INFORMAÇÃO, CODIFICAÇÃO E SEGURANÇA DE REDES

Marcelo Sampaio de Alencar


COPIA NÃO AUTORIZADA É CRIME
ABDR
ASSOCIAÇÃO BRASILEIRA DE DIREITOS REPROGRÁFICOS
RESPEITE O DIREITO AUTORAL

INFORMAÇÃO, CODIFICAÇÃO E SEGURANÇA DE REDES

Marcelo Sampaio de Alencar

ISBN: 978-85-352-8184-2

Copidesque: Wilton Fernandes Palha
Revisão tipográfica: Adriana Patricio

Elsevier Editora Ltda.
Conhecimento sem Fronteiras
Rua Sete de Setembro, 111 – 16º andar
20050-006 – Centro – Rio de Janeiro – RJ

Rua Quintana, 753 – 8º andar
04569-011 – Brooklin – São Paulo – SP

Serviço de Atendimento ao Cliente
0800 026 53 40
atendimento1@elsevier.com

Consulte nosso catálogo completo, os últimos lançamentos e os serviços exclusivos no site www.elsevier.com.br

NOTA

Muito zelo e técnica foram empregados na edição desta obra. No entanto, podem ocorrer erros de digitação, impressão ou dúvida conceitual. Em qualquer das hipóteses, solicitamos a comunicação ao nosso serviço de Atendimento ao Cliente para que possamos esclarecer ou encaminhar a questão. Para todos os efeitos legais, nem a editora, nem os autores, nem os editores, nem os tradutores, nem os revisores ou colaboradores, assumem qualquer responsabilidade por qualquer efeito danoso e/ou malefício a pessoas ou propriedades envolvendo responsabilidade, negligência etc. de produtos, ou advindos de qualquer uso ou emprego de quaisquer métodos, produtos, instruções ou ideias contidos no material aqui publicado.

A Editora

CIP-BRASIL. CATALOGAÇÃO-NA-FONTE
SINDICATO NACIONAL DOS EDITORES DE LIVROS, RJ

xxxx Alencar, Marcelo Sampaio de

Informação, Codificação e Segurança de Redes
/ Marcelo Sampaio de Alencar. - 1. ed. - Rio de Janeiro: Elsevier, 2015.
: il. ; 24 cm.

ISBN 978-85-352-8184-2

1. Tema 1. 2. Tema 2. I. Autor 3. II. Título.

xx-xxxxx CDD: xxx.xxxx
CDU: xxx.x

Dedico esta obra aos meu filhos, Thiago, Raphael e Marcella, razão de minha vida e existência futura.

Marcelo Sampaio de Alencar

Apresentação da Série SBrT/Elsevier

Ao longo dos anos a Sociedade Brasileira de Telecomunicações (SBrT), instituição sem fins lucrativos, promove a difusão do conhecimento na área de telecomunicações no Brasil. Nesse sentido, a SBrT realiza anualmente o Simpósio Brasileiro de Telecomunicações e, a intervalos de quatro anos, o *International Telecommunications Symposium*.

Esses eventos são oportunidades de divulgação e de fortalecimento da pesquisa brasileira na área de telecomunicações e áreas correlatas. Além disso, a SBrT publica a revista *Journal of Communications and Information Systems* (JCIS), com trabalhos inovadores de interesse internacional, selecionados por especialistas.

Em complementação aos eventos científicos organizados pela SBrT e à publicação da revista JCIS, a Série SBrT/Elsevier objetiva o lançamento de livros voltados para a disseminação de conhecimento na área de engenharia elétrica e telecomunicações. A série inclui livros-texto, destinados à formação de estudantes de cursos de graduação e de pós-graduação, com material didático alinhado com o conteúdo programático das universidades brasileiras, bem como livros que se aprofundam em tópicos específicos, destinados a alunos de pós-graduação, pesquisadores e profissionais da área. A Série SBrT/Elsevier é uma demonstração do amadurecimento da comunidade científica brasileira na área de telecomunicações, tanto na formação de recursos humanos qualificados, como na produção de pesquisa científica.

Campinas, 2015.

Prof. Paulo Cardieri
Presidente da Sociedade Brasileira de Telecomunicações (SBrT)

Sobre o Autor

Marcelo Sampaio de Alencar, filho de José I Sampaio de Alencar e Gilvoneide Sampaio de Alencar, nasceu em Serrita, Pernambuco, em 1957. Formou-se em Engenharia Elétrica pela Universidade Federal de Pernambuco, em 1980, recebeu o título de mestre em Engenharia Elétrica pela Universidade Federal da Paraíba, em 1988 e o de Ph.D. em Engenharia Elétrica pela University of Waterloo, Canadá, em 1994. No período de 1982 a 1984, trabalhou na Faculdade de Engenharia da Universidade para o Desenvolvimento do Estado de Santa Catarina, onde foi Membro Titular do Conselho Universitário e vice-presidente da Associação dos Professores. Entre 1984 e 2002, trabalhou no Departamento de Engenharia Elétrica da Universidade Federal da Paraíba (UFPB). Desde 2002, trabalha no Departamento de Engenharia Elétrica da Universidade Federal de Campina Grande (UFCG), no cargo de Professor Titular.

Figura 1: Marcelo Sampaio de Alencar, o autor.

Exerceu os cargos de presidente da Comissão de Ascensão para Avaliação de Desempenho Acadêmico de Docente do CEEI, UFCG, vice-coordenador do Curso de Engenharia Elétrica, Assessor de Extensão do Centro de Ciências e Tecnologia, presidente da Comissão de Extensão do Centro de Ciências e Tecnologia da UFPB e membro do Comitê Assessor de Extensão da Universidade Federal da Paraíba. Atualmente é Líder do Grupo de Comunicações da UFCG, com cadastro no CNPq. Foi Professor do Programa de Pós-Graduação da Universidade Federal de Pernambuco (UFPE) e do Programa de Pós-Graduação *Lato Sensu* da Universidade Federal do Maranhão (UFMA). É fundador do Laboratório de Comunicações (Labcom) do Departamento de Engenharia Elétrica da UFPB. Orientou cinco pós-doutorandos, oito teses de doutorado, vinte dissertações de mestrado e uma monografia de especialização.

Trabalhou como consultor da Empresa Brasileira de Telecomunicações (Embratel), da Empresa de Telecomunicações do Rio Grande do Norte (Telern), da Telecomunicações Brasileiras S. A. (Telebras), da Companhia Hidroelétrica do São Francisco (Chesf), da Siemens, da Bell Mobility Canada, da Contol, da Tele Nordeste Celular Participações S.A. (TIM), do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) da Financiadora de Estudos e Projetos (Finep) e da *Portuguese Foundation for Science and Technology* (FCT), em diversos projetos, e foi Coordenador dos convênios que a UFCG manteve com a Embratel, Telern, Chesf e Atecel desde sua instituição. Foi coordenador do convênio entre a UFPB e a Universidade do Estado da Califórnia (CSU). Membro do Comitê de Avaliação de Professores (CAC) da FEEC Unicamp, entre 2004 e 2006.

Marcelo S. Alencar é fundador e presidente do Instituto de Estudos Avançados em Comunicações (Iecom). Em 1989, trabalhou na Divisão Regional de Engenharia da Embratel, em Recife. Foi Diretor da Sociedade Brasileira de Telecomunicações (SBrT), membro do Conselho Deliberativo e é, atualmente, vice-presidente para Relações Externas. Membro da Sociedade Brasileira de Micro-ondas (SBMO), da Sociedade Brasileira de Engenharia Biomédica (SBEB), Sócio Adjunto da Associação Sociedade Brasileira de Jornalismo Científico (ABJC), *Senior Member* do Instituto dos Engenheiros Eletricistas e Eletrônicos (IEEE).

Integrou a Comissão Organizadora do VI Simpósio Brasileiro de Telecomunicações, em 1988, o *International Advisory Committee do International Symposium on Personal, Indoor and Mobile Radio Communications* (PIMRC'95), da *12th International Conference on Telecommunications* – (ICT 2005), a Comissão de Programa Técnico de diversas edições do Simpósio Brasileiro de Telecomunicações e a *Global Communications Conference* (Globecom'99). Coordenador Técnico do *International Telecommunication Symposium* (ITS 2002), da *IEEE International Communications Conference* – (ICC'2002), da *5th International Conference on Wireless Personal Multimidia Communications* (WPMC'02), do Simpósio Brasileiro de Micro-Ondas e Optoeletrônica (SBMO 2002), da *IEEE Global Communications Conference* (Globecom'03), da *International Microwave and Optoelectronics Conference*

(IMOC 2003), da *IEEE International Communications Conference* (ICC'2004), do *Wireless Communications Symposium*, da *Global Communications Conference* (Globecom'03).

Participou ainda da organização da *IEEE Wireless Communications and Networking Conference* (WCNC'2004), do *International Workshop on Telecommunications* – (IWT 2004), da *International Wireless Communications and Computing Conference* (IWCCC 2006), do XXXIII Congresso Brasileiro de Ensino de Engenharia (COBENGE 2005), do *Advanced Industrial Conference on Telecommunications* (AICT 2006), do *International Workshop on Telecommunications* (IWT 2007), do XII Simpósio Brasileiro de Micro-Ondas e Optoeletrônica (MOMAG 2006), do *8th International Symposium on Systems and Information Security* (SSI'2006), do *Third Advanced International Conference on Telecommunications* (AICT'07), da *The First International Conference on Mobile Ubiquitous Computing, Systems, Services, and Technologies* (UBICOMM 2007), da *Fourth Advanced International Conference on Telecommunications* (AICT 2008), da *International Microwave and Optoelectronics Conference* – (IMOC 2007), da *Wireless Communications & Networking Conference* (WCNC 2008), do *Technical Committee* do *International Workshop on Telecommunications* (IWT 2009), da *2009 IEEE Wireless Communications and Networking Conference* (WCNC 2009), da *16th International Conference on Telecommunications* (ICT'09) e da *The First International Conference on Advances in Future Internet* (AFIN 2009).

Coordenador Geral do *The 13th International Symposium on Wireless Personal Multimedia Communications* (WPMC'10). Vice-coordenador do *The 9th IEEE International Symposium on Spread Spectrum Techniques and Applications* (ISSSTA 2006) e do *International Program Committee* da *The Second International Conference on Mobile Ubiquitous Computing, Systems, Services, and Technologies* (UBICOMM 2008). Membro do Comitê de Organização para Ligação International envolvendo a América Central e a América do Sul do *2004 IEEE Workshop on Signal Processing Advances in Wireless Communications*. Foi Coordenador Adjunto do XV Simpósio Brasileiro de Telecomunicações, em 1997, e do *2008 IEEE Workshop on Signal Processing Advances in Wireless Communications* (SPAWC 2008). Foi membro do *Sister Society Board* da *IEEE Communications Society* (ComSoc) e *Liaison to Latin America Societies* da ComSoc.

Foi Professor Visitante no Departamento de Engenharia Elétrica e de Computação, Universidade de Toronto, entre julho e agosto de 1997. Revisor da revista IEEE *Transactions on Communications*, da Revista Brasileira de Telecomunicações, da SBrT, da revista IEEE *Transactions on Vehicular Technology*, da revista *Wireless Personal Communications*, da Kluwer Academic Publishers. Membro da Comissão Brasileira de Comunicações 2 da Anatel e do Comitê Consultivo do Sistema Brasileiro de Televisão Digital do Ministério das Comunicações. Tem mais de 350 artigos publicados. Publicou mais de 350 artigos e entrevistas de divulgação científica e tem dezenas de artigos e livros referenciados em publicações nacionais e

internacionais.

Tem sua biografia incluída nas publicações *Who's Who in the World*, *Who's Who in Science and Engineering*, publicado por Marquis Who's Who, New Providence, EUA. Relacionado no IEEE ComSoc Volunteer Leaders & Staff Directory. Foi agraciado com a homenagem pelos 20 anos da SBrT, no XX Simpósio Brasileiro de Telecomunicações (SBT 2003). Recebeu o II Prêmio Dª Conceição, na categoria Destaque Projeto de Pesquisa. Recebeu o prêmio de destaque da Engenharia e Geociências, na qualidade de Engenheiro, pelo Centro de Tecnologia e Geociências, Faculdade de Engenharia de Pernambuco, no ano de comemoração de 110 anos de fundação da Escola de Engenharia de Pernambuco. Foi membro do Comitê Consultivo do Sistema Brasileiro de Televisão Digital, Ministério das Comunicações, considerado serviço relevante ao governo federal. Foi agraciado com o **Diploma de Agradecimento** da Escola de Comunicações do Exército Brasileiro. Foi homenageado pela Sociedade Brasileira de Micro-ondas e Optoeletrônica (SBMO) com a Medalha de Mérito Acadêmico Professor Attílio José Giarola. Recebeu uma homenagem pela brilhante atuação na produção e transmissão de conhecimento na área de Ciência e Tecnologia da Comissão Organizadora dos Eventos da Comemoração de 150 Anos de Emancipação Política do Município de Campina Grande. Teve reconhecido o **Notório Saber**, pelo Conselho de Pesquisa e Extensão (Consepe) da UFPB, por meio de certidão emitida em 21 de julho de 1995.

Marcelo Alencar é autor dos livros História da Comunicação no Brasil, Sexo Conexo, Soluços d'Alma, História, Tecnologia e Legislação de Telecomunicações e Divulgação Científica, pela Editora e Gráfica Epgraf, Teoria de Conjuntos, Medida e Probabilidade, Probabilidade e Processos Estocásticos, Televisão Digital, Ondas Eletromagnéticas e Teoria de Antenas, Telefonia Celular Digital, Telefonia Digital e Sistemas de Comunicações, pela Editora Érica Ltda., Princípios de Comunicações, pela Editora Universitária, UFPB, *Digital Television Systems*, pela Cambridge, *Communication Systems*, pela Springer, *Information Theory*, pela Mommentum Press, e do ensaio *Historical Evolution of Telecommunications in Brazil*, para a IEEE Foundation. É autor de capítulos nos livros *Communications, Information and Network Security*, Kluwer Academic Publishers, A Linguagem e a Comunicação entre Pessoas e Computadores, Editora Livro Rápido, A Linguagem e Suas Interfaces, Editora Livro Rápido, Em-TOM-Ação: A Prosódia em Perspectiva, Editora Universitária da UFPE, Jornalismo Científico e Educação para as Ciências, Editora Cabral Universitária, Tecnologia da Informação – TV Digital, pela Secretaria de Ciência, Tecnologia e Inovação da Bahia. É articulista do NE10, portal do Sistema Jornal do Commercio de Comunicação, de Recife, no qual assina a coluna **Difusão**, de divulgação científica, desde abril de 2000. Mais informação sobre o autor no *site* `www.difusaocientífica.com`.

Agradecimentos

A publicação deste livro é fruto do trabalho de muitos anos dedicados pelo autor ao ensino, à pesquisa e à consultoria profissional a empresas, indústrias, além de agências de fomento à pesquisa no Brasil e no exterior.

O professor Marcelo Sampaio de Alencar agradece a oportunidade de ter trabalhado, por mais de três décadas, na Faculdade de Engenharia e Joinville da Universidade para o Desenvolvimento de Santa Catarina, no Departamento de Engenharia Elétrica da Universidade Federal de Campina Grande e no Instituto de Estudos Avançados em Comunicações.

Agradece ainda a cooperação de muitos anos com o Departamento de Eletrônica e Sistemas da Universidade Federal de Pernambuco, com a Universidade Federal do Semi-árido, com a Universidade Católica de Pernambuco e com a Universidade de Pernambuco.

Parte deste trabalho foi desenvolvida em cursos ministrados pelo autor na Universidade Federal de Campina Grande e em outras instituições de ensino superior.

O autor deve este livro à compreensão e ao amor de sua esposa e de seus filhos, que permitiram-lhe realizar o trabalho a partir de notas de aulas ministradas em disciplinas de especialização, graduação e pós-graduação.

Leitores que queiram entrar em contato com o autor, seja para comentar ou fazer críticas ao texto, podem utilizar os seguintes endereços:

Marcelo Sampaio de Alencar
Caixa Postal 547
58.400-971 Campina Grande PB
E. mail: malencar@dee.ufcg.edu.br

Prefácio

A Teoria Matemática da Informação evoluiu a partir dos trabalhos de Claude Elwood Shannon e Andrei Nikolaevich Kolmogorov, no final da década de 1940, tendo com base a Teoria de Probabilidade. Charles Sanders Peirce havia, no século anterior, estabelecido os principais aspectos semânticos da comunicação, base atual da Comunicação Social.

A década de 1950 viu florescer os princípios da Teoria da Codificação, para compactação ou compressão de sinais de voz e de vídeo, além de arquivos de dados, com os trabalhos de David Huffman, Leon Kraft, Brockway McMillan, Abraham Lempel e Jacob Ziv, entre outros pesquisadores.

A codificação também foi desenvolvida para proteção contra erros de transmissão no canal, inicialmente com o trabalho de pesquisa de Richard Wesley Hamming, Peter Elias, Irving Stoy Reed, Gustave Solomon, James Lee Massey, Andrew Viterbi, entre outros.

O advento das redes de computadores, notadamente a Internet, com os trabalhos de Norman Abramson, Leonard Kleinrock, Vint Cerf, entre outros, permitiu a interconexão de bilhões de computadores em todo o mundo, mas também possibilitou o aparecimento de criminosos dedicados a explorar a riqueza informacional e financeira da rede mundial.

O livro é dirigido aos estudantes e profissionais de Engenharia Elétrica, Computação, Sistemas de Informação, Teleinformática e Matemática. Poucos livros têm sido publicados contendo os assuntos tratados, e aqueles disponíveis geralmente são destinados a audiências muito específicas.

Descrição do Livro

O livro começa com a definição de medida da informação e entropia, no primeiro capítulo. O Capítulo 2 trata de fontes de informação. A codificação de fonte é discutida no Capítulo 3, no qual são apresentados os códigos usuais. O Capítulo 4 contém os fundamentos para o cálculo da capacidade de canais de comunicações.

As técnicas de espalhamento espectral, base de vários sistemas de comunicações digitais modernos, são vistas no Capítulo 5. Os conceitos fundamentais dos códigos

corretores de erros são tratados no Capítulo 6. Os códigos convolucionais aparecem no Capítulo 7.

Os princípios e a abordagem matemática da criptografia, essenciais para a proteção da informação, são o assunto do Capítulo 8. O Capítulo 9 discute a aplicação da criptografia a redes de computadores, as alternativas para prevenir ataques e os protocolos de segurança.

O livro tem um apêndice sobre Probabilidades, com os principais resultados necessários ao entendimento da teoria. Há vários exercícios resolvidos e problemas propostos, muitas referências bibliográficas e um índice remissivo para facilitar a consulta a tópicos específicos.

Sumário