World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:11, No:04, 2017

Message Authentication Scheme for Vehicular Ad-Hoc Networks under Sparse RSUs Environment

Authors : Wen Shyong Hsieh, Chih Hsueh Lin

Abstract : In this paper, we combine the concepts of chameleon hash function (CHF) and identification based cryptography (IBC) to build a message authentication environment for VANET under sparse RSUs. Based on the CHF, TA keeps two common secrets that will be embedded to all identities to be as the evidence of mutual trusting. TA will issue one original identity to every RSU and vehicle. An identity contains one public ID and one private key. The public ID, includes three components: pseudonym, random key, and public key, is used to present one entity and can be verified to be a legal one. The private key is used to claim the ownership of the public ID. Based on the concept of IBC, without any negotiating process, a CHF pairing key multiplied by one private key and other's public key will be used for mutually trusting and to be utilized as the session key of secure communicating between RSUs and vehicles. To help the vehicles to do message authenticating, the RSUs are assigned to response the vehicle's temple identity request using two short time secretes that are broadcasted by TA. To light the loading of request information, one day is divided into M time slots. At every time slot, TA will broadcast two short time secretes to all valid RSUs for that time slot. Any RSU can response the temple identity request from legal vehicles. With the collected announcement of public IDs from the neighbor vehicles, a vehicle can set up its neighboring set, which includes the information about the neighbor vehicle's temple public ID and temple CHF pairing key that can be derived by the private key and neighbor's public key and will be used to do message authenticating or secure communicating without the help of RSU.

Keywords : Internet of Vehicles (IOV), Vehicular Ad-hoc Networks (VANETs), Chameleon Hash Function (CHF), message authentication
Conference Title : ICICE 2017 : International Conference on Information and Communication Engineering
Conference Location : Kyoto, Japan
Conference Dates : April 27-28, 2017