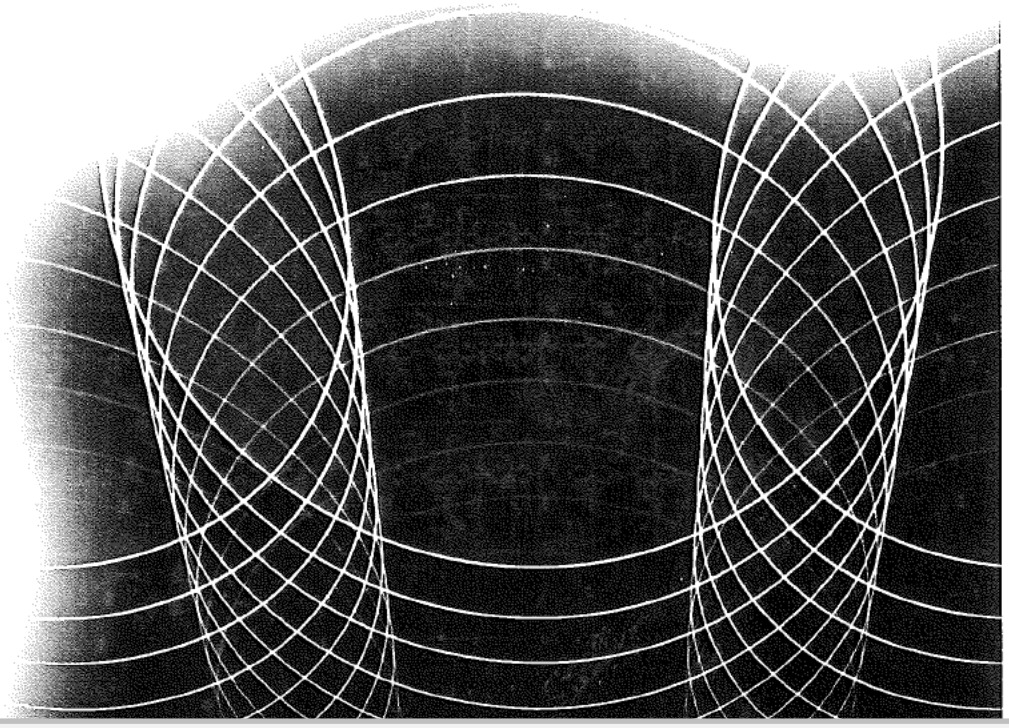
WILEY

# Wireless and Mobile Network Architectures



Yi-Bing Lin

Publisher: Robert Ipsen
Editor: Carol Long
Associate Editor: Margaret Hendrey
Managing Editor: Micheline Frederick
Text Design & Composition: Integre Technical Publishing Co., Inc.



This book is printed on acid-free paper. ♾



Published by John Wiley & Sons, Inc.

Published simultaneously in Canada.



*Library of Congress Cataloging-in-Publication Data:*

0471-39492-0

Printed in the United States of America

10 9 8 7 6 5 4 3

- A TCAP message can have multiple components; each component performs one action. For simplicity, IS-41 TCAP messages are composed of a single component. Some personal communication service implementations under advanced intelligent network platform use multiple component TCAP messages.

## 6.2 IS-41 Authentication

The EIA/TIA *Telecommunications Systems Bulletins* (TSB) 51 defines protocols for authentication, voice privacy, and signaling message encryption, which have been incorporated into IS-41 Revision C and later versions. The TSB-51 algorithm is based on private key cryptographic techniques in which a secret key, known as *shared secret data* (SSD), is shared between the MS and the authentication center (AuC). This key is known only to these two parties.

Two authentication schemes have been proposed in TSB-51. In the *without-sharing* (WS) scheme, the SSD is shared only between the authentication center and the MS. In the *sharing* (S) scheme, the SSD or some aspect of SSD may be shared with the visited system as well. Since the visited system has the SSD, it can authenticate the MS at call origination or delivery, thereby considerably reducing message flow and call setup time. However, as will be seen later, this scheme requires additional message exchanges during registration. Thus, there is a trade-off between the two schemes, based on the expected number of calls to/from the user between two consecutive registrations. For a user with high call frequency, sharing the SSD with the visited system is beneficial; consequently, the S scheme is preferable. For a user with high mobility rate, sharing SSD with the visited system results in considerably increased traffic; consequently, the WS scheme is preferable. For a given user, the call and the move frequencies may vary from time to time; therefore, it is desirable to switch between the two authentication schemes as the user's behavior changes. We describe two adaptive algorithms to select the authentication scheme for a user. Performance studies indicate that as call or move frequencies of a user change, the adaptive algorithms automatically select the appropriate authentication scheme in real time.

### 6.2.1 Privacy and Authentication in TSB-51

In AMPS, every MS is associated with a *mobile identification number* (MIN) and an *electronic serial number* (ESN). A MIN is a North American

Numbering Plan (NANP) number that serves as a mobile telephone number. MINs are programmed into MS at purchase, and are known to the customers. An ESN is created at manufacture, and the customers are not supposed to be aware of it. The ESN is a 32-bit serial number where the highest-order 8 bits represent the manufacturer's code. The remaining bits are used as a unique MS number.

When the first AMPS network was built at Bell Labs, few users were expected. ESN was considered sufficient to authenticate a user. Some unscrupulous people figured out that they could receive MINs and ESNs over the air and then reprogram phones so that other cellular users would get the bills. Scanning test equipment for intercepting MIN/ESN combinations is legitimately available. *Cloned phones* can be created following the scanning and reprogramming procedures. To address this serious security issue, this section describes two EIA/TIA TSB-51 schemes for privacy and authentication. We first describe the without-sharing (WS) scheme, then show how it differs from the sharing (S) scheme. To facilitate the discussion that follows, we reiterate notions and terminologies introduced in Chapter 5, Section 5.2. The AuC is a database connected to the HLR, which provides it with the authentication parameters and ciphering keys used to ensure network security. The AuC is solely responsible for maintaining and updating the SSDs. Users move about *location areas* (LAs) belonging to one or more *PCS service providers* (PSPs). Each PSP may provide some combination of BSs for offering wireless access to the MSs. These BSs are controlled by MSCs. Associated with each location area is a visitor location register (VLR). The VLRs may be part of the PSP network. It is likely that the VLRs are collocated with MSCs. For demonstration purposes, we assume that VLRs are separated from the PSP network. Note that the results of this section are not affected by the locations of VLRs. One or more home location registers (HLRs) are maintained by the PSP, which maintain user profiles, current location area, and so on.

## 6.2.2 Without-Sharing (WS) Scheme

In the WS scheme, the SSD is known to the AuC and the MS only. Message flow for privacy and authentication of the WS scheme is described below.

### 6.2.2.1 Registration (Location Update)

The authentication message flow for MS registration is shown in Figure 6.5 and is described in the following steps:

three dimensions. According to Andy Hopper at Cambridge University, "With active bat, it is possible to determine the spatial relationships of people, displays, telephones, keyboards, and so on, and configure them automatically to create a truely active office environment." Details of active badges and sentient computing can be found in www.uk.research.att.com.

## 24.3 Bluetooth

The efforts to develop an integrated voice/data home wireless network started in 1998, when two working groups began establishing industry standards in this area: the Home RF Working Group (HRFWG) and the Bluetooth Special Interest Group (SIG). Bluetooth technology was a spin-off of an internal Ericsson project on wireless connectivity. Understanding that it would be the best way to make the technology successful, Ericsson made Bluetooth available to the rest of the industry. Consequently, along with Nokia, IBM, Intel, and Tobisha, Ericsson founded Bluetooth. In addition to these two groups, a company named Home Wireless Network (HWN) debuted proprietary home wireless products in January 1999. HWN, with Lucent as its major investor, is targeting home and small businesses, offering integrated voice and data products.

As data and voice merge in the everyday lives of people, an integrated cordless system based on the Bluetooth technology should facilitate access to voice and data. It should also stir the growth of cordless phones, and expand to small office applications. Bluetooth operates in the 2.4–2.483 GHz ISM band. It utilizes fast-frequency hopping with spread-spectrum techniques, whereby packets are delivered in specified time slots at up to 723.2 Kbps. Bluetooth units (such as mobile handsets, PCs, PDAs, printers, and so on) can be connected through the Bluetooth radio link to form a piconet in the office environment.

Figure 24.5 illustrates the Bluetooth protocol stack. A host controller interface is defined, which provides higher-layer protocols and a command interface to control the baseband and link manager, and to access hardware status and control registers. The Bluetooth protocols are described as follows.

### 24.3.1 Bluetooth Core Protocols

These include Bluetooth RF, baseband, Link Manager Protocol (LMP), Logical Link and Control Adaptation Protocol (L2CAP) and Service