260. PROFICIENT PRIVACY- SECURED AUTHENTICATION FOR VANETS

Sridevi Karpaga G.S (deviscrest@gmail.com)
Pugalenthi R (Associate Professor) (rpugalsir@gmail.com)
Department of Computer Science & Engineering
St.Joseph's College of Engineering, OMR, Chennai.

Vehicular ad hoc network (VANET) is trending technology for wireless sensor network that uses car as a mobile device (wireless node). VANET is used to provide privacy, security and authentication to the vehicles. In existing schemes communication occurs between road side unit (RSU) and vehicles which is based on group signatures , suffer from computation delay in the certificate revocation list (CRL) leading to high message loss during signature verification process. As a result security is less and VANET cannot be used efficiently. Thus a scheme is proposed where in communication occurs between vehicle to vehicle. A hash message authentication (HMAC) is been used to reduce time consuming CRL checking, ensuring the integrity of the messages and trusted authority (TA) provides authentication to vehicles. Finally the security is performance analysis shows this scheme is more efficient in terms of authentication and privacy in VANET [1].

Index Terms - Batch group signature, Road Side Unit (RSU), Certificate Revocation List (CRL), hash message authentication code (HMAC) , Vehicular Ad hoc Network (VANETs).

ISBN 978-81-904760-6-5