Abstract

Vehicular Ad Hoc Networks (VANETs) are the most popular application of wireless communication technologies. There are two types of communications i.e. vehicle to vehicle (V to V) and vehicle to road side units (V to RSU). To communicate with other vehicle or to receive services from Trusted authorities (TA) group communication can be held. The group key will be changed during member join into the group or member leave from the group to provide forward secrecy and backward secrecy. To reduce no of rekeying operation this paper proposed cyclic group key administration and provides security member join into the group or member leave from the group to provide forward secrecy and backward secrecy.

References

2. J. Zhou and Y. H. Ou, "Key tree and Chinese remainder theorem based group key
distribution scheme”.


4. Melisa Hajyvahabzadeh“An efficient group key management using code for key calculations for simulations on join/leave CKCS”.

5. Y. Hao, Y. Cheng, C. Zhou, and W. Song, “A distributed key management framework with cooperative message authentication in VANETs”.


**Index Terms**

Computer Science Wireless

**Keywords**

Trusted authorities, Vehicular secret key, cyclic group theory, rekeying operations