

EFFICIENT PRIVACY PRESERVING SCHEME FOR LOCATION BASED SERVICES IN VANET SYSTEM

ABSTRACT

A Vehicular Ad-hoc Network (VANET) is a type of Mobile Ad-hoc Network (MANET) that is used to provide communications between nearby vehicles, and between vehicles and fixed infrastructure on the roadside. VANET is not only used for road safety and driving comfort but also for infotainment. Communication messages in VANET can be used to locate and track vehicles. Tracking can be beneficial for vehicle navigation using Location Based Services (LBS). However, it can lead to threats on location privacy of vehicle users; since it can profile them and track their physical location. Therefore, to successfully deploy LBS, user's privacy is one of major challenges that must be addressed. In this project propose, a Privacy Preserving Fully Homomorphic Encryption over Advanced Encryption Standard (P2FHE-AES) scheme for LBS query. This scheme is required for location privacy protection to encourage drivers to use this service without any risk of being pursued. It is implemented using Network Simulator (NS-2), Simulation of Urban Mobility (SUMO), and Cloud simulation (CloudSim). Analysis and evaluation results demonstrate that P2FHE-AES scheme can preserve the privacy of the drivers' future routes in an efficient and secure way. The results prove the feasibility and efficiency of P2FHE-AES scheme in terms of query's response time, query accuracy, throughput and query overhead.