IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 1, Ver. VI (Jan – Feb. 2015), PP 56-63
www.iosrjournals.org

A Location Dependent Cryptographic Approach Based on Target Coordinate & Distance Tolerant Key transfer for GPS mobile Receiver

Sourish Mitra[1], Avijit Chakraborty[2], Arunabha Bhaumik[3], Joy Dewanjee[4], Mainak Maulik[5]
[1, 2, 3, 4, 5](Department of Computer Science & Engineering, Gurunanak Institute of Technology, India)

Abstract: *Independent location based cryptography technique ensures that after transferring encrypted data from sending end ,decryption can takes place at anywhere from receiving point of view. But according to demand of mobile users if we want to ensures more security at the time of data transfer in mobile communication we need location dependency .It means ,when we encrypt a particular data packet at sending end and after transmitting that data to the receiver ,the receiver can be able to decrypt that packet only from a particular location (not from anywhere) specified by the sender by transferring location based coordinate target .In our proposed location based data encryption-decryption approach a target latitude/longitude coordinate is incorporated with a random key for data encryption. The receiver can only decrypt the cipher text when the coordinate acquired from GPS receiver is matched with target coordinate .The location of a receiver is difficult to exactly match with target coordinate .So we proposed a parameter distance tolerant(DT) in our proposed approach to increase its practicality. The security analysis shows that to probability to break our proposed algorithm is almost impossible since the length of the random key is adjustable.*

Keywords: *Location dependency, latitude/longitude, GPS, Distance tolerant, Target coordinates.*

I. Introduction

In location dependent cryptography method Sender can't restrict the location of the receiver for data decryption .If the encryption algorithm can provide such it is useful for increasing the security of mobile data transmission in the future .Therefore we propose location coordinate based encryption decryption technique where latitude longitude coordinate as the key for data encryption. When a target coordinate is determined for data encryption, the cipher text can only be decrypted at the expected location .Since the GPS receiver is inaccurate and inconsistent depending on how many satellite signal received .It is difficult for receiver to decrypt the text at same location exactly matched with the target coordinate .It is impractical by using inaccurate GPS coordinate as key for data encryption. Concurrently DT (Distance Tolerant) is designed in our proposed method. Sender can also determine the DT and the receiver can decrypt the text within the range of DT.

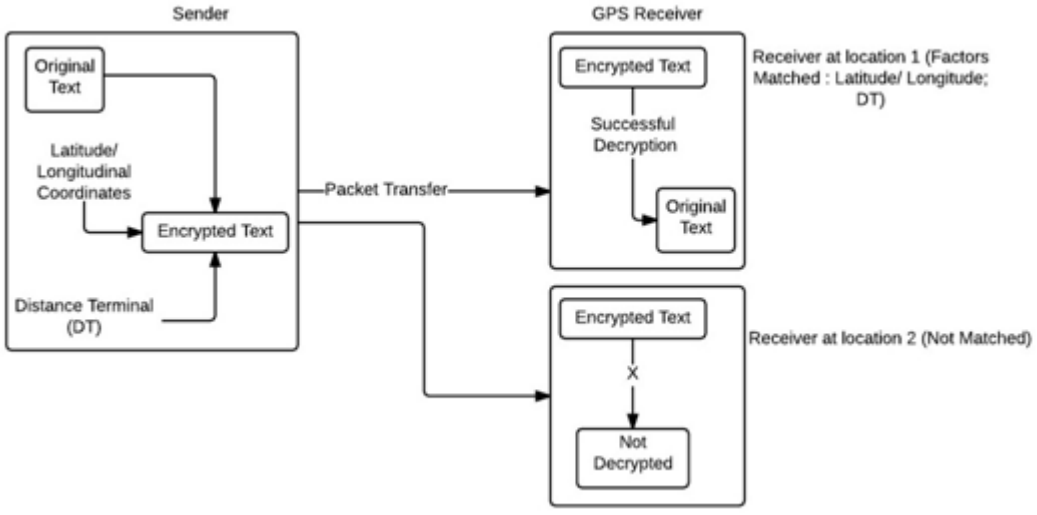


Fig. 1: Location Dependent Approach (Proposed)

II. Related Work

On 2003, Scott and Denning et al. proposed a data encryption algorithm by using the GPS, called Geo-Encryption. Geo-Encryption was based on the traditional encryption system and communication protocol. For

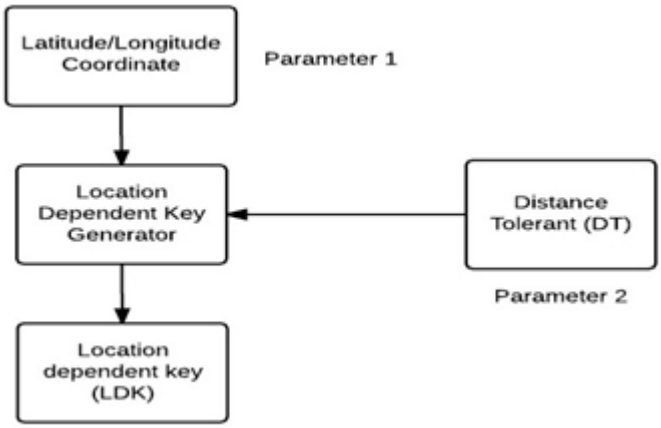
the sender, the data was encrypted according to the expected PVT (Position, Velocity and Time) of the receiver. A PVT-to-Geo Lock mapping function was used to get the Geo Lock key. Geo-Lock key was performed bitwise exclusive OR with a generated random key to get a Geo Lock session key. This key was 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-Geo Lock mapping function was used to get the Geo Lock key. The key was performing exclusive OR operation with the received Geo Lock session key to get the final session key. The final session key was used to decrypt the cipher text. However, the PVT to Geo Lock mapping function is the primary mechanism to ensure that the data can be decrypted successfully. It is troublesome for the sender and the receiver to own the same mapping function before the data transmission if they communicate occasionally.

III. Our proposed work

3.1 Purpose of proposed approach

Purpose of this approach is mainly to include the latitude/longitude co-ordinate in the data encryption and restrict the location of data decryption.DT (Distance Tolerant) is introduced to overcome the inaccuracy and inconsistency of GPS receiver.

3.2 Proposed Encryption –Decryption process discussion step by step



When the target co-ordinate and DT is given by the sender into location dependent key generator as input it will create a location dependent key (LDK).

3.3 Calculation of final keys from LDK by using latitude/longitude co-ordinate & DT

Step-1: According to the protocols of WGS84 (World Geodetic System 1984) defined in NMEA (National Marine Electronics Association) specification, we just explain the calculation of latitude/longitude as per example.

For example:

E 12159.8422 means 121° and 59.8422 minimum east longitude.N 2579.8221 means 25° and 79.8221 minimum north latitude.

Step-2: The co-ordinates are multiplied 10000 to be an integer.

E 12159.8422*10000	**N** 2579.8221*10000
=>121598422	=> 25798221

Step-3: Then the integer is divided by a value corresponding to the DT in order to allow the co-ordinate inaccuracy.

Step-4: According to the estimation of coord Trans tool of Franson Company, the values N: 25798221 divided by (DT*54) and E: 121598422 divided by (DT*60) for latitude and longitude. [Assuming DT=1/2]

So,

$$E \quad \frac{121598422}{DT*60}$$

$$\Rightarrow E \quad \frac{121598422}{½ *60}$$

$$\Rightarrow E \quad (4053280.733)_{10} \quad \text{[Get integral part]}$$

$$\Rightarrow E \quad (4053280)_{10}$$

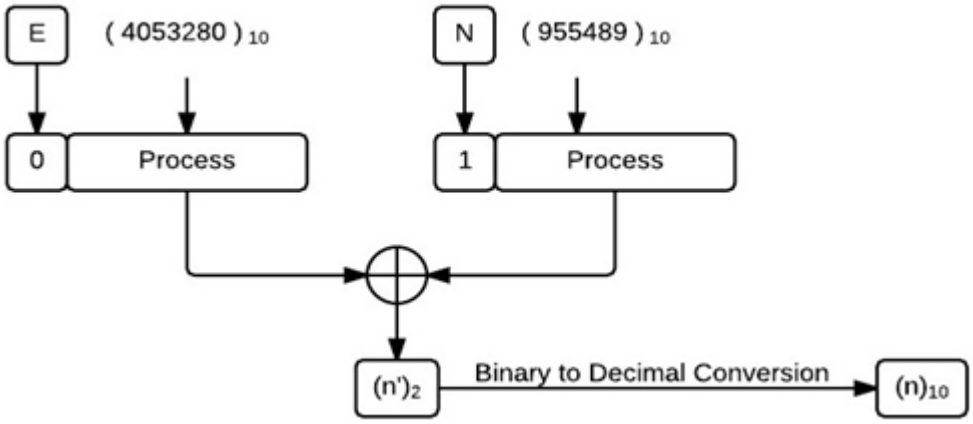
$$N \quad \frac{25798221}{DT*54}$$

$$\Rightarrow N \quad \frac{25798221}{½ * 54}$$

$$\Rightarrow N \quad (955489.667)_{10} \quad \text{[Get integral part]}$$

$$\Rightarrow N \quad (955489)_{10}$$

Step-5: One bit is put in front of the integral part of the result. The bit is zero for East and South and one for West and North.
So,



Step-6: Both binary numbers are involved with bitwise XOR operation and produce $(n')_{2}$. After that it will pass to binary to decimal converter and get $(n)_{10}$.The complete graphical representation is upto step 6 is presented in the next page.

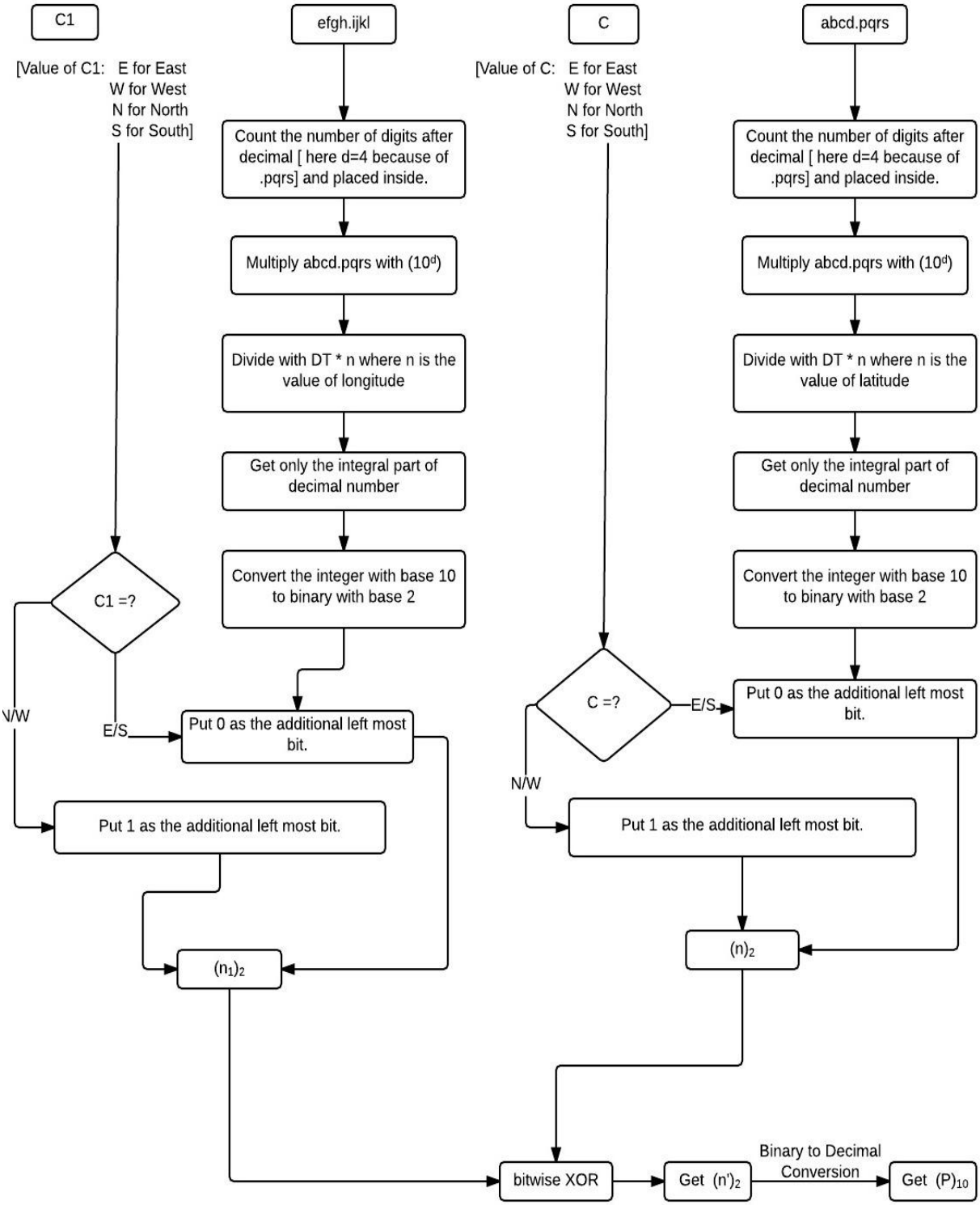


Fig. 2: Graphical Representation up to step 6

Step 7: Then MD5 hash algorithm is utilize and generates a 128 bit digest for the combine result. Then the digest is split into two 64 bit values called location dependent key [LDK] .This step causes
That the target coordinate is unable to be derived from the LDK.

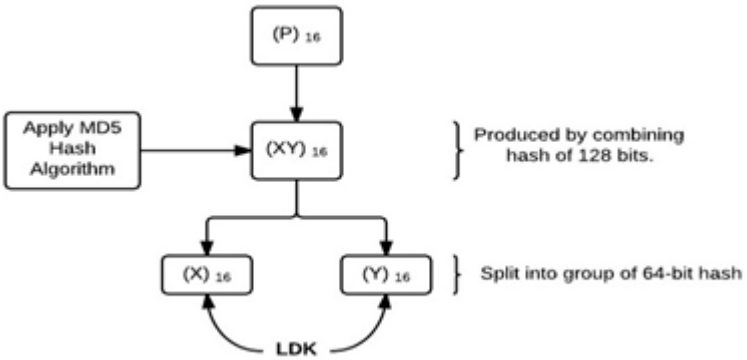


Fig. 3: Generation of Location Dependent Key [LDK]

Step -8: In this step, we can generate a final key pair after performing XOR operation with LDK.

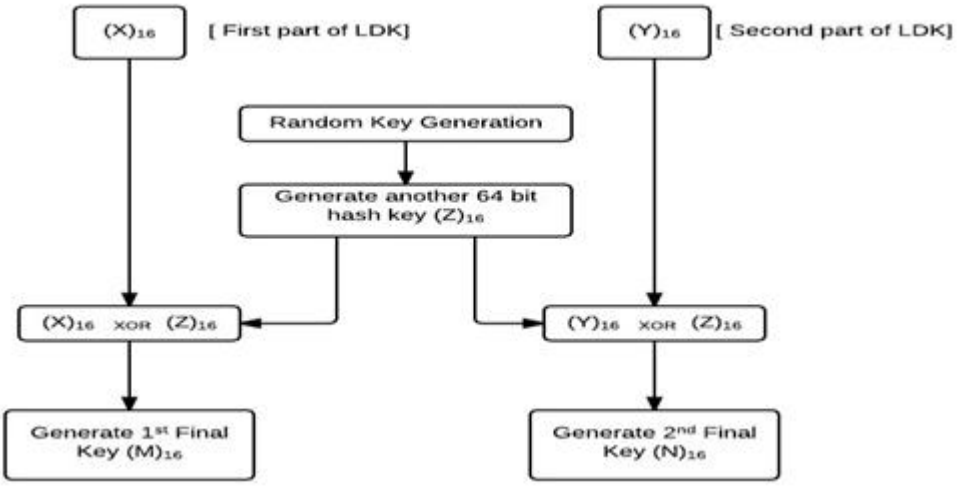


Fig. 4: Generation of Final Key

Step-9: Two final keys after Step-8, $(M)_{16}$ and $(N)_{16}$ are used as the secret key and initial value of symmetric encryption algorithm.(DES, AES, triple DES). Final diagram of proposed system at sending end is presented in the next page.

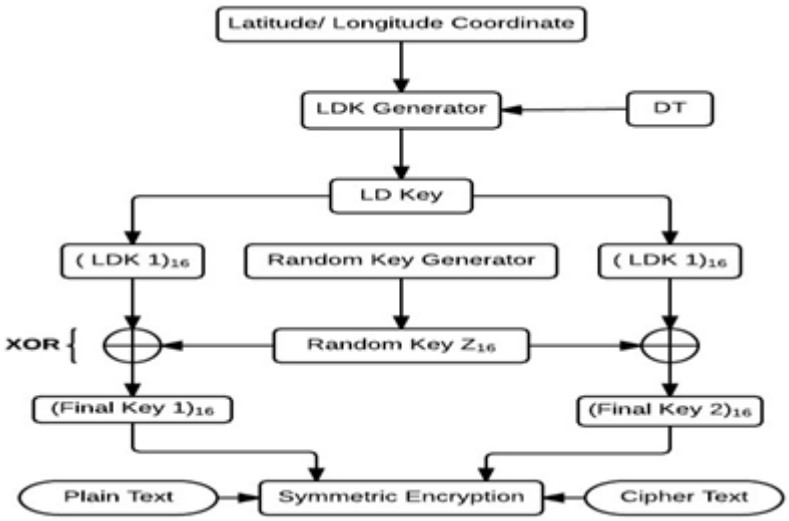
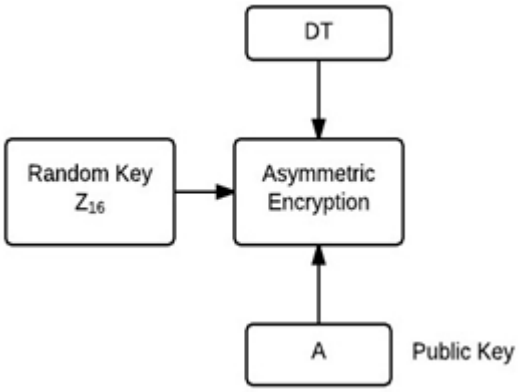


Fig. 5: Symmetric Encryption

Step-10: A and B are the public and private keys generated on the receiver side. A is transmitted to the sender side firstly. Then DT and randomly Z_{16} is transmitted via asymmetric encryption algorithm.



Step-11: When the receiver gets the DT and Z_{16}, the LDK can be generated from DT and the coordinate acquired from GPS receiver. The final key can be generated by XOR of Z_{16} and LDK. If the acquired coordinate is matched with target coordinate within the range of DT, the cipher text can be decrypted back to the original plaintext.

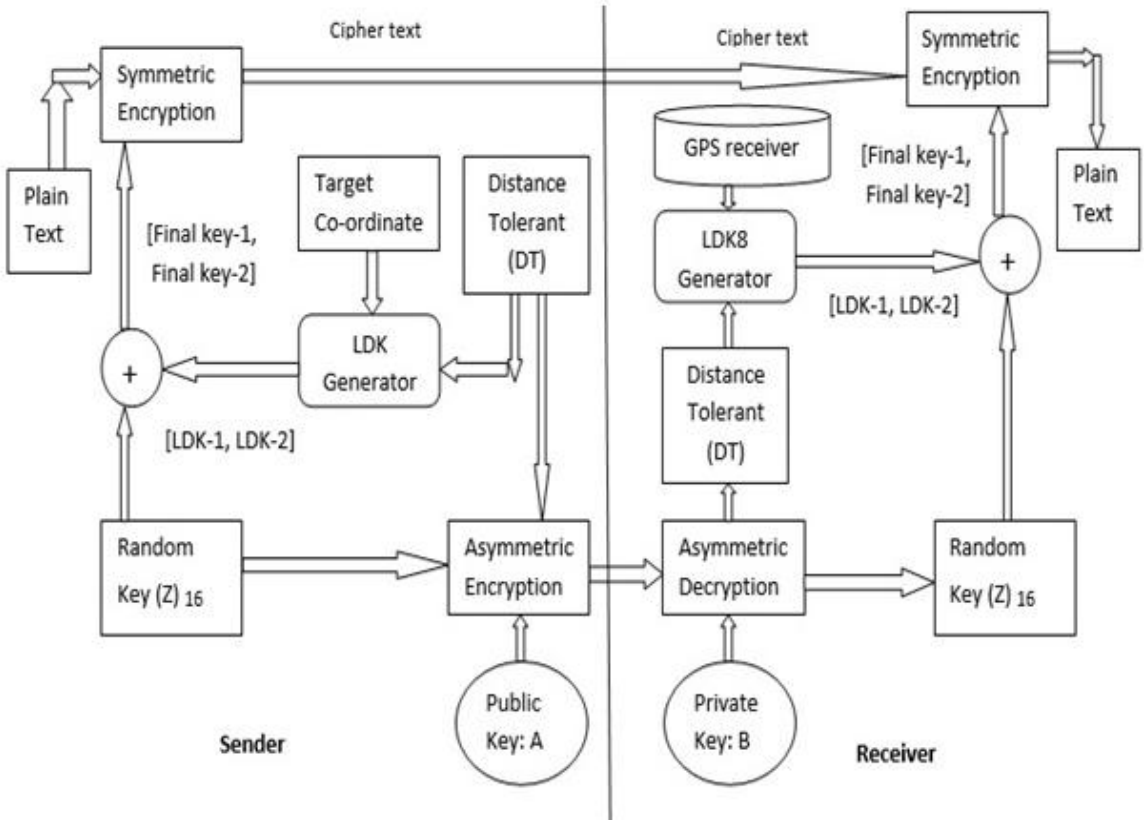
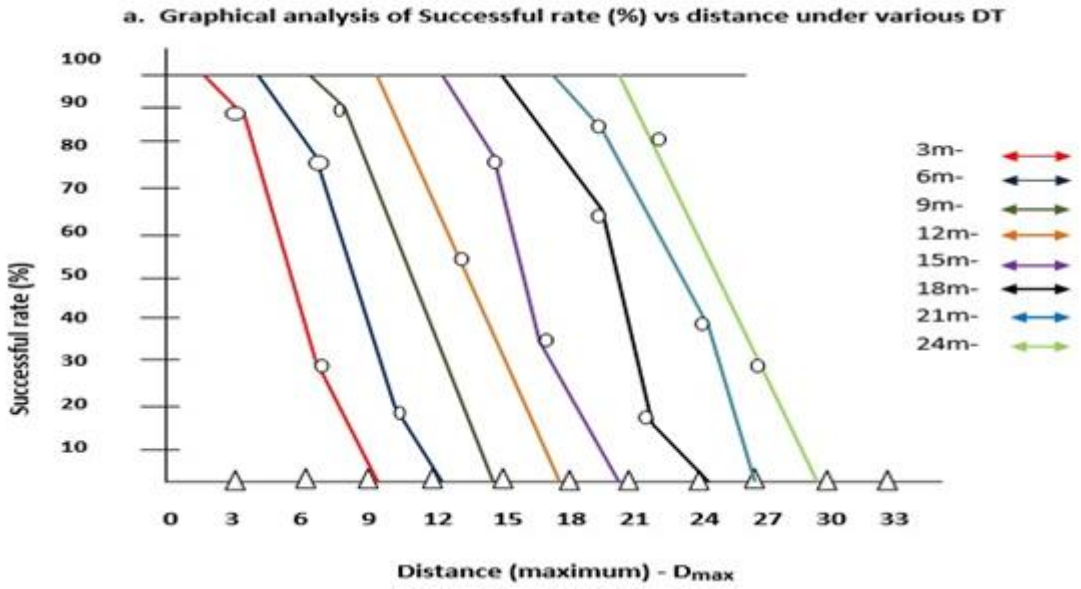


Fig. 6: Complete Encryption – Decryption Process (Proposed)

IV. Experimental Analysis

Fig. 7: Proposed Experimental Site

According to the above experimental site stated in fig-7, a set of concentric circle is defined as the target latitude/longitude location. The settings of DT are 0, 3, 6,9,12,15,18,21 and 24. The testing distance is from 0 to 24 meters for every 3m. The Target co-ordinate at the center is accessed by the GPS receiver. For every DT (Distance tolerant), a plaintext encryption occurs by using Target coordinate and DT. For every circle tester moves randomly along the curve of the circle and tries to decrypt data about every time instance. The destination file is checked whether the content is the same as the original file until finishing the testing of all DTs.



According to the above graph, we calculate successful rate for every combination of DT and testing distance. The experimental result is shown in same figure. The successful rate of all the testing distance is 0 when DT is 0. This is the same as our expectation. The graph clearly defines that the inaccuracy of GPS receiver causes the distance of possible successful decryption may be longer than the setting of DT.

Parameters	Values (unit: meter)								
DT	0	3	6	9	12	15	18	21	24
D_{max}	0	9	12	15	18	21	24	27	30
D_{max}-DT	0	6	6	6	6	6	6	6	6
Modified DT	0	3+6	6+6	9+6	12+6	15+6	18+6	21+6	24+6

The maximum distance for every DT and the difference of D_{max} and DT is shown in above table. According to the results D_{max} is longer than DT about6m in the experiment. It means that the data can be decrypted beyond the constraint of DT. So the settings of DT should be modified as 3+6, 6+6, 9+6 and so on. Users can clearly understand that the first number is the DT with almost 100% successful rate and the 2nd no is the extra distance for possibly successful decryption.

V. Conclusion

Our proposed algorithm provides a new function by using the latitude/longitude co-ordinate as the key of data encryption. A Distance Tolerant (DT) is also designed to overcome the inaccuracy and inconsistency of GPS receiver. The security strength of proposed algorithm is adjustable when necessary. As a result, our approach is effective and practical for data transmission in the mobile environment. Current design of our proposed approach is mainly based on DES, AES, triple DES can be used to replace the DES algorithm when necessary. Our proposed algorithm provides a new way for data security. It also meets the trend of mobile computing.

References

[1]. Jiang, J., 1996.Pipeline algorithms of RSA data encryption and data compression .In: proceeding IEEE International Conference on Communication Technology, 2:1008-1091

[2]. Lian, S., J.Sun,Z. Wang and Y. Dai ,2004.A fast video encryption technique based on chaos .In: Proceeding the 8th IEEE International Conference on Control , Automation ,Robotics and Vision, 1 :126-131.

[3]. Liao,H.C., P.C Lee , Y.H Chao and C.L Chen ,2007 .A location -dependent data encryption approach for enhancing mobile information system security .In:Proceeding the 9th International Conference on Advance Communication Technology, 1 :625-628.

[4]. McLoone , M. and J.V. McCanny , 2000.A high performance FPGA implementation of DES. In: Proceeding IEEE Workshop on Signal Processing Systems, pp:374-383.

[5]. Aikawa, M., K. Takaragi,S. Furuya and M. Sasamoto, 1998.A light weight encryption method suitable for copyright protection IEEE Trans. consumer Electron, 44:902-910.

[6]. Eagle, N. and A. Pentland, 2005. Social Serendipity: Mobilizing social software .IEEE Pervasive computing, pp:4.

[7]. Shaar, M., M. Saeb,M. Elmessiery and U . Badwi,2003.A Hybrid Hiding Encryption Algorithm (HHEA) for data documentation security. In: Proceeding the 46th IEEE International Midwest Symposium on Circuits and Systems: 476-478.

[8]. Smid, M.E. and D.K. Brandstad, 1988.Data Encryption Standard: Past and Fuutre .In: Proceeding the IEEE, 76: 550-559.

[9]. Xu, J., B. Zheng, W.C. Lee and D.L Lee, 2004. The D-Tree:An index structure for planner point queries inlocation-based wireless services. IEEE Trans. Knowledge Data Engine, 16:1526-1542.