Abstract

The VANETs carry several security considerations. One in every of the popular and dangerous attacks is launched within the variety of Sybil, connectivity holes or cut-up attack, wherever associated in Nursing assaulter inserts a faux position inside within the cluster. The inserted faux node data is used by the hackers within the case of inconsiderate driver, traffic jams, selective collisions and different similar dangerous things. To avoid such things the VANETs should be protected against such attacks. During this paper, a completely unique answer has been projected to beat the Sybil and cut-up attacks on the VANETs. The game theoretic approach has been designed to calculate per user resource requirement and the total load of the cell in order to calculate the utility, which denotes the resource consumption on the WSN cluster or cell. In this research, the load measurement is the primary concern in order to perform the load balancing using the game theoretic approach. The proposed model has removed the attack by the means of load balancing mechanism based upon the pushback algorithm. The proposed model shows the improved results than the existing models for the VANET data propagation.
References


31.

Index Terms

Computer Science
Networks
Keywords

VANET security, VANET secure mobility, connectivity hole avoidance, wormhole detection.