SECURE MOBILE RADIO COMMUNICATION OVER NARROWBAND RF CHANNEL

BY

WONG CHUN KAU, JOLLY

(黃振球)

A MASTER THESIS SUBMITTED IN PARTIAL FULFULMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF PHILOSOPHY

IN

DEPARTMENT OF ELECTRONIC ENGINEERING

THE CHINESE UNIVERSITY OF HONG KONG

HONG KONG

MAY 1992

ABSTRACT

This thesis presents an investigation on using digital processes and techniques to provide highly encrypted and paramilitary operated land mobile radio (LMR) communications over a narrowband UHF channel. A phenomenon of this century has been the dramatic growth of LMR for both civil and defence purposes. As a corollary, most governments have not been slow to recognize the potential value of exploiting design and development of paramilitary LMR systems particularly fit for the internal security and counter-terrorists, as a vital part of a nation's armoury. The functional, technical and operational requirements which determine the design of such a system are specified in this paper. Speech compression methods including both waveform coding and source coding are reviewed, and their performance together with implementation practicability are discussed. The importance of the type of modulation and encryption methods to be used in conjunction with the encoder is emphasised. The perspective concluded here is that robust linear predictive coding algorithms would be some pragmatic solutions in the future for digital secure voice transmission over narrowband radio channels in the light of rapid development of digital signal processing techniques and very large scale integrated (VLSI) circuits technology. Specifically, Code Excited Linear Prediction (CELP) with Line Spectral Pair (LSP) coefficients has shown considerable promise for good quality coding of speech at low bit rates with reduced complexity which is suitable for land mobile communications. Furthermore, to meet paramilitary requirements, non-error-propagating stream cipher encryption method with

pseudo-random hybrid synchronization plus a spectrally efficient narrowband digital FM like Gaussian-filtered minimum shift keying (GMSK) is proposed.

ACKNOWLEDGEMENT

I would like to thank my supervisor, Dr. P.C. CHING for his advice and support. Also, thanks are due to the following Units of Royal Hong Kong Police (RHKP) for their assistance in technical evaluation, operational field trials and speech quality assessment :-

Special Duties Unit	- Operations Department, RHKP
Counter Terrorism Unit	- Operations Department, RHKP
Special Project Section	- Communications Branch, RHKP
System Engineering & Research Division	- Communications Branch, RHKP
System Development Division	- Information Technology Branch, RHKP

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Land Mobile Radio (LMR) Communications

Mobile radio systems support their users with opportunities to move freely or halted at unspecified locations within the service area and simultaneously communicate with any other radio, telephone, fax, data modem, and electronic mail subscriber anywhere in the world. These systems allow users to determine their own locations; to track the precious cargo; to improve the management of fleets of vehicles and the distribution of goods; to enforce law and order regarding traffic safety; to provide vital communication links during emergencies, search and rescue operations, etc. All the above wireless communications are made possible by the unique property of the radio to employ an antenna for radiating and receiving electromagnetic waves.

When the user's radio antenna is stationary over a prolonged period of time, the term fixed radio is used. A radio transceiver capable of being carried or moved around, but stationary when in operation, is either called a transportable radio or a (handheld) portable radio, depending on its physical size. A radio transceiver capable of being carried (or sometimes fixed to) and used by a vehicle or by a person on the move is called mobile radio. Meanwhile, according to the location of the user, the terms land, maritime or space radio systems have been

used. The focus of this thesis is on land mobile radio (LMR) communications.

Land mobile radio is the oldest of the mobile communication technologies. It is interesting to note that the original LMR was introduced in 1921 to meet the need for a dedicated, fast and secure mobile communications service for the U.S. Detroit Police department car radio dispatch and other security functions [1] [2]. Notwithstanding its strong connection with the Police department in the past seventy years, to look forward, there will still be a dominant market for LMR in the security and public safety industries including police, fire and ambulance. These major users will definitely benefit from new LMR technologies such as software applications, networking and most importantly, digital radio.

Recently there has been extensive research studies [3] [4] about digital transmission in LMR systems. In particular, some experimental results on various speech coding algorithms related to the 900 MHz pan-European digital cellular mobile radio system have been actively reported [5] [6]. Efficient and effective utilization of the precious and limited frequency spectrum to give higher capacity is the prime driving force for the design of a spectrally efficient digital LMR communications system. Consequently, it is mandatory to develop a speech compression method which can provide good quality speech

at modest data rates. However, the application of many of these speech coding methods to a narrowband VHF/UHF mobile radio channel would lead to a significiant degradation in speech quality because of severe transmission errors caused by both multipath fading and co-channel interference (CCI) [3]. A narrowband modulation scheme is therefore necessary to utilize the limited frequency spectrum as efficiently as possible. Incidentally, bandwidth-efficient digital FM system with noncoherent demodulator is of significant interest, because fast multipath fading makes the use of coherent demodulation difficult, and because carrier frequency drift caused by the relatively unstable frequency oscillators used in handheld portable or mobile units precludes application of differential demodulation.

1.2 Paramilitary Communications Security

Police department mobile/portable radio has traditionally been implemented with analogue frequency modulation (FM). However, the modern security requirements asked for digital processing and modulation schemes. Two different forms of communications security equipment are currently available in the market and commonly used by Police; viz., analogue scrambling systems for low security requirement, and digital encryption systems for high security requirement. Technical principles of these two systems (analogue scrambling and digital encryption) are given in

the next sections. Amongst Police units, security personnel, special forces etc. handling sensitive information should not depend on analogue systems. It is widely felt that only digital voice encryption can offer excellent cryptological security to protect the communication from eavesdropping, even if very sophisticated equipment is used. This feature is, in fact, very decisive especially for custom radios for military or paramilitary operations.

For paramilitary applications, like the British Special Air Service (SAS) and Special Boat Squadron (SBS); the United States Special Naval Warfare Group (commonly known as SEAL); the Germany Grenzschutzgrippe 9 (G9); and locally, the Hong Kong Special Duties Unit (SDU), these are typical police special task forces which carried out some very high risk counterterrorist operations or VIP protection etc., teleconversations in the fields are probably of very sensitive nature and it is, therefore, necessary to warrant adequate and effective countermeasures against active cryptanalystic attacks from professional hostile interceptors who may be armed with technically advanced equipments. To this respect, secure mobile radio communication over narrowband UHF channel, in the range of 400 MHz, which is commonly used by police special task forces, has attracted numerous efforts from researchers and manufacturers. Obviously, the requirements for a low bit rate speech coder to be applied

in a paramilitary custom radio are much more stringent than that of a commercial cellular mobile radio in terms of reliability under very harsh operating conditions, severe environmental factors, recovered speech quality as well as robustness in high error rate transmission channels.

1.3 Voice scrambling method

To support police communications with minimum but essential security, most analogue voice scramblers incorporate either one of the following scrambling concepts :-

(a) Frequency dispersion (and inversion)

(b) Time inversion

(c) Time division scrambling

(d) Multi-level (-dimensional) scrambling

The chief advantage of using analogue voice scramblers is that the scrambled signal can be kept to the same bandwidth as the original clear voice [7] [8]. If this is the case, then the same transmission medium can be used for the scrambled signal as was used for the original clear voice signal. For all of the above listed scrambling methods, the outputs are analogue signals which are transforms of the original signals where these transforms normally take place in the frequency and/or time domains. Incidentally, the above scrambling methods are listed in ascending order of their security levels

which are measured in terms of the amount of residual intelligence (from the scrambled signals) available.

(a) **Frequency dispersion**

Frequency dispersion scrambler divides the typical speech frequency band into several sub-bands and then re-arranges them relative to each other. Sometimes the frequency dispersion technique is combined with the frequency inversion technique so that sub-bands are not only re-arranged but inverted as well. This is a principle in frequency dimension (domain). Fig. 1 illustrates the process of a frequency dispersion scrambler with physically realizable filters, of course, the frequency off settings will not be accurately geometrical focus but with a very small loss of intelligibility.

(b) **Time inversion technique**

This method inverts the temporal sequence of clear speech in the time domain. To illustrate the procedure with a very simplified example the word "office" would be converted into "eciffo". The typical time inversion is organized in frames of about 300 msec.

(c) **Time division scrambling**

The voice signal from the microphone is first digitized by a continuous variable slope delta

modulator. To obtain a high quality speech, the internal sampling rate is very high (e.g. 98 Kbit/sec). The serial digital data stream is temporarily stored in a random access memory (RAM) and divided into 16 equal segments each 20.83 msec long. During a period of 333 msec the 16 time segments are scrambled as function of the built in pseudo random generators and the stored permutations. The randomly distributed permutations are stored in an EPROM (erasable and electrically re-programmable read only memory). Each EPROM will store up to 1024 x 16 (16,384) permutations which are accessed by the built-in pseudo random generators for each scrambling period of 333 msec. The pseudo random generators are initiated by a secret n-digit external code and produce a continuous random data stream for a period in excess of six hours without repetition. Via a digital-to-analogue (D/A) converter the scrambled data stream is converted back into a quasi-analogue signal. This procedure is, by and large, very important to make it possible to transmit the scrambled signal through all normal radio transceivers and telephone lines with a minimum bandwidth of 2.7 KHz, where the length of the transmission path and the differential time delay is uncritical. The total time delay between transmitter and receiver station is approximately 666 msec.

(d) **Multi-level (-dimensional) scrambling**

As the above scrambling methods are regarded as low security standard, they may result a little to some residual intelligence to unauthorized eavesdroppers. Some manufacturers have proposed multi-level (or multi-dimensional) scrambling technique by incorporating all the above methods into a sophisticated scrambling concept. The input voice signal has firstly taken the time division scrambling. Independent from the time division scrambling, a second dimension of time inversion scrambling is then added. Since the human voice is very redundant, the time inversion process is destroying the understanding of the time division segments. Frequency dispersion as the third scrambling dimension is added to the signal. Similarly, independent from the two other processes, the frequency dispersion is to offset the frequency of the signal in several steps. These offset frequencies are controlled by the pseudo random generator and hence dynamically change for every segment. The offset timing is synchronized with the segments of the time division scrambling. Consequently, the frequency dispersion will destroy any phase information between segments of the time division scrambling. Following the three dimensional scrambling, the scrambled signal will be converted back into a pseudo analogue signal which has

practically very little residual intelligence and is possibly to be transmitted over analogue channels of any kind. This multi-level scrambling method has the least residual intelligence relative to all previous methods and is said to have fairly high security at the expense of more complex hardware design.

1.4 Digital Voice Encryption

Fig. 2 shows the principle of digital voice encryption where the digital bitstream from the voice coder is digitally ciphered with a manufacturer proprietary high security algorithm. The whole encryption depends on the Communication Key information which is entered by the user.

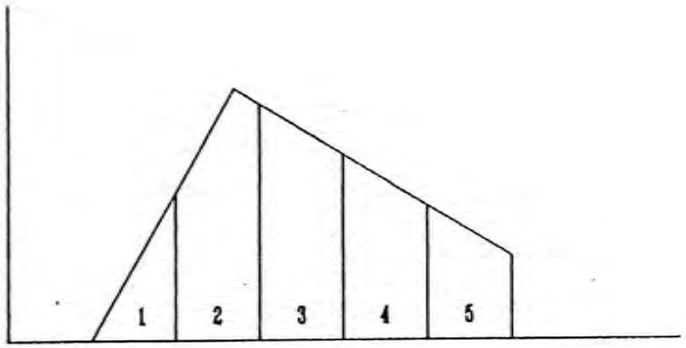
The advantages of digital voice encryption relative to analogue scrambling are obvious. First, it has no residual intelligence as against the analogue processing. Unauthorized eavesdropping without proper key information would end up listening to whitenoise like meaningless intelligence. Thus the digital voice encryption is regarded to have higher level of security than that of analogue scrambling. Also, transmission of digital voice will allow unlimited range with the help of repeaters which do not affect the voice quality.

1.5 Digital Secure LMR

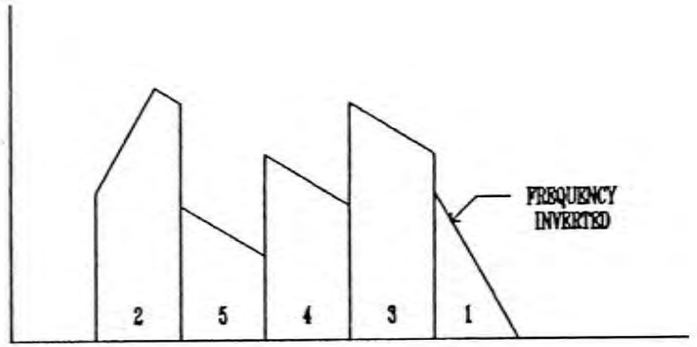
Unfortunately, the transition from traditional analogue to digital transmission creates some thorny problems. Since these digitally encrypted and paramilitary operated LMR systems have to coexist with the conventional ones, they have to comply with the same specifications on channel spacing and adjacent channel interference (ACI). Additional problems stem from the mobile radio channel which is characterized by frequency selective fading and fast variations in the data clock phase. So far, no definite conclusion has yet been reached regarding an optimum design of signal parameters, modulation and coding techniques that will provide sufficient robustness and high quality speech for a digital LMR system operating at low to medium data rate.

In this thesis, we propose the operational, functional and technical specifications which affect the design of a 400 MHz digitally encrypted paramilitary operated LMR system. Basic design considerations covering data rate and bit error rate (BER) requirements, channel and hardware characteristics, modulation design tradeoffs, precoding/decoding and pulse shaping, all at system level analyses, will be described. In next chapter, we shall firstly introduce the system concept, system model, and set out the expected design goals. In Chapter 3, a broad overview of the recent development of speech coding techniques on achieving quality speech, system coverage

and reliable performance necessary for a digital secure LMR communications system will be given. Subjective field testing to assess the performance of various coding methods against the specified requirements from the Special Duties Unit (SDU) of Royal Hong Kong Police (RHKP) is presented. In Chapter 4, we introduce the basic concepts of cryptology and cryptanalysis. Two major cryptographic concerns about digital encryption techniques and crypto synchronization requirement are discussed. Following description of the narrowband channel requirement, a survey on narrowband modulation schemes, together with a comparison between linear and constant envelope modulation and the combined development of speech and channel coding are introduced and analysed in Chapter 5. Chapter 6 sums up the technicalities of the previous chapters and promulgates implementation of the proposed system with highlights on the VLSI realization, crypto key management and some potential EMC problems. The final chapter serves to give a conclusion and throws some insights to the future development trends.



ORIGINAL VOICE SIGNAL



SCRAMBLED BY FREQUENCY DISPERSION

FIG. 1 PRINCIPLE OF SCRAMBLED FREQUENCY DISPERSION

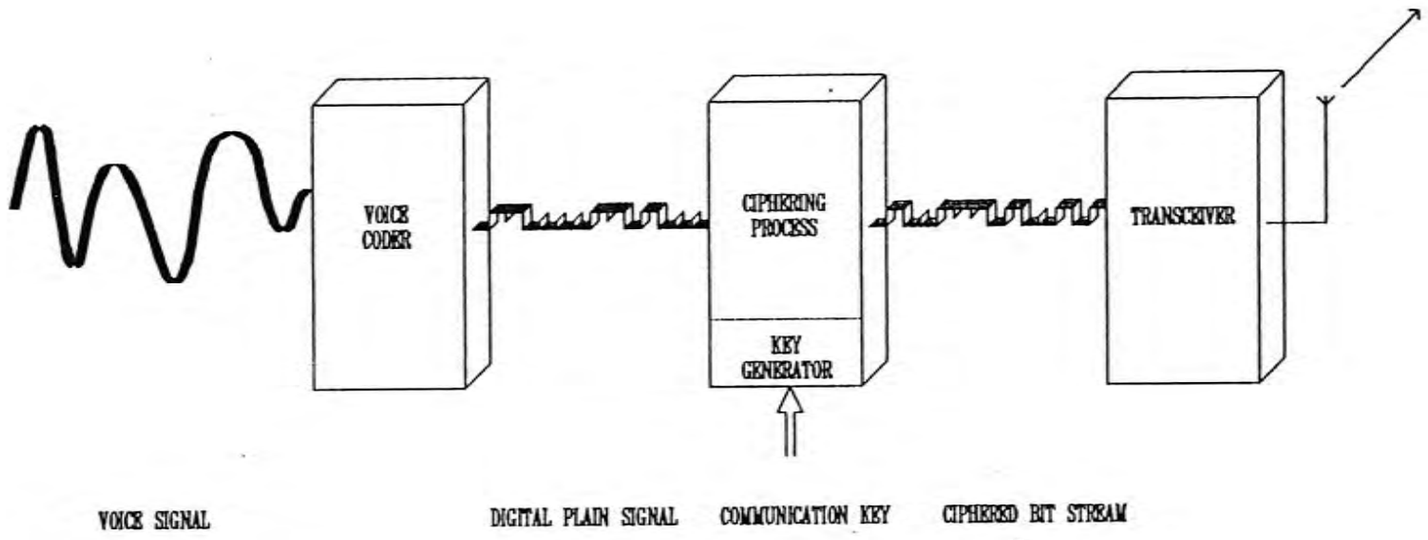


FIG. 2 PRINCIPLE OF DIGITAL VOICE PROTECTION

2 DESIGN GOALS

In this Chapter, the important functional, operational, logistic, technical and in-service maintenance requirements of a digitally encrypted paramilitary operated LMR system are proposed. Many of these requirements are, however, primarily relevant to the design criteria of such a combined system.

2.1 System Concept and Configuration

This proposed secure radio communications system is designed to facilitate highly mobile, survivable, reconfigurable, reliable and secure radio communications among individual group members of a rapid-deployed police special task force. It is obvious that such strategically important communications must be protected from unauthorized eavesdropping by means of sophisticated voice security digital encryptors inherently built inside individual radios. Additionally, the system is designed to meet the most stringent military (MIL) specifications and defence standards (DEF STD) and can be used in all cases for communications links such as transportable microwave radio links or broadband cable systems etc. Fig. 3 shows a configuration diagram of a secure radio communications system operating in the UHF frequency band and consists of several calls which can either work independently or, if required, will be intermeshed.

2.2 Operational Requirements

2.2.1 Operating conditions

The system is designed for use in paramilitary operational environments like counter-terrorist, anti-drug, anti-smuggling, VIP protection and covert surveillance operations. To lend to these different tactical roles, all units of the radio system should firstly be environmentally tested to the relevant sections of defence and military standards such as DEF STD 07-55 and MIL STD 810C. Secondly, the units should be small size and light-weight. This is to provide user mobility (e.g. transportable or manpack option) to allow easy available access. Last, but not least, the units should consume as low power as possible so that regular d.c. batteries can be used for a long time in most battlefield-like environments.

2.2.2 Intelligibility and speech quality

Operationally speaking, great stress is placed on high intelligibility and excellent voice quality. The first one is a qualitative measure of how well the radio system is able to communicate the basic information content of intelligence, the second is a subjective measure of how well the radio system communicates the overall speech information which includes speaker recognition,

reproduction of accent, emotional state, sex of the talker etc. In Hong Kong, the police special task force may consist sniper members of different nationalities, speech quality attributes would become even worse by non-native speakers or listeners in conversing some critical messages, for instance, a `shoot' or `don't shoot' command. Incidentally, under a series of subjective field tests conducted by members of the special task force from the Royal Hong Kong Police with portable radios at data rates from 9.6 Kbit/s to 16 Kbit/s, it was generally agreed that the expected quality of speech from an operational point of view was at least an equivalent to a CVSD coding technique at 16 Kbit/s [9]. A subjective quality assessment for speech coding performed by SDU is given at Appendix I. This 16 Kbit/s requirement is also confirmed by Muilwiz [10] as a good compromise between bit rate and speech quality for mobile radio communications. Furthermore, based on the Speech Transmission Index (STI), an intelligbility measure as suggested by Steeneken and Houtgast [11], it can be shown that the 16 Kbit/s CVSD system is about 19.2% better than a 12 Kbit/s system which is now commonly available in commercial market. Hence speech quality of 16 Kbit/s CVSD system could be regarded as a norm for the paramilitary applications.

2.2.3 **Field coverage and transmission delay**

Coverage engineering, prediction of service area, and service quality, in an ever-changing mobile radio channel environment, is a difficult task. The average path loss depends on terrain microstructure within an area with considerable variation between different types of areas (i.e. urban, suburban, and rural environments). A variety of models based on experimental and theoretic work have been developed to predict path radio propagation losses in a mobile channel. Unfortunately, none of them are universally applicable. In almost all cases, an excessive trasmitting power is necessary to provide an adequate system performance but this would result radio pollution. The curves of path propagation loss L in decibels (dB) versus the distance d in kilometers (km), based on some of these models, are summarized in Appendix II. Since intelligibility will degrade as the mobiles leave the vicinity of their base stations, therefore, having a good range and a good system performance means having intelligibility above a certain percentage at a long distance from the base unit. From an operational standpoint, a reliable operational range of, say, 3 Km in diameter, using mobile units of 15W transmit power and 0.2uv sensitivity is generally expected. A minimum acceptable percentage would be 85% Diagnostic Rhyme Test (DRT), but the paramilitary secure radio system would need a much higher value to ensure reliable performance with

over 95% DRT. Fig. 4 shows a qualification of the STI and relation with the DRT.

On the other hand, the time delay introduced by a speech encryptor become important when radio systems are operated in full duplex mode. The main transmission delay, excluding propagation delays, between press-to-talk (PTT) and receipt of plain speech at the receiver is the time required for synchronization and this is approximately 120 msec. After synchronization, a delay of less than 5 msec occurs due to inherent circuit delays such as filters, A/D and D/A conversions, etc. Technically speaking, if the end-to-end system delay exceeds an upper limit of 200ms, it will not meet the requirement of real time conversation in field operations.

2.2.4 **Reliability and Maintainability**

The proposed system is designed for prolonged, continuous and reliable operation under severe environmental conditions. The design and construction must be of a high engineering standard and must withstand handling and transportation in open space environments without degradation of performance and specifications. All equipment shall be of ruggedised construction, hence relevant MIL or DEF Standards are to be met. The Mean-Time-Between-Failure (MTBF) or Mean-Time-To-Repair (MTTR) of each item of the system of better than 5000 hours is expected.

From a logistic support standpoint, components used are preferably to be obtainable from multiple sources, and non-proprietary. If any proprietary parts are used, they shall be supplied by the manufacturer throughout the lifetime of the equipment. All units, sub-assemblies, components and adjustment controls shall be readily accessible for maintenance purposes. Equipment shall be of modular design so that clearance of faults can be achieved rapidly by replacing faulty interchangeable modules. Adequate test points and other test facilities, such as testing templates and/or test plugs on the side of portable radio, shall be provided to simplify trouble shooting and permit ease of maintenance. Layout, marking, constructor and components are to be designed for robustness and ease of maintenance. All equipment of the system are to be capable of working under direct sunlight and heavy rainfall conditions without causing performance degradation as specified. User accessible controls, ancillaries and aerials must withstand harsh use and severe environmental conditions. Fully solid state equipment is essential, preferably with IC construction. To support subsequent in-service maintenance, any application of "application specific integrated circuit (ASIC)" shall be highlighted regardless how much portion it takes part of the whole equipment.

2.3 Functional requirements

2.3.1 Major system features

A list of major system features is given below :

(a) Enhanced security digital encryption with end-to-end protection for both voice and data transmission.

(b) Simplex or duplex traffic on fixed or trunked narrow-band mobile radio channels.

(c) Outstanding system flexibility and modularity permitting all possible network configurations and later extensions or reconfiguration.

(d) Multiple mode operation : full digital plain or ciphered mode at low bit rate (e.g. 9.6 kbit/s) as well as analogue plain FM or PM mode, therefore providing full interoperability with conventional existing mobile or hand-held radio.

(e) Audio quality in digital ciphered mode comparable or better than that in analogue plain voice mode, thus ensuring unequivocal speaker recognition.

(f) Trouble-free coexistence with existing two-way radio system within the same frequency range and without spectrum loss. In digital mode the adjacent channel power fully meets regulations for analogue equipment, therefore no protection gaps are really needed.

(g) All radio equipment must be able to switch between clear voice and secure speech modes in a very simple and efficient manner. Additionally, they should also have the benefit of secure speech override facility. This means a receiver being switched to secure mode can receive a plain signal.

2.3.2 Cryptographic features

Though it is widely felt that digital encryption method employs stream cipher technique such that no errors propagation results could meet paramilitary requirements, a more elaborate and qualitative description of the cryptographic features is however necessary. Basically, cryptographic features include :

(a) Digital encryption with high-security algorithm.

(b) Key period more than 200 years.

(c) Random initialisation of cipher process.

(d) Communication Key (CK) variety of 3.4×10^{38} independent keys.

(e) 3 x 8 Individual Communication Keys stored in cipher module.

(f) Support of key handling and key identification by key signature.

(g) Authentication and ciphering of key serving via radio channel.

(h) Verification of security functions and key integrity.

(i) Key zeroization capability.

2.3.3 **Phone patch facility**

Most paramilitary systems incorpporate a phone patch facility which provides an interconnection between the clear/secure radio and the public cellular mobile telephone or the standard Public Switched Telephone Network (PSTN) in order to link up the radio user with the telephone subscriber user. Since the system will have to interface to the PSTN, it should operate satisfactorily with speech already encoded as A- or u-law PCM as defined by CCITT in Recommendation G.711 [6].

2.3.3 **Mobile data capability**

When powerful computers and databases become available, Law Enforcement Agencies including Police were among the first users of this new technology. It has become possible to store all information about terrorists, criminals, and suspects as well as stolen goods, cars etc. It is most desirable for the system to support access to a computer database. This offers a wealth of benefits such as efficient screening of suspects, communication of

written messages, especially some important or emergency messages and additional safety to operationals through position reporting and automatic release of alarm. As an outstanding example, the Swiss Federal Police have been, for several years, using a computer-based automatic retrieval system to improve efficiency. It is called Ripol (Recherches informatisees de police) which allows mobile users to have direct access to the database using an existing radio network. In some countries, success in the search for wanted persons or suspects has increased by more than 100% after using a similar secure patrol communication and information system. In Hong Kong, the RHKP has started some research studies into this area.

Fig. 5 shows an overall structure of a possible network. Every patrol in the network uses a secure handheld terminal. Any message or request which is keyed into the terminal is first encrypted by a high security, non-linear ciphering algorithm. This ensures that from the outset, the complete communication is secure. The terminal sends all information via radio (over air) to the nearest radio relay centre where all handling of input and output is performed by a Radio Network Controller (RNC). A block schematic diagram of the radio relay centre with RNC is given in Fig. 6.

2.4 Bandwidth requirement

Nowadays, the specifications on the RF spectrum are still not identical in all countries. In many countries like Hong Kong, the 400 MHz digital secure radio must co-exist with the traditional analogue mobile systems. The adjacent channel interference (ACI) requirements will thus greatly limit the maximum transmitted bit rate of the digital system [12]. It is necessary for the digital system operator to carefully observe existing CCIR Recommendations and Reports [13] to ensure that the ACI is limited to 70 dB below carrier power, measured in a norm-filter bandwidth of 16 KHz for channel separations of 25 KHz, as shown in Fig. 7.

Mathematically,

$$ACI = 10 \log (Px/Px+1) \geq 70 \text{ dB} \quad \ldots (1)$$

Also as stated by Carson's rule, the occupied bandwidth (BW) is given by :

$$BW = 2 (fm + fd) \quad \ldots (2)$$

where fm is the maximum modulating frequency and fd is the frequency deviation. The relationship between fm and the maximum transmitted bit rate (b) as governed by Nyquist theorem is,

$$fm = b/2 \quad \ldots (3)$$

therefore,

$$b = BW - 2fd \quad \ldots (4)$$

Based on an nominal 4 KHz deviation and a 25 KHz channel separation, the theoretical value of b is 17 Kbit/s. This bit rate is however practically too high in a 25 KHz channel spacing environment. That means interference from radios at standard spacing is highly probable. Unless channel spacing of 30-35 KHz is used, interference will be unavoidable. On the other hand, using a 30 KHz or more channel spacing would definitely result in inefficient spectrum utilization and it would also be incompatible with existing analogue radios. To this end, research into a reduction in bit rate to less than 16 Kbit/s, but with equivalent voice quality, to make the signal fit into a standard 25 KHz channel spacing radio is of paramount importance. Following World Administrative Radio Conferencer WARC 92, the US Federal Communicatiions Commission (FCC) has decided to implement options to promote effective and efficient use of the bands in 400 MHz. It is interesting to note that narrowband technologies are developed from existing 25 KHz to 12.5 KHz and towards 6.25 KHz. Like many other western countries, Hong Kong Telecommunications Authority (HKTA) has her VHF/UHF channelling requirement of LMR trends gradually towards a 12.5 KHz width. Therefore, it might be necessary to reduce b further to, say, 8 Kbit/s.

2.5 Bit Error Rate Requirement

The error performance of the secure system can be measured by specifying the required bit error rate (BER) by fading. The acceptable BER is an analogy to a clear radio signal reaches 12 dB SINAD (SIgnal to Noise And Distortion ratio) level and it is usually of one percent. However, the performance of the 16 Kbit/s CVSD modulation is tested as sufficiently good at high error rates to preclude the need for any error detection or correction coding, even against partial-band interference. But a faster data speed is obviously more difficult to recover error-free than a slower one. Hence, radios at higher data rate are harder to capture than one with a lower rate. This results in reduction in coverage range consequently.

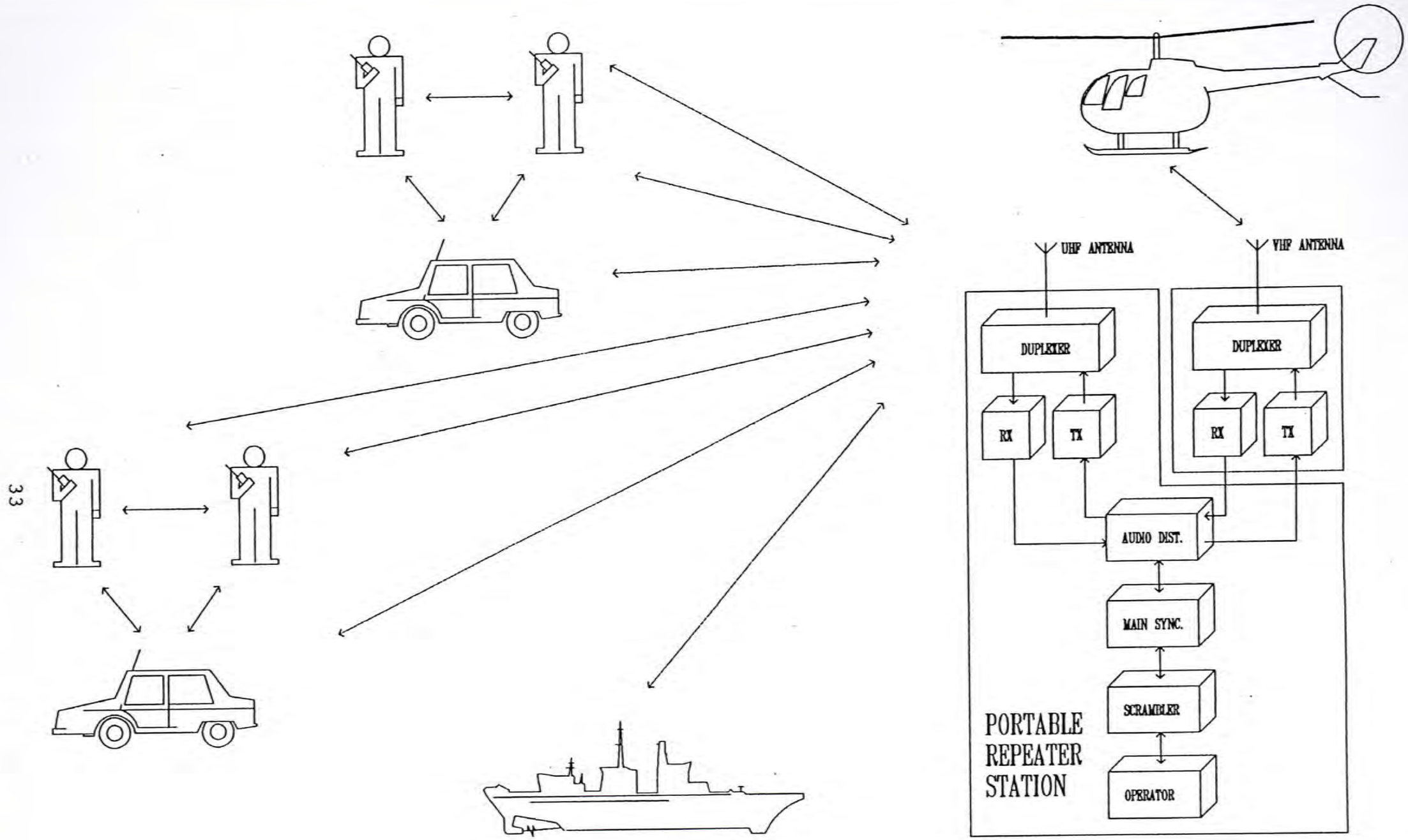


FIG. 3 SECURE RADIO COMMUNICATIONS NETWORK

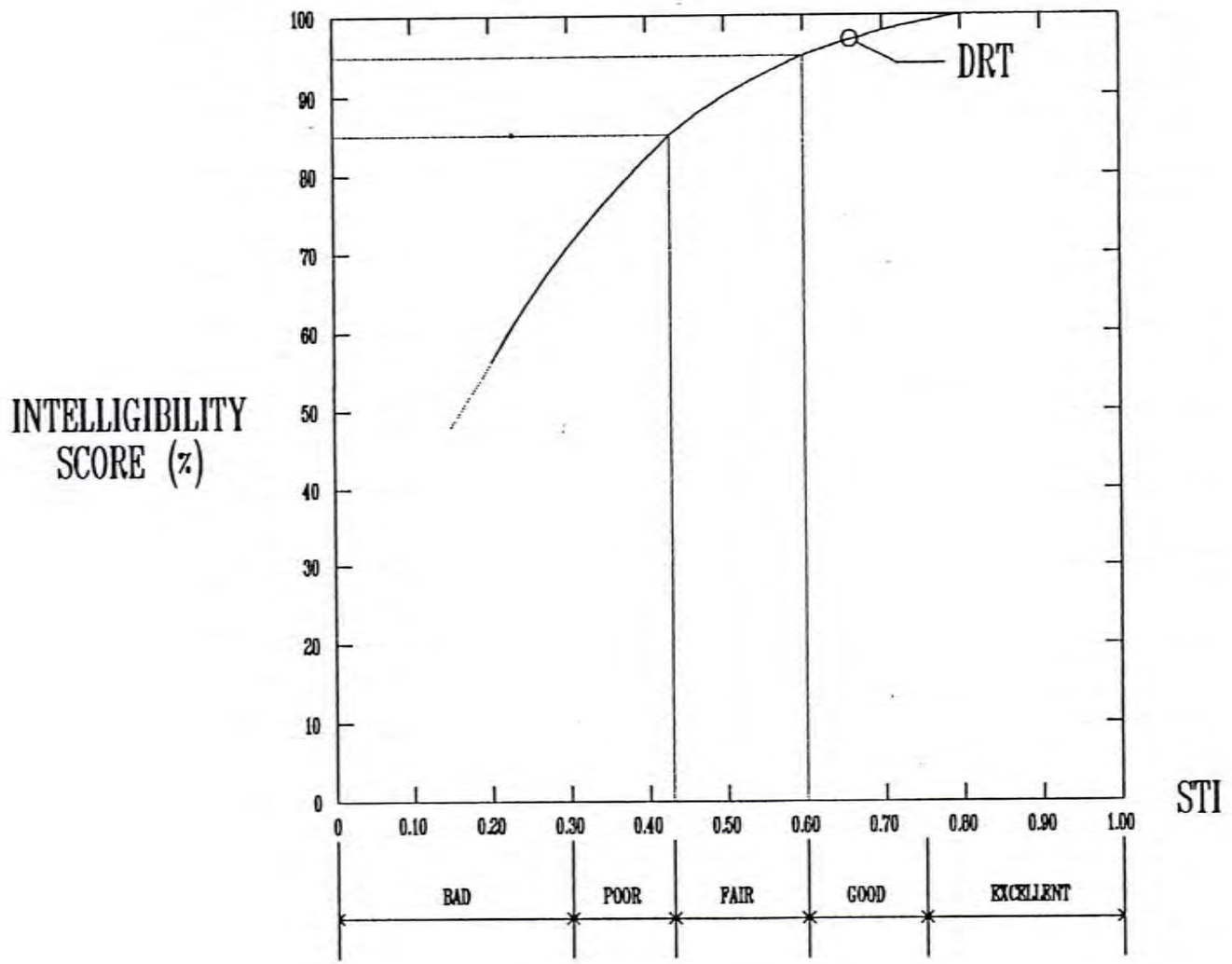


FIG. 4 QUALIFICATION OF THE STI AND RELATION WITH DRT [11]

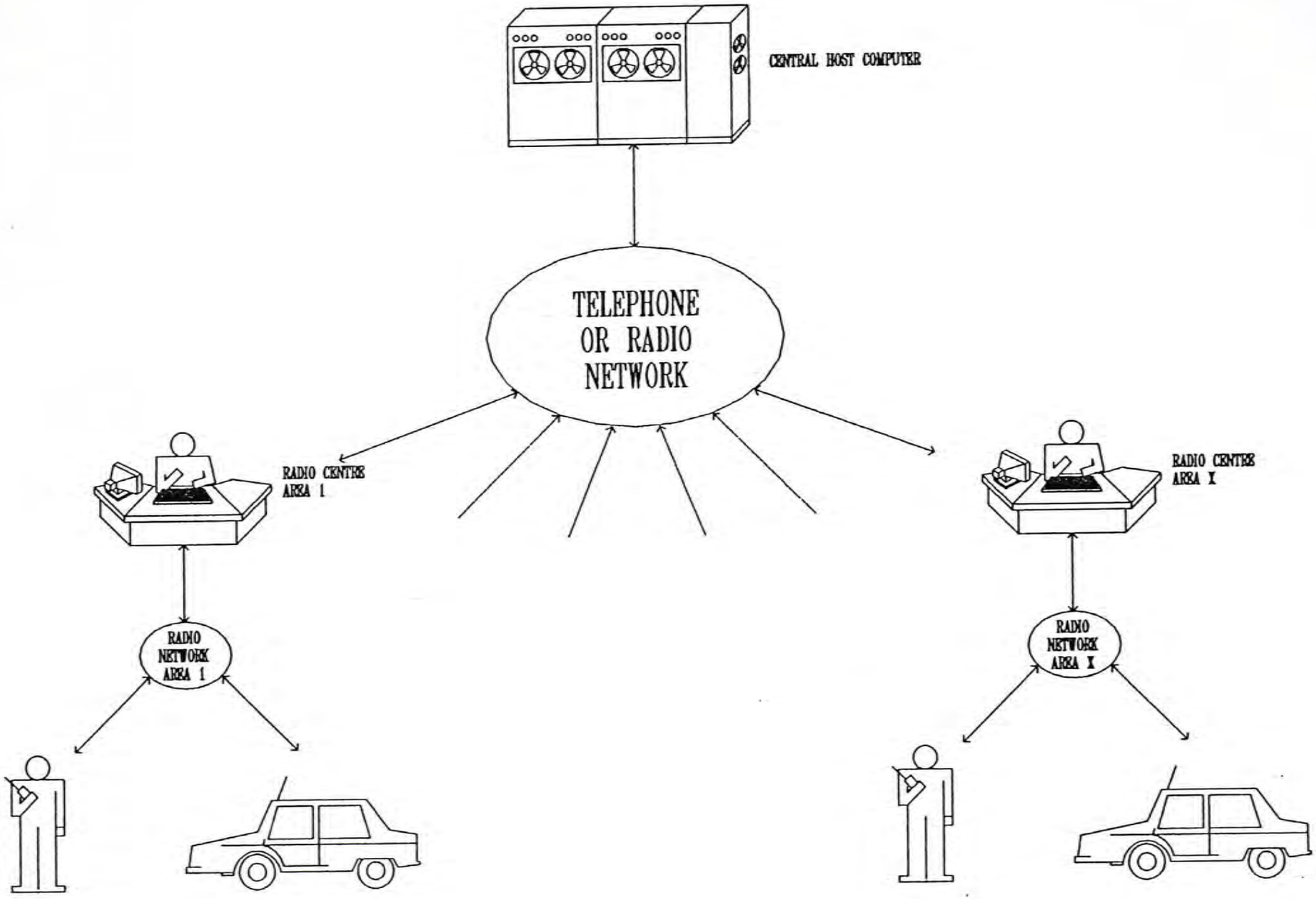


FIG. 5 EXAMPLE OF A COUNTRY WIDE NETWORK :
ALL MOBILE SUBSCRIBERS HAVE DIRECT ACCESS TO THE CENTRAL HOST COMPUTER

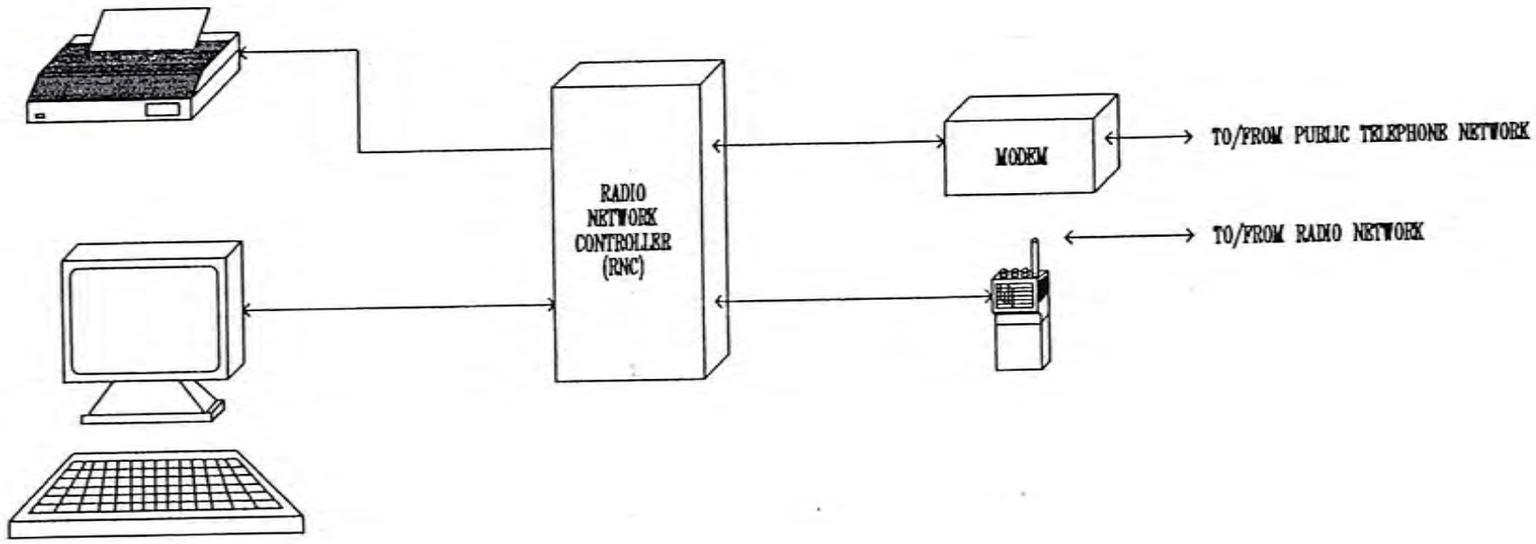


FIG. 6 BLOCK DIAGRAM OF THE RADIO CENTRE WITH RADIO NETWORK CONTROLLER (RNC)

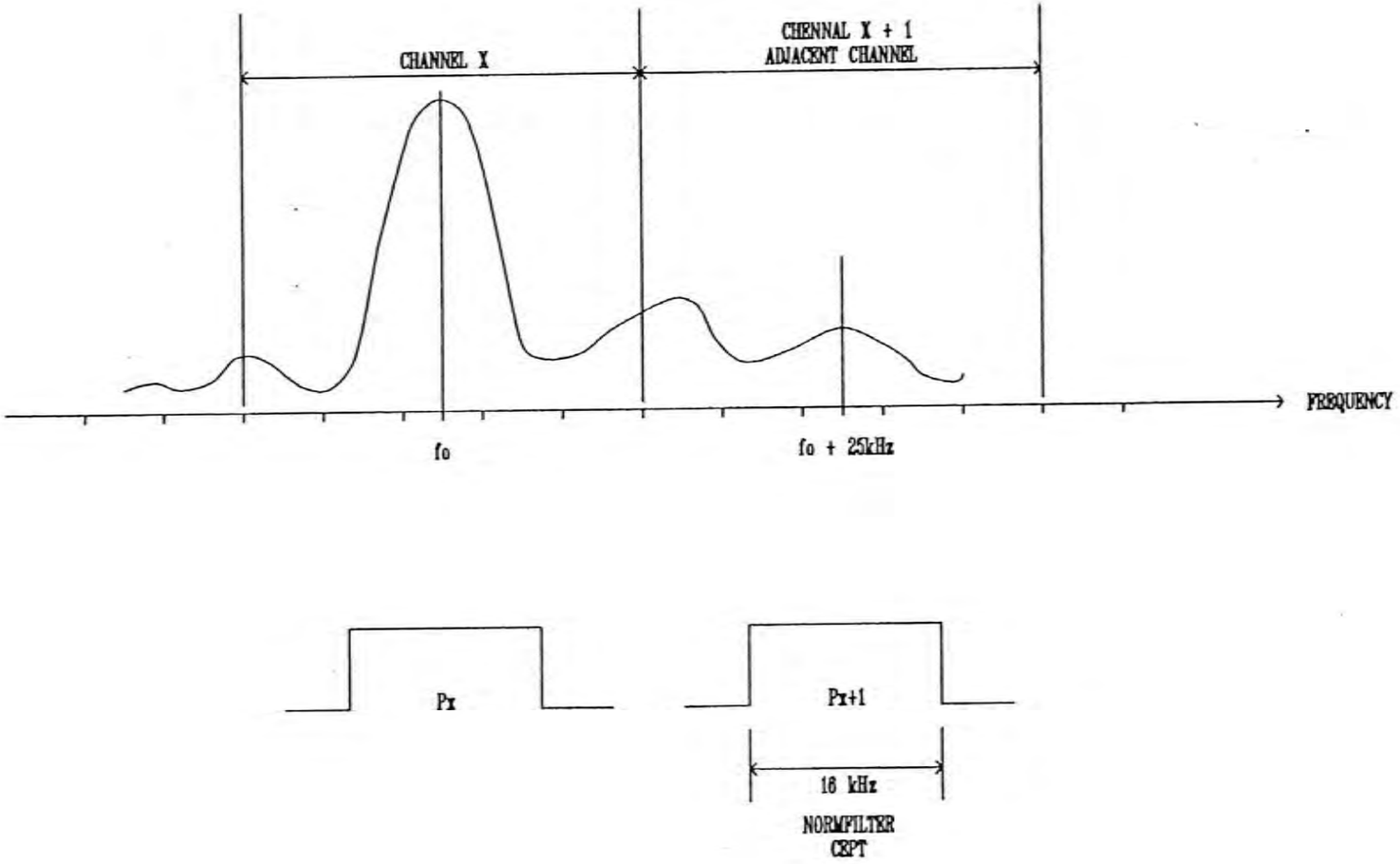


FIG. 7 CCIR RECOMMENDATION ON ADJACENT CHANNEL INTERFERENCE REJECTION

3 VOICE CODERS

Digital speech coding techniques have been divided into two major categories, viz., waveform digitization and analysis-by-synthesis. The first method attempts to reproduce the time-domain voltage waveform of the speech signal in digital form and is referred as a waveform coder. The other type aims to preserve the perceptually significant properties of speech signals of which some parameters, rather than some estimates, are transmitted and is often recognised as a source coder.

3.1 Digital Speech Coding Methods

3.1.1 Waveform Coding

Pulse code modulation (PCM) was invented by Reeves of IT&T in 1938 and put into service by industry in the early 1960. Fig. 8 shows a simplified block diagram of a PCM system. It has been widely used as the conventional method of speech coding (transmission rate 64 Kbit/s, A- or u- law and a SNR of roughly 38 dB) in public telephone networks [14]. Various modifications have been made to the basic PCM principle in an attempt to reduce the transmission bit rate required but without degrading the speech quality significantly. These include differentially-encoded PCM (DPCM), adaptive PCM (APCM) and adaptive differential PCM (ADPCM) which use self-adjusted quantiz-

ing levels to reduce bit rate by about 2 bits per sample and provide fairly good speech quality at 32-40 Kbit/s [15] [16]. However, the relatively high data rate requirement of both methods deter their practical application in narrowband communications. In addition, ADPCM did not work well for some voice band data and other non-speech-like signals which might be present on the telephone network on certain occasions.

Other waveform coding systems using adaptive method such as delta modulation (DM), adaptive delta modulation (ADM) or continuous variable slope delta modulation (CVSD) were also developed. They often operate at around 16-32 Kbit/s for tactical quality speech. Albeit the bit rate is still marginal, the cost effective realization of CVSD codec in VLSI form together with the fairly good speech quality has opened its fruitful market.

3.1.2 Linear Predictive Coding (LPC)

LPC was introduced in the early 70s by several researchers [15] [17]. It is a combination of analysis and synthesis techniques in the time domain. Fig. 9 shows the principle of LPC technique where selected error characteristics including pitch information, rms value of signal, voice/unvoice decision together with predictor coefficients are analysed and transmitted over channel. Typical data rate ranges from 1.2 K to 2.4 Kbit/s but is sensitive to pitch detection errors, background noise, and

multiple speakers. Besides, it also requires high speed special digital signal processor to implement its complicated algorithm.

Adaptive predictive coding (APC), on the other hand, transmits the difference signal between the predicted and actual voice waveform samples along with the amplitude information, pitch period and filter coefficients. Although computational complexity is still high, this scheme reduces sensitivity to pitch detection error which in turn provide a high tolerance to channel errors and can operate at data rates around 8 Kbit/s.

Modern research activities for low bit rate speech coding based on multipluse linear predictive coder (MPLPC) and code-excited linear prediction coder (CELP) has successfully warranted quality output at lower computational complexity. In MPLPC, the coded source excitation is generated by summing the weighted impulse functions, whereas in CELP, the coded source excitation is obtained by searching through a code-book of pre-stored sample sequences. Although a 13 Kbit/s Regular Pulse Excited Linear Predictive Coding (RPE-LPC) with long term prediction has been selected for standardisation, it is believed that further improvement on speech quality, complexity and system delay at even lower bit rates could be possible. Specifically, line spectral pairs (LSP) coefficients have recently been proposed as alternative representation of linear prediction parameters for speech

coding at bit rates between 6.4 to 10 Kbit/s. These coefficients have a closer relationship to the spectral properties of speech signal and are thus easier to quantise for efficient transmission.

A speech analysis system using a split-path (LSP) adaptive filter is depicted in Fig. 10. The analysis model is splitted into two filters, P(z) and Q(z), which are connected in parallel. P(z) has anti-symmetric linear phase property whereas Q(z) has symmetric linear phase property. The two filters share the same input s(n) with $e_p(n)$ and $e_q(n)$ being their respective outputs. The filter coefficients of P(z) and Q(z) are obtained iteratively by minimizing the expectation of their output square errors $E[e_p(n)^2]$ and $E[e_q(n)^2]$ independently. The total system output, e(n), which is basically the speech production driving source, is given by [18]

$$e(n) = \{e_p(n)+e_q(n)\}/2 \qquad \ldots (5)$$

Since P(z) is antisymmetric and Q(z) is symmetric, their coefficients, p_i and q_i are therefore related by

$$p_i = -p_{2N+1-i} \quad , \quad i = 0, \ldots, N \qquad \ldots (6a)$$

$$q_i = q_{2N+1-i} \quad , \quad i = 0, \ldots, N \qquad \ldots (6b)$$

Now, putting $p_0 = q_0$ to unity, the transfer function of P(z) and Q(z) can be represented by the following equations,

$$P(z) = 1+ \sum_{i=1}^{N} p_i (z^{-i} - z^{-2N-1+i}) - z^{-2N-1} \qquad \ldots (7a)$$

$$Q(z) = 1+ \sum_{i=1}^{N} q_i (z^{-i} + z^{-2N-1+i}) + z^{-2N-1} \qquad \ldots (7b)$$

Factorizing (7) yields

$$P(z) = (1 - z^{-1}) \prod_{i=1}^{N} (1 + c_i z^{-1} + z^{-2}) \qquad \ldots (8a)$$

$$Q(z) = (1 + z^{-1}) \prod_{i=1}^{N} (1 + d_i z^{-1} + z^{-2}) \qquad \ldots (8b)$$

where $c_i = -2\cos(w_i)$ and $d_i = 2\cos(w_i)$. It is trivial that the roots of $P(z)$ and $Q(z)$ can actually be obtained from $e^{(jw_i)}$ and $e^{(j\theta_i)}$ respectively with $i = 1, \ldots, N$. It is generally assumed that

$$w_1 < w_2 < \ldots < w_N \quad \text{and} \quad \theta_1 < \theta_2 < \ldots < \theta_N \quad \text{and}$$

in fact, it has been proved that they are alternate to each other on the unit circle [4], i.e.,

$$0 < \theta_1 < w_1 < \theta_2 < \ldots < 0_N < w_N < \pi \qquad \ldots (9)$$

The parameter set $\{ w_1, \theta_1, w_2, \theta_2, \ldots, w_N, \theta_N \}$ are commonly known as the line spectral pair (LSP) parameters. Since these coefficients are closely related to the zeros of the prediction transfer function and hence to the formant structure of the speech signal, they can then be used to characterize the analysis model. In addition, these coefficients are easier to quantize because of their uniform sensitivity across the frequency spectrum. It has also been shown that [33] as long as equation (9) is satisfied, stability of the synthesis filter can be assured. Adaptation of the LSP parameters can be facilitated using the LMS algorithm [18].

Experimentally, a split-band predictive coder has been implemented with a view to evaluating the performance for digital speech transmission at 8Kbit/s in this thesis study. The coder divided speech using quadrature mirror filters into three sub-bands each encoded with fourth order LSP coefficients representing each of the three predictive filters. The filter parameters, which are equivalent to the LSP parameters, are adapted directly with pre-quantized values by using the well known least-mean-square (LMS) algorithm. The speech signal was bandlimited to telephone bandwidth and was sampled at 8 KHz with 8-bit resolution. The LSP coefficients together with other pertinent information were transmitted to the receiver at a frame rate of 30 ms. Subjective listening tests were then performed and they confirmed that output speech quality is highly acceptable.

3.1.3 Sub-Band Coding (SBC)

In SBC, the speech frequency band is divided into 4 to 16 separate sub-bands by passing the speech signal through a bank of parallel filters and each sub-band is then translated to baseband for encoding. The major drawback of SBC is that it is relatively complicated to implement, but it gives good quality speech in the range of 16-24 Kbit/s. SBC using backward adaptive differential PCM, i.e. SBC-ADPCM, can however achieve the shortest system delay at the expense of a measurable rduction in speech quality. In fact, SBC-ADPCM is particularly suitable for harsh channel condition with high BER [10]. In the light of combined design of speech and channel coding, the effects of digital transmission errors on a family of variable-rate embedded SBC have been analysed. Amongst the results, the 12 Kbit/s SBC speech encoder/decoder and the rate-compatible punctured convolutional (RCPC) channel coder/decoder have been implemented on a single AT&T DSP-32 floating point processor [19]. The overall end-to-end delay is reported as about 90 msec which seems very favourable for paramilitary application.

3.1.4 Vocoders

Vocoders were invented by Dudley of Bell Laboratory in the 1939 and had been used in military applications for many years. They use analysis-synthesis techniques and tend to

produce speech with a computer-like synthetic quality. Fig. 11 is a simplified block diagram of a channel vocoder synthesizer. Although intelligibility is only marginally good, vocoders can operate at a bit rate as low as 1 Kbit/s. In general they are among the most complex and expensive voice digitization systems but has very little prospect of permitting recognition of speaker's voice, mood, emphasis, etc. as the speech produced is regarded as "mechanical and montonic" and are therefore not practical enough for secure mobile radios operating in paramilitary environments.

3.2 Performance Comparison

Fig. 12 shows the relationships amongst speech transmission rate, speech quality and relative cost of voice coders [20], [21]. The characterisations are broadcast quality at bit rates exceeding 64 Kbit/s, toll quality at bit rates from 64 Kbit/s to 12 Kbit/s, commmunications quality at bit rates from 12 Kbit/s to 6 Kbit/s, and synthetic quality at bit rates below 6 Kbit/s. The toll quality corresponds to commercial telephone speech quality, which is achieved mainly by speech waveform coding techniques and will be the ultimate target for digital cellular mobile radio systems. Communications quality speech is highly intelligible, but has quality degradation, detectable distortion, and perhaps reduced speaker recognition. The communications quality system

employs the merits of both speech waveform coders and source coders. This is eventually the requisite quality for digital paramilitary LMR systems. Synthetic quality speech is substantially less natural than toll and communications quality and it is ruled out from the assessment.

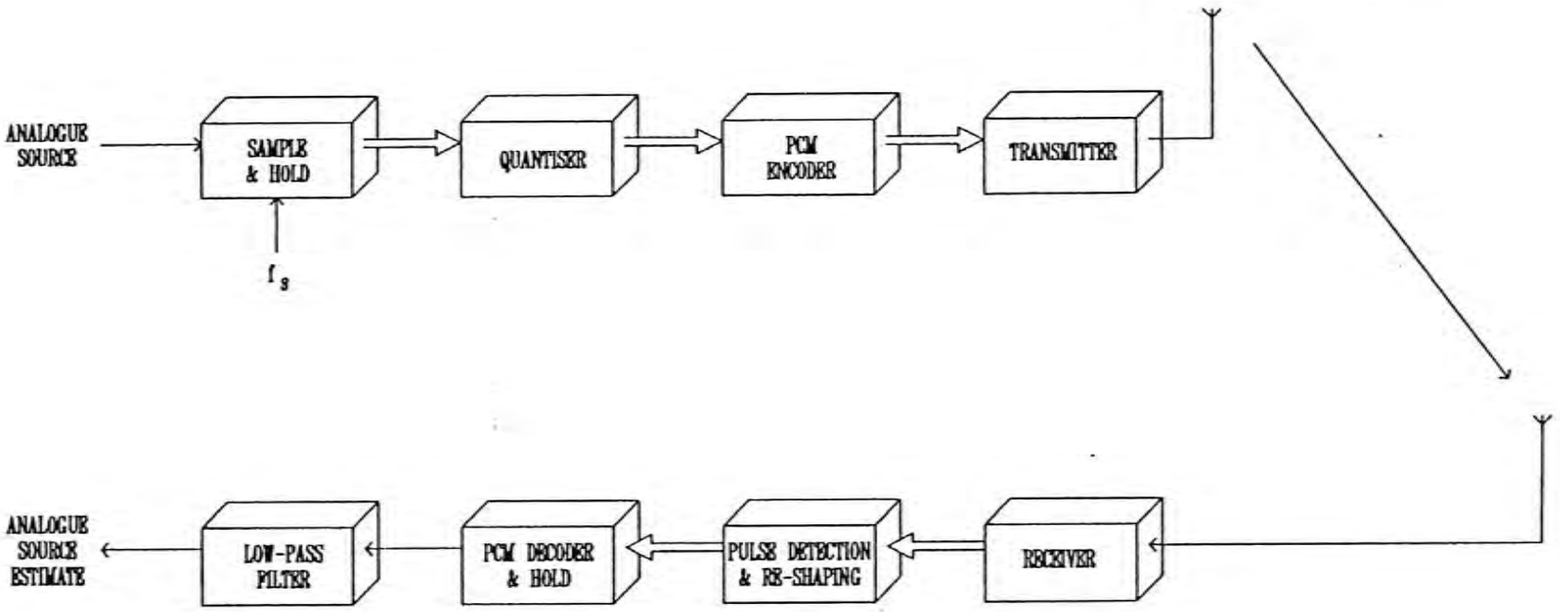


FIG. 8 SIMPLIFIED BLOCK DIAGRAM OF A PCM SYSTEM

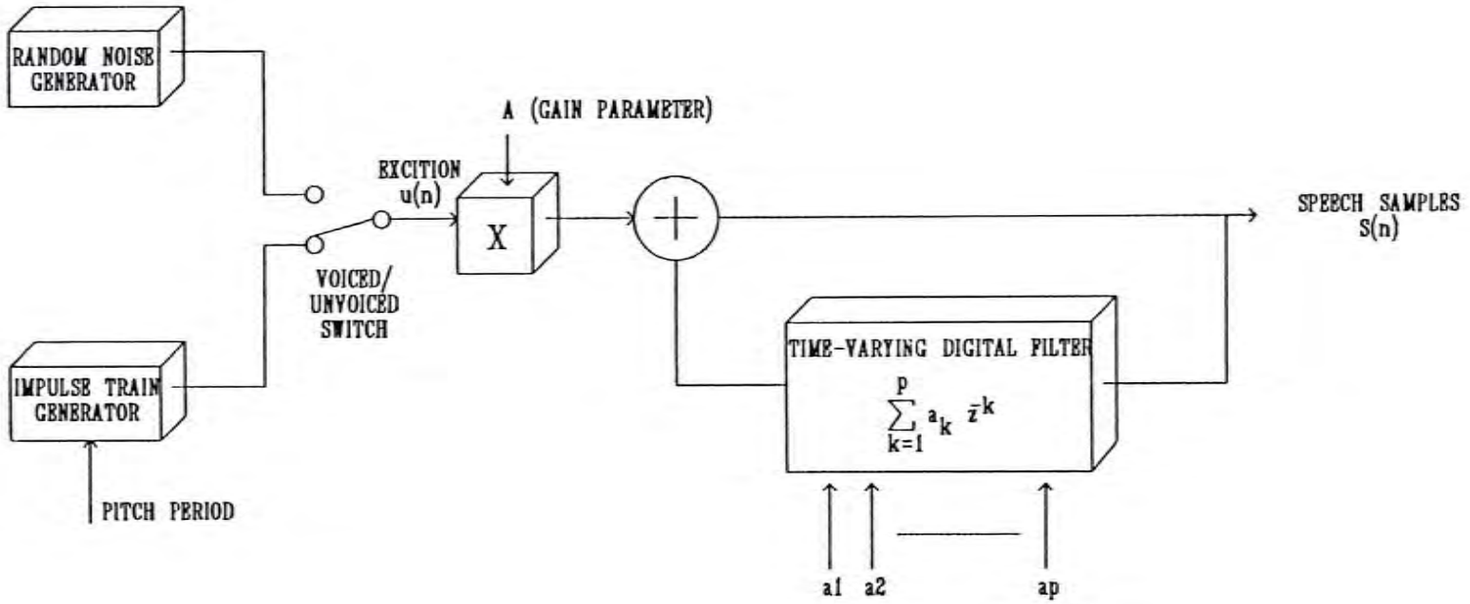


FIG. 9 LPC SYNTHESIZER

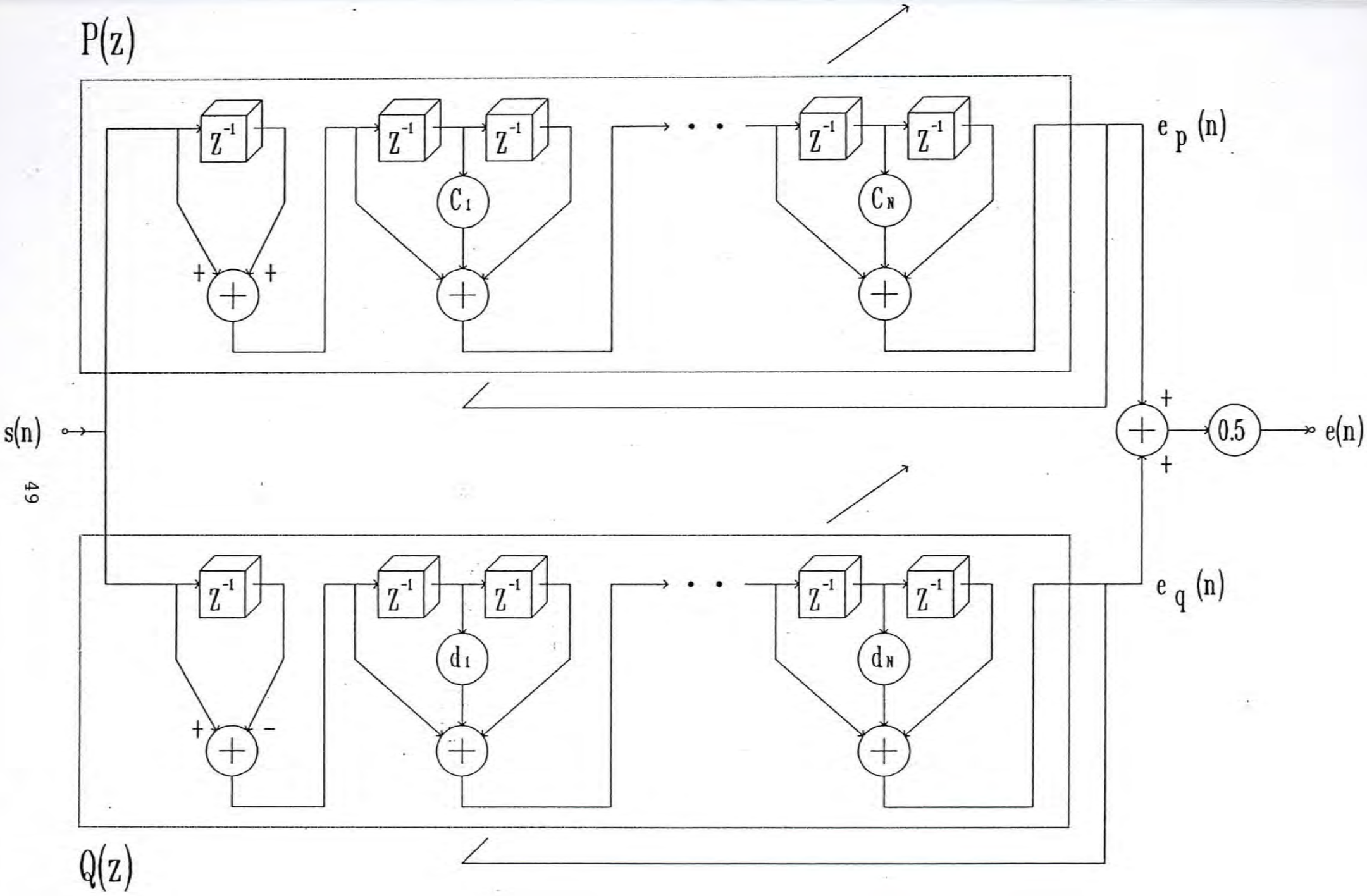


FIG. 10 THE SPLIT-PATH LSP SPEECH ANALYSIS SYSTEM

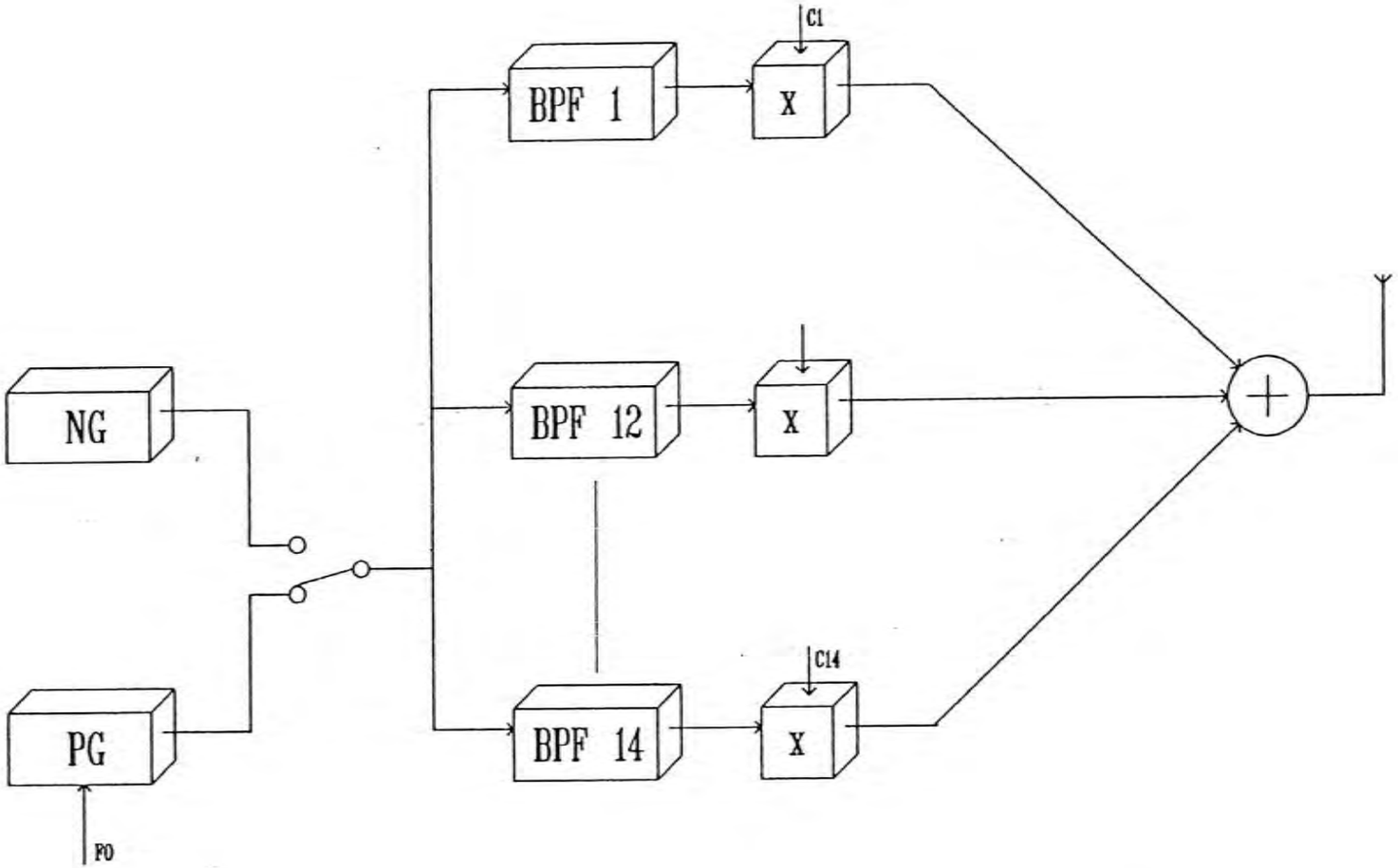


FIG. 11 CHANNEL VOCODER SYNTHESIZER

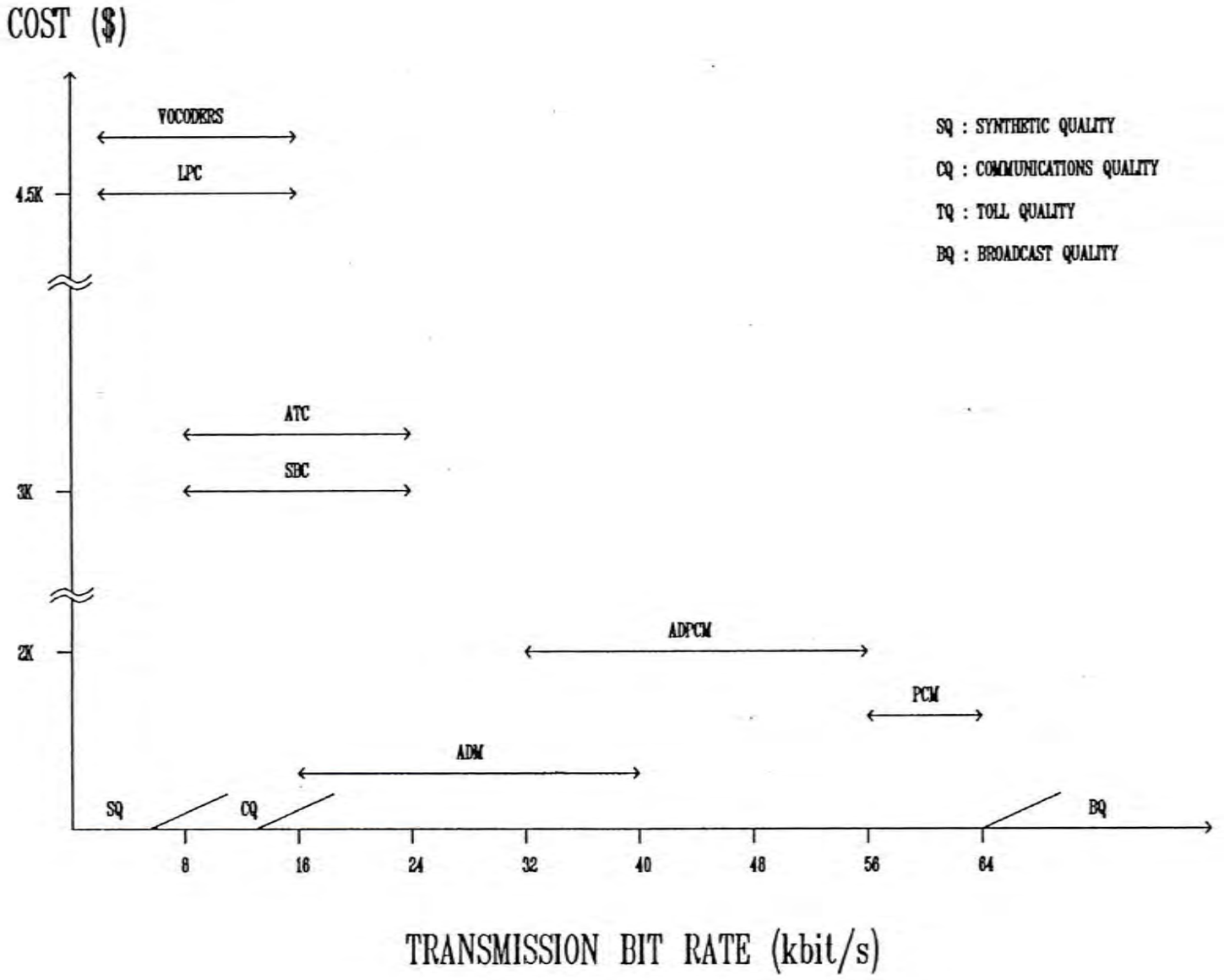


FIG. 12 BIT RATES AND RELATIVE COST OF VOICE CODERS

4 CRYPTOGRAPHIC CONCERNS

4.1 BASIC CONCEPTS AND CRYPTOANALYSIS

Speech cryptography is a set of techniques used to ensure secrecy of speech messages while hostile personnel have the technical capability to intercept and correctly interpret an unprotected message, which is called the clear voice. After transformation into secret form, the message is then referred as the secure voice. The process of transforming clear voice into secure voice is commonly known as encryption. In a cryptographic (or cipher) system as shown in Fig. 13, a set of parameters that determines a specific cryptographic transformation or its inverse is called a key. Cryptoanalysis is the unauthorized extraction of information from the secure voice. Consequently, the security of a system depends upon the inability of the cryptoanalyst to determine the key even if he knows the structure of the cryptographic system.

From a cryptographic point of view, for practical secure LMR system, there are two basic requirements on the secure speech, viz.:

i) to resist cryptoanalysis from unauthorized personnel, and

ii) to be efficiently decrypted by authorized personnel.

The resulting bitstream - the ciphering signal - is fed to the transmitter filter and transmitted in digital mode. In the receiver, the received distorted data are regenerated and processed for deciphering. Using an equivalent sequence of pseudorandom data from the receiver key generator, the received bitstream is calculated back into the plain bitstream and converted fromn the digital into an analogue signal audible at the loudspeaker. It is important that each and every code sequence is a highly complex random ciphering bitstream of guaranteed orthogonality. The complete algorithm circuitry is usually contained in a single high density VLSI chip which can only be changed by the Master of Field Key Programmers. Apparently, an established trade off 16 Kbit/s CVSD digital mobile radio can tolerate a certain error rate even without any protection facility. However, any cipher system which propagates errors are obviously deemed to be usable only for clear voice transmission but not for secure voice communications over non-perfect channels like UHF LMR. To this regard, the cipher feed-back system, though it is simple and needs no synchronization requirement, is not a suitable candidate for paramilitary secure radio communications over narrowband UHF channels. Obviously, a very sophisticated method is required to maintain the synchronization of the transmitter and receiver key generators. To this end, various methods of synchronization will be described in the next section.

These requirements have been more fully achieved by digital encryption and the radio transmission of a digital voice than by analog encryption and transmission. Thus, if secure voice is to be communicated at high level of security, analog-to-digital (A/D) conversion and subsequent digital operations are esssential. The A/D technique and the allowable transmission bit rate limit of radio channel are crucial factors that affect the design of a cryptographic system.

On digital voice encryption, there are two distinct types: encoding and enciphering. Encoding consists of the substitution of groups of bits of variable length for clear voice of variable length. On the other hand, enciphering consists of the substitution of fixed length groups of bits for fixed length clear voice groups. Encoding is difficult to automate the frequent code changes necessary for secrecy which are often difficult to execute. Because enciphering systems are easily automated and modified, they are practically used.

4.2 DIGITAL ENCRYPTION TECHNIQUES

As depicted in Fig. 14, the output bitstream of the coder combined with a pseudo-random key generator, the de facto encrypting means, is a continuously calculating non-linear dynamic algorithm which is programmable for virtually infinite code sequences. These two bitstreams, the voice data bitstream and the key bitstream, are added modulo 2.

For non-error-propagating cipher systems, they are either stream encryption algorithm or block encryption algorithm [23] [23]. The former refers to the encryption of stream of bits in real time whilst in the latter, the first bit cannot be encrypted till the whole block of bits is received. The block encryption technique therefore inherently imposes a considerable time delay which is a function of the block size. This communication delay is probably too high and is unacceptable in a paramilitary operated environment.

4.3 Crypto synchronization

4.3.1 Auto synchronization

Cipher Feedback Systems are available where the ciphered bits themselves contain the synchronization information. A `self-synchronising' cipher feedback system is shown in block diagram from Fig. 15. These systems have the advantages that no additional synch bits have to be transmitted, the initial synch time is short and synchronization has not to be checked continuously. However, there are also the following serious disadvantages : propagation errors result in error extension and data inversions cannot be detected. If any bit, for instance, of the enciphered speech is received in error, not only will that bit be incorrect after deciphering, but in additon between 0 and n of the next n

bits will also be in error after decryption. This is because the bit used to decipher any received bit is a function of the base key and the previous n ciphered (speech) bits. Hence, on average, each bit in error in transmission causes [(n/2)+1] errors in the deciphered and data. In poor radio connections the readability suffers faster than in plain mode, the communication range being smaller. Error propagation may be reduced, but only by causing tremendous reduction in cryptological security. From the point of communication performance and security, cipher feedback systems cannot be recommended.

4.3.2 Initial synchronization

For start or initial synchronization method, burst of synchronization information at the beginning of each transmission, it has the prime advantage of minimizing synchronization overhead (and thus reduce the net bit rate requirements) but it does not allow the late entry of a third party into an estab lished dialogue. That is, if a receiver for some reasons misses the initial synchronization then it is necessary for the user of the receiver to communicate to the transmitter that a new synchronization is required. Therefore it is not effective in a tactical broadcast radio environment. The synchronization information must be continuously distributed in the bitstream to allow late entry and resynchronization after short periods of radio fading or distortions.

4.3.3 Continuous synchronization

Continuous Synchronization is more complicated to achieve and therefore more expensive. The data rate for information is limited since synch bits must be accommodated inside the transmitted bitstream. However, a sophisticated delta pulse code modulation system in the A/D-converter combined with an extremely fast synchronization system overcomes any disadvantages and makes possible the following features :-

(a) No error extension (or error propagation); i.e., one bit error during transmission results in only one bit error after deciphering.

(b) The range of communication remains the same for plain and ciphered operation, readability does not suffer in poor radio connections.

(c) Data inversions can be detected automatically.

4.3.4 Hybrid Synchronization

The hybrid synchronization scheme is based on an advanced long term philosophy which is, in fact, a combination of the initial and continuous synchronization.

At the beginning of any secure communication the synchronization information of a fixed bit length pattern must be received by all partners. This synchronization

signal corrects both the phase and the linear clock generator. Due to the stability of the internal oscillator the scramblers will stay in synchrony for at least five minutes. After elapse of this time period an automatic up-date of the synchronization will take place. During the synchronization process the entire transmission bandwidth is utilized to transmit the bit telegram. During the synchronization period, the communication is temporarily disconnected.

The long term synchronization philosophy has shown several advantages in the field operation :-

(a) Upon reception of the synch telegram there will be no further synchronization required, even by changing the communication direction. This point is not only important in a point to point connection but crucial in a multi-user configuration utilizing repeater stations.

(b) A mobile station may pass through an area of transmission shadow (caused by buildings, tunnels, mountainous terrain etc.) at the point of re-entering the RF signal the secure communication will be instantly back. No time consumign re-synchronization is required. Even if the particular station will miss a synch up-date during passing through the RF blockage area, it will continue to work on the previous synch information. The deciphered voice might be slightly degraded but still understandable.

(c) In areas of multi path reception due to reflection of the RF signal the long term sync will still produce a properly descrambled voice signal. Short term or in-band synchronization will, however, fail due to phase errors in the incoming signal.

In the discussions above, various conclusions have been drawn as to the methods of encryption and synchronization. Practically, these methods have been built into a single small "encryption module" containing everything required to secure a UHF mobile radio. Following extensive operational field trials performed by the SDU, it is concluded that non-error propagating stream cipher encryption with hybrid synchronization gives optimal result (More evaluation details are given in Appendix II).

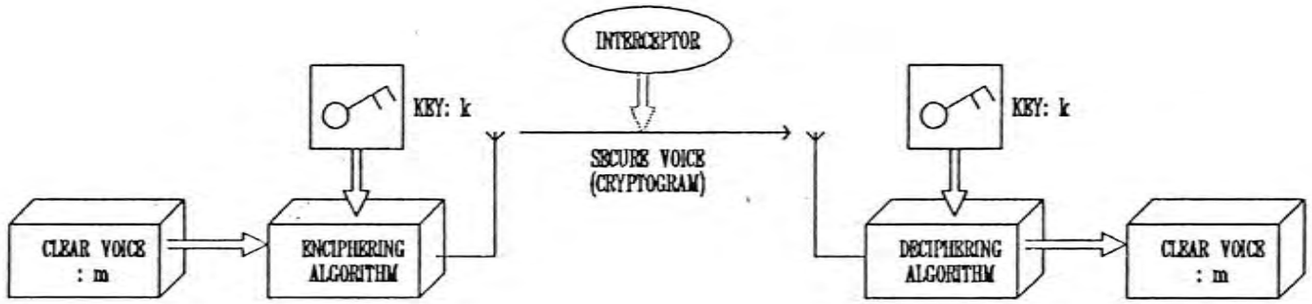


FIG. 13 SIMPLIFIED BLOCK DIAGRAM OF A CIPHER SYSTEM

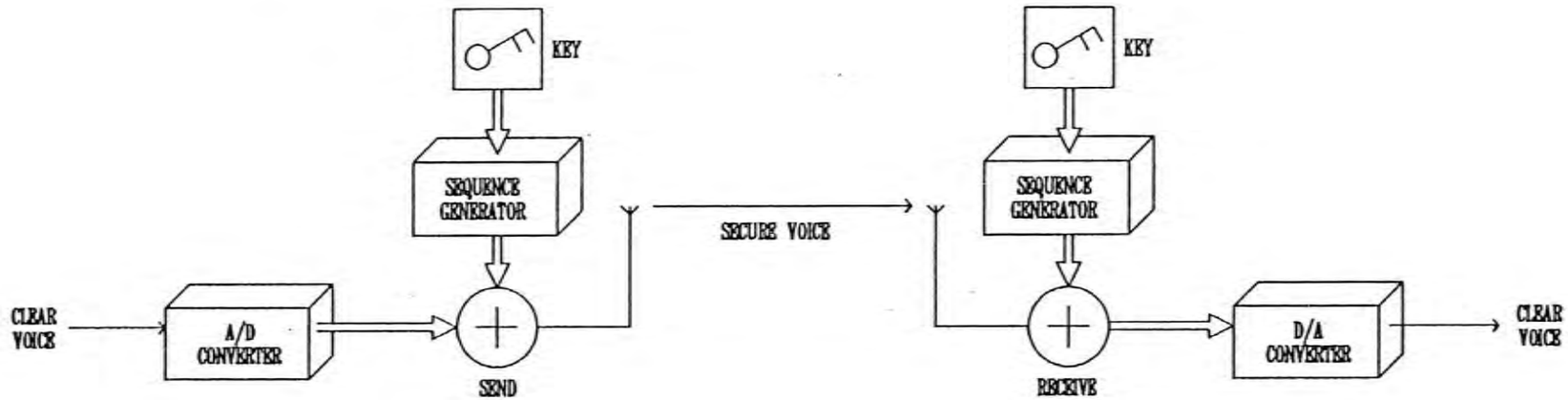


FIG. 14 STREAM CIPHER

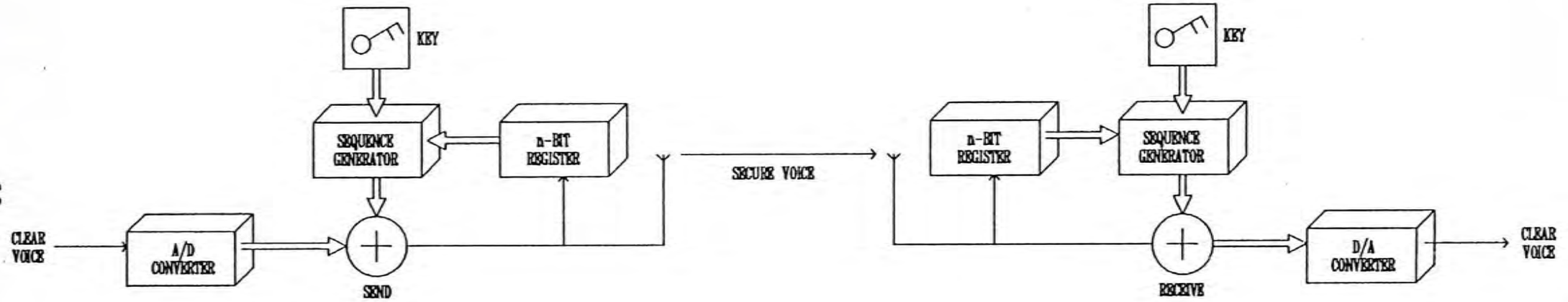


FIG. 15 CIPHER FEEDBACK SYSTEM

5 DIGITAL MODULATION

5.1 Narrowband Channel Requirements

The advent of the above-mentioned highly encrypted speech coupled with an intent for data communications over LMR channels has attracted considerable interests to develop digital modulation techniques for LMR channels. Analog frequency modulation (FM), though sufficiently suitable for analog speech transmission, can also be used as binary FM.

A FM waveform can be written as :

$$FM(t) = A_c \cos [w_c t + 2\pi fd \int_{-\infty}^{\tau} x(\tau)\, d\tau]$$

where fd is the frequency deviation and $x(\tau)$ is the message signal. For digital data, $x(\tau)$ may be binary or multilevel data, the modulation is known as frequency shift keying (FSK). However, from spectral occupancy standpoint, FSK may not be an optimal scheme and continuous research efforts has been devoted for other alternatives.

Basically, a mobile radio channel is characterized by the ubiquitous additive white Gaussian noise (AWGN) and mainly by multipath effects. Based on the channel impairments characteristics, the important aspects required from a digital modulation method for the paramilitary application can be summarized as follows :

a) to use angle modulation to lessen the effect of severe multipath fading,

b) to provide high transmission efficiency within the constraint of the narrowband spacing to reduce crosstalk and ACI,

c) to achieve good error rate performance,

d) to use non-linear (Class C) power amplifier to conserve DC power for this is important especially for portable radios.

5.2 Narrowband Digital FM

Recently, digital signal transmission has been of growing interest in the field of land mobile radio [24]. A narrow-band modulation scheme is necessary to utilize the limited frequency spectrum as efficiently as possible. Digital FM-such as Gaussian-filtered minimum shift keying (GMSK) [25] [26] and continuous-phase modulation (CPM) [27] [28] is one of the most promising modulation schemes because of its compact power spectrum and constant envelope property (GMSK and GTFM are special cases of CPM). A narrow-band power spectrum is achieved by introducing premodulation filtering of the baseband waveform of the input to the FM modulator. Bandwidth-efficient digital FM signals can be demodulated by either coherent or noncoherent (differential and frequency) demodulators. Frequency demodulation is of significant interest, because fast multipath fading makes the use of

coherent demodulation difficult, and because carrier frequency drift caused by the relatively unstable frequency oscillators used in mobile units precludes application of differential demodulation. However, increased baseband intersymbol interference (ISI) due to premodulation filtering severely degrades the bit error rate (BER) performance with frequency demodulation.

In addition to diversity combining, an attractive technique to reduce fading effects is error control, such as forward error correction (FEC) and automatic repeat request (ARQ). The improvements in signal transmission performance using error control techniques depend on the block error rate (BKER) of more than M-bit errors in a block of N bits (we assume the use of block codes for FEC in this paper). Thus, it is very important to investigate the effects of the different decision schemes on BKER performance as well as BER performance.

A block diagram of the narrow-band digital FM transmission system (single branch) is shown in Fig. 16. Nonreturn-to-zero (NRZ) data α_n (= ± 1) is bandlimited by the premodulation filter before input to the FM modulator to achieve a narrow-band power spectrum. At the receiver, the predetection bandpass filter bandlimits the received signal and additive white Gaussian noise (AWGN). The limiter-discriminator (used for frequency demodulation) followed by a postdetection low-pass filter delivers the instantaneous angular frequency deviation of the bandlimited digital FM signal plus AWGN.

5.3 Performance Evaluation

Hence, amplitude modulation schemes are not practical due to rigorous amplitude, variations produced by the multipath propagation. Likewise, common phase modulation schemes like filter shaped FSK, binary phase shift keying (BPSK), quarternary phase shift keying (QPSK) are also not suitable because the restricted bandwidth requirement is violated. On the other hand, the spectral linear modulation, such as 16 quadrature amplitude modulation (16 QAM) requires an inherently inefficient class A linear power amplifier. Therefore, constant envelope digital FM modulation schemes has the advantage of lesser power requirement. The very spectrally efficient CPFSK, GTFM and GMSK are probably some suitable candidates since they have very attractive properties like a constant modulated carrier envelope and a sufficiently compact power. Fig. 17 plots the spectrum diagrams from a practical 16 Kbit/s CVSD system using GTFM operating at clear and secure modes. Quite obviously, it can be shown that the secure transmission can hardly achieve an ACI of 45 dB which is however 20 dB less than that being operated in clear mode. In fact, there are still much room awaiting for improvement in this area. Besides the concern of maximizing spectrum efficiency, simplicity of circuit implementation is of course yet another important consideration. Noncoherent detection by means of a frequency discriminator of the GTFM signal in conjunction

with a simple maximum likelihood sequence estimator has been reported to yield comparable BER performance to coherent detection. The realization of this noncoherent receiver solved not only the technical problem of carrier phase recovery process for coherent detection, but also implied that it is possible to modify a simple receiver with data detection performance but using a great deal of existing analogue FM receiver. The latter feature to become a hybrid demodulator/detector is particularly beneficial to both clear and coded speech requirements for paramilitary radio systems. Based on these preliminary concerns, the optimization of channel coder is depicted in the system layout of baseband modem and conventional FM radio as shown in Fig. 18.

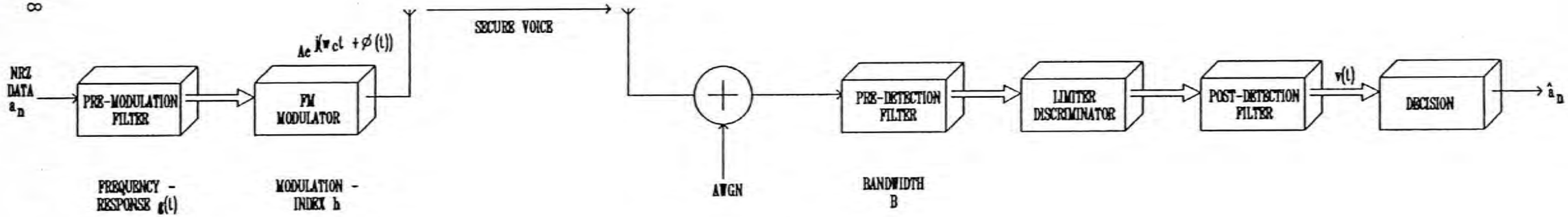


FIG. 16 BLOCK DIAGRAM OF NARROWBAND DIGITAL FM TRANSMISSION SYSTEM

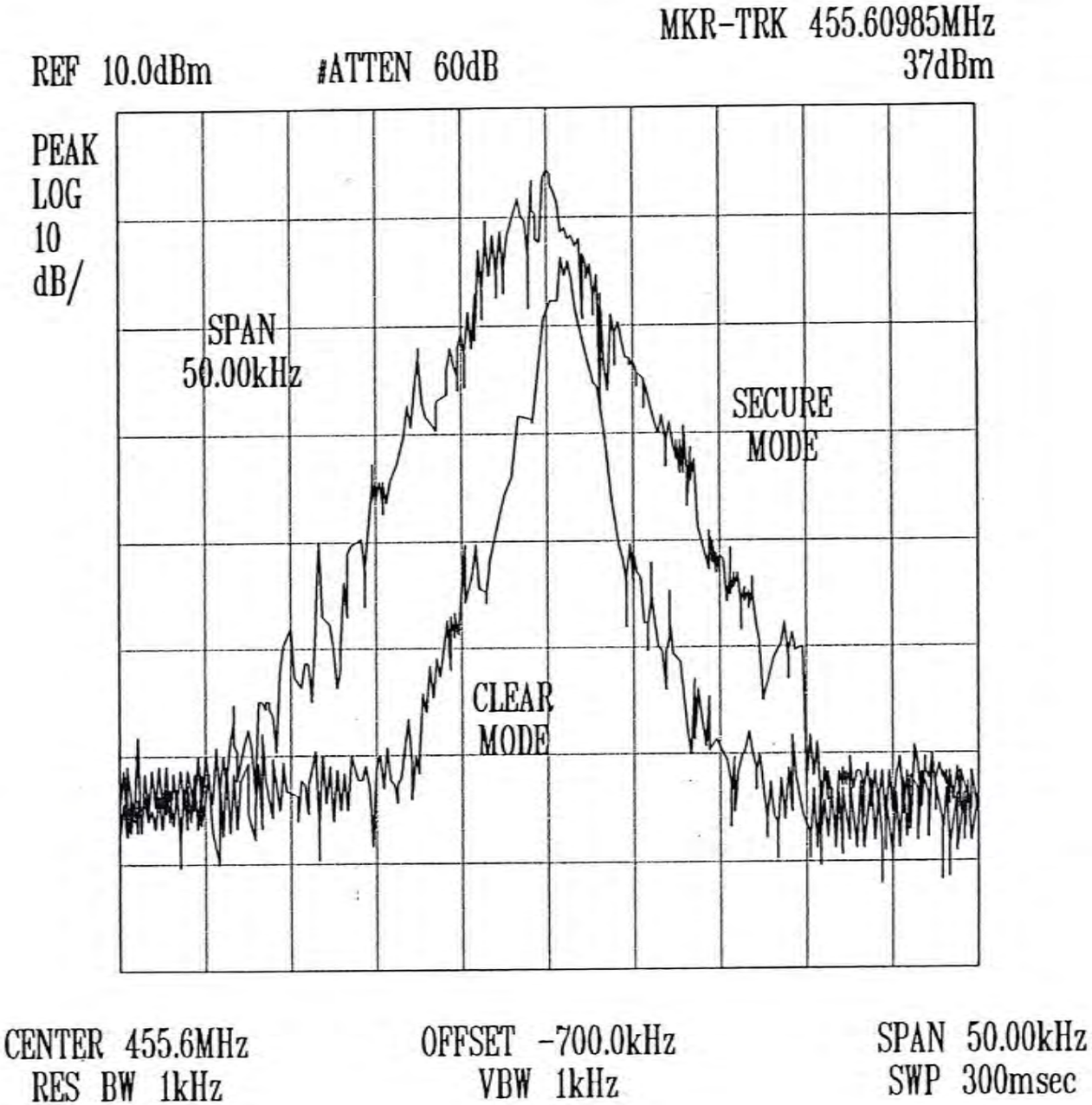


FIG. 17 CLEAR MODE AND SECURE MODE TRANSMISSION

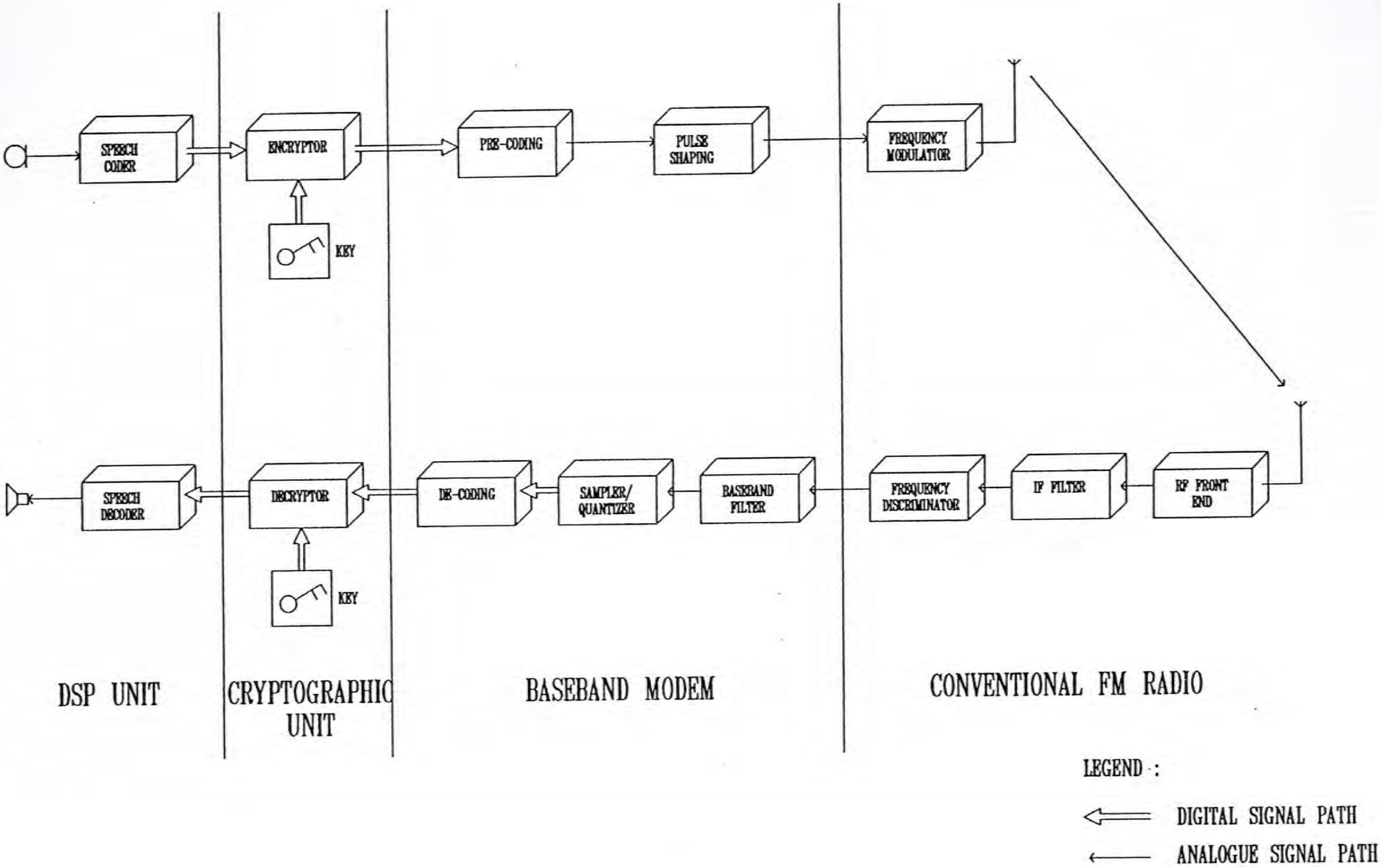


FIG. 18 BLOCK SCHEMATIC DIAGRAM OF A DIGITAL SECURE VOICE SYSTEM

6 SYSTEM IMPLEMENTATION

6.1 POTENTIAL EMC PROBLEMS

In earlier chapters, we have discussed a variety of system concepts, approaches and technicalities in relation to a digital secure LMR for paramilitary application. The fact that we have arrived at a current position where the description of the system implementation is the major tribute, there still remains many essential and practical problems to be solved. For instance, the technology is changing : the prospects for fuller Very Large-Scale Integration (VLSI) of low-power fully monolithic digital radio through the recent advances in high speed silicon technology of Bipolar Complementary Metal Oxide Semiconductor (BiCMOS) has attracted many research efforts [32]. Other important aspects : Frequency (or channel) planning, crypto-key management and some potential electromagnetic compatibility (EMC) problems are particularly emphasized below because they may usually be ignored during the design stage but at a very expensive cost or otherwise for consideration during system implementation.

6.2 Frequency Planning

When using a digital voice ciphering system over VHF/UHF channels there exist close relations between the bit rate

of the coder, the adjacent channel interference and the range. With today's digital modulation systems a coder bit rate of 16 kbit/s or lower excludes practically an adjacent channel operation according to the CCIR Recommendation in the 25 KHz channel spacing. In principle, the ACI could be reduced by lowering the peak modulation to the required level. However, the suffered loss in range would not be acceptable. The optimum in voice quality and range can be achieved with a 16 kbit/s coder and thereby not occupying the adjacent channels. Fig. 19 shows the recommendation of a channel plan with 25 KHz width. In case the occupation of each channel is mandatory then it is the recommendation of coder with 9.6 kbit/s. With this low bit rate the required bandwidth is reduced substantially and favours the system design. However, the voice quality is less than that with 16 kbit/s.

6.3 Key Management

Discussions of security in the past few chapters have concentrated almost entirely on the security of the cipher algorithms. Current interest centres, however, more and more on the management of security aspects, which are of great importance in the operation of large ciphering nets and data storage systems.

The most critical elements of a security set-up are its keys. Nowadays it is a rule that a system must be secure even when the details concerning information processing

and transmission (including the ciphering algorithm) are known. The system security is thus dependent on key rotation, keeping keys secret, the diversity of the keys as well as the prevention of key falsification.

It is clear therefore, that as many aspects of handling secret key information as possible are not left to chance. They are rather planned into the hardware, into the software and into the running and operating procedures. This is referred to as key management which is an essential part of network design and therefore an integral component of the concept for a secure LMR system.

Basically, key management includes the following tributes :

- key generation
- key distribution
- key storage
- key administration
- key verification
- key destruction

Major objectives of each key management scheme are to minimize the key distribution through a physically secure channel (e.g. a courier); to reach a high complexity of the work required by a cryptanalyst to break the system; to use different kinds of keys for maximum security and flexibility; to minimize the amount of obtainable secret information; to use, whenever possible, different kinds of

cipher systems for a distinction between transformation for privacy and for authentification; and to build on existing procedures of the user organization for the storage and distribution of secret information.

From the security point of view, the intervals for key changes are no longer dictated by the security of the equipment, but are mainly a function of the degree of security resulting from the distribution and storage of the keys. The keys must be handled as for any other secret document. Paramilitary organization has to know how secure the documents are which are generated, used and stored in its region and for what period it may be considered secret. This fact is the only criteria dictating the intervals for key changes. The number of people directly involved in the handling of keys must be as limited as possible. Fig. 20 is a schematic diagram of the organisation of key distribution for a paramilitary force.

6.4 Potential Electromagnetic Compatibility (EMC) Problems

In the context of this thesis, the term "electromagnetic compatibility" (EMC) will be taken to refer to the ability of a communication system to operate in conjunction with other electromagnetic systems of both communication and non-communication types. EMC is normally the subject of

emission specifications or guidelines which may, or may not, be the subject of national/international agreements [34].

At its most basic level, EMC depends upon :

(a) The effects of other spectrum users on one's own equipment;

(b) The effects of one's own equipment on other spectrum users.

Both conducted and radiated emissions are potential sources of electromagnetic interference.

At a more sophisticated level, however, in the case of secure communication systems, one may be attempting to counter the efforts of a potential interceptor or disruptor who is employing a high level of technical expertise. Here, emissions at levels which are well below those of the EMC specifications mentioned above may provide information about the nature and functioning of a communication system which might enable its security to be compromised. For this reason, therefore, it is important to examine the design of such systems in far greater depth in order to ascertain whether or not they will be susceptible to this type of threat. The efforts which an interceptor or disruptor will put into his activities will be commensurate with his perception of the value to him of the information being passed by the communication system.

Clearly, to estimate the level of susceptibility, the designer must be aware of the likely nature and performance of the interception and disruption techniques available which could be mounted against the secure communication system.

The security of a communication system is influenced by many factors which will differ in relative importance, depending upon the particular application area. The most important of these factors will now be discussed briefly.

(a) **Traffic Security**

The essential requirement of a secure system is that the data to be trasmitted should be protected by encryption techniques in such a way that unauthorised decoding of the data is impossible (at least, within a time interval where the data would be of value to an interceptor). Non-digital security, e.g. via spectrum scrambling and re-ordering of time segments etc. will, in general, not provide complete security.

(b) **Traffic Flow Security**

The term "traffic flow security" describes the ability of a secure system to conceal from an interceptor the time(s) at which data is being transmitted - as opposed, say, to system idling or control signals. Again, this characteristic of a communication system is determined principally by the nature of the data encryption algorithm and system

control procedures. In some instances, the pattern of system transmission activity could give useful information to a potential interceptor, e.g. in the case of a military command and control network.

(c) **Control of System Parameters**

In general, it is desirable that the spectrum occupancy of a secure communication system should be minimised consistent with maintaining an acceptable performance level. This implies that the transmitted energy should be reduced as far as possible by the use of efficient modulation and coding schemes.

The term "spectrum occupancy" is difficult to define precisely, but it is certainly dependent upon factors such as :

- radiated power levels
- occupied bandwidth of 25 KHz or 12.5 KHz for UHF channels
- spurious product/harmonic levels of better than 80 dB

The relative significance of these factors will again be, of course, application-dependent.

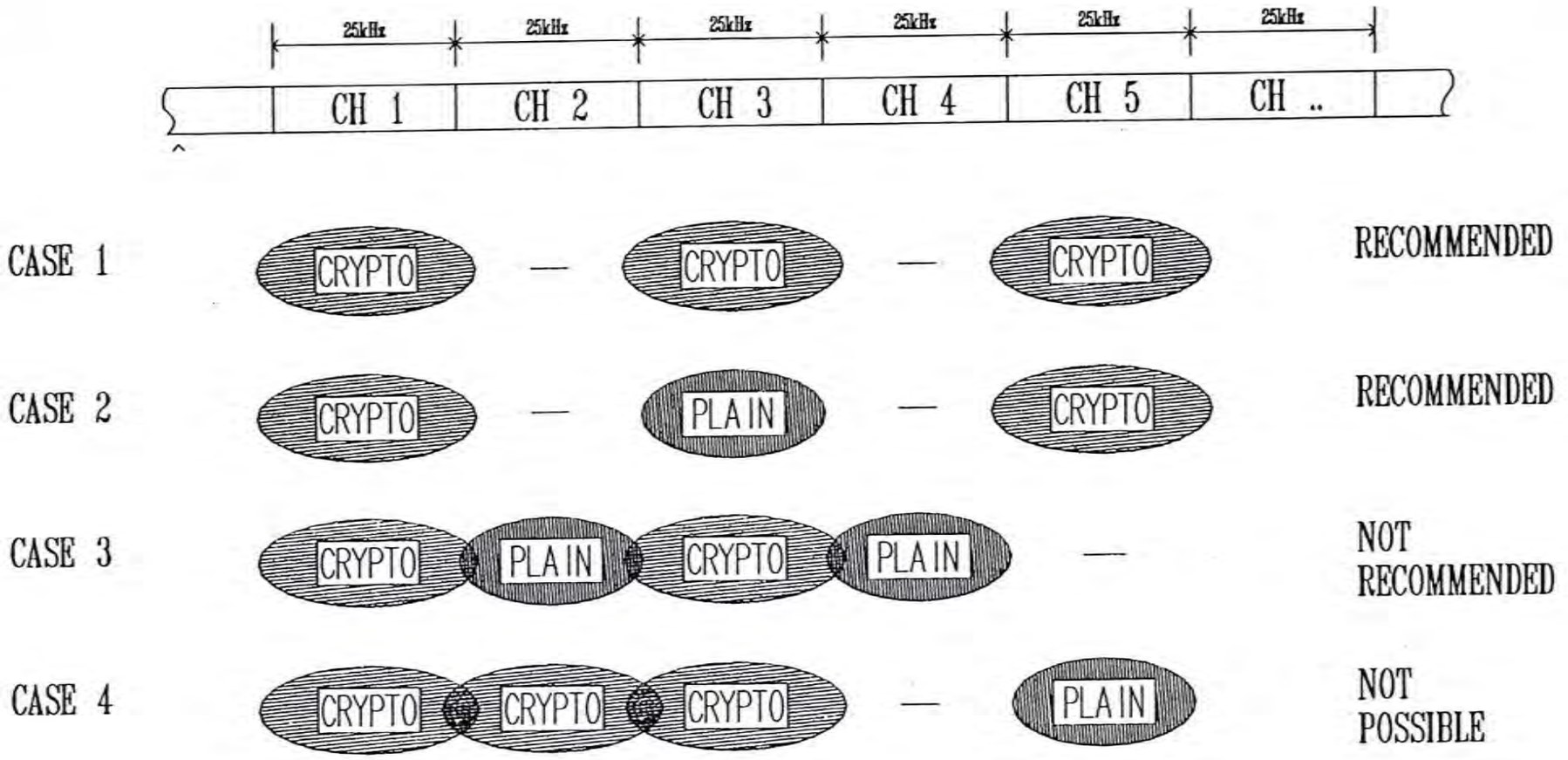


FIG. 19 RECOMMENDATION OF A CHANNEL PLAN WITH 25kHz WIDTH

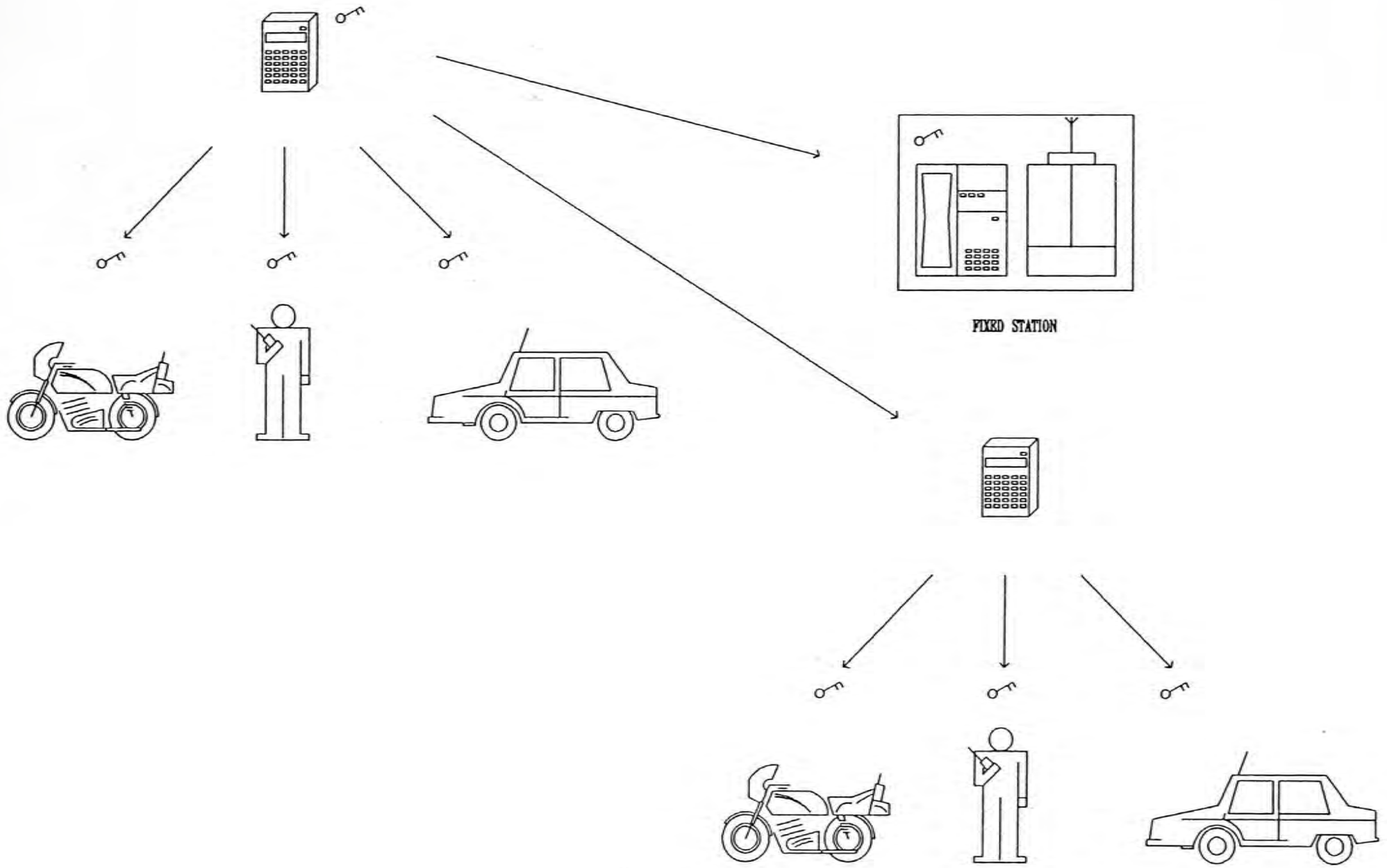


FIG. 20 ORGANIZATION OF KEY DISTRIBUTION

7 CONCLUSION

Fig. 21 shows the variation of speech quality against data rates for voice coders. Since speech coders are assumed to possess comparable quality speech with standard FM system, transmission rate falls within the range from 6 to 12 Kbit/s. Typical gross bit rate in the range of 8 to 9.6 Kbit/s would be a reasonable compromise between the expected audio quality and the required spectrum efficiency at 12.5 KHz channel width. Higher bit rates give better audio quality at the expense of a lower system range and larger bandwidth. A lower bit rate which produces an intelligibility of over 95% DRT would be useful in achieving extra system range with minimum degradation in audio quality. Obviously, none of the existing method can offer a total solution. However, from Fig. 12, it seems that some robust linear predictive coding schemes like self-excited prediction (SELP) and code-excited linear prdiction (CELP) can be singled out as possible candidates whilst SBC with further improvement may deem as an alternative. Indeed, a split-band predictive coder has been implemented to evaluate the performance for digital speech transmission at 8 Kbit/s in this study. Preliminary results by subjective listening tests have illustrated the validity of the technique and further investigation by the author is still undergoing. Furthermore, in order to meet the stringent requirements of paramilitary mobile radio communications, non-error-

propagating stream ciphering method together with pseudo-random hybrid synchronization would be incorporated in conjunction with a spectrally efficient modulation system like GMSK. We envisage that such a system should provide a viable solution for highly encrypted and paramilitary operated LMR communications over a narrowband UHF channel. In addition, with the advances of digital signal processing ICs, a significant reduction in both hardware complexity and system cost is anticipated.

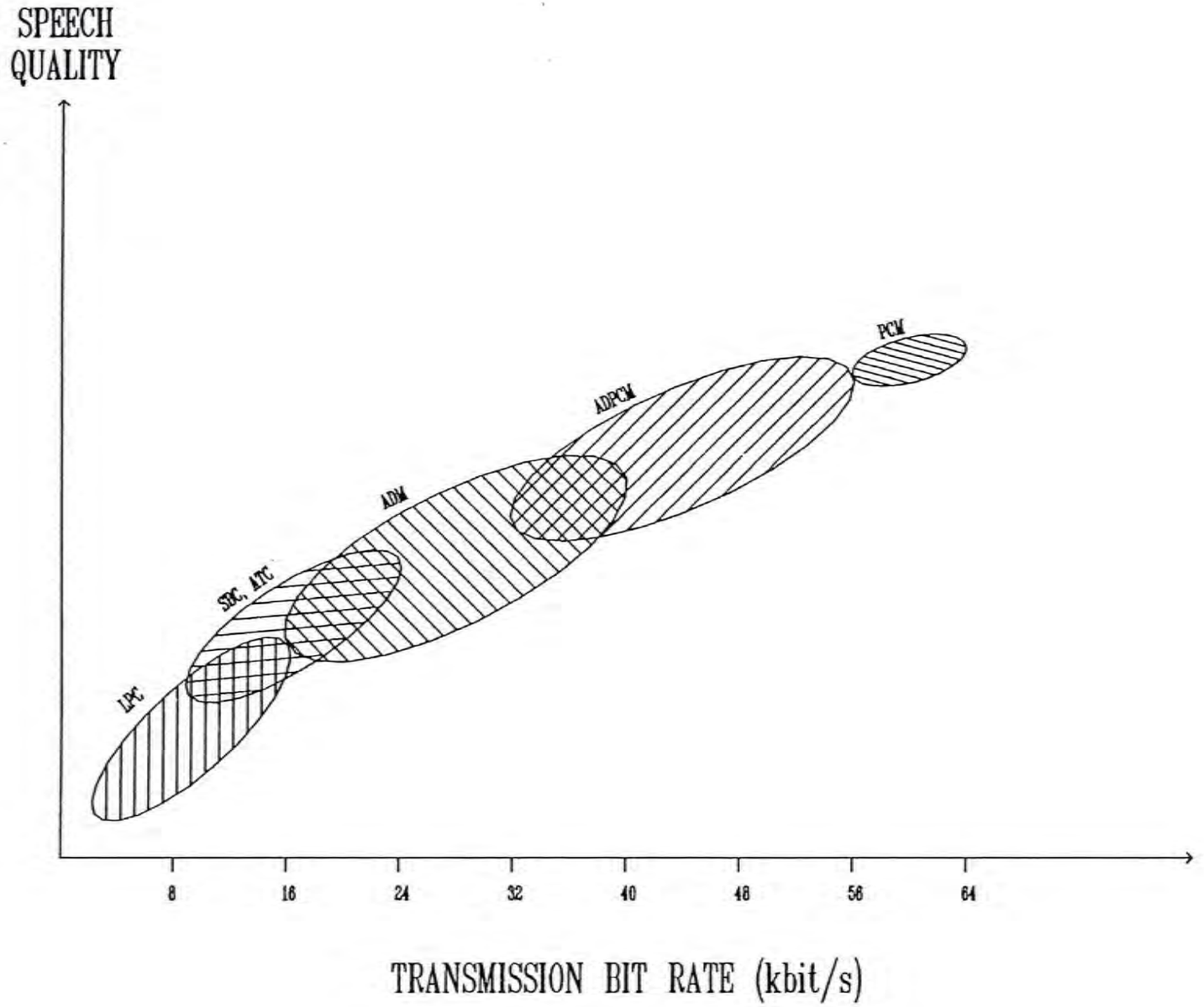


FIG. 21 APPROXIMATE QUALITY VS RATE FOR VOICE CODERS

LIST OF ILLUSTRATIONS

REFERENCES

1. W.C.Y. Lee, **Mobile Communications Engineering**, New York : McGraw-Hill, 1982.

2. A.D. Kucar, **Mobile Radio : An Overview.** IEEE Communications Magazine, Nov. 1991, pp. 72-85.

3. M.J. McLaughlin and P.C. Rasky, **Speech and Channel Coding for Digital Land-Mobile Radio**, IEEE J. Sel. Areas Commun., Vol. SAC-6, no. 2, pp. 332-345, Feb. 1988.

4. D.E. Borth, M.J. McLaughlin, and J.J. Mikulski, **Implementation of a digital mobile radio incorporating combined modulation/coding**, in Proc. 2nd Nordic Seminar on Digital Land Mobile Radio Commun., Oct. 14-16, 1986, pp. 85-89.

5. A. Maloberti, **Radio transmission interface of the digital pan-European mobile system.** 39th IEEE Veh. Technol. Conf., San Francisco, CA, May 1989, pp. 712-717.

6. J.E. Natvig, **Evaluation of Six Medium Bit-Rate Coders for the Pan-European Digital Mobile Radio System**, IEEE J. Sel. Areas Commun., Vol. SAC-6, no. 2, Feb. 1988, pp. 324-331.

7. H.J. Beker and F.C. Piper, **Analogue Speech Scrambling.** New Electronics, Vol. 15, no. 17, 1982 pp. 28-32.

8. N.S. Jayant, **Analogue Scramblers for Speech Privacy.** Computers and Security, Vol. 1, 1982, pp. 275-289.

9. C.K. Wong and P.C. Ching, **Digital Speech Transmission for Highly Encrypted and Paramilitary Operated Land Mobile Radio Communications over a Narrowband UHF Channel.** 3rd IEE Conf. on Telecom., Edinburg, 17-21 March 1991.

10. D. Muilwijk, **Tamed Frequency Modulation - a bandwidth saving digital modulation method, suited for mobile radio.** Philips Telecom Review, Vol. 37, No. 1, March 1979.

11. H.J.M. Steeneken and T. Houtgast. **A physical method for measuring speech transmission quality.** J. Acoust. Soc. Am. 67, 1980, pp. 318-326.

12. P. Constantinon and S.J. Toway, **Digital transmission over conventional mobile channels : maximum bit rate.** ICC'81, June 1981.

13. **Digital transmission in the land mobile service.** CCIR Report 903 Red Book, 1982.

14. K.W. Cattermole, **Principles of pulse code modulation.** Iliffe, 1969.

15. J.D. Markel and A.H. Gray, **Linear prediction of speech.** Springer-Verlag, 1976.

16. E.V. Stansfield, **Speech processing for low data rate digital voice communications.** Sijthoff & Noordhoff, 1978.

17. B.S. Atal and S.L. Hanauer, **Speech analysis and synthesis by linear prediction of speech wave.** Journal of the Acoustical Society of America. Vol. 50, 1971, pp. 583-590.

18. P.C. Ching and K.C. Ho. **An efficient adaptive LSP method for speech coding.** Proc. IEEE Region 10 Conference on Computer and Communication Systems, Hong Kong, 24-27 September, 1990, pp. 324-328.

19. R.V. Cox, Hagenauer, N. Seshadri and C.E.W. Sundberg, **Subband speech coding and matched convolutional channel coding for mobile radio channels.** IEEE Trans. on signal proc. Vol. 39 No. 8, Aug 91, pp. 1717-1731.

20. N. Kitawaki, M. Honda, and K. Itoh. **Speech-Quality Assessment Methods for Speech-Coding Systems.** IEEE Commun. Magazine, Vol. 22, No. 10, 1984, pp. 26-33.

21. N. Kitawaki and H. Nagabuchi, **Quality Assessment of Speech Coding and Speech Synthesis Systems.** IEEE Commun. Magazine, Vol. 26, No. 10, Oct. 1988, pp. 36-44.

22. H.J. Beker and F.C. Piper, **Digital Speech Scrambling.** New Electronics, Vol. 15 No. 18, 1982, pp. 94-100.

23. N.R.F. Mackinnon, **The Development of Speech Enciphering.** The Radio and Electronic Engineer, Vol. 50, 1980, pp. 147-155.

24. K. Ohno and F. Adachi, **Performance evaluation of various decision schemes for frequency demodulation of narrowband digital FM signals in land mobile radio.** IEEE Trans. on Vech. Techn., Vol. 39 No. 2 May 1990, pp. 109-116.

25. K. Murota, K. Kinoshita and K. Hirade. **Spectrum efficiency of GMSK land mobile radio.** ICC'81, June, 1981.

26. K.S. Chung, **Generalized tamed frequency modulation and its application for mobile radio communications.** IEEE J. Select. Areas Commun. Vol. SAC-2, July, 1984, pp. 487-497.

27. T. Aulin and C.E. Sundberg, **Continuous phase modulation - Part 1 : Full response signalling.** IEEE Trans. Commun., Vol. COM-29, pp. 196-209, Mar. 1981.

28. T. Aulin, C.E. Sundberg and N. Rydbeck, **Continuous phase modulation - Part 1 : Partial response signalling.** IEEE Trans. Commun., Vol. COM-29, pp. 210-245, Mar. 1981.

29. M. Hirono, T. Miki, and K. Murota, **Multilevel decision method for band-limited digital FM with limiter-discriminator detection.** IEEE J. Select. Areas Commun., Vol. SAC-2, pp. 498-506, July 1984.

30. F. Adachi and K. Ohno. **Performance analysis of GMSK frequency detection with decision feedback equalization in digital land mobile radio.** Proc. IEE, pt. F, Vol. 135, pp. 199-207, June 1988.

31. T. Andersson and A. Svensson. **Error probability for a discriminator detector with decision feedback for continuous phase modulation.** Electron. Lett., Vol. 24, pp. 753-754, June 1988.

32. M.A. Copeland. **VLSI for Analog/Digital Communications**, IEEE Commun. Magazine, May 1991, pp. 25-29.

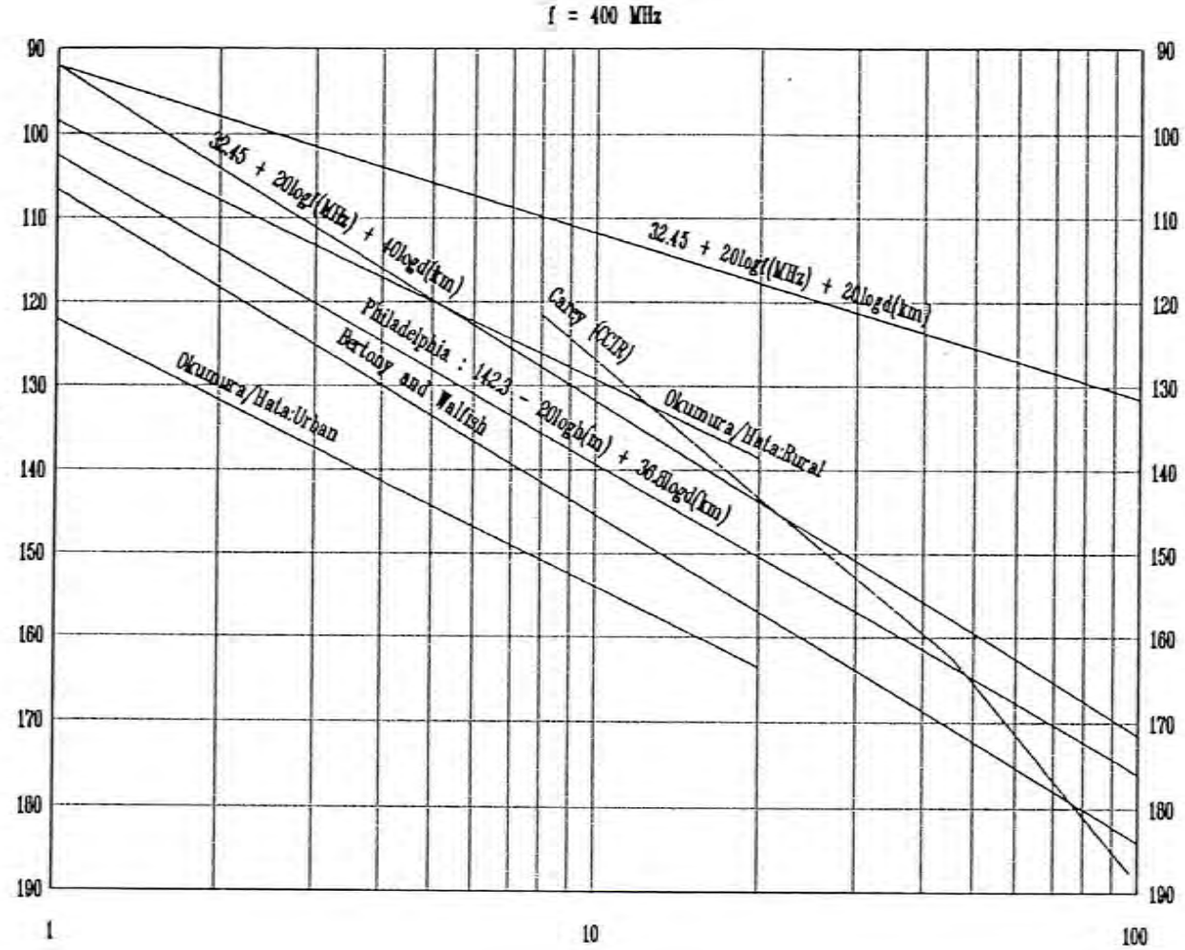
33. F.K. Soong and B.H. Juang. **Line Spectrum Pair (LSP) and Speech Data Compression**, Proc. ICASSP-84, pp. 1.10.1-1.10.4, 1984.

34. M. Darnell and A.C. Marvin. **Potential EMC Problems in the Design of Secure Communication Systems**, Int. Conf. on secure Commun. system, London, U.K. 22-23 Feb. 1984, pp. 38-43.

APPENDICES

I. Path Propagation Loss (L) Vs Distance (d)

II. Speech Quality Assessment Tests performed by Special Duties Unit (SDU)



PATH PROPAGATION LOSS (L) VS DISTANCE (d)

Appendix II

Speech Quality Assessment Tests performed by SDU

I.1. Introduction

The CCITT, in Recommendation G.106, defines quality of service as "the collective effect of service performances which determines the degree of satisfaction of the user of the service. The primary and the most important measure of service quality should be "user satisfaction". This means that an essential aspect of a service performance evaluation is the opinion of the users. In recent years, CCITT has standardized several digital speech coding process (e.g. A- and u-law PCM in Recommendation G.711 and narrow- and wideband ADPCM in G.721 and G.722, respectively), and Recommendation for other processes, such as DCME, are being prepared. To provide the means for assessing how these digital speech coding processesd will affect the performance of telecommunication services from the users' viewpoint, several CCITT Study Groups- and principally Study Group XII (Transmission performance of telephone networks and terminals)- have prepared Recommendations and Supplements describing assessment methods. These methods can be categorized as subjective or objective. The purpose of this appendix is to study these assessment methods and also to briefly report the results from a field trials performed by the SDU of RHKP.

In general, subjective testing is required to assess the performance of new digital coding processes. Subjective testing provides a method for obtaining an empirical relationship between customer opinion and impairment levels. In some cases, subjective-test results have been used to develop objective customer-opinion models. These models, in some instances, can be used instead of subjective testing to assess the quality of a new digital coding process, but usually only for fairly simple and well behaved processes.

I.2. Methods for subjective assessment

Subjective assessment methods can be categorized in numerous ways : laboratory versus field experiments, convwersational versus listening tests, and single stimulus rating versus paired comparisons. Results can be obtained in terms of overall quality, listening effort, percentage difficulty, intelligibility, naturalness or some other scale. Laboratory experiments typically provide results faster and less expensive than field trials, but may be difficult to design so that sufficient realism is provided. Field trials can offer the necessary realism but are costly to conduct, and it is often difficult to maintain control over all the variables that may influence customer opinion. Usually laboratory tests are conducted first, and if deemed necessary, they are followed by field trials.

I.3. Speech Quality Assessment Tests performed by SDU

Subjective speech quality assessment tests on various speech coding schemes were performed by SDU with a view to identifying an operationally acceptable scheme for field tactical purposes. Voice quality is firstly expressed in terms of the mean opinion score (MOS) of subjective evaluation by SDU officers. Details of subjective assessment scales were given at table 1.

The subjective tests were carried out in two stages. First, a typical passage of operational instructions was tape recorded through radio transmissions of which radio equipments of bit rates from 9.6 Kbit/s to 16 Kbit/s were tested. Listening tests for a large number of operational staff were then taken place to poll their opinion. Second, field trials simulating to some realistic operating scenarios were performed on the equipment. Most unfortunately, the fullest details of the above tests are confidential and could not be released. However, it is concluded that the 16 Kbit/s CVSD is unanimously agreed as an acceptable bit rate by SDU.

Table 1

Subjective assessment scales

Grade	Quality	Listening effort	Degradation
4	excellent	complete relaxation possible, no effort required	degradation is inaudible
3	good	attention necessary, no appreciable affort required	degradation is audible but not annoying
2	fair	moderate effort required	degradation is slightly annoying
1	poor	considerable effort required	degradation is annoying
0	bad	no meaning understood with any feasible effort	degradation is very annoying