行動通訊

CHAPTER 9

行動通訊系統

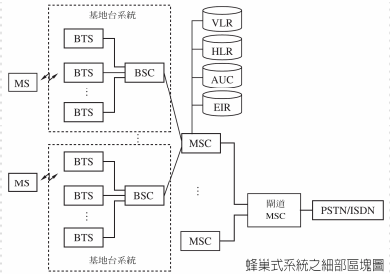
9.2 蜂巢式系統的基礎建設

- 各基地台含有一個基地收發台（BTS）與一個基地台控制器（BSC）。
- 驗證中心（authentication center; AUC）提供驗證與加密等參數。

9.2 蜂巢式系統的基礎建設

- 設備身分資料庫（equipment identity register; EIR）是用來存放有關手機設備的身分資訊。
- 本籍註冊資料庫（home location register; HLR）與客籍註冊資料庫（visitor location register; VLR）是兩組漫遊管理的資料庫。
- HLR是位於MS的本籍MSC。

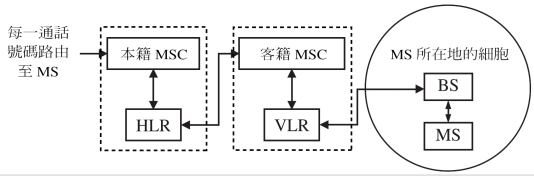
9.2 蜂巢式系統的基礎建設



蜂巢式系統之細部區塊圖

行動通訊 第九章 第212頁 圖9.1

9.2 蜂巢式系統的基礎建設

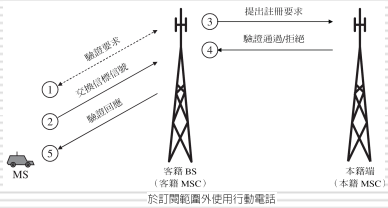


通話轉接至位於客籍的 MS

行動通訊 第九章 第213頁 圖9.3

9.3 註冊

- 註冊的完成需藉助在MS與BS之間交換一種叫做「信標信號」（beacon signals）的資訊。



於訂閱範圍外使用行動電話

行動通訊 第九章 第214頁 圖9.4

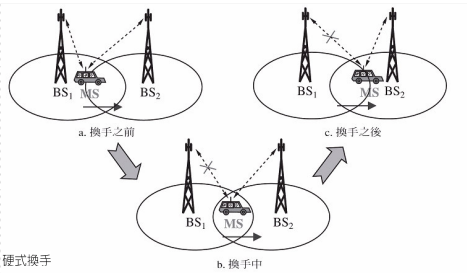
9.4 換手參數與底層支援

- 換手需求可能是由BS或MS所提出，其決定因素包括：
  1. 無線電連結。
     - 無線電連結的換手主要是因為MS的移動性。
  2. 網路管理。
     - 網路管理所造成的換手主要是相鄰細胞的流量有嚴重的不平衡。
  3. 服務議題。
     - 服務相關的換手主要是品質保證（quality of service; QoS）的惡化。

9.4.2 換手之底層支援

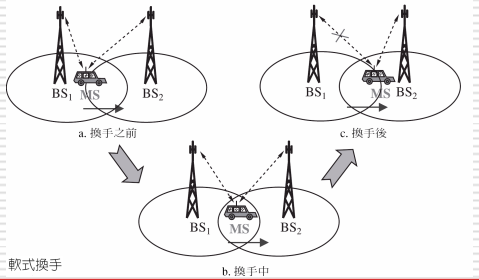
- 換手可以分為兩種類型：硬式換手（hard handoff）與軟式換手（soft handoff）。
- 硬式換手，又叫做「先切斷後建立」（break before make），會先釋放與現有BS之間的無線電資源，然後才與新的BS建立連線。
- 一段短的時間內，MS可同時與舊有BS以及新的BS進行通訊。這種方案叫做軟式換手，或「先建立後切斷」（make before break）。

9.4.2 換手之底層支援



硬式換手

9.4.2 換手之底層支援

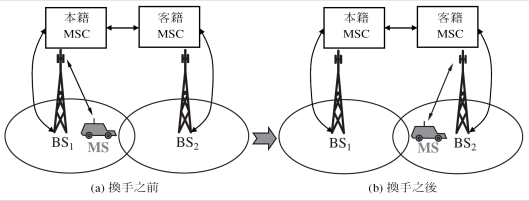


軟式換手

行動通訊 第九章 第218頁 圖9.6

CENGAGE Learning

9.4.2 換手之底層支援

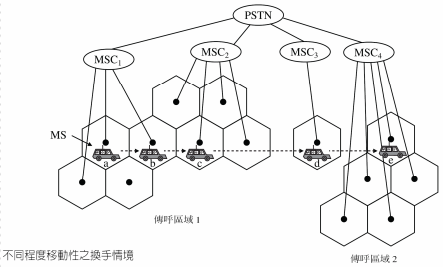


MSC 之間的換手

行動通訊 第九章 第219頁 圖9.7

CENGAGE Learning

9.5 漫遊支援

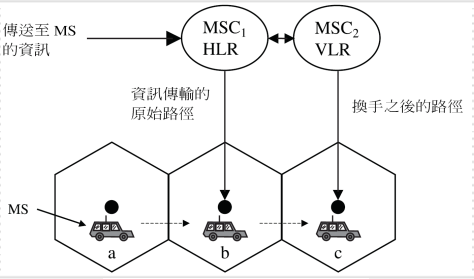


不同程度移動性之換手情境

行動通訊 第九章 第220頁 圖9.8

CENGAGE Learning

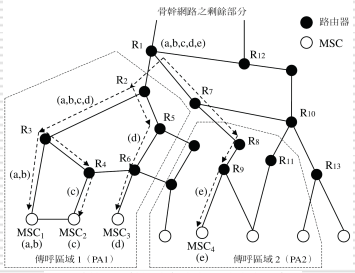
9.5 漫遊支援



當 MS 從“b”換手至“c”之資訊轉移路徑

CENGAGE Learning

9.5 漫遊支援



MSC 連線至骨幹網路與路由/再路由之示意圖

CENGAGE Learning

9.5.1 本籍代理人、客籍代理人，以及行動IP

- 在行動IP（mobile Internet protocol; Mobile IP），有兩個重要的代理人：本籍代理人（home agent; HA）與客籍代理人（foreign agent; FA）。

CENGAGE Learning

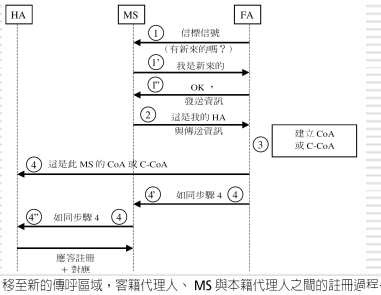
9.5.1 本籍代理人、客籍代理人，以及行動IP

- HA—FA的功能有點類似HLR—VLR的功用，但差別在於前者所能提供的移動性遠大於後者。
- 當FA發現有一個新的MS進入其網域，它會分配一個轉交位址（care-of-address; CoA）給MS。
- CoA可以是FA本身的位址，或也可以透過DHCP（dynamic host configuration protocol）分配一個叫共同分配的轉交位址（collocated CoA; CCoA）作為MS的新位址。

9.5.1 本籍代理人、客籍代理人，以及行動IP

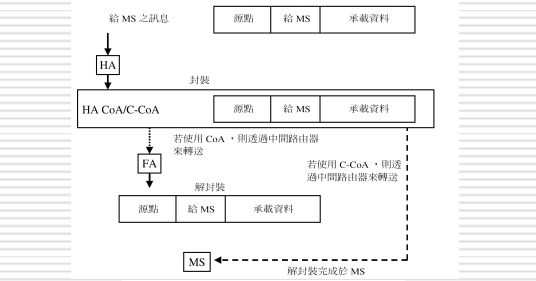
- 一旦MS接收到CoA，就會向它的HA註冊此CoA，以及此CoA的有效時間。
- HA會將封包用MS的CoA進行封裝（encapsulation），然後轉送給FA。
- 如果是使用CCoA位址，則MS會直接收到封包，然後反封裝。

9.5.1 本籍代理人、客籍代理人，以及行動IP



當 MS 移至新的傳呼區域，客籍代理人、 MS 與本籍代理人之間的註冊過程

9.5.1 本籍代理人、客籍代理人，以及行動IP



使用本籍代理人—客籍代理人配對將訊息轉送至 MS

行動通訊 第九章 第223頁 圖9.12

CENGAGE Learning

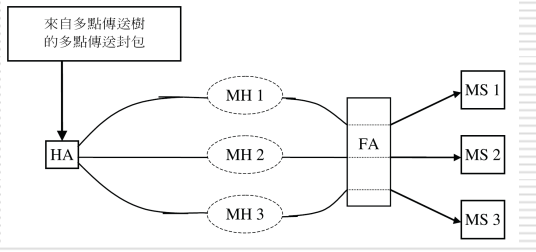
9.6 多點傳送

- 多點傳送（multicasting）[9.8] 是將訊息利用一個稱為群組位址（group address）的位址從原始端傳送至多個目的端的過程。

行動通訊 第九章 第225頁

CENGAGE Learning

9.6 多點傳送

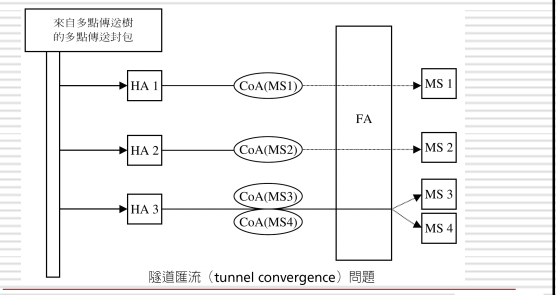


雙向隧道法之封包重複

行動通訊 第九章 第226頁 圖9.14

CENGAGE Learning

9.6 多點傳送

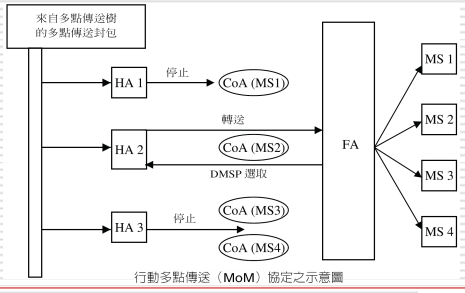


隧道匯流（tunnel convergence）問題

行動通訊 第九章 第227頁 圖9.15

CENGAGE Learning

9.6 多點傳送



行動多點傳送（MoM）協定之示意圖

行動通訊 第九章 第228頁 圖9.16

CENGAGE Learning

9.7 安全與隱私

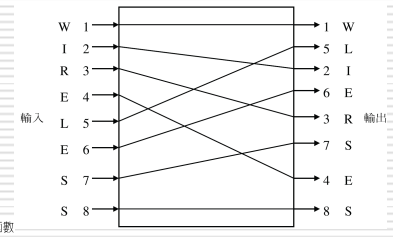
- 有一種攻擊是利用超強功率的發射器來人為干擾（jamming）某個頻率，可以輕易地利用跳頻技術來克服。
- 真正的挑戰是如何確保未獲授權的用戶無法輕易地攔截並解譯信號。

行動通訊 第九章 第228頁

CENGAGE Learning

9.7.1 加密技術

- 訊息的加密可以在傳送前進行簡單的位元排列。



簡易排列函數

CENGAGE Learning

9.7.1 加密技術

- 圖9.18所示為一種輸入位元的資料加密標準（data encryption standard; DES）。

使用 DES 傳輸前與接收後的初始位元樣式與排列效果

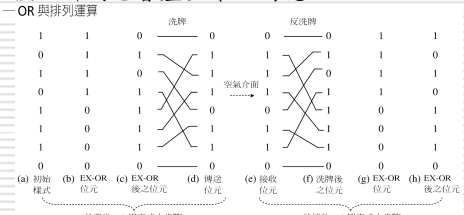
1 2 3 4 5 6 7 8	57 49 41 33 25 17 9 1	8 24 40 56 16 32 48 64
9 10 11 12 13 14 15 16	61 53 45 37 29 21 13 5	7 23 39 55 15 31 47 63
17 18 19 20 21 22 23 24	58 50 42 34 26 18 10 2	6 22 38 54 14 30 46 62
25 26 27 28 29 30 31 32	62 54 46 38 30 22 14 6	5 21 37 53 13 29 45 61
33 34 35 36 37 38 39 40	59 51 43 35 27 19 11 3	4 20 36 52 12 28 44 60
41 42 43 44 45 46 47 48	63 55 47 39 31 23 15 7	3 19 35 51 11 27 43 59
49 50 51 52 53 54 55 56	60 52 44 36 28 20 12 4	2 18 34 50 10 26 42 58
57 58 59 60 61 62 63 64	64 56 48 40 32 24 16 8	1 17 33 49 9 25 41 57
(a) 欲傳送的資訊序列	(b) 傳送前的資訊序列之排列	(c) 接收資訊序列的排列

CENGAGE Learning

9.7.1 加密技術

- EX—OR與它的互補布林函數都能做唯一轉換，解碼也會產生唯一對應。

EX—OR 與排列運算

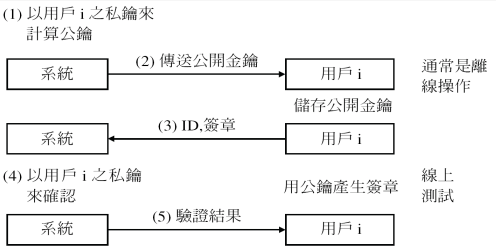


CENGAGE Learning

9.7.2 驗證

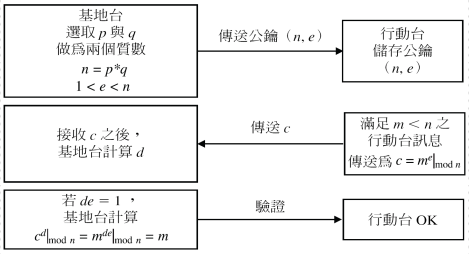
- 用戶的驗證基本上是要確認用戶的真實性。
- 一種作法是使用兩把不同但相關之鑰匙，第一把鑰匙僅有產生此鑰匙的系統所知悉，而第二把是用來公諸於世的。

9.7.2 驗證



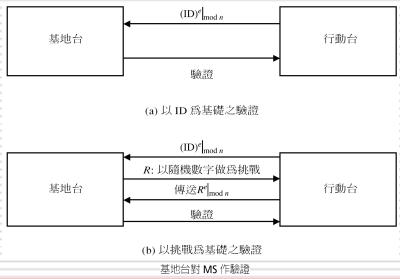
公私鑰的驗證過程

9.7.2 驗證



使用公私鑰作訊息驗證

9.7.2 驗證

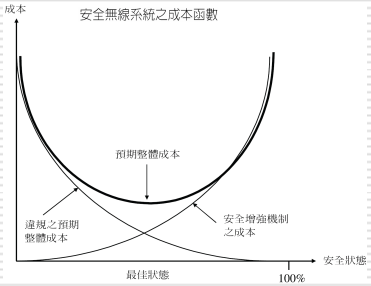


基地台對 MS 作驗證

9.7.3 無線系統安全

- 安全服務可以分為下面幾種類型：
  1. 機密性（confidentiality）
  2. 不可否認性（nonrepudiation）
  3. 驗證
  4. 完整性（integrity）
  5. 可用性（availability）

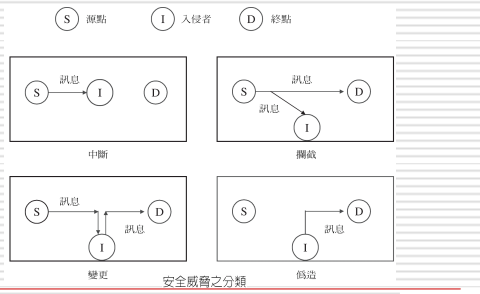
9.7.3 無線系統安全



9.7.3 無線系統安全

- 威脅可廣義地分為兩種：意外威脅與蓄意威脅。
- 這些攻擊可分類為如圖9.26所示。
  1. 中斷（interruption）
  2. 攔截（interception）
  3. 變更（modification）
  4. 偽造（fabrication）

9.7.3 無線系統安全



9.7.3 無線系統安全

- 攻擊可分為主動式與被動式攻擊兩種。
- 各種主動式攻擊的類型：
  1. 偽裝（masquerade）
  2. 重演（replay）
  3. 資料變更（modification of data）
  4. 服務阻斷（denial of service; DoS）
- 被動式攻擊是當未獲授權的攻擊者對網路進行監控與封包攔截。