The DECT Standard

Introduction to DECT standardisation

The members of the European Telecommunications Standards Institute (ETSI) have developed the DECT standard. In ETSI Sub Technical Committee Radio Equipment and Systems 03 (STC RES-03), European telecommunications equipment manufacturers, system operators and regulators work together on the definition and evolution of the DECT standards.

In addition to ETSI, several other bodies are involved in the DECT standardisation process.

The Commission of the European Community provides considerable support by providing the legislation needed to establish (in conjunction with CEPT ERC) a common frequency allocation and (in conjunction with the ACTE committee) by enabling European wide harmonisation of the regulatory environment for DECT products.

After the first edition of the DECT standard was available in 1992, the DECT standardisation work concentrated on the definition of the Generic Access Profile (GAP) and other interworking profiles (DECT/GSM, DECT/ISDN, DECT/Radio Local Loop, CTM and several data profiles). This work and additional demands from the DECT market initiated several extensions and enhancements to the base standard enabling even more effective application of DECT products which led to the 2nd edition of the base standard being finalised by the end of 1995. Some examples of this are:

- inclusion of emergency call procedures to aid acceptance of DECT for public access applications,
- definition of the Wireless Relay Station (WRS) as a new system component to enable more cost efficient infrastructures and
- description of the optional direct portable to portable communication feature for DECT.

The DECT common interface standard has a layered structure and is contained in ETS 300 175, Parts 1 to 8 [1] to [8]. It is a comprehensive set of requirements, protocols and messages providing implementers with the ability to create network access profiles (protocol subsets) to be able to access virtually any type of telecommunications network.

To stimulate interoperability between DECT equipment from different manufacturers ETSI members started to work on the definition of standard interworking profiles by the end of 1993. The Generic Access Pro-file GAP [9] was the first profile, completed in 1994. It contains the protocol subset required for the basic telephony service in residential cordless telephones, business wireless PABX, and public access applications; it provides the basis for all other DECT speech profiles. Interoperability testing for GAP has been finished successfully.

Part	Title	Description
1	Overview	General introduction to the other parts of ETS 300 175
2	Physical layer	Radio requirements of DECT, e.g. carrier frequency allocation, modulation method, transmission frame structure, transmitted power limits, spurious emission requirements etc.
3	Medium Access Control Layer	Description of procedures, messages, and protocols for radio resource man-cess Control agement i.e. link set-up, channel selection, handover, link release and link layer quality maintenance etc.
4	Data Link	Description of provisions to secure a reliable data link to the network layer Control layer
5	Network layer	Description of the signalling layer with call control and mobility management functions and protocols.
6	Identities and Adressing	Description of the portable and fixed part identities requirements for all Addressing DECT application environments.
7	Security aspects	Procedures to prevent eavesdropping, unauthorised access and fraudulent use. pects
8	Telephony	Telephony requirements for systems supporting the 3.1 kHz speech service to ensure proper interworking with public telecommunications networks. De-fines transmission levels, loudness ratings, sidetone levels, frequency re-sponse, echo control requirements etc.

Table 1. Parts 1 to 8 of the DECT CI standard ETS 300 175

Basic Operating Principles

The principles as applied in the DECT standard have been designed to meet the following objectives:

- high capacity cellular structured network access
- allowing for network wide mobility
- Flexible and powerful identities and addressing
- high spectrum efficiency
- reliable - high quality and secure - radio access
- robustness even in hostile radio environments
- speech transmission quality comparable to the wired telephony service
- enabling cost efficient implementations of system components
- allowing for implementation of a wide variety of terminals like e.g. small pocketable handsets
- flexibility towards varying bandwidth needs (which is bandwidth on demand e.g. for ISDN and data applications)

Furthermore, the standard reflects a high degree of flexibility in the protocols to enable future extension.

Mobility

Although network-wide mobility is outside the scope of the DECT standard, the mobility functions in the DECT standard provide the ability to access the mobility capabilities of telecommunications networks through a (multi) cellular infrastructure giving tremendous flexibility to users roaming across their residence or business site.

Wireless users with authorised access to the network (subscribed users) can make and receive calls at any location covered by the DECT infrastructure (if the infrastructure supports mobility) and move around in this area even when in active communication. When the radio channel is interfered, the seamless handover capability of DECT assures an unnoticeable escape to a newly selected non-interfered radio channel.

The MC/TDMA/TDD principle

The DECT radio interface is based on the Multi Carrier, Time Division Multiple Access, Time Division Duplex (MC/TDMA/TDD) radio access methodology. Basic DECT frequency allocation uses 10 carrier frequencies (MC) in the 1880 to 1900 MHz range. The time spectrum for DECT is subdivided into timeframes repeating every 10 ms. Each frame consists of 24 timeslots each individually accessible (TDMA) that may be used for either transmission or reception. For the basic DECT speech service two timeslots - with 5 ms separation - are paired to provide bearer capacity for typically 32 kbit/s (ADPCM G.726 coded speech) full duplex connections. To simplify implementations for basic DECT the 10 ms timeframe has been split in two halves (TDD); where the first 12 timeslots are used for FP transmissions (downlink) and the other 12 are used for PP transmissions (uplink).

The TDMA structure allows up to 12 simultaneous basic DECT (full duplex) voice connections per transceiver providing a significant cost benefit when compared with technologies that can have only one link per transceiver (e.g. CT2). Due to the advanced radio protocol, DECT is able to offer widely varying bandwidths by combining multiple channels into a single bearer. For data transmission purposes error protected net throughput rates of n x 24 kbit/s can be achieved, up to a maximum of 552 kbit/s with full security as applied by the basic DECT standard.

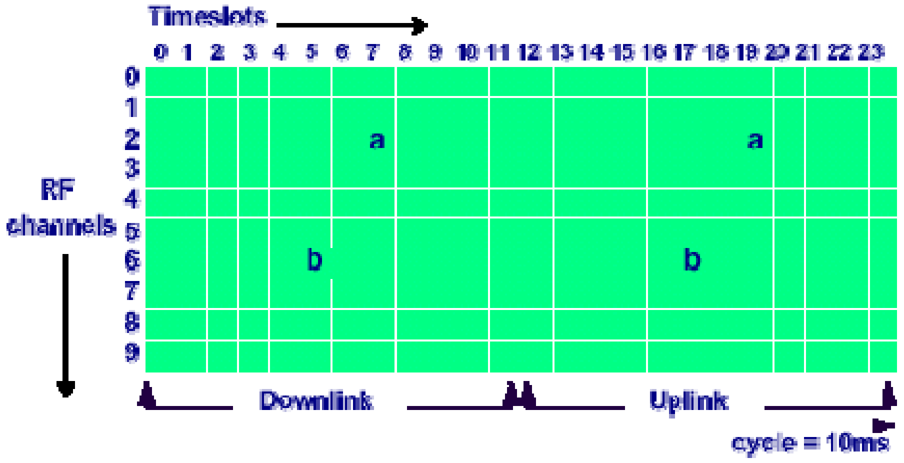

Figure 4. The DECT frequency/time spectrum

Use of the radio spectrum

Using the MC/TDMA/TDD principle for basic DECT (utilising both frequency and time dimensions) a total spectrum of 120 duplex channels is available to a DECT de-vice at any instant location. When adding the third dimension (space) to the principle -given the fact that the capacity of DECT is limited by interference from adjacent cells and Carrier over Interference ratios of C/I = 10 dB can be achieved - a very low channel reuse factor (1) can be obtained. Different communication links in adjacent cells can use the same channel (frequency/timeslot combi-nation. Therefore dense packing of DECT base stations (e.g. at a distance of 25 m in an ideal hexagonal coverage model) will allow for a traffic capacity of the basic DECT tech-nology up to approx. 10000 Erlang/km 2 /floor (see Note 1 below) without the need for fre-quency planning. Installation of DECT is reasonably simple since one only needs to consider radio coverage and traffic needs. Note 1: 1 Erlang represents an average traffic load caused by one basic DECT speech connection -using one frequency/timeslot pair - for 100% of time.

Continuous broadcast service

A DECT base station is continuously transmitting on - at least - one channel, thus providing a beacon function for DECT portables to lock-on to. The transmission can be part of an active communication link with a portable or a dummy bearer transmission. The base station's beacon transmission carries broad-cast information - in a multi-frame multiplexed structure - on base station identity, system capabilities, RFP status and paging information for incoming call set-up. Port- ables locked-on to a beacon transmission will analyse the broadcast information to find out if the portable has access rights to the system (only portables with access rights are allowed to set-up a communication link), determine whether system capabilities match with the services required by the portable and - if a communication is required - whether the base station has free capacity for a radio link with the portable.

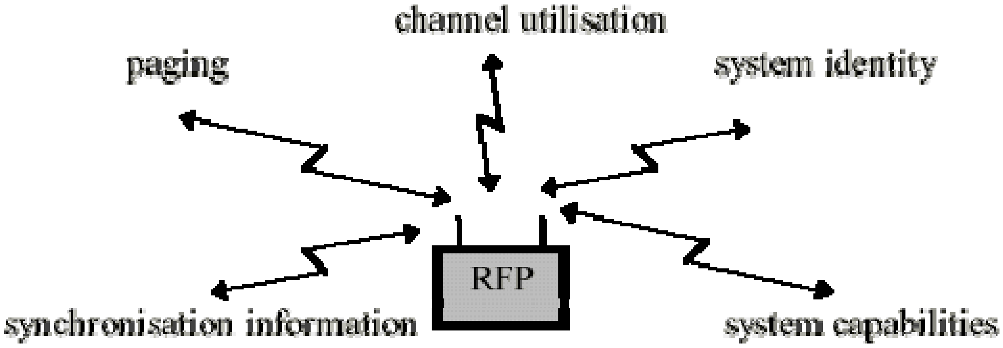

Figure 5. The DECT fixed part beacon function

Dynamic Channel Selection and Allocation

DECT features continuous Dynamic Chan-nel Selection and Allocation. All DECT equipment is obliged to regularly scan - its local radio environment - at least once every 30 seconds. Scanning means receiving and measuring local RF signal strength on all idle channels. Scanning is done as a background process and produces a list of free and occu-pied channels (RSSI list; RSSI = Received Signal Strength Indication), one for each idle timeslot/carrier combination, to be used in the channel selection process. An idle time-slot is (temporarily) not in use for transmis-sion or reception. Within the RSSI list, low signal strength values represent free and non-interfered channels, while high values repre-sent busy or interfered channels. With the aid of the RSSI information, a DECT PP or FP is capable of selecting the most optimal (least interfered) channel to set-up a new commu-nication link.

In a DECT portable part, the channels with highest RSSI values are continuously ana-lysed to check if the transmission originates from a base station to which the portable has access-rights. The portable will lock onto the strongest base station, as mandated by the DECT standard. Channels with lowest RSSI value are used to set-up a radio link with the base station if the portable user decides to establish a communication or when an in-coming call is signalled to the portable through the reception of a paging message.

In a DECT base station the channels with low RSSI values are used when selecting a channel to set-up a beacon transmission (dummy bearer).

The Dynamic Channel Selection and Alloca-tion mechanism guarantees that radio links are always set-up on the least interfered channel available.

Call set-up

Portable user originated call set-up

The initiative to set-up radio links in basic DECT applications is always taken by the portable part. The portable selects (using its Dynamic Channel Selection) the best channel available for set-up, and accesses the fixed part on this channel. To be able to detect the PP's set-up attempts the fixed part must be receiving on the channel when the PP transmits its access request. To allow portables to use all 10 DECT RF carriers, the fixed part continuously scans its idle receive channels for portable setup attempts in a sequential way. Portables synchronise to this sequence by means of the information transmitted through the FP continuous broadcast service. From this information portables can deter-mine the exact moment when successful ac-cess the FP is possible on the selected chan-nel.

Network originated call set-up

When a call comes in for a DECT portable, the access network will page the portable by sending a page message - containing the PP's identity - through its continuous broadcast service. A portable receiving a paging mes-sage with its identity included will set-up a radio link - to serve the incoming call - using the same procedure as used for the PP origi-nated link set-up.

Handover

Due to the powerful Dynamic Channel Se-lection and Allocation and seamless handover capabilities of DECT, portables can escape from an interfered radio connection by estab-lishing a second radio link - on a newly se-lected channel - to either the same (intracell handover as shown in figure 6) or to another base station (intercell handover as shown in figure 7). The two radio links are temporarily maintained in parallel with identical speech information being carried across while the quality of the links is being analysed. After some time the base station determines which radio link has the best quality and releases the other link.

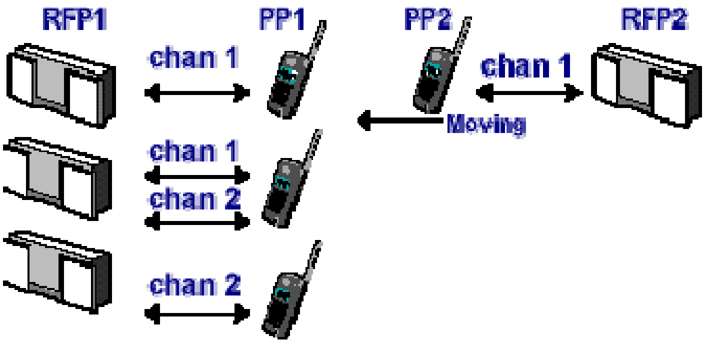

Figure 6. The DECT intracell handover function

If the DECT portable is moving from one cell area into another, the received signal strength - as measured by the portable's Dynamic Channel Selection and Allocation functions - of the base station will reduce gradually. The signal strength of the base station serving the cell towards which the portable is moving will gradually increase. At the moment the new base station's signal becomes stronger than the signal from the old base station, a seamless handover (as described above) will be performed to the new base station (see figure 7.). The seamless handover is a fully autonomous initiative from the DECT portable part, which the user will not notice. Although a handover is always initiated by the DECT portable part, it may also be the uplink (from PP to FP) that suffers from poor quality. For this case, DECT has signalling protocols that enable the fixed part to signal the perceived link quality to the PP, that can subsequently initiate the handover.

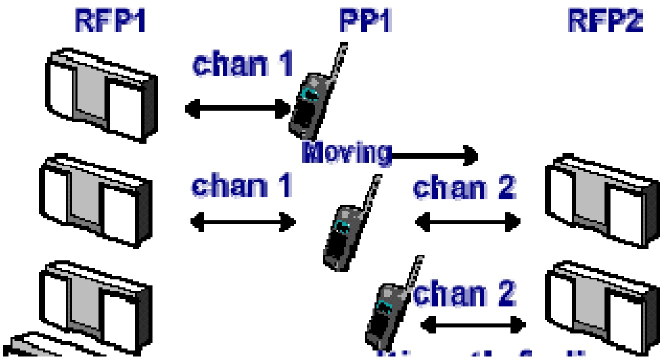

Figure 7. The DECT intercell handover function

Diversity

Handover in DECT is a mechanism to escape from interfered or channels with low signal level. Handover is however not sufficiently fast to counteract fast fading situations. For this purpose the DECT base station can be equipped with antenna diversity (see figure 8). A signalling protocol is available in the standard to control FP antenna diversity from the portable. Due to the TDD nature (symmetry) of the radio link between the FP and PP, the FP antenna diversity not only improves the uplink quality but also the downlink quality, at slow speed.

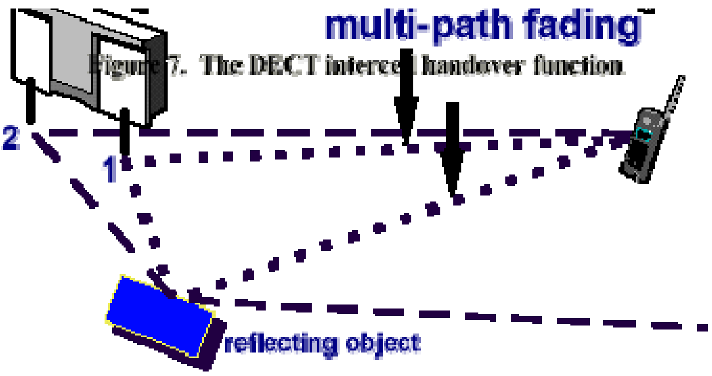

Figure 8. Antenna diversity from 1 to 2

Coexistence

The coexistence properties of radio access technology mainly rely on the ability to escape (handover) - in the frequency domain -from the interfered radio link, not relying on information transferred over the original (interfered) channel. MC/TDMA/TDD, continuous Dynamic Channel Selection and Allocation and the handover procedures in the DECT standard show excellent coexistence properties even under heavy interference conditions.

Security

The use of a radio access technology providing mobility includes considerable risks with respect to security. The DECT standard provides the measures to counteract the natural security flaws that generally appear when applying cordlessness. Effective subscription and authentication protocols have been included to prevent unauthorised access and an advanced ciphering concept provides protection against eavesdropping.

Subscription

The subscription process is the process by which the network opens its service to a particular portable.

The network operator or service provider provides the portable user with a secret subscription key (PIN code), that will be entered into both the fixed and the portable part before the procedure starts. Before the handset initiates the actual subscription procedure it should also know the identity of the fixed part to subscribe to (for security reasons the subscription area could even be limited to a single designated - low power - base station of the system). The time to execute the procedure is usually limited and the subscription key can only be used once, this to further minimise the risk of misuse. Subscription in DECT can be done “over the air,“ a radio link is set-up and both ends verify that they use the same subscription key. Handset and network identities are exchanged, and both sides calculate a secret authentication key to be used for authentication at every call set-up. The secret authentication key is not transferred over the air.

A DECT portable may have multiple subscriptions. With every subscription session, the portable will calculate a new secret authentication key associated with the network to which it subscribes. New keys and network identities are added to a list - kept in the portable - which is used in the locking process. Portables will only lock to a network where it has access rights (network identity is contained in the list).

Authentication

Authentication of a handset may be done as a standard procedure at every call set-up. During the authentication session, the base station checks the secret authentication key without sending it over the air. The principle for hiding the identity information in the air is as follows: the base station sends a random number to the handset that is called the ‘challenge’. The handset calculates a ‘response’ by combining the authentication key with the random information and transmits the ‘response’ to the base station. The base station also calculates the expected ‘response’ and compares it with the received ‘response’. Figure 9 illustrates the authentication mechanism. The comparison results into a continuation of the call set-up or a re-lease. If somebody is eavesdropping on the air interface, in order to steal the authentication key he needs to know the algorithm to recalculate the key from the ‘challenge’ and the ‘response’. This ‘reverse’ algorithm demands for a huge amount of computing power. So the cost of retrieving the key by eavesdrop-ping of the authentication procedure is made extremely high.

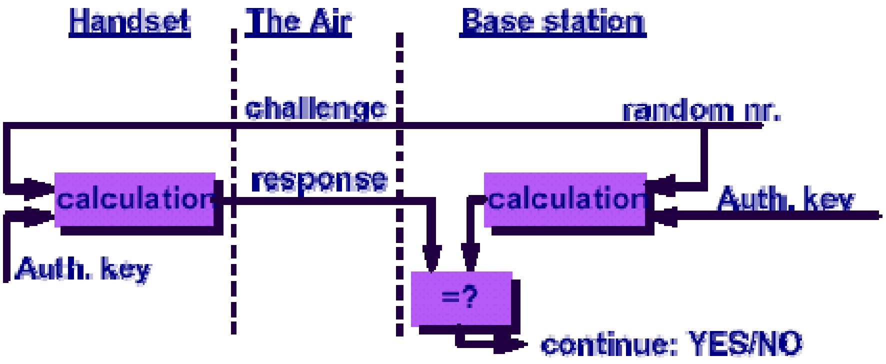

Figure 9. DECT authentication : challenge and response

Encryption

The authentication process uses an algorithm to calculate the ‘response’ from a ‘challenge’ and the authentication key in handset and base station. This is in fact a way to send the identity of the user in an encrypted form over the air in order to preventing theft of the identity. Looking at user data (e.g. speech) the same principle can be applied. During authentication, both sides also calculate a cipher key. This key is used to cipher the data sent over the air. At the receiving side the same key is used to decipher the information (see figure 10.). In DECT, the ciphering process is part of the standard (however not mandatory).

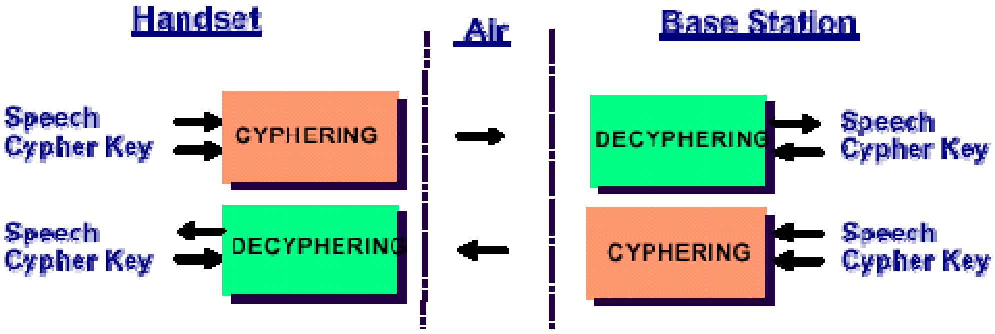

Figure 10. The DECT cyphering function