem, confrontamo-nos com o conceito de canal de comunicação e na última actividade discutimos o conceito de comunicação rádio. Caso algum destes conceitos não tenha ficado claro, tu tens oportunidade de voltares a trabalhar calmamente esta unidade e de consultar outros materiais indicados.

Leituras e outros Recursos

As leituras e outros recursos desta unidade encontram-se na lista de Leituras e Outros Recursos do curso.

Unidade 2. Computação Móvel e Redes sem fios

Introdução à Unidade

Caro estudante,

Dos anos 90 para cá, podemos notar um grande crescimento no desenvolvimento de tecnologias para comunicação celular móvel, comunicação via satélite e redes locais sem fio. A popularização dessas tecnologias tem permitido o acesso a informações remotas onde quer que se esteja, abrindo um leque muito grande de facilidades, aplicações e serviços para os usuários. Nota-se também, uma grande evolução e popularização de dispositivos computacionais móveis. Esse ambiente propicia a criação do conceito de computação móvel e redes sem fio.

Computação móvel pode ser representada como um novo paradigma computacional que permite que usuários desse ambiente tenham acesso a serviços independentemente de sua localização, podendo inclusive, estar em movimento. Mais tecnicamente, é um conceito que envolve processamento, mobilidade e comunicação sem fio. A ideia é ter acesso à informação em qualquer lugar e a qualquer momento. Na unidade que agora começa vamos aprofundar um pouco mais os conceitos que discutimos na unidade 1. Vamos olhar um pouco mais para as redes de comunicação sem fio e voltando a discussão da unidade anterior vamos discutir as técnicas de acesso múltiplo. Esta vai ser uma unidade um pouco mais extensa do que o habitual, mas também estão lhe reservadas 40 horas de actividade. Aplique-se ao fundo nesta aprendizagem e aí poderá de facto obter conhecimentos muito úteis para a tua profissão futura como especialista de IT.

Boa aprendizagem

Objetivos da Unidade

Esta unidade tem como objectivos apresentar os fundamentos da computação móvel e sem fios e as diferentes tecnologias e arquitecturas que lhe dão suporte. Além disso, propõem introduzir os principais conceitos relacionados ao uso de dispositivos móveis, tais como plataformas, mecanismos de adaptação, problemas relacionados à tecnologia, suas vantagens e desvantagens, aplicações e casos de uso.

Após a conclusão desta unidade, deverá ser capaz de:

1. Caracterizar os diferentes componentes de uma rede sem fios
2. Caracterizar a arquitectura do padrão 802.11.
3. Implantar uma rede sem fios extendida (ESS)

Termos-chave

Rede sem fios: Uma rede sem fio é uma infraestrutura de comunicações sem fio que permite a transmissão de dados e informações sem a necessidade do uso de cabos – sejam eles telefónicos, coaxiais ou ópticos.

Computação móvel: é uma área dedicada ao estudo de sistemas computacionais em que existe total mobilidade do usuário.

Conjunto Básico de Serviço (BSS): Representa um grupo de estações comunicando-se por radiodifusão ou infravermelho em uma BSA.

Ponto de acesso (AP): São estações especiais responsáveis pela captura das transmissões realizadas pelas estações de sua BSA, destinadas a estações localizadas em outras BSAs, retransmitindo-as, usando um sistema de distribuição.

Sistema de distribuição : Representa uma infra-estrutura de comunicação que interliga múltiplas BSAs para permitir a construção de redes cobrindo áreas maiores que uma célula.

Conjunto de Serviço Extendido (ESS): Representa um conjunto de estações formado pela união de vários BSSs conectados por um sistema de distribuição.

Actividades de Aprendizagem

Actividade 2.1 - Computação Móvel

O que é a computação móvel?

- Computação Móvel é uma área dedicada ao estudo de sistemas computacionais em que existe total mobilidade do usuário.
- Mobilidade é o ponto essencial, e nos coloca uma série de possibilidades e desafios que são particulares à Computação Móvel.

A computação Móvel consiste em sistemas computacionais distribuídos em diferentes dispositivos que se comunicam entre si através de uma rede de comunicação sem fios, o que permite a mobilidade desses dispositivos.

Existem três elementos que caracterizam e compõem a Computação Móvel!

1. O tipo e capacidade de Processamento do dispositivo portátil
2. A Mobilidade do usuário e da unidade móvel
3. A comunicação com outros elementos computacionais através de um canal de comunicação sem fios.

Tecnicamente, a computação móvel pode-se caracterizar através da seguinte equação:

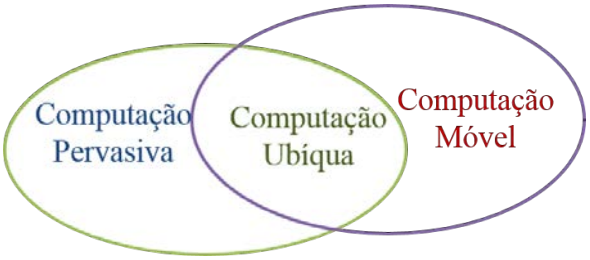
Computação Móvel = Processamento + Mobilidade + Comunicação sem Fio

Por quê computação móvel?

- Comodidade: liberdade para obter e manipular informação relevante a qualquer hora.
- Necessidade: para certos problemas, a mobilidade é essencial.
- "Because we can?" - Infraestrutura finalmente disponível.

Para quê?

- Novas formas de trabalhar.
- Novos estilos de vida.
- Complementar outros paradigmas (Ubiquitous, pervasive computing).



- Omnipresença da informática no dia-a-dia das pessoas.
- Proposta de inserir chips em todos os objectos à nossa volta tornando-os inteligentes, das maçanetas de todas às portas ao fogão e à geleira.

Desafios da Computação Móvel

Comunicação sem fio

- Prover conexão wireless contínua à rede (através de Bluetooth, IEEE 802.11, telefonia celular, ou outras formas);
- Manter o serviço funcionando com os dispositivos em movimento.
- Fazer os computadores e interfaces pequenos;
- Prover e gerenciar energia eléctrica;
- Criar interfaces que se adaptem ao tamanho do dispositivo e continuem sendo amigáveis;
- Inventar novos dispositivos de interface para computadores móveis.

Mobilidade

- Migração de endereço.
- Informação dependente de local.
- Migração de localidade.

Portabilidade

- Baixo consumo de energia.
- Integridade dos dados.
- Pequeno espaço de armazenamento
- Interface HC reduzida

Tipos de redes

- Bluetooth
- 802.11
- 3G
- I-Mode
- CDMA/TDMA/GSM

Resumindo

- Computação móvel:
  - É uma área em franca expansão.
  - Atenção científica recente.
  - Interface extremamente importante; projecto pode determinar sucesso ou fracasso do produto.
  - Computação expande para outros domínios até então inexplorados.
  - Terceira geração de comunicações móveis (3G), que combina as tecnologias móveis sem fios com uma grande capacidade de transmissão de dados

Conclusão

Como deve ter percebido, a computação Móvel consiste em sistemas computacionais distribuídos em diferentes dispositivos que comunicam-se entre sí através de uma rede de comunicação sem fios, o que permite a mobilidade desses dispositivos.

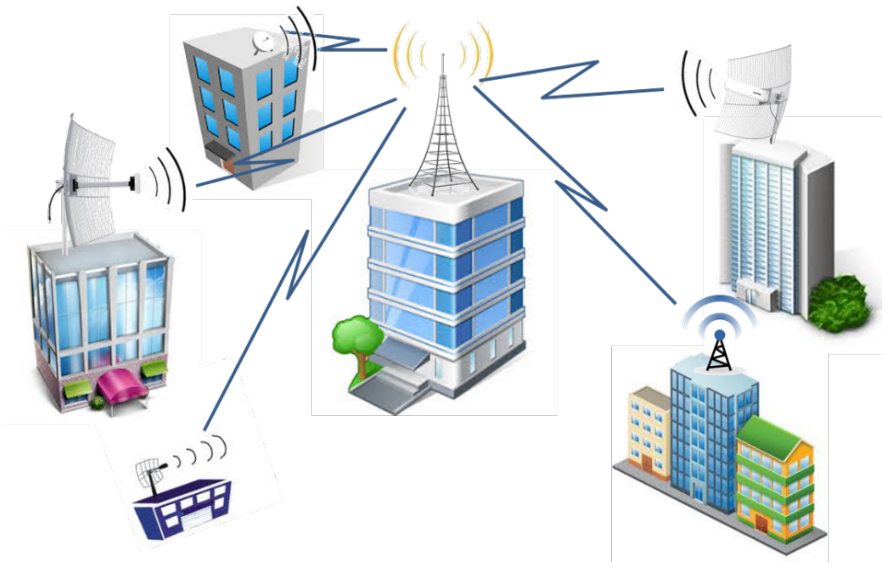
Avaliação

Questões	**Respostas possíveis**
Q1	Fale da computação móvel.
Q2	Mobilidade é um dos factores diferenciais da computação móvel. Que desafios se colocam à computação móvel hoje relativamente a este conceito?
Q3	Quais são os benefícios da computação móvel para os individuos? Para ti, por exemplo.
Q4	Qual é a relação entre a computação móvel e a computação ubíqua.
Q5	Que tipo de redes suportam a computação móvel?
Q6	Portabilidade é um dos desafios da computação móvel. Que factores é que ainda urge resolver a este respeito?
Q7	Nos dias de hoje é comum ouvir-se falar de computação vestível (wearable computing). Qual é o seu entendimento sobre isso? Dê alguns exemplos desta nova tecnologia.
Q8	Que tecnologias de comunicação suportam a computação móvel?

Actividade 2.2 - Redes de Comunicação sem Fios

Introdução

Os avanços nas comunicações nos últimos anos possibilitaram o surgimento de várias tecnologias, que desde então procuram atender a real necessidade de seus usuários, com a melhor qualidade possível. Nos últimos anos a comunicação sem fio ganhou um espaço considerável nas tecnologias de transmissão de dados, deixando de existir apenas nas comunicações de longa distância (feitas através de satélite), para fazer parte de ambientes locais.



Há uma tendência moderna de se implantar cada vez mais as redes sem fio ao invés de redes com fios.

– Qual é a motivação para isso? vamos pensar juntos!

- Inviabilidade da instalação de redes com fio em alguns lugares.
- Interoperabilidade oferecida pela tecnologia Wireless
- Barateamento dos equipamentos sem fio
- Facilidades de mobilidade e flexibilidade que as comunicações sem fio oferecem.

Que é uma rede de comunicação sem fios?

Uma rede sem fio (Wireless) é uma extensão de uma rede local (LAN) convencional com fio, criando-se o conceito de rede local sem fio (Wireless Local Area Network - WLAN).

"Uma rede sem fio é um sistema que interliga vários equipamentos fixos ou móveis utilizando o ar como meio de transmissão" [IEEE 802.11a].

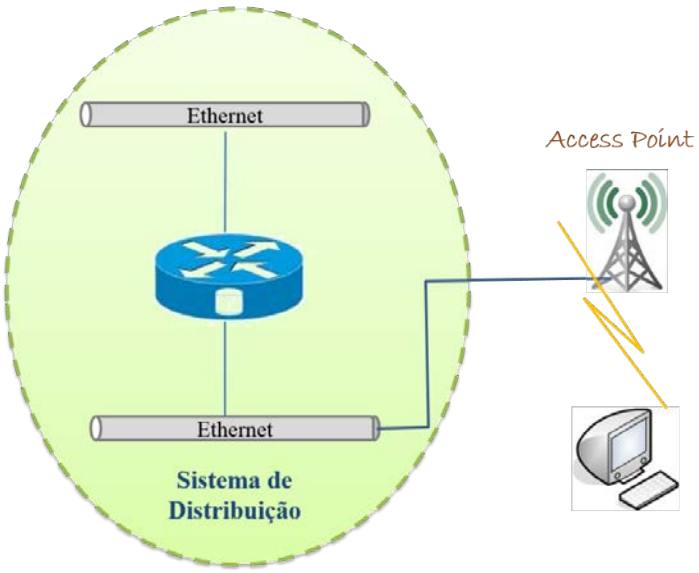
Uma WLAN é, de forma geral, formada por um ou mais pontos de acesso, que estabelecem a comunicação sem fios entre os dispositivos em rede e o sistema de distribuição, que dá acesso aos serviços e às aplicações da rede.

As comunicações WLAN estão definidas no standard 802.11 e baseiam-se na utilização de ondas rádio. Quer dizer, uma WLAN converte pacotes de dados em ondas rádio ou infravermelho e envia-os para outros dispositivos sem fio ou para um AP (Ponto de Acesso) que serve como uma conexão para uma LAN com fio.

O padrão IEEE 802.11 define uma arquitectura para as WLANs que abrange os níveis físico e de enlace (conceitos já discutidos nos modelos OSI e TCP/IP).

No nível físico são tratadas apenas as transmissões com frequência de rádio (RF) e infravermelho (IR), embora outras formas de transmissão sem fio possam ser usadas, como micro-ondas e laser.

No nível de enlace, o IEEE definiu um protocolo de controle de acesso ao meio (protocolo MAC)



Esquema duma WLAN. Fonte: autor

Sistema de distribuição

- Permite interligar vários pontos de acesso entre si à rede principal onde se encontram os servers de serviços e de aplicações.

Pontos de Acesso

- São equipamentos que fazem a ponte entre as comunicações sem fios e o sistema de distribuição.
- O nº de Access Points (AP) depende das necessidades de comunicação e da arquitectura da rede.

Como funcionam as WLAN?

Alguns conceitos importantes:

Espectro Electromagnético

- Quando os eléctrons se movimentam, são geradas ondas electromagnéticas que se propagam no ar. Essas ondas têm três características básicas, são elas: Amplitude, Frequência e Fase.

Amplitude.

– É a medida da altura da onda, voltagem positiva ou negativa, também definida como altura da crista da onda.

Frequência

– Número de cristas ou ciclos por segundo, medido em Hz, 1 ciclo corresponde a 1 Hz.

Fase

É o angulo de inflexão da onda em um ponto específico no tempo, medida em graus.

Como acontece uma comunicação sem fio ?

Em um circuito eléctrico, após se instalar uma antena de tamanho apropriado, as ondas electromagnéticas podem ser transmitidas e recebidas a uma distância bastante razoável por um receptor. Sabendo-se a frequência e o comprimento de onda das ondas electromagnéticas, pode-se definir varias zonas, existido a possibilidade das zonas se sobreporem.

Características das zonas de espectro utilizadas na transmissão de dados

O Rádio, a Micro-onda e o Infra-vermelho podem ser utilizados para transmitirem informações. Para isso basta que se possa modular a frequência, a amplitude ou a fase das ondas. A luz ultra-violeta, o raio X e o raio gama, possuem frequências mais altas, mas que não podem ser utilizados devido a dificuldade de se produzir e modular.

Ondas de Rádio

São produzidas frequentemente por circuitos electrónicos e podem percorrer longas distâncias e facilmente podem entrar em prédios, são utilizadas na comunicação, tanto em ambientes abertos e fechados de uma forma bem ampla.

Características de transmissão de dados via Rádio

Ondas Rádio

- Usadas normalmente nas faixas UHF e VHF para que, com maior velocidade possa diminuir a interferência .
- As ondas são omnidirecionais, ou seja as ondas percorrem todas as direções
- O emissor e o receptor não estão necessariamente alinhados.
- Devido as ondas de rádio percorrem longas distâncias, existe a possibilidade de ocorrer interferências entre os usuários
- O regulador nacional exerce um rígido controle sobre os transmissores de rádio.

Infravermelho

- É subdividido em três regiões:
  - IR próximo (780 – 2500nm)
  - IR Intermediário (2500 - 5000nm)
  - IR longínquo (50000nm – 1mm)

- Principais características da transmissão de dados por infravermelho:
  - Ondas infravermelhas não atravessam objectos sólidos
- Assumem comportamento parecido com o da luz, quando se desloca do rádio de onda longa e vai em direção à luz visível, perdendo as características de rádio.
- Um sistema infravermelho num ambiente fechado, não interfere em outro, instalado em numa sala ao lado, por esse motivo não precisa de autorização do regulaor para operar.
- Em ambientes abertos a comunicação infravermelha é inviável devido o sol enviar radiação infravermelha.

Micro-ondas

- As micro-ondas tem como fonte de radiação os circuitos electrónicos.
- Principais características da transmissão de dados por micro-ondas:
  - As frequências de rádio das micro-ondas são altas, e tem o comportamento de ondas de luz, por esse motivo seguem em linha recta.
  - Precisam de antenas para realizarem a transmissão, recepção e modulação da rádio frequência sendo que essas antenas deverão estar numa distância entre 5 a 80 Km.
  - Vantagem em relação ao uso de cabos, a construção de duas torres é mais barata que a colocação de cabos para interligar grandes distâncias e é de manutenção mais prática também.

Modulação

- A Frequência, Amplitude ou Fase pode ser variada, criando assim combinações, dentro de limites autorizados.
- Modulação é o nome desse processo de variação de um desses atributos.
- As modulações mais conhecidas são:
  - Modulação por Amplitude (AM) e
  - Modulação por Frequência (FM).
- A Modulação por Amplitude usa o sistema de chaveamento de amplitude ASK (Amplitude Shift Keying) e
- A Modulação por Frequência usa o sistema de chaveamento de frequência FSK (Frequency Shift Keying).

Multiplexação

- A forma de se agregar várias informações para que a transmissão seja acelerada, se chama multiplexação.
  - A FDM (Frequency Division Multiplexing) e
  - A TDM (Time Division Multiplexing)
- São as técnicas de multiplexação sem fio que se destacam.
- Elas dividem a largura de banda em canais menores que serão disponibilizados aos usuários.

Como funciona a comunicação?

- Através da utilização de portadoras de rádio ou infravermelho, as Redes Wireless estabelecem a comunicação de dados entre os pontos da rede
- Os dados são modulados na portadora de rádio e transmitidos através de ondas electromagnéticas.Múltiplas portadoras de rádio podem coexistir num mesmo meio, sem que uma interfira na outra.
- Para extrair os dados, o receptor sintoniza numa frequência específica e rejeita as outras portadoras de frequências diferentes.
- Para extrair os dados, o receptor sintoniza numa frequência específica e rejeita as outras portadoras de frequências diferentes.
- O dispositivo transceptor (transmissor/receptor) ou ponto de acesso (access point) é conectado a uma rede local Ethernet convencional (com fio).

Arquitectura do Padrão IEEE 802.11

Tal como foi dito antes, as rede de comunicação sem fios estão definidas no Padrão IEEE 802.11.

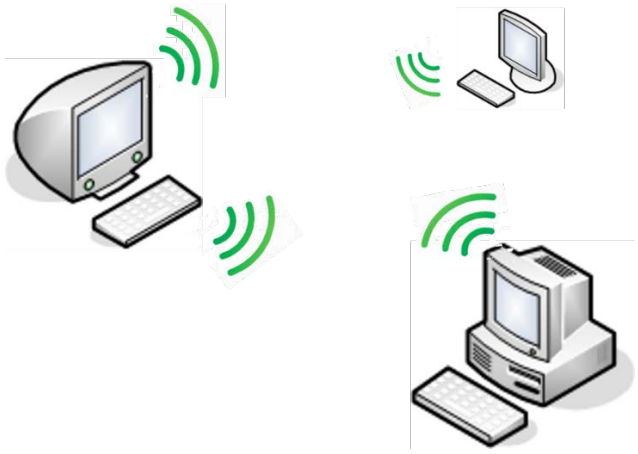
- O padrão IEEE 802.11 define uma arquitetura para as redes sem fio, baseada na divisão da área coberta pela rede em células.
- Essas células são denominadas de BSA (Basic Service Area)
- O tamanho da BSA (célula) depende das características do ambiente e da potência dos transmissores/receptores usados nas estações.
- O padrão IEEE 802.11 define a padronização relativa às camadas físicas (PHY) e a de controle de acesso ao meio (MAC) para redes sem fio.
- Uma rede baseada nesse padrão é composta pelos seguintes componentes:
  - BSS (Basic Service Set) - corresponde a uma célula de comunicação wireless.
  - STA (Stations) - estações de trabalho que comunicam-se entre si dentro da BSS.
  - AP (Access Point) – responsável por coordenar a comunicação entre as STA dentro da BSS.
  - ESS (Estended Service Set) – são células BSS próximas que se interceptam e que os AP estão ligados a uma mesma rede tradicional.

Um STA pode se deslocar de um BSS para outro, mantendo a conexão com a rede - Roaming.

Podem operar de dois modos diferentes:

- Infrastructure mode (Redes de Infra-Estrutura) e
- Ad-Hoc mode (IBSS – Independente BSS)

Arquitectura IBSS (Ad hoc)



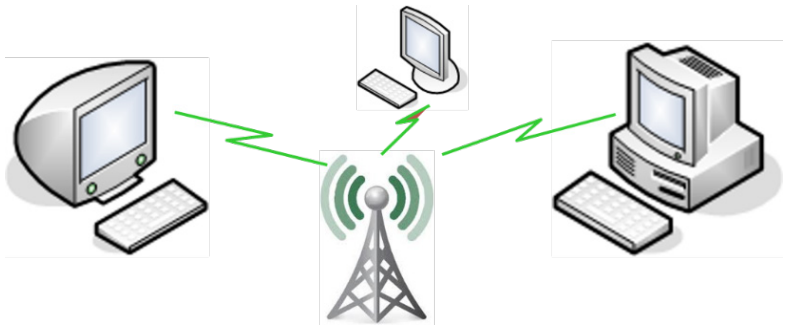
Rede Ad-Hoc. Fonte: autor

Neste modo os dispositivos da BSS comunicam directamente entre si sem usar um ponto de acesso. «WLAN IBSS»

- Não depende de infra-estrutura fixa
- permite que cada nó se comunique directamente com outro nó
- A topologia da rede muda frequentemente já que a conectividade dos nós muda constantemente.

Exemplo: PANs e redes de sensores

Infra-estrutura BSS



Modo Infraestrutura (BSS). Fonte: autor

Neste modo, os dispositivos comunicam através de um ponto de acesso que , por sua vez, garante o acesso ao sistema de distribuição. «WLAN BSS»

- Baseada em infra-estrutura fixa
- Não existe comunicação directa entre os nós
- Toda a comunicação é feita através de estações intermediárias entre os dispositivos e a rede fixa.

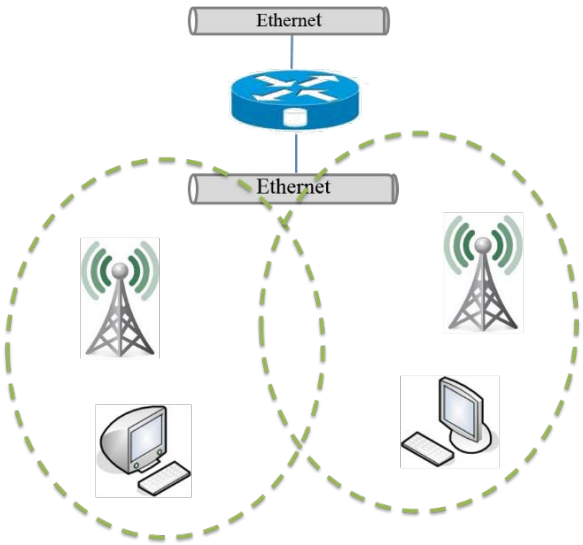
Rede de Bridging

Rede de Bridging. Fonte: Adaptação do autor.

Uma rede sem fios, também pode ser usada para interligar redes com fios. Por exemplo, uma organização que tenha dois edifícios próximos.

Arquitectura ESS

- O alcance de uma rede BSS é determinado pelo alcance do ponto de acesso.
- No caso de querer criar redes sem fios de maior dimensão é necessário juntar várias BSS dando origem às designadas arquitecturas ESS (Extended Service Set).
- A ESS usa mais do que um AP para cobrir uma área WLAN maior.



União de duas BSSs formando uma ESS. Fonte: autor

Redes Mesh

Combinam infra-estrutura com elementos ad hoc. Esta rede pode interligar vários pontos de acesso Wi-Fi (também chamados nós) e formar uma mesh o malha de conexões que proporcionam uma ampla cobertura.

- Uma rede mesh é composta de vários nós/roteadores, que passam a se comportar como uma única e grande rede, possibilitando que o cliente se conecte em qualquer um destes nós.
- Os nós têm a função de repetidores e cada nó está conectado a um ou mais dos outros nós.
- Redes do tipo mesh possuem a vantagem de serem redes de baixo custo, fácil implantação e bastante tolerantes a falhas.
- Uma característica importante das redes mesh é o roaming, também conhecido como "fast handoff"

Numa rede Mesh, alguns APs estão ligados à rede com fios, enquanto outros são usados para comutação das tramas ao longo da rede o que origina dois tipos de Aps:

a) RAP (Root Access Point)

- São Aps que estão ao sistema de distribuição com uma rede com fios.
- Estabelecem a ponte entre a rede sem fios e a rede com fios

b) MAP (Mesh Access Point

- São APs no interior de uma rede sem fios que não tem acesso à rede com fios

802.11 – Camada de Acesso / Enlace

A camada de enlace é divida em duas subcamadas:

a) Controle Lógico do Link (LLC – Logical Link Control);

b) Controle de Acesso ao Meio (MAC – Media Access Control).

A subcamada LLC é idêntica à da especificação IEEE 802.2. Esta subcamada dá suporte à subcamada MAC para serviços de endereçamento, reconhecimento de quadros e detecção de erros.

Controle de Acesso ao Meio – MAC

Esta subcamada está localizada imediatamente acima da camada física, tendo como principal função a alocação do meio físico para cada estação, de forma que a transmissão não sofra interferência das outras estações que também disputam o meio. Outras funções da subcamada MAC: prover garantia de acesso justo e atribuição de prioridades. O meio sem fio apresenta diversas características peculiares que o difere bastante dos meios confinados mais conhecidos (par trançado, cabo coaxial e fibra óptica). Estas características devem ser analisadas para um bom funcionamento da tecnologia e o protocolo da camada de enlace deve ser robusto o suficiente para lidar com todos os novos problemas.

O meio sem fios é um meio partilhado e, como tal, podem ocorrer colisões nas transmissões.

- Uma colisão acontece sempre que dois ou mais dispositivos transmitem ao mesmo tempo com gamas de frequências sobrepostas
- O receptor que recebe o sinal resultante de uma colisão não consegue identificar a mensagem original
- Um dispositivo não pode transmitir e receber ao mesmo tempo, porque usa a mesma frequência na transmissão e na recepção
- Logo, é obrigado a funcionar em modo Half-duplex!
- Ao funcionar assim, não consegue determinar se ocorreu uma colisão!

O funcionamento em half-duplex das comunicações sem fios determina uma diferença para as comunicações com fios

- Nas comunicações com fios é possível o modo full-duplex
- Logo, nas comunicações com fios é possível a detecção de colisões
- Nas comunicações sem fios não é possível detectar colisões!
- Por isso, não se pode recorrer ao mesmo protocolo usado nas redes Ethernet, que se baseia na detecção de colisões, o CSMA/CD.

No Wireless o melhor que se pode fazer é reduzir a probabilidade de ocorrência de colisões! Para isso foi proposto o protocolo CSMA/CA.

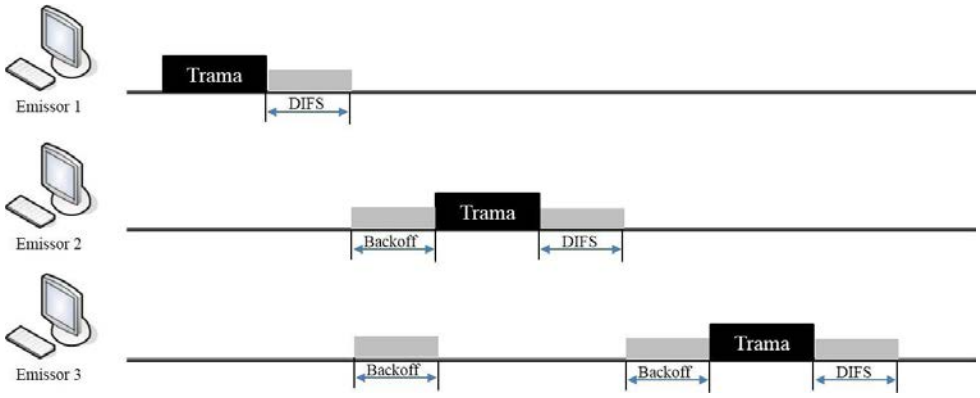
CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance

Uma vez que não é possível detectar colisões, o CSMA/CA determina que todos os pacotes enviados têm de ser confirmados (Acknowledge) de modo que o emissor saiba se a trama foi recebida com sucesso ou não.

Qual é o mecanismo usado para evitar colisões?

- O mecanismo adoptado consiste em escutar o meio antes de iniciar uma comunicação;
- Um dispositivo só pode iniciar uma transmissão se ninguém estiver a transmitir;
- Caso contrário, deverá esperar que a trama seja transmitida antes de iniciar o envio da sua.

No 802.11, um dispositivo deverá esperar um período de tempo chamado DIFS (DCF Interframe Space) após detectar que o meio está livre. Depois deste tempo, ele aguarda durante um período de tempo aleatório (janela de backoff) antes de iniciar a comunicação.



Tempos de espera antes de iniciar a comunicação. Fonte: Adaptação do autor

O Período de espera após o meio ficar livre (DIFS) não é sempre o mesmo. O 802.11 define quatro intervalos de tempo S

SIFS (short interframe space)

É o intervalo de tempo mais curto e é usado nas transmissões de pacotes de maior prioridade.

Por exemplo, a trama ACK usa o tempo SIFS

PIFS (PCF interframe space)

É usado pela função PCF como forma de iniciar uma transmissão antes de outros dispositivos com tramas-base para transmitir.

DIFS (DCF interframe space)

É usado no serviço normal DCF sem requisitos de prioridade

EIFS (Extended Interframe space)

É usado sempre que ocorre um erro de transmissão.

É um intervalo de tamanho variável de acordo com os erros ocorridos.

Funções de Acesso ao Meio

O acesso ao meio é coordenado por duas funções:

DCF (Distributed Coordination Function)

- Implementa o mecanismo CSMA/CA com ou sem a técnica RTS/CTS

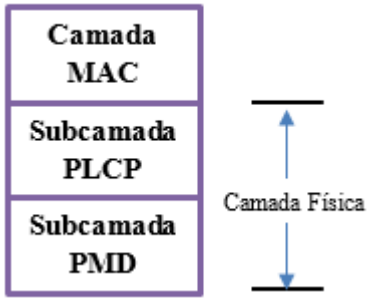
PCF (Point Coordination Function)

- Implementa mecanismos que garantem um meio livre para transmissão
- Baseia-se na utilização de tempos que determinam quando é que um dispositivo pode iniciar a comunicação.

802.11 – Camada Física

A camada física especificada no padrão IEEE 802.11 é responsável pela transmissão dos bits através do canal de comunicação, definindo as especificações eléctricas e mecânicas. A principal função da camada física é a modulação, preparando a informação para ser transmitida no meio, em forma de onda electromagnética. Além da modulação, utiliza-se uma técnica de espalhamento do sinal denominada "Spread Spectrum" que tem a função de proteger o sinal contra interferência co- canal.

O padrão prevê que o nível físico empregará três formas de transmissão: duas de rádio-frequência baseadas em spread spectrum, conhecidas como Frequency Hopping Spread Spectrum (FHSS) e Direct Sequence Spread Spectrum (DSSS), além da transmissão infravermelha difusa. Podemos dividir a camada física em duas subcamadas, conforme mostra a figura a seguir.



Estrutura da camada Física

PMD *(Physical Medium Dependent):*

Esta subcamada trata das diferentes técnicas de transmissão, cuidando da modulação e codificação do sinal, e sendo responsável pelo envio e recebimento de pacotes no meio. Esta função é executada modulando os pacotes provenientes da camada superior (PPDU-PLCP Protocols Data Unit) e demodulando os pacotes recebidos de outra estação;

PLCP (Physical Layer Convergence Procedure):

- Esta subcamada provê os pontos de acesso de serviços comuns ao nível físico, sendo a interface entre a camada de enlace e a camada física.
- Sua principal função é entregar as informações recebidas da PMD, na forma de PPDU, à subcamada MAC, e preparar as informações provenientes da própria subcamada MAC para serem enviadas à PMD.

A troca de informações entre a camada física e a subcamada MAC é realizada através de quadros denominados MPDU (MAC Protocols Data Unit). O MPDU contém campos de informações alocadas pela PLCP necessários à comunicação das camadas. As subcamadas PLCP e PMD comunicam-se através de premissas.

Operações da Camada Física

As operações da camada física são similares, independentemente da técnica de modulação utilizada. O Padrão definiu três estados possíveis, conforme descritos abaixo:

a) Detecção de Portadora: estado que permite a camada MAC "escutar" o meio;

b) Transmissão: modo de transmissão dos dados;

c) Recepção: modo de recebimento dos dados.

Detecção de Portadora

A camada física executa esta operação consultando a PMD periodicamente para saber se o meio está ocioso ou não. A PLCP implementa as seguintes operações, no caso de nenhuma transmissão ou recepção:

1. Detecção de sinais de entrada: a PLCP verifica, periodicamente, o meio para detectar a chegada de alguma mensagem. Quando algum quadro MPDU é detectado, seu cabeçalho é lido de forma a se identificar o destino daquela informação;

2. Determinação de canal ocioso: esta operação verifica, periodicamente, se o canal está ocioso ou não (através de premissas).

Transmissão

A PLCP envia uma mensagem para a PMD alterar seu estado de detecção de portadora para transmissão, assim que recebe um pedido de requisição de transmissão da subcamada MAC. A PMD responde à solicitação garantindo que o serviço está disponível e envia um preâmbulo.

Recepção

O modo recepção tem início sempre que a PMD se encontra no modo de detecção de portadora e um pacote é detectado. O sinal do pacote para ser detectado deverá possuir uma intensidade de potência mínima de 85dBm e seu preâmbulo ser considerado válido, para então o processo de verificação de cabeçalho ser iniciado. Caso o cabeçalho não contenha erro, ele será anexado a uma premissa que é enviada à subcamada MAC pela PLCP para indicar a chegada de um pacote.

WLAN – RF

As comunicações sem fios baseiam-se em ondas de rádio frequência (RF – Rádio Frequency)

- O emissor dispõe de uma antena e de um gerador de sinais RF
- O receptor dispõe igualmente de uma antena e um receptor RF
- O emissor gera um sinal com uma determinada frequência que depois é radiado através da antena e detectado pelo receptor
- As comunicações fazem-se dentro de bandas de frequências que são distribuídas de acordo com a função a que se destinam;
- As comunicações WLAN utilizam a banda [2,412 GHz, 2,484 GHz] chamada a banda dos 2.4 GHz
- E a banda [5,150 GHz, 5,825], a chamada banda dos 5 GHz.
- Para transmitir um sinal é usado uma portadora, que é um sinal periódico a oscilar a uma frequência fixa.

- A portadora é modulada segundo a informação que se pretende enviar.

Actividade 2.3: Relação 802.11 e RM-OSI

Introdução

Após a discussão que acabamos de levar a cabo na unidade anterior sobre o padrão 802.11 e, tendo em consideração que na disciplina de Redes IP te confrontaste com modelos de sete camadas como o RM-OSI e o modelo TCP/IP, a base da internet, faz todo o sentido estabelecermos alguma relação com o padrão 802.11, cuja arquitectura assenta em apenas duas camadas: a Fisica e a de Enlace. Por isso, colocamos-te como primeira actividade de aprendizagem recapitulares os dois modelos referenciados.

Comparação do 802.11 com o RM-OSI

O IEEE (Institute of Electrical and Electronics Engineers) apresentou em 1997 um modelo de referência para redes sem fio denominado IEEE 802.11. Este modelo define especificações que abrangem as camadas física e de enlace (segundo o modelo de referência OSI).

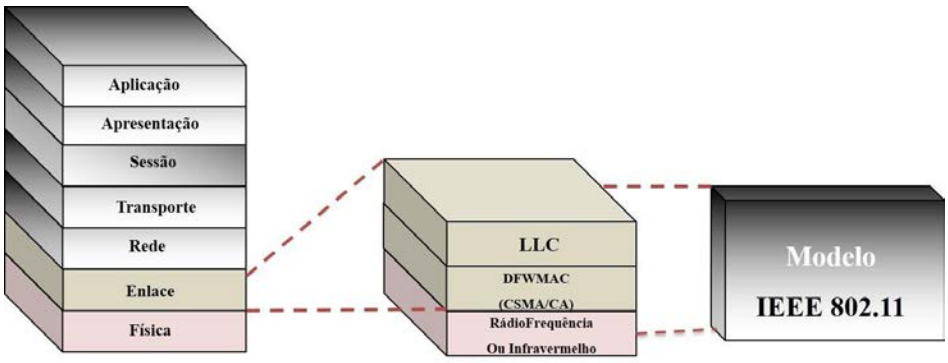
Camada Física:

- Define como as informações são trocadas no meio através de transmissão por radiofrequência ou por infravermelho;

Camada de Enlace:

- Define o método de acesso ao meio. O Padrão IEEE 802.11 utiliza um método denominado CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), semelhante ao das redes locais ethernet, CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

A taxa de transmissão nominal deste Padrão era de 1 a 2Mbps. Atendendo a uma exigência de mercado, em 1999 surgiu uma nova especificação, a IEEE 802.11b, que proporcionava maior velocidade de transmissão. O IEEE alterou as características da camada física para que fosse possível atingir maior velocidade nominal, neste caso, de até 11Mbps.



Comparação do 802.11 com o RM-OSI. fonte: autor

Principais características da família 802.11:

- **802.11a**: Operação em 5GHz, 54Mbps, modulação OFDM
- **802.11b:** Operação em 2,4GHz, 11Mbps, DSSS/FHSS
- **802.11d**: Wold Mode (Europa 20dB, EUA/BRA 36dB)
- **802.11e:** Suporte para aplicações que necessitam de Qualidade de Serviço (QoS)
- **802.11f:** Recomendação para redes ponto a ponto sob protocolo IAP (Inter Access Point)
- **802.11g:** Operação em 2,4GHz, 54Mbps, modulação OFDM, compatibilidade com o 802.11b
- **802.11h:** Gerenciamento do espectro
- 802.11i: Avanços em segurança

Normas das Comunicações sem fios

partir do 802.11 criou-se um vasto conjunto de adendas:

	802.11a	802.11b	802.11g
Banda de Frequência (GHz)	5	2.4	2.4
Número de canais	23	11	11
Nº de canais sem sobreposição	11	3	3
Velocidades especificadas na Norma (Mbps)	6, 12, 24	1.2, 5.5, 11	6, 12, 24
Velocidade máxima com DSSS (Mbps)	-	11	11
Velocidade máxima com OFDM (Mbps)	54	-	54

Normas das Comunicações sem fios

Roaming

- O roaming é uma importante característica de comunicação sem fio.

- Permite que estações mudem de célula e continuem enviando e recebendo informações.
- Sistemas de roaming empregam arquiteturas de microcélulas que usam pontos de acesso estrategicamente localizados.
- O handoff entre pontos de acesso é totalmente transparente para o usuário.

Como é que funciona o Roaming?

- A MS, ao perceber que a qualidade da conexão actual ao seu AP está muito fraca, começa a buscar por um outro AP.
- A MS escolhe então um novo AP baseada por exemplo, na potência do sinal, e envia um pedido de adesão à célula deste novo AP.
- Na célula visitada, o AP desta, irá verificar se a MS visitante não havia se registado anteriormente.
- Caso esse procedimento não tenha sido efectuado, o referido AP irá informar ao AP da célula origem sobre a nova posição
- O novo AP envia uma resposta de adesão, e a estação passa a pertencer a essa nova BSS.
- O AP da célula origem fica sabendo da nova posição da estação móvel, e envia a informação a ela destinada, como se a referida estação estivesse em sua própria célula.

Conclusão

O padrao de comunicação IEEE 802.11 foi criado em 1999 para suportar a comunicação em Redes Locais Sem Fio, (WLANs – Wireless Local Networks). A especificação define uma camada de acesso ao meio, camada MAC, e diferentes camadas físicas, tornando possível aceder o meio de três formas:

– FHSS (Frequency Hopping Spread Spectrum),

– DSSS (Direct Sequence Spread Spectrum) e

– Infra-vermelho

Muitas vezes o padrao 802.11 é chamado de "Ethernet sem fio", por ser uma extensão natural do padrão Ethernet (IEEE 802.3). No protocolo 802.11, a unidade de arquitectura é um BSS (Basic Service Set). Um BSS é definido como um grupo de estações comunicantes sob controle de uma funcão de coordenação (DCF – Distributed Coordination Function), que é responsável por determinar quando um dispositivo pode enviar/receber dados. As estações podem se comunicar directamente (ponto-a-ponto) ou com o suporte de uma infra-estrutura. Redes que se comunicam da primeira forma são conhecidas como redes ad-hoc, enquanto que a segunda são chamadas de redes infra-estruturadas. Essas ultimas utilizam estações-base para interconectar os dispositivos para prover suporte a mobilidade.

Detalhes

Caro estudante,

Tal como dissemos no início, esta unidade é extensa e exige de ti muita atenção. Não precisas terminá-la duma vez! faça tantas pausas quantas achares necessárias. Trabalhe as temáticas com muita calma, dê alguma olhada na disciplina de redes de computadores sempre que se mostrar necessário. À semelhança das outras unidades, no final desta também ser-te-á colocada uma prova. Resolva-a!

Avaliação

1. Que tipo de dispositivos podem comunicar em modo full-duplex com um AP?
2. Numa arquitectura ESS, os APs não podem ter SSID iguais?
3. Suponha que um amigo seu se colocava entre o seu computador e a antena do AP. Dirias para ele sair da frente?
4. As camadas de acesso do Ethernet e do 802.11 usam o mesmo protocolo de controlo do acesso ao meio?
5. De que forma o 802.11 evita que os dispositivos, que esperam que o meio fique livre, iniciem todos a transmissão, simultaneamente, após o período de tempo DIFS?
6. A utilização de redes wireless traz algum perigo por causa da radiação? Qual o impacto da radiação de rádio frequência no corpo humano?
7. O que é a Wi-fi?
8. Caracterize as WMAN - Wireless Metropolitan Area Network
9. Que vantagens uma rede sem fio apresenta sobre uma rede convencional com fios?
10. Porquê ainda usamos redes cabladas?

Guião de Correcção

Questão	**Sugestão de resposta**
Q1	O modo full-duplex não é suportado nas comunicações sem fios. Os dispositivos só podem comunicar em modo half-duplex porque os Aps usam as mesmas frequências de transmissão e recepção.

Q2	Se os SSID forem diferentes, o cliente teria de se identificar com o novo SSID sempre que passasse a comunicar com outro AP, com a consequente interrupção do processo normal de comunicação de dados. Para garantir a continuidade da comunicação do cliente quando este transita entre Aps, os Aps são configurados com o mesmo SSID e dentro da mesma VLAN
Q3	O corpo do seu amigo pode atenuar o sinal. Pedir para ele sair da frente iria depender da qualidade do sinal que lhe estava a chegar, e da qualidade do sinal que considerasse razoável.
Q4	Não. A utilização de um meio partilhado implica a utilização de um protocolo que elimine ou que, pelo menos, reduza a probabilidade de colisão. O protocolo usado nas LAN Ethernet é o CSMA/CD em que o emissor consegue detectar colisões. No caso de wireless, não é possível detectar colisões (o emissor não consegue transmitir e receber ao mesmo tempo), o protocolo usado é CSMA/CA.
Q5	No caso de termos vários dispositivos a escutar o meio simultaneamente, o protocolo força a que após o meio ficar livre se espere durante um DIFS. Findo este tempo, para evitar que todos iniciem as suas transmissões em simultâneo, com a consequente ocorrência de colisões, o 802.11 considera uma janela de contenção após o tempo DIFS (janela de backoff). A janela está dividida em slots. Após o DIFS, o dispositivo escolhe um slot e só acede ao meio no tempo do seu slot.
Q6	– A princípio, os riscos da utilização de uma rede wireless são semelhantes aos da utilização do telefone celular. – Todavia as redes locais sem fio, Wireless LAN (WLAN), trabalham com potências bem inferiores as utilizadas na telefonia celular.
Q7	– Para garantir a compatibilidade entre os equipamentos de diferentes marcas, um grupo de empresas se uniu e formou a Wi-Fi Aliance. – Esta organização tem o objetivo de certificar produtos WLAN e garantir a interoperabilidade entre eles.
Q8	– Refere-se a redes metropolitanas sem fio: redes de uso corporativo que atravessam cidades ou estados. – Neste grupo temos as tecnologias que tratam dos acessos de banda larga para última milha para redes em áreas metropolitanas, com alcance em torno de 6 a 50 km.

Q9	–Flexibilidade;uma vez que ondas de rádio podem atravessar paredes, assim os receptores e transmissores podem ser colocados em qualquer lugar, até mesmo escondidos, dentro de paredes. –Versatilidade; poder interligar os PCs sem precisar passar cabos pelas paredes. Tanto os notebooks quanto handhelds e as futuras webpads podem ser movidos livremente dentro da área coberta pelos pontos de acesso sem que seja perdido o acesso à rede.
Q10	– Maior confiabilidade: - o sinal de rádio está sujeito a interferências, inclusive aquelas provocadas intencionalmente com o objetivo de paralisar a comunicação e a rede. Ex: forno de micro-ondas, telefones sem fio. – O sinal de rádio sofre perdas quando se depara com obstruções físicas. – Espelhos d´agua, árvores, paredes, maços de papel, etc são significativas fontes de atenuação e dispersão do sinal de rádio –Segurança: Em redes sem fio a rede "está no ar". Qualquer um dentro do alcance do sinal pode acessar a rede. Nas redes cabeadas o perímetro de acesso está limitado pelo alcance dos cabos e pelas ativações dos pontos nos paineis de conexão.

Resumo da Unidade

Na unidade que agora termina, entrou em contacto com vários conceitos. Aliás, já tinhamos feito referência que esta unidade seria um pouco mais extensa do que o habitual. Pois, ela é constituida por quatro actividades de aprendizagem, calculadas para cerca de 30 horas de trabalho. Na actividade 2.1 apresentamos a Computação Móvel, sua origem e razãoes/ benefícios, sua relação com computação ubíqua e pervasiva. Terminamos esta actividade olhando para os desafios que hoje se colocam à computação móvel. Na actividade 2.2 apresentamos Redes sem fios (wireless) e o desenvolvimento tecnológico que permitiu o seu surgimento. Discutimos o conceito de WLAN e a norma 802.11 que o sustenta. Olhamos ainda a arquitectura e funcionamento duma WLAN. As camadas Física e de Enlace do 802.11, bem como o protocolo CSMA/CA. Terminamos esta actividade comparando o 802.11 com o RM-OSI.

Reservamos a Actividade 2.3 para discutirmos as Técnicas de acesso ao meio: FDMA, TDMA e CDMA. E por último, vimos na Actividade 2.4 as redes móveis celulares, os conceitos envolvidos, componentes e respectivas características e funções. A terminar lançamos um olhar sobre as redes GSM e GPRS. Cada uma destas actividades foi seguida de um teste de verificação dos conhecimentos.

Avaliação da Unidade

Verifique a sua compreensão!

Instruções

Como se deve ter apercebido, no final de cada actividade de aprendizagem havia uma prova a prestar como forma de verificar o nível da sua aprendizagem. Agora que terminas a unidade toda, há tambem uma prova que engloba as matérias tratadas nas quatro actividades de aprendizagem. Leia a prova com atenção e depois responda às questões colocadas. Sempre pode voltar um pouco para trás para consultar uma e outra coisa. No final, compare as tuas respostas com as sugeridas no final da prova, e atribua a pontuação sugerida.

Critérios de Avaliação

A pontuação e peso das perguntas estão no guião de correcção mais abaixo.

Prova Final da Unidade

1. Comunicações móveis são aquelas onde existe a possibilidade de movimento relativo entre partes ou as partes sistêmicas envolvidas. Indique três características de um sistema móvel quanto aos aspectos listados nos items a seguir:
   a) Aspectos da Mobilidade
   b) Requisitos do Sistema
   c) Tipos de redes
2. Caracterize o termo "Celular" no contexto das comunicações móveis e fale da sua constituição.
3. Quais são os elementos fundamentais de uma rede de telecomunicações móveis?
4. Em que contexto se dá o procedimento de Roaming em comunicações móveis?
5. O procedimento de handoff é iniciado quando a ERB detecta que o nível do sinal recebido da EM está abaixo do limiar permitido ao sistema. Que entende por handoff nas Comunicações Móveis.
6. A camada física especificada no padrão IEEE 802.11 é responsável pela transmissão dos bits através do canal de comunicação, definindo as especificações eléctricas e mecânicas. Indique a função principal desta camada e as suas implementações básicas.
7. Um dos métodos de acesso ao meio em redes 802.11 é o CSMA/CA. Descreva este método de acesso. Mostre que o método é justo (no acesso dos terminais ao meio) e que evita o congestionamento da rede em situações de carga elevada.

8. Na arquitectura GSM, o Mobile Country Code é composto por quantos dígitos? No seu país, quais são esses digitos?
9. O que é e qual a função do IMEI?
10. Nesta unidade discutimos largamente as técnicas de acesso ao meio. Qual é o objectivo técnico dessa discussão?

Guião de Correcção

Questão	**Sugestão de resposta**	**Pontuação**
Q1	Aspectos da Mobilidade • Utilizador desloca-se livremente no espaço • Utilizador comunica em qualquer momento • Utilizador comunica com qualquer outro utilizador • Utilizador acede à rede através de uma ampla gama de terminais	1.5
	Requisitos do Sistema • Equipamento portátil: terminais de pequena dimensão com baterias de capacidade elevada • Interoperação com outras redes: suporta comunicação com redes de outros tipos • Grande capacidade de tráfego • Segurança de serviço: técnicas avançadas de autenticação e encriptagem	1.5
	Tipos de redes • WPAN - Wireless Personal Area Networks: short distances among a private group of devices • WLAN - Wireless Local Area Networks: areas such as an home, office or a group of buildings • WMAN - Wireless Metropolitan Area Networks: from several blocks of buildings to entire cities • PLMN - Public Land Mobile Networks: regions and countries	1.5

Q2	O termo celular refere-se ao facto de que uma área geográfica é dividida em várias áreas de cobertura geográfica, conhecidas como células. Cada célula contém uma estação base que consiste de uma torre e uma pequena construção que contém o equipamento de rádio que se comunica com estações móveis (enviando ou recebendo sinais) dentro da sua célula.	1.5
Q3	Os elementos fundamentais de uma rede de telecomunicações móveis são as estações base (ERB) que efectuam a ligação via rádio entre o telefone móvel e a infra-estrutura da rede de comunicações móveis.	2.5
Q4	Quando uma EM sai de sua área de localização, seja dentro do sistema controlado pela mesma operadora, ou para outro sistema o procedimento de roaming é iniciado. O processo começa quando a EM verifica pelo FOCC que a ID do sistema não corresponde àquela em seu registo interno.	2.0
Q5	Comutação de uma chamada em andamento de uma ERB para outra quando a estação móvel cruza a fronteira entre as células • Terminal move-se para uma célula vizinha • Uma nova estação base passa a assegurar a comunicação • A ligação tem de ser mantida de forma transparente para o utilizador	2.0
Q6	A principal função da camada física é a modulação, preparando a informação para ser transmitida no meio, em forma de onda electromagnética. Além da modulação, utiliza-se uma técnica de espalhamento do sinal denominada “Spread Spectrum” que tem a função de proteger o sinal contra interferência co- canal. Suas implementações são rádio-frequência baseadas em spread spectrum, cujas formas são conhecidas como Frequency Hopping Spread Spectrum (FHSS) e Direct Sequence Spread Spectrum (DSSS), além da transmissão infravermelha difusa.	3.0

Q7	CSMA/CA - Carrier sense multiple access with collision avoidance (Acesso múltiplo com verificação de portadora com anulação/prevenção de colisão) é um método de transmissão que possui um grau de ordenação maior que o (CSMA/CD) e possui também mais parâmetros restritivos, o que contribui para a redução da ocorrência de colisões em uma rede (máquinas interligadas através de uma rede identificam uma colisão quando o nível de sinal aumenta no interior do cabo). Antes de transmitir efectivamente um pacestação avisa sobre a transmissão e em quanto tempo a mesma irá realizar a tarefa.	3.0
Q8	Mobile Country Code – MCC (3 dígitos)	0.5
Q9	Com o IMEI pode-se fazer o rasteio e o bloqueio total do aparelho por parte da operadora. Outra função do IMEI é identificar quando, onde e quem está fazendo determinada ligação.	0.5
Q10	Buscar uma maior eficiência no uso do espectro disponível aos serviços de rádio móvel.	0.5

Unidade 3: Sistemas e normas para a telefonia sem fios

Introdução à Unidade

Buscando uma maior eficiência no uso do espectro disponível aos serviços de rádio móvel, foram criadas técnicas que permitem o acesso de múltiplos usuários ao meio de transmissão, ou seja, o compartilhamento de canais de rádio. Três métodos de acesso ao meio se destacaram nos sistemas de comunicação móvel celular diferenciados apenas pela manipulação adequada da frequência, tempo ou código.

Esta unidade que agora começa, vai-nos permitir adquirir conhecimentos sobre as diferentes gerações de redes móveis e redes de telefonia sem fio. Ele discute em detalhe as técnicas de acesso múltiplo ao meio em comunicações móveis, a rede móvel GSM, GPRS, EDGE, LTE e as gerações CT0, telefone sem fios CT1, CT2, e operação das (DECT) DECT que define uma tecnologia de interface aérea para telecomunicações sem fio.

Objetivos da Unidade

Após a conclusão desta unidade, deverá ser capaz de:

1. Descrever a evolução das tecnologias das diferentes gerações de redes móveis e de telefonia.
2. Caracterizar o funcionamento de redes sem fio da segunda geração: IS-95; CT2; DECT.
3. Descrever o funcionamento das redes móveis GSM, EDGE, GPRS
4. Descrever a operação das redes móveis de terceira e quarta geração (UMTS, LTE).

Termos-chave

FDMA: Acesso Múltiplo por Divisão de Frequência

TDMA: Acesso Múltiplo por Divisão do Tempo

CDMA: Acesso Múltiplo por Divisão de Código

GSM: Sistema Global para Telecomunicações Móveis

GPRS: Serviços Gerais de Pacotes de Dados por Rádio

EDGE: Taxa Melhorada de Transferência de dados para o GSM

UMTS: Sistema Universal de Telecomunicações Móveis

Actividades de Aprendizagem

Actividade 3.1 - [Técnicas de Acesso Múltiplo]

Introdução

Vários esquemas de acesso múltiplo tem sido utilizados para permitir que vários usuários possam usar de maneira compartilhada uma quantidade restrita do espectro de rádio.
O compartilhamento do espectro é necessário para obter o desempenho requerido na comunicação. A implementação do esquema de acesso múltiplo deve ser feito de maneira a suportar a demanda de tráfego.

A primeira questão que se coloca é para quê técnicas de acesso?

- Para permitir o compartilhamento de uma determinada faixa de rádio frequência entre vários terminais móveis.

Porquê o compartilhamento?

- Para maximizar o número de usuários simultâneos numa faixa de frequências.

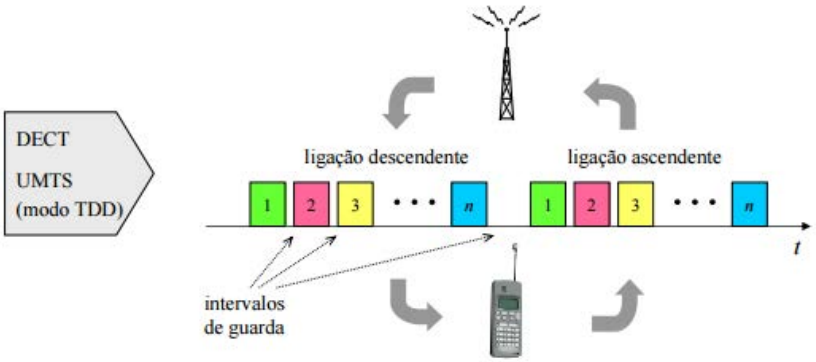
Comunicação bidirecional

Em sistemas de comunicação sem fio frequentemente é necessária a comunicação bidirecional (duplexação), onde cada estação pode enviar e receber dados de maneira simultânea. Num sistema de telefone fixo (ou celular), por exemplo, é possível falar e ouvir simultaneamente.
A duplexação pode ser implementada através de divisão em frequência (FDD=Frequency Division Duplexing) e em tempo (TDD=Time Division Duplexing)

- O canal pode ser dividido temporalmente ou na frequência (TDD & FDD)

Esquema TDD (Time Division Duplexing)

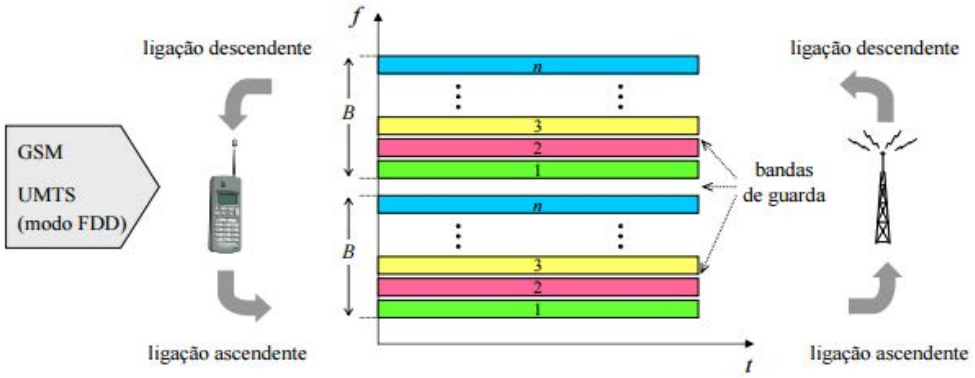
A transmissão só ocorre em momentos permitidos e pré-determinados, atribuídos através de Time Slots. Os terminais móveis são mais simples, pois o duplexador não é necessário e os circuitos receptor e transmissor podem ter partes comuns. Ao invés do duplexador (como no FDD), emprega uma chave T/R (transmite / recebe).



Princípio da transmissão TDD

Esquema FDD (Frequency Division Duplexing)

Num esquema de FDD, usa-se uma frequência de transmissão entre estação base e estação móvel e outra entre a estação móvel e estação fixa. Um dispositivo denominado duplexador permite o uso de uma mesma antena para os módulos de recepção e transmissão do terminal móvel. A separação de frequências de transmissão e recepção geralmente é fixa em todo o sistema. Sendo suficientemente alta para permitir pouco acoplamento entre os módulos receptor e transmissor de um terminal de assinante.



Princípio da transmissão FDD

Em ambos os casos uma parcela do canal é destinada à transmissão e outra à recepção.

Técnicas de Acesso ao Meio

Objectivo:

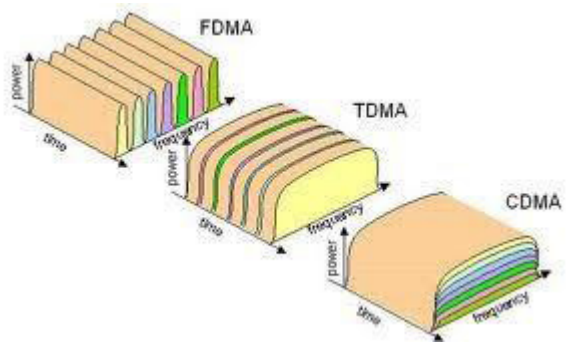
Buscar uma maior eficiência no uso do espectro disponível aos serviços de rádio móvel.

rês métodos de acesso ao meio se destacaram nos sistemas de comunicação móvel celular diferenciados apenas pela manipulação adequada da frequência, tempo ou código. São elas:

- Frequency Division Multiple Access (FDMA)
- Time Division Multiple Access (TDMA)
- Code Division Multiple Access (CDMA)

Os sistemas também podem ser classificados com relação a largura de faixa do canal

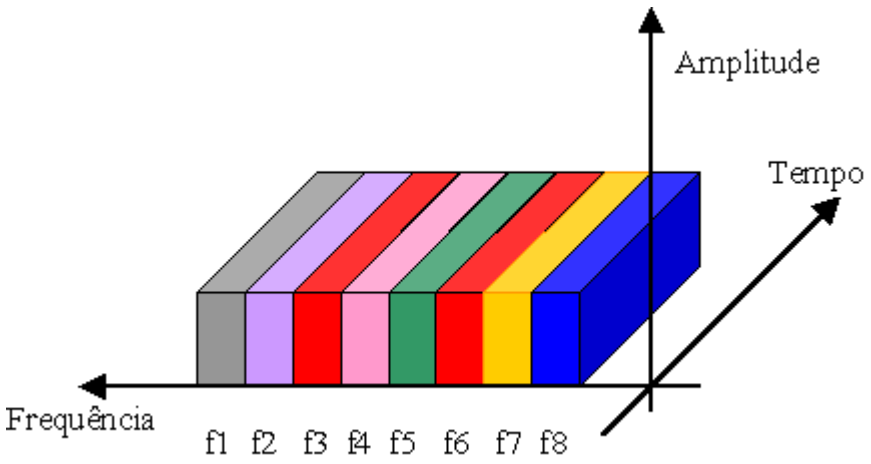
- Um sistema de faixa estreita tem seu espectro dividido em canais de faixa suportando taxas inferiores a 2 Mbps,
- Na arquitectura de faixa larga, todo o espectro é compartilhado pelos usuários
  - O FDMA é uma arquitectura de faixa estreita,
  - O CDMA é uma arquitectura de faixa larga.
  - TDMA pode ser implementado como de faixa estreita ou de faixa larga.



Métodos de acesso ao meio. Fonte: Wikepedia

ACESSO FDMA – Frequency Division Multiple Access

- O Acesso Múltiplo por Divisão de Frequência é o método mais comum de acesso entre os sistemas analógicos
- O espectro é dividido em canais onde cada assinante sintoniza sua portadora
- O número de canais no sistema será função da largura de cada canal



Acesso FDMA . fonte: wikpedia

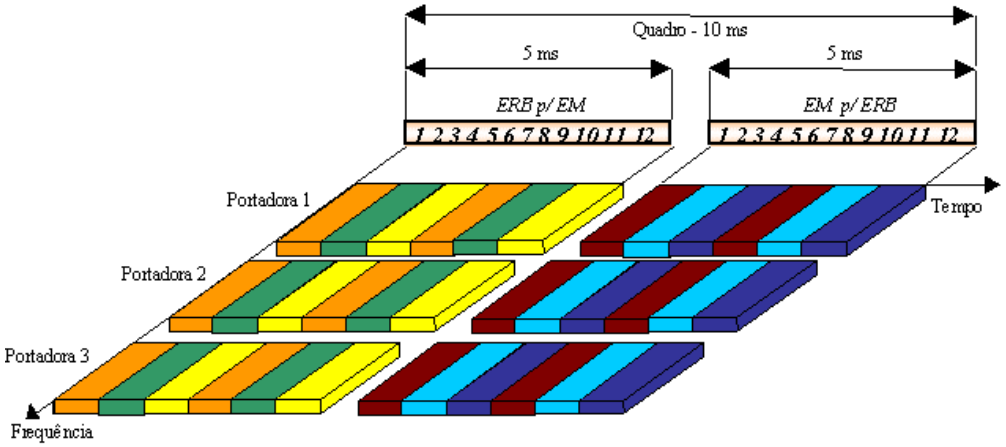
Neste método a largura de faixa total disponível é subdividida e a cada usuário é alocada uma dessas sub-faixas, normalmente por demanda.

Características principais dos sistemas que utilizam FDMA:

- Se um canal não está sendo utilizado há um desperdício de recurso
  - nenhum usuário o estará utilizando
- A largura de faixa de cada canal é normalmente pequena
  - um sistema com FDMA normalmente é um sistema de faixa estreita.
- Pelo facto de o canal ser estreito, em uma transmissão digital tem-se longas durações dos símbolos transmitidos em relação ao espalhamento temporal causado pelo canal.
- A comunicação é contínua no tempo, o que leva à necessidade de poucos bits de overhead com o propósito de sincronização e delimitação de frames em uma transmissão digital.
- Os filtros de canal são normalmente caros, pois necessitam apresentar selectividade suficiente para reduzir a interferência entre canais adjacentes a patamares aceitáveis.
- Por transmitir e receber ao mesmo tempo, os transceptores necessitam de duplexers, o que eleva o custo do sistema.
- Nos casos em que muitos canais compartilham uma mesma antena e, portanto, o mesmo amplificador de potência, pode ocorrer intermodulação.

ACESSO TDMA – Time Division Multiple Access

No método de Acesso Múltiplo por Divisão de Tempo o espectro disponível é dividido em intervalos (slots) de tempo de tal forma que cada usuário possa transmitir ou receber durante o intervalo de tempo a ele reservado.



Acesso TDMA. Wikpedia

Sistemas com TDMA operam somente com sinais digitais.

- Em sistemas com TDMA/TDD, metade dos slots são destinados á transmissão e metade à recepção.
- No caso de TDMA/FDD um mesmo slot é utilizado na transmissão e recepção, sendo a separação feita na frequência.

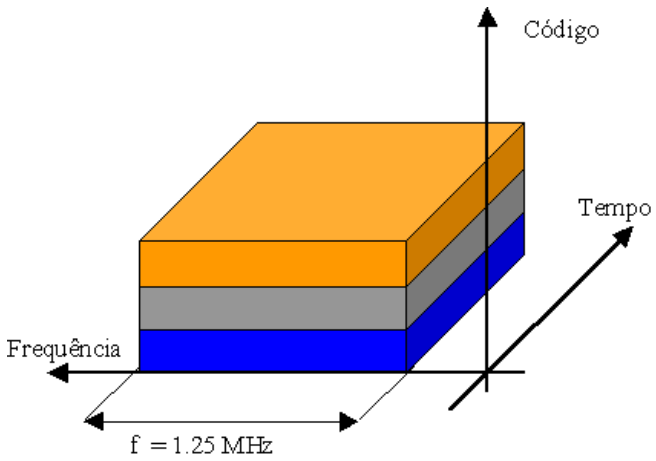
Pela característica digital do sistema há maior imunidade a ruído e interferência e também mais segurança no enlace de comunicação promovendo privacidade ao usuário.

Características principais:

- Devido às descontinuidades na transmissão, o processo de handoff do usuário móvel se torna mais simples, pois ele pode utilizar os intervalos de tempo sem transmissão para "ouvir" outros transmissores de outras estações base, por exemplo, no caso de telefonia celular.
- Os slots de tempo podem ser alocados por demanda para diferentes usuários, baseado em uma prioridade, dessa forma compartilha-se melhor o espectro

Uma grande vantagem deste método é que as taxas de transmissão podem ser variáveis em múltiplo da taxa básica do canal. O método TDMA é atribuído à sistemas digitais como GSM, D-AMPS (IS-136) e PDC.

ACESSO CDMA – Code Division Multiple Access



Acesso CDMA. Fonte: Wikpedia

O Acesso Múltiplo por Divisão de Código foi desenvolvido nos EUA pelo segmento militar.

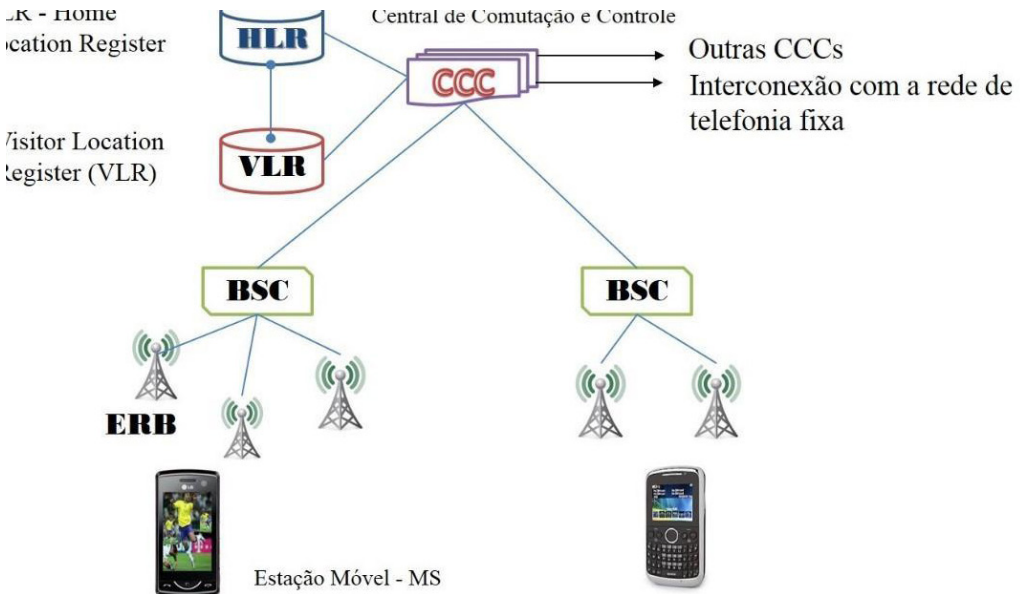
- Sua 1ª utilização foi para a comunicação entre aviões de caça e rádio controle de mísseis teleguiados.
- Neste método de acesso as EMs transmitem na mesma portadora e ao mesmo tempo, mas cada comunicação individual é provida com um código particular. Isto garante alta privacidade na comunicação.

No método de Acesso Múltiplo com Divisão por Código é utilizada a técnica de espalhamento espectral (spread spectrum).

- O transceptor de cada usuário no sistema utiliza uma sequência pseudo aleatória (código) diferente.
- Todos os usuários transmitem ao mesmo tempo e utilizam a mesma faixa de frequência.
- O receptor, através do processo de correlação do sinal recebido com a sequência PN (pseudo-noise) extrai o sinal do usuário desejado.
- Os sinais dos demais usuários parecerão ruído para o receptor em questão.

A eficiência de utilização do espectro, ou capacidade de um sistema CDMA (IS-95), é maior que os demais sistemas existentes AMPS, TDMA (IS-136) e GSM."

Arquitectura Básica



Esquema básico. Fonte: autor

No processo de transmissão pelo método do CDMA a voz é primeiramente codificada, passa por um expansor (spreader) que a multiplica por sequência pré-estabelecida e única para cada estação móvel (EM).

Os sistemas que utilizam o método CDMA tem como padrão de reuso somente uma célula por cluster.

Os sistemas que utilizam o CDMA seguem o padrão IS-95 com taxa de espalhamento a 1,2288 Mbps utilizando uma portadora de 1,25 MHz de faixa.

Vantagens do CDMA

- Mais qualidade e privacidade na comunicação,
- Maior autonomia de baterias,
- Redução no nível de interferência,
- Serviços mais velozes de transmissão de voz e dados

O CDMA foi a tecnologia escolhida para ser a base para a 3ª geração. É claro que para o usuário final as tecnologias usadas são transparentes, importando mesmo os serviços oferecidos pelas operadoras e a qualidade do serviço prestado.

Mas, afinal, qual técnica é a superior?

A questão tem a ver com o número máximo de usuários suportado!

- O CDMA tem-se mostrado promissor a superar as demais técnicas de acesso múltiplo existentes.
- A capacidade de um sistema CDMA é o que se pode chamar de limitada pelas interferências. Ao contrário dos concorrentes FDMA e TDMA que podem ser classificados como limitados em largura de faixa.

Qualquer melhoria deve se refletir directamente em um aumento no número de usuários no sistema.

Conclusão

Na actividade de aprendizagem que agora termina discutimos as técnicas de acesso múltiplo em comunicações móveis. Vimos as razões e a importância que estão por detrás dessa discussão. Isto permite-nos perceber como as comunicações móveis celulares funcionam e que constrangimentos e limites podem acontecer.

Actividade 3.2 - Redes Móveis Celulares

O conceito de rede celular surgiu como uma forma de melhorar a eficiência na utilização do espectro radioelétrico necessário às comunicações móveis. A ideia surgiu no "Bell Laboratories" (USA) no início dos anos 70. As primeiras redes móveis celulares utilizavam transmissão analógica. Na altura, surgiram vários sistemas diferentes, não compatíveis entre si, que foram sendo adoptados por diferentes países.

Espectro Radioeléctrico

O espectro radioeléctrico é um recurso escasso. O lançamento de novos serviços implica a atribuição de novas bandas. As necessidades de um serviço em termos de largura de banda (ocupação do espectro) dependem de:

- Tipo de serviço (voz, vídeo, dados, …)
- Número de utilizadores

As características de propagação dos sinais de rádio obrigam ao estabelecimento de acordos entre os países e a separação física permite a reutilização das bandas de rádio.

Conceitos envolvidos no Sistema Móvel Celular

- Célula
- Área na qual o sinal de uma ERB é adequadamente recebido
- Cluster
- Conjunto de células que ocupam todo o espectro do sistema
- ERB
- Estação Rádio Base
- EM
- Estação Móvel
- CCC
- Central de Controle e Comutação
- RTPC
- Rede Telefónica Pública Comutada
- Área de Controle
- Área sob supervisão de uma CCC
- Área de Serviço
- Toda a área onde a EM tem acesso ao serviço da rádio móvel
- Área de Localização
- Área na qual a EM pode mover-se sem necessidade de actualização do seu registo
- Procedimento de "Handoff"
- Comutação de uma chamada em andamento de uma ERB para outra quando a estação móvel cruza a fronteira entre as células
- Assinante visitante "Roamer"
- Assinante que acede o sistema fora de sua área de localização e necessita da actualização de seu registo de localização.

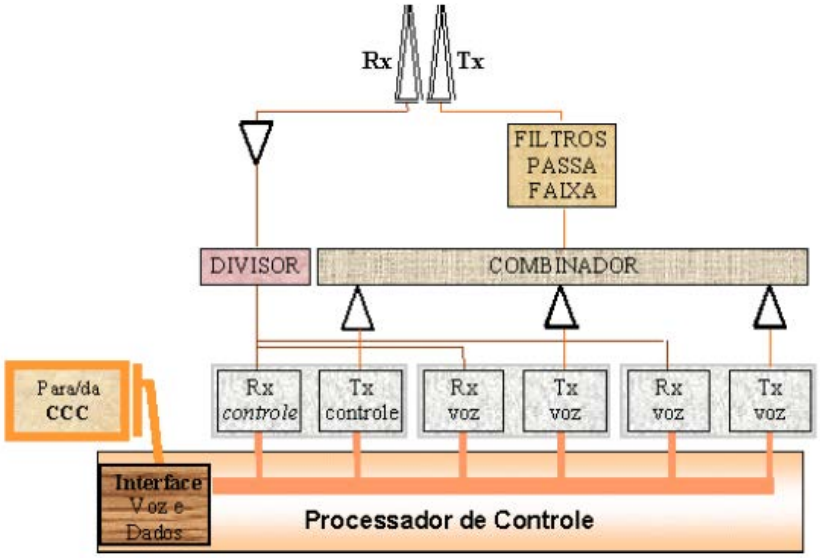
Estação Rádio Base (ERB)

São equipamentos que fazem a conexão entre os telefones celulares e a companhia telefónica, ou mais precisamente a Central de Comutação e Controle (CCC).

- É a repetidora da informação de voz e dados de controle em meio electromagnético;
- Faz de interface entre uma única CCC e diversas EM;
- Cada ERB pode suportar até 154 canais de voz
- A ERB é responsável pela monitoria do sinal recebido de uma EM
- Controle de potência das EM.

Elementos de composição de uma ERB

- Local onde será implantada.
- Infra-estrutura para a instalação dos equipamentos de telecomunicação incluindo a parte civil, eléctrica, climatização e energia CC com autonomia em caso de falta de energia através de baterias e em alguns casos Grupo gerador.
- Torre para colocação de antenas para comunicação com os terminais móveis e enlace de rádio para a CCC.
- Equipamentos de Telecomunicações.



Estação Rádio Base. Fonte: Wikpedia

Sistema de rádio contendo

- Receptores (Rx),
- Transmissores (Tx);
- Combinadores;
- Divisores;
- Filtros e antenas;

Sistema de processamento e controle contendo

- Processador de controle
- Multiplexadores (MUX
- Cabos coaxiais
- Painéis de controle
- Interface com a CCC por MUX a 2Mbps ou mais

Estação Móvel (EM)

- A EM é o terminal móvel do usuário.
- A EM é composto por:
  - Monofone
  - Teclado
  - Unidade de controle
  - Bateria
  - Unidade de rádio e antena

Função:

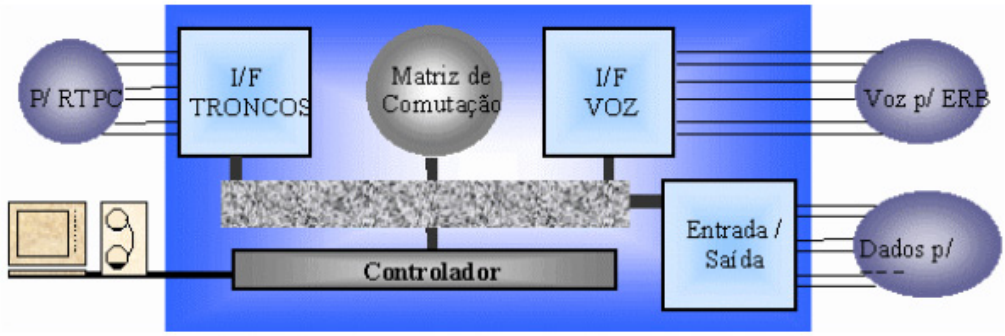
- Fazer a interface electromecânica entre o usuário e o sistema.

Os equipamentos podem ser:

- Portáteis; veiculares ou transportáveis.

Central de Comutação e Controle - CCC

A CCC faz a interface entre o sistema móvel e a rede pública.

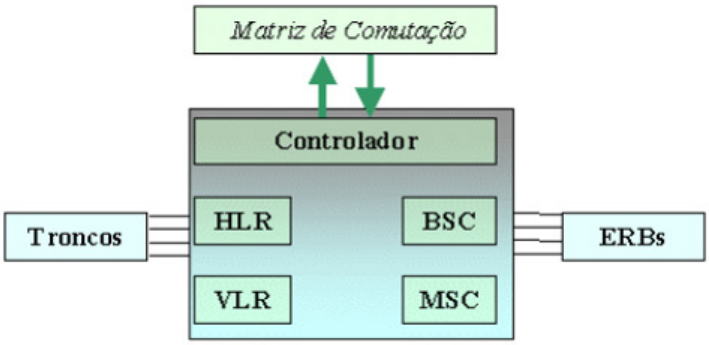


Central de Comutação e Controle – CCC. Fonte: Wikpedia

A CCC é Composto por:

- I/O Devices
- Interface de audio e dados para a ERB
- Terminais de operação e manutenção
- Memória de configuração
- Troncos
- Matriz de comutação
- Controlador

Controlador da CCC



Controlador

O controlador da CCC é composto:

- Da Home Location Register – HLR
- Que é o registo de endereços. Identifica cada móvel pertencente a esta área de localização.
- Da Visit Location Register – VLR
- Que é o registo de endereços de visitantes. Identifica as EM visitantes de outras áreas.
- Da Base Station Controller – BSC
- Que controla cada ERB vinculada a este CCC
- Da Mobile Switch Center – MSC
- Que controla as comutações entre os troncos da rede pública comutada e os canais das ERB vinculadas.

Estação Celular - EC

Funciona como repetidora de informação de voz e de dados entre ERB e o assinante.

Funções:

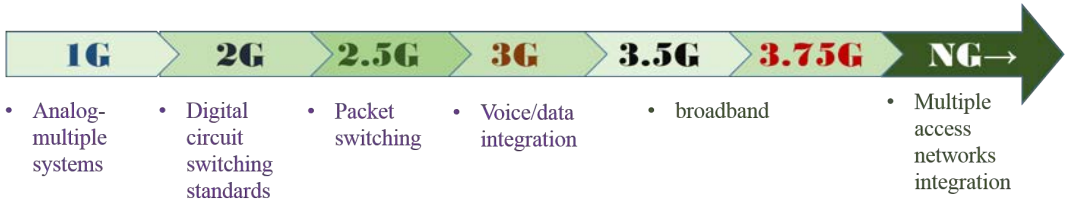
- Recepção
- Tratamento de informação e sua transmissão para o user EM

Unidade Repetidora - UR

Funciona apenas como repetidora dos canais do sistema, ou seja,

- Apenas retransmite informações entre duas ERB ou entre CCC e ERB
- Não há processamento local
- Apenas há recepção
- Filtragem e retransmissão do sinal em potências e relação sinal/ruído adequadas

Evolução das Redes Móveis Celulares



a) Primeira geração (1G):

- baseada em transmissão analógica de voz
- demasiados sistemas diferentes e incompatíveis
- ausência quase total de possibilidades de roaming
- mercados limitados

Exemplos:

- AMPS – Advanced Mobile Phone Service (USA)
- desenvolvida pela AT&T (1971)
- TACS – Total Access Cellular System (Europe)
- C-450 (Europe – Germany, Portugal)
- NMT (Europ2 – Denmark, Spain, …)
- Radiocom 2000 (Europe – France, Belgium)

b) Segunda geração (2G):

Redes completamente digitais, mas ... ainda muito orientadas para os serviços de voz.

- menos sistemas diferentes (existência de normas)
- um único sistema para toda a Europa (GSM)
- mercado mais alargado ► mais competição ► preços mais baixos
- três centros de desenvolvimento: Europa, USA, e Japão

Exemplos:

- GSM (Western Europe)
- IS-54 TDMA (D-AMPS) (USA)
- IS-136 TDMA (USA)
- IS-95 CDMA (CDMAone) (USA)
- PDS (Japan)

c) Terceira geração (3G):

- integração de voz e dados
- suporte nativo para comutação de pacotes
- tendência para núcleos de rede baseados em IP
- utilização mais eficiente do espectro
- maiores taxas de transmissão
- melhor segurança
- ainda assim, demasiados sistemas diferentes

Exemplos:

- UMTS (W-CDMA) (Europe+)
- CDMA2000 (evolution of IS-95) (USA)
- GPRS 136 HS EDGE (evolution of IS-136) (USA)
- UWC-136 (USA)

d) Da terceira geração para a … (3.5G, 3.75G, …):

- ênfase nos serviços de banda larga em comutação de pacotes

Exemplos:

- HSDPA (UMTS) (High-Speed Downlink Packet Access)
- HSUPA (UMTS) (High-Speed Uplink Packet Access)
- HSPA+ (UMTS)
- 1xEV-DO (CDMA2000)
- WiMAX
- Wi-Fi

Conclusão

Mais especificamente, abordamos nesta actividade componentes de um sistema de telefonia móvel e sua evolução histórica.

Actividade 3.3 - Redes GSM

Introdução

Com o avanço da tecnologia, a globalização e a necessidade cada vez maior de as pessoas se comunicarem com rapidez e mobilidade, tornou-se necessária a criação de um sistema capaz de transmitir informações entre usuários em mobilidade.

As necessidades de cada sector impulsionam a evolução da tecnologia, cada qual na sua direcção. O resultado disso é que avanços em um sentido, estimulados pela necessidade de um sector específico, acabam por auxiliar outros sectores. Para que um formato de tecnologia seja amplamente utilizado, é necessário que haja um padrão, maleável o suficiente para que tecnologias mais acessíveis ou mais eficientes possam ser encaixadas em sua estrutura. Pode-se perceber, portanto, a importância de uma organização dessa tecnologia, no sentido de oferecer o serviço de comunicação móvel à maior parcela possível da sociedade. É assim por dizer o que a GSM fez!

Redes GSM - Gênese

1982: o CEPT (Conference of European Post and Telegraph) cria o Groupe Spécial Mobile (GSM)

1989: a normalização do GSM passa para a alçada do ETSI (European Telecommunications Standards Institute)

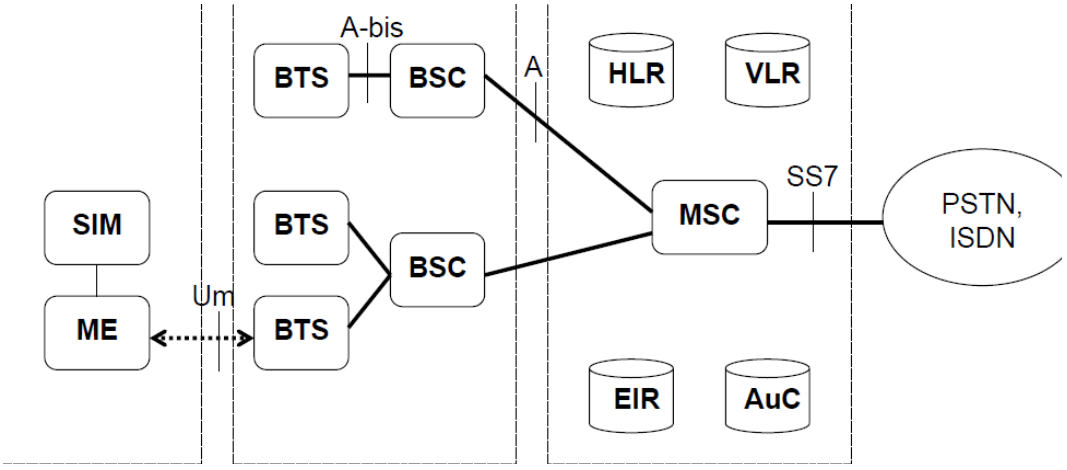
1991: é lançado o primeiro serviço comercial

GSM passa a ser o acrónimo de "Global System for Mobile telecommunications"

Arquitectura

A rede GSM é formada por interfaces abertas e padronizadas, seguindo sua principal intenção, montar uma arquitectura mais abrangente possível. Ela é estruturada para que seja possível a integração entre componentes de diferentes fabricantes, o que enriquece a concorrência e diminui o preço para o usuário. Além do facto, é claro, de torná-la extremamente flexível, logo, mais viável.

Os componentes dessa arquitectura são divididos em 4 grupos O conjunto desses grupos é chamado rede móvel pública terrestre (Public Land Mobile Network – PLMN), e é implementado por uma operadora.



Arquitectura GSM. Fonte: adaptação do autor

- SIM – Subscriber Identity Module
- ME – Mobile Equipment
- BTS – Base Transceiver Station
- BSC – Base Station Controller
- MSC – Mobile Services Switching Center
- HLR – Home Location Register
- VLR – Visitor Location Register
- EIR – Equipment Identity Register
- AuC – Authentication Center

Mobile Station

- Mobile equipment (ME)
  - √ IMEI - International Mobile Equipment Identity
- SIM card (Subscriber Identity Module)
  - √ IMSI - International Mobile Subscriber Identity
    - Mobile Country Code – MCC (3 dígitos)
    - Mobile Network Code – MNC (2 dígitos)
    - Mobile Subscriber Identification Code – MSIC (até 10 dígitos)
- Numeração:
  - √ MSISDN – Mobile Subscriber ISDN

Base Station Subsystem (subsistema da estação base)

- **BTS** - Base Transceiver Station
  - define as células (área de cobertura)
  - contém os emissores/receptores de rádio
  - Implementa os protocolos da ligação rádio
- **BSC** - Base Station Controller
  - Gere a alocação de frequências
  - Gere as alterações nas frequências a usar
  - Contribui para o processo de handover

Network Subsystem (subsistema da rede)

- **MSC** - Mobile services Switching Center
  - Comutação
  - Registo, autenticação, actualização da localização, handover, encaminhamento de chamadas para outras redes, roaming

- **HLR** - Home Location Register
  - armazena informação sobre os assinantes: última localização, estado do terminal, etc.
- **VLR** - Visitor Location Register
  - armazena informação sobre a localização dos assinantes
- **AuC** – Authentication Center
  - serviço responsável pela autenticação dos assinantes
  - inclui os algoritmos de cifragem e as chaves secretas de cada assinante
- **EiR** – Equipment Identity Register
  - suporta serviços de segurança dos equipamentos (terminais)
  - Inclui listas de equipamentos
  - white list (authorized)
  - gray list (under "observation")
  - black list (blocked)

Bandas GSM

- GSM 900: (GSM) – 900 MHz:
- 890-915 MHz (uplink) e 935-960 MHz(downlink)
- GSM 1800 (PCN - Personal Communication Network ou DCS 1800) –1800 MHz:
- 1710-1785 MHz (uplink) e 1805-1880 MHz (downlink)
- GSM 1900 (PCS - Personal Communication Services, PCS 1900, ou DCS 1900) – 1900 MHz:
- é a banda usada nos Estados Unidos e no Canadá para GSM
- 1850-1910 MHz (uplink) e 1930-1990 MHz (downlink)

Interface de rádio

Como já foi referido anteriormente, o principal foco do sistema GSM foi o de permitir que o maior número possível de usuários pudessem ser integrados. As interfaces e protocolos que usa devem ser, portanto, padronizados e flexíveis, de forma a poder incorporar elementos de diferentes fabricantes. Uma interface precisa prover os aspectos físicos dos meios de transmissão, o interfuncionamento e a implementação dos serviços e aplicações móveis entre os elementos da rede GSM.

Utiliza FDD (Frequency Division Dupplexing) e TDMA (Time Division Multiple Access). Cada banda (GSM) é dividida em 124 canais de 200 kHz (FDMA).

- A transmissão em cada banda de 200 kHz é efectuada em frames divididos em 8 time slots (TDMA).

- As frames são agrupadas em multiframes de 26 ou 51 frames.
- As multiframes são agrupadas em superframes de 26 ou 51 multiframes.
- As superframes são agrupadas em hyperframes de 2048 superframes.

Handover em GSM

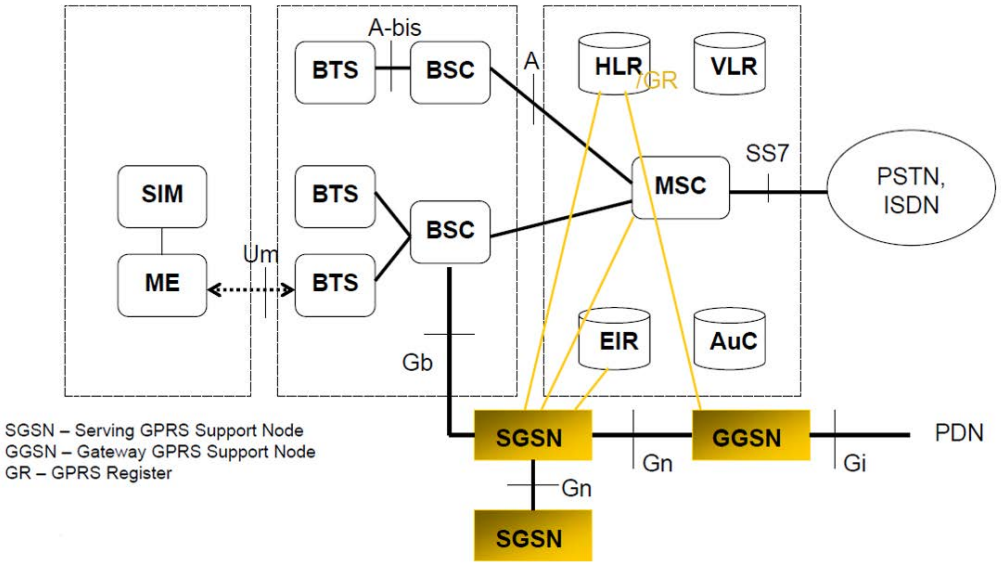
Handover (também designado de handoff) é o processo de comutação de uma chamada de voz de um canal físico para outro. Motivos que conduzem à necessidade de realizar handover:

- O utilizador (MS – mobile station) move-se e a qualidade do actual canal degrada-se
- O canal actual está a provocar demasiada interferência numa outra célula
- O tráfego numa célula é elevado e a capacidade da célula está próximo do seu limite.

GPRS - General Packet Radio Service

O GPRS foi introduzido na especificação GSM fase II. Proporciona um serviço de dados baseado em comutação de pacotes, mais orientado para as necessidades das aplicações da Internet (tráfego em burst). Suporta o conceito "always on": não há estabelecimento de ligações.

Arquitectura



Serviço de dados

Modos:

- PTP-CLNS (Point-To-Point ConnectionLess Network Service): equivalente ao IP
- PTP-CONS (Point-To-Point Connection Oriented Network Service): equivalente ao X.25

Taxas de transmissão

As taxas de transmissão disponíveis dependem do número de canais disponíveis (ou atribuídos pelo operador) e do esquema de codificação:

- esquemas de codificação: CS-1 a CS-4
- número de canais: 1 a 8

Exemplos:

- CS-1 + 1 canal = 9.05 kbps
- CS-4 + 1 canal = 21.4 kbps
- CS-1 + 8 canais = 72.4 kbps
- CS-4 + 8 canais = 171.2 kbps

É importante lembrar que, no nível de rede, a rede GPRS usa os protocolos da internet, TCP, UDP, IP, PPP, entre outros de interface com o computador.

Tecnologia EDGE

A tecnologia EDGE (Enhanced Data Rates for GSM Evolution) caracteriza a geração 2.75G, posterior à 2G ou à 2.5G.

Sua principal função é aumentar a eficiência do sistema GPRS, motivo pelo qual também é conhecida como GPRS Melhorado (Enhanced General Packet Radio Services – EGPRS).

As principais diferenças em relação à rede GPRS são :

- Protocolos de acesso à interface Um com novas facilidades;
- Modulação 8-PSK (8-state Phase Shift Keying);
- Novos procedimentos de codificação de canal.

Arquitectura EDGE

A rede EDGE é idêntica à GPRS, excepto pela interface aérea. Apenas a MS e a BTS sofrem mudanças com o sistema EDGE, portanto. Essas mudanças visam suportar, principalmente, a modulação 8-PSK e os novos tipos de codificação. A interface aérea EDGE suporta as interfaces GSM e GPRS.

Principais diferenças entre as tecnologias GSM, GPRS e EDGE

As principais diferenças entre essas fases da segunda geração de celulares está no transporte de dados e nas taxas de transmissão requeridas por cada um. A figura abaixo compara, resumidamente, GSM, GPRS e EDGE.

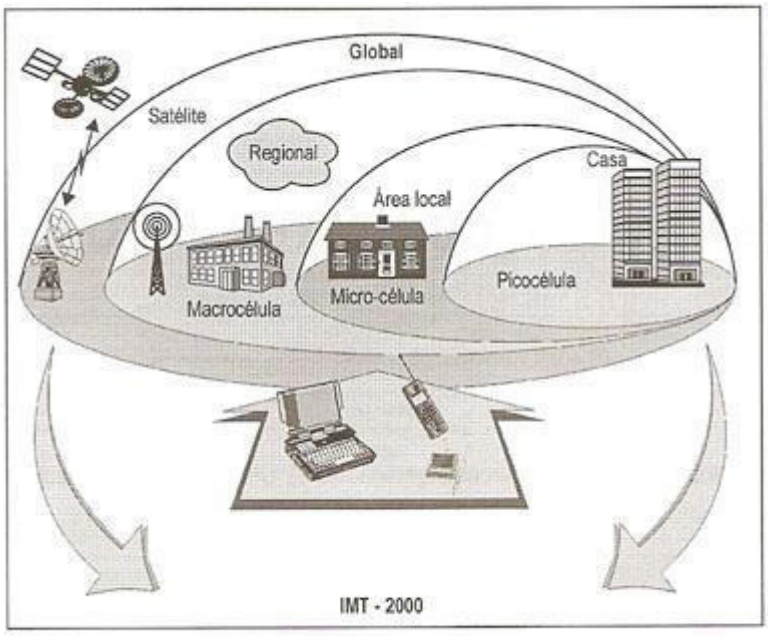
Tecnologia	Serviço	Taxa de transmissão máxima por ITC [kbits/s]	Taxa de transmissão máxima por quadro - 8 ITCs [kbits/s]
GSM	Voz	13	13
	Dados por comutação de circuito	14.4	14.4
GPRS	Voz	13	13
	Dados por comutação por pacotes	21,4	171,2
EDGE	Voz	13	13
	Dados por comutação por pacotes	59,2	473,6

Principais diferenças entre as tecnologias GSM, GPRS e EDGE.

UMTS (Universal Mobile Telecommunication System)

Em 1989, a União Internacional de Telecomunicações (ITU, em inglês) divulgou através de um documento a visão para os sistemas de celulares futuros, chamados de terceira geração, 3G. Essa visão chamou-se IMT-2000 (International Mobile Telephony 2000) e, após ser divulgada, deu início a uma corrida para que fosse projetado um sistema que atingisse às suas necessidades.

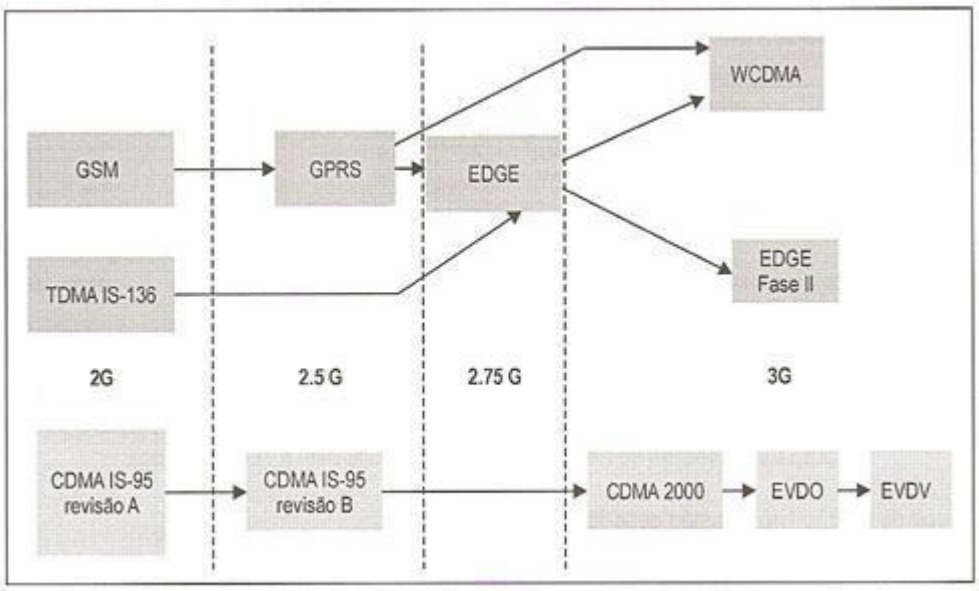
Um aspecto interessante do IMT-2000 é a divisão de ambientes para a operação do sistema, de forma hierárquica.



Ambientes do IMT-2000.

O IMT-2000 exigiu uma nova alocação do espectro de frequências. Diversas propostas foram então desenvolvidas para atender aos requisitos do IMT-2000. As propostas UTRA (Universal Terrestrial Radio Access) e WCDMA (Wideband CDMA) foram as selecionadas, junto com a CDMA2000. As propostas UTRA e WCDMA estão unificadas na mesma especificação, chamada UMTS (Universal Mobile Telecommunications System).

O objectivo era migrar os sistemas de celulares de segunda geração para os de terceira geração. O sistema GSM tem a evolução natural para UMTS, enquanto o sistema CDMA IS-95 evolui naturalmente para o CDMA 2000.



Evolução para as tecnologias 3G.

Arquitectura da rede UMTS

A Arquitetura UMTS é formada pelos seguintes elementos :

- Equipamento de usuário – (User Equipment – UE);
- Rede de suporte (Core Network – CN);
- Rede universal de acesso de RF terrestre (Universal Terrestrial Radio Access Network –UTRAN).

A arquitectura UMTS utiliza a mesma rede de suporte dos sistemas GPRS e EDGE, o que consiste numa estratégia de migração muito interessante, de fácil implementação.

A principal diferença entre esses sistemas está nos protocolos e interfaces da interface aérea.

Conclusão

Nesta actividade olhamos com detalhe algumas das tecnologias mais marcantes em comunicações móveis, a saber; GSM, GPRS, EDGE e UMTS. Procuramos estabelecer sua ligação e integração evolutiva. Vimos que as tecnologias mais recentes evoluem a partir das mais antigas.

Resumo da Unidade

Esta unidade teve por objectivo oferecer-lhe uma abordagem das características principais das tecnologias de sistemas de telefonia móvel GSM, GPRS, EDGE e UMTS. Para tanto, há a devida introdução teórica e histórica, visando prepará-lo para que possa entender aspectos mais profundos sobre os temas.

Os tópicos considerados mais importantes, como certas interfaces, modelos de arquitectura, entre outros, tiveram um nível maior de detalhamento, através de uma abordagem mais técnica, não dispensando por isso, novas pesquisas para a sua complementação.

Como deve ter percebido, os sistemas celulares possuem uma cadeia de evolução, na qual tecnologias mais recentes incrementam as já implantadas. Todas as tecnologias têm, portanto, aspectos em comum, que foram implementados nas tecnologias mais antigas e

Avaliação da Unidade

Verifique a sua compreensão!

Instruções

Tal como aconteceu com as outras unidades, agora que chegamos ao fim desta, precisamos de verificar o nível da sua aprendizagem. Para isso, é-lhe colocado um teste de dez questões, abarcando toda a matéria tratada nesta unidade. Procure respondê-las com precisão. Lembre-se de que sempre tem a possibilidade de voltar para trás e rever a unidade, se achar que alguma coisa não ficou bem clara. No final da prova encontrará um guião de correção, use-a para comparar as suas respostas e avaliar o nível da sua aprendizagem. Bom trabalho.

Critérios de Avaliação

A seguir vem a prova final desta unidade que acabas de abordar. A prova é composta por dois tipos de questões. O primeiro tipo é de perguntas abertas onde deve responder segundo a tua compreensão. O segundo tipo é de perguntas de múltipla escolha. Escolha aquela resposta que no seu entender é a mais acertada. Só existe uma resposta correcta. Bom trabalho.

Avaliação

Parte I

1. Caracterize o termo "Celular" no contexto das comunicações móveis.
2. O procedimento de handoff é iniciado quando a ERB detecta que o nível do sinal recebido da EM está abaixo do limiar permitido ao sistema. Que entende por handoff nas Comunicações Móveis.
3. Considere uma chamada originada na rede fixa e destinada a um utilizador GSM que se encontra em roaming. Explique como é que esta chamada é encaminhada para o utilizador móvel.
4. A ponte entre a 2ª geração de comunicações móveis e a 3ª geração (UMTS) é feita pela chamada "Geração 2.5" que como deve estar lembrado corresponde à introdução da tecnologia de pacotes ou GPRS em redes móveis claramente desenhadas para comutação de circuitos. Que entende por comutação de pacotes?
5. Numa rede celular de comunicações móveis, diga o que entende por sectorização das células e mostre as vantagens da aplicação desta técnica
6. Quais são os elementos fundamentais de uma rede de telecomunicações móveis?

Parte II (5.0 pontos)

1. Assinale o serviço que não é suportado por uma rede GSM.

    a. SMS

    b. Conexão a Internet via GPRS

    c. TV por assinatura

    d. Localização

2. Qual dos padrões abaixo não faz parte dos sistemas celulares de terceira geração (3G)?

    a. UMTS.

    b. GSM-EDGE.

    c. HSPA.

    d. CDMA 1xEV-DO.

3. Por meio de quais dispositivos uma operadora de celular sabe de quem cobrar as chamadas?

   - MIN e ESN
   - FVC e RVC
   - CDMA e TDMA

4. O IMSI (International Mobile Subscriber Identity), é formado por três campos. Assinale a resposta correcta.

   - Código móvel do país, Código da rede móvel, Código da rede Pública.
   - Código móvel do país, Código da rede móvel, Número de identificação móvel.
   - Código móvel do país, Código da rede móvel, Número de identificação do assinante móvel.

5. O que significa tecnologia 3G?

   - Três vezes mais espaço para armazenar dados.
   - Terceira geração tecnológica
   - Três pessoas falando ao mesmo tempo.

Questões	Sugestão de resposta	Pontuação
Q1	O termo celular refere-se ao facto de que uma área geográfica é dividida em várias áreas de cobertura geográfica, conhecidas como células. Cada célula contém uma estação base que consiste de uma torre e uma pequena construção que contém o equipamento de rádio que se comunica com estações móveis(enviando ou recebendo sinais) dentro da sua célula.	2.5
Q2	Comutação de uma chamada em andamento de uma ERB para outra quando a estação móvel cruza a fronteira entre as células. (i) terminal move-se para uma célula vizinha (ii) uma nova ERB passa a assegurar a comunicação. (iii) a ligação tem de ser mantida de forma transparente para o utilizador.	2.5

Q3	Roaming designa a capacidade de um usuário de uma rede em obter conectividade em áreas fora da localidade geográfica onde está registado, ou seja, obtendo conectividade através de uma outra rede onde é visitante. Para que seja possível utilizar um celular em roaming é preciso que a operadora, ou outra com a qual ela tem acordo de roaming, tenha cobertura neste local com tecnologia compatível a do seu Celular. O processo começa quando a EM verifica pelo FOCC que a ID do sistema não corresponde àquela em seu registo interno.	3.0
Q4	A comutação por pacotes não exige o estabelecimento de um circuito dedicado para a comunicação, o que implica menores custos com meios físicos. Este paradigma utiliza a ideia da segmentação de dados em partes Discretas compostas de cabeçalho (com bits de verificação de integridade) corpo e rodapé (onde é realizada a verificação cíclica de redundância), que são denominados pacotes.	2.5
Q5	A sectorização de células é usada para reduzir a interferência, uma vez que cada setor utiliza antenas direcionais e não interfere nos demais setores da célula.	1.5
Q6	Os elementos fundamentais de uma rede de telecomunicações móveis são as estações base (RBS) que efectuam a ligação via rádio entre o telefone móvel e a infra-estrutura da rede de comunicações móveis. Quando um telemóvel se liga a uma rede, para comunicar com a ERB mais próxima, utiliza sinais de radiofrequência (que geram os campos electromagnéticos). Cada ERB cobre uma pequena zona designada por célula, daí a ,designação também usada, de telefone celular. Assim, as comunicações móveis necessitam de um nº suficiente de ERB para garantir cobertura a vastas áreas Geográficas. cada estação fornece cobertura rádio apenas a uma área geográfica específica (uma célula).	3.0

Unidade 4. Segurança em Redes Móveis e sem Fios

Introdução à Unidade

Com a evolução e popularização dos sistemas de comunicação móvel, principalmente para acesso a serviços de dados, torna-se cada vez mais importante um olhar mais atento aos sistemas de segurança para estes usuários. Desde os sistemas analógicos, posteriormente GSM, passando pelo UMTS e mais recentemente com a quarta geração, o LTE, muitas modificações e evoluções ocorreram. Será que as redes móveis dispõem de sistemas suficientemente seguros? Quais são as vulnerabilidades em cada geração e como podemos nos precaver?

Com o intuito de chamar a sua atenção para estes aspectos, que infelizmente, muitos deles ainda estão em aberto, dedicamos esta última unidade. Nela não vai encontrar fórmulas prontas de segurança, mas sim, experiências e dicas de segurança em redes móveis.

Objetivos da Unidade

Após a conclusão desta unidade, deverá ser capaz de:

1. Descrever a segurança em um ambiente sem fio;
2. Descrever os tipos de ataques em uma rede Wi-Fi;
3. Descrever soluções de segurança sem fio.
4. Caracterizar o tipo de vulnerabilidade encontradas em sistemas de comunicações nas diferentes gerações tecnológicas.

Termos-chave

Autenticação: é o acto de estabelecer ou confirmar algo (ou alguém) como autêntico, isto é, que reivindica a autoria, proveniência ou a veracidade de alguma coisa.

Encriptação: é o processo de transformar informação (purotexto) usando um algoritmo (chamado cifra) de modo a impossibilitar a sua leitura a todos excepto aqueles que possuam uma identificação particular, geralmente referida como chave.

Vulnerabilidade: é uma fraqueza que permite que um atacante reduza a garantia da informação de um sistema. Vulnerabilidade é a interseção de três elementos: uma susceptibilidade ou falha do sistema, acesso do atacante à falha e a capacidade do atacante de explorar a falha.

SSID: é um código alfanumérico que identifica uma rede sem fio.

Actividades de Aprendizagem

Actividade 4.1 - Principais ameaças de segurança em redes móveis

[Especial agradecimento pelo material utilizado na elaboração desta actividade de aprendizagem aos estudantes Alisson Stadler de Paula, Marcos Artur Bressan e Takumi Abe do Programa de Pós Graduação em Redes e Segurança de Sistemas, Pontifícia Universidade Católica do Paraná, Brasil, 2013]

Introdução

Em pouco mais de uma década houve um crescimento extraordinário associado à telefonia móvel tanto em número de usuários quanto em tecnologia, que saiu da primeira para a quarta geração. Devido a esse fenômeno os aparelhos celulares mudaram o seu status, se tornando cada vez menos telefones e mais computadores, e, portanto ficando gradativamente mais suscetíveis as diversas formas de ataques. Um celular desprotegido associado a uma rede "insegura" pode resultar numa invasão muitíssimo onerosa à privacidade individual, possibilitando factos como adulteração de dados ou até mesmo um roubo via Internet Banking, por exemplo. Em outras palavras significa que um invasor pode ouvir suas chamadas, ler suas mensagens de texto, acompanhar sua actividade na internet e não obstante apontar sua localização geográfica.

Para que uma rede seja considerada minimamente segura em padrões internacionais, de acordo com a norma ISO IEC 17799 [17], ela deve seguir alguns preceitos básicos de segurança:

- **Confidencialidade**: Garante que o acesso às informações esteja ligado somente a entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação;

- **Integridade**: Garante que toda informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo mudanças, nascimento, manutenção e fim da informação; -
- **Disponibilidade**: Garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.
- **Autenticidade**: Garante que a informação foi produzida, modificada ou descartada por uma determinada pessoa física, órgão, entidade ou sistema com intuito de validar sua origem.

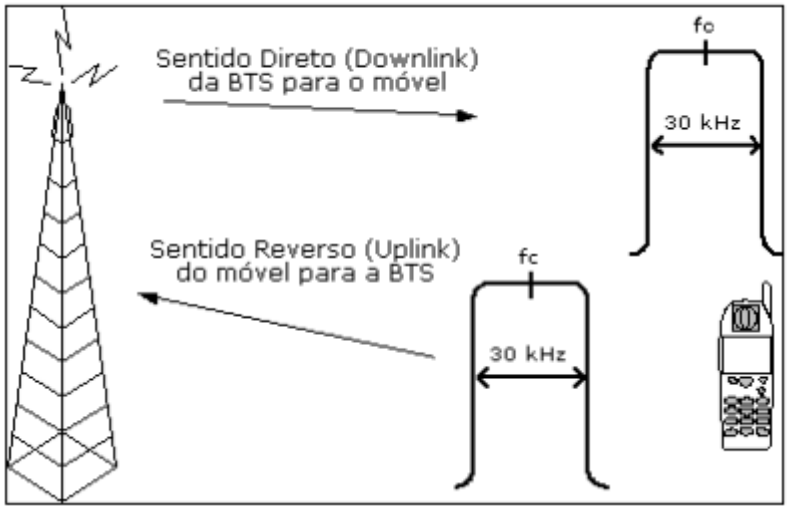
Os conceitos do quarteto acima não se referem apenas a sistemas computacionais, mas sim a todo e qualquer modelo de informações, dados e comunicações. Nesse contexto serão enfocados os seguintes tipos de ataques mais comuns em redes móveis:

- *Acesso não autorizado (Unauthorized Access)*: Se um método de autenticação não é propriamente aplicado ou é mal configurado, então um invasor pode ter acesso livre a rede e usar seus serviços mesmo não sendo autorizado para isso;
- *Obstrução do meio (Channel Jamming)*: É uma técnica usada pelos invasores cujo objectivo é destruir ou degradar o sinal da interface aérea, e dessa forma desabilitar o acesso dos usuários legítimos dessa rede deixando-os expostos a "outras" redes;
- *Negação de serviço (Denial of Service):* É causada pelo envio excessivo de dados na rede, mais do que ela pode suportar, deixando os usuários sem os recursos de rede disponíveis;
- *Espionagem (Eavesdropping):* Se o tráfego na interface aérea não for fortemente criptografado, um invasor pode espiar ou interceptar dados importantes ou ligações telefônicas confidenciais;
- *Mensagens Falsificadas (Message Forgery)*: Se o canal de comunicação não for suficientemente seguro, um invasor pode mudar o conteúdo das mensagens em ambas as direções sem ao menos que os reais receptores perceberem isso;
- *Ataque Invasor-no-meio (Man In The Middle Attack)*: Um atacante pode estar entre um telefone celular e um ponto de acesso da rede para interceptar mensagens;
- *Sequestro de sessão (Session Hijacking)*: Um usuário malicioso pode sequestrar uma sessão já estabelecida e actuar como um legítimo usuário de uma determinada base station.

Devido ao dinamismo da tecnologia e à natureza aérea de uma rede móvel, não há como oferecer qualquer tipo de "certeza de segurança definitiva" na solução destes problemas. Porém existem muitos métodos de minimizar ou em vários casos eliminar essas tentativas de quebra dos mecanismos de segurança das redes móveis.

Segurança em redes móveis 1G - AMPS

Tal como vimos na unidade III, o sistema AMPS (Advanced Mobile Phone System) desenvolvido pela Bell Labs em 1978 e padronizado pela ANSI EIA/TIA-553, foi a primeira geração de telefonia celular adotada em larga escala no mundo. Suas redes eram totalmente analógicas e somente transmitiam informação de voz usando canais de frequência separados para cada chamada. Tinha transmissão full-duplex e usava a faixa de frequência que variava de 800MHz a 900MHz, dependendo da localidade. O método de acesso aos canais de 30kHz (em cada sentido) era via FDMA (Frequency Division Multiple Access) utilizando modulação analógica FM. Isso trazia algumas desvantagens como exigência de largura de banda considerável para vários usuários simultâneos, linhas cruzadas (cross talking), interferências e principalmente problemas de segurança que serão mencionados na sequência.



Banda para Telefonia Celular: 850MHz e o sistema AMPS Fonte: TELECO

Esta topologia de rede não oferecia sistemas de criptografia e, portanto qualquer pessoa que coletasse os dados na interface aérea poderia facilmente decodificar os dados., ou um atacante com equipamentos especializados como um RF Scanner UHF que demodula sinais FM podia facilmente escutar ou reproduzir conversas particulares, quebrando o sigilo telefónico.

Principais vulnerabilidades do 1G

A fraca autenticação e a não existência de criptografia certamente eram os pontos mais fracos dessa rede. Mesmo para os padrões da época era relativamente fácil burlar os poucos mecanismos de confidencialidade, integridade e autenticidade adotados para o AMPS. Nota-se claramente que a rede era suscetível a quase todas as formas de ataque, como acesso não autorizado, espionagem, ataque invasor-no-meio, sequestro de sessão e clonagem.

Segurança em redes móveis 2G – GSM/GPRS/EDGE

A segunda geração de telefonia celular encontrou no GSM (Global System for Mobile Communications) o padrão de maior sucesso, sendo ainda hoje o sistema mais utilizado mundialmente. Foi com esta tecnologia que pela primeira vez dados começaram a ser transmitidos na interface aérea de forma digital. Além disso, novos serviços começaram a ser ofertados, como SMS (Short Message Service), transmissões de pacotes de dados, identificador de chamadas, além de melhor eficiência na utilização do espectro de frequências. Finalmente ganhou-se facilidade e flexibilidade de utilização de recursos convenientes para aperfeiçoar a segurança das informações, pois todo e qualquer dado transmitido tem criptografia digital. Essa nova forma de transmitir dados foi revolucionária em termos de segurança se comparado à tecnologia anterior, porém ainda não foi o suficiente para evitar outras formas de ataques.

Em termos de segurança, os primeiros elementos a serem pensados numa rede 2G foram a identificação e autenticação do utilizador, por isso foi criado o cartão SIM (Subscriber Identity Module). No SIM Card está registado o IMSI (International Mobile Subscriber Identity), que é único na rede e a partir dele que são iniciados os processos de segurança.

A rede GSM realiza o processo de autenticação do assinante através do SIM usando um mecanismo tipo desafio/resposta. Nas redes GPRS/EDGE, o processo é semelhante.

Principais avanços de segurança do 2G

Se comparado com os métodos das redes da geração anterior, nota-se uma significativa melhoria no processo de autenticação e confidencialidade dos utilizadores. Além do SIM Card agora também se utilizam os algoritmos A3/A8 junto ao AuC, e devido a isso a clonagem de telefones ficou reduzida a um valor quase inexpressivo. Outro avanço importante foi a adoção de algoritmos de cifragem A5.1, A5.2 e A5.3 na interface aérea, garantindo maior segurança das informações.

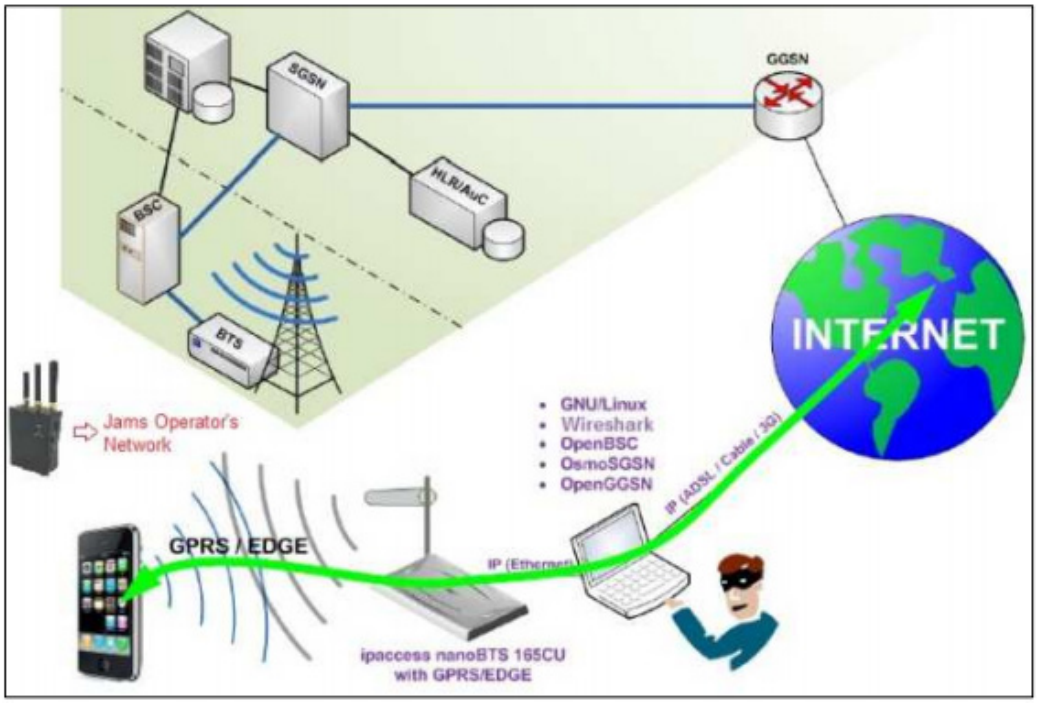
Principais vulnerabilidades do 2G

Com o passar do tempo todos os algoritmos de criptografia e autenticação mencionados acima acabaram se mostrando fracos e já foram quebrados, tendo no A5 os pontos de vulnerabilidade mais explorados.

Dentre os principais pontos fracos de uma rede GSM estão:

- Chaves de tamanho pequeno (64bits);
- Apenas o utilizador se autentica na rede e não vice-versa;
- Não possui verificação na integridade de dados;
- Transmissão de chaves de forma insegura, entre outros.

Diante dessas vulnerabilidades, mais uma vez a rede celular móvel se encontrou diante de problemas já enfrentados no passado, como acesso não autorizado, negação de serviço, espionagem, ataque invasor-no-meio, sequestro de sessão, etc.



Ataque prático contra comunicações móveis Fonte: [¨Paula, Bressan, Abe, 2013]

Resumo

Tal como se pode perceber do acima exposto, medidas de segurança em qualquer sistema tem uma validade limitada e obviamente que os sistemas de segurança das redes 1G e 2G já estão ultrapassados, permitindo os mais variados tipos de ataques. Com a evolução para os sistemas 3G muitas destas vulnerabilidades foram sanadas.

Actividade 4.2 - [Segurança em redes móveis 3G – UMTS]

[Especial agradecimento pelo material utilizado na elaboração desta actividade de aprendizagem aos estudantes Alisson Stadler de Paula, Marcos Artur Bressan e Takumi Abe do Programa de Pós Graduação em Redes e Segurança de Sistemas, Pontifícia Universidade Católica do Paraná, Brasil, 2013]

Introdução

Recordando a unidade III, podemos admitir que nas redes UMTS muitas características foram herdadas da rede GSM, toda a parte de Switching Core e Packet Core da rede foram mantidos, no entanto se diferenciam totalmente na parte de acesso (Radio Access).

Em termos de segurança o processo é idêntico ao das redes GSM/GPRS/EDGE e isso facilita bastante para que se tenha uma migração suave ou interoperabilidade entre redes 2G e 3G.

Para proteção dos dados na interface aérea, Pütz, Schmitz e Martin [25] demonstram que o UMTS adiciona como camada de segurança de proteção, o UEA (UMTS Encryption Algorithm), que possui uma grande vantagem sobre os modelos utilizados nas redes anteriores, pois ele não é secreto, fazendo com que sua força não esteja em seu desconhecimento e sim na sua própria robustez, tornando-se eficaz contra ataques de engenharia reversa.

Principais avanços do 3G

Com o uso do uSIM novas técnicas de autenticação se tornaram possíveis, e então, não mais 3 elementos são usados, mas 5 (RAND, XRES, Ck, Ik e AUTN). Além disso, o tamanho das chaves foi aumentado de 64 para 128bits, dificultando bastante ou até inviabilizando ataques por força bruta. Foi criada também uma camada de segurança, o UEA, e nela os algoritmos de autenticação, cifragem e integridade são aplicados. Para aumentar a confidencialidade, somente o algoritmo UEA1 (AES) é utilizado, por ser o mais forte. Através do algoritmo AKA (Authentication and Key Agreement) é feita a autenticação do terminal com a rede, assim como nos sistemas 2G, mas também a autenticação da rede ao terminal. Desta forma os ataques por falsa estação rádio base se tornam inviáveis.

Principais vulnerabilidades do 3G

Um dos tipos de ataque contra as redes 3G utiliza a técnica de estação rádio base falsa, porém como na rede 3G ocorre a autenticação mútua, faz-se necessário inibir o sinal 3G com o uso de bloqueadores de sinal para que o terminal busque uma outra rede, e desta forma a estação rádio base falsa, em 2G, poderá ser utilizada para o ataque. Ataques oriundos de interfaces IP, tais como negação de serviço - DOS, SYN-flood ou smurf, são possíveis, porém bastante controlados pelas ferramentas de segurança da rede de pacotes.

Segurança em redes móveis 4G - LTE

A 4ª geração (4G) dos sistemas de comunicação móvel teve como princípio de desenvolvimento ser totalmente IP, isto é, todos os elementos, com excepção do terminal, devem se comunicar por interfaces puramente IP. Com isso, várias técnicas de autenticação, integridade e confidencialidade já existentes e utilizadas nas redes IP são empregues no 4G, como por exemplo, o IPSec, o CMP (Certificate Management Protocol) e o TLS (Transport Layer Security).

Principais avanços do 4G

Todas as interfaces, excepto a de rádio, são IP e isto facilita e flexibiliza bastante a instalação e manutenção das redes. Os sistemas de autenticação e troca de chaves foram melhorados, se comparados com os sistemas aplicados às redes 2G e 3G, utilizando chaves HMAC-SHA-256. A criptografia utiliza vetores de autenticação incompatíveis com os utilizados em redes 3G e para se manter a compatibilidade dos usuários, o USIM deve verificar o bit de separação (separation bit). Os algoritmos utilizados são o AES e o SNOW 3G, que utilizam chaves de 128 bits, e com capacidade de processar chaves de 256 bits, num próximo release.

Cada vez mais os sistemas de comunicação móvel são utilizados para transmissão de dados e com isso alguns requisitos básicos de segurança precisam ser seguidos:

- A segurança em LTE deve oferecer pelo menos o mesmo nível de segurança que foi fornecido pelos serviços 3G;
- As medidas de segurança não devem afectar a conveniência do usuário;
- Deverão fornecer defesa de ataques vindos da Internet;
- As medidas de segurança devem ser compatíveis e permitir a transição com 3G.

Principais vulnerabilidades do 4G

Existem vulnerabilidades devido à operação conjunta com redes 2G e 3G e ataques oriundos das interfaces IP (negação de serviço - DOS, SYN-flood ou smurf). Assim como nas redes 3G, onde muitos usuários utilizam smart phones, ataques podem explorar vulnerabilidades dos sistemas operacionais através de códigos maliciosos escondidos em aplicativos, mensagens de texto ou mensagens multimídia.

Segurança em redes móveis 4G - WiMAX

Finalizado em 2001 e publicado em 2002, o padrão IEEE 802.16, especifica uma interface sem fio para redes metropolitanas (WMAN). Foi atribuído a este padrão o nome WiMAX (Worldwide Interoperability for Microwave) criado por um grupo de indústrias cujo objectivo é promover a compatibilidade e interoperabilidade entre equipamentos baseados no padrão IEEE 802.16.

Este padrão é similar ao padrão Wi-Fi (IEEE 802.11), que já é bastante difundido, porém agrega novos recursos, visando um melhor desempenho de comunicação permitindo velocidades de até 1 Gbps.

O padrão WiMAX objectiva estabelecer a parte final da infra-estrutura de conexão de banda larga (last mile) oferecendo conectividade para uso doméstico, empresarial e em hotspots, com possibilidade de taxa de transmissão de 1 a 75Mbps. Reconhecendo a importância da segurança, os grupos de trabalho destinados a especificação do padrão 802.16 desenvolveram vários mecanismos para proteção do prestador de serviço contra roubo de serviço e para proteger o cliente de divulgação de informações não autorizadas.

Principais avanços de segurança do WIMAX

O WiMAX utiliza o RSA (Rivest Shamir Adleman), o DES-CBC (Data Encryption Standard-Cipher Block Chaining) e AES-CCM (Advanced Encryption Standard in Counter with CBC-MAC) como algoritmos de criptografia. Para cifragem, o HMAC (Hashed Message Authentication Code) e o CMAC (Cipher-based Message Authentication Code) são utilizados. O padrão 802.16 ainda especifica que cada estação de assinante (Subscriber Station - SS) deve utilizar o certificado X.509 para identificá-lo. O uso de certificados X.509 torna difícil um atacante falsificar a identidade dos assinantes legítimos, oferecendo ampla proteção contra roubo de serviço.

Principais vulnerabilidades do WIMAX

Apesar das boas intenções para a segurança no WiMAX, existem vulnerabilidades exploradas principalmente por ataques por estações base falsas (Rogue Base Stations), ataques de negação de serviço (DoS Attacks), ataques man-in-the-middle e manipulação de rede com quadros de gerenciamento (Network manipulation with spoofed management frames).

Tabela Comparativa entre quê e quê?

	Confidencialidade	Integridade	Disponibilidade	Autenticidade	Tamanho das Chaves	Possíveis Proteções
1G (AMPS)	Não tem	Não tem	Não tem	ESN/MIN (fraco)	Não tem	Adoção de PIN Code
2G (GSM/EDGE)	A5.1, A5.2 e A5.3.	Não tem	Não tem	Triplets para autenticar o usuário apenas.	64 bits	Adoção da cifragem A5.3
3G (UMTS)	UEA1 ou UEA2 (f8)	UIA1 ou UIA2 (f9)	Não tem	Quintuplets e autenticação mútua	128 bits	Fixar o terminal para operar somente em redes 3G
4G (LTE)	EEA1 (AES) ou EEA2 (SNOW)	EIA1 (AES) ou EIA2 (SNOW)	Não tem	Quintuplets e autenticação mútua	128/256 bits	Cuidados na camada de aplicação e emprego de IPSEC entre a BTS e Core
4G (WiMAX)	RSA, DES-CBC ou AES-CCM	CBC-MAC	Não tem	Certificado X.509	160 bits	Cuidados na camada de aplicação e emprego de EAP

Conclusão

Com a evolução das tecnologias nota-se claramente o emprego de técnicas cada vez mais elaboradas para prevenção de ataques e aumento do nível de segurança em redes móveis. No entando, todas as tecnologias têm vulnerabilidades que podem ser exploradas, com maior ou menor complexidade. As redes de primeira geração praticamente não possuem dispositivos de segurança, e que na segunda geração ganharam maior atenção dos desenvolvedores, criando sistemas de autenticação e confidencialidade, até então inexistentes. As redes 3G trouxeram técnicas de integridade além de avanços nos quesitos de segurança já existentes, como o aumento do tamanho das chaves de segurança para 128 bits. Atualmente as redes de quarta geração, predominantemente baseadas em IP, agregam técnicas de segurança até então utilizadas somente no core da rede.

Detalhes da atividade

[Mais uma sessão de estudo chega ao fim, no qual foram abordados conceitos relativos à Segurança nas redes 3G e 4G. Á semelhança das outras sessões, esta também culmina com uma prova como forma de verificar a sua aprendizagem. São seis questões relacionadas com as temáticas abordadas que te são colocadas. Responda-as com calma e no fim compare as suas respostas com as sugeridas no material de estudo.]

Avaliação

1. Caracterize o padrão IEEE 802.16.
2. Qual é a origem das principais vulnerabilidades do 4G ?
3. Fale da Segurança em redes móveis 4G – LTE.

Sugestões de respostas

Questão	Sugestão de Resposta
Q1	O padrão IEEE 802.16, especifica uma interface sem fio para redes metropolitanas (WMAN). Foi atribuído a este padrão o nome WiMAX. Permite velocidades de até 1 Gbps. objectiva estabelecer a parte final da infra-estrutura de conexão de banda larga (last mile) oferecendo conectividade para uso doméstico, empresarial e em hotspots.
Q2	Existem vulnerabilidades devido à operação conjunta com redes 2G e 3G e ataques oriundos das interfaces IP (negação de serviço - DOS, SYN-flood ou smurf).

Q3	A 4ª geração teve como princípio de desenvolvimento ser totalmente IP, isto é, todos os elementos, com excepção do terminal, devem se comunicar por interfaces puramente IP. Com isso, várias técnicas de autenticação, integridade e confidencialidade já existentes e utilizadas nas redes IP são empregues no 4G, como por exemplo, o IPSec, o CMP (Certificate Management Protocol) e o TLS (Transport Layer Security).

Actividade 4.3 - [Segurança em redes Wi-Fi (802.11)]

Introdução

As comunicações sem fios são mais vulneráveis do que as com fio, porque o acesso ao meio partilhado é mais simples. Basta arranjar um dispositivo com capacidade de comunicar sem fios para ter acesso a informações transmitida por um outro dispositivo. Para reduzir a possibilidade de ataques ao WLAN, podem utilizar-se os seguintes métodos:

- Autenticação
- Encriptação
- Ferramentas de detecção de intrusos

Autenticação

É usada para impedir que um dispositivo externo à rede troque informação com o ponto de acesso. Para o efeito é usada uma palavra-chave apenas conhecida pelo cliente e pelo ponto de acesso para determinar a autenticidade dos dados. Também do lado do utilizador, a autenticação é usada por forma a evitar uma ligação a um access point externo à rede pretendida. A palavra-chave utilizada nas transmissões nunca é enviada nas comunicações para evitar que o atacante a consiga capturar, As normas IEEE consideram dois tipos de autenticação:

- Com chave partilhada
- Com chave aberta

Chave Partilhada

Baseia-se num mecanismo de pergunta/resposta. Após ter identificado um Access Point (AP) cujas características permitam estabelecer uma ligação, o cliente inicia o processo de autenticação. Para tal, envia uma trama de resposta ao AP. Este, por sua vez, responde com um pacote de desafio (challenge) que consiste em dados não encriptados. Ao receber o desafio, o cliente encripta os dados com a sua chave e envia-os de volta ao AP. Este verifica se os dados estão correctamente encriptados e envia de volta uma resposta de autenticação. Se assim for, o cliente tem acesso à rede sem fios.

Chave Aberta

Após ter identificado um AP compatível, o cliente envia um pedido de autenticação, mas o AP não responde com um desafio, assumindo que o cliente pode comunicar. No caso de usar um método de encriptação, o cliente encripta os dados enviados para o AP. Este desencripta com a sua chave. Caso as chaves sejam diferentes, o processo falha.

Encriptação

É usada para esconder a mensagem. Mesmo que o atacante apanhe a mensagem, não a consegue ler sem a palavra-chave que a desencripta. Tal como na autenticação, é usada uma palavra-chave que nunca é transmitida.

IDS – Intrusion Detectetion System

Chama-se IDS (Intrusion Detection System) a um mecanismo que ouve o tráfego na rede de maneira furtiva, para localizar actividades anormais ou suspeitas e permitindo assim ter uma acção de prevenção sobre os riscos de intrusão.

Existem duas grandes famílias distintas de IDS:

- Os N-IDS (Network Based Intrusion Detection System), asseguram a segurança a nível da rede.
- Os H-IDS (Host Based Intrusion Detection System),asseguram a segurança a nível dos hóspedes.

O N-IDS constitui um sistema capaz de controlar os pacotes que circulam numa ou várias ligação(s) de rede, com o objectivo de descobrir se um acto malicioso ou anormal tem lugar.

Geralmente, o H-IDS analisa informações específicas nos diários de registos (syslogs, messages, lastlog, wtmp…) e também captura os pacotes redes que entram/saem do hóspede, para detectar sinais de intrusões (Recusa de Serviços, de Backdoors, cavalos de troia, tentativas de acesso não - autorizados, execução de códigos maliciosos, ataques por profusão de buffeurs…).

Portanto, o sistema de detecção de intrusos consiste na utilização de aplicações de detecção de intrusos.

WEP: Wired Equivalent Privacy

O algoritmo de segurança mais usado do mundo foi criado em 1999 e é compatível com praticamente todos os dispositivos WiFi disponíveis no mercado. Justamente por ser tão popular, é também o mais sujeito a falhas de segurança e o que possui mais buracos conhecidos.

O padrão WEP se torna mais inseguro à medida que o poder de processamento dos computadores aumenta. Por ser um sistema de segurança de 128 bits (factor que define os caracteres possíveis, ou seja, o número máximo de combinações de senha), é possível descobrir a palavra-passe de uma rede WiFi desse tipo em poucos minutos por meio de um software de ataques.

O WEP procura garantir a confidencialidade, a integridade e a autencidade das mensagens.

- A confidencialidade no WEP é baseada em mecanismos de encriptação.
- A integridade é feita com um mecanismo de verificação de sequência
  - Para garantir a integridade, o WEP usa um valor de hash designado valor de verificação de integridade (ICV – Integrity Check Value)
  - A trama e o ICV são depois encriptados para garantir a confidencialidade

A autenticação é realizada por partilha de chaves.

Trama WEP

O WEP usa uma chave de 40 bits que é combinada com 24 bits adicionais especificados na trama (IV – Inicialization Vector), formando uma chave de 64 bits. Considerando que 40 bits era muito pouco para garantir a segurança, muitos fabricantes optaram por considerar uma chave de 128 bits. Para garantir mais alguma segurança, o WEP usa até quatro chaves por defeito (default keys). A informação relativa ao processo de encriptação é incluída no campo da trama destinado aos dados da trama.

Formato da trama WEP

Principais Problemas do WEP

Chaves Estáticas

As chaves são configuradas manualmente no cliente e no AP. Uma alteração das senhas implica uma deslocação a todos os clientes e APs para a respectiva alteração das chaves.

Chaves Pequenas

As chaves usam valores de apenas 40 bits (ou 128). Devido a isto e ao facto das chaves não serem alteradas, é possível ao atacante determinar a senha em tempo útil.

O WEP é assim considerado um mecanismo de segurança de baixa protecção.

SSID – Service Set ID

- SSID como mecanismo de segurança
- Para comunicar com um AP é preciso conhecer o SSID

O processo começa com os APs a enviarem uma trama (beacon) com informação de configuração, onde se inclui o seu SSID. O cliente liga-se ao AP usando o SSID respectivo. Após uma fase inicial em que dá a conhecer o seu SSID, o AP deixa de enviar tramas com esta informação.

Norma 802.1x

O 802.1x é usado para autenticação em redes 802, o que significa que não é exclusivo das comunicações sem fios

A arquitectura da autenticação do 802.1x inclui três componentes principais:

Arquitectura 802.1x

Cliente (Supplicant)

O cliente no 802.1x (designado supplicant) é aquele que tenta aceder aos recursos da rede.

Autenticador

Não tem qualquer informação de autenticação, sendo apenas um intermediário entre o supplicant e o authentication server.

O cliente e o autenticador são designados "Entidades de Autenticação do Porto" (PAE – Porto Authentication Entity).

Sempre que um cliente tem acesso à rede após autenticação diz-se que os seus portos se encontram no estado autorizado. Caso contrário, estão no estado não autorizado.

A comunicação entre o cliente e o autenticador faz-se à custa do protocolo EAPOL (EAP over LAN). A comunicação entre o autenticador e o servidor de autenticação faz-se com o protocolo RADIUS (Remote Authentication Dial-In User Service).

EAPOL - (EAP over LAN)

O EAPOL é uma extensão às tramas do protocolo EAP. Na fase de autenticação, apenas as tramas EAPOL são permitidas entre o cliente e o autenticador. As tramas EAPOL podem ser de vários tipos:

- EAPOL – Packet: trama usada na comunicação de tramas EAP;
- EAPOL – Start: trama usada para iniciar uma autenticação 802.1x;
- EAPOL – Logoff: trama usada para terminar uma autenticação 802.1x;
- EAPOL – Key: trama usada para trocar informação sobre as chaves;
- EAPOL – Encapsulated-ASF-Alert: trama usada na comunicação de informação SNMP.

RADIUS - Remote Authentication Dial-In User Service

´RADIUS é um protocolo de autenticação, autorização e anotação (AAA) «RFC 2865 e 2866». O Protocolo consiste na criação de uma túnel encriptado por onde é enviada informação AAA.

Vantagem do RADIUS:

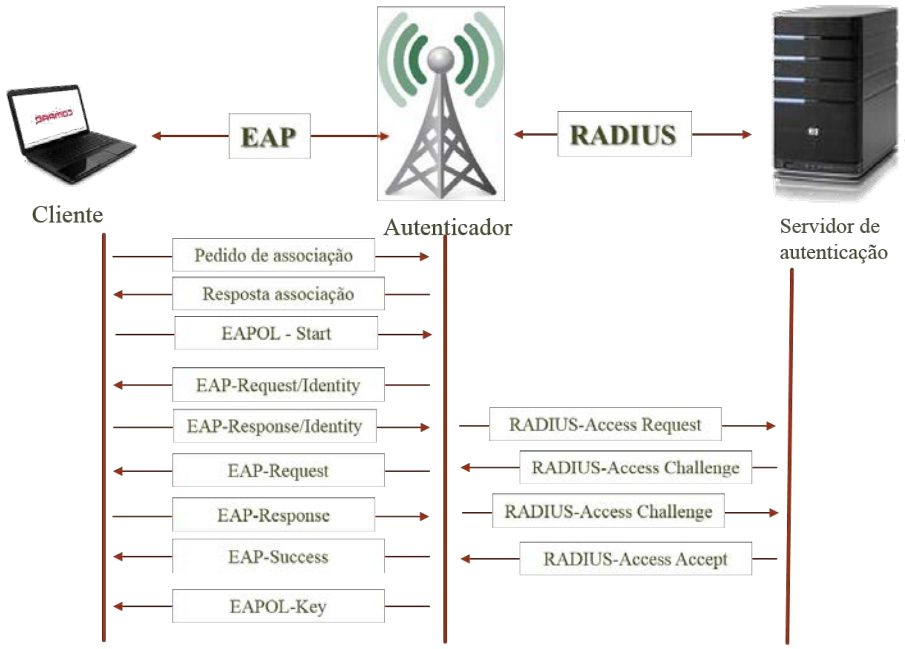
- Centralização do processo de autenticação com recurso a uma base de dados dos users e às respectivas senhas.

Pacotes associados ao protocolo RADIUS:

- Access-Report: inicia um processo de autenticação com RADIUS
- Access-Accept: indica que a autenticação enviada pelo cliente é válida
- Access-Reject: indica que a autenticação enviada não é válida
- Access-Challenge: usado para enviar um desafio ao cliente RADIUS de modo a que este apresente as suas credenciais de autenticação.

A sequência de mensagens necessárias à autenticação de um cliente só começa após se estabelecer a associação entre o cliente e a AP. No âmbito do 802.1x, a associação criada é designada "Porto lógico". Criada a associação, inicia-se o processo de autenticação:

Sequência de sms do processo de autenticação 802.1x



Sequência de operações

A sequência de operações correspondente a uma autenticação com sucesso é a seguinte:

- Após estabelecer a associação, dá-se início ao processo de autenticação com uma sms EAPOL-Start;
- Em seguida, o autenticador faz um pedido de identidade ao cliente (EP-Request/ Identity);
- O cliente responde ao pedido de identidade;
- O autenticador reencaminha a resposta do cliente para o server RADIUS;
- O server RADIUS responde com um pedido de desafio que é reencaminhado para o cliente através de uma trama EAP-Request;
- O cliente responde (EAP-Response)
- A resposta é enviada ao server RADIUS na forma de um pacote RADIUS-Access-Request;
- O server RADIUS responde a aceitar a autenticação (RADIUS-Access-Accept);
- A resposta do server RADIUS é enviada ao cliente na forma de uma sms EAP-Success.

A partir daqui, o cliente está autenticado e pode começar a transmitir através do AP.

EAP – Extensible Authentication Protocol

O EAP é um protocolo de autenticação de acesso a uma rede. O EAP deveria ser suficientemente flexível para permitir diferentes métodos de autenticação. O EAP foi criado na sequência dos protocolos de autenticação PAP e CHAP usados no protocolo PPP que tinham deficiências de segurança. A trama EAP é formada pelos campos:

Formato da trama EAP

Código

Identifica o tipo de pacote EAP, que pode ser um de quatro tipos:

- Request: faz um pedido para iniciar o processo de autenticação;
- Response: indica que o pedido foi aceite;
- Success: indica que a autenticação teve sucesso;
- Failure: indica que a autenticação falhou.

Identificador

Identifica os pedidos e as respostas

No caso em que existem múltiplos clientes a tentarem autenticar-se é necessário identifica-los diferencialmente.

Tamanho

Indica o tamanho da trama EAP, incluindo todos os campos

Dados

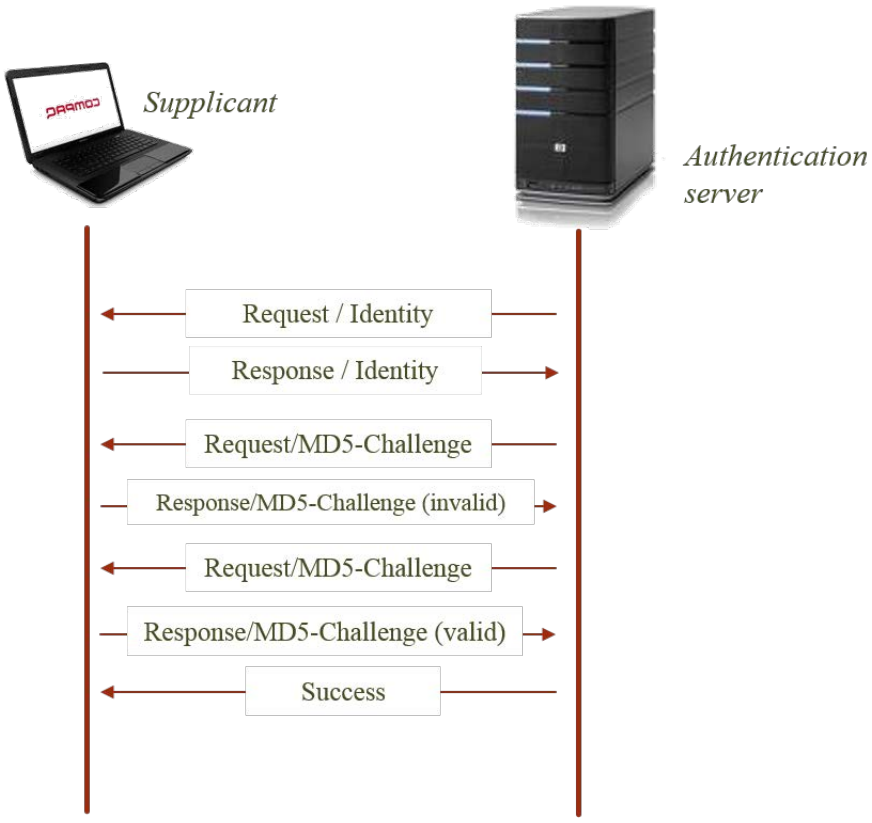
Contém informação associada ao tipo de trama.

Tipo

Identifica a estrutura das tramas EAP Request e response. É neste campo que se identificam os protocolos de autenticação. Os primeiros quatro códigos são usados para identificar tramas EAP do tipo:

1. Identity: usado para interrogar a identidade do cliente:
2. Notification: é usado para notificar ou pedir ao cliente que execute uma determinada acção;
3. NAK: usado para informar o cliente de que o tipo de autenticação não é válido;
4. MD5-Challenge: os restantes tipos são usados para identificar o método de autenticação.

Exemplo de Autenticação EAP



- O exemplo considera um caso em que é feito um pedido com MD5 e o cliente envia uma resposta inválida;
- Depois, o autenticador volta a fazer o pedido MD5, a que o cliente responde correctamente;
- O processo termina com uma trama EAP de sucesso.

WPA – Wi-Fi Protected Access

O aparecimento do WPA foi uma consequência da demora do IEEE em produzir uma norma de segurança (802.11i) que resolvesse os problemas do WEP. Então, a Wi-Fi Alliance decidiu criar um subconjunto do 802.11i designado WPA.

O WPA:

A autenticação pode ser feita com EAP, utilizando o 802.1x e um servidor RADIUS, ou autenticação de dispositivo com chaves partilhadas;

É usado o mecanismo de troca de chaves dinâmicas (TKIP – Temporal Key Integrity Protocol)

O TKIP gera novas chaves para cada pacote;

A chave inicial é gerada durante o processo de autenticação, com base no endereço MAC do emissor;

Depois por cada pacote enviado é gerada uma nova chave.

Norma 802.11i

No 802.11i uma comunicação segura é feita em cinco passos principais:

1. Negociação sobre a política de segurança a utilizar;
2. Autenticação com 802.1x;
3. Cálculo da chave e distribuição da mesma;
4. Autenticação num único AP com o método PKC (Proactive Key Caching)
5. Confidencialidade e integridade dos dados com RSNA (Robust Security Network Association)

Conclusão

Quando o WEP saiu de circulação, o WPA entrou em seu lugar como o protocolo-padrão da indústria. Adotado formalmente em 2003, a novidade trazia encriptação 256 bits e uma segurança muito maior para as redes. Além disso, sistemas de análise de pacotes – para verificar alterações e invasões – e outras ferramentas foram implementadas para melhorar a segurança.

O problema aqui é que a arquitetura WPA foi produzida de forma a não tornar os dispositivos WEP obsoletos, e sim actualizáveis. Com isso, uma série de elementos do protocolo antigo foi reaproveitada e, com ela, diversos dos problemas do antecessor também acabaram presentes na nova versão.

WPA2: Wi-Fi Protected Access II

O sistema-padrão actual e também o mais seguro, foi implementado pela Wi-Fi Alliance em 2006. A diferença aqui é a maneira como o sistema lida com senhas e algoritmos, excluindo completamente a possibilidade de um ataque de força bruta. Sendo assim, esse é o tipo mais seguro da actualidade. Segundo alguns especialistas, o risco de intrusões para usuários domésticos com WPA2 é praticamente zero.

Isso se deve a duas outras tecnologias. O AES (Advanced Encryption Standard), um novo padrão para a segurança das informações, e o CCMP (Counter Cipher Mode), um mecanismo de encriptação que protege os dados que passam pela rede. O WPA2 é tão complexo que muitos dispositivos, mesmo recentes, não são compatíveis com ele.

Detalhes da atividade

[Terminamos assim a terceira lição desta unidade e, à semelhança das anteriores lições, mais abaixo segue uma série de questões que deverás responder como forma de verificares o teu nível de aprendizagem. Faça-o com calma e evite consultar as respostas antes de terminares.]

Resumo da Unidade

Na unidade que agora termina discutimos questões de segurança em redes de comunicação móvel. Começamos por olhar as vulnerabilidades da tecnologia 1G, como estas foram sendo resolvidas, passamos para a segurança na tecnologia 2G, vimos como foram introduzidas melhorias nos esquemas trazidos de 1G. Depois olhamos para a tecnologia 3G e aqui sublinhamos os esforços feitos para tornar estas tecnologias o mais seguro possível. Olhamos as tecnologias 4G com a mesma intenção e por fim detivemo-nos nas redes Wifi. Aqui descrevemos também várias técnicas de segurança.

Avaliação da Unidade

Verifique a sua compreensão!

[Avaliação Final do Curso]

Instruções

De cada uma das três actividades de aprendizagem que teve nesta unidade, serão te colocadas três questões que vão compor a sua avaliação final. Algumas dessas questões provavelmente já encontrou na avaliação da respectiva actividade, nesse caso, será uma espécie de consolidação. Leia com atenção antes de responder, caso precise de consultar, não receie, volte à respectiva unidade, releia a secção ou toda a subunidade até ter a certeza de que está tudo claro para si, e só depois é que retoma a prova. Bom trabalho.]

Critérios de Avaliação

[A prova é composta por nove questões, valendo cada uma, conforme a sua complexidade e exigência um determinado peso (tabela abaixo) numa escala de zero a vinte valores. A mesma tabela abaixo serve de guião de correção, então no final da prova deverás comparar as tuas respostas com as sugeridas no guião e atribuir-se a pontuação. Caso não consigas obter a pontuação igual ou superior a 18 valores, aconselhamos que repita a aprendizagem.]

Avaliação

1. Quais são os diversos métodos de segurança de rede sem fio?
2. Caracterize a Autenticação 802.1x
3. Suponha que um seu amigo estava montando uma rede sem fios no seu serviço. Aproxima-se de ti solicitando conselho sobre o método de segurança a implementar. Qual seria sua recomendação?
4. O padrão IEEE 802.11 especifica dois métodos de autenticação: Autenticação de sistema aberto e autenticação de chave compartilhada. Caracterize a autenticação de sistema aberto.
5. Qual é a importância da Autenticação?
6. Na configuração de um AP, porquê se recomenda desabilitar a opção de "broadcast SSID" ?
7. Com o intuito de fornecer aos usuários de redes sem fio um nível de segurança comparável a da redes cabeadas, o WEP define três objetivos principais a serem atingidos. Confidencialidade – Autenticidade e Integridade. Caracterize cada um destes conceitos.
8. Suponha que seu amigo é administrador da rede sem fios da empresa onde trabalha e que está com problemas sérios de segurança. Indique cinco medidas de segurança que ele deve tomar.
9. Explique o conceito de Vulnerabilidade em sistemas de redes.
10. Como é que estão a ser resolvidas as vulnerabilidades dos sistemas 3G?

Guião de correção e pontuação

Questão	Sugestão da resposta	Pontuação
Q1	· WPA (Wi-Fi Protected Access) e WPA2 · Wired Equivalent Privacy (WEP) · Autenticação 802.1X	2.5
Q2	A autenticação 802.1X pode ajudar a aumentar a segurança de redes sem fio 802.11 e redes Ethernet com fio. A 802.1X usa um servidor de autenticação para validar usuários e fornecer acesso de rede. Em redes sem fio, a 802.1X pode funcionar com chaves WPA, WPA2 ou WEP. Esse tipo de autenticação normalmente é usado na conexão com uma rede de local de trabalho	2.5
Q3	Recomendamos o uso do WPA2, se possível. Não recomendamos o uso do WEP. O WPA e o WPA2 são mais seguros. Se o WPA e o WPA2 não funcionarem, recomendamos a troca do adaptador de rede por um que funcione com WPA e WPA2.	2.0
Q4	É o método padrão usado nos equipamentos wireless. Este método de autenticação é baseado no SSID, ou seja basta que a estação e o AP tenham o mesmo SSID para que a autenticação ocorra.	1.0
Q5	Impedir que um dispositivo externo à rede troque informação com o ponto de acesso (AP)	1.0
Q6	Desabilitando o “broadcast SSID” aumenta a segurança da rede. Quando o “broadcast SSID” está habilitado o ponto de acesso periodicamente envia o SSID da rede permitindo que outros clientes possam conectar-se à rede. Como o SSID pode ser extraído do pacote transmitido através da técnica de “sniffing” ele não oferece uma boa segurança para a rede.	1.0

Q7	Confidencialidade - significa simplesmente que o WEP deve ser capaz de evitar que uma pessoa não autorizada, não possa sequer compreender as mensagens que estão trafegando pela rede; Autenticidade – significa garantir que um usuário é quem ele afirma ser. O WEP, então, deve implementar um controle de acesso à infra-estrutura da rede sem fio, de forma que haja garantias de que o usuário que está se comunicando é um usuário legítimo da rede e não um invasor tentando se passar por usuário legítimo Integridade - O WEP implementa uma função chamada de "checksum" para que o conteúdo da mensagem transmitida seja verificado ao chegar ao destinatário, se o valor calculado no destinatário for igual ao valor do "checksum" então os dados foram mantidos inalterados ao longo da transmissão.	1.5
Q8	1. Mudar constantemente a senha dos Aps 2. Usar o mais alto nível de WEP/WPA (WPA2/802.1i preferivel) 3. Autenticar os users com protocolos como 802.1x, Radius, EAP. Estes protocolos suportam autenticação que inclui certificados digitais, usuários e senhas, tokens seguros, etc. 4. Criptografe o trafego sem fio usando uma VPN. 5. Verifique sempre se o firmware e drivers estão actualizados, actuelize-os se necessário, mantenha-se alerto as evoluções.	1.0
Q9	Vulnerabilidade é a interseção de três elementos: uma susceptibilidade ou falha do sistema, acesso do atacante à falha e a capacidade do atacante de explorar a falha.	1.5
Q10	Um dos tipos de ataque contra as redes 3G utiliza a técnica de estação rádio base falsa ….	1.0

Leituras e outros Recursos

As leituras e outros recursos desta unidade encontram-se na lista de Leituras e Outros Recursos do curso.

Cabianca, L. A.: Bulhman, H.J.: Redes LAN/MAN Wireless III: Aplicação do Padrão 802.11. 2006

Referências do Curso

1. Vestias, Mario, Redes Cisco para Profissionais, 4ª ed., FCA, 2009
2. Zuquete, A.: Segurança em Redes Informáticas, 2ªed., FCA, 2009
3. Paula, A.S.: Segurança em Redes Móveis. PUC Paraná, 2013
4. AREIAS, Gonçalo Menezes. Wireless IP, Universidade do Minho, 1999.
5. MATEUS, Geraldo Robson, Loureiro, Antonio Alfredo, Introdução à Computação Móvel, 11a Escola de Computação, Rio de Janeiro, 1998.
6. Boavida, F., Bernardes, M., Vapi, P.: Administração de Redes Informáticas, 2ª Edição FCA, 2011.
7. Manual ITED – Prescrições e Especificações Técnicas das Infraestruturas de Telecomunicações em Edificios, ANACOM – Autoridade Nacional de Comunicações, 2009.
8. Monteiro, E., Boavida, F.: Engenharia de Redes Informáticas, 10ª Edição, FCA, 2011.
9. Gouveia, J., Magalhães, A.: Redes de Computadores, 10ª edição, FCA, 2013.
10. Ericksson, ―WiMAX tecnologia de banda larga‖, in Workshop WiMAX – Desafios e Oportunidades, ISEL, Lisboa, Portugal, 13 de Dezembro de 2006.

Sede da Universidade Virtual africana

The African Virtual University
Headquarters

Cape Office Park

Ring Road Kilimani

PO Box 25405-00603

Nairobi, Kenya

Tel: +254 20 25283333

contact@avu.org

oer@avu.org

Escritório Regional da Universidade Virtual Africana em Dakar

Université Virtuelle Africaine

Bureau Régional de l'Afrique de l'Ouest

Sicap Liberté VI Extension

Villa No.8 VDN

B.P. 50609 Dakar, Sénégal

Tel: +221 338670324

bureauregional@avu.org