Unit-1:

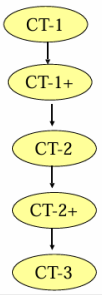
1.Explain the following with all the features

1.Cordless telephone

2.PACS

Cordless Telephone, Second Generation (CT2) (1/2)

- Developed in Europe since 1989.
- 40 FDMA channels
- 32-Kbps speech coding rate
- TDD
- The maximum transmit power of a CT2 handset is 10 mW



48

Cordless Telephone, Second Generation (CT2) (2/2)

- No handoff in CT2
- No call delivery in CT2
- In CT2+, both handoff and call delivery are OK.

Personal Access Communications System (PACS)

- Developed at Telcordia, U.S.A.
- PACS is designed for wireless local loop and PCS.
- TDMA
- 8 voice channels/frequency carrier
- Both TDD and FDD are accommodated.
- The highly effective and reliable mobile-controlled handoff (MCHO) completes in less than 20 msec.

43

Comparison of PCS Systems

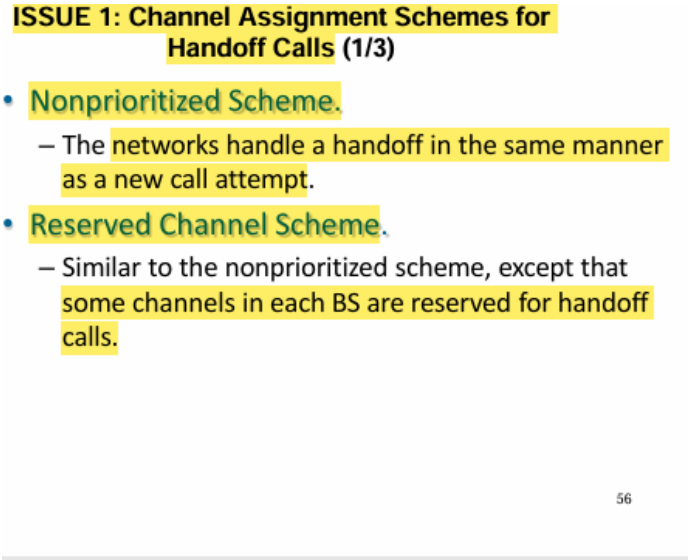
System	CT-2	DECT	PHS	PACS
Region	歐,台灣	歐	日本	美
Duplex	TDD	TDD	TDD	FDD
MAC	FDMA	FDMA TDMA	FDMA TDMA	FDMA TDMA
Frequency (MHz)	864-868	1880-1900	1895-1918	1930-1990(down) 1850-1910(uplink)
Carrier	100kHz	1728kHz	300kHz	300MHz
Channels	1	24	8	8
Speech rate	32kps	32kps	32kps	32kps
Channel bit rate	72kps	1152kps	384kps	384kps

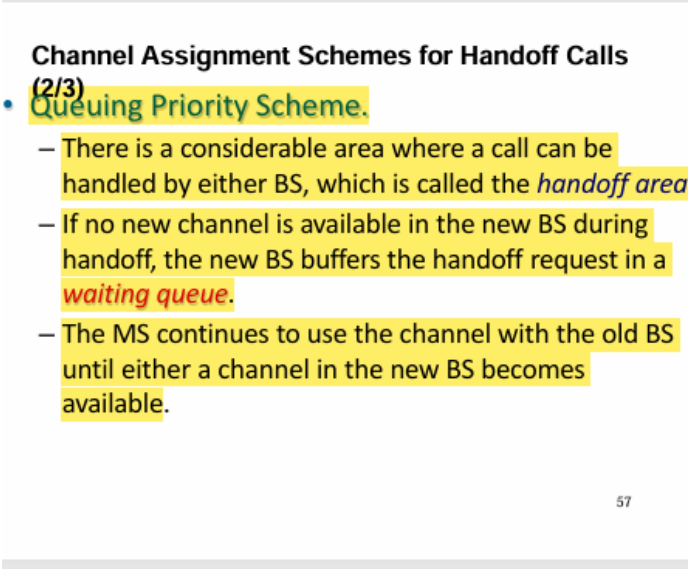
2.Explain the following

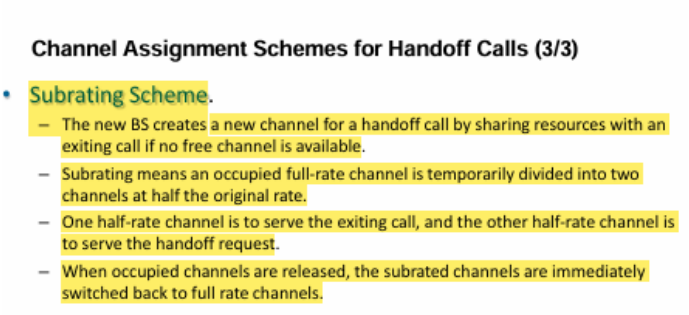
a. Reserved channel scheme

b. Queuing priority scheme

c. Sub rating scheme.







3.Compare and contrast between AMPS and GSM

Comparison of Cellu

System	AMPS	GSM DCS1800
Region	美	歐,台灣
Duplex	FDD	FDD
MAC	FDMA	FDMA TDMA
Downlink (MHz)	870-890	935-960 1805-1880
Uplink (MHz)	825-845	890-915 1710-1785
Carrier	30kHz	200kHz
Channels	1	8
Speech rate	10 kps	13 kps
Channel bit rate		270.833 kps

Advanced Mobile Phone Service (AMPS) (1/2)

- Analog FM radio for voice transmission
- FSK modulation for signal channels
- FDMA
- FDD
- Total 50 MHz=824-849 MHz(down-link) + 869-894 MHz(up-link)
  - 832 full-duplex channels using 1664 discrete frequencies
- 30kMHz spacing

28

Advanced Mobile Phone Service (AMPS) (2/2)

- Frequency reuse scheme for radio communication

Global System for Mobile Communications (GSM) (1/2)

- "Digital" cellular system
  - Group Special Mobile of Conference Europeenne des Posts et Telecommunications (CEPT) and European des Postes et Telecommunications (ETSI)
- TDMA/FDD
- 935-960 MHz for Downlink
- 890-915 MHz for Uplink
- 200 kHz for RF channel spacing
- Speech coding rate 13 Kbps

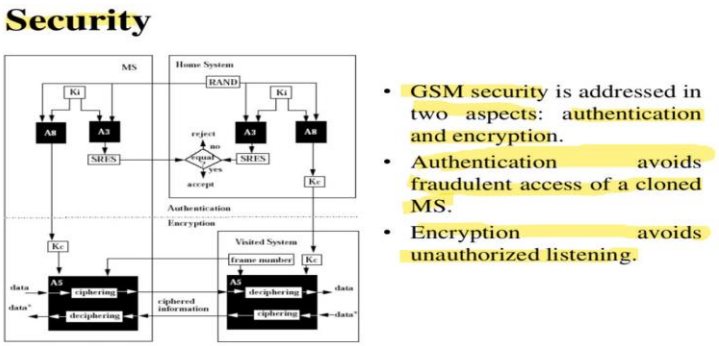
3

Global System for Mobile Communication (GSM) (2/2)

- Frequency carrier is divided into 8 time slots
  - Every pair of radio transceiver-receiver supports 8 voice channels.
- GSM Mobile Application Part (MAP) for roaming management
- Digital switch can provide many applications:
  - Example: point-to-point short messaging, group addressing, call waiting, multiparty services

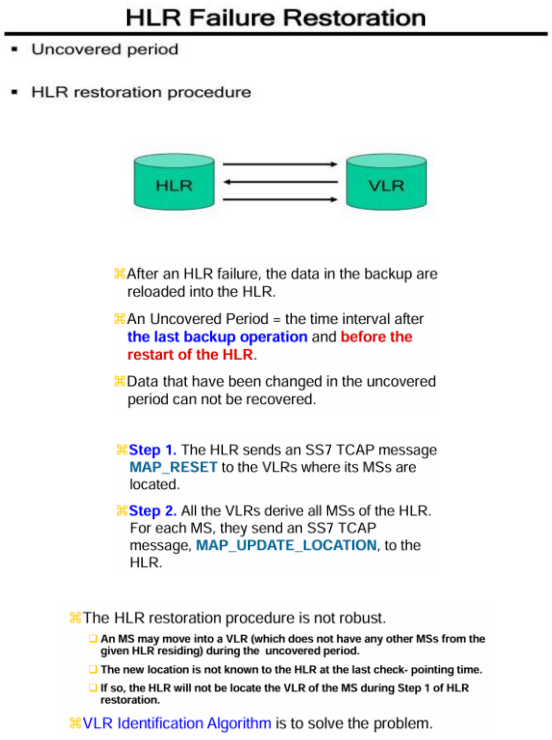
Unit-2:

1.GSM security architecture

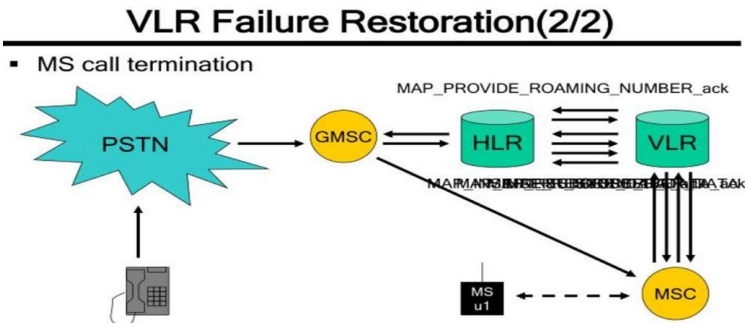


- GSM security is addressed in two aspects: authentication and encryption.
- Authentication avoids fraudulent access of a cloned MS.
- Encryption avoids unauthorized listening.

2.HLR failure restoration



3.VLR failure restoration



- **Service Information** of a VLR record recovered by
  - **The first contact between the VLR and the HLR of the corresponding MS.**
- **Location Information** of a VLR record recovered by
  - **First radio contact between the VLR and the MS**
- **Mobile Station Information** of a VLR record recovered by
  - **Either by contact with the HLR or the MS**

VLR Record Restoration Initiation Event 1—MS Registration

- The VLR considers the registration as a case of inter-VLR movement.
- Following the normal registration procedure defined in inter-VLR movement.
- In this case, the TMSI sent from the MS to the VLR cannot be recognized, and the MS is asked to send IMSI over the air.

VLR Record Restoration Initiation Event 2—MS Call Origination

- When the VLR receives the call origination request **MAP_SEND_INFO_OUTGOING_CALL** from the MSC, the VLR record of the MS is not found.
- The VLR considers the situation as a system error, with the cause "**unidentified subscriber**".
- The request is rejected, and the MS is asked to initiate the location registration procedure.

VLR Record Restoration Initiation Event 3—MS Call Termination (1/)

- **Steps 1-3.** Similar to the first three steps of the basic call termination procedure, the VLR is queried to provide the MSRN.
  - **Note that since the record has been erased after the failure, the search fails. The VLR creates a VLR record for the MS.**
  - **Neither the service nor the location info is available.**
- **Steps 4 and 7.**
  - **Since the VLR does not have the routing information, it uses the MSC number provided by MAP_PROVIDE_ROAMING_NUMBER message to create MSRN.**
  - **The number is sent back to the gateway MSC to setup the call in Step 8.**

VLR Record Restoration Initiation Event 3—MS Call Termination (2/)

- **Steps 5 and 6.**
  - **The VLR recovers the service information of the VLR record by sending a MAP_PROVIDE_ROAMING_NUMBER message to the HLR.**
  - **The HLR sends the service information to the VLR using the MAP_INSERT_SUBSCRIBER_DATA message.**
  - **At this point, the service information of the VLR record has been recovered.**
  - **However, the location information, specifically, the LAI number, still not available. This information will be recovered at Step 11.**
- **Note that** Steps 4 and 5 can be executed in parallel.

VLR Record Restoration Initiation Event 3—MS Call Termination (3/)

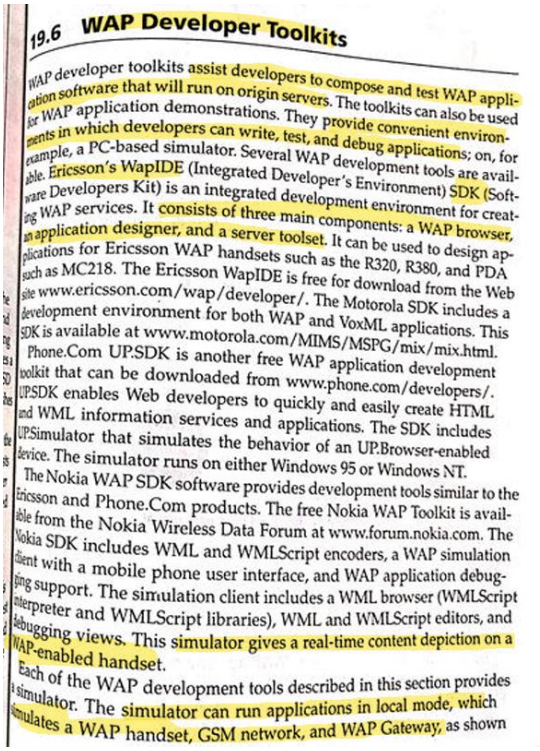
- **Step 8.** After the gateway MSC receives the MSRN in Step 7, the SS7 ISUP message IAM is sent to the target MSC.
- **Steps 9-11.**
  - The target MSC does not have the LAI info of the MS.
  - In order to proceed to set up the call, the MSC sends the message MAP_SEND_INFO_FOR_INCOMING_CALL to the VLR.
  - Unfortunately, the VLR does not have the LAI info either.
  - Hence the VLR asks the MSC to determine the LA of the MS by sending a MAP_SEARCH_FOR_MOBILE_SUBSCRIBER message.

VLR Record Restoration Initiation Event 3—MS Call Termination (4/4)

- **Steps 12 and 13.**
  - The MSC initiates paging of the MS in all LAs.
  - If the paging is successful, the current LA address of the MS is sent back to the VLR by the MAP_PROCESS_ACCESS_REQUEST message.
  - At this point, the location information of the VLR record is recovered.
- Note that
  - MAP_SEARCH_FOR_MOBILE_SUBSCRIBER is an expensive operation because every BTS connected to the MSC must perform the paging operation.
  - To avoid this "Wide Area Paging", the GSM system may periodically asks the MSs to re-register.

Unit-3:

1.WAP simulation environment



19.6 WAP Developer Toolkits

WAP developer toolkits assist developers to compose and test WAP application software that will run on origin servers. The toolkits can also be used for WAP application demonstrations. They provide convenient environments in which developers can write, test, and debug applications; on, for example, a PC-based simulator. Several WAP development tools are available. Ericsson's WapIDE (Integrated Developer's Environment) SDK (Software Developers Kit) is an integrated development environment for creating WAP services. It consists of three main components: a WAP browser, an application designer, and a server toolset. It can be used to design applications for Ericsson WAP handsets such as the R320, R380, and PDA such as MC218. The Ericsson WapIDE is free for download from the Web site www.ericsson.com/wap/developer/. The Motorola SDK includes a development environment for both WAP and VoxML applications. This SDK is available at www.motorola.com/MIMS/MSPG/mix/mix.html.

Phone.Com UP.SDK is another free WAP application development toolkit that can be downloaded from www.phone.com/developers/. UP.SDK enables Web developers to quickly and easily create HTML and WML information services and applications. The SDK includes UP.Simulator that simulates the behavior of an UP.Browser-enabled device. The simulator runs on either Windows 95 or Windows NT.

The Nokia WAP SDK software provides development tools similar to the Ericsson and Phone.Com products. The free Nokia WAP Toolkit is available from the Nokia Wireless Data Forum at www.forum.nokia.com. The Nokia SDK includes WML and WMLScript encoders, a WAP simulation client with a mobile phone user interface, and WAP application debugging support. The simulation client includes a WML browser (WMLScript interpreter and WMLScript libraries), WML and WMLScript editors, and debugging views. This simulator gives a real-time content depiction on a WAP-enabled handset.

Each of the WAP development tools described in this section provides a simulator. The simulator can run applications in local mode, which simulates a WAP handset, GSM network, and WAP Gateway, as shown

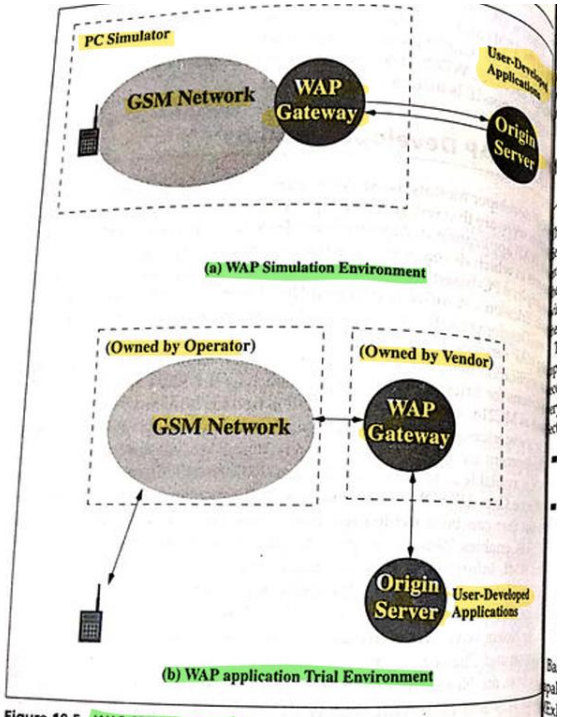


Figure 19.5 WAP SDK simulator.

in Figure 19.5(a). Furthermore, these vendors also provide free access of their WAP Gateways, so that WAP application developers are able to test a complete set of WAP-enabled services and APIs. As shown in Figure 19.5(b)

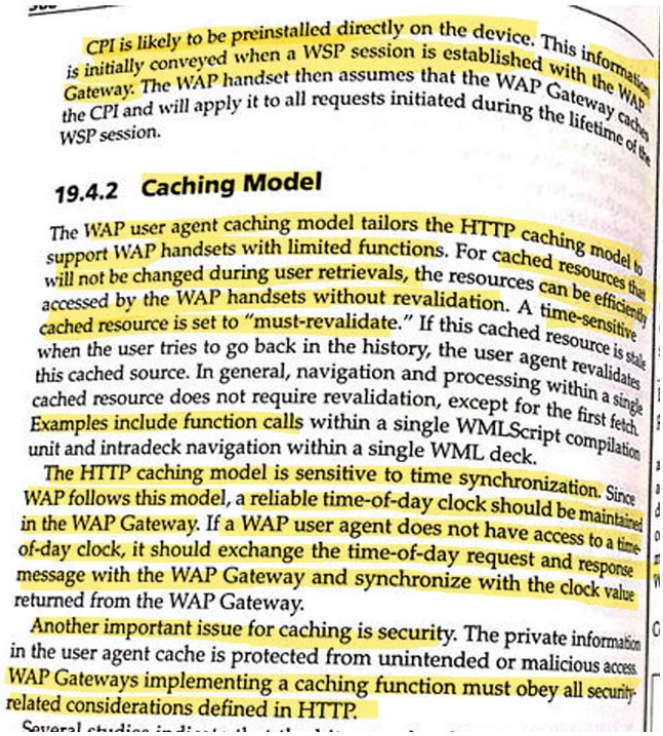
2.User agent profile

19.4.1 User Agent Profile

Existing markup language contents are designed for PCs with large displays and large memory capacities. Under the existing Internet technologies, WAP handsets may not be able to store and display the received contents. To resolve this issue, WAP specifies the User Agent Profile (UAProf), also known as Capability and Preference Information (CPI), that allows content generation to be tailored based on the WAP handset's capabilities. The CPI consists of information gathered from the device hardware, active user agent software, and user preferences, which may include:

- Hardware characteristics, such as screen size, color capabilities, image capabilities, and manufacturer.
- Software characteristics, including operating system vendor and version, support for MExE (to be described in Section 19.7), and a list of audio and video encoders.
- Application/user preferences, such as browser manufacturer and version, markup languages and versions supported, and scripting languages supported.
- WAP characteristics, including WMLScript libraries, WAP version, and WML deck size.
- Network characteristics, such as device location, and bearer characteristics (e.g., latency and reliability).

3.Caching model



CPI is likely to be preinstalled directly on the device. This information is initially conveyed when a WSP session is established with the WAP Gateway. The WAP handset then assumes that the WAP Gateway caches the CPI and will apply it to all requests initiated during the lifetime of the WSP session.

19.4.2 Caching Model

The WAP user agent caching model tailors the HTTP caching model to support WAP handsets with limited functions. For cached resources that will not be changed during user retrievals, the resources can be efficiently accessed by the WAP handsets without revalidation. A time-sensitive cached resource is set to "must-revalidate." If this cached resource is stale when the user tries to go back in the history, the user agent revalidates this cached source. In general, navigation and processing within a single cached resource does not require revalidation, except for the first fetch. Examples include function calls within a single WMLScript compilation unit and intradeck navigation within a single WML deck.

The HTTP caching model is sensitive to time synchronization. Since WAP follows this model, a reliable time-of-day clock should be maintained in the WAP Gateway. If a WAP user agent does not have access to a time-of-day clock, it should exchange the time-of-day request and response message with the WAP Gateway and synchronize with the clock value returned from the WAP Gateway.

Another important issue for caching is security. The private information in the user agent cache is protected from unintended or malicious access. WAP Gateways implementing a caching function must obey all security-related considerations defined in HTTP.

Several studies in

Unit-5

11.1 Security threats to wireless networks

As mentioned earlier, wireless networks are vulnerable to many more security threats than tra... tional wired networks. These are as follows:

1. **Accidental attack:** This gives rise to exposure due to frequent failure of devices and comp... nents, because of their small sizes and capabilities.
2. **Passive attack:** Here, the goal of the intruder is only to monitor or get information that ... being transmitted. Attacks may include releasing message content or traffic characteristics. Since no data are altered, passive attacks are difficult to detect.
3. **Active attack:** In this type of attack, modification of data or false data transmission takes place. (man-in-the-middle attack) giving rise to masquerade or replay. Denial of service (DoS) is possible where there is either temporary prevention of communication facilities or disruption of the entire network. This is done by flooding it with a large number of messages to degrade the performance of the system.
4. **Unauthorized usage:** This attack takes place because of the growing use of the Internet, which leaves the network vulnerable to hackers, viruses and intruders. It can be prevented by using proper user authentication techniques.
5. **Broadcast based:** As mentioned earlier, an eavesdropper is able to tap the communication into the wireless communication channels, by positioning itself within transmission range.
6. **Device vulnerability:** Mobile devices can be hijacked easily, and if secret IDs or codes are embedded in the device, hackers may get access to private information stored on it and to other network resources.
7. **Heterogeneity:** Mobile nodes need to adjust to potentially different physical communication protocols as they move to different locations.
8. **Resource depletion/exhaustion:** In mobile systems, resources like processing power and battery life are very limited. Hence, techniques such as public key cryptography cannot be used during normal operations to conserve power.

   The device may also be left open to an attack that reduces the normal lifespan of the battery. A DoS attack may consume and waste all the power in the battery, leaving the unit unable to function. In ad hoc networks, these attacks can cause routing nodes in the network to fail, making the network partially unreachable.
9. **Detectability:** Mobile systems used in the military do not want to be detected. Even if strong encryption is being used and the data cannot be deciphered, just detecting the signal puts the mobile user at risk if its position can be located. The device can be jammed by local radio frequency (RF) interference or the user attacked.
10. **Theft of service:** It is very easy to install wireless LANs by just taking them 'out of the box' and by plugging them into the network so that they work. In such systems, security settings are either disabled by default or factory-set default passwords are commonly known. Unauthorized, nearby users, malicious or otherwise, can get a dynamically assigned Internet protocol (IP) address and connect to the Internet.
11. **War driving/walking:** This is like the popular war game called war dialing, which was an earlier technique for searching phone numbers with modems attached to them. As wireless LANs gain popularity, hackers can find them by just taking a notebook computer or pocket PC fitted with a wireless card and some detection software like **netstumbler, kismet, airsnort,** etc., an optional global positioning system (GPS) and driving/walking around the city. This information is then used to build a network from the identified APs.

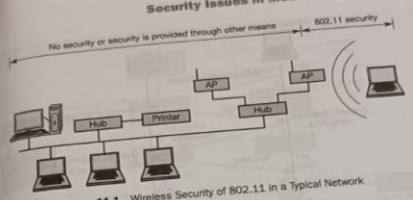


Figure 11.1 Wireless Security of 802.11 in a Typical Network

11.2 IEEE 802.11 security through WEP

This section discusses the built-in security features of 802.11. The IEEE 802.11 specification identified several services to provide a secure operating environment. The security services are provided by the wired equivalent privacy (WEP) protocol to protect link-level data during wireless transmission between clients and APs. WEP does not provide end-to-end security. Only the wireless portion of the connection is made secure, as shown in Figure 11.1. WEP is discussed in detail below.

11.2.1 WEP security features of 802.11 wireless LANs

IEEE defines three basic security services of authentication, confidentiality and integrity for WLANs as given in Karygiannis and Owens (2002). These are given in detail below:

11.2.1.1 *Authentication*

When wireless users attempt to gain access to a wired network, they must first be validated to make sure they are who they claim to be. This is called authentication. The IEEE 802.11 specification provides for two types of authentication—open-system authentication and shared-key authentication. The highlights of these are shown in Figure 11.2 as a taxonomy.

In **Open System authentication**, a client station exchanges messages with an access point (AP). The AP sends a query as a 'challenge' to the station. If the station sends the correct

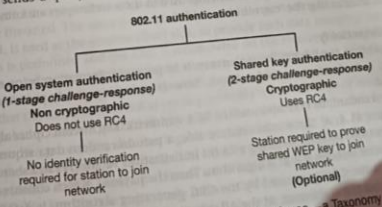


Figure 11.2 802.11 Authentication Techniques—a Taxonomy

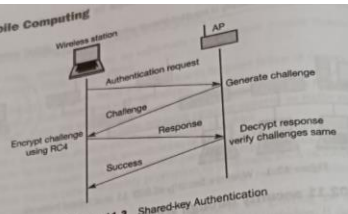


Figure 11.3 Shared-key Authentication

'response', i.e., the correct MAC address fields, it is considered authenticated. Note that there is no cryptographic validation here. Hence open-system authentication is highly vulnerable to unauthorized access and attack. The 802.11 specification only requires this type of 'authentication'. However, this technique cannot be really called authentication, as the AP accepts the mobile station without verifying its identity.

In **Shared key authentication**, another basic 'challenge-response' technique is used which is based on cryptography. In this scheme, shown in Figure 11.3, a random challenge (or nonce) is generated by the AP and sent to the wireless client. The client uses a cryptographic key that is shared with the AP to encrypt the challenge and returns the result to the AP. The AP decrypts the result and if the decrypted value is the same as the random challenge it had sent, it allows access. The 128-bit challenge text is generated using the RC4 symmetric key, stream cipher algorithm as given in Tanenbaum (2002). Unlike open-key authentication, shared key authentication is optional in the IEEE 802.11 specification.

Both the above authentication methods have limitations. Firstly, they do not provide mutual authentication, i.e., the AP authenticates the wireless client, but the client does not authenticate the AP. The mobile station must trust that it is communicating with a legitimate AP. Secondly, the simple challenge-response schemes used in these techniques are known to be weak and suffer from attacks like the 'man-in-the-middle' attack.

11.2.1.2 *Confidentiality*

The aim of providing confidentiality, or privacy, is to prevent information being eavesdropped during transfer, as is done in a wired network. Eavesdropping is a purely passive attack which must be avoided.

The 802.11 standard for WEP also uses the RC4 symmetric key, stream cipher algorithm as is shown in Figure 11.4. At the wireless station side, a pseudo-random data sequence, called 'keystream', is obtained by concatenating a 24-bit Initialization Vector (IV) to a shared 40-bit key and passing the same through the RC4 algorithm. Then the payload, which consists of the plaintext, together with the CRC generated by the CRC generating algorithm, is X-ORed with the keystream to generate the ciphertext. At the AP side, the procedure is performed in reverse to get back the plaintext.

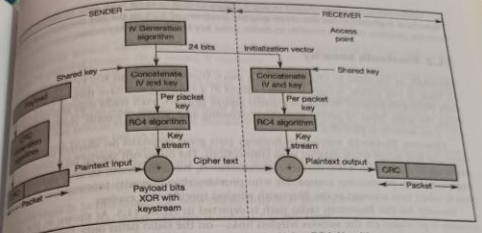


Figure 11.4 WEP Privacy and Integrity Using RC4 Algorithm

In this way, data can be protected from eavesdropping, during transmission over the wireless ... using WEP. WEP is applied to all data above the 802.11 WLAN layers to protect Transmission ... Protocol/Internet Protocol (TCP/IP), Internet Packet Exchange (IPX) and Hyper Text ... Protocol (HTTP) traffic.

The 802.11 standard WEP supports only a 40-bit cryptographic keys size for the shared key, ... nonstandard extensions of WEP that support key lengths upto 104 bits are also prevalent. It ... be noted that increasing the key size increases the security of a cryptographic technique.

11.2.1.3 *Integrity*

Another goal of WEP is to ensure that data/messages between the wireless clients and the AP are ... modified in transit in an active attack, i.e., their 'integrity' is not compromised. The IEEE ... specification provides such a data integrity service so that an active adversary 'in the mid- ... can be thwarted. The same procedure that is used for providing confidentiality, as shown in ... 11.4, is used at the wireless client side, to provide such data integrity. At the receiving AP, ... is performed and the CRC is recomputed on the received message. This is compared ... the one computed with the original message. If the CRCs do not match, this indicates an ... violation and the packet is discarded.

Note that the simple CRC is not as cryptographically secure as a hash or message authentication ... (Tanenbaum, 2003). The IEEE 802.11 specification also does not provide for key management ... like generating, distributing, storing, loading, etc. of keys. Keys must either be pre- ... by the manufacturer or exchanged in advance over a wired backbone network. The base station ... the mobile station could also choose a random key and send it over the air, encrypted with ... other's public key. Such keys generally remain stable for months or years.

The main drawback of the WEP algorithm is that the same key is shared by all wireless clients ... there is no way to distinguish one from another. Also all users can read each others' data.

These drawbacks have resulted in many instances of attacks on [illegible], or the fact that many of the keys have the property that it is possible to derive some key bits from the keystream. These have exploited either the cryptographic weakness of RC4,

11.3 Bluetooth security

Bluetooth, as discussed in Chapter 2, has a much shorter range than 802.11, but security is still an issue. If two people occupy adjacent offices in a building and have their mobiles equipped with Bluetooth-enabled wireless keyboards and/or printers, each could read and capture everything the other types or prints, including incoming and outgoing e-mails, confidential reports, etc., if no security is provided.

However, Bluetooth wireless technology puts great emphasis on wireless security so that users can feel secure while making their connections. The Bluetooth Special Interest Group (SIG), made up of more than 4,000 member manufacturers, has a Bluetooth security experts group of engineers from its member companies who provide critical security information and feedback that is taken into account as the Bluetooth wireless specification evolves.

Security for the Bluetooth radio path is depicted in Figure 11.5. As shown in the diagram, security is provided on the various wireless links—on the radio paths only. Link authentication and encryption is provided, but end-to-end security is not possible without providing higher-layer security solutions on top of Bluetooth. In the example provided, security services are provided between the personal digital assistant (PDA) and the printer, between the cell phone and the laptop, and between the laptop and the desktop.

The three basic security services defined by the Bluetooth specifications are briefly discussed below:

- **Authentication:** Identity verification of communicating devices is the first goal of Bluetooth. This security service addresses the question, 'Do I know with whom I am communicating'? An abort mechanism is provided if the device cannot authenticate itself properly.
- **Confidentiality:** Confidentiality, or privacy, is the second security goal of Bluetooth. The requirement is to prevent passive attacks on information, like eavesdropping. This security service addresses the question, 'Are only authorized devices allowed to view my data'?

Authorization: The third goal of Bluetooth is to allow the control in the use of system resources. This security service addresses the question, 'Is this device authorized to use the requested resource'?

Other security services such as audit and non-repudiation are provided in Bluetooth, and must be provided through other means, if necessary.

Bluetooth uses a frequency-hopping scheme with 1,600 hops/second combined with power control at the radio link to limit the transmit range. These features provide Bluetooth with some protection from eavesdropping and malicious access. The frequency-hopping scheme, which is a technique to avoid interference, makes it difficult for an adversary to locate the Bluetooth transmission. The power control feature makes it necessary for a potential adversary to be close to the Bluetooth network to carry out an attack.

Three modes of security are provided in Bluetooth for implementing the above security services. These are determined by the product or device manufacturer. These modes are as follows:

SecurityMode1: This is a non-secure option

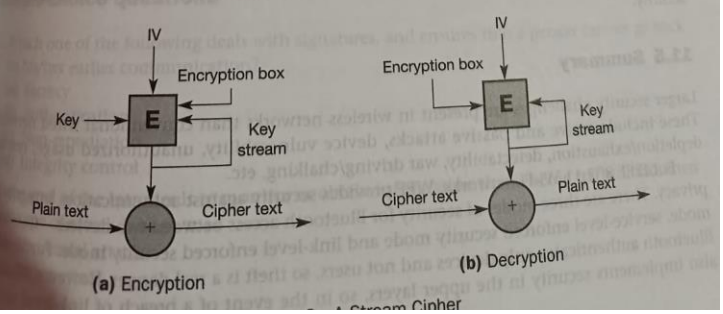
SecurityMode2: In this mode, the enforced security is at service level

SecurityMode3: In this mode, security is enforced at link level

Devices and services also have different security levels. For devices, there are two levels—trusted device and untrusted device. A trusted device, having been paired with one's other device, has unrestricted access to all services. Regarding services, three security levels are defined—services that require authorization and authentication, services that require authentication only and services that are open to all devices.

Bluetooth security starts when a newly arrived slave asks for a channel with the master. The two devices have a shared secret key in advance, which may be hardwired by the manufacturer (for a headset and mobile sold as a unit), or the headset may have a hardwired key and the mobile user may have to enter it in the device as a decimal number. These shared keys are called passkeys.

To establish the channel, the slave and the master each check to see if the other has the passkey and then negotiate whether the channel will be encrypted or integrity will be controlled or both. A random 128-bit session key is then selected. Encryption uses the E0 stream cipher shown in Figure 11.6. The plaintext is XORed with the keystream to generate the ciphertext as shown.



Stream Cipher

Unit-4:please prepare all the topics from the text book.

https://books.google.co.in/books?id=r_cPHw04I0QC&printsec=frontcover#v=onepage&q&f=false