The fusion of mobile devices and social networks is stimulating a wider use of Location Based Service  
(LBS) and makes it become an important part in our daily life. However, the problem of privacy leakage  
has become a main factor that hinders the further development of LBS. When a LBS user sends queries  
to the LBS server, the user’s personal privacy in terms of identity and location may be leaked to the  
attacker. To protect user’s privacy, Niu et al. proposed an algorithm named enhanced-Dummy Location  
Selection (en-DLS). In this paper, we introduce two attacks to en-DLS, namely long-term statistical attack  
(LSA) and regional statistical attack (RSA). In the proposed attacks, an attacker can obtain the privacy  
contents of a user by analyzing LBS historical data, which causes en-DLS to be invalid for user’s privacy  
protection. Furthermore, this paper proposes a set of privacy protection schemes against both LSA and  
RSA. For LSA, we propose two protection methods named multiple user name (MNAME) and same user  
name (SNAME). To solve the regional privacy issue, we divide the map into various regions with different  
requirements on privacy protection. For this purpose, four levels of protection requirements (PLs) are  
defined, and true location is protected by allocating a certain number of positions from the dummies  
according to the location’s PL. Performance analysis and simulation results show that our proposed  
methods can completely avoid the vulnerabilities of en-DLS to both LSA and RSA, and incur marginal  
increase of communication overhead and computational cost.