1 Introduction

Peter Stavroulakis

1.1 Why TETRA

If someone has been following the recent (last five years) International events both in the sphere of technical developments but also in the International politics, he would have noticed that there is a general outcry for the development of secure telecommunication systems covering all aspects of wireless communications. This situation has become much more serious and demanding because of the fact that wireless technology evolution is accelerating to satisfy the ever increasing market demands for more mobility to all kinds of telecommunications services whether they involve voice, IP, Video, WLANS, Ad-Hoc, Mesh, Peer- to-Peer and Sensor Networks to name a few.

This newly created demand, a large part of which comes from the public and private safety sectors such as police, fire brigades, ambulances (telemedicine) and the private sector such as the trucking transport businesses, airport safety authorities e.t.c, is being satisfied by the Public/Private Mobile Radio(PMR) systems. These systems have, on one hand, the general characteristics of cellular systems but, on the other hand possess such unique security characteristics such as end to end encryption, field control by a dispatcher type of capabilities as well as trunking(switching) capability and thus create autonomous telecommunications systems and distinct from cellular.

In this book, we are examining this evolution and we are showing that TETRA is the best candidate to satisfy all above requirements whether they are technological, security or service oriented. The reader who is not familiar with the fundamental aspects of PMR or TETRA is referred to [1 and 2]. Since TETRA was developed mainly for voice communications, the European Telecommunications Standards Institute (ETSI) which is responsible for developing its standards at least for Europe, is continuously updating its them in order to meet new requirements. See chapter 7. We, in this book, examine new ways and go one step further to prove that further improvements and innovative techniques, which we hope one day will become TETRA standards, can make TETRA the building block for future security networks for universal use. As a matter of fact we propose, in the Appendix, a general scheme which is based on the results presented in the chapters 2-7 and on references 2 and 3 that TETRA not only could become the building block for integrating WLANS and Ad-Hoc networks into unified networks for providing general wireless services but will also serve as a global security tool through the use of the proposed chaotic based encryption and/or modulation techniques.[3, 4].

We show in Chapter 2 the basic features of the class of systems to which TETRA belongs, their basic configurations, the different technologies used and the problems that present in their usage as security tools in the Private Mobile Radio (PMR) communications field. Actually, even though these systems have been designed as the security alternatives of their public equivalents such as the GSM, still they have limitations which are pointed out. As the best candidate to satisfy modern security requirements, we present TETRA. It is shown, by identifying the elements on which a comparison of the requirements with its special features of the evolving standards and the improvement that are possible for TETRA, that TETRA can play a major role in the next generations of PMR systems. This comparison takes place in chapter 3 where the differences between TETRA and a GSM solution are analysed in three dimensions in the hope to exhibit the clear and perhaps unique advantages of TETRA for security applications as will be shown in the subsequent chapters. The first dimension compares the applicable ETSI specifications and points out which functions are available according to the standards. Proprietary solutions will not be discussed on that level. The second dimension, a technical analysis, discusses how the end users and the operators perceive the differences between the network-solutions. Since it is possible technically to provide TETRA capabilities using GSM, an economic analysis focusing on the cost of the two alternative solutions, including capital and operational costs for the network infrastructure and end-user terminals which constitutes the third dimension, will be touched upon only briefly because the applications of secure systems do not depend as much on economic terms but on their technical feasibility and the existence of international standards and on their ability to satisfy certain predefined requirements. We go one step further, in chapter 4, to show that the TETRA system can be improved to become an unique tool for security. First area of enhancement is the channel assignment methodology. We first provide an overview of different channel assignment algorithms as they relate to TETRA Networks and compare them in terms of performance, flexibility, and complexity. We first start by giving an overview of the channel assignment problem in a cellular environment and we discuss the general idea behind major channel allocation schemes. Then we proceed to discuss different channel allocation schemes within each category and we follow with the development of an optimization technique in channel assignment. Finally we present multiple access techniques in section 4.3.

In chapter 5 we present the scheme by which we can transmit securely VIDEO through TETRA. Within the context of this chapter, we monitor the QoS regarding MPEG-4 video streaming traffic delivery, in terms of both packet loss and perceived image quality, over TEDS networks.

The rest of the chapter is organized as follows. In Section 5.2, we attempt to follow the evolution in public safety mobile networks and the role of TETRA networks. The need for more complex context in the information exchange, guaranteed quality of service and secure, flexible and scalable infrastructures led to the standardization of TETRA and TEDS systems. Section 5.3, includes an extensive overview of data transmission over TETRA, followed by an insight on the evolutions incorporated in TEDS standard that allowed video and high data rates support. A detailed analysis of the current video encoding techniques and error concealment methods are contained in Section 5.4. Particular interest is given to MPEG-4 encoding standard as it enables higher video compression rates, thus making it an ideal solution for video traffic over TETRA and TEDS networks. The main two techniques of video encryption are described in this section as well. In the following Section 5.5, we provide a performance analysis of video transmission over TEDS network.

In this chapter 6, we present an overview of packet data transmission over Terrestrial Trunked Radio (TETRA) release 1 networks as well as a solution for integrating TETRA with WLANs as a way to improve the packet data transmission capabilities. We first give a brief overview of the TETRA air interface and the available logical and physical channels. We then present various aspects of packet data transmission over TETRA, where we conclude that TETRA release 1 cannot provide the means to support demanding IP-based applications, mainly due to bandwidth and QoS constrains. Motivated from this conclusion, we then present a solution for integrating TETRA with Wireless Local Area Networks (WLANs) and thus realizing hybrid broadband networks suitable to support the next generation of public safety communication systems. The specified solution allows TETRA terminals to interface to the TETRA Switching and Management Infrastructure (SwMI) over a broadband WLAN radio access network, instead of the conventional narrowband TETRA radio network. These terminals are fully interoperable with conventional TETRA terminals and can employ all TETRA services, including group calls, short data messaging, packet data, etc.

Possible extensions of the TErrestrial Trunked RAdio (TETRA) system with the purpose of building a mesh network are analyzed in chapter 7. The main objective is to provide the services, already offered by PMR systems, everywhere and at any moment, taking then profit of the natural advantages that a mesh network presents. We evaluate extensions which make use of already available functionality of TETRA, such as client, relay and gateway functions, in order to minimize the changes that should be made to the standard and make the adaptation as simple as possible. Finally in the Appendix we show that TETRA can be used as a building block for universal super-secure systems using chaotic techniques.

References

1. J. Dunlop et.al, Digital Mobile Communications and the TETRA System, John Wiley 1999.
2. Doug Gray, TETRA : The Advocate's Handbook, Pryntya, 2003
3. Peter Stavroulakis, Chaos Applications in Telecommunications, Taylor and Francis 2006
4. Peter Stavroulakis, Secure Telecommunication Systems based on Chaotic and Interference Reduction Techniques, Pending International Patent PCT/GR000038