DEFTA Costinela-Luminița, **IACOB Nicoleta Magdalena**, *Role of Threshold Cryptography in MANET Security*

Abstract

MANET (Mobile Ad Hoc Networks) are wireless networks formed spontaneously between certain devices such as computers, sensors, mobile phones and others. Because these devices are mobile, they have the following limitations: limited resources (battery, memory, processing power) and doesn't have a central routing device (router) and so each node must ensure also this function. In addition, the network structure changes dynamically as needed. Because of these characteristics, the ad-hoc networks raise many security issues. In this paper we will review some of these problems and we will present some methods to improve their security. We will focus on the solutions that involve threshold cryptography, which is suitable to redundantly fragment the message into multiple parts. Threshold cryptography is already used in computer networks to provide security in terms of availability, confidentiality, and secure key or data distribution, but we will investigate what makes it difficult to implement it in MANET.

Keywords: *MANET, security, network, wireless, threshold, cryptography.*

AMS Classification: 94A60, 68P25