Journal of Navigation and Port Research International Edition
Vol.34, No.2 pp. 97~103, 2010 (ISSN-1598-5725)

A Basic Study on the Jamming Mechanisms and Characteristics against GPS/GNSS Based on Navigation Warfare

Kwang-Soob Ko†

† *Department of Navigation & Shiphandling, Korea Naval Academy, Jinhae 645-797, Korea*

Abstract : *It has been recognized that the risk from the vulnerability of GPS can lead to the extreme damage in the infrastructure of the civil and military in recent years. As an example, the intentional interference to GPS signal, named GPS jamming, was really performed to misguide GPS guided weapons during Iraq war in 2003, and the fact has also followed by the serious issues on GPS in civilian community. In the modernized military society, the navigation warfare(NAVWAR) based on the GPS jamming has been emerged and introduced as a military operation. The intentional interference to the future global navigation satellite system(GNSS) involving GPS must be also an important issue to civilian users in near future. This study is focused on the fundamental research prior to the research on "Potential principle of NAVWAR" under NAVWAR of the future warfare. In this paper, we would study on the investigation of NAVWAR based on electronic warfare(EW) and analyze characteristics of the jamming against GNSS's receivers. Then the general mechanism on GNSS jamming is proposed.*

Key words : *GPS, GNSS, Jamming, Navigation warfare, Electronic Warfare*

1. Introduction

Electromagnetic devices have been increasingly used by civilian and the military in various fields. Especially, they play a key role in intelligence, communications, sensing, information storage and modern radio navigation. The electromagnetic(EM) interference has also been at issue in the use of devices. The global positioning system(GPS), one of the global navigation satellite system(GNSS), would be the most popular system among those in last decade. The worldwide use of GPS is due to the advantage that GPS provides real time 3-D position, velocity of vehicle and precise time. Because of the advantage, it has surely become the reliable infrastructure for transportation, information and communications in networks.

It has also been recognized that the risk from the vulnerability of GPS jamming can lead to extreme damage in the infrastructure of the civil and the military(DOT, 2001; Ko, 2010; Chung, 2004; David, 2009(a); Borje, 2003). The potential interference can cause not only the limited denial of GPS but also the denial of GPS over large geographic area. The intentional interference against GPS signal, named GPS jamming, was really performed to misguide GPS guided weapons during the Iraq-war in 2003(KNWC, 2003), and the navigation warfare(NAVWAR) was also introduced as a military operation.

The NAVWAR against GNSS, which has newly emerged in recent years, has not been well known to civilian and the military as well. Therefore, one of the main issues in the NAVWAR, the jamming against the navigation system, has not been well introduced yet. Especially, the systematic mechanism of the jamming, characteristics of jamming procedures, the effectiveness of the jamming might not be consistent due to the lack of open materials and their limitations for security.

As long as NAVWAR is undertaken in a conflict area, a certain level of principles must be required for maintaining the safe security of infrastructures in civilian and the military. This study is focused on the fundamental research prior to the research on "Potential principle of NAVWAR" under NAVWAR of the future warfare. Because of the restriction of field test, any experimental way is not dealt with in this study.

In the paper, we study the investigation of NAVWAR based on electronic warfare (EW) and the analysis on characteristics of the jamming against GNSS's receivers. Especially, the characteristics of the denial jamming and the deception jamming on NAVWAR referred to EW are investigated. The fundamental mechanisms for the denial jamming and the deception jamming/spoofing are also proposed.

† Corresponding Author : Kwang-Soob Ko, Kwangsoob@hanmail.net, 055)542-0565

2. Characteristics of the jamming in EW and NAVWAR

2.1 Specific concepts of NAVWAR

According to the key references which are widely read in military societies, EW refers to any action involving the use of electromagnetic devices to control the electromagnetic spectrum or to attack the enemy(USN, 2006). The purpose of EW is to deny the opponent advantage and ensure freedom of action for friendly forces in EM environment. The effectiveness of EW has vitally influenced both tactical and strategic decision in a combat. EW includes three major subdivisions: electronic attack(EA), electronic protection(EP), and electronic warfare support(ES). EA is preventing or reducing the enemy's use of EM spectrum and promoting uncertainty. EP is protecting friendly combat capabilities against the undesirable effects of enemy electronic attack. ES is a passive surveillance of EM spectrum to detect the enemy's position, strength, and intention, and warning of targeting or homing. It is sure that the victims to jam and equipments to be protected are mainly related to military's works and operations. This is true with respect to the military but not to civilian.

On the other hand, NAVWAR can be undertaken not only for the purpose of military but also for a malicious action by a hostile civilian or group. The vulnerability of GPS receivers has long been known, and the jamming of civil receivers have also considered as a serious problem.

Even if the Department of Defense of the USA began to initiate a Navigation Warfare program as a GPS security program to ensure the United States retains a military advantage, the characteristics on NAVWAR have not been clearly written in military documents, especially even in well known references(Joint chief of staff, 2007; DATQ, 2007). In addition, any action or policy have not been actively taken regarding NAVWAR.

It might be reasonable that NAVWAR is dealt with a specific EW with respect to GNSS. The following summarized descriptions are the key characteristics investigated through this study referred to materials(DOD & DOT, 2001; Lee, 2007; Lee, 1986).

1) Friendly forces are protected to maintain their ability to use satellite navigation and hostile users are prevented from using satellite navigations and their augmentation systems.

2) Unlike EW belonging to military actions, NAVWAR can be performed by the military and civilian as well.

3) The main victims or targets of the jamming will be all users of existing GNSS, GPS & GLONASS, and the being developed systems, GALILEO, Japan's Quasi Zenith Satellite System(QZSS), COMPASS of China and India's Regional Navigation satellite System(RNSS).

4) Even if civilian uses should be preserved outside an area of conflict under NAVWAR, the threats to civilians and their infrastructures are increasing or may increase in the future.

2.2 Denial jamming in EW and NAVWAR

The more GNSS is applied to enhance the functional capability of modern weapon systems, the more the threat of jamming may increase in military operations, and then the effect can also reach to civilian infrastructures. One of the serious threats from the noise jamming occurs to prevent from using satellite signals. The noise jamming technique, one of the electronic attacks, is separated into two categories, the denial jamming and the deception jamming. The noise jamming in the sense of EA has traditionally been applied to the system such as radars, active sensors, which transmit EM energy into a combat field. It can also be identical to a passive sensor, GNSS.

One of the important issue is selecting the jammer's bandwidth applied or matched to victim's receiver. It is because the bandwidth affects jamming power. Three denial jamming methods in dealing with "bandwidth" have well known in the radar jamming operations(Lee, 1986). These are the spot jamming, the barrage jamming and the sweep jamming. The spot jamming is concentrated the narrow bandwidth which is identical to that of victim's radar or wider than that. The barrage and sweep jamming, which spread their energy over bandwidth much wider than that of the radar signal.

Although the terminology used in the jamming of radars and GNSS is slightly different, it has been recognized that the fundamental techniques of the denial jamming are very similar to ones applied to GNSS in process in this study.

The GPS jamming is defined to be the intentional radio frequency interference to cause a GPS receiver to fail to acquire or break lock, and then the useful solutions of navigation can not be obtained. It is referred to the denial jamming as mentioned previously. To perform the jamming, it is essential that the sufficient intentional interference signal must be induced to the receiver, then jammer to receiver signal power ratio power(J/S) should exceed the tracking threshold. It would be discussed in the next.

2.3 Deception jamming/spoofing in EW and NAVWAR

The deception jamming, named spoofing in GPS community, has actually been applied to a radar in EW for a long time(USN, 2006; Hong, 2000). Whereas the denial jamming blocks the location of the target with noise, the deception jamming misleads by providing a false target location. Then radar and command control systems can be confused by causing the radar to generate incorrect target range, bearing and elevation.

In the case of GPS, the satellite signal manipulated by erroneous mechanism must be propagated to the receiver's antenna as if a genuine signal, and then the receiver is naturally to lock the false satellite signals and create undesired errors in positioning, velocity, timing(PVT)(DOT, 2001). As a result, the receiver can be walked off the desired track prior to the discovery of deception. It should also be noted that the deception jamming of GPS is more difficult to perform and more serious in threat than the typical denial jamming.

3. Fundamental mechanism of the GNSS receiver's jamming

3.1 Mathematical process for modulation, demodulation & navigation solution

For the general process from the GPS satellite to the user's receiver, the signal transmitting is followed by the free space propagation, incoming signal to antenna, acquisition and tracking of the incoming signal, and demodulation for navigation process and the navigation solution. Unlike that of radar jamming techniques, the systematic mechanism of the navigation jamming has not been revealed. The general mechanism of the victim's receiver jamming is discussed in this chapter. The processing of the modulation and demodulation based on the well known mathematical formulas(Spilker, 1978; Ko, 1983; Parkinson, 1996; Jan, 2001) are useful to do this. In order to design the conceptional mechanism of the jamming, it might be the valuable the first step to analyze the transmitting GPS signal equation given by

$$S_{L_1}(t) = A_P D(t) P(t) \cos(w_r t) + A_C D(t)\, C(t) \sin(w_r t) \tag{1}$$

where, A_P : P signal power

A_C : C/A signal power

$D(t)$: ±1 binary data, 50 bps

$P(t)$: ±1 PRN(pseudo random noise) code, 10.23 MHz

$C(t)$: ±1 PRN code, 1.023 MHz

w_r : carrier frequency(radians) of L_1

It is noted that GPS signals contain components of in-phase and quadrature signals which have a relative phase difference of 90 degree. The signal is generated in the manner of quadrature phase shift keying(QPSK), which is used to transmit multiple signals on a single carrier frequency by common transmitter. The equation is for the ordinary GPS satellite signals not for the modernization satellites.

The followings are the steps for the modulation and transmitting of GPS signal in satellites.

STEP1: combining navigation message 50bps, D(t), to PRN code C(t) or P(t)

STEP2: binary phase shift keying(BPSK) modulation with the combined signal and carrier frequency L1

STEP3: transmitting modulation signal L1 from the satellites

One should know that the signal modulation is an important knowledge for the GPS jamming because its occurrence is directly related to tracking the modulated signal and the demodulating the signal in the receiver. It is also distinguished in GPS system that the carrier frequencies in all satellites are the same but each satellite has own PRN code with user's receiver. The receiver must have the same PRN codes as those of satellites and replicate them to demodulate navigation messages while processing coded multiple access (CDMA).

To do this, GPS receiver should generate the PRN codes, C/A or P, which is transmitted from the GPS satellites in space. And the generated replica code is shifted relative to the received code until correlating with satellite's PRN code(C/A or P). Once the time shift is accomplished, the two codes match and measure the time spent for the free space propagation.

The pseudorange observable is based on the time shift between the instant a GPS signal leaves a satellite and the instant it arrives at a receiver. It is noted that the code correlation process must be performed by the autocorrelation function to match the phase of the replica PRN code to that of the incoming satellite's PRN code. The autocorrelation function is given by

$$R_{C/A}(\tau) = \frac{1}{1{,}023\, T_{CA}} \int_{t=0}^{1023} PN(t)\, PN(t+\tau) d\tau \tag{2}$$

where, $PN(t)$: C/A code PRN sequence

T_{CA} : C/A code chipping period(977.5 ns)

τ : phase time shift

The value of the autocorrelation function is equal to 1, maximum correlation, then the receiver's replica code fits the incoming satellite's PRN codes. Once the correlation of two PRN codes is achieved with delay lock loop, the " lock on" state is maintained in each correlation channel of the GPS receiver.

As long as the lock is maintained, important values such as pseudoranges, navigation messages, delta ranges, integrated doppler, are available in the receiver.

The measurement pseudorange from the time shift is given. However, the measurement pseudorange contains the various error sources through the propagation of the transmitting signal in space. Then it should be represented by the equation with the potential error sources, it can be expressed by

$$PR = \rho + c(dt - dT) + d_{ion} + d_{trop} + \varepsilon_p \tag{3}$$

where, PR : measured pseudorange
ρ : true range
c : speed of light
dt : satellite clock offset from GPS time
dT: receiver clock offset from GPS time
d_{ion} : ionospheric delay
d_{trop} : tropospheric delay
ε_p : multipath, receiver noise, etc

The above pseudorange equation must be transformed to the navigation equation in order to compute 3-D position using the following navigation equation given by

$$\begin{aligned} PR_i &= \sqrt{(x_i - x_u)^2 + (y_i - y_u)^2 + (z_i - z_u)^2} + ct_u \\ &= f(x_u, y_u, z_u, t_u) \end{aligned} \tag{4}$$

where, PR_i : i th satellite's pseudorange, i=1, 2... n
x_u, y_u, z_u : the unknown receiver's position
t_u : offset of receiver clock from system time
x_i, y_i, z_i : known satellite's position

It is noted that the satellite positions are obtained from the output of navigation messages transmitted in processing demodulation in the receiver, and the receiver's positions are obtained in navigation processing.

3.2 Simplified evaluation flow of GNSS receiver's jamming under NAVWAR

In this section, we would describe the procedure of tracking the jamming signal to organize the systematic mechanism of the GNSS receiver's jamming. The received signal through an antenna contains not only the desired GPS signal, receiver thermal noise but also jamming signal of the denial or the deception/spoofing in jamming circumstances.

The received signal with the denial jamming signal should effect to the sampling and quantizing of the signal, and then its resultant error also effect in the signal processing of the parallel code and carrier tracking loops.

In the normal case without jamming signal, the outputs of the digital processing produces pseudorange, delta range, doppler shift and data demodulation for proceeding the navigation process. The signal acquisition, carrier tracking and data demodulation depend on the amplitude of the signal to noise ratio. In case of the denial jamming, if J/S is over the tolerable value , the lock of signal tracking may be failed, then the denial jamming is successful. However, the deception jamming signal must be locked by the tracking loops in order to produce the false outputs in PVT, then the deception jamming is successful. In order to examine to the jamming effect of the denial jamming, the tolerable jamming signal to received signal power ratio, J/S, has generally been used, however, there is no proper way for evaluating the deception jamming of GNSS yet. The fundamental simplified mechanism GNSS jamming in a victim's receiver is introduced in figure 1. It can be logically designed by knowledges of the general processing steps in a receiver and the jamming process. It may also progress to "potential principle under NAVWAR" with some advanced experimental tests not only in field but also in laboratory. It is out of scope in this paper.

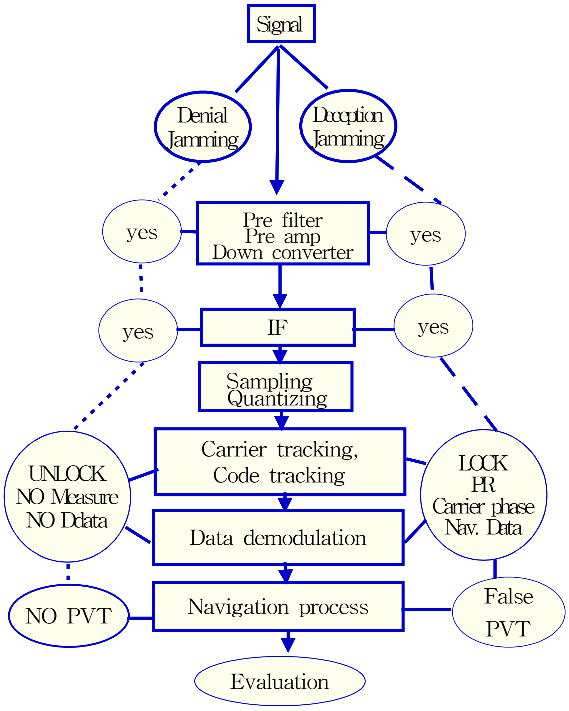

Fig. 1 Simplified evaluation flow in a victim's receiver under NAVWAR

4. Analysis and evaluation of GNSS jamming

4.1 Analysis of GNSS jamming characteristics

The most jamming issues are deeply related to the signal characteristics of GNSS's satellites. Although the GNSS jamming has been focused on GPS receiver, it is sure that the circumstance of the jamming will be rapidly changed with the new global navigation satellite systems, GALILEO and COMPASS, and the modernized systems, GPS and GLONASS.

The modernized GPS signal characteristics and the frequency allocation of GNSS are shown in table(1) and (2),respectively. These have been investigated through references(Van, 1978; Van, 2000; Fonta, 2001) involving the latest ones and rearranged here for analyzing GNSS jamming characteristics.

Table 1 The modernized GPS signal characteristics

Classification	Modernized GPS Signal Characteristics							
Signal	L1 C/A	L1 P(Y)	L2 C/A	L2 P(Y)	L2C	L5	L1 M	L2 M
Received Power(dbW)	-158.5 (-160)	-161.5 (-163)	-164.5	(-166)	-160	-154.9	-158/-138	
SV type	Block IIR(Block II)				Block IIR-M,F/ Block III			
Bandwidth	2.046	20.46	2.046	20.46	2.046	20.46	30.46	
values in parenthesis refer to BLOCK II SV								

Table 2 Frequency allocation of the future integrated GNSS

GNSS	Frequency Band		
GPS	L5(1176.45)	L2(1227.6)	L1(1575.42)
GLONASS		L2(1242.92-1247.75)	L1(1598.04-1604.25)
GALILEO	E5(1164-1215)	E6(1260-1300)	E2-E1(1559-1592
COMPASS	E5B(1207.14)	E6(1268.52)	E2(1561.098)
L5: new frequency(modernized) Galileo/Compass: currently under development			

One must pay attention to the several remarks on the tables to affect the jamming mechanism. These are the received power, bandwidth and carrier frequency band. Even if some of COMPASS frequencies are not clearly allocated due to the signal interference to GPS and GALILEO, most of carrier frequencies of the future GNSS will be similar ones on the table obtained using the newest materials.

The receiver's minimum received power with respect to Block IIR has been increased compared to the received power based on Block II. Futhermore, the new carrier frequency, L2C, L5 and the codes L1(M), L2(M), L2 P(Y) are available in near future.

The received power of those signals including L5, L1(M), L2(M) will be highly stronger than the present signal. Therefore, the jamming device must require more powerful signal to match those signals at receivers. The carrier frequency bands of GPS and GLONASS have been closely allocated since the beginning of their development. In addition, the frequency bands of the new GNSS, Galileo and COMPASS, are also close to all other systems. The major bandwidth of the future GNSS would be matched within 2-30Mhz. It means that those GNSS receivers may easily be jammed by the simplified jammer with modern techniques.

In the manner of EW, the key characteristics of the investigated denial jamming for NAVWAR can be described as follows.

1) The objective of the denial jamming is the prevention of satellite's signal acquisition and tracking. Under the denial jamming against civilian code receivers in peace time, the military receivers also might be affected during the military signal acquisition.

2) Currently, the major types of the jamming are CW jamming, narrowband(NB) jamming, wideband(WB) jamming and the most of jamming devices for NB and WB are generally matched to the bandwidth with respected to 2Mhz and 20.46Mhz centered L1 and L2 carrier frequency, respectively. The bandwidth would become wider and wider with new types of GNSS under development.

3) NB and WB are used by pseudo noise(PN) gaussian distributed noise sequence.

4) The new technology matched to the combined GNSS receivers will be rapidly developed with the development of GALILEO, COMPASS and the modernization of GPS and GLONASS.

5) The effectiveness of jamming mainly depends on jamming power, jamming bandwidth, the type of jamming, antenna gain, masking loss, receiver design technique.

The next is the results for deception jamming/spoofing.

1) The deception jamming signal should be GPS-like signal to spoof against the victim's receiver and the victim's receiver may track the deception signal like a true signal. The deception jamming require the knowledge of PRN, almanac information, modulation, demodulation and navigation solution in order to provide the manipulated PVT errors in victim's receivers.

2) Two types of the deception jamming are expected. One is the PRN manipulation techniques, the other is the navigation message manipulation. The PRN method may produce correlation errors in digital signal processing and

then cause the PVT error. The more sophisticated method, data manipulated method, may produce the expected positions and velocity to control the victim's path. It means that the deception jamming can lead the victim's vehicles unintentional track or false destination. It is most serious case but this jamming may require high technology exceeding that of PRN method. It may be only applicable to the military weapons in real navigation arfare circumstance.

4.2 Evaluation of GNSS jamming

Even though a few conducts of the denial jamming test under the circumstance in a free space and a laboratory have performed by civilian and the military, the results have not revealed in detail(DOT, 2001). Especially, the knowledge of the deception jamming has not been known because the technique of the jamming might be too difficult to be easily performed and the purpose of the deception jamming is mainly against the military receivers.

There have been the valuable test results of the denial jamming and reports related to the GPS receiver's tolerable J/S and the effect of jamming by researchers and the Department of Transportation(DOT) in USA(Matt, 1997; David, 2009; Borje, 2003).

However, most of the them which have provided by various methods, experiment and simulation, are not consistent for evaluating and understanding the effect of satellite navigation receiver's jamming. For having the trend of jamming performance in the receiver, it might be a valuable way to compare with tolerable jamming power regarding the type of receiver and that of jamming. The comparison of the tolerable jamming power is shown in table(3). The tolerable values given in(Kaplan, 2006) for the modern satellites are here rearranged to compare to the ones that we simply computed with respect to the old fashioned satellite. The calculation was also performed using J/S and the user minimum received power provided in references(Kaplan, 1996).

Table 3 Comparison of tolerable jammer power(dbW)

Jamming Type	Receicer's Type		
	L1 C/A	L1 P(Y)	L1 M
Wideband	-118.67 (-125.3)	-111.8 (-118.8)	-107.3
Narrowband	-122.1 (-128.3)	-115.3 (-121.8)	-110.9

values in parenthesis refer to computed values using the present satellite's received signals, other values are designed ones for modernized satellites

From the above three tables, we also recognized as follows. The tolerable J/S values of the WB jamming is higher than one of the NB jamming at same signal code, L1 C/A, P(Y) and L1(M), respectively. And the combined GNSS receivers with receiving GPS signal will have not only the wider bandwidth but also the wider carrier frequency in spectrum band than the present single receiver. Therefore, the future jammer against the combined GNSS receivers must require the higher power than the current potential jammers.

Additionally, even though the most of new satellites of GNSS have the stronger power, the minimum received signal power of the future GNSS receivers might still be weak as much as the oder of the pico watt. It is sure that the multiple-low powered, low-cost jamming devices will be a threat against the civilian GNSS receivers.

5. Conclusion

This study was focused on the fundamental research prior to the designing for "potential principle of NAVWAR" under NAVWAR in future warfare. In the paper, we have studied on the fundamental mechanisms and characteristics of the intentional electromagnetic interference, jamming against GPS receiver. The characteristics of the denial jamming and the deception jamming on NAVWAR referred to EW have been investigated. The fundamental mechanisms for the denial jamming and the deception jamming/spoofing were proposed. It was also noted that the future combined GNSS receivers with receiving GPS signal will have not only the wider bandwidth but also the wider carrier frequency in spectrum band than the present single receiver. Therefore, the future jammer against the combined GNSS receivers must require the higher power than the current potential jammers. For the effectiveness GNSS jamming, the tolerable J/S values of the WB jamming and the NB jamming at various same signal codes, L1 C/A, P(Y) and L1(M), were evaluated. The intentional interference to the future GNSS involving GPS must be also the important issue to civilian users in near future. In the future works, we would like to continue to work for designing "The potential principles of NAVWAR" with proper tests.

References

[1] Borje, F. and Trond, B. O.(2003), "Susceptibilities of Some of Civil GPS Receivers", GPS World, January 2003, GPS Web site:http //:www.gps world.com.

[2] Boggs, M. and Maraffio, K. C.(1997), "Mitigation Path

for Free-Space GPS Jamming", The Federation for America Scientist(FAS) Web Site://http//www. fas.org/ military/program.

[3] Chung, N. S.(2004), "The Analysis of GPS Jamming in Modern Warefare", Graduation Thesis, in Korea Naval War College.

[4] David, L.(2009a), "GPS Forensics, Crime, and Jamming" GPS World, October 2009, GPS World Web Site: http://www.gpsworld.com/defense.

[5] David, L.(2009b), "GNSS Vulnerabilities Conference Discusses Solutions to Jamming, Interference", GPS World September 2009, GPS World Web Site://www.gpsworld.com//gnss.

[6] DATQ(2007), "Report Investigation of Defense Technology in 2007", Regular Report of Defense Agency for Technology Quality in 2007, Vol 3, pp. 225-251.

[7] DOT(2001), "Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Posioning System", John A. Volpe National Transportation Systems Center, Final Report in 2001, pp.29-39, pp.70-80.

[8] DOD & DOT(2001), ''Federal Radio Navigation Plan", The Department of Transportation, USA, pp.I-4-IV-6.

[9] Fonta, R. D., Cheung, W., and Stansell, T.(2001), "The New L2 Civil Signal", GPS World, September 2001, pp.28-34.

[10] Hong, S. R.(2000), "The future EW and perspective of EW in Naval Warfare", Graduation Thesis, in Korea Naval War College.

[11] Joint Chief of Staff(2007), "Electronic Warfare", Joint Publication of Chief Staff, USA, pp. I-2-I-11.

[12] Kaplan, E. D. and Hegarty, C. J.(2006), "Understanding PS:Principles and Applications", 2nd ed., Artec House, London, pp. 243-271.

[13] Kaplan, E. D. and Hegarty, C. J.(1996), "Understanding GPS:Principles and Applications", 1st ed., Artec House, London, pp. 97-100, pp. 219-226.

[14] KNWC(2003), "The Analysis of the Miliary Operation in Iraq War", Korea Naval War College, Daejeon, pp.245-265.

[15] Ko, K. S.(2010), "Circumstance Change of GNSS & Application Strategy of Navigation Technology for Modern Weapon System", The Journal of the Korea Institute of Maritime Information & Communication Science, Vol.14, pp.268-275.

[16] Ko, K. S.(1983), "A Study on PN Phase Modulation Communication System in GPS", Master's Thesis in Korea Maritime University.

[17] Lee, K. S.(2007), "The perspective of the effectiveness EW performance", Graduation Thesis, in Korea Naval War College.

[18] Lee. Y. C. and Hyun, Y. H.(1986), "Principle of EW", The Korea Naval Academy, Jinhae, pp. 14-31.

[19] Parkinson, B. W. and Spilker, Jr.(1996), "Global Positioning System Theory and Applications Volume I", American Istitute of Aeronautics and Astronautics, Washington D.C., pp. 245-257, pp. 329-340.

[20] Spilker, J. J. Jr.(1978), "GPS Signal Structure and Performance Characteristics", The Institute of Navigation, Vol 25. no. 2.

[21] USN(2006), "Principles of Naval Weapon Systems", Naval Institute Press, Annapolis, Maryland, pp. 84-98.

[22] Van Sickle, J.(2001), "GPS for Land Surveyors", CRC Press, London, pp. 15-21.

[23] Van Dierendonck, A. J. and Russel, S. S.(1978), "The GPS Navigation Message", The Institute of Navigation, Vol 25, no. 2, pp. 147-148.

[24] Van Dierendonck, A. J. and Hegarty, C. J.(2000), "The New Civil GPS L5 Signal", GPS World, September 2000, pp. 64-71.

Received 2 March 2010
Revised 24 March 2010
Accepted 24 March 2010