



## A Survey on Location Based Data Encryption Algorithms for Mobile Devices

**Prof. H P Ambulgekar**

Department of CSE.,  
SGGIES &Tech, Nanded, India

**Manisha S Manindraker**

Department of CSE.,  
SGGIES &Tech, Nanded, India

**Pranjala G Kolapwar**

Department of CSE.,  
SGGIES &Tech, Nanded, India

*Abstract— Nowadays mobile communication has become an important part of our daily life. The knowledge of mobile user's location enhance the class of services and applications that can be used by the mobile user. In many environment, wireless technology is the default access technology for a variety of services like sending emails, mobile commerce, etc. In such applications, we need Secure Communication. Secure communication is possible through encryption of data. Most of the existing data encryption techniques are location-independent. Data encrypted with such techniques cannot restrict the location and time of data decryption. The concept of "Geoencryption" or "location-based encryption" is being developed for such a purpose. This paper presents a brief survey of location based services, the technologies deployed to track the mobile user's location, the accuracy and reliability associated with such measurements, and the network infrastructure elements deployed by the wireless network operators to enable these kinds of services.*

*Keywords— Geoencryption, Location Based Encryption, GeoLock, GeoProtocol, GeoTag, Data Encryption, Mobile Networks, Location BasedService, Random Generator, Geo Protocol.*

### I. INTRODUCTION

In recent years, mobile networks have received tremendous attention because of their self-configuration and self-maintenance capabilities. The penetration of mobile wireless technologies has resulted in larger usage of wireless data services in the recent past. For secure communication, different data encryption algorithms are used. But traditional data encryption algorithms are location independent. Data encrypted with such techniques can be decrypted anywhere. They cannot restrict the location of mobile clients for data decryption. So, for secure communication the concept of "geoencryption" is introduced which is location dependent. It is an enhancement to traditional encryption that makes use of physical location or time as a mean to produce additional security and security features. It allows data to be encrypted for a specific place or broad geographic area, and supports constraints in time as well as space. It provides full protection against attempts to bypass the location feature. Depending on the implementation, it can also provide strong protection against location spoofing. The geoencryption algorithm does not replace any of the conventional cryptographic algorithms, but instead adds an additional layer of security. The capability has tremendous potential benefits to applications such as location based services, managing secure data and digital movie distribution where controlling access is the main concern [2]. Location information has many properties good for encryption and authentication.

Logan Scott, Dorothy Denning [1] developed the idea of geoencryption and its use in digital film distribution. In order to meet the demand of mobile users, Hsien-Chou Liao and Yun-Hsiang Chao introduced a location dependent approach called Location Dependent data Encryption Algorithm (LDEA) [2]. This protocol is not strong enough because they are using the static location which is latitude/longitude coordinates of mobile node and they are using the static tolerance distance to overcome the inaccuracy and inconsistent of GPS receiver. Hatem Hamad and Souhir Elkourd [3] proposed a protocol which makes the use of dynamic location of mobile node and dynamic tolerance distance which makes it very strong to attack. However most of them are not strong enough against tampering. If the device is vulnerable to tampering, it may be possible to an advisory to modify it and bypass the location check[5]. To protect against tampering and spoofing, a signal authentication protocol, Timed Efficient Stream Loss-tolerant Authentication (TESLA) is designed [4]. Since then many efforts have been done to complete the above idea and fix its defects [5,6,7]. To Overcome these defects, Rohollahkarimi and Mohammad Kalantari[9] present a modified Geo protocol and improve its efficiency and applicability. Although it is possible to provide security features such as authentication, integrity and confidentiality. So security measures need to be upgraded continuously. What is secure today may not be secure tomorrow. There will always be malicious users trying to exploit and find new holes in a network. Therefore, we need to look into the future so that we are able to face these security issues before they cause damage. This paper revives contemporary location based algorithms and protocols of mobile users.

The paper is organized as follows: Section 2 introduces the basic geoencryption model. Section 3 gives the brief study of existing algorithms. Section 4 explain the possible attacks on existing geosystem. Section 5 explains the comparative study of existing algorithms. Finally we conclude in Section 6.

## II. BASIC GEOENCRYPTION MODEL

The term “location based encryption” of “geoencryption” is used to refer any method of encryption wherein the cipher text can only be decrypted at a specified location. If an attempt to decrypt data at another location, the decryption process fails and reveals no information about the plaintext. Making key depended on target geographic position is an applicable way to strengthen its safety in real time applications.

Fig 1 depicts the basic geoencryption model [1].

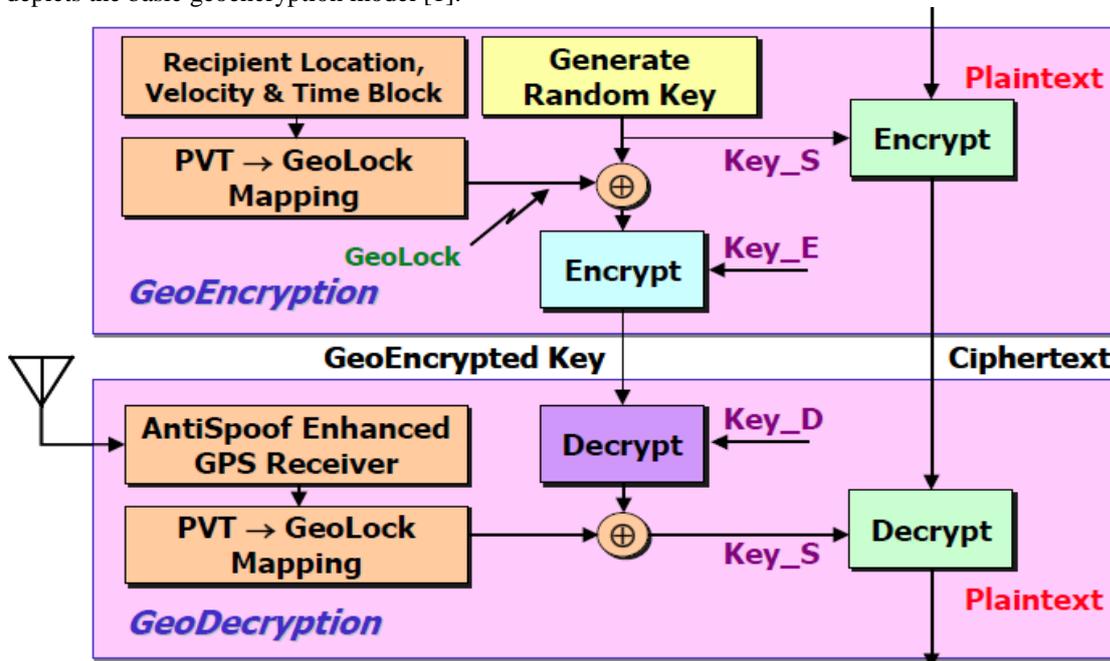


Fig.1 Basic Model Geoencryption-decryption Process

Geo-encryption was based on the traditional encryption system and communication protocol. For the sender, the data was encrypted according to the expected PVT (position, velocity and time) of the receiver. A PVT-to-GeoLock mapping function was used to get the GeoLock key. GeoLock key was performed bitwise exclusive-OR with a generated random key to get a GeoLock session key. This GeoLock session key was then transmitted to the receiver by using asymmetric encryption. For the receiver, an anti-proof GPS receiver was used to acquire the PVT data. Then the same PVT-to-GeoLock mapping function was used to get the GeoLock key. The key was performing exclusive –OR operation with received GeoLock session key to get the final session. The final session was used to decrypt the ciphertext.

## III. RELATED STUDY

Logan Scott, Dorothy Denning [1] developed the idea of geoencryption in which PVT-to-Geolock mapping function is used as a primary mechanism to ensure that the data can be decrypted successfully. It is troublesome for sender and receiver to own the same mapping function before the data transmission if they communicate occasionally.

The solution to this problem was proposed by Hsien-Chou Liao and Yun-Hsiang Chao[2]. They design the LDEA by skipping the mapping function. The purpose of LDEA is mainly to include latitude/longitude coordinate in the data encryption to restrict the location of data decryption. A toleration distance (TD) is designed to overcome the inaccuracy and inconsistent problem of GPS receiver. Fig. 2 depicts the LDEA process [2].

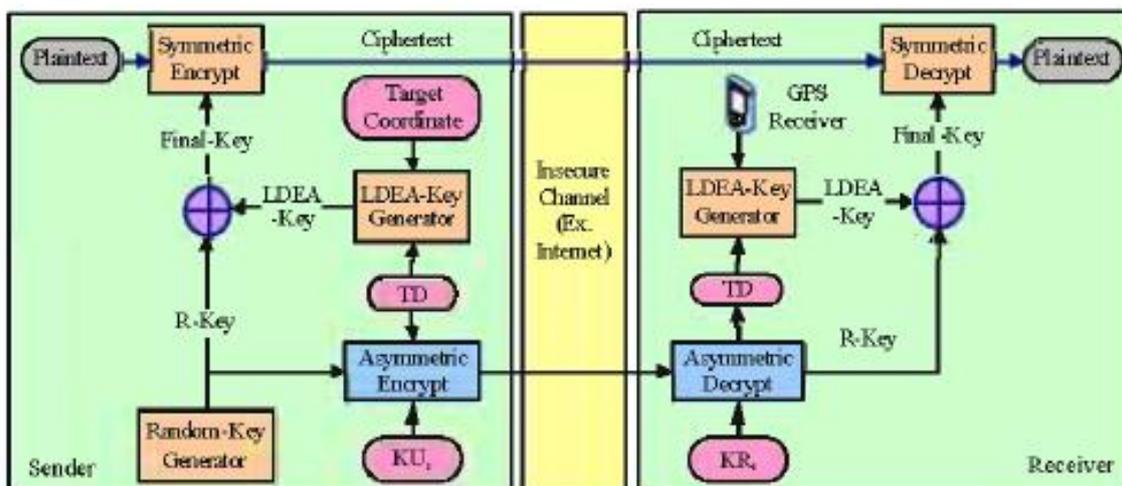


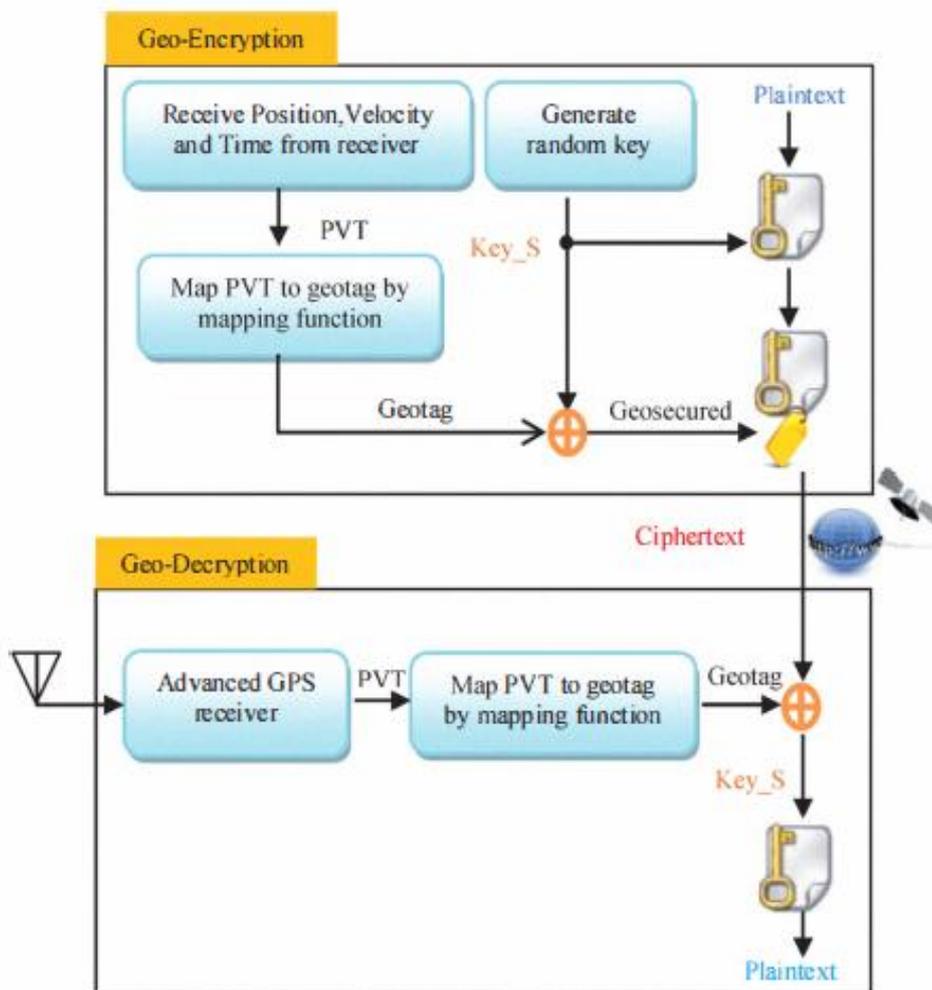
Fig 2 The LDEA process

Prasad Reddy, P.V.G.D, K. R. Sudha, P Sanyasi [4] proposed a location dependent approach for mobile information system by using LDEA process. In this paper, the mobile clients transmits a target latitude/longitude coordinate and an LDEA key is obtained for data encryption to information server. The client can only decrypt the ciphertext when the coordinate acquired from GPS receiver matches with the target coordinate. They makes the use of random key (R-key) an addition to the LDEA key to improve security.

LDEA protocol makes the use of static location. It is difficult for a receiver to decrypt the cipher text at the same location which is exactly matched with the target coordinate. It is impractical by using the inaccurate GPS coordinate as a key for data encryption. So, Hatem Hamad and SouhirElkourid [3] proposed a protocol which makes the use of dynamic location of mobile node and dynamic tolerance distance which makes it very strong to attack. In this protocol, the mobile receiver with GPS service, register a set of coordinates and velocity during movement and estimate the next position. This new coordinate is applied in the secret key with dynamic tolerance distance (DTD). DTD is designed to overcome the inaccuracy and inconsistent problem of GPS receiver and to increase its practicality. These parameters and the type of movement makes this protocol more secure than the static encryption which depends only on a position of mobile nodes and static TD.

However most of them are not strong enough to tampering. By tampering, deals with both physical attacks on the hardware and attacks on the implementation such as spoofing. If the device is vulnerable to tampering, it may be possible to for an adversary to modify it and bypass the location check [1]. if there is an unauthorized tamper access, or attacker sent a faked message, the system assumes a tampering is being attempted and ignores the message and process will be failed. Thus the messages really sent from the sender will distinct from the fake messages and then only these messages will be decode. To protect against tampering and spoofing, a signal authentication protocol, Timed Efficient Stream Loss-tolerant Authentication (TESLA) is proposed [5,6]. Di Qiu, Sherman Lo, Per Enge, Dan Boneh and Ben Peterson propose a mean on implementing TESLA on Loran for authentication [7]. Authentication is important concept in cryptography. It allows the receiver of a message to ascertain its origin. Authentication is not necessarily used in encryption or decryption protocols but it is a key concept in verifying the source of a message.

TESLA is implemented to provide the source authentication of the RF navigation signal. TESLA uses symmetric authentication mechanism to achieve asymmetry property required for a secure broadcast authentication. Instead of using this costly protocol, in addition to encrypt each messages by location based encryption, Rohollah karimi and Mohammad kalantari [9] proposed a new GeoProtocol which makes the use of MAC at the end of them. Fig 3 shows the proposed geoencryption model.



**Fig. 3 Model of geoencryption**

Attackers cannot simulate signals or use any mean to spoof the GPS receiver because they don't have the key used to generate authenticated messages. Therefore, if there is an unauthorized tamper access, or attacker sent a faked message, the system assumes a tampering is being attempted and ignores the message and process will be failed. Thus the messages really sent from the sender will distinct from the fake messages and then only these messages will be decode. V Rajeswari, V Murali and A.V.S. Anil [10] describes the application of this Geo Protocol in the military application.

Xinxin Zhao, Lingjun Li and Guoliang Xue [17] explains the use of geocryption in Location Based Social Networks (LBSNs) for location privacy. In this paper, they designed a framework to safeguard users location information as well as the check in record by considering demands in LBSNs. LBSN is is location based social network system in which users expose their location when they check in at a venue or search a place.

Aasif Hasan and Niraj Sharma added a new level of security in location based services. There are so many encryption methods which converts the information before sending on communication link. Each of these encryption methods has their own merits and demerits. A smooth comparison of various encryption algorithms and their techniques for secured data communication in multinode network is explained by Ajay Kakkar, M. L. Singh and P. K. Bansal [19]. We could not control the leakage/stealing of of information hundred percent by using these encryption algorithm. That's why a new concept is added called Name-Based-Encryption which provides great security level with lesser time complexity [18]. This technique is the combination of stream ciphering and symmetric ciphering. This proposed encryption algorithm work's by user defined dynamic key and ASCII value of the secrete key. Dynamic key is a concept in which key is decided at encryption of any message.

#### IV. POSSIBLE ATTACKS ON GEO SYSTEM

Security analysis is discussed for the confidentiality, authentication, simplicity and practicability.

1) *Confidentiality*

Only the information server and those registered clients own the shared random seed and MAC function C. The server and client must use the same session key for decrypting message successfully.

2) *Authentication*

The client must know the correct session key and MAC function in order to submit a request to server.

3) *Simplicity*

Only simple symmetric encryption algorithm and exclusive-OR operation is used.

4) *Practicability*

The approach is practical and need to satisfy the requirements of mobile information system,.

The purpose of Geo-encryption is to provide security to the transmission of information. As such, it is important that every link of the Geo-encryption chain is secure. This includes protocol and broadcast of RF signals. Adding security in a broadcast communication system is complicated by untrusted or uncertified users and unreliable communication environments. The security analysis of a protocol is complicated as there are no standard metrics to precisely quantify the subject of security. In this section, we take a short review on security weaknesses of geocryption protocol and all possible attacks that might threaten the system. In general these attacks can be divided into three categories. Fig 5 shows how these attacks can be occurred.

- **Spoof/Forgery Attack:** An attacker simulates RF signal to spoof the receiver.
- **Replay Attack:** An attacker replays modified location information to spoof the receiver.
- **"Parking Lot" Attack:** An attacker replies on a probabilistic mapping from a user's location.

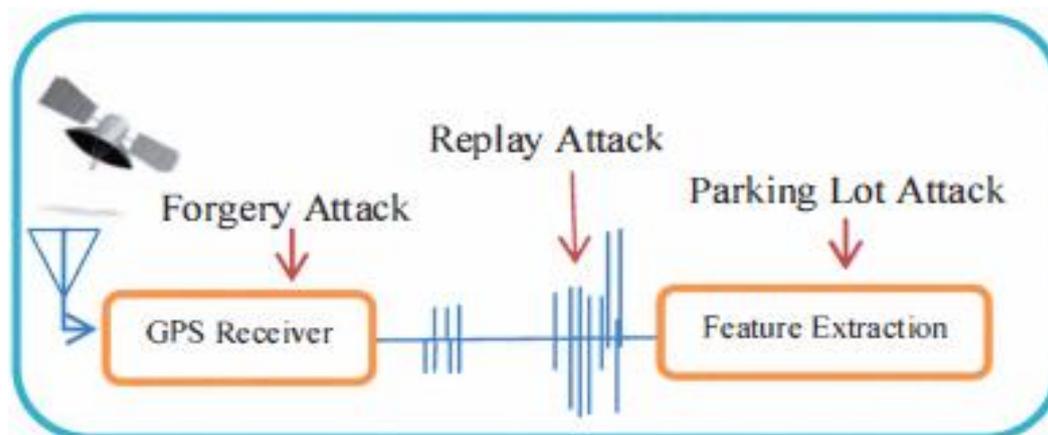


Fig 4 Attacks on Geo system

In geocryption, the power of key depends on the current receiver's location. Therefore, the probability to break the secret key is impossible because no one knows the estimate coordinate.

## V. COMPARATIVE STUDY

In this section, we presents the comparative study in tabular format.

Sr.No	Year	Title	Concept	Remark
1	2003	A location based encryption techniques and some of its applications	PVT-to Geolock mapping function is used	Its difficult for sender and receiver to own same mapping function
2	2008	A new data encryption algorithm based on the location of mobile users	Location Dependent Encryption Algorithm (LDEA) is used by skipping mapping function which makes the of Latitude / Longitude co-ordinates along with Toleration distance (TD)	LDEA protocol makes the use of static location which is difficult for a receiver to decrypt the ciphertrext at the same location and session key is used with less security
3	2010	A modified location dependent image encryption for mobile information system	A new R-key is used an addition to the LDEA key to improve security	Vulnerable to most of the attacks like tampering, spoofing
4	2010	Data encryption using the dynamic location and speed of mobile node	Instead of using static location, they makes the use of dynamic location with dynamic toleration distance	Vulnerable to attacks also
5	2011	Enhancing security and confidentiality in location based data encryption algorithm	Proposed new Geo Protocol which makes the use of MAC at the end of the message which plays graet role in enhancing security	This Geo Protocol is replacement to costly TESLA protocol which increases the security.
6	2013	Checking in without Worries: Location Privacy in Location Based Social Networks	A framework is designed to safeguard users location information as well as check in records considering the special demands in Location Based Social Networks (LBSN) .	This framework reduces the computational overhead of users and the server and improve security against several attacks.
7	2014	A New Method Towards Encryption Schemes (Name-Based-Encryption Algorithm)	It is the combination of stream ciphering and symmetric ciphering technique.	It takes care about increasing security level without increasing complexity of the cryptography algorithm

## VI. CONCLUSION

In this survey paper, we have seen the different location based data encryption algorithms/techniques and authentication protocols. All the algorithms have some merits and demerits and hence new techniques have been evolved. This paper explains the importance of location based system and corresponding security.

## REFERENCES

- [1] Logan Scott, Dorothy Denning, "A Location Based Encryption Techniques and some its Application", ION NTM, pp. 734-740, 2003.
- [2] Hsien-Chou Liao and Yun-Hsiang Chao, "A New Data Encryption Algorithm Based on the Location of Mobile Users", Information Technology Journal 7 (1), pp. 63-69, 2008.
- [3] Hatem Hamad and SouhirElkour, "Data encryption using the dynamic location and speed of mobile node", Journal Media and communication studies, pp. 67-75, 2010.
- [4] Prasad Reddy. P.V.G.D, K. R. Sudha, P Sanyasi, "A Modified Location-Dependent Image Encryption for Mobile Information System", IJEST, pp. 1060-1065, 2010.
- [5] J. Di Qiu, Sherman Lo, Per Enge, Dan Boneh and Ben Peterson, "Geoencryption using Loran".
- [6] A. Perrig, R. Canetti, J.D. Tygar, D. Song, "The TESLA Broadcast Authentication Protocol", 2002, pp. 2-13
- [7] J. Di Qiu, Sherman Lo, Per Enge, Dan Boneh and Ben Peterson, " Geoencryption system security-Loran as a case study".
- [8] Ayesha Khan, "Geolocation Based RSA encryption Techniques", ISSN, 2013, pp. 17-20.
- [9] Rohollah karimi and Mohammad kalantari, "Enhancing security and confidentiality in location based data encryption algritms", IEEE Conference, pp. 30-35, 2011.
- [10] V Rajeswari, V Murali and A.V.S. Anil, "A naval approach to identify Geo-Encryption with GPS and Diffrent Parameteers (Location and Time)", IJCSIT, pp. 4917-4919, 2012.
- [11] Yan Zhu, Di Ma, Dijiang Huang, Changjun, "Enabling Secure Location- Based Seviles in Mobile Cloud Computing", ACM, pp. 27-32, 2013.

- [12] Rohollah karimi and Mohammad kalantari, "Enhancing security and confidentiality on mobile devices by location-based data encryption", IEEE international Conference, pp. 241-245, 2011.
- [13] Guojun Wang, Tao Peng,, QinLiu,, "Privacy Preserving for Location-Based Services Using Location Transformation", Springer International Publisher, pp. 14-28.
- [14] Ganasan S P "An asymmetric authentication protocol for mobile devices using elliptic curve cryptography :, IEEE Conference, pp. 107-109, 2010.
- [15] S U Nimbhorkar, Smruti P patil, "A Survey on Location Based Authentication Protocols for Mobile Devices", IJCSN, pp. 44-48, 2013.
- [16] Ku, We Shinn, "Geo-Store: A Framework for Supporting Semantics-Enabled Location-Based Services", IEEE Conference, pp. 35-43, 2013.
- [17] Xinxin Zhao, Lingjun Li, Guoliang Xue, "Checking in without Worries: Location Privacy in Location Based Social Networks", IEEE Conference, pp. 3003-3011, 2013. Asif Hasan and Neeraj Sharma, "A new Method Towards Encryption Schemes (Name-Based-Encryption Algorithm)", IEEE international Conference, pp. 310-313, 2014.