International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Use of Advanced Encryption Standard to Enhance the Performance of Geo Protocol in Location Based Network

Pranjala G Kolapwar[1], Prof. H. P. Ambulgekar[2]

[1]Department of Computer Science and Engineering, SGGSIE&T, Nanded, India

Abstract: ***Wireless technology is the default access technology in many services like mobile commerce, sending emails, banking application, military applications, etc. In such applications, we need Secure Communication and it is possible only when we secure data. Data encryption algorithms are used to secure such 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. And hence the concept of "Geo-encryption" or "Location Based Data Encryption" is evolved. Much research has been done on location based data encryption algorithms and techniques. In this paper, we are going to investigate the weaknesses of Geo-encryption algorithms and try to improve them so as to enhance the performance of the Geo - protocol. For this purpose, we make the use of Advanced Encryption Standard–Geo-encryption with Dynamic Tolerance Distance (AES-GEDTD) instead of Data Encryption Standard-GEDTD (DES-GEDTD). We also demonstrate the performance of the proposed approach over the existing one.***

Keywords: Geo-encryption, Geo-protocol, AES-GEDTD, DES-GEDTD, Geo-tag, Geo-secured key, Geo-mapping function

1. Introduction

In recent years, mobile networks are widely used in many areas which required secure system. So, it is important issue to protect the confidential information or data from unauthorized access. In order to secure this communication, different data encryption algorithms are used. Usually, these algorithms are location independent. Data encrypted with such techniques can be decrypted anywhere. They cannot restrict the location of mobile clients for data decryption and hence vulnerable to many attacks. In order to avoid this vulnerability, the concept of "Geo-encryption" is introduced which introduces location and time dependency in the process of encryption and decryption. It is an enhancement to traditional encryption-decryption that makes use of physical location or time as a mean to produce an additional security level. It provides full protection against attack. Depending on the implementation, it can also provide strong protection against location spoofing [8]. Logan Scott, Dorothy Denning [1], developed the idea of Geo-encryption and its use in digital film distribution. In order to meet the demands of mobile users, Hsien-Chou Liao and Yun-Hsiang Chao [2], introduced a Location Dependent data Encryption Algorithm (LDEA).

Security measures need to be upgraded continuously. What is secure today may not be secure tomorrow. There will 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. In this paper, we try to improve the existing Geo-protocol, DES-GEDTD and improve its performance by using AES-GEDTD.

The paper is organized as follows: Section 2 introduces the basic concept of Geo-encryption. Section 3 explains the possible attacks on the existing well system. Section 4 explains the DES algorithm by using GEDTD protocol. Section 5 gives the modified approach. Section 6 gives the modification to the existing protocol. And finally we conclude in Section 7.

2. Basics of Geo-encryption

2.1 Basics of Cryptography

Cryptography is basically the process of hiding information. Moreover, it is the science of using mathematics to encrypt and decrypt data. It enables to store sensitive information and transmit it across networks so that it can be read by authorized recipients.

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. The reversal of the encryption process is referred to as decryption. An encryption process has a corresponding decryption process, which is used to reverse the encrypted data, ciphertext back to its original content, plaintext.

2.2 Geo-encryption Process

The term "Geo-encryption" is location based data encryption, where 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. In this method, the key depends on target geographic location which powers it to use in real time applications. Figure 1 depicts the general model of Geo-encryption [1].

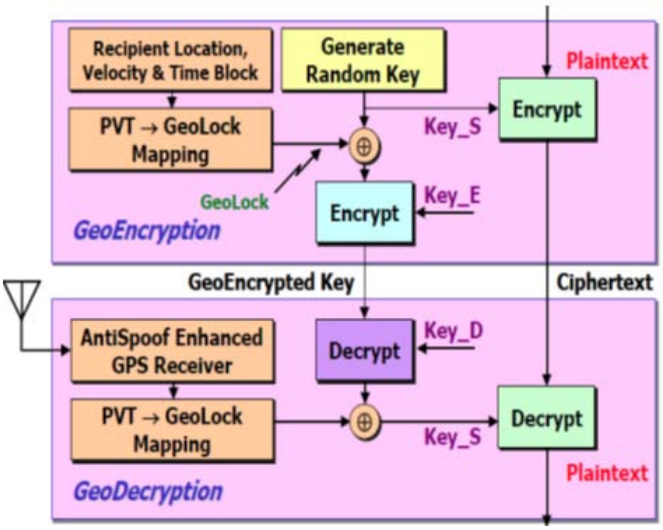

Figure 1: Basic Geo-encryption Model

DES-GEDTD protocol is mainly designed to strengthen and increase the security level of Geo-encryption and Geo-decryption process [8]. The receiver determines the DTD coordinates and the sender can decrypt the ciphertext within the range of the DTD. So, depending upon the rage of the DTD, the success rate of this protocol varies.

3. Possible Attacks on Geo-system

The Geo - encryption process is mainly used to provide security to the communication system for transmission of information. So, it is important that every link of the Geo-encryption chain is secure. This includes protocol and broadcast of RF signals. Due to un-trusted or un-certified users and unreliable or unsecure communication, it's very difficult to secure this communication environment. In this section, we take the brief study of all possible attacks that might affect the system knowingly or unknowingly. In general, these attacks can be divided into three categories [8].

- *Spoof Attack*- Spoofing is a very common type of attack in which an attacker tries to gain access to restricted resources or data and steals information. This type of attack can affect the communication system in various ways. An attacker simulates the RF signal to spoof the receiver. It is also known as forgery attack.
- *Replay Attack*- Replay attacks are the network attacks. In this, an attacker acts like a secret agent, observes the conversation between the sender and receiver and steals the authenticated information like sharing key. By using this key, the attacker tries to communicate to the receiver and the receiver treats this as an authentic communication. Hence, it is also called as *playback attack.*
- *"Parking Lot" Attack*- In "Parking Lot" attack, an attacker can eavesdrop on the communication line by setting up an adapter in the communication range of the wireless communication and replies on a probabilistic mapping from user's location.

4. DES-GEDTD Protocol

4.1 DES-GEDTD Protocol

In this protocol, the mobile receiver with GPS service, register a set of coordinates during movement and estimate the next position. These new coordinates are used to design the secret key by adding DTD. DTD is nothing but a fractional number with a small interval. DTD is basically designed to overcome the inaccuracy and inconsistent problem of GPS receiver and to increase its practicality which acts as an additional security level to this protocol. These parameters make this protocol more secure than any other geo-protocols. To design this protocol for encryption, a Geo-mapping function is used. It is nothing but simply a combination of the recipient's geographic location, time and an encryption key. This is used to produce Geo-secured key.

The strength of geo-secured key is current receiver's location and a DTD. So, it's impossible to break this key as no one knows the estimated coordinates. The current design of this protocol is based on the DES algorithm [4].

4.2 Comparison of DES and AES

AES is one of the best contemporary algorithms. Following table gives the comparison of AES and DES [13].

Parameter	*DES*	*AES*
Key Length	Very short, 56 Bits	128, 192 or 256 Bits
Block Size	64 Bits	128, 192 or 256 Bits
Ciphertext	Symmetric Block Cipher	Symmetric Block Cipher
Max amount of data with block size	32 GB (At this point another key needs to	256 Exabyte/256 billion Gigabytes
Possible key combinations	2^{56}	2^{128}, 2^{192}, 2^{256}
Network Structure	Feistel Network Structure is used	Permutation-Substitution Network Structure is used
Security	Vulnerable to many attacks like Brute Force Attack	More secured algorithm due to long key length

5. Modification to the DES-GEDTD Protocol

As discussed in previous sections, AES algorithm is more secure than DES. Hence we have developed a new modified protocol from the existing one called AES-GEDTD protocol. This AES-GEDTD protocol enhances the packet delivery ratio and delay of data that is to be transferred through the network.

1) Delay- It is an average time taken by a data packet to arrive in the destination.

$$\text{Delay} = \frac{\sum (\text{arrive time} - \text{send time})}{\sum \text{Number of connections}}$$

Arrive time- End time that packets arrive to the destination.
Send time- Starting time that packet send by source.
The lower value of delay means better performance of the protocol.

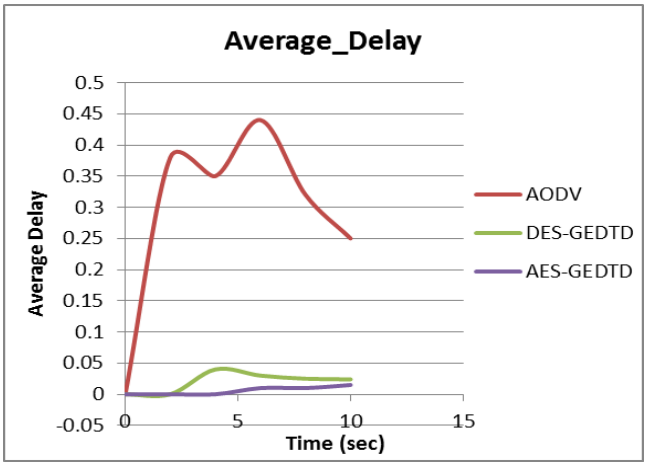

Figure 2: Average Delay

2) Packet Delivery Ratio (PDR) - It is the ratio of number of delivered data packets to the destination.

$$PDR = \frac{\sum \text{Number of packets received}}{\sum \text{Number of packets send}}$$

The greater value of PDR means better performance of the protocol.

Figure 3: Packet Delivery Ratio

3) *Energy Consumption* – It is the use of energy as a source of power.

Consume Energy= ∑ Initial Energy–∑ Final Energy

The lower value of energy consumption means better performance of the protocol.

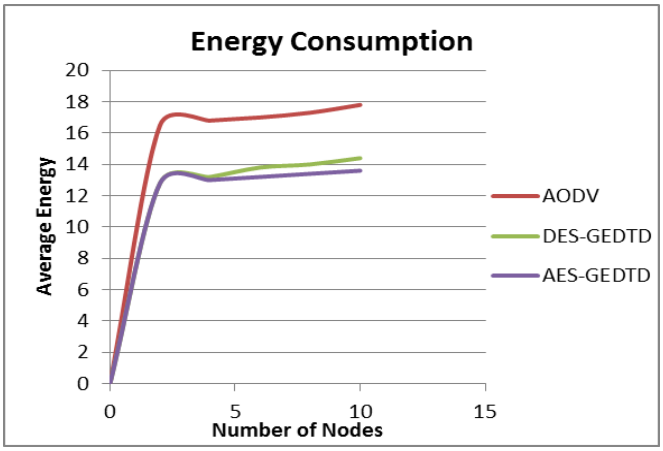

Figure 4: Energy Consumption

Above graphs show that our proposed modified approach of AES-GEDTD gives better performance than any other existing Geo-protocols.

6. Simulation Results

The proposed protocol is implemented in NS2 simulator. Four parameters are mainly considered to illustrate and evaluate the performance of the Geo -protocol as discussed in the above section. The current design of our algorithm depends on AES algorithm. The proposed approach is flexible. Hence, any encryption algorithm is used which gives better performance. But as discussed in an earlier section, AES algorithm has higher performance than any other symmetric algorithms, we used this algorithm in our approach

7. Conclusion

In this paper, we compare the DES-GEDTD and AES-GEDTD depending upon the various parameters like delay, packet delivery ratio and energy consumption. With this comparison, we modify the existing Geo-protocol and evolved a new AES-GEDTD protocol to enhance the performance of data transmission in the location based network. The approach can meet the higher security level.

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, pp. 63-69, 2008.
[3] P G Kolapwar, H P Ambulgekar, “A Survey on Location Based Data Encryption Algorithms for Mobile Devices”, IJARCSSE, pp. 1010-1015, 2014.
[4] Hatem Hamad and SouhirElkourd, "Data encryption using the dynamic location and speed of the mobile node", Journal Media and communication studies, pp. 67-75, 2010.
[5] 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.
[6] A. Perrig, R. Canetti, J.D. Tygar, D. Song, “The TESLA Broadcast Authentication Protocol”, 2002, pp. 2-13
[7] Di Qiu, Sherman Lo, Per Enge, Dan Boneh and Ben Peterson, " Geoencryption system security-Loran as a case study".
[8] Rohollah Karimi and Mohammad kalantari, “Enhancing security and confidentiality in location based data encryption algorithms”, IEEE Conference, pp. 30-35, 2011.
[9] V Rajeswari, V Murali and A.V.S. Anil, "A novel approach to identify Geo-Encryption with GPS and Different Parameters (Location and Time)", IJCSIT, pp. 4917-4919, 2012.
[10] Yan Zhu, DI Ma, Dijiang Huang, Changjun, "Enabling Secure Location- Based Sevices in Mobile Cloud Computing", ACM, pp. 27-32, 2013.
[11] Ganasan S P “An asymmetric authentication protocol for mobile devices using elliptic curve cryptography”, IEEE Conference, pp. 107-109, 2010.
[12] Ku, We Shinn, "Geo-Store: A Framework for Supporting Semantics-Enabled Location-Based Services", IEEE Conference, pp. 35-43, 2013
[13] William stallings, “Cryptography and Network Security”, Fifth Edition.