

November 29, 2000

Log #: PN-0002

Signaling Security and Speech Encryption DCT1900

Introduction

Because the DCT1900 system utilizes radio as a transport media, there is often much concern and speculation about the communications security provided by such a technique. This document gives a general overview of the architecture and procedures that are used to provide an extremely high level of security for signaling and speech transmission in the system. This document is also applicable for submission to regulatory agencies that often require technical explanations regarding this topic.

General

The DCT1900 Digital Cordless Telephone System provides full security for telephone conversations, within the system (which can consist of thousands of subscribers) and against external systems (DCT1900 or other vendors) or intentional malicious eavesdroppers. This is accomplished through several mechanisms. Unlike traditional analog cordless telephone RF signals, which are quite easy to spectrally locate, analyze and demodulate back into voice band speech, the DCT1900 system utilizes a digital radio transport between the Base Station equipment and the Portable Telephone. As a result of using digital technology, the opportunity for secure communications is much greater. In DCT1900, security is implemented in three major ways:

- System Architecture – It is practically impossible to ‘eavesdrop’ on a conversation due to the complexity of the multiple carrier, time-division multiplexed, time division duplexed (MC/TDMA/TDD) system architecture, which utilizes dynamic channel allocation.
- Portable Telephone Authentication – Portable Technical Numbers and System Numbers are programmed into the Portable Telephones. This method logically identifies them and prevents the possibility of accidental access to other subscriber lines and other systems.
- Crypto Algorithm – A unique user independent ‘key’ is generated for each new call, and a hardware encryption/decryption process is applied to the digital speech bits, making eavesdropping virtually impossible.

System Architecture

Analog voice signals are immediately coded into a standard Adaptive Differential Pulse Coded Modulation (ADPCM) 32 Kb/s digital bit stream. This bit stream is then encrypted before transport over the air-interface to the far end of the system where the process is reversed until the analog voice signal is recovered. This entire process makes it nearly impossible for eavesdropping because it requires proper ‘framing’ to the bit stream and decoding it back into an analog signal using the proper ADPCM codec. To add to this complexity, the air-interface carries not just one of these signals, but up to eight that are multiplexed together using time-division multiplex techniques with bi-directional transmission achieved through time-division

November 29, 2000

Log #: PN-0002

duplexing the transmit and receive portions of the signal. Finally, through continuous dynamic channel allocation, the RF transport can be affected on any one of multiple different RF carrier frequencies and timeslots at any given point in time. To eavesdrop on the system would require a complete duplication of the technology and architecture, and the necessary crypto algorithm and 'key' to decode the speech data. The crypto key is unique and different for every DCT1900 Portable Telephone as described in the section 'The Crypto Algorithm' of this document.

In summary, this architectural security is accomplished by many 'layers' of increasingly difficult mechanisms.

1. Analog signals are immediately converted to digital bit stream 'packets' representing samples of the analog speech.
2. The bit-stream packet is encrypted using a sophisticated algorithm.
3. The encrypted packet drives an RF modulator for transport across the air on one of many available carrier frequencies during one of 24 available transmit 'timeslots', which are dynamically and continuously assigned during a call.

Portable Telephone Authentication

On an overall system basis, secure voice communication is ensured by the methods already described. Within the system, certain measures are also taken to ensure that the Portable Telephones have unique 'identities' so that they do not receive erroneous ringing, access the wrong line number, or the wrong system. (Different systems can often be co-located.) Each Portable Telephone is programmed with a Portable Technical Number. This is a number sequentially assigned by the system from a number field of 2^{12} during initialization of the Portable Telephone. Also, a Portable Telephone can be programmed to operate on up to 8 different DCT1900 systems, as might be necessary for different physical site locations, etc. within the same company. The System Number may be assigned from number field of 2^{16} combinations. This combination creates 2^{28} unique Portable Telephone identifiers.

In addition to these safeguards, an authentication key is used. This authentication key is never transmitted over the air. During the pre-call authentication process only mathematical residues based upon time variant one-way transforms of the authentication key are transmitted over the air. The result is that illegal calls from a pirate phone in a DCT1900 system are virtually impossible.

The programming for the system number and the Portable Technical Number is not possible by the individual user. The assignment to and programming of Portable Telephones for users is handled through the Cordless System Manager software utility connected to the DCT1900 system. This utility, operated under password control by responsible technical personnel, maintains a database of users, and their associated identification numbers and insures that duplicate numbers are not assigned. Newly delivered systems will not operate until this procedure has first been completed. The authentication process operates on a continuous basis whenever the Portable Telephone is communicating with the system.

November 29, 2000

Log #: PN-0002

If a user's Portable Telephone is lost or stolen, the responsible technical administrator can exclude it from the system to make sure no one can make 'illegal' telephone calls with it. This is accomplished by removing the Portable Technical Number from the system.

The Crypto Algorithm

The DCT1900 system contains a crypto system, which protects a conversation between the Portable Telephone and the Central Unit against eavesdropping. Each Portable Telephone is programmed with a unique subscriber 'key' which is built up from the unique Portable Technical Number and System Numbers described above. This key is used in a proprietary crypto-hardware circuit implementation to encrypt the 320 speech data bits (per packet) by generating a scrambled bit-sequence in that frame. The process is reversed at the opposite ends of the system to recover the original data.

Regulatory Standards Compliance

Regulatory agencies (such as the Federal Communications Commission in the U.S.) require the incorporation of circuitry and techniques in cordless telephone systems to provide network access and signaling security. This Product Note has shown that the DCT1900 system provides a sophisticated level of security and also includes additional features to ensure complete privacy of communications.

Through the techniques described above, it can be seen that the DCT1900 system fully complies (and exceeds) the FCC Part 15.214 requirements for protection against unintentional access to the public switched telephone network by the base unit (Central Unit) and unintentional ringing by the handset (Portable Telephone). The signaling procedures that allow access to the telephone network or ringing of the handset are continuously preceded by transmission of digitally coded messages through the use of more than 2^{28} unique identities for each Portable Telephone. Access to the network can only occur when the code identity transmitted by handset matches that which is stored in the system. Similarly, ringing of the handset can only occur if the code transmitted by the system matches the identity of the handset. In accordance with the provisions of the FCC requirements, the unique codes are established through a combination of automatic sequential assignment of Portable Technical Numbers and the random assignment of System Numbers by responsible technical personnel using the Cordless System Manager software utility of the DCT1900 system. Until this structured procedure is executed, a newly delivered system and/or Portable Telephone will not function.

The DCT1900 is also UTAM compliant. UTAM Inc. (Unlicensed Transition and Migration) is responsible for monitoring the deployment of unlicensed base stations and handsets to avoid interference with other incumbent microwave operators. One of the safeguards of the UTAM deployment process is the use of a password that must be given by UTAM before a system can be energized. Furthermore, if power is removed from a DCT1900 system for more than 8 hours, the system will be disabled until a new password is received from UTAM. Thus, the compliance to UTAM offers an additional security safeguard against any unlawful or improper deployment of the DCT1900 system.