DEFENCE S&T TECHNICAL BULLETIN

BULETIN TEKNIKAL S&T PERTAHANAN

VOL. JIL. 2 | NO. BIL. 2 | YEAR TAHUN 2009 | ISSN 1985-6571

CONTENTS

Classification Enhancements in Hyperspectral Remote Sensing Using Atmospheric Correction Preprocessing Technique 91 - 99

Peter Yuen, Izzati Ibrahim, Kan Hong, Tong Chen, Aristeidis Tsitiridis, Firmin Kam, James Jackman, David James & Mark Richardson

Vulnerabilities of Civilian Global Navigation Satellite Systems (GNSS) Signals: A Review 100 - 114

Dinesh Sathyamoorthy

Evaluation of the Effect of Radio Frequency Interference (RFI) on Global Positioning System (GPS) Receivers 115 - 129

Dinesh Sathyamoorthy, Wan Mustafa Wan Hanafi, Mohd Faudzi Muhammad, Kamarulzaman Mustapa, Nor Irza Shakhira Bakthir, Siti Robiah Abdul, Norhayaty Zahari, Aliah Ismail, Lim Bak Tiang, Arumugam Periapa, Zainal Fitry M. Amin, Mohd. Rizal Ahmad Kamal, Azlina Besar & Mohd. Hasrol Hisam M. Yusoff

An Overview on Wear Debris Analysis for Engine Condition Monitoring 130 - 135

Chan Keng Sam, Wan Fadilah Wan Abdullah, Nor Azlan Sarjo, Shamsul Akmar Abd Aziz, Adam Hj Gani, Mohd Hairudin Abd Karim & Junaidi Md Tahir

Cetakan Tanda Keselamatan Menggunakan Dakwat *Invisible Ultraviolet* 136 – 141

Mohamad Ismail Haji Ali, Norkamizah Mohd Nor, Zariyah Ariffin, Nor Hafizah Mohamed, Rozita Md Salleh, Jamaliah Mohd Noor, Loo Soon Tong & Shurihan Ahmad

Evaluasi Keberkesanan Penentuan Keutamaan Projek R&D Pertahanan Dengan Menggunakan *Analytical Hierarchy Process* (AHP) 142 – 148

Nor Hafizah Mohamed, Zariyah Ariffin, Khalid Mohammad, Mohamad Ismail Hj Ali, Fadzli Ibrahim & Rozita Md Salleh

STRIDE

SCIENCE & TECHNOLOGY RESEARCH INSTITUTE FOR DEFENCE

INSTITUT PENYELIDIKAN SAINS & TEKNOLOGI PERTAHANAN

ISSN 1985-6571

AIMS AND SCOPE

The Defence S&T Technical Bulletin (*Buletin Teknikal S&T Pertahanan*) is the official technical bulletin of the Science & Technology Research Institute for Defence (STRIDE). It contains articles on research findings in various fields of defence science & technology. The primary purpose of this bulletin is to act as a channel for the publication of defence-based research work undertaken by researchers both within and outside the country.

WRITING FOR THE DEFENCE S&T TECHNICAL BULLETIN

Contributions to the journal should be based on original research in areas related to defence science & technology. All contributions should be in British English or Bahasa Melayu.

PUBLICATION

The editors' decision with regard to publication of any item is final. A paper is accepted on the understanding that it is an original piece of work which has not been accepted for publication elsewhere. Contributors will receive one complimentary copy of the issue in which their work appears.

PRESENTATIONS OF MANUSCRIPTS

The format of the manuscript is as below:

a) MS Word format (preferably in Word 2007 format)
b) Single space.
c) Justified.
d) In Times New Roman 11-point font.
e) Should not exceed 10 pages, including references.
f) Margin should be 2 1/2 cm or 1 inch an all sides.
g) Texts in charts and tables should be in 10-point font.
h) Citations and references should follow the standard format.

Please e-mail the manuscript to :

1) Dr. Zalini bt Yunus (yzalini@yahoo.co.uk)
2) Pn. Norkamizah bt Mohd. Nor (norkamizah@gmail.com)
3) Dinesh Sathyamoorthy (dinsat60@hotmail.com)

The next edition of the bulletin is expected to be published in April 2010. The due date for submissions is 12th March 2009. **It is strongly iterated that authors are solely responsible for taking the necessary steps to ensure that the submitted manuscripts do not contain confidential or sensitive material.**

The template of the paper is as follows:

TITLE OF PAPER

Name of Author(s)

Address
Tel:
Fax:
E-mail:

Abstract

Contents of abstract.

Keywords: *Keyword 1; Keyword 2; Keyword 3.*

1. TOPIC

Paragraph 1.

Paragraph 2.

1.1 Sub Topic 1

Paragraph 1.

Paragraph 2.

2. TOPIC 2

Paragraph 1.

Paragraph 2.

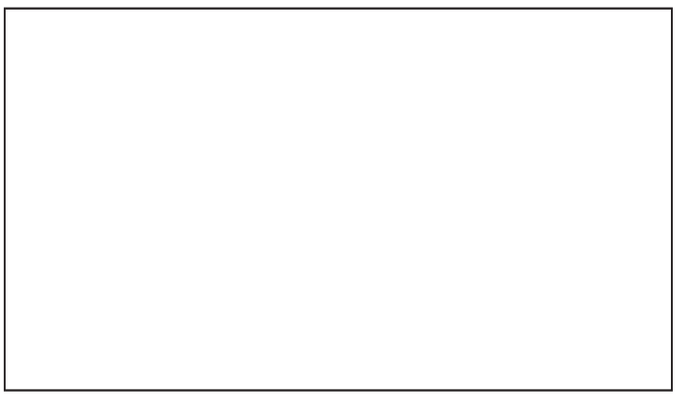


Figure 1: Title

Table 1: Title

Content	Content	Content
Content	Content	Content
Content	Content	Content
Content	Content	Content

Formula 1 (1)
Formula 2 (2)

REFERENCES

Long lists of notes of bibliographical references are generally not required. The method of citing references in the text is 'name date' style, e.g. 'Hanis (1993) claimed that...' or '…including the lack of interoperability (Bohara et al., 2003)'. End references should be in alphabetical order.

1) Author(s) (Year). Title. Publisher, State Published.
2) Author(s) (Year). Title. Journal Title. Vol. , No. , pp. .
3) Website Title (Year). Website address. Accessed date and year.

CLASSIFICATION ENHANCEMENTS IN HYPERSPECTRAL REMOTE SENSING USING ATMOSPHERIC CORRECTION PREPROCESSING TECHNIQUE

Peter Yuen*, Izzati Ibrahim, Kan Hong, Tong Chen, Aristeidis Tsitiridis, Firmin Kam, James Jackman, David James & Mark Richardson

Department of Informatics & Sensors, Cranfield University, Defence College of Management & Technology, Shrivenham, Swindon SN6 8LA
*Email: p.yuen@cranfield.ac.uk

Abstract

This paper reports the result of a study on how atmospheric correction (AC) technique enhances target detection in hyperspectral remote sensing, using different sets of real data. Based on the data employed in this study, it has been shown that AC reduces the masking effect of the atmosphere and effectively improves spectral contrast. By using the standard K-means cluster based unsupervised classifier, it has been shown that the accuracy of the classification obtained from the atmospheric corrected data is almost an order of magnitude better than that achieved using the radiance data. This enhancement is entirely due to the improved separability of the classes in the atmospherically corrected data. Moreover, it has been found that intrinsic information concerning the nature of the imaged surface can be retrieved from the atmospherically corrected data. This has been done to within an error of 5% by using a model-based AC package known as ATCOR.

Keywords: *Atmospheric correction (AC); classification; target detection; hyperspectral imaging (HSI); spectral contrast.*

1 INTRODUCTION

The propagation of electromagnetic radiation through the atmosphere is affected by two essential processes: absorption and scattering. Within the thermal infrared band (wavelengths ~ 4.0-20.0 μm), absorption dominates and is primarily due to ozone and water vapour particles. Atmospheric scattering primarily affects the direction of short wave radiation. At the shorter wavelengths (i.e. 0.2-4.0 μm), attenuation occurs by scattering due to clouds and other atmospheric constituents, as well as reflection. Atmospheric particles include molecules of atmospheric gases, and the small particles and droplets called aerosols, such as smoke, dust, mist, and cloud droplets. There are four types of atmospheric scattering: Rayleigh, Mie, Raman and non-selective, and the exact type of interaction depends on the size of the particle responsible. The most significant of these in the visual / near infrared (NIR) waveband is Rayleigh scattering, which results in haze. Rayleigh scattering occurs when radiation interacts with air molecules smaller than the irradiation wavelength, such as the oxygen and nitrogen molecules in the visible spectrum. The degree of scattering is inversely proportional to the fourth power of the wavelength, i.e., about 4 times more in the blue band than in the red band (Jensen *et al.*, 1986). Mie scattering results when particles are comparable in size to the radiation wavelength such as aerosols in the atmosphere.

In hyperspectral imaging (HSI), the sensor not only receives direct reflected or emitted radiation from the target, it also senses scattered radiation adjacent to the target, and at the same time, scattered radiation from the atmosphere. The aerosols and molecules scatter and absorb solar photons reflected by the surface in such a way that only some of the surface radiation can be detected by a sensor. Even before reflection, atmospheric particles scatter some of the sunlight into the sensor's field of view, resulting in radiation that does not contain any surface information at all. The adjacency effect occurs when light from an object area outside the sensor's field of view which is then scattered into the sensor's view contributing to image blurring. All of these combined factors reduce the spectral contrast between the target and the background in the remote sensing imagery, causing degradation of the target detection and classification efficiency.

The purpose of this paper is to evaluate how target detection/classification can be improved by removing these atmospheric effects, and to understand how these atmospheric factors contribute to classification errors. Previously, there was a study which reported how classification accuracy is affected by atmospheric factors, but the work was conducted using simulated data (Kaufman, 1986). This work utilizes real HSI data (Yuen & Bishop, 2004a) and the atmospheric correction *(AC)* technique adopted in this study has been a model-based algorithm known as ATCOR, which was developed by the German Aerospace Center (DLR) (Richter *et al.*, 2002).

2 ATCOR MODEL DESCRIPTION

2.1 ATCOR overview

Like many other model based algorithms, ATCOR (Richter *et al.*, 2002) performs AC by first computing the AC function for atmospheric transmittance, direct and diffused solar flux, and path radiance as functions of atmospheric conditions and solar-sensor geometries using the MODTRAN atmospheric propagation model. The results are then pre-compiled into a database as a look-up-table (LUT). For data analysis, the first step in ATCOR is to derive a spatial map of the optical depth to evaluate the transmittance (visibility) of the scene. Then, the water vapour map is determined using an atmospheric precorrected differential absorption technique (APDA) (Schlapfer *et al.*, 1998). AC is performed on a pixel-by-pixel basis, and the reflectance is obtained by an iteration process:

1) Evaluate the transmittance of the diffused reflected ground radiation and the spherical albedo from the precompiled LUT. It then assumes an isotropic reflected ground and neglects the influence of the neighbourhood (adjacency effect). The path radiance as obtained from the LUT is subtracted from the at-sensor converted radiance and the remaining signal is converted into an equivalent surface reflectance. So for each pixel j of a line image, the scan angle and the corresponding angular interval in the reflectance-radiance LUT is determined. Then, the radiance $L(j)$ and the correction function are calculated using linear interpolation in this interval to deduce the first round of the reflectance. For the wavelength region < 1.5 μm, the process will continue to the next two steps.

2) The adjacency effect is taken into account to compensate the atmospheric crosstalk between adjacent fields of different reflectance. This is achieved by adding another term of a weighted function (ratio of diffuse to direct transmittance) which essentially measures the scattering efficiency of the atmosphere. The parameter of this weighted function is the difference of the first round estimated reflectance and the averaged reflectance of the neighbourhood.

3) The final reflectance is achieved by including the spherical albedo effect on the global flux. The global flux in the atmospheric LUT has been calculated for a fixed reflectance=0.15 and the final reflectance needs to be adapted to the scene dependent value.

2.2 Aerosol Optical Depth (AOD): Visibility Map

In ATCOR. the AOD is derived based on reference areas with known reflectance values. For example, dense dark coniferous vegetation is known to have reflectance values around 2% in the red band. The visibility of those reference pixels can be readily deduced from the model-derived visibility-radiance curve. ATCOR provides an automatic algorithm to search for these dark pixels in the short-wave infrared (SWIR) band at 1.6 μm or 2.2 μm wavelength, and correlates these to predict the reflectance of the red and blue bands. The red band value is used to estimate the visibility while the blue value is used to measure the deviation of the originally selected aerosol type used in the model. The calculated visibility is expressed as an integer index which is proportional to the total optical depth. The non-reference pixels are assigned to the averaged or triangularly interpolated visibility obtained over the reference regions in the neighbourhood. This averaging or triangular interpolation may also be performed on the basis of small subimages, called sectors, covering the whole scene. The spatial distribution and variability of the visibility within the scene is stored in discrete steps of optical depth

(visibility index image). The information in the atmospheric database is then used to calculate the reflectance image.

Although this is by no means a perfect method for the extraction of atmospheric information from the data, it provides a feasible way to model atmospheric parameters which are otherwise impractical to obtain due to the local variation of particle density and distribution across the scene.

3 ATMOSPHERIC EFFECTS

3.1 Differential spectral contrast

The extent of atmospheric effect is quite significant, particularly for the high altitude remote sensing work such as the Landsat satellite: atmospheric effects with aerosol contributions in the order of 50% are always observed even for relatively clear sky conditions. This imposes a significant effect on the Normalized Difference Vegetation Index (NDVI) assessment: an NDVI of 0.6 on the ground can be interpreted as 0.2 from the top-of-atmosphere (TOA) data (Jensen *et al.*, 1986).

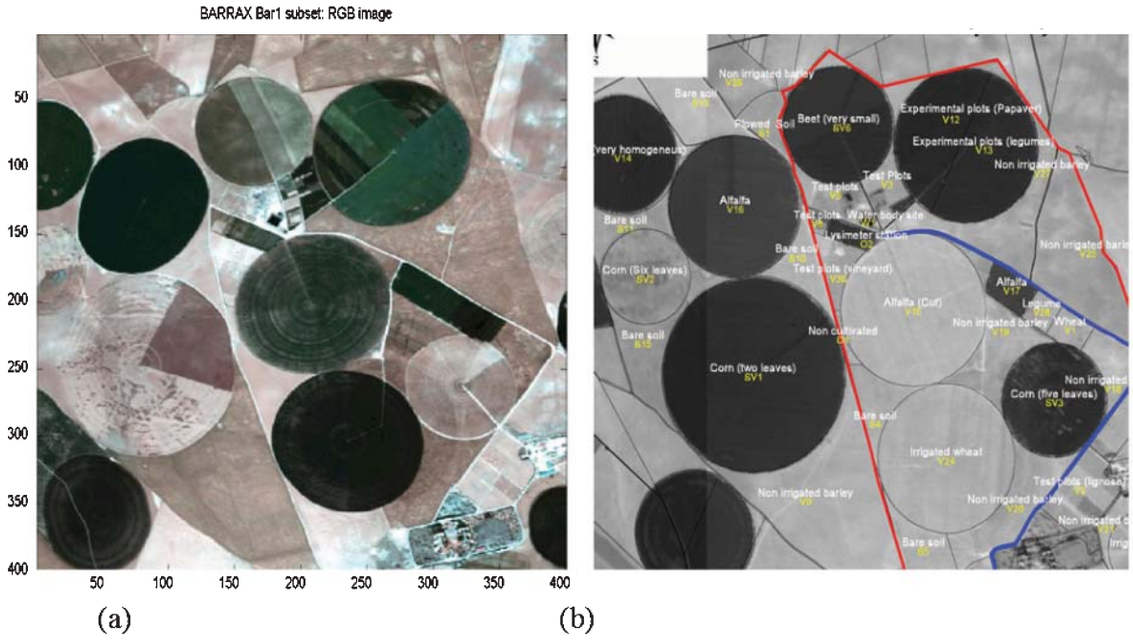
The impact of atmosphere effects on hyperspectral remote sensing can be readily assessed via the differential spectral contrast of the measured image and the corresponding atmospheric corrected data:

$$d^{\rho}{}_{i,j}(\lambda) = (\rho_i(\lambda) - \rho_j(\lambda)) / \rho_i(\lambda) \quad \& \quad d^{S}{}_{i,j}(\lambda) = (S_i(\lambda) - S_j(\lambda)) / S_i(\lambda)$$
$$D_{i,j}(\lambda) = \left| d^{\rho}{}_{i,j}(\lambda) - d^{S}{}_{i,j}(\lambda) \right|$$
$$A_{i,j} = \int D_{i,j}(\lambda) d\lambda \qquad (1)$$

where $S_i(\lambda)$ and $S_j(\lambda)$, are the at-sensor radiance spectra of two materials in close vicinity to each other, and $\rho_i(\lambda)$ and $\rho_j(\lambda)$ are the corresponding atmospheric corrected reflectance spectra. Thus $d^{\rho}{}_{i,j}(\lambda)$ and $d^{\rho}{}_{i,j}(\lambda)$ represent the spectral contrast of materials i,j for the reflectance and radiance data respectively. $D_{i,j}(\lambda)$ represents the differential spectral contrast for the radiance (measured) and reflectance (atmospheric corrected) of materials i,j. The impact of atmospheric effect can then be readily obtained using a wavelength integrated differential spectral contrast and is represented by $A_{i,j.}$

3.2 Hyperspectral data sets

Two sets of hyperspectral data taken by HyMap sensors were processed in this study (Schlapfer *et al.*, 1998, Yuen, 2004b). One set was obtained from a trial that involved military targets, and the other was a vegetation scene. Due to security reasons, the results of the military data set cannot be presented here. The other non-military data was obtained during the ESA DAISEX 1999 campaign (Digital Airborne Imaging Spectrometer Experiment) acquired on 3 June 1999 near Barrax, Spain. Results from both sets of data were found to be very consistent with each other. Figure 1(a) presents the RGB image of the Barrax sub-scene and Figure 1(b) shows the land use map of the scene. The data was taken by a HyMap sensor which records 128 channels in the 400-2500 nm range and has a 61 degree field-of-view. The geographic coordinate of the scene is N 39.08°, W 2.09°. The flight altitude was 4 km above the sea level and the ground elevation was 0.7 km. The scene was recorded at 11:54 UTC with a flight heading of 180°. The solar geometry was calculated from the geographic information for the time when the experiment was performed. To verify the accuracy of the correction method, ground reflectance measurements were performed with a FieldSpec FR spectroradiometer and atmospheric measurements with a Licor 1800 sun photometer.

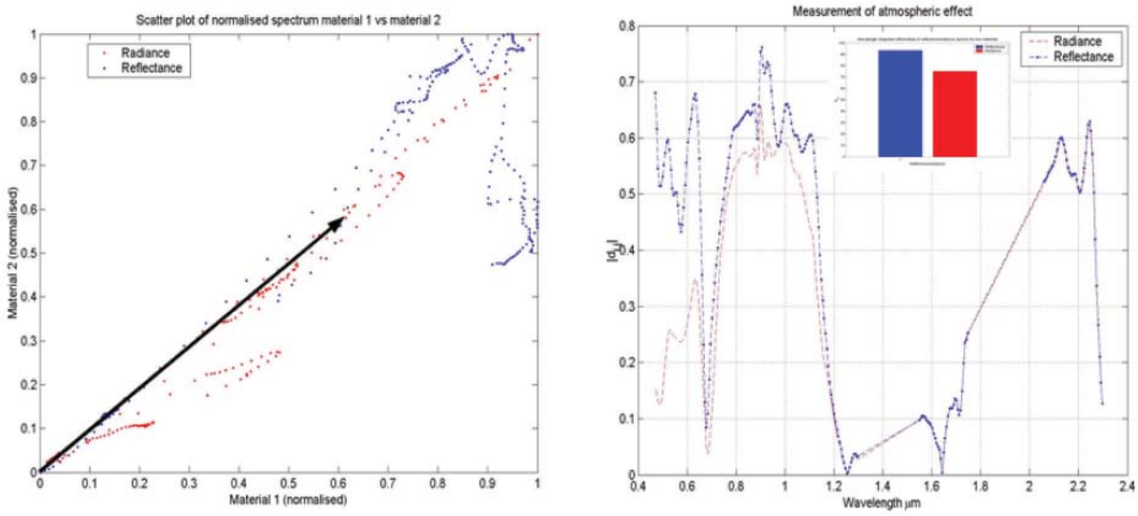


(a) (b)

Figure 1: (a) The RGB image of the Barrax scene. (b) The land use map.

3.3 Experiments: differential spectral contrasts

Figure 2(a) compares the scatter plots of two materials selected from the scene for their radiance (red dots) spectra against their corresponding reflectance (blue dots) data, on a normalised basis. The atmospherically corrected data, shown in blue, deviates more strongly from the line of equality, indicated by the arrow, demonstrating that the spectral differences between the two materials are somewhat greater when the spectra which is presented in the reflectance mode.



(a) (b)

Figure 2: (a) Scatter plot of two materials selected from the scene: radiance data (in red) and reflectance data (in blue). (b) A typical spectral contrast of a pair of materials and their wavelength integrated contrast (inset).

Plots of $d^S_{i,j}(\lambda)$ and $d^\rho_{i,j}(\lambda)$ against the wavelength of these two materials are shown in Figure 2(b). It can be seen that the two sets of data are remarkably similar above a wavelength of about 1.5 μm. However, below 1.2 μm, the values of $d^S_{i,j}(\lambda)$ are substantially smaller than those of $d^\rho_{i,j}(\lambda)$. The wavelength integrated spectral contrasts are shown in the inset of the figure. The integrated $d^\rho_{i,j}(\lambda)$ is about 25% larger than the corresponding integrated $d^S_{i,j}(\lambda)$, showing that the spectral contrast between these two materials is much larger in the atmospherically corrected spectra. Similar results were obtained by repeating the procedure using other pairs of materials selected from the scene. The average atmospheric effect on the data can be estimated by calculating the mean differential spectral contrast between N different pairs of materials selected from the scene:

$$D'(\lambda) = \sum_{i,j=1}^{N} \left\| d^{\rho}_{i,j}(\lambda) - d^{S}_{i,j}(\lambda) \right\| / N \tag{2}$$

Figure 3 shows a plot of the averaged spectral contrast $D'(\lambda)$ versus wavelength, along with the Rayleigh $1/\lambda^4$ scattering law. The proximity of these two plots indicates that the effect of the atmosphere in the short wavelength region is almost dominated by Rayleigh scattering due to air molecules. The average of $A_{i,j}$ for a set of materials selected from the scene has been found to be about 20%. This result shows that larger spectral contrast across a scene, can be achieved using an atmospherically corrected image, in good agreement with the previous study using simulated data (Kaufman, 1986).

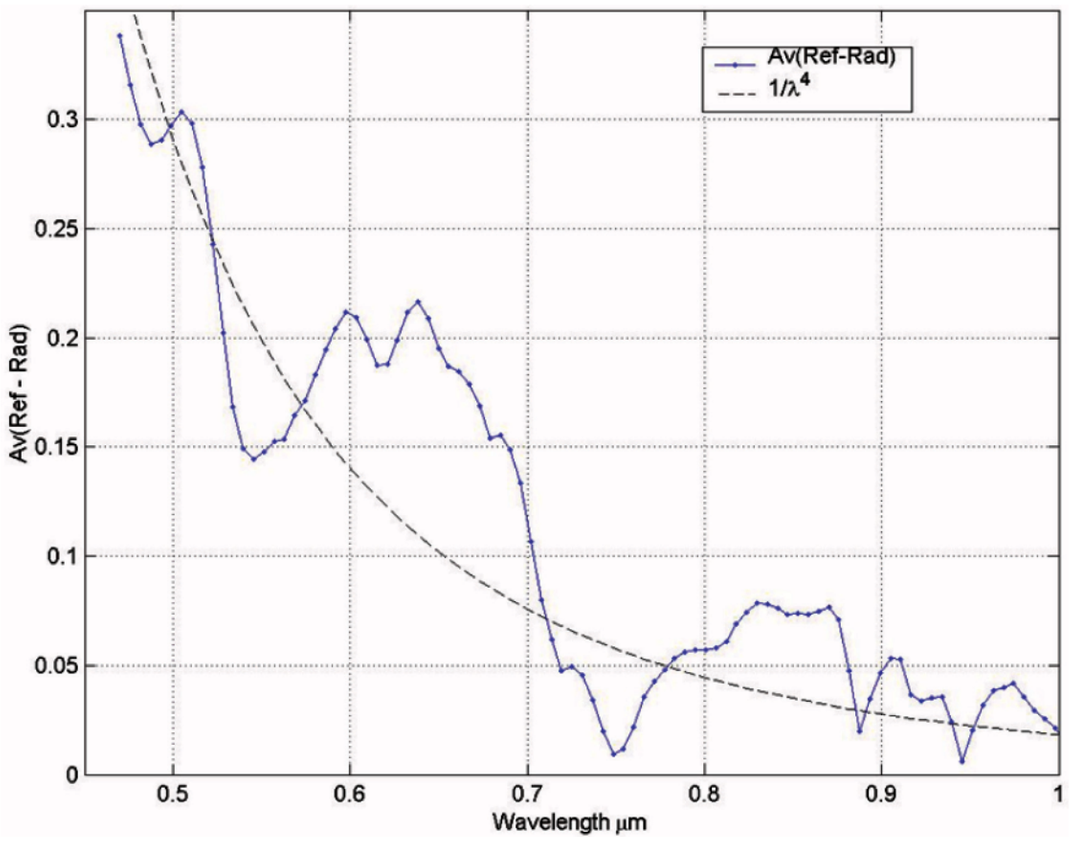


Figure 3: The averaged differential spectral contrast between the radiance and reflectance spectra for a set of pairs of materials selected from the scene. The dashed line depicts the $1/\lambda^4$ dependence.

This improvement of spectral contrast can be seen visually from the false colour image of the scene as shown in Figure 4. The raw data (Figure 4(a)) exhibits a touch of thin haze over the entire scene, typically due to path radiance. Figure 4(b) presents the same data after AC by ATCOR. The figures shown were displayed using the ENVI© package using bands (21, 9, 3) to represent the RGB colours. No stretching or any visual effect had been used throughout this study and the data shown was the entire true information of the data. The atmospherically corrected image (Figure 4(b)) exhibits both a slightly sharper image, and increased visibility of fine details, when compared to the raw measured data (Figure 4(a)). This is due to the removal of blurring and haze caused by adjacency and path radiance. The next question to ask is whether this spectral enhancement really improves classification and this issue is addressed in the next section.

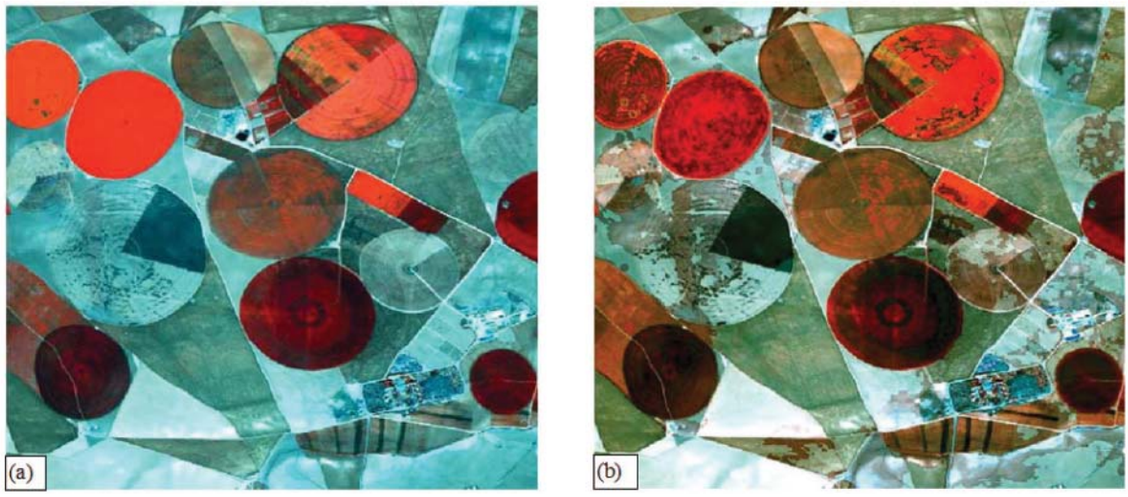


Figure 4: The enhancement of the image: (a) before and (b) after AC. This is a false colour map showing 3 bands of data to represent the RGB.

4 CLASSIFICATION/DETECTION ENHANCEMENT

The two sets of hyperspectral data processed in this study were of different types, and the military one was a relatively homogeneous forest scene, while the other consisted of various types of crops like alfalfa, wheat, barley, bare soil, vineyard and legume (Barrax data). The results for both data sets exhibit very consistent behaviour, and in this paper, we will present the Barrax data for illustration purpose.

Figure 5 shows the classification results of the Barrax scene using ENVI's *K*-means unsupervised classifier, using the radiance and atmospheric corrected (reflectance) data. Similar results had been obtained using another classifier (Isodata). Parameters for the *K*-means classifier were the same for both cases: classes=10, iterations=3, threshold=5%. Figures 5(a) and (b) display the classification results for the radiance and atmospheric corrected reflectance data, respectively. It is quite clear that the classification of the reflectance data (Figure 5(b)) shows substantially finer details than that of the radiance data. For instance, in the cut alfalfa area (labelled B in Figures 5(a) and (b)), a lot of bare soil and stem was exposed. This area had been classified into three different classes (blue, pale blue, light green) in the reflectance classification results, whereas it was labelled as only one class (blue) in the radiance data.

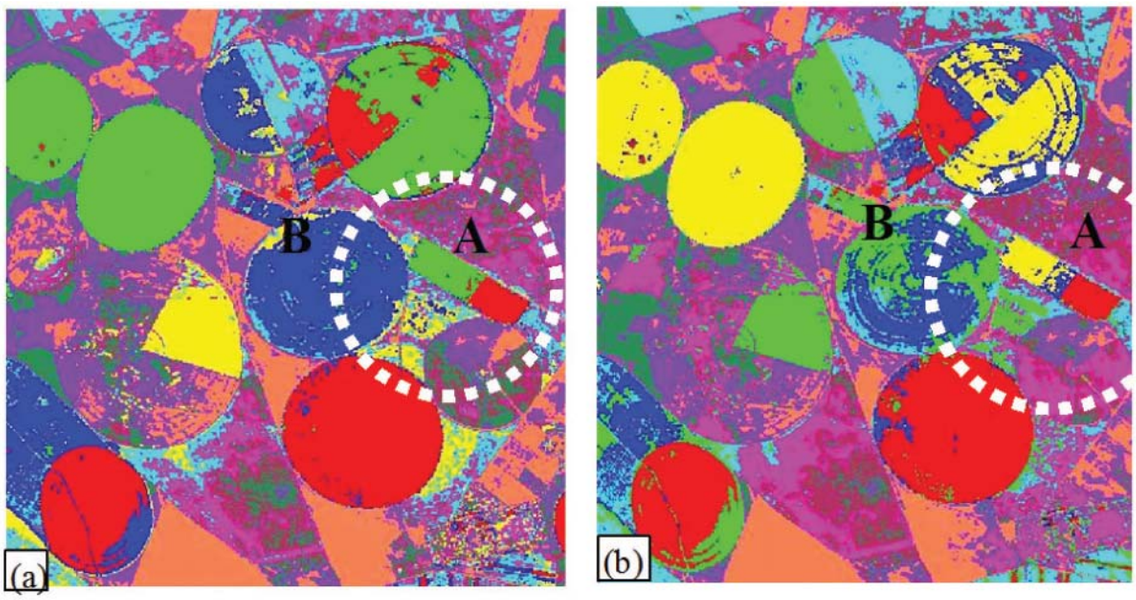


Figure 5: *K*-means unsupervised classification result for the non-military Barrax data. (a) Radiance data. (b) Atmospheric corrected reflectance data. This is a false colour map representing individual classes in different colours. Note that there is no relationship between the colour assignment for the results presented in (a) and (b).

Furthermore, in the circled area A shown in Figures 5(a) and (b), the land use map indicates the existence of three different crops: alfalfa, legume and wheat (Figure 6(a)). The classification map obtained from the reflectance data for this area (Figure 6(c)) shows the identification of these three crops correctly, but the classification map obtained from uncorrected at-sensor radiance data has identified two types of crops in this area, and completely mis-classified the legume to be the same as the alfalfa (Figure 6(b)).

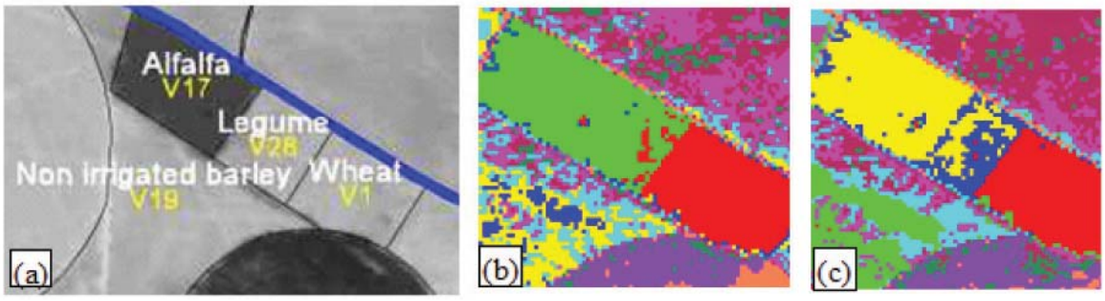


Figure 6: (a) Land use map of area A. (b) & (c) Classification results of area A for the at-sensor radiance and reflectance data respectively. Note that the same *K*-means classification manages to distinguish the legume and alfalfa only from the reflectance data but not using the radiance image (b).

These results give support to the conclusion from the military data (not presented here) that AC can improve the separation of classes and enhance detectability. However, it is important to assess the accuracy of AC, and whether it retrieves correctly the intrinsic spectral properties of the surface.

5 ACCURACY OF ATMOSPHERIC CORRECTION (AC)

The AC adopted in this study is a model-based technique and its accuracy depends very much on the factors such as how the sensor is calibrated, as well as the accuracy of ancillary information such as solar geometry. It is very difficult, if not impossible, to generalise the accuracy of the technique for different kinds of scene under all weather conditions. Here, a set of data is presented only to highlight the degree of accuracy that AC could achieve for retrieving intrinsic information of the surface. The details of its robustness and other parameter dependency will be published in a forthcoming paper.

Table 1: The percentage error of the wavelength integrated reflectance of four materials predicted by ATCOR, compare with that of the ground measurements.

Wavelength integrated reflectance error (%)				Abs. Mean error (%)
Material 1	Material 2	Material 3	Material 4	
-7.8	1.4	-3.6	1.9	3.7

To investigate the degree of accuracy achievable using AC, four spectral profiles were selected from different locations in the scene and compared with that of ground truth data. The scene was atmospherically corrected using one of the ground truth data sets to calibrate the sensor. It is observed that all the atmospherically corrected spectra showed close agreement with the ground measurement data and a typical result for one of the ground materials (soil) is shown in Figure 7. In order to evaluate the degree of accuracy quantitatively, the reflectance data was integrated over wavelength to obtain the surface albedo. All water absorption peaks were removed before the integration, and the results are shown in Table 1. Of the four calibration panels studied, it was found that the best and the worst albedo predicted by ATCOR were about 2% and 8% in error respectively, by comparison with the ground truth data. The mean albedo error for these four calibration panels was about 4%. This is an excellent result, given that the exact atmospheric condition of the scene at the time of the experiment was completely unknown.

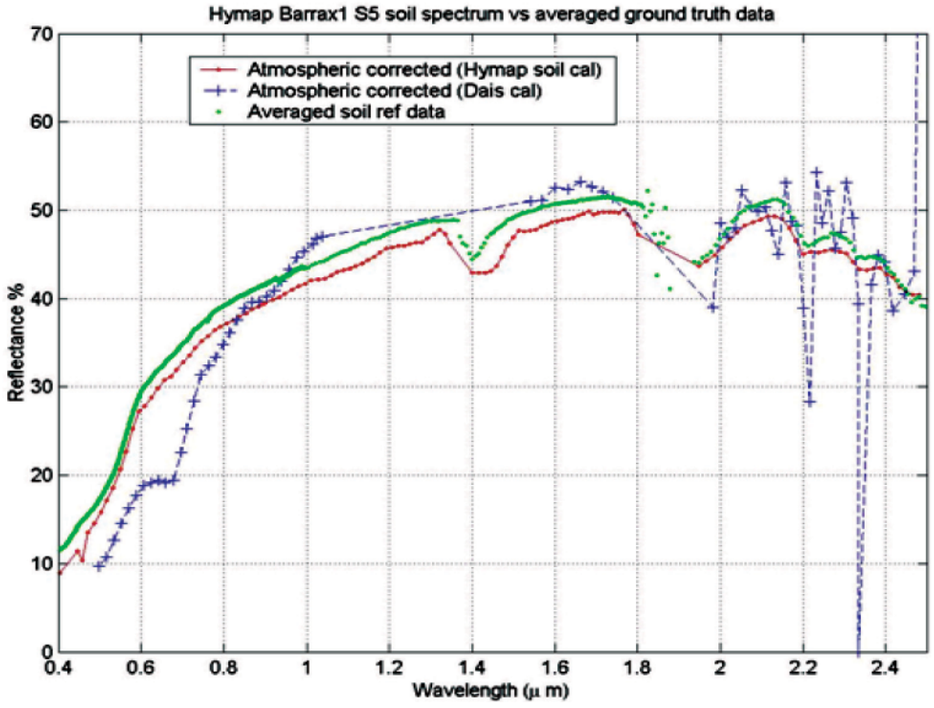


Figure 7: The predicted reflectance (red) of one of the ground materials and compare with the ground truth (green dots).

These results thus shows that AC can achieve a high degree of accuracy within 5% of error, provided that reliable ground measurement data is available for sensor calibration (Yuen, 2004b; Yuen *et al*., 2004c). The experiment also reveals that this accuracy is weakly dependent upon the input atmospheric model employed and also small number of noisy bands (~10%) can be accommodated.

6 CONCLUSIONS

This study has demonstrated how atmospheric correction (AC) enhances the spectral contrast of the remote sensing hyperspectral imagery and this was demonstrated using real data, with an enhancement in the order of 20%, when compared with the uncorrected at-sensor radiance data. The results indicate that AC can improve classification accuracy rather significantly. In one case the improvement was almost a factor of 10 or better. The analysis shows that AC can permit the retrieval of intrinsic information about remote surfaces when accurate ground measurements of calibration panels are available for sensor calibration. The accuracy achieved is about 5% of error.

Although the results cannot be generalised because of the small amount of data analysed, this study has consistently shown that AC can, not only remove local image variability, but also lead to the enhancement of target detectability. On this basis it is suggested that AC is a valuable technique to be employed in hyperspectral target detection, particularly when employing methods, which rely on library data for signature matching.

ACKNOWLEDGEMENTS

The authors would like to thank the DTC EMRS for their financial support during the course of this work. Also, thanks to Drs R Richter and his colleagues at DLR for technical support on ATCOR and the supply of DAISEX data. Thanks to Drs P. Clare, W. Oxford and V. Wilkinson of DSTL for their interest in this work. II (Izzati Ibrahim) would like to thank the Science & Technology Research Institute for Defence, Ministry of Defence, Malaysia, for the provision of her studentship, AT would like to thank EPSRC for the DTA grant and TC, KH & FK would like to thank the DCMT internal funding for the provisions of their studentships.

REFERENCES

Jensen, J.R. (1986). Introductory Digital Image Processing: A Remote Sensing Perspective. Prentice-Hall, New Jersey.

Kaufman Y.J. (1985). The atmospheric effect on the separability of field classes measured from satellites. *Remote Sens. Environ*., **18**: 21-34.

Richter R. & Schlapfer D. (2002). Geo-atmospheric processing of airborne imaging spectrometry data. Part 2: Stmospheric/topographic correction. *Int. J. Remote Sensing* **23**:2631-2649.

Schlapfer D., Borel, C.C, Keller, J. & Itten, K.I (1998). Atmospheric precorrected differential absorption technique to retrieve columnar water vapour'. *Remote Sens. Environ*. **65**: 353-366.

Yuen, P. & Bishop, G. (2004a). Enhancements of target detection using atmospheric correction preprocessing techniques in hyperspectral remote sensing. *SPIE proceeding: Military Remote Sensing, London,* **5613**:111-118.

Yuen, P. (2004b). Atmospheric correction preprocessing for hyperspectral target detection', *DTC EMRS Report No.: EMRC-HAD-03*.

Yuen, P., Killey, A., Hobson, S. & Bishop, G. (2004c). Atmospheric correction preprocessing techniques in Hyperspectral remote sensing. *1st EMRS DTC Conference, Edinburgh*, **B15**.

VULNERABILITIES OF CIVILIAN GLOBAL NAVIGATION SATELLITE SYSTEMS (GNSS) SIGNALS: A REVIEW

Dinesh Sathyamoorthy

Instrumentation and Electronic Technology Division
STRIDE, Ministry of Defence, Malaysia
Tel: 603-87324431
Fax: 603-87348695
E-mail: dinsat60@hotmail.com

Abstract

Global Navigation Satellite Systems (GNSS) are being increasingly used for a variety of important applications, including public safety services (police, fire, rescue and ambulance), marine and aircraft navigation, vehicle theft monitoring, cargo tracking, and critical time synchronization for utility, telecommunications, banking and computer industries. At present, there are two types of GNSS signals; military GNSS signals (L1 P(Y) and L2 for the case of GPS, and high precision (HP) for GLONASS) and civilian GNSS signals (L1 coarse acquisition (C/A) for GPS, and standard precision (SP) for GLONASS). Usage of L1 P(Y) and L2, and HP signals are limited to the US and Russian militaries respectively. Other users only have access to civilian GNSS signals. Usage of civilian GNSS signals is growing rapidly due the quality of service provided by GNSS, ease of use and low user cost. However, unlike military GNSS signals, civilian GNSS signals are unencrypted and unauthenticated, making them vulnerable to jamming and spoofing (also known as counterfitting or meaconing). Jamming and spoofing of civilian GNSS signals are surprisingly simple to conduct by even relatively unsophisticated adversaries. Jamming refers to the blocking of GNSS signals, rendering GNSS receivers in the affected areas inoperable, while spoofing refers to forging and transmission of navigation messages in order to manipulate the navigation solutions of GNSS receivers. Jamming is not surreptitious and affects both civilian and military GNSS signals, while spoofing is surreptitious and primarily affects civilian GNSS signals; military GNSS signals are less affected by spoofing as they are encrypted and authenticated. Due to the increasing reliance of various industries on GNSS, the consequences of GNSS service disruption can be severe, in terms of safety, environmental and economic damage. Hence, GNSS vulnerability mitigations steps should be given emphasis, including navigation/positioning/timing backups, making full use of ongoing GNSS modernization programs, integrity monitoring and augmentation, and anti-jamming and counter-spoofing technologies. This article is aimed at reviewing the vulnerabilities of civilian GNSS signals to jamming and spoofing, and the steps that need to be taken to mitigate these vulnerabilities.

Keywords: *Global Navigation Satellite Systems (GNSS); jamming; spoofing; GNSS vulnerability mitigation.*

1 INTRODUCTION

Global Navigation Satellite Systems (GNSS) are being increasingly used for a variety of important applications, including public safety services (police, fire, rescue, and ambulance), marine and aircraft navigation, vehicle theft monitoring, cargo tracking, and critical time synchronization for utility, telecommunications, banking and computer industries. The US Navigation Satellite Timing and Ranging (NAVSTAR) Global Positioning System (GPS), its Russian counterpart, *Global'naya Navigatsionnaya Sputnikovaya Sistema* (GLONASS), and the upcoming European Galileo system and China's Compass system transmit GNSS signals bearing reference information from the corresponding constellation of satellites. Any receiving device with the appropriate equipment can

decode the signals and utilize the GNSS information to determine its own location (Kaplan & Hegarty, 2006; Gakstatter, 2008a).

Each GNSS receiver is able to receive simultaneously a set of navigation messages, one message from each satellite in the visible satellite constellation. The navigation messages enable each receiver to determine its own position in a Cartesian system, as well as a time correction offset to add to its local clock value in order to maintain the current global time. At least four satellites should be visible so that the receiver can compute the location and time correction offset, with the two quantities together termed as the navigation solution (Kaplan & Hegarty, 2006; Gakstatter, 2008a).

At present, there are two types of GNSS signals; military GNSS signals (L1 P(Y) and L2 for the case of GPS, and high precision (HP) for GLONASS) and civilian GNSS signals (L1 coarse acquisition (C/A) for GPS, and standard precision (SP) for GLONASS). Usage of L1 P(Y) and L2, and HP signals are limited to the US and Russian militaries respectively. Other users only have access to civilian GNSS signals (Kaplan & Hegarty, 2006; Gakstatter, 2008a). Usage of civilian GNSS signals is growing rapidly due the quality of service provided by GNSS, ease of use and low user cost. In addition to obvious positioning and navigation applications, GNSS-based timing synchronization is being increasingly employed, such as timing reference for power station grids, telecommunications systems and digital air-ground communications systems (GAO, 2009; Jewell, 2009). Due to the increasing reliance of various industries on GNSS, the consequences of GNSS service disruption can be severe, in terms of safety, environmental and economic damage.

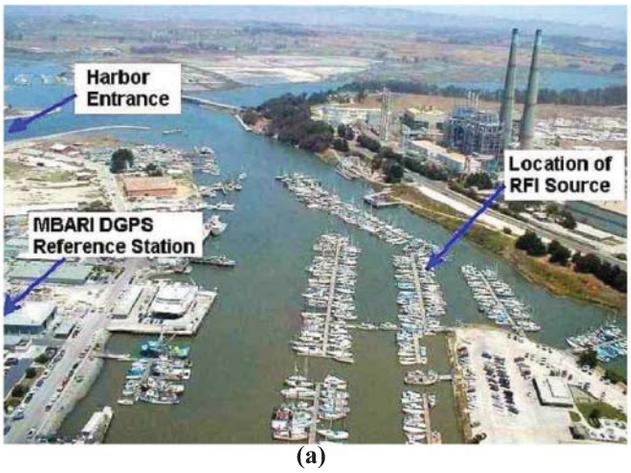
Unlike military GNSS signals, civilian GNSS signals are unencrypted and unauthenticated, making them vulnerable to jamming and spoofing (also known as counterfitting or meaconing). Jamming and spoofing of civilian GNSS signals are surprisingly simple to conduct by even relatively unsophisticated adversaries. Jamming refers to the blocking of GNSS signals, rendering GNSS receivers in the affected areas inoperable, while spoofing refers to forging and transmission of navigation messages in order to manipulate the navigation solutions of GNSS receivers. Jamming is not surreptitious and affects both civilian and military GNSS signals, while spoofing is surreptitious and primarily affects civilian GNSS signals; military GNSS signals are less affected by spoofing as they are encrypted and authenticated (Johnston & Warner, 2004; Papadimitratos & Jovanovic, 2008; Last, 2008; IDA, 2009). This article is aimed at discussing the vulnerabilities of civilian GNSS signals to jamming and spoofing, and the steps that need to be taken to mitigate these vulnerabilities.

2 JAMMING

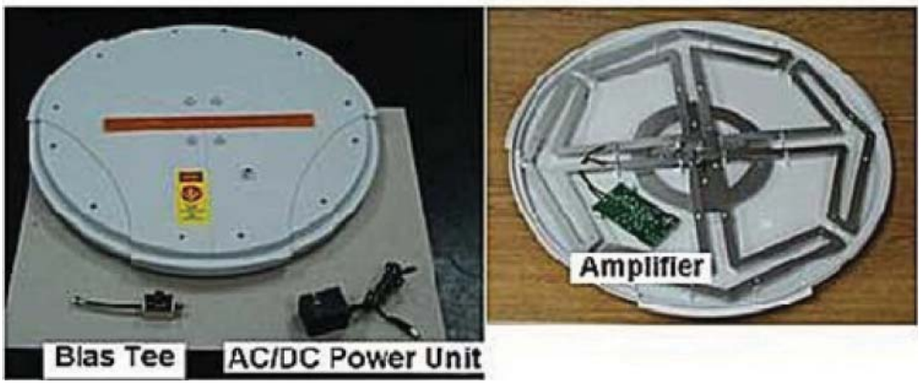
Jamming is defined as the broadcasting of a strong signal that overrides or obscures the signal being jammed (DOA, 2009; JCS, 2007; Poisel, 2002). Since GNSS satellites, powered by photocells, are approximately 20,200 km above the Earth surface, GNSS signals that reach the Earth have very low power (10^{-16} W), rendering them highly susceptible to jamming (Pinker & Smith, 2000; Adams, 2001; Johnston & Warner, 2004; Papadimitratos & Jovanovic, 2008; Last, 2008; IDA, 2009). For example, a simple 1 W battery-powered jammer can block the reception of GNSS signals approximately within a radius of 35 km from the jammer (Papadimitratos & Jovanovic, 2008). Even military GNSS signals are susceptible to jamming, as highlighted by the August 2000 Greek tank test incident (discussed in Adams (2001)) and the January 2007 San Diego communications jamming exercise incident (discussed in Jewell (2007)). Furthermore, as GNSS operates on line-of-sight (LOS) propagation between the GNSS satellites and GNSS receiver, blockage of the LOS propagation, such as by trees and buildings, and being indoors, can cause disruption (Volpe, 2001; Forssell, 2005; Kaplan & Hegarty, 2006; Gakstatter, 2008a). Available indoor navigation systems, such as assisted GPS (A-GPS), enhanced GPS (E-GPS) and pseudolites, have unstable accuracy and face difficulty operating in deep indoors (Manandhar *et al.*, 2008).

In 2001, the US Department of Transportation commissioned a report (Volpe, 2001) into the effects of GPS vulnerability on US transport systems. A similar report was commissioned in the United Kingdom (Harding, 2001). Both report that the most common form of GNSS jamming comes from

unintentional sources such as broadcast television, fixed and mobile VHF transmitters, personal electronic devices (PEDs), aeronautical satellite communications, mobile satellite services, ultra wideband (UWB) radar and communications, and natural phenomena such as ionospheric distortions, scintillations and solar weather effects. For example, in April – May 2001, GPS coverage in Moss Landing, California, was severely disrupted by a poorly designed television amplifier (Clynch *et al.*, 2003; Last, 2008) (Figure 1). The US Navy reported several occurrences of GPS antenna failures in proximity to high-power radars from nearby ships (Williams, 2006). The current 11-year solar cycle is expected to peak in 2012-2013 (NASA, 2006; Gakstatter, 2009), with expected strong storms that can cause severe GNSS disruptions for several hours (Oberst, 2006; Gakstatter, 2008b, 2009).



(a)



(b)

Figure 1: GPS coverage disruption in Moss Landing, California (April-May 2001): (a) The location of the jamming source. (b) The poorly designed television amplifier that caused the jamming. (Source: Last (2008))

Intentional jamming of GNSS signals is not difficult to achieve. The little jammer hidden on the dice shown in Figure 2 radiates 1 kW of power, which is enough to jam GNSS signals throughout a building or across a dock. Some jamming devices/techniques are available on the internet (Figure 3), and proliferation will continue because a single device that could disrupt military and civilian operations would be attractive to malicious governments and groups (Volpe, 2001; Last, 2008; IDA, 2009). In addition, unintentional or natural disruptions, such as produced by the ionosphere or unintentional RF interference, could be used by saboteurs to disguise their intentional disruption, at least to delay government response and warning (Volpe, 2001).

Figure 2: A GNSS jammer hidden on a dice.
(Source: Last (2008))

Figure 3: GNSS jammers found during casual browsing of the internet. The sources of the figures are not given for obvious reasons. Readers are reminded that GNSS jamming is illegal.

The accelerating worldwide dependence of various industries on GNSS makes mechanisms to disrupt GNSS signals potent weapons that many militarily sophisticated countries are actively pursuing. For example, the US military has a policy to block potential adversaries' access to the L1 signal while preserving its ability to utilize the L2 signal, without unduly disrupting or degrading civilian GPS applications outside the area of conflict (DOD/DHS/DOT, 2008; Volpe, 2001). The effort to develop GPS disruption systems for this purpose is known as navigation warfare (NAVWAR). From time to time, the US military conducts NAVWAR exercises which disrupt GNSS coverage within the affected areas. However, the US Department of Defense (DOD), Department of Homeland Security (DHS) and Department of Transport (DOT) have developed mechanisms to coordinate times and places for testing, and to notify users in advance (DOD/DHS/DOT, 2008). However, it is apparent that notifications of these tests do not reach enough GNSS user communities, resulting in numerous GNSS disruption incidents (Volpe, 2001; Last, 2008).

3 SPOOFING

Spoofing signals can be generated by GNSS simulators, equipment which is available today. The received power of the spoofing signal should exceed that of the legitimate signal, this being essentially a form of jamming. The receiver then operates with the forged signal as the input and computes the location induced by the spoofer (Johnston & Warner, 2004; Papadimitratos & Jovanovic, 2008; Last, 2008; Humphreys *et al.*, 2009; IDA, 2009). Spoofing is more sinister than intentional jamming because the targeted receiver cannot detect a spoofing attack and hence, cannot warn users that its navigation solution is untrustworthy. While spoofing is more difficult to achieve than jamming, in many cases even if a spoofer is not fully successful, he/she can still create significant errors and jam GNSS signals over large areas (Volpe, 2001; Last, 2008; Humphreys *et al.*, 2009).

A number of GNSS simulators (Figure 4) have been designed for legal purposes such as user training, system maintenance, vehicle motion simulation, and, ironically, anti-jamming testing. However, in the wrong hands, these GNSS simulators can be used to conduct illegal spoofing. Furthermore, GNSS simulators can be built with relatively low cost equipment (Figure 5), as demonstrated by Rogers (1991), Johnston & Warner (2004), Humphreys *et al.* (2008) and Hanlon *et al.* (2009).

(a) **(b)**

(c) **(d)**

Figure 4: Commercially available GNSS simulators: (a) Cast Navigation's CAST EMT3500-3 EGI (b) Areoflex's GPS-101 Global Positioning Simulator (c) GPS Creations' GPS-RT (d) Flightspectrum's Elite Basic Training Device PI-135 makes use of Garmin's G1000 GPS Simulator.

Figure 5: A homemade GNSS simulator.
(Source: Johnston & Warner (2004))

The spoofing threat continuum can be divided into three categories; simplistic, intermediate, and sophisticated (Hanlon *et al.*, 2009; Montgomery *et al.*, 2009) (Figure 6). Simplistic attacks are conducted using standalone GNSS simulators. The menace posed by such attacks are diminished by the fact that most GNSS simulators are heavy and cumbersome, and that it is likely easy to detect because of the difficulty of synchronizing a simulator's output with the GNSS signals in its vicinity. An unsynchronized attack effectively acts like GNSS jamming, and may cause the victim receiver to lose lock and have to undergo a partial or complete reacquisition, raising suspicion of a spoofing attack.

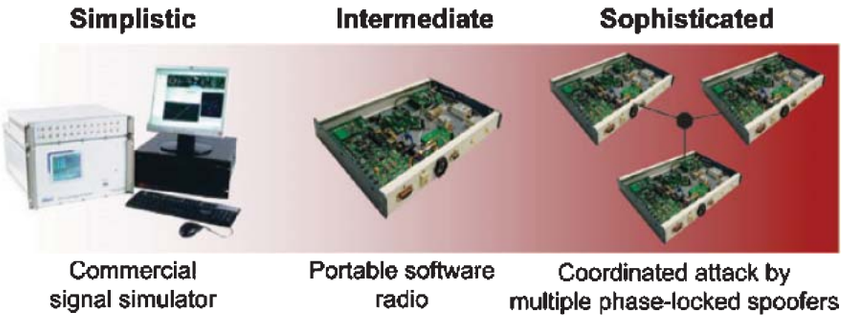


Figure 6: The spoofing threat continuum; simplistic, intermediate and sophisticated spoofing attacks. (Source: Hanlon *et al.* (2009))

Intermediate attacks make use of portable receiver-spoofers, which can be made small enough for inconspicuous placement near the target receiver's antenna. The receiver component draws in genuine GNSS signals to estimate its own position, velocity and time. Based on these estimates, the receiver-spoofer then generates counterfeit signals and generally orchestrates the spoofing attack. The portable receiver-spoofer could even be placed somewhat distant from the target receiver if the target is static and its position relative to the receiver-spoofer had been pre-surveyed. While there are no commercially available portable receiver-spoofer devices, advances in radio frequency (RF) software-defined technologies could see a proliferation of such devices. The only known civilian GNSS equipment based countermeasure that would be completely effective against an attack launched from a portable receiver-spoofer with a single transmitting antenna is multi-antenna angle-of-arrival discrimination. With a single transmitting antenna, it would be impossible to continuously replicate the relative carrier phase between two or more antennas of an appropriately equipped target receiver.

Sophisticated attacks thwart angle-of-arrival defence by a coordinated attack with as many receiver-spoofers as antennas on the target receiver. This type of attack inherits all of the challenges of mounting a single receiver-spoofer attack, with the additional expense of multiple receiver-spoofers and the additional complexity that the perturbations to the incoming signals must be phase-coordinated. Thus, an attack via multiple phase-locked portable receiver-spoofers is somewhat less likely than an attack via single portable receiver-spoofer, but may be impossible to detect with civilian GNSS equipment based spoofing defences, as the only known defence against such an attack is cryptographic authentication.

4 MITIGATION OF GNSS VULNERABILITIES

Given the dependence of various industries on GNSS systems, GNSS disruption could prove to be problematic, if not disastrous, as demonstrated in the incidents highlighted by Adams (2001), Clynch *et al.* (2003) and Jewell (2007). Hence, effective mitigation of GNSS vulnerabilities is required in order to avoid such chaotic scenarios.

The most recommended mitigation step is the application of navigation/positioning backups which can be used in the case of GNSS disruptions (Volpe, 2001; Lilley, 2006; Last, 2008). Navigation backups, such inertial navigation systems (INS), enhanced long range navigation (eLORAN) and VHF omnidirectional range distance measuring equipment (VOR/DME), have the potential to take over seamlessly when GNSS fails, and can be used as a deterrent against spoofing. Recent operational GNSS jamming tests have shown that eLORAN is a highly effective navigation backup in cases of GNSS failure (Basker *et al.*, 2008; GPS World, 2009a; Grant *et al.*, 2009) (Figure 7). An Independent Assessment Team (IAT) report (IDA, 2009), commissioned by the US DOT, recommended that the US government commit to eLoran as the national backup to GPS for the next 20 years. In addition, applications relying on GNSS-based time synchronization should employ suitable timing backups, such as internet time services, network time protocols, and if viable, atomic clocks.

Figure 3-3: Google Earth™ Plot of valid GPS data from DGPS Receiver B. When comparing the reported position (red circle) against the eLoran position (green square) for the same time, one can see an error of 22Km with the reported DGPS Receiver B position being on land. (Colours indicate reported speed: blue <15knts, yellow< 50knts, orange <100knots and red >100knts)

Figure 7: The General Lighthouse Authorities (GLAs) of the United Kingdom and Ireland conducted a GPS jamming exercise from 31st March to 4th April 2008 to investigate the performance of eLoran during GPS service denial. It was reported that eLoran was unaffected by GPS jamming and demonstrated an accuracy of 8.1 m (95%).
(Source: GPS World (2009a))

In order to be able to provide accurate indoor position determination for public and commercial services, such as search-and-rescue, firefighting and location based services (LBS), it has been proposed that indoor positioning transmitters be employed to the solve the GNSS indoor availability issue. The receiver will use GNSS signals outdoors in the usual way, while using signals from transmitters indoors, where GNSS signal quality is strongly reduced. The indoor transmitter signal structure is similar to that of GNSS signals, except for the contents of the navigation message. Thus, the same receiver can be used for both outdoor and indoor applications. Recent indoor positioning technologies include Locata Corporation's LocataNet (Locata, 2003; Barnes *et al.*, 2003), and the Japan Aerospace Exploration Agency's (JAXA) Indoor Messaging System (IMES) (Satoshi *et al.*, 2008; Manandhar *et al.*, 2008) (Figure 8).

(a) **(b)**

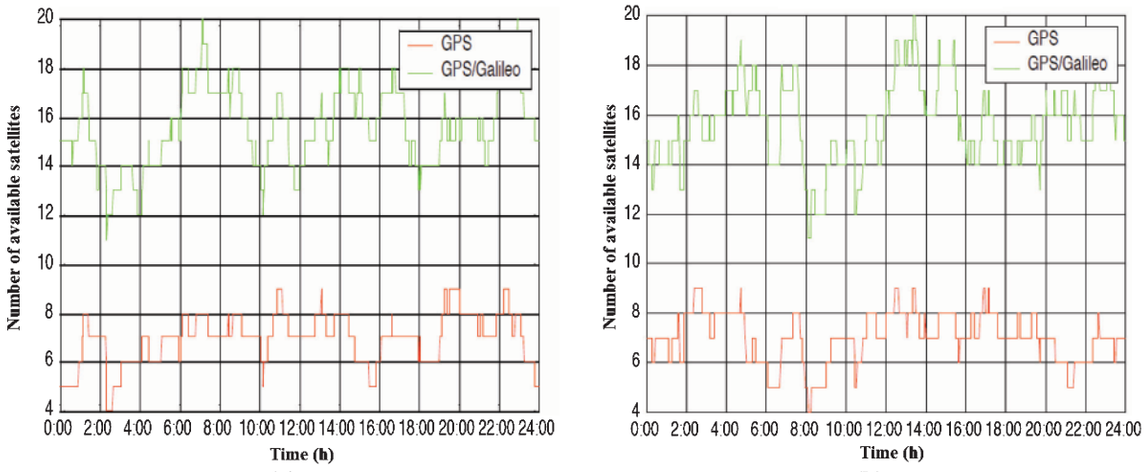
Figure 8: Indoor demonstration of IMES at an underground parking area.
(Source: Manandhar *et al.* (2008))

However, in order for these systems to provide reliable and accurate indoor positioning, the transmitters need to be very densely located in all indoor spaces where location is required, at separations of 20-30 m, requiring large investments in infrastructure (Demspter, 2009). Alternatives that has been proposed to provide cost-effective solutions include RFID (Hähnel *et al.*, 2004; Chang *et al.*, 2008), infrared (Muneyuki *et al.*, 2003; Kemppainen *et al.*, 2006), sensor networks (de Oliveira *et al.*, 2005; Fernandez *et al.*, 2007), and WiFi (Ekahau, 2008; Kawaguchi, 2009).

GNSS users should also take full advantage of the various ongoing GNSS modernization programs (McDonald, 2002; Blomenhofer, 2004; Alkan *et al.*, 2005; Gakstatter & Flick, 2006; Kaplan & Hegarty, 2006; Gibbons, 2006; 2008, 2009; Gakstatter, 2008a,c,d; GAO, 2009; Rizos, 2009). The upcoming new civilian GPS III signals that are to be provided, the L1C, L2C and L5 signals, will be able provide a substantial reduction in the threat of unintentional jamming, and some degree of threat reduction from intentional jamming. With the more robust civil L5 signal (1,176 MHz) being far removed from the L1C ((1,575 MHz) and L2C (1,227 MHz) signals, it is extremely unlikely that unintentional jamming sources can jam all three signals simultaneously, and will be more difficult and costly for intentional jamming. The civilian GPS III signals, in particular the L5 signal, will also have significantly improved code structures that will allow the signals to be acquired and tracked better in tough GPS conditions, such as under tree foliage and extreme solar activity (McDonald, 2002; Gakstatter & Flick, 2006; DOD/DHS/DOT, 2008).

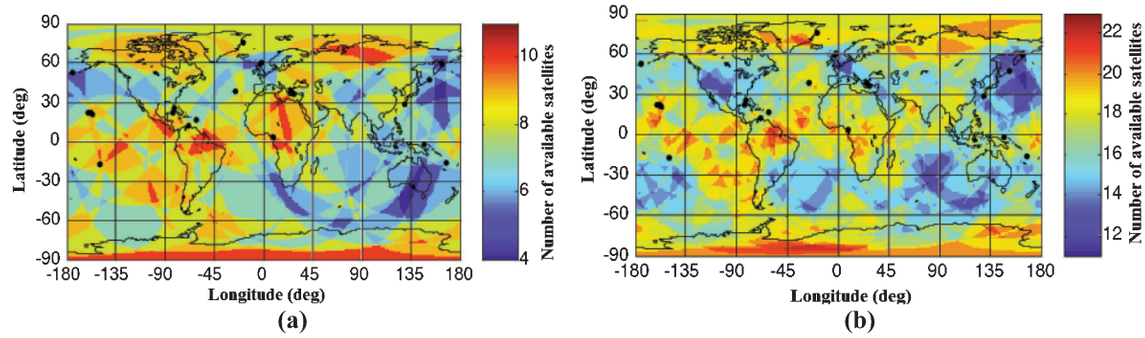
Galileo, which is a GNSS that has been targeted at commercial applications since its inception, is designed to have a 30-satellite constellation (27 operational plus 3 active spares), as well as a complement of groundstation equipment. There are many similarities between the proposed civilian Galileo (L1F, E5a and E5b) and GPS III (L1C, L2C and L5) signals. Galileo's performance is expected to be at least as good as civilian GPS, and some aspects are likely to be superior to GPS (including the onboard atomic clocks). Galileo also has a proposed integrity function that will be much more sophisticated than current GPS (although GPS III will be much improved in this area) (Blomenhofer, 2004; Kaplan & Hegarty, 2006; Gakstatter & Flick, 2006; Gakstatter, 2008c). Studies have also shown that with combined GPS and Galileo constellations, the overall navigation availability in urban areas (where high buildings obstruct the GNSS signals in downtown areas) can be improved from 55% to 95% (Alkan *et al.*, 2005). Using GNSS measurement simulations, Hewitson (2003) demonstrated the increased satellite availability of combined GPS/Galileo over two urban areas in Australia, Sydney and Portland (Figure 9), and worldwide (Figure 10). It can be anticipated that combined GPS/Galileo receivers will be the predominant equipment for critical GNSS applications, and they will also be employed by many massmarket users (Alkan *et al.,* 2005; Gakstatter & Flick, 2006; Gakstatter, 2008a,c,d).

Although GLONASS achieved its full operational capability in January 1996, when 24 GLONASS satellites were available for positioning and timing, its constellation had dropped to just 7 satellites by May 2001 due to decreases in the allocated maintenance budget. In August 2001, the Russian government approved a long-term plan to reconstitute a GLONASS constellation of 24 satellites by 2011 (Revnivykh, 2007, 2008; Sergey et al., 2007). As of 4th November 2009, there are 18 operational GLONASS satellites in orbit, the minimum required to allow for continuous navigation services covering the entire territory of the Russian Federation (GPS World, 2009b). It is expected that the minimum required constellation of 24 satellites will be completed by February 2010 (Inside GNSS, 2009). Due to the difference in signal pattern used by GLONASS (frequency division multiple access (FDMA)) compared to GPS and Galileo (code division multiple access (CDMA)), interoperability between the GNSS systems would require complex and costly receivers. It was reported that during the meeting of the GPS-GLONASS Interoperability and Compatibility Working Group (WG-1) in December 2006, the US and Russian governments made significant progress in understanding the benefits to the user community of changing the GLONASS signal pattern to one that is similar with GPS and Galileo, enabling simply-designed receivers to use the three GNSS systems simultaneously (GPS World, 2007). GLONASS will broadcast CDMA signals beginning with the GLONASS-K generation of satellites which is expected to begin launching in 2010 (Revnivykh, 2007, 2008).



(a) (b)

Figure 9: Satellite availability at (a) Sydney and (b) Portland over 24 hours for GPS and combined GPS/Galileo. The GNSS measurement simulations were carried out at a sample rate of 1 Hz commencing at 0:00 h on 16th January 2003.
(Source: Hewitson (2003))



(a) (b)

Figure 10: Worldwide satellite availability for (a) GPS and (b) combined GPS/Galileo. The results were obtained from snapshot simulations for 0:00 h on 16th January 2003 at 1 degree intervals of latitude and longitude and an altitude of 50 m. Snapshot results permit analysis based on spatial variations as time is held constant. The results from the global snapshot scenario are presented as orthographic global colour maps.
(Source: Hewitson (2003))

The incidents discussed in Adams (2001), Clynch *et al.* (2003) and Jewell (2007) indicate a serious inability to effectively identify and locate jamming sources. Systems and procedures to monitor, report and locate intentional and unintentional jamming sources should be put in place, especially for applications for which GNSS disruption is not tolerable. This should be coupled with a prompt field response to remove the jamming source as quickly as possible. Recent technologies in signal tracking and detection, such as Tektronix's H600 RF Hawk Signal Hunter (Tektronix, 2008) (Figure 11(a)), NAVSYS' High-Gain Advanced GPS Receiver (HAGR) (Brown *et al.*, 2000) (Figure 11(b)), and the Space and Naval Warfare Systems Center's (SPAWAR) Location of GPS Interferers (LOCO GPSI) (Simonsen *et al.*, 2004) (Figure 11(c)), should precipitate this.

The application of autonomous integrity monitoring of GNSS signals should also be looked into, such as receiver autonomous integrity monitoring (RAIM) used in the aviation and maritime industries (ION, 1998; Hewitson & Wang, 2006; Dufresne *et al.*, 2008). RAIM is a method which examines the internal consistency of a set of redundant measurements within the GNSS receiver to detect and remove a faulty measurement (a process known as fault detection and exclusion (FDE)). Navigational warning systems, such as Navigational Telex (NAVTEX) and Safetynet can also provide integrity warnings, but there may be delays in delivering such warnings by these methods (IALA, 2004).

(a) (b) (c)

Figure 11: Recent technologies in signal tracking and detection should allow for the fast and effective identification and location of intentional and unintentional jamming sources: (a) Tektronix's H600 RF Hawk Signal Hunter (b) NAVSYS' High-Gain Advanced GPS Receiver (HAGR) (c) Space and Naval Warfare Systems Center's (SPAWAR) Location of GPS Interferers (LOCO GPSI).

GNSS augmentations are required for several reasons, including improvement of accuracy and availability of integrity monitoring. Satellite Based Augmentation Systems (SBAS) determines GNSS integrity and differential correction data on the ground through a network of monitor stations and a central processing facility. Geostationary satellites are then employed to broadcast integrity messages and differential corrections, as well as a navigation message, via the civilian GNSS frequency. Following operational approval, the SBAS signal can then be used to improve GNSS accuracy, availability and integrity (Kaplan & Hegarty, 2006; Gakstatter, 2008a). Publically available SBAS systems, such as the US Federal Aviation Administration's (FAA) Wide Area Augmentation System (WAAS), the European Geostationary Navigation Overlay Service (EGNOS), and Japan's Multi-functional Satellite Augmentation System (MSAS), do not officially provide coverage in Malaysia. India's GPS Aided Geo Augmented Navigation (GAGAN), likely to be operational by May 2011, is expected to provide coverage to Malaysia (Suryanarayana Rao & Pal, 2004; Gakstatter, 2008a) (Figure 12).

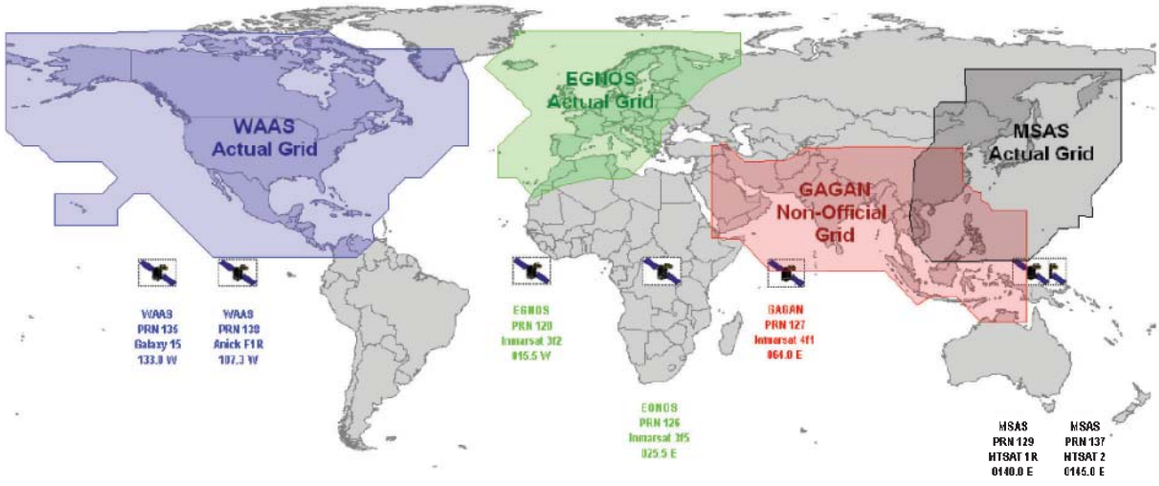


Figure 12: Coverages of various publically available SBAS systems.
(Source: Gakstatter (2008a))

Ground Based Augmentation Systems (GBAS), such as the US Local Area Augmentation System (LAAS), and Ground-based Regional Augmentation Systems (GRAS), such as Differential GPS (DGPS) networks available in many countries, consist of multiple reference antennas/receivers, a processing station and VHF/UHF data broadcast equipment. The GNSS signals received by the multiple reference/monitoring antennas are processed to obtain differential correction and integrity information, which are then broadcast via the VHF/UHF data link (Kaplan & Hegarty, 2006; Gakstatter, 2008a).

It should be noted that integrity monitoring and augmentation systems are dependent on GNSS for position indication and are not standalone services. They are therefore subject to interference, jamming and spoofing of GNSS, but may be able to provide a warning of malfunction (Volpe, 2001; IALA, 2004; Last, 2008).

In addition, continuous assessments should be made on the applicability of anti-jamming technologies, including adaptive antenna array, polarization discrimination and spatial-temporal filtering (Casabona & Rosen, 1999; Gustafon *et al.*, 2000; Deshpande, 2004; Loegering, 2006; Meng *et al.*, 2008), and counter-spoofing technologies, including amplitude discrimination, time-/angle-of-arrival discrimination and cryptographic authentication (Key, 1995; Wen *et al.*, 2005; Papadimitratos & Jovanovic, 2008; Humphreys *et al.*, 2009; Montgomery *et al.*, 2009; Ledvina et al., 2009).

5 CONCLUSION

Civilian GNSS signals are vulnerable to jamming, which blocks GNSS receivers from receiving navigation messages, and spoofing, which manipulates the location and time that the receivers compute. With increasing dependence on GNSS for positioning, navigation and timing synchronization, in order to avoid the possible consequences of intentional and unintentional attacks on GNSS signals, GNSS vulnerability mitigations steps should be given emphasis, including navigation/positioning/timing backups, making full use of ongoing GNSS modernization programs, increased ability to identify and locate GNSS jammers, integrity monitoring and augmentation, and anti-jamming and counter-spoofing technologies.

ACKNOWLEDGEMENT

The author is grateful to Dr. Mahdi Che Isa, Head of the Shipping Technology Branch, Science & Technology Research Institute for Defence (STRIDE), Mr. Eric Gakstatter, Principal, Discovery Management Group LLC, and Dr. Panagiotis Papadimitratos, Senior Researcher, Computer Communications and Applications Laboratory 1, École Polytechnique Fédérale de Lausanne (EPFL), Switzerland, for their suggestions that have helped improved this article.

REFERENCE

Adams, T.K. (2001). GPS Vulnerabilities. *Mil. Rev.*, **1**: 10-16.

Alkan, R.M., Kamman, H. & Sahin, M. (2005). GPS, GALILEO and GLONASS satellite navigation systems & GPS modernization. *2nd International Conference on Recent Advances in Space Technologies (RAST 2005)*, pp. 390-394.

Barnes, J., Rizos, C., Wang, J, Small, D., Voight, G. & Gambale, N. (2003). High precision indoor and outdoor positioning using LocataNet. *J. GPS*, **2**:73-82.

Basker, S., Grant, A., Williams, P. & Ward, N. (2008). The impact of GPS jamming on the safety of navigation. *Presentation to the Civil GPS Service Interface Committee*, 26th September 2008, Savannah, Georgia.

Blomenhofer, H., 2004. GNSS in the 21st century: The user perspective. *Acta Astronautica*, **5**: 965-968.

Brown, A., Atterberg, S. & Gerein, N. (2000). Detection and location of GPS interference sources using digital receiver electronics. *Proceedings of ION Annual Meeting*, June 2000, San Diego, California.

Casabona, M.M. & Rosen, M.W. (1999). Discussion of GPS anti-jam technology. *GPS Solut.*, **2**: 18-23.

Chang, C.C., Lou, P.C. & Chen, H.Y. (2008). Designing and implementing a RFID-based indoor guidance system. *J. GPS*, **7**: 27-34.

Clynch, J.R., Parker, A.A., Badger, G., Vincent, W.R., McGill, P. & Adler, R.W. (2003). The Hunt for RFI: Unjamming a Coast Harbor. Available online at: http://www.gpsworld.com/gpsworld/article/articleDetail.jsp?id=43404 (Last access date: 4th November 2009).

de Oliveira, H.A.B.F., Nakamura, E.F., Loureiro, A.A.F. & Boukerche, A. (2005). Recursive position estimation in sensor networks. *Proceedings of the 14th International Conference on Computer Communications and Networks 2005 (ICCCN 2005)*, pp. 557-562.

Dempster, A. (2009). QZSS's indoor messaging system: GNSS friend or foe? *Inside GNSS*, **4**:37-40.

Department of Army (DOA) (2009). Electronic Warfare in Operations. Army Field Manual 3-36, Department of Army, Washington D.C.

Department of Defense (DOD), Department of Homeland Security (DHS) & Department of Transport (DOT) (2008). 2008 Federal Radionavigation Plan. US Federal Government.

Deshpande, S.M. (2004). Study of Interference Effects on GPS Signal Acquisition. Masters thesis, University of Calgary, Calgary, Alberta.

Dufresne, C., Hansen, A., O'Neill, K., Parmet, J. & Volchansky, L. (2008). Global Positioning System (GPS) receiver autonomous integrity monitoring (RAIM) web service to support area navigation (RNAV) flight planning. *Institute for Navigation National Technical Meeting 2008*, 28th-30th January 2008, San Diego, California.

Ekahau (2008). Ekahau RTLS. Ekahau Inc., California.

Fernandez, T.M., Rodas, J., Escudero, C.J. & Iglesia, D.I. (2007). Bluetooth Sensor Network Positioning System with Dynamic Calibration. *4th International Symposium on Wireless Communication Systems 2007 (ISWCS 2007)*, 17th-19th October 2009, Trondheim, Norway.

Forssell, B. (2005). GPS/GNSS indoors: Possibilities and limitations. *GPS/GNSS Seminar of the Swedish National Survey*, March 2005, Gävle, Sweden.

Gakstatter, E. (2008a). Introduction to GNSS. *GNSS Technology Workshop*, 10th-12th December 2008, Institut Tanah Dan Ukur Negara (INSTUN), Behrang, Perak.

Gakstatter, E. (2008b). Solar Activity: Is There Aspirin for This GNSS Headache? Available online at: http://sc.gpsworld.com/gpssc/article/articleDetail.jsp?id=555255 (Last access date: 4th November 2009).

Gakstatter, E. (2008c). Is Dual-Frequency GPS — As We Know It — Becoming Obsolete? Available online at: http://sc.gpsworld.com/gpssc/ArticleStandard/Article/detail/521868 (Last access date: 4th November 2009).

Gakstatter, E. (2008d). So, You've Been Hearing About L5. Available online at: http://sc.gpsworld.com/gpssc/article/articleDetail.jsp?id=517961 (Last access date: 4th November 2009).

Gakstatter, E. (2009). Personal communication.

Gakstatter, E. & Flick, J. (2006). Navigating the World of GNSS. Available online at: http://www.geospatial-solutions.com/geospatialsolutions/Article/Navigating-the-World-of-GNSS/ArticleStandard/Article/detail/318856 (Last access date: 4th November 2009).

Gibbons, G. (2006). GNSS trilogy: Our story so far. Inside GNSS. *Inside GNSS*, **1**: 25-32.

Gibbons, G. (2008). GPS and regime changes: Part 1-The Bush legacy. *GNSS World*, **3**: 20-23.

Gibbons, G. (2009). GPS and regime changes: Part 2-What lies ahead. *GNSS World*, **4**: 20-27.

Grant, A., Williams, P., Ward, N. and Basker, S. (2009). GPS jamming and the impact on maritime navigation. *J. Navigation*, **62**: 173-187.

GPS World (2007). Radical Change in the Air for GLONASS. Available online at:

http://www.gpsworld.com/gnss-system/news/radical-change-air-glonass-4336 (Last access date: 4th November 2009).

GPS World (2009a). Maritime Jamming Trial Shows GPS Vulnerabilities: eLoran shown to be 95 Percent Accurate. Available online at: http://tl.gpsworld.com/gpstl/Latest+News/Maritime-Jamming-Trial-Shows-GPS-Vulnerabilities/ArticleStandard/Article/detail/584318?ref=25 (Last access date: 4th November 2009).

GPS World (2009b). Three GLONASS Satellites Set for October 29 Launch. Available online at: http://www.gpsworld.com/gnss-system/glonass/news/three-glonass-satellites-set-october-29-launch-9034 (Last access date: 4th November 2009).

Government Accountability Office (GAO) (2009). Global Positioning System: Significant Challenges in Sustaining and Upgrading Widely Used Capabilities. Report to the Subcommittee on National Security and Foreign Affairs, Committee on Oversight and Government Reform, House of Representatives, Government Accountability Office (GAO), U.S.

Gustafon, D., Dowdle, J. & Flueckiger, K. (2000). A high anti-jam GPS-based navigator. *Proceedings of the Institute of Navigation*, 28th-30th June 2000, Cambridge, Massachusetts.

Hähnel, D., Burgard, W., For, D., Fishkin, K. & Philipose, M. (2004). Mapping and localization with RFID technology. *International Conference on Robotics & Automation*, April 2004, New Orleans, Louisiana.

Hanlon, B.O., Ledvina, B., Psiaki, M.L., Kintner. P.M. & Humphreys, T.E. (2009). Assessing the Spoofing Threat. Available online at: http://www.gpsworld.com/defence/security-surveillance/assessing-spoofing-threat-3171?page_id=1 (Last access date: 4th November 2009).

Harding, S.J. (2001). Vulnerability Assessment of the Transport Infrastructure Relying on the Global Positioning System. QinetiQ Group, Buckingham Gate, London.

Hewitson, S. (2003). GNSS receiver autonomous integrity monitoring: A separability analysis. *16th International Technical Meeting of the Satellite Division of the U.S. Institute of Navigation*, 9th-12th September, Portland, Oregon.

Hewitson, S. & Wang, J. (2006). GNSS receiver autonomous integrity monitoring (RAIM) performance analysis. *GPS Solut.*, **10**: 155-170.

Humphreys, T.E., Ledvina, B.M., Psiaki, M.L., & Kintner, J. (2008). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. *ION GNSS 2009*, 16th-19th September 2008, Savannah International Convention Center, Savannah, Georgia.

Humphreys, T.E., Psiaki, M.L. & Kintner, P.M. (2009). GPS Spoofing Threat. Available online at: http://www.telecomasia.net/article.php?id_article=12288&page=4 (Last access date: 4th November 2009).

Inside GNSS (2009). GLONASS Launch Postponed until February. Available online at: http://www.insidegnss.com/node/1718 (Last access date: 4th November 2009).

Institute for Defense Analyses (IDA) (2009). Independent Assessment Team (IAT): Summary of Initial Findings on eLoran. Institute for Defense Analyses (IDA), Alexandria, Virginia.

Institute of Navigation (ION) (1998). RAIM: Requirements, Algorithms, and Performance, Global Positioning System. Papers Published in NAVIGATION, Volume V, Institute of Navigation, Fairfax, Virginia.

International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA) (2004). IALA Recommendation R-129 On GNSS Vulnerability and Mitigation Measures. International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA), Saint Germain en Laye, France.

Jewell, J. (2007). GPS Insights. Available online at: http://www.gpsworld.com/defense/gps-insights-april-2007-8428 (Last access date: 4th November 2009).

Jewell, J. (2009). Time for GPS 101. Available online at: http://mg.gpsworld.com/gpsmg/ArticleStandard/Article/detail/608873 (Last access date: 4th November 2009).

Johnston, R.G. & Warner, J.S. (2004). Think GPS offers high security? Think again! *Business Contingency Planning Conference*, 23rd-27th May 2004, Las Vegas, Nevada.

Joint Chief of Staffs (JCS) (2007). Geospatial Electronic Warfare. Joint Publication 3-13.1, Joint Chief of Staffs, USA.

Kaplan, E.D. & Hegarty, C.J. (2006). Understanding GPS: Principles and Applications, Artech House, Norwood, Massachusetts.

Kawaguchi, N. (2009). WiFi location information system for both indoors and outdoors. *Lect. Notes Comput. Sci.*, **5518**:638-645.

Kemppainen A., Haverinen J. & Röning J. (2006). An infrared location system for relative pose estimation of robots. *16th CISM-IFToMM Symposium of Robot Design, Dynamics, and Control (ROMANSY 2006)*, 20th-24th June, Warsaw, Poland, p. 379-386.

Key, E.L. (1995). Techniques to counter GPS spoofing. Internal memorandum, MITRE Corporation, 17th February 1995.

Last, D. (2008). Navigation satellite systems: The present imperfect. *20th Anniversary Congress of Dutch Pilots (Loodswesen)*, 1st September 2008, Noordwijk, Netherlands.

Lilley, R., Church, G. & Harrison, M. (2006). GPS Backup for Position, Navigation and Timing: Transition Strategy for Navigation and Surveillance. Aviation Management Associates Inc., Alexandria, Virginia.

Locata Corporation (2003). Locata Technology Primer, Version 1.1. Locata Comporation, Australia.

Ledvina, B., Montgomery, P., & Humphreys, T. (2009). A multi-antenna defense: Receiver-autonomous GPS spoofing detection. *Inside GNSS*, **4**: 40-46.

Loegering, G.S. (2006). Dual-resistant antijamming architecture for GPS-guded air vehicle navigation system. *Technol. Rev. J.*, **14**: 1-10.

Manandhar, D., Okano, K., Ishii, M., Asako, M., Torimoto, H., Kogure, S. & Maeda, H. (2008). IMES (Indoor Messaging System): A proposal for new indoor positioning system. *Third Meeting of the International Committee on Global Navigation Satellite Systems*, 8th-12th December 2008, Pasadena, California.

McDonald, K.D. (2002). The modernization of GPS: Plans, new capabilities and the future relationship to Galileo. *J. GPS*, **1**: 1-17.

Meng, D., Feng, Z. & Lu, M. (2008). Anti-jamming with adaptive arrays utilizing power inversion algorithm. *Tsinghua Sci. Technol.*, **13**: 796-799.

Montgomery, P., Humphreys, T.E. & Ledvina, B.M. (2009). A multi-antenna defence receiver-autonomous GPS spoofing detection. *Inside GNSS*, **4**: 40-46.

Muneyuki, S., Yoshihiro, Y., Masataka, I., Yoshitsugu, M. & Kunihiro, C. (2003). Priority roll-call for active IR-tag location system. *Proceedings of the Annual Conference of the Institute of Systems, Control and Information Engineers*, Vol. 47, pp. 301-302.

NASA (2006). Solar Storm Warning. Available online at: http://science.nasa.gov/headlines/y2006/10mar_stormwarning.htm (Last access date: 4th November 2009).

Oberst, T. (2006). Solar Flares Cause GPS Failures, Possibly Devastating for Jets and Distress Calls, Cornell Researchers Warn. Available online at: http://www.news.cornell.edu/stories/Sept06/solar.flares.gps.TO.html (Last access date: 4th November 2009).

Papadimitratos, P. & Jovanovic, A. (2008). Protection and fundamental vulnerability of GNSS. *International Workshop on Satellite and Space Communications 2008 (IWSSC'08)*. 1st-3rd October 2008, Institut Supérieur de l'Aéronautique et de l'Espace (ISAE), Toulouse, France.

Pinker, A. & Smith, C. (2000). Vulnerability of GPS Signal to Jamming, *GPS Sol.*, **3**: 19-27.

Poisel, A.R. (2002). Introduction to Communication Electronic Warfare Systems. Artech House, Boston.

Revnivykh, S. (2007). GLONASS status & development. *Civil GPS Service Interface Committee (CGSIC) Meeting*, 24th-25th September 2009, Fort Worth, Texas.

Revnivykh, S. (2008). GLONASS status & progress. *3rd Meeting of the International Committee on GNSS (ICG)*, 8th-12th December, 2008, Pasadena, California.

Rizos, C. (2009). Generation next. *GIS Dev.*, **13-11**: 20-24.

Rogers, C. (1991). Development of a low cost PC controlled GPS satellite signal simulator. *Proceedings of the 15th Biennial Guidance Test Symposium*, Holloman AFB, New Mexico.

Satoshi. K., Hiroaki, M., Makoto, I., Manandhar, D. & Kazuki, O. (2008). The concept of the Indoor Messaging System. *The European Navigation Conference ENC-GNSS*, April 2008, Toulouse, France.

Sergey, K., Sergey, R. & Suriya, T. (2007). GLONASS as a key element of the Russian positioning service. *Adv. Space Res.*, **39**:1539-1544.

Simonsen, K., Suycott, M., Crumplar, R., & Wohlfiel, J. (2004). LOCO GPSI: Preserve the GPS advantage for defence and security. *IEEE Aerospace Electron. Syst.*, **19**: 3-7.

Suryanarayana Rao, K.N. & Pal, S. (2004). The Indian SBAS system: GAGAN. *India-United States Conference on Space Science, Applications, and Commerce*. June 2004.

Tektronix (2008). H600 RF Hawk Signal Hunter. Available online at: http://www.tektronixcommunications.com/modules/communications/index.php?command=defaultPage&operation=displayDataSheet&catid=3300&id=595 (Last access date: 4th November 2009).

Volpe (2001). Vulnerability Assessment of the Transport Infrastructure Relying on the Global Positioning System. John A. Volpe National Transportation Systems Center, Department of Transport, Washington D.C.

Wen, H., Huang, P.Y.R., Dyer, J., Archinal, A. & Fagan, J. (2005). Countermeasures for GPS signal spoofing. *18th International Technical Meeting of the Satellite Division of the Institute of Navigation ION GNSS 2005*, 13th-16th September 2005, Long Beach Convention Center, Long Beach, California

Williams, S.F. (2006). Radar'd Out: GPS Vulnerable to High-Power Microwaves. Available online at: http://mg.gpsworld.com/gpsmg/article/articleDetail.jsp?id=320030 (Last access date: 4th November 2009).

EVALUATION OF THE EFFECT OF RADIO FREQUENCY INTERFERENCE (RFI) ON GLOBAL POSITIONING SYSTEM (GPS) RECEIVERS

Dinesh Sathyamoorthy*, Wan Mustafa Wan Hanafi, Mohd Faudzi Muhammad, Kamarulzaman Mustapa, Nor Irza Shakhira Bakthir, Siti Robiah Abdul, Norhayaty Zahari, Aliah Ismail, Lim Bak Tiang, Arumugam Periapa, Zainal Fitry M. Amin, Mohd. Rizal Ahmad Kamal, Azlina Besar & Mohd. Hasrol Hisam M. Yusoff

Instrumentation and Electronic Technology Division
STRIDE, Ministry of Defence, Malaysia
Tel: 603-87324431
Fax: 603-87348695
*E-mail: dinsat60@hotmail.com

Abstract

Given the various incidents of intentional and unintentional jamming of Global Navigation Satellite Systems (GNSS) signals, the development of various GNSS anti-jamming technologies has received significant attention. In addition, many current GNSS receiver evaluations are concentrated on radio frequency interference (RFI) operability. In preparation for an upcoming Final Acceptance Test (FAT) for Ground Navigation Equipment (GNE), the Instrumentation & Electronics Technology Division (BTIE), Science & Technology Research Institute for Defence (STRIDE), conducted two tests aimed at evaluating the effect on RFI on three types of Global Positioning System (GPS) receivers; handheld (Garmin GPSmap 60CSx), handphone (Sony Ericsson W760i) and fixed (Pendulum Instruments GPS-12R). All three GPS receivers use the L1 coarse acquisition (C/A) signal. The first test was conducted on 10th November 2009, where a major flaw was made in the test procedure; the antenna for the fixed GPS receiver was place too high compared to the other two GPS receivers. This caused the receivers to receive unequal amount of interference, leading to erroneous results. Using the lessons learnt from the first test, the second test was conducted on 17th November 2009 with a corrected procedure. It is observed that the power levels required to affect the location fixes are significantly high compared to the received GPS signal power received. This is because the noise-like C/A code structure, which modulates the L1 signal over a 2 MHz bandwidth, allows for the signal to be received at low levels of interferences. Of the three GPS receivers, the fixed GPS receiver showed the best RFI operability as it has the highest receiver sensitivity. However, the test was subject to various error parameters, including ionospheric and tropospheric delays, satellite clock, ephemeris and multipath errors, satellite positioning and geometry, and unintentional signal interferences and obstructions, all of which are uncontrollable by users. The ideal testing methodology would be using a GNSS simulator which can be used to generate multi-satellite GNSS configurations, transmit GNSS signals which simulate real world scenarios, and adjust the various error parameters. This would allow for the evaluations of GNSS receiver performance under various repeatable conditions, as defined by the user.

Keywords: *Global Positioning System (GPS) receiver evaluation; radio frequency interference (RFI); location fix; GPS L1 coarse acquisition (C/A) signal; signal power level.*

1 INTRODUCTION

This article follows up on the discussion in Dinesh (2009) on the vulnerabilities of Global Navigation Satellite Systems (GNSS) signals, in particular to jamming. Jamming is defined as the broadcasting of a strong signal that overrides or obscures the signal being jammed (DOA, 2009; JCS, 2007; Poisel, 2002). Since GNSS satellites, powered by photocells, are approximately 20,200 km above the Earth surface, GNSS signals that reach the Earth have very low power (10^{-16} W = -160 dBm), rendering

them highly susceptible to jamming (Pinker & Smith, 2000; Adams, 2001; Johnston & Warner, 2004; Papadimitratos & Jovanovic, 2008; Last, 2008; IDA, 2009). Given the various incidents of intentional and unintentional jamming of GNSS signals, including military GNSS signals (Adams, 2001; Williams, 2006; Jewell, 2007), the development of various GNSS anti-jamming technologies has received significant attention (Casabona & Rosen, 1999; Gustafon *et al.*, 2000; Deshpande, 2004; Loegering, 2006; Meng *et al.*, 2008). In addition, many current GNSS receiver evaluations are concentrated on radio frequency interference (RFI) operability. For example, GNSS evaluations conducted by SIRIM Bhd. only involve RFI testing (Ooi & Mustafa, 2009).

In preparation for an upcoming Final Acceptance Test (FAT) for Ground Navigation Equipment (GNE), the Instrumentation & Electronics Technology Division (BTIE), Science & Technology Research Institute for Defence (STRIDE), conducted two tests aimed at evaluating the effect on RFI on three types of Global Positioning System (GPS) receivers; handheld (Garmin GPSmap 60CSx) (Garmin, 2007), handphone (Sony Ericsson W760i) (Sony Ericsson , 2008) and fixed (Pendulum Instruments GPS-12R (Pendulum, 2006) (Figure 1). All three GPS receivers use the L1 coarse acquisition (C/A) signal. Both tests were conducted at the STRIDE Kajang Block B car park (Figure 2).

(a) **(b)** **(c)**

Figure 1: GPS receivers evaluated in this study: (a) Handheld: Garmin GPSmap 60CSx (b) Handphone: Sony Ericsson W760i (c) Fixed: Pendulum Instruments GPS-12R.

Figure 2: Test area located approximately at N 2º 58' 3" E 101º 48' 35". (Source: Screen capture from Google Earth)

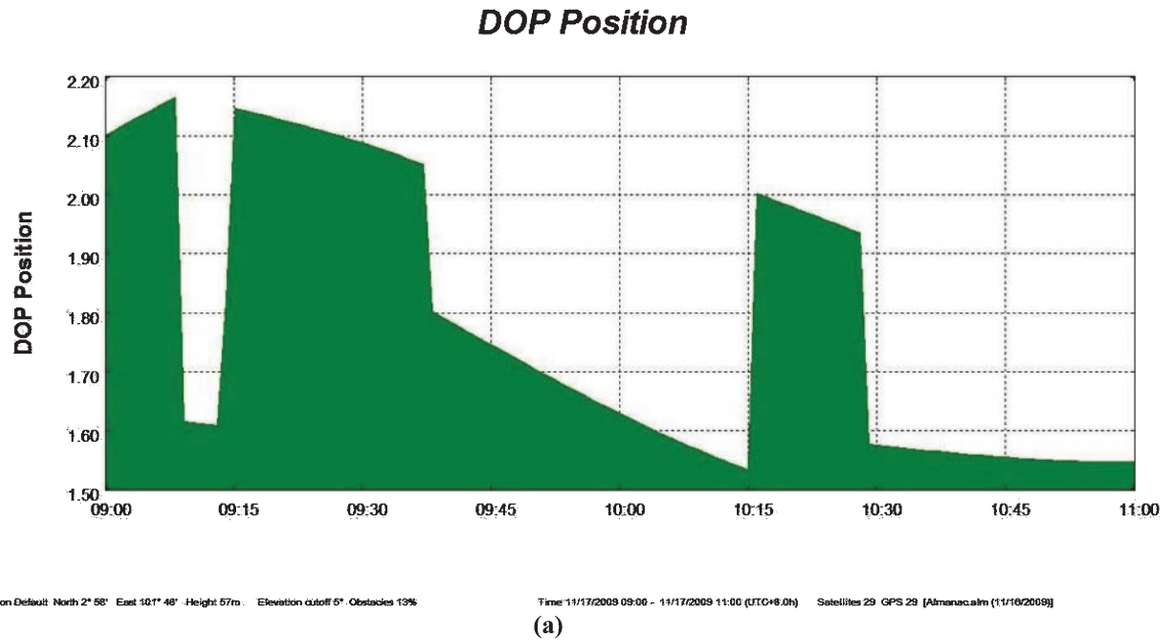
The first test was conducted on 10th November 2009 (STRIDE, 2009a), where a major flaw was made in the test procedure; the antenna for the fixed GPS receiver was place too high compared to the other two GPS receivers. This caused the receivers to receive unequal amount of interference, leading to erroneous results.

Using the lessons learnt from the first test, a second test was conducted on 17th November 2009 with a corrected procedure (STRIDE, 2009b). This article is aimed at discussing the procedure employed during the test, and the overall conclusions observed from its results. In addition, the effectiveness of such GNSS field evaluations is also assessed.

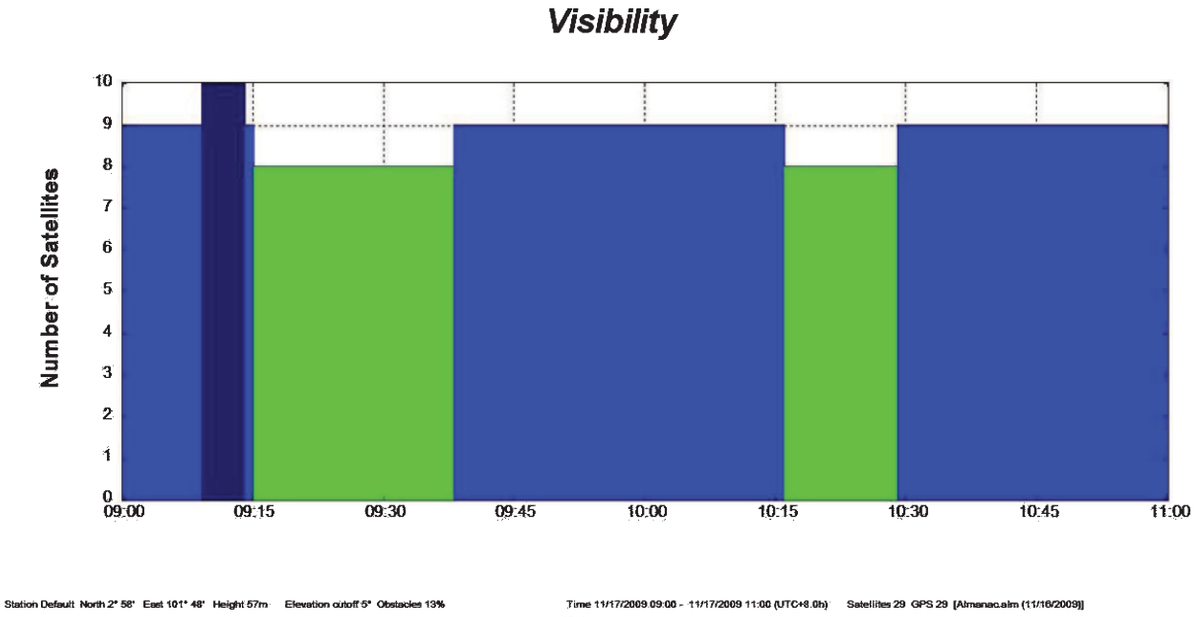
2 METHODOLOGY

2.1 Preliminary Preparations

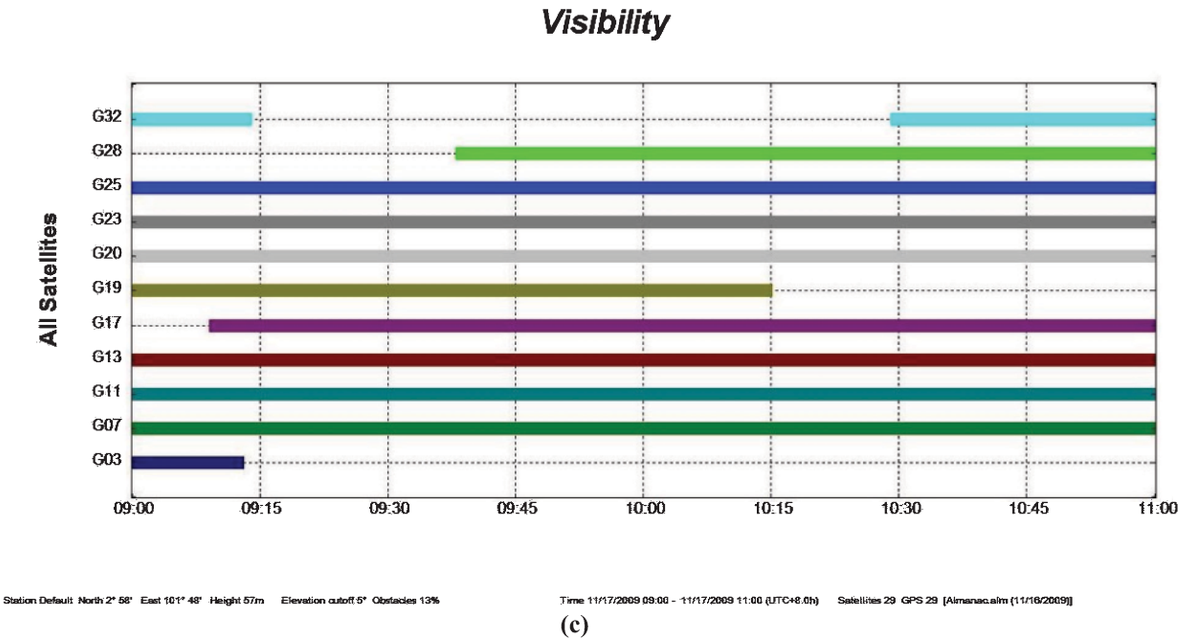
The Trimble Planning software (Trimble, 2009) was employed to estimate the GPS satellite coverage in the test area on 17th November 2009. It was observed that the period of the test, 0900 – 1100, coincided with a period of good GPS coverage (Figure 3), with low position dilution of precision (PDOP) values (1.52-2.15) and high satellite visibility (8-10 satellites). Nevertheless, the Trimble Planning software only takes into account estimated satellite positions and geometry, and does not consider other sources of GNSS errors, including ionospheric and tropospheric delays, satellite clock, ephemeris and multipath errors, and unintentional signal interferences and obstructions. Furthermore, the parameters of elevation cutoff and obstacles were estimated from 30 m resolution terrain models, which do not take into consideration man-made structures, and thereby, are subject to errors.



(a)



(b)



(c)

Figure 3: GPS satellite coverage in the test area during the test period (17th November 2009, 0900 – 01100): (a) PDOP (b), (c) Satellite visibility.
(Source: Screen captures from the Trimble Planning Software)

2.2 Test Procedure

The apparatus used in the test were an Advantest U3751 spectrum analyzer (Advantest, 2009), an IFR 2023B signal generator (IFR, 1999), a Hyperlog 60180 directional antenna (Aaronia, 2009), and a Garmin GPSmap 60CS handheld receiver (Garmin, 2004) (used as a benchmark reference). The test procedure employed is as follows (Figure 4):

1) The signals in the frequency range of 1,560 - 1,590 MHz are measured.

2) For transmitted carrier wave and FM (peak deviations at 0.5, 1, 2, 3, 4 and 8 MHz) signals, at power levels of 13 dBm, the respective received signals are measured.
3) The three GPS receivers are placed at the same height, and as close as possible to each other.
4) The reference GPS receiver is placed in an area unaffected by the jamming (approximately 40 m away).
5) A location fix is obtained using all four GPS receivers.
6) The directional antenna, placed 3 m away from the evaluated GPS receivers, is used to transmit an FM signal with the following properties:
    - Carrier wave frequency: 1,575.42 MHz (frequency of the L1 signal)
    - Peak deviation: 8 MHz
    - Information frequency: 5 kHz
7) The transmission is started at power level of -60 dBm.
8) The power level is increased by increments of 5 dBm.
9) For each GPS receiver, the power levels when following occurs is noted:
    - The first degradation of accuracy is noticed
    - The location fix is lost.
10) Steps 4-9 are repeated with peaks deviations of 4, 2, 1 and 0.5 MHz, and an unmodulated carrier wave.

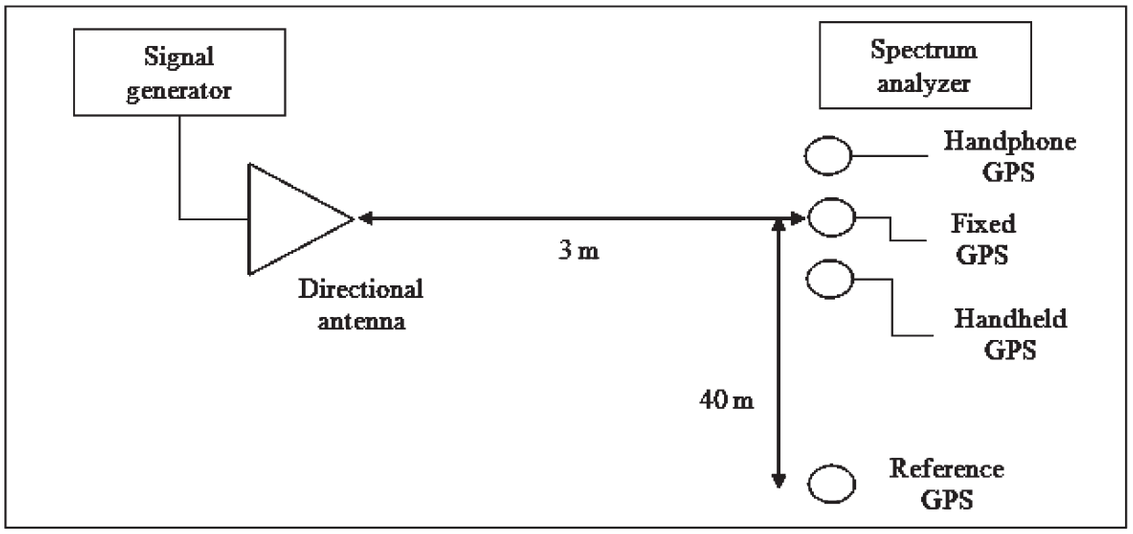


Figure 4: The test setup.

3 OBSERVATIONS

No discernible signals were observed in the range of 1,560 – 1,590 MHz (Figure 5). However, it should be noted that the spectrum analyzer was only able to measure signals above -60 dBm, well over the minimum power levels required to jam GNSS signals. It is unknown if there are any unwanted interference signals below this threshold.

For transmitted carrier wave and FM (peak deviations of 0.5, 1, 2, 3, 4 and 8 MHz) signals, at power levels of 13 dBm, the respective received signals are shown in Figure 6. The measured signals would be used to estimate received power levels which were too low to be measured with the spectrum analyzer (refer to the appendix). It is noted that all four GPS receivers were unable to obtain location fixes during the duration of this step (expect for the reference GPS receiver which was able to obtain a location fix at FM 8 MHz peak deviation signal).

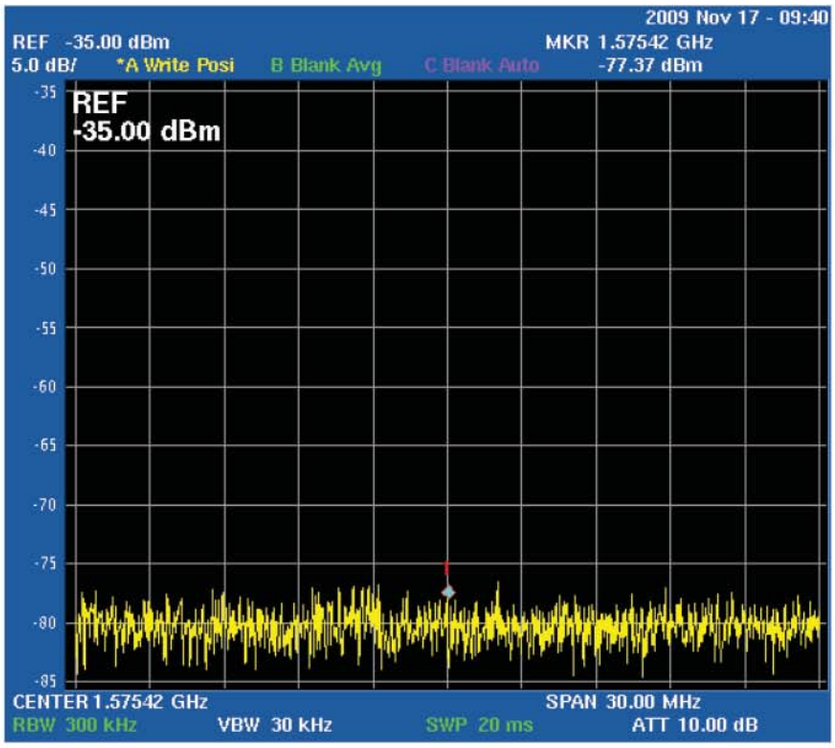
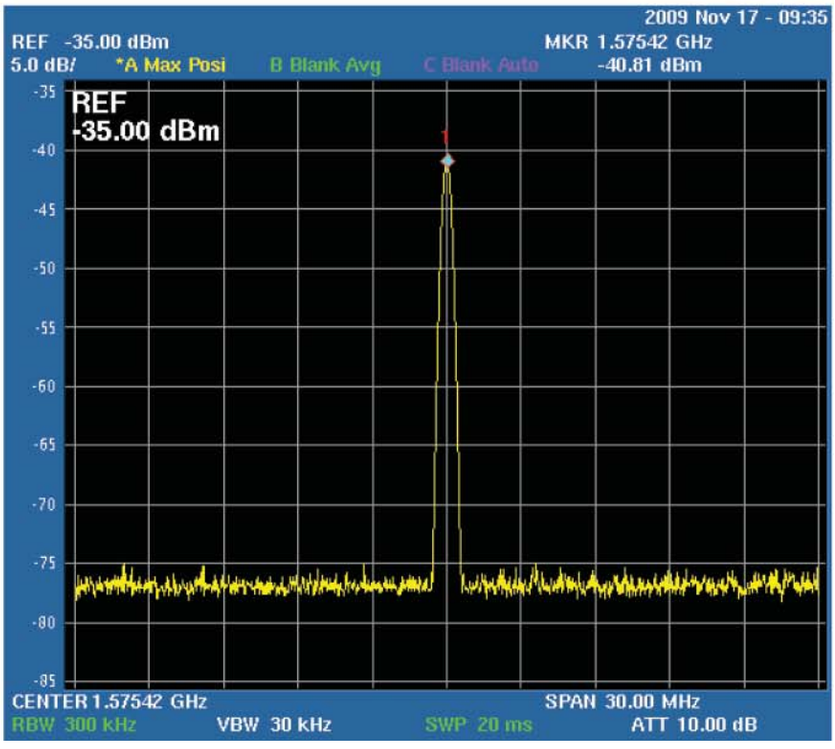
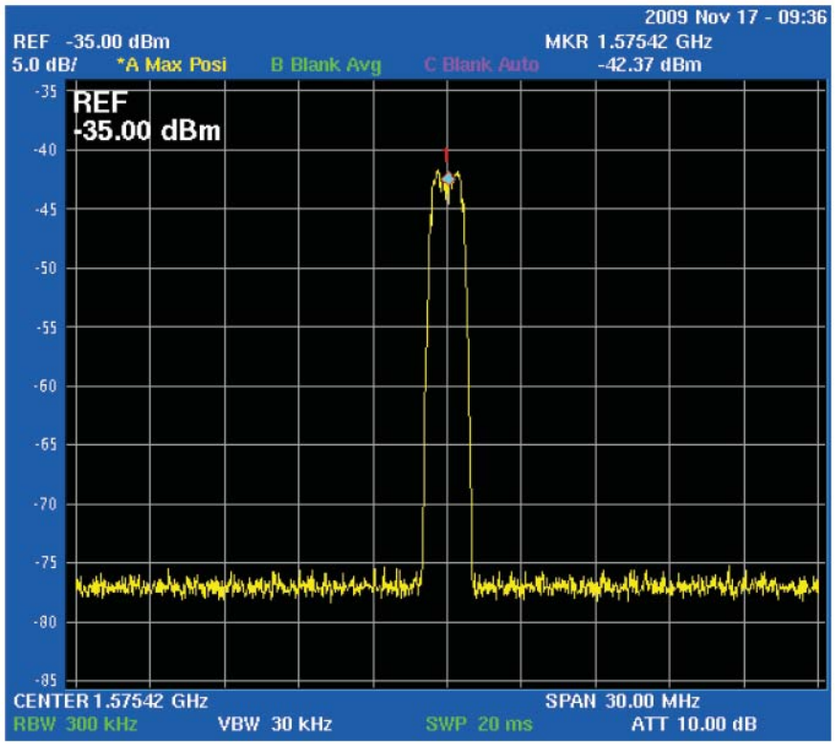


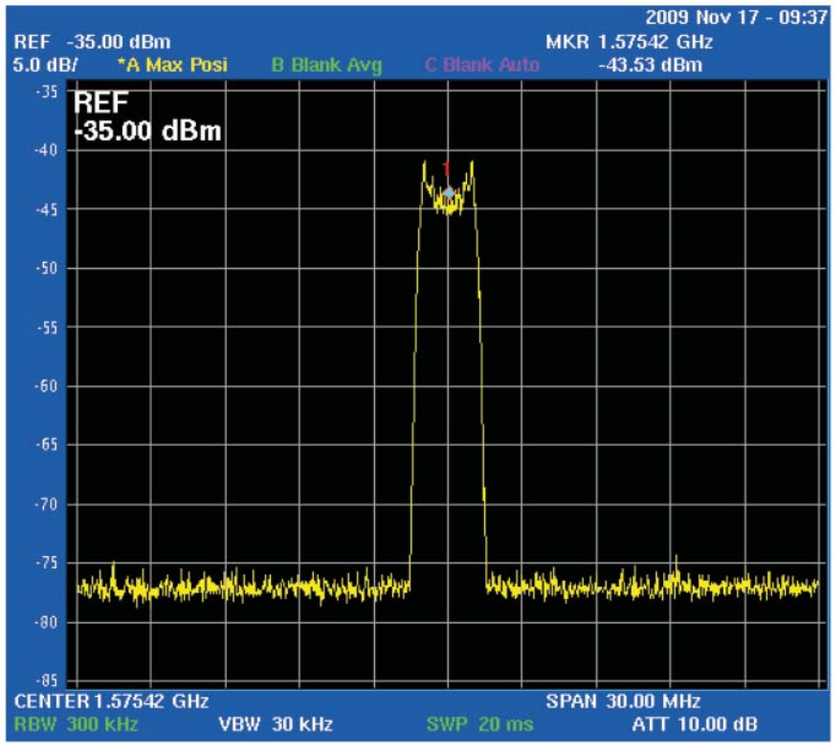
Figure 5: Spectrum analyzer readout for the frequency range of 1,560 – 1,590 MHz. (Source: Screen capture from the Advantest U3751 spectrum analyzer)



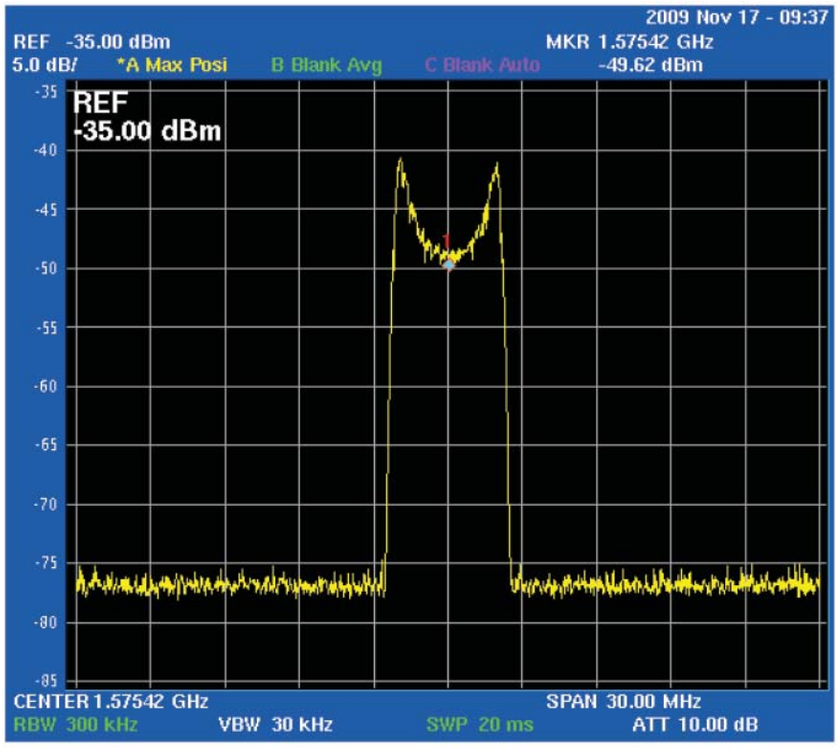
(a)


2009 Nov 17 - 09:36
REF -35.00 dBm
MKR 1.57542 GHz
5.0 dB/ *A Max Posi B Blank Avg C Blank Auto -42.37 dBm
REF
-35.00 dBm
-35
-40
-45
-50
-55
-60
-65
-70
-75
-80
-85
CENTER 1.57542 GHz
SPAN 30.00 MHz
RBW 300 kHz VBW 30 kHz SWP 20 ms ATT 10.00 dB

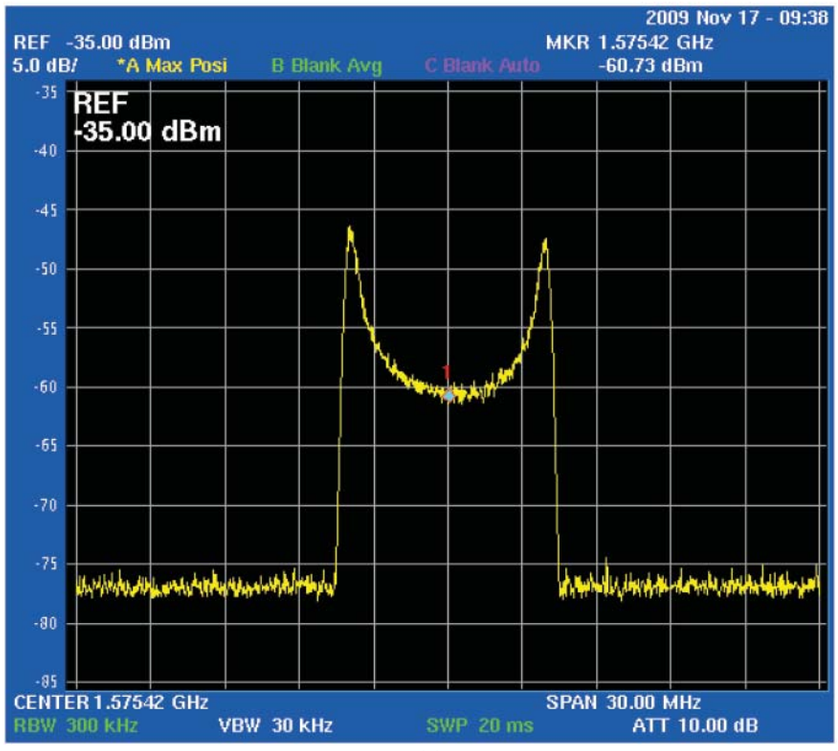
(b)


2009 Nov 17 - 09:37
REF -35.00 dBm
MKR 1.57542 GHz
5.0 dB/ *A Max Posi B Blank Avg C Blank Auto -43.53 dBm
REF
-35.00 dBm
-35
-40
-45
-50
-55
-60
-65
-70
-75
-80
-85
CENTER 1.57542 GHz
SPAN 30.00 MHz
RBW 300 kHz VBW 30 kHz SWP 20 ms ATT 10.00 dB

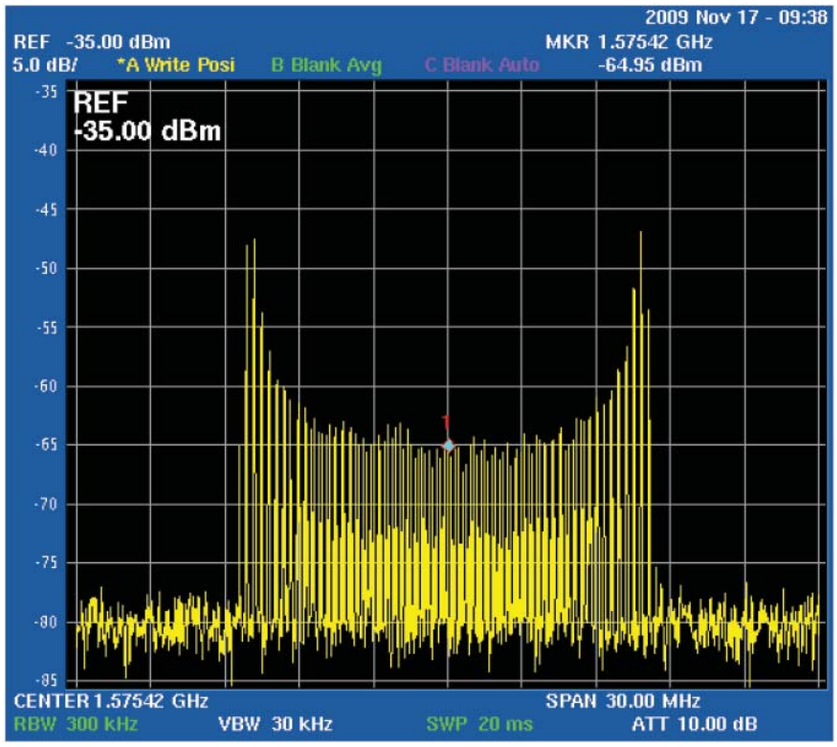
(c)


2009 Nov 17 - 09:37
REF -35.00 dBm
MKR 1.57542 GHz
5.0 dB/ *A Max Posi B Blank Avg C Blank Auto -49.62 dBm
REF
-35.00 dBm
-35
-40
-45
-50
-55
-60
-65
-70
-75
-80
-85
CENTER 1.57542 GHz
SPAN 30.00 MHz
RBW 300 kHz VBW 30 kHz SWP 20 ms ATT 10.00 dB

(d)


2009 Nov 17 - 09:38
REF -35.00 dBm
MKR 1.57542 GHz
5.0 dB/ *A Max Posi B Blank Avg C Blank Auto -60.73 dBm
REF
-35.00 dBm
-35
-40
-45
-50
-55
-60
-65
-70
-75
-80
-85
CENTER 1.57542 GHz
SPAN 30.00 MHz
RBW 300 kHz VBW 30 kHz SWP 20 ms ATT 10.00 dB

(e)



(f)

Figure 6: Received signals of (a) carrier wave, and FM (peak deviations of (b) 0.5 MHz, (c) 1 MHz, (d) 2 MHz, (e) 4 MHz, and (f) 8 MHz) signals transmitted at 13 dBm.
(Source: Screen captures from the Advantest U3751 spectrum analyzer)

The respective location coordinates, accuracies and number of satellites locked for the GPS receivers are shown in Table 1. It is noted that even though the three GPS receivers were placed in the vicinity of each other, there was significant discrepancies in terms of their respective location coordinates. This occurred because the coordinates were recorded too early after the jamming signals in power referencing step were turned off, with the GPS receivers still being unable to obtain full location fix stability. The reference GPS receiver, uninterrupted by the 8 MHz interference bandwidth signal, was able to provide an accurate location coordinate. In a post-test measurement conducted later, it was observed that the evaluated GPS receivers gave roughly the same location coordinates, approximately N 2° 58' 3", E 101° 48' 35". From Table 1, it is observed that the handphone and handheld GPS receivers were able to provide relatively close coordinates, indicating that they had fast reacquisition times, an important parameter for ground navigation applications, where tunnels and bridges frequently block GNSS signals.

Table 1: Location coordinates, accuracies and number of satellites locked of the GPS receivers at 0945.

GPS Receiver	Handphone	Handheld	Fixed	Reference
Location coordinates	N 2° 58' 2.96" E 101° 48' 35.31"	N 2° 58' 3.2" E 101° 48' 35.4"	N 2° 58' 7.151" E 101° 48' 34.656"	N 2° 58' 4.3" E 101° 48' 34.7"
Accuracy (m)	±8	±3	N/A	±8
Number of satellites locked	6	9	9	8

For peak deviations of 8, 4, 2, 1 and 0.5 MHz (FM signal bandwidths of 16.01, 8.01 MHz, 4.01 MHz, 2.01 MHz, and 1.01 MHz), and the carrier wave signals, the power levels at which the first degradation of accuracy is noticed and the location fix is lost are shown in Tables 2-7 respectively.

Table 2: Power levels at which the first degradation of accuracy is noticed and the location fix is lost (for peak deviation of 8 MHz (FM signal bandwidth of 16.01 MHz)).

GPS Receiver		Fixed	Handheld	Handphone
Power Level (Transmitted/ Estimated received) (dBm)	**The first degradation of accuracy is noticed**	5 / -72.95	-5 / -82.95	-10 / -87.95
	The location fix is lost	10 / -67.95	0 / -77.95	-5 / -82.95

Table 3: Power levels at which the first degradation of accuracy is noticed and the location fix is lost (for peak deviation of 4 MHz (FM signal bandwidth of 8.01 MHz)).

GPS Receiver		Fixed	Handheld	Handphone
Power Level (Transmitted/ Estimated received) (dBm)	**The first degradation of accuracy is noticed**	-20 / -93.73	-25 / -98.73	-25 / -98.73
	The location fix is lost	-15 / -88.73	-20 / -93.73	-20 / -93.73

Table 4: Power levels at which the first degradation of accuracy is noticed and the location fix is lost (for peak deviation of 2 MHz (FM signal bandwidth of 4.01 MHz)).

GPS Receiver		Fixed	Handheld	Handphone
Power Level (Transmitted/ Estimated received) (dBm)	**The first degradation of accuracy is noticed**	-30 / -92.62	-40 / -102.62	-40 / -102.62
	The location fix is lost	-25 / -87.62	-35 / -97.62	-35 / -97.62

Table 5: Power levels at which the first degradation of accuracy is noticed and the location fix is lost (for peak deviation of 1 MHz (FM signal bandwidth of 2.01 MHz)).

GPS Receiver		Fixed	Handheld	Handphone
Power Level (Transmitted/ Estimated received) (dBm)	The first degradation of accuracy is noticed	-40 / -96.83	-45 / -101.83	-45 / -101.83
	The location fix is lost	-35 / -91.83	-40 / -96.83	-40 / -96.83

Table 6: Power levels at which the first degradation of accuracy is noticed and the location fix is lost (for peak deviation of 0.5 MHz (FM signal bandwidth of 1.01 MHz)).

GPS Receiver		Fixed	Handheld	Handphone
Power Level (Transmitted/ Estimated received) (dBm)	The first degradation of accuracy is noticed	-40 / -95.87	-45 / -100.87	-55 / -110.87
	The location fix is lost	-35 / -90.87	-40 / -95.87	-50 / -105.87

Table 7: Power levels at which the first degradation of accuracy is noticed and the location fix is lost (for peak unmodulated carrier wave).

GPS Receiver		Fixed	Handheld	Handphone
Power Level (Transmitted/ Estimated received) (dBm)	The first degradation of accuracy is noticed	-40 / -93.81	-45 / -98.81	-45 / -98.81
	The location fix is lost	-35 / -88.81	-40 / -93.81	-40 / -93.81

4 DISCUSSION

It is observed that the received power levels required to affect the location fixes of the GPS receivers are significantly high compared to the received GPS signal power. The noise-like C/A code structure, which modulates the L1 signal over a 2 MHz bandwidth, allows for the signal to be received at low levels of interferences. The P(Y) code (restricted to the US military) has a more robust structure, modulating the L1 and L2 signals over 20 MHz bandwidths, and has better resistance to interference.

It is also observed that FM signals with higher peak deviations require higher power levels to affect the location fixes. This occurs as the power is distributed over a larger bandwidth, reducing the effectiveness of interference and the received signal power.

The FM 0.5 MHz peak deviation (bandwidth of 1.01 MHz) and carrier wave signals are able to jam the GPS receivers, albeit at slightly higher power levels compared to the 2.01 and 4.01 MHz interference bandwidth signals. This occurred even though both have smaller bandwidths than the L1 C/A signal. This indicates that the L1 C/A signal can be jammed by simply interfering its fundamental frequency (1,575.42 MHz).

It should be reiterated that this test was conducted during a period of good GPS satellite coverage, with low range of PDOP values. During periods of poor satellite coverage, the power levels required to interfere the L1 C/A signal will be smaller.

Of the three GPS receivers, the fixed GPS receiver showed the best RFI operability. This is because the fixed GPS receiver, using an active antenna, has the highest receiver sensitivity. The handheld GPS receiver generally showed higher levels of RFI operability as compared to the handphone GPS receiver.

For the purposes of navigation applications, the fixed GPS receiver would be too impractical to be used; it is more suitable for static applications such as time referencing and calibration. The handheld GPS receiver, having fast reacquisition time, and better RFI operability than the handphone GPS receiver, would be the best option of the three receivers.

The reference GPS receiver was unaffected during the jamming test as it only involved low interferences affecting a radius of 3 m. However, during the signal power referencing, when the power levels of signals was set at 13 dBm, the reference GPS receiver was jammed (except for the FM 8 MHz peak deviation signal). An interesting follow up test would be to evaluate the distances required by interference signals of various bandwidths and power levels to conduct GNSS jamming.

5 CONCLUSIONS / RECOMMENDATIONS

According to the International Organization of Navigation Standard 101 (ION STD 101): Recommended Test Procedures for GPS Receivers, Revision C (ION, 1997), some of the key GNSS receiver performance parameters that need to be evaluated include:

- **Static Positioning Accuracy:**
  - Defined as the accuracy of the receiver location fix with respect to a known reference.

- **Radio Frequency Interference:**
  - Establishing the ability of the GPS receiver to operate in the presence of interfering (jamming) signals that may be received through its input.

- **Receiver sensitivity (Carrier to noise power ratio (C/No))**
  - Evaluated by measuring signal strength under various GPS signal power levels.

Field evaluations, such as conducted in this test, are not suitable for measurement of these parameters as ideally, they should be measured under conditions in which the parameters of ionospheric and tropospheric delays, satellite clock, ephemeris and multipath errors, and satellite positioning and geometry are user-controlled and repeatable. Furthermore, field evaluations cannot be employed to measure receiver sensitivity, as this requires precise measurements of GPS signals.

The ideal testing methodology would be using a GNSS simulator which can be used to generate multi-satellite GNSS configurations, transmit GNSS signals which simulate real world scenarios, and adjust the various error parameters. This would allow for the evaluation of GNSS receiver performance under various conditions, as defined by the user. The advantages of GNSS simulators, as compared to field evaluations is discussed in Dinesh et al. (2009)

With the upcoming GNSS modernization programs, including the introduction of new civilian signals under GPS, Galileo and Compass, it is expected that there will be a proliferation of procurements of GNSS positioning, navigation and timing equipment by Malaysian defence & security forces, including the Malaysian Armed Forces (MAF). Hence, it is proposed that STRIDE procure a GNSS simulator in order to be able to conduct trials, evaluations and FATs of such equipment in an effective manner.

ACKNOWLEDGEMENT

The authors are grateful to En. Mohd. Razali Mat Yassin, En. Ab. Sukor Zakariya and En. Shaiful Bahri Zainal Abidin for their support.

REFERENCE

Aaronia (2009). Precompliance Test Antenna Series HyperLOG® 60xxx: Span 680MHz to 18GHz. Aaronia AG, Strickscheid, Germany.

Adams, T.K. (2001). GPS Vulnerabilities. *Mil. Rev.*, **1**: 10-16.

Advantest (2009). U3741/3751 Spectrum Analyzers. Advantest Corporation, Chiyoda-ku, Tokyo.

Casabona, M.M. & Rosen, M.W. (1999). Discussion of GPS anti-jam technology. *GPS Solut.*, **2**: 18-23.

Department of Army (DOA) (2009). Electronic Warfare in Operations. Army Field Manual 3-36, Department of Army, Washington D.C.

Deshpande, S.M. (2004). Study of Interference Effects on GPS Signal Acquisition. Masters thesis, University of Calgary, Calgary, Alberta.

Dinesh, S., 2009. Vulnerabilities of Civilian Global Navigation Satellite Systems (GNSS) Signals: A Review. *Defence S&T Tech. Bull.*, **This edition**: 100-114.

Dinesh , S., Wan Mustafa, Mohd Faudzi., M., W.H., Kamarulzaman, M., Nor Irza Shakhira, B., Siti Robiah, A., Norhayaty, Z., Aliah, I., Lim, B.T., Arumugam, P., Zainal Fitry, M.A., Mohd. Rizal, A.K., Azlina, B. & Mohd. Hasrol, H.M.Y. (2009). The advantages of Global Navigation Satellite Systems (GNSS) receiver evaluation using GNSS simulators. *BUDI*, **2009**: In press.

Garmin (2004). GPSmap 60CS Owner's Manual. Garmin International Inc., Olathe, Kansas.

Garmin (2007). GPSmap 60CSx Owner's Manual. Garmin International Inc., Olathe, Kansas.

Gustafon, D., Dowdle, J. & Flueckiger, K. (2000). A high anti-jam GPS-based navigator. *Proceedings of the Institute of Navigation*, 28th-30th June 2000, Cambridge, Massachusetts.

IFR (1999). 2023A/B, 2025 Signal Generators. IFR Americas Inc., Wichita, Kansas

Institute for Defense Analyses (IDA) (2009). Independent Assessment Team (IAT): Summary of Initial Findings on eLoran. Institute for Defense Analyses (IDA), Alexandria, Virginia.

Institute of Navigation (ION) (1997). Institute of Navigation Standard 101 (ION STD 101): Recommended Test Procedures for GPS Receivers, Revision C. Institute of Navigation (ION), Manassas, Virginia.

Jewell, J. (2007). GPS Insights. Available online at: http://www.gpsworld.com/defense/gps-insights-april-2007-8428 (Last access date: 17th November 2009).

Johnston, R.G. & Warner, J.S. (2004). Think GPS offers high security? Think again! *Business Contingency Planning Conference*, 23rd-27th May 2004, Las Vegas, Nevada.

Joint Chief of Staffs (JCS) (2007). Geospatial Electronic Warfare. Joint Publication 3-13.1, Joint Chief of Staffs, USA.

Last, D. (2008). Navigation satellite systems: The present imperfect. *20th Anniversary Congress of Dutch Pilots (Loodswesen)*, 1st September 2008, Noordwijk, Netherlands.

Loegering, G.S. (2006). Dual-resistant antijamming architecture for GPS-guded air vehicle navigation system. *Technol. Rev. J.*, **14**: 1-10.

Meng, D., Feng, Z. & Lu, M. (2008). Anti-jamming with adaptive arrays utilizing power inversion algorithm. *Tsinghua Sci. Technol.*, **13**: 796-799.

Ooi, W.H. & Mustafa, D.S., 2009. GNSS Receiver's Testing: Study of GPS Test Software. *Map Malaysia 2009*, 21st-22nd April 2009, Equatorial Hotel, Penang.

Papadimitratos, P. & Jovanovic, A. (2008). Protection and fundamental vulnerability of GNSS. *International Workshop on Satellite and Space Communications 2008 (IWSSC'08)*. 1st-3rd October 2008, Institut Supérieur de l'Aéronautique et de l'Espace (ISAE), Toulouse, France.

Pendulum (2006). GPS-12R (GPS-Controlled Frequency Standard). Pendulum Instruments, Oakland, California.

Pinker, A. & Smith, C. (2000). Vulnerability of GPS Signal to Jamming, *GPS Sol.*, **3**: 19-27.

Poisel, A.R. (2002). Introduction to Communication Electronic Warfare Systems. Artech House, Boston.

Science & Technology Research Institute for Defence (STRIDE) (2009a). Evaluation of the Effect of Radio Frequency Interference (RFI) on the GPS L1 C/A Signal. Science & Technology Research Institute for Defence (STRIDE), Ministry of Defence, Malaysia.

Science & Technology Research Institute for Defence (STRIDE) (2009b). Evaluation of Power Levels of Interference Signals Required to Jam the GPS L1 C/A Signal. Science & Technology Research Institute for Defence (STRIDE), Ministry of Defence, Malaysia.

Sony Ericsson (2008). W760i User's Guide. Sony Ericsson, Lund, Sweden.

Trimble (2009). Trimble's Planning Software. Available online at: http://www.trimble.com/planningsoftware.shtml (Last access date: 17th November 2009).

Williams, S.F. (2006). Radar'd Out: GPS Vulnerable to High-Power Microwaves. Available online at: http://mg.gpsworld.com/gpsmg/article/articleDetail.jsp?id=320030 (Last access date: 17th November 2009).

APPENDIX

Estimation of received power:

P_T : Transmitter power
P_R : Receiver power
G_T : Transmitter gain
G_R : Receiver gain
L : Free-space path loss
L_E : External losses
R : Distance (km)
F : Frequency (MHz)
δ : FM signal peak deviation

$$P_R = P_T + G_T + G_R - L - L_E \quad \text{(A1)}$$

$$L = 32.44 + 20\log R + 20\log f \quad \text{(A2)}$$

With G_T, G_R, L_E, R and f being constant:

$$P_R = P_T - L_O \quad \text{(A3)}$$

where:

$$L_O = 32.44 + 20\log R + 20\log f + L_E - G_T - G_R \quad \text{(A4)}$$

Using Equation A3, the values of L_O for various values of δ are computed (Table A1).

Table A1: Values of P_R and L_O, at P_T = 13 dBm, for various values of δ.

δ (MHz)	P_R (dBm)	L_O (dBm)
0	-40.81	53.81
0.5	-42.81	55.87
1	-43.53	56.53
2	-49.62	62.62
4	-60.73	73.73
8	-64.95	77.95

AN OVERVIEW ON WEAR DEBRIS ANALYSIS FOR ENGINE CONDITION MONITORING

Chan Keng Sam[1*], Wan Fadilah Wan Abdullah[1], Nor Azlan Sarjo[1], Shamsul Akmar Abd Aziz[1], Adam Hj Gani[1], Mohd Hairudin Abd Karim[1] & Junaidi Md Tahir[2]

[1]Mechanical & Aerospasce Technology Division,
Science & Technology Research Institute for Defence (STRIDE)
Taman Bukit Mewah Fasa 9, 43000 Kajang, Selangor D.E.
Tel: 03-87324535
Fax: 03-87336219
[*]E-mail: cks.pst@mod.gov.my

[2]881 Squadron, Army Air Wing (PUTD)
Kem Mahkota, 86000 Kluang, Johor

Abstract

This paper gives an overview on various techniques and approaches used for wear debris analysis and their effectiveness in monitoring the mechanical wear conditions of aircraft engines. Three different approaches are used in wear debris analysis; compositional analysis, morphological analysis and particle quantification. Atomic emission spectroscopy (AES), atomic absorption spectroscopy (AAS) and x-ray fluorescence (XRF) are key techniques used for compositional analysis. Techniques used for morphological studies include ferrography, direct imaging and magnetic plug. These techniques are also applicable for the particle quantification approach. By performing wear debris analysis, it will be able to predict component problems significantly earlier before engine failure occurs.

Keywords: *Wear debris; condition monitoring; compositional; morphology; quantification.*

1 INTRODUCTION

Wear debris are microscopic particles resulting from the wear and tear of moving parts in the engine that are held in suspension throughout the oil. When an engine is running normally, the quantity and size of the particles from natural wear remain fairly consistent or in dynamic balance after a certain period of operation. However, the quantity and size of wear particles progress from small to large when the engine begins to wear abnormally. The changes in quantity and size of wear particles give valuable insights into the mechanical condition of the components inside the engine.

Wear debris analysis is concerned with analyzing these wear particles and early diagnosis of abnormal wear. Based on the information extracted from analysis, corrective actions and preventive maintenance can be implemented in a timely fashion to prevent possible impending failures in the engine. It is one of the tools for condition based maintenance (CBM) of aircrafts in the aviation industry.

This paper will present a brief discussion on several techniques used for wear debris analysis and their effectiveness in monitoring the wear conditions of aircraft engines. These techniques can be grouped into three approaches; (i) compositional analysis, (ii) morphological analysis and (iii) particle quantification.

2 COMPOSITIONAL ANALYSIS

The compositional analysis approach involves the determination and monitoring the elemental contents of wear debris suspended in the oil sample. The concentration of each element determined is plotted against the operating time. A sudden increase in element content indicates abnormal wear and impending failure. It is a direct indication of sources of wear particles as most of the moving parts in an engine have different chemical compositions.

For this technique to be effective, threshold limits for key elements need to be established first. Key elements are the major elements in the wear surface of a component or those minor elements which are peculiar to a component. Threshold limits are characteristic for each type of engine and is determined empirically. The engine manufacturer is also able to provide this information. The threshold limits represent normal concentrations of wear elements in an engine that is behaving normally and provides a basis for distinguishing between normal and abnormal wear (Yu, 1985).

2.1 ATOMIC EMISSION SPECTROSCOPY (AES)

This is most the popular technique used for compositional analysis of wear metals. In this technique, the oil sample is subjected to a high energy environment. Ground state atoms in the sample absorb energy and become excited. The atoms spontaneously return to ground state and emit light. The emission spectrum emitted by atoms of different elements in the wear particles is detected and analyzed by the spectrometer. Results are usually reported as concentration in parts per million (ppm). Selected elements present in the wear particles are determined simultaneously.

Two types of AES are commonly used; Rotating Disc Electrode (RDE) method (ASTM D6595, 2005) and Inductively Coupled Plasma (ICP) method (ASTM D 5185, 2005).

The RDE atomic emission spectrometer is specially designed to analyze wear metals in oil. Special sample preparation is not required. After homogenization, sample is analyzed directly. During analysis, the sample is picked up by a rotating graphite disc electrode and subjected to a high voltage electric arc-spark. This method is simple and capable of detecting element concentration to a very low concentration level. However, analytical results are particle size dependent as it is unable to detect particles more than 10 μm in size (Rhine *et al*., 1985). Thus, larger wear particles caused by certain types of failure wear modes remain undetected (Barraclough *et al*., 2001).

In comparison, sample homogenization and dilution is needed prior to analysis for the ICP method. The diluted sample is fed into a high energy plasma torch in the ICP spectrometer for analysis. The ICP is argon plasma generated by the interaction of a radio fequency (RF) field and ionized argon gas. The ICP temperatures can reach around 10,000 K, allowing complete atomization of elements in the sample and minimizing chemical interferences. Thus the ICP method is able to detect elements of very low concentrations in the sample. However this method also suffers from particle size inadequacy, as it is capable of detecting particles of less than 5 μm in size only (Saba *et al*., 1981; Eisentraut *et al*., 1984).

To overcome the particle size inadequacy, a particle size independent method or acid digestion method was developed for ICP in which the oil sample was treated with strong acids to digest the large particles (Brown *et al*., 1980). The resulting solution was then analyzed on an ICP spectrometer.

2.2 ATOMIC ABSORPTION SPECTROSCOPY (AAS)

This is a traditional technique used for elemental analysis of metals. As it is a single element analysis technique, it is no longer a favoured technique for compositional analysis of wear metals in oil.

This technique involves feeding the oil sample into a flame burner to vaporize and atomize the metallic elements. The vaporized atoms are then subjected to a light energy of a specific wavelength for a particular element. The ground state atoms of the element absorb energy as they enter the excited state. The amount of energy absorbed is measured and result is reported as concentration in parts per million or percentage.

Similar sample homogenization and dilution as ICP method is required for AAS. However the single element analysis by AAS technique is slow and laborious when performing multi-element analysis on wear metals. The analytical results are particle size dependent. It is incapable of detecting particles of more than 3 μm. Its detection limit capabilities are lower compared to the AES technique (Saba *et al*., 1981; Woodrose, 2009). All these limitations have rendered AAS as a less popular technique for compositional analysis of wear metals.

2.3 X-RAY FLUORESCENCE (XRF)

XRF analysis is one of the latest elemental analysis techniques that are used for chemical compositional analysis of wear metals. This technique involves radiating the sample with primary x-rays, which are produced by electron bombardment in an x-ray tube. The primary x-rays stimulate the sample to emit its own characteristic x-rays. The emitted x-rays are then detected and analyzed to determine which elements are present and their quantities (Whitlock, 1996).

The two commonly used XRF methods are energy dispersive x-ray analysis (EDX) and wavelength dispersive x-ray analysis (WDX). The main difference between EDX and WDX is the detection and measurement of the intensity x-rays emitted. In an EDX spectrometer, the detector measures the energies of the electrons produced whereas a WDX spectrometer determines the spectral wavelengths by diffraction methods.

This technique is relatively fast and non-destructive to the sample; special sample preparation is not required other than homogenization. The composition of wear particles is readily determined irrespective of particle size. Because of its ability to detect larger particles in oil, it can detect wear metals earlier than AES and AAS technique (Sorvall, 2009).

As XRF technique can be used to perform direct analysis on solid samples, it is being used to analyze the wear particles collected from the oil filter rather than analysis of the oil (Humphrey, 1996; Madhavan, 2004).

3 MORPHOLOGICAL ANALYSIS AND PARTICLE QUANTIFICATION

Morphological analysis involves the examination of wear particles and the study of their structure, form and size. The morphology of wear particles are used to deduce component wear modes inside the engine. Several types of wears are indicative of abnormal behaviour within the engine. The sizes of abnormal wear particles are generally larger than particles from normal wears (Anderson, 1982).

Particle quantification is the measurement of the amount of wear particles generated either by counting or by estimation. It is used to determine the rate of emission of wear. An increasing wear production over time indicates abnormality. Techniques developed for morphological analysis generally are also able to perform particle quantification.

3.1 FERROGRAPHY

Ferography as its name implies, is used mainly for analysis of ferrous particles in wear debris. This technique consists of two methods; analytical ferrograph for morphological analysis and direct reading ferrograph for particle quantification.

Analytical ferrograph method involves separation of wear particles from the oil sample by a magnetic field and subsequent microscopic examination. The oil sample is allowed to flow on an inclined glass substrate (ferrogram) where all wear particles present are deposited with the application of a strong magnetic field. Particles ranging from less than 1 μm to greater than 2000 μm are captured on the substrate (Morovek, 2000; Anderson, 1982).

Microscopic examination of the ferrogram identifies the morphology and size of wear particles. With a high magnification bichromatic microscope, wear particles with different types of wear such as rubbing wear, fatigue, severe sliding, and cutting wear are readily identifiable (Anderson, 1982). Non-ferrous particles and other contaminants can also be identified with sufficient experience. The size of wear particles is determined using an image analyzer software.

The amount of wear particles deposited on the ferrogram is indicative of the severity of the wear condition. It can be used for particle quantification, by non-numerical estimation.

Direct reading ferrograph involves the measurement of size and amount of ferrous wear particles present in the oil sample. After a known volume of oil sample flows through a glass precipitator tube which is subjected to a powerful magnetic gradient field, two sets of readings are obtained; one for particles of larger than 5 μm (DL) and one for particles of less than 5 μm (DS). The DL and DS values may be used to calculate severity of wear index (WI) and wear particle concentration (WPC) (Anderson, 1982; Morovek, 2000). An engine wear trend baseline can be established. The amount of particles measurement is for ferrous particles only.

3.2 DIRECT IMAGE ANALYSIS

Direct image analysis is the latest technique developed for wear debris analysis. It displays morphological characteristics of wear debris and provides particle quantification measurements.

This technique uses a particle counter-cum-particle shape classifier, LaserNet Fines™ (LNF). It does not require any special sample preparation prior to analysis. The sample is directly drawn through a viewing flow cell with a pulsed laser diode. A CCD camera is used to capture image frames provided by the laser pulses. All the image frames are collected and analyzed by the provided software.

The image processing software is able to produce silhouette images of particles larger than 20 μm in major dimension. Morphological analysis is carried out automatically and these particle images are classified into different types of wears (Barraclough *et al*., 2001; Tucker *et al*, 2005).

LNF is also able to provide a highly accurate particle count for particles greater than 4 μm but less than 100 μm from the images obtained. It is able to display particle distributions based on size and type of wear (Spectro, 2005).

The main limitation of this technique is its inability to detect wear particles larger than 100 μm which are indicative of abnormality. Particle counting results also can be erroneous if the particles in the oil samples are not homogeneously re-dispersed prior to analysis.

3.3 MAGNETIC PLUG

This is the simplest technique used for particle quantification. A magnetic plug is inserted along the flow line of the engine lubrication system. The magnet traps ferrous wear particles present when the oil flows past it. The plug is checked regularly and the quantity of the wear particles collected is estimated visually. Particle morphology is examined using a magnifying glass or a microscope. Depending on the magnification of the microscope used, particles examined may range from 25 to 1000 μm (Smith, 2003).

This technique is only specific for ferrous metals. Non-ferrous wear particles escape without detection Quantification is by estimation only, not numerical or qualitative in nature.

Most aircraft operators practice this technique as it is simple and most aircraft engines are fitted with magnetic plugs. It is the first front line maintenance check for the engine. The magnetic plug is also designed so that a warning signal will be sent to the cockpit if excessive wear particles are collected.

4 SELECTION OF APPROACHES AND TECHNIQUES

As discussed above, each approach is able to identify only certain aspects of wear trends and is incapable of providing a full profile of engine wear particles. In order to obtain a full picture of wear condition in an engine, all three approaches should be applied concurrently in a comprehensive wear debris analysis program.

When comes to selection of analysis techniques, several factors need to be considered. Other than the techniques' inherent limitations discussed earlier, factors such as setup cost, availability of equipment, ease of operation, operating cost and sample preparation also need to be deliberated.

Three different techniques are being used in our current project to study the wear debris generated in the engines of Agusta helicopters. The selected techniques, XRF, ferrography and direct image analysis, include all three approaches discussed and will give a good profile of wear particles trends.

5 SUMMARY

The approaches and techniques discussed above are proven and some are in wide usage. Each technique has its own strengths and weaknesses. With the application of various wear debris analysis techniques, it will be able to determine the type, severity and rate of progression of mechanical faults in engines by measuring the size distribution, rate of production and the morphological characteristics of debris particles. Based on the information obtained, corrective actions and preventive maintenance can be implemented in a timely fashion to prevent possible impending failures in the engine.

REFERENCES

Anderson, D.P. (1982). Wear Particle Atlas (Revised). Report NAEC-92-163, Naval Air Engineering Center, Lakehurst, New Jersey.

ASTM D 6595 (2005). Standard test Method for Determination of Wear Metals and Contaminants in Used Lubricating Oils or Used Hydraulic Fluids by Rotating Disc Electrode Atomic Emission Spectroscopy. ASTM International, West Conshohocken, US.

ASTM D 5185 (2005). Standard Test Method for Determination of Additive Elements, Wear Metals, and Contaminants in Used Lubricating Oils and Determination of Selected Elements in Base Oils by Inductively Coupled Plasma Atomic Emission Spectrometry (ICP-AES). ASTM International, West Conshohocken, US.

Barraclough, T.G., Anderson, D.P. & Lukas, M. (2005). Comparison of Wear and Contaminant Particles Analysis Techniques in an Engine Test Cell Run to Failure. *LaserNet Particle Shape Classifier & Particle Counter*, Spectro Incorporated, Littleton, MA, 29-39, 2005.

Barraclough, T.G., Anderson, D.P. & Lukas, M. (2001). Direct Image Analysis for Detecting Abnormal Wear and Contamination in Used Oil Sample, *2001 Practicing Oil Analysis Conference*, Littleton, MA, US.

Brown, J.R., Saba, C.S., Rhine W.E. & Eisentraut, K.J. (1980). Particle Size Independent Spectrometric Determination of Wear Metals in Aircraft Lubricating Oils*, Anal. Chem.*, **52:** 2365-2370.

Eisentraut, K.J., Newman, R.W., Saba, C.S., Kauffman, R.E., & Rhine W.E. (1984). Spectrometric Oil Analysis – Detecting Failures Before they Occur, *Anal. Chem.*, **56:** 1086A-1094A.

Humphrey, G.R., (1996). Joint Strike Fighter – Analysis of Filter Debris by Energy Dispersive X-ray Fluorescence, *JOAP International Condition Monitoring Conference, Technology Showcase 2000,* Mobile, AL, April 3-6, 2000.

Madhavan, P., Steves, M., Rosenberg, G. & Schindler, J. (2004). Condition Monitoring of Aerospace Hydraulic and Lubrication Systems via Filter Debris Analysis', *Joint Oil Analysis Program (JOAP),* April 18-22, 2004.

Morovek, L. (2000). Ferrography: Modern Maintenance Tool, Predict/DLI, Cleveland, Ohio.

Rhine W.E., Saba, C.S., & Kauffman, R.E., (1985). Metal particle detection capabilities of rotating-disk emission spectrometers, *J. of Am. Soc. of Lubrication Eng.*, **42:** 755-761.

Saba, C.S., Rhine, W.E. & Eisentraut, K.J. (1980). Efficiencies of Sample Introduction Systems for the Transport of Metallic Particles in Plasma Emission and Atomic Absorption Spectrometry, *Anal. Chem.*, **53**: 1099-1103.

Smith, M. (2003). Oil Analysis vs. Microscopic Debris Analysis: When and Why to Choose. Analyst Inc., Los Angeles, California.

Sorvall. (2009). EDX Analysis of Filter Debris. Available online at: http://www.sorvall.com/com/cda/product_application_details/0,1063,10782,00. (Last access date: 5th November 20009)

Spectro Inc. (2005). LaserNet Particle Shape Classifier & Particle Counter. Spectro Incorporated, Littleton, MA.

Tucker, J.E., Reintjes, J., Galie, T.R., Schultz A., Lu, C., Tankersley, L.L., Sebok, T., Holloway, C. & Howard, P.L. (2005). Lasernet Fines Optical Wear Debris Monitor, A Navy Shipboard Evaluation of CBM Enabling Technology, *LaserNet Particle Shape Classifier & Particle Counter*, Spectro Incorporated, Littleton, MA, 40-49, 2005.

Walsh, D.P. (2005). Oil Analysis 101. *ORBIT*, **25:** 50-55.

Whitlock, R.R. (1996). Filter Debris Analysis Using XRF. US Naval Research Laboratory, Washington, DC.

Woodrose. (2009). An Overview of Atomic Spectroscopy. Available online at: http://www.woodrose.tripod.com/Atomic Spectroscopy.htm (Last access date: 5th November 2009)

Yu, C.L. (1985). Predicting engine failure. *Defence Science Seminar,* Kuala Lumpur, 1985.

CETAKAN TANDA KESELAMATAN MENGGUNAKAN DAKWAT *INVISIBLE ULTRAVIOLET*

Mohamad Ismail Haji Ali*, Norkamizah Mohd Nor, Zariyah Ariffin, Nor Hafizah Mohamed, Rozita Md Salleh, Jamaliah Mohd Noor, Loo Soon Tong & Shurihan Ahmad

Bahagian Pengurusan Sumber Manusia & Khidmat Sokongan
No 17 & 19, Jalan Seksyen 3/6
Taman Kajang Utama
43000 Kajang Selangor
Tel: 03-87337133
Fax: 03-87335979
*Email: ismail.ali@stride.gov.my

ABSTRAK

Dalam proses perolehan peralatan pertahanan, Institut Penyelidikan Sains & Teknologi Pertahanan (STRIDE) telah diiktiraf oleh Kementerian Pertahanan sebagai organisasi yang terlibat di dalam proses membangun, menyemak dan mengesahkan Spesifikasi Perolehan Pertahanan berdasarkan piawaian yang ditetapkan, di samping memenuhi keperluan pengguna dan mematuhi aturan perkhidmatan. Terdapat beberapa kes di mana maklumat di dalam Spesifikasi Perolehan Pertahanan yang disahkan telah diubahsuai oleh pihak yang tidak bertanggungjawab. Justeru itu, STRIDE telah mengambil inisiatif untuk mewujudkan sistem cetakan tanda keselamatan bagi memastikan keselamatan dokumen Spesifikasi Perolehan Pertahanan dengan menggunakan dakwat invisible Ultraviolet (UV). Tanda keselamatan direka khas untuk dokumen Spesifikasi Perolehan Pertahanan dan dicetak pada setiap helaian dokumen menggunakan dakwat invisible UV. Tanda keselamatan ini akan ditukar setiap bulan bagi menjamin keselamatan dokumen berkenaan.

Keywords: *Invisible UV*; *Spesifikasi Perolehan Pertahanan; cetakan tanda keselamatan.*

1 PENGENALAN

Institut Penyelidikan Sains & Teknologi Pertahanan (STRIDE) telah diberikan tanggungjawab di dalam pembangunan, penyemakan dan pengesahan Spesifikasi Perolehan Pertahanan bagi memastikan semua spesifikasi mematuhi keperluan **Surat Pekeliling Perbendaharaan (SPP) Bil. 5/2007 Tatacara Pengurusan Perolehan Kerajaan Secara Tender**, dan juga semua Arahan, Pekeliling dan Surat Pekeliling Kerajaan lain yang berkaitan. Butir-butir spesifikasi perolehan yang diterima oleh STRIDE dari tahun 2003 hingga 2009 adalah seperti di dalam Jadual 1.

Kronologi pembangunan cetakan keselamatan di dalam Spesifikasi Perolehan Pertahanan bermula apabila dokumen yang telah disahkan dihantar kepada pihak pengguna untuk proses perolehan. Tiada sistem yang dapat menjamin keselamatan dokumen dan memastikan kandungannya dari dipinda oleh pihak yang tidak bertanggungjawab. Maklumat di dalam dokumen boleh dipinda oleh pihak yang berkepentingan tanpa kebenaran dan penipuan ini sukar dikesan.

Sebelum ini, dokumen Spesifikasi Perolehan Pertahanan dicetak menggunakan pencetak biasa. Beberapa masalah telah dikenalpasti, iaitu terdapat beberapa kes di mana isi kandungan dokumen yang telah disahkan oleh STRIDE telah ditukar dan dicetak semula oleh pihak pengguna sebelum dihantar ke Bahagian Perolehan Kementerian Pertahanan. Tandatangan pengesah dokumen telah ditiru dengan menggunakan mesin pengimbas dan penipuan tidak disedari dan tidak dapat dikesan, di mana kes hanya diketahui apabila terdapat aduan daripada pihak pembekal dan Bahagian Perolehan. Keselamatan maklumat di dalam dokumen tidak terjamin dan keaslian dokumen terjejas serta kualiti perolehan yang dibekalkan tidak mengikut spesifikasi sebenar apabila dokumen spesifikasi diubah.

Jadual 1 : Bilangan penerimaan dan pengesahan spesifikasi.
(Sumber: Cawangan Penyelidikan & Kajian Strategik, STRIDE)

Tahun	Bilangan Penerimaan Spesifikasi	Bilangan Pengesahan Spesifikasi
2003	201	146
2004	210	191
2005	281	233
2006	336	253
2007	262	308
2008	172	165
Jun-09	77	93

Menurut Anderson (2008), tanda keselamatan merupakan salah satu teknik dalam cetakan keselamatan untuk melindungi maklumat. Justeru itu, STRIDE mengambil inisiatif untuk mewujudkan sistem cetakan tanda keselamatan bagi memastikan keselamatan dokumen Spesifikasi Perolehan Pertahanan. Cetakan tanda keselamatan merupakan satu teknik percetakan yang berfungsi untuk melindungi dan memelihara isi kandungan dokumen spesifikasi perolehan pertahanan daripada dipinda tanpa kebenaran.

Menurut Almer (2009), trend keselamatan dokumen yang terkini tertumpu kepada kemampuan gabungan sistem yang mempunyai ciri-ciri yang sangat efektif. Usaha menentang penipuan dan mencegah capaian tanpa kebenaran pada kebanyakan aplikasi sektor awam dan swasta menggunakan gabungan pelbagai ciri-ciri integrasi keselamatan. Ciri-ciri tersebut boleh dibahagikan kepada tiga kategori: boleh dilihat, tidak boleh dilihat dan forensik. Ciri-ciri boleh dilihat termasuklah corak garisan, *guilloches*, cetakan pelangi, *OVI* dan *holographic foils* serta boleh dikenalpasti dengan mata kasar. Dalam sesetengah kes, ciri-ciri keselamatan ini hanya boleh dilihat dengan menggunakan peralatan tertentu. Sebagai contoh, cetakan *Ultraviolet* (*UV*) dan *Invisible Personal Information (IPI)*. Kategori ketiga merupakan ciri forensik yang hanya boleh disiasat dengan menggunakan peralatan khas.

Keselamatan maklumat di dalam Spesifikasi Perolehan Pertahanan amatlah penting. Dengan itu, cetakan dengan menggunakan dakwat *invisible UV* merupakan teknik cetakan yang selamat. Dakwat *invisible UV* tidak dapat dilihat dengan mata kasar, tetapi hanya dapat dilihat dibawah sinaran lampu *UV (LDP Net, 2009)*. Ciri-ciri ini merupakan faktor penting mengapa dakwat *invisible UV* dipilih bagi digunakan dalam perlaksanaan cetakan tanda keselamatan untuk melindungi dan mengesahkan dokumen (G7 Productivity Systems,2009).

Tanda keselamatan telah direka khas untuk dokumen Spesifikasi Perolehan Pertahanan dan dicetak pada setiap helaian dokumen menggunakan dakwat *invisible UV*. Tanda keselamatan ini akan ditukar setiap bulan untuk menjamin keselamatan.

Objektif utama pelaksanaan sistem ini adalah untuk memelihara keaslian dokumen bagi mengelakkan maklumat dalam dokumen dipinda tanpa kebenaran. Objektif lain adalah seperti berikut :

a. Melengkapkan STRIDE dengan sistem percetakan yang mempunyai ciri-ciri keselamatan yang terkini

b. Memelihara keaslian maklumat di dalam dokumen spesifikasi dari diubah oleh pihak yang tidak bertanggungjawab

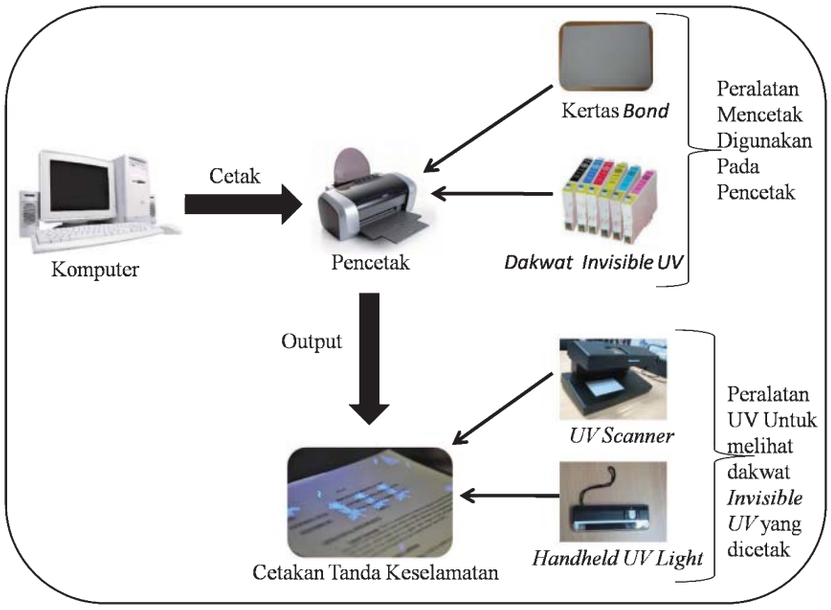
c. Memastikan proses aliran kerja spesifikasi telus dan berintegriti

d. Memastikan perolehan memenuhi tahap kualiti yang ditetapkan dan berpadanan dengan harga yang ditawarkan.

e. Memastikan perolehan yang dilaksanakan adalah tidak menjurus kepada sesuatu produk atau jenama sahaja.

2 KOMPONEN SISTEM

Komponen-komponen bagi sistem cetakan tanda keselamatan adalah terdiri daripada komputer, pencetak, kertas *bond,* dakwat *invisible UV,* dan *UV light* yang terdiri dari jenis *handheld* dan *scanner* (Rajah 1).



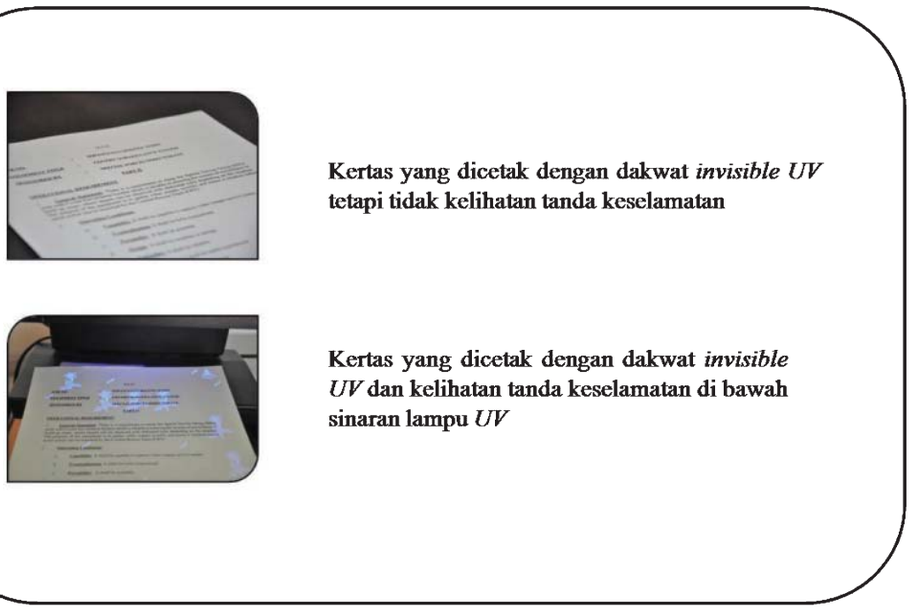
Rajah 1: Komponen sistem cetakan tanda keselamatan.

Rajah 2 menunjukkan contoh tanda keselamatan yang telah dicetak pada kertas *bond* dengan menggunakan dakwat *invisible UV*. Tanda keselamatan ini hanya dapat dilihat di bawah sinaran lampu *UV*.

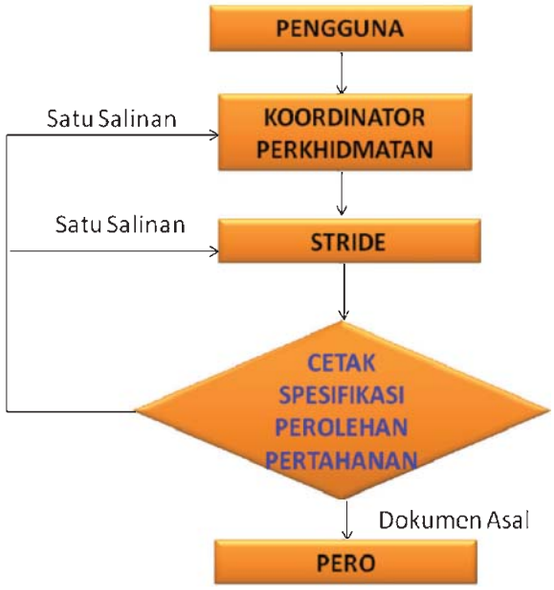
3 PELAKSANAAN

Setiap helaian dokumen Spesifikasi Perolehan Pertahanan yang telah dibuat semakan dan sedia untuk pengesahan dicetak mengunakan tanda keselamatan yang dicipta khusus untuk dokumen perolehan. Tanda keselamatan akan dicetak dengan menggunakan dakwat *invisible UV* dan akan ditukar setiap bulan bagi mengelak dari dikesan oleh mereka yang tidak bertanggungjawab.

Setelah pengesahan dibuat dokumen asal dimajukan kepada Bahagian Perolehan. Salinan diberikan kepada pengguna dan juga untuk simpanan STRIDE. Bahagian Perolehan yang berperanan sebagai bahagian yang menguruskan perolehan pertahanan telah dibekalkan dengan *UV Scanner* bagi tujuan mengimbas dokumen Spesifikasi Perolehan Pertahanan. Tanda keselamatan yang terdapat pada helaian dokumen Spesifikasi Perolehan Pertahanan dimaklumkan kepada Bahagian Perolehan sahaja bagi tujuan mengesan helaian yang dipinda oleh mereka yang tidak bertanggungjawab. Carta alir proses kerja ini adalah seperti di dalam Rajah 3.



Rajah 2: Cetakan tanda keselamatan pada kertas *bond*.



Rajah 3: Aliran proses kerja untuk cetakan tanda keselamatan.

4 KEBERKESANAN SISTEM

Spesifikasi Perolehan Pertahanan memainkan peranan penting di dalam menggariskan panduan untuk menentukan perolehan peralatan yang diperlukan memenuhi kehendak pengguna. Bagi tujuan tersebut, sistem ini dibangunkan untuk memelihara keselamatan dokumen spesifikasi perolehan dari disalahgunakan melalui penggunaan dakwat *invisible UV* yang tidak dapat dilihat dengan mata kasar atau disalin semula. Dengan cara ini, pemalsuan dokumen dapat dikesan bagi memelihara maklumat dalam dokumen dari dipinda tanpa kebenaran setelah dibuat pengesahan, mengelakan perolehan menjurus kepada sesuatu jenama atau buatan sahaja dan memberi peluang yang sama rata kepada semua pembekal yang layak untuk bersaing.

5 ANALISIS CETAKAN TANDA KESELAMATAN

Satu kajian telah dijalankan bagi mendapatkan maklumbalas pihak yang terlibat secara langsung di dalam penggunaan cetakan tanda keselamatan bagi Spesifikasi Perolehan Pertahanan, iaitu Bahagian Perolehan, Kementerian Pertahanan. Responden kajian adalah merupakan penyelaras di unit-unit Perolehan iaitu PERO 1 , PERO 2, PERO 3, PERO 4, PERO 5, PERO 7 dan PERO 8. PERO 6 tidak terlibat di dalam kajian ini kerana tidak menguruskan perolehan peralatan.

Daripada analisis tersebut, didapati bahawa semua responden bersetuju dengan penggunaan cetakan tanda keselamatan bagi Spesifikasi Perolehan Pertahanan kerana sistem ini adalah berkesan, mesra pengguna dan dapat mengelakkan daripada pindaan maklumat oleh pihak yang tidak bertanggungjawab, di samping dapat menyelesaikan masalah yang timbul sebelum ini.

Selain daripada itu, sistem ini adalah merupakan teknik penyelesaian yang kreatif, efektif dan inovatif. Daripada ketujuh-tujuh unit PERO tersebut, didapati bahawa 100% adalah bersetuju agar penggunaan cetakan tanda keselamatan ini diteruskan. Sebanyak 30% daripada responden mencadangkan agar sistem ini dibuat penambahbaikan.

Secara keseluruhannya adalah didapati bahawa sistem ini adalah merupakan penyelesaian terbaik bagi mengatasi masalah yang timbul di dalam proses pembangunan, penyemakan dan pengesahan Spesifikasi Perolehan Pertahanan

6 SIGNIFIKAN

Perlaksanaan cetakan tanda keselamatan telah memberikan impak yang signifikan kepada keberkesanan dan kecekapan sistem penyampaian perkhidmatan awam:

a. Impak kepada Perkhidmatan Awam

Pelaksanaan cetakan tanda keselamatan dapat mengelakkan rasuah di Kementerian Pertahanan, dan melahirkan pegawai serta kakitangan kementerian yang berintegriti tinggi. Di samping itu, keselamatan Spesifikasi Perolehan Pertahanan yang dicetak dengan menggunakan proses ini adalah terjamin. Sebarang pengubahsuaian terhadap dokumen sebenar yang telah dicetak dengan menggunakan kaedah ini tidak dapat dilakukan oleh pihak yang berkepentingan. Dokumen yang dicetak melalui kaedah ini mengandungi ciri-ciri keselamatan yang memberi ketelusan dalam perolehan pertahanan

b. Impak kepada pengguna

Keaslian dokumen Spesifikasi Perolehan Pertahanan tanpa sebarang pengubahsuaian adalah penting bagi memenuhi kepuasan pelanggan dan kebolehpercayaan dalam menilai dokumen yang dihasilkan berdasarkan perbincangan dan rundingan. Di samping itu, cetakan tanda keselamatan dengan menggunakan dakwat invisible *UV* ini dapat memberikan keyakinan kepada pelanggan tentang kesahihan dokumen yang diterima dan diterimapakai tanpa rasa ragu.

c. Impak kepada pengurusan

Impak kepada pengurusan dapat dibahagikan kepada dua, iaitu dari sudut pelaksanaan dan pengurusan tender. Dari sudut pelaksanaan, ianya dapat memberikan jaminan bahawa setiap

dokumen asal yang dicetak dengan menggunakan dakwat *invisible UV* dihantar terus ke Bahagian Perolehan tanpa sebarang penyelewengan. Dokumen boleh dirujuk berdasarkan salinan yang disimpan di STRIDE atau pihak pengguna sendiri. Dari sudut pengurusan tender pula, ia memastikan nilai-nilai ketelusan dan akauntabiliti bagi menghindari sebarang kemungkinan penyelewengan di kalangan pengguna kerajaan dan pembekal di mana perolehan kerajaan dapat dijimatkan dan pengguna dapat memperolehi peralatan yang memenuhi keperluan sebenar.

5. PENUTUP

Secara keseluruhannya, teknik yang dihasilkan ini telah berjaya dilaksanakan sepenuhnya, memenuhi ciri-ciri *replicability* dan terbukti boleh digunapakai oleh agensi-agensi lain dengan pengubahsuaian mengikut keperluan tanpa melibatkan kos yang tinggi. Teknik ini merupakan idea asal STRIDE yang dapat memberi impak yang tinggi terutama dari segi keselamatan Spesifikasi Perolehan Pertahanan. Ianya juga memenuhi ciri-ciri signifikan dan telah terbukti memberi impak kepada keberkesanan dan kecekapan sistem penyampaian perkhidmatan awam. Adalah didapati bahawa sistem ini merupakan penyelesaian terbaik bagi mengatasi masalah pengubahsuaian maklumat dokumen Spesifikasi Perolehan Pertahanan yang telah disahkan oleh STRIDE

PENGHARGAAN

Penulis amat berterima kasih kepada En Hasan bin Rahman, En Wong Siew Kwan dan Puan Halijah Ahmad kerana membantu dalam menjayakan kajian ini.

RUJUKAN

Anderson, R. (2008). Security Engineering**:** A Guide to Building Dependable Distributed Systems (2nd Edition). Wiley, U.S.

Almer, G. (2009). Document security. *Keesing J. Doc. Identity*, **29:** 20-23.

G7 Productivity Systems (2009). G7 Introduces Invisible Ink for Inkjet Printers. Dari laman web: http://www.g7ps.com/scripts/pressrelease/pr_20070910.pdf (Tarikh akses terakhir : 4 Februari 2009).

LDP Net (2009). UV Inks. Dari laman web: http://www.maxmax.com/aUVInks.htm (Tarikh akses terakhir: 12 Januari 2009).

EVALUASI KEBERKESANAN PENENTUAN KEUTAMAAN PROJEK R&D PERTAHANAN DENGAN MENGGUNAKAN *ANALYTICAL HIERARCHY PROCESS (AHP)*

Nor Hafizah Mohamed*, Zariyah Ariffin, Khalid Mohammad,
Mohamad Ismail Hj Ali, Fadzli Ibrahim & Rozita Md Salleh

Bahagian Pengurusan Sumber Manusia & Khidmat Sokongan
STRIDE
Tel: 03-87337133
Faks: 03-87335979
*Email: norhafizah.mohamed@stride.gov.my

Abstrak

Penentuan keutamaan projek-projek R&D Pertahanan Institut Penyelidikan Sains & Teknologi Pertahanan (STRIDE) adalah ditentukan berdasarkan keputusan daripada Bengkel Penentuan Keutamaan R&D yang diadakan setiap dua tahun sekail bagi memastikan projek yang akan dijalankan bertepatan dengan kehendak Angkatan Tentera Malaysia (ATM), Kementerian Pertahanan dan seterusnya, negara. Pemilihan dan penentuan keutamaan projek R&D Pertahanan ditentukan melalui kaedah percambahan fikiran (brainstorming) dan dianalisa menggunakan teknik Analisis Delphi. Analisis Delphi ini hanya menggunakan perbandingan dua kriteria yang terdiri daripada kepentingan strategik (Strategic Importance) dan keupayaan (Capacity) serta tidak mengambil kira kriteria-kriteria lain. Bagi mengatasi limitasi ini, teknik Analytical Hierarchy Process (AHP) telah digunakan untuk menjalankan pemilihan dan penentuan keutamaan cadangan Projek R&D Pertahanan di bawah Rancangan Malaysia Kesepuluh (RMK-10). Teknik ini mengambilkira kepelbagaian kriteria dalam membuat sesuatu keputusan atau lebih dikenali Multicriteria Decision Making (MCDM). AHP telah diaplikasikan semasa dua siri Bengkel Penentuan Keutamaan R&D Pertahanan Rancangan Malaysia Kesepuluh (RMK-10) di mana sebanyak 36 projek R&D Pertahanan telah dibentangkan. Objektif kertas kerja ini adalah untuk menjalankan evaluasi keberkesanan AHP di dalam penentuan keutamaan projek R&D pertahanan. Didapati yang keputusan yang diperolehi melalui teknik AHP adalah lebih efektif berbanding menggunakan teknik Analisis Delphi yang digunakan sebelum ini. Dengan adanya teknik ini, ia telah memberi keputusan yang tepat dan tidak berat sebelah.

Kata Kunci: *Analytical Hierarchy Process* (AHP); *Multicriteria Decision Making* (*MCDM); kriteria; alternatif.*

1 PENDAHULUAN

Bengkel Penentuan Keutamaan R&D Pertahanan yang diadakan setiap dua tahun sekali adalah salah satu inisiatif Institut Penyelidikan Sains & Teknologi Pertahanan (STRIDE) untuk menentukan keutamaan projek-projek R&D Pertahanan. Kaedah penilaian yang digunakan dalam menentukan pemilihan dan keutamaan projek R&D Pertahanan adalah melalui teknik Analisis Delphi. Analisis Delphi ini hanya menggunakan perbandingan dua kriteria yang terdiri daripada kepentingan strategik (*Strategic Importance*) dan keupayaan (*Capacity*) serta tidak mengambil kira kriteria-kriteria lain.

Analisis ini menggunakan teknik model pemarkahan berdasarkan kepada dua kriteria seperti di atas yang dinilai oleh setiap kumpulan mengikut bidang kepakaran. *Bias* telah wujud dalam situasi ini dan berkemungkinan besar ahli bagi setiap kumpulan dipengaruhi dengan pendapat-pendapat ahli yang lain semasa sesi percambahan fikiran (*brainstorming*). Oleh yang demikian, terdapat banyak

percanggahan di dalam memperolehi keputusan penentuan projek semasa menggunakan analisis ini. Kaedah ini juga merupakan metodologi ramalan pendapat secara kualitatif.

Bagi mengatasi limitasi ini, teknik *Analytical Hierarchy Process* (AHP) telah digunakan untuk menjalankan pemilihan dan penentuan keutamaan cadangan Projek R&D Pertahanan di bawah Rancangan Malaysia Kesepuluh (RMK-10). AHP, yang telah diperkenalkan oleh Saaty (1980), merupakan teknik pembuatan keputusan yang melibatkan kepelbagaian kriteria– *Multicriteria Decision Making* (MCDM). Dalam mengaplikasikan teknik AHP, satu struktur permasalahan berdasarkan kajian yang dijalankan telah direkabentuk dalam bentuk hierarki yang mana matlamat (*goal*) diletakkan di tahap paling atas diikuti kriteria, dan yang paling bawah di dalam hierarki adalah alternatif. Melalui teknik ini, satu kaedah yang digunakan ialah perbandingan berpasangan antara kriteria, sub kriteria, sub-sub kriteria dan alternatif yang digambarkan seperti di dalam Rajah 1.

Rajah 1: Contoh bentuk hierarki AHP.
(Sumber: Decision Lens (1994))

Teknik AHP adalah bergantung kepada penilaian dan pengadilan daripada manusia (*human judgement*) dan nilai pemberat (*weights*) dalam membuat keputusan. Penilaian atau perbandingan berpasangan menggunakan matrik timbal balik berdasarkan skala kepentingan{1 – 9} (Stair & Render, 1992; Partovi, 1994; Omkarprasad & Kumar, 2006) dapat menerangkan tahap kepentingan di antara kriteria utama, sub kriteria dan sub-sub kriteria, iaitu sama ada kedua-dua kriteria sama penting, sederhana penting, lebih penting ataupun lebih penting secara ekstrima . Perincian skala tersebut adalah seperti berikut :

1 - Kedua-dua faktor sama penting
3 - Satu faktor lebih penting sedikit daripada faktor yang lain
5 - Satu faktor lebih penting secara kuat daripada satu faktor yang lain
7 - Satu faktor lebih penting secara sangat kuat daripada satu faktor yang lain
9 - Satu faktor lebih penting secara ekstrima daripada satu faktor yang lain

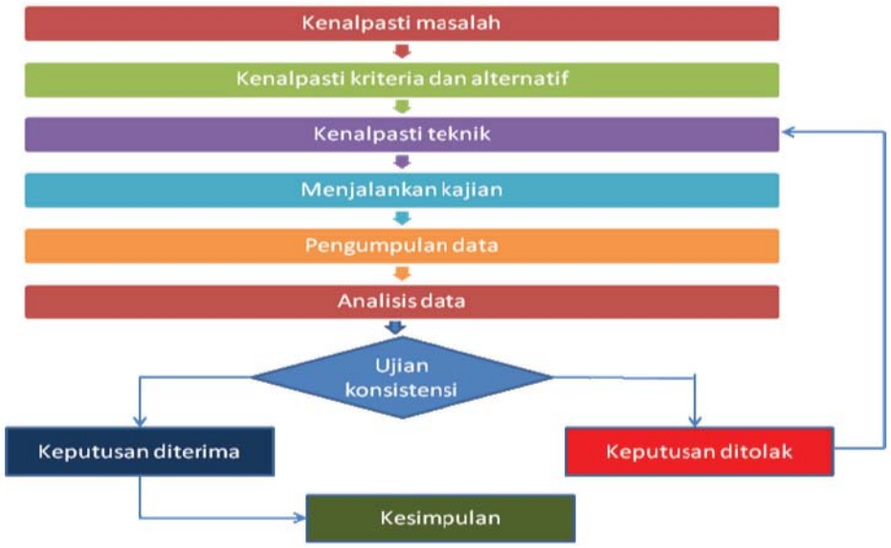
2,4,6,8 - Nilai di antara dua skala

AHP telah diaplikasikan semasa dua siri Bengkel Penentuan Keutamaan R&D Pertahanan Rancangan Malaysia Kesepuluh (RMK-10), iaitu Bengkel Siri 1/2009 yang diadakan pada 20- 21 Julai 2009, dan Bengkel Siri 2/2009 pada 1 Oktober 2009, di mana sebanyak 36 projek R&D Pertahanan telah dibentangkan. Kertas kerja ini akan menjalankan evaluasi keberkesanan AHP di dalam penentuan keutamaan projek R&D pertahanan. Di atas sebab-sebab kerahsian, maklumat terperinci mengenai projek-projek yang dibentangkan di dalam kedua-dua bengkel tersebut tidak akan disertakan di dalam kertas kerja ini. Sebaliknya, tumpuan akan diberikan kepada aspek-aspek berikut:

i) Pengenalpastian kriteria yang diperlukan dalam memilih projek R&D pertahanan
ii) Perbandingan di antara projek R&D Pertahanan yang dipersembahkan
iii) Pengenalpastian kriteria mengikut keutamaan
iv) Pemastian keputusan pemilihan projek R&D adalah tepat dengan merujuk kepada nilai konsistensi

2 METODOLOGI PENENTUAN KEUTAMAAN PROJEK R&D PERTAHANAN

Ringkasan metodologi penentuan keutamaan projek R&D Pertahanan adalah seperti di dalam Rajah 2. Metodologi ini telah digunakan bagi menilai projek-projek yang telah dibentangkan di dalam dua Bengkel Penentuan Keutamaan R&D yang telah diadakan. Sebanyak 36 projek telah dibentangkan, iaitu 27 projek semasa dari Bengkel Siri 1/2009, dan 9 projek semasa Bengkel Siri 2/2009.



Rajah 2: Carta alir proses penyelidikan.

Di dalam kajian ini, terdapat beberapa langkah/peringkat yang telah diikuti bagi memperolehi penentuan keutamaan alternatif yang terbaik dan tepat. Langkah-langkah tersebut dihuraikan di dalam Rajah 3.

Rajah 3: Langkah-langkah penentuan keutamaan alternatif.

2.1 Andaian

Penentuan keutamaan projek telah dibuat berdasarkan andaian berikut:

i) Bagi mengelakkan *bias* di dalam membuat keputusan, setiap kumpulan adalah terdiri daripada multi-disiplin iaitu pelbagai bidang kepakaran, pengalaman, pangkat dan perkhidmatan. Adalah diandaikan responden mempunyai pengetahuan dan memahami setiap projek yang dibentangkan dan mampu untuk menjawab borang soal selidik dengan lebih tepat.

ii) Data yang dikumpul adalah *reliable* berdasarkan ujian kebolehpercayaan di mana nilai *cronbach's alpha* yang diperolehi adalah melebihi 0.80. Menurut *rules of thumb* bagi saiz pekali *cronbach's alpha* yang mempunyai nilai yang lebih besar daripada 0.60 adalah boleh diterimapakai. *Rules of thumb* bagi saiz pekali *cronbach's alpha*, (Hair *et al.*, 2003) secara terperinci adalah seperti Jadual 1.

Jadual 1: *Rules of thumb* bagi saiz pekali *cronbach's alpha.*
(Sumber: Hair *et al.* (2003))

Alpha Coefficient Range	*Strength of Association*
< 0.6	*Poor*
0.6 – < 0.7	*Moderate*
0.7 - < 0.8	*Good*
0.8 - < 0.9	*Very Good*
0.9	*Excellent*

** If alpha > 0.95, items should be inspected to ensure they measure difference aspects of the concept.*

2.1 Instrumen Penentuan

2.2.1 Borang Soal Selidik

Instrumen yang digunakan untuk teknik ini adalah borang soal selidik yang dibangunkan berdasarkan matlamat dan faktor-faktor yang hendak dicapai dan menggunakan kaedah pemberat nombor. Borang soal selidik ini direkabentuk mengikut skala *likert* {1-5} bagi memudahkan pengukuran dibuat. Secara umumnya, borang soal selidik ini terbahagi kepada dua bahagian, iaitu perbandingan berpasangan antara criteria dan perbandingan berpasangan antara alternatif. Borang ini diagihkan kepada semua

peserta untuk mendapatkan skor penilaian bagi setiap projek yang dibentangkan. Selain itu, borang penilaian pemarkahan juga dibangunkan untuk mendapatkan skor pemberat bagi setiap kriteria yang ditetapkan oleh pihak pengurusan STRIDE.

2.2.2 Kriteria

Kriteria yang telah dipilih adalah terdiri daripada 9 kriteria utama, 29 sub kriteria dan 12 sub-sub kriteria. Pemilihan elemen-elemen kriteria,sub kriteria dan sub sub kriteria ditentukan melalui maklumat yang diperolehi dari pihak pengurusan STRIDE.

2.2.3 Alternatif

Sebanyak 36 projek yang telah dibentangkan bagi kedua-dua bengkel tersebut. Kesemua projek yang dibentangkan itu merupakan alternatif di dalam kajian ini dalam menentukan keutamaan projek.

2.3 Analisis Data

Setelah data dikumpul, data telah dianalisa menggunakan matriks perbandingan berpasangan dan dibantu dengan teknik AHP melalui perisian *Expert Choice* bagi memudahkan dan memastikan pengiraan adalah tepat.

2.3.1 Analisis Menggunakan Perisian Expert Choice

2.3.1.1 Input Daripada Pihak Pengurusan

Bagi mendapatkan input daripada pihak pengurusan berkenaan pemberat bagi setiap kriteria, borang penilaian pemarkahan telah diedarkan. Hasil daripada data yang diperolehi telah dimasukkan ke dalam perisian dengan menggunakan kaedah *direct*. Analisis diteruskan dengan membuat perbandingan berpasangan (*pair-wise comparison*) antara setiap kriteria dan output.

2.3.1.2 Input Daripada Responden (Peserta Bengkel)

Bagi mendapatkan input daripada responden, borang soal selidik telah diedarkan kepada setiap peserta bengkel. Responden telah dibahagikan kepada 10 kumpulan, setiap kumpulan adalah terdiri daripada pelbagai disiplin bagi mendapatkan 10 input untuk dimasukkan ke dalam perisian dan seterusnya dianalisis.

2.3.1.3 Ujian Konsistensi Data

Di dalam kajian yang menggunakan teknik AHP, pengujian konsistensi amat penting di dalam memastikan keputusan yang diperolehi melalui pengiraan ataupun perisian boleh diterima pakai. Menurut Ayag & Ozdemir (2006), secara amnya, data adalah konsisten (*Consistency Ratio*) jika:

$$\text{Consistency Ratio (CR)} = \frac{\text{Consistency Index (CI)}}{\text{Random Index (RI)}} < 0.10 \quad \text{Adalah konsisten (boleh diterima)}$$

$$\text{Dan,} \quad \frac{\text{Consistency Index (CI)}}{\text{Random Index (RI)}} > 0.10 \quad \text{Adalah tidak konsisten (tidak boleh diterima)} \qquad (1)$$

Nilai pengujian konsistensi bagi kajian ini adalah bermakna dan boleh diterima kerana nilai konsistensi kurang dan menghampiri 0. Ini menunjukkan bahawa hasil daripada kajian ini boleh diterima untuk dibuat kesimpulan.

3 ANALISA

3.1 Limitasi Dan Masalah Kajian

Secara keseluruhannya dalam menjalankan kajian ini tim kajian terpaksa menghadapi beberapa kekangan dan masalah yang perlu diatasi bagi mendapatkan hasil kajian yang berkualiti dan tepat.

Masalah pertama ialah bilangan responden yang menilai bagi setiap projek adalah berbeza. Oleh yang demikian, tim ini terpaksa mengambil inisiatif untuk membahagikan penilai kepada 10 kumpulan, setiap kumpulan adalah terdiri daripada multi-disiplin dengan mengambil kira purata skor bagi setiap kumpulan

Masalah kedua ialah responden yang menilai bagi setiap projek mempunyai bidang kepakaran yang berbeza. Pembentangan yang dibuat semasa bengkel tersebut adalah terdiri daripada pelbagai bidang kepakaran. Oleh yang demikian, responden tidak dapat menilai dengan teliti dan tepat sekiranya projek tersebut bukan daripada bidang mereka. Ini telah menyebabkan jawapan yang diberikan oleh responden adalah tidak menyeluruh dan kurang tepat.

3.2 Faedah Kajian

Pemilihan dan penentuan keutamaan cadangan Projek R&D Pertahanan dengan menggunakan AHP dapat membantu pihak pengurusan STRIDE dalam pemilihan projek-projek R&D Pertahanan untuk RMK-10 berdasarkan nilai keutamaan tertinggi mengikut kriteria yang ditetapkan dan pemilihan keutamaan projek R&D berdasarkan kepada sumber kewangan dengan penggunaan *resource alligner* yang terdapat di dalam perisian *Expert Choice*. Keputusan yang diperolehi melalui teknik ini lebih efektif berbanding menggunakan teknik Analisis Delphi yang digunakan sebelum ini. Dengan adanya teknik ini, ia telah memberi keputusan yang tepat dan tidak berat sebelah.

4 KESIMPULAN

AHP merupakan satu perisian yang mudah dan amat berkesan dalam membuat keputusan mengikut keutamaan berdasarkan kepada faktor-faktor atau kriteria yang telah ditetapkan. Ia dapat meminimumkan risiko dalam membuat keputusan seperti kelemahan dalam

menentukan fokus dan perancangan yang strategik. Dengan ini, Projek R&D Pertahanan RMK-10 dapat ditentukan berdasarkan skor yang diperolehi daripada analisis yang telah dijalankan. Seterusnya, ini dapat membantu pihak pengurusan dari segi pengawalan pengurusan kewangan projek R&D Pertahanan yang bergantung kepada keupayaan sumber kewangan.

PENGHARGAAN

Penulis amat berterima kasih kepada Dr. Mohmad Asri Abd. Ghani, En. Hasan Rahman, En. Wong Siew Kwan, Pn. Halijah Ahmad, Pn. Norkamizah Mohd Noor, En. Mohd Faizal Halid, En. Mohd Nur Aminullah Abu Hashim, Cik Nur Syazwana Razali, En. Loo Soon Tong, Pn. Shurihan Ahmad, Pn. Jamaliah Mohd Noor dan Pn. Farizah Abd Fatah yang turut membantu dalam menjayakan kajian ini.

RUJUKAN

Ayag, Z & Ozdemir, R.G. (2006). A Fuzzy AHP Approach to Evaluating Machine Tool Alternatives. *J. Intell. Manuf.*, **17**: 179-190.

Decision Lens (2009). Analytic Hierarchy Process. Dari laman web: http://www.decisionlens.com/products/meth_hierarchy.htm (Tarikh akses terakhir: 20 November 2009).

Omkarprasad, S. V. & Kumar, S. (2006). Analytical hierarchy process: An overview of applications. *Euro. J. Oper. Resear.*, **169**: 1-29.

Partovi, F.Y. (1994). Determining what to benchmark: An Analytic Hierarchy Process approach. *Int. J. Oper. Prod. Man.*, **14**: 25-39.

Saaty, T.L. (1980). The Analytic Hierarchy Process. Mc Graw Hill, New York.

Stair, R.M. & Render, B. (1992). Introduction to Management Science. Boston, Massachusetts.

Hair, J.F., Babin, B., Money, A.M. & Samouel, P. (2003). Essentials of Business Research Methods. Leyh Publishing, Austin, Texas.

CATCH OF THE NET

While the ongoing influenza A(H1N1) global pandemic outbreak, fortunately, does not appear to be catastrophically lethal, it serves as a real-life reminder of the potentially catastrophic effects of bioterrorism. A bioterrorist attack releases viruses, bacteria, or other germs to cause illness or death. These biological agents are typically found in nature, but can sometimes be made more harmful by increasing their ability to cause or spread diseases, or to resist medical treatment. These biological agents can spread through air, water, food, or from person to person. Unlike conventional weapons of mass destruction (e.g. bombs, missiles etc.), biological weapons can be very hard to detect, and they do not cause illness for several hours or days. Public health officials worry that deadly biological agents, such as anthrax, botulism, hemorrhagic fever viruses (e.g. Ebola), plague or smallpox, could be used for such bioterrorist attacks. Biodefence refers to medical measures to protect people from bioterrorist attacks, including medicines and vaccinations, and medical research and preparations. The following are relatively interesting and useful websites on bioterrorism and biodefence:

1) **Centers of Disease Control and Prevention: Bioterrorism**
   http://www.bt.cdc.gov/bioterrorism

2) **Biological Weapons Gateway**
   http://www.cbwinfo.com/Biological/BWList.shtml

   Websites providing comprehensive reviews of various potential bioterrorism agents.

3) **World Health Organization: Biorisk Reduction**
   http://www.who.int/csr/bioriskreduction

   Provides descriptions of activities, reports, news and events of various WHO programs and projects in biorisk reduction.

4) **U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID)**
   http://www.usamriid.army.mil

   Website of USAMRIID, which is the U.S. Army's main institution and facility for basic and applied research on biological threats in support of military biodefence requirements.

5) **Institute for Medical Research (IMR): Infectious Diseases Research Centre (IDRC)**
   http://www.imr.gov.my/org/idrc.htm

   IDRC was formed to strengthen research in all aspects of infectious diseases, including those caused by bioterrorist attacks, in collaboration with other relevant Malaysian and foreign bodies.

6) **Federation of American Scientists: Biosecurity and Biodefence Resources**
   http://www.fas.org/programs/ssp/bio/resource/index.html

7) **U.S. Food and Drug Administration: Counterterrorism**
   http://www.fda.gov/oc/opacom/hottopics/bioterrorism.html

8) **Medscape Bioterrorism Resource Center**
   http://www.medscape.com/resource/bioterr

9) **Medline Plus: Biodefense and Bioterrorism**
   http://www.nlm.nih.gov/medlineplus/biodefenseandbioterrorism.html

   Resource centres providing the latest news, reference material and literature selections on bioterrorism and biodefence.

Prepared by Dinesh Sathyamoorthy & Ahmad Razi Mohamed Yunus