ABSTRACT

A Vehicular Ad-Hoc Network or VANET is a technology that uses moving cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range.

We propose a distributed key management framework based on group signature to provision privacy in vehicular ad hoc networks (VANETs). Distributed key management is expected to facilitate the revocation of malicious vehicles, maintenance of the system, and heterogeneous security policies, compared with the centralized key management assumed by the existing group signature schemes. In our framework, each road side unit (RSU) acts as the key distributor for the group. We address the issue of large computation overhead due to the group signature implementation. A practical cooperative message authentication protocol is thus proposed to alleviate the verification burden, where each vehicle just needs to verify a small amount of messages.