THESIS SUMMARY

„Improving the efficiency of radio communications networks security"

Author: Eng. Cristian-Gabriel Apostol

Email: crs.apostol@gmail.com, tel: 0761 693 445

Ph.D. supervisor: prof.univ.dr.ing. Ciprian Răcuciu

In **Chapter I**, the context and introductory elements of the thesis are presented together with some general aspects of radio communications standards and the security they provide. Then the main purpose of the paper and the secondary objectives pursued to achieve it are presented. The results obtained by following this stated plan can be found in the next chapters.

Chapter II is dedicated to presenting the main features of Information Security, focusing on the techniques and principles applied in this paper. The security services are defined and then the security mechanisms used to implement these security services are described.

In **Chapter III** the communications standards on radio carriers are introduced, achieving a parallel in terms of technology between the cellular networks family and the wireless networks family. This parallel is made also in chronologically, to highlight the main technologies that led to the development of the new radio standards.

Chapter IV focuses on describing the techniques of subscriber authentication in radio networks, following the technologies presented in Chapter III. In this chapter reviewing the security mechanisms used by wireless networks is done, focusing on the authentication concept. The notion of entity authentication is a notable component of Information Security, with particular focus in the current radio networks and their future developments, because often encryption is based on entity and data authentication. An analysis of current authentication in wireless and cellular networks is performed in Chapter IV, and proposals for improvements of these methods can be found in Chapters V and VI.

Chapter V has a practical approach, analyzing the authentication process within WiMAX networks and streamlining the process of improving the efficiency using digital certificates on an existing live network with minimal disruption to services. Improved authentication with minimum downtime on services, which can be critical with a particular focus in national security, is an objective of this thesis.

Also in this chapter the authentication process of the globally deployed 4G LTE networks is analyzed, identifying a notable vulnerability in authentication and proposing an improvement based on the introducing the concept of "Security Request Vector".

In **Chapter VI** applications, proposals and improvements are carried out regarding the security algorithms that can be applied in interconnected multi-technologies radio networks, highlighting the components that can be secured and the role of each of these algorithms.

In addition to the classic problems addressed by existing standards in securing cellular and wireless networks, there are certain vulnerabilities not formally approached yet that we want to point out and resolve. Securing radio planning data using the Digital Watermarking techniques, both during transmission and storage is discussed and implemented in this chapter, which represents another objective of this thesis. More specifically algorithms using

Digital Watermarking combined with the Chaos Theory have been developed and tested, which can be used to protect the network confidential planning data, represented through images and graphics. These algorithms are divided into two categories: fragile and robust algorithms based on the role they have in the protection of data integrity or data origin authentication.

Through these networks data can be transmitted in both an encrypted and unencrypted way. The two possibilities are discussed by the existing cellular and wireless standards, but the idea of using the steganographic methods can assure the secured transmission of confidential information without attracting the attention of eavesdroppers. The technique is analyzed and applied in the thesis, proposing improvements for steganography algorithms in Chapter VI.

In this chapter we will also analyze the security level offered by the standards discussed during the paper, in regard to the data transport between the base stations and the core network or gateway point for services access, addressing the possibility of increasing the security of cellular and wireless networks by securing these interfaces using the IPSEC protocol.

Chapter VII is represented by the final conclusions of the paper, highlighting the main contributions both theoretical and practical made during the research conducted within the doctoral studies program, marking also the perspectives and future research directions for improving the security level of wireless and cellular networks.