LOCATION BASED SERVICES OF NEAREST PETROL STATION USING ASYMMETRIC KEY ALGORITHM

MUHAMMAD AWWAB BIN MOHD AMDAN

FACULTY OF ELECTRICAL ENGINEERING
UNIVERSITI TEKNOLOGI MARA
MALAYSIA

ACKNOWLEDGEMENT

First and foremost, I offer my sincerest gratitude to the almighty Allah for all the opportunities given to me in pursuing and finally accomplished my study. I would also like to express my sincere appreciation to my supervisor, Pn. Hanunah Bt. Othman, for her enlightening, guidance, supports, encouragement and unending patience throughout the entire period of my study as well as the write-up of this thesis. Her invaluable suggestions and discussions are truly rewarding.

I am also grateful to all the colleagues at the Faculty of Electrical Engineering, Universiti Teknologi Mara, Shah Alam, for their enjoyable discussions with me on communications concepts and interesting ideas.

Lastly, I greatly appreciate all the supports and helps from the lecturer in Universiti Teknologi Mara, Shah Alam, to completion of this thesis.

ABSTRACT

Location-based applications enabled by advances in sensing and tracking technology but it also create significant privacy risks. Anonymity can provide a high degree of privacy; reduce the service providers' requirements for safeguarding private information and save service users from dealing with service providers' privacy policies. Guaranteeing anonymous usage of location-based services however requires that the precise location information transmitted by a user cannot be easily used to identify the subject. In this paper, asymmetric key algorithm is used. Asymmetric key algorithm is also known as public-key cryptography, is a class of cryptographic algorithms with require two separate keys, one is secret (private) key and another one is public key. El-gamal encryption system is an asymmetric key encryption algorithm which is based on the Diffie-Hellman key exchange. The target petrol station location of longitude/latitude is determined firstly. The coordinate is incorporated with a random key for data encryption. Users only can detect the location by decrypting the El-Gamal encryption.

CONTENTS

CHAPTER I

INTRODUCTION

1.0 BACKGROUND

Location Based Services (LBS) is a network services that use the location coordinates of the end-user to improve the relevance, context, and value of the application. It is a general class of computer program-level services that use locations data to control features [1]. Moreover, LBS is an information service and has a number of uses in social networking today as an entertainment service, which is accessible with mobile devices through the mobile network and which uses information on the geographical position of the mobile device. It has become more and more important with the expansion of the smartphone and tablet markets as well. LBS are also services offered by cellular radio providers that are sensitive the physical location of the terminal device. Such services include descriptions of and directions to restaurants and other retail establishments in proximity. However, the services now may not only be offered by carriers alone.

1.1 CONTRIBUTION OF STUDY

From this study it can provide for more security in location based services. The location of a user is hardly to be detected or recognized by malicious third party or the wrong user that possibly make the user in danger or something bad happen. It provides high degree of security and confidentiality to the user.