DEFENCE S&T TECHNICAL BULLETIN

Vol. 6 | Num. 1 | Year 2013 | ISSN 1985-6571

CONTENTS

Development of a Prototype Unmanned Surface Vessel (USV) Platform — 1-9
Nur Afande Ali Hussain, Dinesh Sathyamoorthy, Norazlina Md Nasuddin, Norzaidi Mat Nawi, Muhammad Nasuha Mansor, Nor Emi Salwani Sulaiman, Rosdi Yaacob, Rozi Ramli, Mohd Ridzuan Mohd Rashid, Idayu Ramli, Ayu Sahida Ismail, Elizabeth Louisnaden & Nor Alyani Ibrahim

Development of Camouflage Patterns for Coastal Patrol Boats — 10-20
Muhamad Muslim Tasdik, Dinesh Sathyamoorthy, Mohd Jalis Md Jelas, Siti Nasuha Mohd Rafien, Hafizi Che Mat, Punitha Ramakrishnan, Hafizah Mohd Yusof, Borhanuddin Mohd Youssof & Maslehah Abd Majid

Development of a Georeferencing Software for Radiological Diffusion in Order to Improve the Safety and Security of First Responders — 21-32
Romeo Gallo , Paolo De Angelis , Andrea Malizia, Fabiana Conetta, Daniele Di Giovanni, Luca Antonelli, Nicola Gallo, Andrea Fiduccia, Fabrizio D'Amico, Roberto Fiorito, Maria Richetta, Carlo Bellecci & Pasquale Gaudi

Evaluation of Biohazard Management of the Italian National Fire Brigade — 33-41
Orlando Cenciarelli, Andrea Malizia, Marianna Marinelli, Stefano Pietropaoli, Romeo Gallo, Fabrizio D'Amico, Carlo Bellecci, Roberto Fiorito, Antonio Gucciardino & Pasquale Gaudio

Global Navigation Satellite System (GNSS) Spoofing: A Review of Growing Risks and Mitigation Steps — 42-61
Dinesh Sathyamoorthy

Evaluation of the Effect of Multipath on Global Positioning System (GPS) Performance via GPS Simulation — 62-74
Dinesh Sathyamoorthy, Shalini Shafii, Zainal Fitry M Amin & Siti Zainun Ali

STRIDE™ SCIENCE & TECHNOLOGY RESEARCH INSTITUTE DEFENCE

EDITORIAL BOARD

Chief Editor
Dr Zalini bt Yunus

Deputy Chief Editors
Dr Mahdi bin Che Isa
Dinesh Sathyamoorthy

Associate Editors
Halijah bt Ahmad
Masliza bt Mustafar

Secretariat
Norkamizah bt Mohd Nor
Siti Zainun bt Ali

ISSN 1985-6571

Copyright of the Science & Technology Research Institute for Defence (STRIDE), 2013

AIMS AND SCOPE

The Defence S&T Technical Bulletin 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 bulletin should be based on original research in areas related to defence science & technology. All contributions should be in English.

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 two complimentary copies of the issue in which their work appears.

PRESENTATION OF MANUSCRIPTS

The format of the manuscript is as follows:

a) Page size B5 (JIS)
b) MS Word format
c) Single space
d) Justified
e) In Times New Roman ,11-point font
f) Should not exceed 20 pages, including references
g) Texts in charts and tables should be in 10-point font.

Please e-mail the manuscript to:

1) Dr. Zalini bt Yunus (zalini.yunus@stride.gov.my)
2) Dr. Mahdi bin Che Isa (mahdi.cheisa@stride.gov.my)
3) Dinesh Sathyamoorthy (dinesh.sathyamoorthy@stride.gov.my)

The next edition of the bulletin is expected to be published in November 2013. The due date for submissions is 11 September 2013. **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 manuscript is as follows:

TITLE OF MANUSCRIPT

Name(s) of author(s)

Affiliation(s)

E-mail:

ABSTRACT

Contents of abstract.

Keywords: *Keyword 1; keyword 2; keyword 3; keyword 4; keyword 5.*

1. TOPIC 1

Paragraph 1.

Paragraph 2.

1.1 Sub Topic 1

Paragraph 1.

Paragraph 2.

2. TOPIC 2

Paragraph 1.

Paragraph 2.

Figure 1: Title of figure.

Table 1: Title of table.

Content	**Content**	**Content**
Content	Content	Content
Content	Content	Content
Content	Content	Content

Equation 1 (1)
Equation 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. The following reference style is to be adhered to:

<u>Books</u>

Serra, J. (1982). *Image Analysis and Mathematical Morphology*. Academic Press, London.

<u>Book Chapters</u>

Goodchild, M.F. & Quattrochi, D.A. (1997). Scale, multiscaling, remote sensing and GIS. *In* Quattrochi, D.A. and Goodchild, M.F. (Eds.), *Scale in Remote Sensing and GIS*. Lewis Publishers, Boca Raton, Florida, pp. 1-11.

<u>Journals / Serials</u>

Jang, B.K. & Chin, R.T. (1990). Analysis of thinning algorithms using mathematical morphology. *IEEE T. Pattern Anal.*, **12**: 541-550.

<u>Online Sources</u>

GTOPO30 (1996). *GTOPO30: Global 30 Arc Second Elevation Data Set*. Available online at: http://edcwww.cr.usgs.gov/landdaac/gtopo30/gtopo30.html (Last access date: 1 June 2009)

<u>Unpublished Materials (e.g. theses, reports and documents)</u>

Wood, J. (1996). *The Geomorphological Characterization of Digital Elevation Models*. PhD Thesis, Department of Geography, University of Leicester, Leicester.

DEVELOPMENT OF A PROTOTYPE UNMANNED SURFACE VESSEL (USV) PLATFORM

Nur Afande Ali Hussain[1], Dinesh Sathyamoorthy[2], Norazlina Md Nasuddin[1], Norzaidi Mat Nawi[3], Muhammad Nasuha Mansor[4], Nor Emi Salwani Sulaiman[1], Rosdi Yaacob[1], Rozi Ramli[1], Mohd Ridzuan Mohd Rashid[1], Idayu Ramli[1], Ayu Sahida Ismail[1], Elizabeth Louisnaden[1] & Nor Alyani Ibrahim[1]*

[1]Maritime Technology Division (BTM), Science & Technology Research Institute for Defence (STRIDE), Ministry of Defence, Malaysia
[2]Instrumentation & Electronics Technology Division (BTIE), Science & Technology Research Institute for Defence (STRIDE), Ministry of Defence, Malaysia
[3]USM Robotics Research Group, School of Electrical & Electronic Engineering, Universiti Sains Malaysia (USM), Malaysia.
[4]Malaysian Institute of Marine Engineering Technology (MIMET), Universiti Kuala Lumpur (UniKL), Malaysia.

[*]Email: afande.hussain@stride.gov.my

ABSTRACT

This paper presents the development of a prototype unmanned surface vessel (USV) platform for water quality measurement. Based on several hull concept designs made using Solidworks, the catamaran design was determined as the most suitable for the platform due to its stability and manoeuvrability performance. The platform's design was optimised using computational fluid dynamics (CFD) analysis to study its resistance and dynamic flow. Hydrostatic simulation was done using Maxsurf to determine the geometry of the platform's hull. Several displacements for selected drafts were obtained, which was used to estimate the maximum total load on board the platform. Glass reinforced plastic (GRP) composite material was selected for the hull's fabrication due to its strength and light weight. Five layers of GRP were applied on the mould to get a strong structure. The development the overall system design of the platform consisted of electrical, mechanical, control and communications systems, and sensors according to the specific draft and displacement. The buoyancy test conducted for the completed prototype showed that its performance is consistent with the results of the hydrostatic simulation.

Keyword: *Unmanned surface vessel (USV); catamaran; hydrodynamic and hydrostatic simulations; glass reinforced plastic (GRP); buoyancy test.*

1. INTRODUCTION

Unmanned surface vessel (USV) (also known as unmanned surface craft (USC)) is one of the solutions for marine, river and lake applications, such as marine environment monitoring, hydrologic survey, target tracking and scientific survey, depending on sensor requirements (DON, 2007; Manley, 2008; Bertram, 2008; Jianhua *et al.,* 2009; Dinesh, 2010). Hardware systems in USV platforms are easily reconfigurable and the safety of the craft does not require the code freeze that is often necessary for work on underwater vehicles (Curcio *et al.,* 2008). Due to the uniqueness of the platform, it can be customised for law enforcement agencies, emergency services and military applications to reduce or eliminate the need to endanger human lives in many situations (Reed *et al.,* 2006; Manley, 2008; Bertram, 2008; Dinesh, 2010). USVs can also be useful as an underwater navigation aid to provide unmanned underwater vehicles (UUVs) with accurate navigation data that is required for successful missions (Leonessa *et al.,* 2003). Using portable side scan sonar, USVs can be used for underwater mapping and acoustic measurement. (Beck *et al.,* 2008). In addition, USVs can also be used for harbour protection systems as they can provide mobile and flexible surveillance. USVs can be equipped with state of the art sensors for underwater and air surveillance, such as surface wave radar, infrared camera and swimmer detection system (DON, 2007; Bertram, 2008; Manley, 2008; Dinesh, 2010).

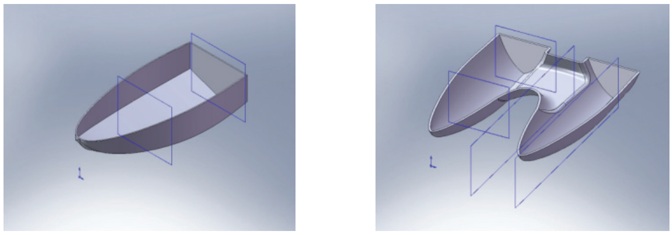
This study is aimed at developing a prototype USV platform for water quality measurement. Such measurements are presently conducted using Royal Malaysian Navy (RMN) vessels, which involves a lot of man power and is only suitable for deep-water applications. The proposed platform will be used for littoral and fresh water applications, as well as areas that are difficult for naval vessels to access.

The prototype will use low cost acoustic transducers integrated with a Global Positioning System (GPS) receiver for localisation. It will be equipped with a digital compass for heading data and a Horiba water quality system. This paper will present the development of the prototype at STRIDE’s Maritime Technology Division (BTM), which includes the concept design using Solidworks, hydrodynamic and hydrostatic simulations using FLUENT and Maxsurf respectively, system design (consisting of fabrication, and electrical, mechanical and communication systems), and buoyancy test.

2. CONCEPT DESIGN AND SIMULATIONS

2.1 Concept Design

Several concept designs were developed using the Solidworks 2009 design software, including mono-hull and catamaran (twin-hull) (Figure 1). It was determined that the catamaran design was the most suitable to meet the requirements for placement of several sensors, electronic systems and batteries, due to its stability with respect to roll and wave, and its shape which reduces resistance at high speeds (Caccia *et al*., 2005; Manley, 2008; Jianhua *et al.,* 2009). Its wider design, as compared to the mono-hull, provides good hotel load and better manoeuvrability.



(a) (b)

Figure 1: USV concept design: (a) Mono-hull. (b) Catamaran.

For the mono-hull concept design, only one propeller unit is needed for propulsion, while catamaran uses one propeller for each hull. The heading control for the mono-hull platform uses an extra actuator for rudder control, which is actuated by a servo motor system, while the catamaran platform does not need any additional actuator controls because the steering is based on differential propeller revolution rates. Figure 2 shows the final design concept of the USV catamaran platform.

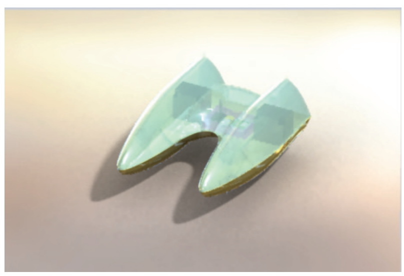


Figure 2: The final concept design of the catamaran platform.

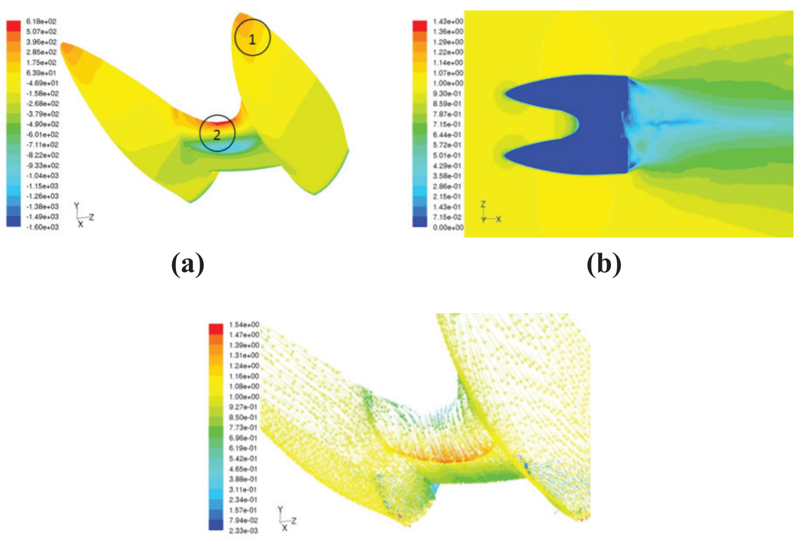
The overall dimensions of the platform are 1.1 x 0.87 x 0.44 m. The total volume of the platform reflected the total of amount displacement of water, which is equal to the buoyancy force or total weight of the water displaced. Based on this principle, the total weight of the total payload, such as the power system, sensors, electronic circuits, navigation system and other related scientific equipment, can be computed. The assembly drawing was converted to *.igs* and *.step* formats for hydrostatic and hydrodynamic analyses.

2.2 Hydrodynamic Simulation

Estimation of hydrodynamic forces is important to investigate the motion and performance of the platform. The numerical approach was used to obtain hydrodynamic parameters, such as velocity and pressure, in order to understand the pressure distribution that acts on the platform, whereby higher pressure provides higher resistance to the platform and vice-versa. Computational fluid dynamics (CFD) analysis is a suitable tool to understand the physical effect of fluid flow on hulls, which is difficult to be measured using other measuring techniques (Muljowidodo *et al.,* 2010a). This simulation was conducted using FLUENT, a CFD software that includes the FLUENT solver and Gambit pre-processor. Gambit was used to create the volume and mesh generation, while the solver was used for simulation setup, solving process and post-processing (Thomas *et al.*, 2008).

Figure 3(a) shows the pressure coefficient distribution on the platform with flow rate of 1 ms^{-1}. The pressure coefficient is not constant but varies as a function of speed, flow direction, object position, object size, and fluid density and viscosity. The flow direction towards the front of the platform (points 1 and 2) gives a greater drag as compared to other parts of the platform as it faces the maximum pressure, which is caused by the maximum velocity drop. The velocity contour in Figure 3(b) indicates a velocity drop at high pressure surfaces, which leads to turbulence after the vehicle passes. Figure 3(c) shows the flow behaviour in the surrounding region of the platform, with the different colour arrows indicating the magnitude and direction of velocity.

The hull design concept is analysed using FLUENT to investigate the critical areas with higher pressure points that will result in velocity drop. Based on the results obtained, these critical areas were adjusted with dynamic design to reduce the total resistance. While the platform will operate at low speeds due to the low sampling rate of the acoustic eco-sounder, lower resistance or drag of the platform will result in better manoeuvring performance and increased efficiency of the thrusters.



(a) **(b)**

(c)

Figure 3: Hydrodynamic simulation of the platform: (a) 3D view of pressure coefficients, (b) velocity contour. (c) velocity magnitude of the flow in the surrounding region of the platform.

2.3 Hydrostatic Simulation

The displacement of the platform at a given draft was obtained by dividing the submerged volume by the appropriate density factor (35 ft^3/tonne for salt water or 36 ft^3/tonne for fresh water). This computation was used to determine the appropriate total payload for platform for the selected drafts (Table 1). This data was used with Maxsurf 15.0 to determine the geometric properties of the hull form, particularly the underwater part (Figure 4). The simulation was conducted in fixed trim condition with fresh water density of 1,000 kg/m^3.

Table 1: Computed displacements for the platform at selected drafts.

Draft (m)	0.050	0.075	0.100	0.150	0.175	0.225
Displacement (kg)	1.807	5.328	11.10	25.12	34.79	55.07

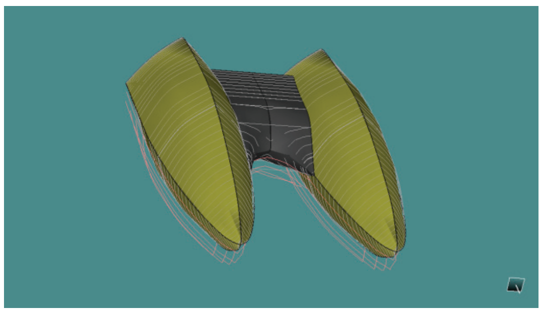
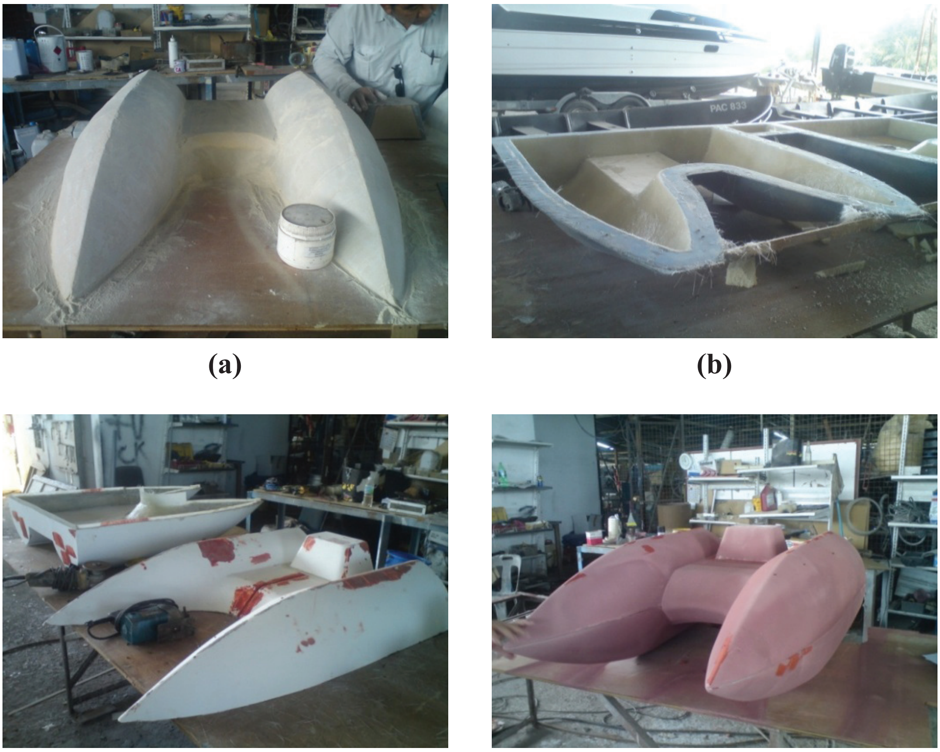


Figure 4: Hydrostatic simulation using Maxsurf.

3. SYSTEM DESIGN

3.1 Fabrication

The platform hull was fabricated using glass reinforced plastic (GRP) composite material due its strength and light weight (Muljowidodo *et al.,* 2010b) (Figure 5). The hull shaping process was conducted manually according to the design until the desired mould was obtained. Epoxy was applied on the mould, and then, GRP matting was applied on top of it. Another layer of epoxy was applied to ensure that the material conformed to the mould and that no air was be trapped between the GRP and the mould. The process was repeated with another layer of epoxy and GRP matting with different directions for five layers for durability and strength, especially to sustain the 8 kg of lead acid battery at each side of the hull. The work had to be done quickly before the epoxy started to cure.



(a) (b) (c) (d)

Figure 5: The platform's fabrication using GRP: (a) The hull shaping process. (b) The moulding process. (c) Five layer of GRP applied on the mould. (d) The completed upper and bottom casing.

3.2 Hardware and Sensor Allocation

The platform is controlled using a ground controller station, located at the shore, using an embedded programmable interface controller (PIC) with low energy consumption (maximum of 7.5 W). Communications between the platform and ground station is bidirectional using a Black Box RF modem. Since all the sensors on the platform use the National Marine Electronic Association (NMEA) protocol, a data rate of 4,800 bits/s was configured on the RF Modem.

The propulsion system consists of two Technadyne 400 W underwater thrusters, providing 10.4 and 5.9 kg forward and reverse thrusts respectively. These two thrusters are the control base for differential propeller revolution to propel the platform for forward, backward and turning movements. The control signals emanate from the keyboard or PS2 controller of a laptop via the RF Modem, together with the GPS, gyrocompass and acoustic eco-sounder data in ASCII format. All the sensors' data will be processed by the NMEA multiplexer unit before being sent by the RF Modem. A PIC controller circuit was developed for the thrusters' control and data acquisition. The platform was also equipped with a wireless camera system for on-board monitoring and localisation purposes. Two units of 12 V, 24 AH lead acid batteries were integrated with DC-DC power converter to provide power for the main propulsion system, sensors and other related equipment. As shown in Figure 6, the power converter provides 24 V for the thruster system, and 12 V supply for GPS, gyrocompass, eco-sounder, electronic circuits, camera and NMEA multiplexer. Figure 7 shows the internal mounting for the batteries, power converter circuit and PIC control system.

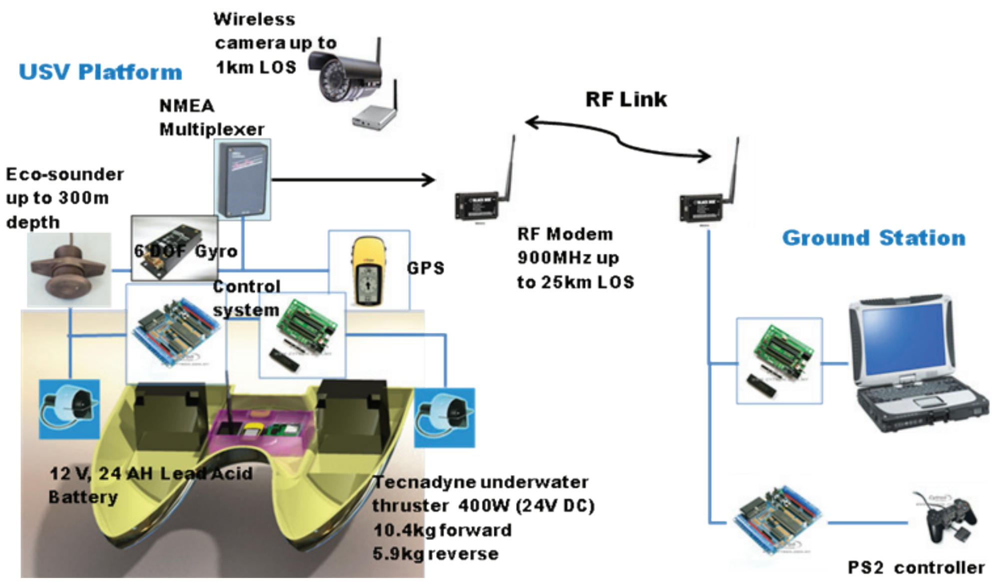


Figure 6: The platform's system design.

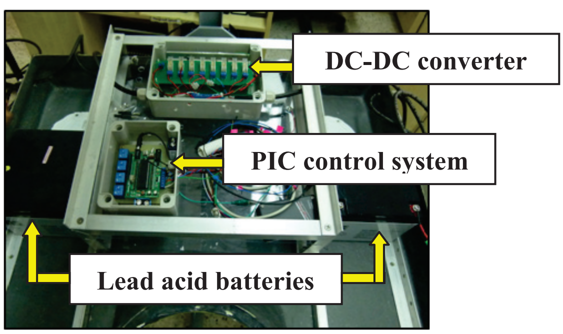


Figure 7: The internal mounting for the batteries, power converter circuit and PIC control system.

4. BUOYANCY TEST

The total payload fitted on board the prototype is at present 20 kg. Based on the hydrostatic simulation, the draft and displacement of the prototype can be predicted. The underwater thrusters should be totally submerged below the waterline level to ensure it operates properly. The prototype was designed for draft ranging from 10 to 18 cm in order to get a variation of total payload that is allowed to be fitted on the platform. The displacement is equal to overall weight of the prototype and payload on board the prototype.

Figure 8 shows the buoyancy test of the prototype using a variation of total payload for comparison with the hydrostatic simulation results. The maximum payload that can be achieved is 34.5 kg for 17 cm of draft in fresh water, indicating that the hydrostatic simulation results are consistent with prototype's performance. There would be a slightly different displacement if the prototype operates in salt water due to the density factor. The density of sea water is 1,025 kg/m^3, while for fresh water, it is 1000 kg/m^3. This would result in different displacements; for example a draft of 17.5 cm would result in 34.79 kg of displacement in fresh water, and 35.66 kg in sea water. As salt water has higher density, extra payload can be added when the prototype operates in the sea water as compared to in fresh water, with the same draft.

Figure 8: Buoyancy test conducted to determine the prototypes's displacements at various drafts.

5. CONCLUSION

In this paper, the concept design, hydrodynamic and hydrostatic simulations, system design, and buoyancy test of the prototype USV platform were described. For future expansions, the total payload of the prototype can reorganised based on the displacements at various drafts, while additional functions can be included by fitting applicable sensors and transducers. Future applications such as side scan sonar capability, laser scanning system and better wireless communication protocols for broadband data transmission will be explored.

ACKNOWLEDGMENT

The authors would like to thank the Science & Technology Research Institute for Defence (STRIDE) for funding allocation under the Tenth Malaysian Plan (RMK10).

REFERENCES

Beck, E., Kirkwood, W., Caress, D., Berk, T., Mahacek, P., Brashem, K., Acain, J., Reddy, V., Kitts, C., Skutnik, J. & Wheat, G. (2008). SeaWASP: A small waterplane area twin hull autonomous platform for shallow water mapping. *Autonomous Underwater Vehicles, 2008, IEEE/OES.* 13-14 October 2008, pp. 1-7.

Bertram, V. (2008). *Unmanned Surface Vehicles: A Survey*. Skibsteknisk Selskab, Copenhagen.

Caccia, M., Bono, R., Bruzzone, Ga., Bruzzone, Gi., Spirandelli, E., Veruggio, G. & Stortini, A., M. (2005). Design and exploitation of an autonomous surface vessel for the study of sea-air interactions. *Proceedings of the IEEE International Conference on Robotics and Automation, 2005. ICRA 2005.*18-22 April 2005, pp. 3582-3587.

Curcio, J., Schneider, T., Benjamin, M. & Patrikalakis, A. (2008). Autonomous surface craft provide flexibility to remote adaptive oceanographic sampling and modeling. *Oceans 2008.* 15-18 September 2008, pp. 1-7.

Department of Navy (2007). *The Navy Unmanned Surface Vehicle (USV) Master Plan*. US Department of Navy, Washington D.C.

Dinesh, S. (2010). Key defence R&D fields to develop the national defence industry: Focus on C4ISR in support of network centric operations and unmanned vehicles. *Defence S&T Tech. Bull.*, **3**: 43-60.

Jianhua, W., Wei, G. & Jianxin, Z. (2009). Design of an Autonomous Surface Vehicle Used for Marine Environment Monitoring. *Advanced Computer Control, 2009. ICACC '09,* 22-24 January 2009, pp. 405-409.

Leonessa, A., Mandello, J., Morel, Y. & Vidal, M. (2003). Design of a small, multi-purpose, autonomous surface vessel. *Oceans 2003.* 22-26 Sept. 2003, pp. 544-550.

Manley, J.E. (2008). Unmanned surface vehicles: 15 years of development. *OCEANS 2008*, 15-18 September 2008, Quebec City.

Muhamad, H., Zahurin, S. & Rizal, M. A. (2009) CFD Simulation of Cooperative AUV Motion, *Indian J. Mar. Sci.*, **38**: 346- 351.

Muljowidodo, K., Sapto, A. N. & Nico, P. (2010a). Design and Analysis of "PARI" Air Deployable AUV. *3rd International Conference on Underwater System Technology: Theory and Application 2010 (USYS'10)*, 1- 2 November 2010, Cyberjaya, Malaysia.

Muljowidodo, K., Sapto, A. N. & Nico, P. (2010b). Design, Analysis, and Testing Composites Hull of "SHRIMP" ROV. *3rd International Conference on Underwater System Technology: Theory and Application 2010 (USYS'10)*, 1- 2 November 2010, Cyberjaya, Malaysia.

Reed, C. M., Bishop, B. E. & Waters, J. K. (2006). Hardware Selection and Modeling for a Small Autonomous Surface Vessel. *Proceeding of the Thirty-Eighth Southeastern Symposium on System Theory, 2006. SSST '06.* 5-7 March 2006, pp. 380-384.

Thomas, G., Christian L., Claudio C., Timo L., Christian M., Remigius N., Wolfgang S., Roland Z. & Peter K. (2008). Computational fluid dynamics (CFD) software tools for microfluidic applications – A case study, *Comput. Fluids.*, **37**: 218-235.

DEVELOPMENT OF CAMOUFLAGE PATTERNS FOR COASTAL PATROL BOATS

*Muhamad Muslim Tasdik**, *Dinesh Sathyamoorthy, Mohd Jalis Md Jelas, Siti Nasuha Mohd Rafien, Hafizi Che Mat, Punitha Ramakrishnan, Hafizah Mohd Yusof, Borhanuddin Mohd Youssof & Maslehah Abd Majid*

Instrumentation & Electronics Technology Division (BTIE), Science & Technology Research Institute for Defence (STRIDE), Ministry of Defence, Malaysia

**E-mail: muslim.tasdik@stride.gov.my*

ABSTRACT

While a number of camouflage patterns have been designed, none of them are suitable for the Malaysian coastal environment. Hence, this research objective is aimed at designing a camouflage pattern for Royal Malaysian Navy (RMN) coastal patrol boats. Representative coastal environment training grounds in Lumut (Perak), Pulau Indah (Selangor) and Port Dickson (Negeri Sembilan) were selected. The captured images of the study areas were converted to digital and artistic patterns. The patterns were then clustered to five index colours, with the colours redefined using the collected field colour measurements and in-service camouflage reference colours of infrared reflectance (IRR) paint. The selection of the regions of interest for the pattern templates were picked based on the variation of colour composition. After comparison of a few generated patterns based on colour composition, the most suitable camouflage pattern template was selected.

Keywords: *Camouflage pattern; coastal patrol boat; Lab colourspace; digital and artistic patterns; k-means clustering.*

1. INTRODUCTION

The primary role of Royal Malaysian Navy (RMN) coastal patrol boats is to uphold the security of the national maritime zone. Their presence should not be easily identified to ensure the success of their operations. Hence, the boats should have an effective camouflage pattern which closely resembles the background of coastal environments in order to reduce the probability of detection. These days, there are many camouflage patterns available on the shelf, from classic woodland patterns to computerised digital patterns for a wide variety of applications (Mitchell & Staples, 1999; Cuthill *et al.*, 2005; Grigoryan *et al.*, 2009; Bartczak *et al.*, 2009; Hambling, 2012; Abdul Ghaffar *et al.*, 2012). However, they do not match the Malaysian coastal environment.

The classic woodland pattern has long been established due to its concealment characteristics and suitability for forest environments (Mitchell & Staples, 1999; Cuthill *et al.*, 2005; Hambling, 2012). The improvement of the woodland pattern to the recent trend of digital (pixelated) camouflage pattern is due to the dithering effect, which does not show solid lines between the colours. The digital pattern is able to degrade edges of shapes to disrupt the form of target objects, and would require more time for detection and recognition in specific environments (Cuthill *et al.*, 2005; Billock *et al.*, 2008; Venezia & Peloquin, 2011; Abdul Ghaffar *et al.*, 2012). In addition, the determination of the pattern size to be created is also a vital criterion. This is due to the visual ability of human eyes significantly being subjected to the spatial resolution of the objects related to its distance. Therefore, the pattern designed usually includes micro- and macro-elements for its effectiveness in close and particular distances. For instance, small elements cannot be seen from a distance (Friskovec *et al.*, 2010; Jia *et al.*, 2010; Cho *et al.*, 2011; Venezia & Peloquin, 2011; Abdul Ghaffar *et al.*, 2012).

By considering these requirements, this research was conducted to design a camouflage pattern for coastal patrol boats which is suitable for the Malaysian coastal environment. At this stage of the study, the pattern was assessed only in the visual spectrum, and did not include the near infrared and thermal spectral regions. As a typical patrol boat is situated at some distance from the observer and from the beach, the camouflage pattern size is determined by the macro-elements that explicitly exhibit bunches of leaves instead of a single leaf. The scope of work of the study is as shown in Figure 1.

2. METHODOLOGY

2.1 Data Acquisition

The selected coastal areas were in Lumut (Perak), Pulau Indah (Klang, Selangor) and Tanjung Tuan (Port Dickson, Negeri Sembilan). In addition, a vegetation area in the STRIDE laboratory compount was used for comparison between coastal and land areas. Digital images of the selected coastal areas were captured using a Canon EOS1000D digital single-lens reflex (DSLR) camera with standard lens (50 mm) from a distance which was affixed with a representative scale such as field markers and colour reference to compensate for different sunlight illuminations at different areas and time. The distance was measured using a Vector 21 laser range finder. The field colours were measured using a Minolta colour meter at 10^o illumination, while gloss was measured using a Micro-TRI gloss meter at 60^o illumination. One of the data acquisition activities conducted by the research team is shown in Figure 2.

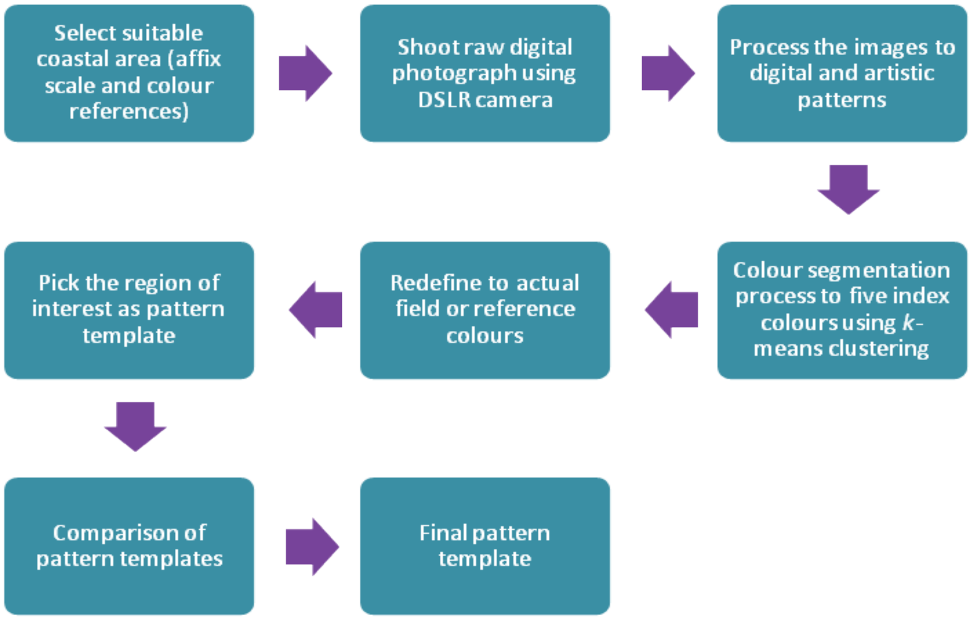


Figure 1: Summary of the processes involved in designing the camouflage pattern for coastal patrol boats.

Figure 2: The research team conducted field data acquisition at Pulau Indah on 21-22 February 2012.

2.2 Image Processing

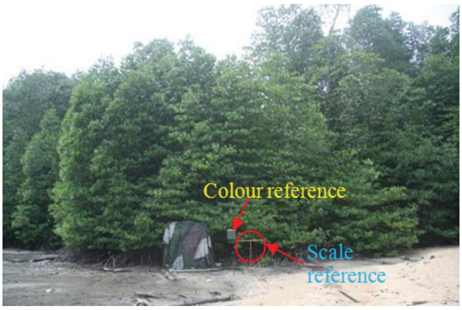
Postprocessing of the captured images was kept at a minimum. Apart from in-camera correction for distortion and white balance, the images were further corrected for white balance based on the colour reference. The images were first converted from the native RGB (red, green, blue) colourspace to the Lab (luminance, red-green, blue-yellow) colourspace. This was done because dyes used in camouflage pattern printing are defined in Lab colourspace (Abdul Ghaffar *et al.*, 2012). The images were then converted to digital and artistic patterns.

The generated patterns, which were in a wide range of colours, were extracted to five index colours using *k*-means clustering (MacQueen, 1967; Wagstaff *et al.*, 2001; Kanungo *et al.*, 2002), which is a method that is commonly used to partition a data set into *k* groups (in the case of this study, five). It selects *k* initial cluster centres and iteratively refines them so that each element (in the case of this study, the colours of the generated patterns) is assigned to its closest cluster centre and each cluster centre is updated to the mean of its constituent elements. The algorithm converges when there is no further change in assignment of the elements to the clusters.

The colours of the resulting clusters were then redefined using the collected field colour measurements and the in-service camouflage reference colours of infrared reflectance (IRR) paint. Finally, after comparison of a few generated patterns based on colour composition, the most suitable pattern template was selected.

3. RESULTS AND DISCUSSION

Hundreds of images of the selected coastal areas, including mangrove vegetation, man-made objects, houses and vessels, were acquired. However, for this manuscript, only the images of mangrove vegetation are shown. The corresponding images at Port Dickson, Pulau Indah and STRIDE are shown in Figures 3-5 respectively. After the digitalisation and artistic conversion processes, the images were then segmented into five index colours using *k*-means clustering. The completed consequent patterns are shown in Figures 6-9.



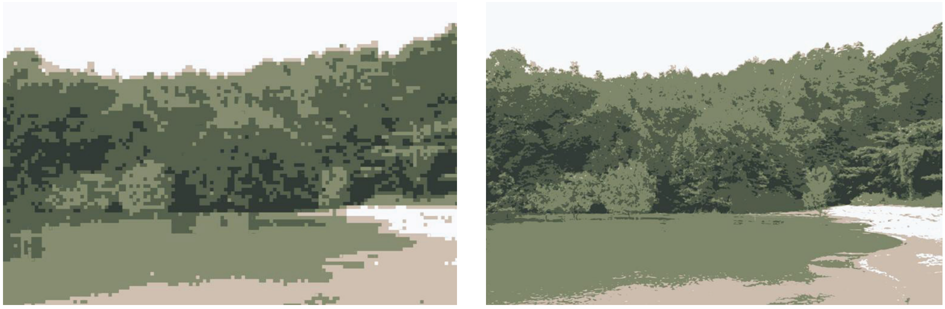
(a) **(b)**

Figure 3: Images of same coastal area at Port Dickson taken from different distances: (a) From 10 m, with 1.2 m rods and colour reference. (b) From 130 m.

(a) **(b)**

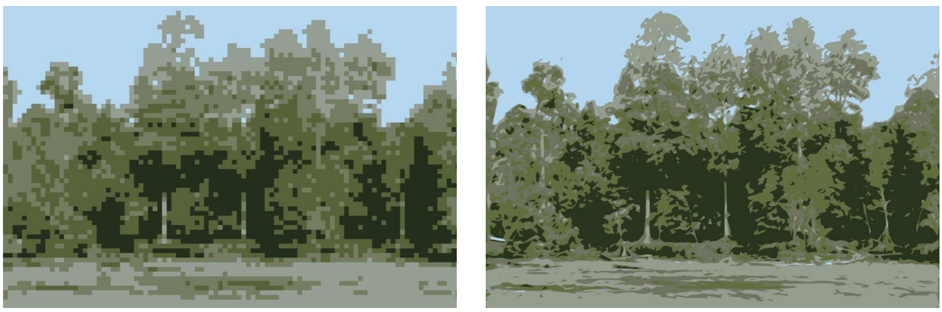
Figure 4: Images of different coastal areas at Pulau Indah taken from different distances: (a) From 10 m. (b) From 130 m.

Figure 5: Image of vegetation at the STRIDE laboratory compound taken from distance of 30m.



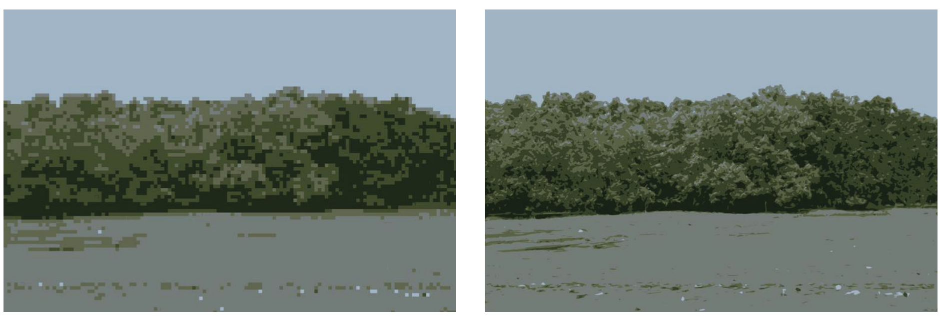
(a) (b)

Figure 6: Images of the coastal area at Port Dickson (Figure 3(b)) after k-means clustering: (a) Digital pattern. (b) Artistic pattern.



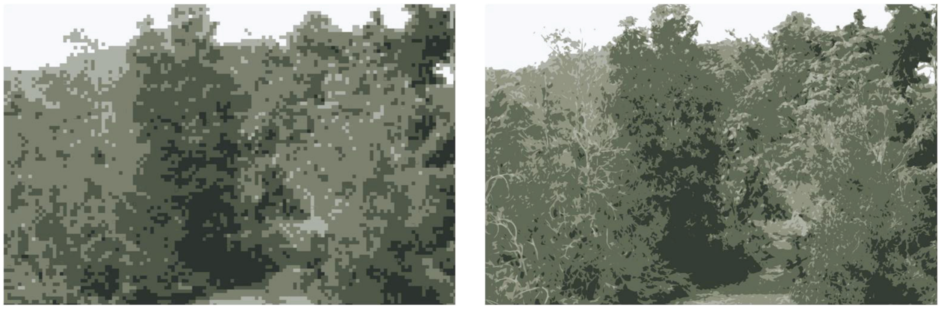
(a) (b)

Figure 7: Images of the coastal are at Pulau Indah taken from 10 m (Figure 4(a)) after k-means clustering: (a) Digital pattern. (b) Artistic pattern.



(a) (b)

Figure 8: Images of the coastal area at Pulau Indah taken from 130 m (Figure 4(b)) after k-means clustering: (a) Digital pattern. (b) Artistic pattern.



(a) (b)

Figure 9: Images of vegetation at the STRIDE laboratory compound (Figure 5) after k-means clustering: (a) Digital pattern. (b) Artistic pattern.

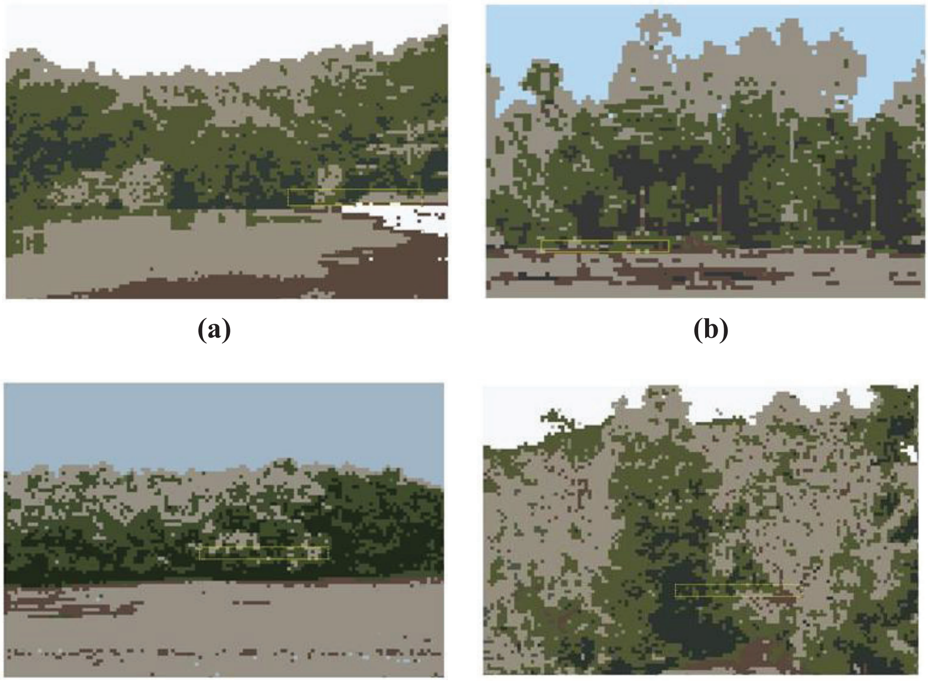
The colours of the patterns were redefined using the in-service camouflage reference colours of IRR paint (Siew, 2009) for black, brown and sand, and the collected field colour measurement for green (i.e., the average colour of mangrove leaves) (Figures 10 and 11). The chromaticity values of the patterns in Lab colour space at 10° observation for the corresponding colours are given in Table 1.

Table 1: Chromaticity values for the colours of the camouflage patterns.

Colour	Lightness *L*	Chromaticity Value		Acceptable colour difference Δ*E*	Gloss
		a	***b***		
Black	23.7	-0.29	0.67	Less than / equal to 2.0	Less than 5
Brown	31.8	6.82	7.83		
Green	36.43	-9.01	20.19		
Sand	59.6	0.31	8.05		

Subsequently, the size of the pattern template was determined by comparing the actual size of the boat (11.5 x 0.9 m) and the image. From Figure 3(a), the actual size of the rod scale is 1.2 m, which is equivalent to 120 pixels in the image. Hence, the size of the pattern template which is equivalent to the size of the boat is 1,130 x 90 pixels.

The selection of the regions of interest for the pattern templates were picked based on the variation of colour composition. The generated pattern templates are shown in Figures 12 and 13. The most appropriate pattern templates could then be selected from comparison of colour composition of the generated patterns as shown in Figures 14 and 15. Based on this comparison, it was determined that the most suitable templates are Figure 14(b) for the digital pattern and Figure 15(c) for the artistic pattern.

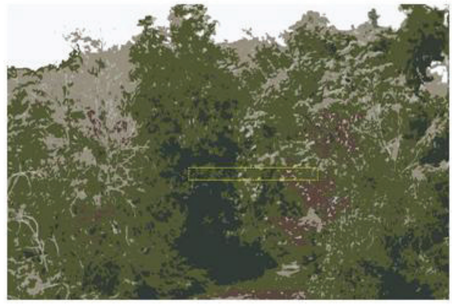


(a) **(b)**

(c) **(d)**

Figure 10: Images of the digital patterns after redefining the colours. The yellow outlined rectangles indicate regions of large colour variations, which were the regions of interest for pattern template selection. (a) The coastal area at Port Dickson. (b, c) The coastal area at Pulau Indah taken from 10 and 130 m respectively. (d) Vegetation at the STRIDE laboratory compound.

(a) **(b)**



(c) **(d)**

Figure 11: Images of the artistic patterns after redefining the colours. The yellow outlined rectangles indicate regions of large colour variations, which were the regions of interest for pattern template selection. (a) The coastal area at Port Dickson. (b, c) The coastal area at Pulau Indah taken from 10 and 130 m respectively. (d) Vegetation at the STRIDE laboratory compound.

(a) **(b)**

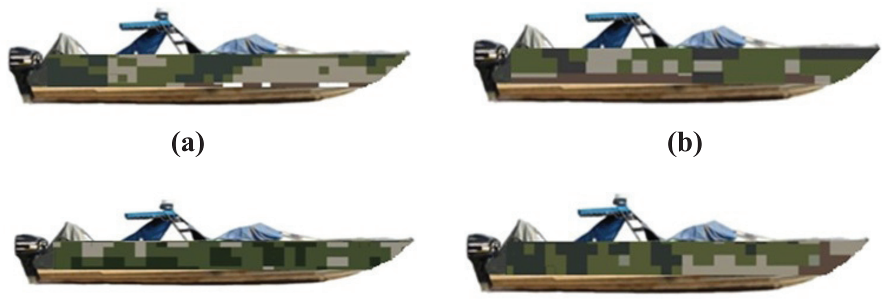
(c) **(d)**

Figure 12: The selected pattern templates for the corresponding digital patterns in Figure 10.

(a) **(b)**

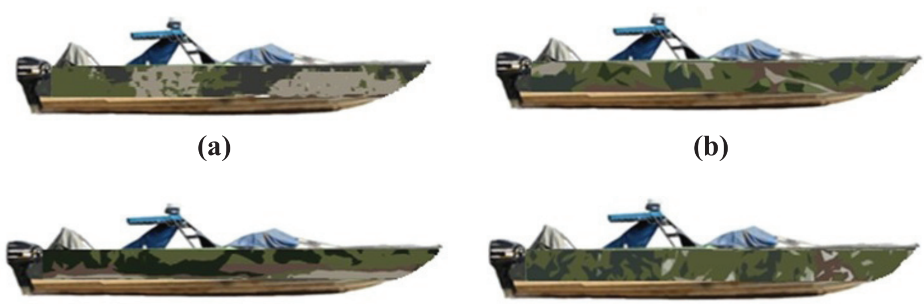
(c) **(d)**

Figure 13: The selected pattern templates for the corresponding artistic patterns in Figure 11.



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

Figure 14: The generated camouflage patterns for the coastal boat using the corresponding digital pattern templates in Figure 12.



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

Figure 15: The generated camouflage patterns for the coastal boat using the corresponding artistic pattern templates in Figure 13.

4. CONCLUSION

This paper has presented a method for generating camouflage patterns for coastal environments. For effective implementation of the proposed method, colour accurate images need to be produced, followed by the appropriate image analysis and segmentation routine to generate the pattern templates. The prototype camouflage patterns proposed in this study will undergo field evaluations using RMN coastal boats. In addition, the proposed method will be adapted to generate camouflage pattern templates for other environments.

ACKNOWLEDGMENT

This manuscript is an extended version of the article entitled *Developing 'Natural' Camouflage Pattern for Coastal Patrol Boats* that was published in BUDI, vol. 2012, no. 2, pp. 13-21 (Mohd Jalis *et al.*, 2012). The authors would like to gratefully acknowledge the Director-General of the National Hydography Centre, First Admiral Dato' Pahlawan Zaaim Hasan and his team for providing a boat and assistance during the data acquisition session at Pulau Indah, Klang.

REFERENCES

Abdul Ghaffar, R., Mohmad Asri, A.G. & Dinesh, S. (2012). Quantitative evaluation of camouflage patterns on textile materials using fractal analysis. *J. Defence Secur.*, **3**: 87-99.

Bartczak, A., Fortuniak, K., Maklewska, Obersztyn, E., Olejnik, M. & Redlich, G. (2009). Camouflage as the additional form of protection during special operations. *Techniczne Wyroby Wlokiennicae*, **2**: 15-22.

Billock, V.A., Cunningham, D.W. & Tsou, B.H. (2008). What visual discrimination of fractal textures can tell us about discrimination of camouflaged targets. *Human Factors Issues in Combat Identification Workshop*, 13 May 2008, Gold Canyon, Arizona.

Cho, W.J., Ahn, W., Kim, M.S., Park, J., Kim, S. & Han, K.H. (2011). Making pixel patterns automatically for camouflage: Using color information from their background. *Commun. Comput. Inform. Sci.*, **174**: 98-101.

Cuthill, I.C., Stevens, M., Sheppard, J., Maddocks, T., Parraga, C.A. & Troscianko, T.S. (2005). Disruptive coloration and background pattern matching. *Nature*, **434**: 72-74.

Friskovec, M., Gabrijelcic, H. & Simoncic, B. (2010). Design and evaluation of a camouflage pattern for Slovenian urban environment. *J. Imaging Sci. Tech.*, **54:** 020507.

Grigoryan, V.A., Antipov, A.P., Potapov, A.V. & Egorov, A.I. (2009). Improvement of soldier survivability by signature management. *Techniczne Wyroby Wlokiennicae*, **2**: 25-29.

Hambling, D. (2012). Cloak of Invisibility. *Def. Tech. Int.*, March 2012.

Jia, Q., Lv, X. & Rong, X. (2011). Application of Markov random field model in the design of digital pattern painting. *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC)*, 8-10 August 2011, Deng Feng, China.

Kanungo, T., Mount, D.M., Netanyahu,N.S., Piatko, C.D., Silverman, R. and Wu, A.Y. (2002). An efficient k-Means clustering algorithm: Analysis and implementation. *IEEE Pattern Anal. Mach. Intell.*, **24**: 881-892.

MacQueen, J. B. (1967). Some methods for classification and analysis of multivariate observations. *Proceedings of the Fifth Symposium on Math, Statistics and Probability,* University of California Press, Berkeley, California, pp. 281-297.

Mitchell, K.D. & Staples, C.R. (1999). Methods for deriving optimum colours for camouflage patterns. *RTO SCI Workshop on Search and Target Acquisition,* 21-23 June 1999, Utrecht, The Netherlands.

Siew, C., 2009. *A Presentation of KT1000F: Thermal Camouflage Paint*. Metro Koats Technology Sdn. Bhd., Puchong, Selangor.

Venezia, J. & Peloquin, A. (2011). Using a constructive simulation to select a camouflage pattern for use in OEF. *2011 Military Modelling & Simulation Symposium (MMS 2011)*, 3-7 April 2011, Boston, Massachusetts.

Wagstaff, K., Cardie, C., Rogers, S. and Schroedl, S. (2001). Constrained k-means clustering with background knowledge. *Proceedings of the Eighteenth International Conference on Machine Learning*, 28 June - 1 July 2001, Williams College, Williamstown, Massachusetts.

Defence S&T Tech. Bull.,6(1) :21-32,2013

DEVELOPMENT OF A GEOREFERENCING SOFTWARE FOR RADIOLOGICAL DIFFUSION IN ORDER TO IMPROVE THE SAFETY AND SECURITY OF FIRST RESPONDERS

Romeo Gallo[1] , Paolo De Angelis[2] , Andrea Malizia[3], Fabiana Conetta[3], Daniele Di Giovanni[3,4], Luca Antonelli[3], Nicola Gallo[5], Andrea Fiduccia[6], Fabrizio D'Amico[3], Roberto Fiorito[7], Maria Richetta[3], Carlo Bellecci[3] & Pasquale Gaudio[3]*

[1]Comando Provinciale dei Vigili del Fuoco di Matera, Italy
[2]Direzione dei Servizi di Sicurezza e Protezione Civile, Corpo dei Vigili del Fuoco, Italy
[3]Department of Industrial Engineering, Faculty of Engineering, University of Rome "Tor Vergata", Italy
[4]CRATI scrl , C/O Università degli Studi della Calabria, Italy
[5]Nicola.Gallo.Name, Italy
[6]Intergraph Italia LLC, via Sante Bargellini 4, 00157 Roma Italy.
[7]Department of Surgery, Faculty of Medicine and Surgery, University of Rome "Tor Vergata", Italy

**E-mail: malizia@ing.uniroma2.it*

ABSTRACT

This study deals with the need to develop analytical instruments to optimise rescue operations involving radiological exposure. It reports several aspects of analysis and characterisation of orphan radioactive sources. The protection problems in cases of detection and securing of radioactive sources are analysed, with particular attention to safety and security of operators and population from exposure, identification of attention areas, and detection of specific values of dose. After defining the characteristics of orphan radioactive sources, the authors examine the fundamental radiometric parameters. All these parameters have been integrated in a customised software, known as GREAT (Georeferenced Radiological Evaluation & Analysis Tool), that allows for rapid mapping of radiological risks by georeferencing of the data collected. Particular attention has been dedicated to the theoretical model and support tools aided to the choices of first responders. Radiological event, their consequences and the tools developed will be described by the authors in order to demonstrate the importance of this software for improvement of rescue operations.

Keyword: *Orphan radioactive source; radiological diffusion; first responders; georeferencing software; radiation dose.*

1. INTRODUCTION

Radioactive sources are used throughout the world for many applications, particularly in heavy industries, medicine and research. The risks associated with such uses are strictly connected to their physical characteristics; activity, types of radionuclides, methods of manufacture, etc. (IAEA-TECDOC, 2004). In the case of conventional applications, the risks associated are usually well known and their activities are officially established. In the European Union (EU), the provisions for the protection of population and workers against the risks of ionising radiation are given by European Atomic Energy Community (EURATOM) directives (EURATOM, 1984, 1989, 1990, 2006), while in Italy, the main guidelines are included in MOI (2009, 2011), which is an extension of MOI (1995).

However, problems related to orphan radioactive sources (the ones that are not under control) are different as they can be accidentally found by persons that do not know their effective harm. They may also present particular risks that do not allow for easy identification, due to their small dimensions, often smaller than of a pen. To protect against such events, melting plants have to equip themselves with radiometric instrumentations for control of metal scrap in the input, so as to reduce the risk of accidental introduction of radioactive sources in the processing cycle (Knoll, 2010).

As part of the community plan of action in the field of radioactive waste (EURATOM, 1992), the European Commission published a study on the management and disposal of disused sealed radioactive sources in the EU (Angus *et al.*, 2000). The authors evaluated 500,000 units of sealed radioactive sources that were distributed to operators in the EU states since 1950. Of this amount, 110,000 units are still in use, while the remaining units have been stocked in temporary storage, returned to the manufacturers for the purpose of reuse, or sent to disposal plants and subjected to the system of management of radioactive waste. The national authorities face unsafe situations when sources are not managed properly or are left without any control, with the possibility of dangerous health consequences. Angus *et al.* indicated that around seventy sources get out of the authorities' control every year.

The study deals with the problems mentioned above and the authors present a software that was developed for rapid mapping of radiological diffusion and associated risks in cases of accidental and deliberate releases. The main research objectives are to define a conceptual model for a spatial decision support system (SDSS), oriented to the problem of radiation hazard, for identifying the requirements of both mobile and control rooms; to develop the prototype of the software for first responders, that allows web access in order to georeference source localisation and dose rate measurements at a safe distance from the source and to develop the prototype of the control room components according to the service oriented architecture (SOA) paradigm, which allows usability through Open Geospatial Consortium's (OGC) web services within the Intergraph's incident command tool, known as the Intergraph Incident & Resource Management System (I^2RMS).

2. RADIOLOGICAL CHARACTERISTICS TO MEASURE RADIOLOGICAL RISKS

The main radiological characteristics, particularly those useful for this study, are commonly divided into (Cazzoli *et al.*, 2003):

1. Source:
   - Activities
   - Constant range
2. Field values:
   - Exposure
   - Kerma, is a size of dose, but its measurement in air is also used as the field value
3. Values of the dose:
   - Absorbed
   - Equivalent
   - Effective.

There is a direct relationship between these variables:

Source ➔ *Field* ➔ *Dose*

2.1 In-Field Operations with Unknown Radiological Sources

In cases of operations with the presence of orphan sources, the operators often work with unknown sources. The external exposure of an operator may be limited by observing the following rules:

- Reducing the irradiation time
- Increasing the distance
- Using a screen / shield to reduce the intensity of radiation

2.1.1 Reducing the Irradiation Time

The value of the dose increases linearly with the intensity of radiation I_{dose} and time t (Figure 1). The operation must therefore be planned carefully in order to minimise, as far as possible, the intervention times. In any case, the dose values established by law should not be exceeded. The dose values are defined from three quantities; absorbed dose D, equivalent dose H and effective dose E. Absorbed dose is the amount of energy that is deposited in any material by ionising radiation. Equivalent and effective doses relate the amount of radiation received by a person with resulting biological damage and hence, are called radio-protection quantities. In order to plan for an operation with sealed sources (in absence of contamination risk) the most important value is the effective dose because the effective dose in radiation protection and radiology is a measure of the cancer risk to a whole organism due to ionizing radiation delivered non-uniformly to part(s) of its body. It takes into account both the type of radiation and the nature of each organ being irradiated. (Gallo *et al.*, 2012).

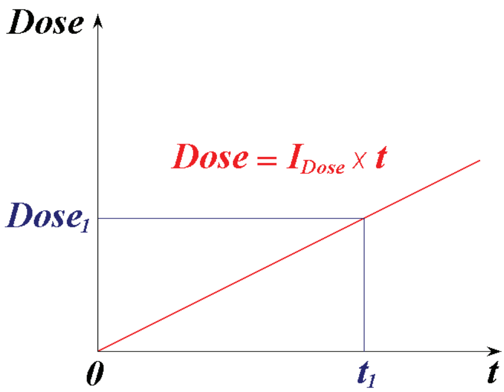


Figure 1: A plot showing the trend of increase of effective dose I_{dose} with time *t*.

2.1.2 Increasing the Distance

Taking into account a generic distance *d* from the source, the value of the field, in terms of intensity of exposure, is inversely proportional to the square of the distance (Figure 2) and directly proportional to the activity, and is expressed using the following equation:

$$I_X = \frac{\Gamma \cdot A}{d^2} \quad (1)$$

where:

- I_x = Exposure intensity [C/(kg*h)]
- Γ = Gamma specific constant, which is a characteristic of each radionuclide [(C*m^2) / (kg*h*Bq)]
- A = Source activity [Bq]
- d = Distance from source [m].

It is evident how it is important to organise rescue operations keeping the greatest possible distance from the source (IAEA TECDOC-1162, 2000). Starting with the knowledge of the radiation field, in the case of exposure to whole body with the radiation (our case study), it is possible to calculate the values of the doses that should be assumed.

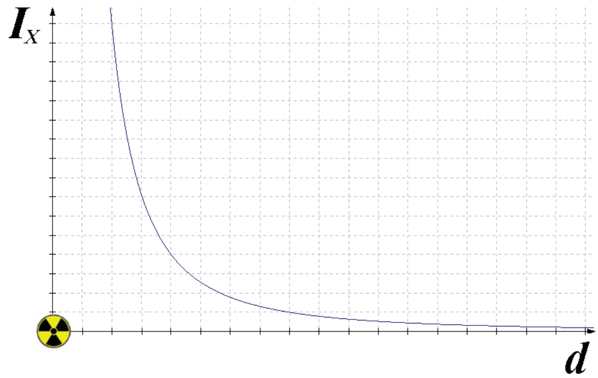


Figure 2: A plot showing the trend of decrease of radiation dose vs time.

2.1.3 Using a Screen / Shield to Reduce the Intensity of Radiation

The radiations, propagating in space, interact with matter in their passage causing ionisation that can be direct (for the alpha and beta radiation) or indirect (for the gamma radiation and neutron) (UNI, 2001). The interaction between radiation and matter and the different penetration capabilities are a function of (IRCP, 1996):

1. Type of radiation
2. Its energy
3. Characteristics of the exposed matter.

Alpha radiations rapidly convert their kinetic energy into material ionisation, with a modest path. The free electrons, in turn, cause a secondary ionisation. Following a possible excitation of atoms, an emission of electromagnetic radiation of low energy (non-ionising) is also possible. Alpha radiation is arrested by less than 10 cm of air or by a simple sheet of paper. In cases of irradiation of people, such radiation stops on the very first layer of the skin, and only in cases of high energy (about 7 MeV) can it reach the germinative layer of the skin, at a depth of 70 μm. This type of radiation is therefore not dangerous in cases of external irradiation. However, the scenario changes in case of internal contamination of the human body (with internal irradiation), where the damage would lead directly to organs and tissues (ICRP, 2007; Knoll, 2010).

Beta radiations and electrons have modest capability of penetration of matter, but higher than those of alpha particles. These radiations can move in the air for about 4 m or 4 mm in water (for energies with order of magnitude of 1 MeV). The germinative layer of the skin can be reached by particles with energies of above 70 keV. Personal protective equipment (PPE) used by firefighters provides good shielding for these types of radiation. In the air, dozens of ionisations per cm are produced. As a result of excitation of the atoms of the exposed material by beta radiation, there is the reemission of energy in the form of electromagnetic waves. The strong deceleration of the beta particles can cause a second order emission of X-ray-called

"Bremsstrahlung". The emission has intensity that increases proportionally with the atomic number of the irradiated material. The phenomenon constitutes a risk greater than the one of the beta radiation from which it derives, being X-rays more difficult to shield. It is useful not use materials with a high atomic number to shield beta radiation. A good shielding of the beta radiation is also given by the first layer of material with low density, which reduces the production of X-rays (ICRP, 2007; Knoll, 2010).

Gamma radiations can absorbed by huge lengths of matter. In terms of interaction mechanism between matter and radiation, at low energies, the photoelectric effect prevails, at medium energies the Compton effect prevails, while at large energies the pairs creation prevails. For the charged particles, the beam of radiation is slowed down in an almost uniform mode and is stopped almost simultaneously, while for photons, the beam is reduced as it progresses within the material, and the photons that continue on their path maintain the same initial energy. For such radiation, it is important to refer to the so called half-value layer (HVL), or half-value thickness, through which the initial intensity of the incident radiation is halved. These thicknesses are a function of the type of exposed material and the energy of the radiation. X and gamma radiations are effectively attenuated by materials with a high atomic number, such as lead (ICRP, 2007; Knoll, 2010; Gallo *et al.*, 2012).

2.2 Intervention Procedures in Cases of Sealed Radioactive Sources

During an operation with the presence of sealed radioactive sources, there is an immediate need to delimit an area which must be kept away the population. This area should have dimensions of not less than those of the so-called "area of concern", so as to ensure that the area outside it does not exceed the legal effective dose limit of 1 mSv. The limits of the attention area can be determined analytically using the data of the source (if known) or following in-field measures of intensity and dose. It is necessary to determine the area of danger for the population. This is possible by making measurements of field intensity or dose, depending on the instruments available. With knowledge that the value of the intensity of dose and relative distance uniquely identifies the intensity-distance curve (Figure 2), the intervention can be planned. Multiple measurements are necessary to reduce the errors. Assuming that the operator is working with a tool that provides the intensity value of the effective dose, at a distance d_1 the operator measures an intensity value of effective dose I_{E1}. The value of I_{E1} compared to the values (unknown) A and Γ is:

$$I_{E_1} = \frac{\Gamma \cdot A}{{d_1}^2} \tag{2}$$

Taking into account a generic distance d_2, the value of intensity I_{E2} can be expressed as:

$$I_{E_2} = \frac{\Gamma \cdot A}{{d_2}^2} \tag{3}$$

For Equations 2 and 3, obtaining the values of *A* and *Γ*, the following equation can be derived:

$$I_{E_1} x d_1^2 = I_{E_2} x d_2^2 \quad (4)$$

from which calculate the value of I_{E2} can be computed as follows:

$$I_{E_2} = I_{E_1} x \frac{d_1^2}{d_2^2} \quad (5)$$

Using Equation 5 (setting the intensity values of effective dose for the operation), it is possible to calculate the relative distances and in particular the width of the attention area (Malizia *et al.*, 2012).

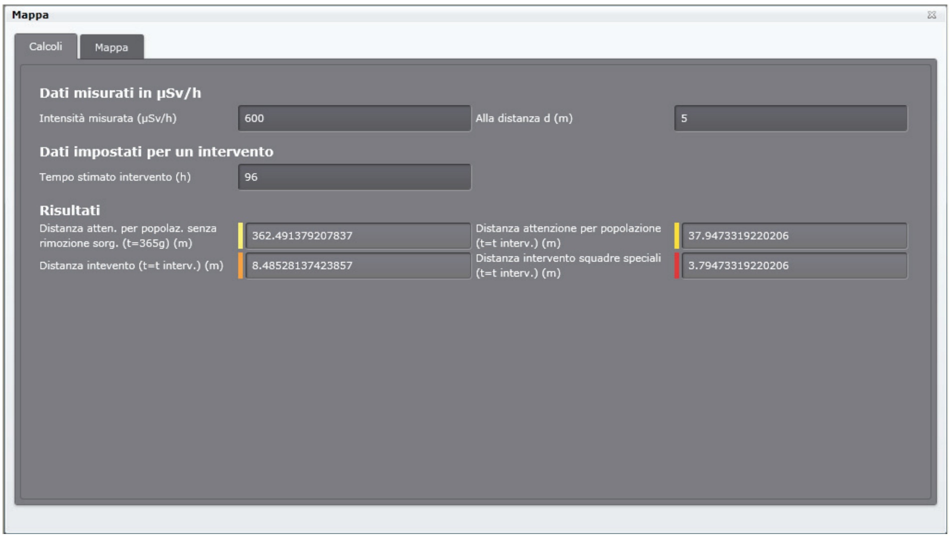
3. ACCELERATING SMARTER DECISIONS: GEOSPATIAL TECNOLOGIES FOR SAFETY IMPROVEMENTS DURING RESCUE OPERATIONS

From this analysis, it is clear that the primary task of first responders is to protect the population from the risks arising from exposure to ionising radiations and then to define promptly the attention area (while working in safe and secure conditions of course) (Malizia *et al.*, 2012; Gallo *et al.*, 2012). It is possible to identify, in an analytical way, the size of the attention area and to carry out calculations of the dose absorbed by those who remain in the irradiated area. One of the problems that need to be dealt with immediately is the possible evacuation of buildings or closure of roads in the attention area. The principal requirements here are essentially:

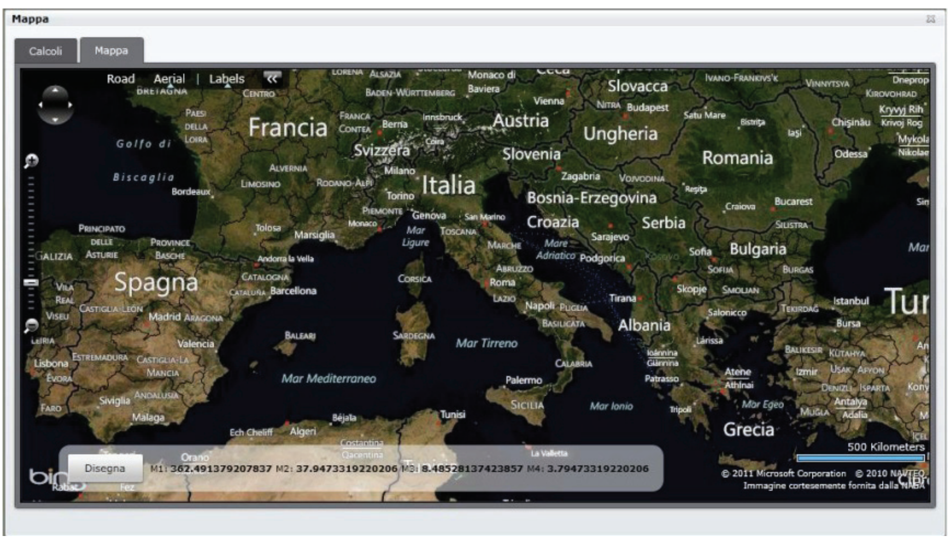
1. To locate the area affected by the radiation
2. To evaluate the possibility moving the source to a safe distance to avoid the evacuation of particular buildings, such as hospitals, or to allow the reopening of important communication routes.

In order to address these problems and improve rescue operations systems, a software that allows the geo-referencing of results of radiological calculations is needed. Hence, the authors have developed the software GREAT (Georeferenced Radiological Evaluation & Analysis Tool), interfaced with Intergraph's geospatial solutions, for an unknown radioactive source case, by applying the equations outlined above. In the first screen of the software (Figure 3(a)), called *Calcoli* (calculations), values of radiation intensity, measured in mSv/h, distance to which the measurement is taken and estimated time of operation is entered. By setting these boundary conditions, the software calculates the values of attention area, operating distance and in-field distance for special rescues teams, as well as the distance of attention for the population in case of non-removal of the source, conventionally identified for a residence time of 365 days.

The second screen of the software (Figure 3(b)) enables the user to display the attention areas on Microsoft Bing Maps (MBM). On the left of the screen, there is a zoom slider and darts to move the sight of the map, an operation which can also be performed using a mouse, in order to frame the area concerned. The display of the various areas of attention is possible by clicking on *Draw* (after assigning the source point on the map). The identification of the source point can be done manually by clicking with the mouse on the point identified or by entering the coordinates of latitude and longitude values.



(a)



(b)

Figure 3: The screens of the software: (a) The first screen, which is used to include boundary condition of operation parameters. (b) The second screen, which is used for mapping operations.

The developed software is a web application built with Silverlight, which is a Microsoft technology that allows for deploying rich internet applications (RIAs). The programming language used is C# (C sharp). Regarding the map, Silverlight Bing Map is used for the control of the components, providing input coordinates and drawing the map.

In Figure 4, the presence of a source is simulated at Policlinico Tor Vergata University as the focus area. The software immediately provides a map of the area to organise the evacuation. The critical areas are identified by the circles, of which the largest is the attention area for the population.

Figure 4: Simulation of a radiological risk at Policlinico Tor Vergata University.

The software has been interfaced with geospatial solutions from of Intergraph's Emergency Operation Centers. An emergency operations centre (EOC) enhances an area's ability to coordinate multi-agency responses to disasters and emergencies. It is equipped to perform a number of crisis management functions but is also able to function as a day-to-day operations resource, and supports efforts to test and exercise contingency and response plans (Cassani *et al.*, 2010). It is activated during emergencies that overwhelm the normal day-to-day functions of first responders. It typically performs the functions of information collection, processing, display and dissemination, management and coordination of interagency activities, implementation of relevant plans, and command and control of assigned resources.

The key to Intergraph's approach is standards and interoperability. Intergraph has enjoyed a long, successful partnership with OGC, since it was found in 1994, to create open and extensible software application programming interfaces for geographic information systems (GIS) and other mainstream technologies. Intergraph's I^2RMS (Figure 5) serves as the core of an EOC, and provides a full-SOA system to view and manage resources and activities associated with an event, as well as providing integrated situational awareness during planning, response, recovery and mitigation. Its open architecture and standards-based design provides the interoperability and information sharing vital for success during each phase of consequence management.

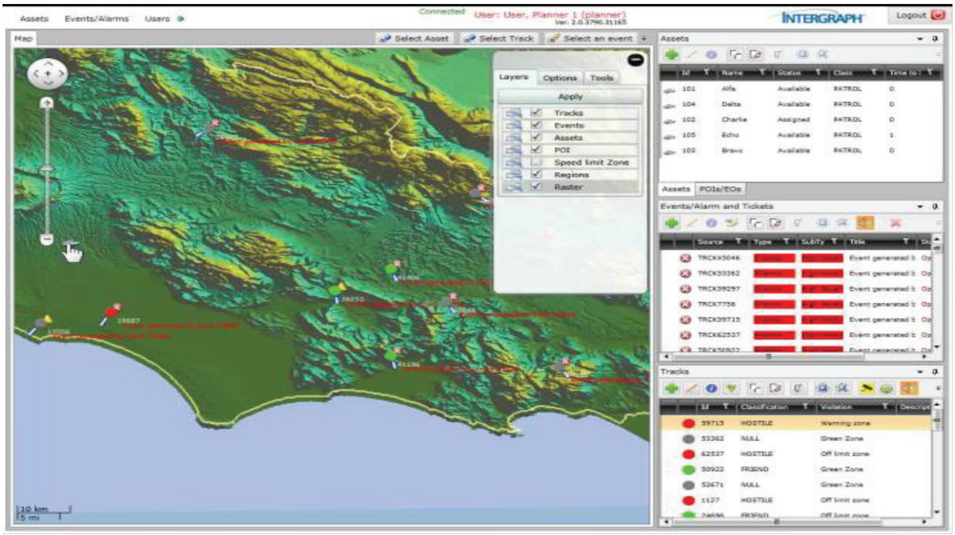


Figure 5: Intergraph I2RMS's 2D Common Operational Picture (COP) interface.

I^{2}RMS goes beyond simple resource monitoring to what is called presence management. The Common Operational Picture (COP) console of I^{2}RMS integrates several key components, including wireless communications, geospatial software, location tracking tools and the Internet, to help operators to plan, manage and track mobile assets and personnel. I^{2}RMS can track and manage multiple resources using the latest in radio frequency identification (RFID) technology, Global Positioning System (GPS), automatic vehicle location (AVL) systems, cell and sensor technologies (using radar and electro-optic sensors) and geospatial mapping applications (2D and 3D COP interfaces). This solution is service oriented architecture (SOA) based and offers a thin-client system to view and manage these resources. Intergraph's SmartClient is used to give EOC's personnel a rich data entry GIS client into a simple web browser using a Java-based technology. The solution is designed to be a client of OGC's web services, and to publish maps and reports on the Internet using Intergraph's geospatial Web servers, GeoMedia WebMap and ERDAS Apollo.

4. CONCLUSION

Orphan radioactive sources are a potential dangerous for the population. In cases of their occurrence, it is important to take the necessary radiation protection measures, such as evacuation and closure of adjacent areas to quickly identify the areas affected by the radiation hazard. The use of the developed georeferencing software makes it simpler to achieve good safety and security standards. It is clear how such a tool, providing an overview of the scenario and areas involved, can optimise the operations of first responders who are equipped with handheld computers with web access. The detection of a safe area in which to temporarily place the source is relatively simple and can be readily verified using the software.

The software can also be a useful aid for companies and institution that deal with transport of radioactive sources, with the possibility to check, for the intended path, the areas potentially affected as a result of an accident with the source of exposure. In addition, it can also be potentiated with a mask for cases of known sources, as well as with the inclusion of other fields for the evaluation of additional elements such as values of doses taken by those who are in the radiological hot spot.

REFERENCES

Angus, M.J., Crumpton, C., McHugh, G., Moreton, A.D. & Roberts, P.T. (2000), *Management and Disposal of Disused Sealed Radioactive Sources in the European Union*. Safeguard International Ltd., Abingdon, Oxfordshire.

Cassani, I., Fiduccia, A., Malizia, A., Mugavero, R. & Quarta, A.M. (2010). Emergency operation center e protezione da eventi CBRN: Un Web-SDSS per le analisi di supporto alla gestione di incidente ad un reattore nucleare. *Atti 14a Conferenza Nazionale ASITA*, 9-12 November 2012, Fiera di Brescia.

Cazzoli,S., Biazzi, L., Campagni, A., Cianchi, A., Malgieri, F., Marinaro, M., Sinigallia, R. & Sumini M. (2003). *Individuazione e confinamento in sicurezza di sorgenti radioattive orfane*. Notiziario dell'Esperto Qualificato, N. 64 -65 / Gennaio – agosto 2003. Anno XXIII N. 1-2

European Atomic Energy Community (EURATOM) (1984). *Council Directive 84 / 466: Basic Safety Standards for the Health Protection of the General Public and Workers Against the Dangers of Ionozing Radiation*. European Atomic Energy Community (EURATOM), Brussels.

European Atomic Energy Community (EURATOM) (1989). *Council Directive 89 / 618: Health Protection Measures to be Applied and Steps to be Taken in the Event of a Radiological Emergency*. European Atomic Energy Community (EURATOM), Brussels.

European Atomic Energy Community (EURATOM) (1990). *Council Directive 90 / 641: Operational Protection of Outside Workers Exposed to the Risk of Ionizing Radiation During Their Activities in Controlled Areas*. European Atomic Energy Community (EURATOM), Brussels.

European Atomic Energy Community (EURATOM) (1992). *Council Resolution OJ C 158: Renewal of the Community Plan of Action in the Field of Radioactive Waste*. European Atomic Energy Community (EURATOM), Brussels.

European Atomic Energy Community (EURATOM) (2006). Council Directive 2006 / 117: *Supervision and Control of Shipments of Radioactive Waste and Spent Fuel*. European Atomic Energy Community (EURATOM), Brussels.

Gallo, R., De Angelis, P., Gallo, N., Malizia, A., Fiduccia, A., D'Amico, F., Fiorito, R., Gucciardino, A., Richetta, M., Bellecci, C., & Gaudio, P. (2012). Development of software for the identification mapping of radiological diffusion in order to improve the rescue operations. *MIMOS Conference*, 10 October 2012, , Rome.

International Atomic Energy Agency (IAEA) (2000). *IAEA-TECDOC-1162: Generic*

Procedures for Assessment and Response During Radiological Emergency. International Atomic Energy Agency (IAEA), Vienna.

International Atomic Energy Agency (IAEA) (2004). *IAEA-TECDOC-1388: Strengthening Control Over Radioactive Sources in Authorized Use and Regaining Control Over Orphan Sources*. International Atomic Energy Agency (IAEA), Vienna.

International Commission on Radiological Protection (ICRP) (1996). *IRCP Publication 72 (1996): Age – Dependent Doses to Members of the Public from Intake of Radionuclides: Part 5 Compilation of Ingestion and Inhalation Dose Coefficients*. International Commission on Radiological Protection (IRCP), Ottawa, Ontario.

International Commission on Radiological (ICRP) (2007). *ICRP Publication 103 (2007): The 2007 Recommendations of the International Commission on Radiological Protection*. International Commission on Radiological Protection (IRCP), Ottawa, Ontario.

Knoll, G.F. (2010). *Radiation Detection and Measurements, 4th Ed.* John Wiley & Sons, New York.

Malizia, A., Lupelli, I., D'Amico, F., Sassolini, A., Fiduccia, A., Quarta, A.M., Fiorito, R., Gucciardino, A., Richetta, M., Bellecci, C. & Gaudio, P. (2012). Comparison of software for rescue operation planning during an accident in a nuclear power plant. *Defence S&T Tech. Bull.*, **5**: 36-45.

Ministry of Interior (MOI) (1995). *Legislative Decree No. 230 / 1995: Regulatory Control of Radioactive Waste Management*. Ministry of Interior (MOI), Italy.

Ministry of Interior (MOI) (2009). *Legislative Decree No. 23/ 2009: Actuation of Council Directive 2006/117 / EURATOM of 20 November 2006 on the Supervision and Control of Shipments of Radioactive Waste and Spent Fuel*. Ministry of Interior (MOI), Italy.

Ministry of Interior (MOI) (2011). *Legislative Decree No.100/11 : Modification of Legislative Decree No. 230 / 1995*. Ministry of Interior (MOI), Italy.

UNI (Ente Nazionale Italiano di Unificazione) (2001). *UNI 10897: Carichi Di Rottami Metallici - Rilevazione Di Radionuclidi Con Misure X E Gamma*. Ente Nazionale Italiano di Unificazione (UNI), Milan.

EVALUATION OF BIOHAZARD MANAGEMENT OF THE ITALIAN NATIONAL FIRE BRIGADE

Orlando Cenciarelli[1,3], Andrea Malizia[1], Marianna Marinelli[2], Stefano Pietropaoli[3], Romeo Gallo[5], Fabrizio D'Amico[1], Carlo Bellecci[1], Roberto Fiorito[4], Antonio Gucciardino[1], Maria Richetta[1] & Pasquale Gaudio[1]*

[1]Department of Industrial Engineering, Faculty of Engineering, University of Rome "Tor Vergata", Italy
[2]Novartis Vaccine and Diagnostics, Italy
[3]Department of Biology, Faculty of Science Mathematical, Physical and Environmental, University of Rome "Tor Vergata", Italy
[4]Department of Bio-Medical & Prevention Faculty of Medicine and Surgery, University of Rome "Tor Vergata, Italy
[5]Comando Provinciale dei Vigili del Fuoco di Matera, Italy

[*]Email: orlando.cenciarelli@uniroma2.it

ABSTRACT

Biohazards are non-conventional threats that are very difficult to manage. This is due to difficulties in the identification of biological agents that are responsible for the onset of a disease, which can be bacteria, viruses, fungus or toxins. In Italy, the first response system to biohazards is provided by the National Fire Brigade (NFB) (Corpo Nazionale dei Vigili del Fuoco - CNVVF). The aim of this work is to evaluate the procedures adopted by the NFB for the management of biohazards. This is done by comparing the statistics of NFB interventions in 2000-2010 for potential biohazard events, and chemical and radioactive risks. A series of solutions is then proposed to improve the NFB's national response system for biohazards.

Keywords: *National Fire Brigade (NFB); biohazards; chemical, biological, radiological and nuclear (CBRN); interventions; specialist biologists.*

1. INTRODUCTION

Biohazards is a very complex subject which is not easily explored. In fact, while for chemical and radiological-nuclear hazards we can often refer to well-known data, it is not the same for risks in the biological context (Kaszeta, 2012). The reason for this lack of information is clear; biohazards have still not been completely understood. For example, the molecular mechanisms of cancer development have only recently been associated with viruses directly transmitted (Butel, 2000). Moreover, commercialised systems and instruments do not currently exist to identify several biological agents, and the ones that exist do not allow instant infield identification. Hence, it is often necessary to use complex laboratory instrumentation for certain and rapid determination. The use of laboratory techniques require extended periods of time to get an answer. Additionally, the appropriate response is not always clear.

In Italy, the first response system to biohazard events is provided by the National Fire Brigade (NFB) (*Corpo Nazionale dei Vigili del Fuoco* - CNVVF). In the last decade, the NFB had to create a new division to operate in these "new risk scenarios" (we used the term "new" taking into account the classical background of infield operators). Following events involving biohazards, such as envelope and package contamination with anthrax spores (2001), and the potential spread of the avian influenza pandemic (2006)), circulars decrees were issued *ad hoc* by the Ministry of Interior (MOI) in order to provide operative directions for firefighters (MOI, 2001a; MOI, 2006). Immediately afterwards, the NFB was equipped with modern facilities for the detection and management of biological agents (e.g. mobile laboratories, decontamination units, etc.).

The aim of this work is to evaluate the procedures adopted by the NFB for the management of biohazard events. This is done by comparing the statistics of NFB interventions in 2000-2010 for potential biohazard events, and chemical and radioactive risks. A series of solutions is then proposed to improve the NFB's national response system for biohazard events.

2. THE NFB AND THE ITALIAN MANAGEMENT OF CBRN RISKS

2.1 NFB's Role in CBRN Events

The NFB, a key element of the Italian civil protection system, is part of the Department of Fire, Rescue Service and Civil Defense, which operates under the MOI. It consists of approximately 35,000 units. The NFB ensures urgent technical rescue, even in circumstances of unconventional risks. Its original primary objective is "*to protect the safety of persons and things, by preventing and extinguishing fires and providing technical services in general, including those related to air defence*" (MOI, 1941). The functions of the NFB was formally updated in MOI (2006), whereby the role of the NFB for chemical, biological, radiological and nuclear (CBRN) events is also defined, particularly in terms of counteracting the risks arising from CBRN substances, including from possible non-conventional crimes aimed at damaging people or property, using adequate instruments and mobile units. Therefore, in order to respond effectively to CBRN events, the NFB requires suitable technical skills, resources and specialised equipments.

2.2 NFB's Response Levels

NFB's model response for CBRN events is described in the NFB intervention model (MOI, 2001b). It is a mechanism of response that involves three different competency levels related to the complexity of the handling of the event. According to the intervention model, the local team (normally the closest one, the "basic team") must reach the location of the event first. This team will then evaluate the situation, and determine the requirements for adequate means and support of other teams more qualified for that type of intervention. The intervention teams based on the level of qualification are as follows:

a) Basic team: Locally qualified to ensure the first intervention;
b) Province specialists: Present in each provincial command;
c) CBRN regional operative unit: Present in each command in the regional capital towns.

Some of the regional commands are equipped with mobile analytical CBRN laboratories. It is specifically built for the CBRN unit of the NFB to carry out chemical, radioactive and biological sample analyses at the event site. Thus, they are able to obtain results in a shorter amount of time (Gulli *et al.*, 2008).

2.3 Scenarios and Type of Intervention

In the case of biohazard events, the NFB refers to MOI (2001b) to define the standard scenarios of intervention. Several possible scenarios of action are presented:

a) Presence of suspicious material without clear traces of powder or liquid;
b) Presence of suspicious material with clear traces of powder or liquid dispersed on surfaces but not spread within the environment;
c) Presence of suspicious material with clear traces of powder dispersed on surfaces and also spread within the environment.

Similarly, the types of events can be traced to the following three categories:

a) Release (or risk of release) without (or no risk of) fire or explosion;
b) Release (or risk of release) with (or risk of) fire or explosion;
c) Recovery of hazardous substance (or suspect) without (or remote) risk of loss.

3. BIOHAZARDS

Biohazards are linked to the exposure to biological agents and represent a potential danger for public health. Biohazards may arise from a variety of events involving biological agents, such as the natural diffusion; the accidental diffusion (e.g., spill from a biotechnology industry) or the intentional release into the environment (e.g., for terroristic attacks or war actions) (EC, 2012).

Biological agents are microorganisms, including those which have been genetically modified, cell cultures and human endoparasites, which can cause any infection, allergy or toxicity (EC, 2000; MOL, 2008; DOL, 2012). According to EC (2000), biological agents can be classified into four risk groups depending on their level of risk of infection:

a) Group 1: Agents that are unlikely to cause human disease.
b) Group 2: Agents that can cause human disease and might be a hazard to workers. They are unlikely to spread to the community, and there is usually effective prophylaxis or treatment available.
c) Group 3: Agents that can cause severe human disease and present a serious hazard to workers. They may present a risk of spreading to the community, but there is usually effective prophylaxis or treatment available.
d) Group 4: Agents that cause severe human disease and are a serious hazard to workers. They may present a high risk of spreading to the community, and there is usually no effective prophylaxis or treatment available.

CDC (2012) further classifies the most important biological agents into three categories:

a) Category A: Agents that can be easily disseminated or transmitted from person to person. They result in high mortality rates and have the potential for major public health impact. They might cause public panic and social disruption, and require special action for public health preparedness.
b) Category B: Agents that are moderately easy to disseminate. They result in moderate morbidity rates and low mortality, and require specific enhanced diagnostic capacity and disease surveillance.
c) Category C: Emerging agents that could be engineered for mass dissemination in the future because of their availability. They are easy to produce and disseminate. They are potentially linked to high morbidity and mortality rates, and major health impact.

Biological agents can be further classified according to certain characteristics that define the hazard to health (NATO, 1996):

a) Infectivity: The aptitude of an agent to penetrate and multiply in the host;
b) Pathogenicity: The ability of the agent to cause a disease after penetrating into the body;
c) Transmissibility: The ability of the agent to be transmitted from an infected individual to a healthy one;
d) Ability to neutralise: Means to have preventive tools and/or therapeutic purposes.

Each biological agent can be transmitted through one or more ways. The transmission modes are mainly (La Placa, 2010):

a) Parenteral: Agents that are transmitted through body fluids or blood;
b) Airway (by droplets): Agents that are emitted by infected people, which can then be inhaled by surrounding people;
c) Contact: Through which the agents present on the surface of the infected organism can infect another organism;

d) Oral-fecal route: Through objects, foods or other items contaminated with the feces of infected patients, or through sexual contact.

4. STATISTICS FOR NFB INTERVENTIONS FOR CHEMICAL AND RADIOLOGICAL RISKS, AND POTENTIAL BIOHAZARDS

Since 2000, the NFB publishes on their website statistics of province command interventions for yearly periods (NFB, 2012). For this work, statistics regarding CBRN was collected for analysis. In particular, as shown in Table 1, the interventions involving chemical and radiological risks were examined. The total number of interventions involving chemical substances was obtained by adding all the events classified as "*chemical substances involved*" and "*other inflammable and liquid and/or gaseous combustibles*", which includes "*accident with a vehicle transporting dangerous substances*", "*flipping over of a truck transporting dangerous substances*" and "*a gas leak*". The total number of interventions involving radioactive substances is reported in the official NFB statistics *tout court* and includes, among others, "*recovery of radioactive lightning rod*" and "*recovery of radioactive substances*".

Table 1: NFB interventions in 2000-2010 involving chemical and radioactive substances. (Adapted from NFB (2012)).

	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	*Mean*
Total interventions	646.395	751.388	706.556	713.184	736.434	750.617	716.053	717.892	745.572	782.897	736.673	
Chemical substances involved	28078	35570	37763	34301	34091	32786	31834	31388	27737	31174	28361	
% of total interventions	4,34	4,73	5,34	4,81	4,63	4,37	4,45	4,37	3,72	3,98	3,85	**4,42**
Radiactive substances involved	207	276	216	205	392	213	173	197	326	1929	243	
% of total interventions	0,03	0,04	0,03	0,03	0,05	0,03	0,02	0,03	0,04	0,25	0,03	**0,05**

The estimation of the percentages of interventions involving chemical and radioactive substances over total interventions is calculated for yearly periods. The mean percentage is obtained by averaging the annual percentages calculated over total yearly interventions.

While chemical and radiological risks are clearly evaluated in the NFB's statistics, this is not done for biohazards, which is neither considered nor put into a table. For this reason, in order to conduct a statistical analysis, we considered the types of interventions that can be potentially associated to biohazards (natural, human related or voluntary) as the following:

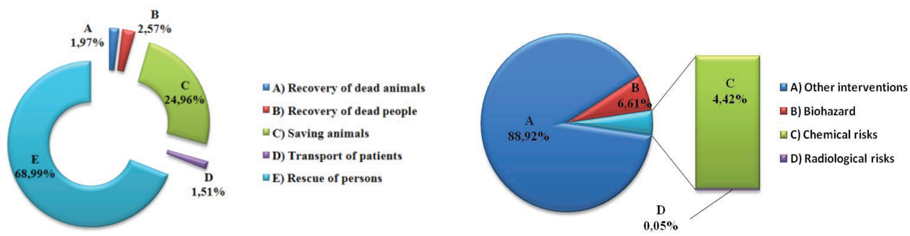
a) Saving of people;
b) Recovery of dead people;
c) Saving of animals;
d) Recovery of dead animals;
e) Transport of patients.

The non-specific category "*general assistance services*" was not considered. Following this notional evaluation, surprising results are obtained, as shown in Table 2. By taking the mean of the 2000-2010 data, we have a high percentage value (6.61%) as compared to chemical and radiological risks (Figure 1). However, it should be noted that since it is a notional estimation, this value can be far from the reality. It is nevertheless important because it highlights potential incidences of biohazards over the total of the interventions.

Table 2: NFB interventions in 2000-2010 potentially involving biohazards. (Adapted from NFB (2012)).

	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	*Mean*
Total interventions	646.395	751.388	706.556	713.184	736.434	750.617	716.053	717.892	745.572	782.897	736.673	
Potential biohazard involved interventions	38460	45999	48704	46466	48106	51782	48161	45933	49161	52941	53676	
% of total interventions	5,95	6,12	6,89	6,52	6,53	6,90	6,73	6,40	6,59	6,76	7,29	**6,61**

The estimation of the percentages of interventions involving biohazards over total interventions is calculated for yearly periods. The mean percentage is obtained by averaging the annual percentages calculated over total yearly interventions.



(a) **(b)**

Figure 1: Statistics of NFB interventions involving potential biohazards for 2000-2010 and comparison other interventions: (a) Types of interventions considered for the evaluation of potential biohazards. The percentages represent the mean percentages obtained for each type of intervention. (b) Rates of interventions involving biohazards, chemical and radiological risks, and other interventions.

5. PROPOSALS FOR IMPROVING THE NFB'S BIOHAZARD MANAGEMENT

The NFB is responsible for first response in case of biohazard events in the context of civil protection and defence. For this reason, the NFB has to be equipped with the necessary apparatus and consequently specialised personnel who can use it. While the NFB has developed its own competencies for chemical and radiological risks since the 1960s, for biohazards, there has been less time spent to put them into action, with all related developments happening in the last decade.

Although there is significant effort in trying to provide guidelines to first intervention operators for biohazard events, it evident that there is a high margin of uncertainty concerning the ability to provide immediate response to an event. There is also a lack of field instruments that can allow the detection and management of biological agents, excluding sheltered labs and rapid reverse transcription polymerase chain reaction (RT-PCR). While rapid RT-PCR allows the identification of a number of biological agents, it requires the right primers to be used and only works in specific analysis conditions.

The correct management of biohazards is very important to ensure that the operators' efforts are not in vain. It is common to consider the ON/OFF emergency response[1], but it is questionable whether it can be applied to biohazard management. In fact, responding with a wrong ON can lead to results that are more damaging as compared to not providing any response at all. This is understandable if we consider the extreme variability and the different pathogenicity, infectivity and transmissibility mechanisms of biological agents, and, consequently, the related methods to contain the dissemination. In addition, the correct identification of the biological agent involved in a biohazard event allows the intervention to take place in a generally secure situation. As the NFB does not have specialist biologists, the training of NFB operators in using instruments, such as rapid RT-PCR, is conducted by specialist biologists, mainly involved in CBRN defence, in the Italian Army.

In order to improve the response to biohazard events, the NFB should be provided with equipment and complex instrumentation for the sampling and detection of a large number of biological agents. This would require the hiring of specialist biologists in the NFB. They can have several important tasks both in the context of prevention and protection, and also in emergency management. Their key roles will include:

a) Development of biological agents detection systems;
b) Central coordination activities;
c) Collaboration with the healthcare offices for risk evaluation of the operators;
d) Updating guidelines, and technical and procedure indications;
e) Specific training for personnel operating in prevention, identification and risk management;
f) Inspecting products and equipment used in the mobile laboratories;
g) Participating in external communications in case of biohazard events.

6. CONCLUSION

Biohazards are, among the non-conventional risks, the most complex and difficult to manage. In this work, we evaluated the responsiveness of the main actor involved in the response to biohazards in Italy, the NFB. It reviewed procedures of NFB operators, in particular present

1 The ON/OFF emergency response is aimed at providing fast response to potential spread of a biological agent. In this first stage, in order to start the procedures, just one question is considered: is the agent present? (ON) or not present? (OFF), not taking into account the biological nature of the agent.

processes specifically developed for the management of biohazards. Although these actions have been developed and are applicable in specific situations (such as deliberate release of anthrax spores or pandemic diffusion of influenza virus), the possible strategies to approach the problem are limited. An effective solution to compensate for this would be the introduction of specialist biologist in the staff of the NFB in order to develop methods and procedures for the management of biohazards.

REFERENCES

Butel, J.S. (2000). Viral carcinogenesis: revelation of molecular mechanisms and etiology of human disease. *Carcinogenesis,* **21**: 405-426.

Centers for Diseases Control and Prevention (CDC). *Bioterrorism Agents / Diseases*. Available online at: http://www.bt.cdc.gov/agent/agentlist-category.asp (Last access date: 11 July 2012).

Department of Labor (DOL) (2012). *Occupational Safety & Health Administration: Biological Agents*. Available online at: http://www.osha.gov/SLTC/ biologicalagents/ index.html (Last access date: 11 July 2012).

European Commission (EC) (2000). European Parliament Directive 2000/54/EC on the Protection of Workers from Risks Related to Exposure to Biological Agents at Work. European Commission (EC), Brussels.

European Commission (EC) (2012). *Health-EU: Biological Risks*. Available online at: http:// ec.europa.eu/health-eu/my_environment/biological_risks/ngo_en .htm #tab_ngos (Last access date: 11 July 2012)

Gulli, R., Mari, G., Surchio, E., Amendola, L. & Garibaldi C. (2008). *CBRN Defence - Shelter mobile lab of the Firefighter Provincial Command of Rome*.

Kaszeta, D. (2012). *CBRN and Hazmat Incidents at Major Public Events: Planning and Response.* John Wiley & Sons, Inc.

La Placa, M. (2010). *Principles of Medical Microbiology*. Esculapio, XII edition.

Ministry of Interior (MOI) (1941). *Law 1570/1941: Establishment of Rules for the Organisation of Firefighting Services*. Ministry of Interior (MOI), Italy.

Ministry of Interior (MOI) (2001a). *Circular Decree 1706/CO-2001: Management in Presence of Anthrax Spores Potentially Contaminated Materials*. Ministry of Interior (MOI), Italy.

Ministry of Interior (MOI) (2001b). *Intervention in the Presence of Unconventional (of Military Type) Chemically Aggressive or Industrial Equivalent.* Ministry of Interior (MOI), Italy.

Ministry of Interior (MOI) (2002). *Legislative Decree 139/2006: Intervention Manual in the Presence of CBRN Risks*. Ministry of Interior (MOI), Italy.

Ministry of Interior (MOI) (2006). *Circular Decree 325/CO-2006. Biohazard – Avian Flu – Individual equipments for potentially exposed NFB staff.* Ministry of Interior (MOI), Italy.

Ministry of Interior (MOI) (2006). *Reorganization of the Provisions Relating to the Functions and Duties of the National Fire Brigades, in Accordance with Article 11 of the Law of 29 July 2003*. Ministry of Interior (MOI), Italy.

Ministry of Labor (MOL) (2006). *Legislative Decree 81/2008: Safety-at-Work Provisions Applicable to Contracts*. Ministry of Labor (MOL), Italy.

National Fire Brigade (NFB) (2012). *Statistics: Operations in the Territory*. Available online at: http://www.vigilfuoco.it/aspx/page.aspx?IdPage=450 (Last access date: 11 October 2012).North Atlantic Treaty Organization (NATO) (1996). *NATO Handbook on the Medical Aspects of NBC Defensive Operations AMedP-6(B*). *Part II - Biological*. U.S. Department of the Army, the Navy and the Air Foce, Washington DC.

Defence S&T Tech. Bull.,6(1) :42-61,2013

GLOBAL NAVIGATION SATELLITE SYSTEM (GNSS) SPOOFING: A REVIEW OF GROWING RISKS AND MITIGATION STEPS

Dinesh Sathyamoorthy

Science & Technology Research Institute for Defence (STRIDE), Ministry of Defence, Malaysia

*E-mail: dinesh.sathyamoorthy@stride.gov.my

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 synchronisation for utility, telecommunications, banking and computer industries. At present, there are two types of GNSS signals; military GNSS signals (L1 P(Y) and L2 P(Y) for the case of GPS, and L1 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 P(Y), 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 spoofing, which refers to forging and transmission of navigation messages in order to manipulate the navigation solutions of GNSS receivers. Spoofing of civilian GNSS signals is surprisingly simple to conduct by even relatively unsophisticated adversaries. Due to the increasing reliance of various industries on GNSS, the consequences of GNSS spoofing can be severe, in terms of safety, environmental and economic damage. Hence, GNSS vulnerability mitigations steps should be given emphasis, including positioning/ navigation / timing (PNT) backups, making full use of on-going GNSS modernisation programmes, inference detection & monitoring (IDM), and counter-spoofing technologies. This paper is aimed at reviewing the vulnerability of civilian GNSS signals to spoofing and the steps that can be taken to mitigate this vulnerability.

Keywords: *Global Navigation Satellite System (GNSS) spoofing; GNSS simulators; meaconing; positioning/navigation/timing (PNT)backups; counter-spoofing.*

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 synchronisation 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 utilise the GNSS information to determine its own location (Kaplan & Hegarty, 2006; RAE, 2011).

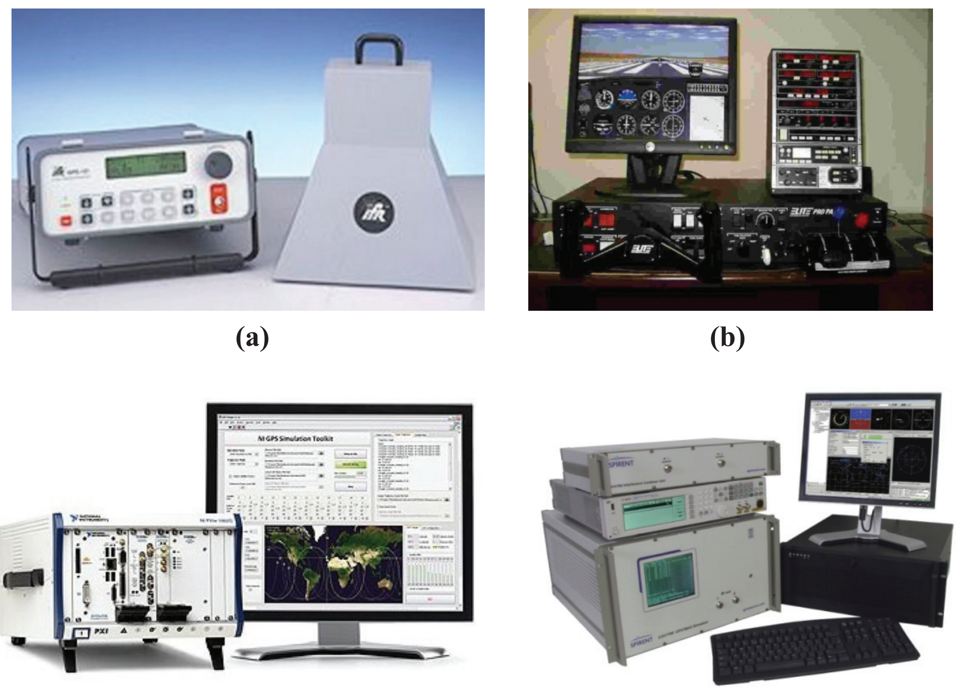
Each GNSS receiver is able to receive simultaneously a set of navigation messages, one message from each satellite in the visible satellite constellation. The navigation messages enable each receiver to determine its own position in a Cartesian system, as well as a time correction offset to add to its 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; RAE, 2011).

At present, there are two types of GNSS signals; military GNSS signals (L1 P(Y) and L2 P(Y) for the case of GPS, and L2 for GLONASS) and civilian GNSS signals (L1 coarse acquisition (C/A) for GPS, and L1 for GLONASS). Usage of GPS L1 P(Y) and L2 P(Y), and GLONASS L2 signals are limited to the US and Russian militaries respectively. Other users only have access to civilian GNSS signals (Kaplan & Hegarty, 2006; RAE, 2011). Usage of civilian GNSS signals is growing rapidly due to 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 synchronisation is being increasingly employed, such as timing reference for power station grids, telecommunications systems and digital air-ground communications systems (GAO, 2009; Last, 2010; RAE, 2011; Caverly, 2011; Merill, 2012). 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 spoofing, which refers to forging and transmission of navigation messages in order to manipulate the navigation solutions of GNSS receivers. 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. 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, it can still create significant errors and jam GNSS signals over large areas (Volpe, 2001; Johnston & Warner, 2004; Papadimitratos & Jovanovic, 2008; Humphreys *et al.*, 2009; Dinesh, 2009, 2011; Last, 2010; Jones, 2011; Wesson *et al.*, 2012; Scott, 2012). This paper is aimed at reviewing the vulnerability of civilian GNSS signals to spoofing and the steps that can be taken to mitigate this vulnerability.

2. THE SPOOFING THREAT CONTINUUM

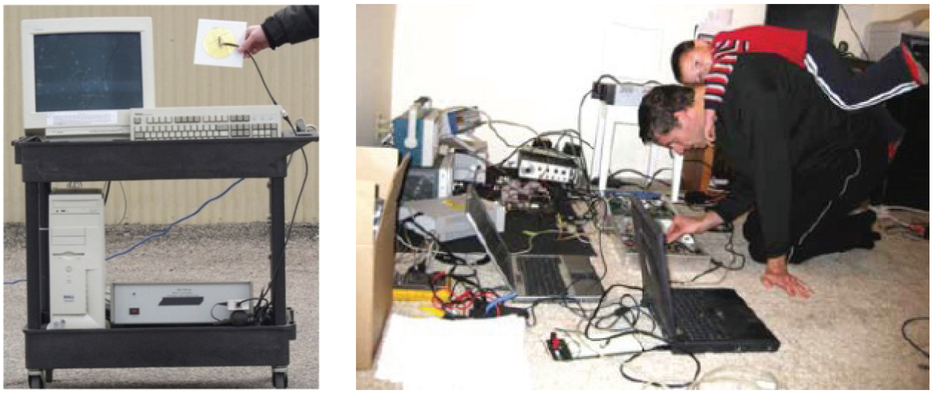
A number of GNSS simulators (Figure 1) have been designed for legal purposes such as user training, system maintenance, vehicle motion simulation and radio frequency interference (RFI) operability tests, such as conducted in Dinesh *et al.* (2012a, b). However, in the wrong hands, these GNSS simulators can be used to conduct illegal spoofing. Furthermore, GNSS simulators can be built with relatively low cost equipment (Figure 2), as demonstrated by Rogers (1991), Johnston & Warner (2004), Humphreys *et al.* (2008), Hanlon *et al.* (2009), Nicola *et al.* (2010) and Humphreys (2012).



(a) (b)

(c) (d)

Figure 1: Commercially available GNSS simulators: (a) Flightspectrum's Elite Basic Training Device PI-135 makes use of Garmin's G1000 GPS simulator. (b) Areoflex's GPS-101 GPS simulator. (c) National Instruments' (NI) PXI GNSS simulator. (d) Spirent's GSS7700 GNSS simulator, with a GSS4766 interference simulation system.



(a) (b)

Figure 2: Homemade GNSS simulators.
(Sources: (a) Johnston & Warner (2004); (b) Humphreys (2012)).

Hanlon *et al.* (2009) and Montgomery *et al.* (2009) classify GNSS spoofers into three categories, simplistic, intermediate and sophisticated, depending on their complexity and level of robustness required to the associated counter-spoofing measures (Figure 3). Simplistic attacks are conducted using standalone GNSS simulators. In this type of spoofing attack, the spoofing signal is not synchronised (in terms of power level, phase, Doppler shift and data content) with the genuine signals received by the target GPS receiver. This could cause the target GPS receiver to temporarily lose position fix lock first, before being taken over by the spoofing signal. Even if the unsynchronised attack could avoid causing loss of lock, it could still cause an abrupt change in the target GPS receiver's time estimate. Rudimentary counter-spoofing measures, such as amplitude and time-of-arrival discrimination, and loss of lock notification, could be used to detect simplistic spoofing attacks. However, many of present civilian GNSS receivers are not equipped with such measures, and hence, are vulnerable to simplistic spoofing attacks.

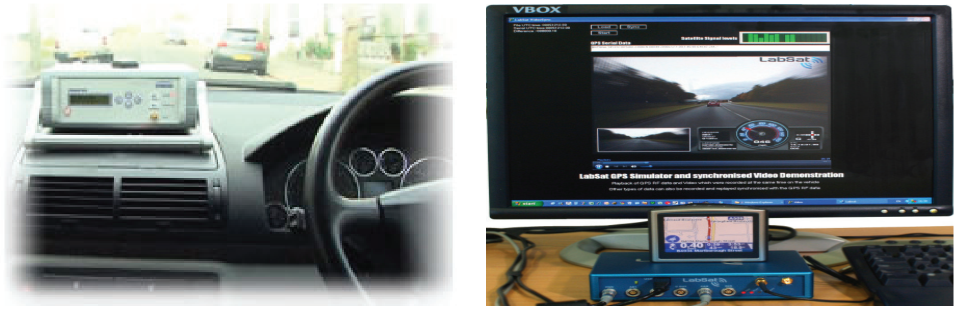
Figure 3: The spoofing threat continuum; simplistic, intermediate and sophisticated spoofing attacks. (Source: Hanlon et al. (2009)).

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.

An alternate method of conducting GNSS spoofing is using GNSS record and playback systems (Figure 4), which have recently become popular for GNSS receiver evaluation. Such systems record real GNSS signals and retransmit the signals to evaluated GNSS receivers. As with GNSS simulators, GNSS record and playback systems can also, in the wrong hands, be used for spoofing. While this method cannot be used to impose user-defined scenarios on a receiver, it can still cause the receiver to compute false location fixes using the transmitted real GNSS signals. Furthermore, this form of attack can be used for spoofing military GNSS signals (Jones, 2011; Humphreys, 2012; Sherman *et al*., 2012).

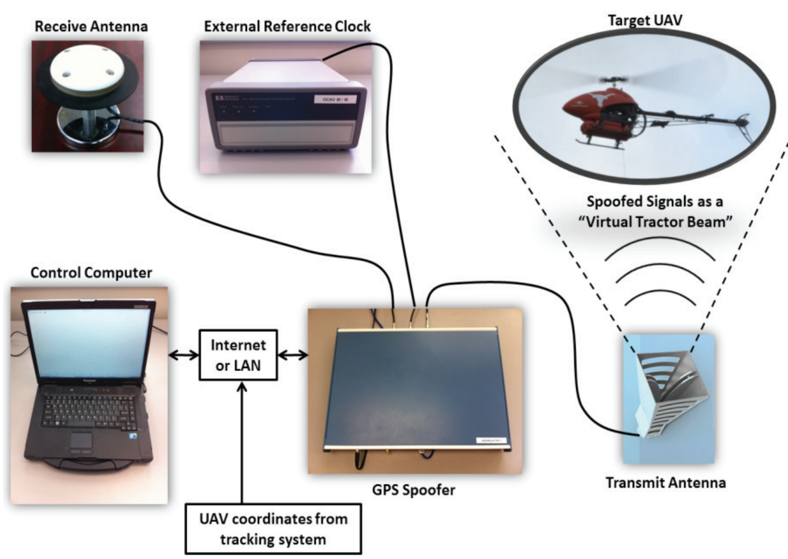
While GNSS spoofing has not yet emerged as a major threat, it represents a growing risk, with a number of successful spoofing experiments on GNSS receivers being conducted, whereby the respective receivers failed to detect the presence of such attacks (Figure 5) (Warner & Johnston, 2002; Humphreys *et al.*, 2008; Motella *et al.*, 2010; Cavaleri *et al.*, 2010; Tippenhauer *et al.*, 2011; Shepard & Humphreys, 2011; Dinesh *et al*., 2012c). In addition, recent studies have demonstrated the vulnerabilities of GNSS-based systems for unmanned aerial vehicle (UAV) navigation and power grid time synchronisation to spoofing (Figure 6) (Shepard *et al.*, 2012).



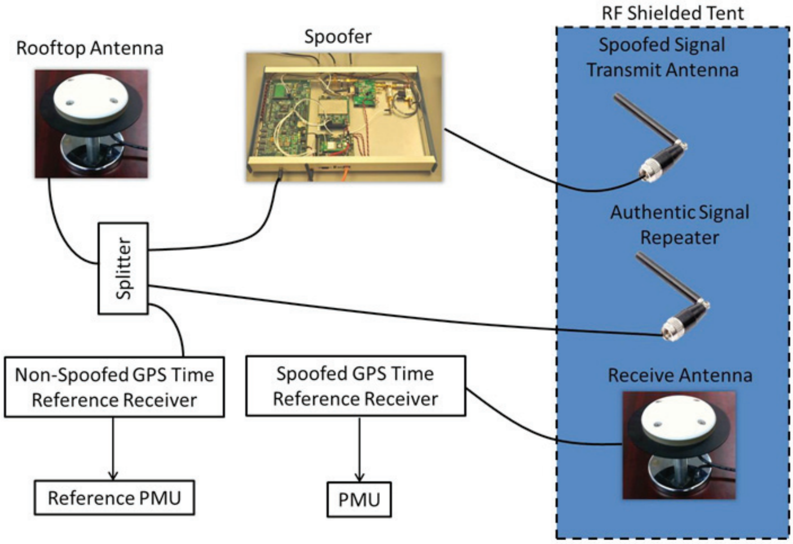
(a) (b)

Figure 4: Commercially available GNSS record and playback systems: (a) Spirent's GSS6400. (b) LabSat 2.

Figure 5: GPS spoofing tests conducted by the Science & Technology Research Institute for Defence (STRIDE) as part of the study in Dinesh *et al*. (2012c).



(a)



(b)

Figure 6: Spoofing setups for: (a) UAV navigation. (b) Phasor measurement unit (PMU) for power grid time synchronisation. (Source: Shepard et al. (2012)).

3. MITIGATION STEPS

3.1 Positioning / Navigation / Timing (PNT) Backups

The most recommended GNSS vulnerability mitigation step is the application of positioning/ navigation backups which can be used in the case of GNSS disruptions (Volpe, 2001; Lilley, 2006; Last, 2010; Groves, 2010; RAE, 2011; El-Sheimy & Goodall, 2011; Schue, 2012). Navigation backups, such as 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 (Grant *et al.*, 2009; Safar *et al.*, 2011; Hargreaves *et al.*, 2012) (Figure 7). An Independent Assessment Team (IAT) report (IDA, 2009), commissioned by the US Department of Transport (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 synchronisation should employ suitable timing backups, such as internet time services, network time protocols and commercially available chip scale atomic clocks (CSACs) (Figure 8) (Klepczynski, 2011).

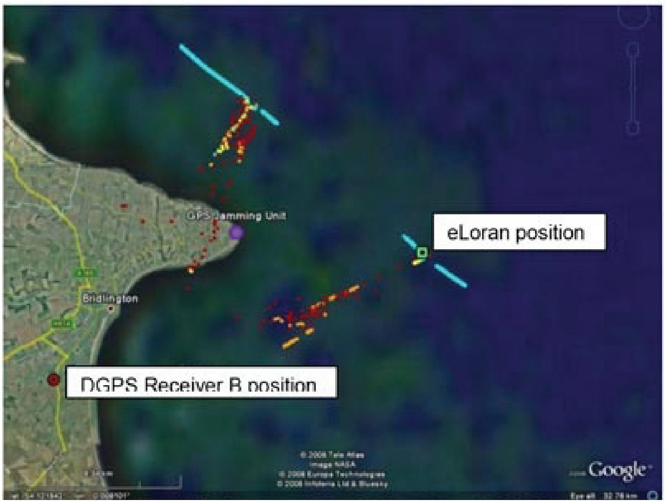


Figure 7: The General Lighthouse Authorities (GLAs) of the United Kingdom and Ireland conducted a GPS jamming exercise from 31 March to 4 April 2008 to investigate the performance of eLoran during GPS service denial. It was reported that eLoran was unaffected by GPS jamming and demonstrated an accuracy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

(a) (b)

Figure 8: Commercially available chip scale atomic clocks (CSACs): (a) Symmetricom's SA.45s. (b) Jackson Labs Technologies' GPSDO.

3.2 GNSS Modernisation Programmes

GNSS users should also take full advantage of the various ongoing GNSS modernisation programmes (Figure 9) (McDonald, 2002; Blomenhofer, 2004; Alkan *et al.*, 2005; Gakstatter & Flick, 2006; Kaplan & Hegarty, 2006; Gakstatter, 2008, 2010, 2011; GAO, 2009; Rizos, 2009; Gibbons, 2011; Marquis & Shaw, 2011). The upcoming new civilian GPS III signals that are to be provided, the L1C, L2C and L5 signals (Figure 10), will be able to provide a substantial reduction in the threat of unintentional jamming, and some degree of threat reduction from intentional jamming and spoofing. 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 and spoofing. 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; Gakstatter, 2010, 2011).

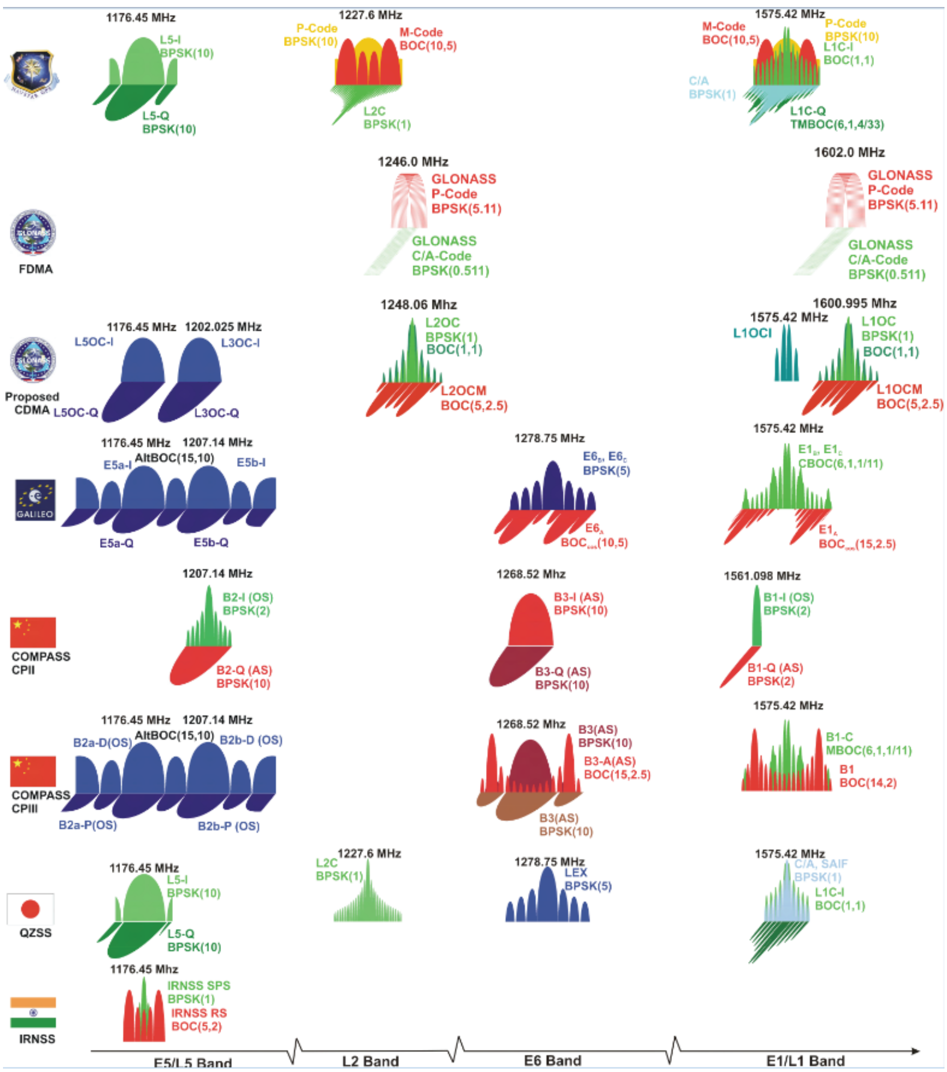


Figure 9: GNSS signals planned under various GNSS modernisation programmes. (Source: Hein et al. (2007)).

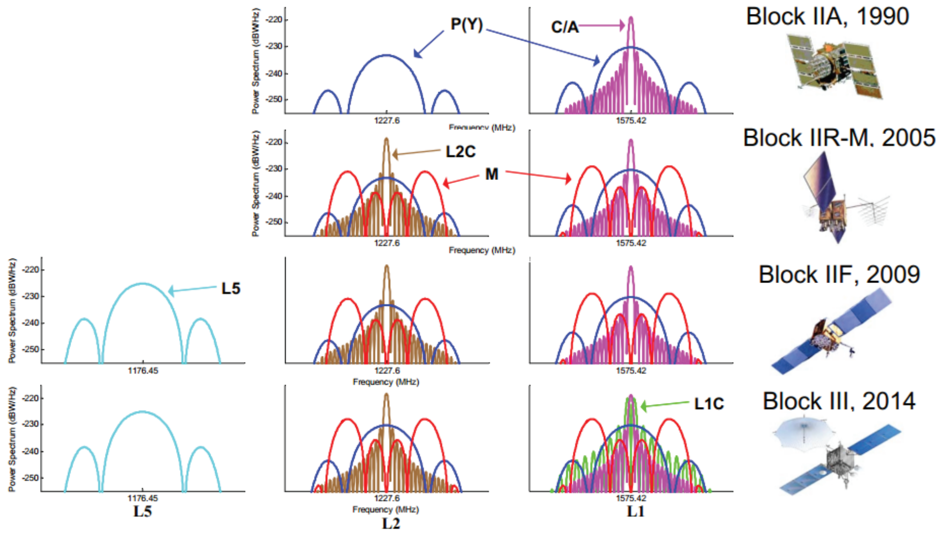
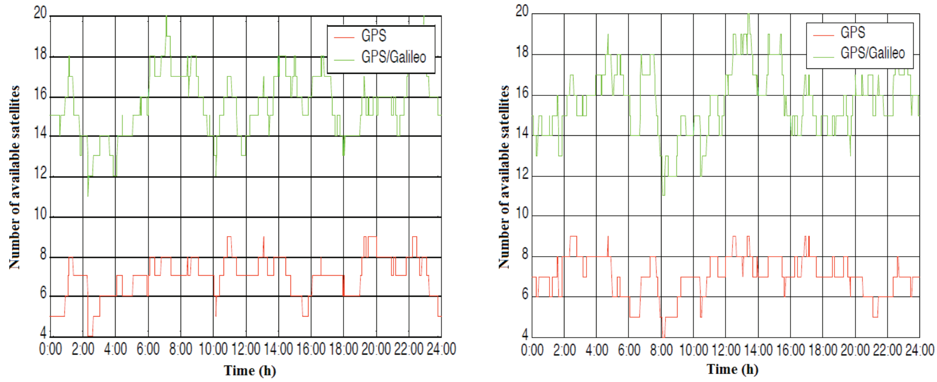


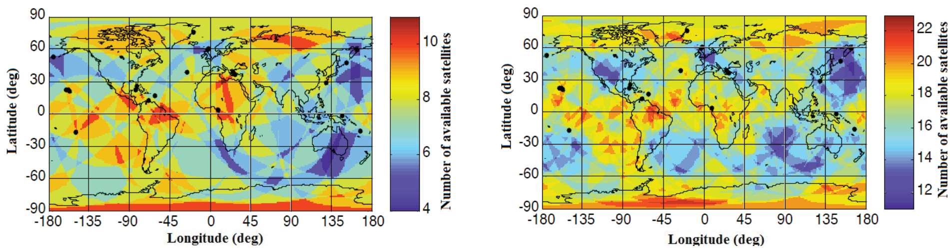
Figure 10: Present and future GPS signals. (Source: Harrington (2008)).

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 ground station 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, 2008; Wistuba *et al*., 2011). 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 11), and worldwide (Figure 12). 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 mass market users (Alkan *et al.,* 2005; Gakstatter & Flick, 2006; Gakstatter, 2008, 2010; Wistuba *et al*., 2011).



(a) **(b)**

Figure 11: Satellite availability at (a) Sydney and (b) Portland over 24 h 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 16 January 2003. (Source: Hewitson (2003))



(a) **(b)**

Figure 12: Worldwide satellite availability for (a) GPS and (b) combined GPS / Galileo. The results were obtained from snapshot simulations for 0:00 h on 16 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)).

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 (Sergey *et al.*, 2007; Revnivykh, 2008). This minimum constellation was completed on 8 December 2011 (Langley, 2011). 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; Ashjaee, 2011). GLONASS has begun broadcasting CDMA signals beginning with the GLONASS-K generation of satellites, the first of which was launched on 26 February 2011 (Urlichich *et al.*, 2011).

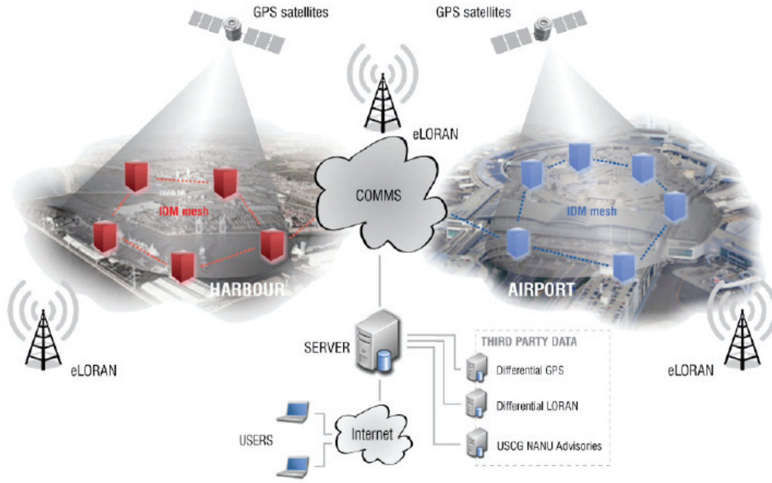
3.3 Interference Detection & Monitoring (IDM)

IDM systems to monitor, report and locate jamming/spoofing 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 / spoofing source as quickly as possible. Recent technologies in signal tracking and detection (Figure 13), such as Tektronix's H600 RF Hawk (Tektronix, 2008), Rohde & Schwarz's PR100 (Rohde & Schwarz, 2011) and Research Electronics International's (REI) Oscor Green (REI, 2012), should precipitate this.

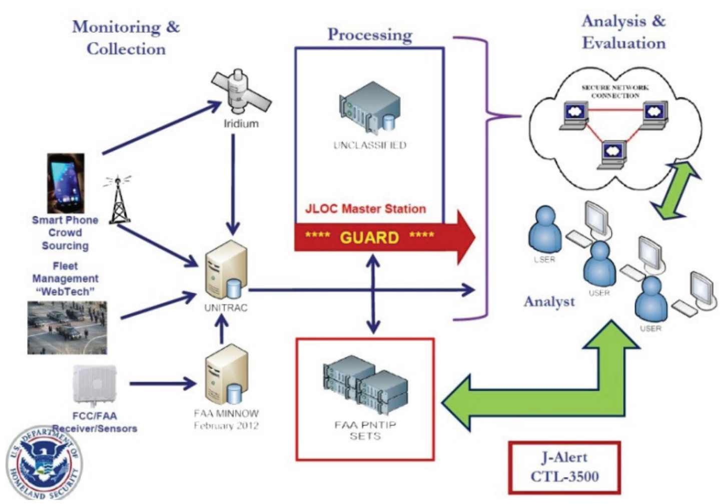
(a) (b) (c)

Figure 13: Recent technologies in signal tracking and detection should allow for the fast and effective identification and location of jamming/spoofing sources: (a) Tektronix's H600 RF Hawk. (b) Rohde & Schwarz's PR100. (c) REI's Oscor Green.

In addition, IDM networks have been developed in UK (GNSS Availability, Accuracy, Reliability and Integrity Assessment for Timing and Navigation (GAARDIAN)) (Chronos, 2010; Curry, 2011) and US (Patriot Watch) (Merill, 2012), which employ networks of IDM sensors for deployment in the vicinity of PNT dependent infrastructure and applications (Figure 14). These sensors will be used to monitor the integrity, reliability and accuracy of locally received GNSS and eLORAN signals, and alert users of possible interferences.



(a)



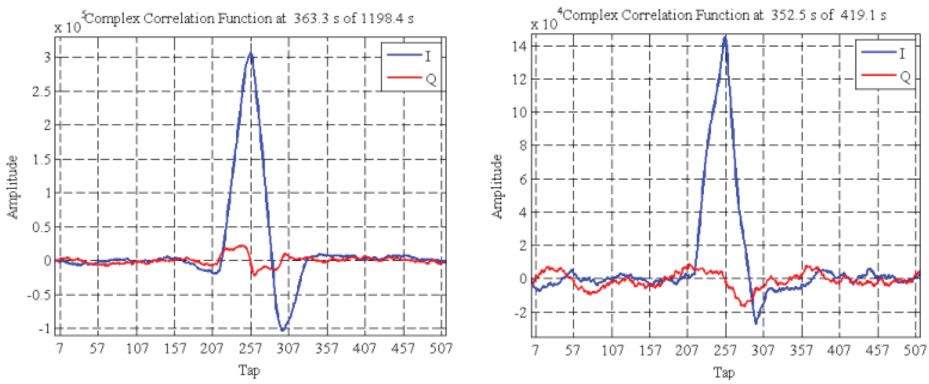
(b)

Figure 14: IDM networks: (a) The GAARDIAN system developed in UK (Chronos, 2010; Curry, 2011). (b) The Patriot Watch system developed in US (Merill, 2012).

3.4 Counter-Spoofing Technologies

The simplest method of detecting GNSS spoofing is by employing a jamming-to-noise (J/N) sensor to monitor for increase in in-band received power caused by spoofing signals. However, for a threshold corresponding to a reasonable false alarm rate, a J/N sensor will not typically detect spoofing attacks in which the spoofed signals are only slightly more powerful than their authentic counterparts (Jones, 2011; Weeson *et al*., 2012; Sherman *et al*., 2012).

The difficulty of nulling out authentic GNSS signals during spoofing attacks results in the remaining portion of the authentic signals manifesting as distortions in the complex correlation domain. These distortions are used by correlation profile anomaly defences to detect spoofing attacks. While these methods are effective for stationary GNSS receivers, such as used for timing applications, for moving GNSS receivers, they suffer from the difficulty in distinguishing between multipath effects and spoofing attacks (Figure 15) (Nielson *et al*., 2011; Weeson *et al*., 2011, 2012).

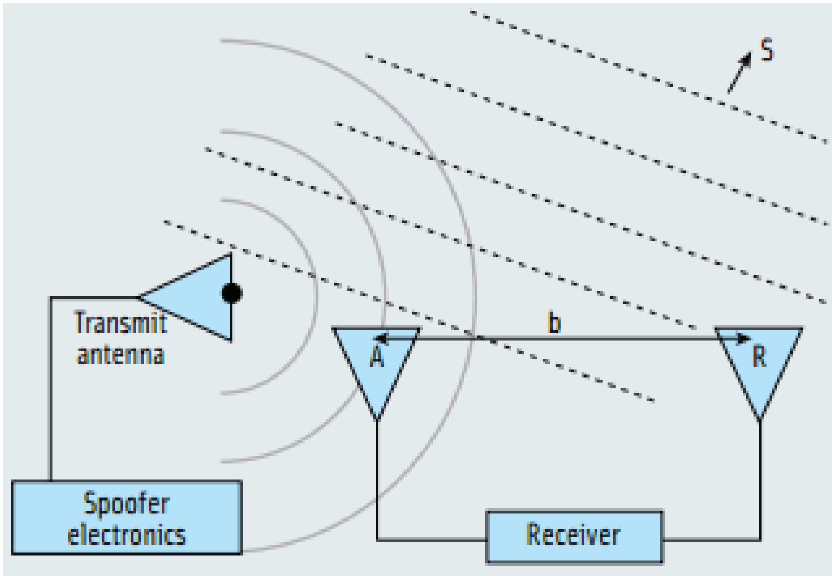


(a) **(b)**

Figure 15: Plots of complex correlation domain during: (a) A spoofing attack on a stationary GNSS receiver. (b) A moving non-spoofed GNSS receiver. The difficulty in distinguishing between multipath effects and spoofing attacks makes correlation profile anomaly defences ineffective in detecting spoofing attacks for moving GNSS receivers. (Source: Wesson et al. (2011)).

Antenna-based defences generally provide effective options for counter-spoofing, but most of these methods require additional hardware and costs. The multi-array antennas employs angle-of-arrival discrimination for spoofing detection, whereby a spoofer will have great difficulty in mimicking the relative carrier phase of authentic GNSS signals as received by two or more spatially-separated antennas (Figure 16) (Montgomery *et al*. 2009; Daneshmand *et al*., 2012). Nielson *et al*. (2011) employed signal spatial correlation to generate a synthetic array using a moving single receiver antenna. A high spatial correlation between received signals indicates a probable inauthentic source for the GNSS signals.

(a)



(b)

Figure 16: Angle-of-arrival discrimination for spoofing detection: (a) A dual-antenna receiver. (b) Antenna diversity geometry for a single satellite and point transmitter, where S is a unit of line of sight (LOS) vector to a GNSS satellite, and b is the baseline vector between the two antennas. (Source: Montgomery et al. (2009)).

4. CONCLUSION

Civilian GNSS signals are vulnerable to spoofing, which manipulates the location and time that the receivers compute. With increasing dependence on GNSS for PNT applications, in order to avoid the possible consequences of spoofing attacks on GNSS signals, GNSS vulnerability mitigations steps should be given emphasis, including PNT backups, making full use of on-going GNSS modernisation programmes, inference detection & monitoring (IDM), and counter-spoofing technologies.

ACKNOWLEDGEMENT

This manuscript is an extended version of the discussions in Dinesh (2009, 2011) on the vulnerabilities of GNSS to jamming and spoofing. It was prepared as part of the preliminary work for the proposed Tenth Malaysian Plan (RMK10) Phase II project entitled *Simulation and Modelling of Global Navigation Satellite System (GNSS) Error Parameters.*

REFERENCES

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.

Ashjaee, J. (2011). *How GPS and GLONASS Got Together - and Other Recent Events*. Available online at: http://www.gpsworld.com/gnss-system/glonass/how-gps-and-glonass-got-together-and-other-recent-events-11720 (Last access date: 3 June 2011).

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

Cavaleri, A., Motella, B., Pini, M. & Fantino, M. (2010). Detection of spoofed GPS signals at code and carrier tracking level. *2010 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, 8-10 December 2010, Noordwijk.

Caverly, J. (2011). Key note address. *GNSS Interference Detection, and Mitigation (IDM) Conference*, 10 March 2011, National Physical Laboratory (NPL), Teddington.

Daneshmand, S., Jafarnia-Jahromi, A., Broumandan, A. & Lachapelle, G. (2012). A low-complexity GPS anti-spoofing method using a multi-antenna array. *ION GNSS 2012*, 17-21 September 2012, Nashville, Tennessee.

Dinesh, S. (2009). Vulnerabilities of civilian Global Navigation Satellite Systems (GNSS) signals: A review. *Defence S&T Tech. Bull.*, **2**: 100-114.

Dinesh, S. (2011). Vulnerabilities of Global Navigation Satellite Systems (GNSS) signals to jamming and spoofing. *GIS Day 2011*, 17 March 2011, Universiti Putra Malaysia (UPM), Serdang, Selangor.

Dinesh, S., Mohd Faudzi., M., Rafidah, M., Nor Irza Shakhira, B., Siti Robiah, A., Shalini, S., Aliah, I., Lim, B.T., Zainal Fitry, M.A., Mohd. Rizal, A.K., & Mohd Hasrol, H.M.Y. (2012). Evaluation of the effect of radio frequency interference (RFI) on the Global Positioning System (GPS) L1 coarse acquisition (C/A) signal via GPS simulation. *11th International Symposium & Exhibition on Geoinformation 2012 (ISG2012)*, 25-26 September 2012, Hotel Istana Kuala Lumpur City Centre, Kuala Lumpur.

Dinesh, S., Mohd Faudzi., M. & Zainal Fitry, M.A. (2012b). Evaluation of the effect of radio frequency interference (RFI) on Global Positioning System (GPS) accuracy via GPS simulation. *Defence Sci. J.*, **62**: 338-347.

Dinesh, S., Mohd Faudzi., M., Nor Irza Shakhira, B., Siti Robiah, A., Shalini, S., Jamilah, J., Aliah, I., Lim, B.T., Zainal Fitry, M.A., Mohd. Rizal, A.K., & Mohd Hasrol, H.M.Y. (2012c). Evaluation of Global Positioning System (GPS) Performance During Simplistic GPS Spoofing Attacks. Defence S&T Tech. Bull., **5:** 99-113.

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

El-Sheimy, N. & Goodall, C. (2011). Everywhere navigation: Integrated solutions on consumer mobile devices. *Inside GNSS,* **6**: 74-82.

Gakstatter, E. (2008). 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: 4 November 2009).

Gakstatter, E. (2010). Remember How Slow Dial-up Was? That's Where GPS Is Today. Available online at: http://www.gpsworld.com/gis/gss-weekly/remember-how-slow-dial-was-thats-where-gps-is-today-10963?utm_source=GSS&utm_medium=email&utm_campaign=Geospatial-Weekly_01_20_2011&utm_content=remember-how-slow-dial-was-thats-where-gps-is-today-10963 (Last access date: 21 January 20010).

Gakstatter, E. (2011). A closer look at L5: The future of high-precision GNSS. *GPS World Market Insights Webinar*, 17 March 2011.

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: 4 November 2009).

Gibbons, G. (2011). Modernization times: Col. Bernard Gruber & the GPS enterprise. *Inside GNSS*, **6**: 38-44.

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), US.

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: 4 November 2009).

Groves, P.D. (2010). Positioning, navigation and timing without using GNSS. *GPS Jamming & Interference: A Clear and Present Danger*, 23 February 2010, National Physics Laboratory, Teddington.

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: 4 November 2009).

Hargreaves, C., Williams, P. & Bransby, M. (2012). ASF quality assurance for eLoran. *2012 IEEE/ION Position Location and Navigation Symposium (PLANS)*. 23-26 April 2012, Myrtle Beach, South Carolina.

Harrington, P. (2008). GPS program update. *ICG Expert Meeting on GNSS,* 15 July 2008, Montreal, Canada.

Hein, G.W., Rodriguez, J.A.A., Wallner, S., Eisfeller, B., Pany, T. & Hartl, P. (2007). Envisioning a future GNSS system of systems: Part 1. *Inside GNSS*, **2**: 58-67.

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*, 9-12 September, Portland, Oregon.

Humphreys, T. (2012). The GPS dot and its discontents: Privacy vs GNSS integrity. *Inside*

GNSS, **7**: 44-48.

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*, 16-19 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: 4 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.

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

Jones, M. (2011). The civilan battlefield: Protecting GNSS receivers from interference and jamming. *Inside GNSS,* **6**: 40-49.

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

Klepczynski, B. (2011). Pillaging and plundering the PNT spectrum. *GPS World Market Insights Webinar*, 17 March 2011.

Langley, R. (2011). *GLONASS Fully Operational, First Time in 15 Years*. Available online at: http://www.gpsworld.com/gnss-system/news/glonass-fully-operational-first-time-15-years-12379?utm_source=GPS&utm_medium=email& utm_campaign=Defense-PNT_12_14_2011&utm_content=glonass-fully-operational-first-time-15-years-12379 (Last access date: 16 December 2011).

Last, D. (2010). GNSS: The present imperfect. *Inside GNSS*, **5**: 60-64.

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.

Marquis, W. & Shaw, M. (2011). GPS III: Bringing new capabilities to the global community. *Inside GNSS*, **6**: 34-48.

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

Merill, J. (2012). *Patriot Watch Interference Detection & Mitigation (IDM): Safeguarding America*. US Department of Homeland Security, Washington, DC.

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

Motella, B., Pini, M., Fantino, M., Mulassano, P., Nicola, M., Fortuny-Guasch, J., Wildemeersch, M. & Symeonidis, D. (2010). Performance assessment of low cost GPS receivers under civilian spoofing attacks. *2010 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, 8-10 December 2010, Noordwijk.

Nicola, M., Musumeci, M., Pini, M., Fantino, M. & Mulassano, P. (2010). Design of a GNSS spoofing devicebased on a GPS/Galileo software receiver for the development of robust countermeasures. *European Navigation Conference 2010 (ENC 2010)*, 19-21 October 2010, Braunchweig, Germany.

Nielsen, J., Broumandan & Lachappelle, G. (2011). GNSS spoofing detection for single antenna handheld receivers. *J. Inst. Nav.*, **58**: 335-344.

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

Research Electronics International (REI) (2012). *Oscor Green Spectrum Analyser*. Research Electronics International (REI), Algood, Tennessee.

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

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

Rohde & Schwarz (2011). *Rohde & Schwarz PR100 Portable Receiver: On-site Radiomonitoring from 9 kHz to 7.5 GHz*. Rohde & Schwarz, Munich.

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.

Royal Academy of Engineering (RAE) (2011). *Global Navigation Space Systems: Reliance and Vulnerabilities*. Royal Academy of Engineering, London.

Safar J., Vejrazka F. & Williams P. (2011). *Assessing the limits of eLoran positioning accuracy. Int. J. Mar. Nav. Safety Sea Transp.*, **5**: 93-101.

Schue, C. (2012). The challenges of realizing a global navigation capability. *ION International Technical Meeting (ITM) 2012*, 30 January - 1 February 2012, Newport Beach, California.

Scott, L.S. (2012). Spoofs, proofs & jamming: Towards a sound national policy for civil location and time assurance. *Inside GNSS*, 7: 42-53.

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

Shepard, D.P. & Humphreys, T.E. (2011). Characterization of receiver response to spoofing attacks. *ION GNSS 2011*, 19-23 September 2011, Portland.

Shepard, D.P., Bhatti, J.A. & Humphreys, T.E. (2012). Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks. *ION GNSS 2012*, 17-21 September 2012, Nashville Convention Center, Nashville, Tennessee.

Sherman, L., Dennis, A., Eklöf, F.M., I.O. & Borowski, H. (2012). *Detecting False Signals with Automatic Gain Control*. Available online at: http://www.gpsworld.com/government/detecting-false-signals-automatic-gain-control-12804 (Last access date: 15 May 2012).

Tippenhauer, N.O., Pöpper, C., Rasmussen, K.B. & Čapkun, S. (2011). On the requirements for successful GPS spoofing attacks. *ACM Conference on Computer and Communications Security (CCS)*, 17-21 October 2011, Chicago, Illinois.

Urlichich, Y. Subbotin, V., Stupak, G., Dvorkin, V., Povalyaev, A. & Karutin, S. (2011).

GLONASS modernization. ION GNSS 2011, 20-23 September 2011, Portland, Oregon.

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.

Warner, J.S. & Johnston, R.G. (2002). A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing. *J. Secur. Admin.*, **25**: 19-28.

Wesson, K.D., Shepard, D.P., Bhatti, J.A. & Humphreys, T.E. (2011). An evaluation of the vestigial signal defense for civil GPS anti-spoofing. *ION GNSS 2011*, Portland, Oregon.

Wesson, K., Shephard, D. & Humphreys, T.E.(2012). *Straight Talk on Anti-Spoofing*. Available online at: http://www.gpsworld.com/GNSS%20 System/Signal%20Processing/straight-talk-anti-spoofing-12471 (Last access date: 10 January 2012).

Wistuba, G., Vasylyev, A., Haas, S., Driesen, J., Dalluge, L., Peitscher, D., Kramer, B., Dohmen, C. & Henkel, F. (2011). *2011 International Conference on Localization and GNSS (ICL-GNSS)*, 29-30 June 2011, Tampere, Finland.

Defence S&T Tech. Bull.,6(1) :62-74,2013

EVALUATION OF THE EFFECT OF MULTIPATH ON GLOBAL POSITIONING SYSTEM (GPS) PERFORMANCE VIA GPS SIMULATION

Dinesh Sathyamoorthy, Shalini Shafii, Zainal Fitry M Amin & Siti Zainun Ali*

Instrumentation & Electronics Technology Division (BTIE), Science & Technology Research Institute for Defence (STRIDE), Ministry of Defence, Malaysia

**E-mail: dinesh.sathyamoorthy@stride.gov.my*

ABSTRACT

In this study, Global Positioning Satellie (GPS) simulation is employed to study the effect of multipath on two handheld GPS receivers; Garmin GPSmap 60CSx (evaluated GPS receiver) and Garmin GPSmap 60CS (reference GPS receiver). Both GPS receivers employ the GPS L1 coarse acquisition (C/A) signal. Based on the results of this study, it is found that the decrease in number of visibles satellites due to physical obsructions and increase in number of multipath signals cause increase in probable error values, due to decreasing carrier-to-noise density (C/N_0) levels for GPS satellites tracked by the receiver. In addition, the differences between horizontal positioning error (HPE) and vertical positioning error (VPE) values increase due to the removal of satellites above the horizon, while overhead satellites are maintained. Varying probable error patterns are observed for readings taken at different times. This is due to the GPS satellite constellation being dynamic, causing varying GPS satellite geometry over time, resulting in GPS accuracy being time dependent. The repeatability of multipath at stationary sites when GPS satellites are in the same positions during each orbital pass (approximately 11 min, 58 s) allows for corrections to be generated based on history of multipath occurances over time.

Keywords: *Global Positioning System (GPS) simulation; multipath; physical obstructions; GPS satellite elevation; probable error.*

1. INTRODUCTION

There is a steady growth in the entrenchment of Global Navigation Satellite Systems (GNSS) in current and upcoming markets, having penetrated various consumer products, such as cell phones, personal navigation devices (PNDs), cameras and assimilation with radio-frequency identification (RFID) tags, for various applications, including navigation, surveying, timing reference and location based services (LBS). While the Global Positioning System (GPS), operated by the US Air Force (USAF), is the primarily used GNSS system worldwide, the upcoming Galileo and Compass systems, and the imminent conversion of *Global'naya Navigatsionnaya Sputnikovaya Sistema* (GLONASS) signals from frequency division multiple access (FDMA) to code division multiple access (CDMA) look set to make multi-satellite GNSS configurations the positioning, navigation & timing (PNT) standard for the future.

However, many GNSS users are still not fully aware of the vulnerabilities of GNSS systems to various error parameters, such as ionospheric and tropospheric delays, satellite clock and ephemeris errors, satellite positioning and geometry, radio freqecuency interference (RFI) and spoofing, and obstructions and multipath. These error parameters can severely affect the accuracy of GNSS readings, and in a number of cases, disrupt GNSS signals (Volpe, 2001; Kaplan & Hegarty, 2006; Dinesh, 2009, 2011; Last, 2010; Schwartz, 2010; RAE, 2011; Schue, 2012).

Multipath refers to the distortion of direct line-of-sight (LOS) GNSS satellite signals by localised reflected / diffracted signals, caused by objects such as trees, buildings, etc. As the multipath signals travel additional distances, they are delayed relative to the LOS signals, resulting in range measurements to the GNSS satellites being severely degraded. The multipath signals' paths are dependent on the reflecting surfaces and satellites' positions. As the satellites move with time, the multipath effect is also a variable of time. Multipath error is dependent on the architecture of GNSS receiver, in terms of the different ways the receivers deal with the signals (Gerdan *et al.*, 1995; Weill, 1997; Hannah, 2001; Kos *et al.*, 2010; Mekik & Can, 2010; Matsushita & Tanaka, 2012).

There are two categories of multipath; diffuse and specular. In diffuse multipath, GNSS signals are incident on a rough surface and the reflected signals are scattered in multiple directions. It is generally uncorrelated with time and noise-like in behaviour. In specular multipath, GNSS signals are reflected from a relatively smooth surface, resulting in systematic errors in range measurement (Hannah, 2001; Bilich & Larson, 2007; Mekik & Can, 2010; Yi *et al.*, 2012). Mutipath can also be categorised in terms of motion; static and dynamic. For a stationary GNSS receiver, the multipath geometry changes slowly, making multipath parameters essentially constant for up to several minutes. In mobile applications, the GNSS receiver can experience rapid fluctuations of multipath parameters which are hard to predict (Weiss, 1997; Nedic, 2009; Obst *et al.*, 2012; Matsushita & Tanaka, 2012).

A number of studies have been conducted to study the effect of multipath on GNSS performance (Gerdan *et al.*, 1995; Bilich & Larson, 2007; Kos *et al.*, 2010; Mekik & Can, 2010; Obst *et al.*, 2012; Matsushita & Tanaka, 2012; Yi *et al.*, 2012). These studies were conducted were via field evaluations using live GPS signals. However, such field evaluations are subject to various error parameters which are uncontrollable by users.

The ideal GNSS receiver evaluation 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 users. As the evaluations are conducted in controlled laboratory environments, they will not be inhibited by unwanted signal interferences and obstructions (Aloi *et al.* 2007; Dinesh *et al.* 2009; Petrovski *et al.* 2010; Kou & Zhang 2011; Pozzobon *et al.*, 2013). As part of the 10th Malaysian Plan Project (RMK10) entitled *Evaluation of the Effect of Radio Frequency Interference (RFI) on Global Positioning System (GPS) Signals via GPS Simulation* (January 2011 - May 2012), the Science & Technology Research Institute for Defence (STRIDE) employed GPS simulation to study the effect of RFI on GPS signals

(Dinesh *et al.*, 2012a, b).

In this study, GPS simulation is employed to study the effect of multipath on two handheld GPS receivers; Garmin GPSmap 60CSx (Garmin 2007) (evaluated GPS receiver) and Garmin GPSmap 60CS (Garmin 2004) (reference GPS receiver). Both GPS receivers employ the GPS L1 coarse acquisition (C/A) signal. The study is conducted based on important characteristics of GPS signal obstruction and multipath (Gerdan *et al.*, 1995; Weill, 1997; Hannah, 2001; Kos *et al.*, 2010; Mekik & Can, 2010; Matsushita & Tanaka, 2012):

i) Physical obstructions prevent certain GPS signals from reaching the GPS receiver, causing a reduction in number of visible GPS satellies
ii) Multipath signals that are reflected off physical obstructions have lower power levels as compared to unaffected GPS signals
iii) The effects of GPS signal obstruction and multipath can be correlated with GPS satellite elevation, with the effects being at a maximum during low elevations and improving for higher elevations.

2. METHODOLOGY

The apparatus used in the study were an Aeroflex GPSG-1000 GPS simulator (Aeroflex, 2010) and a notebook running GPS Diagnostics v1.05 (CNET, 2004). The study was conducted in STRIDE's mini-anechoic chamber (Kamarulzaman, 2010) to avoid external interference signals and multipath errors. The test setup employed is as shown in Figure 1. Simulated GPS signals were generated using the GPS simulator and transmitted via the coupler. The following assumptions were made for the tests conducted:

i) No ionospheric or troposheric delays
ii) Zero clock and ephemeris error
iii) No unintended obstructions or multipath
iv) No interference signals.

The date of simulation was set at 17 February 2013. The almanac data for the period was downloaded from the US Coast Guard's web site (USCG, 2012), and imported into the GPS simulator. The GPS signal power level was set at -130 dBm, while the coordinates were set at N 2° 58' E 101° 48' (Kajang, Selangor). For each GPS receiver, the test procedure was conducted for coordinated universal times (UTC) of 0000, 0300, 0600 and 0900.

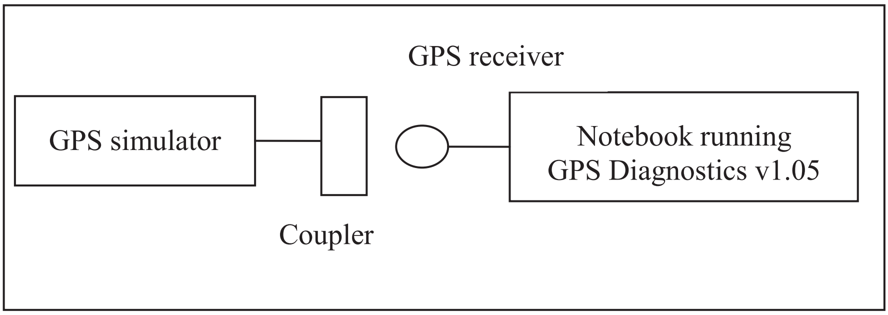


Figure 1: The test setup employed.

Trimble Planning (Trimble, 2013) was used to estimate GPS satellite coverage at the test area for the periods of the study in terms of position dilution of precision (PDOP) (Figure 2), represents the effect of GPS satellite geometry on 3D positioning precision. A PDOP value of 1 is associated with an ideal arrangement of the satellite constellation. To ensure high-precision GPS positioning, a PDOP value of 5 or less is usually recommended. In practice, the actual PDOP value is usually much less than 5, with a typical average value in the neighbourhood of 2 (DOD, 2001; USACE, 2003; Kaplan & Hegarty, 2006; Huihui *et al.*, 2008; Dinesh *et al.*, 2010). The GPS satellites visible at the start of each test period are shown in Table 1.

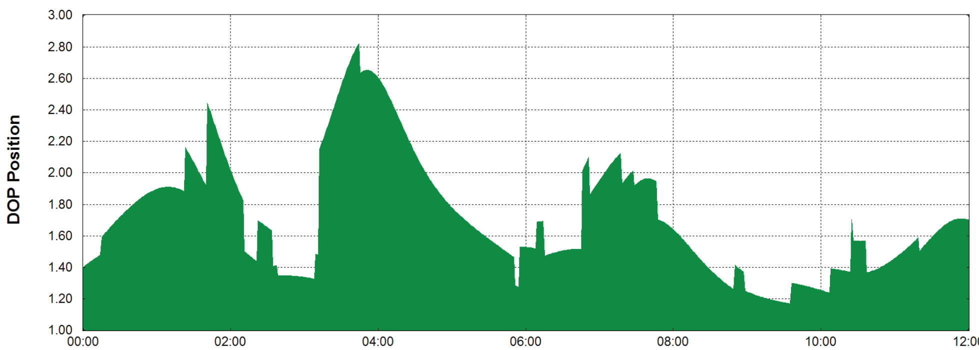


Figure 2: PDOP of GPS coverage at the test area for the period of the tests. (Source: Screen captures from Trimble Planning)

The GPS simulator does not provide specific multipath simulation. However, itdoes allow for selection of GPS satellites and signal power levels. Based on this, the study was conducted by assuming various conditions of physical obstructions and multipath signals (Table 2). It was assumed that each multipath signal underwent a reduction in power level of 15 dBm. For each reading, values of horizontal probable error (HPE), vertical probable error (VPE) and estimate probable error (EPE) were recorded for a period of 15 min.

Table 1: GPS satellites (SV) visible at the start of each test period. The satellites that are in bold have the highest elevations for each period and were selected for multipath simulation.

Time	Number of Satellites	SV	Elevation (°)	Azimuth (°)
0000	9	2	27.19	-5.94
		4	16.84	37.76
		5	**66.53**	**-65.31**
		9	18.02	-165.44
		10	34.35	21.12
		12	**34.49**	**-56.93**
		15	15.73	-157.92
		17	**37.53**	**98.91**
		26	**36.84**	**169.04**
		-	-	-
0300	10	2	32.17	87.93
		5	15.04	30.38
		9	**35.27**	**112.18**
		12	23.37	-161.44
		15	**74.99**	**-5.21**
		18	14.03	-80.58
		24	34.50	163.39
		25	20.14	-125.66
		26	**38.50**	**31.15**
		29	**47.29**	**-46.78**

Time	Number of Satellites	SV	Elevation (°)	Azimuth (°)
0600	8	12	21.84	120.39
		14	**34.04**	**-78.20**
		18	28.44	-6.876
		21	**69.51**	**-29.64**
		22	10.77	-36.41
		24	**38.72**	**40.96**
		25	26.46	157.55
		29	**29.12**	**-172.12**
		-	-	-
		-	-	-
0900	8	14	25.08	10.16
		16	12.63	-155.48
		18	**53.52**	**113.71**
		21	20.69	163.40
		22	**70.70**	**30.16**
		25	32.69	52.99
		30	**41.23**	**-161.73**
		31	**51.09**	**-59.47**
		-	-	-
		-	-	-

Table 2: Test scenarios used for the study.

Reading	Scenario	Number of Visible Satellites	Number of Multipath Signals
1	No physical obstructions or multipath, and hence, the full range of visible satellites are available.	8-10	0
2	Physical obstructions result in only four GPS satellites, with the highest elevations, being visible, but multipath does not occur.	4	0
3	Physical obstructions result in only four GPS satellites, with the highest elevations, being visible. Of the four available GPS signals, the signal from the satellite with the lowest elevation undergoes multipath.	4	1
4	Physical obstructions result in only four GPS satellites, with the highest elevations, being visible. Of the four available GPS signals, two signals from the satellites with the lowest elevations undergo multipath.	4	2
5	Physical obstructions result in only four GPS satellites, with the highest elevations, being visible. Of the four available GPS signals, three signals from the satellites with the lowest elevations undergo multipath.	4	3
6	Physical obstructions result in only four GPS satellites, with the highest elevations, being visible, with all the signals undergoing multipath.	4	4

3. RESULTS & DISCUSSION

As observed in Table 3, and Figures 3 and 4, the decrease in number of visible satellites due to physical obsructions and increase in number of multipath signals caused increase in probable error values. This is due to decreasing carrier-to-noise density (C/N_0) levels for GPS satellites tracked by the receiver, which is the ratio of received GPS signal power level to noise density. Lower C/N_0 levels result in increased data bit error rate when extracting navigation data from GPS signals, and hence, increased carrier and code tracking loop jitter. This, in turn, results in more noisy range measurements and thus, less precise positioning (DOD, 2001; USACE, 2003; Kaplan & Hegarty, 2006; Petovello, 2009). The tests conducted in this study employed GPS signal power level of-130 dBm. Usage of lower GPS signal power levels would result in reduced C/N_0 levels and hence, higher rates of increase of probable error values.

Table 3: Recorded average probable error values.

Time	Number of Visible Satellites	Number of Multipath Signals	Probable Error (m)					
			Evaluated			Reference		
			HPE	VPE	EPE	HPE	VPE	EPE
0000	9	0	2.31	4.01	4.63	7.23	13.57	15.37
	4	0	4.81	8.28	9.58	13.71	25.47	28.92
	4	1	6.39	9.43	11.39	13.84	25.68	29.17
	4	2	7.90	11.21	13.71	13.86	25.78	29.27
	4	3	8.20	11.56	14.17	13.88	25.80	29.30
	4	4	8.20	13.16	15.51	13.90	25.84	29.35
0300	10	0	2.10	3.42	4.01	6.70	11.50	13.31
	4	0	4.19	7.66	8.73	14.29	19.34	24.04
	4	1	6.74	10.43	12.42	14.36	19.37	24.11
	4	2	8.32	11.91	14.53	14.53	19.58	24.38
	4	3	8.88	11.82	14.78	14.73	19.81	24.68
	4	4	9.32	12.02	15.21	14.83	20.11	24.98
0600	8	0	2.36	3.79	4.46	7.69	11.84	14.13
	4	0	3.59	5.56	6.63	11.39	16.66	20.21
	4	1	3.68	8.58	9.35	11.39	16.72	20.26
	4	2	4.91	8.90	10.19	11.42	16.95	20.46
	4	3	5.93	8.95	10.82	11.49	17.58	21.02
	4	4	6.48	9.23	11.30	11.57	17.89	21.33
0900	8	0	2.70	3.48	4.40	7.72	11.97	14.24
	4	0	5.01	10.53	11.66	13.59	25.41	28.83
	4	1	5.63	12.38	13.61	13.93	26.29	29.79
	4	2	6.97	13.53	15.23	14.24	26.73	30.31
	4	3	8.28	13.89	16.19	14.03	27.53	30.92
	4	4	9.88	13.81	17.00	14.50	28.04	31.60

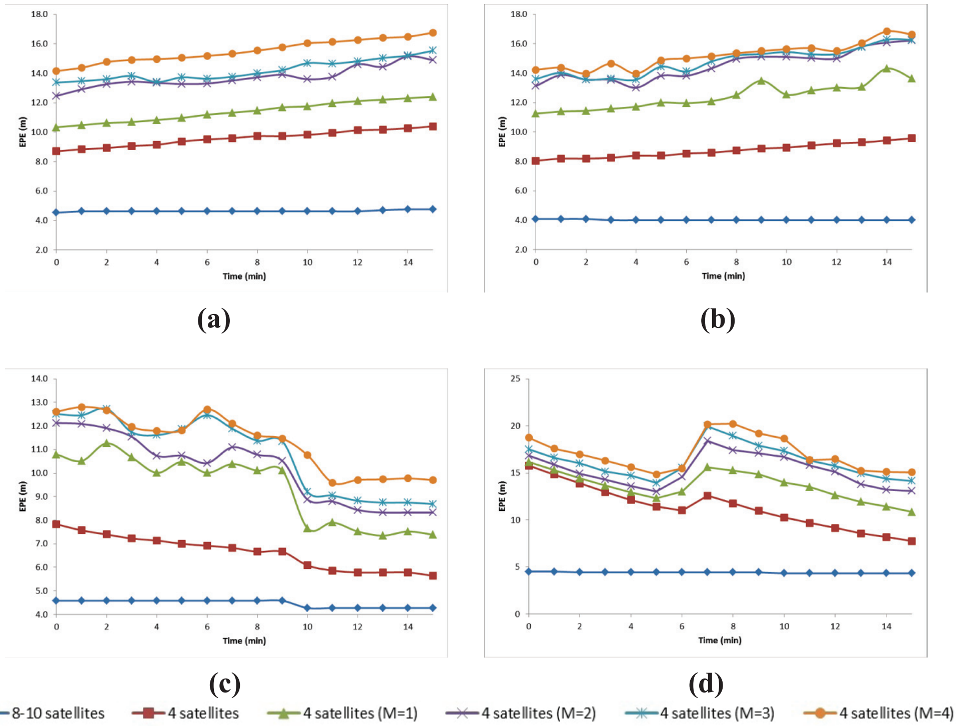


Figure 3: Recorded EPE values for the evaluated GPS receiver at UTC times of: (a) 0000, (b) 0300, (c) 0600 and (d) 0900. M is the number of multipath signals.

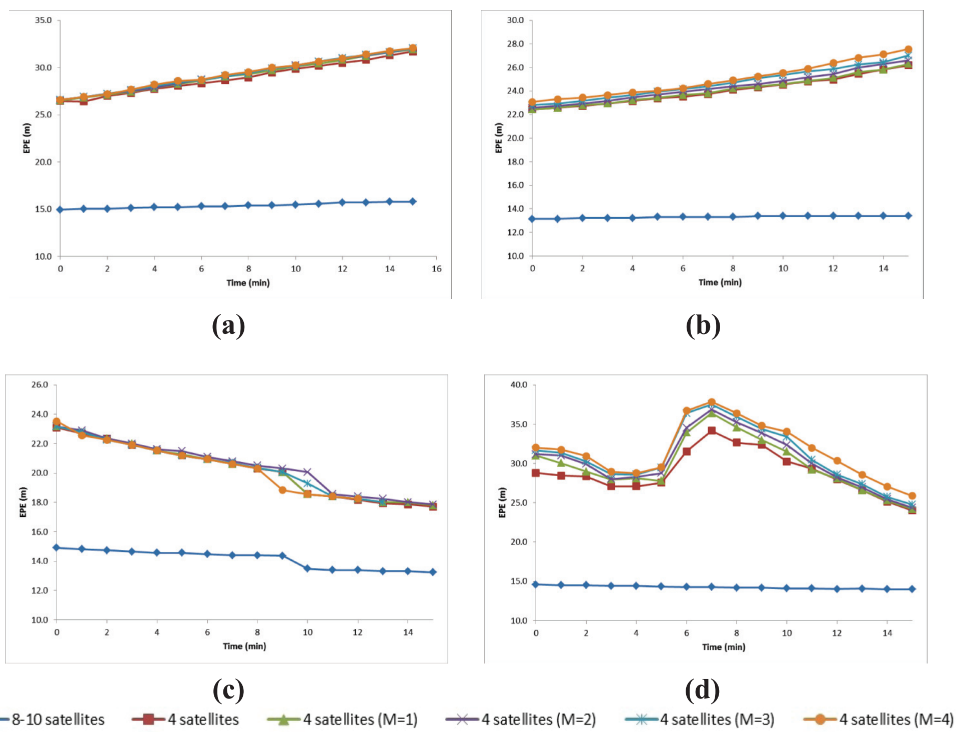


Figure 3: Recorded EPE values for the reference GPS receiver at UTC times of: (a) 0000, (b) 0300, (c) 0600 and (d) 0900. M is the number of multipath signals.

For all the readings, the evaluated GPS receiver recorded lower probable error values as compared to the reference GPS receiver. This occurred as the evaluated GPS receiver has higher receiver sensitivity, and hence, is able to obtain lower PDOP values. In addition, it has lower receiver noise, reducing the value of its user equivalent ranging error (UERE), which is the total expected magnitude of position errors due to measurement uncertainties from the various error components for a particular receiver (DOD, 2001; USACE, 2003; Kaplan & Hegarty, 2006). For the evaluated GPS receiver, for each reading, with the introduction of physical obstructions and iterative addition of multipath signals, its probable error values progressively increased. For the reference GPS receiver, while there is an increase in probable error values after the introduction of physical obstructions, subsequent additions of multipath signals did not cause much differences, as the probable errors at this point are significantly large.

It is observed that for all the readings, the values of VPE were larger than HPE, as GPS receivers can only track satellites above the horizon, resulting in GPS height solution being less precise than the horizontal solution (DOD, 2001; USACE, 2003; Kaplan & Hegarty, 2006; Huihui *et al.*, 2008; Dinesh *et al.*, 2010). The differences between VPE and HPE values were significantly larger for the reference GPS receiver as compared to the evaluated GPS receiver. The reference GPS receiver, having lower receiver sensitivity, has much better horizontal component accuracy as compared to the vertical component. For the evaluated GPS receiver, with higher receiver sensitivity, while the horizontal component accuracy is still larger, the difference with the vertical component is much smaller. The reduction in number of visible satellites due to the introduction of physical obstructions caused increase in the differences between HPE and VPE values (Table 4), due to the removal of satellites above the horizon, while overhead satellites are maintained.

Varying probable error patterns are observed for each of the readings. This is due to the GPS satellite constellation being dynamic, causing varying GPS satellite geometry over time, resulting in GPS accuracy being time dependent (DOD, 2001; USACE, 2003; Kaplan & Hegarty, 2006; Huihui *et al.*, 2008; Dinesh *et al.*, 2010). Multipath is highly repeatable as it is the same when the GPS satellites are in the same positions during each orbital pass (approximately 11 min, 58 s). This repeatability can be used to build a history of multipath occurances over time, which can then be used to generate multipath corrections for stationary sites (Gerdan *et al.*, 1995; Weill, 1997; Hannah, 2001; Kos *et al.*, 2010; Mekik & Can, 2010).

Table 4: Differences between average recorded HPE and VPE values for the readings taken.

Time	Number of Visible Satellites	Number of Multipath Signals	Difference Between Average HPE and VPE Values (m)	
			Evaluated	Reference
0000	9	0	1.70	6.34
	4	0	3.47	11.76
	4	1	3.04	11.84
	4	2	3.31	11.92
	4	3	3.36	11.92
	4	4	4.96	11.94
0300	10	0	1.32	4.80
	4	0	3.47	5.05
	4	1	3.69	5.01
	4	2	3.59	5.05
	4	3	2.94	5.08
	4	4	2.70	5.28
0600	8	0	1.43	4.15
	4	0	1.97	5.28
	4	1	4.89	5.33
	4	2	3.99	5.53
	4	3	3.02	6.09
	4	4	2.75	6.33
0900	8	0	0.77	4.25
	4	0	5.51	11.82
	4	1	6.76	12.36
	4	2	6.56	12.49
	4	3	5.61	13.50
	4	4	3.93	13.54

4. CONCLUSION

Based on the results of this study, it was found that the decrease in number of visibles satellites due to physical obsructions and increase in number of multipath signals caused increase in probable error values, due to decreasing C/N_0 levels for GPS satellites tracked by the receiver. In addition, the differences between HPE and VPE values increased due to the removal of satellites above the horizon, while overhead satellites were maintained. Varying probable error patterns were observed for readings taken at different times. This is due to the GPS satellite constellation being dynamic, causing varying GPS satellite geometry over time, resulting in GPS accuracy being time dependent. The repeatability of multipath at stationary sites when GPS satellites are in the same positions during each orbital pass allows for corrections to be generated based on history of multipath occurances over time. The proposed scope of future work is for the extension of this study for dynamic multipath propagation.

REFERENCES

Aeroflex (2010). *Avionics GPSG-1000 GPS / Galileo Portable Positional Simulator*. Aeroflex Inc., Plainview, New York.

Bilich, A. & Larson, K.M. (2007). Mapping the GPS multipath environment using the signal-to-noise ratio (SNR). *Radio Sci.*, **42**: RS6003.

Aloi, D.N., Alsliety, M. & Akos, D.M. (2011). A methodology for the evaluation of a GPS receiver performance in telematics applications. *IEEE T. Instrum. Meas.*, **56**: 11-24.

CNET (2004). *GPSDiag 1.0*. Available online at:

http://download.cnet.com/GPSDiag/3000-2130_4-4951103.html (Last access date: 31 January 2010).

Department of Defence (DOD) (2001). *Global Positioning System Standard Positioning Service Performance Standard*. Command, Control, Communications, And Intelligence, Department of Defence (DOD), Washington D.C.

Dinesh, S. (2009). Vulnerabilities of civilian Global Navigation Satellite Systems (GNSS) signals: A review. *Defence S&T Tech. Bull.*, **2**: 100-114.

Dinesh, S. (2011). Vulnerabilities of Global Navigation Satellite Systems (GNSS) signals to jamming and spoofing. *GIS Day 2011*, 17 March 2011, Universiti Putra Malaysia (UPM), Serdang, Selangor.

Dinesh , S., Wan Mustafa, W.H., Mohd Faudzi., M., 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**: 6-10.

Dinesh , S., Wan Mustafa, W.H., Mohd Faudzi., M., Kamarulzaman, M., Hasniza, H., Nor Irza Shakhira, B., Siti Robiah, A., Shalini, S., Jamilah, J., Aliah, I., Lim, B.T., Zainal Fitry, M.A., Mohd. Rizal, A.K., Azlina, B. & Mohd. Hasrol, H.M.Y. (2010). Evaluation of the effect of radio frequency interference (RFI) on Global Positioning System (GPS) accuracy. *Defence S&T Tech. Bull.*, **3**: 100-118.

Dinesh, S., Mohd Faudzi., M., Rafidah, M., Nor Irza Shakhira, B., Siti Robiah, A., Shalini, S., Aliah, I., Lim, B.T., Zainal Fitry, M.A., Mohd. Rizal, A.K., & Mohd Hasrol, H.M.Y. (2012). Evaluation of the effect of radio frequency interference (RFI) on the Global Positioning System (GPS) L1 coarse acquisition (C/A) signal via GPS simulation. *11th International Symposium & Exhibition on Geoinformation 2012 (ISG2012)*, 25-26 September 2012, Hotel Istana Kuala Lumpur City Centre, Kuala Lumpur.

Dinesh, S., Mohd Faudzi., M. & Zainal Fitry, M.A. (2012b). Evaluation of the effect of radio frequency interference (RFI) on Global Positioning System (GPS) accuracy via GPS simulation. *Defence Sci. J.*, **62**: 338-347.

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

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

Gerdan, G.P., Coombe, L.J. & Takac, F. (1995). *The Effects of RF Interference, Multipath* *and Signal Obstruction on the GPS Observables*. Department of Land Information, Royal Melbourne Institute of Technology (RMIT), Melbourne, Victoria.

Hannah, B. (2001). *Modelling and Simulation of GPS Multipath Propagation*. PhD Dissertation, Queensland University of Technology, Brisbane, Queensland.

Huihui, W., Xingqun, Z. & Yanhua, Z. (2008). Geometric dilution of precision for GPS single-point positioning based on four satellites. *J. Syst. Eng. Electr.*, **19**: 1058-1063.

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

Kamarulzaman, M. (2010). *Technical Specification for STRIDE's Mini-Anechoic Chamber*. Science & Technology Research Institute for Defence (STRIDE), Ministry of Defence, Malaysia.

Kos, T., Markezic, I. & Pokrajcic, J. (2010). Effects of multipath reception on GPS positioning performance. *52nd International Symposium ELMAR-2010*, 15-17 September 2010, Zadar, Croatia.

Kou, Y. & Zhang, H. (2011). Verification testing of a multi-GNSS RF signal Simulator. *Inside GNSS*, **6**: 52-61.

Last, D. (2010). GNSS: The present imperfect. *Inside GNSS*, **5**: 60-64.

Matsushita, T. & Tanaka, T. (2012). Study on improving the accuracy of satellite measurement in urban areas. *T. Soc. Instrumen. Control Eng.*, **48**: 73-77.

Mekik, C. & Can. O. (2010). Multipath effects on RTK GPS and a case study. *2010 International Symposium on GPS / GNSS*, 26-28 October 2010, Taipei, Taiwan.

Nedic, S. (2009). On GPS signal multipath modelling in dynamic environments. *2009 IEEE Aerospace Conference*, 7-14 March 2009, Big Sky, Montana.

Obst, M., Bauer, S. & Wanielik, G. (2012). Urban multipath detection and mitigation with dynamic 3D maps for reliable land vehicle localization. *2012 IEEE/ION Position Location and Navigation Symposium (PLANS)*, 23-26 April 2012, Myrtle Beach, South Carolina.

Pasetti, A. & Giulicchi, L. (1999). Experimental results on three multipath compensation techniques for GPS-based attitude determination. *21st Annual AAS Guidanceand Control Conference*, 3-7 February 1999, Breckenridge, Colorado.

Petovello, M. (2009). Carrier-to-noise density and AI for INS / GPS integration. *Inside GNSS*, **4**: 20-29.

Petrovski, I., Townsend, B. & Ebinuma, T. (2010). Testing multi-GNSS equipment: Systems, simulators and the production pyramid. *Inside GNSS*, **5**: 52-61.

Pozzobon, O., Sarto, C., Chiara, A.D., Pozzobon, A., Gamba, G., Crisci, M. & Ioannides, R. (2013). Developing a GNSS position and timing authentication testbed: GNSS vulnerability and mitigation techniques. *Inside GNSS*, **8**: 45-53.

Royal Academy of Engineering (RAE) (2011). *Global Navigation Space Systems: Reliance and Vulnerabilities*. Royal Academy of Engineering, London.

Schue, C. (2012). The challenges of realizing a global navigation capability. *ION International*

Technical Meeting (ITM) 2012, 30 January - 1 February 2012, Newport Beach, California.

Schwartz, N. (2010). The United States as an aerospace nation: Challenges and opportunities. *Tuft University Institute for Foreign Policy Analysis (IFPA) Fletcher Conference on National Security Strategy and Policy*, 20-21 January 2010, The Ronald Reagan Building and International Trade Center, Washington, D.C.

Trimble (2013). *Trimble's Planning Software*. Available online at:

http://www.trimble.com/planningsoftware.shtml (Last access date: 21 February 2013).

US Army Corps of Engineers (USACE) (2003). *NAVSTAR Global Positioning System Surveying. Engineer Manual*. EM 1110-1-1003, US Army Corps of Engineers (USACE), Washington D.C.

US Coast Guard (USCG) (2012). *GPS NANUs, Almanacs, & Ops Advisories*. Available online at:

http://www.navcen.uscg.gov/?pageName=gpsAlmanacs (Last access date: 21 February 2013).

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.

Weill, L.R. (1997). Conquering multipath: The GPS accuracy battle. *GPS World*, **April 1997**: 59-66.

Yi, T.H., Li, H.N. & Gu, M. (2012). Effect of different construction materials on propagation of GPS monitoring signals. *Measurement*, **45**: 1126-1139.

CATCH OF THE NET

Climate change refers to significant changes in measures of climate lasting for an extended periods of time. It includes major changes in temperature, precipitation or wind patterns, among other effects, that occur over several decades or longer. Among the factors causing it include oceanic processes, variations in solar radiation, plate tectonics and volcanic eruptions, and human-induced alterations of the natural world. Climate change has become a major, overriding environmental issue with economic, health and safety, food production and security dimensions. For example, shifting weather patterns threaten food production through increased unpredictability of precipitation, while rising sea levels contaminate coastal freshwater reserves, and increase the risk of catastrophic flooding. Over the past century, global average temperatures have risen by 0.8° C (which can give a maximum rise of up to 7 °C) , while sea levels have risen by 20-30 cm. These changes have led to alterations in climate extremes such as heat waves, record high temperatures and, in many regions, heavy precipitation. The effects of these changes are further exacerbated by the increase in density of populations, particularly in areas most vulnerable to climate change. Although the environmental and social factors that influence the risk of disasters vary from region to region, many of the effective strategies for dealing with climate change are similar. The following are relatively interesting and useful websites on climate change and its impact:

1) **National Aeronautics & Space Administration (NASA)**
   http://climate.nasa.gov

2) **United States Environmental Protection Agency (EPA): Climate Change**
   http://www.epa.gov/climatechange

3) **Natural Resources Defense Council (NRDC): Global Warming**
   http://www.nrdc.org/globalwarming

4) **The Guardian: Climate Change**
   http://www.guardian.co.uk/environment/climate-change

   Encyclopaedias on the causes and effects of climate change and solutions.

5) **New Scientist: Climate Change - Timeline**
   http://www.newscientist.com/article/dn9912-timeline-climate-change.html

   Provides a timeline of major events and occurrences in regards to climate change.

6) **Intergovernmental Panel on Climate Change (IPCC)**
   http://www.ipcc.ch

   IPCC is a scientific intergovernmental body that provides comprehensive scientific assessments about the risks of climate change, and possible options for mitigating the effects.

7) **Defence Scientific Advisory Council: Defence in a Changing Climate**
   http://www.mod.uk/NR/rdonlyres/44EC5708-7C49-4E69-AD50-1F516DFE47A7/0/DefenceinaChangingClimateDSACReport.pdf

8) **The CNA Corporation: National Security and the Threat of Climate Change**
   http://www.cna.org/reports/climate

9) **International Institute for Sustainable Develoment (IISD)**
   http://www.iisd.org/ecp/es/climate

   Reports assessing the effects of climate change on defence & security.

10) **E&T: Climate Change - Engineering a Solution**
    http://eandt.theiet.org/magazine/2012/11

    The November 2012 edition of the E&T periodical focused on engineering solutions for climate change.