TCSAP: A New Secure and Robust Modified MANETconf Protocol

Abdelhafid Abdelmalek[1,2], Zohra Slimane[1], Mohamed Feham[1], and Abdelmalik Taleb-Ahmed[2]

[1] STIC Laboratory University of Tlemcen Algeria
[2] LAMIH Laboratory University of Valenciennes France
{a_abdelmalek,m_feham,z_slimani}@mail.univ-tlemcen.dz,
abdelmalik.Taleb-Ahmed@univ-valenciennes.fr

Abstract. Different protocols have been developed throughout the last years to achieve automatic IP address allocation in Mobile Ad hoc Networks (MANETs). However, Autoconfiguration security issues are still an open problem. In this paper, a new secure and robust IP Address allocation protocol for standalone MANETs inspired from MANETconf and named TCSAP is specified and evaluated within NS2. The proposed solution is efficient and thwarts all possible attacks associated with dynamic IP address assignment in MANETs.

1 Introduction

In the last decade, large research efforts have been made to address challenges posed by MANETs, These challenges include mainly IP address autoconfiguration, routing, security and QoS issues. In security context, the major part of research up to now was concentrated mainly on trust models and routing security problems. However, the lack of security in previously suggested autoconfiguration schemes can lead to serious attacks in potentially hostile environments, mainly IP spoofing attack, sybil attack, traffic overload DoS attack, exhaustion address space attack, and conflict address attack. This problem was tackled by some few papers [1]-[5]. We have analyzed these proposals and pointed out their weaknesses and shortcomings in [13]; we have identified also the imperative security requirements related to this problem. In the present paper, we propose a new robust and secure stateful IP address allocation protocol for MANETs, by applying a cooperative security scheme to cope with malicious nodes including misbehaving nodes that could be compromised by potential adversaries. The scheme relies on a fully distributed Certification Authority based trust model in conjunction with a threshold signature scheme for issuing and revoking certificates, and 'On-line Joint IP Address and Public Key Certificate' ; this solves definitively the problem of some attacks such as IP spoofing and Sybil attacks, unsolved up to now by conventional mechanisms. The remainder of the paper is organized as follows. In section 2, we develop our secure and robust autoconfiguration scheme on the basis of threshold cryptographic tools. Section 3 is devoted

A. Özcan, J. Zizka, and D. Nagamalai (Eds.): WiMo/CoNeCo 2011, CCIS 162, pp. 73–82, 2011.