Journal Media and Communication Studies Vol. 2(3)pp. 067-075, March, 2010
Available online http://www.academicjournals.org/jmcs

Full Length Research Paper

Data encryption using the dynamic location and speed of mobile node

Hatem Hamad and Souhir Elkourd*

Islamic University of Gaza, Palestine.

Accepted 29 December, 2009

Due to the fast development in electronic technology, some mobile devices are designed for new services in important applications in life. In this paper, we propose a new method of message security by using the coordinates in GPS service, where it can specify the path of movement by taking some coordinates during travel of mobile node MN and estimate the following situation of MN in a constant time interval. This new estimated coordinate is applied in our secret key. Dynamic Toleration Distance (DTD) is also designed in our key to increase its practicality. The security analysis shows that the probability to break this key is almost impossible due to the security of coordinates and DTD, and adjusting the length of the Random key. Experimental study shows that the ciphertext can only be decrypted under the restriction of DTD. It illustrates that our secret key (Sec_key) is effective and practical for data transmission in mobile environment.

Key words: MN, GPS, DTD, sec_key, data encryption, data decryption.

INTRODUCTION

In today's world of cellular communication, in many environments wireless technology is the default access technology for a variety of services. Its ubiquity combined with the demands on mobility leads to the interesting research area of wireless roaming.

The cellular communication has become an important part of our daily life. Besides using cell phones for voice communication, we are now able to access the internet, conduct monetary transactions, send text, images or video messages etc, using our cell phones, and new services continue to be added. The wide use of mobile node services takes the problem for which makes the system vulnerable to attack and theft [Ali, 2006]. Although it is possible to provide security features such as authentication, integrity and confidentiality So security measures need to be upgraded continuously. What is secure today may not be secure tomorrow. There will always 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; therefore it has become difficult to develop a final solution to solve this problem.

In this paper we propose a new method of key security where the receiver MN register some coordinates and speed during the travel and thus can chart the course of movement. Through this path we can predict the next coordinate expected after a certain time since the GPS receiver is inaccurate and inconsistent depending on how many satellite signals are received [Hsien-Chou and Yun-Hsiang, 2008]. It is difficult for a receiver to decrypt the ciphertext at the same location which is exactly matched with the target coordinate. It is impractical by using the inaccurate GPS coordinate as a key for data encryption. Consequently, a Dynamic toleration distance (DTD) is designed in the secret key. The receiver MN determines the DTD and the sender can decrypt the ciphertext within the range of DTD.

On the other hand, extensive research has been done on data encryption for wireless networks and mobile node transmission, for example:

Hsien-Chou and Yun-Hsiang (2008), proposed a location data encryption algorithm LDEA. This protocol is not strong enough because they are using the static location which is latitude/longitude coordinate of mobile node and they are using a static Toleration distance (TD) to over-

*Corresponding author. E-mail: el_kourd@yahoo.com, hhamad@iugaza.edu.ps.

come the inaccuracy and inconsistence of GPS receiver. However, in our proposal we apply a dynamic location of mobile node and dynamic tolerance distance which makes our protocol very strong to attack.

Ala and Omar (2007) proposed a geo-encryption protocol by restricting the decryption of a message to a particular location and time period. The encryption of this protocol is limited to a static location and can not be used in dynamic location. Scott and Denning (2003), 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. However, the PVT-to-GeoLock mapping function is the primary mechanism to ensure that the data can be decrypted successfully. Vijayalakshmi and Palanivelu (2008) proposed a secure localization using elliptic curve cryptography in wireless sensor networks, where determining the physical positions of sensors is a fundamental and crucial problem in wireless sensor network operation. Their location based authentication scheme is built on the ID-based cryptography by using ECC and ECC key exchange.

Mundt (2005), proposed a location dependent digital rights management system. Location is essential for controlling access to resources protected by the digital rights. A trusted device which incorporates a precise secure clock and a GPS receiver is implemented.

Liao et al. (2007), proposed a static location-dependent data encryption approach for mobile information system. The approach is based on a reverse hashing principle. A series of session keys is generated based one-way hash function. They are generated for mobile client and server in a secure network simultaneously. When the mobile client is operated in an insecure network of the outdoor environment, the session key is incorporated with the GPS coordinate for ensuring the data is decrypted at the desired location.

Pandian (2008) proposed a wireless sensor network for wearable physiological monitoring systems which uses an array of sensors integrated into the fabric of the wearer to continuously acquire and transmit the physiological data to a remote monitoring station. Then the data is correlated to study the overall health status of the wearer. The use of physiological sensors with miniaturized electronics to condition, process, digitize and wireless transmission integrated into the single module is necessary. These sensors are strategically placed at various locations on the vest.

DETAILED DESCRIPTION OF THE PROTOCOL

In this protocol, the mobile receiver with GPS service, register a set of coordinates and velocity during movement and estimate the next position. This new coordinate is applied in the secret key with dynamic tolerance distance (DTD). DTD is designed to overcome the inaccuracy and inconsistent problem of GPS receiver and to increase its practicality. This protocol protect the message of type multimedia messaging service, or MMS, which is a standard way to send messages that include multimedia content to and from mobile phones. It extends the core SMS (short message service) capability which only allowed exchange of text messages up to 160 characters in length. The most popular use is to send photographs from camera-equipped handsets, although it is also popular as a method of delivering news and entertainment content including videos, pictures, text pages, sounds and speech through mobile connectivity.

The Path equations for MN movement

Suppose the receiver mobile node starts at time t_0 at a location whose longitude and latitude values are $L_0(X_0,Y_0)$, which are assumed to be initially known in the path , the mobile phone with GPS service readings $L_t(X_t,Y_t)$ at time t with $t = t_1, t_2, t_3, \ldots$ such that $t_i = t_0 + i*r$ where r is a fixed time unit interval whose value is arbitrary but known. The movement of node itself is arbitrary in any direction and any velocity. The next position is given by the following equations according to the law of speed:

$$xt = x0+ti*v*\cos\theta \quad (1)$$

$$yt = y0+ti*v*\sin\theta \quad (2)$$

Adding 1 to 2 we get;

$$x_t + y_t = x_0 + y_0 + t_i*v*(\cos\_+ \sin\_) \quad (3)$$

Where; v is the velocity of mobile node given by:

$$v = \sqrt{\left(\left(\frac{x_t - x_{t-1}}{r}\right)^2 + \left(\frac{y_t - y_{t-1}}{r}\right)^2\right)}$$

θ is the angle between two coordinate as seen in Figure 1 given by:

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

and the distance between two coordinate given by:

$$d = \sqrt{(x_t - x_{t-1}) + (y_t - y_{t-1})}$$

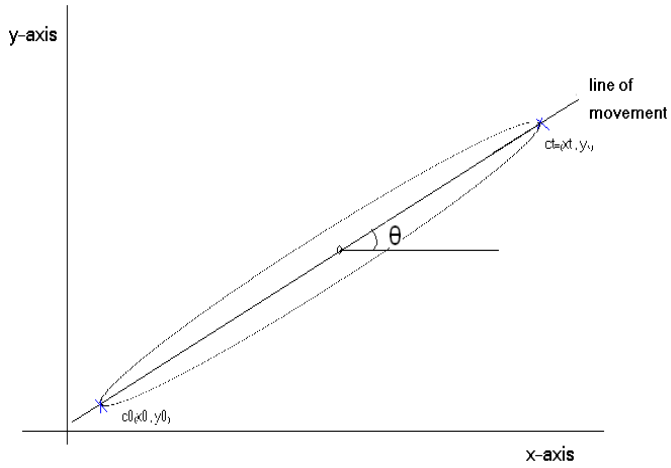

Figure 1. Distribution of coordinate in ellipse shape.

The path equation is:

$$(\Delta): \{y(t) = a_n * x_n(t) + a_{n-1} * x_{n-1}(t) + \ldots\ldots a_1 * x(t) + a_0 \quad (4)$$

Each time the GPS read this parameter "latitude, longitude, altitude and velocity" we do the following test in the program:

a. If the value of velocity is high (v ≥ 100 km/h), it means the distance of the next coordinate is very short because the time is constant, so this movement is uniform which make the function of path (Δ) in equation 4 linear (n = 1)

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

But if the velocity is not high, the path equation follow the size of coordinate belong to the path equation (Δ).
If most of the general coordinates belong to a path, so the path equation is linear:

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

b. If the value of velocity is less high (v < 100 km/s) we find a polynomial that fit this points, in general is probably a cubic function (n = 3).

The estimation of the next coordinate

At time t = t + 1, the algorithm estimate the next position $c_{t+1} = (x_{t+1}, y_{t+1})$
In: $x_{t+1} = x_0 + v*t*\cos\theta + a*t^2$ were a is a constant. Substituting the value of x_{t+1} in the path equation (Δ) of 4 we get y_{t+1}.

Dynamic tolerance distance

A dynamic toleration distance (DTD) is designed to increase its practicality in the interval of encrypt or de-crypt the data, because the GPS receiver have problem in inaccuracy and inconsistent. To calculate DTD we do the following step:

1. Replace the values of latitude into the path function (Δ).
2. Find the absolute values of the difference between the longitude values and the values in the previous step
3. Select the maximum value to be DTD.
4. DTD is multiplied by 10000 to be an integer and divided by 5.4.

*From the estimation of CoordTrans tool of Franson Company, the values are 5.4 and 6 for latitude and longitude corresponding to 1 m [Hsien-Chou and Yun-Hsiang, 2008], the mathematic equation of DTD are:

$y'_l = f(x_i)$, where $0 < l < t + 1$ and f is function of path.
$DTD = \max(|y_i - y'_i|) * 10000/5.4$ the result is in meter.

THE ALGORITHM OF PROTOCOL

Step 1. "The path equation"

Input $c_i(x_i.y_i)$,t0,r,v_i where $0 < i < n$.

Let $t_i = t_0 + i*r$.
$X_t = x_0 + v_i*t_i*\cos\theta$.
$y_t = y_0 + v_i*t_i*\sin\theta$.

So $x_t + y_t = x_0 + y_0 + v_i*t_i(\cos\theta + \sin\theta)$.

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

let $A = [a_1, a_2, \ldots a_n]$ is a set of all points.
$B = \{a_m \in A / a_m \in (\Delta)\}$, B is a set of points which lies on the curve (Δ).

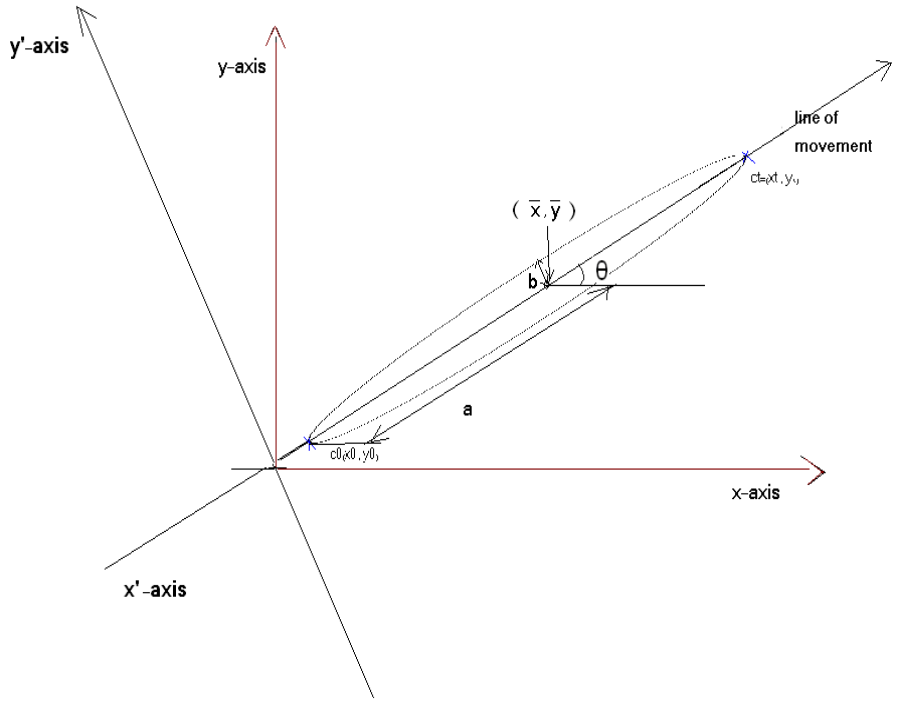

Figure 2. Moving the ellipse form in new axes.

If size(B) ≥ size(A)/2,
then f(A) = (Δ).
If v > 100 km/h , (Δ) = {y(t) = a*x(t)+a_0}.
Else (Δ) = {y(t) = a_n*x_n(t)+a_{n-1}*x_{n-1}(t)+…..+a_1*x(t)+a_0 }.
It is often that the path function is cubic.

Step 2. "The estimate coordinate"

For t = t_{i+1}
X_{t+1} = x_o+v*t_{i+1}*cosθ + a*t^2.
Y_{t+1}=(Δ(x_{t+1})).

Step 3. "The dynamic tolerance distance"

For c_i = (x_i, y_i), 0 < i < n.
DTD = (Max |y_i-f(x_i)|)*1000/5.4.

SECURITY ANALYSIS

In this section, we will show the generation of our proposed secret key. After the receiver mobile estimates the new coordinate and computes DTD, then sends it to the sender by using asymmetric encryption algorithm. This parameter is applied to encrypt the message sent by the sender.

Generation of secret key

Our purpose of secret key given in Figure 3 mainly includes the estimated coordinates and DTD that are computed in the last section. The steps to compute the secret key is as follows:

Transform estimate latitude/longitude coordinates

Enter the estimate coordinate (xt + 1, yt + 1), multiply the estimate latitude by (10000/Dtd*6) and the longitude by (10000/Dtd *5.4) to obtain the coordinate in meter and in the interval of encryption and decryption [Hsien-Chou and Yun-Hsiang, 2008].
The set of coordinates is generally included inside the ellipse shape that take (x0, y0) and (xt + 1, yt + 1) located on the perimeter of the ellipse as in Figure 1.

Ellipse function

From Figure 2, the new axes are given by;

x' = xcosθ - ysinθ.
y' = xsinθ +ycosθ (5)

The function of ellipse given by :

$$R(X,Y)=\left(\frac{x'-\bar{x}}{a}\right)^2+\left(\frac{y'-\bar{y}}{b}\right)^2=1 \quad (6)$$

Substitute (5) in (6) to get (7)

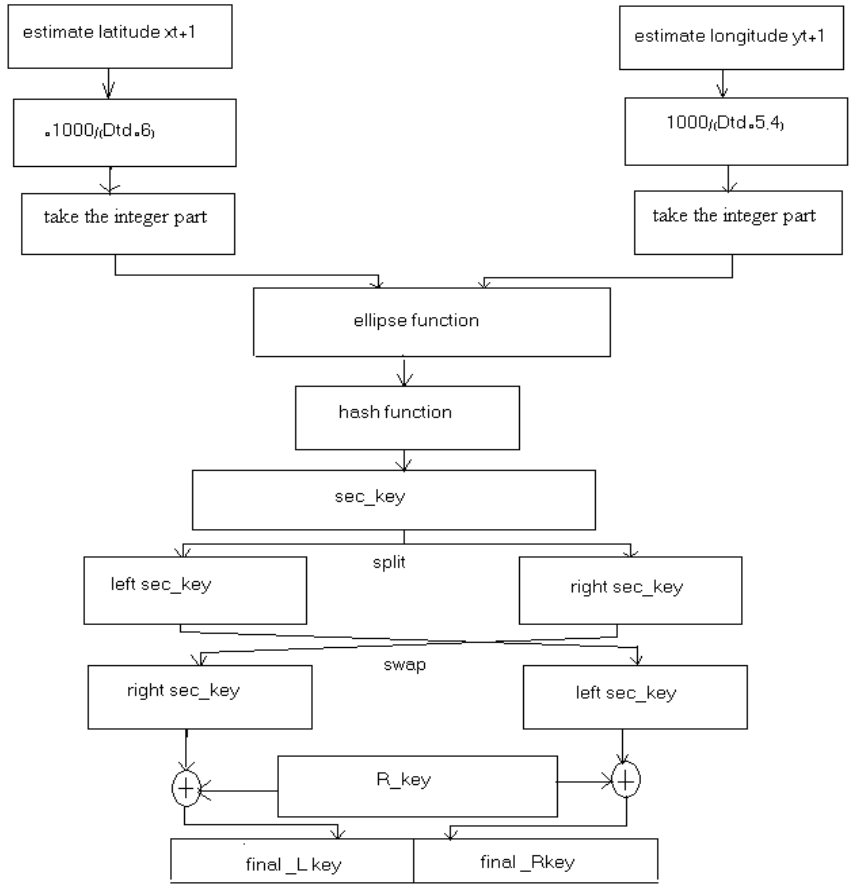

Figure 3. Procedure for final key generation.

$$R(X,Y)=\left(\frac{X*\cos\vartheta-y*\sin\vartheta-\bar{x}}{a}\right)^2+\left(\frac{x*\sin\vartheta+y*\cos\vartheta-\bar{y}}{b}\right)^2=1 \qquad (7)$$

Where;

$$a=\frac{(x_{\max}-x_{\min})}{2},\quad b=\frac{(y_{\max}-y_{\min})}{2},\quad \bar{x}=\frac{x_{t+1}}{2}\cos\theta,$$

$$\bar{y}=\frac{y_{t+1}}{2}\sin\theta,\quad \theta=\arctan\left(\frac{y_t-y_{t-1}}{x_t-x_{t-1}}\right).$$

Substituting the estimate coordinate (x_{t+1},y_{t+1}) in the ellipse function, then R(xt+1 , yt+1) = w, w is fractional number.

Hash function

This is a function that takes a variable length input and converts to a fixed length output, called hash value or hash digest [Ala and Omar, 2007]. Hash functions are relatively easy to compute but significantly harder to reverse. Beside one-way, the other important property of hash functions is collision-free: It is hard to generate two inputs with the same hash value [Richard, 2006].

The 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 then swapped to complicate the sec-keys. This step causes that the target coordinate is unable to be derived from the sec_key.

Final key

Using XOR function between the secret key left (secL_key) and the random key (R_key) with 128 bit, we get the final key left. Also Using XOR function between the secret key right (secR_key) and the random key (R_key) with 128 bit, we get the final key right, then we merge between this two key we get the final key.

Final_Lkey = R_key xor secL_key.
Final_Rkey = R_key xor secR_key.
Final _key = Final_Lkey and Final_Rkey.

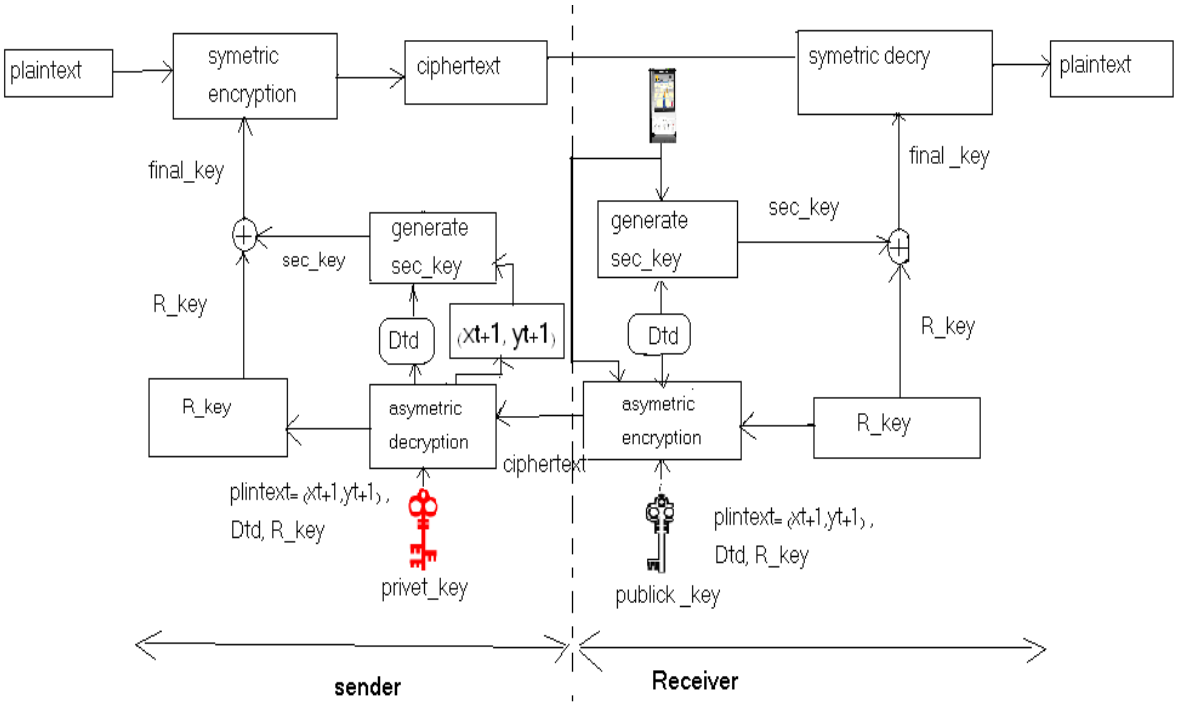

Figure 4. process of secret key.

The secret key process

The process of secret key is shown in Figure 4. When the estimated coordinate and DTD are given by the mobile receiver then a sec_key is generated from this data and the random-key generator, the final key is issued called R-key. Then, the final-key for encrypting the plaintext is generated by exclusive-or R-key with sec_key. The final-key can be used for the symmetric encrypt algorithm, such as DES, AES, triple-DES, etc. The asymmetric encryption algorithm is used to transmit the estimate coordinate, DTD, R_key and public key by the receiver to the sender which is applied to generate the final key where the public and the private keys are generated on the receiver side. This final key is used to encrypt the different type of messages lake audio, video, image, speech and text. If the acquired coordinate is matched with the estimate coordinate within the range of DTD, the ciphertext can be decrypted back to the original plaintext. Otherwise, the result is indiscriminate and meaningless.

When the sender receives this data, it sends the encrypted data to the receiver. The receiver decrypts the ciphertext using the data and sends it to the sender.

Strongest of key

The strongest of key depends on the dynamic path for the receiver MN and DTD. Therefore, the probability to break the secret key is impossible because no one knows the estimate coordinate since it is not yet at this position. Also DTD can be a fractional number with small interval which makes the key more secure. The random key is incorporated by the secret key which makes the final key very strong.

EXPERIMENTAL STUDY AND RESULTS

A prototype was implemented to illustrate and evaluate the practicality of sec_key algorithm. Simulation figures using j2me software are shown below.

The encryption part

The plain text is encrypted using the parameters sent in the asymmetric encryption in Figure 5a, the user chooses encrypt button to encrypt the plaintext. By typing next, the input information is shown in Figure 5b. After the Encrypt button is pressed in Figure 5c, the plaintext file is encrypted as shown in Figure 5d.

The Decryption part

The cipher text is decrypted using the parameter calculated in the algorithm. In Figure 5e, the user chooses the decryption option. After the decryption button is pressed the user detects the estimated coordinate and dynamic

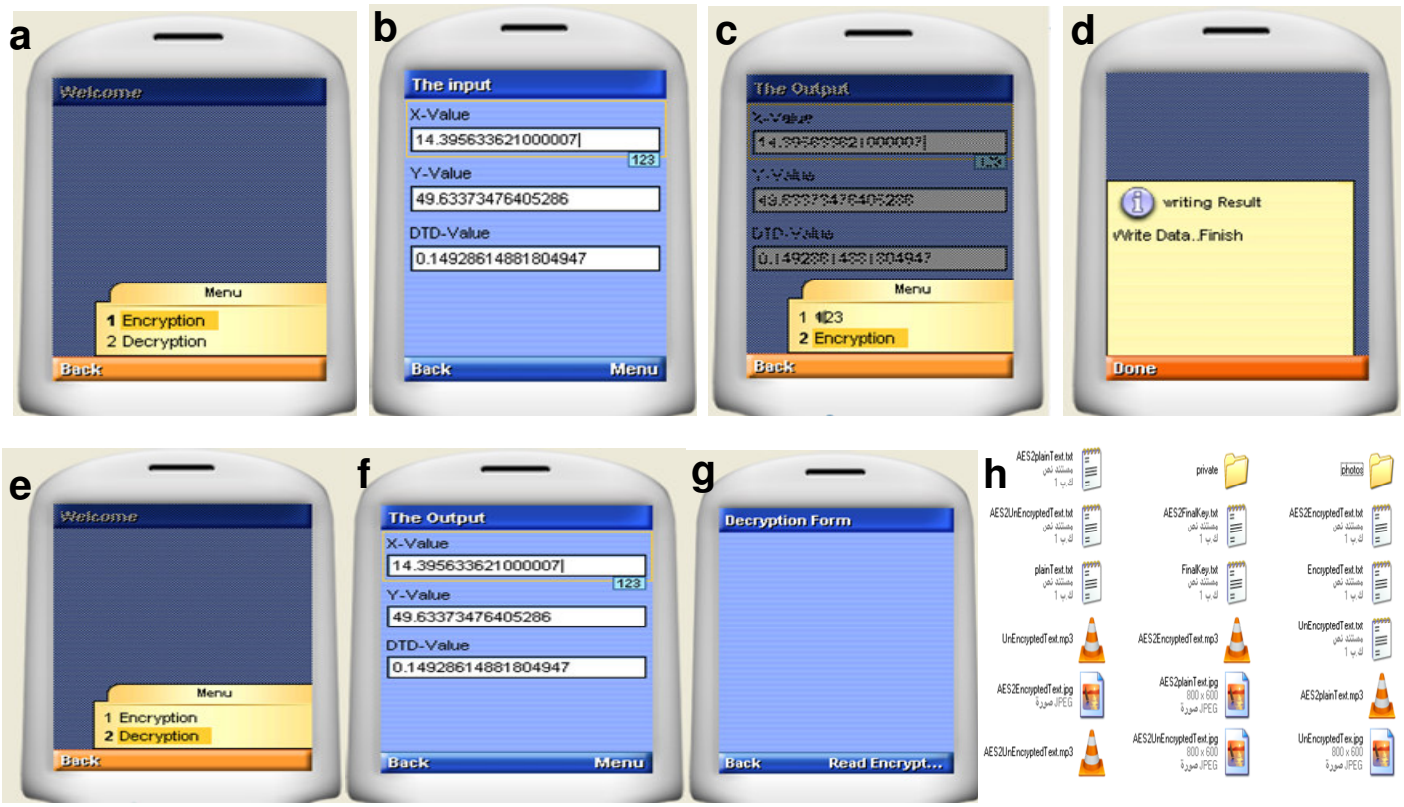

Figure 5. Simulation prototype to encrypt and decrypt different type of data.

dynamic toleration distance (DTD) as in Figure 5f; then by pressing the button next the ciphertext file decrypted as shown in Figure 5g. This means: "Open the folder to see the decryption file". If the acquired coordinate meets the constraint of target coordinate and DTD, the content of the decryption file is the same as the plaintext file which is saved in the folder as shown in Figure 5h. Otherwise, the content is indiscriminate and meaningless. We have implemented this protocol practically, where we have moved by car on the highway and streets of a subsidiary with different speeds. We studied the effectiveness of the secret key by taking the coordinates close to the estimated coordinates in the path. The analytical study of the movement path of the receiver MN can be summarized as follows:

If the receiver MN travels with high speed in constant time interval, the motion path is a linear function. At time t + 1 the expected point is located on the same straight line, so the DTD is very small and hence the success rate of decryption becomes approximately zero; but if it was moving slowly, the motion path is a polynomial function. Generally, it takes the form of cubic function and the region of DTD is higher. Therefore the difficulty of decryption decreases little bit but it remains more difficult than static method which take large range in distance and big value for static tolerance distance as in [Hsien-Chou and Yun-Hsiang, 2008; Ala and Omar, 2007; Scott and De Denning, 2003]. At last we conclude that the successful rate of decryption increases when the speed decreases and DTD increases. This difference is clear from the Figures 6 and 7. For velocity v > 100 km/h, the successful rate given in the Figure 6 demonstrate that the DTD generally take a value between 0 and 1, which means that the successful rate = 100% only if the distance is 0 m, but by increasing the distance, the successful rate decreases to become 0% for distance greater than 1 m. For velocity v < 100 km/h, the DTD varies with the form of path function. The value of DTD increases only if the path function is polynomial and decreases if it is linear. The successful rate given in Figure 7 demonstrates that by increasing DTD, the successful rate decreases which mean that the successful rate is 100% only if the distance is 0 m, but by increasing the distance the successful rate becomes 0%.

Conclusion

In this paper we have proposed a new algorithm for secret key to encryption message translated between mobile phone. This algorithm is very strong, since we use

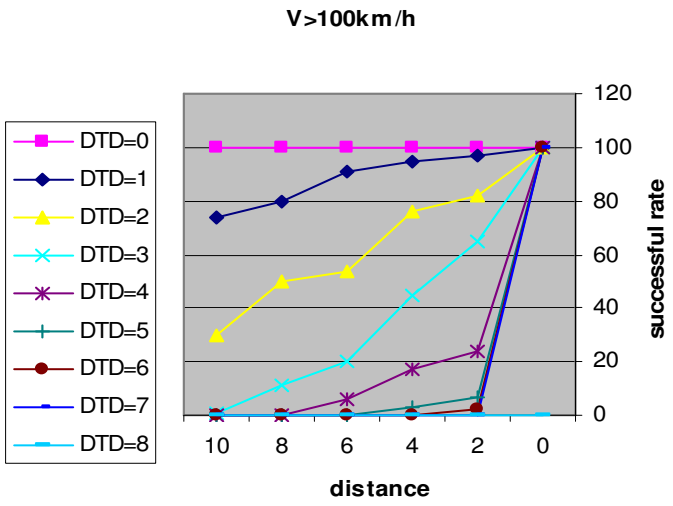

Figure 6. Successful rate vs. distance under various Dtd for v > 100 km/h.

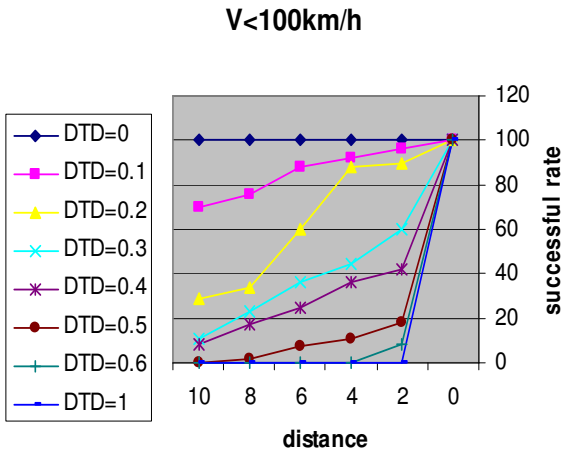

Figure 7. Successful rate vs. distance under various DTD for v < 100 km/h.

a function path that applies the estimate coordinate, we also use a dynamic tolerance distance (DTD), and velocity of MN. This parameter and the type of movement make our system more secure than the static encryption, which depends only about on a position of MN and static tolerance distance. The static location protocol is simple however, its performance varies with the mobility of the mobile. Specifically, if a MN is moving quickly, the error to detect region of encryption will be high. That means the successful rate of decryption is 0% even if the distance and static tolerance distance are equal to zero; if it is moving slowly, the error will be low and the successful rate of decryption augmented, but the dynamic location in this protocol will be more accurate. Thus, when the MN is moving fast, localization will be carried more precisely. When it moves slowly and the successful rate of decryption decreases in the two cases, but in high speed it gives better result then low speed as shown in our results

The results also show that the region of decryption is less because the range of DTD is small where the successful rate is probably narrow.

REFERENCES

Ala A, Omar A (2007) Geo-encryption protocol for mobile networks" ELESEVIER Computer Communications. 30: 2510-2517.

Ali IG (2006). Security In Wireless Cellular Networks" This paper is available online at http://cse.wustl.edu/~jain/cse574-06/ftp/CellularSecurity/index.html

Hsien-Chou L, Yun-Hsiang C (2008). A New Data Encryption Algorithm Based on the Location of Mobile Users ", Info. Tech. J. 7(1): 63-69.

Liao H, Lee P, Chao Y, Chen C (2007). "A location-dependent data encryption approach for mobile information system", in the 9th International Conference on ADVANCED Communicate Technology 1: 625-628.
Mundt TM (2005). "Location dependent digital rights management system", In proceeding the 10th IEEE symposition on computers and communication pp. 617-622.
Pandian PS(2008) " Wireless Sensor Network for Wearable Physiological Monitoring", J. Networks. 3: 5
Richard W (2006). "Cryptography and trust", information security technical report. 11(6): 8 – 71.
Scott L, Denning DE ((2003). Using GPS to enhance data security Geo-Encryption GPS world "
Vijayalakshmi V, Palanivelu TG (2008). "Secure Localization Using Elliptic Curve Cryptography in Wireless Sensor Networks ", IJCSNS Int. J. Comput. Sci. Network. Secur. 8: 6.