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. 3, Issue. 2, February 2014, pg.476 – 482

RESEARCH ARTICLE

PRECIPITATE MESSAGE MANIFEST PROTOCOL FOR VEHICULAR AD HOC NETWORKS

[1]Ramya. K, [2]Nithya. N

[1]PG scholar, Department of Computer Science and Engineering, Anna University Chennai, India

[2]Assistant Professor, Department of Computer Science and Engineering, Anna University Chennai, India

[1,2]Ranganathan Engineering College, Coimbatore

[1] ramyacse015@gmail.com, [2] Nithya.varsha1@gmail.com

Abstract* - *Vehicular ad hoc networks (VANETs) adopt the Expedite Message Authentication Protocol (EMAP) and Certificate Revocation Lists (CRLs) for their security. In any EMAP system, the authentication of a received message is performed by checking if the certificate of the sender is included in the current CRL, and verifying the authenticity of the certificate and signature of the sender. In this paper, We propose a Message Authentication Acceleration (MAAC) protocol for VANETs, which replaces the time-consuming CRL checking process by an efficient revocation check process. The revocation check process uses a keyed Hash Message Authentication Code (HMAC), where the key used in calculating the HMAC is shared only between non-revoked On- Board Units (OBUs). The MAAC protocol uses a novel probabilistic key distribution, which enables non-revoked OBUs to securely share and update a secret key .By conducting security analysis and performance evaluation, the MAAC protocol is demonstrated to be secured and efficient.

Keywords – Vehicular Networks, Message Authentication, Certificate Revocation, Communication Security, ECDS algorithm

---

Full Text: http://www.ijcsmc.com/docs/papers/February2014/V3I2201479.pdf