Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 12, December 2013, pg.100 – 106

RESEARCH ARTICLE

Performance Evaluation of Various Attack Detection Techniques in VANET

Noble Mary Juliet.A [1], Joan Pavithra.R[2]

[1]Department of Computer Science and Engineering, NPR College of Engineering and Technology, India

[2] Department of Computer Science and Engineering, NPR College of Engineering and Technology, India

[1]joanp19@gmail.com

Abstract— Vehicular communications play a substantial role in providing safety transportation by means of safety message exchange. Researchers have proposed several solutions for securing safety messages. Vehicular ad hoc networks aim at enhancing road safety by providing vehicle-to-vehicle communications and safety related applications. But safety-related applications, like Local Danger Warning, need a high trust level in received messages. Indeed, decisions are made depending on these messages. To increase the trustworthiness of these messages various detection techniques are used to detect the attackers in the VANET. But most of these techniques concentrate only on outsider attackers rather than insider attackers. In this research we discuss the various detection techniques such as dynamic thresholds based detection, filtering false data via authentic consensus, and efficient threshold-based event validation that are used to detect the insider attacks in VANET. Then we analyze the performance of these techniques using their simulation results.

Keywords— VANET; Dynamic-Thresholds; authentic consensus; Efficient and secure threshold-based event validation; Proof-of-Relevance

FULL TEXT: HTTP://WWW.IJCSMC.COM/DOCS/PAPERS/DECEMBER2013/V2I12201320.PDF