BOOK REVIEW

Secure communications: applications and management

Roger J. Sutton

John Wiley & Sons Ltd., 2002, 322pp., £39·95,
ISBN 0 47149 904 8

Overall this is a somewhat disappointing book. However, this reaction is partly conditioned by the fact that the contents do not live up to the title. There is no way that this book attempts to provide a comprehensive coverage of secure communications. The preface gives the first hint about the real focus, by stating the book is about secure telecommunications. Reading the contents list makes it immediately clear that there are many topics missing that one would expect in any book with this title—for example, there is no significant coverage of Internet security (apart from a very few pages in chapter 12 on VPN security). This is rather regrettable since the IP protocol and its security are of ever increasing importance in the telecommunications world.

A second and more careful reading of the contents list reveal the coverage to be idiosyncratic in the extreme. The book starts with the obligatory couple of introductory chapters—these already ring alarm bells since, judging by the title of chapter 2, the author seems to think digital signatures are a kind of encryption. (This turns out to be symptomatic of an obsession with the importance of encryption over other types of cryptographic technique.) The next two chapters deal with voice security or, more precisely, voice encryption. This is followed by a chapter on GSM security. Despite claims in various places in the book that security is about more than encryption, it is not clear that the author really believes this statement, since the emphasis in this chapter and elsewhere is very much on data encryption. The authentication of GSM mobiles to the base station is a topic hardly mentioned, despite the fact that it is arguable that this security feature is much more important than air interface encryption. This thesis is supported by the fact that, in some countries (e.g. France), GSM networks were originally (successfully) deployed without any air interface encryption. Whilst GSM without encryption therefore appears to be a viable, albeit perhaps undesirable, option, the level of fraud to which the first generation mobile networks were prone suggests that GSM without mobile authentication would simply not be conveivable.

There follows a series of chapters on security in private radio networks, frequency hopping, bulk encryption and fax security. The common approach of these chapters, and also the two earlier chapters on voice encryption and two later chapters on secure VPNs and military data communications, is that of a series of design studies. These studies are presumably based on personal design experience, and describe just one approach to each problem rather than exploring a variety of different design approaches. This is interesting material nevertheless, although it could only be used as tutorial material with great care, since it makes no pretence to scientific objectivity.

Apart from the chapters already mentioned, there are chapters on PC security, secure e-mail, and security management. However, these are also very idiosyncratic in their coverage. For example, the chapter on PC security does not attempt to describe what a virus is, and gives no general discussion of malicious code.

There are other surprising omissions from the book. For example, chapter 11 (on secure e-mail) makes no mention of any of S-MIME, PEM, X.400 or Open-PGP. Nowhere in the book (that I can find) is there any discussion of public key certificates or PKIs. The chapter on security management is very brief, and manages to avoid any mention of ISO/IEC 17799. The bibliography is very weak indeed; there are a number of major relevant books that are not mentioned.

In conclusion, this book has some merit in being generally well written and accessible, and it also covers topics (notably those relating to military encryption) that are not well covered in other sources. However, it has some very serious omissions, and cannot be recommended as a first (or even second) book to buy on the topic of secure communications; even where topics are covered, the reader should not believe that the coverage is in any way a comprehensive treatment. This book will primarily be of interest and value to the specialist, rather than the reader looking for a general introduction to the subject.

CHRIS MITCHELL

Principles of space–time adaptive processing

Richard Klemm

The Institution of Electrical Engineers, 2002, 556pp., £65
ISBN 0 85296 172 3

Although the basic ideas underlying the theory of STAP (Space–Time Adaptive Processing) can be traced back more than 30 years, it is only recently that the computing power has become available to allow the theory to be put into practice in real systems. Next year Radarsat 2 is due to be launched carrying the world's first spaceborne GMTI (Ground Moving Target Indication) radar, for earth observation, and several military surveillance radars will soon benefit from the ability of STAP to suppress clutter so that small moving targets can be detected.

This book is a revision of an earlier STAP text by the author and is the first of a two part series, concentrating on theoretical principles; the second volume will deal with applications. The early chapters are devoted to preliminary material, including a comprehensive review of basic radar signal-processing techniques, models for radar targets and interference signals, and the properties of airborne radar clutter. A helpful feature of Chapter 2 is the definition of a standard set of radar system parameters, which are used to generate the copious illustrations showing the results of computer simulations.

In the middle of the book we are introduced to the optimum processor, and the relationships between the STAP processor, the DPCA (Displaced Phase-Centre Antenna) and motion compensation are explained. A wide range of suboptimal processors are described and their performances compared to that of the optimum processor to show that huge savings in computation can be made for very little degradation in clutter cancellation performance. Transformations in both the spatial and temporal dimensions as well as space–time transformations are discussed. Space–frequency processing (commonly referred to as post-Doppler STAP) is also covered. The impact of a variety of different antenna array geometries is analysed, including results for circular and planar arrays.

In the final part of the book the author considers some aspects of radar systems that make the application of STAP more challenging. New chapters are devoted to the effects of radar ambiguities, which lead the angle–Doppler relationship of the clutter to be range-dependent, and to bistatic STAP, which is the subject of much current research interest. The material on SAR (Synthetic Aperture Radar), ISAR (Inverse SAR), and jammer mitigation is unchanged from the first edition. It is not until Chapter 14 that some real-world effects, such as finite sampling, are considered, and care must be taken to interpret the results of earlier chapters in this light. The detailed analysis of real-world effects, however, is beyond the scope of this book. Another new chapter on parameter estimation analyses the influence of radar system parameters, such as bandwidth, on the accuracy with which target parameters can be estimated. The book concludes with an appendix describing the application of STAP in sonar systems, and relating much of the theory developed for radar signal processing to the sonar environment.

I found this book to be readable and comprehensive. The bibliography is extensive and without obvious omissions. I would recommend the book to anyone as an introduction to the design of STAP systems for radar and sonar.

S. D. HAYWARD

The J. Langham Thompson Premium 2000-2001, the award for the best paper published in Electronics & Communication Engineering Journal during the period 1st October 2000 to 30th September 2001, has been given to Prof. Alister Burr (University of York) for his paper on ‘Turbo-codes: the ultimate error control codes?’. Prof. Burr is pictured (left) receiving the award from Prof. Will Stewart (a member of Executive Team of the IEE Professional Network on Photonics) at the recent Appleton Lecture at Savoy Place. Prof. Burr’s paper appeared in the August 2001 issue of the Journal.