Military Technical College
Kobry El-Kobbah,
Cairo, Egypt

7th International Conference
on Electrical Engineering
ICEENG 2010

IMPROVED GEO-ENCREYPTION PROTOCOL FOR MOBILE NETWORKS

By

*A.S. Amin**   *K. El Batran+*

Abstract:

The wide spread of WLAN and the popularity of mobile devices increase the frequency of data transmission among mobile users. However, most of the data encryption technology is location-independent. Indeed, an encrypted data can be decrypted anywhere, however, The encryption technology cannot restrict the location of data decryption. Therefore, our objective is to add a layer of security to the network without breaking the network rules and to decrease network traffic. These aims can be achieved by two ways. First, when the receivers decrypt almost all the encrypted messages sent by senders. Second, when a decrease in the message queuing occurs. In order to meet the demand of mobile users in the future, a location-dependent approach is proposed in which target latitude/longitude coordinate must be determined. 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 is matched with the target coordinate.

1. Introduction:

The location-based encryption or geo-encryption refers to a method of encryption in which the encrypted information, ciphertext, can be decrypted merely at a specific location. It enables data to be encrypted for a specific place or broad geographic area and backs up constraints in time in addition to space and fully protects against any attempts to bypass the location feature. Any attempt to decrypt the data at any other location, the original plaintext information is not revealed due to the failure of the decryption process. A location sensor such as a GPS receiver is used to determine the location in order to encrypt and decrypt the data.

2. Improved Geo-Encryption Protocol:

There are many location-independent methods proposed for the security of data transmission in which the location of the receiver for data decryption could not be restricted by the sender. If the location is added to a data encryption algorithm, then this algorithm will be useful for increasing the security of mobile data transmission in the future. Therefore, an Improved Geo-Encryption Protocol (IGEP) was proposed. The latitude/longitude coordinate was used as the key for data encryption in IGEP. 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 GPS coordinate as key for data encryption. Consequently, a Toleration Distance is designed in IGEP. The sender can also determine the Toleration Distance and the receiver can decrypt the ciphertext within the range of Toleration Distance.

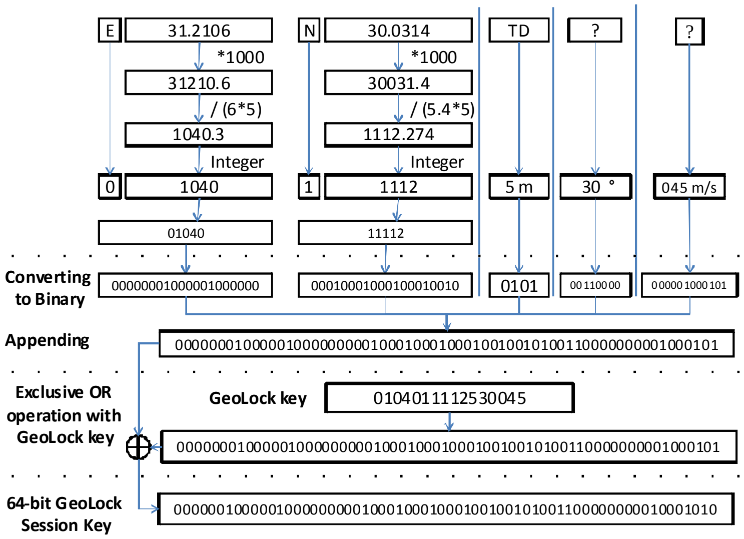
However, this approach presents potential problems: The resultant file reveals the physical location of the intended recipient. Furthermore, it provides vital information to someone who wants to spoof the device.

3. Protocol Overview:

Our Improvement builds on top of existing wireless multihop routing protocols, thus it will not address the routing issues of mobile multi-hop networks. A simplified version of the geo-encryption protocol was evaluated by simulating a modified DSR protocol using GlomoSim. Our Improvement will handle the communication of movement information between mobile nodes and the updating of this information whenever nodes move unexpectedly. One of its main goals is to enable mobile nodes to exchange their movement information accurately and to reduce the overhead on the network.

4. The IGEP proposed model:

A movement model based on the geo-encryption technique was proposed in which both sender and receiver are mobile. The intended movement of each mobile node that will be receiving geo-encrypted messages needs to be delivered to the potential sender nodes in order to estimate the mobile node’s expected location at any point in time. This comes by sending information regarding the mobile node’s movement, called movement parameters, to the sender through a sequence of message exchanges.



5. Simulation results:

First, the data was plotted for one of the files at our disposal and, after proper unit conversion, determined a 150 · 150 m area. The movements of nodes were selected within that area during a 15 min period.

And finally, from the remaining data, the 50 nodes with the most number of updates in the given period were selected as shown in figure 4. From that, an initial position file and movements file were created to include in our simulation file. In order to create several movement files with decreased mobility; the pause times 10, 25, 50, 75, 100, 200, 400, 650 and 900 s were included.

For each mobility file, three runs with 10, 20 and 30 senders with 10, 20 and 30 receivers respectively were simulated to record the decryption ratio, ratio of the successfully decrypted messages amongst those that were received, and the protocol overhead.

The protocol overhead for position updates was measured by the ratio of position update messages to the total number of data messages, decrypted or not that were received.

Both Decryption Ratio and Protocol Overhead of IGEP (TD 2.5) will be measured using different Network Size (10, 20 and 30 senders with 10, 20 and 30 receivers respectively) and compared to GEP (TD 10). Decryption Ratio is measured as the ratio of successfully decrypted messages among those that were received for 10, 20 and 30 senders with 10, 20 and 30 receivers respectively for the IGEP (TD 2.5) and GEP (TD 10) algorithms. Comparing the two values of Tolerance Distance 2.5 and 10 with fixed number of 10 senders and receivers, it was noticed that when Tolerance Distance value was 2.5, the Decryption ratio was approximately 96%, while at the value of 10, the

Decryption ratio was approximately 95.5%. Accordingly, as mobility decreased, the Decryption ratio recorded approximately 98% for the two values of Tolerance Distance. Protocol overhead for position update is the ratio of position update messages to the total number of data messages - decrypted or not - that were received for 10, 20 and 30 senders with 10, 20 and 30 receivers respectively for the IGEP (TD 2.5) and GEP (TD 10) algorithms.

6. Breif Result analysis:

As using 10 senders and 10 receivers, for IGEP (TD 2.5), the Decryption Ratio was approximately 97% and Protocol overhead was approximately 5.81%, while GEP (TD 10), the Decryption Ratio was approximately 95.8% and Protocol overhead was approximately 6.57%. Moreover, as number of senders and receivers increases to 20, for IGEP (TD 2.5), the Decryption Ratio was approximately 95.35% and Protocol overhead was approximately 7.23%, while GEP (TD 10), the Decryption Ratio was approximately 94.71% and Protocol overhead was approximately 8.44%. In addition, as users increase to 30, for IGEP (TD 2.5), the Decryption Ratio was approximately 93.6% and Protocol overhead was approximately 9.38%, while GEP (TD 10), the Decryption Ratio was approximately 93% and Protocol overhead was approximately 9.41% as shown in table 1.

Table (1): *Different Network Size and Fixed Tolerance Distance*

senders and receivers	**IGEP (TD 2.5) algorithm**			**GEP (TD 10) algorithm**		
	10	20	30	10	20	30
Decryption Ratio	97%	95.35%	93.6%	95.8%	94.71%	93%
Protocol overhead	5.81%	7.23%	9.38%	6.57%	8.44%	9.41%

As using fixed Network Size (10 senders and 10 receivers), the IGEP (TD 2.5) algorithm of Tolerance Distance 2.5 comes in the first place with Decryption Ratio approximately 96% and Protocol overhead approximately 8%. While GEP (TD 10) algorithm of Tolerance Distance 10 comes in second place with Decryption Ratio approximately 95.5% and Protocol overhead approximately 8.9%. In the last place comes the GEP (TD 3) algorithm of Tolerance Distance 3, the Decryption Ratio approximately 93.5% and Protocol overhead approximately 16 as shown in table 2.

***Table (2)**: Different Tolerance Distance and Fixed Network Size*

Tolerance Distance	2.5	3	10
Decryption Ratio	96%	93. 5%	95.5%
Protocol overhead	8%	16%	8.9%

After the manifestation of the results, it is proved that, IGEP (TD 2.5) algorithm was better than GEP (TD 10) algorithm concerning the Decryption Ratio and Protocol Overhead. In addition to the results, there is another perspective which is; when the Tolerance Distance is set to 2.5 m, it covers the inaccuracy of the data exported from the GPS receiver. By increasing the Tolerance Distance to 3 m, that means that the inaccuracy problem will be solved using 2.5 m and there is a range of 0.5 m round the node in order to decrypt the messages. That seems to be not proper range to decrypt the messages. By increasing the Tolerance Distance to 10 m, that means that the inaccuracy problem will be solved using a range of 7.5 m round the node for decryption. Subsequently, that results a better value from 3 m for the Tolerance Distance, but still not better than 2.5 m. Eventually, by mentioning the privileges of IGEP (TD 2.5), that reinforces its superiority, and asserts the improvement that was added to Geo-Encryption algorithms.

References:

[1] *Jay A. Farrell, Aided Navigation: GPS with High Rate Sensors, First Edition, McGraw-Hill Professional, 2008.*

[2] *Stephen W. Hinch, Outdoor Navigation with GPS, First Edition, Wilderness Press, 2007.*

[3] *William Stallings, Network security essentials: applications and standards, Third Edition, Prentice Hall 2007.*

[4] *William Stallings, Cryptography and Network Security: Principles and Practice, Fourth Edition, Prentice Hall 2006.*

[5] *L. Scott and D. Denning, "Geo-encryption: Using GPS to Enhance Data Security", GPS World, 2003.*

[6] *Ala Al Fuqaha and Omar Al-Ibrahim, "Geo-encryption Protocol for mobile networks", Journal of Computer Communications , Vol. 30, No. 11-12, pp. 2510-2517, September 2007.*