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. 8, August 2013, pg.70 – 75

RESEARCH ARTICLE

AIM OF PROTECTED ROUTING MESSAGE AUTHENTICATION PROTOCOL FOR VEHICULAR AD HOC NETWORKS

R. UmaSaraswathi[1], N. Kavitha[2], G. KesavaRaj[3]

[1]Research Scholar, Department of Computer science, Vivekanandha College, Elayampalayam, Tiruchengode-637205, India

[2]Research Scholar, Department of Computer science, Vivekanandha College, Elayampalayam, Tiruchengode-637205, India

[3]Assistant Professor, Department of Computer Application, Vivekanandha College, Elayampalayam, Tiruchengode-637205, India

[1] umaraj.tg@gmail.com; [2] msckavithan@gmail.com; [3] kesavaraj@gmail.com

Abstract— Vehicular ad hoc networks (VANETs) recognize the Public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs) for their safety. In some PKI system, the certification of a predictable message is performed by examination if the certificate of the sender is included in the current CRL, and verifying the genuineness of the certificate and signature of the sender. In this paper, we recommend an Aim of protected Routing Message Protocol for VANETs, which replaces the lengthy CRL examination route by an efficient revocation checking process. The revocation check process in PRMAC uses a keyed Hash Message Authentication Code ð PRMAC, where the key used in calculating the PRMAC is shared only between non revoked On-Board Units (OBUs). In addition, PRMAC uses a novel probabilistic key delivery, which enables non revoked OBUs to securely share and update a secret key. PRMAC can extensively reduce the message loss ratio due to the message verification delay compare with the traditional authentication method employing CRL. By perform security analysis and presentation evaluation, PRMAC is confirmed to be protected and resourceful.

Key Terms: - Certificate Revocation; Communication Security; Hash Message; Message Authentication; Vehicular Networks

Full Text: http://www.ijcsmc.com/docs/papers/August2013/V2I8201325.pdf