ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 2, February 2018

Geo-Encryption A Revolutionary Information Security Mechanism

Omkar Tiware[1], Prajkta Khaire[2]

B. E. Student, Dept.of IT, SSJCOE, Affiliated to Mumbai University, India[1]

Asst. Professor, Dept.of IT, SSJCOE, Affiliated to Mumbai University, India[2]

ABSTRACT: There are several security mechanisms available today. Most of the communication systems, websites use SSL/TLS services. So, the communication channel is protected. Although unauthorized users may access any confidential data from distance. Neither do they need to be present at the receiving end nor do they attack the communicationchannel.Our aim is to restrict the unauthorized access to confidential data based on the coordinate system. To properly decrypt the information, a receiver must be present at a particular coordinate. If an unauthorized person tries to decrypt the confidential data, he/she will fail. In this paper we are going to explore the strength of Geo-Encryption Mechanism and also will be exploring various applications & future scope of this technology.

KEYWORDS: Geo-Encryption, GPS, data security, information storage, cryptography.

I. INTRODUCTION

Data security is an important task in our life. GPS device is the best application for data security. Most of the computer users, mostly use data in electronic format. An important question arises here is how to provide a security for data. In this paper, we propose a Location Based DataSecurity System to secure data by applying Encryption-Algorithm and co-ordinate by using GPS device. Encryption means of efficient secure integer comparison. Using the encryption technology the location of data decryption cannot be restricted.

In order to meet the demand of a location-dependent approach, location-dependent data encryption algorithm is needed. A target latitude/longitude coordinate is determined first and the coordinate is incorporated with a random key for data encryption. The receiver can only decrypt the ciphertext when the coordinate acquired from GPS receiver is matched with the target co-ordinate. GPS-based encryption is an innovative technique that uses GPS-technology to encode location information into the encryption keys to provide location-based security. GPS based encryption adds another layer of security on top of existing encryption methods by restricting the decryption of a message to a particular location. Our experimental results not only validate the effectiveness of our scheme but also demonstrate that the proposed integer comparison scheme performs better than previous bitwise comparison scheme.

II. RELATED WORK

The Nowadays mobile communication has become an important part of our daily life. In many environments, wireless technology is the default access technology for a variety of services. Besides using cell phones for voice communication, we are now able to access the internet, conduct monetary transactions, send email, etc. by using our cell phones and new services continue to be added. However, all of them need security for their communication. Secure communication is possible through encryption of data.

Traditional encryption is used to provide assurance that only authorized users can use the secure content. However, it would still be useful to have an additional layer of security that provides assurance that the secure content can only be used at authorized location and time. The concept of location-based encryption or geo-encryption is being developed

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 2, February 2018

for such a purpose. The capability has tremendous potential benefits to applications such as location-based services, managing 978-1-4244-9825-3/11/$26.00 ©2011 IEEE 30 Mohammad Kalantari Department of Computer Islamic Azad University Qazvin Branch, Iran mkalantari@qiau.ac.ir classified/secure data and digital movie distribution where controlling access is the main concern

Logan Scott, Dorothy Denning, and their colleagues (2003) at Geo-codex developed the idea of geo-encryption and its use in digital film distribution. Since then many efforts have been done to complete the above idea and fix its defects. However, most of them are not strong enough because they are not resistant to unauthorized access and tampering. In addition, due to high computational complexity impose the large overhead on the system. By tampering, we mean 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 for an adversary to modify location information and bypass the location check.

In this paper, we try to present a modified Geo protocol and improve its efficiency and applicability. In addition, in order to increase safety and reliability of this protocol, we are going to discuss common types of errors in measurement location based parameters and propose some strategies for reducing it. Furthermore, we consider all types of possible attacks to the Geo protocol and propose some solutions to deal with them. In addition, to protecting against spoofing, we present a simple and efficient method for confirming the received signals.

III. THE PROPOSED SYSTEM

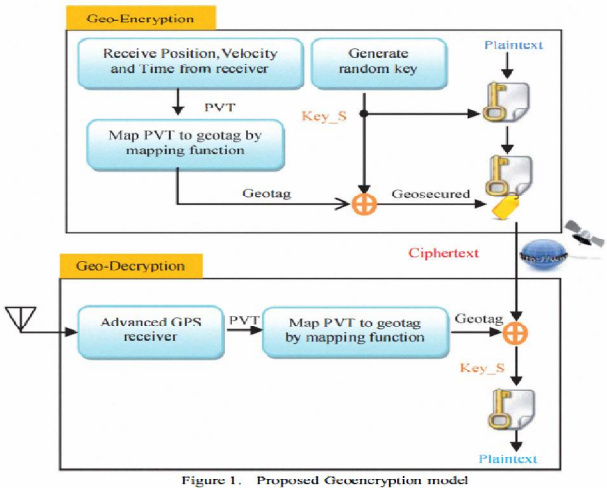


Figure 1. Proposed Geoencryption model

Fig. 1: Proposed Geo-Encryption & Decryption Model

Fig. 1 shows our proposed model simply. A mapping function is employed during encryption process to combine the recipient's geographic location, time and an encryption key to produce a geo-secured key for transmission with a message. The message can only be decrypted if the recipient is physically positioned at the considered location.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 2, February 2018

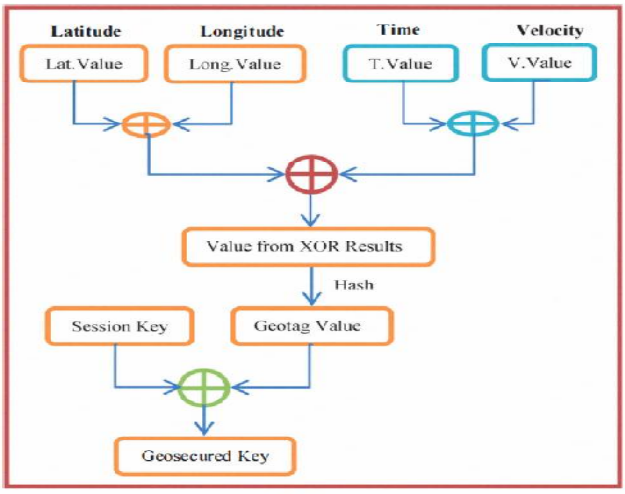


Figure 2. The keys generation process

Fig. 2 Key generation process

Fig. 2 shows the structure of mapping function and keys generation process. In our model geotag value is used to generate a secure key from session key and recover session 31 key from the secure key. Our model takes advantage of GPS technology and it's suitable for a mobile device, which has low computation capability and short battery life.

1. Encryption Process

The sender encrypts the plaintext using a conventional cipher and a key. The receiver delivers his location-based information to the sender. The sender generates a Geo-tag and tags it to the ciphertext. The sender broadcasts the ciphertext and the Geo-tag.

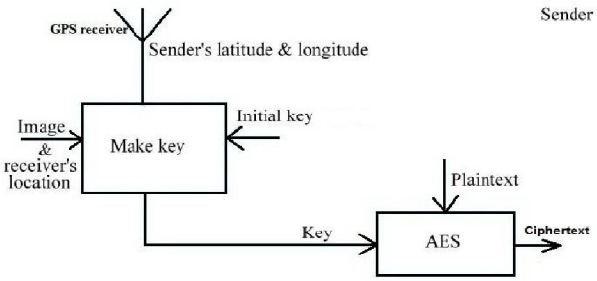


Fig. 3: Encryption Process

2. Decryption Process

The receiver requires a communication channel to receive the ciphertext and Geo-tag. The receiver uses a Radio Frequency (RF) antenna and receiver to capture and signals. The receiver applies a feature extraction algorithm and key generation algorithm to compute a Geo-tag based on the collected RF signals. If the location check is bypassed, the receiver is authorized for the decryption. Figure 1 gives the general concept of Geo-encryption.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 2, February 2018

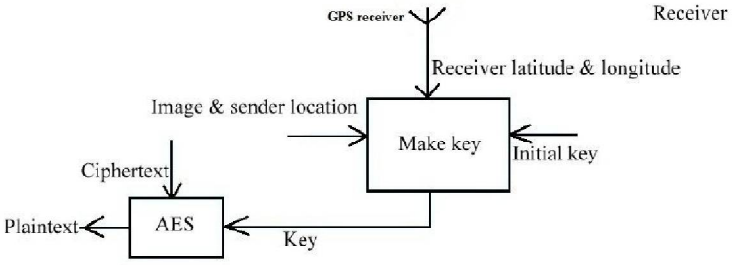


Fig. 4 Decryption Process

To communicate with the world, people use Internet service. Communication process must be protected by some mechanism and Cryptography helps us to protect our information. Both Sender as well as Receiver uses a single key in the symmetric-key based system and uses a pair of keys in the asymmetric key based system. In the real world, symmetric and asymmetric key protocols may not be sufficient to secure our information. An attacker may try to snoop into the communication from either side of the sender/receiver's position. Generally, an attacker is not physically present at the receiver's end. Since GPS information is accessible easily, this GPS information can act as an individual parameter of cryptographic algorithms.

In other words, we can say that geo-location restricts the decryption process which must be done on a particular location. RSA algorithm is used with geo-location information. V. Rajeswari, V. Murali, and A.V.S. Anil proposed geo-location and time as the extra parameters to extend the strength of cryptographic method.

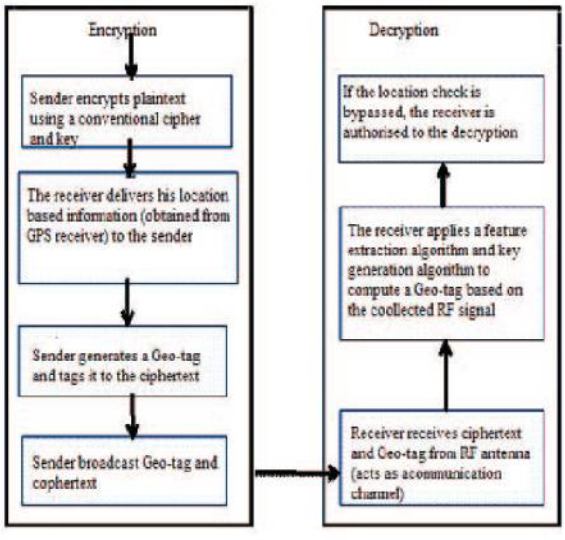


Fig. 1 Basic Geo-encryption Working

Fig. 5: Geo-Encryption Working Model

The encryption process takes receiver's geo-location, an image, and a key. It also fetches the sender's geolocation from the GPS device and hence encrypts the message (as shown in figure 1). Decryption process requires a receiver to be present at the particular location which was earlier used by the sender (as shown in figure 2). Decryption process also requires sender's geo-location, key, and the image (which acts as an extra parameter). Decryption process fails to decrypt successfully if any of the parameters along with the geo-location is mismatched.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 2, February 2018

IV. COORDINATE SYSTEM

Latitude line is parallel to the equator and longitude line is perpendicular to the equator. Every place on earth can be defined by the intersecting point of these two. Lines representing latitude are parallel to each other from 0o (Equator) to 90 degrees north and south.Also, lines representing longitude are perpendicular to each other from 0o (Prime meridian) to 180o east and west. Hundreds digit in a coordinate represents longitude; tens digit represents a location upto 1000 kilometers and units digit represents a location to 111kilometers.

V. DISTANCE

The haversine formula is used to measure the distance between two coordinates over earth's surface. It calculates the shortest distance between two points on earth. The formula is:

$$a = sin^2(\Delta\emptyset + 2) + cos\emptyset_1 . cos\emptyset_2 . sin^2(\Delta\lambda + 2)$$
$$c = 2. atan2(\sqrt{a}, \sqrt{(1-a)})$$
$$distance = r. c$$

VI. SYSTEM SECURITY

The security analysis of a protocol is complicated as there are no standard metrics to preciselyquantify the subject of security. In this section, we first take a short review on security weaknesses of geo-encryption protocol and all possible attacks that might threaten the system. Furthermore, we investigate common errors in measurement location based parameters. Finally, we present approaches to deal with them.
All possible attacks on Geo system Adding security in a broadcast communication system are complicated by untrusted or uncertified users and unreliable communication environments. We are going to investigate all possible attacks that might threaten or weaken the system. In general, these attacks can be divided into three categories:

- 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.

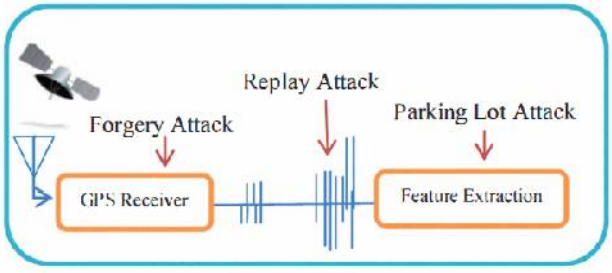


Fig. 6: System Security

Instead of using this costly protocol, in addition, to encrypting each message by location-based encryption, we can use the MAC at the end of them. 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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 2, February 2018

VII. CONCLUSION

Traditional encryption technology cannot restrict the location of mobile clients for data decryption. In order to meet the demand of mobile information system in the future, a modified location-dependent data encryption algorithm is proposed in this paper. The approach provides a novel function by using the latitude/longitude coordinate as the key of data encryption. According to our discussion, the approach can meet the confidentiality, authentication, simplicity, and practicability of security issues. As a result, the approach is effective and practical for the data transmission between information system and mobile clients.

The results also show that the region of decryption is less because the range of DTD is small where the success rate is probably narrow. In this study, we also review the security weaknesses of existent geo-encryption protocol, common false measurements in location-based parameters and then try to propose some approaches to reduce them.

REFERENCES

[1] L. Scott, D. Denning, "Location-Based Encryption & Its Role in DigitalCinema Distribution", Proceedings of ION GPS/GNSS 2003, pp288-297. 35

[2] L. Scott, D. Denning, "A Location-Based Encryption Technique and Some of Its Applications", Proceedings of ION NTM 2003.

[3] AI.Omar, AI.Ala, D.Dyk, N.Akerman, "Mobility Support for Geo-Encryption", IEEE ICC International Conference, 2007.

[4] H.Liao, P.Lee, Y.Chao, C.Chen, "A Location-Dependent Data Encryption Approach for Enhancing Mobile Information System Security", In The 9th International Conference on Advanced Communicate Technology, pp. 625-626, Feb. 2007.

[5] L.Hsien-Chou, C.Yun-Hsiang, "A New Data Encryption Algorithm Based on the Location of Mobile Users", Info. Tech. J., 2008.

[6] A.Krevl, M.Ciglaric, "A Framework for Developing Distributed Location-Based Applications", IEEE International Conference, 2006.

[7] G.Yan, "Providing Location Security in Vehicular ad hoc Networks", Ph.D. Thesis, Old Dominion University, May 2010.

[8] D. Qiu, "Geoencryption Using Loran", Proceeding of ION NTM 2007.

[9] P.Reddy, K.R.Sudha, S.Krishna Rao, "Data Encryption technique using Location-based key dependent Permutation and circular rotation", International Journal of Computer and Network Security, March 2010.

[10] L.Ismail, "Authentication Mechanisms for Mobile Agents", IEEE International Conference on Availability, Reliability, and Security, 2007.

[11] H.Hamad, S.Elkourd, "Data encryption using the dynamic location and speed of mobile node", Journal Media and Communication Studies Vol. 2, pp.67-75, March 2010.

[12] G.Junzhong, H.Liang, Y.Jing, L.Zhao, "Location-Aware Mobile Cooperation-Design and System", International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 2, Issue No. 4, December 2009.

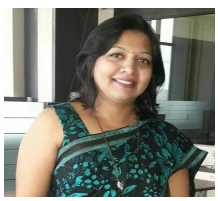
[13] P Sanyasi Naidu, P.Reddy, K.R.Sudha, "A Modified LocationDependent Data Encryption for Mobile information System with Interlacing, key-dependent Permutation and rotation", International Journal of Computer and Network Security, Vo1.2, No.5, May 2010.

[14] G.Yan, S.Olariu, "A probabilistic analysis of link stability in vehicular ad hoc networks", IEEE Transactions on Intelligent Transportation Systems, 2010.

[15] R.Karimi, "Providing safe location-based services in mobile networks by Location-based Data Encryption Algorithm", In Annual International Conference on mobile communications, networks, and applications, 2011

BIOGRAPHY

Omkar R. Tiware is pursuing his B.E. in Information Technology from SSJCOE, University of Mumbai, India. His interested areas include Data Analytics, Business Intelligence, Data Mining and Hadoop. He also loves Digital Marketing and has lead various projects in IT Innovation.



Prof. Prajkta Khaire is an Assistant Professor at SSJCOE, Dombivli Affiliated to the University of Mumbai. She has pursued her masters in the field of Information Technology from VESIT, Chembur Affiliated to theUniversity of Mumbai and has13 years of teaching experience in the field of IT and Computer Science.