Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2006 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

2006

# A Novel Approach for Data Encryption Depending on User Location

Hsien-Chou Liao
*Chaoyang University of Technology*, hcliao@cyut.edu.tw

Yun-Hsiang Chao
*Chaoyang University of Technology*

Chia-Yi Hsu
*Chaoyang University of Technology*

# A Novel Approach for Data Encryption Depending on User Location

Hsien-Chou Liao, Yun-Hsiang Chao, and Chia-Yi Hsu
Department of Computer Science and Information Engineering
Chaoyang University of Technology, Taiwan, R. O. C.
E-mail: hcliao@cyut.edu.tw

**Abstract**

*The wide spread of WLAN and the popularity of mobile devices increases the frequency of data transmission between information system and mobile user. However, most of the data encryption technology is location-independent. An encrypted data can be decrypted anywhere. The encryption technology cannot restrict the location of data decryption. In order to meet the demand of data transmission in the future, a location-dependent approach, called location-dependent data encryption algorithm (LDEA), is proposed in this paper. A target latitude/longitude coordinate is determined firstly. 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 match with the target coordinate. However, current GPS receiver is inaccuracy and inconsistent. The location of a mobile user is difficult to exactly match with the target coordinate. A toleration distance (TD) is also designed in LDEA to increase its practicality. The security analysis shows that the probability to break LDEA is almost impossible since the length of the random key is adjustable. A prototype is also implemented for experimental study. The results show that the ciphertext can only be decrypted under the restriction of TD. It illustrates that LDEA is effective and practical for data transmission to mobile users.*

**Keywords**: data encryption, security, GPS, mobile computing, location-based service

## 1. Introduction

Since the removal of signal-degrading selective availability (SA) from GPS (Global-Positioning System) signals on the 1st May 2000, it is now possible to use hand-held GPS to navigate to within a few meters. The differential GPS (DPGS) can even provide the accuracy to less than one meter. Now, GPS receiver is popular used in our daily life, such as car navigation, fleet management, and so on. In the past, GPS receiver is connected to the mobile devices, such as PDA (personal digital assistant), via cable or Bluetooth. It is a little inconvenient for users. Therefore, a PDA with an integral GPS receiver, called GPS PDA, is designed and announced on the mid of 2005. GPS PDA is also equipped with most of the wireless communication capabilities, including GSM/GPRS/EDGE, quad-band GSM phone capabilities, IEEE 802.11g, *etc*. The size and weight of GPS PDA is close to the mobile phone. But, it's computing power and programming interface is better than mobile phones. It is expectable that the mobile phones will be replaced by such kind of PDA in the future. Unlike the mobile phones which data transmission is mostly based on SMS (Short Message Service), the types and quantities of data transmitted among GPS PDAs or from information system to such PDA must be diverse and huge just like desktop PCs. That is, the data transmission among mobile devices will become more and more frequent according to the above trend.

On the other hand, many methods are proposed for the security of data transmission; for example, M. Aikawa et al. proposed a light-weight encryption algorithm for the copyright protection (Aikawa et al. 1998). T. Jamil proposed an enhanced algorithm for the typical DES algorithm, called AES (Advanced Encryption Standard) (Jamil 2004). J. Jiang proposed a parallel processing algorithm for the RSA (Jiang 1996). S. Lian et al. proposed a fast video encryption scheme based on chaos [4]. M. McLoone and J. V. McCanny designed a hardware circuit for DES based on the FPGA technique (McLoone et al. 2000). M. Shaar et al. proposed a new data encryption algorithm, called HHEA (Shaar et al. 2003). M. E. Smid and D. K. Branstad analyzed the past and future of DES algorithm (Smid et al. 1988). Y. P. Zhang et al. proposed a stream cipher algorithm with respect to the traditional block-based cipher approaches (Zhang et al. 2004).

However, these methods are location-independent. The sender cannot restrict the location of the receiver for data decryption. If the data encryption algorithm can provide such function, it is useful for satisfying the demand of data transmission in the future. Therefore, a location-dependent data encryption algorithm (LDEA) is proposed in this paper. The latitude/longitude coordinate is used as the key for data encryption in LDEA. When a target coordinate is determined for data encryption, the ciphertext can only be decrypted at the expected location. Since the GPS receiver is inaccurate and inconsistent depending on how many satellite signals received. It is difficult for receiver to decrypt the ciphertext at the same location exactly matched with the target coordinate. It is impractical by using the inaccurate coordinate as key for data encryption. Consequently, a toleration distance (TD) is designed in LDEA. The sender can also determine the TD and the receiver can decrypt the ciphertext within the range of TD. In order to verify the performance of LDEA, a prototype tool is also implemented and tested in an outdoor experimental site. The experimental result illustrates that LDEA is effective and practical for data transmission in mobile environment.

The rest of the paper is organized as follows. Section 2 reviews related works. Section 3 presents the process and steps of LDEA. Section 4 presents the security analysis and experimental study. Section 5 gives the conclusion and future works of our research.

## 2. Related Works

The popular of indoor or outdoor positioning devices cause the location-based services (LBSs) are getting important. Information systems can provide LBSs according to the location of users. Current LBSs can be classified into four categories: emergency service, information service, tracking service, and entertainment service (Mohapatra et al. 2005). Emergency services include safety alarm, public safety, and so on. For example, Y. Zhang et al. proposed location-based keys for the sensor network (Zhang et al. 2005). It was an authentication scheme between sensor nodes. Information services include the news, sport, weather, shopping, yellow page, and so on (Becker et al. 2005; Toye et al. 2005). Tracking services include the property, military, cargo tracking, and so on. M. Gruteser et al. discussed the privacy protection problems related to the tracking service (Gruteser et al. 2004). A disclosure-control algorithm was proposed to hide users' position in sensitive area. Entertainment services include dating, game playing, and so on. N. Eagle et al. designed a Bluetooth access point, called BlueDar (Eagle et al. 2005). It can interchange information with the mobile devices of the passing passengers. If the passenger predefines the demands of friends, such as age, hobby, BlueDar can match his

demands with the collected information of the passengers. J. Xu et al. proposed a D-tree structure for the query planning of LBSs (Xu et al. 2004). The proposed LDEA can enhance the security of data transmission on delivering LBSs.

Besides, L. Scott and D. E. Denning proposed a data encryption algorithm by using the GPS, called Geo-Encryption (Scott et al. 2003). 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 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 the received GeoLock session key to get the final session key. The final session key was used to decrypt the ciphertext. However, the PVT-to-GeoLock mapping function is the 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.

## 3. LDEA Algorithm

The purpose of LDEA is mainly to incorporate the latitude/longitude coordinate in the data encryption and thus to restrict the location of data decryption. A toleration distance (TD) is designed to overcome the inaccuracy and inconsistent problem of GPS receiver. The process of LDEA is shown in Figure 1. When the target coordinate and TD is given by the sender (information system or mobile user) on the left-hand side, an LDEA-key is generated from latitude/longitude coordinate and TD. The random-key generator issues a session key, called R-key. Then, the final-key for encrypting the plaintext is generated by exclusive-or R-key with LDEA-key. The final-key can be used for the symmetric encrypt algorithm, such as DES, AES, triple-DES, *etc*. In the bottom of Figure 1, $KU_r$ and $KR_r$ is the public and private keys generated on the receiver side. $KU_r$ is transmitted to the sender side firstly. Then, TD and R-key is transmitted via asymmetric encryption algorithm. When the receiver gets the TD and R-key, the LDEA-key can be generated from TD and the coordinate acquired from GPS receiver. The final-key can be generated by exclusive-or R-key with LDEA-key. If the acquired coordinate is matched with the target coordinate within the range of TD, the ciphertext can be decrypted back to the original plaintext. Otherwise, the result is indiscriminate and meaningless.

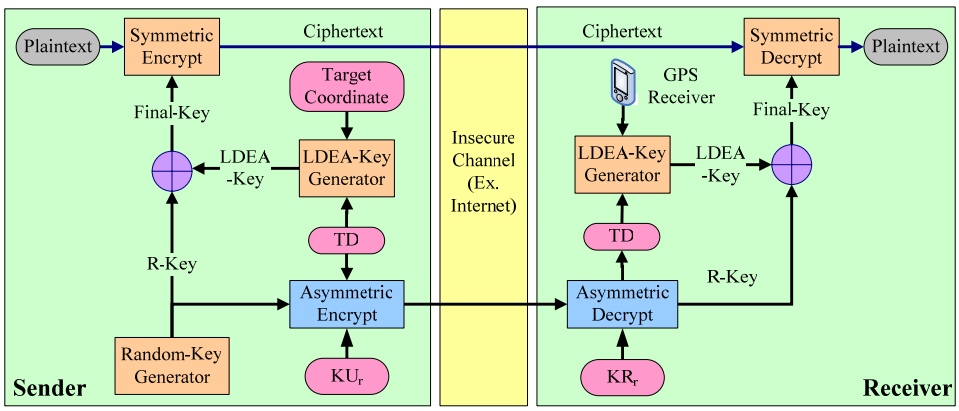



Figure 1: The LDEA process

The target coordinate can be determined by the sender or receiver. If it is determined by the sender, the sender can inform the receiver the physical location for data encryption. A secure communication, such as telephone, is convenient and safety for the sender to notify the receiver. If the target coordinate is determined by the receiver, the receiver can inform the sender in the same way, e.g., telephone. After the sender gets the target coordinate, the data can be transmitted to the receiver according to the above process.

The generation of LDEA-key, R-key, and final-key is presented in more details. An example shown in Figure 2 is used to illustrate the generation process. TD is assumed as five meters in the example.

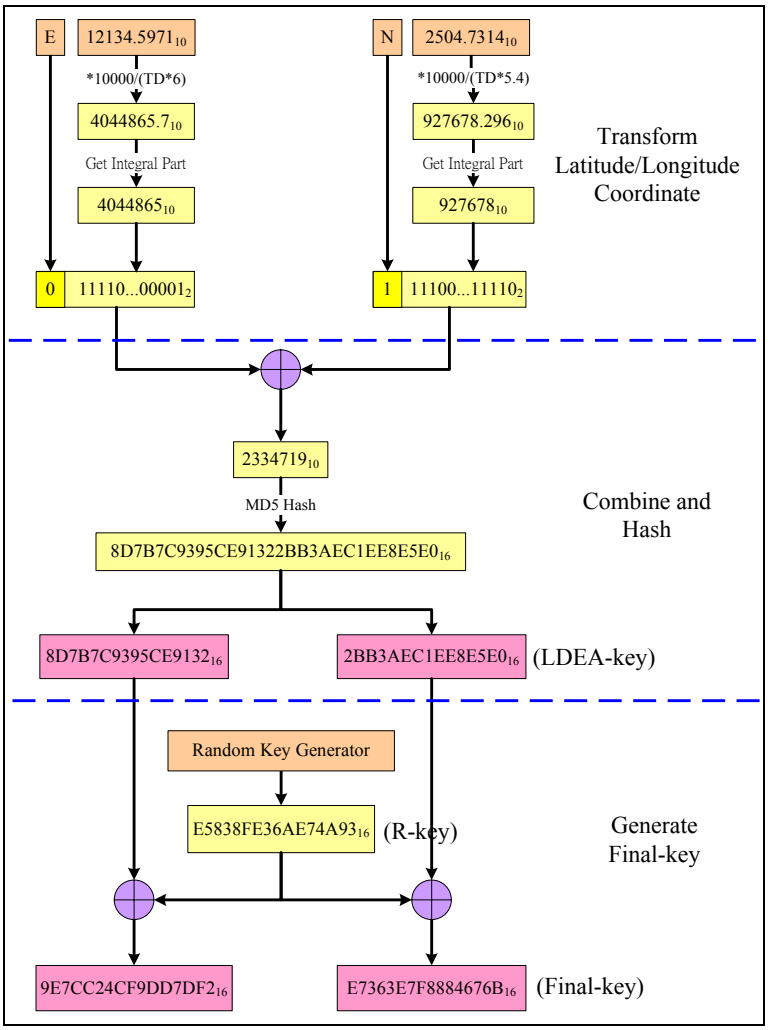



Figure 2: An example for illustrating the generation of the final-key

1. Transform latitude/longitude coordinate
   The format of coordinate acquired from the GPS receiver is WGS84 (world geodetic system 1984) defined in NMEA (National Marine Electronics Association) specification. For example, "E 12134.5971" means 121 degrees and 34.5971 minutes east longitude. "N 2504.7314" means 25 degrees and 4.7314 minutes north latitude. The coordinates are multiplied 10000 to be an integer. Then, the integer is divided by a value corresponding to the TD in order to allow the coordinate inaccuracy. According to the estimation of CoordTrans tool of Franson Company, the values are 5.4 and 6 for latitude and longitude corresponding to one meter, respectively. In advance, one bit is put in front of the integral part of the above result. The bit is zero for east and south and one for west and north.

2. Combine and Hash
   The transformation results of the above step are combined by performing a bitwise exclusive-OR operation. Then, MD5 hash algorithm is utilized and generates a 128-bit digest for the combined result. Then, the digest is split into two 64-bit values, called LDEA-keys. This step causes that the target coordinate is unable to be derived from the LDEA-keys.

3. Generate Final-key
   A session key (R-key) is generated randomly with the same length of LDEA-key, i.e., 64 bits in the example. LEDA-keys are exclusive-OR with the R-key separately to generate the final-keys. Two final-keys are used as the secret key and initial value of DES symmetric encryption algorithm.

Current design of LDEA algorithm is based on the MD5 hash and DES algorithm. However, LDEA is flexible and can be incorporated with other algorithms, such as AES, triple-DES, *etc*. These steps should be redesigned when necessary.

## 4. Security Analysis and Experimental Study

### *4.1 Security Analysis*

If the latitude/longitude coordinate is simply used as the key for data encryption, the possible key space is the same as the surface of the Earth that equals $5.11\times10^8$ square kilometer, i.e., $5.11\times10^{14}\,m^2$. However, 80 percent of people live on only 3 percent of the surface on the Earth. If the setting of TD is considered as 20 meters, the probability to break such key is only $1/1.22\times10^{10}$ as shown in Equation (1). Such strength is not strong enough.

$$\frac{1}{5.11\times10^{14}\,m^2\times0.03/(3.14159\times20^2)m^2}=\frac{1}{1.22\times10^{10}} \quad \text{.....(1)}$$

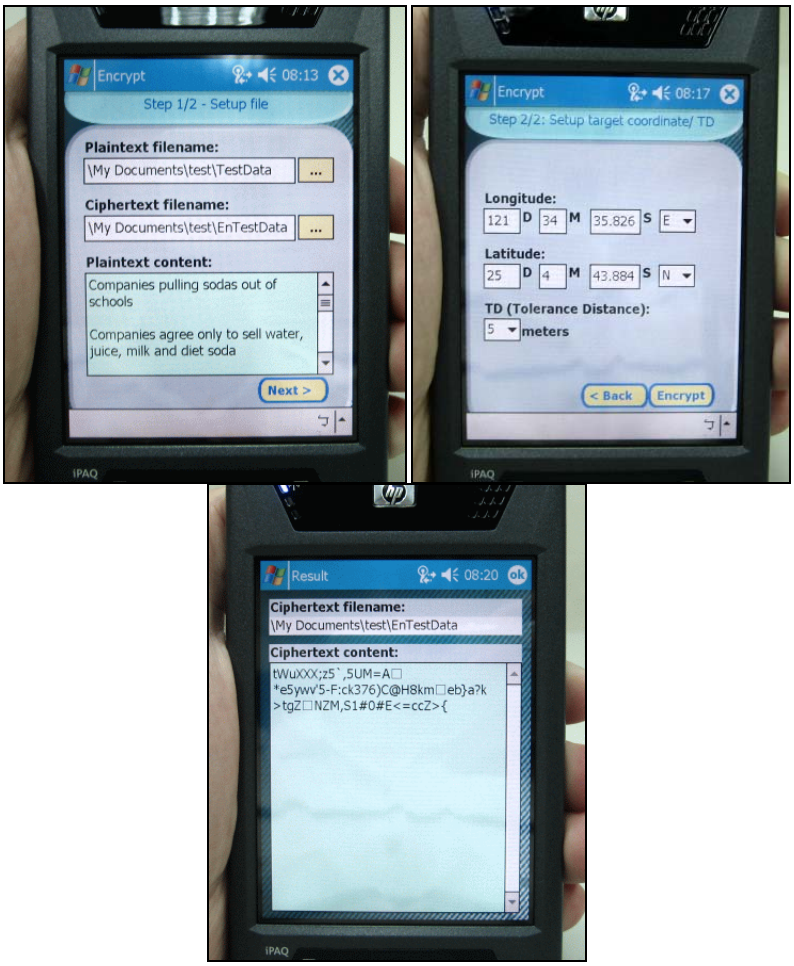
That is the reason why a random key is incorporated into LDEA algorithm. The final-key is generated from the exclusive-OR of R-key and LDEA-key. The DES algorithm is used in current design of LDEA and the length of final-key is 64 bits. The probability of breaking the LDEA is $1/2^{64}\,(\approx1/10^{19})$.

The security strength can still be improved by replacing the symmetric algorithm in LDEA according to the requirement on the security level. For example, the maximal key lengths of triple-DES and AES are 168 and 256 bits, respectively. The corresponding strength is stronger than the DES with key length of 64 bits. However, the increase of the key length also increases the computation load. It is a tradeoff between the strength and computation load.

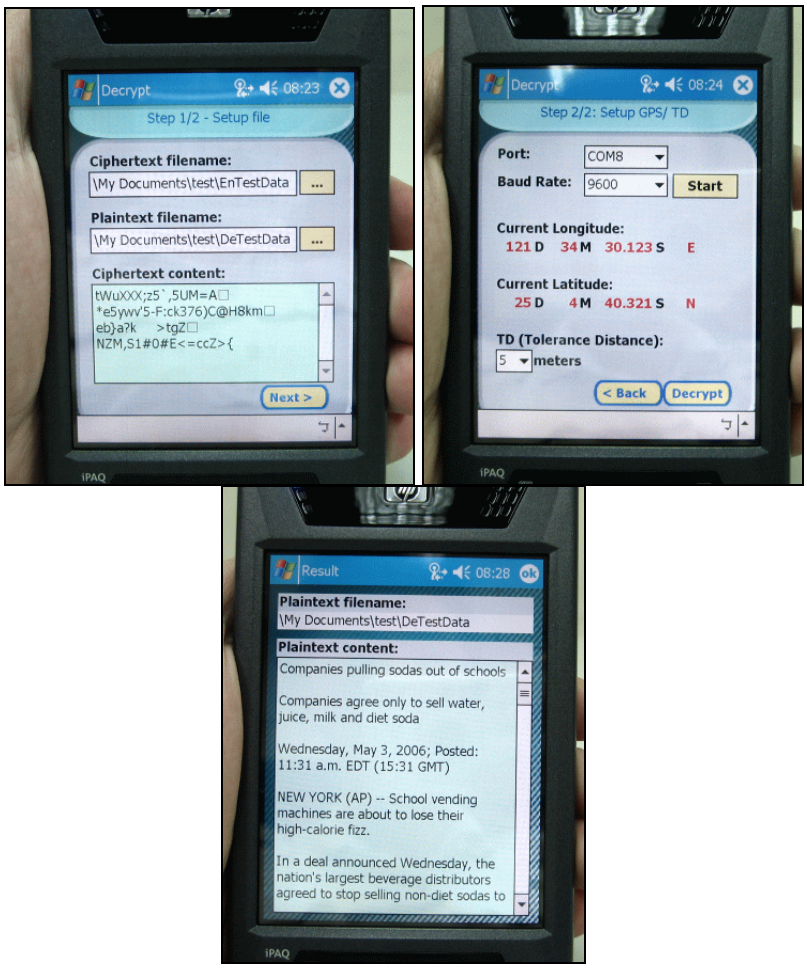
### *4.2 Experimental Study*

A prototype was implemented to illustrate and evaluate the practicality of LDEA algorithm. The functions of encryption and decryption are implemented in the same prototype. Six screen shots of the prototype are used to illustrate the encryption and decryption steps as shown in Figure 3. Assume the sender and receiver is mobile user. In Figure 3 (a), the sender enters the filenames of plaintext and ciphertext. The contents of the plaintext are then displayed in the bottom automatically. In Figure 3 (b), the sender enters the target coordinate and TD. After pressing the 'Encrypt' button, the ciphertext is generated and shown in Figure 3 (c). Similarly, the receiver determines the filenames of ciphertext and plaintext. The contents of the ciphertext are shown in the bottom of Figure 3 (d). In Figure 3 (e), the receiver assigns the port and baud rate for GPS receiver. The latitude/longitude is then acquired from GPS receiver after pressing the 'Start' button. The receiver also selects a TD and presses the 'Decrypt' button. The decrypted result is

saved and displayed on the screen as shown in Figure 3 (f). Therefore, if the acquired coordinate meets the constraint of target coordinate and TD, the contents of the decrypted file are the same as the original file. Otherwise, the contents are indiscriminate and meaningless.




(a) (b) (c)




(d) (e) (f)

Figure 3: The screen shots of the prototype (a)~(c) encryption (d)~(f) decryption

An experimental site is also designed for the prototype as shown in Figure 4. A set of concentric circles is marked on the ground for every five meters. The center of the circle is defined as the target latitude/longitude location. The settings of TD are 0, 5, 10, 15, and 20 meters. The testing distance is from zero to 40 meters for every five meters. The experimental steps are listed in the following:

Step 1. The target coordinate at the center is acquired from the GPS receiver.

Step 2. For every TD, a source file is encrypted by using the target coordinate and TD firstly.

Step 2.1. For every circle, the tester moves randomly along the curve of the circle and tries to decrypt the data about every minute.

Step 2.2. There are totally ten times of data decryption. The destination file is checked whether the content is the same as the original file. The number of successful decryption is recorded.

Step 3. Repeat Step 2 until finishing the testing of all TDs.

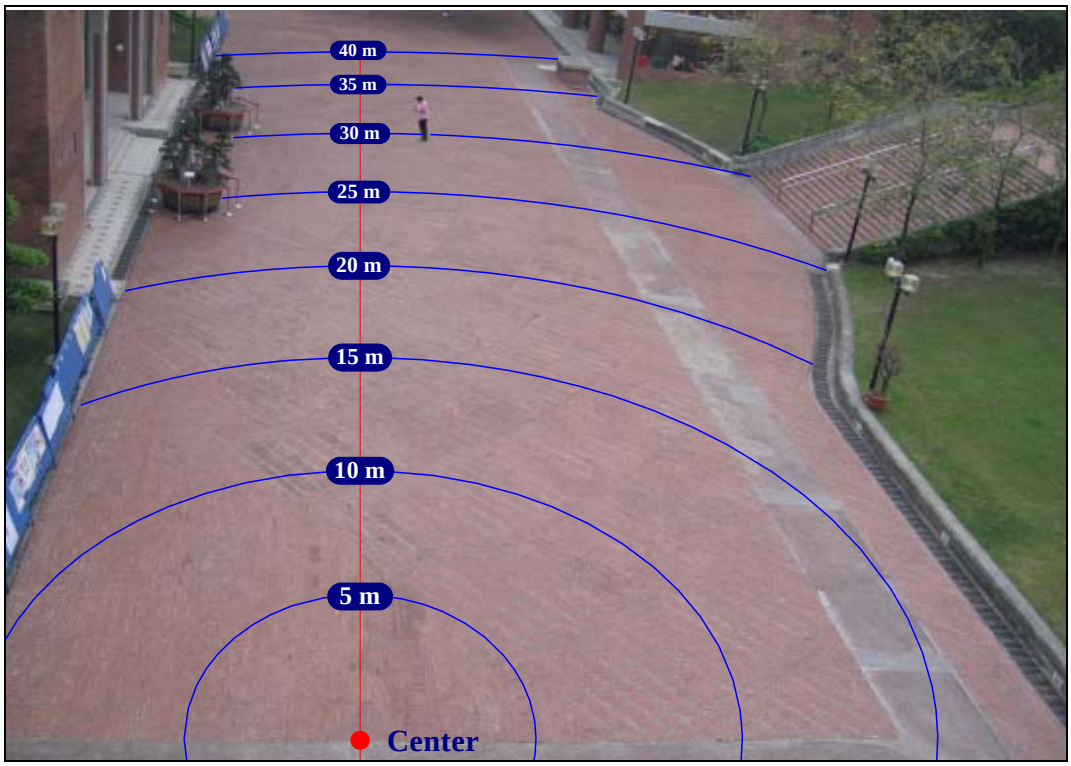



Figure 4: The design of the experimental site

The successful rate is computed for every combination of TD and testing distance. The experimental result is shown in Figure 5.

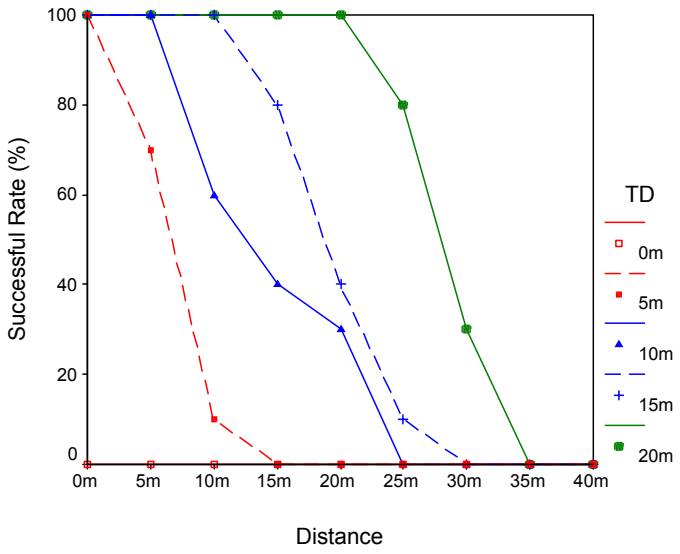



Figure 5: The successful rate vs. distance under various TDs

In Figure 5, the successful rate of all the testing distance is zero when TD is zero. This is the same as our expectation. The inaccuracy of GPS receiver causes the ciphertext is unable to be decrypted successfully. When TD is five meter, the successful rate is 100 percent when the tester is at the center. The rate is decreased to 70 percent when the testing distance is five meters. The maximum distance (MD) is 15 meters when the rate is

zero percent. It means that the inaccuracy of GPS receiver causes the testing distance may be longer than the setting of TD.

The MDs for every TD are listed in Table 1. The difference of MD and TD is also listed in the table. According to the results, MD is longer than TD about 15 meters in the real situation. It means that the data can be decrypted beyond the constraint of TD. The user should know such situation. So, the settings of TD should be modified as 5/20, 10/25, 15/30, and 20/35 meters. The modified TD of five meters should be 5/15 according to the result in Table 1. It is modified as 5/20 in order to be consistent with the other modified TDs. Users can clearly understand that the first number is the distance with 100 percent successful rate and the second number is the maximum distance for data decryption.

Table 1: The MDs under various TDs

| TD | 0 m | 5 m | 10 m | 15 m | 20 m |
|---|---|---|---|---|---|
| MD | 0 m | 15 m | 25 m | 30 m | 35 m |
| MD–TD | 0 m | 10 m | 15 m | 15 m | 15 m |
| Modified TD | 0 m | 5/20 m | 10/25 m | 15/30 m | 20/35 m |

## 5. Conclusion and Future Work

Traditional encryption technology cannot restrict the location of mobile users for data decryption. In order to meet the demand of data transmission in the future, LDEA algorithm is proposed in this paper. LDEA provide a novel function by using the latitude/longitude coordinate as the key of data encryption. A toleration distance (TD) is also designed to overcome the inaccuracy and inconsistent of GPS receiver. The security strength of LDEA is adjustable when necessary. The experimental result of the prototype also shows that the decryption is constrained by the range of TD. As a result, LDEA is effective and practical for the data transmission between information system and mobile user or between mobile users.

Current design of LDEA algorithm is mainly based on the DES algorithm. Other algorithms, such as AES, triple-DES, *etc.*, can used to replace the DES algorithm when necessary. In advance, the future works may include the following topics:

1. The alternative LDEA algorithms incorporating with the mature algorithms can be developed to demonstrate its flexibility.
2. Some factors can be incorporated into LDEA, such as time, moving speed, or moving path, *etc.*, to increase the security strength and usability of LDEA.
3. The LDEA algorithms can be extended to the other application domains, e.g., the authorization of mobile software. If mobile software is authorized within a pre-defined area, such as a city, the execution of the software may activate the location check based on the LDEA algorithm. The software can be executed only when the user is within the authorized area. Besides, the distribution of multimedia content may be utilized the LDEA algorithm for advanced access control except the username/password.

The proposed LDEA algorithm provides a novel way for data security. It is also meet the trend of mobile computing. Many possible applications will be developed in the future to demonstrate and promote the concept of LDEA algorithm.

**Acknowledgement**
This work was funded by the National Science Council under grant NSC94-2815-C-324-007-E.

**References**

Aikawa, M., Takaragi, K., Furuya, S., and Sasamoto, M., "A Lightweight Encryption Method Suitable for Copyright Protection," *IEEE Trans. on Consumer Electronics* (44:3), 1998, pp. 902-910.

Becker, C. and Durr, F., "On Location Models for Ubiquitous Computing," *Personal and Ubiquitous Computing* (9:1), 2005. pp. 20-31.

Eagle, N. and Pentland, A., "Social Serendipity: Mobilizing Social Software," *IEEE Pervasive Computing* (4:2), 2005, pp. 28-34.

Gruteser, M. and Liu, X., "Protecting Privacy in Continuous Location-Tracking Applications," *IEEE Security & Privacy Magazine* (2:2), 2004, pp. 28-34.

Jamil, T., "The Rijndael Algorithm," *IEEE Potentials* (23:2), 2004, pp. 36-38.

Jiang, J., "Pipeline Algorithms of RSA Data Encryption and Data Compression," *Proc. of IEEE Int'l Conf. on Comm. Technology (ICCT'96)* (2), 5-7 May 1996, pp. 1088-1091.

Lian, S., Sun, J., Wang, Z., and Dai, Y., "A Fast Video Encryption Scheme Based-on Chaos," *Proc. of the 8th IEEE Int'l Conf. on Control, Automation, Robotics, and Vision (ICARCV 2004)* (1), 6-9 Dec. 2004, pp. 126-131.

McLoone, M. and McCanny, J. V., "A High Performance FPGA Implementation of DES," *Proc. of IEEE Workshop on Signal Processing Systems (SiPS 2000)*, 11-13 Oct. 2000, pp. 374-383.

Mohapatra, D. and Suma, S. B., "Survey of Location based Wireless Services," *Proc. of IEEE Int'l Conf. on Personal Wireless Comm. (ICPWC 2005)*, 23-25 Jan. 2005, pp. 358-362.

Scott, L. and Denning, D. E., "Using GPS to Enhance Data Security: Geo-Encryption," *GPS World* (14), April 2003, pp. 40-49.

Shaar, M., Saeb, M., Elmessiery, M., and Badwi, U., "A Hybrid Hiding Encryption Algorithm (HHEA) for Data Communication Security," *Proc. of the 46th IEEE Int'l Midwest Symposium on Circuits and Systems (MWSCAS'03)* (1), 27-30 Dec. 2003, pp. 476-478.

Smid, M. E. and Branstad, D. K., "Data Encryption Standard: Past and Future," *Proc. IEEE* (76:5), May 1988, pp. 550-559.

Toye, E., Sharp, R., Madhayapeddy, A., and Scott, D., "Using Smart Phones to Access Site-Specific Services," *IEEE Pervasive Computing* (4:2), Jan.-March 2005, pp. 60-66.

Xu, J., Zheng, B., Lee, W. C., and Lee, D. L., "The D-Tree: An Index Structure for Planner Point Queries in Location-Based Wireless Services," *IEEE Trans. on Knowledge and Data Engineering* (16:12), 2004, pp. 1526-1542.

Zhang, Y., Liu, W., Lou, W., and Fang, Y., "Securing Sensor Networks with Location-Based Keys," *Proc. of IEEE Wireless Comm. and Networking Conf. on Comm. Society (WCNC 2005)* (4), 13-17 March 2005, pp. 1909-1914.

Zhang, Y. P., Sun, J., and Zhang, X., "A Stream Cipher Algorithm Based on Conventional Encryption Techniques," *Proc. of IEEE Canadian Conference on Electrical and Computer Engineering (CCECE 2004)* (2), 2-5 May 2004, pp. 649-652.