GPS CHARACTERIZATION IN CYBERSPACE BETWEEN VULNERABILITY AND GEO-ENCRYPTION: IMPACT ON GBAS LANDING SYSTEM (GLS)

Ahmad ALHOSBAN
National University of Public Service, Budapest, Hungary
ahmad_alhosban@yahoo.com

ABSTRACT

In the cyberterrorism concept, whoever was the type of terrorist group: Religious, Ethno-nationalist separatist, Revolutionary, and Far-right extremist, the most efficient deterrence solution locates in the end-user's protection and hardening. In the cyberterrorism activities, either disruptive and/or destructive, people tend to be the softest link in security chain. Therefore, the threat source would be less important compared with the way of protection. Many efforts have been performed in strengthening the far-end-recipients' infrastructure of communications and critical information systems. Amongst, is the Geo-Encryption Cryptographic Algorithm. It depends on adding a new layer of security by using the most vulnerable signals to cyber-attacks, which is the GPS signals. Hence, its strength came out from its weakness. The Geo-encryption technique assumes the use of anti-jam and anti-spoof GPS receivers, which without, the model would be of no added value to the end-users' security. In this study, an assessment of the model performance among vulnerability challenges is conducted, showing the characterization of the GPS tool in such model being a solution while it is simultaneously a vulnerable target. A special focus was put in the GBAS Landing System (GLS) performance, in both military and civilian aviation aspect.

KEYWORDS: cyberterrorism, Geo-Encryption, Global Positioning System (GPS), GBAS Landing System (GLS)

1. Introduction

Obviously, since the September 11, terrorist attacks against the internet and servers' data base have increased, their tools took another path of the means' curve to achieve their ends and goals. Although the fact they have different levels of skills of hacking and computer knowledge, they were likely able to attack and growing their use of the Internet as a digital battleground. As per Denning (2001), one of the main man-made cyberspaces is the aviation aspect, evidenced by the September 11 event. From which, it is clear that the aircrafts hijacking is possible anywhere and anytime. However, many data and voice messages transfer from the ground controllers to the aircrafts' computers and pilots, could be attacked. Consequently, vast of encryption techniques have been developed using many Advanced Encryption Standards (AES) codes' generation process,

DOI: 10.2478/raft-2020-0018

most focused in this article is the Denning Geo-Located Model (Denning & Scott, 2003).

The Geo-encryption or the Geo-Located model is bases on established cryptographic algorithms to provide an additional layer of security. This added layer is enhancing the conventional cryptography, but not replacing it. It enables data encryption for a predefined place or a given geographic area in time and space. If an adversary, attempts to decrypt the data at different location or time, the decryption process would fail. The decryption device determines its location using some kind of location sensors like a GPS receiver or any positioning system. In all the process, it assumed the use of anti-jam and the anti-spoof receivers.

Following the innovation of this model, many researchers had developed a new enhancing approaches and added features to its original performance. However, all of the previous studies were assuming the same basic hypothesis of using of anti-spoof receivers. Amongst the previous studies in Geo-encryption model, the most relevant study to this article is the (Geo-Encryption Protocol for Mobile Networks) model, which was proposed by (Al-Fuqaha, Al-Ibrahim & Rayes, 2007). Basically, the researchers claimed that they have not identified the characterization of mobility in Denning's geo-encryption model, therefore they proposed a model for mobility when using GPS receiver encryption. Simply their proposed model characterised the mobility in certain parameters within an ellipse shaped receiving area. However, their results showed low efficiency in mobile encryption process, there was decryption decreasing with the increase in mobility, and also there was a decrease in decryption ratio with the increasing of the network traffic due to increasing in message queuing-delay. Furthermore, their future recommended improvements of this model was the using of the next predicted position of the sender or the receiver based on the history of mobility parameters such as the velocity and direction to be sent by the receiver to the sender.

In this article, the objectives are to assess the implementation of the geo-encryption (Denning et al., 2003) Model or the Mobile (Al-Fuqaha et al., 2007) Model in the approaching high-speed landing aircraft using GLS. In addition, to examine to which extent the GPS signal is immune against spoofing/jamming to be used as geo-encryption aiding, especially in final approach path.

2. Assessment of the Geo-Encryption Algorithm: Prospects and Implications

Basically, the proposed algorithm of the (Denning, 2003) Geo-Encryption, or so called the Geo-Codex Geo-Encryption algorithm, addresses new protocols. Referring to Figure no. 1 below, the approach modifies the hybrid (symmetric and asymmetric) algorithm to impose the Geo-Lock. On the encrypting side, a Geo-Lock is added based on the receiver's location, Velocity, and Time (PVT) block. This PVT block determine where the recipient has to be in terms of position, velocity & time for the successful decryption. Then after, the Geo-Lock uses the XOR logic gate with the session key (Key_S) to compute a Geo-Locked session key. The result is being encrypted using an asymmetric algorithm and transferred to the receiver.

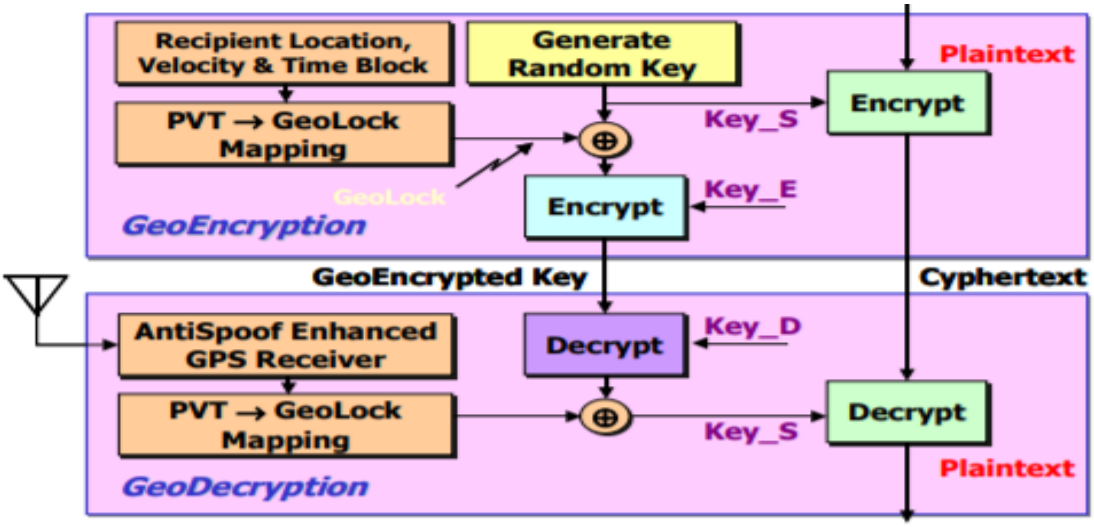


Figure no. 1: *The Geo-Codex Geo-Encryption algorithm*
(Source: Denning, 2003)

In this section of the study, the Geo-encryption concept is assessed by examining two important factors: (1) the mobility of such cryptographic especially in flight mode, and (2) the vulnerability of the GPS coordinates used as keys in terms of Continuity of Service (CoS) and accuracy.

2.1. The Successive Geo-Lock Function of a Predefined Rout While in Mobility

Basically, and as per definition in Denning (2003), the PVT-geo-lock function is a function of Position (Lat/Long), Velocity, and Time of each used key at a given time of usage, so it can be interpreted by the following equation:

$$PVT\text{-}Geo\text{-}Lock = \int(Position(Lat./Long.), Velocity, Time) \quad (1)$$

It can be represented/mapped as shown in Figure no. 2 below:

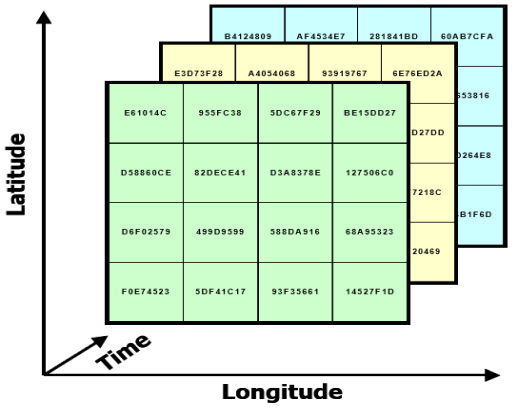


Figure no. 2: *The PVT geo-lock mapping*
(Source: Denning, 2003)

Therefore, and while in mobility, the geo-lock concept changes little, a successive Geo-encryption can be used to force data and/or keys to follow a predefined geographical path before it can be decrypted. It can be achieved by using multiple geo-locks at the originating node prior to transmitting. As each required node is traversed, one more Geo-locking layer is removed, so ensuring that the desired path has been followed. Therefore, supposing that we have a route of three successive predefined waypoints L1, L2, L3, then the

geo lock equation of each waypoint would be as follows:

L1= (RK), L2=L1(RK), and L3=L2(L1(RK)) (2)

And the full route can be geo-encrypted as shown in left panel of Figure no. 3, and decrypted and authenticated as shown in the right panel of Figure no. 3 below:

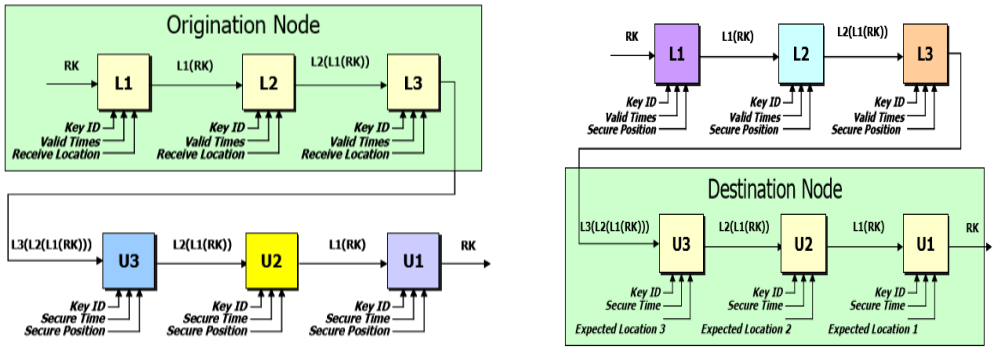


Figure no. 3: *The successive PVT geo-lock waypoints: encrypted (left panel), decrypted (right panel)* (Source: Denning, 2003)

The shown waypoints, as per the Denning (2003) Model, does not mean to be a single point only, it may include the surrounding points as well. Hence, when applying this concept on a real route or a path, as seen in (left panel) of Figure no. 4 below, there is no requirement that the PVT-Geo-Lock mapping be built on a regular grid, therefore, hence, polygonal shapes were chosen according to mission needs. Also, the Geo-Lock regions can be overlapped; they should not be geographically isolated from each other. Furthermore, time and velocity tolerance requirements could also be included. Also an extra refinement, a "keep waypoints" safe region could be specified. On the other hand, more focus of the shape of waypoint area was illustrated by (Al-Fuqaha et al., 2007), trying to reach a proper model of its four parameters; the four mobility parameters of an ellipse zone shape are: velocity (v), direction (θ), speed maneuverability (y-axis β), and breadth maneuverability (x-axis α) as shown in the (right panel) of Figure no. 4 below.

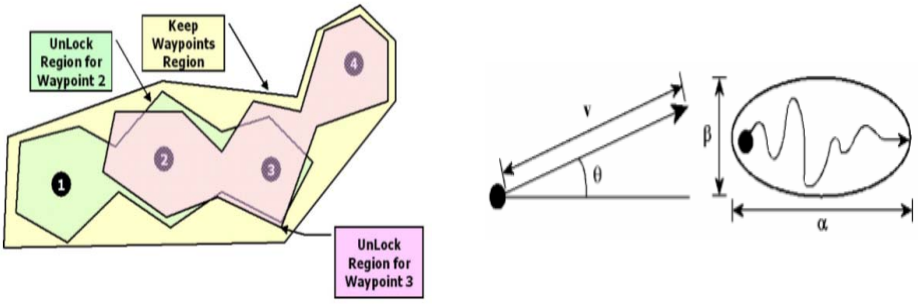


Figure no. 4: *The successive PVT geo-lock waypoints to secure the information in a predefined route of polygon shape, (left panel) (Denning 2003) model, Diagram illustrating the four mobility parameters of an ellipse zone shape: velocity* ***(v)****, direction* ***(θ)****, speed manoeuvrability* ***(y-axis β)****, and breadth manoeuvrability* ***(x-axis α)****, (right panel) model* (Source: Al-Fuqaha et al., 2007)

By examining both models shown above, the mobility concept has not seen fully described nor characterised, for example, in the (Denning, 2003) model, the sender is stationary while the receiver is moving in a discreet waypoints path within some predefined decryption areas surrounded by an extra safe zones that couldn't be exceeded, in where the receiver should receive the PVT geo-lock to decrypt the added layer of security. On the other hand, in (Al-Fuqaha et al., 2007) model, the sender should have a pre-knowledge of the location, velocity and time of all the moving nodes through a "movement update message", this message is intended to be sent back to the sender whenever and wherever it exceeds the predefined tolerances in the sender pre-set map, which is not the possible case in flight encryption methods, where it should be one-way encryption algorithm from the sender to the receiver as per described in Denning (2003) Model.

2.1.1. Results

However, the results of this part can be concluded as follows in both models:

1. The mobility concept hasn't been seen fully characterised in Denning Model of Geo-encryption, but it is an added significant value for the stationary senders and receivers, more or less, can be applied in a well-defined decryption zones discretely and not in continuous moving objects especially in high speeds.

2. The mobility concept in (Al-Faquha et al., 2007) Model of Geo-encryption was characterised deeper, but in the slow moving objects (buses in crowded areas), it was interpreted from their results that the decryption ratio decreases with an increasing in mobility. it is due to the fact that higher mobility means that the nodes are moving far away from their perceived locations at the originating nodes, as a result, more encrypted messages are not being decrypted. Also, the overhead decreases with the increasing of stop times. This behaviour is kind of a reactive to the mobility, hence, if there is no mobility then there is no requirement for updates.

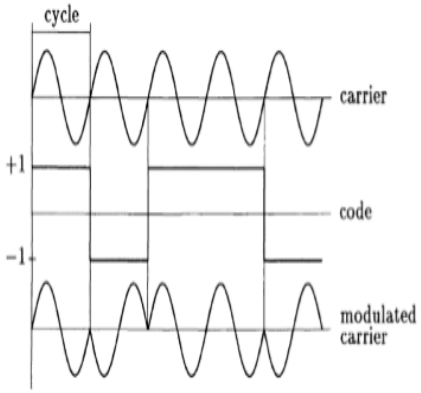
2.2. The Vulnerability of GPS Using the Geo-Encryption while Using the (C/A) Code

In general, the Coarse/Acquisition or (Clear/Access) code, abbreviated as the (C/A-code) in GPS is considered a vulnerable signal, the real vulnerability in not only the well-known locating criteria, but it is also that the GPS signals are weak and not immune enough to resist the higher power of any potential cyber electronic attacks. Actually, the GPS signals tend to have an extremely low level of power density; because satellites' transponders are orbiting almost far as (22,000 Km) above the ground surface, and they transmit the signals through the layers of Troposphere and Ionosphere, hence, the signals reach to users on the earth surface in a very low (signal to noise ratio), it is around (-160dBw for GPS L1, -154dBw for GPS L2 (Military)), and it is speculated to be around -155dBw for Galileo E1/E2. The other part of the vulnerability is the low capability of services' restoring on the proper time. It is not likely the system rescues its service in the allowed time when it gets disrupted. This may cause a high risk in the safety-of-life applications such GLS. However, the GLS reference stations are usually located in a well-surveyed reference positions near the runways, that makes them more vulnerable to the electronic-attacks than the portable or mobile GPS receivers. Full detailed technical data are available in (Alhosban, 2019) published paper and (Hofmann, Lichtenberger & Collins, 2001) book.

2.2.1. GPS's Signal Structure

According to Hofmann, Lichtenberger and Collins (2001), at the satellite space vehicle in the space, the GPS signal consists of three components: Two Carrier

frequencies (L1 and L2), two Codes and the navigation message; The two fundamental frequencies (f_o) are defined by a pseudorandom noise (PRN) sequence as shown in Figure no. 5 below. Secondly, the two codes are: the C/A-code and the P/Y Code; the C/A code uses one tenth of the fundamental frequency ***(f_o/10)*** and repeated every 1ms, these codes are not classified, hence they are available to civilians, and less immune to jamming. On the other hand, the precision code (P-code) uses the full fundamental frequency (f_o) and repeated once every 266,4 days, therefore it is hard to be attacked. Although the P-code is not classified, but it is encrypted to the Y-code by Anti Spoofing (AS). Moreover, the Y-code is the summation of the P-code and the encrypting W-code, that's make the access to the P-code only possible when the secret conversion keys are known, hence, its immunity against jamming is better than the C/A code one. Finally, the navigation message, which contains PVT data, is coded using 1500 bits at the sub-frequency value of 50 Hz, and it is transmitted within 30 seconds.



Component	Frequency (MHz)		
Fundamental frequency	f_0	= 10.23	
Carrier L1	154 f_0	= 1 575.42	(≙19.0 cm)
Carrier L2	120 f_0	= 1 227.60	(≙24.4 cm)
P-code	f_0	= 10.23	
C/A-code	$f_0/10$	= 1.023	
W-code	$f_0/20$	= 0.5115	
Navigation message	$f_0/204\,600$	$= 50 \cdot 10^{-6}$	

Figure no. 5: *GPS coding structure (left panel), GPS Signal components (right panel)* (Source: Hofmann et al., 2001)

At the receiving side, where the ground segment (GLS or the Aircraft receiver), the three transmitted components of the GPS signal (the carrier, the code and the navigation message) are recovered in a reversely sequence, they firstly demodulated to get the codes and the navigation message out from the carrier frequency, and then the useful information PVT of in the navigation message is decoded using decoding algorithms and the code correlation techniques. There are many code correlation techniques Such as: The Cross correlation technique, the Narrow Code Correlation, the Wide Code correlation, the squaring technique, the Code correlation plus squaring technique, and finally the Z-tracking technique. Their efficiency performance is a function time and precision; but the Z-tracking is the most efficient technique amongst them.

The information acquisition is achieved by two methods: The code pseudorange or the phase pseudorange. When using the code pseudorange acquisition method, the position accuracy of 3m (C/A-code) and 0.3m (P-code) can be achieved. But when using the Phase pseudorange acquisition method, a few millimetres precision can be measured. That means the more secured and coded signals the more accurate as well. But they are dedicated to military used only. However, the modernized signal structure in both Galileo and the GPS Block III will hopefully add another security value by the receiver-based mitigation methods.

2.2.2. Characterization of GPS Jamming Model

In general, and according to Adamy (2009), the jamming model of the jamming to signal ratio for GPS/GLS down links, is given by the equation (3) below, and it is modified by this study accordingly to fit the GLS situation as per explained next to each of parameter below:

J/S = ERPj – ERPs – Lj + Ls + GRj – GR (3)

Where:

J/S(dB): is the jammer to the wanted signal power ratio, in GLS the power received from satellite transponder at the input of the antenna of the receiver where it is being jammed by a jammer power most likely higher.

ERPj (dBm): the effective radiated power of the jammer, most likely higher attack power.

ERPs (dBm): the effective radiated power of the wanted satellite transponder signal.

Lj (dBi): the propagation loss during the distance between the jammer position to the targeted receiving position, which is stationary in GLS and Mobile in On-board.

Ls (dBi): during the distance between the satellite vehicle position to the targeted receiving position, which is stationary in GLS and Mobile in On-board.

GRj (dBi): the gain of the receiving antenna of the GLS or the on-board antennas toward jammer direction.

GR (dBi): the gain of the receiving antenna of the GLS or the on-board antennas toward space.

2.2.3. Examples of the GPS's Jamming Cyber-attacks

The cyber-attacks threats could be either professionally and intentionally used, utilizing an expensive, complicated and higher-power jammer, such as the military-grade jammers. Or it can be unprofessionally unintentionally occurred. Many cyber-attacks were observed and had been reported by ICAO and FAA. More details in this subject can be found in the published papers (Alhosban, 2019; 2020). However, here are the two most important of them:

1. In Nov 2018 and during the military joint-exercise of NATO forces in both Finland and Norway, there was collateral damage due to a navigation malfunction led to a collision of a frigate with a tanker. The USA defence officially announced that the jamming had "little or no affect" on their military assets. More details are available in Seidel (2018). However, it can be interpreted here that the said "little or no effect" is most likely due to the using of the military P-code by the US forces, which is classified and not distributed to the other allied forces participating in the exercise. And as per mentioned above, the P-code is much more immune against jamming in terms of coding algorithm. Refer to Figure no. 6 below, it was obvious to have a huge tendency to be a cyber-activity by anonymous party.

Figure no. 6: *The Norwegian frigate "KNM Helge Ingstad" suffered a navigation malfunction leading to a collision with the "Sola TS" tanker on the 8th of Nov, 2018 in the Hjeltefjord nearby Bergen* (Source: AFP)

2. During the period between August 2010 and May 2013, there were many disturbances due to a certain kind of cyber-attacks experienced in South Korea and

Ukraine: In South Korea, it was suspected that a deliberating Military-effect jammer from North Korea had influenced the GPS equipment's in many military aircrafts and ships. In Ukraine, the Organization for Security and Cooperation in Europe (OSCE) reported a military-grade GPS jamming on their UAVs missions, more details can be found in (Pullen & Gao, 2012). It can be interpreted that adversary can use anytime and anywhere what possible of professional jammers and even spoofing to achieve information superiority in the theatre. Regardless what cyber activity may be, the needed of extra security is have to be stronger than expected by the using the GPS coordinates which is originally weak and vulnerable.

Furthermore, the unprofessionally intentionally occurring Cyber-electronic-attacks are using cheap, light-weight, low-power jammers. Those Personal Protection Devices (PPD) are widely available. They are considered more frequently threat of cyber-attacks, and available in the internet market although their usage is not allowed in the most of countries.

In this domain, the most related cyber-attack to be highlighted is the failure of the certification process of the GLS type Honeywell SLS-4000, which was subjecting to approval by the Federal Aviation Agency (FAA) at Newark Liberty International Airport in the USA in 2012, it was fully disturbed by a truck driver using a jammer in a road nearby the airport as per FAA reported, (Pullen, 2012; Heue, 2018). And also the accident was analysed in the meetings of the Future Security Conference 7th in 2012. As shown in the left panel of Figure no. 7 below, the Newark Liberty International Airport is closely surrounded by the crowded traffic roads. Meaning that any cheap jammer with low power can success in disturbing the GLS GPS signals, or even the low-altitude landing aircrafts using the GLs signals as well. When the geographic terrain of the Liszt Ferenc International Airport in Budapest Hungary is examined and compared with Newark Airport, as shown in the right panel of Figure no. 7 below, it was noticed that there is a better but not much difference in the nature of the surrounding roads. In Budapest airport, the googled measured nearest road is about 350 meters from the runways and they are not crowded as the other airport, or at least from any of the position of the two proposed sites of any cites of the GLS system that may be installed there. It may be better but not so far if higher power jammers would have been used.

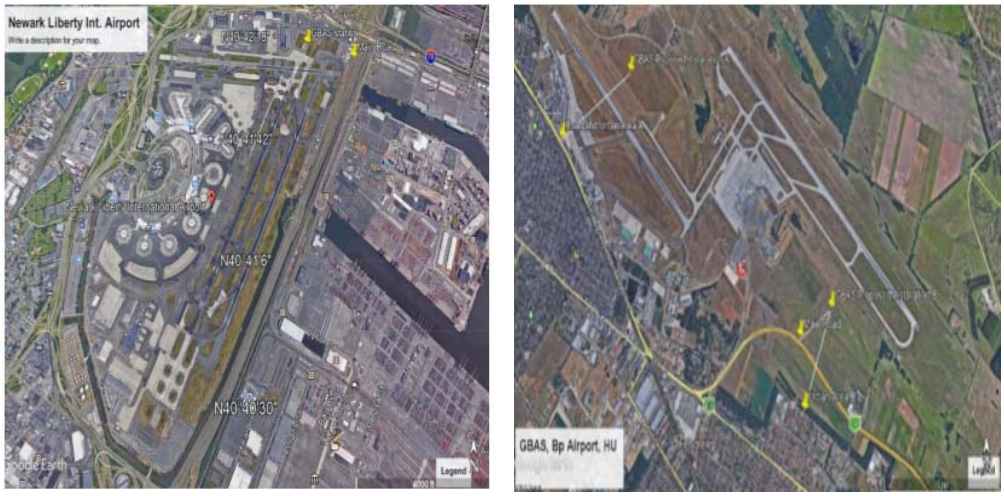


Figure no. 7: *Left Panel: Newark Airport layout, Right Panel: Layout of Liszt Ferenc Airport at Budapest*

2.2.4. Results

However, using the C/A GPS code, the open civilian code, has a higher potential tendency to be jammed or spoofed more than the military restricted P/Y code. Therefore, the GPS coordinates are not guaranteed and could be easily attacked. The drawbacks of the Geo-encryption algorithm in terms of using the Lat/Long coordinates of the GPS system can be summarized as follows:

1. The necessity of using the anti-spoof GPS receivers. Otherwise, the added layer of security would be shortened to the conventional algorithm only.

2. The encryption file would reveal the location of the receiver, especially in the military usages. It may provide vital information to whoever wants to spoof the device.

3. Is the Geo-Encryption Algorithm Necessary for the GBAS Landing System (GLS)?

By principle, the GLS requires that both the ground and aircraft subsystems use the same precisely corrections of the ephemeris and satellite clock. Because the differential principle removes all the ranging errors that are common to the ground and the aircraft subsystems. Mainly, the GBAS Ground Subsystem provides the Final Approach Segment (FAS) Data, as per Alhosban (2015). The GLS subsystem stores data related to the serviced runway end(s), in the form of the (FAS) route construction data blocks. It broadcasts data continuously for reception by the approaching aircraft. However, each GBAS Station has Data Processing and Integrity Units that are responsible for GBAS Messages Elaboration (MT1, MT2, MT4). Most importantly, the MT4 message that contains one sets of FAS data, each defines a single precision approach, including the coordinates of the Landing Threshold Point/Fictitious Threshold Point (LTP/FTP). On the other side, the aircraft subsystem then corrects its own pseudorange measurements for each satellite transponder with the differential correction data received from the ground subsystem over the VHF data link. The corrected pseudorange measurements are used to more precisely determining the aircraft's position relative to the selected FAS. More details can be found in (Alhosban, 2015). Based on the above description, it is clear that the GBAS /GLS system is fully capable to be operated by the GIS-aided precision approach procedures, it is more relevant to data transmission that is timely sent to the approaching aircraft without any delay. Any encryption process, either conventional or added layer as Denning geo-encryption, would not be of an added value, it may cause disruption of waypoint coordinates, and could cause a negative impact rather than being of an added security value, let alone the critical final situation of hosting the aircraft safely to the runway surface.

4. Assessment of Implementation of the Geo- Encryption Algorithm in the GBAS Landing System (GLS), Special Case Study in Budapest International Airport

In order to examine where the Denning Geo-Encryption can be potentially implemented, the phases of flights of any aircraft is fully illustrated. Most importantly, in which flight phase the airborne equipment is most likely vulnerable to be attacked by hackers or intruders. The intended or unintended jamming or spoofing may impact the communication voice messages from the controllers to pilots. As seen before, the navigation messages in those phases are comparatively secured by the GPS structural encryption methods whether it is enough or not. A special case study of the Budapest International Airport was taken as an example, but it can be applied for all airports procedures.

In general, there are three modes of phases of flight, the terminal phase mode (both departure and arrival), the enroute phase mode, and the final approach phase mode, as shown in Figure no. 8 below, each phase has an operational requirements of navigation that are supported by a certain type of equipment, the radio navigation equipment such as (VOR, DME, ILS), they will be gradually replaced by the GNSS technical solutions such as (ABAS, GBAS, SBAS) systems.

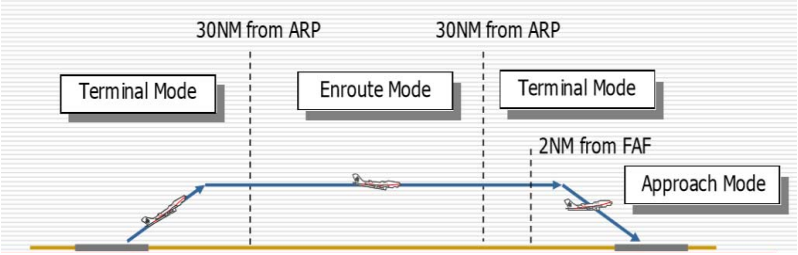


Figure no. 8: *The flight phases Modes*

In terms of existing infrastructure for Budapest airport BUD, the following figures, taken from the official website and have been published since May 2018, data are listed in the official websites of www.hungaryairport.hu and www.ais.hungarocontrol.hu. Hence, in Figure no. 9 below, there are three GIS-aided holding areas in the terminal mode in the BUD airport. The holding areas are used in case of the heavy traffic to delay the coming aircrafts until the runway is clear to land. In those three holding areas, many voice messages can take place between the controller and the pilot, in which adding the extra layer of security by using the Denning geo-encryption could be possible usage.

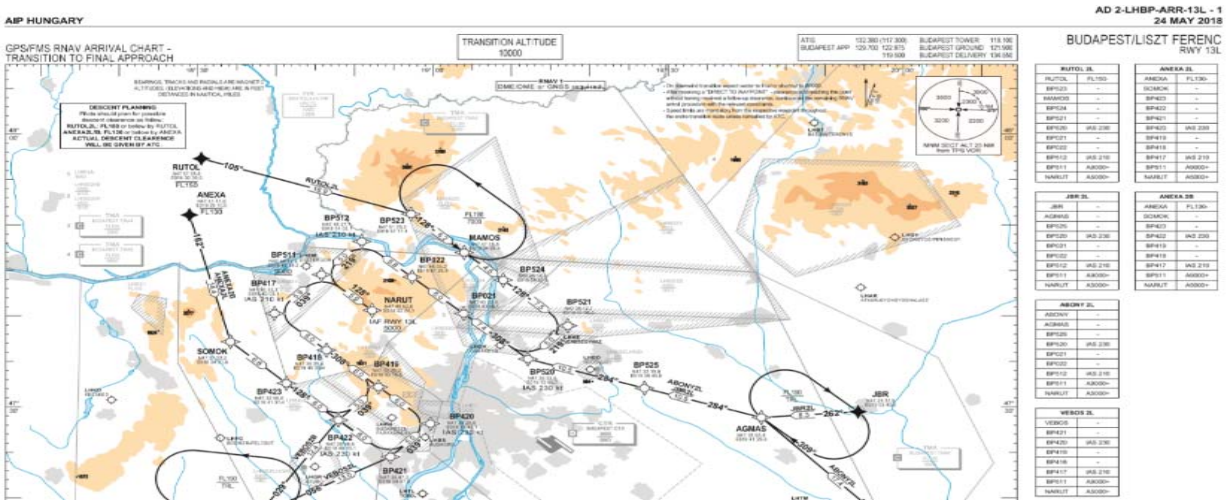


Figure no. 9: *The Terminal RNAV Data for BUD airport 13L including three holding areas for transition to FAS*

Then, in Figure no.10 below, showing the final approach segment data, it contains four (4) Way Points (WP), the three Initial Approach Final (IAF) WPs resemble the three potential coming directions; the straightforward WP named (NARUT), the left one (GIGAN), and the right one (KESID). All the three WPs lead the approaching aircraft to the Initial Final (IF) WP which is the start point to the FAS descending glide path where the ILS and the GLS turn to be used in bad weather of

low visibility. Actually, some voice messages may happen, but more likely the navigation messages dominate. Furthermore, the relatively high speed of a traversing aircraft those waypoints may cause a restrictions and limitations of ciphering the voice messages by the use of geo-encryption model. Due to the fact that its mobility is shortened by high speeds of movement.

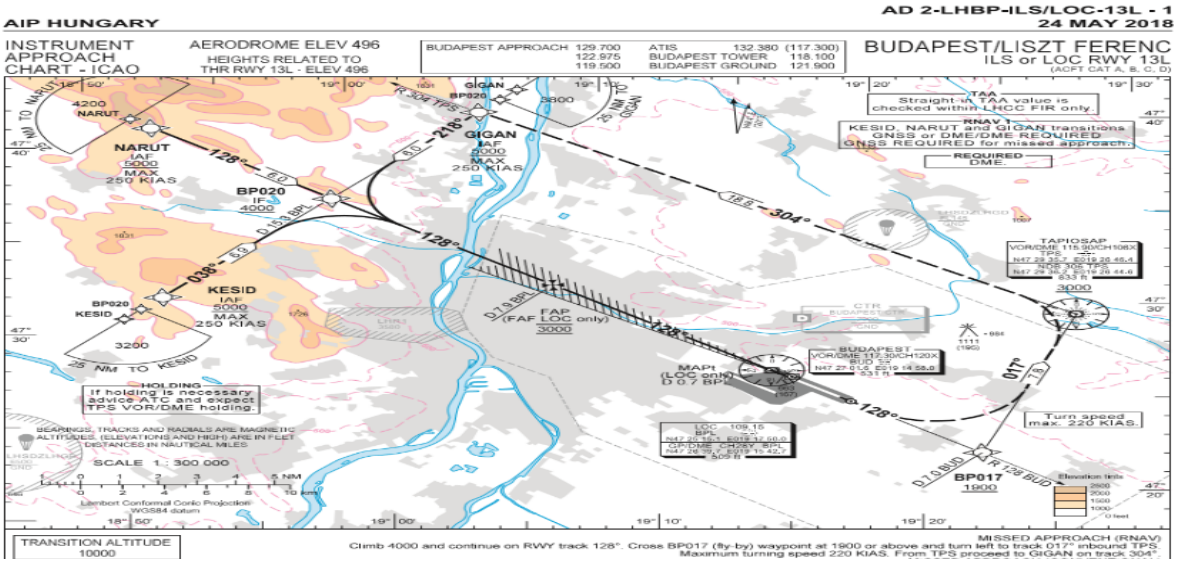


Figure no. 10: *The start of the Final Approach Segment Instrument RNAV Data for BUD airport 13L*

Finally, and as shown in Figure no. 11 below, the final approach fix (FAF) started to be used in the final segment, extended to the 13R Runway's Touch Height (TCH) point called MAPT. In this final segment, the use of ILS or GLS is dependent on the availability of integrity, accuracy and continuity of the system, especially in bad weather or night flights. Hence, the voice messages are so limited and the only guidance would be the GLS system data and coordinates.

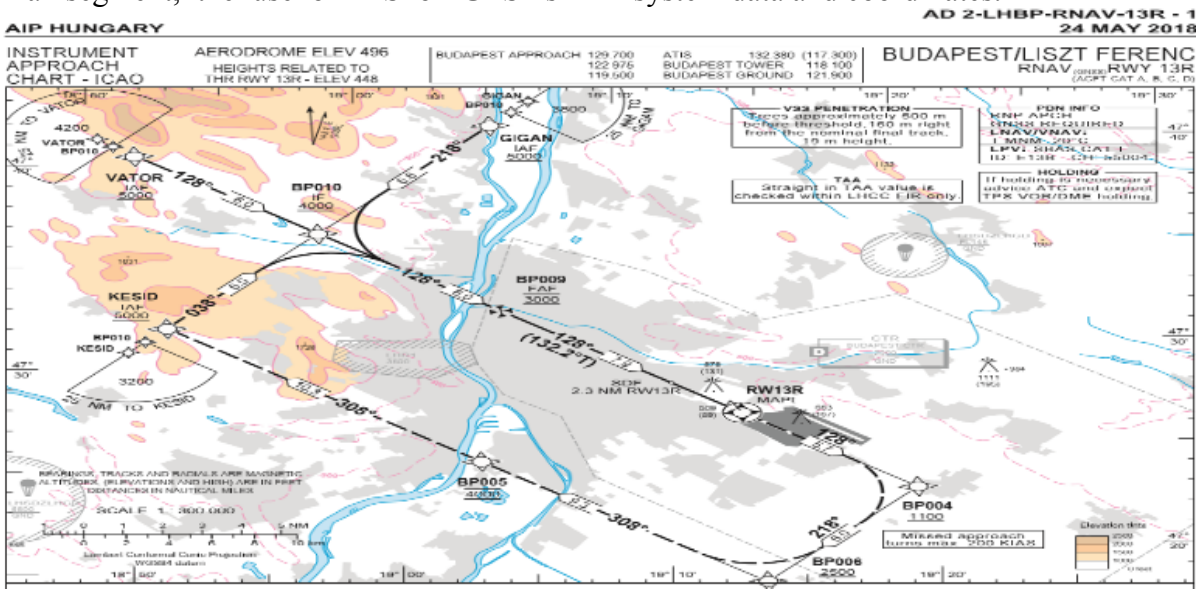


Figure no. 11: *The Final Approach Segment Instrument RNAV Data for BUD airport 13L*

From another perspective, a recent study of (Gurtov, Polishchuk & Weinberg, 2018) has shown the importance of improving the "Controller–Pilot Data Link Communication (CPDLC)" security by adding a secondary VHF communication channel, as much as trustworthy enough to mitigate the already congested VHF communication channel and to enable the ATC growth.

The study of Gurtov, (2018) showed that the implementation of any encryption method needs to have minimum impact on the system's performance as possible while still providing a security protection. They proposed utilizing other than geo-encryption algorithms, such as the existing flight plan and Approach Instrument Plates (AIP) information system. Trying to provide a trust authentication of the CPDLC encryption. Also the Identity-defined networking was proposed as a generic solution to be applied to the ATC communication system as a whole, including the CPLDC and all other communication means. Because it can be gradually deployed and used without the necessity to change the existing hardware.

However, the study unfortunately didn't propose the Denning Geo-encryption method amongst their solutions. And their study lacks to any best approach for security in the CPDLC link, that's approved my study results of existing of challenging constraints in applying any type of encryption during the terminal and final approach phases of flight. Although the encryption is needed in order to strengthen the security of the communication in this phase of flight, but it should be optimized and compromised with other negative impacts may cause disruption of its generic function. The geo-encryption method could be used, with more investigation, in the holding areas prior the final approach is conducted, in which a lot of traffic of voice messages is being transferred between the pilot and the controller while descending in the well-defined holding area.

5. Conclusions and Recommendations

In conclusion, this study argued and examined the possible ways of using the innovated Geo-encryption model in flight phases. The study also analysed the concept of its mobility and the potential limitations. There is a tendency to use this model in a stationary receiver rather than mobility, moreover, it can be used in a semi-moving object in a predefined zone in a pre-set safe areas designed in a well-defined path or route of relatively slow movement. One potential use could be, with more investigation, in the well-defined holding areas, in which a lot of traffic of voice messages being transferred between the pilot and the controller. Above all of this, the model is most likely depends on the assumption of jamming/spoofing free GPS receivers. The added value of the geo encryption method is an extra layer of security, locked to a geographic location, time and limited velocity, which in case of not being met, the conventional encryption could be in use, otherwise, no benefit or information loss will be blamed. It was shown that it is good to have it under certain conditions in flight phases, without negatively affecting the operation of the generic function of communication performance. Its recommended to have further investigations of such better concept of geo-encryption in flight phases by experimental flight tests, which is beyond the capability of the scope of this study.

REFERENCES

Adamy, D. (2009). *EW 103: Tactical Battlefield Communications Electronic Warfare*. London: Artech House.

Al-Fuqaha, A., Al-Ibrahim, O., & Rayes, A. (2007). *Geo-Encryption Protocol for Mobile Networks*. Semantic Scholar, USA: Western Michigan University.

Alhosban, A. (2015). Impact of Multipath Error on the Availability of Integrity in GBAS Application. France/Germany Project. *ICG Expert meetings*, Vienna Austria: UNOOSA.

Alhosban, A. (2019). Electronic Warfare in NAVWAR: Impact of Electronic Attacks on GNSS / GBAS Approach Service Types C and D Landing systems and their proposed Electronic Protection Measures (EPM). *Hadmérnök, Budapest, Hungary, Vol. 14, Issue 2*, pp. 238-255.

Alhosban, A. (2020). Navigation Warfare (NAVWAR): Balancing the Position in Space between GPS and Galileo. *Hadmérnök, Budapest, Hungary, Vol. 14, Issue 4,* pp. 163-177.

Denning, D. (2001). Is cyber terror next?. *Understanding September*, *Vol. 11*, pp. 191-197, USA.

Denning, D., & Scott, L. &. (2003). Geo-Encryption: Using GPS to Enhance Data Security. *GPS World, Vol. 4*, pp. 40-49, USA, Calhoun: Institutional Archive of the Naval Postgraduate School.

Gurtov, A., Polishchuk, T., & Weinberg, M. (2018). Controller–Pilot Data Link Communication Security. *Sensors, Vol. 18, Issue 5, 1636,* pp. 1-12, Sweden.

Heue, R. (2018). GNSS Jamming and Spoofing: Hazard or Hype?. *Space of innovation*. *ESA*, Germany.

Hofmann-Wellenhof, B., Lichtenberger, H., & Collins, J. (2001). *Global Positioning System Theory and Practice.* 5th revised Edition, New York. USA: Springer-Verlag Wien GmbH.

Pullen, S., & Gao, G. (2012). GNSS jamming in the name of privacy: potential threats to GPS Aviation. *Insidegnss Journal*, USA: Standford University.

Seidel, J. (2018). GPS Signal jammed in Norway and Finland. *Technology innovation military news*. News.com.au. Australia.