Key Strength with Encryption and Dynamic Location of Mobile Phone

Hatem Hamad, Souhir ELKourd
Department of computer
Islamic University
Gaza, Palestine
hhamad@iugaza.edu.ps, el_kourd@yahoo.com

***Abstract*—This paper presents a new effective method for MMS message encryption which employs a new key to protect data sent between mobile phones. The novelty of this work lies in the dynamic location and speed of mobile devise which are generated by registering a set of coordinates and velocity during movement and estimate the next position. Dynamic tolerance distance (DTD) are applied in the algorithm to increase its practicality. The security analysis in our practical implementation shows that the probability to break this key is almost impossible due to the dynamic coordinates and DTD and adjusting the length of the Random key.**

The resulting encrypted data is found to be fully distorted, resulting in increasing the robustness of the proposed work. The simulation results validate the proposed data encryption scheme.

Keywords- DTD; data Encryption; GPS; MMS; mobile phone; SMS

I. INTRODUCTION

In this paper, we aim to protect the data sent between mobile phones where spying and spoofing have become a major threat to confidential data, especially in financial transactions as well as in military terms New dynamic location is applied in our secret key to integrate leading security solutions in the key encryption/decryption. On the other hand, Extensive researches have been done on data encryption for wireless networks and mobile phone transmission. However, few of these researches have focused on using dependant location to secure mobile devices. for example: In [HAT 10], proposed Data Encryption using the Dynamic location and Speed of mobile node. This protocol is to generate secret key using dynamic location where , mobile receiver register a set of coordinates and velocity during movement and estimate the next position. The secret key used this new coordinate and the dynamic tolerance distance (DTD) to encrypt/decrypt data . In [HIS 08], proposed a Location Data Encryption Algorithm (LDEA). The purpose of (LDEA) is mainly to include the latitude/longitude coordinate to be used as the key for data encryption in (LDEA). The cipher-text can only be decrypted at the expected location. A Toleration Distance (TD) is designed to overcome the inaccuracy and inconsistent problem mobile node and they are using a static Toleration Distance (TD) to overcome the inaccuracy and inconsistence of (GPS) receiver. On the other hand, the decryption is done while the mobile is moving very slowly which gives high successful rate of decryption. But when the mobile is moving with high speed, it was very difficult to perform successful decryption and that makes the successful rate of decryption equal to zero in the case of high-speed which demonstrates why the use of this approach is limited. In [ALA 07] , proposed a (GPS-based encryption-geo-encryption) protocol by restricting the decryption of a message to a particular location and time period. This protocol related in mobility model for existing geo-encryption techniques to allow mobile nodes to exchange movement parameters. However, the sender is able to geo-encrypt messages to a moving decryption zone that contains a mobile node's estimated location. However, this protocol is limited to a static location and cannot be used in dynamic location

The protocol presented in this paper is independent of the actual localization technique. However, in the current proposal, the dynamic location of the mobile node and the dynamic tolerance distance can be used with both fixed and mobile applications.

II. PROPOSED SOLUTION

The proposed solution is to generate a secret key shown in (Fig. 1) based on the parameter generated by the location of mobile and dynamic tolerance distance (DTD). the process is divide into two parts; the receiver part and the sender part. The right part, represents the mobile phone receiver and the left part, represents the mobile phone sender as it is shown in Fig. 1.

The receiver mobile generates the secret key by reading a set of coordinates during the movement. This movement depends on its speed to find the equation of path function and then calculates the estimated coordinate after a fixed time related to its speed. Moreover, it calculates the DTD to increase its practicality in the interval of encryption / decryption of the data, because the location service receiver has problem in inaccuracy and inconsistently which differ in the type of location service in the device. The details of generation secret key are given in the next section. In addition, it generates R-key randomly with the same length of secret key, therefore it

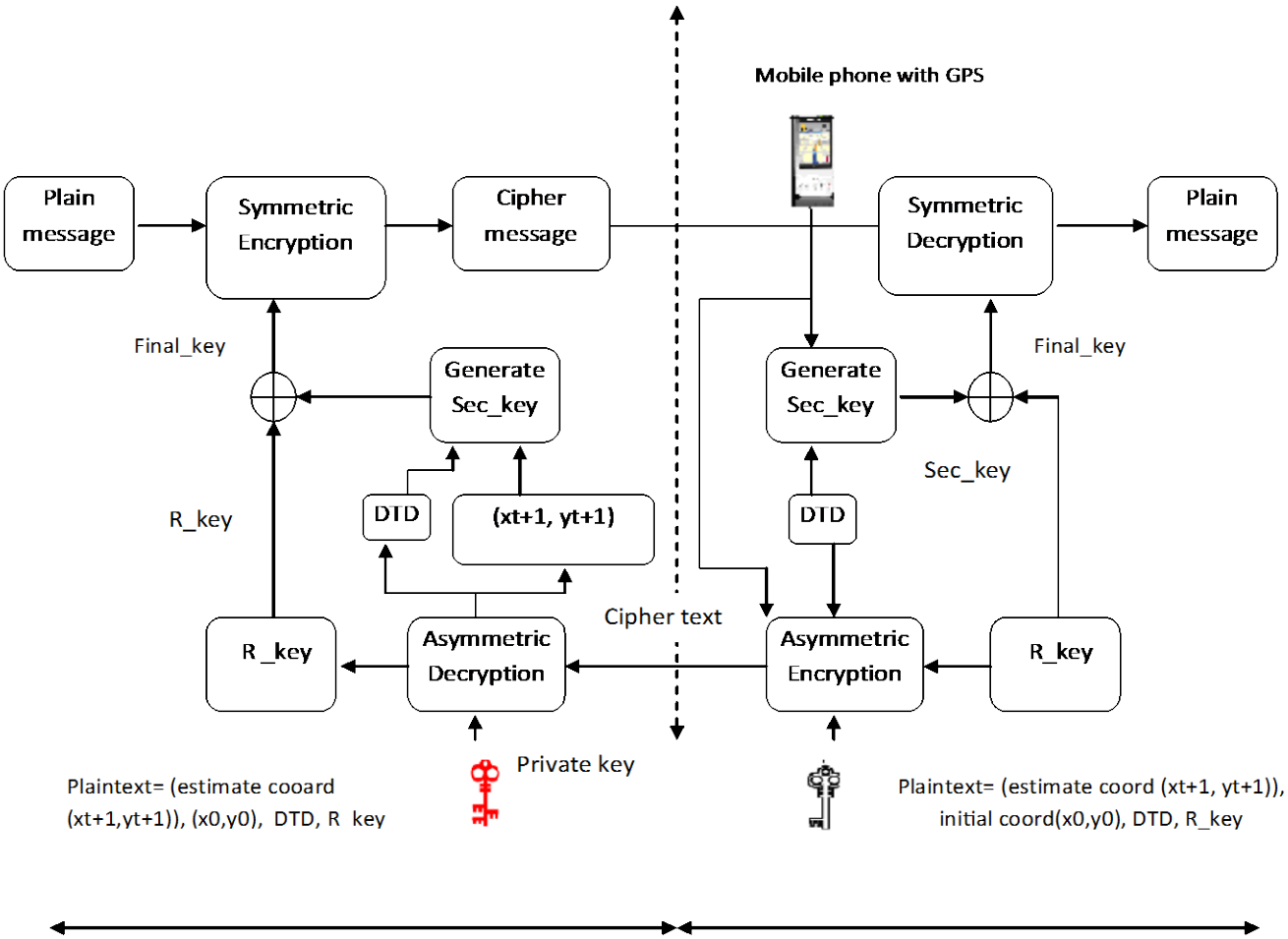


Figure 1. Generation process of secret key.

gets the final key through XOR between the Secret key and the R-key.

After that, the receiver mobile sends the parameter generated on the proposed algorithm and the R-key which are the plaintext given in the Fig. 1 to the sender using encrypted SMS by the public key through the asymmetric encryption. When the sender receives an encrypted SMS message, it decrypts using the private key. The sender generates the secret key using the decrypted parameter from the SMS and determines the final key whereas the XOR between the secret key and the R-key. This final key is used in the symmetric algorithm to encrypt the message sent from the sender to the receiver. The receiver decrypts the message using its final key in the symmetric decryption.

The generation of the secret key consists of the following parameters:

- The initial coordinate in the current location.
- Estimate coordinate, is the expected location at receiving time.
- Dynamic tolerance distance DTD.
- And, the R-key, is the random key.

To compute the estimated coordinate, the study of the path movement of the mobile phone must be studied. So, the mobile phone reads some coordinate during movement. It is supposed that the receiver mobile starts at time t0 at a location as its longitude and latitude values are L0(X0,Y0) which is the initial coordinate read in the path.

The mobile phone receives reading at time (t) is Lt (Xt,Yt) with t = t1, t2, t3, . . Such that ti = t0 + i*d. where d is a fixed time unit interval with arbitrary but known value.

The movement of the mobile device itself is arbitrary in any direction and any velocity means that its movement is not uniform.

The generation of secret key requires computing an estimated coordinate expected after a certain time. So, the next position of coordinate is given by the following equations according to the movement Law [Newton low]:

$$x\text{-}x_0 = v_x*t + (1/2)*a*t^2,$$

$$y\text{-}y_0 = v_y*t + (1/2)*a*t^2,$$

$$v_x\text{-} = v_{0x} *\cos\theta,$$

$$v_y\text{-} = v_{0y} *\sin\theta.$$

So,

$$x_i = x_{i-1} + (v*t + (1/2)*a*t^2)*\cos\theta, \quad (1)$$

$$y_i = y_{i-1} + (v*t + (1/2)*a*t^2)*\sin\theta, \quad (2)$$

where a is the acceleration and v is the velocity of the (x_{i-1},y_{i-1}) coordinate.

Generally, the path equation is a polynomial function given by:

$$(\Delta) :\{y(t)=a_n*x_n(t) + a_{n-1}*x_{n-1}(t) + \ldots a_1*x_1(t) + a_0 . \quad (3)$$

Each time, the mobile receiver reads the parameter "latitude, longitude and velocity", it does the following test:

A. If the value of velocity is not high

(v<100km/h), it means that the distance of the next coordinate is very short because the period time is constant. So, its movement is uniform which makes the function of path (Δ) in (3-3) linear (n=1)

$$(\Delta): \quad y(t) = a_1*x(t) + a_0 ,$$

But if the velocity is high, the path equation follows the size of coordinate belongs to the path equation (Δ).

If most of the general coordinates belongs to a path, the path equation is linear:

$$y(t) = a_1*x(t) + a_0 .$$

B. If the value of velocity is high (v⩾100km/h)

It finds a polynomial that fits these points. For simplification, we approximate this polynomial to be cubic function with third degree (n=3). After selecting the appropriate path, which depends on the nature of the movement, the estimate coordinate is determined by computing the next coordinate used in the secret key.

At time t=t+1 the algorithm estimates the next position using equation (1) and (3)

$$c_{t+1}=(x_{t+1},y_{t+1}),$$
$$\text{In} : x_{t+1} = x_0 + (v*t* + a*t^2)* \cos\theta.$$

θ is the angle between two coordinate as see in Fig. 3 given by:

$$\theta = \arctan\left(\frac{y_t - y_{t-1}}{x_t - x_{t-1}}\right) \quad (4)$$

If the location services in mobile phone read the speed, then the receiver mobile reads its velocity directly from the mobile device. But if the device has not this service, it is determined directly from the Low of Velocity. The velocity equation is given by the following equation:

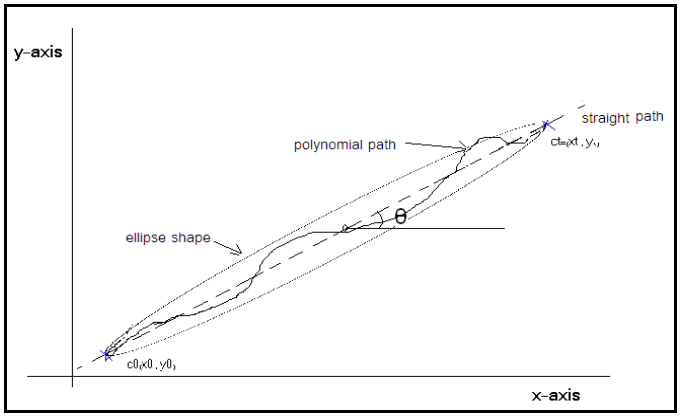


Figure 2. Ellipse Shaped in the Path Movement.

$$Velocity = Distance/Time,$$
$$\Delta\vec{r} = \vec{r}_i - \vec{r}_{i-1} = (x_i - x_{i-1})\vec{i} + (y_i - y_{i-1})\vec{j} .$$

The Distance r given by:

$$|\vec{r}| = \sqrt{(x_i - x_{i-1})^2 + (y_i - y_{i-1})^2} ,$$

Where "d" is a fixed time. So, the velocity v equals:

$$v = \frac{\sqrt{(x_i - x_{i-1})^2 + (y_i - y_{i-1})^2}}{d}, \quad (5)$$

Then, substituting the value of (x_{t+1}) in the path equation (Δ) of (3) gets (y_{t+1}).

In general, the path movement takes the ellipse form that is because the coordinate is distributed inside the ellipse form where the path function is changed through the change of speed. So, if the speed is not high or the path equation follows the size of coordinate belong to the path equation (Δ). The path function is linear. Then, some of this coordinate is arranged in a straight line but the rest of coordinate is arranged around the straight line. Also, if the speed is high the path function is polynomial and the coordinate is arranged in wide interval range. This coordinate in the two cases is distributed inside ellipse form Figure (2).

After calculating the estimate coordinate, it is applied to generate the secret key. This coordinate is multiplied by (10,000) to be an integer value because the mobile devise reads the coordinates as following example:

Latitude: 310 32’ 29, 31’’N

This latitude equals to N 3132.2931, (N) means the north.

Longitude: 340 29’ 27, 49” E

Xt = latitude* 10,000 = N 3132.2931* 10,000

Yt = longitude* 10,000 = E 3429.2749 *10,000

So, Xt = N 31322931 and Yt = E 34292749

From the estimation of CoordTrans tool of Franson Company, the values are (6) and (5.4) for latitude and longitude corresponding to 1 m [HIS 08]. This coordinate is converted to meter by dividing Xt into (6) and Yt into (5.4) to get xt = Xt /6 and yt = Yt /5.4

The second parameter is the dynamic tolerance distance (DTD). A dynamic Toleration Distance (DTD) is designed to increase its practicality in the interval used to encrypt or decrypt the data because the location service receiver has a problem in inaccuracy and inconsistent differs in the type of location service where the result of X_t and Y_t are divided by (DTD). DTD is the allowed region range in which the decrypted can done successfully where the DTD function is calculated as follows:

- the last coordinate that has been read in the path movement is taken as a center of the circle in which its radius is the length of the distance between this coordinate and the expected one. Therefore the DTD distance would be within the validate selected arc angle α which present a circle with the center is the estimated coordinate (x_e,y_e) and the radius is the DTD distance - as shown in Figure 3, DTD is the surface inside this circle. DTD distance= R_{DTD} is varying and depending on velocity and the angle α by the following equation:

  The length of distance

$$|\vec{r}| = \sqrt{(x_i - x_{i-1})^2 + (y_i - y_{i-1})^2}$$

$|\vec{r}|$ = v*t, because the movement is uniform

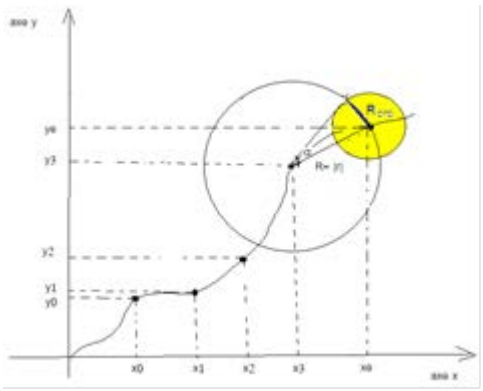


Figure 3. The dynamic tolerance distance (DTD) range

III. FINAL KEY GENERATION

1. The final key is generated by the exclusive OR operation (XOR) between the secret key and the R-key given in Figure (4).

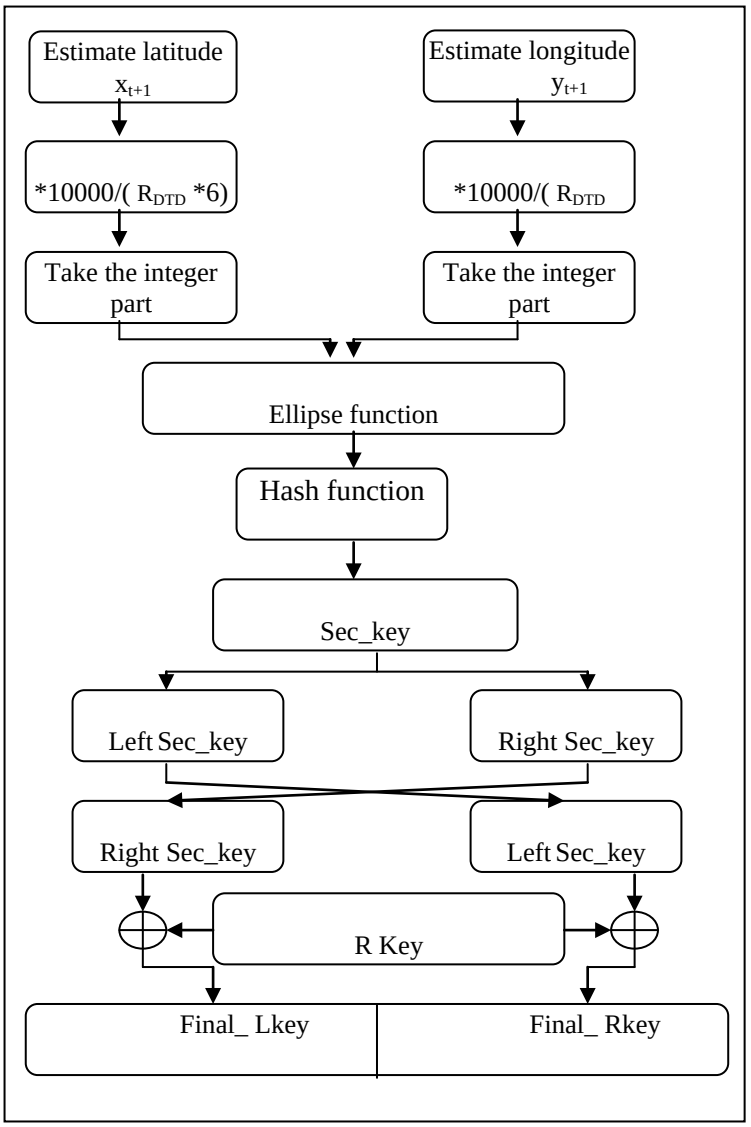


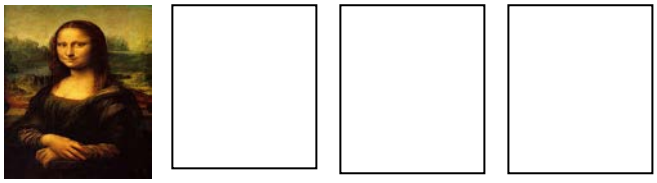
Figure 5. Generation of final key

IV. EXPERIMENTAL STUDY AND RESULT

Security Analysis:

A. *Key Sensitivity Test :*

- An original image in Figure5.a is encrypted by using the final key "ac963d95e449ea1cd409a3c34c8217c1 " (in hexadecimal) and the resultant ciphers are referred as encrypted image "cipher1' as shown in Figure5.b.
- The same original message is encrypted by making slight modification in the final key i.e."ac963d95e449ea1cd409a3c34c8217c2 "(the most significant bit is changed in the final key) and the resultant message is referred as encrypted image "cipher (2) " in Figure5.c.
- Again, the same original message is encrypted by making slight modification in the final key i.e."ad963d95e449ea1cd409a3c34c8217c1 " (the least significant bit is changed in the final key) and the resultant cipher is referred as encrypted image "cipher(3)" Figure5.d.



(a) Lisa (b) lisaEncr (c)lisaEncry (d) lisaEncry

Figure5. (a) plain-image (b) cipher1 (c) cipher2(d) cipher3

The results of the correlation coefficients between the corresponding message of the three encrypted images cipher(1),cipher(2) and cipher(3) are presented in Tables1.

TABLE I. CORRELATION COEFFICIENTS BETWEEN THE THREE DIFFERENT ENCRYPTED IMAGES OBTAINED BY USING SLIGHTLY DIFFERENT SECRET KEYS OF THE IMAGE SHOWN IN FIG. 7UL RATE VS. VELOCITY FOR STATIC AND DYNAMIC LOCATION

IMAGE 1	IMAGE 2	CORRELATION COEFFICIENT
Encrypted image cipher1 Fig. 7b	Encrypted image cipher2 Fig. 7c	0.0609
Encrypted image cipher1 Fig. 7b	Encrypted image cipher3 Fig. 7d	0.0625

It is clear from the tables that no correlation exists among the three encrypted images and texts and even though these have been produced by using slightly different final keys.

Key sensitivity analysis shows that changing one bit in encryption key will result in a completely different cipher message.

Moreover, and in Figure6, another experiment is conducted where attempt to decrypt an encrypted message with slightly different final key than the one used for the encryption of the original message.

Figure6. (a) Bandung-original image
(b) Encrypted image of (a)
(c) Decrypted image with the same final key of (b)
(d) Decrypted image with slightly different final key of (b)

B. Statistical Analysis:

- **Histograms analysis:**

In figure7 shows that the histogram of the cipher images is completely different in which has no any presence in data or effect compared by the original image and hence does not provide any clue to employ any statistical attack on the proposed encryption procedure.

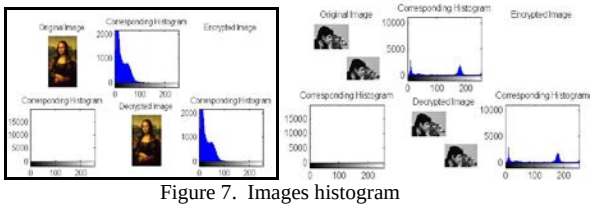


Figure 7. Images histogram

- **Corrélation Coefficient Analysis:**

The results are resumed in Table2 reveal that the correlation between the all (plain message and decryption Message) is equal to one. That means that the successful decryption operation with the proposed secret key.

From the results of this statistic analysis it demonstrates that the relation between secret encryption and cipher-data is of high complexity, and attacker cannot educe the encryption key from cipher- data.

Finally, the test on the histograms of the enciphered (decryption) data and on the correlations coefficient in the ciphered data showed that the proposed encryption algorithm is superior regarding the confusion and diffusion properties which strongly resist statistical attacks.

TABLE 2. CORRELATION COEFFICIENTS BETWEEN THE PLAIN MESSAGE AND CIPHER MESSAGE

PLAINIMAGE	ENCRYPTION IMAGE	CORRELATION COEFFICIENT
Cameraman	Cameramanencrypt	0.0698
Mona_liza	Monalizaencrypt	-0.0725
Bandung Image	Bandungencrypt	0.0390
plainText	cipherText	0.0540

- **Lossless and Opacity:**

Clearly from the above experiments' results, we can note that the use of AES Symmetric encryption was lossless, since the decrypted message is exactly similar to the original message without any loss of data through encryption and decryption operations, which means that there is no recorded noise in the decrypted images which makes the protection of data more strong. It can also be noted that the opacity between the original images and the encrypted images is very high. In other words, the distortion between the original and encrypted images as shown in the above experiments is very high.

- **Duration time:**

To measure the complexity of the proposed algorithm, the time in seconds for doing the encryption and decryption operations for the above experiments was recorded in Table 3.

TABLE3. ENCRYPTION/DECRYPTION SPEED TEST RESULTS OF THE PROPOSED ALGORITHM

	Size of data	Encryption Operation	Decryption Operation
Cameraman 804 x 553)	127KB	2.834000 s	2.664000 s
Monaliza (250 x 378)	20.4KB	1.373000 s	1.259000 s
Text	857B	0.8000 s	0.5000 s

V. CONCLUSION

this paper propose new key to solve the problem of attack through communication between mobile devise like the send of MMS and SMS message the proposed solution is a new security algorithm that uses a complex secret key to encrypt all type of messages transmitted between mobile phone. This secret key is generated from the dynamic coordinate, dynamic tolerance distance (DTD) and velocity of Mobile phone. In this algorithm, a mobile receiver with location service, register a set of

coordinates and velocity during movement and estimate the next position. The algorithm uses this new coordinate and the dynamic tolerance distance (DTD) to generate the secret key. This parameter and the type of movement made our system more secure than the existing solution, which depends only on the position of MN and the static tolerance distance or static location parameter.

The implementation of this algorithm is using J2ME software and it tested for different locations and speeds.

We have carried out key space analysis, statistical analysis, and key sensitivity analysis to demonstrate the security of the new message encryption procedure. According to the results of our security analysis, we conclude that the key is very strong Thus, it shows the strength of our algorithm and we expected to be useful for voice call encryption as future research.

REFERENCES

[1] Ali I. Gardezi, "Security In Wireless Cellular Networks," , 2006.
This paper is vailable online at
http://cse.wustl.edu/~jain/cse574-06/ftp/CellularSecurity/index.html

[2] Hatem H. and Elkourd S. , "Data Encryption using the Dynamic location and Speed of mobile node," Journal Media and Communication Studies , Vol. 2(3) , pp.067-075 , March, 2010.
Available online at http://www.academicjournals.org/jmcs

[3] Hsien-Chou L., Yun-Hsiang C., "A new data Encryption algorithm based on the location of Mobile users ," Information Technology Journal, Vol. 7, No. 1, 2008, p. 63-69.

[4] Ala Al-Fuqaha , Omar Al-Ibrahim, "Geo-encryption protocol for mobile networks," ELESEVIER Computer Communications. No. 30, 2007, p. 2510–2517.

[5] Scott,L & De Denning et al., "Using GPS to enhance data security GeoEncryption GPS world ," , 2003.

[6] Mundt ,TM, "location dependent digital rights management system," In proceeding the 10th IEEE symposition on computers and communication, 2005, p. 617–622.

[7] Liao et al., "A location-dependent data encryption approach for mobile information system," in the 9th international conference on Advanced communicate technology , 2007, p. 625-628 .

[8] P. S. Pandian, Omar Al-Ibrahim, "Wireless sensor network for wearable physiological monitoring," Journal of networks, VOL.3, NO. 5 , 2008.

[9] Richard Walton, "Cryptography and trust," information security technical report Vol. 11, NO. 68 –71 , 2006.