TECHNOLOGIES

abtechchennai@gmail.com
www.abtechnologies.in
9840511458

A CONDITIONAL PRIVACY PROTECTION SCHEME BASED ON RING SIGNCRYPTION FOR VEHICULAR AD HOC NETWORKS

ABSTRACT

Vehicular ad hoc networks (VANETs) leverage information and communications technology to make transportation systems intelligent, safe, and efficient, hence improving people's driving experience. Unfortunately, due to the openness of wireless channels and vehicular mobility, privacy leakage in VANETs poses serious privacy concerns. Once a user's identity is leaked, it will cause serious threats to his/her property and personal safety as a malicious attacker, such as a stalker could utilize the targeted identity to track particular driver and/or launch malicious attack. To address such a privacy problem, by observing the nice properties of ring signature like anonymity, spontaneity, flexibility, and membership equality, we design a novel conditional privacy protection scheme based on ring signcryption, which utilizes the salient features of identity-based cryptosystems and ring signature to achieve conditional privacy. Through security analysis and experiments, we have demonstrated the advantage of our scheme over most existing solutions.