Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 5, Issue 2; April-June, 2018, pp. 92-92
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/Publication.html

Improving Security Mechanism of ECC Keys using Techniques of Soft Computing

Ekta Narwal[1] and Sumeet Gill[2]

[1,2]Departmentof Mathematics, M.D. University, Rohtak, Haryana, India
E-mail: [1]ekta narwal@yahoo.com, [2]drsumeetgill@gmail:com

Abstract—*Vehicular Ad Hoc Networks (VANETs) are the branch of Mobile Ad Hoc Networks (MANETs) in which moving vehicles act as routers and nodes to form a network. In VANETs many cryptographic approaches are used to make the communication secure. Some of them are symmetric key approaches, public key approaches, certi_cate revocation, pseudonym based approaches, identity-based cryptography, identity-based signature, Elliptical Curve Cryptography (ECC) etc. All these techniques use public and private keys for enhancing the security of messages and these keys are stored on hardware devices in VANETs. All these hardware devices are protected by the cryptographic algorithms. The details of all these algorithms and their online simulators are freely available and can be easily intruded. So we need to enhance the security of these keys. In this paper we worked on ECC keys stored in TPDs (Temper Proof Devices) of VANETs. In our experiment we used Arti_cial Neural Networks for all the simulations and for enhancing the security of ECC keys.*

Keywords: *VANETs (Vehicular Ad Hoc Networks), TPD (Temper Proof Devices), ECC (Elliptical Curve Cryptography), ANN (Arti_cial Neural Networks).*

1